

ThreatQuotient



ThreatQ User Guide

Version 5.20.0

September 19, 2023

ThreatQuotient

20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: 703.574.9893

Contents

Warning and Disclaimer.....	15
About the ThreatQ Platform	16
Concept	16
Threat Library.....	16
Adaptive Workbench.....	16
Open Exchange	16
Accessing the Platform	17
About Accessing the Platform	17
User Account Authentication	17
Session Timeout	18
Authentication Methods	19
Changing Authentication Methods	20
2-Step Verification.....	22
Enabling 2-Step Verification	22
Platform Login	23
Local Log In.....	23
Single Sign-On (SSO).....	24
SSL Client Certificate Authentication Log In	24
Air Gapped Data Sync	26
Air_Gapped_Data_Sync_(AGDS).htm	26
System Requirements.....	26
New Installs	26
Air Gapped Data Sync (AGDS) and Investigation Sharing.....	27
Executing Air Gapped Data Sync	28
Running the threatq:sync-export Command	28
Running the threatq:sync-import Command	28
threatq:sync-export	29
Parameters	29
Examples.....	31
Initial Cron for First Time Use	32
Instructions for Larger Data Sets (Starting from the Beginning of Time)	32
Instructions for Larger Data Sets (Starting from a Specified Date)	33
Run Scenarios	33
Export Success.....	33
Export Errors.....	33
Dates	34
Start Date	34
End Date	34
Configuration	34
Default Configuration	34
Cron.....	34
Start Date Provided	35

Output and Sync Report	35
Meta Data	35
Meta Data Objects	35
Objects	36
Object Context	37
Other Data	37
File Output	38
Command Line Output	39
Synchronizations	39
threatq:sync-import	40
Parameters	40
Examples	41
Basic Run	41
Set New created_at Dates on the Write System	41
Increase the Object Limit	42
Initial Setup	42
Run Scenarios	42
Import Success	42
Excluded Files	43
Import Errors	43
Data Processing	43
Basic Table	43
Tables with Pivots	44
File Output	44
threatq sync-import File Output and Sync Report	44
threatq:sync-import Command Line Output	44
Synchronizations	44
Record Handling	45
Hash	45
Initial Creation	45
Finalization	45
Upgrading an Air Gapped ThreatQ Instance	46
Stage 1: Download the Air Gap Upgrade File	46
Stage 2: Upgrade the Air Gapped Box	46
Backup and Restore	48
ThreatQ Backup	48
Backup Options	48
ThreatQ Backup Process	49
ThreatQ Restore	49
ThreatQ Restore Process	50
Command Line Interface (CLI)	51
About the Command Line Interface (CLI)	51
Maintenance Mode	51
Placing the ThreatQ Application into Maintenance Mode	51
Taking the ThreatQ Application out of Maintenance Mode	52
Commands	53
Integration Commands	53

Add/Upgrade CDF	53
View Feed Queues.....	54
Historic Pull	54
System Object Commands	55
Delete Adversary Descriptions.....	55
Merge Attributes	56
Source Consolidation	57
Source Merge.....	57
Convert TLP.....	59
Update TLP Designations	60
Indicator and Signature Statuses Overrides	61
System-Level Commands	62
Airgap Import.....	62
Airgap Export	62
Allow Cross-Origin Resource Sharing for Specific Hostnames	62
Disable Export Logging.....	63
LDAP Diagnostic Searches	63
Auto Configuration MariaDB Command	64
System ThreatQ Purge	65
Reset User Password	65
Dashboards.....	67
About Dashboards	67
Default Dashboard	68
Overview by Intelligence Score.....	68
Incoming Intelligence	69
Watchlist Activity.....	70
Tasks.....	70
Custom Dashboards.....	71
About Custom Dashboards	71
Analytics Dashboard	73
About Analytics Dashboards	73
Adversaries Analytics.....	74
Adversaries Summary Table	74
Adversaries Overlap Table	75
Indicator Distribution Pie Chart.....	76
Events Analytics.....	78
Events History Scatter Plot	78
Events Heatmap.....	79
Files Analytics.....	81
File Type Pie Chart	81
Files Table	82
Indicators Analytics.....	85
Recently Created Indicators Histogram	85
Most Recent 100 Indicators	87
Attributes Table	88
Recent Sources	89
Attack Phases	91

Dashboard Widgets.....	93
Bar Chart	93
Description.....	94
Tips and Tricks for Adding Images to Description Widgets	94
Line Chart.....	95
Count	97
Pie Chart	98
Table	98
Dashboard Management	100
Accessing a Dashboard	100
Add an Existing Dashboard to Your View	101
Creating a Dashboard	102
Editing a Dashboard	104
Deleting a Dashboard.....	105
Reassigning a Dashboard of a Deleted User.....	105
Dashboard Sharing	106
Sharing a Dashboard	106
Updating Dashboard Permissions.....	108
Shared Dashboards of a Deleted User	108
Dashboard Export	109
Creating a Dashboard PDF	109
User View Management	111
Adding a Dashboard to Your View.....	111
Removing a Dashboard from Your View	112
Changing Dashboard Order	112
Data Controls	113
About Data Controls.....	113
Indicator Expiration Policies.....	115
Accessing the Indicator Expiration Page	115
How ThreatQ Calculates Expiration Dates.....	115
Selecting an Expiration Policy per Feed	116
Adding Exceptions.....	117
Applying Expiration Policy Changes to Data	118
Common Expiration Policy Scenarios.....	119
Common Expiration Policy Scenarios - Feed Updates of Indicator Statuses.....	120
Data Retention Policy	122
Accessing the Data Retention Policy Page	122
Creating a Data Collection for the Data Retention Policy.....	123
Creating a Data Retention Policy.....	124
Reviewing Data Retention Policy Performance.....	125
Scoring Algorithms.....	126
Accessing the Scoring Sensitivity Page	126
Scoring Criteria	126
Scoring Tips and Tricks	127
Configuring Your Scoring Algorithm for Indicator Types and Sources.....	127
Configuring Your Scoring Algorithm for Attributes	127
Configuring Your Scoring Algorithm for Adversary Relationships	128

Updating Your Scoring Algorithms.....	128
Traffic Light Protocol (TLP).....	129
Labels	129
TLP Assignment Hierarchy	129
Access TLP Settings	130
Configure TLP Visibility	130
Apply a TLP Label to Source.....	131
Whitelisted Indicators	133
Accessing the Whitelisted Indicator Rules	133
Creating a Whitelisted Rule.....	133
Editing a Whitelisted Rule.....	135
Removing a Whitelisted Rule	136
Exports	138
About Exports.....	138
Managing Exports	139
Accessing the Exports List.....	139
Viewing an Export.....	139
Enabling/Disabling Exports	139
Adding an Export.....	140
Duplicating an Export	143
Editing an Export's Connection Settings	143
Editing an Export's Output Format	144
Deleting an Export.....	144
Output Format Options	145
Customizing the Output Format Template.....	145
Disabling Export Logging.....	145
Adding Special Parameters	145
Adding Differential Flags	160
Adding Parameters to the End of the URL.....	160
Using Logical Operators in Export Filters.....	160
Output Format Templates	162
Adversaries Template	162
Events Template	162
Indicators Template.....	163
Signatures Template	163
Template Variables.....	164
Source Variable	164
Attribute Variable	164
Adversary Variable	164
Attachment Variable	164
Event Variable.....	164
Indicator Variable.....	165
Investigation Variable.....	165
Signature Variable.....	165
Tag Variable	165
Task Variable.....	165
Specific Indicator Export Configurations	166

Integrations Management.....	167
About Integrations Management	167
Integration Types	168
Actions.....	168
Apps.....	168
Configuration-Driven Feeds (CDFs).....	168
Custom Connectors	168
Operations.....	169
About My Integrations.....	170
Accessing My Integrations.....	170
Filtering Your View.....	171
Adding an Integration.....	173
Adding A STIX/TAXII Feed	176
Configuring an Integration	180
Triggering a Manual Run	184
Running an Operation.....	186
Activity Logs (feeds)	188
Accessing a CDF's Activity Log	189
Removing an Integration	191
Removing an Integration.....	191
Disabling an Integration	192
Job Management.....	194
Tips and Tricks.....	194
Accessing the Job Management page:	195
Licensing.....	197
Managing Your ThreatQ License.....	197
Viewing License Status.....	197
Updating a License	198
Navigation Menu	199
Notifications.....	202
About Notifications.....	202
Feed Health Email Notifications.....	203
Configuring Mail Server	203
Enabling Feed Health Notifications.....	205
Notification Center	208
Sharing Notifications	209
Object Management.....	211
About Object Management	211
Indicator Statuses Management.....	212
Indicator Status Assignment.....	212
Indirect Indicator Status.....	212
Protected Indicator Statuses	212
Viewing Indicator Statuses	212
Suppressing Indicator Status Updates	213
Adding an Indicator Status.....	214
Editing an Indicator Status	215
Deleting an Indicator Status	215

Indicator Types.....	217
Event Types.....	219
Viewing Event Types.....	219
Adding an Event Type	221
Editing an Event Type.....	222
Deleting an Event Type	224
Attribute Management.....	226
Selecting an Attribute Key or Value	226
Editing Attribute Keys	227
Merging Attribute Keys	228
Deleting Attribute Keys.....	228
Editing Attribute Values	229
Merging Attribute Values.....	229
Deleting Attribute Values	230
Reports.....	231
Generating Reports	231
Turning Off the Pop-Up Blocker in Chrome.....	232
Report Options	232
Customizing the Report Header	232
Customizing Report Text Colors	232
Adding a Custom Disclaimer to a Report	232
Previewing Report Customization	233
Server Administration.....	234
ThreatQ Monitoring Platform	234
Creating a User Account for the ThreatQ Monitoring Platform.....	234
Accessing the ThreatQ Monitoring Platform	235
Sharing	238
User Permission Levels	238
User Permission Levels and User Roles	239
View-Only Permissions for All Users	239
Sharing Notifications	239
Permission Conversion	240
Permission Levels and Integrations	240
Air Gapped Data Sync (AGDS) and Investigation Sharing	240
System Configuration.....	242
About System Configuration	242
Setting Account Lockout	243
Configuring User Lockout Settings	243
Managing Custom Login Banners	244
Banner Behavior	244
Enabling a Custom Banner	244
Proxy.....	248
Accessing Proxy Configuration	248
Setting Proxy Server Settings for Commands and Custom Connectors	249
Configuring Time and Date Settings	252
Configuring Indicator Parsing Presets	253
Opt In/Out of Product Analytics.....	255

System Objects.....	256
About System Objects	256
Adversaries	259
Adding Adversaries	259
Adding Context	260
Editing Adversaries.....	260
Deleting Adversaries	261
Assets.....	263
Adding Assets.....	263
Adding Context	264
Editing Assets	265
Deleting Assets.....	266
Attack Patterns	267
Adding an Attack Patterns.....	267
Adding Context	268
Editing an Attack Pattern.....	268
Deleting an Attack Pattern	269
Campaigns	271
Adding a Campaign	271
Adding Context	273
Editing a Campaign	273
Deleting a Campaign.....	274
Courses of Action	276
Adding a Course of Action.....	276
Adding Context	277
Editing a Course of Action	277
Deleting a Course of Action	278
Events	280
Adding Events	280
Adding Context	281
Editing Events.....	281
Deleting Events	282
Files	285
Adding Files	285
Adding Context	286
Editing Files.....	286
Deleting Files.....	287
Identities.....	290
Adding an Identity	290
Adding Context	292
Deleting an Identity.....	293
Incidents.....	294
Adding an Incident	294
Adding Context	295
Deleting an Incident	296
Indicators	297
About Indicators.....	297

Adding an Indicator	297
Adding Context	298
Editing Indicators	298
Deleting an Indicator	299
Parsing for Indicators	301
Selecting a File to Parse	301
Step 1 - Import Indicators Settings	303
Step 2 - Organize and Classify	305
Importing Indicators via CSV	310
CSV Columns	310
Parsing a ThreatQ CSV File and Adding Context	312
Troubleshooting	317
Indicator URL Normalization	318
Supported Defanging Techniques	321
Indicator Expiration	323
Ways an Indicator can Expire	323
Changing the Expiration Date for an Individual Indicator	324
Changing the Expiration Date for Multiple Indicators	324
Indicator Scoring	325
Building a Scoring Algorithm	325
Setting a Manual Indicator Score	325
Indicator Status	327
Default Statuses	327
Custom Statuses	327
Changing the Status of an Individual Indicator	327
Changing the Status for Multiple Indicators	328
Intrusion Sets	329
Adding an Intrusion Set	329
Adding Context	330
Deleting an Intrusion Set	331
Malware	332
Adding a Malware Object	332
Adding Context	333
Editing a Malware Object	333
Deleting a Malware Object	334
Reports	336
Adding a Report	336
Adding Context	337
Editing a Report	337
Deleting a Report	338
Signatures	340
Adding a Signature	340
STIX	343
About STIX	343
ThreatQ STIX Object Types	343
Parsing a STIX File for Indicators	343
STIX 1.1.1, 1.2 Data Mapping	346

STIX 2.0 Data Mapping	359
Tasks	384
Assigning a Task.....	384
Managing Tasks	384
Tools.....	386
Adding a Tool	386
Adding Context	387
Editing a Tool.....	387
Deleting a Tool	388
TTP.....	389
Adding a TTP.....	389
Adding Context	390
Editing a TTP.....	390
Deleting a TTP	391
Vulnerabilities.....	393
Adding a Vulnerability.....	393
Adding Context	394
Editing a Vulnerability	394
Deleting a Vulnerability.....	395
Threat Library	397
About Threat Library	397
Managing Your Library View.....	399
Selecting Object Type View	399
Managing Library Columns	401
Selecting System Objects	401
Basic Search.....	403
Performing a Basic Search	403
Wildcards and Symbols in Searches	405
Creating an Object During a Basic Search	405
Building Searches with Filter Sets.....	407
About Building Searches with Filter Sets	407
Adding Filter Sets.....	407
Deleting Filter Sets.....	409
And/Or Order of Operations.....	409
Context Filters	412
Filtering by Author.....	412
Filtering by Attribute	412
Using Multiple Attribute Filters	413
Filtering by CIDR Block Range	416
Filtering by Value Contains.....	417
Filtering by List of Indicators.....	417
Filtering by Keyword.....	419
Filtering by Relationship	420
Filtering by Relationship Criteria	422
Filtering by Score	424
Filtering by Tags	425
Filtering by Source.....	426

Filtering by TLP	427
Date Filters	430
Filtering by Date Created	430
Filtering by Last Modified	430
Filtering by Published Date	431
Filtering by Source Ingest Time	433
Filtering by Expiration Date	434
Status Filters	437
Filtering by Status	437
Tasks Filters	438
Filtering Tasks by Assignment	438
Filtering Tasks by Due Date	439
Filtering Tasks by Priority	440
Filtering Tasks by Reported By	440
Type Filters	443
Filtering by Object Type	443
Managing Search Results	444
Saving Searches as Data Collections	444
Loading Data Collections	445
Modifying a Data Collection	446
Copying a Data Collection	447
Renaming a Data Collection	447
Sharing Data Collections	447
Removing a User's Access to a Data Collection	449
Deleting a Data Collection	449
Exporting Search Results to CSV	450
Exporting Search Results to STIX	451
Bulk Actions	453
Bulk Add Source	454
Bulk Add/Remove Attributes	457
Bulk Add/Remove Attribute Scenarios	459
Bulk Add/Remove Tags	460
Bulk Change Expiration Date	462
Bulk Expiration Change Scenarios	464
Bulk Delete	465
Bulk Add/Remove Relationships	465
Bulk Status Change	467
Object Details	469
About Object Details	469
Adding/Removing an Object to the Watchlist	474
Actions Menu	475
Context Panes	477
About Context Panes	477
Sources Pane	478
Tags Pane	481
Description Pane	482
Spearphish Details Pane	483

Relationships.....	484
About Relationships Panes	484
Additional Related Object Actions	486
Adding a comment to a related adversary	486
Editing a related adversary comment	486
Deleting a related adversary comment.....	486
Related Adversaries - Confidence Level	487
Related Indicators - Bulk Actions.....	487
Related Investigations - Request Access	487
Comments Pane.....	489
Adding Comments to an Object	489
Editing Comments for an Object.....	489
Deleting Comments from an Objects	489
Audit Log.....	491
User Management	492
About User Management	492
Managing User Accounts	493
Accessing Your User Account	493
Accessing Other User Accounts.....	493
User Account Properties	493
Adding a User.....	494
Editing a User	495
Resetting User Password from the Command Line	498
Deleting a User	498
Updating a User Avatar	499
User Roles	500
2 Step Verification.....	501
LDAP Authentication	502
About LDAP Authentication.....	502
Required Information for Creating LDAP Authentication.....	503
Switching LDAP Connections	503
Anonymous Bind	504
Configuring Secure LDAP	506
Authenticated Bind	508
SAML Authentication	512
About SAML Authentication	512
Configuring SAML	512
Setting Up LDAP Users/Groups for SAML	517
Adding ThreatQ as a Service Provider	523
ADFS 2016	523
Azure AD	525
Google G Suite	529
Okta.....	533
SSL Client Certificate Authentication	536
About SSL Client Certificate Authentication.....	536
Requirements.....	536
Configuring Client Certificate Authentication.....	536

Adding a User's Certificate Fingerprint - User Profile.....	538
Adding Your Certificate Fingerprint - Login Page.....	538
Using Certificate Authentication to Log In	539
Managing Certificate Files.....	540
Disabling SSL Client Certificate Authentication.....	540
Removing a Certificate File	540
Replacing a Certificate File	541
Managing Certificate Fingerprints	542
Updating Certificate Fingerprints.....	542
Removing Certificate Fingerprints.....	542
Troubleshooting SSL Client Certificate Authentication	543

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 © 2023 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.

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.

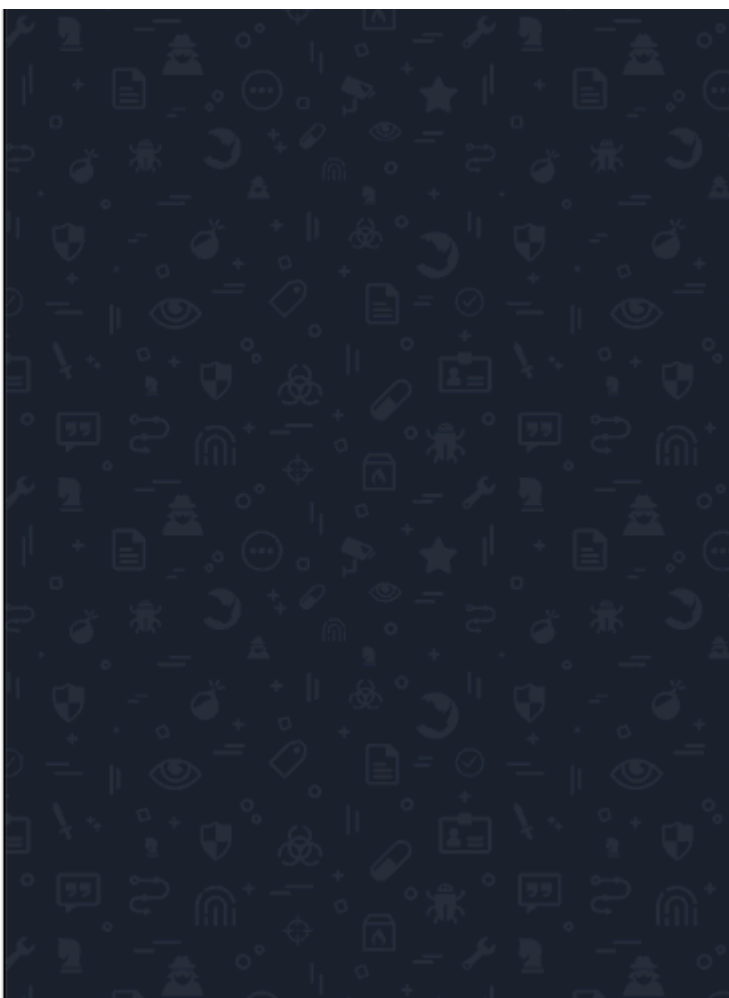
Accessing the Platform

About Accessing the Platform

ThreatQ allows you to securely manage access via user accounts with logins and password.



Copyright © 2023 ThreatQuotient, Inc.



After you log in, you can use the main menu to navigate ThreatQ. Within ThreatQ, your view and options are based on your [user account settings](#) and [permissions](#).

User Account Authentication

User accounts can be authenticated locally within ThreatQ or externally using [LDAP](#), [SAML](#), or [SSL Client Certificate](#) authentication. In addition, you can implement [2-Step Verification](#) at the user account level for additional security. Once enabled, the user needs a login, password, and authentication code to access ThreatQ.

Session Timeout

User sessions time out after sixty minutes of inactivity. Users with Maintenance Account and Administrative Access can update this setting or, disable session timeouts for a specific user. 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 session time by default. However, one can be configured for the account.

Authentication Methods

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

METHOD	DESCRIPTION	REFERENCE
Local Authentication	User accounts are created and maintained manually within the platform. Username, passwords, and permission roles are configured within ThreatQ. Administrators can edit a user's profile including email, password, and permission role in ThreatQ. Local users log in using the local user login method for the ThreatQ platform.	• About User Management • About Accessing the Platform
2-Step Verification	Adds an extra layer of security by requiring a security code in addition to a login and password.	• 2-Step Verification
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, user accounts cannot be modified within the ThreatQ platform (User Management page). LDAP users log in using the local user login method for the ThreatQ platform.	• About 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, user accounts cannot be modified within the ThreatQ platform (User Management page). SAML does not allow user role mapping for maintenance accounts.	• About SAML Authentication

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

Changing Authentication Methods



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

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. 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.
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 the About LDAP Authentication topic for details on this setup process.
LDAP	Local	Contact ThreatQ Support .

CURRENT METHOD	NEW METHOD	DETAILS
LDAP	SAML	LDAP must be disabled before enabling SAML. No account updates are required if the unique account identifier for LDAP was the user's email address. The LDAP group that is mapped to the ThreatQ Maintenance role will have to be mapped to different user role as SAML does not allow maintenance account mapping.
SAML	LDAP	SAML must be disabled before enabling LDAP. No account updates are required if the unique account identifier for SAML was the user's email address.
SAML or LDAP	SSL Client Certificate Authentication	Contact ThreatQ Support .
Local	SSL Client Certificate Authentication	See SSL Client Certificate Authentication .
SSL Client Certificate Authentication	Local	See Managing Certificate Files .

2-Step Verification

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



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

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

Enabling 2-Step Verification

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

What to do next

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

Platform Login

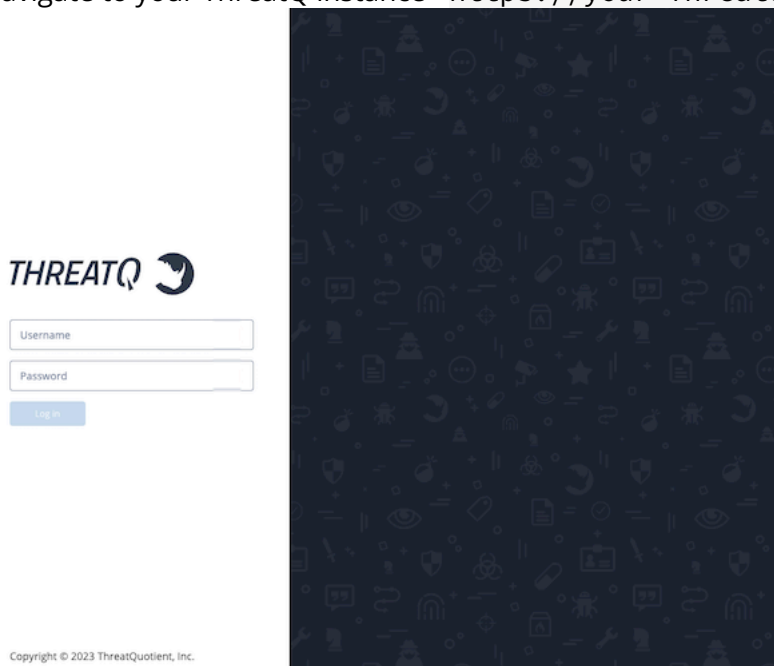
Log in steps vary based on the authentication methods enabled for your instance and/or user account.

AUTHENTICATION METHOD	LOGIN PROCESS
Local or LDAP	Local Log In
SAML	Single Sign-On (SSO)
SSL Client Certificate	SSL Client Certificate Authentication Log In

Local Log In

The local login process applies to instances using local or LDAP authentication.

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



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

Single Sign-On (SSO)

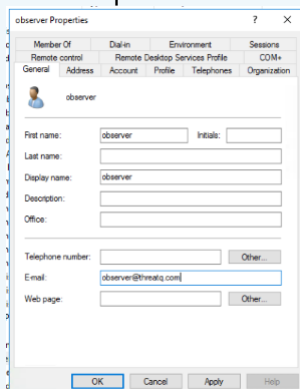


At this time, ThreatQ does not support IdP-initiated SSO, where a user can log in directly from an SSO provider's portal such as Okta's Portal. Users utilizing SSO must click the **Log In Using SSO** button on the ThreatQ landing page to authenticate with their IdP.

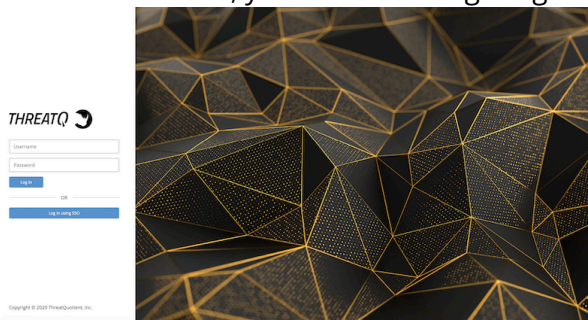
Users using SAML authentication use this log in method.



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



1. Navigate to your ThreatQ instance - <https://your-ThreatQ-web-ip-address>.
If SAML is enabled, you will see a Single Sign-On option.



2. Click the **Log in Using SSO** button.
Navigate to your third-party authenticated site to log in. Once that has been completed, you are automatically sent back to the ThreatQ instance.

SSL Client Certificate Authentication Log In



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

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

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



OR

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

Air Gapped Data Sync

Air_Gapped_Data_Sync_(AGDS).htm

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 does not occur on the air gapped installation.

ThreatQ recommends that you consult with ThreatQ Support or a Threat Intelligence Engineer prior to performing an Air Gapped Data Sync.

An 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 before performing an import.



Do not deviate from or change the following deployment details and configurations without first consulting ThreatQuotient. Any deviation from ThreatQuotient recommended settings could result in system and platform instability, may render the system non-operational, and is 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.

New Installs

See the ThreatQ V5 Platform Air Gapped Installation Guide for detailed information on new installs of ThreatQ V5 on an air gapped device.

Air Gapped Data Sync (AGDS) and Investigation Sharing

The AGDS export process does not include Data Collections or Dashboards, but it can include Investigations if you add the following parameter:

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

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

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

Executing Air Gapped Data Sync

Air Gapped Data Sync is a two stage process. First, you export data from your source ThreatQ instance. Then, you import this data into your target ThreatQ instance.

Running the `threatq:sync-export` Command

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

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

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

3. Run the following command appended by the necessary [parameters](#):

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

4. Review the Output and Sync report; see [threatq sync-imprt File Output and Sync Report](#).

threatq:sync-export

This export command pulls all objects, object context, tags, and object links from the source ThreatQ installation and then stores 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
<code>--target</code>	Required value. Target directory where the output file should be placed. Default: /tmp Example: <code>--target=/my/directory</code>
<code>--start-date</code>	Required value. The start date for data selection. Example: <code>--start-date="2018-01-01 00:00:00"</code>
<code>--end-date</code>	Required value. The end date for data selection. Applies only to objects, not object context or object links. Example: <code>--end-date="2018-01-02 00:00:00"</code>
<code>--include-deleted</code>	Determines whether objects that have been soft-deleted are included in the result set. Options are Y(es) or N(o). Default: N Example: <code>--include-deleted=Y</code>
<code>--include-investigations</code>	Required value. Determines whether Investigations and Tasks are included in the result set. Options are Y(es) or N(o). Default: N

PARAMETER	EXPLANATION
	Example: <code>--include-investigations=N</code>
<code>--meta-only</code>	Optional value. If present, tells the command to only include meta data (no object data) in the result set.
<code>--memory-limit</code>	Required value. Sets the PHP memory limit in megabytes or gigabytes. Default: 2G Example: <code>--memory-limit=4G</code>
<code>--object-limit</code>	Sets the limit on the number of objects selected at a time. ThreatQuotient recommends that you set the limit to a number smaller than the default (50,000) on boxes with very large data sets. Default: 50,000 Example: <code>--object-limit=10000</code>
<code>--ignore-file-types</code>	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: <code>--ignore-file-types="Malware Analysis Report"</code> Example: <code>--ignore-file-types="Malware Analysis Report,Malware Sample"</code>
<code>--sources</code>	Filters objects produced in the sync by the sources they include, allowing the user to send out a subset of data that contains a specific source.  For objects with multiple sources, other sources are included in the filter if the object contains the user-specified source(s). Multiple sources are also supported in search parameters. Existing CRON Runs: Use the <code>initial-start-date</code> option to avoid pulling all historical data.

PARAMETER

EXPLANATION

Example: `--sources="Black Source"`

`--include-all-relationships`

Exports all related data for an object if its source matches the `--sources` parameter value. If so, the command exports the primary object's relationships to any object on the system regardless of the sources of the related objects and/or the source that created the relationships.

Example: `--sources="Black Source" --include-all-relationships`

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 pulls all objects in the system (with the exception of Investigations, Tasks, and soft-deleted Objects). The output appears in `/tmp`.

Meta Data Only

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

This example pulls 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 pulls 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 pulls all objects, but excludes the physical files attached to any File objects with the type Malware Sample. The File objects themselves (as well as their context and relationships) are still 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 searches for a previous synchronization record with the same hash (comprised of the three options provided). If any hash matches are found, the run uses 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
- Investigations/tasks included (Y/N)
- Deleted objects included (Y/N)

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.

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 is no longer 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.

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 is no longer necessary.

Run Scenarios

Export Success

When a run of this command completes successfully, a tarball of data appears in the target directory you specified (or `/tmp` by default). A report file describing the run is available in the data tarball, under the `/sync` directory. There is also a record in the database synchronizations table for the run.

Export Errors

If a run of this command fails before completion, the tarball is not created. There is 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 appears in this directory under `/sync`. Error messages do not appear in the report file. However, they 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 Configuration

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 defaults 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 is 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 is 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 is 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 is honored. However, if the `--target`, `--include_deleted` and `--include_investigations` options are also included, a Cron check against the hash of these three options does **not** occur. The start date provided is included in `config_json` as the **manual_start_date** so that the run does not collide with any Cron-related runs.

If a "beginning of time" run is necessary, use the option as `--start-date="1970-01-01 00:00:00"`.

Output and Sync Report

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

Meta Data

Meta data is transferred with every run of this command by default. You can specify that only meta data (no object data) should be pulled in a run by using the `--meta-only` option.

Meta data includes information about Sources, Attributes, Tags, as well as Object Statuses and Types (both seeded and user-provided).

While meta data like Connectors and Operations are included in this list, they are not installed on the target ThreatQ installation as part of the air gapped data sync process. They are only placed in the requisite tables for use as Sources of Objects that are transferred. The same is true of any Users that are copied - these will not be enabled Users on the target installation; they will be transferred as disabled.

Meta Data Objects

- Attributes
- Clients
- Connectors
- Connector Categories
- Connector Definitions
- Content Types
- Groups
- Investigation Priorities
- <Object Type> Statuses
- <Object Type> Types
- Other Sources
- Operations
- Sources
- Tags
- TLP
- Users

Objects

This command covers any objects installed on the system by default, and any custom objects that have been installed by the user. The only objects that can be excluded are Investigations and Tasks (using the `--include-investigations` command line option).

 Custom Objects that are installed on a source ThreatQ installation that have NOT been installed on a target ThreatQ installation will NOT be installed by the air gapped data sync process. If an object is included in the export data, but is not found on the target, it will be ignored.

Default Objects:

- Adversaries
- Attachments (Files)
- Events
- Indicators
- Signatures
- Campaigns
- Courses of Actions
- Exploit Targets
- Incidents
- TTPs

Storage:

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

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

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

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

- adversaries/adversaries_obj_0.csv
- adversaries/adversaries_obj_attributes_0.csv
- adversaries/adversaries_obj_comments_0.csv
- adversaries/adversaries_obj_investigation_timelines_0.csv
- adversaries/adversaries_obj_object_links_dest_0.csv
- adversaries/adversaries_obj_object_links_src_0.csv
- adversaries/adversaries_obj_sources_0.csv

- adversaries/adversaries_obj_tags_0.csv

Object Context

The date range for queries on Object Context tables uses the `updated_at` date column, with the exception of Adversary Descriptions, which uses the `created_at` date column.

Adversary Descriptions are handled as part of the Object Context gathering process. The `adversary_descriptions` table is queried using the `created_at` date column, and the entirety of the `adversary_description_values` table is pulled, as it does not 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`

Example

```
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).

threatq:sync-import

This import command processes 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`, all parameters for the `threatq:sync-import` command will use the default value unless otherwise defined by the user.

PARAMETER	EXPLANATION
<code>--file</code>	Required value. File path to the tarball created by the <code>threatq:sync-export</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. Options are Y(es) or N(o). Default: Y Example: <code>--keep-created-at=N</code>
<code>--object-limit</code>	Integer value used as the limit for the number of objects updated or inserted at a time. 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>

PARAMETER

EXPLANATION

`--memory-limit`

Sets the PHP memory limit in megabytes or gigabytes.

Default: 2G

Example: `--memory-limit=4G``--override-description`

Determines whether or not the descriptions on existing objects on the target ThreatQ installation are be updated. If an existing object has a NULL description, it will be updated regardless of the use of this flag.

Default: Y

Example: `--override-description=N`

Examples

This command should be run from inside the `/var/www/api` directory.

Basic Run

```
sudo ./artisan threatq:sync-import --file=/tmp/
tqSync-19-01-16-1547660837-8345.tar.gz
```

This example processes 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 is 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 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 processes 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 is left alone in the case of object updates, and changed to the current date 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 processes 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 uses the default setting of Y(es) and `created_at` dates are retained from the Source 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 or later, several tables 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 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. Put the ThreatQ platform into maintenance mode:

```
php artisan down
```

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

Import Success

When a run of this command completes successfully, a report appears in the directory the command was run in (`/var/www/api`). There is also a record in the database synchronizations table for the run. Both of these 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 are not available during the import of those objects. If the import command detects that a file is missing from the export tarball, it creates 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 is 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.

Import Errors

If a run of this command fails before completion, error messages do not appear in the report file - though they do 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 must be restarted and will run through all the data again. Any data from the tarball that was written during the previous failed run is updated (rather than inserted again), meaning the end result is the same - all data is 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 a copy of a base table, with column structure maintained but indexes excluded. Indexes are added to unique columns on sync tables (which are 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 is generated in the `/var/www/api` directory (where the command is run). This file is 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 is similar to the output in the Sync Report.

Synchronizations

SYNCHRONIZATIONS	DESCRIPTION
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.

SYNCHRONIZATIONS	DESCRIPTION
<code>finished_at</code>	The date and time the command run completed.
<code>config_json</code>	A JSON representation of the command run configuration.
<code>report_json</code>	A JSON representation of the command run parameters (command line options, object counts, tables created, etc).
<code>pid</code>	The process ID of the command run.
<code>hash</code>	Unique identifier for a command run (MD5 hash of the <code>config_json</code> column).
<code>created_at</code>	The date and time the Synchronization record was created.
<code>updated_at</code>	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).

Upgrading an Air Gapped ThreatQ Instance

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



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

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



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

Stage 1: Download the Air Gap Upgrade File

To download the air gap upgrade file from a browser:

1. Log into <https://install.threatq.com/> using your YUM credentials.
2. Locate and download the appropriate air gap upgrade file.

File Name Format:

<version>-platform.tar.gz

Example:

5.6.1-platform.tar.gz

3. Open the CLI of the device to upgrade and copy the upgrade file to `/root/` using the SCP client of your choice.
4. Return to the CLI of the device and confirm that the upgrade file is present.

To download the air gap upgrade file via curl:

1. Run the following command:

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

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

Stage 2: Upgrade the Air Gapped Box

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

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

Example:

```
tqadmin platform upgrade -v 5.6.1 -z
```

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

Backup and Restore

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.

Backup Options

ThreatQ supports three backup options:

- A standard backup that includes the threat intelligence data index.
- A backup that excludes the threat intelligence data index
- An online backup that excludes the threat intelligence data index

An online backup backs up your database without performing a Solr backup. This allows users to work in the ThreatQ instance as the backup runs.



The online backup process takes longer to complete and generates a larger backup file.

When you restore from an online backup the following message prompts you to decide when to perform a Solr re-index.

Do you want to re-index Solr now? If not, you may do this manually later. [y/n]

Since an online backup allows users to remain working in the system, you may encounter the following issues when restoring from an online backup file:

- If a CDF was running during the backup, the feed run is listed as `Completed with errors/Run failed to complete`.
- If a bulk job was running, the job remains stuck in progress in the Job Management page.

ThreatQ Backup Process

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 the threat intelligence data index, run the following command:

```
sudo php artisan threatq:backup
```

- To create a backup that excludes the threat intelligence data index, run the following command:

```
sudo php artisan threatq:backup --exclude-solr
```

- To create an online backup that excludes a backup of the threat intelligence data index, run the following command:

```
sudo php artisan threatq:backup --online
```

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.

ThreatQ Restore Process

To restore from a ThreatQ backup, perform the following procedure on the target ThreatQ instance.

1. Complete the first boot process on the new host by navigating to its IP address in a web browser and entering your credentials. If this step is not completed, the remaining steps are not successful.
2. SSH to the command line and elevate your user privileges to root or sudo.
3. Verify that you have the necessary utilities in place by running:

```
yum install policycoreutils-python-2.2.5-20.el7.x86_64
```

4. Change directory to **/var/www/api**.
5. Issue the following commands: **5x command**

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

4x commands

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

php artisan threatq:update-events
```

6. If prompted, provide the **root mysql** password you configured during first boot.
7. If you are restoring from an online backup or if the backup file does not include the intelligence data index required for improved search performance, the following message prompts you to decide when to perform a Solr re-index.

Do you want to re-index Solr now? If not, you may do this manually later. [y/n]



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)

About the 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 automatically place the ThreatQ application into maintenance mode when executed. The Help Center topics for these commands indicates 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 is now 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 is now out of maintenance mode.

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


Commands

This topic contains a list of commands you can execute from ThreatQ's command line interface (CLI). These commands are grouped by their primary area of impact, Integration, System Object, or System-wide.

Integration Commands

Add/Upgrade CDF



ThreatQuotient recommends that you use the user interface to [add or upgrade integrations](#).

Use the steps below to add or upgrade a Configuration Driven Feed (CDF). The command creates connectors for each feed defined in the feed definition file.

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 **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.

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 updates both fields and links the feed to the designated category. ThreatQ confirms that the defined category exists before completing the update command. If the category does not exist, ThreatQ does 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.
```

ThreatQ recommends 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
```

View Feed Queues

Before upgrading a feed, ThreatQ recommends that you allow the previous implementation of the feed to complete processing downloaded data to avoid any data loss. The `threatq:list-queues` command allows you to confirm that the feed's 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.

Historic Pull

If not called out specifically in Historic Feed Pulls, use the following commands to run historic pulls for most connectors, including most TAXII feeds.

1. Run the following command to determine the feed name (\$FEEDNAME):

```
tqconnector -h
```

2. Take note of the desired feed name.
3. 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
```

System Object Commands

Delete Adversary Descriptions

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



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

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

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

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

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

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

Example:

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

Merge Attributes



The [Attribute Management](#) page also allows you to merge attribute keys.

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

You can add the `--source` parameter to only merge attributes that have a specific source(s). If the source identified in the command does not exist, or the parameter is not included, the command merges all OLD-NAME attributes into MERGE-NAME.



If the MERGE-NAME attribute in the command does not exist, it is automatically created upon executing the command.

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

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

3. Place the application into maintenance mode - see the [Maintenance Mode](#) topic.
4. Run the following command:

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



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

5. Bring the application out of maintenance mode - see the [Maintenance Mode](#) topic.

Example - Merge Attribute without using `--source`

The attribute Cuountry is merged into the Country attribute. So if you have an any instance of this attribute name (with value), Cuountry: US, on an object, after running the command, the attribute value would appear as Country: US on that object.

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

Example - Merge Attribute using `--source`

The attribute Cuountry, if it has a source of CrowdStrike, is merged into the Country attribute. So if you have an instance of this attribute name (with value), Cuountry: US, on an object, after running the command, the attribute value appears as Country: US on that object.

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

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

The attribute `Cuentry`, if it has a source of `CrowdStrike` or `McAfee ATD`, is merged into the `Country` attribute. So if you have an instance of this attribute name (with value), `Cuentry: US`, on an object, after running the command, the attribute value appears as `Country: US` on that object.

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

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 is deleted and source changes are 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 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.
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.

EXAMPLE SCENARIO	DETAILS
	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. 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.

Convert TLP

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

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

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

3. Place the application into maintenance mode - see the [Maintenance Mode](#) section.
4. Run the following command:

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

5. Bring the application out of maintenance mode - see the [Maintenance Mode](#) section.

Use Scenarios:

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

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

Object has a single valid TLP Attribute

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

Object has multiple TLP Attributes

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

Update TLP Designations

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



See [Traffic Light Protocol \(TLP\)](#) topic for more details on setting a default TLP designation for a source.

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



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

Update All Sources

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


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

3. Run the following command:

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

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



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

Update a Specific Source

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

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

3. Run the following command:

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



You can apply the command to multiple sources by listing the sources in a comma-delimited format.

Example: `--sources="CrowdStrike, AlienVault"`

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



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

Indicator and Signature Statuses Overrides

The following commands allow you to change status handling on indicators and signatures updated via feed ingestion. When you run the artisan command to enable this functionality:

- An existing indicator's status is overridden with the default status configured in the CDF.
- An existing signature's status is overridden with the default status of Active.

A second artisan command disables this functionality and returns your system to default handling of indicator and signature expiration updates.

Enable Indicator and Signature Status Overrides

1. SSH to your ThreatQ installation.
2. Run the following commands:

```
sudo su -  
/var/www/api/artisan threatq:configuration --key consumer.connectors_override_status --  
value 1  
/var/www/api/artisan cache:clear
```

Disable Indicator and Signature Status Overrides

1. SSH to your ThreatQ installation.
2. Run the following commands:

```
sudo su -  
/var/www/api/artisan threatq:configuration --key consumer.connectors_override_status --  
delete  
/var/www/api/artisan cache:clear
```

System-Level Commands

Airgap Import

See the [threatq:sync-import](#) topic.

Airgap Export

See the [threatq:sync-export](#) topic.

Allow Cross-Origin Resource Sharing for Specific Hostnames

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

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

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



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

Single Domain Example:

```
sudo /var/www/api/artisan threatq:configuration --  
key=cors.allowed_hosts --value https://www.example.com
```

Multiple Domains Example:

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

Disable Export Logging

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

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

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

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

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

LDAP Diagnostic Searches

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



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



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

To perform basic connect and bind authentication tests:

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

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

3. Run the following command:

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

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

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

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

3. Run the following command:

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

Example:

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

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

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.

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
```

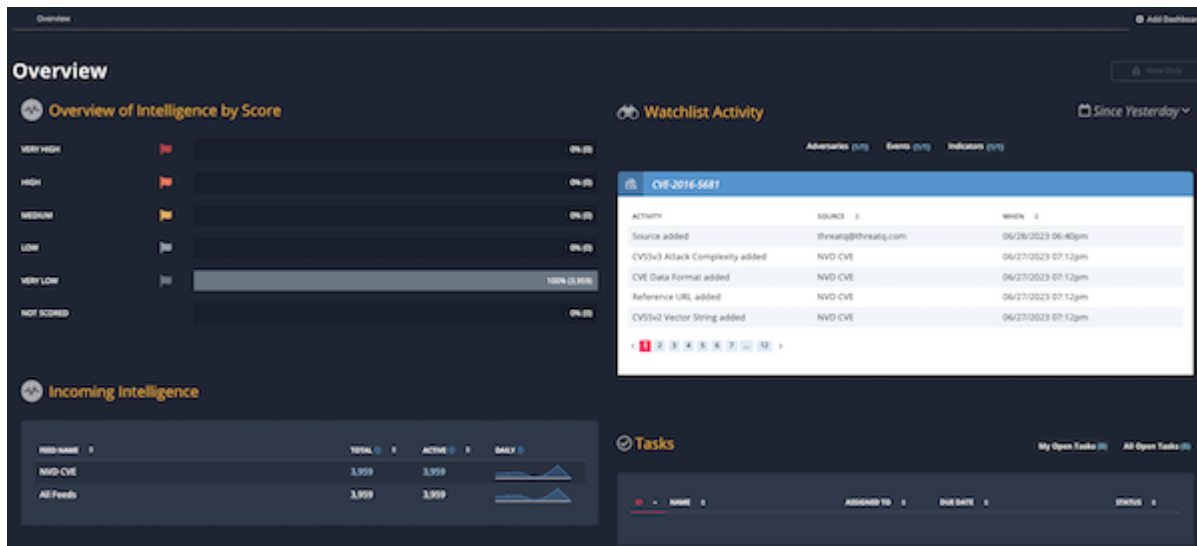
4. At the prompt, enter the email address for the user whose password you are resetting.

5. At the prompt, enter the new password.
6. At the prompt, re-enter the new password to confirm.

Dashboards

About Dashboards

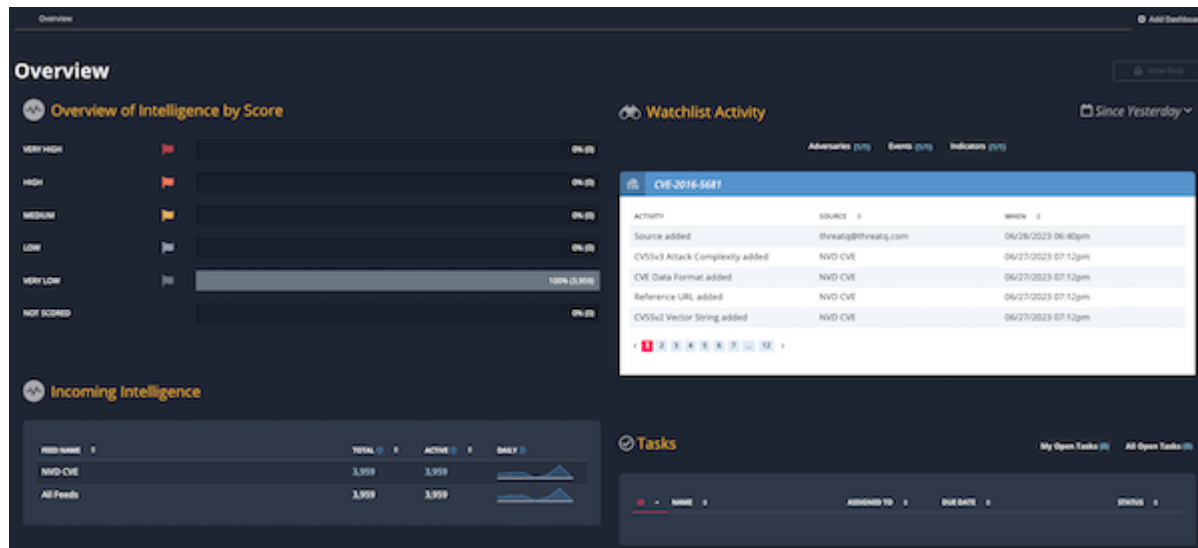
When you log into ThreatQ, your default view is the Overview dashboard. This pre-configured dashboard includes four widgets that give a high-level view of your system activity.



While the Overview dashboard cannot be modified, Primary Contributors, Administrators, and Maintenance users can use ThreatQ widgets to build [custom dashboards](#) that can be [shared](#) with individual users or all users. These custom dashboards allow you to narrow your focus on threat intelligence trends that affect your organization the most.

Default Dashboard

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



Widgets include:

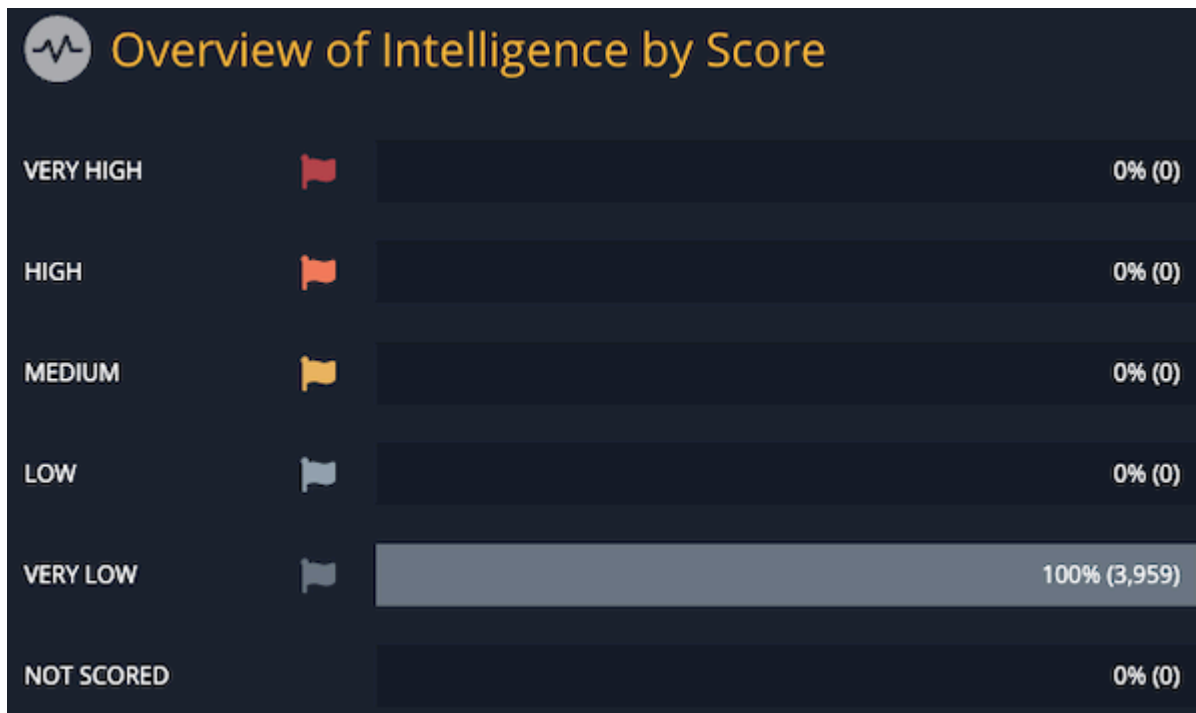
- Overview of intelligence by score
- Watchlist activity
- Incoming intelligence
- Open assigned tasks

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

Ideally, this dashboard reflects a small number of **Very High** indicators with the bulk of the remaining indicators scored as **Low** or **Very Low**. This distribution reflects a focus on key threat intelligence. You can use [Scoring Algorithms](#) or [Indicator Scoring](#) to adjust the scores assigned to your indicators. You can click the percentage/number of indicators to launch an advanced search based on that criteria.



Incoming Intelligence

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



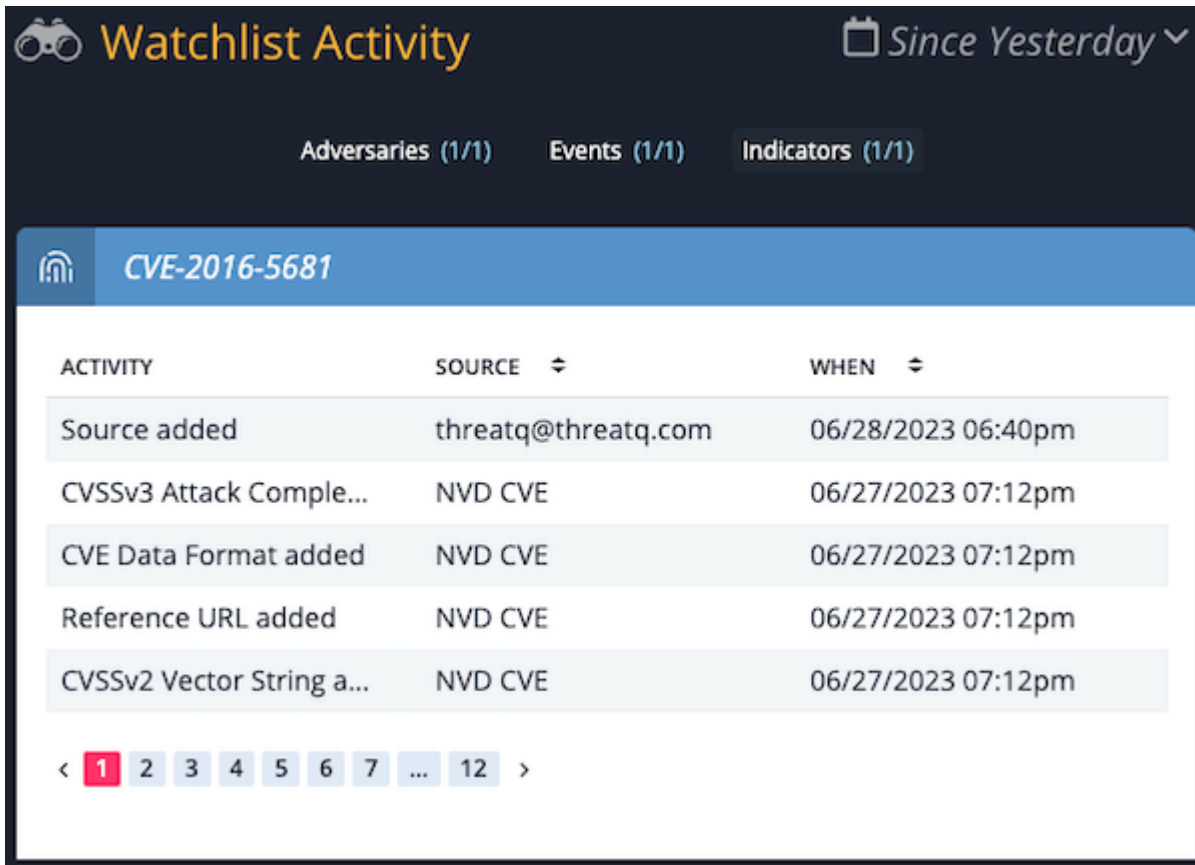
The system categorizes threat intelligence by:

- 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' dashboard. At the top, there's a header with a binoculars icon, the title 'Watchlist Activity', and a date filter 'Since Yesterday'. Below the header, there are three tabs: 'Adversaries (1/1)', 'Events (1/1)', and 'Indicators (1/1)'. The main content area shows a table for the item 'CVE-2016-5681'. The table has three columns: 'ACTIVITY', 'SOURCE', and 'WHEN'. The table contains five rows of activity data. At the bottom of the table, there is a pagination bar with a range of numbers from 1 to 12, with '1' highlighted.

ACTIVITY	SOURCE	WHEN
Source added	threatq@threatq.com	06/28/2023 06:40pm
CVSSv3 Attack Comple...	NVD CVE	06/27/2023 07:12pm
CVE Data Format added	NVD CVE	06/27/2023 07:12pm
Reference URL added	NVD CVE	06/27/2023 07:12pm
CVSSv2 Vector String a...	NVD CVE	06/27/2023 07:12pm

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

About Custom Dashboards

You can create and share multiple custom dashboards to be used on the ThreatQ landing page.



Each dashboard is comprised of system widgets which are populated by data derived from data collections - see [Managing Search Results](#) topic for more details. You can click on an individual segment of data within a widget to view it in the ThreatQ Threat Library.

With the dashboard sharing option, you can determine which dashboards you want to share with other users and which ones you want to keep private. See the [Dashboard Sharing](#) topic for more details.

You can control which shared dashboards created by other users appear in your view. Dashboards added to your view will appear dashboard horizontal menu as well as the Dashboards dropdown menu. You can also remove your own dashboards from your view without deleting them from the platform. See the [User View Management](#) topic for more details.

Topics covered in this section include:

SECTION	DETAILS
About Analytics Dashboards	Deploy pre-configured dashboards for Adversaries , Events , Files , and Indicators .
Dashboard Widgets	You can add the following widgets to your custom dashboards: Bar Chart, Description, Line Chart, Pie Chart, Count, and Table.
Dashboard Management	You can create, edit, and delete your own custom dashboards.

Dashboard Sharing

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

User View Management

Add, remove, and reorder dashboards that you created or have been shared with you.

Analytics Dashboard

About Analytics Dashboards

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



Analytics dashboards cannot be edited.

Options include:

SECTION	DETAILS
Adversaries Analytics	The Adversaries dashboard provides an overview of all the Adversaries within ThreatQ as well as overlapping use of specific indicators.
Events Analytics	The Events dashboard provides a high-level view of what types of Events have occurred and how frequently they are occurring.
Files Analytics	The Files dashboard provides you with a pie chart displays the percentage of different types of Files within the system and a table that lists the files, the date and time they were created, their title, their source, their category, and associated keywords.
Indicators Analytics	The Indicators Dashboard provides an insight into what Indicators have been added to the system within the last 15 days, as well as an overview of how many indicators fall under each indicator type.

Adversaries Analytics

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

Adversaries Summary Table

The Adversaries Summary table lists Adversaries by name, number of Indicators , date created, and the most recent event date associated with the adversary.

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

Click the name in the Adversary Name column.

Performing a search for related indicators

Click the number in the Number of Indicators column to set the adversary name as a search criterion and open the Advanced Search page.

Opening the Event Details page for an adversary event

Click the date in the Most Recent Event Date to open the Event Details page.

Changing the number of entries displayed in the table

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

FUNCTION

DETAILS

Sorting the table by a column

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

Searching within the Adversary Name column

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

Adversaries Overlap Table

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

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

The following functions are available:

FUNCTION

DETAILS

Opening the Adversary Details page for an adversary

Click the name in the Adversary Name column.

Opening the Indicator Details page for an overlapping indicator

Click the identity in the Overlapping Indicator column.

Changing the number of entries displayed in the table

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

Sorting the table by a column

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

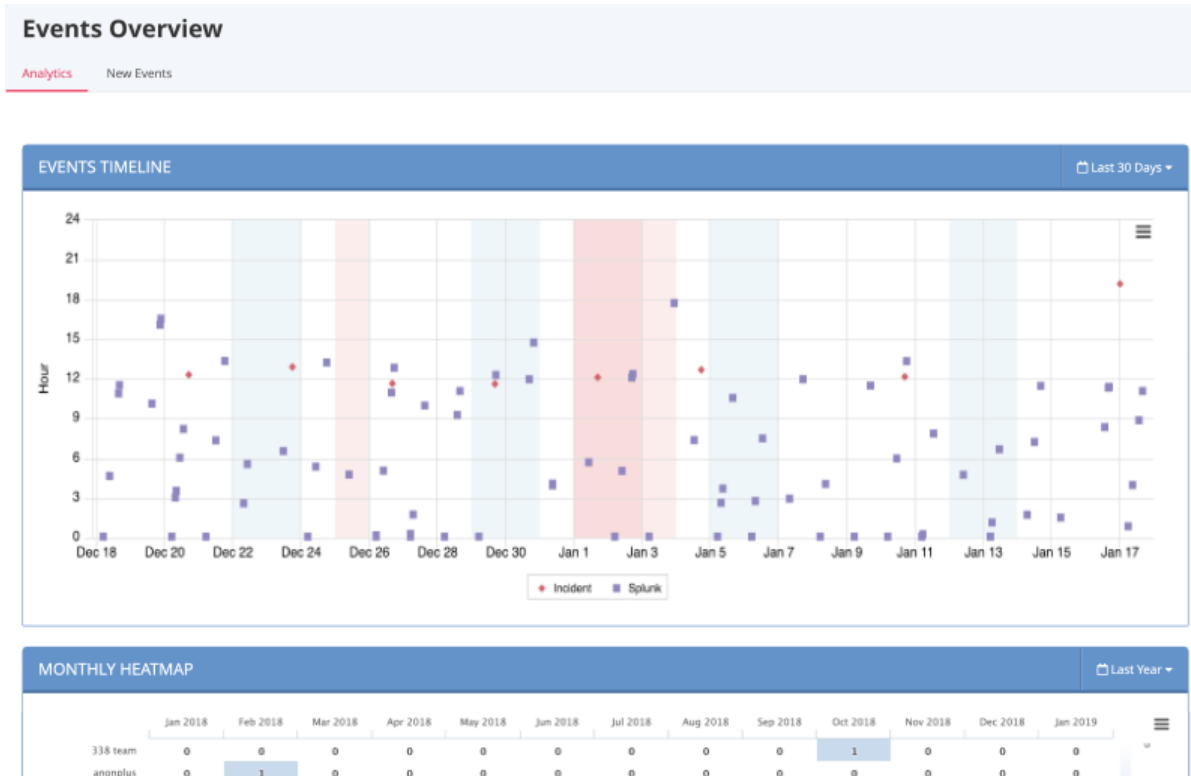
Searching within a column

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

FUNCTION	DETAILS
Printing the graph or saving it as a PNG, JPEG, PDF, or SVG	Click the hamburger menu  and select the desired option.

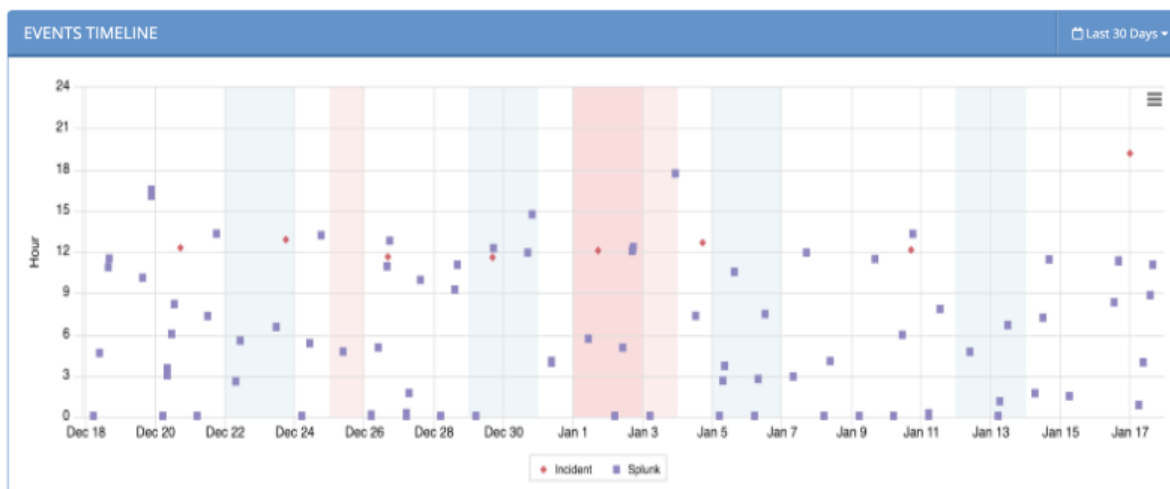
Events Analytics

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



Events History Scatter Plot

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



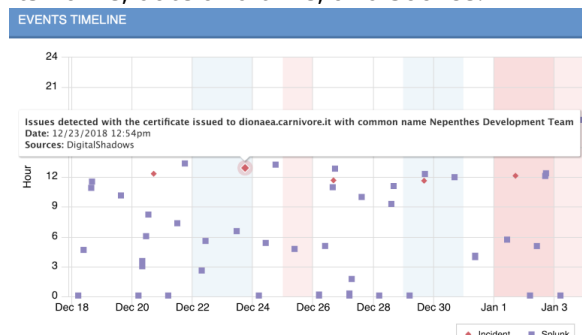
The following functions are available:

FUNCTION

DETAILS

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

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



Opening the Event Details page for one of the events

Click the event in the scatter plot.
For more information, see [About Object Details](#).

Hiding or unhiding one or more of the event types

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

Adjusting the time frame of the information displayed

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

You can select from:

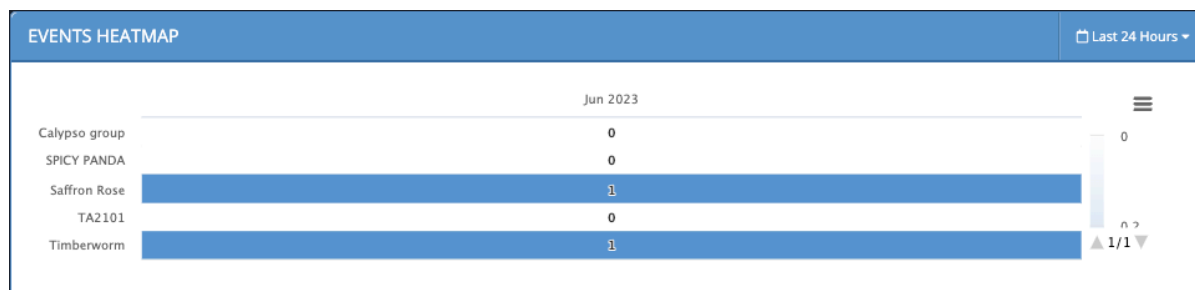
- Last 24 Hours
- Last 7 Days
- Last 30 Days
- Last Year
- User-set custom range

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

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

Events Heatmap

The Events Heatmap table lists events by adversary. Shading of the totals is used to allow you to quickly scan for patterns in the events and to quickly detect events with higher counts.



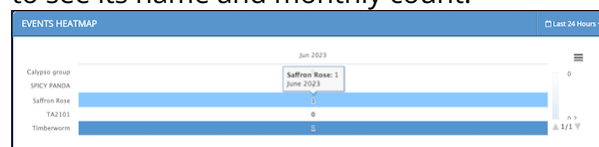
The following functions are available:

FUNCTION

DETAILS

Viewing an event's name and monthly count

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



Adjusting the time frame of the information displayed

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

You can select from:

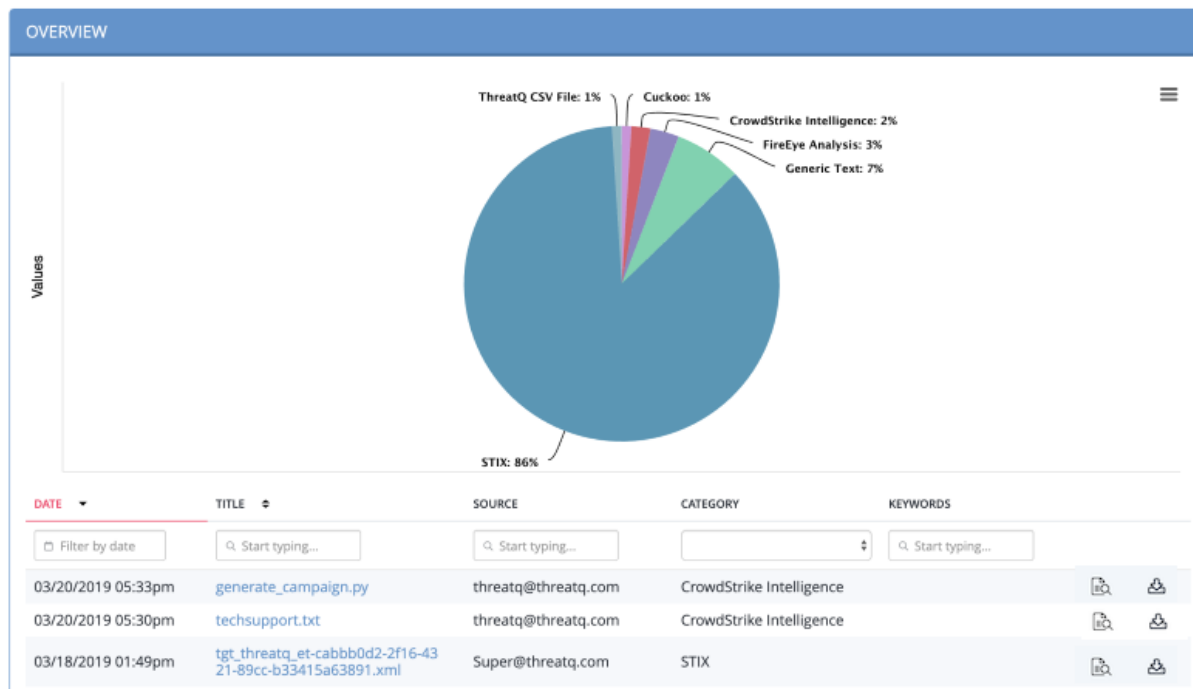
- Last 24 Hours
- Last 7 Days
- Last 30 Days
- Last Year
- User-set custom range

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

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

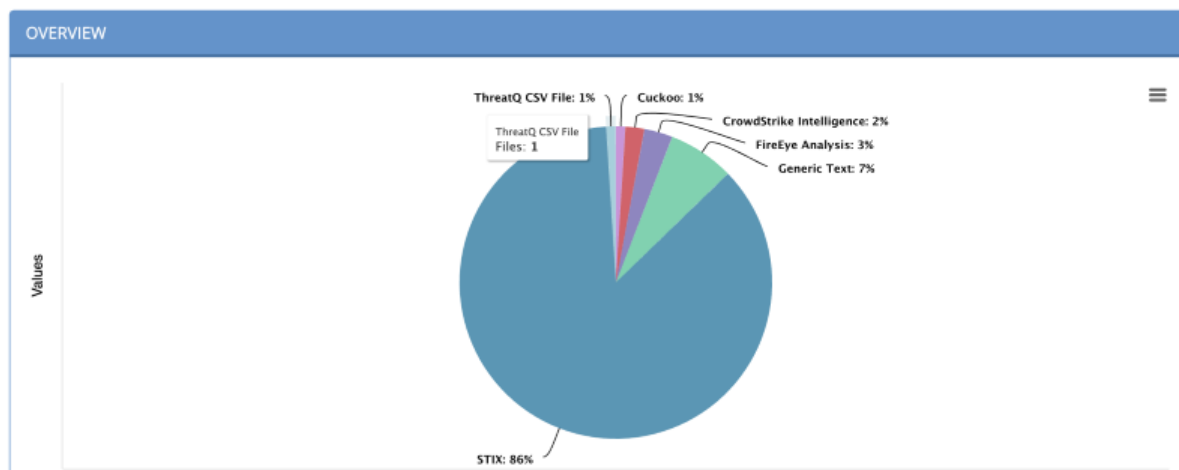
Files Analytics

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



File Type Pie Chart

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



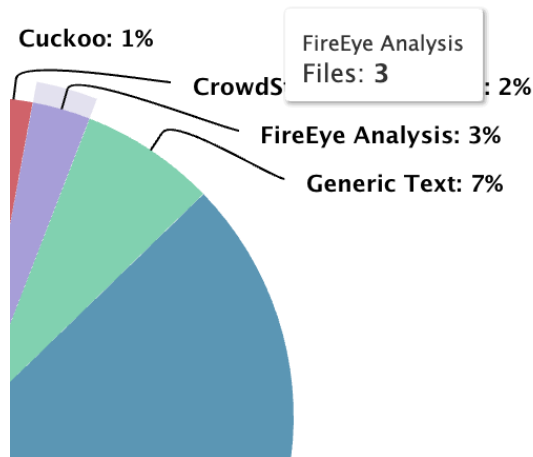
The following functions are available:

FUNCTION

DETAILS

Viewing more information about a selected file

Hover over a colored section of the pie chart to view the number tha corresponds to the file type percentage.



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

Click the hamburger menu  and select the desired option.

Files Table

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

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

< 1 2 3 4 5 6 7 ... 11 > Rows per page 10 ▾

The following functions are available:

FUNCTION

DETAILS

Opening the File Details page for a file

Click the name in the Title column.

Changing the number of entries displayed in the table per page

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

Sorting the table by a column

Click the column header. Click on the header a second time to reverse the column sorting order.

Searching within a column

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

Downloading a file

Click the file's download icon .

Previewing a file

Click the file's preview icon Preview Icon. If your browser does not support file preview for a specific file type, the file is downloaded instead.

FUNCTION

DETAILS



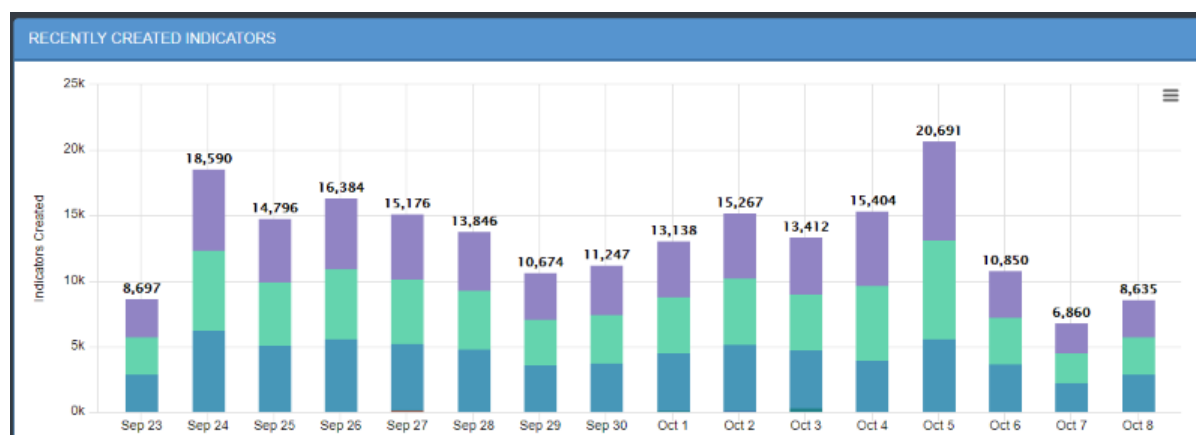
You cannot preview a malware locked file.

Indicators Analytics

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

Recently Created Indicators Histogram

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



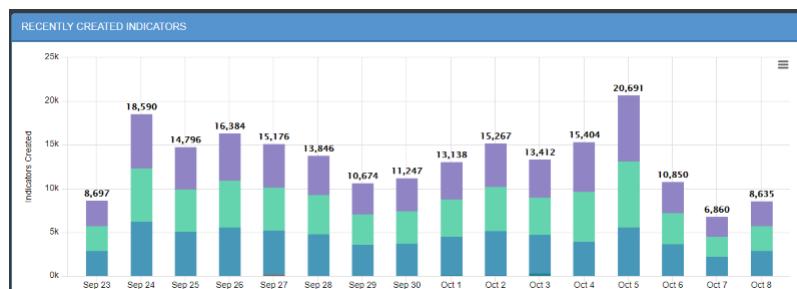
The following functions are available:

FUNCTION

DETAILS

Viewing the number of indicators created each day by type

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.

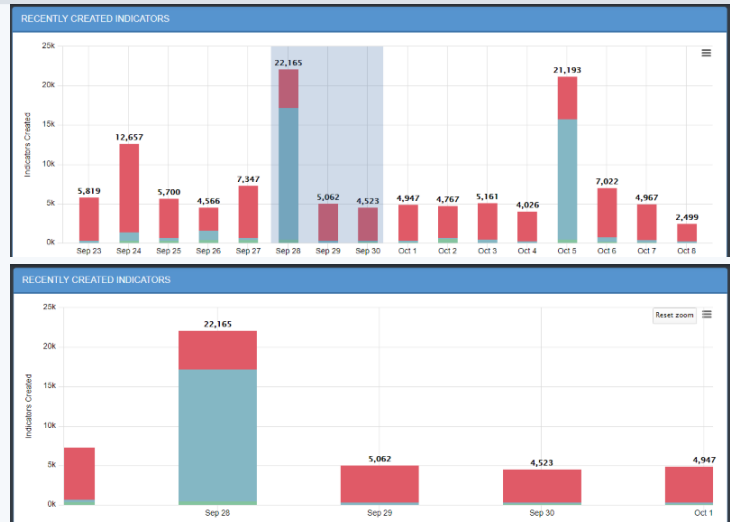


Zooming in for a closer view

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

FUNCTION

DETAILS



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

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

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	4bc0a199fa1792b7c54e49db787a9c60f1842a88	0	SHA-1	Active	CrowdStrike
10/08/2018 05:30pm	77ed439dd3fc839cc95d0197ced2717efc0262545b0dd4e0418779b87a3ea920	0	SHA-256	Active	CrowdStrike
10/08/2018 05:30pm	3b76aeb2083e10cd633ede6c20cbf09e4c60da39a07d45ea050bb438dead1eb0	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	91dbb6bf198622c957233379042868de	0	MD5	Active	CrowdStrike
10/08/2018 05:30pm	1379fe1801679cd33312156ce3193167a150950e3d8bccd1b5805acee909916c	0	SHA-256	Active	CrowdStrike
10/08/2018 05:30pm	0a4f67a79e75f4bef2772c2f60734042f7081e9	0	SHA-1	Active	CrowdStrike
10/08/2018 05:30pm	f8d24fbacdb0c6d5acbb84c3db26d51d7	0	MD5	Active	CrowdStrike
10/08/2018 05:30pm	ededaa1a6c982af03a58dcb0a8b8a7f8f48ca72a	0	SHA-1	Active	CrowdStrike
10/08/2018 05:30pm	74664b624f5ac2f31132642a3f77e44da7f41cafe566f378e5efb9931391090e	0	SHA-256	Active	CrowdStrike
10/08/2018 05:30pm	37404ed847180bd53c3e35a7e19b8382	0	MD5	Active	CrowdStrike

The following functions are available:

FUNCTION

DETAILS

Resort the Table

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

Search and Filter Table Results

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

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

Modify the Number of Rows Displayed

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

Access the Indicator Details Page for a Specific Indicator

Click on the specific Indicator to review to open the Indicator's Details page.

Attributes Table

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

ATTRIBUTES

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 >

Previous

Next

Please select an attribute on the left.

The following functions are available:

FUNCTION

DETAILS

Change the Number of Entries Displayed in the Table

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

Search/Filter Attributes and Values

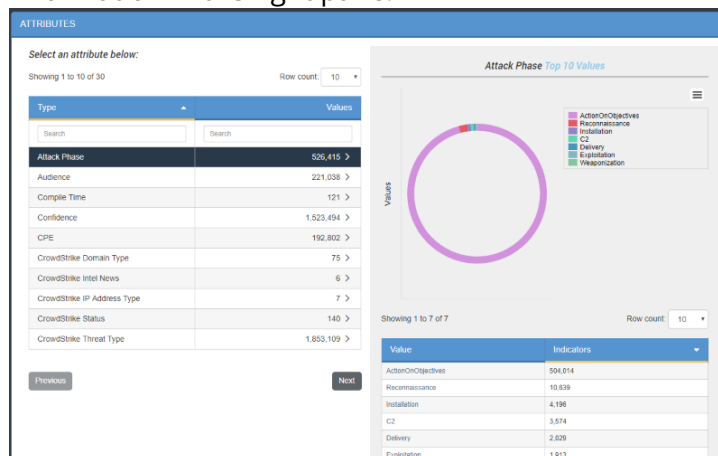
Click within the search box at the top of the column, and enter your search criteria.

FUNCTION

DETAILS

View More Information About a Selected Attribute

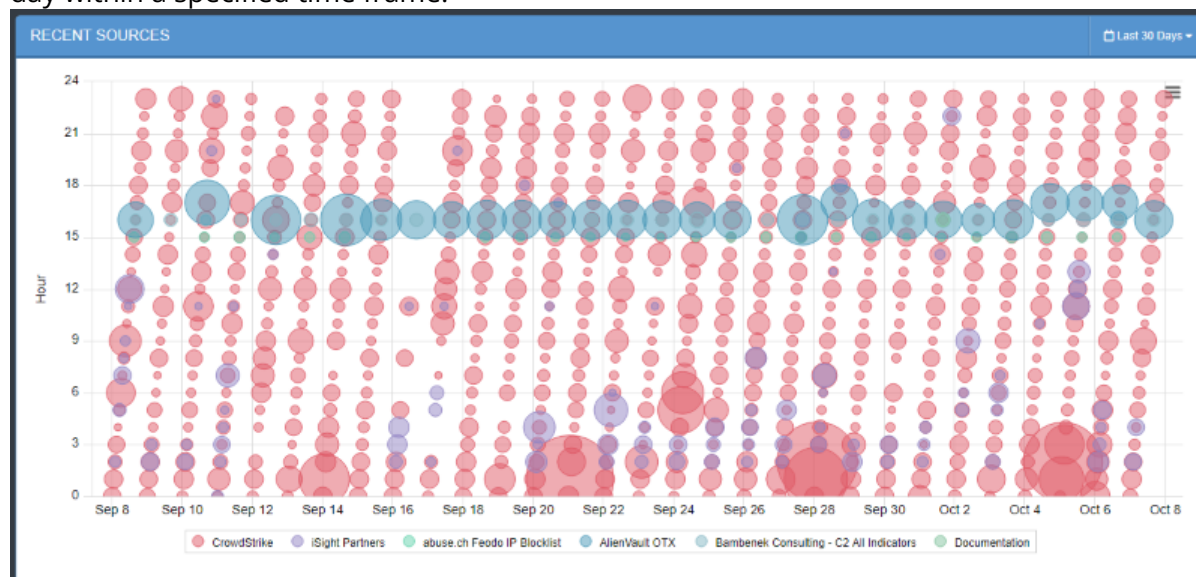
1. Click on an attribute row in the table to view additional information in the right pane.



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.



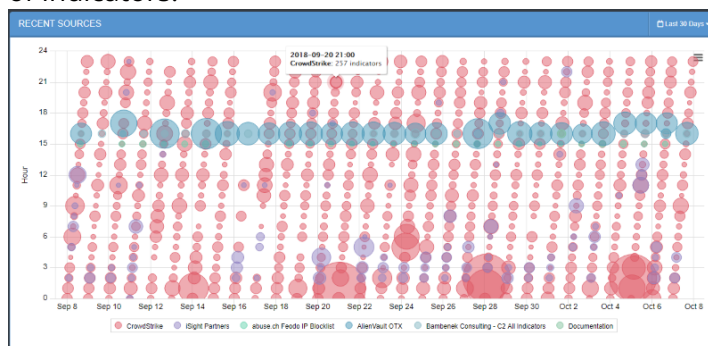
The following functions are available:

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.



2. Click on the one of the scatter plot circles to open the Advanced Search page with the specific filter settings used for that selection.

Adjust the Date Range of the Information Displayed

The default date range is 30 days.

1. Click the date range icon located to the top-right of the chart and use the dropdown menu select the desired range.

You can select from:

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

Hide Values from the Scatterplot

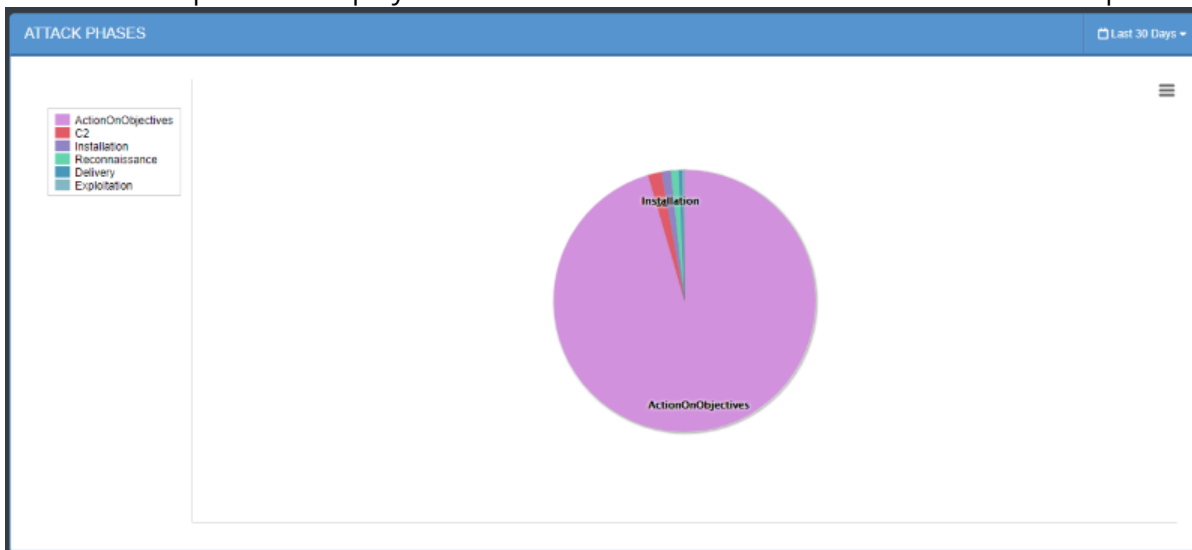
1. Click on a source in the legend under the scatter plot to hide it.

The Source will be removed from the scatter plot and the source in the legend appear grayed out.

2. Click on the source again to add it back to the scatter plot.

Attack Phases

Attack Phases are the ways an indicator might be used and are listed as indicator attributes. The Attack Phases pie chart displays the number of indicators that fall under each attack phase.



The following functions are available:

FUNCTION	DETAILS
View the Number of Indicators for an Attack Phase	1. Hover the mouse over a portion of the pie chart to view a popup the Attack Phase and number of indicators associated with it. 2. Clicking on a pie chart section will open the Advanced Search page with the specific filter settings used for that selection.
Adjust the Date Range for the Information Displayed	The default Date Range is 30 days. 1. Click the date range icon located to the top-right of the chart and use the dropdown menu select the desired range. Users can select from: ○ Last 24 Hours ○ Last 7 Days ○ Last 30 Days ○ 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.

FUNCTION	DETAILS
	The Attack Phase will be removed from the pie chart and the source in the legend appear greyed out. 2. Click on the Attack Phase again to add it back to the pie chart.

Dashboard Widgets

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

Bar Chart



You can click on individual bars within the chart to view those results in the Threat Library.

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



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.

FIELD	DESCRIPTION
Visual Display	Select whether to show the bar chart horizontally or vertically.
Show Top Options	Select the number of results to display. Options include: • Top 5 • Top 10

Description

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

Tips and Tricks for Adding Images to Description Widgets

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

Description

Paragraph

B

I

U







1

=

2

=

≡

≡

≡

≡

≡

≡





↶

↷

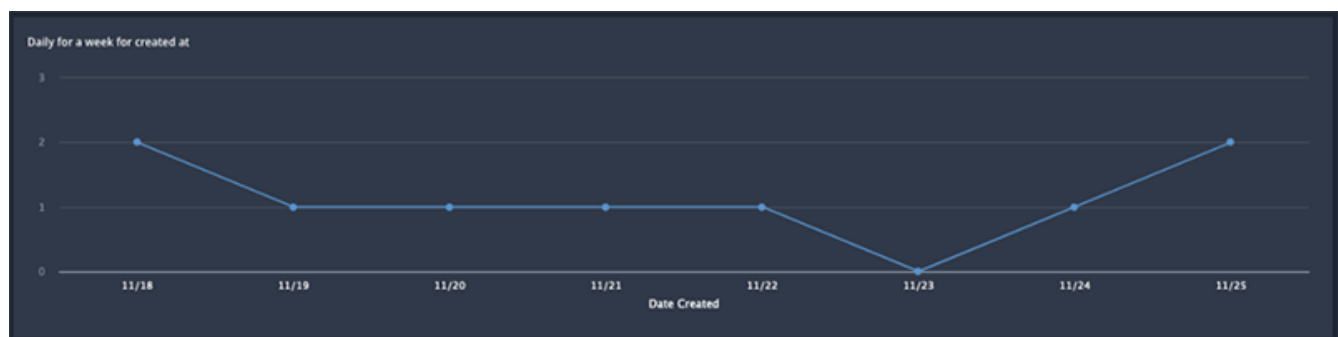
Save

Cancel

Line Chart

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

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

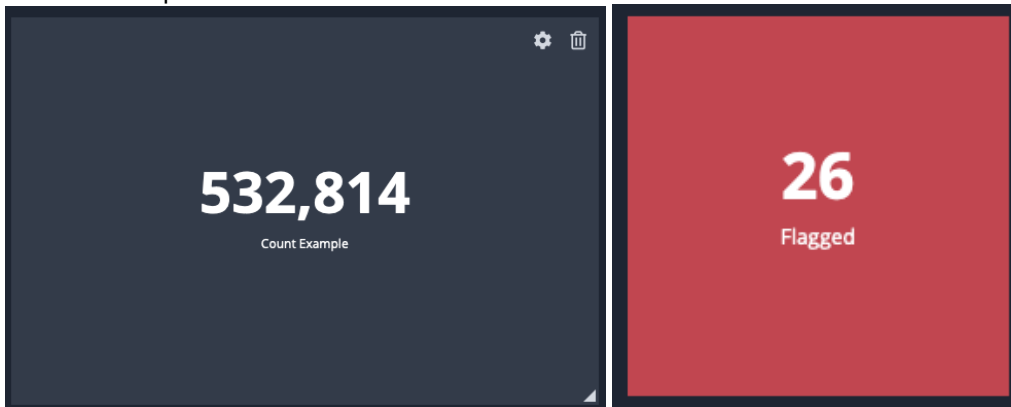


Complete the following fields to add a line chart widget to your custom dashboard.

FIELD	DESCRIPTION
Title	The title that will appear above the widget.
Automatically Update	The refresh time for the data. Options include: • 15 Minutes • 30 Minutes • 60 Minutes • None
Data to Show in Widget	Select the data collection to populate the data.
Object	Select a specific object type to display.
Date Metric	The date stamp to use with the line chart. Options include: • Date Created (all object types) • Last Modified (all object types) • Expiration Date (indicators only)
Time Range	The time range from today to be displayed. Options include: • 1 Week • 3 Months • 6 Months • 1 Year
Time Segments	Select how the dates will be displayed on the line chart. Options include: • Days (1 Week Time Range only) • Weeks (3 Months, 6 Months, 1 Year only) • Months (3 Months, 6 Months, 1 Year only) • Quarters (3 Months, 6 Months, 1 Year only) Quarters will return the following results based on Time Range selection: ○ 3 Months will display the current quarter plus the previous quarter ○ 6 Months will display the current quarter plus the previous two quarters. ○ 1 Year will display the current quarter plus the previous four quarters.

Count

The Count widget displays the total number a specific object type. You can configure the widget to display a different background color if the total number of objects associated with the widget is above or below a specific value.



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

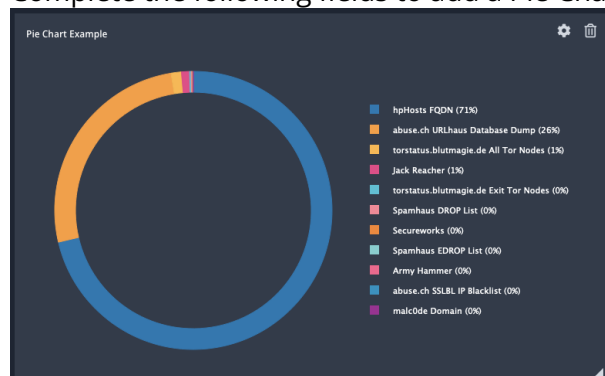
FIELD	DESCRIPTION
Title	The title that will appear above the widget.
Automatically Update	The refresh time for the data. Options include: • 15 Minutes • 30 Minutes • 60 Minutes • None
Data to Show in Widget	Select the data collection to populate the data.
Object	Select a specific object type to display.
Emphasize Data Using Color	Check this box to use different colors to highlight the widget if the count is less than or greater than a specific value. If checked, you will be prompted to select a count value and background color.

Pie Chart



You can click on individual segments within the chart to view those results in the Threat Library.

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



FIELD

DESCRIPTION

Title

The title that will appear above the widget.

Automatically Update

The refresh time for the data. Options include:

- 15 Minutes
- 30 Minutes
- 60 Minutes
- None

Data Collection

Select the data collection to populate the data.

Object

Select a specific object type to display.

Group By

Select a data column to sort the information such as source, tags, etc.

Table

Table widgets allow you to add as many column fields as needed. You can click on a row's **value** entry to view it in the ThreatQ Threat Library. You can also click on the **eye**  icon for a row to view a preview of the system object details.

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



You cannot preview a malware locked file.

Tier Review

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

< 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

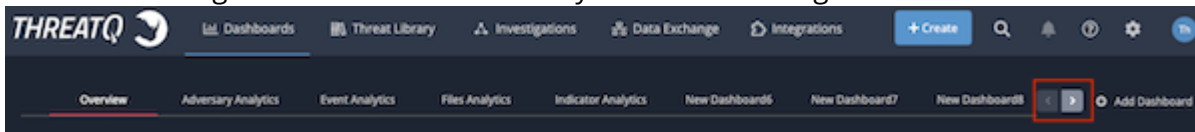
Select the column to sort the table and the order (ascending/descending).

Dashboard Management

Access to dashboards is determined by your user role and [Sharing](#) permission level.

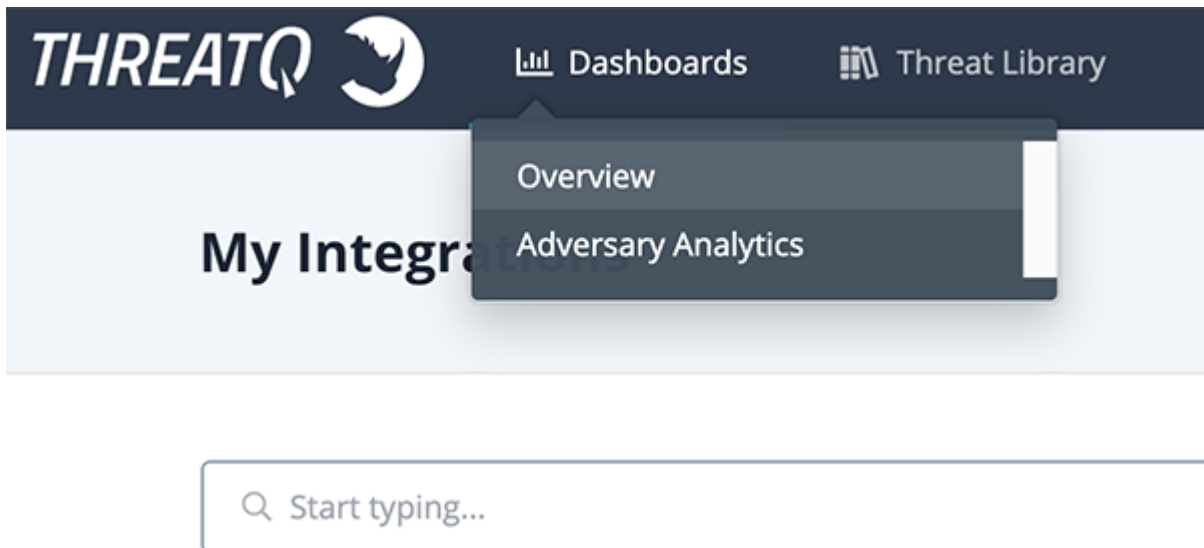
Accessing a Dashboard

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

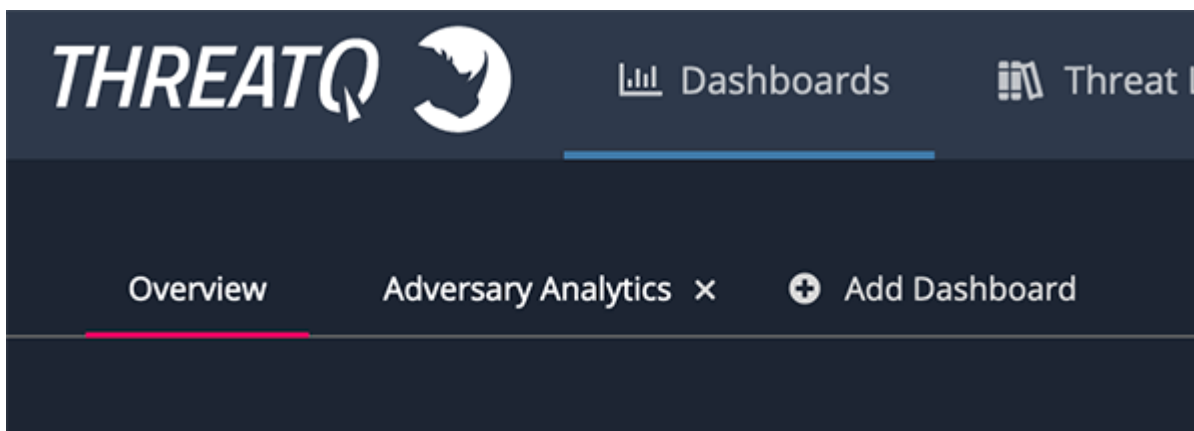


You can access a specific custom dashboard using the following methods:

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

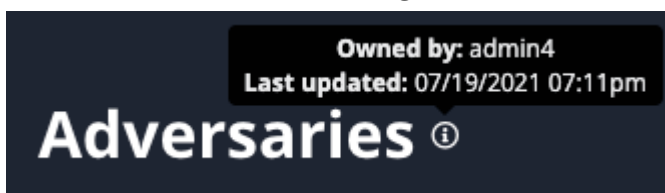


- When viewing a dashboard, click another dashboard tab. If you are not viewing a dashboard at the time, you can click on the ThreatQ logo to load your default dashboard.



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

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



Add an Existing Dashboard to Your View

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

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

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



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

Add Dashboard

All

Owned By Me

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

Create New Dashboard

Cancel

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

Creating a Dashboard

All [User Roles](#), except Read-Only Access can create custom dashboards.

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

Adversary Count

New Dashboard

Add Dashboard

Dashboard Name

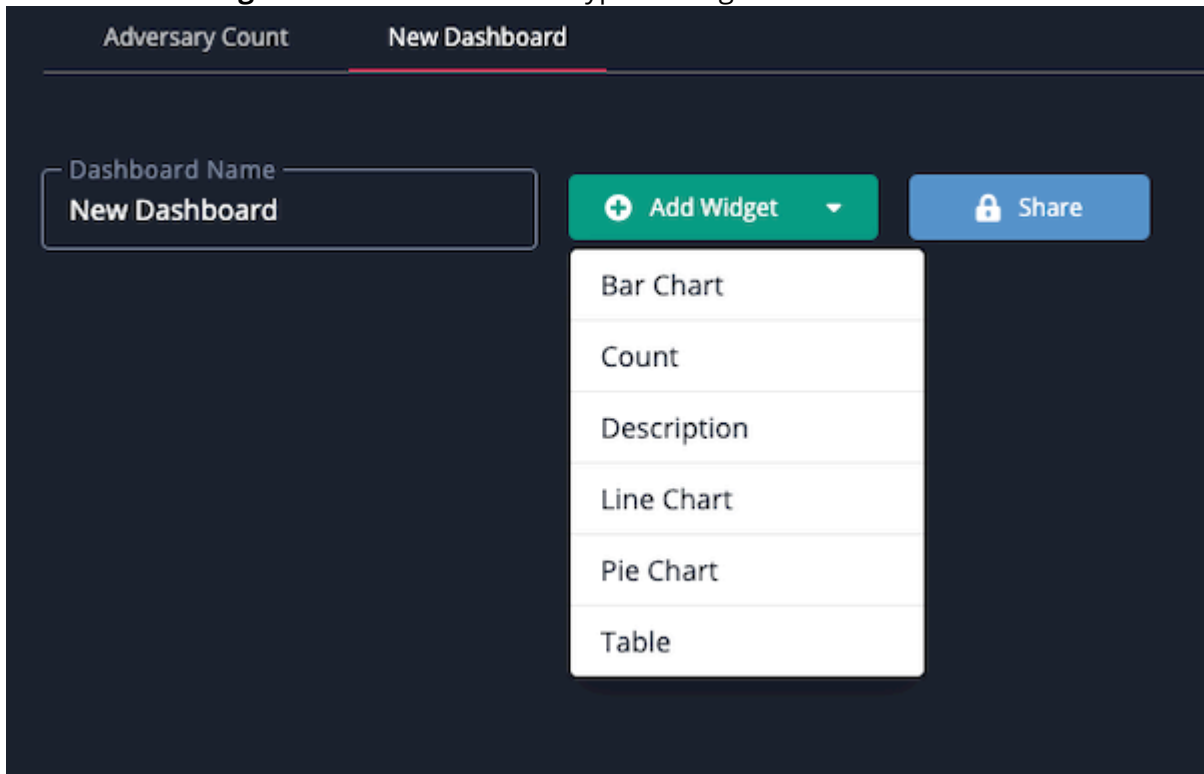
New Dashboard

Add Widget

Share

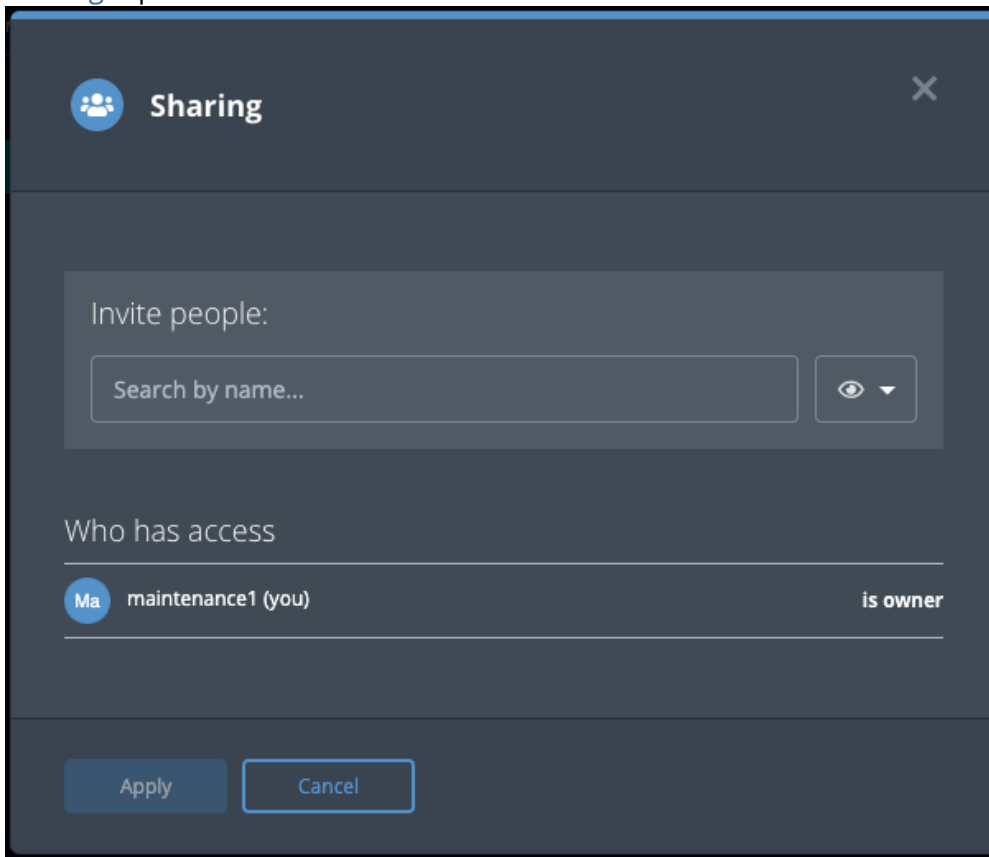
Done Editing

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



- After adding a widget, you can resize it by clicking and dragging the mouse on the bottom-right grey corner.
- You can move the widget around the dashboard by clicking the widget header and dragging it around the page.

- Click on the **Share** button and specify user access to the dashboard. See the [Dashboard Sharing](#) topic for more details.



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

Editing a Dashboard

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

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



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



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

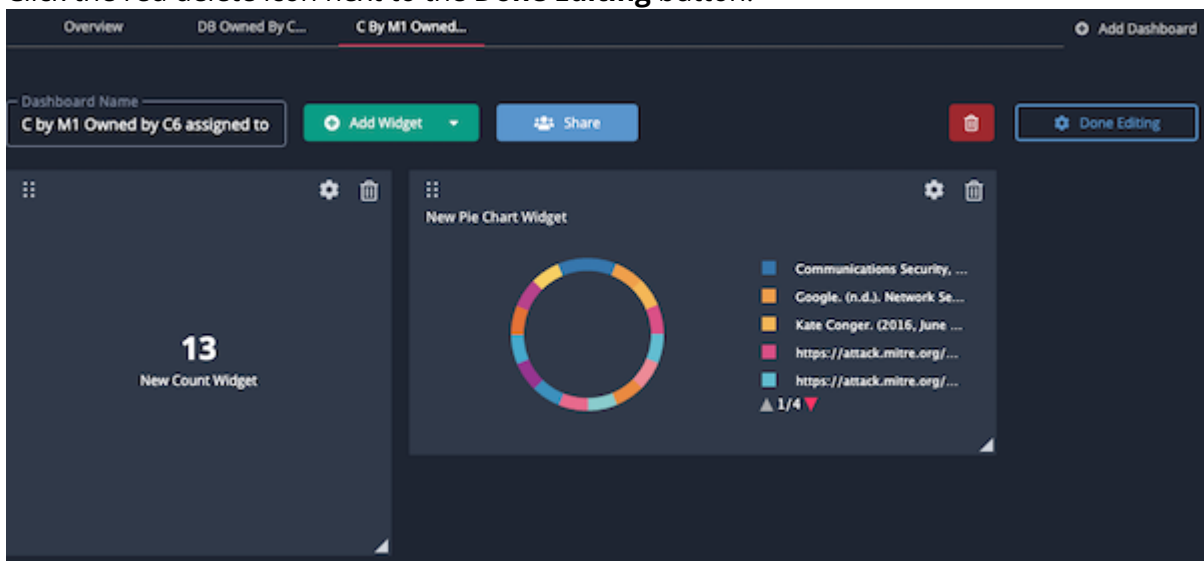
4. After you make your changes, click the **Done Editing** button to save all updates.

Deleting a Dashboard

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

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

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



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

Reassigning a Dashboard of a Deleted User

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

Dashboard Sharing

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

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

See the [Sharing](#) topic for more information on the permissions you can assign to each dashboard.

