

ThreatQuotient



ThreatQ User Guide

Version 4.47.0

February 02, 2021

ThreatQuotient

11400 Commerce Park Dr., Suite 200
Reston, VA 20191

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: 703.574.9893

Warning and Disclaimer

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

Copyright © 2021 ThreatQuotient, Inc.

All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

Contents

About the ThreatQ Platform	11
Concept.....	11
Threat Library	11
Adaptive Workbench.....	11
Open Exchange.....	11
Accessing the Platform	12
Authentication Methods.....	13
Transitioning Authentication Methods	14
Platform Login.....	16
Local Log in.....	16
Single Sign-On (SSO).....	16
2-Step Verification	18
Enabling 2-Step Verification	18
Air Gapped Data Sync (AGDS)	19
System Requirements	19
Executing Air Gapped Data Sync	20
Running the threatq:sync-export Command	20
Running the threatq:sync-import Command.....	20
threatq:sync-import	22
Parameters.....	22
Examples	23
Initial Setup	24
Run Scenarios	25
Data Processing.....	26
Basic Table.....	26
Tables with Pivots.....	27
File Output.....	27
threatq sync-import File Output and Sync Report	27
threatq:sync-import Command Line Output.....	27
Synchronizations	27
threatq:sync-export.....	29
Parameters.....	29
Examples	31
Initial Cron for First Time Use	33
Run Scenarios	34
Dates.....	35
Configuration	35
Output and Sync Report	36
Meta Data.....	36
Meta Data Objects.....	37
Objects.....	37
Object Context.....	39
Other Data.....	39
File Output.....	41
Command Line Output.....	42
Synchronizations	42
Upgrading an Air Gapped ThreatQ Instance.....	44
Analytics	46
Adversaries.....	47
Adversaries Summary Table	47
Adversaries Overlap Table	48
Indicator Distribution Pie Chart.....	49

Events.....	51
Events History Scatter Plot	51
Monthly Heatmap.....	53
New Events Summary	54
Files	56
Files Pie Chart	56
Files Table.....	58
Indicators.....	60
Recently Created Indicators Histogram.....	60
Most Recent 100 Indicators.....	62
Attributes Table	63
Recent Sources	64
Attack Phases.....	66
Backup and Restore.....	68
ThreatQ Backup	68
ThreatQ Restore	69
Command Line Interface (CLI).....	71
Maintenance Mode	71
Placing the ThreatQ Application into Maintenance Mode	71
Taking the ThreatQ Application out of Maintenance Mode	72
Commands	73
Auto Configuration MariaDB Command	73
System ThreatQ Purge.....	73
Add/Upgrade CDF.....	74
Source Consolidation	76
Source Merge.....	76
Historic Pull	79
iSight Historic Pull.....	79
Threat Intelligence Services Custom Feeds Historic Pull Commands.....	80
Reset User Password	80
Update TLP Designations	80
Convert TLP	82
View Feed Queues.....	83
Airgap Import.....	84
Airgap Export	84
Orphaned Attribute Purge	84
Dashboards.....	85
Default Dashboard	86
Overview by Intelligence Score	86
Incoming Intelligence	87
Watchlist Activity.....	88
Tasks	89
Custom Dashboards	90
Widget Options	90
Bar Chart	91
Description	93
Line Chart	93
Count	95
Pie Chart	96
Table	97
User View Management	99
Adding a Dashboard to Your View	99
Removing a Dashboard from Your View	100
Changing Dashboard Order.....	101
Dashboard Sharing	102
Setting Dashboard Sharing	102
Editing Privately Shared Users.....	104

Shared Dashboards of a Deleted User	106
Dashboard Management	107
Creating a Dashboard	107
Editing a Dashboard	109
Deleting a Dashboard	110
Reassigning a Dashboard of a Deleted User	111
Data Management	113
Automatic Expiration	114
Accessing the Automatic Expiration Page	114
How ThreatQ Calculates Expiration Dates	114
Selecting an Expiration Policy per Feed	115
Adding Exceptions	116
Applying Expiration Policy Changes to Data	117
Common Expiration Policy Scenarios	118
Scoring Algorithms	121
Accessing the Scoring Algorithm Page	121
Scoring Criteria	121
Configuring Your Scoring Algorithm	121
Traffic Light Protocol (TLP)	123
TLP Assignment Hierarchy	123
Access TLP Settings	124
Configure TLP Visibility	125
Apply a TLP Designation to Source	125
Whitelisted Indicators	127
Accessing the Whitelisted Indicator Rules	127
Creating a Whitelisted Rule	127
Editing a Whitelisted Rule	129
Removing a Whitelisted Rule	130
Exports	132
Managing Exports	133
Accessing the Exports List	133
Viewing an Export	133
Enabling/Disabling Exports	133
Adding an Export	134
Duplicating an Export	135
Editing an Export's Connection Settings	135
Editing an Export's Output Format	136
Deleting an Export	138
Output Format Options	140
Customizing the Output Format Template	140
Adding Special Parameters	140
Adding Differential Flags	154
Adding Parameters to the end of the URL	154
Using Logical Operators in Export Filters	155
Output Format Templates	156
Adversaries Template	156
Events Template	156
Indicators Template	157
Signatures Template	157
Template Variables	158
Source Variable	158
Attribute Variable	158
Adversary Variable	158
Attachment Variable	158
Event Variable	159
Indicator Variable	159
Investigation Variable	159

Signature Variable	159
Task Variable	159
Specific Indicator Exports	161
Cisco TID Exports	162
Fidelis Exports	169
Fortinet Fortigate Exports	180
Lancope Exports	186
Netwitness Exports	188
OpenIOC Signature Exports	191
Palo Alto Exports	193
Palo Alto: PANOS and Panorama Exports	194
Reservoir Labs Exports	196
Splunk Exports	199
Symantec ProxySG Exports	201
Tenable Exports	207
Zeek Exports	210
Integrations Management	213
Accessing Integrations Management	214
Integration Types	216
Threat Intelligence Feed Categories	216
Operations	217
Managing Integrations	218
Adding Integrations	218
Adding STIX/TAXII Integrations	222
Configuring an Integration	228
Feed Health Notifications	229
Enabling/Disabling Integrations	231
Removing an Integration	234
Performing Manual Runs (feeds)	236
Running an Operation Integration	238
Integration-Related Commands	240
Activity Log (feeds)	241
Accessing an Intel Feed's Activity Log	243
Job Management	245
Licensing	248
Managing Your ThreatQ License	248
Viewing License Status	248
Updating a License	249
Navigation Menu	250
Notifications	253
Feed Health Email Notifications	254
Configuring Mail Server	254
Enabling Feed Health Notifications	257
Notification Center	259
Reports	260
Generating Reports	260
Turning Off the Pop-Up Blocker in Chrome	260
Report Options	261
Customizing the Report Header	261
Customizing Report Text Colors	261
Adding a Custom Disclaimer to a Report	262
Previewing Report Customization	262
Server Administration	263
ThreatQ Monitoring Platform	263
Accessing the ThreatQ Monitoring Platform	263
System Configuration	266
Indicator Statuses	267

Indicator Status Assignment	267
Indirect Indicator Status	267
Protected Indicator Statuses	267
Viewing Indicator Statuses	267
Suppressing Indicator Status Updates	268
Adding an Indicator Status	269
Editing an Indicator Status	270
Deleting an Indicator Status	271
Indicator Types	273
Event Types	274
Viewing Event Types	274
Adding an Event Type	276
Editing an Event Type	277
Deleting an Event Type	279
LDAP Authentication	281
Required Information for Creating LDAP Authentication	282
Switching LDAP Connections	283
Anonymous Bind	284
Configuring Secure LDAP	287
Authenticated Bind	289
SAML Authentication	295
Configuring SAML	295
Setting Up LDAP Users/Groups for SAML	301
Adding ThreatQ as a Service Provider	306
ADFS 2016	306
Azure AD	309
Google G Suite	312
Okta	316
Proxy	320
Accessing Proxy Configuration	320
Account Security	321
Configuring User Lockout Settings:	321
General Settings	323
Configuring Date and Time Format	323
Configuring Indicator Parsing Presets	324
System Objects	327
Adversaries	328
Adding Adversaries	328
Adding Context	329
Editing Adversaries	329
Deleting Adversaries	330
Events	332
Adding Events	332
Adding Context	333
Editing Events	333
Deleting Events	334
Files	337
Adding Files	337
Adding Context	339
Editing Files	339
Deleting Files	341
Indicators	343
Adding an Indicator	343
Adding Context	344
Editing Indicators	344
Deleting an Indicator	345
Parsing for an Indicator	347

CSV File Format Parsing.....	352
Indicator Expiration.....	354
Ways an Indicator can Expire.....	354
Changing the Expiration Date for an Individual Indicator.....	355
Changing the Expiration Date for Multiple Indicators.....	356
Indicator Scoring.....	357
Building a Scoring Algorithm.....	357
Setting a Manual Indicator Score.....	357
Indicator Status.....	359
Default Statuses.....	359
Custom Statuses.....	360
Changing the Status of an Individual Indicator.....	360
Changing the Status for Multiple Indicators.....	361
Indicator URL Normalization.....	362
Supported Defanging Techniques.....	365
Signatures.....	367
Adding a Signature.....	367
STIX.....	371
ThreatQ STIX Object Types.....	371
Parsing a STIX File for Indicators.....	371
STIX 1.1.1, 1.2 Data Mapping.....	373
STIX2.0 Data Mapping.....	386
Tasks.....	411
Assigning a Task.....	411
Managing Tasks.....	411
Threat Library.....	413
Managing Your Library View.....	414
Selecting Object Type View.....	414
Managing Library Columns.....	415
Basic Search.....	417
Performing a Basic Search.....	417
Wildcards and Symbols in Searches.....	419
Building Searches with Filter Sets.....	420
Adding Filter Sets.....	27
Deleting Filter Sets.....	422
And/Or Order of Operations.....	423
Context Filters.....	424
Filtering by Attribute.....	424
Filtering by CIDR Block Range.....	428
Filtering by Value Contains.....	429
Filtering by List of Indicators.....	429
Filtering by Keyword.....	431
Filtering by Relationship.....	433
Filtering by Related Object Type.....	434
Filtering by Score.....	436
Filtering by Tags.....	438
Filtering by TLP.....	439
Date Filters.....	442
Filtering by Date Created.....	442
Filtering by Last Modified.....	443
Filtering by Published Date.....	444
Filtering by Source Ingest Time.....	445
Filtering by Expiration Date.....	446
Status Filters.....	449
Filtering by Status.....	449
Tasks Filters.....	450
Filtering Tasks by Assignment.....	450

Filtering Tasks by Due Date.....	451
Filtering Tasks by Priority	452
Filtering Tasks by Reported By.....	453
Type Filters	455
Filtering by Object Type	455
Managing Search Results.....	456
Saving Searches as Data Collections.....	456
Loading Data Collections.....	457
Deleting a Data Collection	458
Exporting Search Results to CSV.....	459
Bulk Actions.....	461
Bulk Add Source	463
Bulk Add/Remove Attributes.....	465
Bulk Add/Remove Attribute Scenarios	467
Bulk Add/Remove Tags.....	469
Bulk Change Expiration Date	471
Bulk Expiration Change Scenarios	473
Bulk Delete	474
Bulk Add/Remove Relationships	476
Bulk Status Change	479
Object Details.....	481
Adding/Removing an Object to the Watchlist.....	486
Actions Menu	487
Context Panes.....	489
Attributes Pane	490
Adding an Attribute to an Object	490
Deleting an Attribute from an Object	491
Deleting an Attribute Source from an Object	491
Sources Pane	493
Adding a Source to an Object	493
Tags Pane	495
Adding a Tag to an Object	495
Deleting a Tag from an Object.....	495
Description Pane.....	496
Updating the Description of an Object.....	496
Relationships Panes	497
Linking a System Object	497
Unlinking a System Object	498
Additional Related Object Actions.....	499
Adding a comment to a related adversary	499
Editing a related adversary comment	499
Deleting a related adversary comment.....	499
Related Adversaries - Confidence Level	500
Related Indicators - Bulk Actions.....	500
Comments Pane	502
Adding Comments to an Object	502
Editing Comments for an Object.....	502
Deleting Comments from an Objects	503
Audit Log.....	504
Troubleshooting.....	505
Generating a Troubleshooting Package.....	506
SSL Certificates.....	507
Unable to Verify SSL Certificate	507
Configuring Custom SSL Certificates (not self-signed).....	507
ThreatQ Critical System Processes	509
Data and Time Stamps in ThreatQ	511
User Management	513

Managing User Accounts.....	514
Accessing Your User Account.....	514
Accessing Other User Accounts.....	514
User Account Properties.....	514
Adding a User.....	515
Editing a User.....	516
Resetting User Password from the Command Line.....	517
Deleting a User.....	518
Updating User Avatar.....	518
User Roles.....	520
Index.....	522

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

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.	• 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 Authentication

METHOD	DESCRIPTION	REFERENCE
	SAML does not allow user role mapping for maintenance accounts.	
	SAML users will log in using the single sign-on (SSO) login option for the ThreatQ platform - see SSO Login .	

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.  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.

CURRENT METHOD	NEW METHOD	DETAILS
 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.

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

- [Local Log In](#)
- [Single Sign-On \(SSO\)](#)

Local Log in

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

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



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

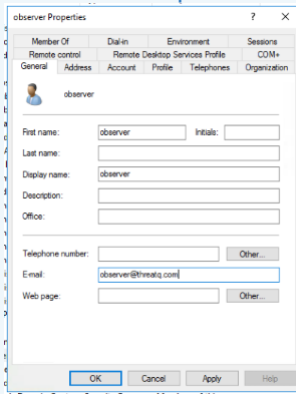
Single Sign-On (SSO)

Users using SAML authentication will use this log in method.



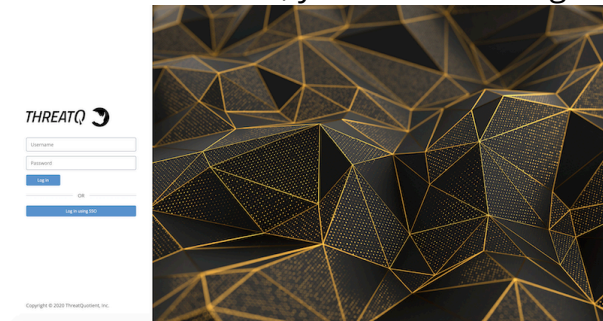
SAML users are required to add their email address to their user profiles in order to use the SSO. As part of the integration process, the ThreatQ platform expects that the user's email address has already been added to their IdP. See the [Setting up LDAP](#)

Users/Groups for SAML topic for more details.



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

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



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

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

2-Step Verification

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

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

Enabling 2-Step Verification

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 your Google Authenticator mobile app.
 - b. Enter the validation code delivered to your mobile device via Google 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.

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-import 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
<code>--file</code>	File path to the tarball created by the <code>threatq:sync-export</code> command. This command is required to run the <code>threatq:sync-import</code> command. example: <code>--file=/tmp/tqSync-19-01-16-1547660837-8345.tar.gz</code>
<code>--keep-created-at</code>	Determines whether the oldest <code>created_at</code> date between the source and target ThreatQ installations should be maintained, or a new <code>created_at</code> is set on the target system. The default if this option is not provided by the user is for the oldest <code>created_at</code> date to be maintained. This value is required. Options are Y(es) or N(o). Default: Y example: <code>--keep-created-at=N</code>

PARAMETER	EXPLANATION
<code>--object-limit</code>	Integer value used as the limit for the number of objects updated or inserted at a time. This value is required. When using this option, the size of the data sets on both source and target ThreatQ installations should be taken into account. Setting the limit too high may hinder performance. Default: 1000 example: <code>--object-limit=50000</code>
<code>--memory-limit</code>	Sets the PHP memory limit in Megabytes or Gigabytes. This value is required. Default: 2G example: <code>--memory-limit=4G</code>
<code>--override-description</code>	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: <code>--override-description=N</code>

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_types` - (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. ex: --start-date="2018-01-01 00:00:00"
--end-date	The end date for data selection. This value is required. Applies only to objects themselves, not object context or object links. example: --end-date="2018-01-02 00:00:00"

PARAMETER	EXPLANATION
--include-deleted	Determines whether objects that have been soft-deleted are included in the result set. Options are Y(es) or N(o). Default: N example: --include-deleted=Y
--include-investigations	Determines whether Investigations and Tasks are included in the result set. This value is required. Options are Y(es) or N(o). Default: N example: --include-investigations=N
--meta-only	If present, tells the command to only include meta data (no object data) in the result set. No value necessary.
--memory-limit	Sets the PHP memory limit in Megabytes or Gigabytes. This value is required. Default: 2G example: --memory-limit=4G
--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

PARAMETER	EXPLANATION
	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"

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 Action
- Exploit Targets
- Incidents
- TTPs

Storage:

The data for each object is copied as a dump file in CSV format using "SELECT * INTO OUTFILE..." MariaDB syntax. The full query for the data is built up using the options you provided (start date, end date, etc).

Dump files contain a maximum object limit of 50,000 (set in the Synchronization base class). Dump files are created (with a counter appended to the file name) until the entire object result has been covered.

To ensure that any Objects present in Object Context (Attributes, Comments, and Sources), Object Links, Tagged Objects, or Investigation Timeline Objects are also included in the base Object data, CSV dump files for each Object type are also created from queries against each of these tables. This is necessary because of the differing date columns used in each query (an object may appear in an Object Link in the specified date range according to the Object Link's `updated_at` date, even though the Objects themselves saw no change to their `touched_at` date in that date range). When the data from all of these object files is transferred to the target ThreatQ installation, any duplicates across dump files will be consolidated. Files that contain Object data will always include "_obj_" in the file title.

Sample Object File List (all of these files will contain Adversary records):

- adversaries/adversaries_obj_0.csv
- adversaries/adversaries_obj_attributes_0.csv

- adversaries/adversaries_obj_comments_0.csv
- adversaries/adversaries_obj_investigation_timelines_0.csv
- adversaries/adversaries_obj_object_links_dest_0.csv
- adversaries/adversaries_obj_object_links_src_0.csv
- adversaries/adversaries_obj_sources_0.csv
- adversaries/adversaries_obj_tags_0.csv

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

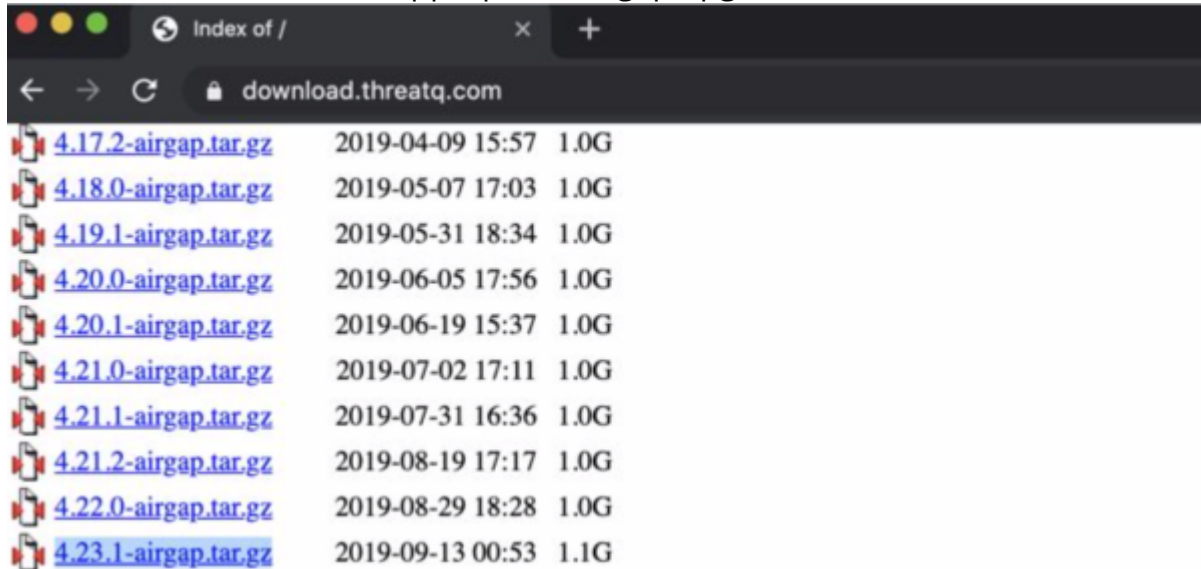
A Synchronization record is finalized when the command run has completed. At this time, the `finished_at` column is filled with the completion datetime, and the `report_json` column is updated to include information about the run (object counts, files created, etc).

Upgrading an Air Gapped ThreatQ Instance



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

1. Log into the ThreatQ download repository, <https://download.threatq.com>, using your YUM credentials.
2. Locate and download the appropriate airgap upgrade file.



4.17.2-airgap.tar.gz	2019-04-09 15:57	1.0G
4.18.0-airgap.tar.gz	2019-05-07 17:03	1.0G
4.19.1-airgap.tar.gz	2019-05-31 18:34	1.0G
4.20.0-airgap.tar.gz	2019-06-05 17:56	1.0G
4.20.1-airgap.tar.gz	2019-06-19 15:37	1.0G
4.21.0-airgap.tar.gz	2019-07-02 17:11	1.0G
4.21.1-airgap.tar.gz	2019-07-31 16:36	1.0G
4.21.2-airgap.tar.gz	2019-08-19 17:17	1.0G
4.22.0-airgap.tar.gz	2019-08-29 18:28	1.0G
4.23.1-airgap.tar.gz	2019-09-13 00:53	1.1G

3. Open the CLI of the device to upgrade and run the following:

```
< > mkdir /var/tmp/upgrade
```

4. Copy the upgrade file you downloaded in step 2 to the newly created directory `/var/tmp/upgrade` using the scp client of your choice.
5. Return to the CLI of the device and confirm that the upgrade file is present.
6. Use the following commands to unpack and run the upgrade file:

```
< > sudo su -  
screen -S threatq  
cd /var/tmp/upgrade  
ls -al  
tar -xvzf /var/tmp/upgrade/<upgrade filename>  
/var/tmp/upgrade/upgrade.sh
```


7. Allow the upgrade process to complete. When complete, the output should resemble the following:

```
Installed:
chrony.x86_64 0:3.2-2.el7
device-mapper-event.x86_64 7:1.02.149-10.el7_6.7
device-mapper-event-libs.x86_64 7:1.02.149-10.el7_6.7
device-mapper-persistent-data.x86_64 0:0.7.3-3.el7
dnsmasq.x86_64 0:2.76-7.el7
gnutls.x86_64 0:3.3.29-9.el7_6
gsettings-desktop-schemas.x86_64 0:3.28.0-2.el7
libXfont.x86_64 0:1.5.4-1.el7
libgnome-keyring.x86_64 0:3.12.0-1.el7
libgudev1.x86_64 0:219-62.el7_6.6
libldb.x86_64 0:1.3.4-1.el7
librabbitmq-devel.x86_64 0:0.8.0-2.el7
libtalloc.x86_64 0:2.1.13-1.el7
libtdb.x86_64 0:1.3.15-1.el7
libtevent.x86_64 0:0.9.36-1.el7
libtirpc.x86_64 0:0.2.4-0.15.el7
libzip-last.x86_64 0:1.1.3-1.el7.remi
lm_sensors.x86_64 0:3.4.0-6.20160601gitf9185e5.el7
lvm2.x86_64 7:2.02.180-10.el7_6.7
lvm2-libs.x86_64 7:2.02.180-10.el7_6.7
mlocate.x86_64 0:0.26-8.el7
net-snmp-libs.x86_64 1:5.7.2-37.el7
net-snmp-utils.x86_64 1:5.7.2-37.el7
nettle.x86_64 0:2.7.1-8.el7
postgresql-libs.x86_64 0:9.2.24-1.el7_5
python-markdown.noarch 0:2.4.1-2.el7
rpcbind.x86_64 0:0.2.0-47.el7
samba-common.noarch 0:4.8.3-4.el7
trousers.x86_64 0:0.3.14-2.el7

Complete!
[root@support02 upgrade]#
[root@support02 upgrade]#
[root@support02 upgrade]#
```



If your terminal session should end prematurely at any point during the upgrade, you can return to it by logging back into the CLI and running the command below.

```
<> screen -r threatq
```

Analytics

The Analytics tab provides a summary view of Adversary, Event, File, and Indicator Object Types.

Search filters are not available for these views nor can you modify the types of columns used. Use the [Threat Library](#) to utilize these options.

To access the ThreatQ Analytics page:

1. Click on the **Analytics** option located in the top navigation menu and select one of the following options:
 - [Adversaries](#)
 - [Events](#)
 - [Files](#)
 - [Indicators](#)

Adversaries

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

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.

ADVERSARIES			
Showing 1 to 10 of 92		Row count: 10	
ADVERSARY NAME	NUMBER OF INDICATORS	DATE CREATED	MOST RECENT EVENT DATE
Start typing...	Start typing...	Start typing...	Start typing...
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
Previous			Next

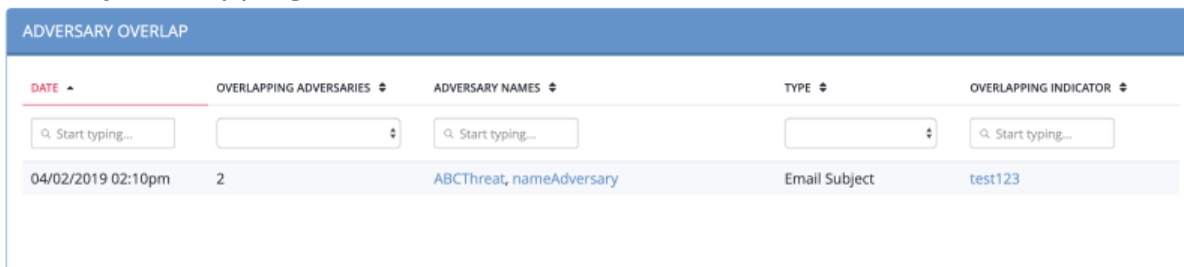
The following functions are available:

FUNCTION	DETAILS
Opening the Adversary Details page for an adversary	1. Click the name in the Adversary Name column.
Performing a search for related indicators	1. Click the number in the Number of Indicators column to set the adversary name as a search criterion and open the Advanced Search page.

FUNCTION	DETAILS
Opening the Event Details page for an adversary event	1. Click the date in the Most Recent Event Date to open the Event Details page.
Changing the number of entries displayed in the table	1. Click the paging batch option located to the bottom-right of the table.
Sorting the table by a column	1. Click the column header. To reverse the column sorting order, click the header a second time.
Searching within the Adversary Name column	1. Click within the search box at the top of the column, and enter your search criteria.

Adversaries Overlap Table

The Adversary Overlap table lists adversaries, the date and time they were created, their type, and any overlapping indicators.



The screenshot shows the 'ADVERSARY OVERLAP' table with the following columns: DATE, OVERLAPPING ADVERSARIES, ADVERSARY NAMES, TYPE, and OVERLAPPING INDICATOR. Each column has a search box at the top. The table contains one row of data.

DATE	OVERLAPPING ADVERSARIES	ADVERSARY NAMES	TYPE	OVERLAPPING INDICATOR
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	1. Click the name in the Adversary Name column.

FUNCTION

DETAILS

Opening the Indicator Details page for an overlapping indicator

1. Click the identity in the Overlapping Indicator column.

Changing the number of entries displayed in the table

1. Click the paging batch option located to the bottom-right of the table.

Sorting the table by a column

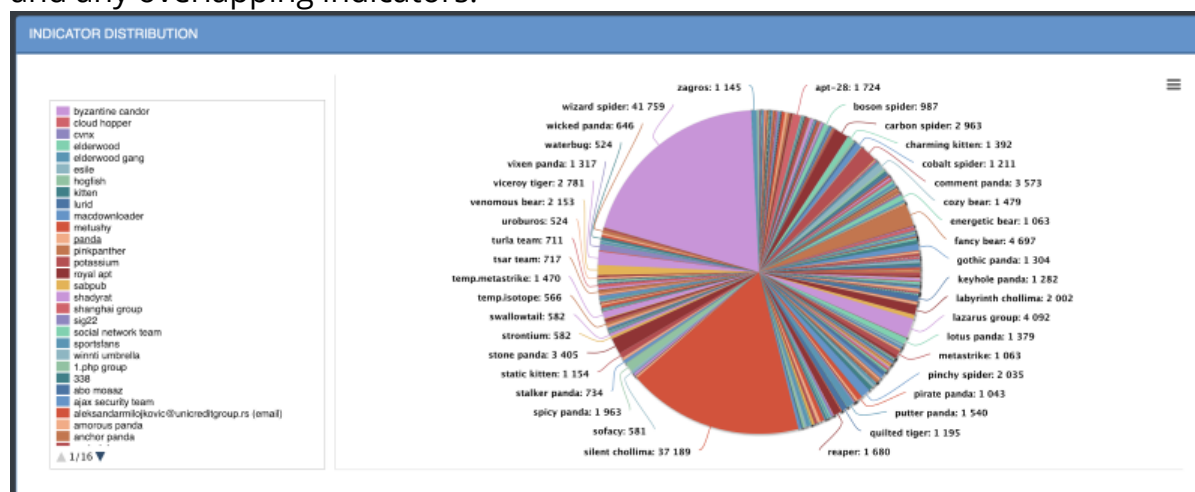
1. Click the column header. To reverse the column sorting order, click the header a second time.

Searching within a column

1. Click within the search box at the top of the column, and enter your search criteria.

Indicator Distribution Pie Chart

The Adversary Overlap table lists adversaries, the date and time they were created, their type, and any overlapping indicators.



The following functions are available:

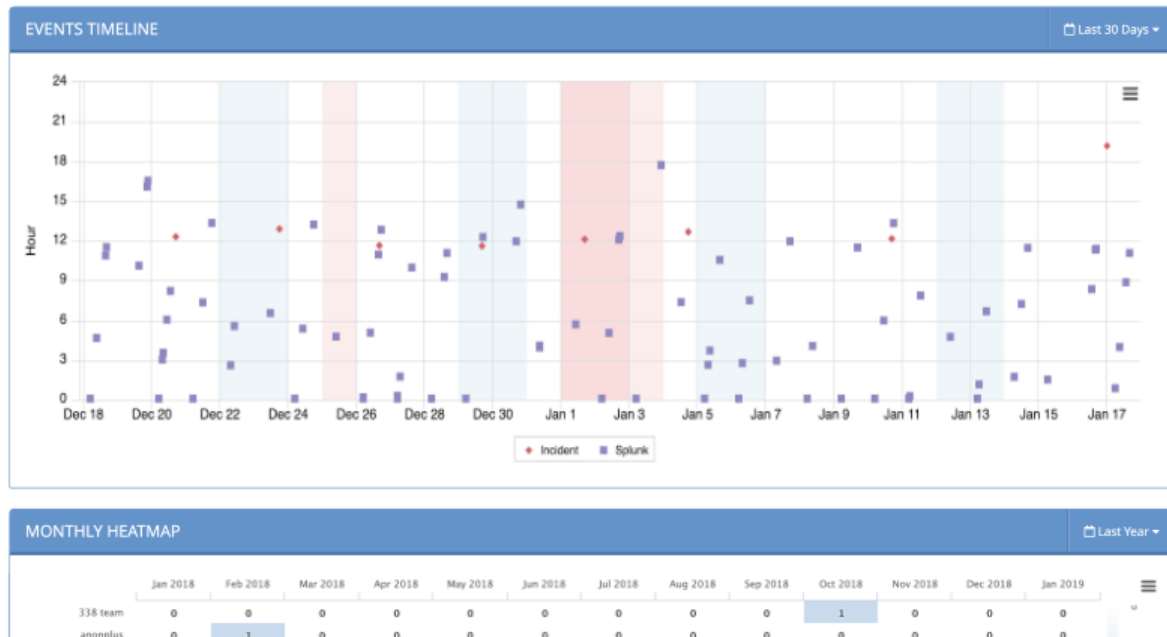
FUNCTION	DETAILS
Viewing more information about a selected value	1. Hover over a colored section of the pie chart to open a popup identifying the indicator. The number of times the indicator was found within the specified time frame, and what percentage of the total number of indicators it represents.
Hiding or unhiding one of the values from the pie chart	1. Click the indicator on the left of the pie chart to remove it; click a second time to reinstate it.
Adjusting the time frame of the information displayed	1. Click the dropdown menu at the top right and select the desired timeframe. You can select from: ◦ Last 24 Hours ◦ Last 7 Days ◦ Last 30 Days ◦ Last Year ◦ User-set custom range
Printing the graph or saving it as a PNG, JPEG, PDF, or SVG	1. Click the hamburger menu  and select the desired option.

Events

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

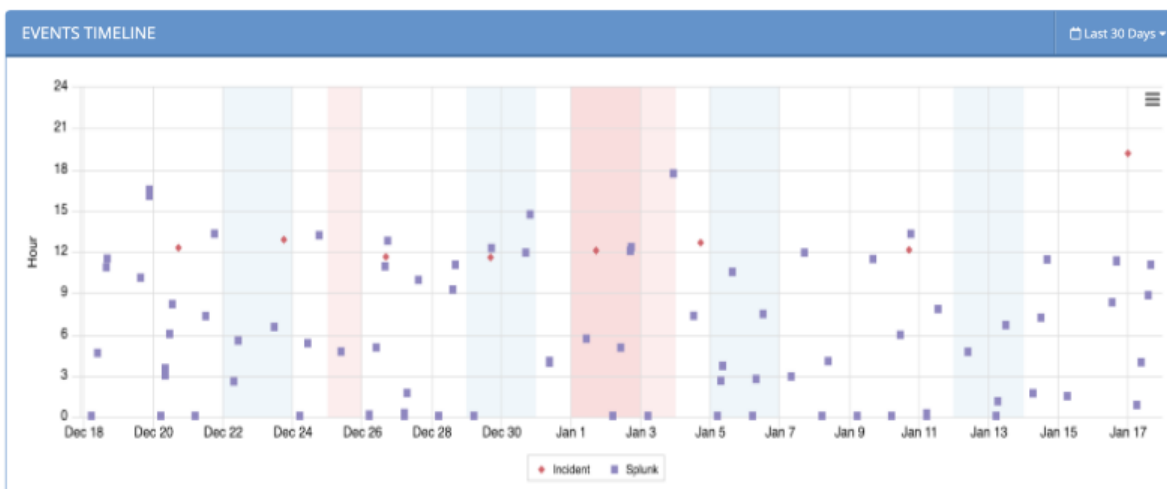
Events Overview

[Analytics](#) [New Events](#)



Events History Scatter Plot

The scatter plot points are plotted by date (x-axis) and hour (y-axis). The legend under the scatter plot identifies the different kinds of events shown.



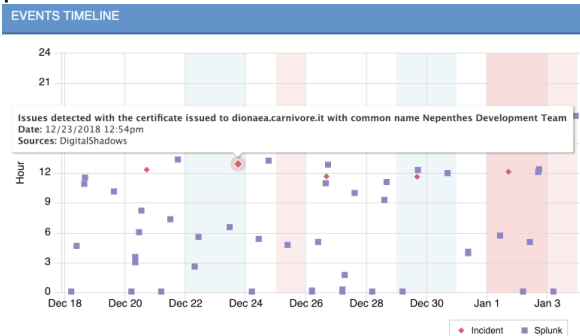
The following functions are available:

FUNCTION

DETAILS

Viewing an event's name, date and time, and source

1. Hover your mouse over an event on the scatter plot to see its name, date and time, and source.



Opening the Event Details page for one of the events

1. Click the event in the scatter plot.

For more information, see [Object Details](#).

Hiding or unhiding one or more of the event types

1. Click the event type in the legend immediately below the scatter plot to remove it from the graph; click it again to reinstate it.

Adjusting the time frame of the information displayed

1. Click the dropdown menu at the top right and select the desired time frame.

You can select from:

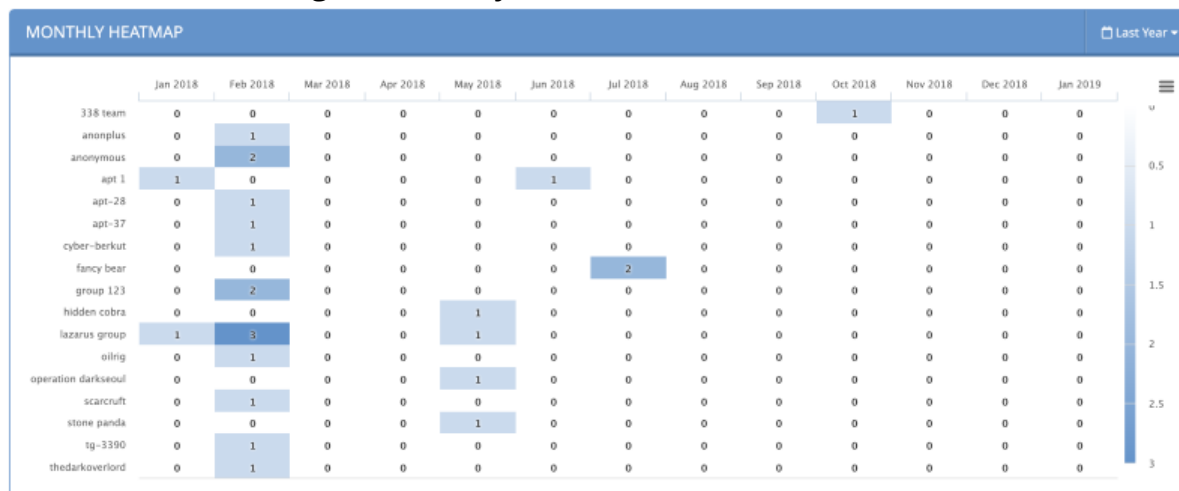
- Last 24 Hours
- Last 7 Days
- Last 30 Days
- Last Year
- User-set custom range

Printing or downloading the scatter plot as a PNG, JPEG, PDF, or SVG file

1. Click the hamburger menu  and select the desired option.

Monthly Heatmap

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



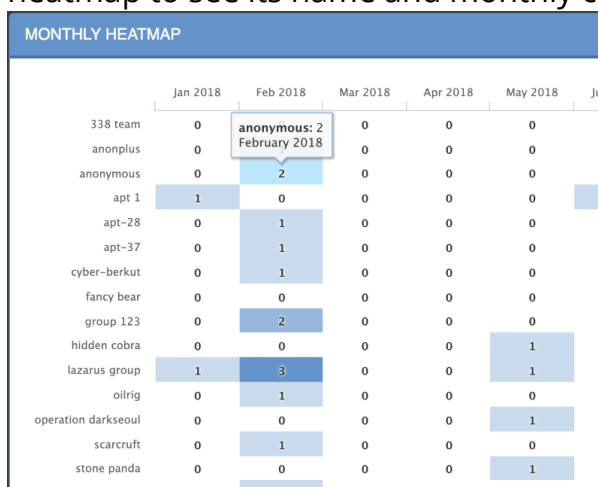
The following functions are available:

FUNCTION

DETAILS

Viewing an event's name and monthly count

1. Hover your mouse over an event on the heatmap to see its name and monthly count.



Adjusting the time frame of the information displayed

1. Click the dropdown menu at the top right and select the desired time frame.

FUNCTION

DETAILS

You can select from:

- Last 24 Hours
- Last 7 Days
- Last 30 Days
- Last Year
- User-set custom range

Printing the graph or saving it as a PNG, JPEG, PDF, or SVG

1. Click the hamburger menu  and select the desired option.

New Events Summary

The New Events Summary table provides a breakdown of events by date, type, title, and

NEW EVENTS			
DATE	TYPE	TITLE	SOURCES
Filter by date		Start typing...	Start typing...
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
< 1 2 3 4 5 6 7 > Rows per page 10			

sources.

The following functions are available:

FUNCTION

DETAILS

Opening the Event Details page for one of the events

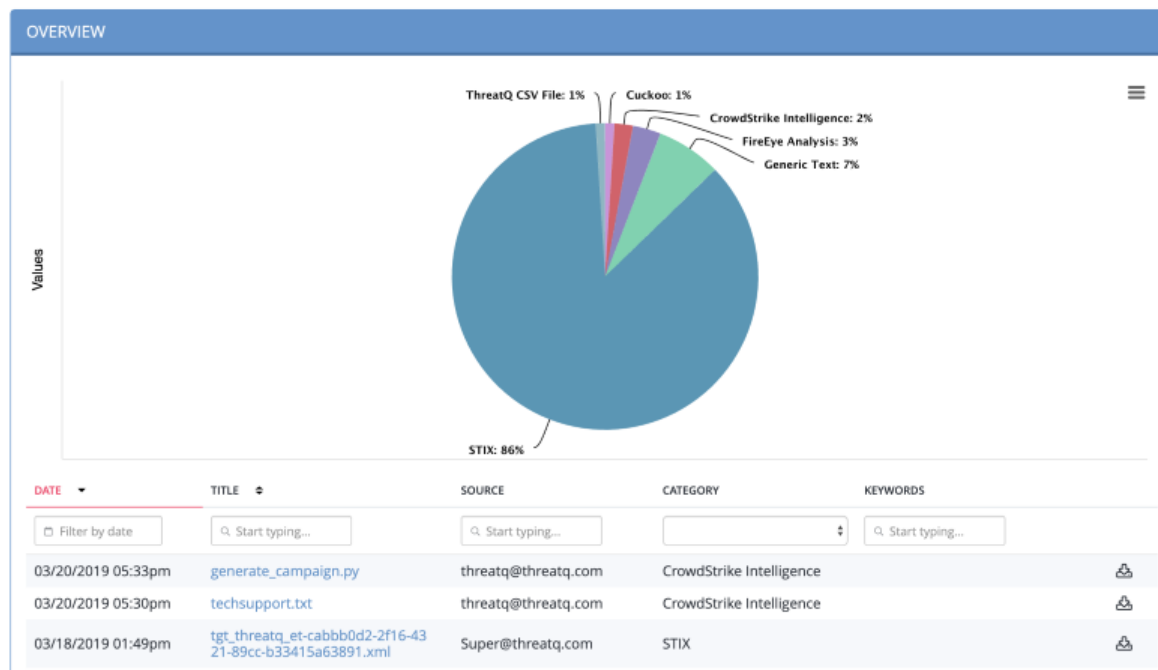
1. Click the event title.

FUNCTION	DETAILS
For more information, see Object Details .	
Changing the number of entries displayed in the table	1. Click the dropdown menu at the top right of the table, and select the desired option.
Sorting the table by a column	1. Click the column header. 2. Click the header a second time to reverse sort order.
Searching within a column	1. Click within the search box at the top of the column, and enter your search criteria.

Files

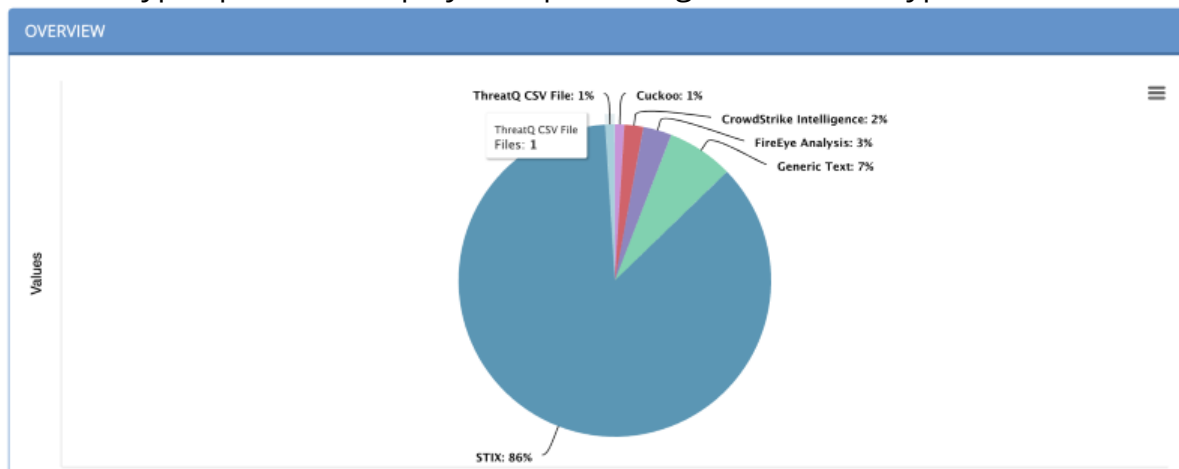
The Files page provides you with a pie chart displays the percentage of different types of files within the system and a table that lists the files, the date and time they were created, their title, their source, their category, and associated keywords.

Files Overview

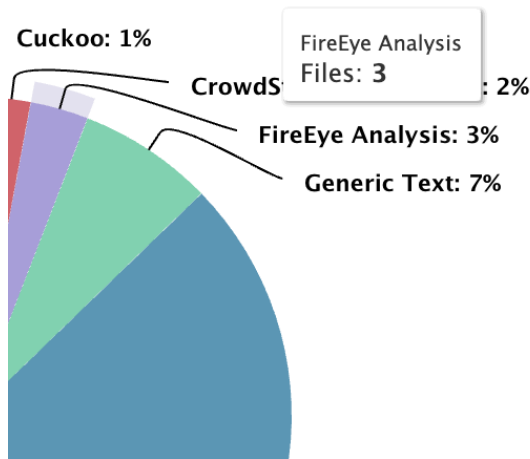


Files Pie Chart

The File Types pie chart displays the percentage of different types of files within the system.



The following function is available:

FUNCTION	DETAILS																		
Viewing more information about a selected file	1. Hover over a colored section of the pie chart to open a popup that gives the number of attachment types. <table><thead><tr><th>Attachment Type</th><th>Percentage</th><th>Count</th></tr></thead><tbody><tr><td>Generic Text</td><td>7%</td><td>-</td></tr><tr><td>FireEye Analysis</td><td>3%</td><td>3</td></tr><tr><td>CrowdStrike</td><td>2%</td><td>-</td></tr><tr><td>Cuckoo</td><td>1%</td><td>-</td></tr><tr><td>Other</td><td>-</td><td>-</td></tr></tbody></table>	Attachment Type	Percentage	Count	Generic Text	7%	-	FireEye Analysis	3%	3	CrowdStrike	2%	-	Cuckoo	1%	-	Other	-	-
Attachment Type	Percentage	Count																	
Generic Text	7%	-																	
FireEye Analysis	3%	3																	
CrowdStrike	2%	-																	
Cuckoo	1%	-																	
Other	-	-																	
Printing the graph or saving it as a PNG, JPEG, PDF, or SVG	1. Click the hamburger menu ☰ and select the desired option.																		

Files Table

Immediately below the Browse pie chart is a table that lists the files, the date and time they were created, their title, their source, their category, and associated keywords.

DATE	TITLE	SOURCE	CATEGORY	KEYWORDS
Filter by date	Start typing...	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-cbc9fcd-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 function is available:

FUNCTION	DETAILS
Opening the File Details page for a file	1. Click the name in the Title column.
Changing the number of entries displayed in the table per page	1. Click the paging batch option located to the bottom-right of the table.
Sorting the table by a column	1. Click the column header. 2. To reverse the column sorting order, click the header a second time.
Searching within a column	1. Click within the search box at the top of a column, and enter your search criteria.

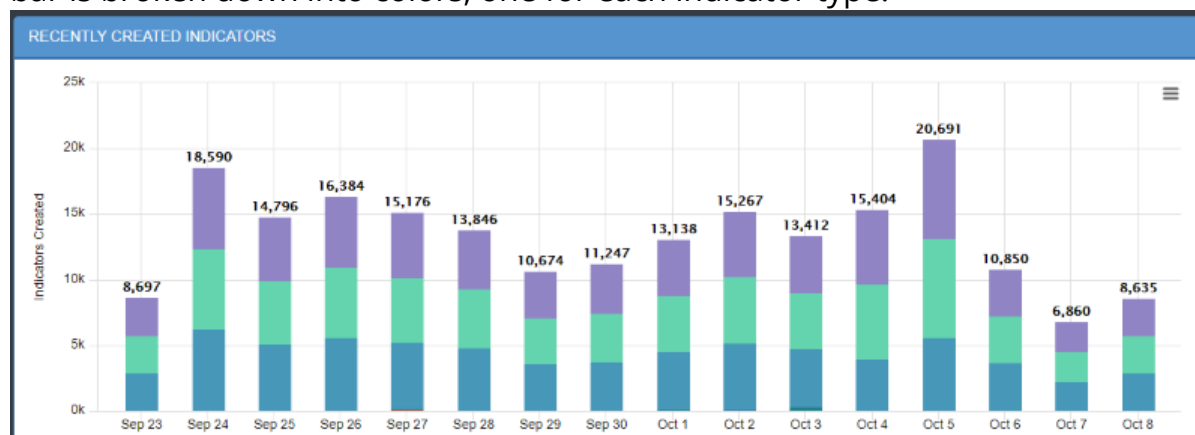
FUNCTION	DETAILS
Downloading a file	1. Click the download  icon.

Indicators

The Indicators Analytics page provides an insight into what indicators have been added to the system within the last 15 days, as well as an overview of how many indicators fall under each indicator type.

Recently Created Indicators Histogram

The histogram is organized by date. Daily indicator totals are at the top of each column. Each bar is broken down into colors, one for each indicator type.



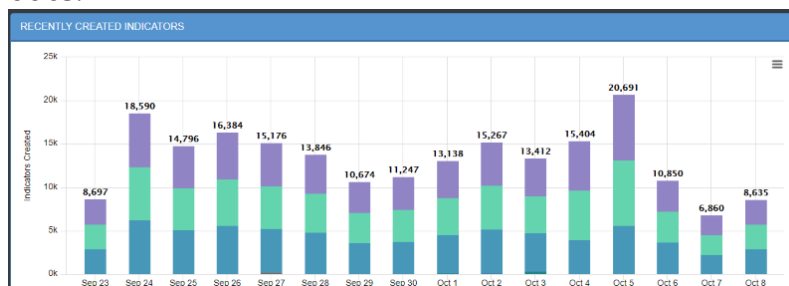
The following functions are available:

FUNCTION

DETAILS

Viewing the number of indicators created each day by type

1. Hover over a colored section to view a popup showing how many attempts of a particular type (for example, MD5, SHA-1, SHA-256) were made on that date.



FUNCTION

Zooming in for a closer view

DETAILS

1. Drag your mouse over a section of the histogram, and your view will be magnified.



2. Click **Reset Zoom** to return to the full histogram.

Printing the histogram or downloading it as a PNG, JPEG, PDF, or SVG file

1. Click the hamburger menu , and select the desired option.

Most Recent 100 Indicators

The Most Recent 100 Indicators list displays the 100 most recently reported indicators.

Most Recent 100 Indicators

Showing 1 to 25 of 100

Row count: 25 ▼

Date ▼	Indicator	Score	Type	Status	Source
Search	Search	Search			Search
10/08/2018 05:30pm	6c1423c4c7906e2da1203b9b550b39b3	0	MD5	Active	CrowdStrike
10/08/2018 05:30pm	4bc0a199fa792b7c54e49db787a9c60f1842a88	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	16a51225f5e762eabc16d76face0041c	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	91dbb6bf198622c95723379042868de	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

1. Click on the different table headings to resort that table by that column.

Search and Filter Table Results

1. Click on one of the search boxes at the top of the columns and enter a keyword to filter the results.

You can use the supplied dropdown selections for the Status and Type columns to filter by system-available values.

Modify the Number of Rows Displayed

1. Click on the **Row Count** icon located to the top-right of the chart and select a new display count from the dropdown.

FUNCTION

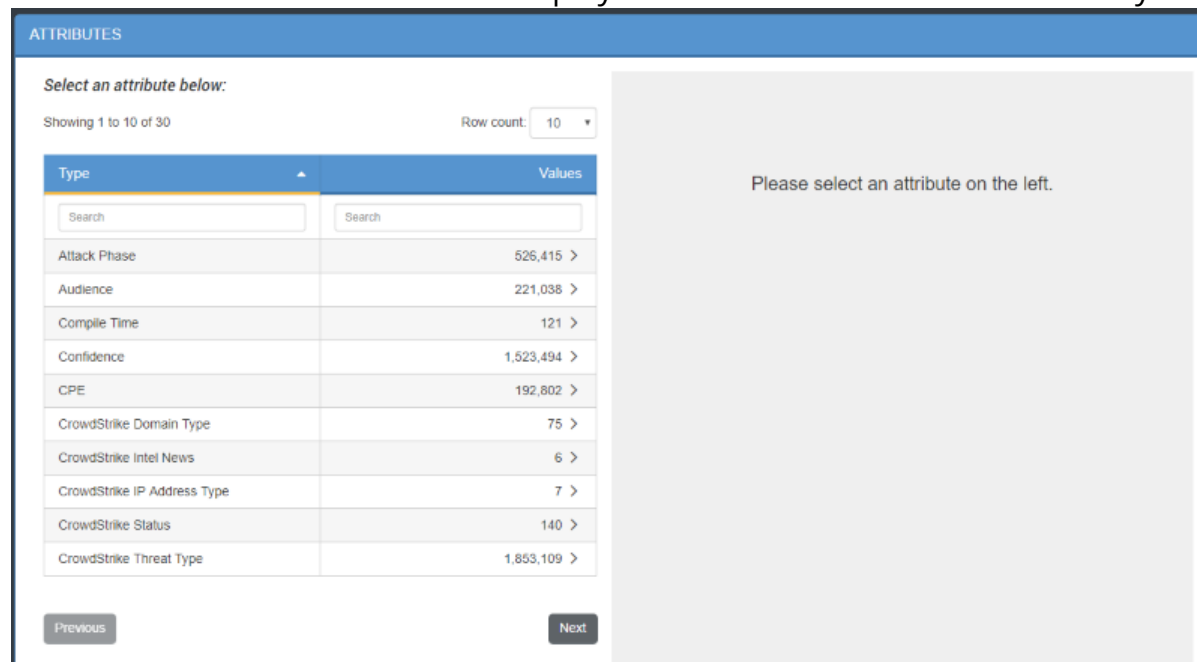
DETAILS

Access the Indicator Details Page for a Specific Indicator

1. 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.



Attributes Table Interface:

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

1. 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

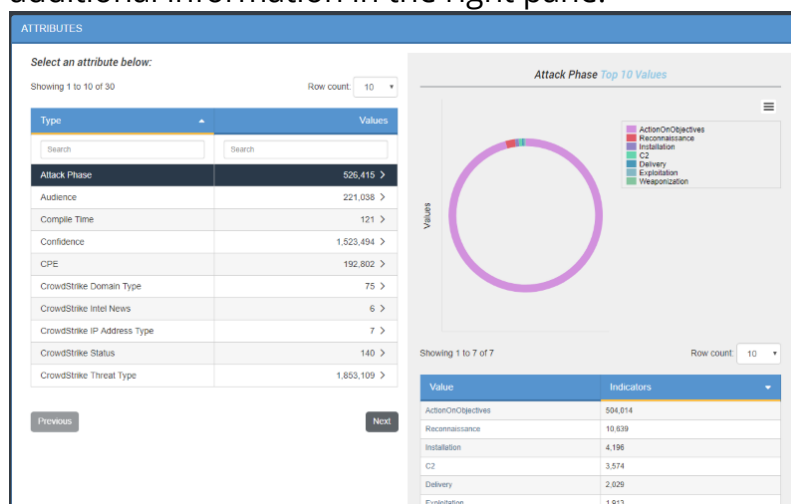
1. Click within the search box at the top of the column, and enter your search criteria.

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.



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.

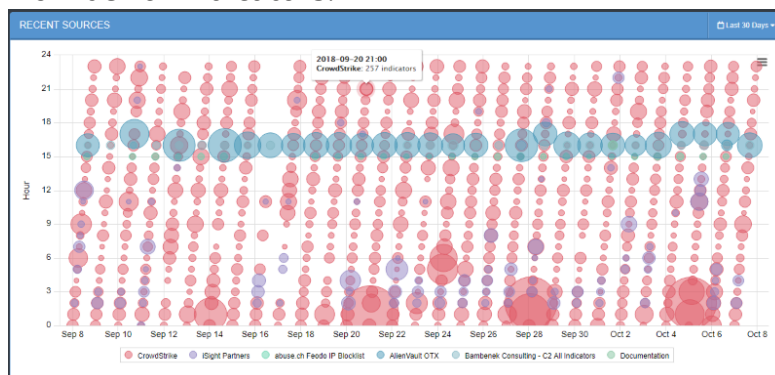
Recent Sources

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:

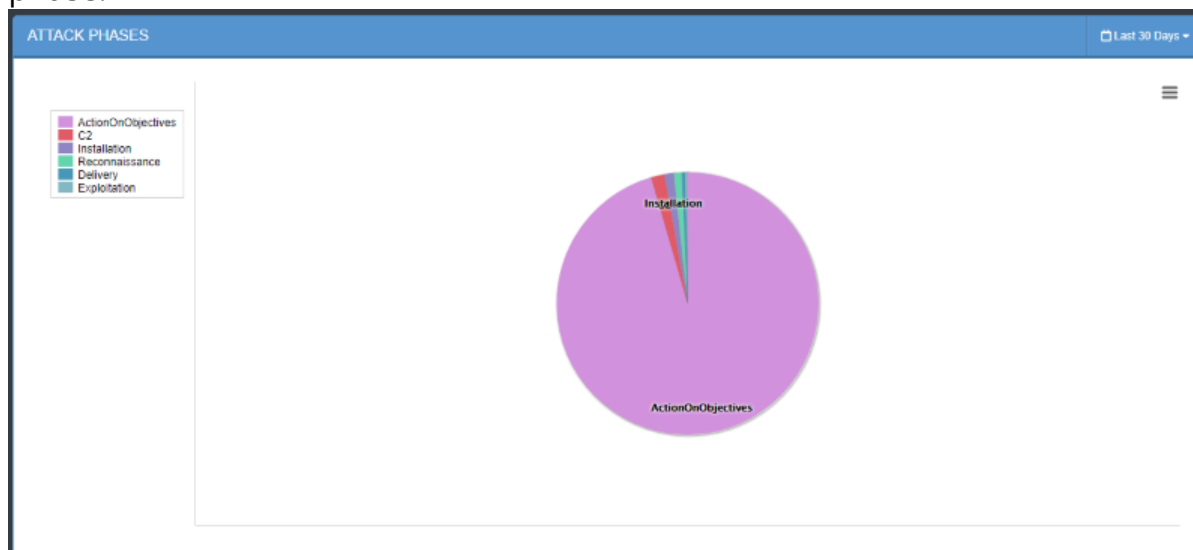
FUNCTION	DETAILS
View the Date and Number of Indicators from a Given Source	1. Hover the mouse over one of the scatter plot circles to view a popup with the Source, Date, Time and Number of Indicators.
Adjust the Date Range of the Information Displayed	The default date range is 30 days. 1. Click the 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.



FUNCTION	DETAILS
	The Source will be removed from the scatter plot and the source in the legend appear grayed out. 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	- Hover the mouse over a portion of the pie chart to view a popup the Attack Phase and number of indicators associated with it. - Clicking on a pie chart section will open the Advanced Search page with the specific filter settings used for that selection.

FUNCTION	DETAILS
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 ◦ 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.

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:

```
<> 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 be 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. 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.

SCENARIO	DETAILS
	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. 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.

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 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
```

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 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 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.

Orphaned Attribute Purge

The following command allows you to purge orphaned attributes:

- **Command Name:** `threatq:purge-orphaned-attributes``>`
- **Command Options:** attribute - a - required array - attribute name(s) to filter on, wildcard * allowed



You can only delete attributes that have no active relationships for any object.

Dashboards

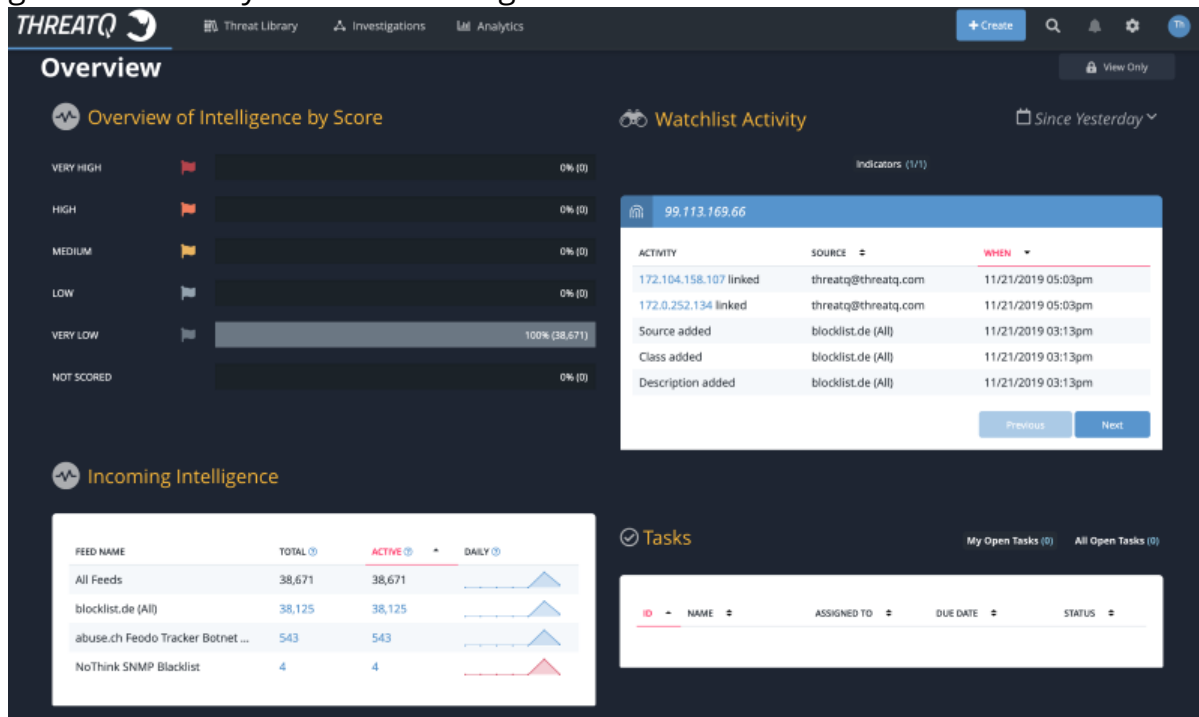
The ThreatQ dashboard serves as your landing page when you log in to ThreatQ.

The serves as your default dashboard.

Users with roles of Primary Contributor, Administrators, and Maintenance can create [custom dashboards](#) that be shared with other users.

Default Dashboard

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



Widgets include:

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

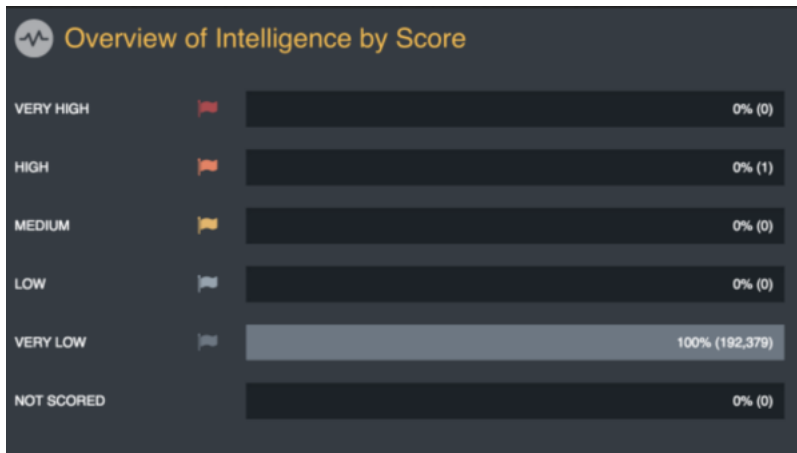
Overview by Intelligence Score

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

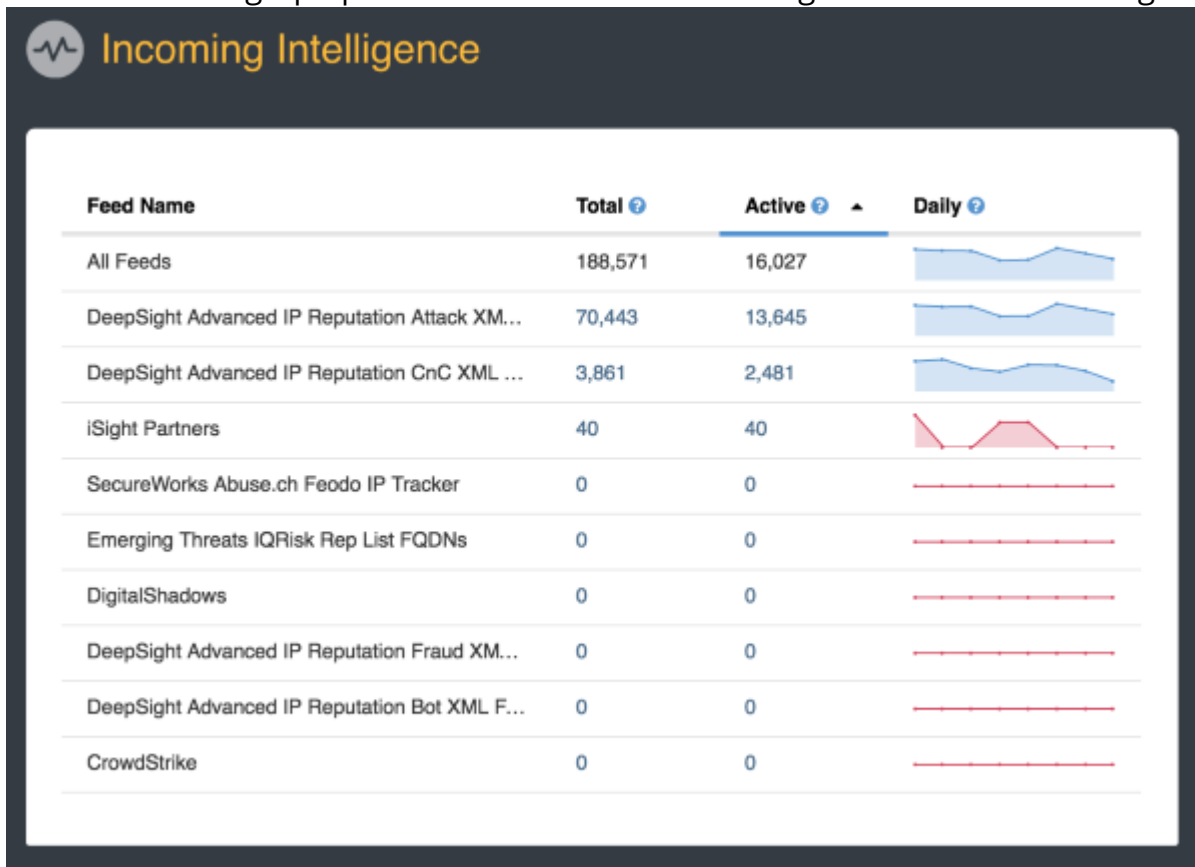
- Not Scored

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



Incoming Intelligence

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



The system categorizes threat intelligence by:

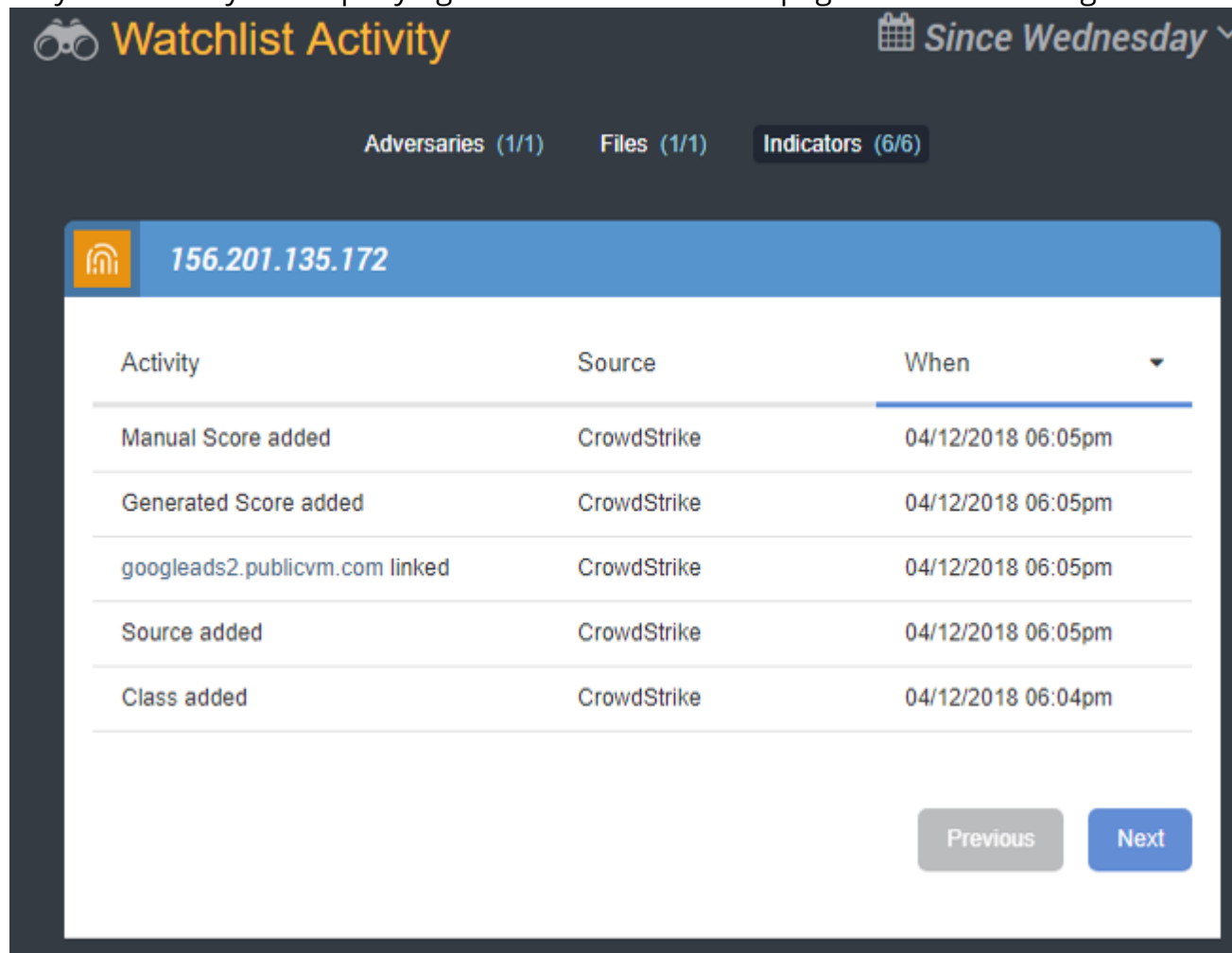
- Feed Name

- Total number of indicators reported by a source
- Indicators reported by a source with a status of active
- All indicators reported by a source per day (includes existing indicators)

Clicking on the **Total** and Active values will navigate you to the Threat Library Advanced Search page with the appropriate filters applied

Watchlist Activity

This dashboard section provides a view of the intelligence data that you selected to watch. You may click on any accompanying link to view the details page of the item being watched.



The screenshot shows the 'Watchlist Activity' section of the ThreatQ dashboard. At the top, there's a header with the title 'Watchlist Activity' and a date filter 'Since Wednesday'. Below this, there are three tabs: 'Adversaries (1/1)', 'Files (1/1)', and 'Indicators (6/6)'. The 'Indicators' tab is selected. Underneath, there's a blue bar with a magnifying glass icon and the IP address '156.201.135.172'. Below this bar is a table with three columns: 'Activity', 'Source', and 'When'. The table contains five rows of activity data. At the bottom right of the table area, there are 'Previous' and 'Next' buttons.

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.

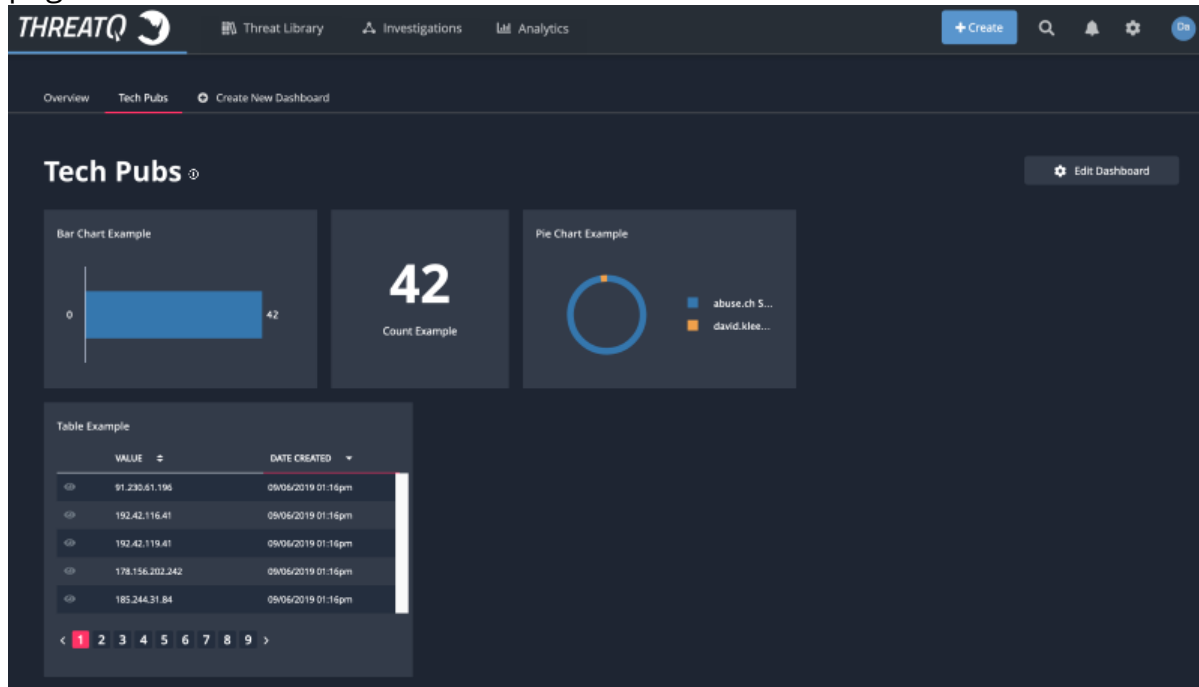
Tasks

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.

Widget Options

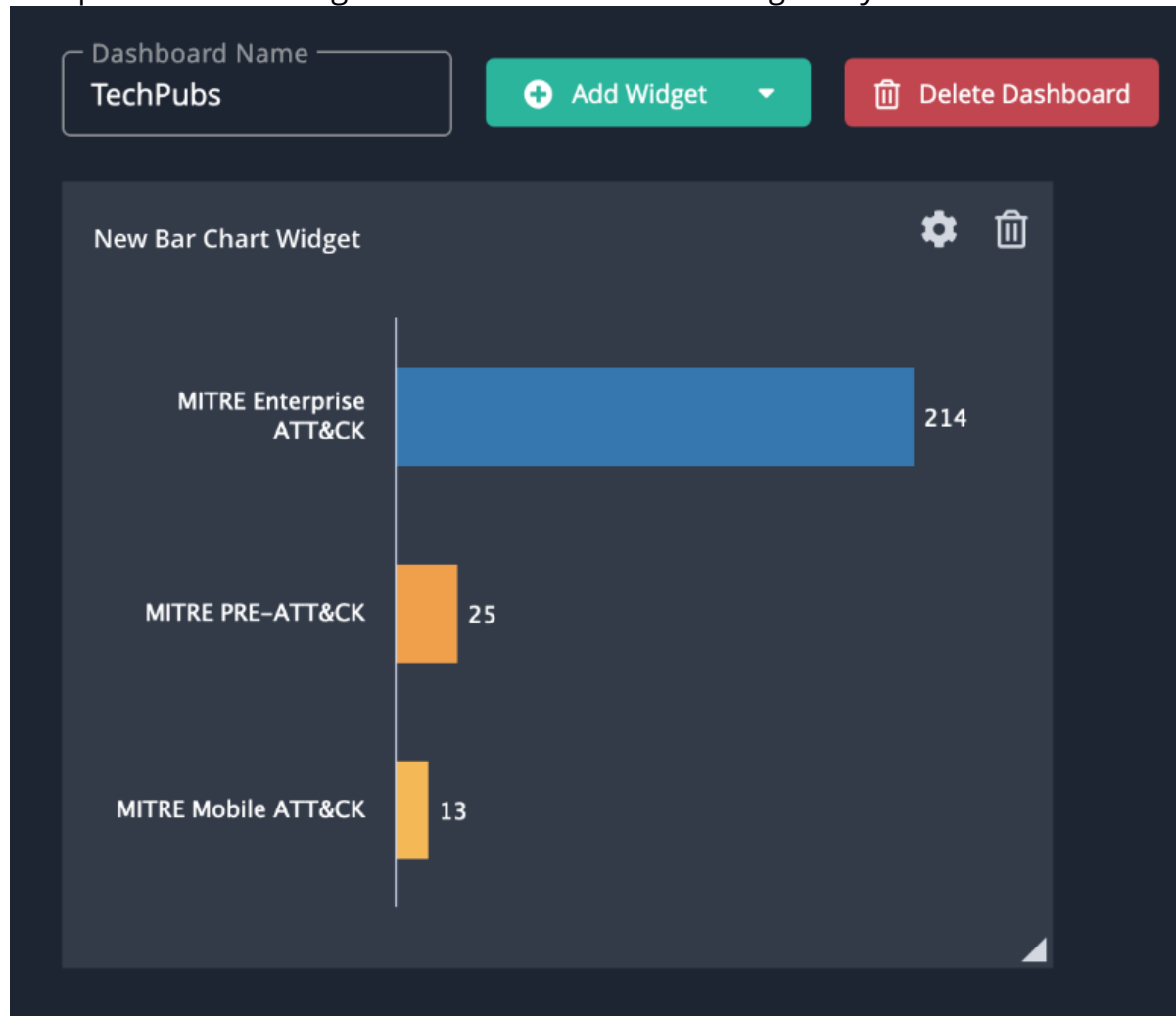
You can add the following widgets to your custom dashboards: Bar Chart, Description, Line Chart, Pie Chart, Count, and Table.

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.



FIELD

DESCRIPTION

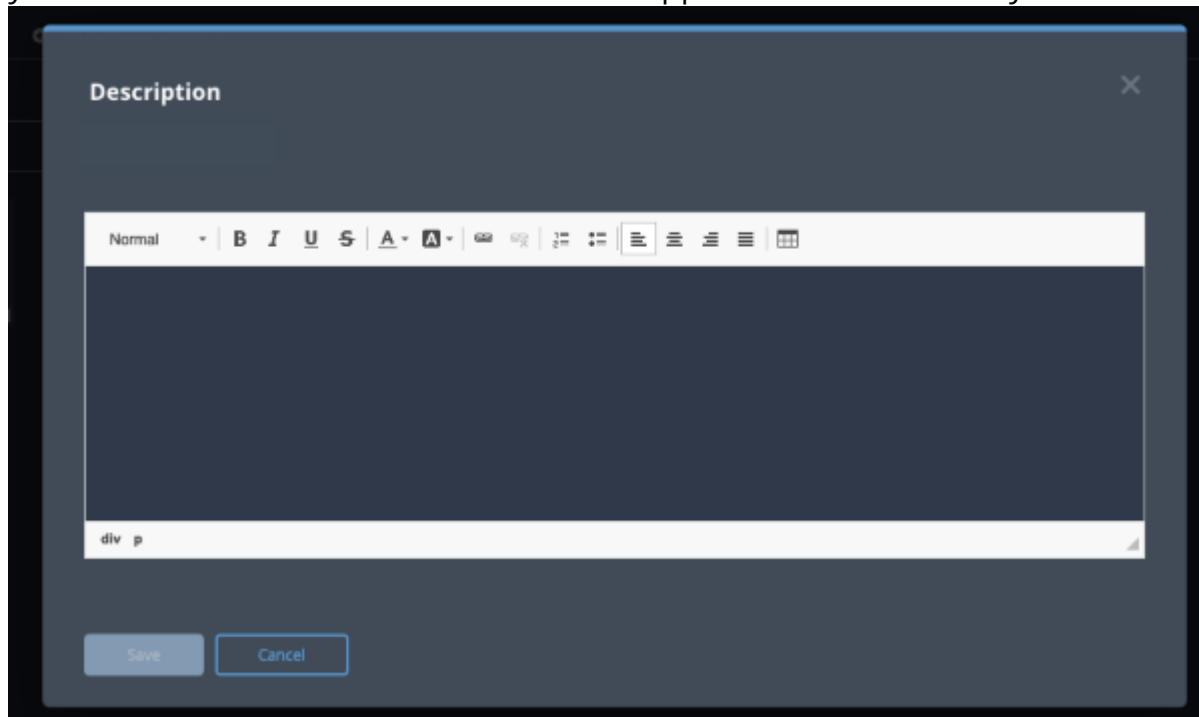
Title

The title that will appear above the widget.

FIELD	DESCRIPTION
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.
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

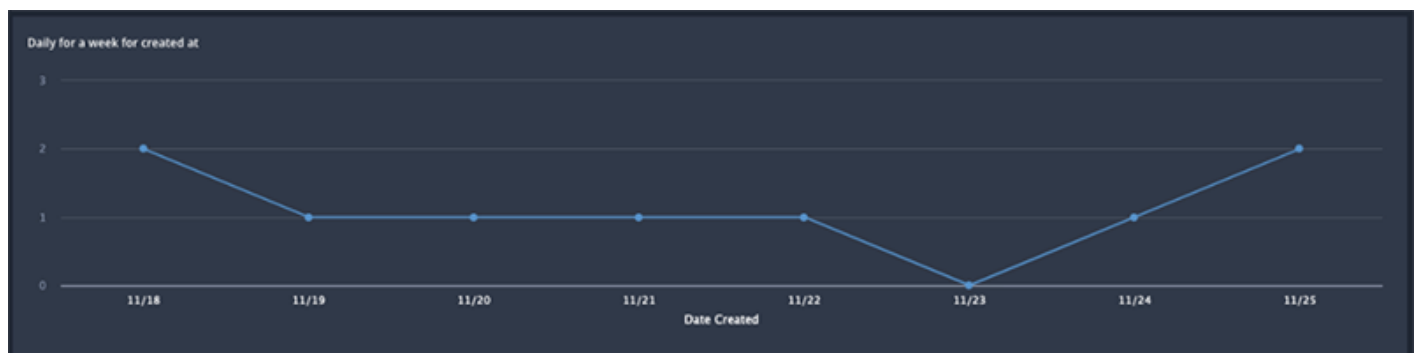
The Description widget allows you to provide further context and additional instructions for your custom dashboard. You can use the supplied editor to format your content.



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)

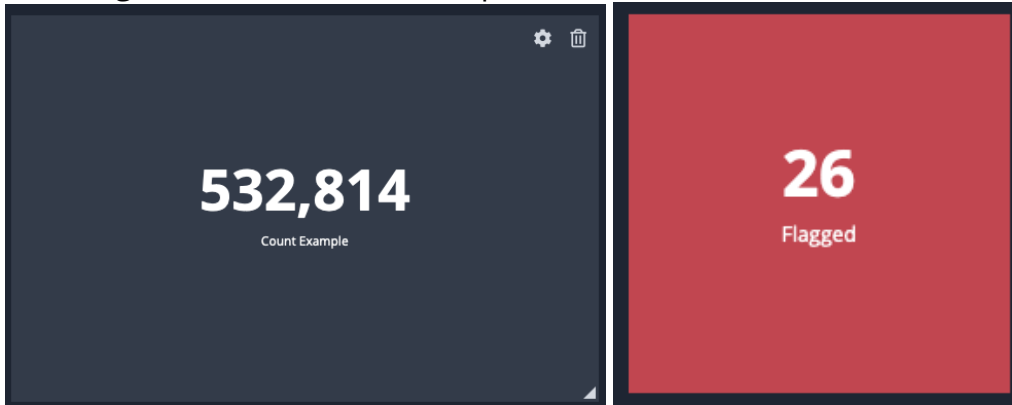


Complete the following fields to add a line chart widget to your custom dashboard.

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:

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.

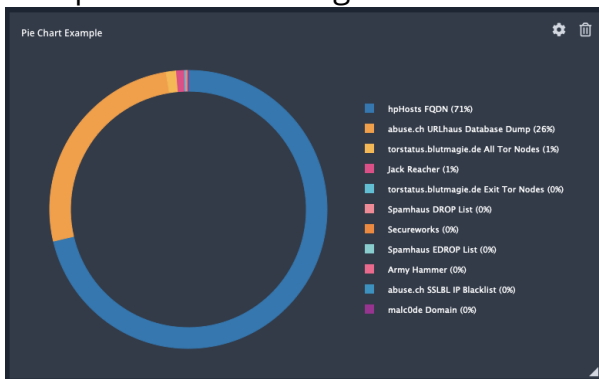
FIELD	DESCRIPTION
Emphasize Data Using Color	Check this box to use different colors to highlight the widget if the count is less than or greater than a specific value. If checked, you will be prompted to select a count value and background color.

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.

