ThreatQuotient

A Securonix Company

ThreatQ User Guide

Version 6.21.0

September 30, 2026

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

Support
Email: tq-support@securonix.com
Web: https://ts.securonix.com
Phone: 703.574.9893

Contents

Warning and Disclaimer **16**
About the ThreatQ Platform **17**
How the ThreatQ Platform Works 17
Threat Library 17
Adaptive Workbench 18
Open Exchange 18
Platform Modules 19
ThreatQ Investigations 19
ThreatQ TDR Orchestrator 20
ThreatQ Data Exchange 21
Getting Started With ThreatQ **23**
Documentation and Training Resources 23
ThreatQ Documentation 23
Support Resources 24
Environment Specifications 25
ThreatQ Backups 25
User Access 26
User Permissions 26
Adding Data 27
Managing Your Data 28
Dashboards 28
Threat Library 28
Threat Library Audits 30
Scoring 30
Additional Resources 31
Accessing the Platform **32**
About Accessing the Platform 32
User Account Authentication 34
Session Timeout 34
Authentication Methods 35
Changing Authentication Methods 36
2-Step Verification 38
Enabling 2-Step Verification 38
Platform Login 39
Local Log In 39
Single Sign-On (SSO) 40
SSL Client Certificate Authentication Log In 42
Air Gapped Data Sync **43**
About Air Gapped Data Sync 43
AGDS Prerequisites 44
Authentication Considerations 44
Export Data 45
Excluded or Limited Data 47
Storage and Other Data Information 47
Storage (Exports) 47
Tags 48
Spearphish 48

ThreatQ Investigations ... 49
Exports ... 50
Executing Exports ... 50
Export Flags ... 52
Commonly Used Flags ... 52
Other AGDS Export Flags ... 54
Scheduled Exports ... 58
Steps for Larger Data Sets ... 60
Steps for Larger Data Sets Starting at the Beginning of Time ... 60
Steps for Larger Data Sets Starting at a Specific Start Date ... 60
Imports ... 62
Executing the AGDS Import Command ... 62
Executing the AGDS Import Command ... 63
Import Command Flags ... 64
Reports, Logs, Synchronization ... 67
Console Output ... 67
Sync Export Report ... 67
Sync Import Report ... 68
AGDS Cron Logs (Export) ... 68
Recording Handling and Synchronization Tables ... 68
Application Logs ... 70
Installing an Air Gapped ThreatQ Instance ... 71
Operating System and Kubernetes Distribution Maintenance ... 71
Supported Hardening Standards by Operating System ... 71
Security Technical Implementation Guide (STIG) Installs ... 72
Prerequisites ... 72
System Requirements ... 72
ThreatQ v6 BYOD Partitioning Overview ... 73
Specific Sizes Overview ... 73
Specific Size Breakdown ... 75
Dedicated Mount /opt ... 77
Before You Begin ... 77
Set up Your Ubuntu or RHEL Environment ... 77
Pin Your RHEL 9 Version ... 79
Pin Your Ubuntu 22.04 Version ... 79
Configure Internal Networking ... 79
Prepare the RKE2 Configuration File ... 80
Change the Kubernetes Subnet (Optional) ... 81
Set Up kubectl ... 81
Verify Your RKE2 Installation ... 83
Air Gapped Installation ... 83
Access Your New ThreatQ 6x Instance ... 88
Upgrading an Air Gapped ThreatQ Instance ... 89
Troubleshooting ... 91
Before you Begin ... 91
Troubleshooting Scenarios ... 92
AGDS Recovery Steps ... 93
Audit Log ... 94
About the Audit Log ... 94
Configuring Audit Log Exports ... 94
Audit Log Entries ... 95
Audit Log Entries ... 96
Authentication/User Activity Logging ... 96

User Management Logging 99
Integration Configuration Logging 100
Data Retention Policy Logging 101
ThreatQ Data Exchange (TQX) Logging 102
TAXII Server Logging 103
ThreatQ TDR Orchestrator (TQO) Configuration Logging 105
Export Audit Log Command 110
Before You Begin 110
Performance Considerations 110
Export Audit Logs Command 111
Export Audit Logs Command Flags 111
Filtering Scenarios 112
Exported Data 114
Schedule Automatic Exports 114
Troubleshooting 115
Backup and Restore 116
ThreatQ Backup 116
ThreatQ Backup Process 117
ThreatQ Restore 118
ThreatQ Restore Process 118
Command Line Interface (CLI) 120
About the Command Line Interface (CLI) 120
Maintenance Mode 120
Commands 122
Integration Commands 122
Add/Upgrade CDF 122
View Feed Queues 123
System Object Commands 124
Delete Adversary Descriptions 124
Merge Attributes 124
Source Consolidation 126
Source Merge 126
Convert TLP 128
Update TLP Designations 129
Indicator and Signature Statuses Overrides 131
System-Level Commands 132
Airgap Import 132
Airgap Export 132
Allow Cross-Origin Resource Sharing for Specific Hostnames 132
Disable Export Logging 133
LDAP Diagnostic Searches 133
Auto Configuration MariaDB Command 134
System ThreatQ Purge 134
Reset User Password 135
Dashboards 136
About Dashboards 136
Default Dashboard 137
Overview of Intelligence by Score 137
Incoming Intelligence 139
Watchlist Activity 139
Tasks 140
Custom Dashboards 141
About Custom Dashboards 141

Analytics Dashboard 143
About Analytics Dashboards 143
Adversary Analytics Dashboard 144
Adversaries Summary Table 144
Adversaries Overlap Table 145
Indicator Distribution Pie Chart 147
Event Analytics Dashboard 148
Events History Scatter Plot 149
Events Heatmap 150
Files Analytics Dashboard 153
File Type Pie Chart 153
Files Table 154
Indicator Analytics Dashboard 156
Recently Created Indicators Histogram 156
Most Recent 100 Indicators 158
Attributes Table 159
Recent Sources 161
Attack Phases 162
Dashboard Widgets 165
Available Widget Types 165
Bar Chart Widget 165
Description Widget 167
Line Chart Widget 168
Count Widget 170
Pie Chart Widget 171
Table Widget 172
Widget Behavior Notes 174
Dashboard Management 175
Accessing a Dashboard 175
Add an Existing Dashboard to Your View 176
Creating a Dashboard 177
Editing a Dashboard 179
Deleting a Dashboard 180
Reassigning a Dashboard of a Deleted User 180
Dashboard Sharing 181
Sharing a Dashboard 181
Updating Dashboard Permissions 183
Shared Dashboards of a Deleted User 184
Dashboard Export 185
Creating a Dashboard PDF 185
User View Management 188
Adding a Dashboard to Your View 188
Removing a Dashboard from Your View 189
Changing Dashboard Order 189
Data Controls 191
About Data Controls 191
Indicator Expiration Policies 193
Accessing the Indicator Expiration Page 193
How ThreatQ Calculates Expiration Dates 194
Selecting an Expiration Policy per Feed 194
Adding Exceptions 195
Applying Expiration Policy Changes to Data 196
Common Expiration Policy Scenarios 197

Common Expiration Policy Scenarios - Feed Updates of Indicator Statuses 199
Data Retention Policy 201
Accessing the Data Retention Policy Page 201
Creating a Data Collection for the Data Retention Policy 203
Creating a Data Retention Policy 203
Reviewing Data Retention Policy Performance 204
Scoring Algorithms 206
How Scoring Works 206
Scoring Criteria 206
Accessing the Scoring Sensitivity Page 207
Configure Scoring by Indicator Type 208
Configure Scoring by Indicator Source 209
Configure Scoring by Attribute 209
Configure Scoring by Adversary Relationship 210
Update a Scoring Algorithm 210
Scoring Considerations 211
Traffic Light Protocol (TLP) 212
Labels 212
TLP Assignment Hierarchy 212
Access TLP Settings 213
Configure TLP Visibility 214
Apply a TLP Label to Source 214
Whitelisted Indicators 216
Wildcard Options 216
Accessing the Whitelisted Indicator Rules 217
Creating a Whitelisted Rule 218
Editing a Whitelisted Rule 219
Removing a Whitelisted Rule 221
Exports 223
About Exports 223
Managing Exports 225
Accessing the Exports List 225
Viewing an Export 226
Enabling/Disabling Exports 226
Adding an Export 227
Duplicating an Export 231
Editing an Export's Connection Settings 231
Editing an Export's Output Format 232
Deleting an Export 232
Output Format Options 233
Special Parameters Field 233
Filtering by Attribute Value 250
Adding Differential Flags 250
Adding Parameters to the End of the URL 251
Using Export Filters 251
Output Format Template Field 252
Inserting Variables 253
Template Format 253
Output Format Template Examples 254
Export Template Examples by Object Type 254
Adversaries Template 254
Assets Template 255
Attack Pattern Template 255