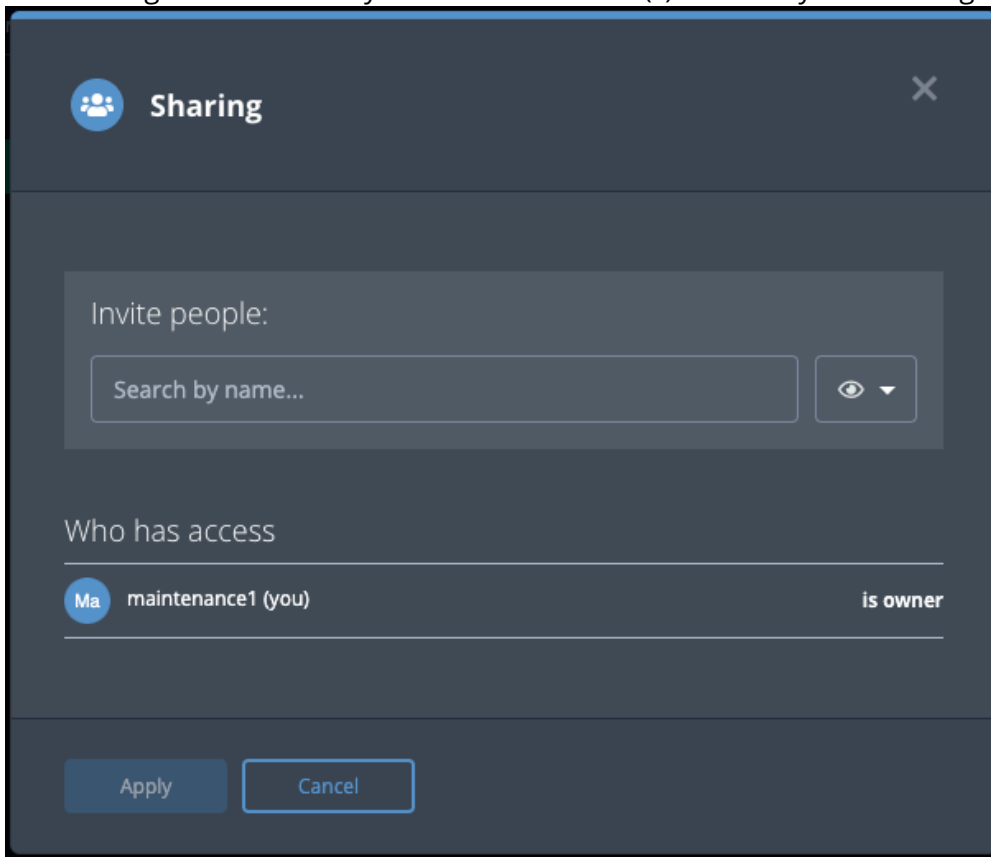
Sharing a Dashboard

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

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

- Click the **Share** button.

The Sharing window allows you to select the user(s) to which you want to grant access.



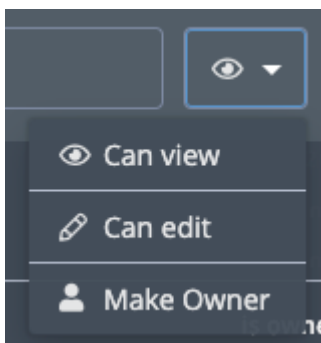
- Click the arrow next to the  icon to select the user's permission level.



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



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



- Use the search field to locate and select a user's name or the **Everybody (Public)** option. This option grants view-only access to all users.
The user is now listed in the **Who has access** list. From this listing, you can change or delete the user's permissions.



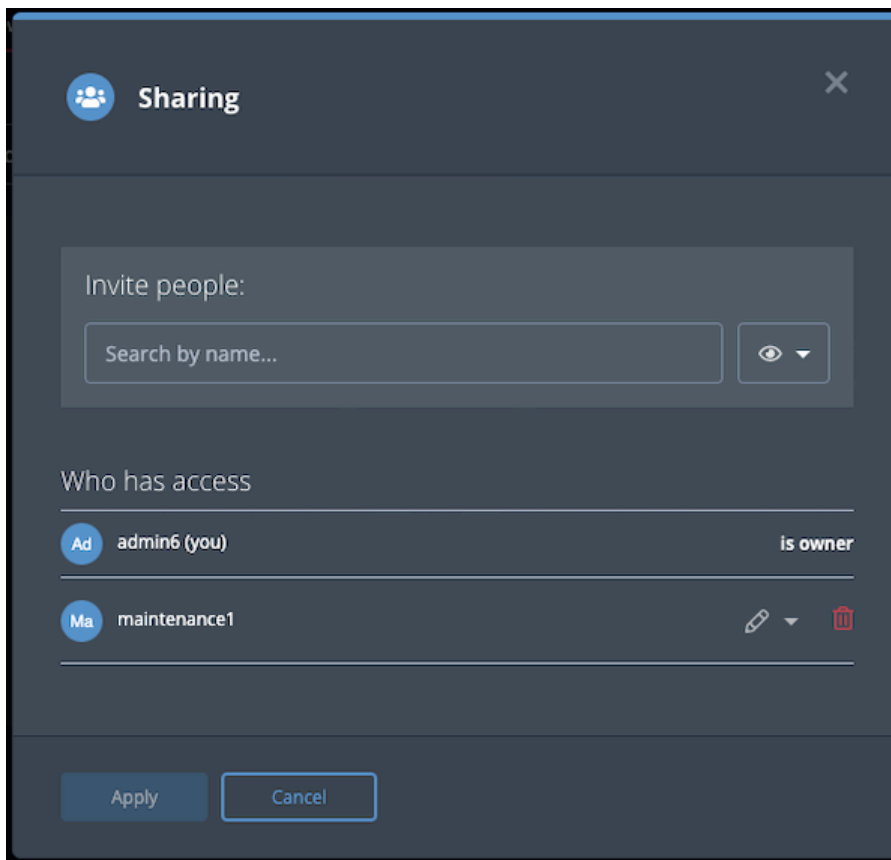
When you share a dashboard with a user, you also give him viewing permissions for all data collections used by the dashboard's widgets.

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

Updating Dashboard Permissions

1. Enter a dashboard's **Edit** view.
2. Click the **Share** button.

The Sharing window lists the users who have access to the dashboard.



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

Shared Dashboards of a Deleted User

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

Dashboard Export

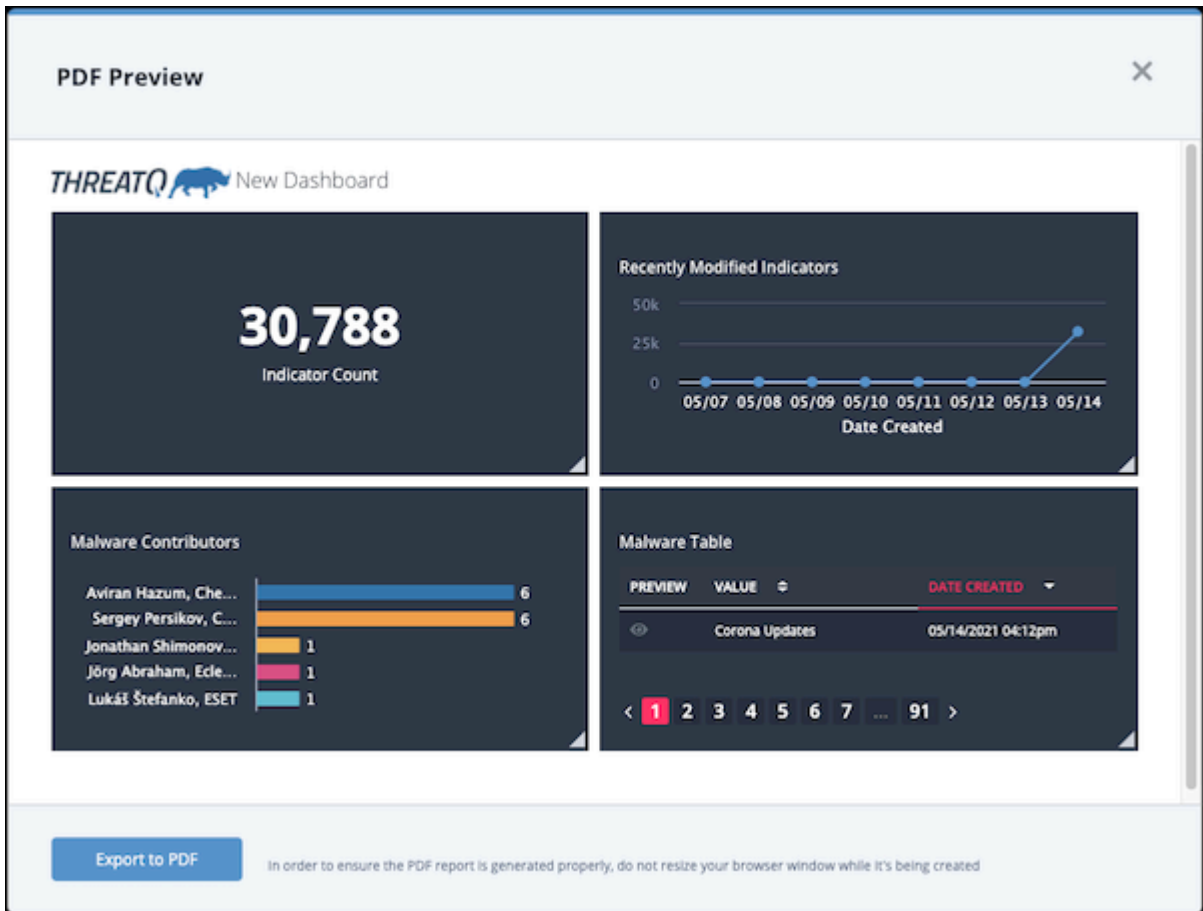
When you select a custom dashboard, the PDF Preview button gives you the option to export a PDF copy of all the widgets in the dashboard. The PDF preview window allows you to rearrange the widget order before you print and/or save the PDF.



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

Creating a Dashboard PDF

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



PDF Preview

THREATQ New Dashboard

Indicator Count
30,788

Recently Modified Indicators

50k
25k
0

05/07 05/08 05/09 05/10 05/11 05/12 05/13 05/14

Date Created

Malware Contributors

Contributor	Count
Aviran Hazum, Che...	6
Sergey Persikov, C...	6
Jonathan Shimonov...	1
Jörg Abraham, Ecle...	1
Lukáš Štefanko, ESET	1

Malware Table

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

< 1 2 3 4 5 6 7 ... 91 >

Export to PDF

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

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



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

- Click a widget header then drag and drop to move it to a new location on the page.

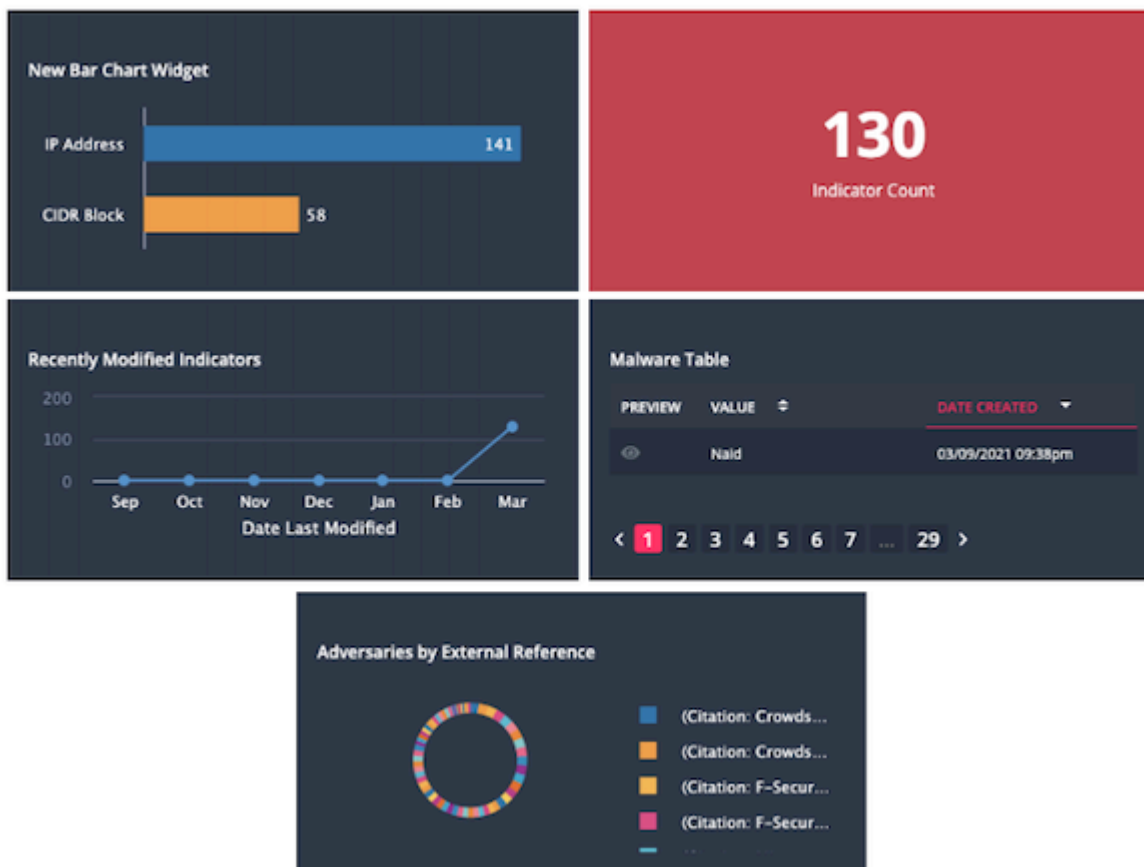
- Resize a widget by clicking and dragging the bottom-right grey corner.
- Click the **Export to PDF** button.
The system exports the dashboard widgets to a PDF file which you can save and/or print. The PDF file name defaults to dashboard.pdf. The PDF title includes the ThreatQ logo and the name of your dashboard.



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

Sample PDF:

THREATQ Head Office



User View Management

The User View refers to your individual view of the ThreatQ landing page. You can create custom dashboards and manage which dashboards, both shared and your own custom ones, appear in your view.

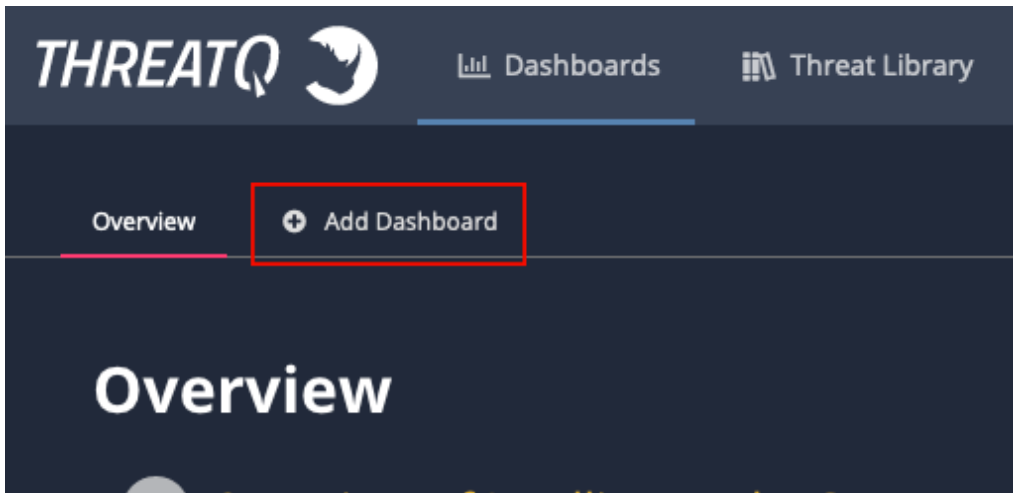


Any dashboard that is part of your User View will also be listed in the Dashboards dropdown menu.

Adding a Dashboard to Your View

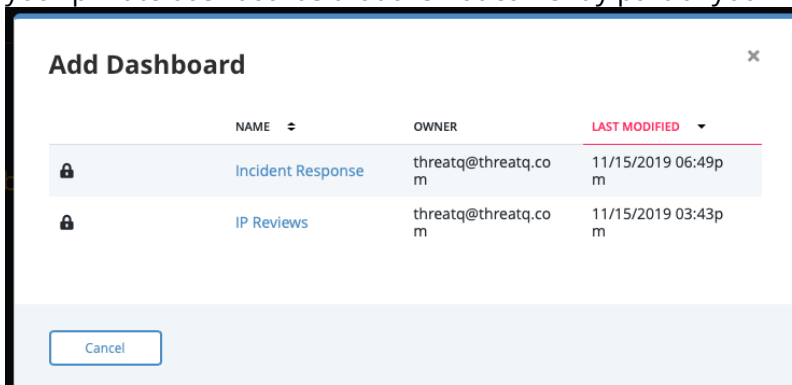
You can add dashboards that have been shared with you as well as your own private dashboards that are not currently part of your view.

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



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

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



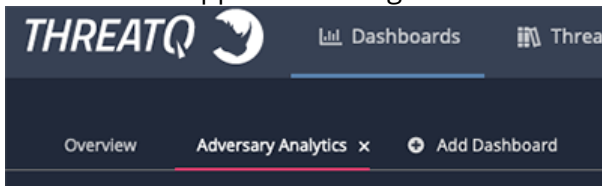
3. Click a dashboard in the list to add it to your view.

Removing a Dashboard from Your View

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

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

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



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

Changing Dashboard Order

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

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

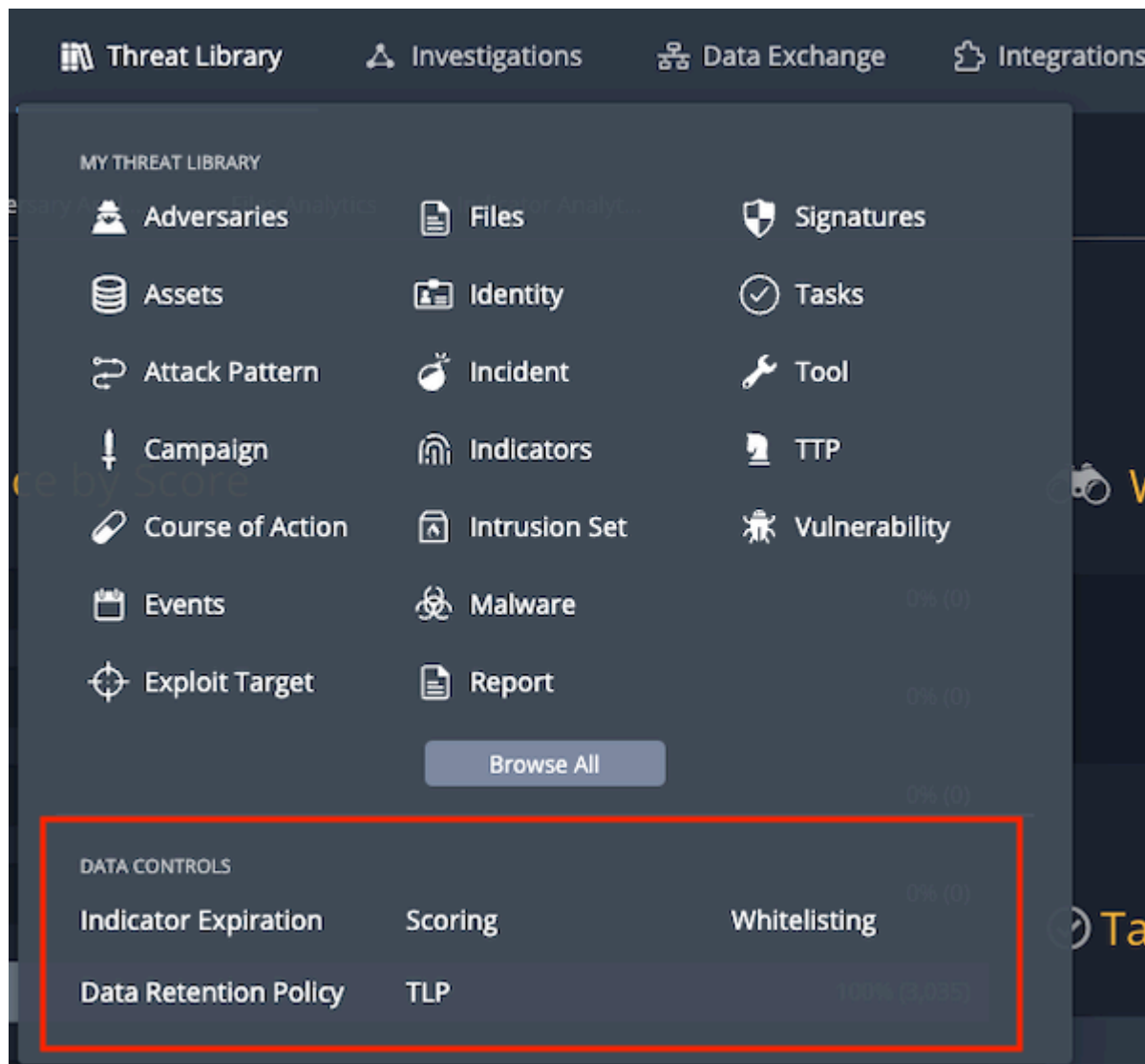


Order changes are saved automatically. These changes also update the order in the Dashboards dropdown menu.

Data Controls

About Data Controls

When you click the Threat Library option on the Main Navigation menu, the Data Controls section of the drop down list allows you to access Indicator Expiration, Data Retention Policy, Scoring, TLP, and Whitelisting options.



These Data Control options allow you to configure:

SECTION

DETAILS

Indicator Expiration Policies Configure expiration policies to automatically deprecate stale intelligence as it becomes less relevant.

Data Retention Policy Automate the deletion of system objects based on the parameters defined in a Data Collection.

Scoring Algorithms Configure scoring to filter through the millions of indicators your platform has ingested to focus on the data that really applies to your environment while retaining all other indicators and context for threat research.

Traffic Light Protocol (TLP) Configure your Traffic Light Protocol (TLP) schema to provide a set of designations to ensure that sensitive information is shared with the appropriate audience.

Whitelisted Indicators Identify non-malicious indicators using the Whitelisting feature.

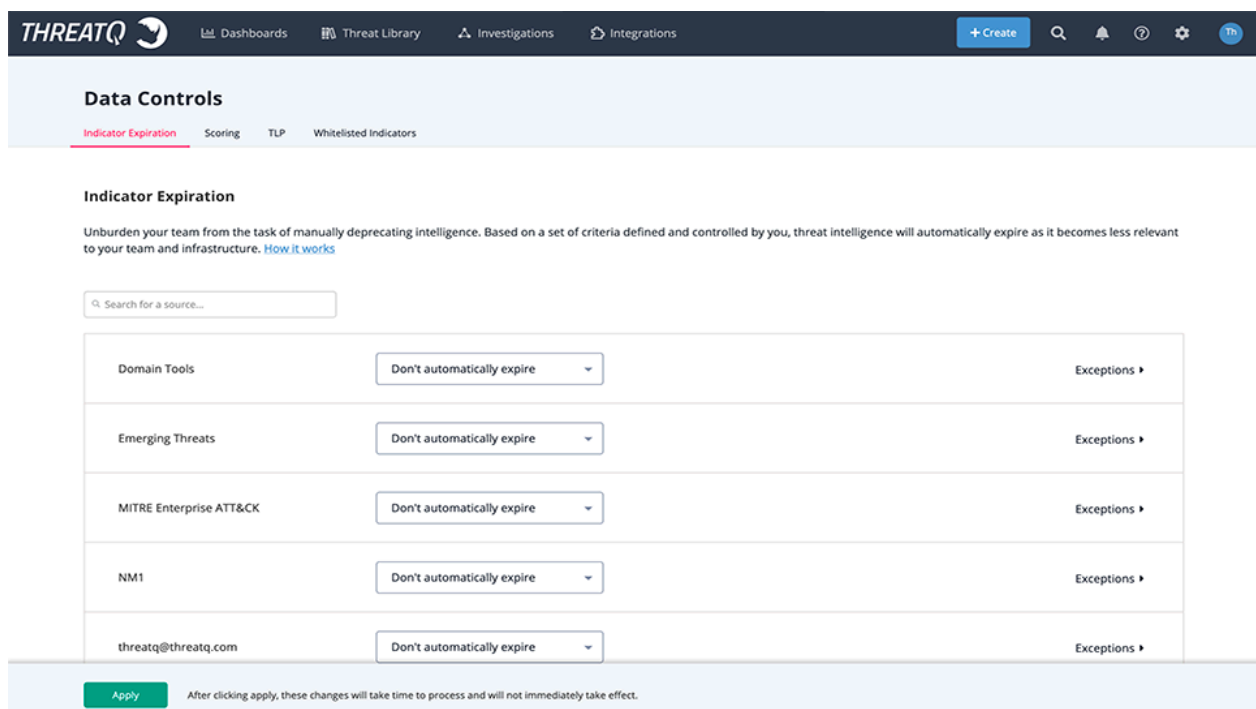
Indicator Expiration Policies

Automatic expiration allows you to deprecate stale intelligence based on a set of defined criteria. As the data becomes less relevant, ThreatQ sets the status to Expired, which relieves the data burden on your team or infrastructure.

Accessing the Indicator Expiration Page

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

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



Data Controls

Indicator Expiration Scoring TLP Whitelisted Indicators

Indicator Expiration

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

Search for a source...

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

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

How ThreatQ Calculates Expiration Dates

SCENARIO

DESCRIPTION

Indicator Reported by Source with an Expiration Policy

If an indicator has an expiration date and it's reported by a new source that has an expiration policy, ThreatQ will set the expiration date using the policy with the greater expiration date.

Indicator Report by a Source with an Expiration Policy of Never Expire

If an indicator has an expiration date and it's reported by a new source that has an expiration policy of Never Expire, ThreatQ sets that indicator to Never Expire.

Indicator Reported by a Source with an Exception for that Indicator

If an indicator is reported by a source that has an exception for the indicator, the exception expiration date will be used regardless of the greater expiration date.
An exception takes precedence over the source's expire policy.

Indicator Reported by Two Different Sources

If an indicator is reported by a source with an Expiration Policy and then reported by a second source with another Expiration Policy, the greatest expiration date is selected to set the expiration date. The expiration date will be set based on the date the second source reported the indicator.

Indicator Reported by Two Different Sources, one with an Exception

If an indicator is reported by a source that has an exception for the indicator and then reported by a second source, the greatest expiration date is selected despite the exception. The expiration date will be set based on the date the second source reported the indicator.

Selecting an Expiration Policy per Feed

You can choose from three options when configuring an expiration policy for a source of intelligence:

OPTION	DESCRIPTION
Don't automatically expire (No policy set)	ThreatQ sets all feeds to Don't Automatically Expire until an analyst decides otherwise. When set, indicators reported from this specific feed do not have an expiration date automatically applied to them. If an indicator is reported by Source A (an intelligence feed without an expiration policy), and is later reported by Source B (an intelligence feed that expires data in 7 days), ThreatQ sets the indicators to automatically expire in 7 days.
Automatically Expire Indicators	When setting a specific intelligence feed to Automatically Expire Indicators, ThreatQ requires you to provide a specific number of days. After you configure this setting, it applies to all intelligence currently in the system, as well as new intelligence as it is ingested. ThreatQ

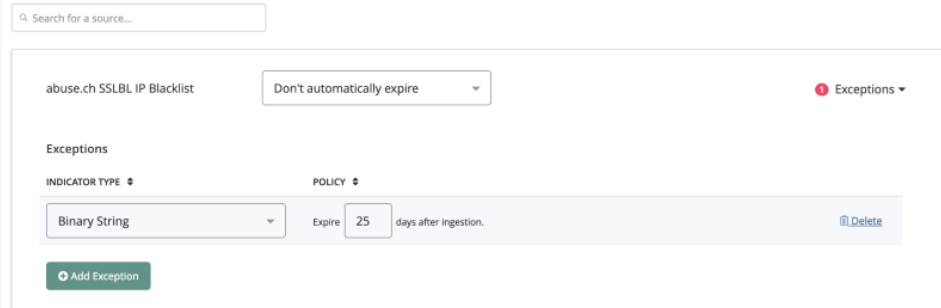
OPTION

DESCRIPTION

calculates the appropriate expiration date based on the number of days from ingestion. Once an indicator's expiration date is met, its status changes to **Expired**.

Automatic Expiration

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



Search for a source...

abuse.ch SSLBL IP Blacklist Don't automatically expire Exceptions

Exceptions

INDICATOR TYPE	POLICY
Binary String	Expire 25 days after ingestion.

Add Exception Delete

Never Expire

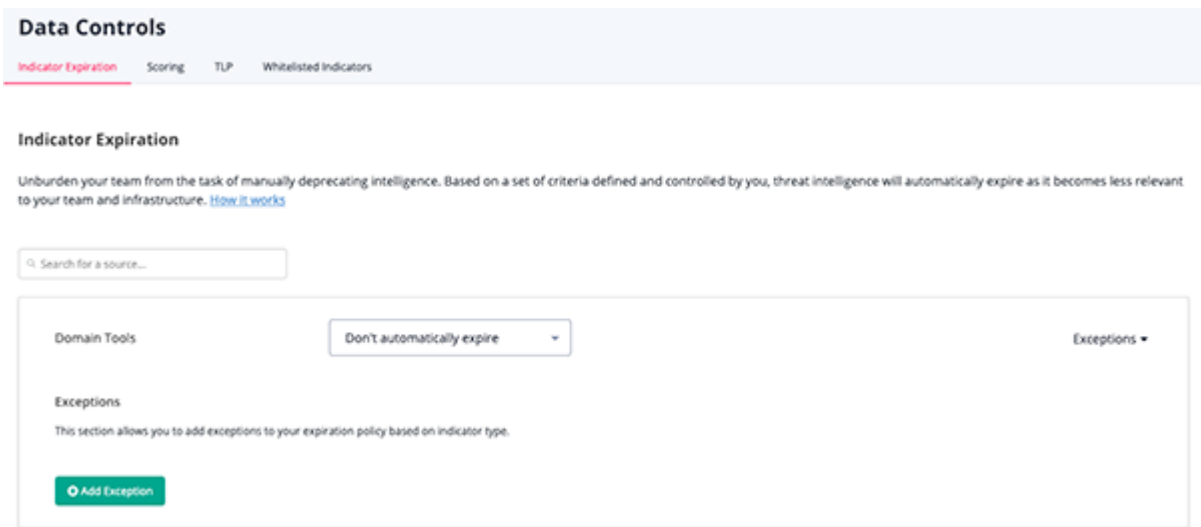
Using this setting ensures that all intelligence reported by a specific feed is protected from automatic expiration, regardless of scenario.

Adding Exceptions

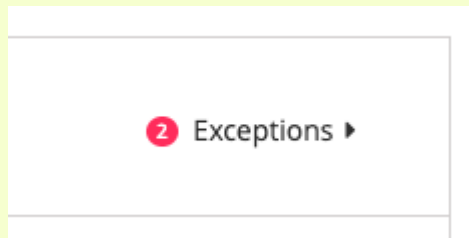
ThreatQ allows you to add exceptions based on specific indicator types within in a feed in addition to setting an expiration policy at a global level for all intelligence ingested by a specific feed.

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

The Exceptions option menu opens.




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)	- On 10/1, Source A reports the indicator and the expiration date is set to 10/8. - When the date switches from 10/7 to 10/8, this indicator is queued to have its status changed to Expired.
An indicator is reported by Source A (with an expiration policy of 7 days) and 3 days later is reported	- On 10/1, Source A reports the indicator and the expiration date is set to 10/8. - 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

SCENARIO	DESCRIPTION
by Source B (with an expiration policy of 10 days).	date will be 10/14 (10 days from when it was reported by Source B). 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).	- On 10/1, Source A reports the indicator and the expiration date is set to 7 days. - 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.
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).	- 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. - 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). - When the date switches from 10/17 to 10/18, this indicator is queued to have its status changed to Expired.

Common Expiration Policy Scenarios - Feed Updates of Indicator Statuses

SCENARIO	DESCRIPTION
Default Indicator Status Behavior:	
An indicator is currently set to Expired and is reported by Source A (with an expiration policy of 7 days).	On 10/1, an indicator is in ThreatQ with a status of Expired.

SCENARIO	DESCRIPTION
	On 10/1, Source A reports the indicator. The status of the indicator does not change.
An indicator is currently set to Expired and is reported by Source A (with an expiration policy of Never Expire).	- An indicator is in ThreatQ with a status of Expired. - Source A, with an expiration policy of Never Expire, reports the indicator. The status of the indicator does not change.
Status Behavior with Indicator/Signature Status Overrides Enabled:	
An indicator is currently set to Expired and is reported by Source A (with an expiration policy of 7 days).	- On 10/1, an indicator is in ThreatQ with a status of Expired. - 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. - 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).	- An indicator is in ThreatQ with a status of Expired. - Source A, with an expiration policy of Never Expire, reports the indicator. The expiration of that indicator changes to Protect from auto-expiration.

Data Retention Policy



We recommend that you perform a backup of your ThreatQ instance before implementing a Data Retention Policy.

Setting up a Data Retention Policy allows you to automatically delete system objects from the Threat Library using a data collection to specify the criteria for deletion.



Similar to the bulk delete process, the Data Retention Policy does not support the deletion of tasks or files.

When ThreatQ applies the Data Retention Policy, it runs a bulk delete job to delete all objects included in the data collection. For example, you can create a data collection that captures all Indicators with an expiration date older than fifteen days ago. When you add this data collection to your Data Retention Policy, a Retention Policy job runs each day that deletes indicators with expiration dates prior to fifteen days ago.

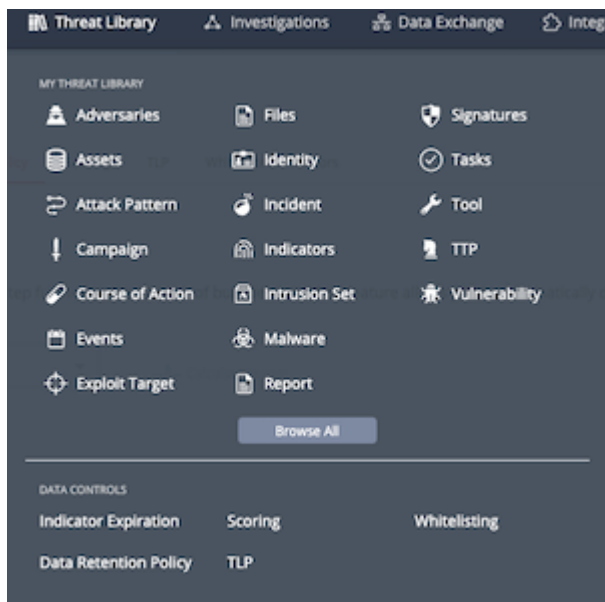
After you enable your data retention policy, ThreatQ provides updates on the associated object deletions through system notifications and the Job Management page.

Tips and Tricks

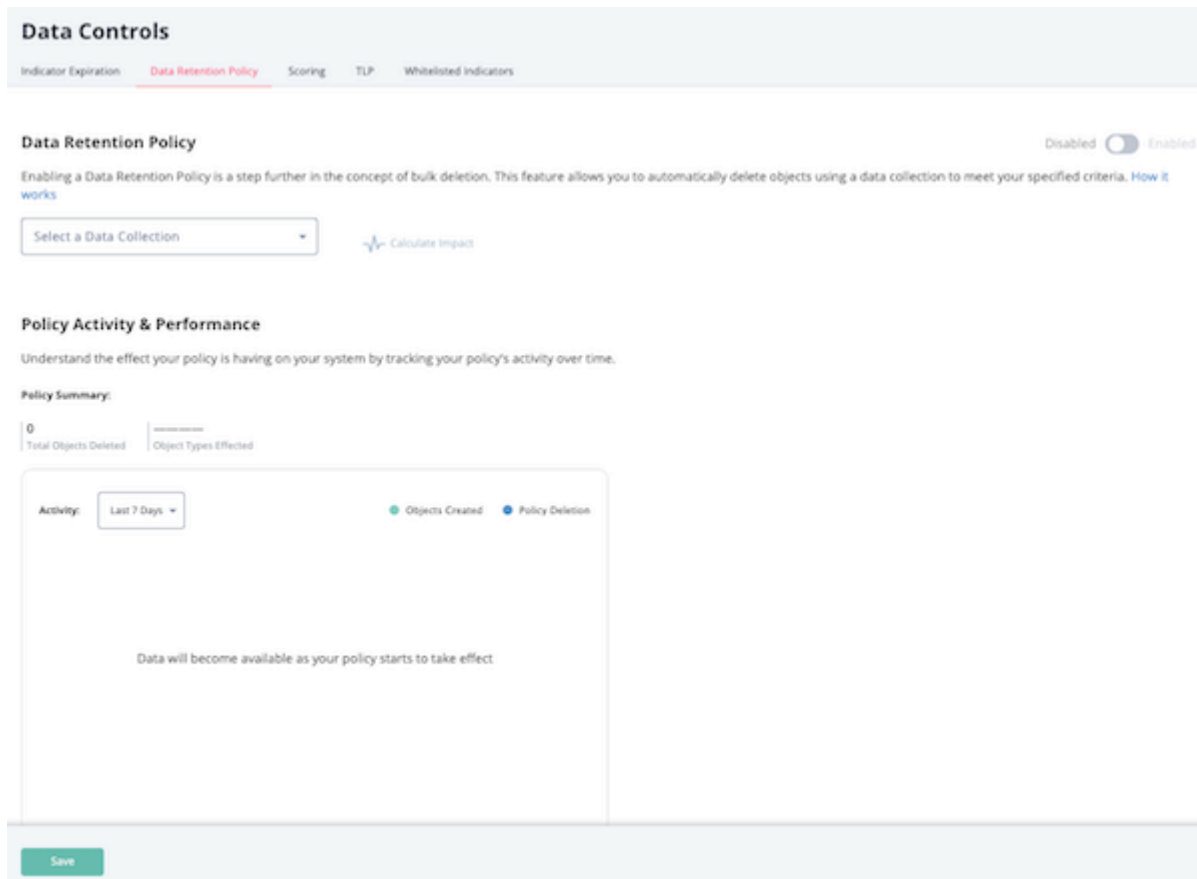
- If the data collection used by a Data Retention Policy is not shared with you the Select a saved search field displays the following text: **This collection has not been shared.** In addition, you cannot disable or enable the data retention policy. As such, ThreatQuotient recommends you give all Admin or Maintenance users who work with this page at least Viewer permissions for the data collection.
- If you disable the data retention policy, the Policy Activity & Performance graph continues to track created objects.

Accessing the Data Retention Policy Page

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



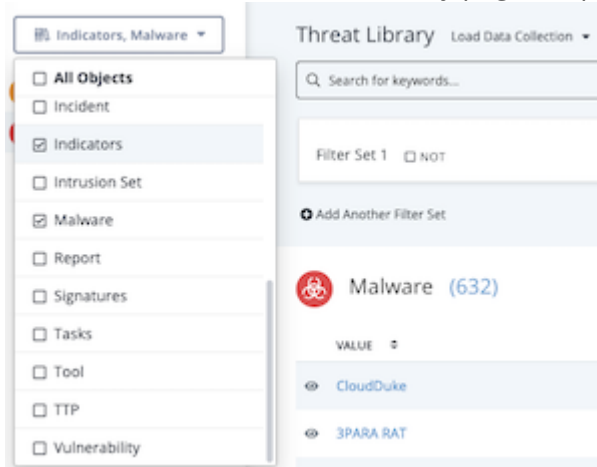
The Data Controls page is displayed with the Data Retention Policy tab selected.



Creating a Data Collection for the Data Retention Policy

Before you create a Data Retention Policy, you must create/select the data collection that used to identify the system objects to be deleted during the Policy's scheduled run. We recommend you apply the following guidelines in creating a Data Collection for use by your Data Retention Policy:

- To restrict your Data Retention Policy to specific object types, use the object type filter on the left side of the main Threat Library page to specify the object types for your data collection.



- Since your Data Retention Policy cannot delete tasks or files, your data collection should not include these system objects.
- If more than one Admin or Maintenance user will maintain/monitor the Data Retention Policy, make sure that each of these users has, at minimum, Viewer permissions for the data collection. This ensures that these users can view the name of the assigned data collection in the Data Retention Policy tab as well as enable/disable the data retention policy.

See the [Managing Search Results](#) topic for step-by-step instructions on creating a data collection.

Creating a Data Retention Policy

1. [Create a data collection](#) that includes the system objects you want to delete.
2. In the Data Retention Policy tab, click the Select a Data Collection field to locate and select the data collection you created in step 1.



The drop-down list for this field displays all the data collections that are shared with you as well as the ones you own.

3. Click the Calculate Impact option to view how many objects will be removed during the initial application of the data retention policy.
4. To save the data collection you selected without enabling the data retention policy, click the **Save** button.

If the data collection is in use in another area such as a dashboard, the **Are You Sure?** window prompts you to click the **Save** button to confirm your action.

To enable the data retention policy with the data collection you selected, move the Disabled/Enabled toggle to Enabled.

5. After you enable the data retention policy:
 - o The system creates and begins processing the first job to apply the data retention policy you configured.
 - o You receive a notification center message reminding you that you can monitor the progress of the job from the [Job Management](#) page where it is listed with a Job Type of Retention Policy.



To view the notification center message, you must refresh your browser.

- After the initial job is complete, the system creates and runs a job for the data retention policy each day at 12 AM UTC. After the daily job run, the Policy & Activity Performance graph reflects the objects deleted by the data retention policy.

Reviewing Data Retention Policy Performance

The Policy Activity & Impact section of the Data Retention Policy page displays a line chart that represents objects deleted by the data retention policy and objects created. By default, the Policy Activity & Performance section displays the last 7 days of activity. You can change the date range displayed by clicking the Activity field and selecting Monthly or Yearly. You can click a point on the graph to view object details for a specific day such as the total objects deleted, total objects created, and deletion counts by object type.

Chart Updates

The object data displayed in the Policy Activity & Impact chart during the day is cached data reflecting the most recent objects created and policy deletion update processes:

- **Objects Created** - Updates at 8 AM UTC and reflects the objects created from 12 AM UTC of the prior day until 12 AM UTC of the current day.
- **Policy Deletion** - Updates after each 12 AM UTC processing of the Data Retention Policy and reflects the policy deletions since the last 12 AM UTC process.

When you update your data retention policy, the line chart does not reflect your updates until the next objects created and policy deletion processes complete.

Policy Activity & Performance

Understand the effect your policy is having on your system by tracking your policy's activity over time.

Policy Summary: Last Modified: 06/03/2021 9:32am

36,000

Total Objects Deleted



Object Types Effectuated



Mon, Feb 15

6,200

Total Deleted

3,240

Total Created

Object Type

Deleted Counts

Events

3,200

Indicators

3,000

Scoring Algorithms

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

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

Accessing the Scoring Sensitivity Page

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

Scoring Criteria

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

- Indicator Type
- Indicator Source
- Attributes
- Adversary Relationship

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

Scoring Tips and Tricks

- The **Calculate Impact** option identifies how many system objects are affected by a score change.
- Scoring configuration and updates take time to process, the Threat Library does not reflect these changes immediately.
- If you use an indicator's object details page to [manually update its score](#), the manually selected score overrides any changes to the calculated score caused by updates to the scoring algorithm.
- You have the option to adjust the score sensitivity of indicators. Indicator scores range from 10, which creates a score of **Very High**, to -10, **Very Low**. A higher indicator score creates increased priority for that indicator.
- By default, indicators are set to a neutral score of 0.

Configuring Your Scoring Algorithm for Indicator Types and Sources

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

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

1. Select the indicator type or source by filtering by source name or by scrolling to the desired indicator.
2. Use one of the following methods to adjust scoring:
 - Click and drag the slider to adjust the score.
 - Click the up/down arrow next to the current score to increase/decrease the score.
3. To save your changes, click the **Apply** button.

Configuring Your Scoring Algorithm for Attributes

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



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

1. From the Attributes tab, click the **Add** button.
2. Use one of the following methods to specify an attribute key:
 - Click the arrow in the Key field to select an attribute type from the dropdown list.
 - Type the attribute key in the Key field.
3. Use one of the following methods to populate the Value field:
 - Enter the attribute value to which the score applies.

- Enter an attribute value that contains the wildcard character (*). The wildcard specifies that any characters can appear in multiple positions represented by the wildcard.
 - 4. Use one of the following methods to adjust the score:
 - Click and drag the slider to adjust the score.
 - Click the up/down arrow next to the current score to increase/decrease the score.
 - 5. Click the **Add** button to continue adding attribute scoring criteria.
 - 6. Click the **Apply** button to save your attribute scoring.
- The Attributes tab now lists your scoring entry in the following format:
- <Key> is <Value>

Configuring Your Scoring Algorithm for Adversary Relationships

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

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

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



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

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

Updating Your Scoring Algorithms

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

- Changes to your risk profile based on political or organization changes.
 - New adversaries
 - New adversary tactics
 - New tool sets
1. Click the appropriate tab (Indicator Type, Indicator Source, Attributes, Adversary Relationship).
 2. Use one of the following methods to adjust the score:
 - Click and drag the slider to adjust the score.
 - Click the up/down arrow next to the current score to increase/decrease the score.
 3. Click the **Apply** button to save your update.

Traffic Light Protocol (TLP)

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



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

Labels

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

LIGHT	LABEL	DESCRIPTION
	Red	Not for disclosure, restricted to participants only.
	Amber+strict	Limited disclosure, restricted to participants' organization.
	Amber	Limited disclosure, restricted to participants' organization and its clients.
	Green	Limited disclosure, restricted to the community.
	Clear	Disclosure is not limited.

TLP Assignment Hierarchy

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

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

Source Provided Data TLP label received from ingested data.

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

No TLP A TLP label has not been set for the source.

Access TLP Settings

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

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

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

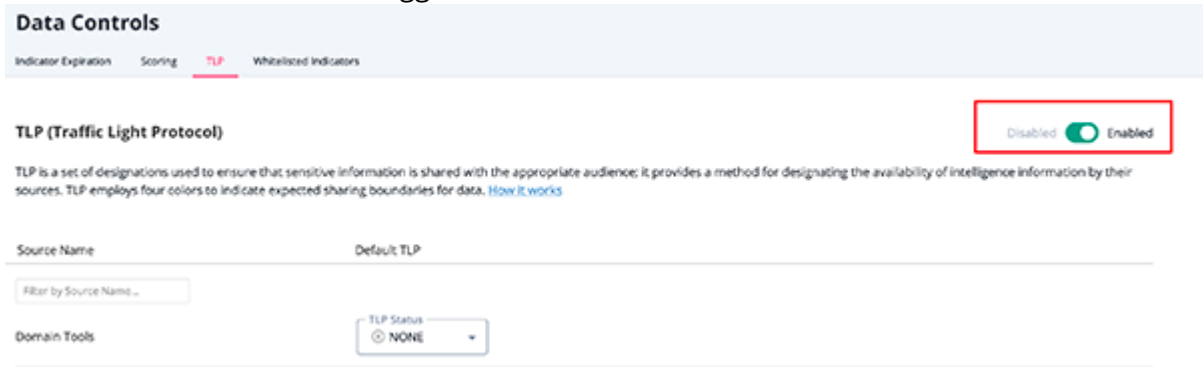
The screenshot shows the ThreatQ interface with the 'Data Controls' section selected. The 'TLP' tab is active. The 'TLP (Traffic Light Protocol)' section is displayed, showing a toggle switch for 'Disabled' (selected) and 'Enabled'. Below this, a table lists system sources and their default TLP status. The table has two columns: 'Source Name' and 'Default TLP'. The sources listed are 'Domain Tools', 'Emerging Threats', 'This Platform', 'threatq@threatq.com', and 'VirusTotal'. Each source has a 'TLP Status' dropdown menu set to 'NONE'. A 'Save' button is located at the bottom of the page.

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

Configure TLP Visibility

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

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



Data Controls

Indicator Expiration Scoring **TLP** Whitelisted Indicators

TLP (Traffic Light Protocol)

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

Source Name Default TLP

Filter by Source Name...

Domain Tools TLP Status: NONE

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

Apply a TLP Label to Source

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



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

TLP (Traffic Light Protocol)

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

Source Name

Default TLP

do

Domain Tools

TLP Status

⊗ NONE

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

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...	
CrowdStrike Indicators	TLP Status RED
Domain Tools	RED AMBER+STRICT AMBER GREEN CLEAR
Emerging Threats	
MITRE Enterprise ATT&CK	AMBER+STRICT

- Click **Save**.



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

Whitelisted Indicators

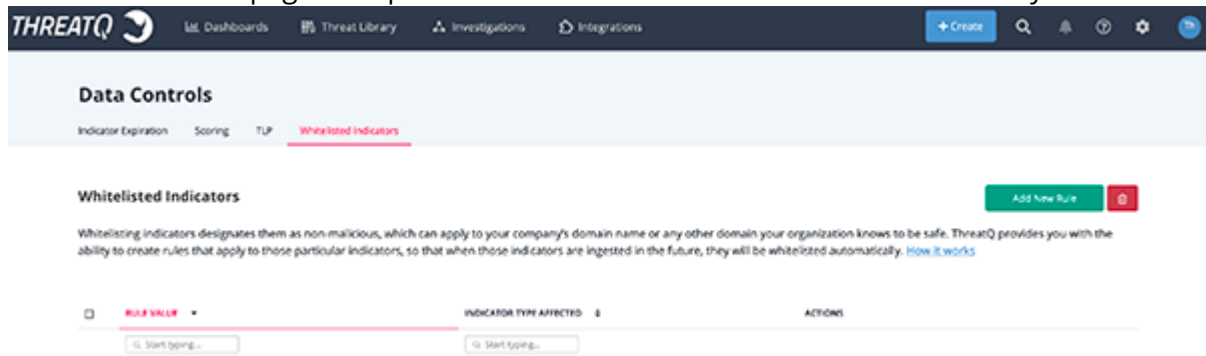
There are some Indicators that should be considered to be whitelisted, or non-malicious, and we do not want those indicators going out to other systems. For example, a company's own domain name would never need to be blocked.

The Whitelisting process creates rules that apply to particular indicators, so that when those indicators come in in the future, they will be automatically whitelisted.

Accessing the Whitelisted Indicator Rules

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

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



Creating a Whitelisted Rule



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

From the Whitelisted Indicators Page:

1. Click **Add Rule**.

The Add Whitelist Rules dialog box opens.



Add Whitelist Rule [Close]

Which indicator type will this rule apply to? CVE

Rule Value CVE-2015-1461

Next

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

Affected indicators are listed in the dialog box.



Add Whitelist Rule [Close]

This rule will affect 1 indicators.

Add Rule [Continue Editing This Rule](#)

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?

Rule Value

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.

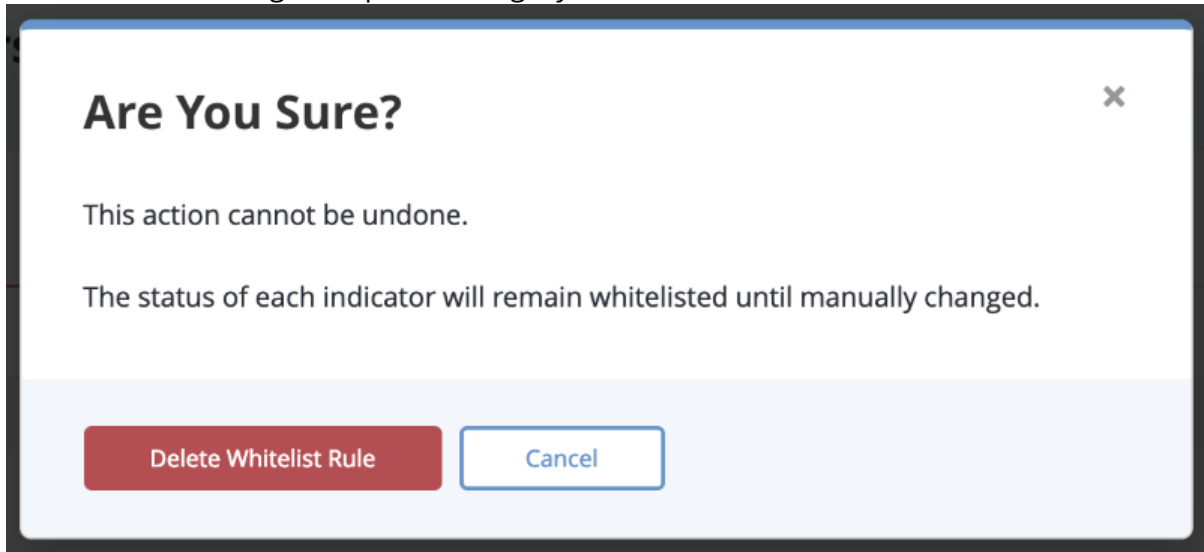


Any new indicators will also have the rule applied to them as they enter the system.

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

About 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.

ExportsNeed help? Click here for Exports documentation.Add New Export

25

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

ThreatQ provides a number of standard system exports that have previously been identified as useful. You have the option to use those and create your own. ThreatQ Exports are built on the Smarty PHP Template Engine; see <https://www.smarty.net/>.



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

Managing Exports

Accessing the Exports List

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

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

Exports

Need help? Click here for Exports documentation. [Add New Export](#) 

25

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

Viewing an Export

1. From the Exports page, click the export's URL.
2. A new tab opens in your browser. This tab displays the data returned from the export.



The load time may be lengthy depending on the amount of data returned.

Enabling/Disabling Exports

1. From the Exports page, locate the export you want to enable/disable.
2. Toggle the switch in the On/Off column to enable/disable the export.

Adding an Export

1. From the Exports page, click + **Add Export**.
The Connection Settings window opens.

Connection Settings ×

Export Name

ArcSight MD5

Token

V9Wm0mRcESFAh1HYTUEkMJPBwhYICpKt

Save Settings

Cancel

2. Enter the export name.
3. Verify or edit the token.

4. Click the **Next Step** button.
The Output Format dialog box opens.

Output Format

Type of information you would like to export?

Indicators

Output type

text/plain

Filter by TLP

☐ Red
 ☐ Amber+Strict
 ☐ Amber
 ☐ Green
 ☐ Clear
 ☐ Not Specified

Special Parameters (optional)

Provide URL Parameters to further refine information being exported: [Learn more about managing exports.](#)

Insert Variable

Output Format Template

{ }

Save Settings

Cancel

5. Populate the following fields:

FIELD	VALUE
Which type of information would you like to export?	Select the system object type you want to include in the export. An admin has the ability to choose between the following options: ○ Adversaries ○ Attack Patterns ○ Campaigns ○ Courses of Actions ○ Events ○ Exploit Targets ○ Identity ○ Incidents ○ Indicators ○ Intrusion Sets ○ Malware ○ Reports ○ Signatures ○ Tools ○ TTPs ○ Vulnerabilities
Output Type	Select a format for the export such as text/plain or text/json. 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. See http://www.w3.org/Protocols/rfc1341/4_Content-Type.html for more information.
Filter by TLP	(Optional) By default, all the TLP filter options are checked so that your export includes all objects regardless of their sources' TLP labels. To exclude objects with a particular TLP label, you can uncheck the box to the left of the label name. For example, to omit objects with sources assigned a Red TLP label, uncheck the Red box.  The Filter by TLP field options will only appear if administrators have enabled Traffic Light Protocol (TLP) viewing. See the Traffic Light Protocol (TLP) topic for more information.
Special Parameters	(Optional) See the Output Format Options topic for more information. 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.

FIELD	VALUE
Output Format Template	(Optional) See the Output Format Templates topic for more information. Choosing this option means you lose the ability to have one place to manage what is being exported.

6. Click **Save Settings**.

The export you just created appears at the bottom of the Exports table. By default, the new export is toggled to Off.

Duplicating an Export

Duplicating an export creates a new version that you can edit.

1. From the Exports page, locate the Export you wish to duplicate.
2. Click the **duplicate** option in the Actions column.

The duplicate appears at the bottom of the Exports table. By default, the copy you just created is toggled to Off.

Editing an Export's Connection Settings

Connection settings are available for each of the exports. The Connection Settings window contains the name of the export as well as the token you need to 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. From the Exports page, locate the export you want to edit.
2. Click **connection settings** in the Connection column.

The Connection Settings window opens.

Connection Settings ×

Export Name

ArcSight MD5

Token

V9Wm0mRcESFAh1HYTUEkMJPBwhYICpKt

Save Settings

Cancel

3. Enter your changes.
4. Click the **Save Settings** button.

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 as well as copies of the original exports.

1. From the Exports page, locate the export you want to edit.
2. Click **output format** in the Output Format column.
3. From the Output Format window, enter your changes.
4. Click the **Save Settings** button.

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. From the Exports page, locate the export(s) you wish to delete.
2. Select one or more exports.
3. Click the delete icon at the top right of the Exports table.

Output Format Options

Customizing the Output Format Template

You can customize the output format template for an custom or duplicated export.

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

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

2. Locate the export for which you want to customize the output format template.
3. Click **output format**.
4. In the Output Format dialog box, customize the output format template by clicking the location for the variable, clicking the **Insert Variable** button and selecting the variable from the dropdown list.

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



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

```
{foreach $data as $indicator}  
  
Your variables go here  
  
{/foreach}
```

The Output Format Template is populated based on your selection.

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

Disabling Export Logging

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

Adding Special Parameters

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

Examples:

TO EXPORT ALL INDICATORS WITH AN
ACTIVE STATUS

INDICATOR.STATUS=ACTIVE

To export all CIDR Block indicators that
have an active status

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

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

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

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

Indicator.Score>=7

Filtering Special Parameters

A wide range of filtering parameters are available:

Indicator

```
indicator.type_id
indicator.status_id
indicator.value
indicator.description
indicator.hash
indicator.last_detected_at
indicator.expires_at
indicator.expired_at
indicator.touched_at
indicator.deleted_at
indicator.deleted
indicator.sources_count
indicator.sources.dates=Y
indicator.id
indicator.status
indicator.type
indicator.sincedeleted
indicator.whitelisted *
indicator.score
indicator.created_at
indicator.updated_at
indicator.Sources
indicator.Attributes
indicator.Tags
indicator.Assets
```

* Using the `indicator.whitelisted=Y` flag allows whitelisted indicators to be exported. It does not filter indicators by the whitelisted status. For that option, use the `indicator.status=whitelistedflag`. Additionally, to include only whitelisted indicators in

your export, you will need to use both flags:
`indicator.status=Whitelisted&indicator.whitelisted=Y`

Indicators - Related Objects

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

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

Assets

```
assets.value
assets.description
assets.Sources
assets.Attributes
assets.Indicators
assets.Adversaries
assets.Events
assets.Attachments
assets.Signatures
assets.Investigations
assets.Tasks
assets.Campaign
assets.Course_of_action
assets.Exploit_target
assets.Incident
assets.Ttp
assets.Attack_pattern
assets.Identity
assets.Intrusion_set
```

```
assets.Malware
assets.Report
assets.Tool
assets.Vulnerability
assets.Tags
assets.Assets
```

Adversary

```
adversary.name
adversary.touched_at
adversary.deleted_at
adversary.deleted
adversary.sources_count
adversary.id
adversary.description
adversary.created_at
adversary.updated_at
adversary.Sources
adversary.sources.dates=Y
adversary.Attributes
adversary.Indicators
adversary.Adversaries
adversary.Events
adversary.Attachments
adversary.Signatures
adversary.Investigations
adversary.Tasks
adversary.Campaign
adversary.Course_of_action
adversary.Exploit_target
adversary.Incident
adversary.Ttp
adversary.Attack_pattern
adversary.Identity
adversary.Intrusion_set
adversary.Malware
adversary.Report
adversary.Tool
adversary.Vulnerability
adversary.Tags
adversary.Assets
```

Event

```
event.type_id
event.title
event.happened_at
event.hash
event.description
```



```
event.deleted_at
event.deleted
event.sources_count
event.id
event.type
event.touched_at
event.created_at
event.updated_at
event.Sources
event.sources.dates=Y
event.Attributes
event.Indicators
event.Adversaries
event.Events
event.Attachments
event.Signatures
event.Investigations
event.Tasks
event.Campaign
event.Course_of_action
event.Exploit_target
event.Incident
event.Ttp
event.Attack_pattern
event.Identity
event.Intrusion_set
event.Malware
event.Report
event.Tool
event.Vulnerability
event.Tags
event.Assets
```

Signature

```
signature.description
signature.hash
signature.last_detected_at
signature.name
signature.status_id
signature.touched_at
signature.type_id
signature.value
signature.deleted_at
signature.deleted
signature.sources_count
signature.id
signature.status
signature.type
signature.created_at
signature.updated_at
```

```
signature.Sources
signature.sources.dates=Y
signature.Attributes
signature.Indicators
signature.Adversaries
signature.Events
signature.Attachments
signature.Signatures
signature.Investigations
signature.Tasks
signature.Campaign
signature.Course_of_action
signature.Exploit_target
signature.Incident
signature.Ttp
signature.Attack_pattern
signature.Identity
signature.Intrusion_set
signature.Malware
signature.Report
signature.Tool
signature.Vulnerability
signature.Tags
signature.Assets
```

Campaign

```
campaign.value
campaign.status_id
campaign.type_id
campaign.description
campaign.objective
campaign.started_at
campaign.ended_at
campaign.deleted_at
campaign.deleted
campaign.sources_count
campaign.id
campaign.status
campaign.type
campaign.touched_at
campaign.created_at
campaign.updated_at
campaign.Sources
campaign.sources.dates=Y
campaign.Attributes
campaign.Indicators
campaign.Adversaries
campaign.Events
campaign.Attachments
campaign.Signatures
```

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

Course of Action

```
course_of_action.value
course_of_action.status_id
course_of_action.type_id
course_of_action.description
course_of_action.deleted_at
course_of_action.deleted
course_of_action.sources_count
course_of_action.sources.dates=Y
course_of_action.id
course_of_action.status
course_of_action.type
course_of_action.touched_at
course_of_action.created_at
course_of_action.updated_at
course_of_action.Sources
course_of_action.Attributes
course_of_action.Indicators
course_of_action.Adversaries
course_of_action.Events
course_of_action.Attachments
course_of_action.Signatures
course_of_action.Investigations
course_of_action.Tasks
course_of_action.Campaign
course_of_action.Course_of_action
course_of_action.Exploit_target
course_of_action.Incident
course_of_action.Ttp
course_of_action.Attack_pattern
course_of_action.Identity
course_of_action.Intrusion_set
course_of_action.Malware
```

```
course_of_action.Report
course_of_action.Tool
course_of_action.Vulnerability
course_of_action.Tags
course_of_action.Assets
```

Exploit

```
exploit_target.value
exploit_target.status_id
exploit_target.type_id
exploit_target.description
exploit_target.deleted_at
exploit_target.deleted
exploit_target.sources_count
exploit_target.sources.dates=Y
exploit_target.id
exploit_target.status
exploit_target.type
exploit_target.touched_at
exploit_target.created_at
exploit_target.updated_at
exploit_target.Sources
exploit_target.Attributes
exploit_target.Indicators
exploit_target.Adversaries
exploit_target.Events
exploit_target.Attachments
exploit_target.Signatures
exploit_target.Investigations
exploit_target.Tasks
exploit_target.Campaign
exploit_target.Course_of_action
exploit_target.Exploit_target
exploit_target.Incident
exploit_target.Ttp
exploit_target.Attack_pattern
exploit_target.Identity
exploit_target.Intrusion_set
exploit_target.Malware
exploit_target.Report
exploit_target.Tool
exploit_target.Vulnerability
exploit_target.Tags
exploit_target.Assets
```

Incident

```
incident.value
incident.status_id
incident.type_id
incident.description
incident.started_at
incident.ended_at
incident.deleted_at
incident.deleted
incident.sources_count
incident.sources.dates=Y
incident.id
incident.status
incident.type
incident.touched_at
incident.created_at
incident.updated_at
incident.Sources
incident.Attributes
incident.Indicators
incident.Adversaries
incident.Events
incident.Attachments
incident.Signatures
incident.Investigations
incident.Tasks
incident.Campaign
incident.Course_of_action
incident.Exploit_target
incident.Incident
incident.Ttp
incident.Attack_pattern
incident.Identity
incident.Intrusion_set
incident.Malware
incident.Report
incident.Tool
incident.Vulnerability
incident.Tags
incident.Assets
```

TTP

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

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

Attack Pattern

```
attack_pattern.value
attack_pattern.status_id
attack_pattern.type_id
attack_pattern.description
attack_pattern.deleted_at
attack_pattern.deleted
attack_pattern.sources_count
attack_pattern.sources.dates=Y
attack_pattern.id
attack_pattern.status
attack_pattern.type
attack_pattern.touched_at
attack_pattern.created_at
attack_pattern.updated_at
attack_pattern.Sources
attack_pattern.Attributes
attack_pattern.Indicators
attack_pattern.Adversaries
attack_pattern.Events
```

```

attack_pattern.Attachments
attack_pattern.Signatures
attack_pattern.Investigations
attack_pattern.Tasks
attack_pattern.Campaign
attack_pattern.Course_of_action
attack_pattern.Exploit_target
attack_pattern.Incident
attack_pattern.Ttp
attack_pattern.Attack_pattern
attack_pattern.Identity
attack_pattern.Intrusion_set
attack_pattern.Malware
attack_pattern.Report
attack_pattern.Tool
attack_pattern.Vulnerability
attack_pattern.Tags
attack_pattern.Assets

```

Identity

```

identity.value
identity.status_id
identity.type_id
identity.description
identity.contact_information
identity.deleted_at
identity.deleted
identity.sources_count
identity.sources.dates=Y
identity.id
identity.status
identity.type
identity.touched_at
identity.created_at
identity.updated_at
identity.Sources
identity.Attributes
identity.Indicators
identity.Adversaries
identity.Events
identity.Attachments
identity.Signatures
identity.Investigations
identity.Tasks
identity.Campaign
identity.Course_of_action
identity.Exploit_target
identity.Incident
identity.Ttp
identity.Attack_pattern

```

```
identity.Identity
identity.Intrusion_set
identity.Malware
identity.Report
identity.Tool
identity.Vulnerability
identity.Tags
identity.Assets
```

Intrusion Set

```
intrusion_set.value
intrusion_set.status_id
intrusion_set.type_id
intrusion_set.description
intrusion_set.started_at
intrusion_set.ended_at
intrusion_set.deleted_at
intrusion_set.deleted
intrusion_set.sources_count
intrusion_set.sources.dates=Y
intrusion_set.id
intrusion_set.status
intrusion_set.type
intrusion_set.touched_at
intrusion_set.created_at
intrusion_set.updated_at
intrusion_set.Sources
intrusion_set.Attributes
intrusion_set.Indicators
intrusion_set.Adversaries
intrusion_set.Events
intrusion_set.Attachments
intrusion_set.Signatures
intrusion_set.Investigations
intrusion_set.Tasks
intrusion_set.Campaign
intrusion_set.Course_of_action
intrusion_set.Exploit_target
intrusion_set.Incident
intrusion_set.Ttp
intrusion_set.Attack_pattern
intrusion_set.Identity
intrusion_set.Intrusion_set
intrusion_set.Malware
intrusion_set.Report
intrusion_set.Tool
intrusion_set.Vulnerability
intrusion_set.Tags
intrusion_set.Assets
```


Malware

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

Report

```
report.value
report.status_id
report.type_id
report.description
report.deleted_at
report.deleted
report.sources_count
report.id
```

```
report.status
report.type
report.touched_at
report.created_at
report.updated_at
report.Sources
report.sources.dates=Y
report.Attributes
report.Indicators
report.Adversaries
report.Events
report.Attachments
report.Signatures
report.Investigations
report.Tasks
report.Campaign
report.Course_of_action
report.Exploit_target
report.Incident
report.Ttp
report.Attack_pattern
report.Identity
report.Intrusion_set
report.Malware
report.Report
report.Tool
report.Vulnerability
report.Tags
report.Assets
```

Tool

```
tool.value
tool.status_id
tool.type_id
tool.description
tool.deleted_at
tool.deleted
tool.sources_count
tool.sources.dates=Y
tool.id
tool.status
tool.type
tool.touched_at
tool.created_at
tool.updated_at
tool.Sources
tool.Attributes
tool.Indicators
tool.Adversaries
tool.Events
```

```

tool.Attachments
tool.Signatures
tool.Investigations
tool.Tasks
tool.Campaign
tool.Course_of_action
tool.Exploit_target
tool.Incident
tool.Ttp
tool.Attack_pattern
tool.Identity
tool.Intrusion_set
tool.Malware
tool.Report
tool.Tool
tool.Vulnerability
tool.Tags
too.Assets

```

Vulnerability

```

vulnerability.value
vulnerability.status_id
vulnerability.type_id
vulnerability.description
vulnerability.deleted_at
vulnerability.deleted
vulnerability.sources_count
vulnerability.sources.dates=Y
vulnerability.id
vulnerability.status
vulnerability.type
vulnerability.touched_at
vulnerability.created_at
vulnerability.updated_at
vulnerability.Sources
vulnerability.Attributes
vulnerability.Indicators
vulnerability.Adversaries
vulnerability.Events
vulnerability.Attachments
vulnerability.Signatures
vulnerability.Investigations
vulnerability.Tasks
vulnerability.Campaign
vulnerability.Course_of_action
vulnerability.Exploit_target
vulnerability.Incident
vulnerability.Ttp
vulnerability.Attack_pattern
vulnerability.Identity

```

```
vulnerability.Intrusion_set  
vulnerability.Malware  
vulnerability.Report  
vulnerability.Tool  
vulnerability.Vulnerability  
vulnerability.Tags  
vulnerability.Assets
```



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

Adding Differential Flags

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

Include the following to limit exports to new data only:

```
differential=1
```

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



external system 1

```
https://{tq-host}/api/export/c2ab6df72e67ee13cef90f0e00981b62/?  
token=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. However, you lose the option of having one place to manage what is being exported via that export.

Using Logical Operators in Export Filters

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

1. Searching using greater than, less than, or equal to
 - Examples in special parameters string section:

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

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

- Examples in request URI:

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

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

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

- Example in special parameters string section:

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

- Example in request URI:

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

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

- Example in special parameters string section:

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

- Example in request URI:

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

Output Format Templates

The following section contains templates that you can use to customize an export's output format. The Output Format Template field for an export is found under its Output Format modal. You can access this by clicking the **Output Format** link for an export from the main Exports page



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

Adversaries Template

```
{foreach $data as $adversary}
ID: {$adversary.id}
Name: {$adversary.name}
Description: {$adversary.description}
Created At: {$adversary.created}
Updated At: {$adversary.updated_at}
Touched At: {$adversary.touched_at}
Deleted At: {$adversary.deleted_at}
Deleted: {$adversary.deleted}
```

Your variables go here

```
{/foreach}
```

Events Template

```
{foreach $data as $event}

{$event.title} ID: {$event.id}
Title: {$event.title}
Type: {$event.type}
Happened: {$event.happened_at}
Description: {$event.description}
Created At: {$event.created}
Updated At: {$event.updated_at}
Touched At: {$event.touched_at}
Deleted At: {$event.deleted_at}
Deleted: {$event.deleted}
```

Your variables go here

```
{/foreach}
```

Indicators Template

```
{foreach $data as $indicator}

{$indicator.value}
ID: {$indicator.id}
Value: {$indicator.value}
Type: {$indicator.type}
Status: {$indicator.status}
Class: {$indicator.class}
Description: {$indicator.description}
Score: {$indicator.score}
Hash: {$indicator.hash}
Source Count: {$indicator.sources_count}
Whitelisted: {$indicator.whitelisted}
Last Detected At: {$indicator.last_detected_at}
Created At: {$indicator.created_at}
Updated At: {$indicator.updated_at}
Touched At: {$indicator.touched_at}
Since Deleted: {$indicator.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 be added to the templates provided above.

Source Variable

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

Attribute Variable

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

Adversary Variable

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

Attachment Variable

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

Event Variable

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



```
Value: {$event.value}  
{/foreach}
```

Indicator Variable

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

Investigation Variable

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

Signature Variable

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

Tag Variable

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

Task Variable

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

Specific Indicator Export Configurations

ThreatQuotient provides several guides with instructions on how to export specific Indicators for use with an external threat detection system. These guides, available in both web and PDF format, can be found under the ThreatQ Integrations section of the Help Center.

Integrations Management

About Integrations Management

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

Topics in this section include:

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

Integration Types

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

Actions

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

Apps

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

Configuration-Driven Feeds (CDFs)

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

- **Commercial** - Commercial CDFs are provided by paid feed providers as a service. To enable these integrations in ThreatQ, you will need an API ID or API Key from the provider. Commercial CDFs typically provide highly contextual threat intelligence data. You can learn more about available CDFs on the ThreatQ Marketplace.
- **OSINT** - OSINT CDFs are open source threat intelligence feeds. Open source feeds are free to use, but some may require you to register with the feed provider to attain an API Key.

Custom Connectors

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

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

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

Operations

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

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

About My Integrations



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

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

My Integrations

Go To Marketplace
Add New Integration

Type: All
Category: All

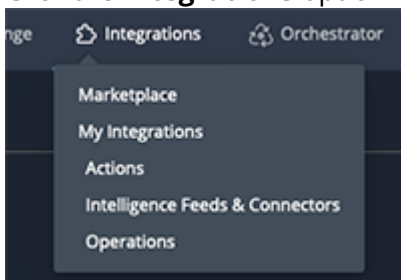
All (14) Enabled (5) Disabled (9)

Clear Search Filters

Domain Tools Operation Version: 2.1.0	Emerging Threats Operation Version: 1.0.1	GreyNoise Action Version: 1.0.0	Greynoise Custom Action Version: 0.0.1
IPInfo Action Version: 1.0.0	MITRE Enterprise ATT&K Feed Category: OSINT Version: 1.0.0 Enabled	MITRE Mobile ATT&K Feed Category: OSINT Version: 1.0.0 Enabled	MITRE PRE-ATT&K Feed Category: OSINT Version: 1.0.0 Enabled
Parkash_Action Custom Action Version: 0.0.1	PhishTank Feed Category: OSINT Version: 2.0.0	Proofpoint ET Block IP Feed Category: OSINT Version: 1.0.0 Enabled	Proofpoint ET Compromised IPs Feed Category: OSINT Version: 1.0.0 Enabled

Accessing My Integrations

1. Navigate to your ThreatQ instance.
2. Click the **Integrations** option in the main navigation and select one of the following options:



MENU OPTION

DETAILS

Marketplace

Opens the ThreatQ Marketplace in a new tab.

My Integrations

Opens the My Integrations page.

Actions

Opens the My Integrations page filtered to only display actions.

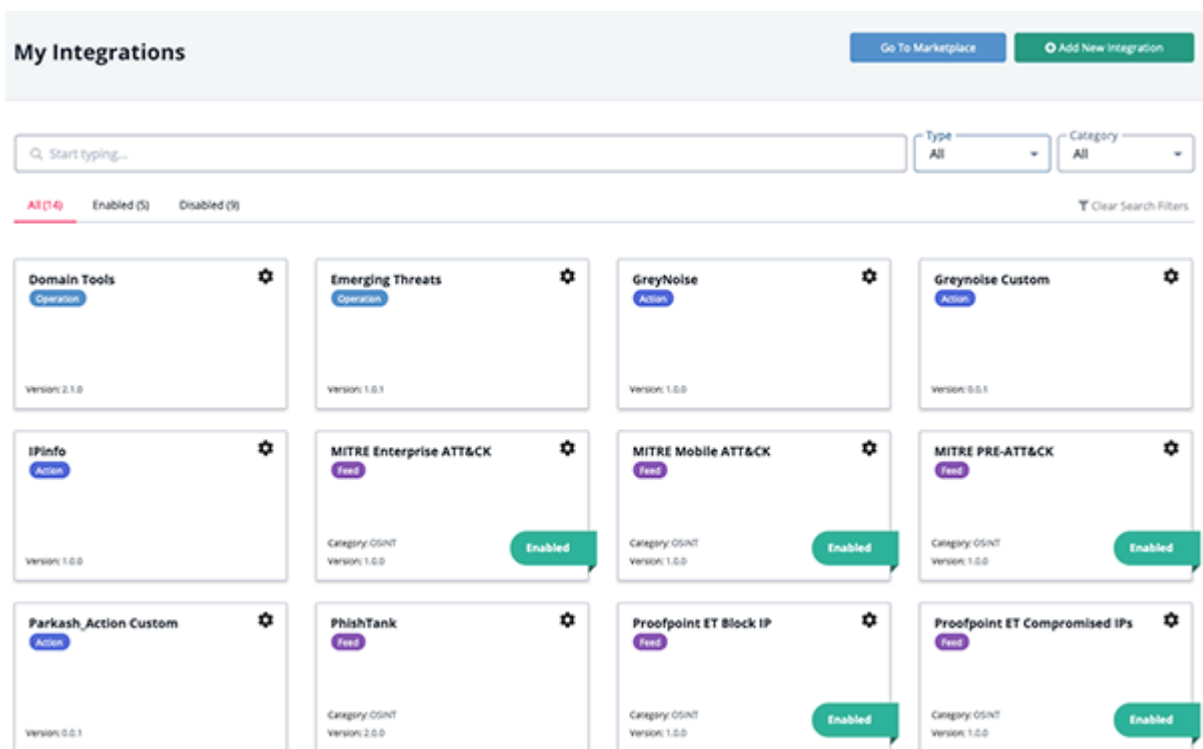
Intelligence Feeds & Connectors

Opens the My Integrations page filtered to only display feeds and connectors.

Operations

Opens the My Integrations page filtered to only display operations.

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



Filtering Your View

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

FILTER

DETAILS

Keyword Filter the integrations list by keyword.

Type Filter the integrations list by integration type. Options include:

- Actions
- Intelligence Feeds and Connectors
- Operations
- All

Category Filter the list by the category of integration:

- **OSINT** - OSINT feeds are open source threat intelligence feeds. Open source feeds are free to use, but some may require you to register with the feed provider to attain an API Key.
- **Commercial** - Commercial feeds are provided by paid feed providers as a service. To enable these feeds in ThreatQ, you will need an API ID or API Key from the provider. Commercial feeds typically provide highly contextual threat intelligence data. You can learn more about these feeds on their vendor's websites.
- **STIX TAXII** - STIX stands for Standard Threat Information Expression, it is an emerging standard for the sharing of machine readable intelligence and incident data. A STIX package is an XML document that can contain many indicators and related context information. For the automated sharing of STIX packages, a protocol called TAXII (Trusted Automated eXchange of Indicator Information) is used to provide a feed to consumers.
- **Labs** - Labs are driven by ThreatQuotient's Threat Intelligence Services Team. Labs feeds provide a solution for data ingestion that is not provided by the feeds pre-configured with the ThreatQ platform. You should inquire with a Threat Intelligence Engineer to see what Labs are available.

Status (All/ Enabled/ Disabled tabs) Filter the list of installed integrations by status: enabled or disabled. A count of integrations appears next to each tab and reflects any filter that is selected.



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

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

Adding an Integration

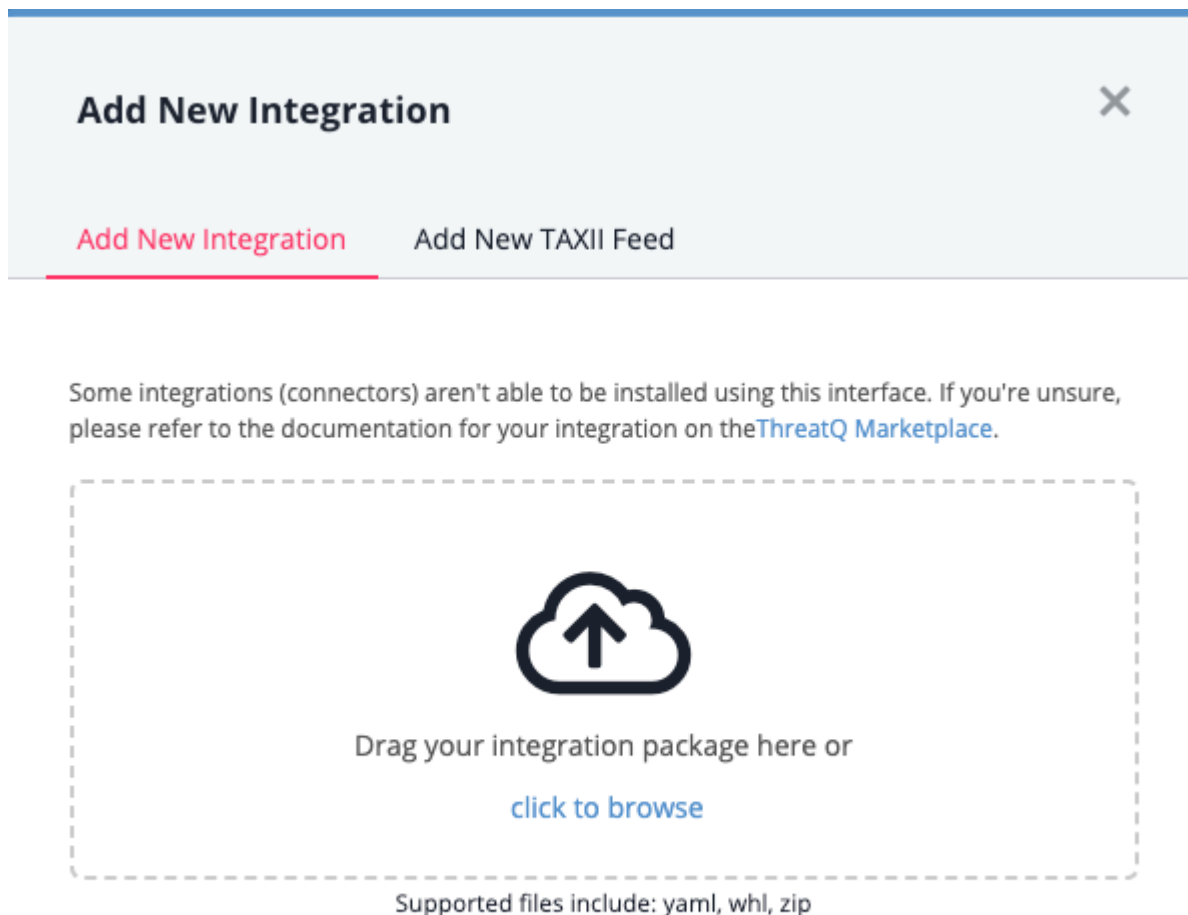


ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integrated-related credentials.

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

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

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

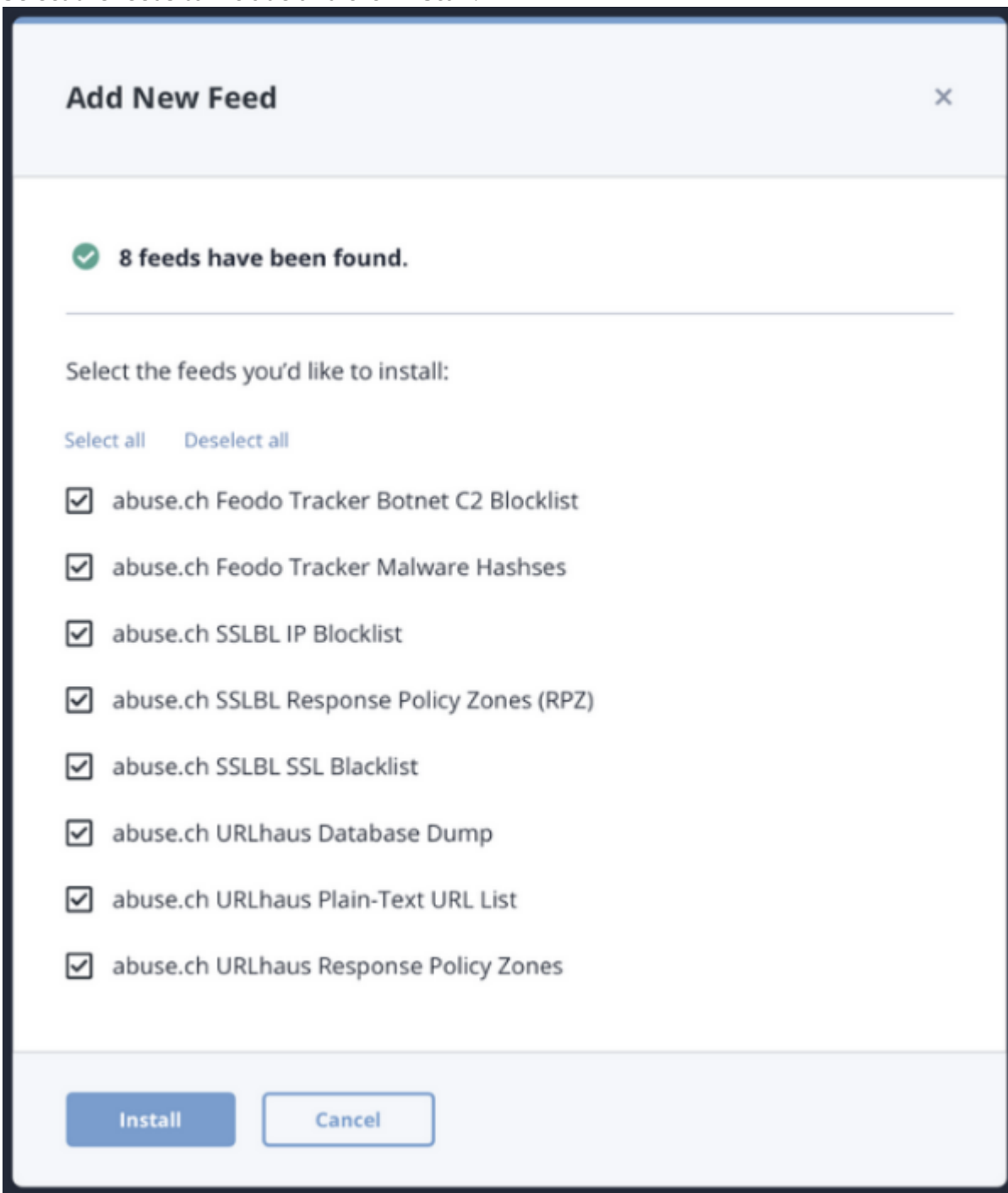


5. Upload the integration file using one of the following methods:
 - Drag and drop the integration file into the dialog box
 - Select the **click to browse** link to locate the integration file on your local machine



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

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



Add New Feed ×

✓ 8 feeds have been found.

Select the feeds you'd like to install:

[Select all](#) [Deselect all](#)

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

Install **Cancel**

7. When the install is complete, you must [configure and enable](#) the integration before it can be used.



Actions will automatically be enabled upon install/upgrade.

Adding A STIX/TAXII Feed

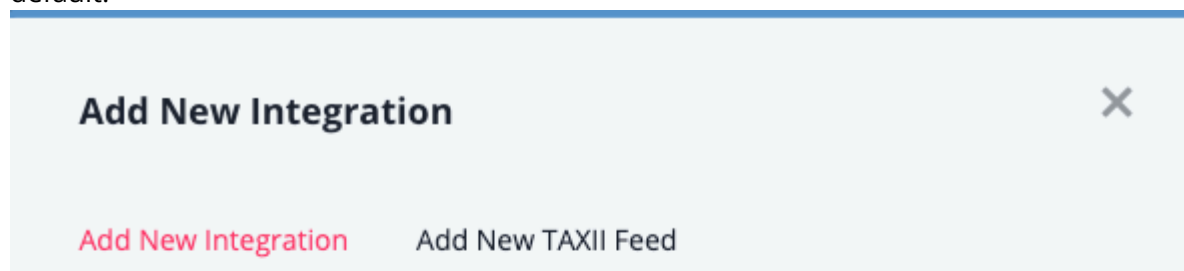


ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integrated-related credentials.

From the [My Integrations](#) page:

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

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



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



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

The Add New TAXII Feed form is displayed.

Add New Integration
Add New TAXII Feed

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 ThreatQuintessence.

Login Credentials (if applicable)

Username

Basic Authentication Username

Password

Basic Authentication Password

Certificates/Keys (if applicable)

Certificate

Client Certificate for authentication with the TAXII Server.

Private Key

Private Key for authentication with the TAXII Server.

☒ **Verify SSL**

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

Host CA Certificate Bundle

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

Add TAXII Feed

Cancel

3. Complete the following fields:

FIELD	INSTRUCTIONS
What would you like to name this feed?	Enter the feed name to be displayed throughout ThreatQ. The name must be at least five characters long. It does not need to match the Collection Name .
How often would you like to pull new data from this feed?	Choose Every Hour or Every Day .
TAXII Connection Settings	
TAXII Server Version	Options include: 1.0, 1.1, 2.0. This field is required.
Discovery URL	This is where the TAXII server can be reached. This field is required.
Poll URL	An optional URL that specifies a specific endpoint on the TAXII Server to poll for data.
Collection Name	The name of the collection of data in the feed you will access. This field is required.
Login Credentials	
Username	If required, enter a username for the feed.
Password	If required, enter a password.
Certificates/Keys	
Certificate	If required, enter a certificate if required for the feed.
Private Key	If required, enter a private key if required for the feed.

FIELD	INSTRUCTIONS
Server Authentication	
Verify SSL	Leave the checkbox checked to require that the TAXII client verify the provider's SSL certificate.
Host CA Certificate Bundle	The provider's CA Certificate used to verify SSL. The Host CA Certificate Bundle will not be honored if the Verify SSL option is not selected.

- Click **Add TAXII** Feed.

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

Configuring an Integration

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

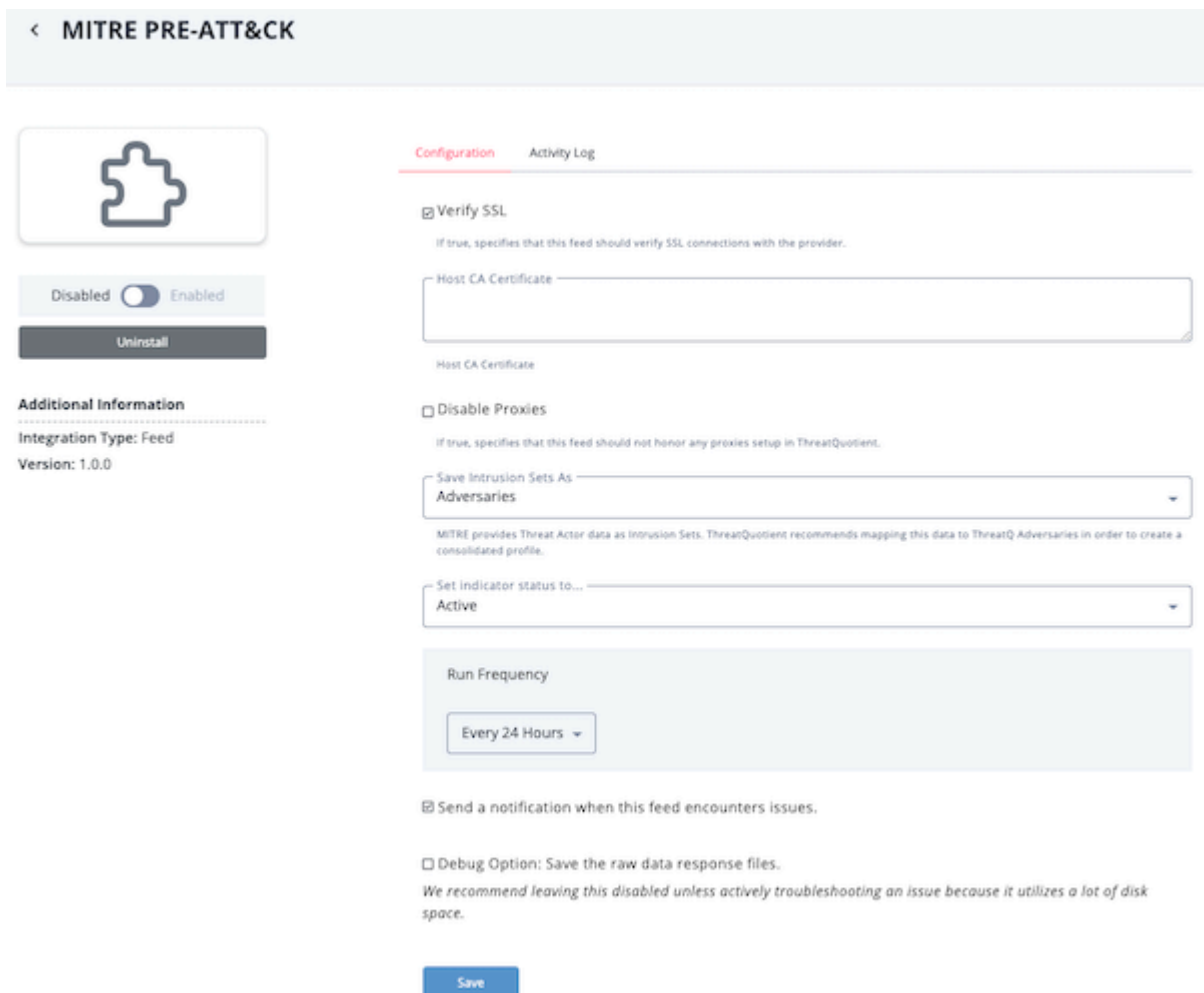


Configuration parameters will differ based on individual integrations. See the individual integration's user guide for configuration and other requirements. Additionally, certain configuration options in the ThreatQ UI will be available for certain types of integrations.

Example: The Run Frequency option will only be accessible for CDFs.

From the [My Integrations](#) page:

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



The screenshot shows the configuration page for the 'MITRE PRE-ATT&CK' integration. The page has a header with a back arrow and the integration name. On the left, there's a puzzle piece icon, a 'Disabled' toggle switch (currently off), and an 'Uninstall' button. Below this is an 'Additional Information' section showing 'Integration Type: Feed' and 'Version: 1.0.0'. The main area has two tabs: 'Configuration' (active) and 'Activity Log'. Under the 'Configuration' tab, there are several settings: 'Verify SSL' (checked), 'Host CA Certificate' (empty text field), 'Disable Proxies' (unchecked), 'Save Intrusion Sets As' (dropdown menu set to 'Adversaries'), 'Set indicator status to...' (dropdown menu set to 'Active'), 'Run Frequency' (dropdown menu set to 'Every 24 Hours'), 'Send a notification when this feed encounters issues.' (checked), and 'Debug Option: Save the raw data response files.' (unchecked). A 'Save' button is at the bottom.

The integration details page displays and lists the following:

- **Integration Information** - details such as the author, required ThreatQ version and targeted object types.
- **Configuration Tab** - Integration-specific configuration parameters for the integration.

- **Activity Log tab** - Display run information such as time stamps, data ingested, and any error messages. The Activity Log on this page only applies to CDFs.
- 2. Enter the required configuration parameters for your integration in the Configuration Tab. These configuration parameters will differ based on the integration. See the individual integration's user guide for more information.



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

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

Periodic Options

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

Schedule Options

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

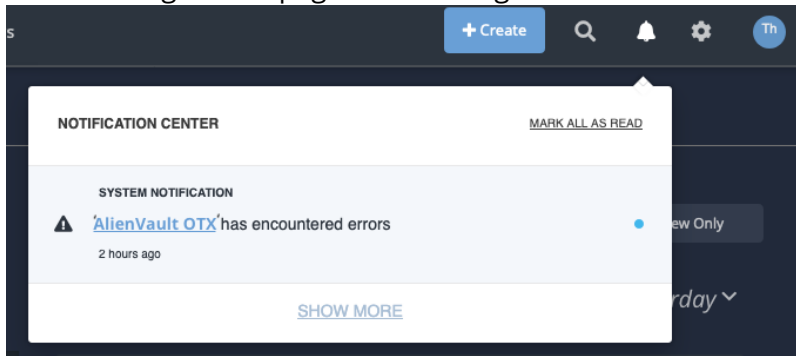
- 4. Select a default **Status** if the integration ingests indicator or signature types.



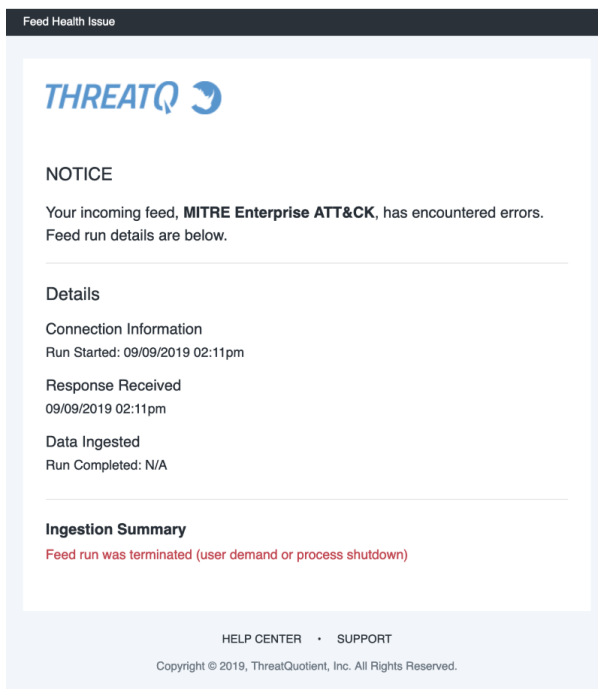
This configuration option will only be available if the integration ingests indicator or signature types.

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

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



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



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

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

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



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

Triggering a Manual Run

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



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

From the [My Integrations](#) page:

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

< MITRE PRE-ATT&CK



Disabled ☒ Enabled

Run Integration

Uninstall

Configuration

Activity Log

Activity Log Details

Scheduled Run

11/02/2020 10:00pm

Additional Information

Integration Type: Feed

Version: 1.0.0



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

2. Confirm that the integration is enabled.
3. Click the **Run Integration** button located beneath Enable/Disable toggle switch.

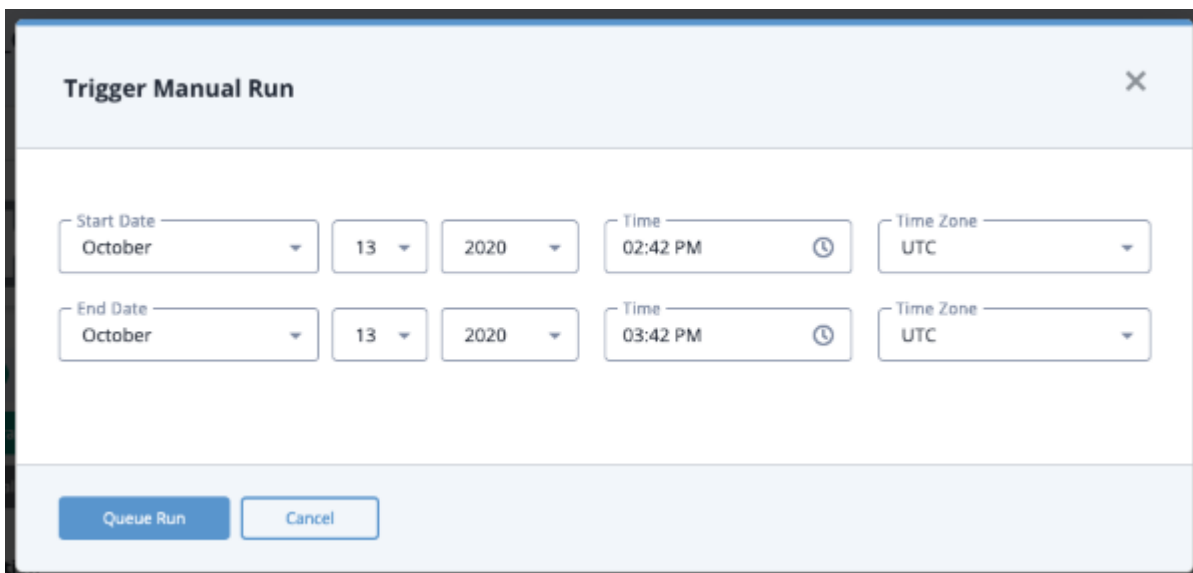


If the **Run Integration** button is not visible, the integration does not support manual runs.

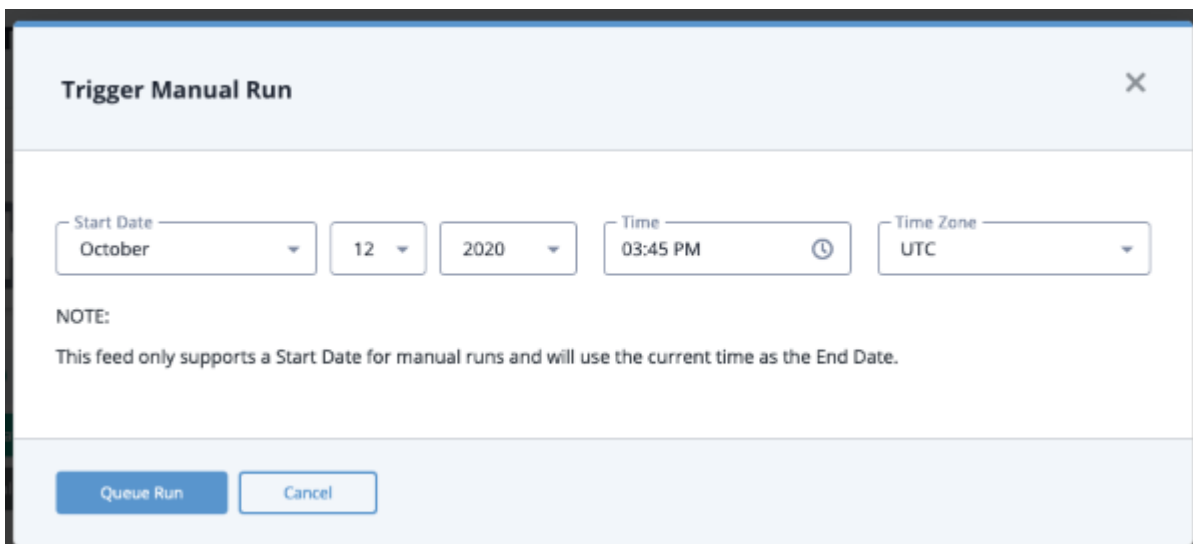
The Trigger Manual Run window will be displayed.



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




Some feeds only support a Start Date.



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

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

Emerging Threats

ThreatQ

Disabled

Enabled

Uninstall

Additional Information

Integration Type: Operation

Author: ThreatQ

Description: Enrichment data from Emerging Threats IQRisk

Version: 1.0.1

Works With:

- Indicator
 - FQDN
 - IP Address
 - MDS

Configuration

Apl Key

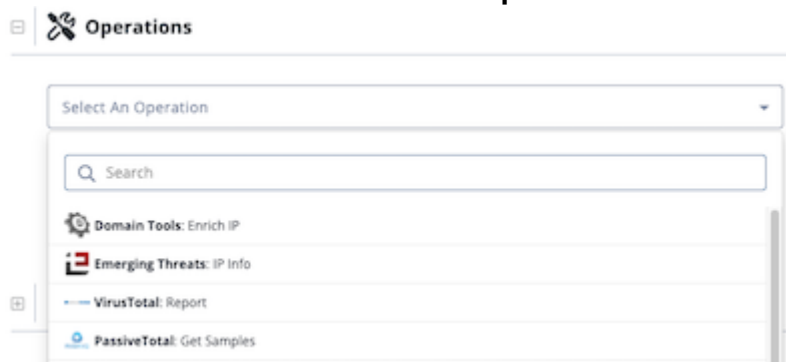
☐ Bypass system proxy configuration for this operation

Save

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



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



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



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

Activity Logs (feeds)

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

Configuration		Activity Log
Activity Log Details 		
Scheduled Run 10/05/2020 05:13pm	 Completed	▶
Scheduled Run 10/04/2020 05:13pm	 Completed	▶
Scheduled Run 10/03/2020 05:13pm	 Completed	▶
Scheduled Run 10/02/2020 05:13pm	 Completed	▶
Scheduled Run	 Completed with errors	▶

The Log Details section displays run details that include:

LOG DATA

DETAILS

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

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

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 a CDF's Activity Log

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

ThreatQ User Guide
Version 5.20.0

189

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

Configuration		Activity Log
Activity Log Details		
Scheduled Run	10/05/2020 05:13pm	 Completed 
Scheduled Run	10/04/2020 05:13pm	 Completed 
Scheduled Run	10/03/2020 05:13pm	 Completed 
Scheduled Run	10/02/2020 05:13pm	 Completed 
Scheduled Run		 Completed with errors 

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

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		

Removing an Integration

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



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

Removing an Integration

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

From the [My Integrations](#) page:

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

< MITRE PRE-ATT&CK



Disabled
Enabled

Uninstall

Additional Information

Integration Type: Feed
Version: 1.0.0

Configuration
Activity Log

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

Host CA Certificate

Host CA Certificate

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

Save Intrusion Sets As Adversaries

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

Set indicator status to...
Active

Run Frequency

Every 24 Hours

☒ Send a notification when this feed encounters issues.

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

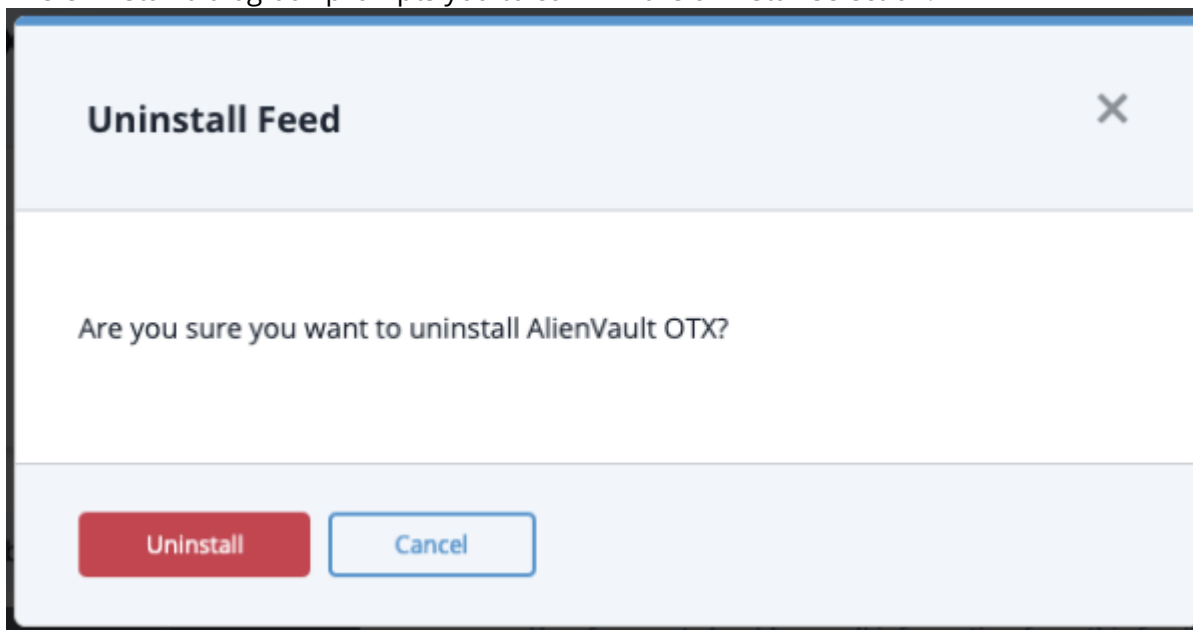
Save



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

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

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



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

Disabling an Integration

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

From the [My Integrations](#) page:

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

MITRE PRE-ATT&CK

Disabled

Enabled

Uninstall

Additional Information

Integration Type: Feed

Version: 1.0.0

Configuration

Activity Log

Verify SSL

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

Host CA Certificate

Host CA Certificate

Disable Proxies

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

Save Intrusion Sets As

Adversaries

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

Set indicator status to...