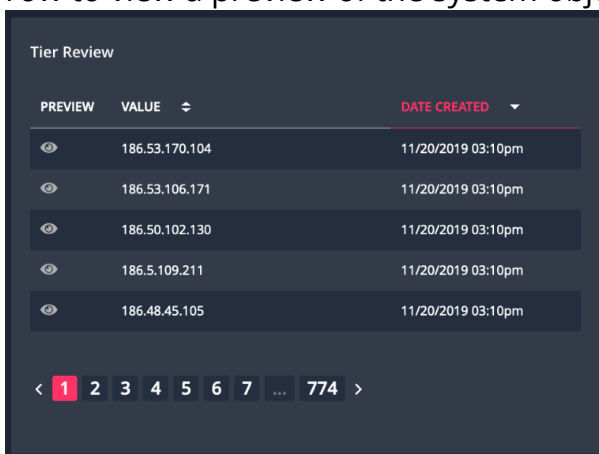


FIELD	DESCRIPTION
Title	The title that will appear above the widget.
Automatically Update	The refresh time for the data. Options include: • 15 Minutes • 30 Minutes • 60 Minutes

FIELD	DESCRIPTION
	• 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.



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

< 1 2 3 4 5 6 7 ... 774 >

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.
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).

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.

Adding a Dashboard to Your View

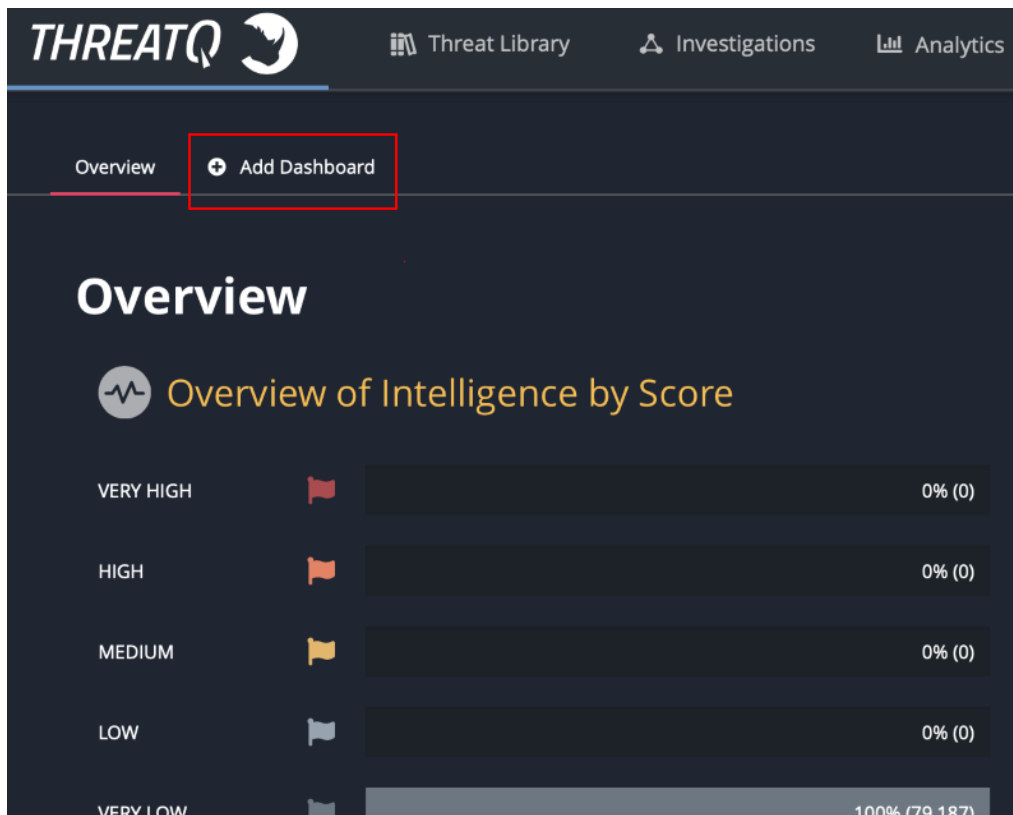
You can add dashboards that have been shared with you as well as your own private dashboards that not currently part of your view.



You cannot edit nor delete a dashboard that has been shared with you.

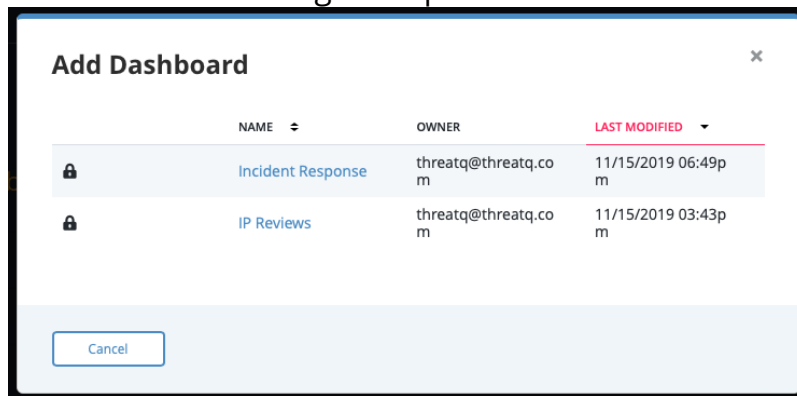
Perform the following steps to add a dashboard to your view:

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



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

The dashboard dialog box opens.



The dialog box contains a list of dashboards that have been shared with you and your own dashboards that are not currently part of your view.

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

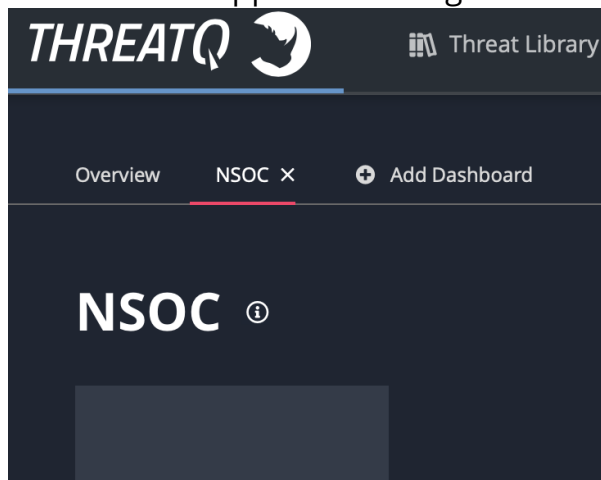
Removing a Dashboard from Your View

You can remove a shared dashboard created by another user from your view as well as your own dashboards. The process listed below does not delete the dashboard from the platform. See the [Dashboard Management](#) topic for instructions on how to delete a dashboard.

Perform the following steps to remove a dashboard to your view:

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

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



2. Click on the **X** to remove the dashboard from your view.

Changing Dashboard Order

You can change the order of dashboard tabs listed in your view, including the default Overview tab.

Perform the following steps to add a dashboard to your view:

1. Navigate to the ThreatQ landing page.
2. Click and hold the mouse down over a dashboard tab.
3. Drag the tab to your desired order and release the mouse button.



Order changes will automatically save.

Dashboard Sharing

You have the ability to configure how your dashboards are shared across the ThreatQ platform.

ThreatQ provides three sharing options:

SHARE OPTION	DESCRIPTION
Private	Only the dashboard owner can view and edit the dashboard. This is the default sharing setting.
Privately Shared	Only individuals selected by the dashboard owner can add the dashboard to their view. Only the dashboard owner can edit the dashboard and the sharing control.
Public	All users can add the dashboard to their view. Only the dashboard owner can edit the dashboard. All custom dashboards created before ThreatQ version 4.25 will be set to Public by default.

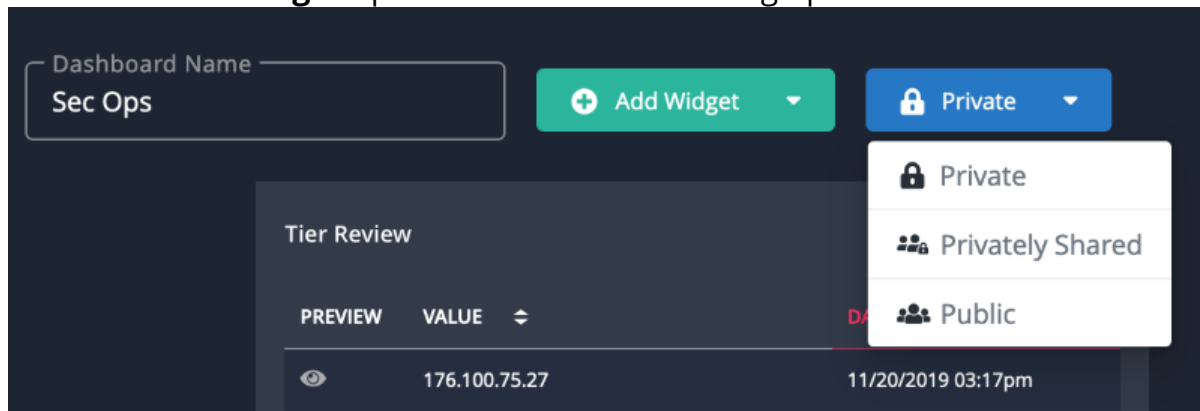
Setting Dashboard Sharing

You can update sharing settings for a dashboard at any time.

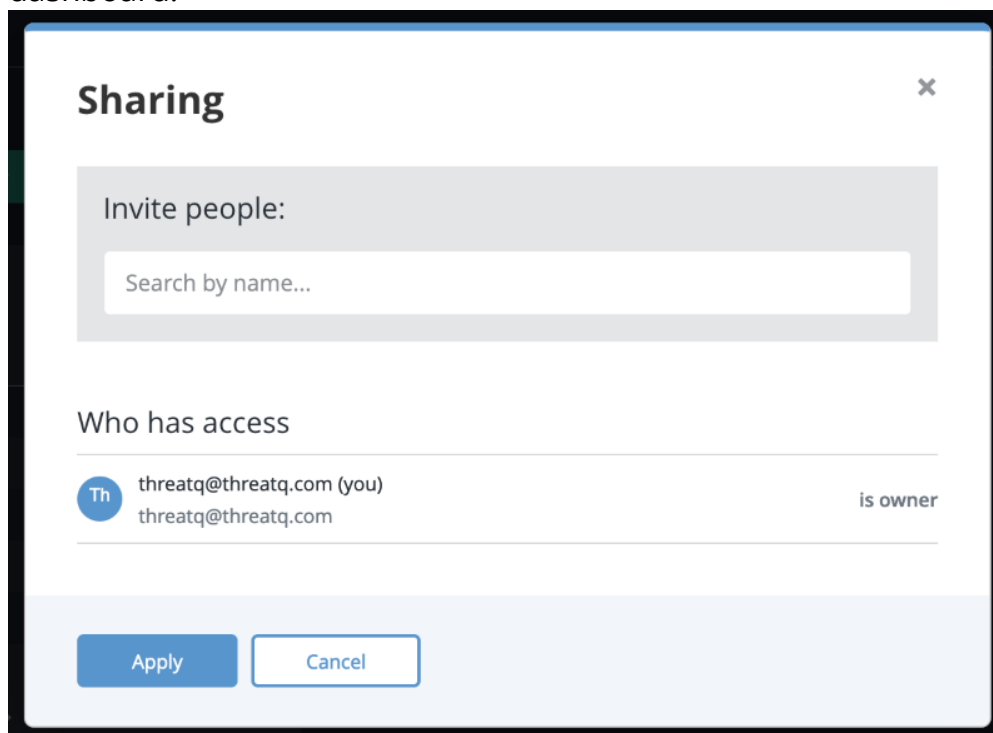
To update a dashboard's sharing setting:

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

- Click on the **Sharing** dropdown and select a sharing option.



- If you selected **Private** or **Public**, click on **Done Editing** to save changes. If you selected **Privately Shared**, continue to step 4.
- The **Sharing** dialog box will open. You can view who currently has access to the dashboard.



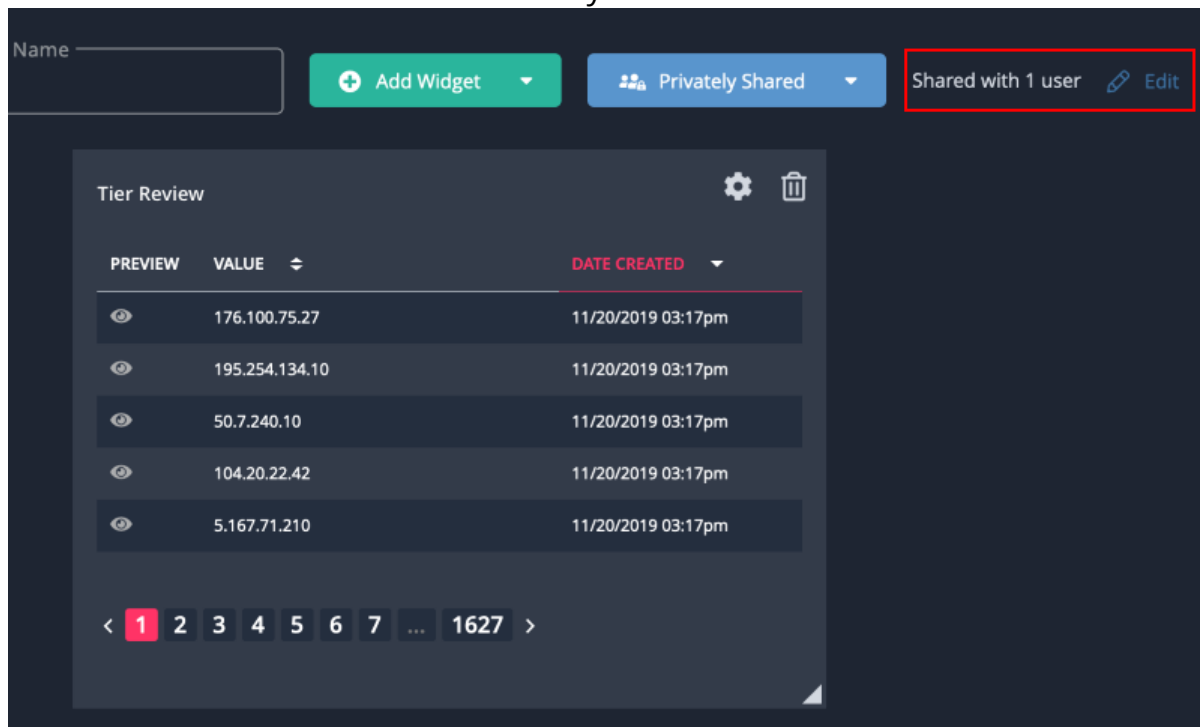
- Enter a user's name in the **Invite People** field. The platform will return system users that fit the name criteria. Click on the correct user.
- The user will now appear under the **Who has access** section of the dialog box.



Repeat steps 5-6 to share with additional users.

- Click on **Apply**.

You will now see **Shared with x user** text next to the sharing dropdown where the x is the number of users the dashboard is currently being shared with. You will also see an **Edit** link next to the text that will allow you to further edit the list of users.



8. Click on **Done Editing** to save changes.

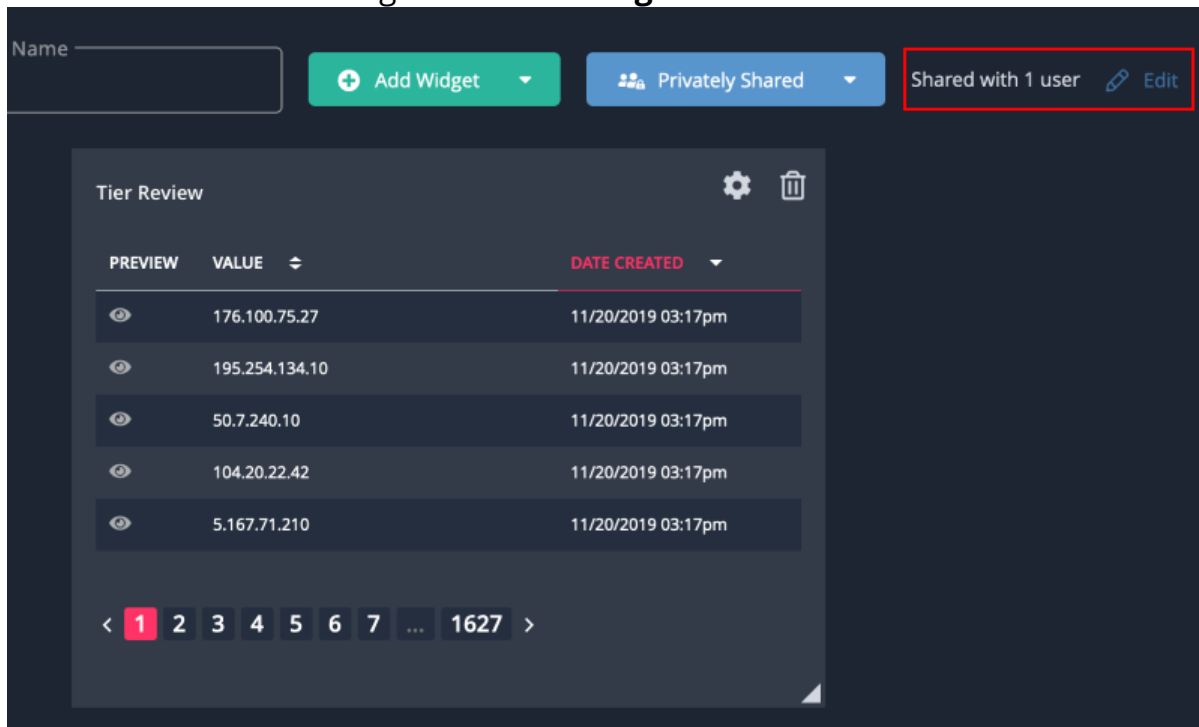
Editing Privately Shared Users

You can add and remove user access for privately shared dashboard.

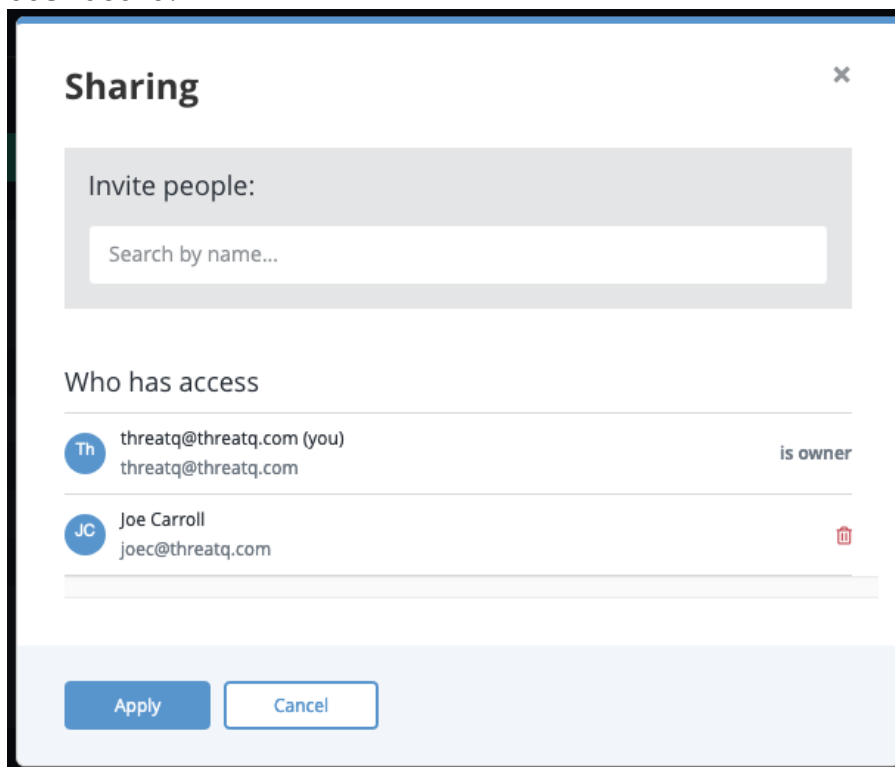
To edit the privately shared list of users:

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

- Click on **Edit** link to the right of the **Sharing** button.



The Sharing dialog box will open. You can view who currently has access to the dashboard.



- Use the **Invite People** field to share with additional users.
- Click on the **Delete** icon next to user under the **Who has access** section to revoke an individual's access.

5. Click on **Apply** and then **Done Editing** to save the changes.

Shared Dashboards of a Deleted User

In the scenario where a user with shared dashboards is deleted from the platform, ThreatQ will automatically reassign dashboard ownership to another user. This ensures that users can continue using those shared dashboards. See the [Dashboard Management](#) topic for more details.

Dashboard Management

Users with permission roles of Primary Contributor Access, Administrative Access, Maintenance Account can add, edit, and delete custom dashboards. See the [Dashboard Sharing](#) topic for dashboard sharing information.

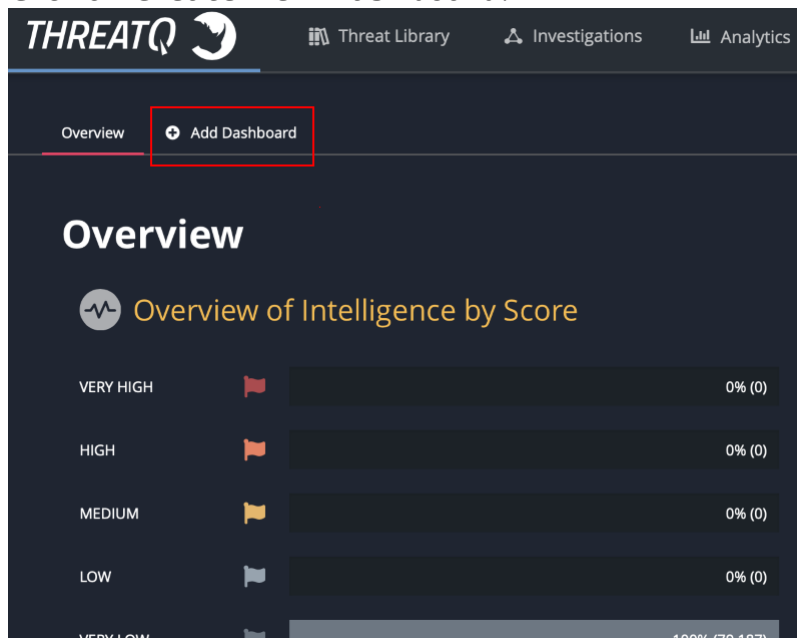


Users with the Read-Only Access role cannot create custom dashboards but can add shared dashboards to their view.

Creating a Dashboard

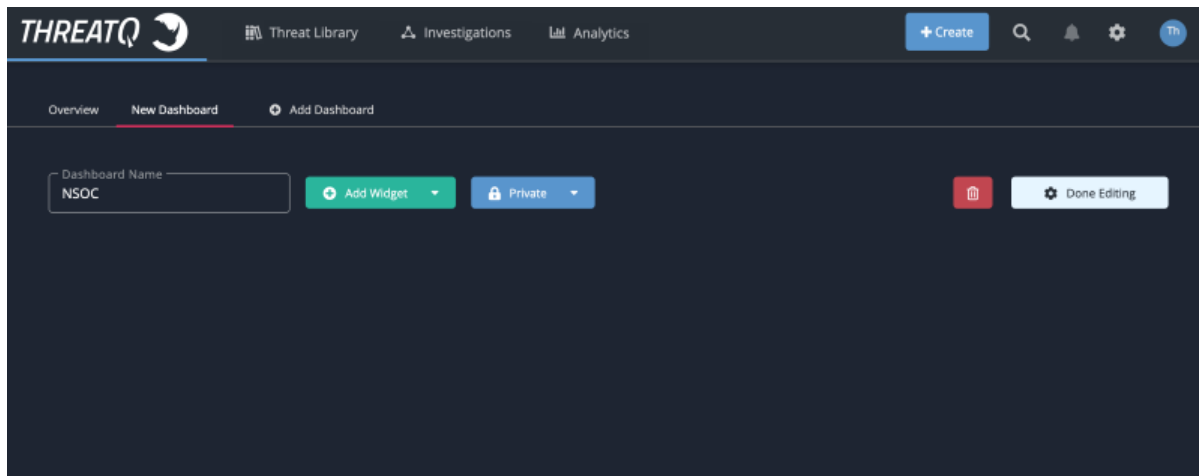
Perform the following steps to create a custom dashboard:

1. Navigate to the ThreatQ landing page.
2. Click on **Create New Dashboard**.

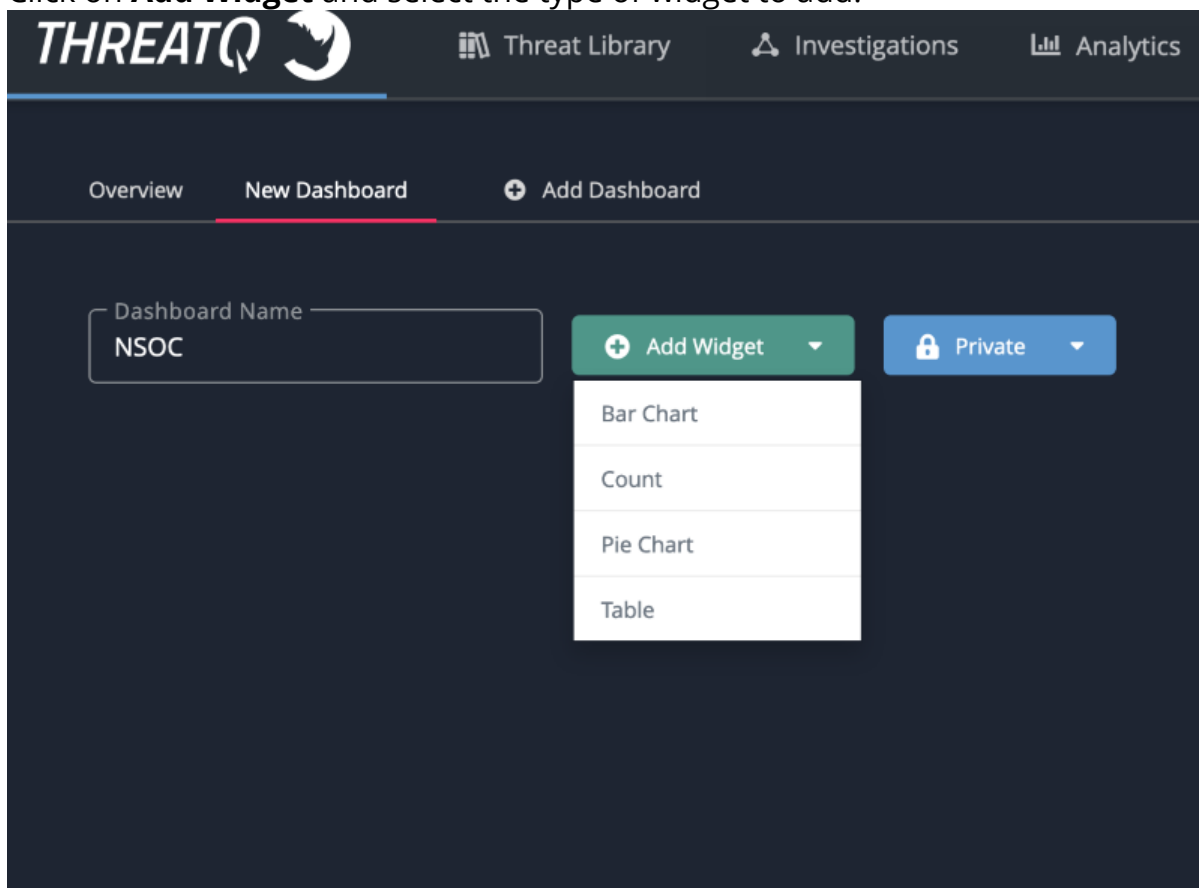


If there are available shared dashboards or if you have any of your own dashboards that are not part of your current view, the **Create New Dashboard** link will be replaced with **Add Dashboard**. Clicking on the **Add Dashboard** link will open the dashboard dialog box with a list of available dashboards not current part of your view. Click on the **Create New Dashboard** link at the bottom of the dialog box.

3. Enter the **Dashboard Name**.



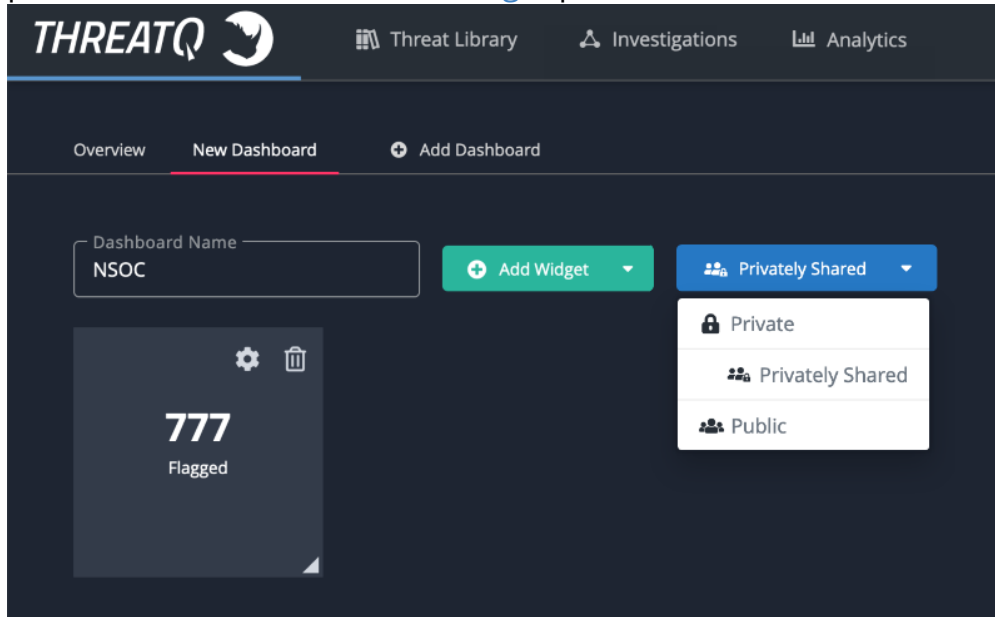
4. Click on **Add Widget** and select the type of widget to add.



5. After adding a widget, you can resize it by clicking and dragging the mouse on the bottom-right grey corner.

6. You can move the widget around the dashboard by clicking on the widget header and dragging it around the page.

- Click on the **Sharing** dropdown and select whether the new dashboard will be private or public. See the [Dashboard Sharing](#) topic for more details.

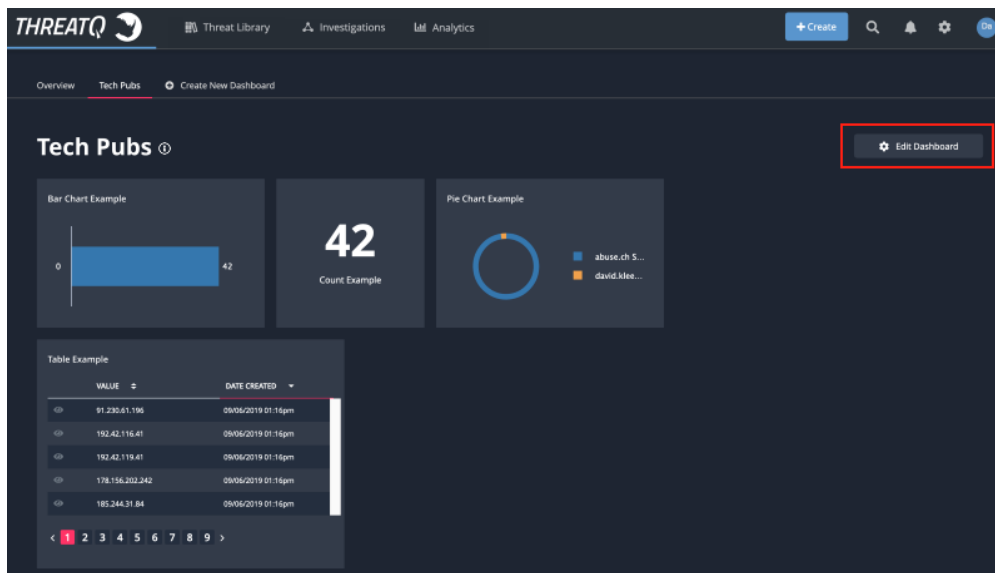


- Click on **Done Editing** to save the dashboard.

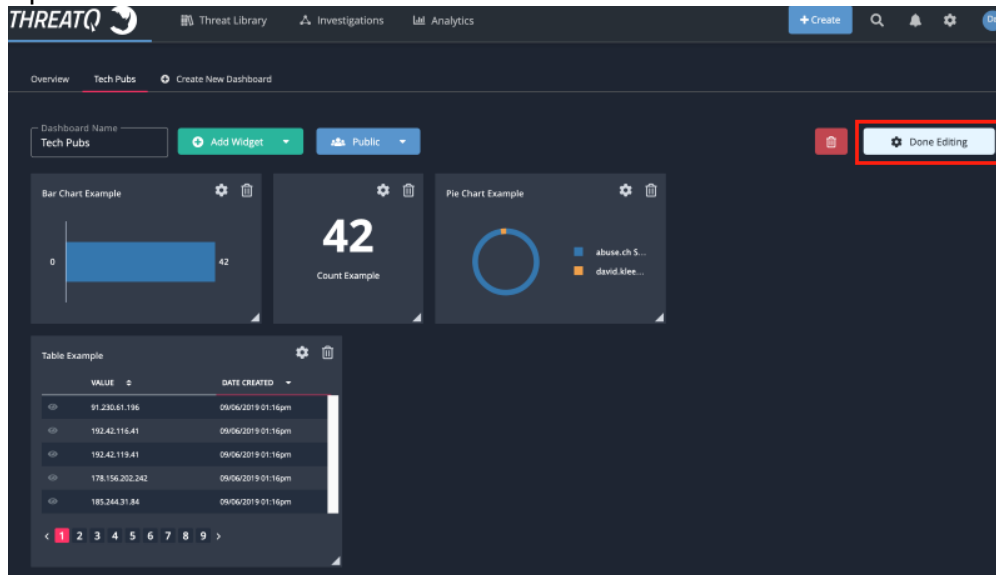
Editing a Dashboard

You can only edit a Dashboard that you have created. If you are viewing a dashboard created by another user, you will see a **View Only** icon in place of the **Edit Dashboard** link.

- Switch to the custom dashboard to edit.
- Click on **Edit Dashboard**.



3. Make your desired changes to the dashboard then click on **Done Editing** to save all updates.



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

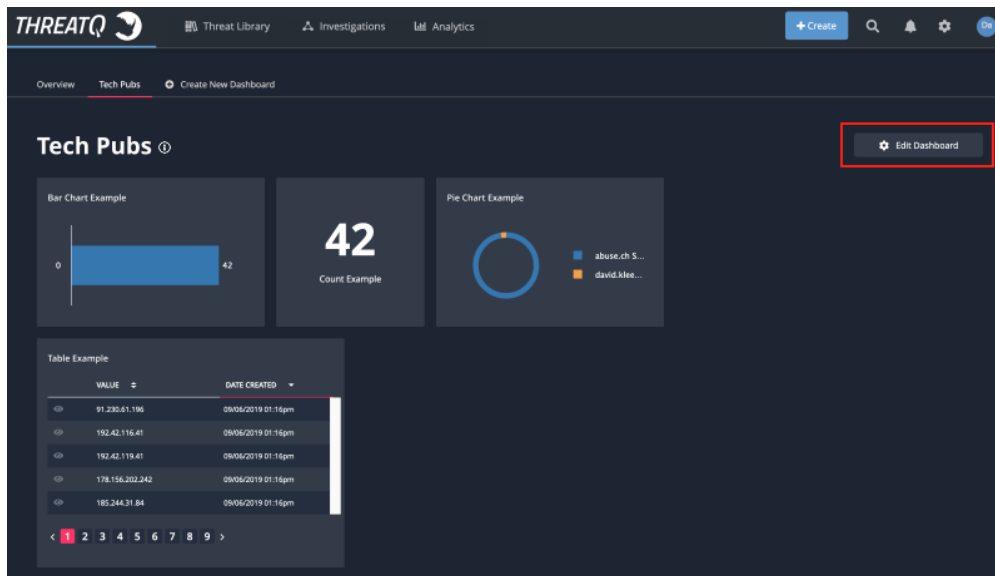
Deleting a Dashboard

This action will delete the dashboard from the platform. You can also remove a dashboard from your view without completely deleting it from the platform. See the [User View Management](#) topic for more details.

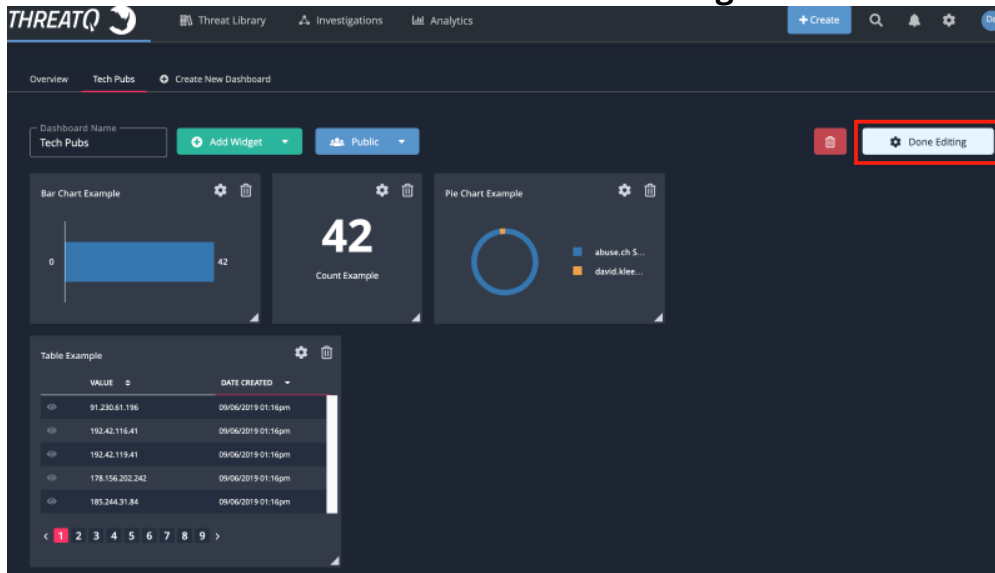
You can not delete the default system dashboard or dashboards created by other users.

1. Switch to the custom dashboard to edit.

2. Click on **Edit Dashboard**.



3. Click on red delete icon next to the **Done Editing** button.



Reassigning a Dashboard of a Deleted User

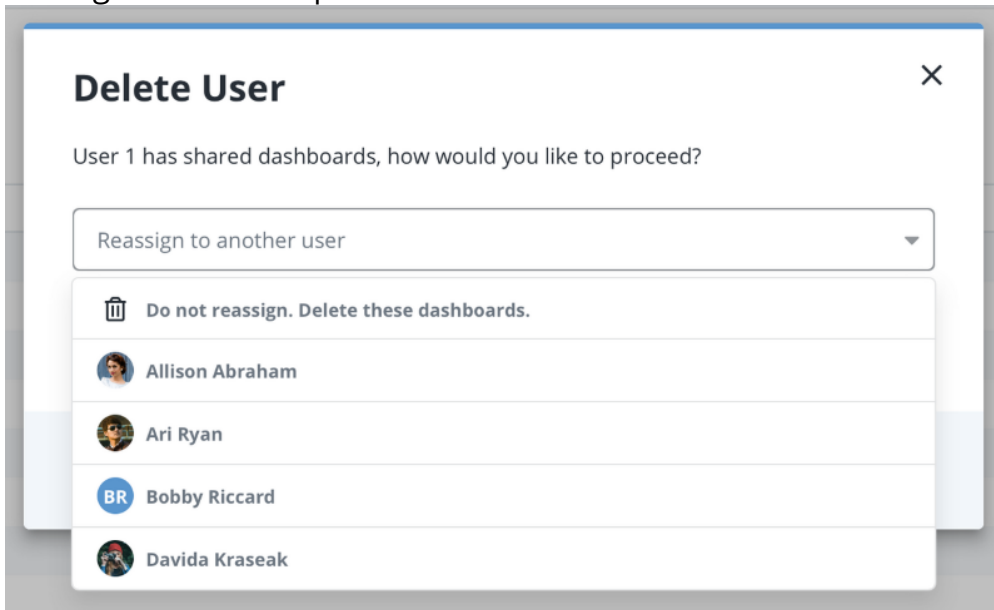
Publicly and Privately Shared dashboards that are owned by a user being deleted from the platform can be reassigned during the deletion process.



Private Dashboards will be deleted along with the user.

When deleting a user, the ThreatQ platform will notify the administrator if the user has any shared (sharing setting of Public or Privately Shared) dashboards in use. The administrator at that point can decide whether to delete the dashboards associated with that user or

reassigned ownership to another user.



See the [Managing User Accounts](#) topic for more details.

Data Management

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

SECTION	DETAILS
Automatic Expiration	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 Whitelist feature.

Automatic Expiration

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 Automatic Expiration Page

1. From the navigation menu, click on settings icon  and select **Data Management**.

The Data Management page will open with the Automatic Expiration tab selected by default.

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

OPTION

DESCRIPTION

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 Exceptions

Exceptions

INDICATOR TYPE	POLICY
Binary String	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. Navigate to the **Automatic Expiration** tab under **Data Management**.
2. Locate the source.
3. Click **Exceptions** to expand the option.

The Exceptions option menu opens.

Data Management

Whitelisted Indicators **Automatic Expiration** Scoring TLP

Automatic Expiration

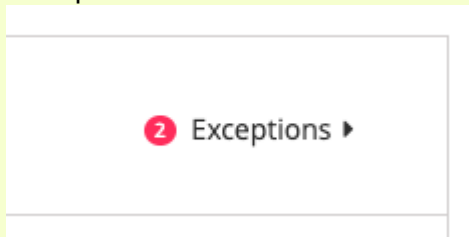
Unburden your team from the task of manually deprecating intelligence. Based on a set of criteria defined and controlled by you, threat intelligence will automatically expire as it becomes less relevant to your team and infrastructure. [How it works](#)

Search for a source...

abuse.ch Feodo Tracker Botnet C2 IP Blocklist	Don't automatically expire	Exceptions ▶
admin@threatq.com	Don't automatically expire	Exceptions ▶



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	1. On 10/1, Source A reports the indicator and the expiration date is set to 10/8.

SCENARIO	DESCRIPTION
is reported by Source B (with an expiration policy of 10 days).	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 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.

SCENARIO	DESCRIPTION
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

As indicators are added to the system, ThreatQ's scoring algorithm automatically calculates and assigns a score based on the weighting you established.

By configuring scoring, you can filter through the millions of indicators it may have collected to focus on the 10% that really apply to your environment while still retaining all other indicators and context for threat research.

Accessing the Scoring Algorithm Page

1. From the navigation menu, click on settings icon  and select **Data Management**.

The Data Management page will open with the Automatic Expiration tab selected by default.

2. Click on the **Scoring** tab to load the Scoring Algorithm page.

Scoring Criteria

As you build a scoring algorithm, you influence indicator scores based on the following criteria:

- Indicator Type
- Indicator Source
- Attributes
- Adversary Relationship

Configuring Your Scoring Algorithm

1. Select the criteria tab to influence your scoring.
2. Use the slider to determine the sensitivity of the criterion you select.



By default, the slider is positioned in neutral position, which in isolation produces an indicator score of zero.

3. Use the sliders to increase or decrease the weighting for the criteria.



You may increase the score up to 10, which creates a score of **Very High**. You may also decrease the score, which creates a score of **Very Low**.

The screenshot shows the THREATQ web application interface. The top navigation bar includes the THREATQ logo, a search icon, and links for Threat Library, Investigations, and Analytics. A '+ Create' button and a 'DK' button are also present. Below the navigation bar is the 'Data Management' section, which includes tabs for Whitelisted Indicators, Automatic Expiration, Scoring (selected), and TLP. The 'Scoring Sensitivity Configuration' section is active, displaying a table of indicator types and their corresponding scores. The table has columns for Indicator Type, Indicator Source, Attributes, and Adversary Relationship. The 'Indicator Type' column is filtered by 'Indicator Type...'. The table lists four indicator types: Binary String, CIDR Block, CVE, and Email Address. Each row has a 'DECREASED' slider and an 'INCREASED' slider. The 'Binary String' row has a score of 10, while the others have a score of 0. An 'Apply' button is at the bottom left, and a note states: 'After clicking save, these changes will take time to process and will not immediately take effect.'

Indicator Type	Indicator Source	Attributes	Adversary Relationship
Binary String			
CIDR Block			
CVE			
Email Address			

4. Click on **Apply** to save changes.

Traffic Light Protocol (TLP)

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



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

Designations

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

LIGHT	DESIGNATION	DESCRIPTION
	Red	Not for disclosure, restricted to participants only.
	Amber	Limited disclosure, restricted to participant's organizations.
	Green	Limited disclosure, restricted to the community.
	White	Disclosure is not limited.

TLP Assignment Hierarchy

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

METHOD	DETAILS
Manually Set	Using the Add New Source option when creating an object will allow you to select a TLP designation.

Source
Provided Data

TLP information received from ingested data.

Source Default

Administrators can set a source's default TLP designation. See the [Add TLP to Source](#) section.

No TLP

A TLP designation has not been set for the source.

Access TLP Settings

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

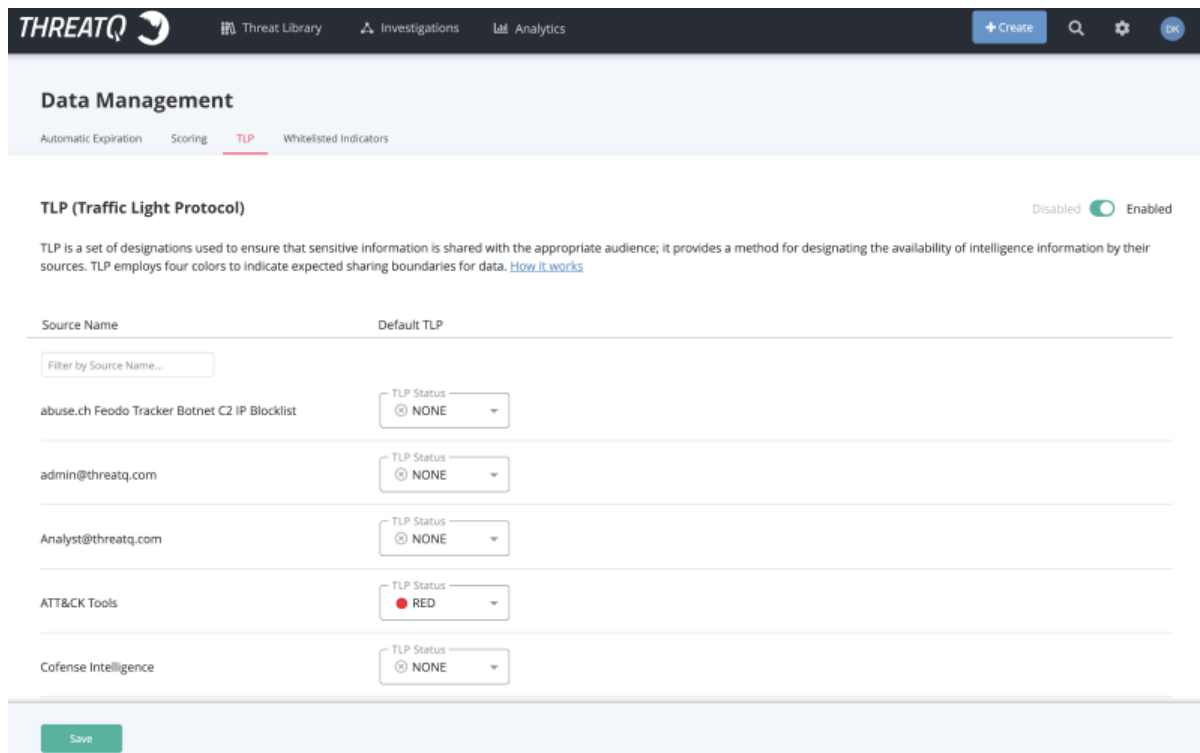
1. From the main menu, select Settings  > **Data Management**.

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

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

The TLP Setting page will open.

3. Click on the **TLP** tab.



Data Management

Automatic Expiration Scoring **TLP** Whitelisted Indicators

TLP (Traffic Light Protocol) Disabled ☒ Enabled

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
Filter by Source Name...	
abuse.ch Feodo Tracker Botnet C2 IP Blocklist	TLP Status ⊙ NONE
admin@threatq.com	TLP Status ⊙ NONE
Analyst@threatq.com	TLP Status ⊙ NONE
ATT&CK Tools	TLP Status ● RED
Cofense Intelligence	TLP Status ⊙ NONE

Save

Configure TLP Visibility

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

Enabled indicates that TLP designations are visible to users.

1. Click on the **Enable/Disable** toggle switch located to the top-right of the TLP page.

Data Management

Automatic Expiration Scoring **TLP** Whitelisted Indicators

TLP (Traffic Light Protocol) Disabled ☒ Enabled

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
Filter by Source Name...	
abuse.ch Feodo Tracker Botnet C2 IP Blocklist	TLP Status ⊕ NONE
admin@threatq.com	TLP Status ⊕ NONE
Analyst@threatq.com	TLP Status ⊕ NONE
ATT&CK Tools	TLP Status ● RED
Cofense Intelligence	TLP Status ⊕ NONE

Save



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

Apply a TLP Designation 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.

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

- Click on **Save**.



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

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.

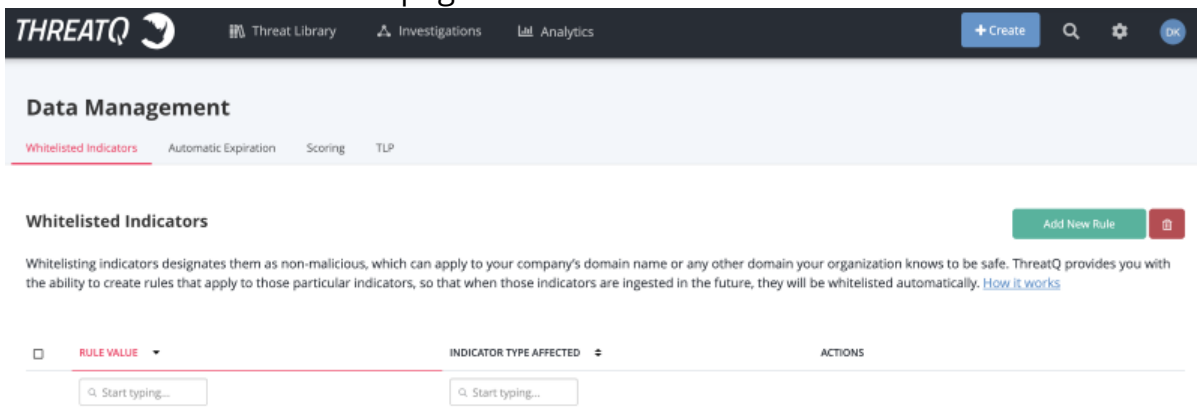
Accessing the Whitelisted Indicator Rules

1. From the navigation menu, click on settings icon  and select **Data Management**.

The Data Management page will open with the Automatic Expiration tab selected by default.

2. Click on the Whitelisted Indicators tab.

The Whitelisted Indicators page will load.



Creating a Whitelisted Rule

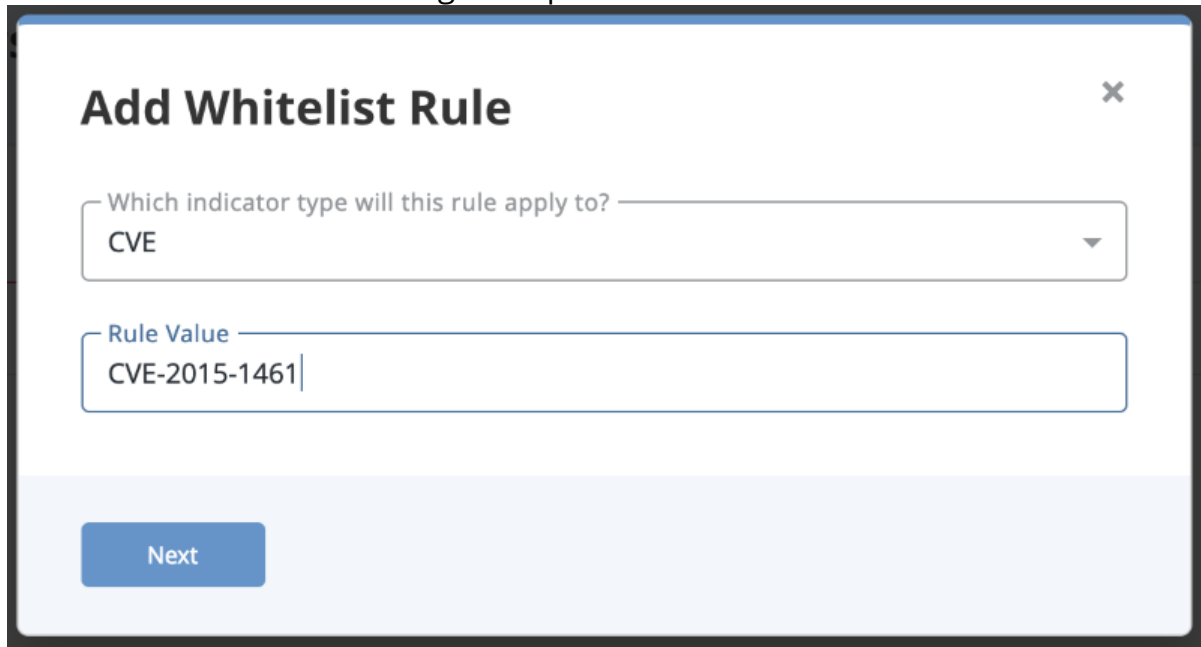


ThreatQ prevents you from creating duplicate whitelist rules through the user interface or an API. If you attempt to do so, the system returns an error message.

From the Whitelisted Indicators Page:

1. Click **Add Rule**.

The Add Whitelist Rules dialog box opens.



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.



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.

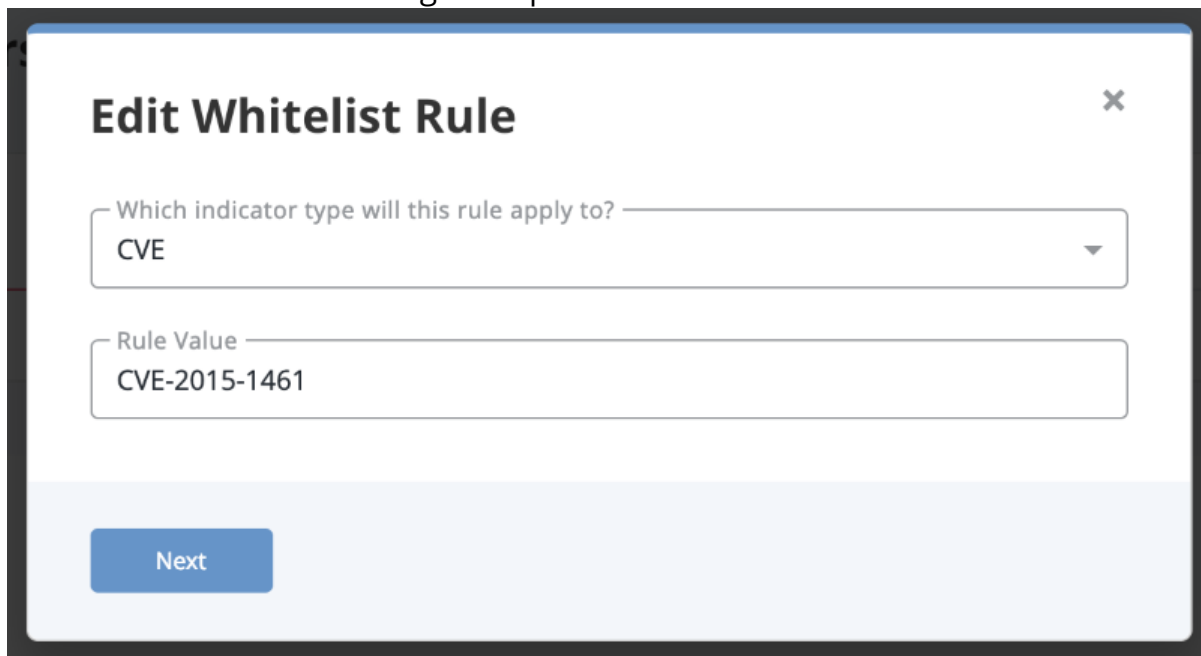


Any new indicators will also have the rule applied to them as they enter the system.

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

Next

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

Affected indicators are listed in the dialog box.



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.

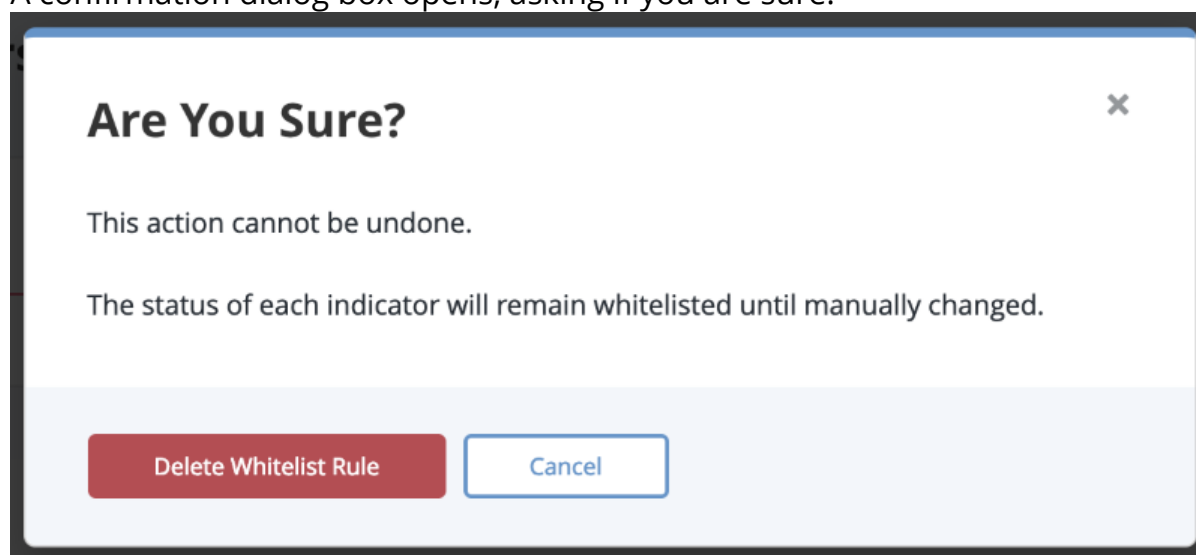


Any new indicators will also have the rule applied to them as they enter the system.

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.



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/>.



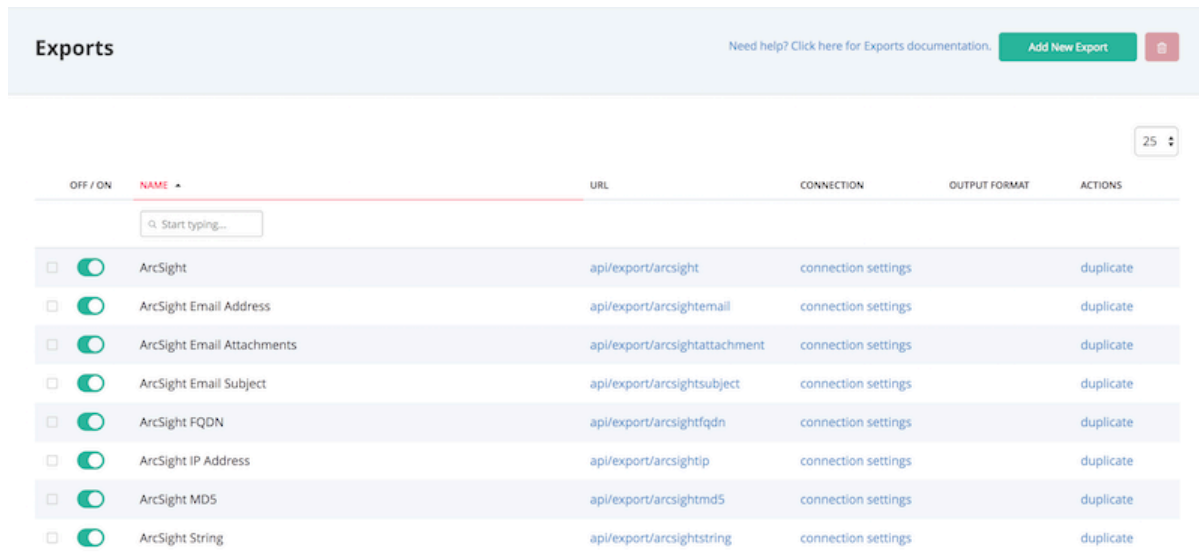
You should NOT attempt to export all of your threat intelligence data with a single export. Attempting to do so will cause system degradation and the export will not complete.

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.



OFF / ON	NAME	URL	CONNECTION	OUTPUT FORMAT	ACTIONS
☐	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** option will only appear if administrators have enabled 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.

Connection Settings ×

Export Name
ArcSight MD5

Token
V9Wm0mRcESFAh1HYTUEkMJPBwhYICpKt

Save Settings

Cancel

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

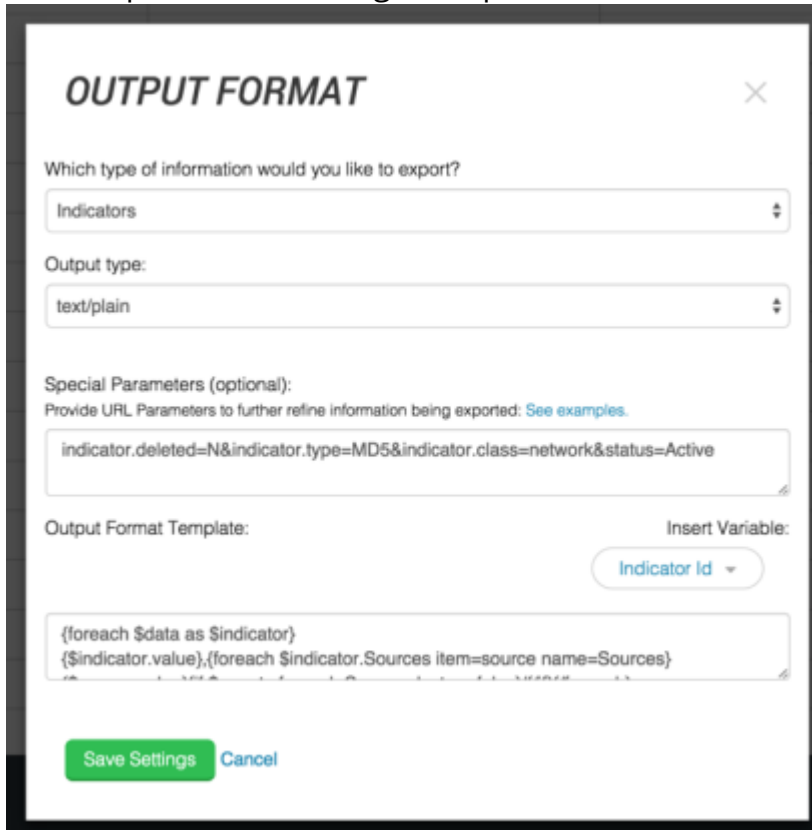
While you cannot edit or delete any of the exports originally supplied by ThreatQ, you can edit exports you have added to ThreatQ or copies of the original exports.

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.

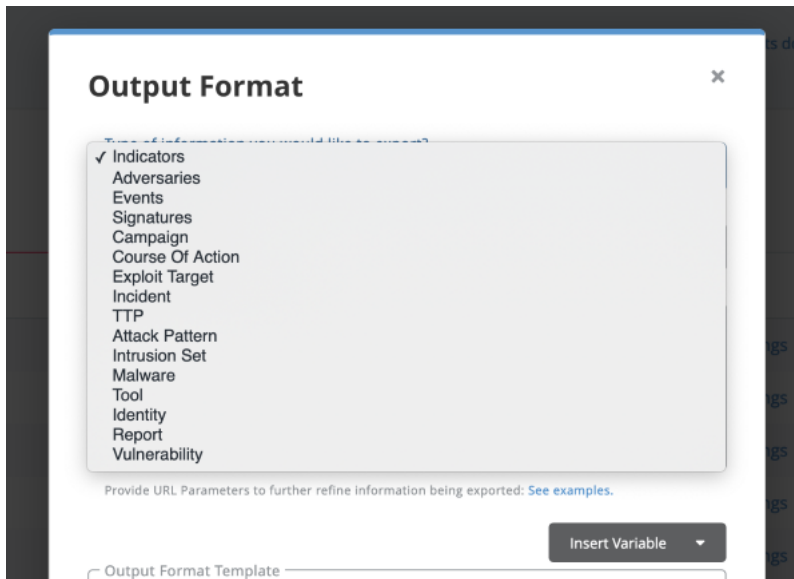


The screenshot shows the 'OUTPUT FORMAT' dialog box. It has a title bar with a close button. The main content area contains the following elements:

- A question: "Which type of information would you like to export?"
- A dropdown menu with "Indicators" selected.
- A label: "Output type:"
- A dropdown menu with "text/plain" selected.
- A section titled "Special Parameters (optional):" with a link "See examples." and a text input field containing "indicator.deleted=N&indicator.type=MD5&indicator.class=network&status=Active".
- A label: "Output Format Template:"
- An "Insert Variable:" button with a dropdown menu showing "Indicator Id".
- A text area containing a JSON-like template:

```
{foreach $data as $indicator}
{$indicator.value},{foreach $indicator.Sources item=source name=Sources}
```
- At the bottom, two buttons: "Save Settings" (green) and "Cancel" (blue).

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



This screenshot shows the 'Output Format' dialog box with the dropdown menu open. The menu lists the following options:

- ✓ Indicators
- Adversaries
- Events
- Signatures
- Campaign
- Course Of Action
- Exploit Target
- Incident
- TTP
- Attack Pattern
- Intrusion Set
- Malware
- Tool
- Identity
- Report
- Vulnerability

The rest of the dialog box is partially visible, showing the "Provide URL Parameters" section and the "Output Format Template" section.

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

- Adversaries
- Indicators

- Attack Pattern
- Campaign
- Course of Action
- Events
- Exploit Target
- Identity
- Incident
- Intrusion Set
- Malware
- Report
- Signatures
- Tool
- TTP
- Vulnerability

5. Select the Output Type from the second dropdown menu.

This sets the content type of the export response to a specific value (e.g. text/plain, text/json). Output Type does not have an impact on how the data is formatted but it does affect the content type within the header of the exported document. For example, if you select Output Type = text/json, when viewing the source of the export, the header will contain a Content Type = text/json attribute.

Please see http://www.w3.org/Protocols/rfc1341/4_Content-Type.html for more information.

6. (Optional) Enter special parameters. There are two ways to do this:

- **Adding Special Parameters within ThreatQ** - One advantage of using this option is that the URL for the export remains non-specific and therefore you can change what is being exported without having to manage each external device individually.
- **Customizing the Output Format Template** - Choosing this option means you lose the ability to have one place to manage what is being exported.



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 putting your cursor where you want the variable to go and selecting the variable you'd like to use from the Insert Variable select box.

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

Important: When formatting your output template, you must wrap all of your declarations within a loop. Please refer to the following as an example:

```
<> {foreach $data as $indicator}

    Your variables go here

{/foreach}
```

The Output Format Template is populated based on your selection.

5. Verify the information entered.
6. Click Save Settings.

Adding Special Parameters

This is where an admin can provide additional parameters to further specify which data will be output via this export. Here are some examples.

**TO EXPORT ALL INDICATORS WITH
AN ACTIVE STATUS****INDICATOR.STATUS=ACTIVE**

To export all CIDR Block indicators
that have an active status

Indicator.Status=Active&Indicator.Type=cidr block

To export all CIDR Block indicators
and IP Addresses that have an
active status

Indicator.Status=Active&Indicator.Type=cidr
block&Indicator.Type=ip address

To export all indicators with a score
greater than or equal to 7

Indicator.Score>=7

A wide range of filtering parameters are available:

> *Indicator*

```
<> indicator.type_id
indicator.status_id
indicator.value
indicator.description
indicator.hash
indicator.last_detected_at
indicator.expires_at
indicator.expired_at
indicator.touched_at
indicator.deleted_at
indicator.deleted
indicator.sources_count
indicator.id
indicator.status
indicator.type
indicator.sincedeleted
indicator.whitelisted *
indicator.score
indicator.created_at
indicator.updated_at
```

```
indicator.Sources  
indicator.Attributes
```

* Using the `indicator.whitelisted=Y` flag allows whitelisted indicators to be exported. It does not filter indicators by the whitelisted status. For that option, use the `indicator.status=whitelisted` flag. Additionally, to include only whitelisted indicators in your export, you will need to use both flags:

```
indicator.status=Whitelisted&indicator.whitelisted=Y
```

>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
```

>Adversary

```
<> adversary.name  
adversary.touched_at  
adversary.deleted_at  
adversary.deleted  
adversary.sources_count  
adversary.id  
adversary.description  
adversary.created_at  
adversary.updated_at
```

```
adversary.Sources
adversary.Attributes
adversary.Indicators
adversary.Adversaries
adversary.Events
adversary.Attachments
adversary.Signatures
adversary.Investigations
adversary.Tasks
adversary.Campaign
adversary.Course_of_action
adversary.Exploit_target
adversary.Incident
adversary.Ttp
adversary.Attack_pattern
adversary.Identity
adversary.Intrusion_set
adversary.Malware
adversary.Report
adversary.Tool
adversary.Vulnerability
```

>Event

```
<> event.type_id
event.title
event.happened_at
event.hash
event.description
event.deleted_at
event.deleted
event.sources_count
event.id
event.type
event.touched_at
event.created_at
event.updated_at
event.Sources
event.Attributes
event.Indicators
event.Adversaries
event.Events
event.Attachments
event.Signatures
event.Investigations
event.Tasks
event.Campaign
event.Course_of_action
event.Exploit_target
event.Incident
```

```
event.Ttp
event.Attack_pattern
event.Identity
event.Intrusion_set
event.Malware
event.Report
event.Tool
event.Vulnerability
```

>Signature

```
<> signature.description
signature.hash
signature.last_detected_at
signature.name
signature.status_id
signature.touched_at
signature.type_id
signature.value
signature.deleted_at
signature.deleted
signature.sources_count
signature.id
signature.status
signature.type
signature.created_at
signature.updated_at
signature.Sources
signature.Attributes
signature.Indicators
signature.Adversaries
signature.Events
signature.Attachments
signature.Signatures
signature.Investigations
signature.Tasks
signature.Campaign
signature.Course_of_action
signature.Exploit_target
signature.Incident
signature.Ttp
signature.Attack_pattern
signature.Identity
signature.Intrusion_set
signature.Malware
signature.Report
signature.Tool
signature.Vulnerability
```

>Campaign

```
<> campaign.value
    campaign.status_id
    campaign.type_id
    campaign.description
    campaign.objective
    campaign.started_at
    campaign.ended_at
    campaign.deleted_at
    campaign.deleted
    campaign.sources_count
    campaign.id
    campaign.status
    campaign.type
    campaign.touched_at
    campaign.created_at
    campaign.updated_at
    campaign.Sources
    campaign.Attributes
    campaign.Indicators
    campaign.Adversaries
    campaign.Events
    campaign.Attachments
    campaign.Signatures
    campaign.Investigations
    campaign.Tasks
    campaign.Campaign
    campaign.Course_of_action
    campaign.Exploit_target
    campaign.Incident
    campaign.Ttp
    campaign.Attack_pattern
    campaign.Identity
    campaign.Intrusion_set
    campaign.Malware
    campaign.Report
    campaign.Tool
    campaign.Vulnerability
```

>Course of Action

```
<> course_of_action.value
    course_of_action.status_id
    course_of_action.type_id
    course_of_action.description
    course_of_action.deleted_at
    course_of_action.deleted
    course_of_action.sources_count
```

```
course_of_action.id
course_of_action.status
course_of_action.type
course_of_action.touched_at
course_of_action.created_at
course_of_action.updated_at
course_of_action.Sources
course_of_action.Attributes
course_of_action.Indicators
course_of_action.Adversaries
course_of_action.Events
course_of_action.Attachments
course_of_action.Signatures
course_of_action.Investigations
course_of_action.Tasks
course_of_action.Campaign
course_of_action.Course_of_action
course_of_action.Exploit_target
course_of_action.Incident
course_of_action.Ttp
course_of_action.Attack_pattern
course_of_action.Identity
course_of_action.Intrusion_set
course_of_action.Malware
course_of_action.Report
course_of_action.Tool
course_of_action.Vulnerability
```

➤ *Exploit*

```
<> exploit_target.value
exploit_target.status_id
exploit_target.type_id
exploit_target.description
exploit_target.deleted_at
exploit_target.deleted
exploit_target.sources_count
exploit_target.id
exploit_target.status
exploit_target.type
exploit_target.touched_at
exploit_target.created_at
exploit_target.updated_at
exploit_target.Sources
exploit_target.Attributes
exploit_target.Indicators
exploit_target.Adversaries
exploit_target.Events
exploit_target.Attachments
exploit_target.Signatures
```

```
exploit_target.Investigations
exploit_target.Tasks
exploit_target.Campaign
exploit_target.Course_of_action
exploit_target.Exploit_target
exploit_target.Incident
exploit_target.Ttp
exploit_target.Attack_pattern
exploit_target.Identity
exploit_target.Intrusion_set
exploit_target.Malware
exploit_target.Report
exploit_target.Tool
exploit_target.Vulnerability
```

>Incident

```
<> incident.value
incident.status_id
incident.type_id
incident.description
incident.started_at
incident.ended_at
incident.deleted_at
incident.deleted
incident.sources_count
incident.id
incident.status
incident.type
incident.touched_at
incident.created_at
incident.updated_at
incident.Sources
incident.Attributes
incident.Indicators
incident.Adversaries
incident.Events
incident.Attachments
incident.Signatures
incident.Investigations
incident.Tasks
incident.Campaign
incident.Course_of_action
incident.Exploit_target
incident.Incident
incident.Ttp
incident.Attack_pattern
incident.Identity
incident.Intrusion_set
incident.Malware
```

```
incident.Report  
incident.Tool  
incident.Vulnerability
```

>TTP

```
<> ttp.value  
    ttp.status_id  
    ttp.type_id  
    ttp.description  
    ttp.deleted_at  
    ttp.deleted  
    ttp.sources_count  
    ttp.id  
    ttp.status  
    ttp.type  
    ttp.touched_at  
    ttp.created_at  
    ttp.updated_at  
    ttp.Sources  
    ttp.Attributes  
    ttp.Indicators  
    ttp.Adversaries  
    ttp.Events  
    ttp.Attachments  
    ttp.Signatures  
    ttp.Investigations  
    ttp.Tasks  
    ttp.Campaign  
    ttp.Course_of_action  
    ttp.Exploit_target  
    ttp.Incident  
    ttp.Ttp  
    ttp.Attack_pattern  
    ttp.Identity  
    ttp.Intrusion_set  
    ttp.Malware  
    ttp.Report  
    ttp.Tool  
    ttp.Vulnerability
```

>Attack Pattern

```
<> attack_pattern.value  
    attack_pattern.status_id  
    attack_pattern.type_id  
    attack_pattern.description  
    attack_pattern.deleted_at
```



```
attack_pattern.deleted
attack_pattern.sources_count
attack_pattern.id
attack_pattern.status
attack_pattern.type
attack_pattern.touched_at
attack_pattern.created_at
attack_pattern.updated_at
attack_pattern.Sources
attack_pattern.Attributes
attack_pattern.Indicators
attack_pattern.Adversaries
attack_pattern.Events
attack_pattern.Attachments
attack_pattern.Signatures
attack_pattern.Investigations
attack_pattern.Tasks
attack_pattern.Campaign
attack_pattern.Course_of_action
attack_pattern.Exploit_target
attack_pattern.Incident
attack_pattern.Ttp
attack_pattern.Attack_pattern
attack_pattern.Identity
attack_pattern.Intrusion_set
attack_pattern.Malware
attack_pattern.Report
attack_pattern.Tool
attack_pattern.Vulnerability
```

>Identity

```
<> identity.value
identity.status_id
identity.type_id
identity.description
identity.contact_information
identity.deleted_at
identity.deleted
identity.sources_count
identity.id
identity.status
identity.type
identity.touched_at
identity.created_at
identity.updated_at
identity.Sources
identity.Attributes
identity.Indicators
identity.Adversaries
```

```
identity.Events
identity.Attachments
identity.Signatures
identity.Investigations
identity.Tasks
identity.Campaign
identity.Course_of_action
identity.Exploit_target
identity.Incident
identity.Ttp
identity.Attack_pattern
identity.Identity
identity.Intrusion_set
identity.Malware
identity.Report
identity.Tool
identity.Vulnerability
```

> *Intrusion Set*

```
<> intrusion_set.value
intrusion_set.status_id
intrusion_set.type_id
intrusion_set.description
intrusion_set.started_at
intrusion_set.ended_at
intrusion_set.deleted_at
intrusion_set.deleted
intrusion_set.sources_count
intrusion_set.id
intrusion_set.status
intrusion_set.type
intrusion_set.touched_at
intrusion_set.created_at
intrusion_set.updated_at
intrusion_set.Sources
intrusion_set.Attributes
intrusion_set.Indicators
intrusion_set.Adversaries
intrusion_set.Events
intrusion_set.Attachments
intrusion_set.Signatures
intrusion_set.Investigations
intrusion_set.Tasks
intrusion_set.Campaign
intrusion_set.Course_of_action
intrusion_set.Exploit_target
intrusion_set.Incident
intrusion_set.Ttp
intrusion_set.Attack_pattern
```

```
intrusion_set.Identity
intrusion_set.Intrusion_set
intrusion_set.Malware
intrusion_set.Report
intrusion_set.Tool
intrusion_set.Vulnerability
```

>Malware

```
<> malware.value
malware.status_id
malware.type_id
malware.description
malware.deleted_at
malware.deleted
malware.sources_count
malware.id
malware.status
malware.type
malware.touched_at
malware.created_at
malware.updated_at
malware.Sources
malware.Attributes
malware.Indicators
malware.Adversaries
malware.Events
malware.Attachments
malware.Signatures
malware.Investigations
malware.Tasks
malware.Campaign
malware.Course_of_action
malware.Exploit_target
malware.Incident
malware.Ttp
malware.Attack_pattern
malware.Identity
malware.Intrusion_set
malware.Malware
malware.Report
malware.Tool
malware.Vulnerability
```

>Report

```
<> report.value
report.status_id
```

```
report.type_id
report.description
report.deleted_at
report.deleted
report.sources_count
report.id
report.status
report.type
report.touched_at
report.created_at
report.updated_at
report.Sources
report.Attributes
report.Indicators
report.Adversaries
report.Events
report.Attachments
report.Signatures
report.Investigations
report.Tasks
report.Campaign
report.Course_of_action
report.Exploit_target
report.Incident
report.Ttp
report.Attack_pattern
report.Identity
report.Intrusion_set
report.Malware
report.Report
report.Tool
report.Vulnerability
```

>Tool

```
<> tool.value
tool.status_id
tool.type_id
tool.description
tool.deleted_at
tool.deleted
tool.sources_count
tool.id
tool.status
tool.type
tool.touched_at
tool.created_at
tool.updated_at
tool.Sources
tool.Attributes
```

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

>Vulnerability

```
<> vulnerability.value
vulnerability.status_id
vulnerability.type_id
vulnerability.description
vulnerability.deleted_at
vulnerability.deleted
vulnerability.sources_count
vulnerability.id
vulnerability.status
vulnerability.type
vulnerability.touched_at
vulnerability.created_at
vulnerability.updated_at
vulnerability.Sources
vulnerability.Attributes
vulnerability.Indicators
vulnerability.Adversaries
vulnerability.Events
vulnerability.Attachments
vulnerability.Signatures
vulnerability.Investigations
vulnerability.Tasks
vulnerability.Campaign
vulnerability.Course_of_action
vulnerability.Exploit_target
vulnerability.Incident
vulnerability.Ttp
vulnerability.Attack_pattern
```

```
vulnerability.Identity  
vulnerability.Intrusion_set  
vulnerability.Malware  
vulnerability.Report  
vulnerability.Tool  
vulnerability.Vulnerability
```

Adding Differential Flags

You can use a differential flag in the Special Parameters section of your export output format to limit the output to new data. This will allow you to include only new data each time the export is run opposed to exporting all data.

Include the following to limit exports to new data only:

```
<> differential=1
```

If you have multiple systems pulling from the same Export, each system should use a unique differential value.



external system 1

```
https://{tq-host}/api/export/c2ab6df72e67ee13cef90f0e00981b62/?  
token=np6z01pFXwfHYb5tm51hMvKQJNYecTG& differential=1
```

external system 2

```
https://{tq-host}/api/export/c2ab6df72e67ee13cef90f0e00981b62/?  
token=np6z01pFXwfHYb5tm51hMvKQJNYecTG& differential=2
```

Adding Parameters to the end of the URL

You can append the same parameters listed above to the end of any export URL to achieve the same results. By pursuing this option, you will lose the option of having one place to manage what is being exported via that export.

Using Logical Operators in Export Filters

You can configure exports to output objects matching filter conditions that use logical AND and OR operators. Exports allow the following filters:

1. Searching using greater than, less than, or equal to

- Examples in special parameters string section:

```
<> indicator.score>=5
```

```
<> indicator.score<=5
```

- Examples in request URI:

```
<> &indicator.score>=5
```

```
<> &indicator.score<=8
```

2. Adding multiple criteria for a single field using an OR comparison

- Example in special parameters string section:

```
<> indicator.score=5&indicator.score=8
```

- Example in request URI:

```
<> &indicator.score[]=5&indicator.score[]=8
```

3. Adding multiple criteria for a single field using an AND comparison

- Example in special parameters string section:

```
<> indicator.score>=5&indicator.score<=8
```

- Example in request URI:

```
<> &indicator.score[]>=5&indicator.score[]<=8
```

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 on the **Output Format** link for an export from the main exports page



Important: 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.since_deleted}
    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}
```

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](#)
- [Filelis 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&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

FIELD	ENTRY
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
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

FIELD	ENTRY
Which type of information would you like to export?	Indicator
Output Type	Text/plain
Special Parameters	indicator.status=Active&indicator.deleted=N&indicator.type=IP Address&indicator.class=network
Output Format 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
Email Address	
◦ To ◦ From ◦ Sender	
Output Format Template	{foreach \$data as \$indicator} {\$indicator.value} {/foreach}

8. In turn click each of the URL's for the exports, a new browser widow will open displaying the first 10 results, make a note of this URL and the IoCs it is associated with it. The URL is made up off the following sections

```
<> https://<TQ Server>/api/export/<endpoint>/?  
limit=10&token=<token>
```

9. Remove the limit section and trailing & symbol, examples are below.

```
<> https://192.168.1.85/api/export/9bc092ce1e318f6c0d10009228729ad6/?  
token=uEyVyzIeYRGBdF2VKcHo9WKYDJvNftSo
```

This new URL format is needed to configure Cisco TID

```
<> https://192.168.1.85/api/export/9bc092ce1e318f6c0d10009228729ad6/?  
token=uEyVyzIeYRGBdF2VKcHo9WKYDJvNftSo
```

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 <i>To export to Cisco TID</i> steps.
Self-Signed Certificate	Toggle the Self-Signed Certificate to active.
Name	Use a descriptive name as we used on the ThreatQ exports. Example: ThreatQ - IP Address
	 This will help simplify sorting and handling of incidents based on TID indicators, use a consistent naming scheme across sources.
Action	You can either Block or Monitor.
Update Every	Select a time in minutes that the source is to be updated (the minimum is 30 mins, Maximum is 14,400).

FIELD

ENTRY

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 begin 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

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

- [Fidelis FQDN](#)
- [Fidelis FQDN Text](#)
- [Fidelis IP Address](#)
- [Fidelis IP Address Text](#)
- [Fidelis MD5](#)
- [Fidelis MD5 Text](#)
- [Fidelis URL](#)
- [Fidelis URL Text](#)

To export to Fidelis FQDN:

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

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

2. Click **Add New Export**.

The Connection Settings dialog box appears.

3. Enter an **Export Name**.

4. Click **Next Step**.

The Output Format dialog box appears.

5. Provide the following information:

FIELD	ENTRY
Which type of information would you like to export?	Indicators
Output Type	text/xml

Special Parameters

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

Under **Output Format Template**, enter:

```
<> <MyMD5feed/>

<description>FQDN feed provided by ThreatQuotient. Possible
request parameters are listed as attributes on the result
node. The dateBegin parameter defaults to one hour prior. Stay
secure my friends!</description>

<entries>

<limit>{$row_count}</limit>

<page>{$row_count}</page>

<start>{$row_count}</start>

<end>{$row_count}</end>

<status>{$row_count}</status>

<rows_returned>{$row_count}</rows_returned>

<entry>

{foreach $data as $indicator}

<hostname>{$indicator.value|escape:"url"}</hostname>

<extra_info>https://{ $http_host }/indicators/{ $indicator.id }/
details</extra_info>

{/foreach}

</entry>

</entries>
```

6. Click **Save Settings**.

7. Under **On/Off**, toggle the switch to enable the export.

To export to Fidelis FQDN Text:

1. 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/plain
Special Parameters	<pre><> indicator.status=Active&indicator.deleted=N&indicator.type=FQDN&indicator.class=host</pre>

Under **Output Format Template**, enter:

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

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

To export to Fidelis IP Address:

1. From the navigation menu, choose the **gear icon > Exports**.

The Exports page appears.