Campaign Template ... 256
Course of Action Template ... 256
Events Template ... 257
Exploit Target Template ... 258
Identity Template ... 258
Indicators Template ... 259
Intrusion Set Template ... 259
Malware Template ... 260
Report Template ... 261
Signatures Template ... 261
Tool Template ... 262
TTP Template ... 262
Vulnerability Template ... 263
Template Variables ... 263
Adversary Examples ... 263
Indicator Examples ... 266
Specific Indicator Exports ... 271
Integrations Management ... 272
About Integrations Management ... 272
Integration Types ... 274
Actions ... 274
Apps ... 274
Configuration-Driven Feeds (CDFs) ... 274
Custom Connectors ... 275
Operations ... 275
About My Integrations ... 276
Accessing My Integrations ... 277
Filtering Your View ... 278
Flagged Integrations ... 280
Adding an Integration ... 282
Adding a STIX/TAXII Feed ... 285
Configuring an Integration ... 289
Triggering a Manual Run ... 294
Running an Operation ... 296
Activity Logs (feeds) ... 298
Activity Log Details ... 298
Accessing a CDF's Activity Log ... 300
Feed Run Activity ... 302
Feed Run Activity Details ... 302
Accessing Feed Run Activity ... 303
Removing an Integration ... 305
Removing an Integration ... 305
Disabling an Integration ... 306
Job Management ... 307
Tips and Tricks ... 307
Accessing the Job Management page: ... 308
Licensing ... 311
Managing Your ThreatQ License ... 311
Viewing License Status ... 311
Updating a License ... 311
Navigation Menu ... 312
Notifications ... 315
Notifications ... 315

Feed Health Email Notifications 317
Configuring Mail Server 317
Enabling Feed Health Notifications 320
Notification Center 323
Sharing Notifications 324
Object Management 326
About Object Management 326
Indicator Statuses Management 327
Indicator Status Assignment 327
Indirect Indicator Status 327
Protected Indicator Statuses 327
Viewing Indicator Statuses 327
Suppressing Indicator Status Updates 329
Adding an Indicator Status 329
Editing an Indicator Status 330
Deleting an Indicator Status 331
Indicator Types 333
Object Statuses 335
Viewing Object Statuses 335
Adding an Object Status 337
Editing an Object Status 338
Editing Object Status Order 338
Deleting an Object Status 339
Event Types 340
Viewing Event Types 340
Adding an Event Type 342
Editing an Event Type 344
Deleting an Event Type 345
Attribute Management 347
Selecting an Attribute Key or Value 348
Editing Attribute Keys 349
Merging Attribute Keys 349
Deleting Attribute Keys 350
Editing Attribute Values 350
Merging Attribute Values 351
Deleting Attribute Values 351
Relationships 352
Relationship Limits 352
What to Do When an Object Exceeds the Relationship Limit 353
Tips and Tricks 354
Reports 355
Generating Reports 355
Turning Off the Pop-Up Blocker in Chrome 356
Report Options 357
Customizing the Report Header 357
Customizing Report Text Colors 357
Adding a Custom Disclaimer to a Report 358
Previewing Report Customization 358
Sharing 359
User Permission Levels 359
User Permission Levels and User Roles 360
View-Only Permissions for All Users 361
Sharing Notifications 361

Permission Conversion ... 362
Permission Levels and Integrations ... 362
Air Gapped Data Sync (AGDS) and Investigation Sharing ... 363
System Configuration ... 364
About System Configuration ... 364
TQAdmin Configuration Options ... 365
Account Security Tab ... 366
Setting Account Lockout ... 366
Configuring User Lockout Settings ... 366
Managing Custom Login Banners ... 368
Banner Behavior ... 368
Enabling a Custom Banner ... 370
Proxy ... 373
Accessing Proxy Configuration ... 373
General Tab ... 376
Configuring Time and Date Settings ... 376
Configuring Indicator Parsing Presets ... 378
Opt In/Out of Product Analytics ... 381
System Banner Display Settings ... 383
About the AI Tab ... 386
TQAdmin Configuration ... 388
Upgrading TQAdmin ... 388
Configuring OpenDXL ... 389
Configuring TAXII ... 390
Configuring Audit Log Exports ... 393
System Objects ... 395
About System Objects ... 395
Adversaries ... 398
Adding Adversaries ... 399
Adding Context ... 400
Editing Adversaries ... 400
Deleting Adversaries ... 401
Assets ... 402
Adding Assets ... 403
Adding Context ... 404
Editing Assets ... 405
Changing the Point of Contact ... 405
Deleting Assets ... 406
Attack Patterns ... 407
Adding an Attack Patterns ... 407
Adding Context ... 409
Editing an Attack Pattern ... 409
Changing the Point of Contact ... 410
Deleting an Attack Pattern ... 411
Campaigns ... 412
Adding a Campaign ... 413
Adding Context ... 417
Editing a Campaign ... 417
Changing the Point of Contact ... 417
Deleting a Campaign ... 418
Courses of Action ... 419
Adding a Course of Action ... 420
Adding Context ... 421

Editing a Course of Action 421
Changing the Point of Contact 422
Deleting a Course of Action 423
Events 424
About Events 424
Adding Events 424
Adding Context 427
Editing Events 427
Changing the Point of Contact 428
Deleting Events 428
Parsing for Events 432
Importing Events with the Spearphish Parser 432
Exploit Targets 438
Adding a Exploit Target 438
Adding Context 440
Deleting a Exploit Target 440
Files 442
Adding Files 442
Adding Context 445
Editing Files 445
Deleting Files 446
Identities 448
Adding an Identity 449
Adding Context 452
Editing an Identity 452
Changing the Point of Contact 453
Deleting an Identity 453
Incidents 455
Adding an Incident 456
Adding Context 457
Editing an Incident 458
Changing the Point of Contact 458
Deleting an Incident 458
Indicators 460
About Indicators 460
Adding an Indicator 460
Adding Context 461
Editing Indicators 462
Deleting an Indicator 462
Parsing for Indicators 464
Selecting a File to Parse 464
Step 1 - Import Indicators Settings 467
Step 2 - Organize and Classify 469
Importing Indicators via CSV 474
CSV Columns 474
Parsing a ThreatQ CSV File and Adding Context 477
Troubleshooting 482
Indicator URL Normalization 483
Supported Defanging Techniques 486
Indicator Expiration 488
Ways an Indicator can Expire 488
Changing the Expiration Date for an Individual Indicator 489
Changing the Expiration Date for Multiple Indicators 489

Indicator Status 490
Default Statuses 490
Custom Statuses 490
Changing the Status of an Individual Indicator 491
Changing the Status for Multiple Indicators 491
Infrastructure 492
Adding Infrastructure Objects 493
Adding Context 494
Editing Infrastructure Objects 495
Changing the Point of Contact 495
Deleting Infrastructure Objects 495
Intrusion Sets 497
Adding an Intrusion Set 498
Adding Context 499
Editing an Intrusion Set 500
Changing the Point of Contact 500
Deleting an Intrusion Set 500
Malware 502
Adding a Malware Object 503
Adding Context 504
Editing a Malware Object 504
Changing the Point of Contact 505
Deleting a Malware Object 505
Notes 507
Adding Notes 508
Adding Context 509
Editing Notes 510
Changing the Point of Contact 510
Deleting Notes 511
Reports 512
Adding a Report 513
Adding Context 514
Editing a Report 514
Changing the Point of Contact 515
Deleting a Report 515
Signatures 517
Adding a Signature 517
STIX 521
About STIX 521
ThreatQ STIX Object Types 521
Attribute Updates 522
Parsing a STIX File for Indicators 522
STIX 1.1.1, 1.2 Data Mapping 525
STIX 2.0 Data Mapping 539
STIX 2.1 Data Mapping 565
Common Properties 568
Tasks 570
Assigning a Task 570
Managing Tasks 573
Tools 574
Adding a Tool 575
Adding Context 576
Editing a Tool 576

Changing the Point of Contact ... 577
Deleting a Tool ... 577
TTPs ... 579
Adding a TTP ... 580
Adding Context ... 581
Editing a TTP ... 581
Changing the Point of Contact ... 582
Deleting a TTP ... 582
Vulnerabilities ... 584
Adding a Vulnerability ... 584
Adding Context ... 586
Editing a Vulnerability ... 586
Changing the Point of Contact ... 587
Deleting a Vulnerability ... 587
Threat Library ... 589
About Threat Library ... 589
Managing Your Library View ... 591
Selecting Object Type View ... 591
Managing Library Columns ... 592
Selecting System Objects ... 593
Basic Search ... 595
What Basic Search Can Match ... 595
Performing a Basic Search ... 595
Search Scope and Object Filtering ... 597
Wildcards and Search Types ... 597
Creating an Object During a Basic Search ... 599
Best Practices and Usage Guidance ... 600
Building Searches with Filter Sets ... 602
About Building Searches with Filter Sets ... 602
Adding Filter Sets ... 602
Deleting Filter Sets ... 604
And/Or Order of Operations ... 605
Context Filters ... 607
Filtering by Author ... 607
Filtering by Attribute ... 607
Using Multiple Attribute Filters ... 608
Filtering by CIDR Block Range ... 612
Filtering by Value Contains ... 612
Filtering by List of Indicators ... 613
Filtering by Keyword ... 615
Filtering by Relationship ... 617
Filtering by Relationship Criteria ... 619
Filtering by Score ... 621
Filtering by Tags ... 623
Filtering by Source ... 624
Filtering by TLP ... 626
Filtering by Point of Contact ... 627
Filtering by Workflow ... 628
Date Filters ... 630
Filtering by Date Created ... 630
Filtering by Last Modified ... 631
Filtering by Published Date ... 632
Filtering by Source Ingest Time ... 634