Active

Run Frequency

Every 24 Hours

Send a notification when this feed encounters issues.

Debug Option: Save the raw data response files.

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

Save

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

Job Management



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

The Job Management page allows you to view the status and outcome of Bulk Actions, Data Retention Policies, and consume-generated attribute deletions. See the [Bulk Actions](#) and [Data Retention Policy](#) sections for more details.

A process runs each day at 2 AM to archive user-initiated jobs 90 days after their creation date and system-initiated jobs 365 days after their creation date. The archived jobs no longer display in the Job Management page but are stored in a historical partition that can be queried.

Tips and Tricks

- Click the refresh icon in the upper right corner to refresh the job information displayed.
- Click a row to expand/collapse job details. The expanded/detailed view varies by job type:

JOB TYPE	DETAILED VIEW INCLUDES...
Delete	• Object Type • Search Criteria • Activity - Lists Start Time and Completed or Failed At timestamps • Error Message
Update	• Object Type • Search Criteria
Relationship	• Update - Attribute names displayed in this field are truncated after fifty characters. • Activity - Lists Start Time and Completed or Failed At timestamps • Error Message
Retention Policy	• Data Collection - Lists the name of the Data Collection assigned to your Data Retention Policy. • Total Objects by Type - Lists the number of system objects deleted by object type. • Activity - Lists Start Time and Completed or Failed At timestamps
System Delete	N/A

- Bulk action jobs applied to a selected subset of objects list the following message in the Search Criteria field: **No search data to display.**

Accessing the Job Management page:

1. Navigate to Settings  > Job Management.

By default, the All tab is displayed. This tab lists all bulk action jobs. Click the tab corresponding to the job type you want to access.

Job Management 						
All	Delete	Update	Relationship	Retention Policy	System Delete	
JOB ID	JOB TYPE	AUTHOR	DATE CREATED	TOTAL OBJECTS	STATUS	PERCENT COMPLETED
2424	Relationship	threatq@threatq.com	08/04/2023 1:48pm	1	Completed	100% 1 of 1
2308	Delete	threatq@threatq.com	08/04/2023 1:39pm	1	Completed	100% 1 of 1
2183	Update	threatq@threatq.com	08/04/2023 1:30pm	1	Completed	100% 1 of 1

The Job Management page allows you to view the following details about Bulk Action, Data Retention, and System Delete jobs:

FIELD

DESCRIPTION

Job ID The unique ID assigned to the job.

Job Type The job type of the Bulk Action such as Delete, Update, or Relationship. Data Retention Policy jobs list a job type of Retention Policy. Attribute deletions initiated by an integration update list a job type of System.

Author The user or integration that initiated the job.

Date Created The timestamp the job was created and queued.

Total Objects The total number of system objects included in the job.

Status The current status of the job including:

- **Created** - The job has been queued.
- **In Queue** - The job is running.
- **Error** - The job failed.

FIELD	DESCRIPTION
	• Waiting - The job is waiting for indexing to be complete. This only applies to the Bulk Change process. • Completed - The job has completed.
Percent Completed	The Percent Completed column displays three indications of the job's progress: • A progress bar with the overall percentage completed. • A count of the number of objects that have been processed from the total number of objects (e.g., 300 of 3,400). • The estimated time remaining.  If a data retention policy does not find any objects that match its parameters and as a result did not delete any objects, its job details display a Percent Completed value of 100% and 0 of 0 objects.  If a data retention policy does not delete any objects due to an error, its job details display a Percent Completed value of 0% and 0 of X objects.

Licensing

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

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



ThreatQ licenses are not perpetual.

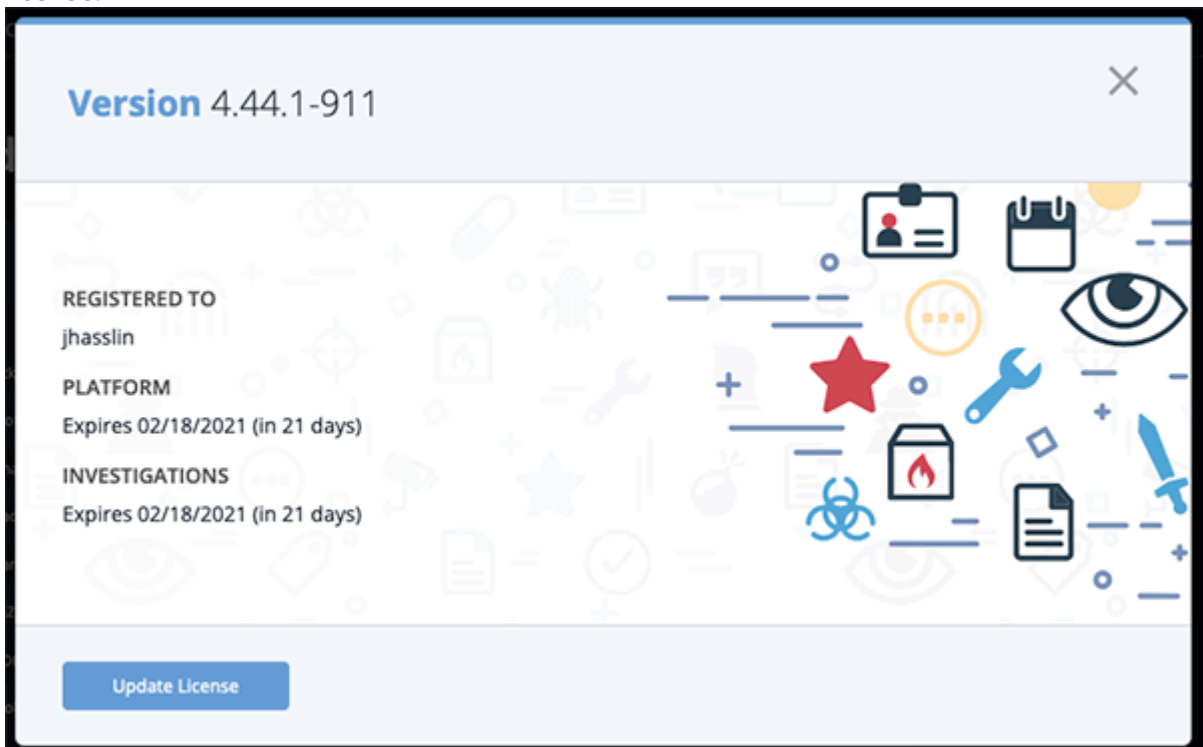
Managing Your ThreatQ License

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

Viewing License Status

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

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



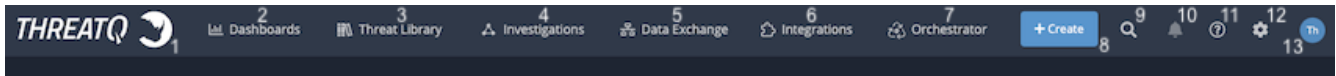
Updating a License

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

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

Navigation Menu

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



#	NAME	DESCRIPTION	REFERENCES
1	ThreatQ Icon	Clicking on the ThreatQ icon will navigate you back to the home page and dashboard.	N/A
2	Dashboards	The Dashboards link in the top navigation bar allows you to access a drop-down list of your dashboards.	About Dashboards
3	Threat Library	Access and search the Threat Library and view system object details.	About Threat Library About Building Searches with Filter Sets About Object Details Bulk Actions About Data Controls
4	Investigations	Navigates to ThreatQ Investigations (TQI) , a cybersecurity situation room that enables collaborative threat analysis, investigation, and coordinated response.	About ThreatQ Investigations
5	Data Exchange	Allows the bi-directional sharing of threat intelligence across multiple ThreatQ instances.	ThreatQ Data Exchange

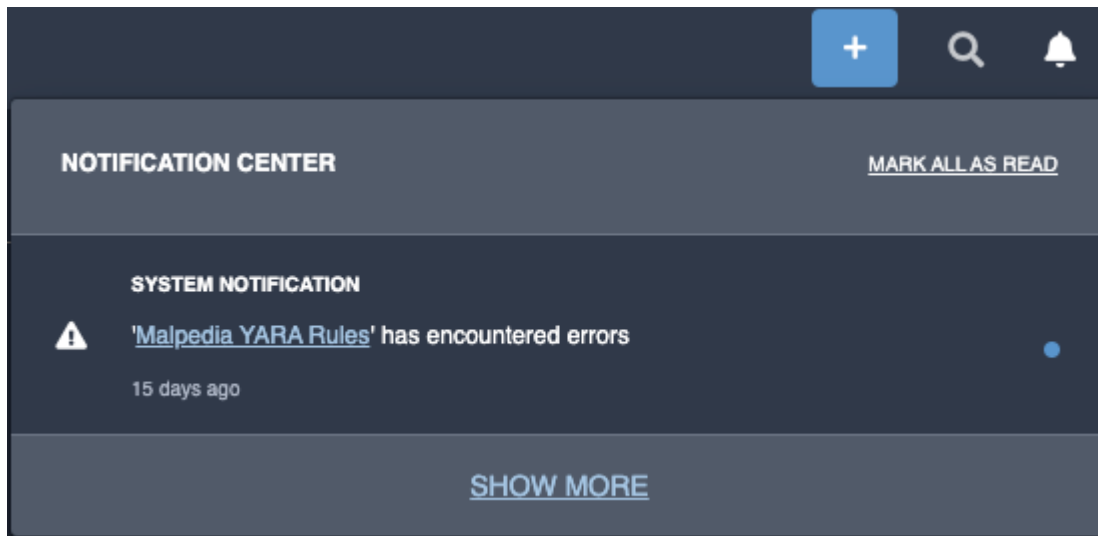
#	NAME	DESCRIPTION	REFERENCES
6	Integrations	Allows you to access the Marketplace as well as you integrations.	• About Integrations Management
7	Orchestrator	Opens the ThreatQuotient TDR Orchestrator (TQO) which includes enhanced automation, analysis and reporting capabilities that accelerate threat detection and response across disparate systems.	• About TQO
8	Create Button	Create system objects.	1. Adversaries 2. Events 3. Files 4. About Indicators 5. Signatures 6. About STIX
9	Search Icon	Perform a basic search for a system object.	• About Building Searches with Filter Sets
10	Message Center Icon	Receive in-app notifications of system job processes such as Bulk Actions . Administrator and Maintenance account users will also receive feed health notifications.	• Notification Center
11	Help Icon	Click the Help icon to quickly access the Help Center, Product Updates, Getting Started Guides, and Video Demos. The search field at the top of the menu also gives you the option to search the Help Center.	• Product Updates • Installation • Videos

#	NAME	DESCRIPTION	REFERENCES
12	Site Settings	Allows you to manage your ThreatQ application settings as well as view your version and licenses.	• About Exports • Job Management • About Object Management • Reports • Server Administration • About System Configuration • About User Management • Licensing
13	User Icon	Access your user profile.	1. About User Management

Notifications

About Notifications

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



In-app notifications include:

- [Bulk Actions](#) updates
- [Data Retention Policy](#) notifications
- Feed health alerts
- Task assignment notifications
- [Sharing notifications](#)



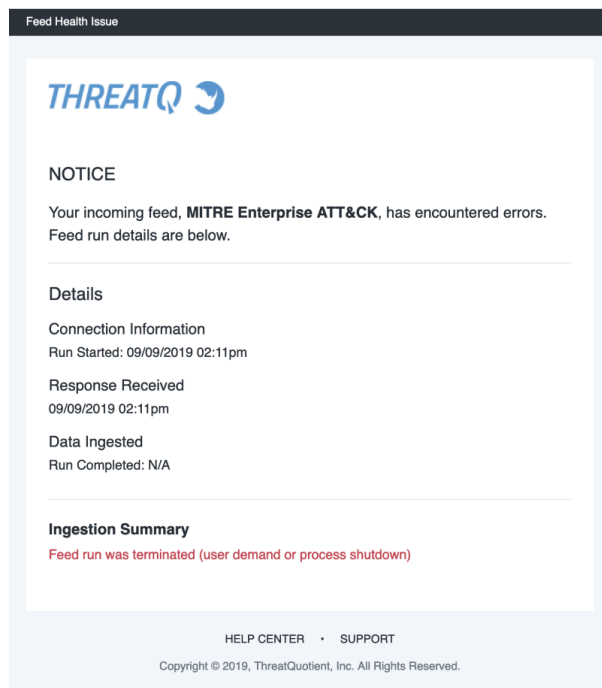
Only users with Administrator and Maintenance roles receive in-app feed health alerts via the Notification Center.

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

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



Configuring Mail Server

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

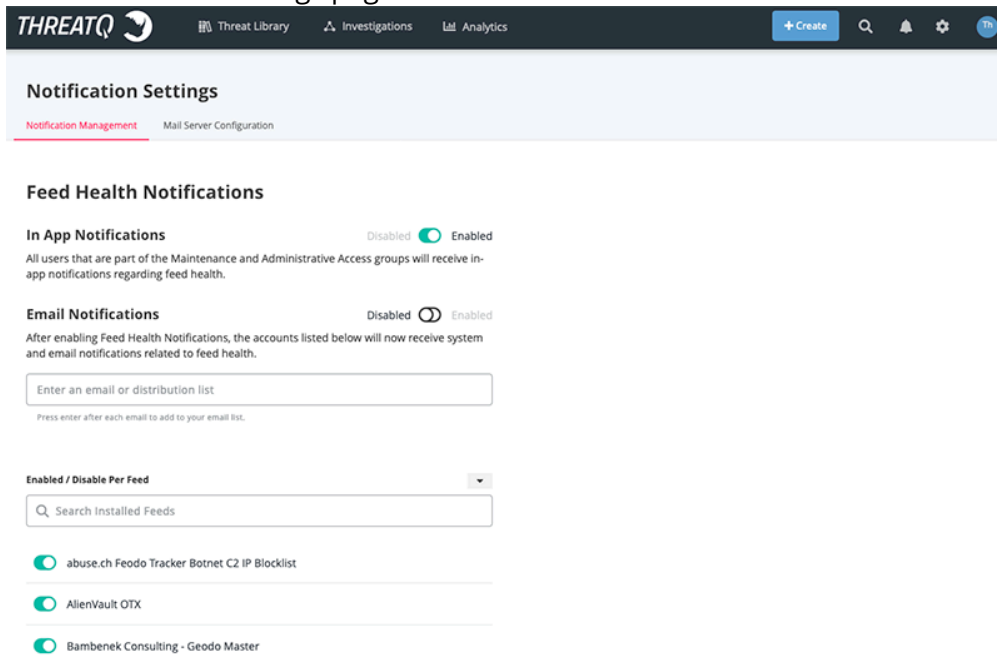


In the event that you have completed the mail server configuration and are still not receiving emails, your email provider may have marked the activity as suspicious. Some services, such as Gmail, will require you to confirm the activity, via an email message, before allowing the ThreatQ application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

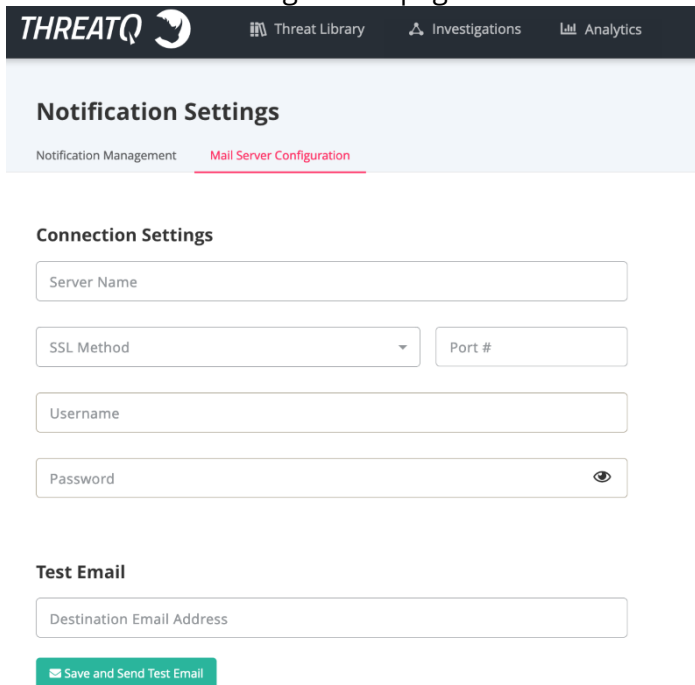
1. Click on the **System Settings**  and select the **Notification Settings** option.

The Notification Settings page loads.



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

The Mail Server Configuration page loads.

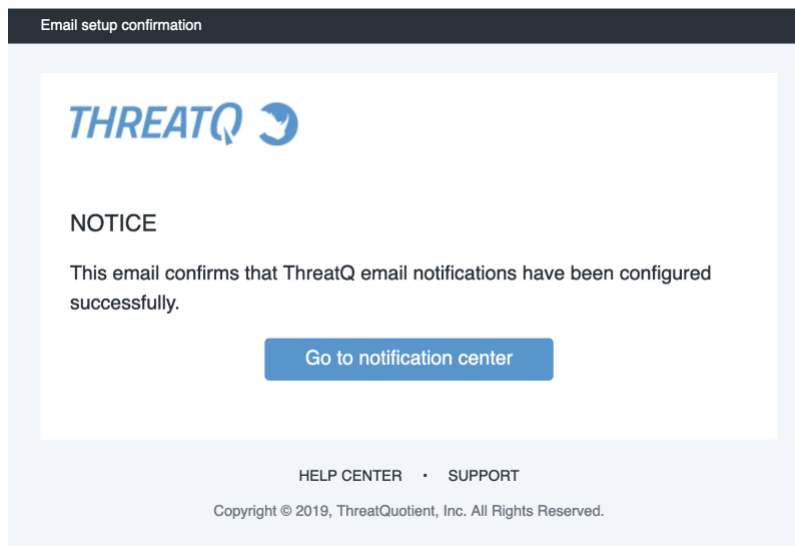


- Complete the following fields:

FIELD	DESCRIPTION
Server Name	The address of your mail server.

FIELD	DESCRIPTION
SSL Method	The SSL method used. There are three options: ○ SSL ○ TLS ○ None
Port #	The mail server port.
User name	The mail server account username.
Password	The mail server account password.

4. Enter an email in the **Test Email** field and click **Save and Send Test Email** to confirm that the settings are correct - this is optional. You will receive a setup confirmation email.



5. If you did not use the **Save and Send Test Email** option, click on **Save Changes** to save your settings.

Enabling Feed Health Notifications

There are two different types of Feed Health Notifications that can be enabled on this page: In-App and Email. While you can enter the email address for a user to receive Email Notifications, only users with administrator and maintenance roles will receive In-App Notifications.

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

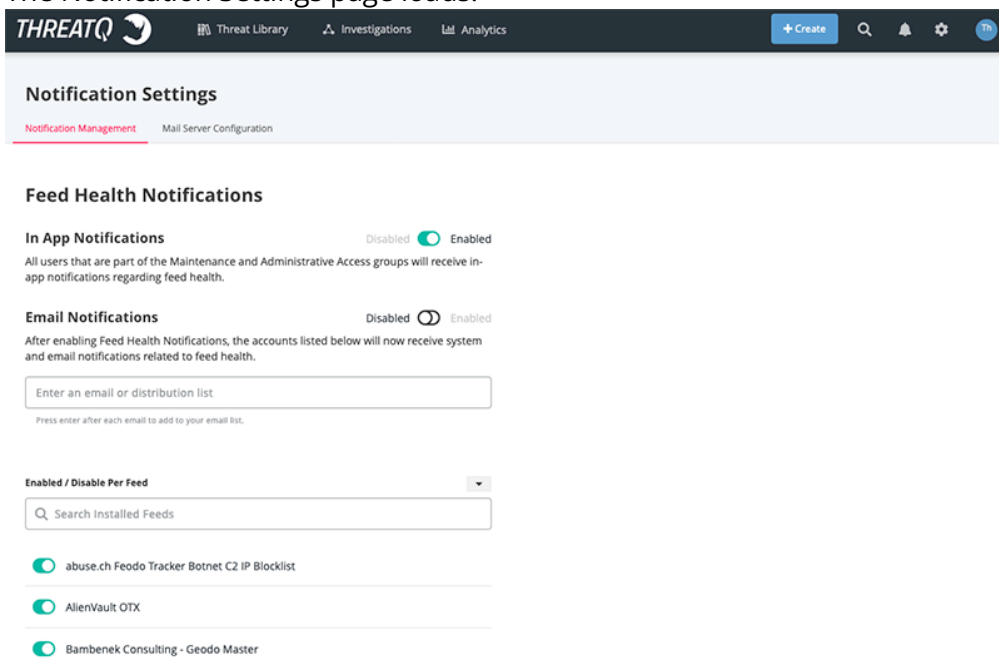


In the event that you have completed the mail server configuration and are still not receiving emails, your email provider may have marked the activity as suspicious. Some services, such as Gmail, will require you to confirm the activity, via an email message, before allowing the ThreatQ application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

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

The Notification Settings page loads.



2. Perform the following steps to enable email and in-app notifications:
 - *Enable In-App Feed Health Notifications*
 1. Click on the **Enable** toggle switch for **In App Notifications**.
 - *Enable Feed Health Email Notifications*

1. 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

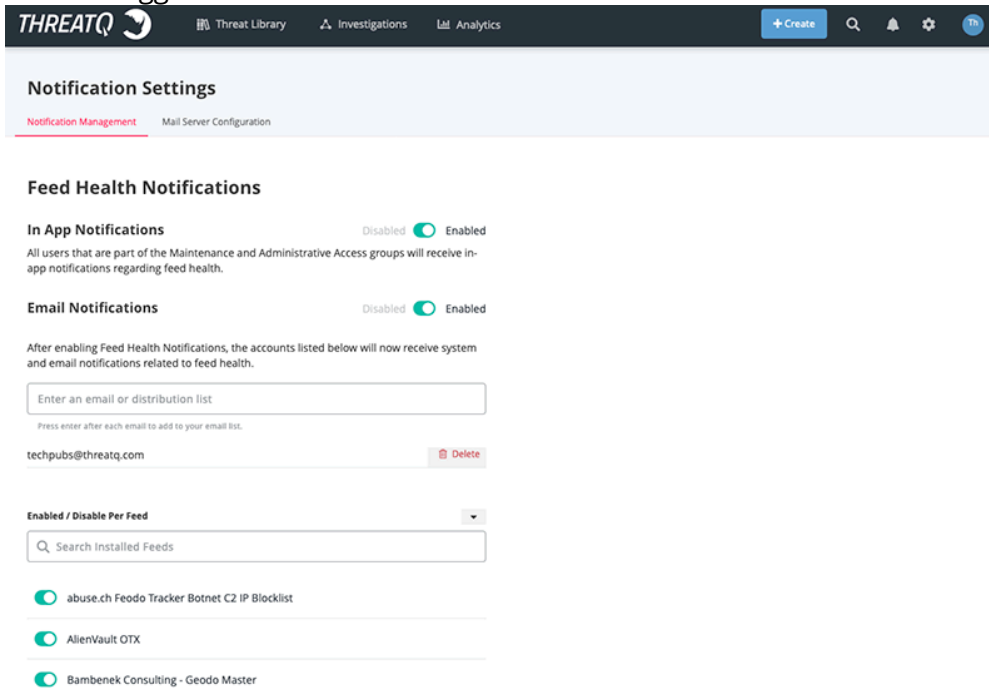
After enabling Feed Health Notifications, the accounts listed below will now receive system and email notifications related to feed health.

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

techpubs@threatq.com

Delete

2. 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.

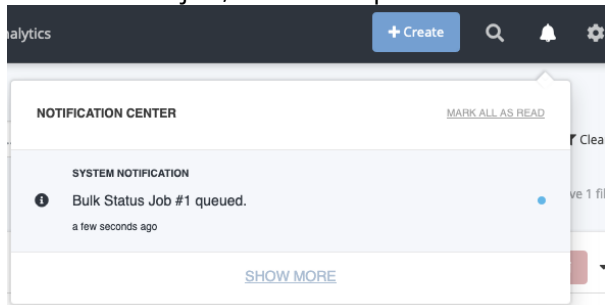



You can also enable/disable individual CDF feed notifications by clicking on the feed under [Integrations](#) and checking/unchecking the notifications checkbox.

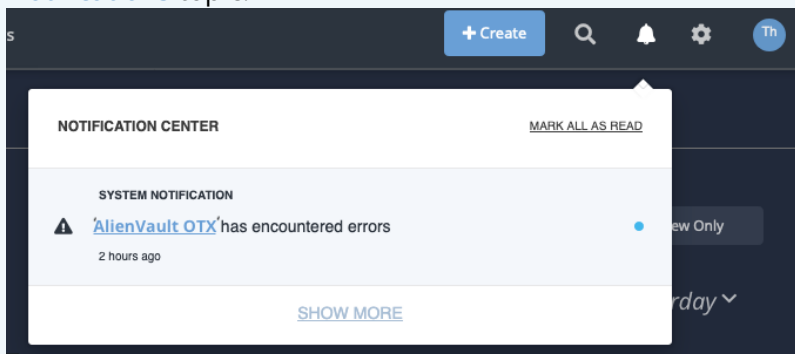
Notification Center

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

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



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.



Sharing Notifications

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

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

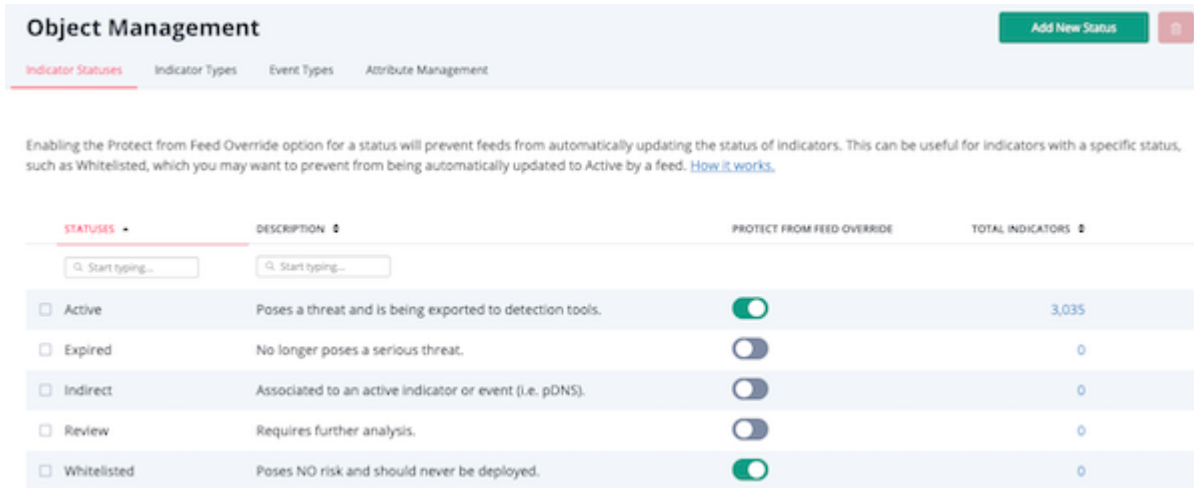
SCENARIO	VIEWER	EDITOR	OWNER
A user shares a data collection, dashboard, or investigation with you.	You have been added as a Viewer to <Name>	You have been added as an Editor to <Name>	N/A
A user changes your permissions to editor or viewer.			
A user changes your permissions to owner.	You have been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

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

Object Management

About Object Management

The Object Management page consists of four tabs, Indicator Statuses, Indicator Types, Event Types, and Attribute Management.



STATUSES	DESCRIPTION	PROTECT FROM FEED OVERRIDE	TOTAL INDICATORS
☐ Active	Poses a threat and is being exported to detection tools.	☒	3,035
☐ Expired	No longer poses a serious threat.	☐	0
☐ Indirect	Associated to an active indicator or event (i.e. pDNS).	☐	0
☐ Review	Requires further analysis.	☐	0
☐ Whitelisted	Poses NO risk and should never be deployed.	☒	0

These tabs allow Maintenance and Admin users to work with:

SECTION

DETAILS

[Indicator Statuses](#) Create and edit custom indicator statuses.

[Indicator Types](#) View your platform's indicator types.

[Event Types](#) Create and edit custom event types.

[Attributes](#) Update attribute keys and values associated with system objects.

Indicator Statuses Management

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

Indicator Status Assignment

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

Indirect Indicator Status

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

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

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

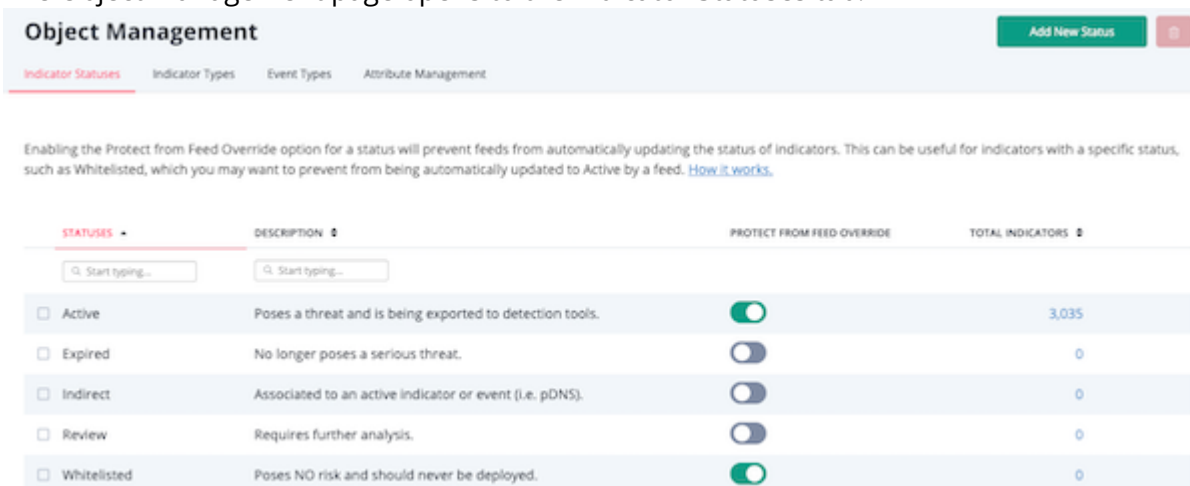
Protected Indicator Statuses

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

Viewing Indicator Statuses

1. Navigate to Settings  > Object Management.

The Object Management page opens to the Indicator Statuses tab.



STATUSES	DESCRIPTION	PROTECT FROM FEED OVERRIDE	TOTAL INDICATORS
☐ Active	Poses a threat and is being exported to detection tools.	☒	3,035
☐ Expired	No longer poses a serious threat.	☐	0
☐ Indirect	Associated to an active indicator or event (i.e. pDNS).	☐	0
☐ Review	Requires further analysis.	☐	0
☐ Whitelisted	Poses NO risk and should never be deployed.	☒	0



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

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

Indicator Statuses Table Functions:

FUNCTION

DESCRIPTION

Status Filter

Enter a keyword in the text field to filter the table by status name. You can click on the Statuses header to sort the table by alphabetical order.

Description Filter

Enter a keyword in the text field to filter the table by status description. You can click on the Description header to sort the table by alphabetical order.

Protect from Feed Override

Clicking on the toggle switch in this column will enable/disable the Protect from Feed Override option for that status. See the [Suppressing Indicator Status Updates](#) section below for more details on this feature.

Total Indicators

The number of indicators currently using the status. Clicking on the value will open the Threat Library filtered to that status. Clicking on the Total Indicators heading will sort the table in ascending/descending order.

Suppressing Indicator Status Updates

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

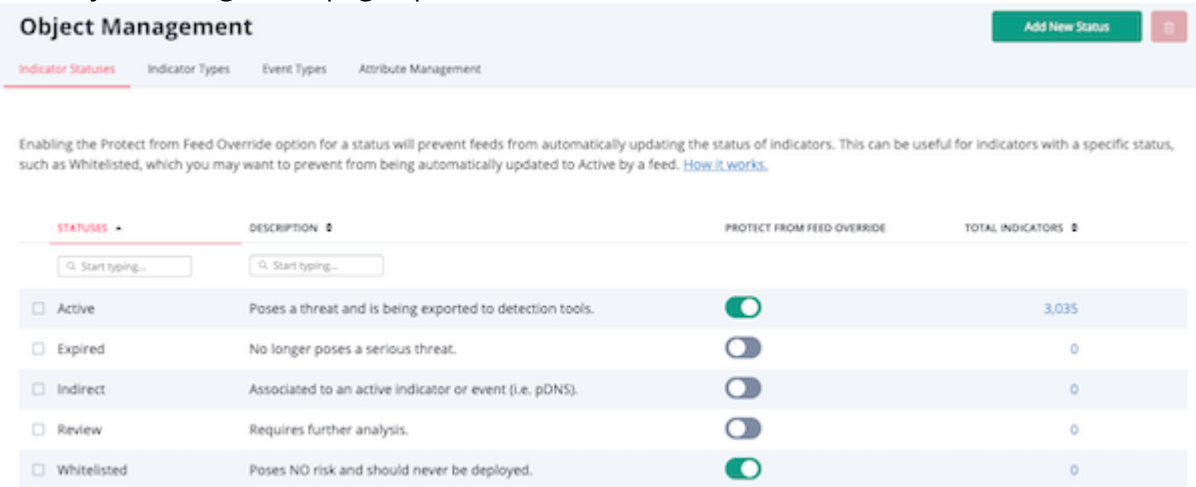


Use Case: You have a well-vetted set of whitelisted indicators that you do not want to update without internal review and discussion. To protect these indicators from automatic status updates from feeds, toggle the **Protect from Feed Override** switch for the **Whitelisted** status to green (active).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

1. Navigate to Settings  > Object Management.
The Object Management page opens to the Indicator Statuses tab.
2. In the Protect From Feed Override column, click the toggle switch corresponding to the status to change it from grey (status updates allowed) to green (status updates suppressed).

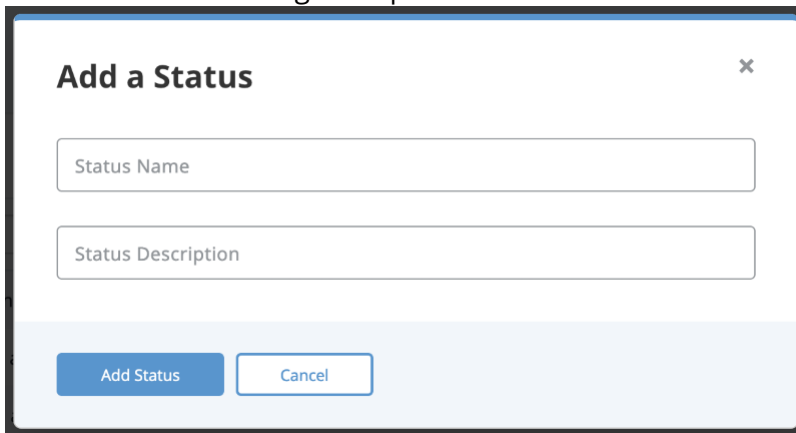
Adding an Indicator Status

1. Navigate to Settings  > Object Management.
The Object Management page opens to the Indicator Statuses tab.



STATUSES	DESCRIPTION	PROTECT FROM FEED OVERRIDE	TOTAL INDICATORS
☐ Active	Poses a threat and is being exported to detection tools.		3,035
☐ Expired	No longer poses a serious threat.		0
☐ Indirect	Associated to an active indicator or event (i.e. pDNS).		0
☐ Review	Requires further analysis.		0
☐ Whitelisted	Poses NO risk and should never be deployed.		0

2. Click **Add New Status**.
The Add a Status dialog box opens.



Add a Status

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

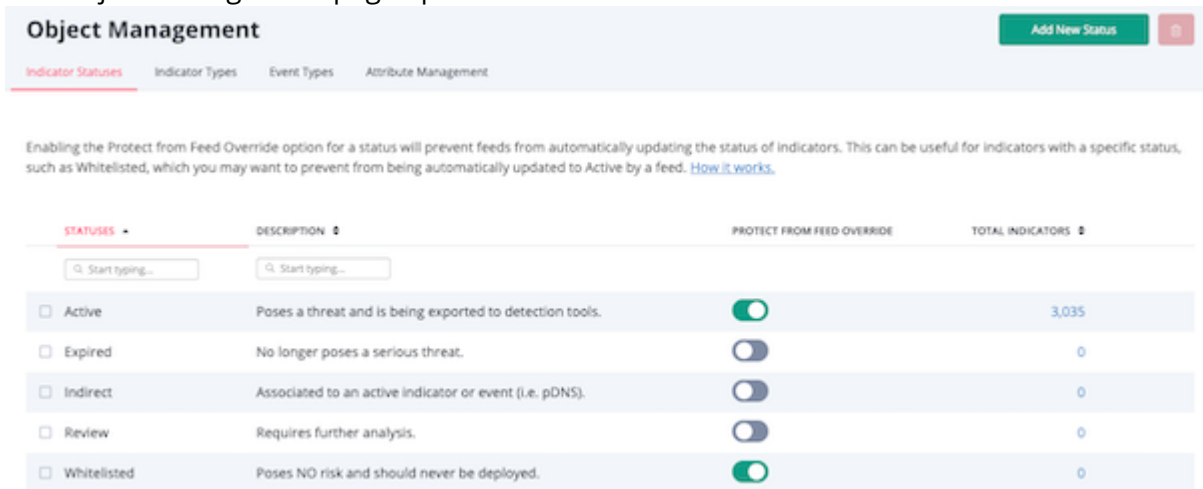
- Click **Add Status**.

Editing an Indicator Status

 You cannot edit an indicator status provided by ThreatQ.

- Navigate to Settings  > Object Management.

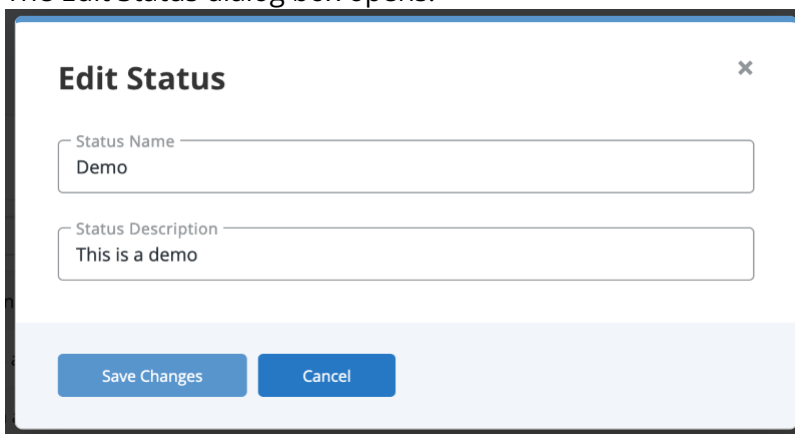
The Object Management page opens to the Indicator Statuses tab.



STATUSES	DESCRIPTION	PROTECT FROM FEED OVERRIDE	TOTAL INDICATORS
Start typing...	Start typing...		
☐ Active	Poses a threat and is being exported to detection tools.	☒	3,035
☐ Expired	No longer poses a serious threat.	☐	0
☐ Indirect	Associated to an active indicator or event (i.e. pDNS).	☐	0
☐ Review	Requires further analysis.	☐	0
☐ Whitelisted	Poses NO risk and should never be deployed.	☒	0

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

The Edit Status dialog box opens.



Edit Status

Status Name: Demo

Status Description: This is a demo

Save Changes Cancel

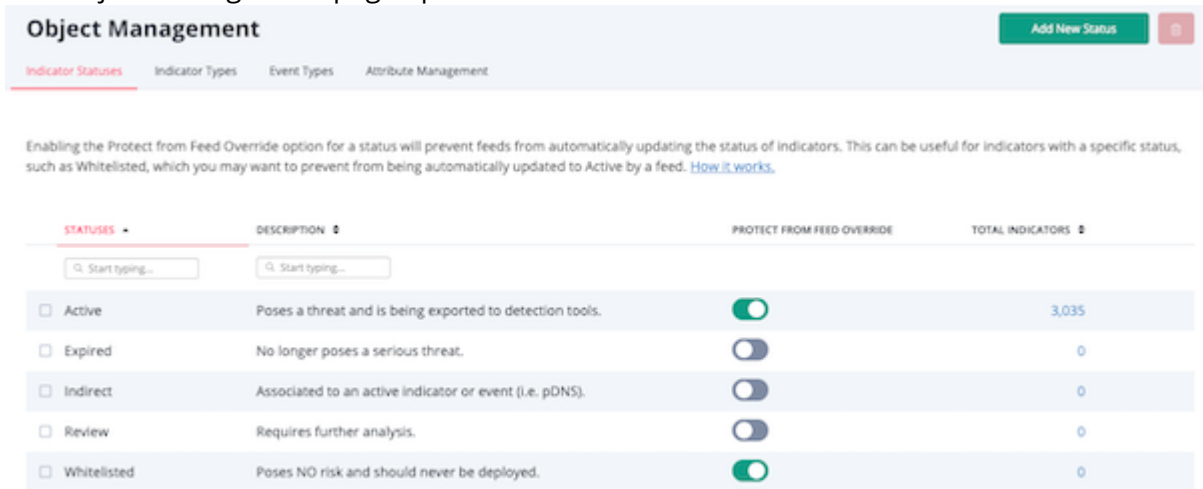
- Optionally, enter a new **Status Name**.
- Optionally, enter a new **Status Description**.
- Click **Save Changes**.

Deleting an Indicator Status

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

1. Navigate to Settings  > Object Management.

The Object Management page opens to the Indicator Statuses tab.



Object Management Add New Status

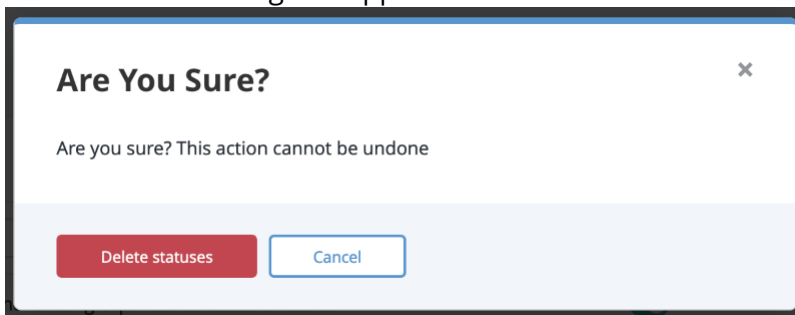
Indicator Statuses | Indicator Types | Event Types | Attribute Management

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

STATUSES	DESCRIPTION	PROTECT FROM FEED OVERRIDE	TOTAL INDICATORS
☐ Active	Poses a threat and is being exported to detection tools.	☒	3,035
☐ Expired	No longer poses a serious threat.	☐	0
☐ Indirect	Associated to an active indicator or event (i.e. pDNS).	☐	0
☐ Review	Requires further analysis.	☐	0
☐ Whitelisted	Poses NO risk and should never be deployed.	☒	0

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

A confirmation dialog box appears.



Are You Sure? ×

Are you sure? This action cannot be undone

Delete statuses Cancel

4. Click **Delete Statuses**.

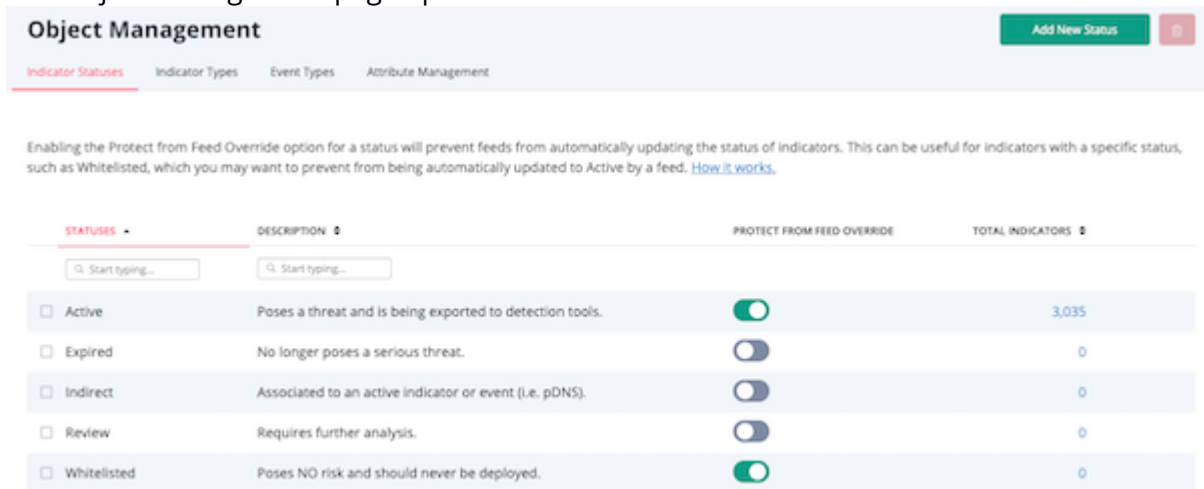
Indicator Types

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

To view Indicator Types found within ThreatQ:

1. Navigate to Settings  > Object Management.

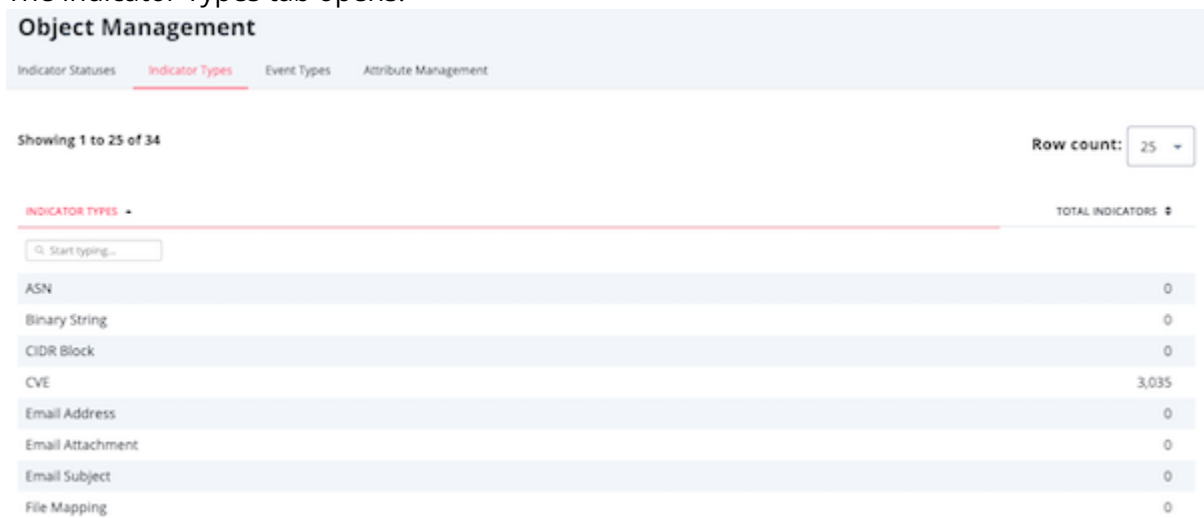
The Object Management page opens.



STATUSES	DESCRIPTION	PROTECT FROM FEED OVERRIDE	TOTAL INDICATORS
☐ Active	Poses a threat and is being exported to detection tools.	☒	3,035
☐ Expired	No longer poses a serious threat.	☐	0
☐ Indirect	Associated to an active indicator or event (i.e. pDNS).	☐	0
☐ Review	Requires further analysis.	☐	0
☐ Whitelisted	Poses NO risk and should never be deployed.	☒	0

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

The Indicator Types tab opens.



INDICATOR TYPES	TOTAL INDICATORS
ASN	0
Binary String	0
CIDR Block	0
CVE	3,035
Email Address	0
Email Attachment	0
Email Subject	0
File Mapping	0

Indicator Types Table Functions:

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

Event Types

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

Object Management

Add New Event Type

Indicator StatusesIndicator TypesEvent TypesAttribute Management

Showing 1 to 14 of 14Row count: 25

EVENT TYPES	TOTAL EVENTS	TOTAL INDICATORS
Q. Start typing...		
☐ Anonymization	1	0
☐ Command and Control	0	0
☐ Compromised PKI Certificate	0	0
☐ DoS Attack	0	0
☐ Exfiltration	2	0
☐ Host Characteristics	0	0
☐ Incident	2	0
☐ Login Compromise	0	0
☐ Malware	1	0
☐ Sighting	3	0
☐ Spearphish	0	0
☐ SQL Injection Attack	0	0
☐ Watchlist	1	0
☐ Watering Hole	2	0

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

System provided Event Types include:

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

Viewing Event Types

1. Navigate to Settings  > Object Management.

The Object Management page opens.

Object Management

Add New Status

Indicator Statuses
Indicator Types
Event Types
Attribute Management

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

STATUSES	DESCRIPTION	PROTECT FROM FEED OVERRIDE	TOTAL INDICATORS
Start typing...	Start typing...		
☐ Active	Poses a threat and is being exported to detection tools.	☒	3,035
☐ Expired	No longer poses a serious threat.	☐	0
☐ Indirect	Associated to an active indicator or event (i.e. pDNS).	☐	0
☐ Review	Requires further analysis.	☐	0
☐ Whitelisted	Poses NO risk and should never be deployed.	☒	0

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

The Event Types tab opens.

Object Management

Add New Event Type

Indicator Statuses
Indicator Types
Event Types
Attribute Management

Showing 1 to 14 of 14

Row count: 25

EVENT TYPES	TOTAL EVENTS	TOTAL INDICATORS
Start typing...		
☐ Anonymization	1	0
☐ Command and Control	0	0
☐ Compromised PKI Certificate	0	0
☐ DoS Attack	0	0
☐ Exfiltration	2	0
☐ Host Characteristics	0	0
☐ Incident	2	0
☐ Login Compromise	0	0
☐ Malware	1	0
☐ Sighting	3	0
☐ Spearphish	0	0
☐ SQL Injection Attack	0	0
☐ Watchlist	1	0
☐ Watering Hole	2	0

Event Types Table Functions:

FUNCTION

DESCRIPTION

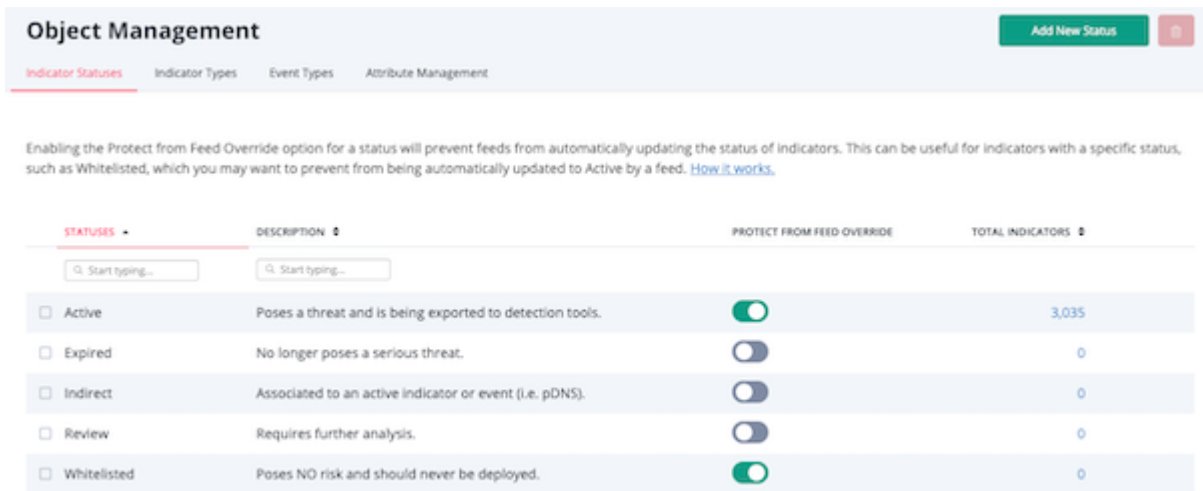
Changing the number of entries displayed in the table

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

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

Adding an Event Type

1. From the main menu, select Settings  > Object Management.
The Object Management page opens to the Indicator Statuses tab.



Object Management Add New Status

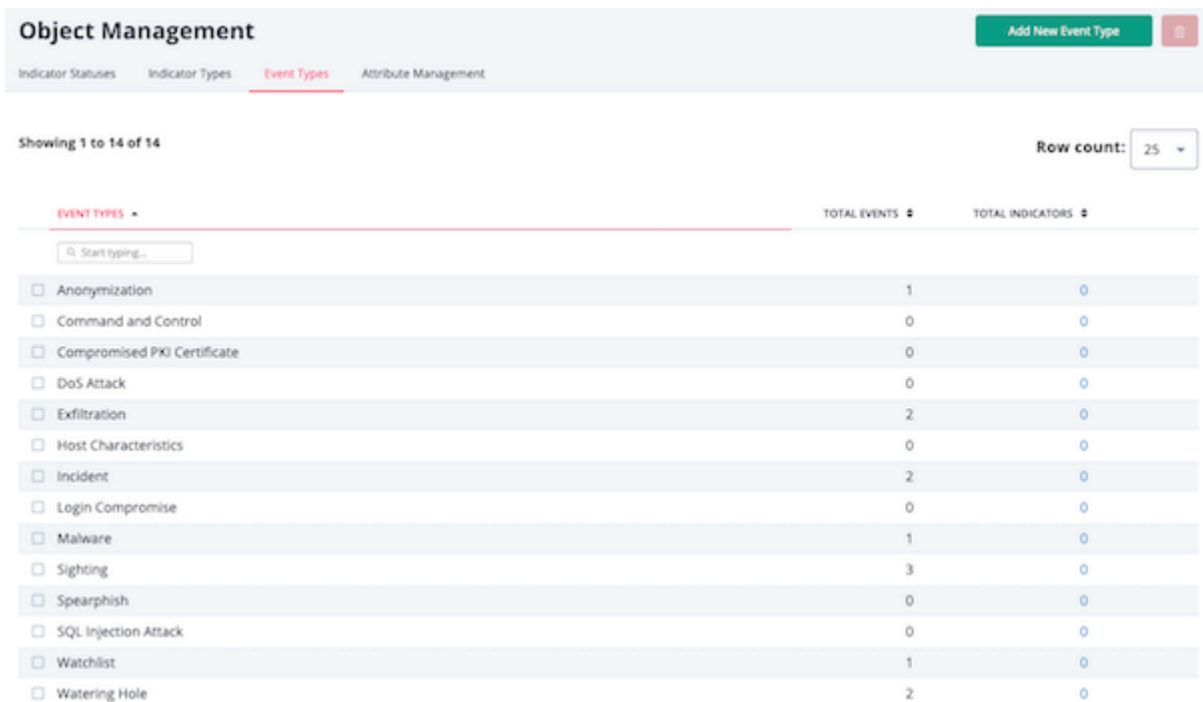
Indicator Statuses Indicator Types Event Types Attribute Management

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

STATUSES	DESCRIPTION	PROTECT FROM FEED OVERRIDE	TOTAL INDICATORS
Start typing...	Start typing...		
☐ Active	Poses a threat and is being exported to detection tools.	☒	3,035
☐ Expired	No longer poses a serious threat.	☐	0
☐ Indirect	Associated to an active indicator or event (i.e. pDNS).	☐	0
☐ Review	Requires further analysis.	☐	0
☐ Whitelisted	Poses NO risk and should never be deployed.	☒	0

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

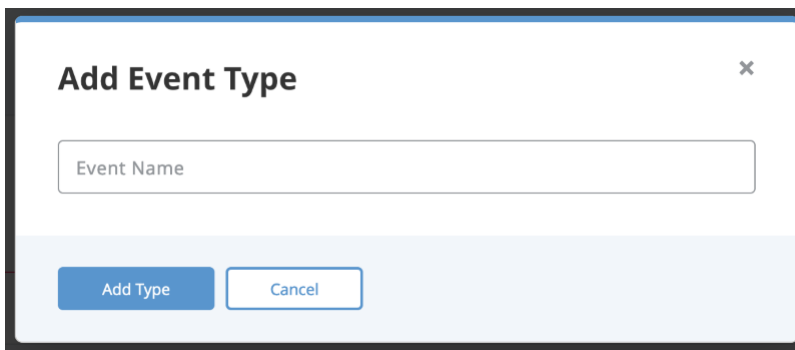
The Event Types tab opens.



EVENT TYPES	TOTAL EVENTS	TOTAL INDICATORS
☐ Anonymization	1	0
☐ Command and Control	0	0
☐ Compromised PKI Certificate	0	0
☐ DoS Attack	0	0
☐ Exfiltration	2	0
☐ Host Characteristics	0	0
☐ Incident	2	0
☐ Login Compromise	0	0
☐ Malware	1	0
☐ Sighting	3	0
☐ Spearphish	0	0
☐ SQL Injection Attack	0	0
☐ Watchlist	1	0
☐ Watering Hole	2	0

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

The Add Event Type dialog box opens.



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

Editing an Event Type

You can edit user-generated event types.

 You cannot edit an Event Type provided by ThreatQ.

1. Navigate to Settings  > Object Management.

The Object Management page opens to the Indicator Statuses tab.

Object Management

Add New Status

Indicator Statuses
Indicator Types
Event Types
Attribute Management

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

STATUSES	DESCRIPTION	PROTECT FROM FEED OVERRIDE	TOTAL INDICATORS
Start typing...	Start typing...		
☐ Active	Poses a threat and is being exported to detection tools.	☒	3,035
☐ Expired	No longer poses a serious threat.	☐	0
☐ Indirect	Associated to an active indicator or event (i.e. pDNS).	☐	0
☐ Review	Requires further analysis.	☐	0
☐ Whitelisted	Poses NO risk and should never be deployed.	☒	0

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

The Event Types tab opens.

Object Management

Add New Event Type

Indicator Statuses
Indicator Types
Event Types
Attribute Management

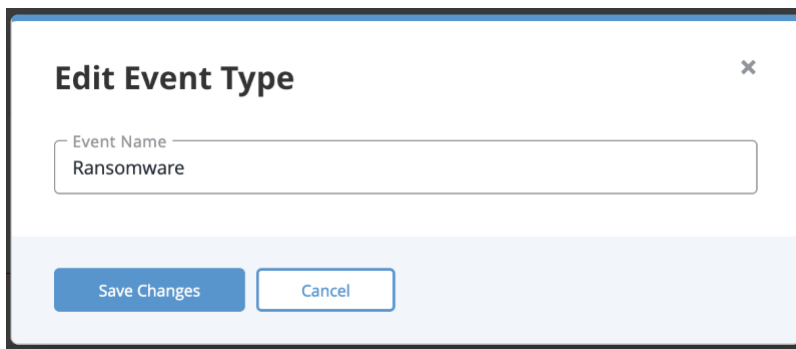
Showing 1 to 14 of 14

Row count: 25

EVENT TYPES	TOTAL EVENTS	TOTAL INDICATORS
Start typing...		
☐ Anonymization	1	0
☐ Command and Control	0	0
☐ Compromised PKI Certificate	0	0
☐ DoS Attack	0	0
☐ Exfiltration	2	0
☐ Host Characteristics	0	0
☐ Incident	2	0
☐ Login Compromise	0	0
☐ Malware	1	0
☐ Sighting	3	0
☐ Spearphish	0	0
☐ SQL Injection Attack	0	0
☐ Watchlist	1	0
☐ Watering Hole	2	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 text "Ransomware". At the bottom of the dialog, there are two buttons: "Save Changes" and "Cancel".

Edit Event Type

Event Name
Ransomware

Save Changes Cancel

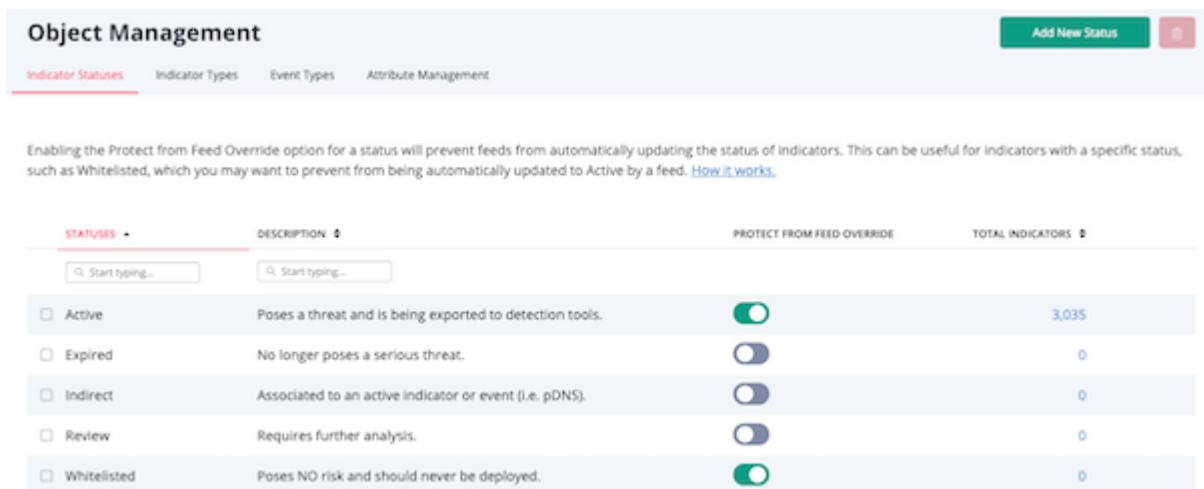
4. Enter a new **Event Name**.
5. Click **Save Changes**.

Deleting an Event Type

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

1. Navigate to Settings  > Object Management.

The Object Management page opens to the Indicator Statuses tab.

The image shows the "Object Management" page in the ThreatQ interface. It has a header with the title "Object Management" and a button "Add New Status". Below the header are four tabs: "Indicator Statuses" (selected), "Indicator Types", "Event Types", and "Attribute Management". A note explains the "Protect from Feed Override" option. Below the note 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, and a count of indicators.

Object Management Add New Status

Indicator Statuses Indicator Types Event Types Attribute Management

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

STATUSES	DESCRIPTION	PROTECT FROM FEED OVERRIDE	TOTAL INDICATORS
☐ Active	Poses a threat and is being exported to detection tools.	☒	3,035
☐ Expired	No longer poses a serious threat.	☐	0
☐ Indirect	Associated to an active indicator or event (i.e. pDNS).	☐	0
☐ Review	Requires further analysis.	☐	0
☐ Whitelisted	Poses NO risk and should never be deployed.	☒	0

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

The Event Types tab opens.

Object Management

Add New Event Type

Indicator Statuses
Indicator Types
Event Types
Attribute Management

Showing 1 to 14 of 14

Row count: 25

EVENT TYPES	TOTAL EVENTS	TOTAL INDICATORS
☐ Anonymization	1	0
☐ Command and Control	0	0
☐ Compromised PKI Certificate	0	0
☐ DoS Attack	0	0
☐ Exfiltration	2	0
☐ Host Characteristics	0	0
☐ Incident	2	0
☐ Login Compromise	0	0
☐ Malware	1	0
☐ Sighting	3	0
☐ Spearphish	0	0
☐ SQL Injection Attack	0	0
☐ Watchlist	1	0
☐ Watering Hole	2	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**.

Attribute Management

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



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

Object Management

Indicator Statuses Indicator Types Event Types **Attribute Management**

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

Select an object
Indicators

Source

Attribute Keys

EditMergeDelete

KEYS

OBJECT COUNT

Search...

☐	Att1	1
☐	Att2	4
☐	att3	1
☐	ParAtt1	1

Att1 Values

EditMergeDelete

VALUE

SOURCE

OBJECT COUNT

Search...

☐	1	threatq@threatq.com	1

Examples:

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

Selecting an Attribute Key or Value

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

Tips and Tricks

- Click the up/down arrows next to a column name to sort a list in ascending/descending order.
- Click the left/right arrows and page numbers below the attribute keys or values lists to view additional list items.
- Use the Rows per page field to select the number of attribute keys or values displayed on each page.

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

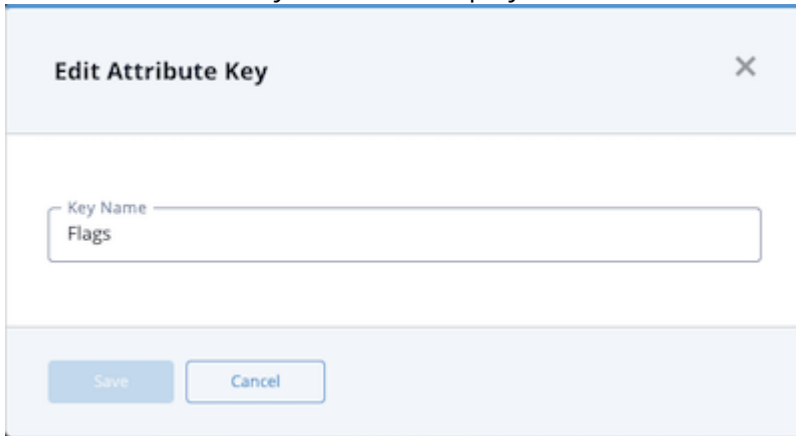
Editing Attribute Keys

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



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

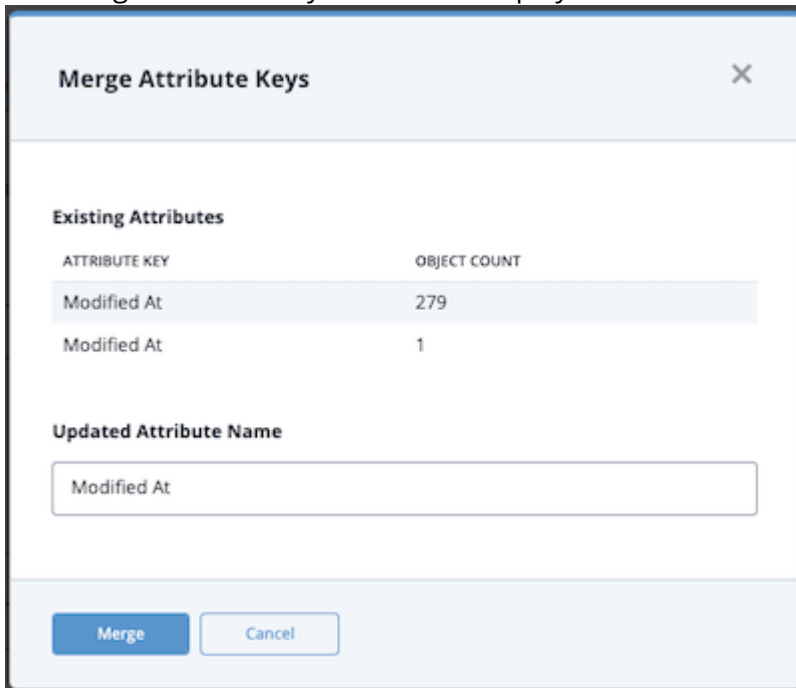
- Click the Edit button.
The Edit Attribute Key window is displayed.



- Enter your changes to the attribute key.
- Click the Save button.

Merging Attribute Keys

- From the Attribute Keys list, click the checkbox next to the attribute types you want to merge.
- Click the Merge button.
The Merge Attribute Keys window is displayed.



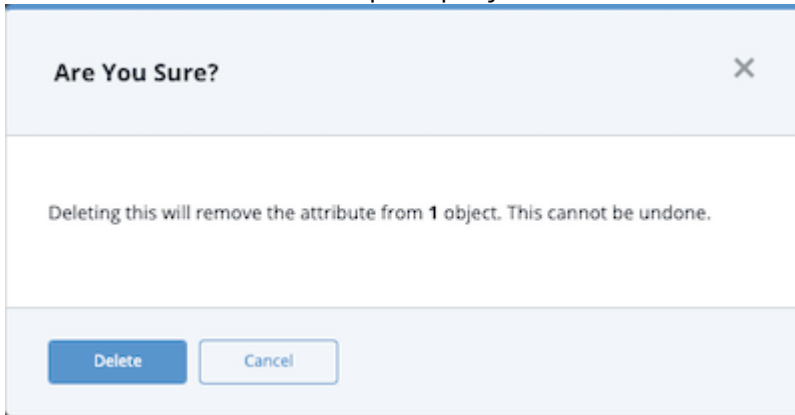
ATTRIBUTE KEY	OBJECT COUNT
Modified At	279
Modified At	1

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

Deleting Attribute Keys

- From the Attribute Keys list, click the checkbox next to the attribute(s) you want to delete.

- Click the trash can button.
- The **Are You Sure?** window prompts you to confirm the deletion.



- Click the Delete button.

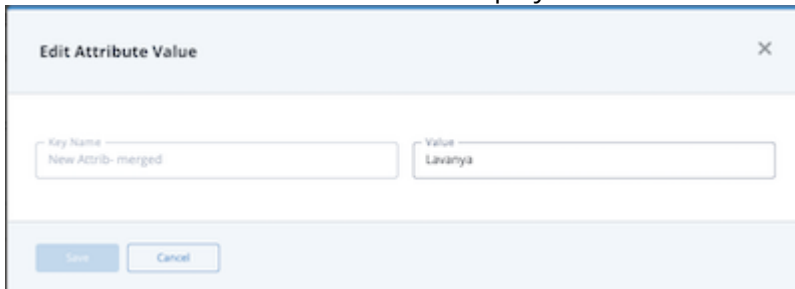
Editing Attribute Values

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



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

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

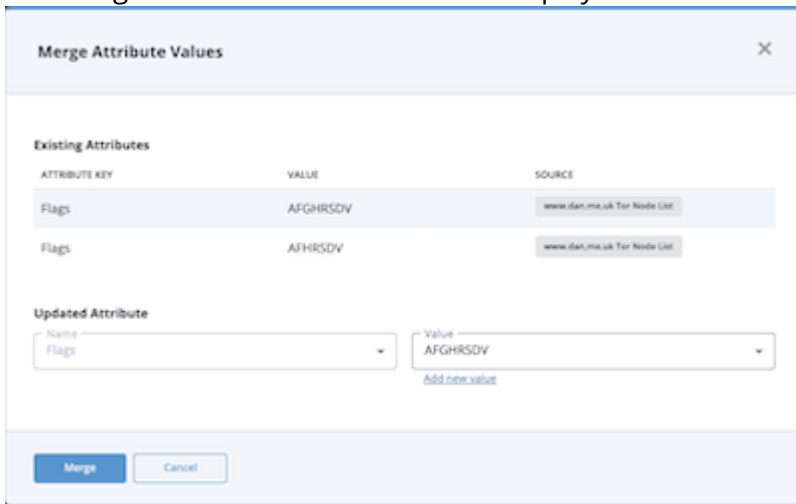


- Enter your changes to the attribute value.
- Click the Save button.

Merging Attribute Values

- From the attribute values list, click the checkbox next to the attribute values you want to merge.

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



The 'Merge Attribute Values' window displays a table of existing attributes and options to update or add new values.

Attribute Key	Value	Source
Flags	AFGHRSDV	www.dan.mca.uk Tor Node List
Flags	AFHRSOV	www.dan.mca.uk Tor Node List

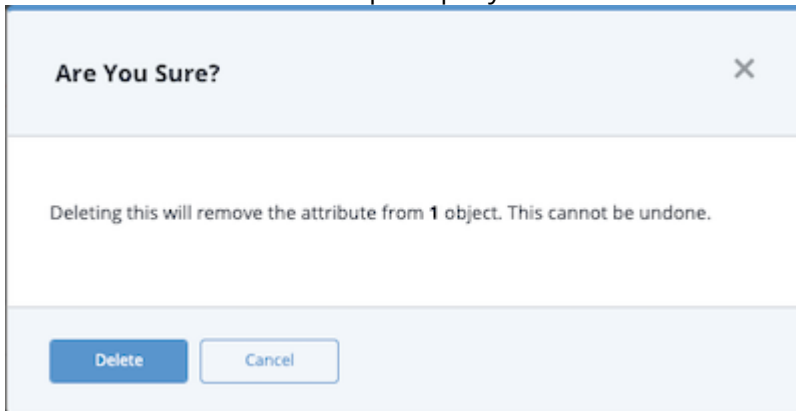
Below the table, the 'Updated Attribute' section shows a dropdown menu for the Name (set to 'Flags') and a dropdown menu for the Value (set to 'AFGHRSDV'). A link 'Add new value' is present below the value dropdown.

At the bottom, there are 'Merge' and 'Cancel' buttons.

3. To specify a new attribute value name for the merged values , use one of the following methods:
 - Click the Value field and use the **Search for attribute values** field to locate an existing value.
 - Click the Add new value link and enter the new value in the **Type new value** field.
4. Click the Merge button.

Deleting Attribute Values

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



The 'Are You Sure?' window displays a confirmation message: 'Deleting this will remove the attribute from 1 object. This cannot be undone.'

At the bottom, there are 'Delete' and 'Cancel' buttons.

4. Click the Delete button.

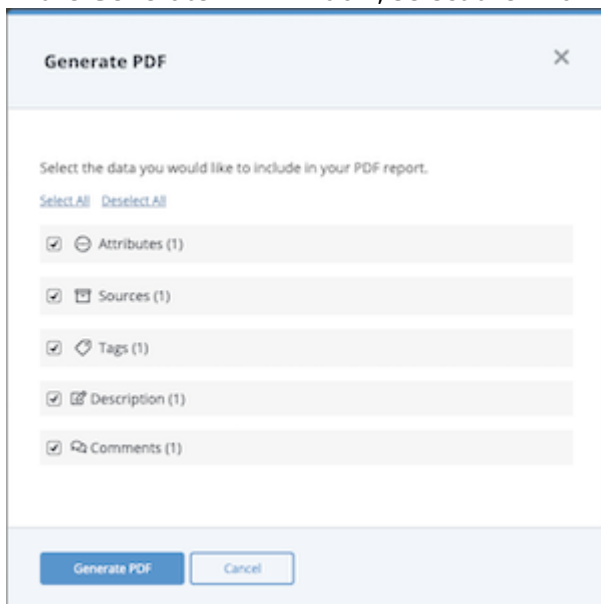
Reports

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

Generating Reports

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

1. Access the system object's details page.
2. Click the **Actions** button.
3. Click the Generate PDF option.
4. In the Generate PDF window, select the information you want to include in the PDF.



5. Click the Generate PDF button.
The PDF summary downloads and opens in a new browser tab.



Google Chrome Users: Google Chrome's pop-up blocker prevents object PDF summary reports from downloading. We recommend changing your browser settings to allow pop-ups from your ThreatQ instance. See [Turning Off the Pop-up Blocker in Chrome](#) for more information.



The generated PDF may contain active links to internal and external locations. Related objects in the PDF link to an internal ThreatQ instance that may require authentication. Please be aware of potential impacts before distribution of the generated report.

Turning Off the Pop-Up Blocker in Chrome

By default, Google Chrome blocks pop-ups from automatically showing up on your screen. When a pop-up is blocked, the address bar will display a pop-up blocked alert. This pop-up blocker will prevent your PDF from being downloaded. Complete the following steps to allow pop-ups from ThreatQ.

Procedure:

1. Go to ThreatQ where pop-ups are blocked.
2. In the address bar, click the **Pop-up blocked** alert icon.
3. Click the link for the pop-up you want to see.
4. To always see pop-ups for the site, select Always allow pop-ups from [your ThreatQ instance].
5. Click **Done**.

Report Options

You can navigate to **Settings > Report Options** to customize the PDF reports that are generated. Report options apply to all reports generated platform-wide. You can make the following customizations:

Customizing the Report Header

1. Select the **Settings** icon > **Report Options**.
2. Under **Header Banner**, complete one of the following steps:
 - Drag and drop the image you want to use as the header.
 - Click **Browse** and navigate to the image you want to use as the header.
3. Optionally, click **Restore header banner to defaults**.
4. Click **Save**.

Customizing Report Text Colors

1. Select the **Settings** icon > **Report Options**.
2. Under **Colors**, use the drop down menus to select:
 - Header Text
 - Heading Text
 - Body Text
3. Click **Save**.

Adding a Custom Disclaimer to a Report

You can add a custom disclaimer to include with your report to communicate any liabilities or limitations to the end users of the report.

1. Select the **Settings** icon > **Report Options**.
2. Under **Disclaimer**, enter your disclaimer text and then use the formatting tools to customize your message.

3. Click **Save**.

Previewing Report Customization

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

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

The sample report downloads to your computer.

Server Administration

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

ThreatQ Monitoring Platform



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

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

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

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

Creating a User Account for the ThreatQ Monitoring Platform

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

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

```
<> groupadd <groupname>
```



```
groupadd cockpit
```

2. Use one of the following methods to create a user:
 - Create a user as a part of a group:

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

```
EX adduser -G cockpit testUser
```

- Create a user not assigned to a group:

```
<> adduser <username>
```

```
EX adduser testUser
```

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

```
<> passwd <username>
```

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

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

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

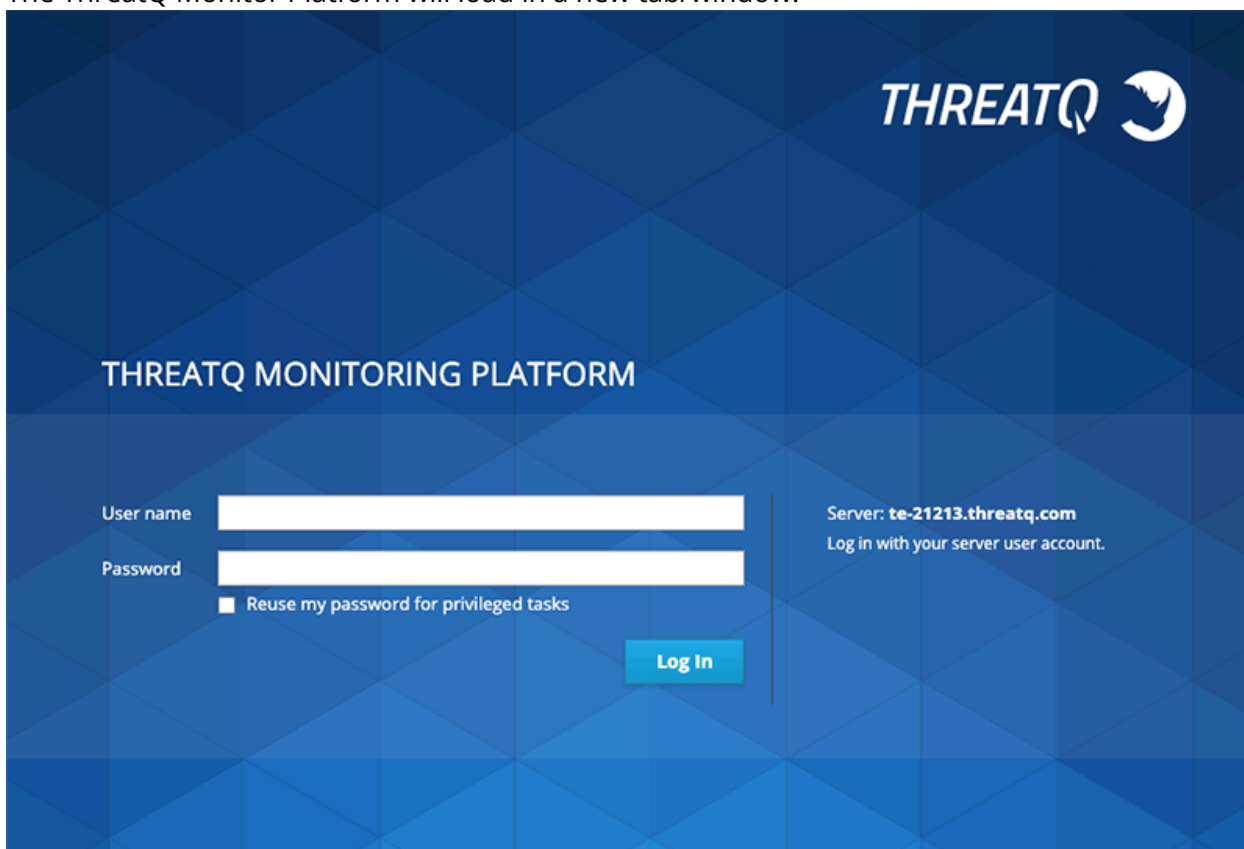
5. Use the new user account to log into the server administrator console.

Accessing the ThreatQ Monitoring Platform

 Root user access is disabled for the ThreatQ Monitoring Platform.

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

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



THREATQ 

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

D diagnostic Reports

Kernel Dump

SELinux

Terminal

Hardware

RDO OpenStack Compute

Asset Tag

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

Machine ID

93fe483e696d47f68791067e240e1427

Operating System

CentOS Linux 7 (Core)

Secure Shell Keys

Show fingerprints

Host Name

te-21213.threatq.com

Domain

Join Domain

System Time

2020-12-15 17:49

Power Options

Restart

Performance Profile

virtual-guest

% of 4 CPU cores

GiB Memory & Swap

MiB/s Disk I/O

Kbps Network Traffic

Sharing

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

User Permission Levels

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

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

Viewer Viewers can access the data collection, dashboard, or investigation but cannot change it. In addition, they can view user permissions for data collections and investigations.

Private If a user creates a data collection, dashboard, or investigation and does not assign permissions to a user or group, only that user (now the owner) can access it.

User Permission Levels and User Roles

A user can assign any permission level to user accounts with the following user roles:

- Maintenance Account
- Administrative Access
- Primary Contributor Access

However, the only permission level a user can assign to a Read Only Access user account is viewer permission.



Ownership and public viewing permissions are applied to all data collections created before upgrading to version 4.54. Any data collections created by custom integrations (instead of Threat Library) are assigned ownership permissions for the custom integration client, but are not shareable. If you want to manage a data collection used by a custom integration in Threat Library in the future, you must first create it in Threat Library and then reference it in the custom integration.

View-Only Permissions for All Users

ThreatQ allows you to assign view-only permissions to all users. To do this, select a permission-level of **Everybody (Public)**. This assigns viewer permissions to all users unless they are assigned user-level permissions that are greater. For example, if I have editor permissions for the Adversary Hunt data collection and the other users have viewer permissions, when Bella (the owner) grants **Everybody (Public)** permissions, I retain my editor permissions. Each individual viewer is now grouped together as **Everybody (Public)** and no longer listed individually in the Sharing modal's **Who has access** list.

Sharing Notifications

The ThreatQ Notification Center alerts you about data collection, dashboard, or investigation permission changes that affect you. As such, you receive a notification when:

- A user shares a data collection, dashboard, or investigation with you.
- A user changes your permissions to owner, editor, or viewer.
- A data collection, dashboard, or investigation you own has been shared with another user.
- Your permissions to a data collection, dashboard, or investigation have been removed.

- A user requests access to an investigation you own.

See the [Sharing Notifications](#) topic for more details.

Permission Conversion

When you upgrade to version 4.54, ThreatQ updates your existing permissions as follows:

- **Data Collections** - For an existing data collection, the creator is automatically assigned owner permissions. All other users are assigned **Everybody (Public)** permissions.
- **Dashboards** - All users are assigned viewer permissions for ThreatQ's default dashboards and these permissions cannot be changed. All other user-created dashboards are assigned permissions based on the previous permission model. Dashboard creators have owner permissions. If a dashboard was shared with a user, the user retains the previously granted editor or viewer permissions.
- **Investigations** - Maintenance Account, Administrative Access, and Primary Contributor Access users are given editor permissions for all existing investigations that have a Visibility of Shared. Read Only Access users receive viewer permissions.

If a user that created a data collection, dashboard, or investigation was deleted prior to your upgrade to 4.54/4.55, the corresponding object is assigned to the most recently created admin or super user.

Permission Levels and Integrations

User-managed integrations use data collections created and maintained in the Threat Library. As such, user and group permission levels control access to these data collections.

Client-managed integrations are managed through the API. As such, user and group permissions do not control a client's ability to view, add, update or delete these data collections.

Legacy, Client-Managed Data Collections

For existing, client-managed data collections, the user who created it is assigned owner-level permissions. All other users are assigned view-only access through **Everybody (Public)** group permissions.

Client-Managed Integrations

Through the API, clients have full access to all data collections (view, add, update, and delete). As a result, the new permission levels (owner, editor, viewer) only apply when authenticating with username and password credentials (for example, as a user accessing the user interface) as opposed to authenticating with client credentials.

Legacy, User-Managed Data Collections

For each existing saved data collection, the user who created it has owner-level permissions. All other users have view access through the **Everybody (Public)** group permission.

Air Gapped Data Sync (AGDS) and Investigation Sharing

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

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

See the [Air Gapped Data Sync \(AGDS\)](#) section for more information.

System Configuration

About System Configuration

The System Configurations page consists of the Proxy, Account Security, and General Settings tabs. These tabs allow you to enable, disable, and update multiple system-level settings. When you access the System Configurations page, the Account Security tab is displayed by default.

System Configurations

Account Security

Proxy

General

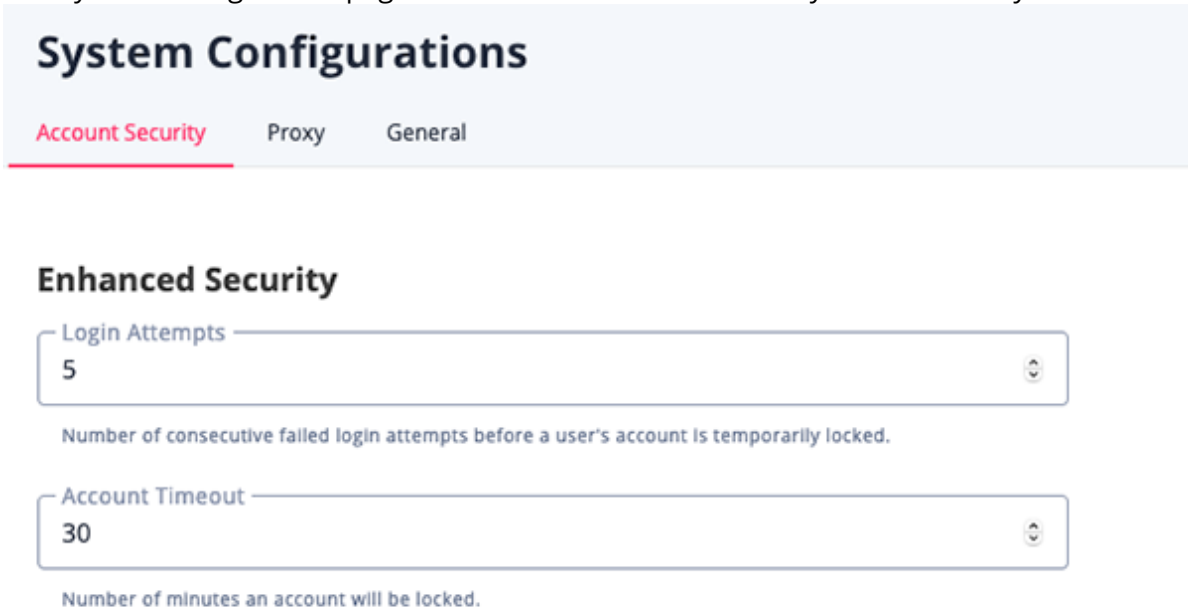
TAB	DESCRIPTION
Account Security	Configure the number of failed login attempts before a user is locked out and the number of minutes a user will be locked out before being able to reattempt login. You can also configure and enable/disable custom login banners.
Proxy	Enable and disable proxy settings.
General Settings	Configure the date and time format, indicator parsing checkbox defaults, and enable/disable the sharing of analytics data with ThreatQuotient.

Setting Account Lockout

The **Enhanced Security** section of the Account Security tab allows you to specify the number of failed login attempts before a user is locked out and the number of minutes a user will be locked out before he can attempt to log in again. By default, failed login attempts are set to five and the timeout period is set to thirty minutes.

Configuring User Lockout Settings

1. Navigate to Settings  > System Configurations.
The System Configuration page loads with the Account Security tab selected by default.



System Configurations

Account Security Proxy General

Enhanced Security

Login Attempts

Number of consecutive failed login attempts before a user's account is temporarily locked.

Account Timeout

Number of minutes an account will be locked.

3. Enter your changes to the following fields:

FUNCTION	DESCRIPTION
Login Attempts	The number of consecutive failed login attempts before a user's account is temporarily locked.
Account Timeout	The number of minutes an account is locked after the specified number of failed log in attempts.

4. Click the Save button to save your changes.

Managing Custom Login Banners

The **Require Disclaimer Acceptance** section of the **Account Security** tab allows system administrators to enable a custom message displayed to all users when logging into the ThreatQ Platform. When enabled, ThreatQ users are required to review and accept the message.



In order to comply with government regulations, a customer could configure a custom banner to display a message during login requiring users to accept additional privacy and security terms.

Banner Behavior

The **Require Disclaimer Acceptance** toggle allows you to enable/disable the display of the custom banner.

Require Disclaimer Acceptance

Disabled  Enabled

Once enabled, all users will be required to accept the disclaimer text provided below in order to log in to their account.

When the toggle is disabled:

- The banner title and body are visible to administrators in the **Account Security** tab, but the banner is not displayed to users upon log in.
- Users can access to the platform using only their credentials

When the toggle is enabled:

- After a user enters their login and password, the custom banner displays. Users must click the **Accept and Continue** button to access the platform.
- If a user closes the banner without clicking the **Accept and Continue** button, he is returned to the login screen and cannot access the platform until he clicks the **Accept and Continue** button.



Users are required to click the **Accept and Continue** button each time they log into platform.

- If a user is logged out and enters a URL for a specific page in the platform, the custom banner is displayed and he must click the **Accept and Continue** button to access the specified page.

Enabling a Custom Banner



Only administrators have access to enable the custom banner configuration fields in the **Account Security** tab on the *System Configuration* page.

1. Navigate to Settings  > System Configurations.
The System Configuration page loads with the Account Security tab selected by default.

System Configurations

Account Security

Proxy

General

Enhanced Security

Login Attempts

5



Number of consecutive failed login attempts before a user's account is temporarily locked.

Account Timeout

30



Number of minutes an account will be locked.

Require Disclaimer Acceptance

Disabled



Enabled

Once enabled, all users will be required to accept the disclaimer text provided below in order to log in to their account.

Disclaimer Title

Disclaimer Title

Format



B



I



U



S



A



A



Description

Save

2. Click the toggle switch in the Require Disclaimer Acceptance section to enable the display of the custom banner.
3. Enter the banner title to be displayed at the top of the banner in the Disclaimer Title field.
4. Enter the body of the message in the Description field.



The Description field supports standard text formatting as well as the use of links and tables.

5. Click the Save button.
The next time a user logs in, he is prompted to review and accept the custom banner before proceeding to the platform.

Proxy

The Proxy configuration page allows you to enable or disable proxies.

 Users are required to set their proxy server settings to use http: for their https: traffic.

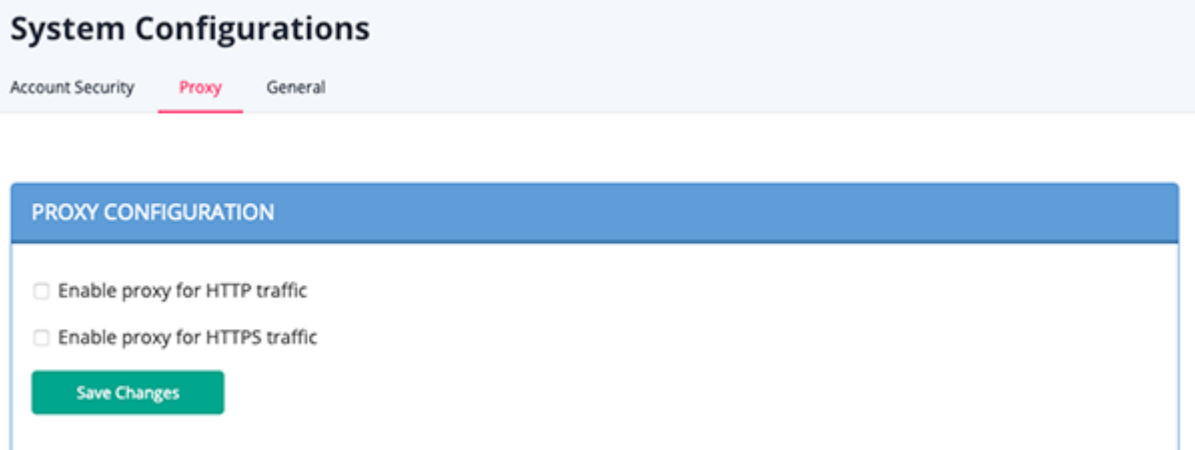
Accessing Proxy Configuration

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

The System Configurations page opens to the Account Security tab selected by default.

2. Click the **Proxy** tab.

The Proxy Configuration tab loads.



System Configurations

Account Security **Proxy** General

PROXY CONFIGURATION

☐ Enable proxy for HTTP traffic

☐ Enable proxy for HTTPS traffic

Save Changes

3. Select the checkboxes for **HTTP** and **HTTPS** traffic options to expand those fields.

PROXY CONFIGURATION

☒ Enable proxy for HTTP traffic

Protocol

Server

Port

80

☐ Proxy server requires password

Username

Password

☒ Enable proxy for HTTPS traffic

Protocol

Server

Port

80

☐ Proxy server requires password

Username

Password

Save Changes

4. Enter your proxy server IP Address and Port in the field provided for both HTTP and HTTPS sections.
5. Optional - Select the **Proxy Server Requires Password**, if your server requires a username and password, and complete the **Username** and **Password** fields. Leave the checkboxes unselected and the username and password fields blank if your server does not require this information.
6. Click on **Save Changes**.

Setting Proxy Server Settings for Commands and Custom Connectors

PIP and YUM upgrade commands, as well as custom connectors and associated cron jobs, require that you set your proxy information in your environment files. This does not replace the process above but must be performed in addition in order to use custom connectors and the commands. Before you begin, you should collect a list of proxy exceptions. These are entries that you do not want to add to the proxy. The exceptions can be hostnames or FQDNs. In the case where DNS is not available, you can use the `/etc/hosts` to ensure hostname resolution is recommended.

1. SSH into your ThreatQ instance.
2. Open the environment file using the `vi` command:

```
vi /etc/environment
```

3. Press the `i` character to enter insert mode. Enter your following entry into the file while replacing the placeholders with your information. These settings are case-sensitive so you must include both the lowercase, ex: `http`, and uppercase, ex: `HTTP`, versions.



You can add exceptions to the no_proxy strings to prevent specific entries that should not be forwarded to the proxy. The minimal value for no_proxy should be the loopback IP address and "localhost" plus the TQ entry for itself "threatq". Do not use CIDR notation or wildcards with no_proxy entries as they are not accepted formats. In that situation, list the IP addresses.

If Proxy Server Requires a Password

```
http_proxy=http://<username>:<password>@<Proxy IP>:<Proxy Port>
HTTP_PROXY=http://<username>:<password>@<Proxy IP>:<Proxy Port>
https_proxy=http://<username>:<password>@<Proxy IP>:<Proxy Port>
HTTPS_PROXY=http://<username>:<password>@<Proxy IP>:<Proxy Port>
no_proxy=localhost,127.0.0.1,threatq,<ThreatQ IP>, <ThreatQ Hostname>
NO_PROXY=localhost,127.0.0.1,threatq,<ThreatQ IP>, <ThreatQ Hostname>
```

If Proxy Server Does Not Require a Password

```
http_proxy=http://<Proxy IP>:<Proxy Port>
HTTP_PROXY=http://<Proxy IP>:<Proxy Port>
https_proxy=http://<Proxy IP>:<Proxy Port>
HTTPS_PROXY=http://<Proxy IP>:<Proxy Port>
no_proxy=localhost,127.0.0.1,threatq,<ThreatQ IP>, <ThreatQ Hostname>
NO_PROXY=localhost,127.0.0.1,threatq,<ThreatQ IP>, <ThreatQ Hostname>
```

4. Press the **ESC** key and enter the following command to close the editor:

```
:wq <Enter Key>
```

The next several steps will show you how to ensure that custom connector CRON jobs are able to use the proxy settings. This is achieved by sourcing the environment script so that it is available to all child sessions and applications.

5. Open the proxy.sh file using the vi command:

```
vi /etc/profile.d/proxy.sh
```

6. Press the **i** key to enter Insert mode and enter the following lines:

```
set -a
source /etc/environment
set +a
```

This will ensure the automatic export of any variables created.

7. Press the **ESC** key and enter the following command to close the editor:

```
:wq <Enter Key>
```

8. Log out of your session and then log back in.
9. Run the following command to confirm your settings:

```
printenv | grep -i proxy
```

10. Remove any other proxy-related files from the `/etc/profile.d` directory.

Configuring Time and Date Settings



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

1. Navigate to **Settings**  > **System Configurations**.
2. Click the **General** tab.

System Configurations

Account Security Proxy **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.

Product Analytics

Disabled ☒ Enabled

When enabled, ThreatQ will automatically collect product analytics data in order to enhance your user experience. For more information, reference our [Privacy Policy](#).

Save

3. Select the desired **Date Format**. Options include: MM/DD/YYYY, DD/MM/YYYY, YYYY/MM/DD
4. Select the desired **Time Format**. Options include: 12 hour, 24 hours.
5. Click the **Save** button.

Configuring Indicator Parsing Presets

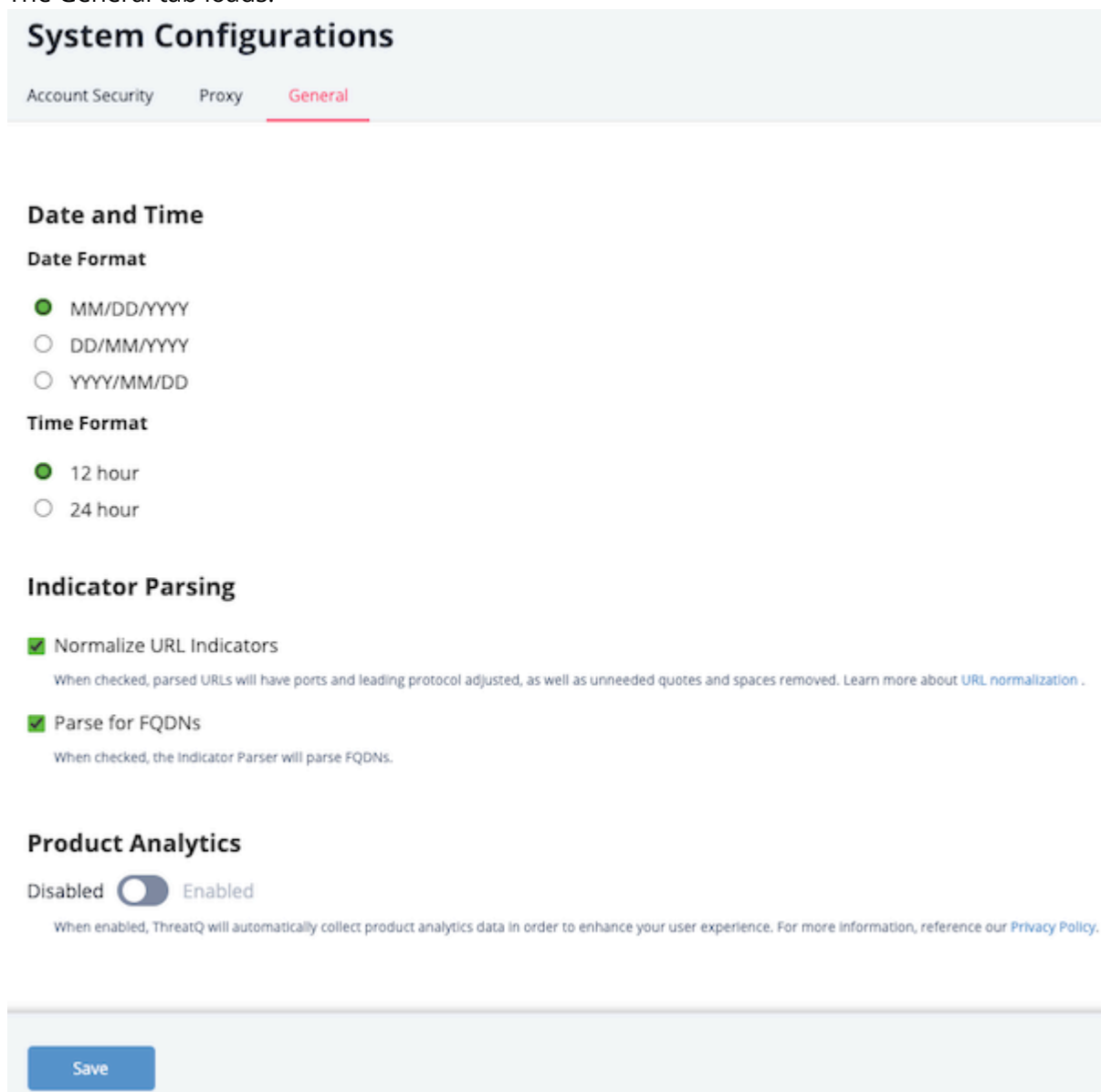
Users with Maintenance and Administrator roles can configure the default state of the **Normalize URL Indicator** and **Parse for FQDNs** checkboxes for the **Parse for Indicators** option of the Add Indicators dialog box.



Setting these default states does not lock the checkboxes. Users can select and deselect each option when parsing for an indicator in the Parse for Indicators dialog box.

1. Navigate to **Settings**  > **System Configurations**.
2. Click the **General** tab.

The General tab loads.



System Configurations

Account Security Proxy **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.

Product Analytics

Disabled ☒ Enabled

When enabled, ThreatQ will automatically collect product analytics data in order to enhance your user experience. For more information, reference our [Privacy Policy](#).

Save

3. In the Indicator Parsing section, set the following options:

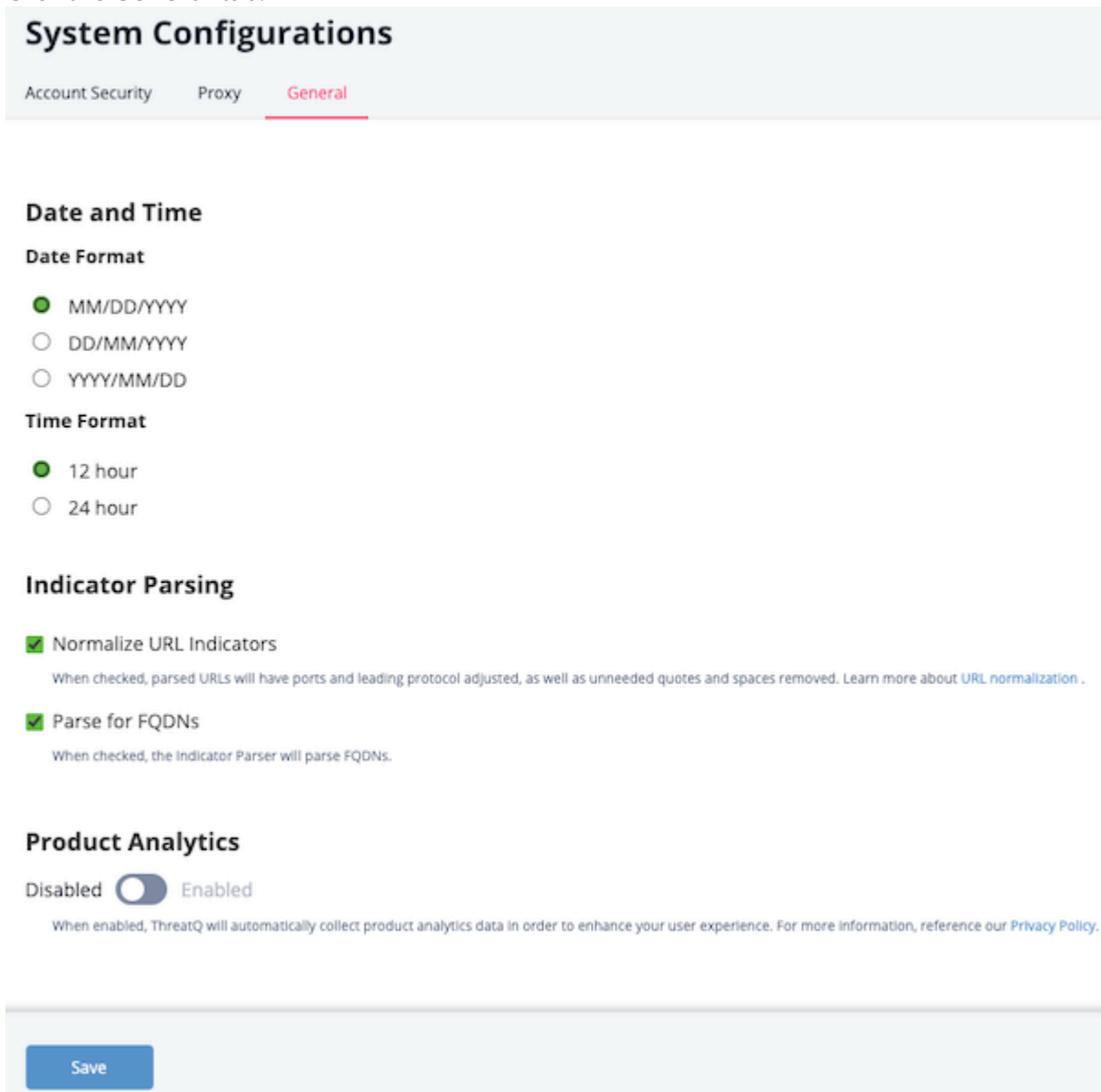
OPTION	DESCRIPTION
Normalize URL Indicators	When checked, parsed URLs will have ports and leading protocol adjusted, as well as unneeded quotes and spaces removed.
Parse for FQDNs	When checked, the Indicator Parser will parse FQDNs from the text and derive FQDN indicators from URLs in the text. Example (checked): URL: https://tqexample.com/table.jspa?query_string_example Indicators created: ○ tqexample.com/table.jspa (the URL) ○ tqexample.com (the derived FQDN from the URL) When unchecked, the Indicator Parser will not generate FQDN indicators from the parsed text. Example (unchecked): URL: https://tqexample.com/table.jspa?query_string_example Indicator created: ○ tqexample.com/table.jspa (the URL)

4. Click the **Save** button.

Opt In/Out of Product Analytics

The Product Analytics toggle allows you to disable/enable the sharing of analytics data with ThreatQuotient. Enabling analytics allows ThreatQuotient to collect anonymized data on user actions to improve the overall user experience.