2. Click **Add New Export**.

The Connection Settings dialog box appears.

3. Enter an **Export Name**.

4. Click **Next Step**.

The Output Format dialog box appears.

5. Provide the following information:

FIELD	ENTRY
Which type of information would you like to export?	Indicators
Output Type	text/xml
Special Parameters	<pre><> indicator.status= Active&indicator. deleted=N&indicat or.type=IP Address&indicator .class=network</pre>

Under **Output Format Template**, enter:

```
<> <MyMD5feed/>

<description>IP feed provided by ThreatQuotient. Possible
request parameters are listed as attributes on the result
node. The dateBegin parameter defaults to one hour prior. Stay
secure my friends!</description>

<entries>

<limit>{$row_count}</limit>
```



```
<page>{$row_count}</page>

<start>{$row_count}</start>

<end>{$row_count}</end>

<status>{$row_count}</status>

<rows_returned>{$row_count}</rows_returned>

<entry>

  {foreach $data as $indicator}

    <ip>{$indicator.value|escape:"url"}</ip>

    <extra_info>https://{ $http_host }/indicators/{ $indicator.id }/
    details</extra_info>

  {/foreach}

</entry>

</entries>
```

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

To export to Fidelis IP Address Text:

1. From the navigation menu, choose the **gear icon > Exports**.

The Exports page appears.

2. Click **Add New Export**.

The Connection Settings dialog box appears.

3. Enter an **Export Name**.
4. Click **Next Step**.

The Output Format dialog box appears.

5. Provide the following information:

FIELD	ENTRY

Which type of information would you like to export?

Indicators

Output Type

text/plain

Special Parameters

```
<> indicator.status=
Active&indicator.
deleted=N&indicat
or.type=IP
Address&indicator
.class=network
```

Under **Output Format Template**, enter:

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

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

To export to Fidelis MD5:

1. 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/xml

Special Parameters

```
<> indicator.status=Active&indicator.deleted=N&indicator.type=MD5&indicator.class=host.
```

Under **Output Format Template**, enter:

```
<> <MyMD5feed/>

<description>MD5 feed provided by ThreatQuotient. Possible
request parameters are listed as attributes on the result
node. The dateBegin parameter defaults to one hour prior. Stay
secure my friends!</description>

<entries>

<limit>{$row_count}</limit>

<page>{$row_count}</page>

<start>{$row_count}</start>

<end>{$row_count}</end>

<status>{$row_count}</status>

<rows_returned>{$row_count}</rows_returned>

<entry>

{foreach $data as $indicator}

<md5>{$indicator.value|escape:"url"}</md5>

<extra_info>https://{ $http_host }/indicators/{$indicator.id}/
details</extra_info>

{/foreach}
```

```
</entry>

</entries>
```

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

To export to Fidelis MD5 Text:

1. 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/plain
Special Parameters	<pre><> indicator.status=Active&indicator.deleted=N&indicator.type=MD5&indicator.class=host</pre>

Under **Output Format Template**, enter:

```
<> {foreach $data as $indicator}

    {$indicator.value}

{/foreach}
```

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

To export to Fidelis URL:

1. 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/plain
Special Parameters	<pre><> indicator.st atus=Active& indicator .deleted=N</pre>

Under **Output Format Template**, enter:

```
<> <MyMD5feed/>

<description>URL feed provided by ThreatQuotient. Possible
```

```
request parameters are listed as attributes on the result
node. The dateBegin parameter defaults to one hour prior. Stay
secure my friends!</description>

<entries>

<limit>{$row_count}</limit>

<page>{$row_count}</page>

<start>{$row_count}</start>

<end>{$row_count}</end>

<status>{$row_count}</status>

<rows_returned>{$row_count}</rows_returned>

<entry>

{foreach $data as $indicator}

<url>{$indicator.value|escape:"url"}</url>

<extra_info>https://{ $http_host }/indicators/{ $indicator.id }/
details</extra_info>

{/foreach}

</entry>

</entries>
```

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

To export to Fidelis URL Text:

1. 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/plain
Special Parameters	<pre><> indicator.status=Active&indicator.deleted=N&indicator.type=URL&indicator.class=host</pre>

Under **Output Format Template**, enter:

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

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

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 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:

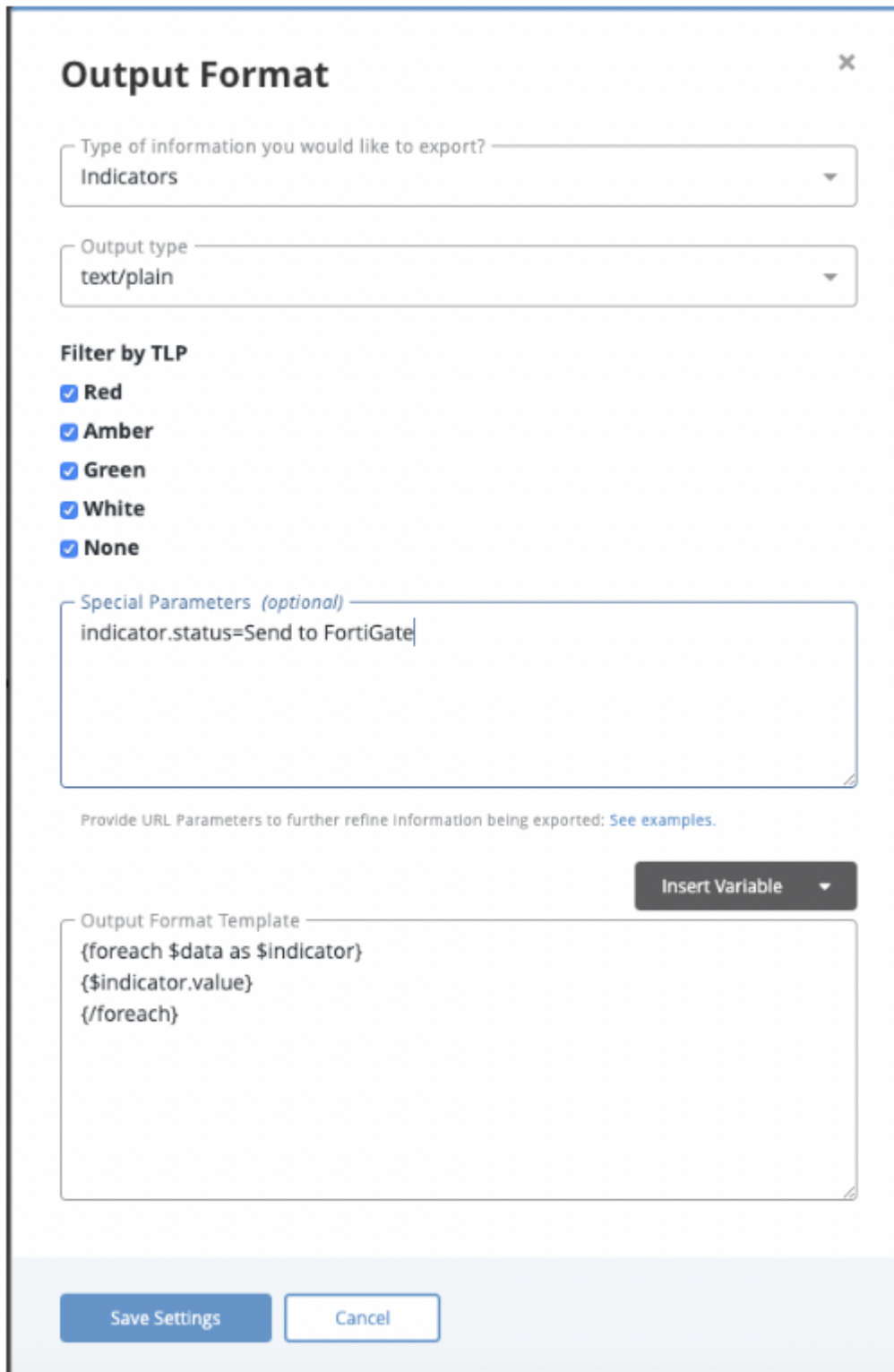
1. Follow the steps in the [Indicator Status](#) topic to create a status called **Send to FortiGate**.
2. Use the following special parameter:

```
<> 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.



The screenshot shows the 'Output Format' configuration window in ThreatQ. It includes a close button (X) in the top right corner. The 'Type of information you would like to export?' dropdown is set to 'Indicators'. The 'Output type' dropdown is set to 'text/plain'. Under 'Filter by TLP', all options (Red, Amber, Green, White, None) are checked. The 'Special Parameters (optional)' text area contains 'indicator.status=Send to FortiGate'. Below this is a link to 'See examples.' and a note: 'Provide URL Parameters to further refine Information being exported: See examples.' There is an 'Insert Variable' button with a dropdown arrow. The 'Output Format Template' text area contains the following code:

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

 At the bottom are 'Save Settings' and 'Cancel' buttons.

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.](#)

Insert Variable

Output Format Template

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

Save Settings Cancel

Configure FortiGate to Download Indicators from ThreatQ

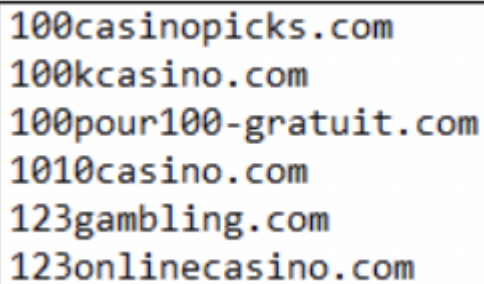
The following detailed steps have been copied from the FortiGate support center and provided here for convenience. The source is <https://docs.fortinet.com/document/fortigate/6.0.0/cookbook/85580>

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.

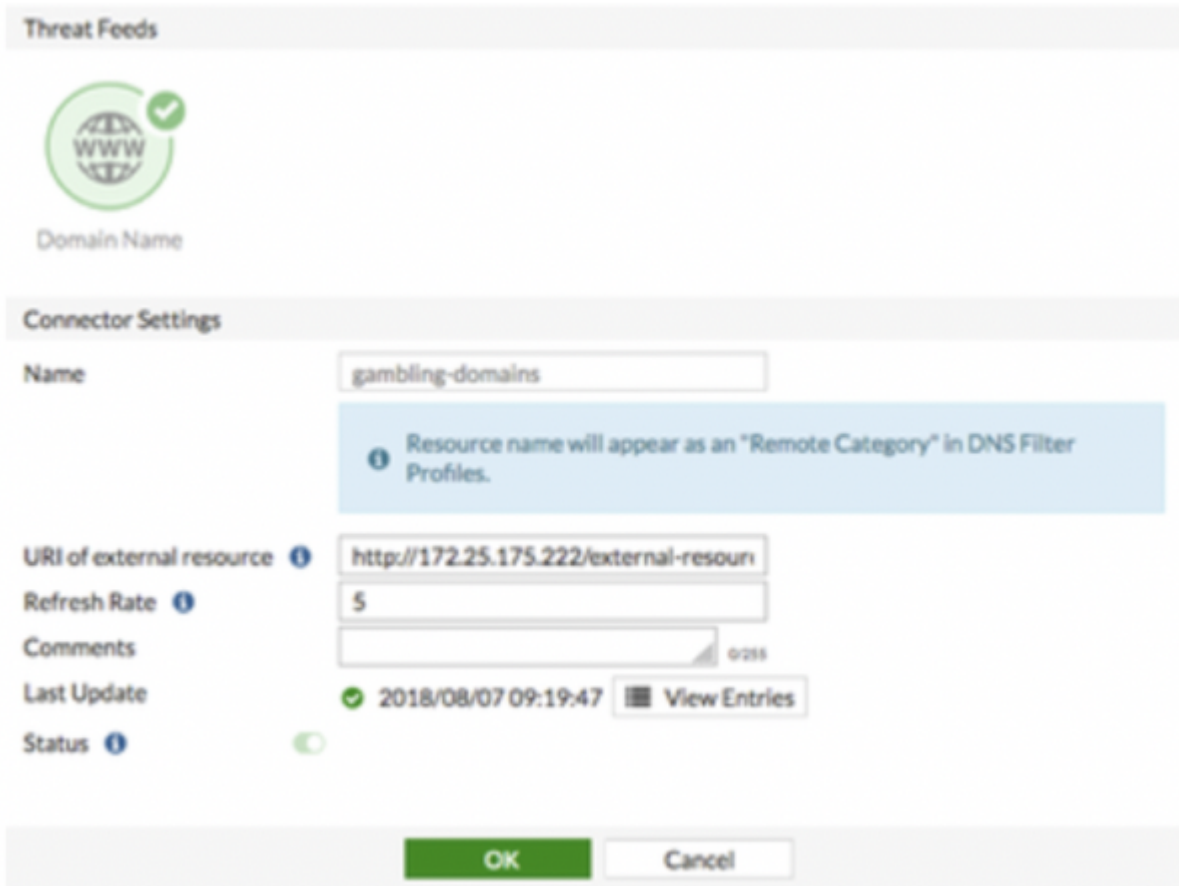
1. Create an external block list. The external block list should be a plain text file with one domain name per line. The use of simple wildcards is supported. You can create your own text file or download it from an external service. Upload the text file to the HTTP file server.



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

2. Configure the threat feed:
 1. In FortiOS, go to Security Fabric -> Fabric Connectors. Click Create New.
 2. Under Threat Feeds, select Domain Name.
 3. 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.



Threat Feeds

 Domain Name

Connector Settings

Name:

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

URI of external resource:

Refresh Rate:

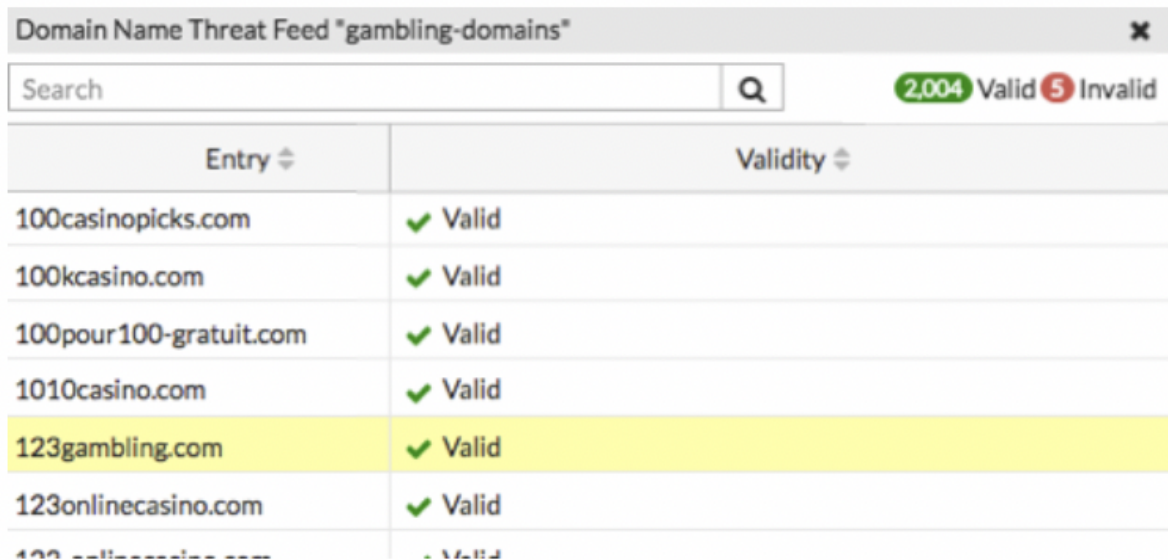
Comments:

Last Update:  2018/08/07 09:19:47 [View Entries](#)

Status: 

OK **Cancel**

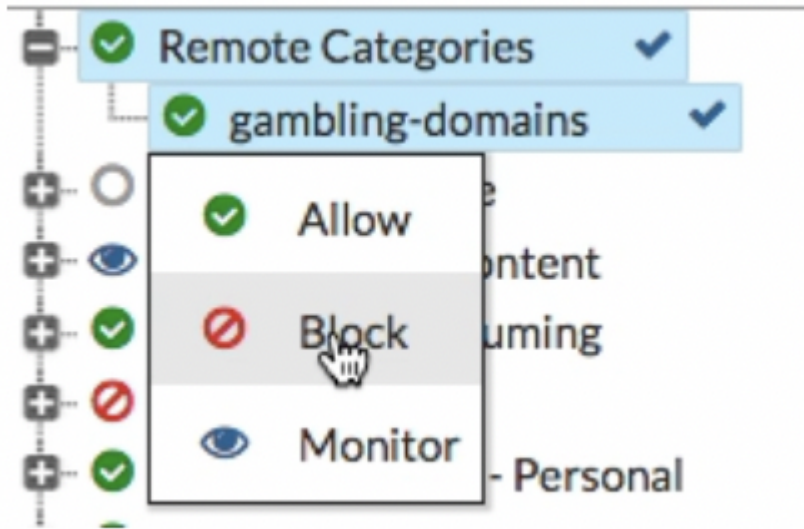
4. Click View Entries to see the text file's domain list.



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

5. Click **OK**.
3. Add the threat feed to the DNS filter:
 1. Go to Security Profiles -> DNS Filter.
 2. Scroll to the list of preconfigured FortiGuard filters.

3. The resource file uploaded earlier is listed under Remote Categories. Set the action for this category to Block.

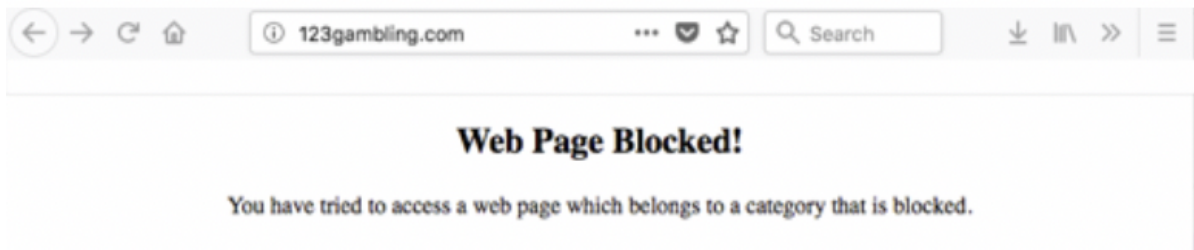


4. Configure the outgoing Internet policy:

1. Go to **Policy & Objects -> IPv4 Policy**.
2. Enable the **DNS Filter** under the *Security Profiles*.
3. From the SSL Inspection dropdown list, select an SSL inspection profile.

5. View the results:

1. Visit a domain on the external resource file. This example visits 123gambling.com. A Web Page Blocked! message appears.



2. 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	<pre><> indicator.status= Active&indicator. deleted=N&indicat or.type=IPAddress & indicator.type=CI DR Block&indicator.c lass=network</pre>

Under **Output Format Template**, enter:

```
<> RECORD_NUMBER, GROUP_NAME, GROUP_ID, NETWORK_DEFINITION, PARENT_NAME, SPACE  
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	<pre><> indicator.status=Active&indicator.deleted=N&indicator.type=FQDN&indicator.class=network</pre>

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	<pre><> indicator.status=Active&indicator.deleted=N&indicator.type=IP</pre>

```
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	<pre><> signature.status=Active&signature.deleted=N&signature.type=OpenIOC</pre>

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	<pre><> indicator.status=Active&indicator.deleted=N&indicator.type=FQDN&indicator.class=network</pre>

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

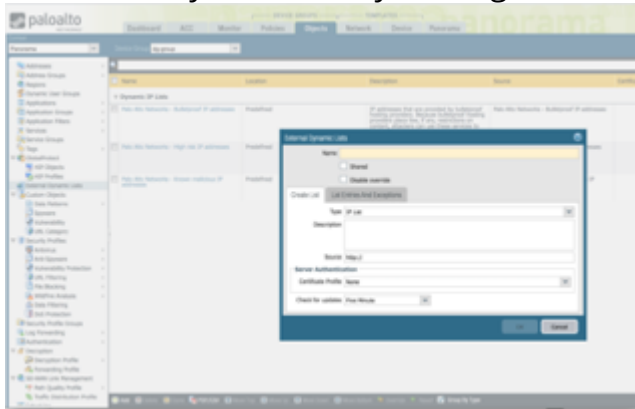
To add the dynamic list to Palo Alto, follow the instructions from here.

<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>

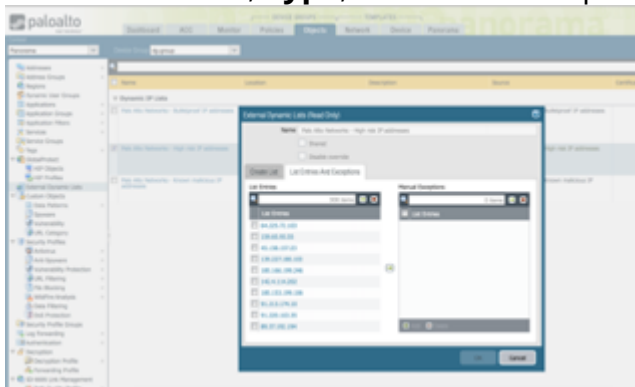
Configure an External Dynamic List (EDL) in Panorama

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	<pre><> indicator.status=Active& indicator. deleted=N</pre>

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 ""}

{$indicator.value}{$stab}{$indicator_type}{$stab}{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}

{$stab}https://{ $http_host}/indicators/{$indicator.id}/
details

{/if}

{/foreach}
```

6. Click **Save Settings**.

7. Under **On/Off**, toggle the switch to enable the export.



## 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                                  | <pre>&lt;&gt; indicator.sincecreated=Y</pre> |

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](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](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 -

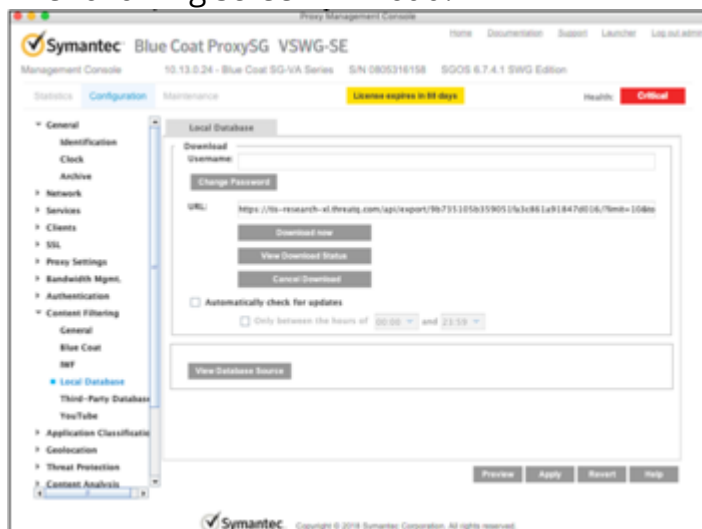
- via the [Management Console](#)
- via the [Proxy's CLI](#)

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 ?
```

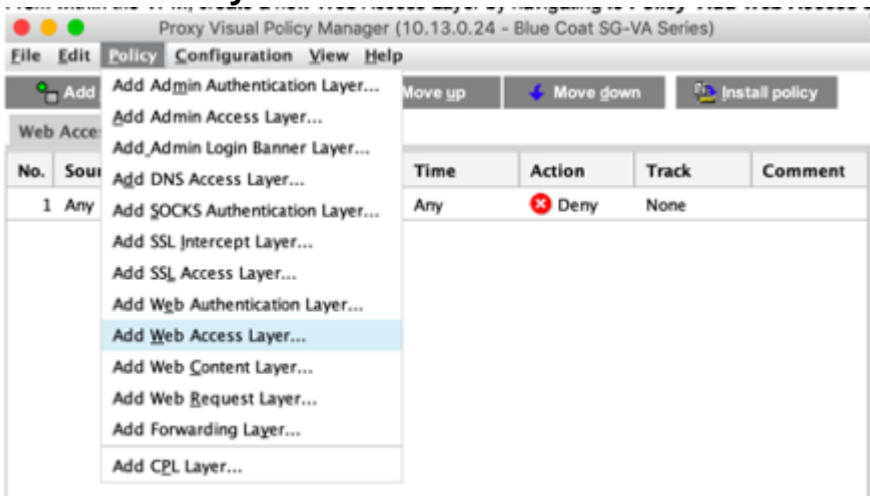
## Create and Install a Content Filtering Policy

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**.

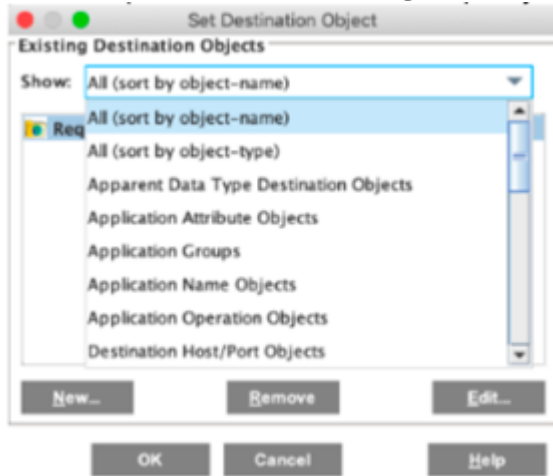


3. From within the VPM, create a new **Web Access Layer** by navigating to **Policy Add > Web Access Layer**.





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



This will open a new window, in which you can select all the categories to be blocked by the ProxySG appliance. The list of URLs exported from ThreatQ will be available under the Local category.

6. Expand **Local** and select the name you've given the export from ThreatQ. In this example, the name is **tq\_malicious\_url**.



7. Click **OK**, and then again **OK** to go back to the **VPM**.
8. Highlight the newly created policy layer, and click on the **Install policy** button in the upper right corner.

 Before installing the policy, make sure that the type of **Action** on the policy is **Deny**. If it shows **Allow**, make sure to change it to **Deny**. The action instruction what type action ProxySG should enforce when it detects that a user sends a request to any of the indicators in the list exported from ThreatQ.



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

## 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=r**

- 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                                  | <pre>&lt;&gt; indicator.status=Active&amp;indicator.deleted=N&amp;indicator.type=MD5&amp;indicator.class=network</pre> |

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:

**Which type of information would you like to export?**

Indicators

**Output Type**

text/plain

**Special Parameters**

```
<> indicator.stat
us=Active&indi
cator.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 ""}

{ $indicator.value}{$stab}{$indicator_type}{$stab}{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}