Filtering by Expiration Date 636
Status Filters 638
Filtering by Status 638
System Maintenance Filters 639
Filtering by Flagged Objects 639
Tasks Filters 640
Filtering Tasks by Assignment 640
Filtering Tasks by Due Date 641
Filtering Tasks by Priority 642
Filtering Tasks by Reported By 643
Type Filters 646
Filtering by Object Type 646
Managing Search Results 647
About Managing Search Results 647
Data Collections 648
Saving Searches as Data Collections 648
Loading Data Collections 649
Modifying a Data Collection 651
Copying a Data Collection 651
Renaming a Data Collection 652
Sharing Data Collections 652
Removing a User's Access to a Data Collection 654
Deleting a Data Collection 655
CSV Exports 657
Exporting Search Results to CSV 657
STIX Exports 658
Bulk Actions 661
Bulk Add Source 662
Bulk Add/Remove Attributes 665
Bulk Add/Remove Attribute Scenarios 667
Bulk Add/Remove Tags 668
Bulk Change Expiration Date 671
Bulk Expiration Change Scenarios 673
Bulk Delete 674
Bulk Add/Remove Relationships 675
Bulk Status Change 677
Object Details Page 679
About Object Details Page 679
Manually Setting an Object's Score 686
Setting a Manual Score for an Object 686
Adding/Removing an Object to the Watchlist 688
Actions Menu 689
Context Panes 692
About Context Panes 692
Attributes Pane 693
Adding an Attribute to an Object 693
Deleting an Attribute from an Object 694
Deleting an Attribute Source from an Object 694
Editing an Object's Attribute 695
Sources Pane 697
Tags Pane 701
Descriptions Pane 702
Spearphish Details Pane 708

Comments Pane ... 710
Adding Comments to an Object ... 710
Editing Comments for an Object ... 711
Deleting Comments from an Object ... 711
Orchestrator Pane ... 713
Audit Log ... 715
Threat Research Agent ... 716
About the Threat Research Agent ... 716
Requirements ... 718
Services ... 720
How the Services Work Together ... 720
Agent Toolbar ... 722
Enable and Configure Agent ... 724
Configuring and Enabling the Agent ... 724
Enabling Tools ... 729
Using the Agent ... 730
Agent Bubble ... 730
Insights Button ... 730
Working with the Agent ... 732
Using ThreatQ Operations as Agent Tools ... 732
Generating Chat Reports ... 733
Generate Report (ThreatQ 6.20.0 and later) ... 733
Generate Report (ThreatQ 6.19.1 and earlier) ... 738
AI-Assisted Report Templates ... 740
Default Categories and Reports ... 741
Sections ... 743
Creating a New Report Template ... 744
Editing / Deleting a AI-Assisted Report Template ... 747
User Management ... 750
About User Management ... 750
Managing User Accounts ... 754
Accessing Your User Account ... 756
Accessing Other User Accounts ... 756
Adding a User ... 757
Editing a User ... 758
Resetting a User Password from the Command Line ... 758
Deleting a User ... 759
Updating a User Avatar ... 760
... 760
Default User Roles ... 761
Custom User Roles ... 765
About Custom User Roles ... 765
Creating a Custom User Role ... 765
Assigning a User Role to a User Account ... 766
Assign a User Role From the Desired User Role ... 766
Assign a User Role from the Current User Role ... 767
Updating a Custom User Role ... 767
Deleting a Custom User Role ... 768
Action Permissions ... 769
Administrative Functions Permission Group ... 770
Artifact Management Permission Group ... 771
Object & Context Permission Group ... 772
Data Control Permission Group ... 775

Integrations Permissions Group ... 776
Orchestration Permissions Group ... 777
Data Exchange Permissions Group ... 777
Agentic Assistance Permissions Group ... 778
Data Access Permissions ... 779
Availability and Scope ... 779
How the Objects Permission and Object-Type Permissions Interact ... 779
Permission Conflicts ... 780
System Object Access Rules ... 780
System Object Imports ... 781
Threat Library ... 781
Feature-Specific Behavior ... 781
Interdependent Permissions ... 783
2-Step Verification ... 788
Enabling 2-Step Verification ... 788
LDAP Authentication ... 789
About LDAP Authentication ... 789
LDAP Connection Requirements ... 791
Switching LDAP Connections ... 793
Anonymous Bind ... 794
Configuring Secure LDAP ... 797
Authenticated Bind ... 799
SAML Authentication ... 804
About SAML Authentication ... 804
Configuring SAML ... 805
Setting Up LDAP Users/Groups for SAML ... 811
Adding ThreatQ as a Service Provider ... 817
ADFS 2016 ... 817
Azure AD ... 821
Google G Suite ... 824
Okta ... 829
SSL Client Certificate Authentication ... 833
About SSL Client Certificate Authentication ... 833
Requirements ... 833
Adding a User's Certificate Fingerprint - User Profile ... 835
Adding Your Certificate Fingerprint - Login Page ... 835
Using Certificate Authentication to Log In ... 836
Managing Certificate Files ... 837
Disabling SSL Client Certificate Authentication ... 837
Replacing a Certificate File ... 838
Managing Certificate Fingerprints ... 839
Updating Certificate Fingerprints ... 839
Removing Certificate Fingerprints ... 839
Troubleshooting SSL Client Certificate Authentication ... 841

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 © 2026 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 (CTI) platform designed to help organizations collect, prioritize, analyze, and operationalize threat intelligence at scale. It acts as a centralized intelligence hub that integrates data from multiple internal and external sources, enabling security teams to turn raw threat data into actionable insights.

At its core, ThreatQ ingests threat intelligence from commercial feeds, open-source intelligence, ISACs, partners, and internal tools such as SIEMs, EDRs, sandboxes, and ticketing systems. This data is normalized, correlated, and enriched to provide context around indicators, adversaries, campaigns, and incidents. Built-in scoring and prioritization mechanisms help analysts focus on the most relevant threats based on risk, confidence, and organizational relevance.

How the ThreatQ Platform Works

The ThreatQ platform is built to centralize, contextualize, and operationalize threat intelligence across the security ecosystem. By combining automated intelligence processing with analyst-driven workflows and an open integration framework, ThreatQ enables organizations to transform disparate threat data into actionable, prioritized intelligence.

Threat Library
Centralized, Contextual Intelligence Management

The Threat Library serves as the foundation of the ThreatQ platform, providing a centralized repository for threat intelligence from both internal and external sources. Intelligence is automatically normalized, enriched, scored, and prioritized based on customer-defined parameters and organizational context. By correlating data across multiple sources, ThreatQ delivers a single source of truth that reduces noise, minimizes false positives, and allows analysts to focus on the threats that pose the greatest risk.

Key Capabilities include:

- Automated, self-tuning scoring and prioritization
- Aggregated context from internal and external intelligence sources
- Support for structured and unstructured data ingestion
- Custom enrichment sources to extend existing security systems

Adaptive Workbench

Automation Combined with Human Intelligence

The Adaptive Workbench enables analysts to operationalize intelligence by combining automation with human expertise. Customer-defined configurations and integrations align ThreatQ with existing tools, processes, and workflows. Customizable enrichment, workflows, and prioritization logic streamline investigations, support continuous threat assessment, and automate key stages of the intelligence lifecycle—enabling faster, more informed detection and response.

Key Capabilities include:

- Consolidated, unified intelligence view across all sources
- Automated prioritization driven by aggregated context
- Continuous threat assessment and lifecycle management
- Push-button operations using existing tools and workflows
- User-specific watchlists for tailored intelligence monitoring

Open Exchange

Open and Extensible Integration Ecosystem

ThreatQ's Open Exchange provides an open, extensible architecture that enables seamless integration across the security stack. Organizations can ingest intelligence from a wide range of internal and external sources, leverage existing enrichment and analysis tools, and distribute prioritized intelligence to downstream systems at the right time. Standard interfaces, APIs, and SDKs allow teams to customize integrations and maximize the value of existing security investments.

Key Capabilities include:

- Flexible ingestion and export of intelligence across tools
- Integration with enrichment, detection, and response platforms
- Standard APIs and SDKs for customization and extensibility
- Support for custom and customer-built connectors

Platform Modules

ThreatQ Modules extend the functionality of the core ThreatQ application. The current ThreatQ modules available are: ThreatQ Investigations, ThreatQ Data Exchange, and ThreatQ TDR Orchestrator.