1. Navigate to **Settings**  > **System Configurations**.
2. Click the **General** tab.



System Configurations

Account Security Proxy **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.

Product Analytics

Disabled ☐ Enabled

When enabled, ThreatQ will automatically collect product analytics data in order to enhance your user experience. For more information, reference our [Privacy Policy](#).

Save

3. In the Product Analytics section, click the toggle button to change the setting from Disabled to Enabled or vice versa.
4. Click the **Save** button.

System Objects

About System Objects

System objects are threat data ingested or manually added to your Threat Library. ThreatQ is seeded with the following system object types:

SYSTEM OBJECT	DESCRIPTION	RELATED TOPICS
Adversaries	Individuals or groups that attempt to perform malicious actions against other individuals or organizations.	Adversaries
Assets	Tangible or intangible items of value to stakeholders.	Assets
Attack Patterns	Descriptions of methods used to exploit software.	Attack Patterns
Campaigns	Groups of behaviors that describe malicious activities taken against specific targets over a period of time.	Campaigns
Courses of Action	A combination of risk response measures taken to address or prevent malicious attacks.	Courses of Action
Events	Objects that focus on temporal incidents that have significant security impact.	Events
Exploit Targets	Identified vulnerabilities in a system, software, or network that can be targeted by tactics, techniques, and procedures (TTP).	Exploit Targets
Files	Received from various intelligence providers and may contain technical cybersecurity data such as Indicator , Adversary , and Malware samples.	Files

SYSTEM OBJECT	DESCRIPTION	RELATED TOPICS
Identities	Contain basic identifying information for targeted groups such as information sources, threat actor identities, and targets of attack.	Identities
Incidents	Records of any violation of an organization's established security/network policy that may compromise security, integrity, or general access.	Incidents
Indicators	Information that describes or identifies methods used to defeat security controls, exploit vulnerabilities, and gain unauthorized access to an internal network. Indicators can also describe malicious reconnaissance to gather technical information, malicious cyber command and control, and any other attribute of cyber security whose disclosure is prohibited by law.	About Indicators
Intrusion Sets	Grouped sets of adversarial behaviors and resources, sometimes referred to as attack packages, used to target an individual organization.	Intrusion Sets
Malware	Targets devices, services, and networks with the intent to gain unauthorized access or damage a network or programmable device.	Malware
Reports	Contain information and related details for a specific threat such as Malware .	Reports
Signatures	Contain the blueprints or patterns associated with a malicious attack on a network or system.	Signatures
STIX	Refers to data in the STIX (Structured Threat Information eXpression) format. STIX is a standardized XML programming language for conveying data about cybersecurity threats.	About STIX
Tasks	Allow you to create and assign tasks to yourself or other users in the platform.	Tasks

SYSTEM OBJECT	DESCRIPTION	RELATED TOPICS
Tools	A legitimate application that can be leveraged to perform malicious activities.	Tools
TTP	Describes how an intruder may attempt to access your system.	TTP
Vulnerabilities	Applications that can be exploited to infiltrate systems/ networks.	Vulnerabilities

Adversaries

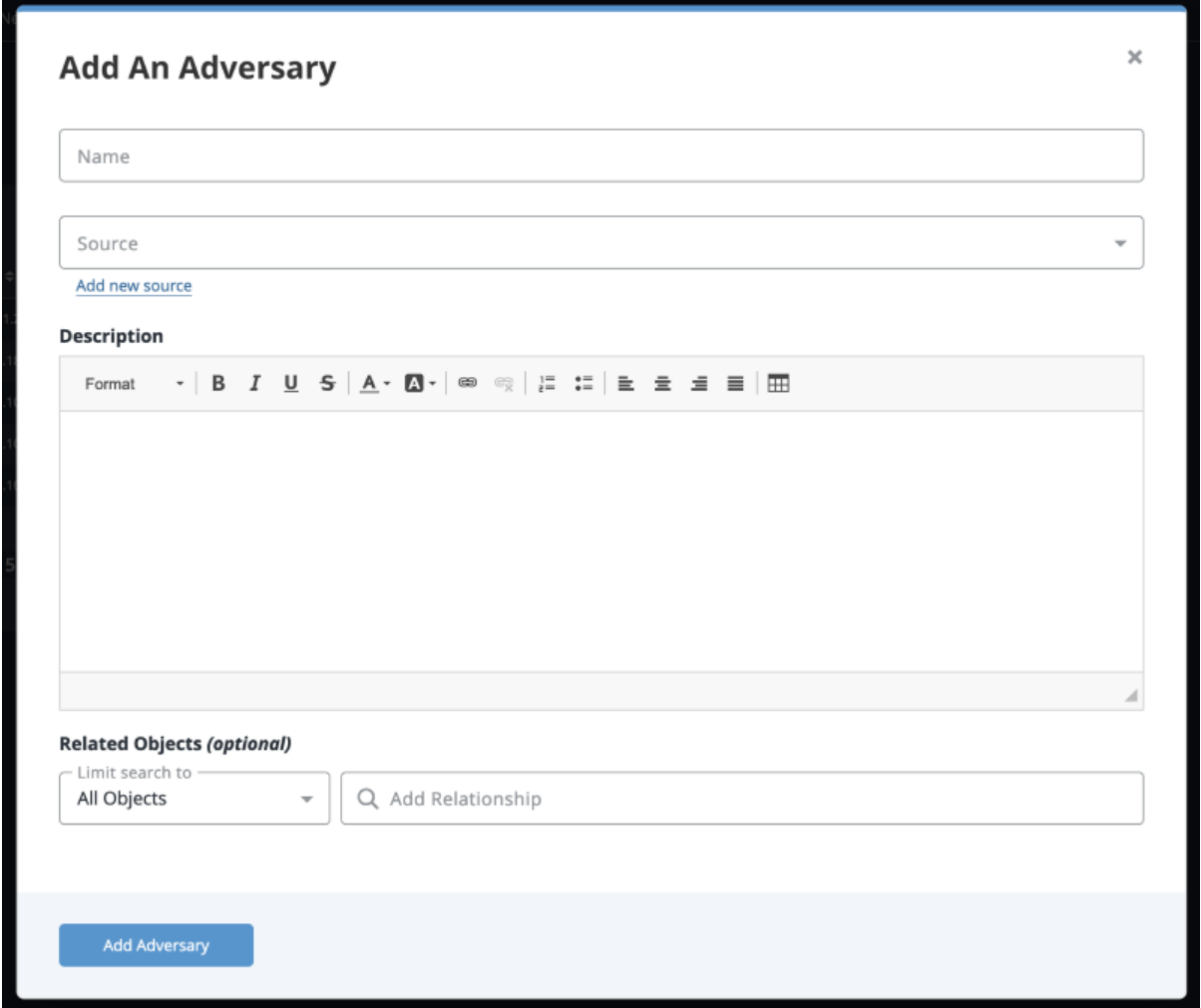
An Adversary is an individual or group that attempts to perform malicious actions against another individual or organization.

Use the steps below to create, edit and delete an Adversary.

Adding Adversaries

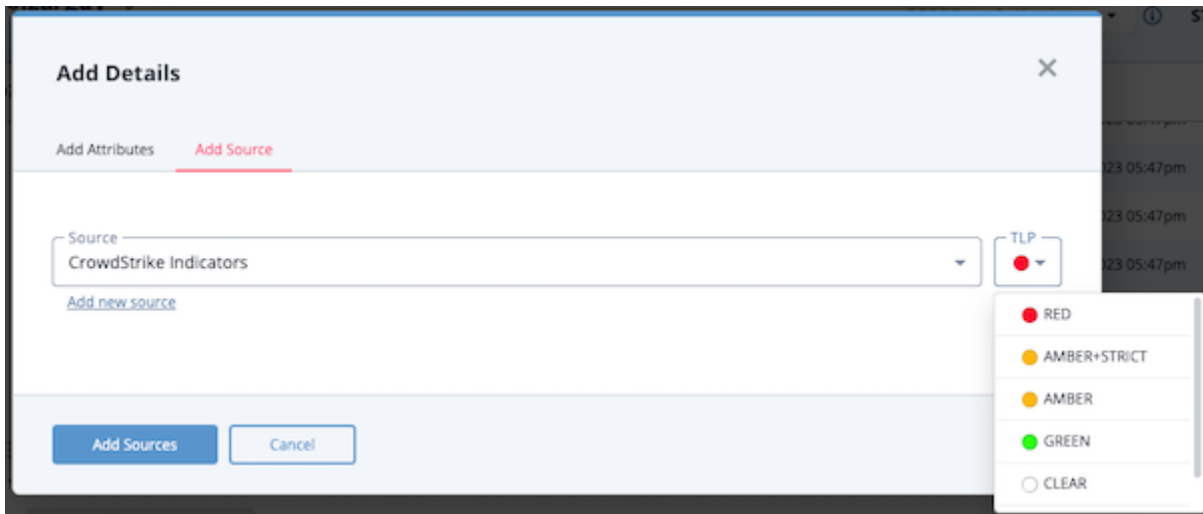
1. Go to **Create > Adversary**.

The Add an Adversary window is displayed.



2. Enter a name.
3. Select a **Source** from the dropdown provided.
You can also click the **Add a New Source** option if the desired source is not listed in the dropdown list. If administrators have enabled TLP view settings, you can select a TLP label for the new source in the dropdown list provided. See the Traffic Light Protocol (TLP) topic for more

information on TLP schema.



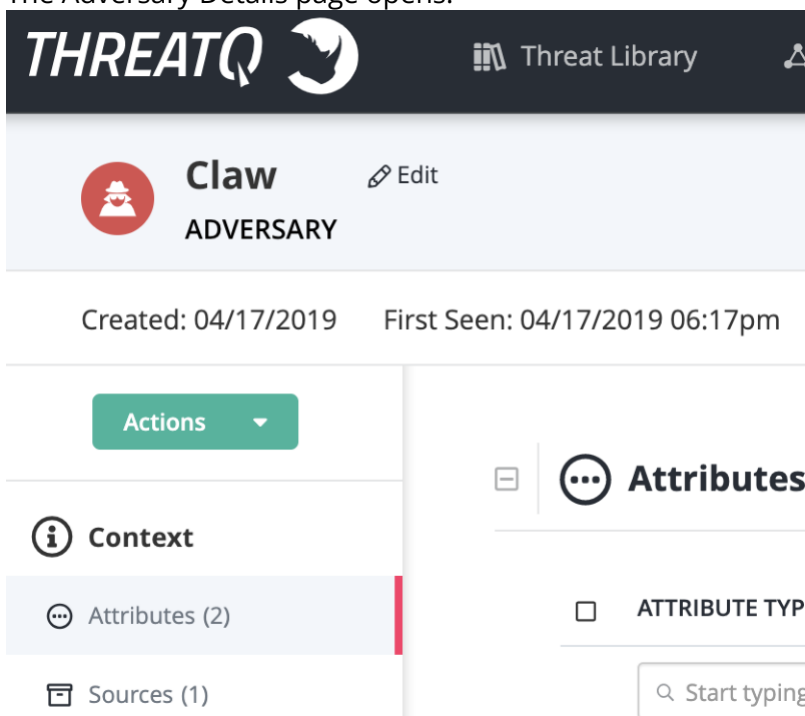
4. Enter a description.
5. Select any **Related Objects** you need to link to the adversary. This field is optional.
6. Click the **Add Adversary** button.

Adding Context

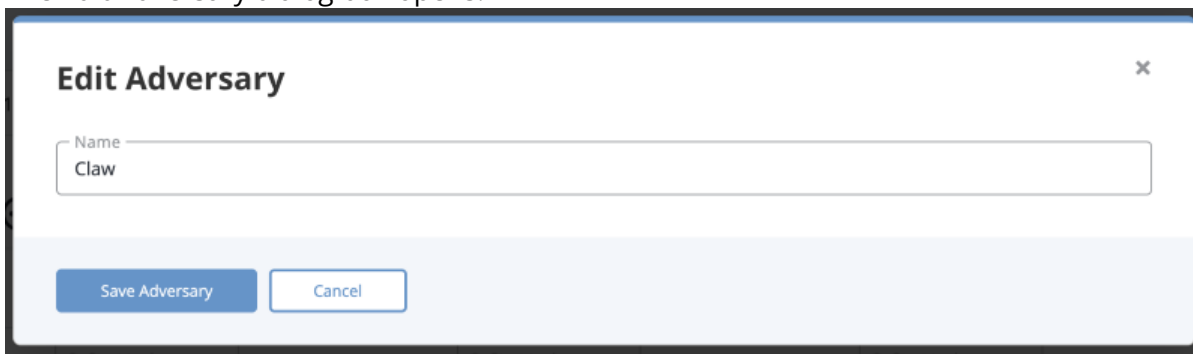
See the [About Object Details](#) section and its topics for details on adding context to an object such as adding sources, attributes, and related objects.

Editing Adversaries

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



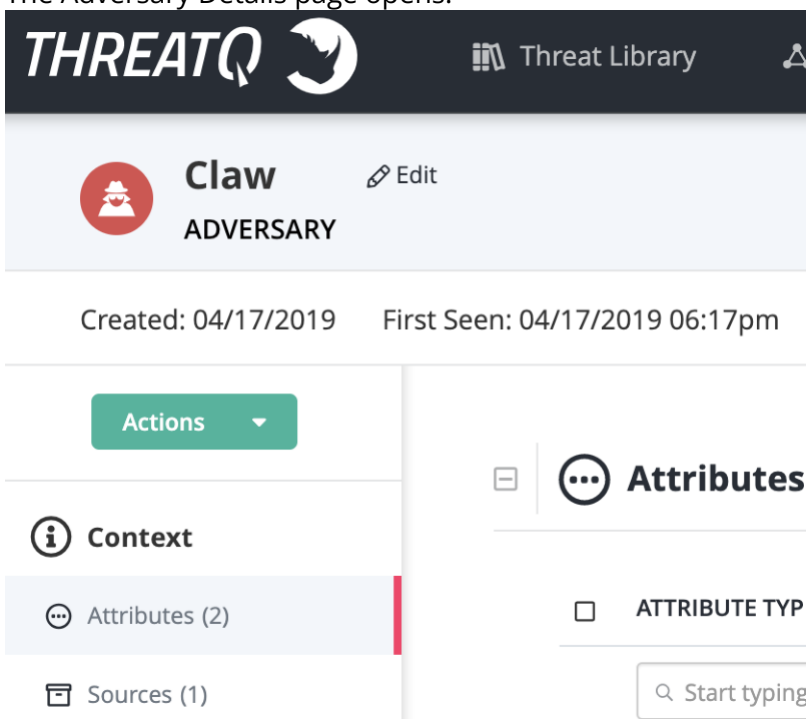
2. Click on **Edit** next to the Adversary name.
The Edit Adversary dialog box opens.

A dialog box titled "Edit Adversary" with a close button (X) in the top right corner. It contains a text input field labeled "Name" with the value "Claw". At the bottom, there are two buttons: "Save Adversary" (blue) and "Cancel" (white with blue border).

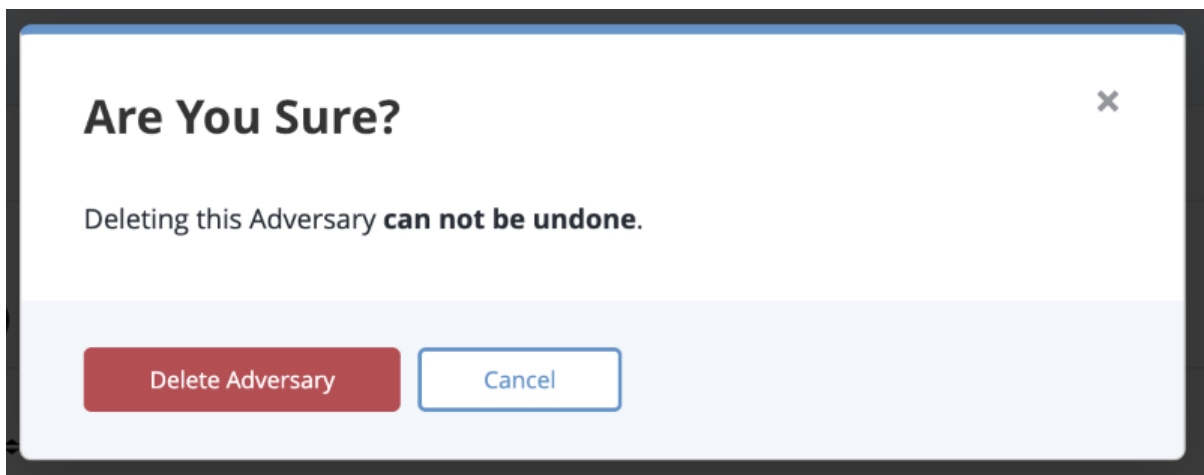
3. Make the desired change to the Adversary name.
4. Click the **Save Adversary** button.

Deleting Adversaries

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

The Adversary Details page for "Claw" in the ThreatQ Threat Library. The header shows the ThreatQ logo and "Threat Library". Below the header, there's a section for "Claw" with a red bull icon, the name "Claw", and the word "ADVERSARY". An "Edit" button is next to the name. Below this, it says "Created: 04/17/2019" and "First Seen: 04/17/2019 06:17pm". On the left, there's a sidebar with "Actions" (a green button with a dropdown arrow), "Context" (with an info icon), "Attributes (2)" (selected, with a red bar), and "Sources (1)". On the right, there's a section for "Attributes" with a menu icon and a search bar labeled "Start typing".

2. Click the **Actions** menu and select **Delete Adversary**.
A confirmation dialog box appears.



3. Click the **Delete Adversary** button.

Assets

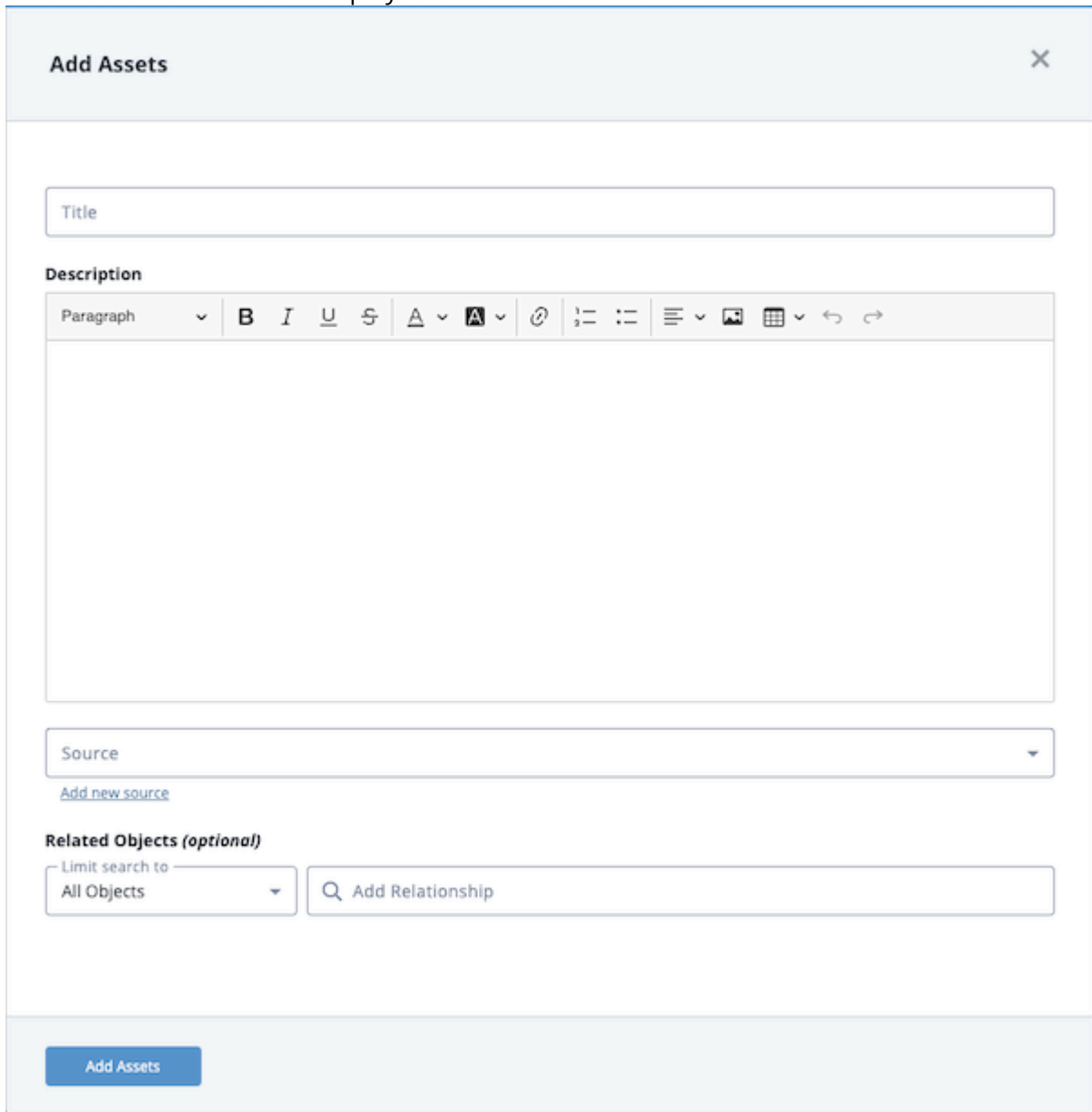
Assets are tangible or intangible items of value to stakeholders. An asset's value is usually based on the impact of the loss of use of the asset. For instance, a company's billing application is a high value asset since the loss of access to this application impacts revenue.

Use the steps below to create, edit and delete Assets.

Adding Assets

1. Go to **Create > Assets**.

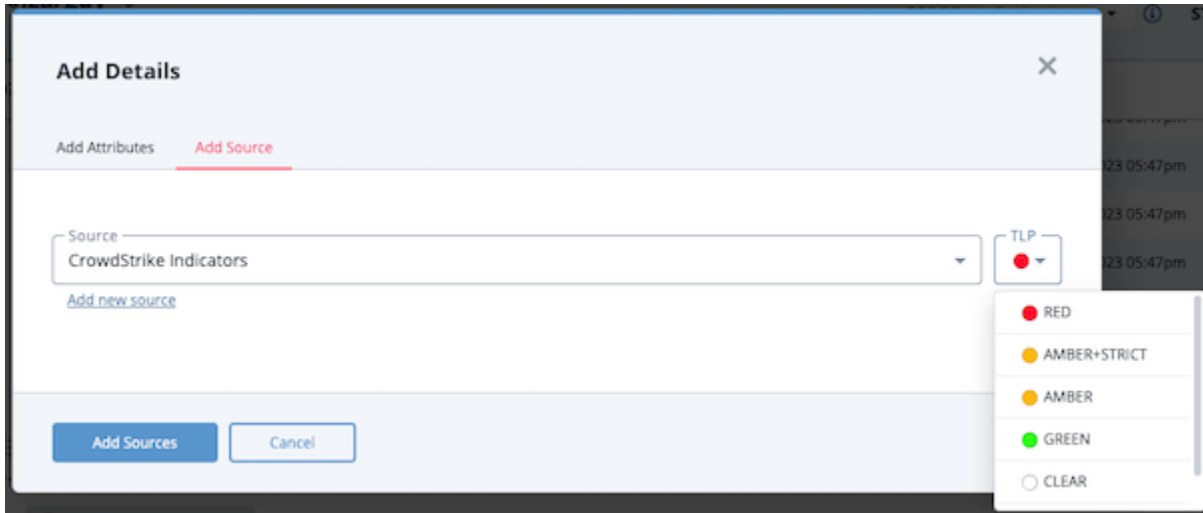
The Add Assets window is displayed.



2. Enter the asset name.

3. Enter a description of the asset.
4. Select a **Source** from the dropdown provided.

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



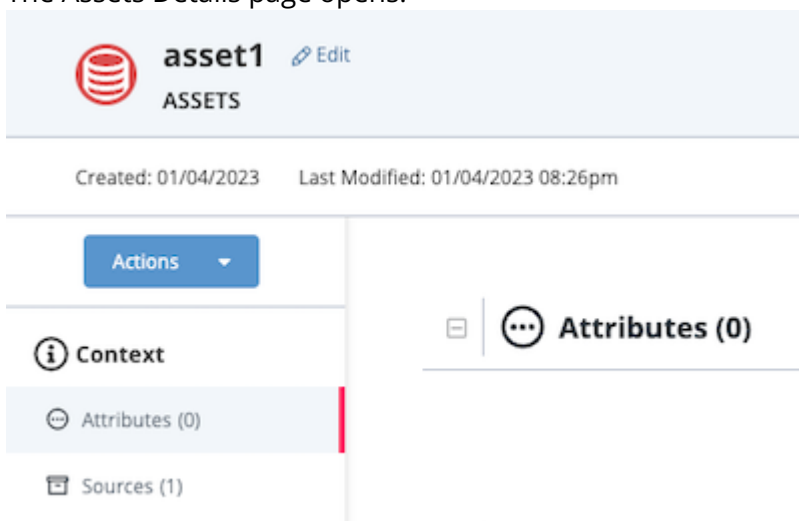
5. Select any **Related Objects** you need to link to the asset. This field is optional.
6. Click **Add Assets**.

Adding Context

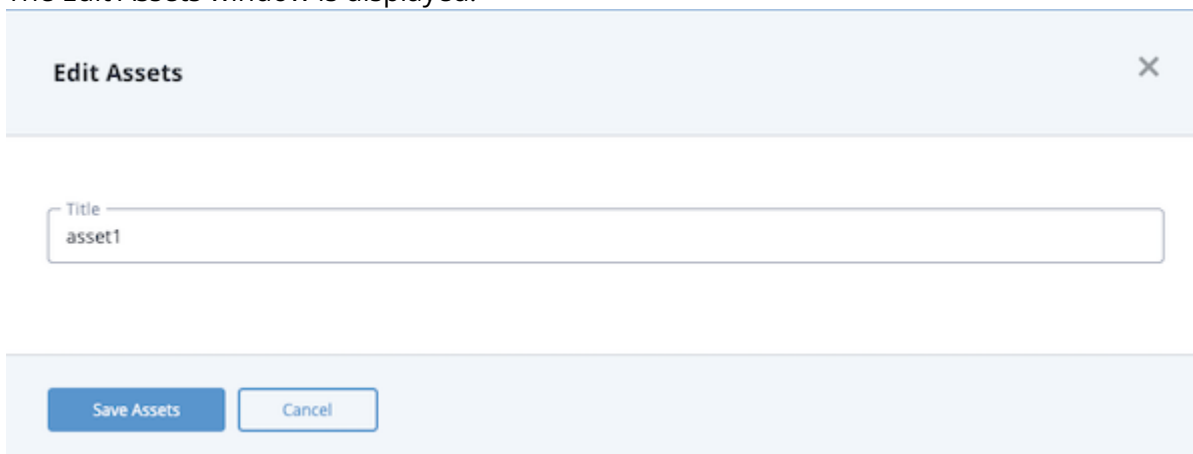
See the [About Object Details](#) section and its topics for details on adding context to an object such as adding sources, attributes, and related objects.

Editing Assets

1. Locate and click the assets object.
The Assets Details page opens.



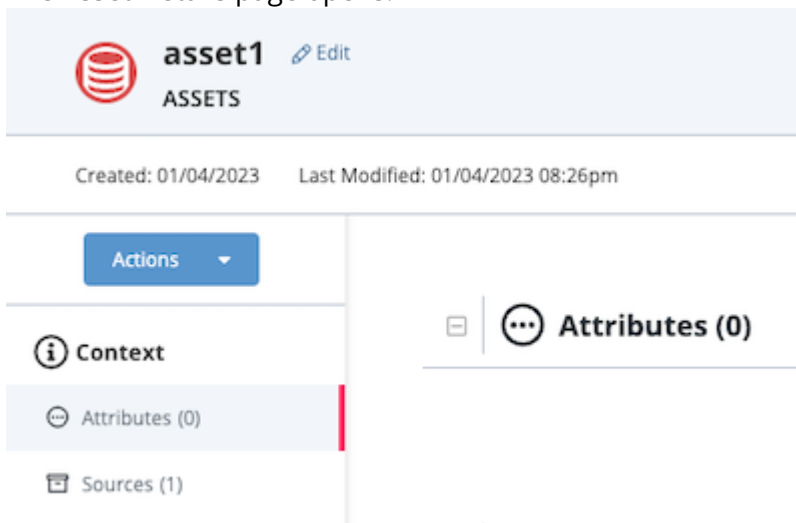
2. Click the **Edit** option next to the Assets object name.
The Edit Assets window is displayed.



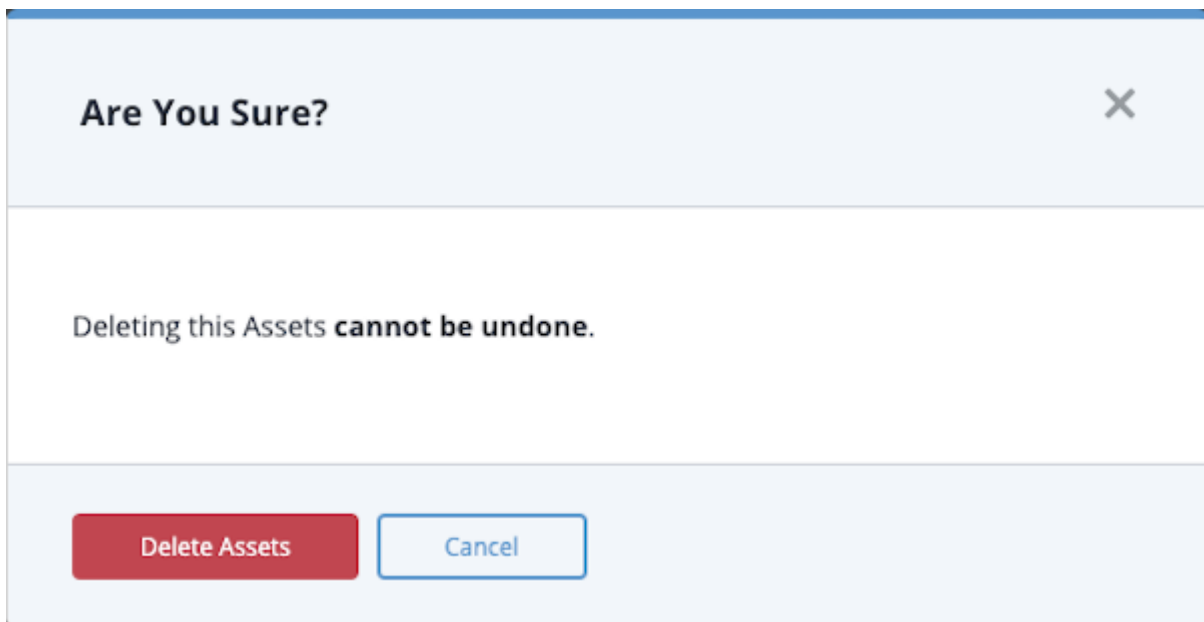
3. Make the desired change to the Adversary name.
4. Click the **Save Assets** button.

Deleting Assets

1. Locate and click the assets object.
The Asset Details page opens.



2. Click on the **Actions** menu and select **Delete Assets**.
The Are You Sure window prompts you confirm the deletion.



3. Click the **Delete Assets** button.

Attack Patterns

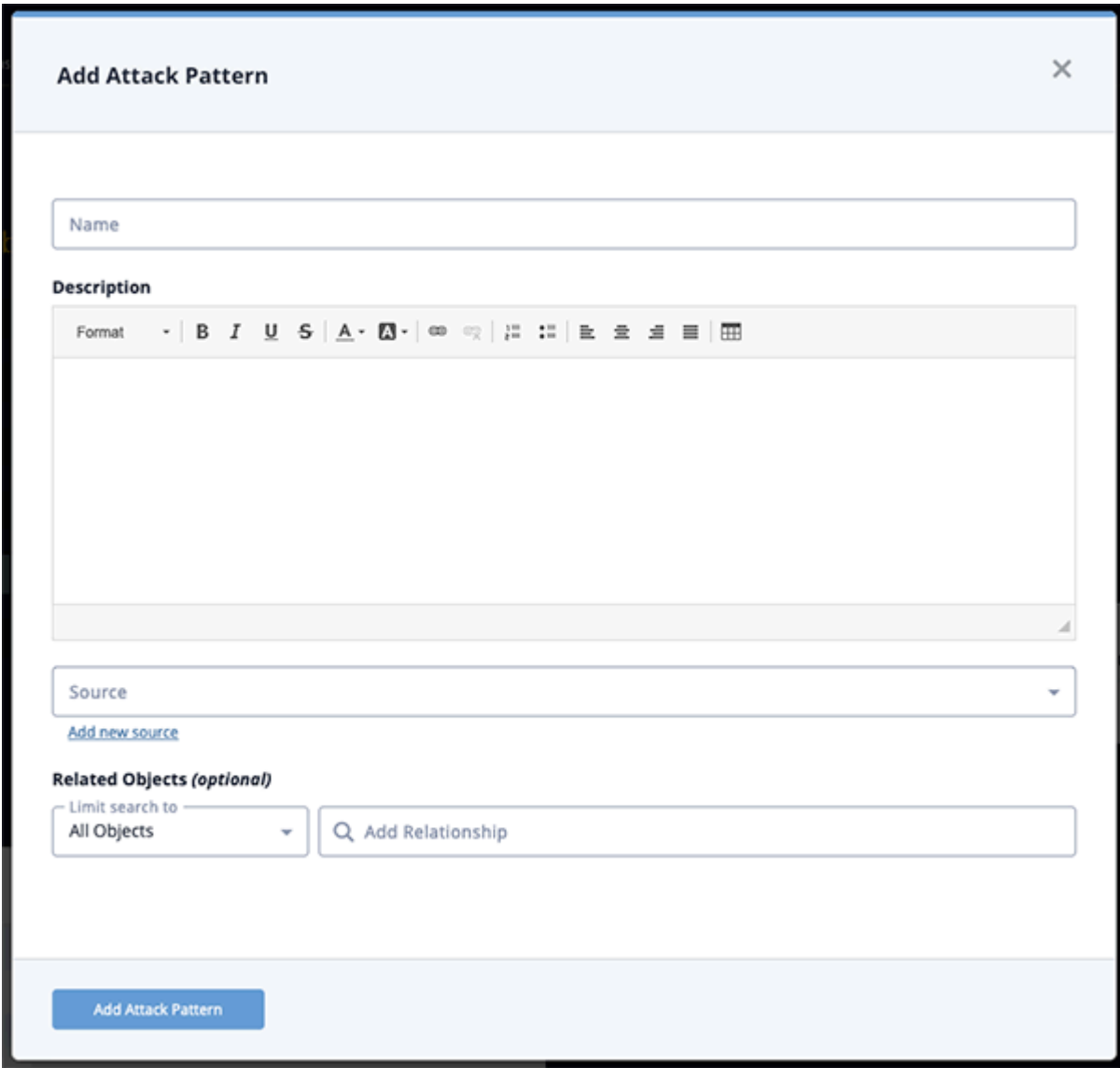
Attack Pattern are descriptions of methods used to exploit software.

Use the steps below to create, edit and delete an Attack Pattern.

Adding an Attack Patterns

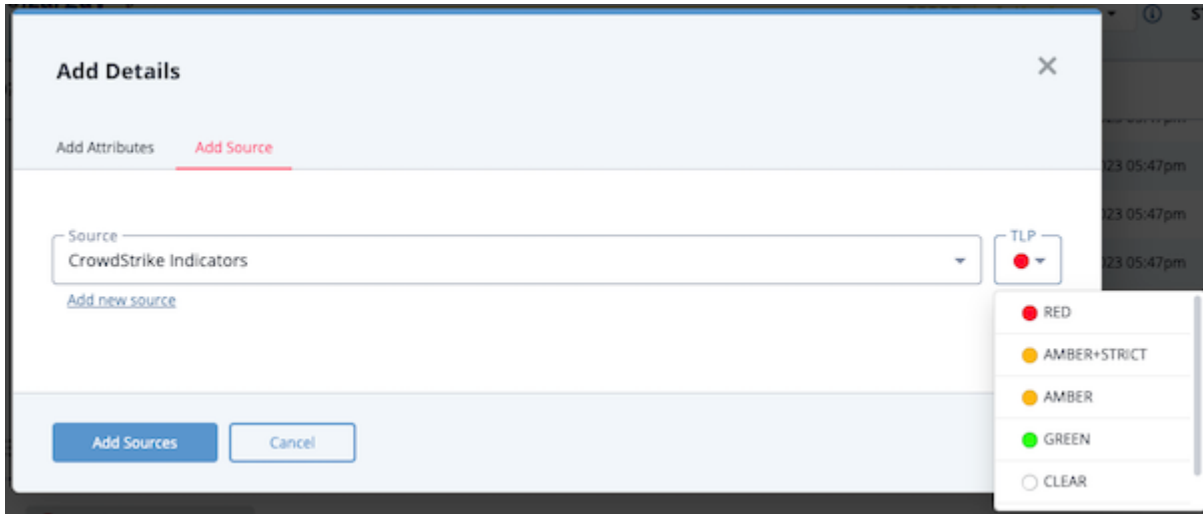
1. Go to **Create > Attack Pattern**.

The Add Attack Pattern dialog box opens.



2. Enter a name.
3. Enter a description in the field provided.
4. Select a **Source** from the dropdown provided.

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



5. Select any **Related Objects** you need to link to the Attack Pattern. This field is optional.
6. Click **Add Attack Pattern**.

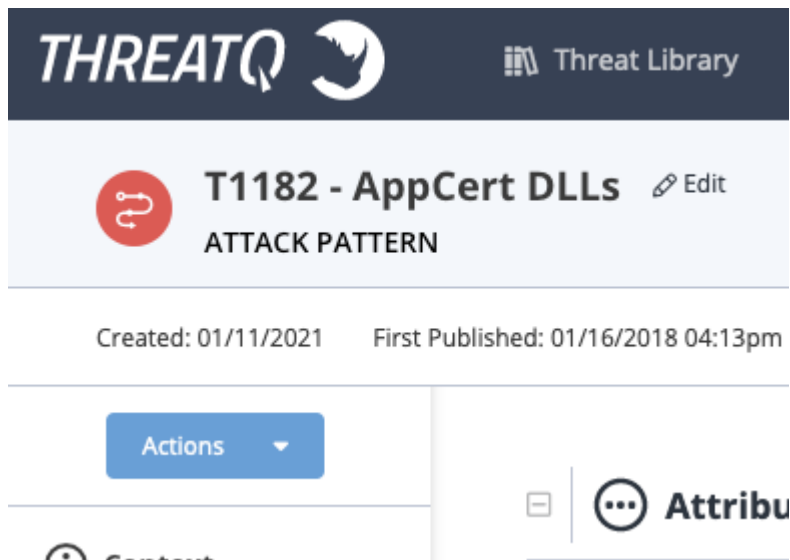
Adding Context

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

Editing an Attack Pattern

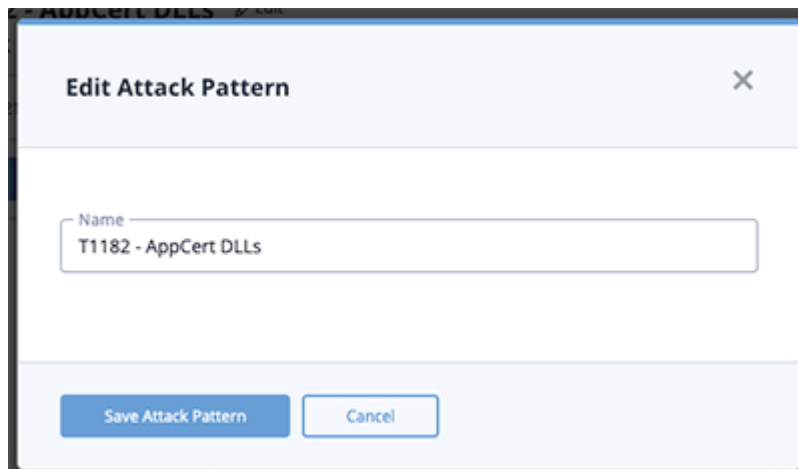
1. Locate and click on the attack pattern.

The Attack Pattern's detail page opens.



2. Click on **Edit** next to the Attack Pattern's name.

The Edit Attack Pattern dialog box opens.

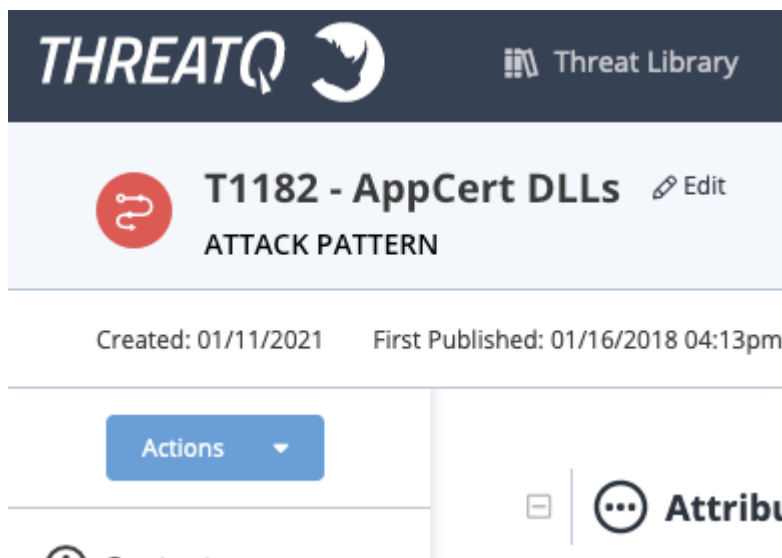


3. Make the desired change to the Attack Pattern name and click **Save Attack Pattern**.

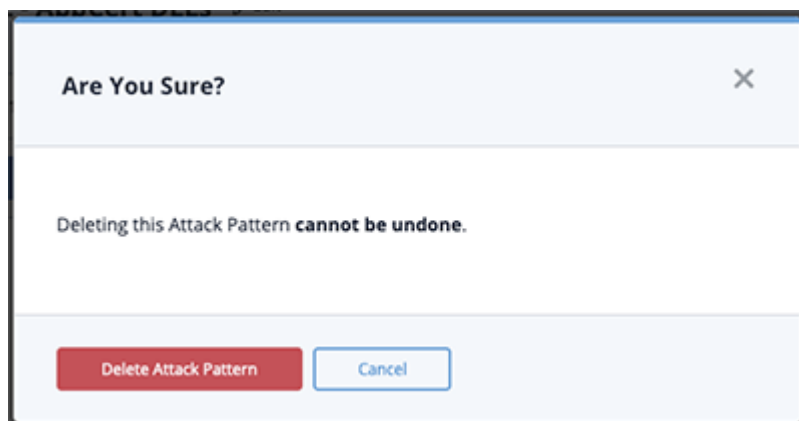
Deleting an Attack Pattern

1. Locate and click on the Attack Pattern.

The Attack Pattern's details page opens.



2. Click on the **Actions** menu and select **Delete Attack Pattern**. A confirmation dialog box appears.



3. Click on **Delete Attack Pattern**.

Campaigns

Campaigns are groups of behaviors that describe malicious activities taken against specific targets over a period of time.

Use the steps below to create, edit and delete a Campaign.

Adding a Campaign

1. Go to **Create > Campaign**.

The Add Campaign dialog box opens.

Add Campaign

Name

Description

Format

B
I
U
S
A
A

Objective

Format

B
I
U
S
A
A

First Seen

January

21

2021

Time

08:34 PM

Time Zone

UTC

Last Seen

January

21

2021

Time

08:34 PM

Time Zone

UTC

Source

Add new source

Related Objects (optional)

Limit search to

All Objects

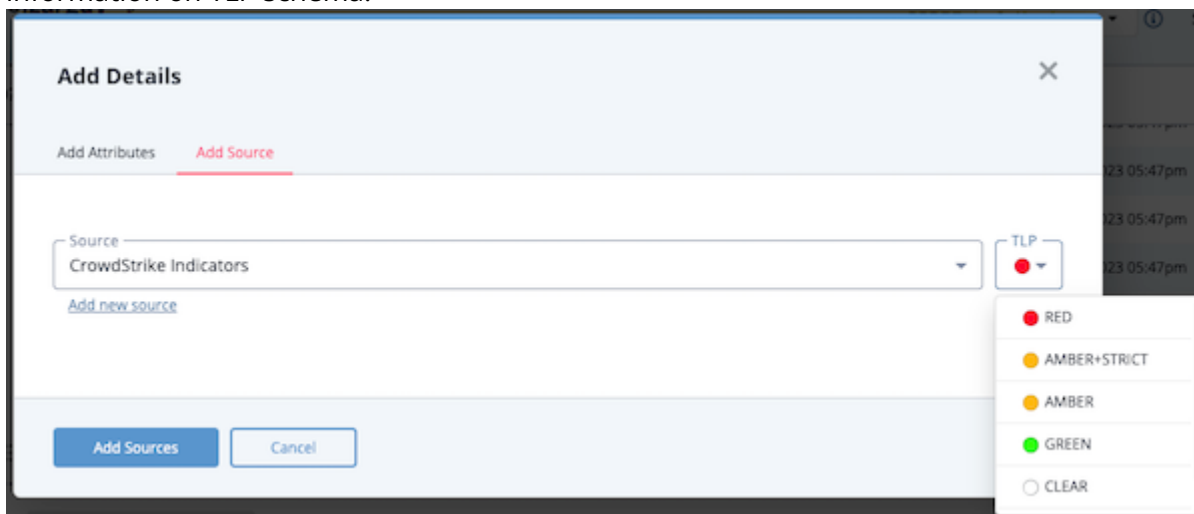
Add Relationship

Add Campaign

2. Enter a **Name**.

3. Enter a **Description** in the field provided.
4. Enter an **Objective**.
5. Select the **First Seen** and **Last Scene** times.
6. Select a **Source** from the dropdown provided.

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



7. Select any **Related Objects** you need to link to the Campaign. This field is optional.
8. Click **Add Campaign**.

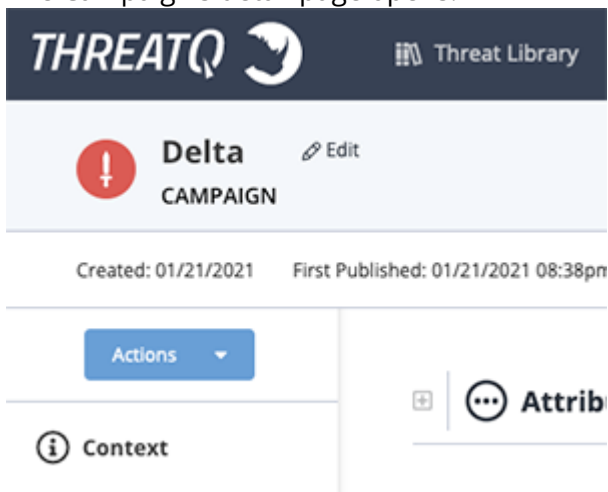
Adding Context

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

Editing a Campaign

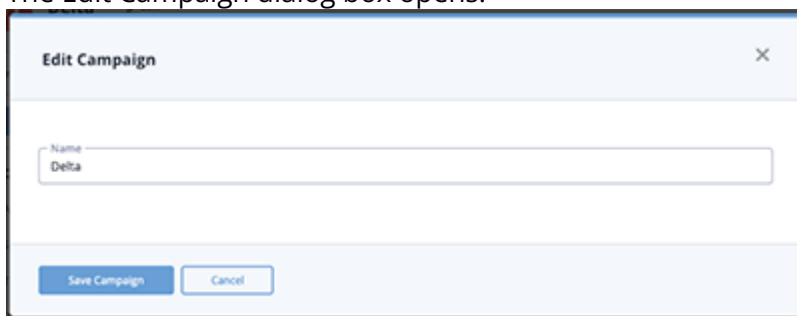
1. Locate and click on the Campaign.

The Campaign's detail page opens.



2. Click on **Edit** next to the Campaign's name.

The Edit Campaign dialog box opens.

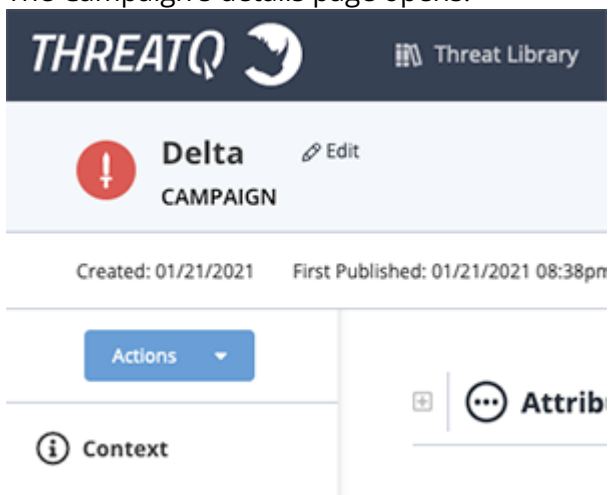


3. Make the desired change to the Campaign name and click **Save Campaign**.

Deleting a Campaign

1. Locate and click on the Campaign.

The Campaign's details page opens.



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

A confirmation dialog box appears.



3. Click on **Delete Campaign**.

Courses of Action

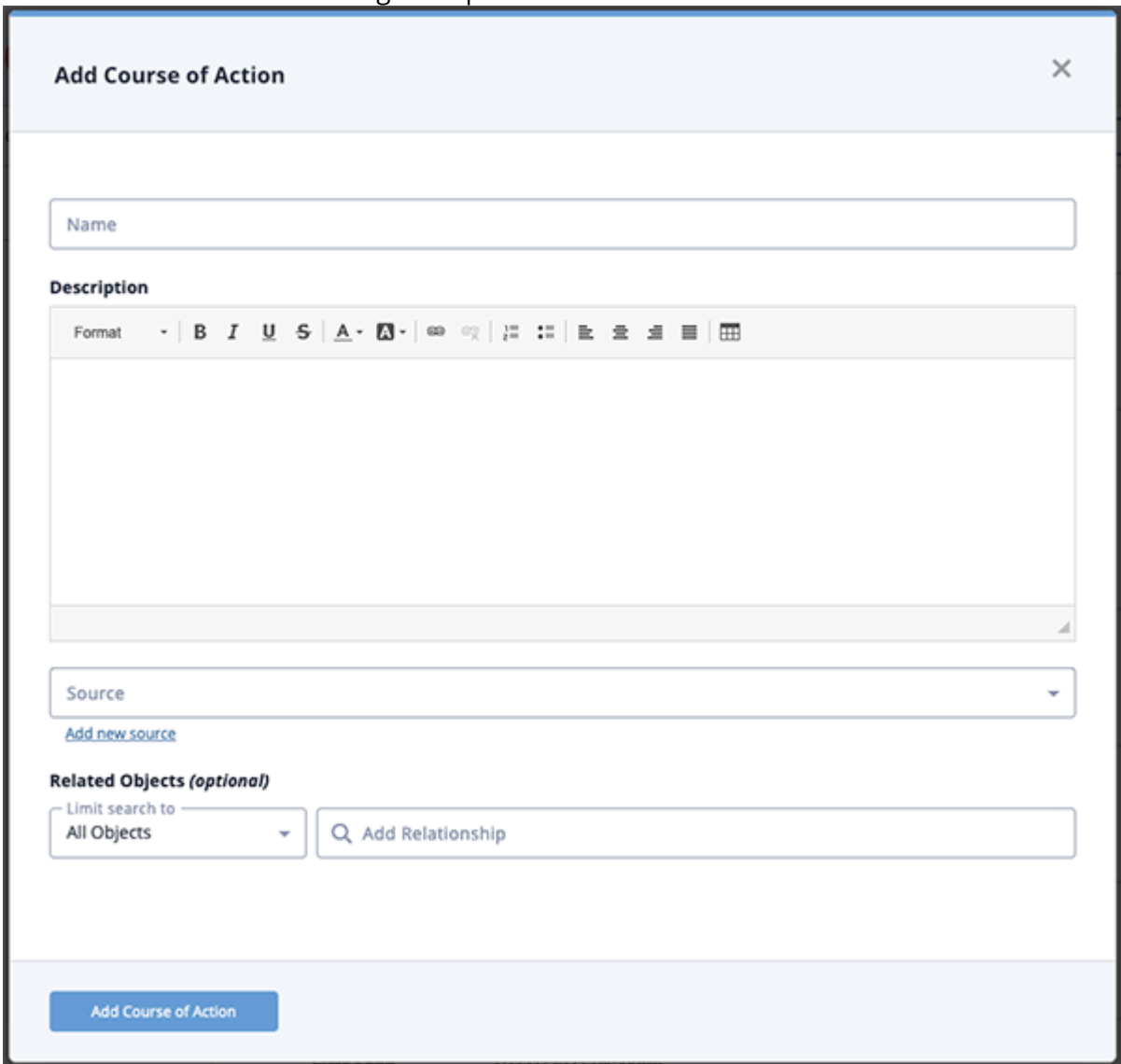
Courses of Action are a combination of risk response measures taken to address or prevent malicious attacks.

Use the steps below to create, edit and delete a Course of Action.

Adding a Course of Action

1. Go to **Create > Course of Action**.

The Add Course of Action dialog box opens.



2. Enter a **Name**.
3. Enter a **Description** in the field provided.
4. Select a **Source** from the dropdown provided.

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

5. Select any **Related Objects** you need to link to the Course of Action. This field is optional.
6. Click **Add Course of Action**.

Adding Context

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

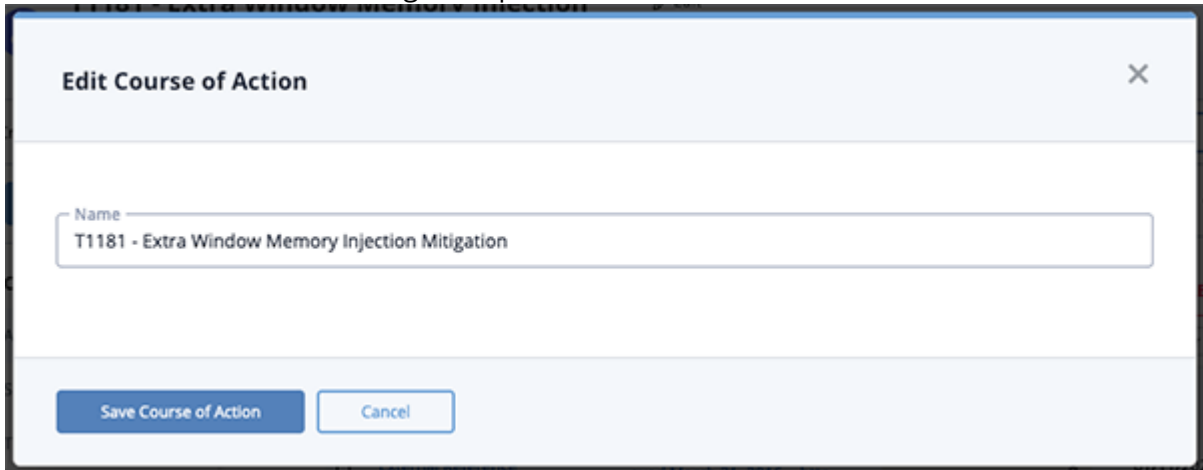
Editing a Course of Action

1. Locate and click on the Course of Action.

The Course of Action's detail page opens.

2. Click on **Edit** next to the Course of Action's name.

The Edit Course of Action dialog box opens.



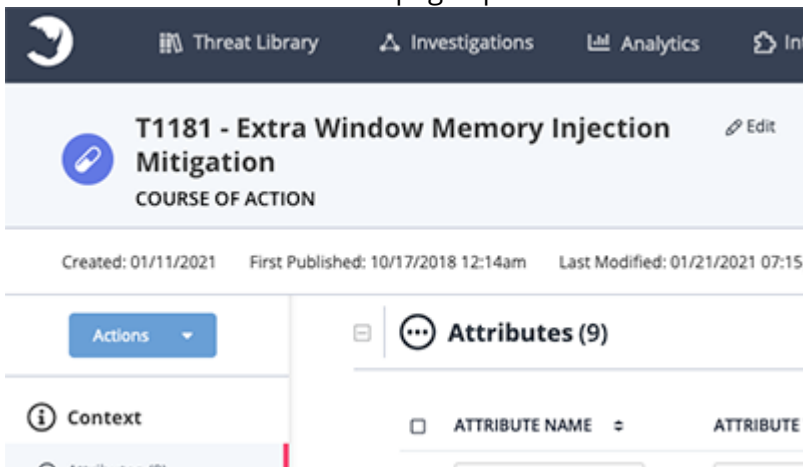
The dialog box titled "Edit Course of Action" has a close button (X) in the top right corner. It contains a text input field labeled "Name" with the text "T1181 - Extra Window Memory Injection Mitigation". At the bottom, there are two buttons: "Save Course of Action" and "Cancel".

3. Make the desired change to the Course of Action's name and click **Save Course of Action**.

Deleting a Course of Action

1. Locate and click on the Course of Action.

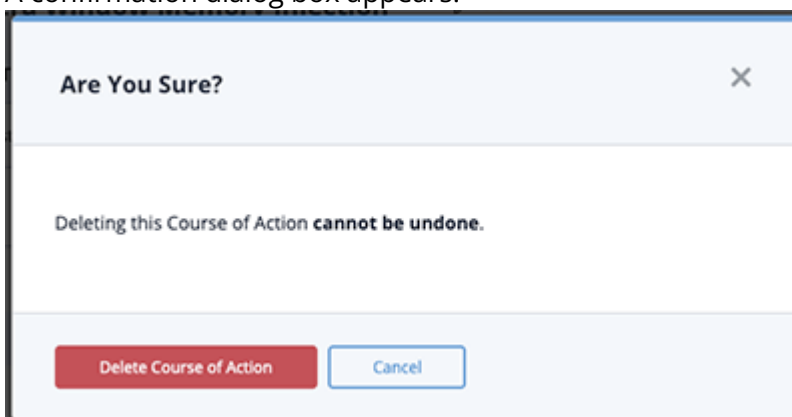
The Course of Action's details page opens.



The details page for the Course of Action "T1181 - Extra Window Memory Injection Mitigation" is shown. It includes a header with navigation links (Threat Library, Investigations, Analytics, Int) and an "Edit" button. Below the header, it shows the course name, a "COURSE OF ACTION" label, and metadata: "Created: 01/11/2021", "First Published: 10/17/2018 12:14am", and "Last Modified: 01/21/2021 07:15". A sidebar on the left has an "Actions" menu and a "Context" section. The main content area shows "Attributes (9)" with a table header "ATTRIBUTE NAME" and "ATTRIBUTE".

2. Click on the **Actions** menu and select **Delete Course of Action**.

A confirmation dialog box appears.



The confirmation dialog box titled "Are You Sure?" has a close button (X) in the top right corner. It contains the text "Deleting this Course of Action cannot be undone." At the bottom, there are two buttons: "Delete Course of Action" and "Cancel".

3. Click on **Delete Course of Action**.

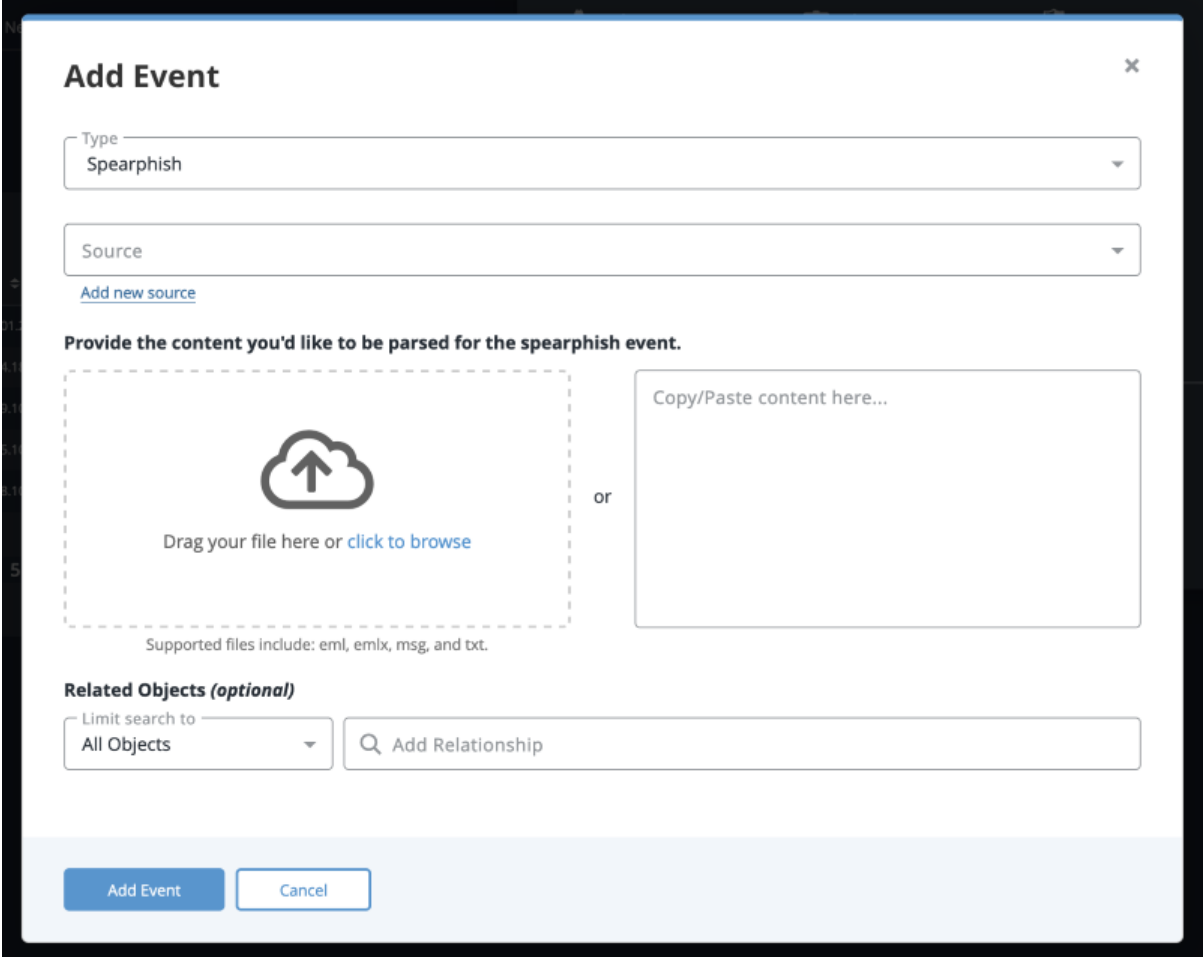
Events

Events are objects that focus on temporal incidents that have significant security impact. Use the steps below to create, edit and delete an Event.

Adding Events

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

The Add Event dialog box opens.



Add Event [Close]

Type: Spearphish [Dropdown]

Source: [Dropdown]

[Add new source](#)

Provide the content you'd like to be parsed for the spearphish event.

Drag your file here or [click to browse](#) or Copy/Paste content here...

Supported files include: eml, emlx, msg, and txt.

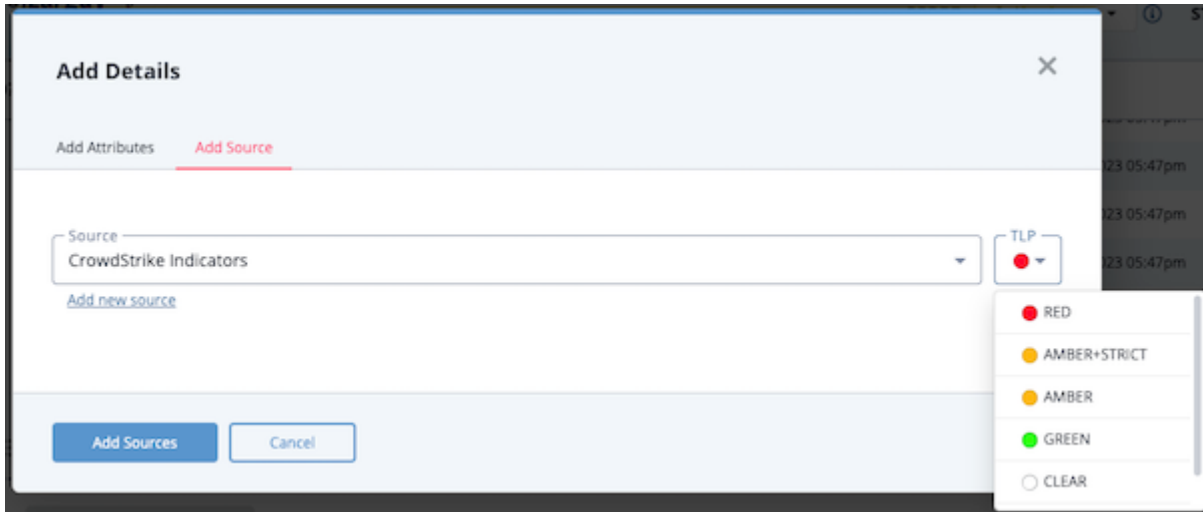
Related Objects (optional)

Limit search to: All Objects [Dropdown] [Search] Add Relationship

Add Event Cancel

2. Select the **Event Type**.
3. Select a **Source** from the dropdown list provided.
You can also click the **Add a New Source** option if the desired source is not listed in the dropdown list. If administrators have enabled TLP view settings, you can select a TLP label for the new source in the dropdown list provided. See the Traffic Light Protocol (TLP) topic for more

information on TLP schema.



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

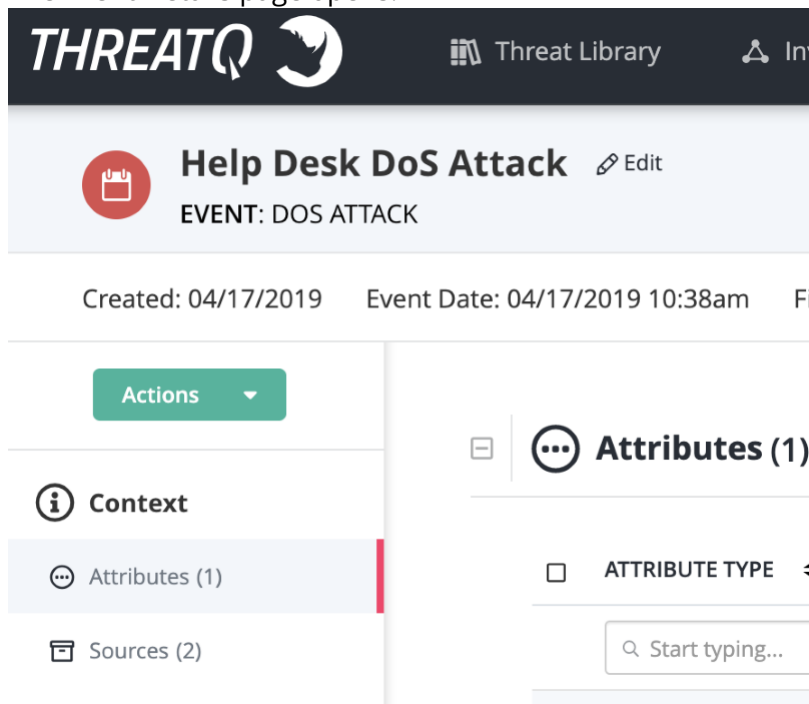
See the [About Object Details](#) section and its topics for details on adding context to an object such as adding sources, attributes, and related objects.

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.

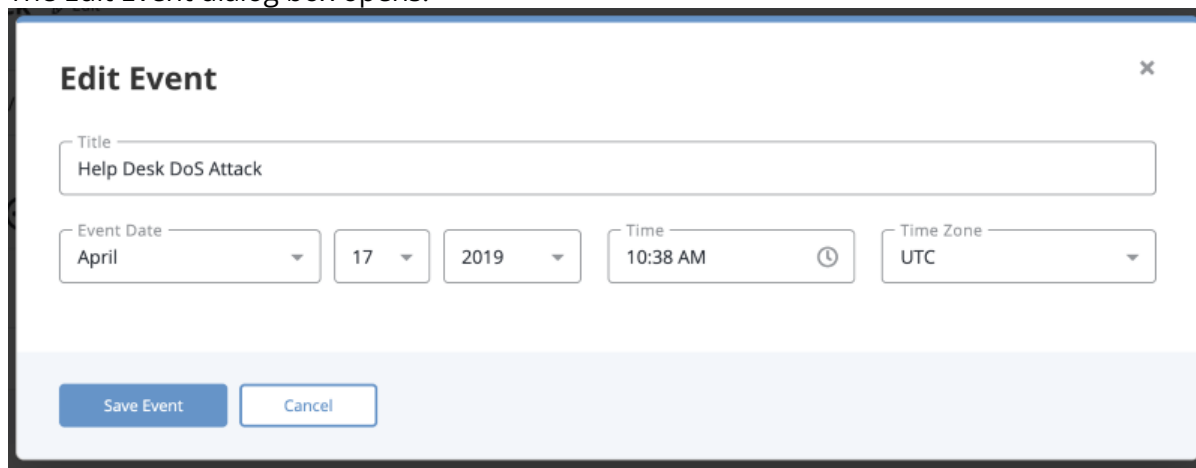
The Event Details page opens.



The screenshot shows the ThreatQ interface. At the top, there's a dark header with the ThreatQ logo, a 'Threat Library' link, 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 the title, 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', 'Attributes (1)', and 'Sources (2)'. The main area shows 'Attributes (1)' with a search bar and a table header 'ATTRIBUTE TYPE'.

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

The Edit Event dialog box opens.



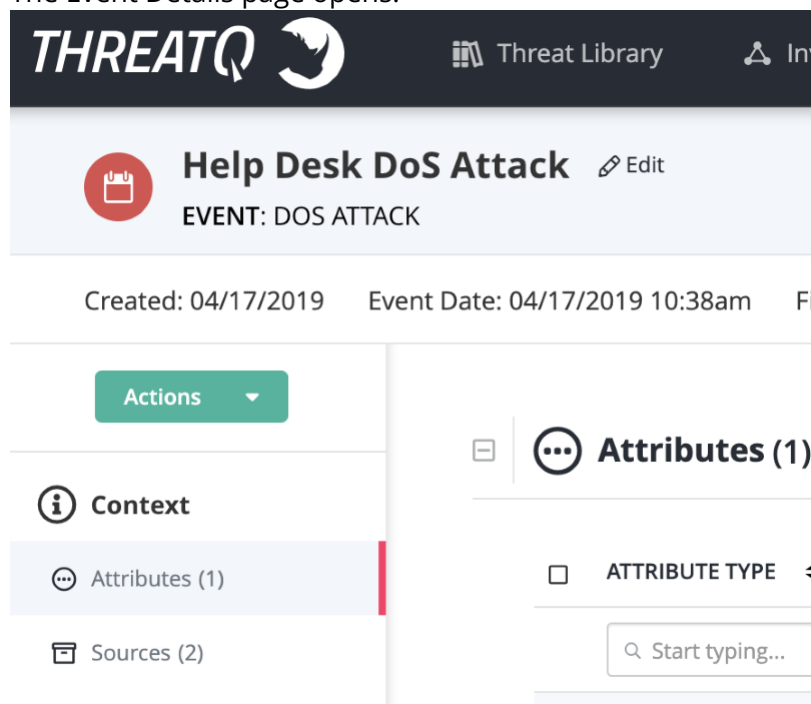
The 'Edit Event' dialog box is shown. It has a title 'Edit Event' and a close button. The 'Title' field contains 'Help Desk DoS Attack'. Below it, the 'Event Date' is set to 'April 17, 2019' and the 'Time' is '10:38 AM'. The 'Time Zone' is set to 'UTC'. At the bottom, there are 'Save Event' and 'Cancel' buttons.

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

Deleting Events

- Locate and click the event.
The Events Details page opens.

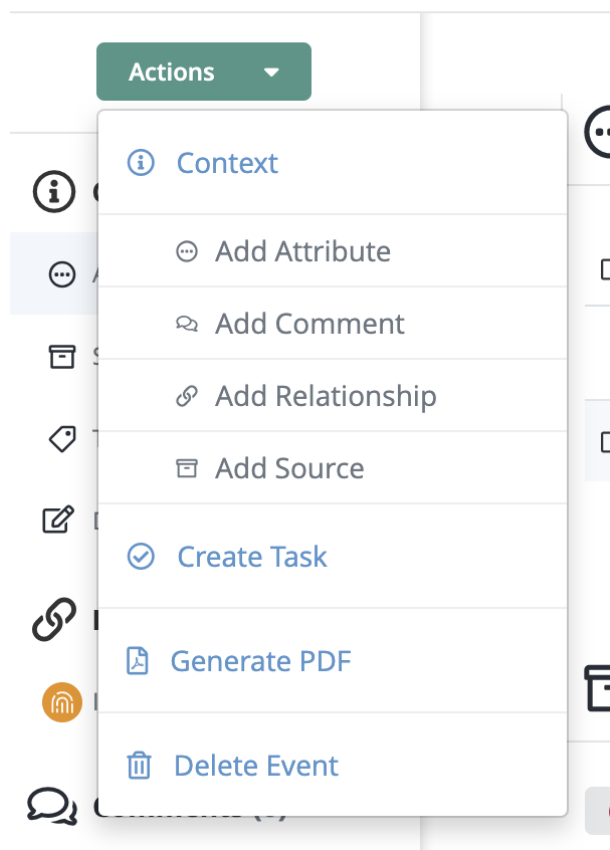
The Event Details page opens.



The screenshot shows the ThreatQ interface for an event titled "Help Desk DoS Attack". The event is categorized as "EVENT: DOS ATTACK". It was created on 04/17/2019 and has an event date of 04/17/2019 10:38am. The interface includes a sidebar with "Context", "Attributes (1)", and "Sources (2)". The main area shows "Attributes (1)" with a search bar labeled "Start typing...".

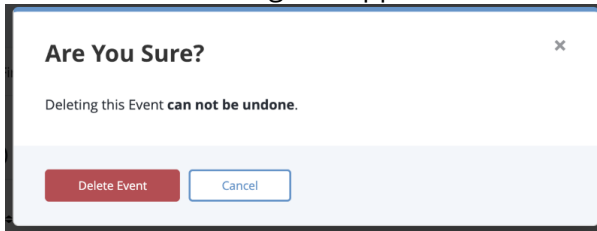
- Click on the **Actions** menu and select **Delete Event**.

Created: 04/17/2019 Event Date: 04/1



The screenshot shows the "Actions" menu open, displaying a list of options: Context, Add Attribute, Add Comment, Add Relationship, Add Source, Create Task, Generate PDF, and Delete Event. The "Delete Event" option is highlighted at the bottom of the list.

A confirmation dialog box appears.



3. Click on **Delete Event**.

Files

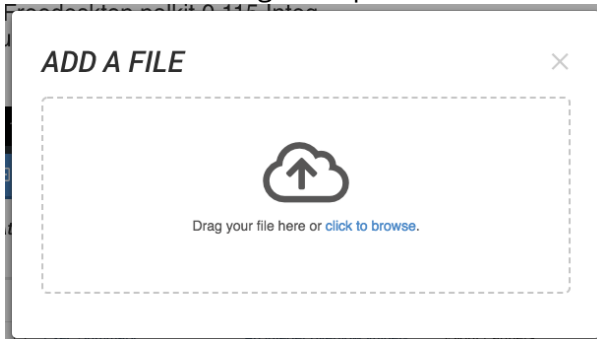
Files are received from various intelligence providers and may contain technical cybersecurity data such as Indicator , Adversary , and Malware samples.

Use the steps below to create, edit and delete a File.

Adding Files

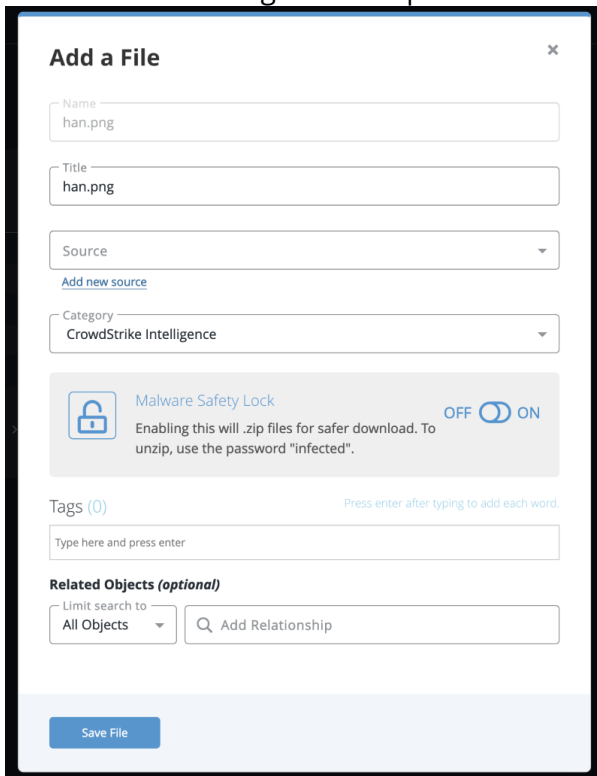
1. Click **Create > File**.

The Add a File dialog box opens.



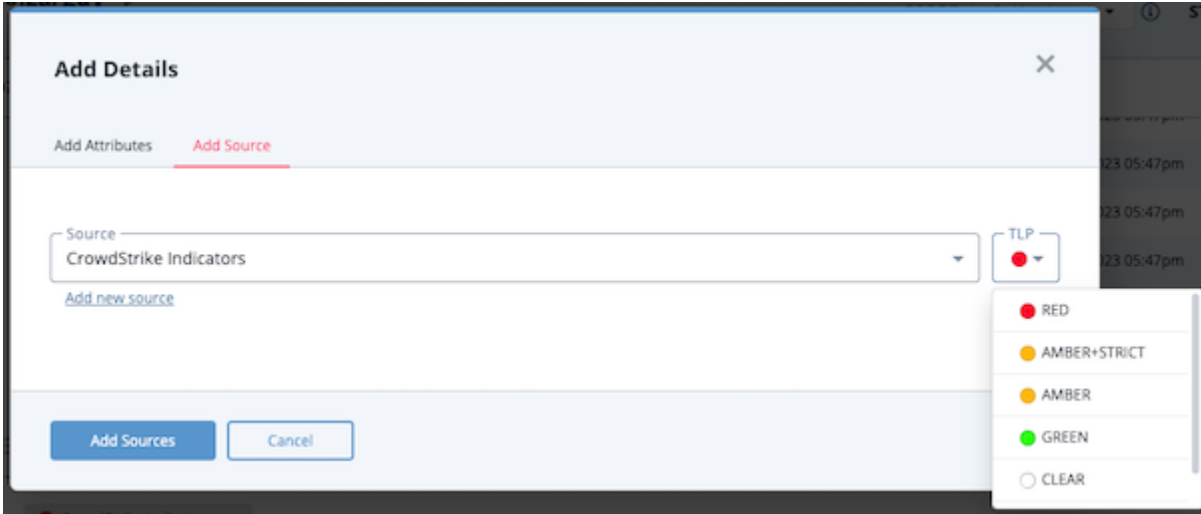
2. Drag the file into the dialog box or browse and locate the file.

The Add a File Dialog box will update.



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

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



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**.

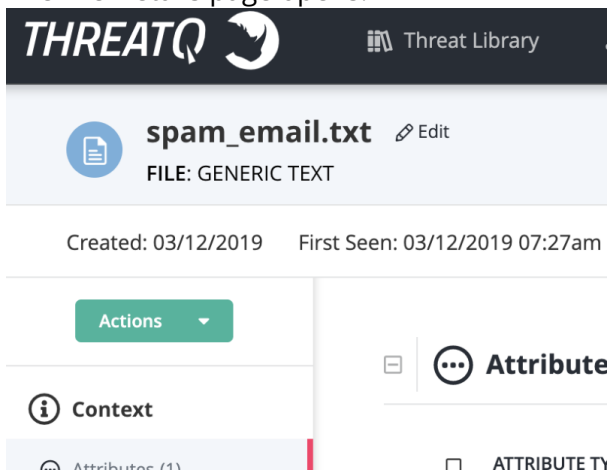
Adding Context

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

Editing Files

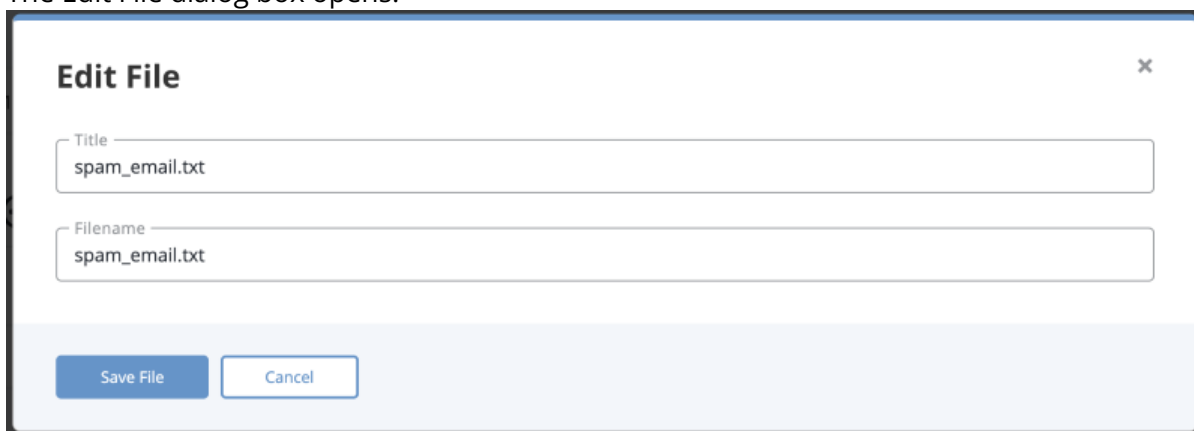
1. Locate and click on the file.

The File Details page opens.



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

The Edit File dialog box opens.

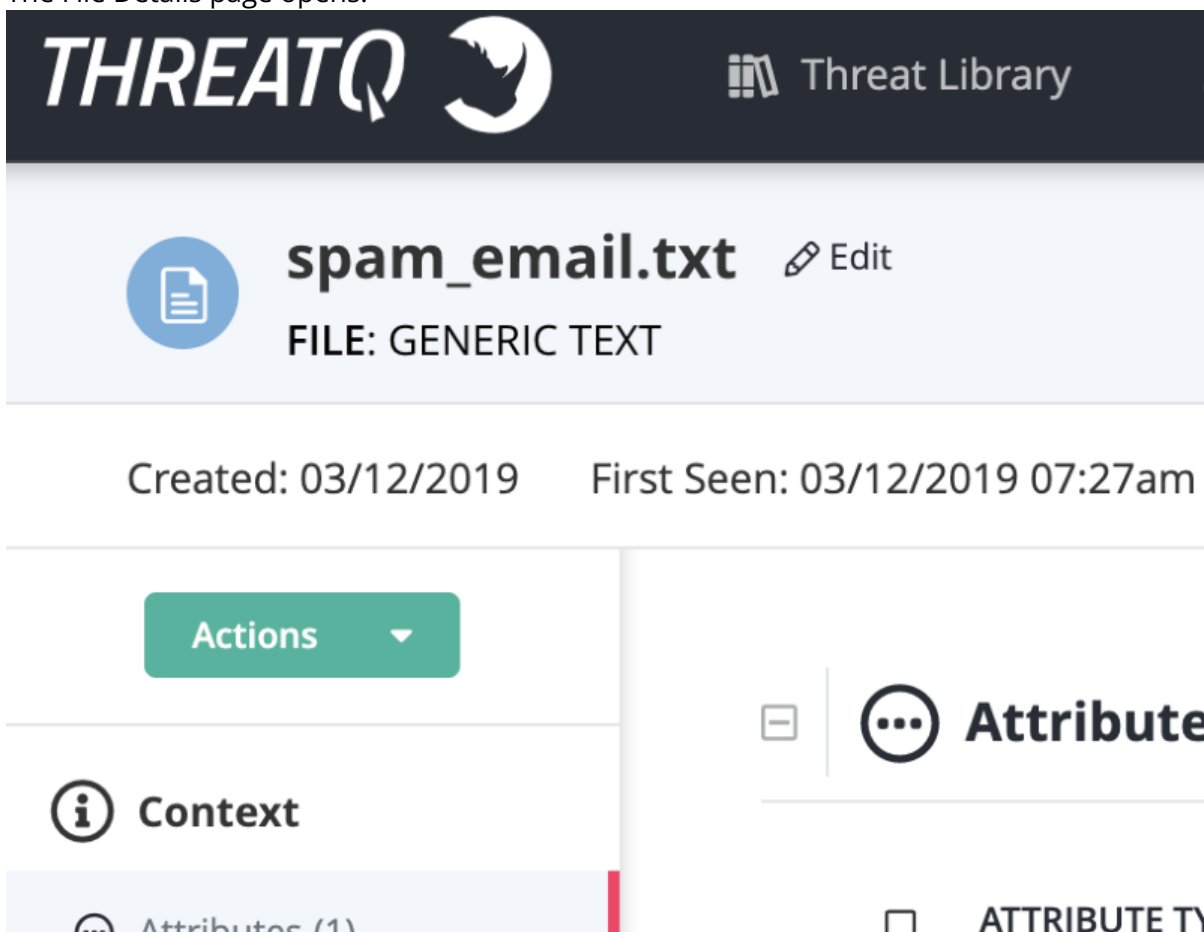


3. Make the desired change to the File Name.
4. Click on **Save File**.

Deleting Files

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, the file 'spam_email.txt' is displayed with a document icon and an 'Edit' button. The file type is listed as 'FILE: GENERIC TEXT'. Below the file name, the creation and first seen dates are shown: 'Created: 03/12/2019' and 'First Seen: 03/12/2019 07:27am'. On the left side, there is a sidebar with an 'Actions' button and a 'Context' section. The 'Context' section shows 'Attributes (1)'. On the right side, there is an 'Attribute' section with a minus icon and a plus icon. Below the 'Attribute' section, there is a checkbox and the text 'ATTRIBUTE TY'.

THREATQ Threat Library

 **spam_email.txt**  Edit

FILE: GENERIC TEXT

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

Actions

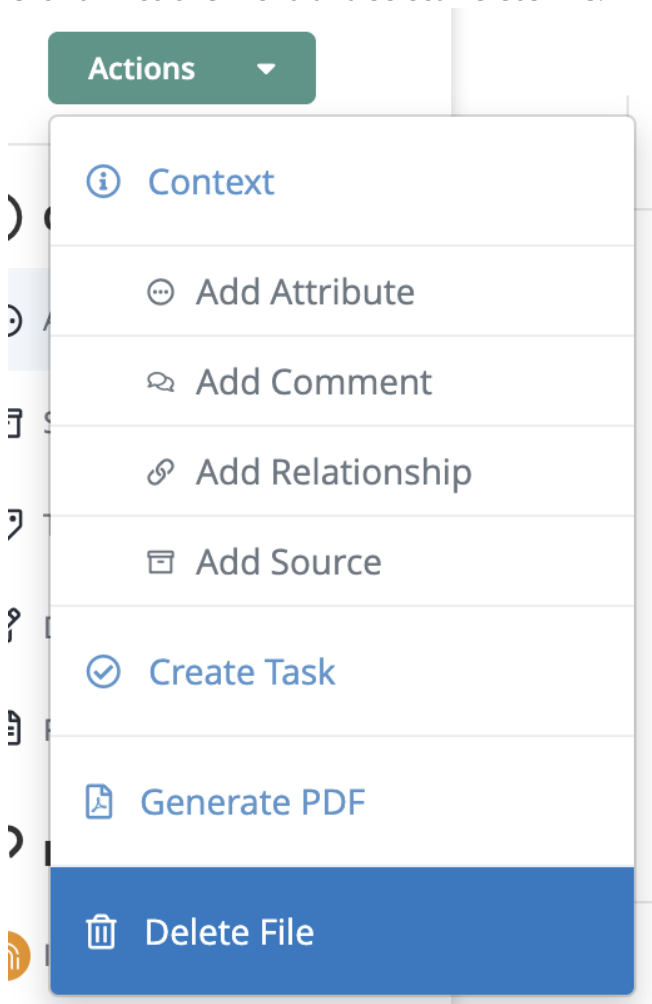
 **Context**

 Attributes (1)

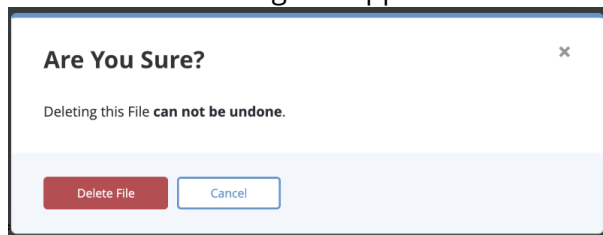
  **Attribute**

☐ ATTRIBUTE TY

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



A confirmation dialog box appears.



- Click on **Delete File**.

Identities

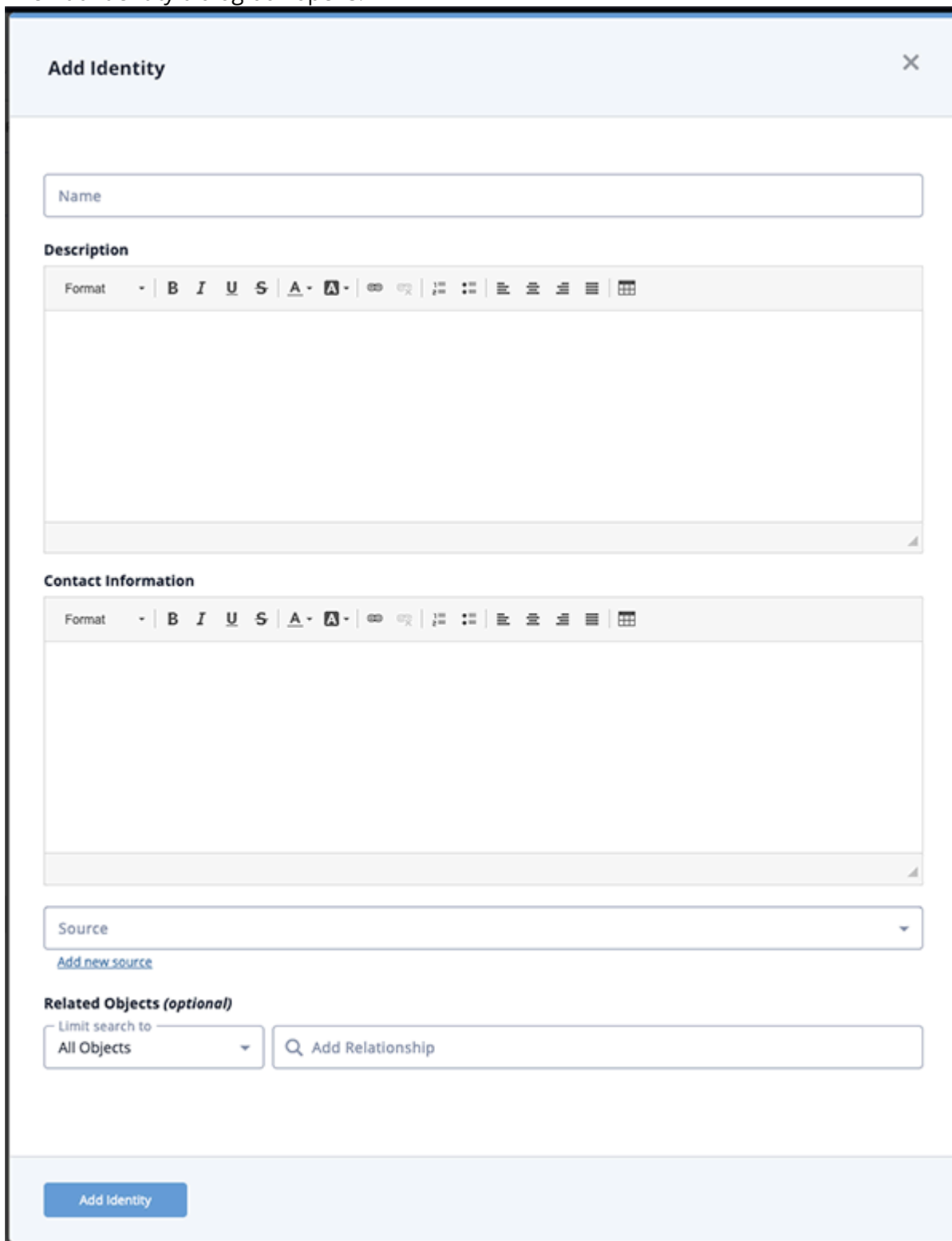
Identity contain basic identifying information for targeted groups such as information sources, threat actor identities, and targets of attack.

Use the steps below to create, edit and delete an Identity.

Adding an Identity

1. Go to **Create > Identity**.

The Add Identity dialog box opens.



Add Identity [Close]

Name

Description

Format [Dropdown] | **B** **I** **U** **S** | **A** [Dropdown] **A** [Dropdown] | [Link] [Image] | [List] [List] [List] [List] [List] [List]

Contact Information

Format [Dropdown] | **B** **I** **U** **S** | **A** [Dropdown] **A** [Dropdown] | [Link] [Image] | [List] [List] [List] [List] [List] [List]

Source [Dropdown] [Dropdown Arrow]

[Add new source](#)

Related Objects (optional)

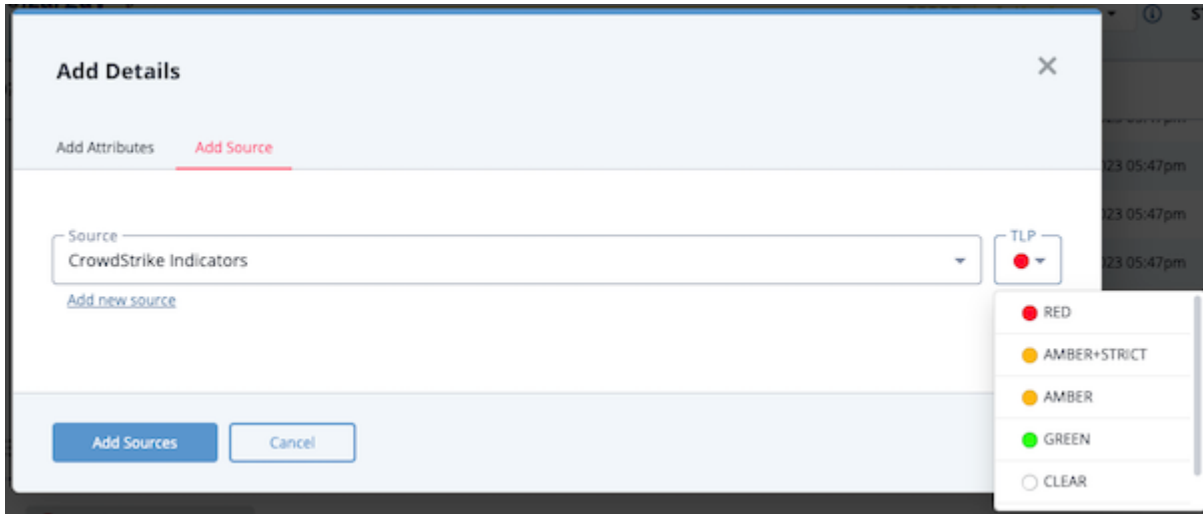
Limit search to [Dropdown] [Dropdown Arrow]

[Search Icon] Add Relationship

Add Identity

2. Enter a **Name**.
3. Enter a **Description** in the field provided.
4. Enter the **Contact Information** in field provided.
5. Select a **Source** from the dropdown provided.

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



6. Select any **Related Objects** you need to link to the Identity. This field is optional.
7. Click **Add Identity**.

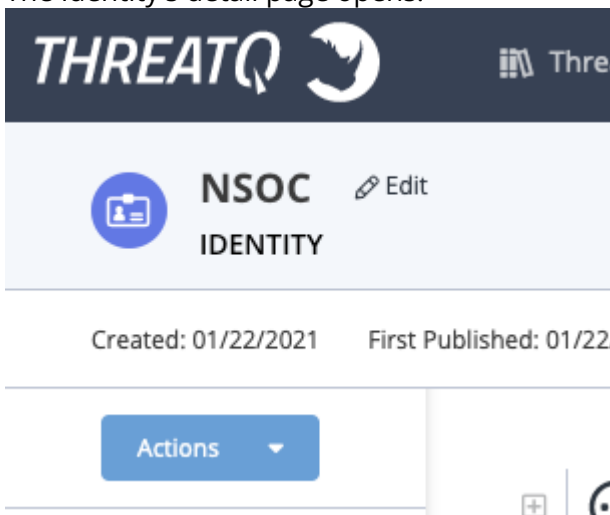
Adding Context

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

Editing an Identity

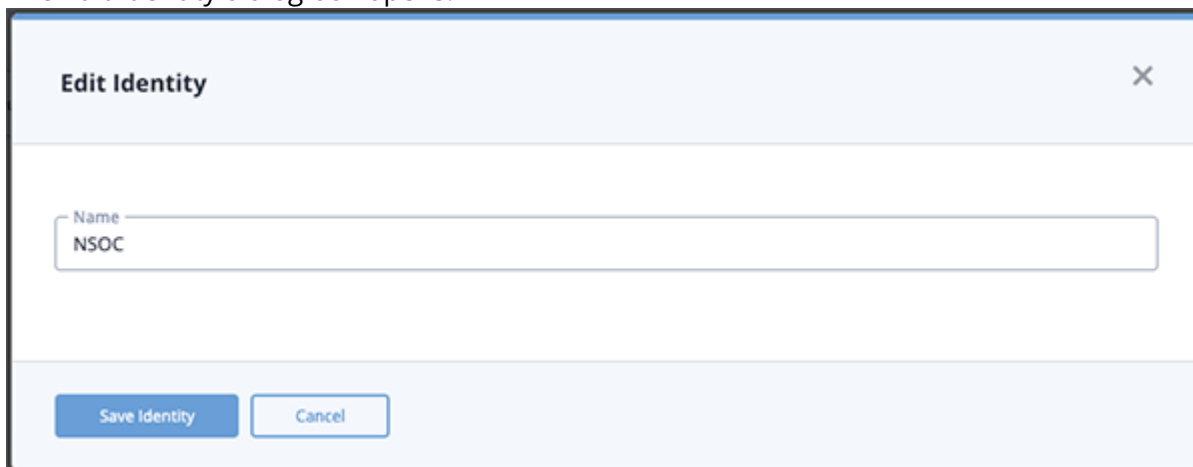
1. Locate and click on the Identity.

The Identity's detail page opens.



2. Click on **Edit** next to the Identity's name.

The Edit Identity dialog box opens.

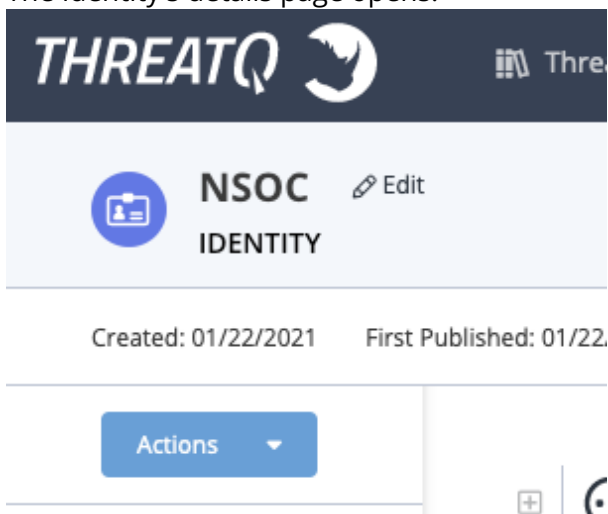
The dialog box is titled "Edit Identity" with a close button (X) in the top right corner. It contains a text input field labeled "Name" with the value "NSOC". At the bottom, there are two buttons: "Save Identity" and "Cancel".

3. Make the desired change to the Identity's name and click **Save Identity**.

Deleting an Identity

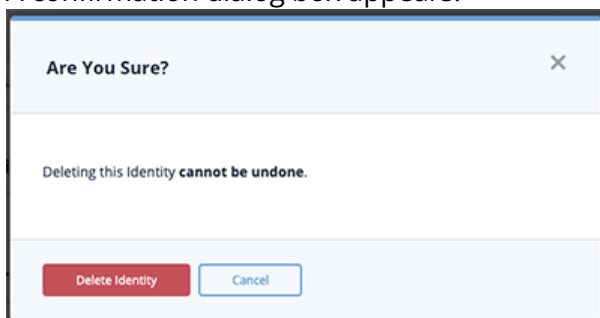
1. Locate and click on the Identity.

The Identity's details page opens.

The page shows the ThreatQ logo and a Twitter icon in the header. Below, there's a section for "NSOC IDENTITY" with an "Edit" button. It also displays "Created: 01/22/2021" and "First Published: 01/22/2021". At the bottom, there's an "Actions" dropdown menu and a plus icon.

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

A confirmation dialog box appears.

The dialog box is titled "Are You Sure?" with a close button (X) in the top right corner. It contains the text "Deleting this Identity cannot be undone." At the bottom, there are two buttons: "Delete Identity" and "Cancel".

3. Click on **Delete Identity**.

Incident are records of any violation of an organization's established security/network policy that may compromise security, integrity, or general access.

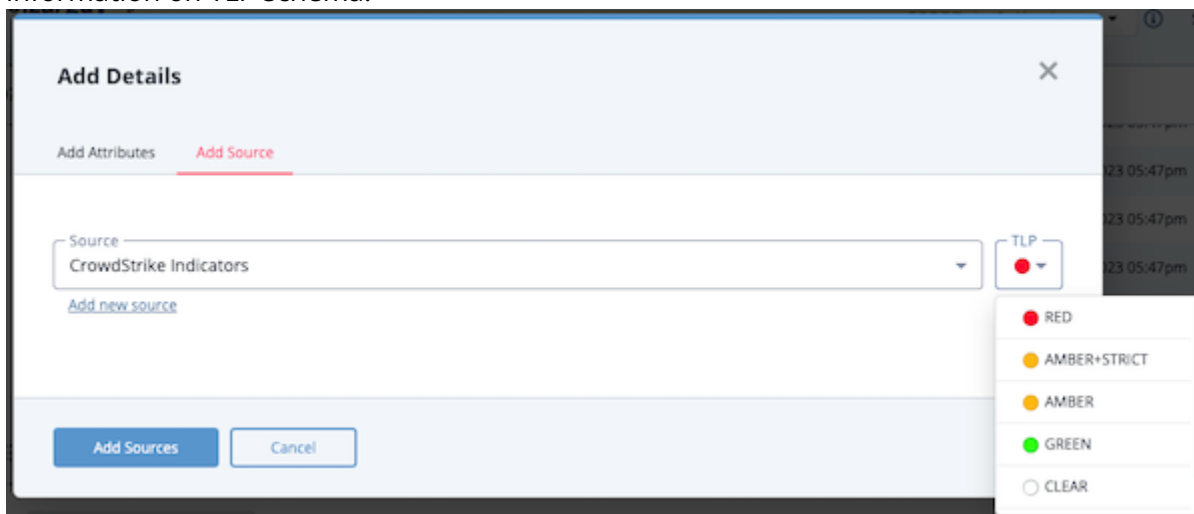
Adding an Incident

- The Add Incident dialog box opens.

ThreatQ User Guide
Version 5.20.0

2. Enter a **Name**.
3. Enter a **Description** in the field provided.
4. Select the **First Seen** and **Last Scene** times.
5. Select a **Source** from the dropdown provided.

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



6. Select any **Related Objects** you need to link to the Incident. This field is optional.
7. Click **Add Incident**.

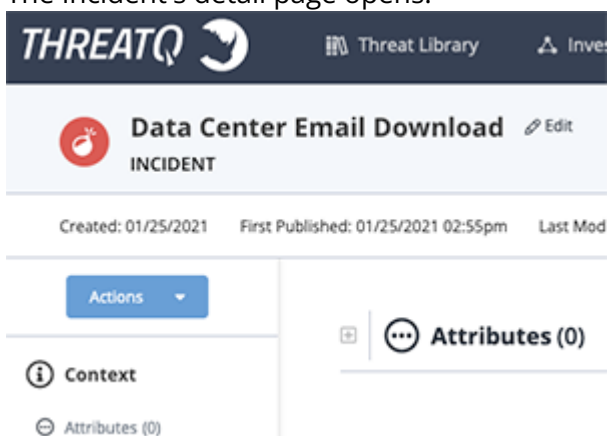
Adding Context

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

Editing an Incident

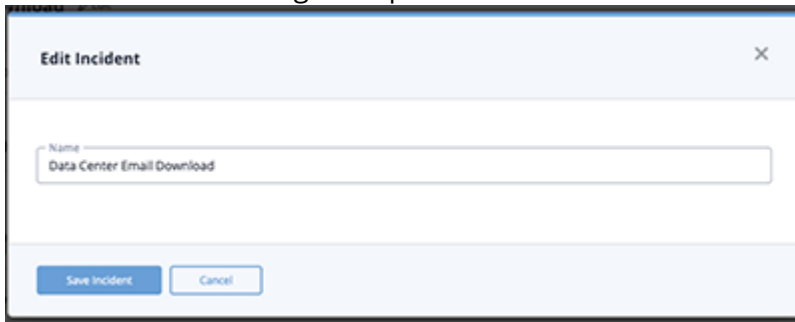
1. Locate and click on the Incident.