{ $stab}https://{ $http_host}/indicators/{ $indicator.id}/details

{/if}
```

```
{/foreach}
```

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

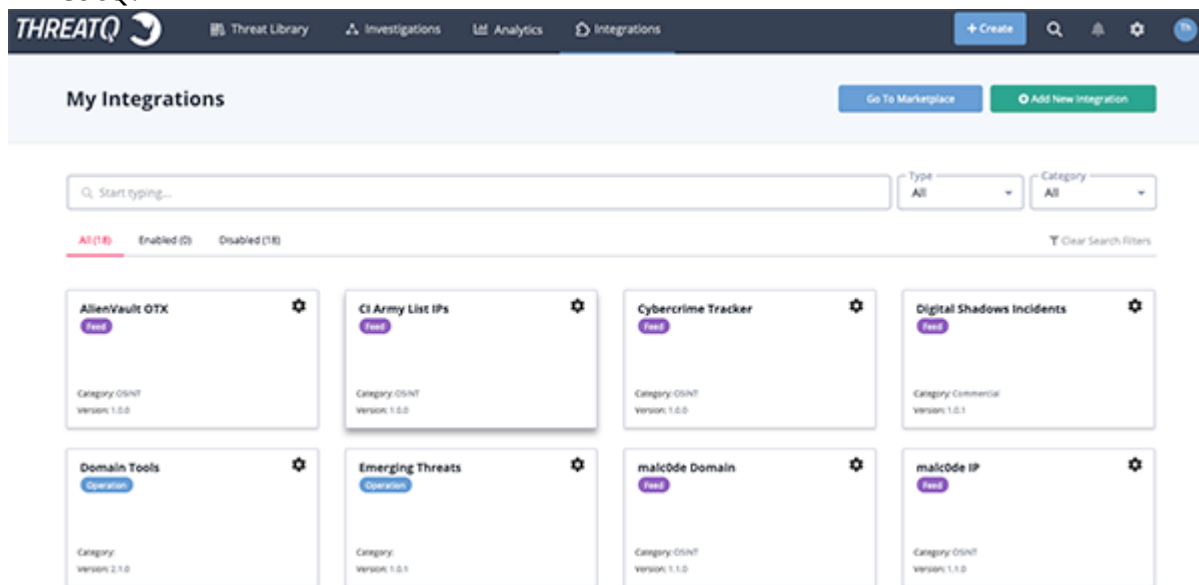


# Integrations Management



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, custom connectors, and operations that you have downloaded from the ThreatQ Marketplace or are seeded in ThreatQ.



From the My Integrations page, you can view all integrations installed on your ThreatQ instance.

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                                                                                                                                                |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Keyword</b> | Filter the integrations list by keyword.                                                                                                               |
| <b>Type</b>    | Filter the integrations list by integration type. Options include: <ul style="list-style-type: none"><li>• Intelligence Feeds and Connectors</li></ul> |

- Operations

**Category** Filter the list by the category of integration: Labs, Commercial, OSINT, STIX/TAXII.

**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.

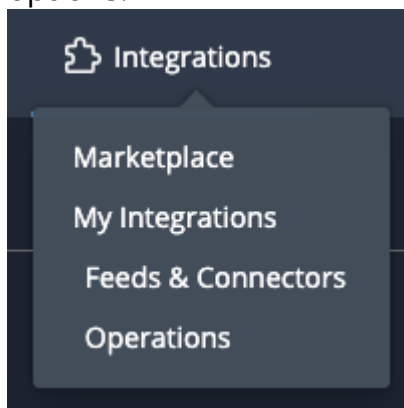


The **All** tab, which displays both enabled and disabled integrations, is selected by default.

**Clear Search Filters** Clears the current search filters that are currently in use.

## Accessing Integrations Management

1. Navigate to your ThreatQ instance.
2. Click on 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.

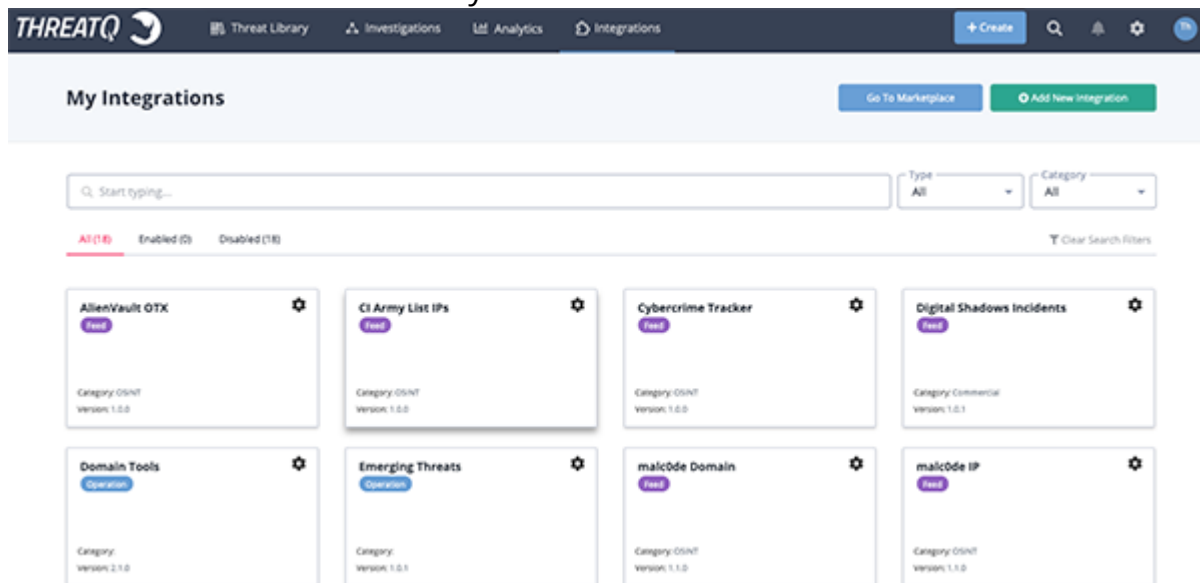
**Feeds and Connectors**

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 will load based on your selection. All integrations currently installed on your platform, both enabled and disabled, can be found on this page. The **All** status tab will be selected by default.



# Integration Types

ThreatQ integrations include threat intelligence feeds, custom connectors, and operations. This topic will highlight specific information about each type of integration.



Custom connectors typically fall under the **Labs** category of Threat Intelligence Feeds.

## Threat Intelligence Feed Categories

Threat Intelligence feeds are organized into the following categories:

| CATEGORY             | DETAILS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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.                                                                                                                                                                              |
| OSINT or Open Source | OSINT feeds are open source threat intelligence feeds. Open source feeds are free to use, but some may require you to register with the feed provider to attain an API Key.                                                                                                                                                                                                                                                                                                             |
| STIX/TAXII           | STIX stands for Standard Threat Information Expression, it is an emerging standard for the sharing of machine readable intelligence and incident data. A STIX package is an XML document that can contain many indicators and related context information. For the automated sharing of STIX packages, a protocol called TAXII (Trusted Automated eXchange of Indicator Information) is used to provide a feed to consumers. ThreatQ provides a feature for consuming STIX/Taxii feeds. |
| 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.                                                                                                                                                                                              |

## Operations

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

To develop custom operations, you should possess a basic functional knowledge of Python version 3 development.

ThreatQ operations are written in Python v3.5.5. We recommend allocating a non-production ThreatQ appliance for Operations development. You may use this development appliance to troubleshoot your operations before deploying them to production. You may also set up a local Python environment, write your script, and then copy it onto your ThreatQ appliance.

# Managing Integrations

You can add/remove, enable/disable, and configure integrations from the My Integrations page.



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

Steps may slightly differ depending on the individual integration. Refer to the integration's individual guide for specific details.

## Adding Integrations



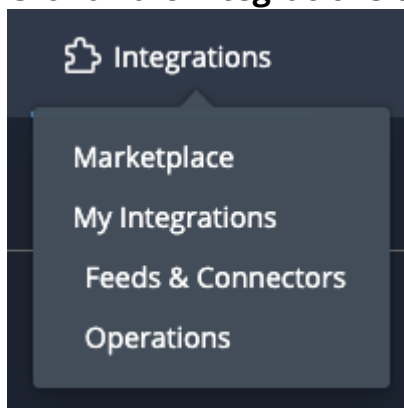
ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integrated-related credentials.

You can add integrations using the My Integration page. The steps for upgrading an integration are the same as adding an integration.

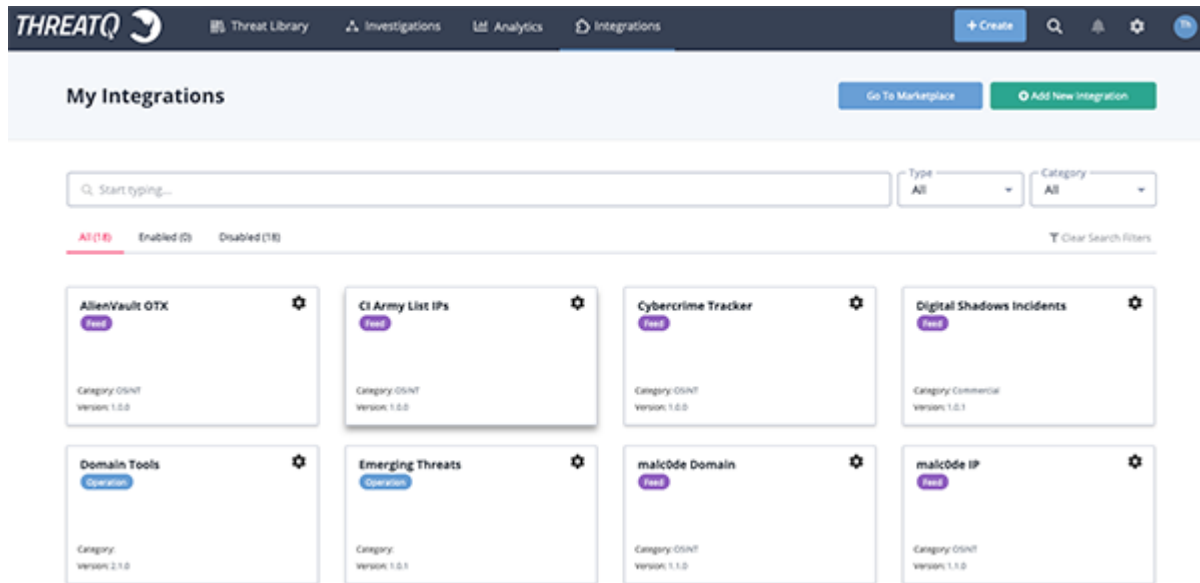


Some custom connectors cannot be installed via the ThreatQ UI. See your connector's documentation for specific installation steps.

1. Log into <https://marketplace.threatq.com>.
2. Locate and download the desired integration file.
3. Navigate to your ThreatQ instance.
4. Click on the **Integrations** option in the main navigation and select **My Integrations**.

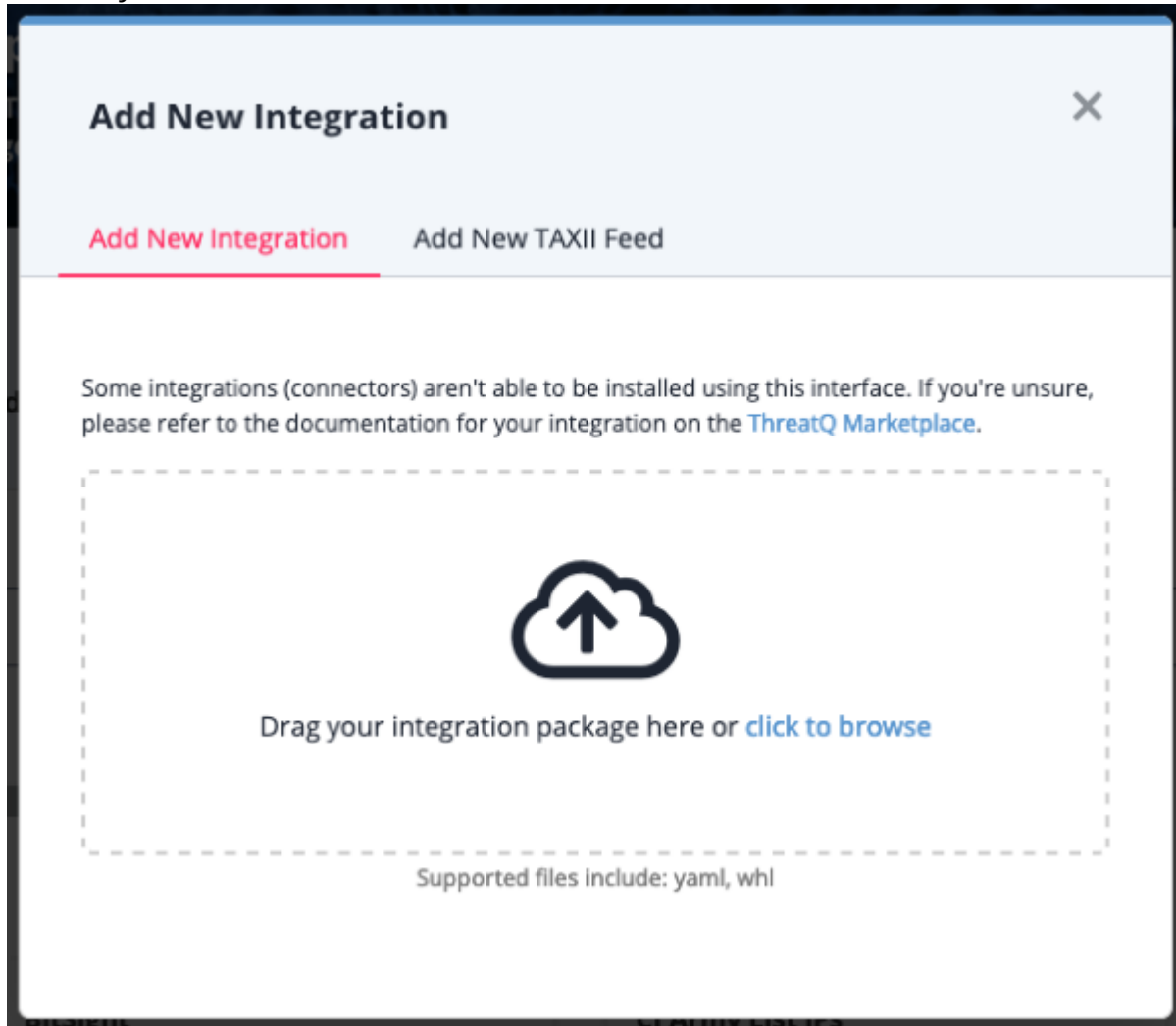


5. The My Integrations page will load. All integrations currently installed on your platform, both enabled and disabled, can be found on this page. The **All** tab will be selected by default.



6. Click on the **Add New Integration** button located to the top-right of the page.

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



7. Upload the integration file using one of the following methods:

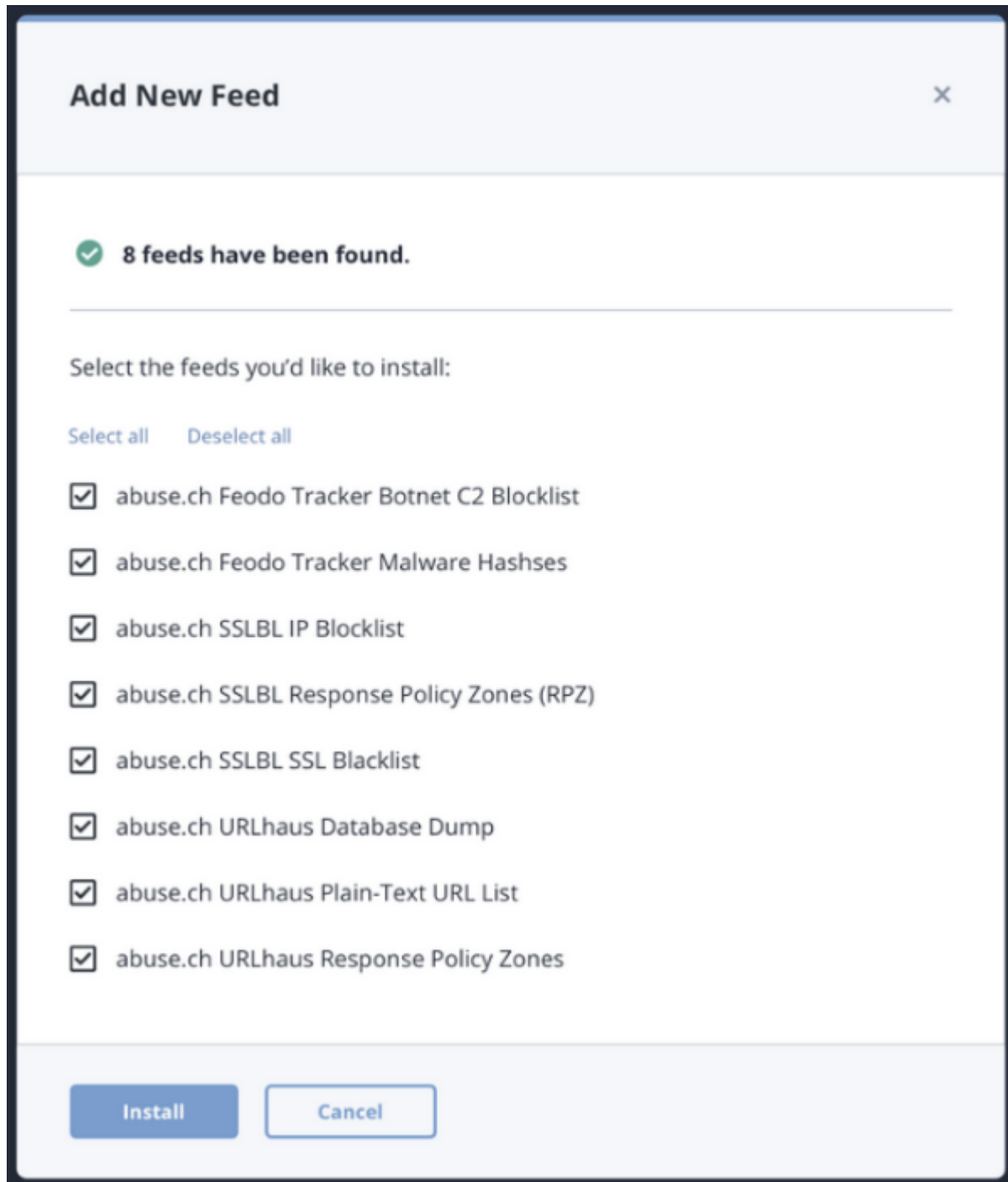
- Drag and drop the integration file into the dialog box
- Select Click to Browse to locate the integration file on your local machine



ThreatQ will inform you if the integration already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the integration contains changes to the user configuration. The new user configurations will overwrite the existing ones for the integration and will require user confirmation before proceeding.



8. If the integration file contains multiple feeds, you will be prompted to select which feeds to install. Select the feeds to include and click on **Install**.



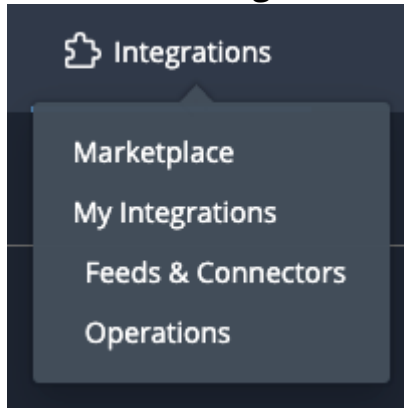
The integration will now be installed on the platform. You will still need to [configure](#) and [enable](#) the integration before it can be used.

## Adding STIX/TAXII Integrations

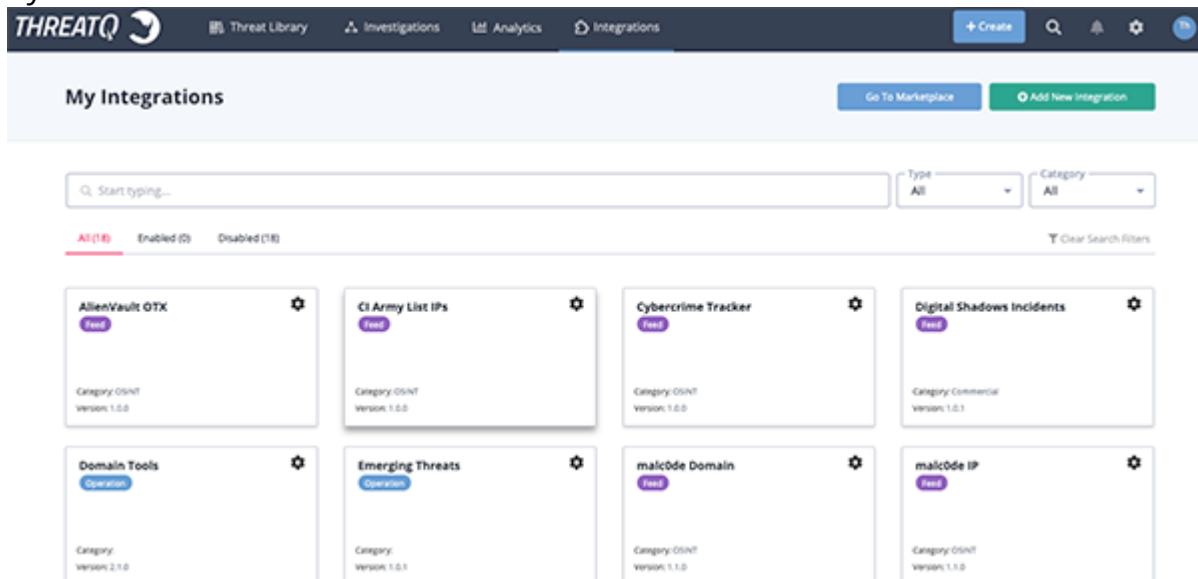


ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integrated-related credentials.

1. Click on the **Integrations** option in the main navigation and select **My Integrations**.

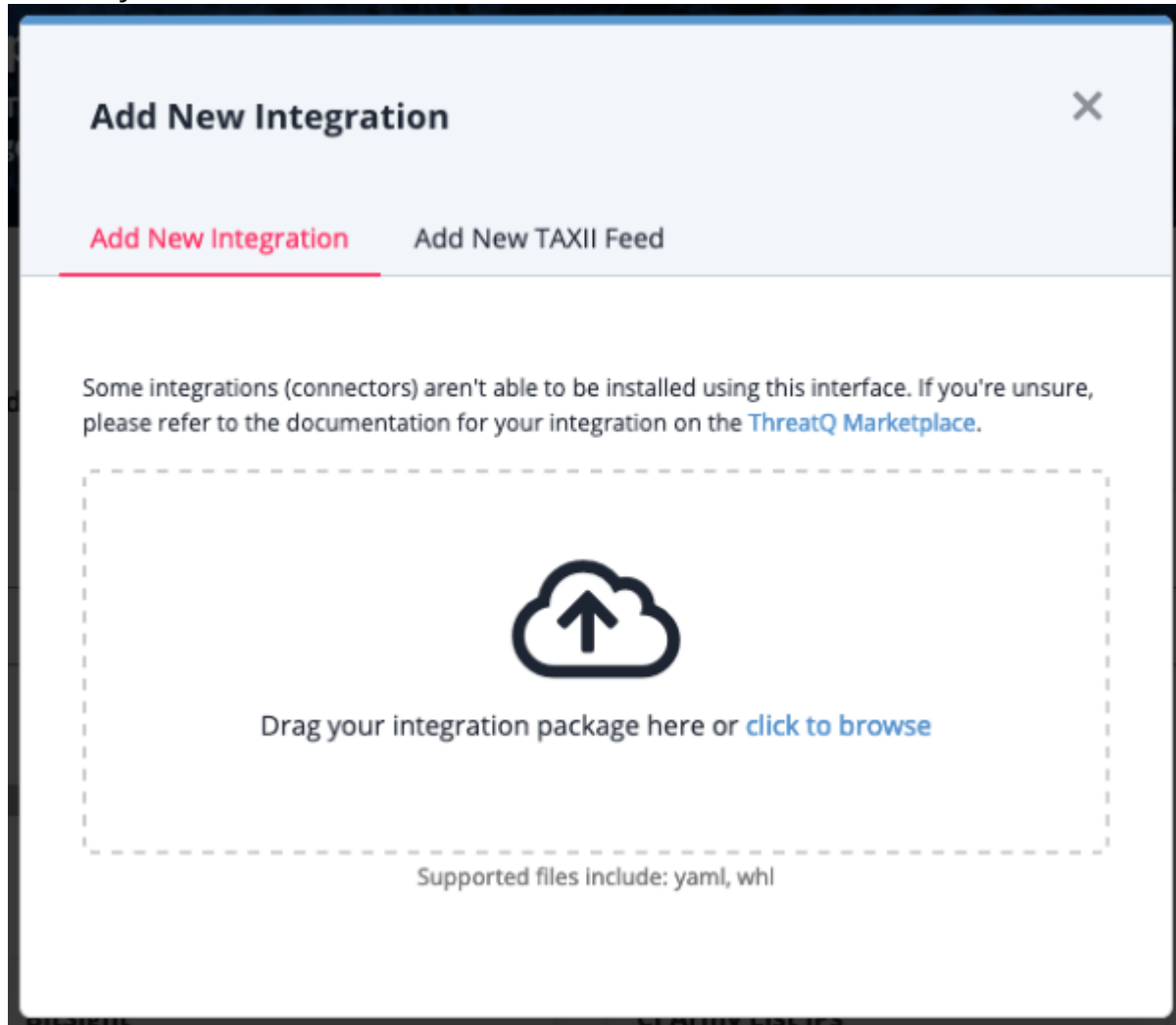


The My Integrations page will load. All integrations currently installed on your platform, both enabled and disabled, can be found on this page. The Enabled tab will be selected by default.



2. Click on the **Add New Integration** button located to the top-right of the page.

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



3. Click on the **Add New TAXII Feed** option.

The Add TAXII Feed form will load.

## Add New Feed



Add New Feed

**Add TAXII Feed**

What would you like to name this feed?

How often would you like to pull new data from this feed?

Every Hour



### TAXII Connection Settings

TAXII Server Version

2.0



The version of the TAXII Server to poll for data.

Discovery URL

Path to the TAXII Server's Discovery Service

Poll URL (Optional)

Optional URL specifying a specific endpoint on the TAXII Server to poll for data. If not supplied, the TAXII Client will attempt to determine the appropriate path via the Collections Service.

Collection Name

Name of the collection to poll data from

☐ **Disable Proxies**

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

### Login Credentials (if applicable)

Username

threatq@threatq.com

Basic Authentication Username

Password

.....



Basic Authentication Password

## 4. Complete the following fields:

| FIELD                                                     | INSTRUCTIONS                                                                                                                                                               |
|-----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| What would you like to name this feed?                    | Enter the feed's name that will be displayed throughout ThreatQ. The name must be at least 5 characters long<br><br>It does not need to match the <b>Collection Name</b> . |
| How often would you like to pull new data from this feed? | Choose <b>Every Hour</b> or <b>Every Day</b> .                                                                                                                             |

**TAXII Connection Settings**

|                      |                                                                                                |
|----------------------|------------------------------------------------------------------------------------------------|
| TAXII Server Version | Options include: 1.0, 1.2, 2.0.<br><br>This field is required.                                 |
| Discovery URL        | This is where the TAXII server can be reached.<br><br>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.<br><br>This field is required. |

**Client User Authentication**

| FIELD                                | INSTRUCTIONS                                                                                                                                                 |
|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Username                             | Enter a username if required for the feed.                                                                                                                   |
| Password                             | Enter a password if required for the feed.                                                                                                                   |
| <b>Client TLS/SSL Authentication</b> |                                                                                                                                                              |
| Client Certificate                   | Enter a certificate if required for the feed.                                                                                                                |
| Client Key                           | Enter a private key if required for the feed.                                                                                                                |
| <b>Server Authentication</b>         |                                                                                                                                                              |
| Verify SSL                           | Leave the checkbox checked to require that the TAXII client verify the provider's SSL certificate.                                                           |
| Host CA Certificate Bundle           | <p>The provider's CA Certificate used to verify SSL.</p> <p>The Host CA Certificate Bundle will not be honored if the Verify SSL option is not selected.</p> |

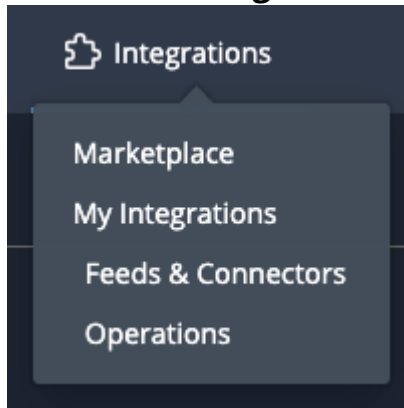
5. Click on **Add TAXII** Feed.

The TAXII/STIX feed will be added to the Integrations page. You will still need to [configure](#) and [enable](#) the integration.

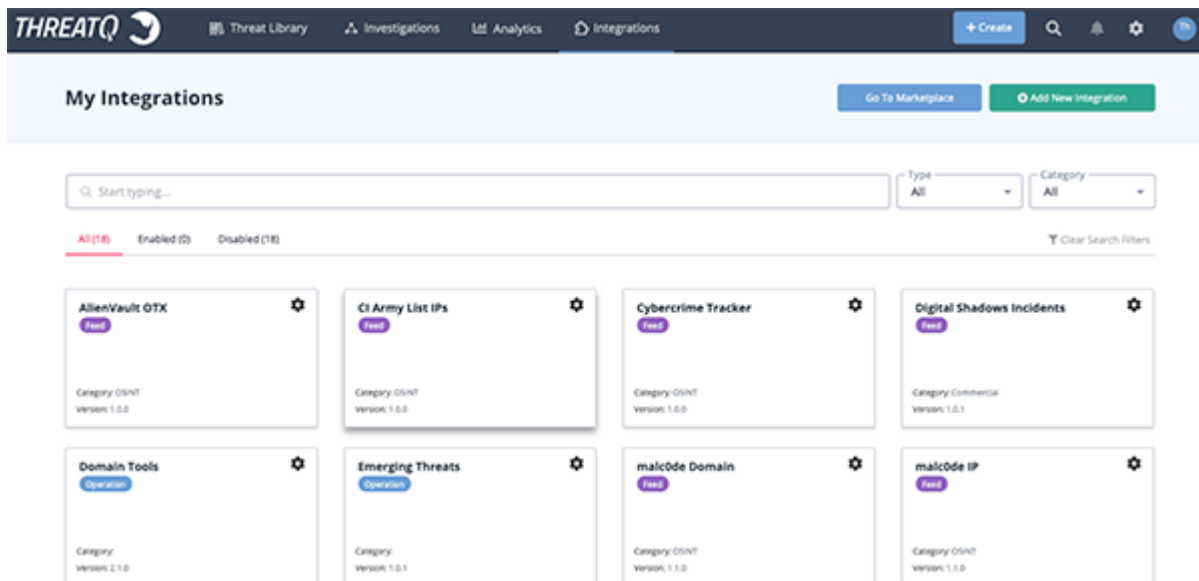
## Configuring an Integration

The integration must already be installed in order to access its configuration. See the [Adding Integrations](#) topic for more details.

1. Click on the **Integrations** option in the main navigation and select **My Integrations**.

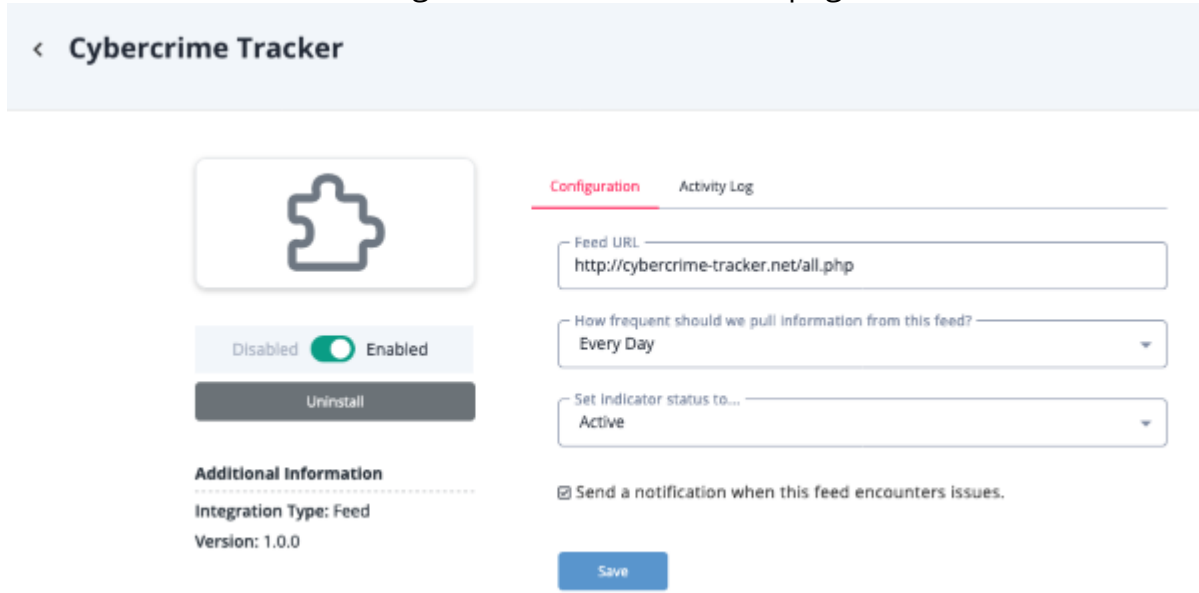


The My Integrations page will load. All integrations currently installed on your platform, both enabled and disabled, can be found on this page. The **All** tab will be selected by default.





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



The integration details page will load. Integration details, such as the author, required ThreatQ version and targeted object types will be listed to the left. The **Configuration** and **Activity Log** (if the integration is a feed) will be listed to the right. If the integration is a feed, the **Activity Log** will load after the initial run.

3. Enter the integration's required configuration parameters and then click on **Save**.



For feeds and some connectors, you can configure feed run frequency and default object status (if the object is an indicator or signature). Refer to the integration's user guide for more details. For instructions on performing a manual feed run - see [Performing Manual Runs \(feeds\)](#).

You can also enable feed health notifications for that specific feed. See the [Feed Health Notifications](#) for more information.

4. Click on the **Enable/Disable** toggle switch to enable the integration.



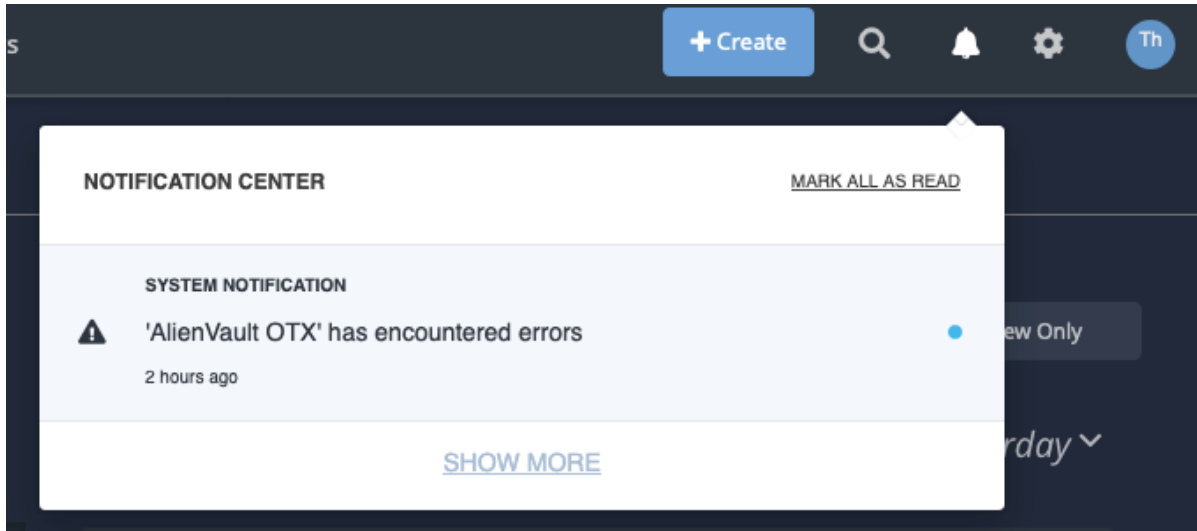
After being enabled, the Feed will automatically start a run.

The integration has now been configured and enabled for use.

## Feed Health Notifications

Feed Health Notifications allows the ThreatQ application to send you, and other designated users, email and in-app notifications when a feed encounters an issue.

The in-app notifications will appear in [Notification Center](#) for users with an administrator or maintenance account.



The emails, sent to users designated on the Notification Settings page, will contain useful information such as connection information, data ingested, and an ingestion summary.

**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)

HELP CENTER • SUPPORT

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

See the [Notification Settings](#) topic for more information.

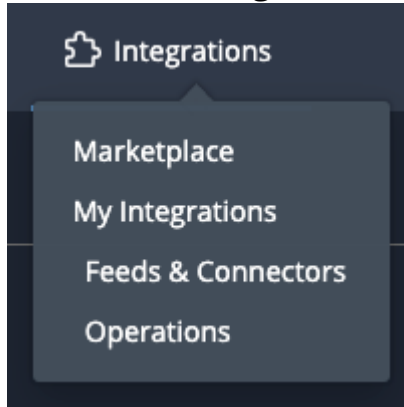
## Enabling/Disabling Integrations

You can enable and disable installed integrations for an integration's details page. Disabling an integration allows you deactivate an integration without completely removing it from your instance.

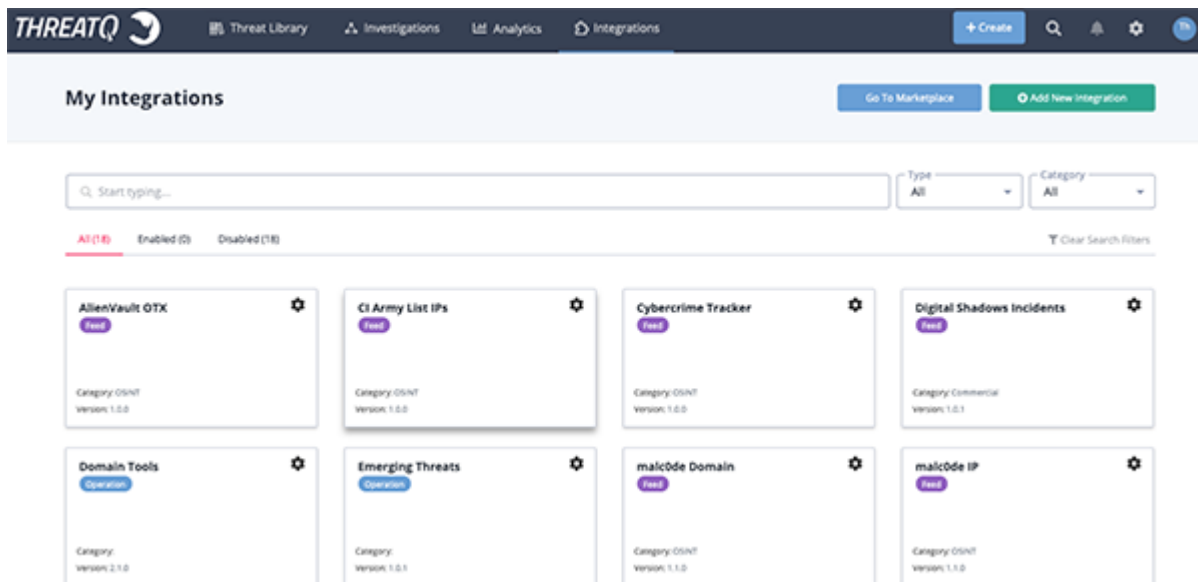


The integration must already be installed in order to access its configuration. See the [Adding Integrations](#) for more details.

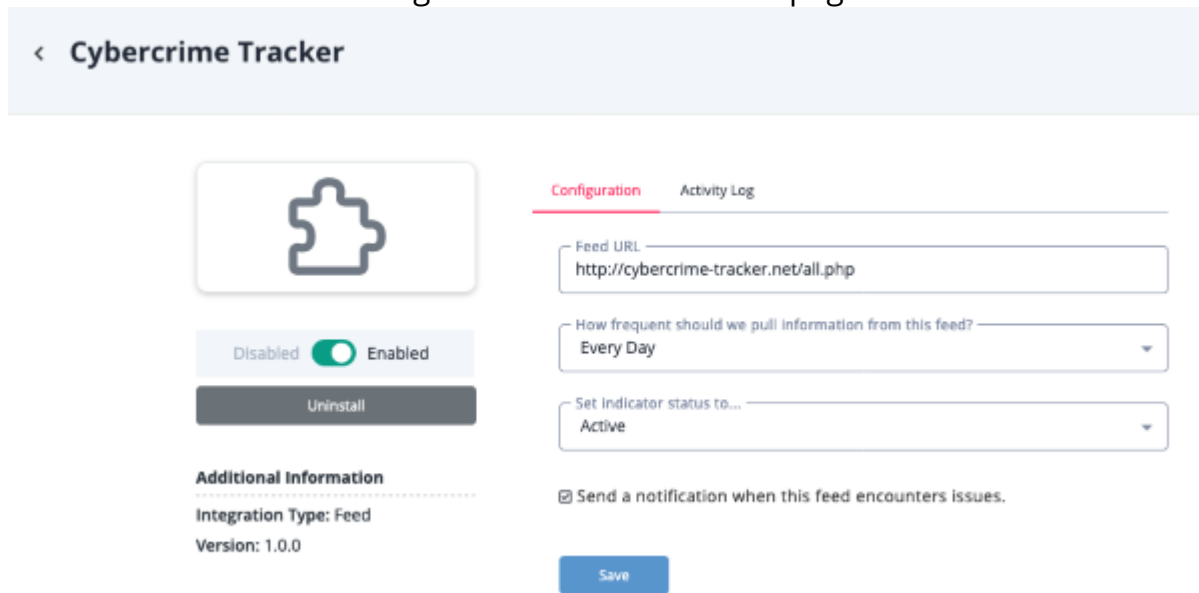
1. Click on the **Integrations** option in the main navigation and select **My Integrations**.



The My Integrations page will load. All integrations currently installed on your platform, both enabled and disabled, can be found on this page. The **All** tab will be selected by default.



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

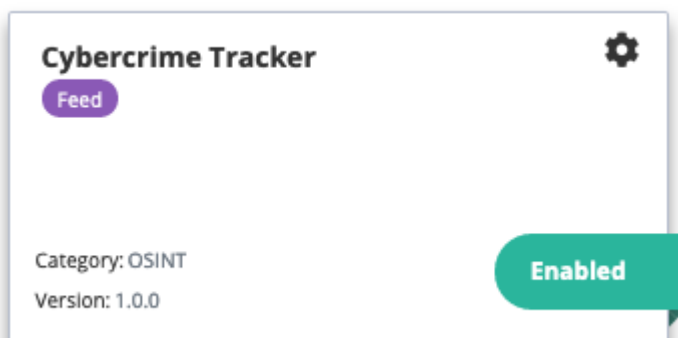


The screenshot shows the 'Cybercrime Tracker' integration details page. On the left, there is a puzzle piece icon, a toggle switch set to 'Enabled', and an 'Uninstall' button. Below this, under 'Additional Information', it lists 'Integration Type: Feed' and 'Version: 1.0.0'. On the right, there are two tabs: 'Configuration' (active) and 'Activity Log'. The 'Configuration' tab contains three input fields: 'Feed URL' with the value 'http://cybercrime-tracker.net/all.php', 'How frequent should we pull information from this feed?' with a dropdown set to 'Every Day', and 'Set Indicator status to...' with a dropdown set to 'Active'. There is a checkbox for 'Send a notification when this feed encounters issues.' which is checked. A 'Save' button is at the bottom right.

The integration details page will load. Integration details, such as the author, required ThreatQ version and targeted object types will be listed to the left. The **Configuration** and **Activity Log** (if the integration is a feed) will be listed to the right. If the integration is a feed, the **Activity Log** will load after the initial run.

3. Click on the **Enable/Disable** toggle switch to either enable or disable the integration.

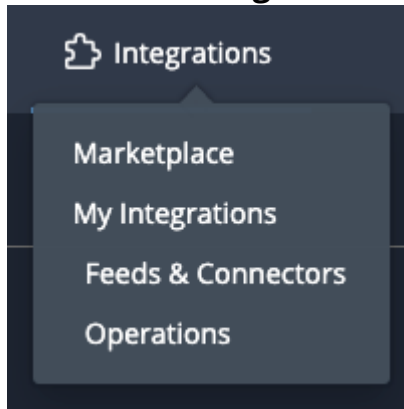
Enabled integrations will have a green header and an **Enabled** banner on the My Integrations page.



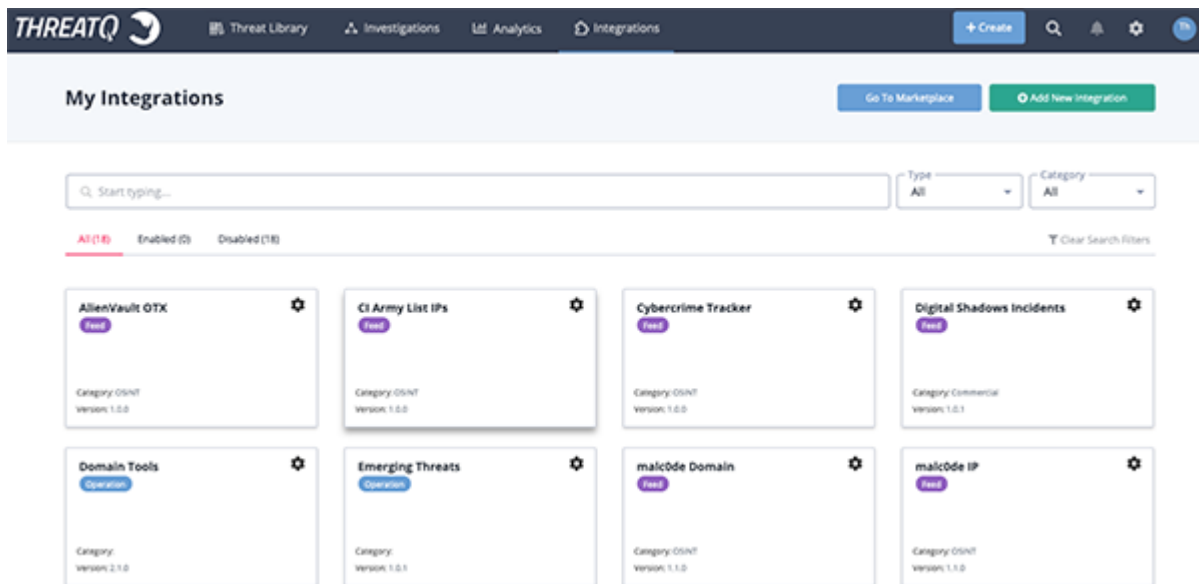
## Removing an Integration

Removing an integration will uninstall an integration for your instance. All previously ingested data will remain in the system. You can also disable an integration, which will deactivate it without completely removing the integration from your instance.

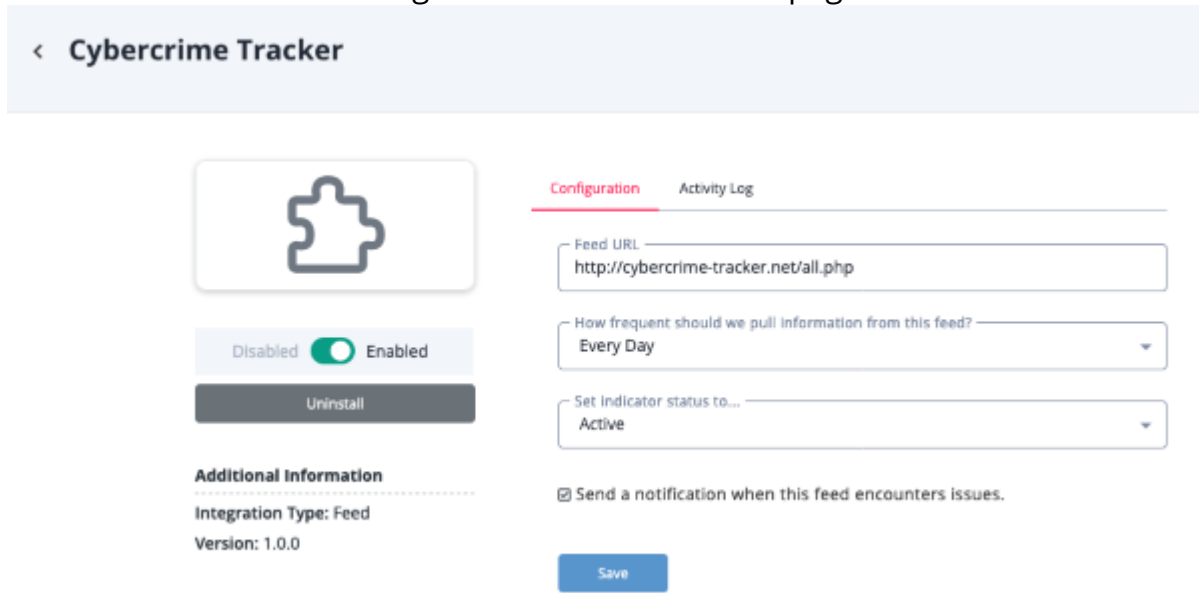
1. Click on the **Integrations** option in the main navigation and select **My Integrations**.



The My Integrations page will load. All integrations currently installed on your platform, both enabled and disabled, can be found on this page. The **All** tab will be selected by default.



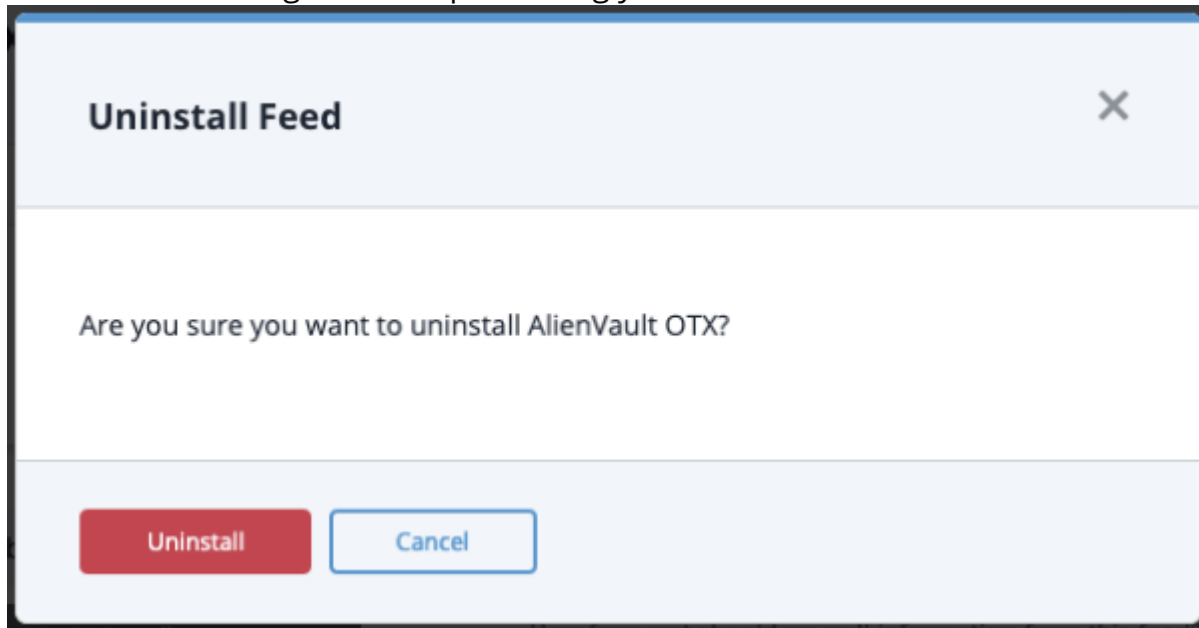
2. Locate and click on the integration to load its details page.



There are several filter options to assist in locating the integration including a key word filter, integration category, and integration status (enabled, disabled).

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

The Uninstall dialog box will open asking you to confirm the uninstall selection.



4. Click on **Uninstall** to confirm and remove the integration.

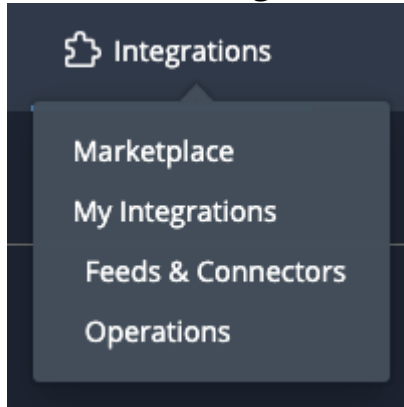
## Performing Manual Runs (feeds)



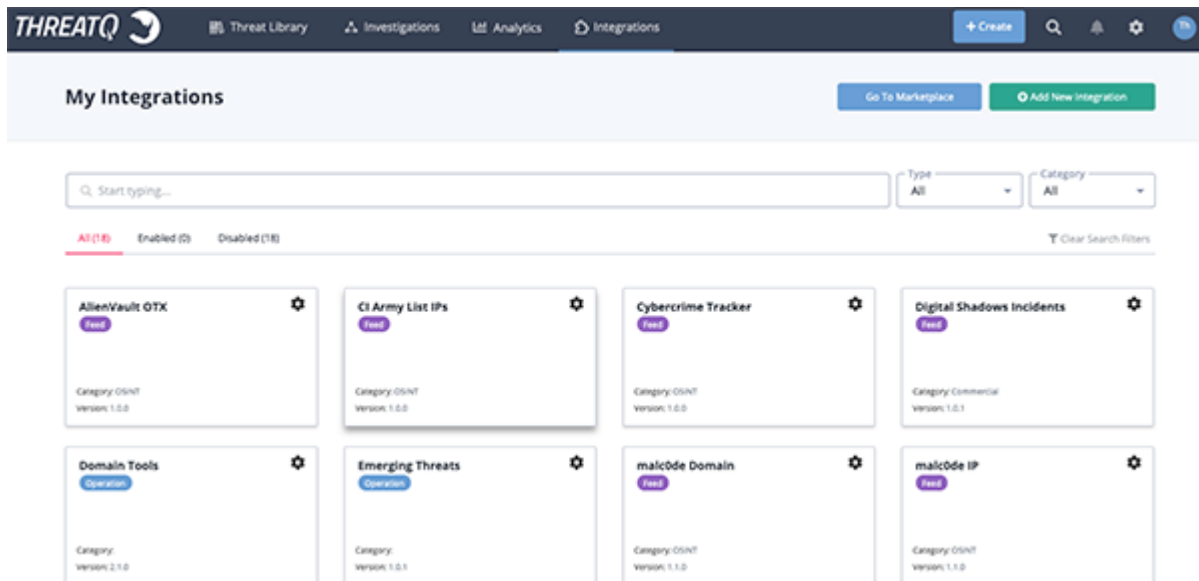
Not every feed integration allows users to perform a manual run.

To initiate a manual feed integration run:

1. Click on the **Integrations** option in the main navigation and select **My Integrations**.



The My Integrations page will load. All integrations currently installed on your platform, both enabled and disabled, can be found on this page. The **All** tab will be selected by default.





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

[<](#) **MITRE PRE-ATT&CK**



Configuration

Activity Log

**Activity Log Details**

Scheduled Run  
11/02/2020 10:00pm

Disabled

☒

Enabled

Run Integration

Uninstall

**Additional Information**

Integration Type: Feed

Version: 1.0.0



There are several filter options to assist in locating the integration including a key word filter, integration category, and integration status (enabled, disabled).

3. Confirm that the integration is enabled.
4. Click on 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 dialog box will open.

**Trigger Manual Run** [X]

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

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

Queue Run Cancel

5. Select a **Start Date**, **Start Time**, and **Time Zone** for your run.
6. Select an **End Date**, **End Time**, and **Time Zone** for your run.

Some feed integrations only support a **Start Date**.

**Trigger Manual Run** [X]

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.

Queue Run Cancel

7. Click on **Queue Run**.

## Running an Operation Integration

Depending on the operation, 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 list of object types that work with operation.

**< Emerging Threats**



Disabled ☒ Enabled

Uninstall

**Configuration**

Api Key 

☐ Bypass system proxy configuration for this operation

Save

**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 on the object to access it's details page.
3. Scroll down to the *Operations* pane on the details page.

You can also click on the Operations heading located in the left-hand menu to jump the operations pane.

A list of available operations will be listed in the pane.

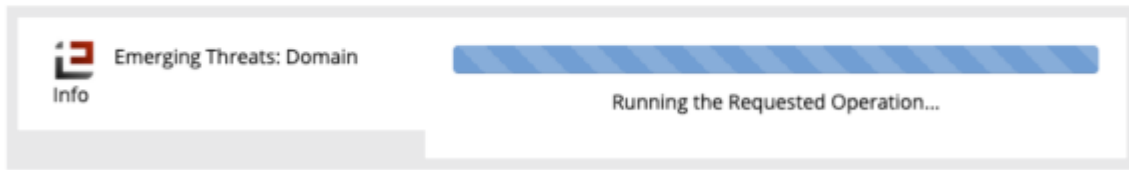
 **Operations**

 Emerging Threats: Domain Info

Select an operation on the left hand side to load results in this panel.

4. Click on an operation to run it.

  Operations



## Integration-Related Commands

The following integration-related commands can be found in the [Command Line Interface \(CLI\)](#) section:

- [Add/Update a CDF](#)
- [Source Consolidation](#)
- [Source Merge](#)
- [View Feed Queues](#)
- [Historic Feed Pulls](#)
- [iSight Historic Feed Pulls](#)
- [TIS Custom Connector Historic Feed Pulls](#)

## Activity Log (feeds)

The Activity Log provides you with details regarding recent runs performed by an feed integration.

|                                                                                                                 |                           |
|-----------------------------------------------------------------------------------------------------------------|---------------------------|
| Configuration                                                                                                   | Activity Log              |
| <b>Activity Log Details</b>  |                           |
| Scheduled Run<br>10/05/2020 05:13pm                                                                             | ✓ Completed ▶             |
| Scheduled Run<br>10/04/2020 05:13pm                                                                             | ✓ Completed ▶             |
| Scheduled Run<br>10/03/2020 05:13pm                                                                             | ✓ Completed ▶             |
| Scheduled Run<br>10/02/2020 05:13pm                                                                             | ✓ Completed ▶             |
| Scheduled Run                                                                                                   | ⚠ Completed with errors ▶ |

Log Details include 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.

Configuration

Activity Log

### 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

Download Files

#### Ingestion Summary

25 Adversaries

522 Adversary Attributes

174 Attack Patterns

1892 Attack Pattern  
Attributes

#### 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.

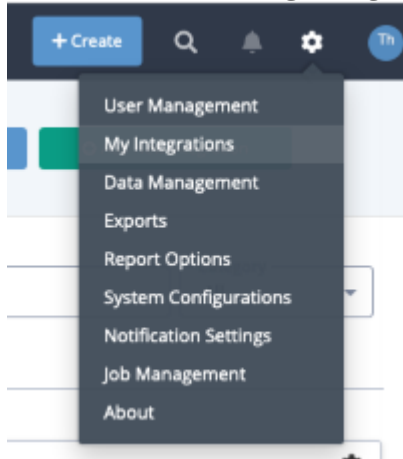
Ingested  
Summary

A summary of ingested object types.

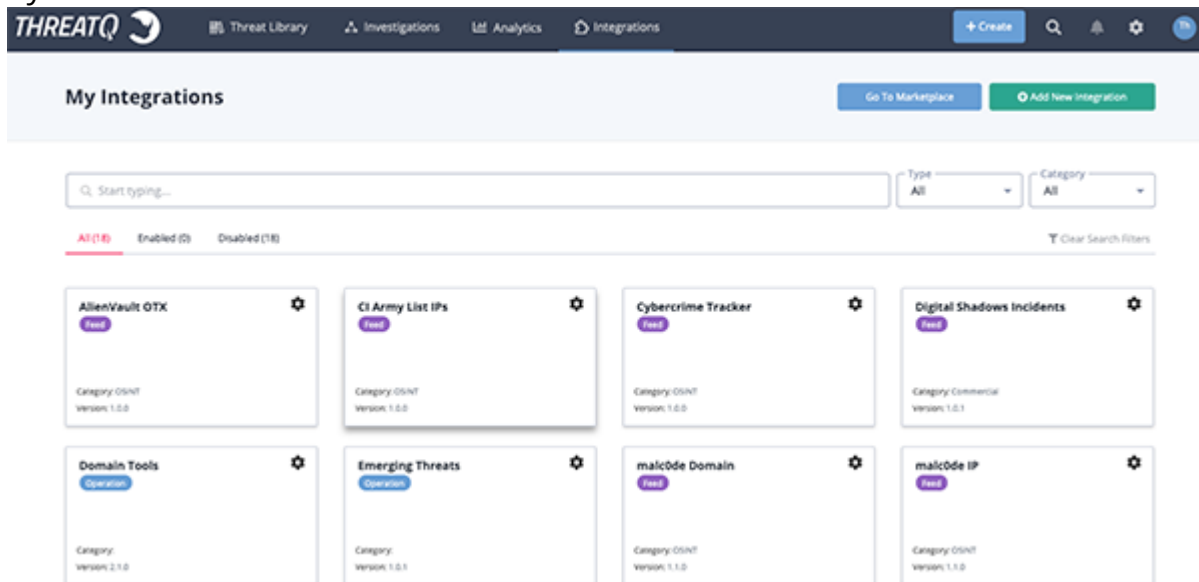
## Accessing an Intel Feed's Activity Log

The Activity for a feed will appear after the feed has performed an initial run.

1. Click on the **Settings**  and select **My Integrations**.



The My Integrations page will load. All integrations currently installed on your platform, both enabled and disabled, can be found on this page. The Enabled tab will be selected by default.



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

The integration details page will load.

| Configuration                                                                                                   | Activity Log                                                                                                |
|-----------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| <b>Activity Log Details</b>  |                                                                                                             |
| Scheduled Run<br>10/05/2020 05:13pm                                                                             | ✓ Completed              |
| Scheduled Run<br>10/04/2020 05:13pm                                                                             | ✓ Completed              |
| Scheduled Run<br>10/03/2020 05:13pm                                                                             | ✓ Completed              |
| Scheduled Run<br>10/02/2020 05:13pm                                                                             | ✓ Completed              |
| Scheduled Run                                                                                                   | ⚠ Completed with errors  |

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

| Configuration                                                                                                   | Activity Log                                                                                      |
|-----------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| <b>Activity Log Details</b>  |                                                                                                   |
| Scheduled Run<br>10/08/2020 05:25pm                                                                             | ✓ Completed  |

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

Query Range  
After 10/07/2020 05:25pm

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

Stored Files  
Download 2 files  
Password: threatq  
[Download Files](#)

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

Ingestion Summary  
⚠ 25 Adversaries  
⚠ 522 Adversary Attributes  
⚠ 174 Attack Patterns  
⚠ 1892 Attack Pattern Attributes



# Job Management

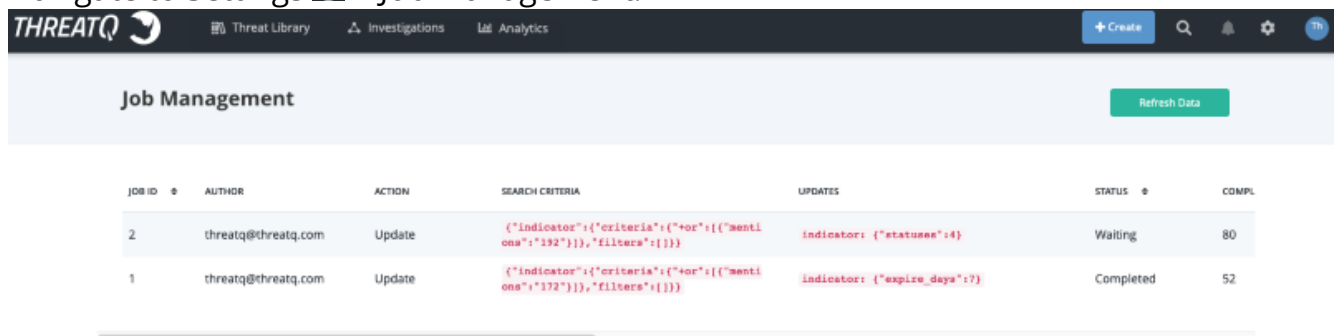


The Job Management page is only accessible to users with Administrator or Maintenance accounts.

The Job Management page allows you to view the status and outcome of [Bulk Actions](#).

## To access the Job Management page:

1. Navigate to Settings  > Job Management.



| JOB ID | AUTHOR              | ACTION | SEARCH CRITERIA                                                                                    | UPDATES                                      | STATUS    | COMPL |
|--------|---------------------|--------|----------------------------------------------------------------------------------------------------|----------------------------------------------|-----------|-------|
| 2      | threatq@threatq.com | Update | <code>{ "indicator": { "criteria": { "+or": { { "mentlona": "192" } } }, "filters": { } } }</code> | <code>indicator: { "statusee": 4 }</code>    | Waiting   | 80    |
| 1      | threatq@threatq.com | Update | <code>{ "indicator": { "criteria": { "+or": { { "mentlona": "172" } } }, "filters": { } } }</code> | <code>indicator: { "expire_days": 7 }</code> | Completed | 52    |

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                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                          | <p><b>Example:</b> 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_at": "2020-02-29"}</p>                                                                                                                                                                                                                            |
| Status                   | <p>The current status of the job.</p> <p>Possible statuses include:</p> <ul style="list-style-type: none"><li>• Created - The job has been queued.</li><li>• In-Progress - The job is running.</li><li>• Error - The job failed.</li><li>• Waiting - The job is waiting for indexing to be complete. This only applies to the Bulk Change process.</li><li>• Completed - The job has completed.</li></ul> |
| 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        | <p>This represents the amount of system objects associated with the job that have been processed.</p> <p><b>Example:</b> 100 indicators out of the 1000 associated with the job have been deleted = 10%.</p>                                                                                                                                                                                              |
| 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, are tied to your ThreatQ platform license. Adding these features will result in ThreatQ Support issuing a new license to apply to your platform.



ThreatQ licenses are not perpetual.

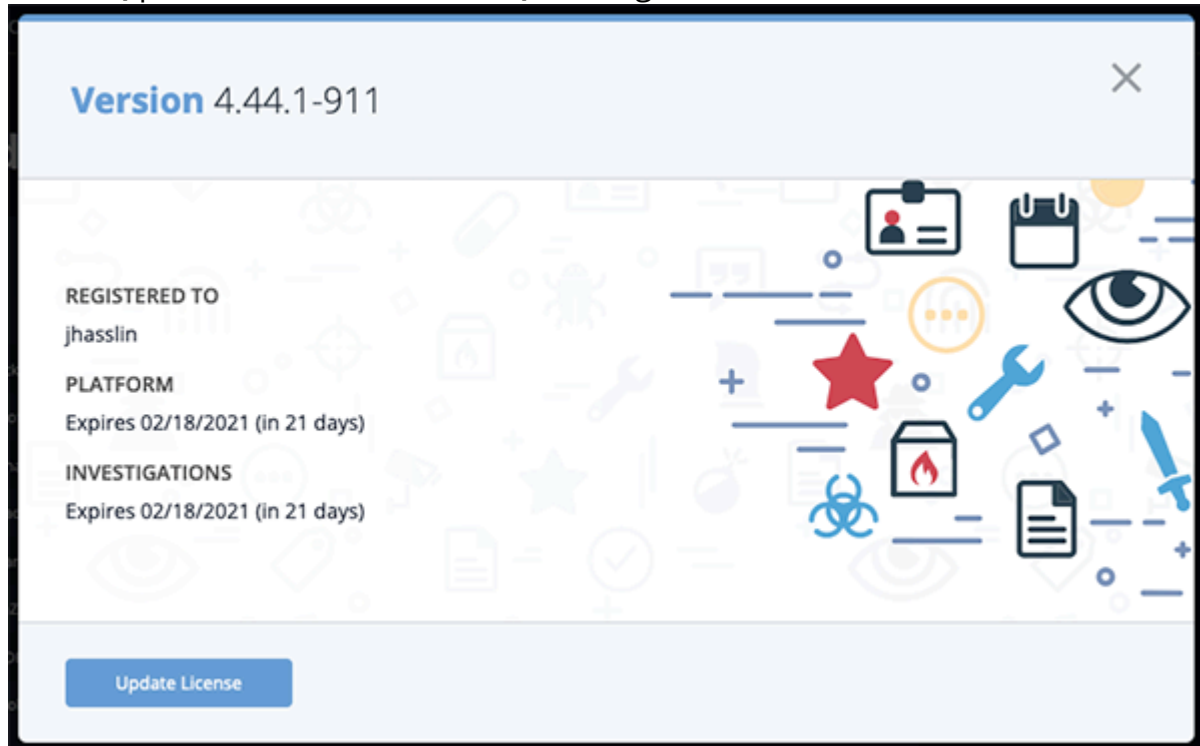
## Managing Your ThreatQ License

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.



## 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 | Threat Library | Access and search the Threat Library and view system object details.                                                                                     | <ul style="list-style-type: none"><li>• <a href="#">Threat Library</a></li><li>• <a href="#">Building Searches with Filter Sets</a></li><li>• <a href="#">Object Details</a></li><li>• <a href="#">Bulk Actions</a></li></ul> |
| 3 | Investigations | Navigates to ThreatQ Investigations, a cybersecurity situation room that enables collaborative threat analysis, investigation, and coordinated response. | <ul style="list-style-type: none"><li>• <a href="#">ThreatQ Investigations</a></li></ul>                                                                                                                                      |
| 4 | Analytics      | Navigates to the Analytics section which provides a summary view of Adversary, Event, File, Indicator, and Signature Object Types.                       | <ul style="list-style-type: none"><li>• <a href="#">Analytics</a></li></ul>                                                                                                                                                   |

| # | NAME                | DESCRIPTION                                                                                                                                                                                                   | REFERENCES                                                                                                                                                                                                                                              |
|---|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 5 | Integrations        | Allows you to access the Marketplace as well as you integrations.                                                                                                                                             | <ul style="list-style-type: none"><li>• ThreatQ Integrations</li></ul>                                                                                                                                                                                  |
| 6 | Create Button       | Create system objects.                                                                                                                                                                                        | <ul style="list-style-type: none"><li>• <a href="#">Adversaries</a></li><li>• <a href="#">Events</a></li><li>• <a href="#">Files</a></li><li>• <a href="#">Indicators</a></li><li>• <a href="#">Signatures</a></li><li>• <a href="#">STIX</a></li></ul> |
| 7 | Search Icon         | Perform a basic search for a system object.                                                                                                                                                                   | <ul style="list-style-type: none"><li>• <a href="#">Building Searches with Filter Sets</a></li></ul>                                                                                                                                                    |
| 8 | Message Center Icon | <p>Receive in-app notifications of system job processes such as Bulk Actions.</p> <p>Administrator and Maintenance account users will also receive feed health notifications.</p>                             | <ul style="list-style-type: none"><li>• <a href="#">Notification Center</a></li></ul>                                                                                                                                                                   |
| 9 | 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. | <ul style="list-style-type: none"><li>• Product Updates</li><li>• Installation</li><li>• Videos</li></ul>                                                                                                                                               |

| #  | NAME          | DESCRIPTION                                                               | REFERENCES                                                                                                                                                                                                                                                                                       |
|----|---------------|---------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 10 | Site Settings | Configure site settings such as user management, incoming feeds, TLP etc. | <ul style="list-style-type: none"><li>• <a href="#">User Management</a></li><li>• <a href="#">Integrations Management</a></li><li>• <a href="#">Data Management</a></li><li>• <a href="#">System Configuration</a></li><li>• <a href="#">Exports</a></li><li>• <a href="#">Reports</a></li></ul> |
| 10 | User Icon     | Access your user profile.                                                 | <ul style="list-style-type: none"><li>• <a href="#">User Management</a></li></ul>                                                                                                                                                                                                                |



# Notifications

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

In-app notifications include Bulk Action updates and feed health alerts.



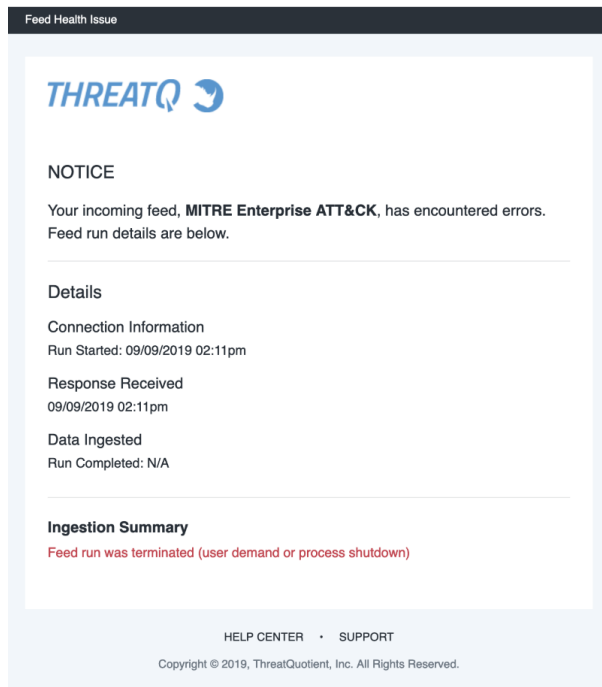
Only users with Administrator and Maintenance roles will receive in-app feed health alerts via the Notification Center.

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 performing a run.

# Feed Health Email Notifications

Feed Health Notifications allows the ThreatQ platform to send you, and other designated users, email notifications when a feed 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.



## Configuring Mail Server

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

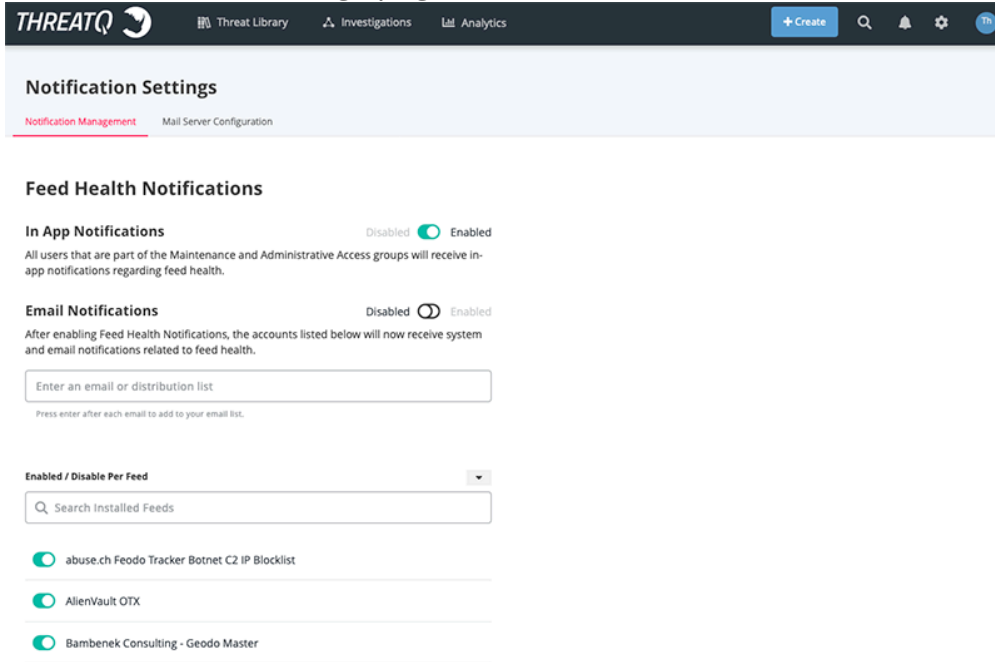


In the event that you have completed the mail server configuration and are still not receiving emails, your email provider may have marked the activity as suspicious. Some services, such as Gmail, will require you to confirm the activity, via an email message, before allowing the ThreatQ application 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:

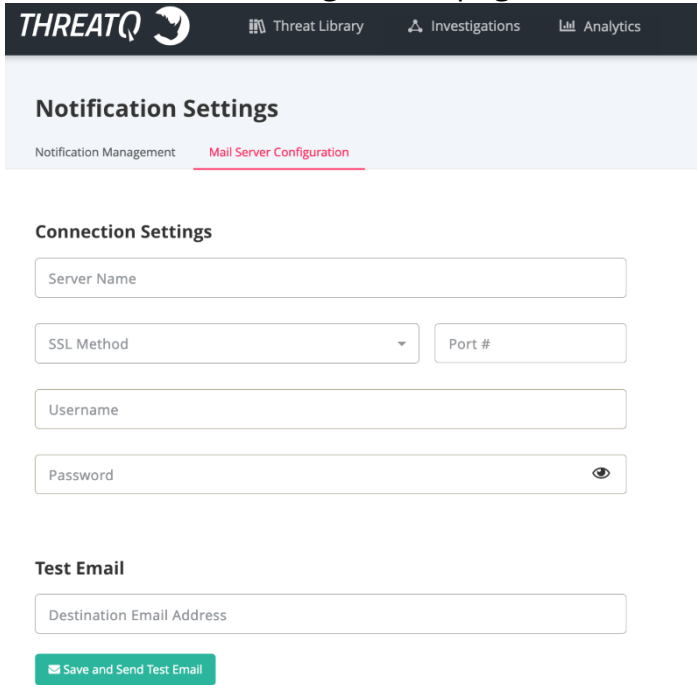
1. Click on the **System Settings**  and select the **Notification Settings** option.

The Notification Settings page loads.



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

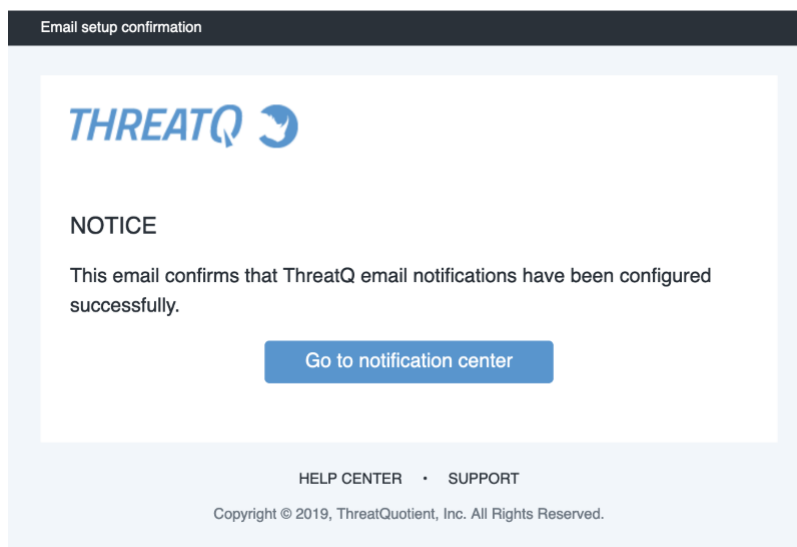
The Mail Server Configuration page loads.



3. Complete the following fields:

| FIELD       | DESCRIPTION                                                                                                                      |
|-------------|----------------------------------------------------------------------------------------------------------------------------------|
| Server Name | The address of your mail server.                                                                                                 |
| SSL Method  | The SSL method used. There are three options: <ul style="list-style-type: none"><li>◦ SSL</li><li>◦ TLS</li><li>◦ None</li></ul> |
| 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.



- 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 be completed before you enable the feature.

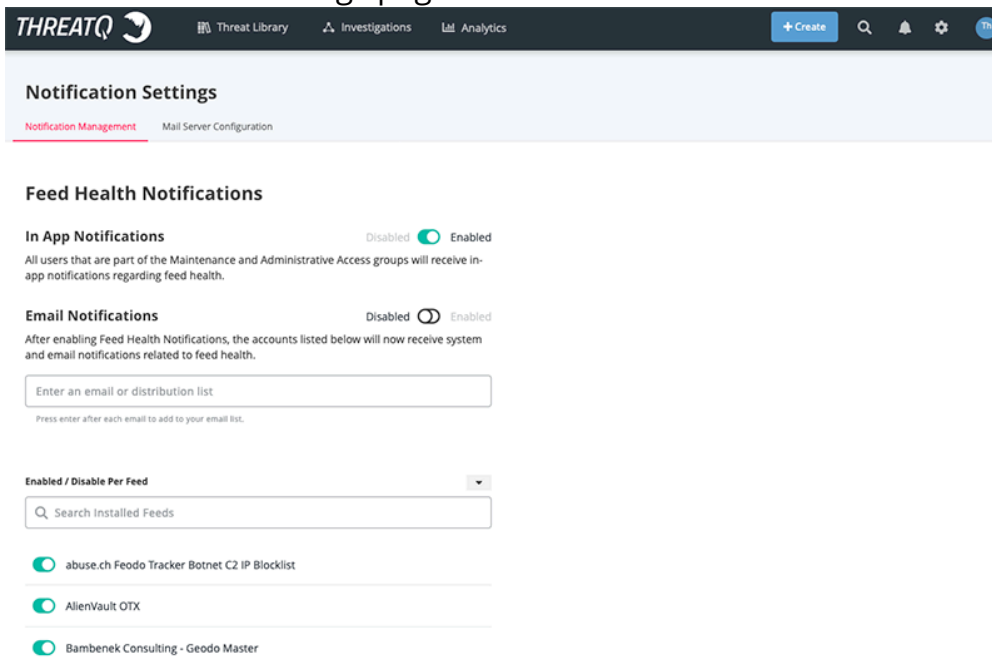


In the event that you have completed the mail server configuration and are still not receiving emails, your email provider may have marked the activity as suspicious. Some services, such as Gmail, will require you to confirm the activity, via an email message, before allowing the ThreatQ application 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:

- Click on the **System Settings**  gear icon and select the **Notification Settings** option.

The Notification Settings page loads.



The screenshot shows the ThreatQ web interface. The top navigation bar includes the ThreatQ logo, links to Threat Library, Investigations, and Analytics, and a + Create button. The main content area is titled 'Notification Settings' and has two tabs: 'Notification Management' (selected) and 'Mail Server Configuration'. Under 'Notification Management', there are two sections: 'In App Notifications' and 'Email Notifications'. Both sections have a toggle switch set to 'Enabled'. The 'Email Notifications' section includes a text input field for 'Enter an email or distribution list' and a dropdown menu for 'Enabled / Disable Per Feed'. Below these are three entries, each with a toggle switch set to 'Enabled': 'abuse.ch Feodo Tracker Botnet C2 IP Blocklist', 'AlienVault OTX', and '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

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

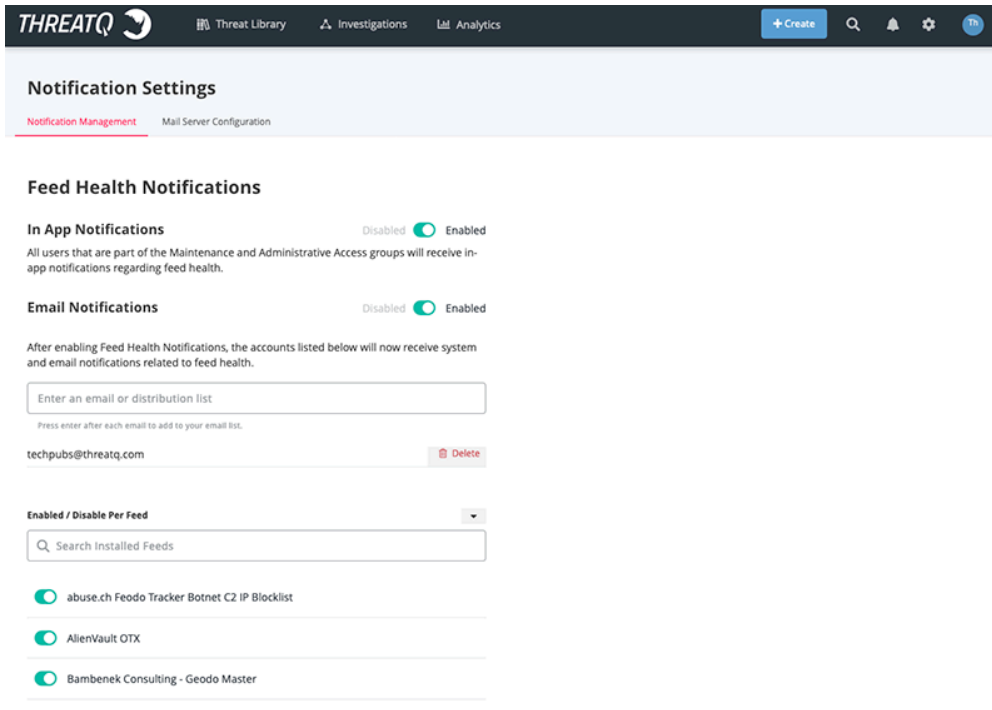
Press enter after each email to add to your email list.

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  
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.

techpubs@threatq.com [Delete](#)

Enabled / Disable Per Feed

Search Installed Feeds

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

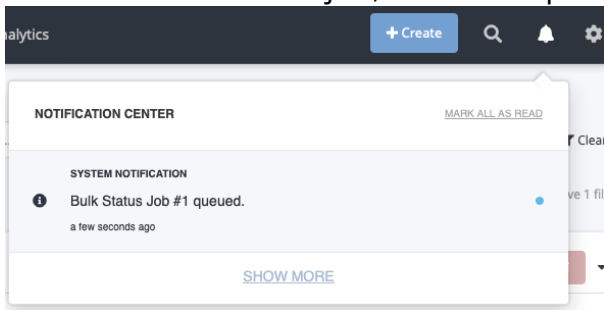


You can also enable/disable individual CDF feed notifications by clicking on the feed under [Integrations](#) and checking/unchecking the notifications checkbox.

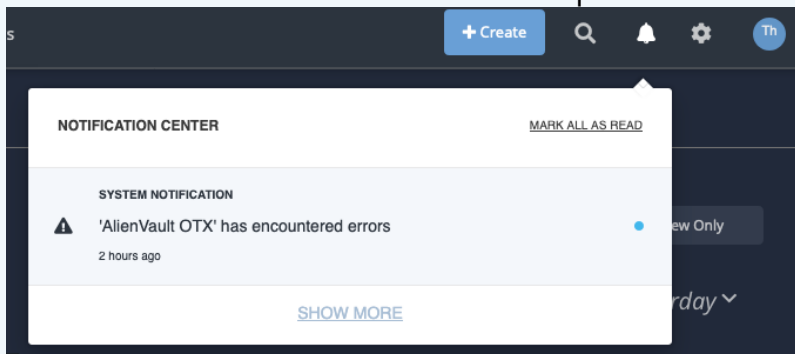
# Notification Center

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 Action job, has been queued and/or completed.



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.



# Reports

You can export a PDF Summary of an object from an object's details page.

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

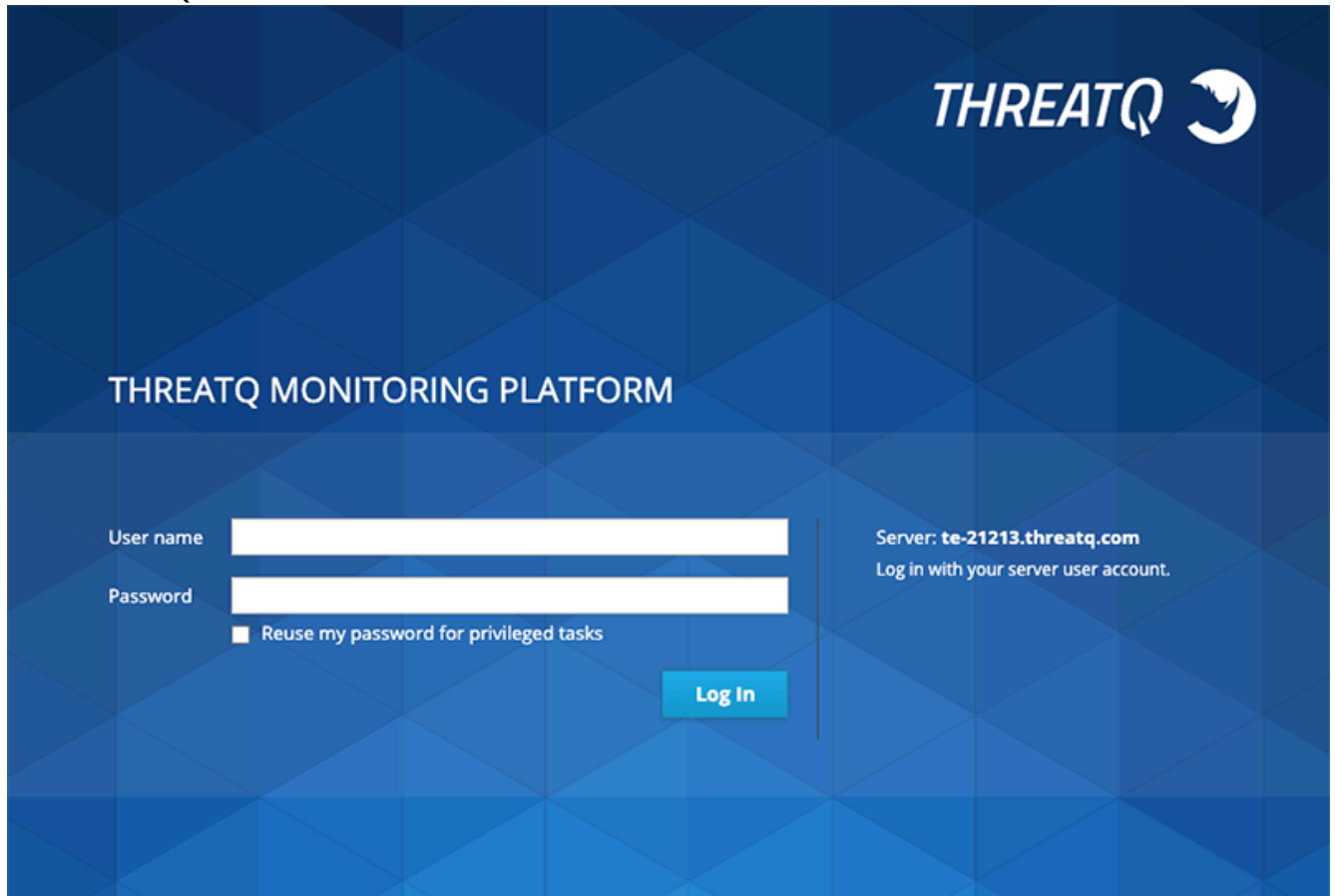
## Accessing the ThreatQ Monitoring Platform



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 

THREATQ MONITORING PLATFORM

User name

Password

☐ Reuse my password for privileged tasks

Log In

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.

THREATQ

Cloud User

te-21213.threat...

System

Logs

Storage

Networking

Containers

Accounts

Services

Dagnostic Reports

Kernel Dump

SELinux

Terminal

Hardware

Asset Tag

Machine ID

Operating System

Secure Shell Keys

Host Name

Domain

System Time

Power Options

Performance Profile

RDO OpenStack Compute

a0cd0e72-7f15-4ced-ae1d-6fc579107ab2

93fe483c696d47f68791067e240e1427

CentOS Linux 7 (Core)

[Show fingerprints](#)

te-21213.threatq.com

Join Domain

2020-12-15 17:49 ⓘ

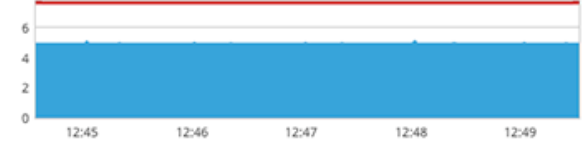
Restart

virtual-guest

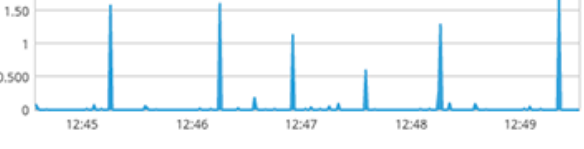
% of 4 CPU cores



GIB Memory & Swap



MIB/s Disk I/O



Kbps Network Traffic



# System Configuration

The System Configuration section of the ThreatQ platform allows you:

| SECTION                             | DETAILS                                                                                                                                                             |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">Indicator Statuses</a>  | Create and edit custom indicator statuses.                                                                                                                          |
| <a href="#">Indicator Types</a>     | View your platform's indicators types.                                                                                                                              |
| <a href="#">Event Types</a>         | Create and edit custom event types.                                                                                                                                 |
| <a href="#">Proxy</a>               | Enable and disable proxy settings.                                                                                                                                  |
| <a href="#">Account Security</a>    | 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. |
| <a href="#">LDAP Authentication</a> | Configure system access via LDAP, the Lightweight Directory Access Protocol.                                                                                        |
| <a href="#">SAML Authentication</a> | Configure system single sign-on (SSO) access via SAML, Security Assertion Markup Language.                                                                          |
| <a href="#">General Settings</a>    | Configure system date and time format as well as indicator parsing checkbox defaults.                                                                               |

## Indicator Statuses

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  > System Configurations.

The System Configurations page opens to the Indicator Statuses tab.

**System Configurations**

Indicator Statuses | Indicator Types | Event Types | Proxy | Account Security | LDAP | SAML | General

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.](#)

| STATUS                               | DESCRIPTION                                              | PROTECT FROM FEED OVERRIDE          | TOTAL INDICATORS |
|--------------------------------------|----------------------------------------------------------|-------------------------------------|------------------|
| <input type="checkbox"/> Active      | Poses a threat and is being exported to detection tools. | <input checked="" type="checkbox"/> | 0                |
| <input type="checkbox"/> Expired     | No longer poses a serious threat.                        | <input type="checkbox"/>            | 0                |
| <input type="checkbox"/> Indirect    | Associated to an active indicator or event (i.e. pONS).  | <input type="checkbox"/>            | 0                |
| <input type="checkbox"/> Review      | Requires further analysis.                               | <input type="checkbox"/>            | 0                |
| <input type="checkbox"/> Whitelisted | Poses NO risk and should never be deployed.              | <input checked="" type="checkbox"/> | 0                |

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

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

### Indicator Statuses Table Functions:

| FUNCTION                                             | DESCRIPTION                                                                                                                                             |
|------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| Change the number of entries displayed in the table. | 1. Click the dropdown menu at the top right of the table and select the desired option.                                                                 |
| Sort the table by a column.                          | <ol style="list-style-type: none"> <li>Click the column header.</li> <li>To reverse the column sorting order, click the header a second time</li> </ol> |

## 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.

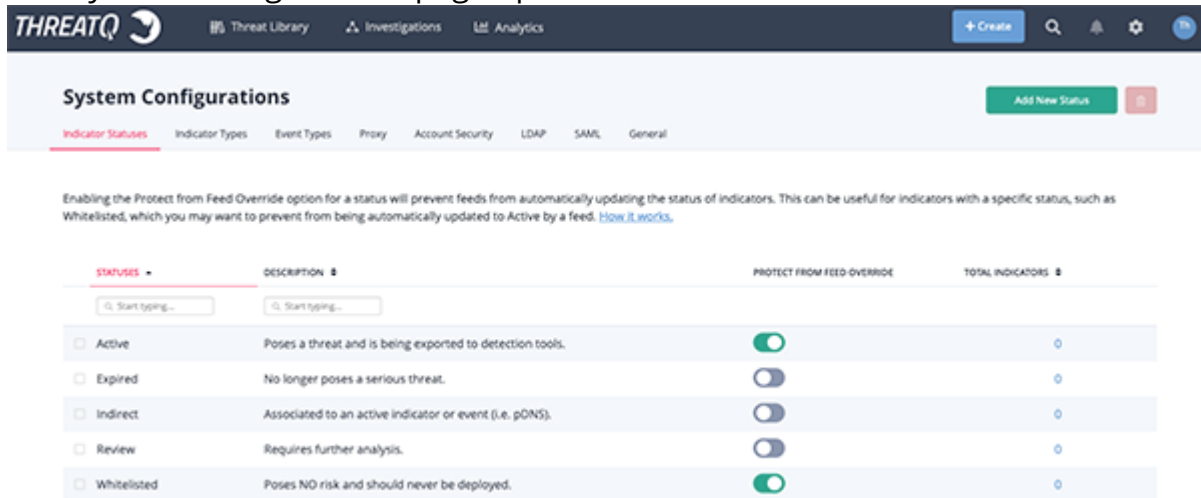
The System Configurations page opens to the Indicator Statuses tab.

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

The System Configurations page opens to the Indicator Statuses tab.



**System Configurations** Add New Status

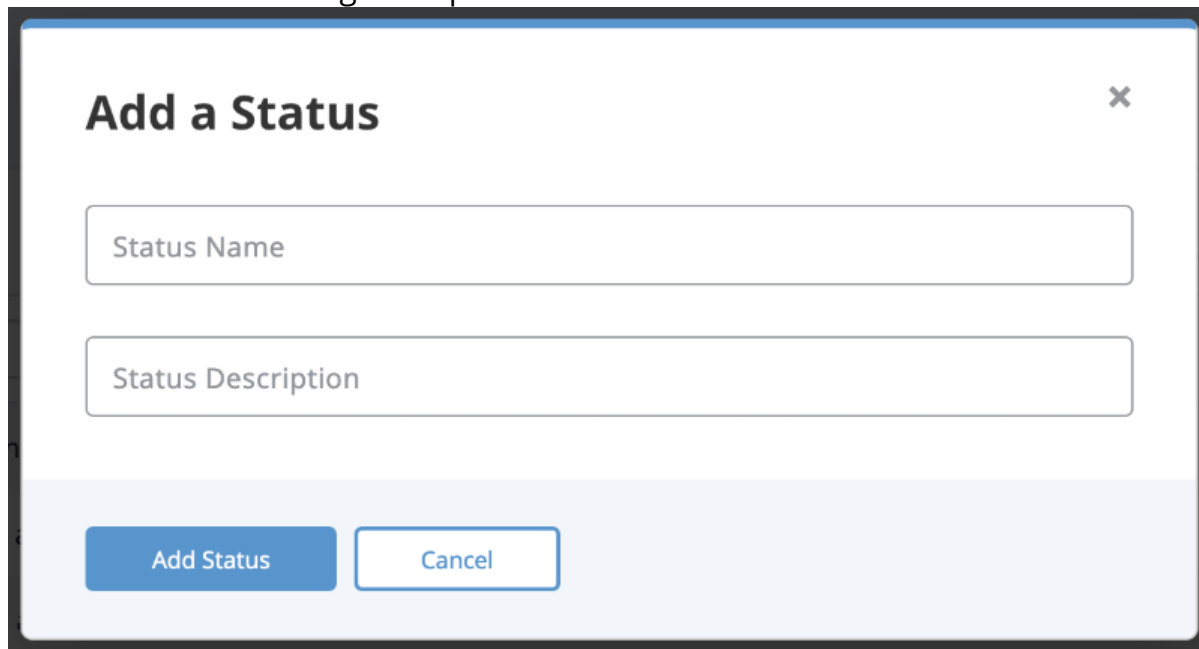
Indicator Statuses | Indicator Types | Event Types | Proxy | Account Security | LDAP | SAML | General

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 |
|--------------------------------------|----------------------------------------------------------|-------------------------------------|------------------|
| <input type="checkbox"/> Active      | Poses a threat and is being exported to detection tools. | <input checked="" type="checkbox"/> | 0                |
| <input type="checkbox"/> Expired     | No longer poses a serious threat.                        | <input type="checkbox"/>            | 0                |
| <input type="checkbox"/> Indirect    | Associated to an active indicator or event (i.e. pDNS).  | <input type="checkbox"/>            | 0                |
| <input type="checkbox"/> Review      | Requires further analysis.                               | <input type="checkbox"/>            | 0                |
| <input type="checkbox"/> Whitelisted | Poses NO risk and should never be deployed.              | <input checked="" type="checkbox"/> | 0                |

2. Click **Add New Status**.

The Add a Status dialog box opens.

A dialog box titled "Add a Status" with a close button (X) in the top right corner. It contains two text input fields: "Status Name" and "Status Description". At the bottom, there are two buttons: "Add Status" (blue) and "Cancel" (white with blue border).

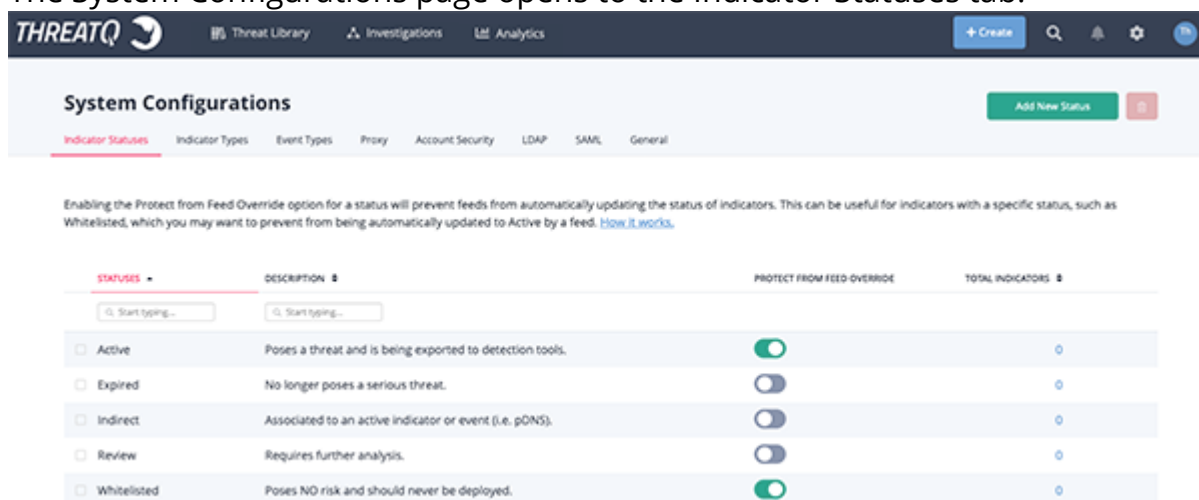
3. Enter a **Status Name**.
4. Optionally, enter a **Status Description**.
5. Click **Add Status**.

## Editing an Indicator Status

 You cannot edit an indicator status provided by ThreatQ.

1. Navigate to Settings  > System Configurations.

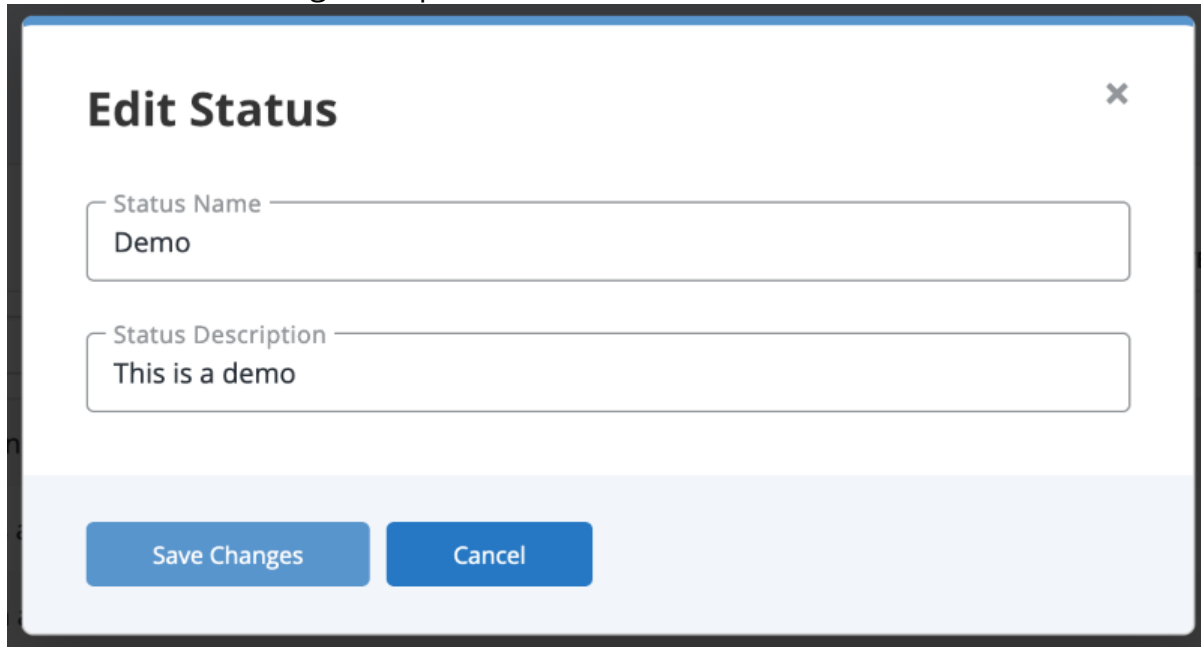
The System Configurations page opens to the Indicator Statuses tab.

The System Configurations page in ThreatQ. The top navigation bar includes ThreatQ logo, Threat Library, Investigations, Analytics, and a + Create button. The main header is "System Configurations" with a sub-header "Indicator Statuses" and a "Add New Status" button. Below the header, there is a table with columns: STATUSES, DESCRIPTION, PROTECT FROM FEED OVERRIDE, and TOTAL INDICATORS. The table lists five statuses: Active, Expired, Indirect, Review, and Whitelisted, each with a checkbox, a description, a toggle switch for "PROTECT FROM FEED OVERRIDE", and a count of "TOTAL INDICATORS".

| STATUSES                             | DESCRIPTION                                              | PROTECT FROM FEED OVERRIDE          | TOTAL INDICATORS |
|--------------------------------------|----------------------------------------------------------|-------------------------------------|------------------|
| <input type="checkbox"/> Active      | Poses a threat and is being exported to detection tools. | <input checked="" type="checkbox"/> | 0                |
| <input type="checkbox"/> Expired     | No longer poses a serious threat.                        | <input type="checkbox"/>            | 0                |
| <input type="checkbox"/> Indirect    | Associated to an active indicator or event (i.e. pONS).  | <input type="checkbox"/>            | 0                |
| <input type="checkbox"/> Review      | Requires further analysis.                               | <input type="checkbox"/>            | 0                |
| <input type="checkbox"/> Whitelisted | Poses NO risk and should never be deployed.              | <input checked="" type="checkbox"/> | 0                |

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

The Edit Status dialog box opens.

The image shows a dialog box titled "Edit Status" with a close button (X) in the top right corner. It contains two text input fields. The first field is labeled "Status Name" and contains the text "Demo". The second field is labeled "Status Description" and contains the text "This is a demo". At the bottom of the dialog box, there are two buttons: "Save Changes" and "Cancel".

**Edit Status** ×

Status Name

Status Description

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  > System Configurations.

The System Configurations page opens to the Indicator Statuses tab.

System Configurations

Indicator Statuses | Indicator Types | Event Types | Proxy | Account Security | LDAP | SAML | General

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 |
|------------------------------------------|----------------------------------------------------------|-------------------------------------|------------------|
| <input type="checkbox"/> Start typing... | <input type="text" value="Start typing..."/>             |                                     |                  |
| <input type="checkbox"/> Active          | Poses a threat and is being exported to detection tools. | <input checked="" type="checkbox"/> | 0                |
| <input type="checkbox"/> Expired         | No longer poses a serious threat.                        | <input type="checkbox"/>            | 0                |
| <input type="checkbox"/> Indirect        | Associated to an active indicator or event (i.e. pONS).  | <input type="checkbox"/>            | 0                |
| <input type="checkbox"/> Review          | Requires further analysis.                               | <input type="checkbox"/>            | 0                |
| <input type="checkbox"/> Whitelisted     | Poses NO risk and should never be deployed.              | <input checked="" type="checkbox"/> | 0                |

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

Delete statuses Cancel

- Click **Delete Statuses**.

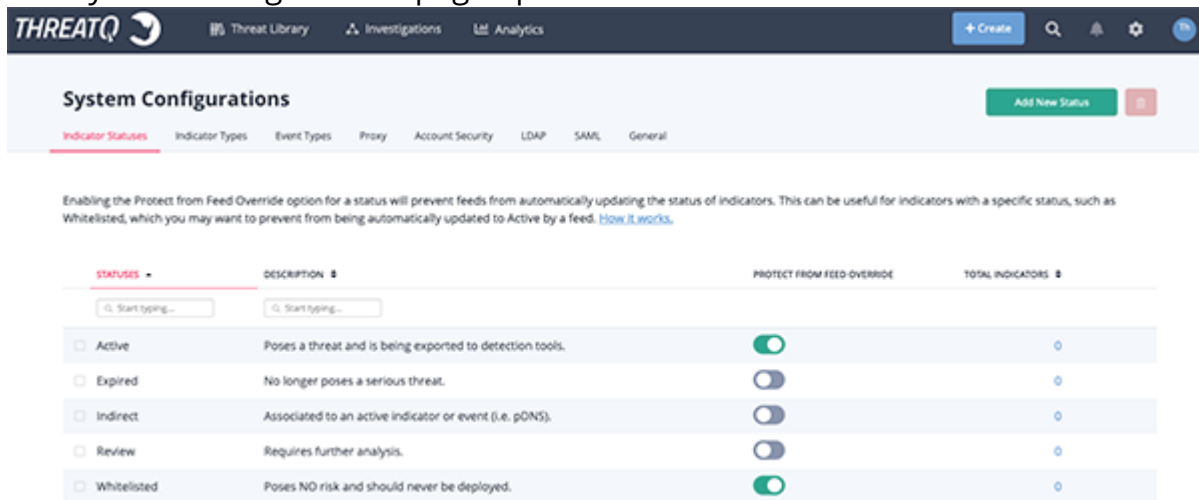
# Indicator Types

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

To view Indicator Types found within ThreatQ:

1. Navigate to Settings  > System Configurations.

The System Configurations page opens.

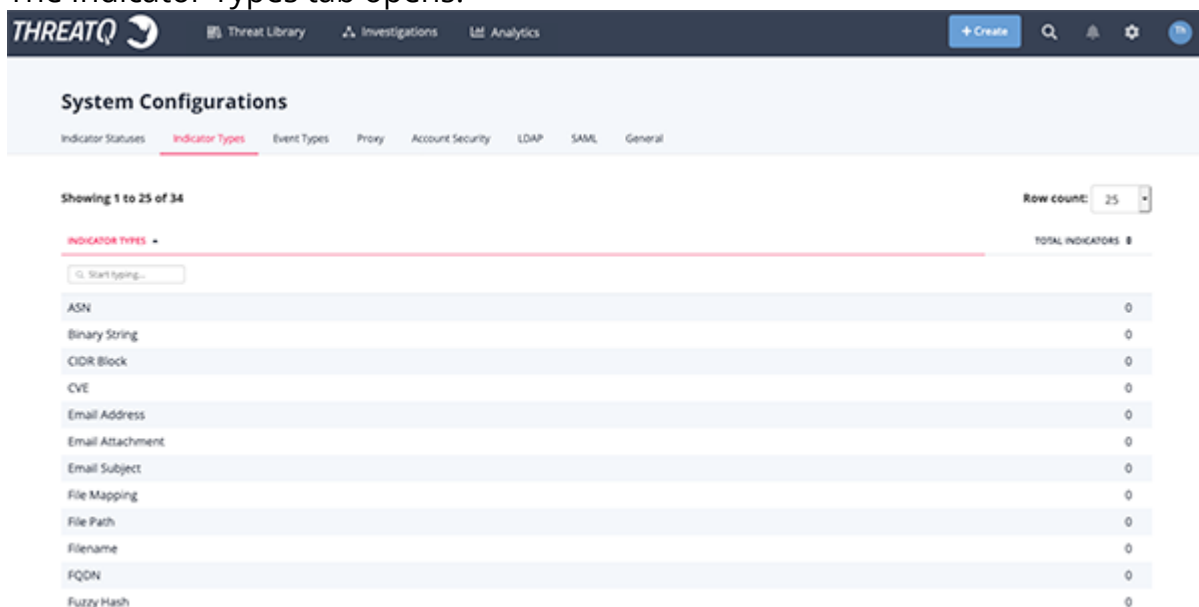


The screenshot shows the ThreatQ System Configurations page with the 'Indicator Statuses' tab selected. The page includes a header with navigation links and a 'Create' button. Below the header, there's a section for 'System Configurations' with a sub-tab 'Indicator Statuses'. A note explains the 'Protect from Feed Override' option. The main table lists various indicator statuses with their descriptions, protection toggle, and total indicator count.

| STATUS                               | DESCRIPTION                                              | PROTECT FROM FEED OVERRIDE          | TOTAL INDICATORS |
|--------------------------------------|----------------------------------------------------------|-------------------------------------|------------------|
| <input type="checkbox"/> Active      | Poses a threat and is being exported to detection tools. | <input checked="" type="checkbox"/> | 0                |
| <input type="checkbox"/> Expired     | No longer poses a serious threat.                        | <input type="checkbox"/>            | 0                |
| <input type="checkbox"/> Indirect    | Associated to an active indicator or event (i.e. pDNS).  | <input type="checkbox"/>            | 0                |
| <input type="checkbox"/> Review      | Requires further analysis.                               | <input type="checkbox"/>            | 0                |
| <input type="checkbox"/> Whitelisted | Poses NO risk and should never be deployed.              | <input checked="" type="checkbox"/> | 0                |

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

The Indicator Types tab opens.

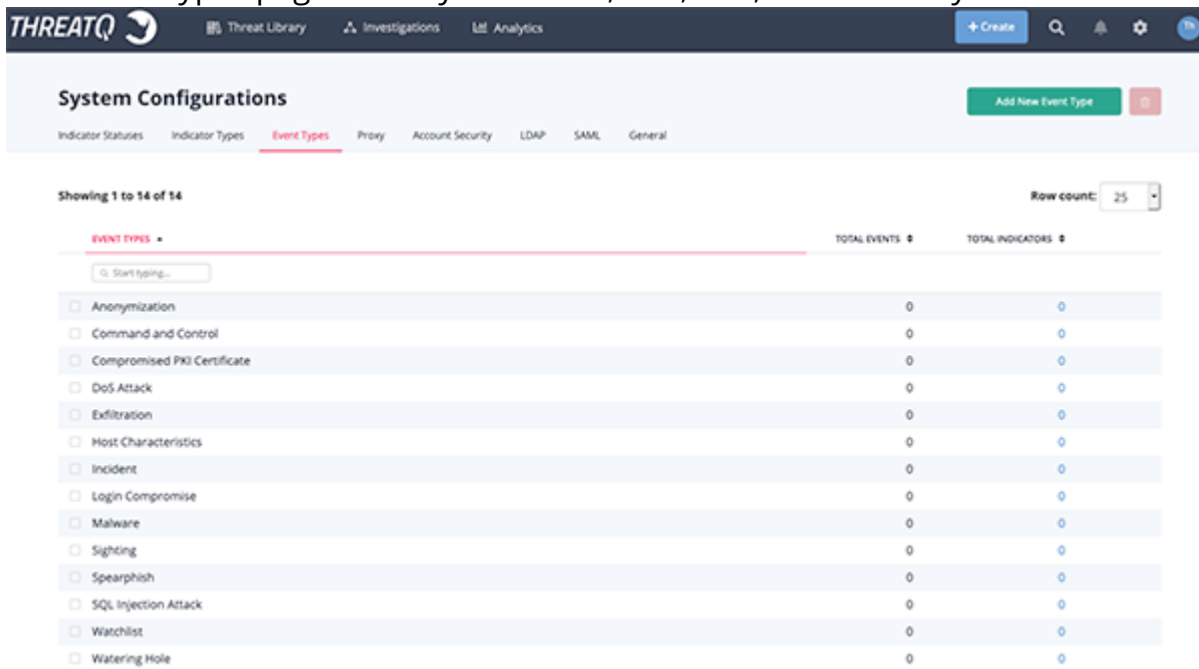


The screenshot shows the ThreatQ System Configurations page with the 'Indicator Types' tab selected. The page displays a list of indicator types and the total number of indicators for each. The row count is set to 25.

| 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                |
| File Path        | 0                |
| Filename         | 0                |
| FQDN             | 0                |
| Fuzzy Hash       | 0                |

# Event Types

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



The screenshot shows the ThreatQ interface for managing Event Types. The top navigation bar includes 'Threat Library', 'Investigations', and 'Analytics'. The 'System Configurations' section is active, with a sub-tab for 'Event Types'. A table lists 14 event types, each with a checkbox, a name, and two columns for 'TOTAL EVENTS' and 'TOTAL INDICATORS'. All values are currently 0. A search bar is at the top of the table, and a 'Row count' dropdown is set to 25.

| EVENT TYPES                                          | TOTAL EVENTS | TOTAL INDICATORS |
|------------------------------------------------------|--------------|------------------|
| <input type="checkbox"/> Anonymization               | 0            | 0                |
| <input type="checkbox"/> Command and Control         | 0            | 0                |
| <input type="checkbox"/> Compromised PKI Certificate | 0            | 0                |
| <input type="checkbox"/> DoS Attack                  | 0            | 0                |
| <input type="checkbox"/> Exfiltration                | 0            | 0                |
| <input type="checkbox"/> Host Characteristics        | 0            | 0                |
| <input type="checkbox"/> Incident                    | 0            | 0                |
| <input type="checkbox"/> Login Compromise            | 0            | 0                |
| <input type="checkbox"/> Malware                     | 0            | 0                |
| <input type="checkbox"/> Sighting                    | 0            | 0                |
| <input type="checkbox"/> Spearphish                  | 0            | 0                |
| <input type="checkbox"/> SQL Injection Attack        | 0            | 0                |
| <input type="checkbox"/> Watchlist                   | 0            | 0                |
| <input type="checkbox"/> 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  > System Configurations.

The System Configurations page opens.

The screenshot shows the ThreatQ System Configurations page with the 'Indicator Statuses' tab selected. The page header includes the ThreatQ logo, navigation links (Threat Library, Investigations, Analytics), and a '+ Create' button. Below the header, there's a sub-header 'System Configurations' with a tab bar containing 'Indicator Statuses', 'Indicator Types', 'Event Types', 'Proxy', 'Account Security', 'LDAP', 'SAML', and 'General'. A green 'Add New Status' button is visible. A descriptive paragraph explains the 'Protect from Feed Override' option. Below this is a table with columns: 'STATUSES', 'DESCRIPTION', 'PROTECT FROM FEED OVERRIDE', and 'TOTAL INDICATORS'.

| STATUSES                             | DESCRIPTION                                              | PROTECT FROM FEED OVERRIDE          | TOTAL INDICATORS |
|--------------------------------------|----------------------------------------------------------|-------------------------------------|------------------|
| <input type="checkbox"/> Active      | Poses a threat and is being exported to detection tools. | <input checked="" type="checkbox"/> | 0                |
| <input type="checkbox"/> Expired     | No longer poses a serious threat.                        | <input type="checkbox"/>            | 0                |
| <input type="checkbox"/> Indirect    | Associated to an active indicator or event (i.e. pONS).  | <input type="checkbox"/>            | 0                |
| <input type="checkbox"/> Review      | Requires further analysis.                               | <input type="checkbox"/>            | 0                |
| <input type="checkbox"/> Whitelisted | Poses NO risk and should never be deployed.              | <input checked="" type="checkbox"/> | 0                |

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

The Event Types tab opens.

The screenshot shows the ThreatQ System Configurations page with the 'Event Types' tab selected. The page header is identical to the previous screenshot. The sub-header 'System Configurations' now has 'Event Types' selected in the tab bar. A green 'Add New Event Type' button is visible. Below the header, there's a 'Showing 1 to 14 of 14' indicator and a 'Row count: 25' dropdown menu. The table below has columns: 'EVENT TYPES', 'TOTAL EVENTS', and 'TOTAL INDICATORS'.

| EVENT TYPES                                          | TOTAL EVENTS | TOTAL INDICATORS |
|------------------------------------------------------|--------------|------------------|
| <input type="checkbox"/> Anonymization               | 0            | 0                |
| <input type="checkbox"/> Command and Control         | 0            | 0                |
| <input type="checkbox"/> Compromised PKI Certificate | 0            | 0                |
| <input type="checkbox"/> DoS Attack                  | 0            | 0                |
| <input type="checkbox"/> Exfiltration                | 0            | 0                |
| <input type="checkbox"/> Host Characteristics        | 0            | 0                |
| <input type="checkbox"/> Incident                    | 0            | 0                |
| <input type="checkbox"/> Login Compromise            | 0            | 0                |
| <input type="checkbox"/> Malware                     | 0            | 0                |
| <input type="checkbox"/> Sighting                    | 0            | 0                |
| <input type="checkbox"/> Spearphish                  | 0            | 0                |
| <input type="checkbox"/> SQL Injection Attack        | 0            | 0                |
| <input type="checkbox"/> Watchlist                   | 0            | 0                |
| <input type="checkbox"/> Watering Hole               | 0            | 0                |

## Event Types Table Functions:

### FUNCTION

### DESCRIPTION

Changing the number of entries displayed in the table

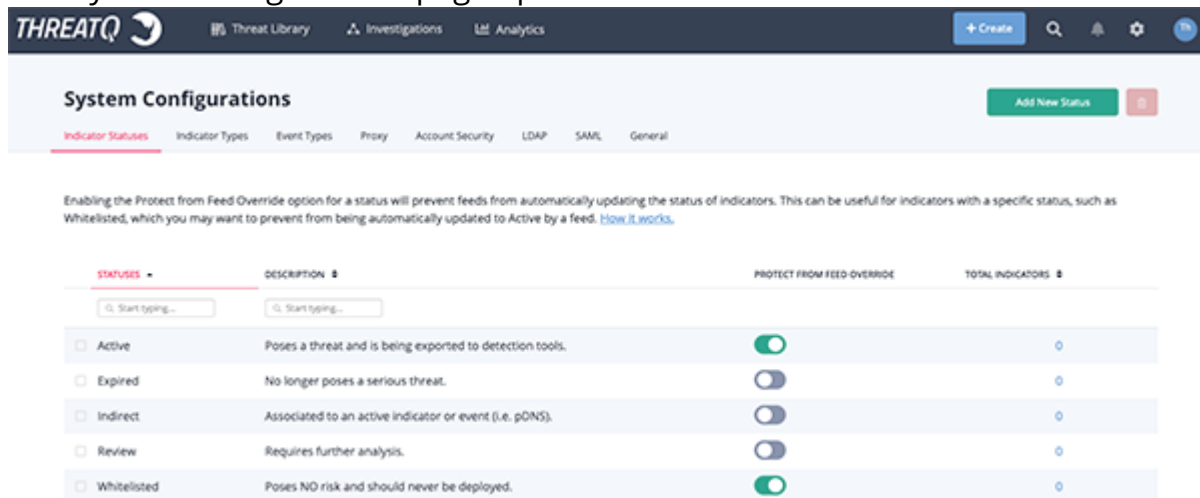
1. Click the dropdown menu at the top right of the table and select the desired option.

| FUNCTION                      | DESCRIPTION                                                                                                                                                 |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Sorting the table by a column | <ol style="list-style-type: none"><li>1. Click the column header.</li><li>2. To reverse the column sorting order, click the header a second time.</li></ol> |

## Adding an Event Type

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

The System Configurations page opens to the Indicator Statuses tab.



**System Configurations**

Indicator Statuses | Indicator Types | Event Types | Proxy | Account Security | LDAP | SAML | General

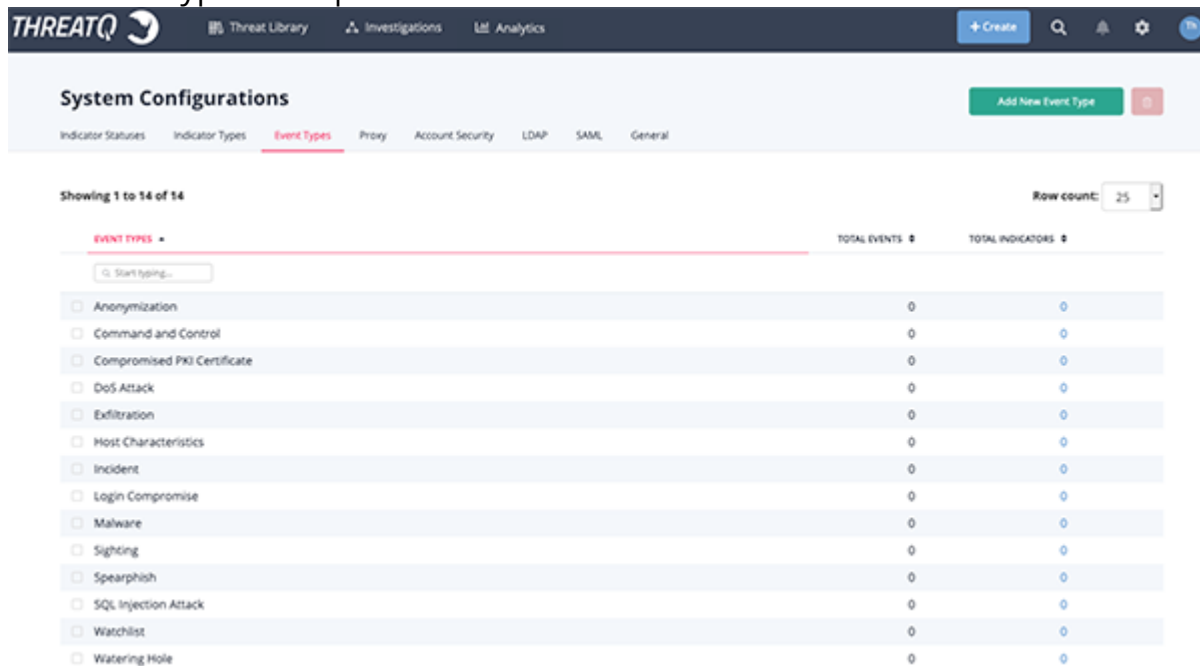
Enabling the Protect from Feed Override option for a status will prevent feeds from automatically updating the status of indicators. This can be useful for indicators with a specific status, such as Whitelisted, which you may want to prevent from being automatically updated to Active by a feed. [How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

| STATUSES ▾                           | DESCRIPTION ▾                                            | PROTECT FROM FEED OVERRIDE          | TOTAL INDICATORS ▾ |
|--------------------------------------|----------------------------------------------------------|-------------------------------------|--------------------|
| <input type="checkbox"/> Active      | Poses a threat and is being exported to detection tools. | <input checked="" type="checkbox"/> | 0                  |
| <input type="checkbox"/> Expired     | No longer poses a serious threat.                        | <input type="checkbox"/>            | 0                  |
| <input type="checkbox"/> Indirect    | Associated to an active indicator or event (i.e. pONS).  | <input type="checkbox"/>            | 0                  |
| <input type="checkbox"/> Review      | Requires further analysis.                               | <input type="checkbox"/>            | 0                  |
| <input type="checkbox"/> Whitelisted | Poses NO risk and should never be deployed.              | <input checked="" type="checkbox"/> | 0                  |

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

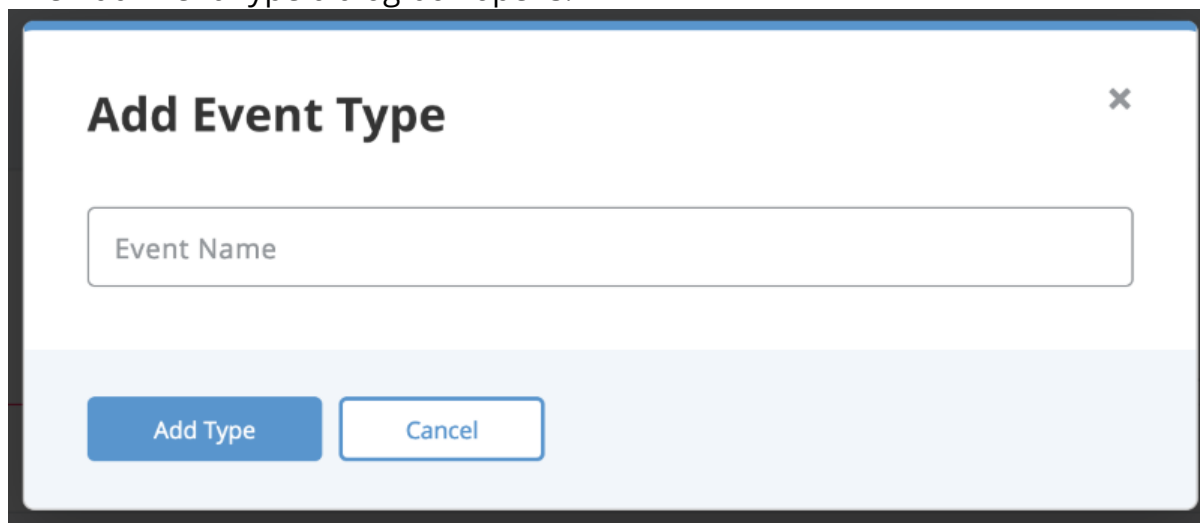


The Event Types tab opens.



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

The Add Event Type dialog box opens.



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

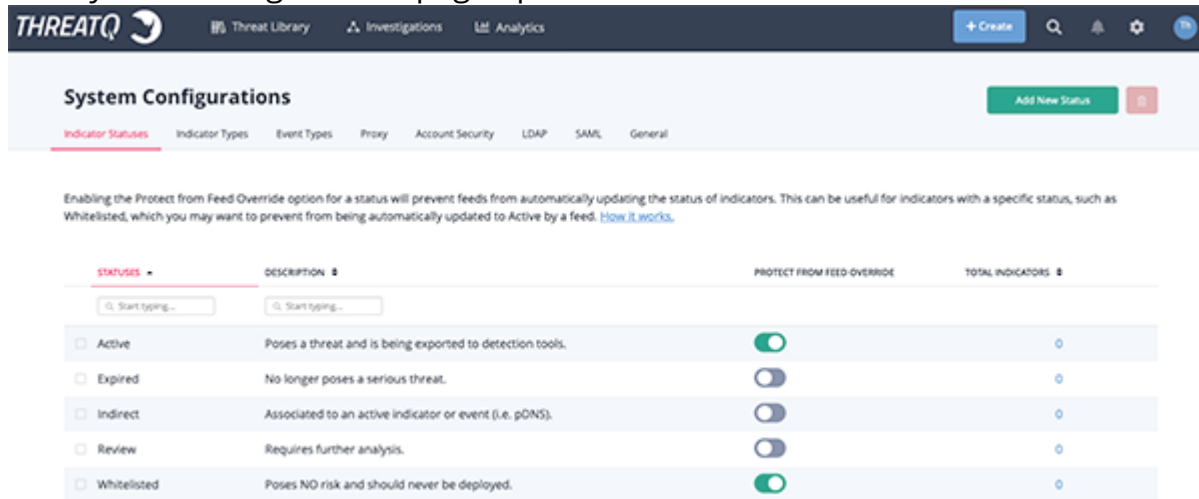
## Editing an Event Type

You can edit user-generated event types.

 You cannot edit an Event Type provided by ThreatQ.

1. Navigate to Settings  > System Configurations.

The System Configurations page opens to the Indicator Statuses tab.

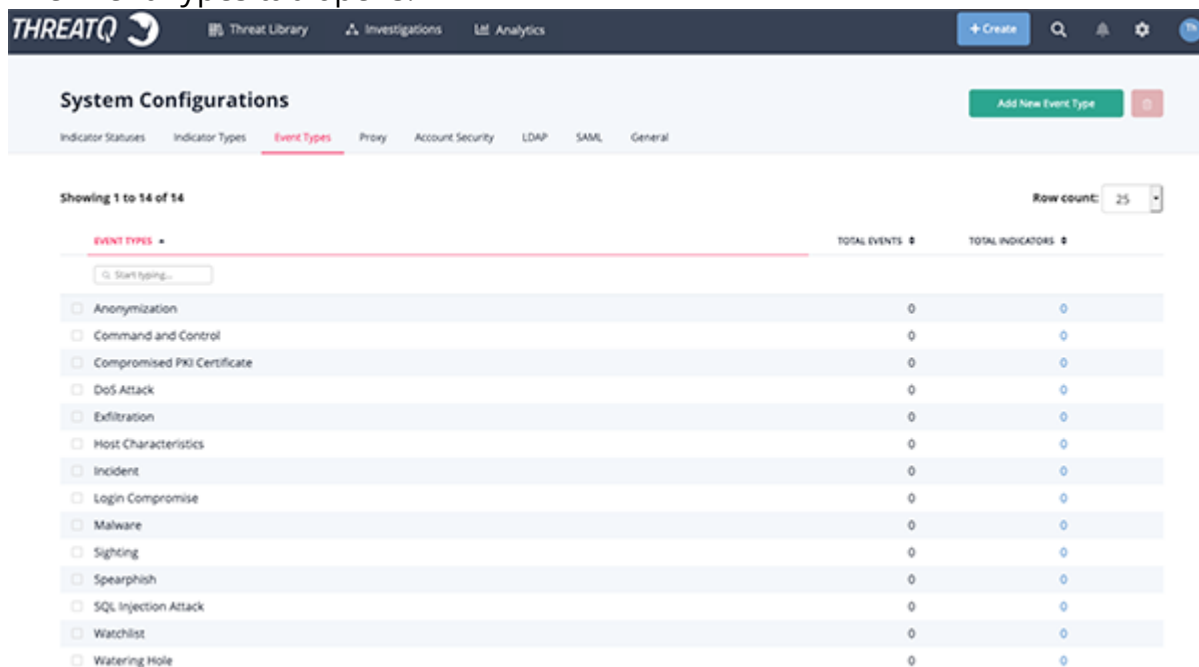


The screenshot shows the ThreatQ System Configurations page with the 'Indicator Statuses' tab selected. The page header includes the ThreatQ logo, navigation links (Threat Library, Investigations, Analytics), and a '+ Create' button. Below the header, the 'System Configurations' section has tabs for Indicator Statuses, Indicator Types, Event Types, Proxy, Account Security, LDAP, SAML, and General. A green 'Add New Status' button is visible. A note explains the 'Protect from Feed Override' option. The main table lists indicator statuses with their descriptions, protection settings, and indicator counts.

| STATUS                               | DESCRIPTION                                              | PROTECT FROM FEED OVERRIDE          | TOTAL INDICATORS |
|--------------------------------------|----------------------------------------------------------|-------------------------------------|------------------|
| <input type="checkbox"/> Active      | Poses a threat and is being exported to detection tools. | <input checked="" type="checkbox"/> | 0                |
| <input type="checkbox"/> Expired     | No longer poses a serious threat.                        | <input type="checkbox"/>            | 0                |
| <input type="checkbox"/> Indirect    | Associated to an active indicator or event (i.e. pDNS).  | <input type="checkbox"/>            | 0                |
| <input type="checkbox"/> Review      | Requires further analysis.                               | <input type="checkbox"/>            | 0                |