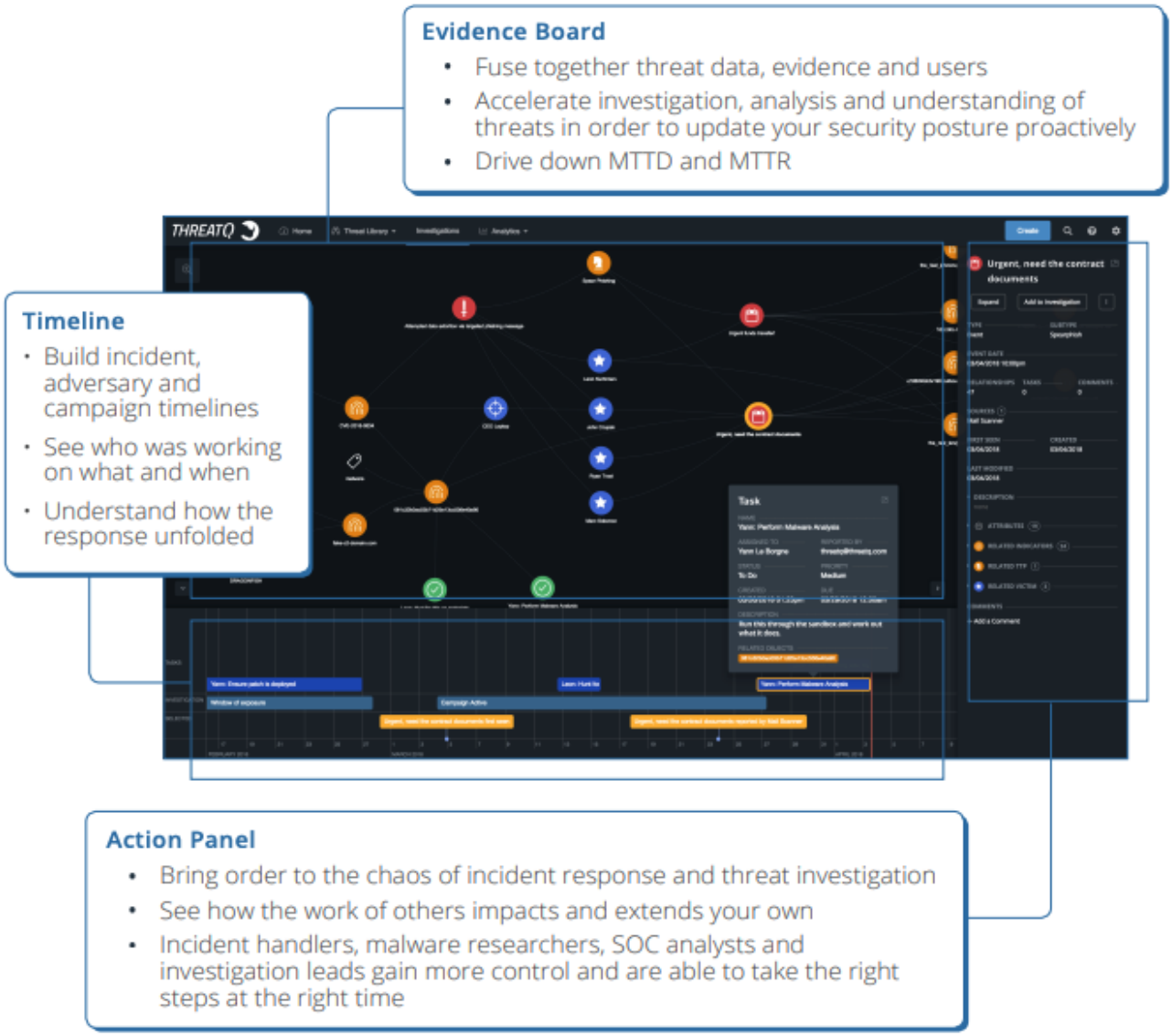
These modules are not included in default ThreatQ deployment. Contact your Technical Account Manager to add one or more modules to your deployment.

ThreatQ Investigations

ThreatQ Investigations (TQI) is a collaborative investigation and analysis module built on the ThreatQ threat intelligence platform that provides a shared, centralized environment for managing complex security investigations. Designed as a cybersecurity “situation room,” it combines visualization, documentation, and intelligence context to deliver a unified view of threats, incidents, and response activities across teams.

The module enables security teams to capture, correlate, and share knowledge throughout the investigation lifecycle, creating a single, authoritative representation of each investigation—including associated threat data, evidence, user actions, and timelines. This shared understanding improves analytical focus, reduces investigative friction, and ensures transparency into who performed which actions and when.

ThreatQ Investigations enhances collaboration and coordination across distributed teams by streamlining communication, supporting parallel analysis, and enabling analysts to test hypotheses before sharing them more broadly. Team leads can assign tasks, guide investigative efforts, and monitor progress in near real time, helping organizations reduce mean time to detect (MTTD) and mean time to respond (MTTR) while bringing greater structure and efficiency to security operations.



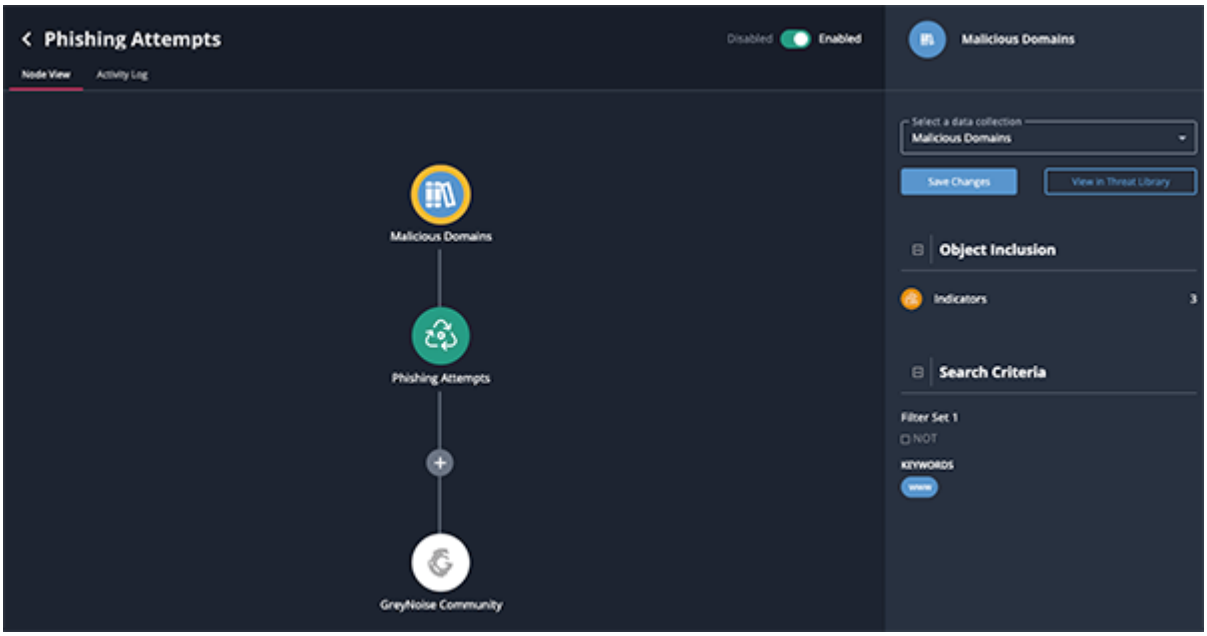
ThreatQ TDR Orchestrator

ThreatQ TDR Orchestrator (TQO) is an automation module designed to operationalize threat intelligence by enabling data-driven detection and response workflows across the security ecosystem. Built on ThreatQ data collections and ThreatQ Orchestration (TQO) actions, it simplifies configuration and ongoing maintenance while delivering more efficient, relevant, and scalable automation outcomes.

The module addresses the full automation lifecycle through a structured Initiate, Run, and Learn approach. During initiation, ThreatQ TDR Orchestrator uses curated intelligence and data-driven triggers to determine when automation should occur, ensuring actions are taken only when intelligence is relevant. In the execution phase, it orchestrates response actions using integrated third-party tools or native, data-driven playbooks defined within the ThreatQ platform. Finally, the learning phase captures

resulting data and contextual outcomes to continuously refine analytics, improve triggering logic, and enhance future automation.

By prioritizing intelligence upfront and automating selectively, ThreatQ TDR Orchestrator reduces noise, streamlines response actions, and improves overall operational efficiency. It can function alongside other playbook and orchestration capabilities within the ThreatQuotient ecosystem, enabling organizations to build adaptive, intelligence-driven automation that continuously improves detection and response effectiveness over time.

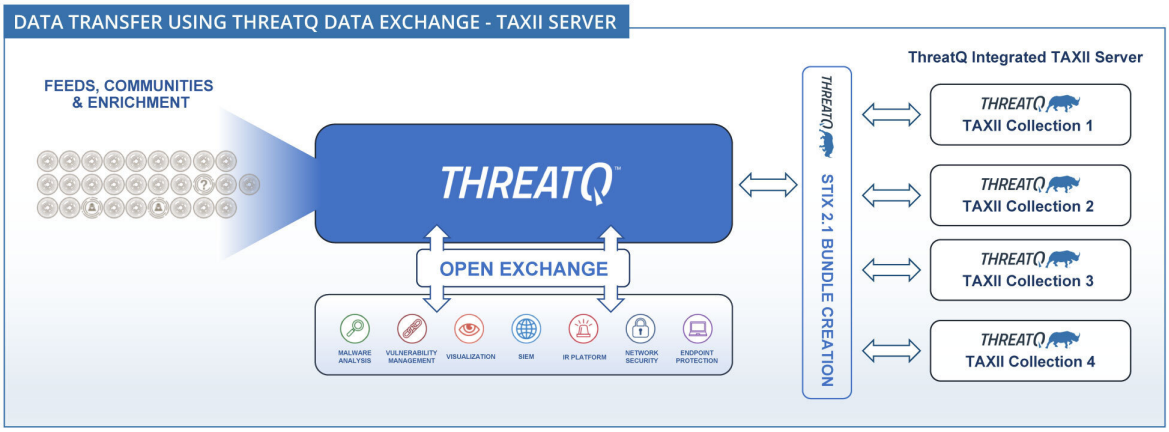


ThreatQ Data Exchange

ThreatQ Data Exchange (TQX) is a secure intelligence-sharing module that enables organizations to distribute and consume threat intelligence using industry-standard transport mechanisms. It supports both bidirectional and unidirectional sharing models, allowing teams to collaborate effectively while maintaining control over how intelligence is shared and accessed.

