ThreatQuotient

ThreatQ User Guide

Version 5.11.0

February 02, 2023

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

Support

Email: support@threatq.com
Web: support.threatq.com
Phone: 703.574.9893

Warning and Disclaimer

Contents

About the ThreatQ Platform

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

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.

Accessing the Platform

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.

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* section of the Managing User Accounts 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.

Authentication Methods

There are multiple authentication methods you can implement to secure access to the ThreatQ Platform (TQ):

METHOD	DESCRIPTION	REFERENCE
Local Authentication	User accounts are created and maintained manually within 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 method for the ThreatQ platform - see Local Login.	• User Management • Accessing the Platform
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 Local Login.	• 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 Authentication

METHOD	DESCRIPTION	REFERENCE
	SAML users will log in using the single sign-on (SSO) login option for the ThreatQ platform - see SSO Log In.	
SSL Client Certificate Authentication	User accounts are created in the ThreatQ platform. Then, the individual users or Administrative/Maintenance user can add a certificate fingerprint to the user account. These certificate fingerprints are validated agains a certificate file uploaded to ThreatQ. SSL Client Certificate Authentication users will login using the **Log in with CAC/PIV Card** option - see SSL Client Certificate Authentication Log In	• SSL Client Certificate 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 SSO Login. 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.

CURRENT METHOD	NEW METHOD	DETAILS
		⚠ 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 Local Login. 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 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.
SAML or LDAP	**SSL Client Certificate Authentication**	If you want to migrate from LDAP or SAML authentication to SSL Client Certificate

CURRENT METHOD	NEW METHOD	DETAILS
		Authentication, please contact ThreatQ Support for assistance.
Local	**SSL Client Certificate Authentication**	See SSL Client Certificate Authentication.
SSL Client Certificate Authentication	**Local**	See Managing Certificate Files.

Platform Login

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

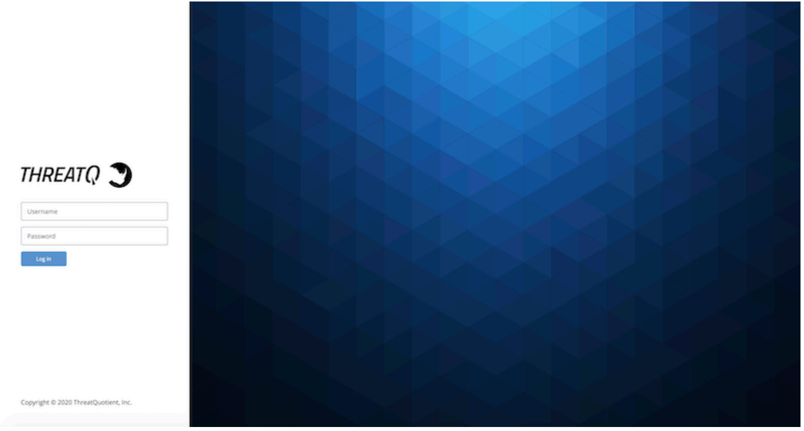
There are multiple methods that can be used to log into your ThreatQ instance:

- Local Log In
- Single Sign-On (SSO)
- SSL Client Certificate Authentication Log In

Local Log In

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

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



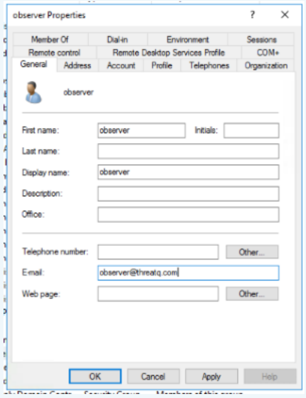
2. Enter your username (email address) and password.
3. Optionally, if you have 2-step verification enabled, complete the following steps:
    - Enter your verification code from Google Authenticator.
    - Optionally, choose to **Remember this computer for 30 days**.
4. Click **Login** or **Submit**.

Single Sign-On (SSO)

> At this time, ThreatQ does not support IdP-initiated SSO, where a user can log in directly from an SSO provider's portal such as Okta's Portal. Users utilizing SSO must

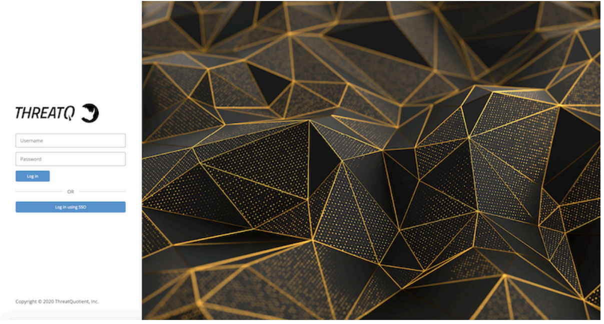
click the **Log In Using SSO** button on the ThreatQ landing page to authenticate with their IdP.

Users using SAML authentication 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.
>
> 
>
>
> First name: observer
>
> Display name: observer
>
> E-mail: observer@threatq.com

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 the **Log in Using SSO** button.

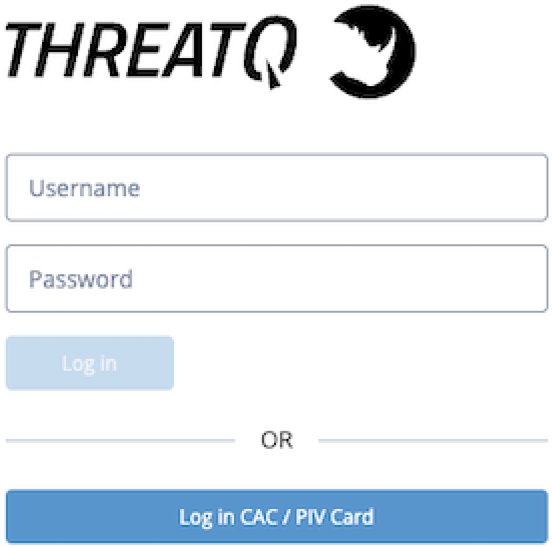
   You will navigate to your third-party authenticated site to log in. Once that has been completed, you will be automatically sent back to the ThreatQ instance.

SSL Client Certificate Authentication Log In

> Maintenance users can log into ThreatQ using either username/password or certificate authentication. Administrative, Primary Contributor, and Read-Only users are required to use certificate authentication to log into ThreatQ if it is enabled.

After SSL Client Certificate Authentication is configured and you have added a certificate fingerprint to your user profile, you can use the following login method.

1. Access your certificate, and enter your PIN. Your certificate must be active in the browser before you navigate to your ThreatQ instance.
2. Navigate to your ThreatQ instance - `https://your-ThreatQ-web-ip-address`.



3. Click the **Log in CAC/PIV Card** button.

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.

> You will need an authenicator app that supports the scanning of QR codes to utilize this feature. Apps such as Microsoft and Google Authenticator are recommended.

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

Enabling 2-Step Verification

1. Click on your avatar icon, located to the top-right of the platform, and select **My Account**.
2. Under Enable 2-Step Verification, click **Enabled**.
3. In the Enable 2 Step Verification dialog box, complete the following:
   a. Scan the QR code using a mobile app such as Google or Microsoft Authenicator.
   b. Enter the validation code delivered to your mobile device via your authenticator.
   c. Click **Submit**.
4. Click **Save**.

What to do next

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

Air Gapped Data Sync (AGDS)

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.

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.

Air Gapped Data Sync (AGDS) and Investigation Sharing

The AGDS export process does not include data collections or dashboards, but it can include investigations if the following command is included and set to Y:

```
--include-investigations=Y
```

The AGDS export/import process transfers users from an outside system to an air-gapped system, but only for the purpose of maintaining them as sources. These users are automatically disabled on the air-gapped system. As such any permissions assigned to these users will be invalid on the air gapped system, so permissions are not transferred as part of the AGDS export process.

When you run the AGDS import process on the target box, ownership of any new investigation is assigned to the most recently created admin or super user. This owner is responsible for assigning permissions to other users on the air-gapped system. The import process does not apply any changes to existing permissions even if the investigation receives updates.

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 Parameters: section of the threatq:sync-export topic.

```
sudo ./artisan threatq:sync-export
```

4. Review the Output and Sync report; see the Output and Sync Report section of the threatq:sync-export topic.

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:

```
sudo ./artisan threatq:sync-import
```

4. Review the Output and Sync report; see threatq sync-imprt File Output and Sync Report.

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.

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
`--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

PARAMETER	EXPLANATION
	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 regardless of the use of this flag. Default: Y **Example:** --override-description=N

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.

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.

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.

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>.

> 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.

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)

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).

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"

> 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.

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).

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.

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. **Example:** --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. **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

PARAMETER	EXPLANATION
	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
`--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"

PARAMETER	EXPLANATION
--sources	Filter objects produced in the sync by which sources they include, allowing the user to send out a subset of data that contains their specified source. For objects with multiple sources, other sources will be included in the filter if the object contains the user-specified source(s). Multiple sources are also supported in search parameters. **Existing CRON Runs:** Use the `initial-start-date` option to avoid pulling all historical data. **Example**: --sources=“Black Source”

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).

Initial Cron for First Time Use

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" --target=/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.

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.

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.

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"`.

Output and Sync Report

The following sections detail the data you may find in the export output and sync report.

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

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 Actions
- 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

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

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

File Output

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` tqSync-19-01-16-1547649934-0849.tar.gz

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.

Command Line Output

Command line output displays command progress, object totals, and files written.

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).

Upgrading an Air Gapped ThreatQ Instance

If you are upgrading from the most recent ThreatQ 4x release to 5x, you must contact ThreatQ support for assistance with the upgrade process.

> ⚠ ThreatQ requires you to be on the latest version of 4x in order to upgrade to ThreatQ version 5x.

If you are upgrading from the most recent ThreatQ 4x release to 5x, or are upgrading from one 5x release to another, you can use the following steps.

> Contact ThreatQ Support if you encounter any issues during the upgrade or require assistance.

Stage 1: Download the Air Gap Upgrade File

To download the air gap upgrade file from a browser:

1. Log into https://install.threatq.com/ using your YUM credentials.
2. Locate and download the appropriate air gap upgrade file.
   File Name Format:
   <version>-platform.tar.gz
   Example:
   5.6.1-platform.tar.gz
3. Open the CLI of the device to upgrade and copy the upgrade file to `/root/` using the SCP client of your choice.
4. Return to the CLI of the device and confirm that the upgrade file is present.

To download the air gap upgrade file via curl:

1. Run the following command:

   ```
   curl https://<YUM_USER>:<YUM_PASSWORD>@install.threatq.com/
   <version>-platform.tar.gz -o <version>-platform.tar.gz
   ```

2. Transfer the upgrade file to `/root/` on the air gapped box.

Stage 2: Upgrade the Air Gapped Box

1. Log into the air gapped box as a root user.
2. Run the following command to upgrade the air gapped box:

   ```
   tqadmin platform upgrade -v <release number> -z
   ```

   Example:

   > tqadmin platform upgrade -v 5.6.1 -z

3. The upgrade process looks for the upgrade tarball in the `/root/` location. If the file is not in that location, you are prompted to enter the absolute path of the tarball.

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.

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.

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: **5x command**

```
php artisan threatq:restore </path/to/backup_file>
```

4x 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 section below before executing CLI commands.

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 commands will indicate if the command will automatically place the ThreatQ application into maintenance mode.

Placing the ThreatQ Application into Maintenance Mode

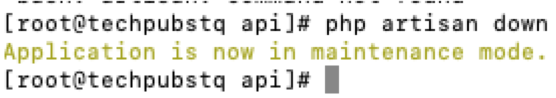
1. SSH to your ThreatQ installation.
2. Navigate to the api directory using the following command:

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

3. Run the following command:

```
sudo php artisan down
```

The platform will now be in maintenance mode.



```
[root@techpubstq api]# php artisan down
Application is now in maintenance mode.
[root@techpubstq api]#
```

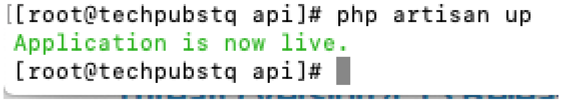
Taking the ThreatQ Application out of Maintenance Mode

> 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.



```
[[root@techpubstq api]# php artisan up
 Application is now live.
 [root@techpubstq api]#
```

Commands

This topic contains a list of useful CLI commands.

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
```

System ThreatQ Purge

> ⚠ Read this section 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

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.

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 section.

4. Run the following command:

```
sudo php artisan threatq:purge-threat-intelligence
```

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 section.

Add/Upgrade CDF

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:

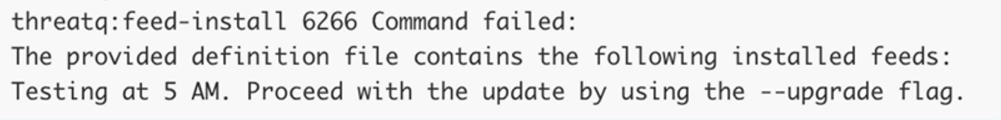
```
cd /var/www/api
```

3. Place the application into maintenance mode - see the Maintenance Mode section.

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 section.

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
```

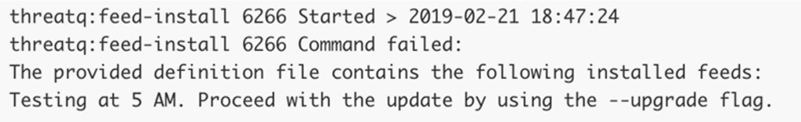
3. Place the application into maintenance mode - see the Maintenance Mode section.
4. Run the following command:

```
sudo php artisan threatq:feed-install <Feed Definition File>
--upgrade
```

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

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 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.
```

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
```

Source Consolidation

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

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 become 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 section.
4. Run the following command:

```
sudo php artisan threatq:merge-sources --origin-source=“<source a>” --destination-source=“<source b>”
```

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

Example Scenarios:

SCENARIO	DETAILS
Merge user-created source (origin source) with a system source (destination source).	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.

SCENARIO	DETAILS
	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. The user receives a command success message. 8. The user brings the platform out of maintenance 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. The 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 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.

SCENARIO	DETAILS
	9. The platform will record the source merge in the audit log for affected data. 10. The user receives a command success message. 11. The 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 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. The user receives a command success message. 8. The user brings the platform out of maintenance mode.

Historic Pull

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
```

Merge Attributes

The Merge Attributes command allows you to merge an existing attribute to a new or different existing attribute name. This is useful in the case that an attribute key is outdated or entered incorrectly.

> If the `MERGE-NAME` attribute in the command does not exist, it will be automatically created upon executing the command.

You can also filter the command to only merge attributes that have a specific source(s) using an optional `--source` argument. If the source identified in the command does not exist, or the argument is not included, the command will merge all `OLD-NAME` attributes into `MERGE-Name`.

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 threatq:merge-attributes --old-name='OLD-NAME' --merge-name='MERGE-NAME' --source='SOURCE'
```

> The `--source` argument is optional. You can omit this parameter in order to target all attributes with the `OLD-NAME`.

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

Example - Merge Attribute without using --source option

```
sudo threatq:merge-attributes --old-name='Cuontry' --merge-name='Country'
```

In the example above, the attribute `Cuontry` would be merged into the `Country` attribute. So if you have an any instance of this attribute name (with value), `Cuontry: US`, on an object, after running the command, the attribute value would appear as `Country: US` on that object.

Example - Merge Attribute using --source option

```
sudo threatq:merge-attributes --old-name='Cuontry' --merge-name='Country' --
source='CrowdStrike'
```

In the example above, the attribute `Cuontry` , if it has a source of `CrowdStrike`, would be merged into the `Country` attribute. So if you have an instance of this attribute name (with value), `Cuontry: US`, on an object, after running the command, the attribute value would appear as `Country: US` on that object.

Example - Merge Attribute using --source option (multiple sources)

```
sudo threatq:merge-attributes --old-name='Cuontry' --merge-name='Country' --
source='CrowdStrike' --source='McAfee ATD'
```

In the example above, the attribute `Cuontry` , if it has a source of `CrowdStrike` or `McAfee ATD`, would be merged into the `Country` attribute. So if you have an instance of this attribute name (with value), `Cuontry: US`, on an object, after running the command, the attribute value would appear as `Country: US` on that object.

iSight Historic Pull

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
```

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.

Reset User Password

> 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.

Update TLP Designations

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

> See Traffic Light Protocol (TLP) 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

Use the following command to update all object sources and object attribute sources that have Traffic Light Protocol (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 section.
4. Run the following command:

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

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

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.

View Feed Queues

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.

Airgap Import

See the threatq:sync-import topic.

Airgap Export

See the threatq:sync-export topic.

LDAP Diagnostic Searches

This command runs LDAP diagnostic searches for authentication and authorization using the LDAP configuration stored in the database. Methods for searching are contained in try/catch blocks so that stack traces are printed to the debug output. You can run this command with or without the `--test-user` parameter. This parameter allows you to use a known username on the LDAP server to test authentication and group searching.

> The test connection and bind aspects of this command work for the anonymous LDAP configuration. However, all other aspects, including test user authentication and group searching, only work with the authenticated bind LDAP configuration.

> ⚠ This command has only been tested and confirmed for use with AD server configurations.

To perform basic connect and bind authentication tests:

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:

```
<> php artisan threatq:ldap-debug
```

To perform basic connect and bind authentication as well as authentication with the test username:

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:

```
<> php artisan threatq:ldap-debug --test-user=username
```

EX php artisan threatq:ldap-debug --test-user=administrator

4. When prompted, enter the username's password.
   Regardless of whether authentication is successful, an attempt is made to pull the LDAP user entry for the username. If authentication is successful, a group search (authorization) is performed as well.

Allow Cross-Origin Resource Sharing for Specific Hostnames

ThreatQ's explicit domain access restrictions prevent cross-origin resource sharing (CORS) attacks. This allows API requests from ThreatQ and third-party integrations but blocks cross-origin JavaScript requests unless you use the following command to specifically configure a list of allowed hosts.

1. SSH to your ThreatQ installation.

2. Run the following command:

```
<> sudo /var/www/api/artisan threatq:configuration --
   key=cors.allowed_hosts --value https://www.site-a.com,https://
   www.site-b.com
```

The value parameter allows you to enter a single domain or multiple domains separated by a comma.

EX **Single Domain:**
sudo /var/www/api/artisan threatq:configuration --key=cors.allowed_hosts --value https://www.example.com

EX **Multiple Domains:**
sudo /var/www/api/artisan threatq:configuration --key=cors.allowed_hosts --value https://www.example.com,https://www.my-allowed-host.com

Disable Export Logging

The exports.disable_logging configuration option allows you to disable export logging. However, if a differential parameter is included as a URL parameter. the export logging process continues regardless of this configuration.

1. SSH to your ThreatQ installation.
2. Run the following command to disable export logging:

```
sudo /var/www/api/artisan threatq:configuration --key exports.disable_logging --value 1
```

3. To turn logging back on, run the following command:

```
sudo /var/www/api/artisan threatq:configuration --key exports.disable_logging --value 0
```

Delete Adversary Descriptions

The `adversary-descriptions-cleanup` command allows you to delete duplicated `adversary_descriptions` and orphaned `adversary_description_values`.

By default, the `adversary-descriptions-cleanup` command deletes 1,000 adversary descriptions at a time. If there are performance concerns with deleting this many adversaries at a time, you can use the optional `delete-limit` parameter to specify an integer value as the limit for the number of adversary descriptions deleted at a time. For example, you can run the command with a `delete-limit` of 100 to delete 100 orphaned/duplicate adversary descriptions at a time.

> Setting the `delete-limit` too high may hinder performance.

1. SSH to your ThreatQ installation.
2. To delete adversary descriptions in batches of 1,000, run the following command:

```
sudo /var/www/api/artisan threatq:adversary-descriptions-cleanup
```

3. To specify the number of adversary descriptions to be deleted at a time, run the following command:

```
<> sudo /var/www/api/artisan threatq:adversary-descriptions-
   cleanup --delete-limit number
```

The **number** variable above represents the maximum number of adversary descriptions you want to delete at a time. The following example command deletes a maximum of 100 adversary descriptions at a time.

> EX sudo /var/www/api/artisan threatq:adversary-descriptions-cleanup --delete-limit 100

Dashboards

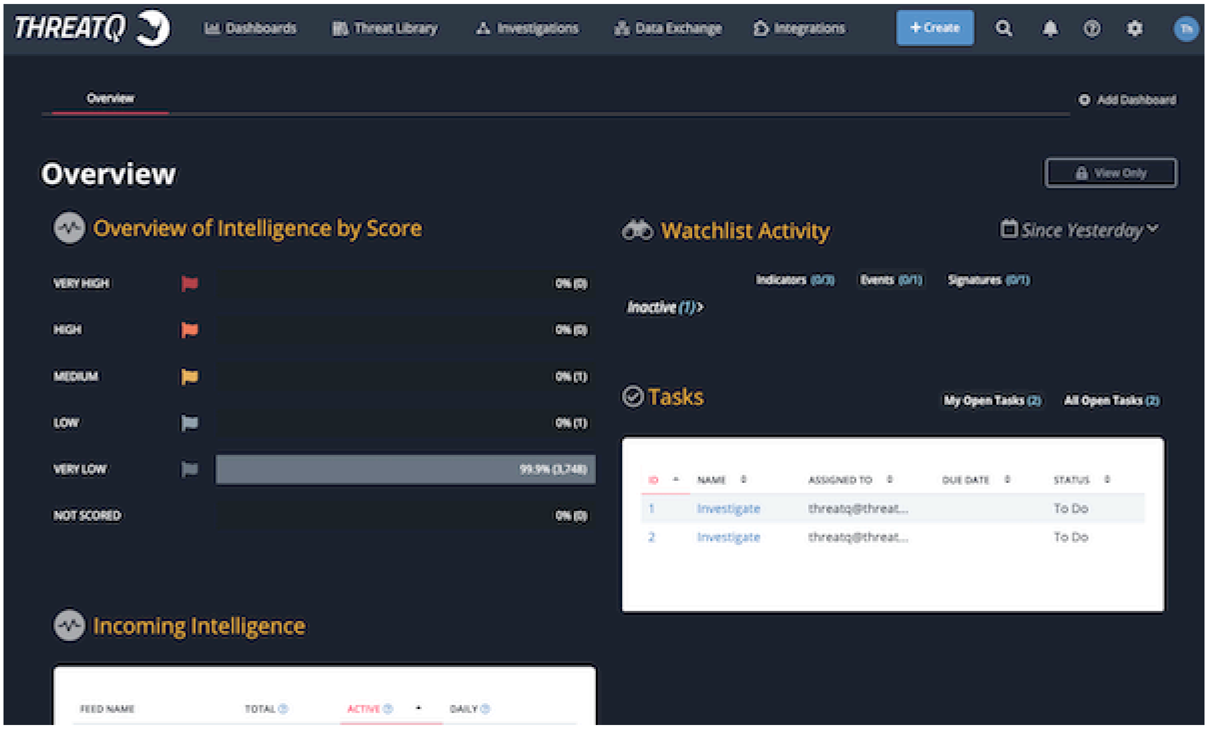
Upon install, the system default ThreatQ dashboard serves as your initial landing page when you log into ThreatQ.

While this dashboard cannot be modified, you can create your own data-driven dashboards.

Users with roles of Primary Contributor, Administrators, and Maintenance can create custom dashboards that can be shared with individual users or all users.

Default Dashboard

The system default dashboard, Overview, displays metrics and visualizations to provide at-a-glance views of your threat intelligence data.



VERY HIGH		0% (0)
HIGH		0% (0)
MEDIUM		0% (1)
LOW		0% (1)
VERY LOW		99.9% (3,748)
NOT SCORED		0% (0)

ID	NAME	ASSIGNED TO	DUE DATE	STATUS
1	Investigate	threatq@threat...		To Do
2	Investigate	threatq@threat...		To Do

Widgets include:

- Overview of intelligence by score
- Watchlist activity
- Incoming intelligence
- Open assigned tasks

Overview by Intelligence Score

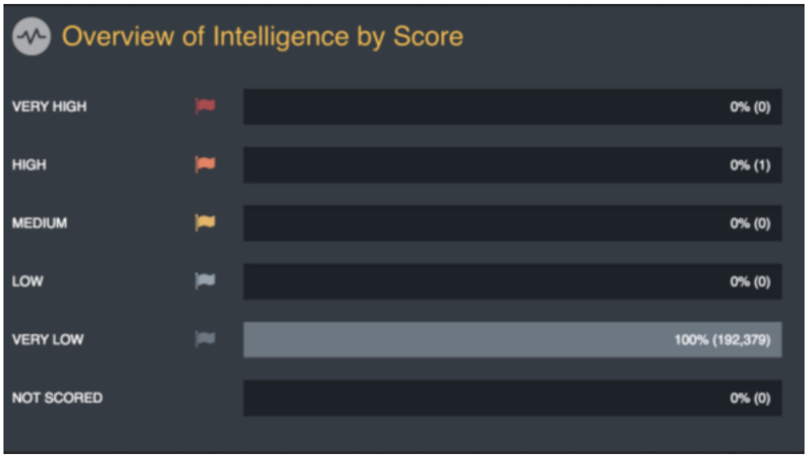
This dashboard graph provides a summary of indicator scoring in the system. It lists total indicators by score in the following order:

- Very High
- High
- Medium

- Low
- Very Low
- Not Scored

Ideally, this dashboard reflects a small number of **Very High** indicators with the bulk of the remaining indicators scored as **Low** or **Very Low**. This distribution reflects a focus on key threat intelligence. You can use Scoring Algorithms or Indicator Scoring to adjust the scores assigned to your indicators.

You can click the percentage/number of indicators to launch an advanced search based on that criteria.

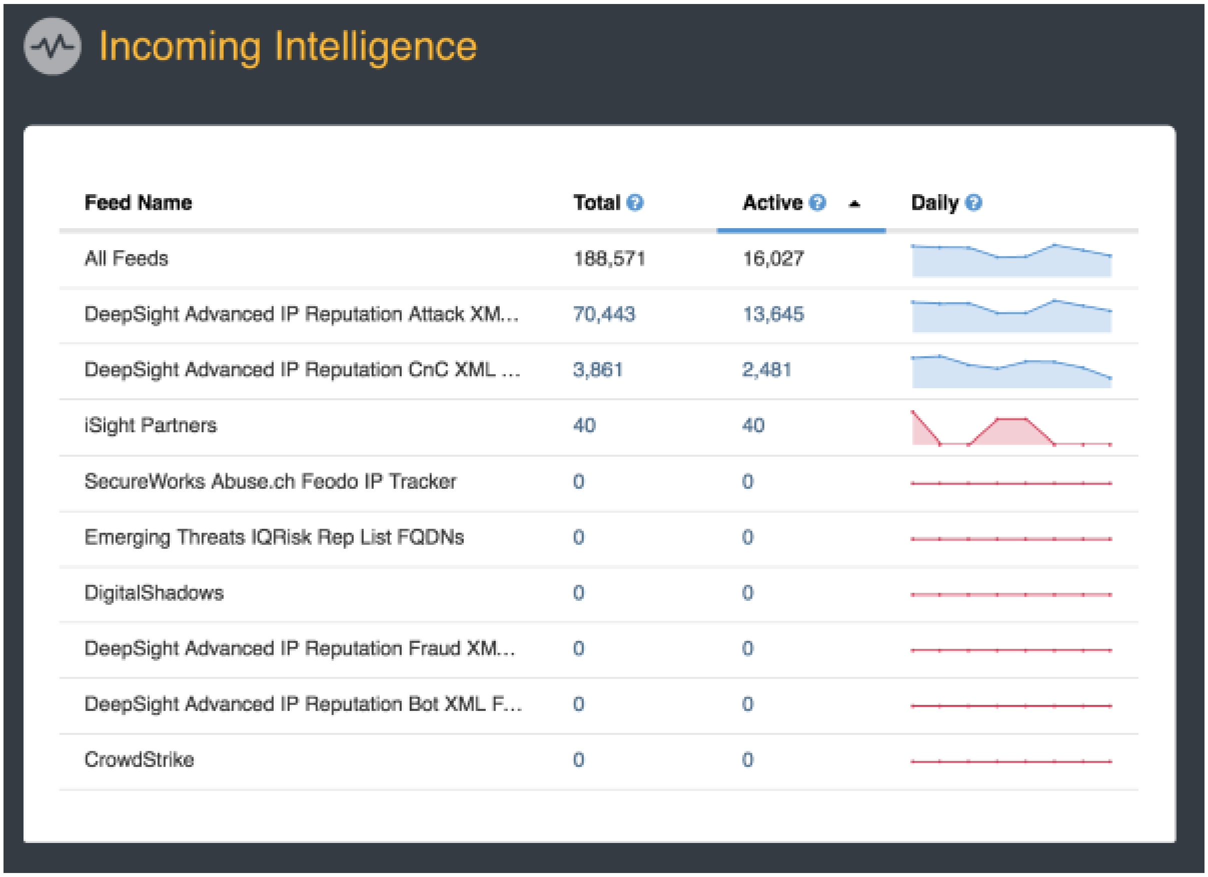


Overview of Intelligence by Score

VERY HIGH	0% (0)
HIGH	0% (1)
MEDIUM	0% (0)
LOW	0% (0)
VERY LOW	100% (192,379)
NOT SCORED	0% (0)

Incoming Intelligence

This dashboard graph provides a view of threat intelligence from all incoming feeds.



Incoming Intelligence

Feed Name	Total	Active	Daily
All Feeds	188,571	16,027	
DeepSight Advanced IP Reputation Attack XM...	70,443	13,645	
DeepSight Advanced IP Reputation CnC XML ...	3,861	2,481	
iSight Partners	40	40	
SecureWorks Abuse.ch Feodo IP Tracker	0	0	
Emerging Threats IQRisk Rep List FQDNs	0	0	
DigitalShadows	0	0	
DeepSight Advanced IP Reputation Fraud XM...	0	0	
DeepSight Advanced IP Reputation Bot XML F...	0	0	
CrowdStrike	0	0	

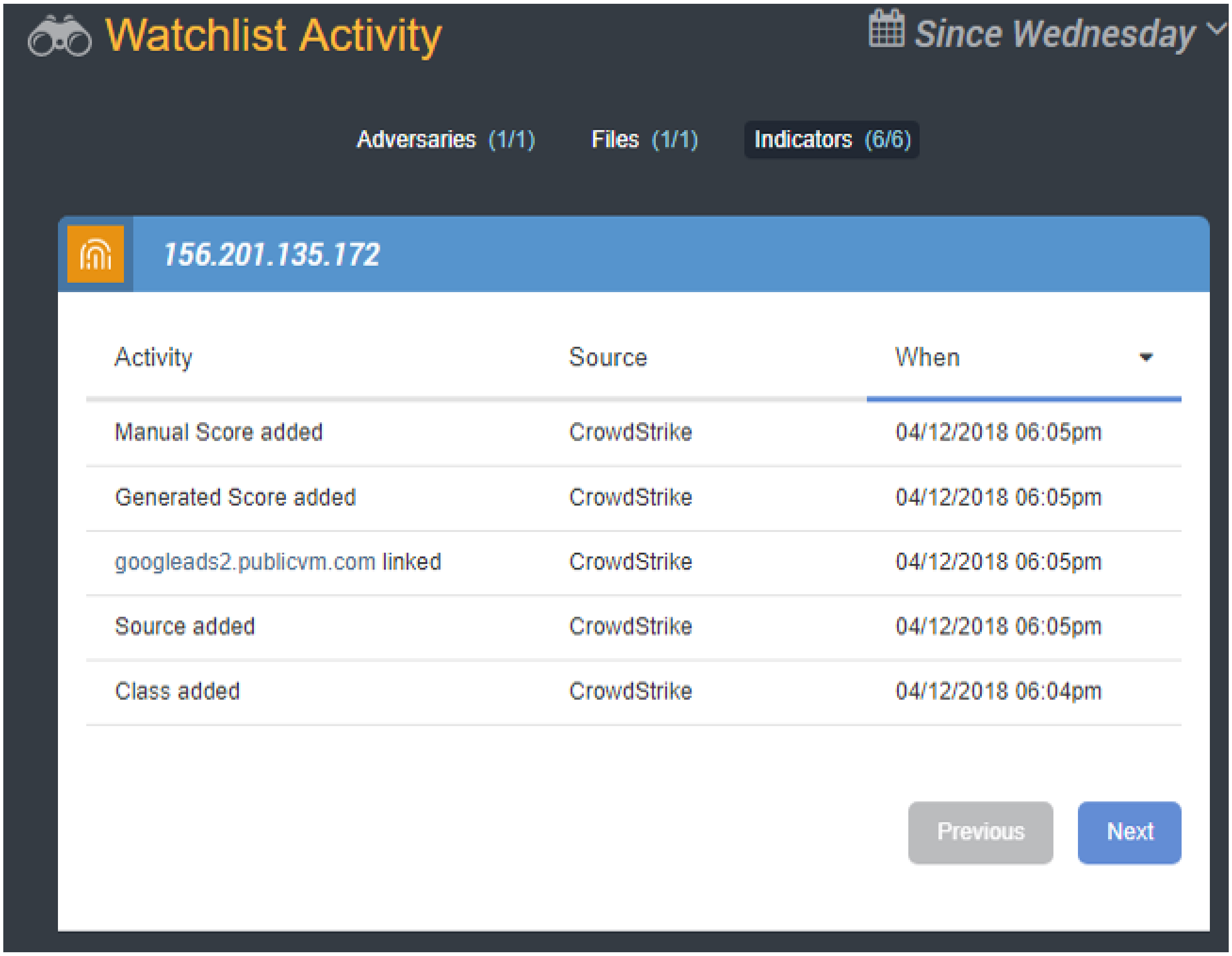
The system categorizes threat intelligence by:

- 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.



Activity	Source	When
Manual Score added	CrowdStrike	04/12/2018 06:05pm
Generated Score added	CrowdStrike	04/12/2018 06:05pm
googleads2.publicvm.com linked	CrowdStrike	04/12/2018 06:05pm
Source added	CrowdStrike	04/12/2018 06:05pm
Class added	CrowdStrike	04/12/2018 06:04pm

See the Add/Remove an Object to the Watchlist topic for steps on how to add an object to your watchlist.

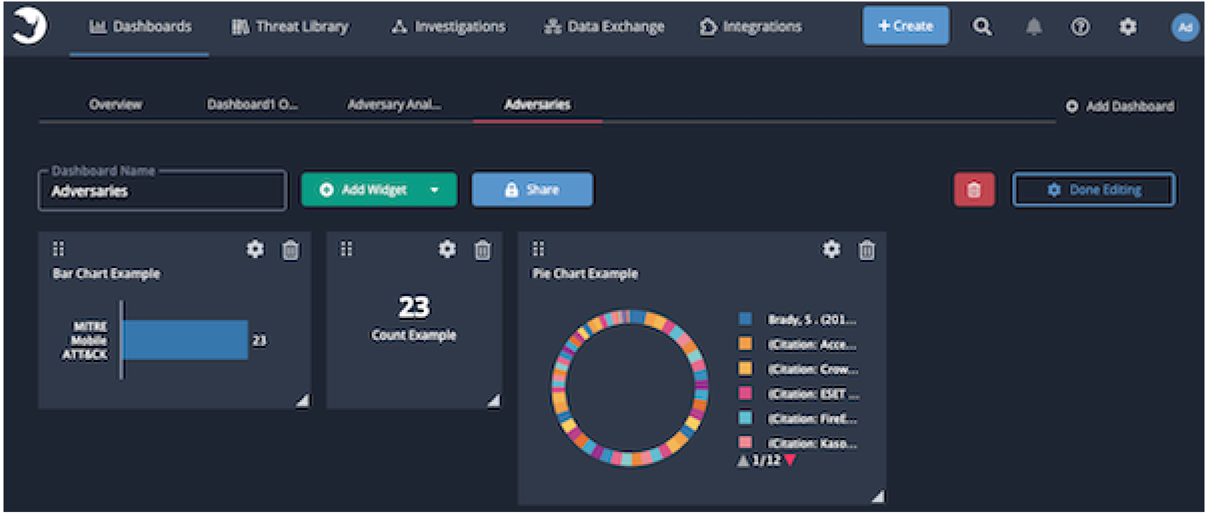
Tasks

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 data collections - see Managing Search Results topic for more details. You can click on an individual segment of data within a widget to view it in the ThreatQ Threat Library.

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. Dashboards added to your view will appear dashboard horizontal menu as well as the Dashboards dropdown menu. 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.

Topics covered in this section include:

SECTION	DETAILS
Analytics Dashboards	Deploy pre-configured dashboards for Adversaries, Events, Files, and Indicators.

Dashboard Widgets	You can add the following widgets to your custom dashboards: Bar Chart, Description, Line Chart, Pie Chart, Count, and Table.
Dashboard Management	You can create, edit, and delete your own custom dashboards.
Dashboard Sharing	You have the ability to configure how your custom dashboards are shared across the ThreatQ platform.
User View Management	Add, remove, and reorder dashboards that you created or have been shared with you.

Analytics Dashboards

You can deploy preconfigured dashboards, formerly known as Analytics, to your dashboard view.

> Analytics dashboards cannot be edited.

Options include:

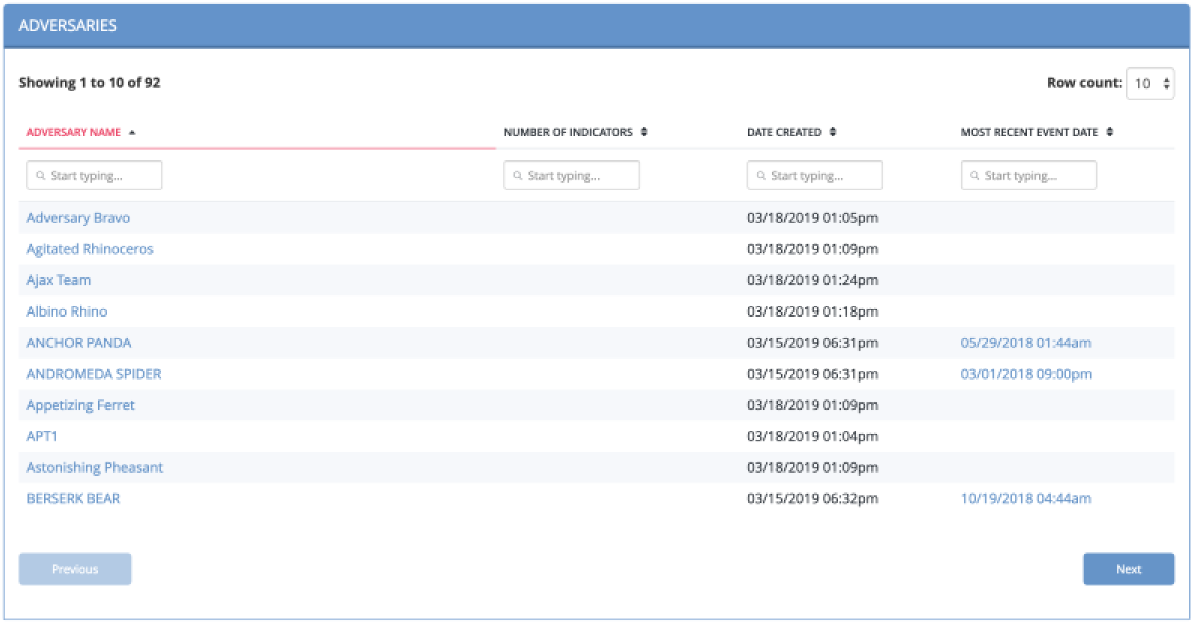
SECTION	DETAILS
Adversaries Analytics	The Adversaries dashboard provides an overview of all the Adversaries within ThreatQ as well as overlapping use of specific indicators.
Events Analytics	The Events dashboard provides a high-level view of what types of Events have occurred and how frequently they are occurring.
Files Analytics	The Files dashboard 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.
Indicators Analytics	The Indicators Dashboard 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.

Adversaries Analytics Dashboard

The Adversaries dashboard provides an overview of all the Adversaries within ThreatQ as well as overlapping use of specific indicators.

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.



Showing 1 to 10 of 92

Row count: 10

ADVERSARY NAME	NUMBER OF INDICATORS	DATE CREATED	MOST RECENT EVENT DATE
Adversary Bravo		03/18/2019 01:05pm	
Agitated Rhinoceros		03/18/2019 01:09pm	
Ajax Team		03/18/2019 01:24pm	
Albino Rhino		03/18/2019 01:18pm	
ANCHOR PANDA		03/15/2019 06:31pm	05/29/2018 01:44am
ANDROMEDA SPIDER		03/15/2019 06:31pm	03/01/2018 09:00pm
Appetizing Ferret		03/18/2019 01:09pm	
APT1		03/18/2019 01:04pm	
Astonishing Pheasant		03/18/2019 01:09pm	
BERSERK BEAR		03/15/2019 06:32pm	10/19/2018 04:44am

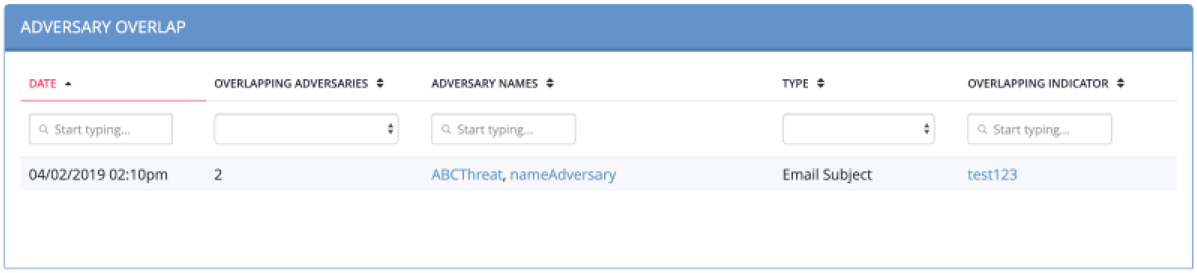
The following functions are available:

FUNCTION	DETAILS
Opening the Adversary Details page for an adversary	Click the name in the Adversary Name column.
Performing a search for related indicators	Click the number in the Number of Indicators column to set the adversary name as a search criterion and open the Advanced Search page.

FUNCTION	DETAILS
Opening the Event Details page for an adversary event	Click the date in the Most Recent Event Date to open the Event Details page.
Changing the number of entries displayed in the table	Click the paging batch option located to the bottom-right of the table.
Sorting the table by a column	Click the column header. To reverse the column sorting order, click the header a second time.
Searching within the Adversary Name column	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.



ADVERSARY OVERLAP

DATE ▲	OVERLAPPING ADVERSARIES ⬍	ADVERSARY NAMES ⬍	TYPE ⬍	OVERLAPPING INDICATOR ⬍
Start typing...	⬍	Start typing...	⬍	Start typing...
04/02/2019 02:10pm	2	ABCThreat, nameAdversary	Email Subject	test123

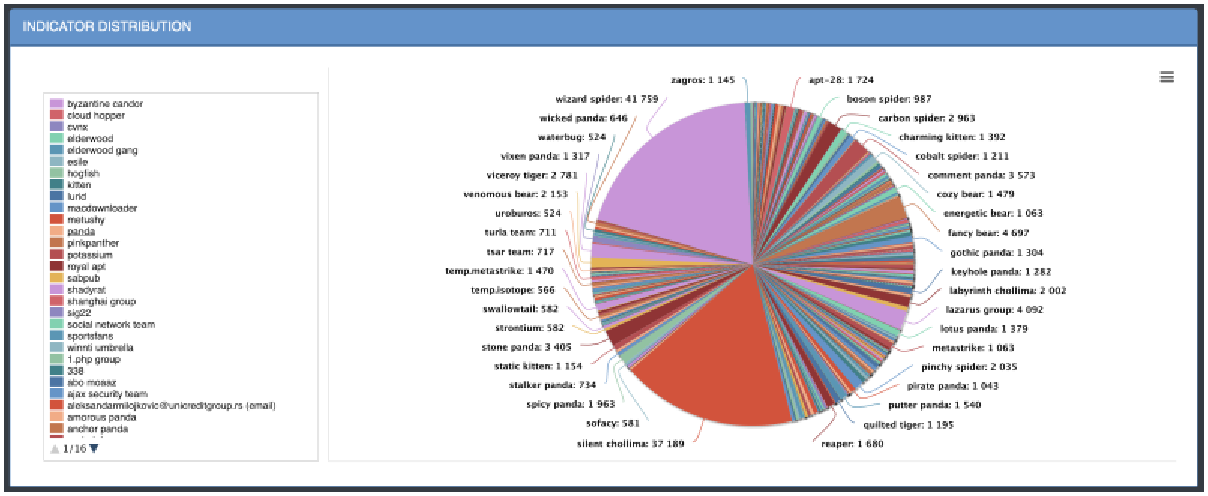
The following functions are available:

FUNCTION	DETAILS
Opening the Adversary Details page for an adversary	Click the name in the Adversary Name column.
Opening the Indicator Details page for an overlapping indicator	Click the identity in the Overlapping Indicator column.

FUNCTION	DETAILS
Changing the number of entries displayed in the table	Click the paging batch option located to the bottom-right of the table.
Sorting the table by a column	Click the column header. To reverse the column sorting order, click the header a second time.
Searching within a column	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.



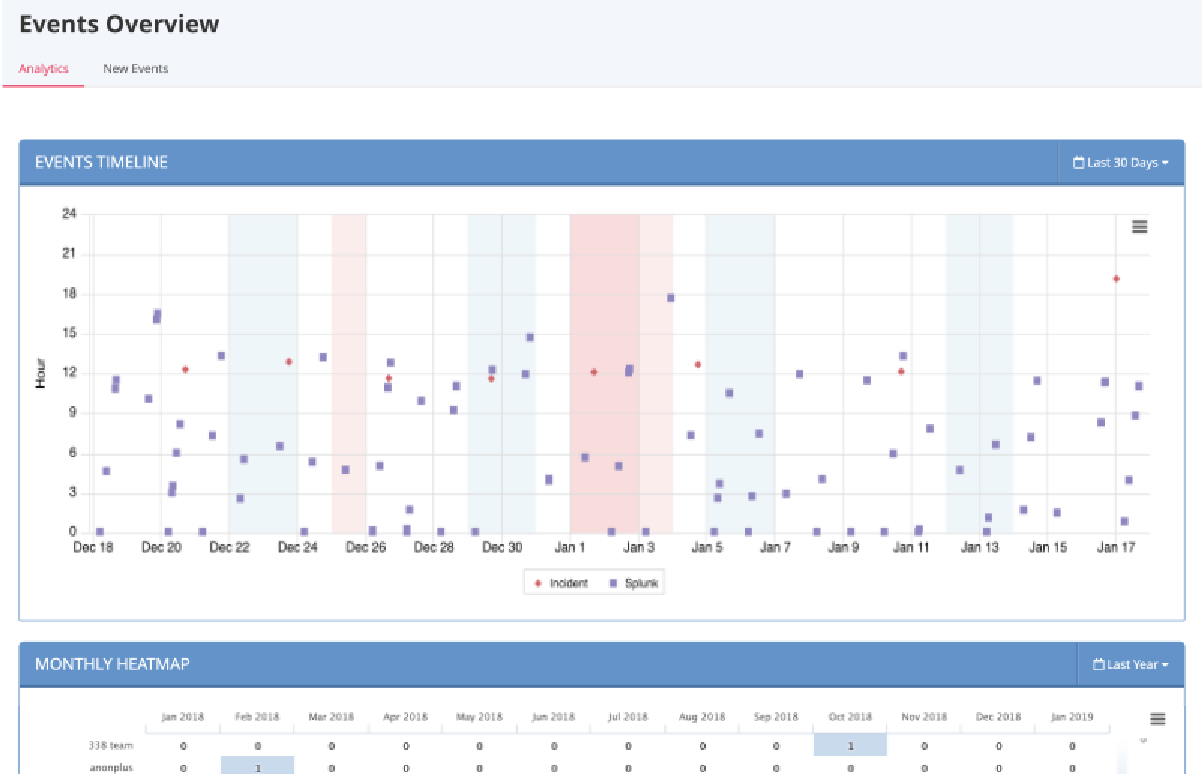
The following functions are available:

FUNCTION	DETAILS
Viewing more information about a selected value	Hover over a colored section of the pie chart to open a popup identifying the indicator.

FUNCTION	DETAILS
	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	Click the indicator on the left of the pie chart to remove it; click a second time to reinstate it.
Adjusting the time frame of the information displayed	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	Click the hamburger menu ≡ and select the desired option.

Events Analytics Dashboard

The Events dashboard provides a high-level view of what types of Events have occurred and how frequently they are occurring.

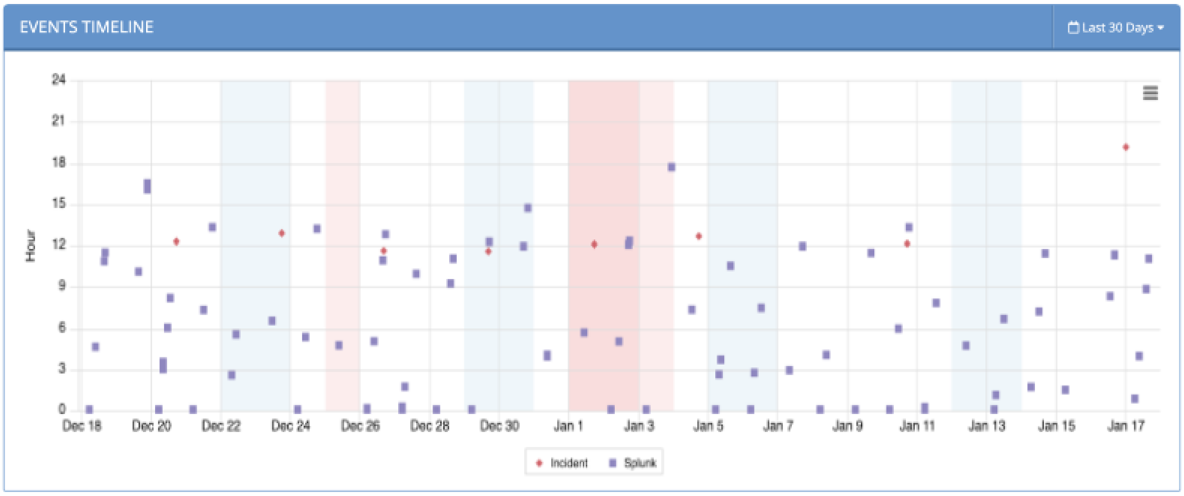


Events Overview

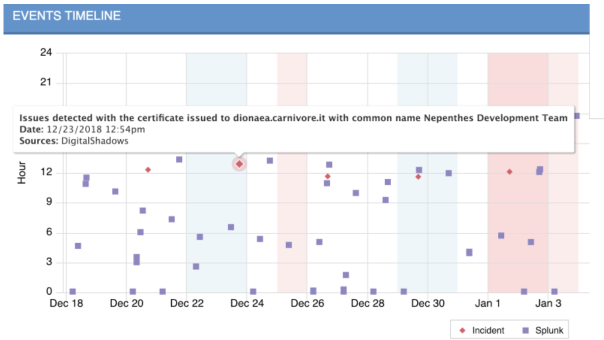
	Jan 2018	Feb 2018	Mar 2018	Apr 2018	May 2018	Jun 2018	Jul 2018	Aug 2018	Sep 2018	Oct 2018	Nov 2018	Dec 2018	Jan 2019
338 team	0	0	0	0	0	0	0	0	0	1	0	0	0
anonplus	0	1	0	0	0	0	0	0	0	0	0	0	0

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.



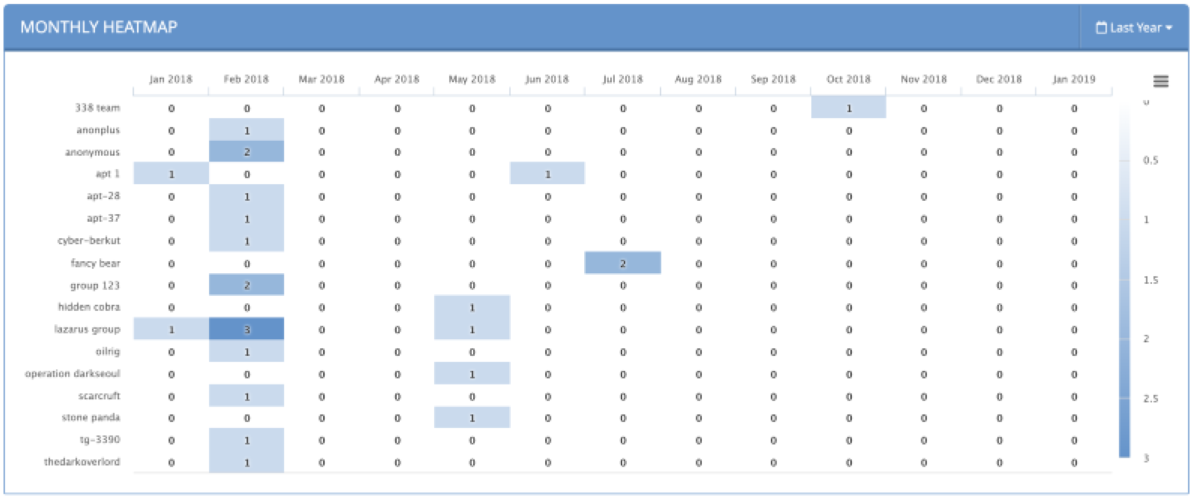
The following functions are available:

FUNCTION	DETAILS
Viewing an event's name, date and time, and source	Hover your mouse over an event on the scatter plot to see its name, date and time, and source.  EVENTS TIMELINE Hour 24 21 12 9 6 3 0 Dec 18 Dec 20 Dec 22 Dec 24 Dec 26 Dec 28 Dec 30 Jan 1 Jan 3 Incident Splunk Issues detected with the certificate issued to dionaea.carnivore.it with common name Nepenthes Development Team **Date:** 12/23/2018 12:54pm **Sources:** DigitalShadows
Opening the Event Details page for one of the events	Click the event in the scatter plot. For more information, see Object Details.

FUNCTION	DETAILS
Hiding or unhiding one or more of the event types	Click the event type in the legend immediately below the scatter plot to remove it from the graph; click it again to reinstate it.
Adjusting the time frame of the information displayed	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

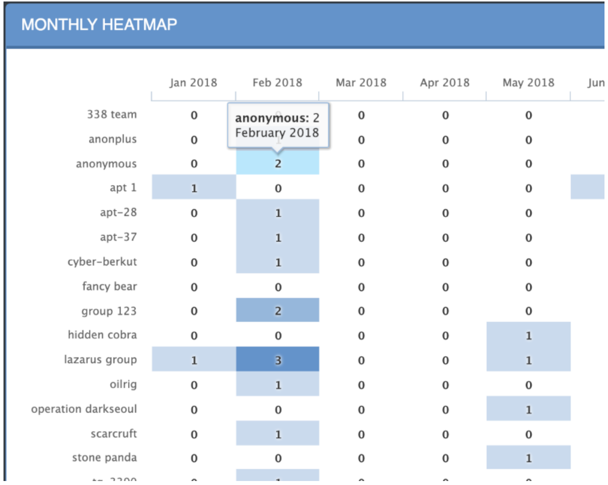
The Monthly Heatmap table lists events that happened per adversary each month. Shading of the monthly totals is used to allow you to quickly scan for patterns in the events and to quickly detect events with higher monthly counts.



MONTHLY HEATMAP

	Jan 2018	Feb 2018	Mar 2018	Apr 2018	May 2018	Jun 2018	Jul 2018	Aug 2018	Sep 2018	Oct 2018	Nov 2018	Dec 2018	Jan 2019
338 team	0	0	0	0	0	0	0	0	0	1	0	0	0
anonplus	0	1	0	0	0	0	0	0	0	0	0	0	0
anonymous	0	2	0	0	0	0	0	0	0	0	0	0	0
apt 1	1	0	0	0	0	1	0	0	0	0	0	0	0
apt-28	0	1	0	0	0	0	0	0	0	0	0	0	0
apt-37	0	1	0	0	0	0	0	0	0	0	0	0	0
cyber-berkut	0	1	0	0	0	0	0	0	0	0	0	0	0
fancy bear	0	0	0	0	0	0	2	0	0	0	0	0	0
group 123	0	2	0	0	0	0	0	0	0	0	0	0	0
hidden cobra	0	0	0	0	1	0	0	0	0	0	0	0	0
lazarus group	1	3	0	0	1	0	0	0	0	0	0	0	0
oilrig	0	1	0	0	0	0	0	0	0	0	0	0	0
operation darkseoul	0	0	0	0	1	0	0	0	0	0	0	0	0
scarcruft	0	1	0	0	0	0	0	0	0	0	0	0	0
stone panda	0	0	0	0	1	0	0	0	0	0	0	0	0
tg-3390	0	1	0	0	0	0	0	0	0	0	0	0	0
thedarkoverlord	0	1	0	0	0	0	0	0	0	0	0	0	0

The following functions are available:

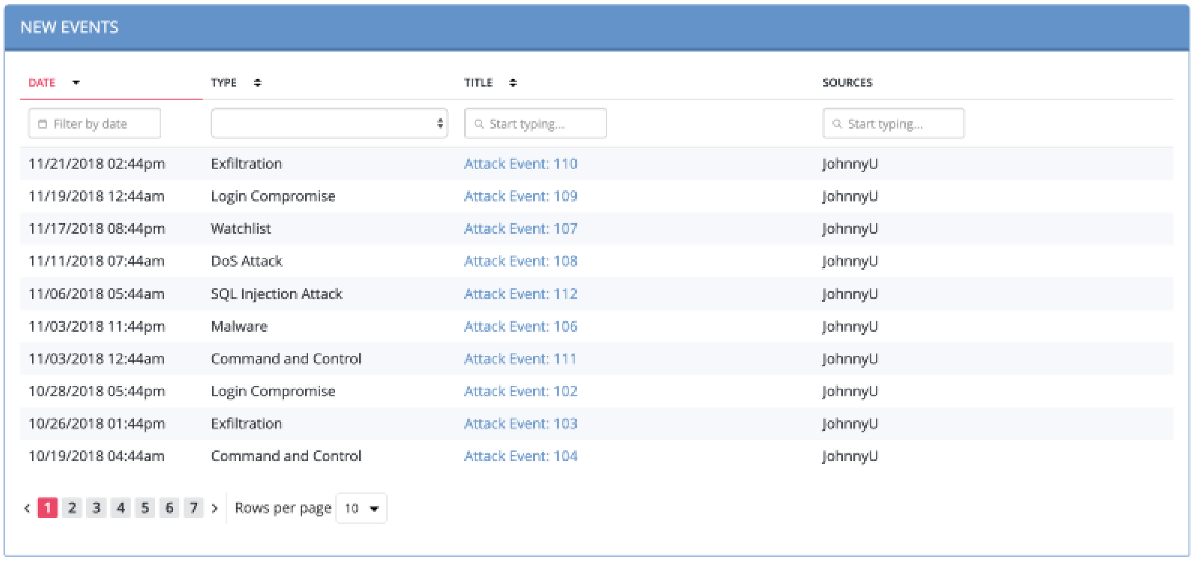
FUNCTION	DETAILS
Viewing an event's name and monthly count	1. Hover your mouse over an event on the heatmap to see its name and monthly count.  MONTHLY HEATMAP anonymous: 2 February 2018
Adjusting the time frame of the information displayed	1. Click the dropdown menu at the top right and select the desired time frame. You can select from: ◦ Last 24 Hours ◦ Last 7 Days

	Jan 2018	Feb 2018	Mar 2018	Apr 2018	May 2018
338 team	0		0	0	0
anonplus	0		0	0	0
anonymous	0	2	0	0	0
apt 1	1	0	0	0	0
apt-28	0	1	0	0	0
apt-37	0	1	0	0	0
cyber-berkut	0	1	0	0	0
fancy bear	0	0	0	0	0
group 123	0	2	0	0	0
hidden cobra	0	0	0	0	1
lazarus group	1	3	0	0	1
oilrig	0	1	0	0	0
operation darkseoul	0	0	0	0	1
scarcruft	0	1	0	0	0
stone panda	0	0	0	0	1

FUNCTION	DETAILS
	◦ 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.



DATE	TYPE	TITLE	SOURCES
11/21/2018 02:44pm	Exfiltration	Attack Event: 110	JohnnyU
11/19/2018 12:44am	Login Compromise	Attack Event: 109	JohnnyU
11/17/2018 08:44pm	Watchlist	Attack Event: 107	JohnnyU
11/11/2018 07:44am	DoS Attack	Attack Event: 108	JohnnyU
11/06/2018 05:44am	SQL Injection Attack	Attack Event: 112	JohnnyU
11/03/2018 11:44pm	Malware	Attack Event: 106	JohnnyU
11/03/2018 12:44am	Command and Control	Attack Event: 111	JohnnyU
10/28/2018 05:44pm	Login Compromise	Attack Event: 102	JohnnyU
10/26/2018 01:44pm	Exfiltration	Attack Event: 103	JohnnyU
10/19/2018 04:44am	Command and Control	Attack Event: 104	JohnnyU

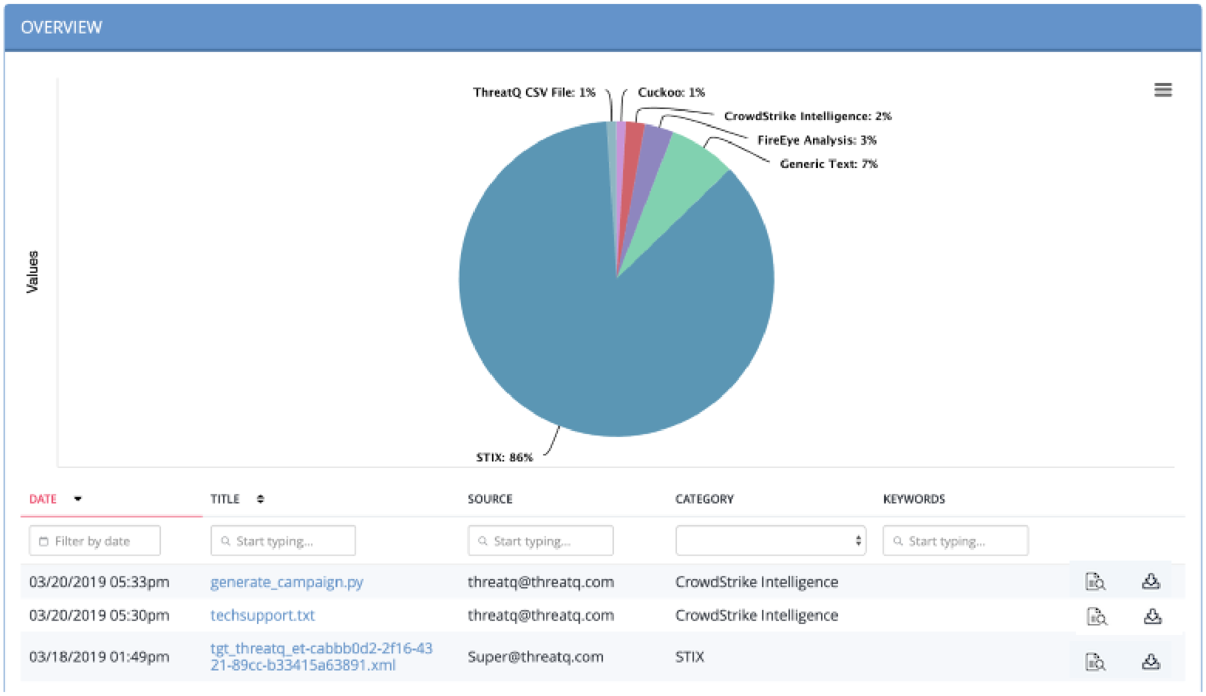
The following functions are available:

FUNCTION	DETAILS
Opening the Event Details page for one of the events	Click the event title. For more information, see Object Details.

FUNCTION	DETAILS
Changing the number of entries displayed in the table	Click the dropdown menu at the top right of the table, and select the desired option.
Sorting the table by a column	Click the column header. Click on the header a second time to reverse the sort order.
Searching within a column	Click within the search box at the top of the column, and enter your search criteria.

Files Analytics Dashboard

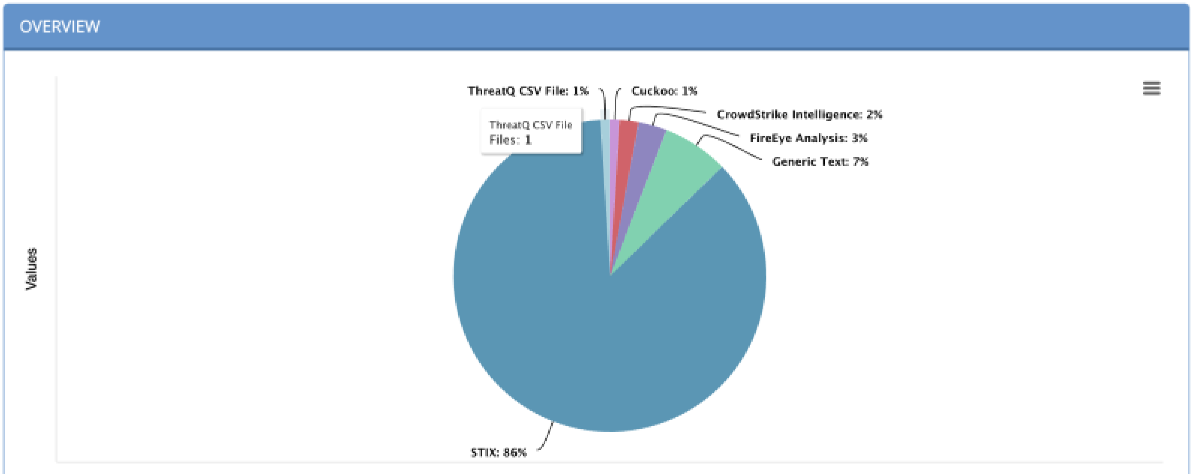
The Files dashboard provides you with a pie chart displays the percentage of different types of Files within the system and a table that lists the files, the date and time they were created, their title, their source, their category, and associated keywords.



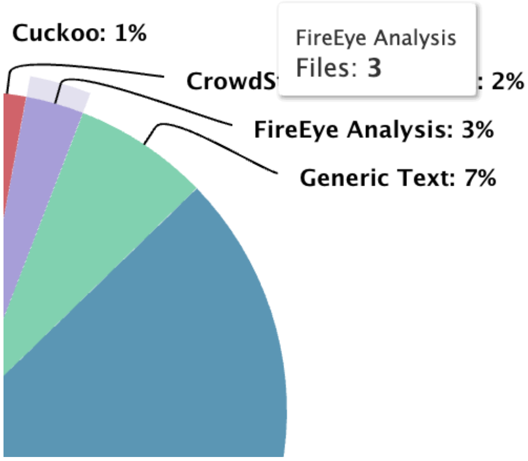
DATE	TITLE	SOURCE	CATEGORY	KEYWORDS
03/20/2019 05:33pm	generate_campaign.py	threatq@threatq.com	CrowdStrike Intelligence	
03/20/2019 05:30pm	techsupport.txt	threatq@threatq.com	CrowdStrike Intelligence	
03/18/2019 01:49pm	tgt_threatq_et-cabbb0d2-2f16-4321-89cc-b33415a63891.xml	Super@threatq.com	STIX	

File Type Pie Chart

The file type pie chart displays the percentage of different types of files within the system.

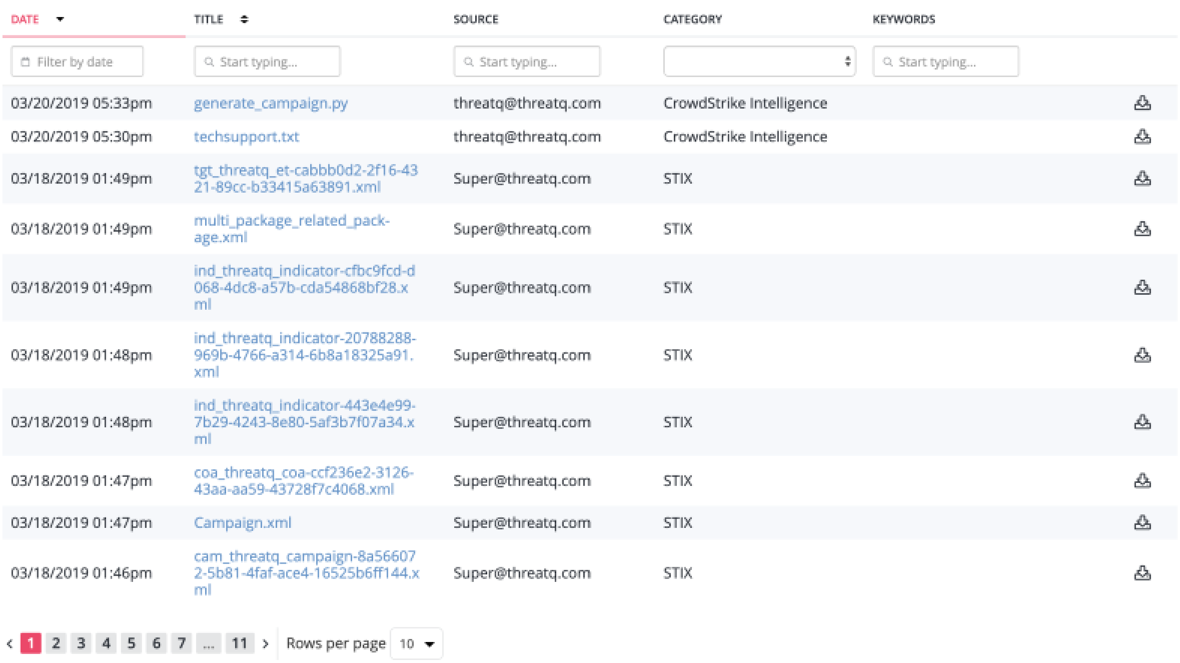


The following functions are available:

FUNCTION	DETAILS
Viewing more information about a selected file	Hover over a colored section of the pie chart to view the number tha corresponds to the file type percentage. 
Printing the graph or saving it as a PNG, JPEG, PDF, or SVG	Click the hamburger menu ≡ and select the desired option.

Files Table

Immediately below the file type 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.



DATE	TITLE	SOURCE	CATEGORY	KEYWORDS
Filter by date	Start typing...	Start typing...		Start typing...
03/20/2019 05:33pm	generate_campaign.py	threatq@threatq.com	CrowdStrike Intelligence	
03/20/2019 05:30pm	techsupport.txt	threatq@threatq.com	CrowdStrike Intelligence	
03/18/2019 01:49pm	tgt_threatq_et-cabbb0d2-2f16-4321-89cc-b33415a63891.xml	Super@threatq.com	STIX	
03/18/2019 01:49pm	multi_package_related_package.xml	Super@threatq.com	STIX	
03/18/2019 01:49pm	ind_threatq_indicator-cfbc9fcd-d068-4dc8-a57b-cda54868bf28.xml	Super@threatq.com	STIX	
03/18/2019 01:48pm	ind_threatq_indicator-20788288-969b-4766-a314-6b8a18325a91.xml	Super@threatq.com	STIX	
03/18/2019 01:48pm	ind_threatq_indicator-443e4e99-7b29-4243-8e80-5af3b7f07a34.xml	Super@threatq.com	STIX	
03/18/2019 01:47pm	coa_threatq_coa-ccf236e2-3126-43aa-aa59-43728f7c4068.xml	Super@threatq.com	STIX	
03/18/2019 01:47pm	Campaign.xml	Super@threatq.com	STIX	
03/18/2019 01:46pm	cam_threatq_campaign-8a566072-5b81-4faf-ace4-16525b6ff144.xml	Super@threatq.com	STIX	

‹ 1 2 3 4 5 6 7 ... 11 › Rows per page 10

The following functions are available:

FUNCTION	DETAILS
Opening the File Details page for a file	Click the name in the Title column.
Changing the number of entries displayed in the table per page	Click the paging batch option located to the bottom-right of the table.
Sorting the table by a column	Click the column header. Click on the header a second time to reverse the column sorting order.
Searching within a column	Click within the search box at the top of a column, and enter your search criteria.
Downloading a file	Click the file's download icon 📥 .

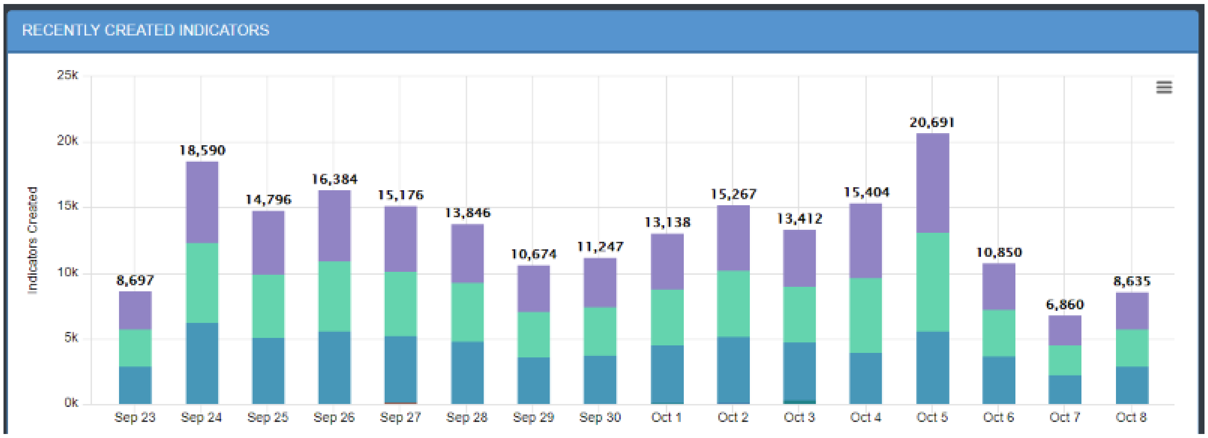
FUNCTION	DETAILS
Previewing a file	Click the file's preview icon Preview Icon. If your browser does not support file preview for a specific file type, the file is downloaded instead. You cannot preview a malware locked file.

Indicators Analytics Dashboard

The Indicators Dashboard 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.

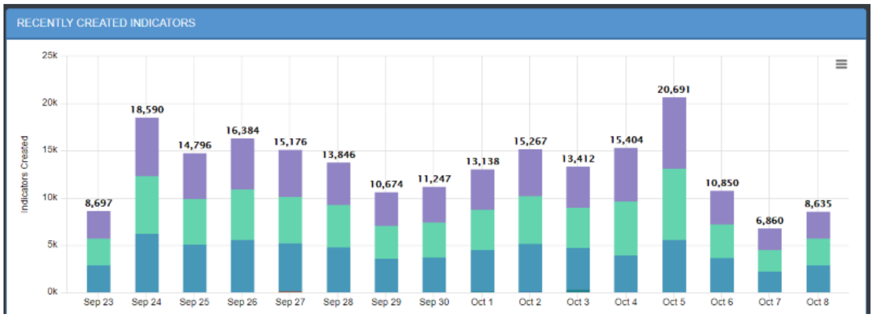
Recently Created Indicators Histogram

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.

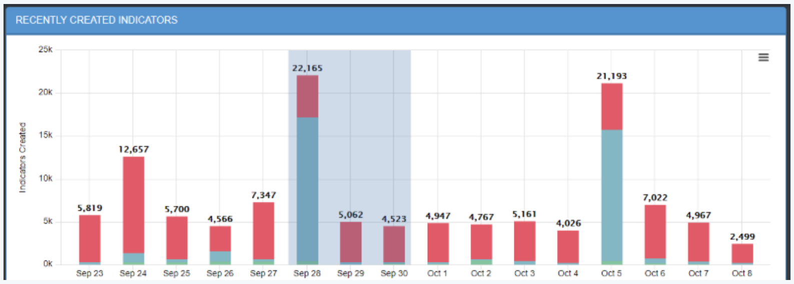


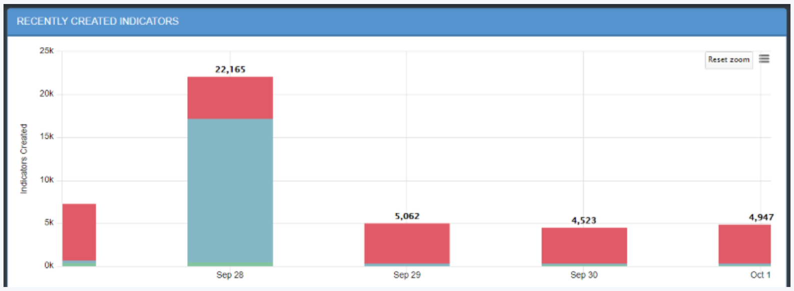
The following functions are available:

<table>
<tr><th>FUNCTION</th><th>DETAILS</th></tr>
<tr><td><strong>Viewing the number of indicators created each day by type</strong></td><td>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.


</td></tr>
</table>

<table>
<tr><th>FUNCTION</th><th>DETAILS</th></tr>
<tr><td><b>Zooming in for a closer view</b></td><td>
1. Drag your mouse over a section of the histogram, and your view will be magnified.

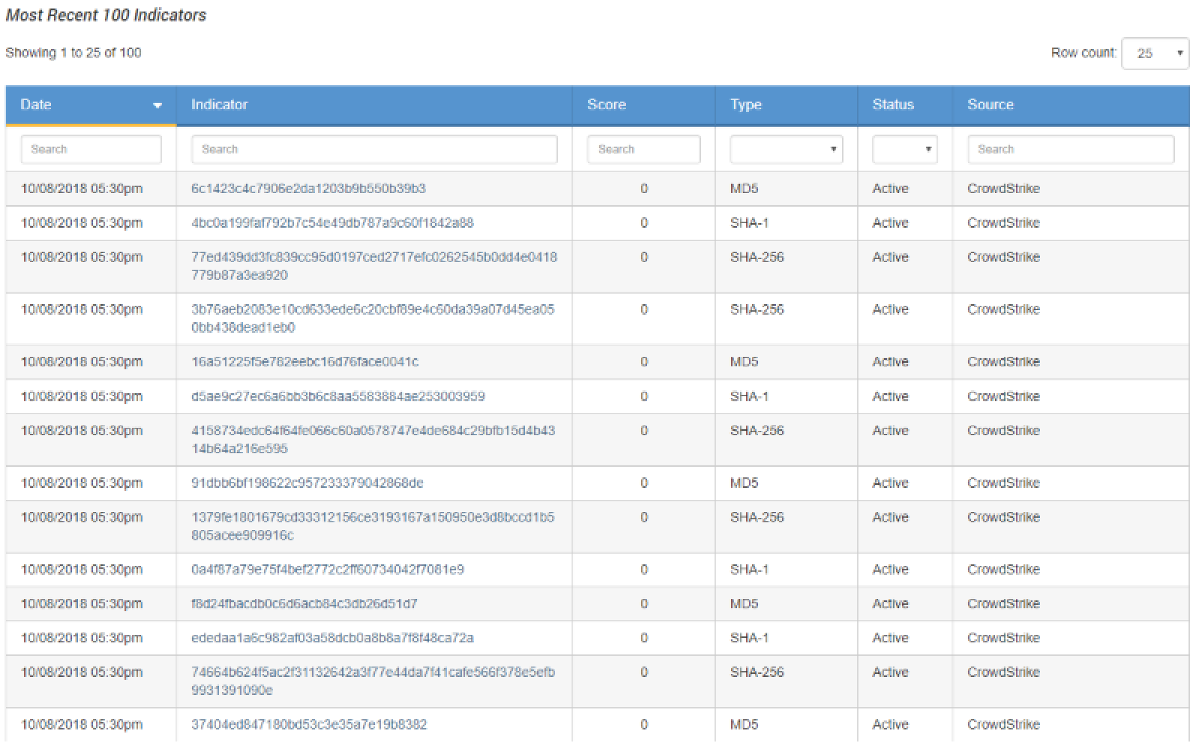




2. Click <b>Reset Zoom</b> to return to the full histogram.
</td></tr>
<tr><td><b>Printing the histogram or downloading it as a PNG, JPEG, PDF, or SVG file</b></td><td>Click the hamburger menu ☰, and select the desired option.</td></tr>
</table>

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
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	0a4f87a79e75f4bef2772c2ff60734042f7081e9	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

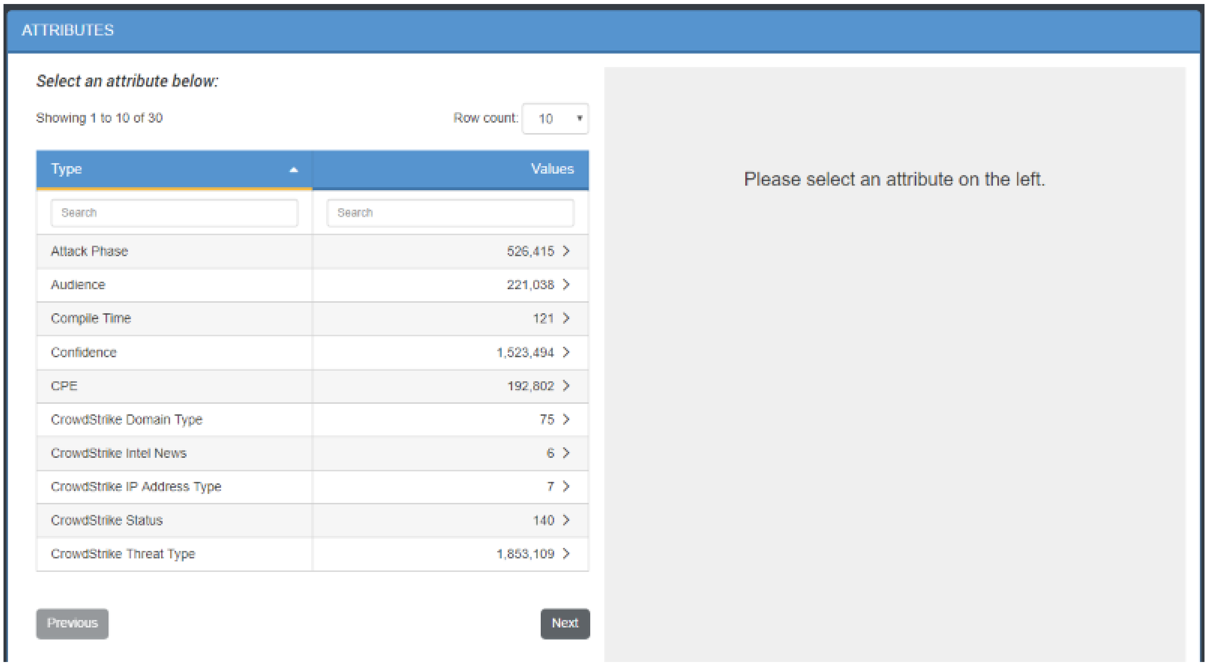
The following functions are available:

FUNCTION	DETAILS
Resort the Table	Click on the different table headings to resort that table by that column.
Search and Filter Table Results	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 Rows Displayed	Click on the **Row Count** icon located to the top-right of the chart and select a new display count from the dropdown.

FUNCTION	DETAILS
Access the Indicator Details Page for a Specific Indicator	Click on the specific Indicator to review to open the Indicator's Details page.

Attributes Table

The attributes list on the left side displays attributes related to Indicators in your system.



Select an attribute below:

Showing 1 to 10 of 30

Row count: 10

Type	Values
Attack Phase	526,415
Audience	221,038
Compile Time	121
Confidence	1,523,494
CPE	192,802
CrowdStrike Domain Type	75
CrowdStrike Intel News	6
CrowdStrike IP Address Type	7
CrowdStrike Status	140
CrowdStrike Threat Type	1,853,109

Please select an attribute on the left.

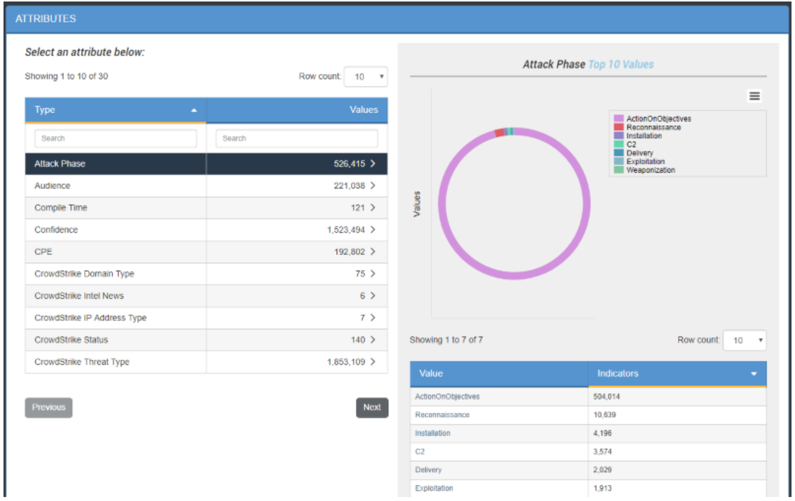
The following functions are available:

FUNCTION	DETAILS
Change the Number of Entries Displayed in the Table	Click the **Row Count** icon located to the top-right of the chart and select a new display count from the dropdown.
Search/Filter Attributes and Values	Click within the search box at the top of the column, and enter your search criteria.

FUNCTION **DETAILS**

View More Information About a Selected Attribute

1. Click on an attribute row in the table to view additional information in the right pane.



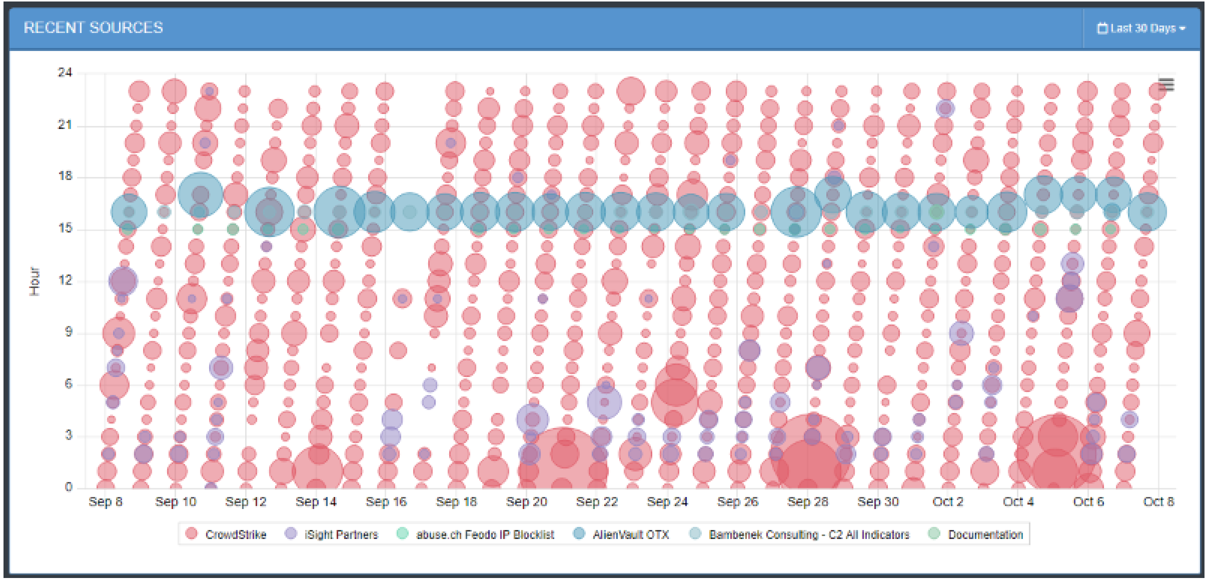
Type	Values
Attack Phase	526,415
Audience	221,038
Compile Time	121
Confidence	1,523,494
CPE	192,802
CrowdStrike Domain Type	75
CrowdStrike Intel News	6
CrowdStrike IP Address Type	7
CrowdStrike Status	140
CrowdStrike Threat Type	1,853,109

Value	Indicators
ActionOnObjectives	504,014
Reconnaissance	10,639
Installation	4,196
C2	3,574
Delivery	2,029
Exploitation	1,913

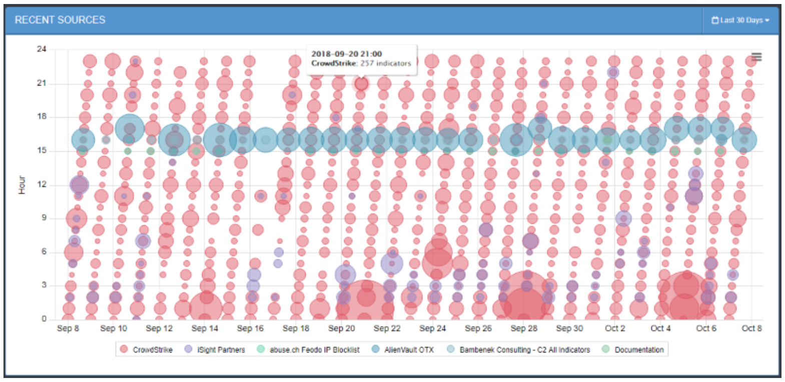
2. Hover the mouse over different portions of the pie chart to reveal the segment's value.
3. Click on an **Attribute Value** in the summary table below the pie chart to open the Advanced Search page with those attribute values applied.

Recent Sources

The Recent Sources Scatter plot displays how many indicators were provided by a given source each day within a specified time frame.



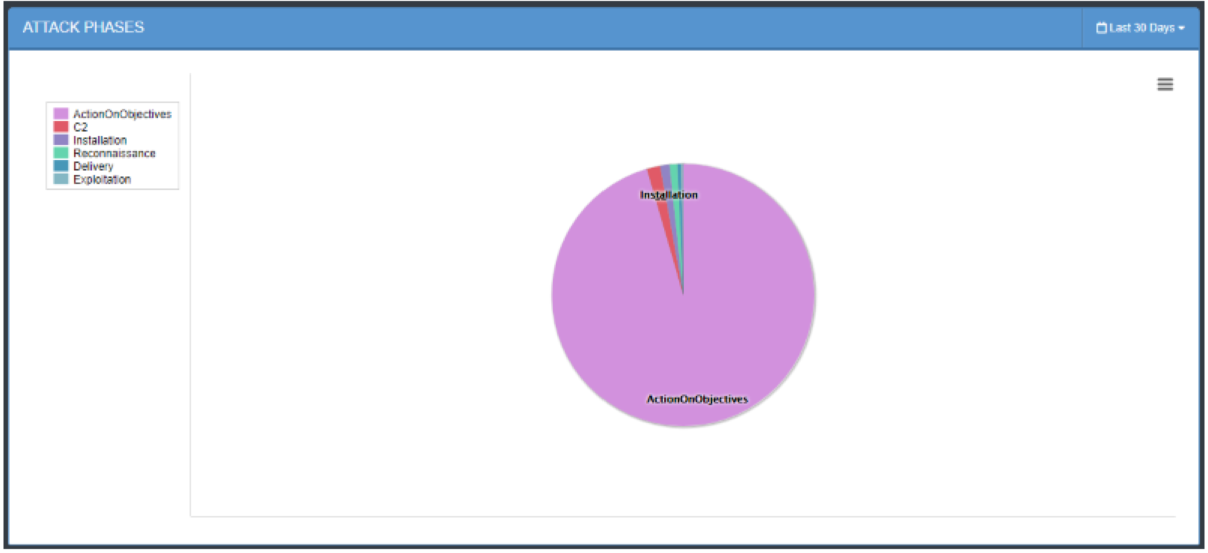
The following functions are available:

FUNCTION	DETAILS
View the Date and Number of Indicators from a Given Source	1. Hover the mouse over one of the scatter plot circles to view a popup with the Source, Date, Time and Number of Indicators.  RECENT SOURCES Last 30 Days Hour Sep 8 Sep 10 Sep 12 Sep 14 Sep 16 Sep 18 Sep 20 Sep 22 Sep 24 Sep 26 Sep 28 Sep 30 Oct 2 Oct 4 Oct 6 Oct 8 CrowdStrike iSight Partners abuse.ch Feodo IP Blocklist AlienVault OTX Bambenek Consulting - C2 All Indicators Documentation 2018-09-20 21:00 CrowdStrike: 257 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.

FUNCTION	DETAILS
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 the source in the legend appear grayed out. 2. Click on the source again to add it back to the scatter plot.

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 chart and use the dropdown menu select the desired range. Users can select from: ◦ Last 24 Hours ◦ Last 7 Days ◦ Last 30 Days

FUNCTION	DETAILS
	◦ 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.

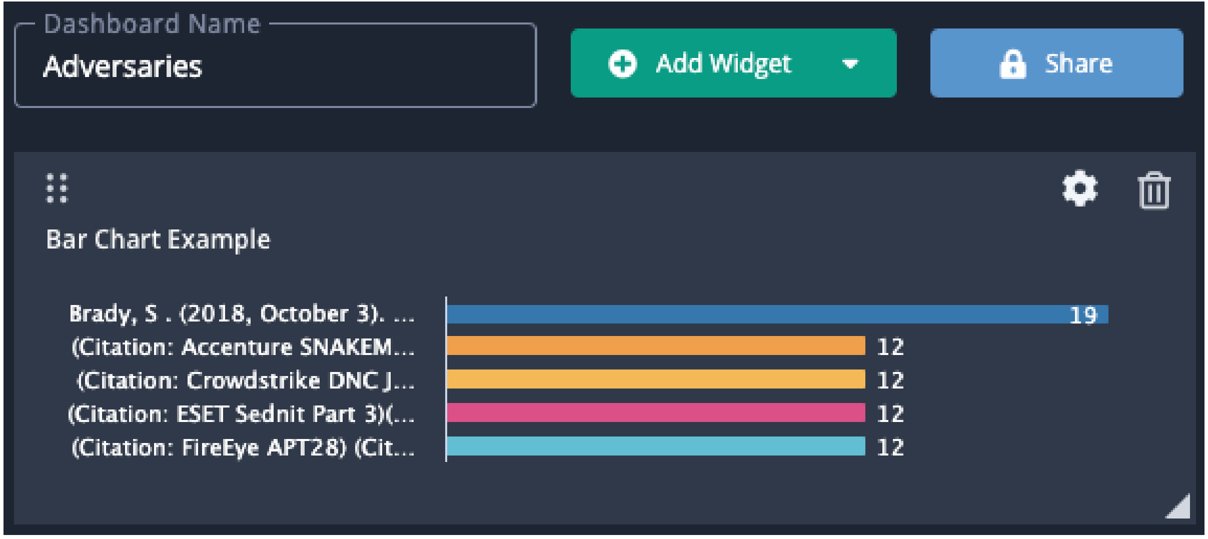
Dashboard Widgets

You can use the following Dashboard Widgets to build your custom dashboards: Bar Chart, Description, Line Chart, Pie Chart, Count, and Table.

Bar Chart

> 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.


Dashboard Name
Adversaries
Add Widget
Share
Bar Chart Example
Brady, S . (2018, October 3). ...
(Citation: Accenture SNAKEM...
(Citation: Crowdstrike DNC J...
(Citation: ESET Sednit Part 3)(...
(Citation: FireEye APT28) (Cit...
19
12
12
12
12

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

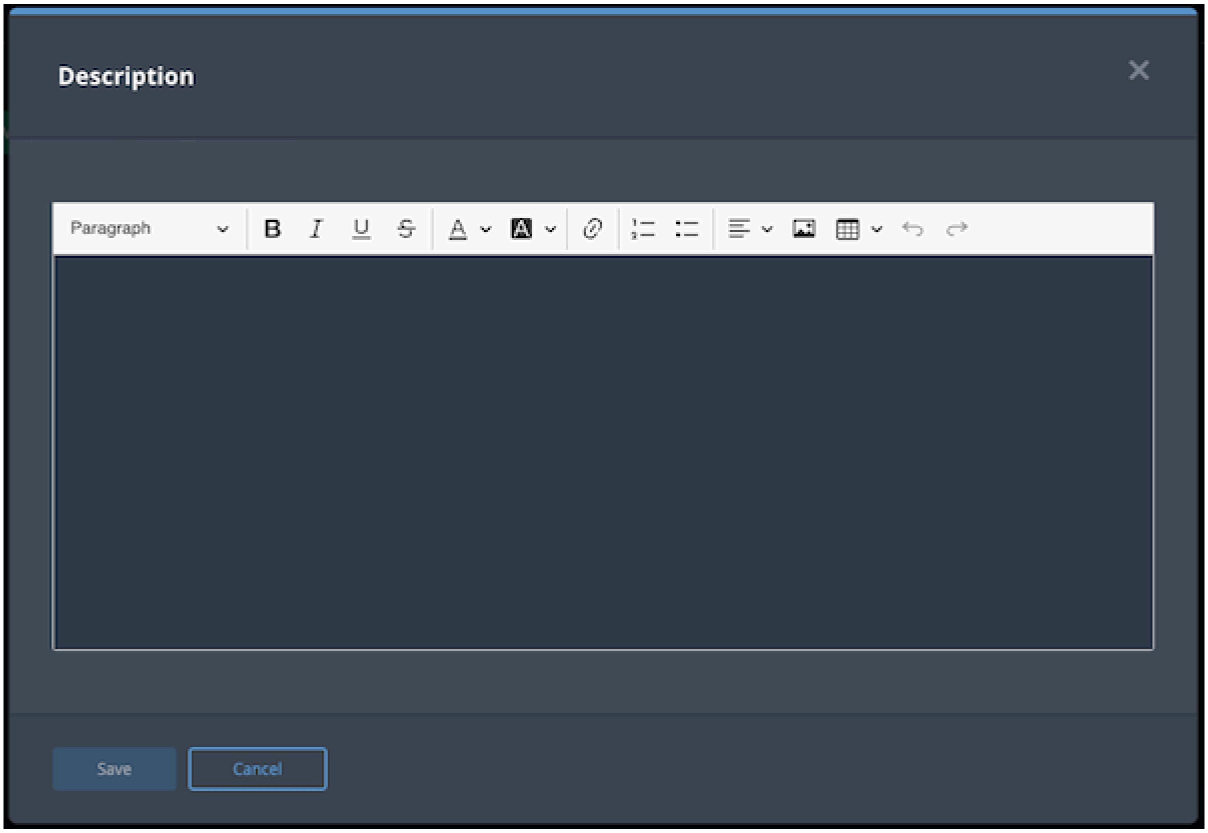
FIELD	DESCRIPTION
Data Collection	Select the data collection to populate the data.
Object	Select a specific object type to display.
Group By	Select a data column to sort the information such as source, tags, etc.
Visual Display	Select whether to show the bar chart horizontally or vertically.
Show Top Options	Select the number of results to display. Options include: • Top 5 • Top 10

Description

The Description widget allows you to provide further context and additional instructions for your custom dashboard. You can use the supplied editor to format your content.

Tips and Tricks for Adding Images to Description Widgets

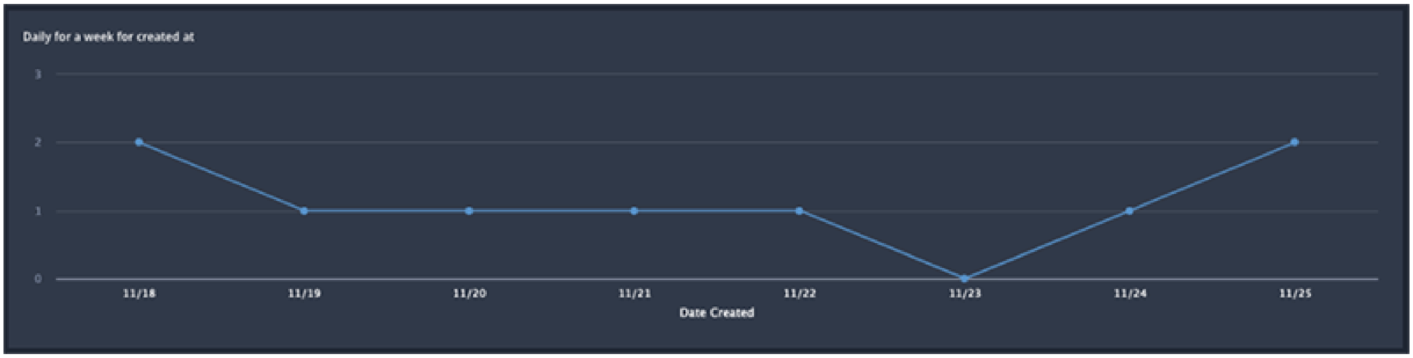
- **Image captions** - Add your image captions after you select your image alignment. If you change alignment after adding a caption, the caption is removed and must be added again.
- **Image text alternatives** - If you add an image text alternative to an image, it is available for use by screen reading tools but is only displayed on screen if the image fails to load. It is not displayed when you hover on the image.
- **Add a line above or below** - When you click an image, the arrow icons located on the bottom left and top right corners allow you to insert a line above (top right arrow) or below (bottom left arrow) the image.
- **Resize an image** - The resize image option allows you to adjust your image to 25%, 50%, or 75% of the size of the Description field. Or, you can return your image to its original size.



Line Chart

The Line Chart widget displays object information in a linear graph using the following date stamps:

- Date Created (all object types)
- Last Modified (all object types)
- Expiration Date (indicators only)

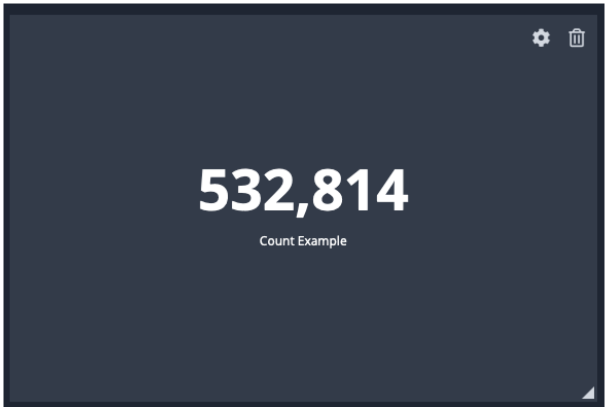


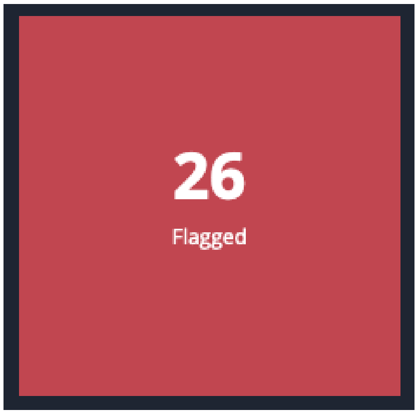
Complete the following fields to add a line chart widget to your custom dashboard.

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
Data to Show in Widget	Select the data collection to populate the data.
Object	Select a specific object type to display.
Date Metric	The date stamp to use with the line chart. Options include: • Date Created (all object types) • Last Modified (all object types) • Expiration Date (indicators only)
Time Range	The time range from today to be displayed. Options include: • 1 Week • 3 Months • 6 Months • 1 Year
Time Segments	Select how the dates will be displayed on the line chart. Options include: • Days (1 Week Time Range only) • Weeks (3 Months, 6 Months, 1 Year only) • Months (3 Months, 6 Months, 1 Year only) • Quarters (3 Months, 6 Months, 1 Year only) Quarters will return the following results based on Time Range selection: ◦ 3 Months will display the current quarter plus the previous quarter ◦ 6 Months will display the current quarter plus the

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.





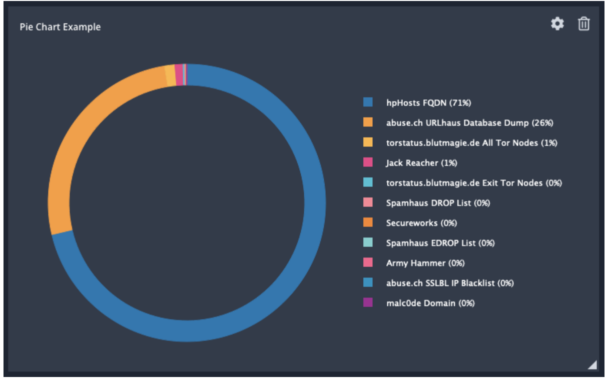
Complete the following fields to add a Count widget to your custom dashboard.

FIELD	DESCRIPTION
Title	The title that will appear above the widget.
Automatically Update	The refresh time for the data. Options include: • 15 Minutes • 30 Minutes • 60 Minutes • None
Data to Show in Widget	Select the data collection 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 Chart

> 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.



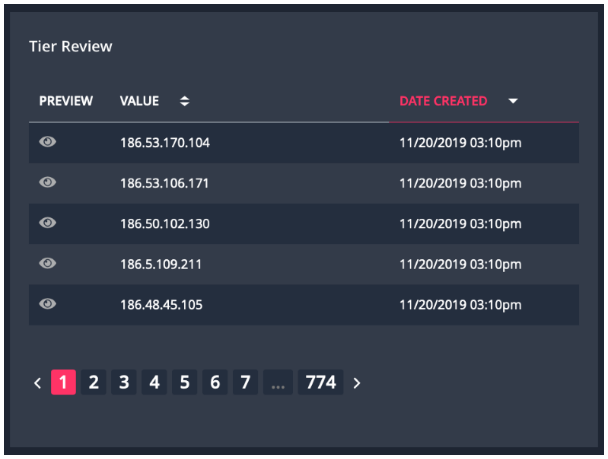
FIELD	DESCRIPTION
Title	The title that will appear above the widget.
Automatically Update	The refresh time for the data. Options include: • 15 Minutes • 30 Minutes • 60 Minutes • None
Data Collection	Select the data collection to populate the data.
Object	Select a specific object type to display.
Group By	Select a data column to sort the information such as source, tags, etc.

Table

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 details.

If your table lists files, you also have the option to preview or download each file as long as the file is not malware locked.

> You cannot preview a malware locked file.



Tier Review

PREVIEW	VALUE	DATE CREATED
👁	186.53.170.104	11/20/2019 03:10pm
👁	186.53.106.171	11/20/2019 03:10pm
👁	186.50.102.130	11/20/2019 03:10pm
👁	186.5.109.211	11/20/2019 03:10pm
👁	186.48.45.105	11/20/2019 03:10pm

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
Data Collection	Select the data collection to populate the data.

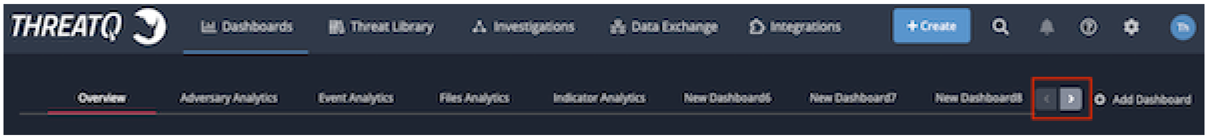
FIELD	DESCRIPTION
Object	Select a specific object type to display.
Group By	Select a data column to sort the information such as source, tags, etc.
Manage Columns	Select the data columns to display in the table.
Sorting	Select the column to sort the table and the order (ascending/ descending).

Dashboard Management

Access to dashboards is determined by your user role and Sharing permission level.

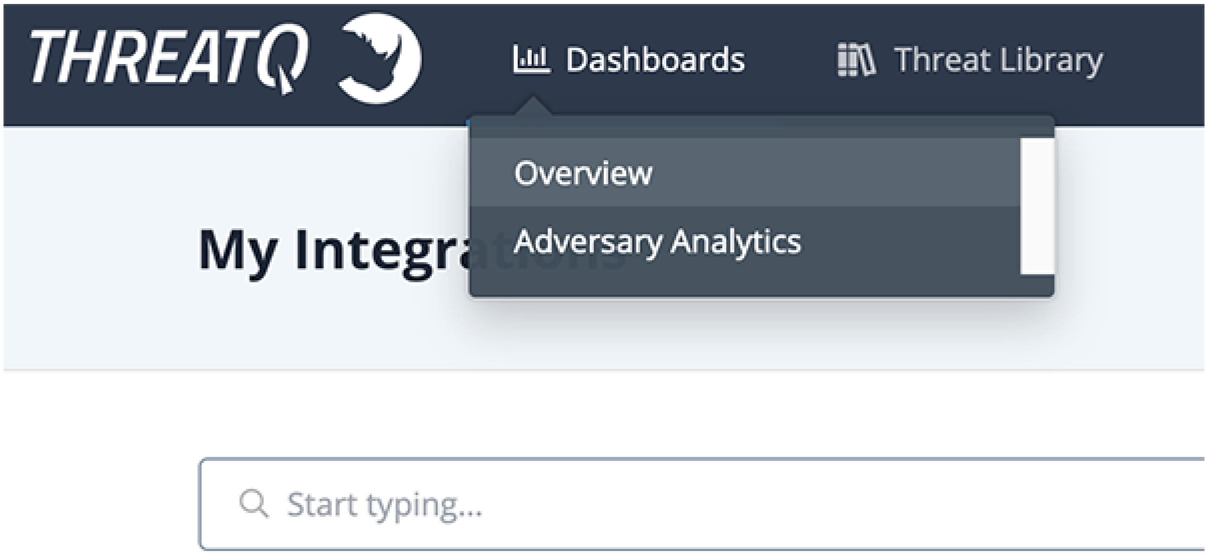
Accessing a Dashboard

If your dashboard view includes more tabs than can be displayed in a single screen, the left and right arrows on the right side of the screen allow you to scroll through the list of dashboard tabs.

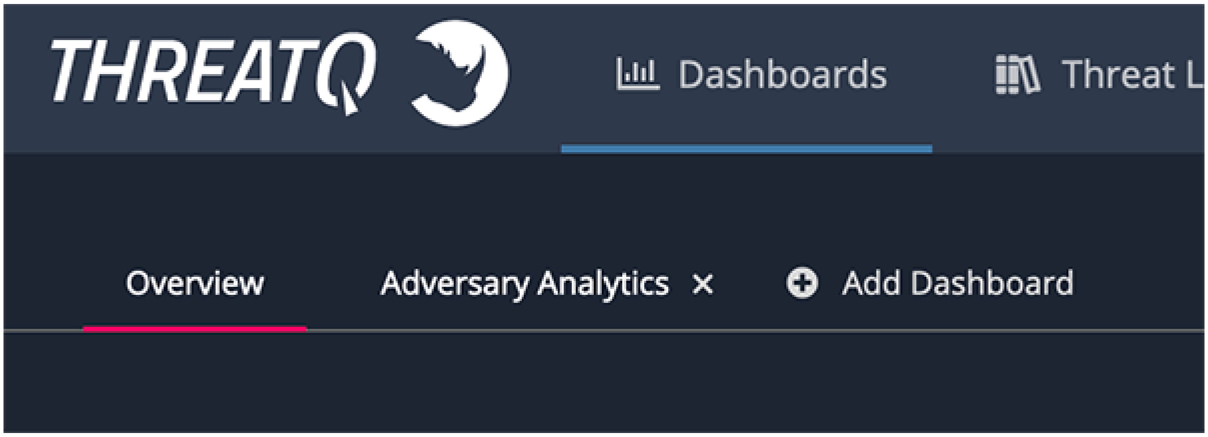


You can access a specific custom dashboard using the following methods:

- Click the **Dashboards** link in the top navigation and select a dashboard from the dropdown menu.

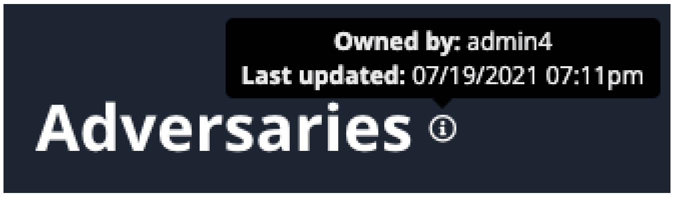


- When viewing a dashboard, click another dashboard tab. If you are not viewing a dashboard at the time, you can click on the ThreatQ logo to load your default dashboard.



After you select a dashboard, you can click the ⓘ icon next to the dashboard name to view:

- Dashboard owner
- Date and time of the last change to the dashboard



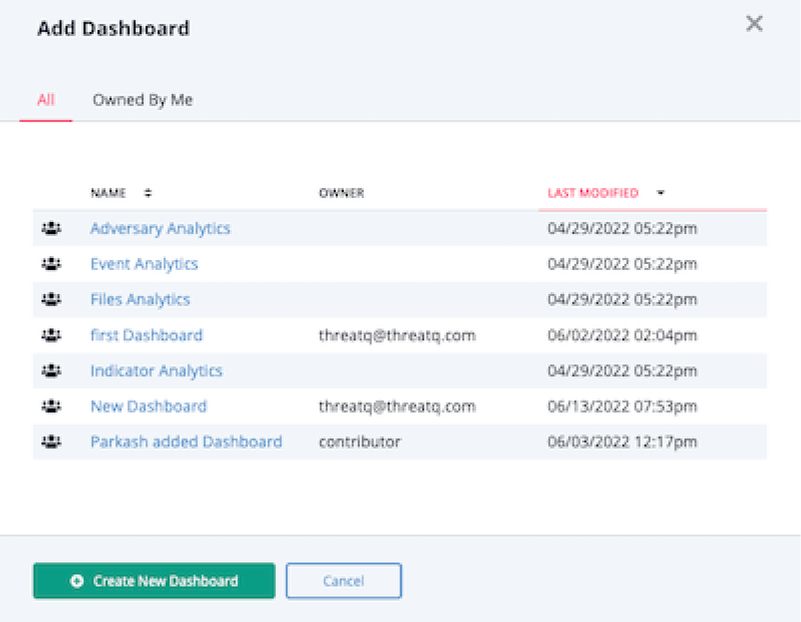
Owned by: admin4
Last updated: 07/19/2021 07:11pm

Add an Existing Dashboard to Your View

You can customize your dashboard view by adding a dashboard you created, a default dashboard, or a dashboard shared with you by another user.

1. Navigate to the ThreatQ landing page.
2. Click the Add Dashboard link.
   The Add Dashboard window displays an All and an Owned By Me tab. The All tab lists all of the dashboards you have access to including default, shared, and owned dashboards. The Owned By Me tab lists only the dashboards for which you are designated as the owner.

   > If you are a read-only user or do not own any dashboards, the Owned By Me tab is grayed out and inactive.



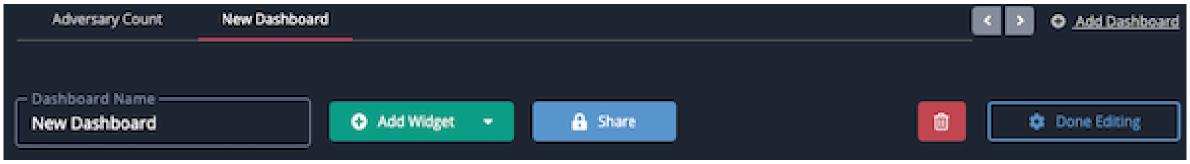
NAME	OWNER	LAST MODIFIED
Adversary Analytics		04/29/2022 05:22pm
Event Analytics		04/29/2022 05:22pm
Files Analytics		04/29/2022 05:22pm
first Dashboard	threatq@threatq.com	06/02/2022 02:04pm
Indicator Analytics		04/29/2022 05:22pm
New Dashboard	threatq@threatq.com	06/13/2022 07:53pm
Parkash added Dashboard	contributor	06/03/2022 12:17pm

3. Click the dashboard you want to add to your view.

Creating a Dashboard

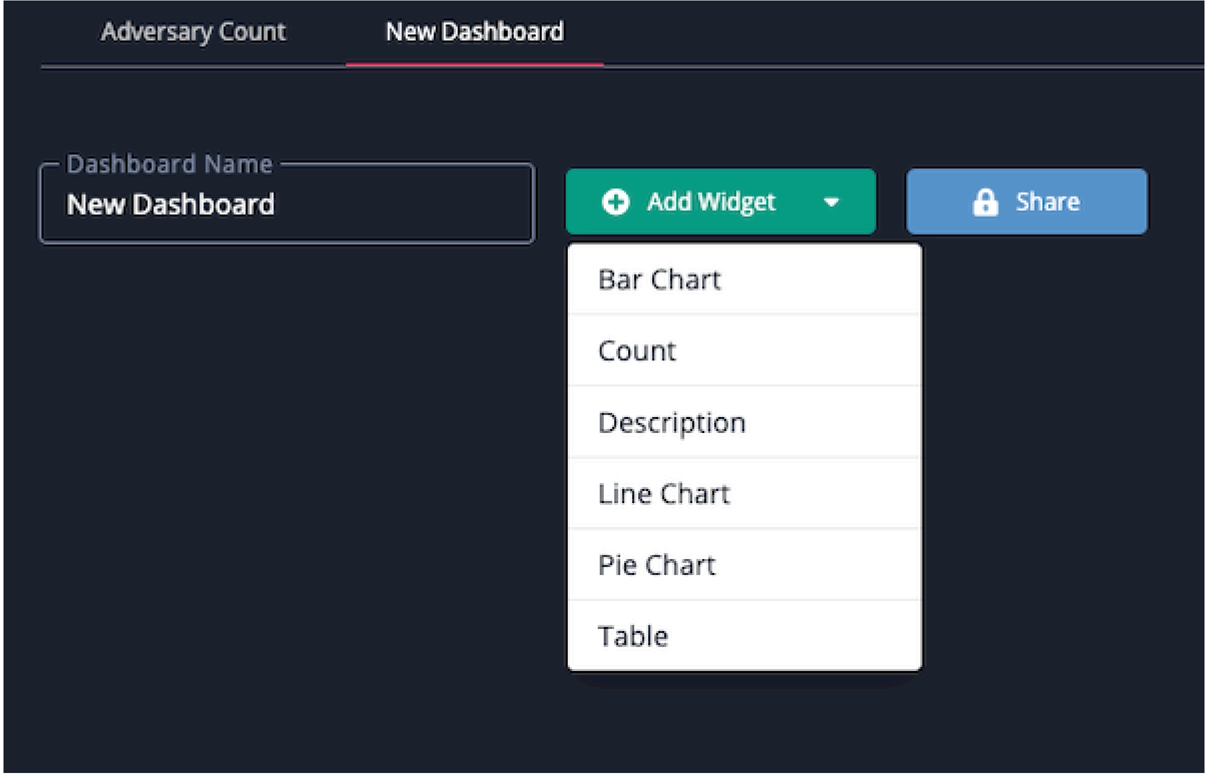
All User Roles, except Read-Only Access can create custom dashboards.

1. Navigate to the ThreatQ landing page.
2. Click one of the following options:
   - **Create New Dashboard** - If your view includes all the dashboards that you created and that are shared with you, click this link to begin creating a new dashboard.
   - **Add Dashboard** - If your view does not include all of the dashboards you created or that are shared with you, click this link to access the Add Dashboard window and then click the Create New Dashboard button.
3. Enter the **Dashboard Name**.



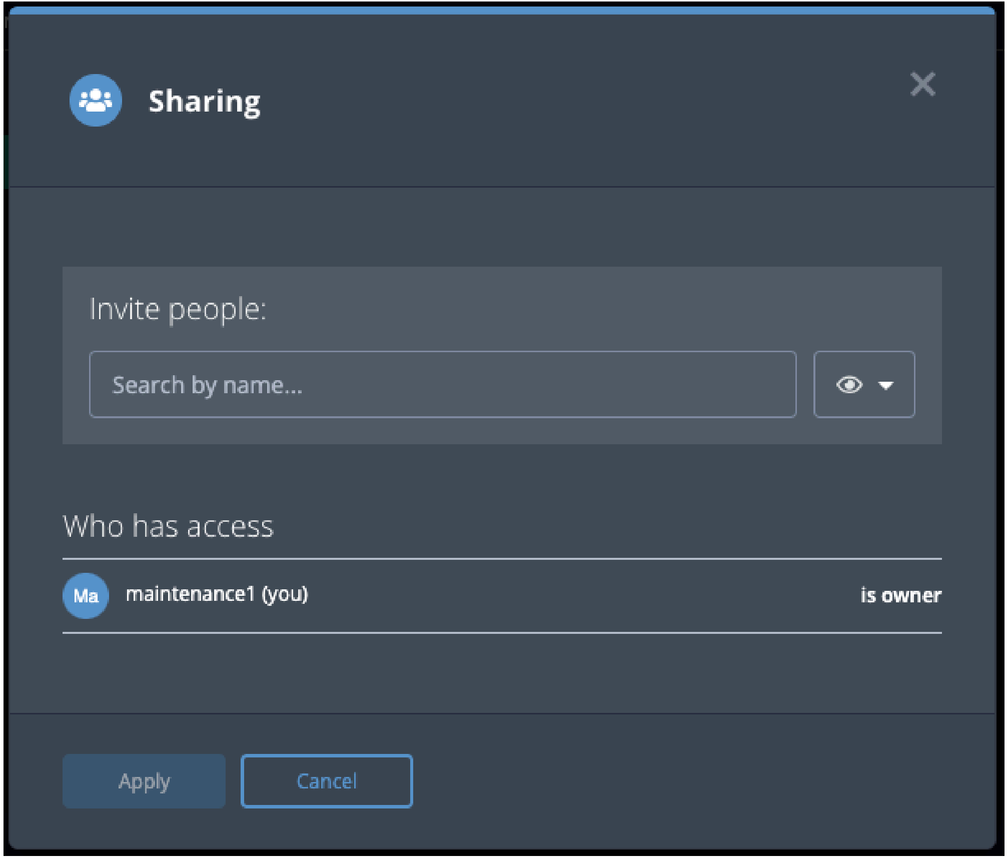
Dashboard Name: New Dashboard

4. Click the **Add Widget** button and select the type of widget to add.



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 the widget header and dragging it around the page.

7. Click on the **Share** button and specify user access to the dashboard. See the Dashboard Sharing topic for more details.

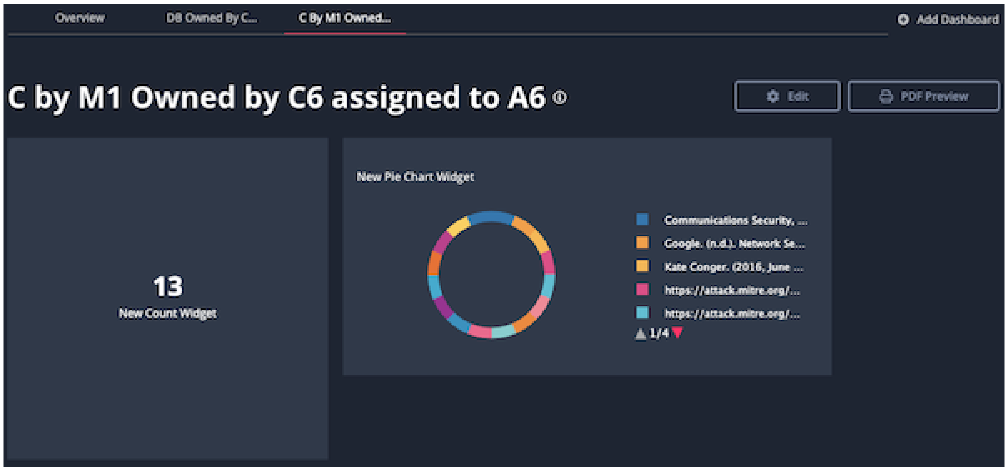


8. Click the **Done Editing** button to save the dashboard.

Editing a Dashboard

You can only edit a Dashboard for which you have owner or editor permissions.

1. Switch to the custom dashboard you want to edit.
2. Click the **Edit** button.


Overview
DB Owned By C...
C By M1 Owned...
Add Dashboard
C by M1 Owned by C6 assigned to A6
Edit
PDF Preview
13
New Count Widget
New Pie Chart Widget
Communications Security, ...
Google. (n.d.). Network Se...
Kate Conger. (2016, June ...
https://attack.mitre.org/...
https://attack.mitre.org/...
1/4

3. You can click the gear ⚙ icon in the header of a widget to edit individual widget settings. You can click the delete 🗑 icon to delete the widget.

> If you add and save a new widget that references a data collection, all users who have access to the dashboard are also granted viewing access to the data collection.

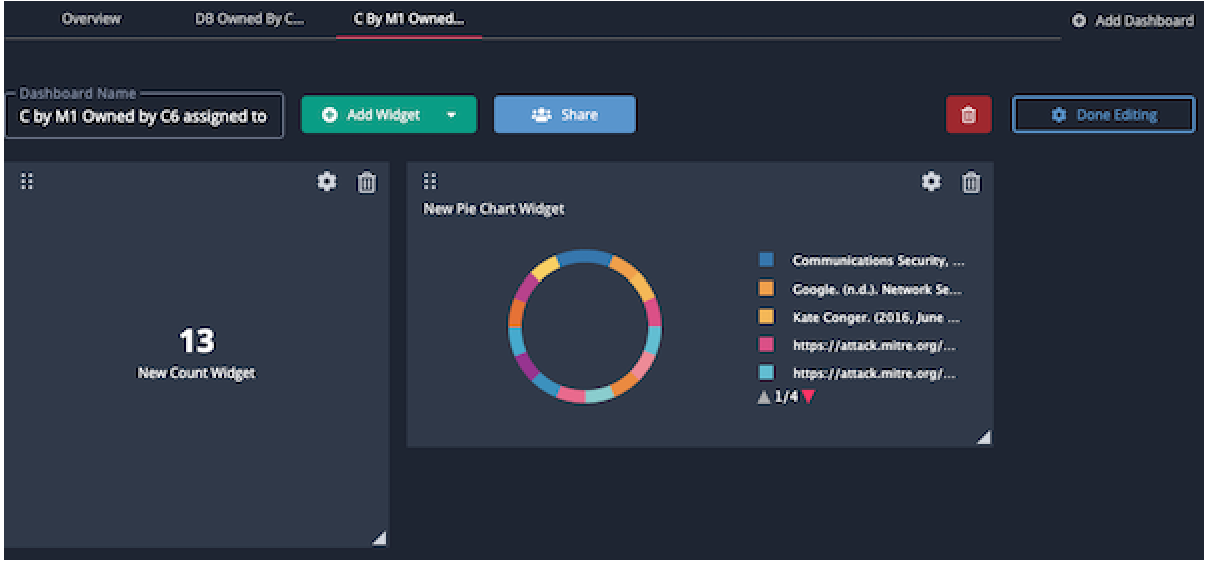
4. After you make your changes, click the **Done Editing** button to save all updates.

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 cannot delete the default system dashboard or dashboards created by other users.

1. Switch to the custom dashboard you want to delete.
2. Click the **Edit Dashboard** button.
3. Click the red delete icon next to the **Done Editing** button.


Overview
DB Owned By C...
C By M1 Owned...
Add Dashboard
Dashboard Name
C by M1 Owned by C6 assigned to
Add Widget
Share
Done Editing
13
New Count Widget
New Pie Chart Widget
Communications Security, ...
Google. (n.d.). Network Se...
Kate Conger. (2016, June ...
https://attack.mitre.org/...
https://attack.mitre.org/...
1/4

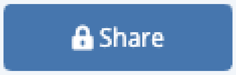
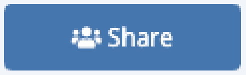
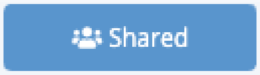
4. Confirm the deletion by clicking the **Delete Dashboard** button in the **Are you sure?** window.

Reassigning a Dashboard of a Deleted User

When you delete a user, you must reassign ownership of his dashboards or they will be automatically deleted with his account. See the Managing User Accounts topic for more details.

Dashboard Sharing

Owners and editors have the option to share a dashboard with other users. However, only the dashboard owner can remove a user's permissions entirely. In addition, the Share(d) button displayed to depends on your permission level and the sharing status of the dashboard.

PERMISSION LEVEL	SHARED WITH OTHERS?	SHARE(D) BUTTON
Owner	No	 Share
Owner, Editor	Yes	 Share
Viewer	Yes	 Shared

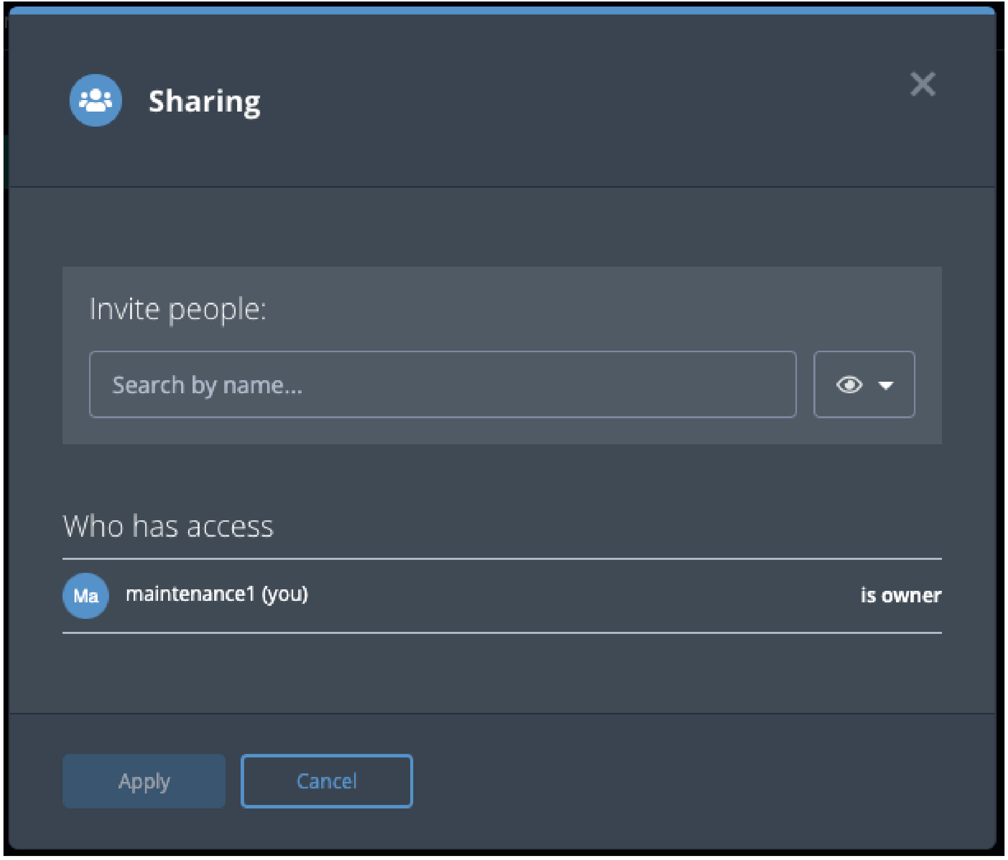
See the Sharing topic for more information on the permissions you can assign to each dashboard.

Sharing a Dashboard

Dashboard owners and editors can update sharing settings for a dashboard at any time.

1. Enter a dashboard's **Edit** view.

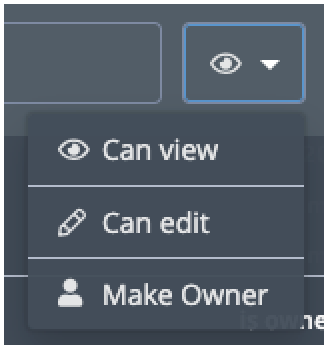
2. Click the **Share** button.
   The Sharing window allows you to select the user(s) to which you want to grant access.



3. Click the arrow next to the 👁 icon to select the user's permission level.

> If you are granting access to all users, you must select the **Can View** option. You can only assign editing permission to individual users not to all users.

> If you assign owner permissions to another user, your permissions automatically change to editor-level.



4. Use the search field to locate and select a user's name or the **Everybody (Public)** option. This option grants view-only access to all users.

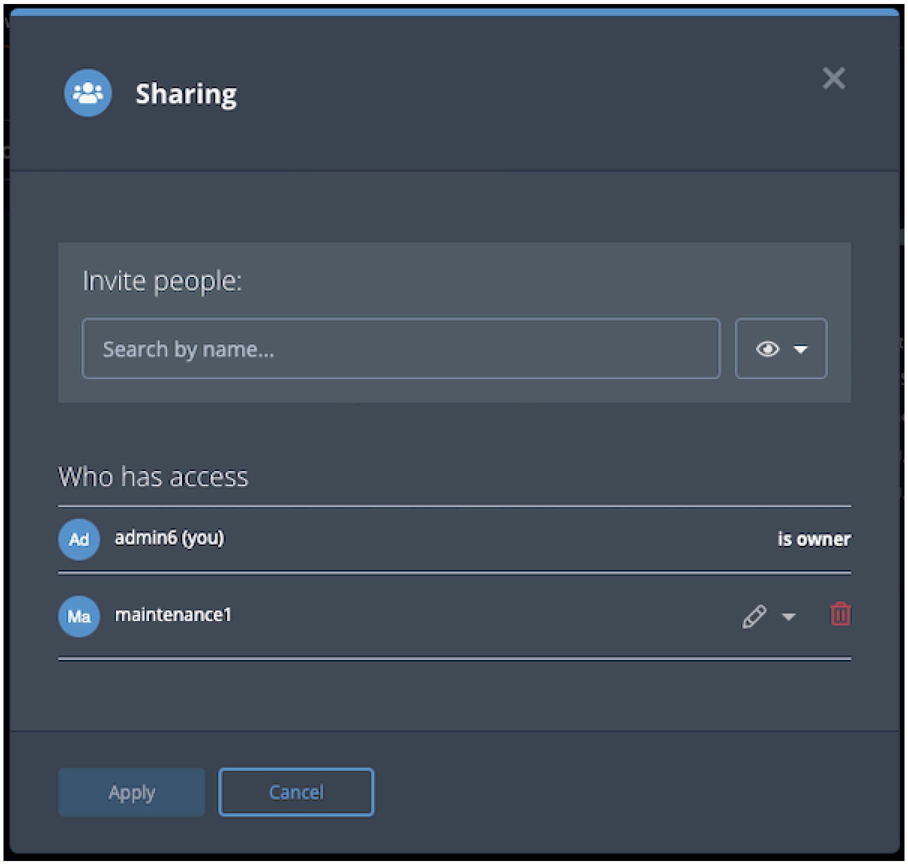
The user is now listed in the **Who has access** list. From this listing, you can change or delete the user's permissions.

> When you share a dashboard with a user, you also give him viewing permissions for all data collections used by the dashboard's widgets.

5. Click the Apply button to save the user's permission level.

Updating Dashboard Permissions

1. Enter a dashboard's **Edit** view.
2. Click the **Share** button.
   The Sharing window lists the users who have access to the dashboard.



3. From the Sharing window, you can:
   - **Remove a user's permissions** - If you are the dashboard owner, click the trashcan icon to the right of the user name.
   - **Change a user's permission** - Click the arrow next to the user's current permission icon and select a new permission level.

4. Click the **Apply** button to save the user's permission level.

Shared Dashboards of a Deleted User

When you delete the owner of a dashboard from the platform, ThreatQ prompts you to reassign the dashboard to another user or to delete it. See the Managing User Accounts topic for more details.

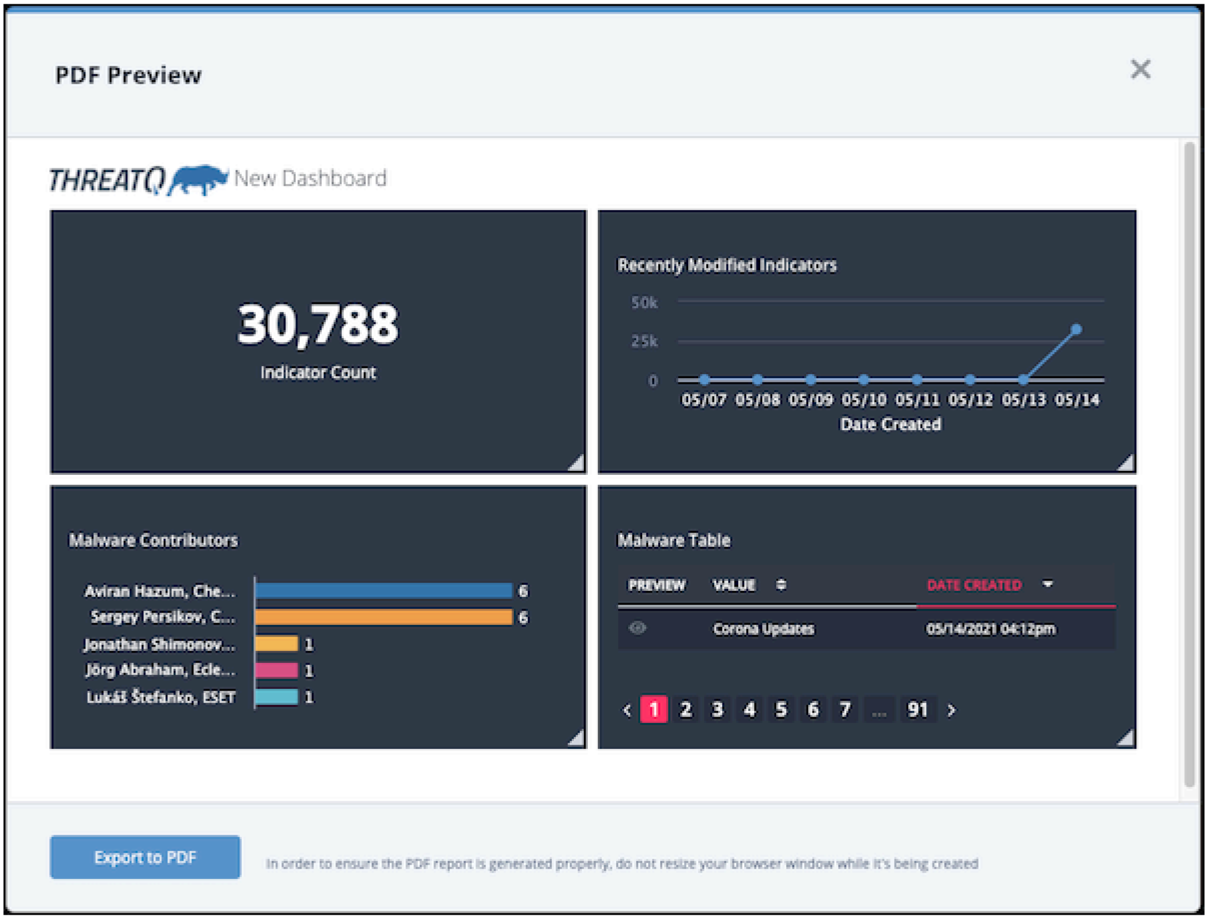
Dashboard Export

When you select a custom dashboard, the PDF Preview button gives you the option to export a PDF copy of all the widgets in the dashboard. The PDF preview window allows you to rearrange the widget order before you print and/or save the PDF.

> You cannot export the default dashboard or the Analytics dashboards to PDF.

Creating a Dashboard PDF

1. Navigate to the ThreatQ landing page.
2. Click a custom dashboard.
3. Click the **PDF Preview** button.



PREVIEW	VALUE	DATE CREATED
👁	Corona Updates	05/14/2021 04:12pm

In order to ensure the PDF report is generated properly, do not resize your browser window while it's being created

4. Review the layout of the PDF. You can use the following methods to customize the widget display:

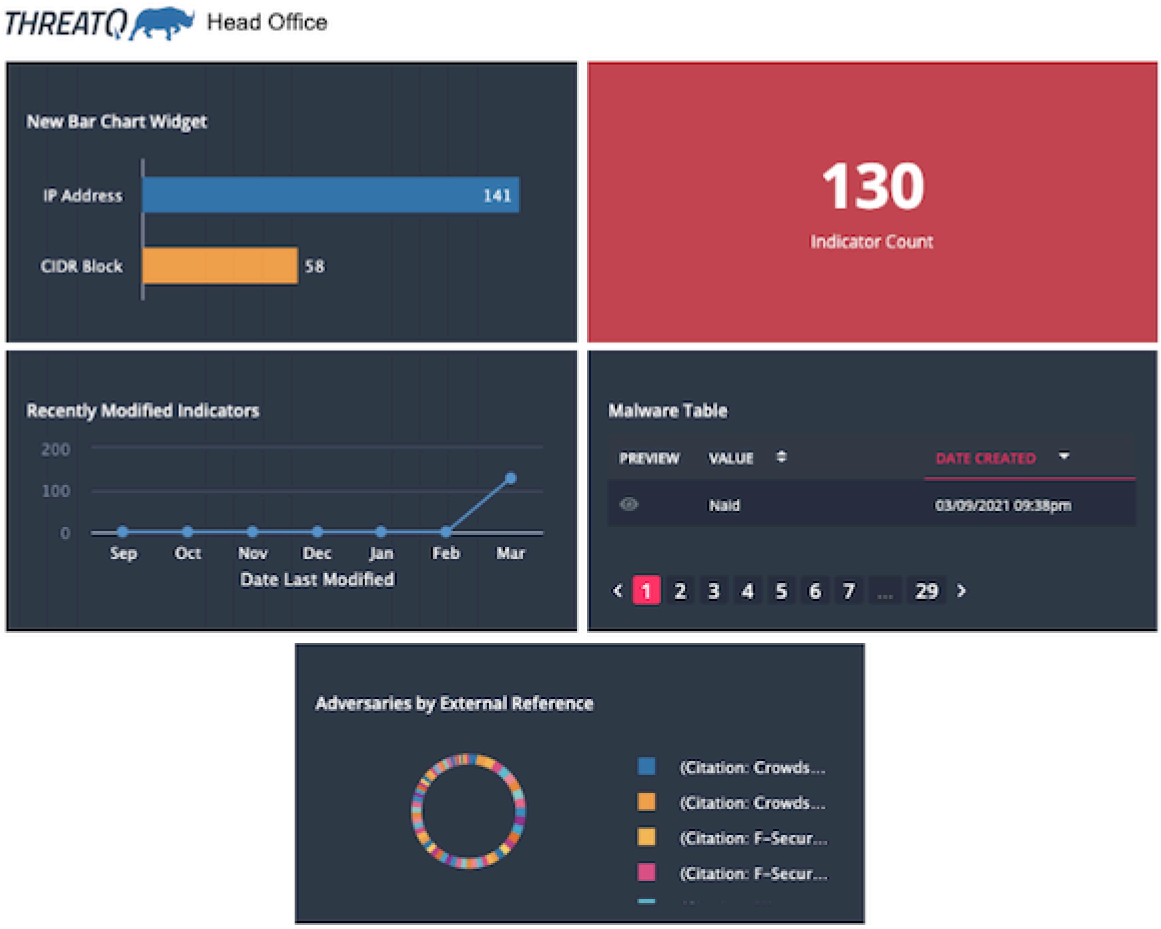
> ThreatQ saves your changes locally so that you do not have to repeat the process the next time you generate a PDF for the dashboard.

- Click a widget header then drag and drop to move it to a new location on the page.
- Resize a widget by clicking and dragging the bottom-right grey corner.

5. Click the **Export to PDF** button.
   The system exports the dashboard widgets to a PDF file which you can save and/or print. The PDF file name defaults to dashboard.pdf. The PDF title includes the ThreatQ logo and the name of your dashboard.

> ⚠ Do not attempt to resized your browser window during PDF generation.

Sample PDF:



PREVIEW	VALUE ⇕	DATE CREATED ▾
👁	Naid	03/09/2021 09:38pm

‹ 1 2 3 4 5 6 7 ... 29 ›

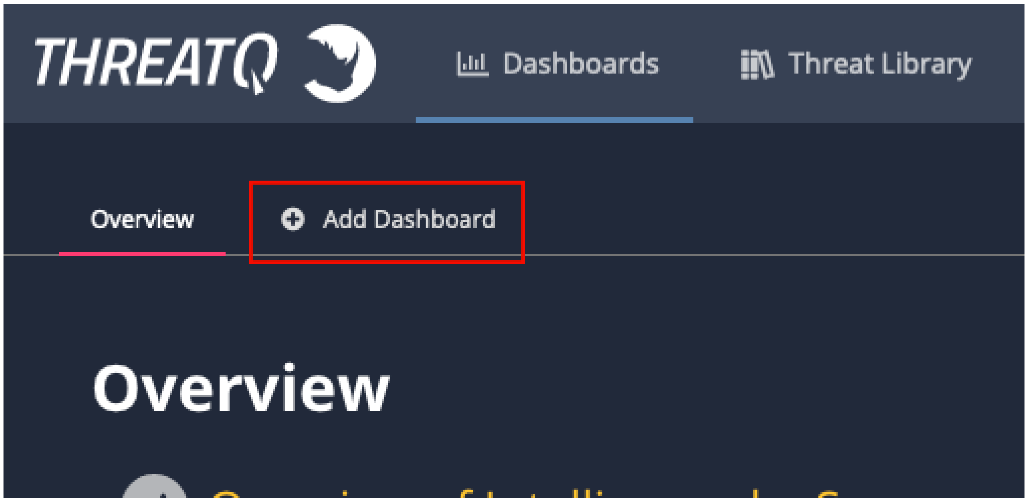
User View Management

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.

> Any dashboard that is part of your User View will also be listed in the Dashboards dropdown menu.

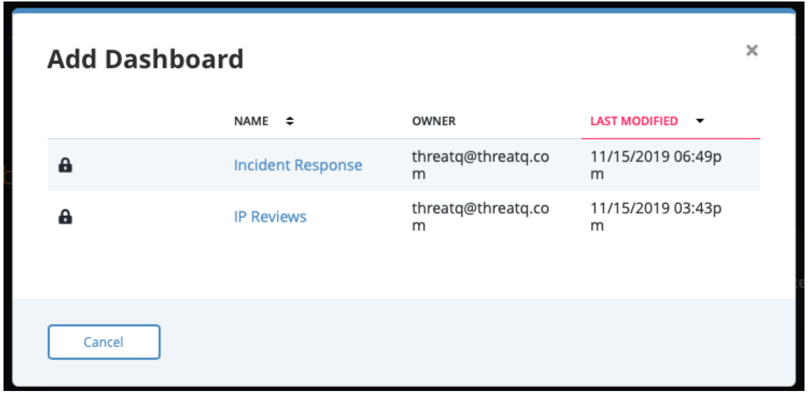
Adding a Dashboard to Your View

You can add dashboards that have been shared with you as well as your own private dashboards that are not currently part of your view.

1. Navigate to the ThreatQ landing page.
2. Click the **Add Dashboard** button.


> If there are no available shared dashboards, the **Add Dashboard** link will be replaced with **Create New Dashboard**.

The Add Dashboard window lists the dashboards that have been shared with you and any of your private dashboards that are not currently part of your view.



Add Dashboard

	NAME	OWNER	LAST MODIFIED
🔒	Incident Response	threatq@threatq.com	11/15/2019 06:49pm
🔒	IP Reviews	threatq@threatq.com	11/15/2019 03:43pm

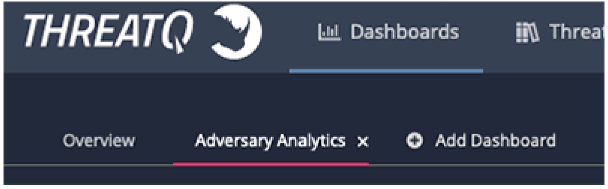
3. Click a dashboard in the list to add it to your view.

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. This process does not delete the dashboard from the platform. See the Dashboard Management topic for instructions on how to delete a dashboard.

1. Hover your cursor over the name of the dashboard you want to remove.

   An **X** icon will appear to the right of the dashboard name.



2. Click 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.

1. Navigate to a custom dashboard.
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 are saved automatically. These changes also update the order in the Dashboards dropdown menu.

Data Controls

The Data Controls section of the ThreatQ platform allows you to setup and configure:

SECTION	DETAILS
Indicator Expiration Policies	Configure expiration policies to automatically deprecate stale intelligence as it becomes less relevant.
Scoring Algorithms	Configure scoring to filter through the millions of indicators your platform has ingested to focus on the data that really applies to your environment while retaining all other indicators and context for threat research.
Traffic Light Protocol (TLP)	Configure your Traffic Light Protocol (TLP) schema to provide a set of designations to ensure that sensitive information is shared with the appropriate audience.
Whitelisted Indicators	Identify non-malicious indicators using the Whitelisting feature.

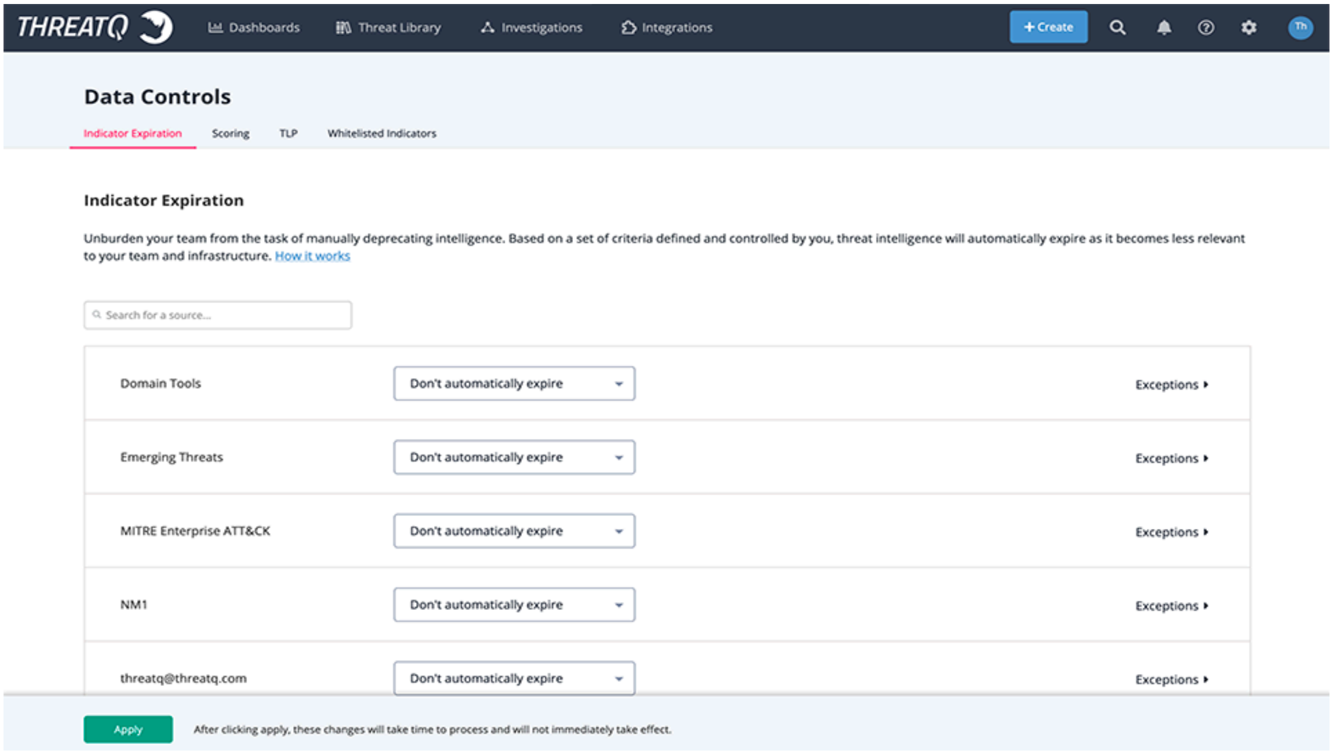
Indicator Expiration Policies

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.

Accessing the Indicator Expiration Page

1. From the navigation menu, click on Threat Library and select **Indicator Expiration** under the *Data Controls* heading.

   The Data Controls page will open with the Indicator Expiration tab selected by default.



Data Controls

Indicator Expiration

Unburden your team from the task of manually deprecating intelligence. Based on a set of criteria defined and controlled by you, threat intelligence will automatically expire as it becomes less relevant to your team and infrastructure. How it works

Domain Tools	Don't automatically expire	Exceptions ▸
Emerging Threats	Don't automatically expire	Exceptions ▸
MITRE Enterprise ATT&CK	Don't automatically expire	Exceptions ▸
NM1	Don't automatically expire	Exceptions ▸
threatq@threatq.com	Don't automatically expire	Exceptions ▸

After clicking apply, these changes will take time to process and will not immediately take effect.

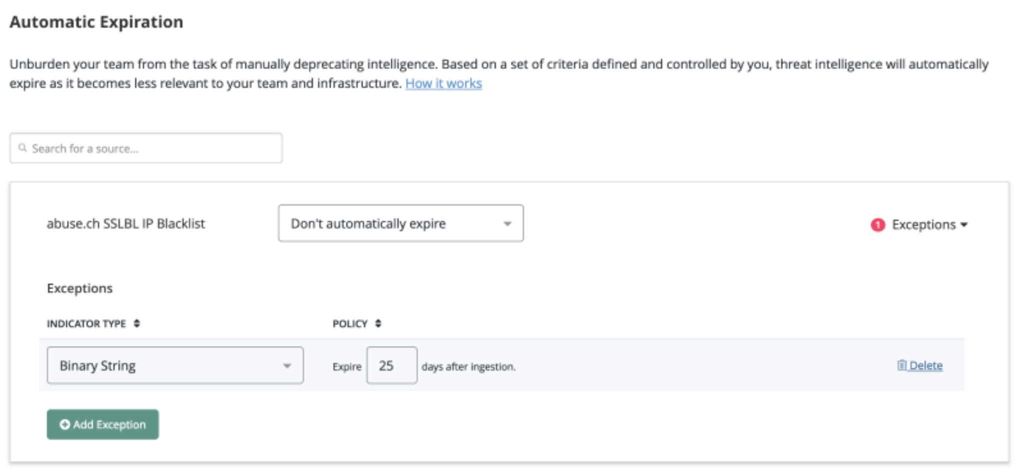
How ThreatQ Calculates Expiration Dates

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 Source with an Exception for that Indicator	If an indicator is reported by a source that has an exception for the indicator, the exception expiration date will be used regardless of 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:

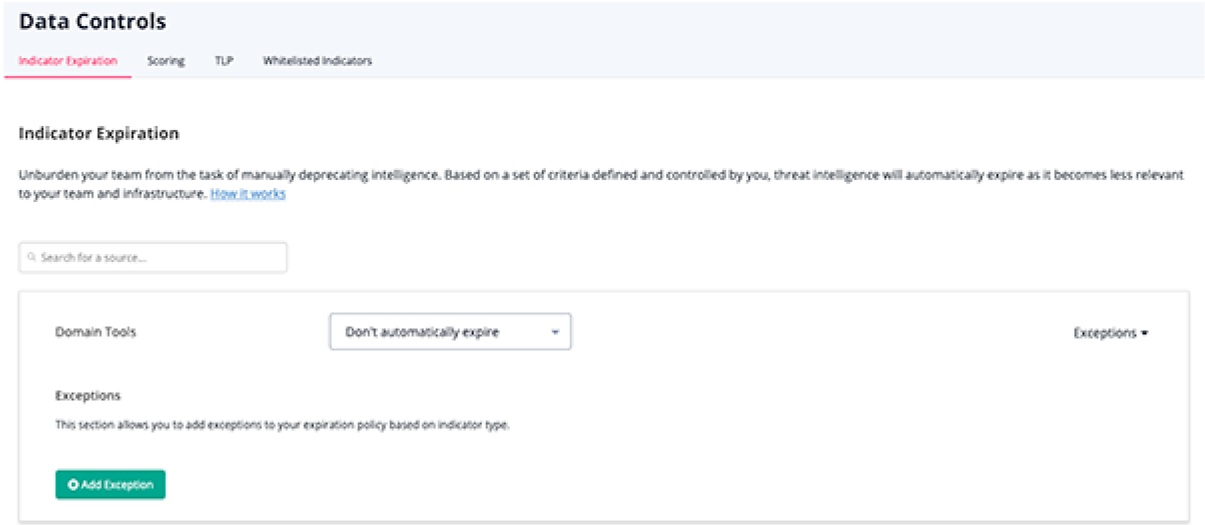
OPTION	DESCRIPTION
Don't automatically expire (No policy set)	ThreatQ sets all feeds to **Don't Automatically Expire** until an analyst decides otherwise. When set, indicators reported from this specific feed do not have an expiration date automatically applied to them. If an indicator is reported by 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 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**.  Automatic Expiration Unburden your team from the task of manually deprecating intelligence. Based on a set of criteria defined and controlled by you, threat intelligence will automatically expire as it becomes less relevant to your team and infrastructure. How it works Search for a source... abuse.ch SSLBL IP Blacklist: Don't automatically expire 1 Exceptions Exceptions INDICATOR TYPE: Binary String POLICY: Expire 25 days after ingestion. Delete Add Exception
Never Expire	Using this setting ensures that all intelligence reported by a specific feed is protected from automatic expiration, regardless of scenario.

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.

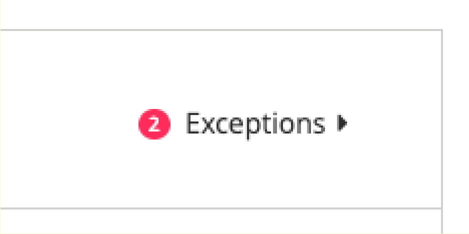
1. From the navigation menu, click on Threat Library and select **Indicator Expiration** under the *Data Controls* heading.
2. Locate the source.
3. Click **Exceptions** to expand the option.

   The Exceptions option menu opens.



Unburden your team from the task of manually deprecating intelligence. Based on a set of criteria defined and controlled by you, threat intelligence will automatically expire as it becomes less relevant to your team and infrastructure. How it works

This section allows you to add exceptions to your expiration policy based on indicator type.

> 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**.

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

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**.
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

SCENARIO	DESCRIPTION
	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 B). 3. When the date switches from 10/17 to 10/18, this indicator is queued to have its status changed to **Expired**.

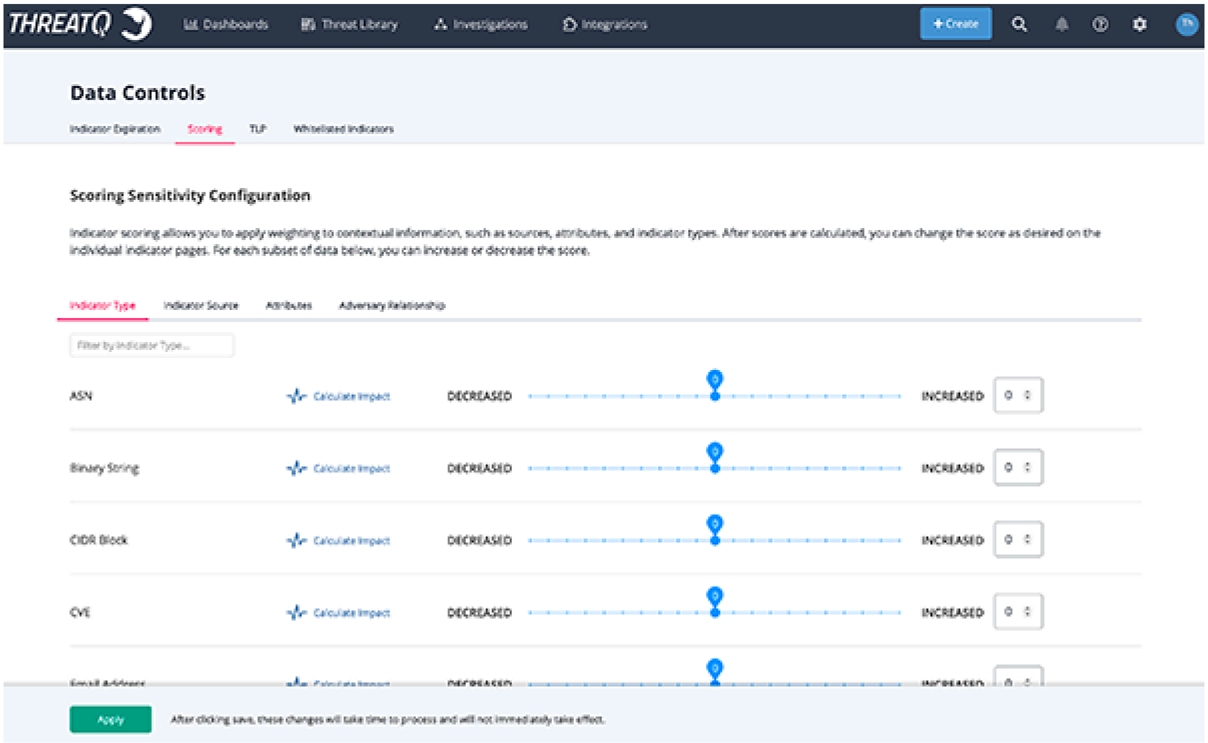
Scoring Algorithms

ThreatQ's scoring algorithms calculate and assign scores to indicators as they are added to the system. By configuring scoring, you can filter through the millions of Indicators that may have been collected to focus on the percentage that applies to your organization. Scoring allows you to prioritize key indicators while still retaining all other indicators and context for threat research.

ThreatQ's Overview dashboard contains the Overview of Intelligence by Score which shows the current distribution of indicator scores. You can also filter Threat Library searches by score and create data collections based on scoring.

Accessing the Scoring Sensitivity Page

From the navigation menu, click Threat Library and select **Scoring** under the *Data Controls* heading. The Data Controls page opens with the Scoring tab and Indicator Type sub-tab selected.



Indicator scoring allows you to apply weighting to contextual information, such as sources, attributes, and indicator types. After scores are calculated, you can change the score as desired on the individual indicator pages. For each subset of data below, you can increase or decrease the score.

After clicking save, these changes will take time to process and will not immediately take effect.

Scoring Criteria

ThreatQ's scoring algorithm allows you to influence indicator scores by:

- Indicator Type
- Indicator Source
- Attributes
- Adversary Relationship

Customizing scoring based on these criteria updates the score assigned to the associated indicators.

Scoring Tips and Tricks

- The **Calculate Impact** option identifies how many system objects are affected by a score change.
- Scoring configuration and updates take time to process, the Threat Library does not reflect these changes immediately.
- If you use an indicator’s object details page to manually update its score, the manually selected score overrides any changes to the calculated score caused by updates to the scoring algorithm.
- You have the option to adjust the score sensitivity of indicators. Indicator scores range from 10, which creates a score of **Very High**, to -10, **Very Low**. A higher indicator score creates increased priority for that indicator.

- By default, indicators are set to a neutral score of 0.

Configuring Your Scoring Algorithm for Indicator Types and Sources

Scoring by indicator type allows you to prioritize indicators based on their usefulness to your organization. If your organization cannot process or does not want to use a specific indicator type, such as Fuzzy Hash, you can assign a lower score, such as -3, to the indicator type.

Scoring by indicator source allows you to prioritize indicators based on your confidence in the source of the data. For example, you may have higher confidence in the value of data from paid feeds and would therefore want to assign a higher score, such as a 3, to indicators from these sources.

1. Select the indicator type or source by filtering by source name or by scrolling to the desired indicator.
2. Use one of the following methods to adjust scoring:

  - Click and drag the slider to adjust the score.
  - Click the up/down arrow next to the current score to increase/decrease the score.
3. To save your changes, click the **Apply** button.

Configuring Your Scoring Algorithm for Attributes

The Attributes tab allows you to specify scoring by attribute key and value. You can use attribute scoring to prioritize indicators based on attributes provided by a vendor and/or customer attributes applied by internal users.

> If your organization applies a Department attribute (attribute key) to indicators based on the team targeted by the threat (attribute value), for instance *Department - Tech Pubs*, you can apply higher scores to indicators with attributes associated with high value targets such as *Department - Finance*.

1. From the Attributes tab, click the **Add** button.
2. Use one of the following methods to specify an attribute key:
   - Click the arrow in the Key field to select an attribute type from the dropdown list.
   - Type the attribute key in the Key field.
3. Use one of the following methods to populate the Value field:
   - Enter the attribute value to which the score applies.
   - Enter an attribute value that contains the wildcard character (*). The wildcard specifies that any characters can appear in multiple positions represented by the wildcard.
4. Use one of the following methods to adjust the score:
   - Click and drag the slider to adjust the score.
   - Click the up/down arrow next to the current score to increase/decrease the score.
5. Click the **Add** button to continue adding attribute scoring criteria.
6. Click the **Apply** button to save your attribute scoring.
   The Attributes tab now lists your scoring entry in the following format:
   <Key> is *<Value>*

Configuring Your Scoring Algorithm for Adversary Relationships

The Adversary Relationship tab allows you to configure the scoring of indicators associated with specific adversaries. You can use this scoring to prioritize indicators associated with adversaries that tend target your industry in general and/or your organization specifically.

Adversary relationship scoring supports a wildcard option, *Any Adversary*, that allows you to specify a score for any indicator with a positive attribution.

1. From the Adversary Relationship tab, click the **Add** button.
2. Click the arrow in the Select Adversary field to select an adversary from the dropdown list. You can use the scroll bar or Search field to locate the adversary.

> Select the *Any Adversary* option to prioritize any indicator with a positive attribution.

3. Use one of the following methods to adjust the score:
    - Click and drag the slider to adjust the score.
    - Click the up/down arrow next to the current score to increase/decrease the score.
4. Click the **Add** button to continue adding adversary relationship scoring.
5. Click the **Apply** button to save your scoring.

Updating Your Scoring Algorithms

After you set up your initial scoring, you can update assigned scores to reflect changes in your threat environment and priorities. Periodic reviews and updates to your scoring algorithms ensure they reflect:

- Changes to your risk profile based on political or organization changes.
- New adversaries
- New adversary tactics
- New tool sets

1. Click the appropriate tab (Indicator Type, Indicator Source, Attributes, Adversary Relationship).
2. Use one of the following methods to adjust the score:
    - Click and drag the slider to adjust the score.

  - Click the up/down arrow next to the current score to increase/decrease the score.
3. Click the **Apply** button to save your update.

Traffic Light Protocol (TLP)

Traffic Light Protocol (TLP) schema provides a set of labels 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** section in the Managing Exports topic for more details.

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

Labels

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

LIGHT	LABEL	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 label.

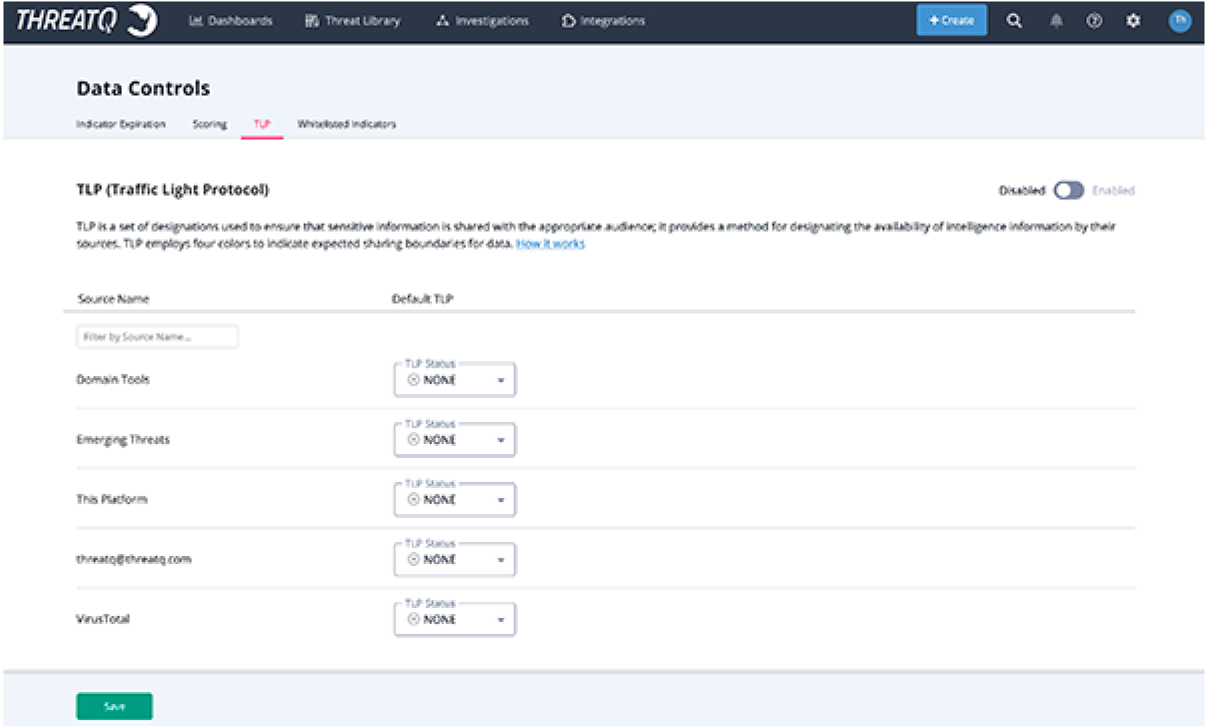
Source Provided Data	TLP label received from ingested data.
Source Default	Administrators can set a source's default TLP label. See the Add TLP to Source section.
No TLP	A TLP label has not been set for the source.

Access TLP Settings

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

1. From the navigation menu, click on Threat Library and select **TLP** under the *Data Controls* heading.

   The Data Controls page will load with TLP tab selected by default.



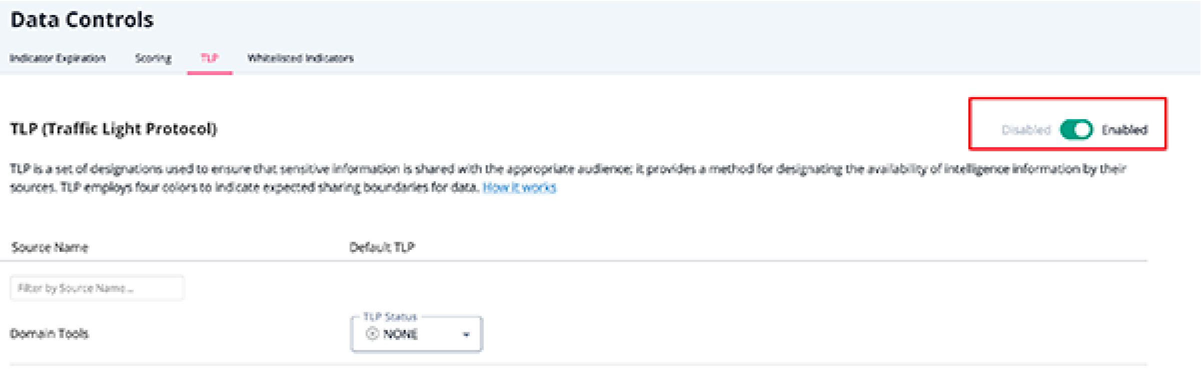
TLP is a set of designations used to ensure that sensitive information is shared with the appropriate audience; it provides a method for designating the availability of intelligence information by their sources. TLP employs four colors to indicate expected sharing boundaries for data. How it works

Source Name	Default TLP
Domain Tools	TLP Status: NONE
Emerging Threats	TLP Status: NONE
This Platform	TLP Status: NONE
threatq@threatq.com	TLP Status: NONE
VirusTotal	TLP Status: NONE

Configure TLP Visibility

System administrators can set visibility settings to either hide or show TLP labels to users. Enabled indicates that TLP labels are visible to users.

1. Click the **Enabled/Disabled** toggle.



TLP (Traffic Light Protocol)

TLP is a set of designations used to ensure that sensitive information is shared with the appropriate audience; it provides a method for designating the availability of intelligence information by their sources. TLP employs four colors to indicate expected sharing boundaries for data. How it works

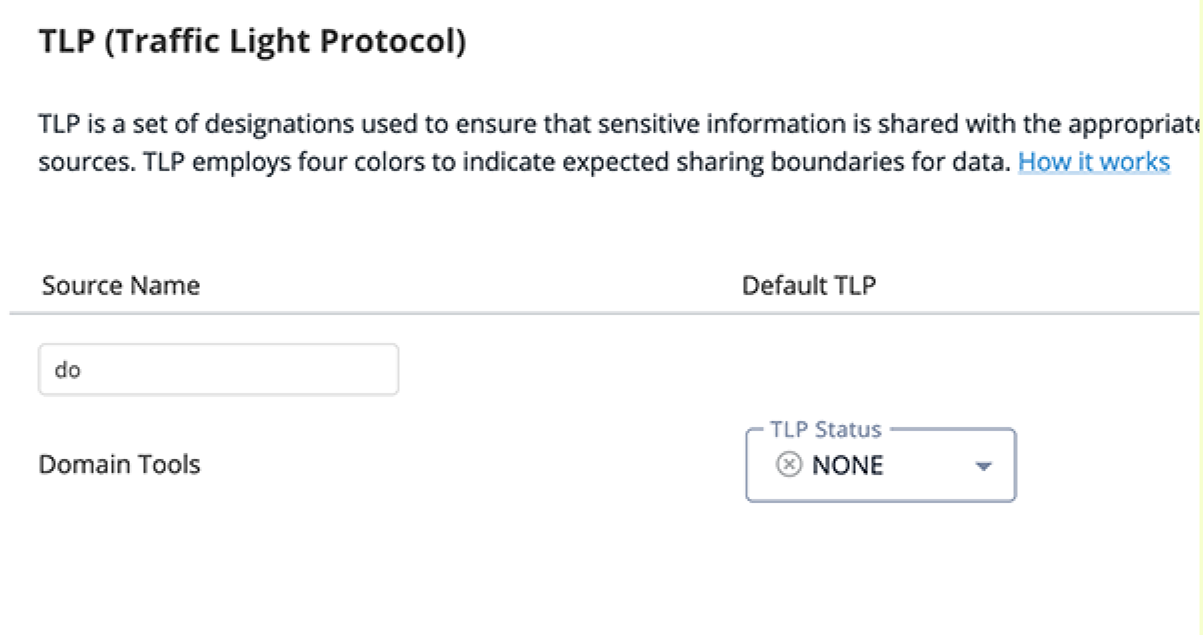
Domain Tools

> You do not need to click the **Save** button. Changes to the Enabled/Disabled status are made immediately.

Apply a TLP Label to Source

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

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



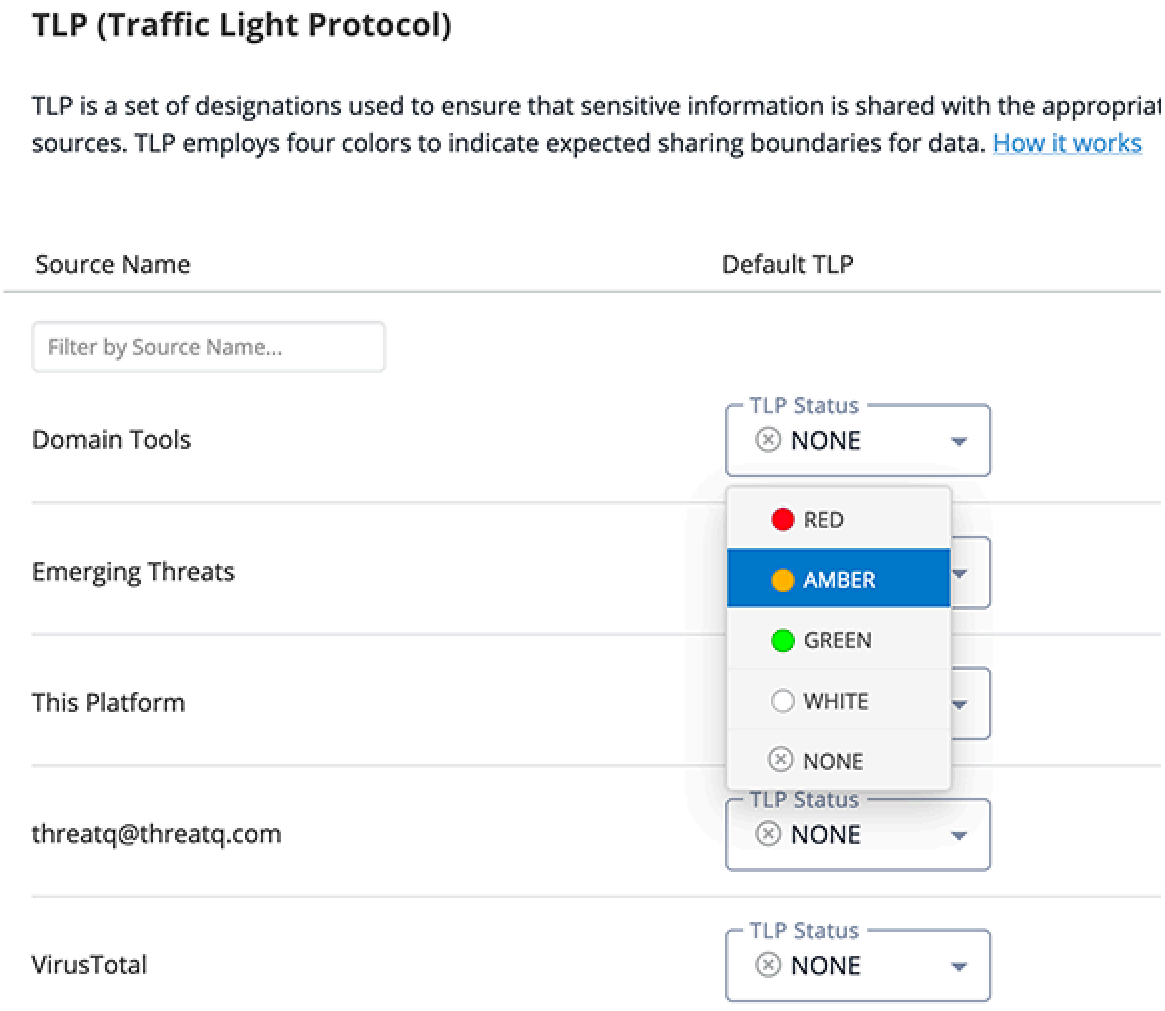
TLP (Traffic Light Protocol)

TLP is a set of designations used to ensure that sensitive information is shared with the appropriat
sources. TLP employs four colors to indicate expected sharing boundaries for data. How it works

do

Domain Tools

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



TLP (Traffic Light Protocol)

TLP is a set of designations used to ensure that sensitive information is shared with the appropriat sources. TLP employs four colors to indicate expected sharing boundaries for data. How it works

Source Name	Default TLP
Domain Tools	TLP Status: NONE
Emerging Threats	
This Platform	
threatq@threatq.com	TLP Status: NONE
VirusTotal	TLP Status: NONE

3. Click **Save**.

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

Whitelisted Indicators

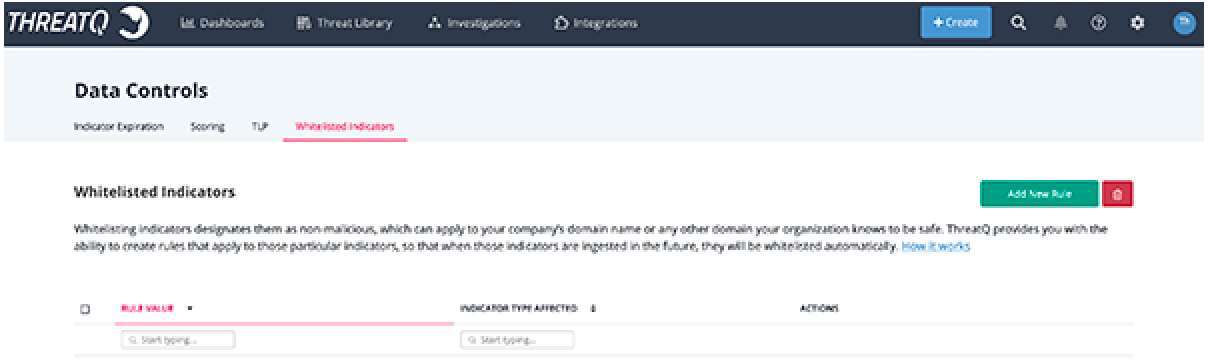
There are some Indicators that should be considered to be whitelisted, or non-malicious, and we do not want those indicators going out to other systems. For example, a company's own domain name would never need to be blocked.

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.

Accessing the Whitelisted Indicator Rules

1. From the navigation menu, click on Threat Library and select **Whitelisting** under the *Data Controls* heading.

   The Data Controls page will open with the Whitelisted Indicators tab selected by default.



Whitelisting indicators designates them as non-malicious, which can apply to your company's domain name or any other domain your organization knows to be safe. ThreatQ provides you with the ability to create rules that apply to those particular indicators, so that when those indicators are ingested in the future, they will be whitelisted automatically. How it works

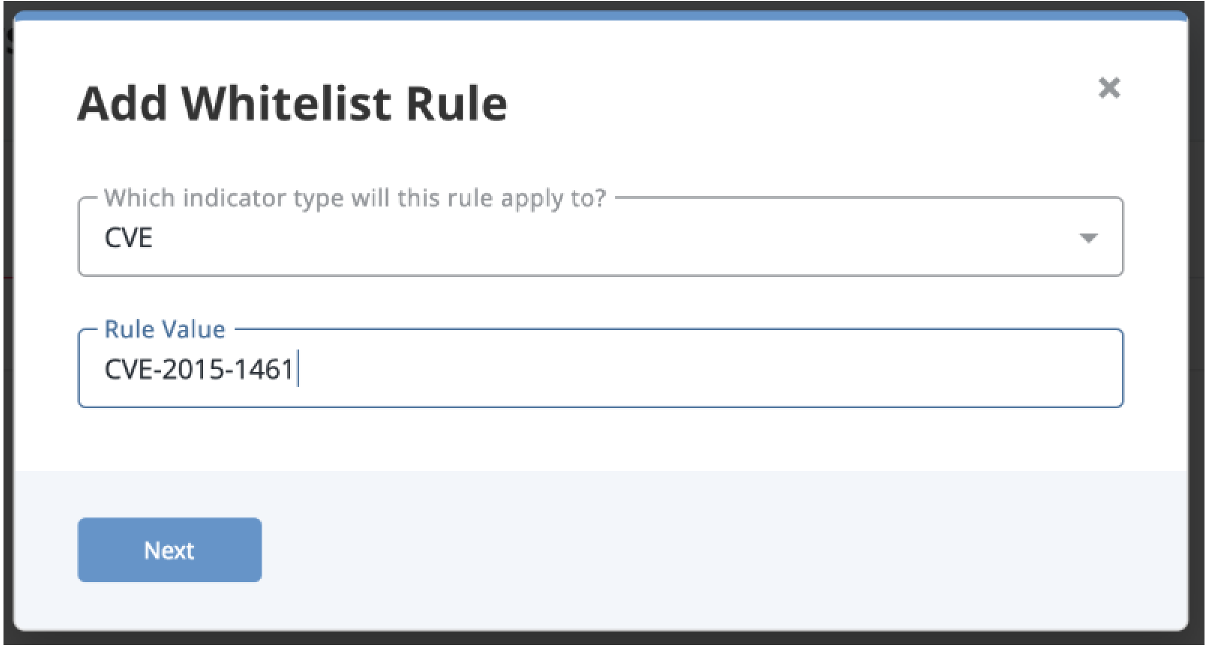
Creating a Whitelisted Rule

> ThreatQ prevents you from creating duplicate whitelist rules through the user interface or an API. If you attempt to do so, the system returns an error message.

From the Whitelisted Indicators Page:

1. Click **Add Rule**.

The Add Whitelist Rules dialog box opens.



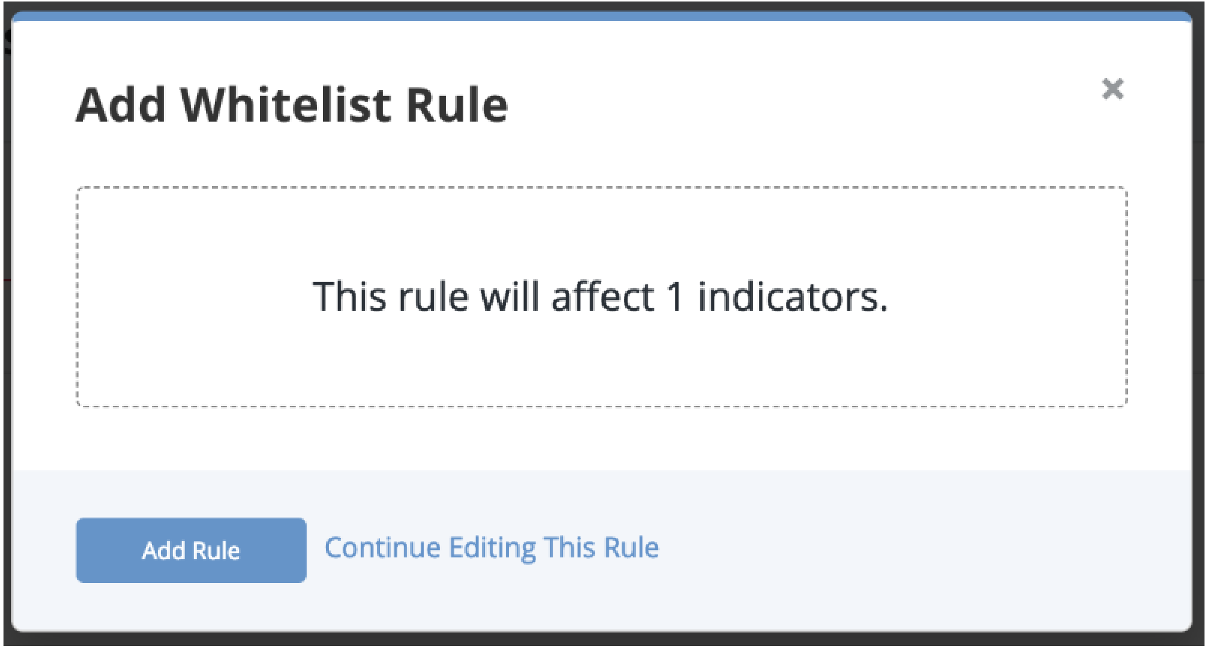
Add Whitelist Rule

Which indicator type will this rule apply to?: CVE

Rule Value: CVE-2015-1461

2. Select the Indicator type the rule will apply to.
3. Add a Rule Value.
4. Click **Next**.

   Affected indicators are listed in the dialog box.



Add Whitelist Rule

This rule will affect 1 indicators.

5. 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.

6. Click **Continue Editing this Rule**.

7. If you are satisfied with the rule, click **Add Rule**.

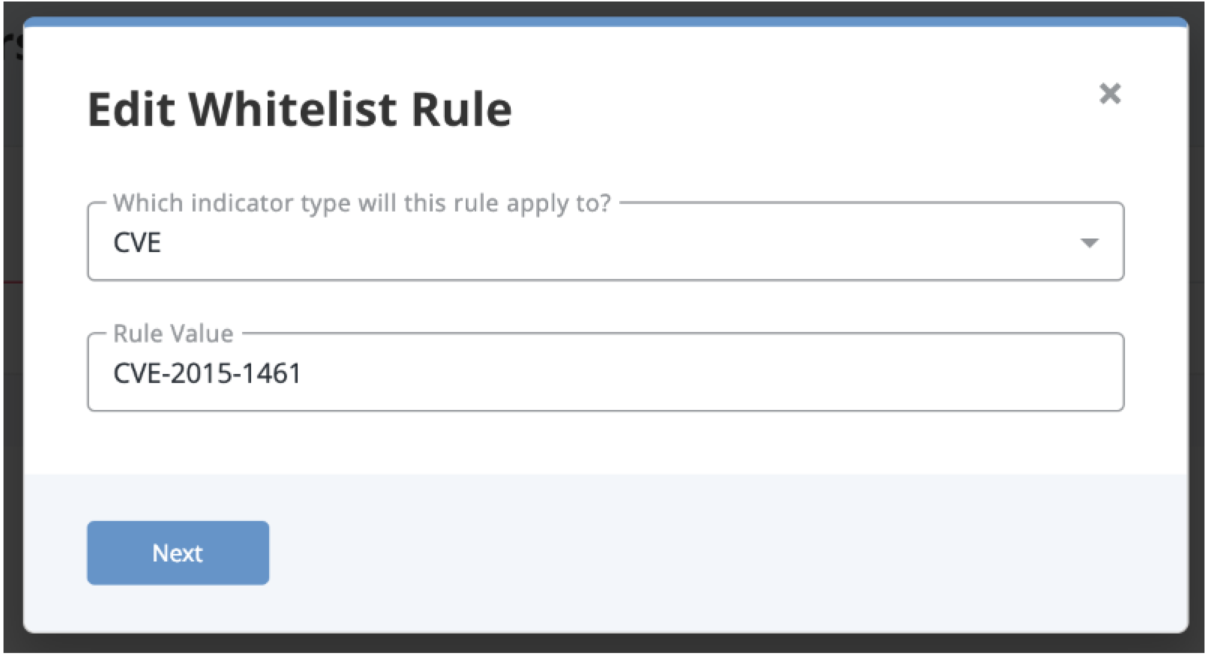
   The rule is applied to existing indicators, and it is entered into the Whitelisted Rules table.

> Any new indicators will also have the rule applied to them as they enter the system.

Editing a Whitelisted Rule

1. In the Whitelisted Rules table, locate the rule you wish to edit.
2. Click **Edit**.

   The Edit Whitelist Rule dialog box opens.



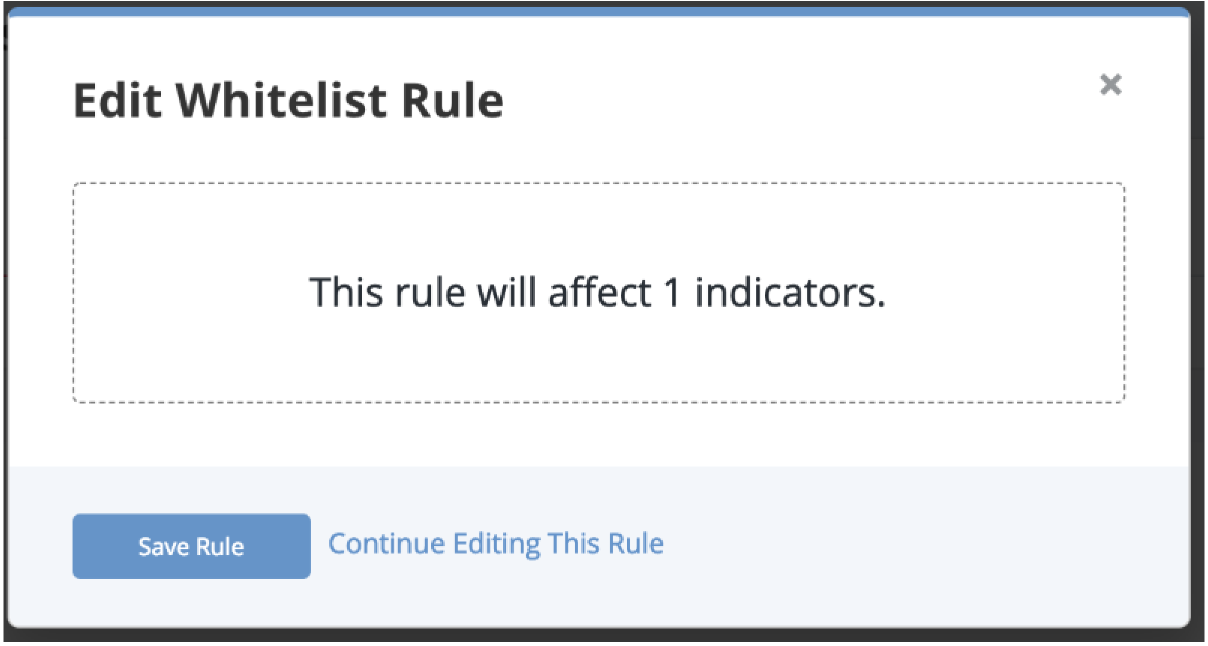
Edit Whitelist Rule

Which indicator type will this rule apply to?: CVE

Rule Value: CVE-2015-1461

3. Make the desired edits and click **Next**.

Affected indicators are listed in the dialog box.



This rule will affect 1 indicators.

4. 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.

5. If you are satisfied, click **Edit Rule**.

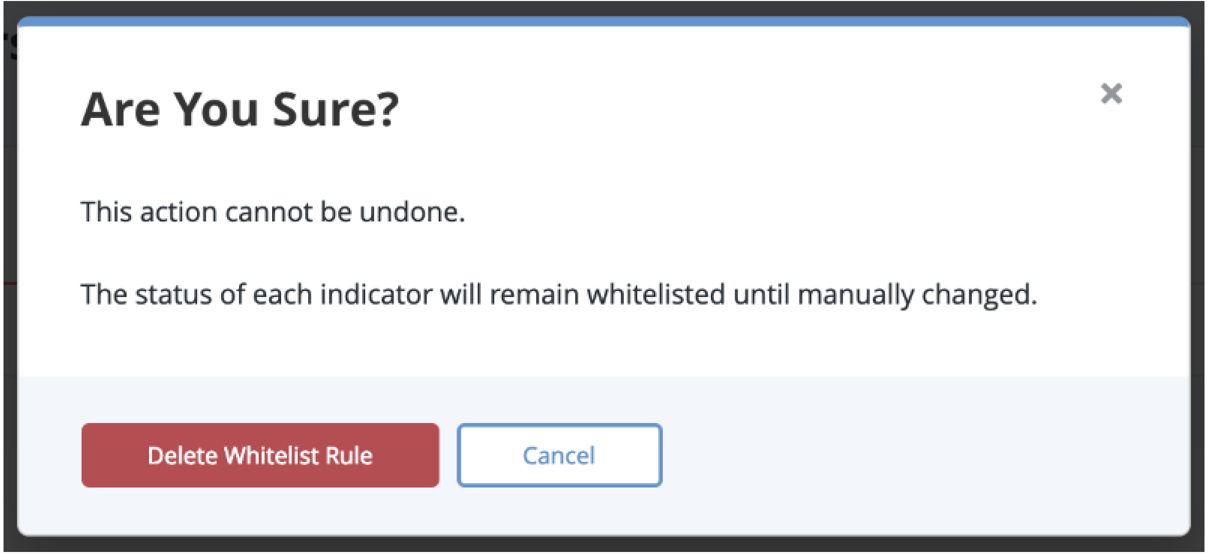
   The rule is applied to existing indicators, and it is updated in the Whitelist Rules table.

> Any new indicators will also have the rule applied to them as they enter the system.

Removing a Whitelisted Rule

1. Locate and select the rule(s) from the Whitelisted Indicators table that you wish to remove.
2. Click on the delete Icon 🟥.

A confirmation dialog box opens, asking if you are sure.



Are You Sure?

This action cannot be undone.

The status of each indicator will remain whitelisted until manually changed.

3. Click **Delete Whitelist Rule**.

   The rule be now be removed.

Exports

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/.

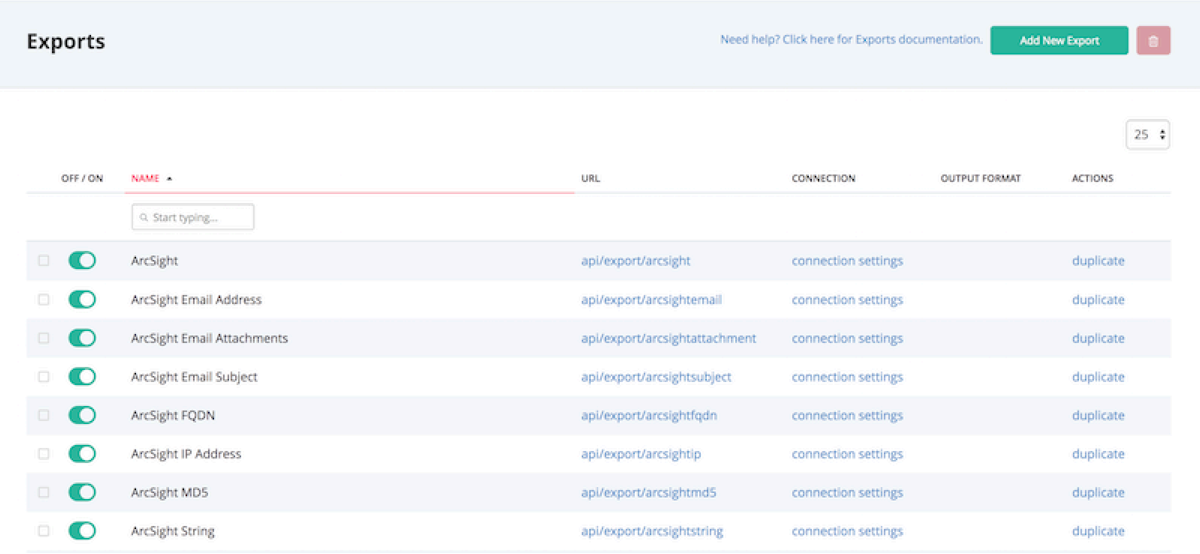
> ⚠ You should NOT attempt to export all of your threat intelligence data with a single export. Attempting to do so will cause system degradation and the export will not complete.

Managing Exports

Accessing the Exports List

1. Select the **Settings** ⚙ **icon** >**Exports**.

   The Exports page appears with a table listing all exports in alphabetical order.



Exports

	OFF / ON	NAME ▲	URL	CONNECTION	OUTPUT FORMAT	ACTIONS
		Start typing...				
☐	●	ArcSight	api/export/arcsight	connection settings		duplicate
☐	●	ArcSight Email Address	api/export/arcsightemail	connection settings		duplicate
☐	●	ArcSight Email Attachments	api/export/arcsightattachment	connection settings		duplicate
☐	●	ArcSight Email Subject	api/export/arcsightsubject	connection settings		duplicate
☐	●	ArcSight FQDN	api/export/arcsightfqdn	connection settings		duplicate
☐	●	ArcSight IP Address	api/export/arcsightip	connection settings		duplicate
☐	●	ArcSight MD5	api/export/arcsightmd5	connection settings		duplicate
☐	●	ArcSight String	api/export/arcsightstring	connection settings		duplicate

Viewing 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.

Enabling/Disabling Exports

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.

Adding an Export

The **Filter by TLP** field options will only appear if administrators have enabled Traffic Light Protocol (TLP) viewing. See the Traffic Light Protocol (TLP) topic for more information.

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 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.
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**.

Duplicating an Export

Duplicating an export allows you to have a version that you can edit.

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.

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.

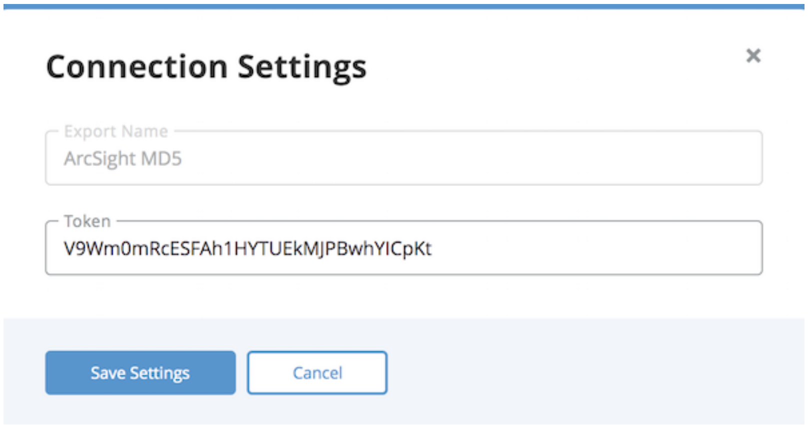
While you cannot edit or delete any of the exports originally supplied by ThreatQ, you can edit exports you have added to ThreatQ or copies of the original exports.

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.



Export Name: ArcSight MD5

Token: V9Wm0mRcESFAh1HYTUEkMJPBwhYICpKt

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.

Editing an Export's Output Format

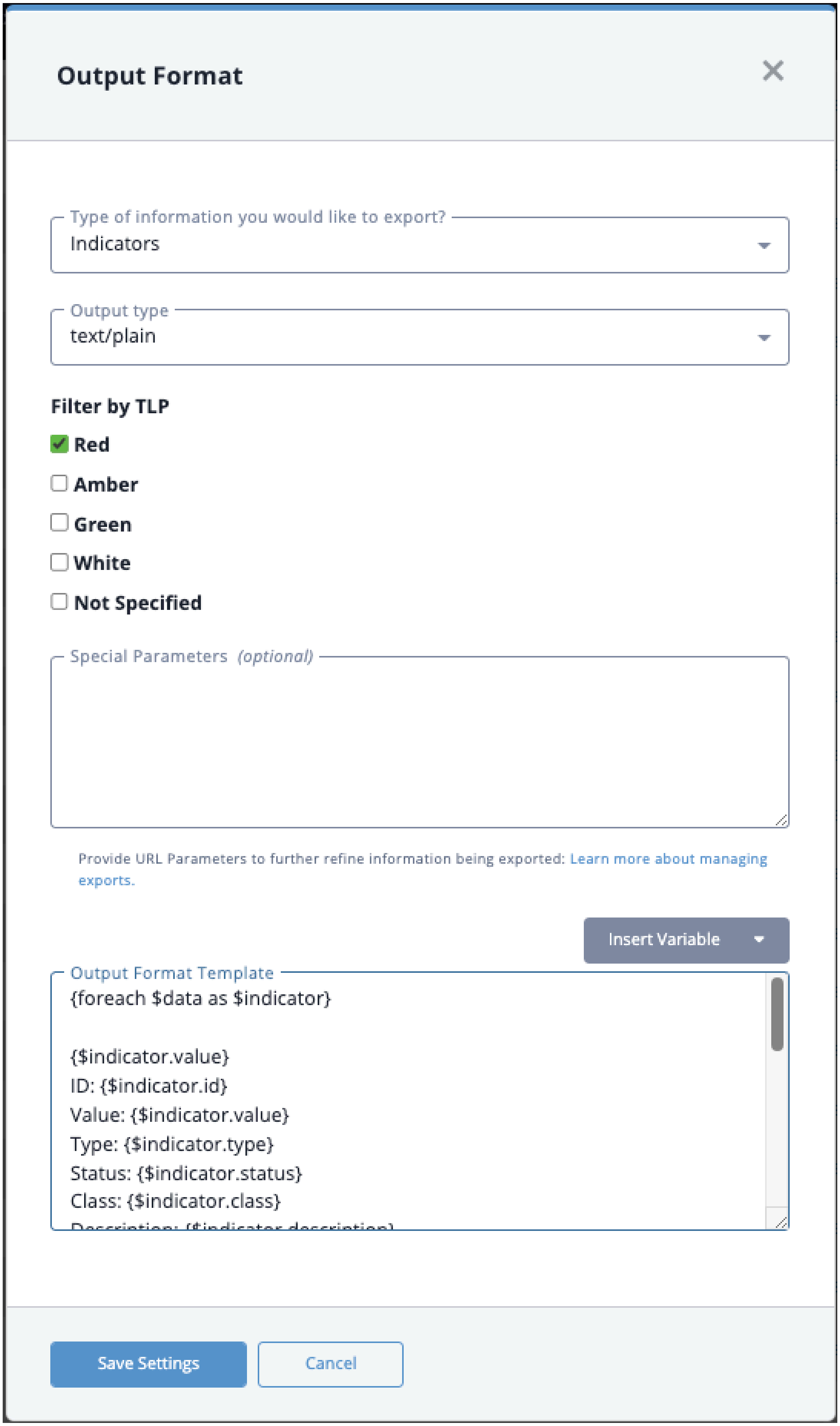
While you cannot edit or delete any of the exports originally supplied by ThreatQ, you can edit exports you have added to ThreatQ or copies of the original exports.

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.



Output Format

Type of information you would like to export?
Indicators

Output type
text/plain

Filter by TLP
☑ Red
☐ Amber
☐ Green
☐ White
☐ Not Specified

Special Parameters (optional)

Provide URL Parameters to further refine information being exported: Learn more about managing exports.

Output Format Template