| <input type="checkbox"/> Whitelisted | Poses NO risk and should never be deployed.              | <input checked="" type="checkbox"/> | 0                |

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

The Event Types tab opens.

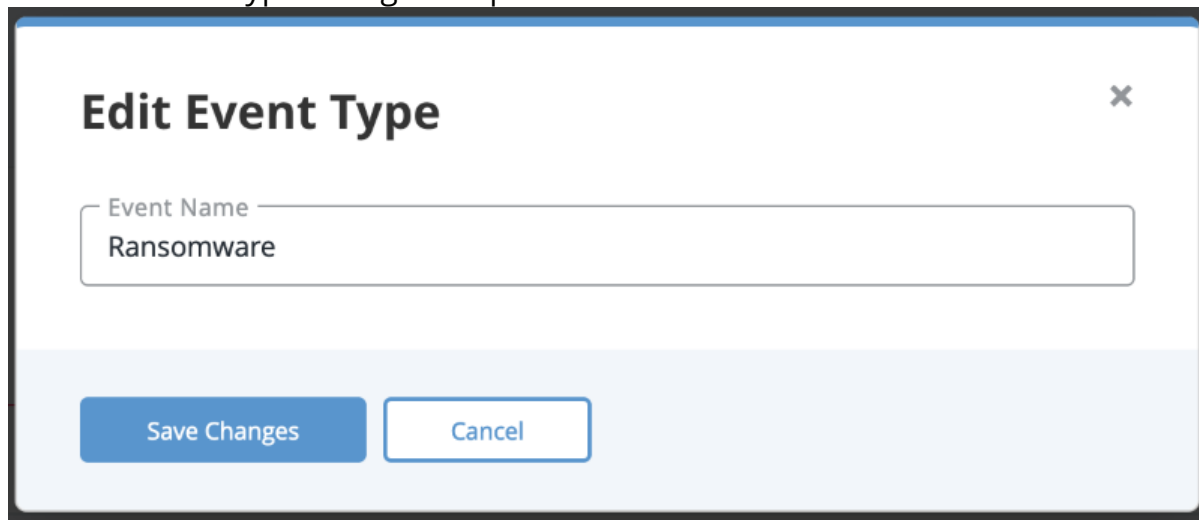


The screenshot shows the ThreatQ System Configurations page with the 'Event Types' tab selected. The page header is the same as the previous screenshot. The 'System Configurations' section now shows the 'Event Types' tab. A green 'Add New Event Type' button is visible. The main table lists event types with their descriptions, total event counts, and total indicator counts.

| EVENT TYPES                                          | TOTAL EVENTS | TOTAL INDICATORS |
|------------------------------------------------------|--------------|------------------|
| <input type="checkbox"/> Anonymization               | 0            | 0                |
| <input type="checkbox"/> Command and Control         | 0            | 0                |
| <input type="checkbox"/> Compromised PKI Certificate | 0            | 0                |
| <input type="checkbox"/> DoS Attack                  | 0            | 0                |
| <input type="checkbox"/> Exfiltration                | 0            | 0                |
| <input type="checkbox"/> Host Characteristics        | 0            | 0                |
| <input type="checkbox"/> Incident                    | 0            | 0                |
| <input type="checkbox"/> Login Compromise            | 0            | 0                |
| <input type="checkbox"/> Malware                     | 0            | 0                |
| <input type="checkbox"/> Sighting                    | 0            | 0                |
| <input type="checkbox"/> Spearphish                  | 0            | 0                |
| <input type="checkbox"/> SQL Injection Attack        | 0            | 0                |
| <input type="checkbox"/> Watchlist                   | 0            | 0                |
| <input type="checkbox"/> 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.

The image shows a dialog box titled "Edit Event Type" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Event Name" containing the word "Ransomware". At the bottom of the dialog, there are two buttons: "Save Changes" (a solid blue button) and "Cancel" (a white button with a blue border).

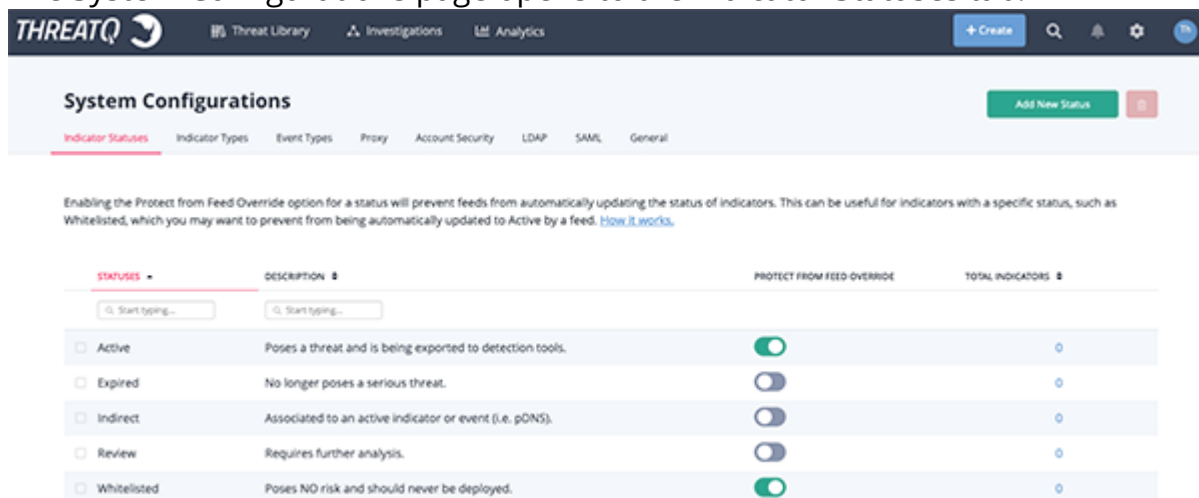
4. Enter a new **Event Name**.
5. Click **Save Changes**.

## 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  > System Configurations.

The System Configurations page opens to the Indicator Statuses tab.

The image shows the "System Configurations" page in the ThreatQ interface. The top navigation bar includes "ThreatQ", "Threat Library", "Investigations", and "Analytics", along with a "+ Create" button and search, notification, and user icons. The "System Configurations" section has tabs for "Indicator Statuses" (selected), "Indicator Types", "Event Types", "Proxy", "Account Security", "LDAP", "SAML", and "General". A green "Add New Status" button is in the top right. Below the tabs, a note explains the "Protect from Feed Override" option. A table lists five indicator statuses: Active, Expired, Indirect, Review, and Whitelisted. Each row includes a checkbox, a description, a "Protect from Feed Override" toggle, and a "Total Indicators" count (all are 0).

| STATUS                               | DESCRIPTION                                              | PROTECT FROM FEED OVERRIDE          | TOTAL INDICATORS |
|--------------------------------------|----------------------------------------------------------|-------------------------------------|------------------|
| <input type="checkbox"/> Active      | Poses a threat and is being exported to detection tools. | <input checked="" type="checkbox"/> | 0                |
| <input type="checkbox"/> Expired     | No longer poses a serious threat.                        | <input type="checkbox"/>            | 0                |
| <input type="checkbox"/> Indirect    | Associated to an active indicator or event (i.e. pONS).  | <input type="checkbox"/>            | 0                |
| <input type="checkbox"/> Review      | Requires further analysis.                               | <input type="checkbox"/>            | 0                |
| <input type="checkbox"/> Whitelisted | Poses NO risk and should never be deployed.              | <input checked="" type="checkbox"/> | 0                |

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

The Event Types tab opens.

System Configurations

Indicator Statuses Indicator Types **Event Types** Proxy Account Security LDAP SAML General

Showing 1 to 14 of 14 Row count: 25

| EVENT TYPES                                          | TOTAL EVENTS | TOTAL INDICATORS |
|------------------------------------------------------|--------------|------------------|
| <input type="checkbox"/> Anonymization               | 0            | 0                |
| <input type="checkbox"/> Command and Control         | 0            | 0                |
| <input type="checkbox"/> Compromised PKI Certificate | 0            | 0                |
| <input type="checkbox"/> DoS Attack                  | 0            | 0                |
| <input type="checkbox"/> Exfiltration                | 0            | 0                |
| <input type="checkbox"/> Host Characteristics        | 0            | 0                |
| <input type="checkbox"/> Incident                    | 0            | 0                |
| <input type="checkbox"/> Login Compromise            | 0            | 0                |
| <input type="checkbox"/> Malware                     | 0            | 0                |
| <input type="checkbox"/> Sighting                    | 0            | 0                |
| <input type="checkbox"/> Spearphish                  | 0            | 0                |
| <input type="checkbox"/> SQL Injection Attack        | 0            | 0                |
| <input type="checkbox"/> Watchlist                   | 0            | 0                |
| <input type="checkbox"/> Watering Hole               | 0            | 0                |

- Determine the event type you want to delete and select the corresponding checkbox in the first column.
- 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

Delete types Cancel

- Click **Delete Types**.

# 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](#)

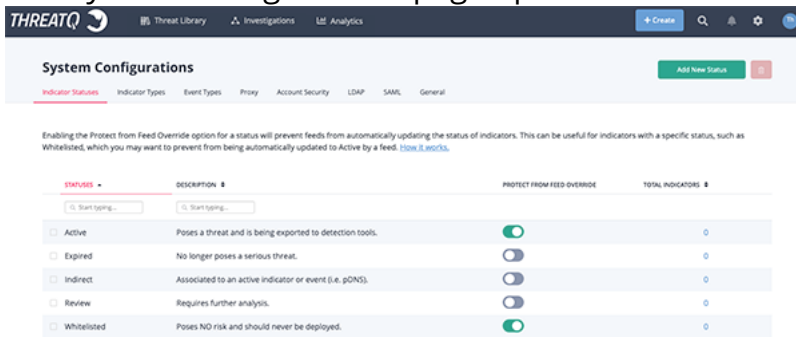


It is highly recommended that you review the Required Information for Creating LDAP Authentication section of the [LDAP Authentication](#) topic before configuring your LDAP settings.

## To Access the LDAP tab:

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

The System Configurations page opens to the Indicator Statuses tab.



System Configurations

Indicator Statuses | Indicator Types | Event Types | Proxy | Account Security | LDAP | SAML | General

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. [Look it up.](#)

| STATUS                                     | DESCRIPTION                                              | PROTECT FROM FEED OVERRIDE          | TOTAL INDICATORS |
|--------------------------------------------|----------------------------------------------------------|-------------------------------------|------------------|
| <input type="checkbox"/> Start typing...   | <input type="checkbox"/> Start typing...                 |                                     |                  |
| <input checked="" type="checkbox"/> Active | Poses a threat and is being exported to detection tools. | <input checked="" type="checkbox"/> | 0                |
| <input type="checkbox"/> Expired           | No longer poses a serious threat.                        | <input type="checkbox"/>            | 0                |
| <input type="checkbox"/> Indirect          | Associated to an active indicator or event (i.e. pDNS).  | <input type="checkbox"/>            | 0                |
| <input type="checkbox"/> Review            | Requires further analysis.                               | <input type="checkbox"/>            | 0                |
| <input type="checkbox"/> Whitelisted       | Poses NO risk and should never be deployed.              | <input checked="" type="checkbox"/> | 0                |

2. Click the **LDAP** tab.

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

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

# 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  > System Configurations.
2. Click on the **LDAP** option.

The Legacy LDAP Settings form will load by default.

3. Complete the following server settings:

| FIELD          | DESCRIPTION                                                                                   |
|----------------|-----------------------------------------------------------------------------------------------|
| Server Address | Enter the name of the server where LDAP is hosted.<br><br><b>Example:</b> ldap://[servername] |



| FIELD                     | DESCRIPTION                                                                                                                                                        |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Port #                    | 389 for LDAP<br><br>636 for LDAPS<br><br>If LDAPS is used, the Port # will default to 636.                                                                         |
| LDAP Domain               | Enter the domain for which LDAP is configured to authenticate.<br><br><b>Example:</b> threatq.com                                                                  |
| Append Domain to Username | Choose from the following options: <ul style="list-style-type: none"><li>◦ Yes for most Active Directory servers</li><li>◦ No for most Open LDAP servers</li></ul> |
| Filter Field Name         | This field is specific to your LDAP directory configuration.<br><br><b>AD Example:</b> memberuid<br><br><b>OpenLDAP Example:</b> uid                               |
| Group Field Name          | This field is specific to your LDAP directory configuration.<br><br><b>AD Example:</b> memberof<br><br><b>OpenLDAP Example:</b> cn                                 |

| FIELD                    | DESCRIPTION                                                                                                                                                                |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Use RDN?                 | Choose from the following options: <ul style="list-style-type: none"><li>◦ Yes to use Relative Distinguished Names.</li><li>◦ No to use full Distinguished Names</li></ul> |
| 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.<br><b>AD Example:</b> memberUid<br><b>OpenLDAP Example:</b> uid                                               |

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



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

| FIELD                 | EXAMPLE                                                                                                           |
|-----------------------|-------------------------------------------------------------------------------------------------------------------|
| Maintenance Account   | <b>OpenLDAP Example:</b> ldapSuper<br><br><b>AD Example:</b><br>CN=tq.maintenance,CN=Builtin,DC=yourdomain,DC=com |
| Administrative Access | <b>OpenLDAP Example:</b> administrator                                                                            |

| FIELD                      | EXAMPLE                                                                                                                  |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------|
|                            | <b>AD Example:</b><br>CN=linux_admins,CN=Builtin,DC=yourdomain,DC=com                                                    |
| Read Only Access           | <b>OpenLDAP Example:</b> ldapObserver<br><br><b>AD Example:</b><br>CN=read_onlyCN=Builtin,DC=yourdomain,DC=com           |
| Primary Contributor Access | <b>OpenLDAP Example:</b> ldapAnalyst<br><br><b>AD Example:</b><br>CN=primary_contributor,CN=Builtin,DC=yourdomain,DC=com |

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



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

## Configuring Secure LDAP

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

The Updated LDAP Settings form will load.

THREATQ

Threat LibraryInvestigationsAnalytics

Create

System Configurations

Indicator StatusesIndicator TypesEvent TypesProxyAccount SecurityLDAPSAMLGeneral

LDAP

DisabledEnabled

Lighweight Directory Access Protocol (LDAP) is a lightweight client-server protocol for accessing directory services and is used for authentication and storing information. Complete the fields below to set the primary server settings and map your permission levels to LDAP.

Legacy LDAP SettingsUpdated LDAP Settings

Server Connection Settings

Account Suffix

@threatq.com

LDAP account suffix

Host Address

tqad.threatq.com

Name of the LDAP domain controller, without the protocol. E.g. "ldap.your\_organization.com"

Port Number

389

LDAP port number

Admin Username

tqadmin

LDAP Administrative Username, e.g. For OpenLDAP: "uid=admin email, ou=People, dc=server, dc=com"

Admin Password

\*\*\*\*\*

LDAP Administrative Password

Test Connection

LDAP Schema

Base DN

DC=threatq,DC=com

Base DN of the LDAP server connection. E.g. "DC=server, DC=com"

DN Field Name

dn

Field used to retrieve the DN or users and groups, should be 'dn' for both OpenLDAP and Active Directories.

User Search Filter

user

Used to search for users. For OpenLDAP: objectClass=posixAccount, for Active Directory: objectClass=user

Group Search Filter

group

Used to search for all groups. For OpenLDAP: objectClass=posixGroup, for Active Directory: objectClass=group

Primary Group Name

tqusers

Primary group name, e.g. 'memberUid' or 'your\_organizationusers'

Group Member Field Name

memberof

Used to search for groups that a user belongs to. For OpenLDAP: 'dn', for Active Directory: 'memberof'

User Id Key Field Name

sAMAccountName

User field used to search for users based on email. For OpenLDAP: uid, for Active Directory: sAMAccountName

User Group Member Key Field Name

uid

Used to search for groups that a user belongs to. For OpenLDAP: memberUid, for Active Directory: uid

Save

Protocols

Use SSL

NoYes

Map Your Permission Levels to LDAP

(Note: You can not list the same LDAP User Group for Multiple permission levels)

Maintenance Account

administrator

This should be the CN value of your LDAP Query.

Administrative Access

ldapSuper

Primary Contributor Access

ldapAnalyst

Read Only Access

ldapObserver

Connect To Retrieve Data

List Groups

Connect

List Users

Connect

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

ThreatQ User Guide Version 4.47.0

290

| FIELD          | DESCRIPTION                                                                                                                                                                                |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Account Suffix | The LDAP account suffix.                                                                                                                                                                   |
| Host Address   | Name of the LDAP domain controller without the protocol.<br><b>Example:</b> tqldap.threatq.com                                                                                             |
| Port Number    | The LDAP port; either <b>636</b> or <b>389</b> .<br><br>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.                                                                                                                                                          |

- Click on **Test Connections** to verify the settings are correct.
- Complete the **LDAP Schema** section:

| FIELD   | DESCRIPTION                                                                             |
|---------|-----------------------------------------------------------------------------------------|
| Base DN | The Base DN of the LDAP server connection.<br><br><b>Example:</b> DC=[server], DC="com" |

| FIELD                   | DESCRIPTION                                                                                                                                        |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| DN Field Name           | <p>The field used to retrieve the DN or users and groups.</p> <p>This field should be <b>DN</b> for both OpenLDAP and Active Directory.</p>        |
| User Search Filter      | <p>The field to search for users.</p> <p>For <b>OpenLDAP</b>: objectClass=posixAccount</p> <p>For <b>Active Directory</b>: objectClass=user</p>    |
| Group Search Filter     | <p>The field to search for grpups.</p> <p>For <b>OpenLDAP</b>: objectClass=posixGroup</p> <p>For <b>Active Directory</b>: objectClass=group</p>    |
| Primary Group Name      | <p>The primary group name.</p>                                                                                                                     |
| Group Member Field Name | <p>This field is used to search for groups that a user belongs to.</p> <p>For <b>OpenLDAP</b>: cn</p> <p>For <b>Active Directory</b>: memberof</p> |



| FIELD                            | DESCRIPTION                                                                                                                           |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| User ID Key Field Name           | Field used to search for users based on email.<br><br>For <b>OpenLDAP</b> : uid<br><br>For <b>Active Directory</b> : sAMAccountName   |
| User Group Member Key Field Name | Field used to search for groups that user belongs to.<br><br>For <b>OpenLDAP</b> : memberUid<br><br>For <b>Active Directory</b> : 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.<br><br><b>Open LDAP Example:</b> ldapSuper<br><br><b>AD Example:</b><br>CN=tq.maintenance,CN=Builtin,DC=yourdomain,DC=com |

| FIELD                      | DESCRIPTION                                                                                                                                                                                                           |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Administrative Access      | <p>The LDAP account the ThreatQ Administrative group will map to for permissions.</p> <p><b>Open LDAP Example:</b> administrator</p> <p><b>AD Example:</b><br/>CN=linux.admins,CN=Builtin,DC=yourdomain,DC=com</p>    |
| Primary Contributor Access | <p>The LDAP account the ThreatQ Primary Contributor group will map to for permissions.</p> <p><b>Open LDAP Example:</b> ldapAnalyst</p> <p><b>AD Example:</b><br/>CN=linux.admins,CN=Builtin,DC=yourdomain,DC=com</p> |
| Read-Only Access           | <p>The LDAP account the ThreatQ Read-Only group will map to for permissions.</p> <p><b>Open LDAP Example:</b> ldapObserver</p> <p><b>AD Example:</b><br/>CN=read.onlyCN=Builtin,DC=yourdomain,DC=com</p>              |

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



Green indicates the feature is active.

## SAML Authentication

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

Email addresses and passwords are authenticated outside of ThreatQ and user roles are determined 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.

The screenshot shows a 'observer Properties' dialog box. It has a title bar with a question mark and a close button. Below the title bar is a tabbed interface with tabs for 'Member Of', 'Dial-in', 'Environment', 'Sessions', 'Remote control', 'Remote Desktop Services Profile', and 'COM+'. The 'General' tab is selected. Under the 'General' tab, there is a user icon and the name 'observer'. Below this are several text input fields: 'First name' (containing 'observer'), 'Initials' (empty), 'Last name' (empty), 'Display name' (containing 'observer'), 'Description' (empty), 'Office' (empty), 'Telephone number' (empty), 'Email' (containing 'observer@threatq.com'), and 'Web page' (empty). There are 'Other...' buttons next to the 'Telephone number' and 'Web page' fields. At the bottom of the dialog are four buttons: 'OK', 'Cancel', 'Apply', and 'Help'. The 'OK' button is highlighted with a blue border.

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

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

The System Configurations page opens.

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

The SAML configuration page opens.

**System Configurations**

Indicator Statuses Indicator Types Event Types Proxy LDAP **SAML** General

**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. When you provide one method, the other method will autopopulate.

**Provide IDP Metadata File**

FederationMetadata.xml [download](#)

**Provide IDP Metadata URL**

IDP URL

**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  
  
Copy and paste this to your IDP platform

**Service Provider Metadata File**

threatq-sp.xml [download](#)

**Service Provider Server Certificate Information**

☐ Use server key and certificate

**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

[Save](#)

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



Drag your files here or [click to browse](#)

#### 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

Copy and paste this to your IDP platform

#### Service Provider Metadata File

 threatq-sp.xml [download](#)

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

#### Primary Contributor Access

#### Read Only Access

### Mapping Notes:

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

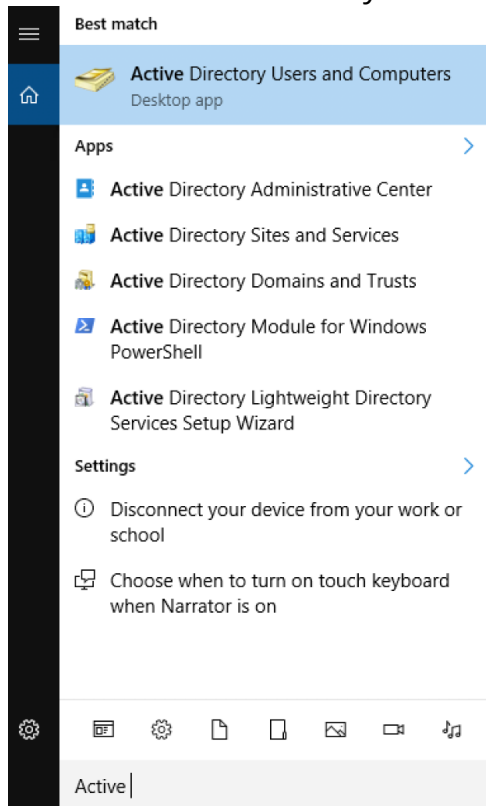
- You do not have to map all ThreatQ roles but at least one role has to be mapped to use SAML. **Example:** Administrator and Primary Contributor will be mapped but the Read Only Access role will be blank.
7. Click on **Save** located at the bottom of the page.
  8. Confirm that your network administrator has completed [Adding ThreatQ as a Service Provider](#) before proceeding with the final steps listed below.
  9. Click on **Test Authentication** to confirm that the ThreatQ platform and your IdP can connect.
  10. Click on the **Enable** toggle switch located at the top-right of the page to enable SAML.



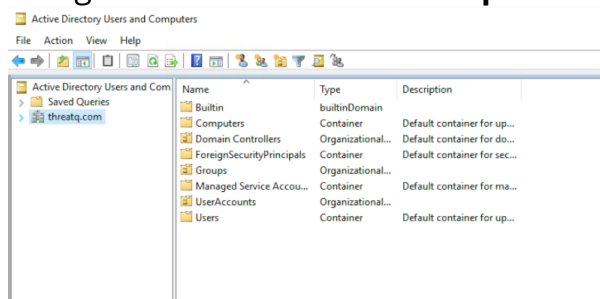
## Setting Up LDAP Users/Groups for SAML

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

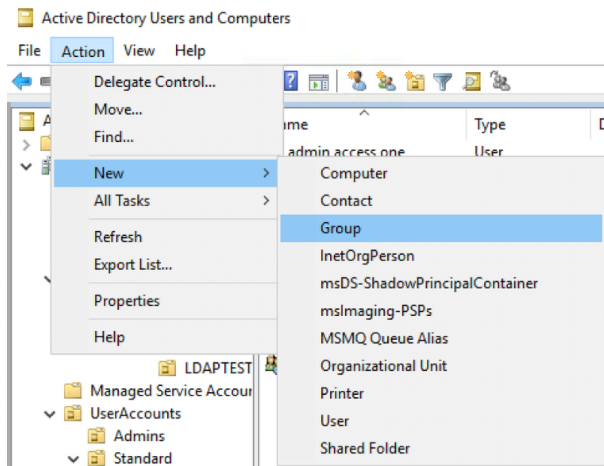
1. Log into the Windows Server.
2. Start the Active Directory Users and Computers application from the Start Menu.



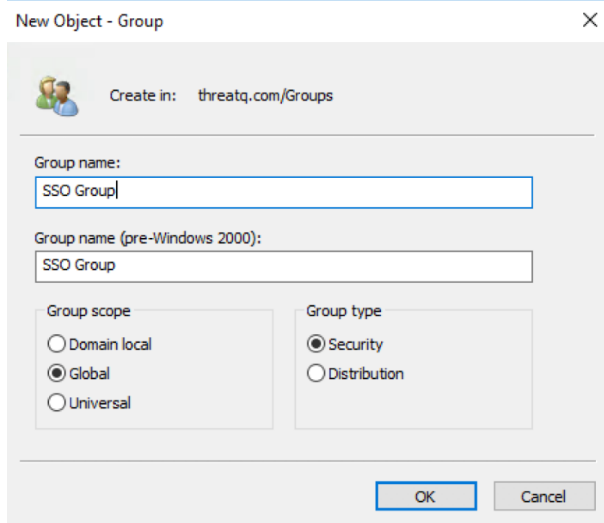
3. Navigate to and select the **Groups** folder under your LDAP domain.



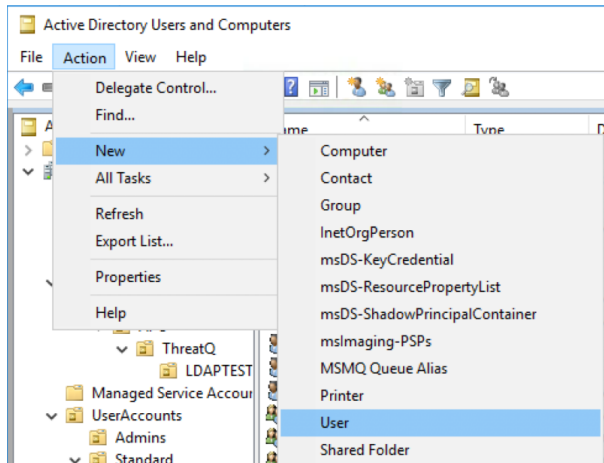
#### 4. Click on **Actions > New > Group**.



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



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



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

The screenshot shows the 'New Object - User' dialog box with the title bar 'New Object - User' and a close button. The 'Create in:' field shows 'threatq.com/Users'. The 'First name:' field contains 'Pat', 'Initials:' is empty, 'Last name:' contains 'User', and 'Full name:' contains 'Pat User'. The 'User login name:' field contains 'pat' and the domain dropdown is '@threatq.com'. The 'User login name (pre-Windows 2000):' field contains 'THREATQ0\pat'. At the bottom are '< Back', 'Next >', and 'Cancel' buttons. The 'Next >' button is highlighted with a blue border.

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

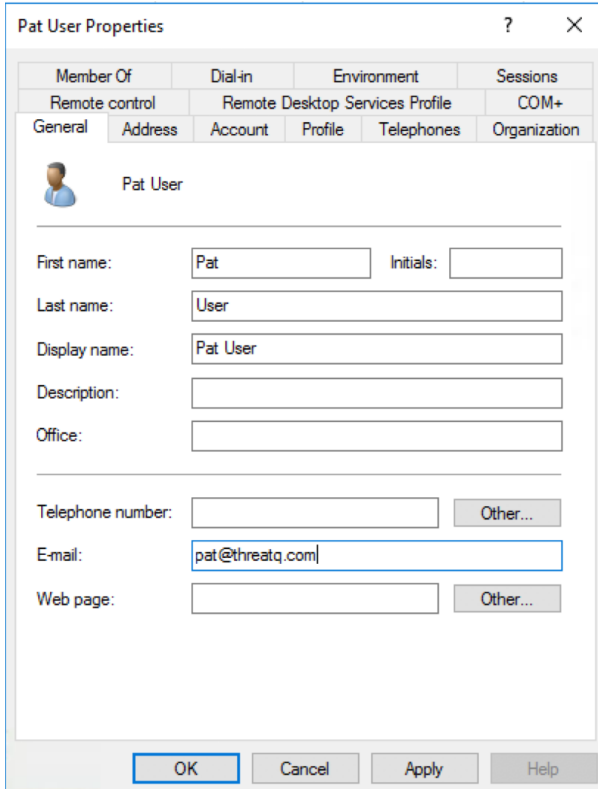
The screenshot shows the 'New Object - User' dialog box with the title bar 'New Object - User' and a close button. The 'Create in:' field shows 'threatq.com/Users'. The 'Password:' and 'Confirm password:' fields are filled with dots. Below these are four checkboxes: 'User must change password at next logon' (checked), 'User cannot change password' (unchecked), 'Password never expires' (unchecked), and 'Account is disabled' (unchecked). At the bottom are '< Back', 'Next >', and 'Cancel' buttons. The 'Next >' button is highlighted with a blue border.

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

The screenshot shows the 'New Object - User' dialog box with the title bar 'New Object - User' and a close button. The 'Create in:' field shows 'threatq.com/Users'. A text box contains the summary: 'When you click Finish, the following object will be created: Full name: Pat User, User login name: pat@threatq.com, The password never expires.' At the bottom are '< Back', 'Finish', and 'Cancel' buttons. The 'Finish' button is highlighted with a blue border.

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.



Pat User Properties

| Member Of      | Dial-in                         | Environment | Sessions |
|----------------|---------------------------------|-------------|----------|
| Remote control | Remote Desktop Services Profile | COM+        |          |

General Address Account Profile Telephones Organization

Pat User

First name: Pat Initials:

Last name: User

Display name: Pat User

Description:

Office:

Telephone number: Other...

E-mail: pat@threatq.com

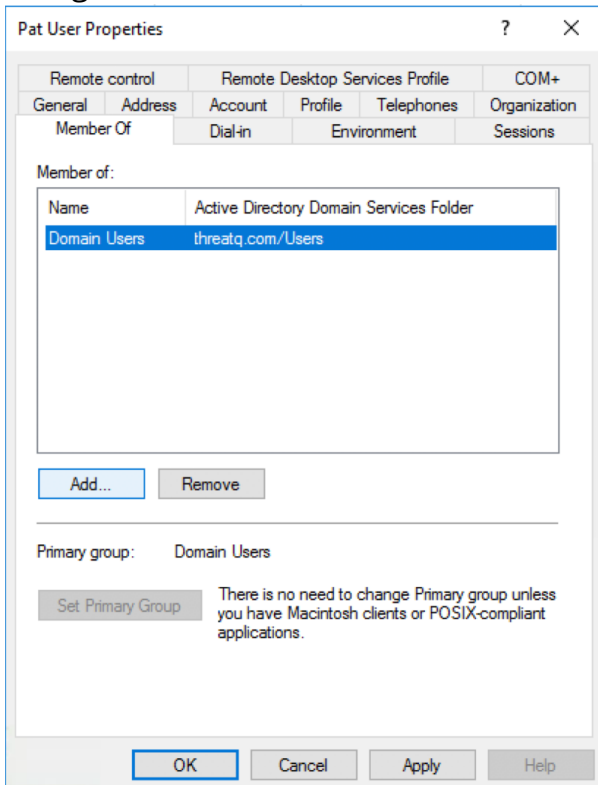
Web page: Other...

OK Cancel Apply Help



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**.



Pat User Properties

| Remote control | Remote Desktop Services Profile | COM+    |
|----------------|---------------------------------|---------|
| General        | Address                         | Account |

Member Of Dial-in Environment Sessions

Member of:

| Name         | Active Directory Domain Services Folder |
|--------------|-----------------------------------------|
| Domain Users | threatq.com/Users                       |

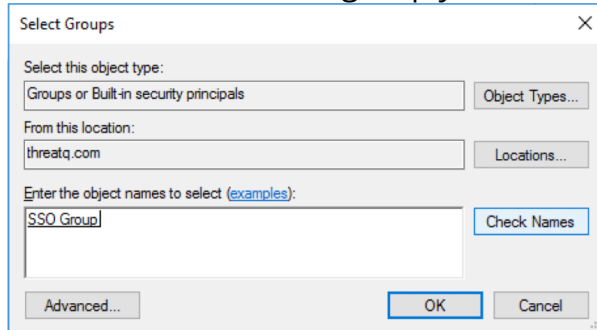
Add... Remove

Primary group: Domain Users

Set Primary Group There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

OK Cancel Apply Help

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



Select Groups

Select this object type:  
Groups or Built-in security principals

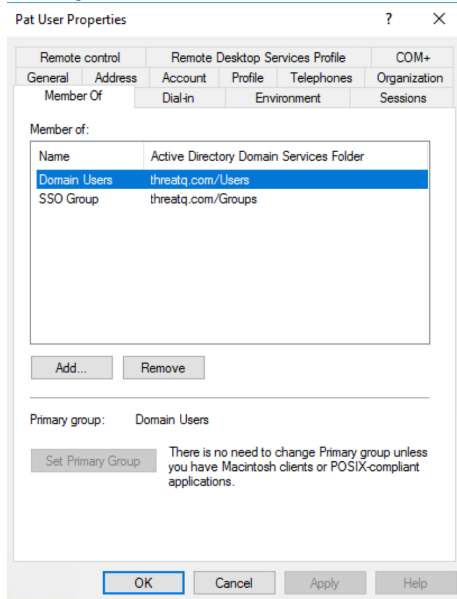
From this location:  
threatq.com

Enter the object names to select (examples):  
SSO Group

Check Names

Advanced... OK Cancel

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.



Pat User Properties

Remote control Remote Desktop Services Profile COM+  
General Address Account Profile Telephones Organization  
Member Of Dial-in Environment Sessions

Member of:

| Name         | Active Directory Domain Services Folder |
|--------------|-----------------------------------------|
| Domain Users | threatq.com/Users                       |
| SSO Group    | threatq.com/Groups                      |

Add... Remove

Primary group: Domain Users

Set Primary Group

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

OK Cancel Apply Help

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.

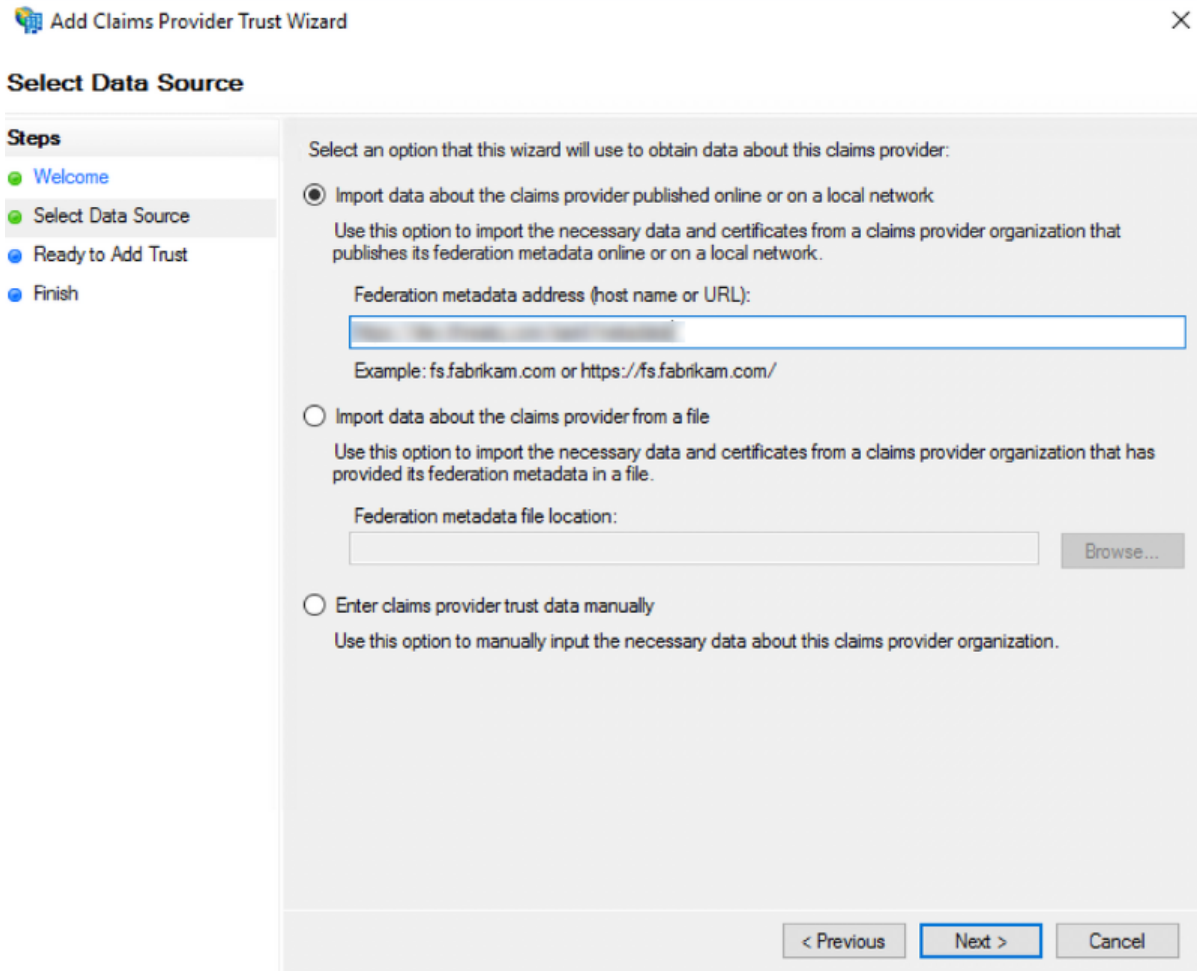
### ADFS 2016

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.



The screenshot shows the 'Add Claims Provider Trust Wizard' dialog box. The title bar says 'Add Claims Provider Trust Wizard' with a close button. The main heading is 'Select Data Source'. On the left, there is a 'Steps' pane with four items: 'Welcome' (green dot), 'Select Data Source' (green dot and highlighted), 'Ready to Add Trust' (blue dot), and 'Finish' (blue dot). The main area contains three radio button options:

- ☒ **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):  
  
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.

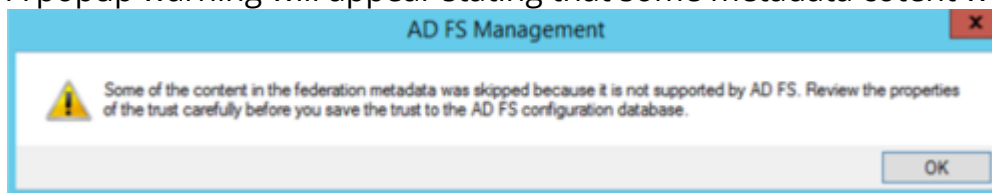
At the bottom right are three buttons: '< Previous' (disabled), 'Next >' (highlighted), and 'Cancel' (disabled).

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

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

8. Click **Next**.

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



9. Click **Ok** to proceed.

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

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

Contact your Network Administrator to receive the appropriate group mapping.

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

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

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

| LDAP ATTRIBUTE   | OUTGOING CLAIM TYPE |
|------------------|---------------------|
| E-Mail-Addresses | email               |
| SAM-Account-Name | uid                 |

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

| LDAP ATTRIBUTE   | OUTGOING CLAIM TYPE |
|------------------|---------------------|
| E-Mail-Addresses | E-Mail Address      |

24. Click on **OK** to create the rule.
25. Click on **Add Rule**.



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

| LDAP ATTRIBUTE                   | OUTGOING CLAIM TYPE |
|----------------------------------|---------------------|
| Token-Groups - Unqualified Names | SSO                 |

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

| FIELD                   | SELECTION      |
|-------------------------|----------------|
| Incoming Claim Type     | E-Mail Address |
| Outgoing Claim Type     | Name ID        |
| Outgoing Name ID Format | Email          |

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

## Azure AD

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

### Setting Up the SAML App

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

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

1

Basic SAML Configuration

Identifier (Entity ID)

https://192.168.1.100/api/saml/metadata

Reply URL (Assertion Consumer Service URL)

https://192.168.1.100/api/saml/acs

Sign on URL

Optional

Relay State

Optional

Logout Uri

Optional

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

| FIELD                          | VALUE                                                 | DESCRIPTION                                                                                             |
|--------------------------------|-------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| ACS /<br>Single Sign<br>on URL | https://<br>threatq.example.com/api/<br>saml/acs      | Assertion Consumer Service (ACS) is the ThreatQ URL + appended the "/api/saml/acs" string.              |
| SP Entity ID                   | https://<br>threatq.example.com/api/<br>saml/metadata | This is the ThreatQ entity ID which is the ThreatQ URL + appended with the "/api/saml/metadata" string. |

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

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



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

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

included in the SAML assertion upon login.

Home > ThreatQ > Enterprise applications | All applications > ThreatQ | Single sign-on > SAML-based Sign-on > User Attributes & Claims

### User Attributes & Claims

+ Add new claim + Add a group claim Columns

**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)

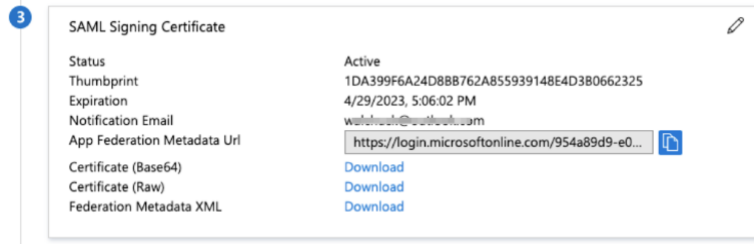
Groups

Namespace (optional)

☐ Emit groups as role claims ⓘ

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

topic.

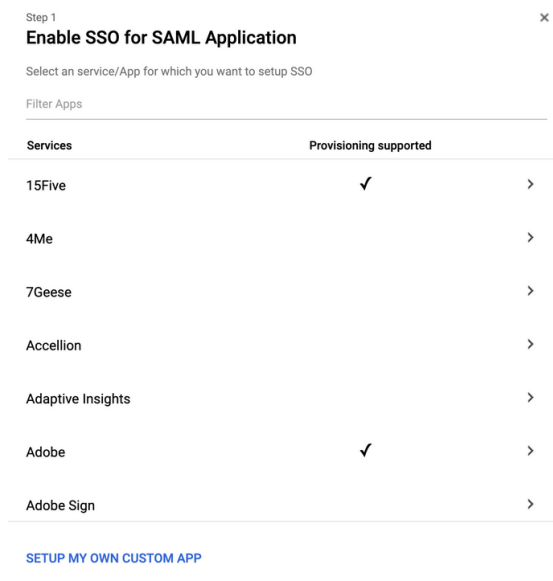


## Google G Suite

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

### Setting Up the SAML App

1. Log into your **Google Administrative Console**.
2. Navigate to **Apps > SAML Apps**.
3. Click on the **+** icon located at the bottom-right on the page.
4. Select the **Setup my own custom app** option.



## The Google IdP information page loads.

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

[Download](#)

OR

**Option 2**

IDP metadata Download

[Previous](#) [Cancel](#) [Next](#)

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 Choose File

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.

[Previous](#) [Cancel](#) [Next](#)

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 <b>Email</b> .                                                      | 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

PREVIOUS

CANCEL [NEXT](#)

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

[ADD NEW MAPPING](#)

[PREVIOUS](#)[CANCEL](#) [FINISH](#)

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

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

11. Create the **email** mapping:

| ATTRIBUTE | TYPE              | GOOGLE DATA FIELD |
|-----------|-------------------|-------------------|
| email     | Basic Information | Primary Email     |

12. Click on **Add New Mapping**.

13. Create the **uid** mapping:

| ATTRIBUTE | TYPE              | GOOGLE DATA FIELD |
|-----------|-------------------|-------------------|
| uid       | Basic Information | Primary Email     |

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

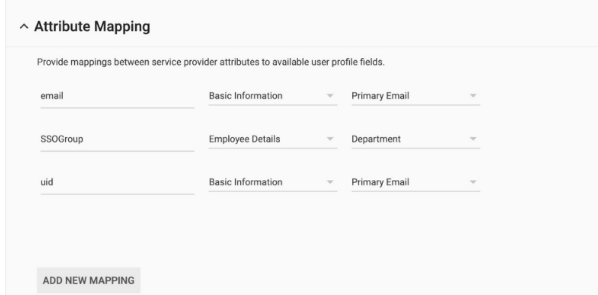
15. Create the **SSOGroup** mapping for ThreatQ roles:

| ATTRIBUTE | TYPE             | GOOGLE DATA FIELD            |
|-----------|------------------|------------------------------|
| SSOGroup  | Employee Details | < specific to your company > |



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

16. Your setup should now resemble the following screenshot:



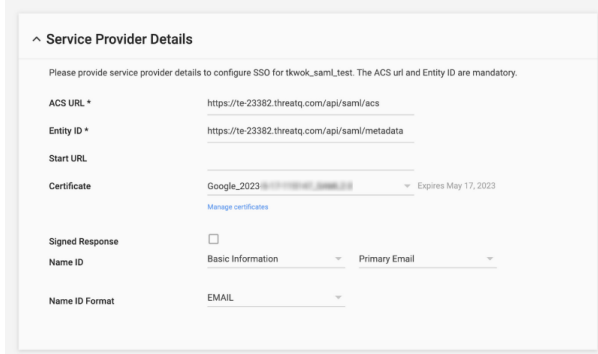
17. Click on **Finish**.

18. Locate your new app under **Apps > SAML Apps**, click on the vertical ellipsis, and select **On for Everyone**.

19. Click on the app to open its settings details.

20. Click on **Service Provider Details**.

The Service Provider Details page opens.



21. Click on **Manage Certificates**.

22. Download the **certificate** and the **IdP Metadata** files that are required in steps 4 and 5 in the *Configuring SAML* 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**.

The Add Applications page loads.

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

The Create New Application dialog box opens.

6. Select **Web** from the Platform dropdown.

7. Select **SAML 2.0** for the Sign on method.

8. Click on the **Create** button.

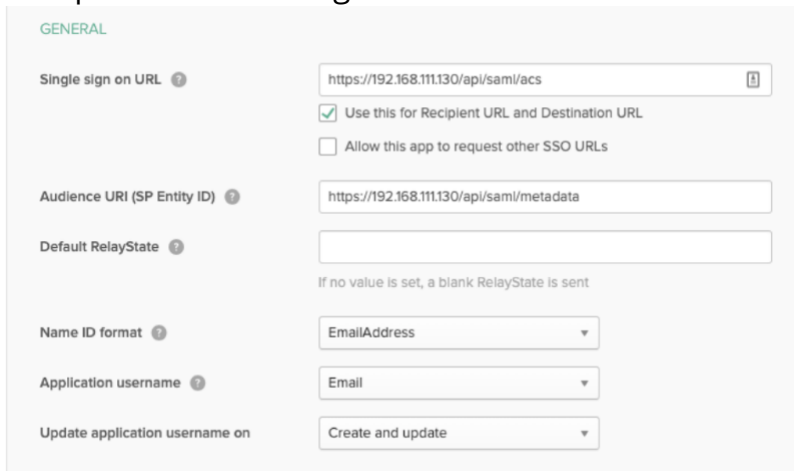
The Create SAML Integration page opens with the General Settings tab selected.

9. Enter a name for the app in the **App Name** field.

10. Click on **Next**.

The Configure SAML section loads.

11. Complete the following fields:



**GENERAL**

Single sign on URL   

☒ Use this for Recipient URL and Destination URL

☐ Allow this app to request other SSO URLs

Audience URI (SP Entity ID) 

Default RelayState 

If no value is set, a blank RelayState is sent

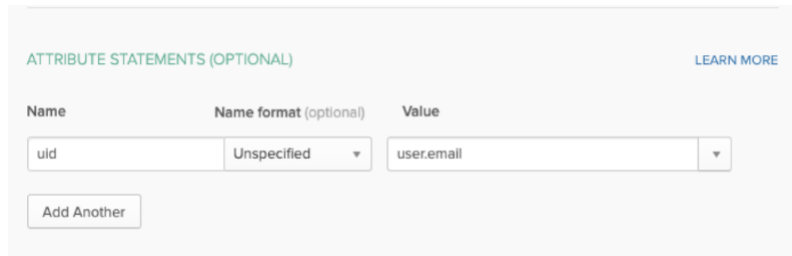
Name ID format 

Application username 

Update application username on

| 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.           |
| Default RelayState          | https://< Host-name >/api/saml/acs      | The Default RelayState is your ThreatQ URL + appended with the “/api/saml/metadata” string.     |
| Name ID format              | EmailAddress                            |                                                                                                 |
| Application username        | Email                                   | ThreatQ requires that this field be set to Email.                                               |

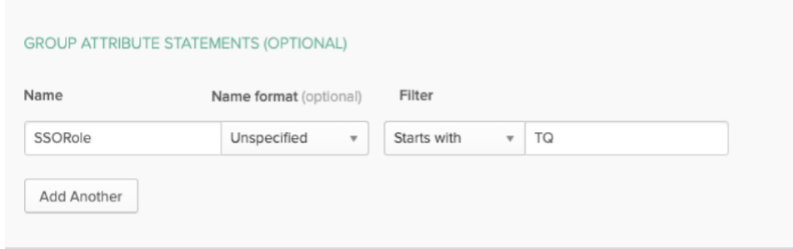
12. Scroll down to the **Attribute Statements** section and add the following attribute:



| NAME | NAME FORMAT | VALUE      |
|------|-------------|------------|
| uid  | Unspecified | user.email |

13. Add the required attributes to the **Group Attribute Statements** that will be used to map Okta groups to ThreatQ user roles. In the example image below, an attribute called

**SSORole** was created and is mapped to all Okta group names that starts with **TQ**.



See Okta's [Custom Expression](#) help article for additional information on assigning an attribute.

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

The Feedback section loads.

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

The Application details page loads.

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



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

25. Click on **Download Certificate**. The certificate and Identity Provider metadata file downloaded in step 23 are required in steps 4 and 5 in the Configuring SAML section of the [SAML Authentication](#) topic.

# 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.

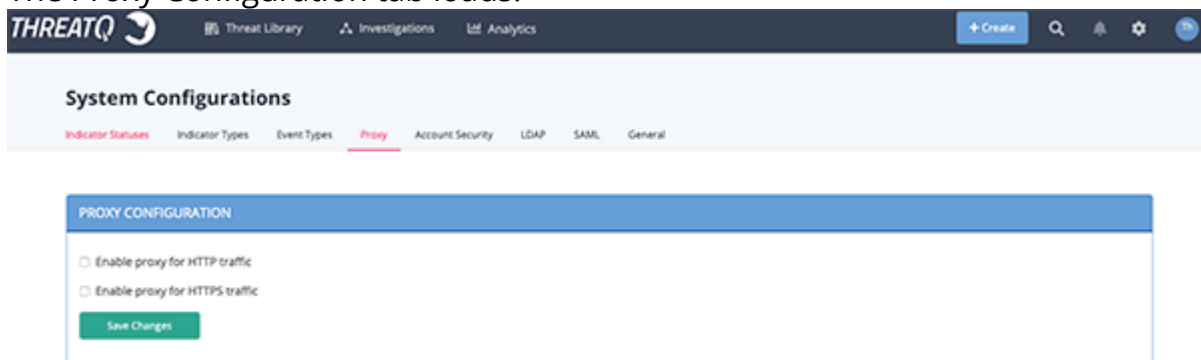
## Accessing Proxy Configuration

1. Navigate to Settings  > System Configurations.

The System Configurations page opens to the Indicator Statuses tab.

2. Click the **Proxy** tab.

The Proxy Configuration tab loads.



### Proxy Table Functions:

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

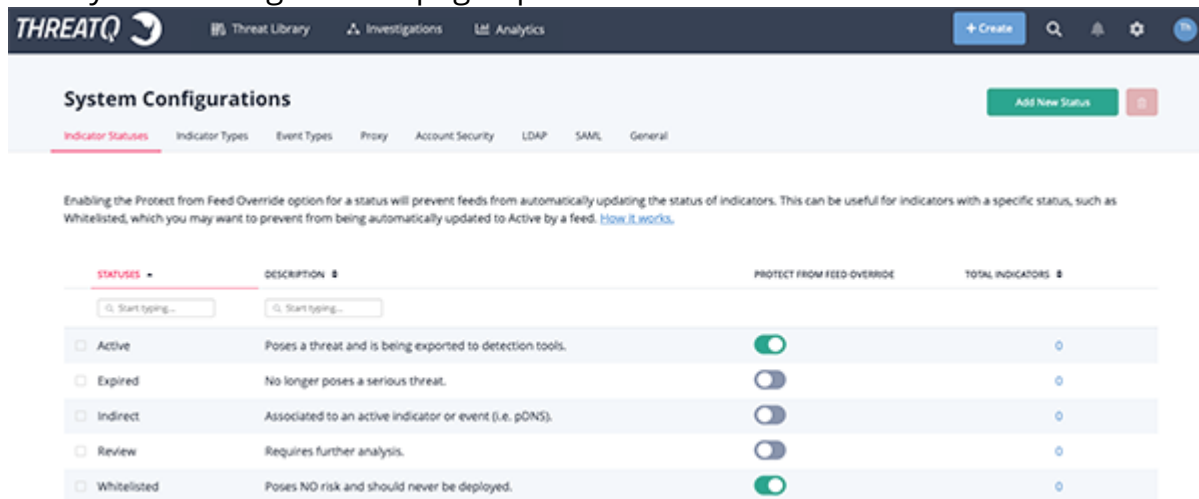
# Account Security

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

## Configuring User Lockout Settings:

1. Navigate to Settings  > System Configurations.

The System Configurations page opens to the Indicator Statuses tab.



**System Configurations**

Indicator Statuses | Indicator Types | Event Types | Proxy | Account Security | LDAP | SAML | General

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 |
|--------------------------------------|----------------------------------------------------------|-------------------------------------|------------------|
| <input type="checkbox"/> Active      | Poses a threat and is being exported to detection tools. | <input checked="" type="checkbox"/> | 0                |
| <input type="checkbox"/> Expired     | No longer poses a serious threat.                        | <input type="checkbox"/>            | 0                |
| <input type="checkbox"/> Indirect    | Associated to an active indicator or event (i.e. pDNS).  | <input type="checkbox"/>            | 0                |
| <input type="checkbox"/> Review      | Requires further analysis.                               | <input type="checkbox"/>            | 0                |
| <input type="checkbox"/> Whitelisted | Poses NO risk and should never be deployed.              | <input checked="" type="checkbox"/> | 0                |

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

The Account Security Configuration tab opens.

## System Configurations

[Indicator Statuses](#)[Indicator Types](#)[Event Types](#)[Proxy](#)[Account Security](#)[LDAP](#)[SAML](#)[General](#)

### 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.

3. The following functions are available:

| 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 will be locked after reaching the set login attempts.         |

# General Settings

You can configure default indicator parsing options and the date and time format of your choice system-wide within the ThreatQ platform from the **General** tab.

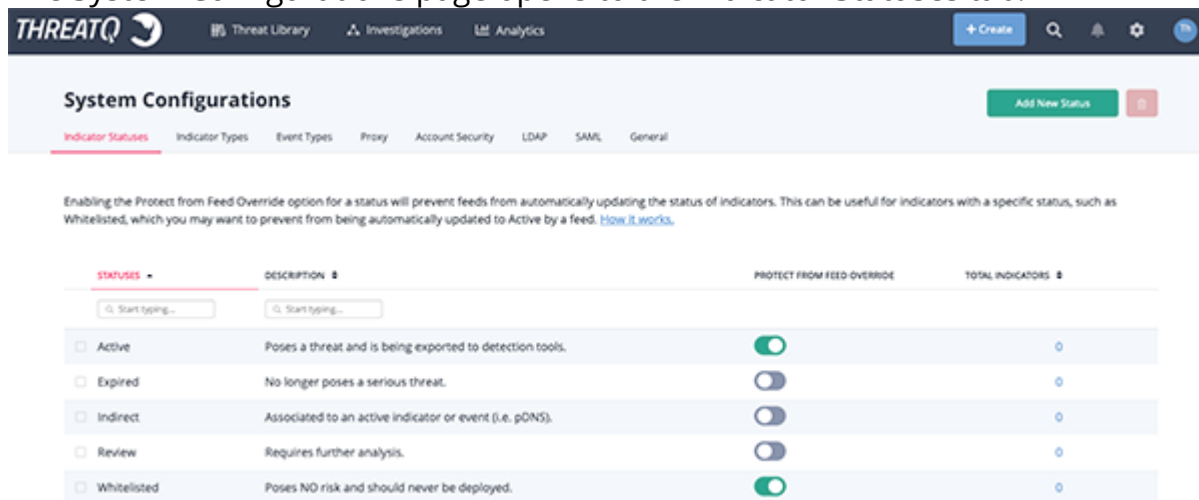


If you make changes to the date and time format while another user is working concurrently in the same ThreatQ installation, that user must refresh their browser for the changes to take effect.

## Configuring Date and Time Format

1. Navigate to Settings  > System Configurations.

The System Configurations page opens to the Indicator Statuses tab.



**System Configurations**

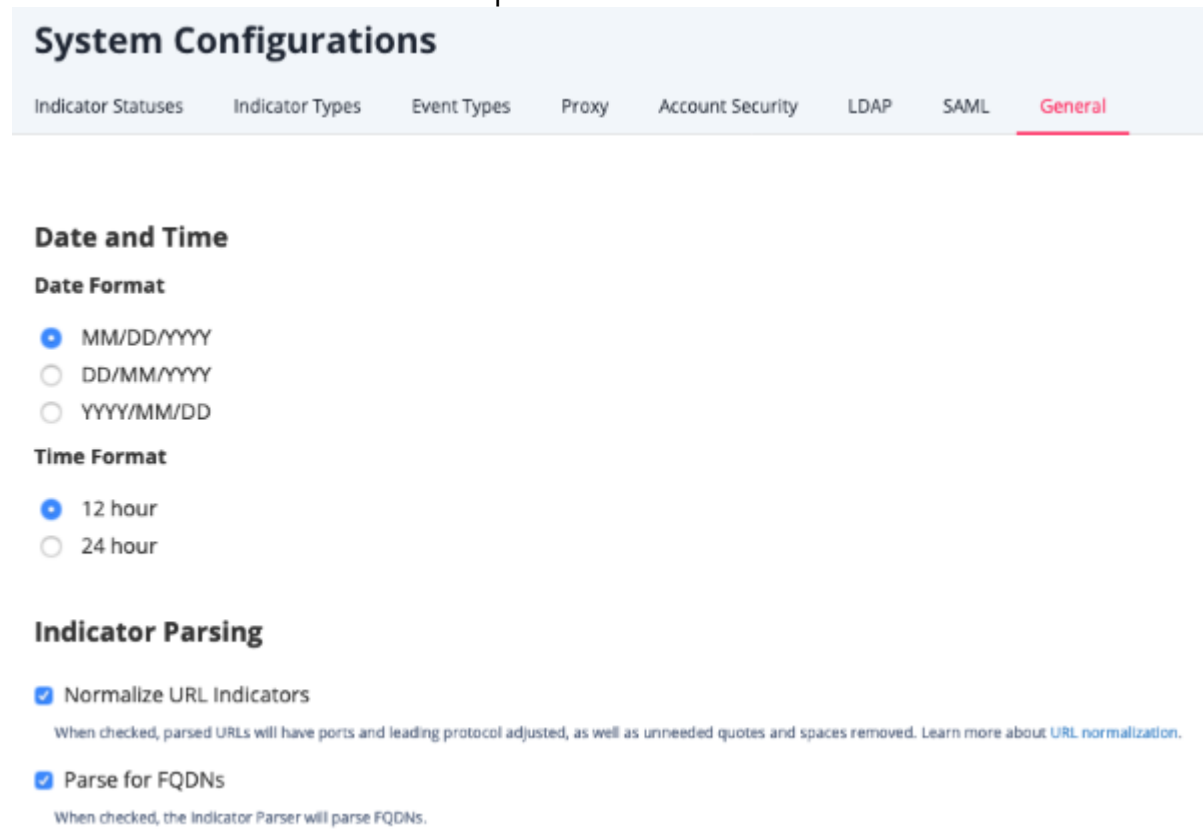
Indicator Statuses | Indicator Types | Event Types | Proxy | Account Security | LDAP | SAML | General

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 |
|--------------------------------------|----------------------------------------------------------|-------------------------------------|------------------|
| <input type="checkbox"/> Active      | Poses a threat and is being exported to detection tools. | <input checked="" type="checkbox"/> | 0                |
| <input type="checkbox"/> Expired     | No longer poses a serious threat.                        | <input type="checkbox"/>            | 0                |
| <input type="checkbox"/> Indirect    | Associated to an active indicator or event (i.e. pONS).  | <input type="checkbox"/>            | 0                |
| <input type="checkbox"/> Review      | Requires further analysis.                               | <input type="checkbox"/>            | 0                |
| <input type="checkbox"/> Whitelisted | Poses NO risk and should never be deployed.              | <input checked="" type="checkbox"/> | 0                |

2. Click the **General** tab.

The Date and Time Format tab opens.



**System Configurations**

Indicator Statuses   Indicator Types   Event Types   Proxy   Account Security   LDAP   SAML   **General**

**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.

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

## 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.



The System Configurations page opens to the Indicator Statuses tab.

The screenshot shows the ThreatQ System Configurations page with the 'Indicator Statuses' tab selected. The page has a dark blue header with the ThreatQ logo and navigation links: Threat Library, Investigations, and Analytics. A '+ Create' button is in the top right. Below the header, the 'System Configurations' title is followed by a tab bar with 'Indicator Statuses' (active), 'Indicator Types', 'Event Types', 'Proxy', 'Account Security', 'LDAP', 'SAML', and 'General'. A green 'Add New Status' button is on the right. A note explains the 'Protect from Feed Override' option. Below is a table of indicator statuses.

| STATUSES                             | DESCRIPTION                                              | PROTECT FROM FEED OVERRIDE          | TOTAL INDICATORS |
|--------------------------------------|----------------------------------------------------------|-------------------------------------|------------------|
| <input type="checkbox"/> Active      | Poses a threat and is being exported to detection tools. | <input checked="" type="checkbox"/> | 0                |
| <input type="checkbox"/> Expired     | No longer poses a serious threat.                        | <input type="checkbox"/>            | 0                |
| <input type="checkbox"/> Indirect    | Associated to an active indicator or event (i.e. pONS).  | <input type="checkbox"/>            | 0                |
| <input type="checkbox"/> Review      | Requires further analysis.                               | <input type="checkbox"/>            | 0                |
| <input type="checkbox"/> Whitelisted | Poses NO risk and should never be deployed.              | <input checked="" type="checkbox"/> | 0                |

2. Click the **General** tab.

The Date and Time Format tab opens.

The screenshot shows the ThreatQ System Configurations page with the 'General' tab selected. The page has a dark blue header with the ThreatQ logo and navigation links: Threat Library, Investigations, and Analytics. A '+ Create' button is in the top right. Below the header, the 'System Configurations' title is followed by a tab bar with 'Indicator Statuses', 'Indicator Types', 'Event Types', 'Proxy', 'Account Security', 'LDAP', 'SAML', and 'General' (active). The 'Date and Time' section has 'Date Format' and 'Time Format' options. The 'Indicator Parsing' section has 'Normalize URL Indicators' and 'Parse for FQDNs' options.

### 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.

3. Locate the Indicator Parsing heading and 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.

### 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 **Save**.

# System Objects

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

System Objects include:

- [Adversaries](#)
- [Events](#)
- [Files](#)
- [Indicators](#)
- [Signatures](#)
- [STIX](#)
- [Tasks](#)

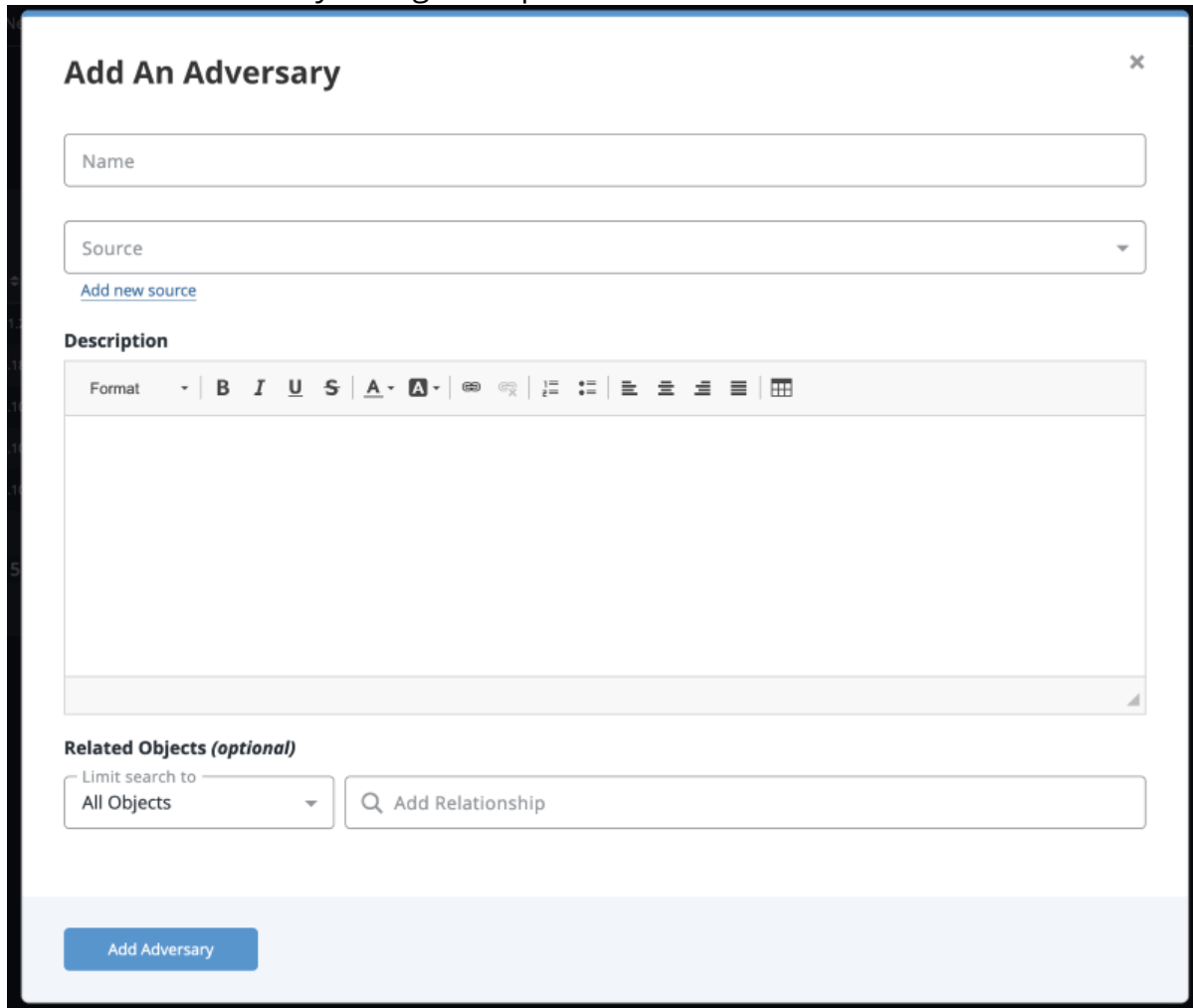
# Adversaries

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

## Adding Adversaries

1. Go to **Create > Adversary**.

The Add an Adversary dialog box opens.

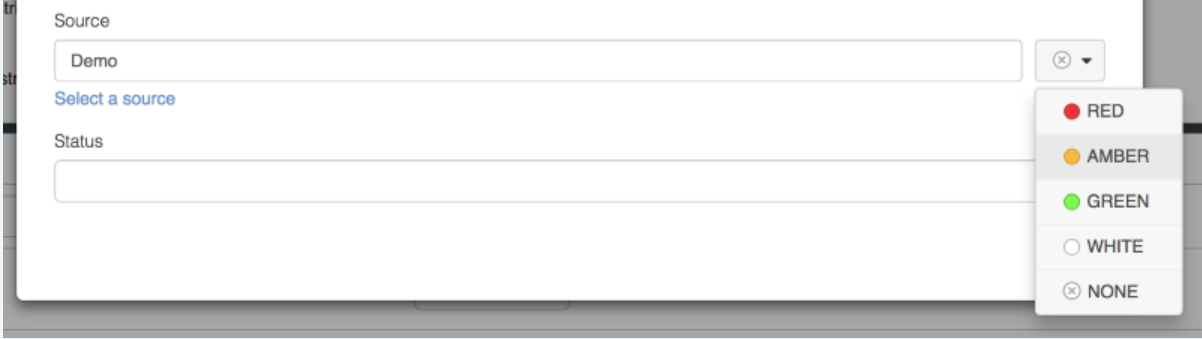


2. Enter a name.
3. Select a **Source** from the dropdown provided.



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

See the [Traffic Light Protocol \(TLP\)](#) topic for more information on TLP schema.



The screenshot shows a web form for adding an adversary. It has two main input fields: 'Source' and 'Status'. The 'Source' field contains the text 'Demo' and has a link 'Select a source' below it. The 'Status' field is empty. To the right of the 'Status' field is a dropdown menu for the Traffic Light Protocol (TLP) with the following options: RED (red circle), AMBER (yellow circle), GREEN (green circle), WHITE (white circle), and NONE (grey circle with an X). The dropdown menu is currently open, showing these options.

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

## 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.

THREATQ Threat Library

**Claw** Edit

ADVERSARY

Created: 04/17/2019 First Seen: 04/17/2019 06:17pm

Actions

Context

Attributes (2)

Sources (1)

**Attributes**

☐ ATTRIBUTE TYP

Start typing

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

The Edit Adversary dialog box opens.

**Edit Adversary**

Name

Claw

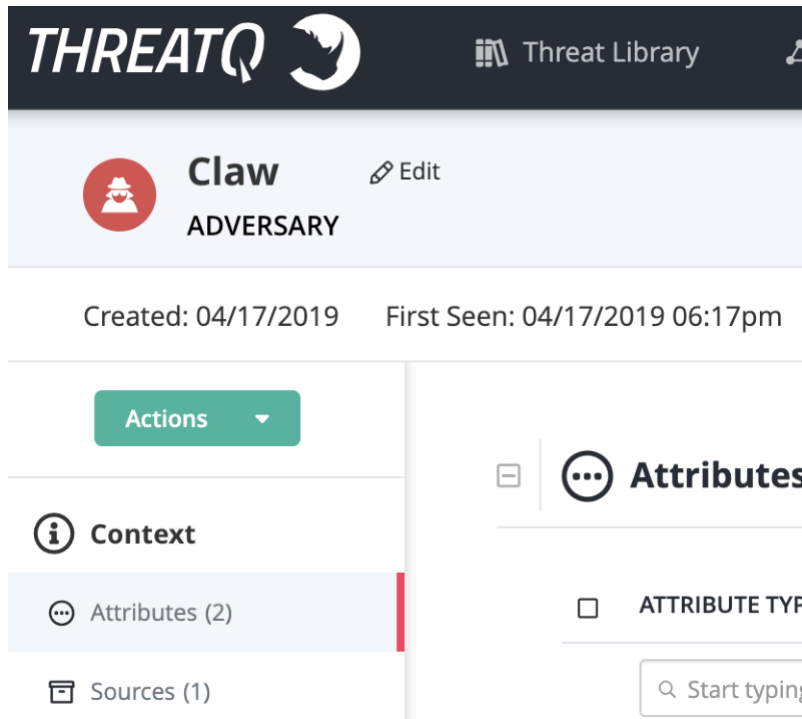
Save Adversary Cancel

3. Make the desired change to the Adversary name.
4. Click on **Save Adversary**.

## Deleting Adversaries

1. Locate and click on the adversary.

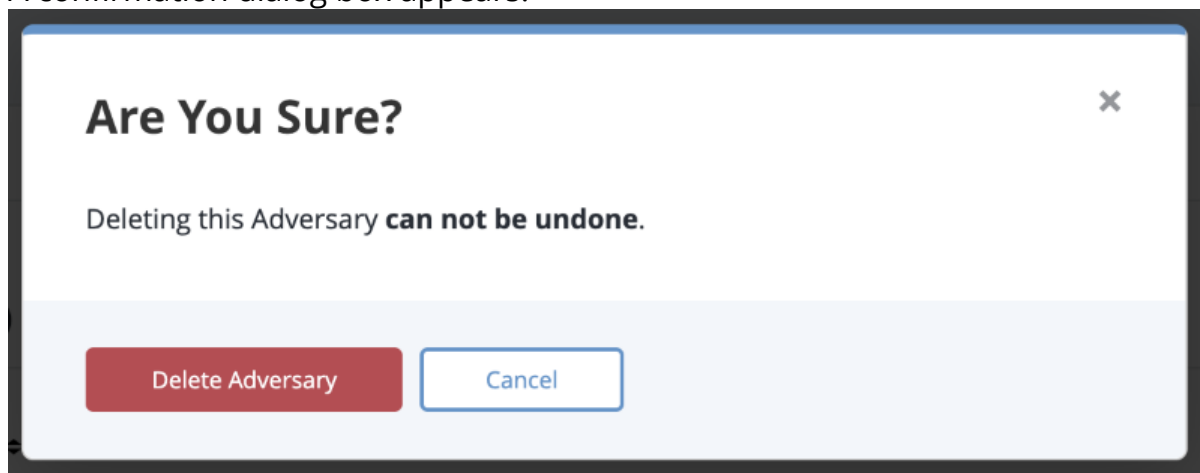
The Adversary Details page opens.



The screenshot shows the ThreatQ interface. At the top, there's a dark header with the ThreatQ logo and a 'Threat Library' link. Below this, the 'Claw' adversary is displayed with a red circular icon containing a white mountain and a red dot. The word 'ADVERSARY' is written below the icon. To the right of the icon is an 'Edit' button. Below the adversary name, the creation and first seen dates are listed: 'Created: 04/17/2019' and 'First Seen: 04/17/2019 06:17pm'. On the left side, there's a sidebar with a green 'Actions' button at the top. Below it, there's a 'Context' section with a list of items: 'Attributes (2)' and 'Sources (1)'. The 'Attributes (2)' item is highlighted. On the right side, there's an 'Attributes' section with a search bar labeled 'Start typing' and a table header 'ATTRIBUTE TYP'.

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

A confirmation dialog box appears.



3. Click on **Delete Adversary**.

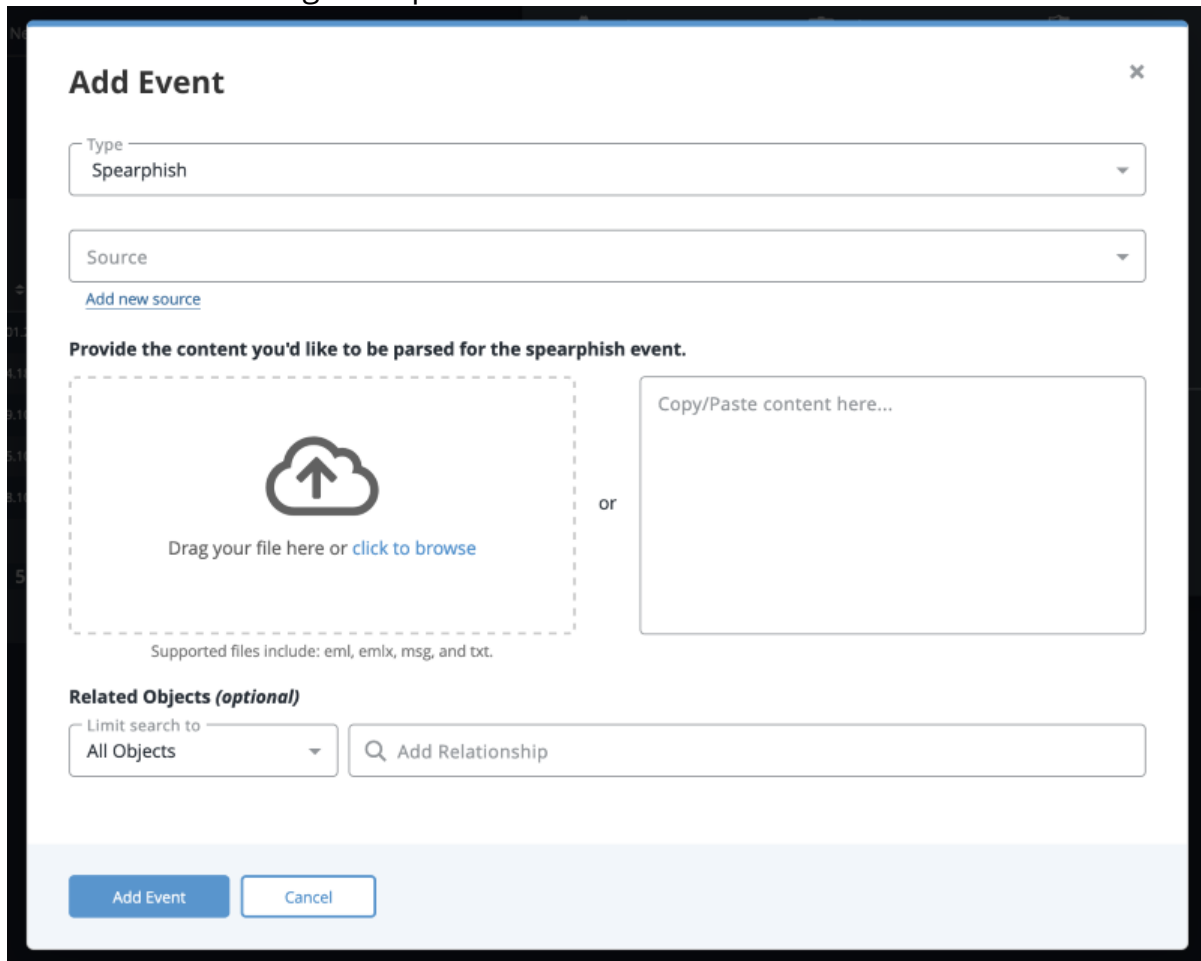
# Events

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

## Adding Events

1. Go to **Create > Event**.

The Add Event dialog box opens.

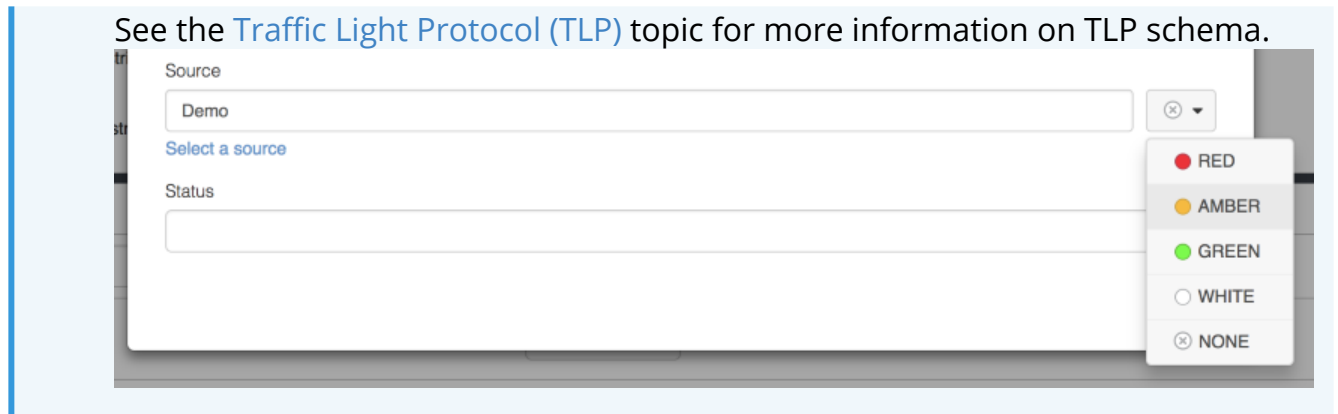


2. Select the **Event Type**.
3. Select a **Source** from the dropdown list provided.



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





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

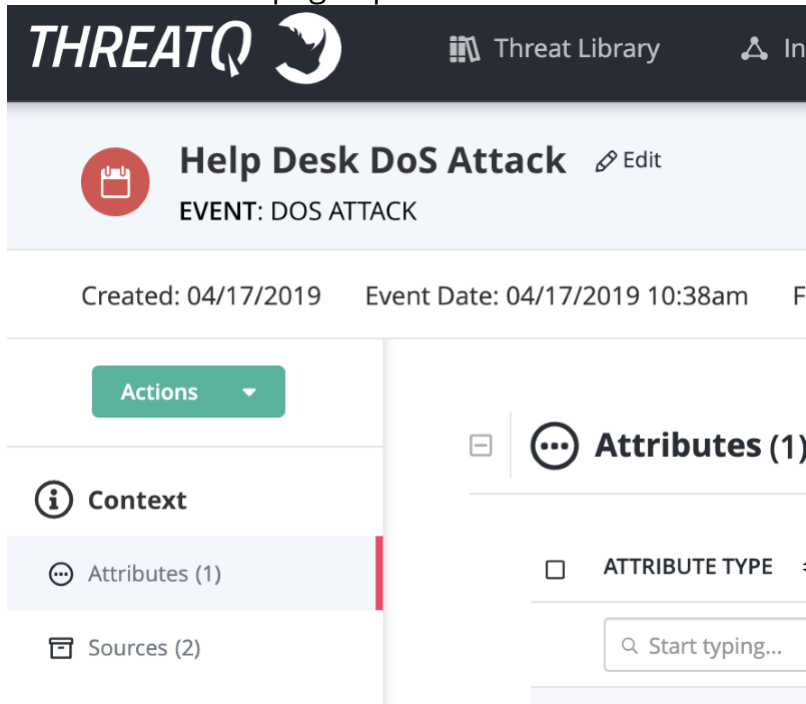
See the [Object Details](#) section and its topics for details on adding context to an object such as adding sources, attributes, and related objects.

## 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.

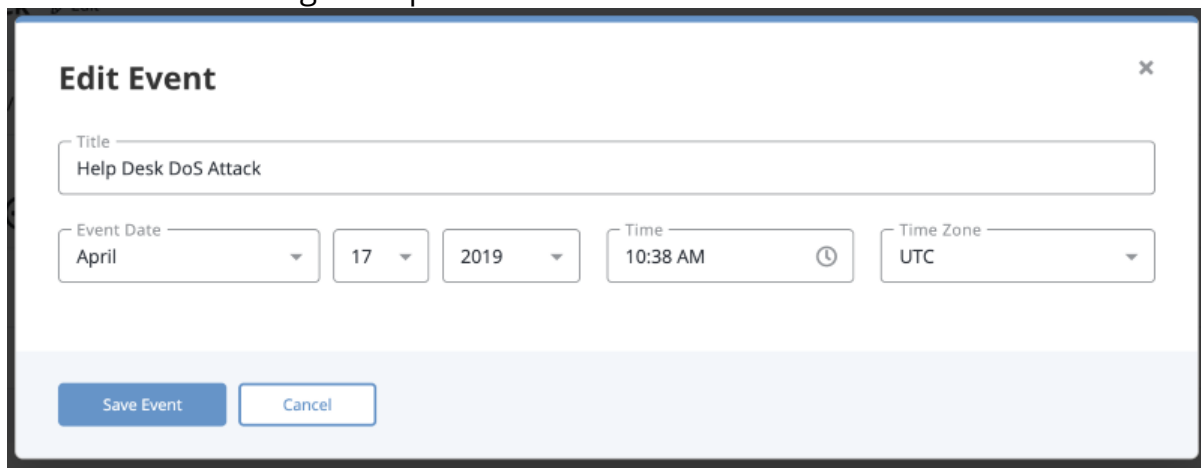
The Event Details page opens.



The screenshot shows the ThreatQ interface. At the top, there's a dark header with the ThreatQ logo, a 'Threat Library' icon, and a share icon. Below this, the event title 'Help Desk DoS Attack' is displayed with a red calendar icon and an 'Edit' link. Underneath, it says 'EVENT: DOS ATTACK'. A status bar shows 'Created: 04/17/2019' and 'Event Date: 04/17/2019 10:38am'. On the left, there's a sidebar with 'Actions', 'Context' (with sub-items 'Attributes (1)' and 'Sources (2)'), and a red vertical bar. The main area shows 'Attributes (1)' with a search bar labeled 'Start typing...'.

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

The Edit Event dialog box opens.



The screenshot shows the 'Edit Event' dialog box. It has a title bar with a close button. The form contains a 'Title' field with 'Help Desk DoS Attack'. Below it, there are fields for 'Event Date' (April, 17, 2019), 'Time' (10:38 AM), and 'Time Zone' (UTC). At the bottom, there are 'Save Event' and 'Cancel' buttons.

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.




 Threat Library
  In



## Help Desk DoS Attack

EVENT: DOS ATTACK

Edit

Created: 04/17/2019    Event Date: 04/17/2019 10:38am    F

Actions

 Context

 Attributes (1)

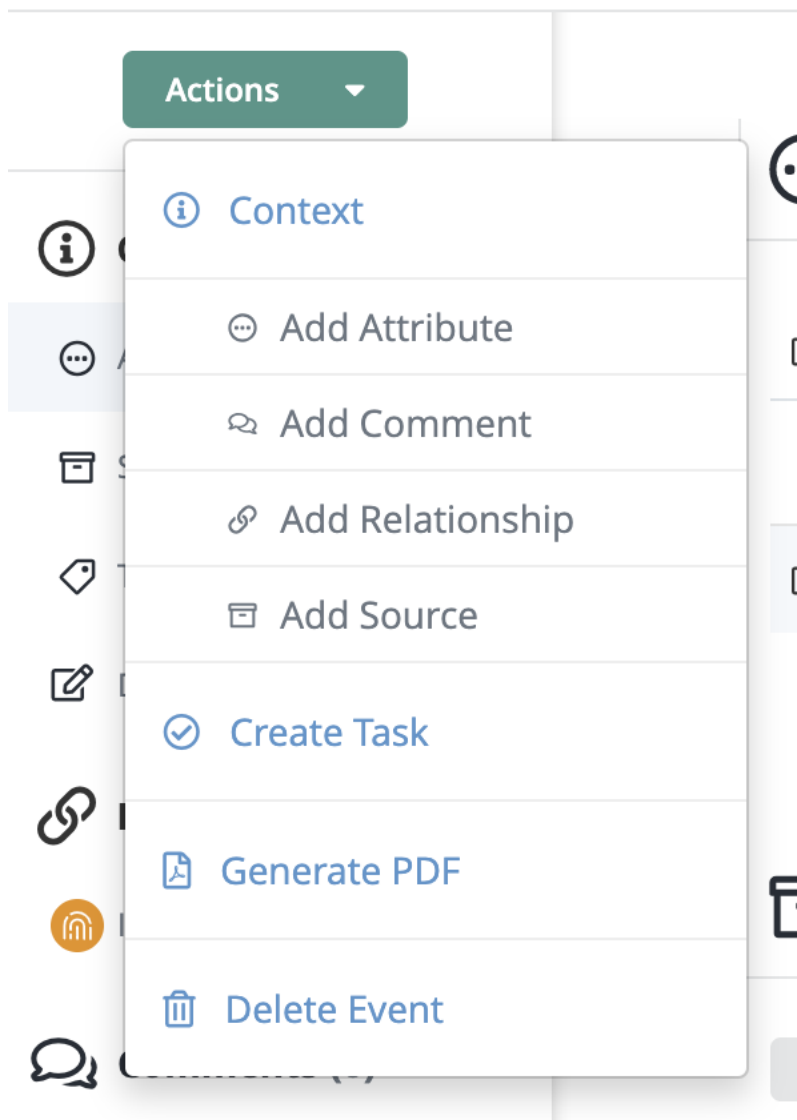
 Sources (2)



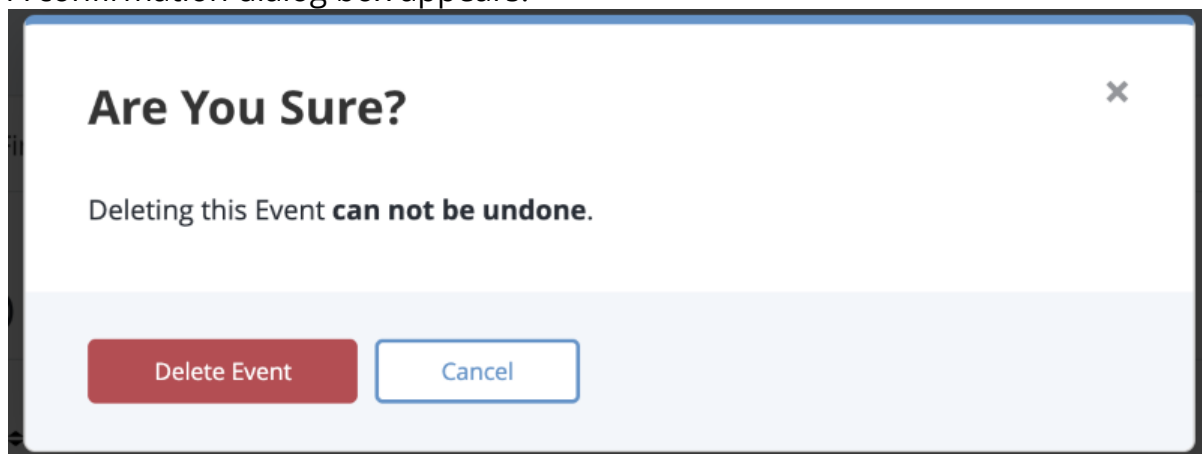
**Attributes (1)**

☐ ATTRIBUTE TYPE

- Click on the **Actions** menu and select **Delete Event**.  
Created: 04/17/2019    Event Date: 04/1



A confirmation dialog box appears.



- Click on **Delete Event**.

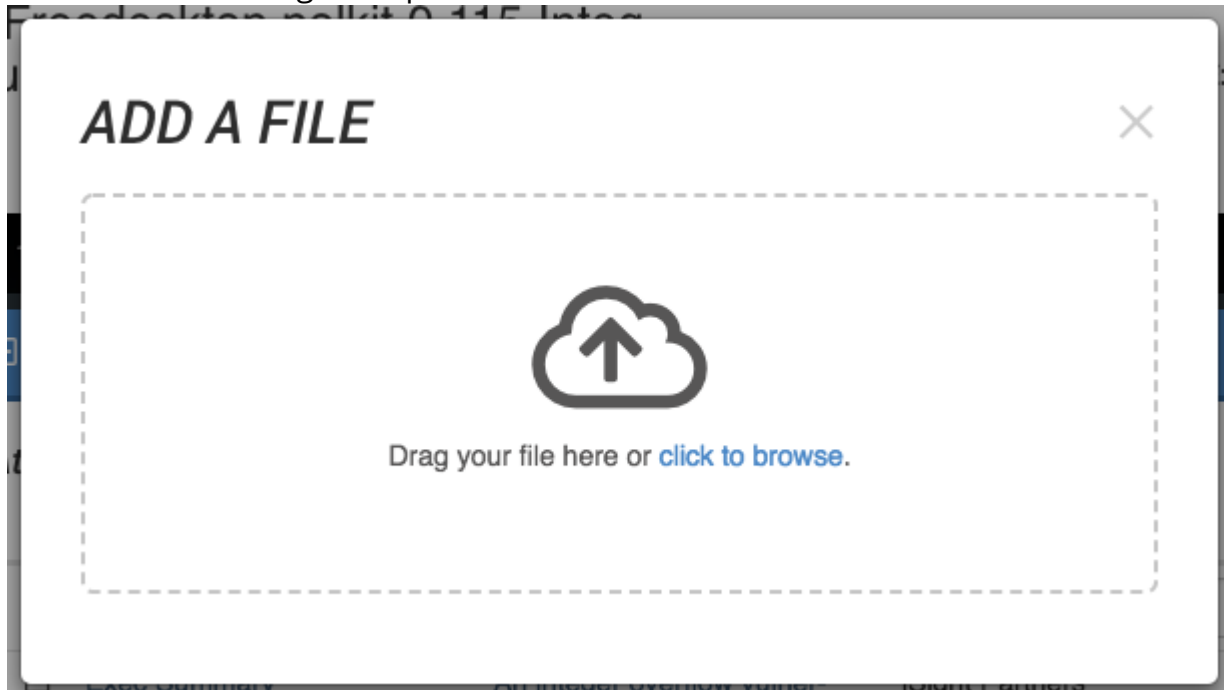
# Files

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

## 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.

**Add a File** [X]

Name  
han.png

Title  
han.png

Source [v]  
[Add new source](#)

Category  
CrowdStrike Intelligence [v]

**Malware Safety Lock** OFF [ON]  
Enabling this will .zip files for safer download. To unzip, use the password "infected".

Tags (0) Press enter after typing to add each word.  
Type here and press enter

**Related Objects (optional)**  
Limit search to: All Objects [v]

**Save File**

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



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

Source  
Demo [X] [v]

[Select a source](#)

Status  
[ ]

TLP Designation:  
● RED  
● AMBER  
● GREEN  
○ WHITE  
⊗ NONE

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**.

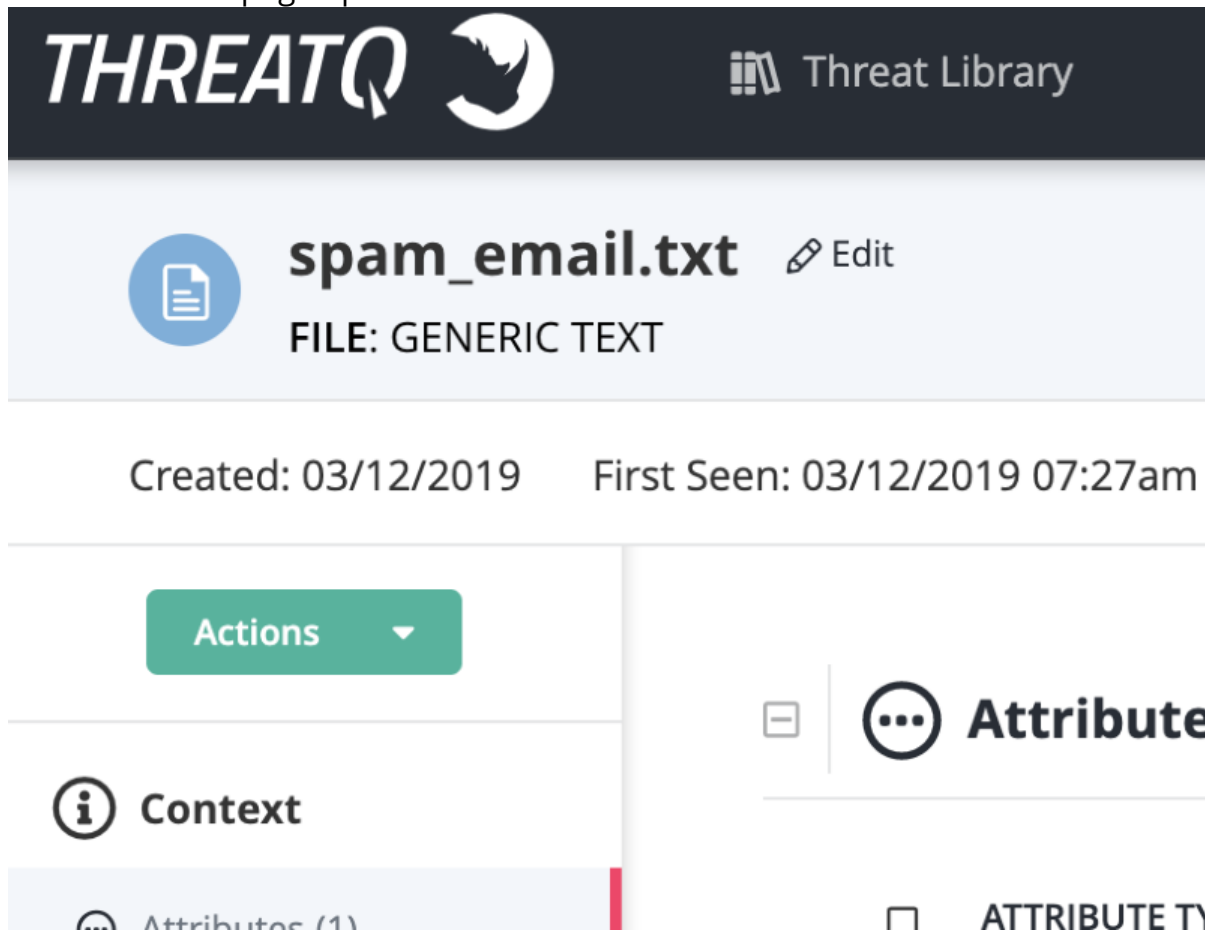
## Adding Context

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.

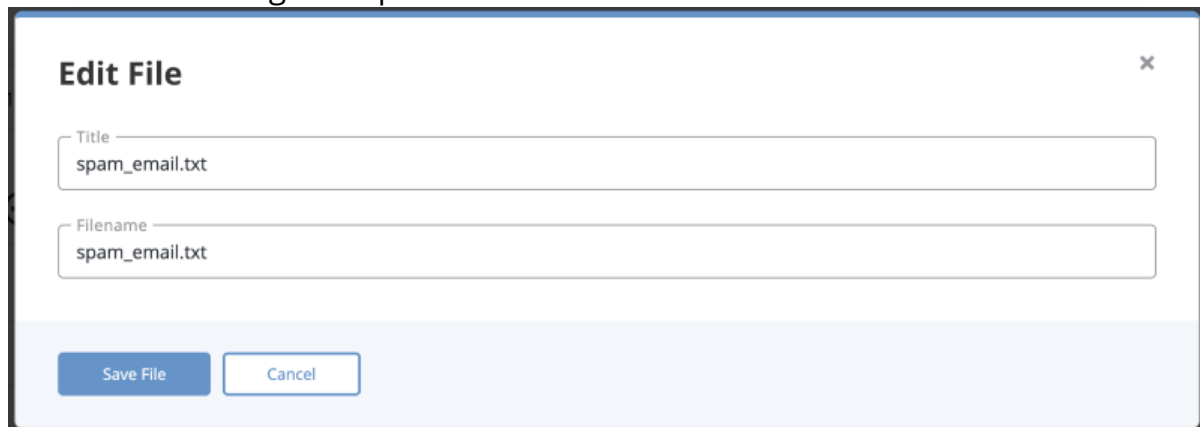
The File Details page opens.



The screenshot shows the ThreatQ interface. At the top is a dark header with the ThreatQ logo and a 'Threat Library' link. Below this is a light blue section for the file 'spam\_email.txt', which is identified as a 'GENERIC TEXT' file. It includes an 'Edit' button. Below the file name, it shows the creation date '03/12/2019' and the first seen time '03/12/2019 07:27am'. On the left, there is a sidebar with an 'Actions' button and a 'Context' section. On the right, there is an 'Attribute' section with a list of attributes, one of which is 'ATTRIBUTE TY'.

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

The Edit File dialog box opens.



The 'Edit File' dialog box is shown. It has a title bar with a close button. Inside, there are two input fields: 'Title' and 'Filename', both containing the text 'spam\_email.txt'. At the bottom, there are two buttons: 'Save File' and 'Cancel'.

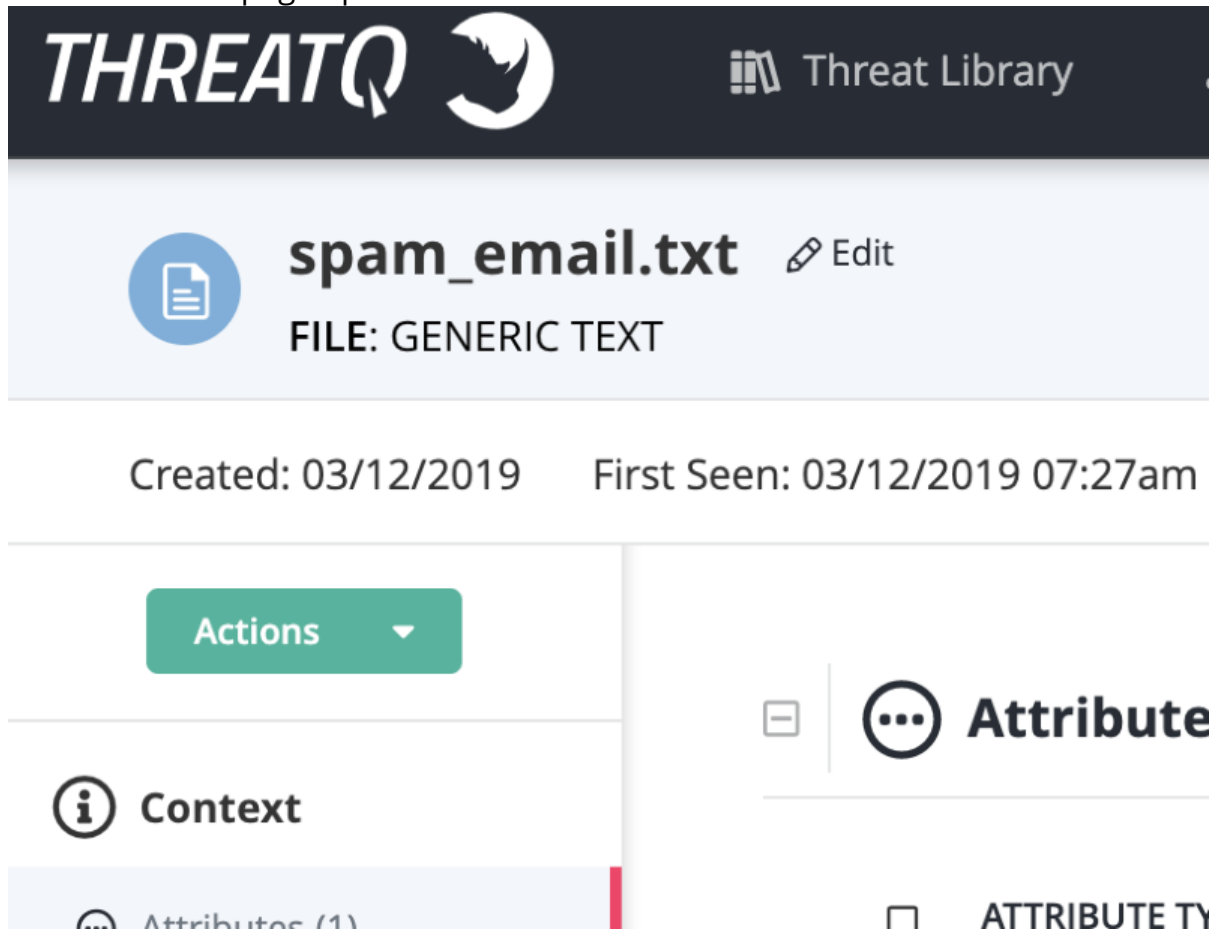
3. Make the desired change to the File Name.
4. Click on **Save File**.



## Deleting Files

1. Locate and click on the file.

The File Details page opens.



The screenshot shows the ThreatQ interface. At the top is a dark header with the ThreatQ logo and a 'Threat Library' link. Below this is a light blue card for the file 'spam\_email.txt', which is identified as a 'FILE: GENERIC TEXT'. It includes an 'Edit' button. Below the card, the file's creation date '03/12/2019' and first seen time '07:27am' are displayed. The main content area is split into two panels. The left panel has an 'Actions' button and a 'Context' section. The right panel has an 'Attribute' section with a list of attributes, including 'ATTRIBUTE TY'.

**THREATQ** Threat Library

 **spam\_email.txt**  Edit  
FILE: GENERIC TEXT

Created: 03/12/2019 First Seen: 03/12/2019 07:27am

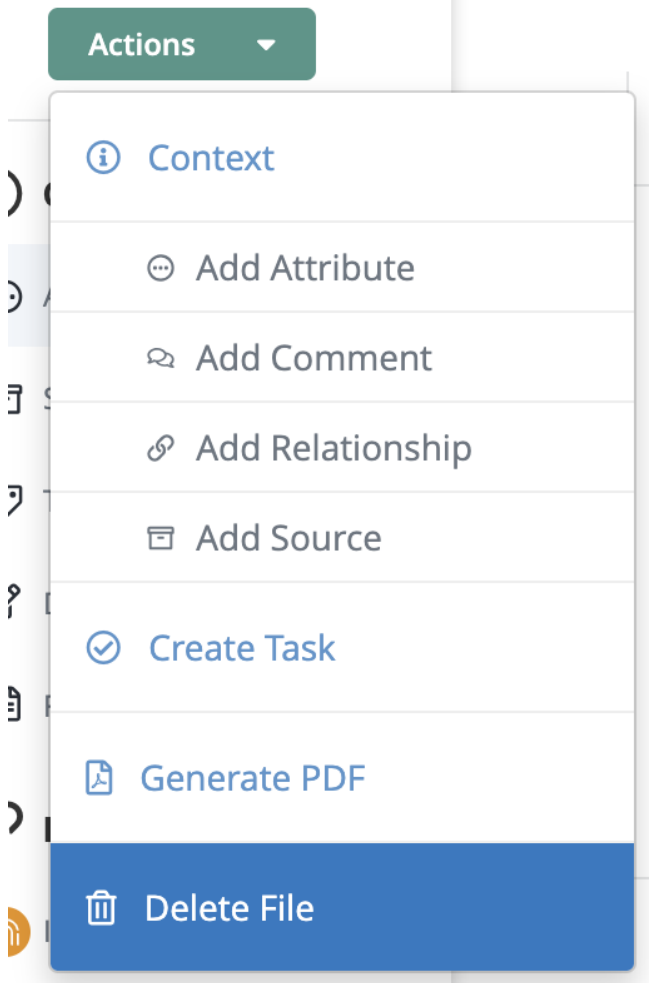
**Actions**

**Context**

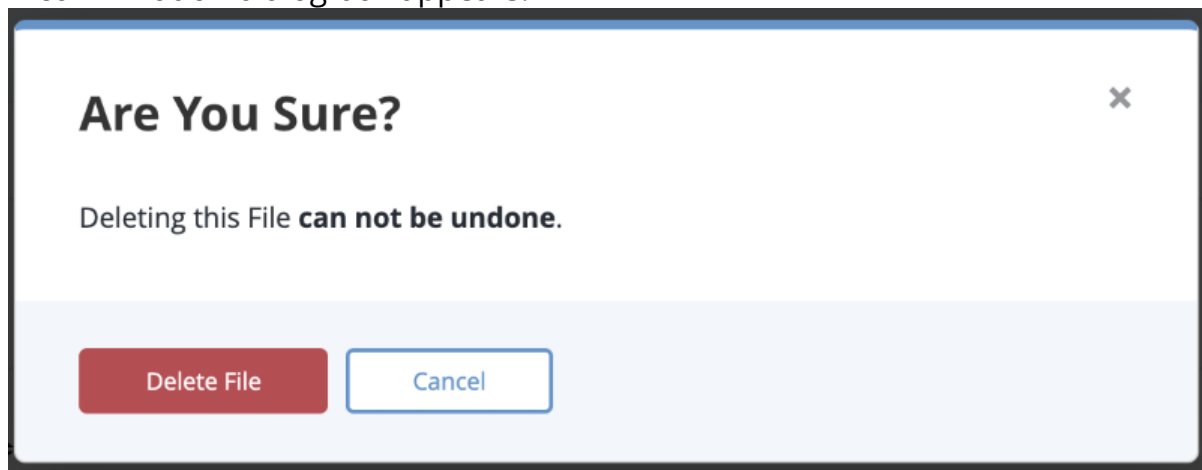
**Attribute**

ATTRIBUTE TY

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



A confirmation dialog box appears.



3. Click on **Delete File**.

# Indicators

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

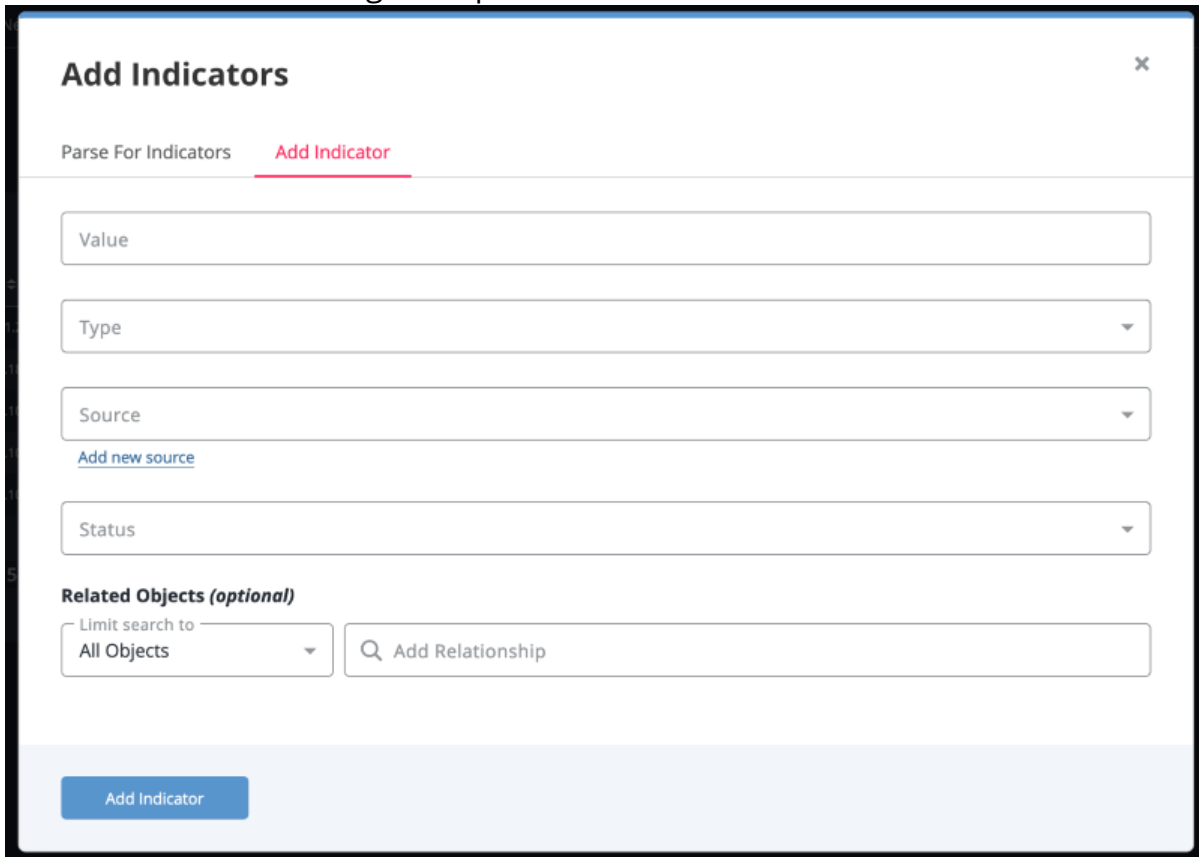
Indicators can be scored to allow you to apply weighting using contextual information, such as sources, attributes, and indicator types, as they are added to ThreatQ. You can also set a manual score per indicator.

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

## Adding an Indicator

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

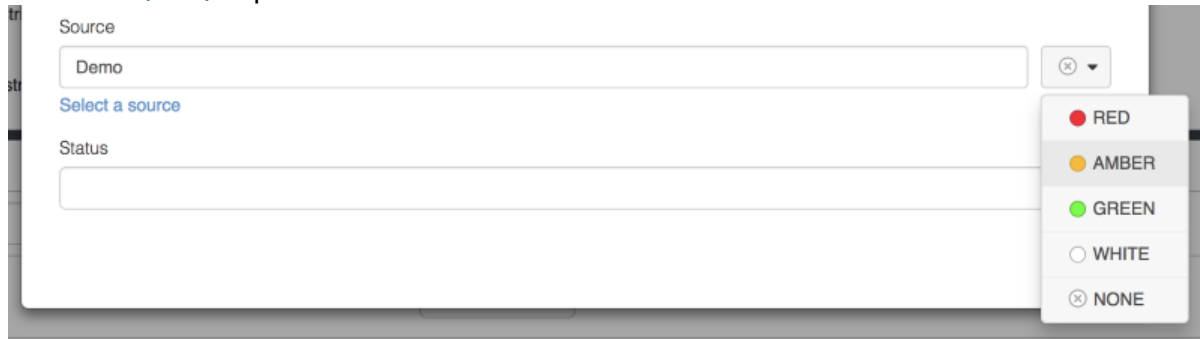
The Add Indicators dialog box opens.



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



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

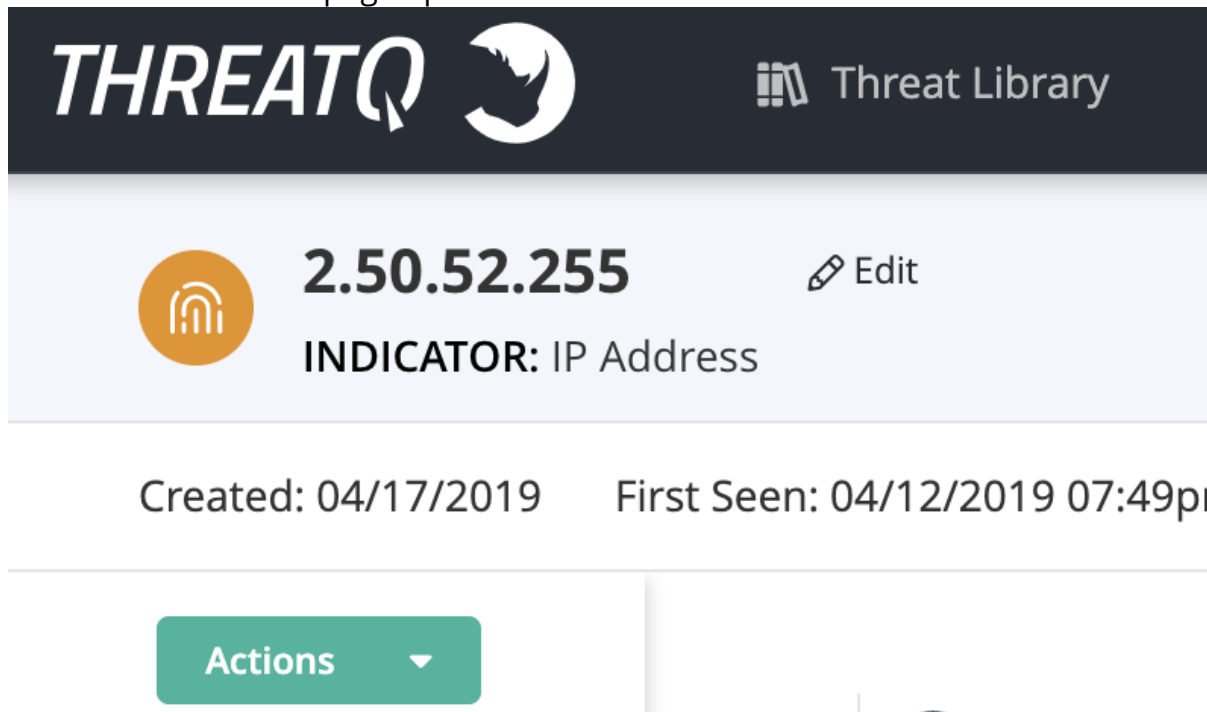
## Adding Context

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

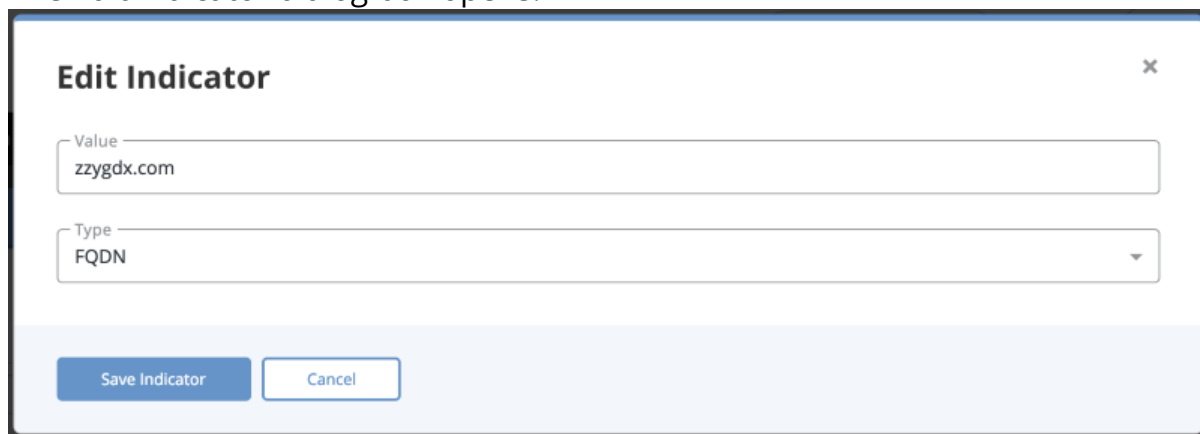
1. Locate and click on the indicator.

The Indicator Details page opens.



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

The Edit Indicator dialog box opens.

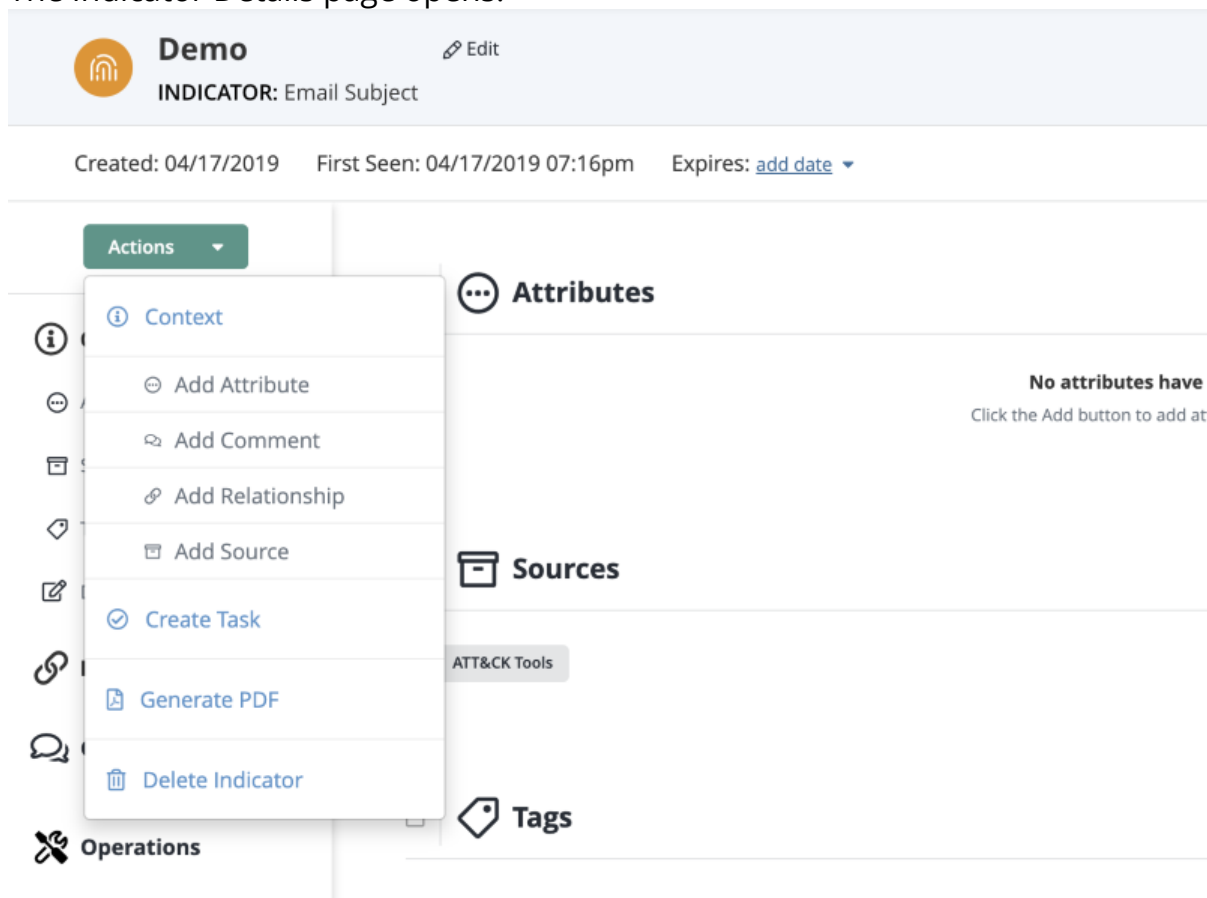


3. Make the desired change to the indicator **Value** and **Type**.
4. Click on **Save Indicator**.

## Deleting an Indicator

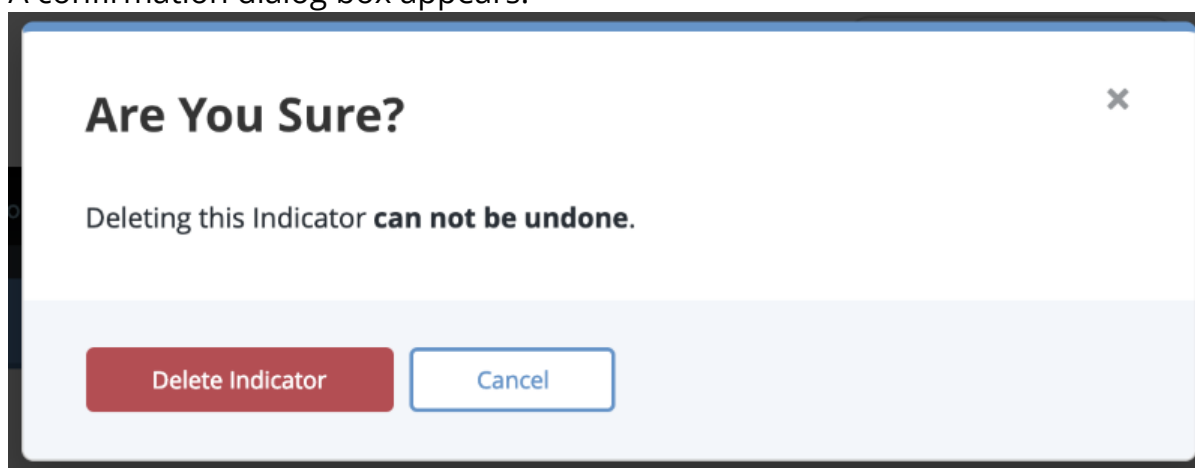
1. Locate and click on the Indicator.

The Indicator Details page opens.



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

A confirmation dialog box appears.



3. Click on **Delete Indicator**.

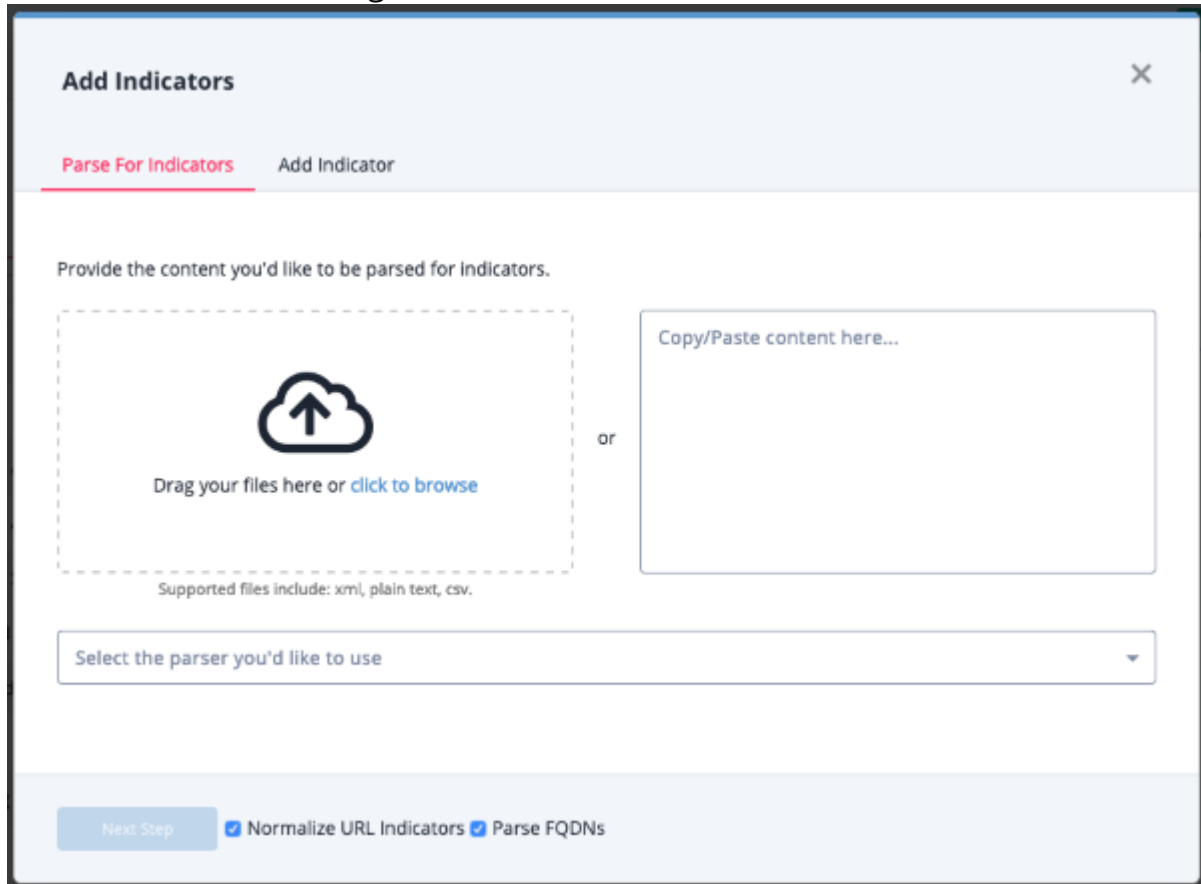
## Parsing for an Indicator

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



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

The Add Indicators dialog box will load.



2. Do one of the following:
  - Drag your file(s) into the left pane.
  - Click on **Click to Browse**, and locate the file you wish to upload.
  - Copy/paste the content in the right pane.
3. Select the **Parser**.
4. Review and update, if needed, the parsing checkbox options.

Parsing options include:

| OPTION                   | DESCRIPTION                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Normalize URL Indicators | <p>When checked, parsed URLs will have ports and leading protocol adjusted, as well as unneeded quotes and spaces removed.</p> <p>See the <a href="#">Indicator URL Normalization</a> topic for more details.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Parse FQDNs              | <p>When checked, the Indicator Parser will parse FQDNs from the text and derive FQDN indicators from URLs in the text.</p> <p><b>Example (checked):</b> URL: <code>https://tqexample.com/table.jspa?query_string_example</code></p> <p>Indicators created:</p> <ul style="list-style-type: none"><li>◦ <code>tqexample.com/table.jspa</code> (the URL)</li><li>◦ <code>tqexample.com</code> (the derived FQDN from the URL)</li></ul> <p>When unchecked, the Indicator Parser will not generate FQDN indicators from the parsed text.</p> <p><b>Example (unchecked):</b> URL: <code>https://tqexample.com/table.jspa?query_string_example</code></p> <p>Indicator created:</p> <ul style="list-style-type: none"><li>◦ <code>tqexample.com/table.jspa</code> (the URL)</li></ul> |



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**.



The Step 1 Import page will load.

## Import Indicators

[Abandon this import](#)

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.

google.rtf  
359 bytes

File Title (required)

google.rtf

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

[Add new name](#)

Value

[Add new value](#)

Source

[Add new source](#)

+

Next Step

Step 1: Tell us about the import > Step 2: Organize and classify



If at any point, you wish to abandon the import, click **Abandon this Import**.

6. Select whether to save or delete the file after the import.



Steps 7-9 pertain to saving the file. Skip to step 10 if you are not saving the file after import or did not upload a file on the previous step.

7. Update the **File Title** if needed.

8. Enter an optional **File Description**.
9. Confirm or update the **File Category**.
10. Select a **Source** from the dropdown menu provided.



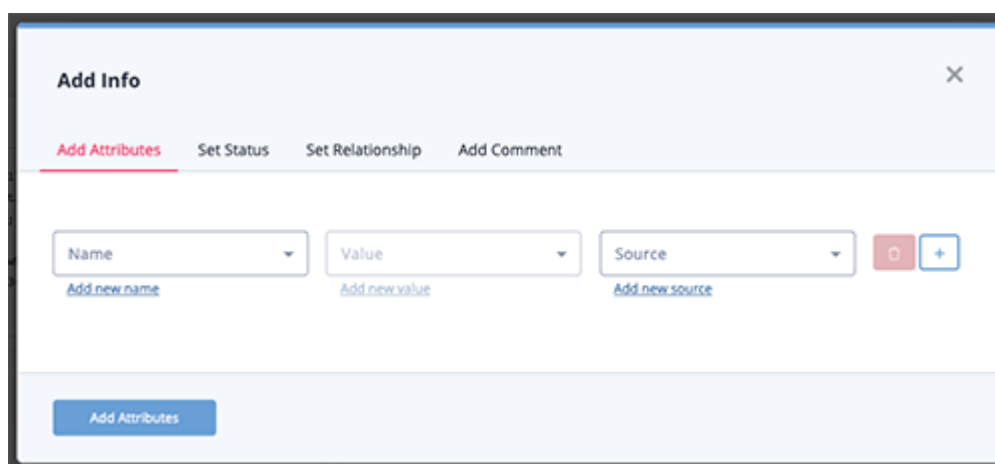
You can also click on **Add a New Source** if the desired source is not listed in the dropdown list. If administrators have enabled TLP view settings, users can select a TLP designation light for the new source in the dropdown list provided. See the [Traffic Light Protocol \(TLP\)](#) topic for more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

11. Select a **Status** to be applied to the extracted indicators.
12. Enter any **Tags** that should be applied to the extracted indicators.
13. Select any optional **Attributes** to be applied.
14. Click on **Next Step**.

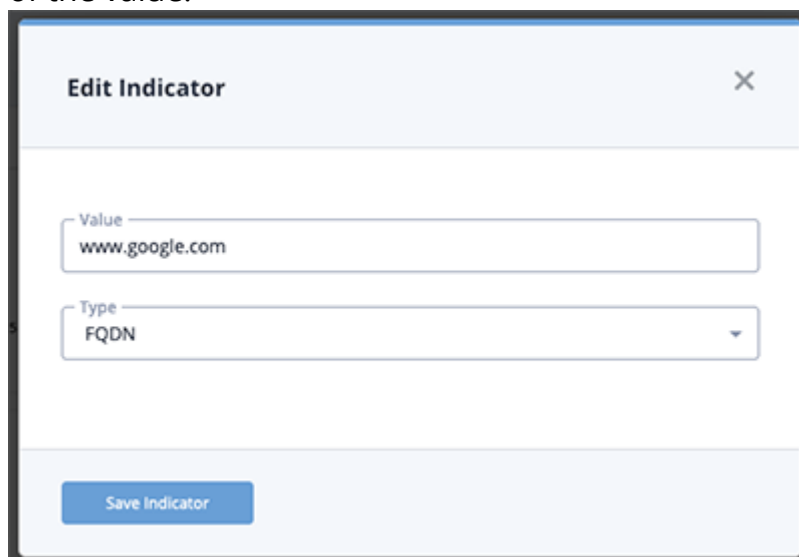
The Step 2: Organize and Classify page will load.

15. Locate and select one or more indicators using one of the following options:
  - Original Content (on the left)
  - From the table (on the right)
  - By using the Select dropdown menu
  - The Value, Type, Status, and Source sortable headers.
16. Once you have selected one or more indicators, you can perform these functions via the **Add Info** button:

| FUNCTION                | DETAILS                                                |
|-------------------------|--------------------------------------------------------|
| <b>Add Attributes</b>   | Add one or more attributes to the selected indicators. |
| <b>Set Status</b>       | Set a status for the selected indicators.              |
| <b>Set Relationship</b> | Link the selected indicator(s) to another object.      |
| <b>Add Comment</b>      | Add a comment to the selected indicators.              |



17. You can edit the value or type of an indicator by clicking the pencil icon located to the left of the value.



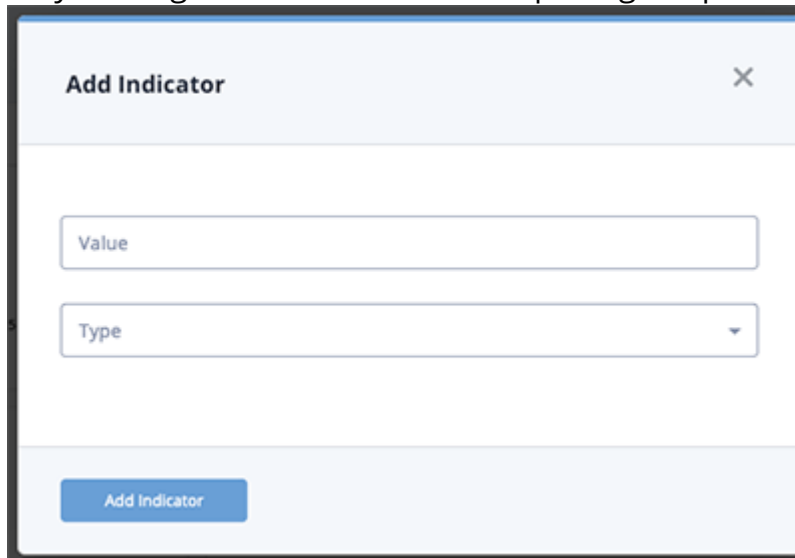
You can also update the **Status** and **Type** of an indicator listed in the table by clicking the existing value in the row to reveal a dropdown. Use the dropdown to select a new Status

or Type.



The screenshot shows the ThreatQ Indicators interface. At the top, there are tabs for 'All (1)', 'New (1)', and 'Pre-Existing (0)'. Below the tabs, there is a 'Select' dropdown, 'Add Info' and 'Remove' buttons, and a green 'Add Indicator' button. The main area is a table with columns: VALUE, TYPE, STATUS, and SOURCE. Below the table, there is a search bar with the text 'Q Start typing...'. At the bottom, there is a browser address bar showing 'www.google.com' and a search bar with the text 'CI Army List IPs'.

18. **Add Indicator** - If you notice an indicator on the left that was not extracted, you can add it by clicking Add Indicator and completing the process.



The screenshot shows the 'Add Indicator' modal form. It has a title bar with a close button. The form contains two input fields: 'Value' and 'Type'. Below the fields is a blue 'Add Indicator' button.

19. Click on **Finish Import**.

## CSV File Format Parsing

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

- The file must be comma-delimited.
- The file must include at least the following columns:
  - Indicator
  - Type: This column cannot contain types that are not already established in ThreatQ. You cannot add custom indicator types and indicator types are case sensitive. Choose from the following:
    - CIDR
    - Block
    - CVE

- Email Address
  - Email Attachment
  - Email Subject
  - File Path
  - Filename
  - FQDN
  - Fuzzy
  - Hash
  - GOST
  - Hash
  - IP Address
  - MD5
  - Mutex
  - Password
  - Registry Key
  - SHA-1
  - SHA-256
  - SHA-384
  - SHA-512
  - String
  - URL
  - URL Path
  - User-agent
  - Username
  - X-Mailer
- Status

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

## 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.

### 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 [Automatic Expiration](#) 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.

The screenshot shows the ThreatQ interface for a specific indicator. The indicator is identified by a URL: 195.123.245.83:447/tt0002/william-pc\_w629200.f71819bb1edf5078c2b2ab2aff931102/5/bcclientdll64/. The interface includes a sidebar with 'Context' and 'Attributes (10)' sections. The 'Expires' field shows 'add date' with a dropdown arrow. The dropdown menu is open, showing four options: 'Add 7 days', 'Add 14 days', 'Protect from auto-expiration', and 'Remove current expiration 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 you can rely on ThreatQ's scoring algorithm to calculate scores. After scores are calculated, you can change the score as desired to your custom value or accept the calculated value.

## Building a Scoring Algorithm

You can build a scoring algorithm that will automatically assign 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.

The screenshot displays the ThreatQ web application interface. At the top, the 'THREATQ' logo is on the left, and navigation links for 'Threat Library', 'Investigations', and 'Analytics' are in the center. On the right, there are buttons for '+ Create', a search icon, a settings icon, and a user profile icon labeled 'DK'. Below the navigation bar, the page title is 'Demo' with an 'Edit' link. The indicator being viewed is 'INDICATOR: Email Subject'. To the right of the title, there is a 'SCORE' dropdown menu currently set to '0 - Very Low', and a 'STATUS' dropdown set to 'Active'. A 'Created: 04/17/2019' and 'First Seen: 04/17/2019 07:16pm' timestamp is shown, along with an 'Expires: add date' link. On the left sidebar, under the 'Actions' dropdown, there is a 'Context' section with links to 'Attributes (0)', 'Sources (1)', 'Tags (0)', 'Description', 'Relationships', 'Comments (0)', 'Operations', and 'Audit Log'. The main content area has a tabbed interface with 'Attributes', 'Sources', 'Tags', and 'Description' tabs. The 'Attributes' tab is active, showing a list of attributes. The 'Sources' tab shows a single source 'ATT&CK Tools'. The 'Tags' tab shows a text input field 'add tag' and a 'Tags (0)' label. The 'Description' tab shows a text input field and an 'Edit' link. The 'SCORE' dropdown menu is open, showing a list of scores from 0 to 10, with '6 - Low' selected. The list includes: 10 - Very High, 9 - High, 8 - Medium, 7 - Medium, 6 - Low (selected), 5 - Low, 4 - Very Low, 3 - Very Low, 2 - Very Low, 1 - Very Low, and 0 - Very Low. There are also 'Add' and 'Delete' buttons next to the list.