TQX enables bidirectional intelligence sharing through an OpenDXL data transport, allowing multiple ThreatQ instances to exchange threat intelligence in near real time. Using this approach, publisher and subscriber instances share intelligence defined within Threat Library Data Collections, ensuring that only curated and relevant data is exchanged.

For unidirectional sharing, ThreatQ Data Exchange provides a TAXII server that formats intelligence from Threat Library Data Collections into STIX and makes it available to authorized external users and organizations. The module includes built-in credential generation and access management, enabling organizations to securely control who can access shared intelligence via TAXII.



By supporting open standards and flexible sharing models, ThreatQ Data Exchange enables scalable, controlled collaboration across teams, partners, and communities, helping organizations operationalize shared threat intelligence more effectively.

Getting Started With ThreatQ

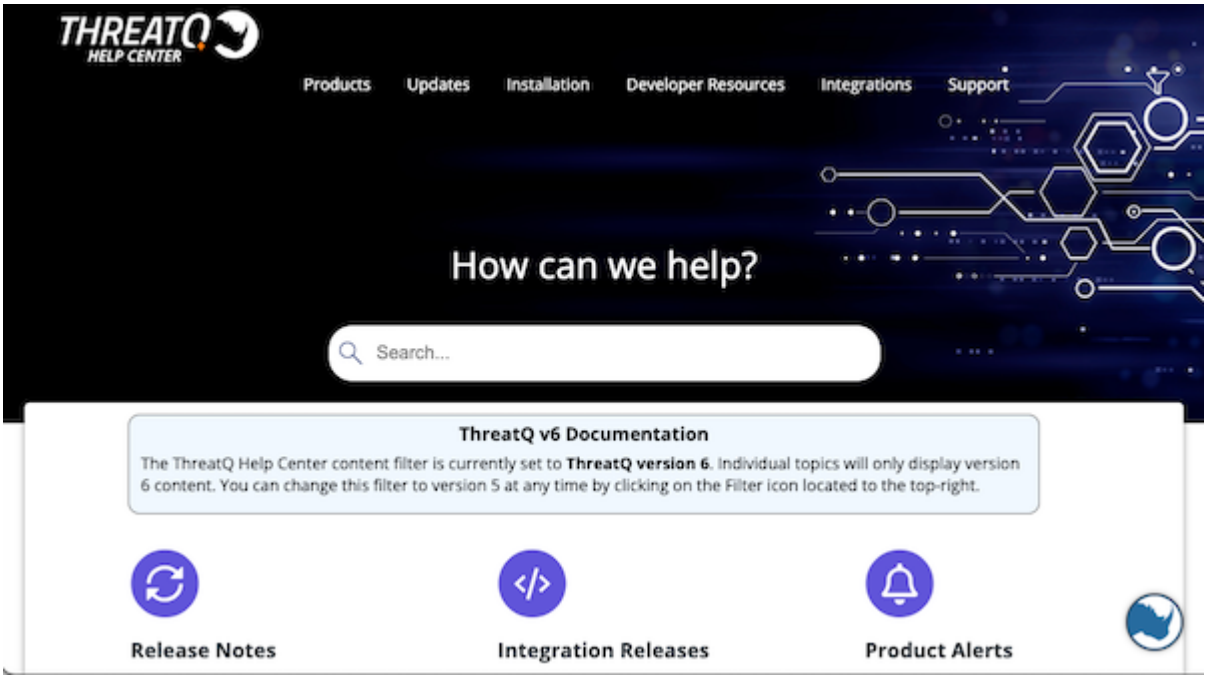
As you begin to use any new application, it is always best to think about your goals and to begin your configuration and use with these goals in mind. This Getting Started guide is a compilation of recommendations for making the most of your new ThreatQ Platform installation and laying the foundations for effective threat intel management. For more detailed and comprehensive instructions on specific tasks and processes, see the ThreatQ Help Center.

Documentation and Training Resources

ThreatQuotient provides training and documentation resources for all new and existing customers. These resources provide you with an overview of the product as a whole as well as focused content based on your role.

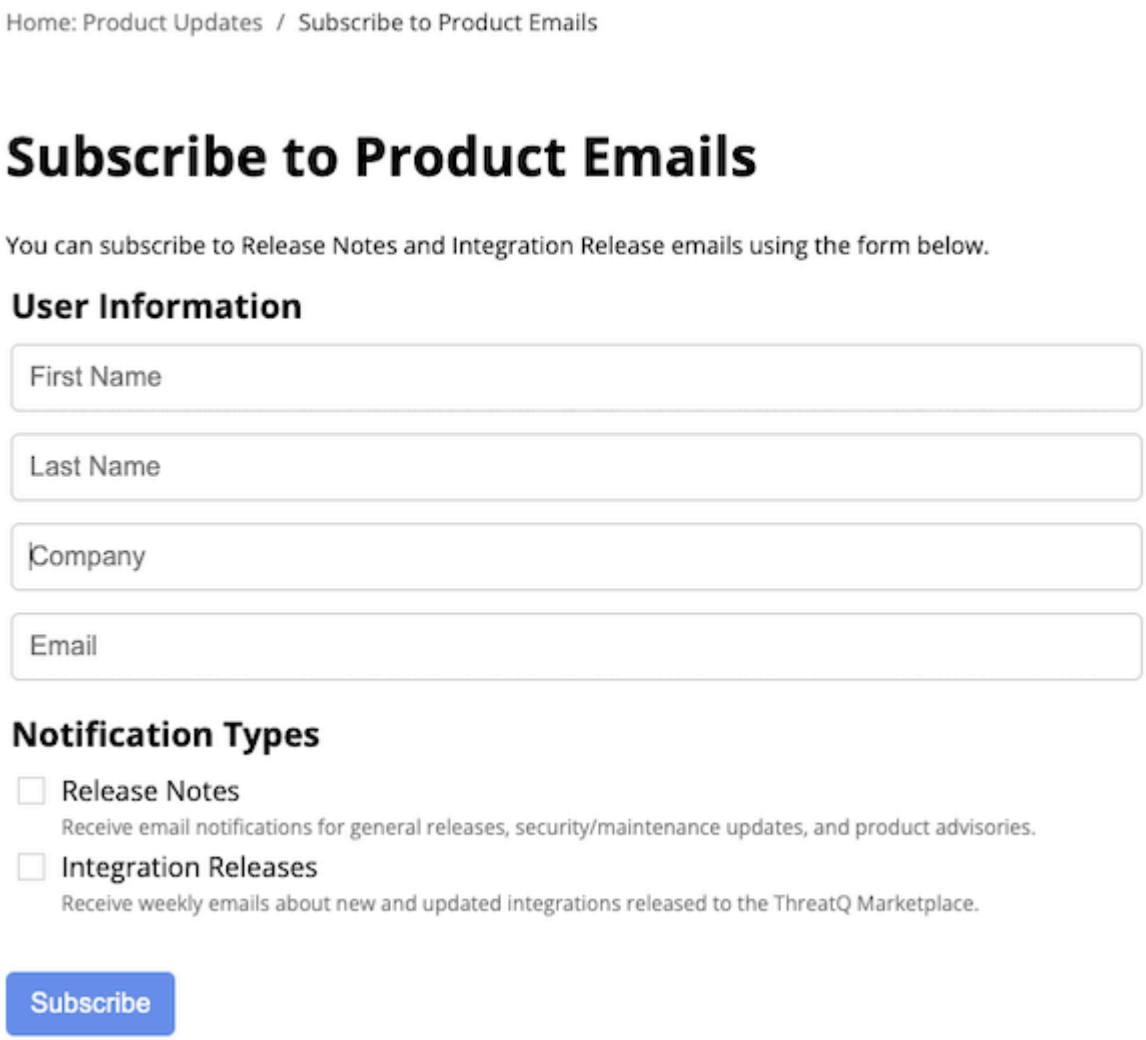
ThreatQ Documentation

The ThreatQ Help Center, accessible from the ThreatQ Help Menu, is your go-to resource for all product documentation, release notes, integration guides, and developer resources.



The topics available on this site reflect the most current version of ThreatQ. User Guides, in the form of PDFs, are available for all major ThreatQ versions on each topic.

In addition, you can stay up-to-date on ThreatQ product changes by subscribing to Product Release and Integration Release emails.



Support Resources

ThreatQuotient's dedicated Customer Support team provides the assistance you need via the communication method you prefer such as:

- Email
- Web
- Phone - 703.574.9893
- Live Chat

Our primary support hours are 12:00AM to 5:00 PM ET Monday through Friday except for holidays. And the Rhino Support AI is available to assist with product questions 24/7.