The Incident's detail page opens.



2. Click on **Edit** next to the Incident's name.

The Edit Incident dialog box opens.

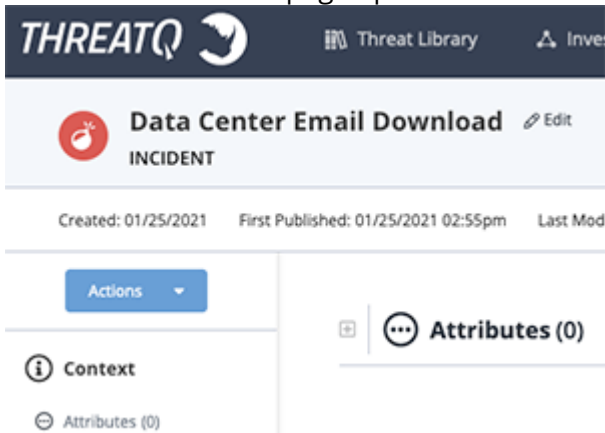


3. Make the desired change to the Incident's name and click **Save Incident**.

Deleting an Incident

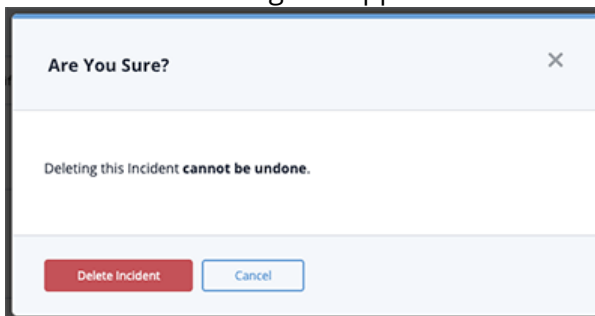
1. Locate and click on the Incident.

The Incident's details page opens.



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

A confirmation dialog box appears.



3. Click on **Delete Incident**.

Indicators

About Indicators

An Indicator is information that describes or identifies methods used to defeat security controls, exploit vulnerabilities, and gain unauthorized access to an internal network. Indicators can also describe malicious reconnaissance to gather technical information, malicious cyber command and control, and any other attribute of cyber security whose disclosure is prohibited by law.

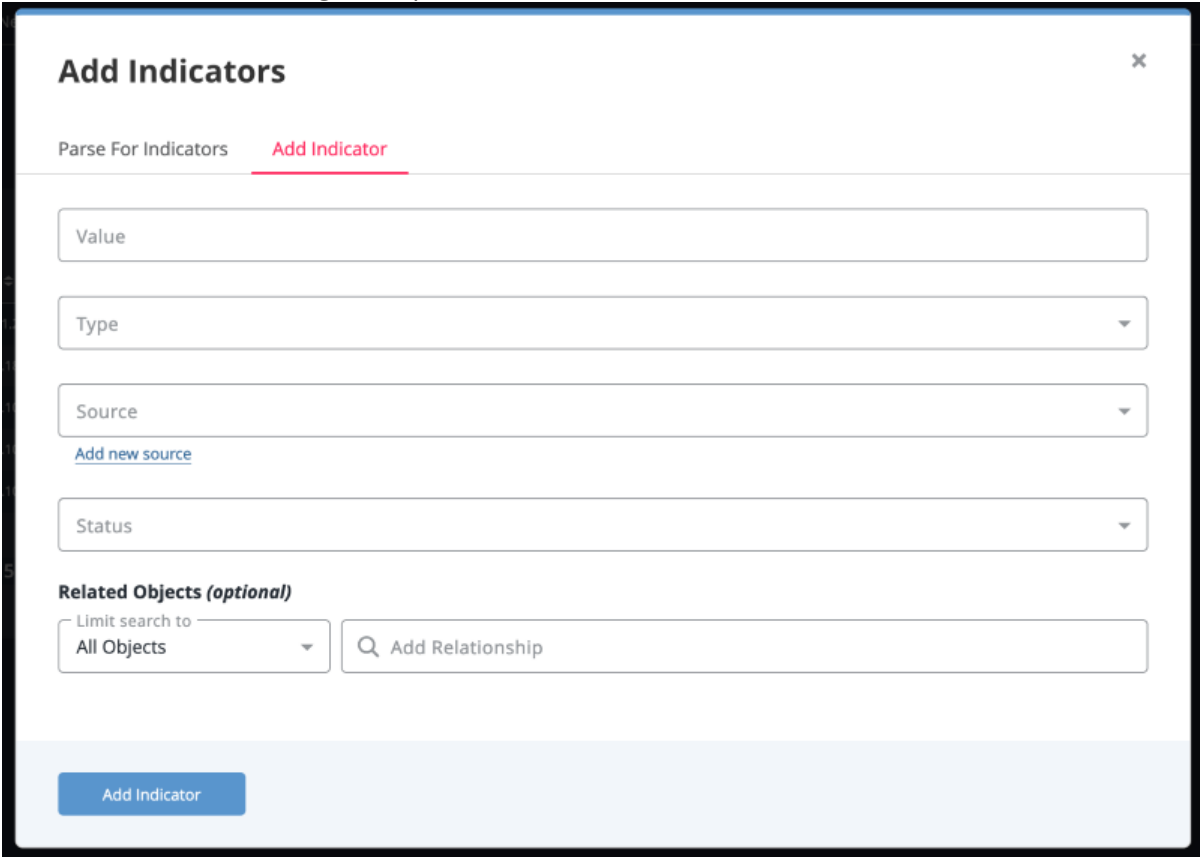
Indicators can be scored to allow you to apply weighting using contextual information, such as sources, attributes, and indicator types, as they are added to ThreatQ. You can also set a manual score per indicator.

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

Adding an Indicator

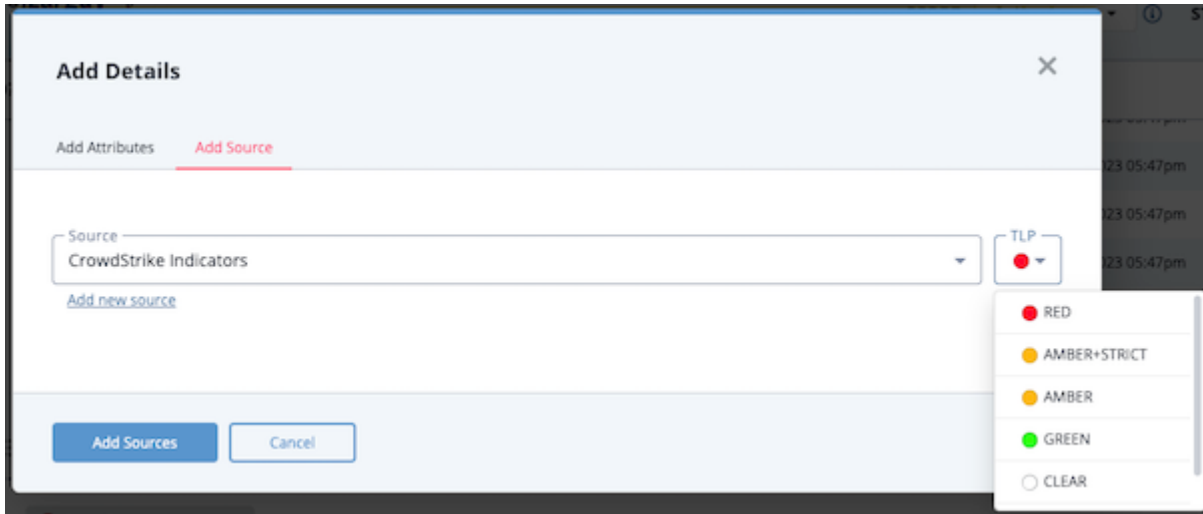
1. Click on **Create > Indicator**.

The Add Indicators dialog box opens.



2. Enter a value in the **Value** field.
3. Select the **Type** of Indicator.
4. Select a **Source** from the provided dropdown list.

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



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**.

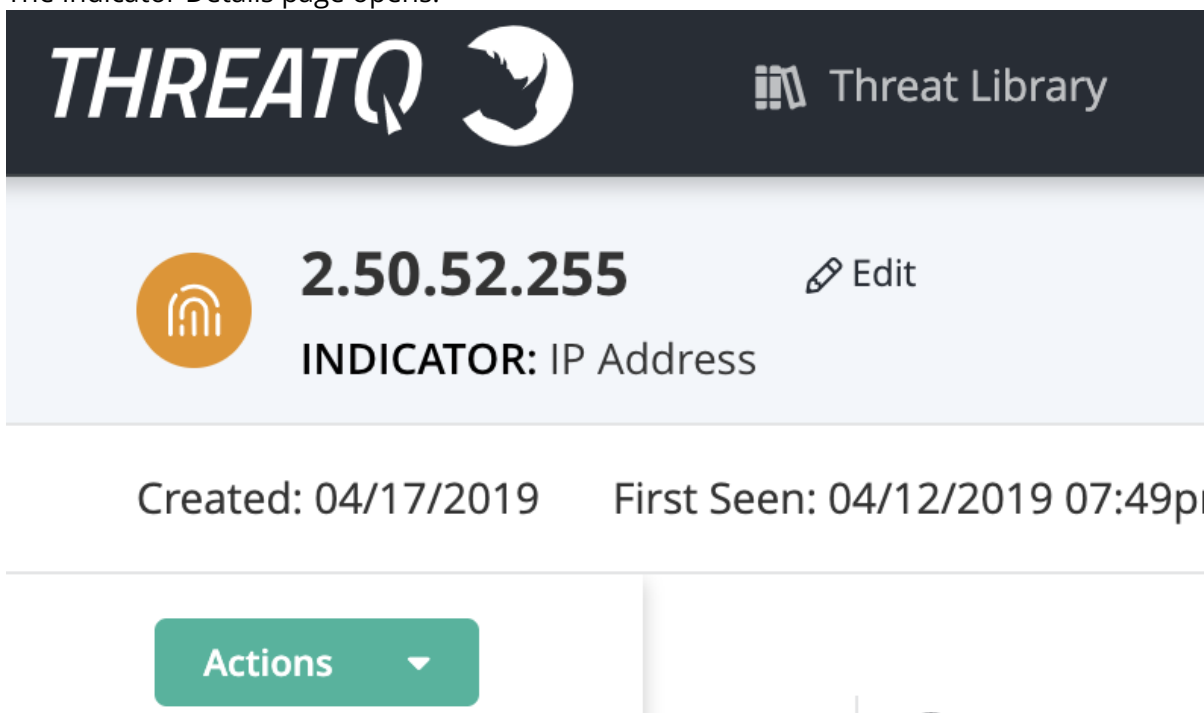
Adding Context

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

Editing Indicators

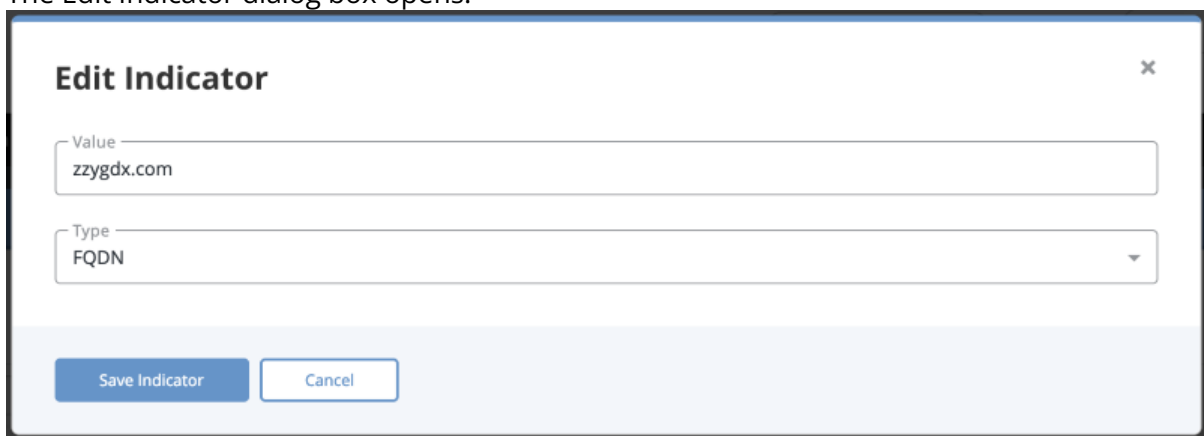
1. Locate and click on the indicator.

The Indicator Details page opens.



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

The Edit Indicator dialog box opens.

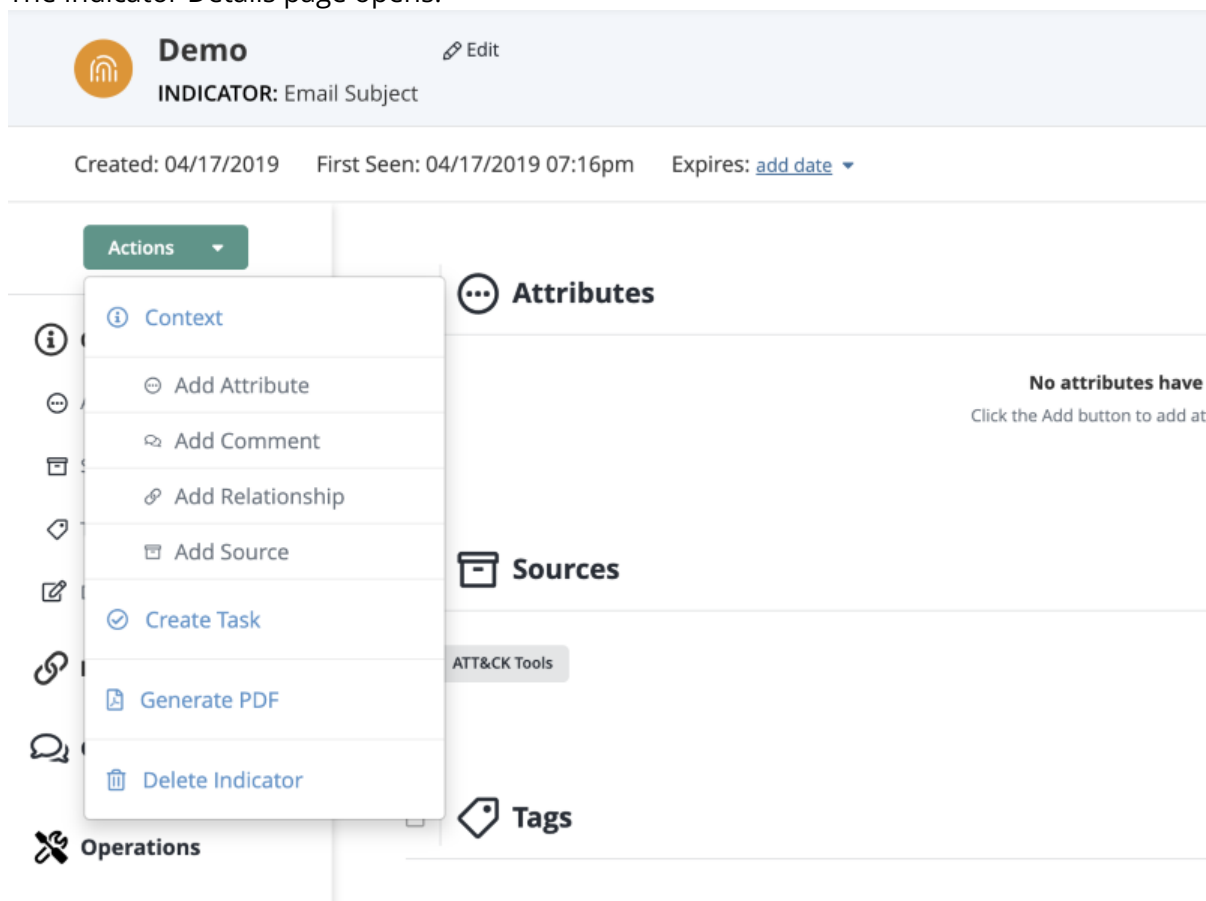


3. Make the desired change to the indicator **Value** and **Type**.
4. Click on **Save Indicator**.

Deleting an Indicator

1. Locate and click on the Indicator.

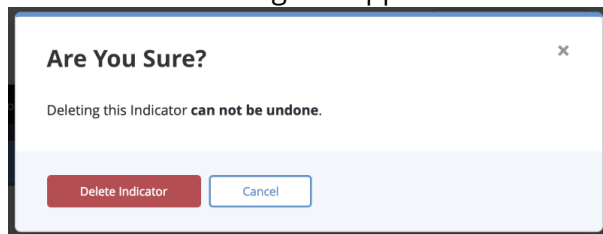
The Indicator Details page opens.



The screenshot shows the 'Indicator Details' page for an indicator named 'Demo' with the subject 'INDICATOR: Email Subject'. The page includes a header with the indicator name and an 'Edit' button. Below the header, it shows the creation date (04/17/2019), first seen date (04/17/2019 07:16pm), and expiration date (add date). A sidebar on the left contains an 'Actions' dropdown menu with options: Context, Add Attribute, Add Comment, Add Relationship, Add Source, Create Task, Generate PDF, and Delete Indicator. The main content area has sections for 'Attributes' (No attributes have), 'Sources' (ATT&CK Tools), and 'Tags'.

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

A confirmation dialog box appears.



The screenshot shows a confirmation dialog box titled 'Are You Sure?'. It contains the text 'Deleting this Indicator can not be undone.' and two buttons: 'Delete Indicator' (red) and 'Cancel' (blue).

3. Click on **Delete Indicator**.

Parsing for Indicators

ThreatQ gives you the option to import a file, parse it for indicators, and add those indicators to your Threat Library. During the import process you can assign a source, tag, and a relationship to the imported indicators.



See the [Importing Indicators via CSV](#) topic for specific instructions and examples on parsing indicators from a .csv file.

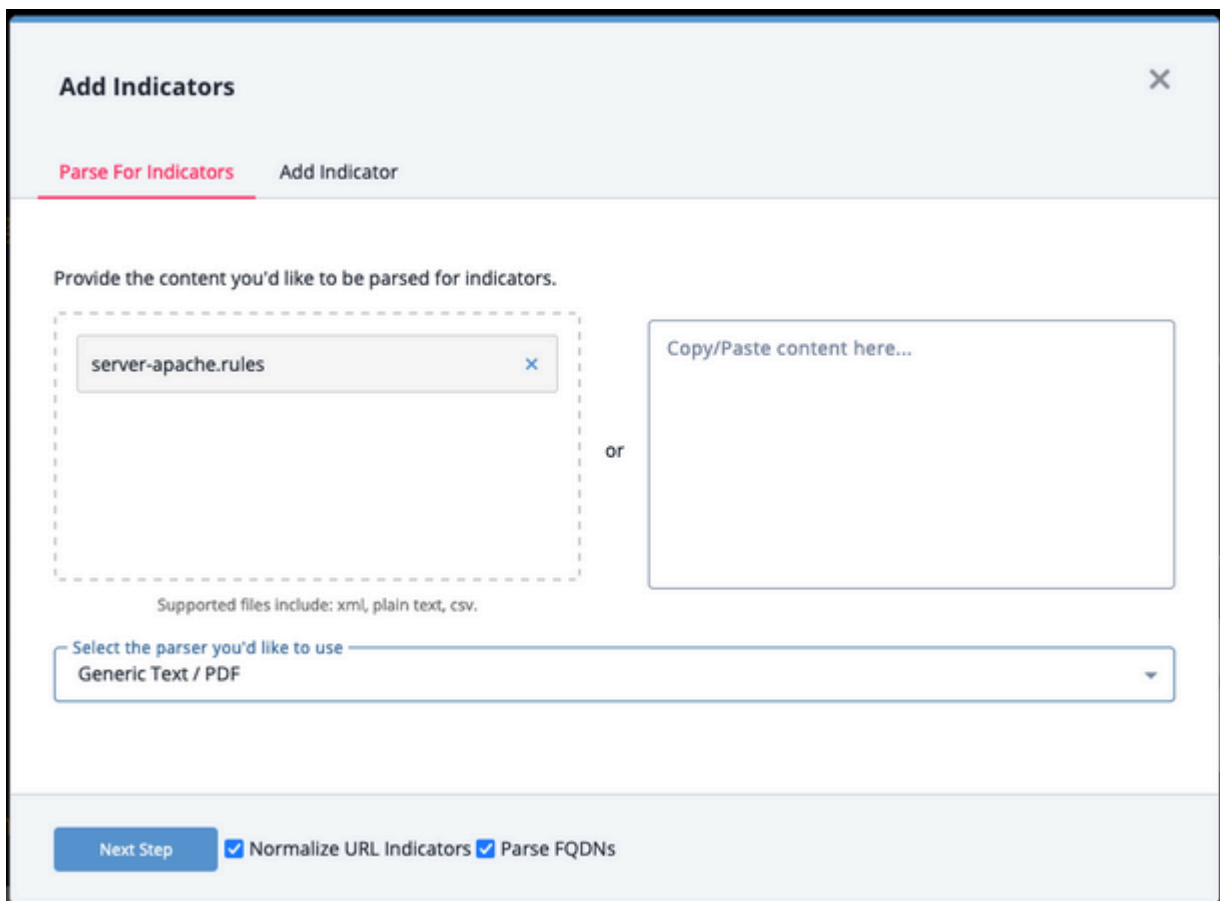
Selecting a File to Parse

1. Click the **Create** button, located at the top-right of the menu bar, and select the **Indicator Parser** option.



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

The Add Indicators dialog box will open.



2. Select the file to upload by either:
 - Dragging and dropping the file into the dialog window

- Clicking on the Click to Browse option and locating the file on your local device
 - Copying and pasting the file's contents in the text field provided.
3. Select the type of parser to use. Options include
 - Cuckoo
 - FireEye Analysis
 - Generic Text / PDF
 - Palo Alto Networks WildFire XML
 - ThreatAnalyzer Analysis
 - ThreatQ CSV File - see the [Importing Indicators via CSV](#) topic for specific instructions on using this parser.
 4. Use the checkboxes to select your parsing options:

OPTION	DESCRIPTION
Normalize URL Indicators	When checked, parsed URLs will have ports and leading protocol adjusted, as well as unneeded quotes and spaces removed.  Normalization also adds attributes for protocol and query string. See the Indicator URL Normalization topic for more details.
Parse FQDNs	When checked, the Indicator Parser will parse FQDNs from the text and derive FQDN indicators from URLs in the text. Example (checked): URL: https://tqexample.com/table.jspsa?query_string_example Indicators created: ○ tqexample.com/table.jspsa (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.jspsa?query_string_example Indicator created: ○ tqexample.com/table.jspsa (the URL)
 Administrators can configure the default setting for these options under the General Tab on the System Configurations page. See the Indicator Parsing Presets topic for more details.	

5. Click on **Next Step**.

The Step 1 - Import Indicators form will load.

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.

 server-apache.rules
46 KB

File Title (required)

server-apache.rules

File Description (optional)

Since file names aren't always descriptive, use this to easily identify this file.

File Category

Generic Text / PDF

☐ No, delete this file after import.

Provide the source of this information.

Source

[Add new source](#)

Select a status to be applied to all extracted indicators.

Review

This will not override the status of any pre-existing indicators.

Apply tags to all extracted indicators. (optional)

Type here and press enter

Apply attributes to all extracted indicators. (optional)

Name

[Add new name](#)

Value

[Add new value](#)

Source

[Add new source](#)

Add relationships to all extracted indicators. (optional)

Limit search to

All Objects

Add Relationship

[Next Step](#) Step 1: Tell us about the import > Step 2: Organize and classify

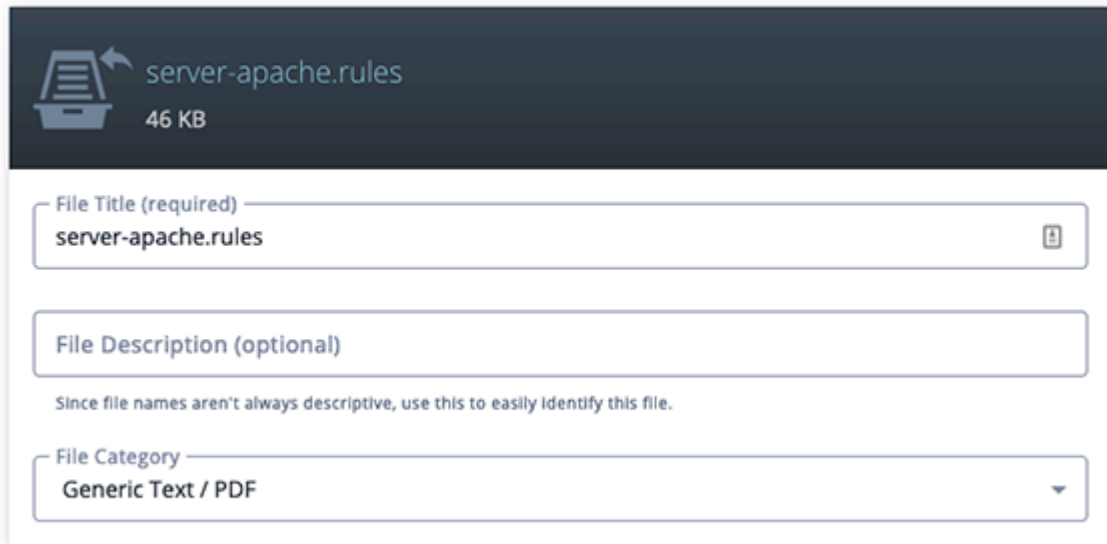
Step 1 - Import Indicators Settings

6. Select whether or not to save the import file. Saving the file will result in all extracted indicators being linked to the file for reference. If you select **Yes**, review the **File Title** and **File Category**. You can also add an option **File Description**.

Would you like to save this file?

☒ Yes, save this file. **(Recommended)**

All indicators extracted during this import will be linked to this file for future reference.

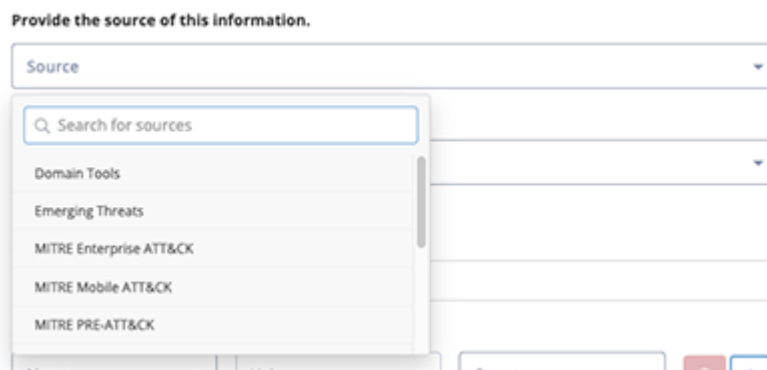


The screenshot shows a file upload interface. At the top, there's a dark header with a file icon and the text 'server-apache.rules' and '46 KB'. Below this is a form with three main sections: 'File Title (required)' with a text input containing 'server-apache.rules', 'File Description (optional)' with a text input and a note 'Since file names aren't always descriptive, use this to easily identify this file.', and 'File Category' with a dropdown menu showing 'Generic Text / PDF'.

☐ No, delete this file after import.

7. Select a **Source** for the extracted indicators.

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



The screenshot shows a dropdown menu titled 'Provide the source of this information.' The dropdown is open, showing a search bar 'Search for sources' and a list of sources: 'Domain Tools', 'Emerging Threats', 'MITRE Enterprise ATT&CK', 'MITRE Mobile ATT&CK', and 'MITRE PRE-ATT&CK'.

8. Select a **Status** for the extracted indicators.



The screenshot shows a dropdown menu titled 'Select a status to be applied to all extracted indicators.' The dropdown is open, showing the option 'Review'.

9. Enter any **Tags** to apply to the extracted indicators. This field is optional.
10. Select any attribute, attribute value, and attribute source to apply to the extracted indicators.
11. Add **Relationships** for the extracted indicators.



If you enter an object name that is not found, you can click the **Create** link to add the new object. If you limited your search to a specific object type, you are linked to the corresponding form. For example, if you limit your search to Adversaries, the **Create** link opens the Add An Adversary form. If you leave the **Limit search to** field set to All Objects, you can select the object type you want to create from a drop-down list.

12. Click on **Next Step**.

The Organize and Classify form will load.

The screenshot shows the 'Import Indicators' form. On the left, there's a section for 'Original Content' with a text area containing a large block of raw indicator data. On the right, there's a table of extracted indicators. The table has columns for 'VALUE', 'TYPE', 'STATUS', and 'SOURCE'. Each row represents an indicator, and each cell has a 'Pre-Existing' link and a 'Remove' button. The 'SOURCE' column for all indicators is 'amy pond'.

VALUE	TYPE	STATUS	SOURCE
a271c341549e19a23728d5e4a4e85aad	MDS	Indirect	amy pond
eed79b586c96674f99473a3d1b60a29a	MDS	Indirect	amy pond
c130b60d5f7f00dd3009a81e8093311	MDS	Indirect	amy pond
0424ebf80c9a0c1deda8965e0db3e65	MDS	Indirect	amy pond
a6f6e4bdcac434c10862e42ce0153649a	MDS	Indirect	amy pond
a9784b31da9ec8a850e1f739a5c0112a	MDS	Indirect	amy pond
7016792f564d19a7e6b0dc062e60922c8	MDS	Indirect	amy pond
36a376e904717307f9a912488580997a	MDS	Indirect	amy pond
138d22a03084324d7f81a259ad18741	MDS	Indirect	amy pond
eeef9792d2a9a81b684f0b1480c49962	MDS	Indirect	amy pond
44a15802a44b4a060c59a84a1146f007	MDS	Indirect	amy pond

Step 2 - Organize and Classify

13. You can review the original content of the file and the extracted indicators' information.

Filtering Extracted Indicators List

- The top tabs allow you to filter the list of indicators by New and Pre-existing. This allows you isolate any indicators that already exist in the platform.

All (263)

New (0)

Pre-Existing (263)

Select

Add info

Remove

Add Indicator

VALUE	TYPE	STATUS	SOURCE
Start typing...			Start typing...
a271c341849e19a23728d5e4a4e86aad Pre-Existing	MD5	Indirect	amy pond
eed79b586c96674f99473a3d1b60ad9a Pre-Existing	MD5	Indirect	amy pond
c130b60d5f5f100dd3009a81e8093311 Pre-Existing	MD5	Indirect	amy pond
0404ebf60cd9a0c1deda8965e0db3e65 Pre-Existing	MD5	Indirect	amy pond
a6fe64bdca434c10862e42ce01536a9a Pre-Existing	MD5	Indirect	amy pond
a9784b31da9ec8a6850e1f39a5c0112a Pre-Existing	MD5	Indirect	amy pond
7036792fd4d19a7e6b0dc062e60922c8 Pre-Existing	MD5	Indirect	amy pond

Pre-existing indicators will also be marked with a Pre-existing label in the list. You can click this label to view the preview panel for the object.

☐ a271c341849e19a23728d5e4a4e86aad	Pre-Existing	MD5

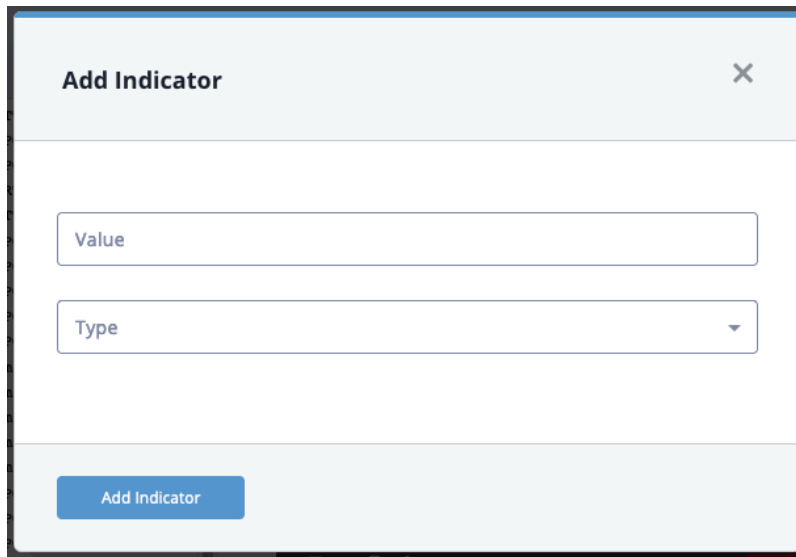
- You can click on the **Select** dropdown to automatically select indicators by sub-type.

Select ▼

! Selecting **All** will select all extracted indicators, not just the ones in your current filtered view (New, Pre-Existing).

Adding Indicators

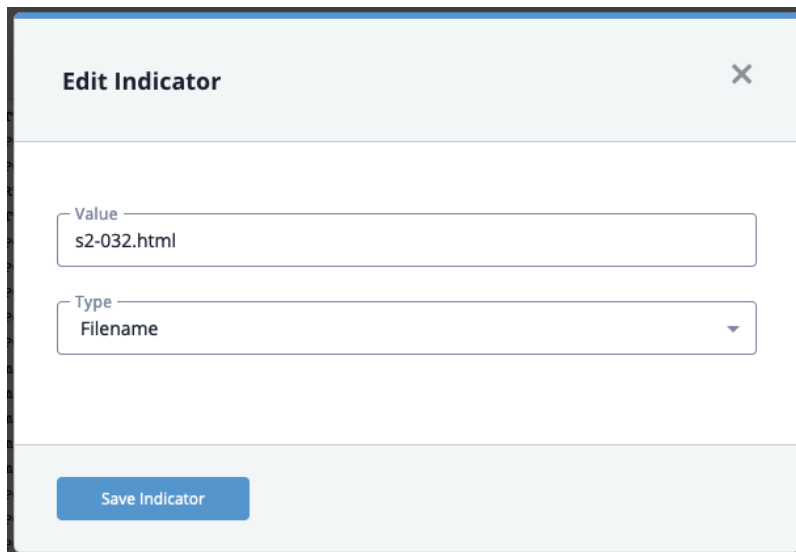
- You can click on the **Add Indicator** option, located to the top-right of the list, to add an indicator to the extracted list. You can add further context to the new indicator using the Editing Extracted Indicators actions listed below.



The 'Add Indicator' dialog box has a title bar with the text 'Add Indicator' and a close button (X). It contains two input fields: a text field labeled 'Value' and a dropdown menu labeled 'Type'. At the bottom, there is a blue button labeled 'Add Indicator'.

Editing Extracted Indicators

- Clicking on the  icon will show you where the indicator appeared in the Original Content window.
- Clicking on the  icon will open the **Edit Indicator** dialog box and allow you to edit the indicator value and indicator sub-type.



The 'Edit Indicator' dialog box has a title bar with the text 'Edit Indicator' and a close button (X). It contains two input fields: a text field labeled 'Value' with the text 's2-032.html' and a dropdown menu labeled 'Type' with the text 'Filename'. At the bottom, there is a blue button labeled 'Save Indicator'.

- Selecting one or more indicators and clicking on **Add Info** option allows you to perform the following actions:

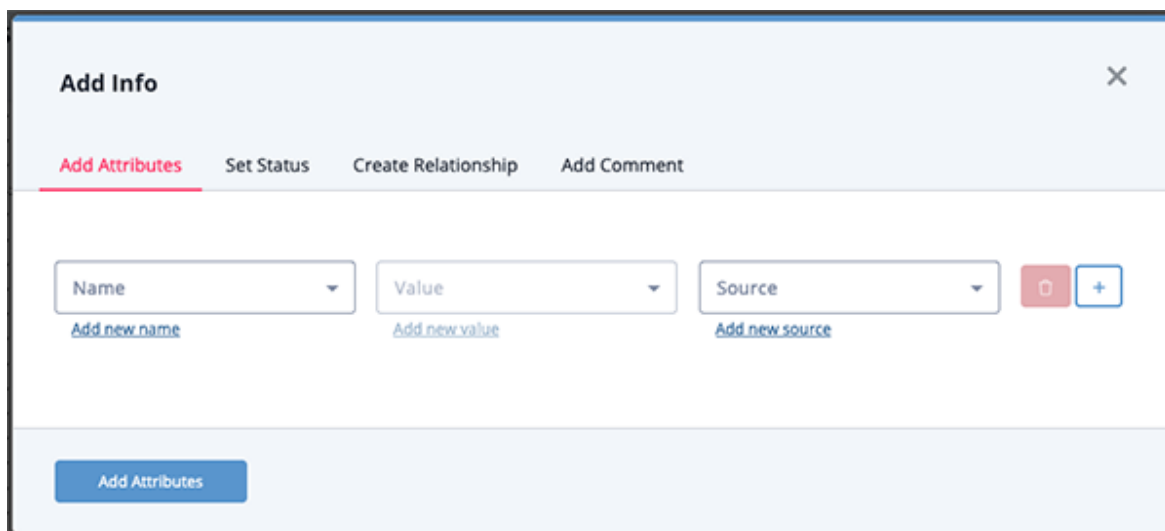
ACTION

DETAILS

Add Attribute

You can add an attribute to one or more extracted indicators. Select the checkbox next to the indicator(s) to update and then click on the **Add Info** option. The Add Attributes tab will be

ACTION	DETAILS
	selected by default. Select an Attribute Name, Value, and Source to apply to the selected indicator(s).
Set/Update Status	You can update the status of one or more extracted indicators. Select the checkbox next to the indicator(s) to update and then click on the Add Info option. Click on the Set Status tab and select your new status.
Create Relationship	You can link one or more extracted indicators to another system object. Select the checkbox next to the indicator(s) to update and then click on the Add Info option. Click on the Set Relationship tab and set the relationship. When you add a relationship, it is displayed in the indicator list and you can click it to view its details in a preview panel.  If the object you want to link is not found, you can you can click the Create link to add the new object. If you limited your search to a specific object type, you are linked to the corresponding form. For example, if you limited your search to Adversaries, the Create link opens the Add An Adversary form. If you leave the Limit search to field set to All Objects, you can select the object type you want to create from a drop-down list. In the Add form, the indicators you selected in the second step of the import process are listed in the Create Relationship section.
Add Comment	You can add a comment to one or more extracted indicators. Select the checkbox next to the indicator(s) to update and then click on the Add Info option. Click on the Set Comment tab and enter your comment.



Removing Extracted Indicators

- You can delete one or more extracted indicators. Select the checkbox next to the indicator(s) to delete and then click on the **Remove** icon.



Selecting **All** from the Select dropdown will select all extracted indicators, not just the ones in your current filtered view (New, Pre-Existing).

14. When finished editing the extracted indicators list, click **Finish Export** to complete the process.

Importing Indicators via CSV

You can parse a CSV file for indicators using the ThreatQ CSV File Parser.



A CSV example file is available for download to serve a reference as you build your own CSV.

[Download CSV Example](#)

CSV Files with 1000+ Rows

- Attempt to break the file into smaller parts and import.
- If you cannot break down the file, contact ThreatQ Customer Success about implementing a dedicated parser using the Configuration Driven Feed (CDF) framework.

CSV Columns

The column headers marked with an * in the table below are required for the CSV file. Failure to include these required columns will result in the import process failing. All other column headers are optional and will not cause the import process to fail if not included.



Object and Attribute Sources cannot be added through the CSV file itself. A source value is added in the [Step 7](#) of the import process, listed below, and is selected by the user.



The ThreatQ parser is case sensitive. When creating your CSV file, confirm that you are using the correct spelling and case for column headers as listed below.

COLUMN HEADER

DETAILS

*Indicator

This field identifies the indicator name/value.

ThreatQ requires that the Indicator column be included in the CSV file and that each entry have a value.

Example

	A	B	C	D	E	F
1	Indicator	Type	Status	Attribute::Country	Attribute::State	Comments
2	trustme@refundszus.com	Email Address	Active	USA	MA	Phishing attempt
3	officer@irspolice.com	Email Address	Active	USA	MD	Fraudulent robocall
4	6c277b5ea26178c5	MD5	Review	USA	CA	
5	172.54.542.236	IP Address	Active	USA	CO	
6	39.38.116.53	IP Address	Active	USA	FL	

***Type**

This field identifies the indicator type.

ThreatQ requires that the Type column be included in the CSV file and that each entry have a value.



You must use a type that already exists in your ThreatQ instance. If you are unable to provide an Indicator Type for each indicator, you can use the **Generic Text/PDF** parsing option that attempts to identify indicator type values automatically.

Example

	A	B	C	D	E	F
1	Indicator	Type	Status	Attribute::Country	Attribute::State	Comments
2	trustme@refundsus.com	Email Address	Active	USA	MA	Phishing attempt
3	officer@irspolice.com	Email Address	Active	USA	MD	Fraudulent robocall
4	6c277b5ea26178c5	MD5	Review	USA	CA	
5	172.54.542.236	IP Address	Active	USA	CO	
6	39.38.116.53	IP Address	Active	USA	FL	

***Status**

The Status column is required. You must use a status that already exists in your ThreatQ instance. You can review your existing status by clicking on the **Settings** gear icon and selecting **Object Management**.



The status supplied in the CSV overrides the status selected during the import process.

Example

	A	B	C	D	E	F
1	Indicator	Type	Status	Attribute::Country	Attribute::State	Comments
2	trustme@refundsus.com	Email Address	Active	USA	MA	Phishing attempt
3	officer@irspolice.com	Email Address	Active	USA	MD	Fraudulent robocall
4	6c277b5ea26178c5	MD5	Review	USA	CA	
5	172.54.542.236	IP Address	Active	USA	CO	
6	39.38.116.53	IP Address	Active	USA	FL	

Attribute

The Attribute columns are optional. You can apply one or more attributes to an indicator by adding an Attribute column.

Attribute keys are **case** and **space** sensitive, 'MalwareFamily' and 'malware family' will generate a separate key in ThreatQ. In order to map to an existing Attribute Key in ThreatQ, you must match it exactly.

Each attribute column heading must use the follow format:

Attribute::<Attribute Name>



ThreatQuotient recommends you review existing attribute keys and values in ThreatQ prior to importing so that you can maintain consistent and normalized attribute data.

Example

	A	B	C	D	E	F
1	Indicator	Type	Status	Attribute::Country	Attribute::State	Comments
2	trustme@refundszus.com	Email Address	Active	USA	MA	Phishing attempt
3	officer@irspolice.com	Email Address	Active	USA	MD	Fraudulent robocall
4	6c277b5ea26178c5	MD5	Review	USA	CA	
5	172.54.542.236	IP Address	Active	USA	CO	
6	39.38.116.53	IP Address	Active	USA	FL	

Comments

The optional Comments column allows you to add a comment for the indicator.

The ThreatQ user that performs the import process is marked as the author of the comment in ThreatQ.

Comments (1)

threatq@threatq.com a minute ago
 Phishing attempt
[Edit](#) [Delete](#)

Example

	A	B	C	D	E	F
1	Indicator	Type	Status	Attribute::Country	Attribute::State	Comments
2	trustme@refundszus.com	Email Address	Active	USA	MA	Phishing attempt
3	officer@irspolice.com	Email Address	Active	USA	MD	Fraudulent robocall
4	6c277b5ea26178c5	MD5	Review	USA	CA	
5	172.54.542.236	IP Address	Active	USA	CO	
6	39.38.116.53	IP Address	Active	USA	FL	

Parsing a ThreatQ CSV File and Adding Context

1. Click the **Create** button and select **Indicator Parser** under the *Import* heading.

The Add Indicators dialog box opens with the Parse for Indicators tab selected.

Add Indicators

Parse For Indicators
Add Indicator

Provide the content you'd like to be parsed for indicators.



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

Supported files include: xml, plain text, csv.

or

Copy/Paste content here...

Select the parser you'd like to use

Next Step
☒ Normalize URL Indicators
☒ Parse FQDNs

- Upload your CSV file by either:
 - Dragging and dropping your file into the window
 - Clicking the Click to Browse option and uploading your file
- Select **ThreatQ CSV File** as the parser to use.
- Use the checkboxes to select your parsing options:

OPTION	DESCRIPTION
Normalize URL Indicators	When checked, parsed URLs will have ports and leading protocol adjusted, as well as unneeded quotes and spaces removed.  Normalization also adds attributes for protocol and query string. See the Indicator URL Normalization topic for more details.
Parse FQDNs	When checked, the Indicator Parser will parse FQDNs from the text and derive FQDN indicators from URLs in the text. Example (checked): URL: <code>https://tqexample.com/table.jspa?query_string_example</code> Indicators created: - tqexample.com/table.jspa (the URL) - tqexample.com (the derived FQDN from the URL) When unchecked, the Indicator Parser will not generate FQDN indicators from the parsed text.

Example (unchecked): URL: https://tqexample.com/table.jspa?query_string_example

Indicator created:

- tqexample.com/table.jspa (the URL)



Administrators can configure the default setting for these options under the General Tab on the System Configurations page. See the Indicator Parsing Presets topic for more details.

5. Click **Next Step**.
6. Select whether or not to save the CSV file. Saving the file will result in all extracted indicators being linked to the file for reference.

Import Indicators

Abandon

Would you like to save this file?

☒ Yes, save this file. **(Recommended)**

All indicators extracted during this import will be linked to this file for future reference.



cvsexample.csv

327 bytes

File Title (required)

cvsexample.csv

File Description (optional)

Since file names aren't always descriptive, use this to easily identify this file.

File Category

ThreatQ CSV File

☐ No, delete this file after import.

7. Select a **Source** for the extracted indicators.
You can also click the **Add a New Source** option if the desired source is not listed in the dropdown list . If administrators have enabled TLP view settings, you can select a TLP label for the new source in the dropdown list provided. See the Traffic Light Protocol (TLP) topic for more

information on TLP schema.

Provide the source of this information.

Source

- Domain Tools
- Emerging Threats
- MITRE Enterprise ATT&CK
- MITRE Mobile ATT&CK
- MITRE PRE-ATT&CK

8. Select a **Status** for the extracted indicators. The indicator's Status value supplied in the CSV overrides this value.

Select a status to be applied to all extracted indicators.

Review

This will not override the status of any pre-existing indicators.

9. Enter any **Tags** to apply to the extracted indicators. This field is optional.
10. Select any attribute, attribute value, and attribute source to apply to the extracted indicators.
11. Add **Relationships** for the extracted indicators.



If you enter an object name that is not found, you can click the **Create** link to add the new object. If you limited your search to a specific object type, you are linked to the corresponding form. For example, if you limit your search to Adversaries, the **Create** link opens the Add An Adversary form. If you leave the **Limit search** field set to All Objects, you can select the object type you want to create from a drop-down list.

12. Click on **Next Step**.

The Step 2: Organize and Classify page will load.

Import Indicators

Abandon this import

Original Content

Indicator Type

Status

Source

Comment

Indicator Type

Status

Source

Comment

Indicator Type

Status

Source

Comment

Indicator Type

Status

Source

Comment

Indicator Type

Status

Source

Comment

Indicator Type

Status

Source

Comment

13. You can review the extracted indicators' information and attributes.

You can perform the following actions:

ACTION

DETAILS

Add Indicator

You can add additional indicators by clicking on the Add Indicator button.

Edit Indicator Type and Value

You can edit the Indicator Type by clicking on the Pencil icon next to the indicator name. The Edit Indicator screen will load. You can edit the extracted indicator's value and type from this box.

Set/Update Status

You can update the status of one or more extracted indicators. Select the checkbox next to the indicator(s) to update and then click on the **Add Info** option. Click on the **Set Status** tab and select your new status.

Add Attribute

You can add an attribute to one or more extracted indicators. Select the checkbox next to the indicator(s) to update and then click on the **Add Info** option. The Add Attributes tab will be selected by default. Select an **Attribute Name**, **Value**, and **Source** to apply to the selected indicator(s).

Create Relationship

You can link one or more extracted indicators to another system object. Select the checkbox next to the indicator(s) to update and then click on the **Add Info** option. Click on the **Set Relationship** tab and set the relationship. When you add a relationship, it is displayed in the indicator list and you can click it to view its details in a preview panel.



If the object you want to link is not found, you can click the **Create** link to add the new object. If you limited your search to a specific object type, you are linked to the corresponding form. For example, if you limited your search to Adversaries, the **Create** link opens the Add An Adversary form. If you leave the **Limit search to** field set to All Objects, you can select the object type you want to create from a drop-down list. In the Add form, the indicators you selected in the second step of the import process are listed in the Create Relationship section.

Add Comment

You can add a comment to one or more extracted indicators. Select the checkbox next to the indicator(s) to update and then click on the **Add Info** option. Click on the **Set Comment** tab and enter your comment.

**Delete
Extracted
Indicator**

You can delete one or more extracted indicators. Select the checkbox next to the indicator(s) to delete and then click on the **Remove** icon.

14. Click **Finish Export**.

Troubleshooting

If the CSV fails to parse please review the following points:

- Verify that the file is a CSV.
- Verify that column headers are spelled exactly as they are listed, the parser is case sensitive.
- Verify that all rows have a value for Indicator and Type.
- Verify that all Type and Status values are valid and exist in ThreatQ.



If you have previously hit a failed parse run and believe you have fixed the error but the file will still not parse, logout of TQ, log back in and attempt to parse again.

Indicator URL Normalization

Remove Quotes from the Beginning and/or End of an Indicator

Single and double quote characters are removed if they are the first or last character of an indicator.

Remove Unneeded Spaces found within an Indicator

All spaces irrelevant of their position in the Indicator value are removed (when applicable).

Adjust Leading Protocol from Indicators

Indicators with a leading protocol [http://, https://, ftp://, or ftps://] are extracted and included as an attribute. When applicable, this indicator adjustment could change the indicator type from URL to FQDN.



Original URL indicator of http://evilsubdomain.no-ip.biz/ would convert to a FQDN = evilsubdomain.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 ASCII Values > 127	<space>

Ascii 96	-

Ascii145	'

Ascii146	'

Ascii147	"
Ascii148	"
Ascii151	-
carriage return and line feed	<space>
Control Characters	Remove
Convert to UTF8	Remove leading and trailing space, tab, newline, carriage return, vertical tabs and null characters.

Supported Defanging Techniques

The table below lists all supported indicator defanging techniques.

[.] => .

[dot] => .

(dot) => .

[d] => .

-dot- => .

dot => .

[:] => :

[:/] => ://

hxxp:// => http://

hxxx:// => http://

hxxps:// => https://

hxxxs:// => https://

[hxxp] => http

hxtp:// => http://

htxp:// => http://

hxtps:// => https://

htxps:// => https://

[http] => http

[http://] => http://

[https] => https

[https://] => https://

[at] => @

-at- => @

at => @

-@- => @

@ => @

[@] => @

[www] => www

Indicator Expiration

Expiration ("Expired") is a status that can be assigned to an indicator. The expired status should be used when an indicator is deemed by an analyst to pose less of a threat to their infrastructure than other indicators.



See the [Indicator Expiration Policies](#) topic for more information on setting up automatic expiration policies for indicators.

Ways an Indicator can Expire

- **An analyst manually changes an indicator(s) status to "Expired"**

This can be achieved by visiting an individual indicator's details page, then using the Status dropdown in the top right hand corner of the page to change the status.

If the analyst wishes to change the status of multiple indicators at the same time, they can use the advanced search tool to find the indicators they'd like to update, then click the Bulk Update button found directly to the right above the search results.

- **An analyst manually sets an expiration date for a specific indicator**

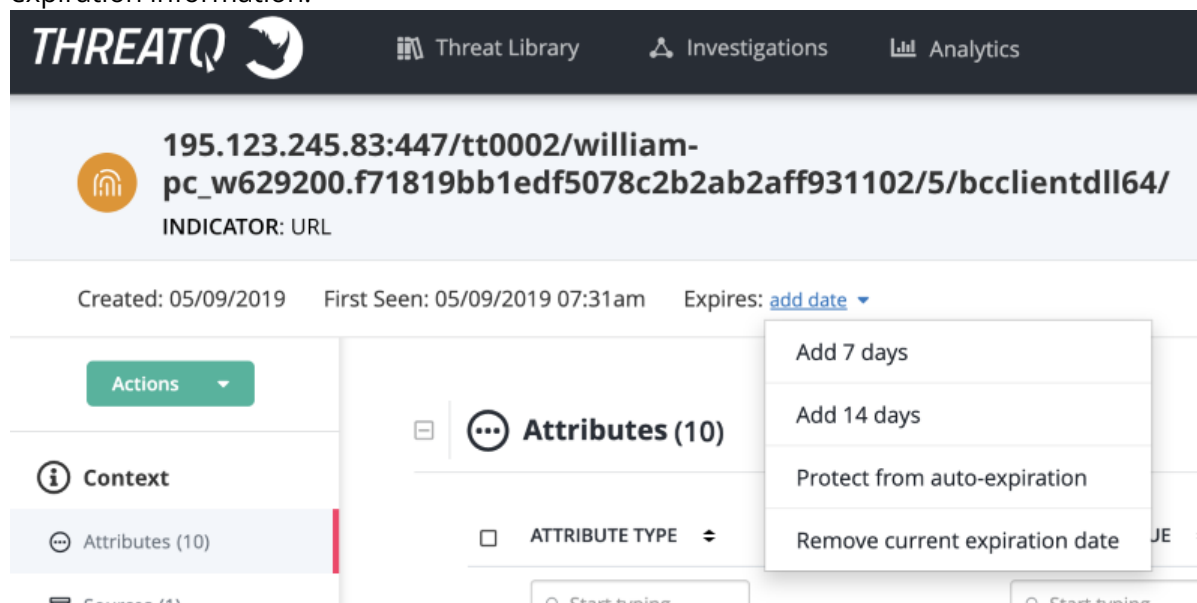
Each indicator has the option to have an expiration date set, which once past, will toggle the status of that indicator from it's current status to "Expired".

- **An expiration policy has been applied to the source reporting an indicator and therefore an expiration date is automatically set for that indicator during ingestion**

Using the "Expiration" tab on the Indicator Management page, a ThreatQ admin has the ability to apply expiration policies to all ingested information, both new and existing, coming from a specific intelligence source. See the [Indicator Expiration Policies](#) topic for more details.

Changing the Expiration Date for an Individual Indicator

When viewing a specific indicator, its expiration date can be changed by clicking on the link next to the expiration information.



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 indicator type is URL. The expiration date is currently set to 'add date'. A dropdown menu is open, showing options: 'Add 7 days', 'Add 14 days', 'Protect from auto-expiration', and 'Remove current expiration date'. The 'Attributes (10)' section is also visible.

Options include:

OPTION	DESCRIPTION
Add 7 Days	This will extend the current expiration date by 7 days.
Add 14 Days	This will extend the current expiration date by 14 days.
Protect from Auto-Expiration	This will set the indicator to "Never Expire". Once set, this indicator will be exempt from all automated expiration processes regardless of circumstances. The only way for this indicator to expire moving forward is by analyst choice.
Remove Current Expiration Date	This will remove the currently set expiration date. If this indicator is reported by an intelligence feed (with an expiration policy) in the future, a new expiration date will be added at that point in time.

Changing the Expiration Date for Multiple Indicators

You can apply expiration changes for a set of indicators using the Bulk Action function. See the [Bulk Actions](#) topic for further details.

Indicator Scoring

Indicator scoring allows you to apply weighting to indicators and their contextual information, such as sources, attributes, and indicator types, as they are added to ThreatQ. Indicator scoring allows you to set manual scores or rely on ThreatQ's scoring algorithm to calculate scores. After scores are calculated, you can change the score to your custom value or accept the calculated value.

Building a Scoring Algorithm

You can build a scoring algorithm that automatically assigns an indicator score based on user-designed criteria. See the [Scoring Algorithms](#) topic for further details.

Setting a Manual Indicator Score



You can use this process to override an individual indicators score set by the scoring algorithm.

1. Navigate to an Indicator's Details page.
2. Click the **Score** dropdown and select a score.

The screenshot displays the ThreatQ user interface for an indicator named 'Demo'. The top navigation bar includes 'Threat Library', 'Investigations', and 'Analytics'. The indicator details page shows a 'SCORE' dropdown menu with the following options: 10 - Very High, 9 - High, 8 - Medium, 7 - Medium, 6 - Low (highlighted), 5 - Low, 4 - Very Low, 3 - Very Low, 2 - Very Low, 1 - Very Low, and 0 - Very Low. The 'STATUS' is set to 'Active'. The left sidebar contains a list of navigation items: Context, Attributes (0), Sources (1), Tags (0), Description, Relationships, Comments (0), Operations, and Audit Log. The main content area is divided into sections: Attributes, Sources (with an 'ATTACK Tools' tag), Tags (with an 'add tag' input field), and Description (with an 'Edit' button).



Optionally, you may revert to the calculated score by clicking on the Score dropdown and selecting **Generated Score**.

SCORE: 7 - Medium

10 - Very High

9 - High

8 - Medium

7 - Medium

6 - Low

5 - Low

4 - Very Low

3 - Very Low

2 - Very Low

1 - Very Low

0 - Very Low

10 - Generated Score

STATUS: Active

Add to Watchlist

+ Add

Delete

+ Add

Indicator Status

All Indicator in the system have statuses.



Most exports in ThreatQ are configured to use the **Active** status to signal deployment to external devices. However this can be modified and each status can be used however your organization sees fit.

Default Statuses

The default statuses that ship with a standard installation of ThreatQ are as follows:

STATUS	DESCRIPTION
Active	Poses a threat and is being exported to detection tools.
Indirect	Associated to an active indicator or event (i.e. pDNS).
Review	Requires further analysis.
Whitelisted	Poses NO risk and should never be deployed.
Expired	Indicator has reached its expiration and has been is deemed by an analyst to pose less of a threat to their infrastructure than other indicators.

Custom Statuses

You can create custom statuses for use in your ThreatQ instance. See the Indicator Statuses topic for more details.

Changing the Status of an Individual Indicator

Changing an indicator's status is straightforward, except in the case of whitelisting CIDR Block indicators. When Whitelisting a CIDR Block indicator, this process generates a whitelisting rule. See the [Whitelisted Indicators](#) topic for more information.

1. Locate and click the indicator to open its details page.

- Click the status dropdown menu, and select the desired status.

SCORE:

0 - Very Low
▼

i

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

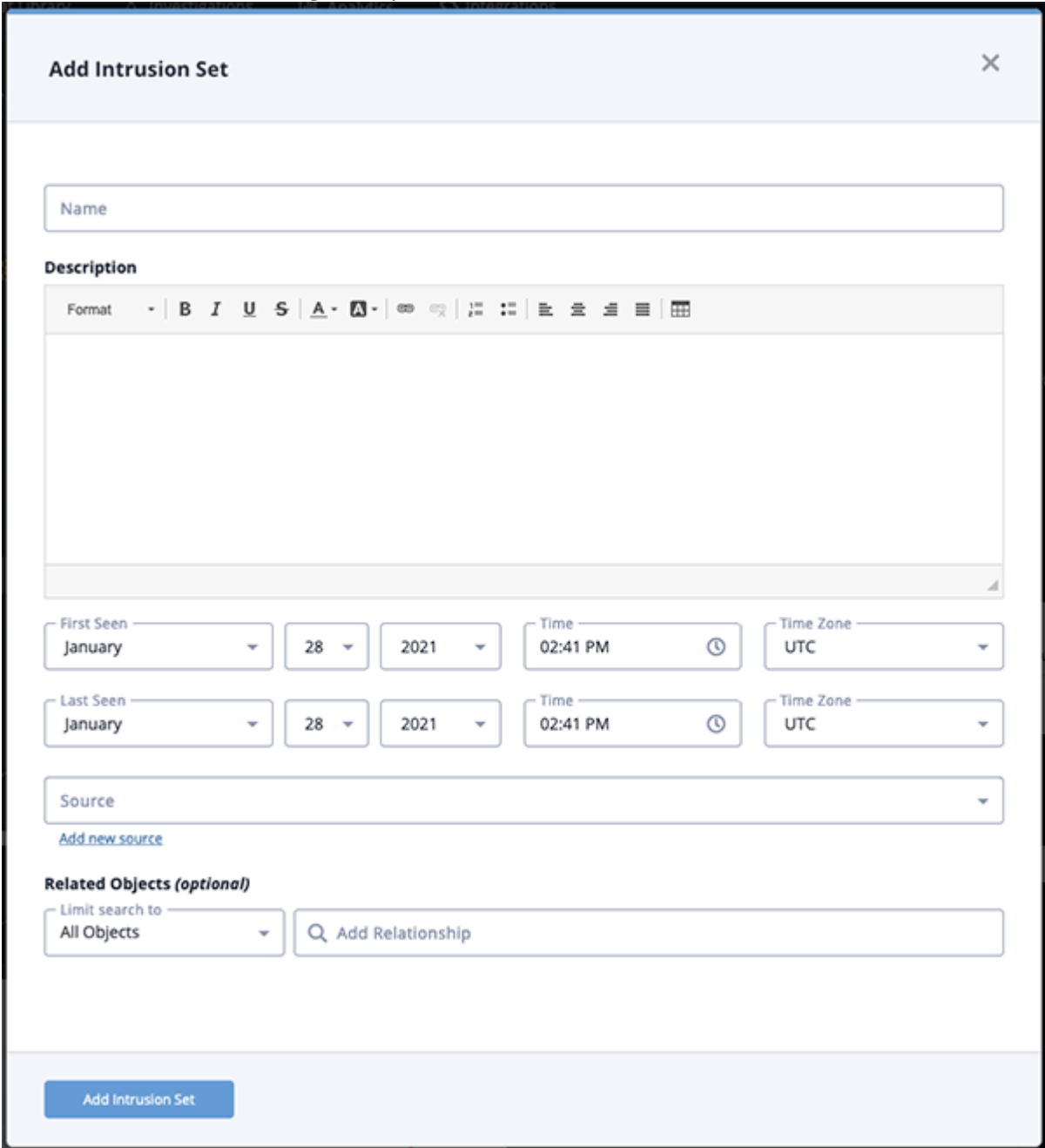
You can change the status for multiple indicators using the Bulk Status Change. See the [Bulk Actions](#) topic for more information.

Intrusion Sets

An Intrusion Set is grouped sets of adversarial behaviors and resources, sometimes referred to as attack packages, used to target an individual organization.

Adding an Intrusion Set

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



Add Intrusion Set [Close]

Name

Description

Format [Dropdown] | **B** *I* U ~~S~~ | **A** - **A** - | [Color Picker] [Color Picker] | [List Icon] [List Icon] | [List Icon] [List Icon] [List Icon] [List Icon] [List Icon] [List Icon]

First Seen [Month: January] [Day: 28] [Year: 2021] Time [Time: 02:41 PM] [Clock Icon] Time Zone [Time Zone: UTC] [Dropdown]

Last Seen [Month: January] [Day: 28] [Year: 2021] Time [Time: 02:41 PM] [Clock Icon] Time Zone [Time Zone: UTC] [Dropdown]

Source [Dropdown]

[Add new source](#)

Related Objects (optional)

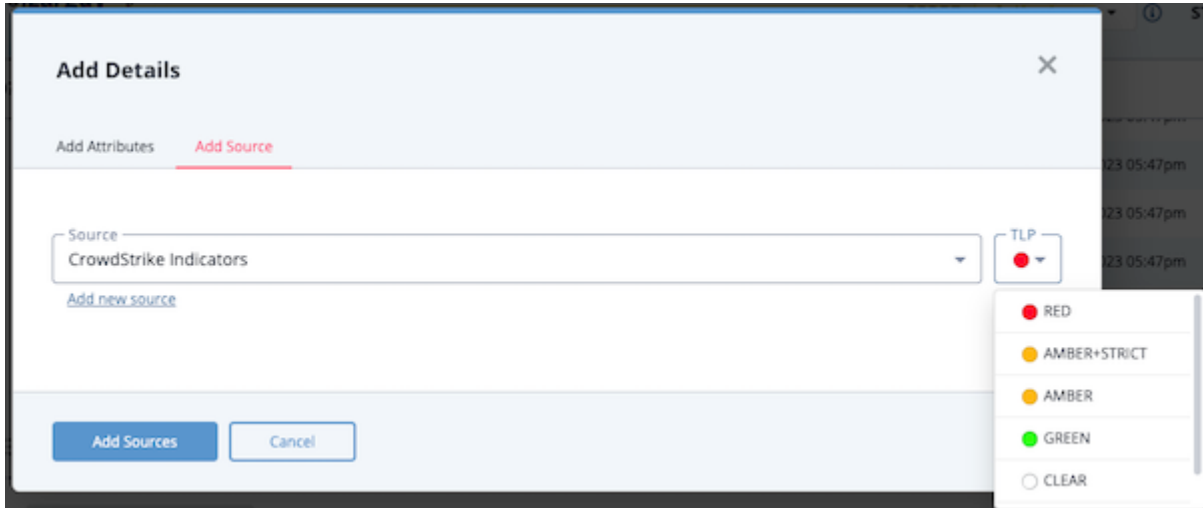
Limit search to [Dropdown: All Objects] [Add Relationship]

Add Intrusion Set

2. Enter a **Name**.

3. Enter a **Description** in the field provided.
4. Select the **First Seen** and **Last Scene** times.
5. Select a **Source** from the dropdown provided.

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



6. Select any **Related Objects** you need to link to the Intrusion Set. This field is optional.
7. Click **Add Intrusion Set**.

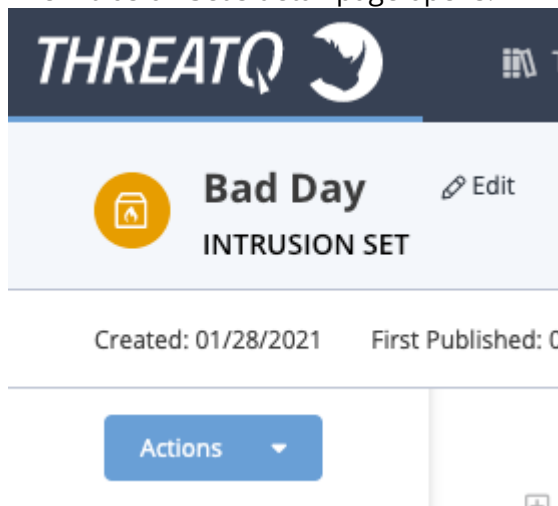
Adding Context

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

Editing an Intrusion Set

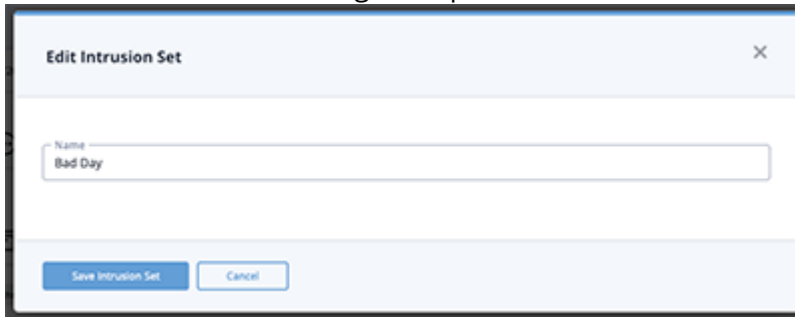
1. Locate and click on the Intrusion Set.

The Intrusion Set's detail page opens.



2. Click on **Edit** next to the Intrusion Set's name.

The Edit Intrusion Set dialog box opens.



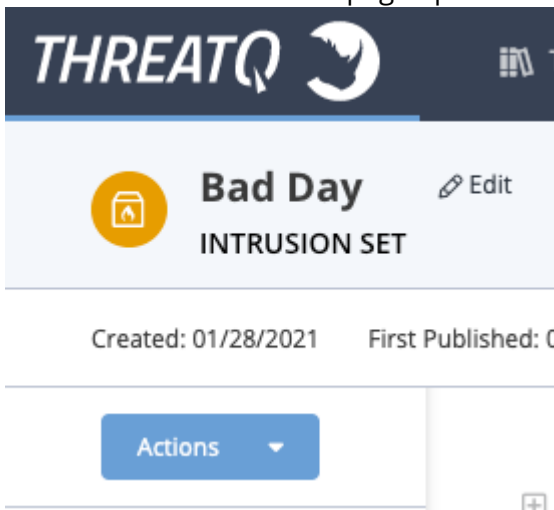
The dialog box titled "Edit Intrusion Set" has a close button (X) in the top right corner. It contains a text input field labeled "Name" with the value "Bad Day". At the bottom, there are two buttons: "Save Intrusion Set" and "Cancel".

3. Make the desired change to the Intrusion Set's name and click **Save Intrusion Set**.

Deleting an Intrusion Set

1. Locate and click on the Intrusion Set.

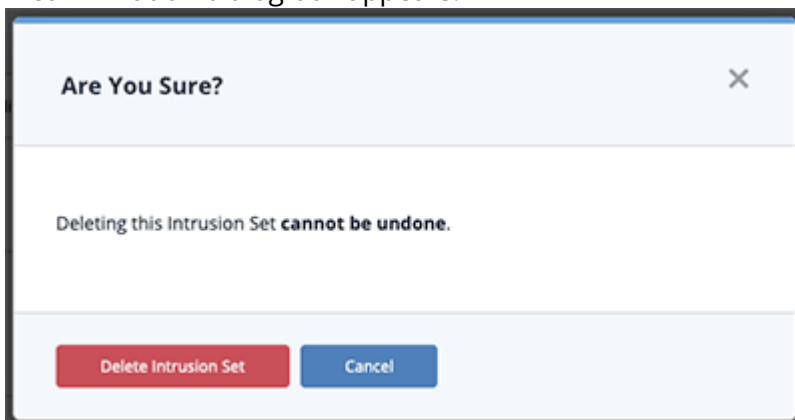
The Intrusion Set's details page opens.



The details page for the "Bad Day" intrusion set. It features the ThreatQ logo at the top. Below it, there's a yellow circular icon with a flame, followed by the text "Bad Day" and "INTRUSION SET". To the right of the name is an "Edit" button with a pencil icon. Below this, it shows "Created: 01/28/2021" and "First Published: 0". At the bottom, there's a blue "Actions" button with a dropdown arrow.

2. Click on the **Actions** menu and select **Delete Intrusion Set**.

A confirmation dialog box appears.



The confirmation dialog box titled "Are You Sure?" has a close button (X) in the top right corner. It contains the text "Deleting this Intrusion Set cannot be undone." At the bottom, there are two buttons: "Delete Intrusion Set" (in red) and "Cancel" (in blue).

3. Click on **Delete Intrusion Set**.

Malware

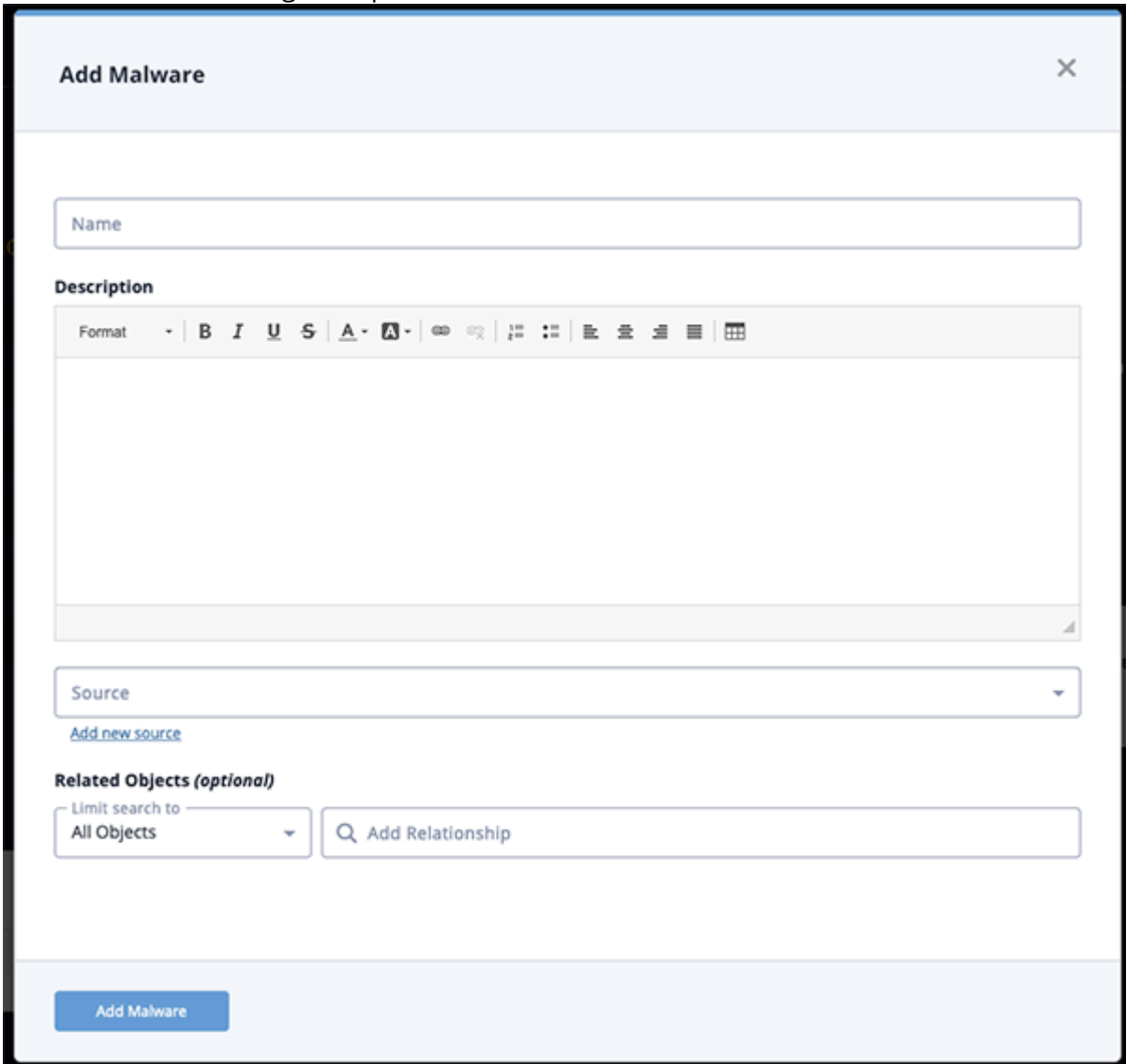
Malware , short for malicious software, targets devices, services, and networks with the intent to gain unauthorized access or damage a network or programmable device.

Use the steps below to create, edit and delete a Malware object.

Adding a Malware Object

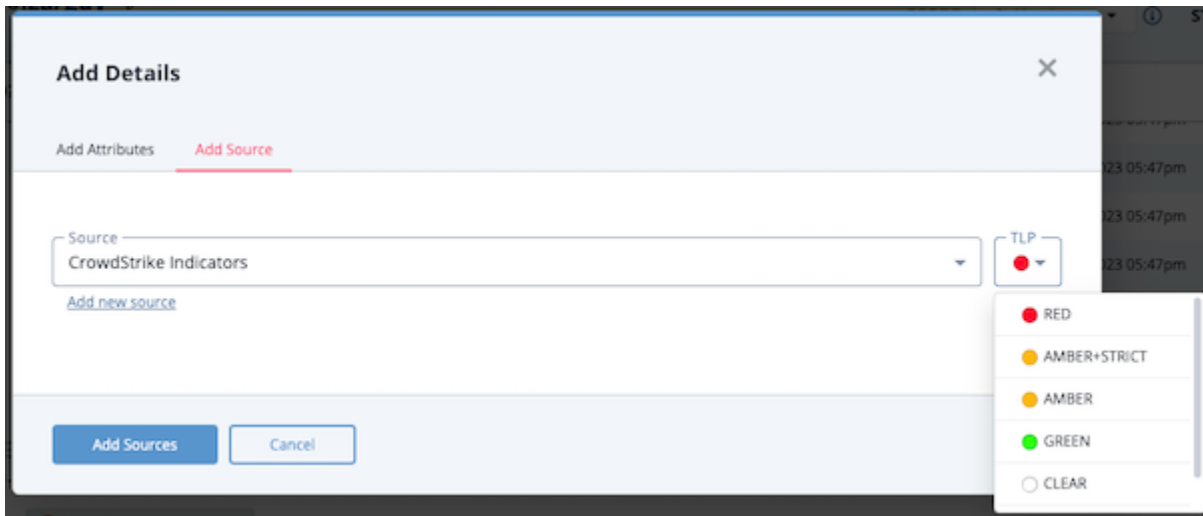
1. Go to **Create > Malware**.

The Add Malware dialog box opens.



2. Enter a name.
3. Enter a description in the field provided.
4. Select a **Source** from the dropdown provided.
You can also click the **Add a New Source** option if the desired source is not listed in the drop-down list. If administrators have enabled TLP view settings, you can select a TLP label for the

new source in the dropdown list provided. See the Traffic Light Protocol (TLP) topic for more information on TLP schema.



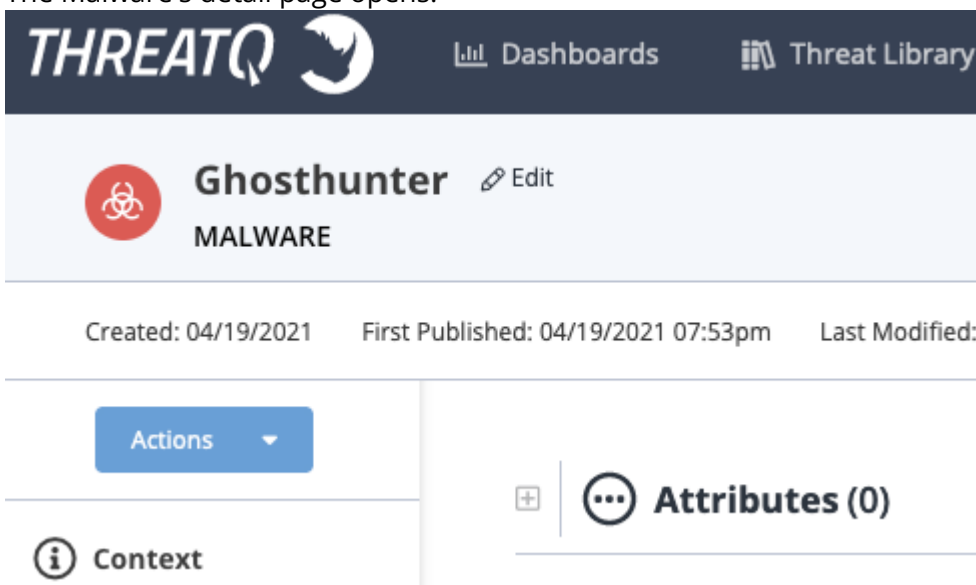
5. Select any **Related Objects** you need to link to the Malware. This field is optional.
6. Click **Add Malware**.

Adding Context

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

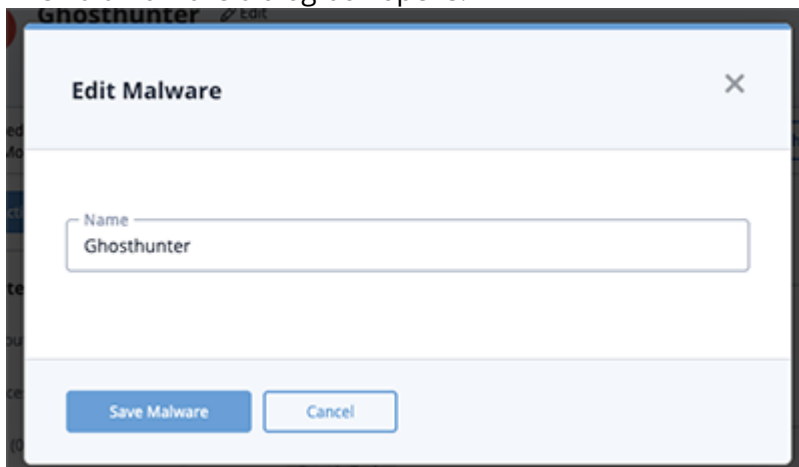
Editing a Malware Object

1. Locate and click on the Malware.
The Malware's detail page opens.



2. Click on **Edit** next to the Malware's name.

The Edit Malware dialog box opens.

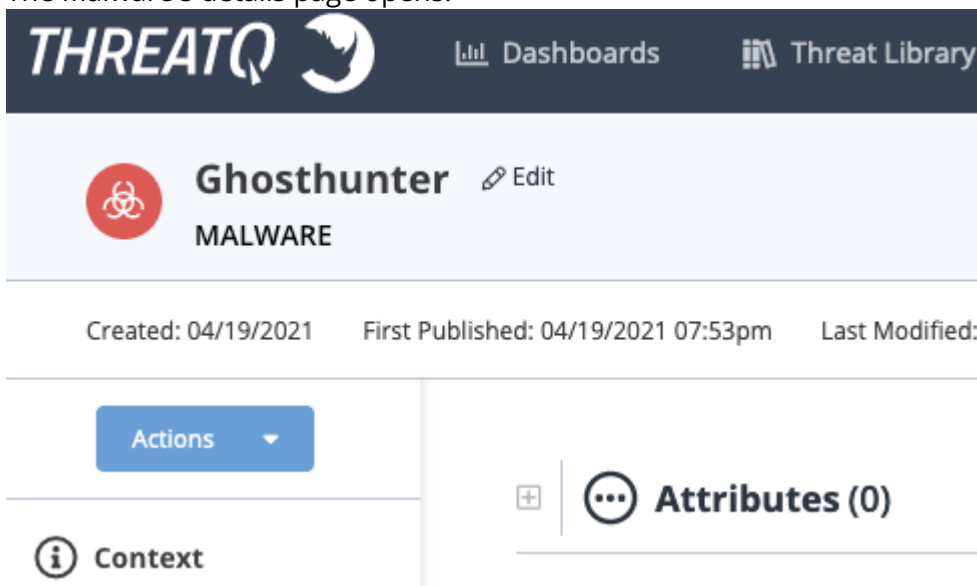


3. Make the desired change to the Malware name and click **Save Malware**.

Deleting a Malware Object

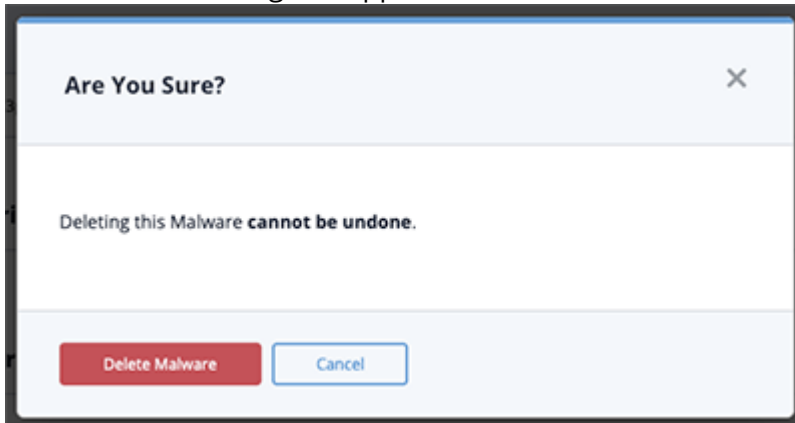
1. Locate and click on the Malware.

The Malware's details page opens.



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

A confirmation dialog box appears.



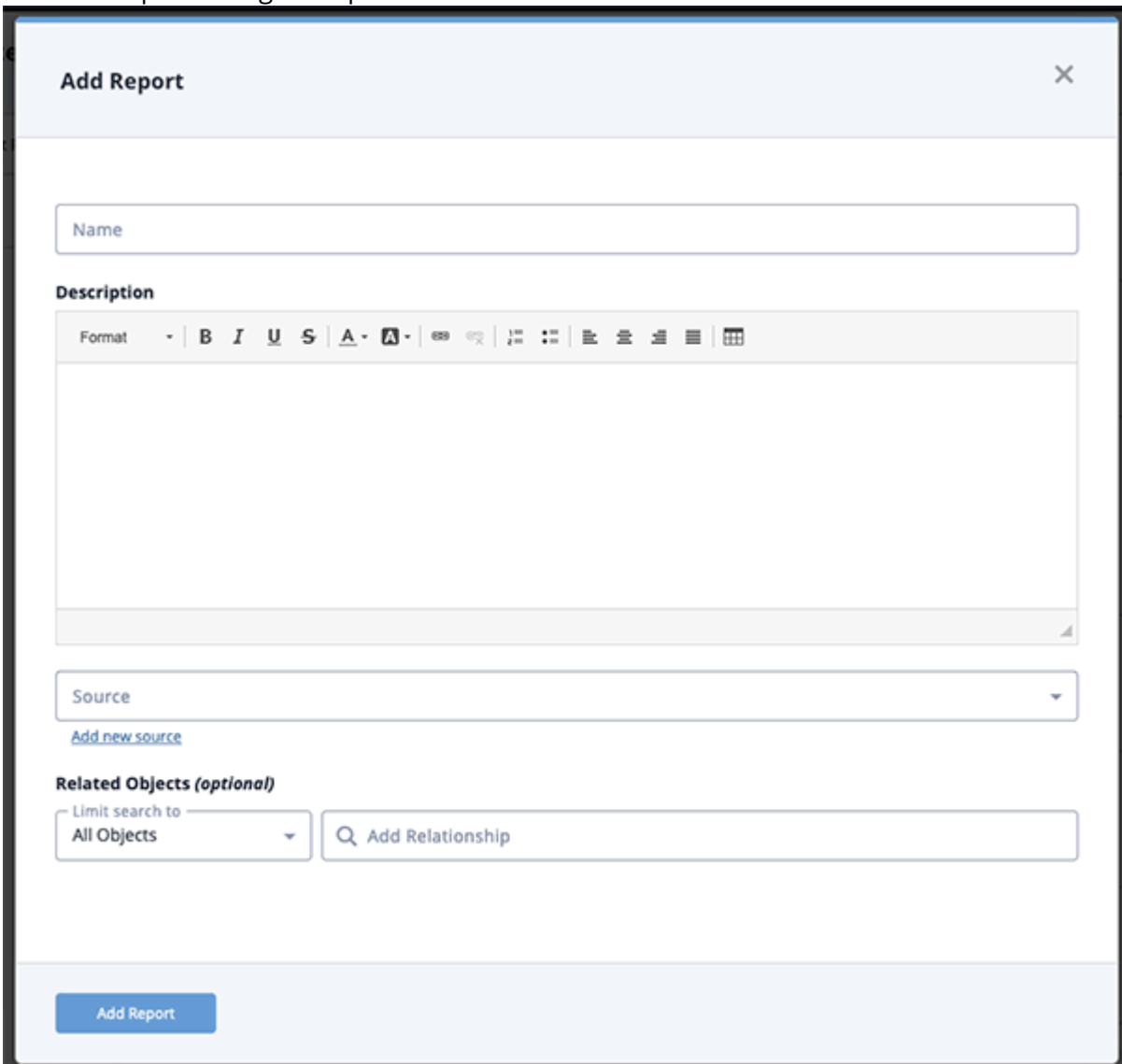
3. Click on **Delete Malware**.

Reports

Report contain information and related details for a specific threat such as Malware .
Use the steps below to create, edit and delete a Report.

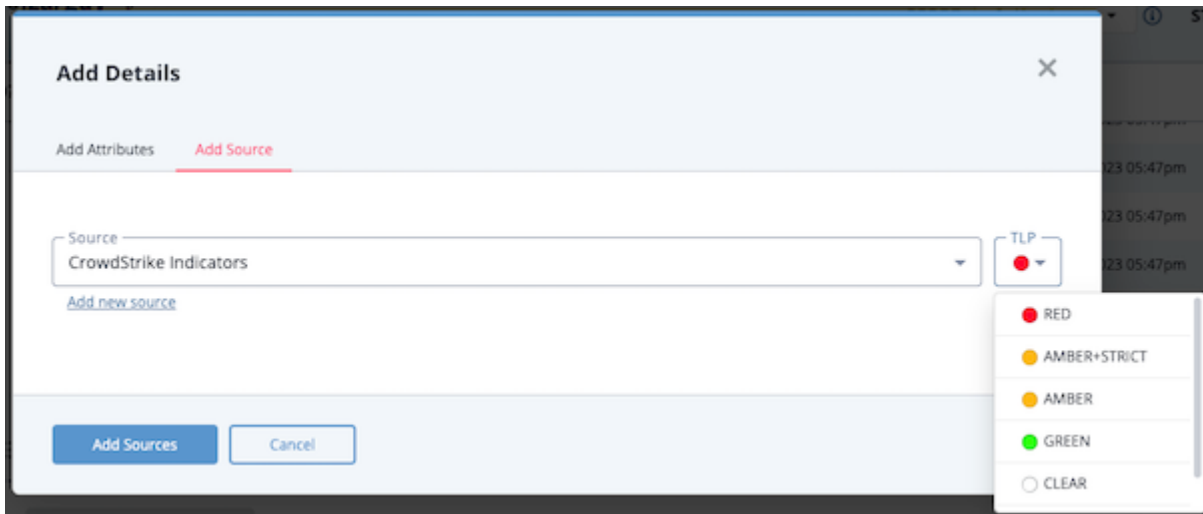
Adding a Report

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



2. Enter a name.
3. Enter a description in the field provided.
4. Select a **Source** from the dropdown provided.
You can also click the **Add a New Source** option if the desired source is not listed in the drop-down list. If administrators have enabled TLP view settings, you can select a TLP label for the

new source in the dropdown list provided. See the Traffic Light Protocol (TLP) topic for more information on TLP schema.



5. Select any **Related Objects** you need to link to the Report. This field is optional.
6. Click **Add Report**.

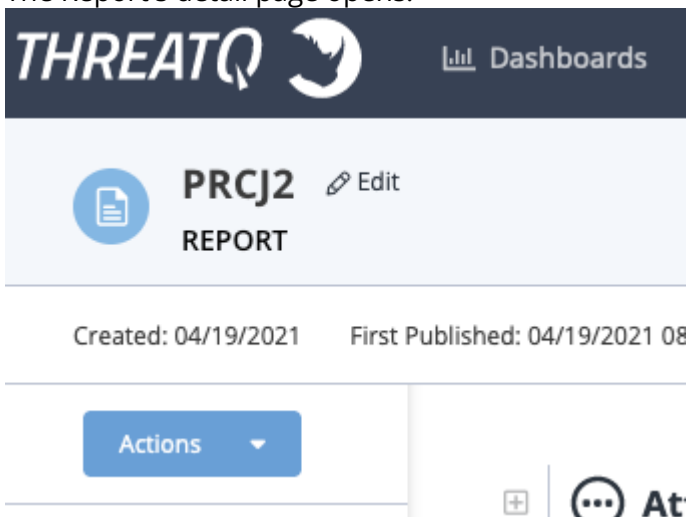
Adding Context

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

Editing a Report

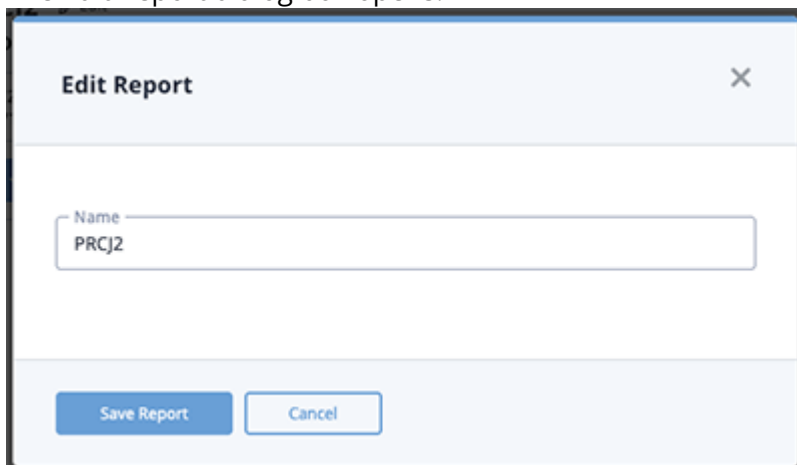
1. Locate and click on the Report.

The Report's detail page opens.



2. Click on **Edit** next to the Report's name.

The Edit Report dialog box opens.



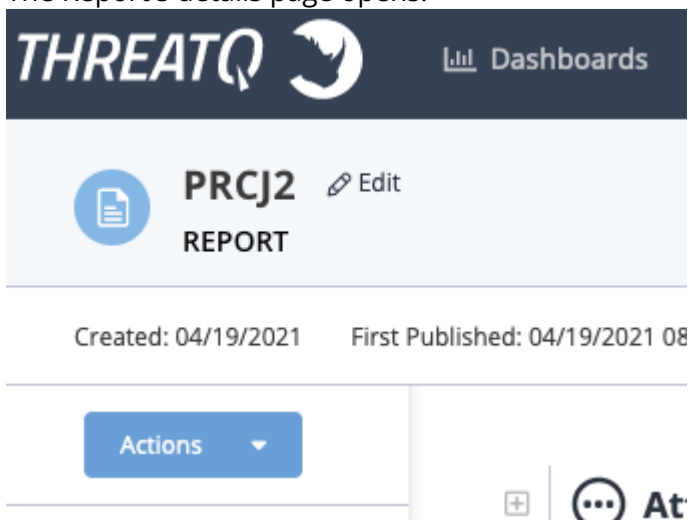
The dialog box is titled "Edit Report" and has a close button (X) in the top right corner. It contains a text input field labeled "Name" with the value "PRCJ2". At the bottom, there are two buttons: "Save Report" and "Cancel".

3. Make the desired change to the Report name and click **Save Report**.

Deleting a Report

1. Locate and click on the Report.

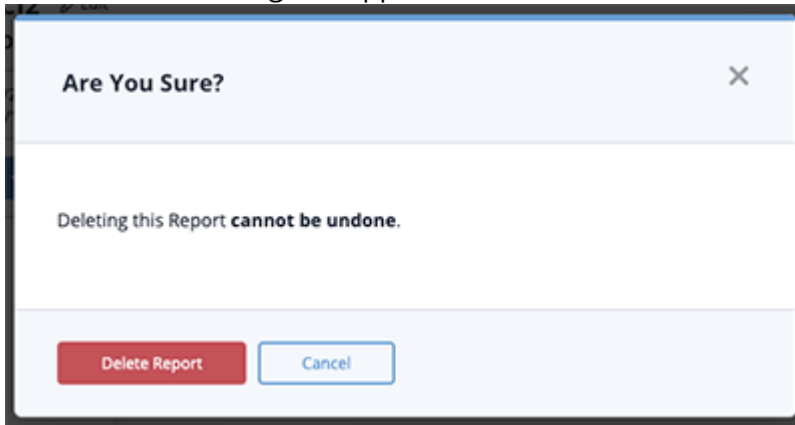
The Report's details page opens.



The page shows the ThreatQ logo and a "Dashboards" link in the top navigation bar. Below this, there is a section for the report "PRCJ2" with a document icon and an "Edit" link. The report is labeled "REPORT". Below this, it shows the creation and publication dates: "Created: 04/19/2021" and "First Published: 04/19/2021 08". At the bottom, there is an "Actions" dropdown menu and a "At" button.

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

A confirmation dialog box appears.



3. Click on **Delete Report**.

Signatures

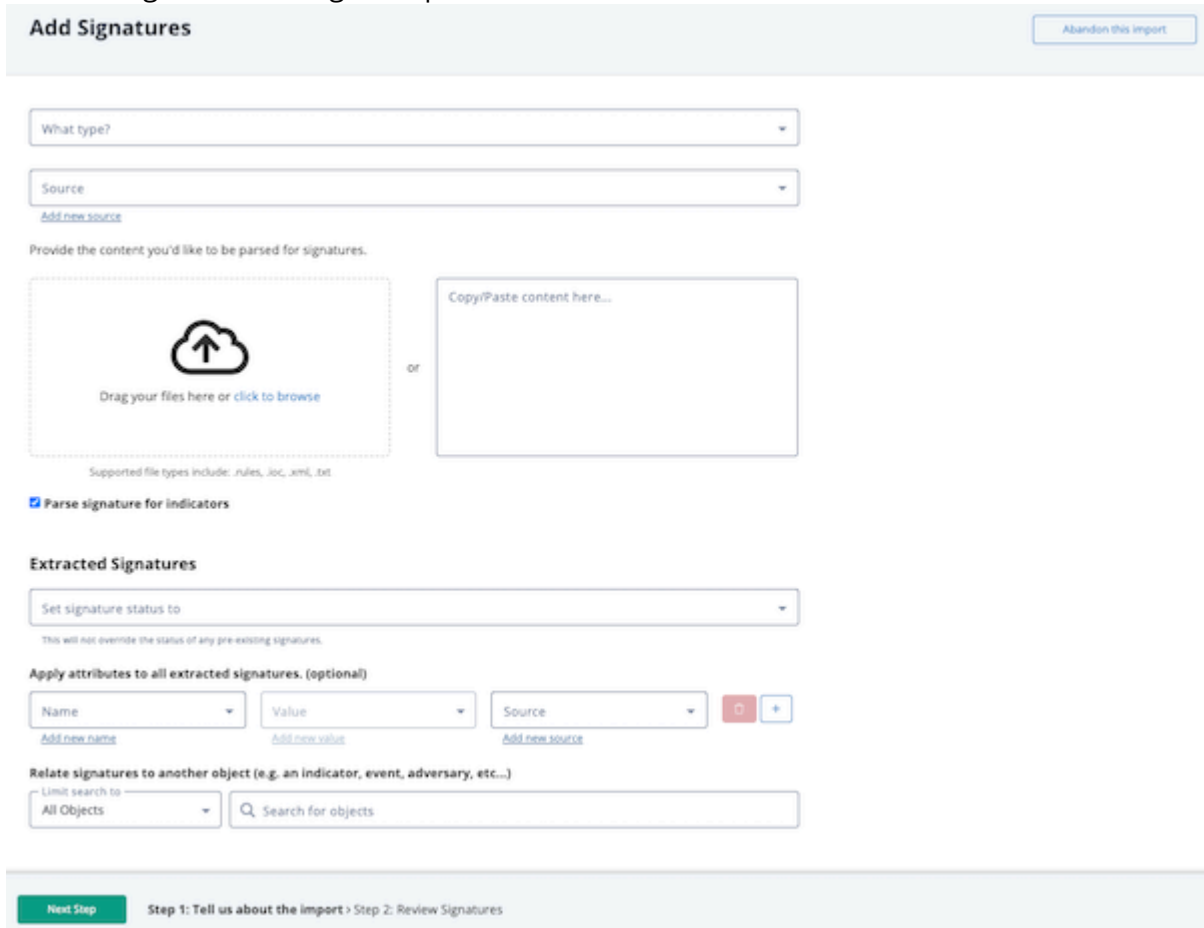
Signatures contain the blueprints or patterns associated with a malicious attack on a network or system.

ThreatQ provides you with the ability to ingest and manage Signatures, such as Snort, YARA, and OpenIOC. While importing, ThreatQ parses the signature file for Indicators to add. Once signatures are included in your deployment, you can add contextual information and correlate them with Indicator, Events, Adversary, and Files.

Adding a Signature

1. From the main menu, choose **Create > Signature**.

The Add Signatures dialog box opens.



2. Choose the type of signature from the dropdown.
3. Select a **Source** from the dropdown provided.
You can also click the **Add a New Source** option if the desired source is not listed in the dropdown list. If administrators have enabled TLP view settings, you can select a TLP label for the new source in the dropdown list provided. See the [Traffic Light Protocol \(TLP\)](#) topic for more information on TLP schema.

4. Do one of the following:
 - Drag your file(s) into the left pane.
 - Click click to browse, and locate the file you wish to upload.
 - Copy/paste content into the right pane.
5. Optionally, select to parse the signature for indicators.
6. Choose a **Signature Status** from the drop-down menu.
7. Optionally, **Apply attributes to all extracted signatures:**
 - Select an **Attribute Type**.
 - Enter an **Attribute Value**.
 - Enter an **Attribute Source**.



You can click on the **Add** icon for additional attributes.

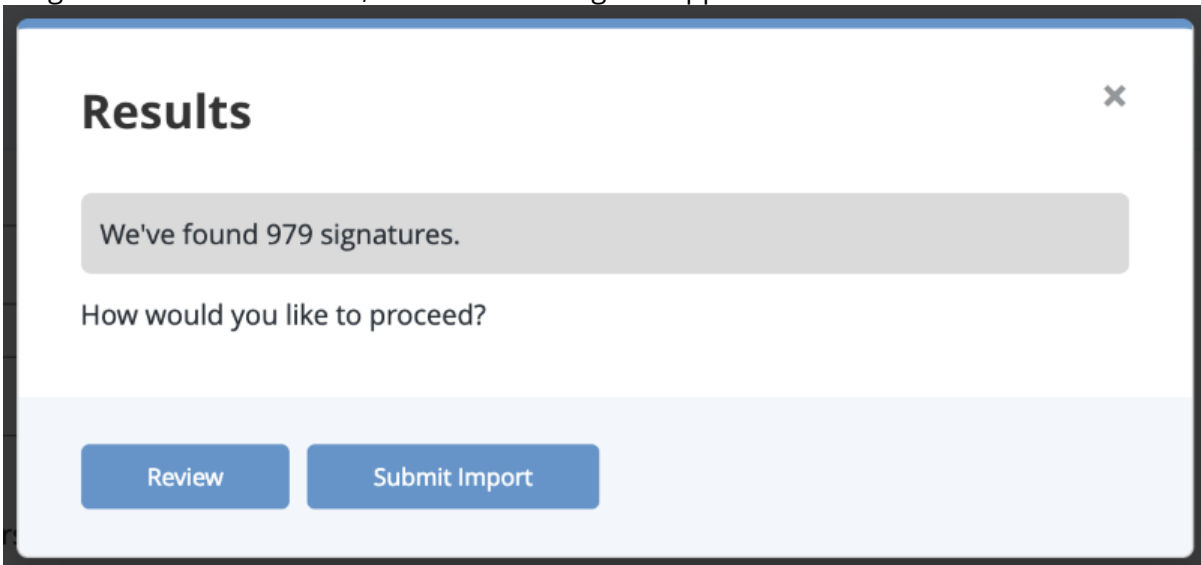
8. Optionally, relate the signature to another object by entering the object in the **Relate signatures to another object** field.



If you enter an object name that is not found, you can click the **Create** link to add the new object. If you limit your search to a specific object type, you are linked to the corresponding form. For example, if you limit your search to Adversaries, the **Create** link opens the Add An Adversary form. If you leave the **Limit search to** field set to All Objects, you can select the object type you want to create from a drop-down list.

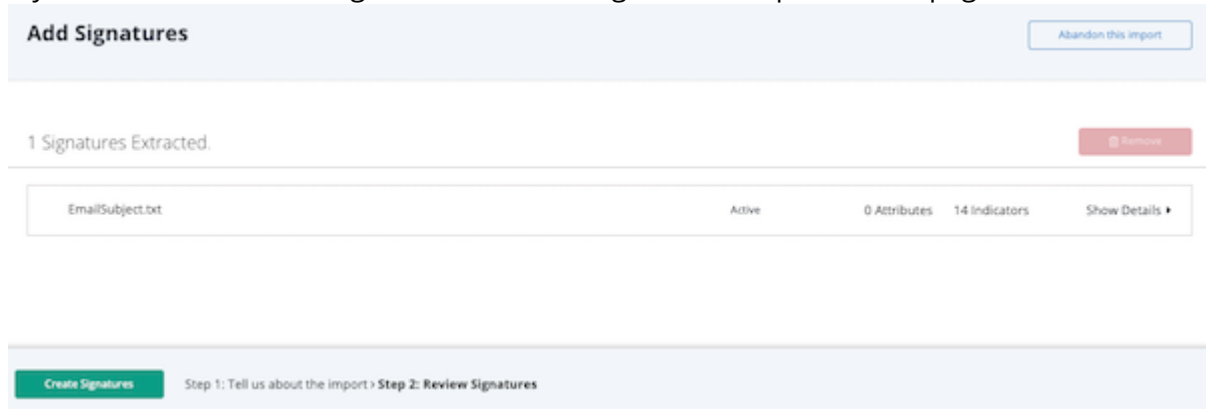
9. Click **Next Step**.

If signatures are discovered, the Results dialog box appears.



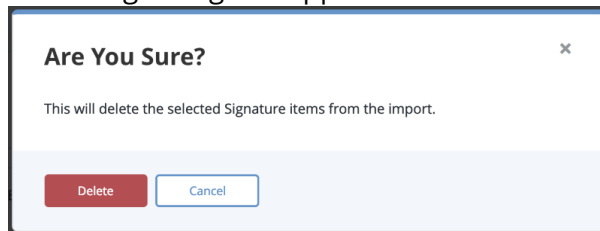
10. You can either select **Submit Import** to finish adding the signatures or **Review** to customize what data is imported.

If you selected to review signatures, the Add Signatures Step 2: Review page loads.



11. Select one or more signatures and click **Delete**.
12. Click on **Show Details** for a signature to review individual items in a signature. Use the checkboxes to select unwanted signature items and click **Delete**.

A warning dialog box appears.



13. Click **Delete** to remove the unwanted items.
14. Click **Create Signatures** when finished.

STIX

About STIX



ThreatQ supports STIX 1.1.1, STIX 1.2 and STIX 2.0.

Although the ThreatQ STIX parser does not support version 2.1, it will parse 2.1 files in the same manner as 2.0 files. As such, it does not parse out any object types introduced in STIX 2.1, such as Opinions.

ThreatQ allows you to ingest and manage STIX files. You can ingest STIX data in two ways:

- You can set up a STIX/TAXII Feed.
- You can upload a STIX file or insert STIX data to parse for indicators.

ThreatQ STIX Object Types

STIX integration provides ThreatQ with the following additional object types.

- Campaign
- Courses of Action
- Exploit Target
- Incident
- TTP objects
- Identity (STIX 2.0)
- Report (STIX 2.0)
- Vulnerability (STIX 2.0)

These objects enable better understanding and communication of STIX data. STIX data will be mapped to these objects and existing objects in the system.

Parsing a STIX File for Indicators

ThreatQ allows you to upload a STIX file or insert STIX data to parse for indicators.

1. Click the **Create** button, located at the top of the dashboard and select **STIX Parser** under the *Import* heading.
The Parse for Intelligence window is displayed.
2. Do one of the following:
 - Drag your file(s) into the left pane.
 - Click on **Click to Browse**, and locate the file you wish to upload.
 - Copy/paste the content in the right pane.
3. The **Normalize URL Indicators** check box defaults to checked. You can click the check box to unselect it or leave it checked. See [Indicator URL Normalization](#) for more information.
4. Click the **Next Step** button.