Optionally, you may revert to the calculated score by clicking on the Score dropdown and selecting **Generated Score**.

Press enter after typing to add each word.

## Indicator Status

Every indicator in the system will have a status applied to it.



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. |

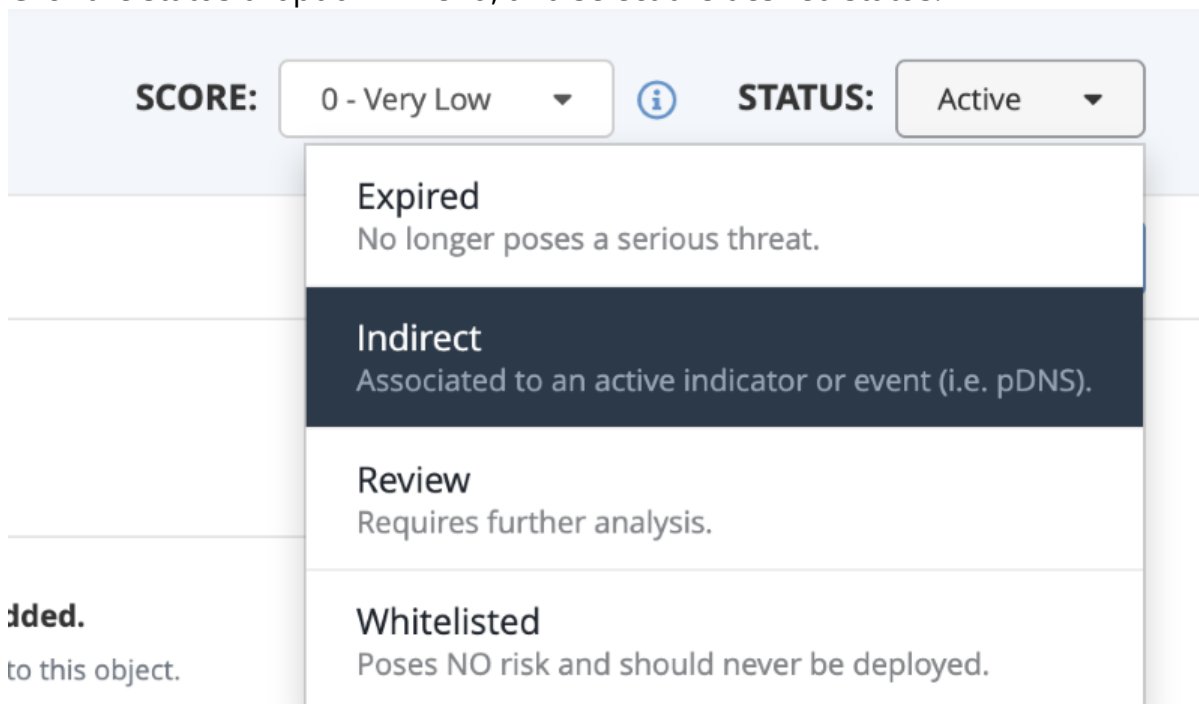
## Custom Statuses

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.



The screenshot shows the 'STATUS:' dropdown menu open. The current status is 'Active'. The dropdown menu lists four options: 'Expired' (No longer poses a serious threat.), 'Indirect' (Associated to an active indicator or event (i.e. pDNS).), 'Review' (Requires further analysis.), and 'Whitelisted' (Poses NO risk and should never be deployed.). The 'Indirect' option is highlighted.

**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.

**Added.**  
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.

# 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.



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&fid0=c27] are important but can significantly limit pattern-matching detection capabilities due to the likelihood of parameter deviations, as well as, hamper the volume of URL indicators being deployed. To increase the probability of detection the http parameters are extracted and created as attributes.

In this example:

| FIELD                                 | VALUE                                       |
|---------------------------------------|---------------------------------------------|
| URL IOC                               | chained.j3oilgasinc.net/civis/viewforum.php |
| Attribute = HTTP Parameter = keywords | 9obo&fid0=c27                               |

## Maintain “WWW” on FQDN Indicators

When parsing or importing a FQDN the “www” will be maintained.

## Replace and/or Remove Special Characters

| CHARACTER                               | REPLACEMENT                                                                                          |
|-----------------------------------------|------------------------------------------------------------------------------------------------------|
| ASCII Values < 32<br>ASCII Values > 127 | <space>                                                                                              |
| Ascii 96                                | -                                                                                                    |
| Ascii145                                | '                                                                                                    |
| Ascii146                                | '                                                                                                    |
| Ascii147                                | "                                                                                                    |
| Ascii148                                | "                                                                                                    |
| Ascii151                                | -                                                                                                    |
| carriage return and line feed           | <space>                                                                                              |
| Control Characters                      | Remove                                                                                               |
| Convert to UTF8                         | Remove leading and trailing space, tab, newline, carriage return, vertical tabs and null characters. |



## Supported Defanging Techniques

The table below lists all supported indicator defanging techniques.

[.] => .

[dot] => .

(dot) => .

[d] => .

-dot- => .

\_dot\_ => .

hxxp:// => http://

hxxx:// => http://

hxxps:// => https://

hxxxs:// => https://

[hxxp] => http

hxtp:// => http://

htxp:// => http://

hxtps:// => https://

htxps:// => https://

|        |    |      |
|--------|----|------|
| [http] | => | http |
|--------|----|------|

|           |    |         |
|-----------|----|---------|
| [http://] | => | http:// |
|-----------|----|---------|

|         |    |       |
|---------|----|-------|
| [https] | => | https |
|---------|----|-------|

|            |    |          |
|------------|----|----------|
| [https://] | => | https:// |
|------------|----|----------|

|      |    |   |
|------|----|---|
| [at] | => | @ |
|------|----|---|

|      |    |   |
|------|----|---|
| -at- | => | @ |
|------|----|---|

|      |    |   |
|------|----|---|
| _at_ | => | @ |
|------|----|---|

|     |    |   |
|-----|----|---|
| -@- | => | @ |
|-----|----|---|

|     |    |   |
|-----|----|---|
| _@_ | => | @ |
|-----|----|---|

|     |    |   |
|-----|----|---|
| [@] | => | @ |
|-----|----|---|

|       |    |     |
|-------|----|-----|
| [www] | => | www |
|-------|----|-----|

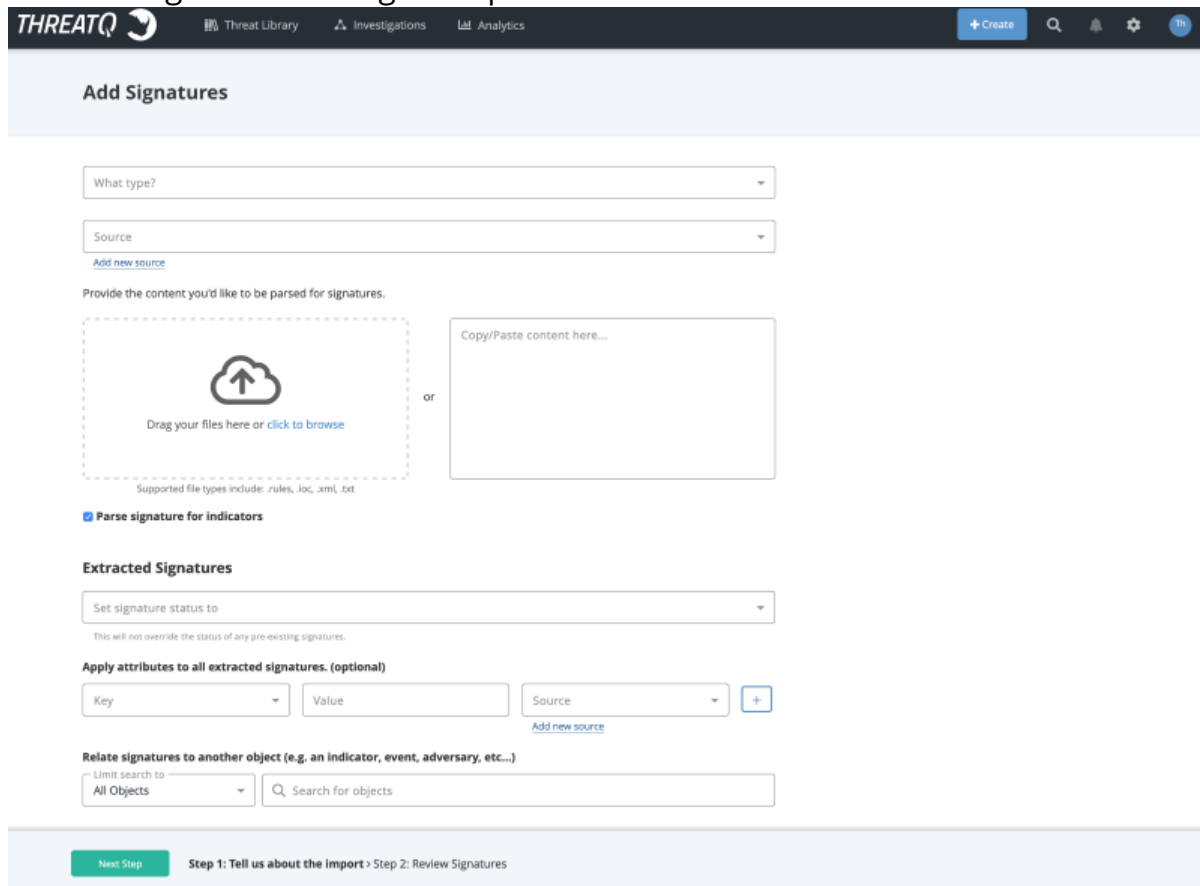
# Signatures

ThreatQ 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 Indicators, Events, Adversaries, and Files.

## Adding a Signature

1. From the main menu, choose **Create > Signature**.

The Add Signatures dialog box opens.



The screenshot shows the 'Add Signatures' dialog box in the ThreatQ interface. The dialog has a header bar with the ThreatQ logo and navigation links: Threat Library, Investigations, and Analytics. A '+ Create' button is in the top right. The main content area is titled 'Add Signatures' and contains several sections:

- What type?** A dropdown menu.
- Source** A dropdown menu with an 'Add new source' link below it.
- Provide the content you'd like to be parsed for signatures.** This section has two options: a dashed box with a cloud upload icon and the text 'Drag your files here or [click to browse](#)' (with supported file types: .rules, .ioc, .xml, .txt) and a text area labeled 'Copy/Paste content here...'. There is an 'or' between the two options.
- Parse signature for indicators** A checkbox that is checked.
- Extracted Signatures** A section with a 'Set signature status to' dropdown and a note: 'This will not override the status of any pre-existing signatures.'
- Apply attributes to all extracted signatures. (optional)** A section with 'Key', 'Value', and 'Source' dropdowns, an 'Add new source' link, and a '+' button.
- Relate signatures to another object (e.g. an indicator, event, adversary, etc...)** A section with a 'Limit search to' dropdown (set to 'All Objects') and a 'Search for objects' input field.

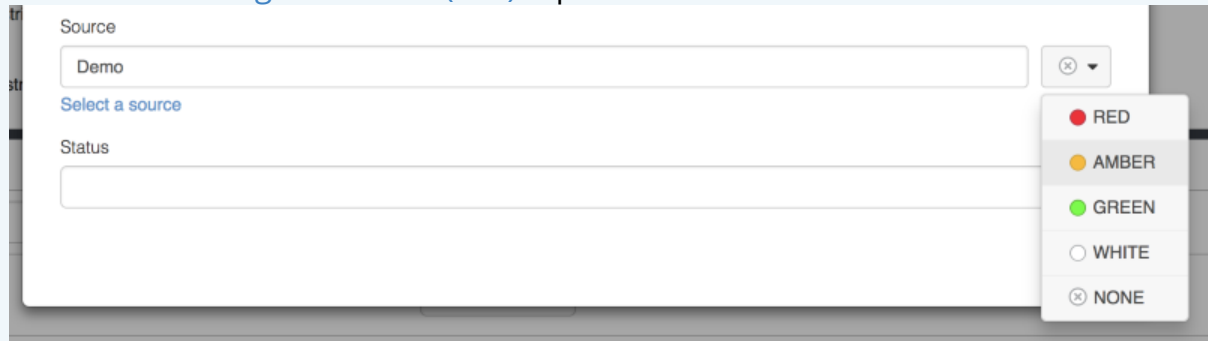
At the bottom, there is a 'Next Step' button and a progress indicator showing 'Step 1: Tell us about the import' and 'Step 2: Review Signatures'.

2. Choose the type of signature from the dropdown .
3. Select a **Source** from the dropdown provided.



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

See the [Traffic Light Protocol \(TLP\)](#) topic for more information on TLP schema.



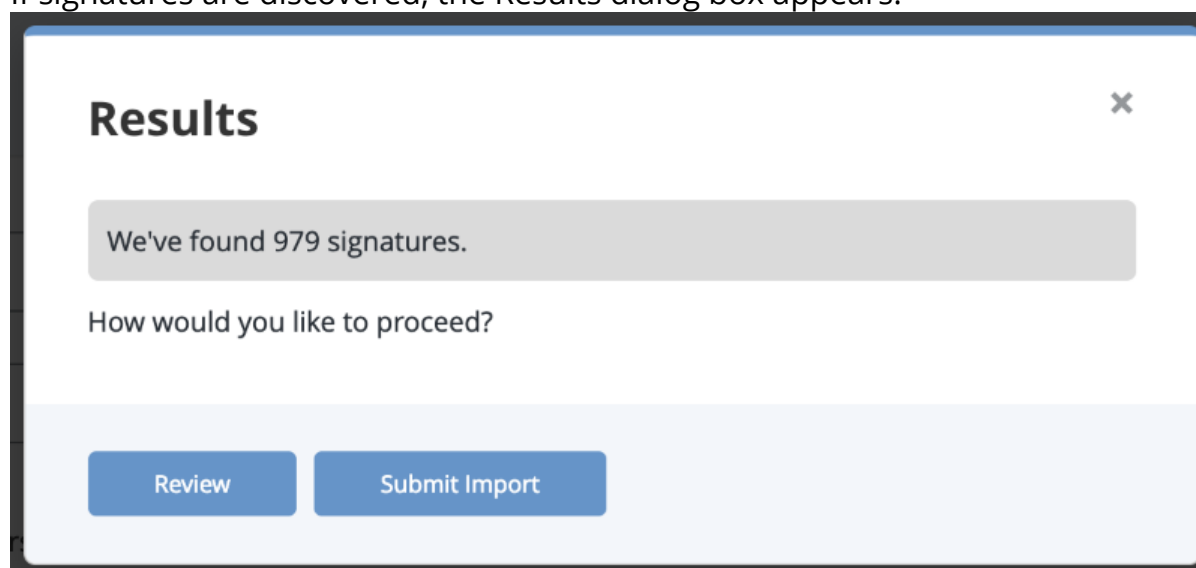
4. Do one of the following:
  - Drag your file(s) into the left pane.
  - Click click to browse, and locate the file you wish to upload.
  - Copy/paste content into the right pane.
5. Optionally, select to parse the signature for indicators.
6. Choose a **Signature Status** from the drop-down menu.
7. 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.
9. Click **Next Step**.

If signatures are discovered, the Results dialog box appears.



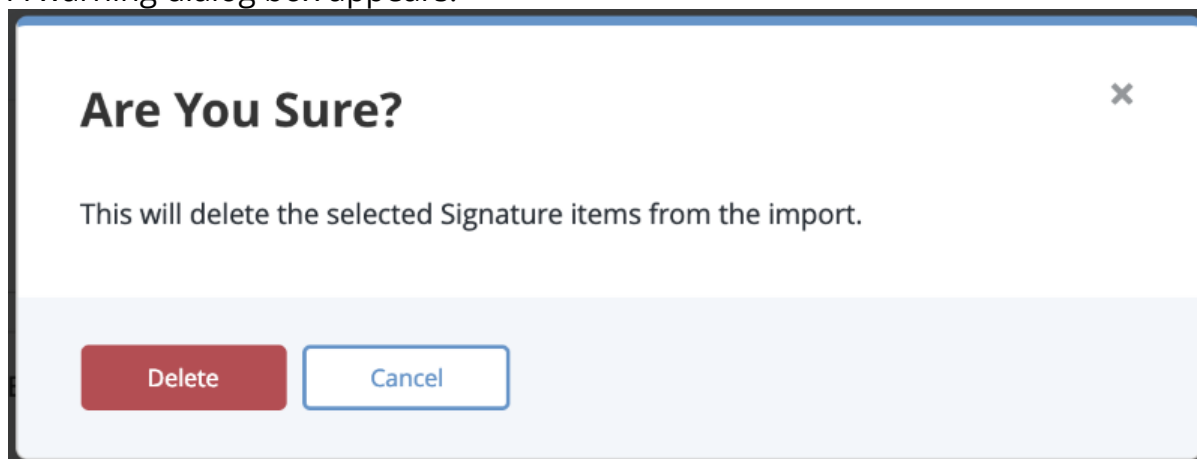
- You can either select **Submit Import** to finish adding the signatures or **Review** to customize what data is imported.

If you selected to review signatures, the Add Signatures Step 2: Review page loads.

|                          | Signature Name                                                                                      | Status | Attributes    | Indicators   | Action         |
|--------------------------|-----------------------------------------------------------------------------------------------------|--------|---------------|--------------|----------------|
| <input type="checkbox"/> | BROWSER-IE Microsoft Internet Explorer CDocument use after free attempt (26890:1)                   | Active | 15 Attributes | 0 Indicators | Show Details ▶ |
| <input type="checkbox"/> | BROWSER-IE Microsoft Internet Explorer CTreeNode use after free memory corruption attempt (26889:1) | Active | 15 Attributes | 0 Indicators | Show Details ▶ |
| <input type="checkbox"/> | BROWSER-IE Microsoft Internet Explorer CTreeNode use after free memory corruption attempt (26888:2) | Active | 15 Attributes | 0 Indicators | Show Details ▶ |
| <input type="checkbox"/> | BROWSER-IE Microsoft Internet Explorer onscroll use after free attempt (26887:5)                    | Active | 13 Attributes | 0 Indicators | Show Details ▶ |
| <input type="checkbox"/> | BROWSER-IE Microsoft Internet Explorer onscroll use after free attempt (26886:5)                    | Active | 13 Attributes | 0 Indicators | Show Details ▶ |
| <input type="checkbox"/> | BROWSER-IE Microsoft Internet Explorer onscroll use after free attempt (26885:5)                    | Active | 14 Attributes | 0 Indicators | Show Details ▶ |

- Select one or more signatures and click **Delete**.
- 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.



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.

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.

- Campaigns
- Courses of Action
- Exploit Targets
- Incidents
- TTP objects
- Identities (STIX 2.0)
- Reports (STIX 2.0)
- Vulnerabilities (STIX 2.0)

These objects enable better understanding and communication of STIX data. STIX data will be mapped to these objects and existing objects in the system.

## Parsing a STIX File for Indicators

ThreatQ allows you to upload a STIX file or insert STIX data to parse for indicators.

### To parse a STIX file for indicators:

The Parse For Intelligence dialog box will load.

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

2. Do one of the following:
  - Drag your file(s) into the left pane.
  - Click on **Click to Browse**, and locate the file you wish to upload.
  - Copy/paste the content in the right pane.
3. Select or clear the **Normalize URL Indicators** check box. See [Indicator URL Normalization](#) for more information.
4. Click **Next Step**.
5. Enter an optional **Name**.
6. Select a **Source** from the dropdown menu provided.



You can also click on **Add a New Source** if the desired source is not listed in the dropdown menu

7. Select any optional **Attributes** to be applied.
8. Optionally, enter a comment.
9. Optionally, use the **Add relationships** search field to add object relationships.
10. Optionally, add any desired **Tags**.



If at any point, you wish to abandon the import, click **Cancel**.

15. Click **Apply**.

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                    |                   |
| Associated_Actors | Adversary              |                   |

| STIX FIELD           | THREATQ FIELD MAPPING | THREATQ NAME |
|----------------------|-----------------------|--------------|
| 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          |                   |
| Confidence        | Indicator.attribute    | Confidence        |

| STIX FIELD          | THREATQ FIELD MAPPING      | THREATQ NAME |
|---------------------|----------------------------|--------------|
| Related_Observables | Indicator.attribute.source |              |
|                     |                            |              |
|                     |                            |              |
| 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 |
| Description | Exploit Target.attribute | Description       |

| STIX FIELD              | THREATQ FIELD MAPPING    | THREATQ NAME                    |
|-------------------------|--------------------------|---------------------------------|
| Short Description       | Exploit Target.attribute | Short Description               |
| Weakness                | Exploit Target.attribute | CWE ID                          |
| Weakness                | Exploit Target.attribute | Weakness Description            |
| Configuration           | Exploit Target.attribute | CCE ID                          |
| Configuration           | Exploit Target.attribute | Configuration Description       |
| Configuration           | Exploit Target.attribute | Configuration Short Description |
| Vulnerability           | Exploit Target.attribute | CVE ID                          |
| Potential_COAs          | Course of Action         |                                 |
| Related_Exploit_Targets | Exploit Target           |                                 |

- [>Observables Mapping](#)

| STIX FIELD | THREATQ FIELD MAPPING | THREATQ NAME      |
|------------|-----------------------|-------------------|
| ID         | Indicator.attribute   | STIX Reference ID |
|            | Indicator.attribute   | Description       |
|            | Indicator.type        | IP Address        |
|            | Indicator.value       |                   |
|            | Indicator.type        | Filename          |
|            | Indicator.value       |                   |

| STIX FIELD | THREATQ FIELD MAPPING | THREATQ NAME  |
|------------|-----------------------|---------------|
|            | Indicator.type        | File Path     |
|            | Indicator.value       |               |
|            | Indicator.attribute   | File Size     |
|            | Indicator.attribute   | File Format   |
|            | Indicator.attribute   | Packer        |
|            | Indicator.type        | MD5           |
|            | Indicator.type        | SHA-256       |
|            | Indicator.type        | SHA-1         |
|            | Indicator.type        | SHA-512       |
|            | Indicator.value       |               |
|            | Indicator.type        | SSDEEP        |
|            | Indicator.value       |               |
|            | Indicator.type        | FQDN          |
|            | Indicator.value       |               |
|            | Indicator.type        | URL           |
|            | Indicator.value       |               |
|            | Indicator.type        | Email Subject |

| STIX FIELD | THREATQ FIELD MAPPING | THREATQ NAME  |
|------------|-----------------------|---------------|
|            | 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      |
|            | Object.Description    |               |
|            | Spearphish.value      |               |
|            | Indicator.type        | Registry Key  |
|            | Indicator.value       |               |

| STIX FIELD | THREATQ FIELD MAPPING | THREATQ NAME |
|------------|-----------------------|--------------|
|------------|-----------------------|--------------|

|                     |      |
|---------------------|------|
| 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 |
|----------|--------------------|----------|

|              |     |
|--------------|-----|
| 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                 |
| 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 |



| STIX FIELD              | THREATQ FIELD MAPPING | THREATQ NAME            |
|-------------------------|-----------------------|-------------------------|
| 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    |
| 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                |

| STIX FIELD               | THREATQ FIELD MAPPING | THREATQ NAME     |
|--------------------------|-----------------------|------------------|
|                          | 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      |                  |
| COA_Taken                | Course of Action      |                  |
| Confidence               | Incident.attribute    | Confidence       |
| Attributed_Threat_Actors | Adversary             |                  |
| Discovery_Method         | Incident.attribute    | Discovery Method |
| Related_Incidents        | Incident              |                  |

- [>TTP Mapping](#)

| STIX FIELD        | THREATQ FIELD MAPPING | THREATQ NAME                     |
|-------------------|-----------------------|----------------------------------|
| Title             | TTP.value             |                                  |
| ID                | TTP.attribute         | STIX Reference ID                |
| Description       | TTP.attribute         | Description                      |
| Handling          | TTP.tlp               |                                  |
| Kill_Chain_Phases | TTP.attribute         | Kill Chain Phase                 |
| Intended_Effect   | TTP.attribute         | Intended Effect                  |
|                   | TTP.attribute         | CAPEC ID                         |
| Behavior          | TTP.attribute         | Attack Pattern                   |
|                   | TTP.attribute         | Attack Pattern Description       |
|                   | TTP.attribute         | Attack Pattern Short Description |
|                   | TTP.attribute         | Malware Type                     |
|                   | 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                          |

| STIX FIELD       | THREATQ FIELD MAPPING | THREATQ NAME                     |
|------------------|-----------------------|----------------------------------|
|                  | TTP.attribute         | Exploit Description              |
|                  | TTP.attribute         | Exploit Short Description        |
| Exploit_Targets  | Exploit Target        |                                  |
| Related_TTPs     | TTP                   |                                  |
| Resources        | TTP.attribute         | Tool                             |
|                  | TTP.attribute         | Tool                             |
|                  | TTP.attribute         | Tool Type                        |
|                  | TTP.attribute         | Tool Description                 |
|                  | TTP.attribute         | Tool Short Description           |
|                  | TTP.attribute         | Infrastructure Type              |
|                  | TTP.attribute         | Infrastructure                   |
|                  | TTP.attribute         | Infrastructure Short Description |
|                  | TTP.attribute         | Infrastructure Description       |
|                  | Indicator             |                                  |
| Victim Targeting | TTP.attribute         | Persona                          |
|                  | TTP.attribute         | Victim Name                      |
|                  | TTP.attribute         | Victim <CIQ Identity Name>       |

| STIX FIELD | THREATQ FIELD MAPPING | THREATQ NAME         |
|------------|-----------------------|----------------------|
|            | TTP.attribute         | Targeted Systems     |
|            | TTP.attribute         | Targeted Information |
|            | Indicator             |                      |

- [>CIQ Identity Mapping](#)

| STIX FIELD        | THREATQ FIELD MAPPING | THREATQ NAME   |
|-------------------|-----------------------|----------------|
| Party Name        | Object.attribute      | Name           |
| Organization Name | Object.attribute      | Organization   |
| Industry Sector   | Object.attribute      | Industry       |
| Nationality       | Object.attribute      | Nationality    |
| Languages         | Object.attribute      | Language       |
| Address           | Object.attribute      | Country        |
| Email Address     | Object.attribute      | E-Mail Address |
| Chat Handle       | Object.attribute      | Chat Handle    |
| Phone             | Object.attribute      | Phone          |

## 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 <a href="#">External References</a> |              |
| kill_chain_phases.[]e        | See <a href="#">Kill Chain Table</a>    |              |
| 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 |
| created        | Adversary.Published_At |                                                                                                                                               |

| STIX 2.0 FIELD                  | THREATQ FIELD MAPPING                   | THREATQ NAME         |
|---------------------------------|-----------------------------------------|----------------------|
| 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<br>(if revoked == true) | Adversary.Attribute                     | Revoked              |
| external_references[]           | See <a href="#">External References</a> |                      |
| personal_motivations            | Adversary.Attribute                     | Personal Motivation  |

- [>Indicators Mapping](#)

| STIX 2.0 FIELD | THREATQ FIELD MAPPING  | THREATQ NAME |
|----------------|------------------------|--------------|
| created        | Signature.Published_at |              |
| description    | Signature.Description  |              |

| STIX 2.0 FIELD               | THREATQ FIELD MAPPING                   | THREATQ NAME                                                                                     |
|------------------------------|-----------------------------------------|--------------------------------------------------------------------------------------------------|
| external_references[]        | See <a href="#">External References</a> |                                                                                                  |
| 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 <a href="#">Kill Chain Table</a>    |                                                                                                  |

ThreatQ Indicator and / or Event objects based on the Observables Mapping may be derived from the `pattern` field and related back to the resulting Signature.

- [>Identities Mapping](#)

| STIX 2.0 FIELD      | THREATQ FIELD MAPPING        | THREATQ NAME |
|---------------------|------------------------------|--------------|
| contact_information | Identity.Contact_Information |              |



| STIX 2.0 FIELD               | THREATQ FIELD MAPPING                   | THREATQ NAME   |
|------------------------------|-----------------------------------------|----------------|
| created                      | Identity.Published_at                   |                |
| description                  | Identity.Description                    |                |
| external_references[]        | See <a href="#">External References</a> |                |
| identity_class               | Identity.Attribute                      | Identity Class |
| modified                     | Identity.Attribute                      | Modified At    |
| name                         | Identity.Value                          |                |
| sectors                      | Identity.Attribute                      | Sector         |
| labels                       | Identity.Attribute                      | Label          |
| revoked (if revoked == true) | Identity.Attribute                      | Revoked        |

- [>Observables Mapping](#)

| STIX 2.0 FIELD               | THREATQ FIELD MAPPING   | THREATQ NAME                                                    |
|------------------------------|-------------------------|-----------------------------------------------------------------|
| created                      | Observable.Published_at |                                                                 |
| modified                     | Observable.Attribute    | Modified At                                                     |
| revoked (if revoked == true) | Observable.Attribute    | Revoked                                                         |
| external_references          | Observable.Attribute    | External Reference<br>See <a href="#">External References</a> . |
| number_observed              | Observable.Attribute    | Number Observed                                                 |

| STIX 2.0 FIELD | THREATQ FIELD MAPPING | THREATQ NAME                                                                                                |
|----------------|-----------------------|-------------------------------------------------------------------------------------------------------------|
| objects[]      |                       | Specifies Cyber Observable Objects representing this observation. See the tables below for parsing details. |

- [➤Artifact Mapping](#)

| STIX 2.0 FIELD | THREATQ FIELD MAPPING  | THREATQ NAME                                           |
|----------------|------------------------|--------------------------------------------------------|
| type: artifact | Indicator.Type         | URL                                                    |
| mime_type      | Indicator.Attribute    | MIME Type                                              |
| url            | Indicator.Value        |                                                        |
| hashes{}       | Indicator.relationship |                                                        |
| hashes{}.key   | Indicator.Type         | MD5 / SHA-1 / SHA-256 / SHA-384 / SHA-512 / Fuzzy Hash |
| hashes{}.value | Indicator.Value        |                                                        |

- [➤Autonomous System Mapping](#)

| STIX 2.0 FIELD          | THREATQ FIELD MAPPING | THREATQ NAME               |
|-------------------------|-----------------------|----------------------------|
| type: autonomous-system | Indicator.Type        | ASN                        |
| number                  | Indicator.Value       |                            |
| 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<br>Indicator.Type                 | Spearphish<br>Email Subject  |
| subject**                                                                | Event.Title<br>Indicator.Value               |                              |
| is_multipart                                                             | Indicator.Attribute                          | Is Multipart                 |
| date (if parsing as an event)*<br>sent date (if parsing as an indicator) | Event.happened_at<br>Indicator.Attribute     |                              |
| content_type                                                             | Indicator.Attribute                          | Content Type                 |
| from_ref                                                                 | Event.Relationship<br>Indicator.Relationship | From                         |
| sender_ref                                                               | Event.Relationship<br>Indicator.Relationship | Sender                       |
| to_refs                                                                  | Event.Relationship<br>Indicator.Relationship | To                           |
| cc_refs                                                                  | Event.Relationship                           | CC                           |
| bcc_refs                                                                 | Event.Relationship<br>Indicator.Relationship | BCC                          |
| received_lines                                                           | Event.Attribute<br>Indicator.Attribute       | Received Lines               |
| additional_header_fields                                                 | Event.Attribute<br>Indicator.Attribute       | Additional Header -<br>{key} |

| STIX 2.0 FIELD                                | THREATQ FIELD MAPPING                                                  | THREATQ NAME                                                                                         |
|-----------------------------------------------|------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
|                                               |                                                                        | An attribute is created for each key-value pair of the <code>additional_header_fields</code> object. |
| <code>body</code>                             | <code>Event.Attribute</code><br><code>Indicator.Attribute</code>       | Body                                                                                                 |
| <code>body_multipart[].body_raw_ref***</code> | Indicator                                                              | Filename                                                                                             |
| <code>raw_email_ref</code>                    | <code>Event.Relationship</code><br><code>Indicator.Relationship</code> |                                                                                                      |

\* To parse an event from an email message, the email must have a **date** and **subject** field.

\*\* To parse an indicator from an email message, the email must contain a **subject** field.

\*\*\* 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 |
|-------------------------|----------------------------------|--------------|
| <code>type: file</code> | <code>Indicator.Type</code>      | Filename     |
| <code>size</code>       | <code>Indicator.Attribute</code> | File Size    |

| STIX 2.0 FIELD       | THREATQ FIELD MAPPING  | THREATQ NAME                                                     |
|----------------------|------------------------|------------------------------------------------------------------|
| hashes{}             |                        |                                                                  |
| hashes{}.key         | Indicator.Type         | MD5 / SHA-1<br>SHA-256 /<br>SHA-384 /<br>SHA-512 /<br>Fuzzy Hash |
| hashes{}.value       | Indicator.Value        |                                                                  |
| name                 | Indicator.Value        |                                                                  |
| name_enc             | Indicator.Attribute    | File Name<br>Encoding                                            |
| magic_number_hex     | Indicator.Attribute    | Magic<br>Number Hex                                              |
| mime_type            | Indicator.Attribute    | MIME Type                                                        |
| created              | Indicator.Attribute    | Created At                                                       |
| accessed             | Indicator.Attribute    | Last Accessed                                                    |
| parent_directory_ref | Indicator.Relationship |                                                                  |
| is_encrypted         | Indicator.Attribute    | Encrypted                                                        |
| encryption_algorithm | Indicator.Attribute    | Encryption<br>Algorithm                                          |
| decryption_key       | Indicator.Attribute    | Decryption<br>Key                                                |

| STIX 2.0 FIELD                                              | THREATQ FIELD MAPPING  | THREATQ NAME                                           |
|-------------------------------------------------------------|------------------------|--------------------------------------------------------|
| contains_refs[]                                             | Indicator.Relationship |                                                        |
| content_ref                                                 | Indicator.Relationship |                                                        |
| extensions.archive-ext.contains_refs[]                      | Indicator.Relationship |                                                        |
| extensions.archive-ext.version                              | Indicator.Attribute    | Archive Version                                        |
| extensions.archive-ext.comment                              | Indicator.Attribute    | Archive File Comment                                   |
| extensions.ntfs-ext.sid                                     | Indicator.Attribute    | Security ID                                            |
| extensions.ntfs-ext.alternate_data_streams[].hashes{}       |                        |                                                        |
| extensions.ntfs-ext.alternate_data_streams[].hashes{}.key   | Indicator.Type         | MD5 / SHA-1 / SHA-256 / SHA-384 / SHA-512 / Fuzzy Hash |
| extensions.ntfs-ext.alternate_data_streams[].hashes{}.value | Indicator.Value        |                                                        |
| extensions.ntfs-ext.alternate_data_streams[].name           | Indicator.Attribute    | Alternate Data Stream Name                             |
| extensions.ntfs-ext.alternate_data_streams[].size           | Indicator.Attribute    | Alternate Data Stream Size                             |
| extensions.pdf-ext.version                                  | Indicator.Attribute    | PDF Specification Version                              |

| STIX 2.0 FIELD                                          | THREATQ FIELD MAPPING | THREATQ NAME                            |
|---------------------------------------------------------|-----------------------|-----------------------------------------|
| extensions.pdf-ext.is_optimized                         | Indicator.Attribute   | PDF Is Optimized                        |
| extensions.pdf-ext.document_info_dict{}.key/value       | Indicator.Attribute   | Formatted as 'PDF {key.title()}'        |
| extensions.pdf-ext.pdfid0                               | Indicator.Attribute   | PDF First File Identifier               |
| extensions.pdf-ext.pdfid1                               | Indicator.Attribute   | PDF Second File Identifier              |
| extensions.raster-image-ext.image_height                | Indicator.Attribute   | Image Height                            |
| extensions.raster-image-ext.image_width                 | Indicator.Attribute   | Image Width                             |
| extensions.raster-image-ext.bits_per_pixel              | Indicator.Attribute   | Image Bits Per Pixel                    |
| extensions.raster-image-ext.image_compression_algorithm | Indicator.Attribute   | Image Compression Algorithm             |
| extensions.raster-image-ext.exif_tags{}.key/value       | Indicator.Attribute   | Formatted as 'Image EXIF {key.title()}' |
| extensions.windows-pebinary-ext.pe_type                 | Indicator.Attribute   | Executable Extension Type               |
| extensions.windows-pebinary-ext.imphash                 | Indicator.Attribute   | Executable Imphash                      |



| STIX 2.0 FIELD                                              | THREATQ FIELD MAPPING | THREATQ NAME                                           |
|-------------------------------------------------------------|-----------------------|--------------------------------------------------------|
| extensions.windows-pebinary-ext.machine_hex                 | Indicator.Attribute   | Target Machine Hex                                     |
| extensions.windows-pebinary-ext.number_of_sections          | Indicator.Attribute   | PE Binary Section Count                                |
| extensions.windows-pebinary-ext.time_date_stamp             | Indicator.Attribute   | PE Binary Created Date                                 |
| extensions.windows-pebinary-ext.pointer_to_symbol_table_hex | Indicator.Attribute   | Symbol Table Hex Offset                                |
| extensions.windows-pebinary-ext.number_of_symbols           | Indicator.Attribute   | PE Binary Symbol Table Size                            |
| extensions.windows-pebinary-ext.size_of_optional_header     | Indicator.Attribute   | PE Binary Optional Header Size                         |
| extensions.windows-pebinary-ext.characteristics_hex         | Indicator.Attribute   | PE Binary Characteristic 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       |                                                        |

| STIX 2.0 FIELD                                                             | THREATQ FIELD MAPPING | THREATQ NAME                         |
|----------------------------------------------------------------------------|-----------------------|--------------------------------------|
| extensions.windows-pebinary-ext.optional_header.magic_hex                  | Indicator.Attribute   | PE Binary Magic Hex                  |
| extensions.windows-pebinary-ext.optional_header.major_linker_version       | Indicator.Attribute   | PE Binary Major Linker Version       |
| extensions.windows-pebinary-ext.optional_header.minor_linker_version       | Indicator.Attribute   | PE Binary Minor Linker Version       |
| extensions.windows-pebinary-ext.optional_header.size_of_code               | Indicator.Attribute   | PE Binary Code Size                  |
| extensions.windows-pebinary-ext.optional_header.size_of_initialized_data   | Indicator.Attribute   | PE Binary Initialized Data Size      |
| extensions.windows-pebinary-ext.optional_header.size_of_uninitialized_data | Indicator.Attribute   | PE Binary Uninitialized Data Size    |
| extensions.windows-pebinary-ext.optional_header.address_of_entry_point     | Indicator.Attribute   | PE Binary Memory Address Entry Point |
| 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   |

| STIX 2.0 FIELD                                                          | THREATQ FIELD MAPPING | THREATQ NAME                         |
|-------------------------------------------------------------------------|-----------------------|--------------------------------------|
| extensions.windows-pebinary-ext.optional_header.image_base              | Indicator.Attribute   | PE Binary Base Image Memory Address  |
| extensions.windows-pebinary-ext.optional_header.section_alignment       | Indicator.Attribute   | PE Binary Section Alignment Bytes    |
| extensions.windows-pebinary-ext.optional_header.file_alignment          | Indicator.Attribute   | PE Binary Image File Alignment Bytes |
| extensions.windows-pebinary-ext.optional_header.major_os_version        | Indicator.Attribute   | Windows OS Major Version             |
| extensions.windows-pebinary-ext.optional_header.minor_os_version        | Indicator.Attribute   | Windows OS Minor Version             |
| extensions.windows-pebinary-ext.optional_header.major_image_version     | Indicator.Attribute   | Image Major Version                  |
| extensions.windows-pebinary-ext.optional_header.minor_image_version     | Indicator.Attribute   | Image Minor Version                  |
| extensions.windows-pebinary-ext.optional_header.major_subsystem_version | Indicator.Attribute   | Subsystem Major Version              |
| extensions.windows-pebinary-ext.optional_header.minor_subsystem_version | Indicator.Attribute   | Subsystem Minor Version              |
| extensions.windows-pebinary-ext.optional_header.win32_version_value_hex | Indicator.Attribute   | Win32 Version Hex                    |

| STIX 2.0 FIELD                                                          | THREATQ FIELD MAPPING | THREATQ NAME                     |
|-------------------------------------------------------------------------|-----------------------|----------------------------------|
| extensions.windows-pebinary-ext.optional_header.size_of_image           | Indicator.Attribute   | Image Byte Size                  |
| extensions.windows-pebinary-ext.optional_header.size_of_headers         | Indicator.Attribute   | PE Binary Combined Header Size   |
| extensions.windows-pebinary-ext.optional_header.checksum_hex            | Indicator.Attribute   | PE Binary Checksum Hex           |
| extensions.windows-pebinary-ext.optional_header.subsystem_hex           | Indicator.Attribute   | PE Binary Required Subsystem Hex |
| extensions.windows-pebinary-ext.optional_header.dll_characteristics_hex | Indicator.Attribute   | DLL Characteristics Hex          |
| extensions.windows-pebinary-ext.optional_header.size_of_stack_reserve   | Indicator.Attribute   | Reserved Stack Size              |
| extensions.windows-pebinary-ext.optional_header.size_of_stack_commit    | Indicator.Attribute   | Stack Commit Size                |
| extensions.windows-pebinary-ext.optional_header.size_of_heap_reserve    | Indicator.Attribute   | Heap Space Reserve Size          |
| extensions.windows-pebinary-ext.optional_header.size_of_heap_commit     | Indicator.Attribute   | Heap Space Commit Size           |
| extensions.windows-pebinary-ext.optional_header.loader_flags_hex        | Indicator.Attribute   | Loader Flags Hex                 |

| STIX 2.0 FIELD                                                          | THREATQ FIELD MAPPING | THREATQ NAME                                                     |
|-------------------------------------------------------------------------|-----------------------|------------------------------------------------------------------|
| extensions.windows-pebinary-ext.optional_header.number_of_rva_and_sizes | Indicator.Attribute   | Number of RVA and Size                                           |
| extensions.windows-pebinary-ext.optional_header.hashes{}                |                       |                                                                  |
| extensions.windows-pebinary-ext.optional_header.hashes{}.key            | Indicator.Type        | MD5 / SHA-1<br>SHA-256 /<br>SHA-384 /<br>SHA-512 /<br>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<br>SHA-256 /<br>SHA-384 /<br>SHA-512 /<br>Fuzzy Hash |
| extensions.windows-pebinary-ext.sections[].hashes{}.value               | Indicator.Value       |                                                                  |
| extensions.windows-pebinary-ext.sections[].name                         | Indicator.Attribute   | PE Binary Section Name                                           |
| extensions.windows-pebinary-ext.sections[].size                         | Indicator.Attribute   | PE Binary Section Size                                           |
| extensions.windows-pebinary-ext.sections[].entropy                      | Indicator.Attribute   | PE Binary Section Entropy                                        |

- [IPv4 Mapping](#)

| STIX 2.0 FIELD     | THREATQ FIELD MAPPING  | THREATQ NAME                                                                                                                                              |
|--------------------|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| type: ipv4-addr    | Indicator.Type         | CIDR Block (if value contains a / and does not end with /32)<br>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             |
| account_created    | Indicator.Attribute   | Account Created         |

| STIX 2.0 FIELD                       | THREATQ FIELD MAPPING | THREATQ NAME           |
|--------------------------------------|-----------------------|------------------------|
| account_expires                      | Indicator.Attribute   | Account Expires        |
| password_last_changed                | Indicator.Attribute   | Password Last Changed  |
| account_first_login                  | Indicator.Attribute   | Account First Login    |
| account_last_login                   | Indicator.Attribute   | Account Last Login     |
| extensions.unix-account-ext.gid      | Indicator.Attribute   | Account Group ID       |
| extensions.unix-account-ext.groups[] | Indicator.Attribute   | Account Group          |
| extensions.unix-account-ext.home_dir | Indicator.Attribute   | Account Home Directory |
| extensions.unix-account-ext.shell    | Indicator.Attribute   | Account Command Shell  |

- [Windows Registry Key Mapping](#)

| STIX 2.0 FIELD             | THREATQ FIELD MAPPING  | THREATQ NAME         |
|----------------------------|------------------------|----------------------|
| type: windows-registry-key | Indicator.Type         | Registry Key         |
| key                        | Indicator.Value        |                      |
| values[].name              | Indicator.Attribute    | Registry Name        |
| modified                   | Indicator.Attribute    | Registry Modified At |
| creator_user_ref           | Indicator.Relationship |                      |



- [>Campaigns Mapping](#)

| STIX 2.0 FIELD               | THREATQ FIELD MAPPING                   | THREATQ NAME |
|------------------------------|-----------------------------------------|--------------|
| aliases                      | Campaign                                |              |
| created                      | Campaign.Published_at                   |              |
| description                  | Campaign.Description                    |              |
| first_seen                   | Campaign.Started_at                     |              |
| last_seen                    | Campaign.Ended_at                       |              |
| modified                     | Campaign.Attribute                      | Modified At  |
| name                         | Campaign.Value                          |              |
| objective                    | Campaign.Objective                      |              |
| revoked (if revoked == true) | Campaign.Attribute                      | Revoked      |
| external_references[]        | See <a href="#">External References</a> |              |
| 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  |              |

| STIX 2.0 FIELD               | THREATQ FIELD MAPPING                   | THREATQ NAME |
|------------------------------|-----------------------------------------|--------------|
| action                       |                                         |              |
| revoked (if revoked == true) | Course of Action.Attribute              | Revoked      |
| external_references[]        | See <a href="#">External References</a> |              |
| labels                       | Course of Action.Attribute              | Label        |

- [➤Intrusion Sets Mapping](#)

| STIX 2.0 FIELD        | THREATQ FIELD MAPPING                   | THREATQ NAME         |
|-----------------------|-----------------------------------------|----------------------|
| aliases               | Intrusion Set                           |                      |
| created               | Intrusion Set.Published_at              |                      |
| description           | Intrusion Set.Description               |                      |
| first_seen            |                                         |                      |
| goals                 | Intrusion Set.Attribute                 | Goal                 |
| modified              | Intrusion Set.Attribute                 | Modified At          |
| name                  | Intrusion Set.Value                     |                      |
| primary_motivation    | Intrusion Set.Attribute                 | Primary Motivation   |
| resource_level        | Intrusion Set.Attribute                 | Resource Level       |
| secondary_motivations | Intrusion Set.Attribute                 | Secondary Motivation |
| external_references[] | See <a href="#">External References</a> |                      |

## STIX 2.0 FIELD

## THREATQ FIELD MAPPING

## THREATQ NAME

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

| STIX 2.0 FIELD        | THREATQ FIELD MAPPING                   | THREATQ NAME |
|-----------------------|-----------------------------------------|--------------|
| external_references[] | See <a href="#">External References</a> |              |
| description           | Tool.Description                        |              |
| kill_chain_phases.[]  | See <a href="#">Kill Chain Table</a>    |              |
| tool_version          | Tool.Attribute                          | Tool Version |

- [>Reports Mapping](#)

| STIX 2.0 FIELD               | THREATQ FIELD MAPPING                   | THREATQ NAME |
|------------------------------|-----------------------------------------|--------------|
| created                      | Report.Published_at                     |              |
| modified                     | Report.Attribute                        | Modified At  |
| name                         | Report.Value                            |              |
| description                  | Report.Description                      |              |
| labels                       | Report.Attribute                        | Label        |
| object_refs                  | Report.Relationship.Link                |              |
| external_references[]        | See <a href="#">External References</a> |              |
| 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    |              |

| STIX 2.0 FIELD               | THREATQ FIELD MAPPING                   | THREATQ NAME  |
|------------------------------|-----------------------------------------|---------------|
| 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 <a href="#">External References</a> |               |
| 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* |

| STIX 2.0 FIELD                           | THREATQ FIELD MAPPING | THREATQ NAME        |
|------------------------------------------|-----------------------|---------------------|
| 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 Indicators, Events, Adversaries, Signatures, and Files. You can also add comments, change the task priority, change the task status, and delete the task.

## Assigning a Task

Complete the following steps to assign a task in ThreatQ.

1. From the main menu, choose **Create > Task**.



The Add Task dialog box opens.

2. Enter a task **Name**.
3. Enter the assignee's email address in the **Assigned To** field.
4. Optionally, use the date picker to select a **Due Date**.
5. Select one of the following statuses:
  - To Do
  - In Progress
  - Review
  - Done
6. Select one of the following task priorities:
  - Low
  - Medium
  - High
7. Optionally, enter any **Associated Objects**.
8. Enter a **Description** for the task.
9. Click **Save**.

## Managing Tasks

After a task is created, you can manage it on the task's Details page.

The following table describes the actions you can take to manage your tasks on a Task Details page.

| TO                                                   | YOU CAN...                                                      |
|------------------------------------------------------|-----------------------------------------------------------------|
| Change task priority                                 | Choose the <b>Priority</b> drop-down and select a new priority. |
| Change task status                                   | Choose the <b>Status</b> drop-down and select a new status.     |
| Add Attributes, Comments, Relationships, and Sources | Choose the <b>Add Context</b> drop-down and select an item.     |
| View and Add Comments                                | Choose <b>Comments</b> .                                        |
| View the Audit Log                                   | Choose <b>Audit Log</b> .                                       |



# 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.

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 ThreatQ Threat Library view and configure which data columns will be displayed in your search results.

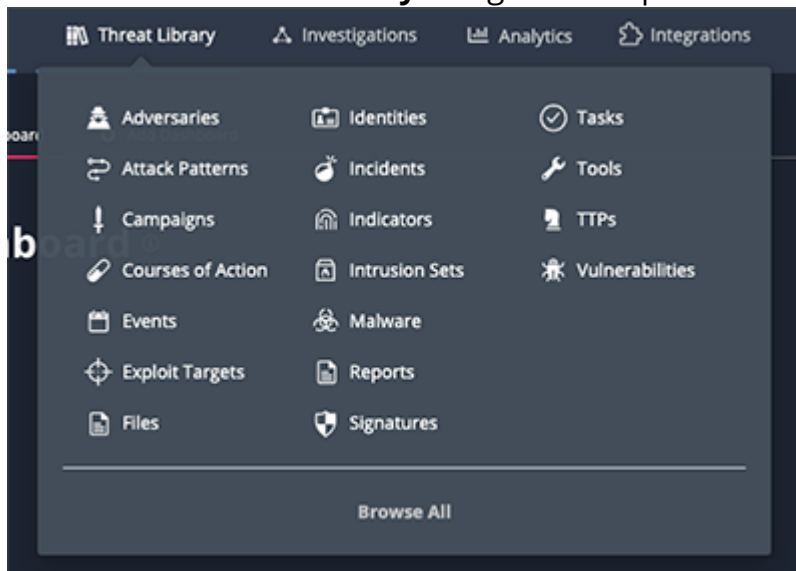
## Selecting Object Type View

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**.

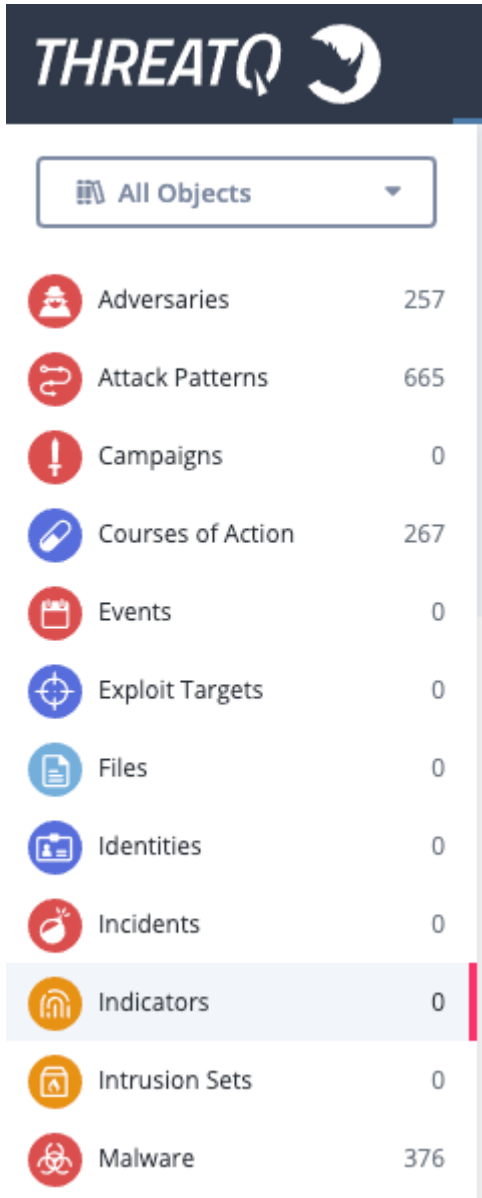


The Advanced Results page opens with the applied object type filter.

### 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.



## Managing Library Columns

You can choose which columns to display in your Threat Library view.

To select columns:

1. Navigate to the Threat Library page.

## 2. Choose **Manage Columns**.

The screenshot shows the ThreatQ Threat Library interface. On the left is a sidebar with various object types and their counts: Adversaries (257), Attack Patterns (665), Campaigns (0), Courses of Action (267), Events (0), Exploit Targets (0), Files (0), Identities (0), Incidents (0), Indicators (0), Intrusion Sets (0), Malware (376), Reports (0), Signatures (0), and Tasks (0). The main panel is titled 'Threat Library' and contains a search bar, filter settings (Filter Set 1: NOT), and a table of Attack Patterns. The table has columns for VALUE, DATE CREATED, LAST MODIFIED, and TAGS. A 'Manage Columns' dropdown menu is open, showing a search bar and a list of columns to be managed: Date Created, Description, Last Modified, Related Adversaries, Sources, Tags, and Attributes. The table lists several attack patterns, including T1069-003 - Cloud Groups, T1172 - Domain Fronting, T1022 - Data Encrypted, T1192 - Spearphishing Link, T1132-001 - Standard Encoding, T1553 - Subvert Trust Controls, and T1133 - External Remote Services.

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

## 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: indicators, events, adversaries, files, signatures, and so on. The search capability looks at high level aspects of each object, including:

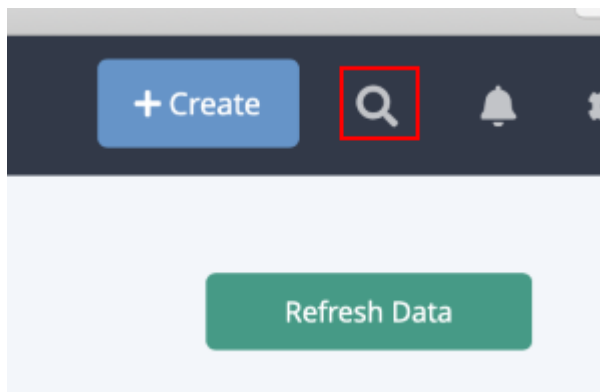
- Indicators (network or host)
- Attachment titles, hashes, keywords
- Attributes
- Adversary name
- Event title

If searching for google.com, the following indicators will also be returned:

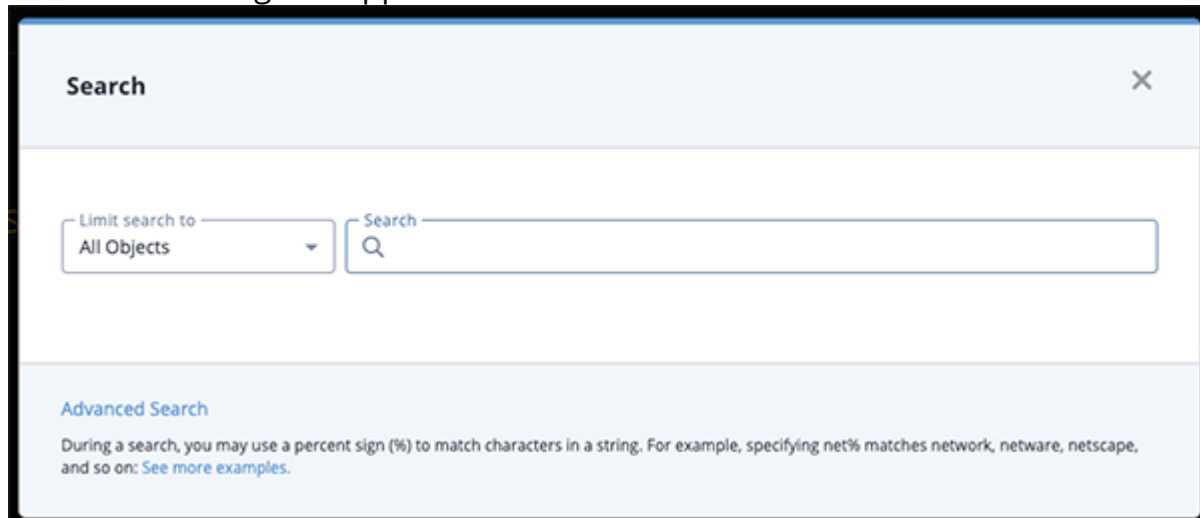
- [www.google.com](http://www.google.com) (FQDN)
- [analytic.google.com](http://analytic.google.com) (FQDN)
- [www.google.com/analytic](http://www.google.com/analytic) (URL)
- [analytic@google.com](mailto:analytic@google.com) (email address)

## Performing a Basic Search

1. Choose the Search icon.

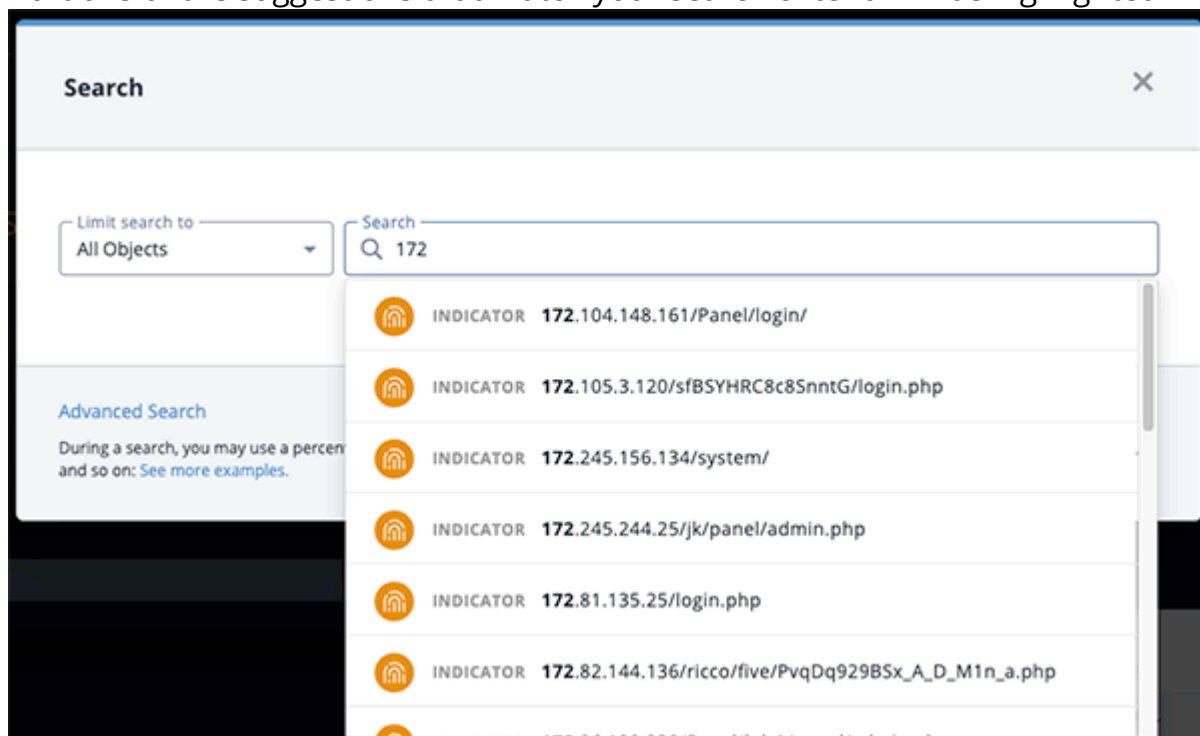


The Search dialog box appears.



2. Use the **Limit Search** dropdown to filter your search to a specific object type.
3. Enter the search criteria.

The Search field provides type ahead suggestions, if any, based on what you have typed. Portions of the suggestions that match your search criteria will be highlighted in bold.



4. Select the desired result.
  - If you do not retrieve any search results, we recommend trying the [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:

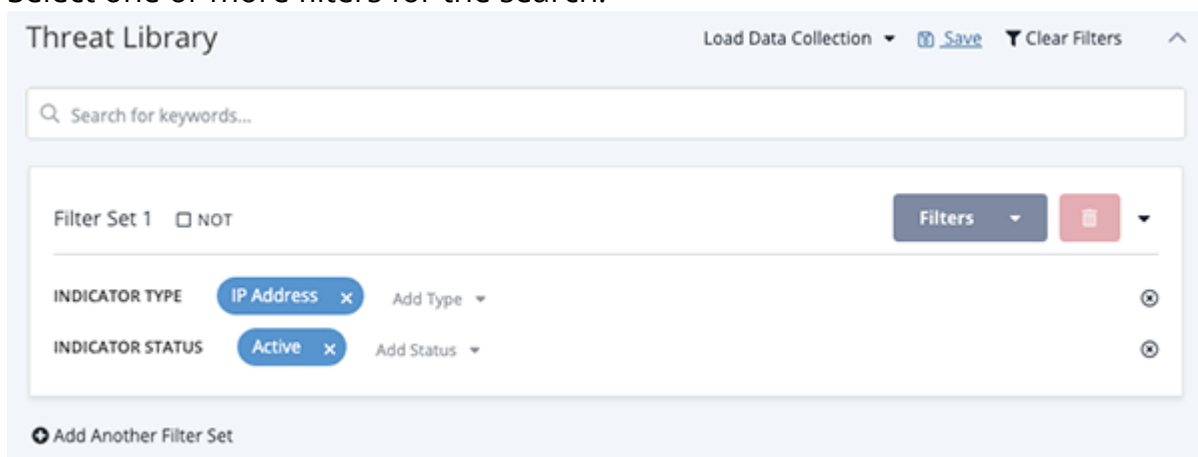
| SEARCH QUERY | DESCRIPTION                                                                               |
|--------------|-------------------------------------------------------------------------------------------|
| % panda      | Finds any adversaries and indicators with <name> panda                                    |
| %ear         | Finds any character string that ends with "ear," such as bear                             |
| %panda%      | Finds any character string that has panda in any position                                 |
| panda%       | Finds any character string that begins with panda                                         |
| pan%a        | Finds any character string that has pan in the first three positions and ends with an "a" |

# 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.

The screenshot shows the 'Threat Library' interface. At the top, there's a search bar labeled 'Search for keywords...'. Below it, a section titled 'Filter Set 1' contains a 'NOT' checkbox and a 'Filters' dropdown menu. Two filters are currently selected: 'INDICATOR TYPE' with the value 'IP Address' and 'INDICATOR STATUS' with the value 'Active'. Each filter has an 'Add' button and a removal 'x' icon. At the bottom of the filter set, there is a button labeled 'Add Another Filter Set'.

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.

Threat Library Load Data Collection Save Clear Filters

Search for keywords...

Filter Set 1 ☐ NOT Filters

INDICATOR TYPE IP Address Add Type

INDICATOR STATUS Active Add Status

Filter Set 2 OR ☐ NOT Filters

+ Add Another Filter 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.

Threat Library Load Data Collection Save Clear Filters

Search for keywords...

Filter Set 1 ☐ NOT Filters

INDICATOR TYPE IP Address Add Type

INDICATOR STATUS Active Add Status

Filter Set 2 OR ☐ NOT Filters

+ Add Another Filter Set

Indicators (22,683)

Type  Status  Score  Expiration Date

| VALUE                      | TYPE       | DATE CREATED | STATUS |
|----------------------------|------------|--------------|--------|
| <span>223.96.91.105</span> | IP Address | 12/16/2019   | Active |

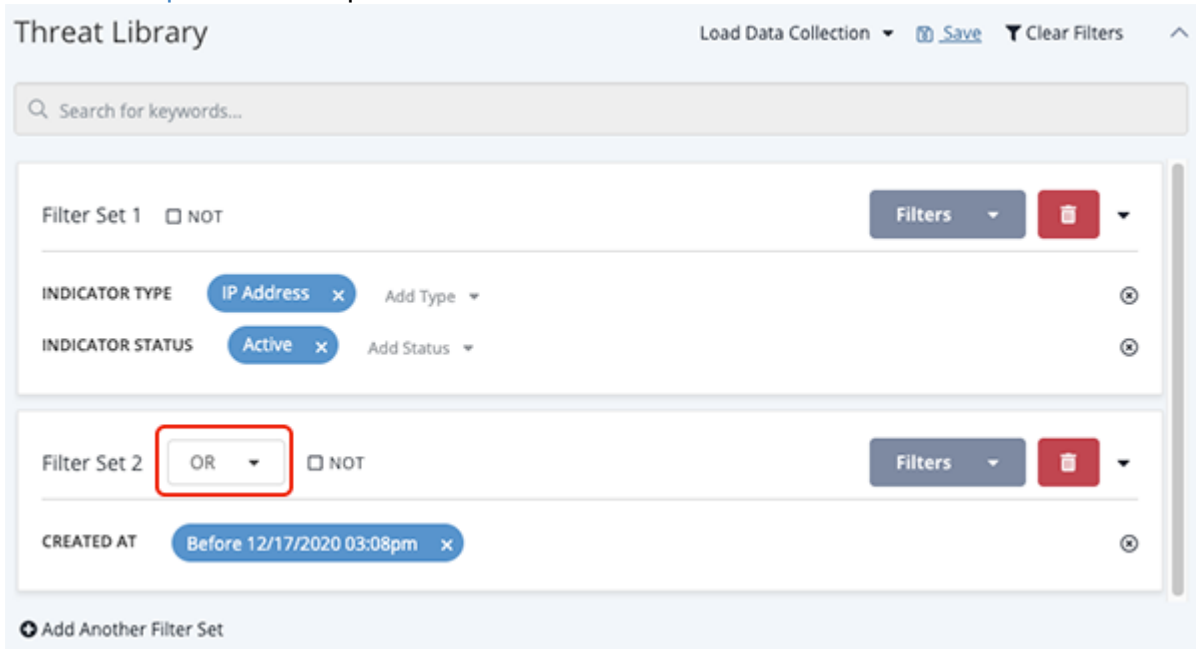
Search...

Dates

- Date Created
- Expiration Date
- Published Date
- Source Ingest Time

Actions

- 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.



Threat Library

Load Data Collection ▾ Save Clear Filters ^

Search for keywords...

Filter Set 1 ☐ NOT Filters ▾ 🗑️ ▾

INDICATOR TYPE IP Address x Add Type ▾ ⊗

INDICATOR STATUS Active x Add Status ▾ ⊗

Filter Set 2 OR ▾ ☐ NOT Filters ▾ 🗑️ ▾

CREATED AT Before 12/17/2020 03:08pm x ⊗

+ Add Another Filter Set



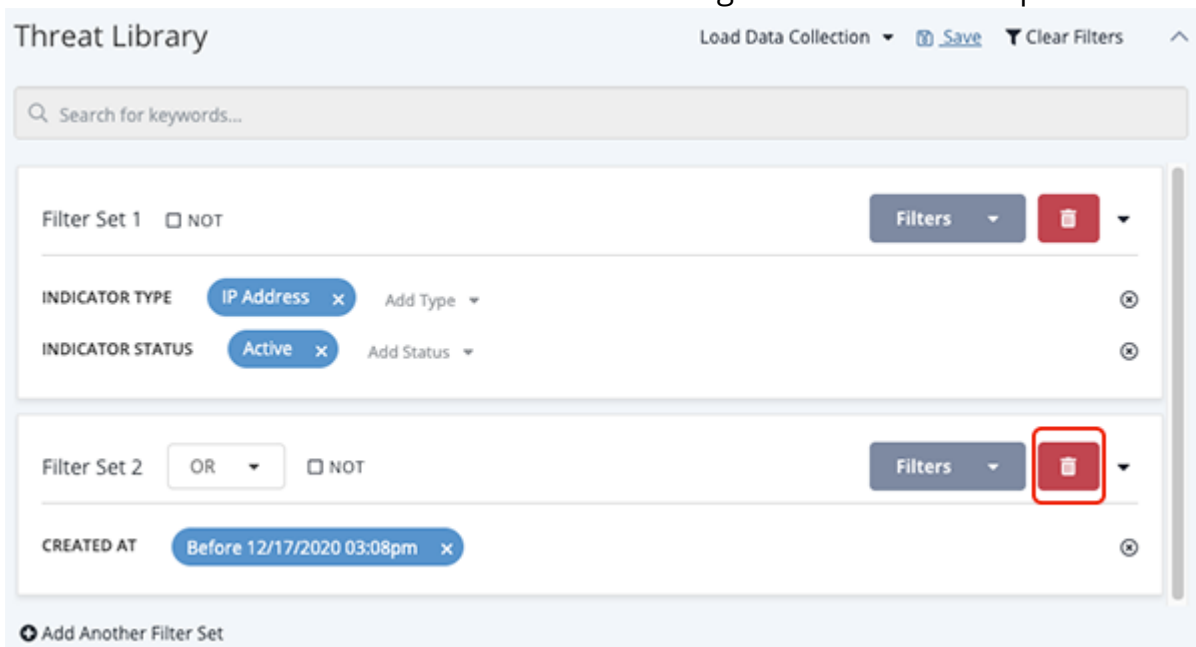
Repeat steps 3-6 to add additional filter sets.

## Deleting Filter Sets



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

- Click on the delete 🗑️ icon located next to the right of the Filters dropdown.



Threat Library

Load Data Collection ▾ Save Clear Filters ^

Search for keywords...

Filter Set 1 ☐ NOT Filters ▾ 🗑️ ▾

INDICATOR TYPE IP Address x Add Type ▾ ⊗

INDICATOR STATUS Active x Add Status ▾ ⊗

Filter Set 2 OR ▾ ☐ NOT Filters ▾ 🗑️ ▾

CREATED AT Before 12/17/2020 03:08pm x ⊗

+ Add Another Filter Set



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                              |    |
| Single OR                   | Filter 1 OR Filter 2                               |    |
| Single AND, Single OR       | (Filter 1 AND Filter 2) OR Filter 3                |   |
| Multiple ANDs, Single OR    | (Filter 1 AND Filter 2 AND Filter 3) OR Filter 4   |  |
| Multiple ANDs, Multiple ORs | (Filter 1 AND Filter 2) OR (Filter 3 AND Filter 4) |  |

# Context Filters

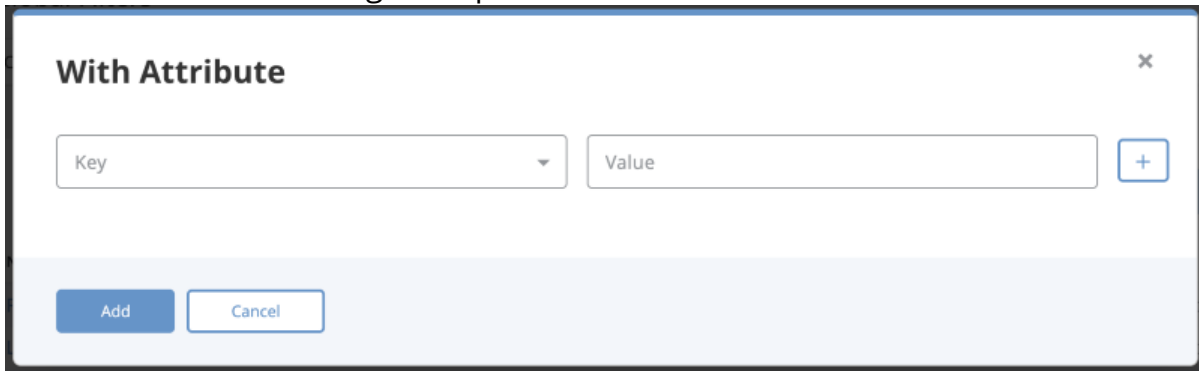
Context filters allow you to filter advanced search results by specific details associated with an object.

## Filtering by Attribute

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

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

The Attribute Filter dialog box opens.

The image shows a dialog box titled "With Attribute" with a close button (X) in the top right corner. Inside the dialog, there is a "Key" dropdown menu, a "Value" text input field, and a plus icon (+) to the right of the input field. At the bottom of the dialog, there are two buttons: "Add" and "Cancel".

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



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

4. Click on the **Add** button.

The filters will be applied to the search results.

The following section applies to using multiple attribute filters.

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

**Example:**

**ANY - Match Toggle Selection**

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

**ALL - Match Toggle Selection**

| Setting               | Field                                                                                                              | Value        |
|-----------------------|--------------------------------------------------------------------------------------------------------------------|--------------|
| <b>Filter A</b>       | Attribute Type                                                                                                     | Attack Phase |
|                       | Attribute Value                                                                                                    | C2           |
| <b>Filter B</b>       | Attribute Type                                                                                                     | Severity     |
|                       | Attribute Value                                                                                                    | High         |
| <b>Filter Options</b> | Any/All Toggle                                                                                                     | All          |
| <b>Result</b>         | Search Results are filtered to include/exclude objects with Attack Phase: C2 <b>AND</b> 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 **Without 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**.

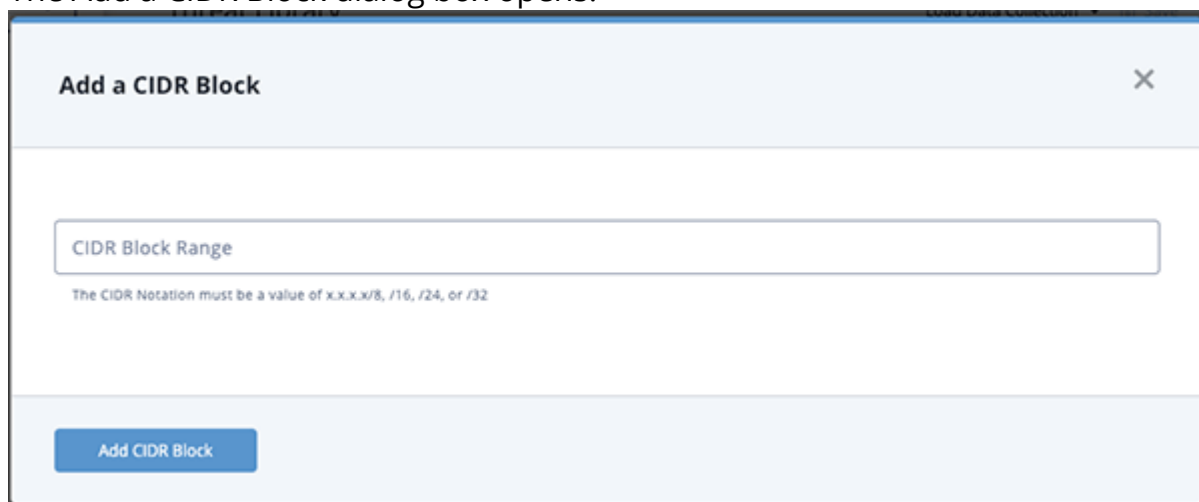
*The filtered results will display any indicator that has both of those attributes*

## 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 on the **Filters** option and select **CIDR block range**.

The Add a CIDR Block dialog box opens.



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.

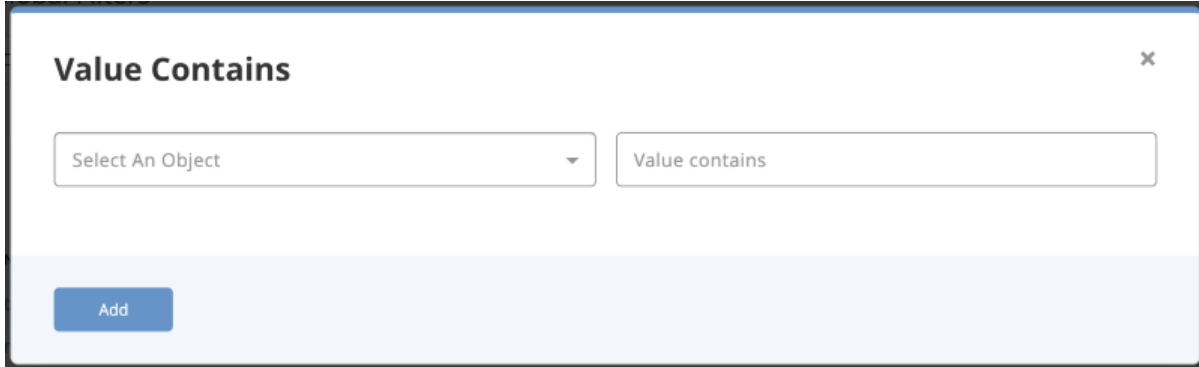