```
{foreach $data as $indicator}

{$indicator.value}
ID: {$indicator.id}
Value: {$indicator.value}
Type: {$indicator.type}
Status: {$indicator.status}
Class: {$indicator.class}
```

3. Select which type of information you would like to export from the first dropdown menu.

4. An admin has the ability to choose between the following options:

    - Adversaries
    - Attack Patterns
    - Campaigns
    - Courses of Actions
    - Events
    - Exploit Targets
    - Identity
    - Incidents
    - Indicators
    - Intrusion Sets
    - Malware
    - Reports
    - Signatures
    - Tools
    - TTPs
    - Vulnerabilities

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.

        > Details on both methods are detailed in the Output Format Options topic.

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.

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.

Output Format Options

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 clicking the location for the variable, clicking the **Insert Variable** button and selecting the variable from the dropdown list.

   This template provides you with the ability to format exactly how your data is printed out within an export.

   > 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 the **Save Settings** button.

Disabling Export Logging

In some instances, you may need to stop the export log process. ThreatQ provides a CLI configuration command that allows you to disable export logging.

Adding Special Parameters

The Special Parameters field gives admins the option to use additional parameters to further specify the data exported.

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

Filtering Special Parameters

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.sources.dates=Y
indicator.id
indicator.status
indicator.type
indicator.sincedeleted
indicator.whitelisted *
indicator.score
indicator.created_at
indicator.updated_at
indicator.Sources
indicator.Attributes
indicator.Tags
indicator.Assets
```

* 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`

Indicators - Related Objects

The following fields are not available for use in the Special Parameters section but can be used in output templates.

```
indicator.Indicators
indicator.Adversaries
indicator.Events
indicator.Attachments
indicator.Signatures
indicator.Investigations
indicator.Tasks
indicator.Campaign
indicator.Course_of_action
indicator.Exploit_target
indicator.Incident
indicator.Ttp
indicator.Attack_pattern
indicator.Identity
indicator.Intrusion_set
indicator.Malware
indicator.Report
```

```
    indicator.Tool
    indicator.Vulnerability
```

Assets

```
assets.value
assets.description
assets.Sources
assets.Attributes
assets.Indicators
assets.Adversaries
assets.Events
assets.Attachments
assets.Signatures
assets.Investigations
assets.Tasks
assets.Campaign
assets.Course_of_action
assets.Exploit_target
assets.Incident
assets.Ttp
assets.Attack_pattern
assets.Identity
assets.Intrusion_set
assets.Malware
assets.Report
assets.Tool
assets.Vulnerability
assets.Tags
assets.Assets
```

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.sources.dates=Y
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
    adversary.Tags
    adversary.Assets
```

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.sources.dates=Y
    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
    event.Tags
    event.Assets
```

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.sources.dates=Y
    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
signature.Tags
signature.Assets
```

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.sources.dates=Y
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
campaign.Tags
campaign.Assets
```

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.sources.dates=Y
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
course_of_action.Tags
course_of_action.Assets
```

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.sources.dates=Y
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
exploit_target.Tags
exploit_target.Assets
```

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.sources.dates=Y
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
incident.Tags
incident.Assets
```

TTP

```
ttp.value
ttp.status_id
ttp.type_id
ttp.description
ttp.deleted_at
ttp.deleted
ttp.sources_count
ttp.sources.dates=Y
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
ttp.Tags
ttp.Assets
```

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.sources.dates=Y
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
    attack_pattern.Tags
    attack_pattern.Assets
```

Identity

```
    identity.value
    identity.status_id
    identity.type_id
    identity.description
    identity.contact_information
    identity.deleted_at
    identity.deleted
    identity.sources_count
    identity.sources.dates=Y
    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
    identity.Tags
    identity.Assets
```

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.sources.dates=Y
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
intrusion_set.Tags
intrusion_set.Assets
```

Malware

```
malware.value
malware.status_id
malware.type_id
malware.description
```

```
    malware.deleted_at
    malware.deleted
    malware.sources_count
    malware.sources.dates=Y
    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
    malware.Tags
    malware.Assets
```

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.sources.dates=Y
    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
    report.Tags
    report.Assets
```

Tool

```
    tool.value
    tool.status_id
    tool.type_id
    tool.description
    tool.deleted_at
    tool.deleted
    tool.sources_count
    tool.sources.dates=Y
    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
tool.Tags
too.Assets
```

Vulnerability

```
vulnerability.value
vulnerability.status_id
vulnerability.type_id
vulnerability.description
vulnerability.deleted_at
vulnerability.deleted
vulnerability.sources_count
vulnerability.sources.dates=Y
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
    vulnerability.Tags
    vulnerability.Assets
```

> You can add parameters to the .Tags variable to filter exported objects based on the presence of all specified tags (ex: `&<object>.Tags=tag1,tag2,tag3`) or the presence of at least one of the specified tags (ex: `&<object>.Tags=tag1|tag2|tag3`)

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 allows you to include only new data each time the export is run instead of 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.

> **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. However, you 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
      ```

Output Format Templates

The following section contains templates 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 the **Output Format** link for an export from the main Exports page

> ⚠ When formatting your output template, you must wrap all of your declarations within a loop.

Adversaries 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}
```

Events 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}
```

Indicators 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}
```

Signatures 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}
```

Template Variables

The following items are variables that can added to the templates provided above.

Source Variable

```
{foreach $adversary.Sources item=source name=Sources}
{$source.value} {if !empty($source.tlp)}({$source.tlp}){/if}
{/foreach}
```

Attribute Variable

```
{foreach $adversary.Attributes item=attribute name=Attributes}
Name: {$attribute.name}
Value: {$attribute.value}
{/foreach}
```

Adversary Variable

```
{foreach $adversary.Adversaries item=adversary name=Adversaries}
Name: {$adversary.name}
Value: {$adversary.value}
{/foreach}
```

Attachment Variable

```
{foreach $adversary.Attachments item=attachment name=Attachments}
Name: {$attachment.name}
Value: {$attachment.value}
{/foreach}
```

Event Variable

```
{foreach $adversary.Events item=event name=Events}
Name: {$event.name}
Value: {$event.value}
{/foreach}
```

Indicator Variable

```
{foreach $adversary.Indicators item=indicator name=Indicators}
Name: {$indicator.name}
Value: {$indicator.value}
{/foreach}
```

Investigation Variable

```
{foreach $adversary.Investigations item=investigation
name=Investigations}
Name: {$investigation.name}
Value: {$investigation.value}
{/foreach}
```

Signature Variable

```
{foreach $adversary.Signatures item=signature name=Signatures}
Name: {$signature.name}
Value: {$signature.value}
{/foreach}
```

Tag Variable

```
{foreach $adversary.Tags item=Tags name=Tags}
Name: {$tag.name}
Value: {$tag.value}
{/foreach}
```

Task Variable

```
{foreach $adversary.Tasks item=task name=Tasks}
Name: {$task.name}
Value: {$task.value}
{/foreach}
```

Specific Indicator Exports

The following topics provide instructions on how to export specific Indicators for use with an external threat detection system.

See Managing Exports and Output Format Options for more details about configuring exports.

- Cisco TID Exports
- Fidelis Exports
- Fortinet Fortigate Exports
- Lancope Exports
- Netwitness Exports
- OpenIOC Signatures Exports
- Palo Alto Exports
- Reservoir Labs Exports
- Splunk Exports
- Symantec ProxySG Exports
- Tenable Exports
- Zeek Exports

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.

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

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 Output Format Options topic for more information 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=IPAddress&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 would you like to export?	Indicator
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 like to export?	Indicator
Output Type	Text/plain

FIELD	ENTRY
Special Parameters	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 information would you like to export?	Indicator
Output Type	Text/plain
Special Parameters	indicator.status=Active&indicator.deleted=N&indicator.type=IPAddress&indicat class=network

Output Format Template	{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	indicator.status=Active&indicator.type=Email Address&indicator.class=network

Output Format Template	{foreach $data as $indicator}
	{$indicator.value}
	{/foreach}

8. Click on 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>
```

9. Remove the limit section and trailing &amp; 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
```

10. Click **Save Settings**.
11. Under **On/Off**, toggle the switch to enable the export.

Cisco FMC Configuration:

1. Navigate to the Intelligence director on the Firepower Management Center.
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
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.

FIELD	ENTRY
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**.

Fidelis Exports

ThreatQ exports to send indicators of compromise (Email Address, IP Address, MD5, URL and FQDN) to Fidelis Elevate. Elevate has the capability to ingest IOCs from external threat feeds and use them to create rules and policies, and define the reaction by the sensors if such a policy is violated. The exports defined here are in an XML format, although Elevate offers also the option to ingest feed in CSV format.

More details about custom threat feeds and their configuration in Elevate can be found on the help pages of a Fidelis Elevate device: `https://<Fidelis Elevate Host or IP>/help/MyWebHelp/Content/FidelisCreatePoliciesHelpVersion/P_InsightCustomFeed.htm`

Configuring exports in ThreatQ

Review the Managing Exports topic for a detailed description no how to create and manage exports. If you need further assistance, please open a support ticket with ThreatQ Support.

To export Email Addresses:

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:

FIELD	VALUE
Type of information you would like to export?	Indicators
Output type	text/plain

FIELD	VALUE
Special Parameters	`indicator.status=Active&indicator.deleted=N&indicator.type=EmailAddress&indicator.class=network&differential=1`

6. Under **Output Format Template**, enter:

```
<ThreatQEmailAddressFeed>
  <description>Email addresses feed from ThreatQ</description>
  <entries>
  {foreach $data as $indicator}
  <entry>
      <email>{$indicator.value}</email>
      <extra_info>{$indicator.id}</extra_info>
    </entry>
  {if !$indicator.last}{/if}
  {/foreach}
</entries>
</ThreatQEmailAddressFeed>
```

7. Click **Save Setting**s.
8. Under **On/Off**, toggle the switch to enable the export.
9. Click on the export URL with the data.

> Make sure to remove the limit parameter from the URL: `limit=10&`.
> The URL should be similar to this one:
> `https://<ThreatQ Host>/api/export/<export ID>/?token=<Authentication Token>`

To export IP Addresses:

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:

FIELD	VALUE
Type of information you would like to export?	Indicators
Output type	text/plain
Special Parameters	`indicator.status=Active&indicator.deleted=N&indicator.type=IP Address&indicator.class=network&differential=1`

6. Under **Output Format Template**, enter:

```
<ThreatQIPAddressFeed>
  <description>IP address feed from ThreatQ</description>
  <entries>
  {foreach $data as $indicator}
  <entry>
      <ip>{$indicator.value}</ip>
      <extra_info>{$indicator.id}</extra_info>
    </entry>
  {if !$indicator.last}{/if}
  {/foreach}
</entries>
</ThreatQIPAddressFeed>
```

7. Click **Save Settings**.
8. Under **On/Off**, toggle the switch to enable the export
9. Click on the export URL with the data.

> Make sure to remove the limit parameter from the URL: `limit=10&`.
> The URL should be similar to this one:
> `https://<ThreatQ Host>/api/export/<export ID>/?token=<Authentication Token>`

To export MD5 hashes:

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:

FIELD	VALUE
Type of information you would like to export?	Indicators
Output type	text/plain
Special Parameters	`indicator.status=Active&indicator.deleted=N&indicator.type=MD5&indicator.class=network&differential=1`

6. Under **Output Format Template**, enter:

```
<ThreatQMD5Feed>
  <description>MD5 feed from ThreatQ</description>
  <entries>
  {foreach $data as $indicator}
  <entry>
      <md5>{$indicator.value}</md5>
      <extra_info>{$indicator.id}</extra_info>
    </entry>
  {if !$indicator.last}{/if}
  {/foreach}
</entries>
</ThreatQMD5Feed>
```

7. Click **Save Settings**.
8. Under **On/Off**, toggle the switch to enable the export.
9. Click on the export URL with the data. Make sure to delete from the URL this parameter `limit=10&`. The URL should be similar to this one `https://<ThreatQ Host>/api/export/<export ID>/?token=<Authentication Token>`

To export FQDNs and URLs:

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:

FIELD	VALUE
Type of information you would like to export?	Indicators
Output type	text/plain
Special Parameters	`indicator.status=Active&indicator.deleted=N&indicator.type=URL&indicator.type=FQDN&indicator.class=network&differential=1`

6. Under **Output Format Template**, enter:

```
<ThreatQFQDNURLFeed>
  <description>Threat feed from ThreatQ with FQDNs and URLs</description>
  <entries>
  {foreach $data as $indicator}
  <entry>
      <url>{$indicator.value}</url>
      <extra_info>{$indicator.id}</extra_info>
    </entry>
  {if !$indicator.last}{/if}
  {/foreach}
</entries>
</ThreatQFQDNURLFeed>
```

7. Click **Save Settings**.
8. Under **On/Off**, toggle the switch to enable the export.
9. Click on the export URL with the data.

> Make sure to remove the limit parameter from the URL: `limit=10&`.
> The URL should be similar to this one:
> `https://<ThreatQ Host>/api/export/<export ID>/?token=<Authentication Token>`

Adding the exports as custom threat feeds in Fidelis Elevate

For a detailed description of the configuration steps, visit the following page on your Fidelis Elevate CommandPost appliance: https://<Fidelis Elevate Host>/help/MyWebHelp/Content/FidelisCreatePoliciesHelpVersion/P_InsightAddCustomFeed.htm.

To add a new feed:

1. Go to **Policies -> Threat Feeds -> Feed Config** and click on **Add Feed**.
2. Enter the name of the feed.

> The entered name must be unique among all custom feeds on CommandPost.

3. Optional - Add a description that will be displayed in the list of feeds on the Feed Config page.
4. Select **XML** as the feed format.
5. Enter **entry** for the XML format descriptor.
6. Click the **Add** button.
7. Enter a **Description** of the feed on the detailed configuration page.
8. Select the feed content for the indicator type that is being ingested.
9. Make sure the following boxes are checked, at a minimum:
    - Enable
    - Dynamic
    - Verify SSL Certificate
10. Select the **Refresh Frequency** that is needed for the environment.
11. Enter the **ThreatQ export URL** in the *Location (URL)* box.
12. Click the *Save* button to save the configuration. To test the feed click on the *Download Now* button

> Custom feeds can be set up for a one-time manual upload, manual refresh, or automated refresh.

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 the Managing Exports topic.

Use the following information to configure the export:

FIELD	SELECTION
Type of information you would like to export	Indicators
Output Type	text/plain

Special Parameters

There are two options for special parameters:

If the security policy of your organization requires that all IP Addresses and FQDNs are sent to FortiGate, use these filters for the special parameters:

```
indicator.status=Active&indicator.deleted=N&indicator.type=IP Address&indicator.type=FQDN
```

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 Indicator Status topic to create a status called **Send to FortiGate**.
2. Use the following special parameter:

   ```
   indicator.status=Send to FortiGate
   ```

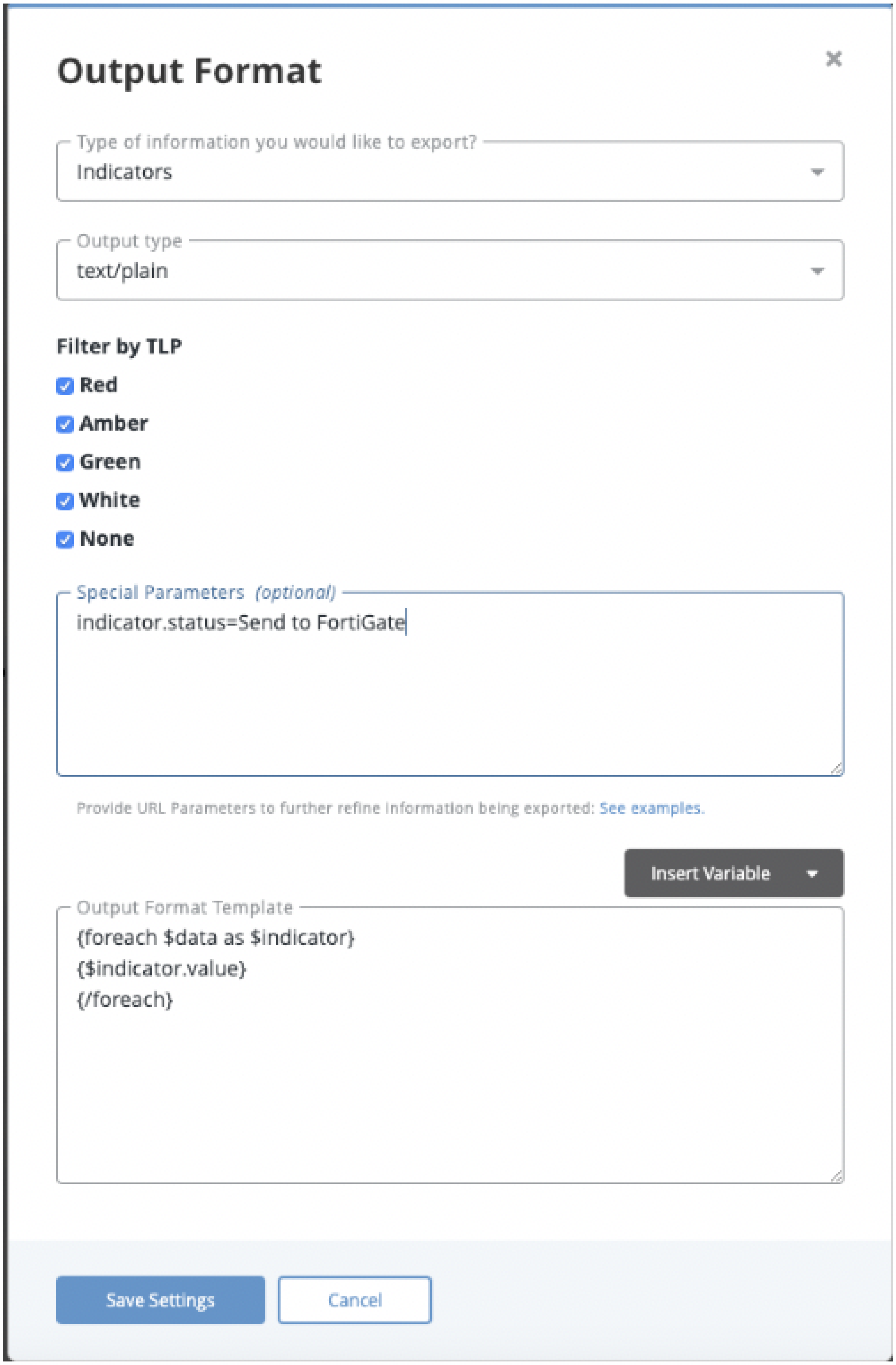
Output Template

```
{foreach $data as $indicator}

{$indicator.value}

{/foreach}
```

Once configured, the export will look similar to the snapshot below.



Output Format

Type of information you would like to export?: Indicators

Output type: text/plain

Filter by TLP

☑ Red
☑ Amber
☑ Green
☑ White
☑ None

Special Parameters (optional): indicator.status=Send to FortiGate

Provide URL Parameters to further refine information being exported: See examples.

Output Format Template:

```
{foreach $data as $indicator}
{$indicator.value}
{/foreach}
```

Configure FortiGate to Download Indicators from ThreatQ

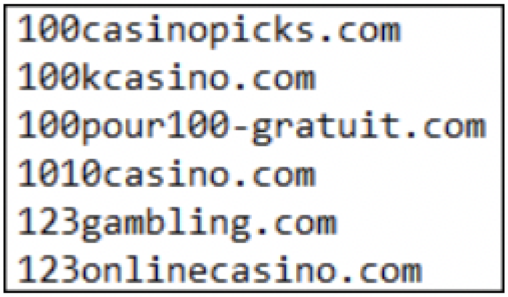
The following detailed steps have been copied from the FortiGate support center and provided here for convenience. The source is https://docs.fortinet.com/document/fortigate/6.0.0/cookbook/85580

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.

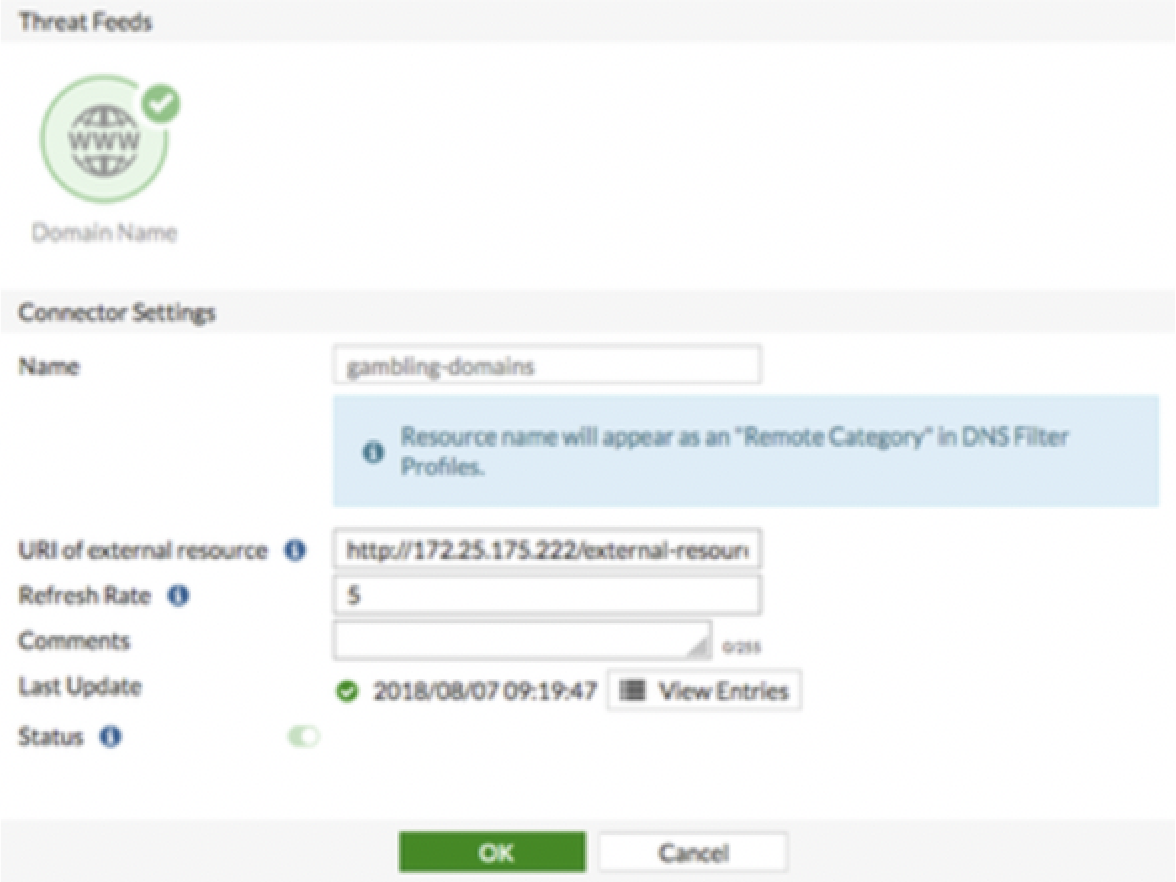
1. Create an external block list. The external block list should be a plain text file with one domain name per line. The use of simple wildcards is supported. You can create your own text file or download it from an external service. Upload the text file to the HTTP file server.



```
100casinopicks.com
100kcasino.com
100pour100-gratuit.com
1010casino.com
123gambling.com
123onlinecasino.com
```

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.



Name: gambling-domains

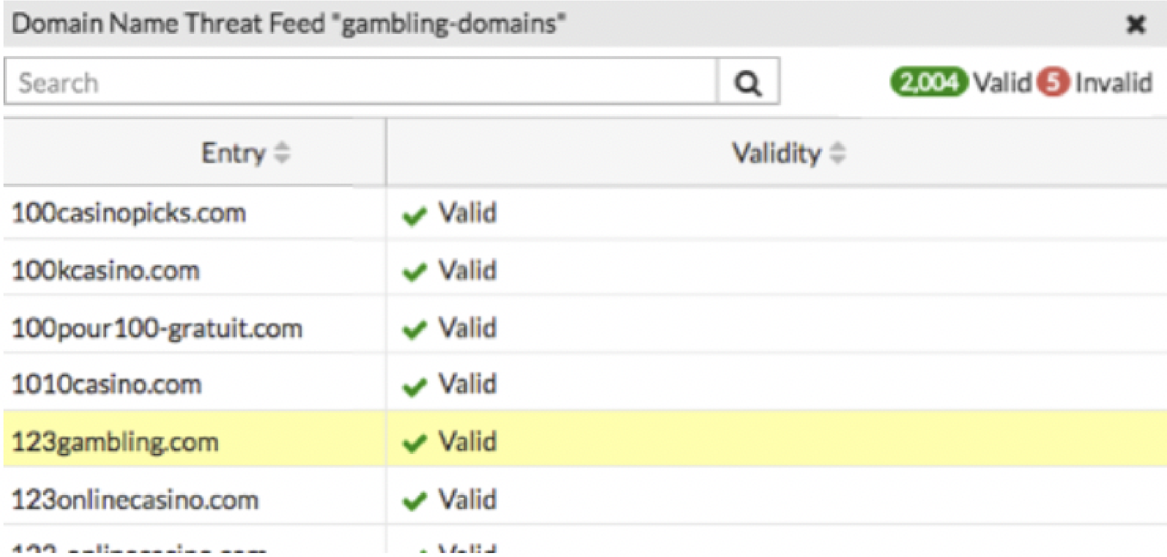
Resource name will appear as an "Remote Category" in DNS Filter Profiles.

URI of external resource: http://172.25.175.222/external-resour

Refresh Rate: 5

Last Update: 2018/08/07 09:19:47

d. Click View Entries to see the text file's domain list.



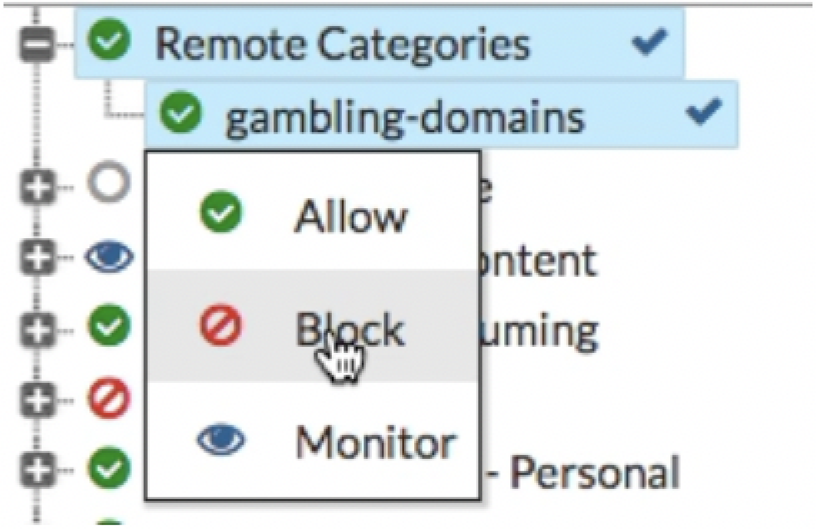
Domain Name Threat Feed "gambling-domains"

Entry	Validity
100casinopicks.com	✓ Valid
100kcasino.com	✓ Valid
100pour100-gratuit.com	✓ Valid
1010casino.com	✓ Valid
123gambling.com	✓ Valid
123onlinecasino.com	✓ Valid

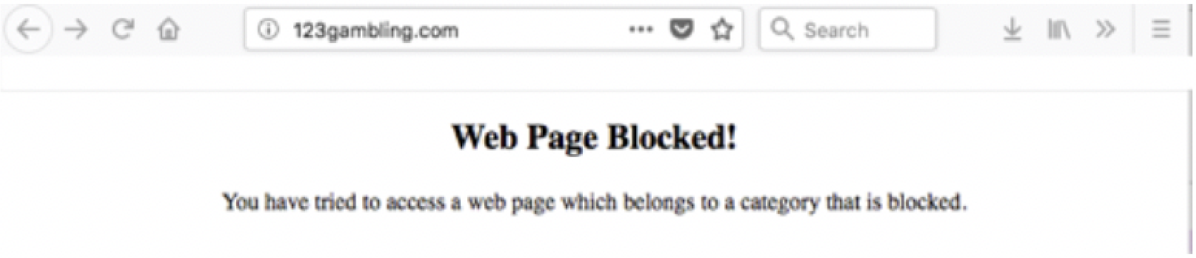
e. Click **OK**.

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.



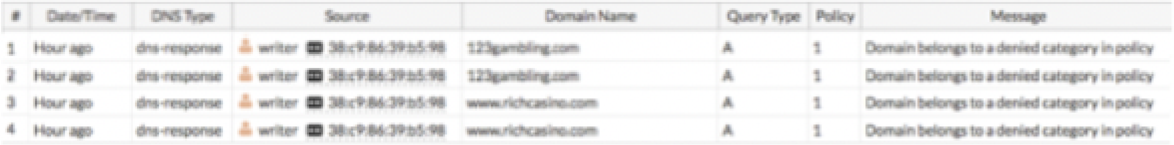
4. Configure the outgoing Internet policy:
   a. Go to **Policy & Objects -> IPv4 Policy**.
   b. Enable the **DNS Filter** under the *Security Profiles*.
   c. From the SSL Inspection dropdown list, select an SSL inspection profile.
5. View the results:
   a. Visit a domain on the external resource file. This example visits 123gambling.com. A Web Page Blocked! message appears.



Web Page Blocked!

You have tried to access a web page which belongs to a category that is blocked.

   b. In FortiOS, go to **Log & Report -> DNS Query**. The logs show that the 123gambling.com domain belongs to a blocked category.



#	Date/Time	DNS Type	Source	Domain Name	Query Type	Policy	Message
1	Hour ago	dns-response	writer 38:c9:86:39:b5:98	123gambling.com	A	1	Domain belongs to a denied category in policy
2	Hour ago	dns-response	writer 38:c9:86:39:b5:98	123gambling.com	A	1	Domain belongs to a denied category in policy
3	Hour ago	dns-response	writer 38:c9:86:39:b5:98	www.richcasino.com	A	1	Domain belongs to a denied category in policy
4	Hour ago	dns-response	writer 38:c9:86:39:b5:98	www.richcasino.com	A	1	Domain belongs to a denied category in policy

Lancope Exports

These Steps explain how to export Lancope indicators for use with an external threat detection system. 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:

FIELD	ENTRY
Which type of information would you like to export?	Indicators
Output Type	text/csv; charset=utf-8
Special Parameters	`indicator.status=Active&indicator.deleted=N&indicator.type=IPAddress&indicator.type=CIDR Block&indicator.class=network`

   Under **Output Format Template**, enter:

```
RECORD_NUMBER,GROUP_NAME,GROUP_ID,NETWORK_DEFINITION,PARENT_NA
MESPACE

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.

Netwitness Exports

This topic explains how to export Netwitness indicators for use with an external threat detection system. 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:

FIELD	ENTRY
Which type of information would you like to export?	Indicators
Output Type	text/csv; charset=utf-8
Special Parameters	`indicator.status=Active&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. Select the **Settings 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:

FIELD	ENTRY
Which type of information would you like to export?	Indicators
Output Type	text/csv; charset=utf-8
Special Parameters	`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.

OpenIOC Signature Exports

This topic explains how to export OpenIOC signatures for use with an external threat detection system. 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:

FIELD	ENTRY
Which type of information would you like to export?	Signatures
Output Type	text/csv
Special Parameters	`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.

Palo Alto Exports

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:

FIELD	ENTRY
Which type of information would you like to export?	Indicators
Output Type	text/plain
Special Parameters	`indicator.status=Active&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.

Palo Alto: PANOS and Panorama Exports

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.

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

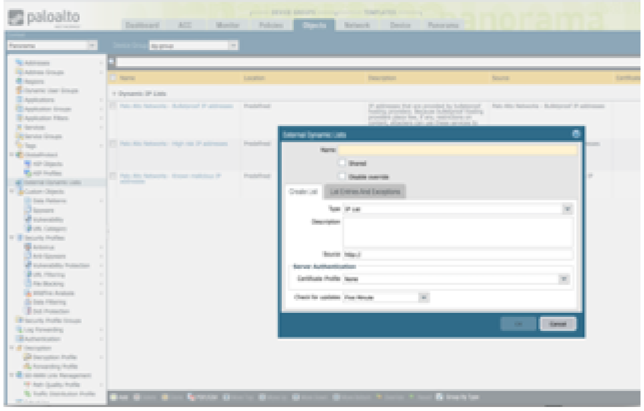
To add the dynamic list to Palo Alto, follow the instructions from here.

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

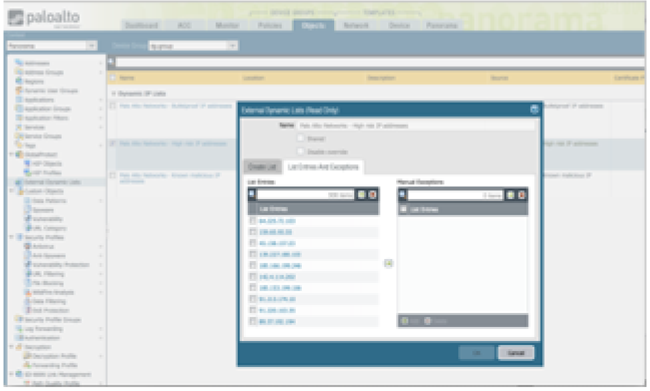
Configure an External Dynamic List (EDL) in Panorama

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

Reservoir Labs Exports

This topic explains how to export Reservoir Labs indicators for use with an external threat detection system. 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:

FIELD	ENTRY
Which type of information would you like to export?	Indicators
Output Type	text/plain
Special Parameters	`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.

Securonix Exports

Securonix IOC exports enable the dissemination of prioritized IOCs from ThreatQ to Securonix, to be used for log enrichment and policy alerts.

ThreatQ Configuration

Review the Managing Exports topic for a detailed description on how to create and manage exports. If you need further assistance, please open a support ticket with ThreatQ Support.

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 and click on **Next Step**.

   The Output Format dialog box appears.

4. Enter the following information:

FIELD	VALUE
Type of information you would like to export?	Indicators
Output type	custom
Special Parameters	`indicator.type=IP Address&indicator.score>=3&indicator.deleted=N&indicator.status=Active` You will need to configure different exports per IOC type you'd want to export to Securonix. This means, changing the

FIELD	VALUE
	indicator.type special parameter above to match the corresponding IOC type.

5. Under **Output Format Template**, enter:

```
# tpi_ioc,tpi_risk,tpi_src_organization,tpi_description,tpi_malware,tpi_dt_firstseen
{foreach $data as $indicator} {$indicator.value|json_encode},"{if $indicator.score
lte 3}Low{elseif $indicator.score lte 6}Medium{elseif $indicator.score lte 9}
High{elseif $indicator.score gt 9}Very High{/if}","ThreatQ",{if
$indicator.description}{$indicator.description|json_encode}{else}""{/if},{if !
empty($indicator.Malware)}{$indicator.Malware[0].value}{else}""{/if},
{$indicator.created_at|json_encode} {/foreach}
```

6. Click **Save Settings**.
7. Under On/Off, toggle the switch to enable the export
8. Click on the export URL with the data.

Example Output

tpi_ioc,tpi_risk,tpi_src_organization,tpi_description,tpi_malware,tpi_dt_firstseen

````
"13.84.134.105","Very High","ThreatQ","","","2021-04-20 21:14:26"
"13.92.233.22","Very High","ThreatQ","","","2021-04-20 21:14:26"
"52.171.135.15","Very High","ThreatQ","","","2021-04-20 21:14:28"
"3.134.125.175","Very High","ThreatQ","",njRAT,"2021-05-04 15:14:29"
"3.14.182.203","Very High","ThreatQ","",njRAT,"2021-05-04 15:14:29"
"67.209.195.198","Very High","ThreatQ","",QakBot,"2021-05-04 15:14:51"
"47.146.32.175","Very High","ThreatQ","",Emotet,"2021-05-05 15:14:41"
"79.134.225.7","Very High","ThreatQ","",AsyncRAT,"2021-05-06 15:14:28"
"3.22.15.135","Very High","ThreatQ","",njRAT,"2021-05-06 15:14:47"
"3.131.147.49","Very High","ThreatQ","",njRAT,"2021-05-06 15:14:47" ```
````

Configuring Imports into Securonix

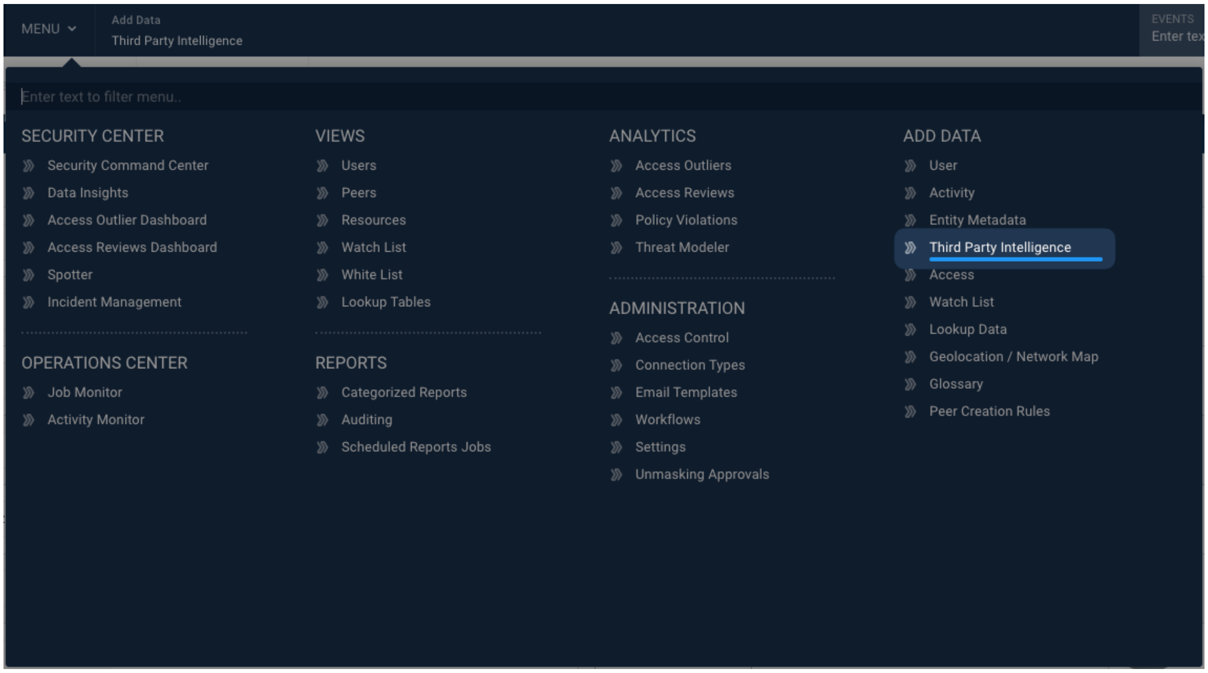
The following section contains ThreatQ-specific instructions. You can view Securonix's guides on importing Third-Party Intelligence can be found at the links below.

- Import Third-Party Intelligence | SNYPR 6.3.1 | Cloud
- Attributes by Field Group

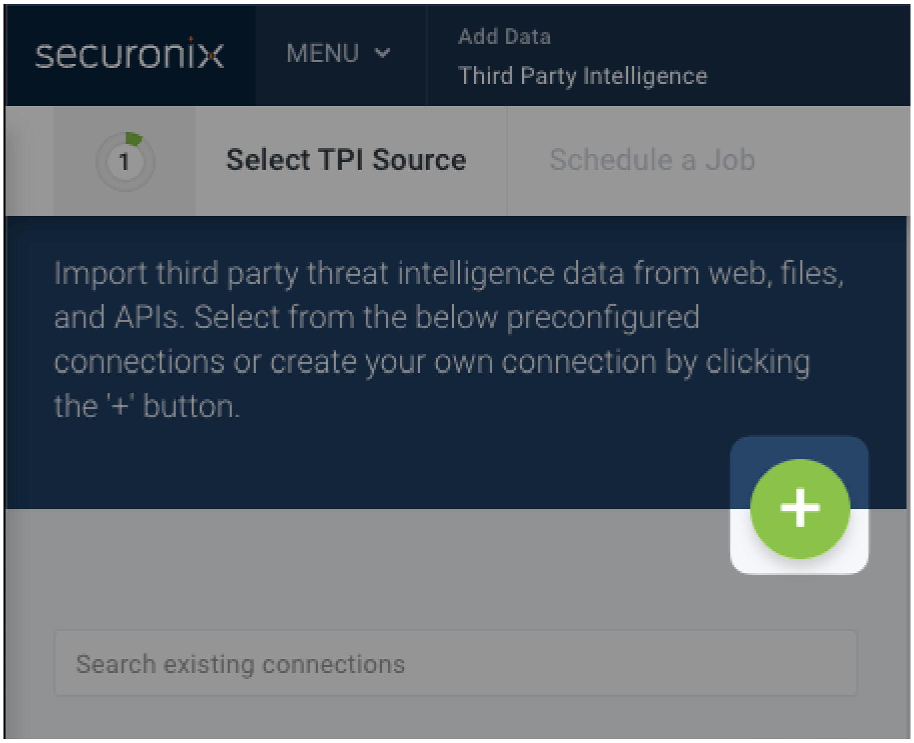
Configuring a new TPI Source (Third-Party Intelligence)

1. Log into Securonix SNYPR.

2. Click on the **MENU** and navigate to **ADD DATA -> Third Party Intelligence**.



3. Click on the **+** button to create a new TPI Source.



Import third party threat intelligence data from web, files, and APIs. Select from the below preconfigured connections or create your own connection by clicking the '+' button.

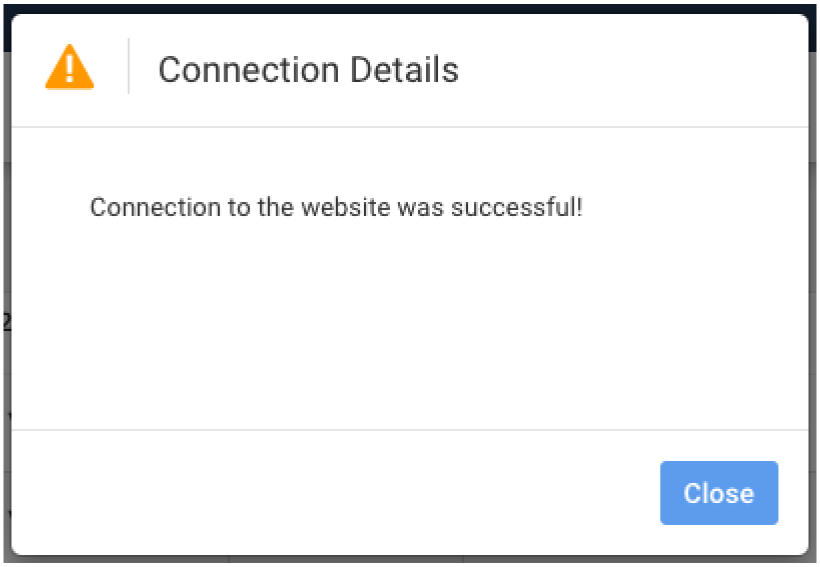
4. Enter the following values for the connection:

VALUE	DESCRIPTION
Connection Name	This can be any name you choose but you should be able to identify the export you are disseminating from ThreatQ. **Example**: ThreatQ_IP_Blacklist The name cannot contain any spaces.
Connection Method	Web
URL	Copy and paste the ThreatQ Export URL. Make sure to remove the limit parameter (i.e. limit=10) from the URL.
Filename	The filename can be any name you choose but you should be able to identify the export you are disseminating from ThreatQ. **Example**: threatq_ip_blacklist.csv This may be overwritten by Securonix after saving.
TPI Type	Update this field to type of IoC you are exporting from ThreatQ.
Parser Type	Delimited
Column Delimiter	,
Contains Column Identifier	No

VALUE	DESCRIPTION
Delete Old TPI Data	Yes
Exclude Header	Yes
Header Lines	1
Exclude Footer	No
Criticality	Select the Critiality to use.
Modify Criticality	Select either Yes or No.

5. Once the configuration has been completed, click the **Test Connection** button in Securonix.

   Example of Successful Connection:

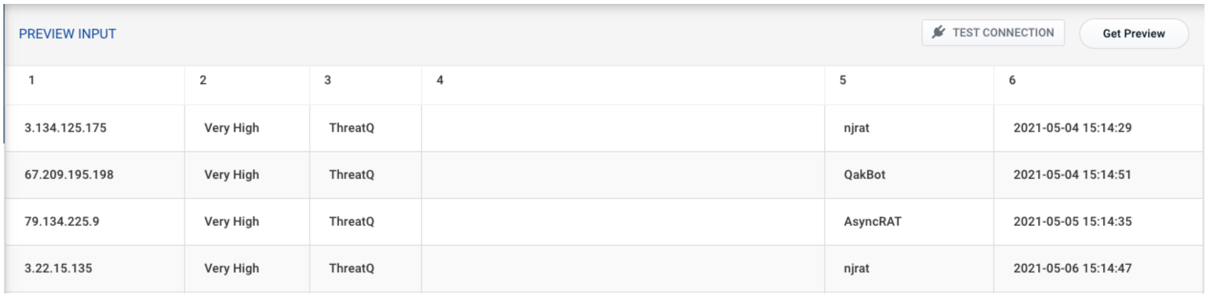


Connection Details

Connection to the website was successful!

6. Once the connection is successful, click on the **Get Preview** button to view a preview of the Export.

Preview Example:



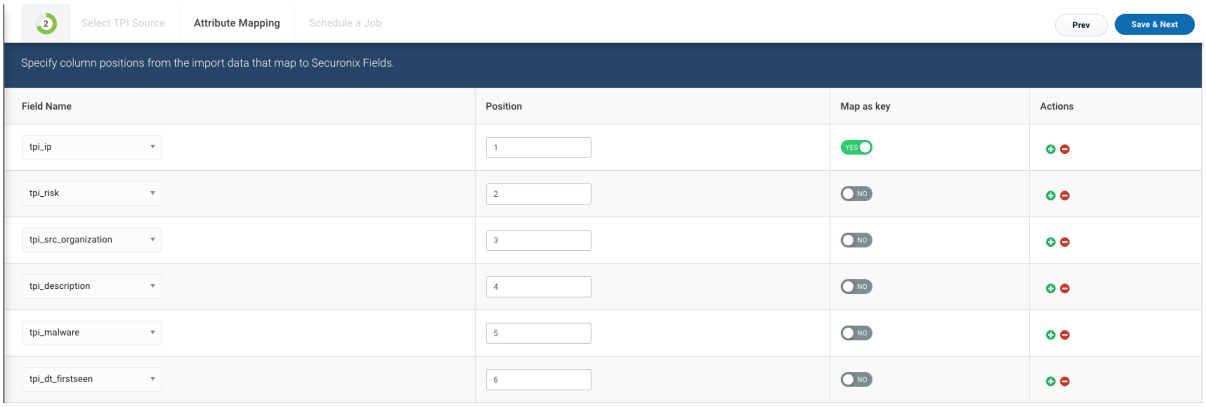
1	2	3	4	5	6
3.134.125.175	Very High	ThreatQ		njrat	2021-05-04 15:14:29
67.209.195.198	Very High	ThreatQ		QakBot	2021-05-04 15:14:51
79.134.225.9	Very High	ThreatQ		AsyncRAT	2021-05-05 15:14:35
3.22.15.135	Very High	ThreatQ		njrat	2021-05-06 15:14:47

> If the connection was unsuccessful, please make sure that there is a proper route for Securonix (cloud) to communicate with ThreatQ (on-prem or cloud-hosted).

7. Click on **Save & Next** if you are satisfied with preview.

Attribute Mapping

The Attribute Mapping page takes the column indexes and maps them to specific fields that Securonix understands. In the example below, the **tpi_ip** field has been selected to **Map as Key**.



Specify column positions from the import data that map to Securonix Fields.

Field Name	Position	Map as key	Actions
tpi_ip	1	YES	⊕ ⊖
tpi_risk	2	NO	⊕ ⊖
tpi_src_organization	3	NO	⊕ ⊖
tpi_description	4	NO	⊕ ⊖
tpi_malware	5	NO	⊕ ⊖
tpi_dt_firstseen	6	NO	⊕ ⊖

There are other IoCs that can be selected, instead of the tpi_ip in the example above, depending on the type of IoCs that you are exporting. Some examples of these types include (but are not limited to):

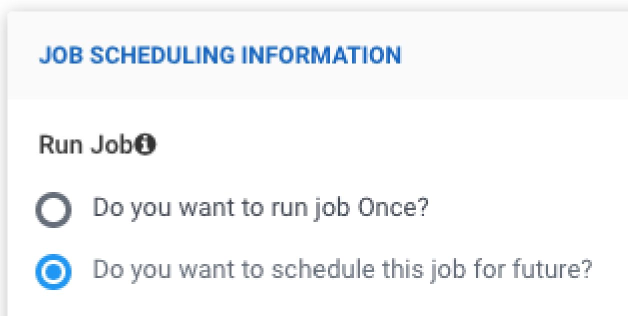
- tpi_hash
- tpi_domain
- tpi_url
- tpi_vulnerability

- tpi_risk
- tpi_src_organization
- tpi_description
- tpi_malware
- tpi_dt_firstseen

Scheduling a Job

To schedule futures jobs:

1. Navigate to the Job Scheduling Information section.
2. Select the radio box for the **Do you want to schedule this for for future** option.



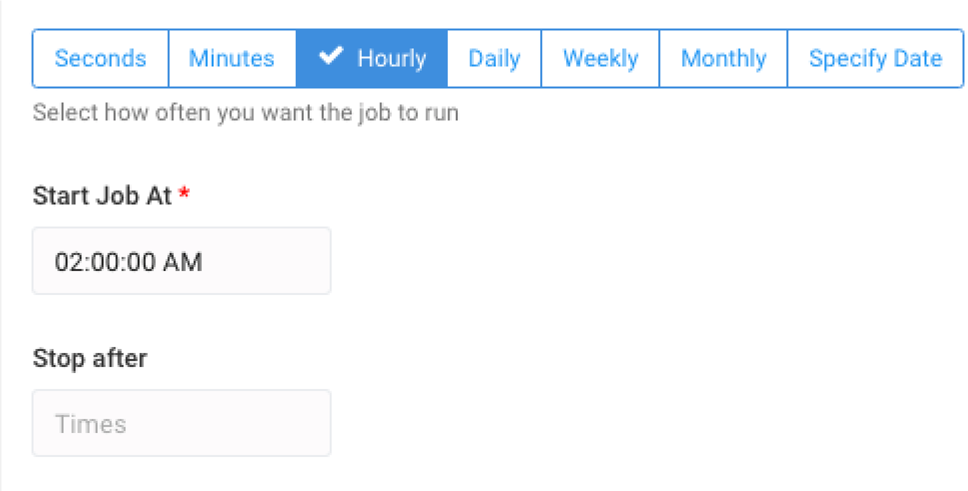
JOB SCHEDULING INFORMATION

Run Job

○ Do you want to run job Once?

● Do you want to schedule this job for future?

3. Use the UI provided to select how often to run the job.



Select how often you want the job to run

Start Job At *: 02:00:00 AM

Stop after: Times

> ThreatQuotient recommends running the job hourly.

4. Click on **Save**.

Splunk Exports

This topic explains how to export indicators for use with an external threat detection system. 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.

5. Provide the following information:

FIELD	ENTRY
Which type of information would you like to export?	Indicators
Output Type	text/plain
Special Parameters	`indicator.sinceddeleted=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}
```

6. Click **Save Settings**.
7. Under **On/Off**, toggle the switch to enable the export.

Symantec ProxySG Exports

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 -

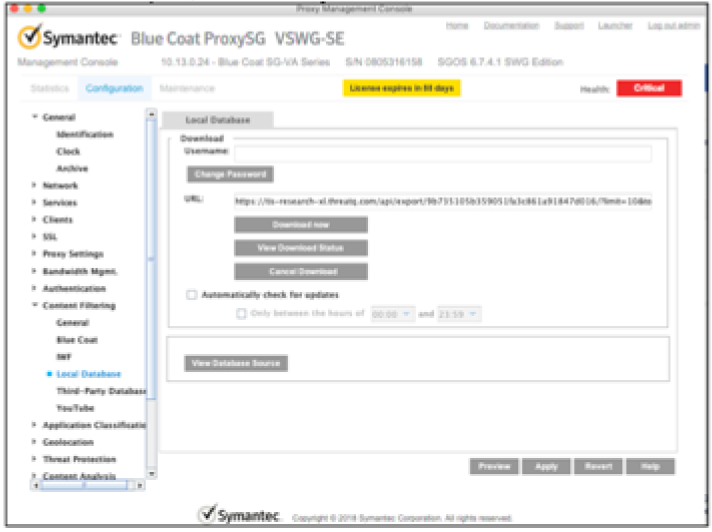
- via the Management Console
- via the Proxy's CLI

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&token=<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
```

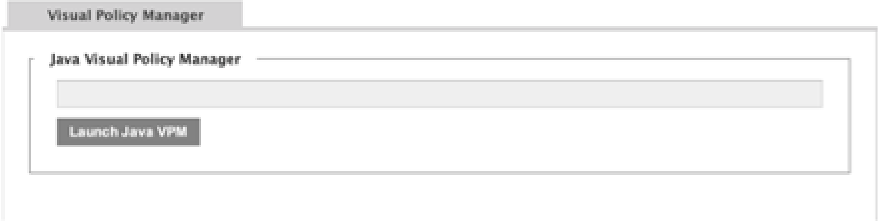
13. If you want to configure auto downloads there are various options available. To list all the download options use the following command