To expedite your Support interactions, please provide the following information, if available:

- **Issue Description** - Include information on actual behavior and expected behavior as well as your current application and integration versions if relevant. To focus troubleshooting, it's also helpful to report one issue per ticket.
- **Recent Changes** - Describe any recent internal/external changes to your environment such as network changes or upgrades.
- **Documentation** - Provide error logs and screenshots
- **Urgency** - Specify issue urgency and describe how it impacts your business operations including examples.
- **Point of Contact** - Identify a primary and secondary point of contact for the issue and list any communication limits (i.e. not available for calls after 6 PM).

You can also send your new feature requests to ThreatQuotient Support. For these requests, you will want to describe the business need and a use case.

Environment Specifications

One of the keys to success with any threat intelligence platform is understanding and managing your data storage needs. As such, we strongly recommend you verify that your environment meets ThreatQ's system requirements before you enter production and periodically reassess to ensure your environment keeps pace with your data needs.

ThreatQ Backups

Before you begin using ThreatQ in production, make a plan for how you will protect your data with data backups:

- **Frequency** - At a minimum, you will want to perform nightly backups as well as a backup before each upgrade.
- **Time** - You can run these backups during a scheduled maintenance window or you can run an online backup that allows your users to work in ThreatQ during the backup.

  Online backups cover your database but do not include a Solr backup.

- **Storage** - We recommend storing backups on a mounted drive or file location rather than the local file system.

In addition to planning for routine data protection, you should also document a disaster recovery plan to prepare for contingencies.

User Access

Before you add user accounts to ThreatQ, we recommend you determine, identify, and implement your desired authentication method(s):

- Local authentication
- 2-step verification
- LDAP authentication
- SAML authentication
- SSL client certificate authentication

If you plan to use local authentication with or without 2-step verification, you can proceed to create user accounts immediately. If you plan to use any of the other authentication methods listed above, we recommend you implement the authentication method and enable it in ThreatQ before creating local user accounts.

User Permissions

In keeping with the principle of least privilege (PoLP), we recommend that you set up users with the minimum access privileges required to perform their job functions. ThreatQ supports the following access levels:

- **Administrator** - Configure at least one local login with administrator privileges. And, set up an Admin or Maintenance user account to access the ThreatQ Monitoring Platform.
- **Maintenance**
- **Contributor**
- **Read-Only**

You should avoid tying ThreatQ integrations to an individual user's account. For instance, create an user account named *integrations_user* to install integrations. This future-proofs the user account against employee turnover. In addition, add a group email to the user profile so that multiple employees receive email notifications about the integration. If a login/password is required on the provider side, you might also want to specify a non-user specific account.

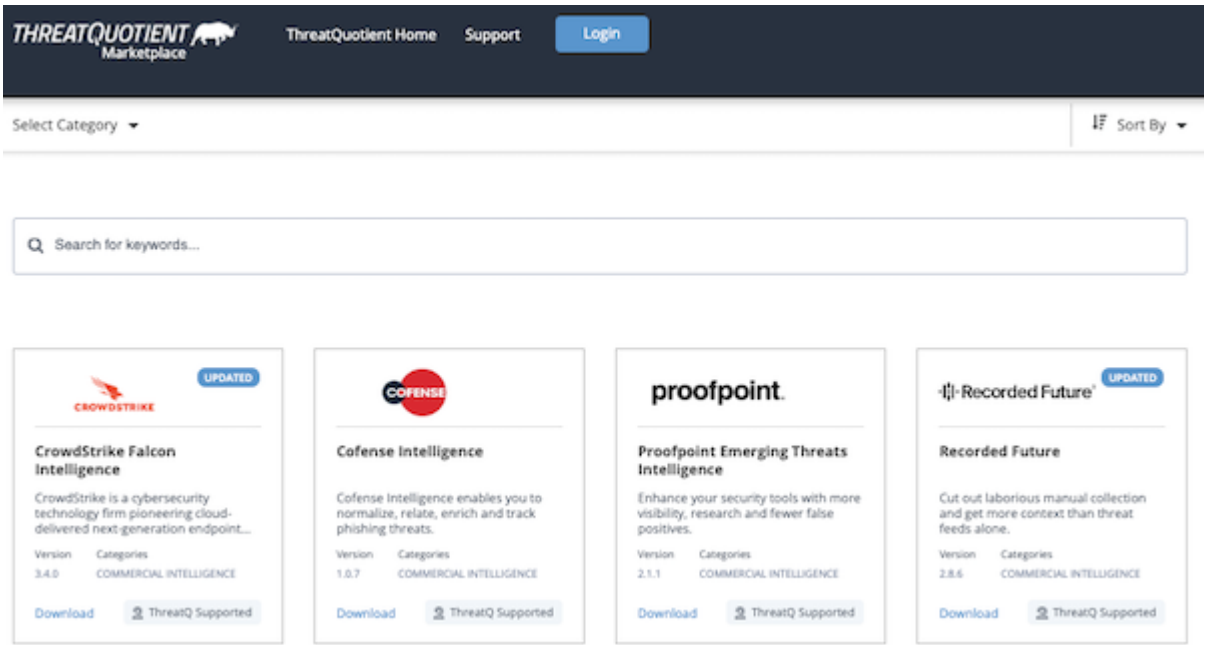
ThreatQ also allows you to control access to data collections, dashboards, and investigations by assigning sharing permissions

Adding Data

To begin using ThreatQ to manage and enrich your threat intel, you must configure integrations that allow you to ingest data into the Threat Library. ThreatQuotient recommends you configure the following open source integrations (OSINT):

- National Vulnerability Database (NVD)
- Abuse.Ch Feeds
- Malpedia CDF
- CISA Reports CDF

The ThreatQ Marketplace allows you to download these integrations and others that support the ingestion of additional data feeds.



After you download an integration, you can use the My Integrations page to install and configure it.

ThreatQ publishes frequent updates and new integrations each month. We recommend you periodically review your installed integrations and any associated filters to make sure they are providing the intel you need.

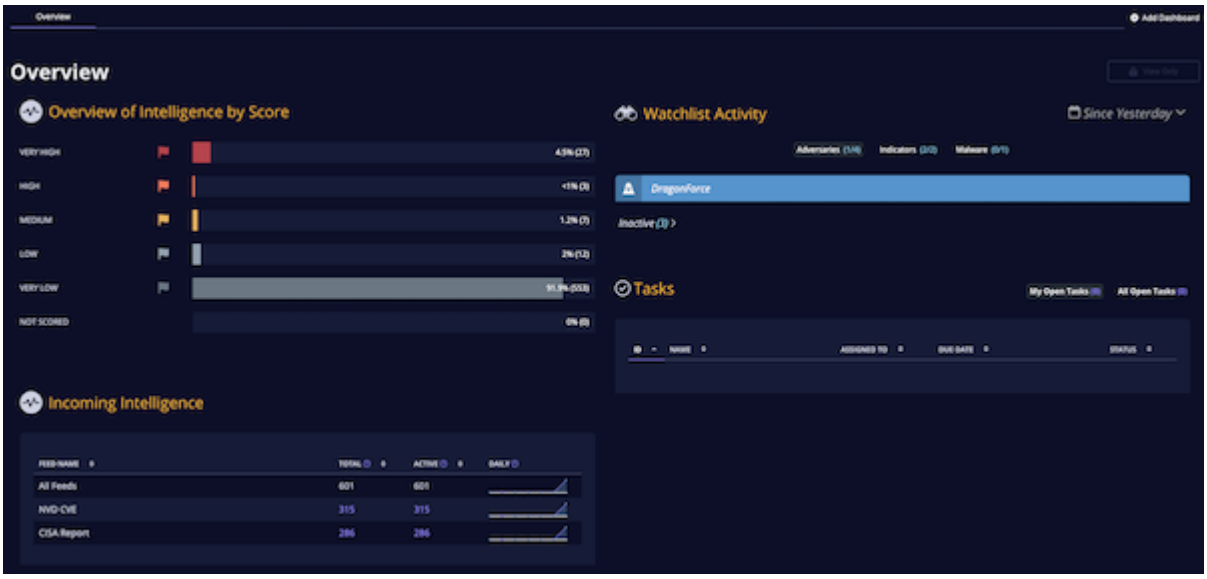
As with the ThreatQ platform, we recommend you upgrade to the most recent integration version after thorough user acceptance and soak testing.

Managing Your Data

The key to data management in ThreatQ is maintaining focus. You need to hone in on the threats that affect your organization and filter out noise. ThreatQ provides many tools for doing just that. In the early days of your implementation, we recommend you focus on Dashboards, the Threat Library, Scoring, and Threat Library Audits.

Dashboards

Each time you log into ThreatQ, your initial view is the Overview Dashboard.



This dashboard consists of four widgets, Overview of Intelligence by Score, Incoming Intelligence, Watchlist Activity, and Tasks. As a whole, these widgets give you a high-level view of your threat intel and system activity.