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

5. Populate the following fields:

FIELD	REQUIRED	DESCRIPTION
Name	Y	Enter the name of your import file.
Source	Y	Select a Source from the dropdown menu provided.  You can also click the Add a New Source option if the desired source is not listed in the dropdown list . If administrators have enabled TLP view settings, you can select a TLP label for the new source in the dropdown list provided. See the Traffic Light Protocol (TLP) topic for more information on TLP schema.
Select a status	Y	Select a Status to be applied to the imported objects.
Add attributes	N	Select Attributes to be assigned to the imported objects.
Add comment	N	Add a comment to the imported objects.
Add relationships	N	Add Relationships for the imported objects.  If you enter an object name that is not found, you can click the Create link to add the new object. If you limit your search to a specific object type, you are linked to the corresponding form. For example, if you limit your search to Adversaries, the Create link opens the Add An Adversary form. If you leave the Limit search to field set to All Objects, you can select the object type you want to create from a drop-down list.

Tags

N

Enter any **Tags** that should be applied to the imported objects.

6. Click the **Submit** button.

New objects will become available in the Threat Library.

STIX 1.1.1, 1.2 Data Mapping

You can click on the expand icon located to top-right of this topic to expand and collapse all mapping tables below.

- *Threat Actors Mapping*

STIX FIELD	THREATQ FIELD MAPPING	THREATQ NAME
Identity	Adversary.value	
ID	Adversary.attribute	STIX Reference ID
Title	Adversary.value	
Type	Adversary.attribute	Type
Timestamp	Adversary.published_at	
Description	Adversary.attribute	Description
Motivation	Adversary.attribute	Motivation
Sophistication	Adversary.attribute	Sophistication
Intended_Effect	Adversary.attribute	Intended Effect
Role	Adversary.attribute	Role
Confidence	Adversary.attribute	Confidence
Handling	Adversary.tlp	
Observed_TTPs	TTP	
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
	Indicator.attribute.source	
Related_Observables		
Related_Indicators	Indicator	
Related_Campaigns	Campaign	
	Signature	
	Signature.type = "Snort"	
	Signature.value	
	Indicator.source	
	Course of Action	
	Indicator.attribute	Start Time
	Indicator.attribute	End Time
	Indicator.published_at	

- *Exploit Target Mapping*

STIX FIELD	THREATQ FIELD MAPPING	THREATQ NAME
Title	Exploit Target.value	
ID	Exploit Target.attribute	STIX Reference ID
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	
	TTP.attribute	Persona
Victim Targeting	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

STIX 2.0 Data Mapping



Although the ThreatQ STIX parser does not support version 2.1, it will parse 2.1 files in the same manner as 2.0 files. As such, it does not parse out any object types introduced in STIX 2.1, such as Opinions.

You can click on the expand icon located to top-right of this topic to expand and collapse all mapping tables below.

- *Attack Patterns Mapping*

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
created	Attack Pattern.Published_at	
description	Attack Pattern.Attribute	Description
external_references[]	See External References	
kill_chain_phases.[]e	See Kill Chain Table	
modified	Attack Pattern.Attribute	Modified At
name	Attack Pattern.Value	
revoked (if revoked == true)	Attack Pattern.Attribute	Revoked
labels	Attack Pattern.Attribute	Label

- *Threat Actors Mapping*

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
aliases	Adversary	* The Adversary created will have all the same attributes and published_at as the base Attribute. All alias Adversaries will be inter-related

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
created	Adversary.Published_At	
goals	Adversary.Attribute	Goal
labels	Adversary.Attribute	Label
modified	Adversary.Attribute	Modified At
name	Adversary.Value	
primary_motivation	Adversary.Attribute	Primary Motivation
resource_level	Adversary.Attribute	Resource Level
roles	Adversary.Attribute	Role
secondary_motivation	Adversary.Attribute	Secondary Motivation
sophistication	Adversary.Attribute	Sophistication
revoked (if revoked == true)	Adversary.Attribute	Revoked
external_references[]	See External References	
personal_motivations	Adversary.Attribute	Personal Motivation

- *Indicators Mapping*

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
created	Signature.Published_at	

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
description	Signature.Description	
external_references[]	See External References	
labels	Signature.Attribute	Label
modified	Signature.Attribute	Modified At
name	Signature.Name	ThreatQ will default to using Indicator Pattern as the signature name if a name is not provided.
pattern	Signature.Value	
	Signature.Type	Indicator Pattern
valid.from	Signature.Attribute	Valid From
valid.until	Signature.Attribute	Valid Until
revoked (if revoked == true)	Signature.Attribute	Revoked
kill_chain_phases.[]	See Kill Chain Table	

ThreatQ Indicator and / or Event objects based on the Observables Mapping may be derived from the `pattern` field and related back to the resulting Signature.

- *Identities Mapping*

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
contact_information	Identity.Contact_Information	

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
created	Identity.Published_at	
description	Identity.Description	
external_references[]	See External References	
identity_class	Identity.Attribute	Identity Class
modified	Identity.Attribute	Modified At
name	Identity.Value	
sectors	Identity.Attribute	Sector
labels	Identity.Attribute	Label
revoked (if revoked == true)	Identity.Attribute	Revoked

- *Observables Mapping*

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
created	Observable.Published_at	
modified	Observable.Attribute	Modified At
revoked (if revoked == true)	Observable.Attribute	Revoked
external_references	Observable.Attribute	External Reference See External References .
number_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.

1. *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	

2. *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

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
rir	Indicator.Attribute	Regional Internet Registry

3. *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	

4. *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	

5. *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

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
value	Indicator.Value	
belongs_to_ref[]	Indicator.relationship	

6. *Email Message Mapping*

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
type: email-message	Event.Type Indicator.Type	Spearphish Email Subject
subject**	Event.Title Indicator.Value	
is_multipart	Indicator.Attribute	Is Multipart
date (if parsing as an event)* sent date (if parsing as an indicator)	Event.happened_at Indicator.Attribute	
content_type	Indicator.Attribute	Content Type
from_ref	Event.Relationship Indicator.Relationship	From
sender_ref	Event.Relationship Indicator.Relationship	Sender
to_refs	Event.Relationship Indicator.Relationship	To
cc_refs	Event.Relationship	CC
bcc_refs	Event.Relationship Indicator.Relationship	BCC

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
received_lines	Event.Attribute Indicator.Attribute	Received Lines
additional_header_fields	Event.Attribute Indicator.Attribute	Additional Header - {key} An attribute is created for each key-value pair of the additional_header_fields object.
body	Event.Attribute Indicator.Attribute	Body
body_multipart[].body_raw_ref***	Indicator	Filename
raw_email_ref	Event.Relationship Indicator.Relationship	

* To parse an event from an email message, the email must have a **date** and **subject** field.

** To parse an indicator from an email message, the email must contain a **subject** field.

*** 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 .

7. File Mapping

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
type: file	Indicator.Type	Filename

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
size	Indicator.Attribute	File Size
hashes{}		
hashes{}.key	Indicator.Type	MD5 / SHA-1 / SHA-256 / SHA-384 / SHA-512 / Fuzzy Hash
hashes{}.value	Indicator.Value	
name	Indicator.Value	
name_enc	Indicator.Attribute	File Name Encoding
magic_number_hex	Indicator.Attribute	Magic Number Hex
mime_type	Indicator.Attribute	MIME Type
created	Indicator.Attribute	Created At
accessed	Indicator.Attribute	Last Accessed
parent_directory_ref	Indicator.Relationship	
is_encrypted	Indicator.Attribute	Encrypted
encryption_algorithm	Indicator.Attribute	Encryption Algorithm

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
decryption_key	Indicator.Attribute	Decryption Key
contains_refs[]	Indicator.Relationship	
content_ref	Indicator.Relationship	
extensions.archive-ext.contains_refs[]	Indicator.Relationship	
extensions.archive-ext.version	Indicator.Attribute	Archive Version
extensions.archive-ext.comment	Indicator.Attribute	Archive File Comment
extensions.ntfs-ext.sid	Indicator.Attribute	Security ID
extensions.ntfs-ext.alternate_data_streams[].hashes{}		
extensions.ntfs-ext.alternate_data_streams[].hashes{}.key	Indicator.Type	MD5 / SHA-1 / SHA-256 / SHA-384 / SHA-512 / Fuzzy Hash
extensions.ntfs-ext.alternate_data_streams[].hashes{}.value	Indicator.Value	
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

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
extensions.pdf-ext.version	Indicator.Attribute	PDF Specification Version
extensions.pdf-ext.is_optimized	Indicator.Attribute	PDF Is Optimized
extensions.pdf-ext.document_info_dict{}.key/value	Indicator.Attribute	Formatted as: 'PDF {key.title()}'
extensions.pdf-ext.pdfid0	Indicator.Attribute	PDF First File Identifier
extensions.pdf-ext.pdfid1	Indicator.Attribute	PDF Second File Identifier
extensions.raster-image-ext.image_height	Indicator.Attribute	Image Height
extensions.raster-image-ext.image_width	Indicator.Attribute	Image Width
extensions.raster-image-ext.bits_per_pixel	Indicator.Attribute	Image Bits Per Pixel
extensions.raster-image-ext.image_compression_algorithm	Indicator.Attribute	Image Compression Algorithm
extensions.raster-image-ext.exif_tags{}.key/value	Indicator.Attribute	Formatted as: 'Image EXIF {key.title()}'
extensions.windows-pebinary-ext.pe_type	Indicator.Attribute	Executable Extension Type

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
extensions.windows-pebinary-ext.imphash	Indicator.Attribute	Executable Imphash
extensions.windows-pebinary-ext.machine_hex	Indicator.Attribute	Target Machine Hex
extensions.windows-pebinary-ext.number_of_sections	Indicator.Attribute	PE Binary Section Count
extensions.windows-pebinary-ext.time_date_stamp	Indicator.Attribute	PE Binary Created Date
extensions.windows-pebinary-ext.pointer_to_symbol_table_hex	Indicator.Attribute	Symbol Table Hex Offset
extensions.windows-pebinary-ext.number_of_symbols	Indicator.Attribute	PE Binary Symbol Table Size
extensions.windows-pebinary-ext.size_of_optional_header	Indicator.Attribute	PE Binary Optional Header Size
extensions.windows-pebinary-ext.characteristics_hex	Indicator.Attribute	PE Binary Characteristics Hex
extensions.windows-pebinary-ext.file_header_hashes{}		
extensions.windows-pebinary-ext.file_header_hashes{}.key	Indicator.Type	MD5 / SHA-1 / SHA-256 / SHA-384 / SHA-512 / Fuzzy Hash

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
extensions.windows-pebinary-ext.file_header_hashes{}.value	Indicator.Value	
extensions.windows-pebinary-ext.optional_header.magic_hex	Indicator.Attribute	PE Binary Magic Hex
extensions.windows-pebinary-ext.optional_header.major_linker_version	Indicator.Attribute	PE Binary Major Linker Version
extensions.windows-pebinary-ext.optional_header.minor_linker_version	Indicator.Attribute	PE Binary Minor Linker Version
extensions.windows-pebinary-ext.optional_header.size_of_code	Indicator.Attribute	PE Binary Code Size
extensions.windows-pebinary-ext.optional_header.size_of_initialized_data	Indicator.Attribute	PE Binary Initialized Data Size
extensions.windows-pebinary-ext.optional_header.size_of_uninitialized_data	Indicator.Attribute	PE Binary Uninitialized Data Size
extensions.windows-pebinary-ext.optional_header.address_of_entry_point	Indicator.Attribute	PE Binary Memory Address Entry Point
extensions.windows-pebinary-ext.optional_header.base_of_code	Indicator.Attribute	PE Binary Base Code Memory Address

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
extensions.windows-pebinary-ext.optional_header.base_of_data	Indicator.Attribute	PE Binary Base Data Memory Address
extensions.windows-pebinary-ext.optional_header.image_base	Indicator.Attribute	PE Binary Base Image Memory Address
extensions.windows-pebinary-ext.optional_header.section_alignment	Indicator.Attribute	PE Binary Section Alignment Bytes
extensions.windows-pebinary-ext.optional_header.file_alignment	Indicator.Attribute	PE Binary Image File Alignment Bytes
extensions.windows-pebinary-ext.optional_header.major_os_version	Indicator.Attribute	Windows OS Major Version
extensions.windows-pebinary-ext.optional_header.minor_os_version	Indicator.Attribute	Windows OS Minor Version
extensions.windows-pebinary-ext.optional_header.major_image_version	Indicator.Attribute	Image Major Version
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

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
extensions.windows-pebinary-ext.optional_header.minor_subsystem_version	Indicator.Attribute	Subsystem Minor Version
extensions.windows-pebinary-ext.optional_header.win32_version_value_hex	Indicator.Attribute	Win32 Version Hex
extensions.windows-pebinary-ext.optional_header.size_of_image	Indicator.Attribute	Image Byte Size
extensions.windows-pebinary-ext.optional_header.size_of_headers	Indicator.Attribute	PE Binary Combined Header Size
extensions.windows-pebinary-ext.optional_header.checksum_hex	Indicator.Attribute	PE Binary Checksum Hex
extensions.windows-pebinary-ext.optional_header.subsystem_hex	Indicator.Attribute	PE Binary Required Subsystem Hex
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

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
extensions.windows-pebinary-ext.optional_header.size_of_heap_commit	Indicator.Attribute	Heap Space Commit Size
extensions.windows-pebinary-ext.optional_header.loader_flags_hex	Indicator.Attribute	Loader Flags Hex
extensions.windows-pebinary-ext.optional_header.number_of_rva_and_sizes	Indicator.Attribute	Number of RVA and Sizes
extensions.windows-pebinary-ext.optional_header.hashes{}		
extensions.windows-pebinary-ext.optional_header.hashes{}.key	Indicator.Type	MD5 / SHA-1 / SHA-256 / SHA-384 / SHA-512 / Fuzzy Hash
extensions.windows-pebinary-ext.optional_header.hashes{}.value	Indicator.Value	
extensions.windows-pebinary-ext.sections[].hashes{}		
extensions.windows-pebinary-ext.sections[].hashes{}.key	Indicator.Type	MD5 / SHA-1 / SHA-256 / SHA-384 / SHA-512 / Fuzzy Hash
extensions.windows-pebinary-ext.sections[].hashes{}.value	Indicator.Value	
extensions.windows-pebinary-ext.sections[].name	Indicator.Attribute	PE Binary Section Name

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ 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

8. IPv4 Mapping

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
type: ipv4-addr	Indicator.Type	CIDR Block (if value contains a / and does not end with /32) IP Address (if the value ends with /32, the /32 is omitted and reported as an IP Address)
value	Indicator.Value	
resolves_to_refs[]	Indicator.Relationship	
belongs_to_refs[]	Indicator.Relationship	

9. 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	

10. MAC Mapping

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
type: mac-addr	Indicator.Type	MAC Address
value	Indicator.Value	

11. *Mutex Mapping*

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
type: mutex	Indicator.Type	Mutex
name	Indicator.Value	

12. *URL Mapping*

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
type: url	Indicator.Type	URL
value	Indicator.Value	

13. *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

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
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
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

14. *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

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
external_references[]	See External References	

labels

Campaign.Attribute

Label

- Courses of Action Mapping*

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
created	Course of Action.Published_at	
modified	Course of Action.Attribute	Modified At
name	Course of Action.Value	
description	Course of Action.Description	
action		
revoked (if revoked == true)	Course of Action.Attribute	Revoked
external_references[]	See External References	
labels	Course of Action.Attribute	Label

- Intrusion Sets Mapping*

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
aliases	Intrusion Set	
created	Intrusion Set.Published_at	
description	Intrusion Set.Description	
first_seen		

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
goals	Intrusion Set.Attribute	Goal
modified	Intrusion Set.Attribute	Modified At
name	Intrusion Set.Value	
primary_motivation	Intrusion Set.Attribute	Primary Motivation
resource_level	Intrusion Set.Attribute	Resource Level
secondary_motivations	Intrusion Set.Attribute	Secondary Motivation
external_references[]	See External References	
revoked (if revoked == true)	Intrusion Set.Attribute	Revoked

- *Malware Mapping*

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
created	Malware.Published_at	
description	Malware.Description	
kill_chain_phases.[]	See Kill Chain Table	
labels	Malware.Attribute	Label
modified	Malware.Attribute	Modified At
name	Malware.Value	
external_references[]	See External References	

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
revoked (if revoked == true)	Malware.Attribute	Revoked

- *Tools Mapping*

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
created	Tool.Published_at	
modified	Tool.Attribute	Modified At
labels	Tool.Attribute	Label
name	Tool.Value	
revoked (if revoked == true)	Tool.Attribute	Revoked
external_references[]	See External References	
description	Tool.Description	
kill_chain_phases.[]	See Kill Chain Table	
tool_version	Tool.Attribute	Tool Version

- *Reports Mapping*

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
created	Report.Published_at	
modified	Report.Attribute	Modified At
name	Report.Value	
description	Report.Description	

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
labels	Report.Attribute	Label
object_refs	Report.Relationship.Link	
external_references[]	See External References	
revoked (if revoked == true)	Report.Attribute	Revoked

• *Sightings Mapping*

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
count	Event.Attribute	Count
created	Event.published_at	
first_seen	Event.happened_at	
last_seen	Event.Attribute	Last Seen
observed_data_refs	Event.relationship.link	
sighting_of_ref	Event.relationship.link	
where_sighted_refs	Event.relationship.link	
revoked (if revoked == true)	Object.attribute	Revoked
	Event.name	STIX Sighting
	Event.type	Sighting
external_references[]	See External References	

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
modified	Event.Attribute	Modified

External References

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
Object.external_references[].source_name	Object.Attribute	External Reference*
Object.external_references[].external_id	Object.Attribute	External Reference*
Object.external_references[].description	Object.Attribute	External Reference*
Object.external_references[].url	Object.Attribute	External Reference*

* Formatted as: {source_name} ({external_id}): {description} - {url}

Kill Chain Phrases

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
kill_chain_phases[].kill_chain_name	Object.Attribute	Kill Chain Name
kill_chain_phases[].phase_name	Object.Attribute	Kill Chain Phrase

Tasks

ThreatQ allows you to create and assign tasks to yourself or other users in the platform.

Once tasks are included in your deployment, you can add contextual information and correlate them with Indicator , Events , Adversary , Signatures , and Files . You can also add comments, change the task priority, change the task status, and delete the task.

Assigning a Task

Complete the following steps to assign a task in ThreatQ.

1. From the main menu, choose **Create > Task**.



The Add Task dialog box opens.

2. Enter a task **Name**.
3. Enter the assignee's email address in the **Assigned To** field.
4. Optionally, use the date picker to select a **Due Date**.
5. Select one of the following statuses:
 - To Do
 - In Progress
 - Review
 - Done
6. Select one of the following task priorities:
 - Low
 - Medium
 - High
7. Optionally, enter any **Associated Objects**.
8. Enter a **Description** for the task.
9. Click **Save**.

The assignee receives a Notification Center alert about the task. This alert includes a link to the assigned task.

Managing Tasks

After a task is created, you can manage it on the task's Details page.

The following table describes the actions you can take to manage your tasks on a Task Details page.

TO

YOU CAN...

Change task priority

Choose the **Priority** drop-down and select a new priority.

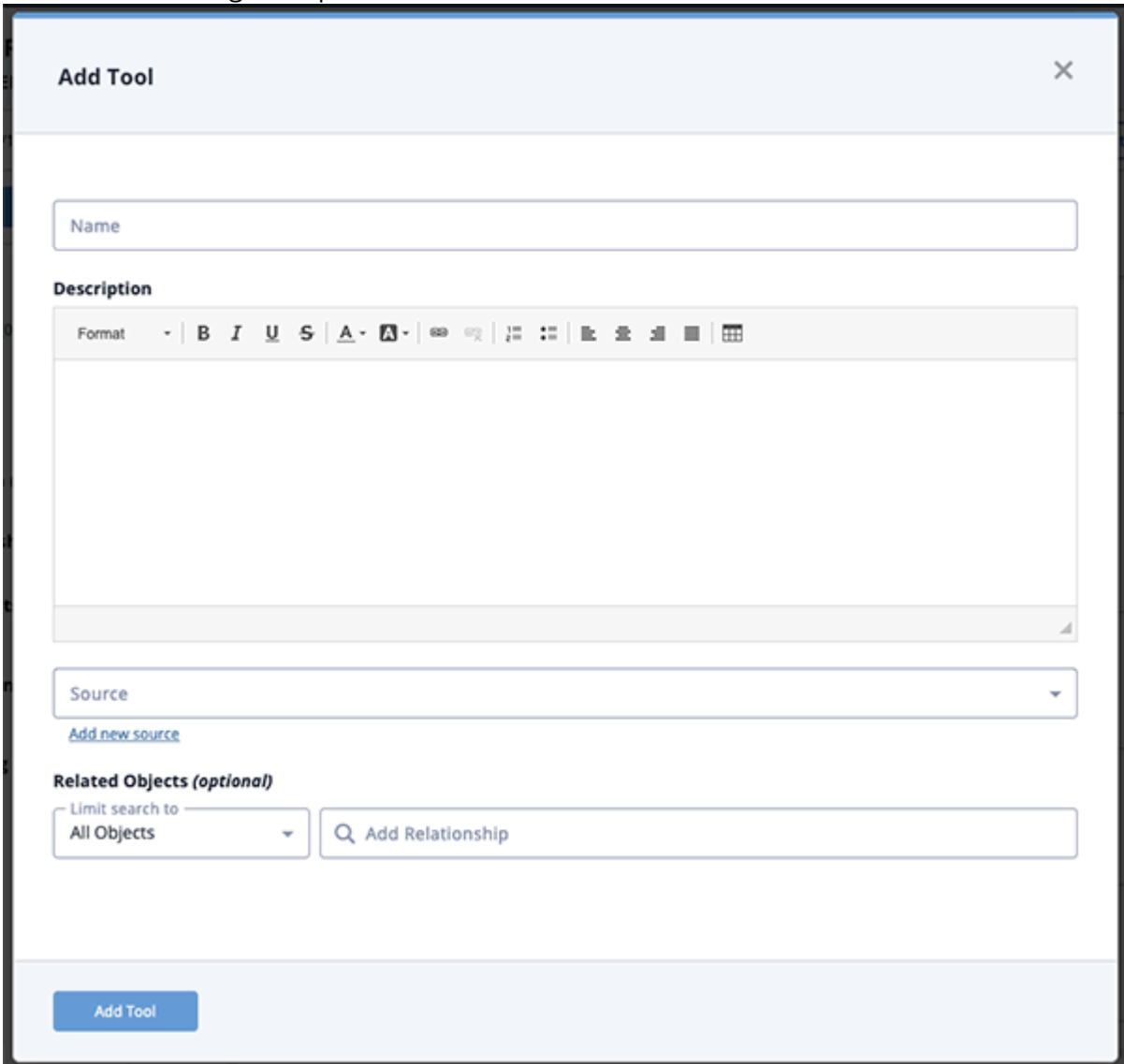
TO	YOU CAN...
Change task status	Choose the Status drop-down and select a new status.
Add Attributes, Comments, Relationships, and Sources	Choose the Add Context drop-down and select an item.
View and Add Comments	Choose Comments .
View the Audit Log	Choose Audit Log .
Request Investigation Access	1. Choose Investigations. 2. Click the related investigation to open the Access Denied window. 3. Click the Request Access button. When you click this button, the investigation owner receives a Notification Center alert indicating you have requested access to the investigation.

Tools

A Tool is a legitimate application that can be leveraged to perform malicious activities. Use the steps below to create, edit and delete a Tool.

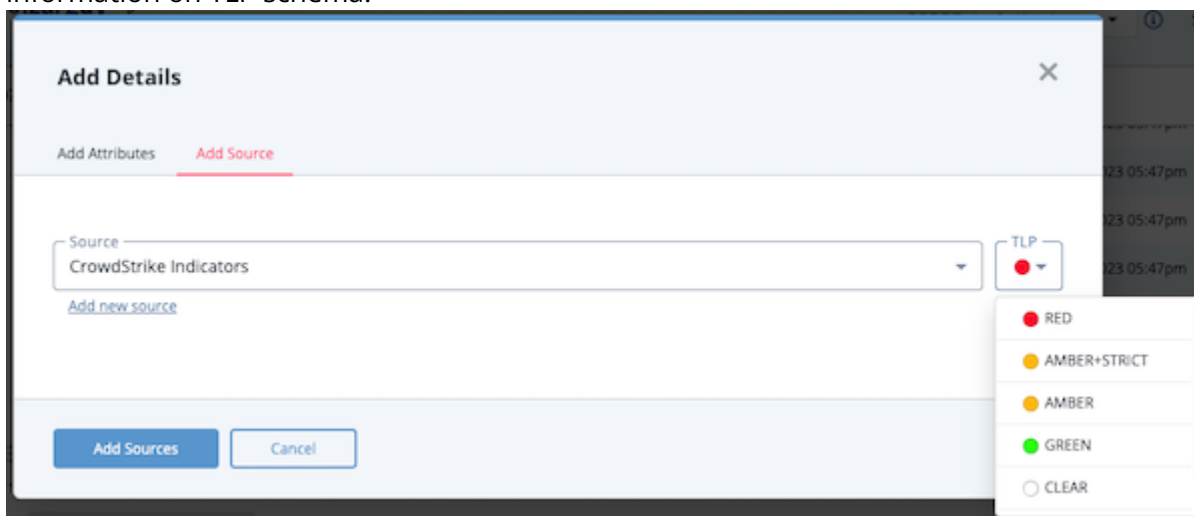
Adding a Tool

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



2. Enter a name.
3. Enter a description in the field provided.
4. Select a **Source** from the dropdown provided.
You can also click the **Add a New Source** option if the desired source is not listed in the drop-down list. If administrators have enabled TLP view settings, you can select a TLP label for the

new source in the dropdown list provided. See the Traffic Light Protocol (TLP) topic for more information on TLP schema.



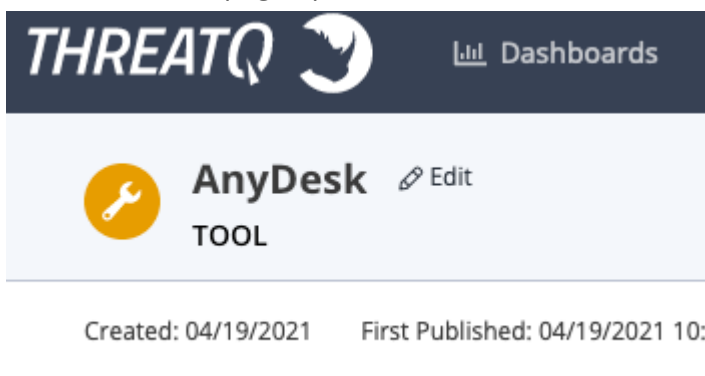
5. Select any **Related Objects** you need to link to the Tool. This field is optional.
6. Click **Add Tool**.

Adding Context

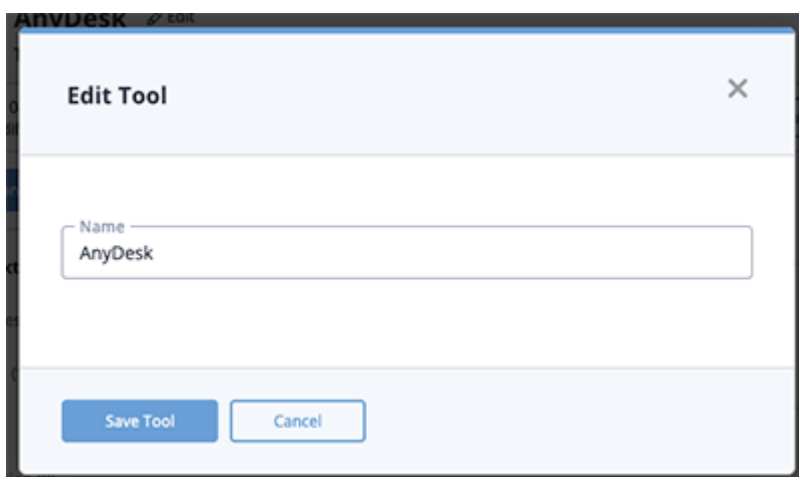
See the [About Object Details](#) section and its topics for details on adding context to an object such as adding sources, attributes, and related objects.

Editing a Tool

1. Locate and click on the Tool.
The Tool's detail page opens.



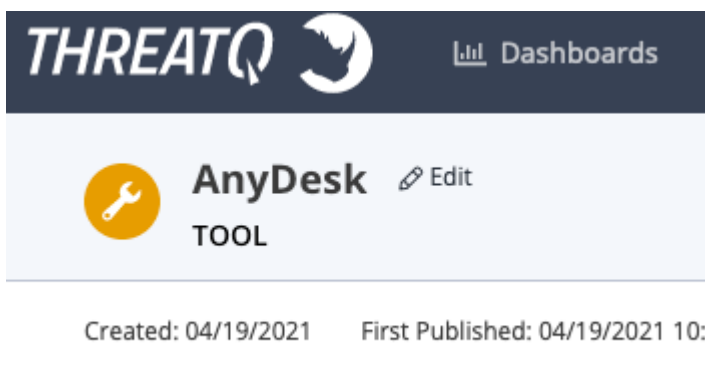
2. Click on **Edit** next to the Tool's name.
The Edit Tool dialog box opens.



3. Make the desired change to the Tool name and click **Save Tool**.

Deleting a Tool

1. Locate and click on the Tool.
The Tool's details page opens.



2. Click on the **Actions** menu and select **Delete Tool**.
A confirmation dialog box appears.



3. Click on **Delete Tool**.

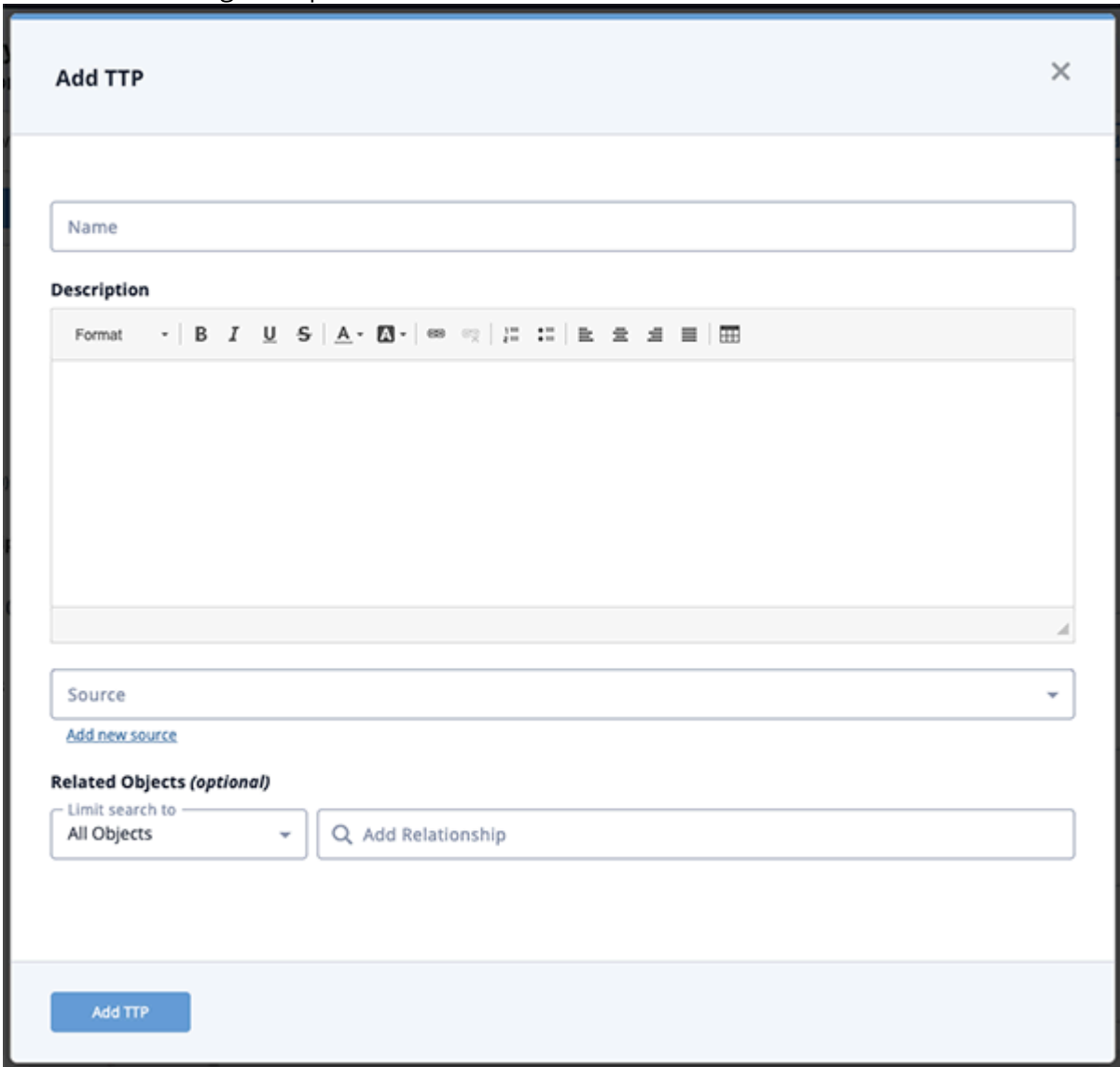
TTP

TTP, which stands for tactics, techniques, and procedures, describes how an intruder may attempt to access your system.

Use the steps below to create, edit and delete a TTP.

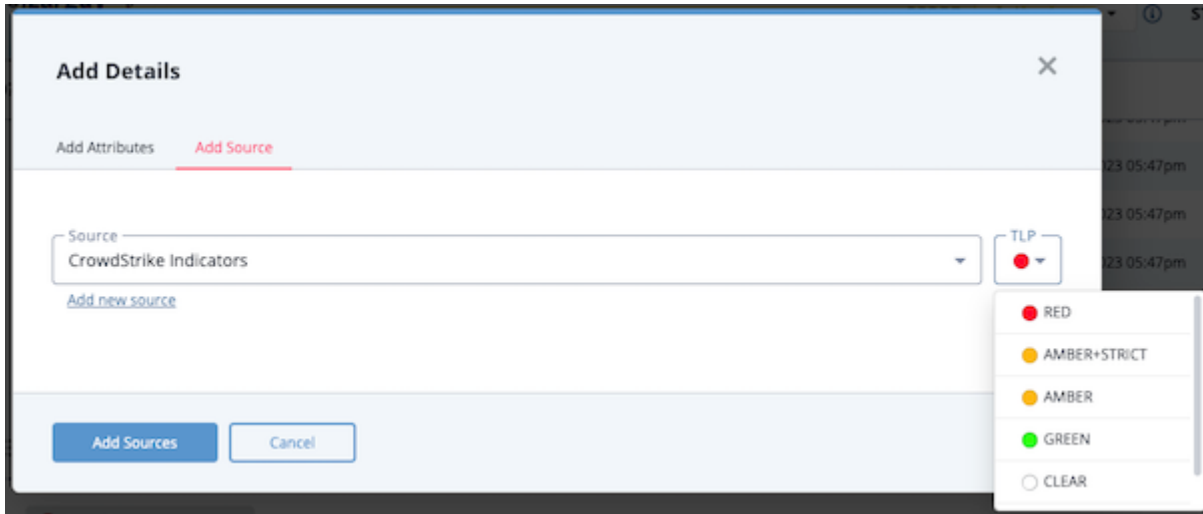
Adding a TTP

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



2. Enter a name.
3. Enter a description in the field provided.
4. Select a **Source** from the dropdown provided.

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



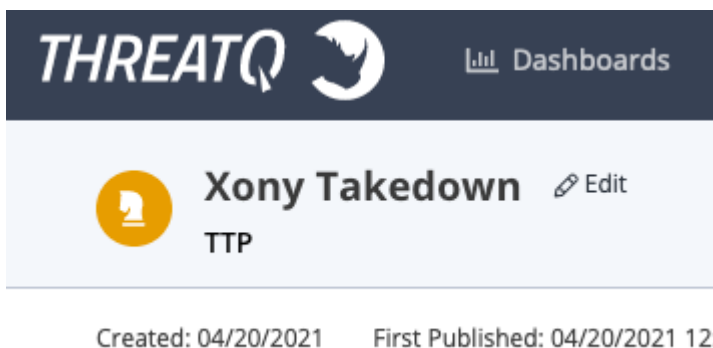
5. Select any **Related Objects** you need to link to the TTP. This field is optional.
6. Click **Add TTP**.

Adding Context

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

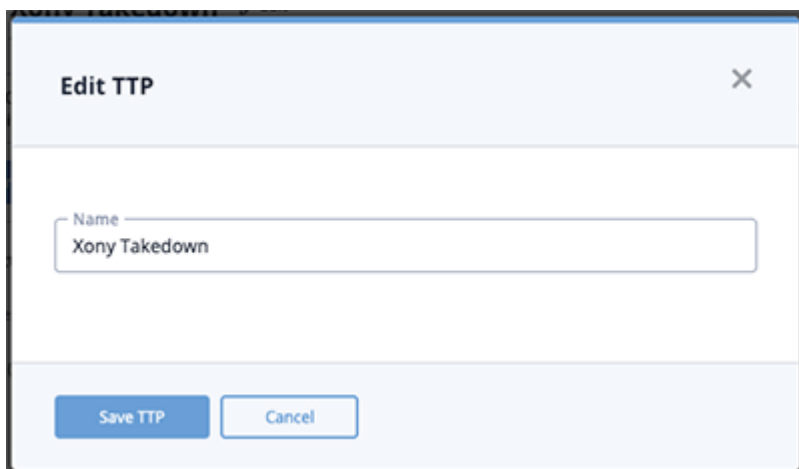
Editing a TTP

1. Locate and click on the TTP.
The TTP's detail page opens.



2. Click on **Edit** next to the TTP's name.

The Edit TTP dialog box opens.



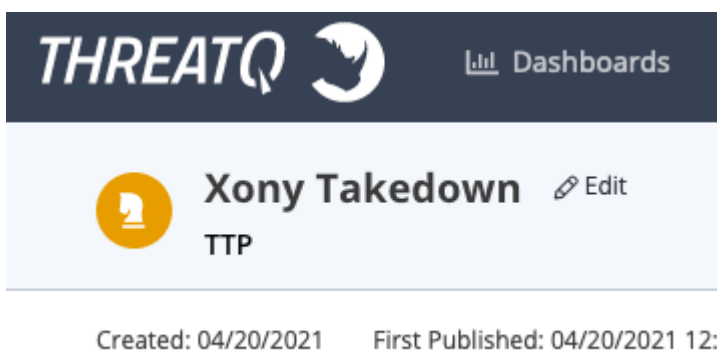
The 'Edit TTP' dialog box is shown. It has a title bar with 'Edit TTP' and a close button. Below the title bar is a text input field labeled 'Name' containing the text 'Xony Takedown'. At the bottom of the dialog are two buttons: 'Save TTP' and 'Cancel'.

3. Make the desired change to the TTP name and click **Save TTP**.

Deleting a TTP

1. Locate and click on the TTP.

The TTP's details page opens.



The details page for the 'Xony Takedown' TTP is shown. It features the ThreatQ logo and a 'Dashboards' link at the top. Below this is a section with an orange circular icon containing a white rhino, the name 'Xony Takedown', and an 'Edit' button. Underneath, it says 'TTP'. At the bottom, it shows the creation date 'Created: 04/20/2021' and the first published date 'First Published: 04/20/2021 12:00'.

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

A confirmation dialog box appears.



The 'Are You Sure?' confirmation dialog box is shown. It has a title bar with 'Are You Sure?' and a close button. Below the title bar is a message: 'Deleting this TTP cannot be undone.' At the bottom are two buttons: 'Delete TTP' (in red) and 'Cancel'.

3. Click on **Delete TTP**.

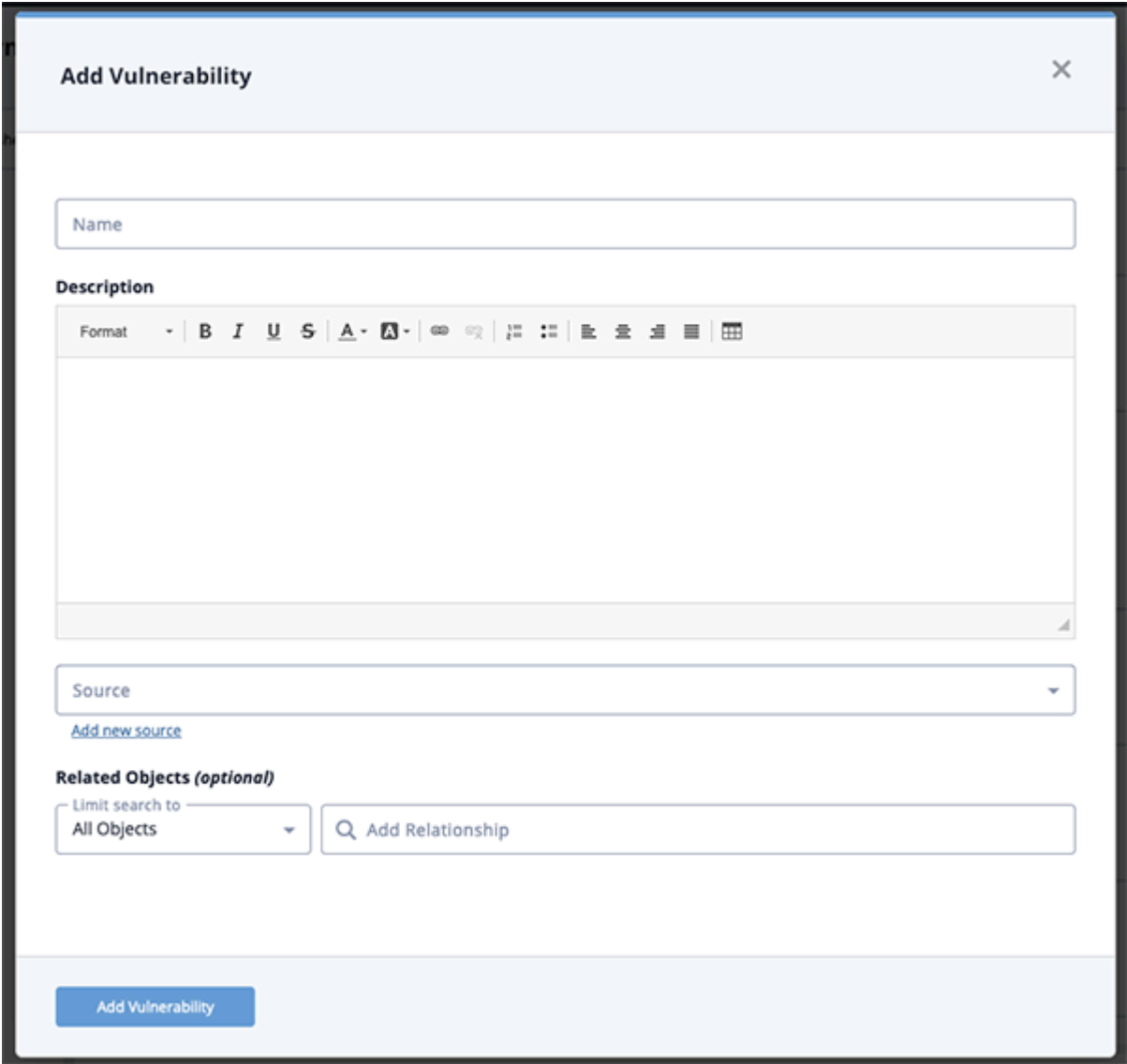
Vulnerabilities

A Vulnerability, as its name suggests, is a vulnerability in an application that can be exploited to infiltrate systems/networks.

Use the steps below to create, edit and delete a Vulnerability.

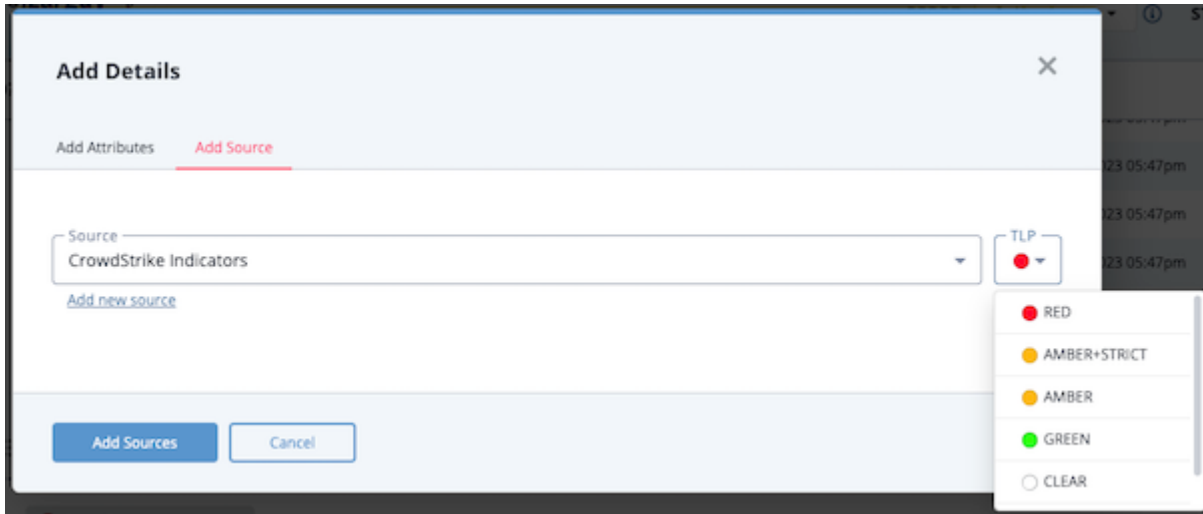
Adding a Vulnerability

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



2. Enter a name.
3. Enter a description in the field provided.
4. Select a **Source** from the dropdown provided.

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



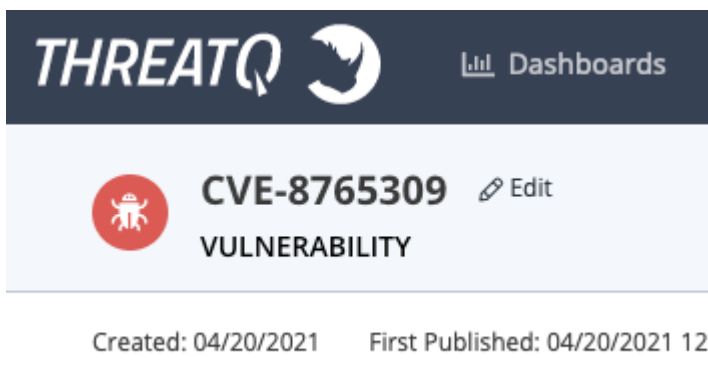
5. Select any **Related Objects** you need to link to the Vulnerability. This field is optional.
6. Click **Add Vulnerability**.

Adding Context

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

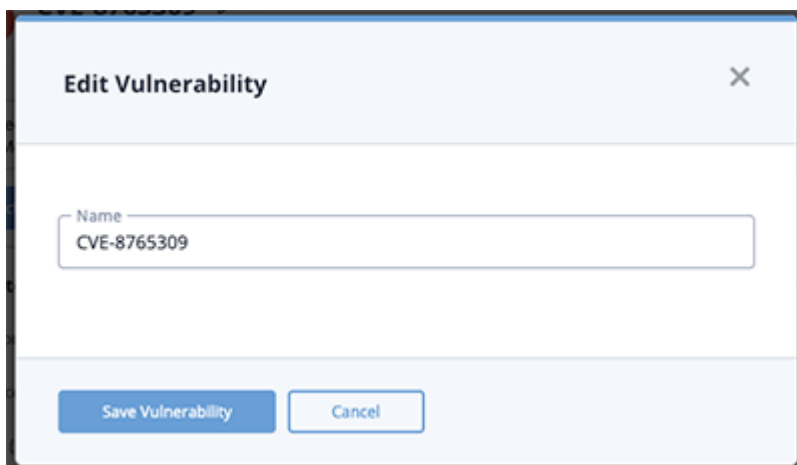
Editing a Vulnerability

1. Locate and click on the Vulnerability.
The Vulnerability's detail page opens.



2. Click on **Edit** next to the Vulnerability's name.

The Edit Vulnerability dialog box opens.

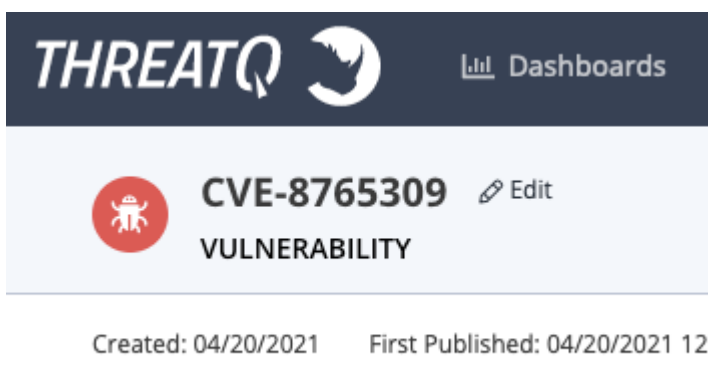


3. Make the desired change to the Vulnerability name and click **Save Vulnerability**.

Deleting a Vulnerability

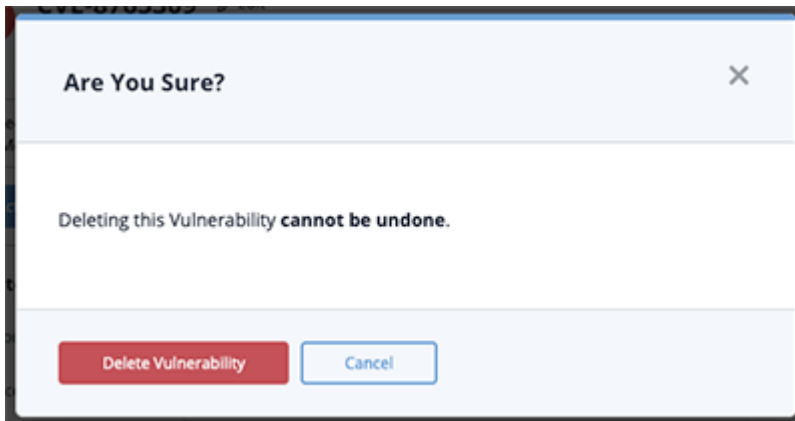
1. Locate and click on the Vulnerability.

The Vulnerability's details page opens.



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

A confirmation dialog box appears.

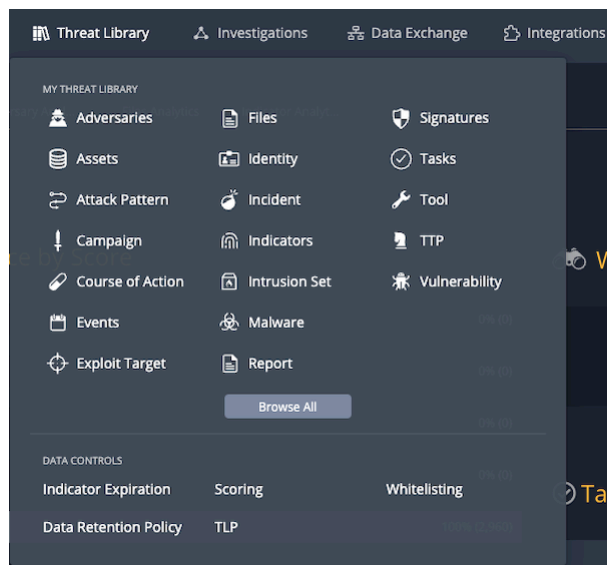


3. Click on **Delete Vulnerability**.

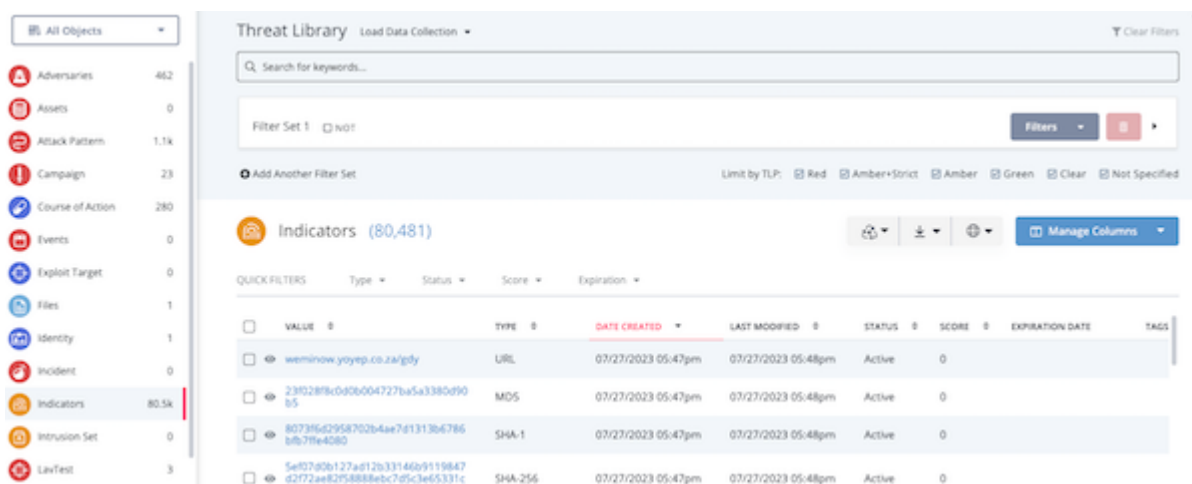
Threat Library

About Threat Library

The Threat Library is your interactive hub for managing the threat intelligence ingested into the the ThreatQ Platform. You can access the Threat Library from the Main Navigation bar.



The Threat Library drop-down list allows you to control the focus of your initial view by selecting an object type or you can click the Browse All button to access the default view of all object types with an initial focus on Indicators.



From the Threat Library, you can:

- [Customize the object information displayed in the results list.](#)
- Perform [basic searches](#) and/or narrow your search results using [filter sets](#).
- Perform [bulk updates or deletes](#) of system objects.

- Save your searches as [data collections](#) which you can use in dashboards, your data retention policy, ThreatQ Data Exchange feeds, and ThreatQ TDR Orchestrator workflows.
- [Enrich your data objects](#) by adding context and relationships or applying operations.

Managing Your Library View

You can limit the object types displayed in your Threat Library view and configure the data columns displayed in your search results.

Selecting Object Type View

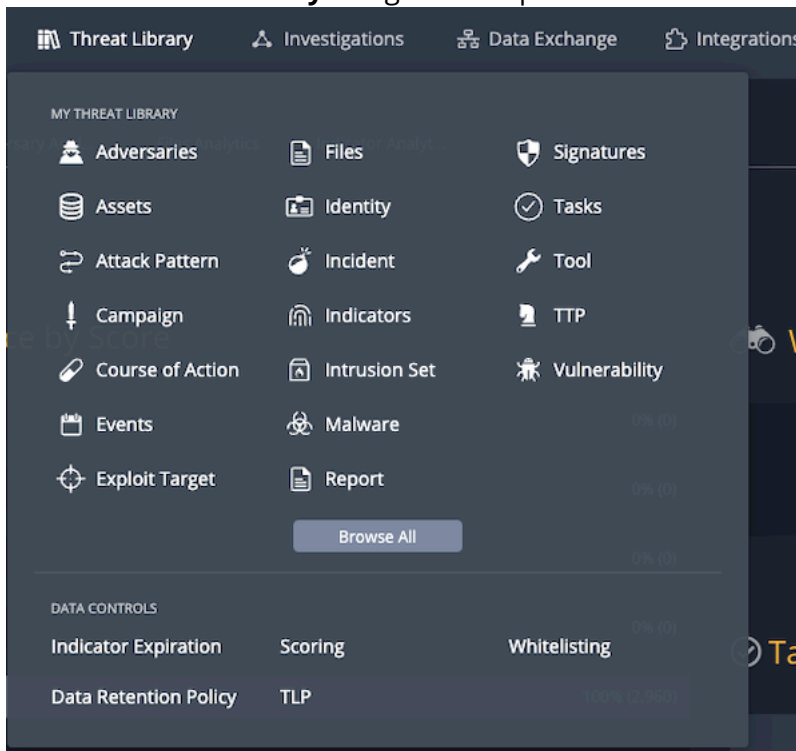
You can select which object types appear in your view of the Threat Library using the following methods:



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 the **Threat Library** navigation dropdown and select an **Object Type** or **Browse All**.



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



You can also access the [Data Controls](#) from this menu.

Object Type Left-Hand Menu

You can use the left-hand menu of the Threat Library to select view specific system object types.

You can either use the **Object Type** dropdown list or click directly on a object type listed in the menu.

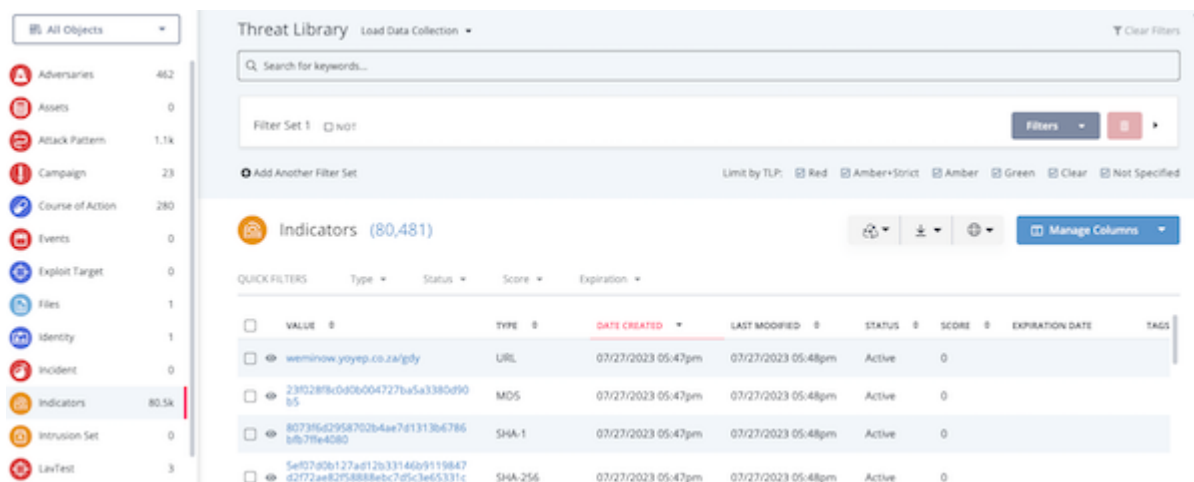


All Objects		
	Adversaries	26
	Assets	0
	Attack Pattern	175
	Campaign	1
	Course of Action	13
	Events	0
	Exploit Target	0
	Files	0
	Identity	0
	Incident	0
	Indicators	19.5k
	Intrusion Set	0
	Malware	92
	Report	0
	Signatures	0
	Tasks	0
	Tool	2
	TTP	0
	Vulnerability	0

Managing Library Columns

You can choose which columns to display in your Threat Library view. Your column options will vary by object type.

1. Navigate to the Threat Library page.



The screenshot shows the Threat Library interface. On the left, a sidebar lists object types: Adversaries (462), Assets (0), Attack Pattern (1.1k), Campaign (23), Course of Action (280), Events (0), Exploit Target (0), Files (1), Identity (1), Incident (0), Indicators (80.5k), Intrusion Set (0), and LiveTest (3). The main area is titled 'Threat Library' and shows a search bar, filter set (Filter Set 1: not), and a table of indicators. The table has columns: VALUE, TYPE, DATE CREATED, LAST MODIFIED, STATUS, SCORE, EXPIRATION DATE, and TAGS. The 'Indicators' view shows 80,481 objects. A 'Manage Columns' button is located in the top right of the table area.

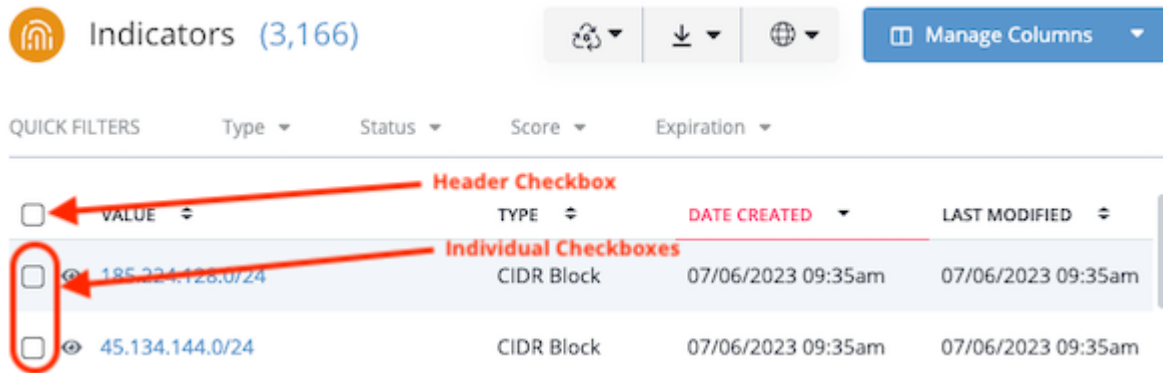
2. Click the **Manage Columns** button.
3. Use one of the following methods to locate the columns you want to display/hide:
 - Scroll through the list of column options.
 - Begin typing the column name until it is displayed below the search field.
4. To display a column, check the checkbox next to the column name.
5. To hide a column, uncheck the checkbox next to the column name.



You can click the values in related object columns to view a list of the related objects. For instance, if the Related Adversaries column lists a value of 10, you can click the 10 to view a list of the ten related adversaries. To return from this list to your original review, use your browser back button or remove the filter set displayed above the list.

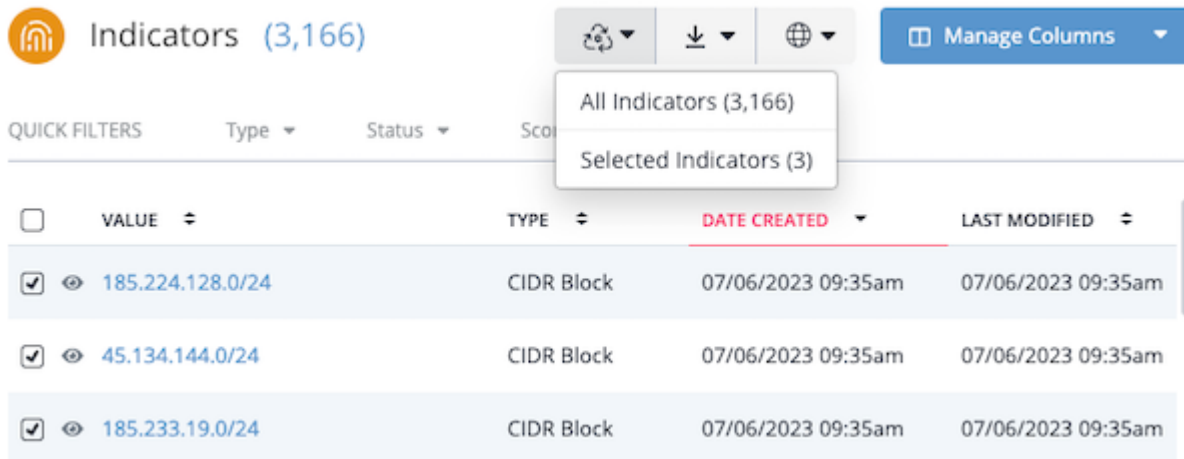
Selecting System Objects

The Threat Library results list allows you to select multiple objects of the same type for workflows, [exports](#), or [bulk actions](#). You can select individual objects by checking the checkbox to the left of the object or select all the objects currently displayed by clicking the header checkbox next to the Value column title.



☐	VALUE	TYPE	DATE CREATED	LAST MODIFIED
☐	185.224.128.0/24	CIDR Block	07/06/2023 09:35am	07/06/2023 09:35am
☐	45.134.144.0/24	CIDR Block	07/06/2023 09:35am	07/06/2023 09:35am

In addition, the drop down options for the Start Workflow, [Export](#), and [Bulk Actions](#) buttons give you the option to apply your choice to all objects or just the selected objects.



☐	VALUE	TYPE	DATE CREATED	LAST MODIFIED
☒	185.224.128.0/24	CIDR Block	07/06/2023 09:35am	07/06/2023 09:35am
☒	45.134.144.0/24	CIDR Block	07/06/2023 09:35am	07/06/2023 09:35am
☒	185.233.19.0/24	CIDR Block	07/06/2023 09:35am	07/06/2023 09:35am

Tips and Tricks

- Clicking the header checkbox selects all objects displayed on your current page of system objects. If your search results or data collection includes multiple pages, you must access those pages to select additional objects. For instance, if your search returns 100 indicators and you want to select the first 50, you can click the header checkbox on page 1 and page 2.
- When you navigate pages of results for the same indicator type, Threat Library retains your checked checkboxes. However, if you change your search filter(s) or switch to a different data collection, object type, or ThreatQ page, your checked checkboxes return to a default state of unchecked.
- In [job details](#), Bulk action jobs applied to a selected subset of objects list the following message in the Search Criteria field: **No search data to display.**

Basic Search

The basic Search, located to the right of the **Create** button in the ThreatQ navigation, allows you to find objects you are looking for quickly, without having to browse through a large number of objects.

Basic Search allows you to search for all objects in the system: Indicator , Events , Adversary , Files , Signatures , and so on. The search capability looks at high level aspects of each object, including:

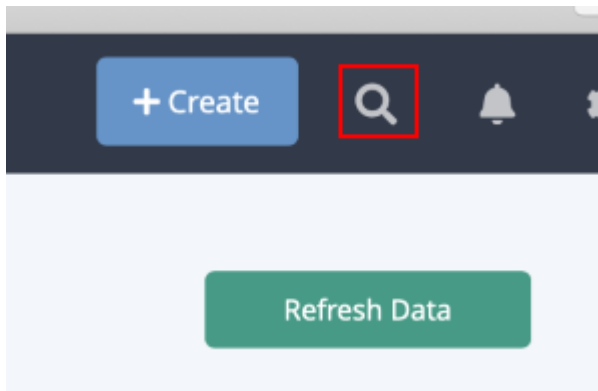
- Indicators (network or host)
- Attachment titles, hashes, keywords
- Attributes
- Adversary name
- Event title

For example, if you search for google.com, the following indicators are also returned:

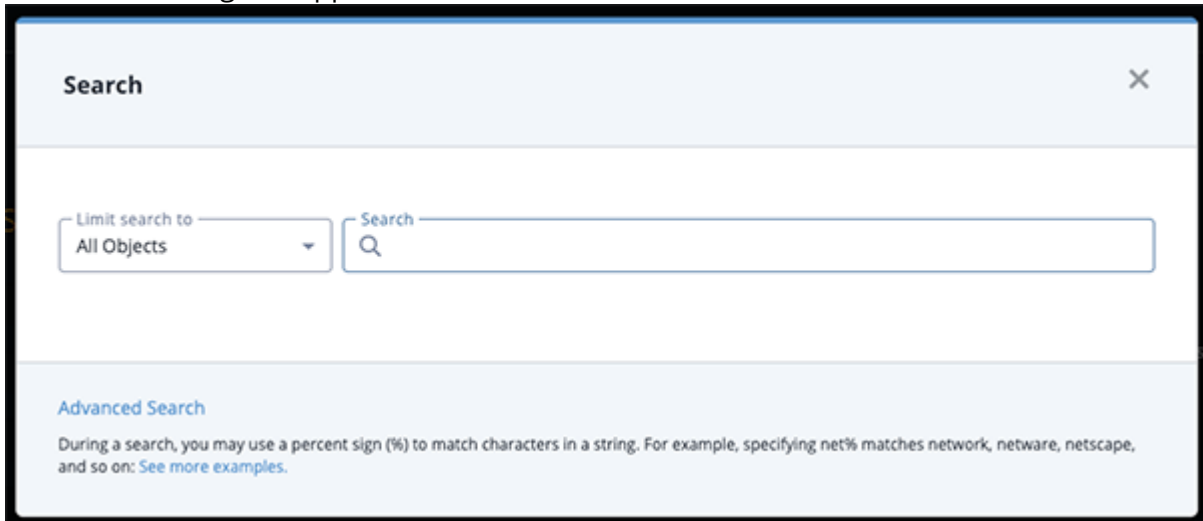
- www.google.com (FQDN)
- analytic.google.com (FQDN)
- www.google.com/analytic (URL)
- analytic@google.com (email address)

Performing a Basic Search

1. Choose the Search icon.



The Search dialog box appears.



Search [X]

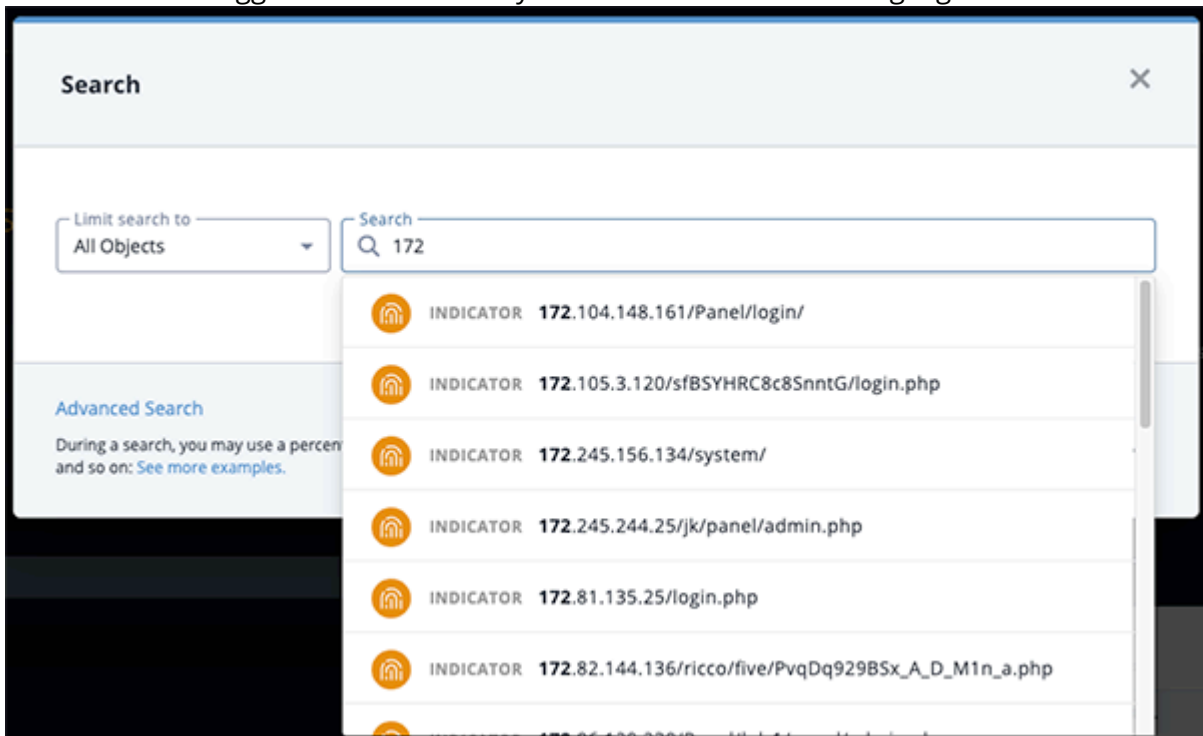
Limit search to: All Objects [v] Search [Q]

Advanced Search

During a search, you may use a percent sign (%) to match characters in a string. For example, specifying net% matches network, netware, netscape, and so on: [See more examples.](#)

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.



Search [X]

Limit search to: All Objects [v] Search [Q] 172

Advanced Search

During a search, you may use a percent sign (%) to match characters in a string. For example, specifying net% matches network, netware, netscape, and so on: [See more examples.](#)

- INDICATOR 172.104.148.161/Panel/login/
- INDICATOR 172.105.3.120/sfBSYHRC8c8SntG/login.php
- INDICATOR 172.245.156.134/system/
- INDICATOR 172.245.244.25/jk/panel/admin.php
- INDICATOR 172.81.135.25/login.php
- INDICATOR 172.82.144.136/ricco/five/PvqDq929BSx_A_D_M1n_a.php

4. Select the desired result.
 - If you do not retrieve any search results, we recommend trying the [Threat Library advanced search](#).
 - If there is only one result, the object details page appears.

Wildcards and Symbols in Searches

During a search, you may use a percent sign (%) to match characters in a string. The percent wildcard specifies that any characters can appear in multiple positions represented by the wildcard. For example, specifying net% matches network, netware, netscape, and so on.

Here are a number of examples showing search terms with percent wildcards:

SEARCH QUERY	DESCRIPTION
% panda	Finds any adversaries and indicators prefaced by another word, such as "red panda"
%ear	Finds any character string that ends with "ear," such as bear
%panda%	Finds any character string that has panda in any position
panda%	Finds any character string that begins with panda
pan%a	Finds any character string that has pan in the first three positions and ends with an "a"
p%a	Finds any character string that contains "p" and "a" with characters between them, such as "panda" and "pappa"

Creating an Object During a Basic Search

The Basic Search window gives you the option to add a new object. If you enter an object name that is not found, you can click the **Create** link to select the object type from a drop-down list and add the new object. In addition, if you limit a basic search to a specific object type, you are linked to the corresponding form. For example, if you limit your search to Adversaries, the **Create** link opens the **Add An Adversary** form.

Search

Limit search to
Adversaries

Search
smaug

No results found [Create Adversary "smaug"](#)

Advanced Search

During a search, you may use a percent sign (%) to match characters in a string. For example, specifying net% matches network, netware, netscape, and so on: [See more examples](#).

If you leave the **Limit search to** field set to All Objects, you can select the object type you want to create from a drop-down list.

Search

Limit search to
All Objects

Search
smaug

No results found [Create "smaug"](#)

Advanced Search

During a search, you may use a percent sign (%) to match characters in a string. For example, specifying net% matches network, netware, netscape, and so on: [See more examples](#).

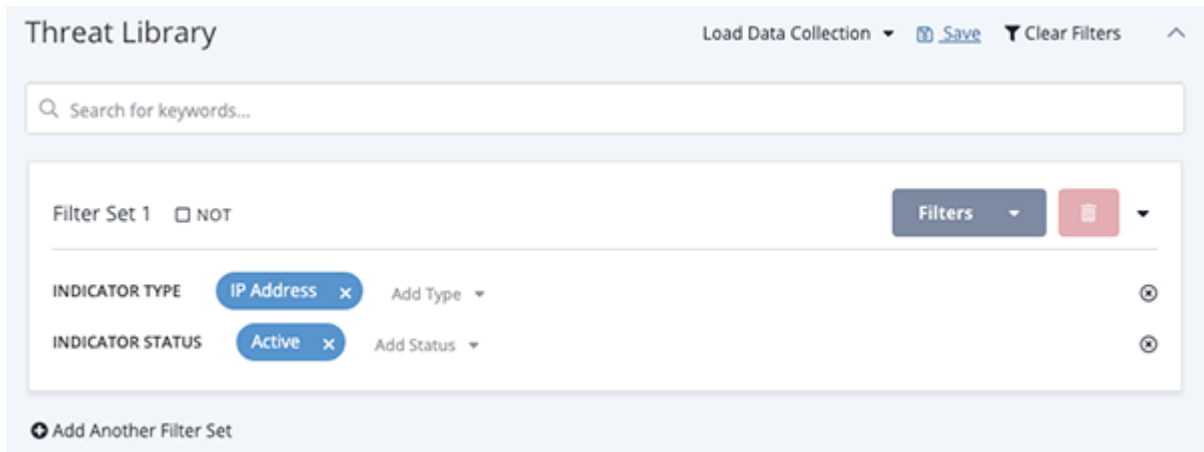
Building Searches with Filter Sets

About 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.

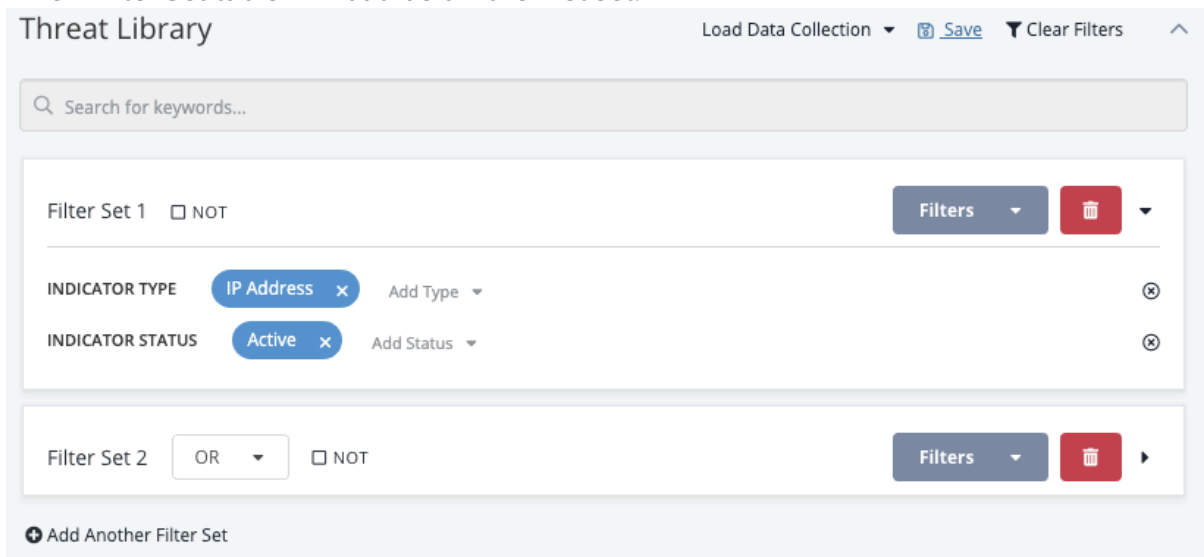


The screenshot shows the 'Threat Library' interface. At the top, there's a search bar labeled 'Search for keywords...'. Below it, 'Filter Set 1' is displayed with a 'NOT' checkbox. To the right of the filter set name are 'Filters' and 'Clear Filters' buttons. The filter set contains two filters: 'INDICATOR TYPE' with a value of 'IP Address' and 'INDICATOR STATUS' with a value of 'Active'. Each filter has an 'Add' button and a removal icon. At the bottom, 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.

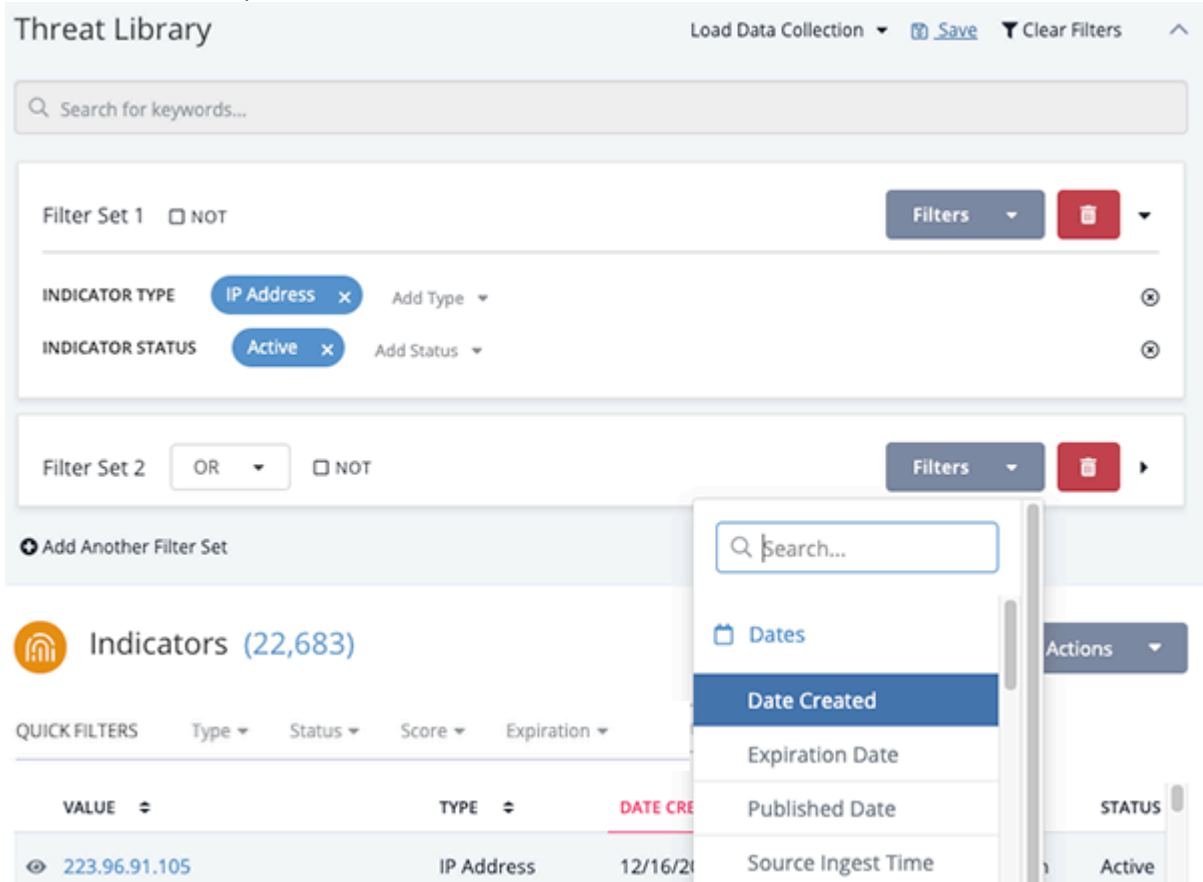
3. Click on **Add Another Filter Set**.

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



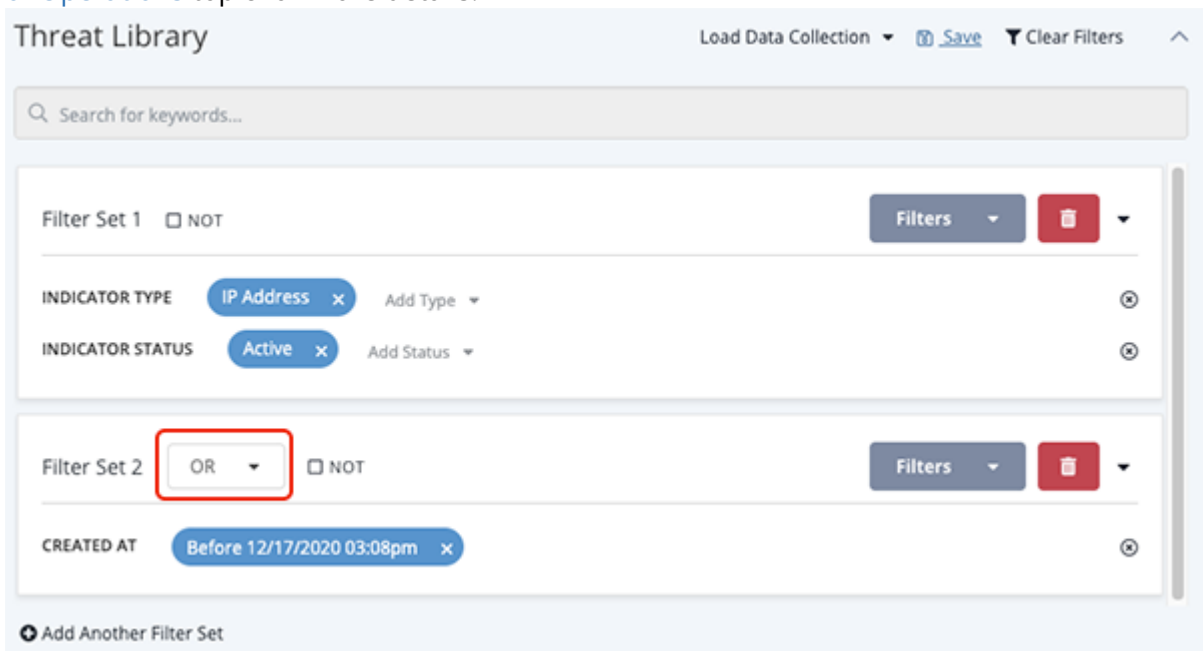
This screenshot shows the 'Threat Library' interface after adding a second filter set. 'Filter Set 1' remains at the top with its filters. Below it, 'Filter Set 2' is added, featuring a dropdown menu set to 'OR' and a 'NOT' checkbox. It also has 'Filters' and 'Clear Filters' buttons. The 'Add Another Filter Set' button is still visible at the bottom.

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.



The screenshot shows the Threat Library interface. At the top, there's a search bar and buttons for 'Load Data Collection', 'Save', and 'Clear Filters'. Below this, there are two filter sets. Filter Set 1 is labeled 'Filter Set 1' and has a 'NOT' checkbox. It contains two filters: 'INDICATOR TYPE' with 'IP Address' selected and 'INDICATOR STATUS' with 'Active' selected. Filter Set 2 is labeled 'Filter Set 2' and has an 'OR' dropdown and a 'NOT' checkbox. Below the filter sets, there's a section for 'Indicators (22,683)' with 'QUICK FILTERS' for Type, Status, Score, and Expiration. A table of indicators is shown with columns for VALUE, TYPE, DATE CREATED, and STATUS. The first row shows the value '223.96.91.105', type 'IP Address', date '12/16/20', and status 'Active'.

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



This screenshot shows the Threat Library interface with Filter Set 2. The 'OR' dropdown in the 'Filter Set 2' section is highlighted with a red box. The filter set also includes a 'NOT' checkbox and a filter for 'CREATED AT' with the value 'Before 12/17/2020 03:08pm'.

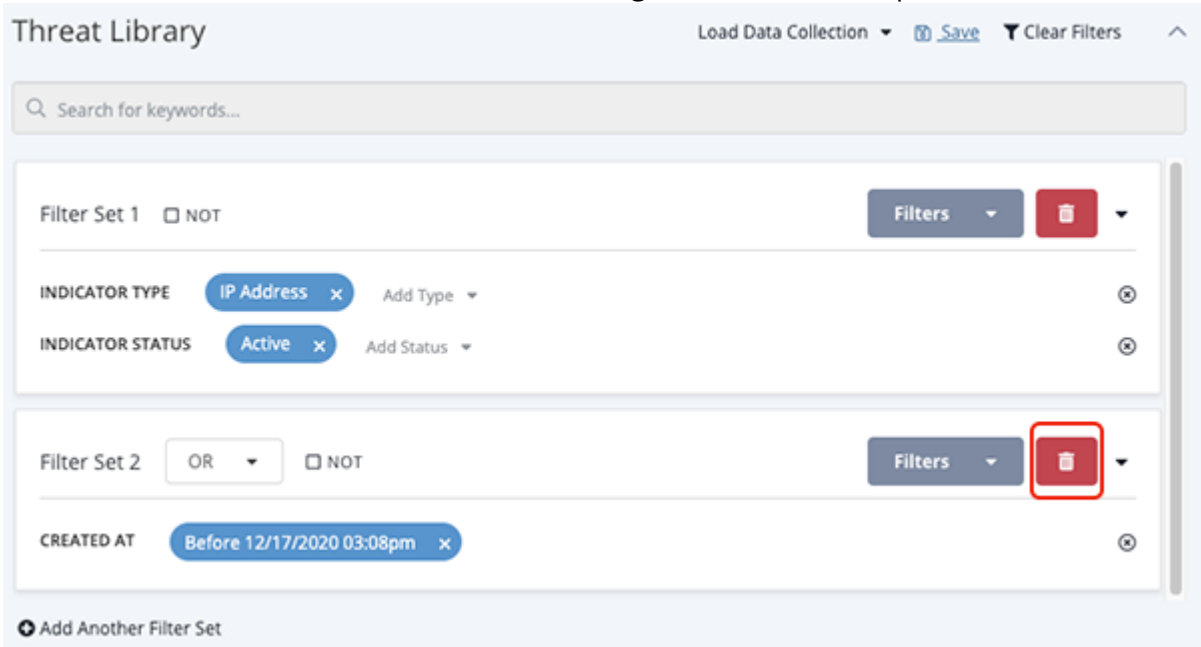
Repeat steps 3-6 to add additional filter sets.

Deleting Filter Sets



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

1. Click on the delete  icon located next to the right of the Filters dropdown.

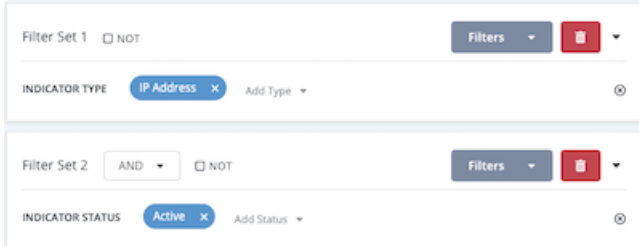


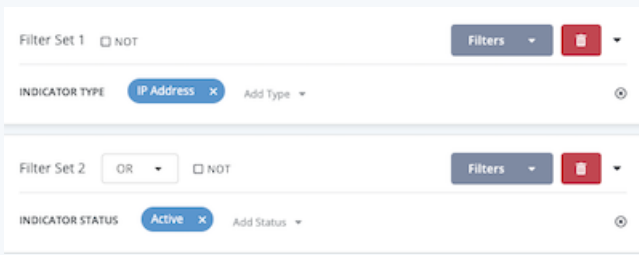
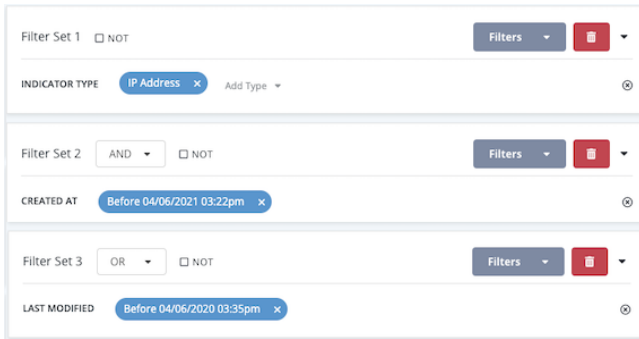
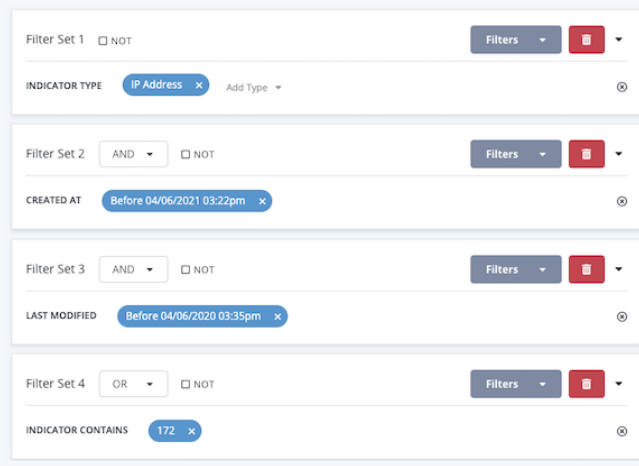
The screenshot shows the 'Threat Library' interface. At the top, there's a search bar and buttons for 'Load Data Collection', 'Save', and 'Clear Filters'. Below the search bar, there are two filter sets. Filter Set 1 is labeled 'Filter Set 1' and has a 'NOT' operator. It contains two indicators: 'INDICATOR TYPE' with 'IP Address' and 'INDICATOR STATUS' with 'Active'. Filter Set 2 is labeled 'Filter Set 2' and has an 'OR' operator. It contains one indicator: 'CREATED AT' with 'Before 12/17/2020 03:08pm'. Both filter sets have a 'Filters' dropdown and a red delete icon. The delete icon for Filter Set 2 is highlighted with a red box.

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	

SCENARIO	ORDER	EXAMPLE
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	

SCENARIO	ORDER	EXAMPLE

Multiple ANDs,
Multiple ORs

(Filter 1 AND Filter 2)
OR (Filter 3 AND Filter 4)

Filter Set 1 ☐ NOT

Filters

INDICATOR TYPE

IP Address

Add Type

Filter Set 2

AND

☐ NOT

Filters

CREATED AT

Before 04/06/2021 03:22pm

Filter Set 3

OR

☐ NOT

Filters

LAST MODIFIED

Before 04/06/2020 03:35pm

Filter Set 4

AND

☐ NOT

Filters

INDICATOR CONTAINS

172

Context Filters

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

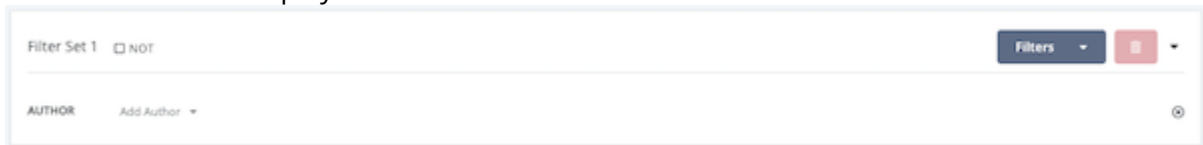
Filtering by Author

The Author context filter allows you to filter the system objects displayed based on the objects' source and attribute source authors. It allows you to filter by:

- Configuration Driven Feed (CDF)
- Operation
- ThreatQ Data Exchange (TQX) feed
- ThreatQ TDR Orchestrator (TQO) Workflow/CDW
- User

1. Click the **Filters** option and select **Author**.

The Author row is displayed under the filter set name.



2. Click the **Add Author** option to access a drop-down list of authors.
3. Locate and click the checkbox next to the author value(s) for your filter by scrolling through the drop-down list or entering the name in the Search field. You can select one or more authors at a time from this list.

When you apply the Author filter, the Author column is automatically added to the results listing. The Author column displays the source author(s) listed alphabetically in pill format.



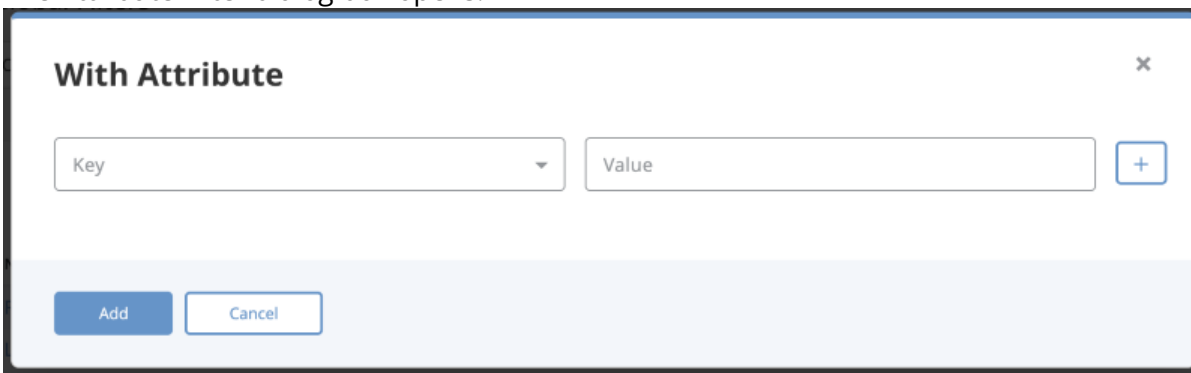
The Author column only lists an object's source author(s). It does not list an object's attribute source author(s). If your author filter only matches an object's attribute source author, the column is blank.

Filtering by Attribute

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

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

The Attribute Filter dialog box opens.



2. Select an **Attribute Type**.

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

When you apply a **With Attribute** filter, you can use wildcard values to more easily locate indicators. The Value field supports the following search methods:

SEARCH TYPE	SEARCH QUERY	SEARCH RESULTS
Exact Match	us	US only
Ends With	*us or %us	US and Lazarus
Begins With	us* or us%	US, USBferry, and USBStealer
Value Contains	*us* or %us%	US, USBferry, USBStealer, Lazarus, and Dust Storm



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

4. Click the **Add** button.

The filters are applied to the search results.

Using Multiple Attribute Filters

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

Multiple Attribute Filters ANY - Match Toggle Selection Example

SETTING	FIELD	VALUE

Filter A	Attribute Type	Attack Phase
	Attribute Value	C2
Filter B	Attribute Type	Severity
	Attribute Value	High
Filter Options	Any/All Toggle	Any

Result Search Results are filtered to include/exclude objects with Attack Phase: C2 **OR** Severity: High attributes.

Multiple Attribute Filters ALL - Match Toggle Selection Example

SETTING	FIELD	VALUE
Filter A	Attribute Type	Attack Phase
	Attribute Value	C2
Filter B	Attribute Type	Severity
	Attribute Value	High
Filter Options	Any/All Toggle	All

Result Search Results are filtered to include/exclude objects with Attack Phase: C2 **AND** Severity: High attributes.

Attribute Common Scenarios

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

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

The Attribute Filter dialog box opens.

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

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

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

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

The Attribute Filter dialog box opens.

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

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

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

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

The Attribute Filter dialog box opens.

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

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

Applying keyword filters then applying a "With Attribute" filter

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

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

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

The Attribute Filter dialog box opens.

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

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

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

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

The Attribute Filter dialog box opens.

3. The User specifies two attributes:
 - o Attack Pattern:C2

- Severity: High
4. User clicks on **Add**.

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

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

A form will load with all applied filter attributes.

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

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

Add multiple attributes and toggle Match from Any to All

1. User applies two attribute filters to the indicators results: **Attack Phase: C2** and **Severity: High**.
The filtered results will display any indicators that has either of those attributes.
2. User clicks on the **Any/All** Match toggle button and select **All**.

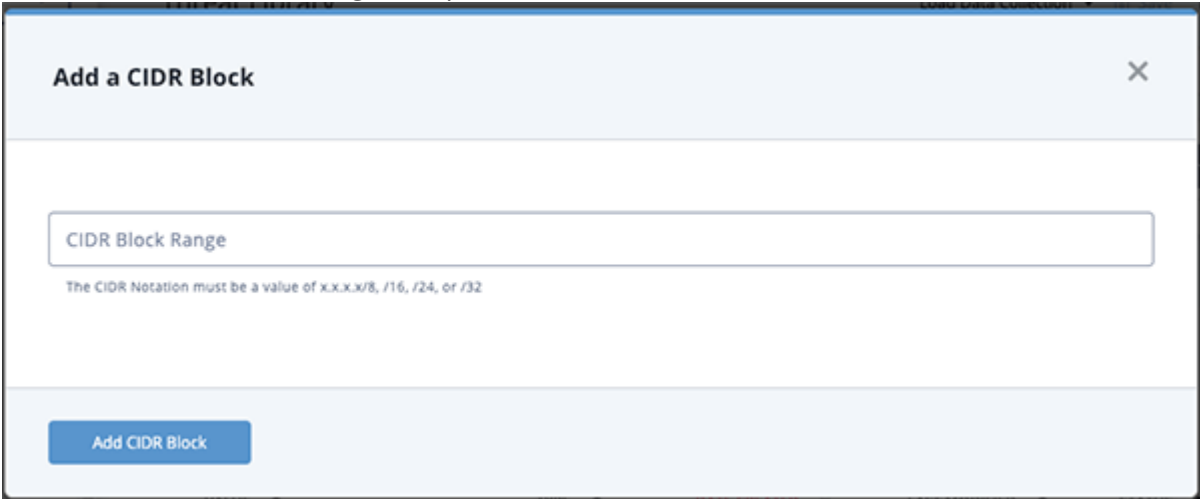
The filtered results will display any indicator that has both of those attributes

Filtering by CIDR Block Range

You can filter Threat Library objects by a block of IP addresses using the CIDR block range filter. The CIDR Block Range filter allows you to specify a CIDR block with prefix and suffix for an IPv4 search.

1. Click the **Filters** option and select **CIDR block range**.

The Add a CIDR Block dialog box opens.



2. Enter the CIDR block in one of the following formats:
 - x.x.x.x/8
 - x.x.x.x/16

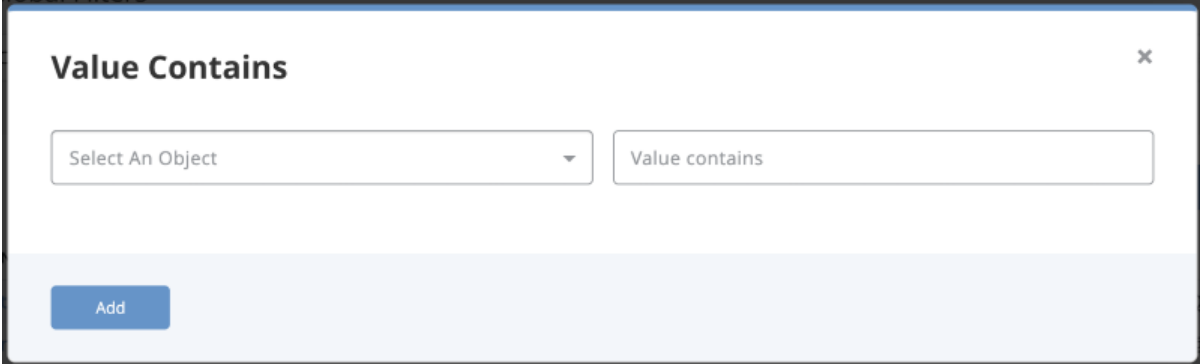
- x.x.x.x/24
 - x.x.x.x/32
3. Click **Add CIDR Block** to apply the filter.

Filtering by Value Contains

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

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

The Contains dialog box opens.



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

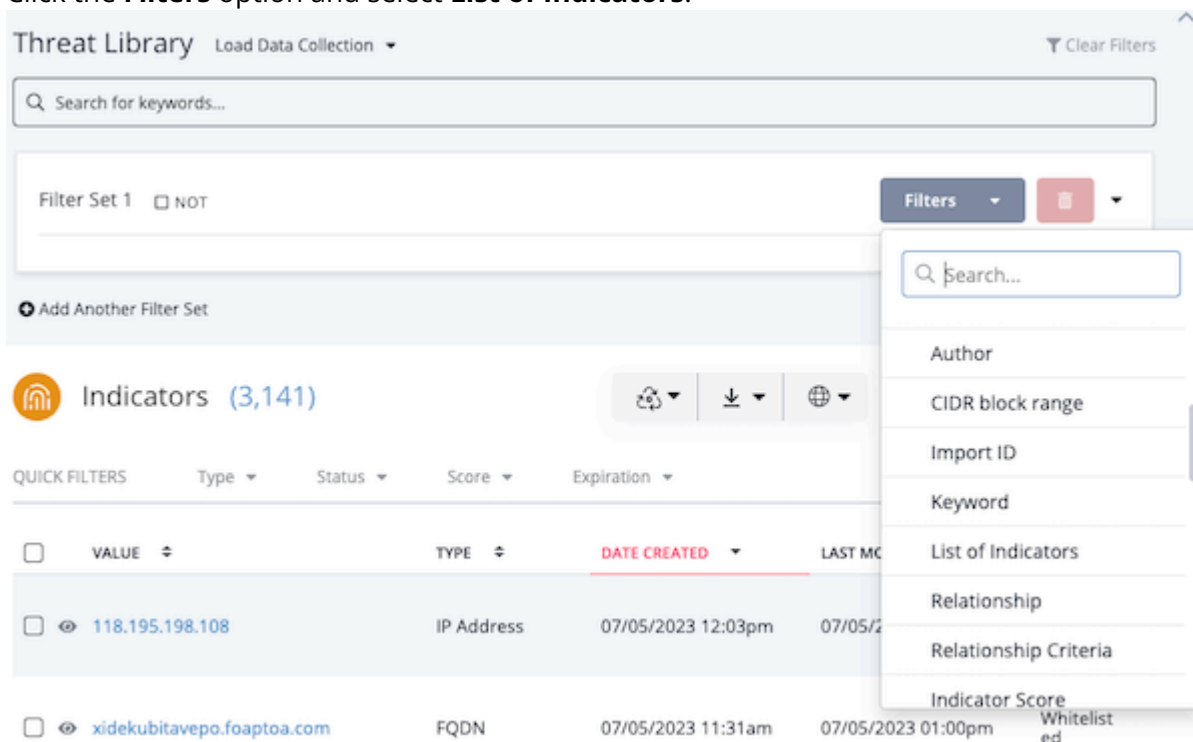
Filtering by List of Indicators

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



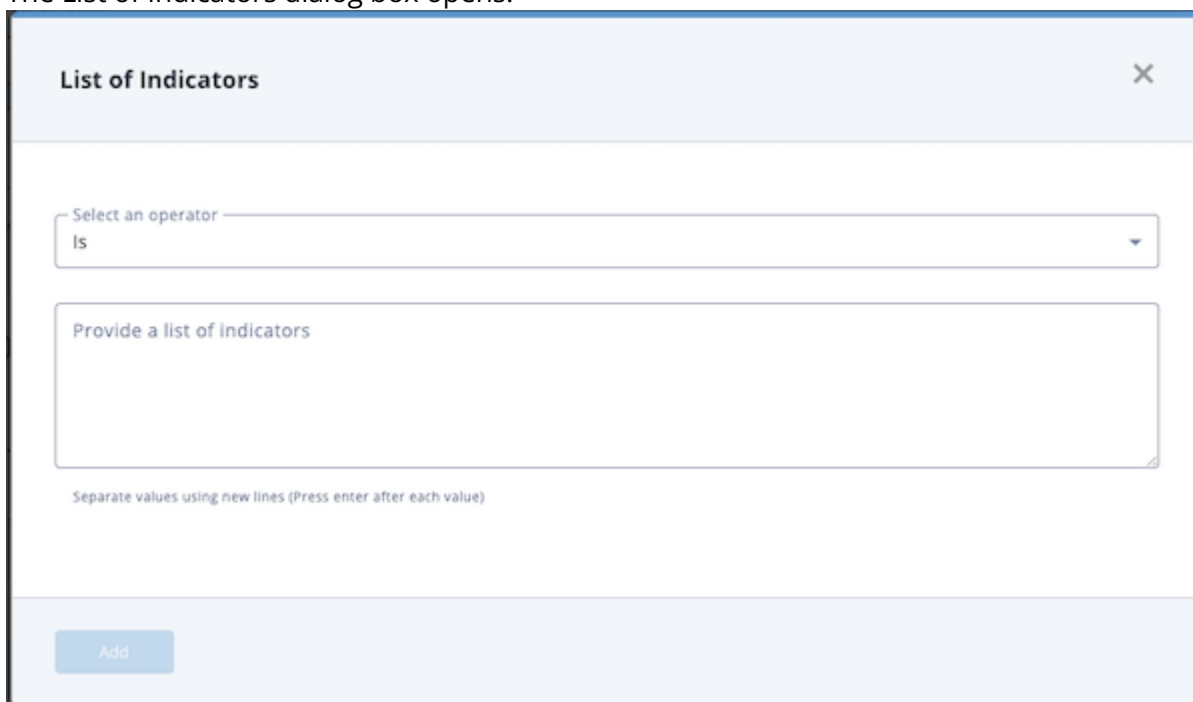
The filter will return indicators that are an exact match. It does not return partial matches.