```
< > download ?
```

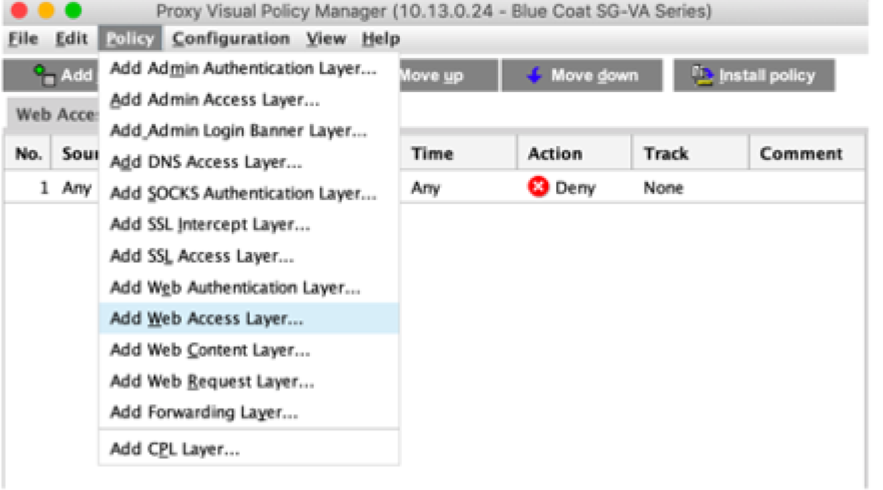
Create and Install a Content Filtering Policy

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.

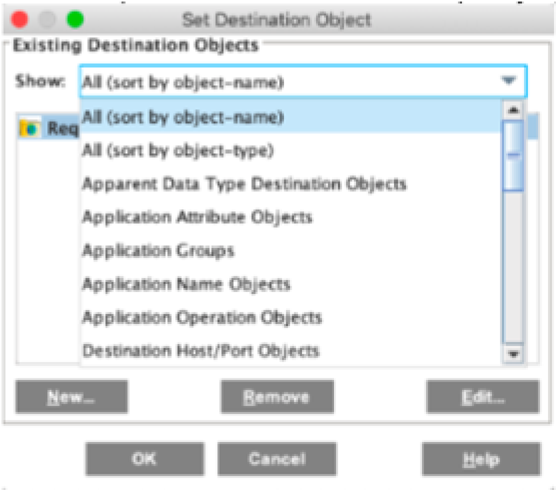
1. Open ProxySG (the example here uses the virtual proxy appliance).
2. Navigate to **Configuration Policy > Visual Policy Manager** and click on **Launch Java VPM**.



3. From within the VPM, create a new **Web Access Layer** by navigating to **Policy Add > Web Access Layer**.


Proxy Visual Policy Manager (10.13.0.24 - Blue Coat SG-VA Series)
File Edit Policy Configuration View Help
Add
Move up
Move down
Install policy
Web Acce
No.
Sour
Time
Action
Track
Comment
1
Any
Any
Deny
None
Add Admin Authentication Layer...
Add Admin Access Layer...
Add Admin Login Banner Layer...
Add DNS Access Layer...
Add SOCKS Authentication Layer...
Add SSL Intercept Layer...
Add SSL Access Layer...
Add Web Authentication Layer...
Add Web Access Layer...
Add Web Content Layer...
Add Web Request Layer...
Add Forwarding Layer...
Add CPL Layer...

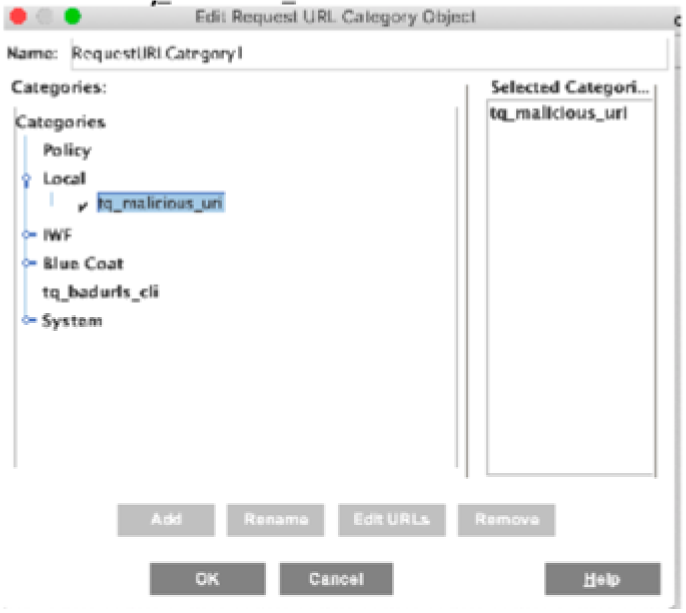
4. Assign a name for the new layer, and after it's created right click on the **Destination object** and select **Set**.
5. Under the drop down in the modal window select **All (sort by object name)** and then click on **Edit** in the lower right corner.


Set Destination Object
Existing Destination Objects
Req
All (sort by object-name)
All (sort by object-type)
Apparent Data Type Destination Objects
Application Attribute Objects
Application Groups
Application Name Objects
Application Operation Objects
Destination Host/Port Objects
New...
Remove
Edit...
OK
Cancel
Help

Show: All (sort by object-name)

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**.

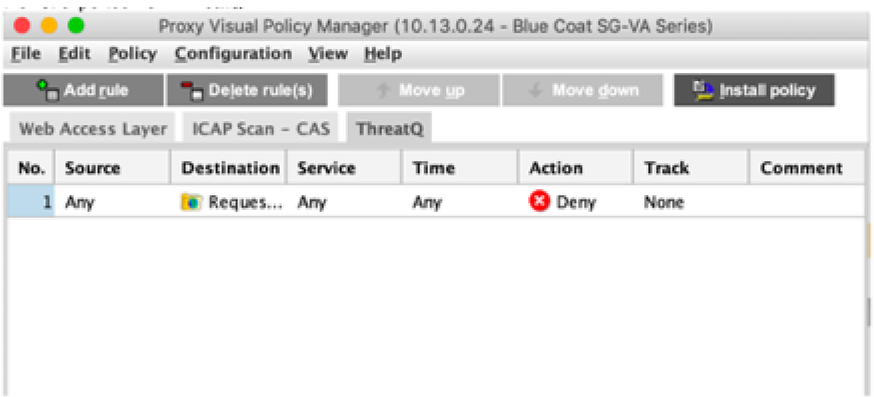


Name: RequestURLCategory1

Selected Categories: 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.



No.	Source	Destination	Service	Time	Action	Track	Comment
1	Any	Reques...	Any	Any	Deny	None	

9. The new policy is now installed and any active indicators exported from ThreatQ will be blocked by the ProxySG.

Tenable Exports

This topic explains how to export Tenable indicators for use with an external threat detection system. 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:

     indicator.status=Active&indicator.deleted=N&indicator.type=FQDN&indicator.class=networ

   - 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. Select the **Settings 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:

FIELD	ENTRY
Which type of information would you like to export?	Indicators
Output Type	text/plain
Special Parameters	`indicator.status=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=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.

Zeek Exports

> Bro is now known as Zeek.

These steps explain how to export Zeek indicators for use with an external threat detection system. Follow the instructions below to export your data.

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:

FIELD	VALUE
Which type of information would you like to export?	Indicators
Output Type	text/plain
Special Parameters	`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.

Integrations Management

The ThreatQ platform allows you install, manage and remove integrations from the My Integrations page.

Topics in this section include:

TOPIC	DESCRIPTION
Integration Types	Learn about the different types of integration available for the ThreatQ platform.
About My Integrations	Learn about managing your installed integrations from the My Integrations page.
Adding an Integration	Learn how to add a new integration to your ThreatQ instance.
Adding A STIX/TAXII Feed	Learn how to add a new STIX/TAXII feed to your ThreatQ instance.
Configuring an Integration	Learn to configure and enable your installed integrations.
Triggering a Manual Run	Learn how to trigger a manual run for your installed CDF integrations.
Running an Operation	Learn how to run an operation against a ThreatQ system object.
Activity Logs (feeds)	Learn about your CDF runs by viewing the Activity Log.
Removing an Integration	Learn how to disable or remove unwanted integrations from your ThreatQ instance.

Integration Types

ThreatQ integrations include Actions, Apps, Configuration-Driven Feeds (CDFs), Custom Connectors, and Operations. This topic will highlight specific information about each type of integration.

Actions

ThreatQ Actions are YAML snippets, utilized by ThreatQ TDR, that you can use to build custom worflows to enrich the data in a specified data collection. See the ThreatQ TDR Orchestrator (TQO) section for more information.

Apps

ThreatQ Apps are designed to operate outside of the ThreatQ platform. The app communicates with third-party applications, such as QRadar and Splunk, and executes user-defined actions. This can result in information being push to and from the third-party application and your ThreatQ instance. Threat intelligence information from these actions can then be ingested back into ThreatQ.

Configuration-Driven Feeds (CDFs)

ThreatQ Configuration-Driven Feeds, CDFs, utilize one or more threat intelligence endpoints for a provider. You can configure what type of information and how you will ingest it into the ThreatQ platform. CDFs fall under one of two categories on the ThreatQ My Integrations page:

- **Commercial** - Commercial CDFs are provided by paid feed providers as a service. To enable these integrations in ThreatQ, you will need an API ID or API Key from the provider. Commercial CDFs typically provide highly contextual threat intelligence data. You can learn more about available CDFs on the ThreatQ Marketplace.
- **OSINT** - OSINT CDFs 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.

Custom Connectors

ThreatQ Custom Connectors are driven by ThreatQuotient’s Threat Intelligence Services Team and provides a solution for data ingestion that is not provided by existing CDFs available on the ThreatQ Marketplace.

Custom Connectors are typically installed via the command line interface and usually require a CRON job to be created to manage connector runs.

Once installed, Custom Connectors are located under the **Labs** category dropdown on the My Integrations page.

Operations

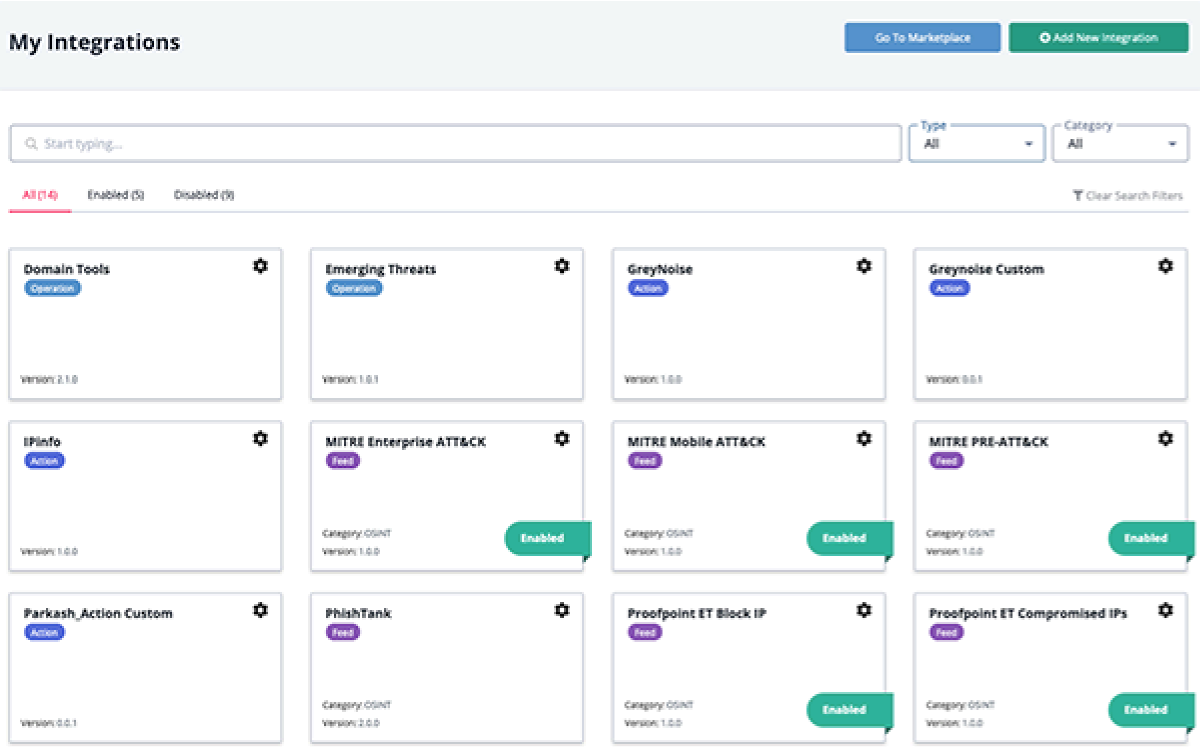
ThreatQ Operations enhance your threat intelligence data by allowing you to add attributes, as well as related indicators, from third party security services, both commercial and open source. You accomplish this by creating objects to connect to a desired service, receive threat intelligence, and display that threat intelligence in ThreatQ.

Installed operation will appear under the **Operations** option for the **Type** dropdown in the My Integration filters. You can execute operations from a threat object's details page - see the Running an Operation topic for more details.

About My Integrations

> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integrated-related credentials.

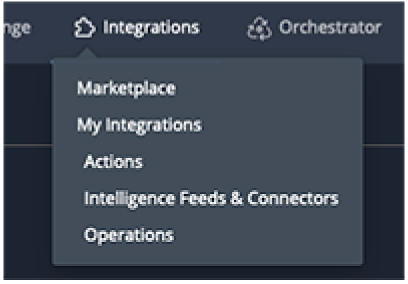
The My Integrations page allows you to add, remove, and configure feeds, actions, custom connectors, and operations that you have downloaded from the ThreatQ Marketplace or are seeded in ThreatQ.



Accessing My Integrations

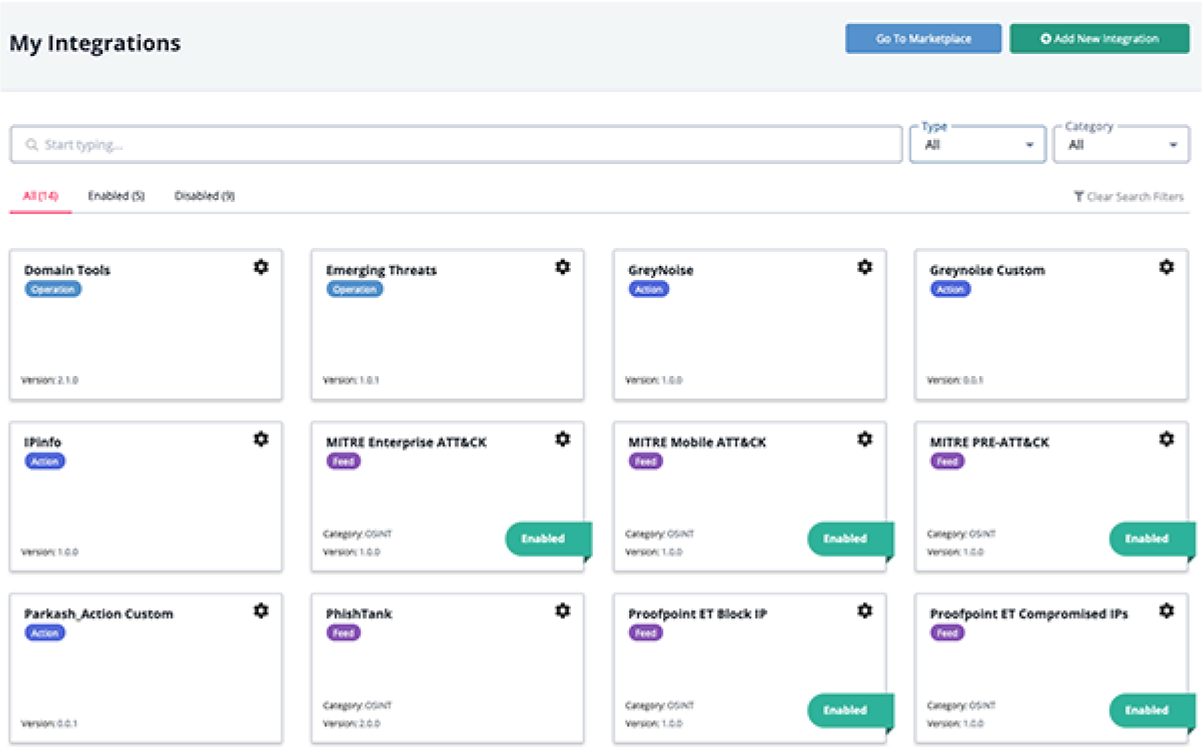
1. Navigate to your ThreatQ instance.

2. Click the **Integrations** option in the main navigation and select one of the following options:



MENU OPTION	DETAILS
Marketplace	Opens the ThreatQ Marketplace in a new tab.
My Integrations	Opens the My Integrations page.
Actions	Opens the My Integrations page filtered to only display actions.
Intelligence Feeds & Connectors	Opens the My Integrations page filtered to only display feeds and connectors.
Operations	Opens the My Integrations page filtered to only display operations.

The My Integrations page loads and defaults to the **All** tab which lists all integrations currently installed on your platform, both enabled and disabled.



Filtering Your View

There are several filters available that allow you to narrow down your integrations. The platform will remember your filter selections for the duration of your session. These filters include:

FILTER	DETAILS
Keyword	Filter the integrations list by keyword.
Type	Filter the integrations list by integration type. Options include: • Actions • Intelligence Feeds and Connectors • Operations • All

Category	Filter the list by the category of integration: • **OSINT** - 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. • **Commercial** - 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. • **STIX TAXII** - 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. • **Labs** - 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.
Status (All/ Enabled/ Disabled tabs)	Filter the list of installed integrations by status: enabled or disabled. A count of integrations appears next to each tab and reflects any filter that is selected. The **All** tab, which displays both enabled and disabled integrations, is selected by default.
Clear Search Filters	Clears the current search filters that are currently in use.

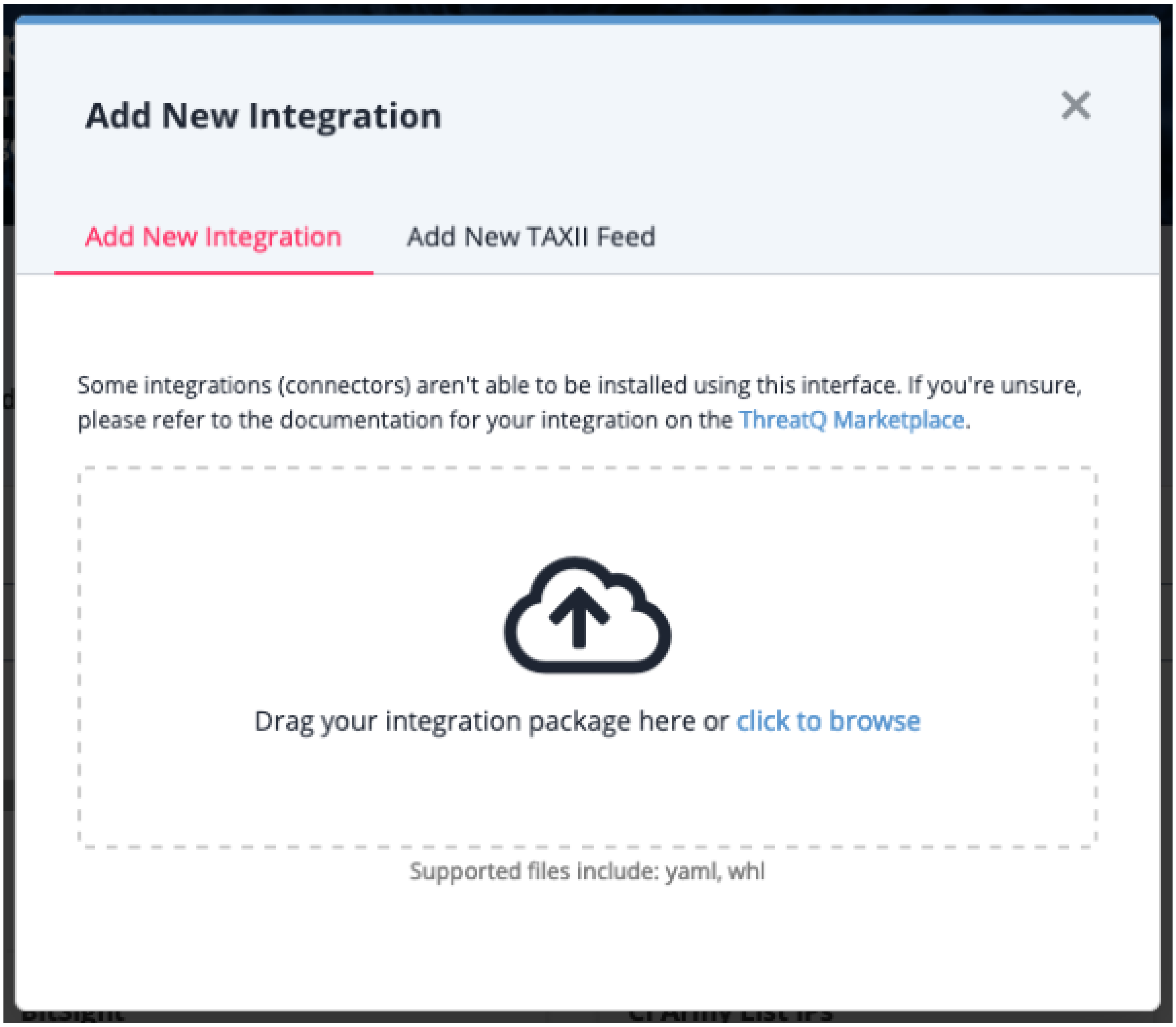
Adding an Integration

> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integrated-related credentials.

The steps for upgrading an integration are the same as for adding an integration. You can use the steps below to install CDFs, Actions, and Operations. See the ThreatQ Orchestrator guide for steps on creating/adding CDWs. See the individual user guide for installation steps on custom connectors and apps.

1. Log into https://marketplace.threatq.com.
2. Locate and download the desired integration file.
3. Navigate to My Integrations page on your ThreatQ instance.
4. Click the **Add New Integration** button.

   The Add New Integration dialog box opens with the **Add New Integration** option selected by default.



Add New Integration
Add New Integration
Add New TAXII Feed

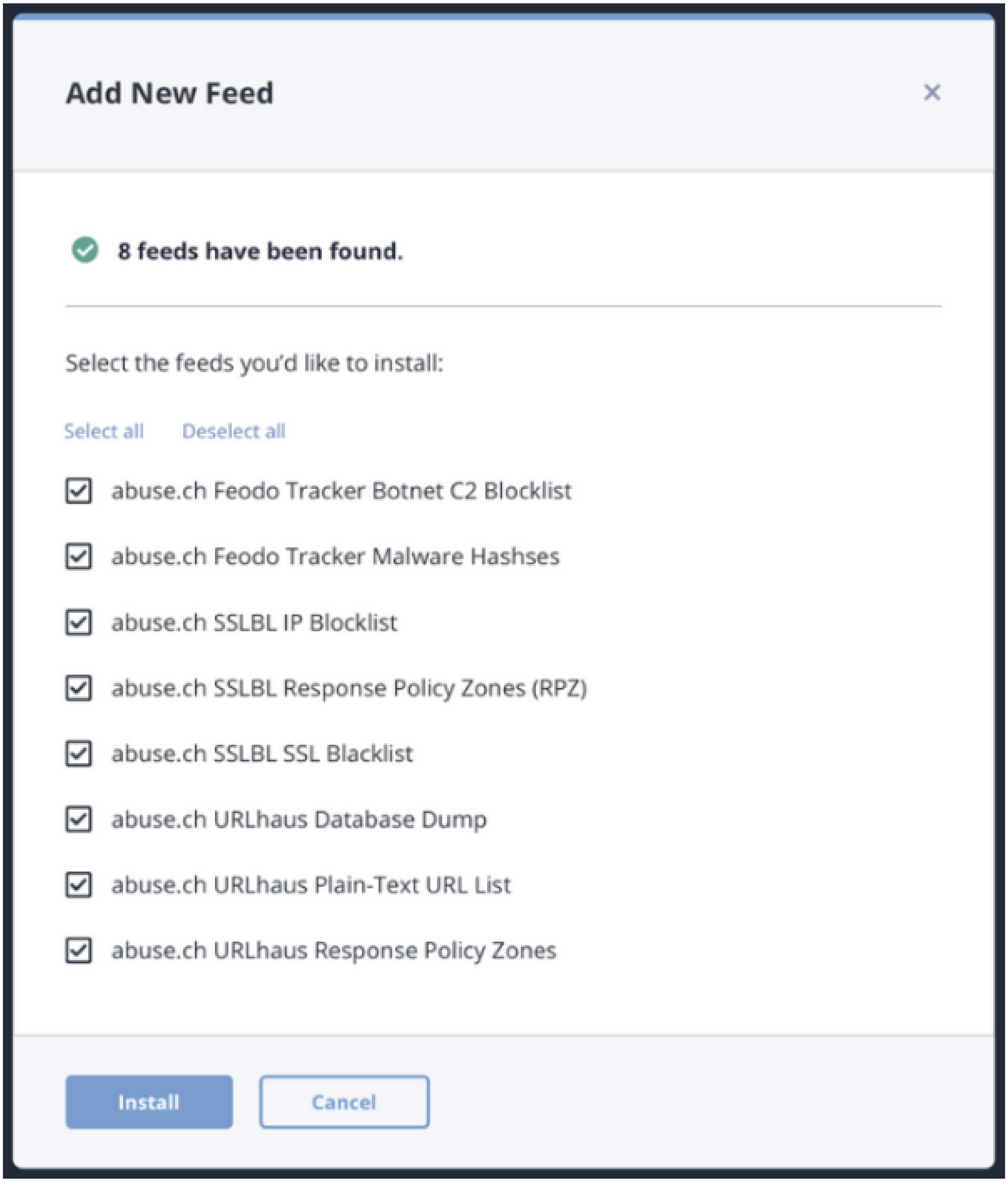
Some integrations (connectors) aren't able to be installed using this interface. If you're unsure, please refer to the documentation for your integration on the ThreatQ Marketplace.

Drag your integration package here or click to browse
Supported files include: yaml, whl

5. Upload the integration file using one of the following methods:
    - Drag and drop the integration file into the dialog box
    - Select the **click to browse** link to locate the integration file on your local machine

> If the integration already exists on the platform, ThreatQ informs you and requires user confirmation before proceeding. If the new version of the integration contains changes to the user configuration and requires user confirmation before overwriting the existing configuration.

6. If the integration file contains multiple feeds, you are prompted to select which feeds to install. Select the feeds to include and click **Install**.



Add New Feed

8 feeds have been found.

Select the feeds you'd like to install:

☑ abuse.ch Feodo Tracker Botnet C2 Blocklist
☑ abuse.ch Feodo Tracker Malware Hashses
☑ abuse.ch SSLBL IP Blocklist
☑ abuse.ch SSLBL Response Policy Zones (RPZ)
☑ abuse.ch SSLBL SSL Blacklist
☑ abuse.ch URLhaus Database Dump
☑ abuse.ch URLhaus Plain-Text URL List
☑ abuse.ch URLhaus Response Policy Zones

7. When the install is complete, you must configure and enable the integration before it can be used.

> Actions will automatically be enabled upon install/upgrade.

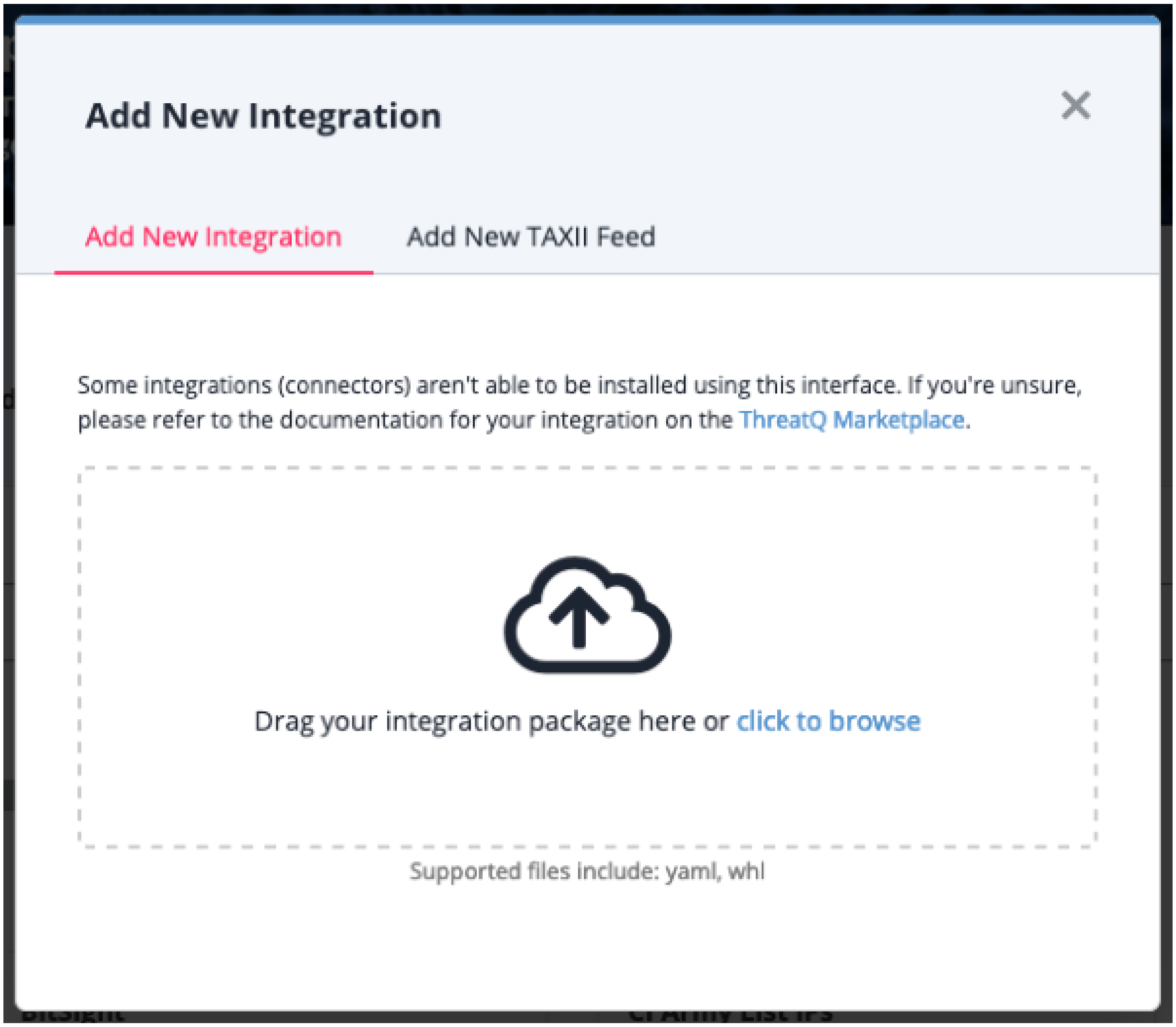
Adding a STIX/TAXII Feed

> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integrated-related credentials.

From the My Integrations page:

1. Click the **Add New Integration** button.

   The Add New Integration dialog box opens with the **Add New Integration** option select by default.



Add New Integration

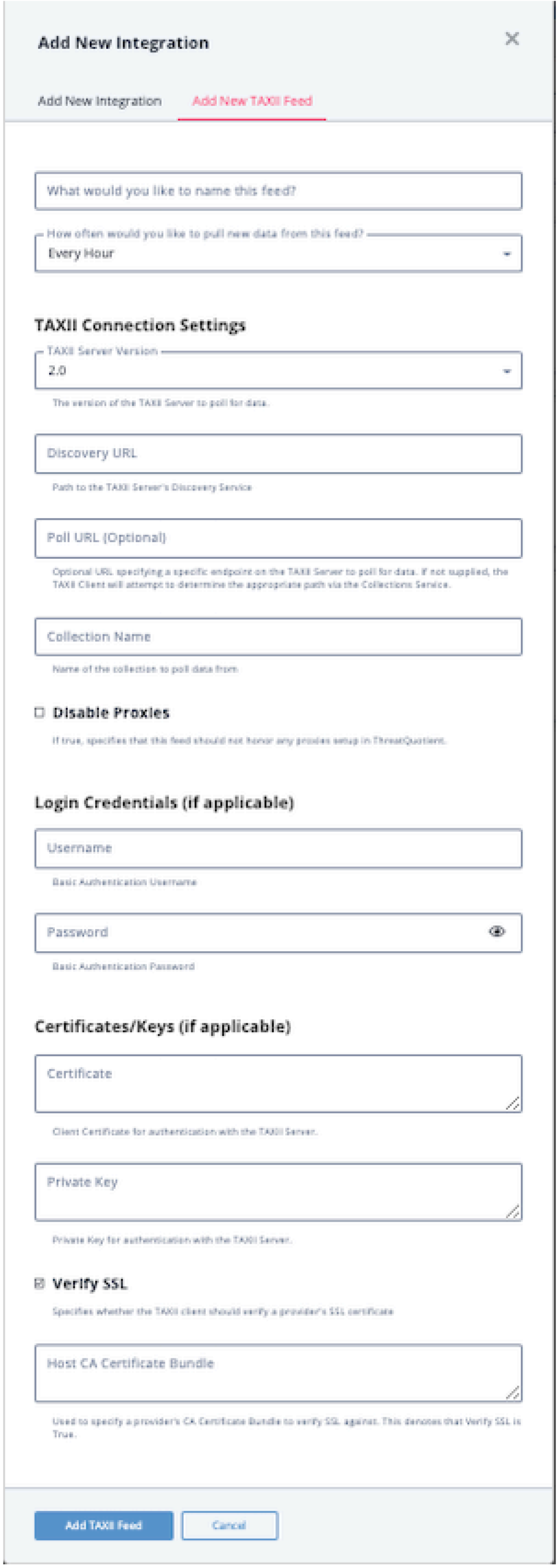
Some integrations (connectors) aren't able to be installed using this interface. If you're unsure, please refer to the documentation for your integration on the ThreatQ Marketplace.

Drag your integration package here or click to browse

Supported files include: yaml, whl

2. Click the **Add New TAXII Feed** option.

The Add New TAXII Feed form is displayed.



Add New Integration

×

Add New Integration | Add New 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

Basic Authentication Username

Password

Basic Authentication Password

Certificates/Keys (if applicable)

Certificate

Client Certificate for authentication with the TAXII Server.

Private Key

Private Key for authentication with the TAXII Server.

☑ **Verify SSL**

Specifies whether the TAXII client should verify a provider's SSL certificate

Host CA Certificate Bundle

Used to specify a provider's CA Certificate Bundle to verify SSL against. This denotes that Verify SSL is True.

Add TAXII Feed | Cancel

3. Complete the following fields:

FIELD	INSTRUCTIONS
What would you like to name this feed?	Enter the feed name to be displayed throughout ThreatQ. The name must be at least five 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, 1.1, 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.
Login Credentials	
Username	If required, enter a username for the feed.
Password	If required, enter a password.
Certificates/Keys	
Certificate	If required, enter a certificate if required for the feed.

FIELD	INSTRUCTIONS
Private Key	If required, 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.

4. Click **Add TAXII** Feed.

   The TAXII/STIX feed is added to the Integrations page. You must configure and enable the integration before it can be used.

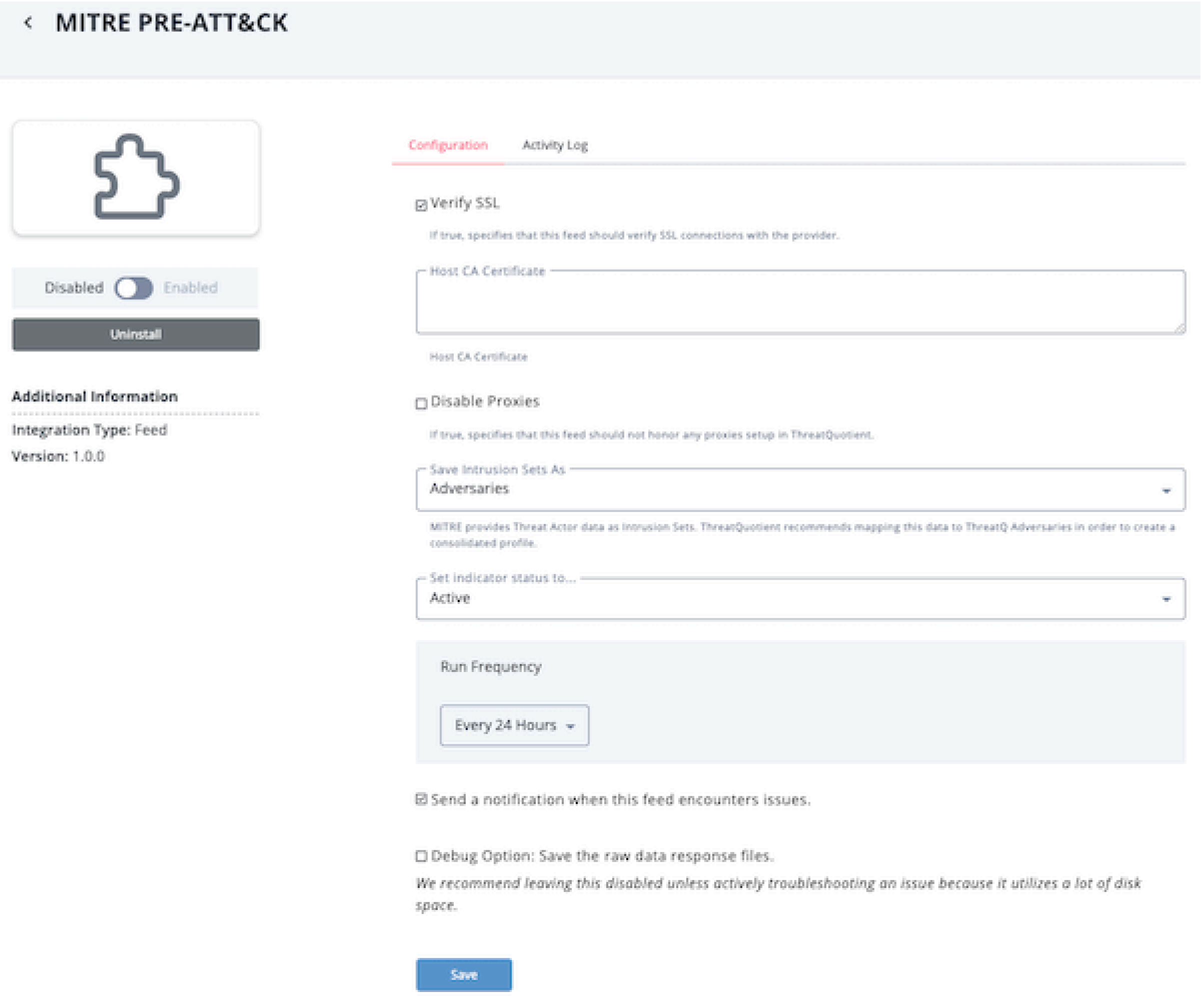
Configuring an Integration

The integration must already be installed in order to access its configuration. See the Adding an Integration topic for more details.

> Configuration parameters will differ based on individual integrations. See the individual integration's user guide for configuration and other requirements. Additionally, certain configuration options in the ThreatQ UI will be available for certain types of integrations. **Example:** The Run Frequency option will only be accessible for CDFs.

From the My Integrations page:

1. Locate and click the integration to load its details page.



Additional Information
Integration Type: Feed
Version: 1.0.0

☑ Verify SSL
If true, specifies that this feed should verify SSL connections with the provider.

Host CA Certificate
Host CA Certificate

☐ Disable Proxies
If true, specifies that this feed should not honor any proxies setup in ThreatQuotient.

Save Intrusion Sets As: Adversaries
MITRE provides Threat Actor data as Intrusion Sets. ThreatQuotient recommends mapping this data to ThreatQ Adversaries in order to create a consolidated profile.

Set indicator status to...: Active

Run Frequency: Every 24 Hours

☑ Send a notification when this feed encounters issues.

☐ Debug Option: Save the raw data response files.
We recommend leaving this disabled unless actively troubleshooting an issue because it utilizes a lot of disk space.

The integration details page displays and lists the following:

  - **Integration Information** - details such as the author, required ThreatQ version and targeted object types.
  - **Configuration Tab** - Integration-specific configuration parameters for the integration.
  - **Activity Log tab** - Display run information such as time stamps, data ingested, and any error messages. The Activity Log on this page only applies to CDFs.

2. Enter the required configuration parameters for your integration in the Configuration Tab. These configuration parameters will differ based on the integration. See the individual integration's user guide for more information.

   Any configurations set on this form for an Action will be applied by default when adding a new instance of the action to an orchestration workflow. If you edited an action's configuration fields in a specific workflow's view, those settings will honored instead for that specific workflow.

3. Select a **Run Frequency** for the integration (CDFs only).

   Periodic Options

SELECTION	DESCRIPTION
Hourly	Run the integration every hour.
Every 6 Hours	Run the integration every six hours.
Every 24 Hours	Run the integration every day.
Every 2 Days	Run the integration every two days.
Every 14 Days	Run the integration every two weeks.
Every 30 Days	Run the integration every month.

   Schedule Options

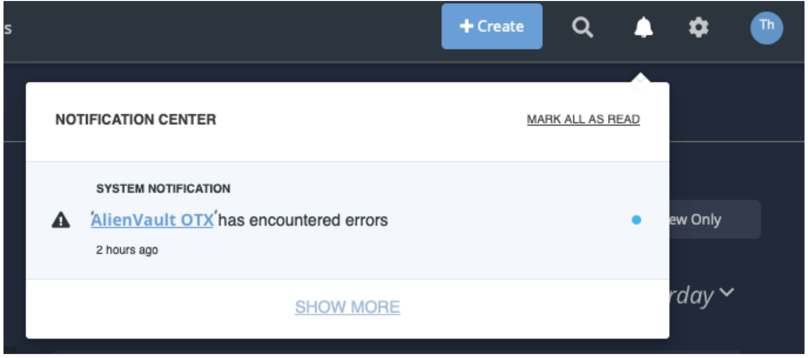
SELECTION	DESCRIPTION
Daily	Allows you to run the integration at a specific time every day.
Weekly	Allows you to run the integration at a specific time, on a specific day, every week.

4. Select a default **Status** if the integration ingests indicator or signature types.

> This configuration option will only be available if the integration ingests indicator or signature types.

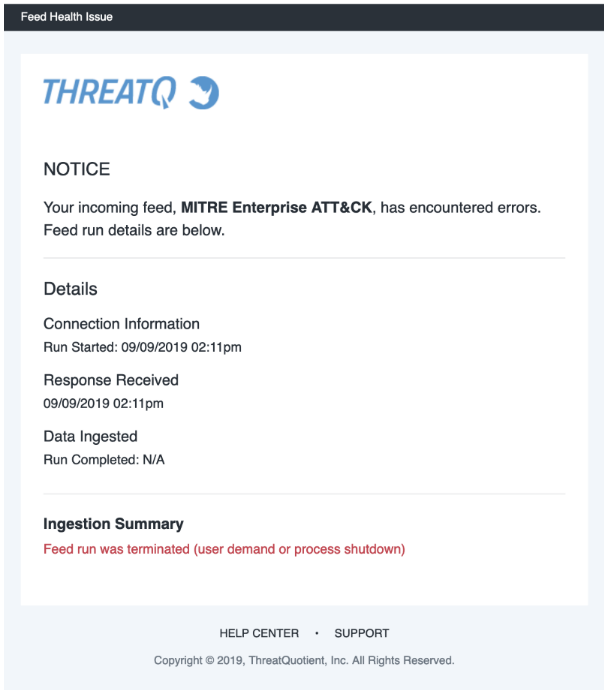
5. Enable or disable **Feed Health Notifications** (CDFs only) for the integration. Feed Health Notifications allow the ThreatQ application to send you, and other designated users, email and in-app notifications when a feed encounters an issue.

   The in-app notifications appear in Notification Center for users with an administrator or maintenance account. These notifications include a link that redirects you to the Activity Log tab on the configuration page for the integration.

   SYSTEM NOTIFICATION
   'AlienVault OTX' has encountered errors
   2 hours ago

   The emails contain useful information such as connection information, data ingested, and an ingestion summary.



Feed Health Issue

THREATQ

NOTICE

Your incoming feed, **MITRE Enterprise ATT&CK**, has encountered errors. Feed run details are below.

Details

Connection Information
Run Started: 09/09/2019 02:11pm

Response Received
09/09/2019 02:11pm

Data Ingested
Run Completed: N/A

Ingestion Summary
Feed run was terminated (user demand or process shutdown)

HELP CENTER • SUPPORT

Copyright © 2019, ThreatQuotient, Inc. All Rights Reserved.

> See the Notifications topic for more information.

6. Enable or disable the **Debug option** (for CDFs only) - The Debug Option checkbox gives you the option to save raw data response files for troubleshooting purposes. Since this option uses a large amount of disk space, it defaults to unchecked. We recommend temporarily enabling the option when you are troubleshooting a feed issue.
7. Click **Save**.
8. Click the **Enable/Disable** toggle switch to enable the integration.

> If the integration is a CDF, a run will be start automatically after the integration is enabled.

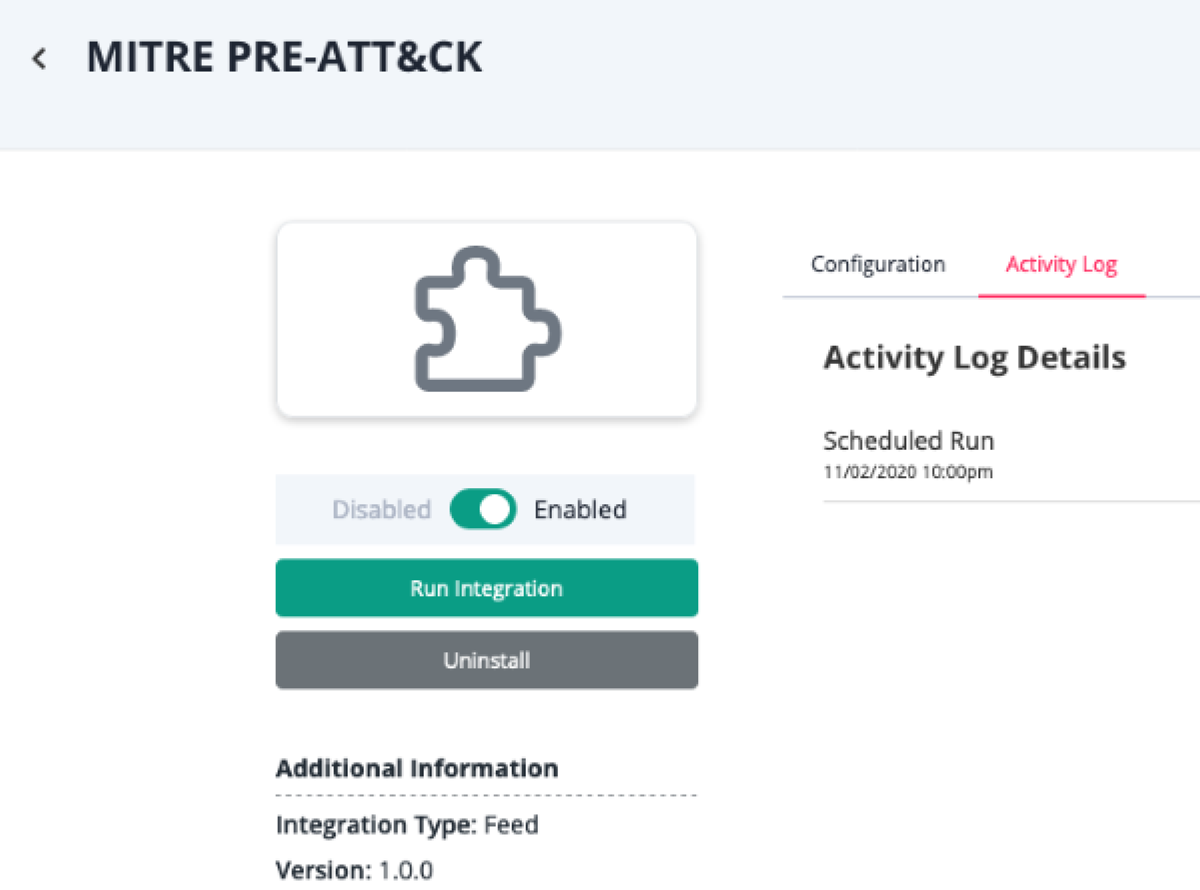
Triggering a Manual Run

The steps provided below are for performing manual runs for a CDF. See the Managing Workflows section of the ThreatQ Orchestrator TDR guide for steps on performing manual runs for CDWs.

> Not every CDF integration allows you to perform a manual run. If your CDF does not support manual runs, the Run Integration option will not load on the integration's details page.

From the My Integrations page:

1. Locate and click the integration to load its details page.



Scheduled Run
11/02/2020 10:00pm

Integration Type: Feed

Version: 1.0.0

> To locate an integration, you can filter the list by keyword, integration category, and/or status (enabled or disabled).

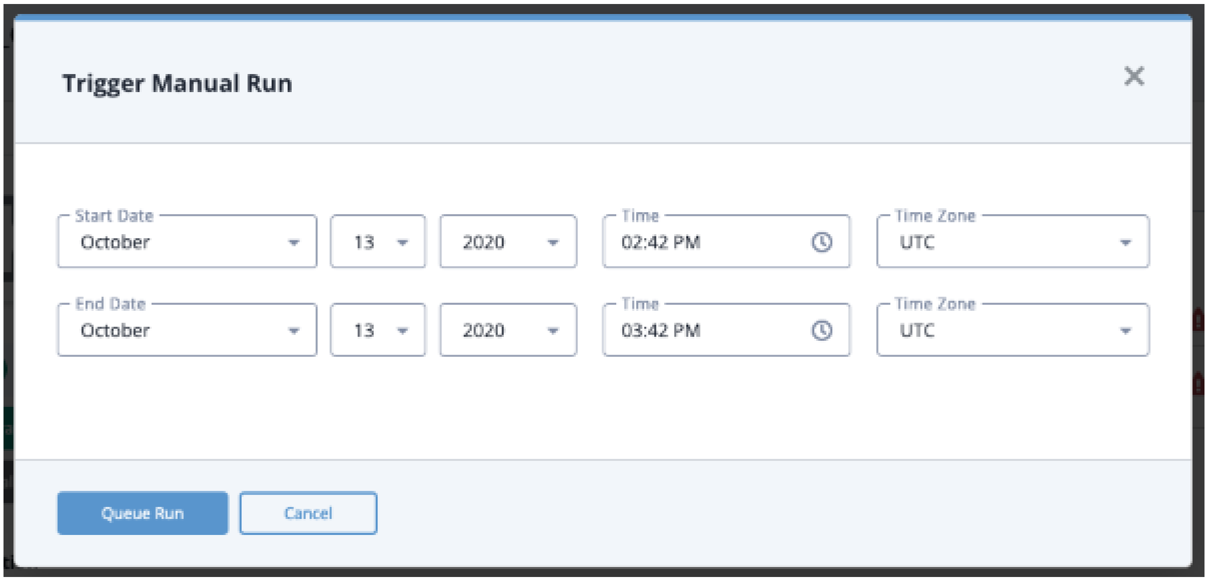
2. Confirm that the integration is enabled.

3. Click the **Run Integration** button located beneath Enable/Disable toggle switch.

> If the **Run Integration** button is not visible, the integration does not support manual runs.

The Trigger Manual Run window will be displayed.

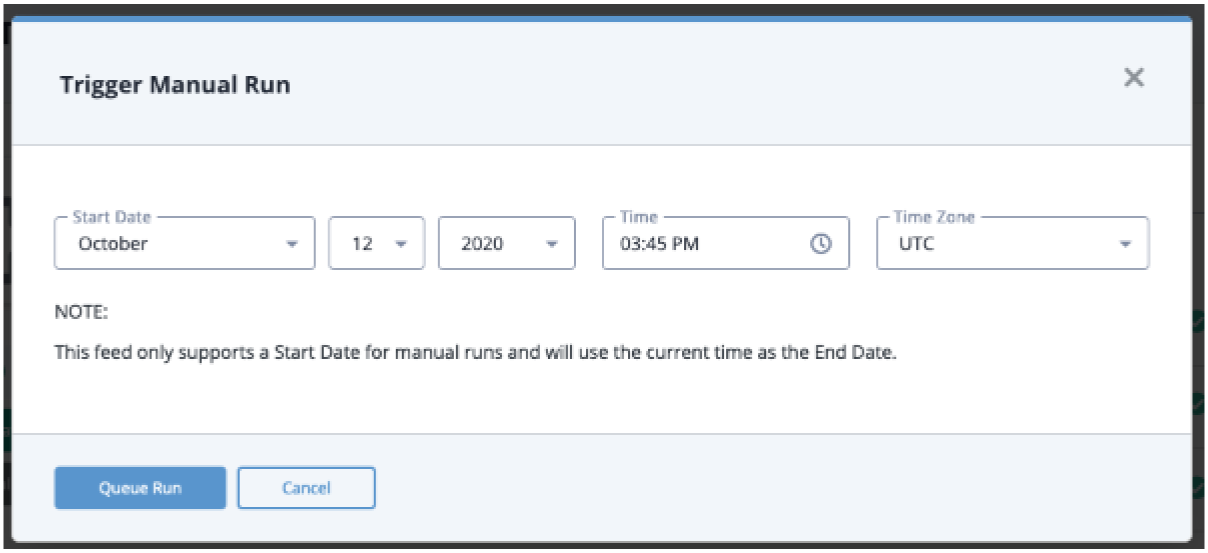
> The Start and End dates will tell the ThreatQ platform to pull new and updated information published by the feed provider for that time range.



Start Date: October 13 2020 Time: 02:42 PM Time Zone: UTC

End Date: October 13 2020 Time: 03:42 PM Time Zone: UTC

> Some feeds only support a Start Date.



Start Date: October 12 2020 Time: 03:45 PM Time Zone: UTC

NOTE:

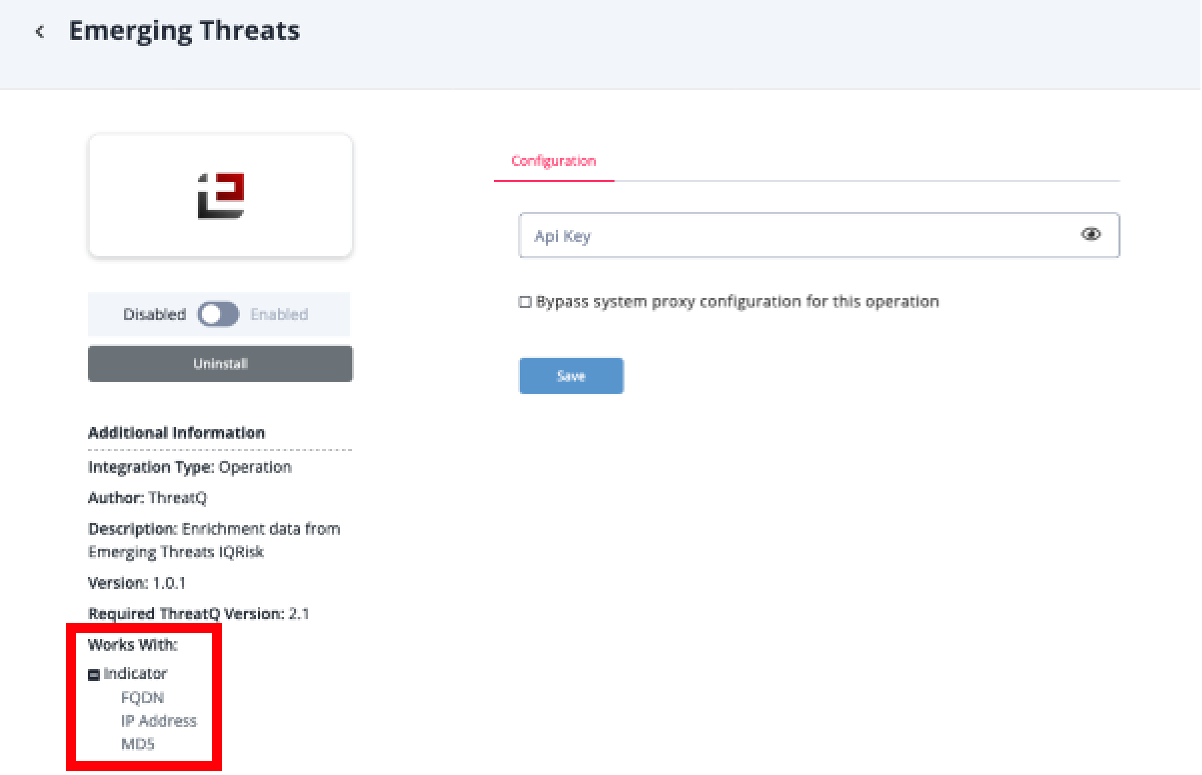
This feed only supports a Start Date for manual runs and will use the current time as the End Date.

4. Enter values into the Start and End Date fields and click the **Queue Run** button.

Running an Operation

The following steps may differ based on the individual operation. See the operation’s individual user guide for specific details.

Operations are designed to work with specific object types and sub-types. The operation's details page provides you with a list of object types that work with the operation.



☐ Bypass system proxy configuration for this operation

Additional Information

Integration Type: Operation

Author: ThreatQ

Description: Enrichment data from Emerging Threats IQRisk

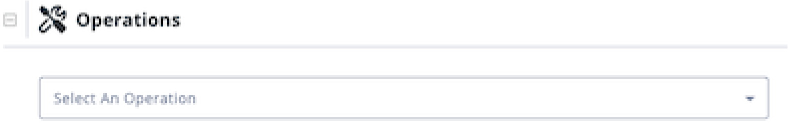
Version: 1.0.1

Required ThreatQ Version: 2.1

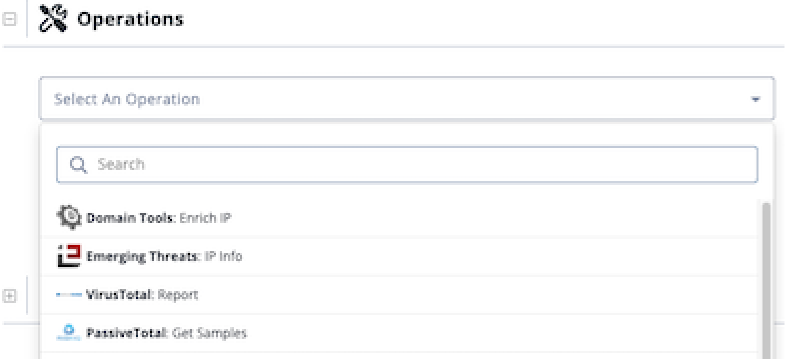
Works With:

- Indicator
  - FQDN
  - IP Address
  - MD5

1. Navigate to the Threat Library and locate a system object your operation works with.
2. Click the object to access its details page.
3. Scroll to the **Operations** pane on the details page.
   You can also click the Operations heading located in the left-hand menu to jump to the operations pane.
4. Expand the **Operations** pane by clicking the plus sign (+).



5. Click the arrow next to the **Select An Operation** field.

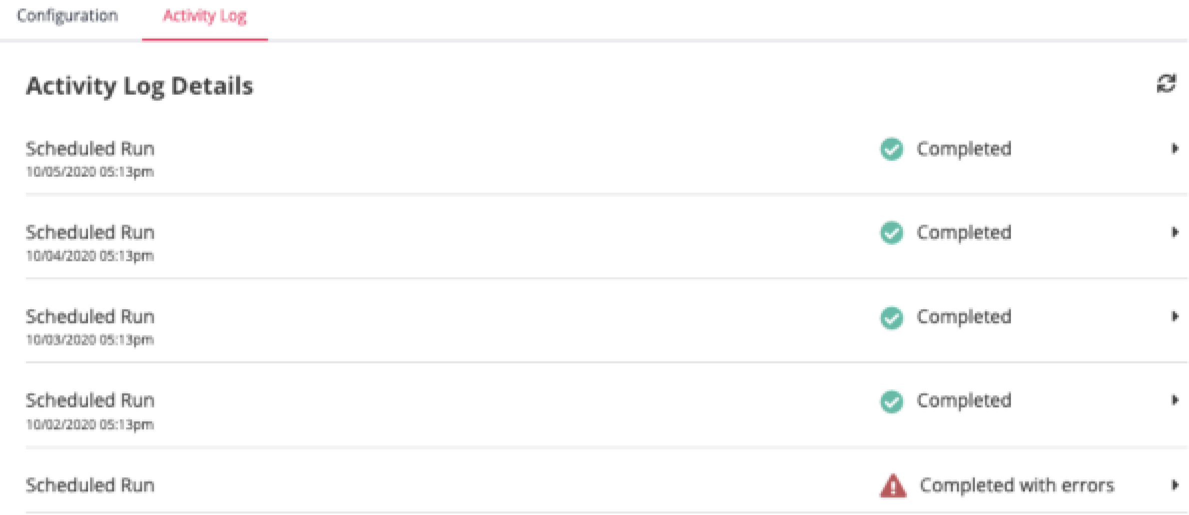


6. From this field you can:
    - Browse a list of all available operations.
    - Type the full or partial operation name in the Search field.
7. Click on an operation.

> Applicable configuration parameters are displayed below the operation name. After you update these fields, click the Run button to run the operation. If there are no configuration parameters for the operation, the operation will run automatically.

Activity Log (feeds)

The Activity Log provides you with details regarding recent runs performed by a CDF integration.



Activity Log Details

Scheduled Run 10/05/2020 05:13pm ✓ Completed

Scheduled Run 10/04/2020 05:13pm ✓ Completed

Scheduled Run 10/03/2020 05:13pm ✓ Completed

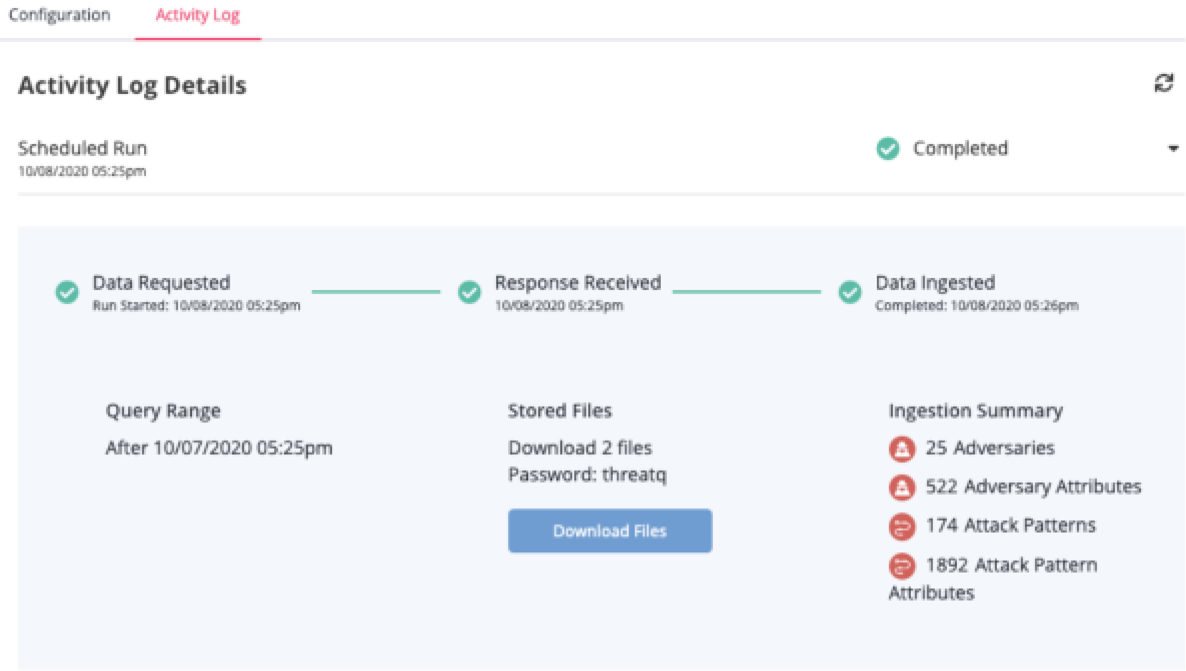
Scheduled Run 10/02/2020 05:13pm ✓ Completed

Scheduled Run ⚠ Completed with errors

The Log Details section displays run details that include:

LOG DATA	DETAILS
Type of Run	Whether the run was scheduled or triggered manually.
Date and Time	When the run, data and time, was initiated.
Outcome	Whether the run completed successfully or if it encountered errors.

You can click on the arrow icon next to the output to view run details such as an ingestion summary of objects ingested, download files (stored files), and additional timestamps regarding the run.



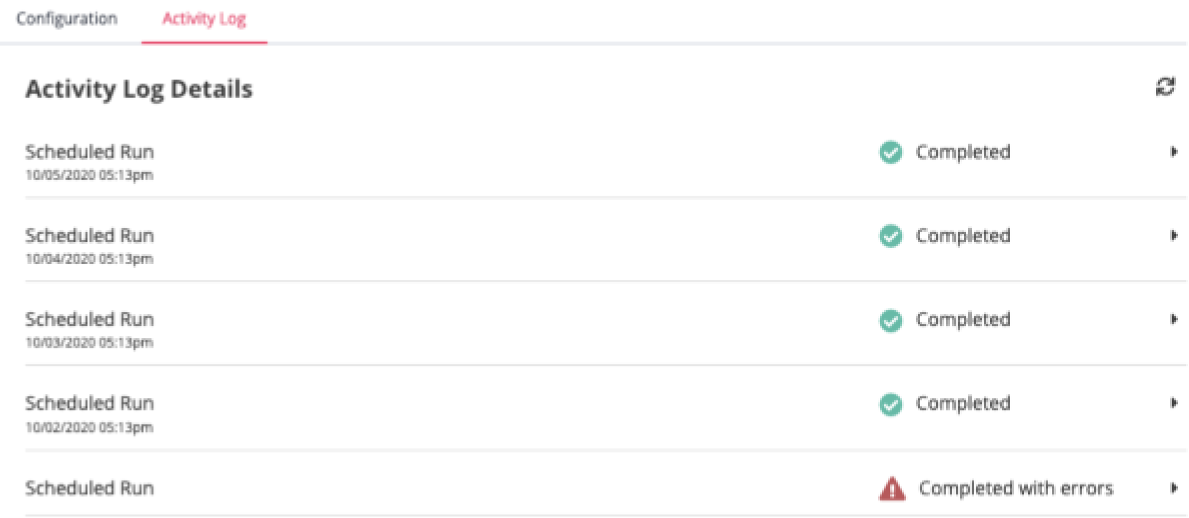
FIELD	DESCRIPTION
Run Started	The timestamp of when the run was initiated.
Response Received	The timestamp when the feed endpoint responded.
Data Ingested	The timestamp when the run was completed and intel data was ingested.
Query Range	The time frame for the data ingested.
Store Files	Zipped password-locked file(s) of the ingested data.
Ingested Summary	A summary of ingested object types.

Accessing a CDF's Activity Log

You can access CDF's activity log from the My Integrations page.

1. Locate and click on the integration to load its details page.

   The integration details page will load.



Activity Log Details

Scheduled Run 10/05/2020 05:13pm — Completed

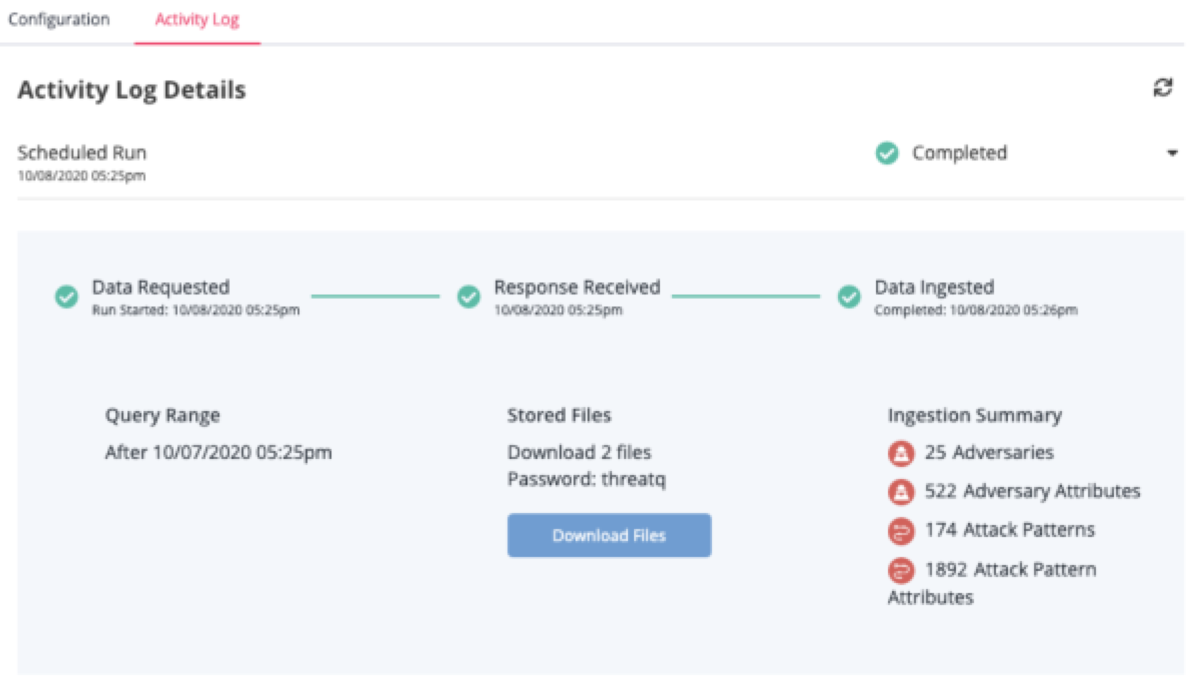
Scheduled Run 10/04/2020 05:13pm — Completed

Scheduled Run 10/03/2020 05:13pm — Completed

Scheduled Run 10/02/2020 05:13pm — Completed

Scheduled Run — Completed with errors

2. Select the **Activity Log** tab if not already selected.
3. Click on the arrow icon located next to a run’s outcome status to view additional details regarding the run.



Activity Log Details

Scheduled Run 10/08/2020 05:25pm — Completed

Data Requested — Run Started: 10/08/2020 05:25pm

Response Received — 10/08/2020 05:25pm

Data Ingested — Completed: 10/08/2020 05:26pm

Query Range

After 10/07/2020 05:25pm

Stored Files

Download 2 files

Password: threatq

Ingestion Summary

25 Adversaries

522 Adversary Attributes

174 Attack Patterns

1892 Attack Pattern Attributes

Removing an Integration

You can remove or disable an installed integration for the integration's details page. The key difference between these two actions is that removing an integration removes the integration from your instance (and UI) while disabling an integration deactivates an integration.

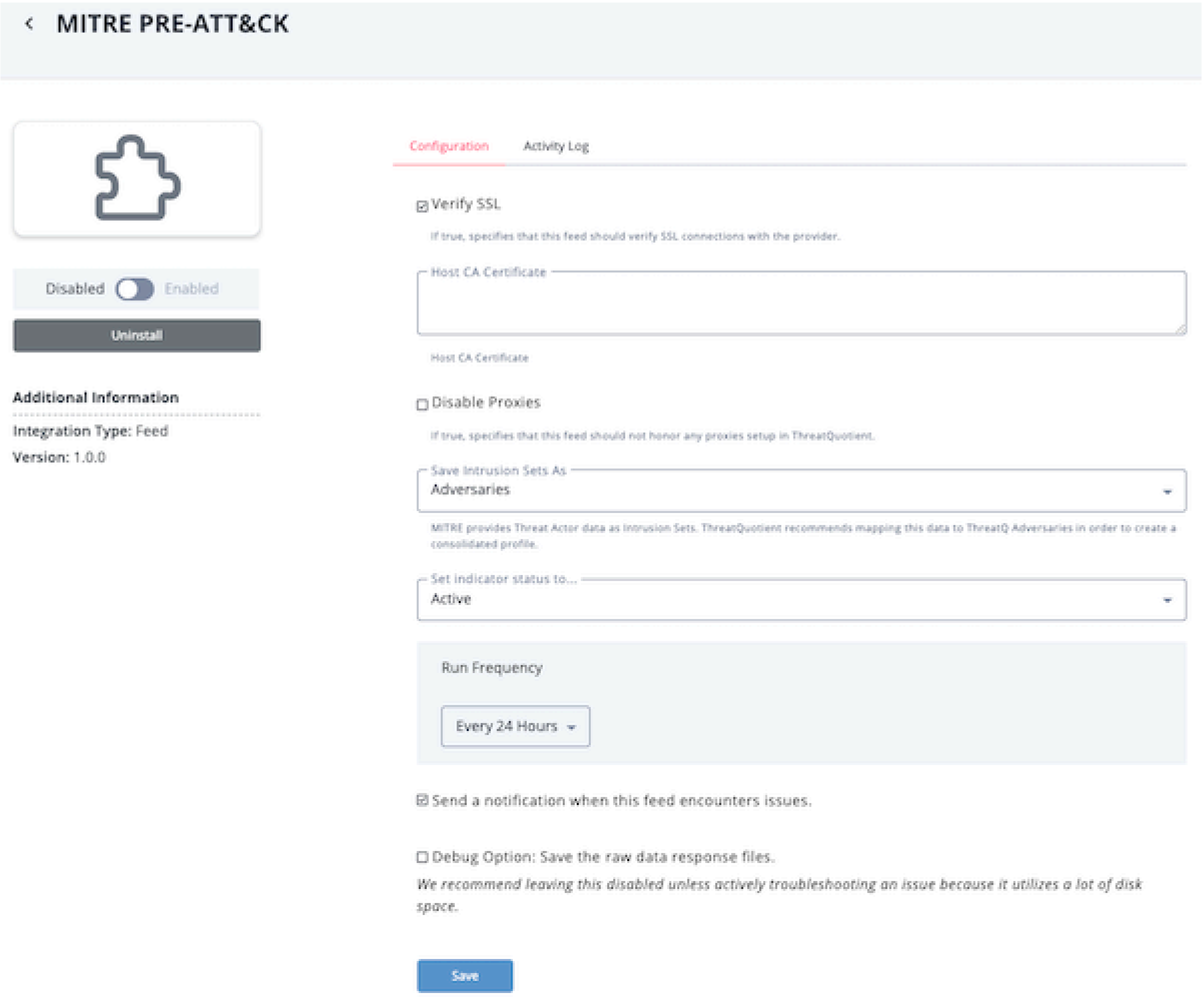
> Neither action will affect the threat data that you have already ingested into your ThreatQ instance.

Removing an Integration

Removing an integration will be remove the integration from the My Integrations UI. You can also disable an integration to deactivate it without completely removing the integration from your instance.

From the My Integrations page:

1. Locate and click the integration to load its details page.



Additional Information

Integration Type: Feed

Version: 1.0.0

☑ Verify SSL

If true, specifies that this feed should verify SSL connections with the provider.

Host CA Certificate

Host CA Certificate

☐ Disable Proxies

If true, specifies that this feed should not honor any proxies setup in ThreatQuotient.

Save Intrusion Sets As: Adversaries

MITRE provides Threat Actor data as Intrusion Sets. ThreatQuotient recommends mapping this data to ThreatQ Adversaries in order to create a consolidated profile.

Set indicator status to...: Active

Run Frequency: Every 24 Hours

☑ Send a notification when this feed encounters issues.

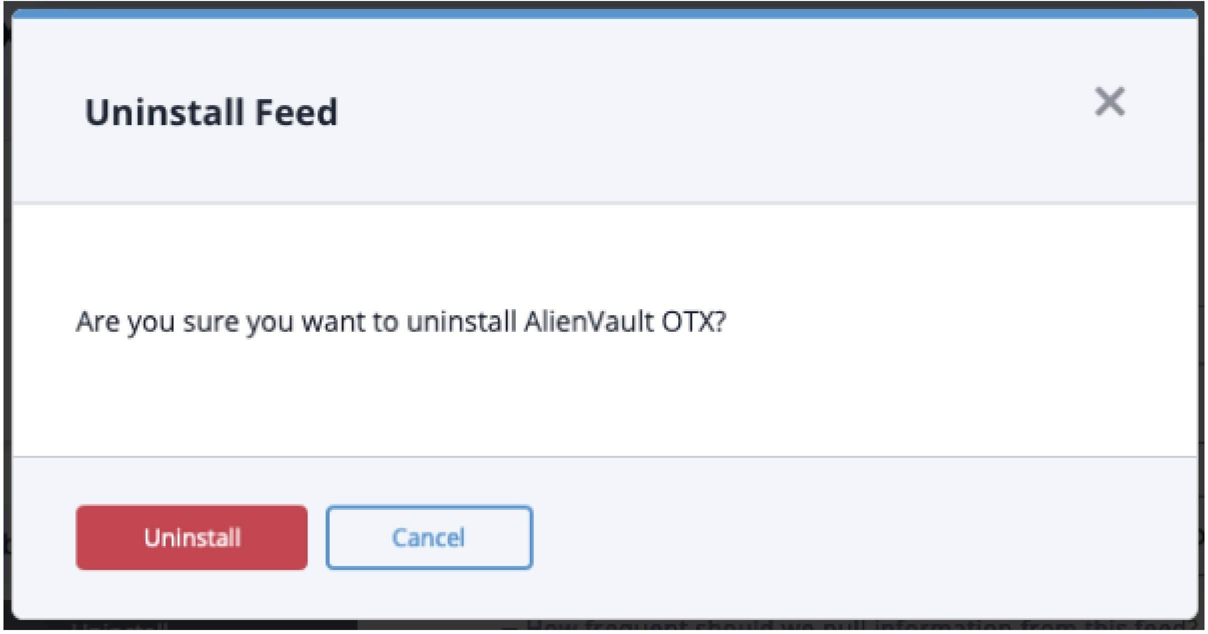
☐ Debug Option: Save the raw data response files.

We recommend leaving this disabled unless actively troubleshooting an issue because it utilizes a lot of disk space.

> To locate an integration, you can filter the list by keyword, integration category, and/or status (enabled or disabled).

2. Click the **Uninstall** button located below the Enable/Disable toggle.

The Uninstall dialog box prompts you to confirm the uninstall selection.



Uninstall Feed

Are you sure you want to uninstall AlienVault OTX?

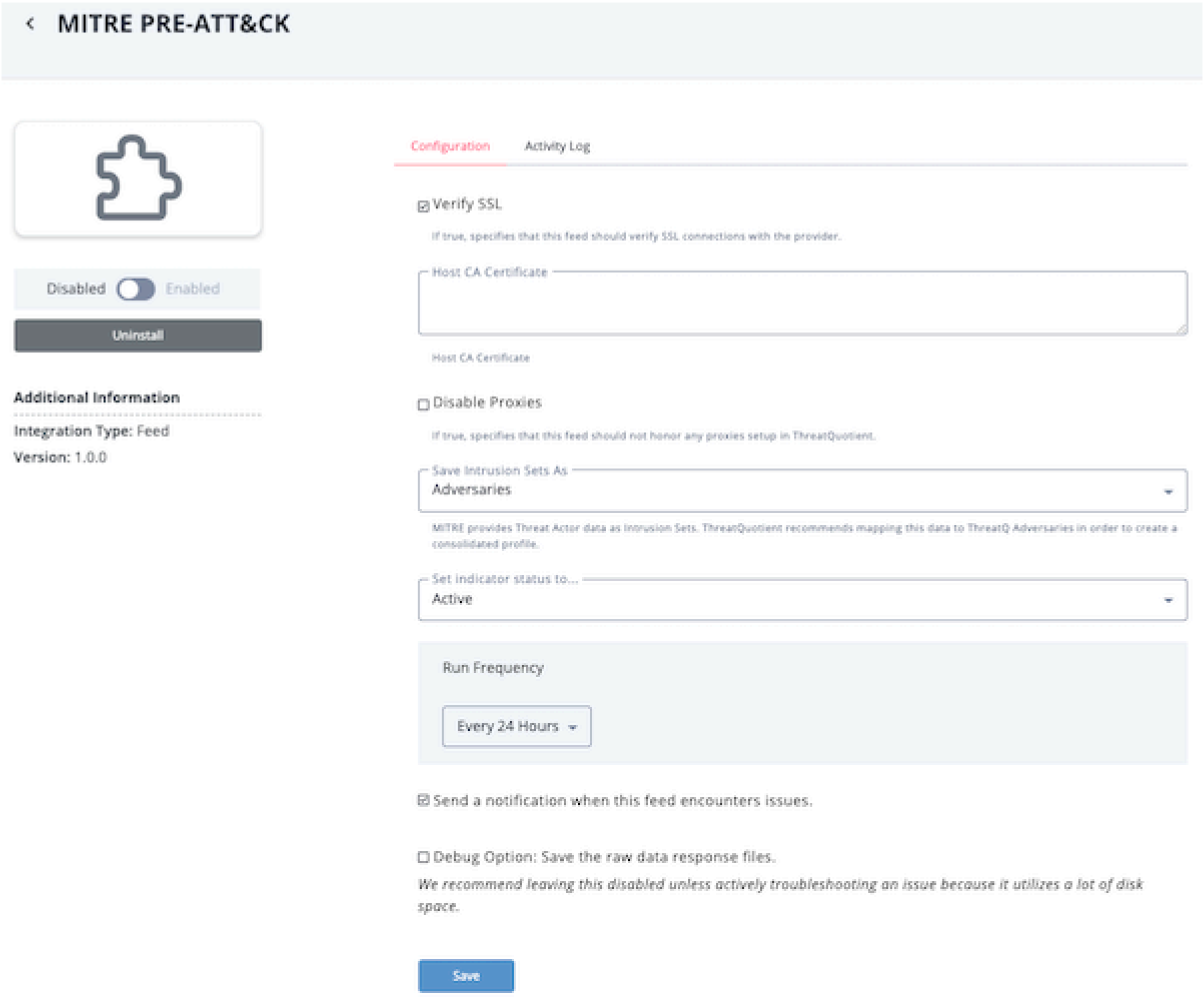
3. Click **Uninstall** to confirm and remove the integration.

Disabling an Integration

Perform the following steps to disable an integration installed on your ThreatQ instance:

From the My Integrations page:

1. Locate and click on the integration to load its details page.



Additional Information

Integration Type: Feed

Version: 1.0.0

☑ Verify SSL

If true, specifies that this feed should verify SSL connections with the provider.

Host CA Certificate

Host CA Certificate

☐ Disable Proxies

If true, specifies that this feed should not honor any proxies setup in ThreatQuotient.

Save Intrusion Sets As: Adversaries

MITRE provides Threat Actor data as Intrusion Sets. ThreatQuotient recommends mapping this data to ThreatQ Adversaries in order to create a consolidated profile.

Set indicator status to...: Active

Run Frequency: Every 24 Hours

☑ Send a notification when this feed encounters issues.

☐ Debug Option: Save the raw data response files.

We recommend leaving this disabled unless actively troubleshooting an issue because it utilizes a lot of disk space.

2. Click the **Enable/Disable** toggle switch to disable the integration.

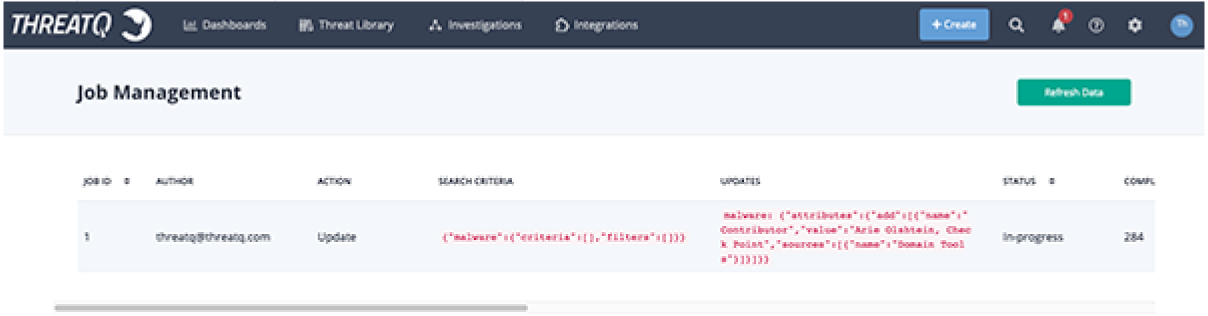
Job Management

> 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. See the Bulk Actions section for more details.

To access the Job Management page:

1. Navigate to Settings ⚙ > Job Management.



JOB ID	AUTHOR	ACTION	SEARCH CRITERIA	UPDATES	STATUS	COMPL
1	threatq@threatq.com	Update	{"malware":{"criteria":[],"filters":[]}}	malware: {"attributes":{"add":[{"name":"Contributor","value":"Arie Olshtein, Check Point","sources":[{"name":"Domain Tools"}]}]}}	In-progress	284

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.
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.

FIELD	DESCRIPTION
	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 Remaining	The estimated time remaining until the job is complete.
Date Created	The timestamp of when the job was created and queued.

FIELD	DESCRIPTION
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.

Licensing

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 Installation. Any subsequent license updates can be applied in the ThreatQ user interface.

Access to additional ThreatQ products, such ThreatQ Investigations and ThreatQ Data Exchange, are tied to your ThreatQ Platform (TQ) license. Adding these features will result in ThreatQ Support issuing a new license to apply to your platform.

> ThreatQ licenses are not perpetual.

Managing Your ThreatQ License

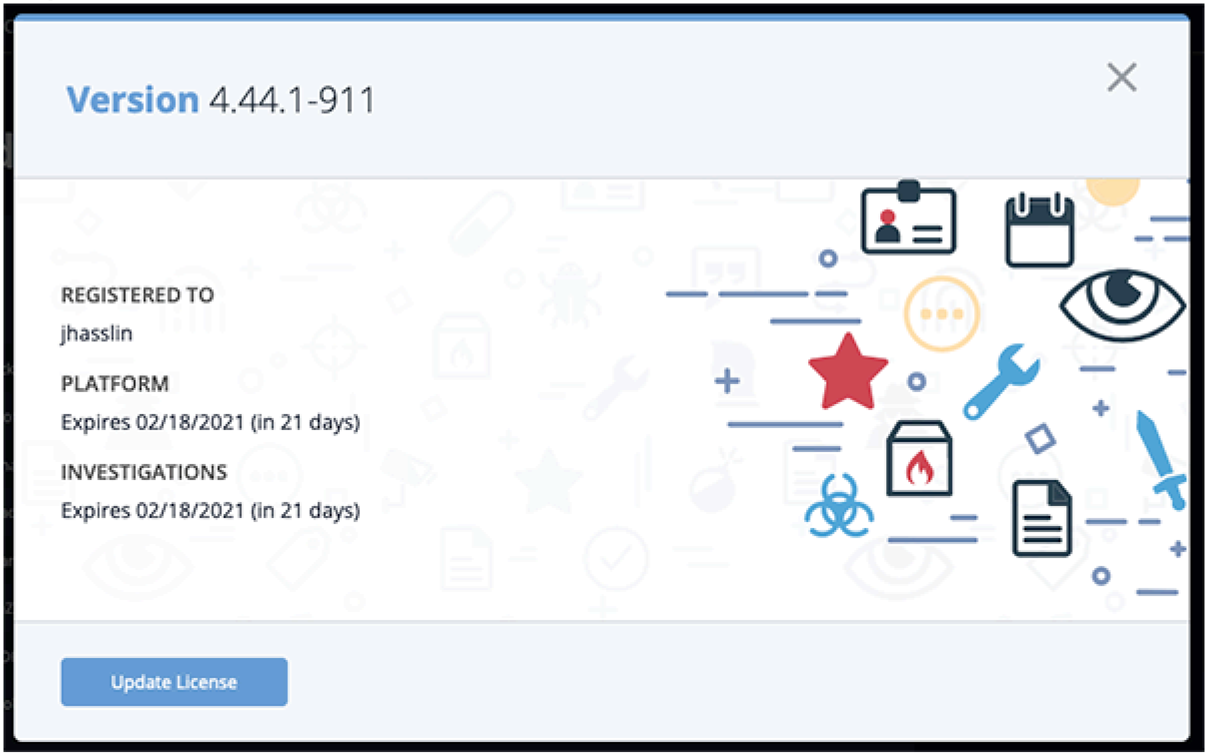
You can view and update your ThreatQ license using the ThreatQ user interface.

Viewing License Status

1. Click on the **Settings** ⚙ icon and select **About**.

   The License information window loads. You can also view additional licensing-based ThreatQ products, such as ThreatQ Investigations (TQI) and ThreatQ Data Exchange

(TQX) - Publisher license.



Version 4.44.1-911

REGISTERED TO
jhasslin

PLATFORM
Expires 02/18/2021 (in 21 days)

INVESTIGATIONS
Expires 02/18/2021 (in 21 days)

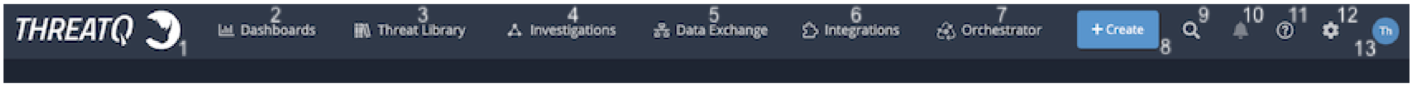
Updating a License

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

1. Click on the **Settings** ⚙ icon and select **About**.
   The License information window loads.
2. Select the **Update License** option.
3. Enter the new license key.
4. Click on **Submit**.

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	Dashboards	The Dashboards link in the top navigation bar allows you to access a drop-down list of your dashboards.	• Dashboards
3	Threat Library	Access and search the Threat Library and view system object details.	• Threat Library • Building Searches with Filter Sets • Object Details • Bulk Actions • Data Controls
4	Investigations	Navigates to ThreatQ Investigations (TQI), a cybersecurity situation room that enables collaborative threat	• ThreatQ Investigations

#	NAME	DESCRIPTION	REFERENCES
		analysis, investigation, and coordinated response.	
5	Data Exchange	Allows the bi-directional sharing of threat intelligence across multiple ThreatQ instances.	• ThreatQ Data Exchange
6	Integrations	Allows you to access the Marketplace as well as you integrations.	• Integrations Management
7	Orchestrator	Opens the ThreatQuotient TDR Orchestrator (TQO) which includes enhanced automation, analysis and reporting capabilities that accelerate threat detection and response across disparate systems.	• ThreatQ TDR Orchestrator (TQO)
8	Create Button	Create system objects.	• Adversaries • Events • Files • Indicators • Signatures • STIX
9	Search Icon	Perform a basic search for a system object.	• Building Searches with Filter Sets

#	NAME	DESCRIPTION	REFERENCES
10	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
11	Help Icon	Click the Help icon to quickly access the Help Center, Product Updates, Getting Started Guides, and Video Demos. The search field at the top of the menu also gives you the option to search the Help Center.	• Product Updates • Installation • Videos
12	Site Settings	Allows you to manage your ThreatQ application settings as well as view your version and licenses.	• Exports • Job Management • Object Management • Reports • Server Administration • System Configuration • User Management • Licensing
13	User Icon	Access your user profile.	• User Management

Notifications

The ThreatQ Platform (TQ) offers platform-related alerts in the form of in-app notifications, via the Notification Center, and feed health emails.

In-app notifications include:

- Bulk Actions updates
- Feed health alerts
- Task assignment notifications
- Sharing notifications

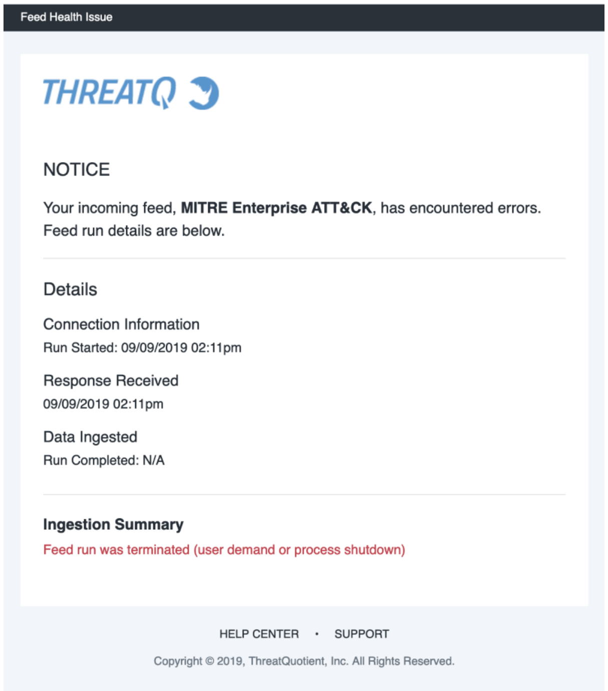
> Only users with Administrator and Maintenance roles will receive in-app feed health alerts via the Notification Center.

Administrators and Maintenance account users can subscribe users to Feed Health Email Notifications . These users will receive an email when a feed encounters an error when preforming a run.

Feed Health Email Notifications

Feed Health Notifications allows the ThreatQ Platform (TQ) to send you, and other designated users, email notifications when a Configuration Driven Feed (CDF) or Configuration Driven Workflow (CDW) encounters an issue.

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.



Feed Health Issue

NOTICE

Your incoming feed, **MITRE Enterprise ATT&CK**, has encountered errors. Feed run details are below.

Details

Connection Information
Run Started: 09/09/2019 02:11pm

Response Received
09/09/2019 02:11pm

Data Ingested
Run Completed: N/A

Ingestion Summary
Feed run was terminated (user demand or process shutdown)

Configuring Mail Server

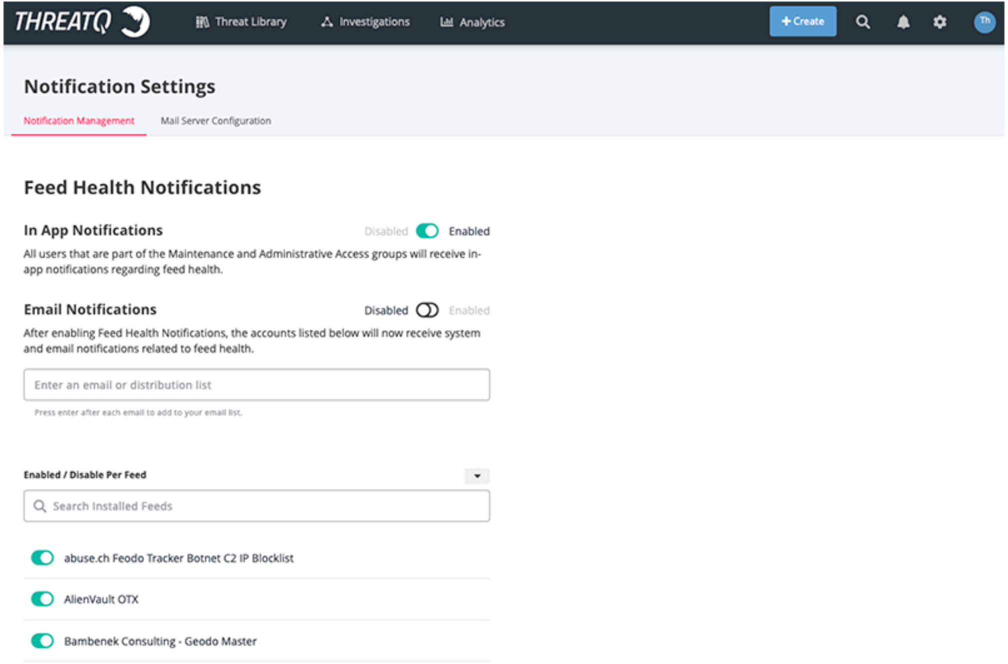
You must enter your mail server information on the Mail Server Configuration tab before enabling Feed Health Notifications.

> 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.



In App Notifications Disabled / Enabled

All users that are part of the Maintenance and Administrative Access groups will receive in-app notifications regarding feed health.

Email Notifications Disabled / Enabled

After enabling Feed Health Notifications, the accounts listed below will now receive system and email notifications related to feed health.

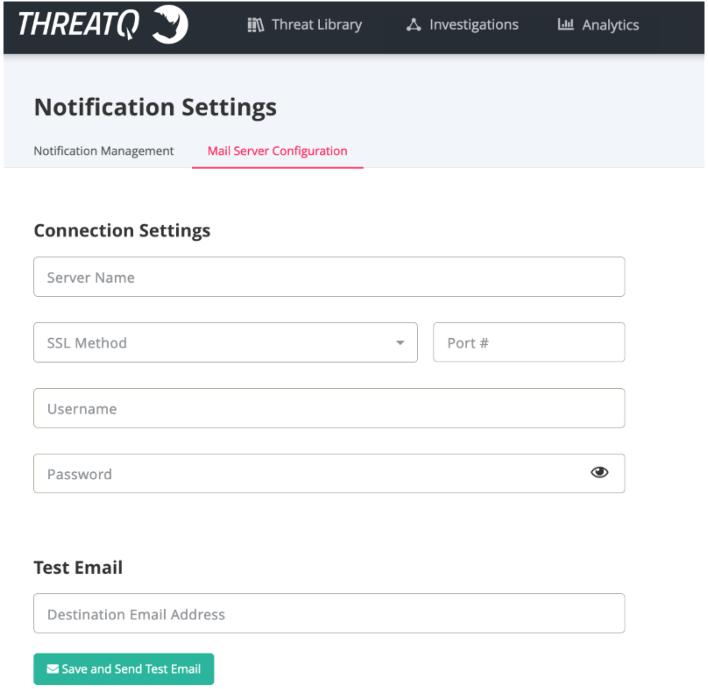
Enter an email or distribution list

Press enter after each email to add to your email list.

- abuse.ch Feodo Tracker Botnet C2 IP Blocklist
- AlienVault OTX
- Bambenek Consulting - Geodo Master

2. Click on the **Mail Server Configuration** tab.

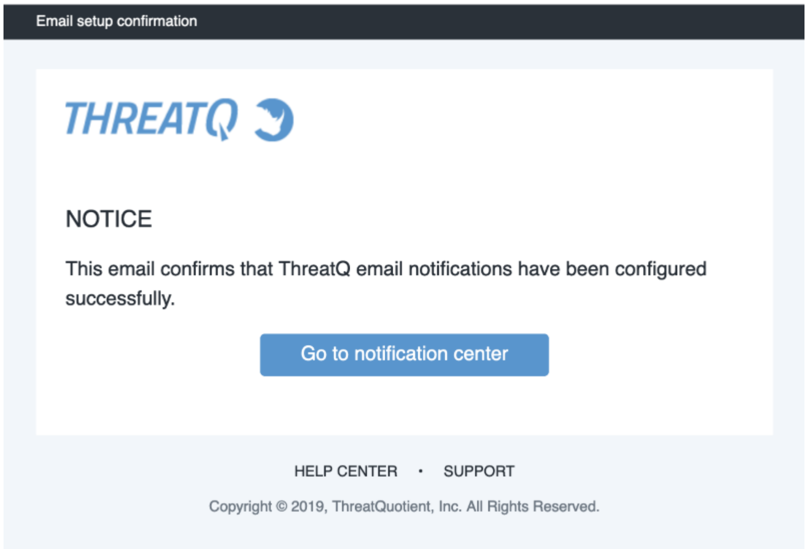
   The Mail Server Configuration page loads.



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: ◦ 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.



NOTICE

This email confirms that ThreatQ email notifications have been configured successfully.

Copyright © 2019, ThreatQuotient, Inc. All Rights Reserved.

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.

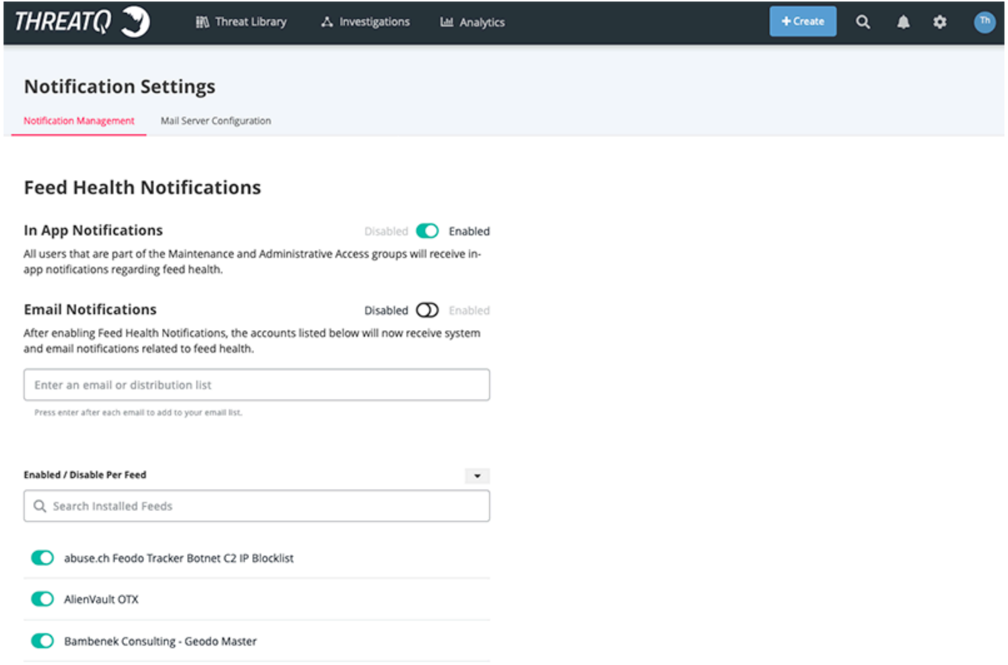
If using Email Notifications, the Mail Server Configuration tab must completed before you enable the feature.

> 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.



All users that are part of the Maintenance and Administrative Access groups will receive in-app notifications regarding feed health.

After enabling Feed Health Notifications, the accounts listed below will now receive system and email notifications related to feed health.

Press enter after each email to add to your email list.

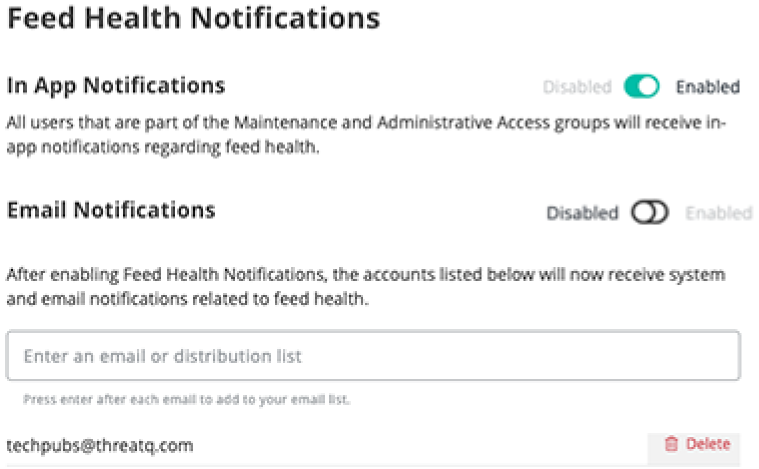
abuse.ch Feodo Tracker Botnet C2 IP Blocklist

AlienVault OTX

Bambenek Consulting - Geodo Master

2. Perform the following steps to enable email and in-app notifications:

- > *Enable In-App Feed Health Notifications*
    a. Click on the **Enable** toggle switch for **In App Notifications**.
- > *Enable Feed Health Email Notifications*
    a. Enter an email address in the account field and press the **<Enter>** or **<Return>** key.



Feed Health Notifications

In App Notifications — Disabled / Enabled (enabled)

All users that are part of the Maintenance and Administrative Access groups will receive in-app notifications regarding feed health.

Email Notifications — Disabled (disabled) / Enabled

After enabling Feed Health Notifications, the accounts listed below will now receive system and email notifications related to feed health.

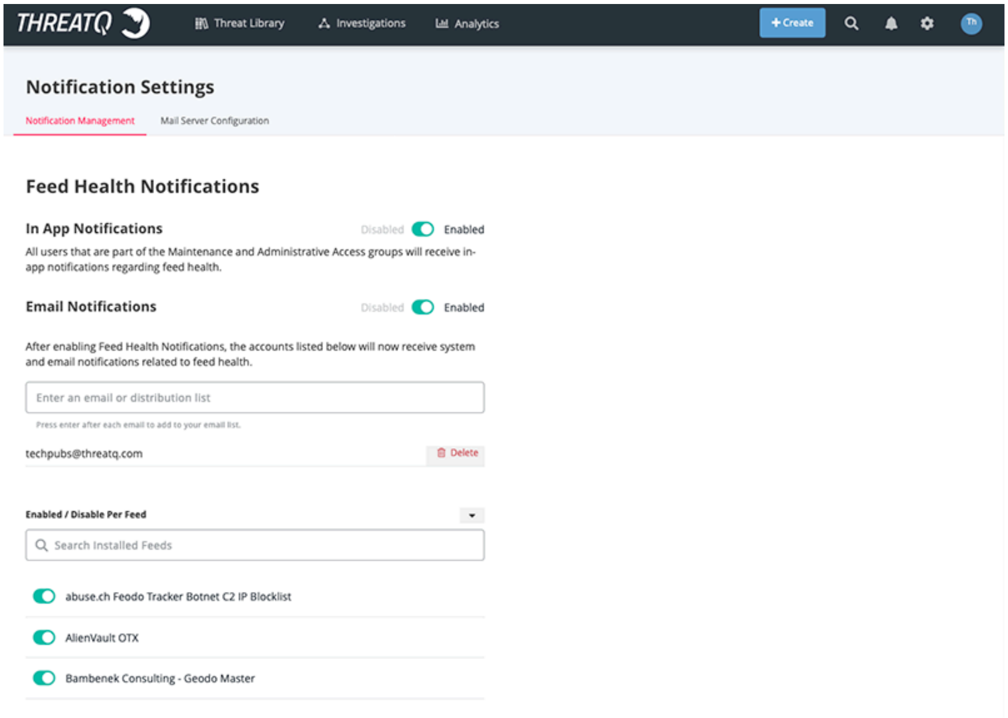
Enter an email or distribution list

Press enter after each email to add to your email list.

techpubs@threatq.com — Delete

    b. Click on the **Enable** toggle switch for **Email Notifications**.

3. Use the toggle switch next to each feed to enable/disable notifications for individual feeds.



Notification Settings

Notification Management | Mail Server Configuration

Feed Health Notifications

In App Notifications — Disabled / Enabled (enabled)

All users that are part of the Maintenance and Administrative Access groups will receive in-app notifications regarding feed health.

Email Notifications — Disabled / Enabled (enabled)

After enabling Feed Health Notifications, the accounts listed below will now receive system and email notifications related to feed health.

Enter an email or distribution list

Press enter after each email to add to your email list.

techpubs@threatq.com — Delete

Enabled / Disable Per Feed

Search Installed Feeds

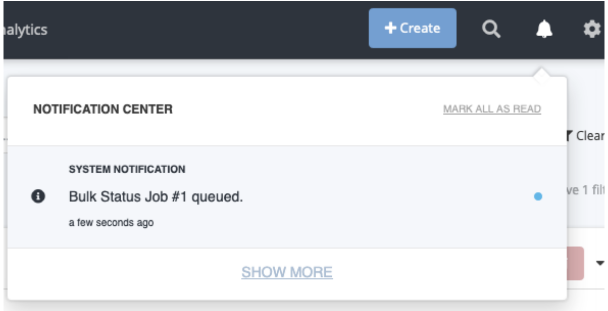
- abuse.ch Feodo Tracker Botnet C2 IP Blocklist (enabled)
- AlienVault OTX (enabled)
- Bambenek Consulting - Geodo Master (enabled)

> You can also enable/disable individual CDF feed notifications by clicking on the feed under Integrations and checking/unchecking the notifications checkbox.

Notification Center

The icon is located on the navigation menu for the platform. This allows you to monitor system processes while working within ThreatQ.

The Notification Center alerts you, via an in-app notification icon, when a platform process, such as a Bulk Actions job, has been queued and/or completed.

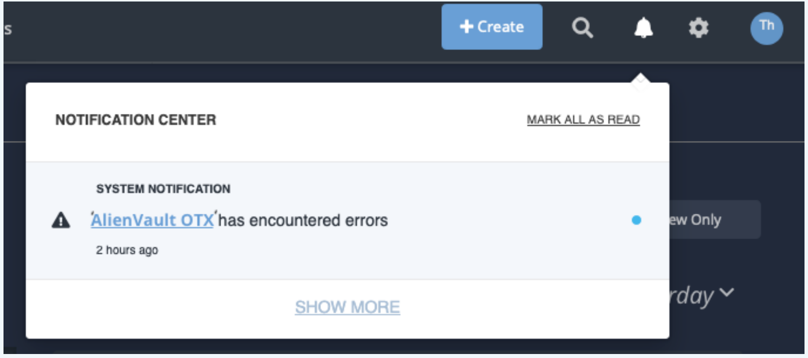


SYSTEM NOTIFICATION

Bulk Status Job #1 queued.

a few seconds ago

> Administrator and maintenance accounts can also receive feed health notifications via the Notification Center. See Enabling Feed Health Notifications section in the Feed Health Email Notifications topic.



SYSTEM NOTIFICATION

'AlienVault OTX' has encountered errors

2 hours ago

Sharing Notifications

The ThreatQ Notification Center alerts you about data collection, dashboard, or investigation permission changes that affect you. For instance, it notifies you when another user shares a data collection, dashboard, or investigation with you or when a data collection, dashboard, or investigation you own is shared with another user.

The following table describes the actions that trigger a sharing notification and the content of these notifications. The data collection, dashboard, or investigation name included in a sharing notification also includes a hyperlink to the corresponding object.

SCENARIO	VIEWER	EDITOR	OWNER
A user shares a data collection, dashboard, or investigation with you.	`You have been added as a Viewer to` **_<Name>_**	`You have been added as an Editor to` **_<Name>_**	N/A
A user changes your permissions to editor or viewer.			
A user changes your permissions to owner.	`You have been assigned as the Owner of` **_<Name>_**		
A data collection, dashboard, or investigation you own has been shared with another user.	N/A	N/A	**_<Name>_** `has been shared`
Your permissions to a data collection, dashboard, or	`You have been removed from` **_<Name>_**		N/A

investigation have been removed.			
A user request access to an investigation via an object details page.	N/A	N/A	`User` **`<User Name>`** `has requested access to` **`<Name>`**

Object Management

The Object Management section of the ThreatQ platform allows Maintenance and Admin users to work with:

SECTION	DETAILS
Indicator Statuses	Create and edit custom indicator statuses.
Indicator Types	View your platform's indicator types.
Event Types	Create and edit custom event types.
Attributes	Update attribute keys and values associated with system objects.

Indicator Statuses Management

The Indicator Statuses page allows you to view, duplicate, add, edit, and delete available system-wide indicator statuses. You cannot edit or delete indicator statuses provided by ThreatQ (Active, Expired, Indirect, Review, Whitelisted), but you can add, edit, and delete your custom statuses.

Indicator Status Assignment

Multiple factors affect the indicators created from the relations on an individual object in a request. When using API/Indicators/Consume, each individual object in the request JSON is an indicator, and each indicator can have additional indicator relations stored under an indicators field in that object. As a result, the status of an indicator depends on the configuration of the request JSON.

Indirect Indicator Status

When you set up a default status of Indirect, the system assigns this status to indicators in the following scenarios:

- A status or status_id field is not provided for the parent object.
- A status or status ID is not provided for the additional indicator relations of the object.
- The JSON request body includes duplicate indicators and one of the duplicates has a default status ID. If none of the duplicates has a default status ID, the system uses the status ID of the last duplicate.

Currently, the Indirect Indicator status only applies to IOCs related to a main indicator.

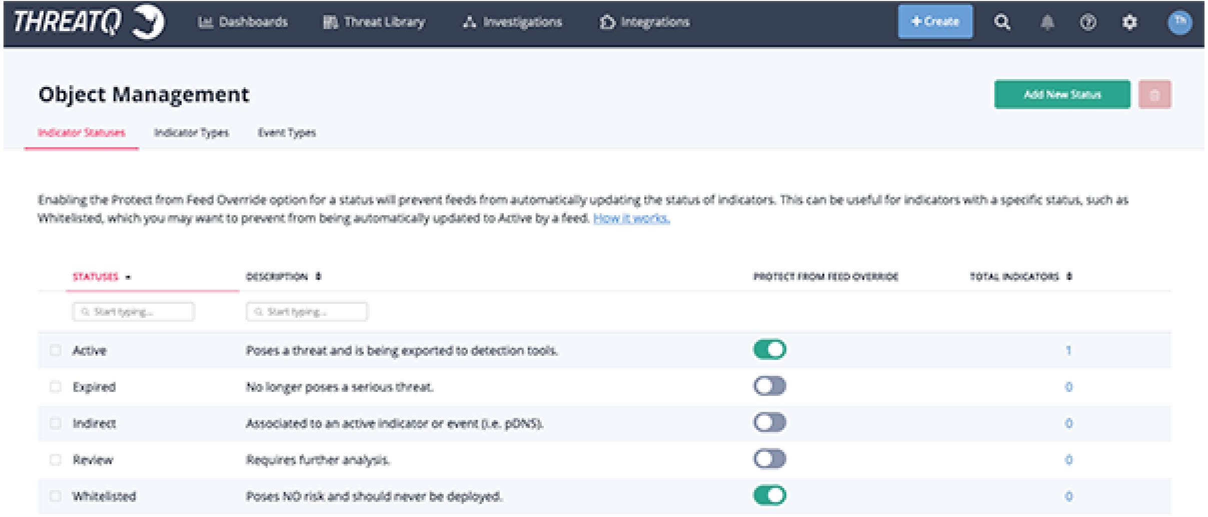
Protected Indicator Statuses

When doing insertions, ThreatQ determines if the indicator already exists and the Indicator status is a protected status, If so, the system retains the status.

Viewing Indicator Statuses

1. Navigate to Settings ⚙ > Object Management.

The Object Management page opens to the Indicator Statuses tab.



Object Management

Enabling the Protect from Feed Override option for a status 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. How it works.

	STATUSES	DESCRIPTION	PROTECT FROM FEED OVERRIDE	TOTAL INDICATORS
☐	Active	Poses a threat and is being exported to detection tools.	●	1
☐	Expired	No longer poses a serious threat.	○	0
☐	Indirect	Associated to an active indicator or event (i.e. pDNS).	○	0
☐	Review	Requires further analysis.	○	0
☐	Whitelisted	Poses NO risk and should never be deployed.	●	0

> 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
Status Filter	Enter a keyword in the text field to filter the table by status name. You can click on the Statuses header to sort the table by alphabetical order.
Description Filter	Enter a keyword in the text field to filter the table by status description. You can click on the Description header to sort the table by alphabetical order.
Protect from Feed Override	Clicking on the toggle switch in this column will enable/disable the Protect from Feed Override option for that status. See the Suppressing Indicator Status Updates section below for more details on this feature.
Total Indicators	The number of indicators currently using the status. Clicking on the value will open the Threat Library filtered to that status. Clicking on the

FUNCTION	DESCRIPTION
	Total Indicators heading will sort the table in ascending/descending order.

Suppressing Indicator Status Updates

Enabling the **Protect from Feed Override** option for a status, prevents feeds from automatically updating indicators with this status to another. Any status with a green toggle switch is currently protected from status updates. Those with grey toggle switches are not.

Use Case: You have a well-vetted set of whitelisted indicators that you do not want to update without internal review and discussion. To protect these indicators from automatic status updates from feeds, toggle the **Protect from Feed Override** switch for the **Whitelisted** status to green (active). After you make this change, ThreatQ retains the status of **Whitelisted** for any indicator to which it is assigned and suppresses any updated status information received from a feed.

1. Navigate to Settings ⚙ > Object Management.

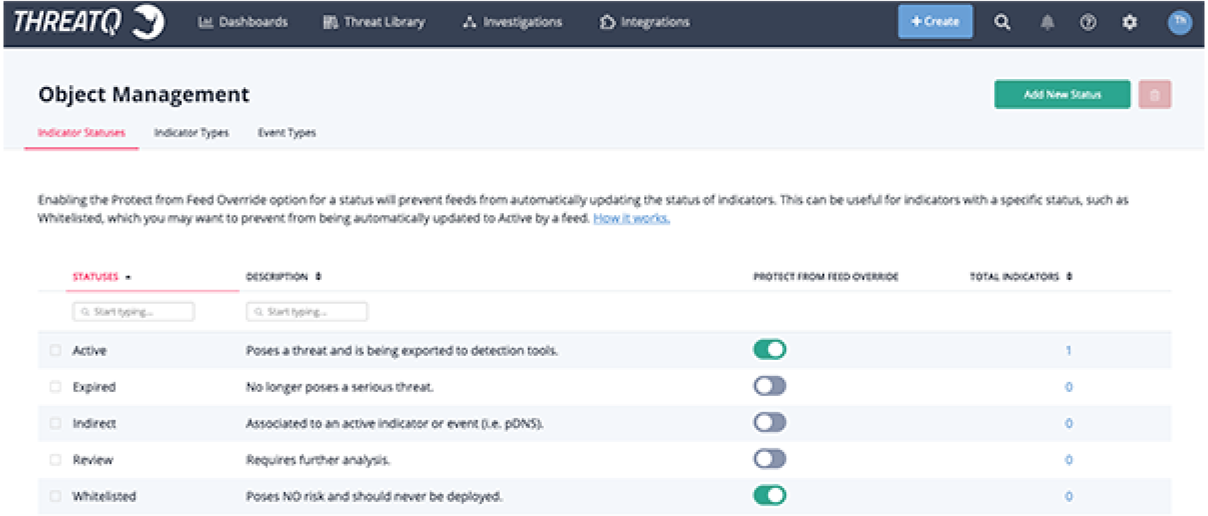
   The Object Management page opens to the Indicator Statuses tab.

2. In the Protect From Feed Override column, click the toggle switch corresponding to the status to change it from grey (status updates allowed) to green (status updates suppressed).

Adding an Indicator Status

1. Navigate to Settings ⚙ > Object Management.

The Object Management page opens to the Indicator Statuses tab.

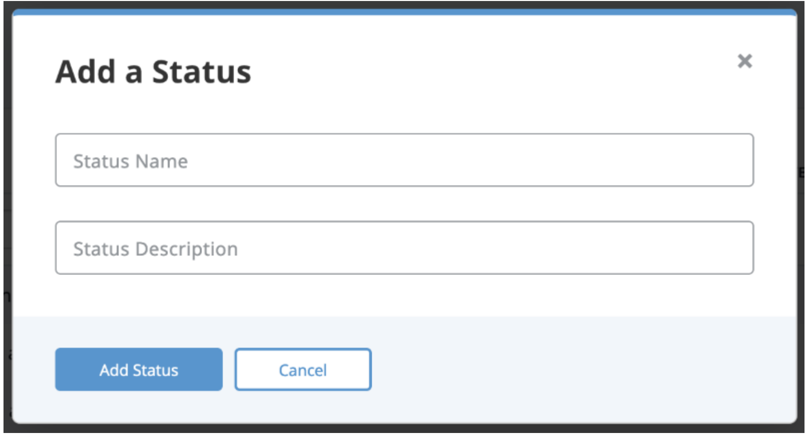


Enabling the Protect from Feed Override option for a status will prevent feeds from automatically updating the status of indicators. This can be useful for indicators with a specific status, such as Whitelisted, which you may want to prevent from being automatically updated to Active by a feed. How it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

STATUSES	DESCRIPTION	PROTECT FROM FEED OVERRIDE	TOTAL INDICATORS
☐ Active	Poses a threat and is being exported to detection tools.	●	1
☐ Expired	No longer poses a serious threat.	○	0
☐ Indirect	Associated to an active indicator or event (i.e. pDNS).	○	0
☐ Review	Requires further analysis.	○	0
☐ Whitelisted	Poses NO risk and should never be deployed.	●	0

2. Click **Add New Status**.

   The Add a Status dialog box opens.



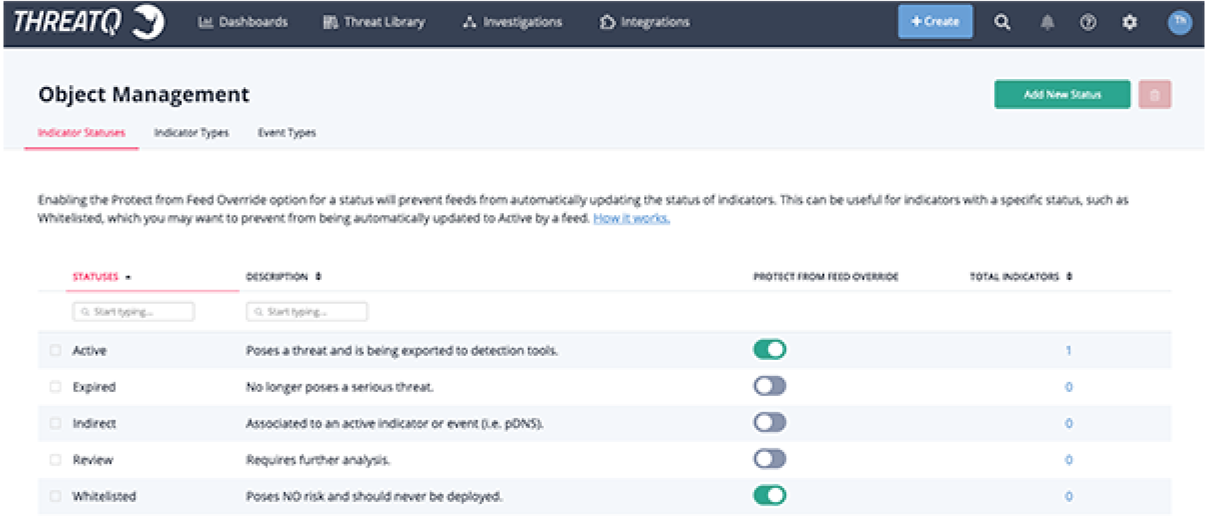
3. Enter a **Status Name**.
4. Optionally, enter a **Status Description**.
5. Click **Add Status**.

Editing an Indicator Status

⚠ You cannot edit an indicator status provided by ThreatQ.

1. Navigate to Settings ⚙ > Object Management.

The Object Management page opens to the Indicator Statuses tab.

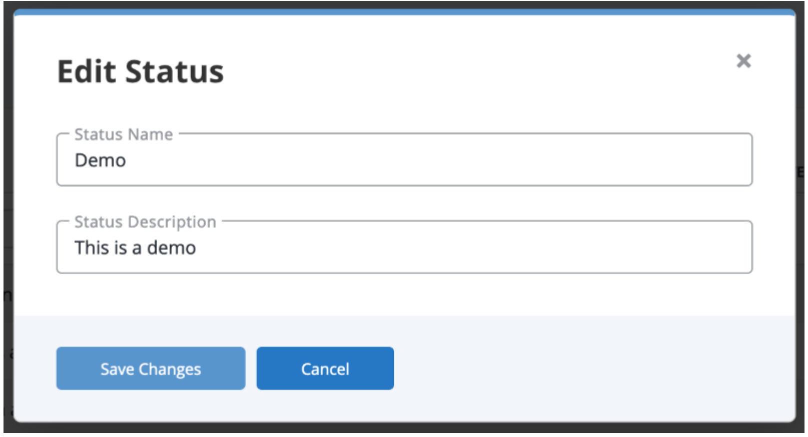


Enabling the Protect from Feed Override option for a status will prevent feeds from automatically updating the status of indicators. This can be useful for indicators with a specific status, such as Whitelisted, which you may want to prevent from being automatically updated to Active by a feed. How it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

STATUSES	DESCRIPTION	PROTECT FROM FEED OVERRIDE	TOTAL INDICATORS
Active	Poses a threat and is being exported to detection tools.	●	1
Expired	No longer poses a serious threat.	○	0
Indirect	Associated to an active indicator or event (i.e. pDNS).	○	0
Review	Requires further analysis.	○	0
Whitelisted	Poses NO risk and should never be deployed.	●	0

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

   The Edit Status dialog box opens.



Status Name: Demo

Status Description: This is a demo

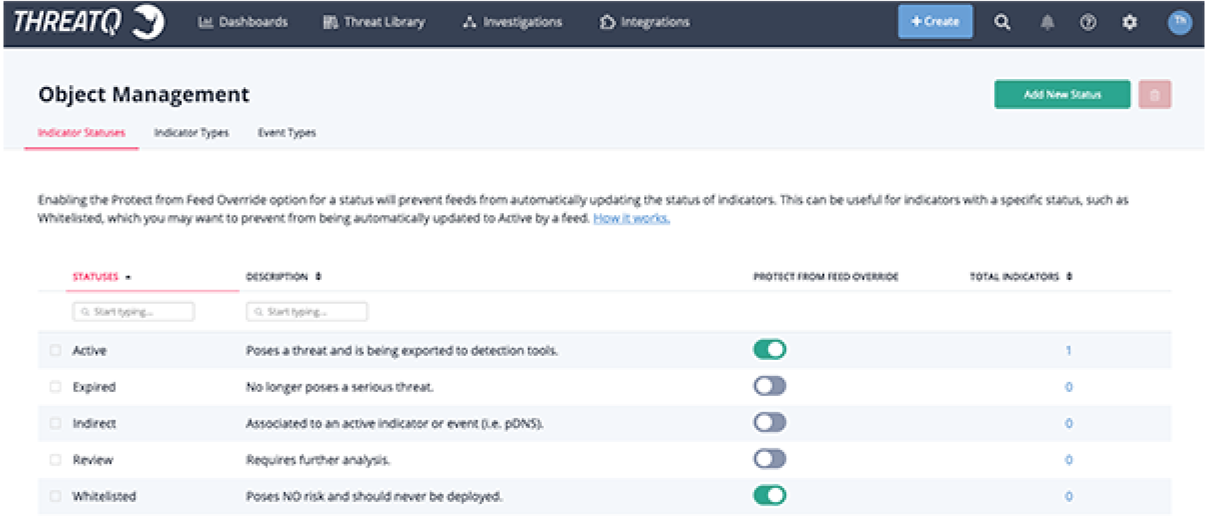
3. Optionally, enter a new **Status Name**.
4. Optionally, enter a new **Status Description**.
5. Click **Save Changes**.

Deleting an Indicator Status

⚠ You cannot delete indicator statuses provided by ThreatQ. Custom statuses can only be deleted if there are no indicators using that status.

1. Navigate to Settings ⚙ > Object Management.

The Object Management page opens to the Indicator Statuses tab.



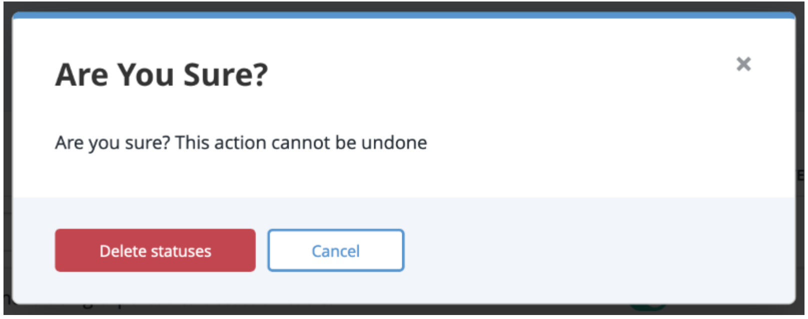
Object Management

Enabling the Protect from Feed Override option for a status 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. How it works.

	STATUSES	DESCRIPTION	PROTECT FROM FEED OVERRIDE	TOTAL INDICATORS
☐	Active	Poses a threat and is being exported to detection tools.	●	1
☐	Expired	No longer poses a serious threat.	○	0
☐	Indirect	Associated to an active indicator or event (i.e. pDNS).	○	0
☐	Review	Requires further analysis.	○	0
☐	Whitelisted	Poses NO risk and should never be deployed.	●	0

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.



Are You Sure?

Are you sure? This action cannot be undone

4. Click **Delete Statuses**.

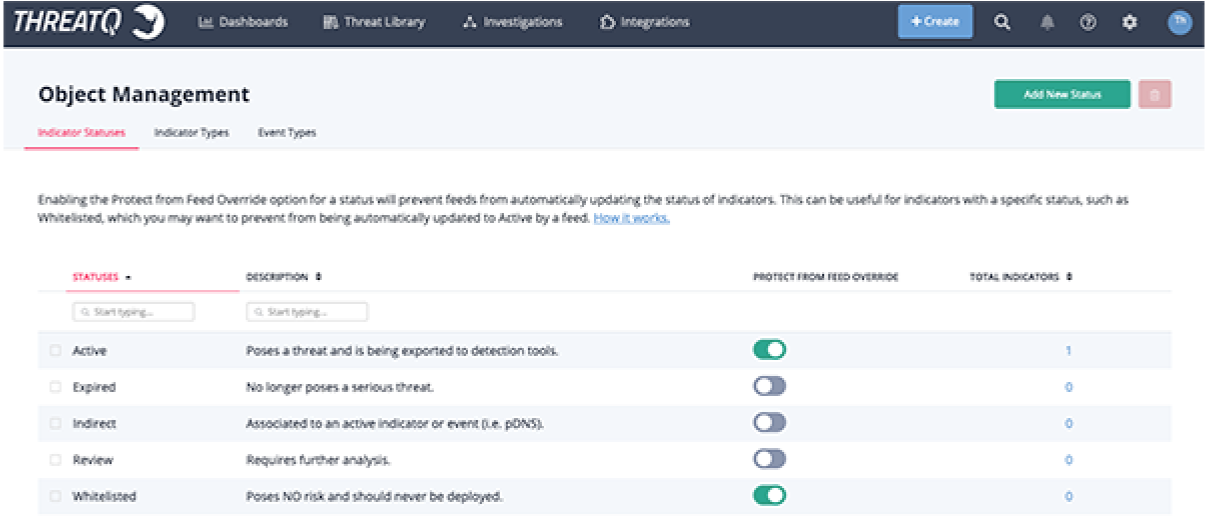
Indicator Types

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 ⚙ > Object Management.

   The Object Management page opens.

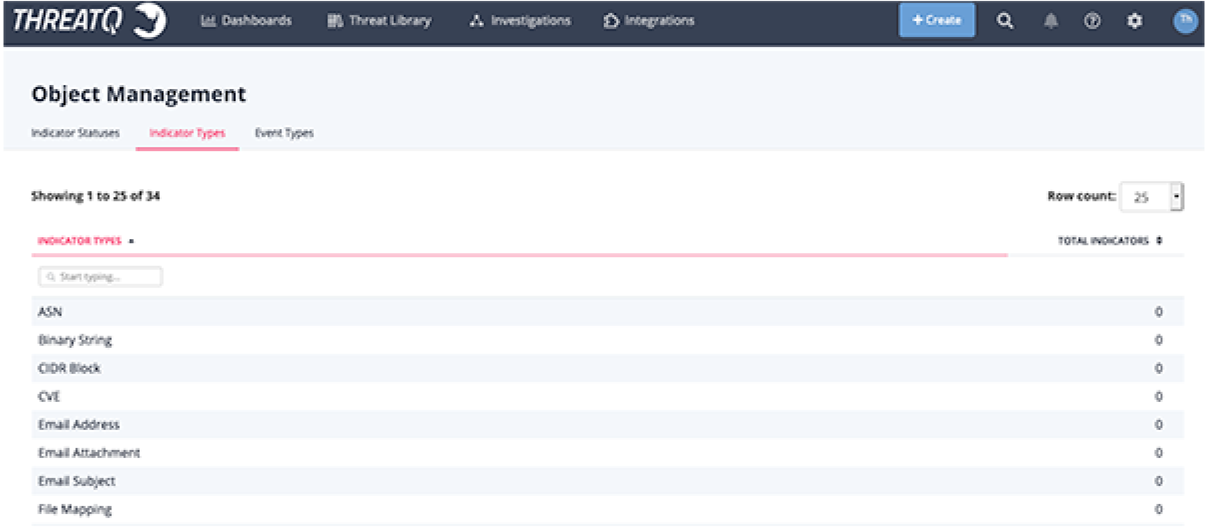


Enabling the Protect from Feed Override option for a status will prevent feeds from automatically updating the status of indicators. This can be useful for indicators with a specific status, such as Whitelisted, which you may want to prevent from being automatically updated to Active by a feed. How it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

	STATUSES	DESCRIPTION	PROTECT FROM FEED OVERRIDE	TOTAL INDICATORS
☐	Active	Poses a threat and is being exported to detection tools.	●	1
☐	Expired	No longer poses a serious threat.	○	0
☐	Indirect	Associated to an active indicator or event (i.e. pDNS).	○	0
☐	Review	Requires further analysis.	○	0
☐	Whitelisted	Poses NO risk and should never be deployed.	●	0

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

   The Indicator Types tab opens.



Showing 1 to 25 of 34

Row count: 25

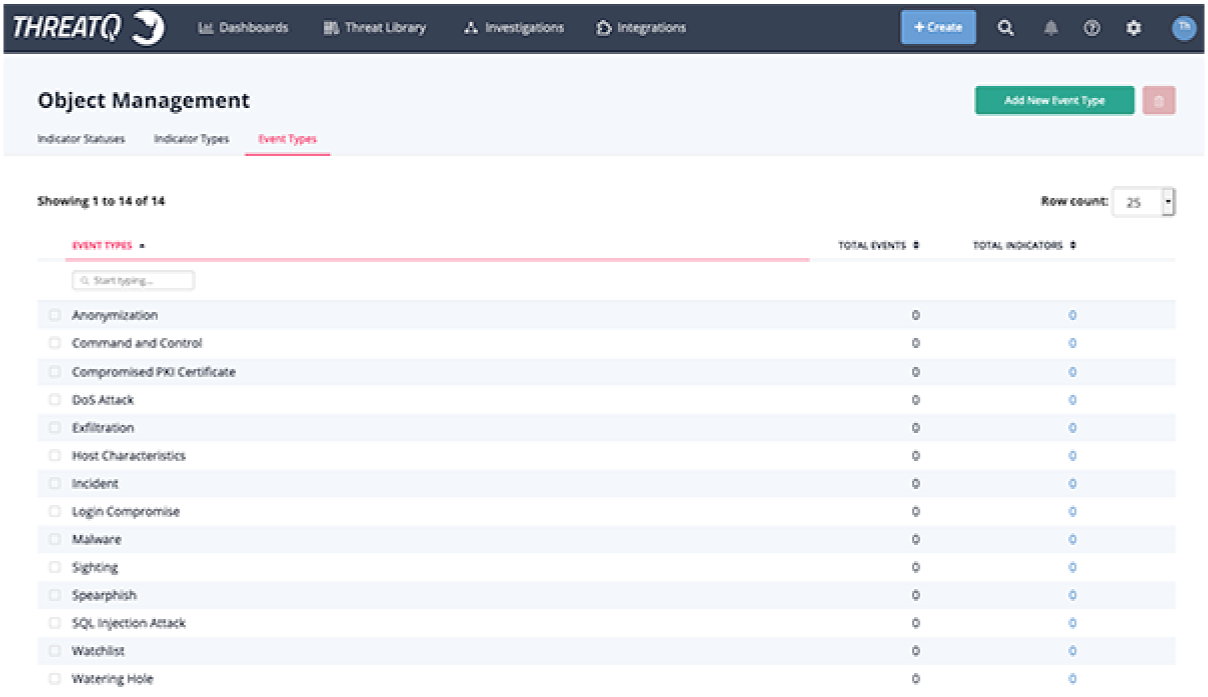
INDICATOR TYPES	TOTAL INDICATORS
ASN	0
Binary String	0
CIDR Block	0
CVE	0
Email Address	0
Email Attachment	0
Email Subject	0
File Mapping	0

Indicator Types Table Functions:

FUNCTION	DESCRIPTION
Changing the number of entries displayed in the table	Click the dropdown menu at the top right of the table and select the desired option.
Filter table by Indicator Type	Enter a keyword in the text field provided to filter the table by indicator type.
Sort table by Total Indicators	Click the Total Indicators column header to sort the table by ascending/descending order.

Event Types

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



Showing 1 to 14 of 14

Row count: 25

EVENT TYPES	TOTAL EVENTS	TOTAL INDICATORS
☐ Anonymization	0	0
☐ Command and Control	0	0
☐ Compromised PKI Certificate	0	0
☐ DoS Attack	0	0
☐ Exfiltration	0	0
☐ Host Characteristics	0	0
☐ Incident	0	0
☐ Login Compromise	0	0
☐ Malware	0	0
☐ Sighting	0	0
☐ Spearphish	0	0
☐ SQL Injection Attack	0	0
☐ Watchlist	0	0
☐ Watering Hole	0	0

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

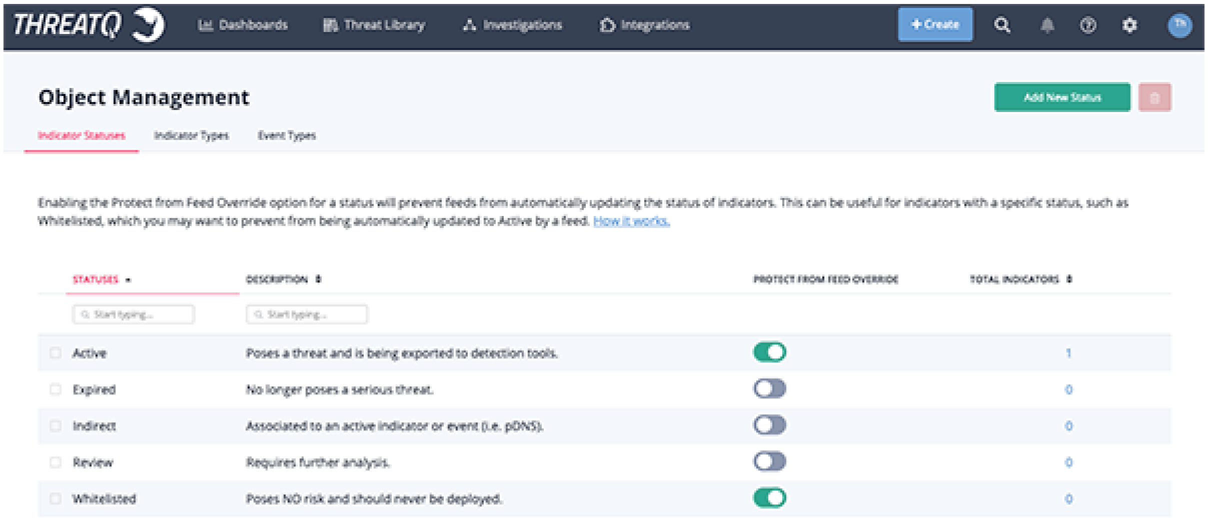
System provided Event Types include:

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

Viewing Event Types

1. Navigate to Settings ⚙ > Object Management.

   The Object Management page opens.



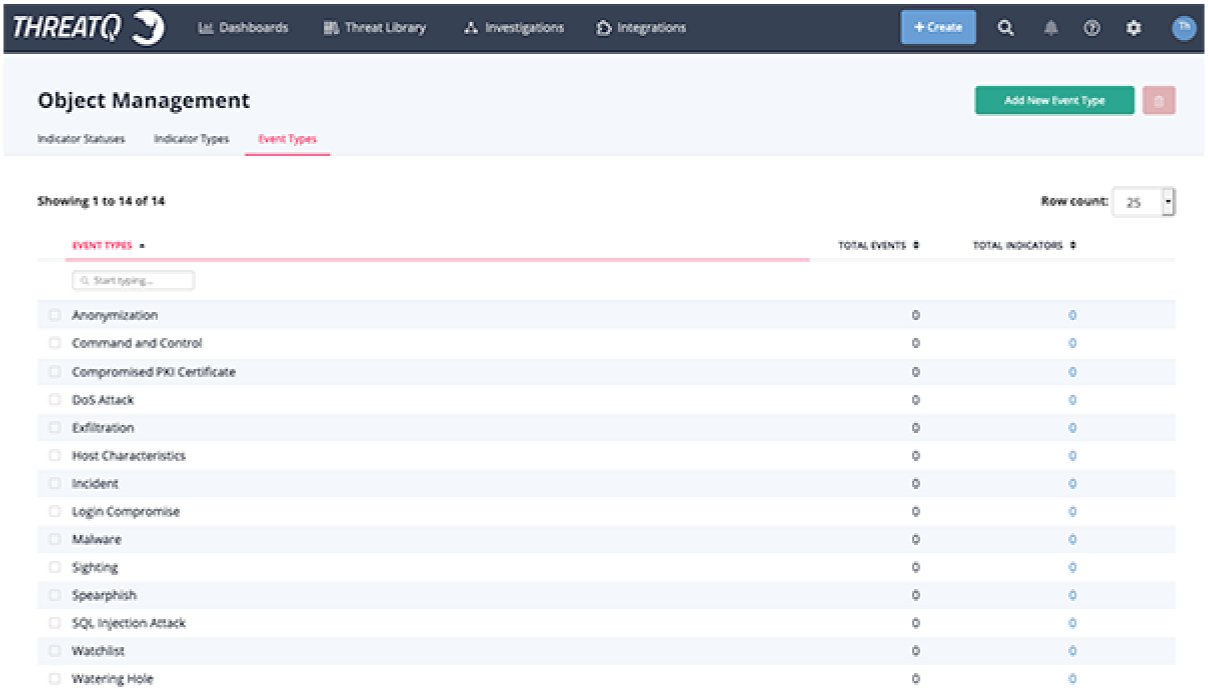
Object Management

Enabling the Protect from Feed Override option for a status 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. How it works.

	STATUSES	DESCRIPTION	PROTECT FROM FEED OVERRIDE	TOTAL INDICATORS
☐	Active	Poses a threat and is being exported to detection tools.	●	1
☐	Expired	No longer poses a serious threat.	○	0
☐	Indirect	Associated to an active indicator or event (i.e. pDNS).	○	0
☐	Review	Requires further analysis.	○	0
☐	Whitelisted	Poses NO risk and should never be deployed.	●	0

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

   The Event Types tab opens.



Object Management

Showing 1 to 14 of 14

Row count: 25

	EVENT TYPES	TOTAL EVENTS	TOTAL INDICATORS
☐	Anonymization	0	0
☐	Command and Control	0	0
☐	Compromised PKI Certificate	0	0
☐	DoS Attack	0	0
☐	Exfiltration	0	0
☐	Host Characteristics	0	0
☐	Incident	0	0
☐	Login Compromise	0	0
☐	Malware	0	0
☐	Sighting	0	0
☐	Spearphish	0	0
☐	SQL Injection Attack	0	0
☐	Watchlist	0	0
☐	Watering Hole	0	0

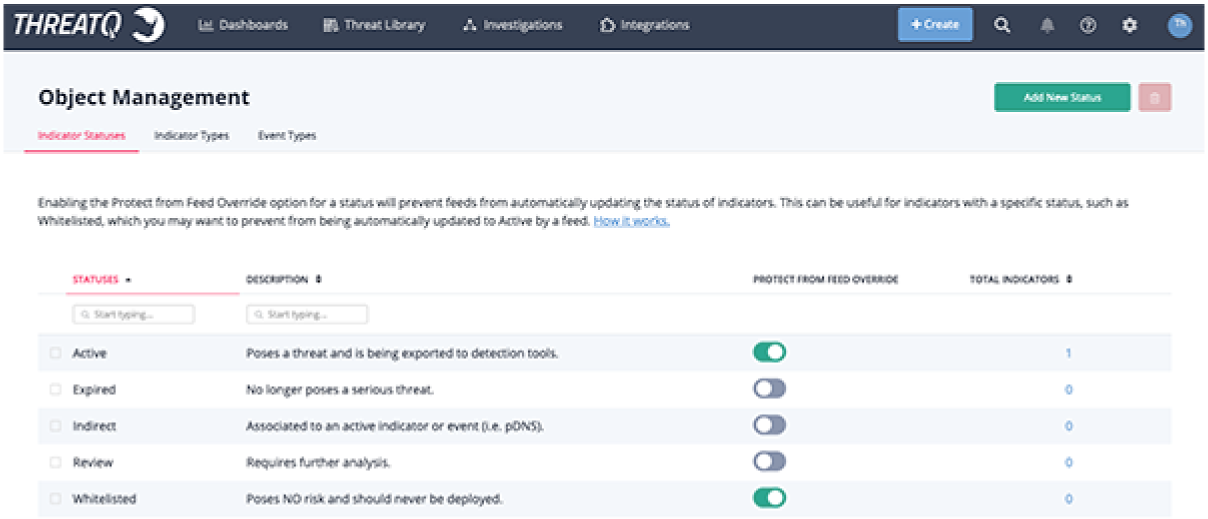
Event Types Table Functions:

FUNCTION	DESCRIPTION
Changing the number of entries displayed in the table	Click the dropdown menu at the top right of the table and select the desired option.
Filter table by Event Type	Enter a keyword in the text field provided to filter the table by event type.
Sort table by Total Events	Click on Total Events column header to sort the table by ascending/descending order.
Sort table by Total Indicators	Click the Total Indicators column header to sort the table by ascending/descending order. Clicking on the value will open the Threat Library filtered to indicators linked to the event type as a related object. User-created Event Types will have an Edit link located to the right of the Total Indicator value. Clicking on the Edit link will open the Edit Event Type dialog box.

Adding an Event Type

1. From the main menu, select Settings ⚙ > Object Management.

The Object Management page opens to the Indicator Statuses tab.

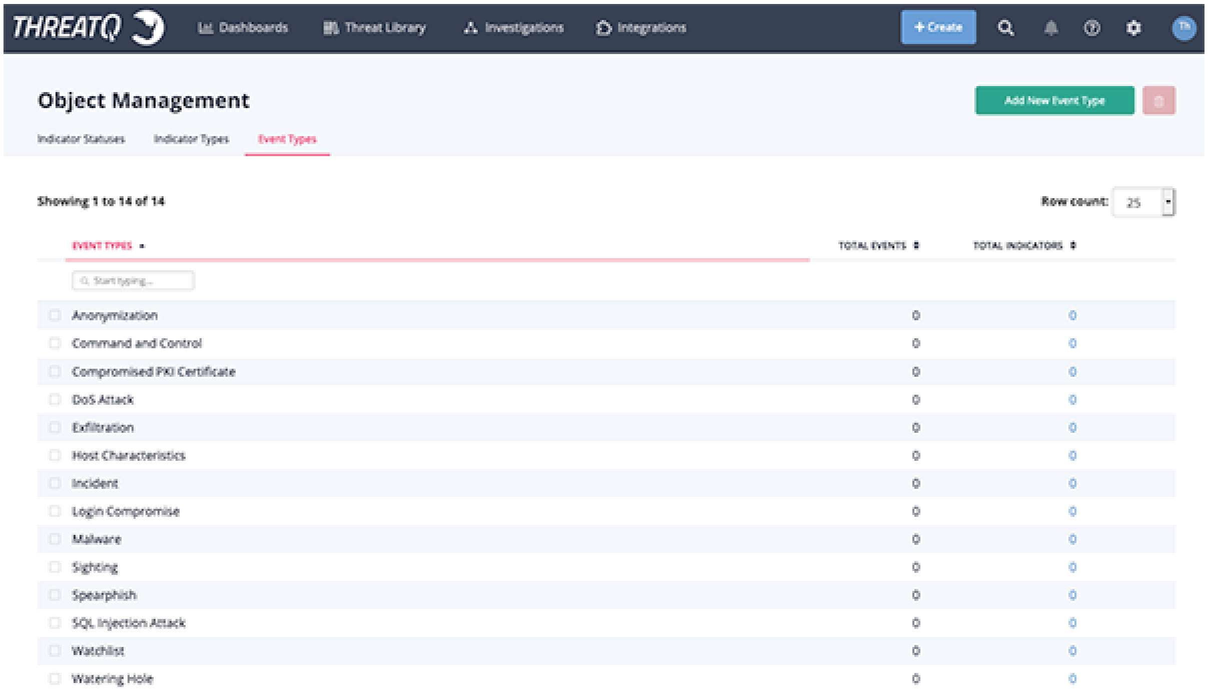


Enabling the Protect from Feed Override option for a status will prevent feeds from automatically updating the status of indicators. This can be useful for indicators with a specific status, such as Whitelisted, which you may want to prevent from being automatically updated to Active by a feed. How it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

STATUSES	DESCRIPTION	PROTECT FROM FEED OVERRIDE	TOTAL INDICATORS
Active	Poses a threat and is being exported to detection tools.	●	1
Expired	No longer poses a serious threat.	○	0
Indirect	Associated to an active indicator or event (i.e. pDNS).	○	0
Review	Requires further analysis.	○	0
Whitelisted	Poses NO risk and should never be deployed.	●	0

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

   The Event Types tab opens.

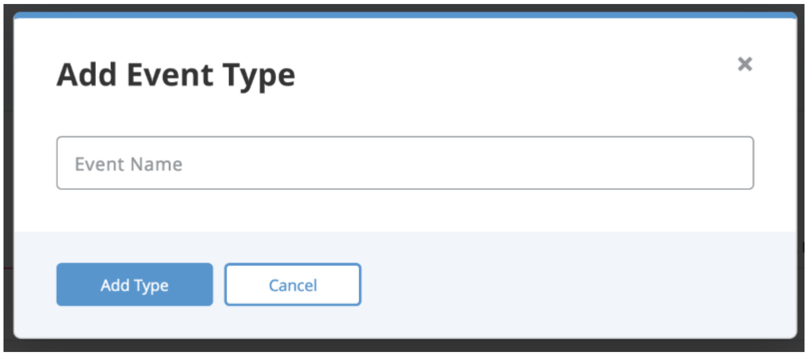


Showing 1 to 14 of 14

EVENT TYPES	TOTAL EVENTS	TOTAL INDICATORS
Anonymization	0	0
Command and Control	0	0
Compromised PKI Certificate	0	0
DoS Attack	0	0
Exfiltration	0	0
Host Characteristics	0	0
Incident	0	0
Login Compromise	0	0
Malware	0	0
Sighting	0	0
Spearphish	0	0
SQL Injection Attack	0	0
Watchlist	0	0
Watering Hole	0	0

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

The Add Event Type dialog box opens.



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

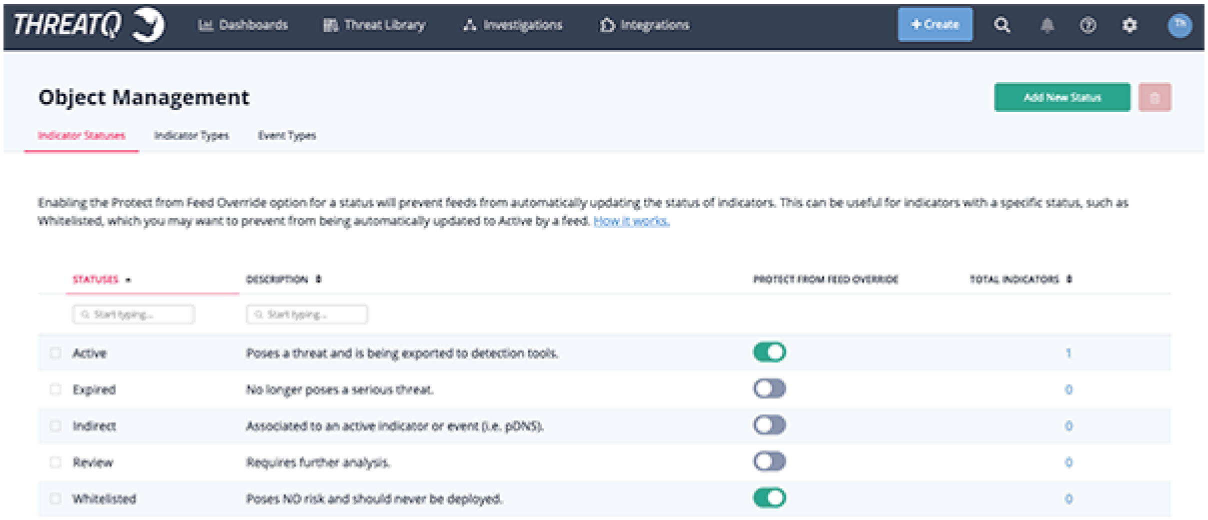
Editing an Event Type

You can edit user-generated event types.

> ⚠ You cannot edit an Event Type provided by ThreatQ.

1. Navigate to Settings ⚙ > Object Management.

   The Object Management page opens to the Indicator Statuses tab.

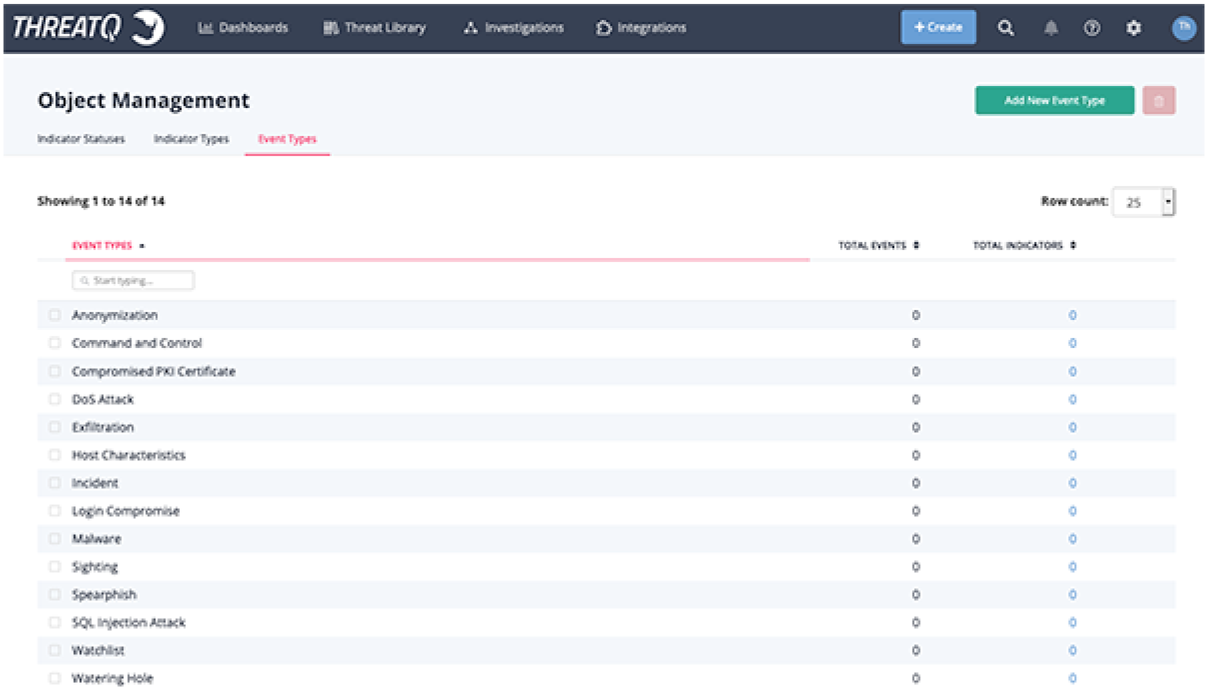


Enabling the Protect from Feed Override option for a status will prevent feeds from automatically updating the status of indicators. This can be useful for indicators with a specific status, such as Whitelisted, which you may want to prevent from being automatically updated to Active by a feed. How it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

	STATUSES	DESCRIPTION	PROTECT FROM FEED OVERRIDE	TOTAL INDICATORS
☐	Active	Poses a threat and is being exported to detection tools.	●	1
☐	Expired	No longer poses a serious threat.	○	0
☐	Indirect	Associated to an active indicator or event (i.e. pDNS).	○	0
☐	Review	Requires further analysis.	○	0
☐	Whitelisted	Poses NO risk and should never be deployed.	●	0

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

The Event Types tab opens.



Object Management

Indicator Statuses · Indicator Types · Event Types

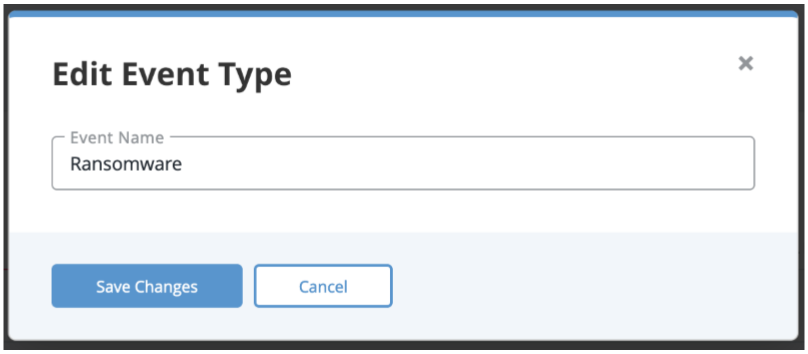
Showing 1 to 14 of 14

Row count: 25

EVENT TYPES	TOTAL EVENTS	TOTAL INDICATORS
☐ Anonymization	0	0
☐ Command and Control	0	0
☐ Compromised PKI Certificate	0	0
☐ DoS Attack	0	0
☐ Exfiltration	0	0
☐ Host Characteristics	0	0
☐ Incident	0	0
☐ Login Compromise	0	0
☐ Malware	0	0
☐ Sighting	0	0
☐ Spearphish	0	0
☐ SQL Injection Attack	0	0
☐ Watchlist	0	0
☐ Watering Hole	0	0

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

   The Edit Event Type dialog box opens.



Edit Event Type

Event Name: Ransomware

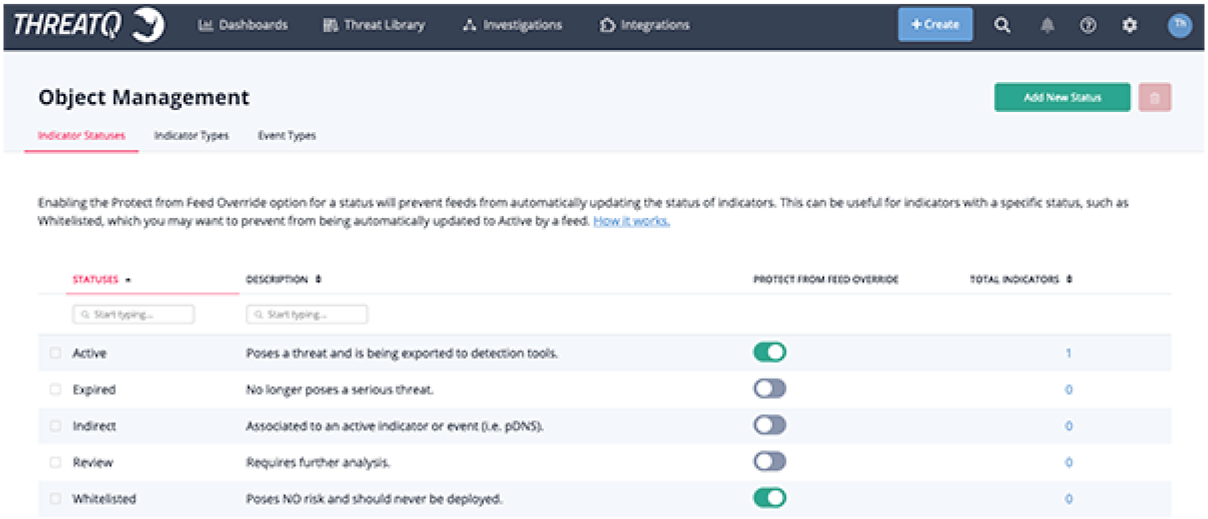
4. Enter a new **Event Name**.
5. Click **Save Changes**.

Deleting an Event Type

⚠ You cannot delete an Event Type provided by ThreatQ. Custom Event Types can only be deleted if there are no events using that event type.

1. Navigate to Settings ⚙ > Object Management.

   The Object Management page opens to the Indicator Statuses tab.

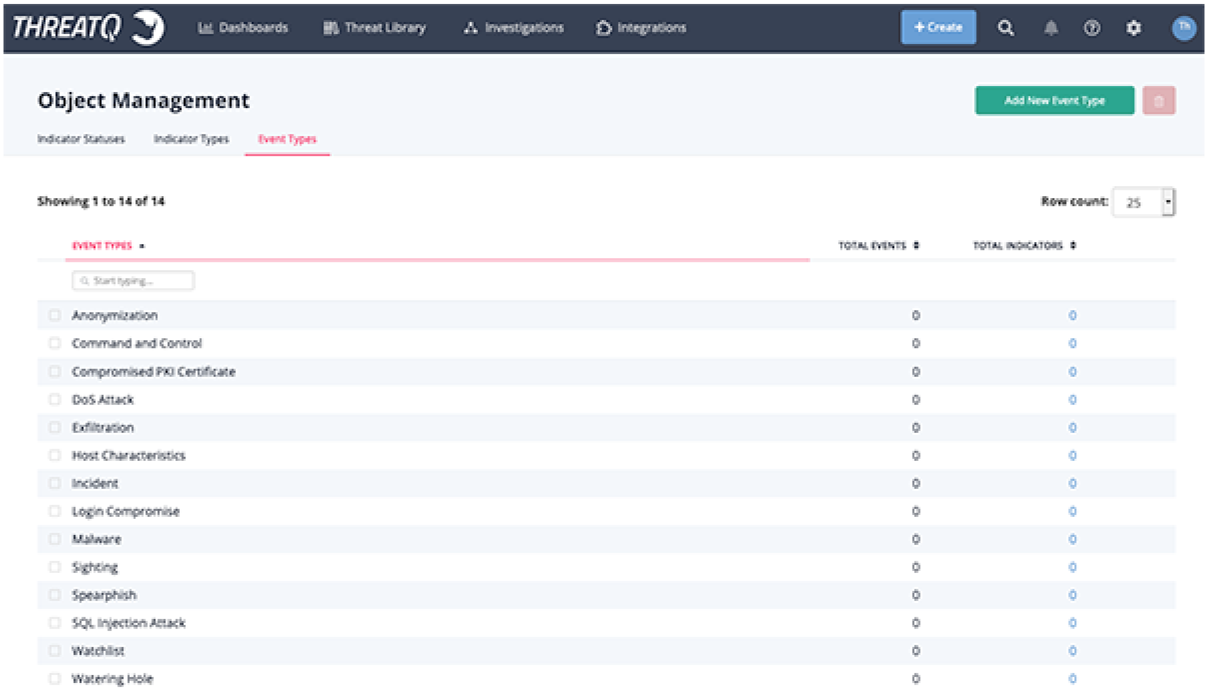


Enabling the Protect from Feed Override option for a status will prevent feeds from automatically updating the status of indicators. This can be useful for indicators with a specific status, such as Whitelisted, which you may want to prevent from being automatically updated to Active by a feed. How it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

	STATUSES	DESCRIPTION	PROTECT FROM FEED OVERRIDE	TOTAL INDICATORS
☐	Active	Poses a threat and is being exported to detection tools.	●	1
☐	Expired	No longer poses a serious threat.	○	0
☐	Indirect	Associated to an active indicator or event (i.e. pDNS).	○	0
☐	Review	Requires further analysis.	○	0
☐	Whitelisted	Poses NO risk and should never be deployed.	●	0

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

   The Event Types tab opens.

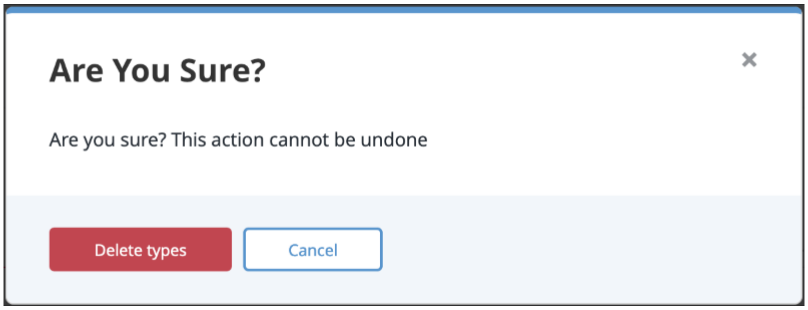


Showing 1 to 14 of 14

	EVENT TYPES	TOTAL EVENTS	TOTAL INDICATORS
☐	Anonymization	0	0
☐	Command and Control	0	0
☐	Compromised PKI Certificate	0	0
☐	DoS Attack	0	0
☐	Exfiltration	0	0
☐	Host Characteristics	0	0
☐	Incident	0	0
☐	Login Compromise	0	0
☐	Malware	0	0
☐	Sighting	0	0
☐	Spearphish	0	0
☐	SQL Injection Attack	0	0
☐	Watchlist	0	0
☐	Watering Hole	0	0

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

A confirmation dialog box appears.



Are You Sure?

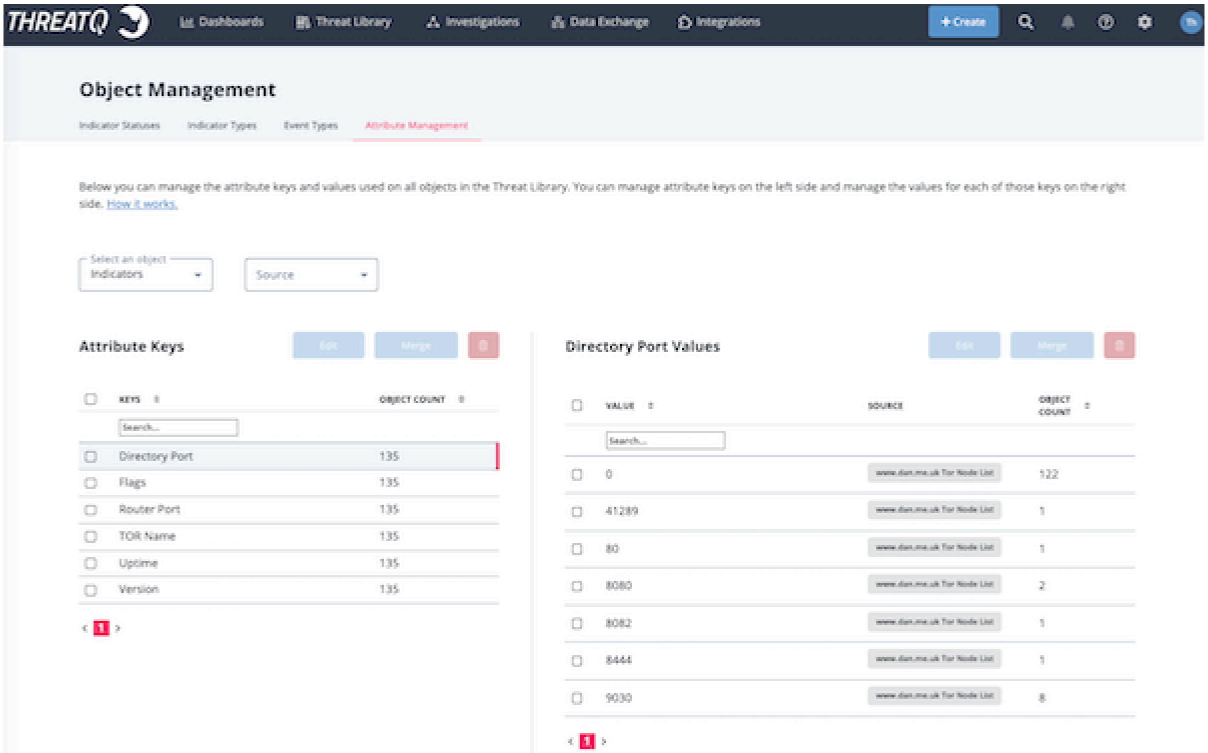
Are you sure? This action cannot be undone

5. Click **Delete Types**.

Attribute Management

The Attribute Management page provides you with an overview of attribute data across the Threat Library and allows you to filter this data by Source. In addition, this page allows you to refine and consolidate your Threat Library by editing, merging, and deleting attribute keys and values associated with system objects.

⚠ When you edit, merge, or delete an attribute key or value, it may take up to one minute for your changes to be reflected in the Attribute Management page and/or Threat Library.



Below you can manage the attribute keys and values used on all objects in the Threat Library. You can manage attribute keys on the left side and manage the values for each of those keys on the right side. How it works.

☐	KEYS	OBJECT COUNT
☐	Directory Port	135
☐	Flags	135
☐	Router Port	135
☐	TOR Name	135
☐	Uptime	135
☐	Version	135

☐	VALUE	SOURCE	OBJECT COUNT
☐	0	www.dan.me.uk Tor Node List	122
☐	41289	www.dan.me.uk Tor Node List	1
☐	80	www.dan.me.uk Tor Node List	1
☐	8080	www.dan.me.uk Tor Node List	2
☐	8082	www.dan.me.uk Tor Node List	1
☐	8444	www.dan.me.uk Tor Node List	1
☐	9030	www.dan.me.uk Tor Node List	8

Examples:

- If you have two attribute keys, "Country" and "Cuontry", you can use the merge attribute key option to merge both attributes and their associated values into an attribute key of "Country".
- If your Country attribute key contains values of "US", "U.S.", and "America", you can merge all of these into an attribute value of "US".

Selecting an Attribute Key or Value

To make it easier to locate the attribute you want to update, the Attribute Management page allows you to filter your view by object type, source, attribute key, and attribute value.

> Click the up/down arrows next to a column name to sort a list in ascending/descending order.

> Click the left/right arrows and page numbers below the attribute keys or values lists to view additional list items.

> Use the Rows per page field to select the number of attribute keys or values displayed on each page.

1. By default, the Attribute Management page lists indicator attributes. To select another object type, click the **Select an object** field and use one of the following methods to specify the object type:
    - Select the object type from the dropdown list.
    - Begin typing the object type and click it when it is displayed below the field.
2. To filter the attributes listed by source, click the **Source** field and use one of the following methods to specify the object source:
    - Select the source from the dropdown list.
    - Begin typing the source and click it when it is displayed below the field.
3. Repeat step 2 to select additional sources.
   Each time you select a source, it is displayed to the right of the Source field. You can remove a source by clicking the X to the right of the source name.
4. From the Attribute Keys list, use one of the following methods to locate the attribute type you want to work with: The values for this attribute are displayed to the right of the Attribute Keys list.
    - Browse the list of attribute keys and click the attribute key.
    - Begin typing the attribute key in the Search box and click it when it is displayed below the field.
5. From the attribute values list, use one of the following methods to locate the value you want to work with: The values for this attribute are displayed to the right of the Attribute Keys list.
    - Browse the list of attribute values and click the attribute key.

- Begin typing the attribute value in the Search box and click it when it is displayed below the field.

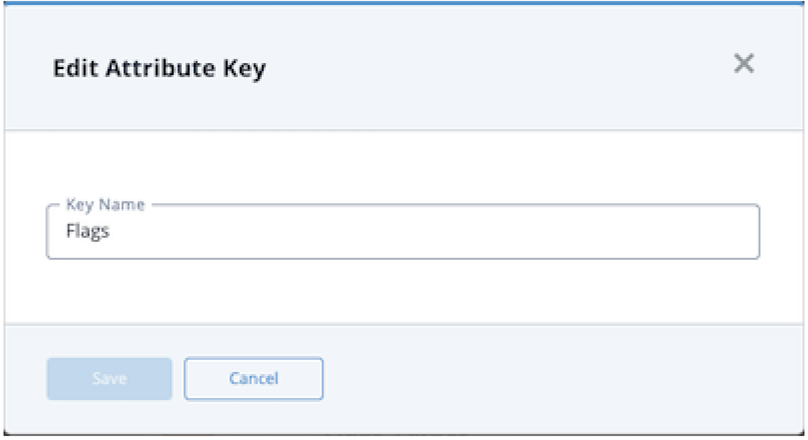
> You can click on an attribute's object count to access the corresponding Threat Library object(s).

Editing Attribute Keys

1. From the Attribute Keys list, click the checkbox next to the attribute type you want to edit.

> You can only edit one attribute type at a time. If you select more than one attribute type, the Edit button is inactive.

2. Click the Edit button.
   The Edit Attribute Key window is displayed.



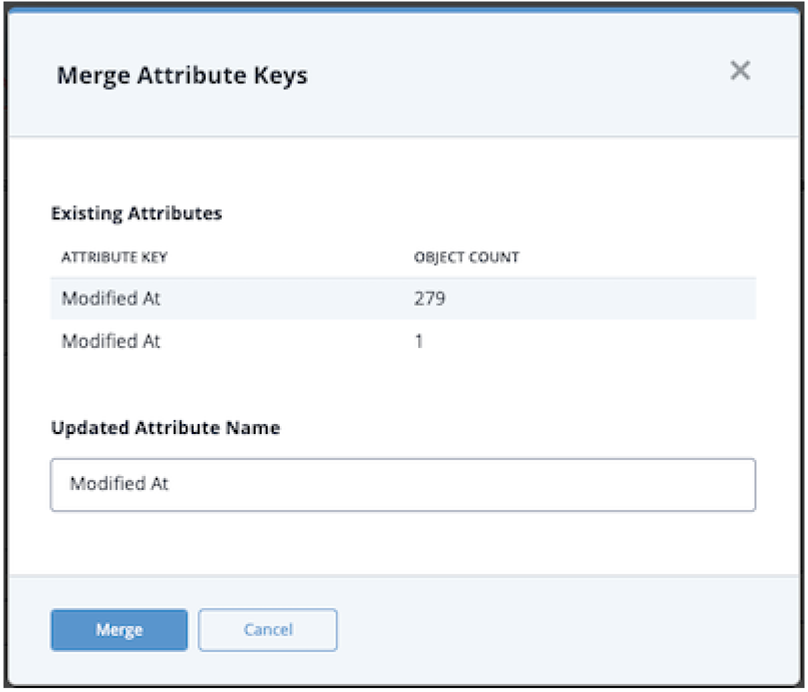
Key Name: Flags

3. Enter your changes to the attribute key.
4. Click the Save button.

Merging Attribute Keys

1. From the Attribute Keys list, click the checkbox next to the attribute types you want to merge.

2. Click the Merge button.
   The Merge Attribute Keys window is displayed.



Merge Attribute Keys

Existing Attributes

ATTRIBUTE KEY	OBJECT COUNT
Modified At	279
Modified At	1

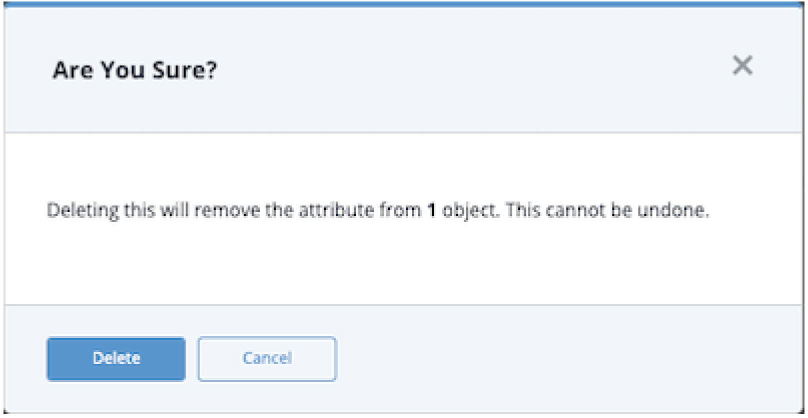
Updated Attribute Name

Modified At

3. If desired, enter a new attribute name for the merged attributes.
4. Click the Merge button.

Deleting Attribute Keys

1. From the Attribute Keys list, click the checkbox next to the attribute(s) you want to delete.
2. Click the trash can button.
3. The **Are You Sure?** window prompts you to confirm the deletion.



Are You Sure?

Deleting this will remove the attribute from **1** object. This cannot be undone.

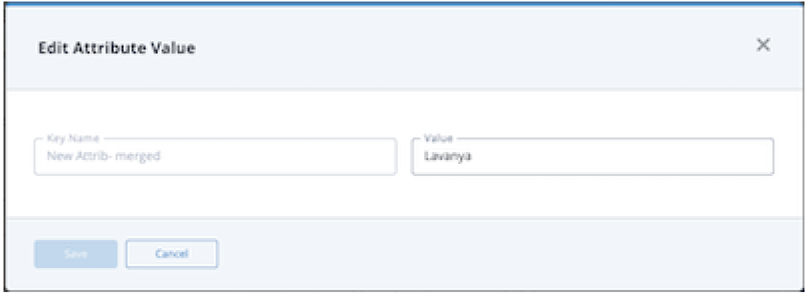
4. Click the Delete button.

Editing Attribute Values

1. From the attribute values list, click the checkbox next to the attribute value you want to edit.

   > You can only edit one attribute value at a time. If you select more than one attribute value, the Edit button is inactive.

2. Click the Edit button.
   The Edit Attribute Value window is displayed.



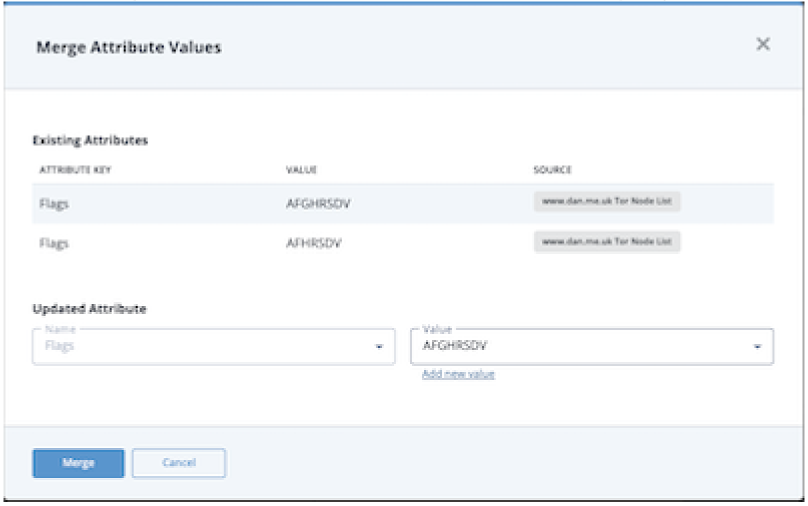
Key Name: New Attrib- merged

Value: Lavanya

3. Enter your changes to the attribute value.
4. Click the Save button.

Merging Attribute Values

1. From the attribute values list, click the checkbox next to the attribute values you want to merge.
2. Click the Merge button.
   The Merge Attribute Values window is displayed.



Existing Attributes

ATTRIBUTE KEY	VALUE	SOURCE
Flags	AFGHRSDV	www.dan.me.uk Tor Node List
Flags	AFHRSDV	www.dan.me.uk Tor Node List

Updated Attribute

Name: Flags

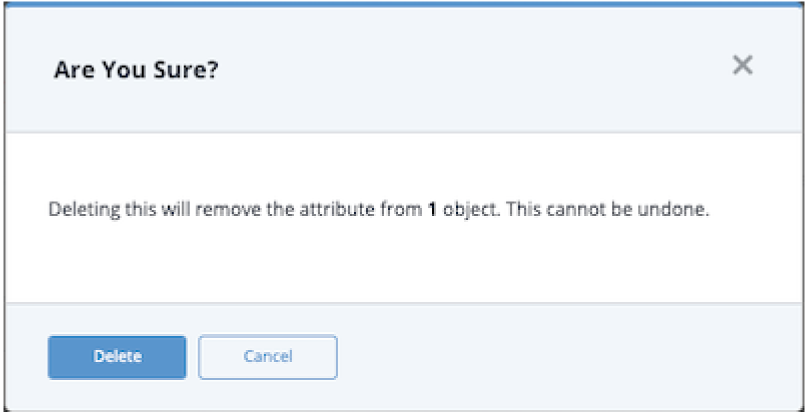
Value: AFGHRSDV

3. To specify a new attribute value name for the merged values , use one of the following methods:

    - Click the Value field and use the **Search for attribute values** field to locate an existing value.
    - Click the Add new value link and enter the new value in the **Type new value** field.
4. Click the Merge button.

Deleting Attribute Values

1. From the attribute values list, click the checkbox next to the attribute value(s) you want to delete.
2. Click the trash can button.
3. The **Are You Sure?** window prompts you to confirm the deletion.


Are You Sure?

Deleting this will remove the attribute from 1 object. This cannot be undone.

4. Click the Delete button.

Reports

You can export a PDF Summary of an object from an object's details page. Images in an object's description are displayed in the PDF report for the object as left aligned regardless of the alignment you select in the Description pane.

Generating Reports

Complete the following steps to export a PDF Summary of an object from an object's details page.

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

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**.

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 the Report Header

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

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.

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**.

Previewing Report Customization

You can preview report customization to view a representation of a report's output.

1. Select the **Settings** icon > **Report Options**.
2. Under Customized PDF Reports, click **Preview**.

   The sample report downloads to your computer.

Server Administration

The Server Administration dropdown link is only accessible to users with Administrative and Maintenance Accounts. Clicking on this option, found under the Settings, will open the **ThreatQ Monitoring Platform** in a new tab/window.

ThreatQ Monitoring Platform

> The Server Administration dropdown link is only accessible to users with **Administrative** and **Maintenance** roles.

The ThreatQ Monitoring Platform provides a way for users with Administrative and Maintenance roles to monitor system resources and logs.

This feature is built upon Cockpit, a web-based interface that allows you to view the health of your server, system resources, as well as adjust configurations. You can access the full documentation on its operations at:

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html-single/getting_started_with_cockpit/index#using_cockpit

Creating a User Account for the ThreatQ Monitoring Platform

Since you cannot use a root user account to access the Server Administration console, you may need to use the Command Line Interface (CLI) to create a second non-root user account for access. Depending on your business processes, you may decide to assign ThreatQ user accounts to a specific group. However, you are not required to do so.

1. **Optional Step. You do not have to create a group for non-root users.** However, you can create one by entering the following command::

   ```
   groupadd <groupname>
   ```

   > groupadd cockpit

2. Use one of the following methods to create a user:

- Create a user as a part of a group:

  ```
  adduser -G <groupname> <username>
  ```

  ```
  adduser -G cockpit testUser
  ```

- Create a user not assigned to a group:

  ```
  adduser <username>
  ```

  ```
  adduser testUser
  ```

3. Enter the following command to create a password for the user:

   ```
   passwd <username>
   ```

   ```
   passwd testUser
   Changing password for user testUser.
   New password:
   Retype new password:
   passwd: all authentication tokens updated successfully.
   ```

4. **Optional Step.** Enter the following command to create an admin user by adding the user account to the wheel group:

   ```
   adduser -G wheel <username>
   ```

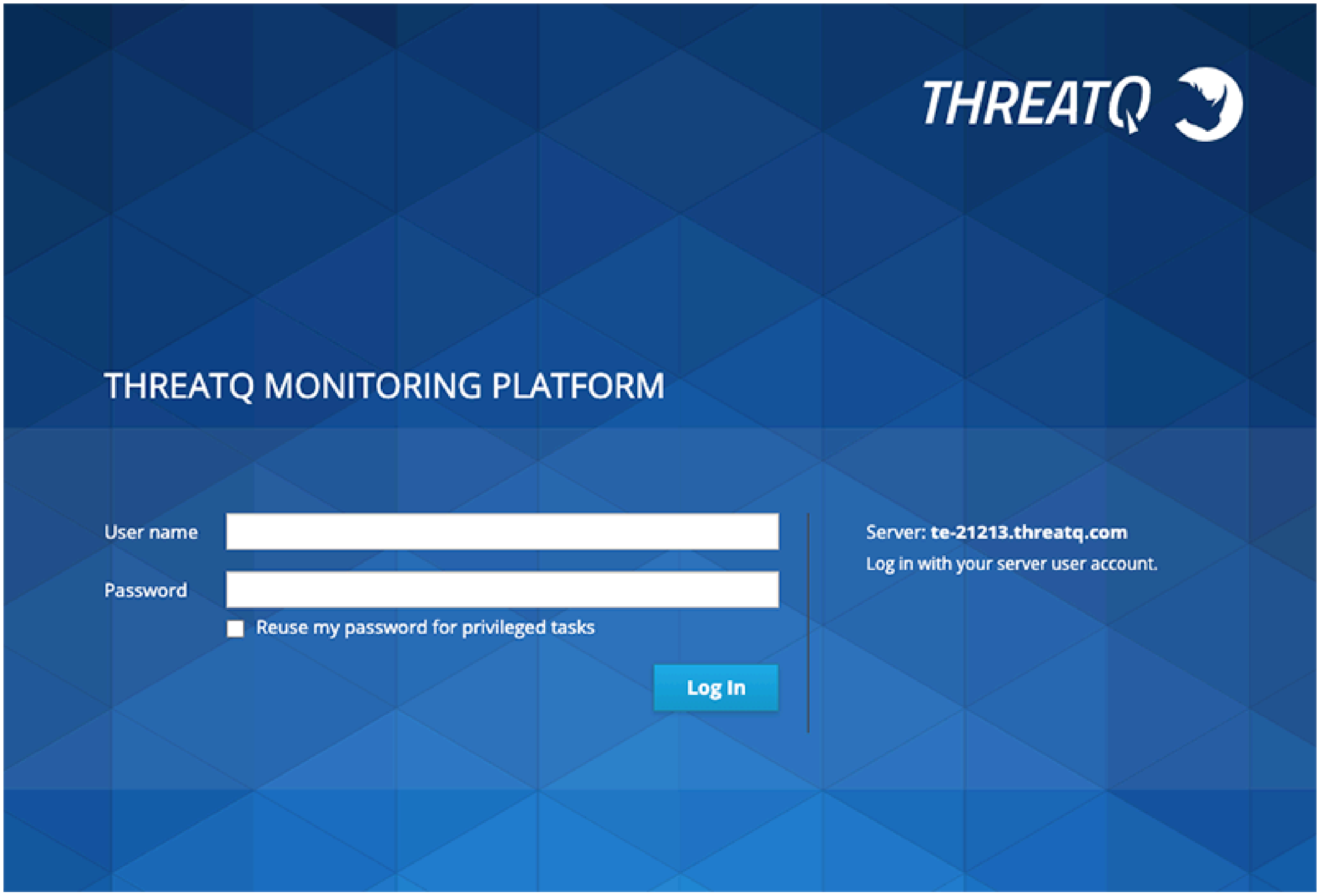
5. Use the new user account to log into the server administrator console.

Accessing the ThreatQ Monitoring Platform

> ⚠ Root user access is disabled for the ThreatQ Monitoring Platform.

1. Navigate to **Settings** ⚙ > **Server Administration**.

The ThreatQ Monitor Platform will load in a new tab/window.



THREATQ MONITORING PLATFORM

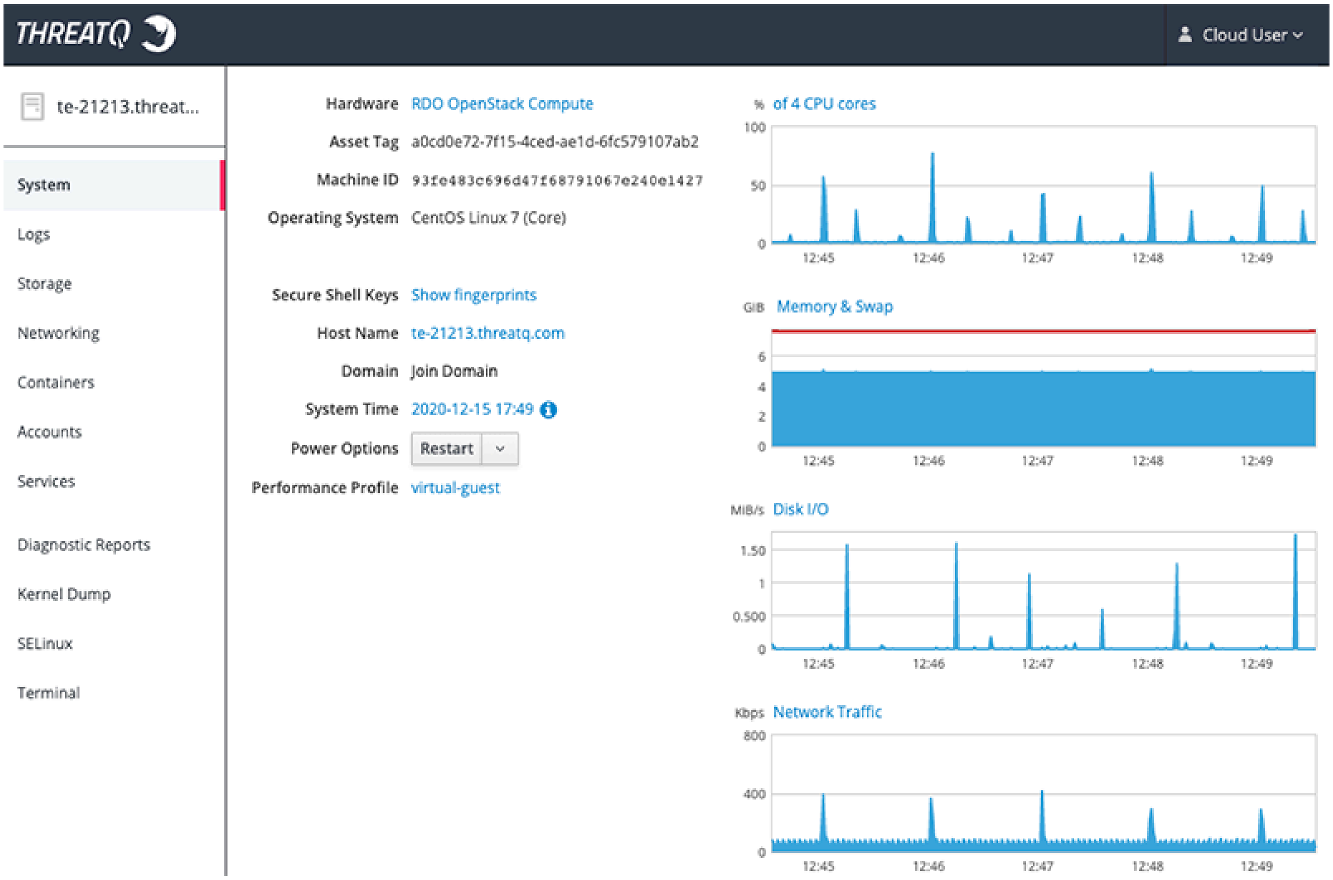
Server: **te-21213.threatq.com**

Log in with your server user account.

2. Log into the platform using your user server credentials.

> These credentials are not the same credentials that you use to log into the ThreatQ UI.

3. You will now be logged into the ThreatQ Monitoring Platform.



Hardware RDO OpenStack Compute
Asset Tag a0cd0e72-7f15-4ced-ae1d-6fc579107ab2
Machine ID 93fe483c696d47f68791067e240e1427
Operating System CentOS Linux 7 (Core)

Secure Shell Keys Show fingerprints
Host Name te-21213.threatq.com
Domain Join Domain
System Time 2020-12-15 17:49
Power Options Restart
Performance Profile virtual-guest

Sharing

ThreatQ's sharing functionality allows you to control access to data collections, dashboards, and investigations at the user level or give view-only access to all users. You can assign permissions when you create a data collection, dashboard, or investigation and then update them at any time.

User Permission Levels

You can assign each user one of the following permission levels:

PERMISSION LEVEL	DESCRIPTION
Owner	By default, the user who creates a data collection, dashboard, or investigation is designated as the owner. However, ownership can be reassigned by the owner at any time. If an owner selects a new owner, the original owner becomes an editor. In addition, if you delete an owner's user record, the system requires you to either reassign ownership to another user or delete the owner's data collections, dashboards, and investigations. Users with owner-level permission can: • Reassign ownership. • Change user and group permissions for the data collection, dashboard, or investigation. • Remove a user's permissions. • Modify or delete the data collection, dashboard, or investigation. • Change the name of the data collection, dashboard, or investigation. • Pin an investigation to the Investigations menu.
Editor	Editors have similar permissions to owners but cannot re-assign ownership of or delete the data collection, dashboard, or

	investigation. In addition, they cannot change owner permissions. Users with editor-level permissions can: • Change or remove user and group permission-levels for the shared data collection, dashboard, or investigation. • Modify the data collection, dashboard, or investigation. • Pin an investigation to the Investigations menu.
Viewer	Viewers can access the data collection, dashboard, or investigation but cannot change it. In addition, they can view user permissions for data collections and investigations.
Private	If a user creates a data collection, dashboard, or investigation and does not assign permissions to a user or group, only that user (now the owner) can access it.

User Permission Levels and User Roles

A user can assign any permission level to user accounts with the following user roles:

- Maintenance Account
- Administrative Access
- Primary Contributor Access

However, the only permission level a user can assign to a Read Only Access user account is viewer permission.

> ⚠ Ownership and public viewing permissions are applied to all data collections created before upgrading to version 4.54. Any data collections created by custom integrations (instead of Threat Library) are assigned ownership permissions for the custom integration client, but are not shareable. If you want to manage a data collection used by a custom integration in Threat Library in the future, you must first create it in Threat Library and then reference it in the custom integration.

View-Only Permissions for All Users

ThreatQ allows you to assign view-only permissions to all users. To do this, select a permission-level of **Everybody (Public)**. This assigns viewer permissions to all users unless they are assigned user-level permissions that are greater. For example, if I have editor permissions for the Adversary Hunt data collection and the other users have viewer permissions, when Bella (the owner) grants **Everybody (Public)** permissions, I retain my editor permissions. Each individual viewer is now grouped together as **Everybody (Public)** and no longer listed individually in the Sharing modal's **Who has access** list.

Sharing Notifications

The ThreatQ Notification Center alerts you about data collection, dashboard, or investigation permission changes that affect you. As such, you receive a notification when:

- A user shares a data collection, dashboard, or investigation with you.
- A user changes your permissions to owner, editor, or viewer.
- A data collection, dashboard, or investigation you own has been shared with another user.
- Your permissions to a data collection, dashboard, or investigation have been removed.
- A user requests access to an investigation you own.

See the Sharing Notifications topic for more details.

Permission Conversion

When you upgrade to version 4.54, ThreatQ updates your existing permissions as follows:

- **Data Collections** - For an existing data collection, the creator is automatically assigned owner permissions. All other users are assigned **Everybody (Public)** permissions.
- **Dashboards** - All users are assigned viewer permissions for ThreatQ's default dashboards and these permissions cannot be changed. All other user-created dashboards are assigned permissions based on the previous permission model. Dashboard creators have owner permissions. If a dashboard was shared with a user, the user retains the previously granted editor or viewer permissions.
- **Investigations** - Maintenance Account, Administrative Access, and Primary Contributor Access users are given editor permissions for all existing investigations that have a Visibility of Shared. Read Only Access users receive viewer permissions.

If a user that created a data collection, dashboard, or investigation was deleted prior to your upgrade to 4.54/4.55, the corresponding object is assigned to the most recently created admin or super user.

Permission Levels and Integrations

User-managed integrations use data collections created and maintained in the Threat Library. As such, user and group permission levels control access to these data collections.

Client-managed integrations are managed through the API. As such, user and group permissions do not control a client's ability to view, add, update or delete these data collections.

Legacy, Client-Managed Data Collections

For existing, client-managed data collections, the user who created it is assigned owner-level permissions. All other users are assigned view-only access through **Everybody (Public)** group permissions.

Client-Managed Integrations

Through the API, clients have full access to all data collections (view, add, update, and delete). As a result, the new permission levels (owner, editor, viewer) only apply when authenticating with username and password credentials (for example, as a user accessing the user interface) as opposed to authenticating with client credentials.

Legacy, User-Managed Data Collections

For each existing saved data collection, the user who created it has owner-level permissions. All other users have view access through the **Everybody (Public)** group permission.

Air Gapped Data Sync (AGDS) and Investigation Sharing

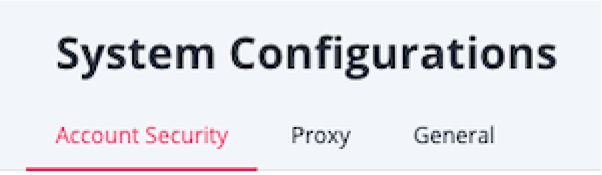
The AGDS export process does not include data collections or dashboards, but it can include investigations if the following command is included and set to Y:

```
--include-investigations=Y
```

See the Air Gapped Data Sync (AGDS) section for more information.

System Configuration

The System Configurations page consists of the Proxy, Account Security, and General Settings tabs. These tabs allow you to enable, disable, and update multiple system-level settings. When you access the System Configurations page, the Account Security tab is displayed by default.



TAB	DESCRIPTION
Proxy	Enable and disable proxy settings.
Account Security	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.
General Settings	Configure the system display mode, date and time format, and indicator parsing checkbox defaults as well as enable/disable the sharing of analytics data with ThreatQuotient.

Proxy

The Proxy configuration page allows you to enable or disable proxies.

> ⚠ Users are required to set their proxy server settings to use http: for their https: traffic.

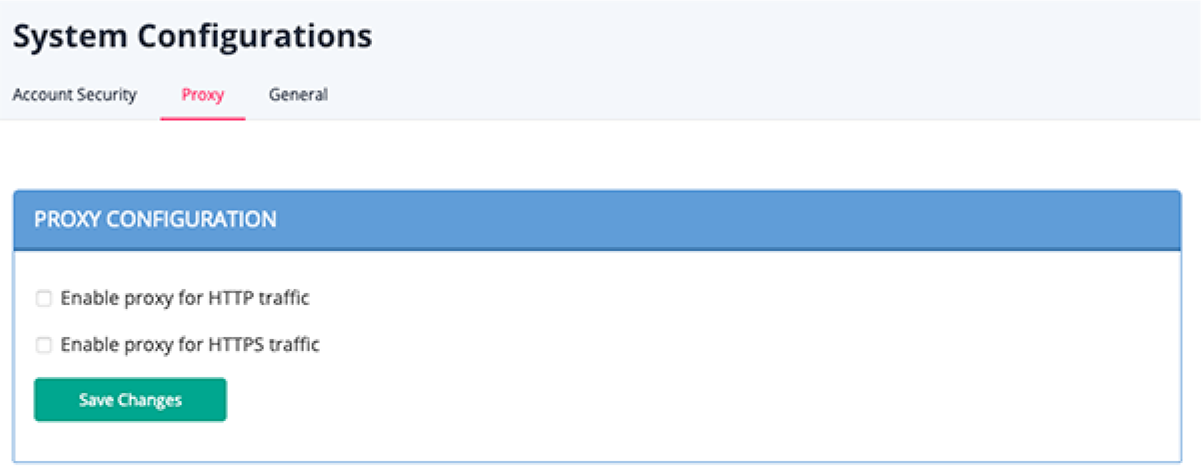
Accessing Proxy Configuration

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

   The System Configurations page opens to the Account Security tab selected by default.

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.

FUNCTION	DESCRIPTION
Disabling a proxy for HTTP or HTTPS traffic	1. Uncheck the proxy you wish to disable, and click **Save Changes**.

Account Security

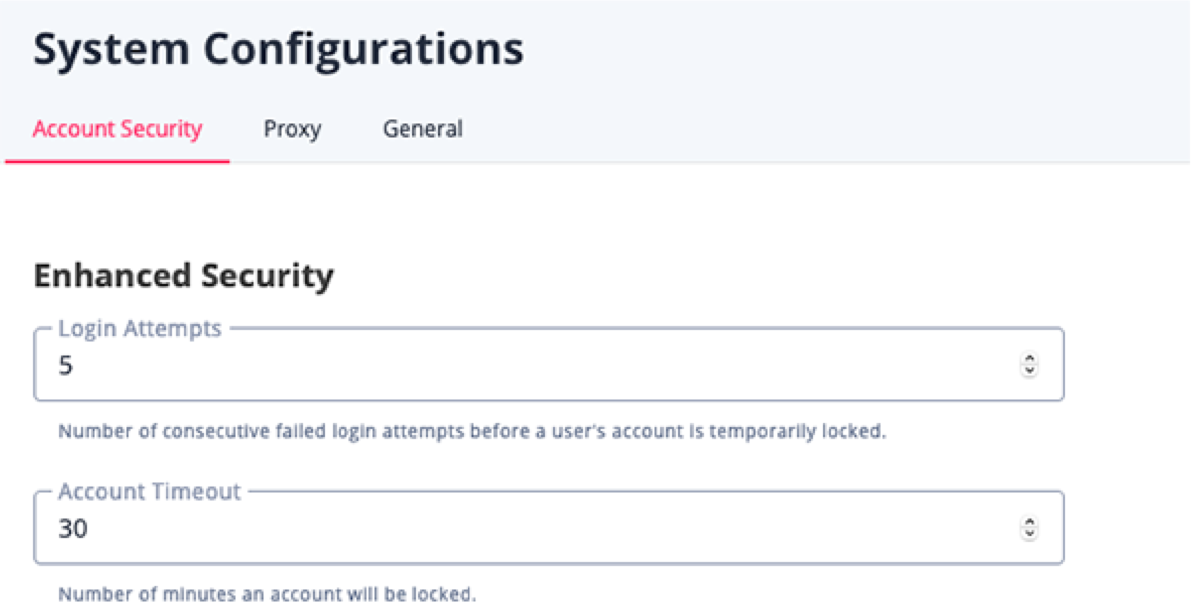
The System Configuration: Account Security tab allows you to configure user lock out settings as well as the display of a custom login banner.

User Lockout Settings

The **Enhanced Security** section of the Account Security tab allows you to specify the number of failed login attempts before a user is locked out and the number of minutes a user will be locked out before he can attempt to log in again. By default, failed login attempts are set to five and the timeout period is set to thirty minutes.

Configuring User Lockout Settings

1. Navigate to Settings ⚙ > System Configurations.
   The System Configuration page loads with the Account Security tab selected by default.



System Configurations

Enhanced Security

Login Attempts: 5

Number of consecutive failed login attempts before a user's account is temporarily locked.

Account Timeout: 30

Number of minutes an account will be locked.

3. Enter your changes to the following fields:

FUNCTION	DESCRIPTION
Login Attempts	The number of consecutive failed login attempts before a user's account is temporarily locked.

Account Timeout	The number of minutes an account is locked after the specified number of failed log in attempts.

4. Click the Save button to save your changes.

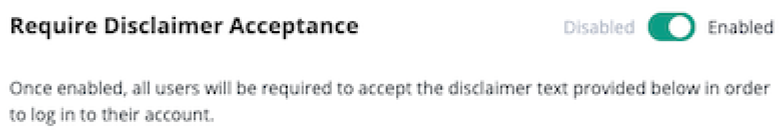
Custom Login Banner

The Require Disclaimer Acceptance section of the **Account Security** tab allows system administrators to enable a custom message displayed to all users when logging into the ThreatQ Platform. When enabled, ThreatQ users are required to review and accept the message.

> In order to comply with government regulations, a customer could configure a custom banner to display a message during login requiring users to accept additional privacy and security terms.

Banner Behavior

The **Require Disclaimer Acceptance** toggle allows you to enable/disable the display of the custom banner.



Once enabled, all users will be required to accept the disclaimer text provided below in order to log in to their account.

When the toggle is disabled:

- The banner title and body are visible to administrators in the **Account Security** tab, but the banner is not displayed to users upon log in.
- Users can access to the platform using only their credentials

When the toggle is enabled:

- After a user enters their login and password, the custom banner displays. Users must click the **Accept and Continue** button to access the platform.
- If a user closes the banner without clicking the **Accept and Continue** button, he is returned to the login screen and cannot access the platform until he clicks the **Accept and Continue** button.

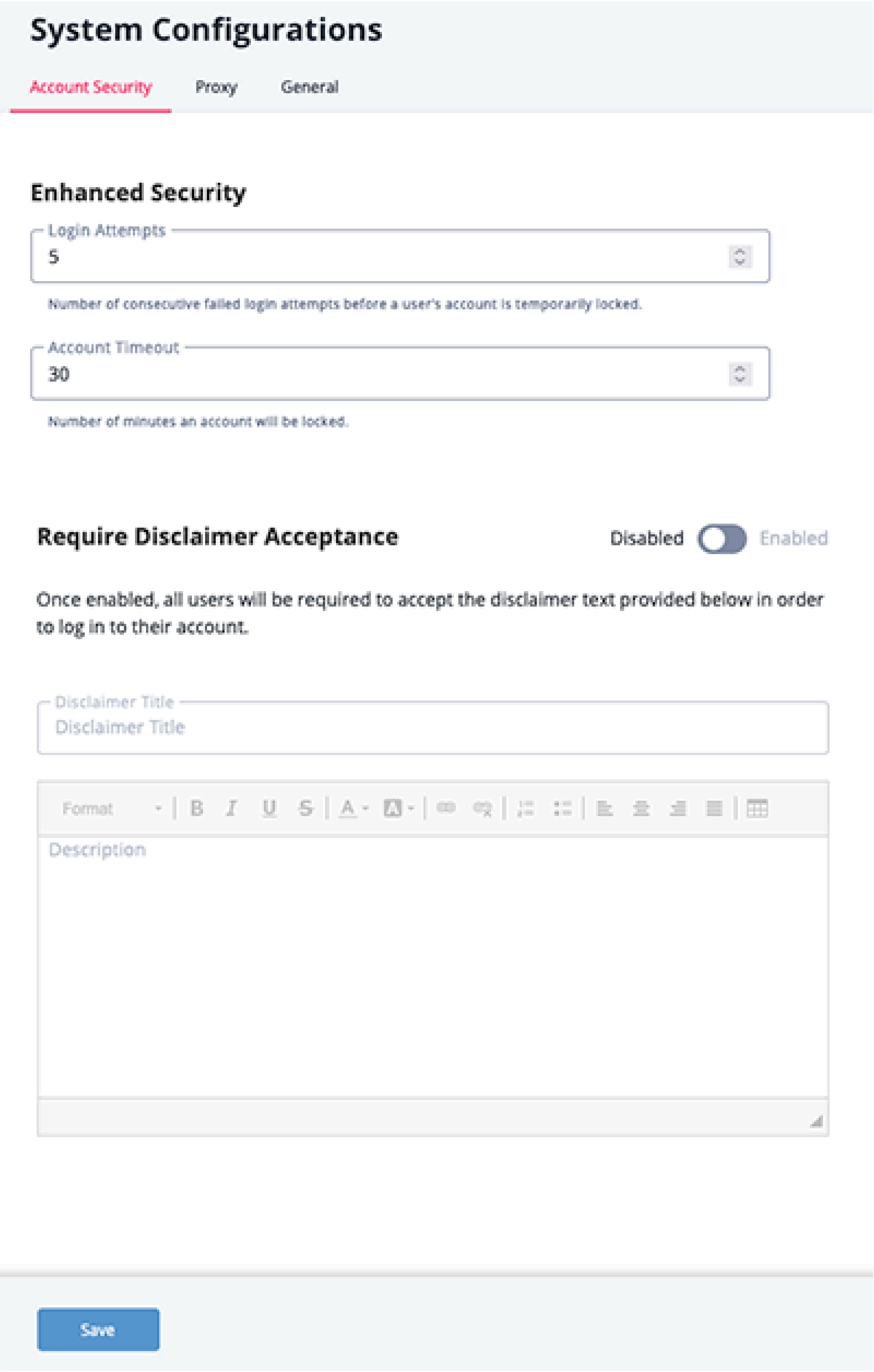
> Users are required to click the **Accept and Continue** button each time they log into platform.

- If a user is logged out and enters a URL for a specific page in the platform, the custom banner is displayed and he must click the **Accept and Continue** button to access the specified page.

Enabling a Custom Banner

> Only administrators have access to enable the custom banner configuration fields in the **Account Security** tab on the *System Configuration* page.

1. Navigate to Settings ⚙ > System Configurations.
   The System Configuration page loads with the Account Security tab selected by default.



System Configurations

Enhanced Security

Login Attempts: 5

Number of consecutive failed login attempts before a user's account is temporarily locked.

Account Timeout: 30

Number of minutes an account will be locked.

Require Disclaimer Acceptance

Disabled ● Enabled

Once enabled, all users will be required to accept the disclaimer text provided below in order to log in to their account.

Disclaimer Title: Disclaimer Title

2. Click the toggle switch in the Require Disclaimer Acceptance section to enable the display of the custom banner.
3. Enter the banner title to be displayed at the top of the banner in the Disclaimer Title field.
4. Enter the body of the message in the Description field.

> The Description field supports standard text formatting as well as the use of links and tables.

5. Click the Save button.
   The next time a user logs in, he is prompted to review and accept the custom banner before proceeding to the platform.

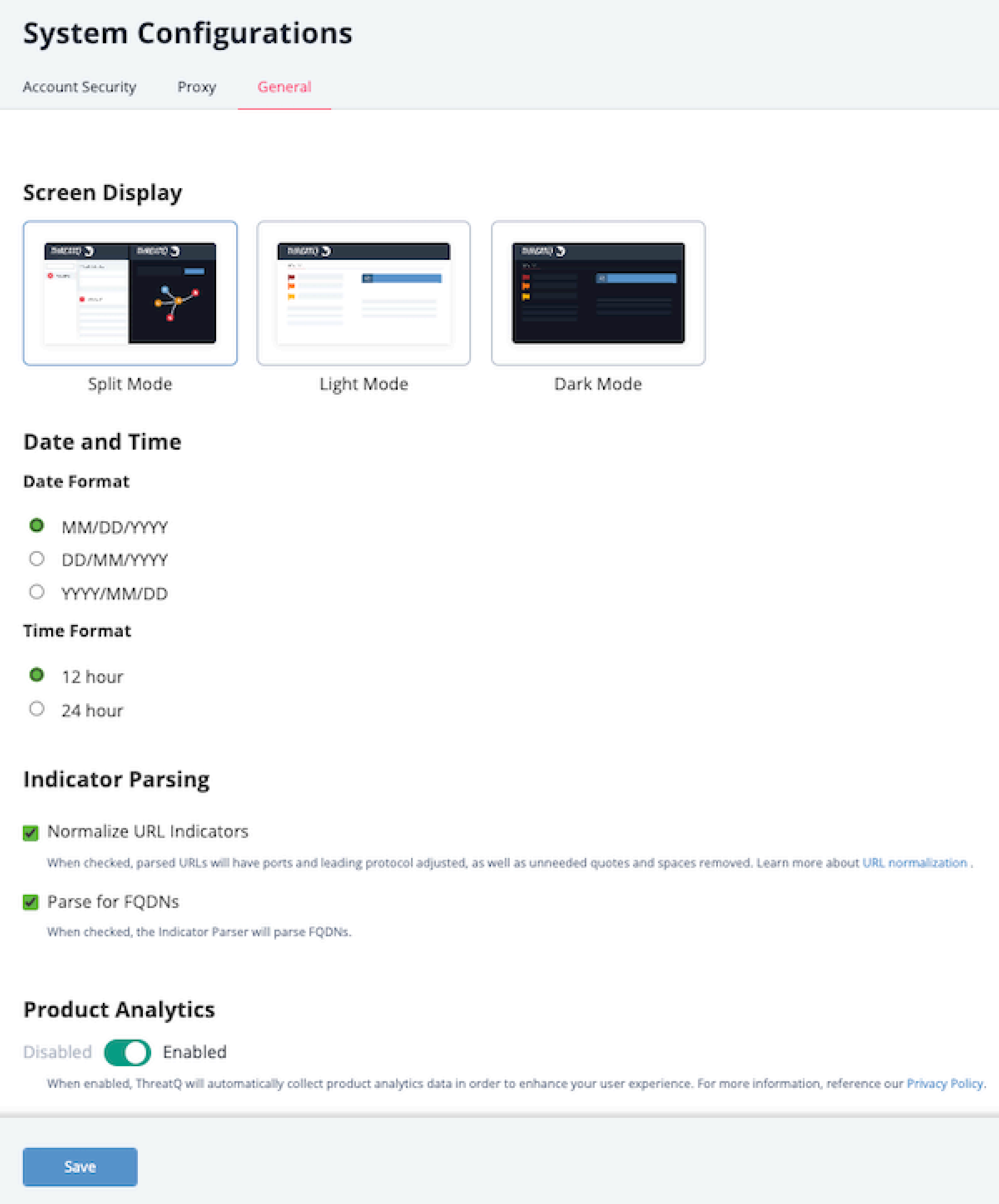
General Settings

In the System Configuration page, the General tab allows Maintenance and Administrative Access users to configure the system display mode, date and time format, and indicator parsing checkbox defaults as well as enable/disable the sharing of analytics data with ThreatQuotient.

Configuring Display Mode

By default, ThreatQ enables the Split display mode. This mode includes a mix of light and dark page formats. Based on user preference, you can change the display mode to Light or Dark mode. When you change the display mode, you will see the changes immediately and all other users will see the changes upon their next login.

1. Navigate to **Settings** ⚙ > **System Configurations**.
2. Click the **General** tab.



System Configurations

Account Security | Proxy | General

Screen Display

Split Mode | Light Mode | Dark Mode

Date and Time

Date Format

● MM/DD/YYYY
○ DD/MM/YYYY
○ YYYY/MM/DD

Time Format

● 12 hour
○ 24 hour

Indicator Parsing

☑ Normalize URL Indicators

When checked, parsed URLs will have ports and leading protocol adjusted, as well as unneeded quotes and spaces removed. Learn more about URL normalization .

☑ Parse for FQDNs

When checked, the Indicator Parser will parse FQDNs.

Product Analytics

Disabled | Enabled

When enabled, ThreatQ will automatically collect product analytics data in order to enhance your user experience. For more information, reference our Privacy Policy.

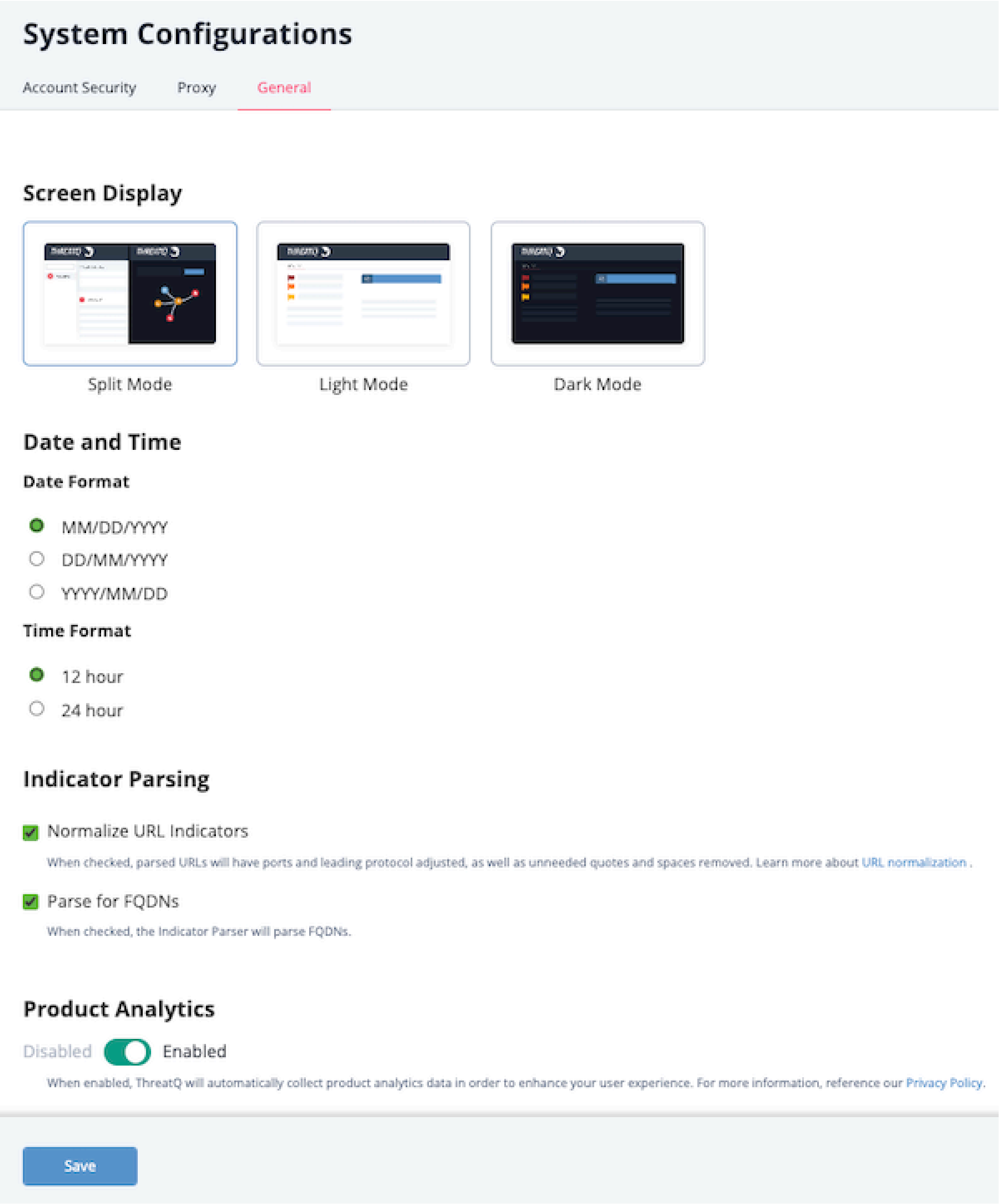
Save

3. From the Screen Display section, click the desired display mode, Split, Light, or Dark.
4. Click the **Save** button.
   ThreatQ applies the display mode change to your current session and to all other users at their next login.

Configuring Date and Time Format

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

1. Navigate to **Settings** ⚙ > **System Configurations**.
2. Click the **General** tab.



Screen Display

Date and Time

Date Format

● MM/DD/YYYY
○ DD/MM/YYYY
○ YYYY/MM/DD

Time Format

● 12 hour
○ 24 hour

Indicator Parsing

☑ Normalize URL Indicators

When checked, parsed URLs will have ports and leading protocol adjusted, as well as unneeded quotes and spaces removed. Learn more about URL normalization .

☑ Parse for FQDNs

When checked, the Indicator Parser will parse FQDNs.

Product Analytics

Disabled Enabled

When enabled, ThreatQ will automatically collect product analytics data in order to enhance your user experience. For more information, reference our Privacy Policy.

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 the **Save** button.

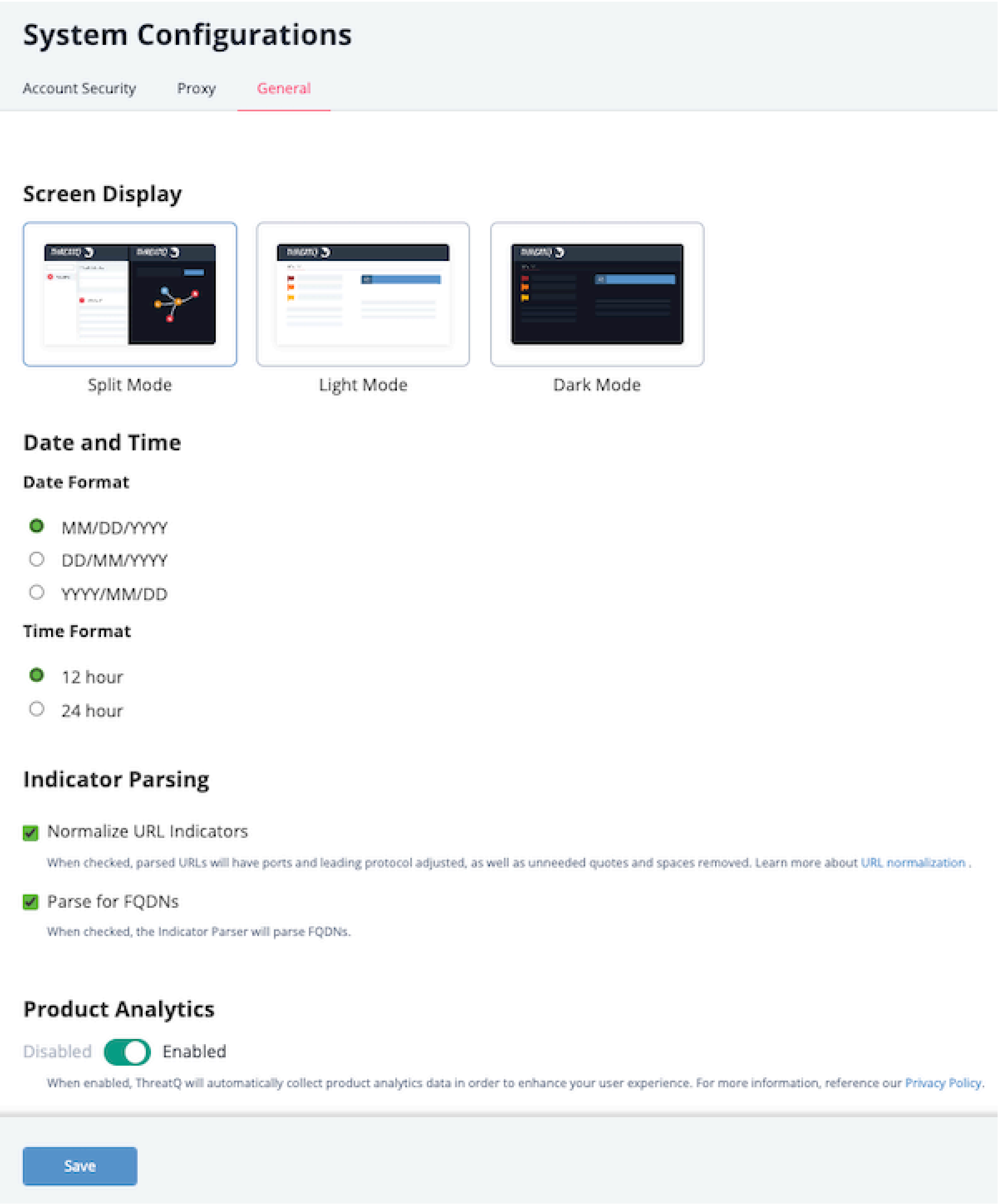
Configuring Indicator Parsing Presets

Users with Maintenance and Administrator roles can configure the default state of the **Normalize URL Indicator** and **Parse for FQDNs** checkboxes for the **Parse for Indicators** option of the Add Indicators dialog box.

> Setting these default states does not lock the checkboxes. Users can select and deselect each option when parsing for an indicator in the Parse for Indicators dialog box.

1. Navigate to **Settings** ⚙ > **System Configurations**.
2. Click the **General** tab.

The General tab loads.



System Configurations

Screen Display

Date and Time

Date Format

● MM/DD/YYYY
○ DD/MM/YYYY
○ YYYY/MM/DD

Time Format

● 12 hour
○ 24 hour

Indicator Parsing

☑ Normalize URL Indicators

When checked, parsed URLs will have ports and leading protocol adjusted, as well as unneeded quotes and spaces removed. Learn more about URL normalization .

☑ Parse for FQDNs

When checked, the Indicator Parser will parse FQDNs.

Product Analytics

Disabled Enabled

When enabled, ThreatQ will automatically collect product analytics data in order to enhance your user experience. For more information, reference our Privacy Policy.

3. In the Indicator Parsing section, set the following options:

OPTION	DESCRIPTION
Normalize URL Indicators	When checked, parsed URLs will have ports and leading protocol adjusted, as well as unneeded quotes and spaces removed.

OPTION	DESCRIPTION
Parse for FQDNs	When checked, the Indicator Parser will parse FQDNs from the text and derive FQDN indicators from URLs in the text. **Example (checked)**: URL: https://tqexample.com/table.jspa?query_string_example Indicators created: ◦ tqexample.com/table.jspa (the URL) ◦ tqexample.com (the derived FQDN from the URL) When unchecked, the Indicator Parser will not generate FQDN indicators from the parsed text. **Example (unchecked)**: URL: https://tqexample.com/table.jspa?query_string_example Indicator created: ◦ tqexample.com/table.jspa (the URL)

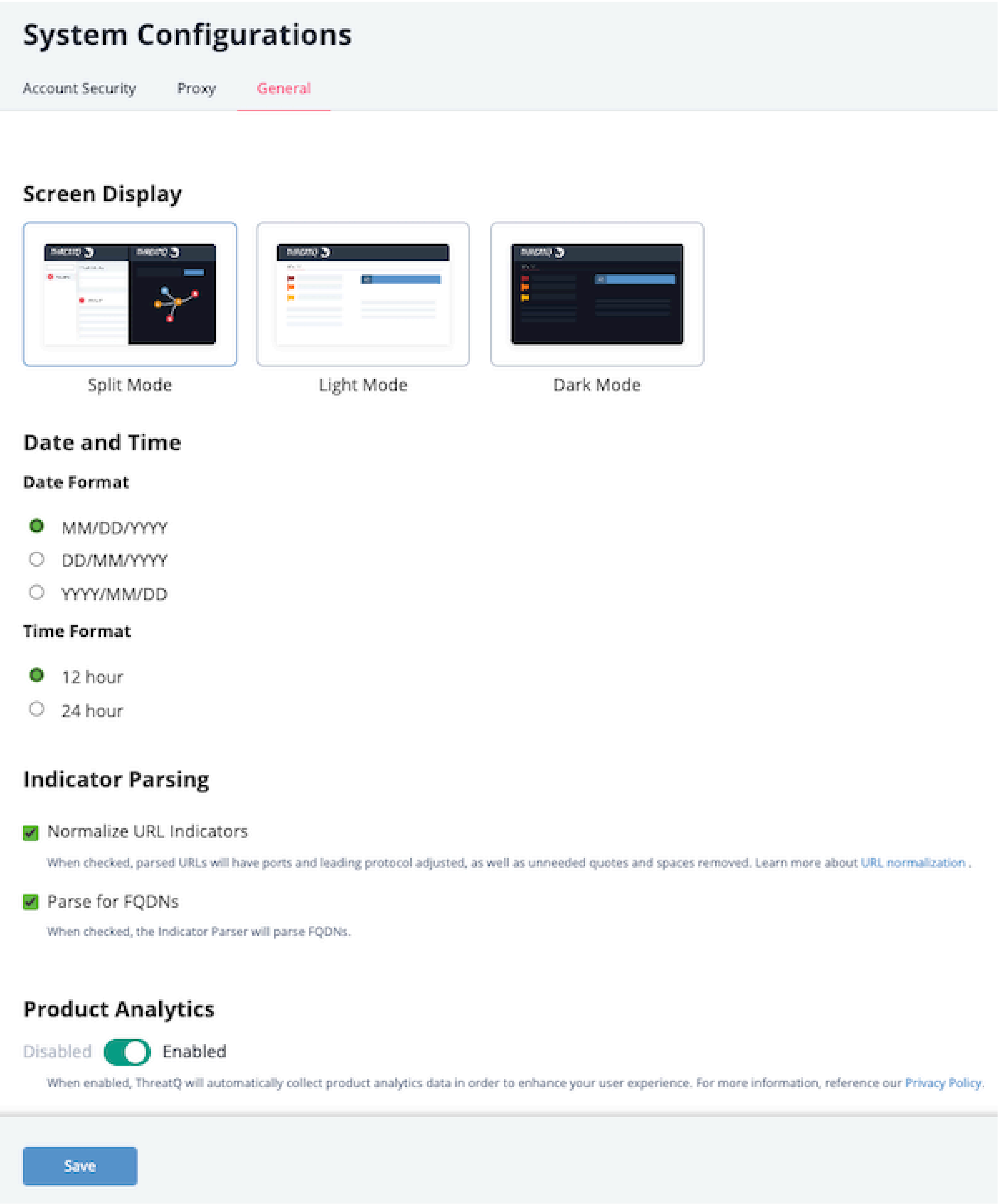
4. Click the **Save** button.

Opt In/ Opt Out of Product Analytics

The Product Analytics toggle allows you to disable/enable the sharing of analytics data with ThreatQuotient. Enabling analytics allows ThreatQuotient to collect anonymized data on user actions to improve the overall user experience.

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

2. Click the **General** tab.



System Configurations

Screen Display

Split Mode | Light Mode | Dark Mode

Date and Time

Date Format

● MM/DD/YYYY
○ DD/MM/YYYY
○ YYYY/MM/DD

Time Format

● 12 hour
○ 24 hour

Indicator Parsing

☑ Normalize URL Indicators

When checked, parsed URLs will have ports and leading protocol adjusted, as well as unneeded quotes and spaces removed. Learn more about URL normalization .

☑ Parse for FQDNs

When checked, the Indicator Parser will parse FQDNs.

Product Analytics

Disabled ● Enabled

When enabled, ThreatQ will automatically collect product analytics data in order to enhance your user experience. For more information, reference our Privacy Policy.

Save

3. In the Product Analytics section, click the toggle button to change the setting from Disabled to Enabled or vice versa.
4. Click the **Save** button.

System Objects

System objects are threat data which has been ingested or manually added to your Threat Library. ThreatQ is seeded with the following system object types:

- Adversaries
- Assets
- Attack Patterns
- Campaigns
- Courses of Action
- Events
- Exploit Targets
- Files
- Identities
- Indicators
- Intrusion Sets
- Malware
- Reports
- Signatures
- STIX
- Tasks

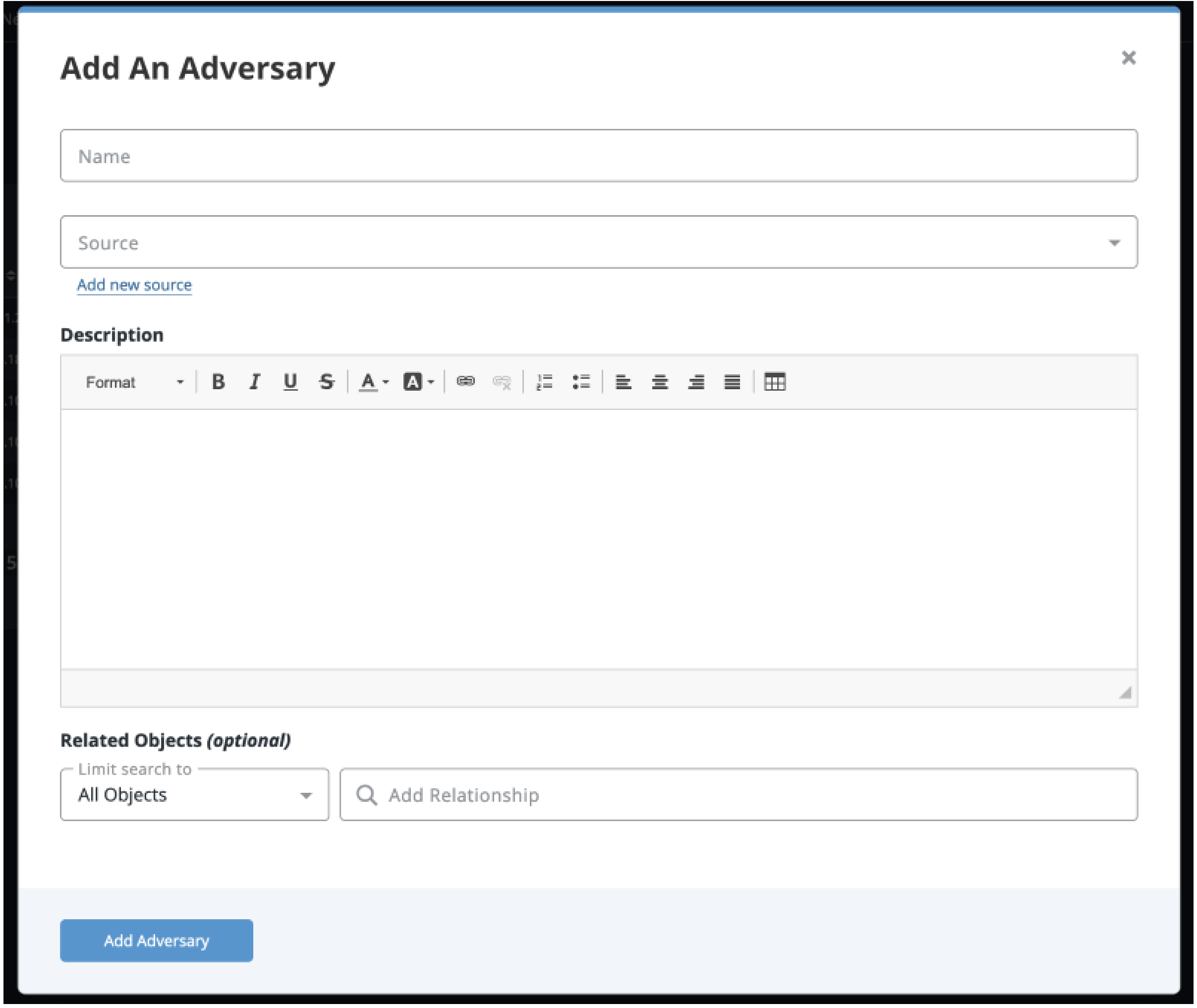
Adversaries

An Adversary is an individual or group that attempts to perform malicious actions against another individual or organization.

Use the steps below to create, edit and delete an Adversary.

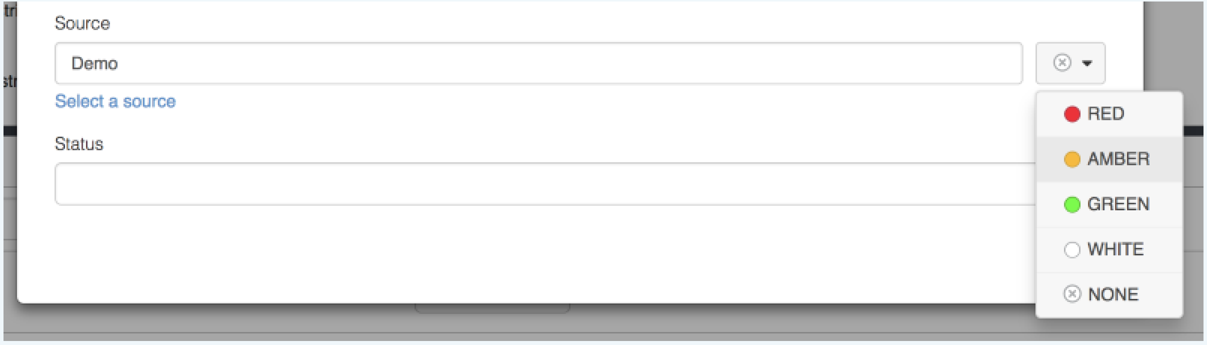
Adding Adversaries

1. Go to **Create** > **Adversary**.
   The Add an Adversary window is displayed.



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

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



Source: Demo

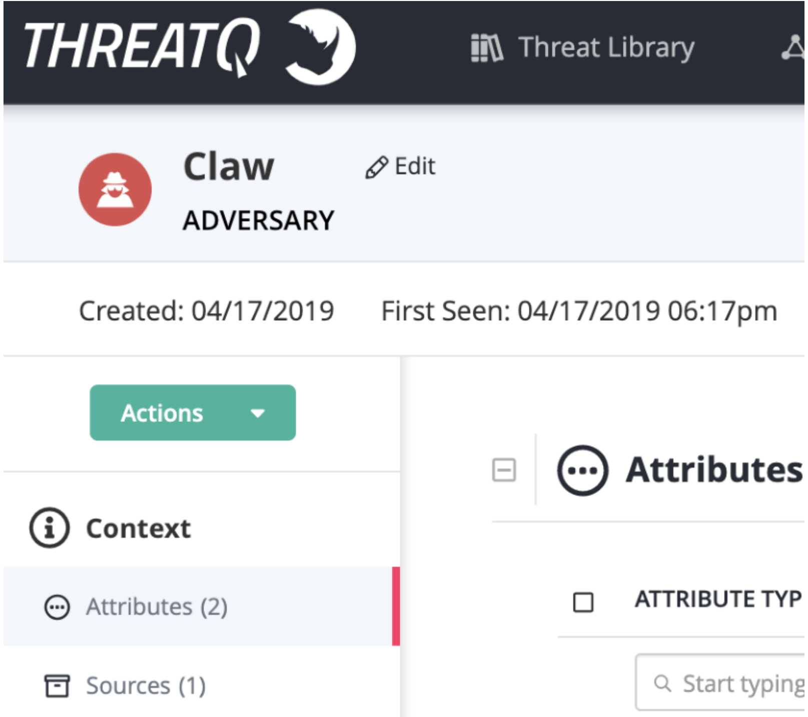
4. Enter a description.
5. Select any **Related Objects** you need to link to the adversary. This field is optional.
6. Click the **Add Adversary** button.

Adding Context

See the Object Details section and its topics for details on adding context to an object such as adding sources, attributes, and related objects.

Editing Adversaries

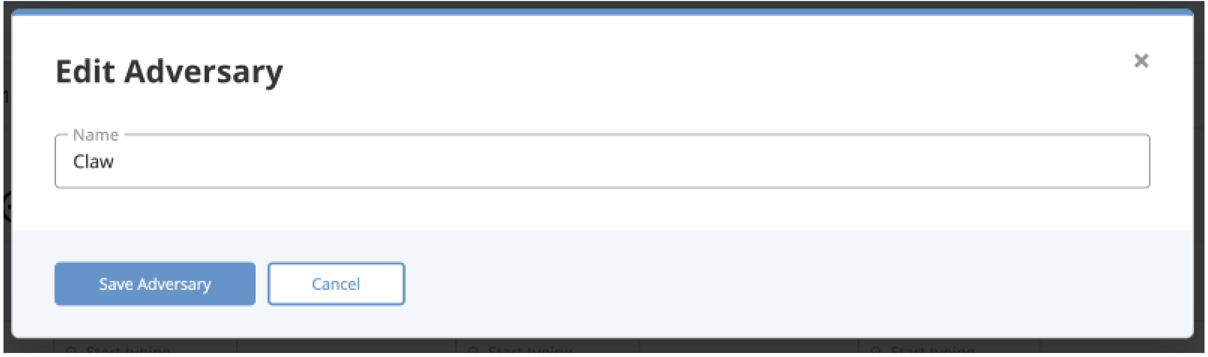
1. Locate and click the adversary.
   The Adversary Details page opens.



Created: 04/17/2019

First Seen: 04/17/2019 06:17pm

2. Click on **Edit** next to the Adversary name.
   The Edit Adversary dialog box opens.

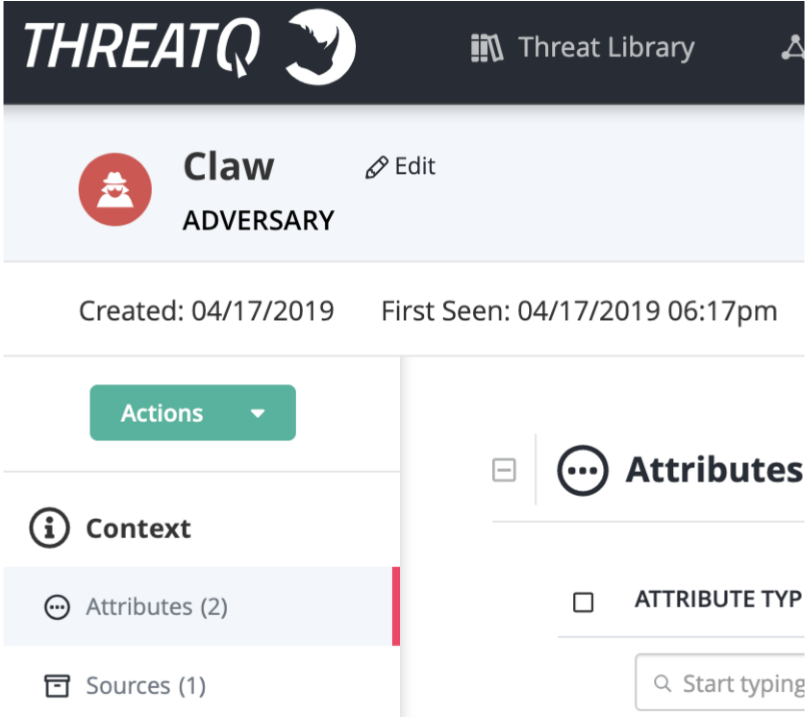


Name: Claw

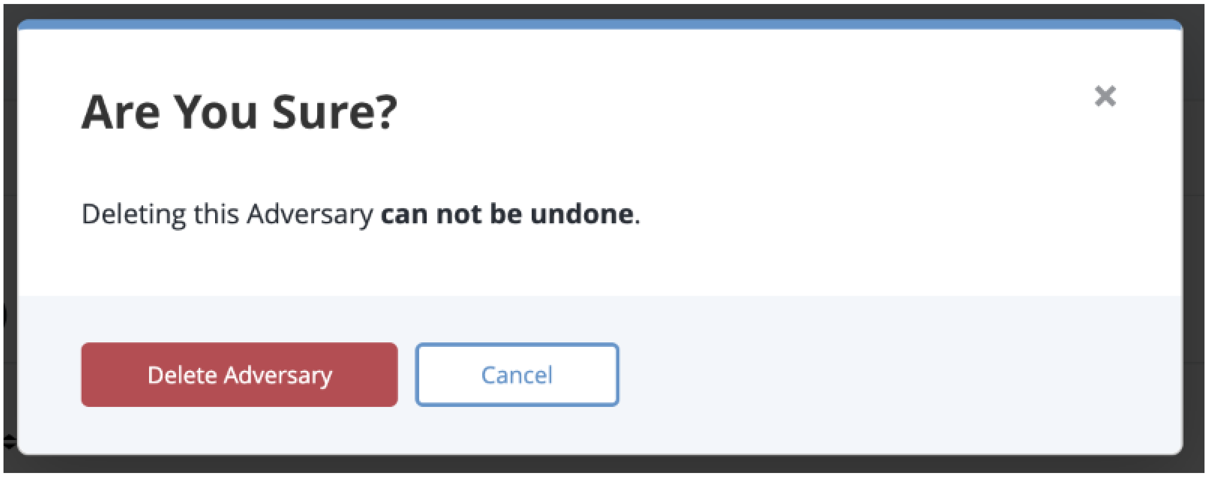
3. Make the desired change to the Adversary name.
4. Click the **Save Adversary** button.

Deleting Adversaries

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



2. Click the **Actions** menu and select **Delete Adversary**.
   A confirmation dialog box appears.



Are You Sure?

Deleting this Adversary **can not be undone**.

3. Click the **Delete Adversary** button.

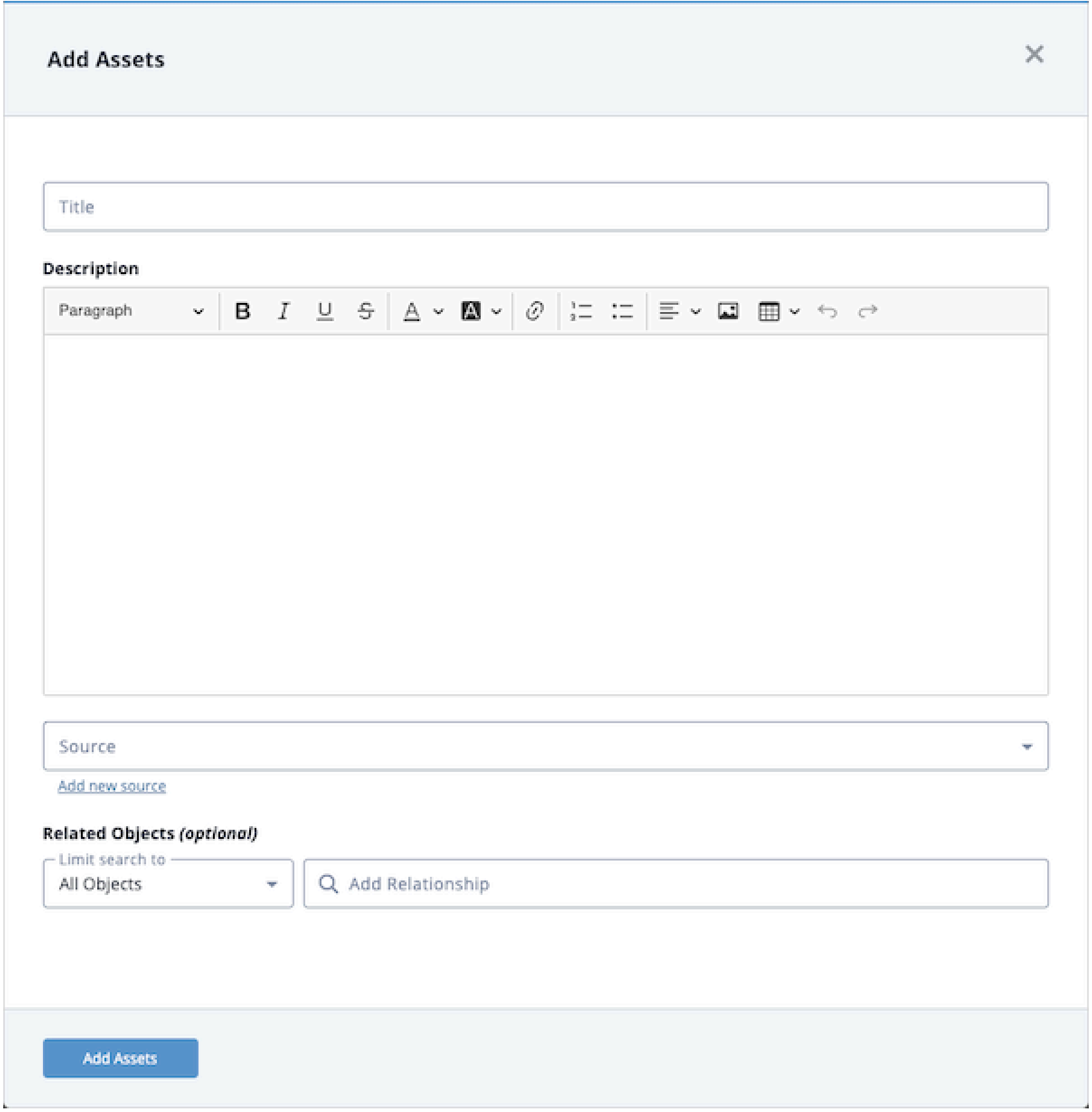
Assets

Assets are tangible or intangible items of value to stakeholders. An asset's value is usually based on the impact of the loss of use of the asset. For instance, a company's billing application is a high value asset since the loss of access to this application impacts revenue.

Use the steps below to create, edit and delete Assets.

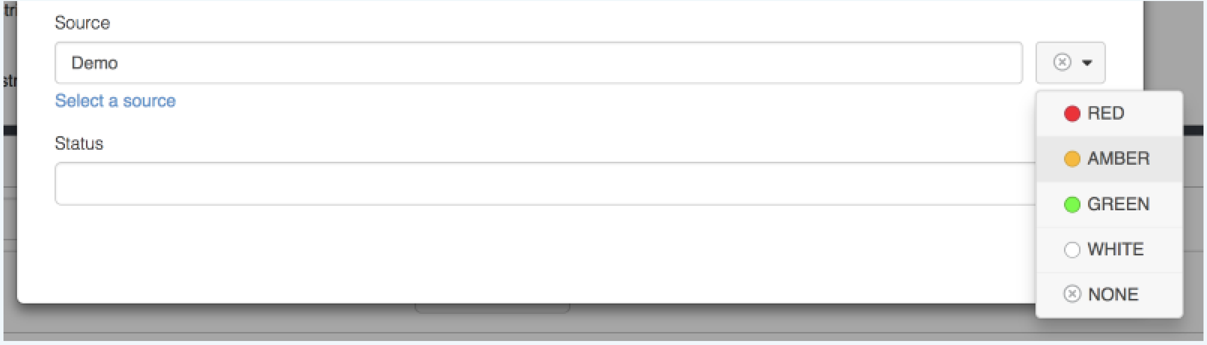
Adding Assets

1. Go to **Create** > **Assets**.
   The Add Assets window is displayed.



2. Enter the asset name.
3. Enter a description of the asset.
4. Select a **Source** from the dropdown provided.

> You can also click the **Add a New Source** option if the desired source is not listed in the dropdown list . If administrators have enabled TLP view settings, you can select a TLP label for the new source in the dropdown list provided. See the

> Traffic Light Protocol (TLP) topic for more information on TLP schema.
>
> 
>
> Source: Demo
>
> Select a source
>
> Status
>
>

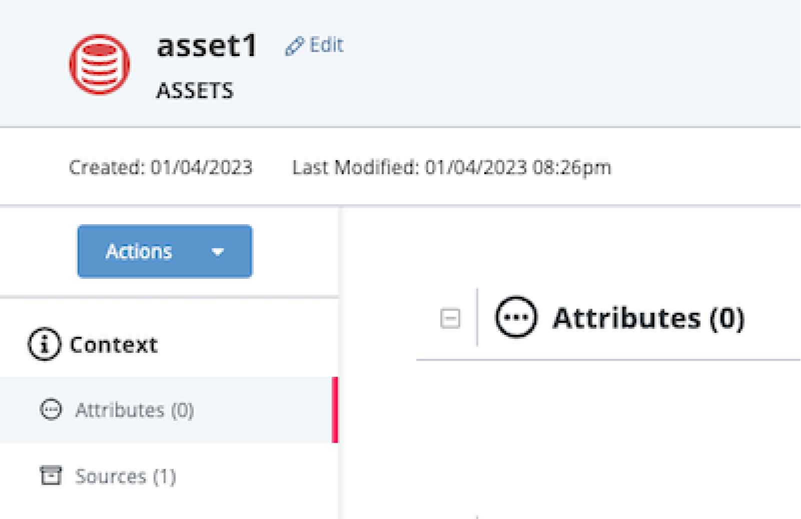
5. Select any **Related Objects** you need to link to the asset. This field is optional.
6. Click **Add Assets**.

Adding Context

See the Object Details section and its topics for details on adding context to an object such as adding sources, attributes, and related objects.

Editing Assets

1. Locate and click the assets object.
   The Assets Details page opens.

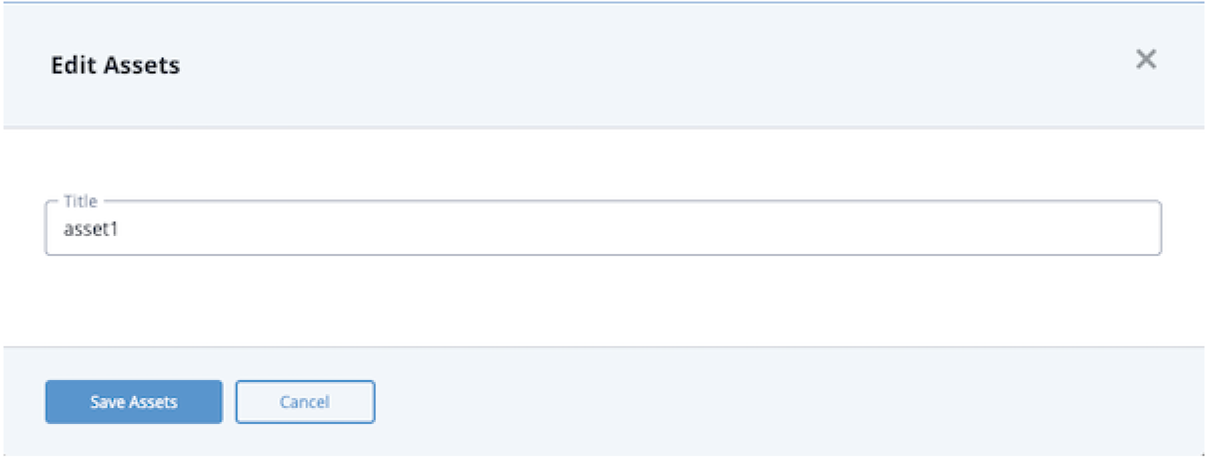


asset1

ASSETS

Created: 01/04/2023 Last Modified: 01/04/2023 08:26pm

2. Click the **Edit** option next to the Assets object name.
   The Edit Assets window is displayed.

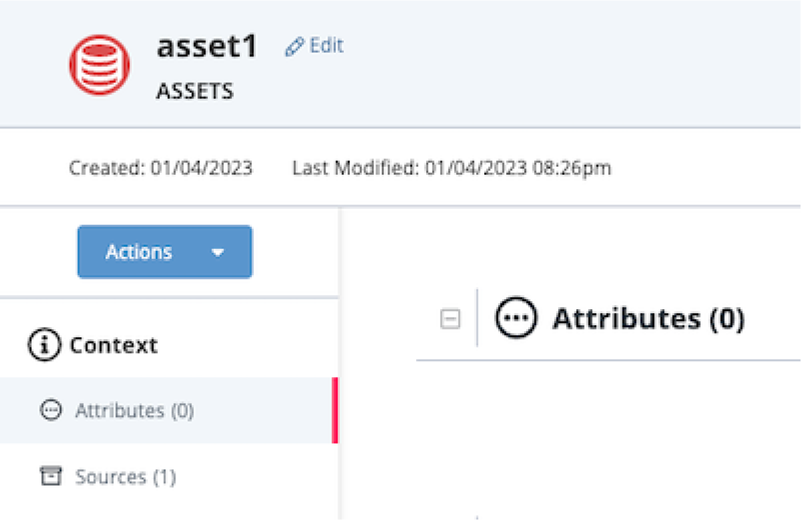


Title: asset1

3. Make the desired change to the Adversary name.
4. Click the **Save Assets** button.

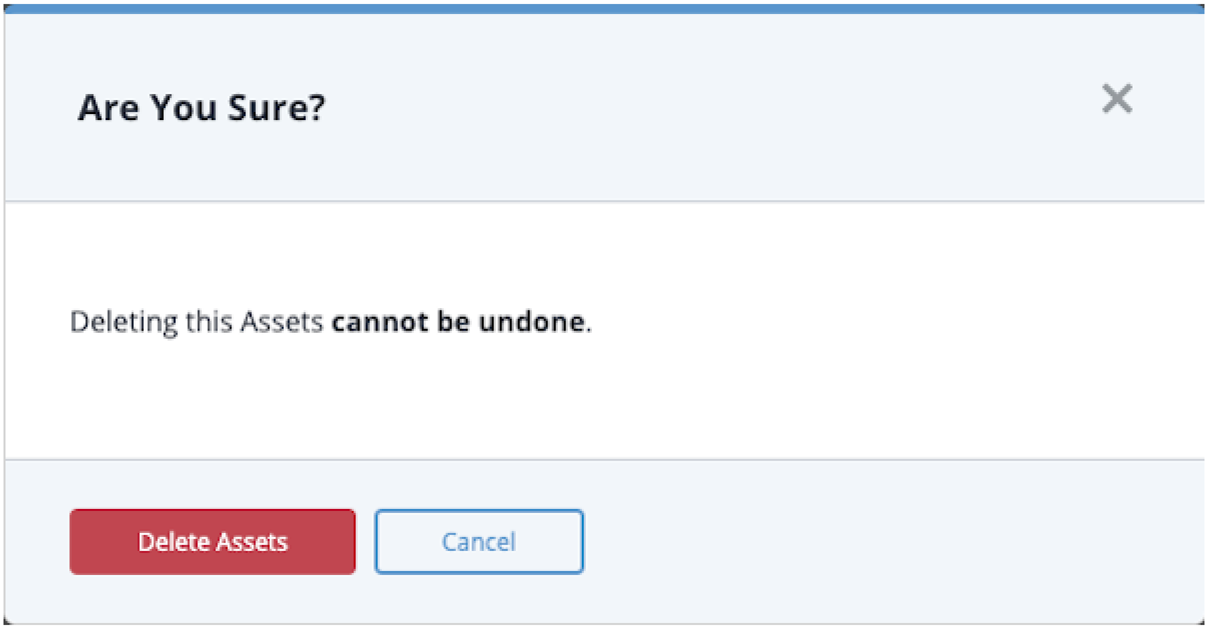
Deleting Assets

1. Locate and click the assets object.
   The Asset Details page opens.



Created: 01/04/2023 Last Modified: 01/04/2023 08:26pm

2. Click on the **Actions** menu and select **Delete Assets**.
   The Are You Sure window prompts you confirm the deletion.



Deleting this Assets **cannot be undone**.

3. Click the **Delete Assets** button.

Attack Patterns

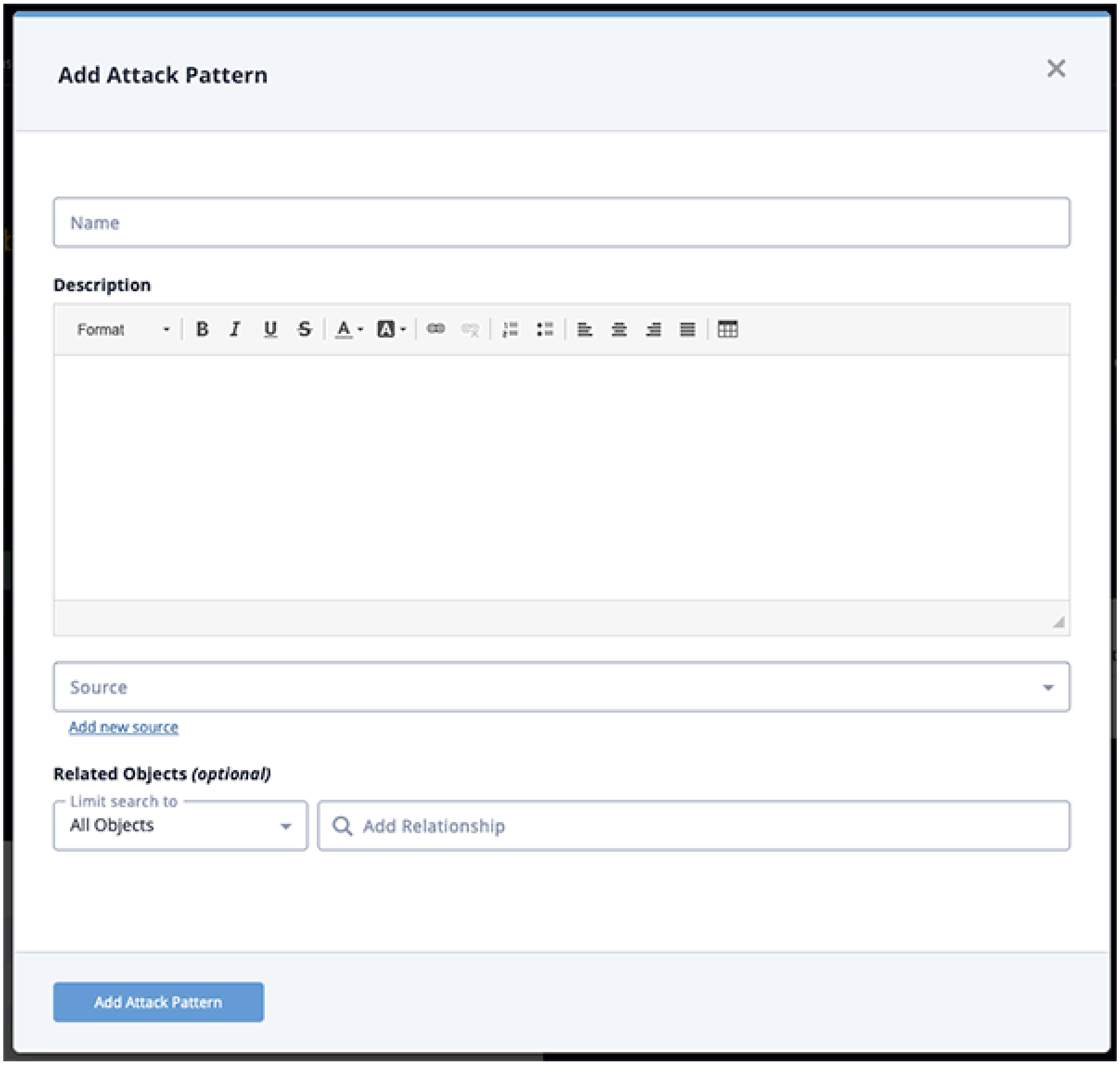
Attack Pattern are descriptions of methods used to exploit software.

Use the steps below to create, edit and delete an Attack Pattern.

Adding an Attack Patterns

1. Go to **Create > Attack Pattern**.

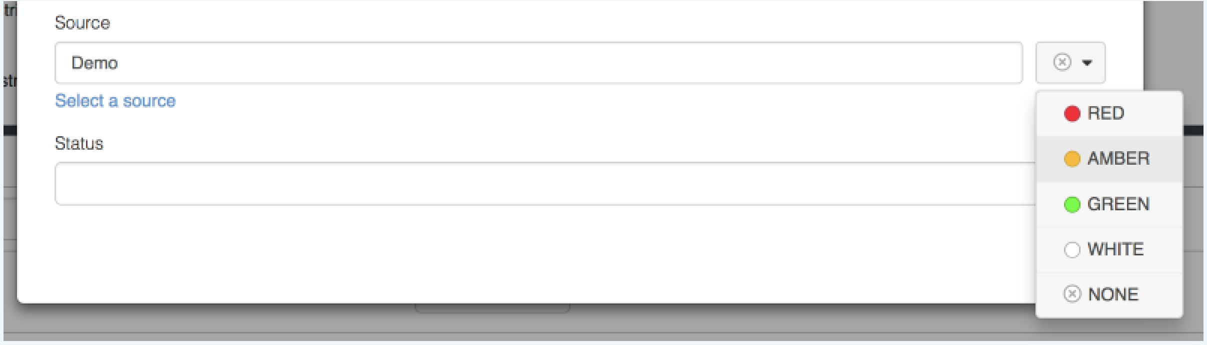
   The Add Attack Pattern dialog box opens.



2. Enter a name.

3. Enter a description in the field provided.
4. Select a **Source** from the dropdown provided.

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



Source: Demo

Status:

5. Select any **Related Objects** you need to link to the Attack Pattern. This field is optional.
6. Click **Add Attack Pattern**.

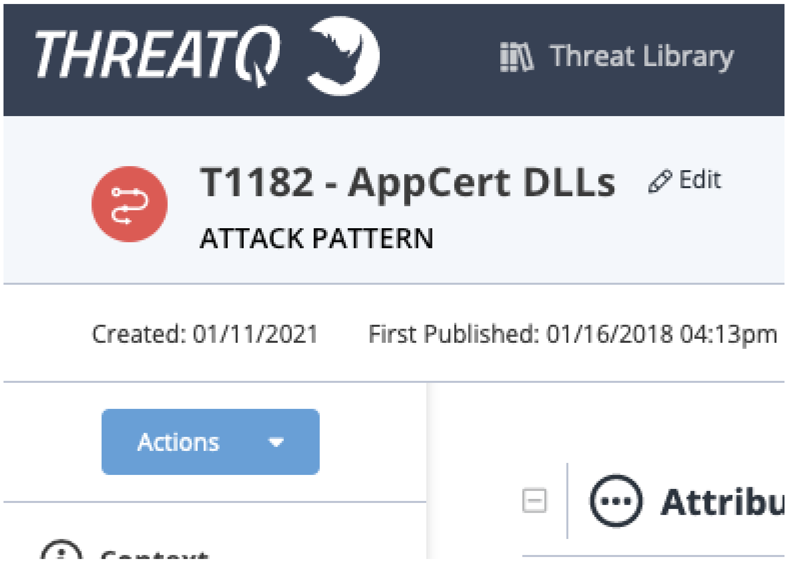
Adding Context

See the Object Details section and its topics for details on adding context to an object such as adding sources, attributes, and related objects.

Editing an Attack Pattern

1. Locate and click on the attack pattern.

The Attack Pattern's detail page opens.

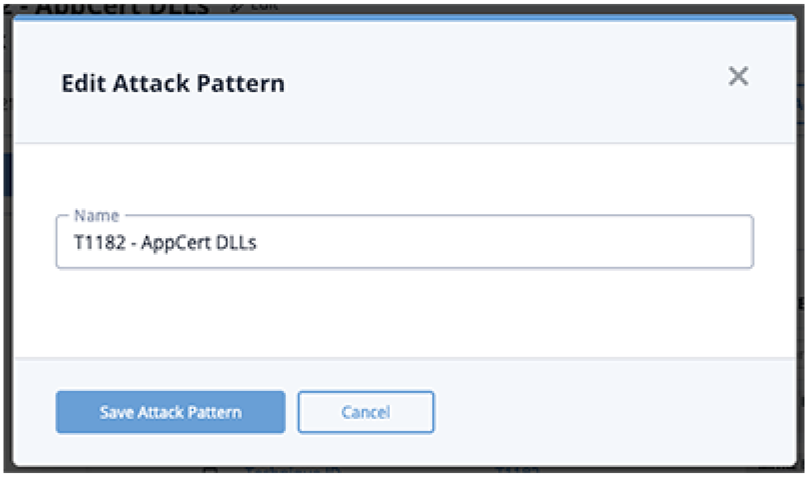


T1182 - AppCert DLLs

Created: 01/11/2021 First Published: 01/16/2018 04:13pm

2. Click on **Edit** next to the Attack Pattern's name.

   The Edit Attack Pattern dialog box opens.



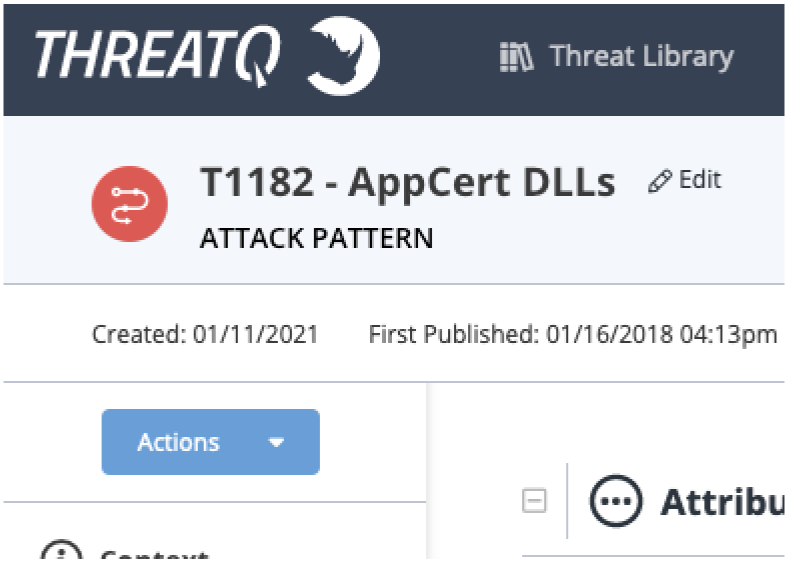
Name
T1182 - AppCert DLLs

3. Make the desired change to the Attack Pattern name and click **Save Attack Pattern**.

Deleting an Attack Pattern

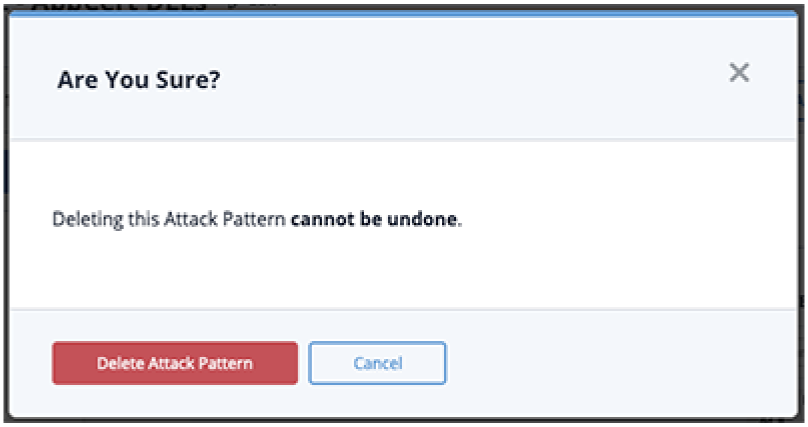
1. Locate and click on the Attack Pattern.

The Attack Pattern's details page opens.



2. Click on the **Actions** menu and select **Delete Attack Pattern**.

   A confirmation dialog box appears.



Deleting this Attack Pattern **cannot be undone**.

3. Click on **Delete Attack Pattern**.

Campaigns

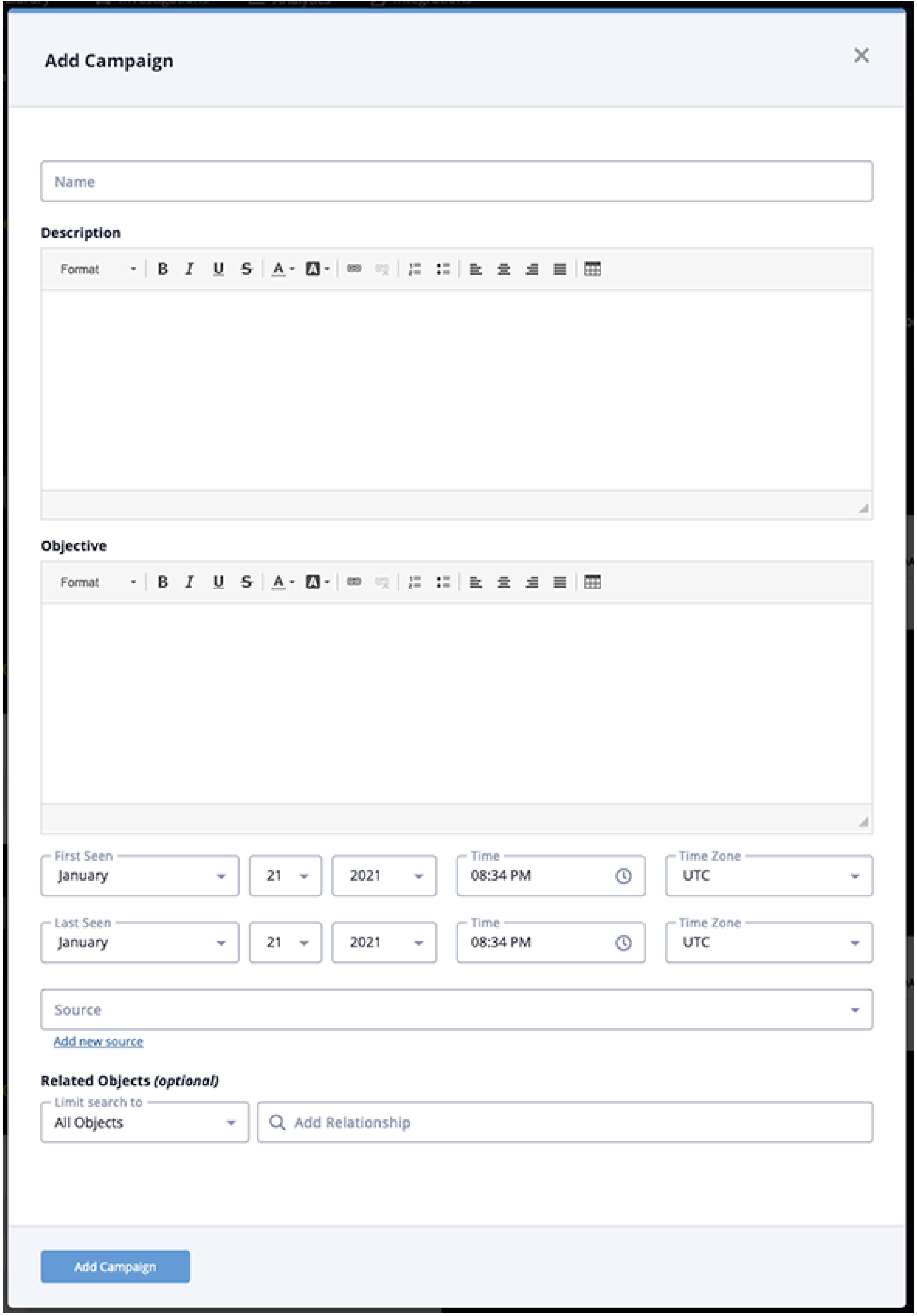
Campaign are groups of behaviors that describe malicious activities taken against specific targets over a period of time.

Use the steps below to create, edit and delete a Campaign.

Adding a Campaign

1. Go to **Create** > **Campaign**.

The Add Campaign dialog box opens.



Add Campaign

Name

Description

Objective

First Seen: January 21 2021, Time: 08:34 PM, Time Zone: UTC

Last Seen: January 21 2021, Time: 08:34 PM, Time Zone: UTC

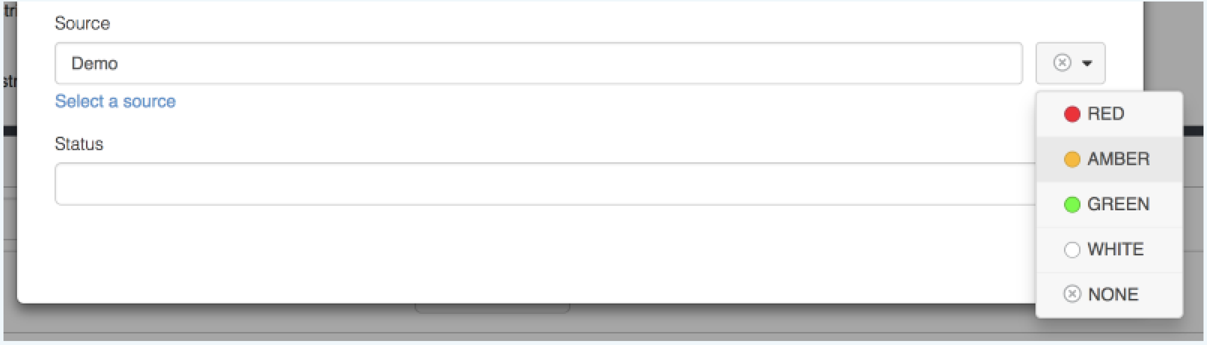
Source

Related Objects *(optional)*

Limit search to: All Objects

2. Enter a **Name**.

3. Enter a **Description** in the field provided.
4. Enter an **Objective**.
5. Select the **First Seen** and **Last Scene** times.
6. Select a **Source** from the dropdown provided.

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

7. Select any **Related Objects** you need to link to the Campaign. This field is optional.
8. Click **Add Campaign**.

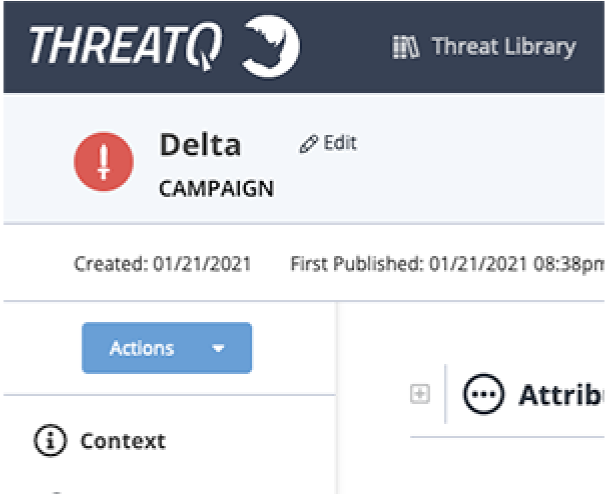
Adding Context

See the Object Details section and its topics for details on adding context to an object such as adding sources, attributes, and related objects.

Editing a Campaign

1. Locate and click on the Campaign.

The Campaign's detail page opens.

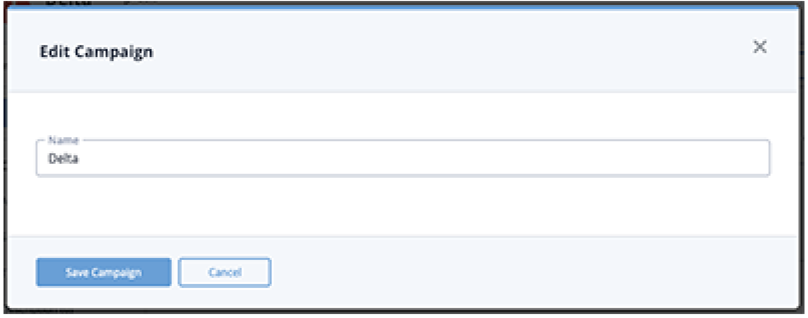


Created: 01/21/2021

First Published: 01/21/2021 08:38pn

2. Click on **Edit** next to the Campaign's name.

   The Edit Campaign dialog box opens.



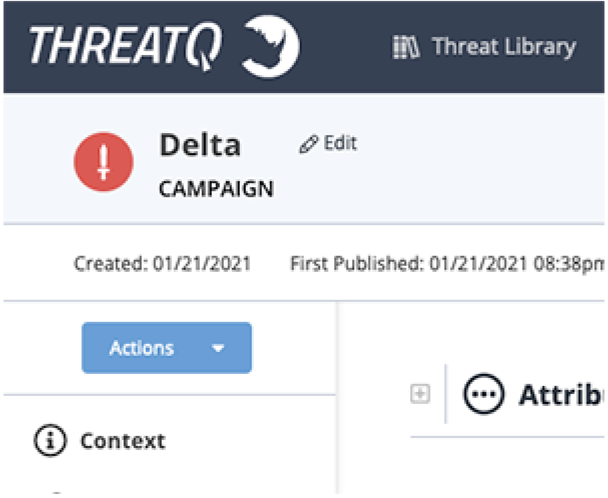
Name: Delta

3. Make the desired change to the Campaign name and click **Save Campaign**.

Deleting a Campaign

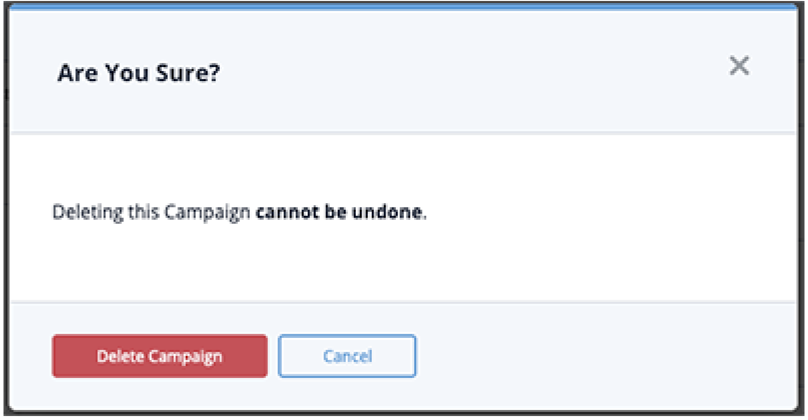
1. Locate and click on the Campaign.

The Campaign's details page opens.



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

   A confirmation dialog box appears.



Deleting this Campaign **cannot be undone**.

3. Click on **Delete Campaign**.

Courses of Action

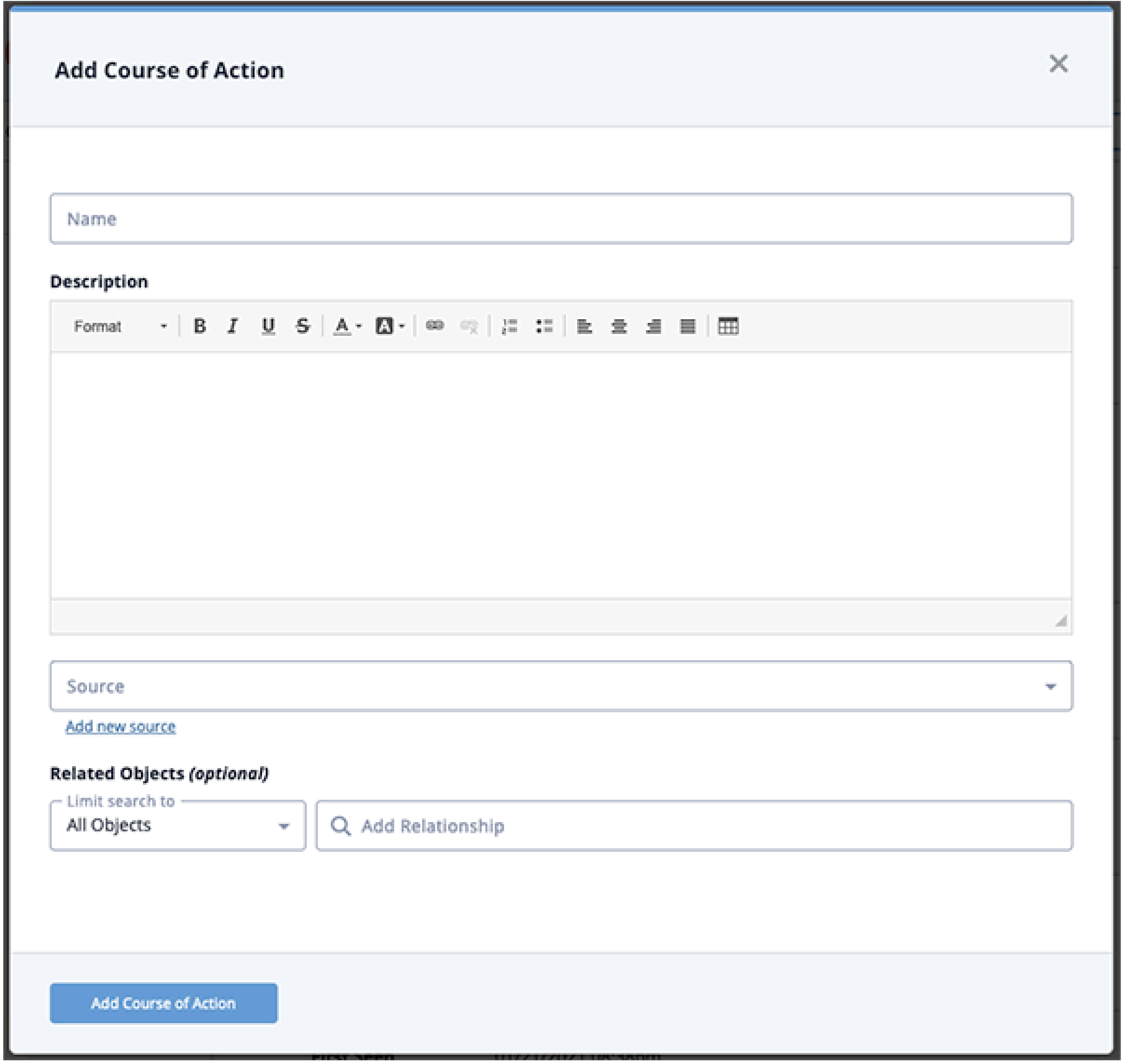
Courses of Action are a combination of risk response measures taken to address or prevent malicious attacks.

Use the steps below to create, edit and delete a Course of Action.

Adding a Course of Action

1. Go to **Create > Course of Action**.

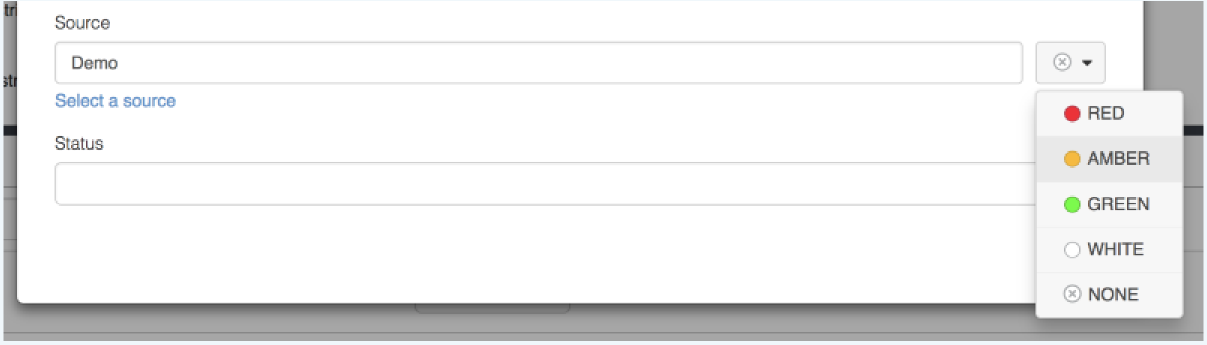
   The Add Course of Action dialog box opens.



2. Enter a **Name**.

3. Enter a **Description** in the field provided.
4. Select a **Source** from the dropdown provided.

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



Source: Demo

Status:

5. Select any **Related Objects** you need to link to the Course of Action. This field is optional.
6. Click **Add Course of Action**.

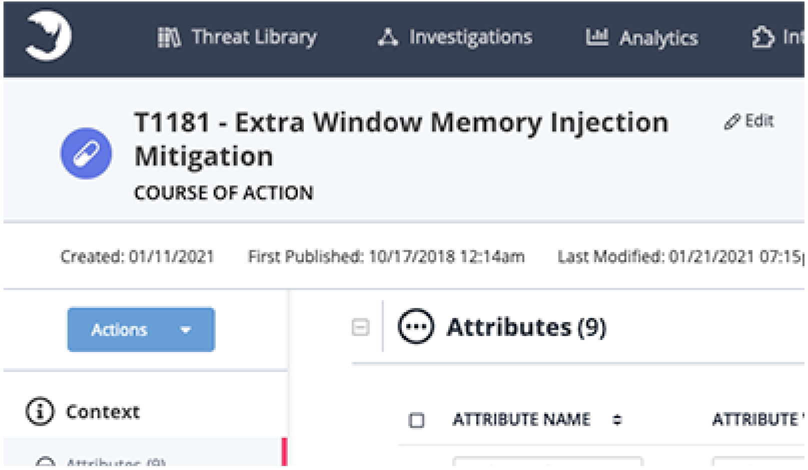
Adding Context

See the Object Details section and its topics for details on adding context to an object such as adding sources, attributes, and related objects.

Editing a Course of Action

1. Locate and click on the Course of Action.

   The Course of Action's detail page opens.



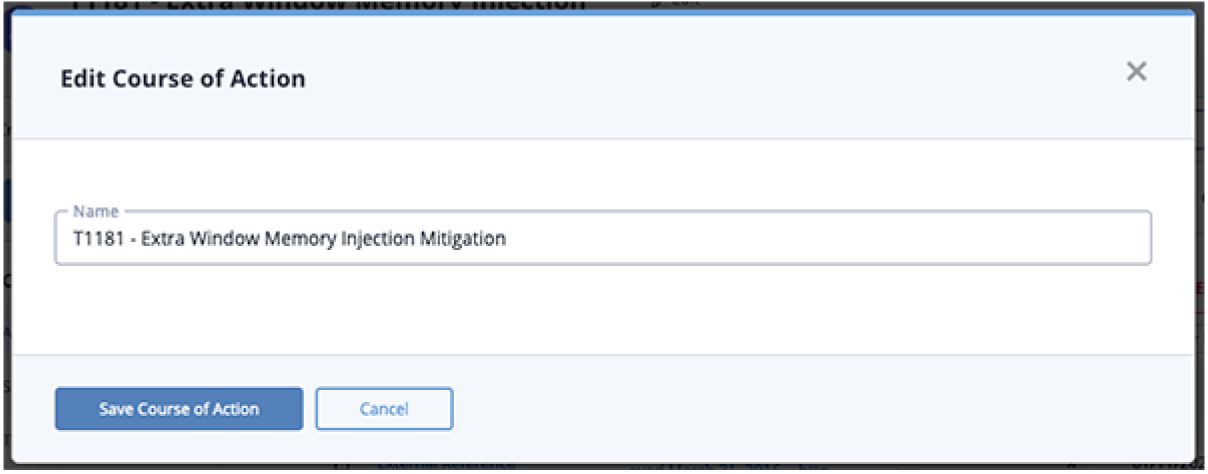
T1181 - Extra Window Memory Injection Mitigation

COURSE OF ACTION

Created: 01/11/2021 First Published: 10/17/2018 12:14am Last Modified: 01/21/2021 07:15

2. Click on **Edit** next to the Course of Action's name.

   The Edit Course of Action dialog box opens.

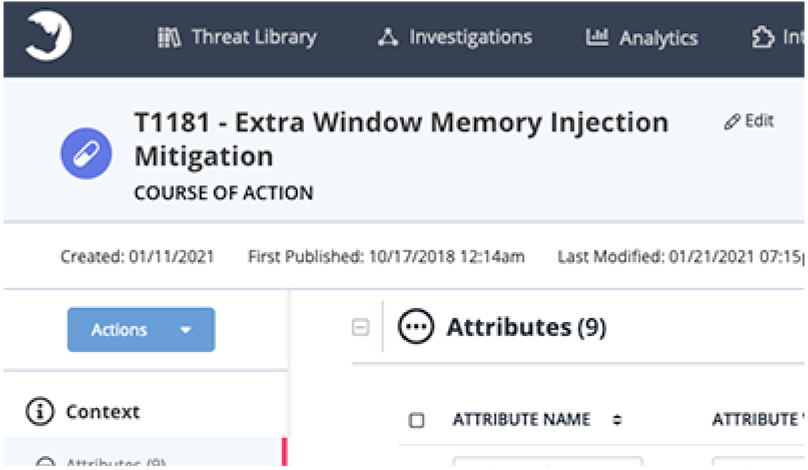


3. Make the desired change to the Course of Action's name and click **Save Course of Action**.

Deleting a Course of Action

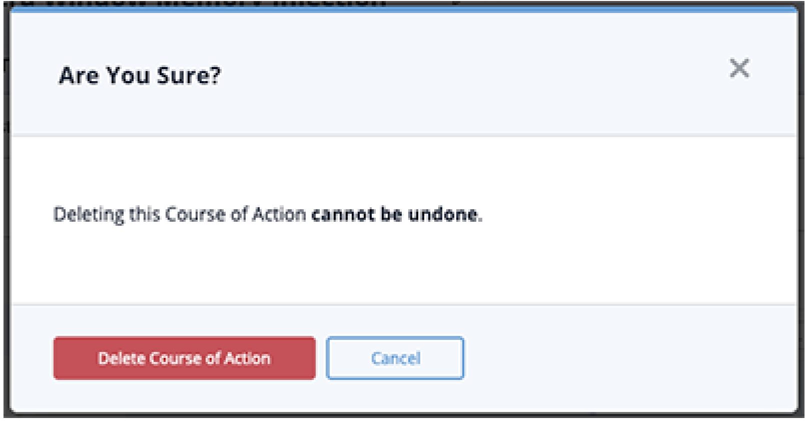
1. Locate and click on the Course of Action.

   The Course of Action's details page opens.



2. Click on the **Actions** menu and select **Delete Course of Action**.

A confirmation dialog box appears.



Deleting this Course of Action **cannot be undone.**

3. Click on **Delete Course of Action**.

Events

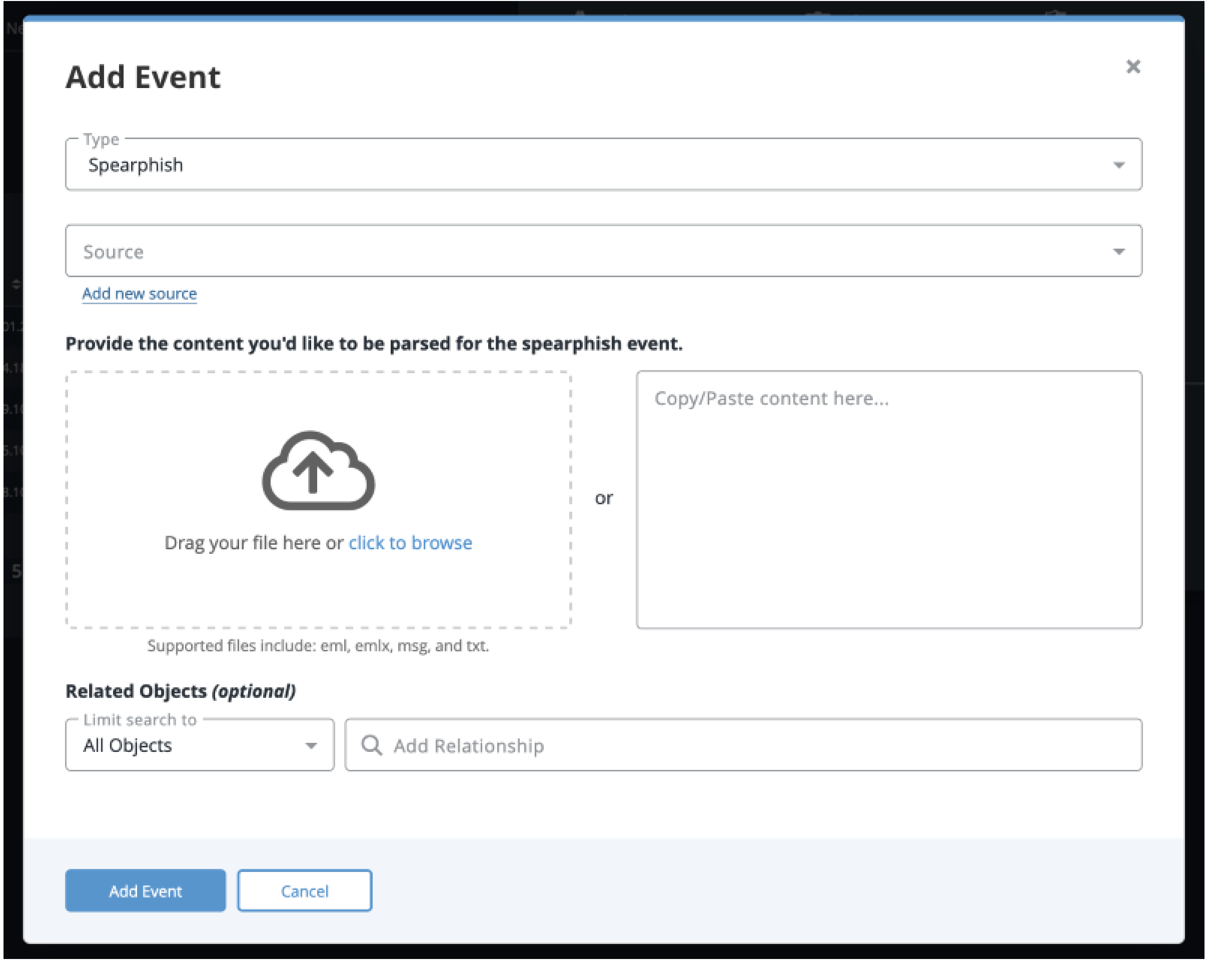
Events are objects that focus on temporal incidents that have significant security impact.

Use the steps below to create, edit and delete an Event.

Adding Events

1. Go to **Create > Event**.

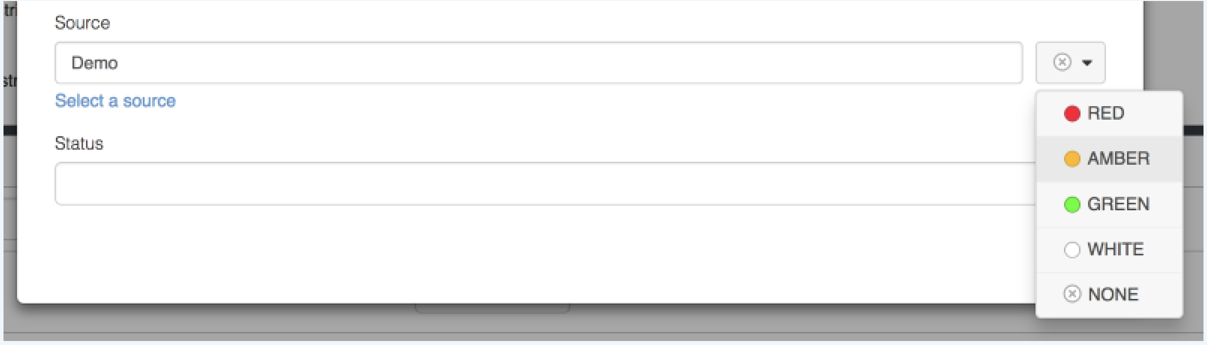
   The Add Event dialog box opens.


Add Event
×
Type
Spearphish
Source
Add new source
Provide the content you'd like to be parsed for the spearphish event.
Drag your file here or click to browse
or
Copy/Paste content here...
Supported files include: eml, emlx, msg, and txt.
Related Objects (optional)
Limit search to
All Objects
Add Relationship
Add Event
Cancel

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

> You can also click the **Add a New Source** option if the desired source is not listed in the dropdown list . If administrators have enabled TLP view settings, you can select a TLP label for the new source in the dropdown list provided. See the

> Traffic Light Protocol (TLP) topic for more information on TLP schema.



Source

Demo

Select a source

Status

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**.

Adding Context

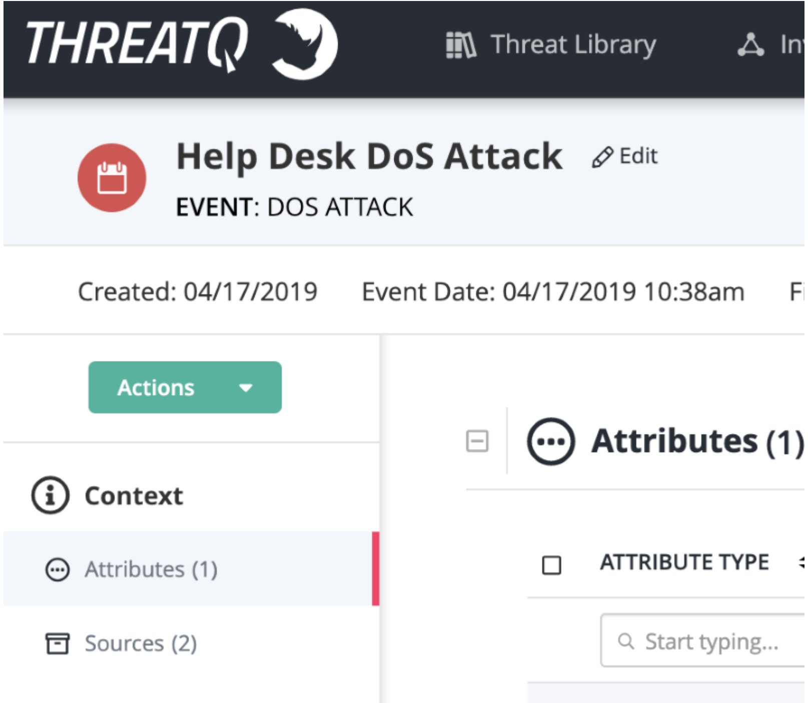
See the Object Details section and its topics for details on adding context to an object such as adding sources, attributes, and related objects.

Editing Events

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.



Help Desk DoS Attack

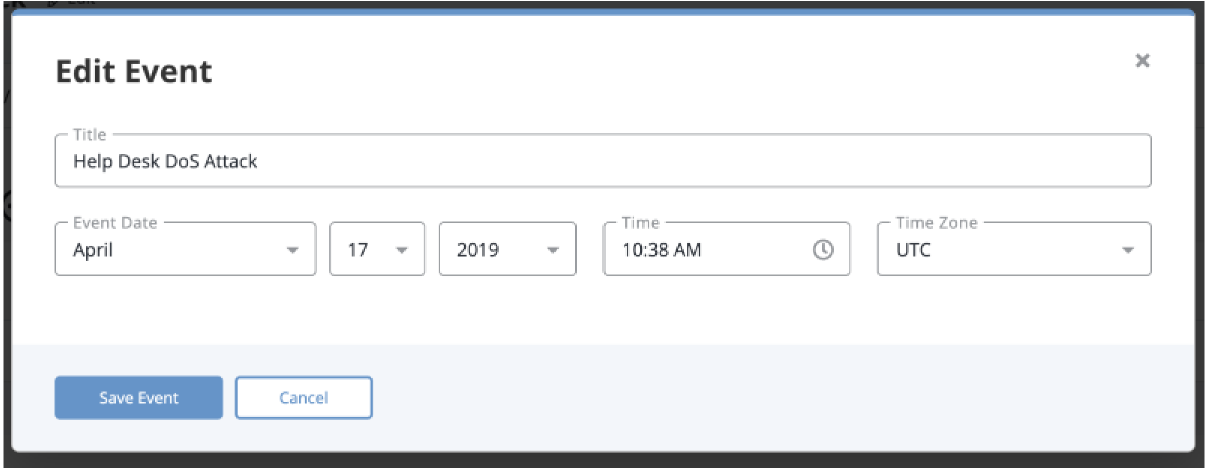
EVENT: DOS ATTACK

Created: 04/17/2019

Event Date: 04/17/2019 10:38am

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

   The Edit Event dialog box opens.



Edit Event

Title: Help Desk DoS Attack

Event Date: April 17 2019

Time: 10:38 AM

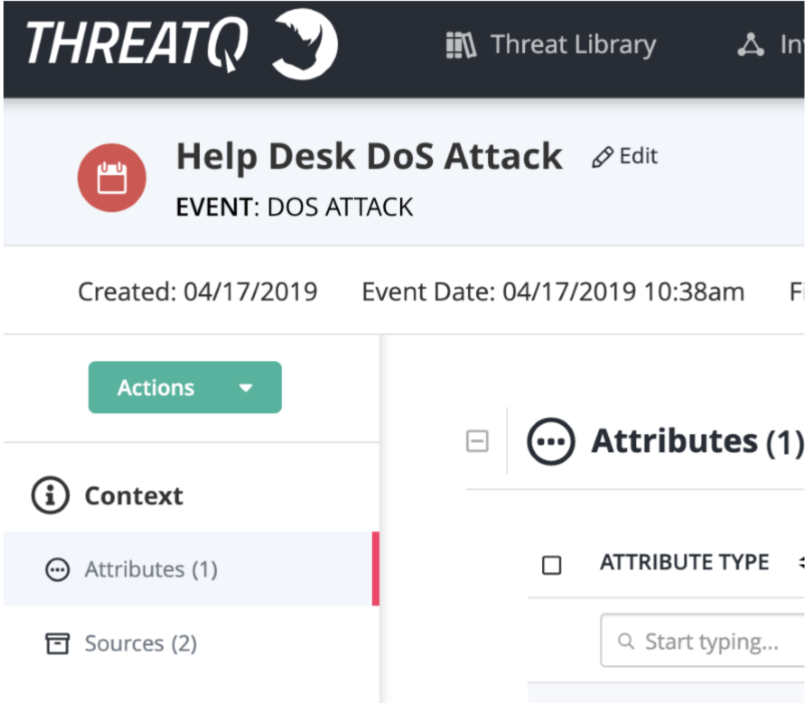
Time Zone: UTC

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

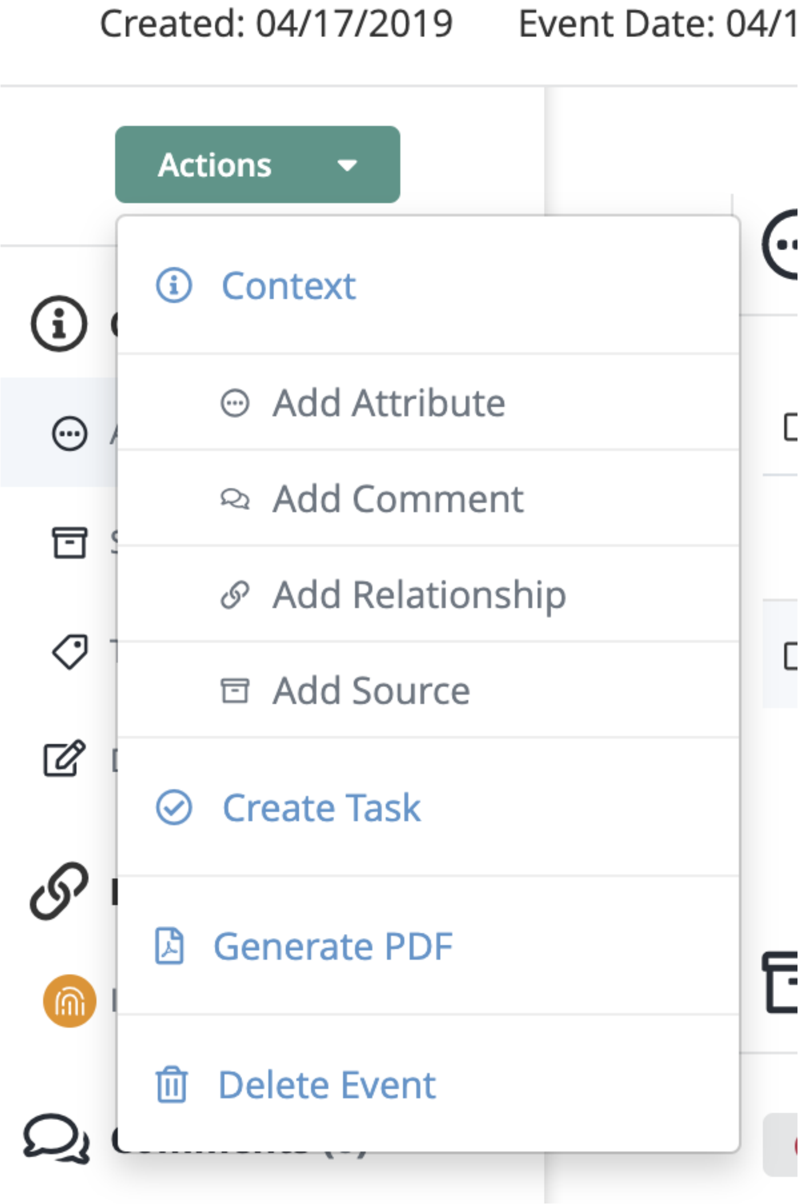
Deleting Events

1. Locate and click the event.
   The Events Details page opens.

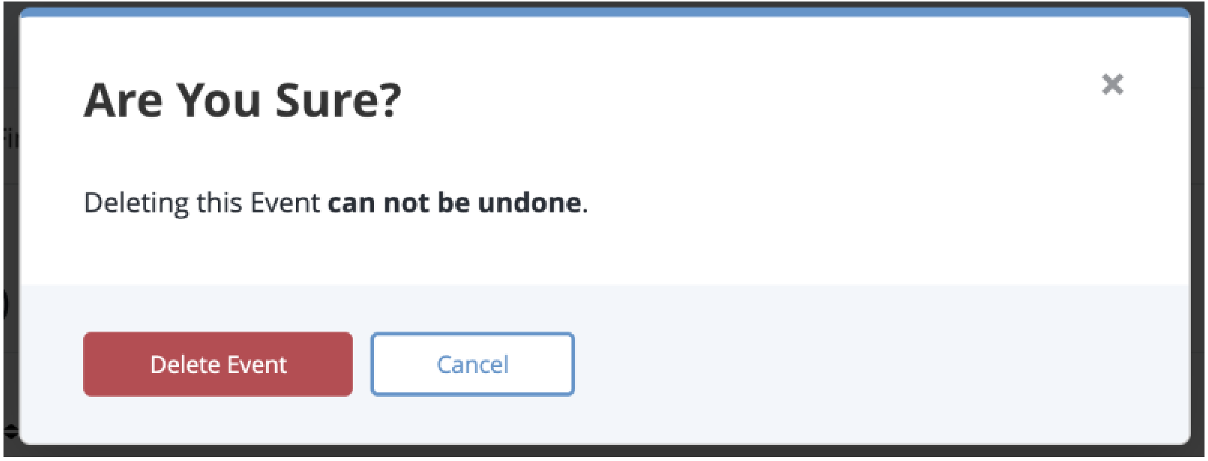
The Event Details page opens.



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



A confirmation dialog box appears.



Are You Sure?

Deleting this Event **can not be undone**.

3. Click on **Delete Event**.

Files

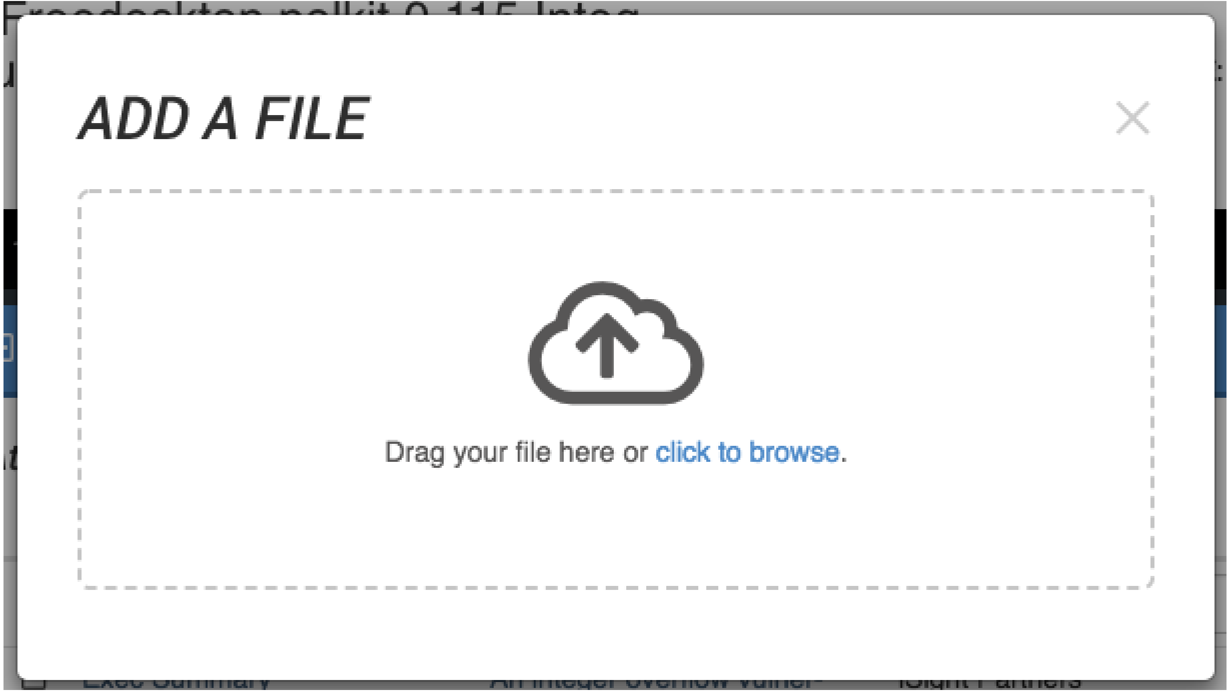
Files are received from various intelligence providers and may contain technical cybersecurity data such as Indicator, Adversary, and Malware samples.

Use the steps below to create, edit and delete a File.

Adding Files

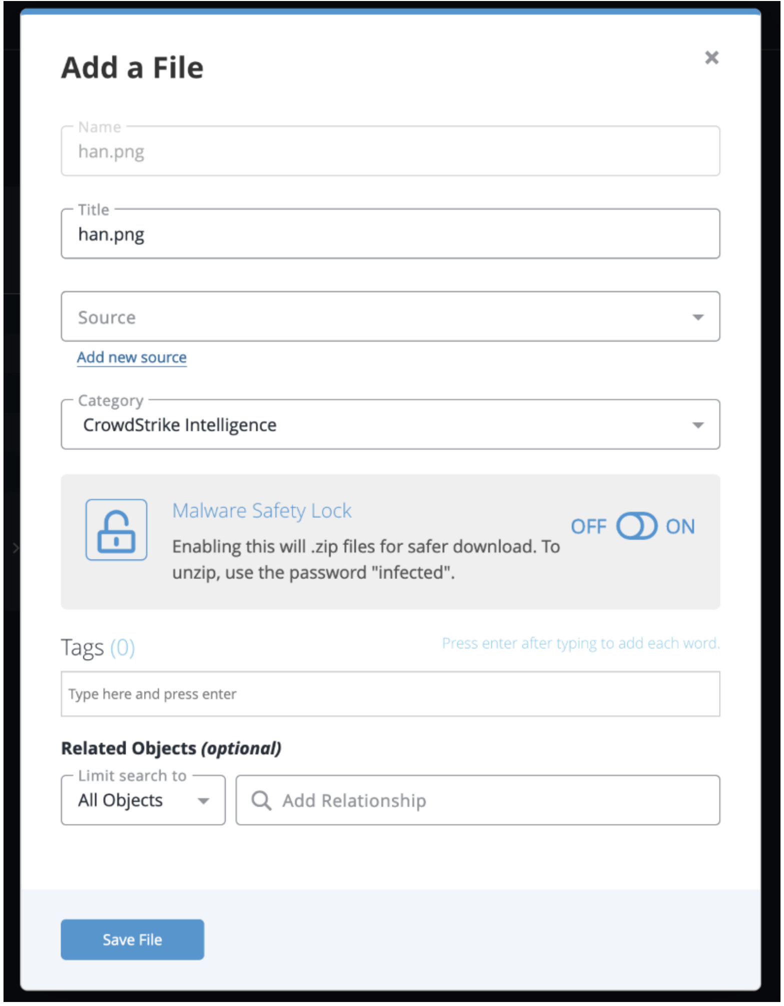
1. Click **Create** > **File**.

   The Add a File dialog box opens.



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

The Add a File Dialog box will update.


×
Source
Add new source
OFF
ON
Tags (0)
Press enter after typing to add each word.
Type here and press enter
Add Relationship
Save File

Add a File

Name: han.png

Title: han.png

Category: CrowdStrike Intelligence

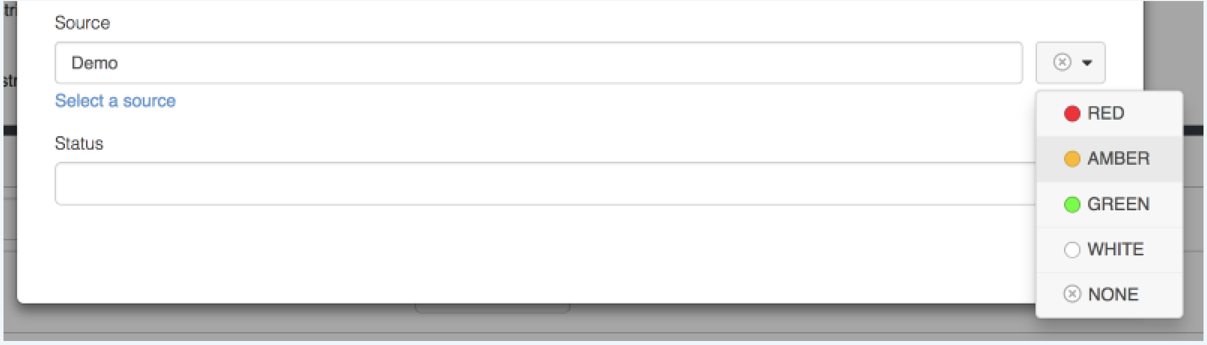
Malware Safety Lock

Enabling this will .zip files for safer download. To unzip, use the password "infected".

Related Objects *(optional)*

Limit search to: All Objects

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

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

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 will appear on the File's Details page.

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

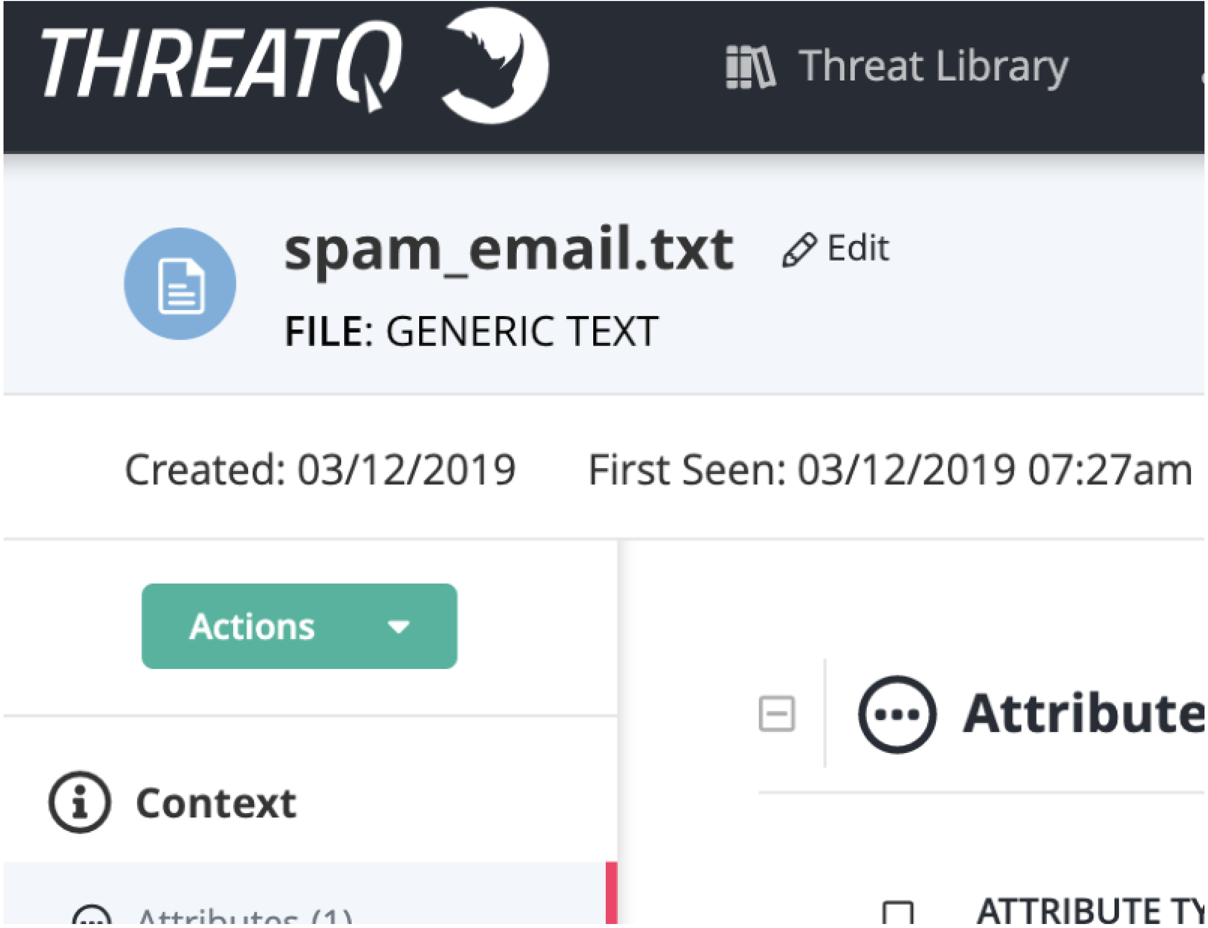
Adding Context

See the Object Details section and its topics for details on adding context to an object such as adding sources, attributes, and related objects.

Editing Files

1. Locate and click on the file.

The File Details page opens.



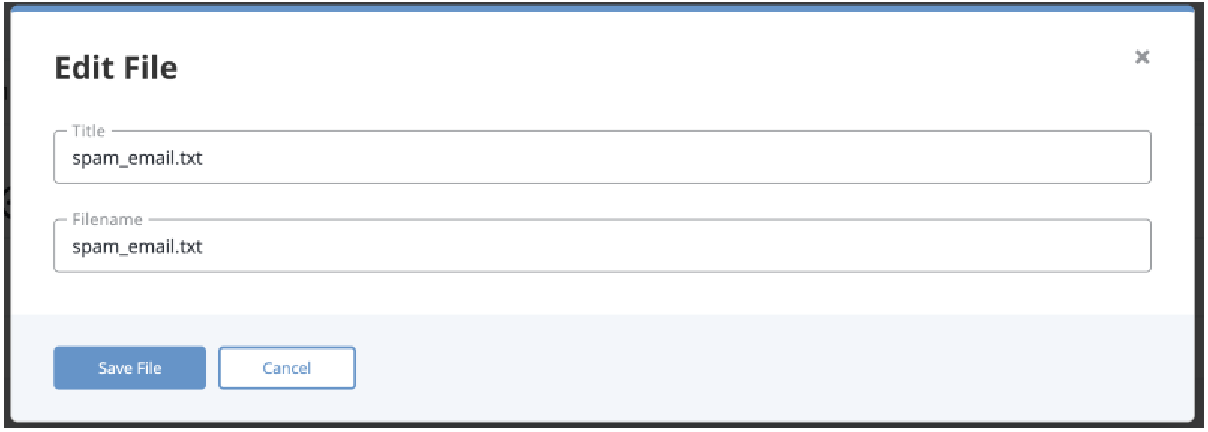
spam_email.txt

FILE: GENERIC TEXT

Created: 03/12/2019 First Seen: 03/12/2019 07:27am

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

   The Edit File dialog box opens.



Title: spam_email.txt

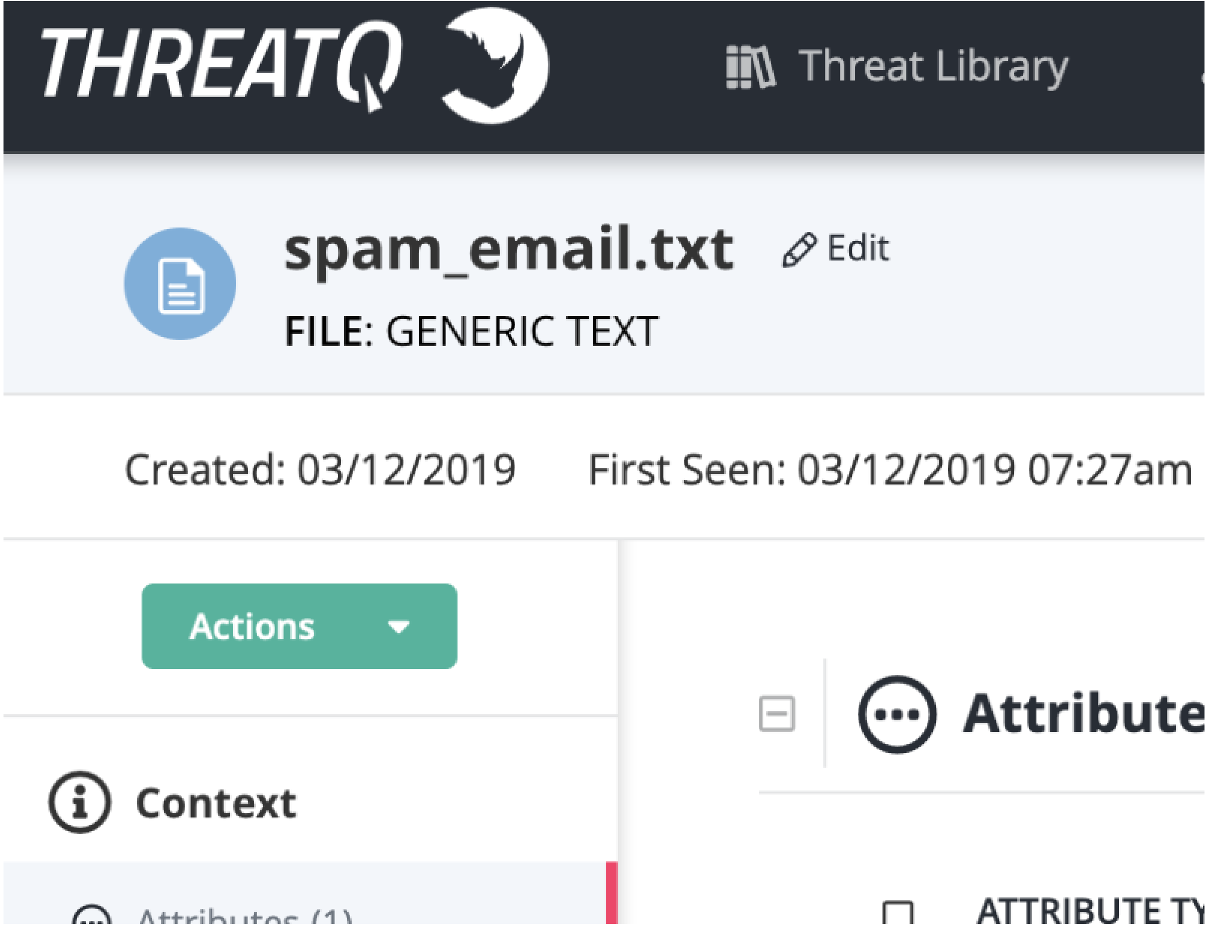
Filename: spam_email.txt

3. Make the desired change to the File Name.
4. Click on **Save File**.

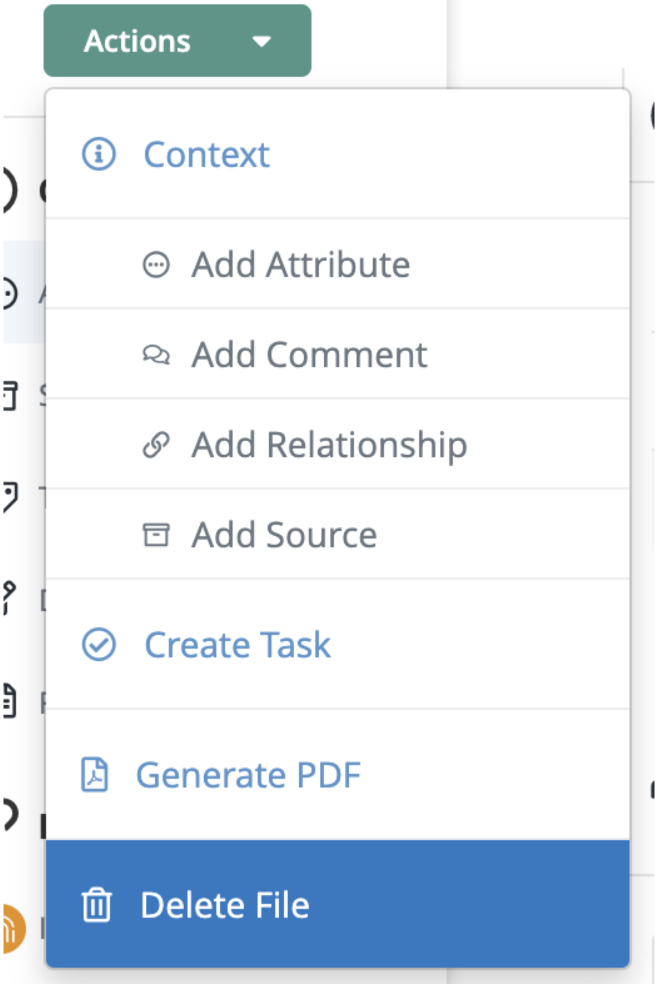
Deleting Files

1. Locate and click on the file.

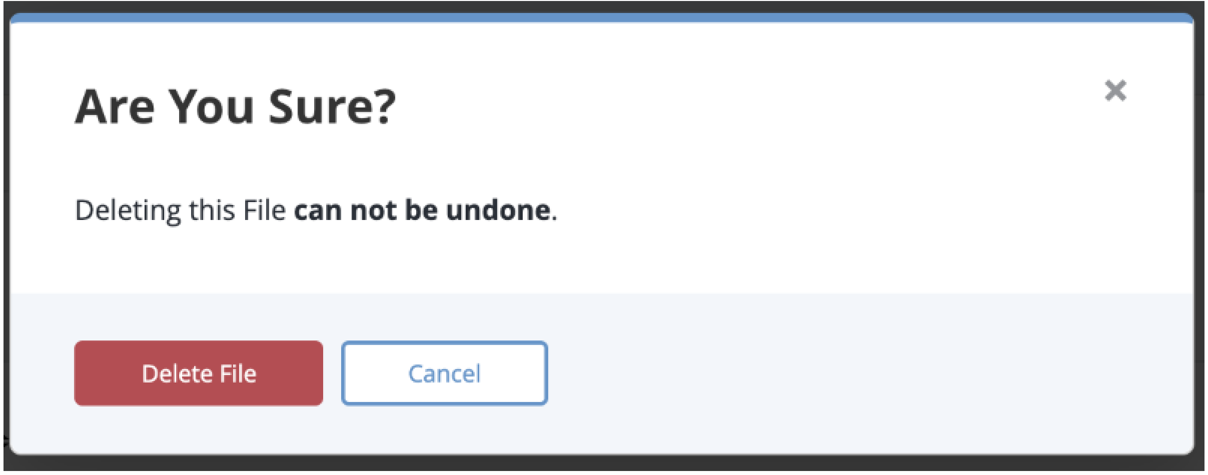
   The File Details page opens.



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



A confirmation dialog box appears.



Are You Sure?

Deleting this File **can not be undone**.

3. Click on **Delete File.**

Identities

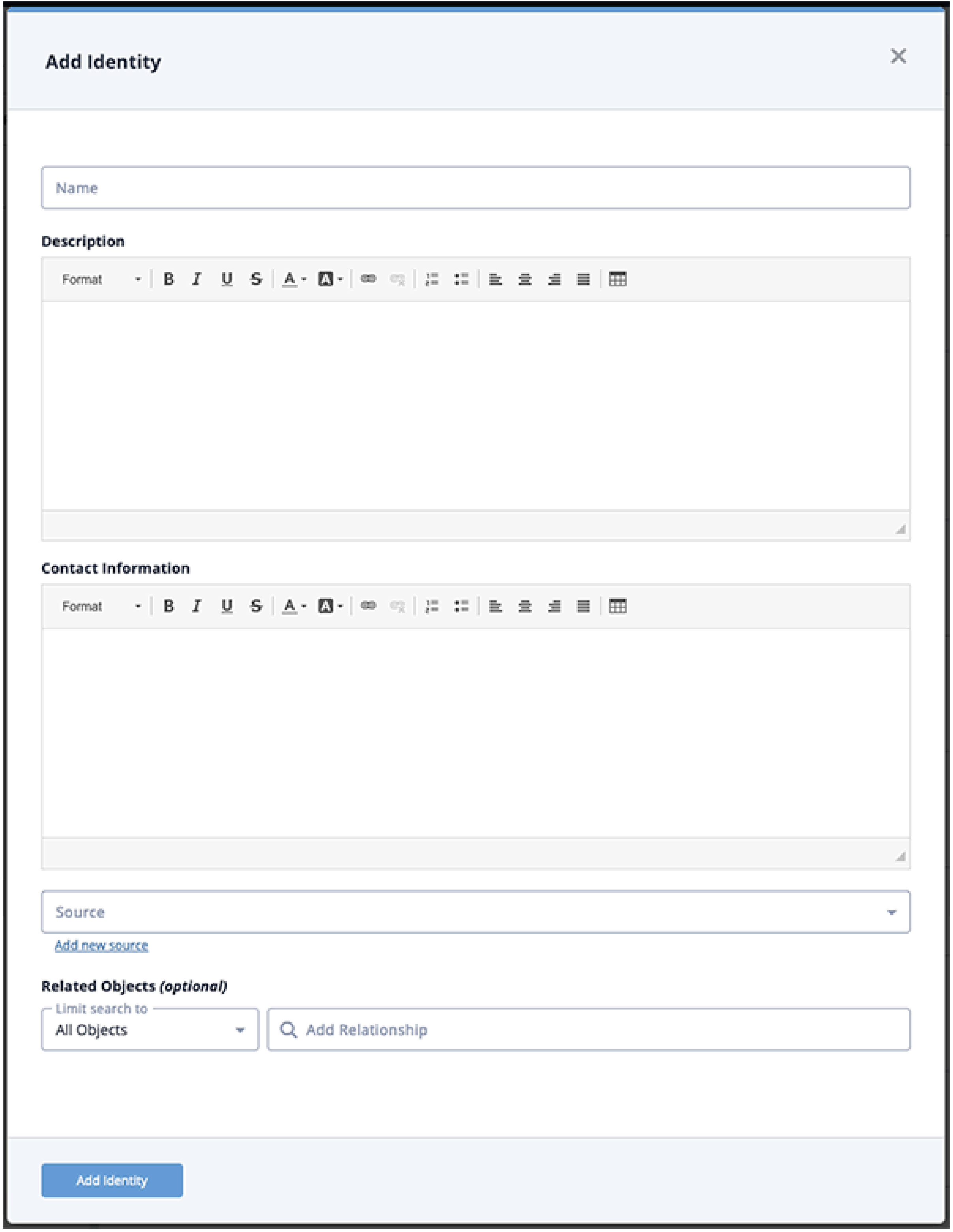
Identity contain basic identifying information for targeted groups such as information sources, threat actor identities, and targets of attack.

Use the steps below to create, edit and delete an Identity.

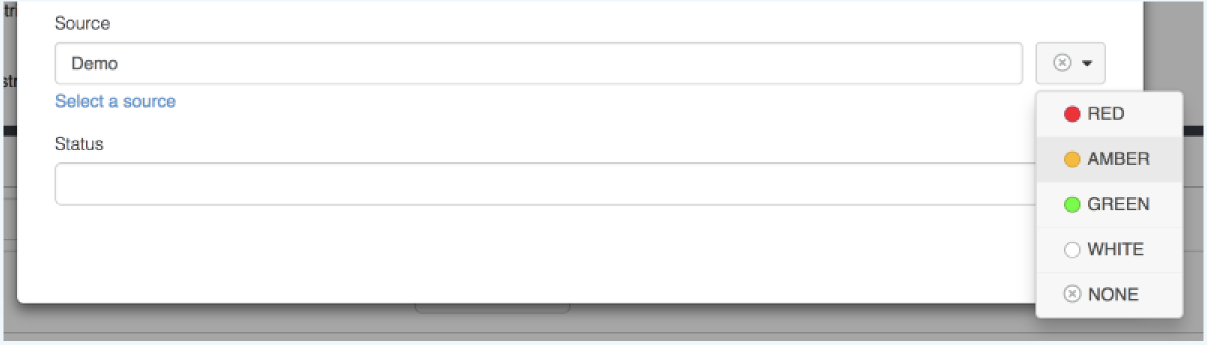
Adding an Identity

1. Go to **Create** > **Identity**.

The Add Identity dialog box opens.



2. Enter a **Name**.
3. Enter a **Description** in the field provided.
4. Enter the **Contact Information** in field provided.
5. Select a **Source** from the dropdown provided.

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

6. Select any **Related Objects** you need to link to the Identity. This field is optional.
7. Click **Add Identity**.

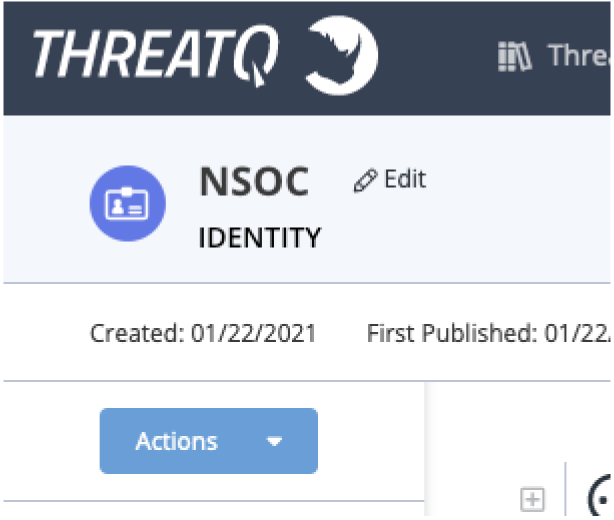
Adding Context

See the Object Details section and its topics for details on adding context to an object such as adding sources, attributes, and related objects.

Editing an Identity

1. Locate and click on the Identity.

   The Identity's detail page opens.

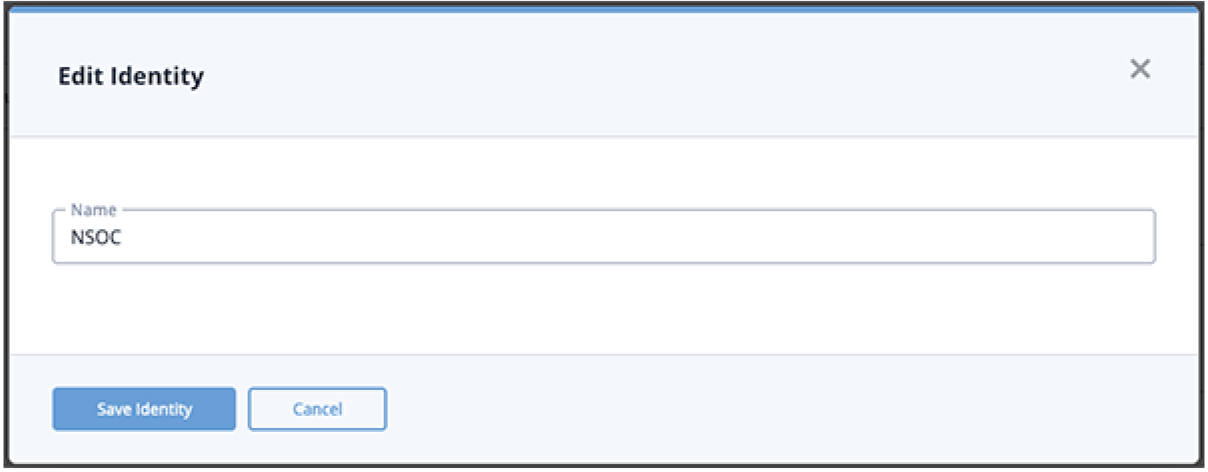
   NSOC

   IDENTITY

   Created: 01/22/2021 First Published: 01/22.

2. Click on **Edit** next to the Identity's name.

The Edit Identity dialog box opens.



Edit Identity

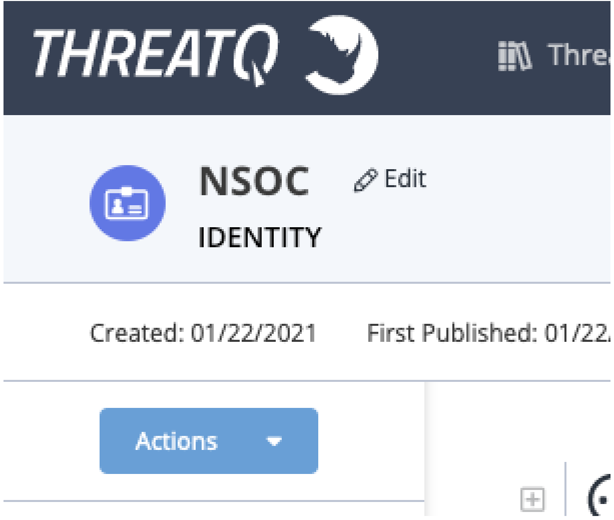
Name: NSOC

3. Make the desired change to the Identity's name and click **Save Identity**.

Deleting an Identity

1. Locate and click on the Identity.

   The Identity's details page opens.

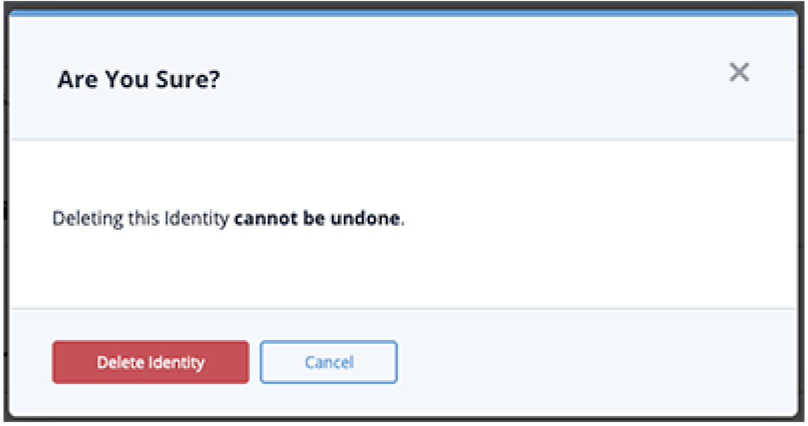


NSOC
IDENTITY

Created: 01/22/2021

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

A confirmation dialog box appears.



Are You Sure?

Deleting this Identity **cannot be undone.**

3. Click on **Delete Identity**.

Incidents

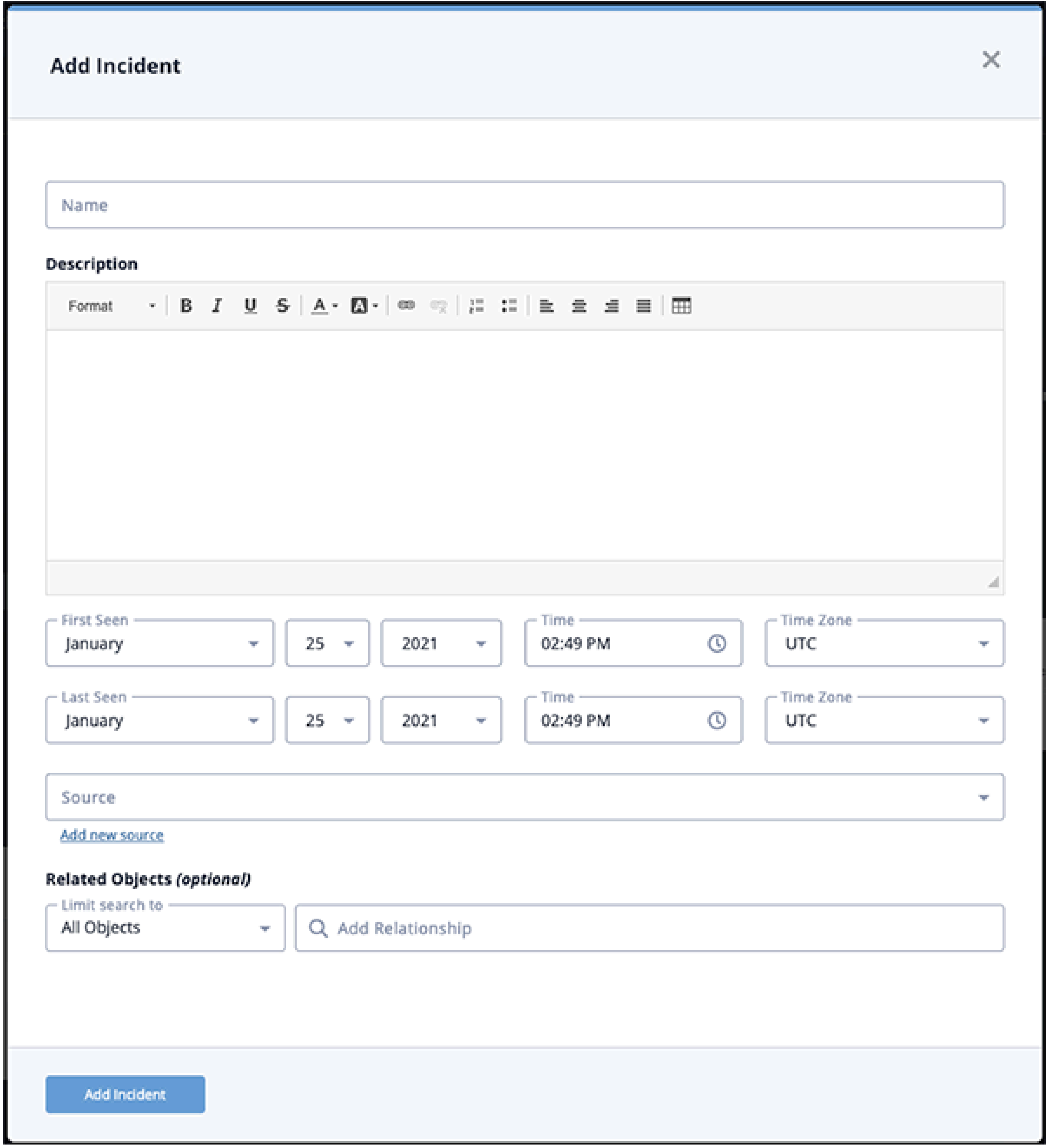
Incident are records of any violation of an organization's established security/network policy that may compromise security, integrity, or general access.

Use the steps below to create, edit and delete an Incident.

Adding an Incident

1. Go to **Create** > **Incident**.

The Add Incident dialog box opens.



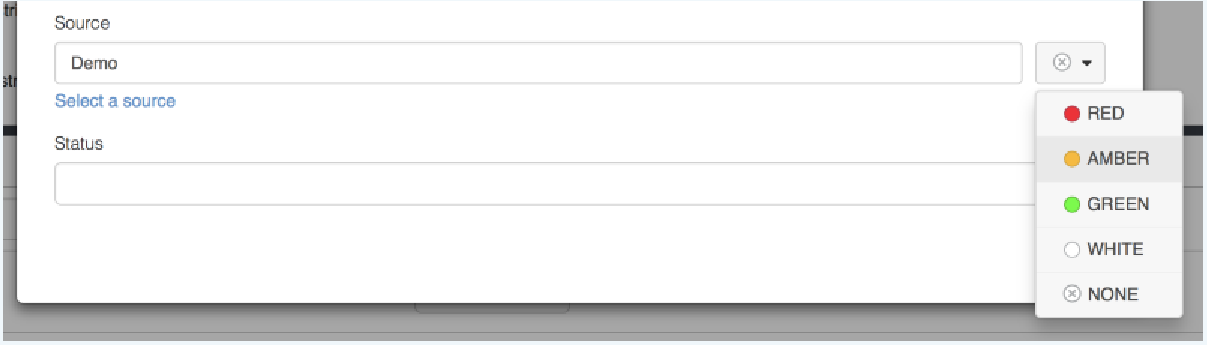
First Seen: January 25 2021 Time: 02:49 PM Time Zone: UTC

Last Seen: January 25 2021 Time: 02:49 PM Time Zone: UTC

Limit search to: All Objects

2. Enter a **Name**.
3. Enter a **Description** in the field provided.
4. Select the **First Seen** and **Last Scene** times.
5. Select a **Source** from the dropdown provided.

> You can also click the **Add a New Source** option if the desired source is not listed in the dropdown list . If administrators have enabled TLP view settings, you can select a TLP label for the new source in the dropdown list provided. See the

> Traffic Light Protocol (TLP) topic for more information on TLP schema.
>
> 
>
> Source: Demo
>
> Status:
>
>

6. Select any **Related Objects** you need to link to the Incident. This field is optional.
7. Click **Add Incident**.

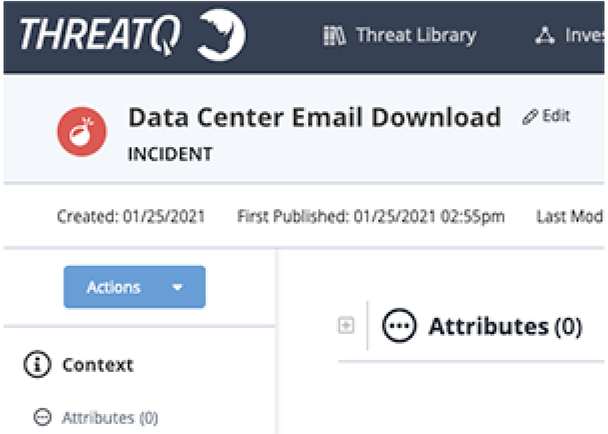
Adding Context

See the Object Details section and its topics for details on adding context to an object such as adding sources, attributes, and related objects.

Editing an Incident

1. Locate and click on the Incident.

   The Incident's detail page opens.

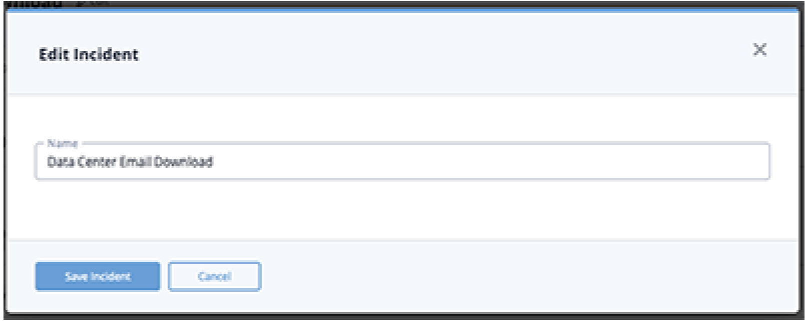
   Data Center Email Download

   INCIDENT

   Created: 01/25/2021 First Published: 01/25/2021 02:55pm

2. Click on **Edit** next to the Incident's name.

The Edit Incident dialog box opens.



Edit Incident

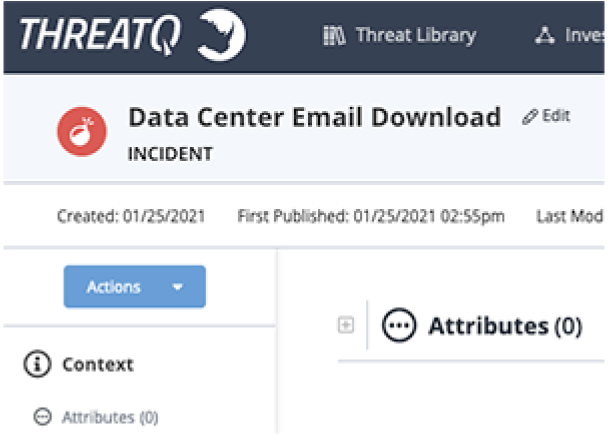
Name: Data Center Email Download

3. Make the desired change to the Incident's name and click **Save Incident**.

Deleting an Incident

1. Locate and click on the Incident.

   The Incident's details page opens.



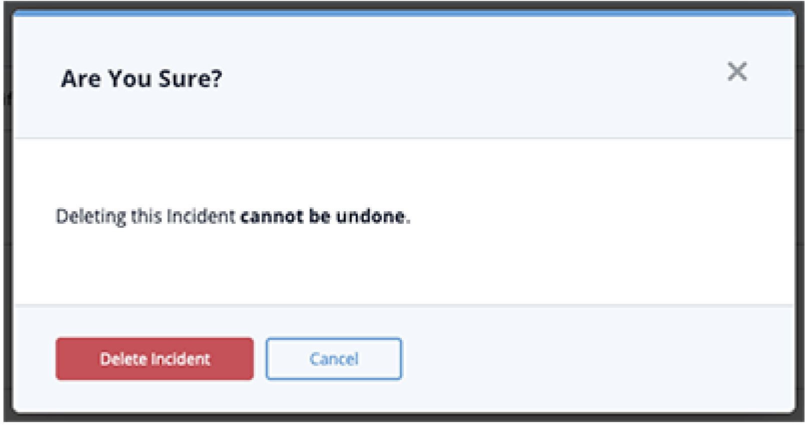
Data Center Email Download

INCIDENT

Created: 01/25/2021 First Published: 01/25/2021 02:55pm Last Mod

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

   A confirmation dialog box appears.



Are You Sure?

Deleting this Incident **cannot be undone**.

3. Click on **Delete Incident**.

Indicators

Indicator are information that describes or identifies methods used to defeat security controls, exploit vulnerabilities, and gain unauthorized access to an internal network. Indicators can also describe malicious reconnaissance to gather technical information, malicious cyber command and control, and any other attribute of cyber security whose disclosure is prohibited by law.

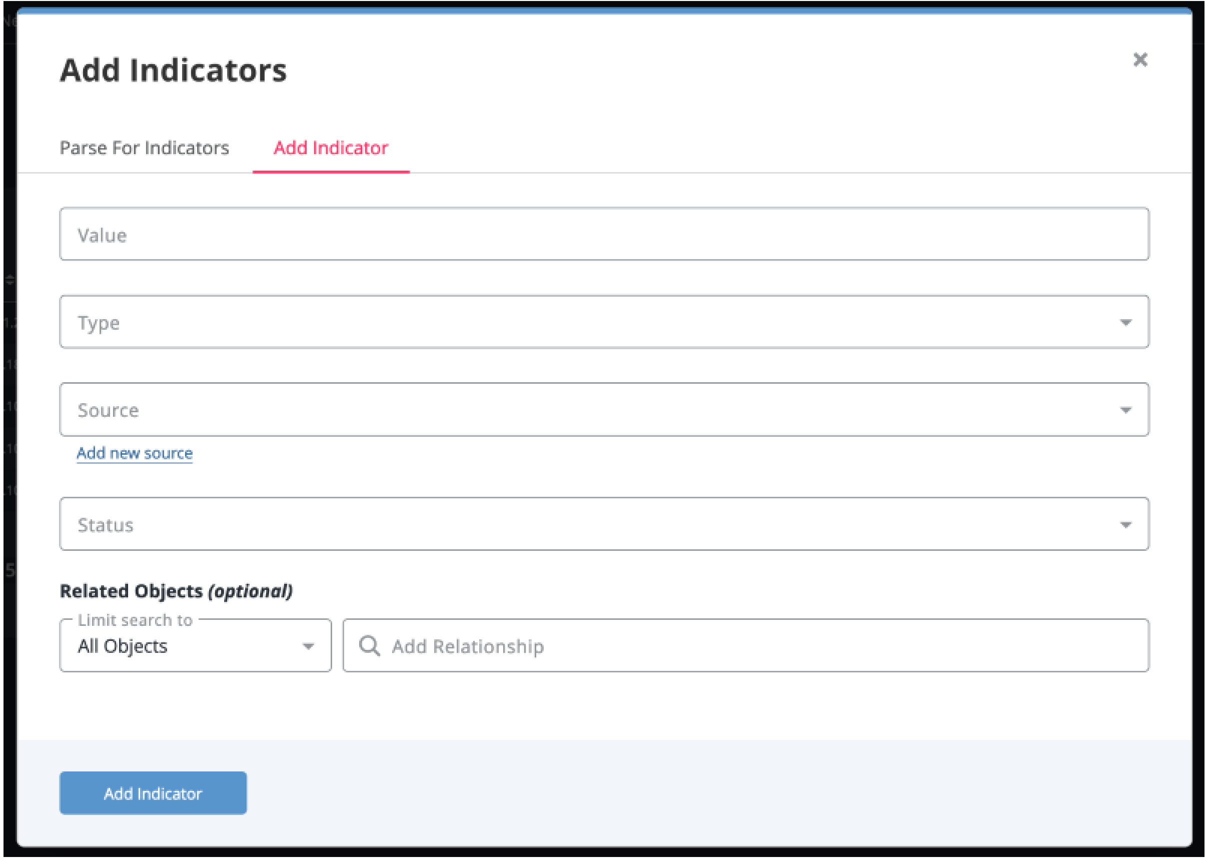
Indicators can be scored to allow you to apply weighting using contextual information, such as sources, attributes, and indicator types, as they are added to ThreatQ. You can also set a manual score per indicator.

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.

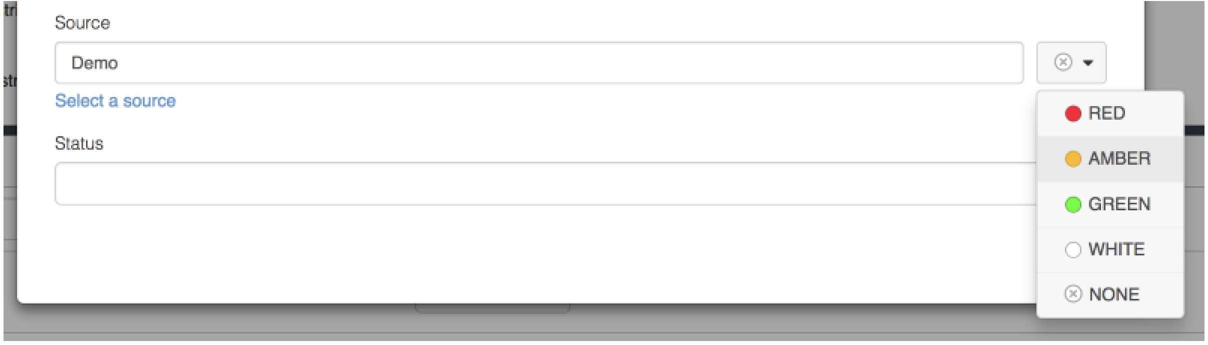
Adding an Indicator

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

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



Source

Demo

Select a source

Status

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**.

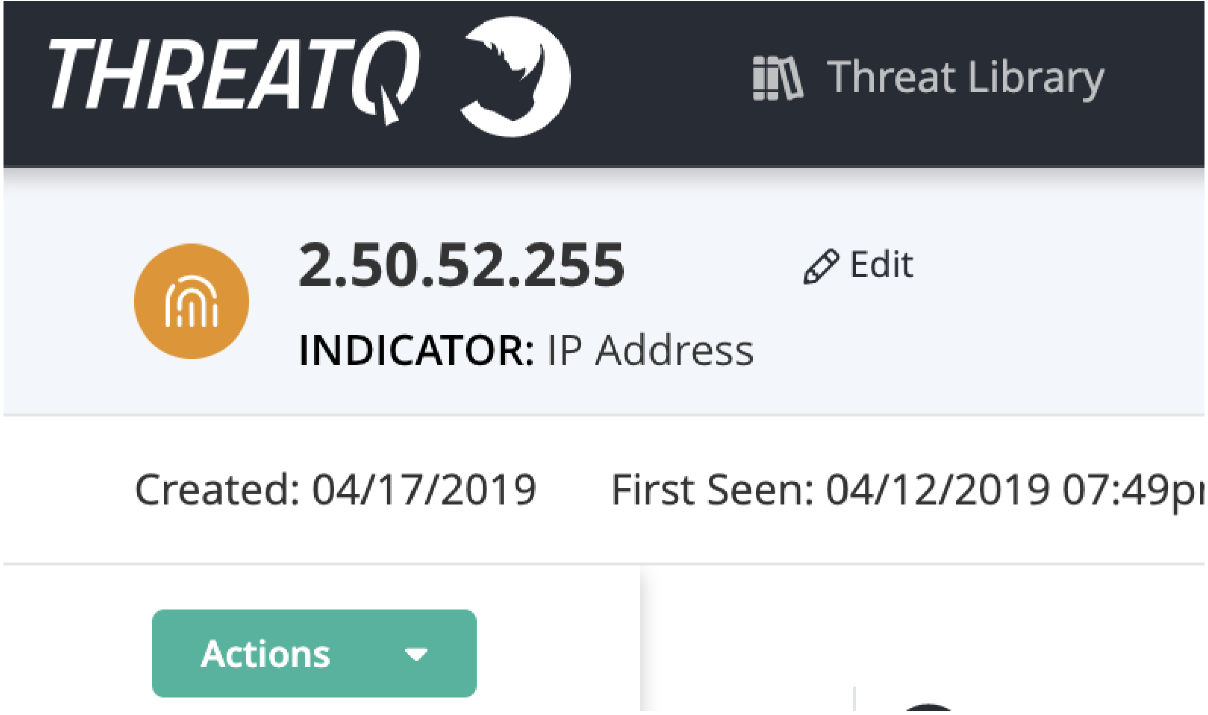
Adding Context

See the Object Details section and its topics for details on adding context to an object such as adding sources, attributes, and related objects.

Editing Indicators

1. Locate and click on the indicator.

The Indicator Details page opens.



2.50.52.255

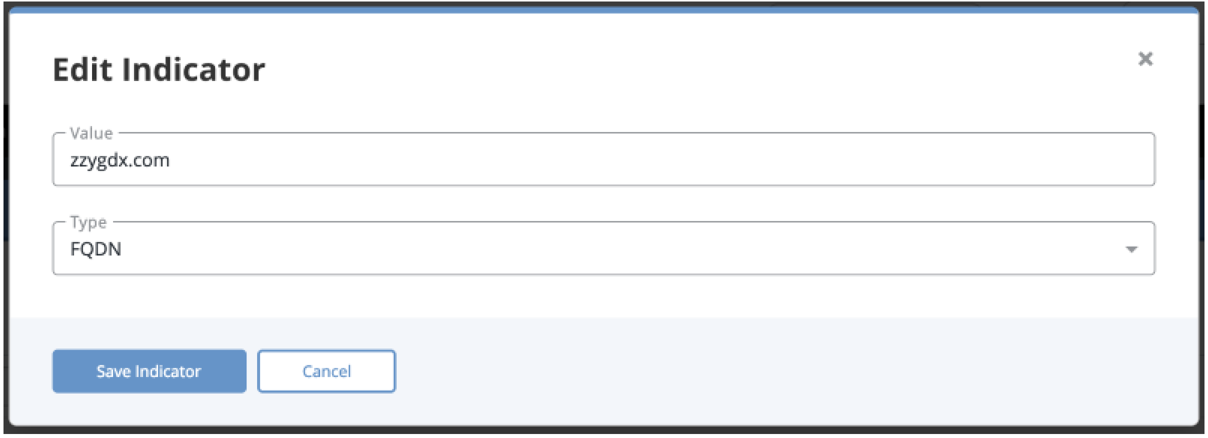
INDICATOR: IP Address

Created: 04/17/2019

First Seen: 04/12/2019 07:49p

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

   The Edit Indicator dialog box opens.



Edit Indicator

Value: zzygdx.com

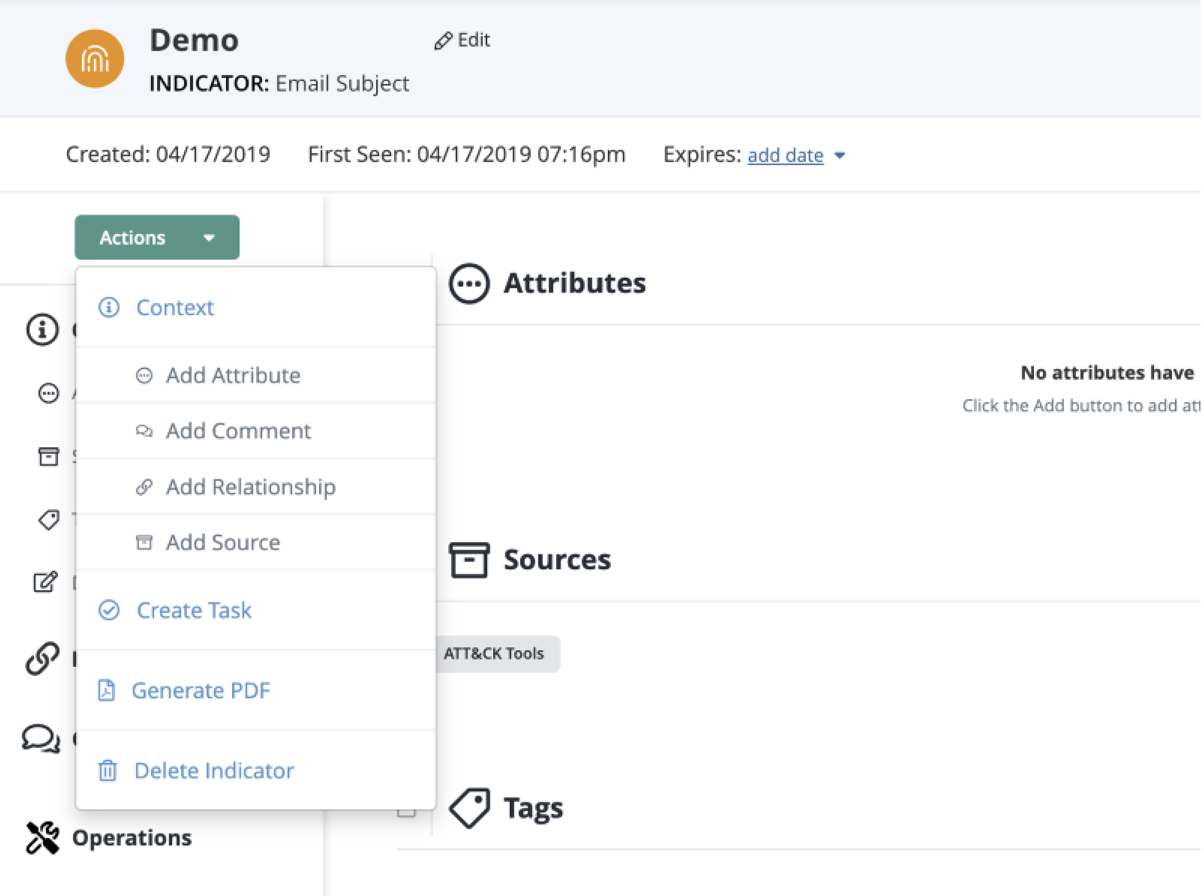
Type: FQDN

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

Deleting an Indicator

1. Locate and click on the Indicator.

The Indicator Details page opens.



Demo

INDICATOR: Email Subject

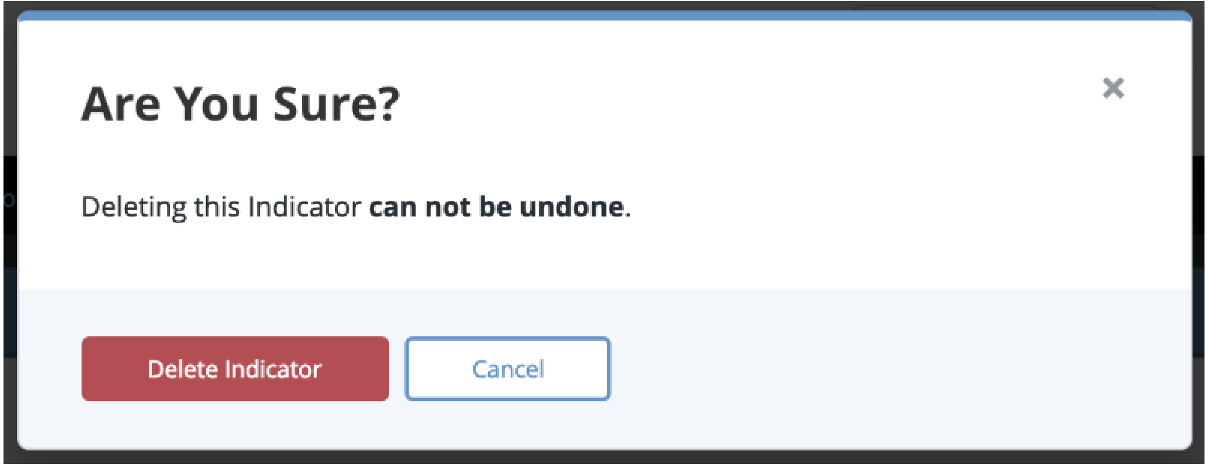
Created: 04/17/2019 First Seen: 04/17/2019 07:16pm Expires: add date

No attributes have

Click the Add button to add at

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

   A confirmation dialog box appears.



Are You Sure?

Deleting this Indicator **can not be undone**.

3. Click on **Delete Indicator**.

Parsing for Indicators

ThreatQ gives you the option to import a file, parse it for indicators, and add those indicators to your Threat Library. During the import process you can assign a source, tag, and a relationship to the imported indicators.

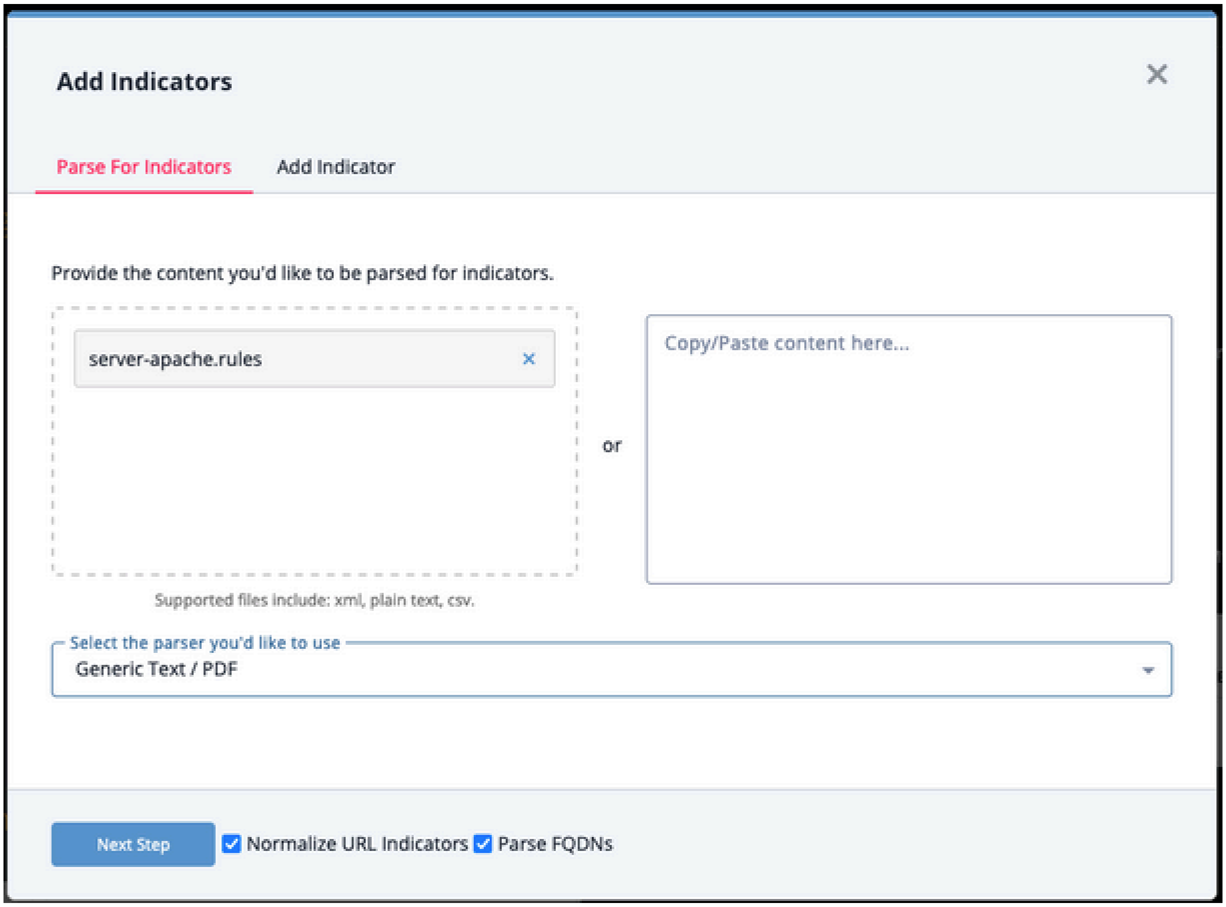
> See the Importing Indicators via CSV topic for specific instructions and examples on parsing indicators from a .csv file.

Selecting a File to Parse

1. Click the **Create** button, located at the top-right of the menu bar, and select the **Indicator Parser** option.

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

The Add Indicators dialog box will open.



Provide the content you'd like to be parsed for indicators.

server-apache.rules

or

Copy/Paste content here...

Supported files include: xml, plain text, csv.

Select the parser you'd like to use: Generic Text / PDF

☑ Normalize URL Indicators ☑ Parse FQDNs

2. Select the file to upload by either:
   - Dragging and dropping the file into the dialog window
   - Clicking on the Click to Browse option and locating the file on your local device
   - Copying and pasting the file's contents in the text field provided.
3. Select the type of parser to use. Options include
   - Cuckoo
   - FireEye Analysis
   - Generic Text / PDF
   - Palo Alto Networks WildFire XML
   - ThreatAnalyzer Analysis
   - ThreatQ CSV File - see the Importing Indicators via CSV topic for specific instructions on using this parser.
4. Use the checkboxes to select your parsing options:

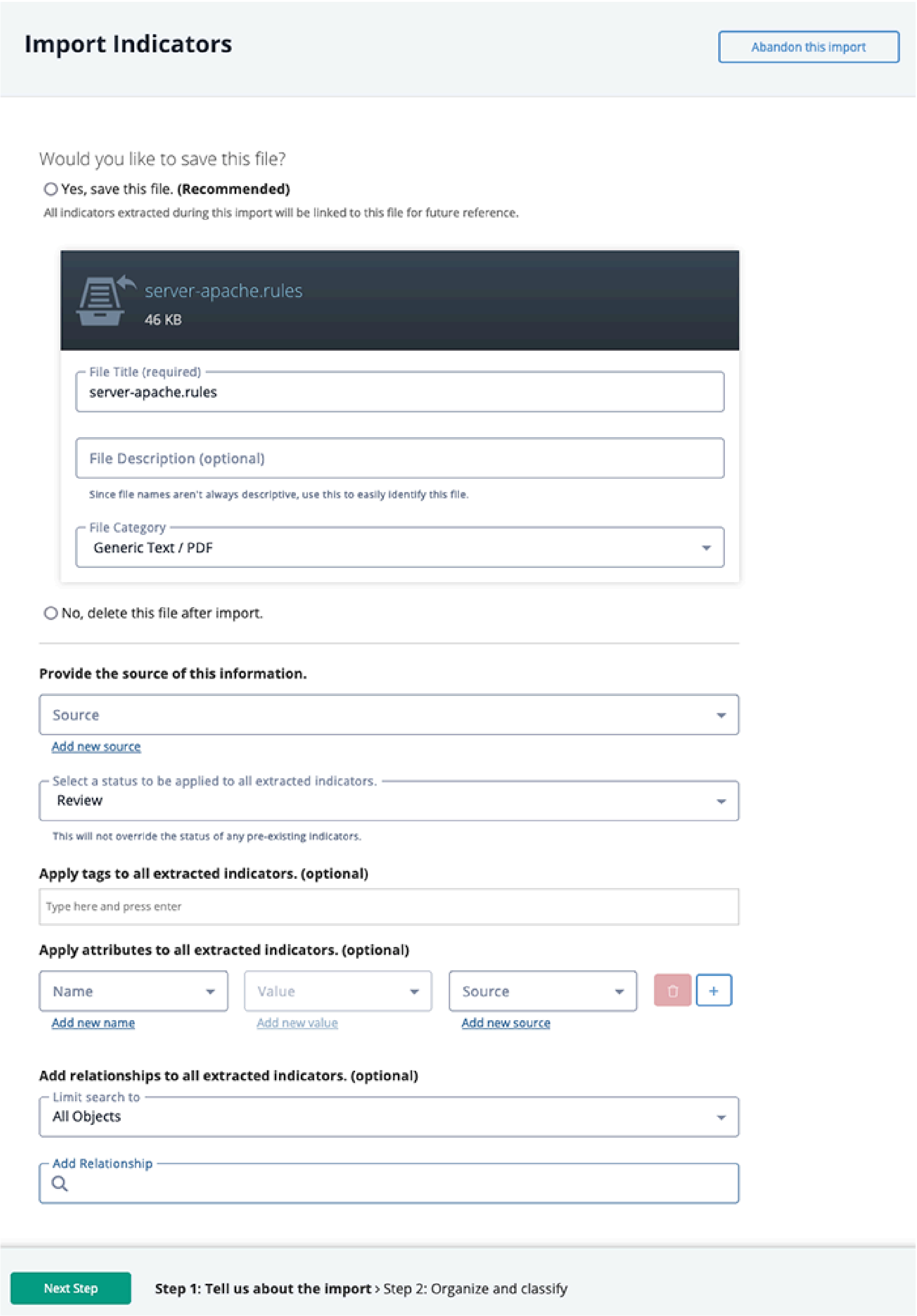
OPTION	DESCRIPTION

Normalize URL Indicators	When checked, parsed URLs will have ports and leading protocol adjusted, as well as unneeded quotes and spaces removed. Normalization also adds attributes for protocol and query string. See the Indicator URL Normalization topic for more details.
Parse FQDNs	When checked, the Indicator Parser will parse FQDNs from the text and derive FQDN indicators from URLs in the text. **Example (checked)**: URL: https://tqexample.com/table.jspa?query_string_example Indicators created: ◦ tqexample.com/table.jspa (the URL) ◦ tqexample.com (the derived FQDN from the URL) When unchecked, the Indicator Parser will not generate FQDN indicators from the parsed text. **Example (unchecked)**: URL: https://tqexample.com/table.jspa?query_string_example Indicator created: ◦ tqexample.com/table.jspa (the URL)

> Administrators can configure the default setting for these options under the General Tab on the System Configurations page. See the Indicator Parsing Presets topic for more details.

5. Click on **Next Step**.

   The Step 1 - Import Indicators form will load.



Would you like to save this file?

○ Yes, save this file. **(Recommended)**

All indicators extracted during this import will be linked to this file for future reference.

server-apache.rules
46 KB

File Title (required): server-apache.rules

File Description (optional)

Since file names aren't always descriptive, use this to easily identify this file.

File Category: Generic Text / PDF

○ No, delete this file after import.

Provide the source of this information.

Source

Add new source

Select a status to be applied to all extracted indicators.: Review

This will not override the status of any pre-existing indicators.

Apply tags to all extracted indicators. (optional)

Type here and press enter

Apply attributes to all extracted indicators. (optional)

Name | Value | Source

Add new name | Add new value | Add new source

Add relationships to all extracted indicators. (optional)

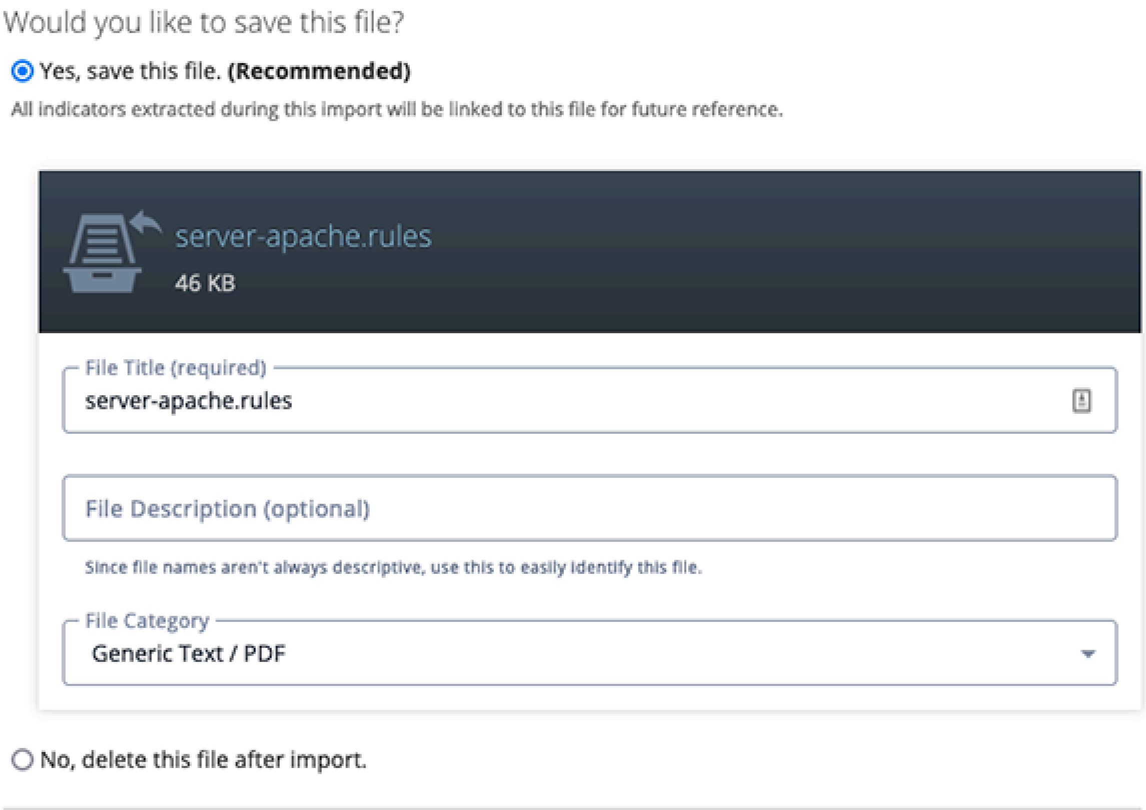
Limit search to: All Objects

Add Relationship

Next Step
Step 1: Tell us about the import › Step 2: Organize and classify

Step 1 - Import Indicators Settings

6. Select whether or not to save the import file. Saving the file will result in all extracted indicators being linked to the file for reference. If you select **Yes**, review the **File Title** and **File Category**. You can also add an option **File Description**.



Would you like to save this file?

● Yes, save this file. **(Recommended)**

All indicators extracted during this import will be linked to this file for future reference.

server-apache.rules

46 KB

File Title (required): server-apache.rules

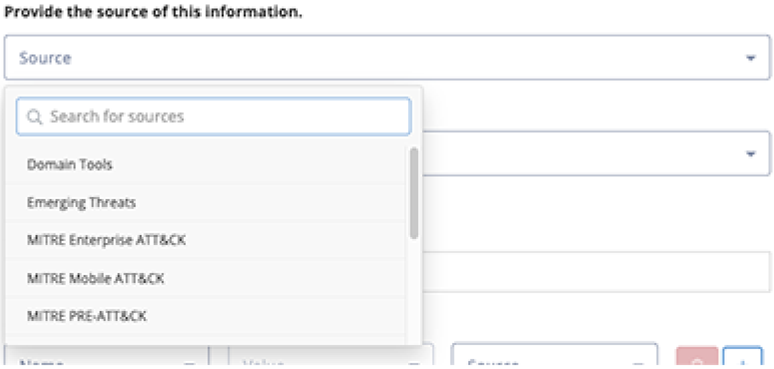
File Description (optional)

Since file names aren't always descriptive, use this to easily identify this file.

File Category: Generic Text / PDF

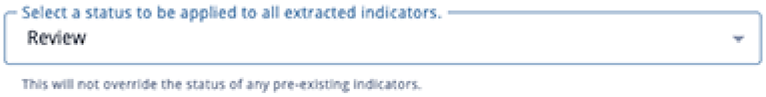
○ No, delete this file after import.

7. Select a **Source** for the extracted indicators.



Provide the source of this information.

8. Select a **Status** for the extracted indicators.



Select a status to be applied to all extracted indicators.: Review

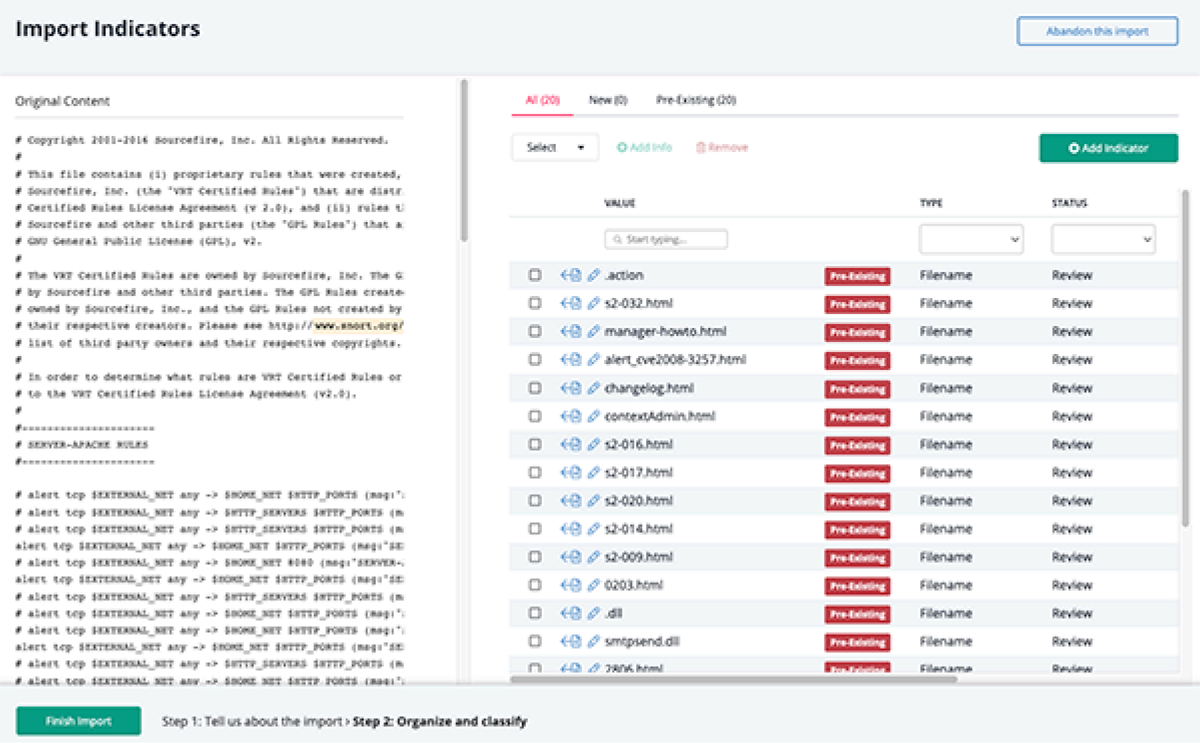
This will not override the status of any pre-existing indicators.

9. Enter any **Tags** to apply to the extracted indicators. This field is optional.
10. Select any attribute, attribute value, and attribute source to apply to the extracted indicators.
11. Add **Relationships** for the extracted indicators.

> If you enter an object name that is not found, you can click the **Create** link to add the new object. If you limited your search to a specific object type, you are linked to the corresponding form. For example, if you limit your search to Adversaries, the **Create** link opens the Add An Adversary form. If you leave the **Limit search to** field set to All Objects, you can select the object type you want to create from a drop-down list.

12. Click on **Next Step**.

    The Organize and Classify form will load.