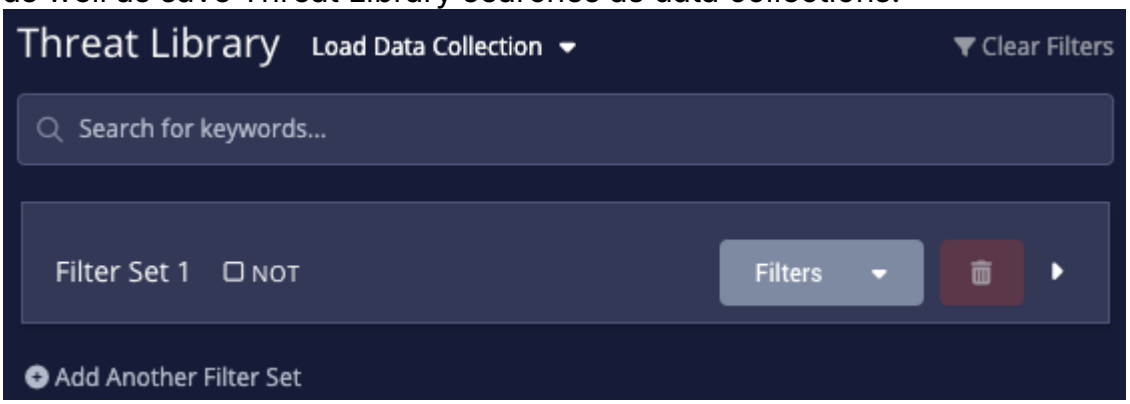
You can also create your own custom dashboards that you can share with other users. These custom dashboards pull data from saved Threat Library searches known as Data Collections.

The data is then displayed using system widgets that allow you to control the data visualization and the frequency of updates.

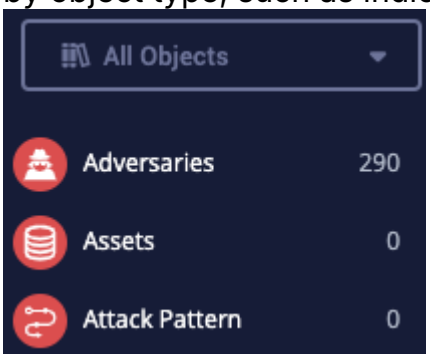
Threat Library

The Threat Library is the central hub for organizing, managing and searching your threat intel. It consists of:

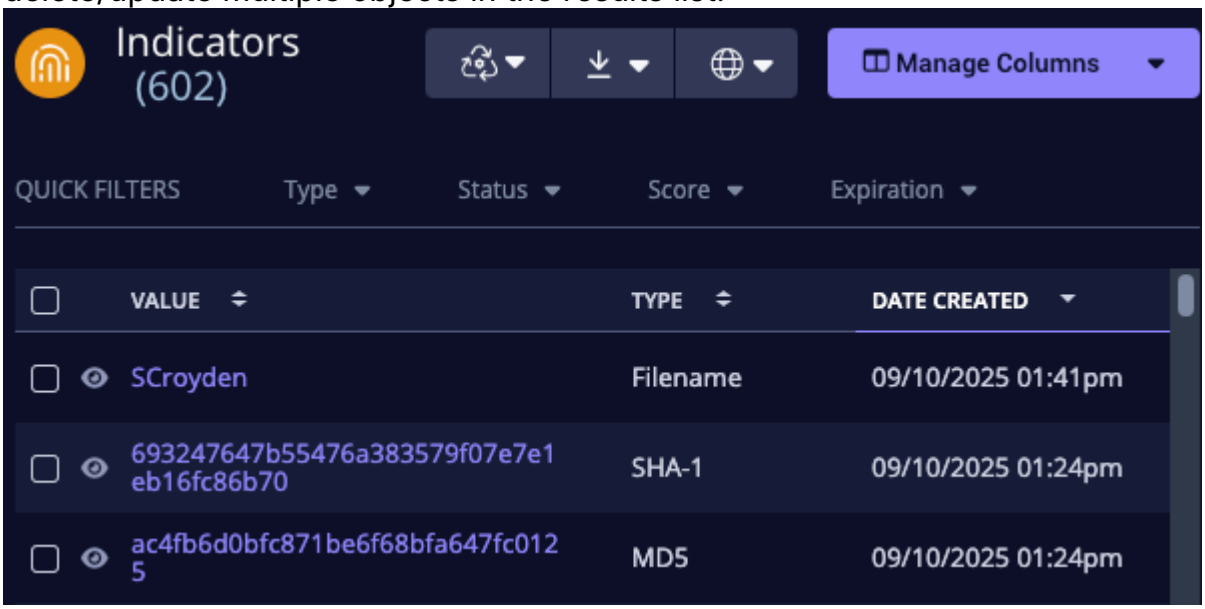
- **Search fields** - These fields allow you to filter and search your Threat Library data as well as save Threat Library searches as data collections.



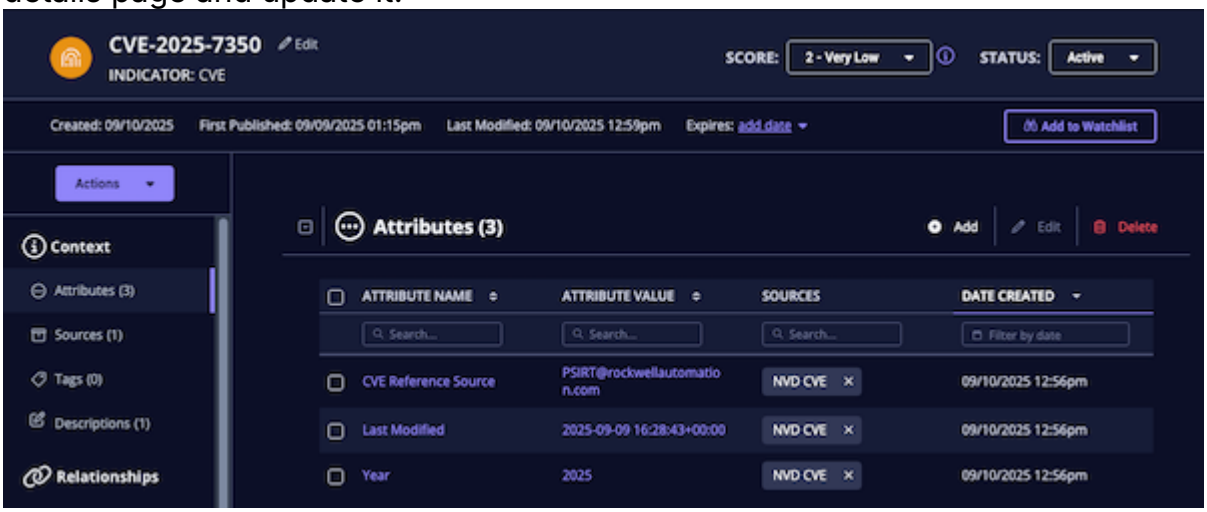
- **Object type menu** - This menu allows you to view the data in your Threat Library by object type, such as indicator, adversary, or malware.



- **Results list** - The results list displays the objects that match your current search and object type selection. You can customize this view by adding or removing columns. In addition, you can export your results to a CSV or STIX file as well as delete/update multiple objects in the results list.



- **Object details view** - You can click an item in your results list to view its object details page and update it.



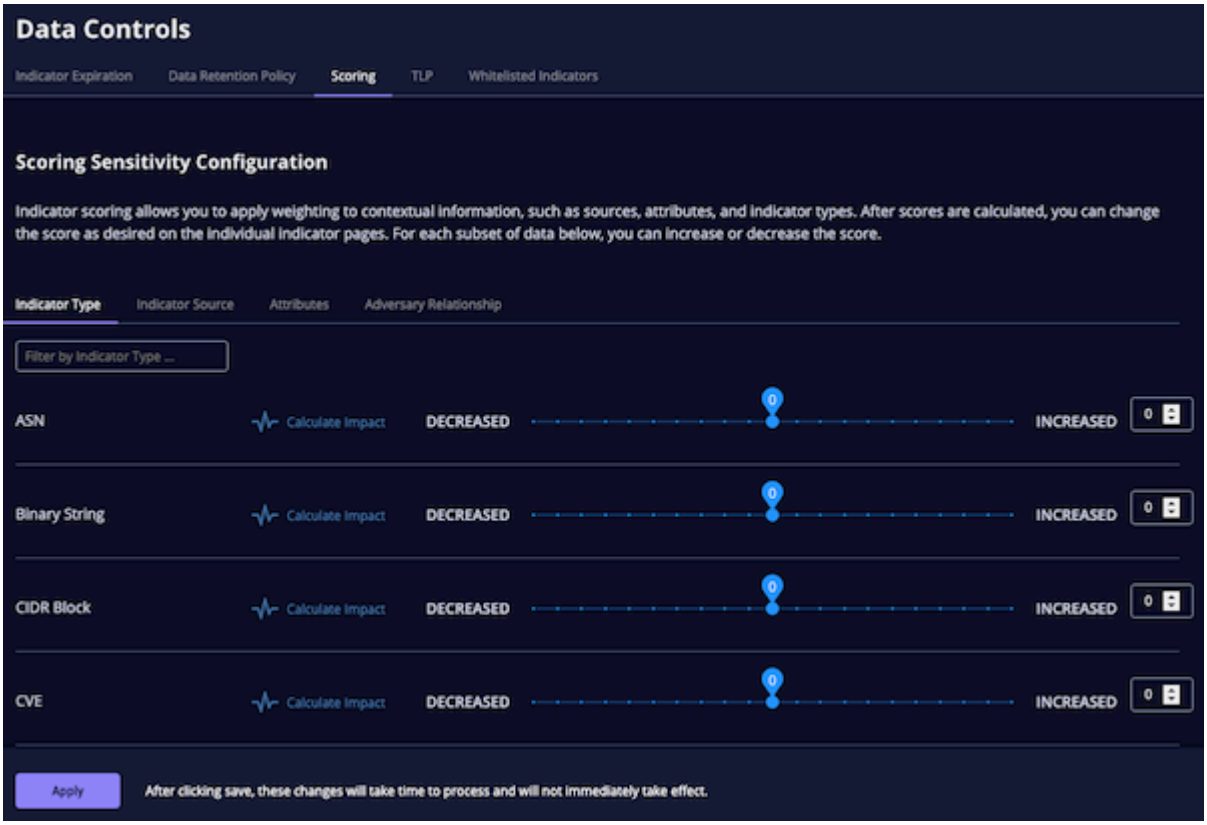
Threat Library Audits

With the volume of threat activity and intel, one of the biggest challenges customers face is filtering out noise to maintain focus. ThreatQ provides several methods for methods that support automatic and periodic Threat Library audits.