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



The screenshot shows the Threat Library interface. At the top, there's a search bar and a 'Clear Filters' button. Below the search bar, there's a 'Filter Set 1' section with a 'NOT' button and an 'Add Another Filter Set' button. A 'Filters' dropdown menu is open, showing a search bar and a list of filter options: Author, CIDR block range, Import ID, Keyword, List of Indicators (highlighted), Relationship, Relationship Criteria, Indicator Score, and Whitelisted. Below the filters, there's a table of indicators. The table has columns for 'VALUE', 'TYPE', 'DATE CREATED', and 'LAST MODIFIED'. The first row shows an IP address '118.195.198.108' with a score of 100. The second row shows a domain 'xidekubitavepo.foaptoa.com' with a score of 100.

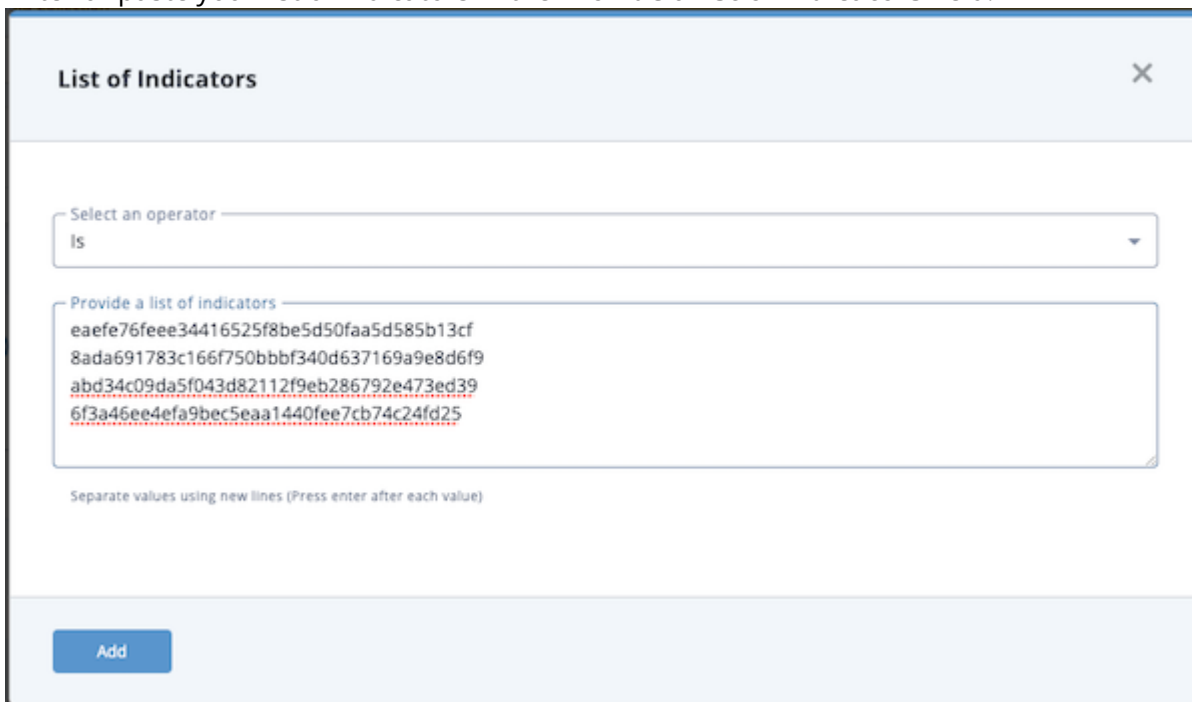
The List of Indicators dialog box opens.



The 'List of Indicators' dialog box is shown. It has a title bar with a close button. Inside, there's a 'Select an operator' dropdown menu with 'Is' selected. Below this is a large text area labeled 'Provide a list of indicators'. At the bottom, there's an 'Add' button. A note at the bottom of the text area says 'Separate values using new lines (Press enter after each value)'.

2. The **Specify an operator** field defaults to a value of *Is* which returns exact matches. However, you can click the arrow next to this field and select *Contains* as the operator to return partial matches.

3. Enter or paste your list of indicators in the **Provide a list of indicators** field.



The accepted list format is one indicator per line.

4. Click **Add** to apply the filter.

Filtering by Keyword

1. Enter your keyword search term or phrase in the **Search for keywords** field and press Enter
OR
Click the **Filters** option and select Keyword to access the Filter by Keyword window. Then, enter your search term or phrase in the **Keyword** field and click the Add button.
2. To add more keywords, repeat step 1.
3. If you add more than one keyword, you can specify a **Must Match** setting of:
 - **ANY** - Search results include objects that include any of the keywords.
 - **ALL** - Search results include objects that include all of the keywords.
4. Click the **X** for each filter to remove it or select **Clear All Filters** to remove all filters

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

○ Source Names	○ Spearphish Value (for Events of Type 'Spearphish')
○ Attribute Names	○ Indicator Type Name
○ Attribute Values	○ Indicator Status Name
○ Comments	○ Indicator Value

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

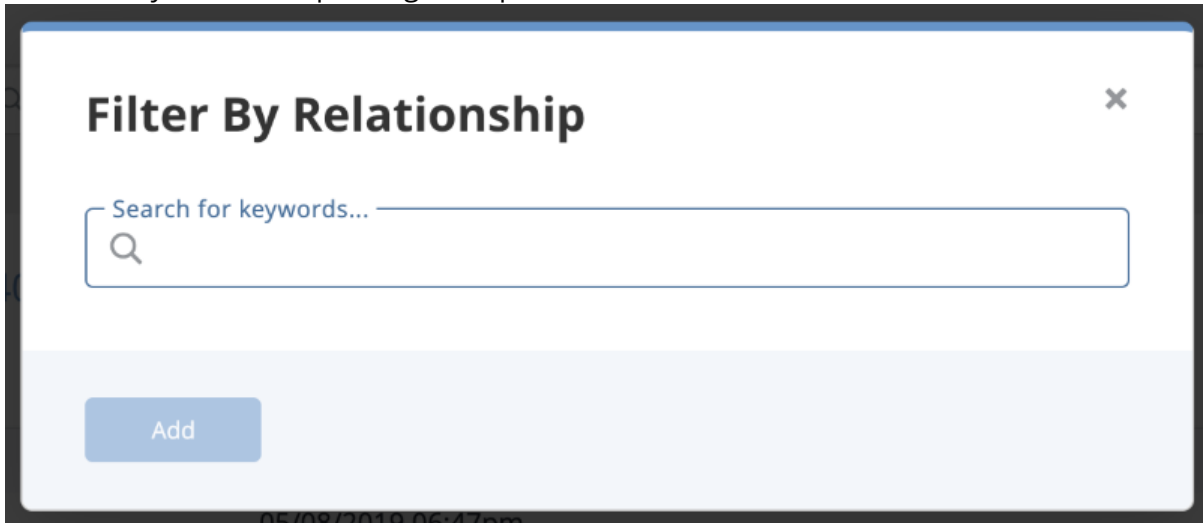
Filtering by Relationship

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

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

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

The Filter by Relationship dialog box opens.



2. Use the text box provided to select an object.
3. Click **Add** to apply the filter.



The **Match Any/All** toggle option will 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.

Filtering by Relationship ANY - Match Toggle Selection Example

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

Filtering by Relationship ALL - Match Toggle Selection Example

SETTING	RELATED OBJECT
Filter A	ABC Indicator

Filter B DEF Event

Filter Option All

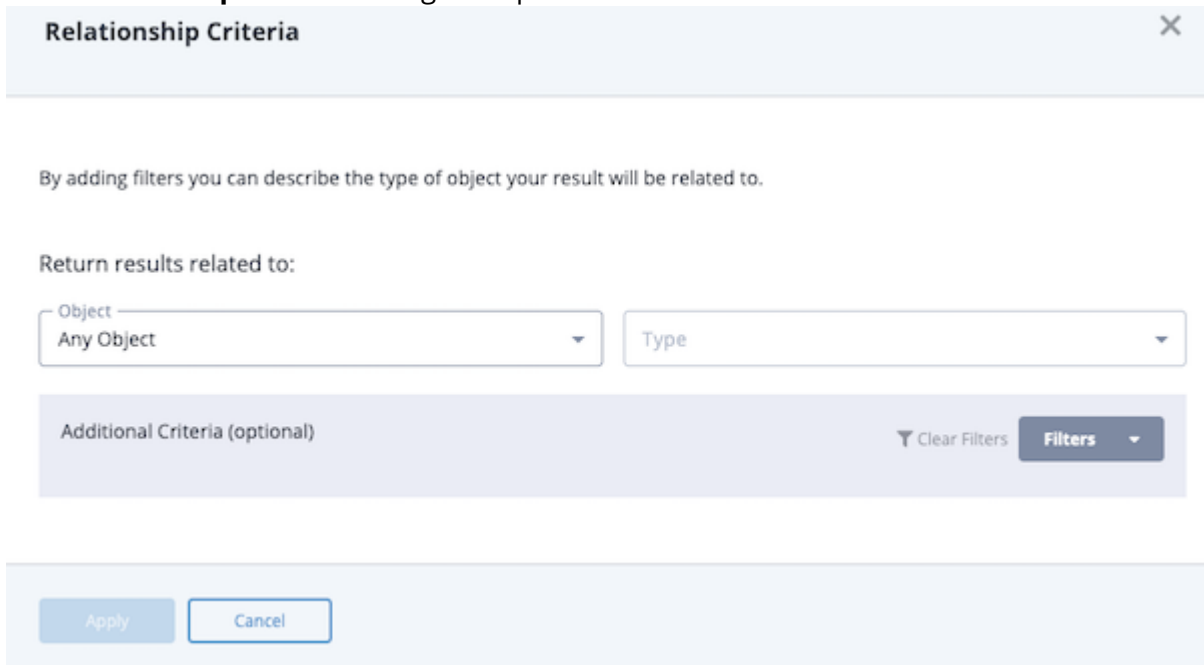
Result Search Results are filtered to include objects related to the ABC Indicator **AND** the DEF Event.

Filtering by Relationship Criteria

The Relationship Criteria filter allows you to filter system objects based on the characteristics of their related objects. For instance, you can filter a list of indicators to include only those with related login compromise event objects.

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

The **Relationship Criteria** dialog box opens.



2. Use the text box to select your **Object** and **Type**.
3. Optional. You can further filter your results based on the following additional criteria.

Date Created Filter

The Date Created option allows you to narrow your results based on the date a related object was created. This filter allows you to specify creation before or after a date, within a date range, or within a specific number of preceding days.

1. To add a Date Created filter, click the **Filters** dropdown and select **Date Created**.
2. Click the date type dropdown to specify creation before (**is before**) or after (**is after**) a date, within a date range (**is between**), or within a specific number of preceding days (**is within the last**).

3. Based on the date type you selected, enter a date and time, date and time range, or number of days.

Source Filter

The Source option allows you to filter your results based on one or more sources. In addition, you can specify that an object must meet all or at least one of your Source criteria.

1. To add a Source filter, click the **Filters** dropdown and select **Source**.
2. Click the Add Source option
3. Locate the source by scrolling through the list or typing the source name in the Search for sources field.
4. Click the source you want to add as a filter criteria.
5. To add more source filters, repeat steps 2 through 4.



When you add multiple Source filters, the Must Match field allows you to select ALL to indicate that an object must meet the requirements of all the Source filters or ANY to specify that your results include objects that meet the requirements of at least one Source filter.

Value Contains Filter

1. To add a Value Contains filter, click the **Filters** dropdown and select **Value Contains**.
2. Enter your desired value in the field provided.

With Attribute Filter

The With Attribute option allows you to filter results based on one or more specific attribute keys or attribute key and value combinations. In addition, you can specify that an object must meet all or at least one of your With Attribute criteria.

1. To add a With Attribute filter, click the **Filters** dropdown and select **With Attribute**.
2. Enter the attribute key and attribute value (optional) you want to filter by.
3. To add more attribute key/value filters, click the + icon and repeat step 7.



When you add multiple With Attribute filters, the Must Match field is displayed and defaults to ALL to indicate that an object must meet the requirement of all the With Attribute filters. You can change this value to ANY so that your results include objects that meet the requirements of at least one With Attribute filter.

Tag Filter

The Tag option allows you to filter your results based on the tag(s) associated with a related object. In addition, you can specify that an object must meet all or at least one of your Tag criteria.

1. To add a Tag filter, click the **Filters** dropdown and select **Tag**.
2. Click the Add Tag option
3. Locate the tag by scrolling through the list or typing the tag name in the Search for tags field.
4. Click the tag you want to add as a filter criteria.
5. To add more tag filters, repeat steps 2 through 4.



When you add multiple Tag filters, the Must Match field allows you to select ALL to indicate that an object must meet the requirements of all the Tag filters or ANY to specify that your results include objects that meet the requirements of at least one Tag filter.

4. After you select all of your filter options, click **Apply** to filter your Threat Library results.

Filtering by Score

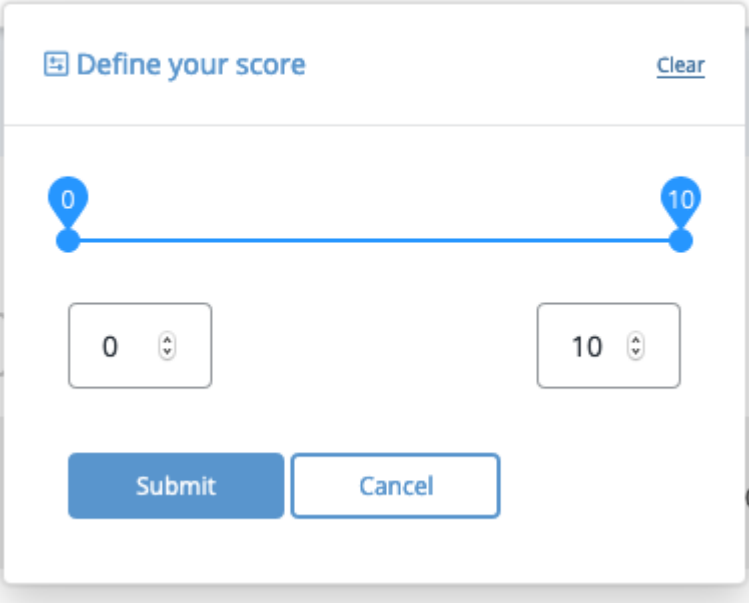
You can filter indicators in the advanced search results by score.



This option is only available for indicators.

1. Navigate to the Advanced Search results page by selecting **Search > Advanced Search** then selecting **Indicators** from the left-hand object type menu.
You can also select **Threat Library > Indicators** from the main menu.
2. Click the **Filters** dropdown and select the **Indicator Score** filter option.
The Indicator Score dialog row will load in the filter set.

Update Score ▼



The dialog box is titled "Define your score" with a "Clear" link in the top right. It features a horizontal scale from 0 to 10, with blue circular markers at each end. Below the scale are two input boxes: the left one contains "0" and the right one contains "10", both with up and down arrow icons. At the bottom are "Submit" and "Cancel" buttons.



The scale offers a range of 1-10.

3. Adjust the score scale to filter the results.

Filtering by Scoring Range

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



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

Filtering by Specific Score

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



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

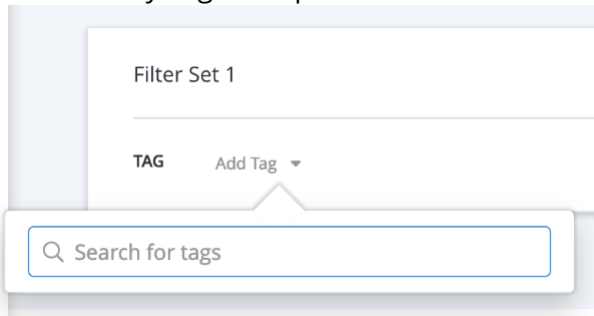
Select the **Update Score** filter again or select **Clear** to remove the filter.

Filtering by Tags

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

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

The Filter by Tag row opens.



2. Select **Add Tag**.
The Add Tag dialog box opens.
3. Use the supplied text field to select a tag.
4. Repeat steps 2-3 to apply multiple tag filters.



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

ANY - Match Toggle Selection Example

SETTING	TAG
Filter A	Phishing
Filter B	DDoS

Filter Option	Any

Result	Search Results are filtered to include items with either Phishing OR the DDoS tags.

ALL - Match Toggle Selection Example

SETTING	TAG
Filter A	Phishing
Filter B	DDoS

Filter Option	All

Result	Search Results are filtered to include items with both Phishing AND DDoS tags.

Filtering by Source

The Source filter allows you to filter Threat Library search results by object or attribute source.

1. Click the **Filters** option and select **Source**.
The Source row is displayed below the filter name.
2. Locate and select the source for your filter by scrolling through the drop-down list or entering the source in the Search for sources field.
3. Click the arrow next to Source to specify whether the filter references all sources or is restricted to object or attribute sources.
4. Click the checkbox next to **Is Only** to specify that the filter includes objects that only include the selected source(s) and do not include any other sources not specified by the filter.
5. To continue adding sources to the filter, click the Add Source option and repeat step 2.



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

Filtering by Source ANY - Match Toggle Selection Examples

SETTING	SOURCE
Filter A	This Platform

Filter B Domain Tools

Filter Option Any

Result Search Results are filtered to include objects with a source of This Platform **OR** Domain Tools.

Filtering by Source ALL - Match Toggle Selection

SETTING

SOURCE

Filter A This Platform

Filter B Domain Tools

Filter Option All

Result Search Results are filtered to include objects with both This Platform **AND** Domain Tools as sources.

Filtering by TLP

Users can filter Threat Library search results by specific TLP color designations. For reference on Traffic Light Protocol (TLP), view the [Traffic Light Protocol \(TLP\)](#) topic.

By default, all the TLP filter options are checked so that your Threat Library view includes all objects regardless of their sources' TLP labels. To exclude objects with a particular TLP label, you can uncheck the box to the left of the label name. For example, to omit objects with sources assigned a Red TLP label, uncheck the Red box.

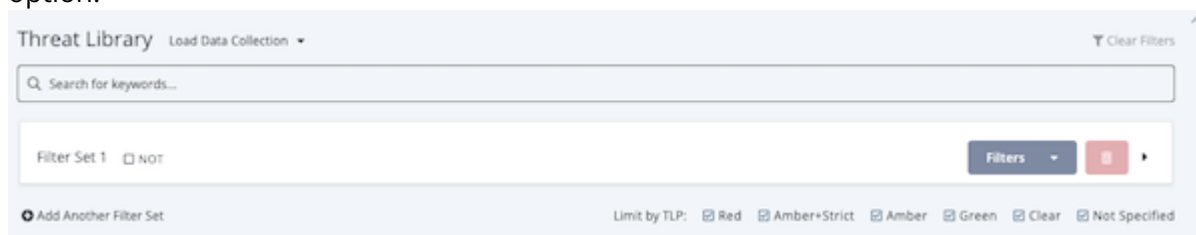
The filter functions in two ways. First, the filter will be applied to the object's source TLP and will only return system objects that contain a source that matches the TLP values selected in the TLP filter. The filter will then limit source and attribute column data of the search results to only display 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.



The screenshot shows the Threat Library interface. At the top, there's a search bar with the placeholder text "Search for keywords...". Below the search bar, there's a filter set section labeled "Filter Set 1" with a "NOT" toggle. To the right of the filter set, there's a "Filters" button. At the bottom, there's a "Limit by TLP:" section with checkboxes for "Red", "Amber+Strict", "Amber", "Green", "Clear", and "Not Specified".

2. Use the **Limit by TLP** filter check boxes to select which TLP designations to apply to your search results.



If TLP Green is checked, only objects with any source of TLP Green will be returned in the search results.

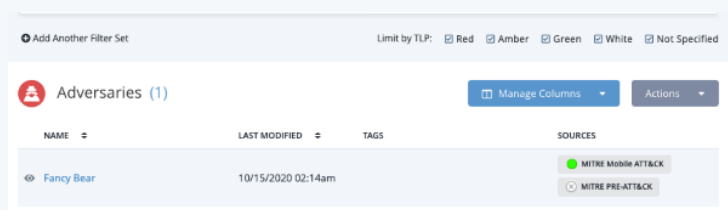
From the Objects retrieved, the TLP filter also impacts the information returned in search results columns, including Sources and Attributes.

Sources - In the Sources column of the search results, only sources that match the selected TLP colors will be displayed.

SCENARIO

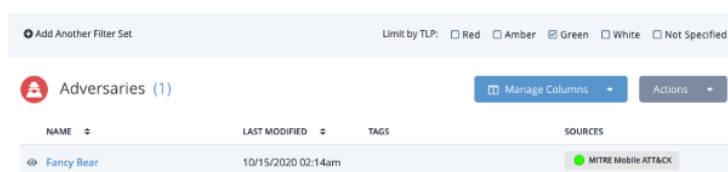
RESULTS DISPLAY

Sources displayed before applying the TLP filter



The screenshot shows the ThreatQ interface with the "Limit by TLP:" section at the top. The "Green" checkbox is checked. Below the table, the "Sources" column for the "Fancy Bear" entry shows two sources: "MITRE Mobile ATTACK" (with a green dot) and "MITRE PRE-ATTACK" (with a grey dot).

Sources displayed after applying the TLP filter



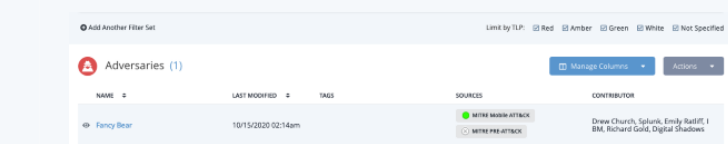
The screenshot shows the ThreatQ interface with the "Limit by TLP:" section at the top. The "Green" checkbox is checked. Below the table, the "Sources" column for the "Fancy Bear" entry shows only one source: "MITRE Mobile ATTACK" (with a green dot). The "MITRE PRE-ATTACK" source is no longer visible.

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



The screenshot shows the ThreatQ interface with the "Limit by TLP:" section at the top. The "Green" checkbox is checked. Below the table, the "Contributor" column for the "Fancy Bear" entry shows two contributors: "Drew Church, Spaford, Emily Radtke, I BM, Richard Gold, Digital Shadows" (with a green dot) and "MITRE PRE-ATTACK" (with a grey dot).

Attribute Contributors displayed after applying the TLP filter

Add Another Filter Set		Limit by TLP: ☐ Red ☐ Amber ☒ Green ☐ White ☐ Not Specified	
Adversaries (1)		Manage Columns Actions	
NAME	LAST MODIFIED	TAGS	CONTRIBUTOR
Fancy Bear	10/15/2020 02:14am	MITRE MANDRILL ATTACK	Drew Church, Splunk, Emily Ratoff

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

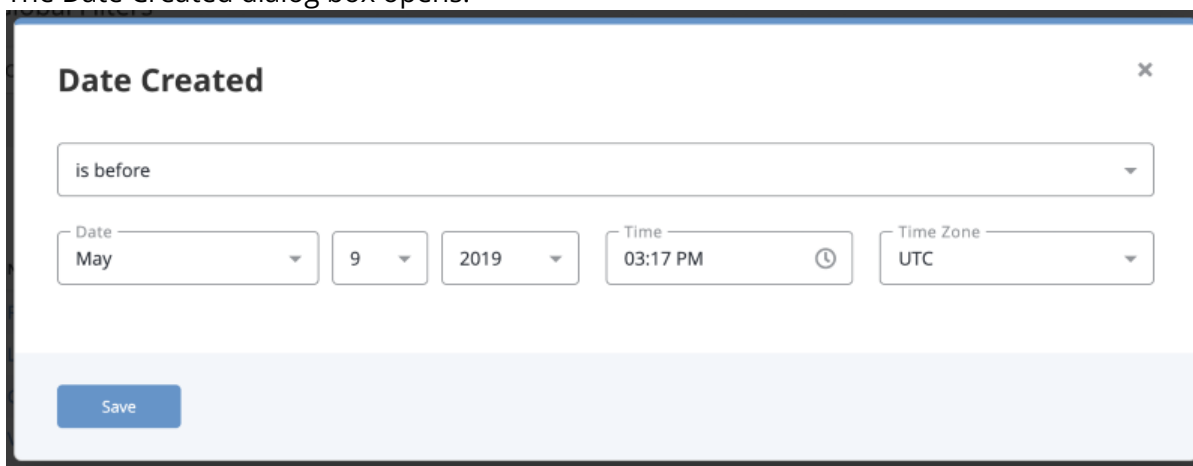
Date filters allow you to filter advanced search results by date-related values.

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

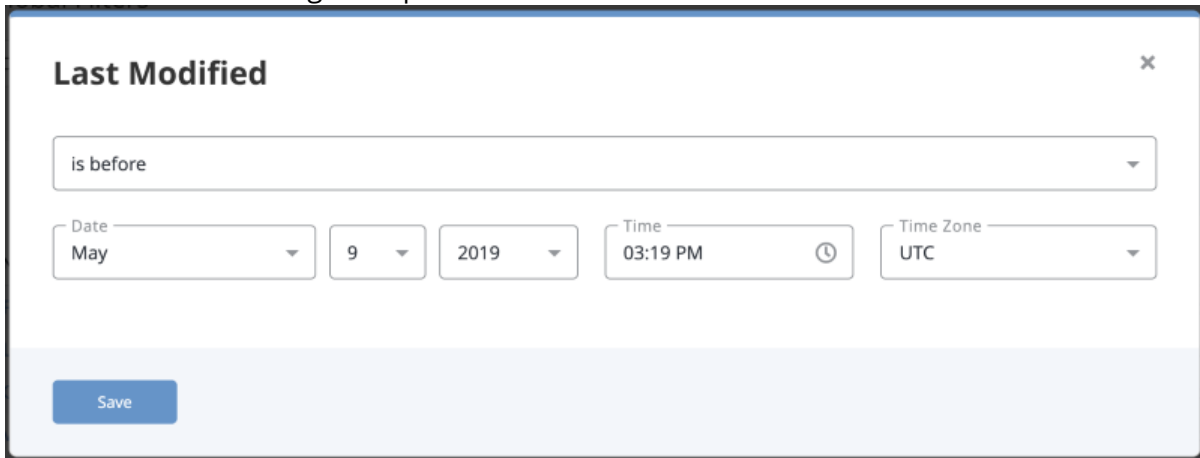
3. Use the controls to select date options based upon the selection in step 2.
4. Click **Save**.

Filtering by Last Modified

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

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

The Last Modified dialog box opens.



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

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

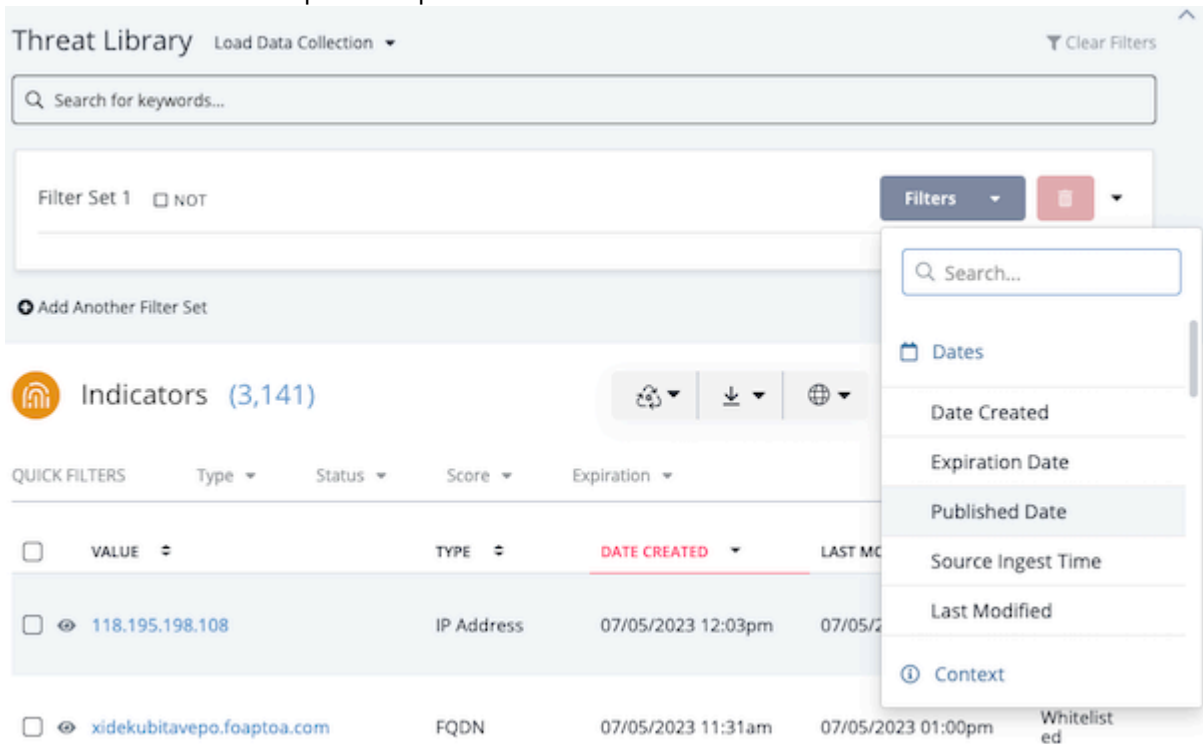
3. Use the controls to select date options based upon the selection in step 2.
4. Click **Save**.

Filtering by Published Date

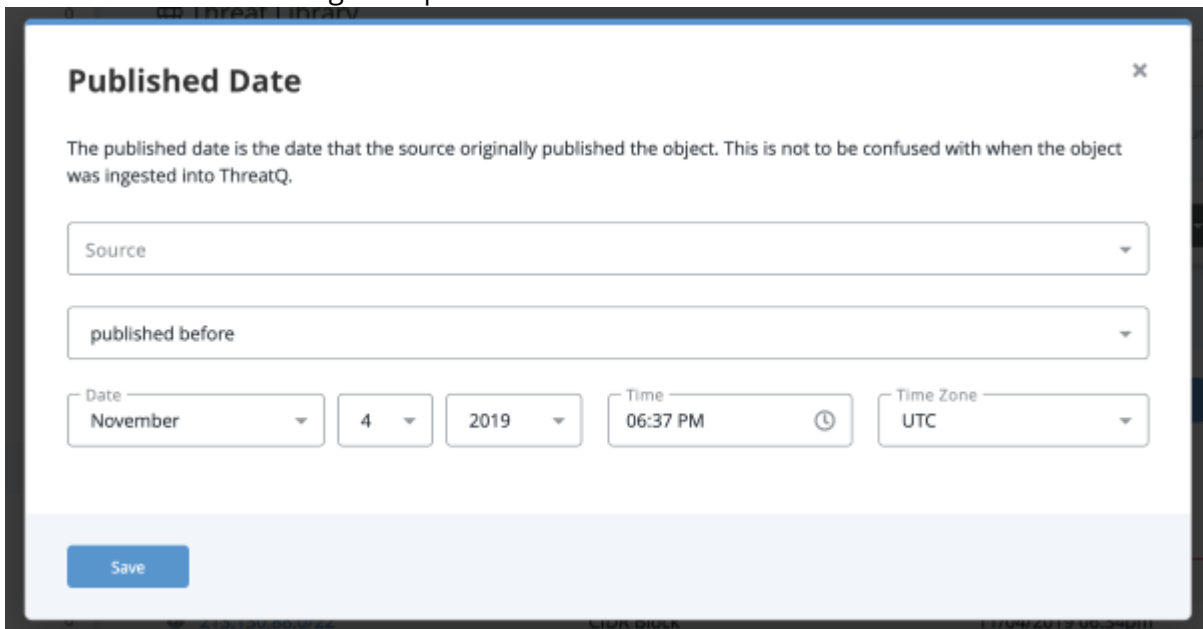


The Published Date is the date that an object was originally published by the source. This is not to be confused with when the object was ingested into ThreatQ.

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



The Published Date dialog box opens.



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

OPTION

RESULT

published before

Search results include items before a selected date

OPTION	RESULT
published after	Search results include items after a selected date
published between	Search results include items in a selected range of dates
published within the last	Search results include items within the selected number of days.

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

Filtering by Source Ingest Time

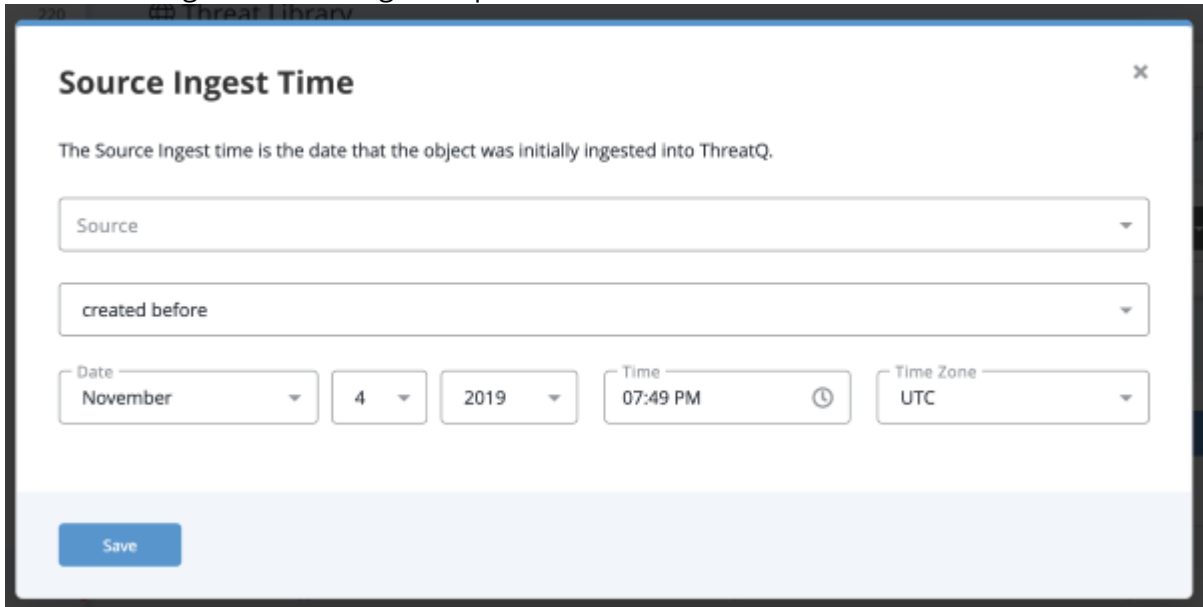


The Source Ingest Time is the date that an object was ingested into ThreatQ.

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

The screenshot shows the Threat Library interface. At the top, there's a search bar labeled 'Search for keywords...'. Below it, a filter set is shown as 'Filter Set 1' with a 'NOT' toggle. A 'Filters' dropdown menu is open, displaying a search bar and a list of filter options: 'Dates', 'Date Created', 'Expiration Date', 'Published Date', 'Source Ingest Time' (highlighted), 'Last Modified', and 'Context'. The main content area shows a table of indicators with columns: 'VALUE', 'TYPE', 'DATE CREATED', and 'LAST MODIFIED'. Two indicators are visible: one for IP address '118.195.198.108' and another for FQDN 'xidekubitavepo.foaptoa.com'.

The Source Ingest Time dialog box opens.



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

OPTION	RESULT
created before	Search results include items before a selected date
created after	Search results include items after a selected date
created between	Search results include items in a selected range of dates
created within the last	Search results include items within the selected number of days.

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

Filtering by Expiration Date

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

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



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

Indicators (3,141)

QUICK FILTERS Type Status Score Expiration

VALUE TYPE

118.195.198.108 IP Address

xidekubitavepo.foaptoa.com FQDN

dijezoxafupib.yubit.co.za FQDN

gufinegagarudin.yoyep.co.za FQDN

Expiration Date

is

Month Day Year

Jul 5 2023

Submit Cancel

The Expiration Date dialog box opens.

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

OPTION

RESULT

is	Search results include the specified date.
is not	Search results exclude items from a range of dates.
is after	Search results include items after a selected date.
is before	Search results include items before a selected date.
is between	Search results include items in a selected range of dates.
is greater than	Search results include items have exceeded their expiration date by a selected number of days.
is within the last	Search results include items within the selected number of days.
is within the next	Search results include items within a range of future dates.

OPTION	RESULT
is protected from auto-expiration	Search results include items that are protected from auto-expiration.
3. Based on the filter option you selected, select the date, date range, or number of days for the filter to use. 4. Click Submit.	

Status Filters

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



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

Filtering by Status

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



The Status filter row will appear in the filter set.

2. Click on **Add Status**.



You can select multiple statuses using the check boxes.

The search results will update with the applied filter.

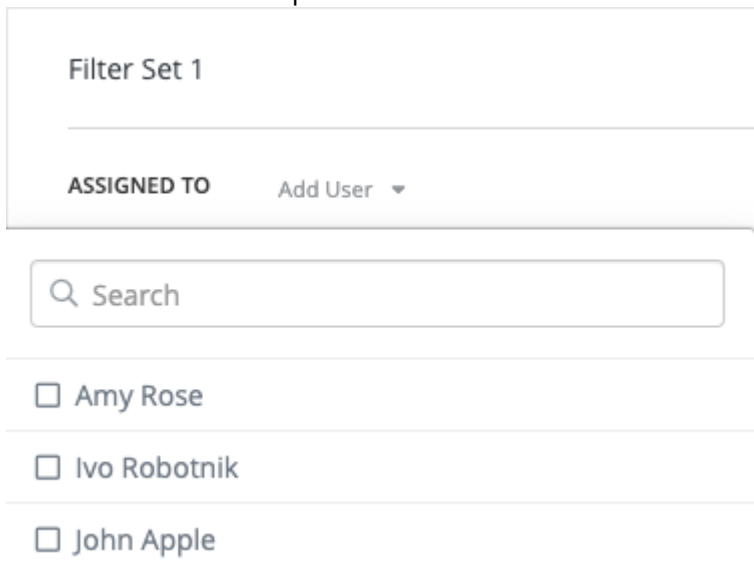
Tasks Filters

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

Filtering Tasks by Assignment

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

1. Click on the **Filters** option and select **Assigned To**.
2. Use the **Add User** dropdown to select the user.



Filter Set 1

ASSIGNED TO Add User ▼

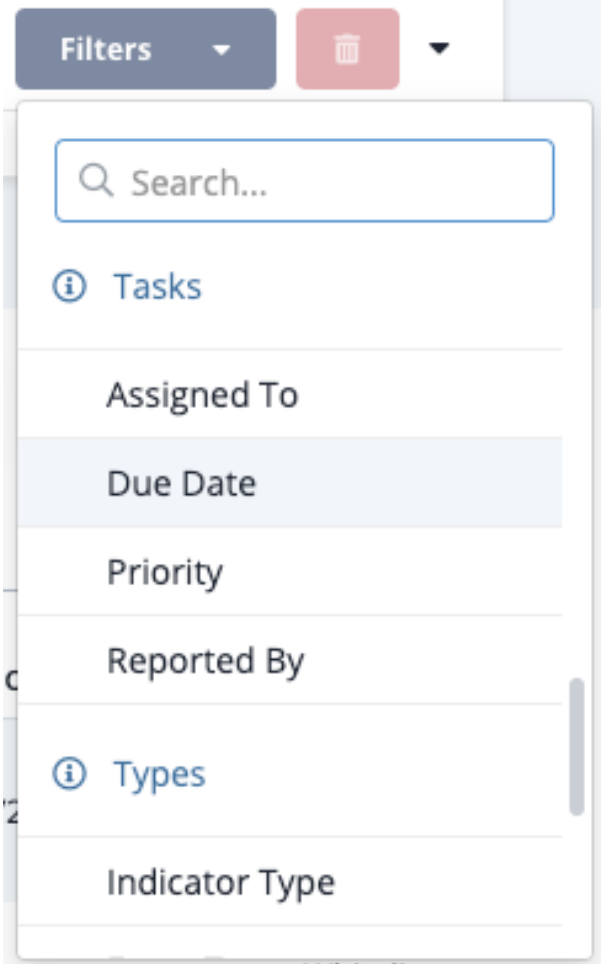
☐ Amy Rose

☐ Ivo Robotnik

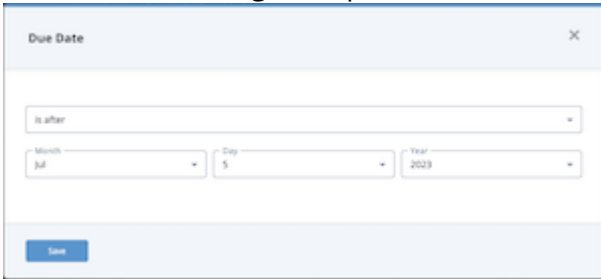
☐ John Apple

Filtering Tasks by Due Date

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



The Due Date dialog box opens.



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

OPTION	RESULT
is after	Search results include tasks with a due date after a selected date.
is before	Search results include tasks with a due date before a selected date.

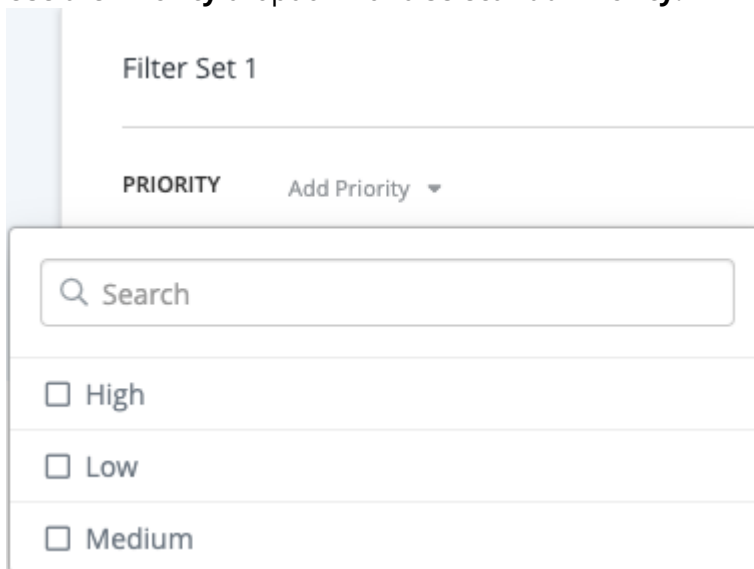
OPTION	RESULT
is between	Search results include tasks with a due date that set between the selected range of dates.
Is within the last	Search results include tasks with a due date within the last user-specified number of days.
Is within the next	Search results include tasks with a due date within the 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

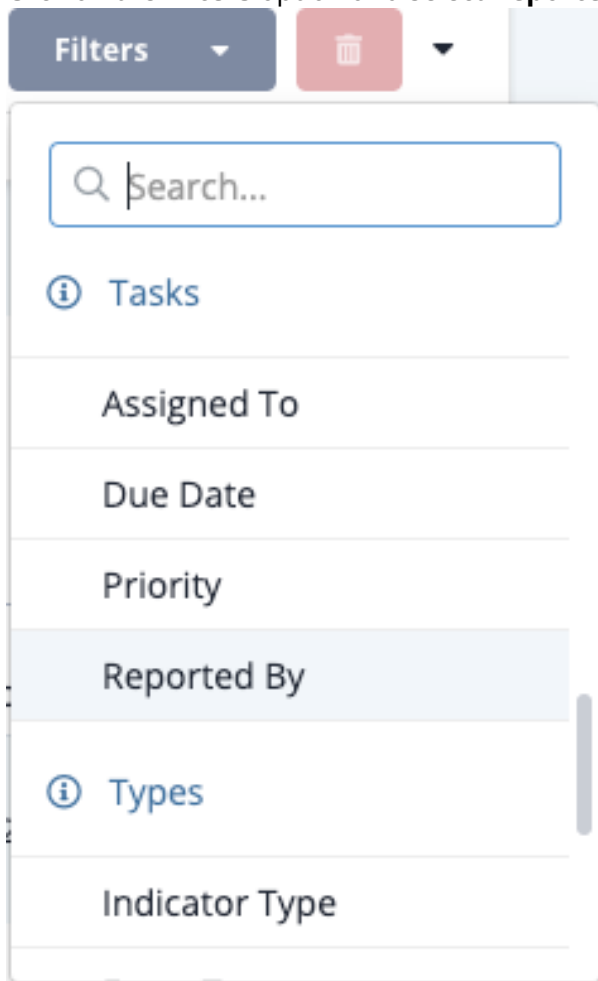
☐ Low

☐ Medium

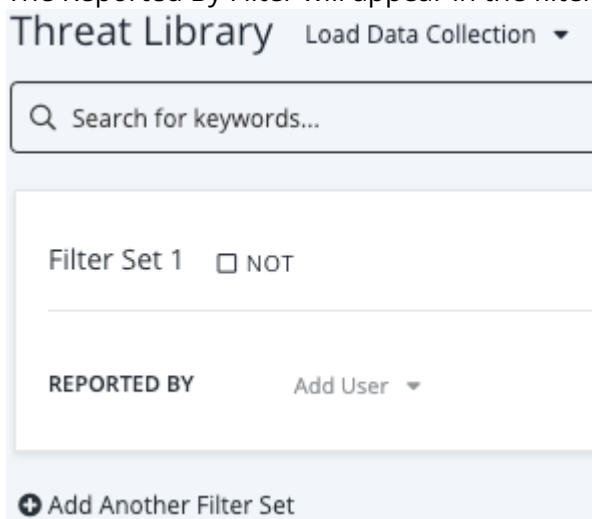
Filtering Tasks by Reported By

You can filter tasks based on who created them.

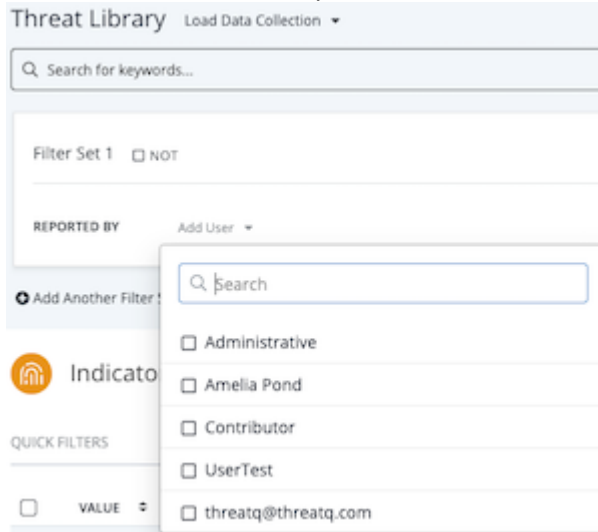
1. Click on the **Filters** option and select **Reported By**.



The Reported By Filter will appear in the filter set.



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



The screenshot shows the ThreatQ Threat Library interface. At the top, there's a search bar labeled "Search for keywords...". Below it, there's a filter section with "Filter Set 1" and a "NOT" checkbox. The "REPORTED BY" section is active, showing a dropdown menu with the "Add User" option selected. The dropdown menu lists several users: Administrative, Amelia Pond, Contributor, UserTest, and threatq@threatq.com. There's also a "QUICK FILTERS" section with a "VALUE" dropdown.

Type Filters

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

Filtering by Object Type



Filter the Signature list to include YARA types only.

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



The Type filter row will appear in the filter set.

2. Click on **Add Type**.



You can select multiple types using the check boxes.

The search results will update with the applied filter.

Managing Search Results

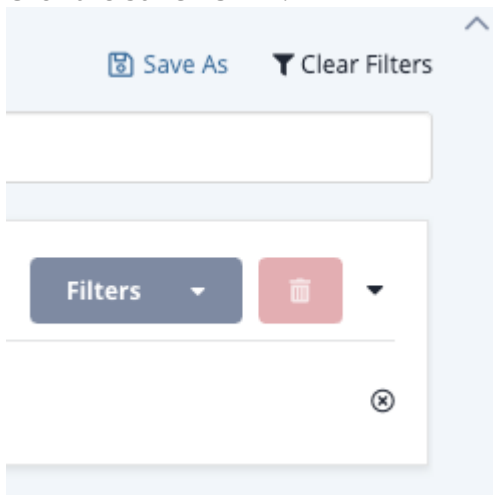
ThreatQ allows you to save your Threat Library searches as Data Collections and/or export your search results to a [CSV file](#) or [STIX bundle](#). Once saved, a Data Collection can be used by dashboard widgets, integrations, TQO actions, and other workflows.



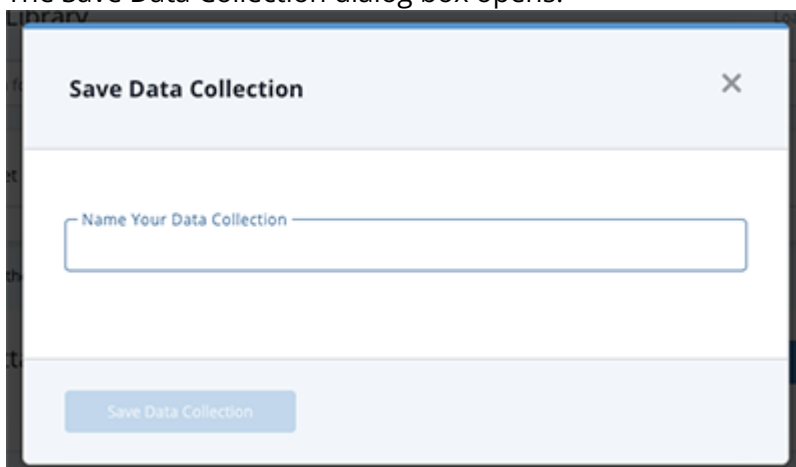
Use caution when deleting a data collection since this also removes the data collection from any widgets, integrations, TQO actions, and other workflows using it.

Saving Searches as Data Collections

1. Perform a [search](#) on the Threat Library.
2. Click the **Save As** link.



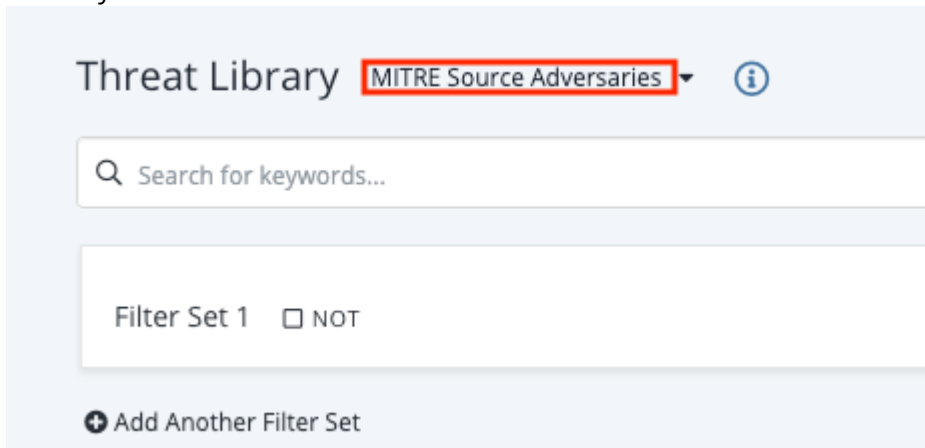
The Save Data Collection dialog box opens.



3. Enter a name for the search in the Data Collection dialog box.
4. Click the **Save Data Collection** button.

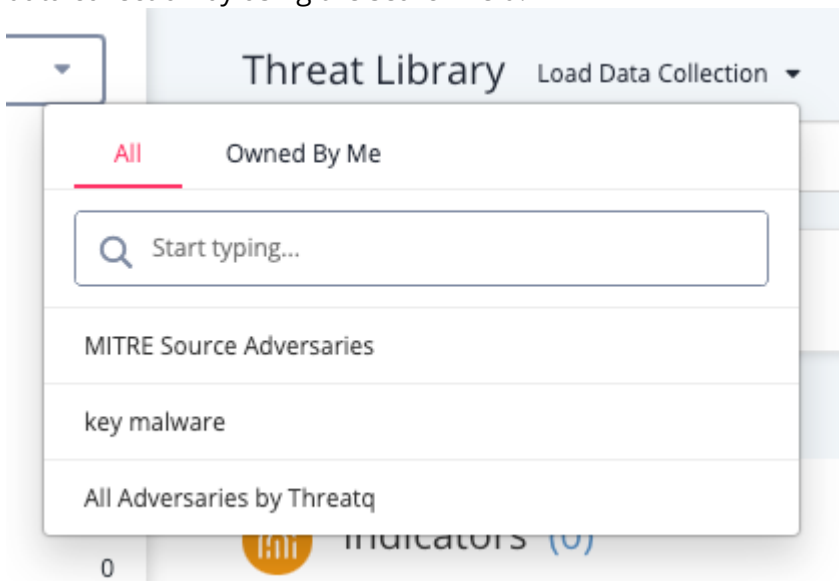
The name of the data collection is displayed at the top of the page. As the data collection creator, you have owner-level permissions and are the only user who can view or edit the data

collection. See the [Sharing Data Collections](#) section for information on allowing other users to access your data collection.



Loading Data Collections

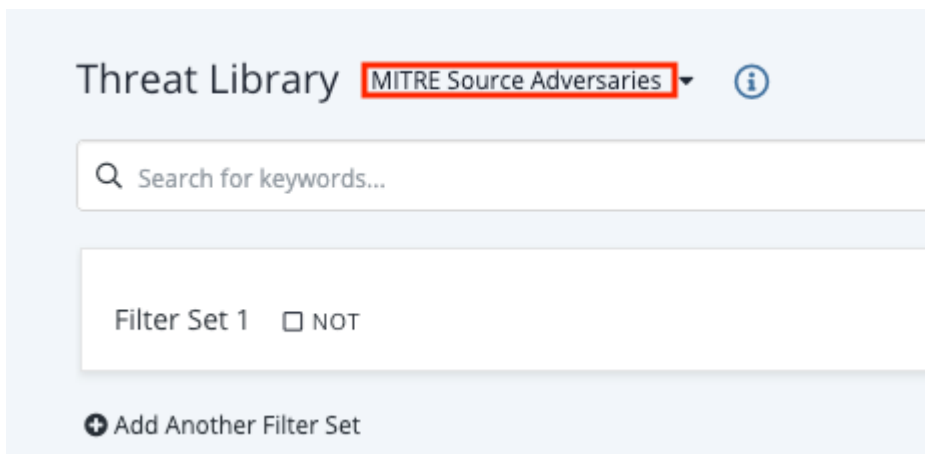
1. Navigate to the Threat Library page.
2. Click the **Load Data Collection Search** option. The data collection window defaults to the All tab that lists all the data collections you own or to which you have view or edit access. The Owned By Me tab lists the data collections for which you are the owner. You can also locate a data collection by using the search field.



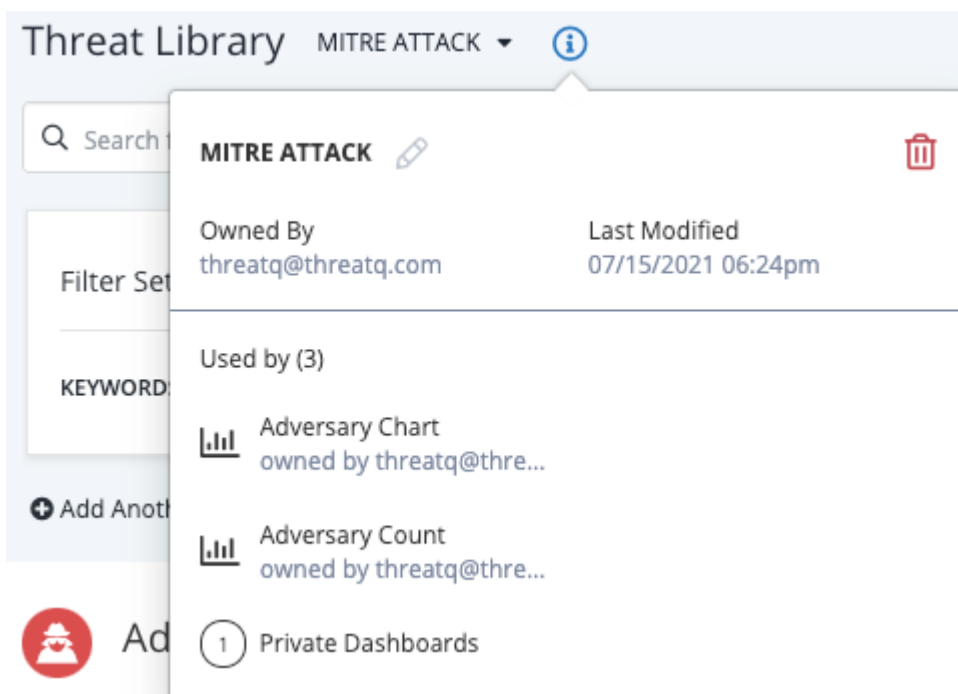
3. Select the data collection.
The data collection is displayed in the Threat Library page. The name of the data collection is listed at the top of the page.



If the data collection name is longer than forty characters, it is truncated with ellipses



4. Click the  icon to view:
 - Data collection name and owner
 - Date of the last change to the data collection
 - Dashboards, data feeds, and workflows that use the data collection. You can click these items to access the corresponding dashboard or data feed.
 - The number of private dashboards that use the data collection



Modifying a Data Collection

Users with owner or editor permissions for a data collection can make changes to it.

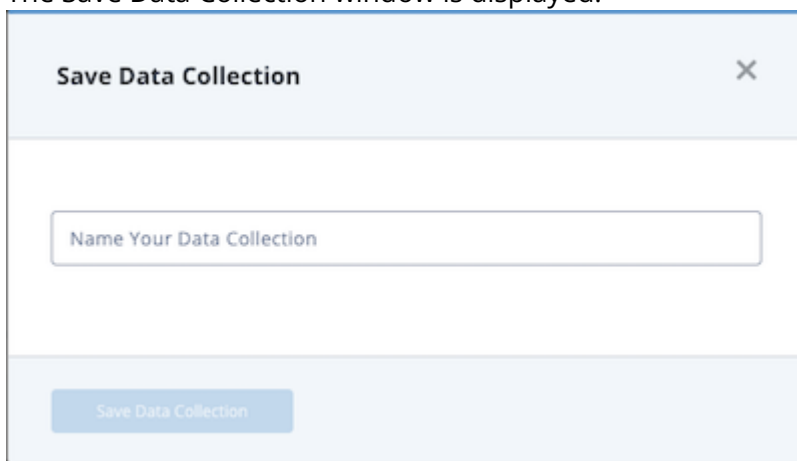
1. Navigate to the Threat Library.
2. Load the data collection you want to change.
3. Enter your changes to the data collection.
4. Click the Save link.

Copying a Data Collection

When an owner or editor makes changes to a data collection, the Save As link allows the creation of a new data collection that reflects these changes and leaves the original data collection unchanged. For example, you can add a filter to an existing Adversaries data collection to include only MITRE Enterprise ATT&CK sources, then save the new data collection as Adversaries - MITRE Enterprise.

1. Navigate to the Threat Library.
2. Load the data collection you want to copy.
3. Enter your changes to the data collection.
4. Click the **Save As** link.

The Save Data Collection window is displayed.



5. Enter the name of the new data collection.
6. Click the Save Data Collection button.

ThreatQ creates your new data collection and displays it in the Threat Library page.

Renaming a Data Collection

Only the owner of a data collection can change its name.

1. Navigate to the Threat Library.
2. Load the data collection whose name you want to change.
3. Click the  icon.
4. Click the  icon next to the data collection's name.
5. Enter the new name.
6. Click the  to save your change.

Sharing Data Collections

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

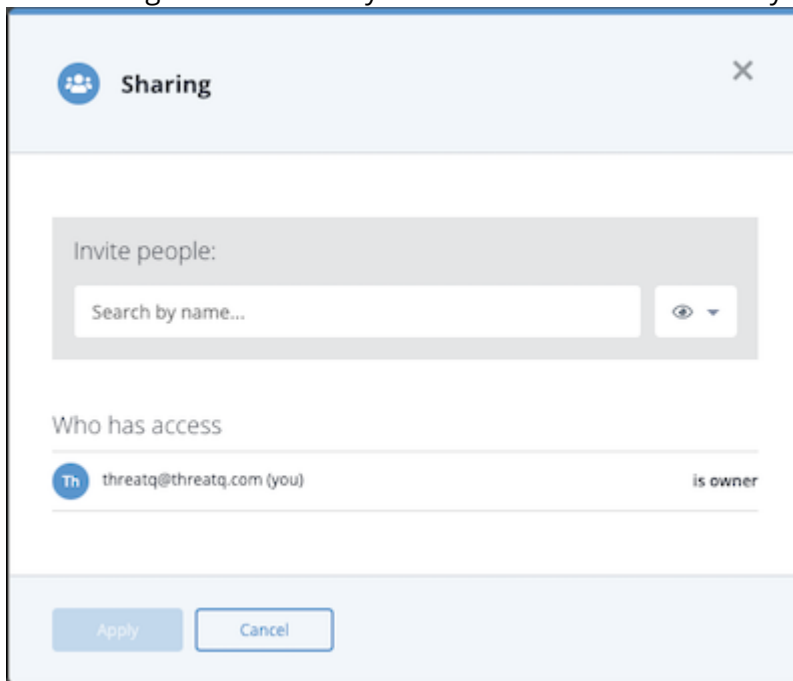
PERMISSION LEVEL	SHARED WITH OTHERS?	SHARE(D) BUTTON

Owner	No	
Owner, Editor	Yes	
Viewer	Yes	

See the [Sharing](#) topic for more information on the permissions you can assign to each data collection.

1. Navigate to the Threat Library.
2. Load the data collection you want to share.
3. Click the **Share** button.

The Sharing window allows you to select the user to which you want to grant access.



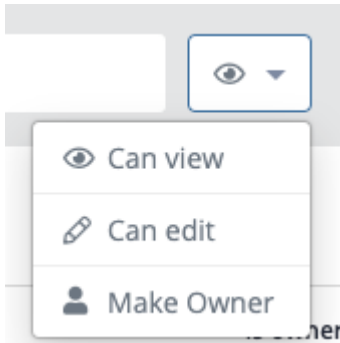
4. Click the arrow next to the  icon to select the user's permission level.



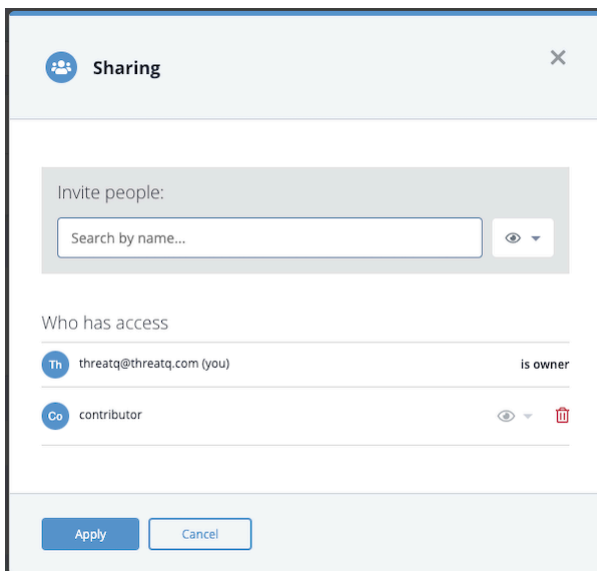
If you are granting access to all users, you must select the **Can View** option. You can only assign editing permission to individual users not to all users.



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



5. Use the search field to locate and select the user name or the **Everybody (Public)** option. This option grants view-only access to all users. The user is now listed in the Who has access list. From this listing, you can change or delete the user's permissions.



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

Removing a User's Access to a Data Collection

Only the data collection owner can remove a user's permissions.

1. Navigate to the Threat Library.
2. Load the data collection to which you want to remove a user's access.
3. Click the Share button.
4. Click the  icon next to the user's name.

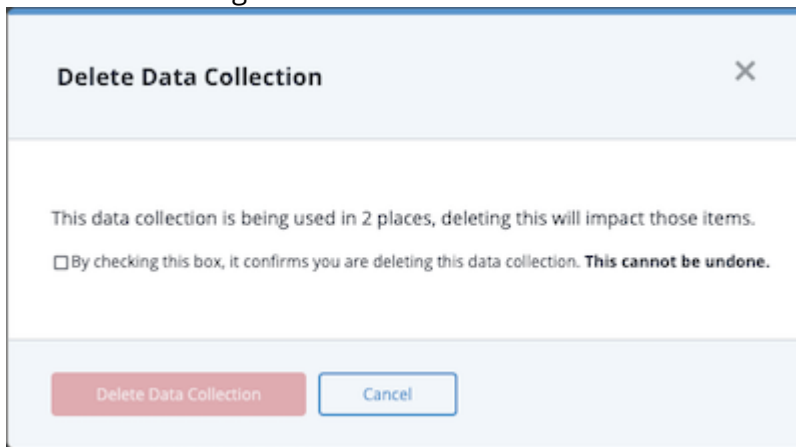
Deleting a Data Collection

To delete a data collection, you must have owner-level permissions for the data collection.

 Deletion of a data collection cannot be undone. Exercise caution before deleting a data collection as it could be associated with integrations, custom dashboards, and other workflows in use with your organization.

Method 1:

1. Navigate to the Threat Library.
2. Click the **Load Data Collection Search** option.
3. Click the Owned By Me tab.
4. Check the box next to the data collection you want to delete.
5. Click the  icon.
The Delete Data Collection window prompts you to confirm your deletion
6. Check the warning checkbox and click the **Delete Data Collection** button to confirm.



Method 2:

1. Navigate to the Threat Library.
2. Load the data collection you want to delete.
3. Click the  icon next to the data collection name.
4. Click the  icon.
The Delete Data Collection window prompts you to confirm your deletion
5. Check the warning checkbox and click the **Delete Data Collection** button to confirm.

Exporting Search Results to CSV

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

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

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

To export search results to a CSV file:

1. Navigate to the Threat Library.
2. Perform your [search](#) or load the appropriate data collection.
3. You can further customize your export by checking the checkbox next to each object you want to include.
4. Click the **Export** button  and select the option to export all objects or the option to select only checked objects.
The CSV file downloads to your desktop.

Exporting Search Results to STIX

ThreatQ supports STIX exports for all custom objects and the following seeded objects:

- Adversaries
- Assets
- Attack Pattern
- Campaign
- Course of Action
- Exploit Target
- Identity
- Incident
- Indicators
- Intrusion Set
- Malware
- Report
- Tool
- TTP
- Vulnerability

For indicators, you can create STIX export bundles for the following indicator types:

- ASN
- Binary String
- CIDR Block
- CVE
- Email Address
- Email Attachment
- Email Subject
- File Path
- Filename
- FQDN
- IP Address
- IPv6 Address
- MAC Address
- MD5
- Mutex
- Password
- SHA-1
- SHA-256
- SHA-512
- x509 Serial
- x509 Subject
- URL
- User-agent
- Username
- X-Mailer



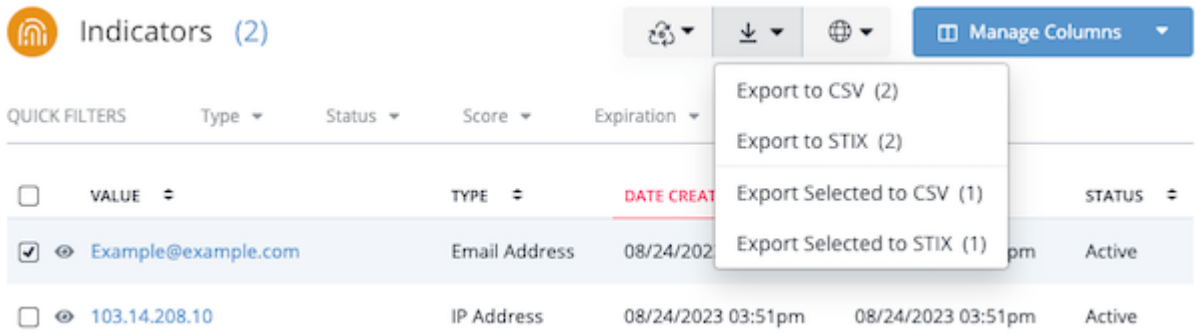
The STIX export does not include related objects.

Each STIX export can contain up to 50,000 system objects. If you attempt to exceed this maximum, a tooltip is displayed indicating that the export option is available for searches under 50,000 objects.

To export search results to a STIX file:

1. Navigate to the Threat Library.
2. Perform your [search](#) or load the appropriate data collection.
3. You can further customize your export by checking the checkbox next to each object you want to include.

- Click the **Export** button  and select the option to export all objects or the option to select only checked objects.



The screenshot shows the ThreatQ Indicators interface. At the top, there's a header with the ThreatQ logo, the text "Indicators (2)", and a toolbar with icons for refresh, export, and a globe, along with a "Manage Columns" button. Below the header, there's a table with columns: VALUE, TYPE, DATE CREATED, and STATUS. The first row is selected, showing "Example@example.com" as an "Email Address" with a "DATE CREATED" of "08/24/2023 03:51pm" and a "STATUS" of "Active". A dropdown menu is open from the export icon, showing options: "Export to CSV (2)", "Export to STIX (2)", "Export Selected to CSV (1)", and "Export Selected to STIX (1)".

The STIX file downloads to your desktop.

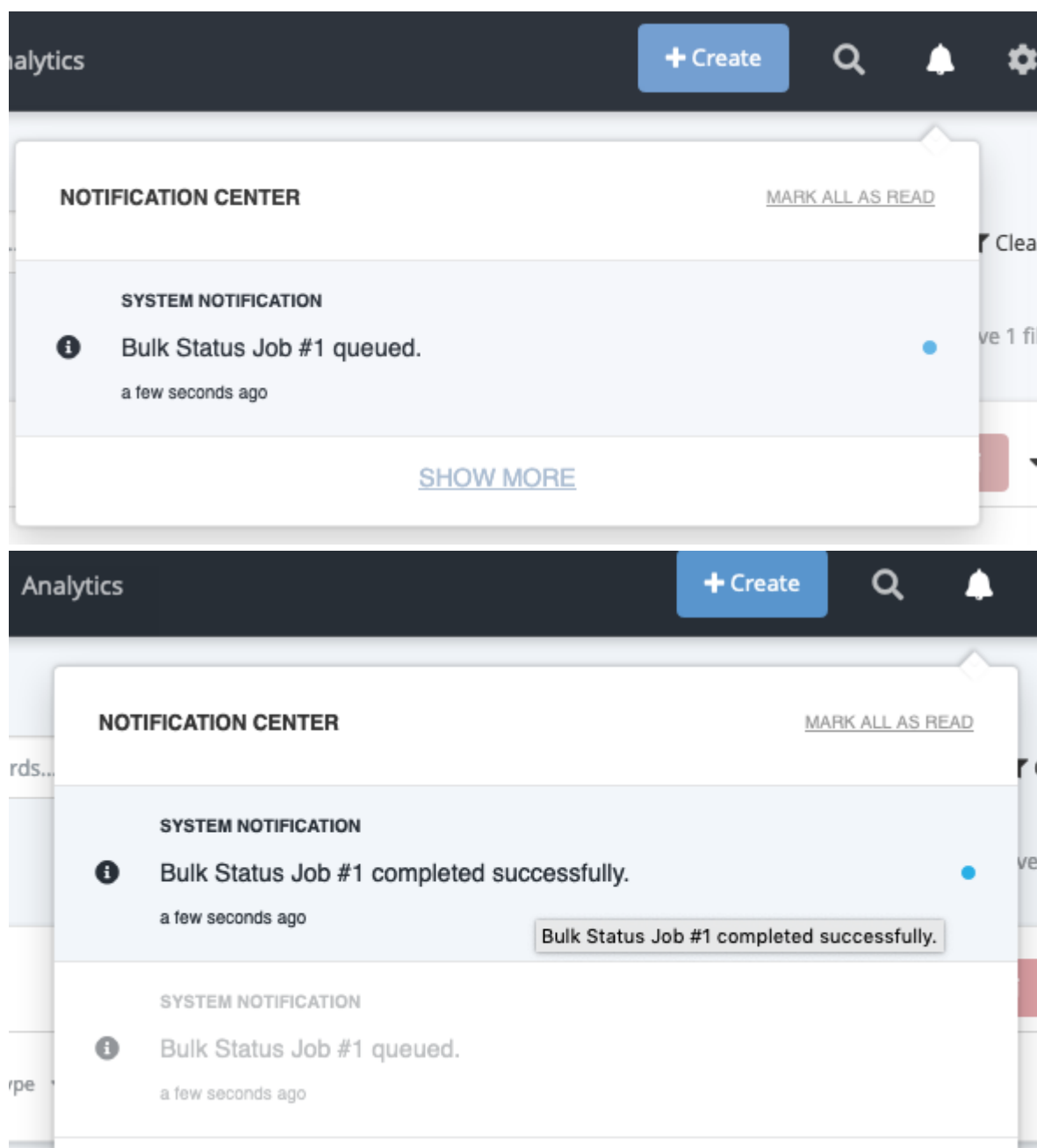
Bulk Actions

The Bulk Actions feature gives you the ability to update and delete large groups (1000+) of system objects. Once selected, the job process runs in the background and allows 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.

Upon initiating a Bulk Action, the job is queued by the system and you receive an in-app notification via the [Notification Center](#) icon. The system also notifies you, via the Notification Center, that the job has been completed.



Bulk Add Source



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

1. Perform a [search](#) on the Threat Library.

2. Click the **Bulk Actions** button .

Threat Library Load Data Collection  Save As  Clear Filters

Search for keywords...

Filter Set 1 ☐ NOT  Filters  

 Add Another Filter Set

 Indicators (3,141)     Manage Columns

QUICK FILTERS Type Status Score Expiration

☒	VALUE	TYPE	DATE CREATED		
☒	 118.195.198.108	IP Address	07/05/2023 12:03pm		
☒	 xidekubitavepo.foaptoa.com	FQDN	07/05/2023 11:31am		
☒	 dijezoxafupib.yubit.co.za	FQDN	07/05/2023 11:31am	07/05/2023 01:00pm	Whitelisted

-  Bulk Changes
 - All Indicators (3,141)
 - Selected Indicators (25)
-  Bulk Delete
 - All Indicators (3,141)
 - Selected Indicators (25)

- Click the **All** <System Object> or **Selected** <System Object> option under the *Bulk Changes* heading.

Bulk Changes Your changes will affect 100 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](#)

Apply Changes

Cancel

- Click **Add Row** under the **Source** heading.
A new row with a dropdown option is displayed.

Sources

Source

[Add new source](#)

[Add Row](#)

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.

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.
2. Click the **Bulk Actions** button .

Threat Library Load Data Collection Save As Clear Filters

Filter Set 1 ☐ NOT Filters

Add Another Filter Set

Indicators (3,141) Manage Columns

QUICK FILTERS Type Status Score Expiration

☒	VALUE	TYPE	DATE CREATED
☒	118.195.198.108	IP Address	07/05/2023 12:03pm
☒	xidekubitavepo.foaptoa.com	FQDN	07/05/2023 11:31am
☒	dijezoxafupib.yubit.co.za	FQDN	07/05/2023 11:31am

Bulk Changes

All Indicators (3,141)
Selected Indicators (25)

Bulk Delete

All Indicators (3,141)
Selected Indicators (25)

3. Click the **All <System Object>** or **Selected <System Object>** option under the *Bulk Changes* heading.

The Bulk Changes page is displayed.

Bulk Changes

Your changes will affect 100 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](#)

Apply Changes

Cancel



Only the Bulk Actions that relate to the type of system object you selected will load on the Bulk Changes form.

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

Attributes

Add / Remove Add	Name ASN	Value 13335	Source abuse.ch URLhaus Plai...	
	Add new name	Add new value	Add new source	

Add Row +

Attributes

Add / Remove Remove	Name ASN	Value 13335	

Add Row +



Click **Add Row** and repeat steps 4-5 to add/remove multiple attributes. See the [Scenarios](#) section below for more details.

- Click the **Apply Changes** button located at the bottom of the form.

Bulk Add/Remove Attribute Scenarios

Add Multiple Attributes

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

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

Results

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



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

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



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

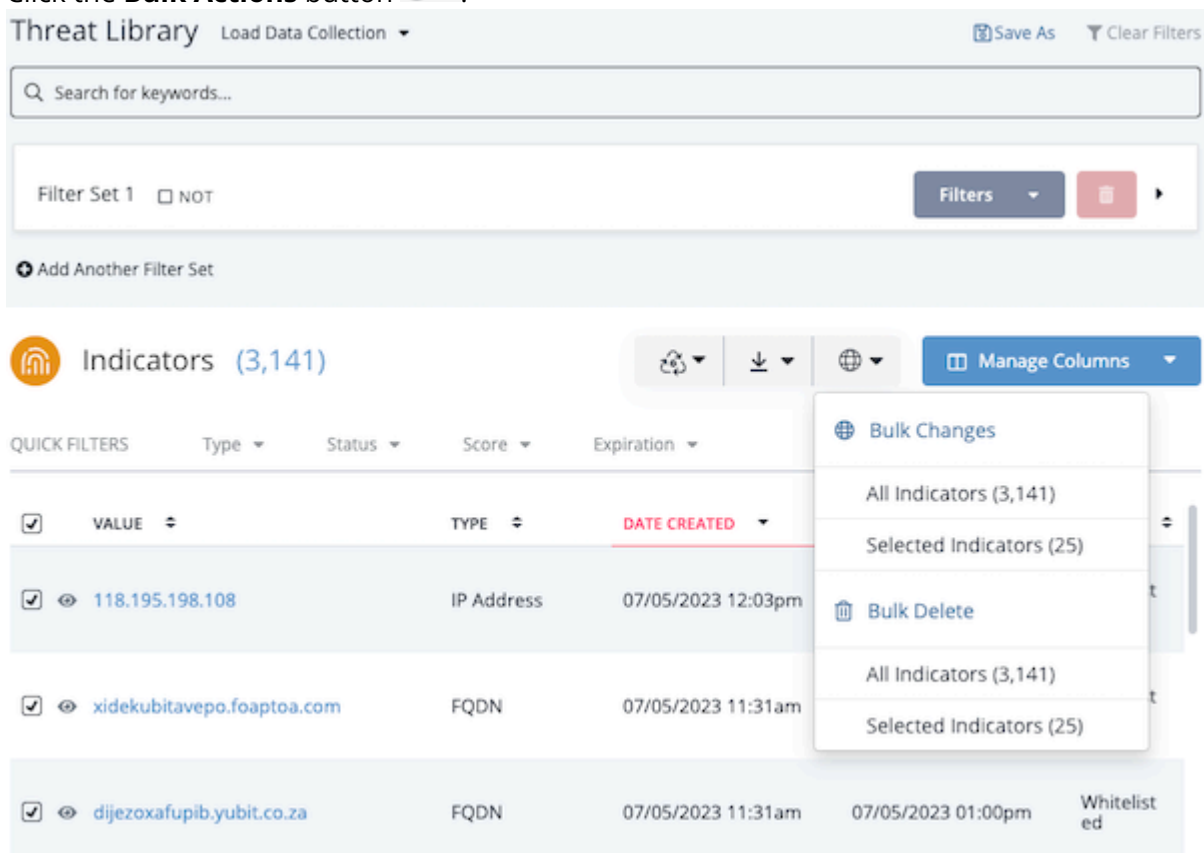
Add and Remove Attributes

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

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

Bulk Add/Remove Tags

1. Perform a [search](#) on the Threat Library.
2. Click the **Bulk Actions** button .



The screenshot shows the Threat Library interface. At the top, there's a search bar and a 'Load Data Collection' dropdown. Below the search bar, there's a filter section with 'Filter Set 1' and a 'NOT' checkbox. A 'Filters' button is also present. Below the filter section, there's a 'Add Another Filter Set' button. The main content area shows a table of indicators. The table has columns for 'Type', 'Status', 'Score', and 'Expiration'. The first row is selected, and a context menu is open over it. The context menu has two main sections: 'Bulk Changes' and 'Bulk Delete'. Under 'Bulk Changes', there are two options: 'All Indicators (3,141)' and 'Selected Indicators (25)'. Under 'Bulk Delete', there are also two options: 'All Indicators (3,141)' and 'Selected Indicators (25)'. The table data includes indicators like '118.195.198.108' (IP Address), 'xidekubitavepo.foaptoa.com' (FQDN), and 'dijezoxafupib.yubit.co.za' (FQDN).

3. Click the **All <System Object>** or **Selected <System Object>** option under the *Bulk Changes* heading.

The Bulk Changes page is displayed.

Bulk Changes

Your changes will affect 100 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](#)

Apply Changes

Cancel

4. 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 



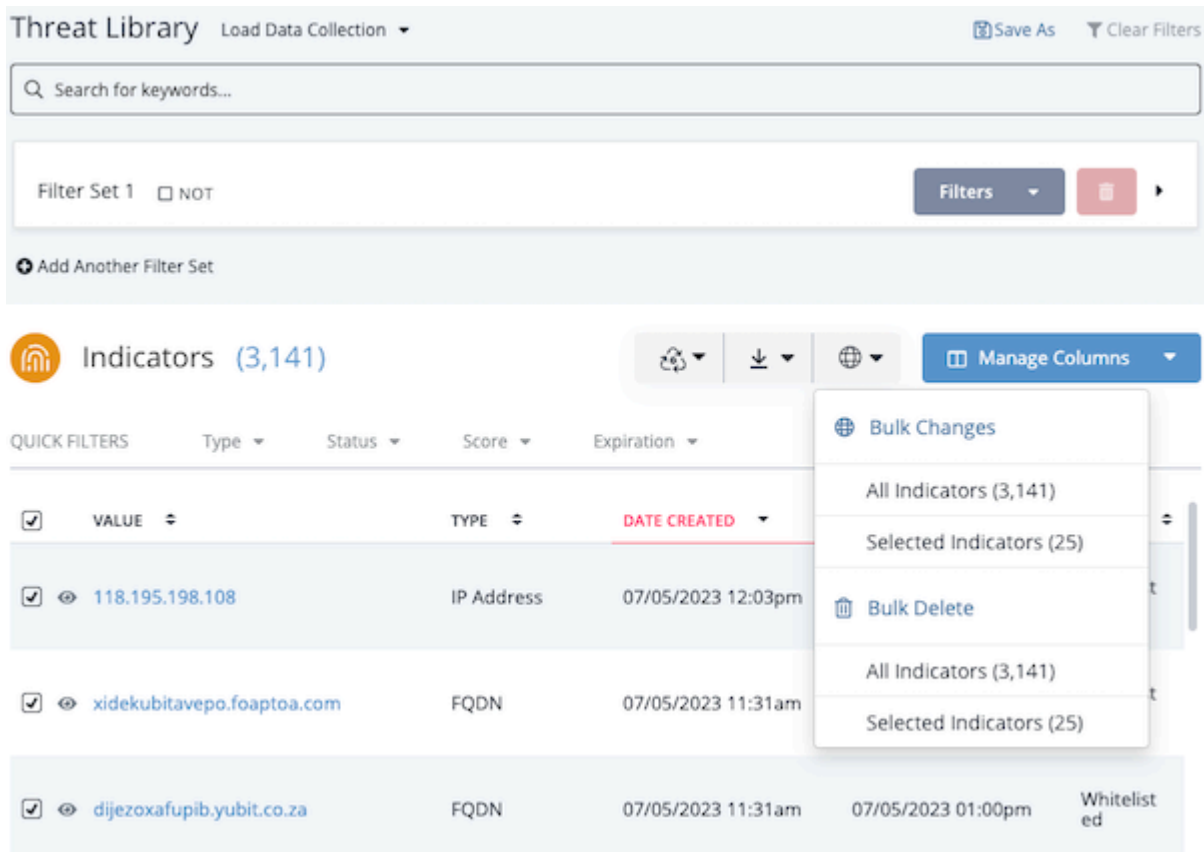
Click on **Add Row** and repeat step 3 to add/remove multiple tags.

- Click the **Apply Changes** button located at the bottom of the form.

Bulk Change Expiration Date

 This function can only be performed on Indicators.

- Perform a [search](#) on the Threat Library.
- Click the **Bulk Actions** button .



The screenshot shows the ThreatQ Threat Library interface. At the top, there is a search bar labeled "Search for keywords...". Below the search bar, there is a filter section with "Filter Set 1" and a "NOT" checkbox. To the right of the filter section, there are buttons for "Filters" and a red button with a trash icon. Below the filter section, there is a link to "Add Another Filter Set".

The main section of the interface is titled "Indicators (3,141)". It features a table with columns for "QUICK FILTERS", "Type", "Status", "Score", and "Expiration". The table contains three rows of indicators:

QUICK FILTERS	Value	Type	Score	Expiration
☒	118.195.198.108	IP Address		07/05/2023 12:03pm
☒	xidekubitavepo.foaptoa.com	FQDN		07/05/2023 11:31am
☒	dijezoxafupib.yubit.co.za	FQDN		07/05/2023 11:31am

On the right side of the table, there is a "Bulk Actions" menu. The menu is open, showing options for "Bulk Changes" and "Bulk Delete". Under "Bulk Changes", there are two options: "All Indicators (3,141)" and "Selected Indicators (25)". Under "Bulk Delete", there are also two options: "All Indicators (3,141)" and "Selected Indicators (25)".

- Click the **All <System Object>** or **Selected <System Object>** option under the *Bulk Changes* heading.

The Bulk Changes page is displayed.

Bulk Changes Your changes will affect 100 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](#)

Apply Changes

Cancel

4. 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.

- Click the **Apply Changes** button 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

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

Setting Expiration policy to a specific day

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



The date selected must be a future date.

- 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

- The user selects a set of indicators using the advanced search.
- The user selects **Extend Expiration Date** from the Change Expiration option.
- The user enters the number of days to extend.
- 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

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

Protecting items from auto-expiration

- The user selects a set of indicators using the advanced search.
- The user selects **Protect from Auto-Expiration** from the Change Expiration option.
- 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

- The user selects a set of expired indicators using the advanced search.
- The user selects **Set a New Expiration Date** from the Change Expiration option.
- The users selects a day using the date picker.
The date selected must be a future date.
- 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

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

2. The user selects **Remove Expiration Date** from the Change Expiration option.
3. The expired indicators in the set are skipped.

Bulk Delete

The Bulk Delete feature offers users with Maintenance and Administrative roles the ability to select and delete system objects of all types, excluding Files and Tasks, from the Advanced Search page. In addition to the system object, bulk delete will also delete all child records such as attributes and relationships.



Individual Tasks and Files can be deleted by accessing the object's details page and selecting Delete Task/File from the Actions menu.

Once selected, the job process will run in the background and allow you to continue working within ThreatQ. An in-app notification will alert you when a Bulk Delete job has been queued and when it has been completed. You can also view the status and outcome of the job from the [Job Management](#) page.



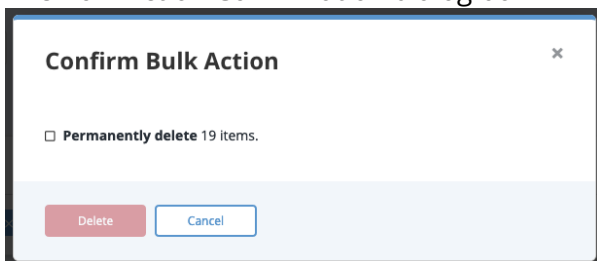
The Bulk Delete function **permanently** deletes selected indicators from the system. Once deleted, you will be unable to undo the action. If you are executing a Bulk Delete on a large group of indicators, ThreatQuotient highly recommends performing a backup of your system before performing this function.



Based on the size of your bulk delete job and the system resources available, you may find that the estimated job duration is quite long. In these rare instances, contact ThreatQ support to explore your other options for deleting a large number of objects.

1. Perform a [search](#) on the Threat Library.
2. Click the **Bulk Actions** button  .
3. Click the **All <System Object>** option under the *Bulk Delete* heading.

The Bulk Action Confirmation dialog box will load.



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

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. Bulk relationship updates are restricted to less than ten thousand objects and up to ten relationships per batch.



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.
2. Click the **Bulk Actions** button .
3. Click the **All <System Object>** or **Selected <System Object>** option under the *Bulk Changes* heading.

The Bulk Changes page is displayed.

Bulk Changes
Your changes will affect 100 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](#)

Add Row

Attributes

Add / Remove

Add

Name

Value

Source

[Add new name](#)
[Add new value](#)
[Add new source](#)

Add Row

Sources

Source

[Add new source](#)

Add Row

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.

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

Relationships

Limit search to
All Objects

Adversaries

5. Enter an object name.



By default, this field searches for objects that begin with the search string you enter. To search for objects that include your search string but do not begin with it, you must use a wildcard (% OR *) search.

Examples:

1. When you enter "us", your search returns **USB**ferry and **USB**Stealer.
2. When you enter "%us" or "*us", your search returns **Aquarius**, **Lazarus** Group, **Dust** Storm, **USB**ferry, and **USB**Stealer.

6. After you select an object, the Add/Remove option appears.

Relationships

Limit search to
All Objects

Add / Remove
Add

INDICATOR abdahmani.serveftp.net

7. Select either **Add** or **Remove**.
8. 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.
9. Click the **Apply Changes** button located at the bottom of the form.

Bulk Status Change



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

Whitelisted Indicators are not affected by Bulk Status Change. If a Whitelisted Indicator is included in the set of system objects selected for a Bulk Status Change, the platform will skip the object without making a status change.

1. Perform a [search](#) on the Threat Library.
2. Click the **Bulk Actions** button .
3. Click the **All <System Object>** or **Selected <System Object>** option under the *Bulk Changes* heading.
The Bulk Changes page is displayed.

Bulk Changes

Your changes will affect 100 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](#)

Apply Changes

Cancel

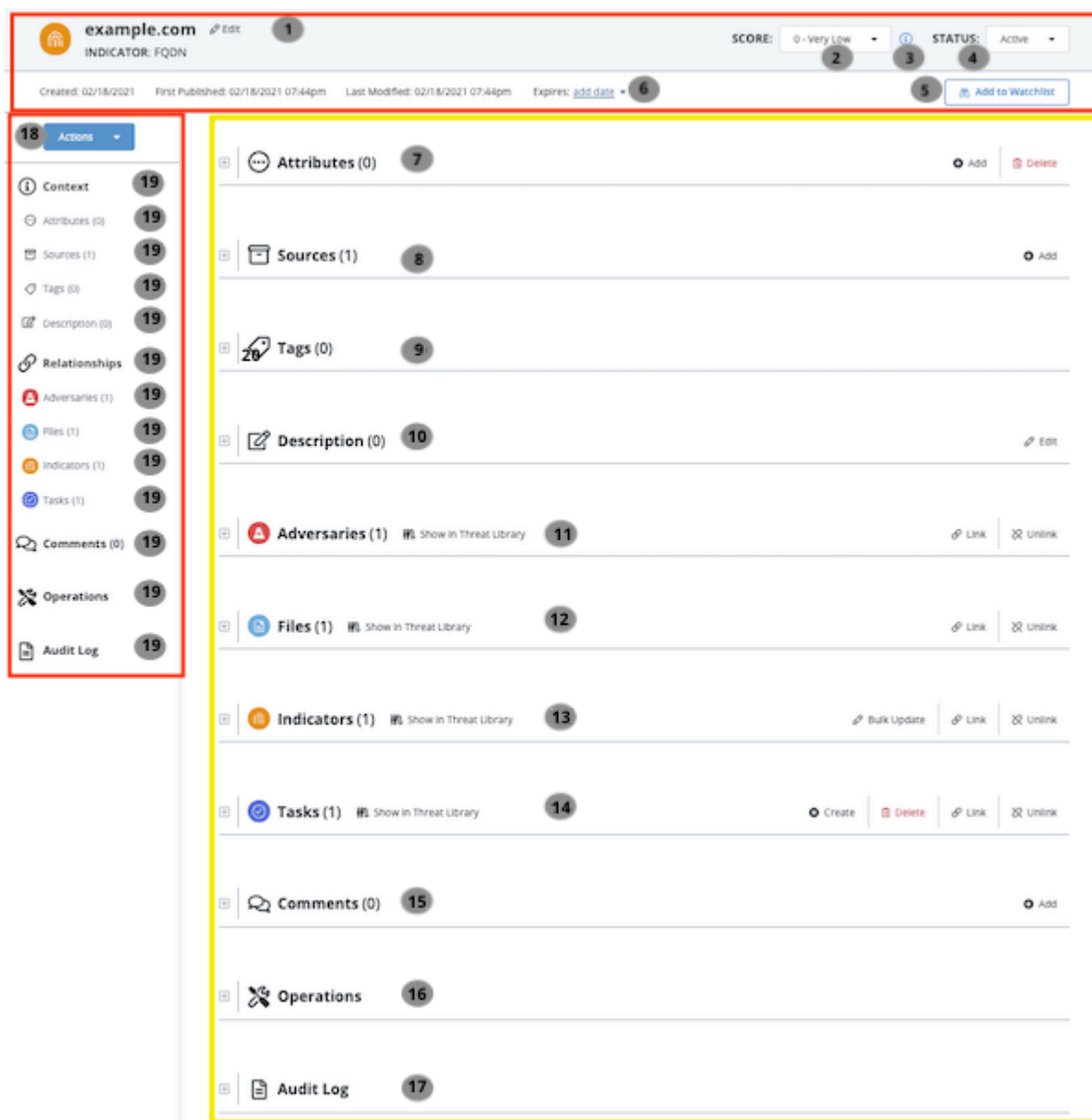
4. Use the dropdown provided to select a new status to be applied to the selected objects.
5. Click on **Apply Changes** button located at the bottom of the form.

Object Details

About Object Details

You can click on an object within the ThreatQ application to access its details page. The Object Details page provides you with an in-depth look at an individual object. You can enter comments for others to view, link related objects, and view an audit log of all activity associated with the object.

Specific objects, such as Indicators, display additional information such as the indicator's status, score, and expiration data.



Items marked with an * in the Object Details Legend indicate an option only available to specific object types.

OBJECT DETAILS PAGE LEGEND

Header Section

NUMBER	FIELD	DESCRIPTION	REFERENCE
1	Edit Object Link	The Edit link allows you to edit specific details about an object. Edit fields will differ based on the type of object.	N/A
2	Score Selection* Applies to Indicator Object Types Only	The Score Selection dropdown allows you to override an indicator's score set by the scoring algorithm.	1. Indicator Expiration 2. Scoring Algorithms
3	Scoring Influence* Applies to Indicator Object Types Only	You can click on the icon to review the criteria utilized by the application's scoring algorithm to generate the Indicator's score.	• Scoring Algorithms
4	Status* Applies to Indicator Object Types Only	The Status dropdown menu allows you to manually set the status of an indicator. Default statuses include: Active, Expired, Indirect, Review, and Whitelisted.	• Indicator Status • Indicator Statuses Management (Object Management)
5	Add to Watchlist	The Watchlist toggle button allows you to add and remove the object from the Watchlist widget.	1. Add/Remove an Object to the Watchlist
6	Expiration* Applies to Indicator Object Types Only	The Expire link allows you to set an expiration date for the indicator, protect from auto-expiration policies, and remove an existing set expiration date.	• Indicator Expiration • Indicator Expiration

OBJECT DETAILS PAGE LEGEND

[Policies](#) (Data Controls)

Details Section

Number	Pane	Description	Reference
7	Attributes	The Attributes pane displays attributes associated with the object. You can Add, Edit, and Delete attributes found in this section.	• Attributes Pane
8	Sources	The Sources pane displays sources associated with the object. You can Add, Edit, or Remove sources.	• Sources Pane
9	Tags	The Tags pane displays tags associated with the object. You can Add and Delete tags found in this section.	• Tags Pane
10	Description	The Description pane allows you to add general information about the object.	• Description Pane
11	Adversary	The Adversaries pane displays adversaries associated with the object.	• Relationships Panes
12	Files	The Files pane displays files associated with the object and gives you the option to preview, download, and/or parse the file. If your browser does not support file preview for a specific file type, the file is downloaded instead.	• Relationships Panes

OBJECT DETAILS PAGE LEGEND



You cannot preview a malware locked file.

13	Indicators	The Indicators pane displays indicators associated with the object.	• Relationships Panes
14	Tasks	The Tasks pane displays tasks associated with the object.	• Relationships Panes
15	Comments	The Comments pane allows you to record comments about the object for other users to read and reference.	• Relationships Panes
16	Operations	The Operations pane allows you to associate third-party attributes and related indicators to the indicator.  This options requires the installation of Operations. See the Managing Integrations topic for more details.	• About Integrations Management
17	Audit Log	The Audit Log panel displays all actions and changes made to an Object.	• Audit Log

Left-Hand Navigation

Number	Field	Description	Reference

OBJECT DETAILS PAGE LEGEND

18	Actions Menu	The Actions menu lists the following options: • Add Attribute • Add Comment • Add Relationship • Add Source • Create Task • Generate PDF • Delete Indicator • Start Investigation • Add to Investigation	• Actions Menu
19	Details Navigation Tabs	This allows you to jump to a particular pane on the Object Details page.	N/A

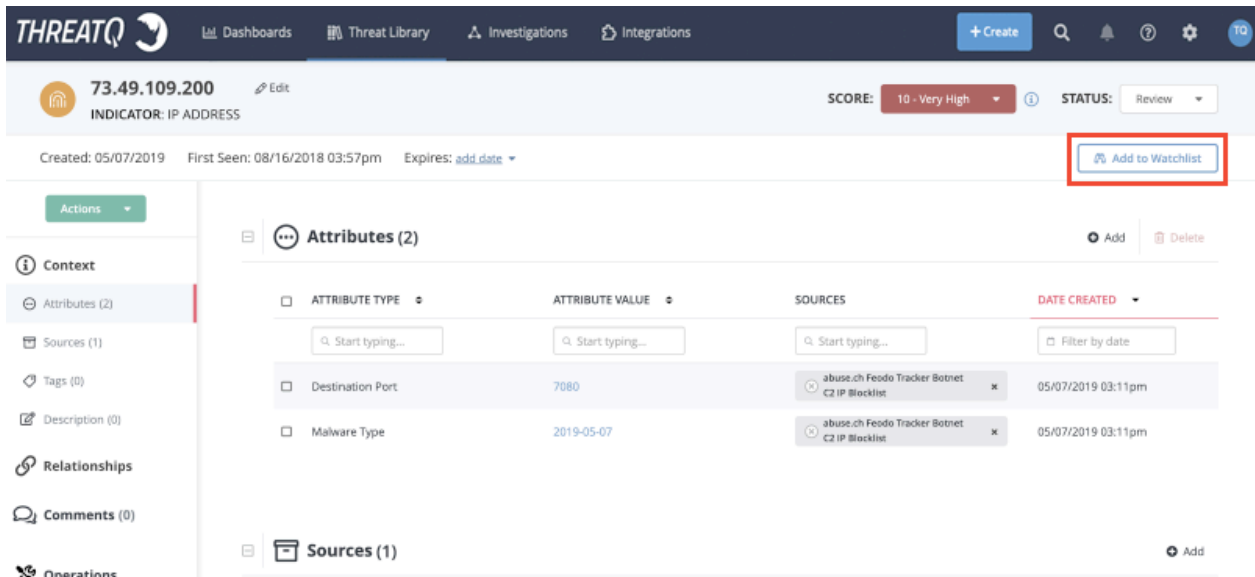
Adding/Removing an Object to the Watchlist

Read Only users do not have the option to add 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 the object. Or, click **Remove from Watchlist** to remove the object.



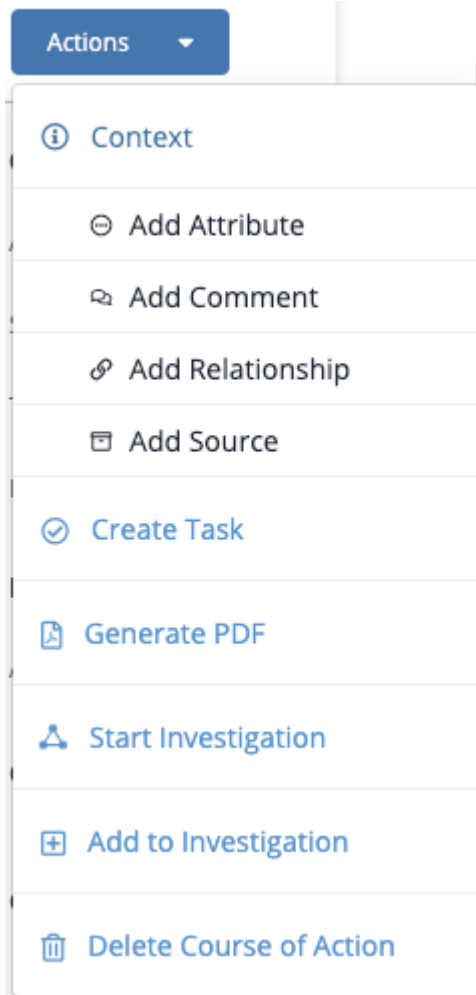
The screenshot shows the ThreatQ user interface. At the top, there's a navigation bar with 'Dashboards', 'Threat Library', 'Investigations', and 'Integrations'. Below this, the main header displays the indicator '73.49.109.200' with a score of '10 - Very High' and a status of 'Review'. A red box highlights the 'Add to Watchlist' button in the top right corner. The left sidebar contains a 'Context' menu with options like 'Attributes (2)', 'Sources (1)', 'Tags (0)', 'Description (0)', 'Relationships', 'Comments (0)', and 'Operations'. The main content area shows 'Attributes (2)' with a table listing attributes like 'Destination Port' and 'Malware Type'. Below this, there's a 'Sources (1)' section.

ATTRIBUTE TYPE	ATTRIBUTE VALUE	SOURCES	DATE CREATED
Destination Port	7080	abuse.ch Feodo Tracker Botnet C2 IP Blocklist	05/07/2019 03:11pm
Malware Type	2019-05-07	abuse.ch Feodo Tracker Botnet C2 IP Blocklist	05/07/2019 03:11pm

Depending on your selection, the object is added to/removed from the Watchlist on the system default dashboard.

Actions Menu

The Action Menu, located on the left-hand of the Object Details page, allows users to quickly execute system object processes.



Actions Include:

ACTION	FUNCTION	REFERENCE
Add Attribute	Brings up the Add Details dialog box which allows you to add an attribute to the object.	• Attributes Pane
Add Comment	Displays a new text entry field in the Comments pane.	• Comments Pane

ACTION	FUNCTION	REFERENCE
Add Relationship	Brings up the Add Relationships window which allows you to link other system objects to the object.	• About Relationships Panes • Additional Related Object Actions
Add Source	Brings up the Add Details window which allows you to add a source to the object.	• Sources Pane
Create Task	Opens the Add Task window.	
Generate PDF	Generates a PDF report of the object.	• Reports
Start Investigation	Opens the Create Investigation window so that you can create a new investigation to which the object is automatically added.	• Editing an Investigation
Add to Investigation	Opens the Select Investigation window which allows you to add the object to one or more existing investigations.	
Delete <Object>	The Are You Sure? window prompts you to confirm the deletion by clicking the Delete button.	

Context Panes

About Context Panes

Based on the system object type, the Context section of the object details page displays:

- Attributes
- [Sources](#)
- [Tags](#)
- [Descriptions](#)
- [Spearphish Details](#)

Sources Pane

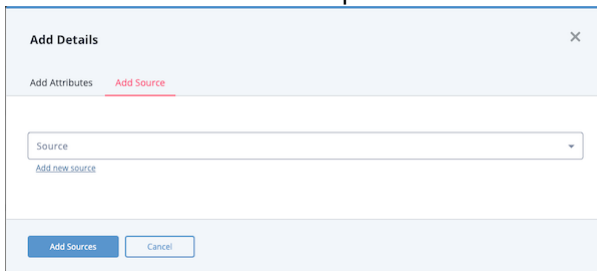
The Sources pane displays all Sources associated with the system object. From this pane, Maintenance Account, Administrative Access, and Primary Contributor Access accounts can add a source to the object, update a source's TLP label, or remove a source from the object. Read Only Access accounts can view sources but not remove or update them.

See the *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

1. Locate the Sources pane on the object details page.
2. Click the Add option.

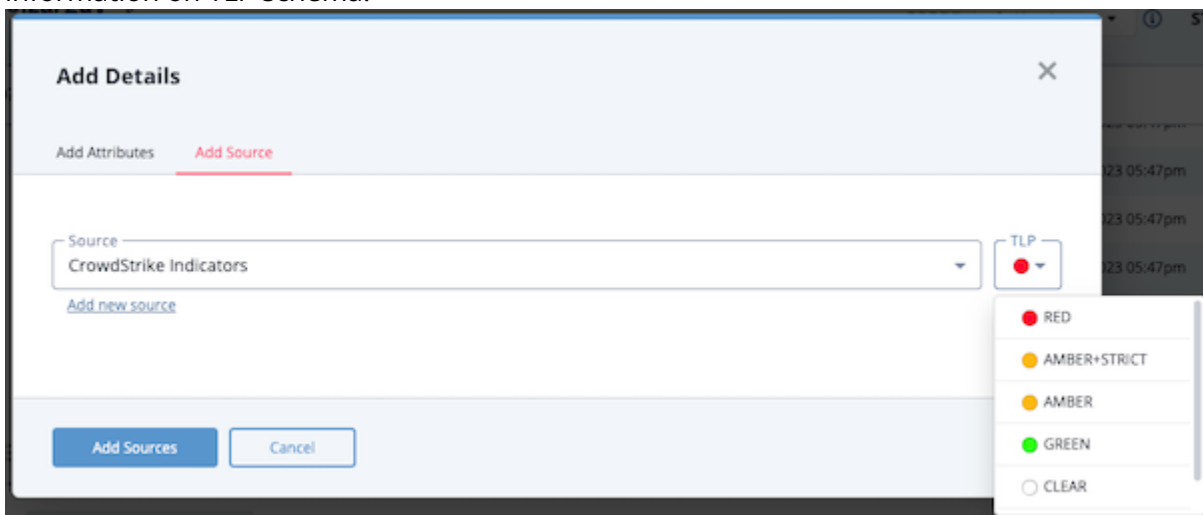
The Add Details window opens with the Add Source tab selected by default.