```
# Copyright 2001-2016 Sourcefire, Inc. All Rights Reserved.
#
# This file contains (i) proprietary rules that were created,
# Sourcefire, Inc. (the 'VRT Certified Rules') that are distr
# Certified Rules License Agreement (v 2.0), and (ii) rules t
# Sourcefire and other third parties (the 'GPL Rules') that a
# GNU General Public License (GPL), v2.
#
# The VRT Certified Rules are owned by Sourcefire, Inc. The G
# by Sourcefire and other third parties. The GPL Rules create
# owned by Sourcefire, Inc., and the GPL Rules not created by
# their respective creators. Please see http://www.snort.org/
# list of third party owners and their respective copyrights.
#
# In order to determine what rules are VRT Certified Rules or
# to the VRT Certified Rules License Agreement (v2.0).
#
#---------------------
# SERVER-APACHE RULES
#---------------------

# alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:'
# alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (m
# alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (m
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:'SE
# alert tcp $EXTERNAL_NET any -> $HOME_NET 8080 (msg:'SERVER-
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:'SE
# alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (m
# alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:'
# alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:'
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:'SE
# alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (m
# alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:'
```

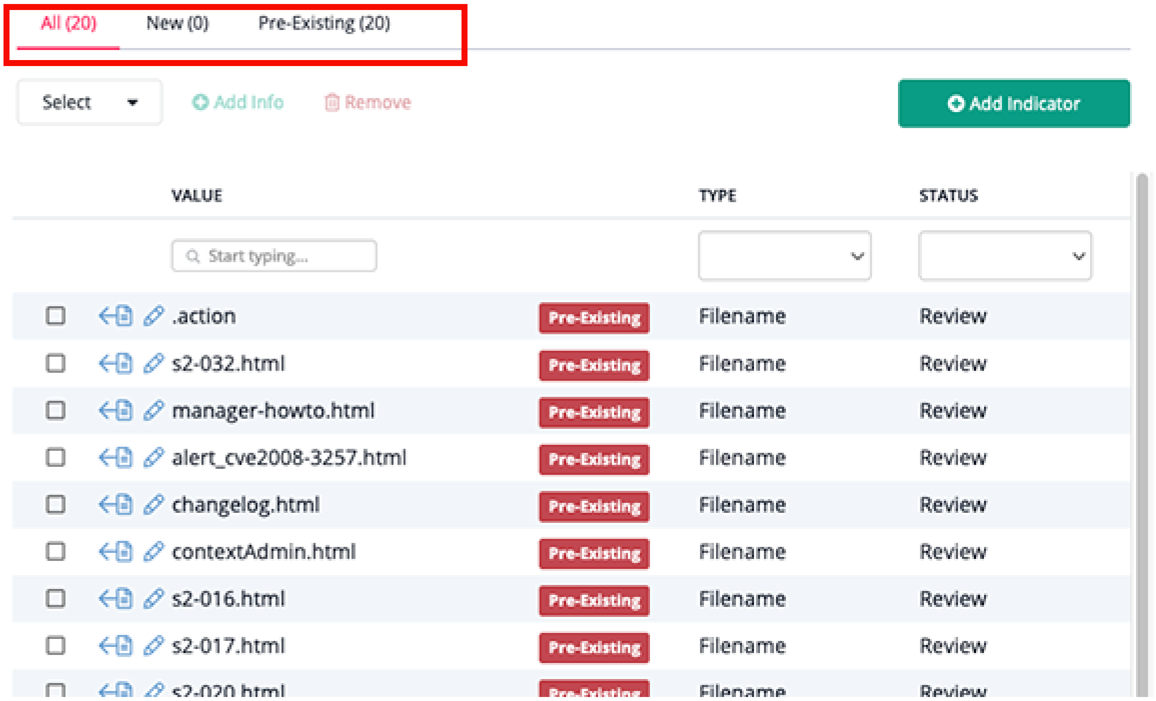
	VALUE		TYPE	STATUS
☐	.action	Pre-Existing	Filename	Review
☐	s2-032.html	Pre-Existing	Filename	Review
☐	manager-howto.html	Pre-Existing	Filename	Review
☐	alert_cve2008-3257.html	Pre-Existing	Filename	Review
☐	changelog.html	Pre-Existing	Filename	Review
☐	contextAdmin.html	Pre-Existing	Filename	Review
☐	s2-016.html	Pre-Existing	Filename	Review
☐	s2-017.html	Pre-Existing	Filename	Review
☐	s2-020.html	Pre-Existing	Filename	Review
☐	s2-014.html	Pre-Existing	Filename	Review
☐	s2-009.html	Pre-Existing	Filename	Review
☐	0203.html	Pre-Existing	Filename	Review
☐	.dll	Pre-Existing	Filename	Review
☐	smtpsend.dll	Pre-Existing	Filename	Review
☐	2806.html	Pre-Existing	Filename	Review

Step 2 - Organize and Classify

13. You can review the original content of the file and the extracted indicators' information.

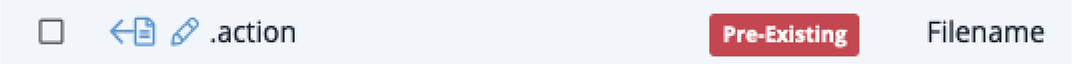
    ### Filtering Extracted Indicators List

    - The top tabs allow you to filter the list of indicators by New and Pre-existing. This allows you isolate any indicators that already exist in the platform.



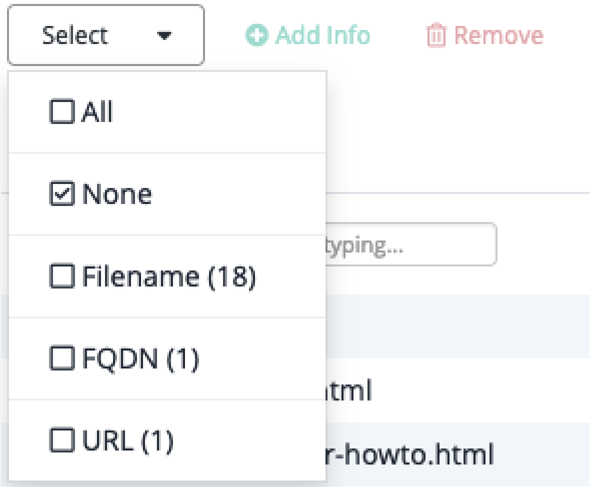
	VALUE		TYPE	STATUS
☐	.action	Pre-Existing	Filename	Review
☐	s2-032.html	Pre-Existing	Filename	Review
☐	manager-howto.html	Pre-Existing	Filename	Review
☐	alert_cve2008-3257.html	Pre-Existing	Filename	Review
☐	changelog.html	Pre-Existing	Filename	Review
☐	contextAdmin.html	Pre-Existing	Filename	Review
☐	s2-016.html	Pre-Existing	Filename	Review
☐	s2-017.html	Pre-Existing	Filename	Review
☐	s2-020.html	Pre-Existing	Filename	Review

Pre-existing indicators will also be marked with a Pre-existing label in the list.



☐ .action Pre-Existing Filename

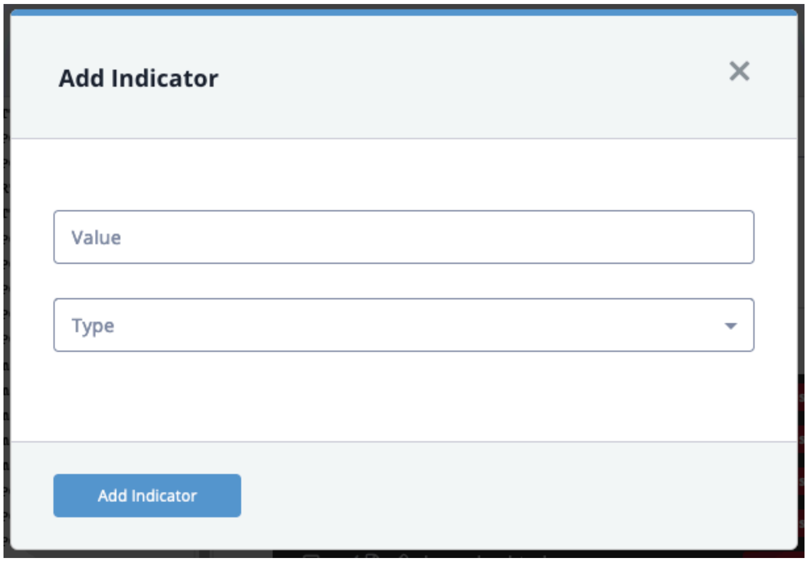
- You can click on the **Select** dropdown to automatically select indicators by sub-type.



> ⚠ Selecting **All** will select all extracted indicators, not just the ones in your current filtered view (New, Pre-Existing).

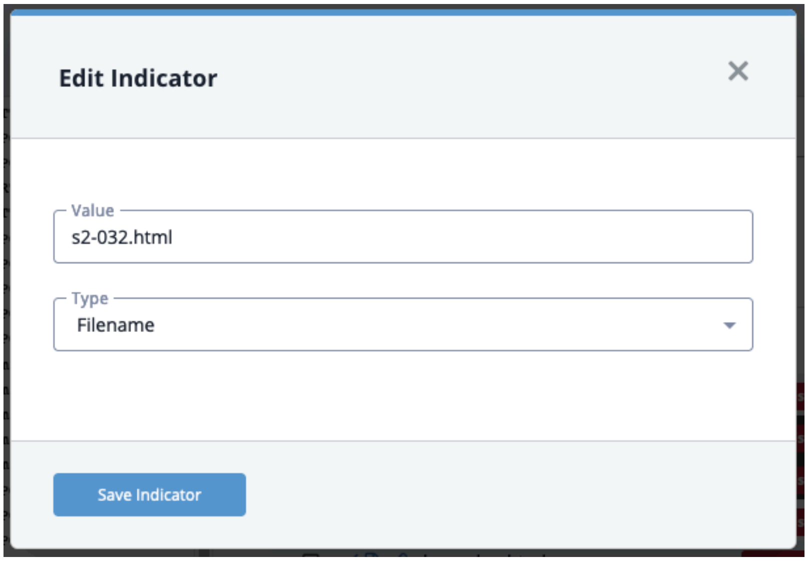
Adding Indicators

- You can click on the **Add Indicator** option, located to the top-right of the list, to add an indicator to the extracted list. You can add further context to the new indicator using the Editing Extracted Indicators actions listed below.



Editing Extracted Indicators

- Clicking on the ⇐ icon will show you where the indicator appeared in the Original Content window.
- Clicking on the ✎ icon will open the **Edit Indicator** dialog box and allow you to edit the indicator value and indicator sub-type.



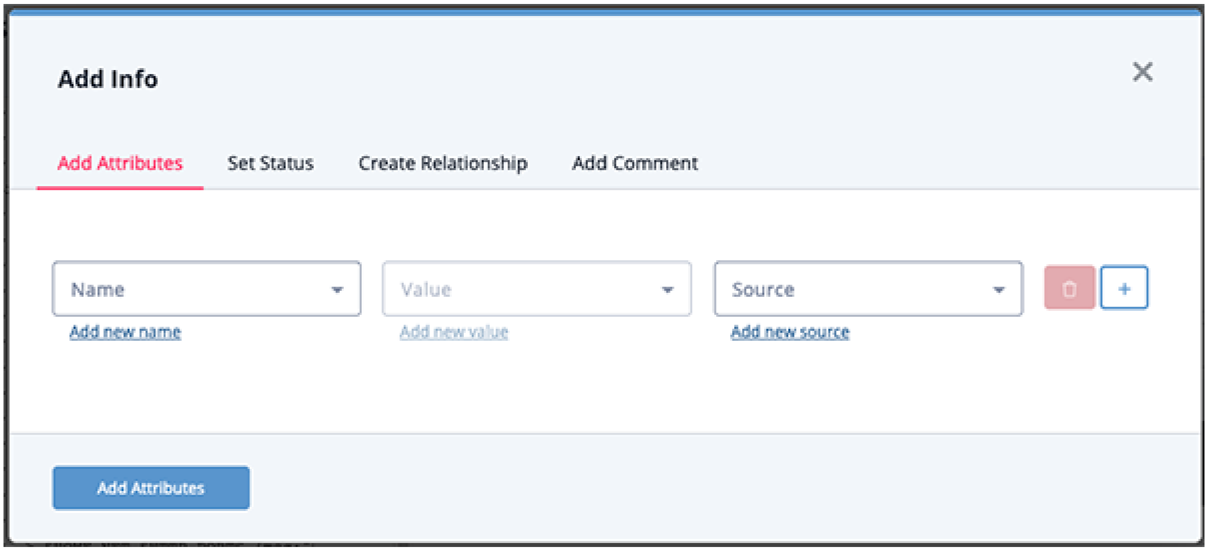
Value: s2-032.html

Type: Filename

- Selecting one or more indicators and clicking on **Add Info** option allows you to perform the following actions:

ACTION	DETAILS

ACTION	DETAILS
Add Attribute	You can add an attribute to one or more extracted indicators. Select the checkbox next to the indicator(s) to update and then click on the **Add Info** option. The Add Attributes tab will be selected by default. Select an **Attribute Name**, **Value**, and **Source** to apply to the selected indicator(s).
Set/Update Status	You can update the status of one or more extracted indicators. Select the checkbox next to the indicator(s) to update and then click on the **Add Info** option. Click on the **Set Status** tab and select your new status.
Create Relationship	You can link one or more extracted indicators to another system object. Select the checkbox next to the indicator(s) to update and then click on the **Add Info** option. Click on the **Set Relationship** tab and set the relationship. When you add a relationship, it is displayed in the indicator list and you can click it to view its details in a preview panel. If the object you want to link is not found, you can you can click the **Create** link to add the new object. If you limited your search to a specific object type, you are linked to the corresponding form. For example, if you limited your search to Adversaries, the **Create** link opens the Add An Adversary form. If you leave the **Limit search to** field set to All Objects, you can select the object type you want to create from a drop-down list. In the Add form, the indicators you selected in the second step of the import process are listed in the Create Relationship section.
Add Comment	You can add a comment to one or more extracted indicators. Select the checkbox next to the indicator(s) to update and then click on the **Add Info** option. Click on the **Set Comment** tab and enter your comment.



Removing Extracted Indicators

- You can delete one or more extracted indicators. Select the checkbox next to the indicator(s) to delete and then click on the **Remove** icon.

> ⚠ Selecting **All** from the Select dropdown will select all extracted indicators, not just the ones in your current filtered view (New, Pre-Existing).

14. When finished editing the extracted indicators list, click **Finish Export** to complete the process.

Importing Indicators via CSV

You can parse a .csv file for Indicator using the ThreatQ CSV File Parser.

> A .csv example file is available for download to serve a reference as you build your own .csv.
>
> Download CSV Example

CSV Files with 1000+ Rows

- Attempt to break the file into smaller parts and import.
- If you cannot break down the file, contact ThreatQ Customer Success about implementing a dedicated parser using the Configuration Driven Feed (CDF) framework.

CSV Columns

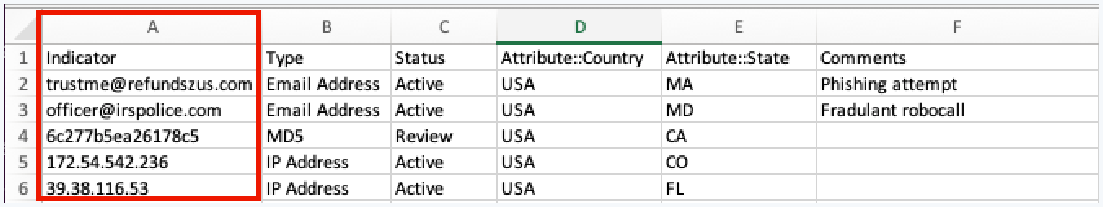
The column headers marked with an ***** in the table below are required for the CSV file. Failure to include these required columns will result in the import process failing. All other column headers are optional and will not cause the import process to fail if not included.

> Object and Attribute Sources cannot be added through the CSV file itself. A source value is added in the Step 7 of the import process, listed below, and is selected by the user.

> ⚠ The ThreatQ parser is case sensitive. When creating your CSV file, confirm that you are using the correct spelling and case for column headers as listed below.

COLUMN HEADER	DETAILS
***Indicator**	This field identifies the indicator name/value. ThreatQ requires that the Indicator column be included in the csv file and that each entry have a value.

Example



	A	B	C	D	E	F
1	Indicator	Type	Status	Attribute::Country	Attribute::State	Comments
2	trustme@refundszus.com	Email Address	Active	USA	MA	Phishing attempt
3	officer@irspolice.com	Email Address	Active	USA	MD	Fradulant robocall
4	6c277b5ea26178c5	MD5	Review	USA	CA	
5	172.54.542.236	IP Address	Active	USA	CO	
6	39.38.116.53	IP Address	Active	USA	FL	

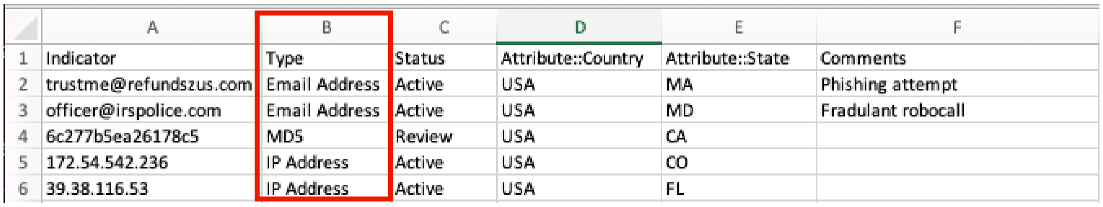
***Type**

This field identifies the indicator type.

ThreatQ requires that the Type column be included in the csv file and that each entry have a value.

> You must use a type that already exists in your ThreatQ instance. If you are unable to provide an Indicator Type for each indicator, you can use the **Generic Text/PDF** parsing option that will attempt to ID indicator type values automatically.

Example



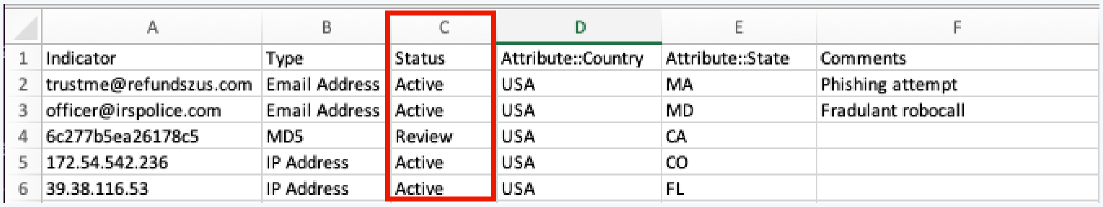
	A	B	C	D	E	F
1	Indicator	Type	Status	Attribute::Country	Attribute::State	Comments
2	trustme@refundszus.com	Email Address	Active	USA	MA	Phishing attempt
3	officer@irspolice.com	Email Address	Active	USA	MD	Fradulant robocall
4	6c277b5ea26178c5	MD5	Review	USA	CA	
5	172.54.542.236	IP Address	Active	USA	CO	
6	39.38.116.53	IP Address	Active	USA	FL	

***Status**

The Status column is required. You may leave the values blank as you will have the option to select a status to use during the import process. If you decide to enter values in the CSV, you must use a status that already exists in your ThreatQ instance. You can review your existing status by clicking on the **Settings** gear icon and selecting **Object Management**.

> The status supplied in the CSV will be used over the status selected during the import process. Any blank fields will use the status selected during the import process.

Example



	A	B	C	D	E	F
1	Indicator	Type	Status	Attribute::Country	Attribute::State	Comments
2	trustme@refundszus.com	Email Address	Active	USA	MA	Phishing attempt
3	officer@irspolice.com	Email Address	Active	USA	MD	Fradulant robocall
4	6c277b5ea26178c5	MD5	Review	USA	CA	
5	172.54.542.236	IP Address	Active	USA	CO	
6	39.38.116.53	IP Address	Active	USA	FL	

Attribute

The Attribute columns are optional. You can apply one or more attributes to an indicator by adding an Attribute column.

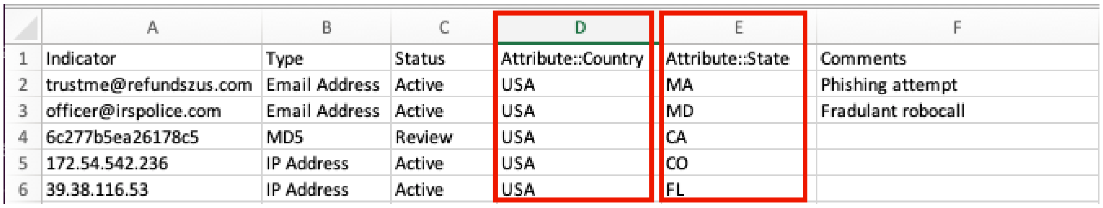
Attribute keys are **case** and **space** sensitive, 'MalwareFamily' and 'malware family' will generate a separate key in ThreatQ. In order to map to an existing Attribute Key in ThreatQ, you must match exactly.

Each attribute column heading must use the follow format:

```
Attribute::<Attribute Name>
```

> It is recommended to review existing attribute keys and values in ThreatQ prior to importing so that you can maintain consistent and normalized attribute data.

Example

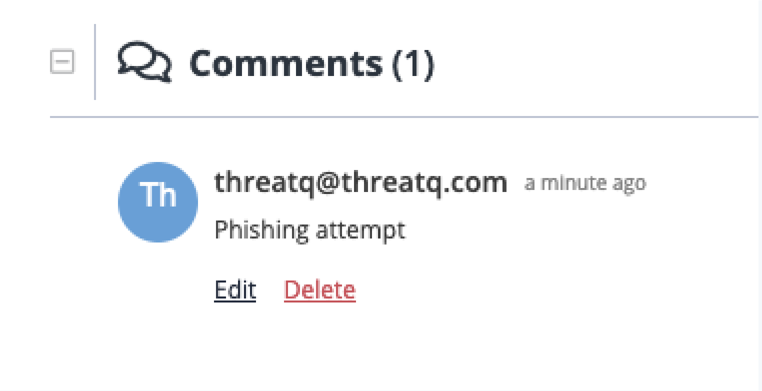


	A	B	C	D	E	F
1	Indicator	Type	Status	Attribute::Country	Attribute::State	Comments
2	trustme@refundszus.com	Email Address	Active	USA	MA	Phishing attempt
3	officer@irspolice.com	Email Address	Active	USA	MD	Fradulant robocall
4	6c277b5ea26178c5	MD5	Review	USA	CA	
5	172.54.542.236	IP Address	Active	USA	CO	
6	39.38.116.53	IP Address	Active	USA	FL	

Comments

The optional Comments allows you to add a comment to include with the indicator.

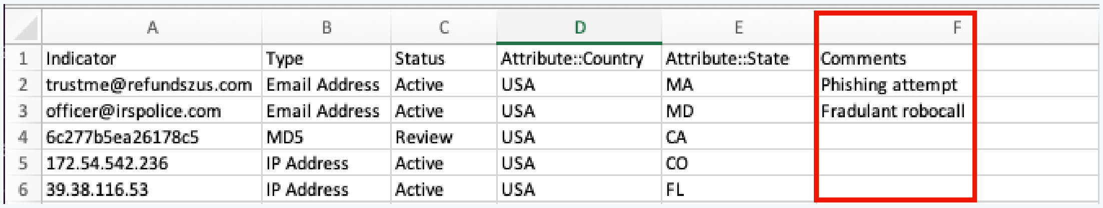
The ThreatQ user that performs the import process will be marked as the author of the comment in ThreatQ.



threatq@threatq.com a minute ago

Phishing attempt

Example

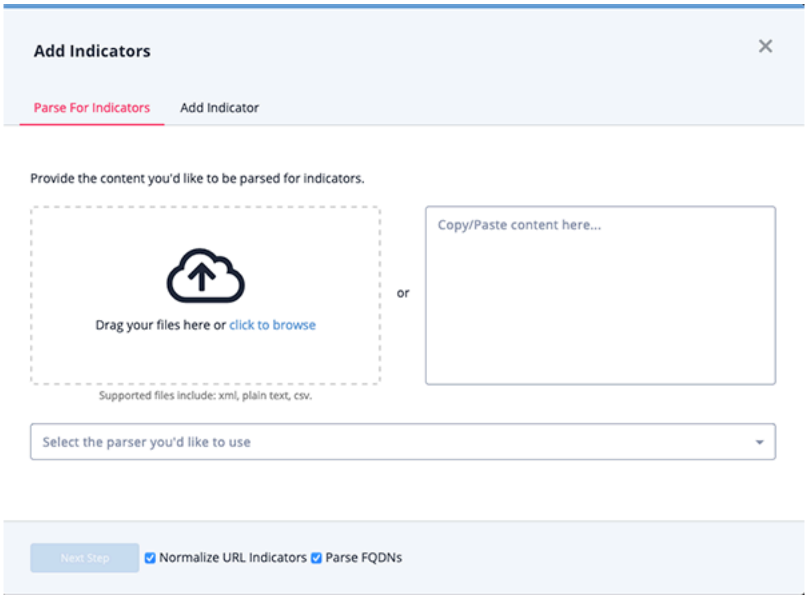


	A	B	C	D	E	F
1	Indicator	Type	Status	Attribute::Country	Attribute::State	Comments
2	trustme@refundszus.com	Email Address	Active	USA	MA	Phishing attempt
3	officer@irspolice.com	Email Address	Active	USA	MD	Fradulant robocall
4	6c277b5ea26178c5	MD5	Review	USA	CA	
5	172.54.542.236	IP Address	Active	USA	CO	
6	39.38.116.53	IP Address	Active	USA	FL	

Parsing a ThreatQ CSV File and Adding Context

1. Click the **Create** button and select **Indicator Parser** under the *Import* heading.

   The Add Indicators dialog box will open with the Parse for Indicators tab selected.


Add Indicators
Parse For Indicators
Add Indicator

Provide the content you'd like to be parsed for indicators.

Drag your files here or click to browse
or
Copy/Paste content here...

Supported files include: xml, plain text, csv.

Select the parser you'd like to use
Next Step

☑ Normalize URL Indicators ☑ Parse FQDNs

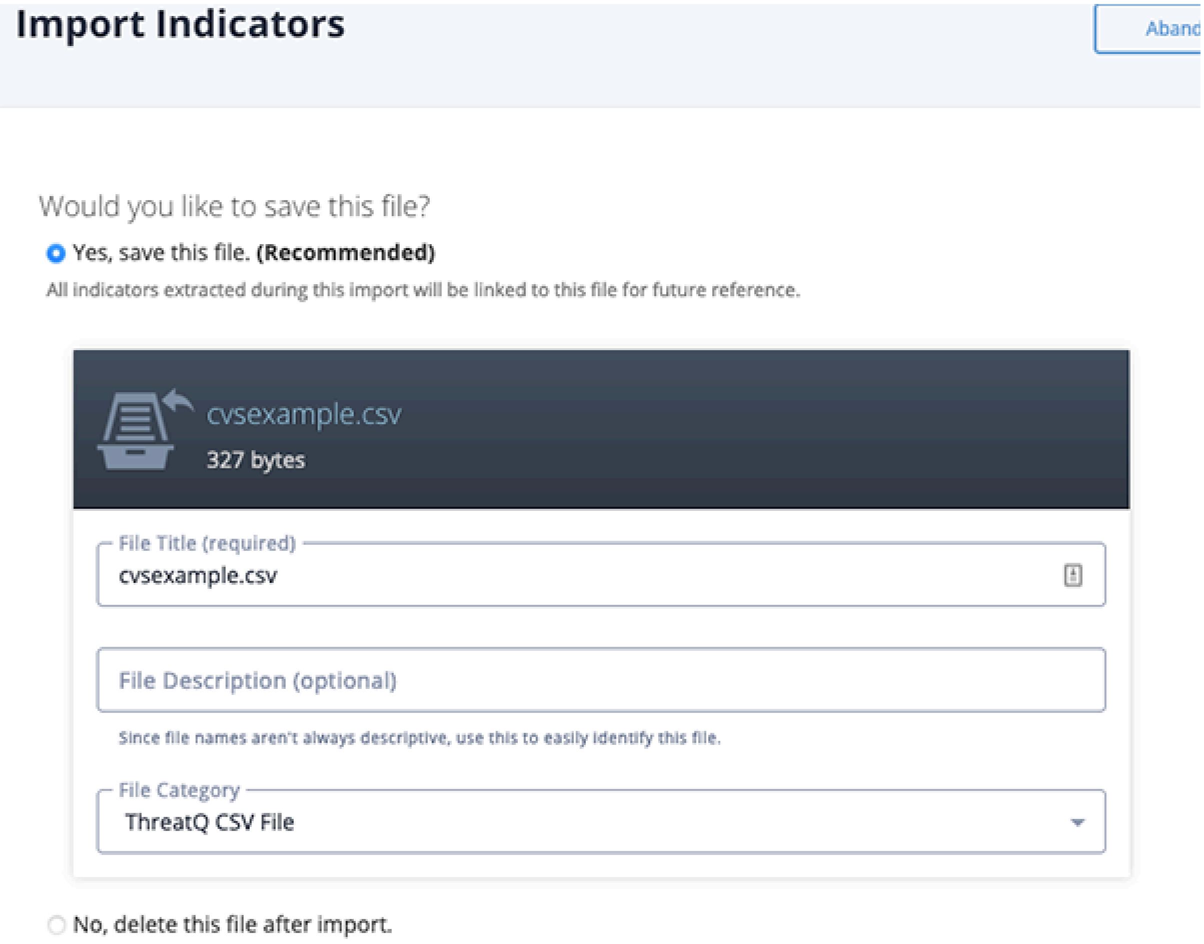
2. Upload your CSV file by either:

  - Dragging and dropping your file into the window
  - Clicking on the Click to Browse option and uploading your file
3. Select **ThreatQ CSV File** as the parser to use.
4. Use the checkboxes to select your parsing options:

OPTION	DESCRIPTION
Normalize URL Indicators	When checked, parsed URLs will have ports and leading protocol adjusted, as well as unneeded quotes and spaces removed. 💡 Normalization also adds attributes for protocol and query string. See the Indicator URL Normalization topic for more details.
Parse FQDNs	When checked, the Indicator Parser will parse FQDNs from the text and derive FQDN indicators from URLs in the text. **Example (checked)**: URL: https://tqexample.com/table.jspa?query_string_example Indicators created: ◦ tqexample.com/table.jspa (the URL) ◦ tqexample.com (the derived FQDN from the URL) When unchecked, the Indicator Parser will not generate FQDN indicators from the parsed text. **Example (unchecked)**: URL: https://tqexample.com/table.jspa?query_string_example Indicator created: ◦ tqexample.com/table.jspa (the URL)

> Administrators can configure the default setting for these options under the General Tab on the System Configurations page. See the Indicator Parsing Presets topic for more details.

5. Click **Next Step**.
6. Select whether or not to save the CSV file. Saving the file will result in all extracted indicators being linked to the file for reference.



Would you like to save this file?

● Yes, save this file. **(Recommended)**

All indicators extracted during this import will be linked to this file for future reference.

cvsexample.csv

327 bytes

File Title (required): cvsexample.csv

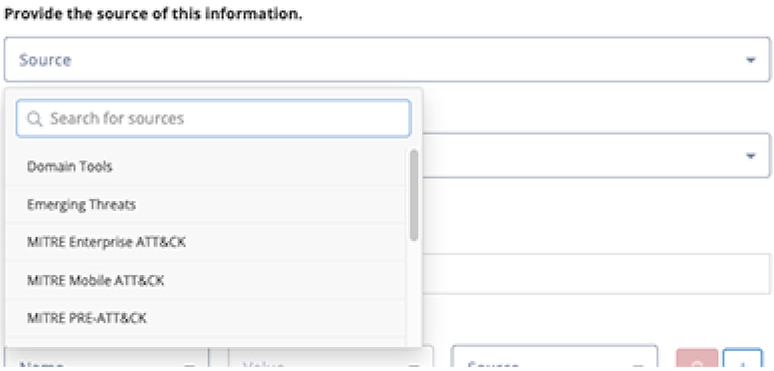
File Description (optional)

Since file names aren't always descriptive, use this to easily identify this file.

File Category: ThreatQ CSV File

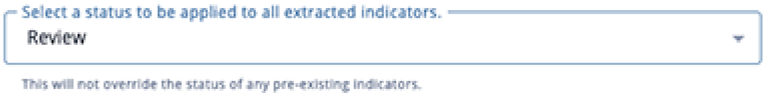
○ No, delete this file after import.

7. Select a **Source** for the extracted indicators.



Provide the source of this information.

8. Select a **Status** for the extracted indicators. If you supplied a status in the CSV file, that value will be applied to the indicators. Any entries in the CSV without a status value will be assigned the status you select in this step.



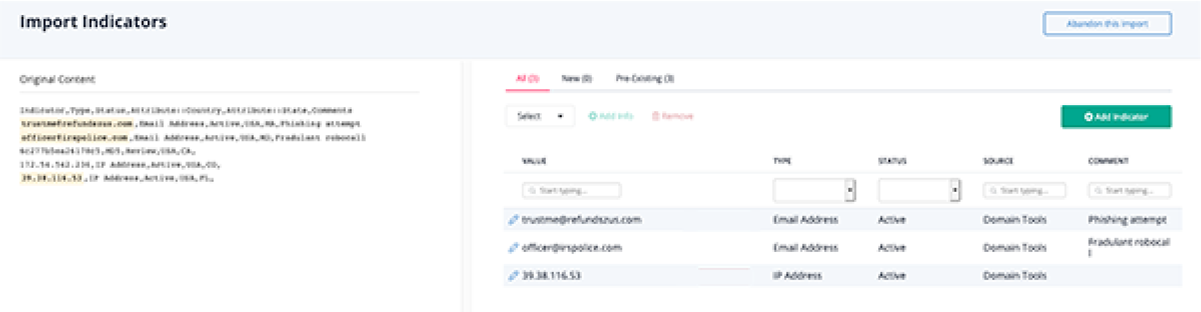
Select a status to be applied to all extracted indicators.
Review
This will not override the status of any pre-existing indicators.

9. Enter any **Tags** to apply to the extracted indicators. This field is optional.
10. Select any attribute, attribute value, and attribute source to apply to the extracted indicators.
11. Add **Relationships** for the extracted indicators.

> If you enter an object name that is not found, you can click the **Create** link to add the new object. If you limited your search to a specific object type, you are linked to the corresponding form. For example, if you limit your search to Adversaries, the **Create** link opens the Add An Adversary form. If you leave the **Limit search to** field set to All Objects, you can select the object type you want to create from a drop-down list.

12. Click on **Next Step**.

The Step 2: Organize and Classify page will load.



VALUE	TYPE	STATUS	SOURCE	COMMENT
trustme@refundszus.com	Email Address	Active	Domain Tools	Phishing attempt
officer@irspolice.com	Email Address	Active	Domain Tools	Fradulant robocall
39.38.116.53	IP Address	Active	Domain Tools	

13. You can review the extracted indicators' information and attributes.

You can perform the following actions:

ACTION	DETAILS
Add Indicator	You can add additional indicators by clicking on the Add Indicator button.

Edit Indicator Type and Value	You can edit the Indicator Type by clicking on the Pencil icon next to the indicator name. The Edit Indicator screen will load. You can edit the extracted indicator's value and type from this box.
Set/Update Status	You can update the status of one or more extracted indicators. Select the checkbox next to the indicator(s) to update and then click on the **Add Info** option. Click on the **Set Status** tab and select your new status.
Add Attribute	You can add an attribute to one or more extracted indicators. Select the checkbox next to the indicator(s) to update and then click on the **Add Info** option. The Add Attributes tab will be selected by default. Select an **Attribute Name**, **Value**, and **Source** to apply to the selected indicator(s).
Create Relationship	You can link one or more extracted indicators to another system object. Select the checkbox next to the indicator(s) to update and then click on the **Add Info** option. Click on the **Set Relationship** tab and set the relationship. When you add a relationship, it is displayed in the indicator list and you can click it to view its details in a preview panel. If the object you want to link is not found, you can you can click the **Create** link to add the new object. If you limited your search to a specific object type, you are linked to the corresponding form. For example, if you limited your search to Adversaries, the **Create** link opens the Add An Adversary form. If you leave the **Limit search to** field set to All Objects, you can select the object type you want to create from a drop-down list. In the Add form, the indicators you selected in the second step of the import process are listed in the Create Relationship section.
Add Comment	You can add a comment to one or more extracted indicators. Select the checkbox next to the indicator(s) to update and then click on the **Add Info** option. Click on the **Set Comment** tab and enter your comment.

Delete Extracted Indicator	You can delete one or more extracted indicators. Select the checkbox next to the indicator(s) to delete and then click on the **Remove** icon.

14. Click **Finish Export**.

Troubleshooting

If the CSV fails to parse please review the following points:

- Verify that the file is a CSV.
- Verify that column headers are spelled exactly as they are listed, the parser is case sensitive.
- Verify that all rows have a value for Indicator and Type.
- Verify that all Type and Status values are valid and exist in ThreatQ.

> If you have previously hit a failed parse run and believe you have fixed the error but the file will still not parse, logout of TQ, log back in and attempt to parse again.

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.

> EX 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/gate777.php
FQDN	bat99-11611.co

Extract HTTP Parameters from a URL Indicator

HTTP parameters [chained.j3oilgasinc.net/civis/viewforum.php?keywords=9obo&amp;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&amp;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

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.

> See the Indicator Expiration Policies topic for more information on setting up automatic expiration policies for indicators.

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**

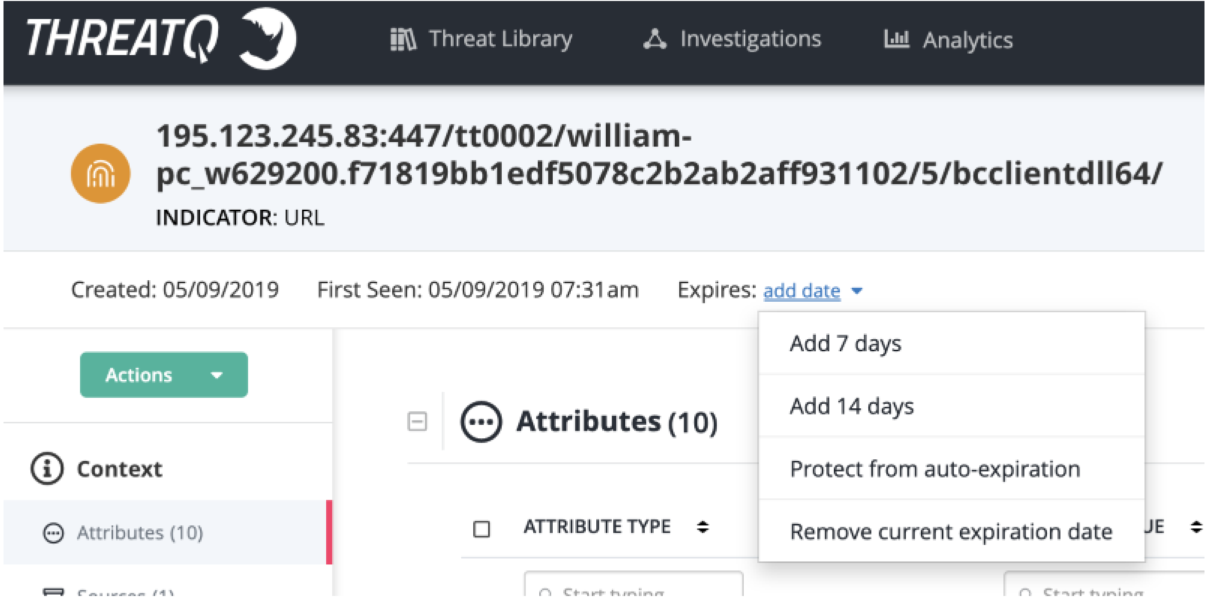
  Each indicator has the option to have an expiration date set, which once past, will toggle the status of that indicator from it's current status to "Expired".

- **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. See the Indicator Expiration Policies topic for more details.

Changing the Expiration Date for an Individual Indicator

When viewing a specific indicator, its expiration date can be changed by clicking on the link next to the expiration information.



195.123.245.83:447/tt0002/william-pc_w629200.f71819bb1edf5078c2b2ab2aff931102/5/bcclientdll64/

INDICATOR: URL

Created: 05/09/2019
First Seen: 05/09/2019 07:31am
Expires: add date

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.

Changing the Expiration Date for Multiple Indicators

You can apply expiration changes for a set of indicators using the Bulk Action function. See the Bulk Actions topic for further details.

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 rely on ThreatQ's scoring algorithm to calculate scores. After scores are calculated, you can change the score to your custom value or accept the calculated value.

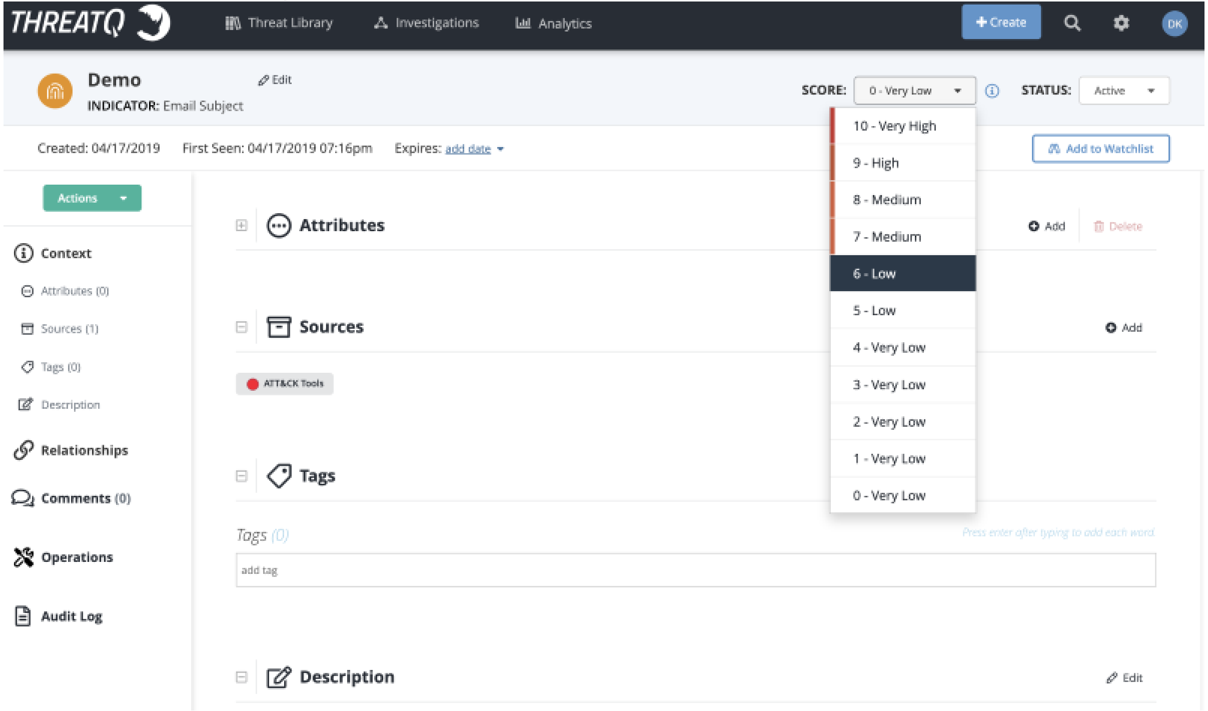
Building a Scoring Algorithm

You can build a scoring algorithm that automatically assigns an indicator score based on user-designed criteria.   See the Scoring Algorithms topic for further details.

Setting a Manual Indicator Score

> You can use this process to override an individual indicators score set by the scoring algorithm.

1. Navigate to an Indicator's Details page.
2. Click the **Score** dropdown and select a score.



Demo

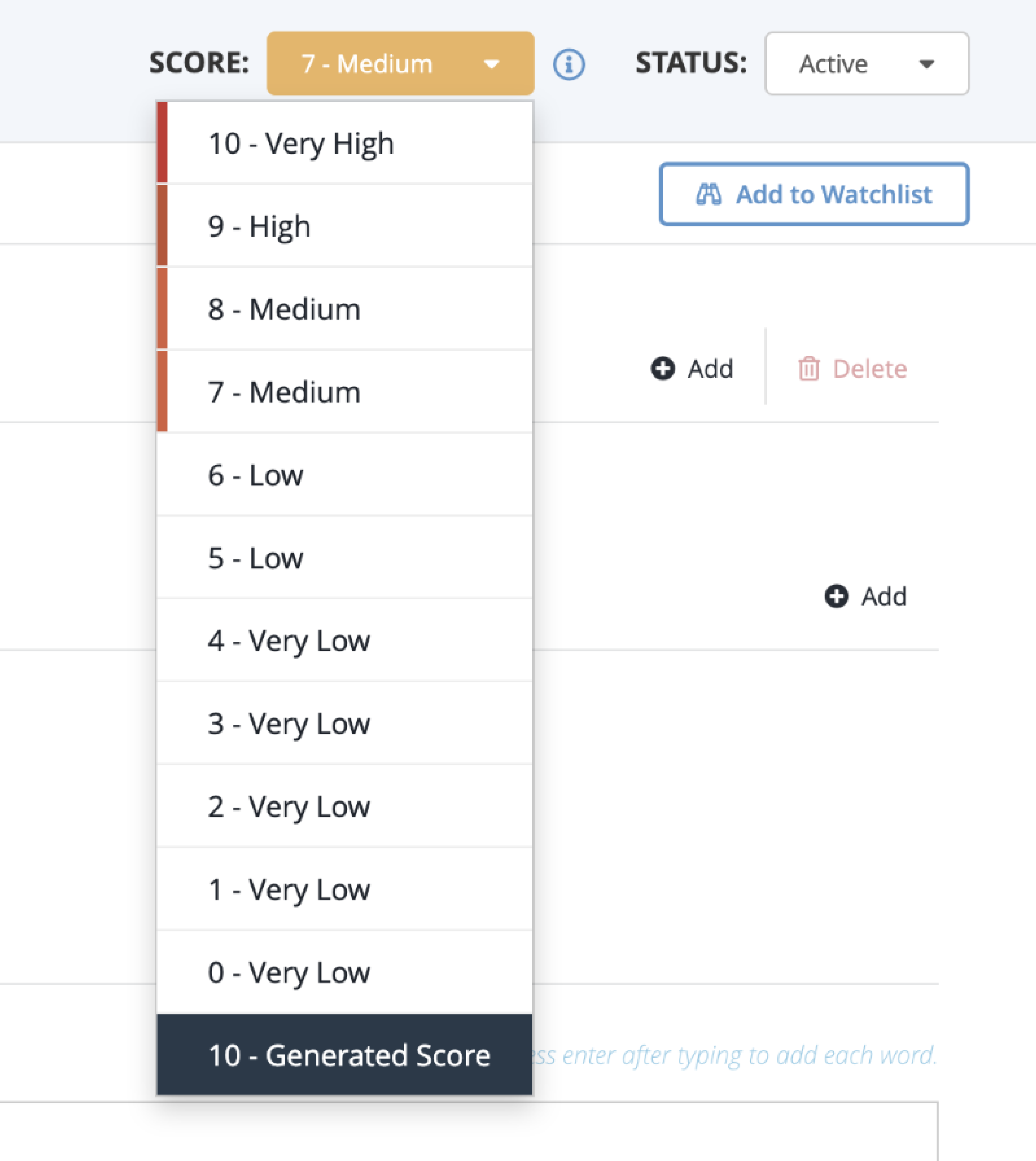
INDICATOR: Email Subject

SCORE: 0 - Very Low

STATUS: Active

Created: 04/17/2019 First Seen: 04/17/2019 07:16pm Expires: add date

Optionally, you may revert to the calculated score by clicking on the Score dropdown and selecting **Generated Score**.



Indicator Status

All Indicator in the system have statuses.

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.

Default Statuses

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.

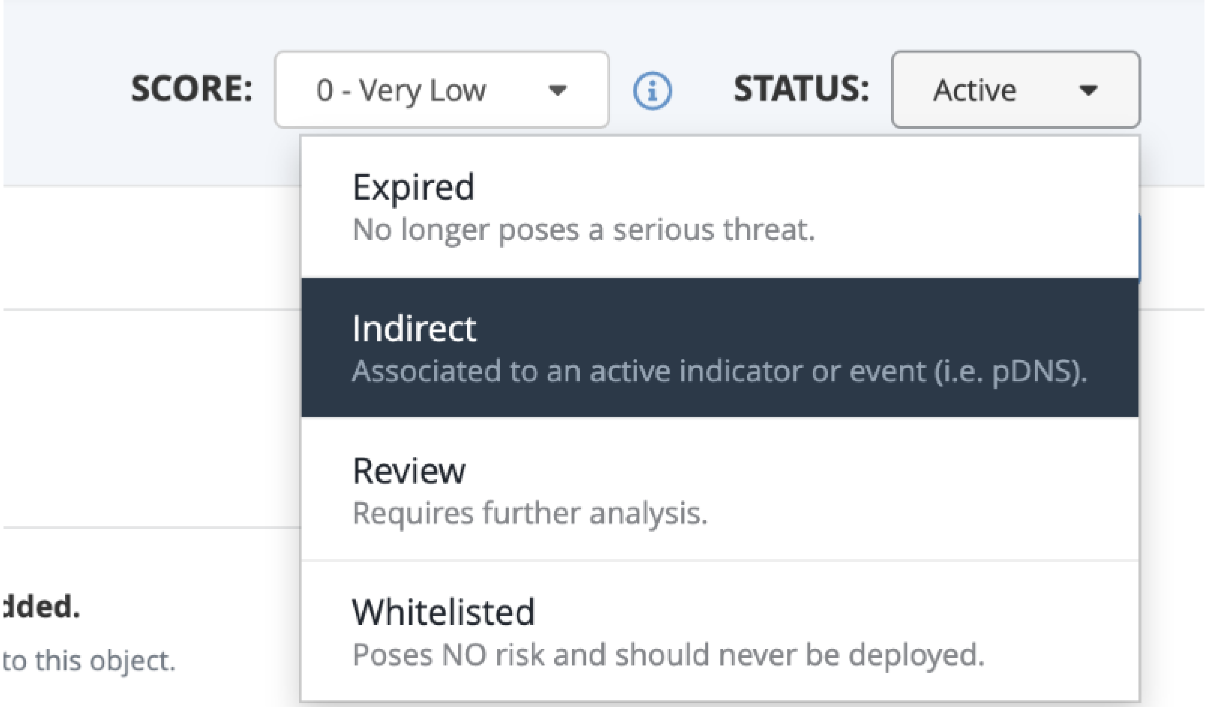
Custom Statuses

You can create custom statuses for use in your ThreatQ instance. See the Indicator Statuses topic for more details.

Changing the Status of an Individual 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 the Whitelisted Indicators topic for more information.

1. Locate and click the indicator to open its details page.
2. Click the status dropdown menu, and select the desired status.


SCORE:
0 - Very Low
STATUS:
Active
Expired
No longer poses a serious threat.
Indirect
Associated to an active indicator or event (i.e. pDNS).
Review
Requires further analysis.
Whitelisted
Poses NO risk and should never be deployed.
dded.
to this object.

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 section of the Whitelisted Indicators topic.

Changing the Status for Multiple Indicators

You can change the status for multiple indicators using the Bulk Status Change. See the Bulk Actions topic for more information.

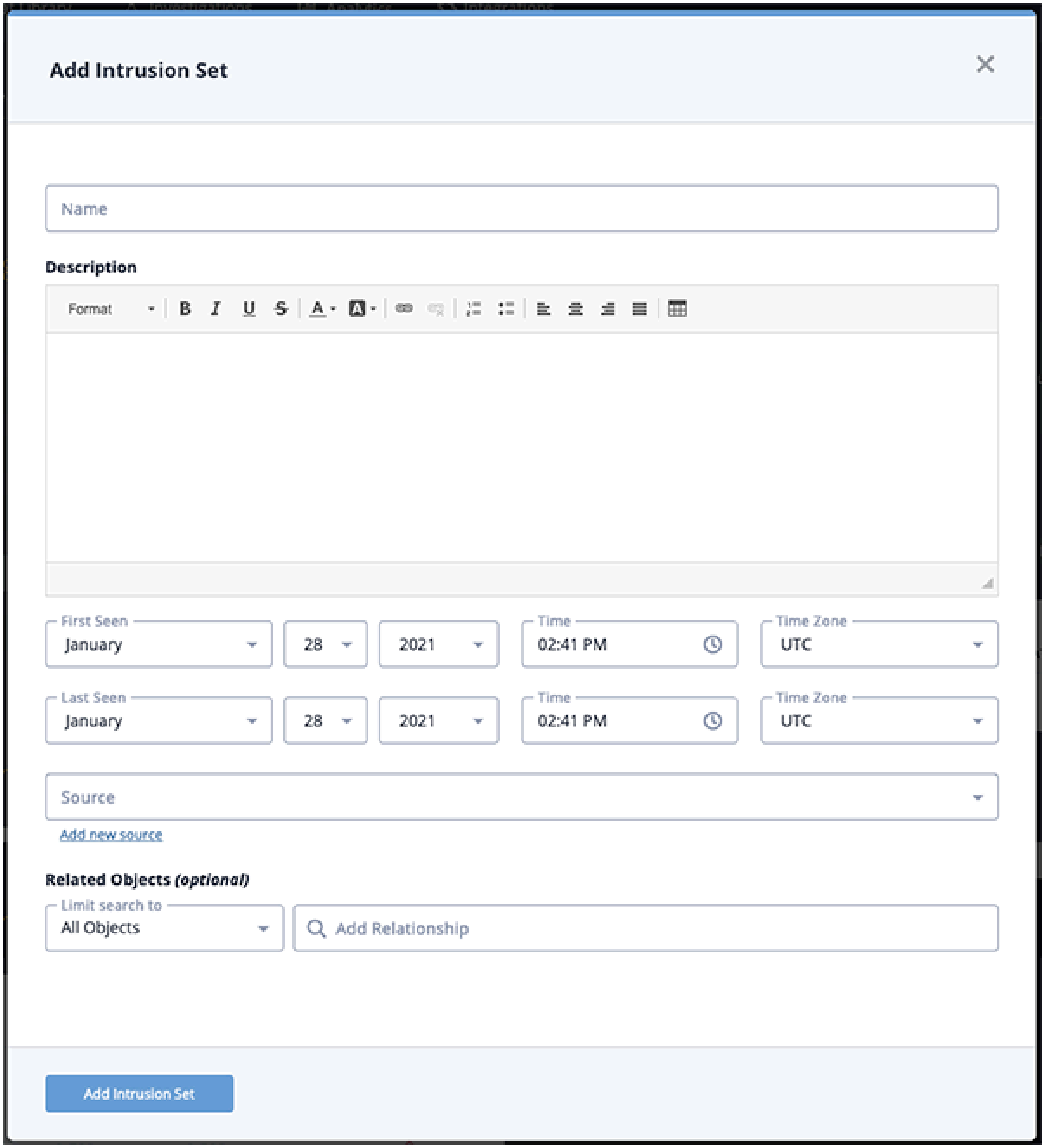
Intrusion Sets

Intrusion Set are grouped sets of adversarial behaviors and resources, sometimes referred to as attack packages, used to target an individual organization.

Adding an Intrusion Set

1. Go to **Create > Intrusion Set**.

   The Add Intrusion Set dialog box opens.



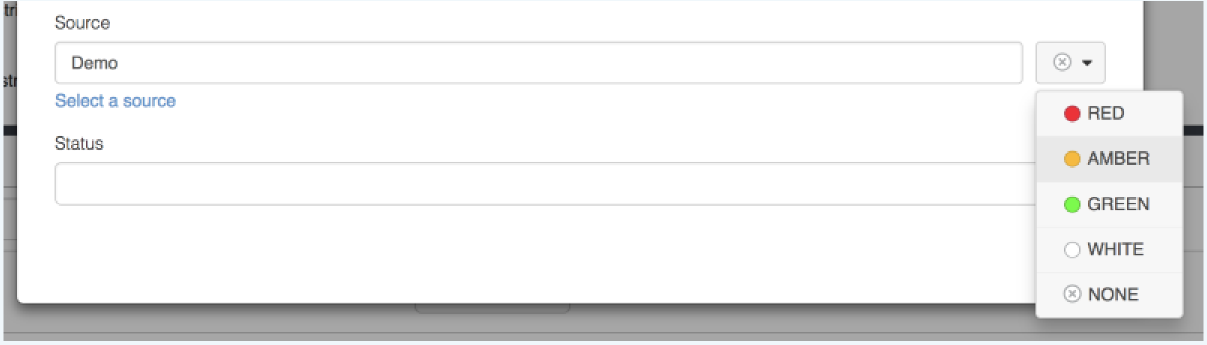
First Seen: January 28 2021 — Time: 02:41 PM — Time Zone: UTC

Last Seen: January 28 2021 — Time: 02:41 PM — Time Zone: UTC

Limit search to: All Objects

2. Enter a **Name**.
3. Enter a **Description** in the field provided.
4. Select the **First Seen** and **Last Scene** times.
5. Select a **Source** from the dropdown provided.

> You can also click the **Add a New Source** option if the desired source is not listed in the dropdown list . If administrators have enabled TLP view settings, you can select a TLP label for the new source in the dropdown list provided. See the

> Traffic Light Protocol (TLP) topic for more information on TLP schema.
>
> 
>
> Source
>
> Demo
>
>

6. Select any **Related Objects** you need to link to the Intrusion Set. This field is optional.
7. Click **Add Intrusion Set**.

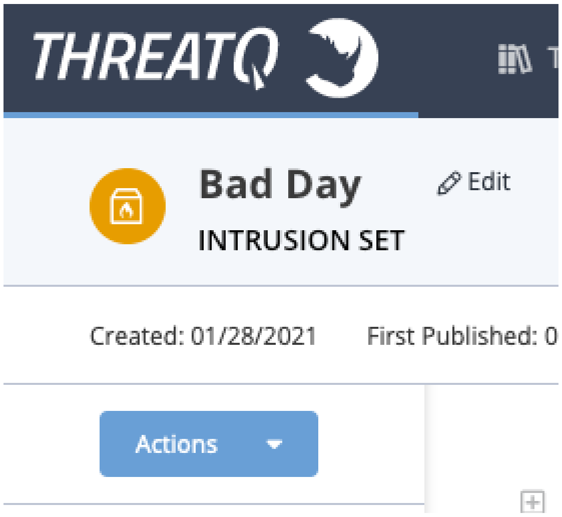
Adding Context

See the Object Details section and its topics for details on adding context to an object such as adding sources, attributes, and related objects.

Editing an Intrusion Set

1. Locate and click on the Intrusion Set.

   The Intrusion Set's detail page opens.

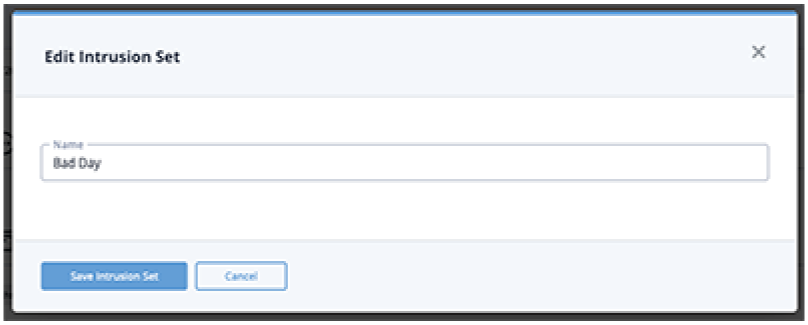
   Bad Day

   INTRUSION SET

   Created: 01/28/2021 First Published: 0

2. Click on **Edit** next to the Intrusion Set's name.

The Edit Intrusion Set dialog box opens.



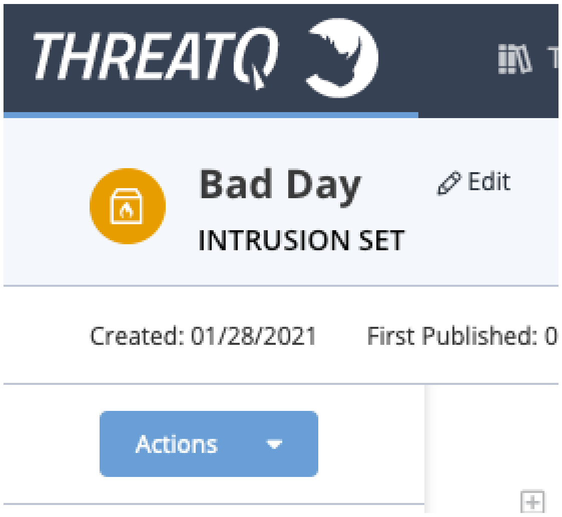
Name
Bad Day

3. Make the desired change to the Intrusion Set's name and click **Save Intrusion Set**.

Deleting an Intrusion Set

1. Locate and click on the Intrusion Set.

   The Intrusion Set's details page opens.

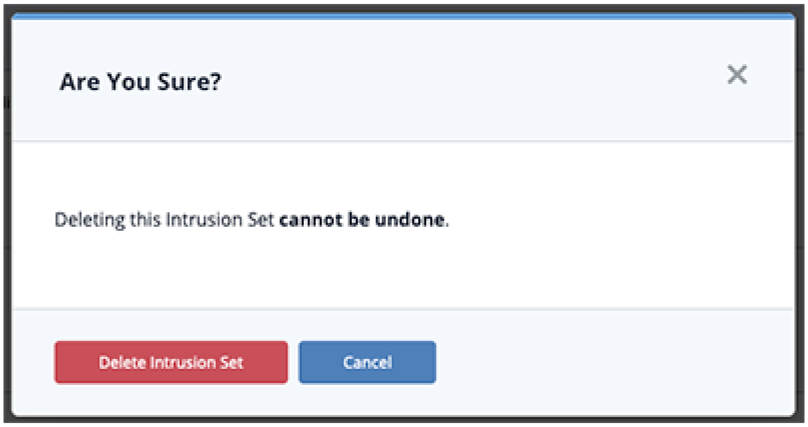


Created: 01/28/2021

First Published: 0

2. Click on the **Actions** menu and select **Delete Intrusion Set**.

A confirmation dialog box appears.



Are You Sure?

Deleting this Intrusion Set **cannot be undone.**

3. Click on **Delete Intrusion Set**.

Malware

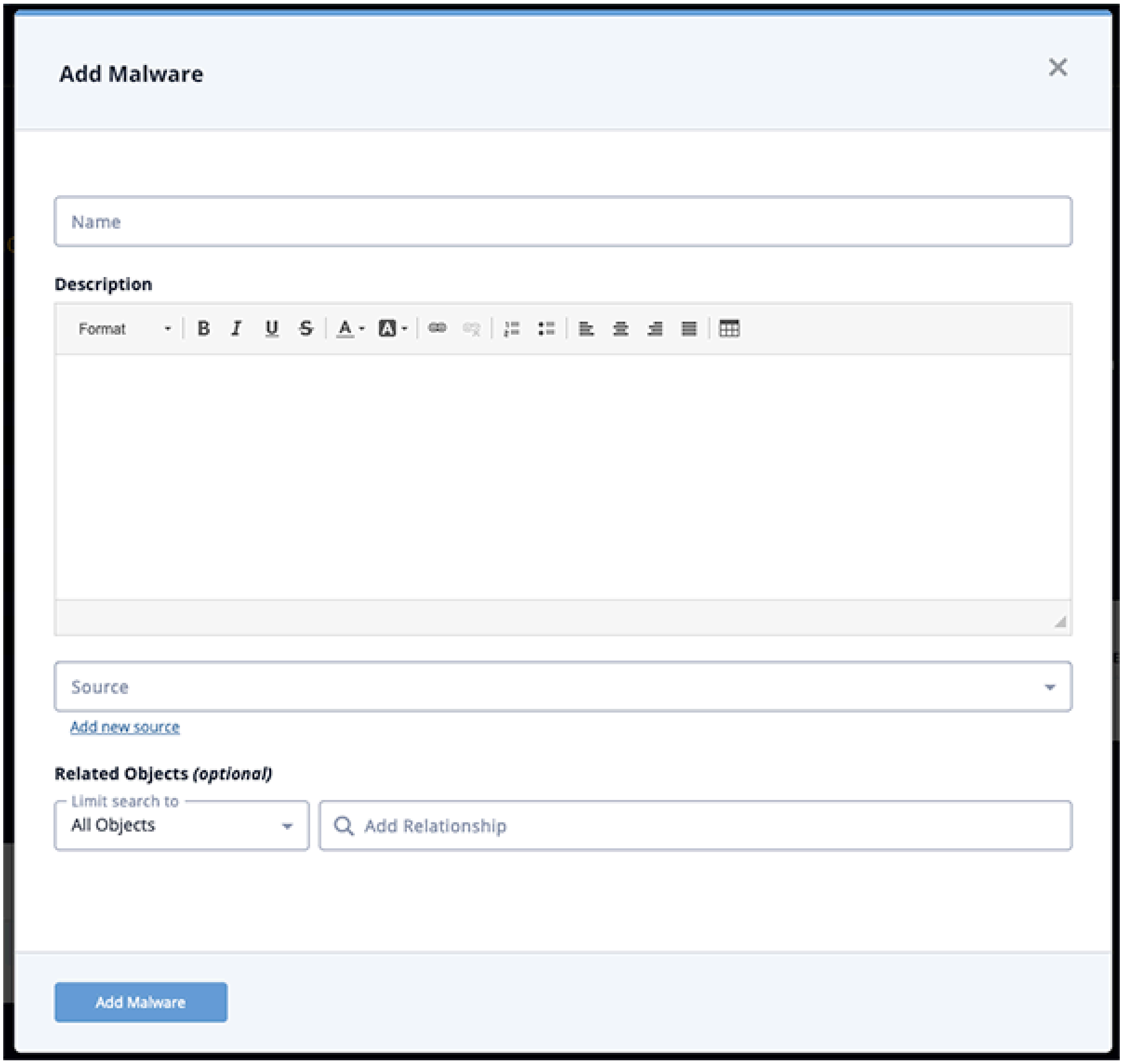
Malware, short for malicious software, targets devices, services, and networks with the intent to gain unauthorized access or damage a network or programmable device.

Use the steps below to create, edit and delete a Malware object.

Adding a Malware Object

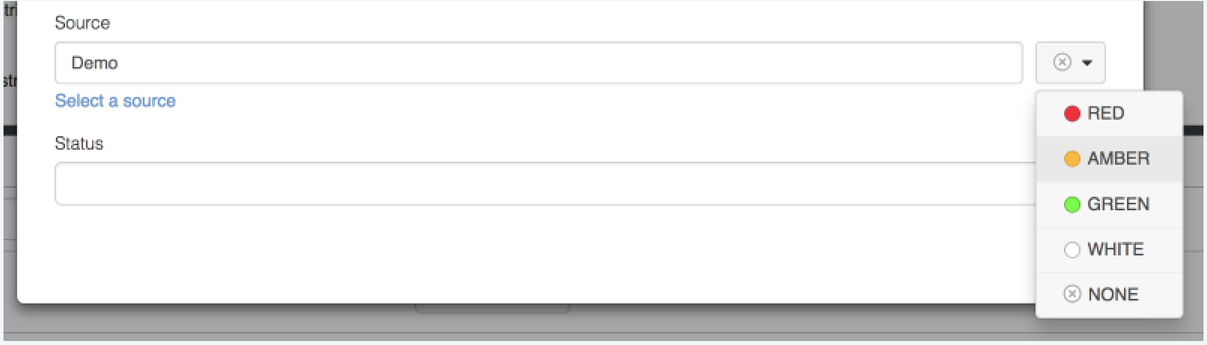
1. Go to **Create** > **Malware**.

   The Add Malware dialog box opens.



2. Enter a name.
3. Enter a description in the field provided.
4. Select a **Source** from the dropdown provided.

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



Source: Demo

5. Select any **Related Objects** you need to link to the Malware. This field is optional.
6. Click **Add Malware**.

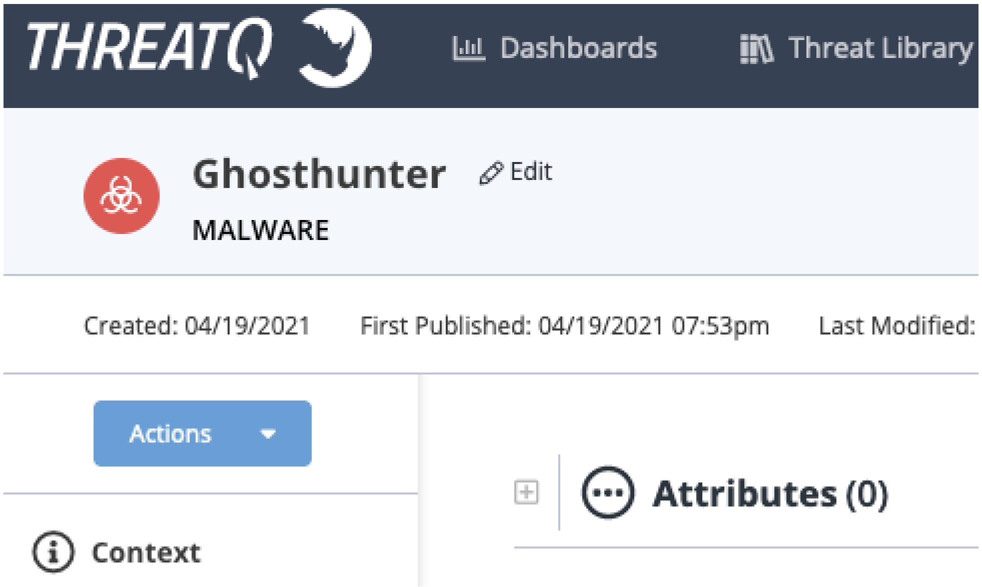
Adding Context

See the Object Details section and its topics for details on adding context to an object such as adding sources, attributes, and related objects.

Editing a Malware Object

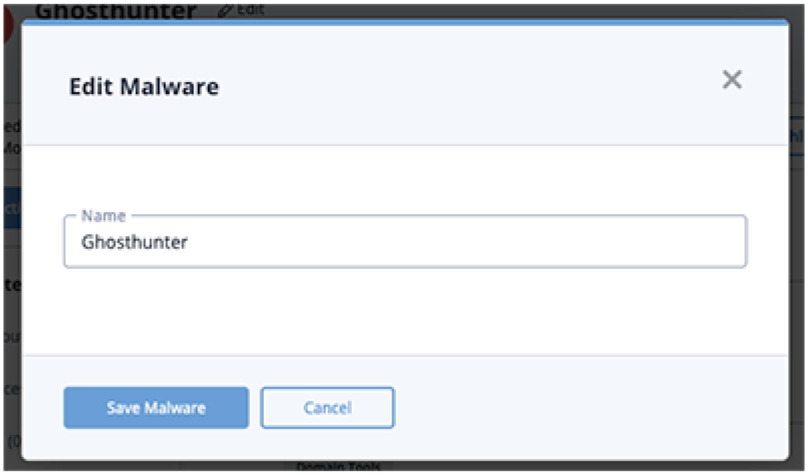
1. Locate and click on the Malware.

The Malware's detail page opens.



2. Click on **Edit** next to the Malware's name.

   The Edit Malware dialog box opens.



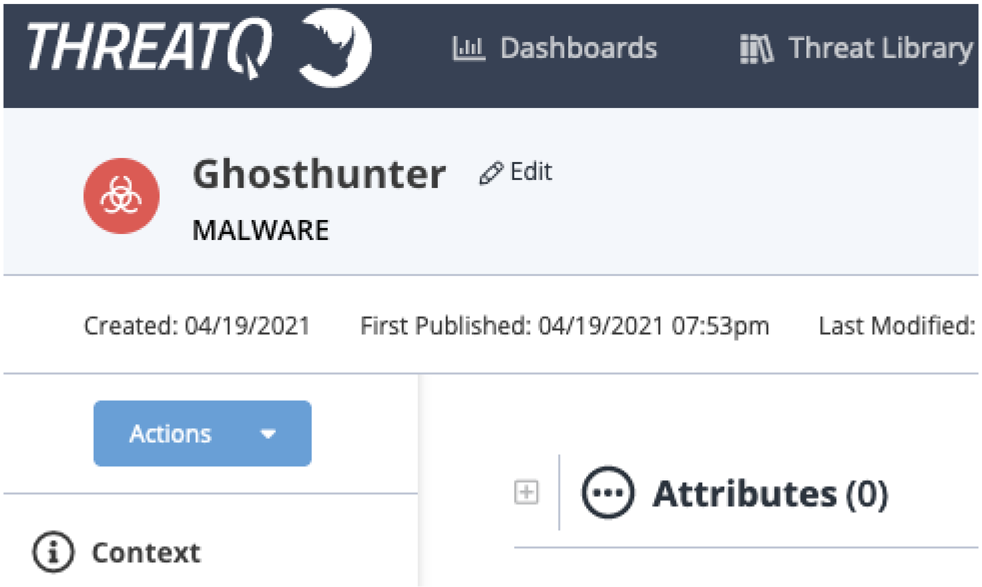
Name: Ghosthunter

3. Make the desired change to the Malware name and click **Save Malware**.

Deleting a Malware Object

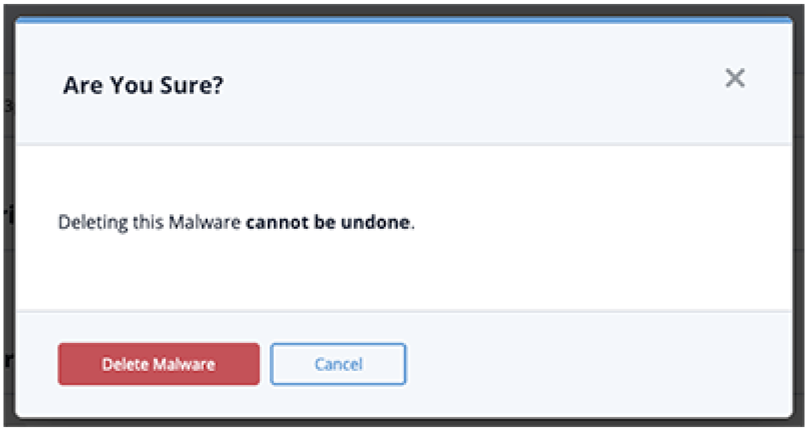
1. Locate and click on the Malware.

The Malware's details page opens.



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

   A confirmation dialog box appears.



Deleting this Malware **cannot be undone**.

3. Click on **Delete Malware**.

Reports

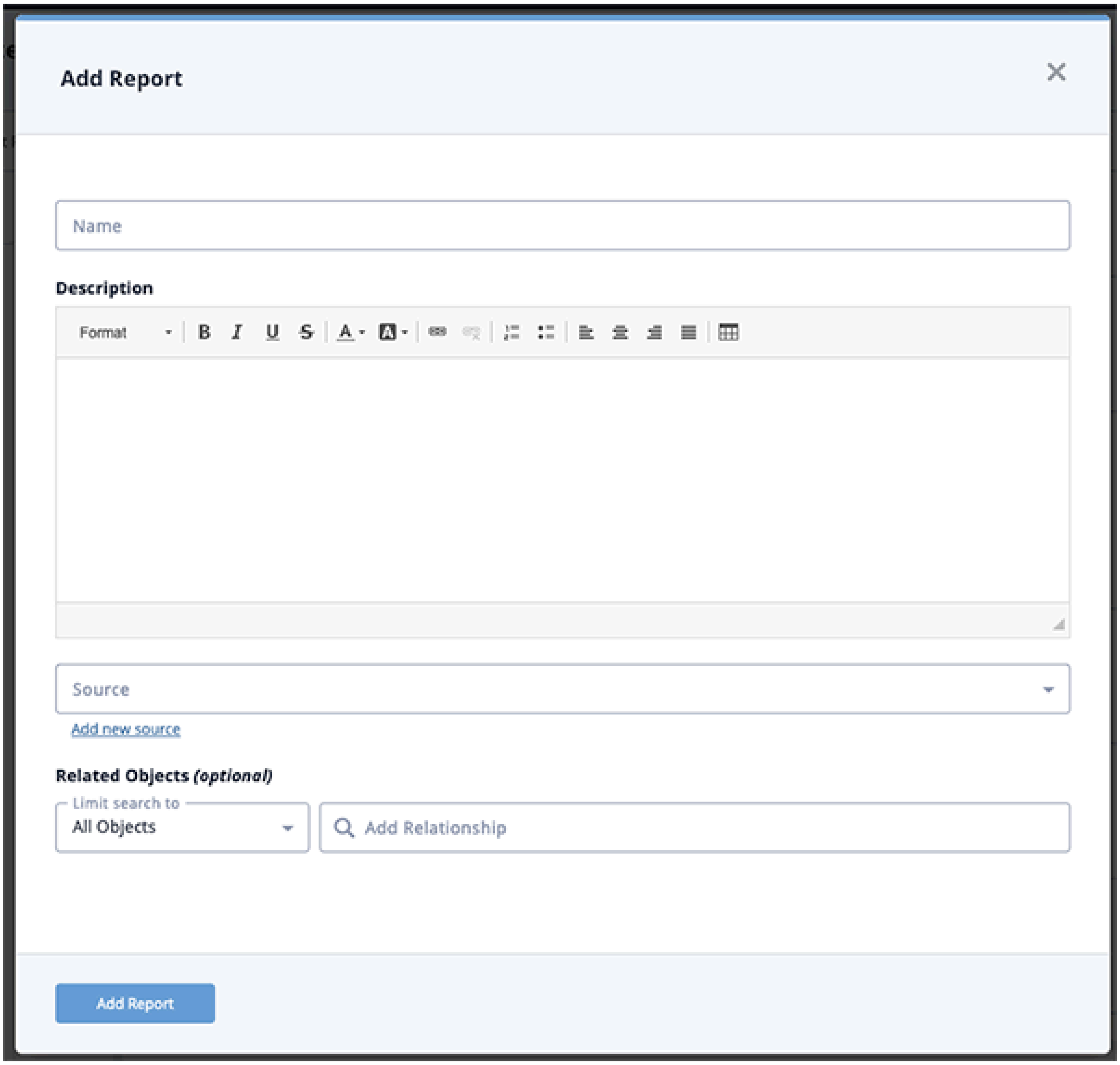
Report contain information and related details for a specific threat such as Malware.

Use the steps below to create, edit and delete a Report.

Adding an Reports

1. Go to **Create > Report**.

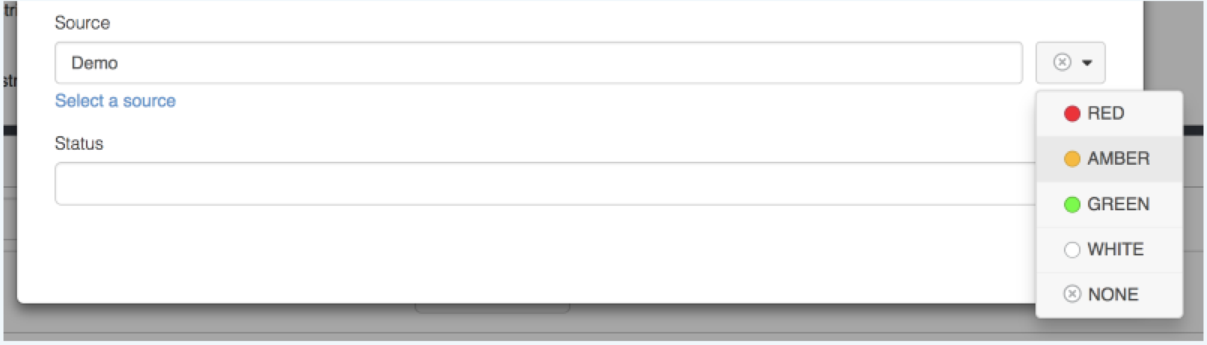
   The Add Report dialog box opens.



2. Enter a name.

3. Enter a description in the field provided.
4. Select a **Source** from the dropdown provided.

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



Source

Demo

Select a source

Status

5. Select any **Related Objects** you need to link to the Report. This field is optional.
6. Click **Add Report**.

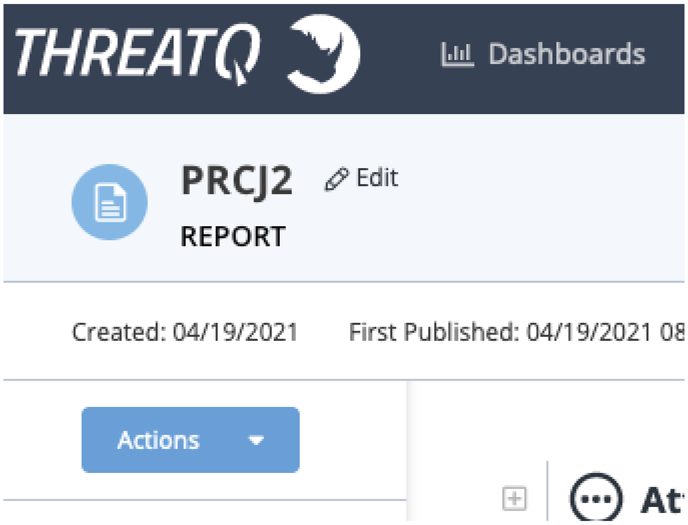
Adding Context

See the Object Details section and its topics for details on adding context to an object such as adding sources, attributes, and related objects.

Editing an Report

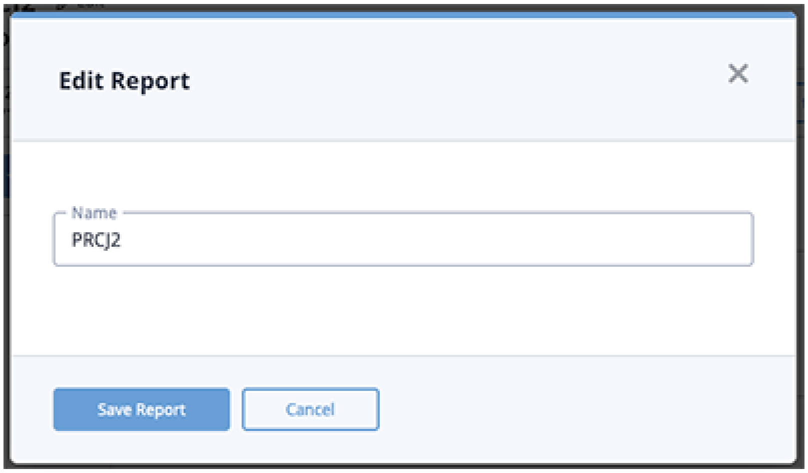
1. Locate and click on the Report.

The Report's detail page opens.



2. Click on **Edit** next to the Report's name.

   The Edit Report dialog box opens.

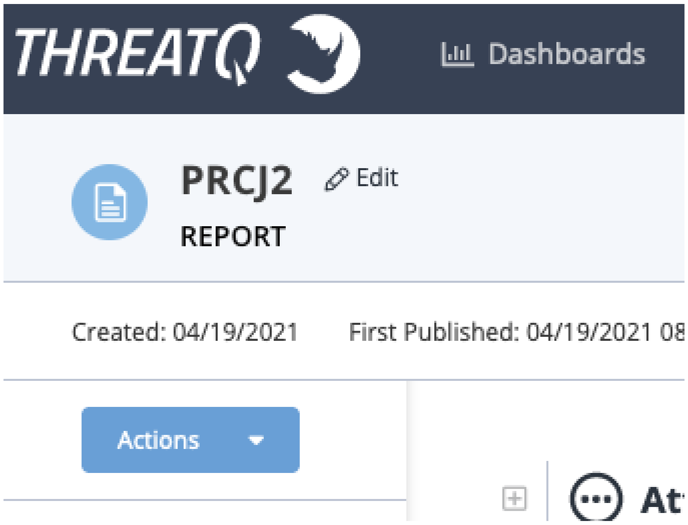


3. Make the desired change to the Report name and click **Save Report**.

Deleting an Report

1. Locate and click on the Report.

The Report's details page opens.

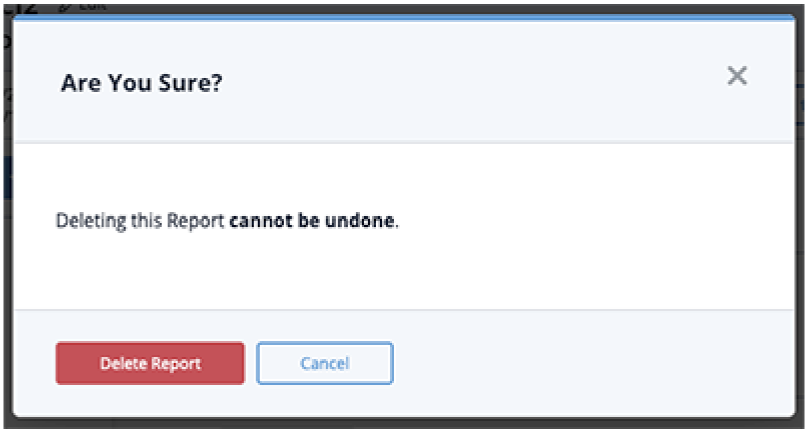


Created: 04/19/2021

First Published: 04/19/2021 08

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

   A confirmation dialog box appears.



Are You Sure?

Deleting this Report **cannot be undone**.

3. Click on **Delete Report**.

Signatures

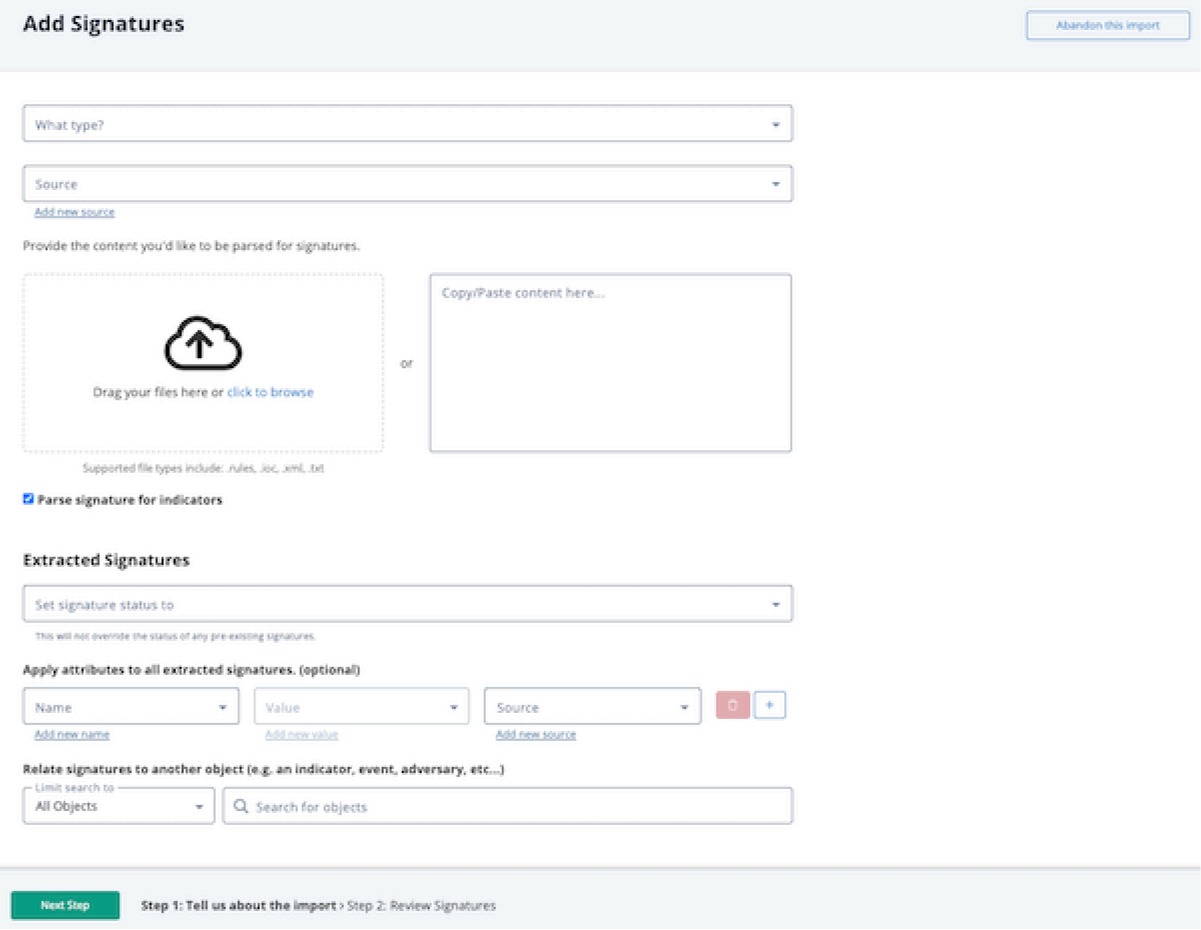
Signatures contain the blueprints or patterns associated with a malicious attack on a network or system.

ThreatQ provides you with the ability to ingest and manage Signatures, such as Snort, YARA, 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 Indicator, Events, Adversary, and Files.

Adding a Signature

1. From the main menu, choose **Create > Signature**.

   The Add Signatures dialog box opens.



Provide the content you'd like to be parsed for signatures.

Drag your files here or click to browse

Supported file types include: .rules, .ioc, .xml, .txt

☑ Parse signature for indicators

This will not override the status of any pre-existing signatures.

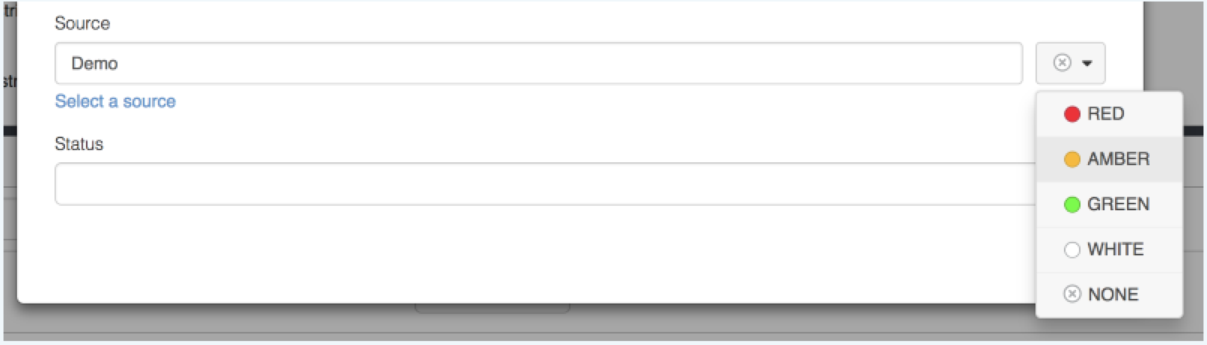
Apply attributes to all extracted signatures. (optional)

Relate signatures to another object (e.g. an indicator, event, adversary, etc...)

Limit search to: All Objects

Step 1: Tell us about the import › Step 2: Review Signatures

2. Choose the type of signature from the dropdown .
3. Select a **Source** from the dropdown provided.

> You can also click the **Add a New Source** option if the desired source is not listed in the dropdown list . If administrators have enabled TLP view settings, you can select a TLP label for the new source in the dropdown list provided. See the Traffic Light Protocol (TLP) topic for more information on TLP schema.
>
> 
>
> Source: Demo
>
> Select a source
>
> Status
>
>

4. 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.
5. Optionally, select to parse the signature for indicators.

6. Choose a **Signature Status** from the drop-down menu.

7. Optionally, **Apply attributes to all extracted signatures**:

    - Select an **Attribute Type**.
    - Enter an **Attribute Value**.
    - Enter an **Attribute Source**.

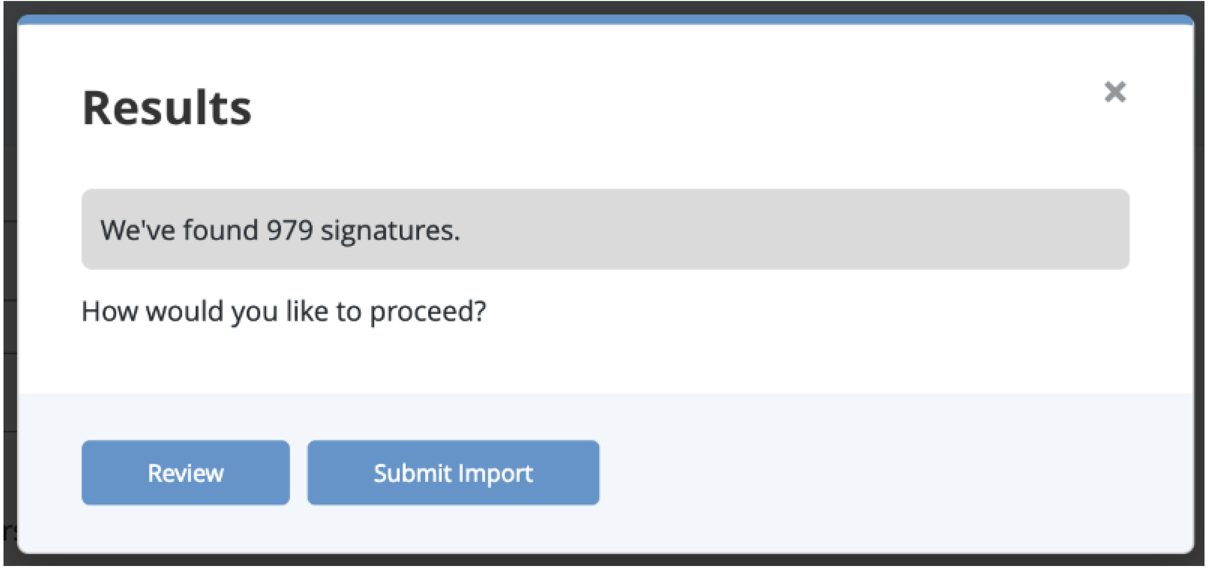
    > You can click on the **Add** icon for additional attributes.

8. Optionally, relate the signature to another object by entering the object in the **Relate signatures to another object** field.

    > If you enter an object name that is not found, you can click the **Create** link to add the new object. If you limit your search to a specific object type, you are linked to the corresponding form. For example, if you limit your search to Adversaries, the **Create** link opens the Add An Adversary form. If you leave the **Limit search to** field set to All Objects, you can select the object type you want to create from a drop-down list.

9. Click **Next Step**.

If signatures are discovered, the Results dialog box appears.

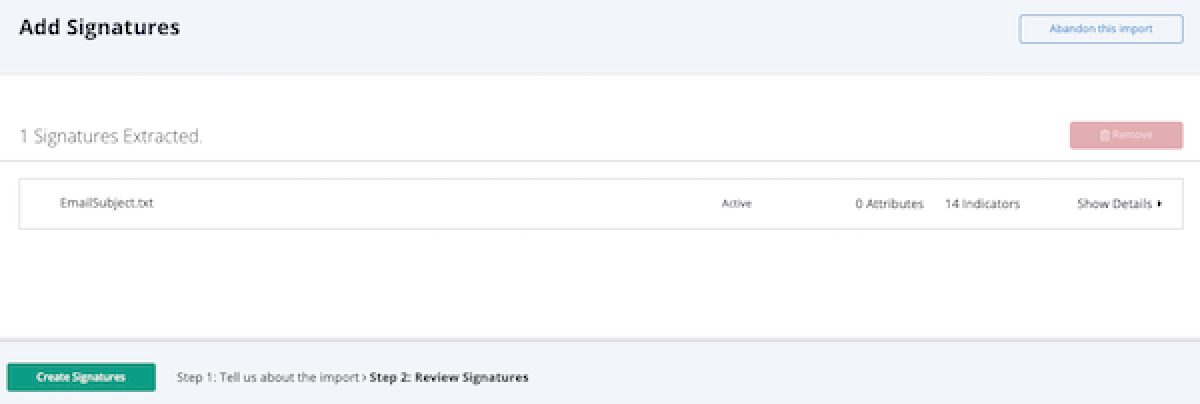


We've found 979 signatures.

How would you like to proceed?

10. 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.



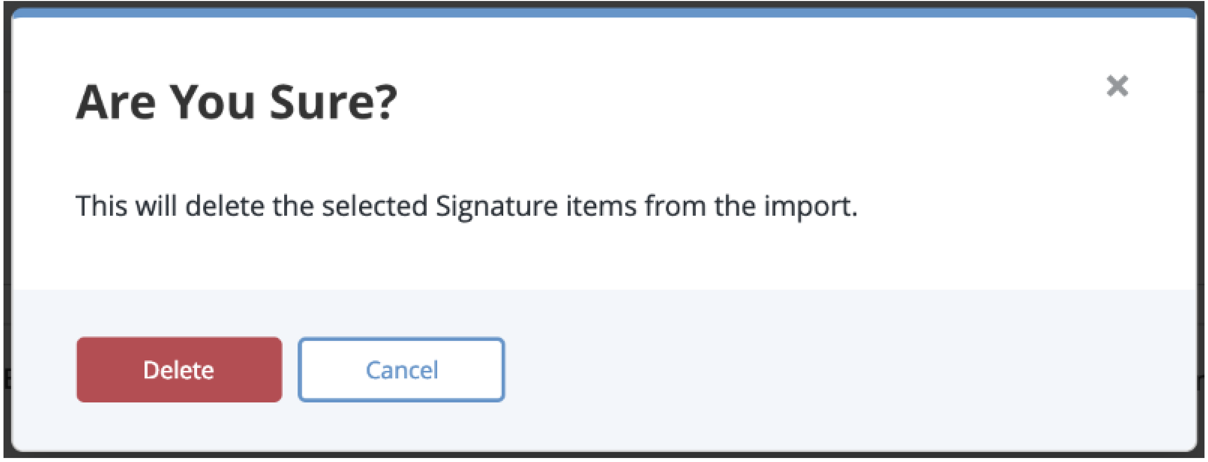
1 Signatures Extracted.

EmailSubject.txt Active 0 Attributes 14 Indicators

Step 1: Tell us about the import › **Step 2: Review Signatures**

11. Select one or more signatures and click **Delete**.
12. 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.



Are You Sure?

This will delete the selected Signature items from the import.

13. Click **Delete** to remove the unwanted items.
14. Click **Create Signatures** when finished.

STIX

> ThreatQ supports STIX 1.1.1, STIX 1.2 and STIX 2.0.
>
> Although the ThreatQ STIX parser does not support version 2.1, it will parse 2.1 files in the same manner as 2.0 files. As such, it does not parse out any object types introduced in STIX 2.1, such as Opinions..

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.
- You can upload a STIX file or insert STIX data to parse for indicators.

ThreatQ STIX Object Types

STIX integration provides ThreatQ with the following additional object types.

- Campaign
- Courses of Action
- Exploit Target
- Incident
- TTP objects
- Identity (STIX 2.0)
- Report (STIX 2.0)
- Vulnerability (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.

Parsing a STIX File for Indicators

ThreatQ allows you to upload a STIX file or insert STIX data to parse for indicators.

1. Click the **Create** button, located at the top of the dashboard and select **STIX Parser** under the *Import* heading.
   The Parse for Intelligence window is displayed.

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. The **Normalize URL Indicators** check box defaults to checked. You can click the check box to unselect it or leave it checked. See Indicator URL Normalization for more information.
4. Click the **Next Step** button.

> If at any point, you wish to abandon the import, click **Abandon this import**.

5. Populate the following fields:

FIELD	REQUIRED	DESCRIPTION
Name	Y	Enter the name of your import file.
Source	Y	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
Select a status	Y	Select a **Status** to be applied to the imported objects.
Add attributes	N	Select **Attributes** to be assigned to the imported objects.
Add comment	N	Add a comment to the imported objects.
Add relationships	N	Add **Relationships** for the imported objects.

		If you enter an object name that is not found, you can click the **Create** link to add the new object. If you limit your search to a specific object type, you are linked to the corresponding form. For example, if you limit your search to Adversaries, the **Create** link opens the Add An Adversary form. If you leave the **Limit search to** field set to All Objects, you can select the object type you want to create from a drop-down list.
Tags	N	Enter any **Tags** that should be applied to the imported objects.

6. Click the **Submit** button.

   New objects will become available in the Threat Library.

STIX 1.1.1, 1.2 Data Mapping

You can click on the expand 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	
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	

STIX FIELD	THREATQ FIELD MAPPING	THREATQ NAME
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	
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	

STIX FIELD	THREATQ FIELD MAPPING	THREATQ NAME
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 Target Mapping*

STIX FIELD	THREATQ FIELD MAPPING	THREATQ NAME
Title	Exploit Target.value	
ID	Exploit Target.attribute	STIX Reference ID

STIX FIELD	THREATQ FIELD MAPPING	THREATQ NAME
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	

STIX FIELD	THREATQ FIELD MAPPING	THREATQ NAME
	Indicator.type	Filename
	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	

STIX FIELD	THREATQ FIELD MAPPING	THREATQ NAME
	Indicator.type	URL
	Indicator.value	
	Indicator.type	Email Subject
	Indicator.value	
	Indicator.type	Email Address
	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

STIX FIELD	THREATQ FIELD MAPPING	THREATQ NAME
	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	
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

STIX FIELD	THREATQ FIELD MAPPING	THREATQ NAME
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
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

STIX FIELD	THREATQ FIELD MAPPING	THREATQ NAME
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
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

STIX FIELD	THREATQ FIELD MAPPING	THREATQ NAME
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
COA_Requested	Course of Action	

STIX FIELD	THREATQ FIELD MAPPING	THREATQ NAME
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

STIX FIELD	THREATQ FIELD MAPPING	THREATQ NAME
	TTP.attribute	Malware Type
	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

STIX FIELD	THREATQ FIELD MAPPING	THREATQ NAME
	TTP.attribute	Infrastructure Type
	TTP.attribute	Infrastructure
	TTP.attribute	Infrastructure Short Description
	TTP.attribute	Infrastructure Description
	Indicator	
	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

STIX FIELD	THREATQ FIELD MAPPING	THREATQ NAME
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

STIX2.0 Data Mapping

You can click on the expand 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 Motivation
sophistication	Adversary.Attribute	Sophistication
revoked (if revoked == true)	Adversary.Attribute	Revoked
external_references[]	See External References	
personal_motivations	Adversary.Attribute	Personal Motivation

- > *Indicators Mapping*

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
created	Signature.Published_at	
description	Signature.Description	
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	
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

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
external_references	Observable.Attribute	External Reference See External References.
number_observed	Observable.Attribute	Number 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	

- >*Automous System Mapping*

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
type: autonomous-system	Indicator.Type	ASN

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
number	Indicator.Value	
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
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

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
to_refs	Event.Relationship Indicator.Relationship	To
cc_refs	Event.Relationship	CC
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.		

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
** To parse an indicator from an email message, the email must contain a **subject** field. *** 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

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
magic_number_hex	Indicator.Attribute	Magic Number Hex
mime_type	Indicator.Attribute	MIME Type
created	Indicator.Attribute	Created At
accessed	Indicator.Attribute	Last Accesse
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

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
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	
extensions.ntfs-ext.alternate_data_streams[].name	Indicator.Attribute	Alternate Dat Stream Nam
extensions.ntfs-ext.alternate_data_streams[].size	Indicator.Attribute	Alternate Dat 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

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
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 Pe Pixel
extensions.raster-image-ext.image_compression_algorithm	Indicator.Attribute	Image Compressio Algorithm
extensions.raster-image-ext.exif_tags{}.key/ value	Indicator.Attribute	Formatted as 'Image EXIF {key.title()}'
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 Cour
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

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
extensions.windows-pebinary-ext.number_of_symbols	Indicator.Attribute	PE Binary Symbol Tabl 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 Characteristi 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 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

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
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 Entr Point
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

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
		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 Versio
extensions.windows-pebinary-ext.optional_header.minor_os_version	Indicator.Attribute	Windows OS Minor Versio
extensions.windows-pebinary-ext.optional_header.major_image_version	Indicator.Attribute	Image Major Version
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 Versio
extensions.windows-pebinary-ext.optional_header.minor_subsystem_version	Indicator.Attribute	Subsystem Minor Versio
extensions.windows-pebinary-ext.optional_header.win32_version_value_hex	Indicator.Attribute	Win32 Versio Hex
extensions.windows-pebinary-ext.optional_header.size_of_image	Indicator.Attribute	Image Byte Size

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
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
extensions.windows-pebinary-ext.optional_header.dll_characteristics_hex	Indicator.Attribute	DLL Characteristi 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 Commi 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 Size

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
extensions.windows-pebinary-ext.optional_header.hashes{}		
extensions.windows-pebinary-ext.optional_header.hashes{}.key	Indicator.Type	MD5 / SHA-1 SHA-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 Nam
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

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ 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		
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	

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
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	

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
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
	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

Tasks

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 Indicator, Events, Adversary, 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**.
   The assignee receives a Notification Center alert about the task. This alert includes a link to the assigned task.

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.
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**.
Request Investigation Access	1. Choose **Investigations**. 2. Click the related investigation to open the Access Denied window. 3. Click the **Request Access** button. When you click this button, the investigation owner receives a Notification Center alert indicating you have requested access to the investigation.

Threat Library

The ThreatQ Threat Library provides an organized and searchable index of threat intel system objects that have been ingested into the ThreatQ Platform (TQ).

From the Threat Library, you can view system objects by type, search the Threat Library by Building Searches with Filter Sets, perform Bulk Actions on search results, and view Object Details.

Managing Your Library View

You can limit the object types displayed in your Threat Library view and configure which data columns will be displayed in your search results.

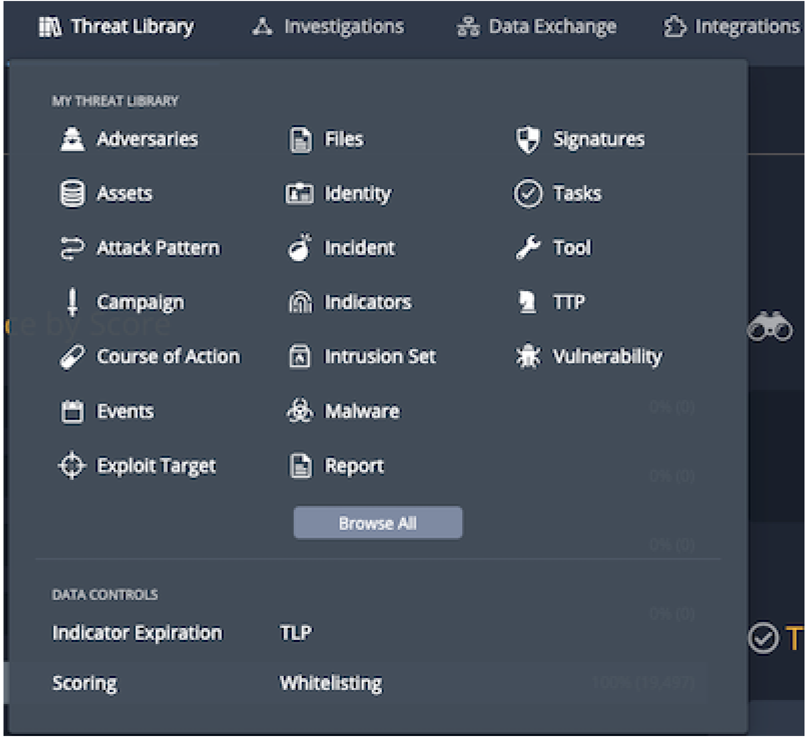
Selecting Object Type View

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 Type Filters 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** or **Browse All**.



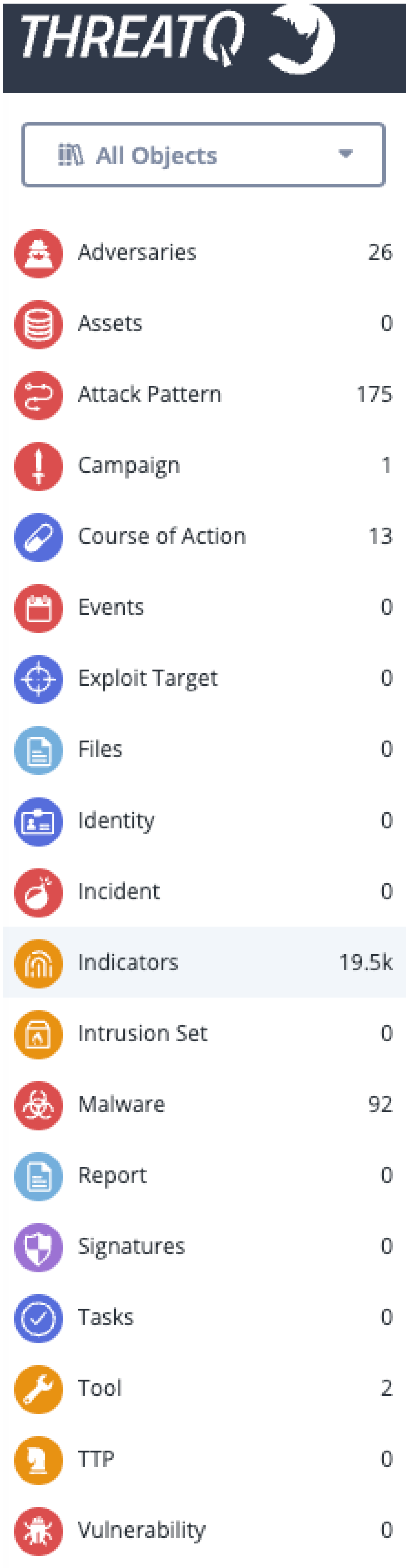
The Advanced Results page opens with the applied object type filter.

> You can also access the Data Controls from this menu.

Object Type Left-Hand Menu

You can use the left-hand menu of the Threat Library to select view specific system object types.

You can either use the **Object Type** dropdown list or click directly on a object type listed in the menu.

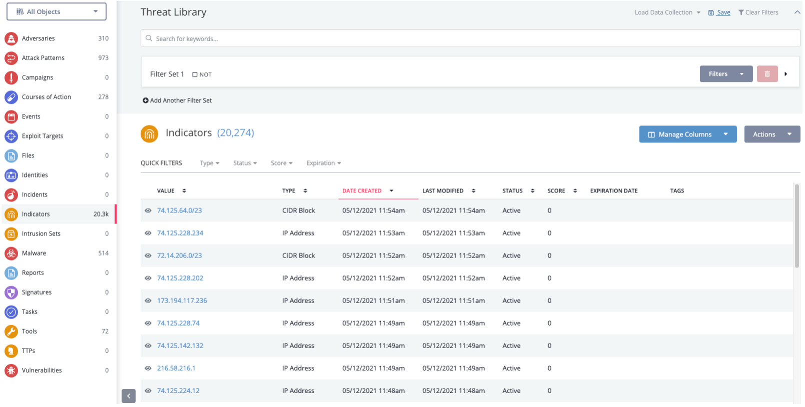


Adversaries	26
Assets	0
Attack Pattern	175
Campaign	1
Course of Action	13
Events	0
Exploit Target	0
Files	0
Identity	0
Incident	0
Indicators	19.5k
Intrusion Set	0
Malware	92
Report	0
Signatures	0
Tasks	0
Tool	2
TTP	0
Vulnerability	0

Managing Library Columns

You can choose which columns to display in your Threat Library view. Your column options will vary by object type.

1. Navigate to the Threat Library page.



Adversaries	310
Attack Patterns	973
Campaigns	0
Courses of Action	278
Events	0
Exploit Targets	0
Files	0
Identities	0
Incidents	0
Indicators	20.3k
Intrusion Sets	0
Malware	514
Reports	0
Signatures	0
Tasks	0
Tools	72
TTPs	0
Vulnerabilities	0

VALUE	TYPE	DATE CREATED	LAST MODIFIED	STATUS	SCORE	EXPIRATION DATE	TAGS
74.125.64.0/23	CIDR Block	05/12/2021 11:54am	05/12/2021 11:54am	Active	0		
74.125.228.234	IP Address	05/12/2021 11:53am	05/12/2021 11:53am	Active	0		
72.14.206.0/23	CIDR Block	05/12/2021 11:52am	05/12/2021 11:52am	Active	0		
74.125.228.202	IP Address	05/12/2021 11:52am	05/12/2021 11:52am	Active	0		
173.194.117.236	IP Address	05/12/2021 11:51am	05/12/2021 11:51am	Active	0		
74.125.228.74	IP Address	05/12/2021 11:49am	05/12/2021 11:49am	Active	0		
74.125.142.132	IP Address	05/12/2021 11:49am	05/12/2021 11:49am	Active	0		
216.58.216.1	IP Address	05/12/2021 11:49am	05/12/2021 11:49am	Active	0		
74.125.224.12	IP Address	05/12/2021 11:48am	05/12/2021 11:48am	Active	0		

2. Click the **Manage Columns** button.
3. Use one of the following methods to locate the columns you want to display/hide:
    - Scroll through the list of column options.
    - Begin typing the column name until it is displayed below the search field.
4. To display a column, check the checkbox next to the column name.
5. To hide a column, uncheck the checkbox next to the column name.

> You can click the values in related object columns to view a list of the related objects. For instance, if the Related Adversaries column lists a value of 10, you can click the 10 to view a list of the ten related adversaries. To return from this list to your original review, use your browser back button or remove the filter set displayed above the list.

Basic Search

The basic Search, located to the right of the **Create** button in the ThreatQ navigation, allows you to find objects you are looking for quickly, without having to browse through a large number of objects.

Basic Search allows you to search for all objects in the system: Indicator, Events, Adversary, Files, Signatures, and so on. The search capability looks at high level aspects of each object, including:

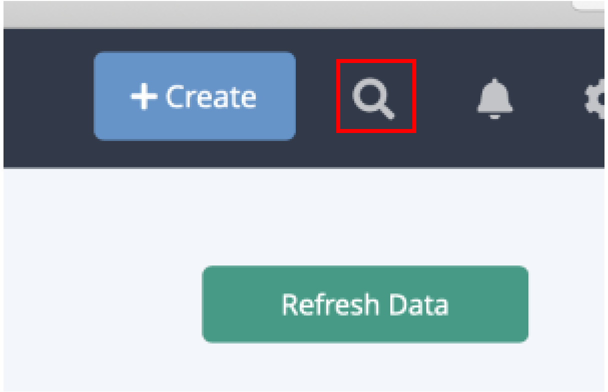
- Indicators (network or host)
- Attachment titles, hashes, keywords
- Attributes
- Adversary name
- Event title

For example, if you search for google.com, the following indicators are also returned:

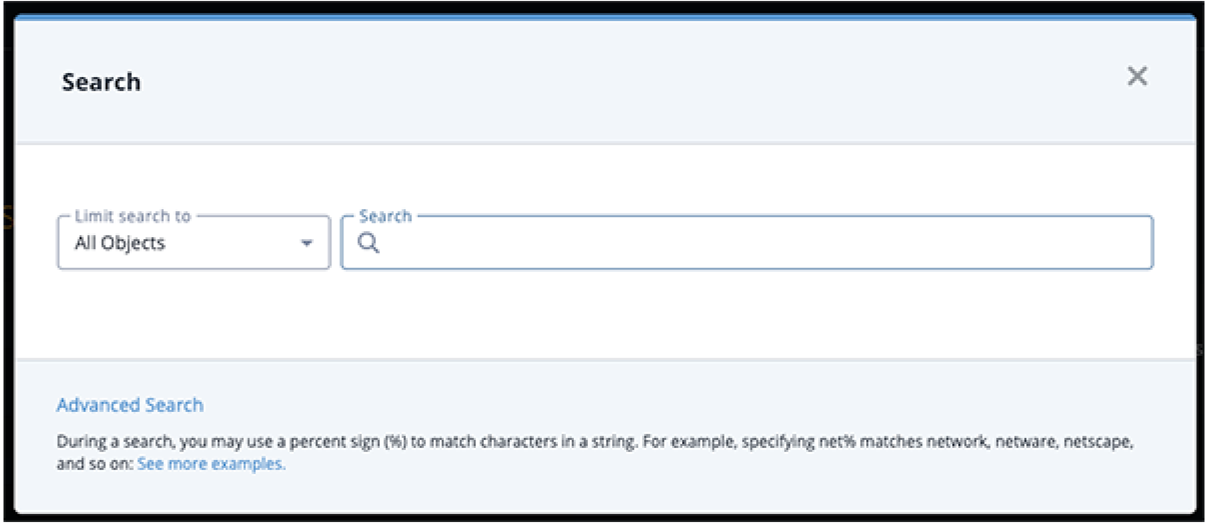
- www.google.com (FQDN)
- analytic.google.com (FQDN)
- www.google.com/analytic (URL)
- analytic@google.com (email address)

Performing a Basic Search

1. Choose the Search icon.



The Search dialog box appears.



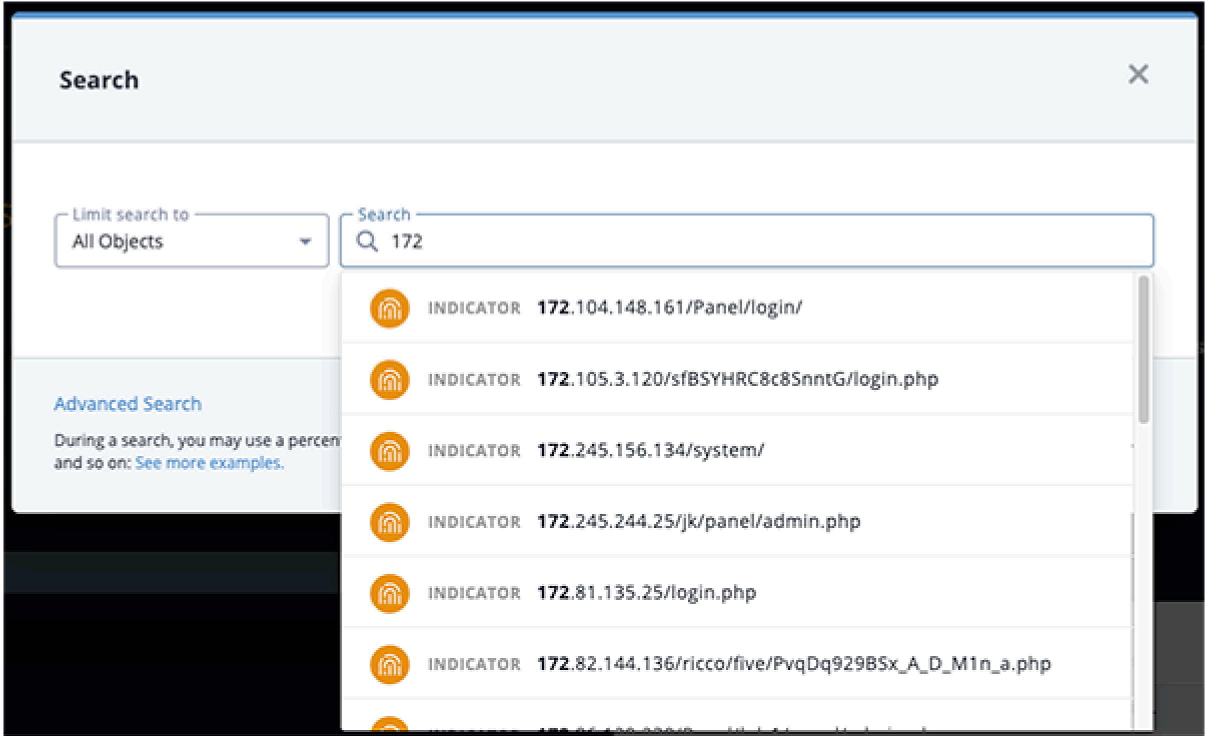
Limit search to: All Objects

Search:

During a search, you may use a percent sign (%) to match characters in a string. For example, specifying net% matches network, netware, netscape, and so on: See more examples.

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.



Limit search to: All Objects

Search: 172

INDICATOR **172**.104.148.161/Panel/login/
INDICATOR **172**.105.3.120/sfBSYHRC8c8SnntG/login.php
INDICATOR **172**.245.156.134/system/
INDICATOR **172**.245.244.25/jk/panel/admin.php
INDICATOR **172**.81.135.25/login.php
INDICATOR **172**.82.144.136/ricco/five/PvqDq929BSx_A_D_M1n_a.php

During a search, you may use a percen
and so on: See more examples.

4. Select the desired result.
   - If you do not retrieve any search results, we recommend trying the Threat Library advanced search.
   - If there is only one result, the object details page appears.

Wildcards and Symbols in Searches

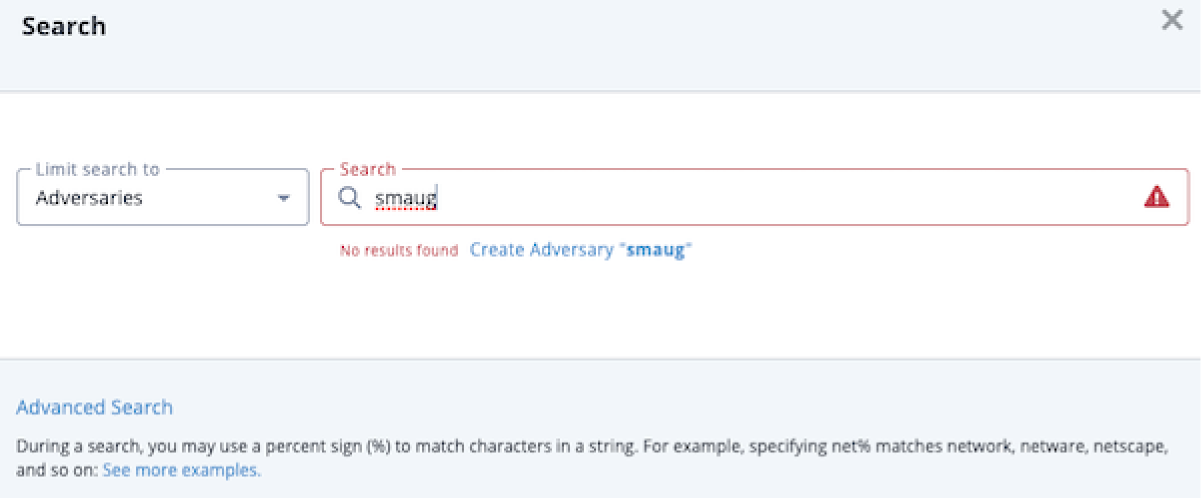
During a search, you may use a percent sign (%) to match characters in a string. The percent wildcard specifies that any characters can appear in multiple positions represented by the wildcard. For example, specifying net% matches network, netware, netscape, and so on.

Here are a number of examples showing search terms with percent wildcards:

SEARCH QUERY	DESCRIPTION
% panda	Finds any adversaries and indicators prefaced by another word, such as "red 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"
p%a	Finds any character string that contains "p" and "a" with characters between them, such as "panda" and "pappa"

Creating an Object During a Basic Search

The Basic Search window gives you the option to add a new object. If you enter an object name that is not found, you can click the **Create** link to select the object type from a drop-down list and add the new object. In addition, if you limit a basic search to a specific object type, you are linked to the corresponding form. For example, if you limit your search to Adversaries, the **Create** link opens the **Add An Adversary** form.



Search

Limit search to: Adversaries

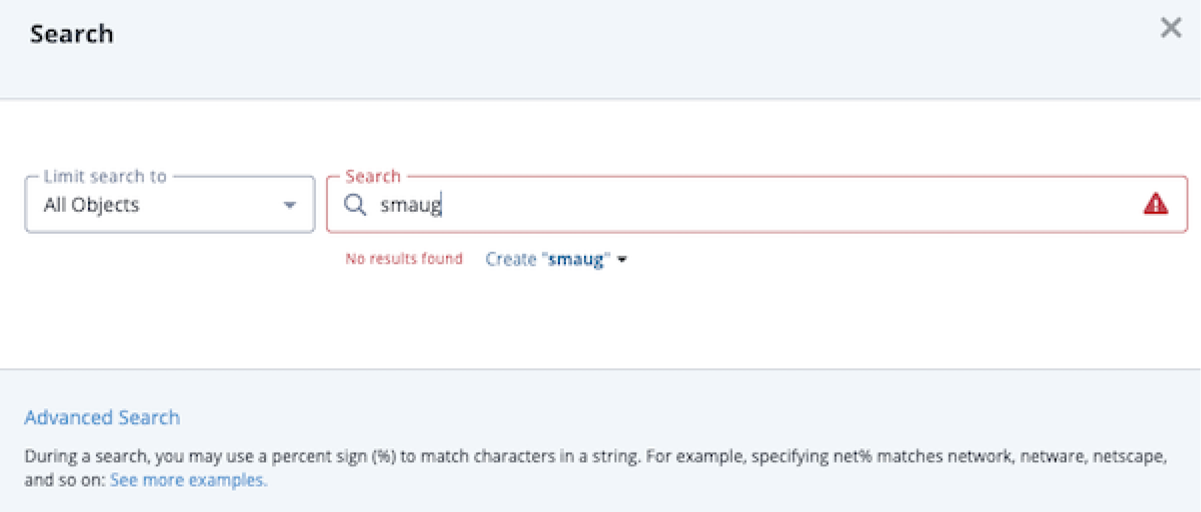
Search: smaug

No results found Create Adversary "**smaug**"

Advanced Search

During a search, you may use a percent sign (%) to match characters in a string. For example, specifying net% matches network, netware, netscape, and so on: See more examples.

If you leave the **Limit search to** field set to All Objects, you can select the object type you want to create from a drop-down list.



Search

Limit search to: All Objects

Search: smaug

No results found Create "**smaug**"

Advanced Search

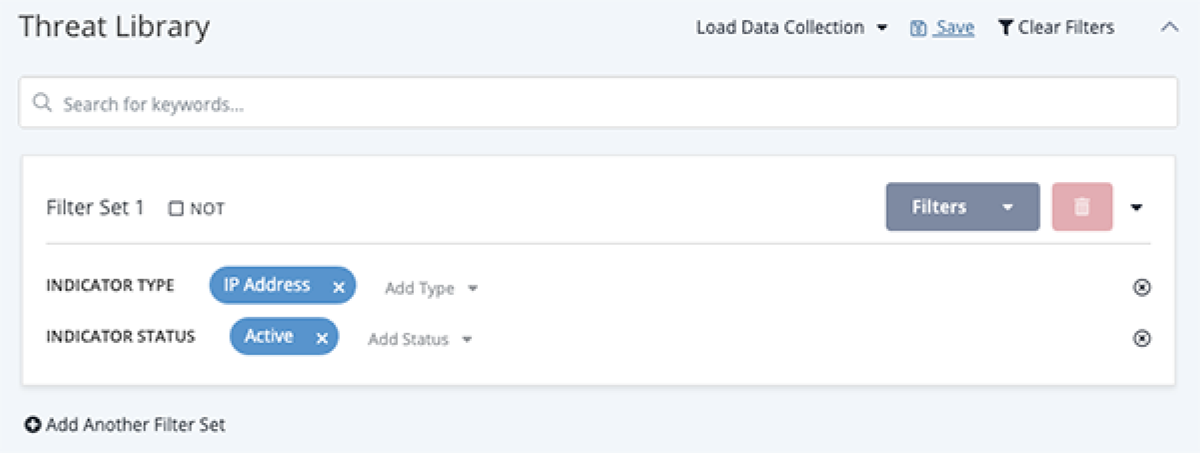
During a search, you may use a percent sign (%) to match characters in a string. For example, specifying net% matches network, netware, netscape, and so on: See more examples.

Building Searches with 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 section in the Managing Search Results topic for more details.

Adding Filter Sets

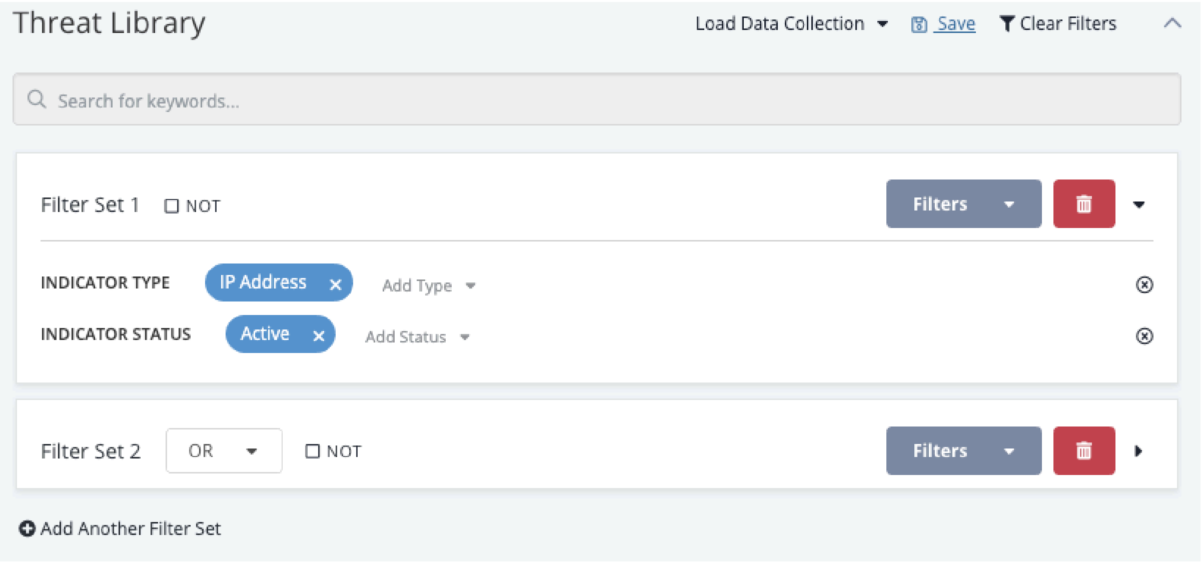
1. Use the **NOT** checkbox to determine if the filters in the initial filter set will be used to include or exclude Threat Library objects.
2. Select one or more filters for the search.



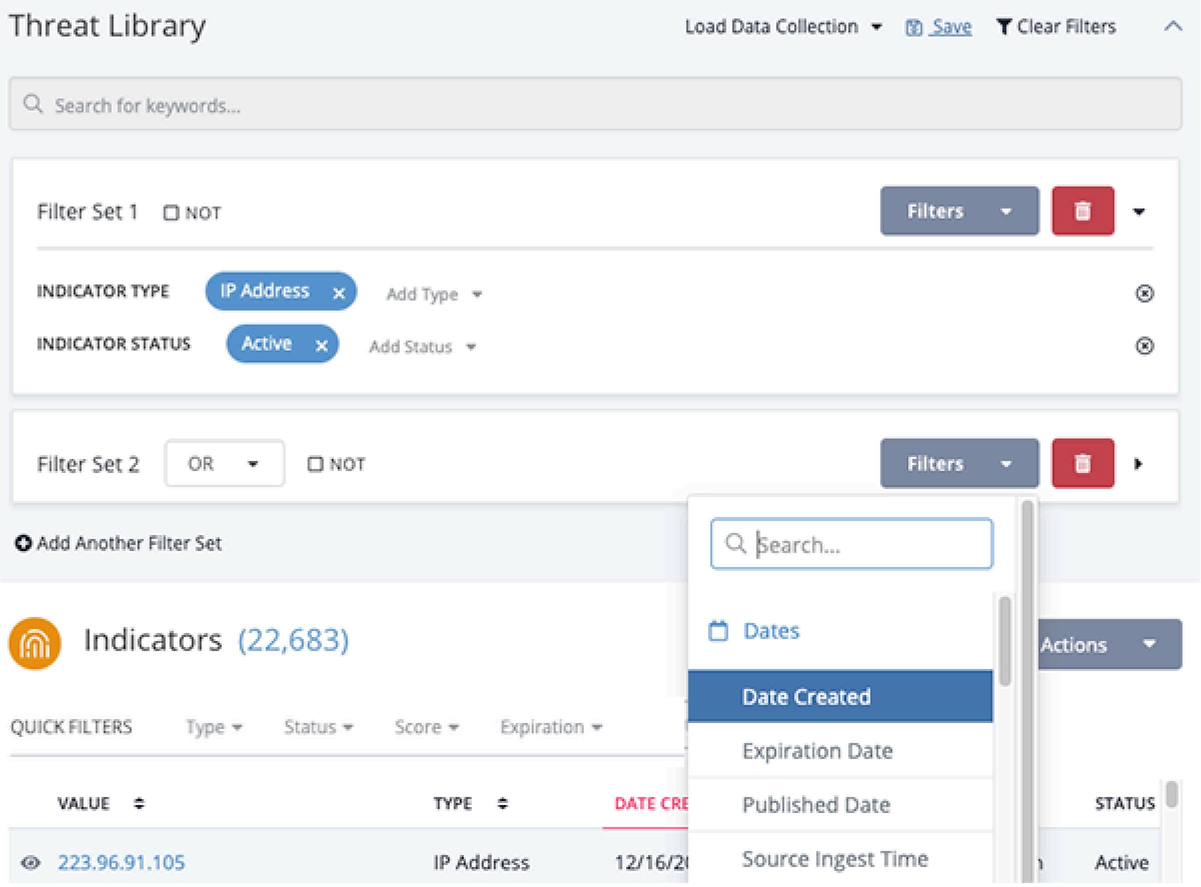
   You can use the search box provided at the top of the filters dropdown to narrow down the list of available filters.

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

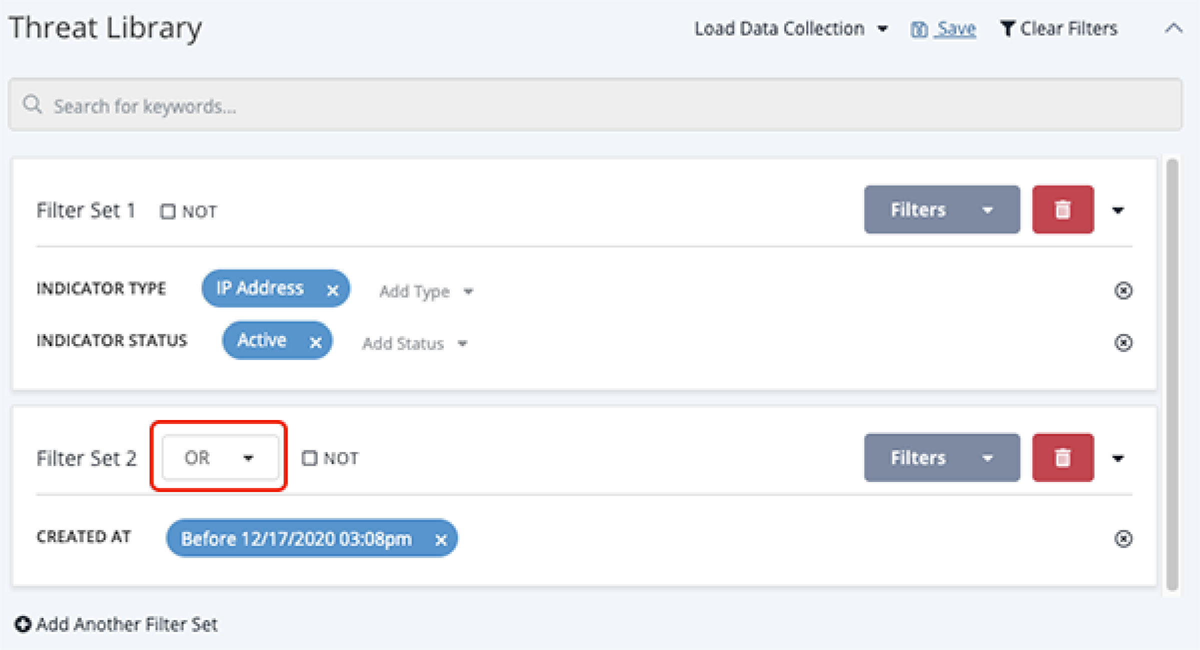
A new Filter Set table will load below the first set.



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.

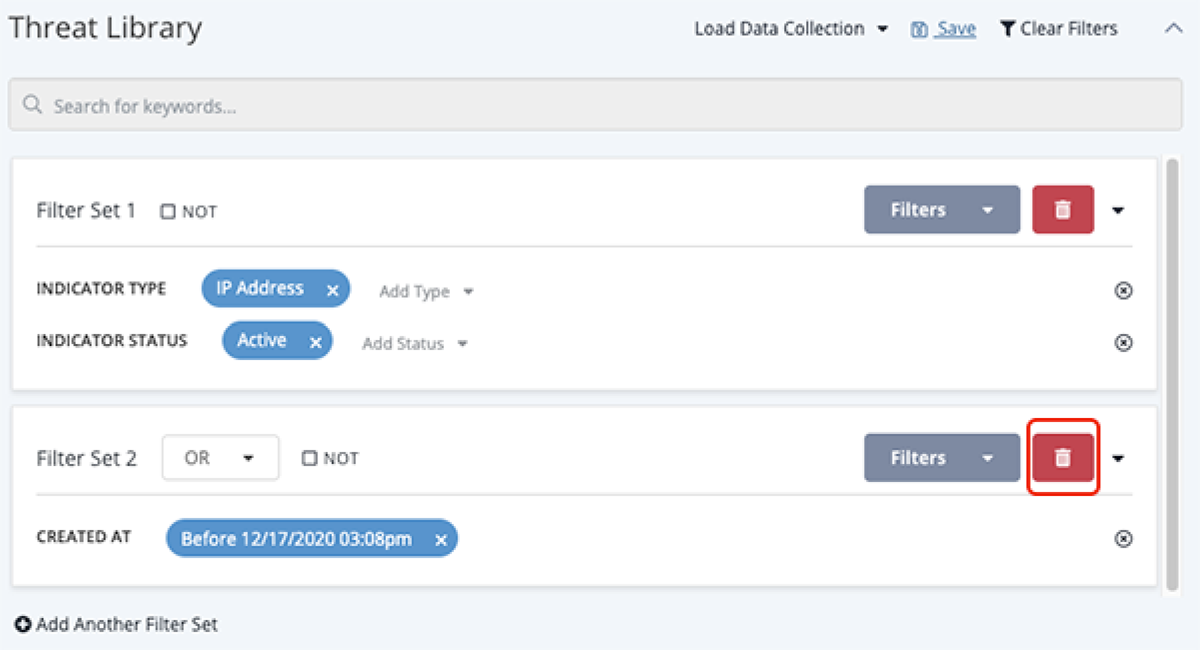


Repeat steps 3-6 to add additional filter sets.

Deleting Filter Sets

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

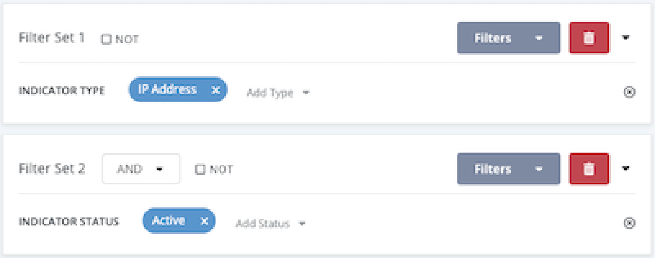
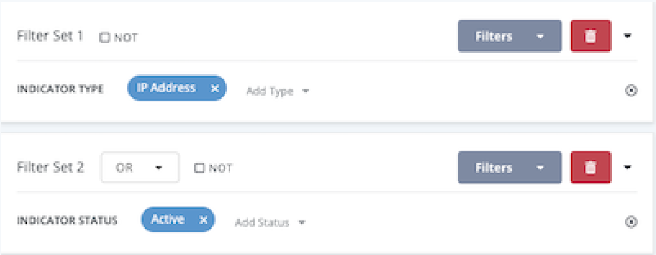
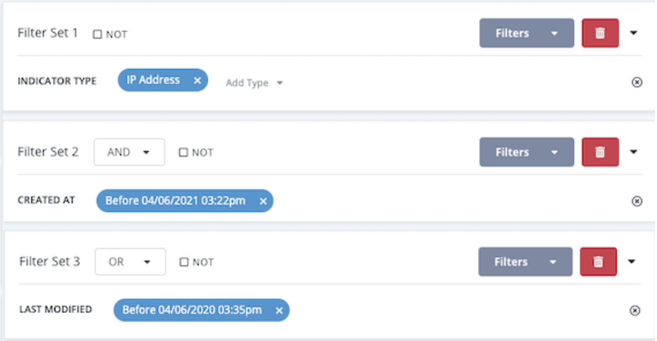
1. Click on the delete 🗑 icon located next to the right of the Filters dropdown.

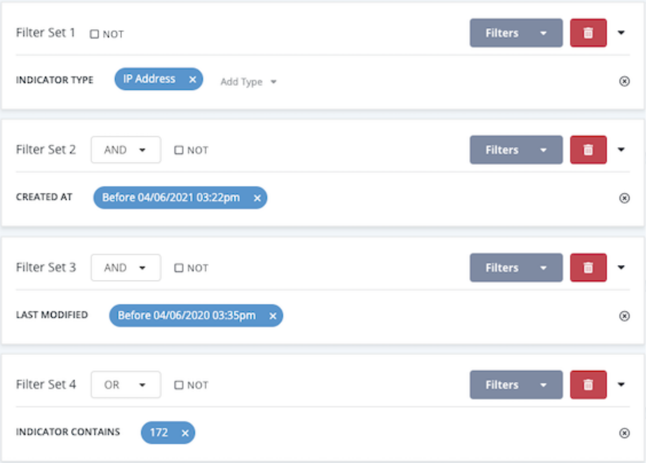
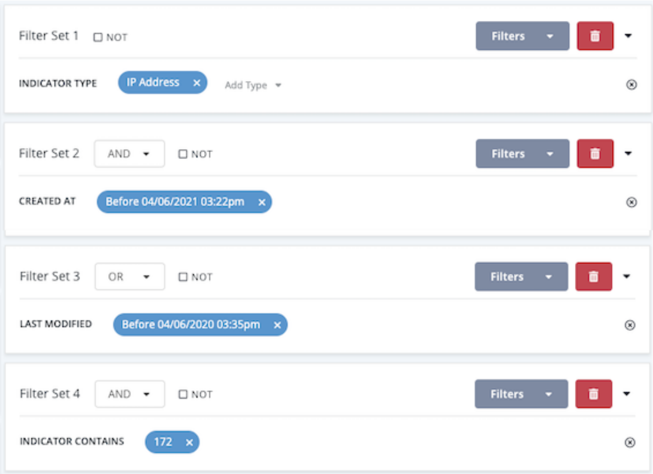


> You can click on **Clear Filters**, located above the filter sets, to remove all filter sets from the current search.

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	 Filter Set 1 ☐ NOT INDICATOR TYPE IP Address Filter Set 2 AND ☐ NOT INDICATOR STATUS Active
Single OR	Filter 1 OR Filter 2	 Filter Set 1 ☐ NOT INDICATOR TYPE IP Address Filter Set 2 OR ☐ NOT INDICATOR STATUS Active
Single AND, Single OR	(Filter 1 AND Filter 2) OR Filter 3	 Filter Set 1 ☐ NOT INDICATOR TYPE IP Address Filter Set 2 AND ☐ NOT CREATED AT Before 04/06/2021 03:22pm Filter Set 3 OR ☐ NOT LAST MODIFIED Before 04/06/2020 03:35pm

SCENARIO	ORDER	EXAMPLE
Multiple ANDs, Single OR	(Filter 1 AND Filter 2 AND Filter 3) OR Filter 4	 Filter Set 1 ☐ NOT INDICATOR TYPE IP Address × Filter Set 2 AND ☐ NOT CREATED AT Before 04/06/2021 03:22pm × Filter Set 3 AND ☐ NOT LAST MODIFIED Before 04/06/2020 03:35pm × Filter Set 4 OR ☐ NOT INDICATOR CONTAINS 172 ×
Multiple ANDs, Multiple ORs	(Filter 1 AND Filter 2) OR (Filter 3 AND Filter 4)	 Filter Set 1 ☐ NOT INDICATOR TYPE IP Address × Filter Set 2 AND ☐ NOT CREATED AT Before 04/06/2021 03:22pm × Filter Set 3 OR ☐ NOT LAST MODIFIED Before 04/06/2020 03:35pm × Filter Set 4 AND ☐ NOT INDICATOR CONTAINS 172 ×

Context Filters

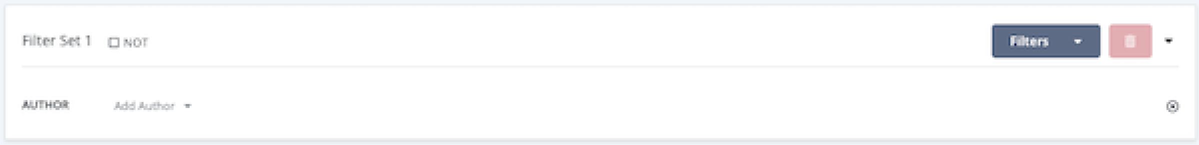
Context filters allow you to filter advanced search results by specific details associated with an object.

Filtering by Author

The Author context filter allows you to filter the system objects displayed based on the object’s source author. It allows you to filter by:

- Configuration Driven Feed (CDF)
- Operation
- ThreatQ Data Exchange (TQX) feed
- ThreatQ TDR Orchestrator (TQO) Workflow/CDW
- User

1. Click the **Filters** option and select **Author**.
   The Author row is displayed under the filter set name.



2. Click the **Add Author** option to access a drop-down list of authors.
3. Locate and click the checkbox next to the author value(s) for your filter by scrolling through the drop-down list or entering the name in the Search field. You can select one or more authors at a time from this list.

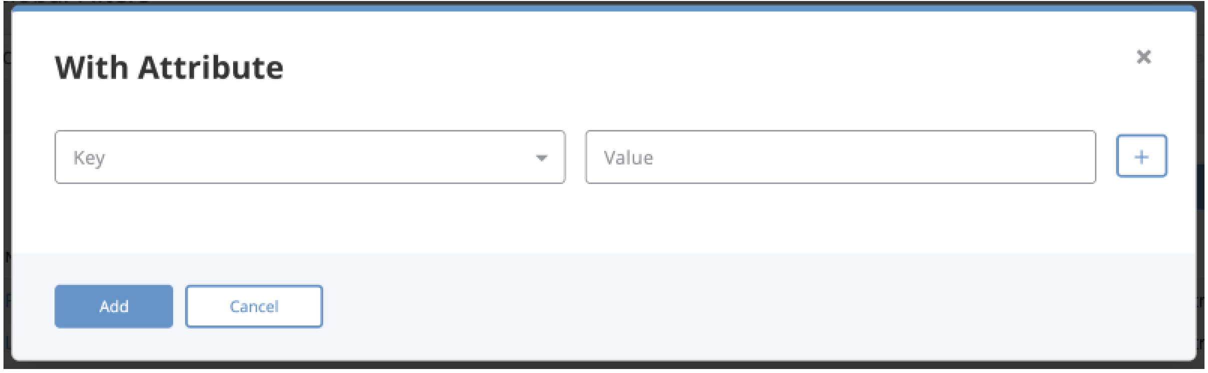
   When you apply the Author filter, the Author column is automatically added to the results listing. The Author column displays the source author(s) listed alphabetically in pill format.

Filtering by Attribute

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

1. Click 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**.
   When you apply a **With Attribute** filter, you can use wildcard values to more easily locate indicators. The Value field supports the following search methods:

SEARCH TYPE	SEARCH QUERY	SEARCH RESULTS
Exact Match	us	US only
Ends With	*us or %us	US and Lazarus
Begins With	us* or us%	US, USBferry, and USBStealer
Value Contains	*us* or %us%	US, USBferry, USBStealer, Lazarus, and Dust Storm

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

4. Click the **Add** button.
   The filters are applied to the search results.

Using Multiple Attribute Filters

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

Multiple Attribute Filters ANY - Match Toggle Selection Example

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.	

Multiple Attribute Filters ALL - Match Toggle Selection Example

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.

Attribute Common Scenarios

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**.

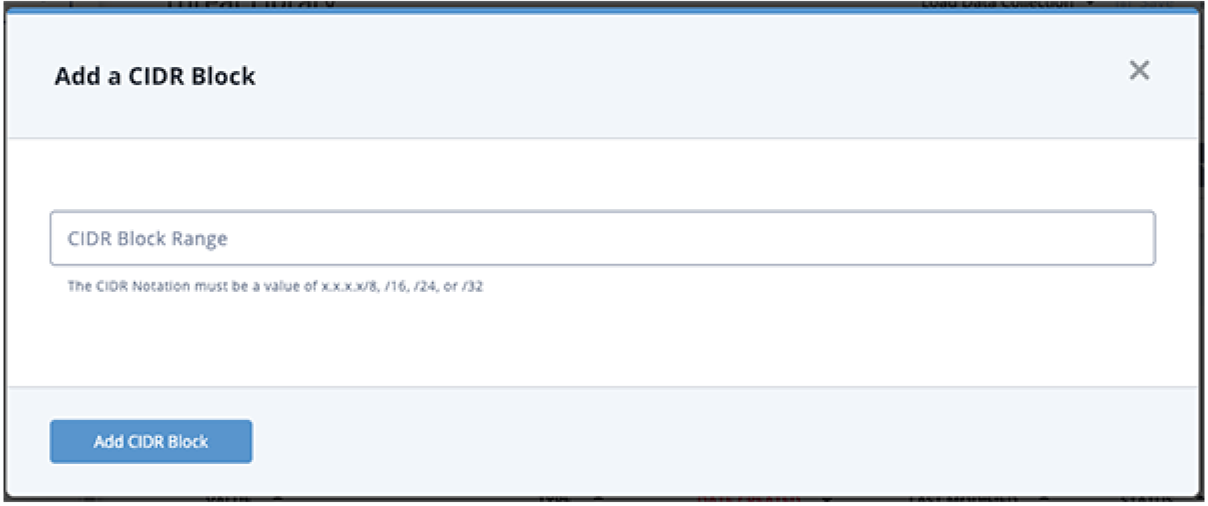
   The filtered results will display any indicator that has both of those attributes

Filtering by CIDR Block Range

You can filter Threat Library objects by a block of IP addresses using the CIDR block range filter. The CIDR Block Range filter allows you to specify a CIDR block with prefix and suffix for an IPv4 search.

1. Click the **Filters** option and select **CIDR block range**.

   The Add a CIDR Block dialog box opens.



The CIDR Notation must be a value of x.x.x.x/8, /16, /24, or /32

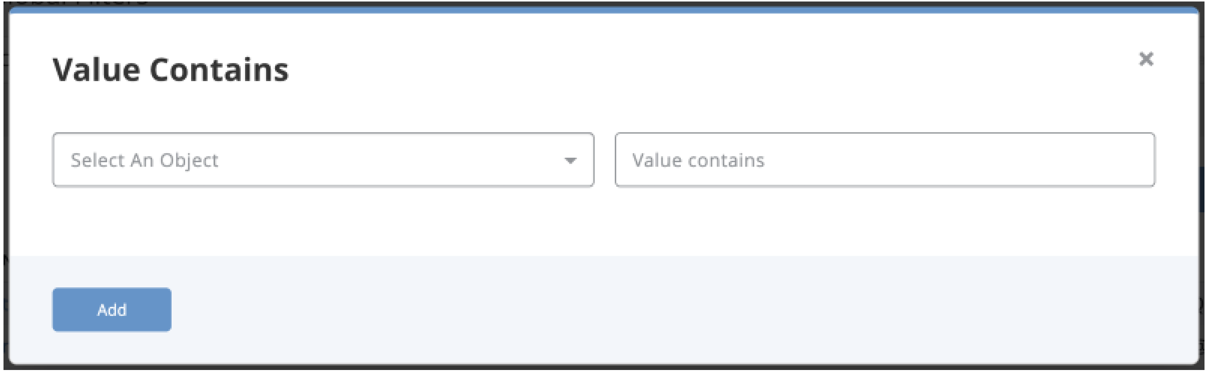
2. Enter the CIDR block in one of the following formats:
    - x.x.x.x/8
    - x.x.x.x/16
    - x.x.x.x/24
    - x.x.x.x/32
3. Click **Add CIDR Block** to apply the filter.

Filtering by Value Contains

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

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

   The Contains dialog box opens.



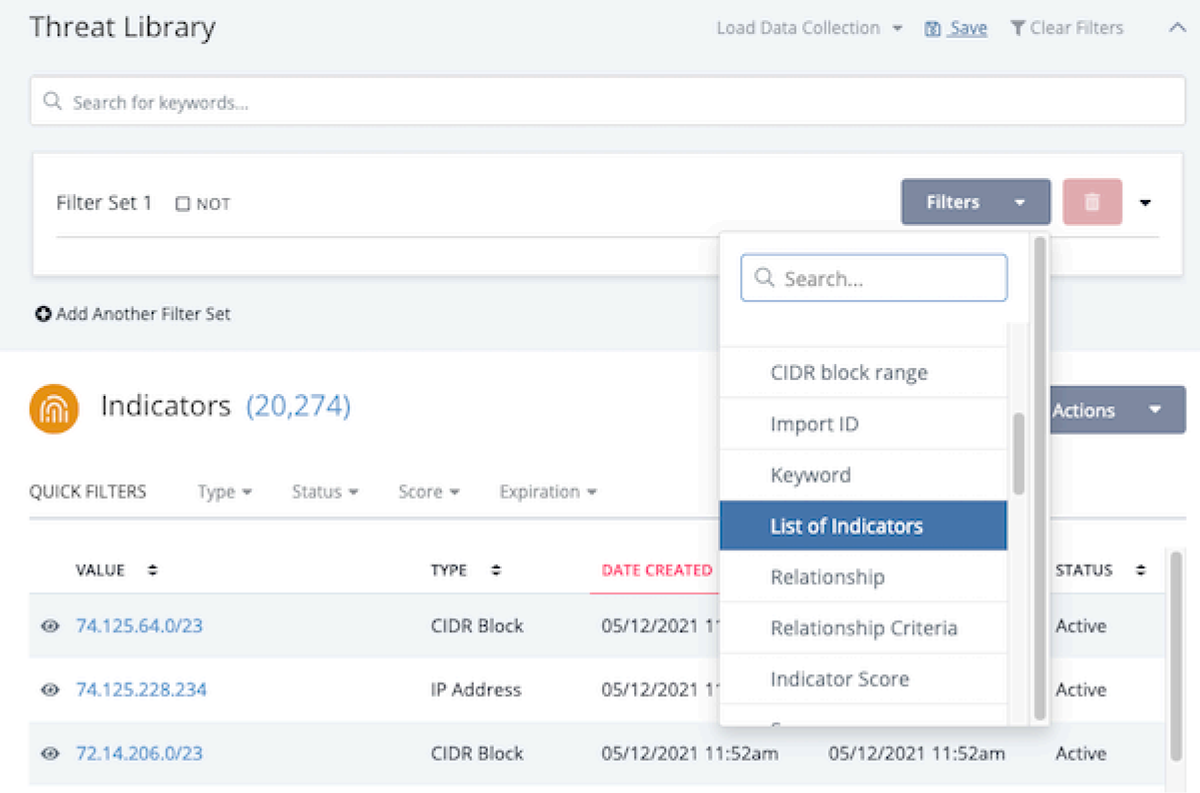
2. Select an **Object**, enter a **Value**, and click **Add** to apply the filter.

Filtering by List of Indicators

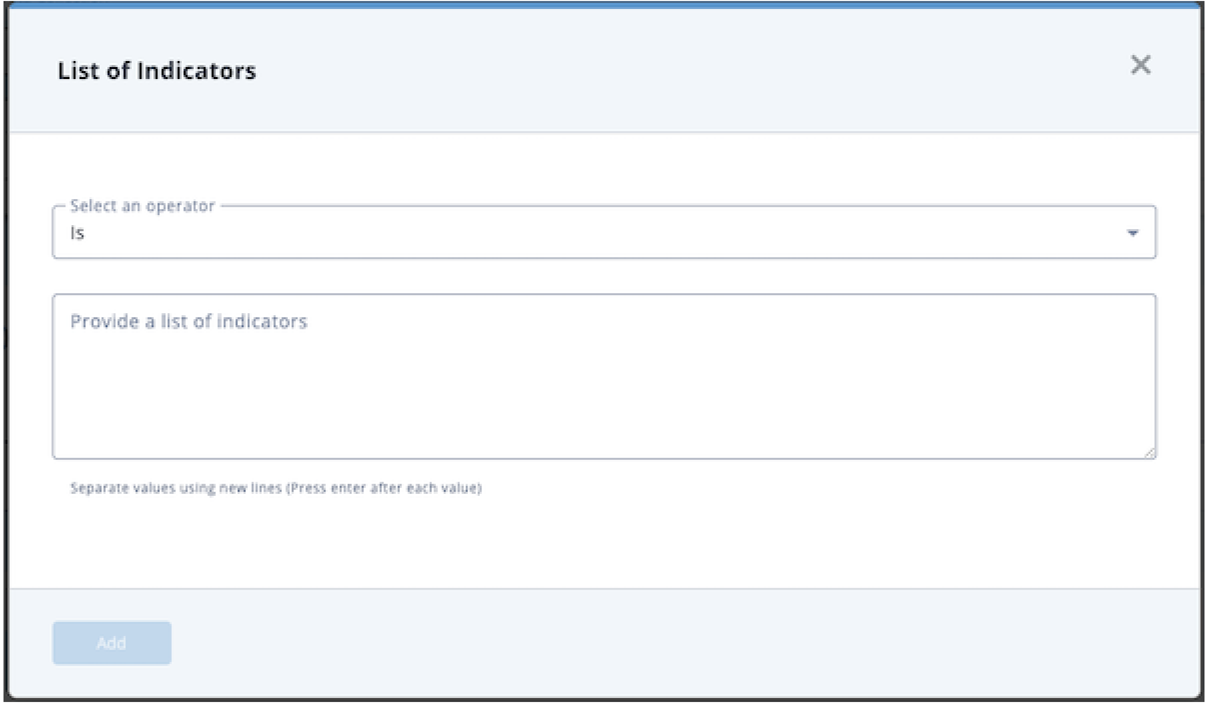
The List of Indicators Filter option allows you to filter the Threat Library by pasting a list of indicators, in raw text.

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

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

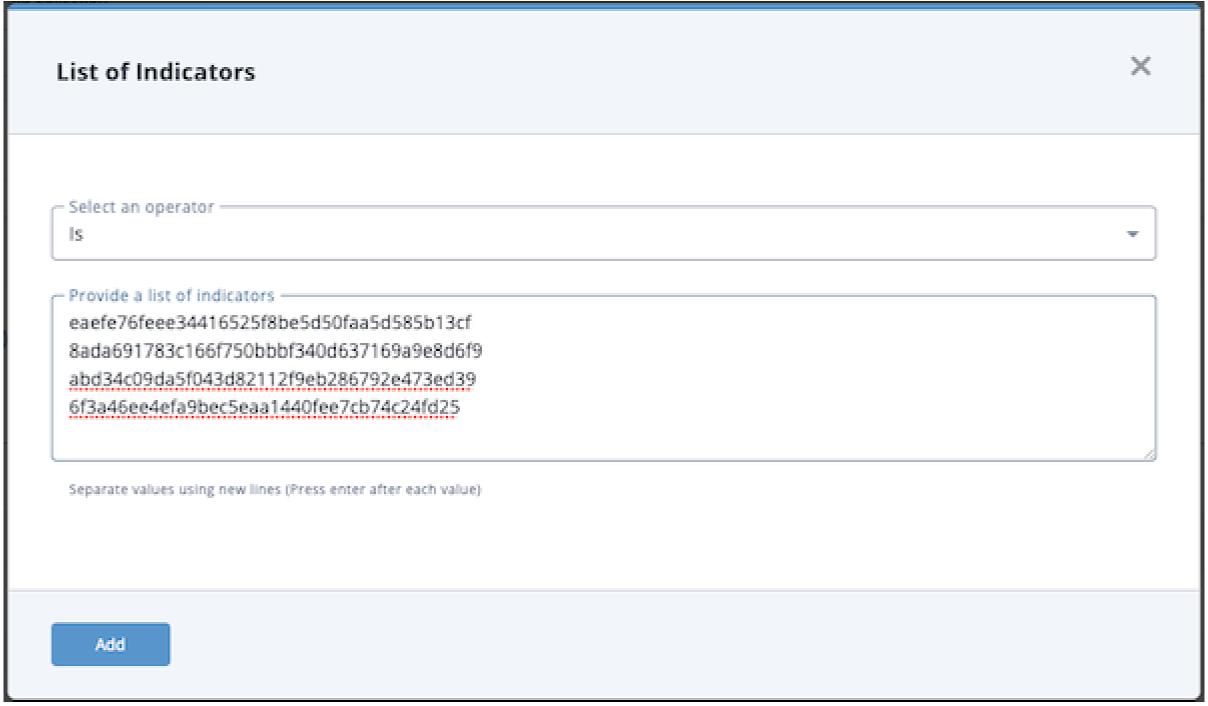


The List of Indicators dialog box opens.


List of Indicators
Select an operator
Is
Provide a list of indicators
Separate values using new lines (Press enter after each value)
Add

2. The **Specify an operator** field defaults to a value of *Is* which returns exact matches. However, you can click the arrow next to this field and select *Contains* as the operator to return partial matches.

3. Enter or paste your list of indicators in the **Provide a list of indicators** field.



Select an operator: Is

Provide a list of indicators:

```
eaefe76feee34416525f8be5d50faa5d585b13cf
8ada691783c166f750bbbf340d637169a9e8d6f9
abd34c09da5f043d82112f9eb286792e473ed39
6f3a46ee4efa9bec5eaa1440fee7cb74c24fd25
```

Separate values using new lines (Press enter after each value)

The accepted list format is one indicator per line.

4. Click **Add** to apply the filter.

Filtering by Keyword

1. Enter your keyword search term or phrase in the **Search for keywords** field and press Enter
   OR
   Click the **Filters** option and select Keyword to access the Filter by Keyword window. Then, enter your search term or phrase in the **Keyword** field and click the Add button.
2. To add more keywords, repeat step 1.
3. If you add more than one keyword, you can specify a **Must Match** setting of:
   - **ANY** - Search results include objects that include any of the keywords.
   - **ALL** - Search results include objects that include all of the keywords.
4. Click 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
   - Spearphish Value (for Events of Type 'Spearphish')

- 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
- 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

  - Event Type Name
  - Event Description
  - Spearphish Subject (for Events of Type 'Spearphish')
  - Task Assignee Source Name
  - Task Creator Source Name

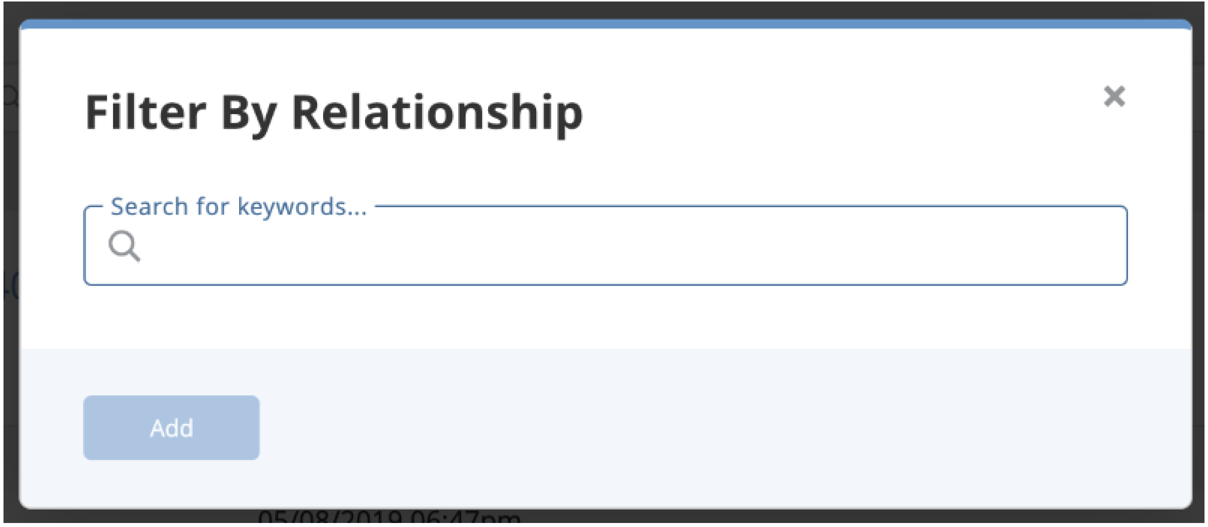
Filtering by Relationship

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.

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

   The Filter by Relationship dialog box opens.



2. Use the text box provided to select an object.
3. Click **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.

Filtering by Relationship ANY - Match Toggle Selection Example

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.

Filtering by Relationship ALL - Match Toggle Selection Example

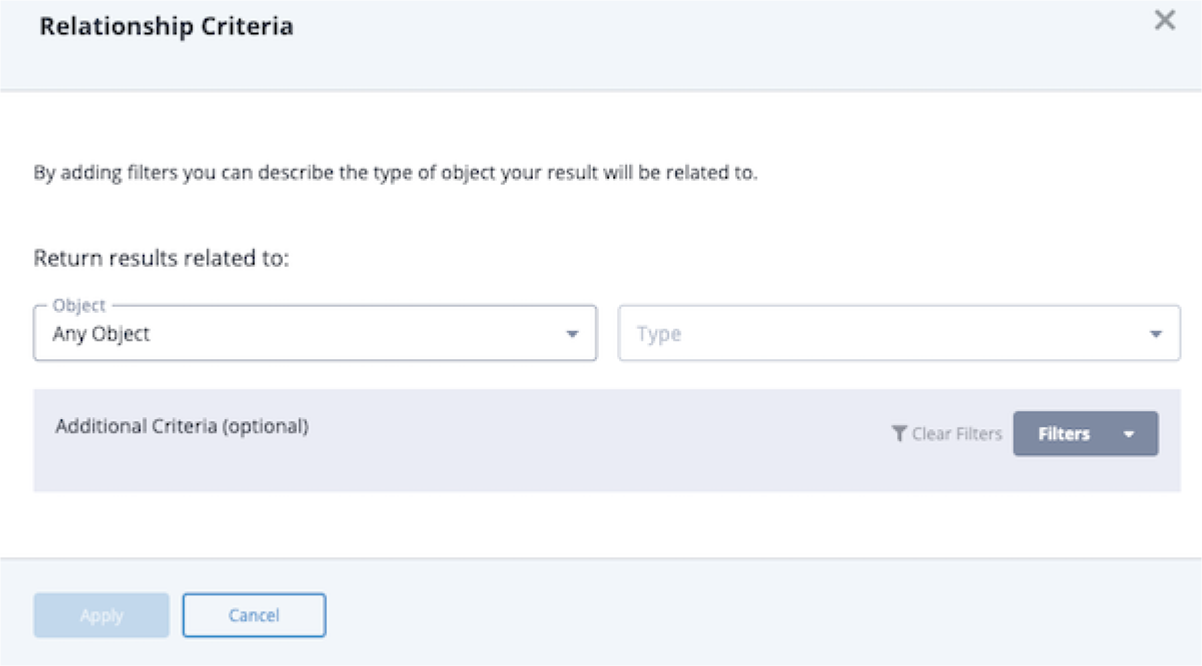
SETTING	RELATED OBJECT
Filter A	ABC Indicator
Filter B	DEF Event
Filter Option	All
Result	Search Results are filtered to include objects related to the ABC Indicator **AND** the DEF Event.

Filtering by Relationship Criteria

The Relationship Criteria filter allows you to filter system objects based on the characteristics of their related objects. For instance, you can filter a list of indicators to include only those with related login compromise event objects.

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

   The **Relationship Criteria** dialog box opens.


Relationship Criteria
×
By adding filters you can describe the type of object your result will be related to.
Return results related to:
Object
Any Object
Type
Additional Criteria (optional)
Clear Filters
Filters
Apply
Cancel

2. Use the text box to select your **Object** and **Type**.
3. Optional. You can further filter your results based on the following additional criteria.

Date Created Filter

The Date Created option allows you to narrow your results based on the date a related object was created. This filter allows you to specify creation before or after a date, within a date range, or within a specific number of preceding days.

1. To add a Date Created filter, click the **Filters** dropdown and select **Date Created**.
2. Click the date type dropdown to specify creation before (**is before**) or after (**is after**) a date, within a date range (**is between**), or within a specific number of preceding days (**is within the last**).
3. Based on the date type you selected, enter a date and time, date and time range, or number of days.

Source Filter

The Source option allows you to filter your results based on one or more sources. In addition, you can specify that an object must meet all or at least one of your Source criteria.

1. To add a Source filter, click the **Filters** dropdown and select **Source**.
2. Click the Add Source option
3. Locate the source by scrolling through the list or typing the source name in the Search for sources field.
4. Click the source you want to add as a filter criteria.
5. To add more source filters, repeat steps 2 through 4.

> When you add multiple Source filters, the Must Match field allows you to select ALL to indicate that an object must meet the requirements of all the Source filters or ANY to specify that your results include objects that meet the requirements of at least one Source filter.

Value Contains Filter

1. To add a Value Contains filter, click the **Filters** dropdown and select **Value Contains**.
2. Enter your desired value in the field provided.

With Attribute Filter

The With Attribute option allows you to filter results based on one or more specific attribute keys or attribute key and value combinations. In addition, you can specify that an object must meet all or at least one of your With Attribute criteria.

1. To add a With Attribute filter, click the **Filters** dropdown and select **With Attribute**.
2. Enter the attribute key and attribute value (optional) you want to filter by.
3. To add more attribute key/value filters, click the + icon and repeat step 7.

> When you add multiple With Attribute filters, the Must Match field is displayed and defaults to ALL to indicate that an object must meet the requirement of all the With Attribute filters. You can change this value to ANY so that your results include objects that meet the requirements of at least one With Attribute filter.

Tag Filter

The Tag option allows you to filter your results based on the tag(s) associated with a related object. In addition, you can specify that an object must meet all or at least one of your Tag criteria.

1. To add a Tag filter, click the **Filters** dropdown and select **Tag**.
2. Click the Add Tag option
3. Locate the tag by scrolling through the list or typing the tag name in the Search for tags field.
4. Click the tag you want to add as a filter criteria.
5. To add more tag filters, repeat steps 2 through 4.

> When you add multiple Tag filters, the Must Match field allows you to select ALL to indicate that an object must meet the requirements of all the Tag filters or ANY to specify that your results include objects that meet the requirements of at least one Tag filter.

4. After you select all of your filter options, click **Apply** to filter your Threat Library results.

Filtering by Score

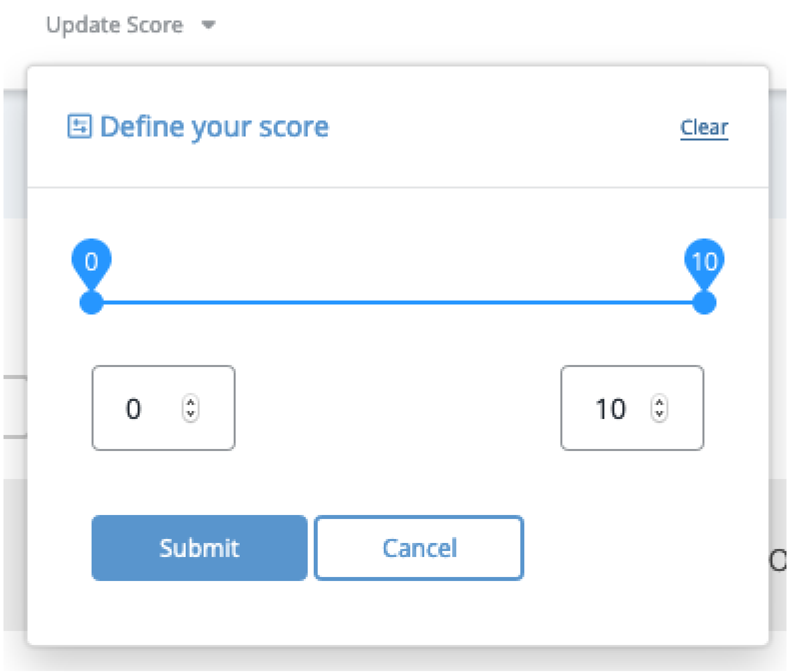
You can filter indicators in the advanced search results by score.

> This option is only available for indicators.

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 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.

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.

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

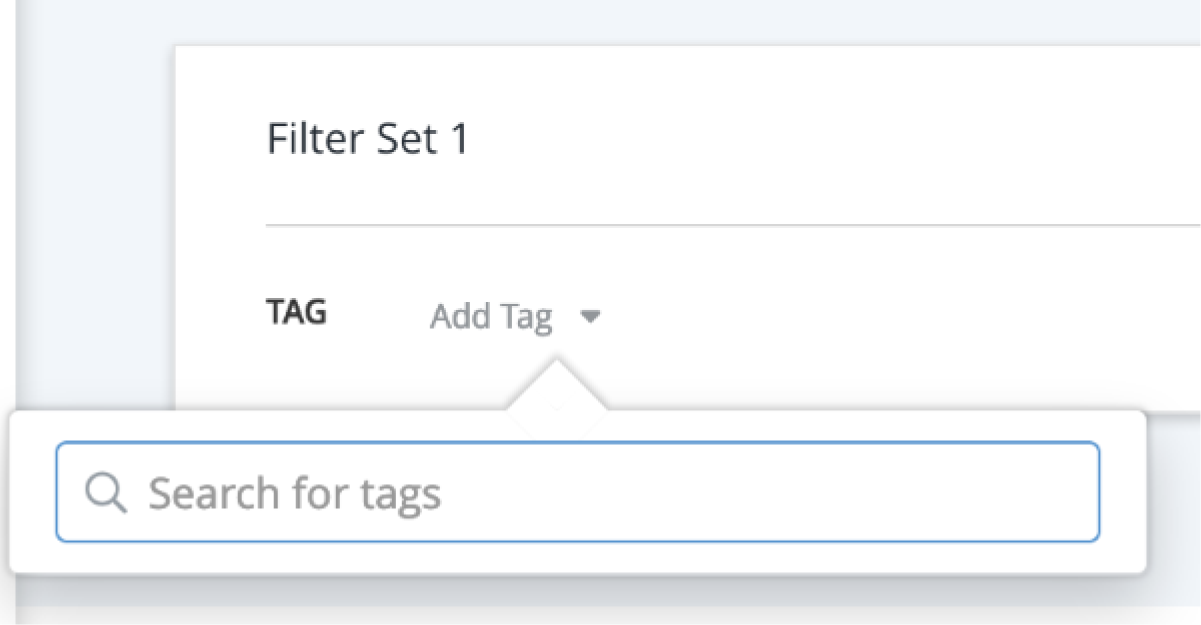
Select the **Update Score** filter again or select **Clear** to remove the filter.

Filtering by Tags

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

1. Click 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. Repeat 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.

ANY - Match Toggle Selection Example

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 Example

SETTING	TAG
Filter A	Phishing
Filter B	DDoS
Filter Option	All
Result	Search Results are filtered to include items with both Phishing **AND** DDoS tags.

Filtering by Source

The Source filter allows you to filter Threat Library search results by object or attribute source.

1. Click the **Filters** option and select **Source**.
   The Source row is displayed below the filter name.
2. Locate and select the source for your filter by scrolling through the drop-down list or entering the source in the Search for sources field.
3. Click the arrow next to Source to specify whether the filter references all sources or is restricted to object or attribute sources.
4. Click the checkbox next to **Is Only** to specify that the filter includes objects that only include the selected source(s) and do not include any other sources not specified by the filter.
5. To continue adding sources to the filter, click the Add Source option and repeat step 2.

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

Filtering by Source ANY - Match Toggle Selection Examples

SETTING	SOURCE
Filter A	This Platform
Filter B	Domain Tools
Filter Option	Any
Result	Search Results are filtered to include objects with a source of This Platform **OR** Domain Tools.

Filtering by Source ALL - Match Toggle Selection

SETTING	SOURCE
Filter A	This Platform
Filter B	Domain Tools
Filter Option	All
Result	Search Results are filtered to include objects with both This Platform **AND** Domain Tools as sources.

Filtering by TLP

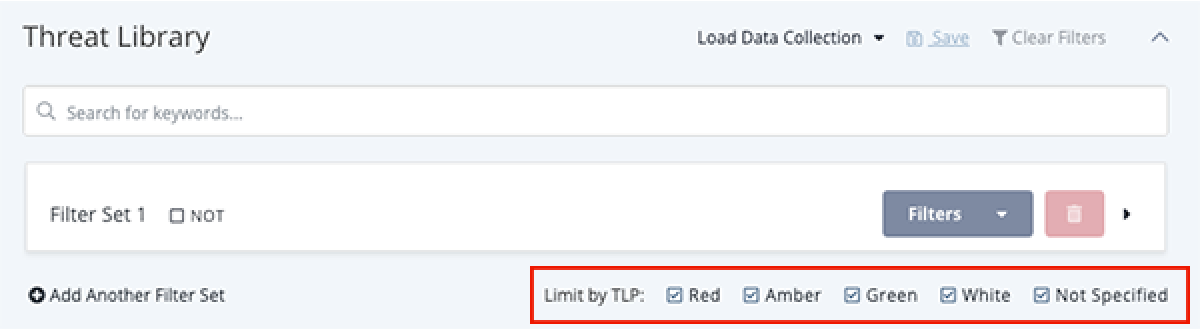
Users can filter Threat Library search results by specific TLP color designations. For reference on Traffic Light Protocol (TLP), view the Traffic Light Protocol (TLP) topic.

The filter functions in two ways. First, the filter will be applied to the object's source TLP and will only return system objects that contain a source that matches the TLP values selected in the TLP filter. The filter will then limit source and attribute column data of the search results to only display data that matches the TLP filter.

> TLP visibility must be enabled to use the TLP filter in the Threat Library search. See the Configure TLP Visibility section for more details.

1. Navigate to Threat Library.

   The option to filter by TLP color designation will be located under the search bar and Filter Set option.



Limit by TLP: ☑ Red ☑ Amber ☑ Green ☑ White ☑ Not Specified

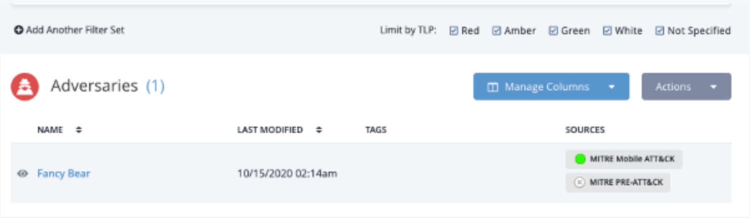
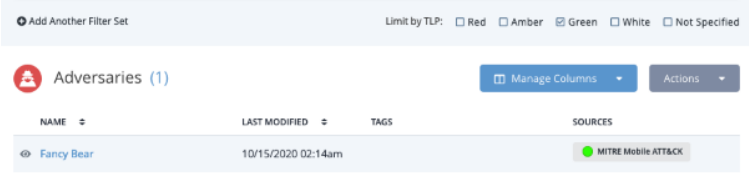
2. Use the **Limit by TLP** filter check boxes to select which TLP designations to apply to your search results.

   > If TLP Green is checked, only objects with any source of TLP Green will be returned in the search results.

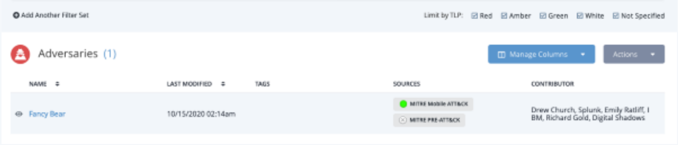
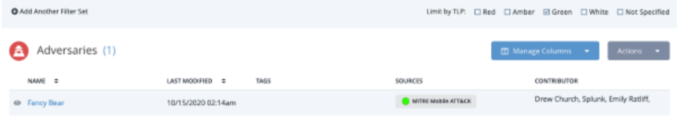
   From the Objects retrieved, the TLP filter also impacts the information returned in search results columns, including Sources and Attributes.

   Sources - In the Sources column of the search results, only sources that match the selected TLP colors will be displayed.

SCENARIO	RESULTS DISPLAY

Sources displayed before applying the TLP filter	
Sources displayed after applying the TLP filter	

Attributes - In any displayed Attribute column of the search results, only attribute values with sources that match the selected TLP colors will be displayed.

SCENARIO	RESULTS DISPLAY
Attribute Contributors displayed before applying the TLP filter	
Attribute Contributors displayed after applying the TLP filter	

Additional Notes:

- TLP filters can be stored as part of data collections, similar to other filter types.
- The TLP filter is a global filter in that it is applied across all object types and all filter sets for a given search query (i.e. it cannot be applied to individual object types or within individual filter sets).
- TLP filters impact the Threat Library CSV output and CSV results output will match those in the Threat Library results UI.
- In any displayed Attribute column of the search results, only attribute values with sources that match the selected TLP colors will be displayed.

Date Filters

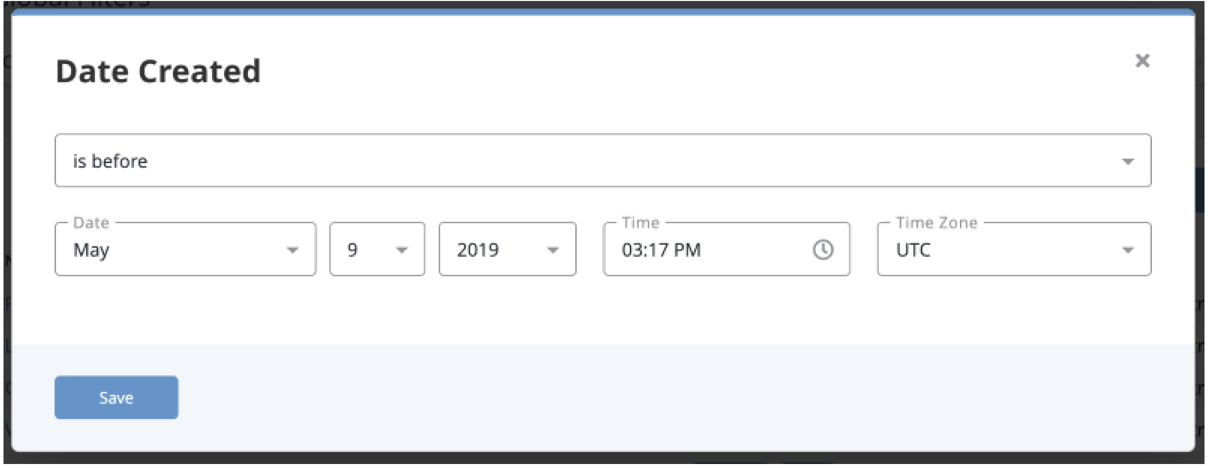
Date filters allow you to filter advanced search results by date-related values.

Filtering by Date Created

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

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

   The Date Created dialog box opens.



Date Created

is before

Date: May 9 2019

Time: 03:17 PM

Time Zone: UTC

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.

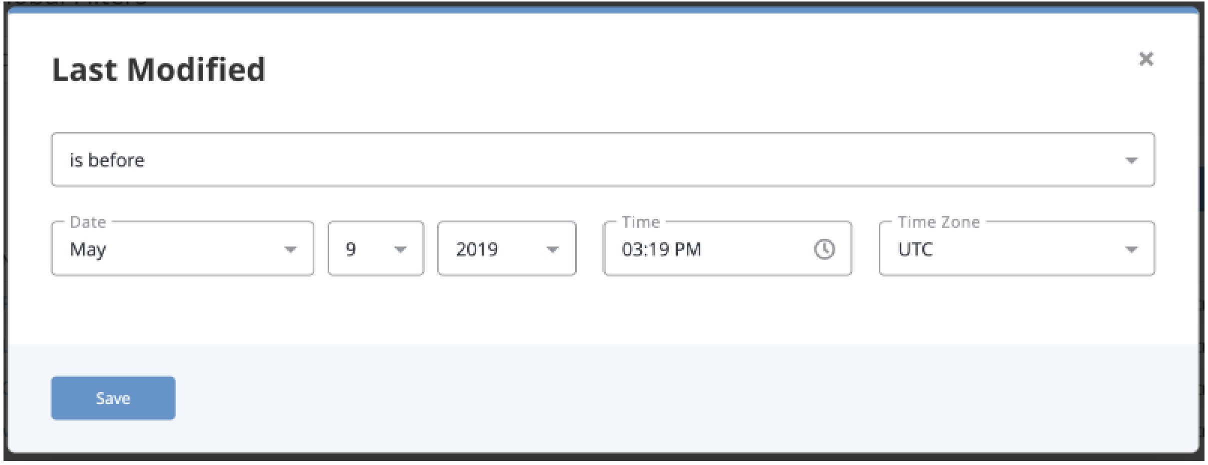
4. Click **Save**.

Filtering by Last Modified

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

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

   The Last Modified dialog box opens.



Last Modified

is before

Date: May

9

2019

Time: 03:19 PM

Time Zone: UTC

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

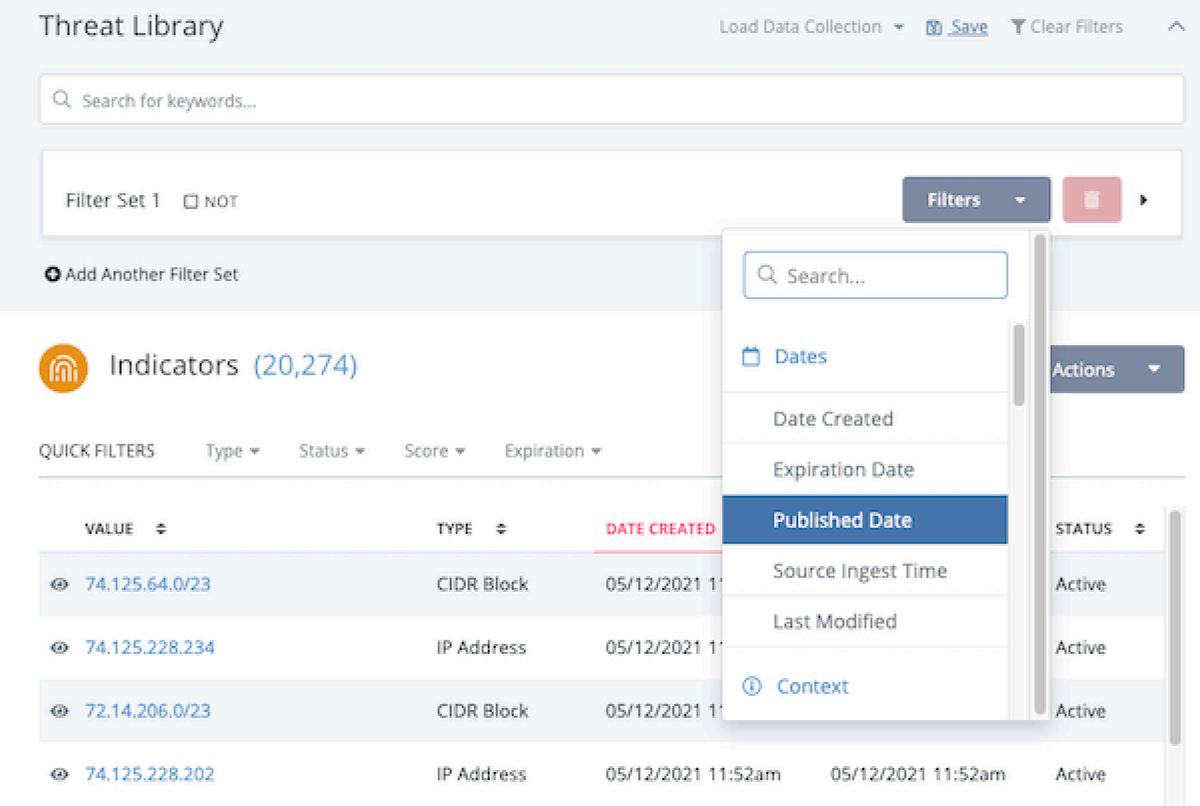
OPTION	RESULT
is before	Search results include items before a selected date
is after	Search results include items after a selected date
is in the range of	Search results include items in a selected range of dates
is within the last	Search results include items within the selected number of days.

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

Filtering by Published Date

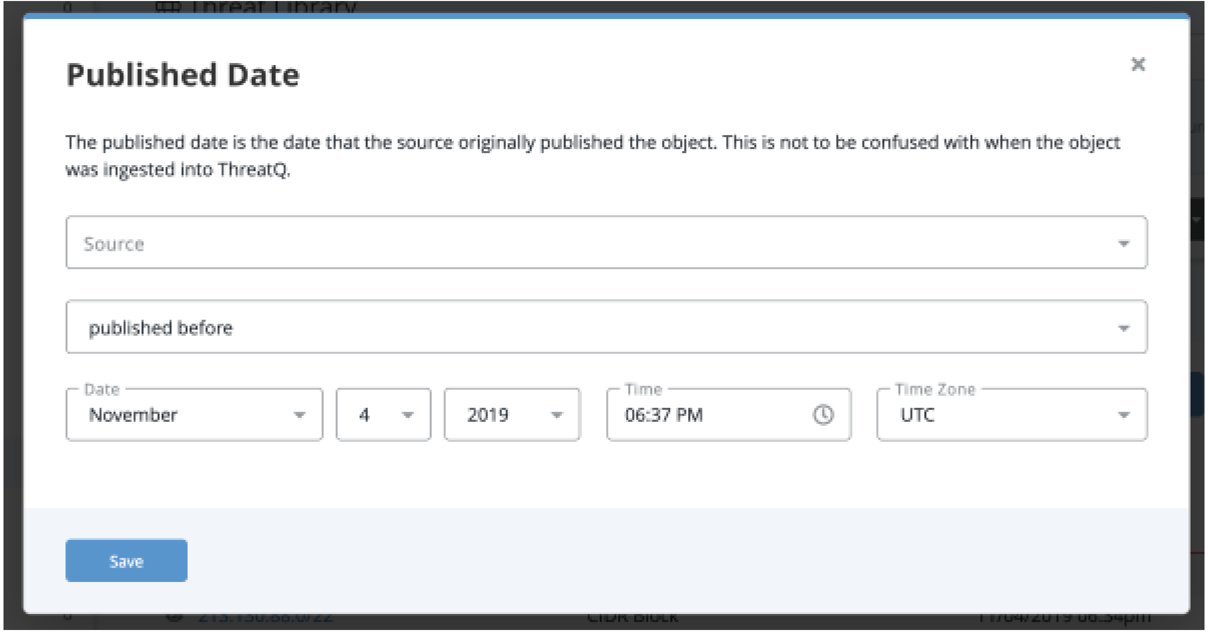
> The Published Date is the date that an object was originally published by the source. This is not to be confused with when the object was ingested into ThreatQ.

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



VALUE	TYPE	DATE CREATED		STATUS
74.125.64.0/23	CIDR Block	05/12/2021 1		Active
74.125.228.234	IP Address	05/12/2021 1		Active
72.14.206.0/23	CIDR Block	05/12/2021 1		Active
74.125.228.202	IP Address	05/12/2021 11:52am	05/12/2021 11:52am	Active

The Published Date dialog box opens.



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

Source

published before

Date: November 4 2019

Time: 06:37 PM

Time Zone: UTC

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

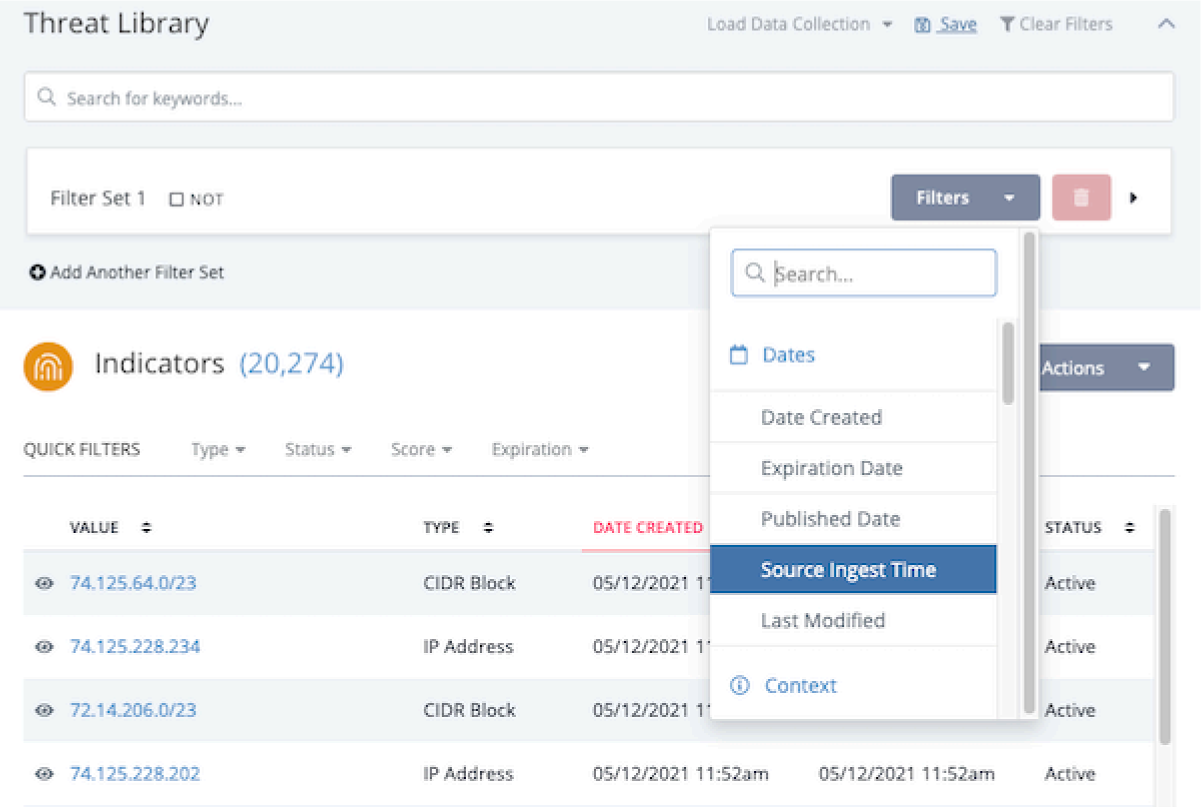
OPTION	RESULT
published before	Search results include items before a selected date
published after	Search results include items after a selected date
published between	Search results include items in a selected range of dates
published within the last	Search results include items within the selected number of days.

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

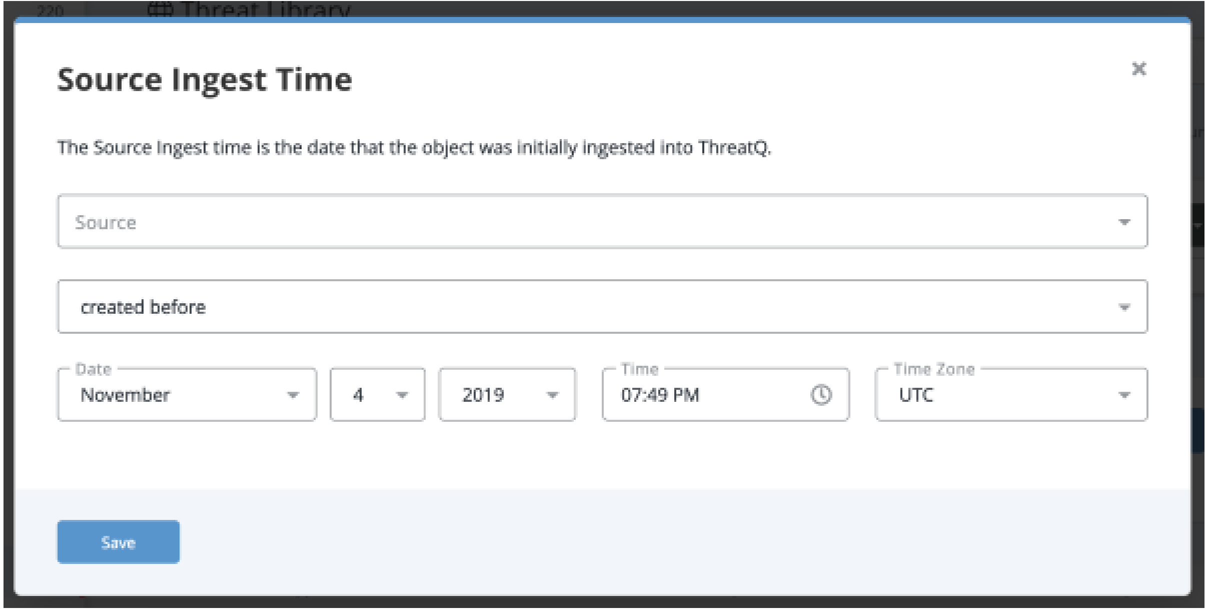
Filtering by Source Ingest Time

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

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



The Source Ingest Time dialog box opens.



The Source Ingest time is the date that the object was initially ingested into ThreatQ.

Source

created before

Date: November 4 2019

Time: 07:49 PM

Time Zone: UTC

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

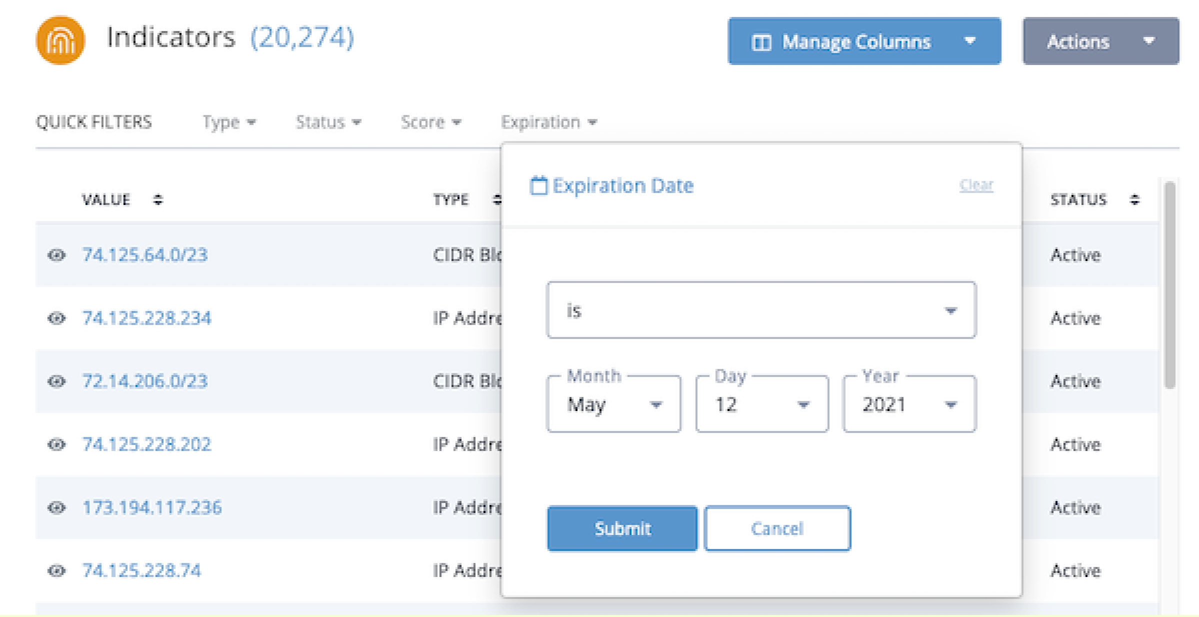
4. Select **Date**, **Time**, and **Time Zone** for the filter to use.
5. Click **Save**.

Filtering by Expiration Date

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

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** Quick Filter located above the search results.



VALUE	TYPE	STATUS
74.125.64.0/23	CIDR Bl	Active
74.125.228.234	IP Addre	Active
72.14.206.0/23	CIDR Bl	Active
74.125.228.202	IP Addre	Active
173.194.117.236	IP Addre	Active
74.125.228.74	IP Addre	Active

is
Month: May
Day: 12
Year: 2021

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 greater than	Search results include items have exceeded their expiration date by a selected number of days.
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. Based on the filter option you selected, select the date, date range, or number of days for the filter to use.
4. Click **Submit**.

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.

Filtering 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.

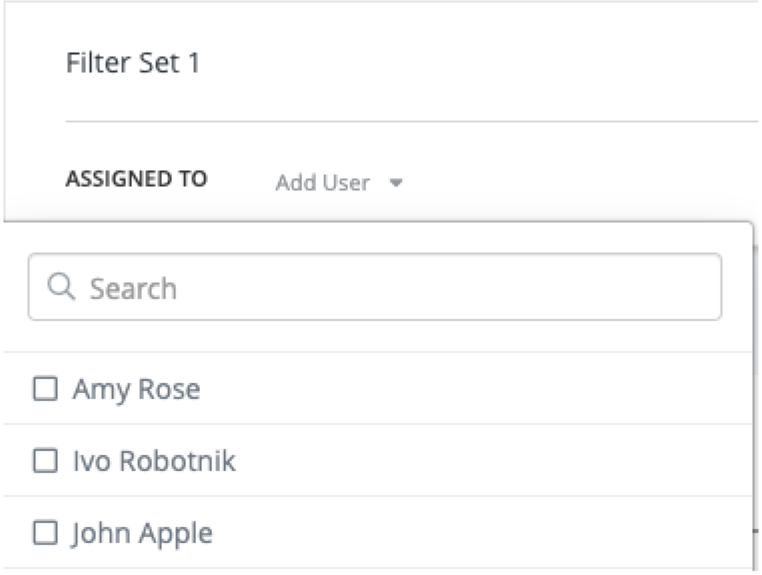
Tasks Filters

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

Filtering Tasks by Assignment

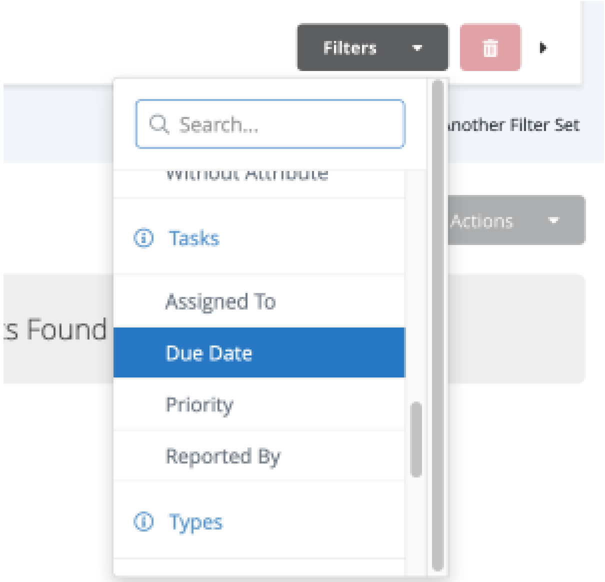
You can filter tasks based on whom they are assigned to.

1. Click on the **Filters** option and select **Assigned To**.
2. Use the **Add User** dropdown to select the user.

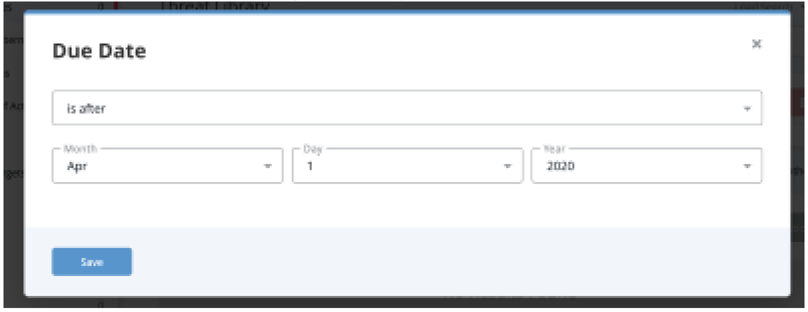


Filtering Tasks by Due Date

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



The Due Date dialog box opens.



Due Date

is after

Month: Apr

Day: 1

Year: 2020

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 between	Search results include tasks with a due date that set between the selected range of dates.

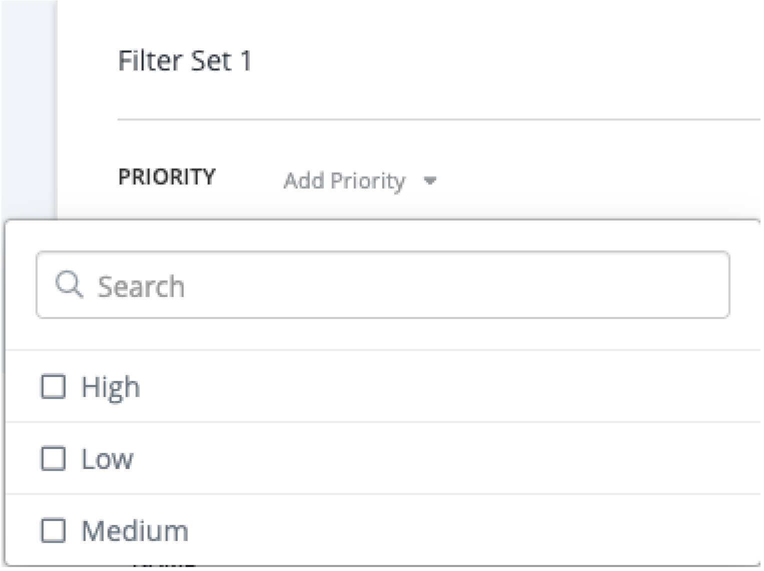
OPTION	RESULT
Is within the last	Search results include tasks with a due date within the last user-specified number of days.
Is within the next	Search results include tasks with a due date within the next user-specified number of days.

3. Click **Save**.

Filtering Tasks by Priority

You can filter tasks based on their priority.

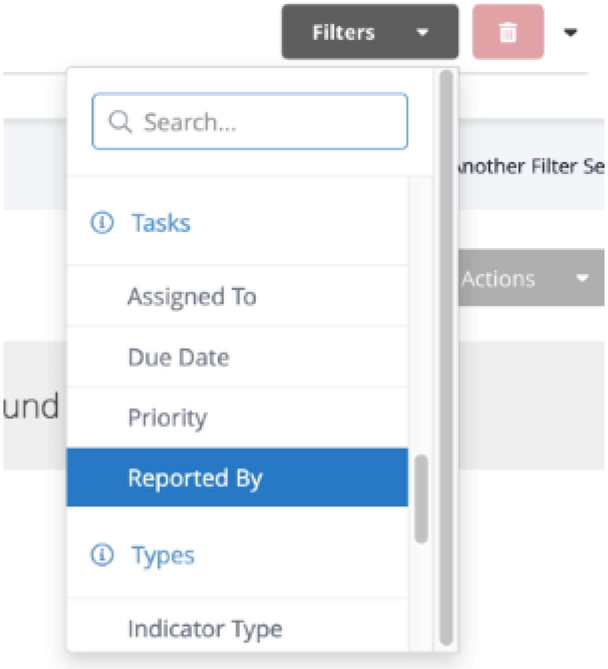
1. Click on the **Filters** option and select **Priority**.
2. Use the **Priority** dropdown and select **Add Priority.**



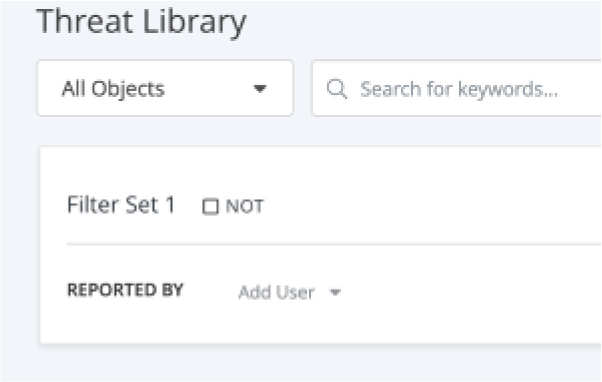
Filtering Tasks by Reported By

You can filter tasks based on who created them.

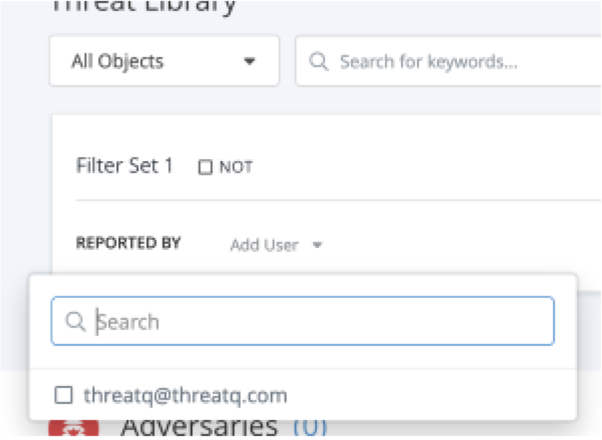
1. Click on the **Filters** option and select **Reported By**.



The Reported By Filter will appear in the filter set.



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



Type Filters

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

Filtering by Object Type

> Filter the Signature list to include YARA types only.

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.

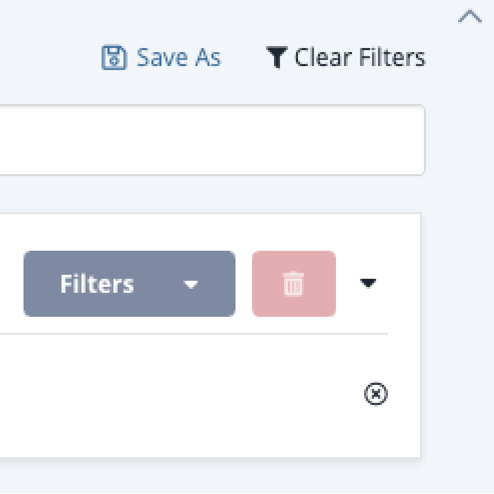
Managing Search Results

You can save your Threat Library searches as Data Collections for future use, integration workflows, and to be used with ThreatQ Custom Dashboards.

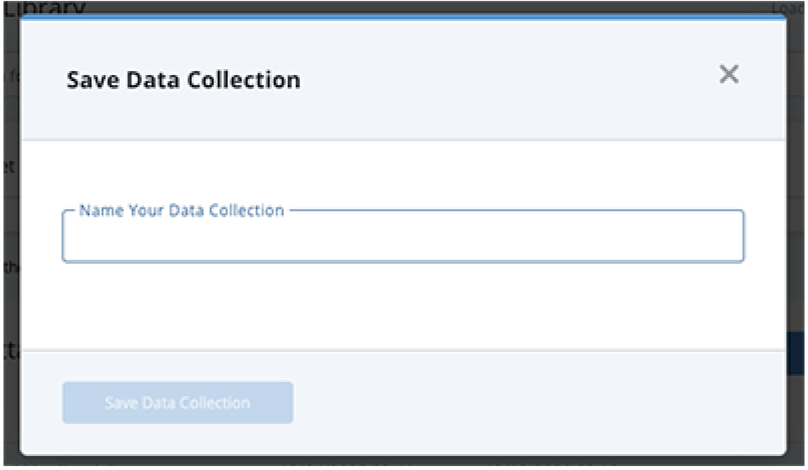
⚠ Integrations and custom dashboards use data collections and are affected if an associated data collection is deleted. Use caution when deleting a data collection.

Saving Searches as Data Collections

1. Perform a search on the Threat Library.
2. Click the **Save As** link.



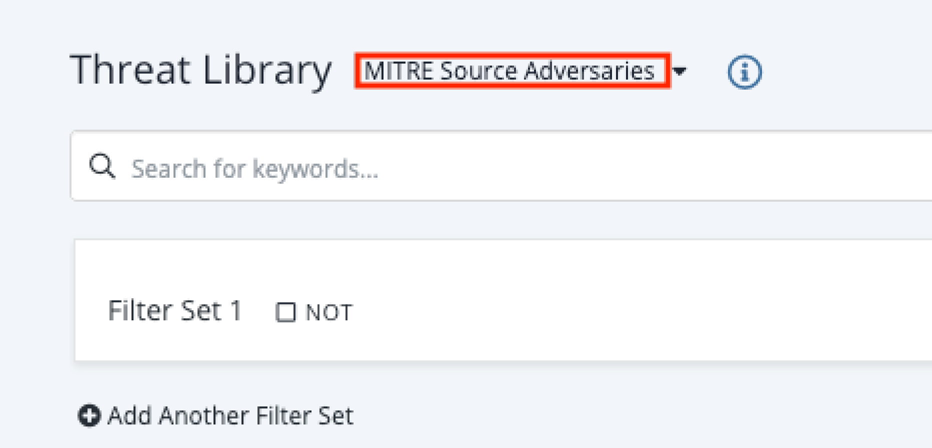
The Save Data Collection dialog box opens.



3. Enter a name for the search in the Data Collection dialog box.

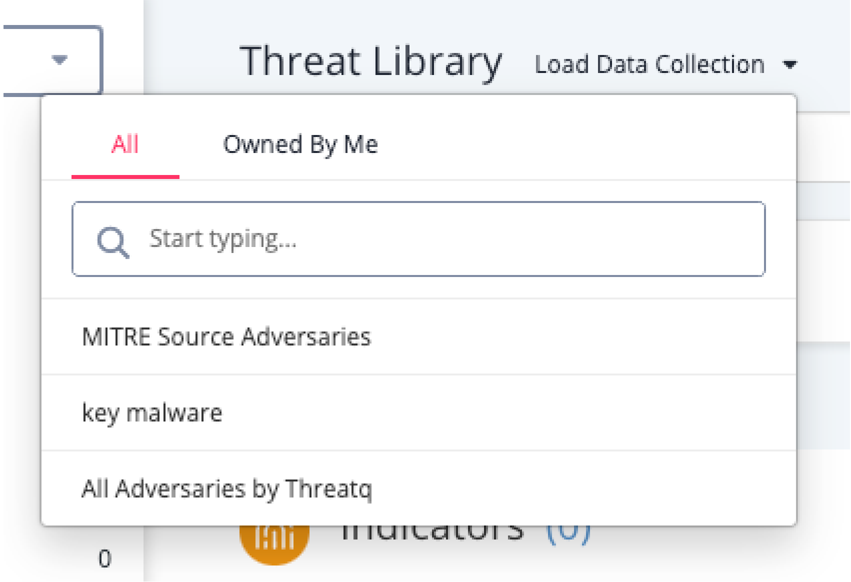
4. Click the **Save Data Collection** button.

   The name of the data collection is displayed at the top of the page. As the data collection creator, you have owner-level permissions and are the only user who can view or edit the data collection. See the Sharing Data Collections section for information on allowing other users to access your data collection.



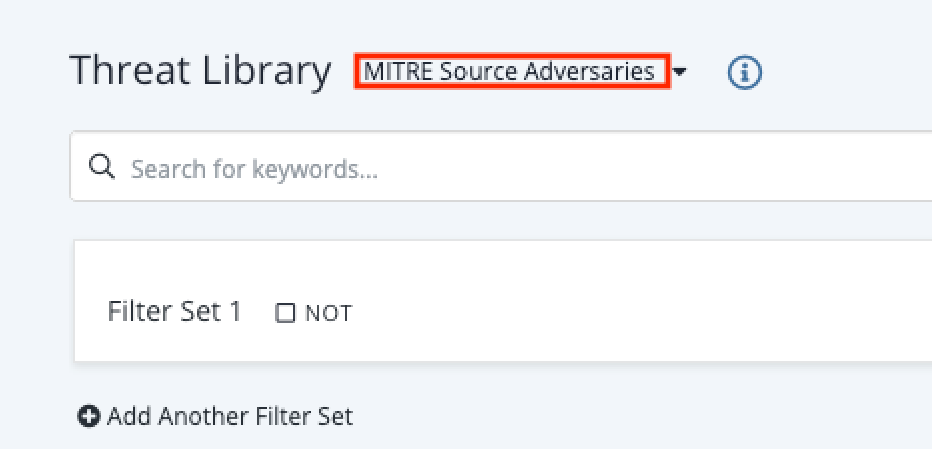
Loading Data Collections

1. Navigate to the Threat Library page.
2. Click the **Load Data Collection Search** option. The data collection window defaults to the All tab that lists all the data collections you own or to which you have view or edit access. The Owned By Me tab lists the data collections for which you are the owner. You can also locate a data collection by using the search field.

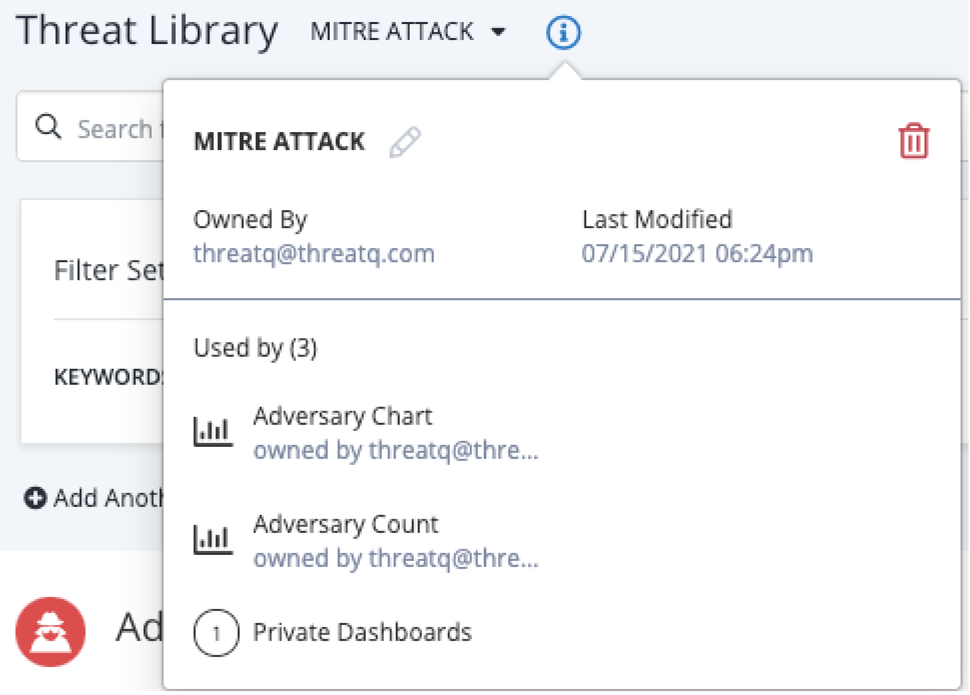


3. Select the data collection.
   The data collection is displayed in the Threat Library page. The name of the data collection is listed at the top of the page.

> If the data collection name is longer than forty characters, it is truncated with ellipses



4. Click the ⓘ icon to view:
   - Data collection name and owner
   - Date of the last change to the data collection
   - Dashboards, data feeds, and workflows that use the data collection. You can click these items to access the corresponding dashboard or data feed.
   - The number of private dashboards that use the data collection



Modifying a Data Collection

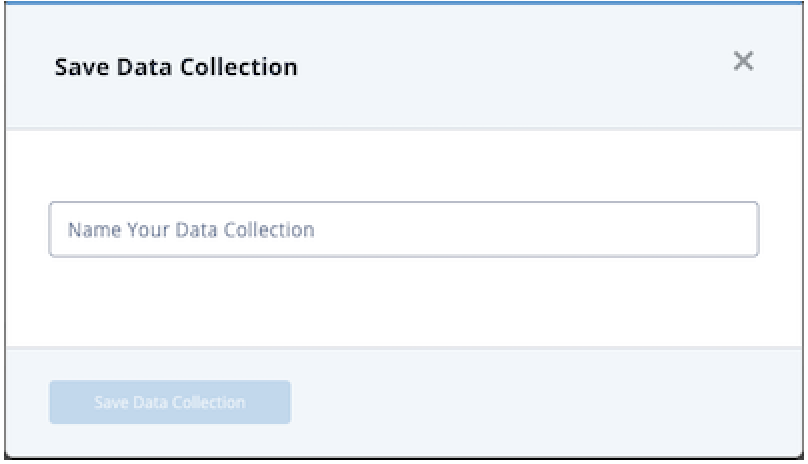
Users with owner or editor permissions for a data collection can make changes to it.

1. Navigate to the Threat Library.
2. Load the data collection you want to change.
3. Enter your changes to the data collection.
4. Click the Save link.

Copying a Data Collection

When an owner or editor makes changes to a data collection, the Save As link allows the creation of a new data collection that reflects these changes and leaves the original data collection unchanged. For example, you can add a filter to an existing Adversaries data collection to include only MITRE Enterprise ATT&CK sources, then save the new data collection as Adversaries - MITRE Enterprise.

1. Navigate to the Threat Library.
2. Load the data collection you want to copy.
3. Enter your changes to the data collection.
4. Click the **Save As** link.
   The Save Data Collection window is displayed.



5. Enter the name of the new data collection.
6. Click the Save Data Collection button.
   ThreatQ creates your new data collection and displays it in the Threat Library page.

Renaming a Data Collection

Only the owner of a data collection can change its name.

1. Navigate to the Threat Library.
2. Load the data collection whose name you want to change.
3. Click the ⓘ icon.
4. Click the ✎ icon next to the data collection's name.
5. Enter the new name.
6. Click the ✓ to save your change.

Sharing Data Collections

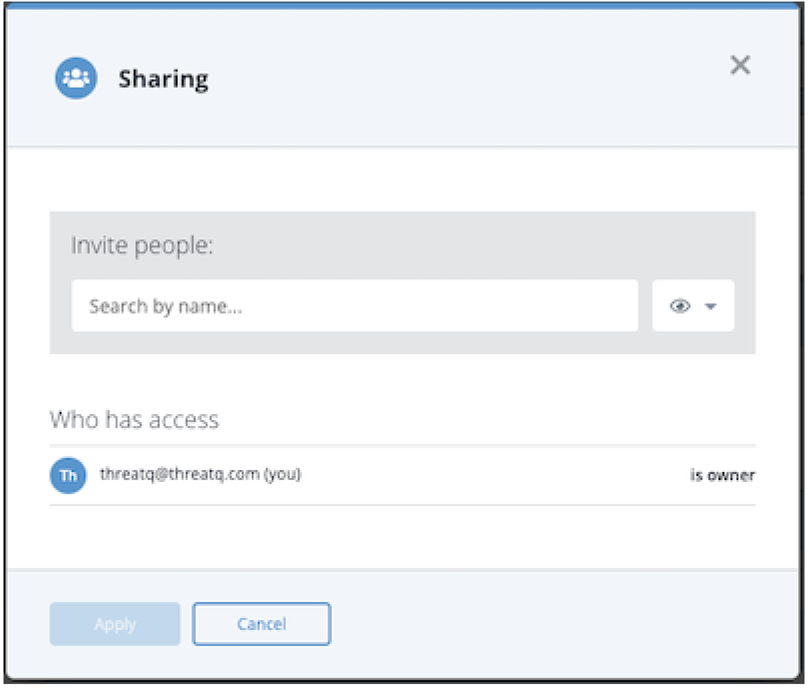
Owners and editors have the option to share a data collection with other users. However, only the data collection owner can remove a user's permissions. In addition, the Share(d) button displayed depends on your permission level and the sharing status of the data collection.

PERMISSION LEVEL	SHARED WITH OTHERS?	SHARE(D) BUTTON
Owner	No	🔒 Share
Owner, Editor	Yes	👥 Share
Viewer	Yes	👥 Shared

See the Sharing topic for more information on the permissions you can assign to each data collection.

1. Navigate to the Threat Library.
2. Load the data collection you want to share.

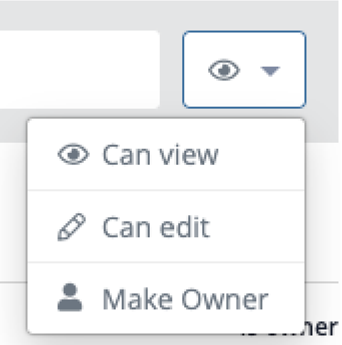
3. Click the **Share** button.
   The Sharing window allows you to select the user to which you want to grant access.



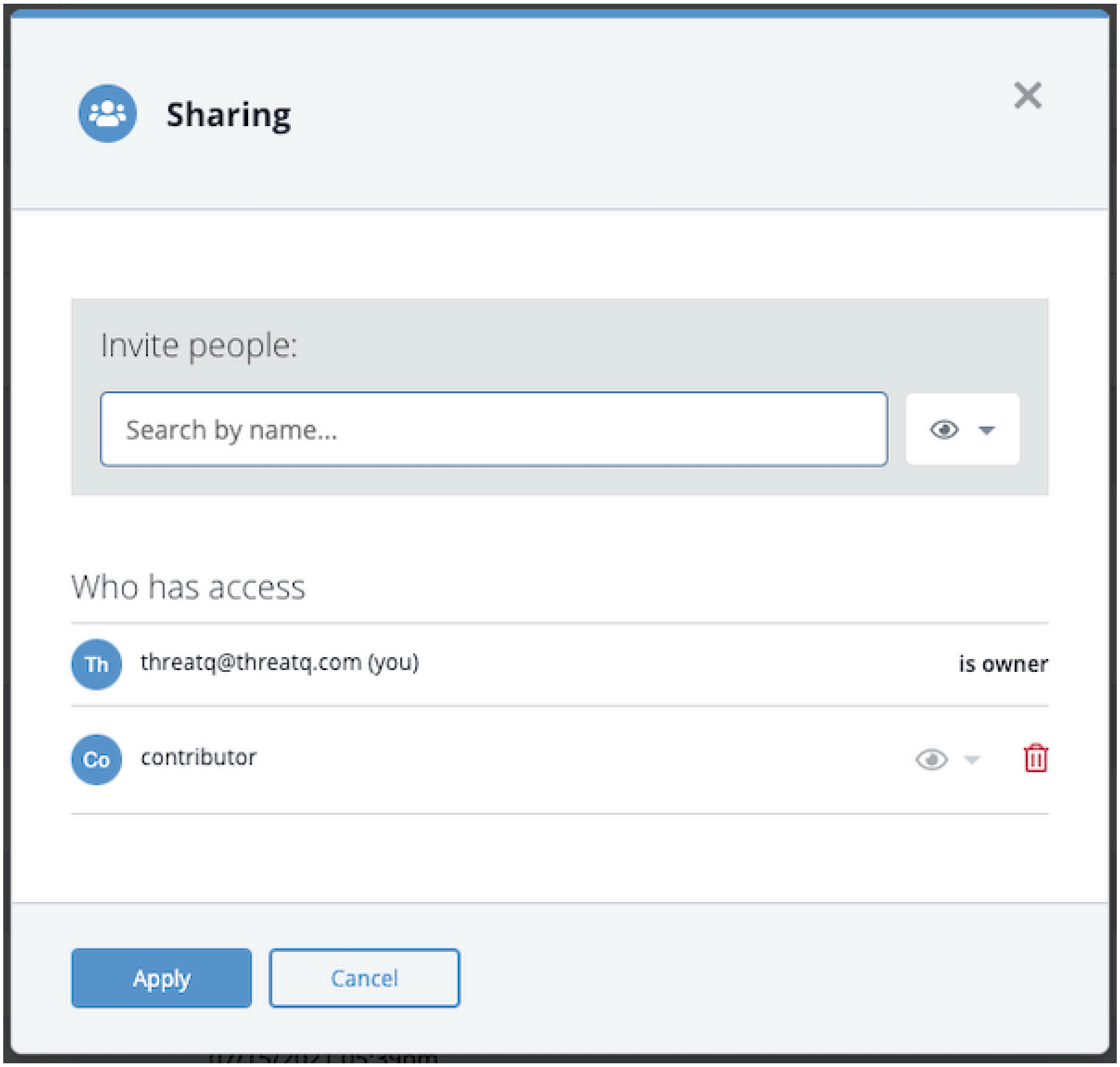
4. Click the arrow next to the 👁 icon to select the user's permission level.

> If you are granting access to all users, you must select the **Can View** option. You can only assign editing permission to individual users not to all users.

> If you assign owner permissions to another user, your permissions automatically change to editor-level.



5. Use the search field to locate and select the user name or the **Everybody (Public)** option. This option grants view-only access to all users.
   The user is now listed in the Who has access list. From this listing, you can change or delete the user's permissions.



6. Click the **Apply** button to save the user's permission level.

Removing a User's Access to a Data Collection

Only the data collection owner can remove a user's permissions.

1. Navigate to the Threat Library.
2. Load the data collection to which you want to remove a user's access.
3. Click the Share button.
4. Click the 🗑 icon next to the user's name.

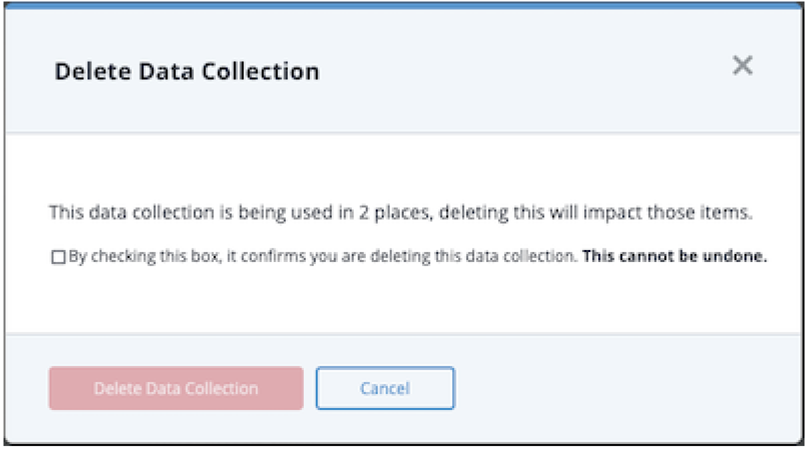
Deleting a Data Collection

To delete a data collection, you must have owner-level permissions for the data collection.

⚠ Deletion of a data collection cannot be undone. Exercise caution before deleting a data collection as it could be associated with integrations, custom dashboards, and other workflows in use with your organization.

Method 1:

1. Navigate to the Threat Library.
2. Click the **Load Data Collection Search** option.
3. Click the Owned By Me tab.
4. Check the box next to the data collection you want to delete.
5. Click the 🗑 icon.
   The Delete Data Collection window prompts you to confirm your deletion
6. Check the warning checkbox and click the **Delete Data Collection** button to confirm.



This data collection is being used in 2 places, deleting this will impact those items.

☐ By checking this box, it confirms you are deleting this data collection. **This cannot be undone.**

Method 2:

1. Navigate to the Threat Library.
2. Load the data collection you want to delete.
3. Click the ⓘ icon next to the data collection name.
4. Click the 🗑 icon.
   The Delete Data Collection window prompts you to confirm your deletion
5. Check the warning checkbox and click the **Delete Data Collection** button to confirm.

Exporting Search Results to CSV

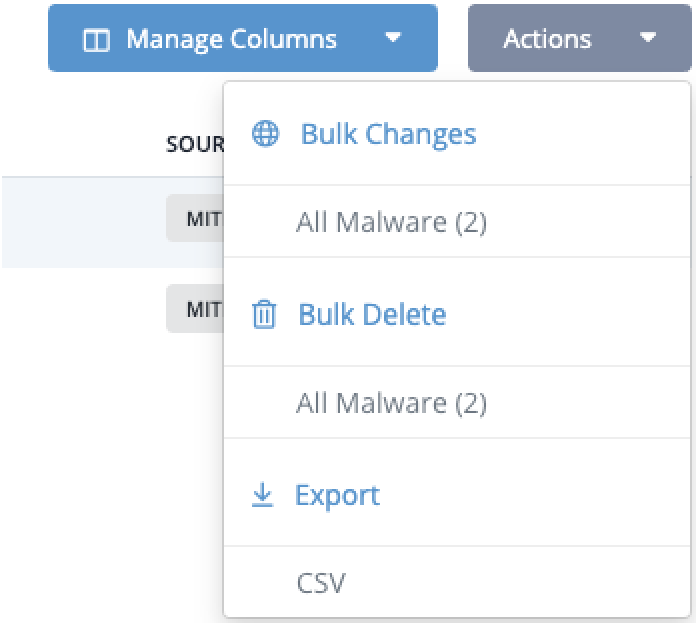
You can export your search results as a CSV file, which allows you to use the data in another application, such as external spreadsheet software.

> ⚠ 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 segments of data.

> When exporting data collections 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 Threat Library.
2. Perform your search or load the appropriate data collection.
3. Click the **Actions** dropdown and select the **CSV** option under the *Export* heading.



The CSV file downloads to your desktop.

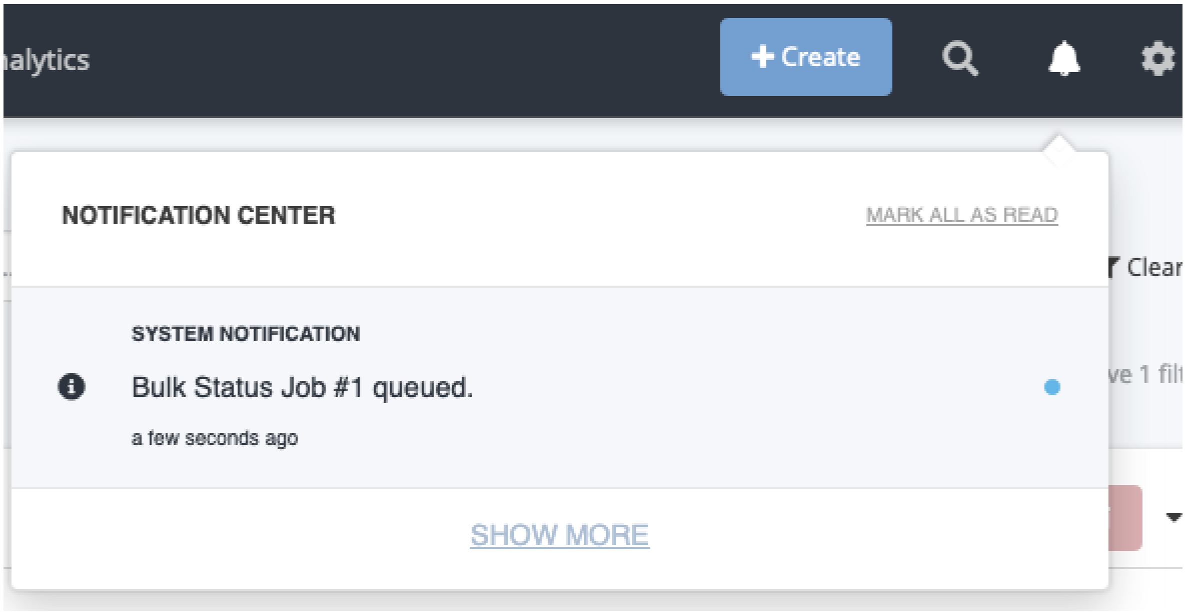
Bulk Actions

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.

> The fields listed in the **Bulk Actions Bulk Change form** may differ based on the type of system objects you have selected. **Example:** If you selected a set of events, the Change Expiration options will not be listed as expiration pertains to indicators only.

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.

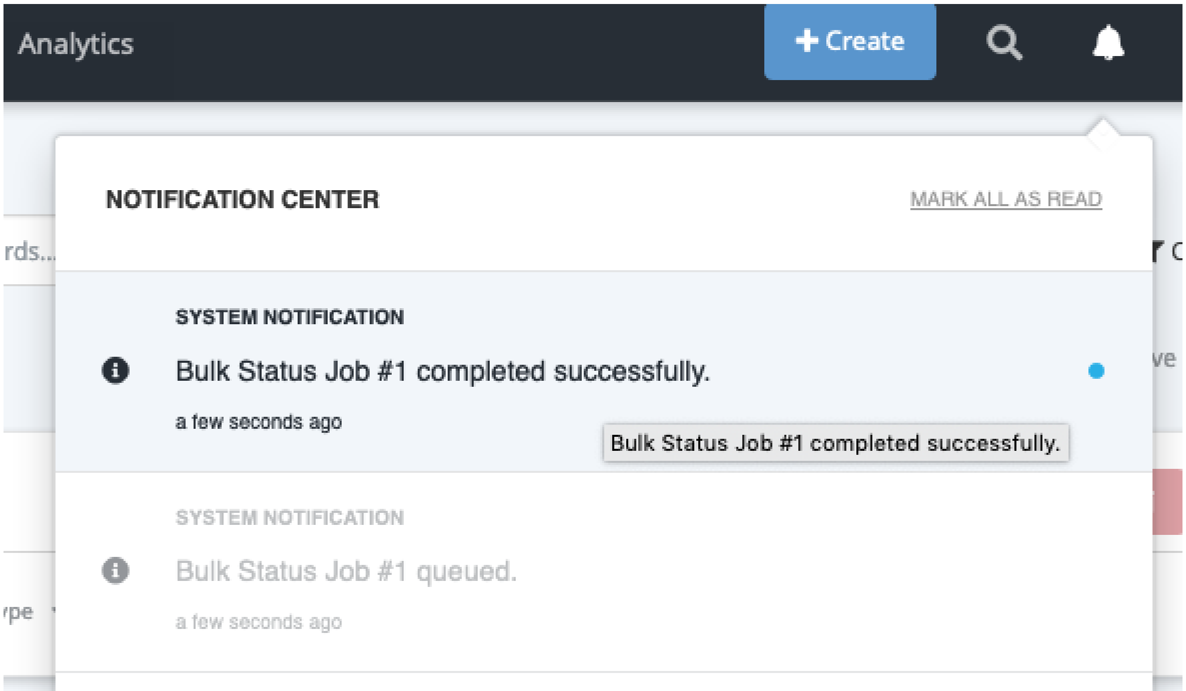
Upon initiating a Bulk Action, the job will be queued by the system and you will receive an in-app notification via the Notification Center icon. The system will also notify you, via the Notification Center, that the job has been completed.



SYSTEM NOTIFICATION

Bulk Status Job #1 queued.

a few seconds ago



SYSTEM NOTIFICATION

Bulk Status Job #1 completed successfully.

a few seconds ago

Bulk Status Job #1 completed successfully.

SYSTEM NOTIFICATION

Bulk Status Job #1 queued.

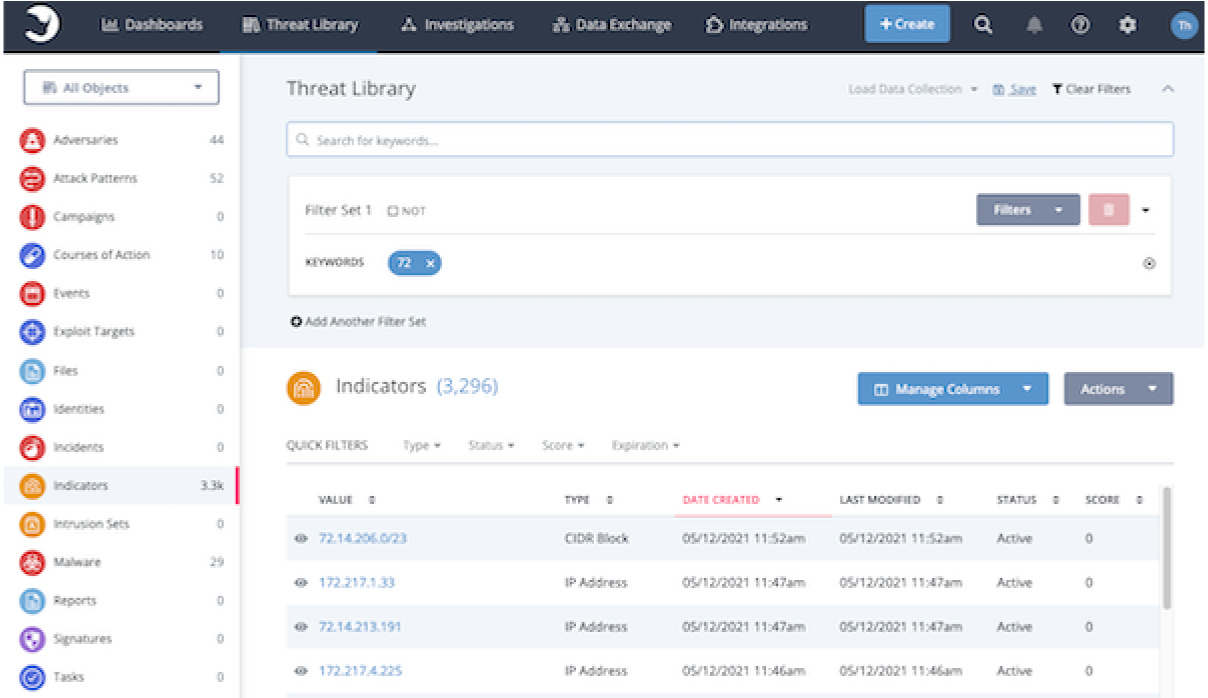
a few seconds ago

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

Bulk Add Source

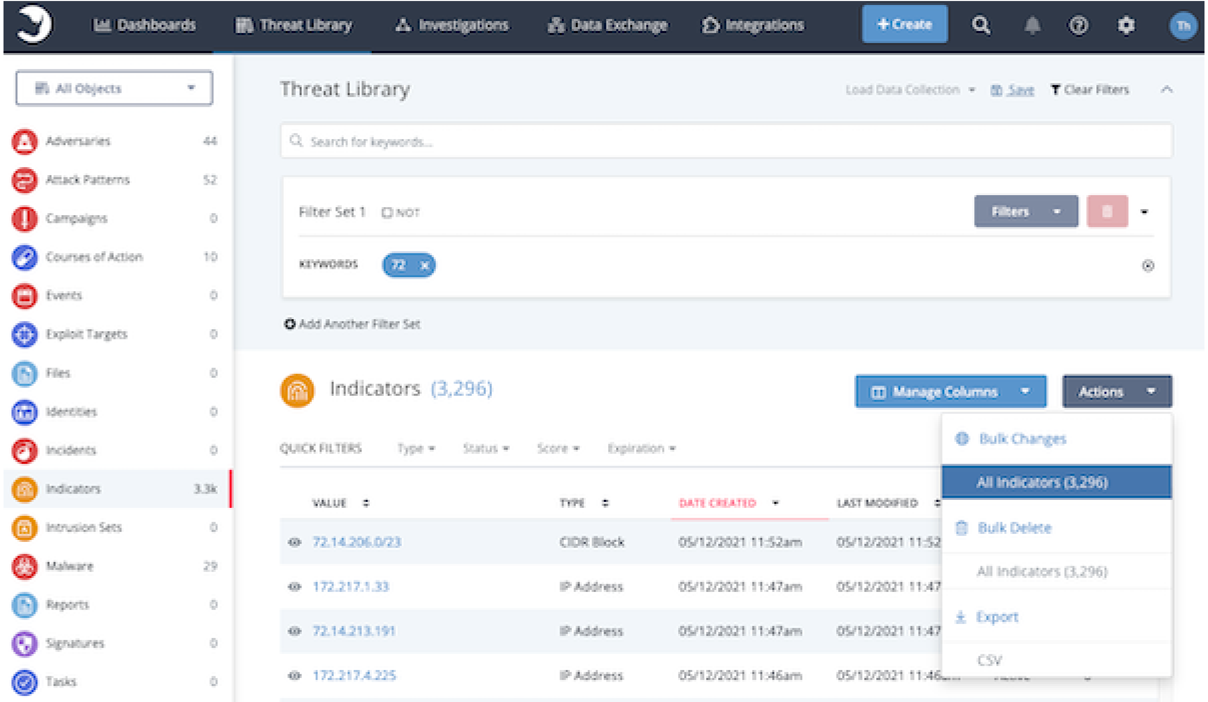
If an object is already associated with the source selected for the Bulk Add Sources action, the object will be skipped during the bulk process.

1. Perform a search on the Threat Library.



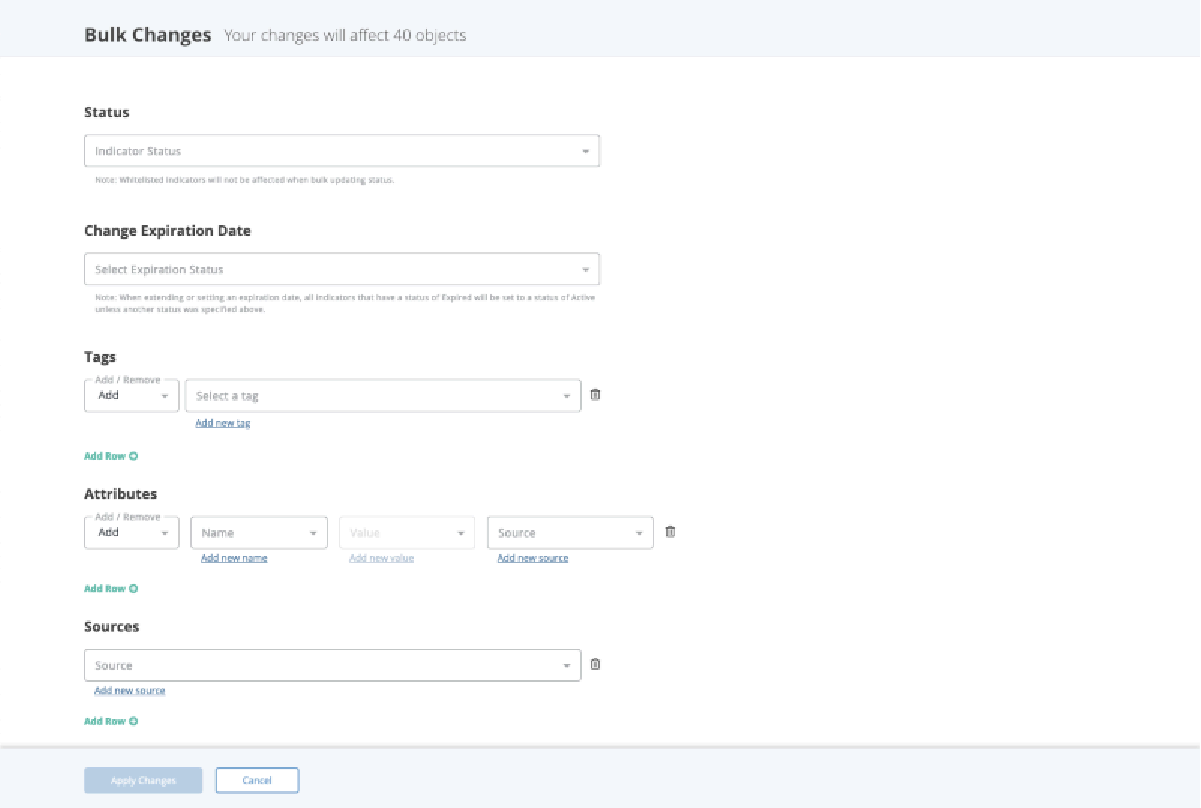
VALUE	TYPE	DATE CREATED	LAST MODIFIED	STATUS	SCORE
72.14.206.0/23	CIDR Block	05/12/2021 11:52am	05/12/2021 11:52am	Active	0
172.217.1.33	IP Address	05/12/2021 11:47am	05/12/2021 11:47am	Active	0
72.14.213.191	IP Address	05/12/2021 11:47am	05/12/2021 11:47am	Active	0
172.217.4.225	IP Address	05/12/2021 11:46am	05/12/2021 11:46am	Active	0

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.



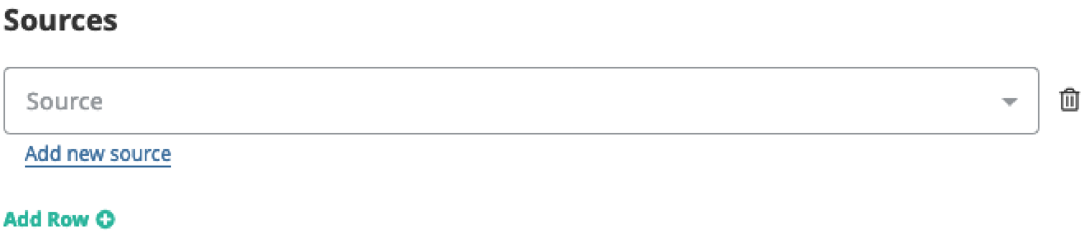
Bulk Changes Your changes will affect 40 objects

Note: Whitelisted indicators will not be affected when bulk updating status.

Note: When extending or setting an expiration date, all indicators that have a status of Expired will be set to a status of Active unless another status was specified above.

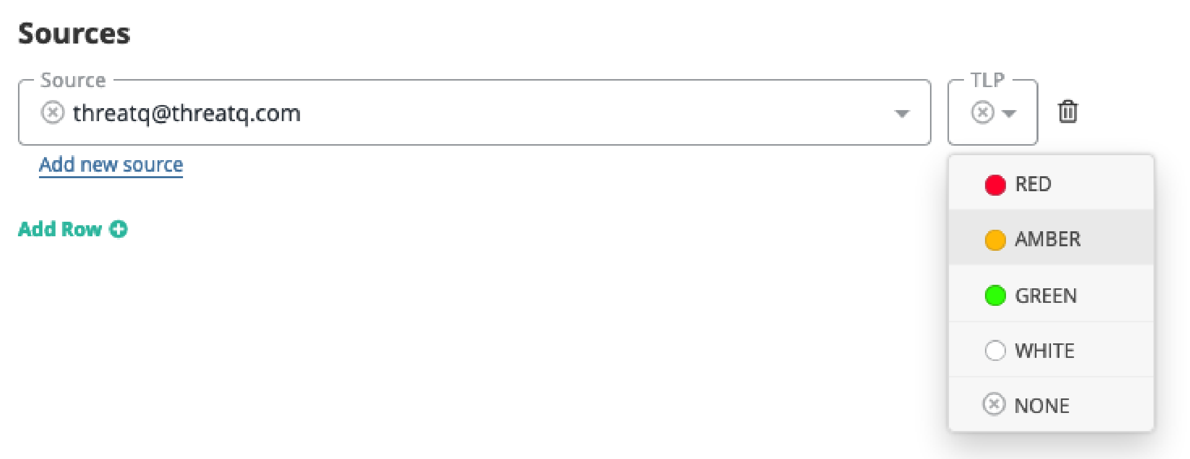
3. Click on **Add Row** under the **Source** heading.

   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.

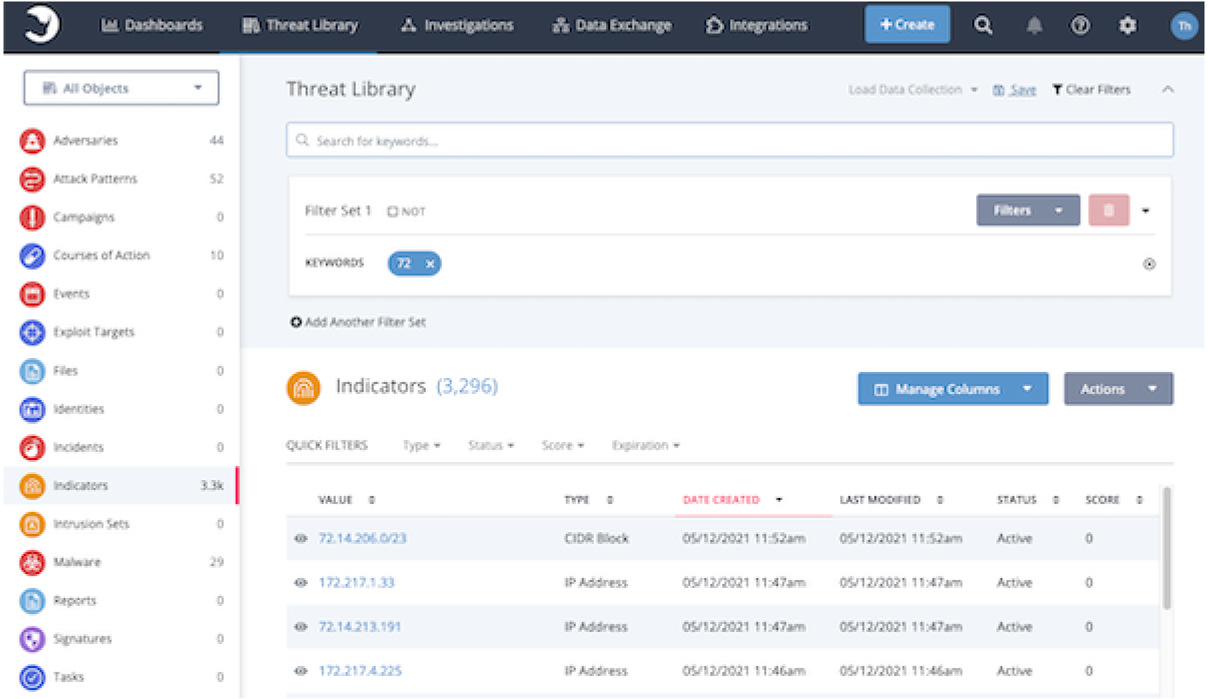
If you have TLP enabled, you will also be able to update the designation for the source selected or keep the source-default designation.



Source: threatq@threatq.com

Bulk Add/Remove Attributes

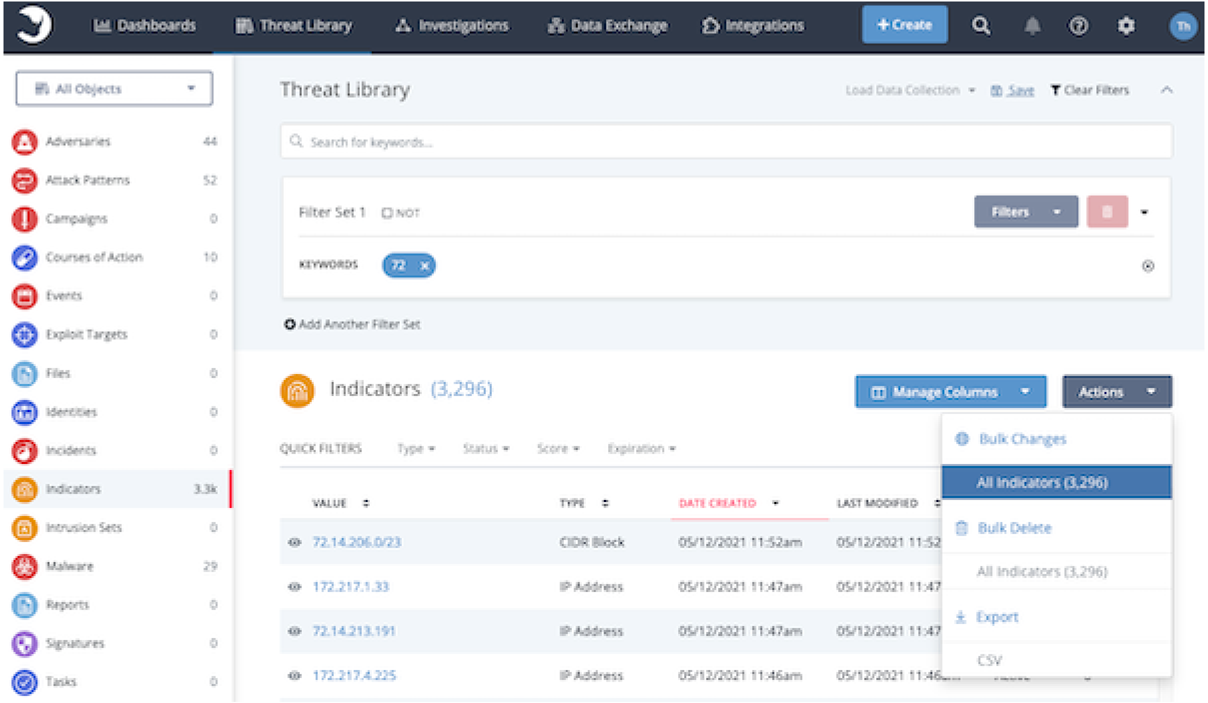
1. Perform a search on the Threat Library.



KEYWORDS 72

VALUE	TYPE	DATE CREATED	LAST MODIFIED	STATUS	SCORE
72.14.206.0/23	CIDR Block	05/12/2021 11:52am	05/12/2021 11:52am	Active	0
172.217.1.33	IP Address	05/12/2021 11:47am	05/12/2021 11:47am	Active	0
72.14.213.191	IP Address	05/12/2021 11:47am	05/12/2021 11:47am	Active	0
172.217.4.225	IP Address	05/12/2021 11:46am	05/12/2021 11:46am	Active	0

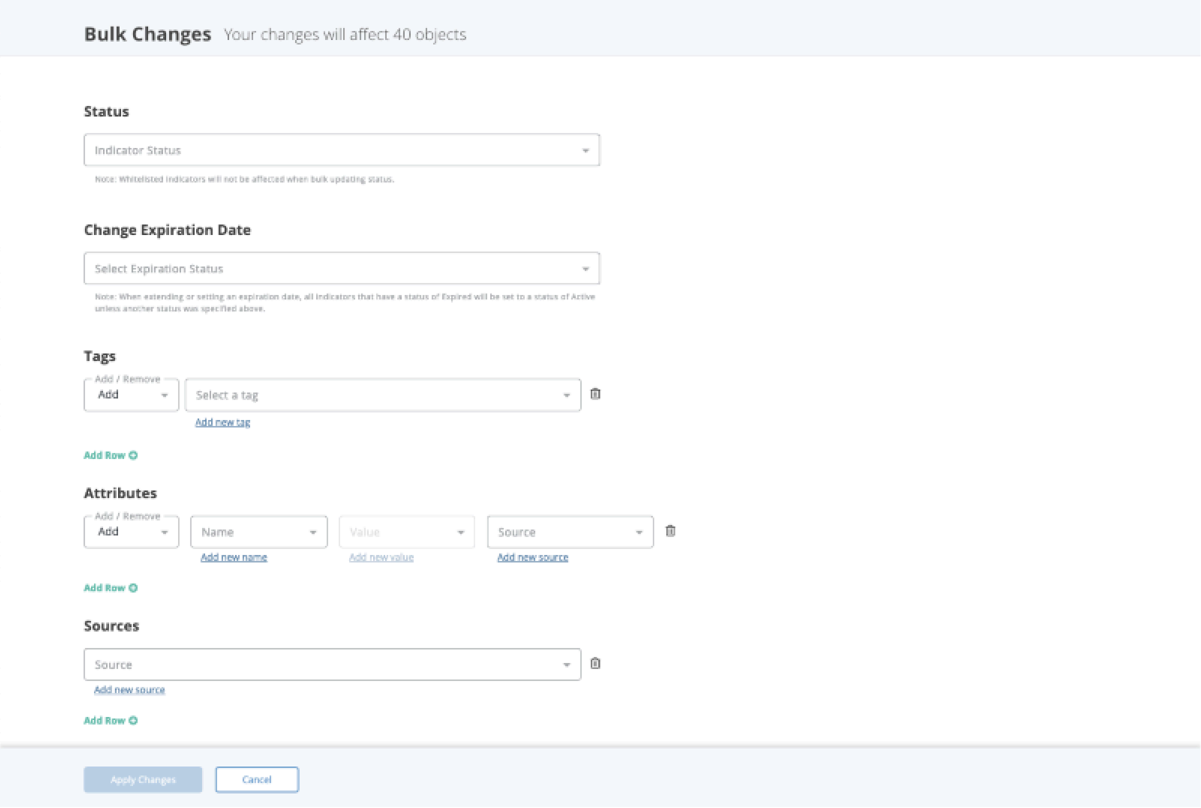
2. Click on the **Actions** dropdown and select **All <System Object>** under the *Bulk Changes* heading.



VALUE	TYPE	DATE CREATED	LAST MODIFIED
72.14.206.0/23	CIDR Block	05/12/2021 11:52am	05/12/2021 11:52
172.217.1.33	IP Address	05/12/2021 11:47am	05/12/2021 11:47
72.14.213.191	IP Address	05/12/2021 11:47am	05/12/2021 11:47
172.217.4.225	IP Address	05/12/2021 11:46am	05/12/2021 11:46

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

The Bulk Changes form will load.


Bulk Changes Your changes will affect 40 objects

Status

Indicator Status

Note: Whitelisted indicators will not be affected when bulk updating status.

Change Expiration Date

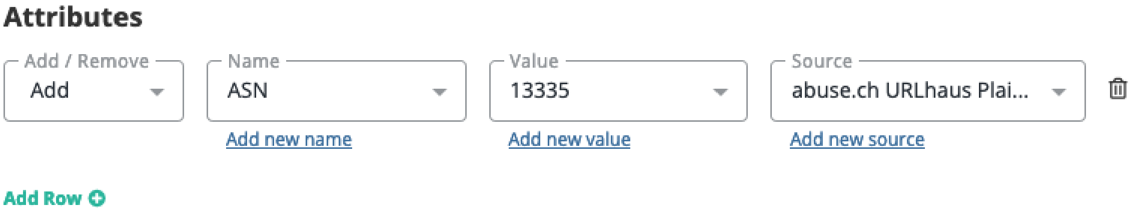
Select Expiration Status

Note: When extending or setting an expiration date, all indicators that have a status of Expired will be set to a status of Active unless another status was specified above.

> Only the Bulk Actions that relate to the type of system object you selected will load on the Bulk Changes form.

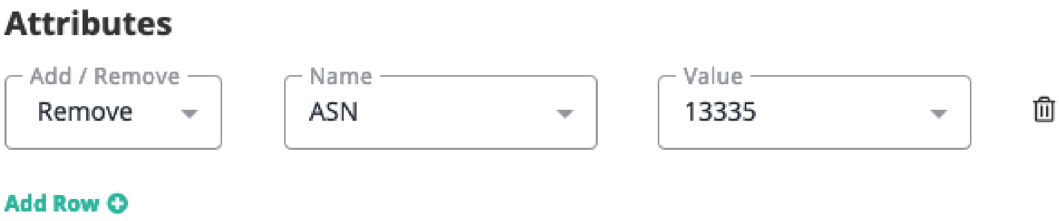
> Bulk Expiration Change will not load for non-indicators.

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.



Attributes

Add / Remove: Add
Name: ASN
Value: 13335
Source: abuse.ch URLhaus Plai...



Attributes

Add / Remove: Remove
Name: ASN
Value: 13335

> 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.

Bulk Add/Remove Attribute 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.

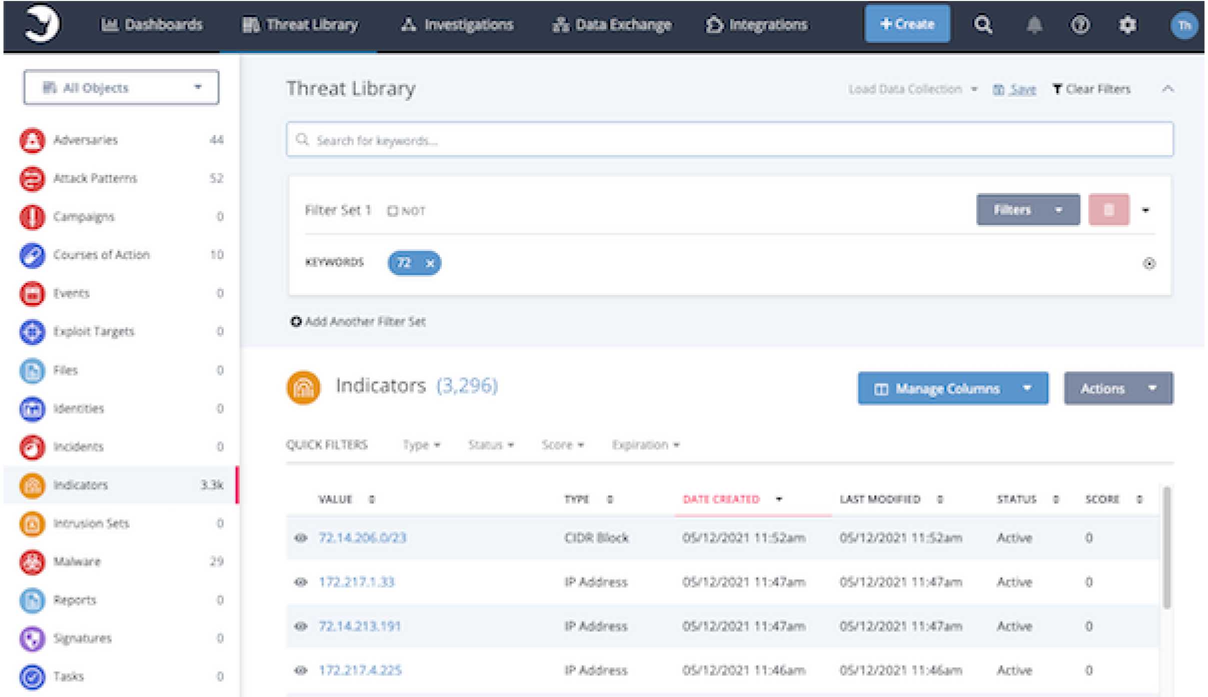
Add and Remove Attributes

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

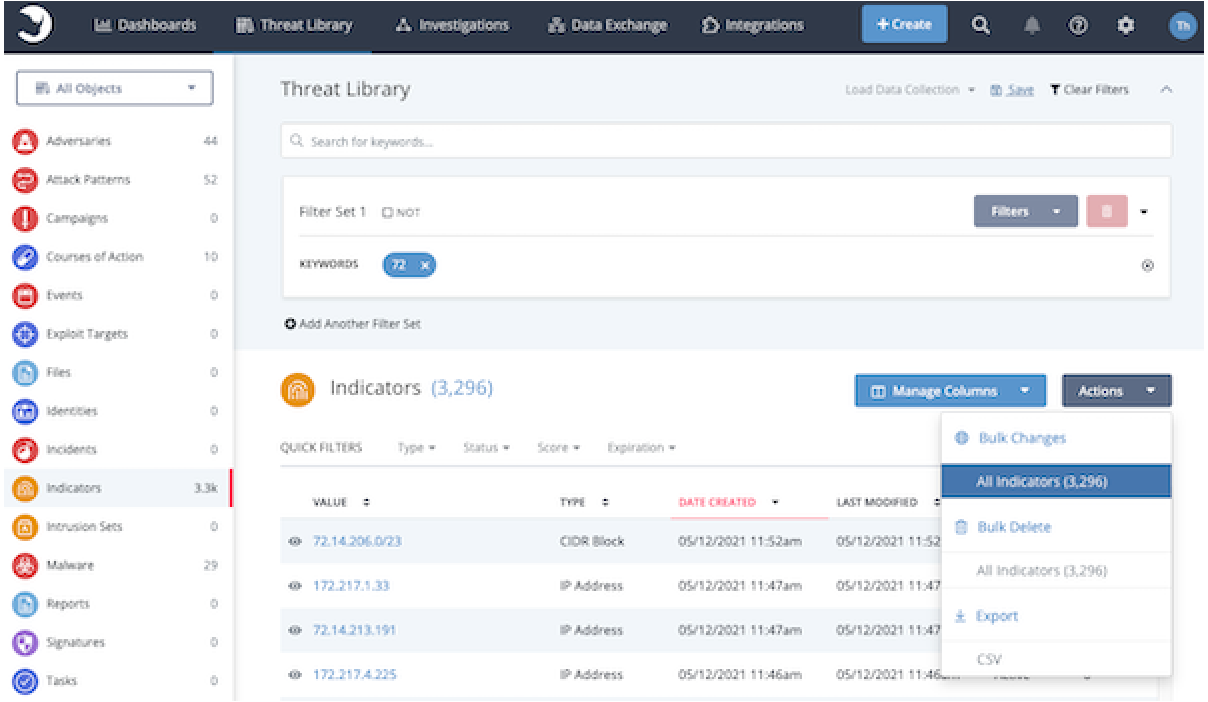
1. Add Attributes - See the Add Multiple Attributes Scenario above.
2. Remove Attributes - See the Remove Multiple Attributes Scenario above.

Bulk Add/Remove Tags

1. Perform a search on the Threat Library.

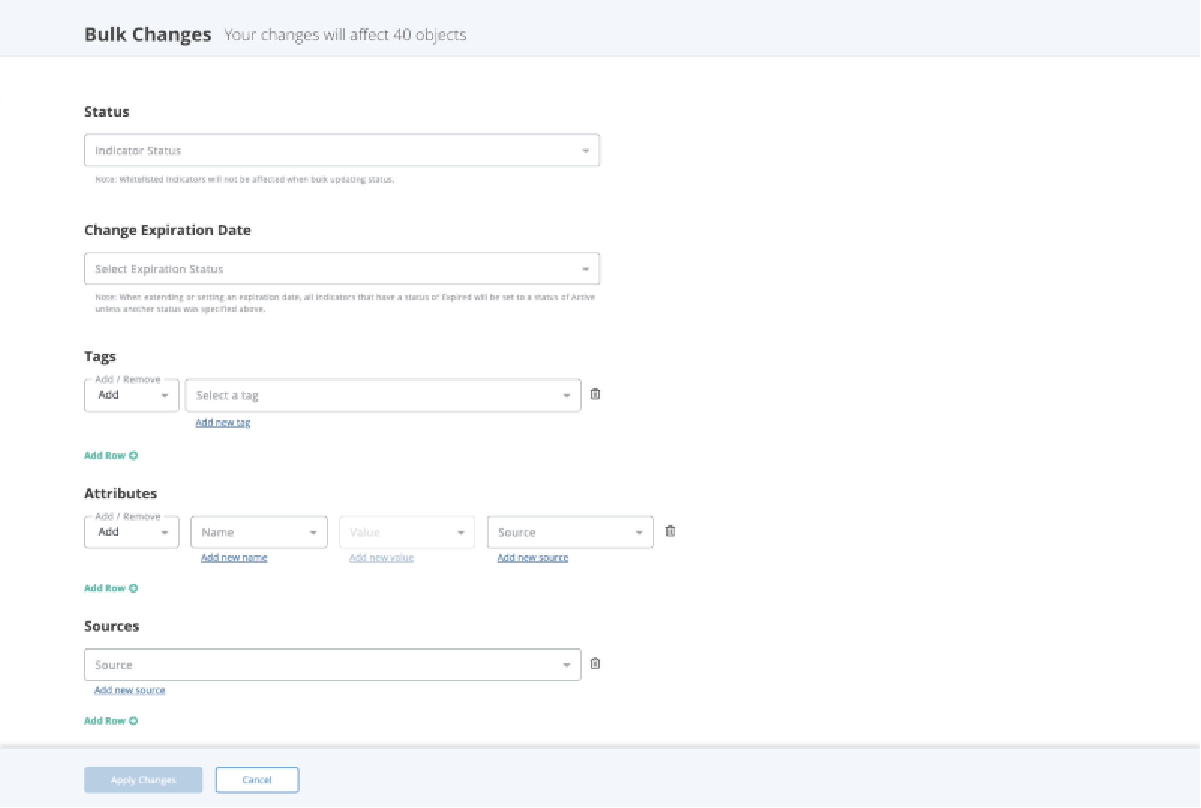


2. Click on the **Actions** dropdown and select **All <System Object>** under the *Bulk Changes* heading.



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

The Bulk Changes form will load.

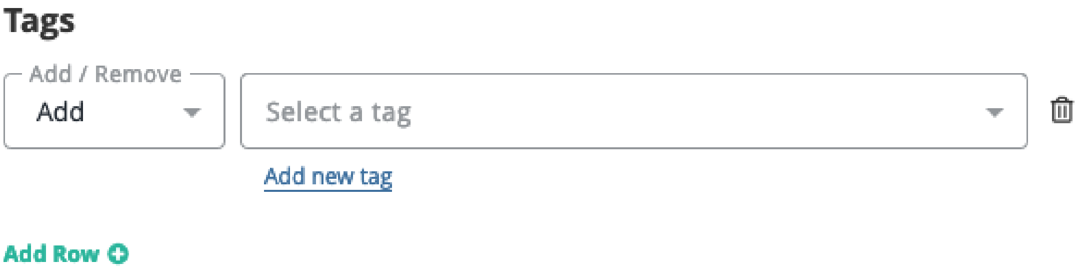


Your changes will affect 40 objects

Note: Whitelisted indicators will not be affected when bulk updating status.

Note: When extending or setting an expiration date, all indicators that have a status of Expired will be set to a status of Active unless another status was specified above.

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.



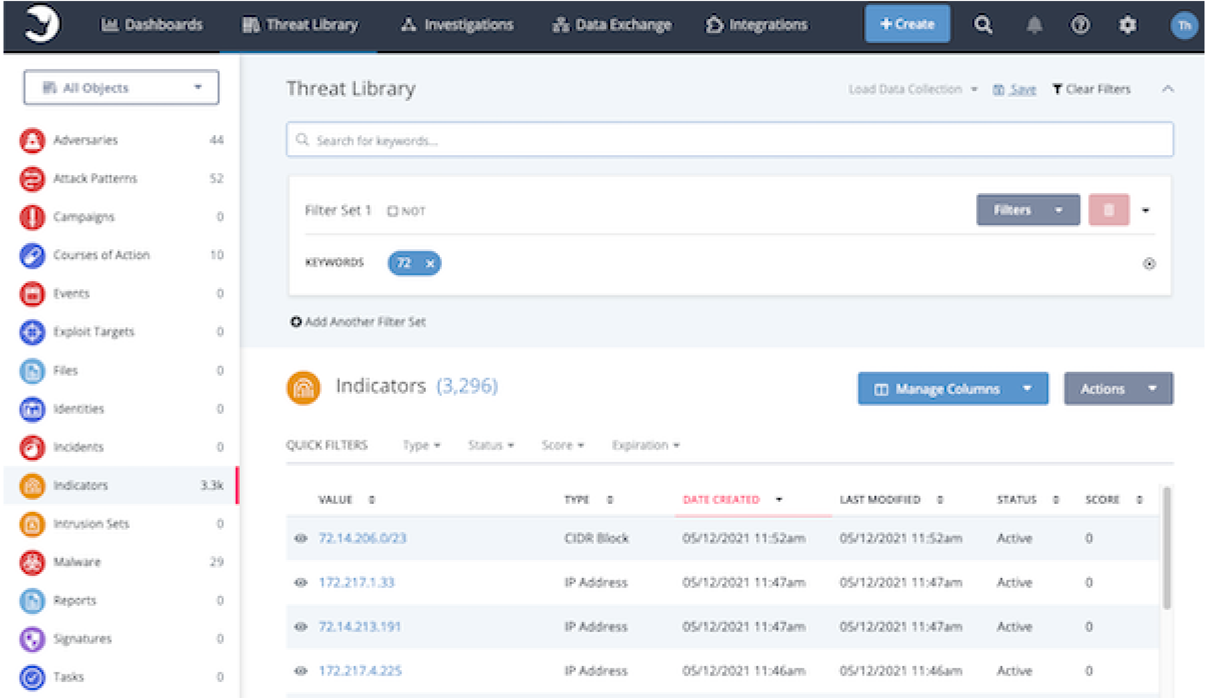
Click on **Add Row** and repeat step 3 to add/remove multiple tags.

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

Bulk Change Expiration Date

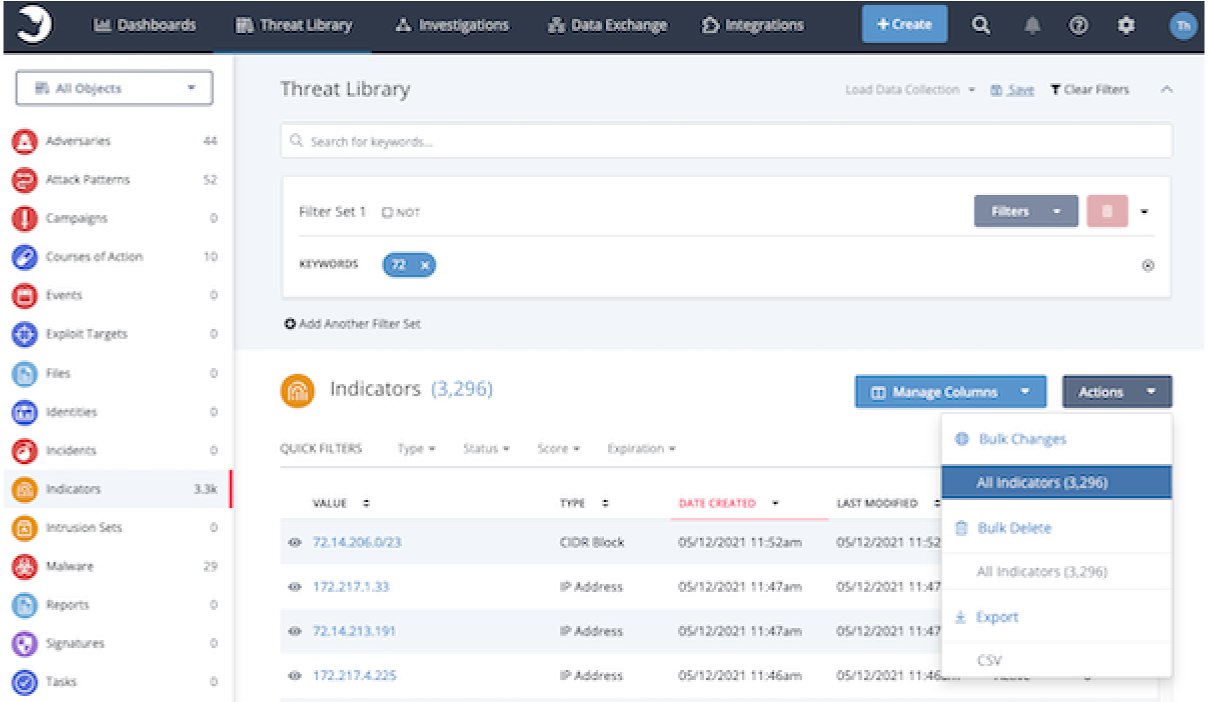
This function can only be performed on Indicators.

1. Perform a search on the Threat Library.



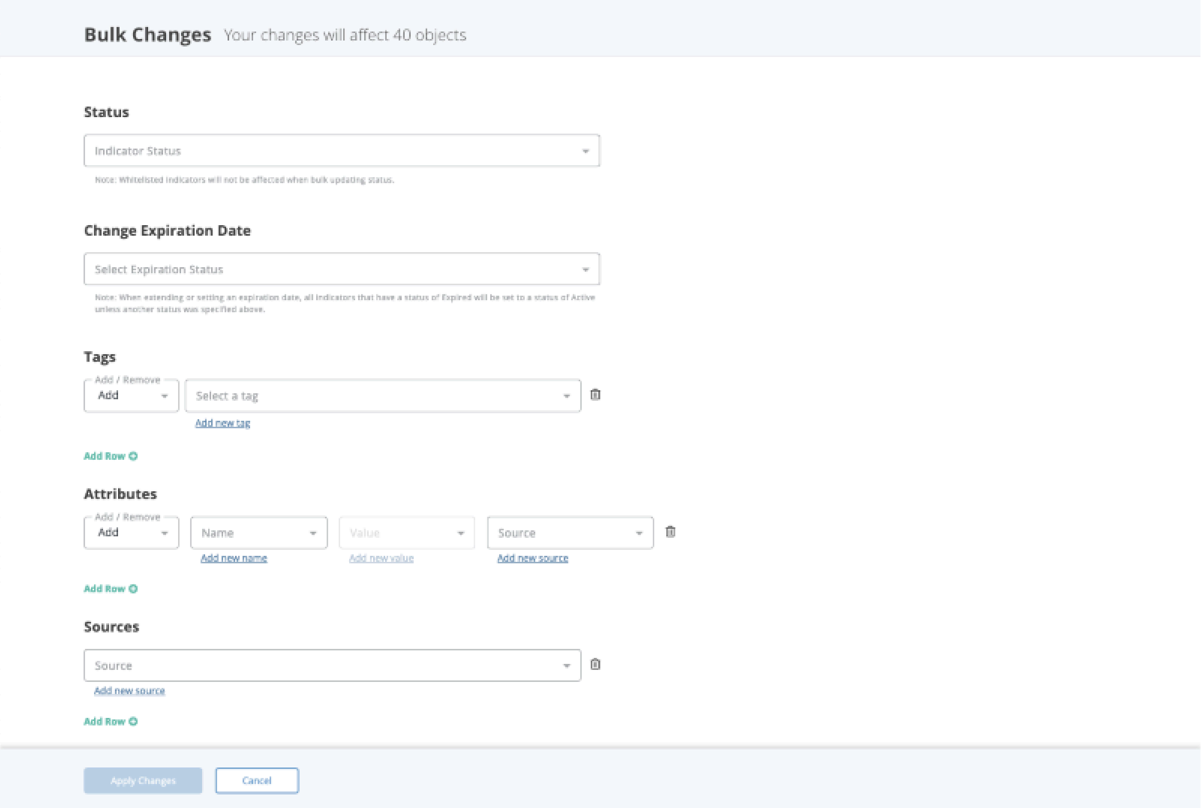
VALUE	TYPE	DATE CREATED	LAST MODIFIED	STATUS	SCORE
72.14.206.0/23	CIDR Block	05/12/2021 11:52am	05/12/2021 11:52am	Active	0
172.217.1.33	IP Address	05/12/2021 11:47am	05/12/2021 11:47am	Active	0
72.14.213.191	IP Address	05/12/2021 11:47am	05/12/2021 11:47am	Active	0
172.217.4.225	IP Address	05/12/2021 11:46am	05/12/2021 11:46am	Active	0

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.



Bulk Changes Your changes will affect 40 objects

Note: Whitelisted indicators will not be affected when bulk updating status.

Note: When extending or setting an expiration date, all indicators that have a status of Expired will be set to a status of Active unless another status was specified above.

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.

Bulk Expiration Change Scenarios

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.

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.

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.

Remove 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.

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.

Extending/Setting an expiration date of 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.

Extending/Setting an expiration date of an indicator with a status of Whitelisted

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

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 Delete

The Bulk Delete feature offers users with Maintenance and Administrative roles the ability to select and delete system objects of all types, excluding Files and Tasks, from the Advanced Search page. In addition to the system object, bulk delete will also delete all child records such as attributes and relationships.

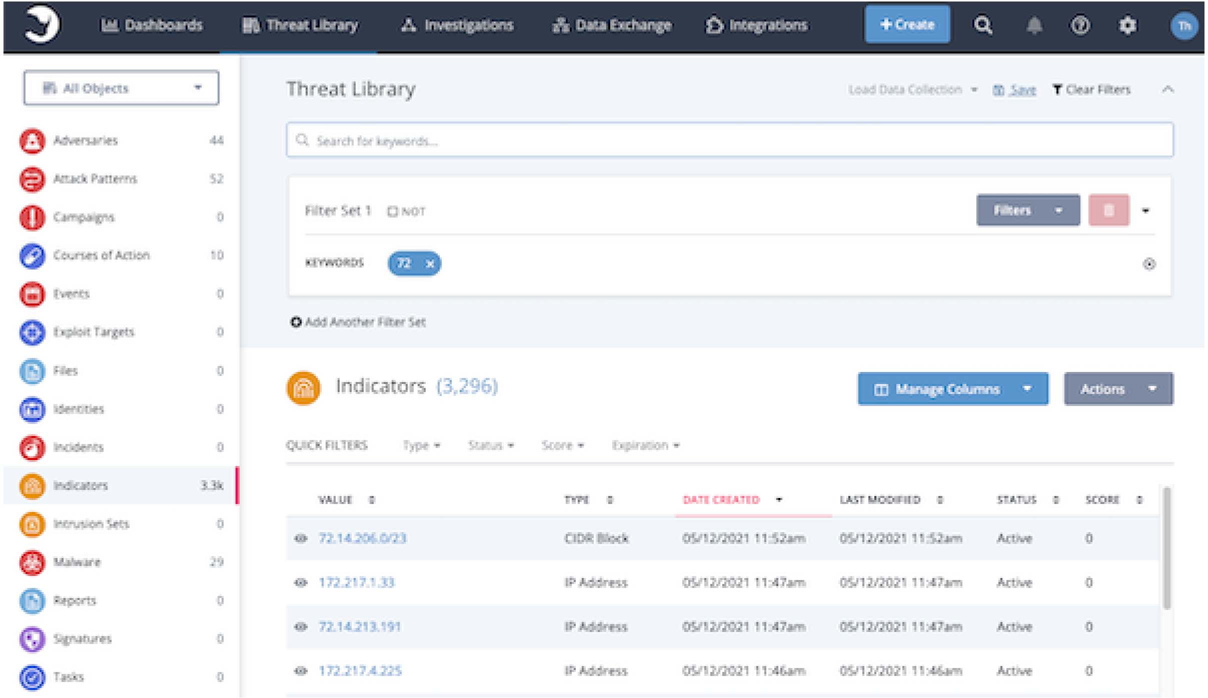
> Individual Tasks and Files can be deleted by accessing the object's details page and selecting Delete Task/File from the Actions menu.

Once selected, the job process will run in the background and allow you to continue working within ThreatQ. An in-app notification will alert you when a Bulk Delete job has been queued and when it has been completed. You can also view the status and outcome of the job from the Job Management page.

⚠ 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.

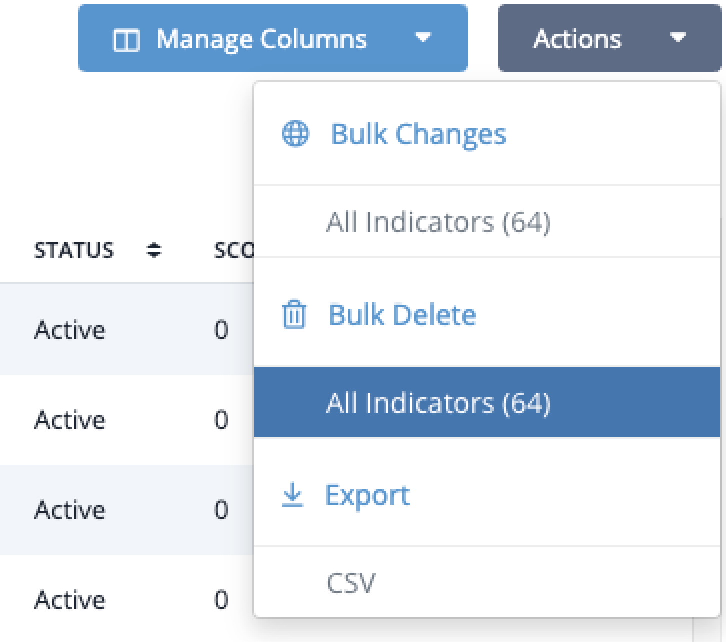
⚠ Based on the size of your bulk delete job and the system resources available, you may find that the estimated job duration is quite long. In these rare instances, contact ThreatQ support to explore your other options for deleting a large number of objects.

1. Perform a search on the Threat Library.



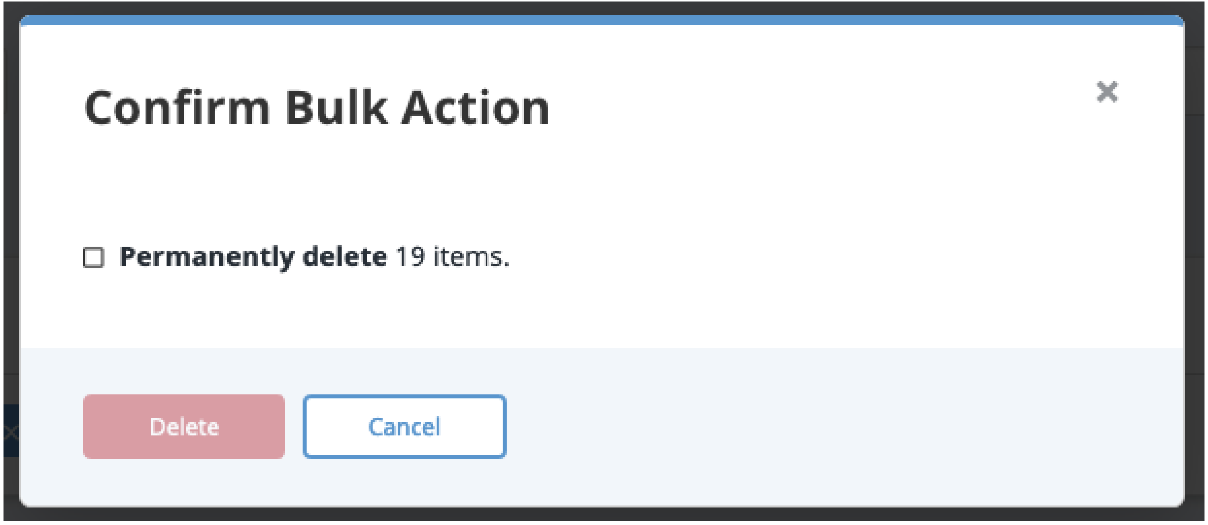
VALUE	TYPE	DATE CREATED	LAST MODIFIED	STATUS	SCORE
72.14.206.0/23	CIDR Block	05/12/2021 11:52am	05/12/2021 11:52am	Active	0
172.217.1.33	IP Address	05/12/2021 11:47am	05/12/2021 11:47am	Active	0
72.14.213.191	IP Address	05/12/2021 11:47am	05/12/2021 11:47am	Active	0
172.217.4.225	IP Address	05/12/2021 11:46am	05/12/2021 11:46am	Active	0

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.



Confirm Bulk Action

☐ **Permanently delete** 19 items.

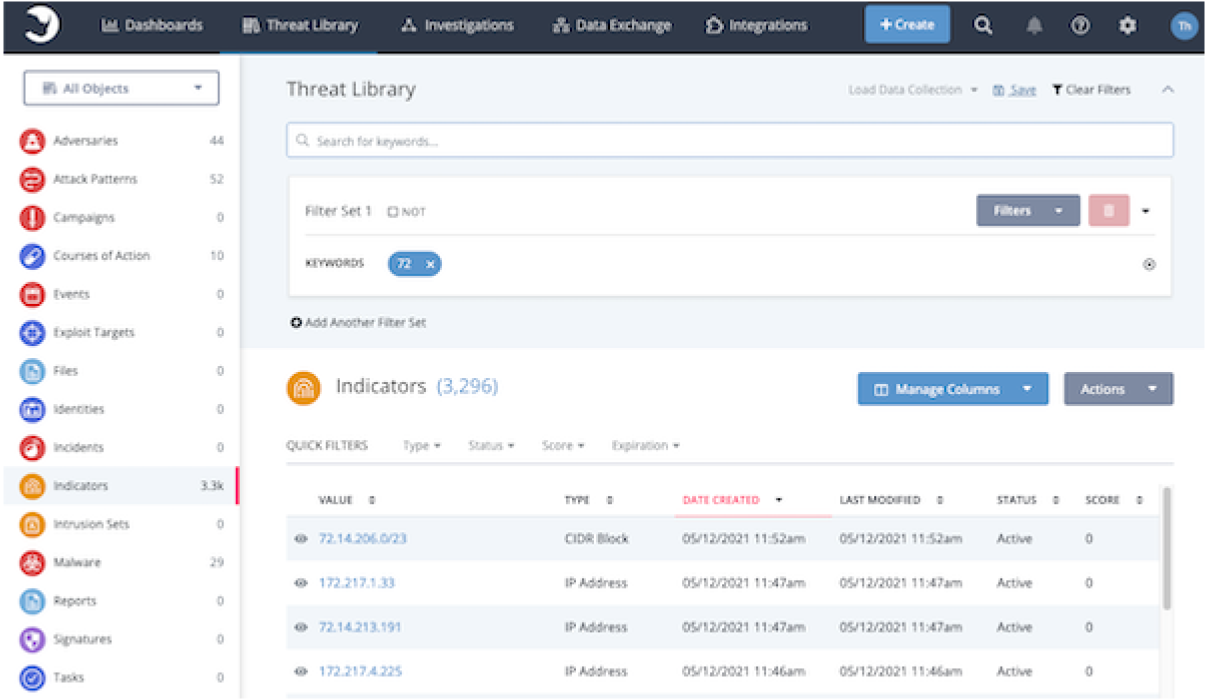
3. Click on the checkbox to confirm deletion and then click on **Delete**.

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.

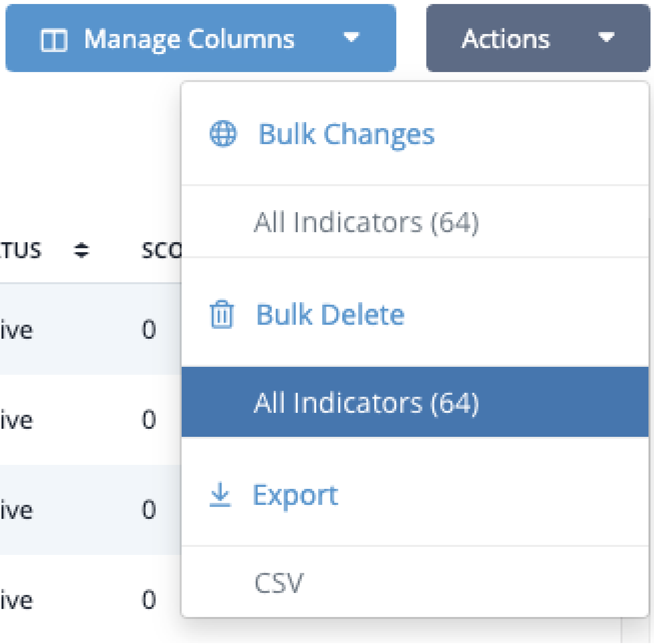
> If an object is already associated with the source selected for the Bulk Add Relationships action, the object will be skipped during the bulk process.

1. Perform a search on the Threat Library.



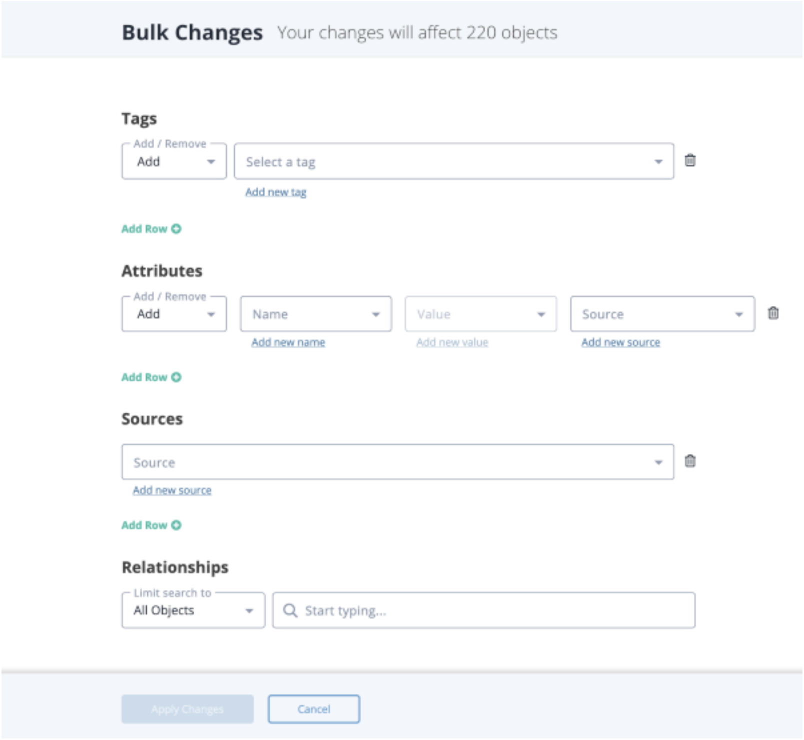
VALUE	TYPE	DATE CREATED	LAST MODIFIED	STATUS	SCORE
72.14.206.0/23	CIDR Block	05/12/2021 11:52am	05/12/2021 11:52am	Active	0
172.217.1.33	IP Address	05/12/2021 11:47am	05/12/2021 11:47am	Active	0
72.14.213.191	IP Address	05/12/2021 11:47am	05/12/2021 11:47am	Active	0
172.217.4.225	IP Address	05/12/2021 11:46am	05/12/2021 11:46am	Active	0

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.

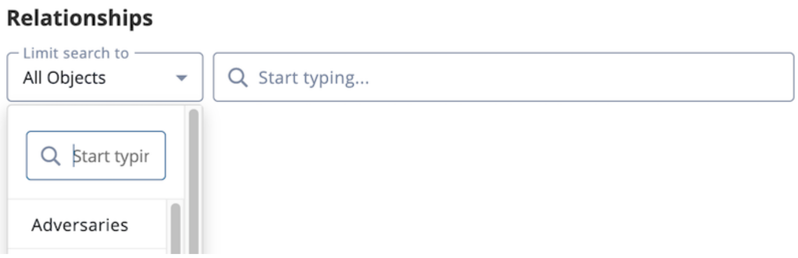
The Bulk Changes form will load.



Your changes will affect 220 objects

> 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.

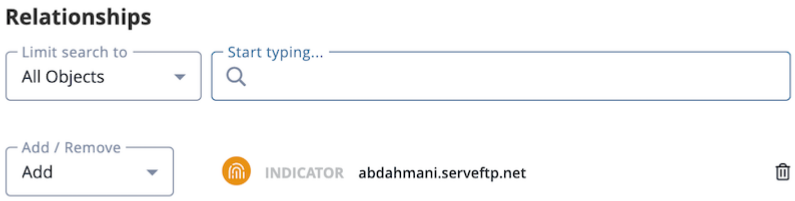


Limit search to: All Objects

4. Enter an object name.

> By default, this field searches for objects that begin with the search string you enter. To search for objects that include your search string but do not begin with it, you must use a wildcard (% OR *) search.
> **Examples:**
> 1. When you enter "us", your search returns **US**Bferry and **US**BStealer.
> 2. When you enter "%us" or "*us", your search returns Aquari**us**, Lazar**us** Group, D**us**t Storm, **US**Bferry, and **US**BStealer.

5. After you select an object, the Add/Remove option appears.



Limit search to: All Objects

Add / Remove: Add

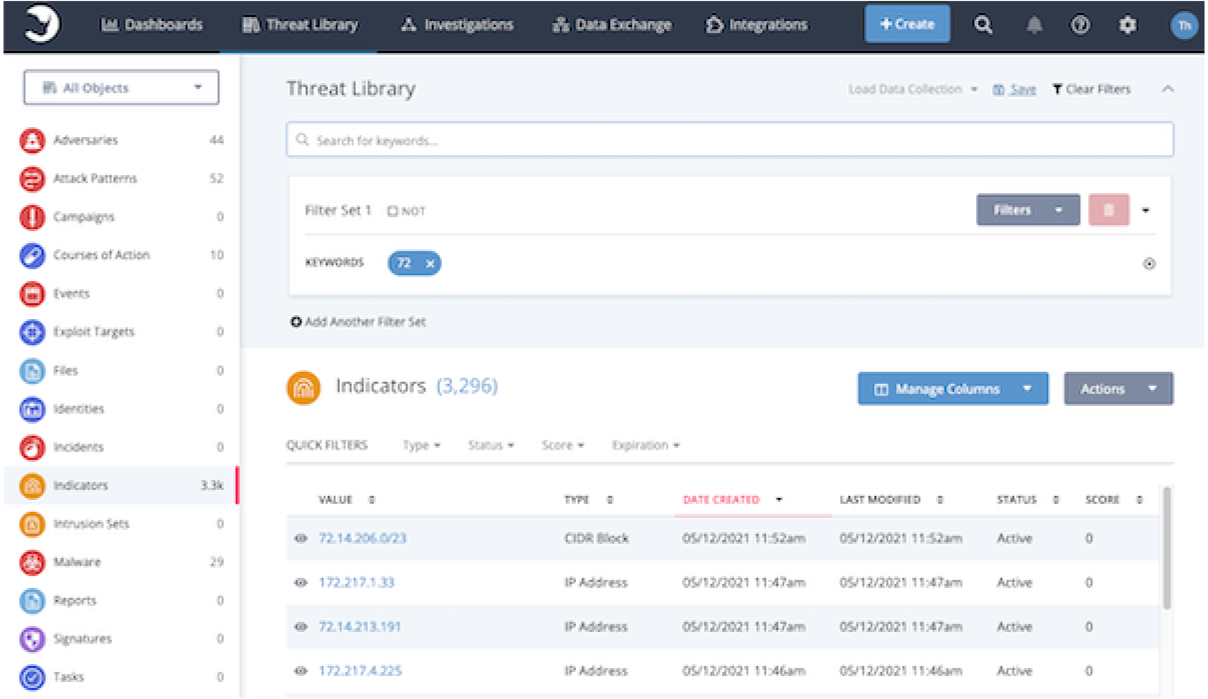
abdahmani.serveftp.net

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.

Bulk Status Change

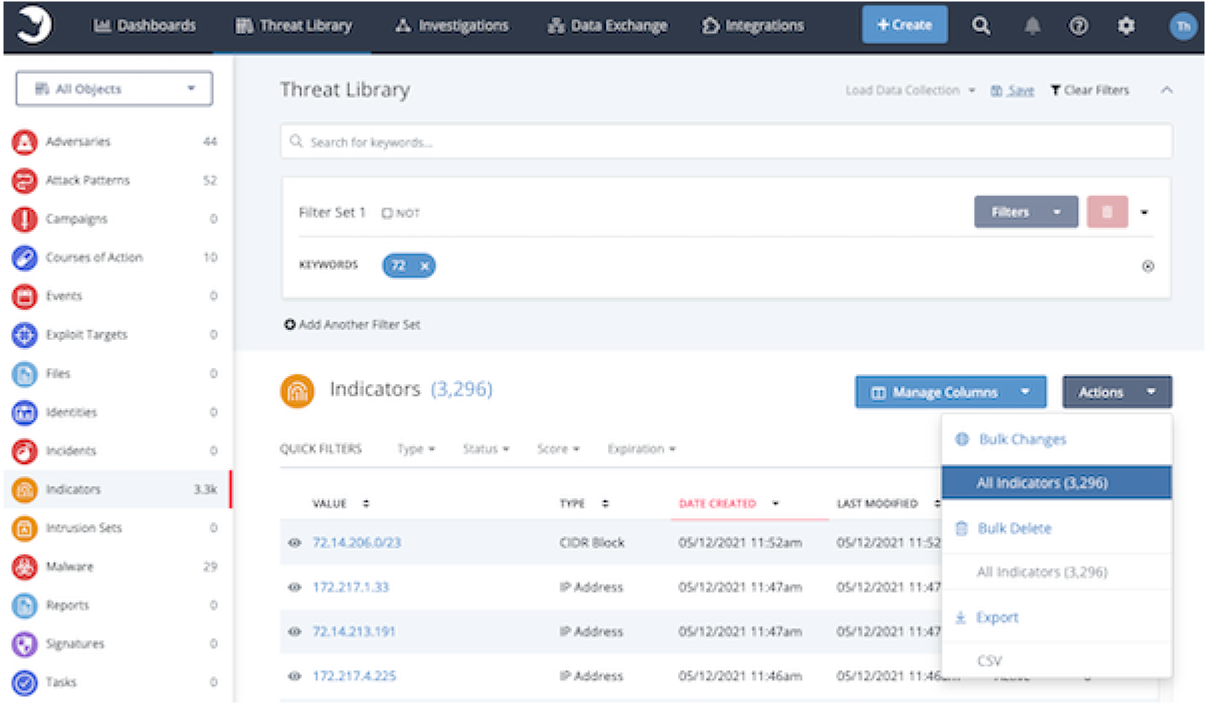
> This function can only be performed on objects that use the status field such as Indicators, Signatures, etc.
>
> Whitelisted Indicators are not affected by Bulk Status Change. If a Whitelisted Indicator is included in the set of system objects selected for a Bulk Status Change, the platform will skip the object without making a status change.

1. Perform a search on the Threat Library.



VALUE	TYPE	DATE CREATED	LAST MODIFIED	STATUS	SCORE
72.14.206.0/23	CIDR Block	05/12/2021 11:52am	05/12/2021 11:52am	Active	0
172.217.1.33	IP Address	05/12/2021 11:47am	05/12/2021 11:47am	Active	0
72.14.213.191	IP Address	05/12/2021 11:47am	05/12/2021 11:47am	Active	0
172.217.4.225	IP Address	05/12/2021 11:46am	05/12/2021 11:46am	Active	0

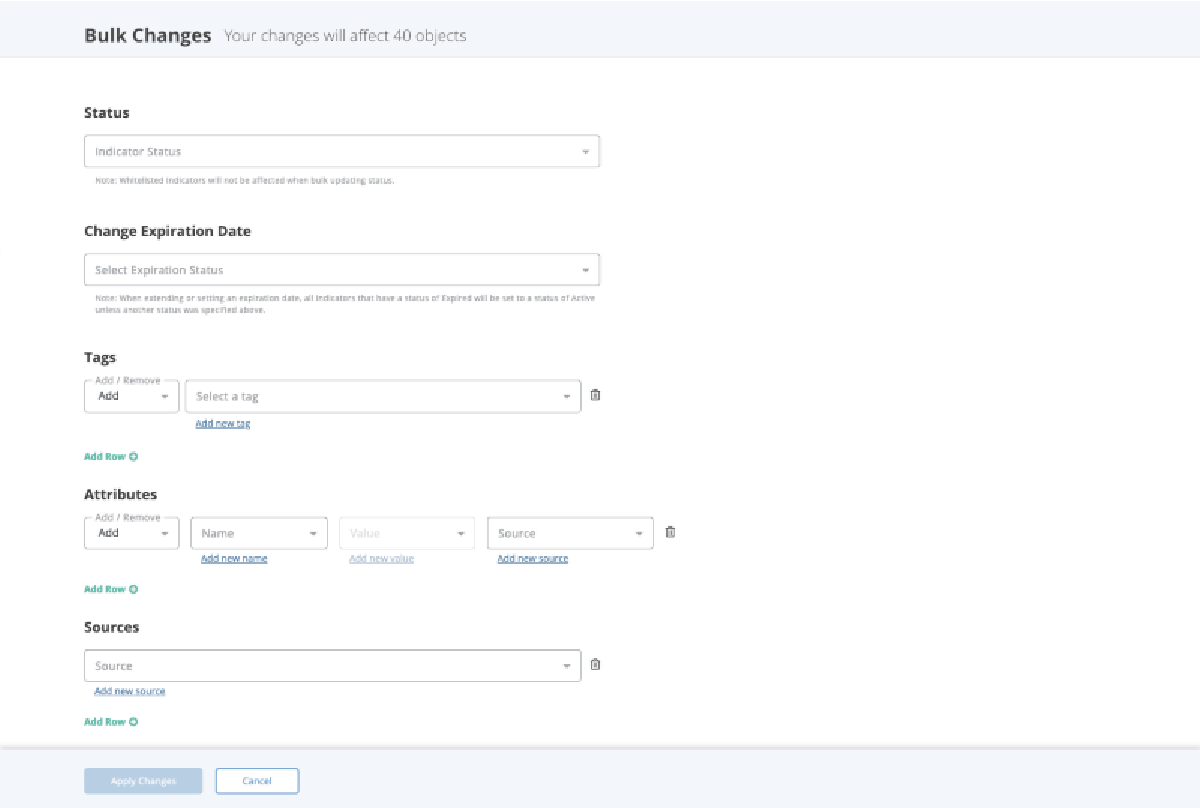
2. Click on the **Actions** dropdown and select **All <System Object>** under the *Bulk Changes* heading.



VALUE	TYPE	DATE CREATED	LAST MODIFIED
72.14.206.0/23	CIDR Block	05/12/2021 11:52am	05/12/2021 11:52
172.217.1.33	IP Address	05/12/2021 11:47am	05/12/2021 11:47
72.14.213.191	IP Address	05/12/2021 11:47am	05/12/2021 11:47
172.217.4.225	IP Address	05/12/2021 11:46am	05/12/2021 11:46

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

The Bulk Changes form will load.


Bulk Changes Your changes will affect 40 objects

Note: Whitelisted indicators will not be affected when bulk updating status.

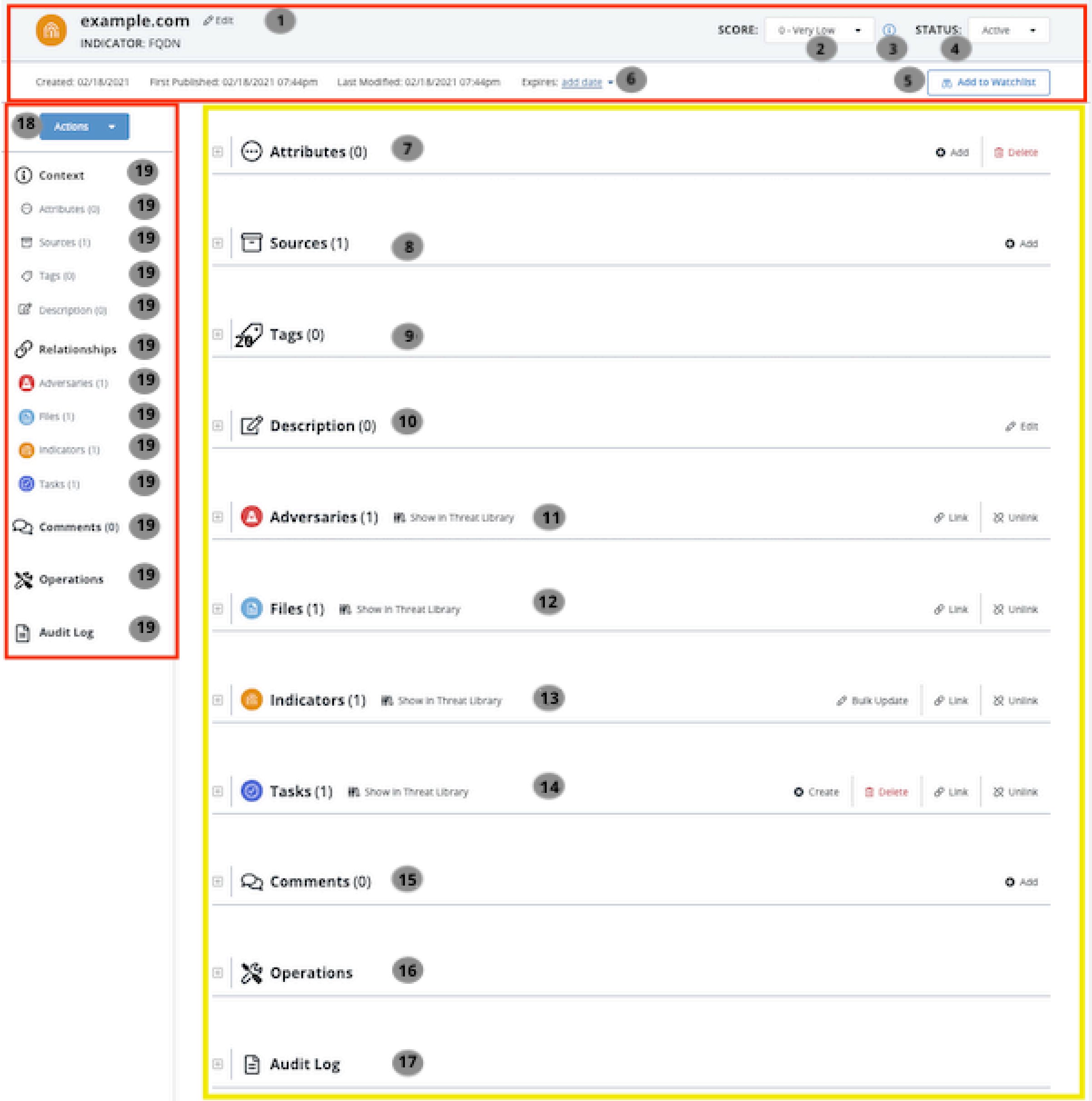
Note: When extending or setting an expiration date, all indicators that have a status of Expired will be set to a status of Active unless another status was specified above.

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.

Object Details

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, display additional information such as the indicator's status, score, and expiration data.



example.com

INDICATOR: FQDN

SCORE: 0 - Very Low

STATUS: Active

Created: 02/18/2021 First Published: 02/18/2021 07:44pm Last Modified: 02/18/2021 07:44pm Expires: add date

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
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.	N/A
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.	• Indicator Expiration • Scoring Algorithms
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.	• Scoring Algorithms
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 • Indicator Statuses Management (Object Management)

OBJECT DETAILS PAGE LEGEND

5	Add to Watchlist	The Watchlist toggle button allows you to add and remove the object from the Watchlist widget.	- Add/Remove an Object to 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 - Indicator Expiration Policies (Data Controls)

Details Section

Number	Pane	Description	Reference
7	Attributes	The Attributes pane displays attributes associated with the object. You can Add, Edit, and Delete attributes found in this section.	- Attributes Pane
8	Sources	The Sources pane displays sources associated with the object. You can Add additional sources to an object.	- Sources Pane
9	Tags	The Tags pane displays tags associated with the object. You can Add and Delete tags found in this section.	- Tags Pane
10	Description	The Description pane allows you to add general information about the object.	- Description Pane

OBJECT DETAILS PAGE LEGEND

11	Adversary	The Adversaries pane displays adversaries associated with the object.	• Relationships Panes
12	Files	The Files pane displays files associated with the object and gives you the option to preview, download, and/or parse the file. If your browser does not support file preview for a specific file type, the file is downloaded instead. You cannot preview a malware locked file.	• Relationships Panes
13	Indicators	The Indicators pane displays indicators associated with the object.	• Relationships Panes
14	Tasks	The Tasks pane displays tasks associated with the object.	• Relationships Panes
15	Comments	The Comments pane allows you to record comments about the object for other users to read and reference.	• Relationships Panes
16	Operations	The Operations pane allows you to associate third-party attributes and related indicators to the indicator.	• Integrations Management

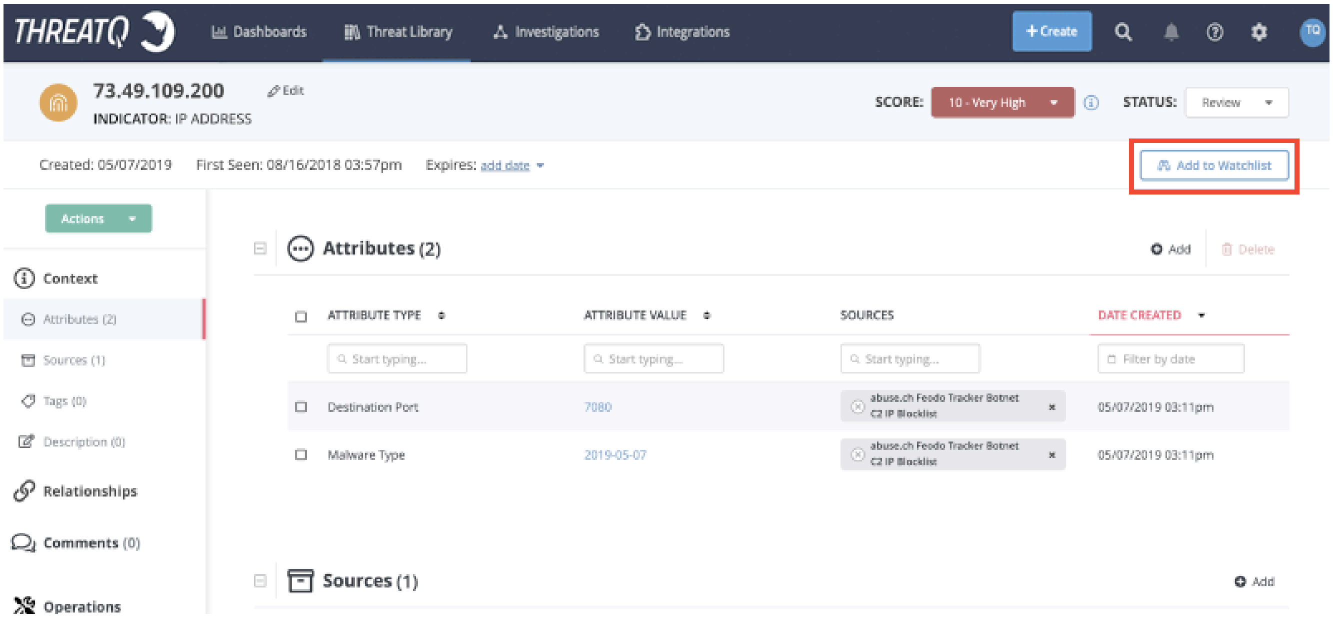
OBJECT DETAILS PAGE LEGEND

		This options requires the installation of Operations. See the Managing Integrations topic for more details.	
17	Audit Log	The Audit Log panel displays all actions and changes made to an Object.	• Audit Log
Left-Hand Navigation			
Number	Field	Description	Reference
18	Actions Menu	The Actions menu lists the following options: • Add Attribute • Add Comment • Add Relationship • Add Source • Create Task • Generate PDF • Delete Indicator • Start Investigation • Add to Investigation	• Actions Menu
19	Details Navigation Tabs	This allows you to jump to a particular pane on the Object Details page.	N/A

Adding/Removing an Object to the Watchlist

> The steps to remove an item from the Watchlist are the same as adding an item.

1. From the ThreatQ user interface, navigate to the Details page of system object you want to track.
2. Click **Add to Watchlist** to track that item.



73.49.109.200

INDICATOR: IP ADDRESS

SCORE: 10 - Very High

STATUS: Review

Created: 05/07/2019 First Seen: 08/16/2018 03:57pm Expires: add date

Attributes (2)

ATTRIBUTE TYPE	ATTRIBUTE VALUE	SOURCES	DATE CREATED
Destination Port	7080	abuse.ch Feodo Tracker Botnet C2 IP Blocklist	05/07/2019 03:11pm
Malware Type	2019-05-07	abuse.ch Feodo Tracker Botnet C2 IP Blocklist	05/07/2019 03:11pm

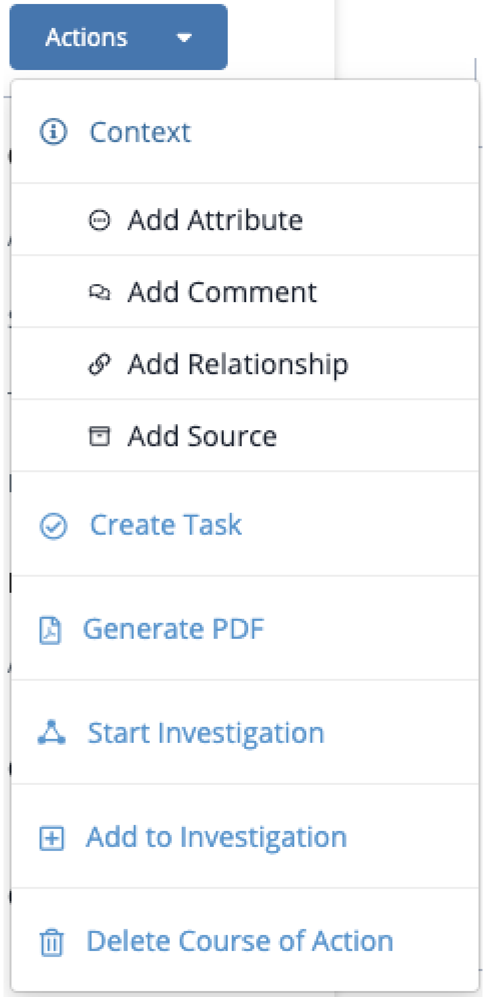
Sources (1)

> Click on **Remove from Watchlist** to remove an item.

The object will be added to the Watchlist on the system default dashboard.

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 which allows you to add an attribute to the object.	• Attributes Pane
Add Comment	Displays a new text entry field in the Comments pane.	• Comments Pane

ACTION	FUNCTION	REFERENCE
Add Relationship	Brings up the Add Relationships window which allows you to link other system objects to the object.	• Relationships Panes • Additional Related Object Actions
Add Source	Brings up the Add Details window which allows you to add a source to the object.	• Sources Pane
Create Task	Opens the Add Task window.	
Generate PDF	Generates a PDF report of the object.	• Reports
Start Investigation	Opens the Create Investigation window so that you can create a new investigation to which the object is automatically added.	• Editing an Investigation
Add to Investigation	Opens the Select Investigation window which allows you to add the object to one or more existing investigations.	
Delete <*Object*>	The Are You Sure? window prompts you to confirm the deletion by clicking the **Delete** button.	

Context Panes

Based on the system object type, the Context section of the object details page displays:

- Attributes
- Sources
- Tags
- Descriptions
- Spearphish Details
- Additional Information

Sources Pane

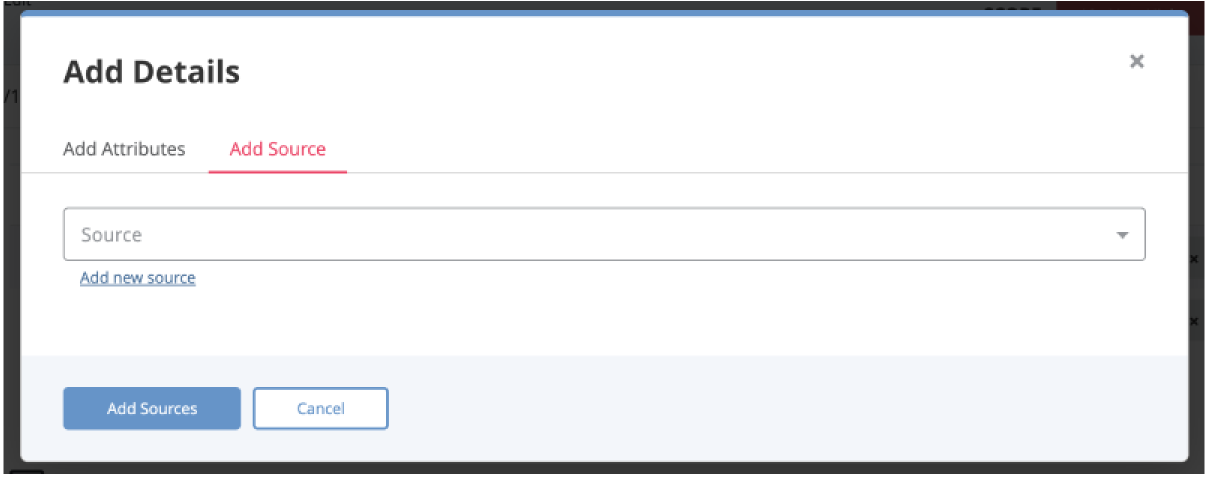
The Sources pane displays all Sources associated with the system object.

See *Bulk Add Source* section in the Bulk Actions topic for information on adding a source to a group of system objects.

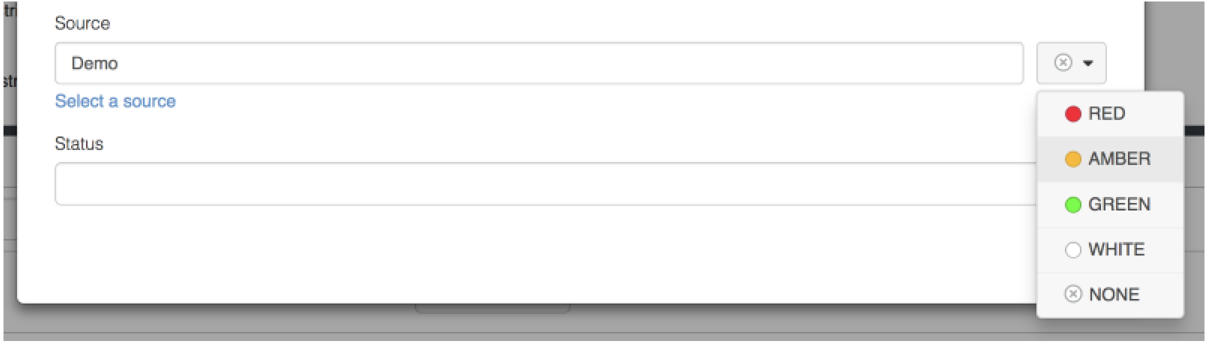
Adding a Source to an Object

You can add sources to a system object in its details pane.

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



Source
Demo

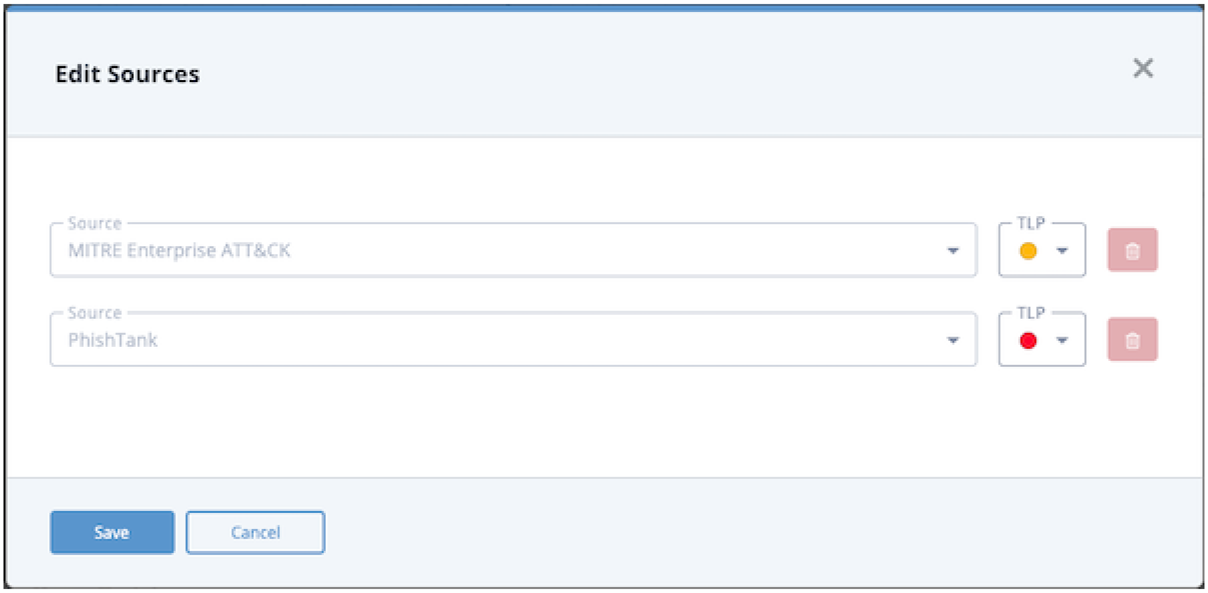
4. Select **Add Sources**.

Editing a Source's TLP Label

> The option to edit a source’s TLP label is only available if TLP visibility is enabled via the TLP tab in the Data Controls page.

1. Locate the Sources pane on the object details page.
2. Click a source to access the Edit Sources window. This window lists all the sources associated with the system object.

   > The delete button displayed next to each source's TLP label is inactive and reserved for future functionality.



Edit Sources

Source: MITRE Enterprise ATT&CK — TLP: ●

Source: PhishTank — TLP: ●

3. Select the new TLP label from the dropdown list and click the **Save** button.

Tags Pane

You can add and remove tags in the Tags pane on the object details page.

See Bulk Actions Add/Remove Tags for information on adding/removing tags from a group of system objects.

Adding an Existing Tag to an Object

1. Locate the Tags pane on the object details page.
2. Click the **Select an existing tag** field.
3. Select the tag you want to add from the dropdown list.

> You can narrow the dropdown list options by entering all or part of the tag name. As you type, the dropdown list displays matches for your entry.

Adding a New Tag to an Object

1. Locate the Tags pane on the object details page.
2. Click the **Create a new tag** option.
3. Type the new tag's name in the **Tag name** field.
4. Press **Enter** to save the new tag and add it to the system object.

Deleting a Tag from an Object

1. Locate the Tags pane on the object details page.
2. Select the **X** next to the tag name.

Description Pane

The Description Pane section of the object details page allows you to add a description for the system object. Object descriptions can include text, tables, and images.

Tips and Tricks

- **Image alignment** - Images in an object's description are displayed in the PDF report for the object as left aligned regardless of the alignment you select in the Description pane.
- **Image captions** - Add your image captions after you select your image alignment. If you change alignment after adding a caption, the caption is removed and must be added again.
- **Image text alternatives** - If you add an image text alternative to an image, it is available for use by screen reading tools but is only displayed on screen if the image fails to load. It is not displayed when you hover on the image.
- **Add a line above or below** - When you click an image, the arrow icons located on the bottom left and top right corners allow you to insert a line above (top right arrow) or below (bottom left arrow) the image.
- **Resize an image** - The resize image option allows you to adjust your image to 25%, 50%, or 75% of the size of the Description field. Or, you can return your image to its original size.
- **Paste rows into an existing table** - To paste rows into an existing table, insert a blank row in the table, click in the first cell of the blank row, and then paste the additional rows.

> After upgrading to ThreatQ 5x, you can no longer click and drag the right corner of the Description field to resize it while entering data. However, the entry field does scroll. When you save your entry, the Description pane expands to display your entry.

Updating the Description of an Object

1. Locate the Description pane on the object details page.
2. Click the **Edit** option to add/update the object descriptions text, tables, or images.
3. Make the required changes and click the **Save** button.

Spearphish Details Pane

You can update spearphish file details as well as add or delete recipients from the Spearphish Details pane in a Spearphish event's object details page.

Adding a Recipient

1. Locate the Spearphish Details pane on the object details page.
2. Click the Add Recipients option.
   The Add Recipients window is displayed.
3. Populate the following fields:
    - **Recipient type** - This field defaults to a value of To. Use this field to specify whether the email was sent directly to the recipient (To) or the recipient received it as a carbon copy (CC) or blind carbon copy (BCC).
    - **Email address** - Enter the email address that received the spearphish file.
    - **Link all emails as related indicators** - This field defaults to checked. Leave this box checked to add a releated indicator record to the system object for each email address.
3. To add another recipient, click the + button and repeat step 3.
3. To save your recipient additions and return to the Spearphish Details pane, click the Add Recipients button.

Deleting a Recipient

1. Locate the Spearphish Details pane on the object details page.
2. Click the checkbox(es) next to the recipient(s) you want to delete.
3. Click the Delete option.
   The Are You Sure? window prompts you to confirm your action.
4. Click the Delete Recipients button.

Editing a Spearphish File

1. Locate the Spearphish Details pane on the object details page.
2. Click the Edit button.

2. Enter your changes in the Email Content field.
2. Click the Save button.

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.

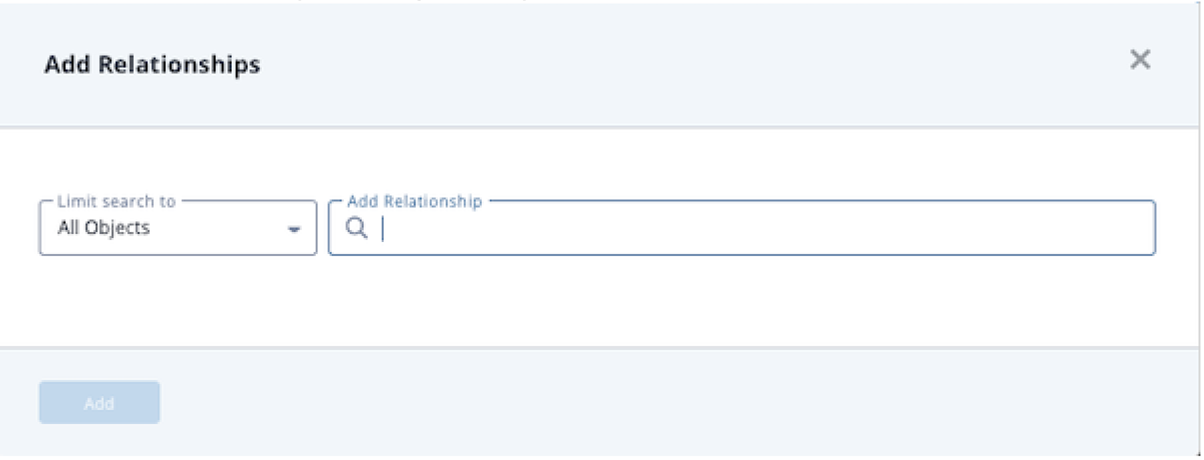
> Certain related system objects, such as related indicators, will have additional actions available. See the Additional Related Object Actions topic.

Linking a System Object

1. Locate the desired system object type pane on the 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**.

2. Select the 🔗 Link icon.
   The Add Relationships dialog box opens.



Limit search to: All Objects

3. Use one of the following methods to add an object to the Add Relationships field:
   - For existing objects, enter the object name and select the match from the down list.

     > Repeat this step to add multiple objects.

   - To create a new object, enter the new object name. The, click the **Create** link to add the new object to Threat Library. If you limited your search to a specific object type, you are linked to the corresponding form. For example, if you limited your search to Adversaries, the Create link opens the Add An Adversary form. If you left the **Limit search to field** set to All Objects, you can select the object type you want to create from a drop-down list.

4. Click **Add**.

Unlinking a System Object

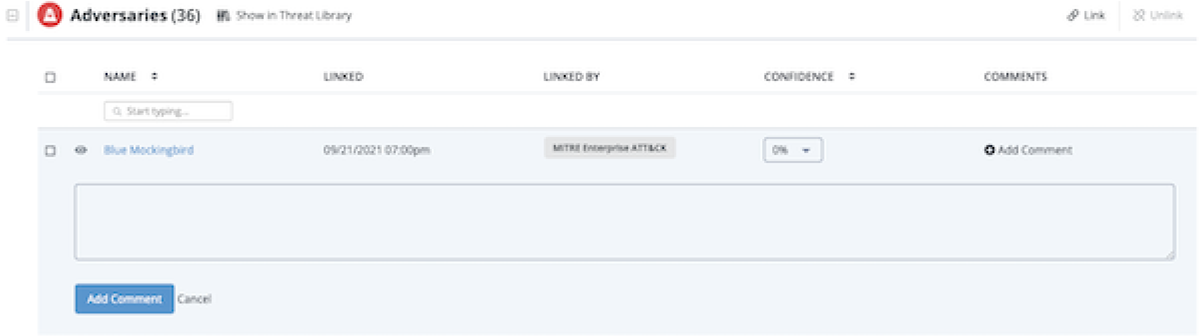
1. Locate the Related <System Object> pane on the object's details page.
2. Select the checkbox(es) next to the system objects to unlink.
3. Select the Unlink icon.

Additional Related Object Actions

Certain system object types will offer you additional actions after relating the objects to another object.

Adding 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.



☐	NAME	LINKED	LINKED BY	CONFIDENCE	COMMENTS
☐	Blue Mockingbird	09/21/2021 07:00pm	MITRE Enterprise ATT&CK	0%	Add Comment

3. Enter a comment.
4. Click **Add Comment**.

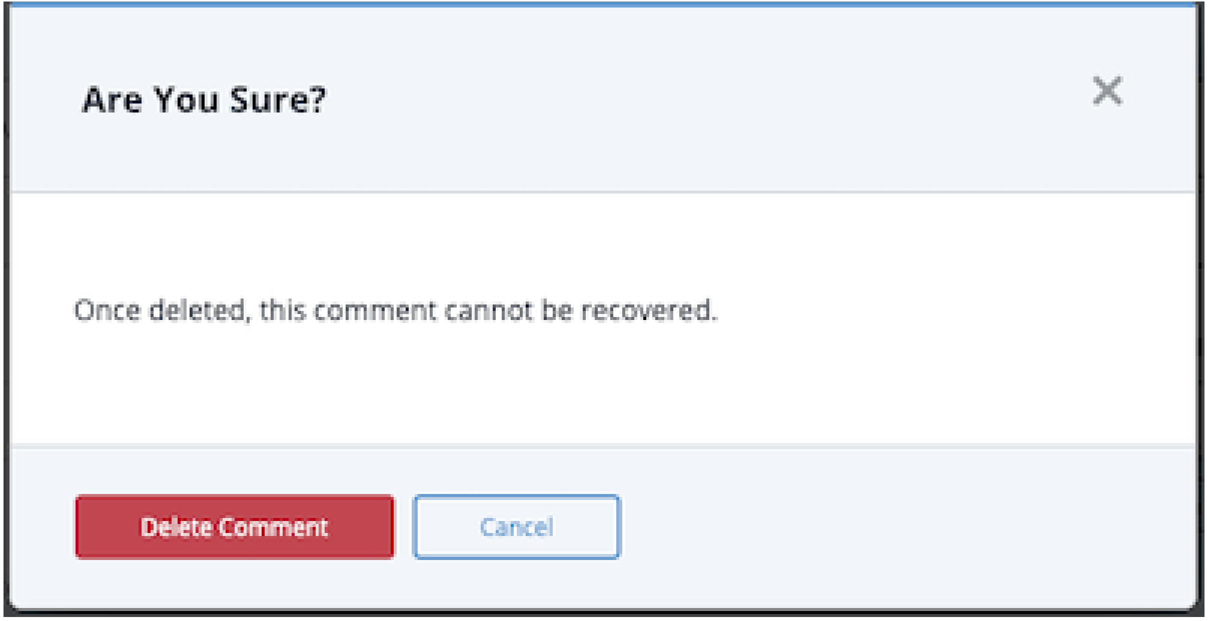
Editing a related adversary comment

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**.

Deleting 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.



Are You Sure?

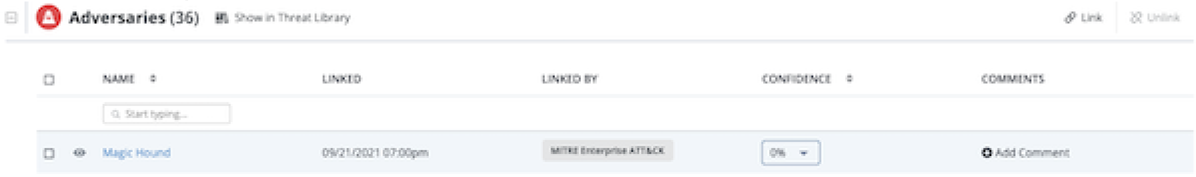
Once deleted, this comment cannot be recovered.

3. Select **Delete Comment**.

Related Adversaries - Confidence Level

You can configure a related adversary's confidence level from the Adversaries pane.

1. Locate the Adversaries pane on the object details page.
2. Click the dropdown arrow in the Confidence field to select the desired confidence level.



☐	NAME	LINKED	LINKED BY	CONFIDENCE	COMMENTS
☐	Magic Hound	09/21/2021 07:00pm	MITRE Enterprise ATT&CK	0%	Add Comment

> The confidence level can be set to 0, 25, 50, 75, and 100.

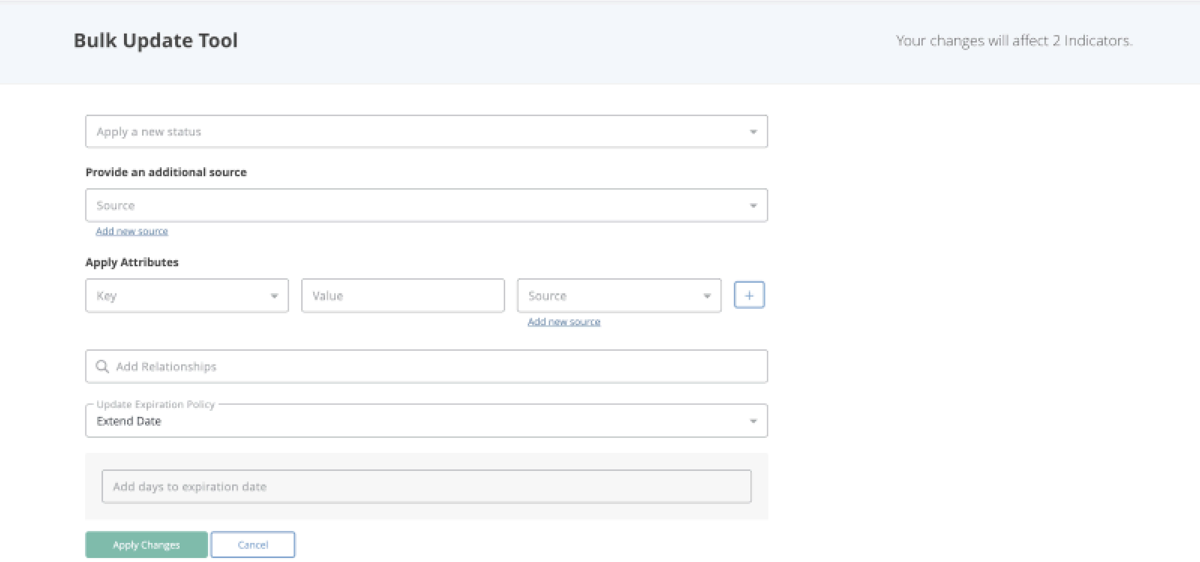
The displayed confidence level will be modified to reflect your selection.

Related Indicators - Bulk Actions

You can perform bulk updates to linked indicators listed in the Indicators pane of an object.

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.



Bulk Update Tool

Your changes will affect 2 Indicators.

Update Expiration Policy: Extend Date

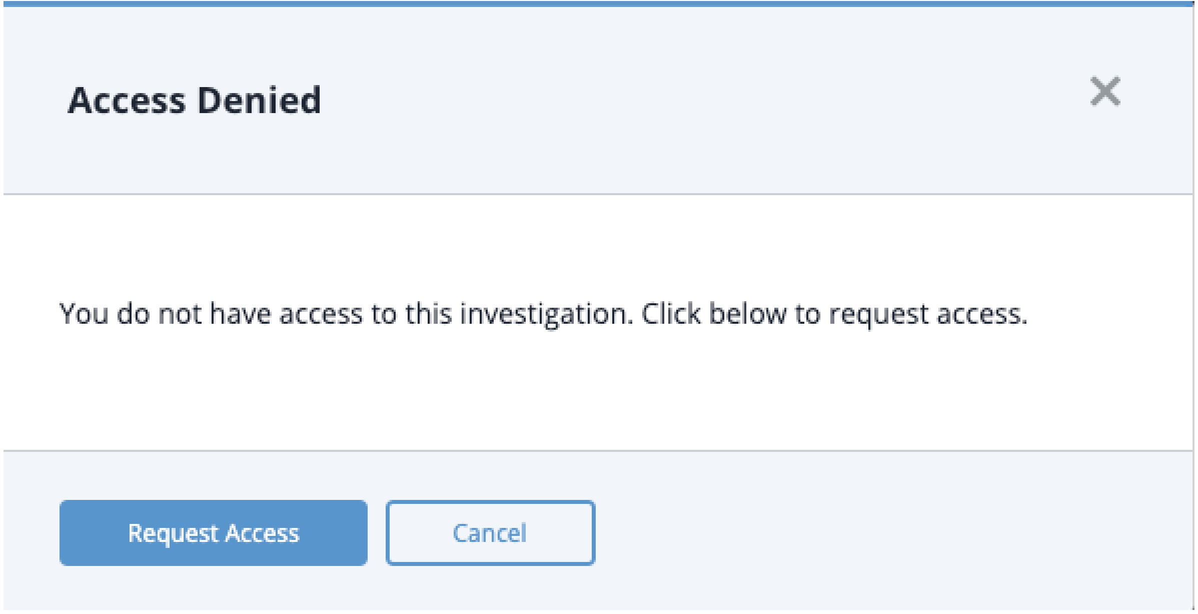
4. Select the desired changes and click **Apply Changes**.

Related Investigations - Request Access

If you do not have Owner, Editor, or Viewer permissions to an investigation related to a system object, you cannot access it unless the investigation owner assigns you one of these permission levels.

1. Locate the Related Investigations pane on the object details page.
2. Click the investigation name.
   If you have permission to access the Investigation, this link takes you to the investigation's evidence board.
   If you do not have permission to access the investigation, the Access Denied window is

displayed. Go to step 3.



You do not have access to this investigation. Click below to request access.

3. From the Access Denied window, click the **Request Access** button.
   The investigation owner receives a Notification Center alert indicating you have requested access to the investigation.

Comments Pane

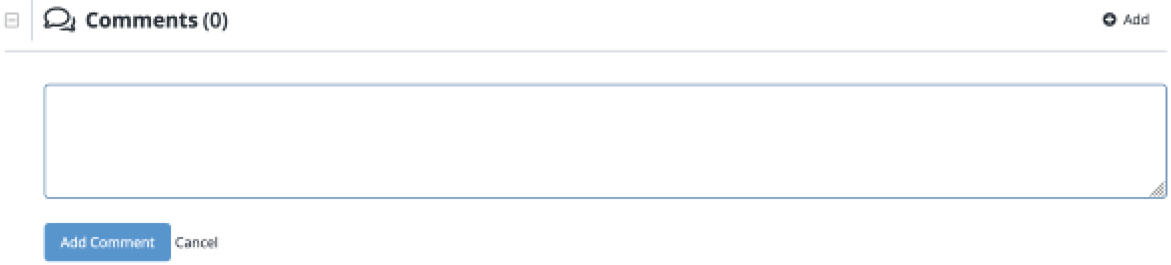
The Comments pane allows users to record comments about the system object for other users to see.

Adding Comments to an Object

> Users can also click on the **Actions** menu and select the **Comment** option.

1. Click on the expand icon ⊞ to expand the Comments pane.
2. Click on the **Add** link located at the top-right of the pane.

   The new comment text box opens.

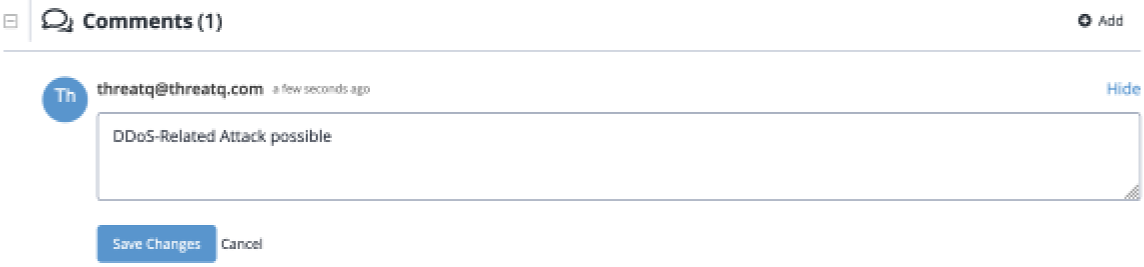


3. Enter a comment.
4. Click on the **Add Comment** button.

Editing Comments for an Object

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.



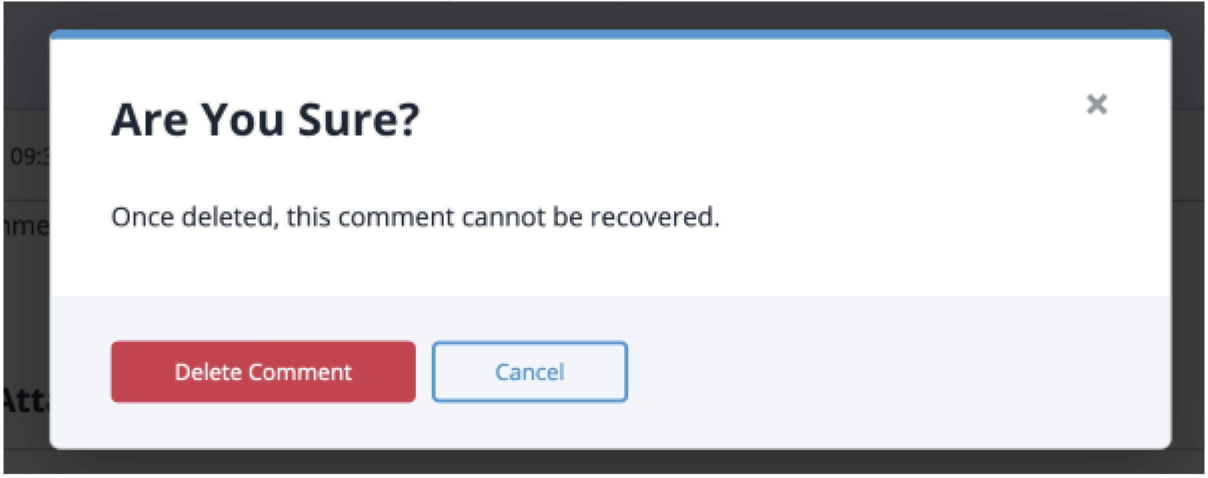
DDoS-Related Attack possible

3. Edit the comment.
4. Click on the **Save Changes** button.

Deleting Comments from an Objects

1. Click on the expand icon ⊞ to expand the Comments pane.
2. Click on the **Delete** link located beneath the comment to update..

   The delete confirmation dialog text box opens.



Are You Sure?

Once deleted, this comment cannot be recovered.

3. Click on the **Delete Comment** button.

Audit Log

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 (Adversary, Files, Events, Indicator, 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.

Troubleshooting

The following topics provide basic troubleshooting steps and platform information.

- Generating a Troubleshooting Package
- SSL Certificates
- ThreatQ v4 Critical System Processes
- Date and Time Stamps

Generating a Troubleshooting Package

In the event that ThreatQ Support requests a troubleshooting package, this topic explains how to create the package. This is a command line tool for gathering all the useful information for troubleshooting issues on a ThreatQ host.

1. Access the ThreatQ host command line via SSH or console.
2. Change directories:

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

3. Run the following command:

   ```
   sudo php artisan threatq:get-debug-info
   ```

   The command for getting hardware info (hwinfo) may not be installed. In this case, an error message is shown, but the execution is not affected.

   You may get a tar notification about the laravel.log file being modified as it is read, this does not affect the process outcome.

   The process creates a file named `debug_info.tar.zip` in /var/tmp/.

4. Send the file to ThreatQ Support and remove it from the host to conserve disk space.

SSL Certificates

ThreatQ performs SSL certification validation on outgoing connections. At times, an incoming feed (particularly TAXII feeds) or operation may require access to sites with CA certificates that are not included in the default bundle included in the software packages ThreatQ uses by default. These certificates will need to be added to the ThreatQ server for these connections to pass validation.

Unable to Verify SSL Certificate

If you find that a feed or operation is not working and results in an "unable to verify SSL certificate" error, complete the following steps:

1. Obtain the remote site's CA in PEM format and upload it to the ThreatQ filesystem:

   ```
   /etc/pki/ca-trust/source/anchors/
   ```

2. Enable it in the system with the command:

   ```
   sudo update-ca-trust extract
   ```

3. Restart the feed ingestion engine:

   ```
   sudo systemctl restart threatq-dynamo
   ```

Contact ThreatQ Support for assistance with obtaining or installing needed CA certs, or if you experience problems with SSL connections.

Configuring Custom SSL Certificates (not self-signed)

You may wish to install your own custom SSL certs to ThreatQ. This can be done according to the standard CentOS Linux instructions, which are included below:

1. Copy the files to your server:

   ```
   scp sslfiles.tar.gz [username]@[server].threatq.com:~
   ```

2. SSH into your server.
3. Create the following directory if it does not currently exist:

```
mkdir /etc/httpd/ssl
```

4. Copy the sslfiles.tar.gz file to the SSL directory created above:

   ```
   sudo cp ~/sslfiles.tar.gz /etc/httpd/ssl/
   ```

5. Navigate to the SLL directory:

   ```
   cd /etc/httpd/ssl
   ```

6. Extract the files from the sslfiles.tar.gz file:

   ```
   sudo tar xzvf sslfiles.tar.gz
   ```

7. Restrict the permissions for your .crt and .key files:

   ```
   sudo chmod 400 yourcert.crt yourkey.key yourca.crt
   ```

8. Open the the ssl.conf file in the terminal:

   ```
   sudo vi /etc/httpd/conf.d/ssl.conf
   ```

9. Comment the following lines with a **#** if they exist:

   ```
   #SSLCertificateFile /etc/pki/tls/certs/localhost.crt
   #SSLCertificateKeyFile /etc/pki/tls/private/localhost.key
   ```

10. Add the following lines as appropriate

    ```
    SSLCertificateFile /etc/httpd/ssl/yourcert.crt
    SSLCertificateKeyFile /etc/httpd/ssl/yourkey.key
    SSLCertificateChainFile /etc/httpd/ssl/yourca.crt (if a certificate chain is
    required)
    ```

11. Save the file.
12. Restart Apache:

    ```
    sudo systemctl restart httpd
    ```

Critical System Processes

The topics below contains a list of critical ThreatQ processes specific to a particular ThreatQ platform release.

SECTION	DESCRIPTION
ThreatQ v5 Critical System Processes	View critical processes for ThreatQ v5 releases.
ThreatQ v4 Critical System Processes	View critical processes for ThreatQ v4 releases.

ThreatQ v5 Critical System Processes

The table below contains a list of critical ThreatQ processes and how they are utilized by the ThreatQ platform.

PROCESS	DESCRIPTION
threatq-containers / docker.service	Threatq-containers houses these processes: • memcached • opendxlbroker - Only present for ThreatQ Data Exchange (TQX) licensed instances. • pynoceros-messenger • websocket • rabbitmq - Used to queue worker jobs and general system messaging such as sending configuration updates. • tika - Document parsing service • tq-dx - Data Exchange service • zookeeper
httpd.service	httpd.service is the Apache web host service for the ThreatQ user interface (UI) and API.
mariadb.service	The mariadb database, which functions as the ThreatQ data persistence service.
threatq-solr.service	SolrCloud is a highly flexible and distributed data processing engine that is used as the primary index for the ThreatQ user interface (UI).
threatq-dynamo.service	ThreatQ-dynamo is the process that handles CDF feed runs and the processing of data returned by feed providers.

PROCESS	DESCRIPTION
threatq-jobs.target	Threatq-jobs.target manages the ThreatQ worker processes that handle Bulk Update actions such as Bulk Delete and Bulk Update.

ThreatQ v4 Critical System Processes

The table below contains a list of critical ThreatQ processes and how they are used by the ThreatQ 4x platform.

PROCESS	DESCRIPTION
threatq-containers / docker.service	Threatq-containers houses these processes: • memcached • opendxlbroker - Only present for ThreatQ Data Exchange (TQX) licensed instances. • websocket • rabbitmq - Used to queue worker jobs and general system messaging such as sending configuration updates. • tq-dx - Data Exchange service
httpd.service	httpd.service is the Apache web host service for the ThreatQ user interface (UI) and API.
mariadb.service	The mariadb database, which functions as the ThreatQ data persistence service.
solr.service	Solr is an open-source enterprise search platform that is used as the primary index for the ThreatQ user interface (UI).
threatq-dynamo.service	ThreatQ-dynamo is the process that handles CDF feed runs and the processing of data returned by feed providers.
threatq-jobs.target	Threatq-jobs.target manages the ThreatQ worker processes that handle Bulk Update actions such as Bulk Delete and Bulk Update.

Date and Time Stamps in ThreatQ

ThreatQ provides date and time stamps for threat intelligence, so that you can track the flow of data in the platform. The following table provides an overview of what these various stamps indicate in the ThreatQ platform.

ThreatQ UI Date and Time Stamps

DATE AND TIME STAMP	DEFINITION
(Date) Created	This indicates the date when the object was added to ThreatQ.
Due Date	The due date set by the user for a task. See the Tasks topic for more details.
Expiration Date	This is the expiration date for a system object. See the Indicator Expiration and Automatic Expiration topics for more details.
First Published	Varies, depending on the object source: • If the source doesn't contain a publication date, this date indicates the first time the object is imported into ThreatQ. In this case, the created and first published dates will match. • If the source contains a publication date, this date indicates the first time the object was published by the feed.
Last Modified	The date and time when object-specific information was last updated, such as updating an indicator's status.
Source Ingest Time	The date and time that an object was initially reported by a source.

User Management

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 its user role group, display name, and email address.

Managing User Accounts

While all users can update their own individual accounts, only users with Maintenance Account and Administrative Access user roles have permission to access the User Management functionality. You must be logged in as one of these roles in order to create new user accounts.

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

Accessing Your User Account

1. Click on your avatar icon, located to the top-right of the platform, and select **My Account**.
   The Edit User screen allows you to review and update your User Account Properties.

Accessing Other User Accounts

> Only users with Maintenance and Administrative accounts can add, edit, and delete other user accounts.

1. Click the **Settings** icon ⚙ and select **User Management**.
   The User Management screen displays a list of user accounts.
2. You can filter and/or sort the user accounts displayed by:
   - Display Name
   - Status
   - Username
   - Email
   - Group
   - 2-Step Verification
3. If you are logged in with a Maintenance or Administrative account, you can also click a display name to access the corresponding User Account Properties.

User Account Properties

FIELD	DESCRIPTION
Name	Update the user's name.
Title	Update the user's job title.
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 avatar.
2-Step Verification	Optional. The toggle switch in this section allows you to enable/disable 2-step verification.
Client CERT Authentication Enabled	If SSL Client Certificate Authentication is enabled, this section displays the user's certificate fingerprint or allows you to add/update a certificate fingerprint.
Activity Log	You can click on the Activity log tab to view the following information: • The last date and time the user logged in. • The IP Address where the user logged in. • Whether the login was successful or not.

Adding a User

> Only users with Maintenance and Administrative accounts can add user accounts.

1. From the main menu, choose the **Settings icon** ⚙ > **User Management**.
2. Click **Add User**.
   The Add User window is displayed.
3. Populate the following fields:
   - **Display Name** - *Required.* Enter the user's name.
   - **Title** - Optional. Enter the user's title.
   - **Group** - *Required.* Select the level of access for the user from the **Group** drop-down menu:
     - Maintenance Account
     - Administrative Access
     - Primary Contributor Access
     - Read Only Access

     > See the User Roles topic for more detail on these access levels.
   - **Username** - *Required.* Enter the user's login ID.
   - **Email** - Optional. Enter the user's email address.
   - **Password** - *Required.* Enter the user's password.
   - **Retype Password** - *Required.* Re-enter the user's password.
4. Click the **Add User** button.
   The System User tab displays the new user. See the Editing a User topic for information on further customizing the user profile.

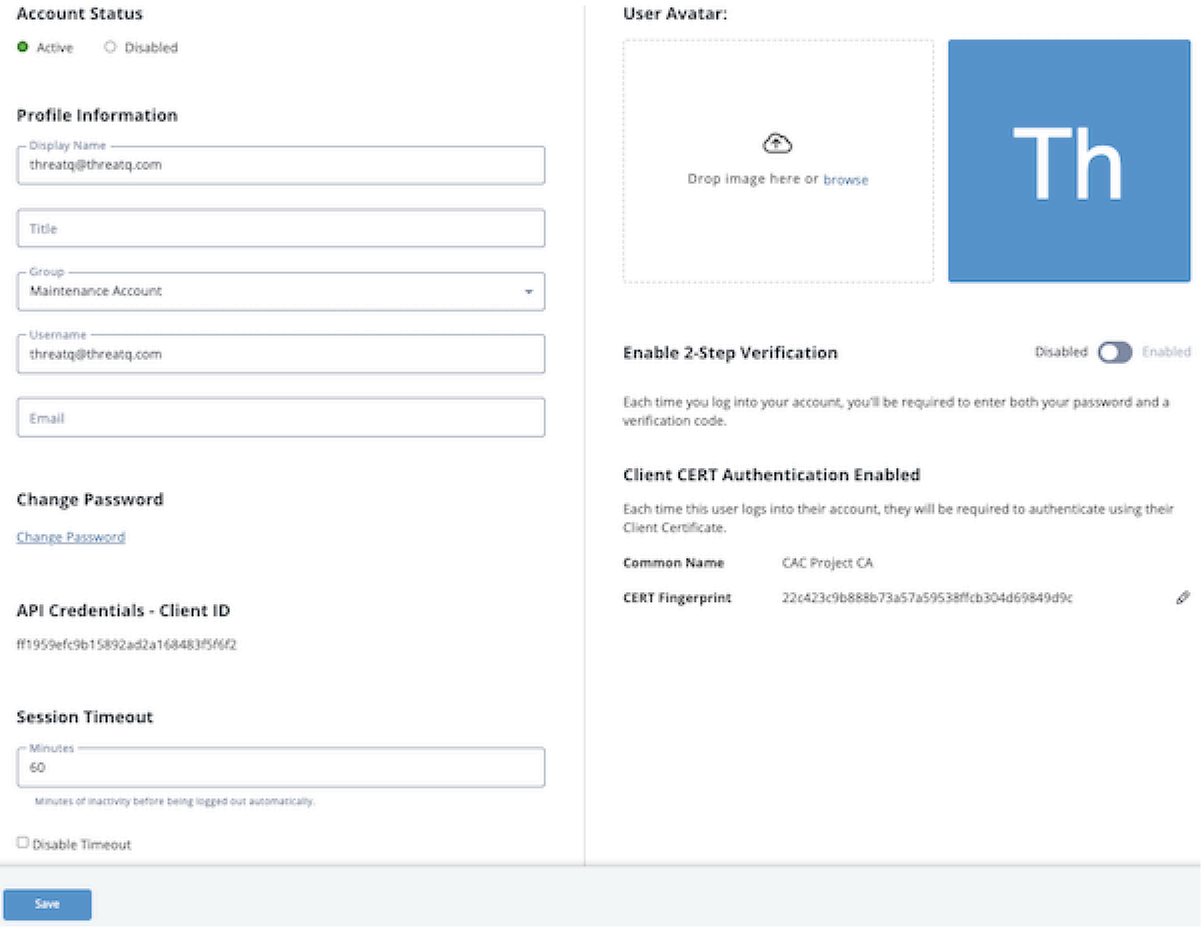
Editing a User

> Only users with Maintenance and Administrative accounts can edit another user's account. You cannot edit user details for SAML nor LDAP users from the User Management page.

1. Click the **Settings** icon ⚙ and select **User Management**.

> To edit your own account, click your avatar icon and select My Account. Proceed to step 3 below.

2. Click the user's display name.
   The User Profile page loads.



Account Status

● Active ○ Disabled

Profile Information

Display Name: threatq@threatq.com

Title:

Group: Maintenance Account

Username: threatq@threatq.com

Email:

Change Password

Change Password

API Credentials - Client ID

ff1959efc9b15892ad2a168483f5f6f2

Session Timeout

Minutes: 60

Minutes of inactivity before being logged out automatically.

☐ Disable Timeout

User Avatar:

Enable 2-Step Verification Disabled / Enabled

Each time you log into your account, you'll be required to enter both your password and a verification code.

Client CERT Authentication Enabled

Each time this user logs into their account, they will be required to authenticate using their Client Certificate.

Common Name CAC Project CA

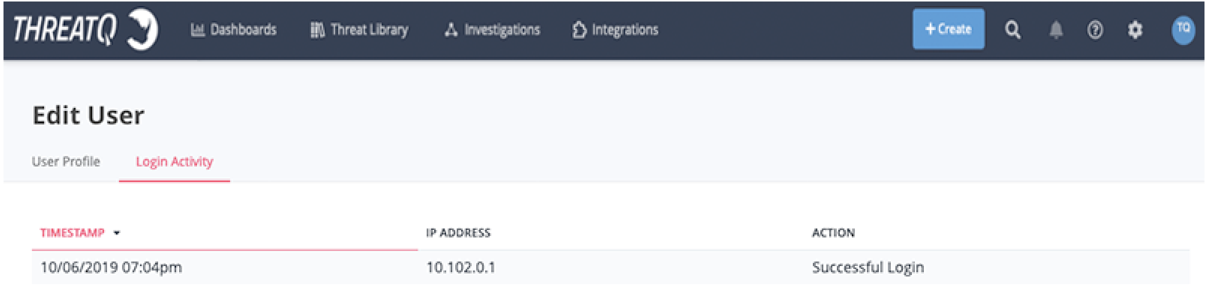
CERT Fingerprint 22c423c9b888b73a57a59538ffcb304d69849d9c

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

FIELD	DESCRIPTION
Name	Update the user's name.
Title	Update the user's job title.
Email	You can update the user's email address.

FIELD	DESCRIPTION
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 avatar.
2-Step Verification	Optional. The toggle switch in this section allows you to enable/disable 2-step verification.
Client CERT Authentication Enabled	If SSL Client Certificate Authentication is enabled, this section displays the user's certificate fingerprint or allows you to add/update a certificate fingerprint.

4. You can also 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.



TIMESTAMP	IP ADDRESS	ACTION
10/06/2019 07:04pm	10.102.0.1	Successful Login

5. After you enter your changes, click the **Save** button.

Resetting User Password from the Command Line

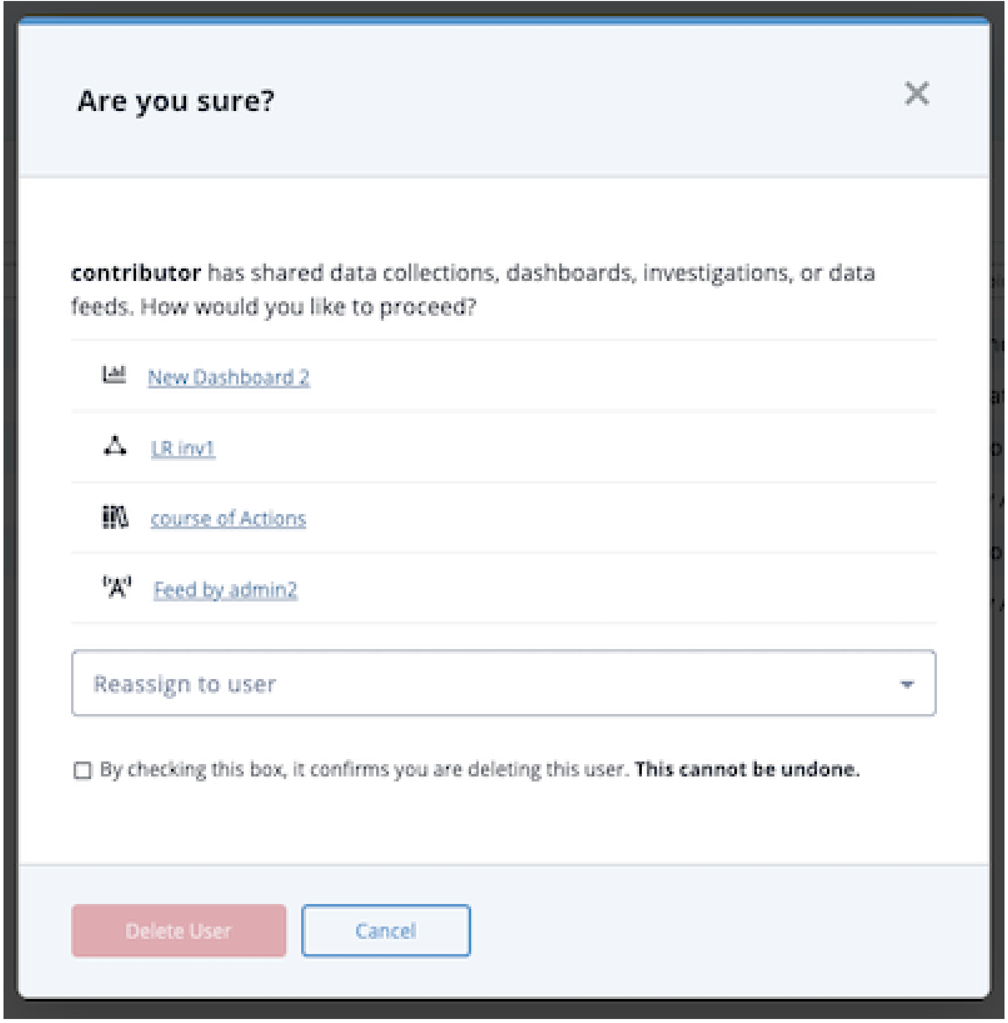
If you have root access to your ThreatQ installation, you can reset any user's password from the command line. See the Resetting User Passwords from the Command Line section in the Commands topic.

Deleting a User

⚠ Deleting a user cannot be undone.

1. From the main menu, choose the **Settings icon > User Management**.
2. In the System Users tab, click the check box next to each user you want to delete.
3. Click the trashcan button.
   If the user has any shared data collections, data feeds, dashboards, or investigations, the **Are you sure?** window notifies you and lists them. You must reassign owner permissions or delete them. These objects are linked so that, if you have the corresponding viewer or

editor permissions, you can click and view the object in a new tab.



Are you sure?

contributor has shared data collections, dashboards, investigations, or data feeds. How would you like to proceed?

- New Dashboard 2
- LR inv1
- course of Actions
- Feed by admin2

☐ By checking this box, it confirms you are deleting this user. **This cannot be undone.**

4. Click the **Reassign to user** field and do one of the following:
    - **Reassign Ownership** - Select the new owner of the data collections, data feeds, dashboards, and/or investigations.
    - **Delete** - Select the **Do not reassign. Delete these items.** option to delete all of the user's data collections, data feeds, dashboards, and/or investigations.
5. Check the confirmation checkbox and click the **Delete User** button.

Updating a User Avatar

User avatars provide a personalized look to your ThreatQ dashboard. ThreatQ supports the use of all standard image types for avatars and a maximum image size of 260 x 260 pixels.

1. Click the avatar icon and select **My Account**.
   The Edit User page is displayed.
2. From the Use Avatar section, you can:

  - Click the browse link and select the icon to upload.
  - Click and drag the new icon onto the page.
3. Click the **Save** button.

User Roles

The following details the user roles and their base-level permissions. A user account's access to data collections and dashboards can be further customized by the Sharing permissions assigned to it.

USER ROLE	PERMISSION
Maintenance Account	Members have access to the entire ThreatQ user interface and can edit all data. **Important Notes:** • The initial local Maintenance Account, created when installing ThreatQ, cannot 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 can: • Edit their own user info • Manually create system objects • Create and manage ThreatQ Investigations • Access Whitelist Management (Data Controls) • Perform a basic search • Access the Threat Library, object metadata, export search results, and manage Data Collections • Create custom dashboards and add shared dashboards to their user view.
Read Only Access	Members can:

- Access the Threat Library, object metadata, export search results
- Add shared dashboards to their user view
- Load saved Data Collections

> Members cannot edit any data.

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:

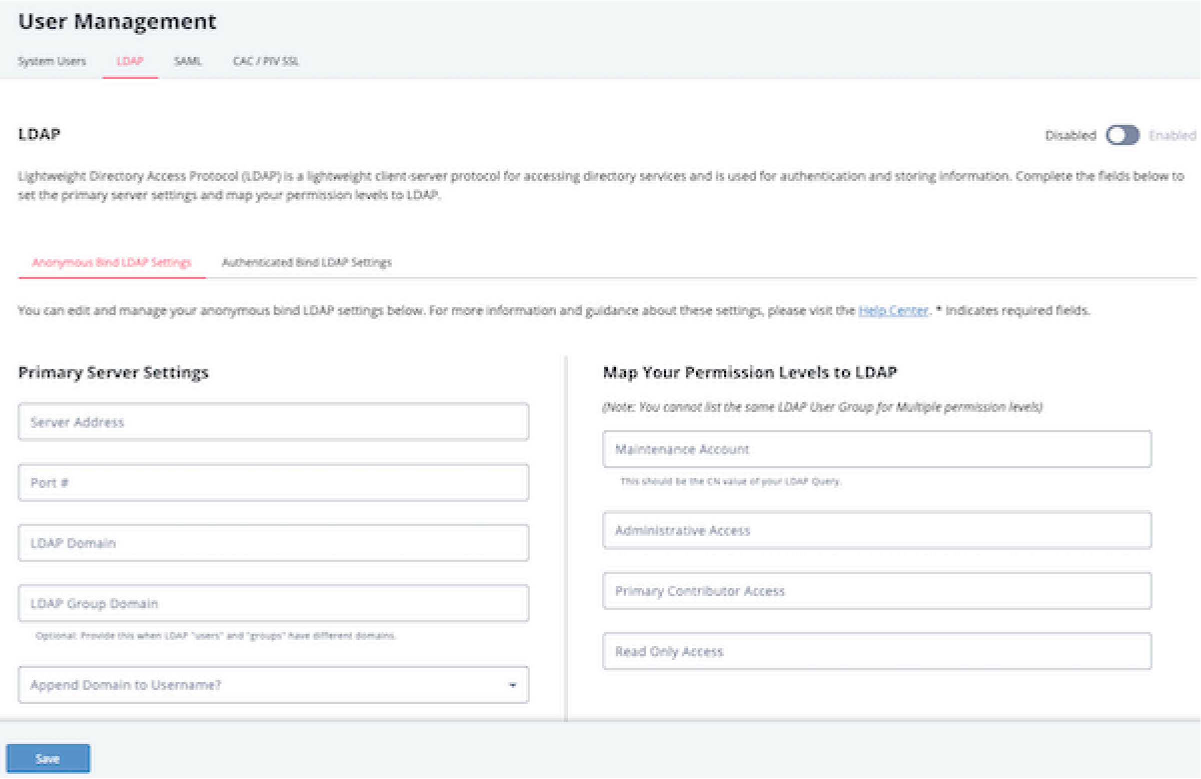
- Anonymous Bind (previously referred to as basic)
- Authenticated Bind

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

To Access the LDAP tab:

1. From the main menu, select the Settings ⚙ icon > User Management.
2. Click the **LDAP** tab.

The LDAP tab opens with the Anonymous Bind LDAP Settings form loaded by default.



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.

You can edit and manage your anonymous bind LDAP settings below. For more information and guidance about these settings, please visit the Help Center. * Indicates required fields.

Optional: Provide this when LDAP "users" and "groups" have different domains.

(Note: You cannot list the same LDAP User Group for Multiple permission levels)

This should be the CN value of your LDAP Query.

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

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:** You are using the Anonymous Bind LDAP option. You switch to the Authenticated Bind LDAP Settings tab and click Save. ThreatQ will now use these settings. If you switch back to the Anonymous Bind LDAP Settings tab and click Save again, ThreatQ will start using the Anonymous Bind LDAP settings again.

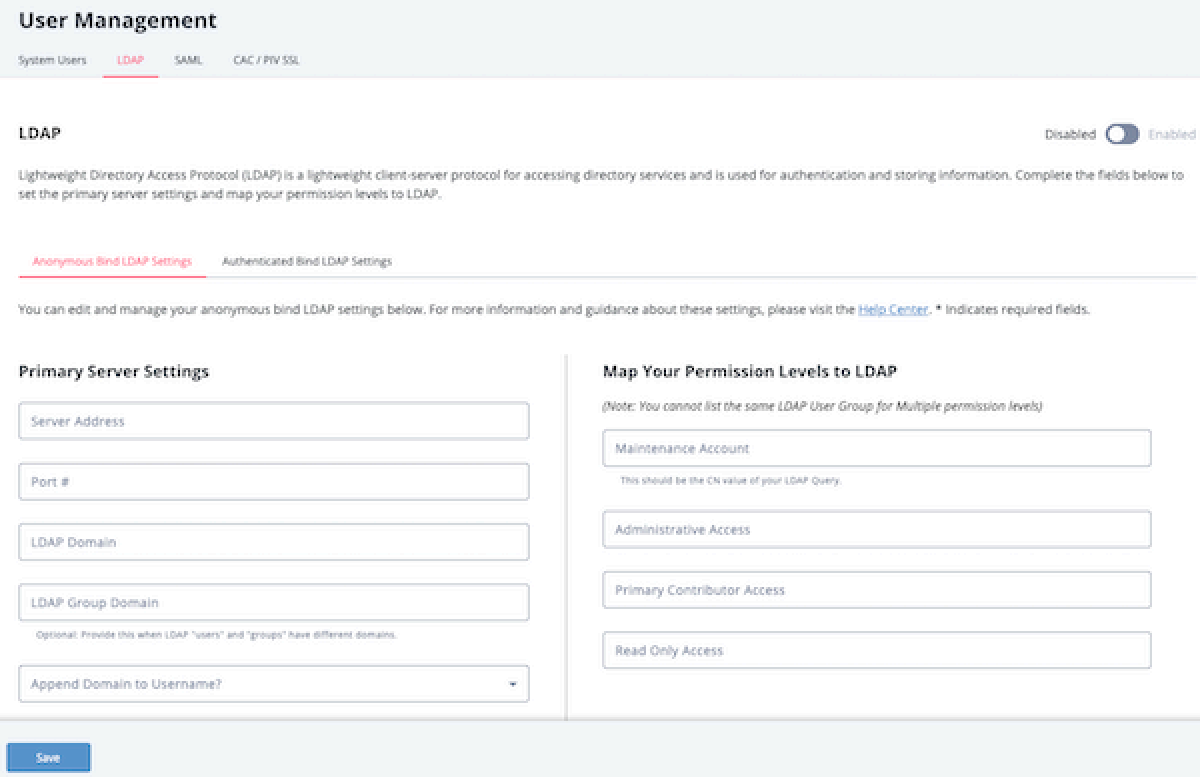
Anonymous Bind

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.

1. Navigate to Settings ⚙ > User Management.
2. Click on the **LDAP** option.

   The Anonymous Bind LDAP Settings form will load by default.



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.

You can edit and manage your anonymous bind LDAP settings below. For more information and guidance about these settings, please visit the Help Center. * Indicates required fields.

(Note: You cannot list the same LDAP User Group for Multiple permission levels)

This should be the CN value of your LDAP Query.

Optional: Provide this when LDAP "users" and "groups" have different domains.

3. Populate the fields in the **Primary Server Settings** section:

FIELD	DESCRIPTION
Server Address	Enter the name of the server where LDAP is hosted. **Example:** ldap://[servername]

FIELD	DESCRIPTION
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
LDAP Group Domain	
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
Use RDN?	Choose from the following options: ◦ Yes to use Relative Distinguished Names. When you select this option, the Organization Unit (OU) and User Lookup Name fields are displayed. ◦ No to use full Distinguished Names

FIELD	DESCRIPTION
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 cannot 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
Primary Contributor Access	**OpenLDAP Example:** ldapAnalyst **AD Example:** CN=primary_contributor,CN=Builtin,DC=yourdomain,DC=com
Read Only Access	**OpenLDAP Example:** ldapObserver **AD Example:** CN=read_onlyCN=Builtin,DC=yourdomain,DC=com

5. Click **Save**.
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

The following instructions are 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 Anonymous Bind steps above 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.

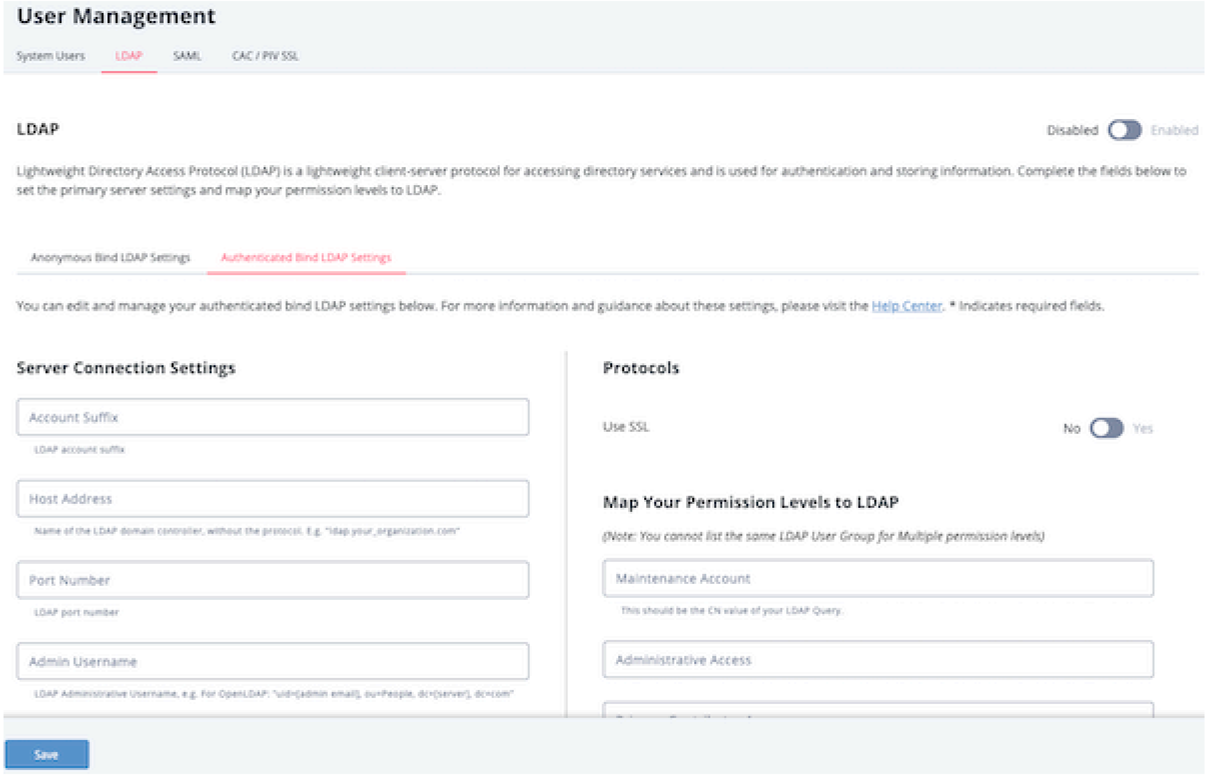
If your LDAP fails to enable or fails to function properly, validate your inputs. If the configuration continues to fail, please contact ThreatQ Support.

Authenticated Bind

⚠ 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.

1. Navigate to Settings ⚙ > User Management.
2. Click on the **LDAP** option and select the **Authenticated Bind LDAP Settings** tab.



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.

You can edit and manage your authenticated bind LDAP settings below. For more information and guidance about these settings, please visit the Help Center. * Indicates required fields.

LDAP account suffix

Name of the LDAP domain controller, without the protocol. E.g. "ldap.your_organization.com"

LDAP port number

LDAP Administrative Username, e.g. For OpenLDAP: "uid={admin email}, ou=People, dc={server}, dc=com"

(Note: You cannot list the same LDAP User Group for Multiple permission levels)

This should be the CN value of your LDAP Query.

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

FIELD	DESCRIPTION
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. This field should be **DN** for both OpenLDAP and Active Directory.
User Search Filter	The field to search for users. For **OpenLDAP**: objectClass=poslxAccount For **Active Directory**: objectClass=user
Group Search Filter	The field to search for grpups. For **OpenLDAP**: objectClass=poslxGroup For **Active Directory**: objectClass=group
Primary Group Name	The primary group name.

FIELD	DESCRIPTION
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 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 **Save**.
10. Click 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 Accessing the Platform topic.

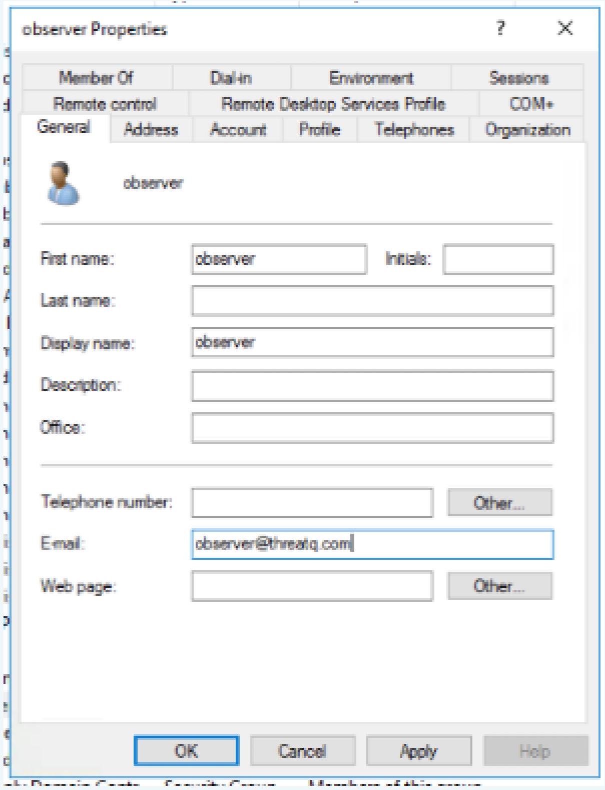
> Users cannot use SSO to log into a ThreatQ Local Maintenance account.

> ⚠ **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.

Configuring SAML

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

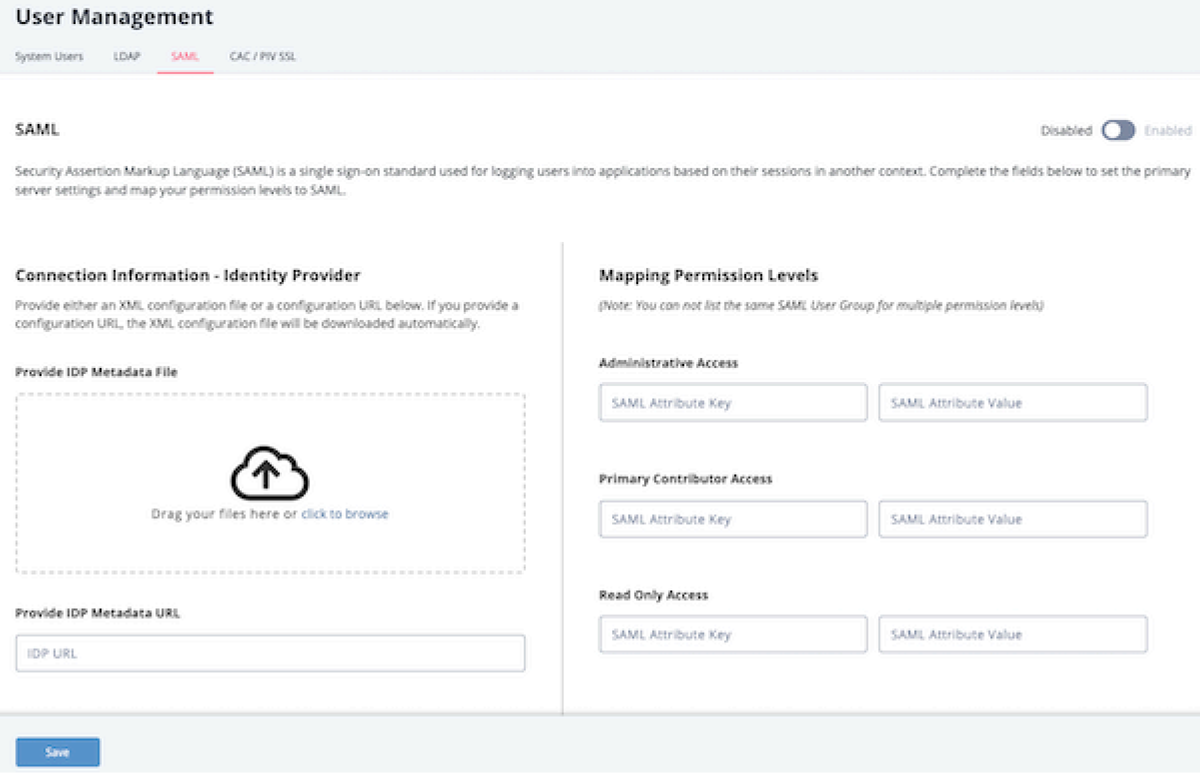
> SAML users are required to add their email address to their user profiles in order to use the SSO. As part of the integration process, the ThreatQ platform expects that the user's email address has already been added to their IdP. See the Setting Up LDAP

> Users/Groups for SAML topic for more details.
>
> 
>
> observer Properties
>
> First name: observer
>
> Display name: observer
>
> E-mail: observer@threatq.com
>
>

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 ⚙ > User Management.
2. From the User Management page, click the **SAML** tab.

The SAML configuration page opens.



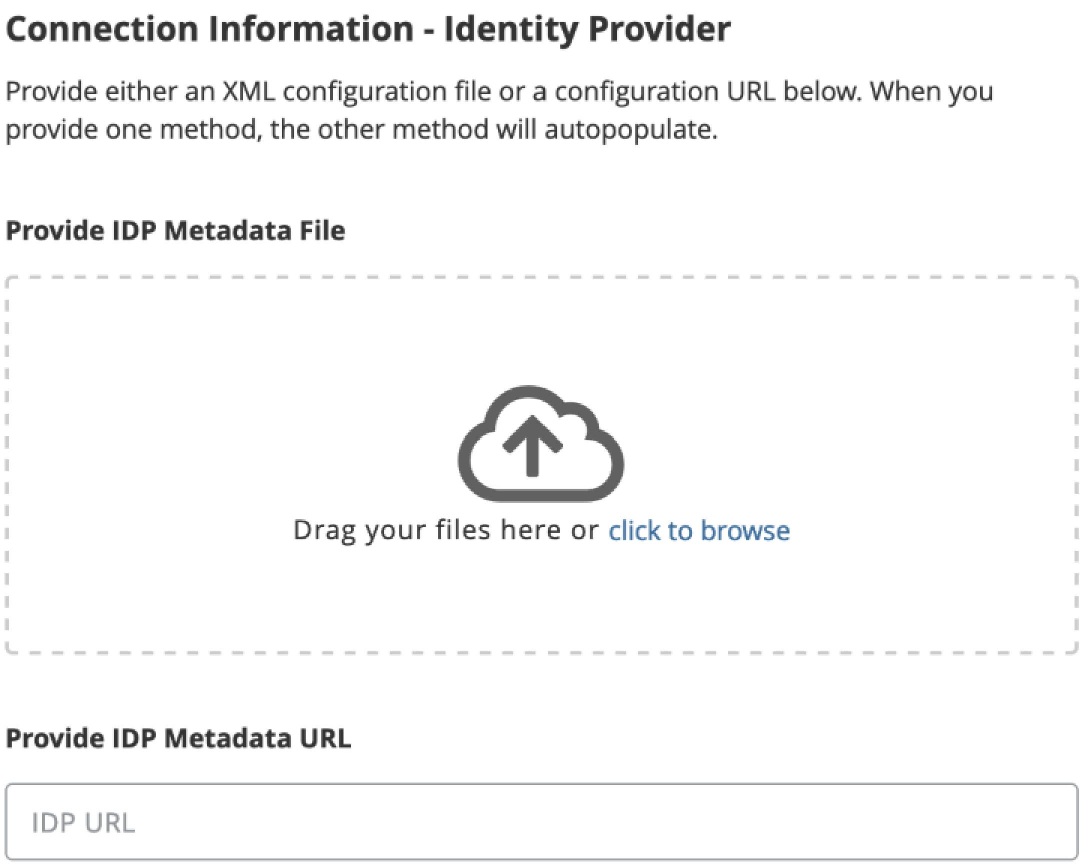
Security Assertion Markup Language (SAML) is a single sign-on standard used for logging users into applications based on their sessions in another context. Complete the fields below to set the primary server settings and map your permission levels to SAML.

Provide either an XML configuration file or a configuration URL below. If you provide a configuration URL, the XML configuration file will be downloaded automatically.

(Note: You can not list the same SAML User Group for multiple permission levels)

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.



Connection Information - Identity Provider

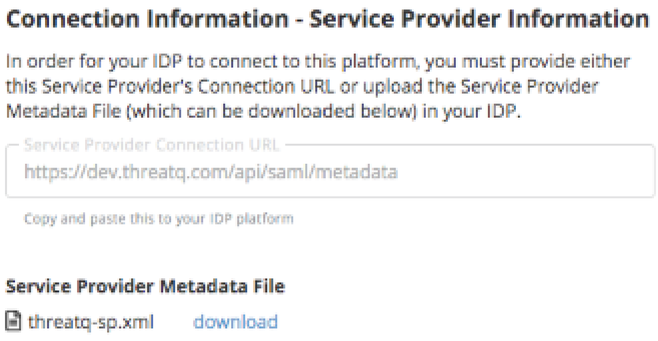
Provide either an XML configuration file or a configuration URL below. When you provide one method, the other method will autopopulate.

Provide IDP Metadata File

Provide IDP Metadata URL

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 topic.



Connection Information - Service Provider Information

In order for your IDP to connect to this platform, you must provide either this Service Provider's Connection URL or upload the Service Provider Metadata File (which can be downloaded below) in your IDP.

Service Provider Connection URL: https://dev.threatq.com/api/saml/metadata

Copy and paste this to your IDP platform

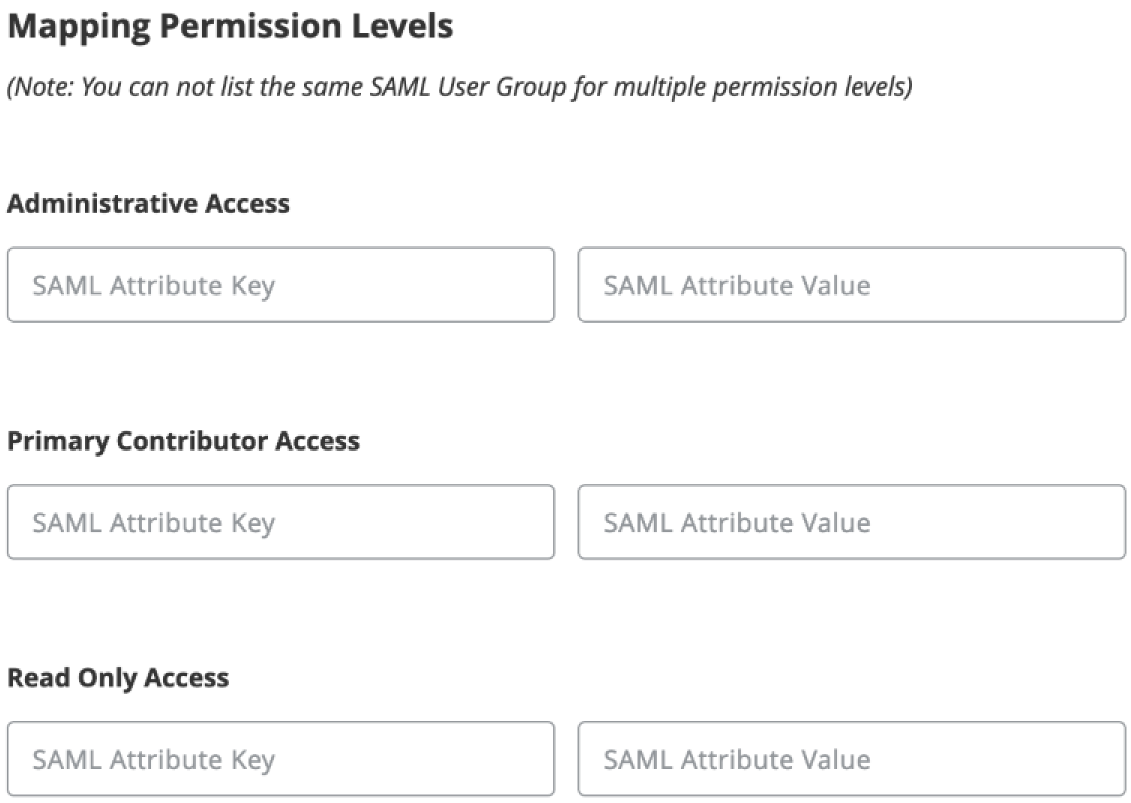
Service Provider Metadata File

threatq-sp.xml

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 Permission Levels

(Note: You can not list the same SAML User Group for multiple permission levels)

Administrative Access

SAML Attribute Key | SAML Attribute Value

Primary Contributor Access

SAML Attribute Key | SAML Attribute Value

Read Only Access

SAML Attribute Key | SAML Attribute Value

Mapping Notes:

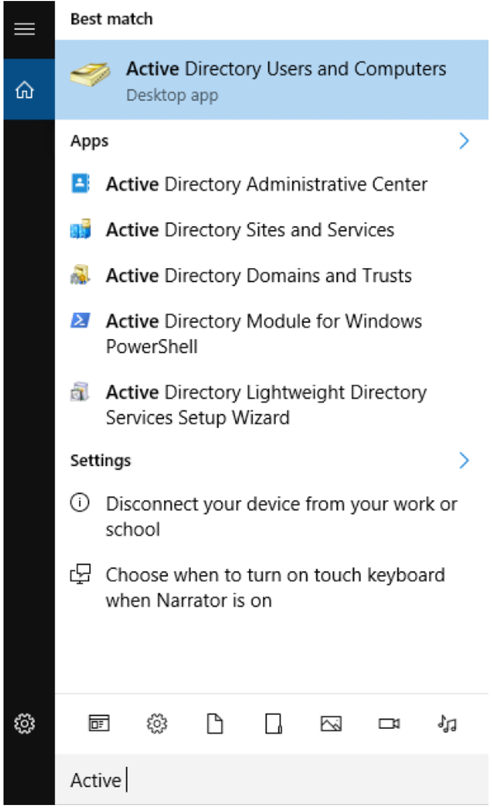
- SAML cannot be used for Maintenance Accounts.
    - Local Maintenance Accounts cannot be mapped when enabling SAML.
    - If converting from LDAP authentication, LDAP groups that were mapped to the ThreatQ Maintenance role will have to be mapped to another user role.

    - 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.

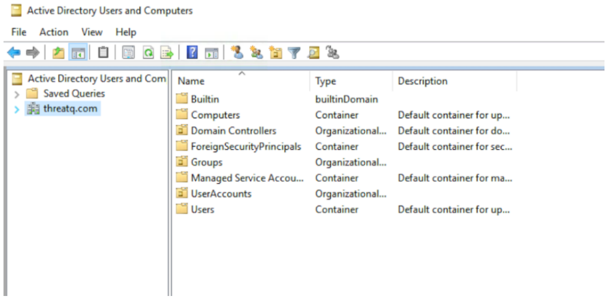
Setting Up LDAP Users/Groups for SAML

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.

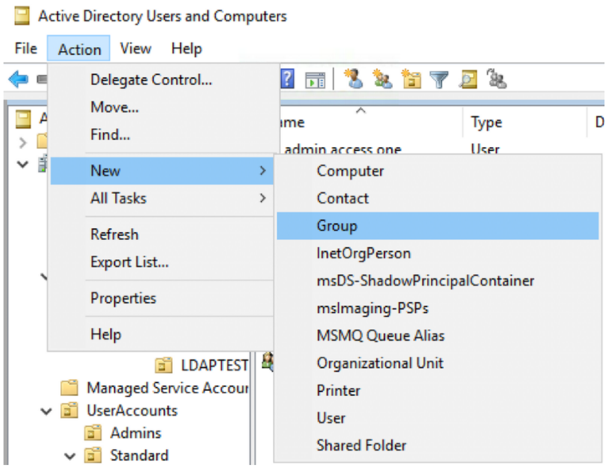

Best match
Active Directory Users and Computers
Desktop app
Apps
Active Directory Administrative Center
Active Directory Sites and Services
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Lightweight Directory Services Setup Wizard
Settings
Disconnect your device from your work or school
Choose when to turn on touch keyboard when Narrator is on
Active

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

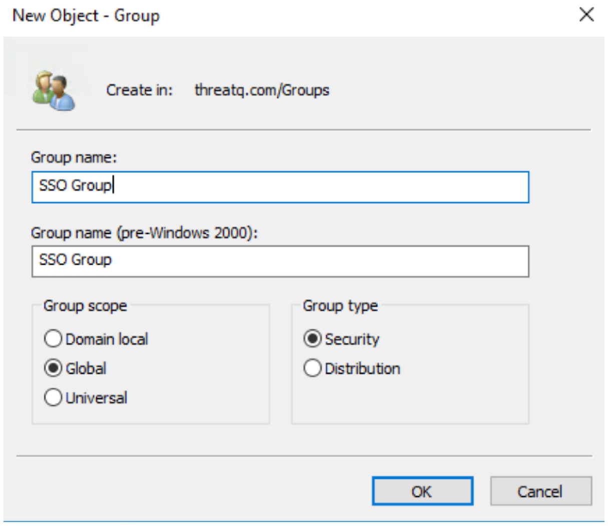

Active Directory Users and Computers
File
Action
View
Help
Active Directory Users and Com
Saved Queries
threatq.com

Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default container for up...
Domain Controllers	Organizational...	Default container for do...
ForeignSecurityPrincipals	Container	Default container for sec...
Groups	Organizational...	
Managed Service Accou...	Container	Default container for ma...
UserAccounts	Organizational...	
Users	Container	Default container for up...

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



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



Create in: threatq.com/Groups

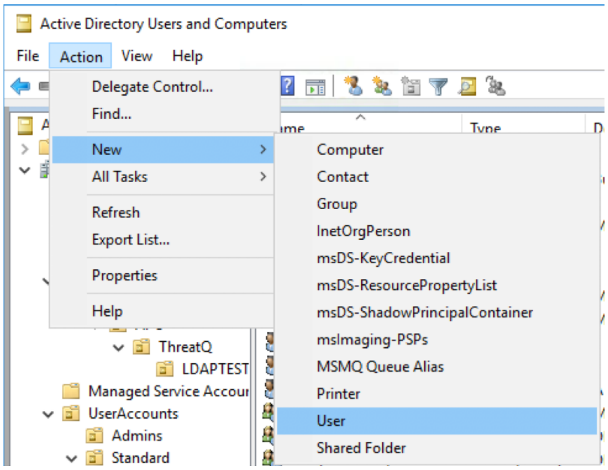
Group name: SSO Group

Group name (pre-Windows 2000): SSO Group

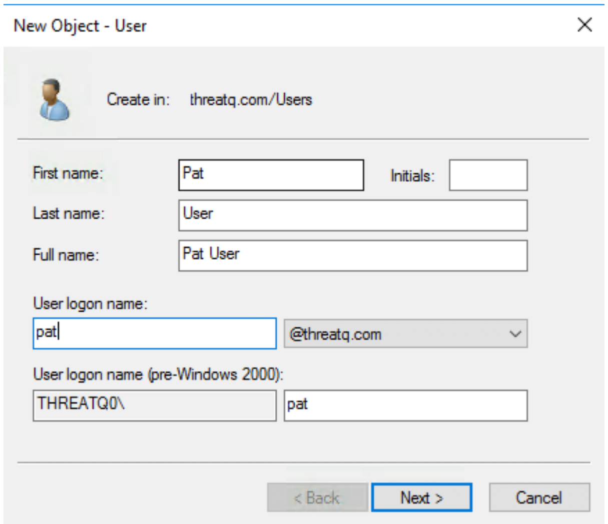
Group scope
○ Domain local
● Global
○ Universal

Group type
● Security
○ Distribution

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



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

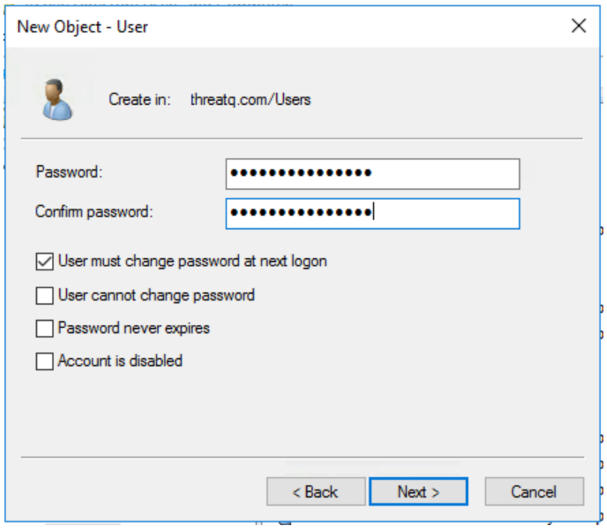


New Object - User

Create in: threatq.com/Users

First name: Pat
Initials:
Last name: User
Full name: Pat User
User logon name: pat @threatq.com
User logon name (pre-Windows 2000): THREATQ0\ pat

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



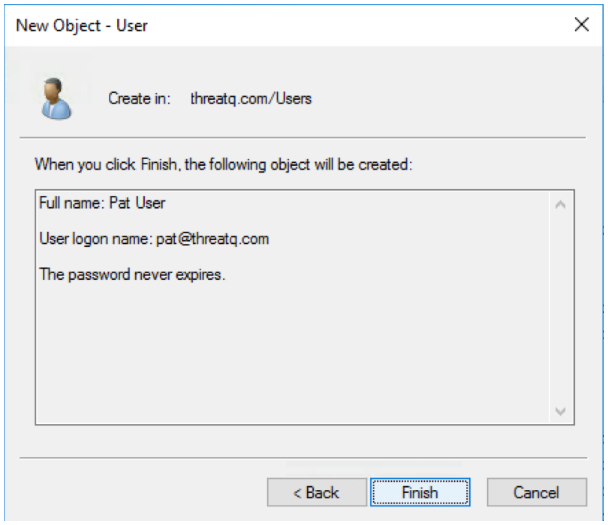
New Object - User

Create in: threatq.com/Users

Password: •••••••••••••••
Confirm password: •••••••••••••••

☑ User must change password at next logon
☐ User cannot change password
☐ Password never expires
☐ Account is disabled

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



New Object - User

Create in: threatq.com/Users

When you click Finish, the following object will be created:

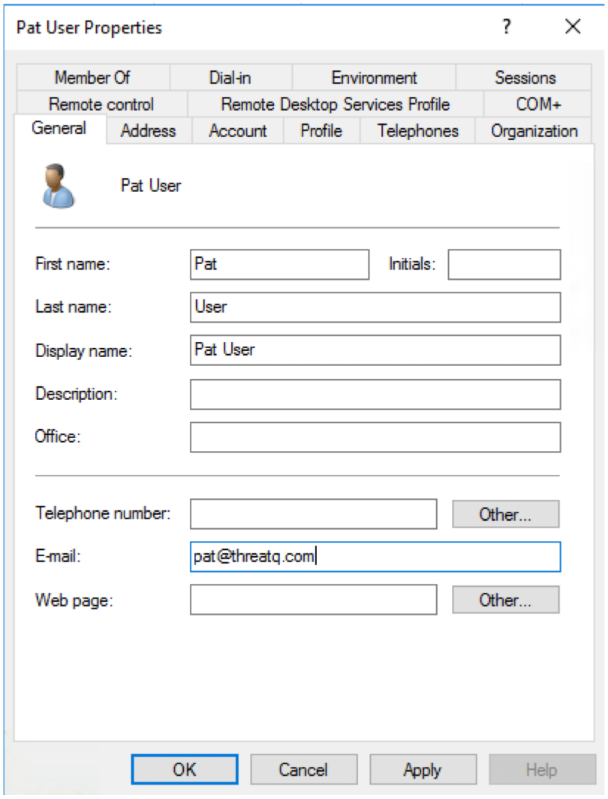
Full name: Pat User

User logon name: pat@threatq.com

The password never expires.

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.



First name: Pat

Initials:

Last name: User

Display name: Pat User

Description:

Office:

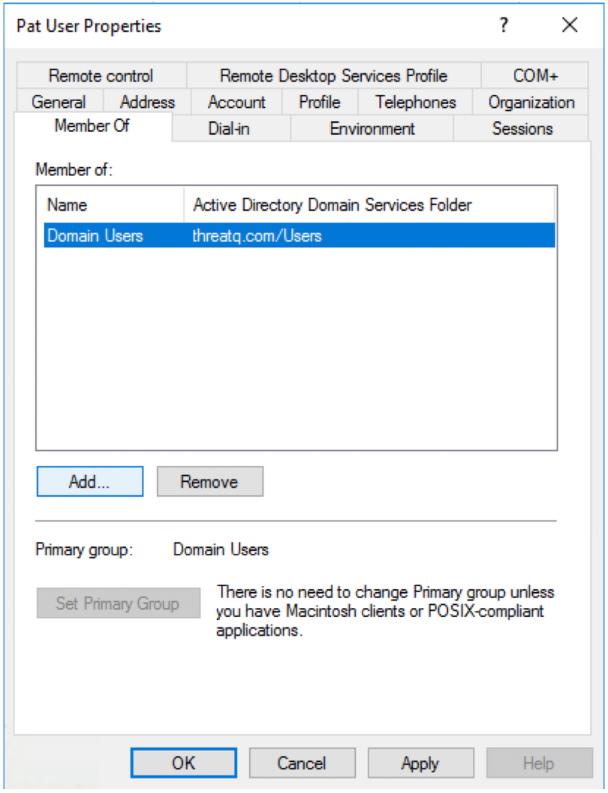
Telephone number:

E-mail: pat@threatq.com

Web page:

> ⚠ 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**.



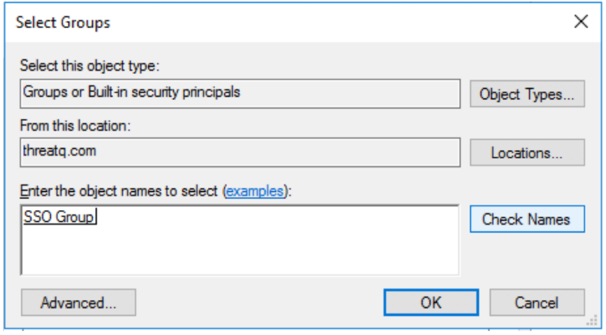
Member of:

Name	Active Directory Domain Services Folder
Domain Users	threatq.com/Users

Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

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



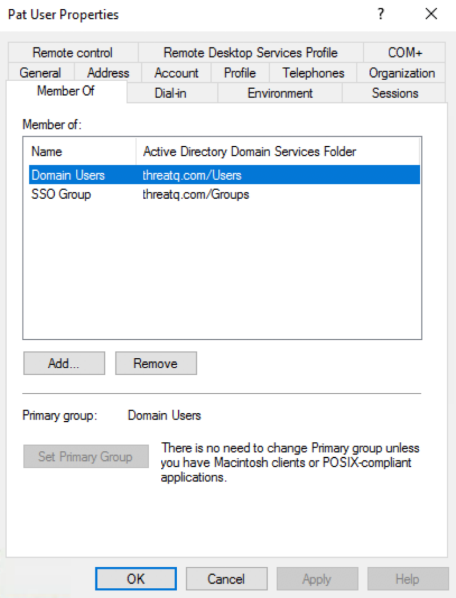
Select this object type: Groups or Built-in security principals

From this location: threatq.com

Enter the object names to select (examples): SSO Group

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.



Member of:

Name	Active Directory Domain Services Folder
Domain Users	threatq.com/Users
SSO Group	threatq.com/Groups

Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

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

Adding ThreatQ as a Service Provider

ThreatQ supports SAML configurations for all identity providers that are compliant with the Security Assertion Markup Language v2.

The sections listed in this topic serve as identity provider examples and include the required steps to add ThreatQ as a service provider for your IdP. Contact ThreatQ Support if your identity provider is not listed and you require assistance with configuration.

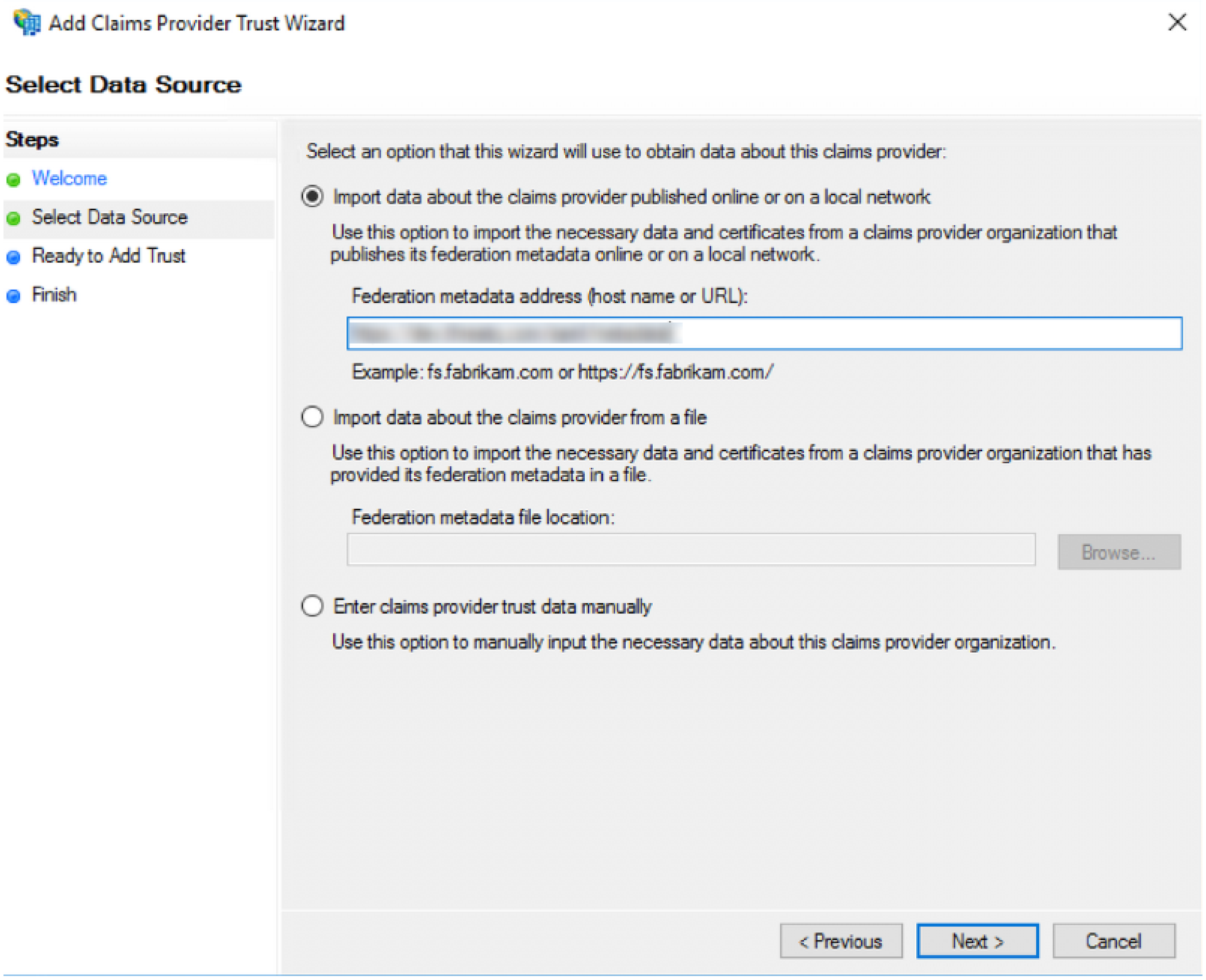
ADFS 2016

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.



Add Claims Provider Trust Wizard

Select Data Source

Select an option that this wizard will use to obtain data about this claims provider:

● Import data about the claims provider published online or on a local network

Use this option to import the necessary data and certificates from a claims provider organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

[redacted]

Example: fs.fabrikam.com or https://fs.fabrikam.com/

○ Import data about the claims provider from a file

Use this option to import the necessary data and certificates from a claims provider organization that has provided its federation metadata in a file.

Federation metadata file location:

○ Enter claims provider trust data manually

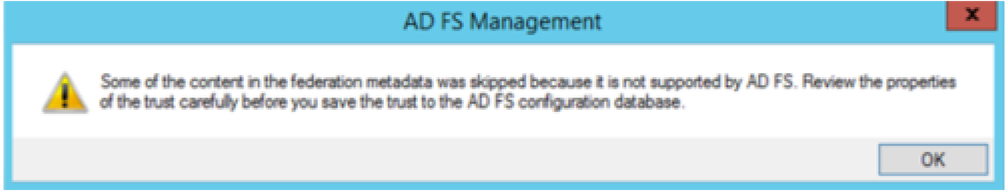
Use this option to manually input the necessary data about this claims provider organization.

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 IdP hostname>/FederationMetadata/2007-06/FederationMetadata.xml
```

8. Click **Next**.

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



AD FS Management

Some of the content in the federation metadata was skipped because it is not supported by AD FS. Review the properties of the trust carefully before you save the trust to the AD FS configuration database.

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	NOTES
E-Mail-Addresses	email	
Email-Addresses	uid	Email-Addresses is the recommended value. However, you can use SAM-Account-Name as an alternative.

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

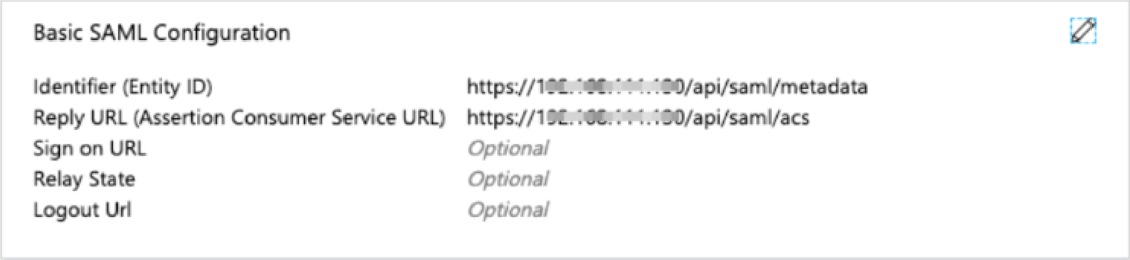
35. Select the **Pass through all claim value** radio option.
36. Click on **OK** to create the rule.
37. Click **OK** to close the Issuance Transform Rules dialog box.

Azure AD

ThreatQ supports SP-Initiated SSO in Azure AD. 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 into the Azure portal with administrator permissions.
2. Go to **Azure Active Directory > Enterprise applications**
3. Click on **+New Application** then **Create your own application.**
4. Choose **Integrate any other application you don't find in the gallery (Non-gallery)**.
5. Enter an application name such as **ThreatQ** then click **Add**.
6. Select **Set up single sign on** then choose **SAML**.
7. Select Edit on **Basic SAML Configuration**.
8. Enter the **Entity ID** and **Reply URL(Assertion Consumer Service URL)** as follows:



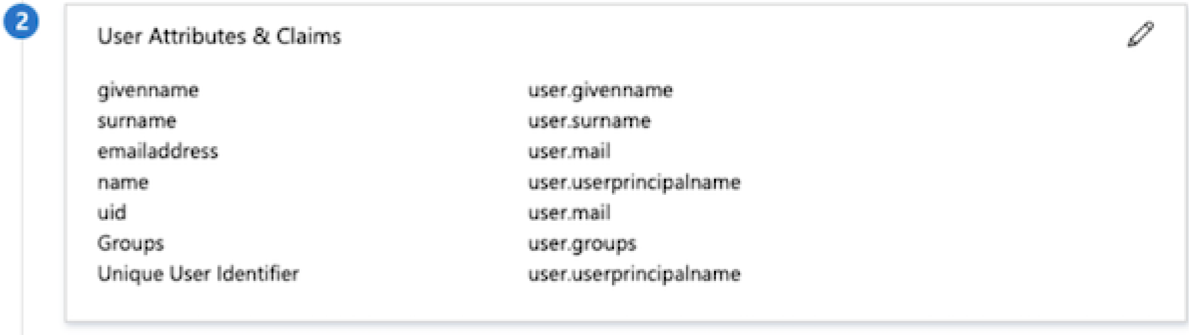
Basic SAML Configuration

Identifier (Entity ID)	https://1[redacted]0/api/saml/metadata
Reply URL (Assertion Consumer Service URL)	https://1[redacted]0/api/saml/acs
Sign on URL	*Optional*
Relay State	*Optional*
Logout Url	*Optional*

FIELD	VALUE	DESCRIPTION
ACS / Single Sign on URL	https://threatq.example.com/api/saml/acs	Assertion Consumer Service (ACS) is the ThreatQ URL + appended the "/api/saml/acs" string.
SP Entity ID	https://threatq.example.com/api/saml/metadata	This is the ThreatQ entity ID which is the ThreatQ URL + appended with the "/api/saml/metadata" string.

9. Under **Attributes & Claims**, set the **Unique User identifier (Name ID) format** to **Email Address**.
10. 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.

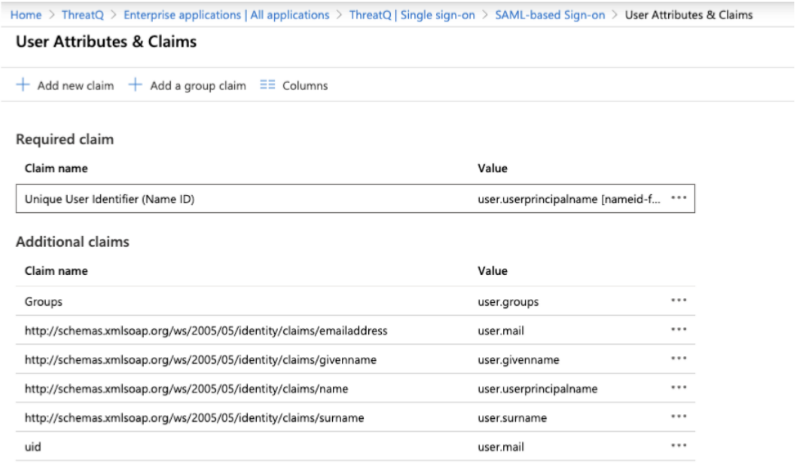


2

User Attributes & Claims

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
uid	user.mail
Groups	user.groups
Unique User Identifier	user.userprincipalname

11. 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.



Home > ThreatQ > Enterprise applications | All applications > ThreatQ | Single sign-on > SAML-based Sign-on > User Attributes & Claims
+ Add new claim
+ Add a group claim
Columns

User Attributes & Claims

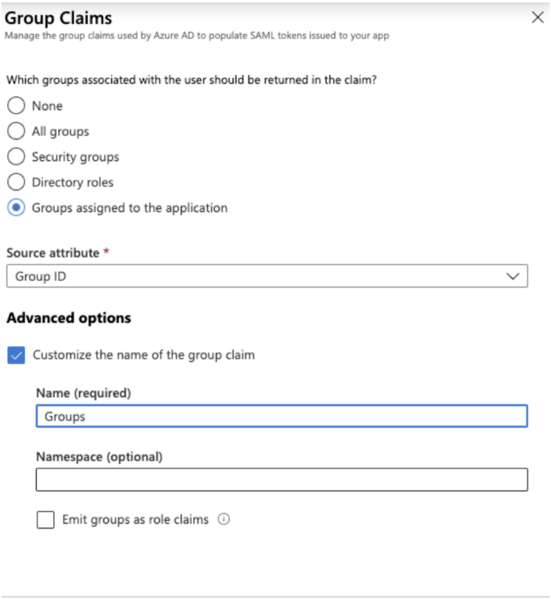
Required claim

Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [nameid-f...

Additional claims

Claim name	Value
Groups	user.groups
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname
uid	user.mail

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 information. See the example below:



Group Claims

Manage the group claims used by Azure AD to populate SAML tokens issued to your app

Which groups associated with the user should be returned in the claim?

○ None
○ All groups
○ Security groups
○ Directory roles
● Groups assigned to the application

Source attribute *
Group ID

Advanced options

☑ Customize the name of the group claim

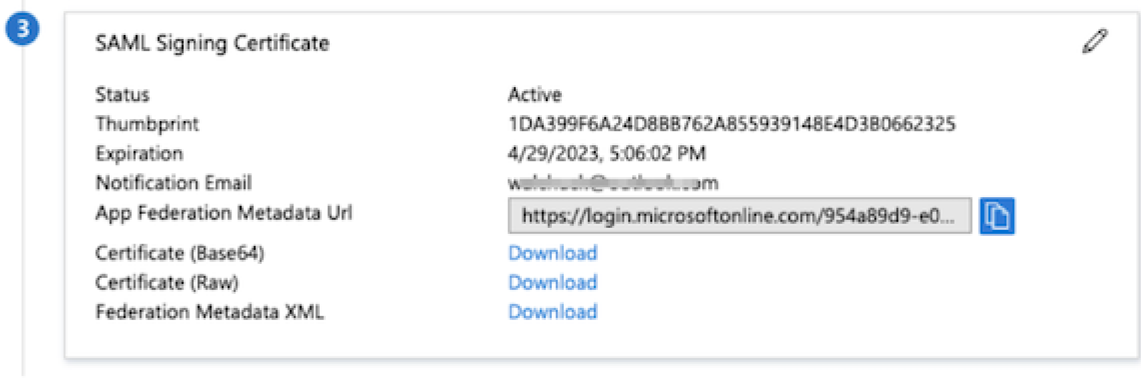
Name (required)
Groups

Namespace (optional)

☐ Emit groups as role claims

> In the example above, **Groups** would be entered as the Attribute Key in ThreatQ. The Attribute Value would be one of the Group IDs (Group Object ID) assigned to the application in Step 9.

12. On the Assignments tab, verify that each of the users or groups that should have access have been assigned to the application.
13. 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.

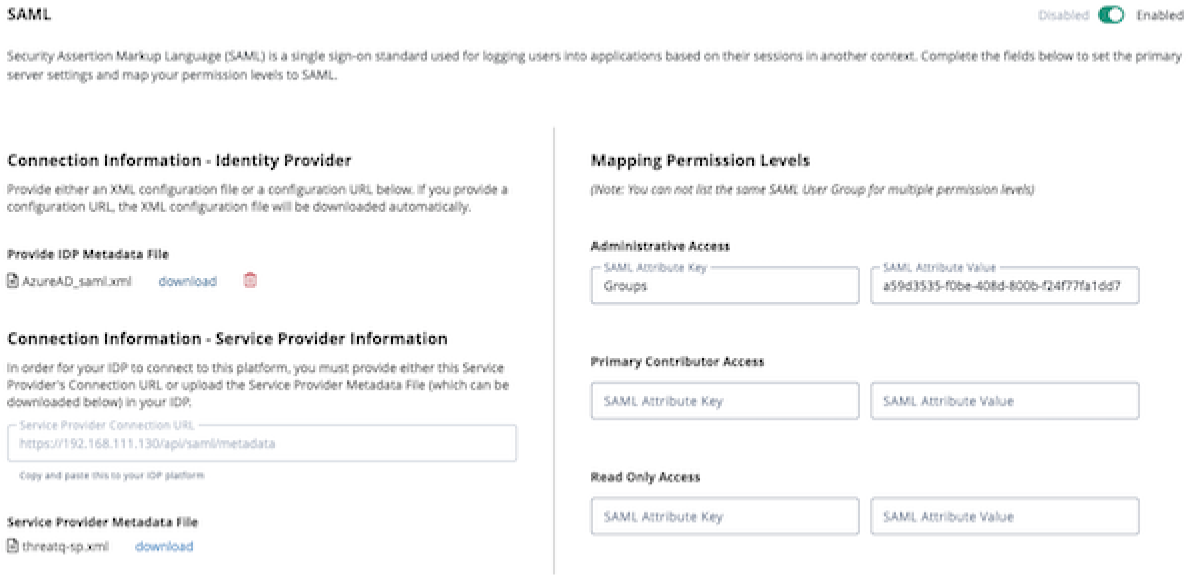


SAML Signing Certificate

Status	Active
Thumbprint	1DA399F6A24D8BB762A855939148E4D3B0662325
Expiration	4/29/2023, 5:06:02 PM
Notification Email	[redacted]
App Federation Metadata Url	https://login.microsoftonline.com/954a89d9-e0...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

14. After you complete the Configuring SAML process, add the SAML Attribute Key and SAML Attribute Value for each ThreatQ user role to the Mapping Permissions section.
    In the example below, we mapped an Azure AD Group to the Administrative Access using

the group’s Object ID as the SAML attribute value.



SAML

Disabled Enabled

Security Assertion Markup Language (SAML) is a single sign-on standard used for logging users into applications based on their sessions in another context. Complete the fields below to set the primary server settings and map your permission levels to SAML.

Connection Information - Identity Provider

Provide either an XML configuration file or a configuration URL below. If you provide a configuration URL, the XML configuration file will be downloaded automatically.

Provide IDP Metadata File

AzureAD_saml.xml download

Connection Information - Service Provider Information

In order for your IDP to connect to this platform, you must provide either this Service Provider's Connection URL or upload the Service Provider Metadata File (which can be downloaded below) in your IDP.

Service Provider Connection URL: https://192.168.111.130/api/saml/metadata

Copy and paste this to your IDP platform

Service Provider Metadata File

threatq-sp.xml download

Mapping Permission Levels

(Note: You can not list the same SAML User Group for multiple permission levels)

Administrative Access

SAML Attribute Key: Groups

SAML Attribute Value: a59d3535-f0be-408d-800b-f24f77fa1dd7

Primary Contributor Access

SAML Attribute Key

SAML Attribute Value

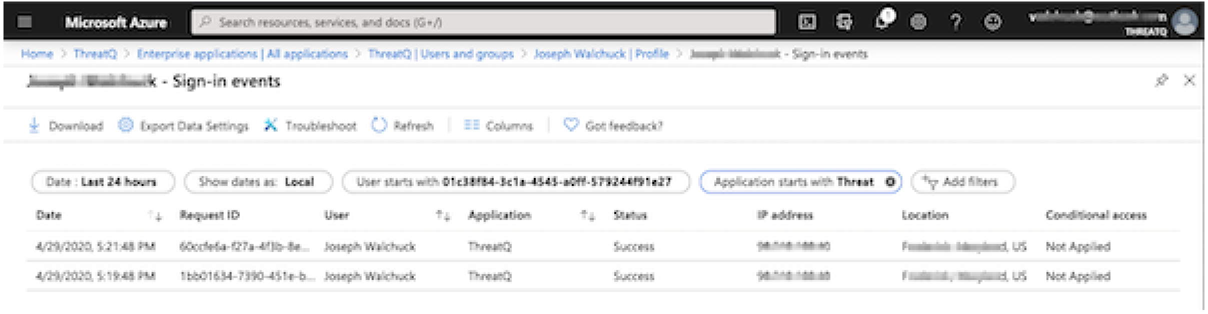
Read Only Access

SAML Attribute Key

SAML Attribute Value

> When you test the application from the Azure Portal, you will receive the following error message: `SAML authenticated but missing Client ID parameter`. This happens because we do not yet support IdP-initiated SSO. You must validate the authentication from the ThreatQ application.

15. In the Azure Portal, you can navigate to the User Sign-Ins under the user to view the login attempts.
    If your authentication is successful but you receive a `SAML authenticated but missing group requirements message` this indicates that the required attributes mapped to the TQ roles are not configured correctly.



Home > ThreatQ > Enterprise applications | All applications > ThreatQ | Users and groups > Joseph Walchuck | Profile > [redacted] - Sign-in events

[redacted]k - Sign-in events

Date : Last 24 hours | Show dates as: Local | User starts with 01c38f84-3c1a-4545-a0ff-579244f91e27 | Application starts with Threat | Add filters

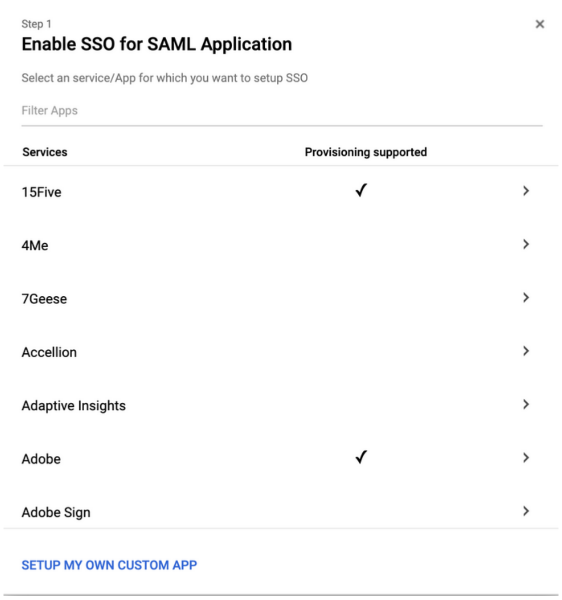
Date	Request ID	User	Application	Status	IP address	Location	Conditional access
4/29/2020, 5:21:48 PM	60ccfe6a-f27a-4f3b-8e...	Joseph Walchuck	ThreatQ	Success	[redacted]	[redacted], US	Not Applied
4/29/2020, 5:19:48 PM	1bb01634-7390-451e-b...	Joseph Walchuck	ThreatQ	Success	[redacted]	[redacted], US	Not Applied

Google G Suite

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.



Step 1

Enable SSO for SAML Application

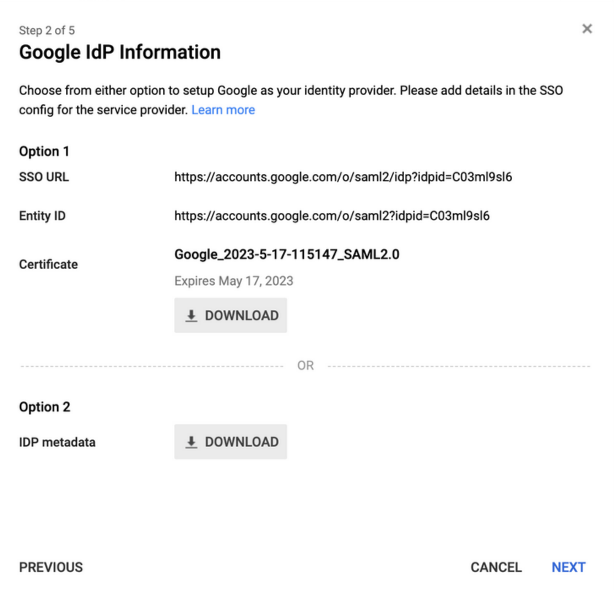
Select an service/App for which you want to setup SSO

Filter Apps

Services	Provisioning supported
15Five	✓
4Me	
7Geese	
Accellion	
Adaptive Insights	
Adobe	✓
Adobe Sign	

SETUP MY OWN CUSTOM APP

The Google IdP information page loads.



Step 2 of 5

Google IdP Information

Choose from either option to setup Google as your identity provider. Please add details in the SSO config for the service provider. Learn more

Option 1

SSO URL https://accounts.google.com/o/saml2/idp?idpid=C03ml9sl6

Entity ID https://accounts.google.com/o/saml2?idpid=C03ml9sl6

Certificate Google_2023-5-17-115147_SAML2.0

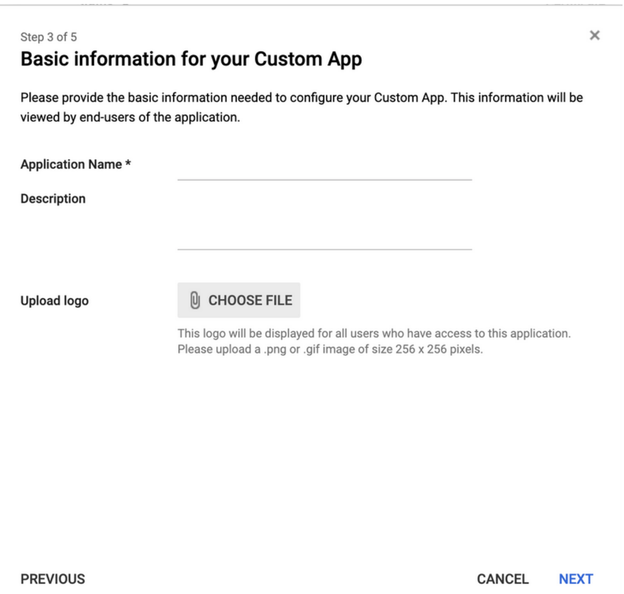
Expires May 17, 2023

Option 2

IDP metadata

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



Step 3 of 5

Basic information for your Custom App

Please provide the basic information needed to configure your Custom App. This information will be viewed by end-users of the application.

Application Name *

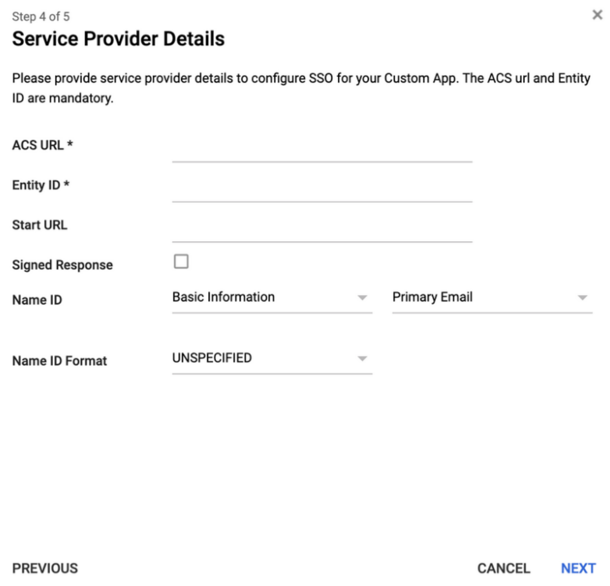
Description

Upload logo

This logo will be displayed for all users who have access to this application. Please upload a .png or .gif image of size 256 x 256 pixels.

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 “/api/saml/metadata” string.	https://threatq.example.com/api/saml/metadata
Name ID Format	Set this field to **Email**.	N/A



Step 4 of 5

Service Provider Details

Please provide service provider details to configure SSO for your Custom App. The ACS url and Entity ID are mandatory.

ACS URL *

Entity ID *

Start URL

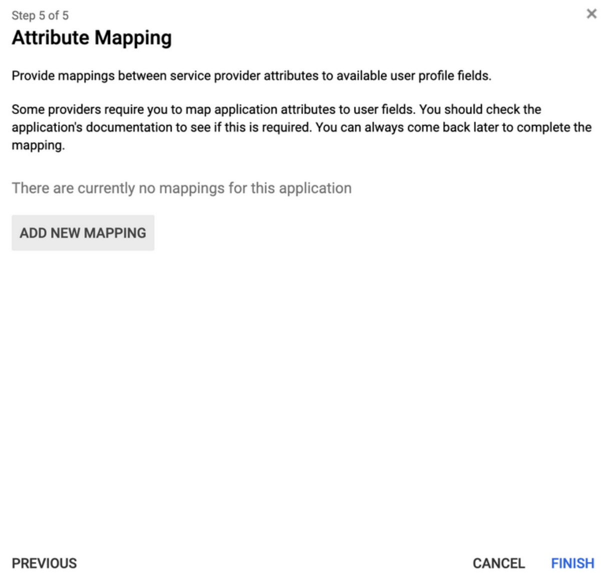
Signed Response ☐

Name ID: Basic Information | Primary Email

Name ID Format: UNSPECIFIED

9. Click on **Next**.

   The Attribute Mapping page loads.



Step 5 of 5

Attribute Mapping

Provide mappings between service provider attributes to available user profile fields.

Some providers require you to map application attributes to user fields. You should check the application's documentation to see if this is required. You can always come back later to complete the mapping.

There are currently no mappings for this application

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:

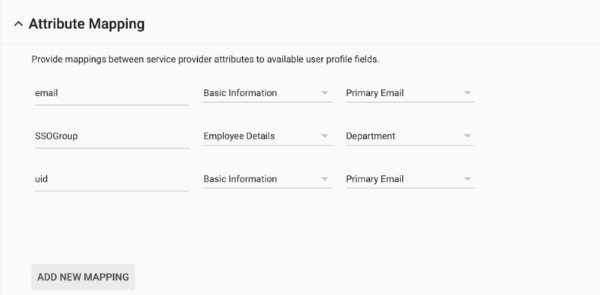
ATTRIBUTE	TYPE	GOOGLE DATA FIELD
uid	Basic Information	Primary Email

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:



Attribute Mapping

Provide mappings between service provider attributes to available user profile fields.

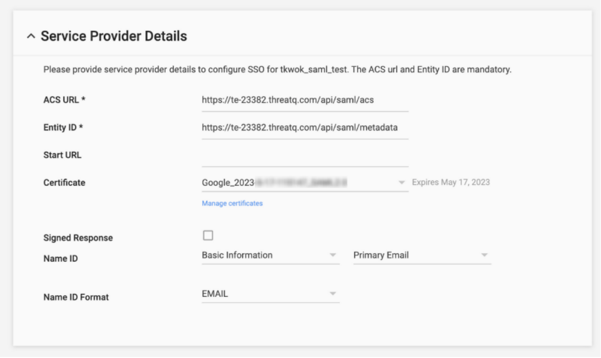
email | Basic Information | Primary Email

SSOGroup | Employee Details | Department

uid | Basic Information | Primary Email

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.



Service Provider Details

Please provide service provider details to configure SSO for tkwok_saml_test. The ACS url and Entity ID are mandatory.

ACS URL * https://te-23382.threatq.com/api/saml/acs

Entity ID * https://te-23382.threatq.com/api/saml/metadata

Start URL

Certificate Google_2023[redacted] Expires May 17, 2023

Signed Response ☐

Name ID Basic Information Primary Email

Name ID Format EMAIL

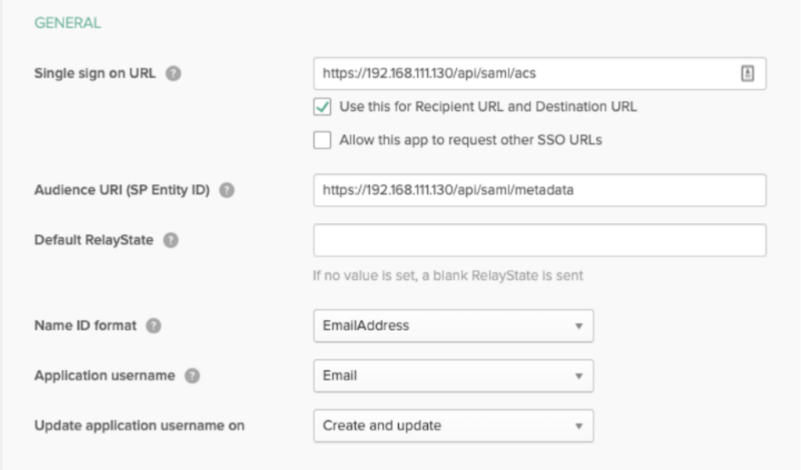
21. Click on **Manage Certificates**.
22. Download the **certificate** and the **IdP Metadata** files that are required in steps 4 and 5 in the *Configuring SAML* section in the SAML Authentication topic.

Okta

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**.
5. The Add Applications page loads.
6. Click on **Create New App**. The Create New Application dialog box opens.
7. Select **Web** from the Platform dropdown.
8. Select **SAML 2.0** for the Sign on method.
9. Click on the **Create** button. The Create SAML Integration page opens with the General Settings tab selected.
10. Enter a name for the app in the **App Name** field.
11. Click on **Next**. The Configure SAML section loads.

12. Complete the following fields:



GENERAL

Single sign on URL: https://192.168.111.130/api/saml/acs

☑ Use this for Recipient URL and Destination URL

☐ Allow this app to request other SSO URLs

Audience URI (SP Entity ID): https://192.168.111.130/api/saml/metadata

Default RelayState:

If no value is set, a blank RelayState is sent

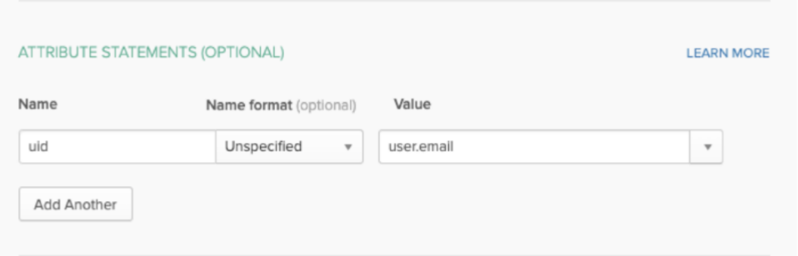
Name ID format: EmailAddress

Application username: Email

Update application username on: Create and update

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 "/api/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.
Name ID format	EmailAddress	
Application username	Email	ThreatQ requires that this field be set to Email.

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

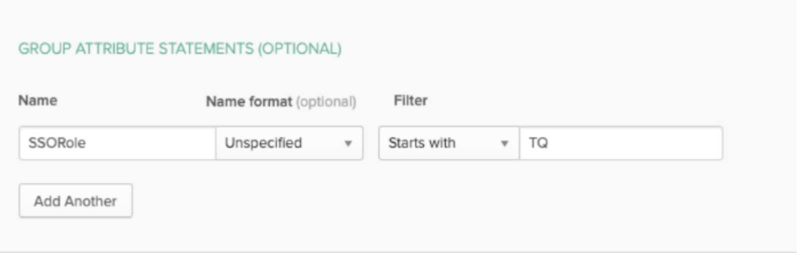


ATTRIBUTE STATEMENTS (OPTIONAL)

Name	Name format (optional)	Value
uid	Unspecified	user.email

NAME	NAME FORMAT	VALUE
uid	Unspecified	user.email

14. 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**.



GROUP ATTRIBUTE STATEMENTS (OPTIONAL)

Name: SSORole
Name format (optional): Unspecified
Filter: Starts with TQ

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

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

    The Feedback section loads.

17. 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.

18. Click on the **Assignments** tab.
19. Click on the **Assign** dropdown and select **Assign to Groups**.
20. Assign the app to groups that will be used to map ThreatQ roles.
21. Click on **Save and Go Back**.
22. Click on **Done**.
23. Click on the **Sign On** tab.
24. In the **Sign On Methods** section, right-click and download the **Identity Provider metadata** file.
25. 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**.

26. 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 section of the SAML Authentication topic.

SSL Client Certificate Authentication

ThreatQ supports SSL Client Certificate Authentication by allowing on-premise customers to upload PEM-encoded CA certificate files. After this file is uploaded and configured, individual ThreatQ logins can be associated with a user's certificate SHA-1 fingerprint. This allows users to authenticate and access ThreatQ via their:

- Common Access Cards (CACs)
- Personal Identity Verification (PIV) cards
- Smart cards
- SSL client certificates

⚠ If you want to migrate from LDAP or SAML authentication to SSL Client Certificate Authentication, please contact ThreatQ Support for assistance.

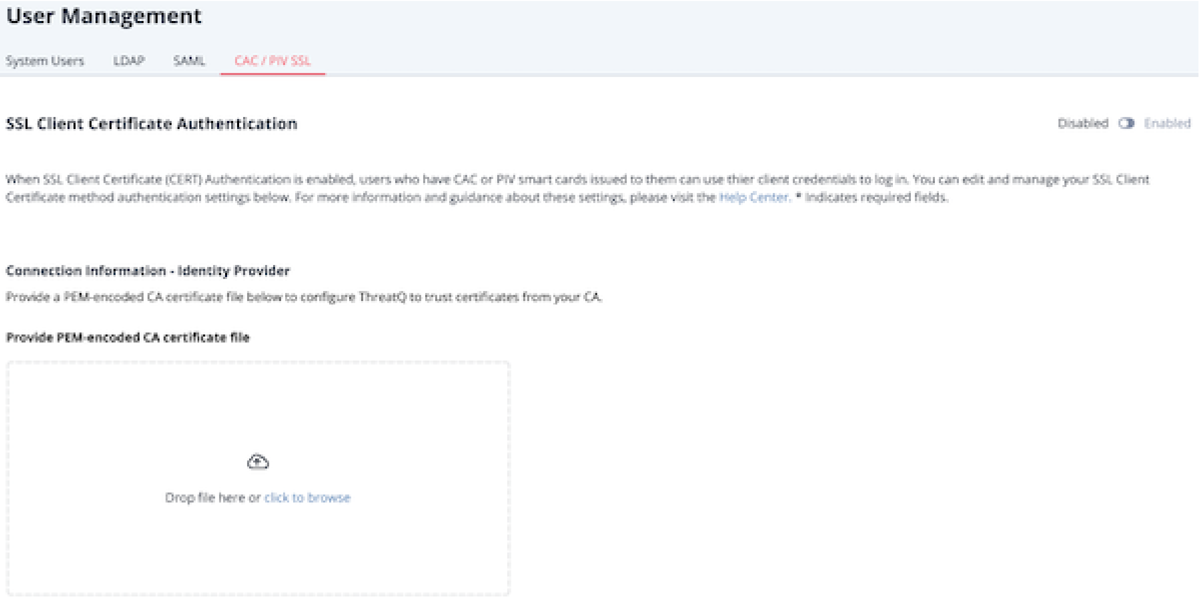
Requirements

- On-premise instance of the ThreatQ Platform 5.9 or greater.
- PEM-encoded, X.509 CA certificate file
- CAC, PIV card, Smart card, or SSL client certificate
- Administrative or maintenance login

Configuring Client Certificate Authentication

Only Administrative or Maintenance logins have access to the CAC/PIV SSL tab in the User Management page. This tab is used to configure SSL Client Certificate Authentication.

1. From the User Management page, click the CAC/PIV SSL tab.



SSL Client Certificate Authentication

When SSL Client Certificate (CERT) Authentication is enabled, users who have CAC or PIV smart cards issued to them can use thier client credentials to log in. You can edit and manage your SSL Client Certificate method authentication settings below. For more information and guidance about these settings, please visit the Help Center. * Indicates required fields.

Connection Information - Identity Provider

Provide a PEM-encoded CA certificate file below to configure ThreatQ to trust certificates from your CA.

Provide PEM-encoded CA certificate file

2. Upload the CA certificate file using one of the following methods:
   - Drag and drop the file into the dialog box.
   - Select the click to browse link to locate the file on your local machine.
3. After you upload the file:
   - The system displays the following message:
     ```
     Once enabled, CAC / PIV SSL Authentication will take effect for system users
     upon the next login.
     ```
   - The Disabled/Enabled toggle switches to Enabled.
   - The certificate's serial number and expiration date is displayed.

   > If SAML authentication is active on your ThreatQ instance, the Are you sure? window returns the following warning and prompts you to confirm your choice:
   >
   > ```
   > Currently you have SAML authentication enabled on your system. By
   > enabling CAC / PIV SSL authentication, SAML will become disabled
   > immediately. Upon next login, SAML users will no longer be able to
   > authenticate via that method. Would you like to proceed?
   > ```
   >
   > You must click the **Confirm** button to continue.

4. Now that SSL Client Certificate Authentication is enabled, use one of the following methods to add a certificate fingerprint to your profile.

   > Until you add a certificate fingerprint to your user profile, each time you access a new ThreatQ page you will be prompted to select a certificate.

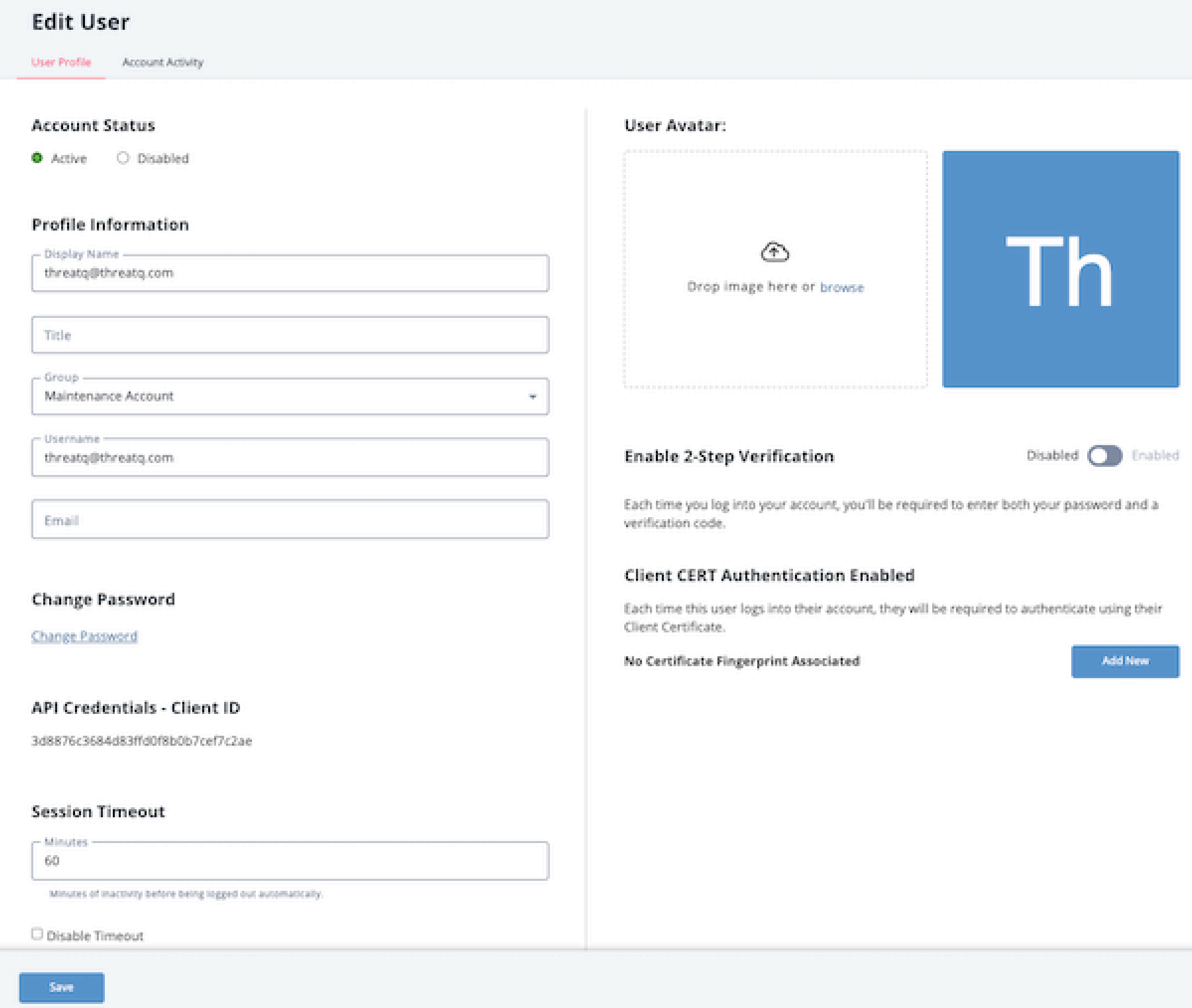
  - Log out of ThreatQ and add your certificate fingerprint during log in.
  - Use the System Users tab to add your certificate fingerprint to your user profile.
5. Use one of the following methods to add certificate fingerprints for users:
  - Users can add their own certificate fingerprint during their next login. If needed, you can set up usernames and passwords in the System Users tab on the User Management page.
  - Maintenance or Administrative users can use the System Users tab to add the new certificate fingerprint to user profiles.

Adding a User's Certificate Fingerprint - User Profile

After Client Certificate Authentication is enabled, an Administrative or Maintenance user can add a certificate fingerprint to a ThreatQ user profile.

1. From the User Management screen, click the User Management tab.
2. Locate and click the user's display name.

3. From the User Profile tab in the Edit User page, click the **Add New** button.



Account Status

● Active ○ Disabled

Profile Information

Display Name: threatq@threatq.com

Title

Group: Maintenance Account

Username: threatq@threatq.com

Email

Change Password

API Credentials - Client ID

3d8876c3684d83ffd0f8b0b7cef7c2ae

Session Timeout

Minutes: 60

Minutes of inactivity before being logged out automatically.

☐ Disable Timeout

User Avatar:

Enable 2-Step Verification

Each time you log into your account, you'll be required to enter both your password and a verification code.

Client CERT Authentication Enabled

Each time this user logs into their account, they will be required to authenticate using their Client Certificate.

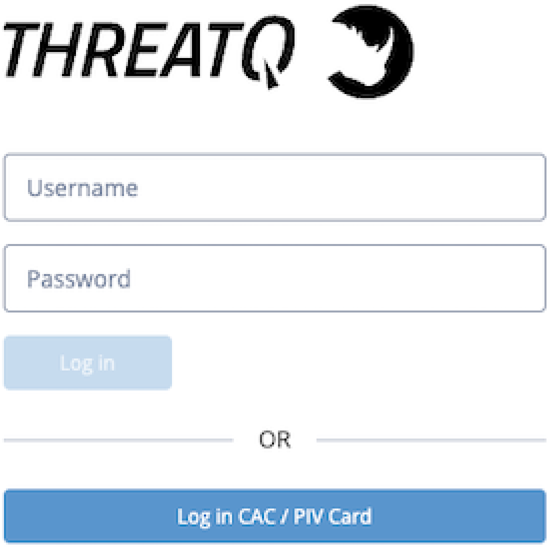
No Certificate Fingerprint Associated

4. Enter the user's certificate fingerprint.
5. Click the **Submit** button.

Adding Your Certificate Fingerprint - Login Page

1. Access your certificate, and enter your PIN. Your certificate must be active in the browser before you navigate to your ThreatQ instance.

2. Navigate to your ThreatQ instance.



3. Enter your username and password.
4. Click the **Log in** button.
5. The Store Fingerprint to Profile window prompts you to save your certificate fingerprint to your ThreatQ user profile.
6. Click the **Acknowledge & Login** button.
ThreatQ saves your certificate fingerprint. The next time you login, you can click the **Log in with CAC/PIV Card** button to access ThreatQ.

Using Certificate Authentication to Log In

> Maintenance users can log into ThreatQ using either username/password or certificate authentication. Administrative, Primary Contributor, and Read-Only users are required to use certificate authentication to log into ThreatQ if it is enabled.

After you or an Administrative/Maintenance user add a certificate fingerprint to your ThreatQ user profile, click the **Log in with CAC/PIV Card** button to access ThreatQ.

Managing Certificate Files

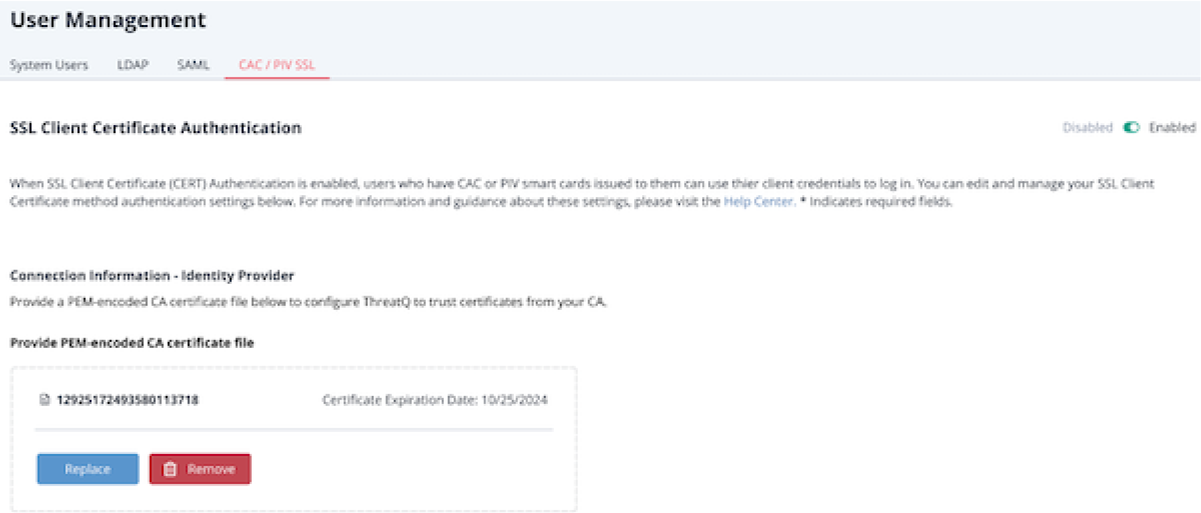
After you upload a certificate file and enable SSL Client Certificate Authentication, you may need to disable authentication to troubleshoot an issue or to migrate to a new authentication method. Or, you may want to remove or replace you current certificate file.

> Only Administrative or Maintenance logins have access to the CAC/PIV SSL tab in the User Management page which is used to manage SSL Client Certificate Authentication.

Disabling SSL Client Certificate Authentication

> After you disable SSL Client Certificate Authentication, you must reset all Admin, Primary Contributor, and Read Only access user passwords so that users can log in with their ThreatQ username and password. Maintenance Account users do not require a password reset and can continue to use their current password.

1. From the User Management page, click the CAC/PIV SSL tab.



User Management

SSL Client Certificate Authentication

When SSL Client Certificate (CERT) Authentication is enabled, users who have CAC or PIV smart cards issued to them can use thier client credentials to log in. You can edit and manage your SSL Client Certificate method authentication settings below. For more information and guidance about these settings, please visit the Help Center. * Indicates required fields.

Connection Information - Identity Provider

Provide a PEM-encoded CA certificate file below to configure ThreatQ to trust certificates from your CA.

Provide PEM-encoded CA certificate file

12925172493580113718 Certificate Expiration Date: 10/25/2024

2. Click the Disabled/Enabled toggle to change the status to Disabled.
   The Are You Sure? window prompts you to confirm the change.
3. Click the **Confirm** button.
   Even though SSL Client Certificate Authentication is disabled, the file that contains the certificate information is not deleted. This makes it easier for you to re-enable authentication.
4. Reset user passwords to allow users to log in with their ThreatQ username/password.

Removing a Certificate File

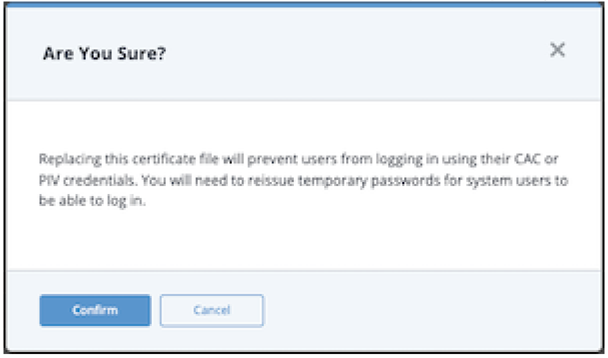
> ⚠ After you remove the certificate file, you must reset all Admin, Primary Contributor, and Read Only access user passwords so that users can log in with their ThreatQ username and password. Maintenance Account users do not require a password reset and can continue to use their current password.

1. From the User Management page, click the CAC/PIV SSL tab.
2. Click the **Remove** button.
   The Are You Sure? window prompts you to confirm the change.
3. Click the **Remove** button.
   SSL Client Certificate Authentication is disabled and all information is deleted from the certificate file.
4. Rest user passwords to allow users to log in with their ThreatQ username/password.

Replacing a Certificate File

> ⚠ After you replace a certificate file, you must either reset all Admin, Primary Contributor, and Read Only access user passwords so that users can log in and associate a new certificate with their user profile or add the new certificate fingerprints to each user profile. Maintenance Account users do not require a password reset and can continue to use their current password. However, they will also need to select a new certificate to log in using SSL Client Certificate Authentication.

1. From the User Management page, click the CAC/PIV SSL tab.
2. Click the **Replace** button.
   The Are You Sure? window prompts you to confirm the change.



Replacing this certificate file will prevent users from logging in using their CAC or PIV credentials. You will need to reissue temporary passwords for system users to be able to log in.

3. Click the **Confirm** button.
4. Upload the new certificate file using one of the following methods:

  - Drag and drop the file into the dialog box.
  - Select the click to browse link to locate the file on your local machine.

5. After you upload the file, the new certificate's serial number and expiration date is displayed
6. Use one of the following methods to add new certificate fingerprints for users:
    - Reset user passwords so that they can add their own certificate fingerprint during their next login.
    - Maintenance or Administrative users can use the System Users tab to add the new certificate fingerprint to user profiles.

Managing Certificate Fingerprints

Maintenance and Administrative users can use the User Management page to update or remove the certificate fingerprint associated with a username. Primary Contributor and Read-Only users can view certificate fingerprints but cannot edit them.

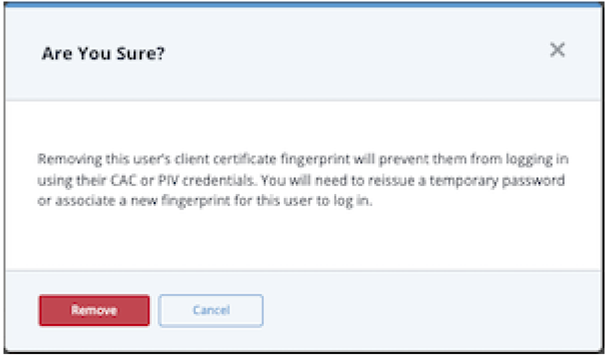
Updating Certificate Fingerprints

After SSL Client Certificate Authentication is enabled, you can change the certificate fingerprint on a user profile.

1. From the User Management screen, click the User Management tab.
2. Locate and click the user's display name.
3. From the User Profile tab in the Edit User page, click the pencil icon next to the user's CERT fingerprint.
4. Enter the new certificate fingerprint.
5. Click the **Submit** button.

Removing Certificate Fingerprints

1. From the User Management screen, click the User Management tab.
2. Locate and click the user's display name.
3. From the User Profile tab in the Edit User page, click the pencil icon next to the user's CERT fingerprint.
4. Click the **Remove** button.
   The Are You Sure? window prompts you to confirm the removal.



Are You Sure?

Removing this user's client certificate fingerprint will prevent them from logging in using their CAC or PIV credentials. You will need to reissue a temporary password or associate a new fingerprint for this user to log in.

5. Click the **Remove** button.

Troubleshooting SSL Client Certificate Authentication

The following is a list of common authentication errors a user may encounter when accessing ThreatQ.

ERROR MESSAGE	CAUSE	RESOLUTION

`Password Expired`
`Your temporary password has expired. Please use your CAC / PIV credentials to log in to this system. If your client credentials do not authenticate, please contact your administrator.`
	An Administrative, Primary Contributor, or Read-Only user attempted to use a password to log in after a CAC / PIV SSL fingerprint was added to the user profile.	From the ThreatQ login page, click the **Log in with CAC/PIV Card** button to access ThreatQ.

`Certificate Error`
`Your stored fingerprint indicates that your CAC / PIV certificate has encountered an error or has expired. Please contact your administrator for new credentials.`
	A user attempted to use an expired CAC / PIV SSL certificate.	Ask a Maintenance or Administrative user to add your new certificate fingerprint to your user profile.

`The fingerprint has already been taken.`	A user attempted to log in using a certificate/ fingerprint that is already associated with another user profile.	Contact a Maintenance or Administrative user to determine the root cause of the certificate duplication.

The following is a list of common authentication errors a user may encounter when configuring SSL Client Certificate Authentication.

ERROR MESSAGE	CAUSE	RESOLUTION
`Upload a valid RSA certificate to enable.`	An Administrative or Maintenance user tried to move the Disabled/ Enabled toggle to Enabled without uploading a CA certificate file.	See the SSL Client Certificate Authentication topic for the steps required to enable SSL Client Certificate Authentication.
`The certificate file is not a valid X.509 certificate.`	An Administrative or Maintenance user tried to upload a certificate file that was not a PEM-encoded, X.509 CA certificate file.	Upload a PEM-encoded, X.509 CA certificate file.
`This certificate is expired.`	An Administrative or Maintenance user tried to upload a certificate file with an expiration prior to the current date.	Upload a certificate file with an expiration date after than the current date.

Index