## Filtering by Value Contains

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

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

The Contains dialog box opens.



The dialog box titled "Value Contains" has a close button (X) in the top right corner. It contains two input fields: "Select An Object" with a dropdown arrow and "Value contains". At the bottom left is a blue "Add" button.

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

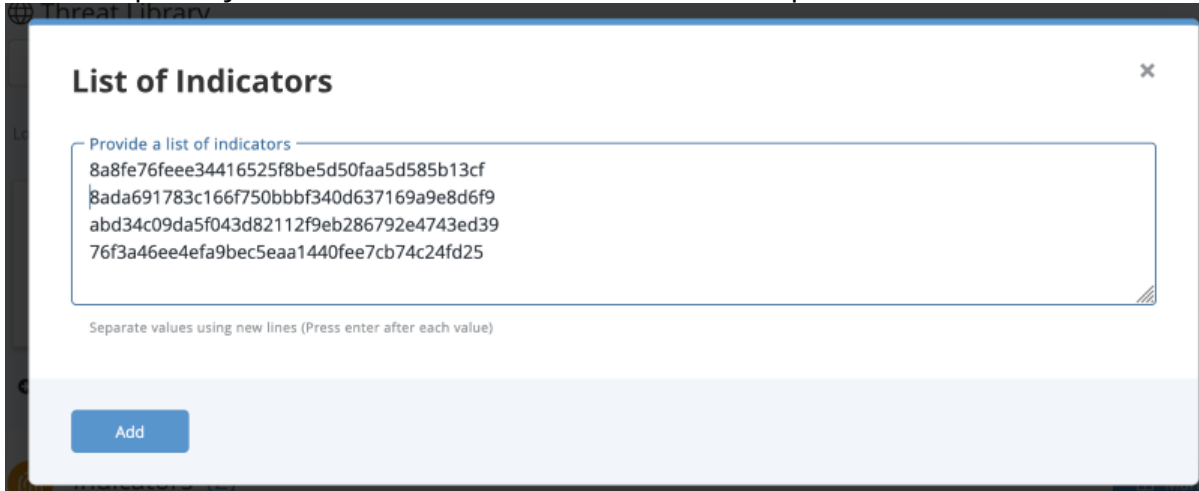
The screenshot shows the Threat Library interface. At the top, there's a search bar and a 'Filters' dropdown menu. The 'Filters' menu is open, showing options like 'Date Created', 'Published Date', 'Source Ingest Time', 'Last Modified', 'Context', 'Import ID', 'Keyword', 'List of Indicators' (highlighted), 'Relationship', and 'Indicator Score'. Below the menu, there's a table of indicators with columns for VALUE, TYPE, and DATE CREATED. The table contains three rows of SHA-1 hashes.

| VALUE                                    | TYPE  | DATE CREATED       |
|------------------------------------------|-------|--------------------|
| 8a8fe76fee34416525f8be5d50faa5d585b13cf  | SHA-1 | 12/09/2019 06:18pm |
| 8ada691783c166f750bbbf340d637169a9e8d6f9 | SHA-1 | 12/09/2019 06:18pm |
| 46ffef697f4021093660586dbdfc0087a0489571 | SHA-1 | 12/09/2019 06:18pm |

The List of Indicators dialog box opens.

The 'List of Indicators' dialog box is shown. It has a title bar with a close button. Inside, there's a text area with the placeholder 'Provide a list of indicators'. Below the text area, there's a note: 'Separate values using new lines (Press enter after each value)'. At the bottom, there's an 'Add' button.

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



The accepted list format is one indicator per line.

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

## Filtering by Keyword

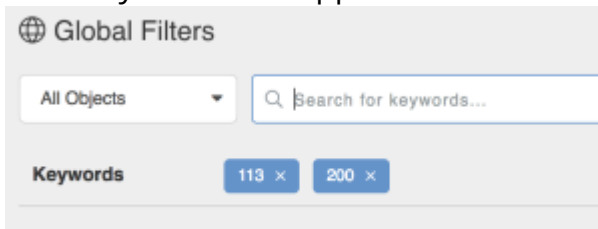
You can filter the Threat Library items on the Advanced Search by keyword.

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



Repeat Step 2 to apply multiple keyword filters

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



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

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

- Source Names
- Attribute Names
- Attribute Values

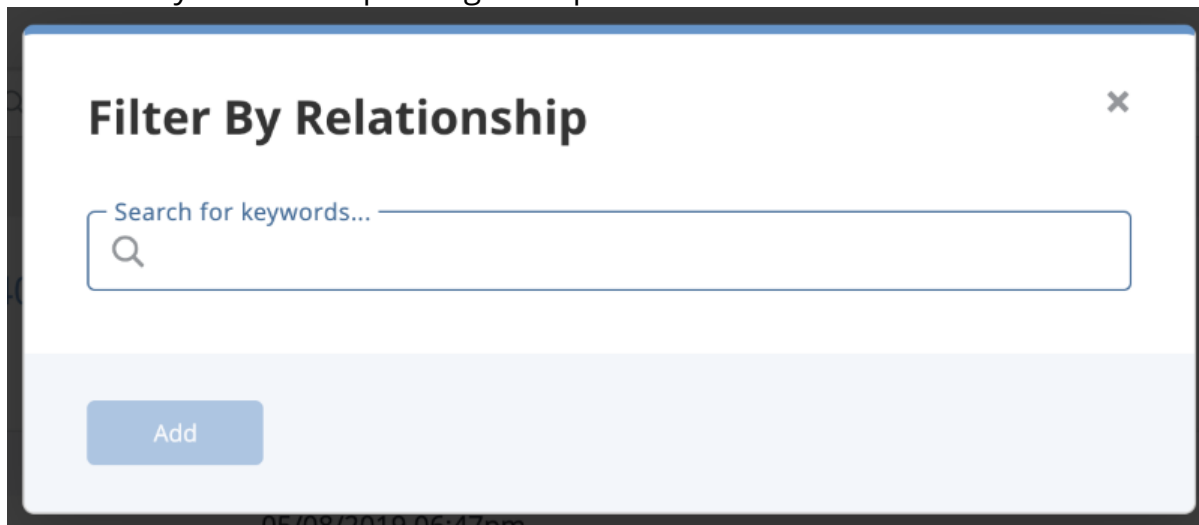
- Comments
- Tags
- Adversary Name
- Adversary Description
- File/Attachment Name
- File/Attachment Title
- File/Attachment Type Name
- File/Attachment Content-Type Name
- File/Attachment Hash
- File/Attachment Description
- File/Attachment Contents
- Event Title
- Event Type Name
- Event Description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

## Filtering by 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 on the **Filters** option and select **Relationship**.

The Filter by Relationship dialog box opens.



2. Use the textbox provided to select an object.
3. Click on **Add** to apply the filter.



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

### Examples:

#### ANY - Match Toggle Selection

| Setting | Related Object |
|---------|----------------|
|---------|----------------|

|                      |                                                                                                      |
|----------------------|------------------------------------------------------------------------------------------------------|
| <b>Filter A</b>      | ABC Indicator                                                                                        |
| <b>Filter B</b>      | DEF Event                                                                                            |
| <b>Filter Option</b> | Any                                                                                                  |
| <b>Result</b>        | Search Results are filtered to include objects related to the ABC Indicator <b>OR</b> the DEF Event. |

### ALL - Match Toggle Selection

|                      |                                                                                                       |
|----------------------|-------------------------------------------------------------------------------------------------------|
| <b>Setting</b>       | Related Object                                                                                        |
| <b>Filter A</b>      | ABC Indicator                                                                                         |
| <b>Filter B</b>      | DEF Event                                                                                             |
| <b>Filter Option</b> | All                                                                                                   |
| <b>Result</b>        | Search Results are filtered to include objects related to the ABC Indicator <b>AND</b> the DEF Event. |

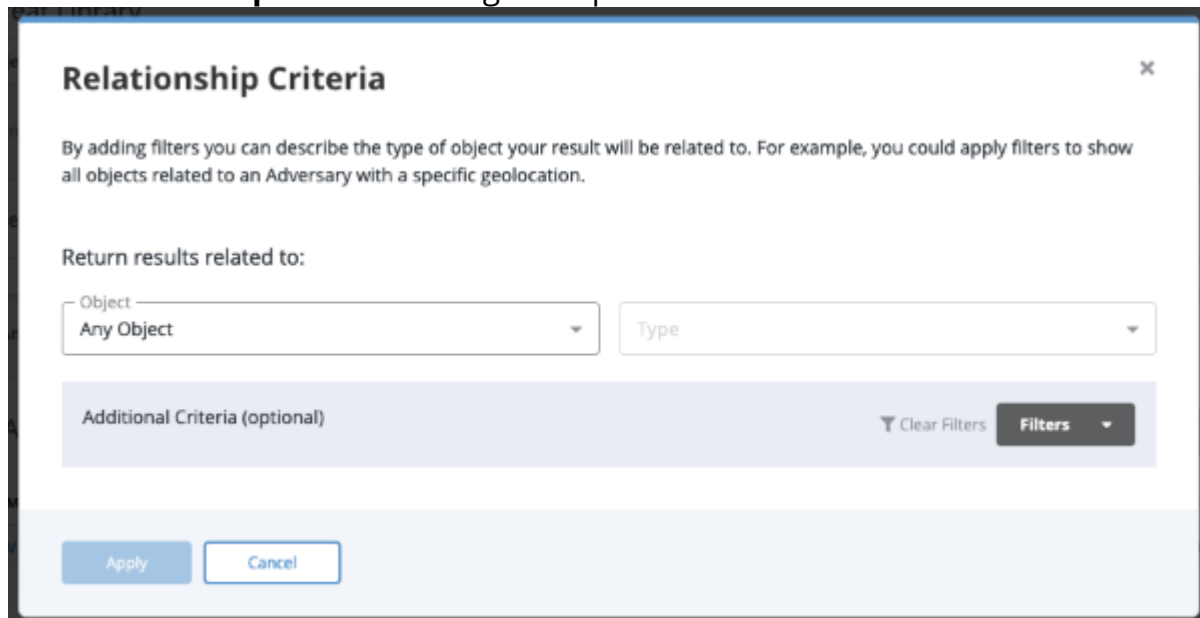
## Filtering by Related Object Type

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

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

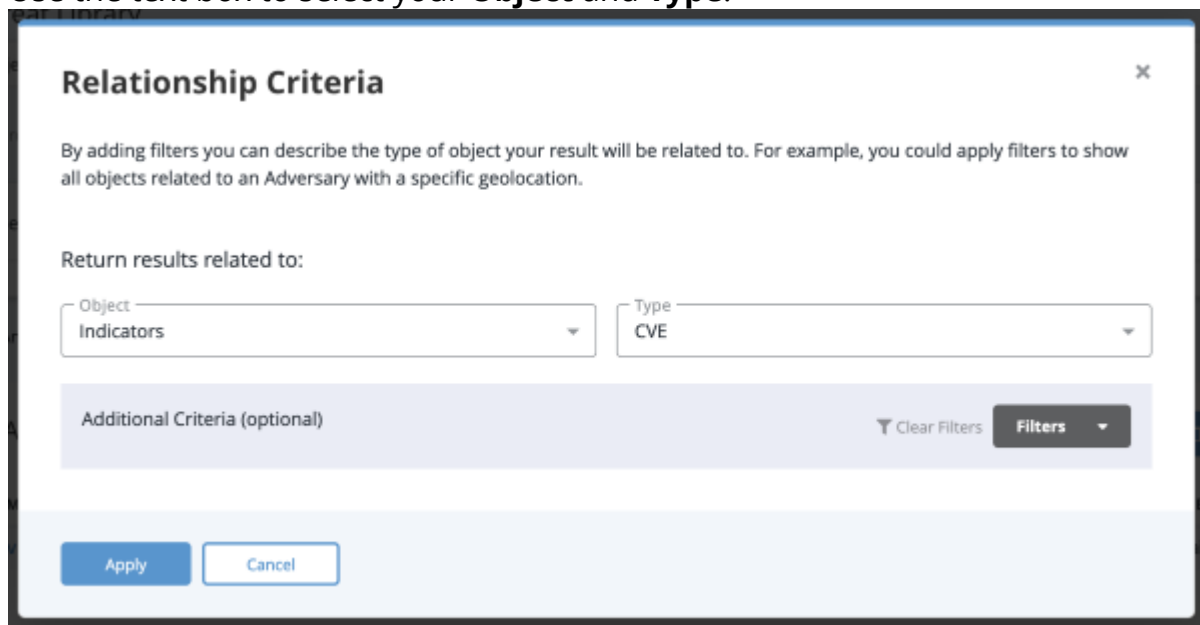
1. Click on the **Filters** option and select **Relationship Criteria**.

The **Relationship Criteria** dialog box opens.



The screenshot shows the 'Relationship Criteria' dialog box. At the top, it says 'By adding filters you can describe the type of object your result will be related to. For example, you could apply filters to show all objects related to an Adversary with a specific geolocation.' Below this, under 'Return results related to:', there are two dropdown menus. The first is labeled 'Object' and has 'Any Object' selected. The second is labeled 'Type' and is empty. Below these is a light blue section labeled 'Additional Criteria (optional)' which contains a 'Clear Filters' button and a 'Filters' dropdown. At the bottom are 'Apply' and 'Cancel' buttons.

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

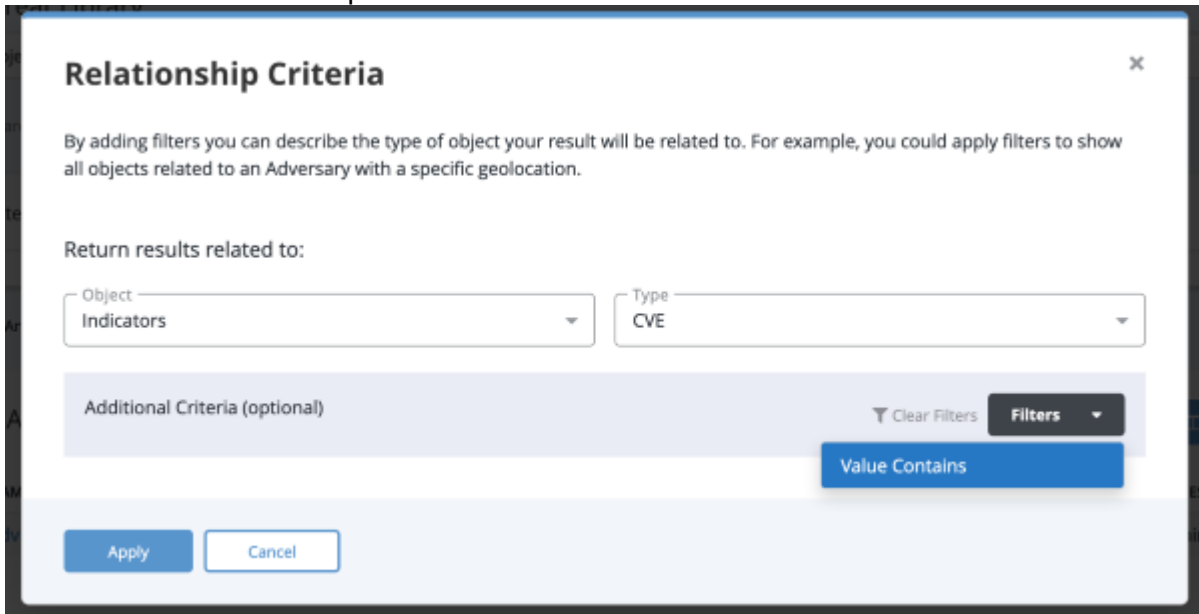


This screenshot is identical to the previous one, but the 'Object' dropdown now shows 'Indicators' and the 'Type' dropdown now shows 'CVE'.



Steps 3-4 are optional.

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



**Relationship Criteria** ✕

By adding filters you can describe the type of object your result will be related to. For example, you could apply filters to show all objects related to an Adversary with a specific geolocation.

Return results related to:

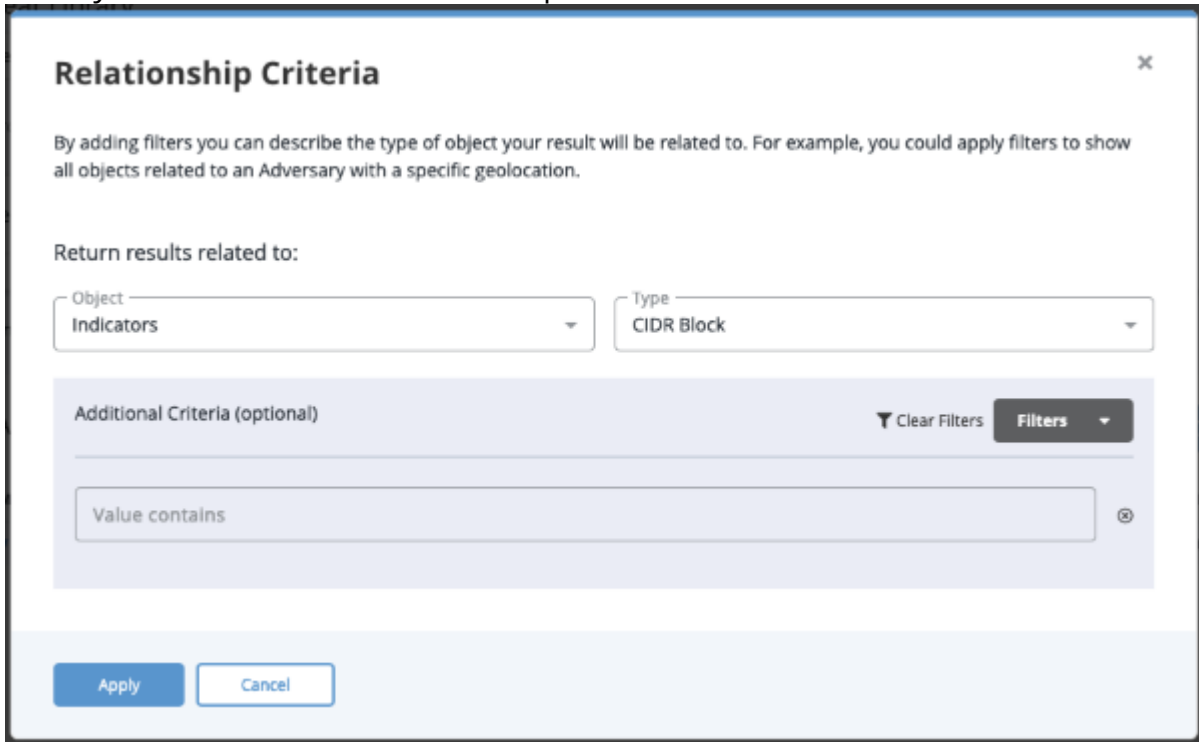
Object: Indicators ▼ Type: CVE ▼

Additional Criteria (optional)

Clear Filters Filters Value Contains

Apply Cancel

- Enter your desired value in the field provided.



**Relationship Criteria** ✕

By adding filters you can describe the type of object your result will be related to. For example, you could apply filters to show all objects related to an Adversary with a specific geolocation.

Return results related to:

Object: Indicators ▼ Type: CIDR Block ▼

Additional Criteria (optional)

Clear Filters Filters

Value contains ⊕

Apply Cancel

- Click on **Apply** to filter.

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

Update Score ▼

Define your score

Clear

0

10

0

10

Submit

Cancel



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.



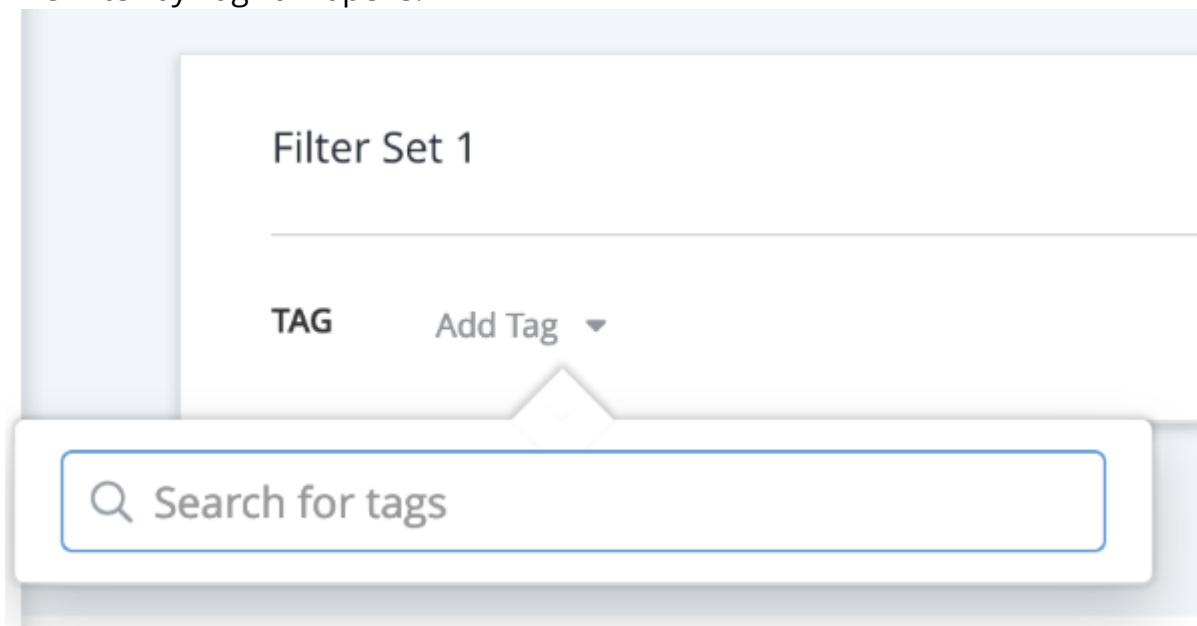
Select the **Update Score** filter again or select **Clear** to remove the filter.

## Filtering by Tags

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

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

The Filter by Tag row opens.



2. Select **Add Tag**.  
The Add Tag dialog box opens.
3. Use the supplied text field to select a tag.
4. Repeats steps 2-3 to apply multiple tag filters.



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

### Examples:

### ANY - Match Toggle Selection

| Setting       | Tag                                                                                        |
|---------------|--------------------------------------------------------------------------------------------|
| Filter A      | Phishing                                                                                   |
| Filter B      | DDoS                                                                                       |
| Filter Option | Any                                                                                        |
| Result        | Search Results are filtered to include items with either Phishing <b>OR</b> the DDoS tags. |

### ALL - Match Toggle Selection

| Setting       | Tags                                                                                  |
|---------------|---------------------------------------------------------------------------------------|
| Filter A      | Phishing                                                                              |
| Filter B      | DDoS                                                                                  |
| Filter Option | All                                                                                   |
| Result        | Search Results are filtered to include items with both Phishing <b>AND</b> DDoS tags. |

## 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

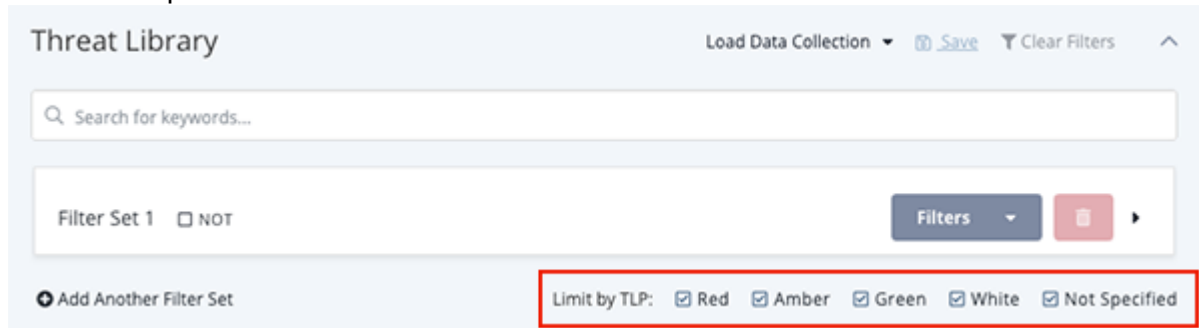
the TLP filter. The filter will then limit source and attribute column data of the search results to only display data that matches the TLP filter.



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.



### 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

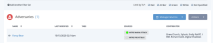
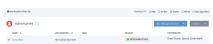
Sources displayed before applying the TLP filter



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

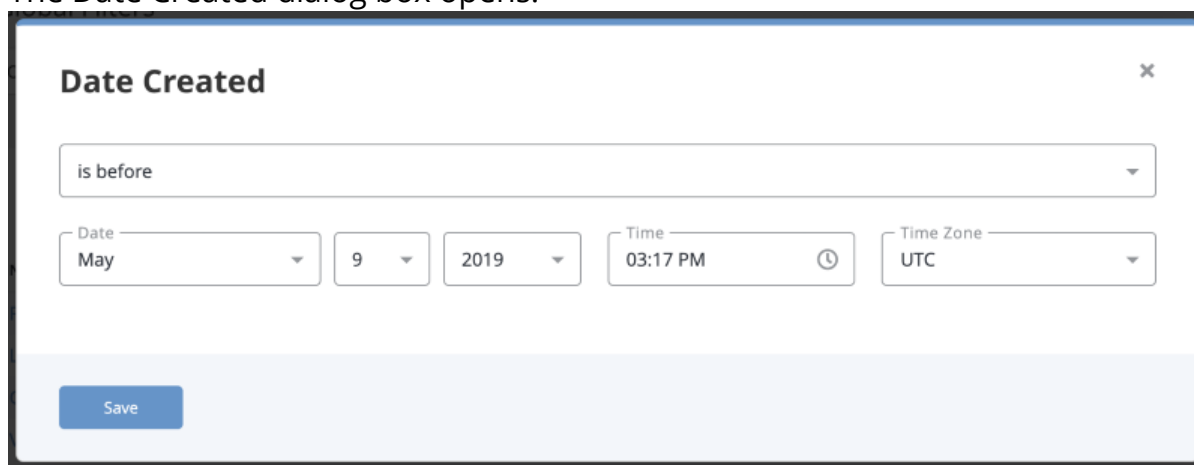
Date filters allow you to filter advanced search results by date-related values.

## 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.



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

| OPTION                    | RESULT                                                           |
|---------------------------|------------------------------------------------------------------|
| <b>is before</b>          | Search results include items before a selected date              |
| <b>is after</b>           | Search results include items after a selected date               |
| <b>is in the range of</b> | Search results include items in a selected range of dates        |
| <b>is within the last</b> | 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.

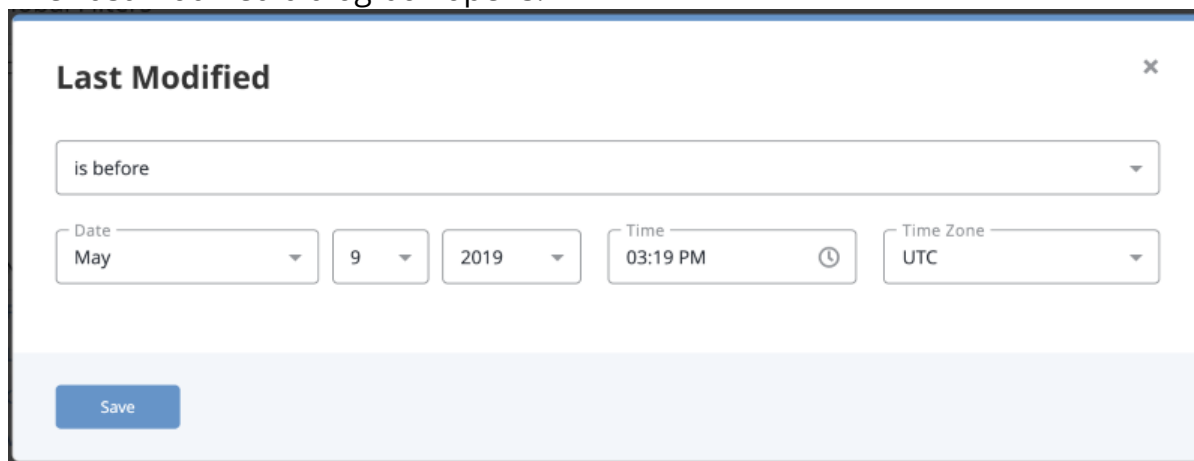
4. Click **Save**.

## 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.



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

| OPTION                    | RESULT                                                           |
|---------------------------|------------------------------------------------------------------|
| <b>is before</b>          | Search results include items before a selected date              |
| <b>is after</b>           | Search results include items after a selected date               |
| <b>is in the range of</b> | Search results include items in a selected range of dates        |
| <b>is within the last</b> | Search results include items within the selected number of days. |

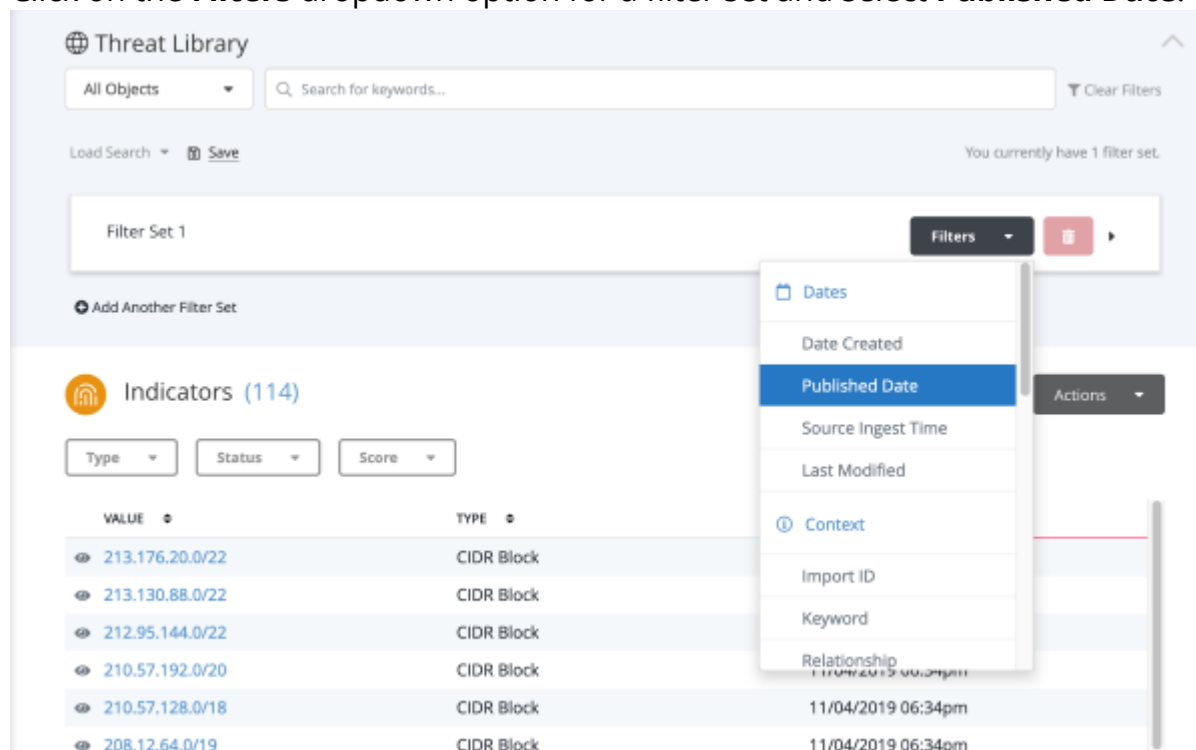
3. Use the controls to select date options based upon the selection in step 2.
4. Click **Save**.

## Filtering by Published Date

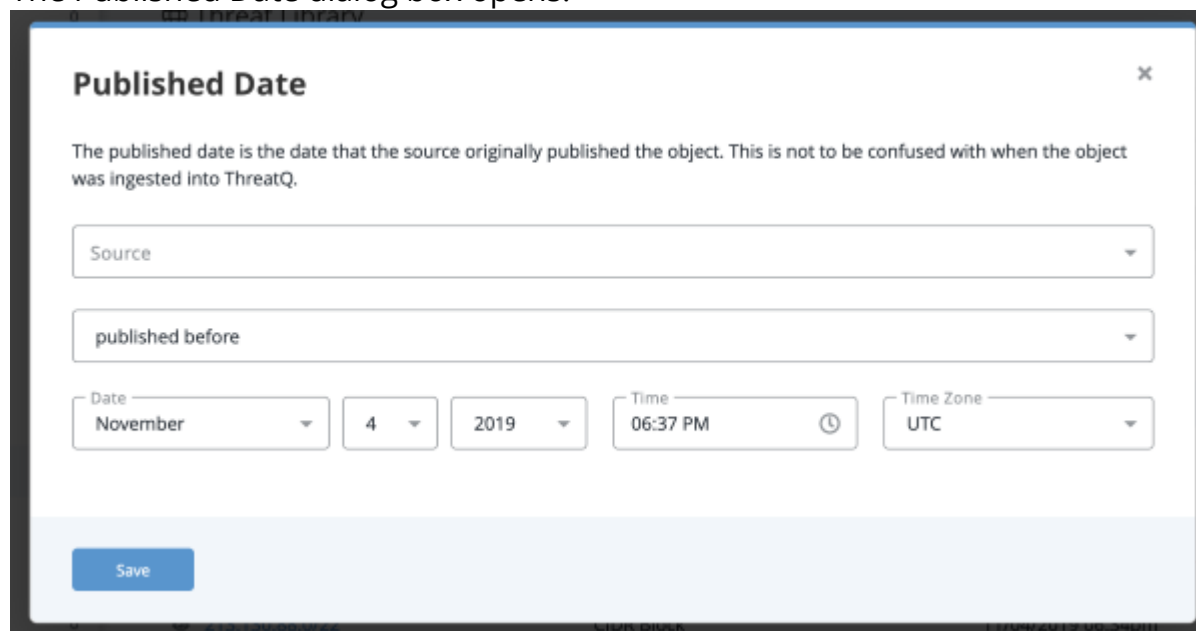


The Published Date is the date that an object was originally published by the source. This is not to be confused with when the object was ingested into ThreatQ.

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



The Published Date dialog box opens.



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



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

| OPTION                           | RESULT                                                           |
|----------------------------------|------------------------------------------------------------------|
| <b>published before</b>          | Search results include items before a selected date              |
| <b>published after</b>           | Search results include items after a selected date               |
| <b>published between</b>         | Search results include items in a selected range of dates        |
| <b>published within the last</b> | 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

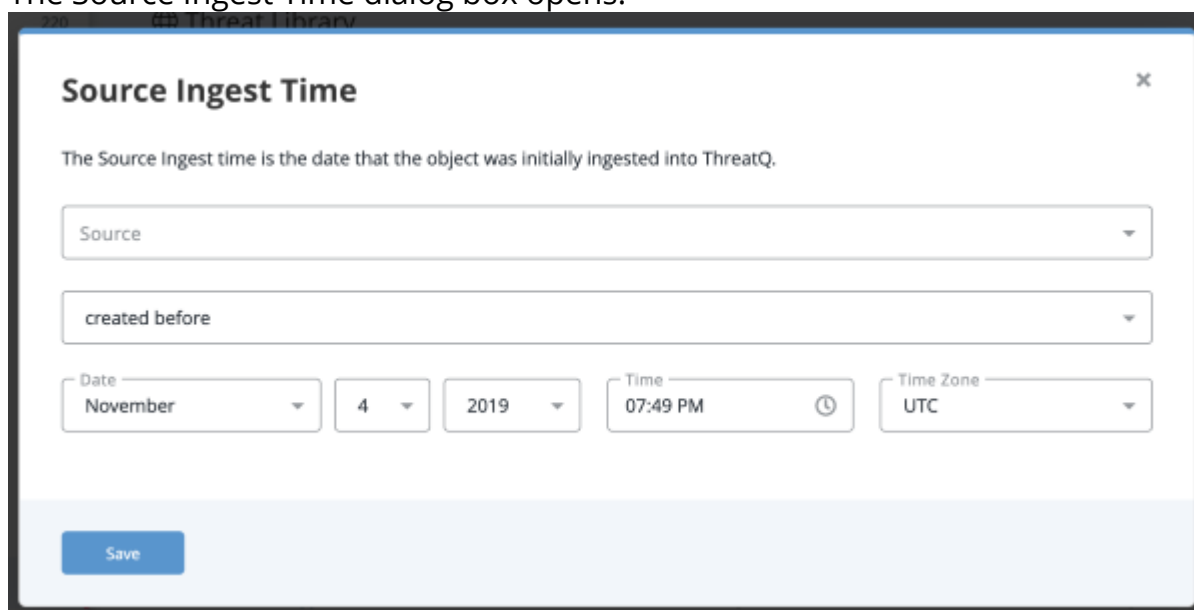


The Source Ingest Time is the date that an object was ingested into ThreatQ.

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

The screenshot shows the Threat Library interface. At the top, there's a search bar with 'All Objects' selected and a search input field. Below the search bar, there's a 'Load Search' button and a 'Save' button. A 'Filter Set 1' box is visible. A 'Filters' dropdown menu is open, showing options: 'Dates', 'Date Created', 'Published Date', 'Source Ingest Time' (highlighted), 'Last Modified', 'Context', 'Import ID', 'Keyword', and 'Relationship'. Below the menu, a table of malware objects is displayed, including 'OSX\_OCEANLOTUS.D', 'FlawedAmmyy', 'RDFSNIFFER', 'NETWIRE', and 'FakeM', all with a 'DATE CREATED' of '11/04/2019 06:39pm'.

The Source Ingest Time dialog box opens.



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

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

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

| OPTION                         | RESULT                                                           |
|--------------------------------|------------------------------------------------------------------|
| <b>created before</b>          | Search results include items before a selected date              |
| <b>created after</b>           | Search results include items after a selected date               |
| <b>created between</b>         | Search results include items in a selected range of dates        |
| <b>created within the last</b> | 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** button located above the search results.

The screenshot shows the ThreatQ interface with a search bar and filters. The 'Expiration' filter is selected, and the 'Expiration Date' dialog box is open. The dialog box has a dropdown menu set to 'is', and three input fields for 'Month' (jan), 'Day' (7), and 'Year' (2020). There are 'Submit' and 'Cancel' buttons at the bottom.

The Expiration Date dialog box opens.

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

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

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

ml>

# 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.

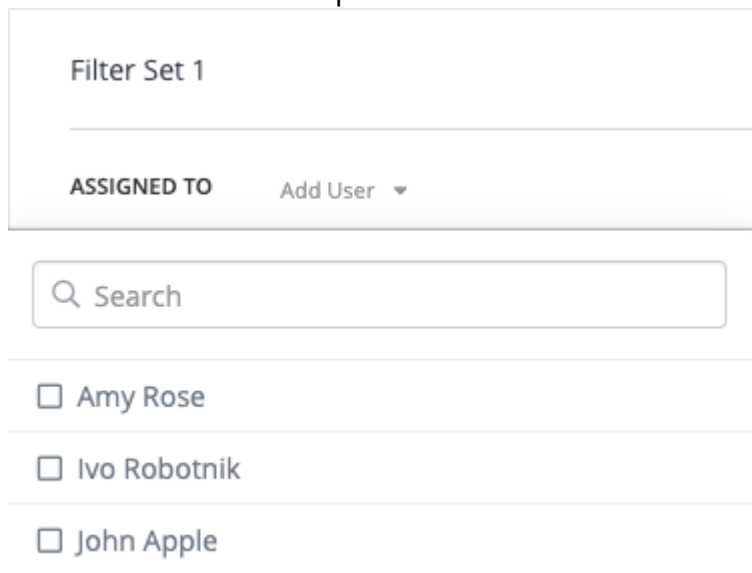
# Tasks Filters

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.

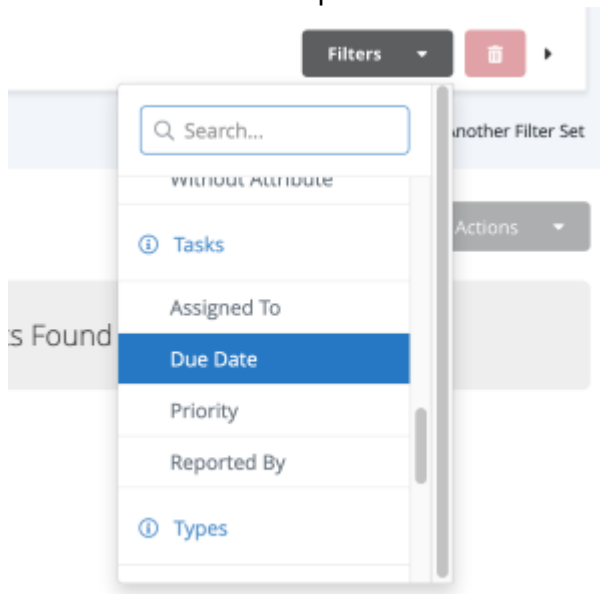
1. Click on the **Filters** option and select **Assigned To**.
2. Use the **Add User** dropdown to select the user.



The screenshot shows a user interface for filtering tasks. At the top, there is a section labeled "Filter Set 1". Below this, there is a dropdown menu currently set to "ASSIGNED TO". To the right of this dropdown is a button labeled "Add User" with a downward arrow. Below the dropdown menu, there is a search bar with a magnifying glass icon and the text "Search". Below the search bar, there is a list of three users, each with a checkbox to its left: "Amy Rose", "Ivo Robotnik", and "John Apple".

## Filtering Tasks by Due Date

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



The Due Date dialog box opens.

A screenshot of the 'Due Date' dialog box. It has a title bar with 'Due Date' and a close button. Inside, there is a dropdown menu labeled 'is after'. Below it, there are three input fields: 'Month' (set to 'Apr'), 'Day' (set to '1'), and 'Year' (set to '2020'). At the bottom left, there is a 'Save' button.

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.  |
| Is within the last | Search results include tasks with a due date within the last user-specified number of days. |

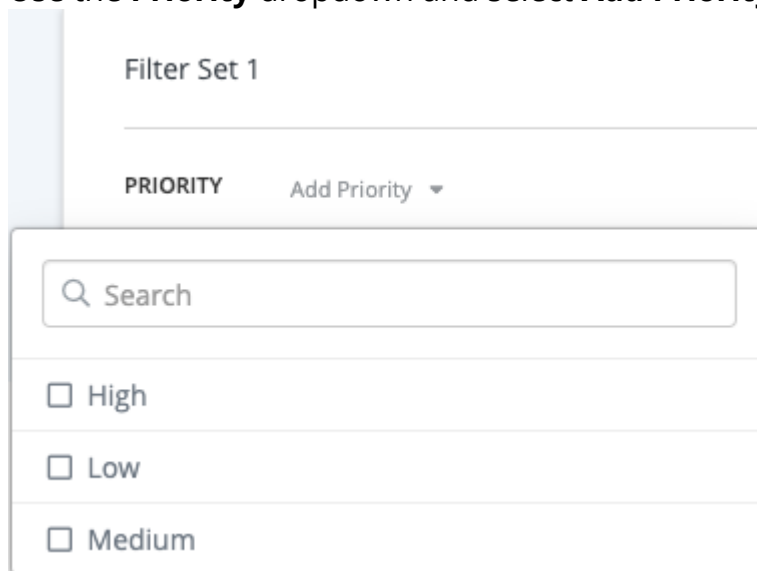
| OPTION             | RESULT                                                                                      |
|--------------------|---------------------------------------------------------------------------------------------|
| Is within the next | Search results include tasks with a due date 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**.



Filter Set 1

PRIORITY Add Priority ▼

Search

☐ High

☐ Low

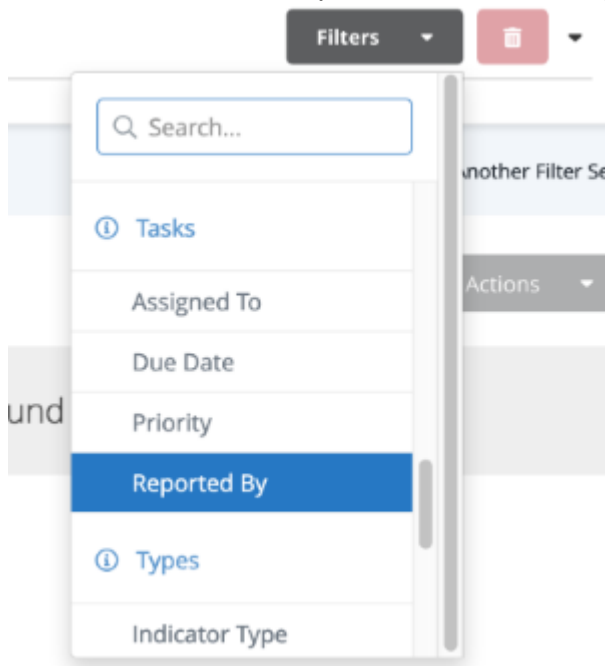
☐ Medium



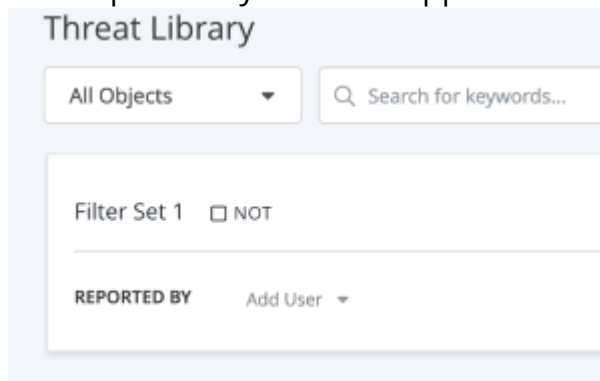
## Filtering Tasks by Reported By

You can filter tasks based on who created it.

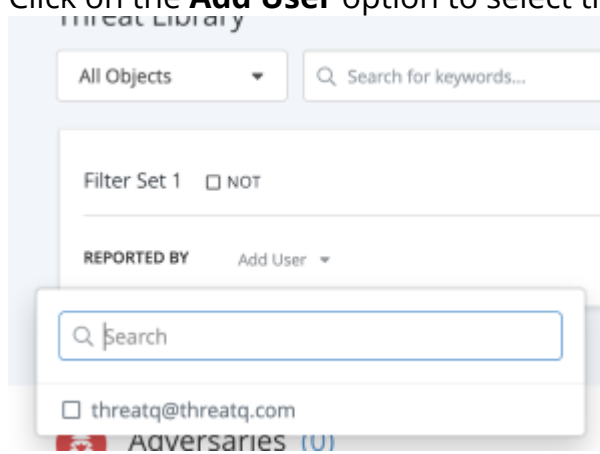
1. Click on the **Filters** option and select **Reported By**.



The Reported By Filter will appear in the filter set.



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



tml>

# Type Filters

You can filter Indicators, 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](#).

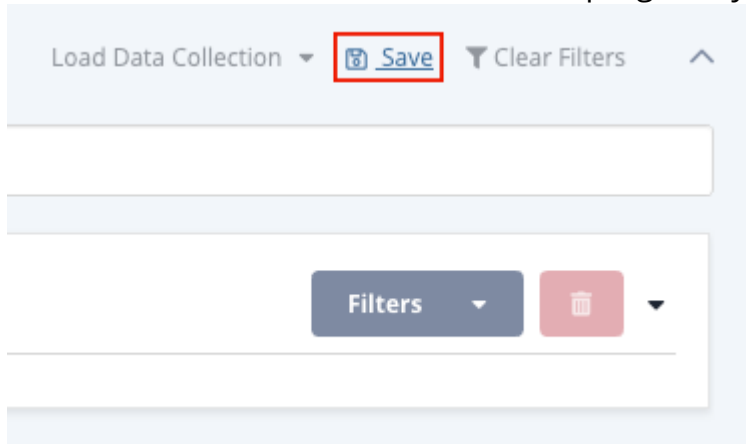


Data collections are accessible to all users on your platform. Integrations and custom dashboards use datacollections and will be affected if an associated data collection is deleted. Use caution when deleting a data collection.

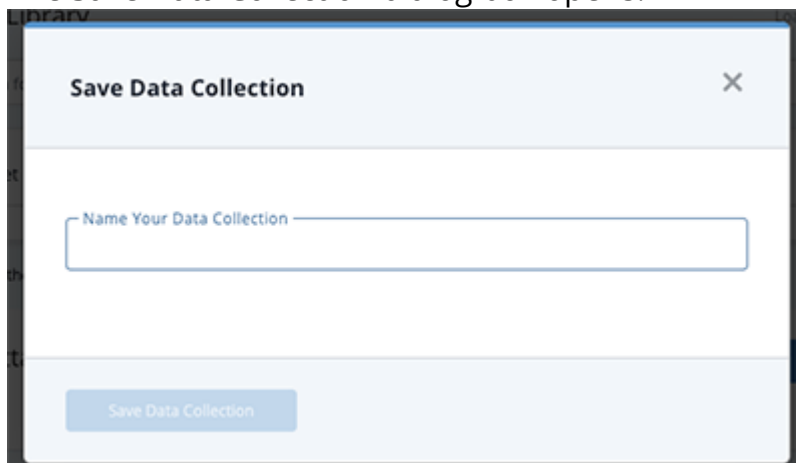
## Saving Searches as Data Collections

To save a search:

1. Perform a [search](#) on the Threat Library.
2. Click on the **Save** icon located to the top-right of your search filters.



The Save Data Collection dialog box opens.



3. Enter a name for the search in the Data Collection dialog box.

#### 4. Click on **Save Data Collection**.

The name of the data collection will appear at the top of the page.

The screenshot shows the ThreatQ Threat Library interface. On the left is a sidebar with a list of object types: Adversaries (0), Attack Patterns (5), Campaigns (0), Courses of Action (3), Events (0), Exploit Targets (0), Files (0), Identities (0), Incidents (0), Indicators (0), and Intrusion Sets (0). The 'Attack Patterns' category is selected. The main content area is titled 'Example Data Collection' (highlighted with a red box). Below the title is a search bar with the placeholder 'Search for keywords...'. A filter set is applied: 'Filter Set 1' with 'KEYWORDS' set to '172'. Below the filters, there is a table of results for 'Attack Patterns (5)'. The table has columns: VALUE, DATE CREATED, LAST MODIFIED, TAGS, and SOURCES. Two results are visible:

| VALUE                         | DATE CREATED       | LAST MODIFIED      | TAGS | SOURCES                 |
|-------------------------------|--------------------|--------------------|------|-------------------------|
| T1172 - Domain Fronting       | 12/04/2020 03:11pm | 12/10/2020 03:10pm |      | MITRE Enterprise ATT&CK |
| T1003 - OS Credential Dumping | 12/04/2020 03:11pm | 12/10/2020 03:10pm |      | MITRE Enterprise ATT&CK |

## Loading Data Collections

To load a data collection:

1. Navigate to the Threat Library page.
2. Click on the **Load Data Collection Search** dropdown list and then select the desired data collection from the list.

This close-up screenshot shows the 'Load Data Collection' dropdown menu. The dropdown is open, displaying a search input field with the text 'Example Data Collection'. Below the search field are buttons for 'Filters' and a red 'X' button. The background shows the top part of the Threat Library interface.

- The data collection will load. The name of data collection will appear at the top of the page.

The screenshot shows the ThreatQ Threat Library interface. On the left is a sidebar with a list of object types: Adversaries (0), Attack Patterns (5), Campaigns (0), Courses of Action (3), Events (0), Exploit Targets (0), Files (0), Identities (0), Incidents (0), Indicators (0), and Intrusion Sets (0). The 'Attack Patterns' category is selected. The main content area is titled 'Example Data Collection' and contains a search bar with the placeholder 'Search for keywords...'. Below the search bar is a filter section with 'Filter Set 1' and a 'NOT' checkbox. A 'KEYWORDS' filter is applied with the value '172'. To the right of the filter section are buttons for 'Filters', 'Save', and 'Clear Filters'. Below the filter section is a table of results. The table has columns for 'VALUE', 'DATE CREATED', 'LAST MODIFIED', 'TAGS', and 'SOURCES'. The results are filtered to show 'Attack Patterns (5)'. The first two results are 'T1172 - Domain Fronting' and 'T1003 - OS Credential Dumping', both created on 12/04/2020 at 03:11pm and last modified on 12/10/2020 at 03:10pm. The source for both is 'MITRE Enterprise ATT&CK'.

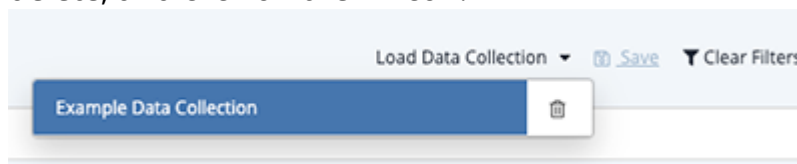
| VALUE                         | DATE CREATED       | LAST MODIFIED      | TAGS | SOURCES                 |
|-------------------------------|--------------------|--------------------|------|-------------------------|
| T1172 - Domain Fronting       | 12/04/2020 03:11pm | 12/10/2020 03:10pm |      | MITRE Enterprise ATT&CK |
| T1003 - OS Credential Dumping | 12/04/2020 03:11pm | 12/10/2020 03:10pm |      | MITRE Enterprise ATT&CK |

## Deleting a Data Collection

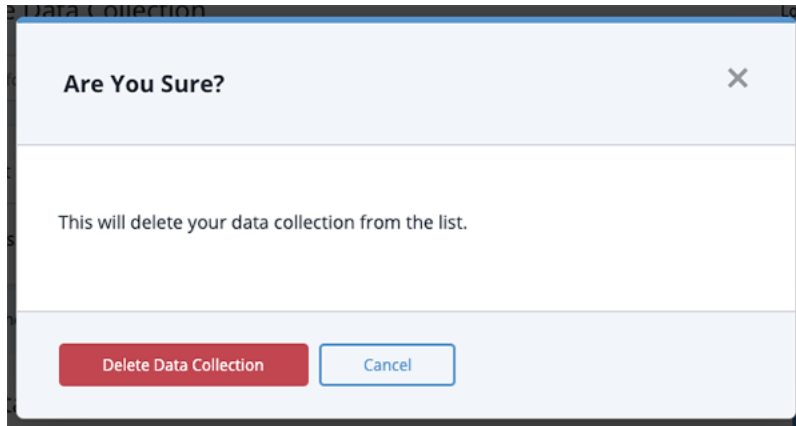
**⚠** Deletion of a data collection cannot be undone. Exercise caution before deleting a data collection as it could be associated with integrations, custom dashboards, and other workflows in use with your organization.

### To delete a data collection:

- Navigate to the Threat Library.
- Click on the **Load Data Collection** dropdown, hover the mouse over the collection to delete, and click on the  icon.



3. Click on **Delete Data Collection** 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.

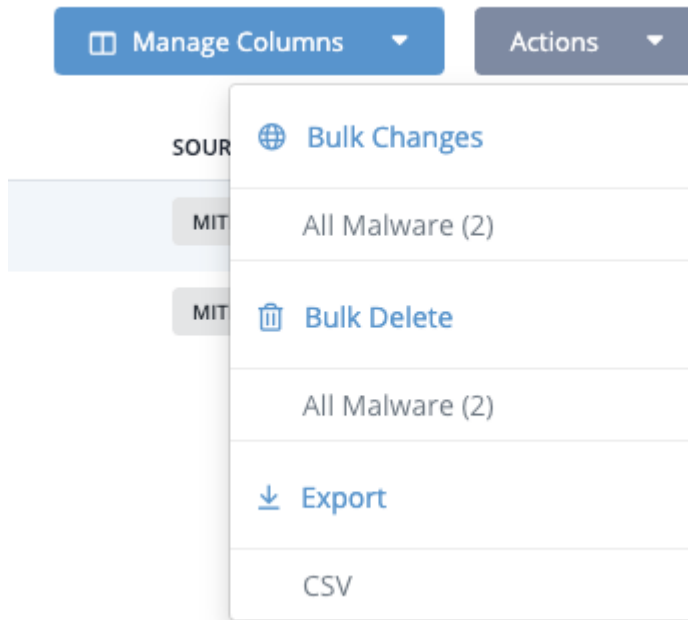


When exporting data collections to a CSV file, if you include additional columns beyond the default, this modification will impact the performance of the export process.

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 on the **Actions** dropdown and select the **CSV** option under the *Export* heading.



The CSV file downloads to your desktop.



## Bulk Actions

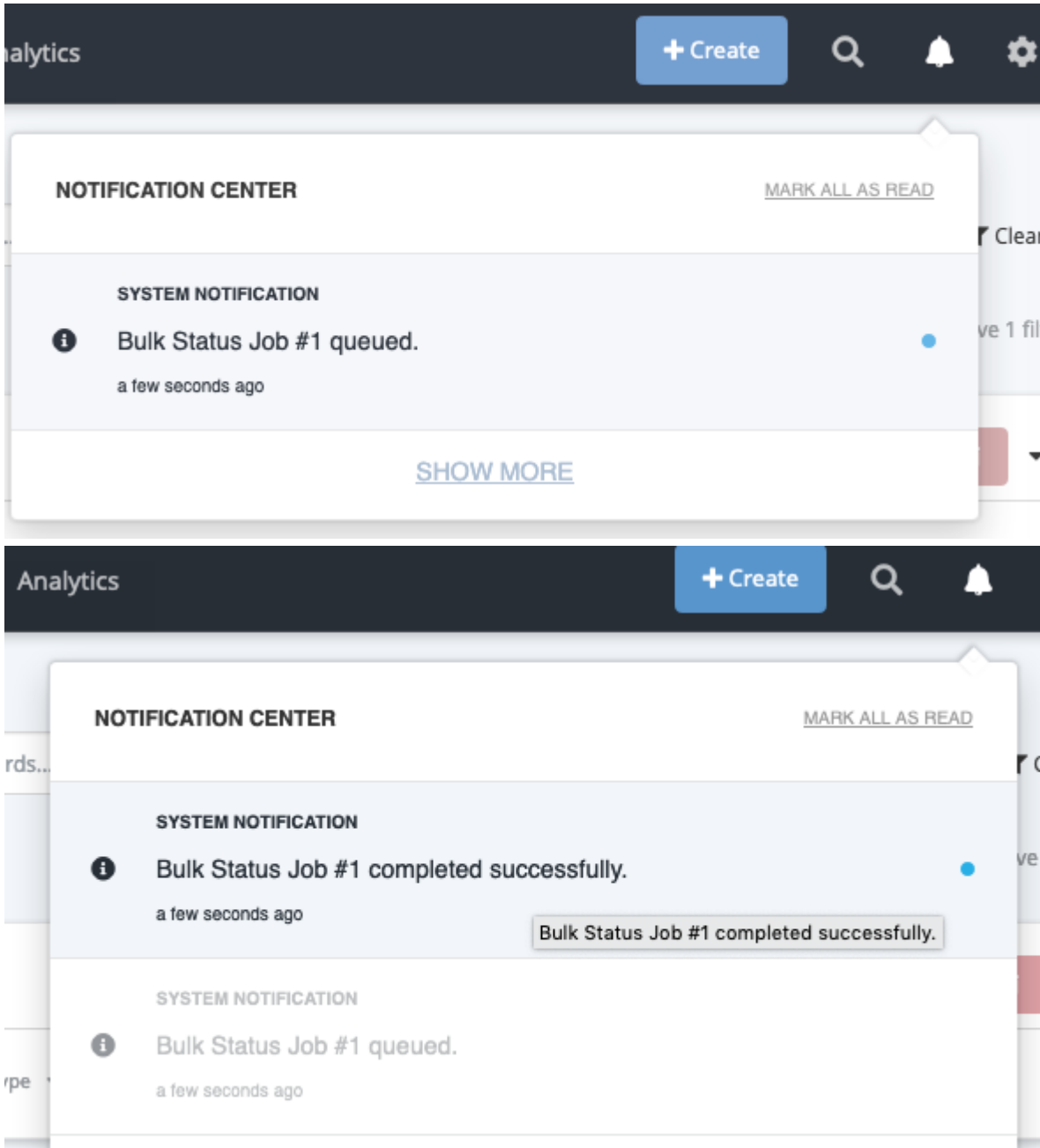
The Bulk Actions feature gives you the ability to update and delete large groups (1000+) of system objects from the Advanced Search page. Once selected, the job process will run in the background and allow you to continue working within ThreatQ. You can review the status of the job and its results on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



The image displays two screenshots of the ThreatQ Notification Center. The top screenshot shows a notification for 'Bulk Status Job #1 queued.' with a timestamp of 'a few seconds ago' and a 'SHOW MORE' link. The bottom screenshot shows a notification for 'Bulk Status Job #1 completed successfully.' with a timestamp of 'a few seconds ago' and a 'Bulk Status Job #1 completed successfully.' link. Both notifications are part of a list in the 'NOTIFICATION CENTER' section, which also includes a 'MARK ALL AS READ' link.



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.

Threat Library

Search for keywords...

Filter Set 1 ☐ NOT

KEYWORDS 172

Limit by TLP: ☐ Red ☐ Amber ☐ Green ☐ White ☐ Not Specified

Indicators (64)

Type Status Score Expiration

| VALUE          | TYPE       | DATE CREATED       | LAST MODIFIED      | STATUS | SCORE | EXPIRATION DATE |
|----------------|------------|--------------------|--------------------|--------|-------|-----------------|
| 88.127.172.137 | IP Address | 12/11/2020 01:58pm | 12/11/2020 01:59pm | Active | 0     |                 |
| 85.172.174.46  | IP Address | 12/11/2020 01:58pm | 12/11/2020 01:58pm | Active | 0     |                 |
| 80.80.172.3    | IP Address | 12/11/2020 01:58pm | 12/11/2020 01:58pm | Active | 0     |                 |
| 52.172.46.238  | IP Address | 12/11/2020 01:58pm | 12/11/2020 01:58pm | Active | 0     |                 |

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

Threat Library

Search for keywords...

Filter Set 1 ☐ NOT

KEYWORDS 172

Limit by TLP: ☐ Red ☐ Amber ☐ Green ☐ White ☐ Not Specified

Indicators (64)

Type Status Score Expiration

| VALUE          | TYPE       | DATE CREATED       | LAST MODIFIED      | STATUS | SCORE | EXPIRATION DATE |
|----------------|------------|--------------------|--------------------|--------|-------|-----------------|
| 88.127.172.137 | IP Address | 12/11/2020 01:58pm | 12/11/2020 01:59pm | Active | 0     |                 |
| 85.172.174.46  | IP Address | 12/11/2020 01:58pm | 12/11/2020 01:58pm | Active | 0     |                 |
| 80.80.172.3    | IP Address | 12/11/2020 01:58pm | 12/11/2020 01:58pm | Active | 0     |                 |
| 52.172.46.238  | IP Address | 12/11/2020 01:58pm | 12/11/2020 01:58pm | Active | 0     |                 |

Actions

- Bulk Changes
- All Indicators (64)
- Bulk Delete
- All Indicators (64)
- Export
- CSV

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.

**Tags**

Add / Remove Add Select a tag

[Add new tag](#)

**Attributes**

Add / Remove Add Name Value Source

[Add new name](#) [Add new value](#) [Add new source](#)

**Sources**

Source

[Add new source](#)

[Add Row](#)

[Apply Changes](#) [Cancel](#)

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

A new row with a dropdown option will load.

### Sources

Source

[Add new source](#)

[Add Row](#)

- 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.

### Sources

Source

[Add new source](#)

[Add Row +](#)

TLP

- ☒ RED
- ☐ AMBER
- ☐ GREEN
- ☐ WHITE
- ☒ NONE

## Bulk Add/Remove Attributes

1. Perform a [search](#) on the Threat Library.

The screenshot shows the ThreatQ Threat Library interface. On the left is a sidebar with a list of object types: Adversaries (0), Attack Patterns (5), Campaigns (0), Courses of Action (3), Events (0), Exploit Targets (0), Files (0), Identities (0), Incidents (0), Indicators (64), Intrusion Sets (0), Malware (2), Reports (0), Signatures (0), and Vulnerabilities (0). The 'Indicators' section is selected. The main panel is titled 'Threat Library' and contains a search bar with the placeholder 'Search for keywords...'. Below the search bar is a filter section with 'Filter Set 1' and a 'not' operator. A 'KEYWORDS' filter is applied with the value '172'. To the right of the filter section are buttons for 'Limit by TLP' with options: Red, Amber, Green, White, and Not Specified. Below the filter section is a section for 'Indicators (64)' with buttons for 'Manage Columns' and 'Actions'. Below this is a table of indicators.

| VALUE          | TYPE       | DATE CREATED       | LAST MODIFIED      | STATUS | SCORE | EXPIRATION DATE |
|----------------|------------|--------------------|--------------------|--------|-------|-----------------|
| 88.127.172.137 | IP Address | 12/11/2020 01:58pm | 12/11/2020 01:59pm | Active | 0     |                 |
| 85.172.174.46  | IP Address | 12/11/2020 01:58pm | 12/11/2020 01:58pm | Active | 0     |                 |
| 80.80.172.3    | IP Address | 12/11/2020 01:58pm | 12/11/2020 01:58pm | Active | 0     |                 |
| 52.172.46.238  | IP Address | 12/11/2020 01:58pm | 12/11/2020 01:58pm | Active | 0     |                 |

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

The screenshot shows the ThreatQ Threat Library interface. On the left is a sidebar with a list of categories: Adversaries (0), Attack Patterns (5), Campaigns (0), Courses of Action (3), Events (0), Exploit Targets (0), Files (0), Identities (0), Incidents (0), Indicators (64), Intrusion Sets (0), Malware (2), Reports (0), Signatures (0), and Tasks (0). The 'Indicators' category is selected. The main panel shows a search bar, filter sets, and a table of indicators. The table has columns: VALUE, TYPE, DATE CREATED, LAST MODIFIED, STATUS, and SCORE. Four indicators are listed, all with a status of 'Active'. An 'Actions' dropdown menu is open, showing options: Bulk Changes, All Indicators (64), Bulk Delete, All Indicators (64), Export, and CSV.

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

The Bulk Changes form will load.

The screenshot shows the 'Bulk Changes' form in ThreatQ. The header indicates 'Your changes will affect 40 objects'. The form is divided into several sections: Status (Indicator Status), Change Expiration Date (Select Expiration Status), Tags (Add / Remove, Add, Select a tag), Attributes (Add / Remove, Add, Name, Value, Source), and Sources (Source). Each section has a corresponding 'Add new' link. At the bottom are 'Apply Changes' and 'Cancel' buttons.



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<br>Add | Name<br>ASN                  | Value<br>13335                | Source<br>abuse.ch URLhaus Plai... |  |
|                     | <a href="#">Add new name</a> | <a href="#">Add new value</a> | <a href="#">Add new source</a>     |  |

Add Row

#### Attributes

|                        |             |                |  |
|------------------------|-------------|----------------|--|
| Add / Remove<br>Remove | Name<br>ASN | Value<br>13335 |  |
|------------------------|-------------|----------------|--|

Add Row



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

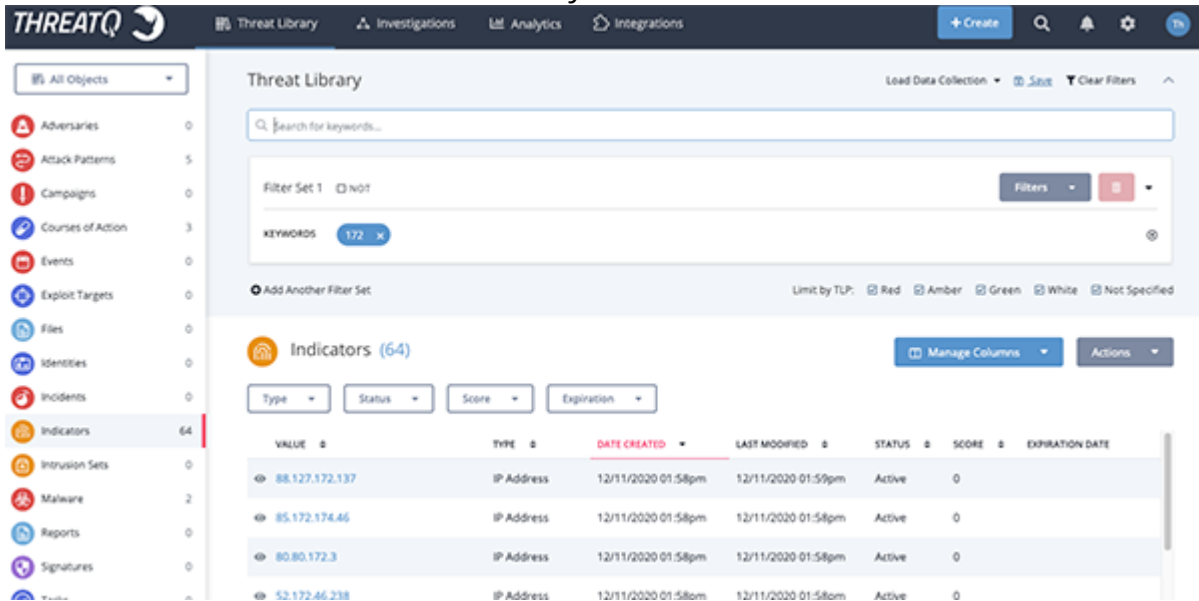
In this scenario, the platform will execute the Bulk Changes in the following order:

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



## Bulk Add/Remove Tags

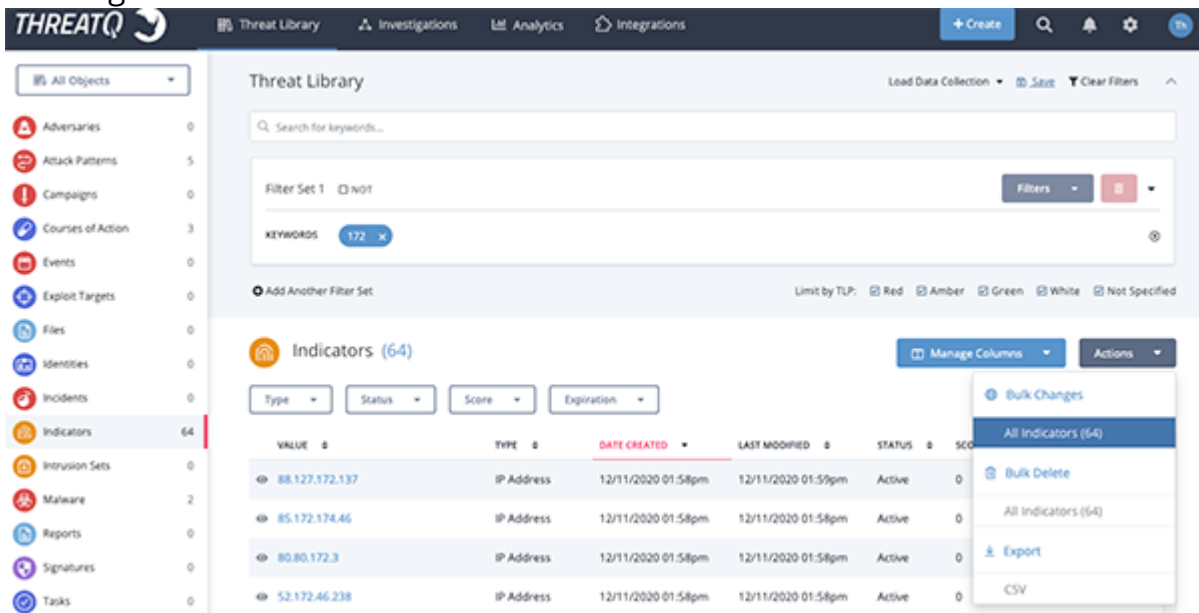
1. Perform a [search](#) on the Threat Library.



The screenshot shows the ThreatQ Threat Library interface. The left sidebar lists various object types, with 'Indicators' selected and showing 64 items. The main panel displays a table of indicators with columns for Value, Type, Date Created, Last Modified, Status, Score, and Expiration Date. The table shows four IP address indicators.

| VALUE          | TYPE       | DATE CREATED       | LAST MODIFIED      | STATUS | SCORE | EXPIRATION DATE |
|----------------|------------|--------------------|--------------------|--------|-------|-----------------|
| 88.127.172.137 | IP Address | 12/11/2020 01:58pm | 12/11/2020 01:59pm | Active | 0     |                 |
| 85.172.174.46  | IP Address | 12/11/2020 01:58pm | 12/11/2020 01:58pm | Active | 0     |                 |
| 80.80.172.3    | IP Address | 12/11/2020 01:58pm | 12/11/2020 01:58pm | Active | 0     |                 |
| 52.172.46.238  | IP Address | 12/11/2020 01:58pm | 12/11/2020 01:58pm | Active | 0     |                 |

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



The screenshot shows the ThreatQ Threat Library interface with the 'Actions' dropdown menu open. The menu is open, displaying options for Bulk Changes, Bulk Delete, Export, and CSV. The 'Bulk Changes' option is highlighted.



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.

**Tags**

Add / Remove  
Add

Select a tag

[Add new tag](#)

**Attributes**

Add / Remove  
Add

Name

Value

Source

[Add new name](#) [Add new value](#) [Add new source](#)

**Sources**

Source

[Add new source](#)

Apply Changes Cancel

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.

**Tags**

Add / Remove  
Add

Select a tag

[Add new tag](#)

**Add Row** +



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.

Threat Library

Search for keywords...

Filter Set 1 ☐ not

KEYWORDS 172

Limit by TLP: ☐ Red ☐ Amber ☐ Green ☐ White ☐ Not Specified

Indicators (64)

Manage Columns Actions

| VALUE          | TYPE       | DATE CREATED       | LAST MODIFIED      | STATUS | SCORE | EXPIRATION DATE |
|----------------|------------|--------------------|--------------------|--------|-------|-----------------|
| 88.127.172.137 | IP Address | 12/11/2020 01:58pm | 12/11/2020 01:59pm | Active | 0     |                 |
| 85.172.174.46  | IP Address | 12/11/2020 01:58pm | 12/11/2020 01:58pm | Active | 0     |                 |
| 80.80.172.3    | IP Address | 12/11/2020 01:58pm | 12/11/2020 01:58pm | Active | 0     |                 |
| 52.172.46.238  | IP Address | 12/11/2020 01:58pm | 12/11/2020 01:58pm | Active | 0     |                 |

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

Threat Library

Search for keywords...

Filter Set 1 ☐ not

KEYWORDS 172

Limit by TLP: ☐ Red ☐ Amber ☐ Green ☐ White ☐ Not Specified

Indicators (64)

Manage Columns Actions

- Bulk Changes
  - All Indicators (64)
- Bulk Delete
  - All Indicators (64)
- Export
  - CSV

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.

**Tags**

Add / Remove Add Select a tag Add new tag

**Attributes**

Add / Remove Add Name Value Source Add new name Add new value Add new source

**Sources**

Source Add new source

Apply Changes Cancel

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

he 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.

The screenshot shows the ThreatQ Threat Library interface. On the left is a sidebar with a list of object types: Adversaries (0), Attack Patterns (5), Campaigns (0), Courses of Action (3), Events (0), Exploit Targets (0), Files (0), Identities (0), Incidents (0), Indicators (64), Intrusion Sets (0), Malware (2), Reports (0), and Signatures (0). The 'Indicators' section is selected. The main panel is titled 'Threat Library' and contains a search bar with the placeholder 'Search for keywords...'. Below the search bar is a filter section with 'Filter Set 1' and a 'KEYWORDS' tag. To the right of the filter section are buttons for 'Filters' and 'Clear Filters'. Below the filter section is a table of indicators. The table has columns: VALUE, TYPE, DATE CREATED, LAST MODIFIED, STATUS, SCORE, and EXPIRATION DATE. The table shows four rows of IP addresses, all with a status of 'Active' and a score of '0'. The 'Actions' dropdown menu is open, showing options: 'Bulk Changes', 'All Indicators (64)', 'Bulk Delete', 'All Indicators (64)', 'Export', and 'CSV'.

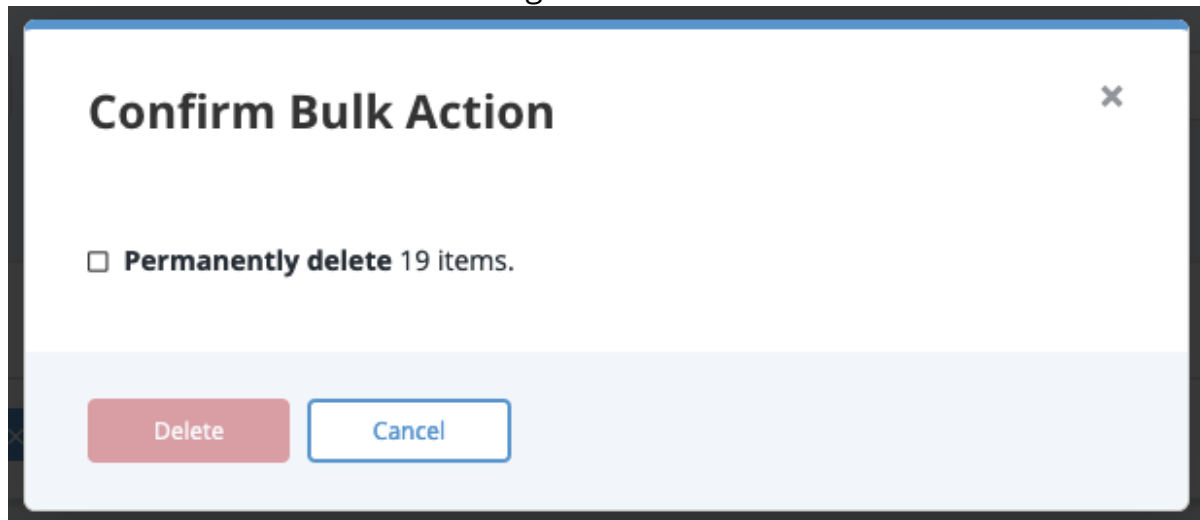
2. Click on the **Actions** dropdown and select **All <System Object>** under the *Bulk Delete* heading.

The screenshot shows the 'Actions' dropdown menu open. The menu has a header 'Bulk Changes' with a globe icon. Below the header are four items: 'All Indicators (64)', 'Bulk Delete' (with a trash icon), 'All Indicators (64)' (highlighted in blue), and 'Export' (with a download icon). Below these items is a 'CSV' option. The background shows a table with columns 'STATUS' and 'SCORE' and rows of 'Active' status and '0' score.



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

The Bulk Action Confirmation dialog box will load.



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

## 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.

The screenshot shows the ThreatQ Threat Library interface. On the left is a sidebar with various object types, with 'Indicators' selected and showing a count of 64. The main area has a search bar with the text 'Search for keywords...'. Below the search bar, there's a filter section with 'Filter Set 1' and a 'KEYWORDS' filter set to '172'. A table of indicators is displayed with columns: VALUE, TYPE, DATE CREATED, LAST MODIFIED, STATUS, SCORE, and EXPIRATION DATE. The table shows several IP addresses, all with a status of 'Active' and a score of 0.

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

The screenshot shows the 'Actions' dropdown menu. The menu is open, displaying options under the 'Bulk Changes' heading. The options are: 'All Indicators (64)', 'Bulk Delete', 'All Indicators (64)' (highlighted), 'Export', and 'CSV'. The 'All Indicators (64)' option is highlighted in blue.

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 220 objects

**Tags**

Add / Remove  
Add Select a tag  
Add new tag

**Attributes**

Add / Remove  
Add Name Value Source  
Add new name Add new value Add new source

**Sources**

Source  
Add new source

**Relationships**

Limit search to  
All Objects Start typing...

Apply Changes Cancel



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.

**Relationships**

Limit search to  
All Objects Start typing...

Start typing...

Adversaries

4. Enter an object name.

The Add/Remove option appears.

**Relationships**

Limit search to  
All Objects Start typing...

Add / Remove  
Add

INDICATOR 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.

- 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.

- Perform a [search](#) on the Threat Library.

The screenshot shows the ThreatQ Threat Library interface. On the left is a sidebar with a list of object types: Adversaries (0), Attack Patterns (5), Campaigns (0), Courses of Action (3), Events (0), Exploit Targets (0), Files (0), Identities (0), Incidents (0), Indicators (64), Intrusion Sets (0), Malware (2), Reports (0), Signatures (0), and Vulnerabilities (0). The 'Indicators' category is selected. The main panel is titled 'Threat Library' and contains a search bar with the placeholder 'Search for keywords...'. Below the search bar is a filter section with 'Filter Set 1' and a 'NOT' operator. A 'KEYWORDS' filter is applied with the value '172'. To the right of the filter section are buttons for 'Filters' and 'Clear Filters'. Below the filter section is a 'Limit by TLP' section with checkboxes for Red, Amber, Green, White, and Not Specified. The main content area displays a table of indicators, with a header 'Indicators (64)' and buttons for 'Manage Columns' and 'Actions'. The table has columns for VALUE, TYPE, DATE CREATED, LAST MODIFIED, STATUS, SCORE, and EXPIRATION DATE. The first four rows of the table are visible, all showing IP addresses with a status of 'Active' and a score of '0'.

| VALUE          | TYPE       | DATE CREATED       | LAST MODIFIED      | STATUS | SCORE | EXPIRATION DATE |
|----------------|------------|--------------------|--------------------|--------|-------|-----------------|
| 88.127.172.137 | IP Address | 12/11/2020 01:58pm | 12/11/2020 01:59pm | Active | 0     |                 |
| 85.172.174.46  | IP Address | 12/11/2020 01:58pm | 12/11/2020 01:58pm | Active | 0     |                 |
| 80.80.172.3    | IP Address | 12/11/2020 01:58pm | 12/11/2020 01:58pm | Active | 0     |                 |
| 52.172.46.238  | IP Address | 12/11/2020 01:58pm | 12/11/2020 01:58pm | Active | 0     |                 |

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

The screenshot shows the ThreatQ Threat Library interface. On the left is a sidebar with a list of categories: Adversaries (0), Attack Patterns (5), Campaigns (0), Courses of Action (3), Events (0), Exploit Targets (0), Files (0), Identities (0), Incidents (0), Indicators (64), Intrusion Sets (0), Malware (2), Reports (0), Signatures (0), and Tasks (0). The 'Indicators' category is selected. The main panel shows a search bar, filter sets, and a table of indicators. The 'Actions' dropdown menu is open, showing options: Bulk Changes, All Indicators (64), Bulk Delete, All Indicators (64), Export, and CSV.

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

The Bulk Changes form will load.

The screenshot shows the 'Bulk Changes' form in ThreatQ. The form has a header bar with the title 'Bulk Changes' and a subtitle 'Your changes will affect 40 objects'. The form is divided into several sections: 'Status' with a dropdown menu for 'Indicator Status'; 'Change Expiration Date' with a dropdown menu for 'Select Expiration Status'; 'Tags' with an 'Add / Remove' button and a 'Select a tag' dropdown; 'Attributes' with an 'Add / Remove' button and a table with columns 'Name', 'Value', and 'Source'; and 'Sources' with a 'Source' dropdown. At the bottom are 'Apply Changes' and 'Cancel' buttons.

- Use the dropdown provided to select a new status to be applied to the selected objects.
- 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, will display additional information such as the indicator's status, score, and expiration data.

The screenshot displays the 'Object Details' page for an indicator named 'example.com'. The page is divided into a header section and a main content area. The header section includes the object name, score (10 - Very High), status (Active), and creation/expiration dates. The main content area is organized into a sidebar with a list of sections and a main panel with details for each section. The sidebar sections are: Context (Attributes, Sources, Tags, Description), Relationships (Adversaries, Files, Indicators, Tasks), Comments, Operations, and Audit Log. The main panel sections are: Attributes, Sources, Tags, Description, Adversaries, Files, Indicators, Tasks, Comments, Operations, and Audit Log. The 'Indicators' section in the main panel includes options for Bulk Update, Link, and Unlink. The 'Tasks' section includes options for Create, Delete, Link, and Unlink. The 'Comments' section includes an Add button. The 'Operations' section includes a button for Add. The 'Audit Log' section includes a button for Add. The page is annotated with numbered circles 1 through 19, indicating specific UI elements.

**Header Section:**

- 1: Object Name (example.com)
- 2: Score (10 - Very High)
- 3: Status (Active)
- 4: Add to Watchlist button
- 5: Expiration Date (Expires: add date)
- 6: First Seen (03/08/2019 06:02pm)
- 7: Created (03/08/2019)

**Sidebar Section:**

- 18: Actions dropdown
- 19: Context (Attributes (7), Sources (3), Tags (1), Description (1))
- 19: Relationships (Adversaries (2), Files (1), Indicators (15), Tasks (2))
- 19: Comments (1)
- 19: Operations
- 19: Audit Log

**Main Content Area:**

- 7: Attributes
- 8: Sources
- 9: Tags
- 10: Description
- 11: Adversaries
- 12: Files
- 13: Indicators
- 14: Tasks
- 15: Comments
- 16: Operations
- 17: Audit Log

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*<br>Applies to Indicator Object Types Only   | The Score Selection dropdown allows you to override an indicator's score set by the scoring algorithm.                                                        | <ul style="list-style-type: none"><li>• <a href="#">Indicator Expiration</a></li><li>• <a href="#">Scoring Algorithms</a></li></ul>                    |
| 3      | Scoring Influence*<br>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.                           | <ul style="list-style-type: none"><li>• <a href="#">Scoring Algorithms</a></li></ul>                                                                   |
| 4      | Status*<br>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. | <ul style="list-style-type: none"><li>• <a href="#">Indicator Status</a></li><li>• <a href="#">Indicator Statuses</a> (System Configuration)</li></ul> |
| 5      | Add to Watchlist                                             | The Watchlist toggle button allows you to add and remove the object from the Watchlist widget.                                                                | <ul style="list-style-type: none"><li>• <a href="#">Add/Remove an Object to the Watchlist</a></li></ul>                                                |

## OBJECT DETAILS PAGE LEGEND

|   |                                                                |                                                                                                                                                            |                                                                                                                                                    |
|---|----------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| 6 | Expiration*<br>Applies to<br>Indicator<br>Object Types<br>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. | <ul style="list-style-type: none"><li>• <a href="#">Indicator Expiration</a></li><li>• <a href="#">Automatic Expiration and Policies</a></li></ul> |
|---|----------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|

## 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. | <ul style="list-style-type: none"><li>• <a href="#">Attributes Pane</a></li></ul>     |
| 8      | Sources     | The Sources pane displays sources associated with the object. You can Add additional sources to an object.                          | <ul style="list-style-type: none"><li>• <a href="#">Sources Pane</a></li></ul>        |
| 9      | Tags        | The Tags pane displays tags associated with the object. You can Add and Delete tags found in this section.                          | <ul style="list-style-type: none"><li>• <a href="#">Tags Pane</a></li></ul>           |
| 10     | Description | The Description pane allows you to add general information about the object.                                                        | <ul style="list-style-type: none"><li>• <a href="#">Description Pane</a></li></ul>    |
| 11     | Adversaries | The Adversaries pane displays adversaries associated with the object.                                                               | <ul style="list-style-type: none"><li>• <a href="#">Relationships Panes</a></li></ul> |

## OBJECT DETAILS PAGE LEGEND

|    |                 |                                                                                                                                                                                                                                                      |                                                                                           |
|----|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
| 12 | Files           | The Files pane displays files associated with the object.                                                                                                                                                                                            | <ul style="list-style-type: none"><li>• <a href="#">Relationships Panes</a></li></ul>     |
| 13 | Indicators      | The Indicators pane displays indicators associated with the object.                                                                                                                                                                                  | <ul style="list-style-type: none"><li>• <a href="#">Relationships Panes</a></li></ul>     |
| 14 | Tasks           | The Tasks pane displays tasks associated with the object.                                                                                                                                                                                            | <ul style="list-style-type: none"><li>• <a href="#">Relationships Panes</a></li></ul>     |
| 10 | Related Objects | <p>There are several different related panes depending on the types of objects linked to the object.</p> <p>You can use these panes to view and add/remove linked indicators, files, signatures, events, adversaries, tasks, and investigations.</p> | <ul style="list-style-type: none"><li>• <a href="#">Relationships Panes</a></li></ul>     |
| 15 | Comments        | The Comments pane allows you to record comments about the object for other users to read and reference.                                                                                                                                              | <ul style="list-style-type: none"><li>• <a href="#">Relationships Panes</a></li></ul>     |
| 16 | Operations      | <p>The Operations pane allows you to associate third-party attributes and related indicators to the indicator.</p> <p><b>Note:</b> This options requires the installation of Operations. See</p>                                                     | <ul style="list-style-type: none"><li>• <a href="#">Integrations Management</a></li></ul> |



---

**OBJECT DETAILS PAGE LEGEND**

---

the [Managing Integrations](#) topic for more details.

|    |           |                                                                         |                             |
|----|-----------|-------------------------------------------------------------------------|-----------------------------|
| 17 | Audit Log | The Audit Log panel displays all actions and changes made to an Object. | • <a href="#">Audit Log</a> |
|----|-----------|-------------------------------------------------------------------------|-----------------------------|

**Left-Hand Navigation**

| Number | Field       | Description                                                                                                                                                                                                                                                                                                          | Reference                      |
|--------|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|
| 18     | Action Menu | <p>The Actions menu allows you to execute the following actions for an object:</p> <ul style="list-style-type: none"><li>• Add a New Attribute</li><li>• Add a New Comment</li><li>• Create a Task</li><li>• Generate a Report</li><li>• Add a Relationship</li><li>• Add a Source</li><li>• Delete Object</li></ul> | • <a href="#">Actions Menu</a> |

|    |                         |                                                                          |     |
|----|-------------------------|--------------------------------------------------------------------------|-----|
| 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.

The screenshot shows the ThreatQ interface for an indicator with IP address 73.49.109.200. The score is 10 - Very High, and the status is Review. The indicator was created on 05/07/2019 and first seen on 08/16/2018 03:57pm. The 'Add to Watchlist' button is highlighted with a red box. The left sidebar shows the 'Context' menu with options like Attributes (2), Sources (1), Tags (0), Description (0), Relationships, Comments (0), and Operations. The main content area shows the 'Attributes (2)' table with columns for Attribute Type, Attribute Value, Sources, and Date Created. The table lists two attributes: Destination Port (7080) and Malware Type (2019-05-07). The Sources column for both attributes lists 'abuse.ch Feodo Tracker Botnet' and 'C2 IP Blocklist'. The Date Created column shows '05/07/2019 03:11pm' for both. Below the attributes table, there is a 'Sources (1)' section with an 'Add' button.

| ATTRIBUTE TYPE   | ATTRIBUTE VALUE | SOURCES                                          | DATE CREATED       |
|------------------|-----------------|--------------------------------------------------|--------------------|
| Destination Port | 7080            | abuse.ch Feodo Tracker Botnet<br>C2 IP Blocklist | 05/07/2019 03:11pm |
| Malware Type     | 2019-05-07      | abuse.ch Feodo Tracker Botnet<br>C2 IP Blocklist | 05/07/2019 03:11pm |

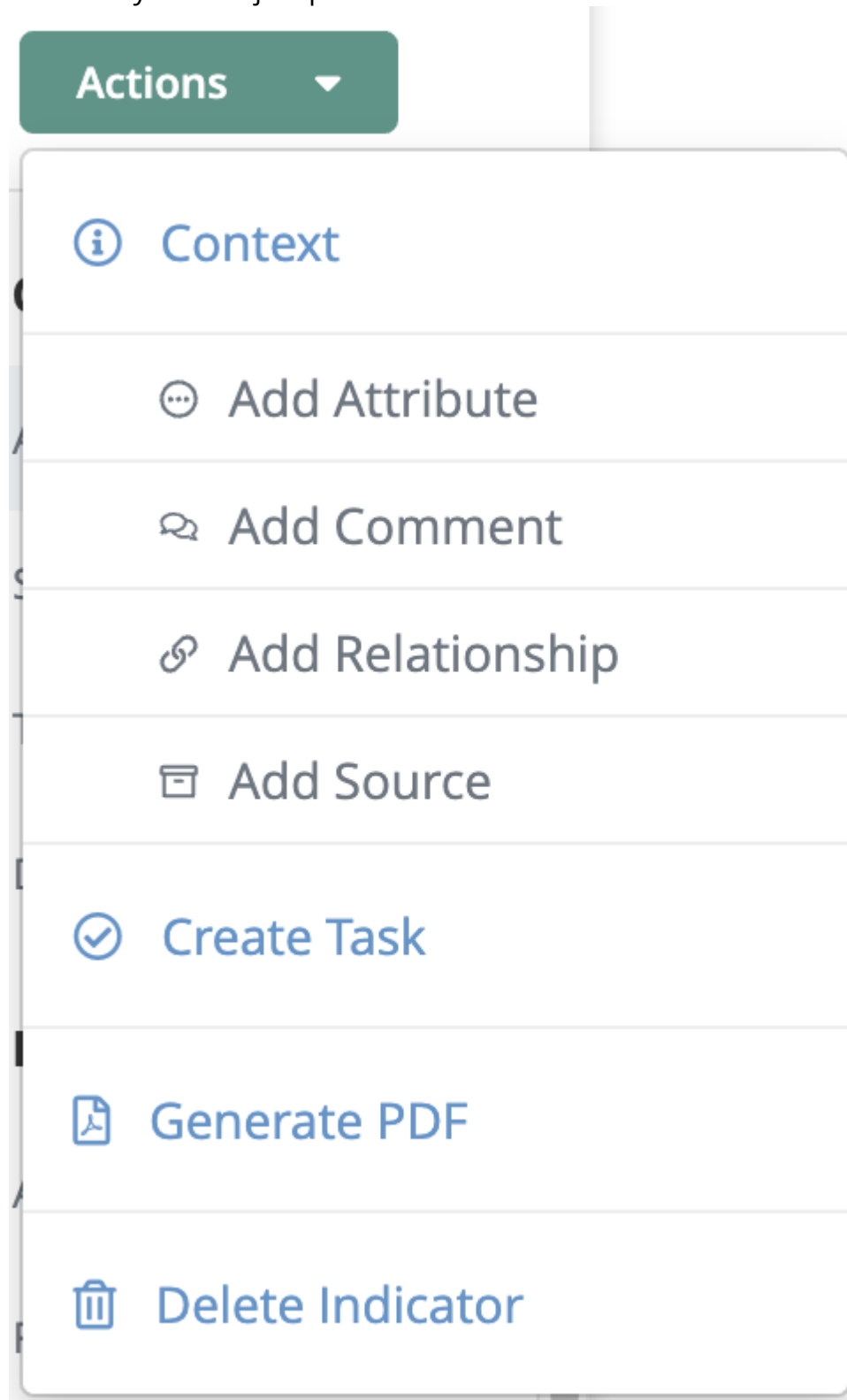


Click on **Remove from Watchlist** to remove an item.

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:**

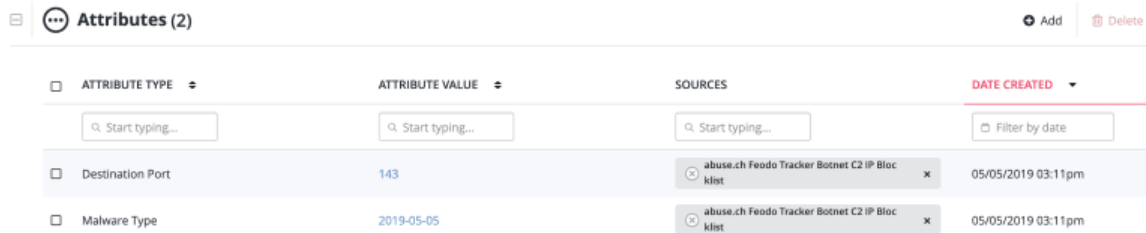
| ACTION           | FUNCTION                                                                               | REFERENCE                                                                                    |
|------------------|----------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|
| Add Attribute    | Brings up the Add Details dialog box to add an attribute to the object.                | • <a href="#">Attributes Pane</a>                                                            |
| Add Comment      | Creates a new text box entry in the comment pane.                                      | • <a href="#">Comments Pane</a>                                                              |
| Add Relationship | Brings up the Add Relationships dialog box to link other system objects to the object. | • <a href="#">Relationships Panes</a><br>• <a href="#">Additional Related Object Actions</a> |
| Add Source       | Brings up the Add Details dialog box to add a source to the object.                    | • <a href="#">Sources Pane</a>                                                               |
| Create Task      | Opens up the Add Task dialog box.                                                      | • <a href="#">Tags Pane</a>                                                                  |
| Generate Report  | Generates a PDF report of the object.                                                  | • <a href="#">Reports</a>                                                                    |
| Delete Object    | Delete the system object.                                                              | N/A                                                                                          |

## Context Panes

The Context section of the object details page displays attributes, sources, and tags associated with the system object.

## Attributes Pane

The Context section of the object details page displays attributes, sources, and tags associated with the system object.



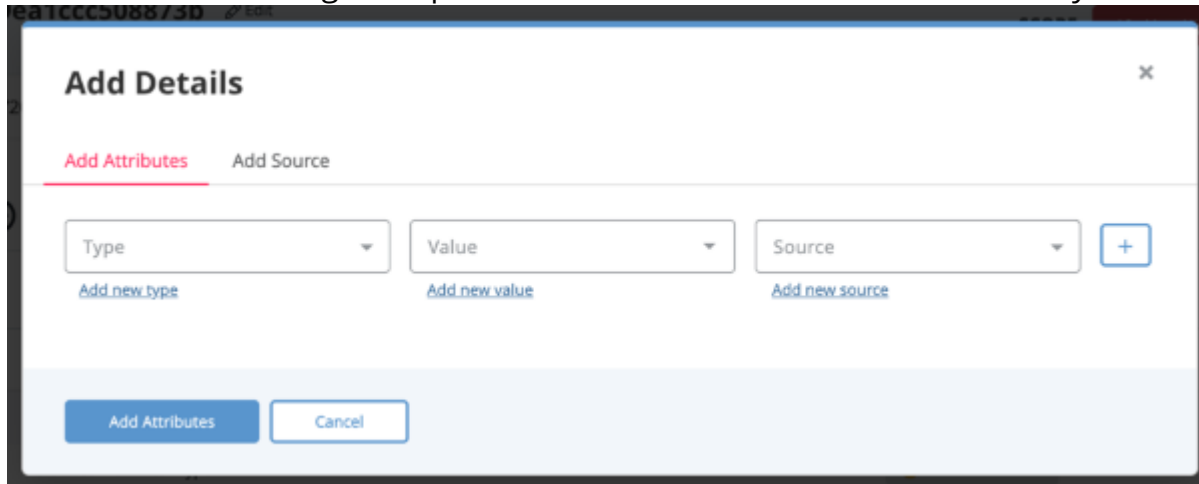
| ATTRIBUTE TYPE   | ATTRIBUTE VALUE | SOURCES                                       | DATE CREATED       |
|------------------|-----------------|-----------------------------------------------|--------------------|
| Destination Port | 143             | abuse.ch Feodo Tracker Botnet C2 IP Blocklist | 05/05/2019 03:11pm |
| Malware Type     | 2019-05-05      | abuse.ch Feodo Tracker Botnet C2 IP Blocklist | 05/05/2019 03:11pm |

## Adding an Attribute to an Object

You can link adversaries to a system object.

1. Locate the Attributes pane on the object details page.
2. Click on the **+ Add Details** link located to the top-right.

The Add Details dialog box opens with the Add Attributes tab selected by default.



3. Select an **Attribute Type** from the Attributes dropdown or enter a new type.
4. Select an existing **Attribute Value** from the dropdown or enter a new value.
5. Select a **Source** from the dropdown or enter a new source.



You can select the + icon to add additional attributes.

6. Select **Add Attributes**.

## Deleting an Attribute from an Object

You can delete an attribute from the object details page.

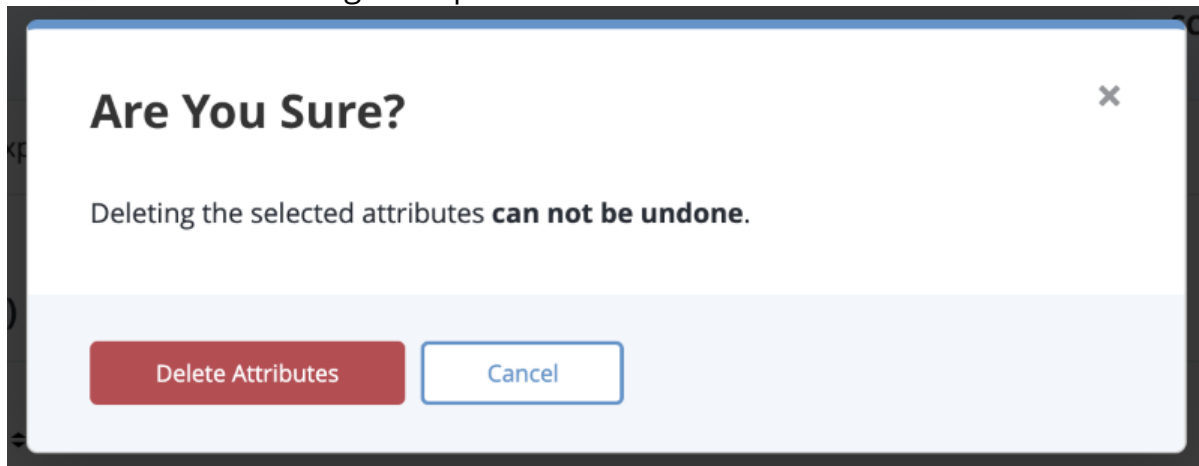
1. Locate the Attributes pane on the object details page.
2. Select the checkbox next to the attribute to delete.



You can select more than one attribute to delete

3. Select **Delete**.

The confirmation dialog box opens.



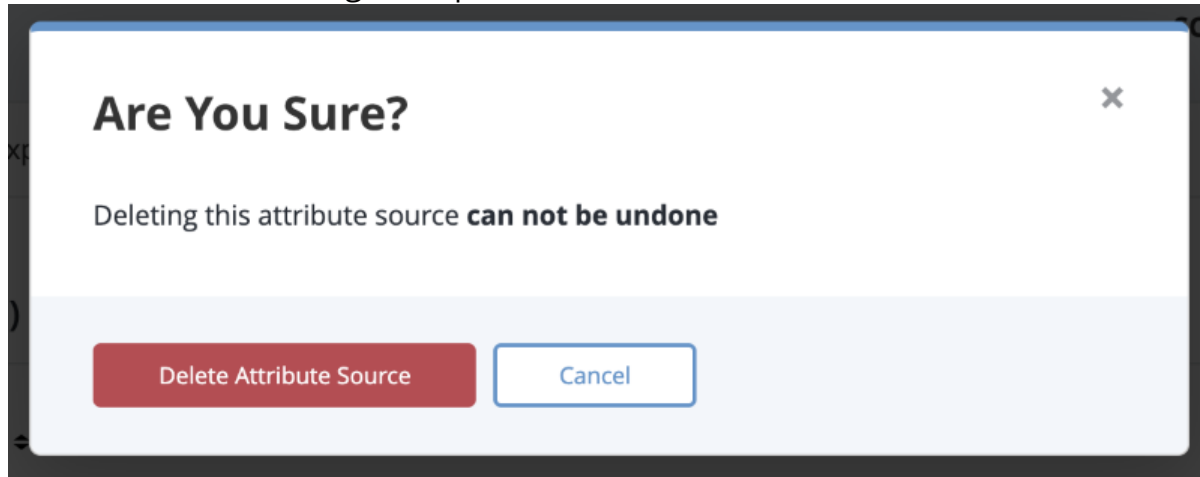
4. Select **Delete Attributes**.

## Deleting an Attribute Source from an Object

You can delete an attribute's source from the object details page.

1. Locate the Attributes pane on the object details page.

2. Select the **X** next to the attribute's source.  
The confirmation dialog box opens.



3. Select **Delete Attribute Source**.

ml>|>



## Sources Pane

The Sources pane displays all sources associated with the system object.

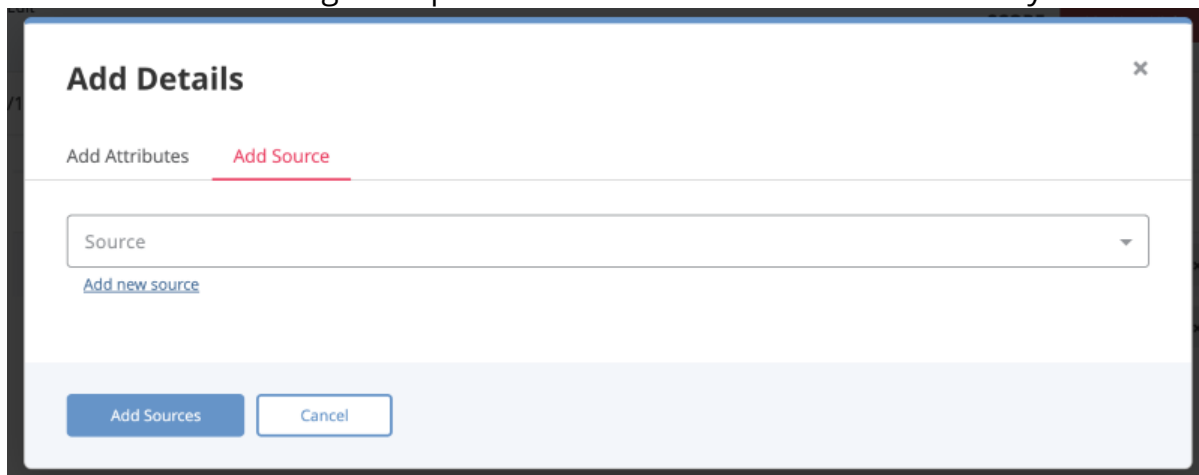
See *Bulk Add Source* section in the [Bulk Actions](#) topic for information on adding a source to a group of system objects.

## Adding a Source to an Object

You can add sources to a system object in its details pane.

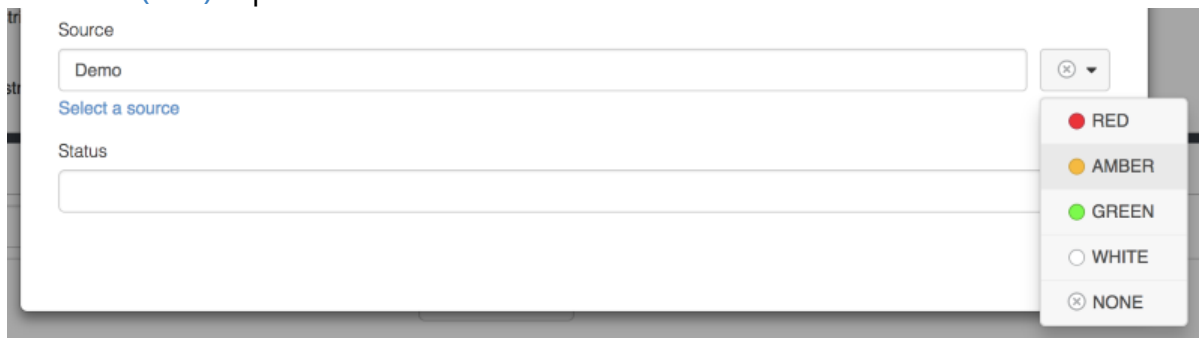
1. Locate the Sources pane on the object details page.
2. Click on the **+ Add** link located to the top-right.

The Add Details dialog box opens with the Add Source tab selected by default.

The screenshot shows a modal dialog titled "Add Details" with a close button (X) in the top right corner. Inside the dialog, there are two tabs: "Add Attributes" and "Add Source", with "Add Source" being the active tab. Below the tabs is a dropdown menu labeled "Source" with a downward arrow. Underneath the dropdown is a link that says "Add new source". At the bottom of the dialog are two buttons: "Add Sources" and "Cancel".

3. Select a **Source** from the dropdown provided. If TLP is enabled, you can override the source-default TLP designation.

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

This screenshot shows the "Add Details" dialog box with the "Add Source" tab selected. The "Source" dropdown menu is open, showing a list of sources with "Demo" selected. Below the source list is a link "Select a source". To the right of the source list is a TLP designation dropdown menu, which is also open, showing options: RED (red circle), AMBER (yellow circle), GREEN (green circle), WHITE (white circle), and NONE (circle with an X). Below the source list is a "Status" field.

4. Select **Add Sources**.

## 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 a Tag to an Object

1. Locate the Tags pane on the object details page.
2. Select the Tags text field and enter the tag.
3. Press **[Enter]** or **[Return]**.



Repeat steps 2-3 to add additional tags.

### Deleting a Tag from an Object

1. Locate the Details pane on the object details page.
2. Select the **X** next to the tag to delete.

# Description Pane

The Description Pane section of the object details page allows you to add a description for the system object.

## Updating the Description of an Object

1. Locate the Description pane on the object details page.
2. Select **Edit**.
3. Make the required changes and select **Save**.

## Relationships Panes

The Relationship section of the object details page displays other system objects that have been related to the current object.

You can link/unlink system objects from relationship panes and perform bulk updates (related indicators pane only). You can click on a related object to navigate to its object details page.



Certain related system objects, such as related indicators, will have additional actions available. See the [Additional Related Object Actions](#) topic.

## Linking a System Object

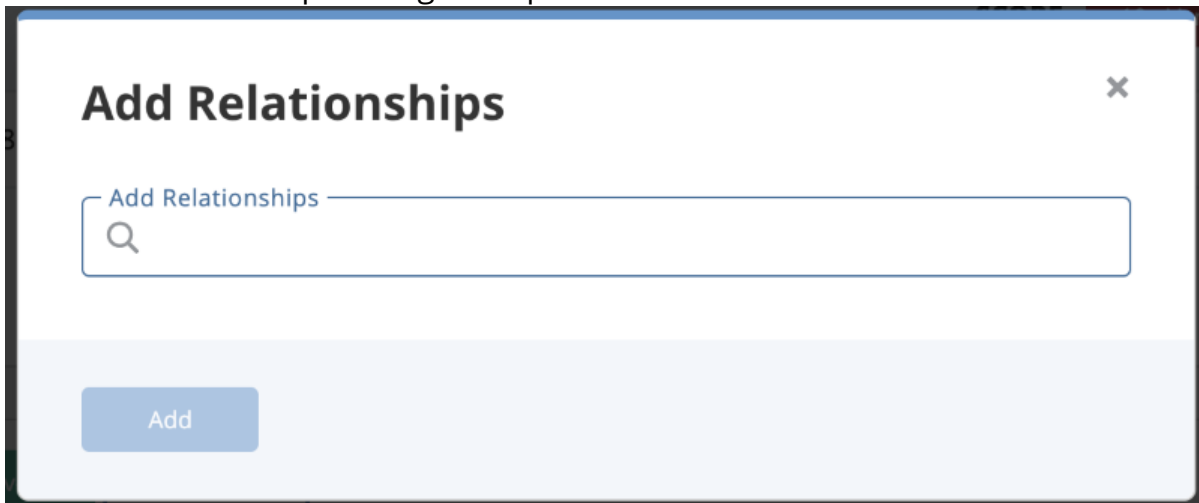
1. Locate the desired system object type pane on the object details page.



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.



The image shows a screenshot of the 'Add Relationships' dialog box. It has a title bar with a close button (X) in the top right corner. Below the title, there is a search input field with the placeholder text 'Add Relationships' and a magnifying glass icon. At the bottom of the dialog, there is a blue button labeled 'Add'.

3. Use the supplied text field to select a file.



Repeat Step 3 to select multiple adversaries.

4. Click **Add**.

## Unlinking a System Object

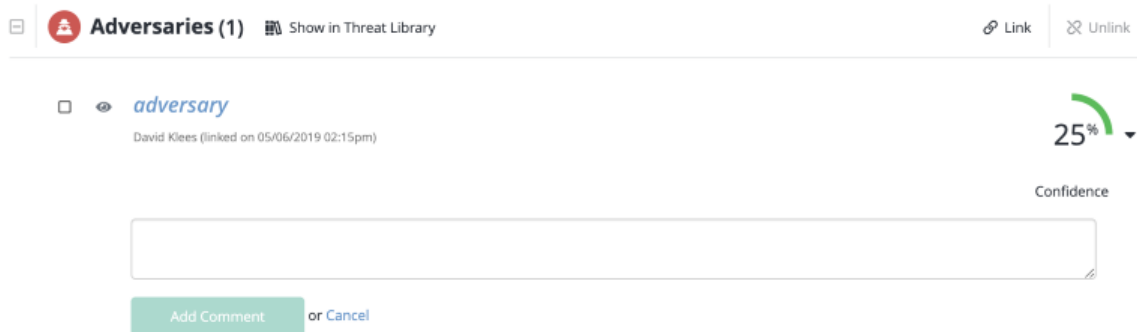
1. Locate the Related <System Object> pane on the object's details page.
2. Select the checkbox(es) next to the system objects to unlink.
3. Select the  Unlink icon.

## 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.



3. Enter a comment.
4. Click **Add Comment**.

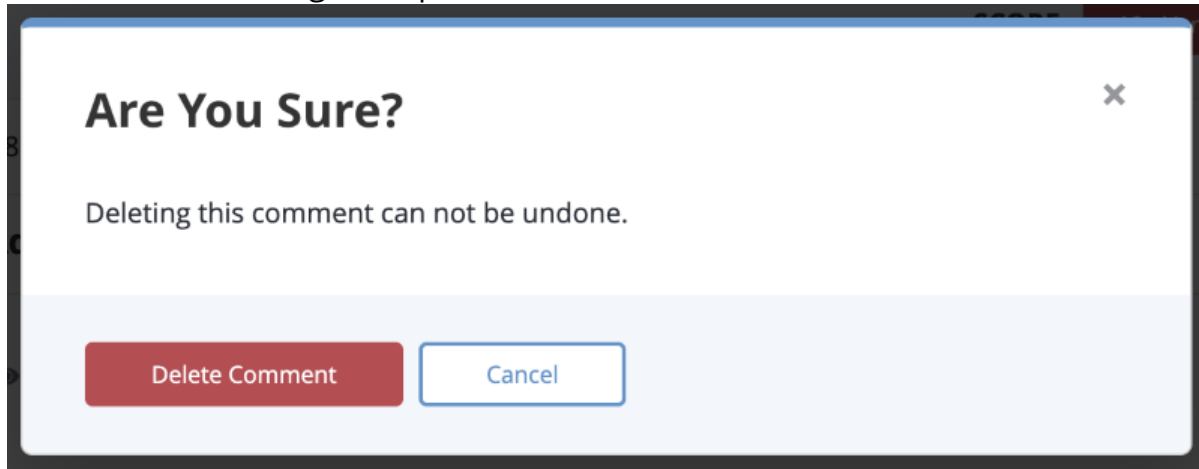
### Editing a related adversary comment

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.

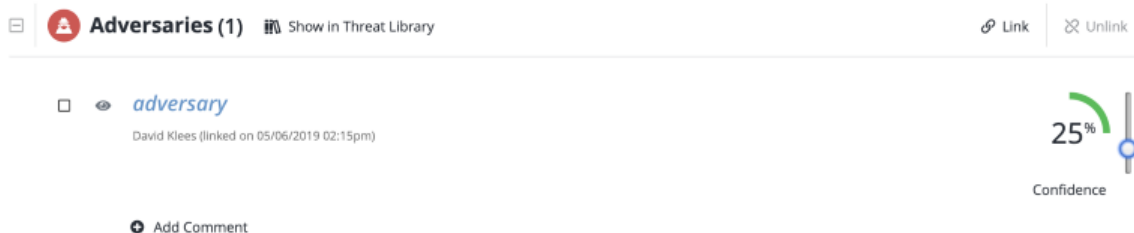


3. Select **Delete Comment**.

## 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 to the right of the adversary, and slide the scale to the desired confidence level.



The confidence level can be set to 0, 25, 50, 75, and 100.

The displayed confidence level will be modified to reflect your selection.

## Related Indicators - Bulk Actions

You can perform bulk updates to linked indicators listed in the Indicators pane of an object.

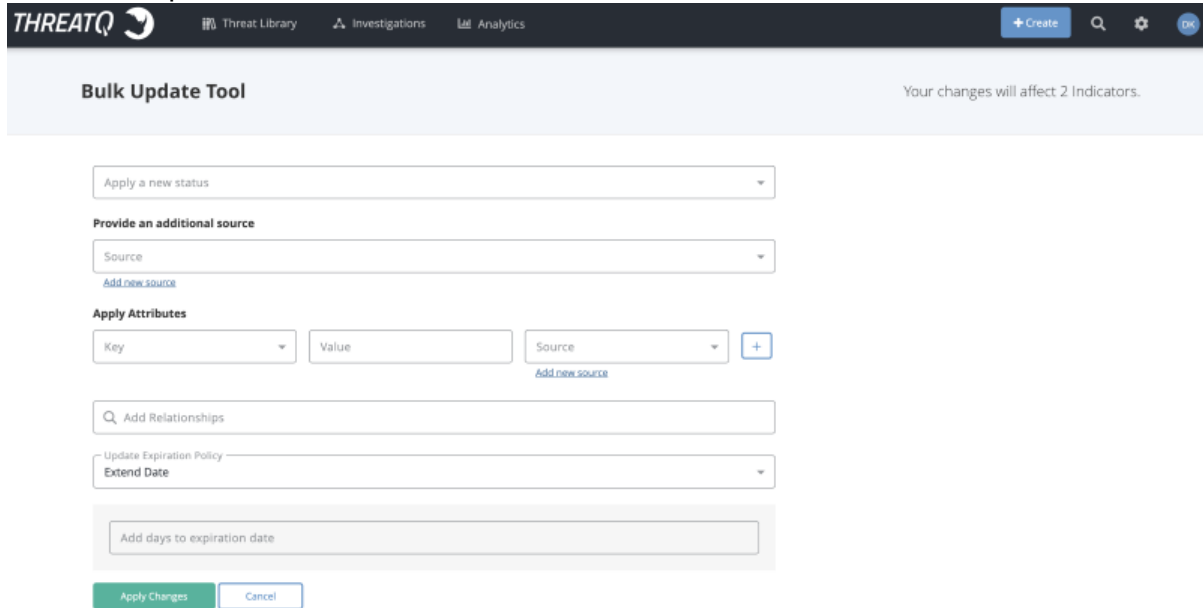
1. Locate the Indicators pane on the object details page.



2. Select the checkbox(es) next to the indicator(s) to update.

3. Select the  Bulk Update icon.

The Bulk Update form loads.



4. Select the desired changes and click **Apply Changes**.

## Comments Pane

The Comments pane allows users to record comments about the system object for other users to see.

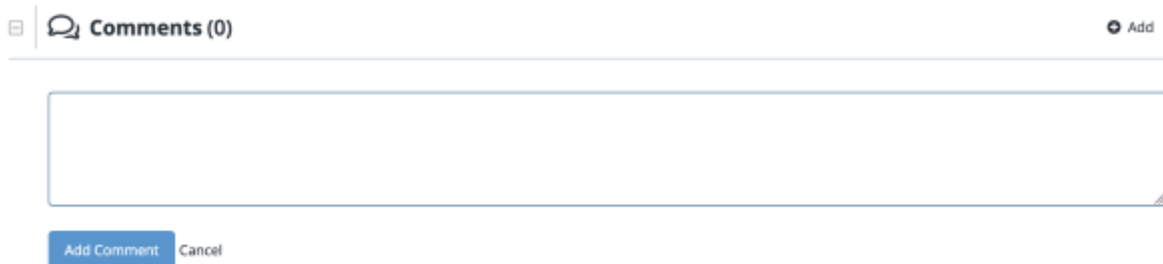
### Adding Comments to an Object



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.



The screenshot shows the 'Comments (0)' pane. At the top right is an 'Add' button. Below it is a large text input field. At the bottom left of the input field are two buttons: 'Add Comment' and 'Cancel'.

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.



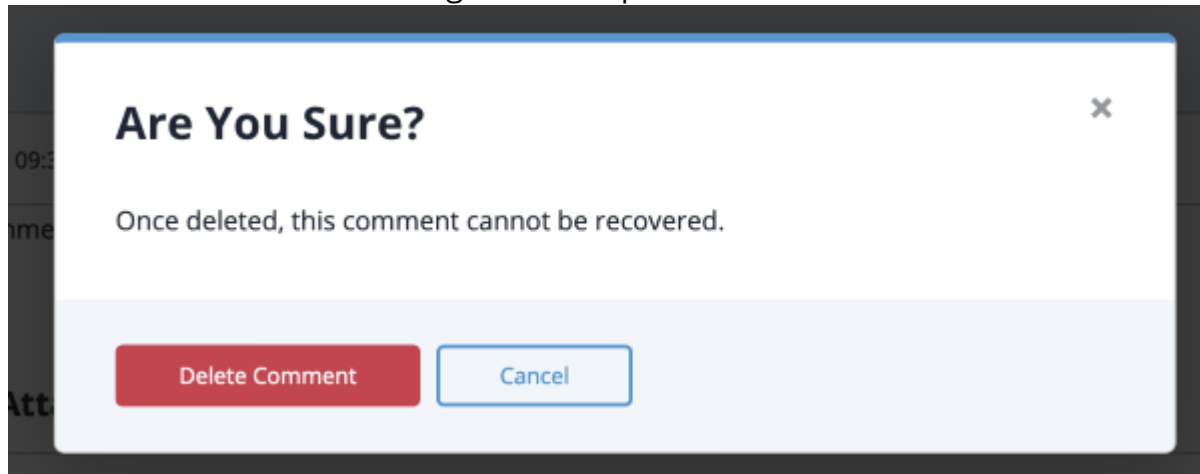
The screenshot shows the 'Comments (1)' pane. At the top right is an 'Add' button. Below it is a comment from 'threatq@threatq.com' with the text 'DDoS-Related Attack possible'. Below the comment is an edit text box. At the bottom left of the text box are two buttons: 'Save Changes' and 'Cancel'.

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.



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 (Adversaries, Files, Events, Indicators, and Signatures) that indicates when a relation of the object has been changed.

### **Is there another raw audit log within the system where events are logged?**

No, there are no other raw audit logs where events are logged.

### **Is there an option in the User Interface to enable all activities to be shown in the Audit Log?**

There is no option in the User Interface to limit or expand the audit log. All entries are pulled for an object when the Audit Log panel is opened. The audit log displays changes to the individual fields of an object; object comments, sources, attributes, and tags; as well as to object links, object link comments, and object link attributes. Additionally, any changes to the score of an Indicator are included.

# Troubleshooting

The following topics provide basic troubleshooting steps and platform information.

- [Generating a Troubleshooting Package](#)
- [SSL Certificates](#)
- [ThreatQ Critical System Processes](#)
- [Data 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. Create the following directory if it does not currently exist:

```
<> mkdir /etc/httpd/ssl
```

2. Copy your .crt and .key files to the ThreatQ file system, into the SSL directory, and then restrict the permissions:

```
<> scp sslfiles.tar.gz [username]@[server].threatq.com:~ sudo cp
~/sslfiles.tar.gz /etc/httpd/ssl/
cd /etc/httpd/ssl tar xzvf sslfiles.tar.gz
chmod 400 yourcert.crt yourkey.key yourca.crt
```

3. SSH to your server and edit the ssl.conf file:

```
<> sudo vi /etc/httpd/conf.d/ssl.conf
```

4. Comment the following lines with a **#** if they exist:

```
<> #SSLCertificateFile /etc/pki/tls/certs/localhost.crt
#SSLCertificateKeyFile /etc/pki/tls/private/localhost.key
```

5. 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)
```

6. Save the file.

7. Restart Apache:

```
<> sudo systemctl restart httpd
```



# ThreatQ 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 /<br>docker.service | <p>The threatq-containers houses three processes:</p> <ul style="list-style-type: none"><li>• memcache</li><li>• websocket</li><li>• rabbitmq*</li></ul> <p>*rabbitmq is used to queue worker jobs and general system messaging such as sending configuration updates, received from the API, to dynamo. In ThreatQ instances prior to 4.39.0, rabbitmq is used for legacy feed data ingestion.</p> |
| 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-<br>dynamo.service             | ThreatQ-dynamo is the process that handles CDF feed runs and the processing of data returned by feed providers.                                                                                                                                                                                                                                                                                     |
| threatq-<br>feeds.service              | The threatq-feeds.service is utilized by ThreatQ instances prior to version 4.39.0 The service controls the feed scheduling and data processing of legacy feed data from 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. |

# Data 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                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>(Date) Created</b>  | This indicates the date when the object was added to ThreatQ.                                                                                                                                                                                                                                                                                                                                                            |
| <b>Due Date</b>        | <p>The due date set by the user for a task.</p> <p>See the <a href="#">Tasks</a> topic for more details.</p>                                                                                                                                                                                                                                                                                                             |
| <b>Expiration Date</b> | <p>This is the expiration date for a system object.</p> <p>See the <a href="#">Indicator Expiration</a> and <a href="#">Automatic Expiration</a> topics for more details.</p>                                                                                                                                                                                                                                            |
| <b>First Published</b> | <p>Varies, depending on the object source:</p> <ul style="list-style-type: none"><li>• 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.</li><li>• If the source contains a publication date, this date indicates the first time the object was published by the feed.</li></ul> |
| <b>Last Modified</b>   | The date and time when object-specific information was last updated, such as updating an indicator's status.                                                                                                                                                                                                                                                                                                             |

**DATE AND TIME  
STAMP****DEFINITION**

Adding/editing/removing associated information, such as attributes, sources, and relationships, does not update the Last Modified time stamp.

**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 the user role group, full 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 permissions to access the User Management functionality. You can only create new user accounts if logged in as one of these roles.



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

## Accessing Your User Account

1. Click on your avatar icon, located to the top-right of the platform, and select **My Account**.

## Accessing Other User Accounts



Only users with Maintenance and Administrative accounts can add, edit, and delete other user accounts.

1. Click on the **Settings** icon  and select **User Management**.

## 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 <b>Change Password</b> 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 graphic.

**2-Step Verification** Optionally, you can enable/disable 2-step verification; see [2-Step Verification](#) for more details.

**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**.
3. Enter the user's **Name**.
4. Optionally, enter the user's **Title**.
5. Select the level of access for the user from the **Group** drop-down menu.

Choose from the following options:

- Maintenance Account
- Administrative Access
- Primary Contributor Access
- Read Only Access

6. Enter the user's **Email** address.

7. Enter a password for the user.
8. Retype the password.
9. Click **Add User**.

## Editing a User



Only users with Maintenance and Administrative accounts can add user accounts.

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

1. Click on the **Settings** icon  and select **User Management**.



To edit your own account, click on your avatar icon and select My Account. Proceed to step 3 below.

2. Click the name of the user whose profile you wish to edit.

The User Profile page loads.

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

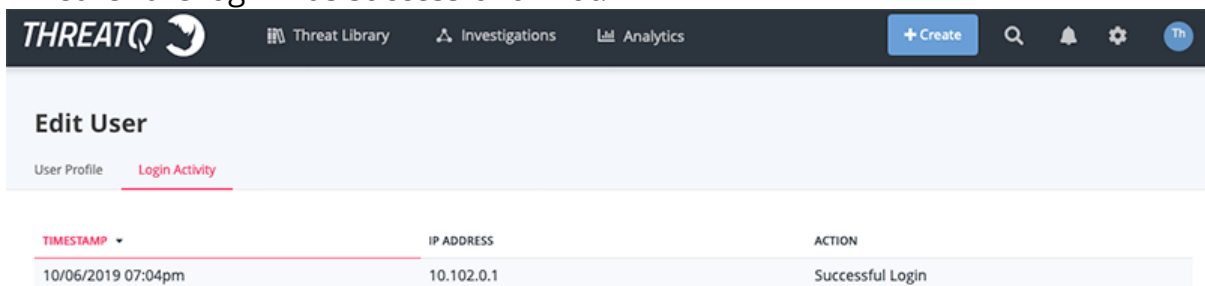
| FIELD | DESCRIPTION             |
|-------|-------------------------|
| Name  | Update the user's name. |



|                     |                                                                                                                      |
|---------------------|----------------------------------------------------------------------------------------------------------------------|
| Title               | Update the user's job title.                                                                                         |
| Email               | You can update the user's email address.                                                                             |
| Password            | You can click on the <b>Change Password</b> 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 graphic.                                                                              |
| 2-Step Verification | Optionally, you can disable 2-step verification; see <a href="#">2-Step Verification</a> for more details.           |

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

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



| Edit User          |                |                  |
|--------------------|----------------|------------------|
| User Profile       | Login Activity |                  |
| TIMESTAMP          | IP ADDRESS     | ACTION           |
| 10/06/2019 07:04pm | 10.102.0.1     | Successful Login |

5. Click **Save**.

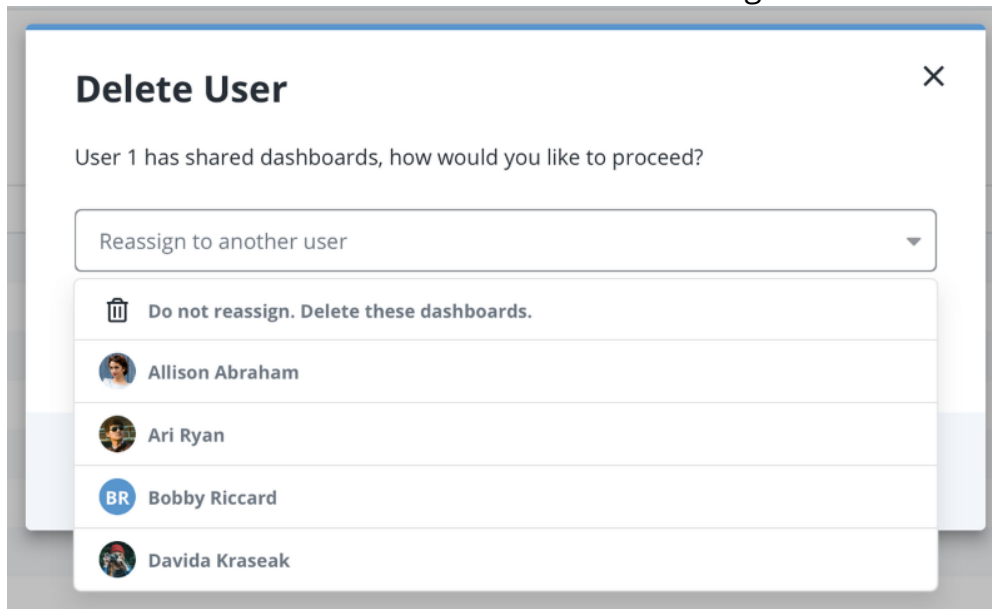
## Resetting User Password from the Command Line

If you have root access to your ThreatQ installation, you can reset any user's password from the command line. See the commands and instructions in the [Resetting User Passwords from the Command Line](#) entry in the Command Line section of this guide.

## Deleting a User

 Deleting a user cannot be undone.

1. From the main menu, choose the **Settings icon > User Management**.
2. Select the user(s) you wish to delete.
3. Click the Delete icon.
4. Confirm the deletion when prompted. If the user has any shared custom dashboards, select whether to delete the dashboards or reassign them to another user.



5. Click **Delete User**.

## Updating User Avatar

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

You can update your avatar by clicking on the avatar icon and selecting **My Account**.

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

The Edit User form will load.

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

3. Click **Save** at the bottom of the page.

# User Roles

The following details the user roles and their associated permissions.

| USER ROLE                         | PERMISSION                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Maintenance Account</b>        | <p>Members have access to the entire ThreatQ user interface and can edit all data.</p> <p><b>Important Notes:</b></p> <ul style="list-style-type: none"><li>• The initial local Maintenance Account, created when installing ThreatQ, can not be deleted</li><li>• Local Maintenance Accounts (manually created within ThreatQ) cannot be migrated to SAML authentication groups</li></ul>                                                                                       |
| <b>Administrative Access</b>      | <p>Members have access to the entire ThreatQ user interface and can edit all data.</p>                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Primary Contributor Access</b> | <p>Members can:</p> <ul style="list-style-type: none"><li>• Edit their own user info</li><li>• Manually create system objects</li><li>• Create and manage ThreatQ Investigations</li><li>• Access Whitelist Management (Data Controls)</li><li>• Perform a basic search</li><li>• Access the Threat Library, object meta data, export search results, and manage Data Collections</li><li>• Create custom dashboards and add shared dashboards to the their user view.</li></ul> |
| <b>Read Only Access</b>           | <p>Members can:</p> <ul style="list-style-type: none"><li>• Access the Threat Library, object meta detail, export search results</li><li>• Add shared dashboards to their user view</li><li>• Load saved Data Collections</li></ul>                                                                                                                                                                                                                                              |



Members cannot edit any data.

# Index

- Adversaries [49](#), [48](#), [47](#), [328](#), [330](#), [329](#), [497](#), [498](#), [499](#), [500](#)
- Air Gapped Data Sync (AGDS) [19](#), [19](#), [22](#), [29](#), [44](#)
- Analytics [46](#)
- Audit Log [504](#)
- Authentication [13](#), [14](#), [281](#), [295](#)
- Automatic Expiration [114](#)
- Bulk Actions [463](#), [465](#), [476](#), [469](#), [474](#), [471](#), [479](#)
- Command Line Interface [71](#), [74](#), [82](#), [79](#), [79](#), [73](#), [80](#), [80](#), [76](#), [76](#), [73](#), [80](#)
- Dashboard (default) [87](#), [86](#), [89](#), [88](#)
- Dashboards (custom) [91](#), [95](#), [93](#), [93](#), [96](#), [97](#), [0](#), [101](#), [100](#), [104](#), [102](#)
- Data Collections [456](#)
- Date and Time Format [323](#), [511](#)
- Events [51](#), [53](#), [54](#), [276](#), [279](#), [277](#), [332](#), [334](#), [333](#)
- Expiration [114](#), [116](#), [117](#), [115](#), [355](#), [354](#), [354](#), [471](#)
- Exports [134](#), [135](#), [138](#), [135](#), [136](#), [133](#), [140](#), [156](#), [161](#)
- Feed Health Notifications [254](#)
- Files [56](#), [58](#), [337](#), [341](#), [339](#)
- Filter Sets [420](#), [424](#), [428](#), [431](#), [434](#), [433](#), [436](#), [438](#), [429](#), [442](#), [446](#), [443](#), [444](#), [445](#), [449](#), [450](#), [451](#), [452](#), [453](#)
- Indicator Defanging [365](#)
- Indicator Parsing Presets [324](#)
- Indicator Scoring [357](#)
- Indicator Status [269](#), [271](#), [270](#), [267](#), [361](#), [360](#)
- Indicator URL Normalization [362](#)
- Indicators [66](#), [63](#), [62](#), [64](#), [60](#), [343](#), [345](#), [344](#), [347](#)
- Integrations [218](#), [222](#), [228](#), [231](#), [236](#), [234](#), [238](#)
- Job Management [245](#)
- LDAP [281](#), [284](#), [289](#)
- Licensing [249](#), [248](#)
- Logging In [16](#), [16](#)
- Navigation [250](#)
- Notifications [253](#)
- Object Details [487](#), [489](#), [490](#), [493](#), [495](#), [497](#), [502](#)
- Proxy [320](#)
- Reports [262](#), [261](#), [261](#), [261](#), [262](#)
- SAML [295](#), [295](#), [301](#), [306](#), [306](#), [309](#), [312](#), [316](#)

|                                                                                                                            |                                                                                                                                                 |
|----------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| Scoring Algorithms <a href="#">121</a>                                                                                     | ThreatQ Backup/Restore <a href="#">68</a>                                                                                                       |
| Scoring Criteria <a href="#">121</a>                                                                                       | ThreatQ Critical System Processes <a href="#">509</a>                                                                                           |
| Search Filters <a href="#">424</a> , <a href="#">442</a> , <a href="#">449</a> , <a href="#">450</a> , <a href="#">455</a> | ThreatQ Platform <a href="#">11</a>                                                                                                             |
| Search Results <a href="#">459</a> , <a href="#">457</a> , <a href="#">456</a>                                             | Traffic Light Protocol (TLP) <a href="#">125</a> , <a href="#">123</a> , <a href="#">123</a> , <a href="#">125</a>                              |
| Searches <a href="#">420</a>                                                                                               | Troubleshooting Packages <a href="#">506</a>                                                                                                    |
| Signatures <a href="#">367</a>                                                                                             | User Accounts <a href="#">514</a> , <a href="#">514</a> , <a href="#">515</a> , <a href="#">518</a> , <a href="#">516</a> , <a href="#">517</a> |
| SSL Certificates <a href="#">507</a>                                                                                       | User Lockout Settings <a href="#">321</a>                                                                                                       |
| STIX <a href="#">371</a> , <a href="#">371</a> , <a href="#">373</a> , <a href="#">386</a>                                 | User Roles <a href="#">520</a> , <a href="#">520</a> , <a href="#">520</a> , <a href="#">520</a>                                                |
| Tasks <a href="#">411</a> , <a href="#">411</a>                                                                            | Whitelists <a href="#">127</a> , <a href="#">130</a> , <a href="#">129</a>                                                                      |
| Threat Library <a href="#">413</a>                                                                                         |                                                                                                                                                 |