The screenshot shows a modal window titled 'Add Details' with a close button (X) in the top right corner. Inside, there are two tabs: 'Add Attributes' and 'Add Source', with 'Add Source' being the active tab. Below the tabs is a 'Source' dropdown menu with a downward arrow. Underneath the dropdown is a link that says 'Add new source'. At the bottom of the window are two buttons: 'Add Sources' and 'Cancel'.

3. Use the Source field's drop-down list to select a source. If TLP is enabled, you can override the source's default TLP label.

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



This screenshot shows the 'Add Details' window with the 'Add Source' tab active. The 'Source' dropdown menu is open, showing 'CrowdStrike Indicators' as the selected option. To the right of the source dropdown is a 'TLP' dropdown menu, which is also open, showing a list of TLP labels: RED (with a red dot), AMBER+STRICT (with an orange dot), AMBER (with a yellow dot), GREEN (with a green dot), and CLEAR (with a white dot). The 'Add Sources' and 'Cancel' buttons are visible at the bottom.



Even though the Source drop-down lists displays all sources, you cannot add a source to an object if it has already been added.

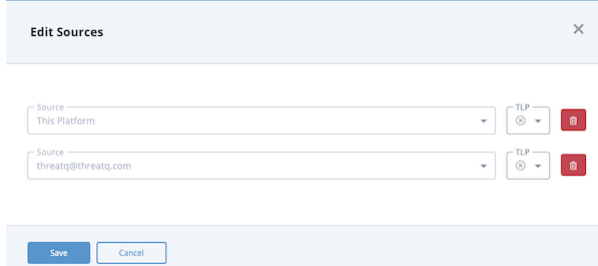
4. Click the **Add Sources** button.

Editing a Source

The Edit Sources window allows you to edit a source's TLP label (if TLP visibility is enabled via the [TLP tab](#)) or remove the source from the object.

1. Locate the Sources pane on the object details page.
2. Click the Edit option.

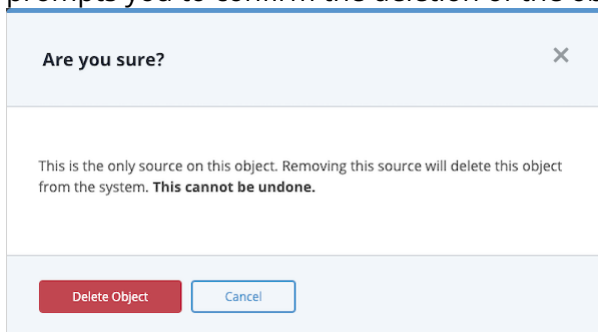
This Edit Sources window lists all the sources associated with the system object.



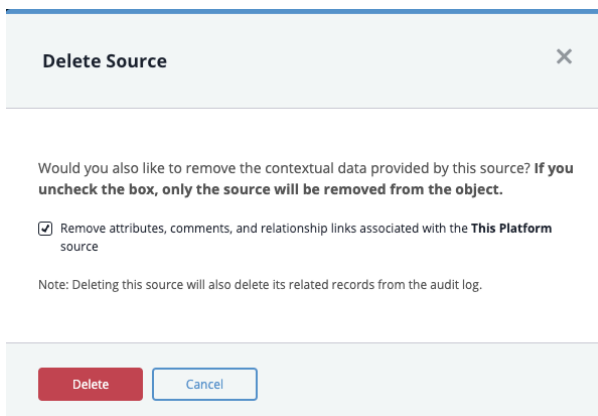
3. To update the source's TLP, select the new TLP label from the dropdown list and click the **Save** button.

To delete the source, click the trashcan icon next to the TLP field and go to step 4.

4. If you are removing the only source associated with the object, the **Are you sure** window prompts you to confirm the deletion of the object by clicking the **Delete Object** button.



If the object has multiple sources, the Delete Source window prompts you to specify whether you want to delete the source and its related context. Go to step 5.



5. To remove the object and its related context, leave the **Remove attributes, comments, and relationship links associated with the <source name> source** field checked.



Removing a relationship link does not delete the linked object. It only removes the link between the objects.

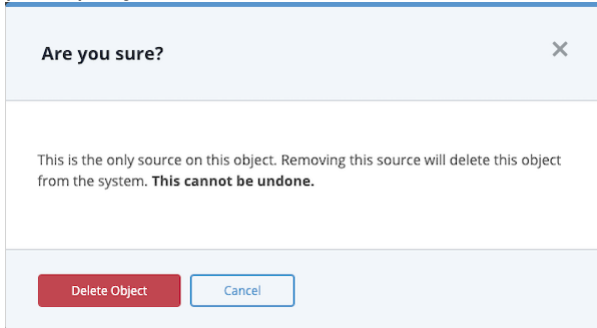
To remove the source but retain its related context, uncheck the option.

6. Click the **Delete** button.

Deleted sources are recorded in the audit log as Removed. Removed contexts such as attributes, comments, or relationships are not recorded in the audit log.

Removing a Source from an Object

1. Locate the Sources pane on the object details page.
2. Click the + next to pane title, **Sources**, to expand your view of the pane.
3. Click the **X** located to the right of the source's name.
4. If you are removing the only source associated with the object, the **Are you sure** window prompts you to confirm the deletion of the object by clicking the **Delete Object** button.

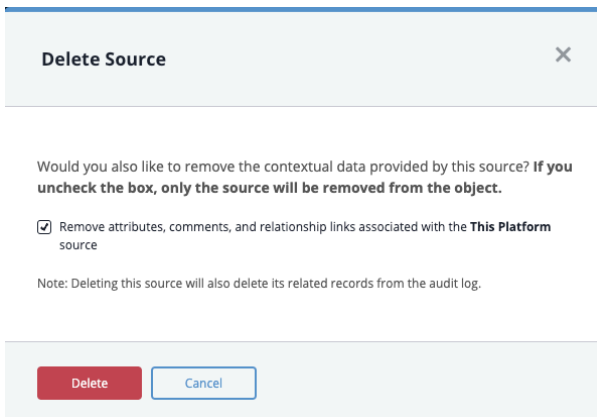


Are you sure?

This is the only source on this object. Removing this source will delete this object from the system. **This cannot be undone.**

Delete Object Cancel

If the object has multiple sources, the Delete Source window prompts you to specify whether you want to delete the source and its related context. Go to step 5.



Delete Source

Would you also like to remove the contextual data provided by this source? If you **uncheck the box, only the source will be removed from the object.**

☒ Remove attributes, comments, and relationship links associated with the **This Platform** source

Note: Deleting this source will also delete its related records from the audit log.

Delete Cancel

5. To remove the object and its related context, leave the **Remove attributes, comments, and relationship links associated with the <source name> source** field checked.



Removing a relationship link does not delete the linked object. It only removes the link between the objects.

To remove the source but retain its related context, uncheck the option.

6. Click the **Delete** button.

Deleted sources are recorded in the audit log as Removed. Removed contexts such as attributes, comments, or relationships are not recorded in the audit log.

Tags Pane

Maintenance Account, Administrative Access, and Primary Contributor Access accounts can add and remove tags in the Tags pane on the object details page. Read Only Access accounts can view tags but not remove them.

See [Bulk Actions Add/Remove Tags](#) for information on adding/removing tags from a group of system objects.

Adding an Existing Tag to an Object

1. Locate the Tags pane on the object details page.
2. Click the **Select an existing tag** field.
3. Select the tag you want to add from the dropdown list.



You can narrow the dropdown list options by entering all or part of the tag name. As you type, the dropdown list displays matches for your entry.

Adding a New Tag to an Object

1. Locate the Tags pane on the object details page.
2. Click the **Create a new tag** option.
3. Type the new tag's name in the **Tag name** field.
4. Press **Enter** to save the new tag and add it to the system object.

Deleting a Tag from an Object

1. Locate the Tags pane on the object details page.
2. Select the **X** next to the tag name.

Description Pane

The Description Pane section of the object details page allows you to add a description for the system object. Object descriptions can include text, tables, and images.

Tips and Tricks

- **Image alignment** - Images in an object's description are displayed in the PDF report for the object as left aligned regardless of the alignment you select in the Description pane.
- **Image captions** - Add your image captions after you select your image alignment. If you change alignment after adding a caption, the caption is removed and must be added again.
- **Image text alternatives** - If you add an image text alternative to an image, it is available for use by screen reading tools but is only displayed on screen if the image fails to load. It is not displayed when you hover on the image.
- **Add a line above or below** - When you click an image, the arrow icons located on the bottom left and top right corners allow you to insert a line above (top right arrow) or below (bottom left arrow) the image.
- **Resize an image** - The resize image option allows you to adjust your image to 25%, 50%, or 75% of the size of the Description field. Or, you can return your image to its original size.
- **Paste rows into an existing table** - To paste rows into an existing table, insert a blank row in the table, click in the first cell of the blank row, and then paste the additional rows.
- **Resize the Description field** - Click and drag the right corner to resize the Description field.

Updating the Description of an Object

1. Locate the Description pane on the object details page.
2. Click the **Edit** option to add/update the object descriptions text, tables, or images.
3. Make the required changes and click the **Save** button.

Spearphish Details Pane

You can update spearphish file details as well as add or delete recipients from the Spearphish Details pane in a Spearphish event's object details page.

Adding a Recipient

1. Locate the Spearphish Details pane on the object details page.
2. Click the Add Recipients option.
The Add Recipients window is displayed.
3. Populate the following fields:
 - **Recipient type** - This field defaults to a value of To. Use this field to specify whether the email was sent directly to the recipient (To) or the recipient received it as a carbon copy (CC) or blind carbon copy (BCC).
 - **Email address** - Enter the email address that received the spearphish file.
 - **Link all emails as related indicators** - This field defaults to checked. Leave this box checked to add a related indicator record to the system object for each email address.
3. To add another recipient, click the + button and repeat step 3.
3. To save your recipient additions and return to the Spearphish Details pane, click the Add Recipients button.

Deleting a Recipient

1. Locate the Spearphish Details pane on the object details page.
2. Click the checkbox(es) next to the recipient(s) you want to delete.
3. Click the Delete option.
The Are You Sure? window prompts you to confirm your action.
4. Click the Delete Recipients button.

Editing a Spearphish File

1. Locate the Spearphish Details pane on the object details page.
2. Click the Edit button.
2. Enter your changes in the Email Content field.
2. Click the Save button.

Relationships

About 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

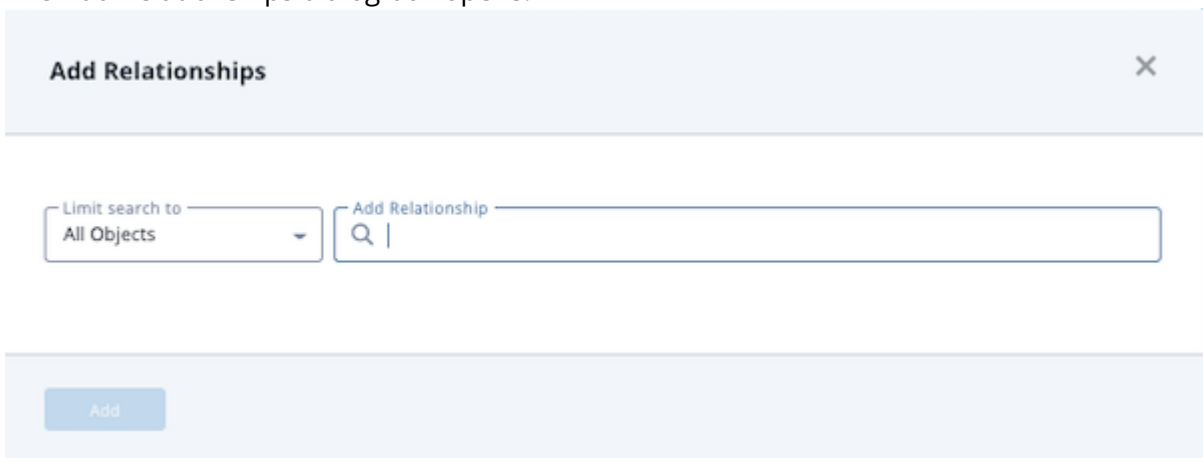
1. Locate the desired system object type pane on the object details page.



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.



3. Use one of the following methods to add an object to the Add Relationships field:
 - For existing objects, enter the object name and select the match from the down list.



Repeat this step to add multiple objects.

- To create a new object, enter the new object name. Then, click the **Create** link to add the new object to Threat Library. If you limited your search to a specific object type, you are linked to the corresponding form. For example, if you limited your search to Adversaries, the Create link opens the Add An Adversary form. If you left the **Limit search to** field set to All Objects, you can select the object type you want to create from a drop-down list.

4. Click **Add**.

Unlinking a System Object

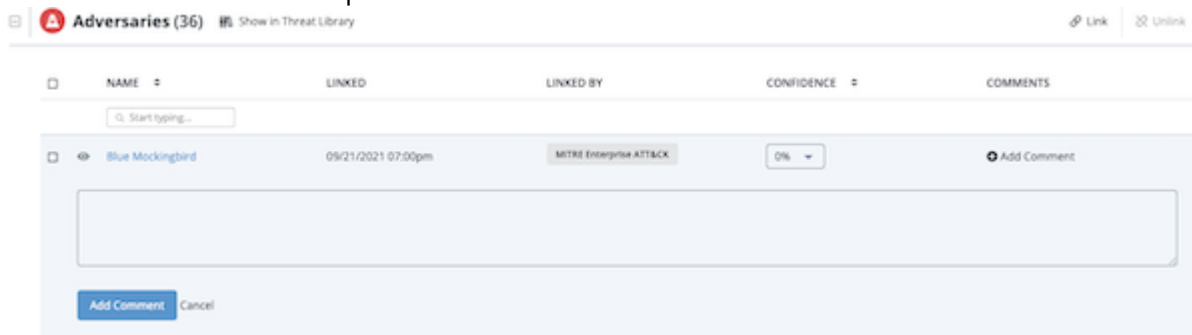
1. Locate the Related <System Object> pane on the object's details page.
2. Select the checkbox(es) next to the system objects to unlink.
3. Select the  Unlink icon.

Additional Related Object Actions

Certain system object types will offer you additional actions after relating the objects to another object.

Adding a comment to a related adversary

1. Locate the Adversaries pane on the object details page.
2. Select **Add a Comment**.
The Comments text field opens.



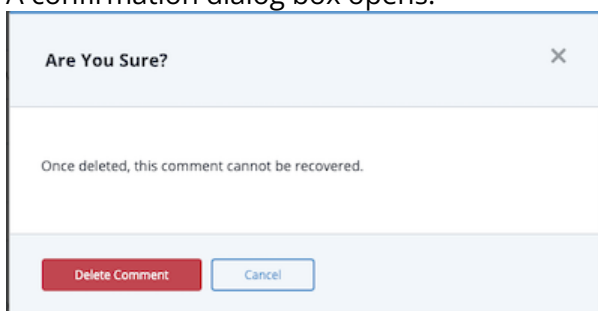
3. Enter a comment.
4. Click **Add Comment**.

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 in the Confidence field to select the desired confidence level.



NAME	LINKED	LINKED BY	CONFIDENCE	COMMENTS
Magic Hound	09/21/2021 07:00pm	MITRE Enterprise ATTACK	0%	Add Comment



The confidence level can be set to 0, 25, 50, 75, and 100.

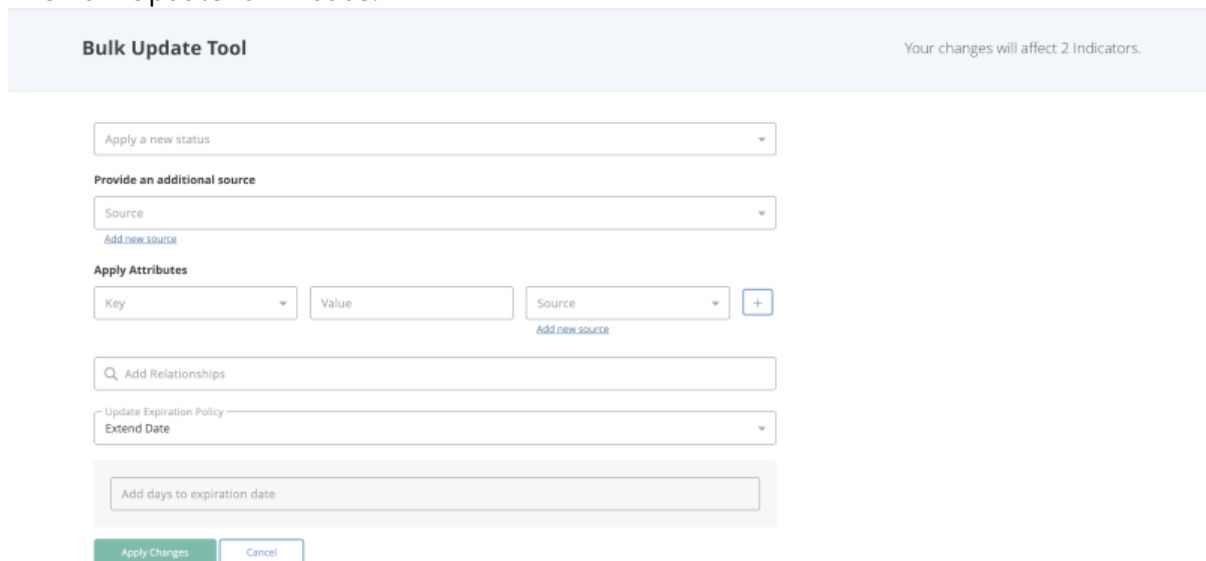
The displayed confidence level will be modified to reflect your selection.

Related Indicators - Bulk Actions

You can perform bulk updates to linked indicators listed in the Indicators pane of an object.

1. Locate the Indicators pane on the object details page.
2. Select the checkbox(es) next to the indicator(s) to update.
3. Select the  Bulk Update icon.

The Bulk Update form loads.



Bulk Update Tool Your changes will affect 2 Indicators.

Apply a new status

Provide an additional source

Source

Add new source

Apply Attributes

Key Value Source

Add new source

Add Relationships

Update Expiration Policy

Extend Date

Add days to expiration date

Apply Changes Cancel

4. Select the desired changes and click **Apply Changes**.

Related Investigations - Request Access

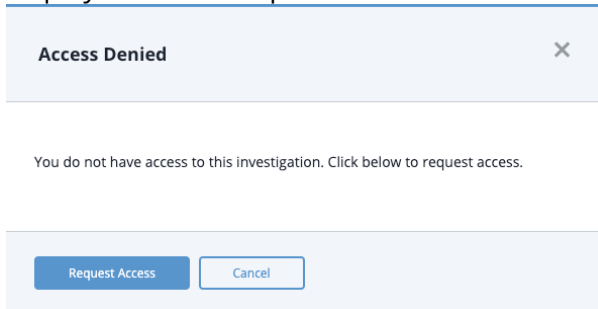
If you do not have Owner, Editor, or Viewer permissions to an investigation related to a system object, you cannot access it unless the investigation owner assigns you one of these permission levels.

1. Locate the Related Investigations pane on the object details page.

2. Click the investigation name.

If you have permission to access the Investigation, this link takes you to the investigation's evidence board.

If you do not have permission to access the investigation, the Access Denied window is displayed. Go to step 3.



3. From the Access Denied window, click the **Request Access** button.
The investigation owner receives a Notification Center alert indicating you have requested access to the investigation.

Comments Pane

The Comments pane allows users to record comments about the system object for other users to see.

Adding Comments to an Object



Users can also click on the **Actions** menu and select the **Comment** option.

1. Click on the expand icon  to expand the Comments pane.
2. Click on the **Add** link located at the top-right of the pane.

The new comment text box opens.



The screenshot shows the top of the Comments pane. On the left, there is a toggle switch and the text 'Comments (0)'. On the right, there is an 'Add' link. Below this, a large text input box is open. At the bottom of the input box, there 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 pane with one comment. The comment header includes a profile picture, the email 'threatq@threatq.com', and the time 'a few seconds ago'. To the right of the header is a 'Hide' link. Below the header is a text input box containing the text 'DDoS-Related Attack possible'. At the bottom of the input box, there are two buttons: 'Save Changes' and 'Cancel'.

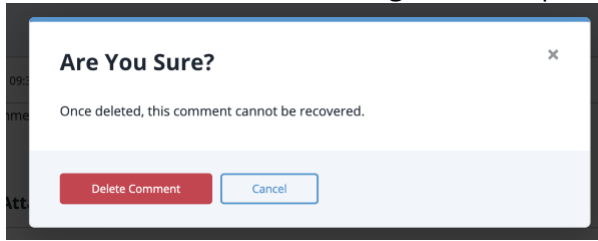
3. Edit the comment.
4. Click on the **Save Changes** button.

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 (Adversary , Files , Events , Indicator , and Signatures) that indicates when a relation of the object has been changed.

Is there another raw audit log within the system where events are logged?

No, there are no other raw audit logs where events are logged.

Is there an option in the User Interface to enable all activities to be shown in the Audit Log?

There is no option in the User Interface to limit or expand the audit log. All entries are pulled for an object when the Audit Log panel is opened. The audit log displays changes to the individual fields of an object; object comments, sources, attributes, and tags; as well as to object links, object link comments, and object link attributes. Additionally, any changes to the score of an Indicator are included.

User Management

About User Management

ThreatQ uses role-based access control to manage user accounts. The system provides several [user roles](#), each containing a set of permissions for accessing system functionality. You create user accounts, and assign them to a user role. The user role determines each account's set of permissions. After you create a user account, you can modify its user role group, display name, and email address.

Managing User Accounts

While all users can update their own individual accounts, only users with Maintenance Account and Administrative Access user roles have permission to access the User Management functionality. You must be logged in as one of these roles in order to create new user accounts.



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

Accessing Your User Account

1. Click on your avatar icon, located to the top-right of the platform, and select **My Account**. The Edit User screen allows you to review and update your [User Account Properties](#).

Accessing Other User Accounts



Only users with Maintenance and Administrative accounts can add, edit, and delete other user accounts.

1. Click the **Settings** icon  and select **User Management**. The User Management screen displays a list of user accounts.
2. You can filter and/or sort the user accounts displayed by:
 - Display Name
 - Status
 - Username
 - Email
 - Group
 - 2-Step Verification
3. If you are logged in with a Maintenance or Administrative account, you can also click a display name to access the corresponding [User Account Properties](#).

User Account Properties

FIELD	DESCRIPTION
Name	Update the user's name.
Title	Update the user's job title.

Email	You can update the user's email address.
Password	You can click on the Change Password link to update the user's password.
API Credentials	You can view the user's API credentials, a unique Client ID, which will allow him/her to connect with ThreatQ's API.
Session Timeout	You can update or disable the user's session timeouts.
Screen Display	If you change your display theme, you will see the update immediately. If you change another user's display theme, the new mode updates the display the next time they log in.
User Avatar	You can update the user avatar .
2-Step Verification	Optional. The toggle switch in this section allows you to enable/disable 2-step verification .
Client CERT Authentication Enabled	If SSL Client Certificate Authentication is enabled, this section displays the user's certificate fingerprint or allows you to add/update a certificate fingerprint.
Activity Log	You can click on the Activity log tab to view the following information: • The last date and time the user logged in. • The IP Address where the user logged in. • Whether the login was successful or not.

Adding a User



Only users with Maintenance and Administrative accounts can add user accounts.

1. From the main menu, choose the **Settings icon**  > **User Management**.
2. Click **Add User**.
The Add User window is displayed.
3. Populate the following fields:
 - **Display Name** - *Required*. Enter the user's name.
 - **Title** - Optional. Enter the user's title.
 - **Group** - *Required*. Select the level of access for the user from the **Group** drop-down menu:

- Maintenance Account
- Administrative Access
- Primary Contributor Access
- Read Only Access



See the [User Roles](#) topic for more detail on these access levels.

- **Username** - *Required*. Enter the user's login ID.
 - **Email** - Optional. Enter the user's email address.
 - **Password** - *Required*. Enter the user's password.
 - **Retype Password** - *Required*. Re-enter the user's password.
4. Click the **Add User** button.
The System User tab displays the new user. See the [Editing a User](#) topic for information on further customizing the user profile.

Editing a User



Only users with Maintenance and Administrative accounts can edit another user's account. You cannot edit user details for SAML nor LDAP users from the User Management page.

1. Click the **Settings** icon  and select **User Management**.



To edit your own account, click your avatar icon and select My Account. Proceed to step 3 below.

2. Click the user's display name.
The User Profile page loads.

Edit User

User Profile
Account Activity

Account Status

☒ Active
☐ Disabled

Profile Information

Display Name
threatq@threatq.com

Title

Group
Maintenance Account

Username
threatq@threatq.com

Email

Change Password

[Change Password](#)

API Credentials - Client ID

f5441a3246e28cfb3348115520e12c65

Session Timeout

Minutes
60

Minutes of inactivity before being logged out automatically.

☐ Disable Timeout

Screen Display

Split Mode

Light Mode

Dark Mode

User Avatar:

Drop image here or browse

Th

Enable 2-Step Verification

Disabled
☒ Enabled

Each time you log into your account, you'll be required to enter both your password and a verification code.

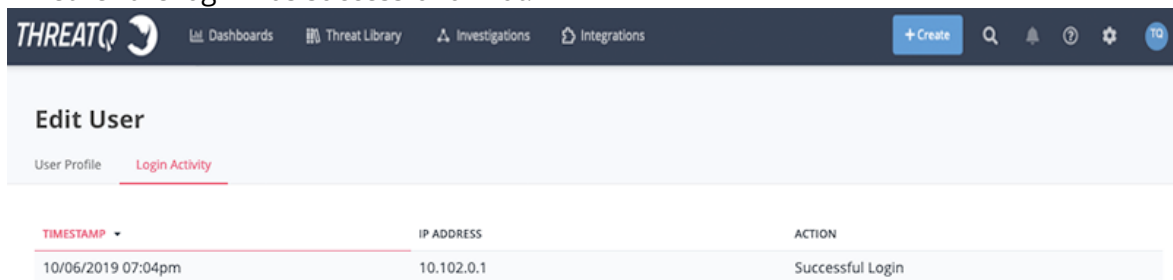
Save

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

FIELD	DESCRIPTION
Name	Update the user's name.
Title	Update the user's job title.
Email	You can update the user's email address.

FIELD	DESCRIPTION
Password	You can click on the Change Password link to update the user's password.
API Credentials	You can view the user's API credentials, a unique Client ID, which will allow him/her to connect with ThreatQ's API.
Session Timeout	You can update or disable the user's session timeouts.
Screen Display	Allows you to update a user's display theme. If you change another user's display the new mode updates the display the next time they log in.
User Avatar	You can update the user avatar .
2-Step Verification	Optional. The toggle switch in this section allows you to enable/disable 2-step verification .
Client CERT Authentication Enabled	If SSL Client Certificate Authentication is enabled, this section displays the user's certificate fingerprint or allows you to add/update a certificate fingerprint.

4. You can also click on the **Login Activity** tab to view:
 - The last date and time the user logged in.
 - The IP Address where the user logged in.
 - Whether the login was successful or not.



TIMESTAMP	IP ADDRESS	ACTION
10/06/2019 07:04pm	10.102.0.1	Successful Login

5. After you enter your changes, click the **Save** button.

Resetting User Password from the Command Line

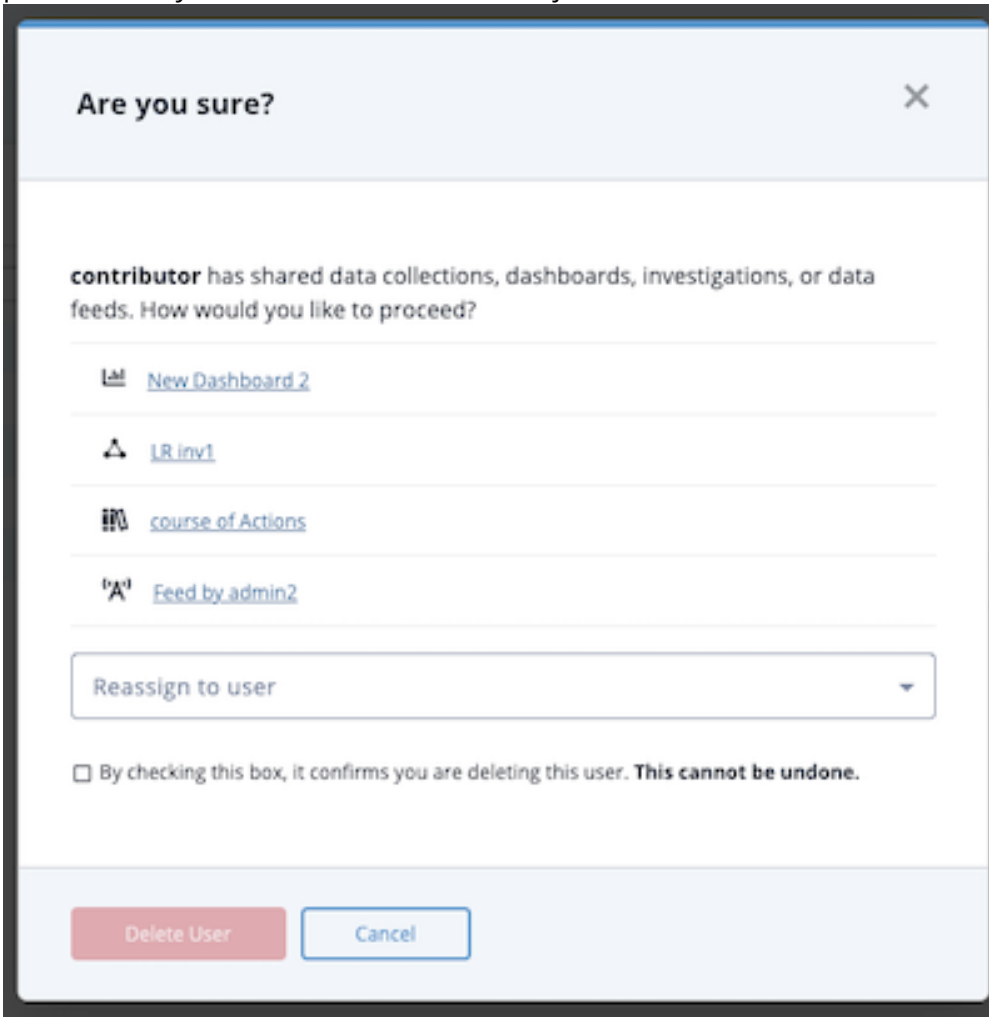
If you have root access to your ThreatQ installation, you can reset any user's password from the command line. See the [Resetting User Passwords from the Command Line](#) section in the Commands topic.

Deleting a User

 Deleting a user cannot be undone.

1. From the main menu, choose the **Settings icon > User Management**.
2. In the System Users tab, click the check box next to each user you want to delete.
3. Click the trashcan button.

If the user has any shared data collections, data feeds, dashboards, or investigations, the **Are you sure?** window notifies you and lists them. You must reassign owner permissions or delete them. These objects are linked so that, if you have the corresponding viewer or editor permissions, you can click and view the object in a new tab.



4. Click the **Reassign to user** field and do one of the following:

- **Reassign Ownership** - Select the new owner of the data collections, data feeds, dashboards, and/or investigations.
 - **Delete** - Select the **Do not reassign. Delete these items.** option to delete all of the user's data collections, data feeds, dashboards, and/or investigations.
5. Check the confirmation checkbox and click the **Delete User** button.

Updating a User Avatar

User avatars provide a personalized look to your ThreatQ dashboard. ThreatQ supports the use of all standard image types for avatars and a maximum image size of 260 x 260 pixels.

1. Click the avatar icon and select **My Account**.
The Edit User page is displayed.
2. From the Use Avatar section, you can:
 - Click the browse link and select the icon to upload.
 - Click and drag the new icon onto the page.
3. Click the **Save** button.

User Roles

The following details the user roles and their base-level permissions. A user account's access to data collections and dashboards can be further customized by the [Sharing](#) permissions assigned to it.

USER ROLE	PERMISSION
Maintenance Account	Members have access to the entire ThreatQ user interface and can edit all data. Important Notes: • Each ThreatQ instance must have at least one Maintenance Account. • Local Maintenance Accounts (manually created within ThreatQ) cannot be migrated to SAML authentication groups
Administrative Access	Members have access to the entire ThreatQ user interface and can edit all data.
Primary Contributor Access	Members can: • Edit their own user info • Manually create system objects • Create and manage ThreatQ Investigations • Access Whitelist Management (Data Controls) • Perform a basic search • Access the Threat Library, object metadata, export search results, and manage Data Collections • Create custom dashboards and add shared dashboards to their user view.
Read Only Access	Members can: • Access the Threat Library, object metadata, export search results • Add shared dashboards to their user view • Load saved Data Collections  Members cannot edit any data.

2 Step Verification

Users can configure a second layer of security for their user accounts.



Transcript: [TEXT](#)

Footage from ThreatQ Version 4.55.0

Reference

- [2-Step Verification](#)
- [About Accessing the Platform](#)
- [Managing User Accounts](#)

LDAP Authentication

About 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 [About LDAP Authentication](#) topic before configuring your LDAP settings.

To Access the LDAP tab:

1. From the main menu, select the Settings  icon > User Management.
2. Click the **LDAP** tab.

The LDAP tab opens with the Anonymous Bind LDAP Settings form loaded by default.

User Management

System Users **LDAP** SAML CAC / PIV SSL

LDAP

Disabled ☒ Enabled

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

Anonymous Bind LDAP Settings

Authenticated Bind LDAP Settings

You can edit and manage your anonymous bind LDAP settings below. For more information and guidance about these settings, please visit the [Help Center](#). * Indicates required fields.

Primary Server Settings

Server Address

Port #

LDAP Domain

LDAP Group Domain

Optional: Provide this when LDAP "users" and "groups" have different domains.

Append Domain to Username?

Map Your Permission Levels to LDAP

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

Maintenance Account

This should be the CN value of your LDAP Query.

Administrative Access

Primary Contributor Access

Read Only Access

Save

Required Information for Creating LDAP Authentication

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

Anonymous Bind

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

Authenticated Bind

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

Switching LDAP Connections

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



Example: You are using the Anonymous Bind LDAP option. You switch to the Authenticated Bind LDAP Settings tab and click Save. ThreatQ will now use these settings. If you switch back to the Anonymous Bind LDAP Settings tab and click Save again, ThreatQ will start using the Anonymous Bind LDAP settings again.

Anonymous Bind



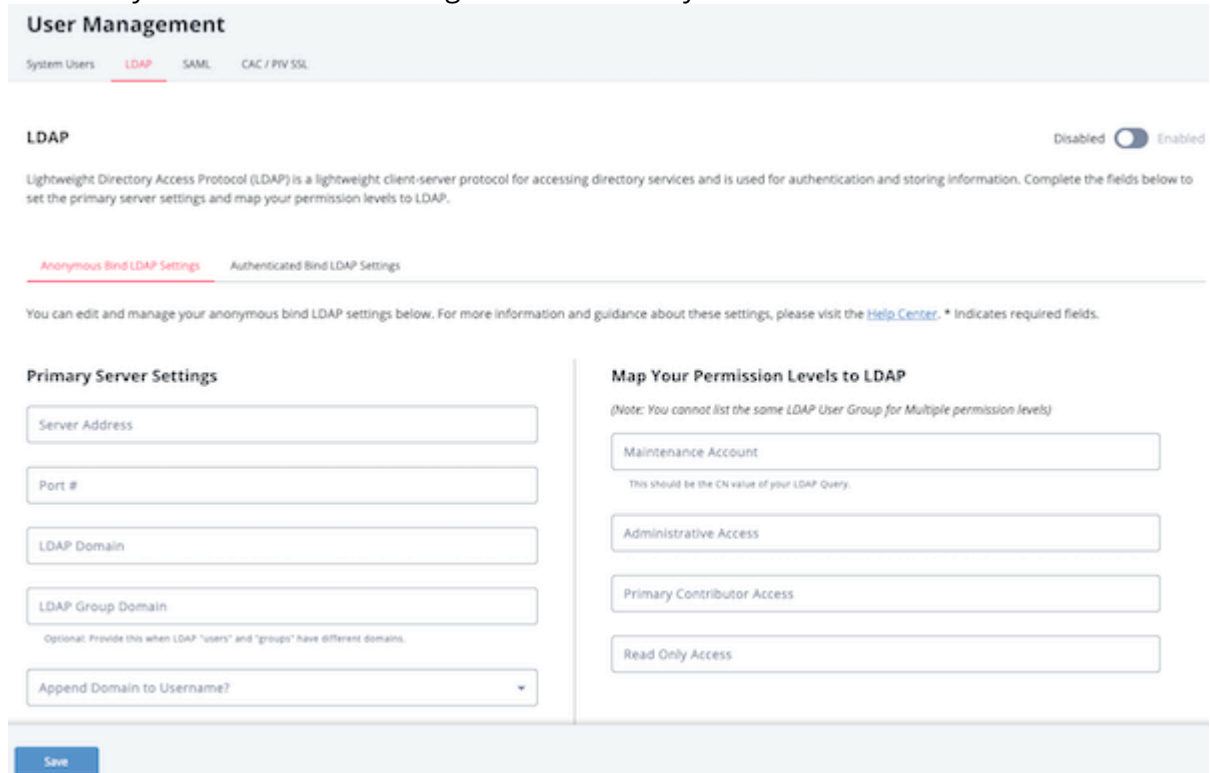
Only users with an Administrative or Maintenance account can access LDAP settings.



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

1. Navigate to Settings  > User Management.
2. Click on the **LDAP** option.

The Anonymous Bind LDAP Settings form will load by default.



3. Populate the fields in the **Primary Server Settings** section:

FIELD	DESCRIPTION
Server Address	Enter the name of the server where LDAP is hosted. Example: ldap://[servername]
Port #	389 for LDAP 636 for LDAPS If LDAPS is used, the Port # will default to 636.

FIELD	DESCRIPTION
LDAP Domain	Enter the domain for which LDAP is configured to authenticate. Example: threatq.com
LDAP Group Domain	
Append Domain to Username?	Choose from the following options: ○ Yes for most Active Directory servers ○ No for most Open LDAP servers
Filter Field Name	This field is specific to your LDAP directory configuration. AD Example: memberuid OpenLDAP Example: uid
Group Field Name	This field is specific to your LDAP directory configuration. AD Example: memberof OpenLDAP Example: cn
Use RDN?	Choose from the following options: ○ Yes to use Relative Distinguished Names. When you select this option, the Organization Unit (OU) and User Lookup Name fields are displayed. ○ No to use full Distinguished Names
Organizational Unit (OU)	This field is specific to your LDAP directory configuration. Your LDAP administrator should provide the correct value for this field.
User Lookup Name	This field is specific to your LDAP directory configuration. AD Example: memberUid OpenLDAP Example: uid

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



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

FIELD	EXAMPLE
Maintenance Account	OpenLDAP Example: ldapSuper AD Example: CN=tq-maintenance,CN=Builtin,DC=yourdomain,DC=com
Administrative Access	OpenLDAP Example: administrator AD Example: CN=linux-admins,CN=Builtin,DC=yourdomain,DC=com
Primary Contributor Access	OpenLDAP Example: ldapAnalyst AD Example: CN=primary-contributor,CN=Builtin,DC=yourdomain,DC=com
Read Only Access	OpenLDAP Example: ldapObserver AD Example: CN=read-onlyCN=Builtin,DC=yourdomain,DC=com

- Click **Save**.
- 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:

- Enter your LDAP settings in the ThreatQ user interface. See the Anonymous Bind steps above for more details.
- Access the ThreatQ appliance command line as root and edit and navigate to the following directory: /etc/openldap/.
- Use vi to edit ldap.conf and update/confirm that your settings are as follows:

```
#
# LDAP Defaults
#
```

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

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

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

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

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



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



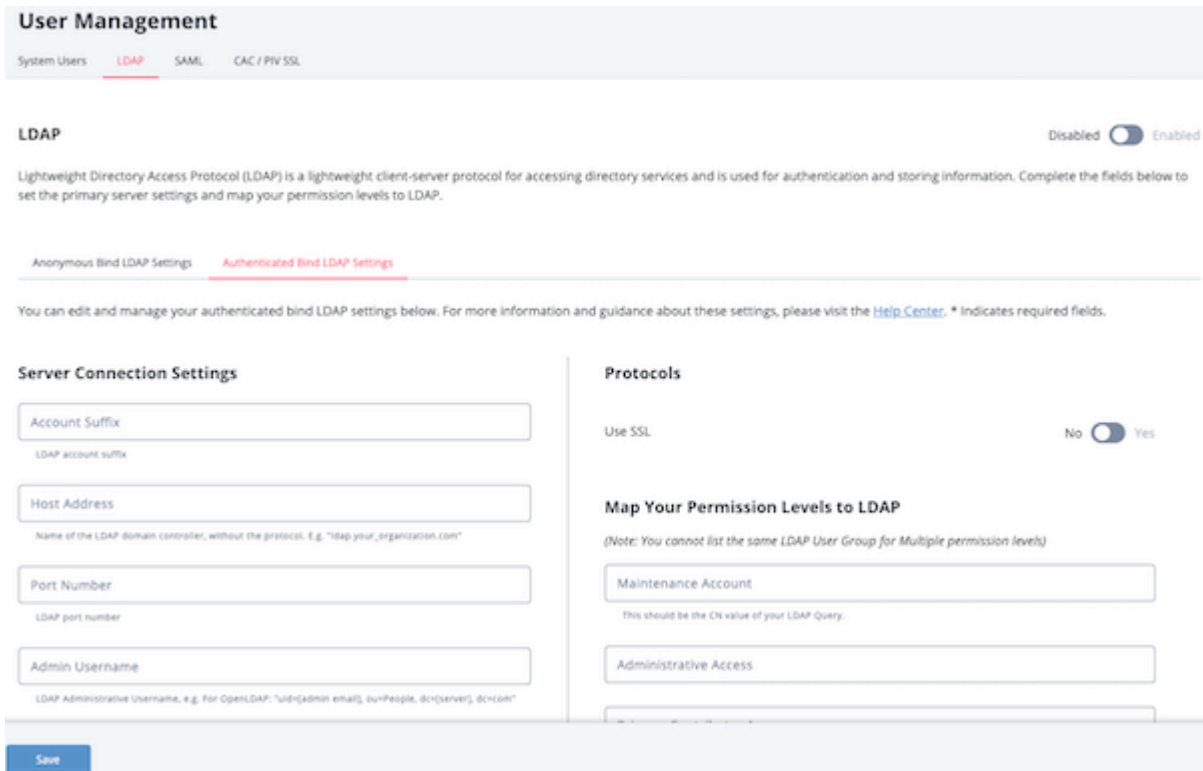
If your LDAP fails to enable or fails to function properly, validate your inputs. If the configuration continues to fail, please contact ThreatQ Support.

Authenticated Bind

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

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

1. Navigate to Settings  > User Management.
2. Click on the **LDAP** option and select the **Authenticated Bind LDAP Settings** tab.



User Management

System Users **LDAP** SAML CAC / PIV SSL

LDAP Disabled ☐ Enabled

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

Anonymous Bind LDAP Settings **Authenticated Bind LDAP Settings**

You can edit and manage your authenticated bind LDAP settings below. For more information and guidance about these settings, please visit the [Help Center](#). * Indicates required fields.

Server Connection Settings

Account Suffix
LDAP account suffix

Host Address
Name of the LDAP domain controller, without the protocol. E.g. "ldap.your_organization.com"

Port Number
LDAP port number

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

Protocols

Use SSL No ☐ Yes

Map Your Permission Levels to LDAP
(Note: You cannot list the same LDAP User Group for Multiple permission levels)

Maintenance Account
This should be the CN value of your LDAP Query.

Administrative Access

Save

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

FIELD	DESCRIPTION
Account Suffix	The LDAP account suffix.
Host Address	Name of the LDAP domain controller without the protocol. Example: tqldap.threatq.com

FIELD	DESCRIPTION
Port Number	The LDAP port; either 636 or 389 . Only standard ports for secured and unsecured connections are supported. Use port 636 if using SSL to create a secured connection.
Admin Username	The LDAP administrative username.
Admin Password	The LDAP administrative password.

- 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. Example: DC=[server], DC="com"
DN Field Name	The field used to retrieve the DN or users and groups. This field should be DN for both OpenLDAP and Active Directory.
User Search Filter	The field to search for users. For OpenLDAP : objectClass=posixAccount For Active Directory : objectClass=user
Group Search Filter	The field to search for grpups. For OpenLDAP : objectClass=posixGroup For Active Directory : objectClass=group
Primary Group Name	The primary group name.
Group Member Field Name	This field is used to search for groups that a user belongs to. For OpenLDAP : cn For Active Directory : memberof

FIELD	DESCRIPTION
User ID Key Field Name	Field used to search for users based on email. For OpenLDAP : uid For Active Directory : sAMAccountName
User Group Member Key Field Name	Field used to search for groups that user belongs to. For OpenLDAP : memberUid For Active Directory : uid

- 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.

- Complete the **MAP your Permission Levels to LDAP** section:

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

FIELD	DESCRIPTION
Maintenance Account	The LDAP account the ThreatQ Maintenance group will map to for permissions. Open LDAP Example: ldapSuper AD Example: CN=tq-maintenance,CN=Builtin,DC=yourdomain,DC=com
Administrative Access	The LDAP account the ThreatQ Administrative group will map to for permissions. Open LDAP Example: administrator AD Example: CN=linux-admins,CN=Builtin,DC=yourdomain,DC=com
Primary Contributor Access	The LDAP account the ThreatQ Primary Contributor group will map to for permissions. Open LDAP Example: ldapAnalyst AD Example: CN=linux-admins,CN=Builtin,DC=yourdomain,DC=com
Read-Only Access	The LDAP account the ThreatQ Read-Only group will map to for permissions.

FIELD
DESCRIPTION

Open LDAP Example: ldapObserver

AD Example: CN=read-onlyCN=Builtin,DC=yourdomain,DC=com

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



Green indicates the feature is active.

SAML Authentication

About 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 [About 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

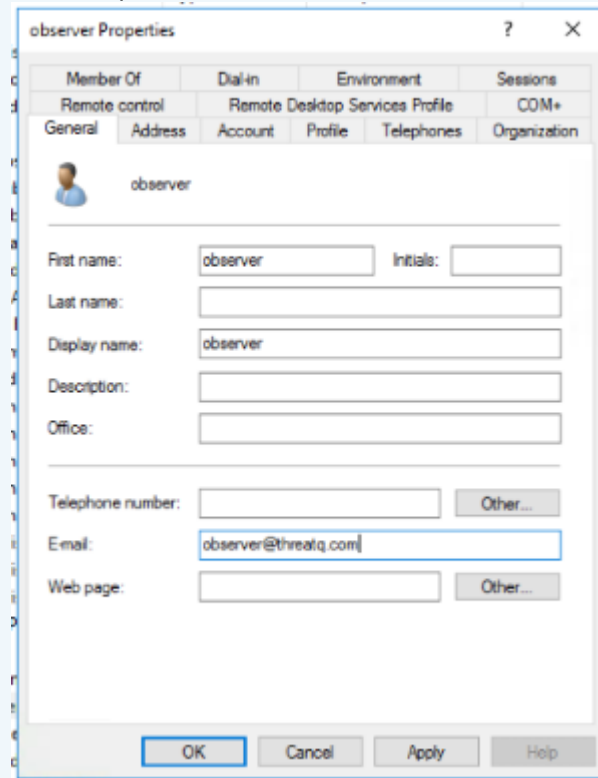


ThreatQuotient strongly recommends that you perform a full backup before changing your authentication method.



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.



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

1. From the main menu, select Settings  > User Management.
2. From the User Management page, click the **SAML** tab.

The SAML configuration page opens.

System Users
LDAP
SAML
CAC / PIV SSL

User Management

SAML

Disabled
☒
Enabled

Security Assertion Markup Language (SAML) is a single sign-on standard used for logging users into applications based on their sessions in another context. Complete the fields below to set the primary server settings and map your permission levels to SAML.

Connection Information - Identity Provider

Provide either an XML configuration file or a configuration URL below. If you provide a configuration URL, the XML configuration file will be downloaded automatically.

Provide IDP Metadata File



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

Provide IDP Metadata URL

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

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.

ThreatQ User Guide
Version 5.20.0

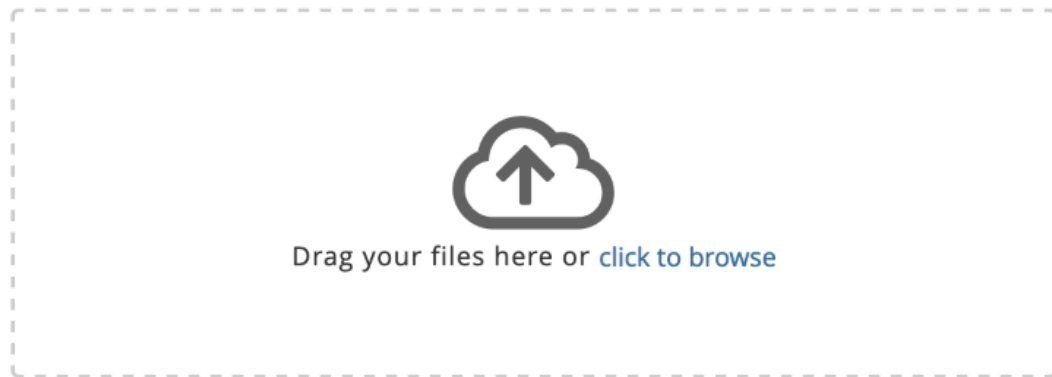
514

- Entering your IdP metadata file's URL in the **Provide IdP Metadata URL** field.

Connection Information - Identity Provider

Provide either an XML configuration file or a configuration URL below. When you provide one method, the other method will autopopulate.

Provide IDP Metadata File



Provide IDP Metadata URL

Whichever method you choose to use will result in the auto-completion of the other field.

Example: Uploading a metadata file will result in the IdP Metadata URL being populated with data parsed from the file.

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

Connection Information - Service Provider Information

In order for your IDP to connect to this platform, you must provide either this Service Provider's Connection URL or upload the Service Provider Metadata File (which can be downloaded below) in your IDP.

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

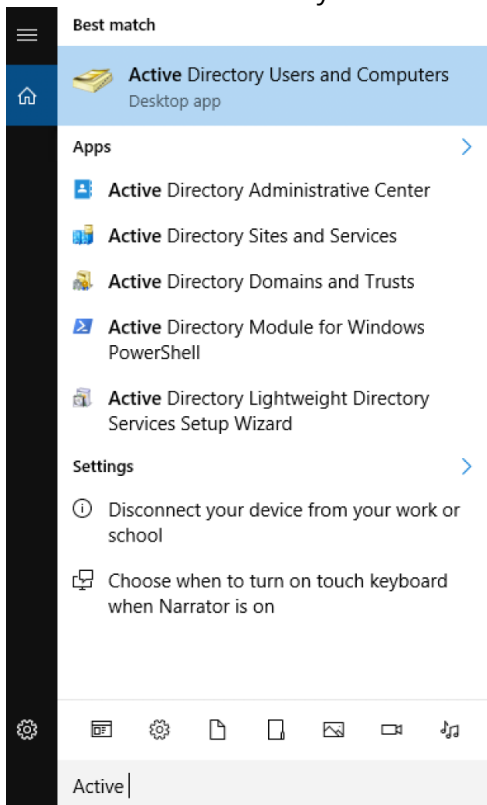
Mapping Notes:

- 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.
 - SAML accounts imported with the same user name and email as a local account will be converted.
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.

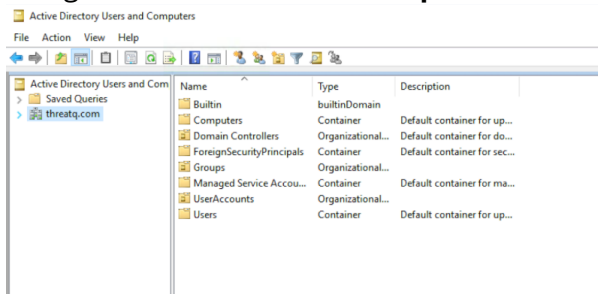
Setting Up LDAP Users/Groups for SAML

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

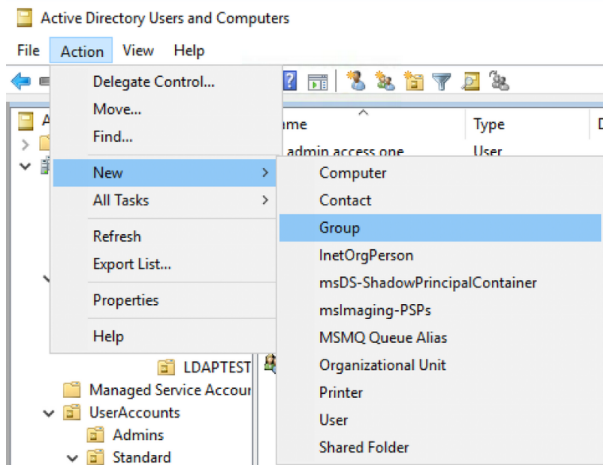
1. Log into the Windows Server.
2. Start the Active Directory Users and Computers application from the Start Menu.



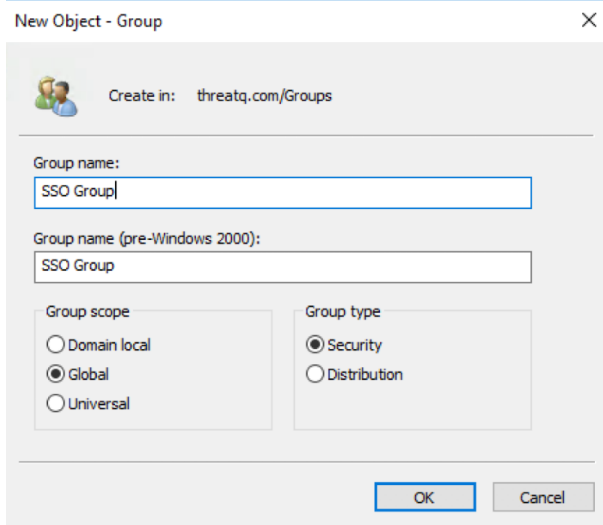
3. Navigate to and select the **Groups** folder under your LDAP domain.



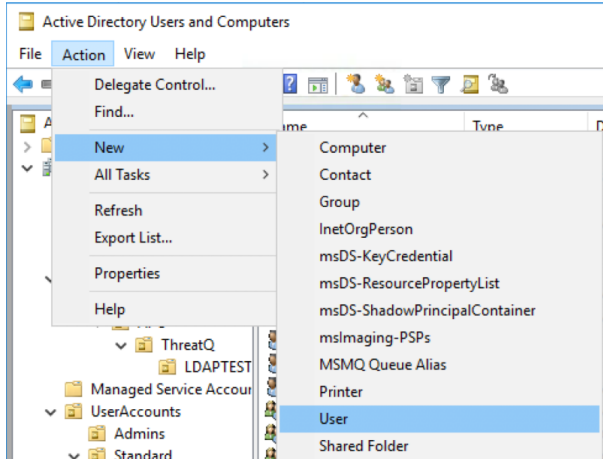
4. Click on **Actions > New > Group**.



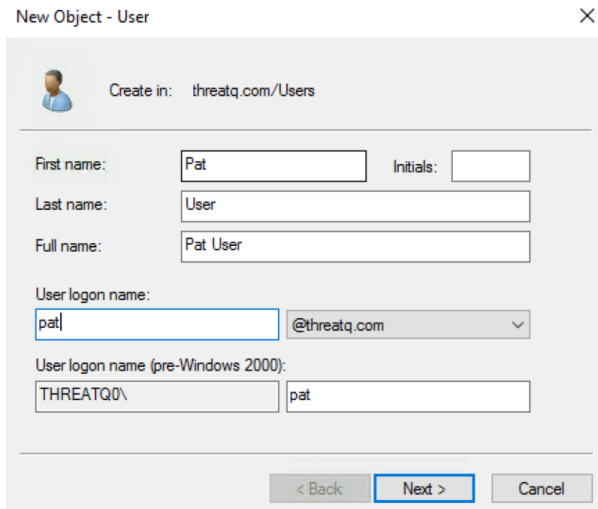
5. Enter in the **Group name** and click on **OK**.



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



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



New Object - User

Create in: threatq.com/Users

First name: Pat Initials:

Last name: User

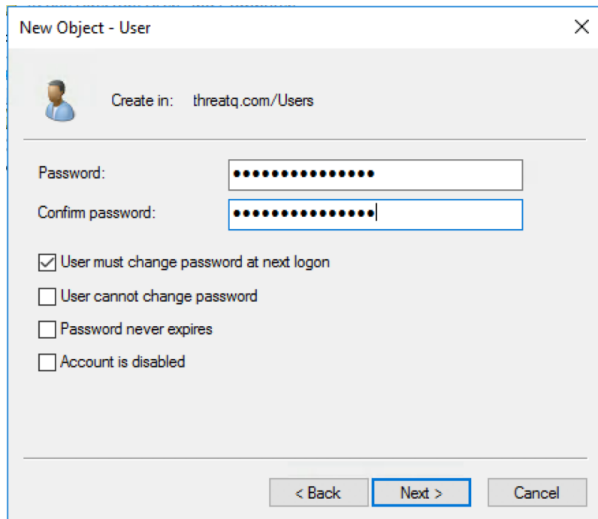
Full name: Pat User

User logon name: pat @threatq.com

User logon name (pre-Windows 2000): THREATQ0\ pat

< Back Next > Cancel

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



New Object - User

Create in: threatq.com/Users

Password:

Confirm password:

☒ User must change password at next logon

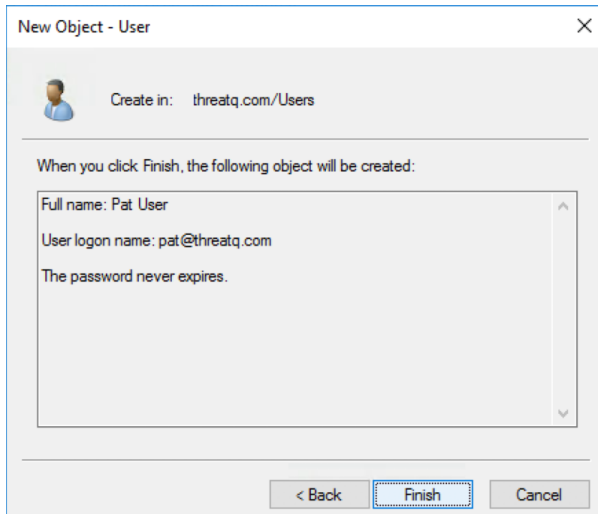
☐ User cannot change password

☐ Password never expires

☐ Account is disabled

< Back Next > Cancel

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



New Object - User

Create in: threatq.com/Users

When you click Finish, the following object will be created:

Full name: Pat User

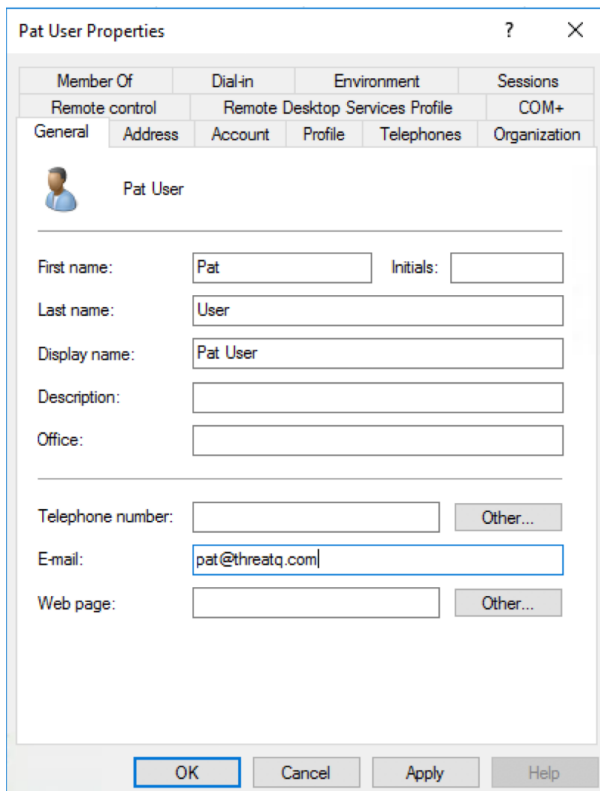
User logon name: pat@threatq.com

The password never expires.

< Back Finish Cancel

- 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

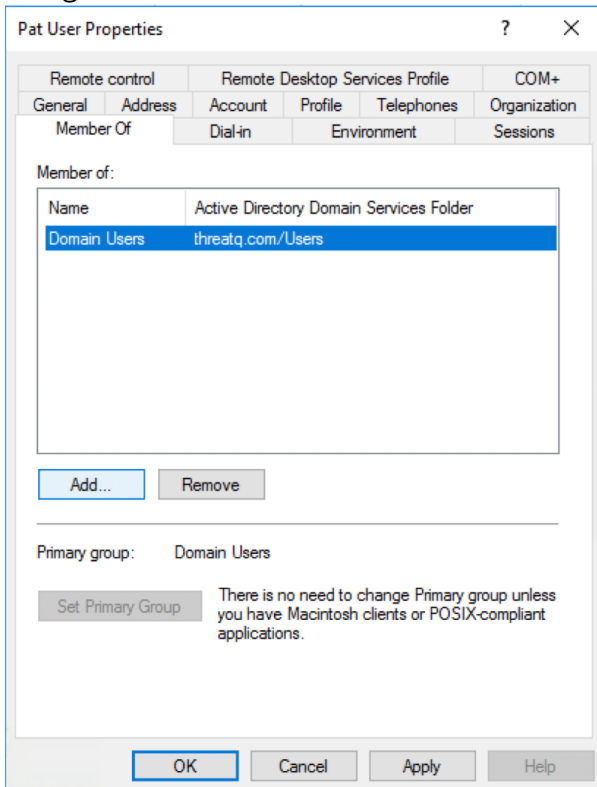
Web page: Other...

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	Profile
	Environment	Telephones
		Organization
		Sessions

Member of:

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

Add... Remove

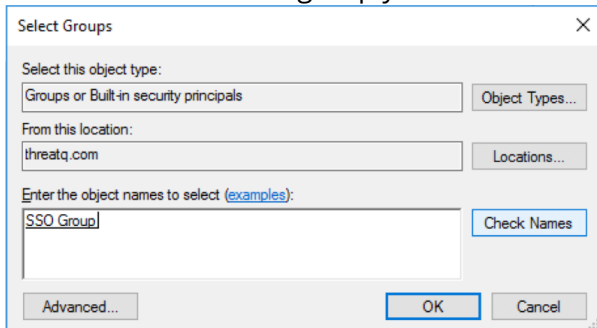
Primary group: Domain Users

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

Object Types...

From this location:

threatq.com

Locations...

Enter the object names to select (examples):

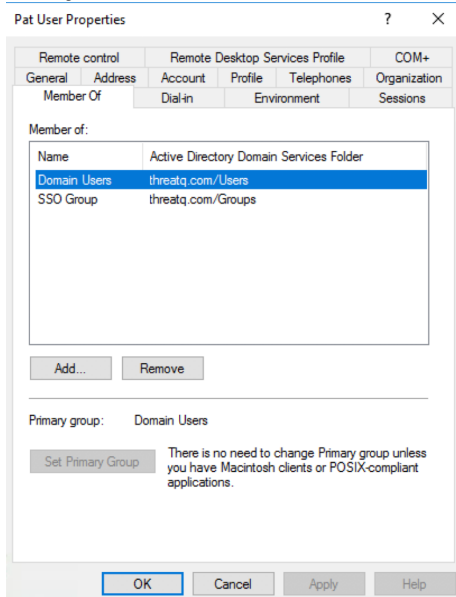
SSO Group

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 ? X

Remote control	Remote Desktop Services Profile	COM+
General	Address	Account
Member Of	Profile	Telephones
	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.

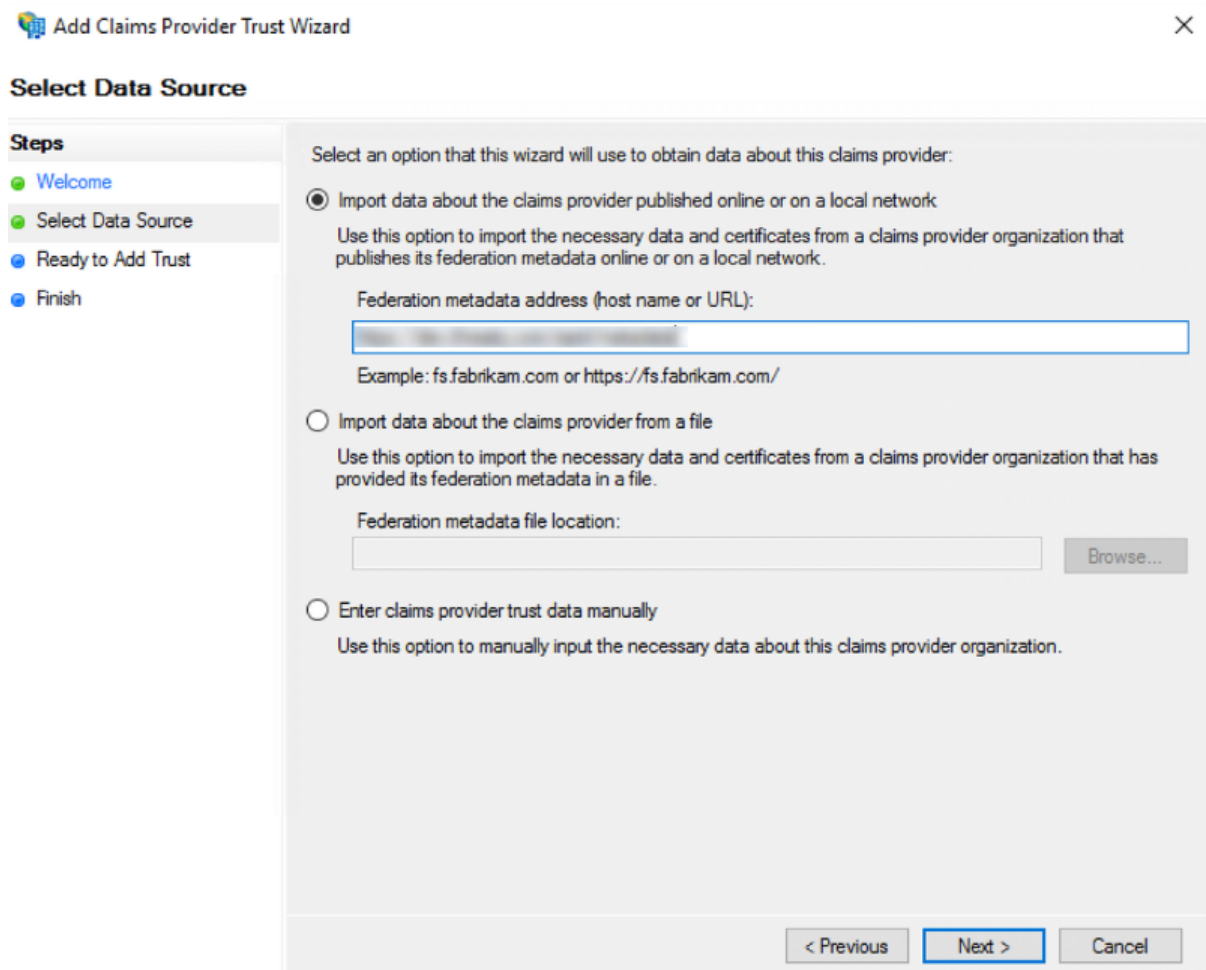
ADFS 2016

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.



Add Claims Provider Trust Wizard

Select Data Source

Steps

- Welcome
- Select Data Source
- Ready to Add Trust
- Finish

Select an option that this wizard will use to obtain data about this claims provider:

☒ Import data about the claims provider published online or on a local network

Use this option to import the necessary data and certificates from a claims provider organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

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

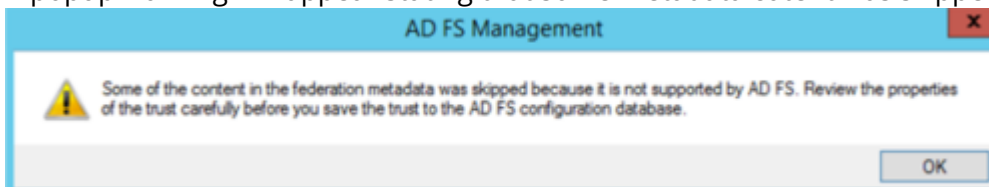
Use this option to manually input the necessary data about this claims provider organization.

< Previous Next > Cancel

6. Confirm that the first radio option, **Import data about the claims provider published online...**, is selected.
7. Paste the **Platform Connection URL** located on the ThreatQ SAML page, step 4 on the [Configuring SAML](#) topic, into the Federation Metadata Address field in the following format:
`https://<your IdP hostname>/FederationMetadata/2007-06/FederationMetadata.xml`

8. Click **Next**.

A popup warning will appear stating that some metadata 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	NOTES
E-Mail-Addresses	email	
Email-Addresses	uid	Email-Addresses is the recommended value. However, you can use SAM-Account-Name as an alternative.

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

23. Add the following row in the LDAP Mapping Attributes table:

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

24. Click on **OK** to create the rule.

25. Click on **Add Rule**.

26. Select the **Send LDAP Attribute as Claims** claim rule template and click **Next**.

27. Enter a name for the rule. **Example:** Groups.

28. Select the **Active Directory** as the Attribute Store.

29. Add the following row in the LDAP Mapping Attributes table:

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

30. Click on **OK** to create the rule.

31. Click on **Add Rule**.

32. Select the **Transform an Incoming Claim** claim rule template and click **Next**.

33. Enter a name for the rule. **Example:** Named ID Transform.

34. Complete the following fields:

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

35. Select the **Pass through all claim value** radio option.

36. Click on **OK** to create the rule.

37. Click **OK** to close the Issuance Transform Rules dialog box.

Azure AD

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

Setting Up the SAML App

1. Log into the Azure portal with administrator permissions.
2. Go to **Azure Active Directory > Enterprise applications**
3. Click on **+New Application** then **Create your own application**.
4. Choose **Integrate any other application you don't find in the gallery (Non-gallery)**.

5. Enter an application name such as **ThreatQ** then click **Add**.
6. Select **Set up single sign on** then choose **SAML**.
7. Select Edit on **Basic SAML Configuration**.
8. Enter the **Entity ID** and **Reply URL(Assertion Consumer Service URL)** as follows:

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 Url	Optional

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

9. Under **Attributes & Claims**, set the **Unique User identifier (Name ID) format** to **Email Address**.
10. In the **Additional claims** section **add uid** and set the value as `user.mail`.

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

2 User Attributes & Claims


givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
uid	user.mail
Groups	user.groups
Unique User Identifier	user.userprincipalname

11. You also need to add an attribute you want to map to the roles in ThreatQ. In this example we added a Claim and created a **Groups** attribute and mapped it to all **user.groups** assigned to the

application. The group id the user belongs to is then included in the SAML assertion upon login.

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

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 ⓘ



In the example above, **Groups** would be entered as the Attribute Key in ThreatQ. The Attribute Value would be one of the Group IDs (Group Object ID) assigned to the application in Step 9.

- On the Assignments tab, verify that each of the users or groups that should have access have been assigned to the application.

13. Under **SAML Signing Certificate**, click the **Download** link for the **Certificate (Base64)** and the **Metadata** file. These files are required in steps 4 and 5 in the [Configuring SAML](#) topic.

3
SAML Signing Certificate ✎

Status	Active
Thumbprint	1DA399F6A24D8BB762A855939148E4D380662325
Expiration	4/29/2023, 5:06:02 PM
Notification Email	welshh@outlook.com
App Federation Metadata Url	https://login.microsoftonline.com/954a89d9-e0... 📄
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

14. After you complete the [Configuring SAML](#) process, add the SAML Attribute Key and SAML Attribute Value for each ThreatQ user role to the Mapping Permissions section. In the example below, we mapped an Azure AD Group to the Administrative Access using the group's Object ID as the SAML attribute value.

SAML
Disabled ☒ Enabled

Security Assertion Markup Language (SAML) is a single sign-on standard used for logging users into applications based on their sessions in another context. Complete the fields below to set the primary server settings and map your permission levels to SAML.

Connection Information - Identity Provider

Provide either an XML configuration file or a configuration URL below. If you provide a configuration URL, the XML configuration file will be downloaded automatically.

Provide IDP Metadata File

📄 AzureAD_saml.xml
download
🔒

Connection Information - Service Provider Information

In order for your IDP to connect to this platform, you must provide either this Service Provider's Connection URL or upload the Service Provider Metadata File (which can be downloaded below) in your IDP.

Service Provider Connection URL

https://192.168.111.130/api/saml/metadata

Copy and paste this to your IDP platform

Service Provider Metadata File

📄 threatq-sp.xml
download

Mapping Permission Levels

(Note: You can not list the same SAML User Group for multiple permission levels)

Administrative Access

SAML Attribute Key
Groups

SAML Attribute Value
a59d3535-f0be-408d-800b-f24f77fa1dd7

Primary Contributor Access

SAML Attribute Key

SAML Attribute Value

Read Only Access

SAML Attribute Key

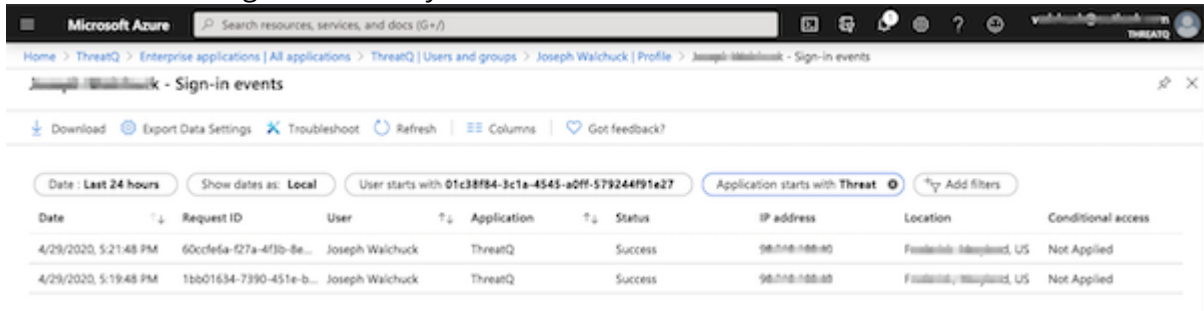
SAML Attribute Value



When you test the application from the Azure Portal, you will receive the following error message: SAML authenticated but missing Client ID parameter. This happens because we do not yet support IdP-initiated SSO. You must validate the authentication from the ThreatQ application.

15. In the Azure Portal, you can navigate to the User Sign-Ins under the user to view the login attempts.
If your authentication is successful but you receive a SAML authenticated but missing group requirements message this indicates that the required attributes mapped to the TQ

roles are not configured correctly.



The screenshot shows the Microsoft Azure portal interface for ThreatQ sign-in events. The breadcrumb navigation is: Home > ThreatQ > Enterprise applications | All applications > ThreatQ | Users and groups > Joseph Walchuck | Profile > Joseph Walchuck - Sign-in events. The page title is "Joseph Walchuck - Sign-in events". Below the title are links for Download, Export Data Settings, Troubleshoot, Refresh, Columns, and Got feedback?. There are filters for Date (Last 24 hours), Show dates as (Local), User starts with (01c38f84-3c1a-4545-a0ff-579244f91e27), and Application starts with (ThreatQ). The table below shows two sign-in events.

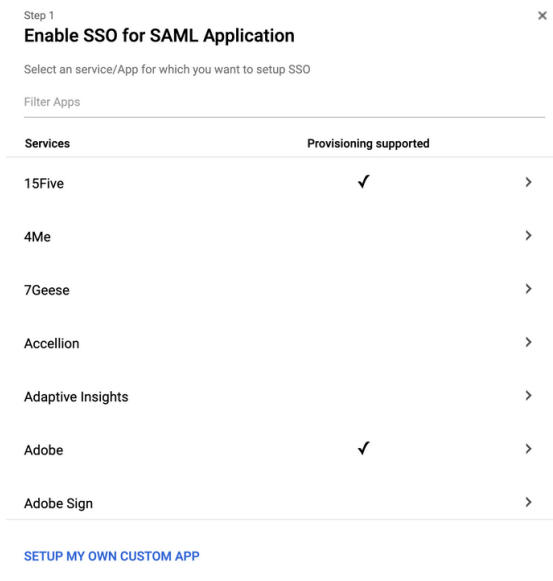
Date	Request ID	User	Application	Status	IP address	Location	Conditional access
4/29/2020, 5:21:48 PM	60c0cfe1a-f27a-4f3b-8e...	Joseph Walchuck	ThreatQ	Success	98.118.118.10	Fresno, CA, US	Not Applied
4/29/2020, 5:19:48 PM	1bb01634-7390-451e-b...	Joseph Walchuck	ThreatQ	Success	98.118.118.10	Fresno, CA, US	Not Applied

Google G Suite

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

Setting Up the SAML App

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



The screenshot shows the Google Administrative Console SAML Apps page. The title is "Step 1 Enable SSO for SAML Application". Below the title is the instruction "Select an service/App for which you want to setup SSO". There is a "Filter Apps" input field. The table below lists services and their provisioning support.

Services	Provisioning supported
15Five	✓
4Me	
7Geese	
Accellion	
Adaptive Insights	
Adobe	✓
Adobe Sign	

At the bottom of the table is a link: [SETUP MY OWN CUSTOM APP](#).

The Google IdP information page loads.

Step 2 of 5

Google IdP Information

Choose from either option to setup Google as your identity provider. Please add details in the SSO config for the service provider. [Learn more](#)

Option 1

SSO URL

https://accounts.google.com/o/saml2/idp?idpid=C03ml9sl6

Entity ID

https://accounts.google.com/o/saml2?idpid=C03ml9sl6

Certificate

Google_2023-5-17-115147_SAML2.0

Expires May 17, 2023

Download

OR

Option 2

IDP metadata

Download

PREVIOUS
CANCEL
NEXT

- Click on **Next**.
- 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

- Click on **Next**.
- Complete the *Service Provider Details* fields:

FIELD	DESCRIPTION	EXAMPLE
ACS URL	Assertion Consumer Service is your ThreatQ URL + appended the “/api/saml/acs” string.	https://threatq.example.com/api/saml/acs
Entity ID	The Entity ID is your ThreatQ URL + appended with the “/api/saml/metadata” string.	https://threatq.example.com/api/saml/metadata
Name ID Format	Set this field to Email .	N/A

Step 4 of 5 ×

Service Provider Details

Please provide service provider details to configure SSO for your Custom App. The ACS url and Entity ID are mandatory.

ACS URL *

Entity ID *

Start URL

Signed Response ☐

Name ID Basic Information Primary Email

Name ID Format UNSPECIFIED

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**:

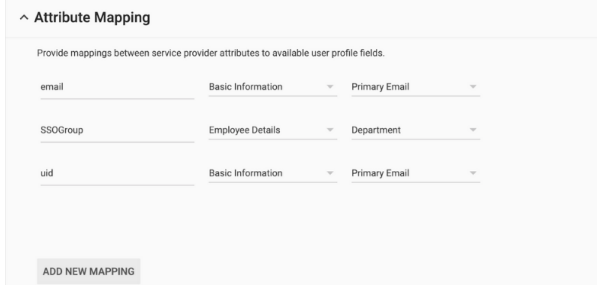
15. Create the **SSOGroup** mapping for ThreatQ roles:

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:



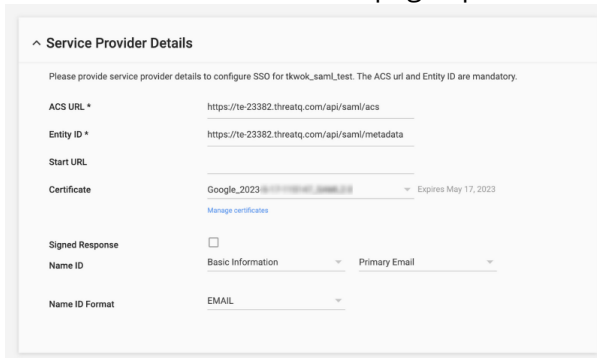
17. Click on **Finish**.

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**.

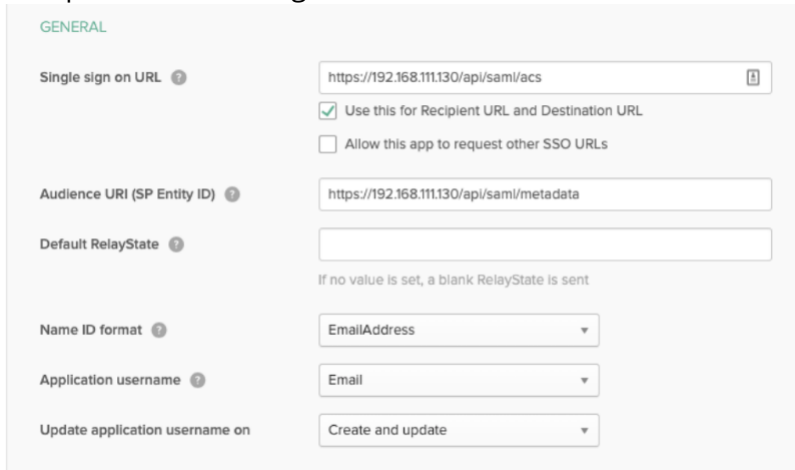
22. Download the **certificate** and the **IdP Metadata** files that are required in steps 4 and 5 in the *Configuring SAML* section in the [About SAML Authentication](#) topic.

Okta

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

1. Log into the Okta web application.
2. Click on the **Admin** button located to the top-right of the screen.
The Dashboard page loads.
3. Click on the **Applications** tab.
The Application page loads.
4. Click on **Add Application**.
5. The Add Applications page loads.
6. Click on **Create New App**.
The Create New Application dialog box opens.
7. Select **Web** from the Platform dropdown.
8. Select **SAML 2.0** for the Sign on method.
9. Click on the **Create** button.
The Create SAML Integration page opens with the General Settings tab selected.

10. Enter a name for the app in the **App Name** field.
11. Click on **Next**.
The Configure SAML section loads.
12. Complete the following fields:



GENERAL

Single sign on URL  

☒ 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

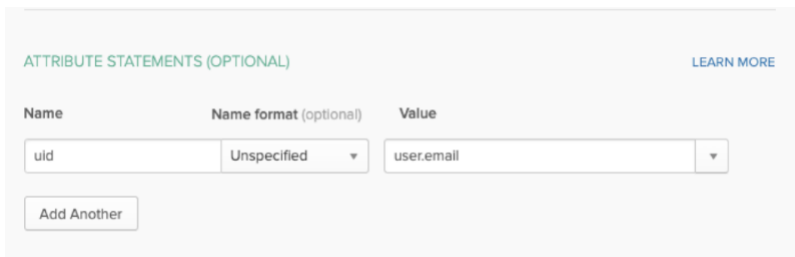
Name ID format 

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.
Name ID format	EmailAddress	
Application username	Email	ThreatQ requires that this field be set to Email.

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



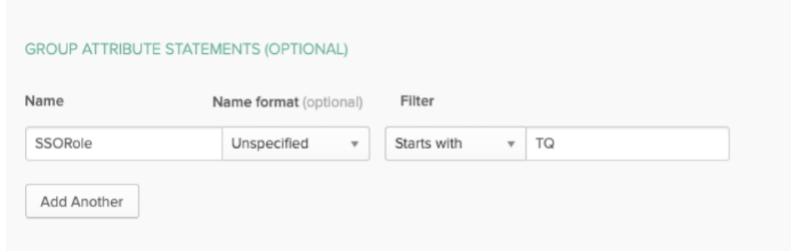
ATTRIBUTE STATEMENTS (OPTIONAL) [LEARN MORE](#)

Name	Name format (optional)	Value
uid	Unspecified	user.email

[Add Another](#)

NAME	NAME FORMAT	VALUE
uid	Unspecified	user.email

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




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

15. Click on **Preview the SAML Assertion** to confirm that the settings are correct.
16. Click on **Next**.
The Feedback section loads.
17. Select **I'm a software vendor. I'd like to integrate my app with Okta** and then click on **Finish**.
The Application details page loads.
18. Click on the **Assignments** tab.
19. Click on the **Assign** dropdown and select **Assign to Groups**.
20. Assign the app to groups that will be used to map ThreatQ roles.
21. Click on **Save and Go Back**.
22. Click on **Done**.
23. Click on the **Sign On** tab.
24. In the **Sign On Methods** section, right-click and download the **Identity Provider metadata** file.
25. Click on the **View Setup Instructions** button.



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

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

SSL Client Certificate Authentication

About SSL Client Certificate Authentication

ThreatQ supports SSL Client Certificate Authentication by allowing on-premise customers to upload PEM-encoded CA certificate files. After this file is uploaded and configured, individual ThreatQ logins can be associated with a user's certificate SHA-1 fingerprint. This allows users to authenticate and access ThreatQ via their:

- Common Access Cards (CACs)
- Personal Identity Verification (PIV) cards
- Smart cards
- SSL client certificates



If you want to migrate from LDAP or SAML authentication to SSL Client Certificate Authentication, please contact ThreatQ Support for assistance.

Requirements

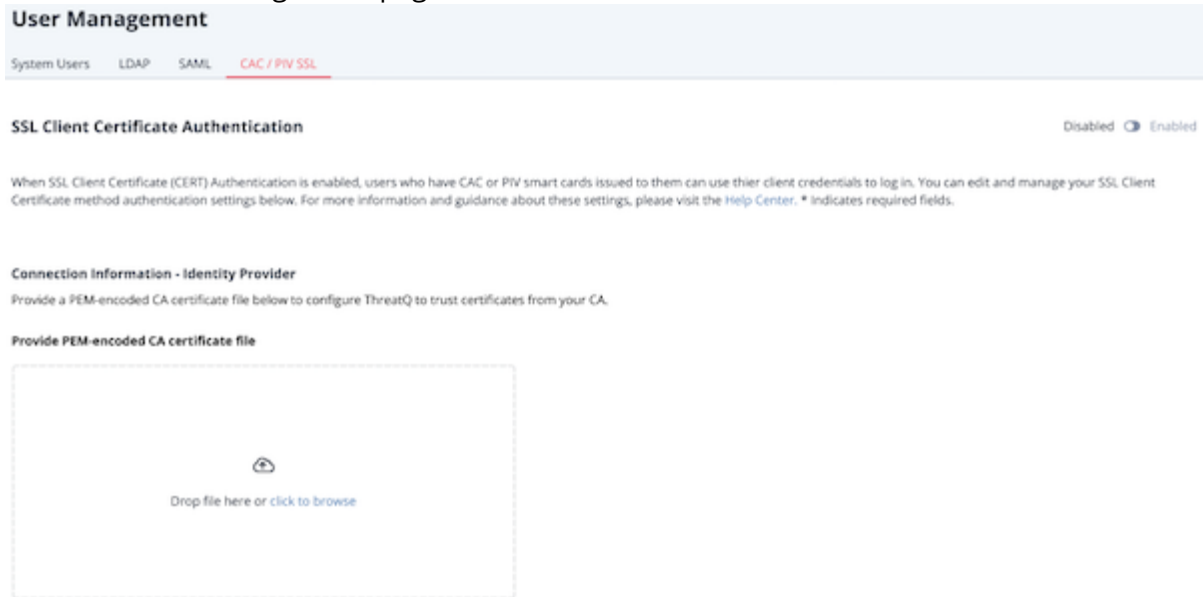
- On-premise instance of the ThreatQ Platform 5.9 or greater.
- PEM-encoded, X.509 CA certificate file
- CAC, PIV card, Smart card, or SSL client certificate
- Administrative or maintenance login

Configuring Client Certificate Authentication



Only Administrative or Maintenance logins have access to the CAC/PIV SSL tab in the User Management page. This tab is used to configure SSL Client Certificate Authentication.

1. From the User Management page, click the CAC/PIV SSL tab.



2. Upload the CA certificate file using one of the following methods:
 - Drag and drop the file into the dialog box.
 - Select the click to browse link to locate the file on your local machine.
3. After you upload the file:
 - The system displays the following message:
Once enabled, CAC / PIV SSL Authentication will take effect for system users upon the next login.
 - The Disabled/Enabled toggle switches to Enabled.
 - The certificate's serial number and expiration date is displayed.



If SAML authentication is active on your ThreatQ instance, the Are you sure? window returns the following warning and prompts you to confirm your choice: Currently you have SAML authentication enabled on your system. By enabling CAC / PIV SSL authentication, SAML will become disabled immediately. Upon next login, SAML users will no longer be able to authenticate via that method. Would you like to proceed?
You must click the **Confirm** button to continue.

4. Now that SSL Client Certificate Authentication is enabled, use one of the following methods to add a certificate fingerprint to your profile.



Until you add a certificate fingerprint to your user profile, each time you access a new ThreatQ page you will be prompted to select a certificate.

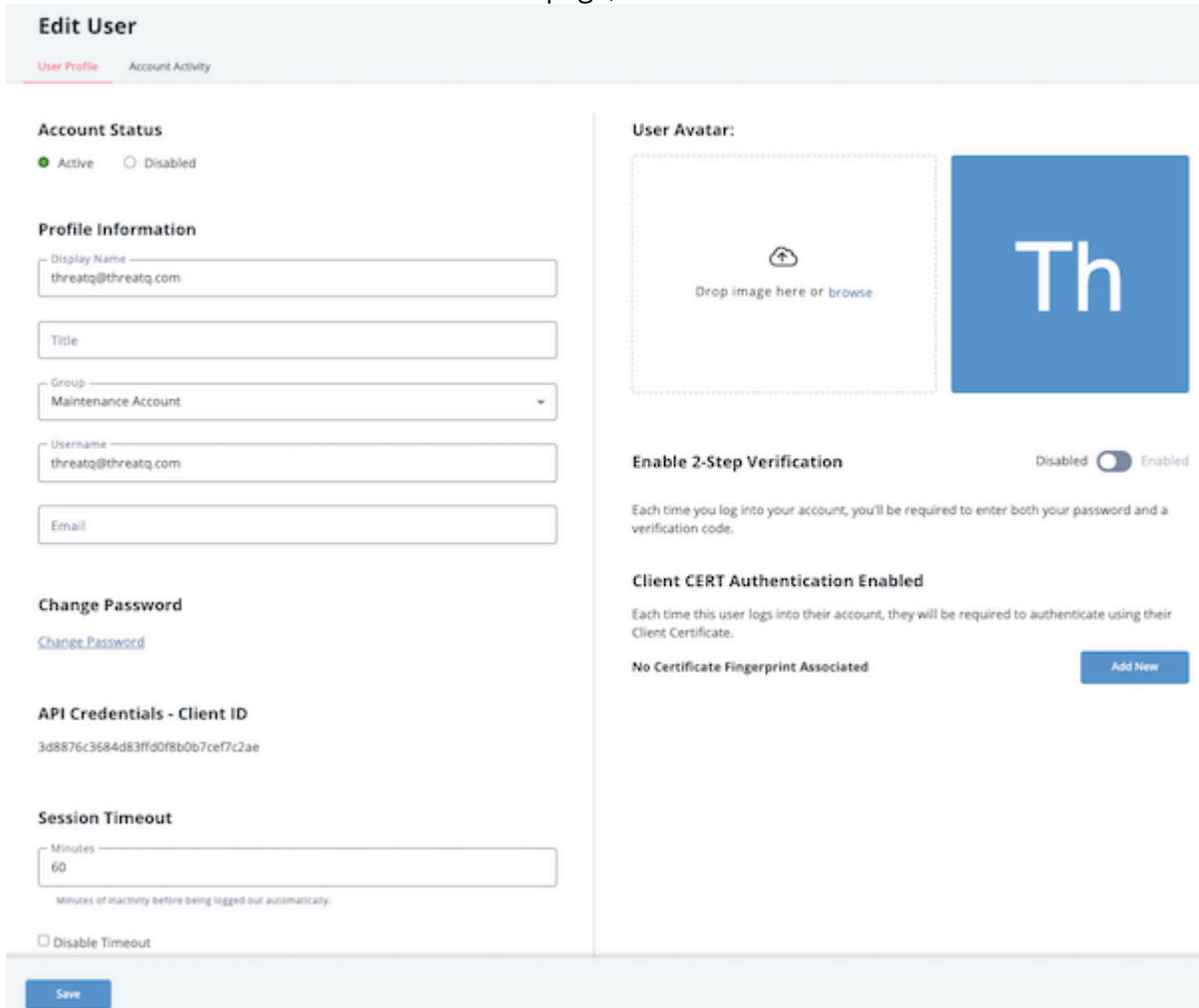
- Log out of ThreatQ and add your certificate fingerprint during log in.
 - Use the System Users tab to add your certificate fingerprint to your user profile.
5. Use one of the following methods to add certificate fingerprints for users:
 - Users can add their own certificate fingerprint during their next login. If needed, you can [set up usernames and passwords](#) in the System Users tab on the User Management page.

- Maintenance or Administrative users can use the System Users tab to add the new certificate fingerprint to user profiles.

Adding a User's Certificate Fingerprint - User Profile

After Client Certificate Authentication is enabled, an Administrative or Maintenance user can add a certificate fingerprint to a ThreatQ user profile.

1. From the User Management screen, click the User Management tab.
2. Locate and click the user's display name.
3. From the User Profile tab in the Edit User page, click the **Add New** button.



Edit User

User Profile Account Activity

Account Status

☒ Active ☐ Disabled

Profile Information

Display Name
threatq@threatq.com

Title

Group
Maintenance Account

Username
threatq@threatq.com

Email

Change Password

[Change Password](#)

API Credentials - Client ID

3d8876c3684d83ff0f8b0b7cef7c2ae

Session Timeout

Minutes
60

Minutes of inactivity before being logged out automatically.

☐ Disable Timeout

User Avatar:

Drop image here or browse

Enable 2-Step Verification Disabled ☒ Enabled

Each time you log into your account, you'll be required to enter both your password and a verification code.

Client CERT Authentication Enabled

Each time this user logs into their account, they will be required to authenticate using their Client Certificate.

No Certificate Fingerprint Associated [Add New](#)

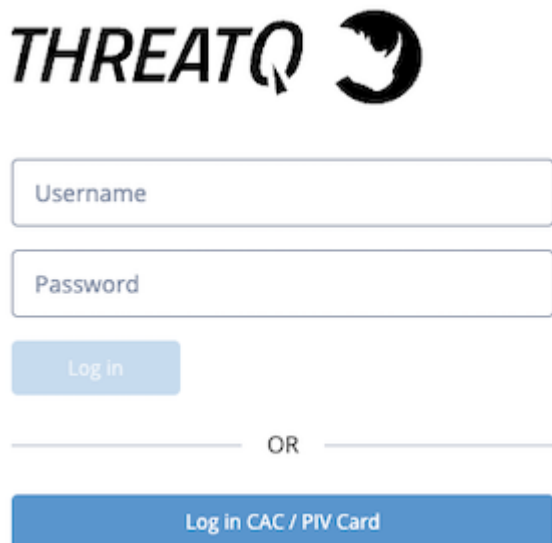
[Save](#)

4. Enter the user's certificate fingerprint.
5. Click the **Submit** button.

Adding Your Certificate Fingerprint - Login Page

1. Access your certificate, and enter your PIN. Your certificate must be active in the browser before you navigate to your ThreatQ instance.

2. Navigate to your ThreatQ instance.



3. Enter your username and password.
4. Click the **Log in** button.
5. The Store Fingerprint to Profile window prompts you to save your certificate fingerprint to your ThreatQ user profile.
6. Click the **Acknowledge & Login** button.
ThreatQ saves your certificate fingerprint. The next time you login, you can click the **Log in with CAC/PIV Card** button to access ThreatQ.

Using Certificate Authentication to Log In



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

After you or an Administrative/Maintenance user add a certificate fingerprint to your ThreatQ user profile, click the **Log in with CAC/PIV Card** button to access ThreatQ.

Managing Certificate Files

After you upload a certificate file and enable SSL Client Certificate Authentication, you may need to disable authentication to troubleshoot an issue or to migrate to a new authentication method. Or, you may want to remove or replace you current certificate file.



Only Administrative or Maintenance logins have access to the CAC/PIV SSL tab in the User Management page which is used to manage SSL Client Certificate Authentication.

Disabling SSL Client Certificate Authentication



After you disable SSL Client Certificate Authentication, you must reset all Admin, Primary Contributor, and Read Only access user passwords so that users can log in with their ThreatQ username and password. Maintenance Account users do not require a password reset and can continue to use their current password.

1. From the User Management page, click the CAC/PIV SSL tab.

Help Center. * Indicates required fields.' Below this is a section titled 'Connection Information - Identity Provider' with the instruction 'Provide a PEM-encoded CA certificate file below to configure ThreatQ to trust certificates from your CA.' and a label 'Provide PEM-encoded CA certificate file'. A text input field contains the value '12925172493580113718' and a label 'Certificate Expiration Date: 10/25/2024'. Below the input field are two buttons: 'Replace' (blue) and 'Remove' (red)." data-bbox="141 430 878 671"/>

2. Click the Disabled/Enabled toggle to change the status to Disabled. The Are You Sure? window prompts you to confirm the change.
3. Click the **Confirm** button.
Even though SSL Client Certificate Authentication is disabled, the file that contains the certificate information is not deleted. This makes it easier for you to re-enable authentication.
4. Reset user passwords to allow users to log in with their ThreatQ username/password.

Removing a Certificate File



After you remove the certificate file, you must reset all Admin, Primary Contributor, and Read Only access user passwords so that users can log in with their ThreatQ username and

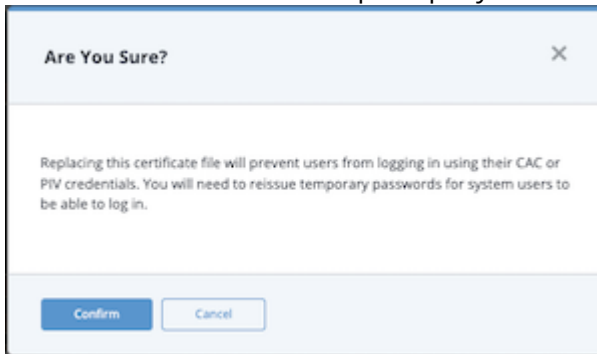
password. Maintenance Account users do not require a password reset and can continue to use their current password.

1. From the User Management page, click the CAC/PIV SSL tab.
2. Click the **Remove** button.
The Are You Sure? window prompts you to confirm the change.
3. Click the **Remove** button.
SSL Client Certificate Authentication is disabled and all information is deleted from the certificate file.
4. Rest user passwords to allow users to log in with their ThreatQ username/password.

Replacing a Certificate File

 After you replace a certificate file, you must either reset all Admin, Primary Contributor, and Read Only access user passwords so that users can log in and associate a new certificate with their user profile or add the new certificate fingerprints to each user profile. Maintenance Account users do not require a password reset and can continue to use their current password. However, they will also need to select a new certificate to log in using SSL Client Certificate Authentication.

1. From the User Management page, click the CAC/PIV SSL tab.
2. Click the **Replace** button.
The Are You Sure? window prompts you to confirm the change.



3. Click the **Confirm** button.
4. Upload the new certificate file using one of the following methods:
 - Drag and drop the file into the dialog box.
 - Select the click to browse link to locate the file on your local machine.
5. After you upload the file, the new certificate's serial number and expiration date is displayed
6. Use one of the following methods to add new certificate fingerprints for users:
 - Reset user passwords so that they can add their own certificate fingerprint during their next login.
 - Maintenance or Administrative users can use the System Users tab to [add the new certificate fingerprint to user profiles](#).

Managing Certificate Fingerprints

Maintenance and Administrative users can use the User Management page to update or remove the certificate fingerprint associated with a username. Primary Contributor and Read-Only users can view certificate fingerprints but cannot edit them.

Updating Certificate Fingerprints

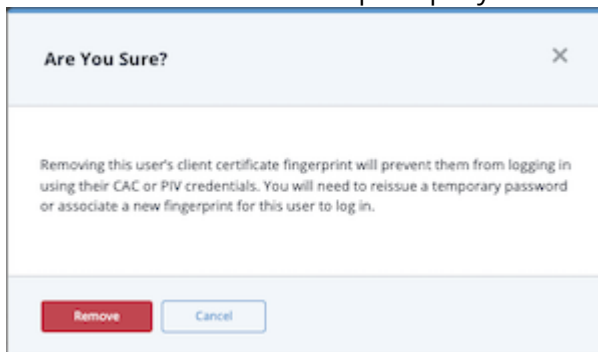
After SSL Client Certificate Authentication is enabled, you can change the certificate fingerprint on a user profile.

1. From the User Management screen, click the User Management tab.
2. Locate and click the user's display name.
3. From the User Profile tab in the Edit User page, click the pencil icon next to the user's CERT fingerprint.
4. Enter the new certificate fingerprint.
5. Click the **Submit** button.

Removing Certificate Fingerprints

1. From the User Management screen, click the User Management tab.
2. Locate and click the user's display name.
3. From the User Profile tab in the Edit User page, click the pencil icon next to the user's CERT fingerprint.
4. Click the **Remove** button.

The Are You Sure? window prompts you to confirm the removal.



5. Click the **Remove** button.

Troubleshooting SSL Client Certificate Authentication

The following is a list of common authentication errors a user may encounter when accessing ThreatQ.

ERROR MESSAGE	CAUSE	RESOLUTION
Password Expired Your temporary password has expired. Please use your CAC / PIV credentials to log in to this system. If your client credentials do not authenticate, please contact your administrator.	An Administrative, Primary Contributor, or Read-Only user attempted to use a password to log in after a CAC / PIV SSL fingerprint was added to the user profile.	From the ThreatQ login page, click the Log in with CAC/ PIV Card button to access ThreatQ.
Certificate Error Your stored fingerprint indicates that your CAC / PIV certificate has encountered an error or has expired. Please contact your administrator for new credentials.	A user attempted to use an expired CAC / PIV SSL certificate.	Ask a Maintenance or Administrative user to add your new certificate fingerprint to your user profile.
The fingerprint has already been taken.	A user attempted to log in using a certificate/fingerprint that is already associated with another user profile.	Contact a Maintenance or Administrative user to determine the root cause of the certificate duplication.

The following is a list of common authentication errors a user may encounter when configuring SSL Client Certificate Authentication.

ERROR MESSAGE	CAUSE	RESOLUTION

Upload a valid RSA certificate to enable.

An Administrative or Maintenance user tried to move the Disabled/Enabled toggle to Enabled without uploading a CA certificate file.

See the [SSL Client Certificate Authentication](#) topic for the steps required to enable SSL Client Certificate Authentication.

The certificate file is not a valid X.509 certificate.

An Administrative or Maintenance user tried to upload a certificate file that was not a PEM-encoded, X.509 CA certificate file.

Upload a PEM-encoded, X.509 CA certificate file.

This certificate is expired.

An Administrative or Maintenance user tried to upload a certificate file with an expiration prior to the current date.

Upload a certificate file with an expiration date after than the current date.

A

Adversaries [259](#), [261](#), [260](#), [484](#), [486](#), [487](#), [484](#)
Air Gapped Data Sync (AGDS) [29](#), [40](#), [0](#)
Audit Log [491](#)
Authentication [0](#), [20](#)
Automatic Expiration [115](#)

B

Bulk Actions [454](#), [457](#), [465](#), [460](#), [465](#), [462](#), [467](#)

C

Command Line Interface [51](#)
Commands [53](#)

D

Dashboard (default) [69](#), [68](#), [70](#), [70](#)
Dashboards (custom) [73](#), [112](#), [93](#), [112](#), [106](#)
Data Collections [444](#)
Data Controls [113](#)

E

Events [280](#), [282](#), [281](#)
Expiration [115](#), [462](#), [324](#), [117](#), [323](#), [118](#), [116](#), [323](#)
Exports [140](#), [143](#), [144](#), [143](#), [144](#), [139](#), [145](#), [162](#),
[166](#)

F

Feed Health Notifications [203](#), [209](#)
Files [285](#), [287](#), [286](#)
Filter Sets [407](#), [438](#), [412](#), [416](#), [430](#), [439](#), [434](#), [419](#),
[430](#), [440](#), [431](#), [422](#), [420](#), [440](#), [424](#), [433](#), [437](#), [425](#),
[417](#)

I

Indicator Defanging [321](#)
Indicator Scoring [325](#)
Indicator Status [328](#), [327](#), [212](#)
Indicators [297](#), [299](#), [298](#), [0](#), [89](#)

J

Job Management [194](#)

L

Licensing [198](#), [197](#)
Logging In [23](#), [24](#)

N

Navigation [199](#)
Notifications [202](#)

O

Object Details [477](#), [484](#), [475](#), [489](#), [478](#), [483](#), [481](#)
Object Management [211](#)

P

Proxy [248](#)

R

Reports [232](#), [232](#), [232](#), [232](#), [233](#)

S

SAML [512](#), [523](#)
Scoring [325](#)
Scoring Algorithms [126](#)
Search Filters [412](#), [430](#), [437](#), [438](#), [443](#)
Search Results [450](#), [445](#), [444](#)
Searches [407](#)
Signatures [340](#)
STIX [343](#), [343](#), [346](#), [359](#)

T

Tasks [384](#), [384](#)
Threat Library [397](#)
ThreatQ Backup/Restore [48](#)
Traffic Light Protocol (TLP) [131](#), [129](#), [129](#), [130](#)

U

User Accounts [493](#), [493](#), [494](#), [498](#), [495](#), [498](#)
User Roles [500](#), [500](#), [500](#), [500](#)

W
Whitelisting [133](#)