We recommend that you set up a review schedule for your system objects and use bulk delete processes and/or a data retention policy to remove noise. In addition, you can configure CDF filters to ensure the data you ingest is more relevant to your objectives and set up indicator expiration policies to automatically deprecate stale intelligence based on source, indicator type, and age.

Scoring

ThreatQ's automatic scoring system allows you to focus on relevant threat intelligence by creating scoring rules for ingested objects by indicator type, indicator source, attributes, and adversary relationships.



Optimizing scoring is an ongoing effort. You should periodically review and update your scoring to reflect changes in your industry and organization such as the addition of new intelligence feeds or tools.

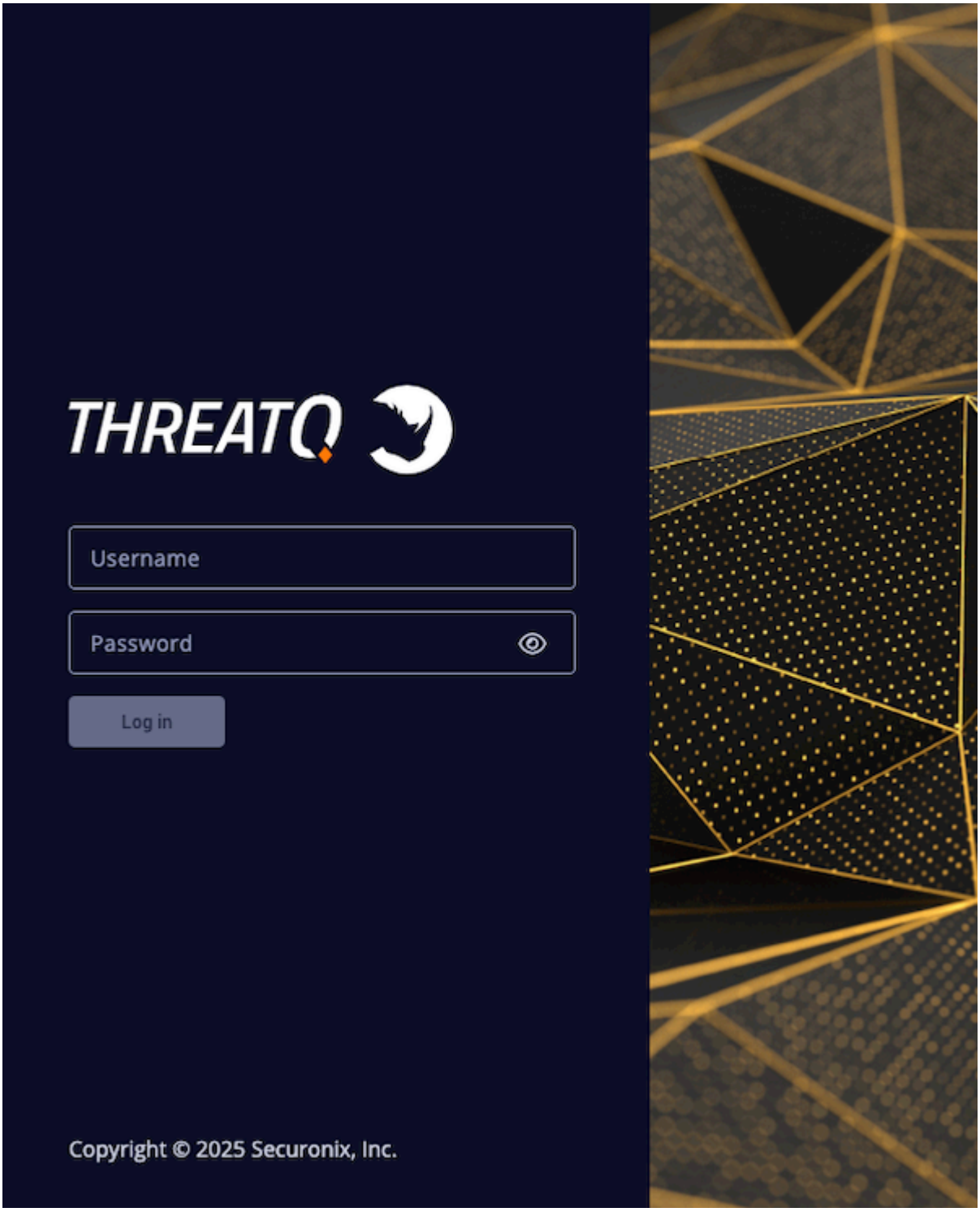
Additional Resources

Implementing a threat intelligence platform is a challenging effort. As you go through this process, ThreatQuotient Customer Support are available to assist with any questions.

Accessing the Platform

About Accessing the Platform

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



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).	• About SAML Authentication

METHOD	DESCRIPTION	REFERENCE
	SAML does not allow user role mapping for maintenance accounts. 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 agains 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.

CURRENT METHOD	NEW METHOD	DETAILS
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.
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

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative or Maintenance
Custom Role - Action Permissions: Administrative Functions - Edit User Management

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

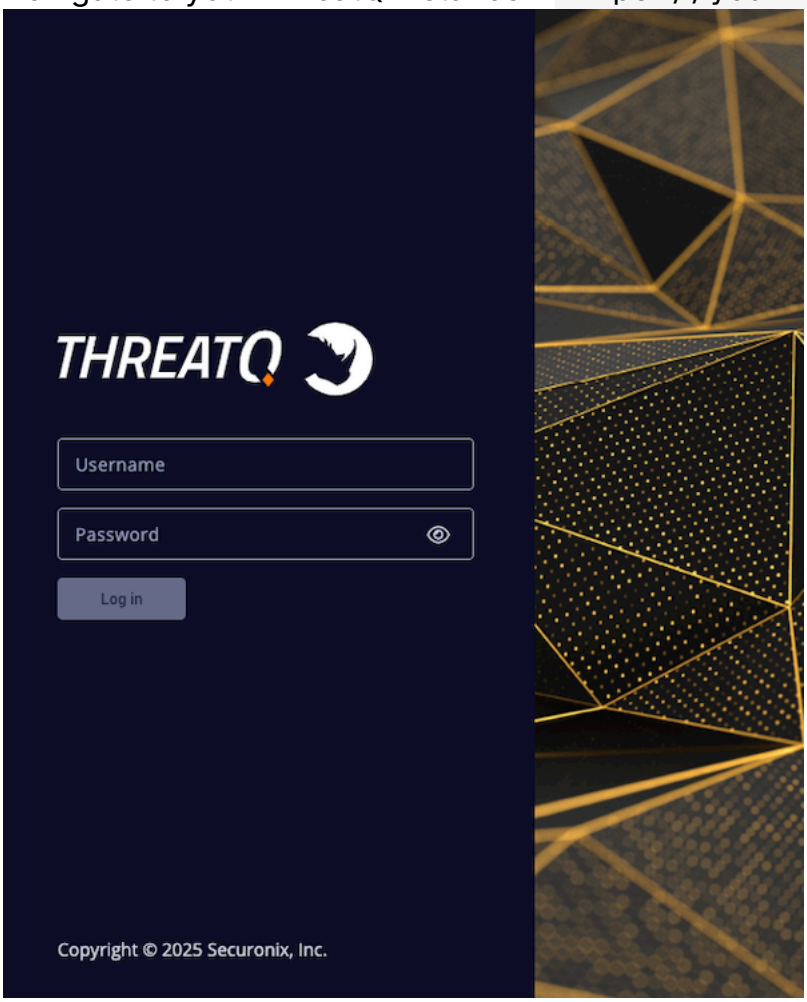
Log in steps vary based on the authentication methods enabled for your instance and/or user account.

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`.



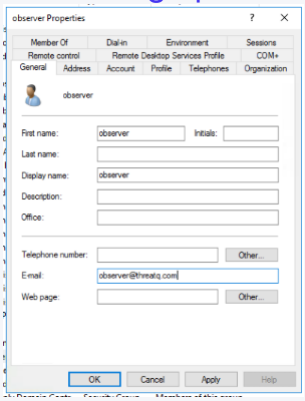
2. Enter your username (email address) and password.
3. If you have 2-step verification enabled, complete the following steps:
   - Enter your verification code from Google Authenticator.
   - Optionally, choose to **Remember this computer for 30 days**.
4. Click **Login** or **Submit**.

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.

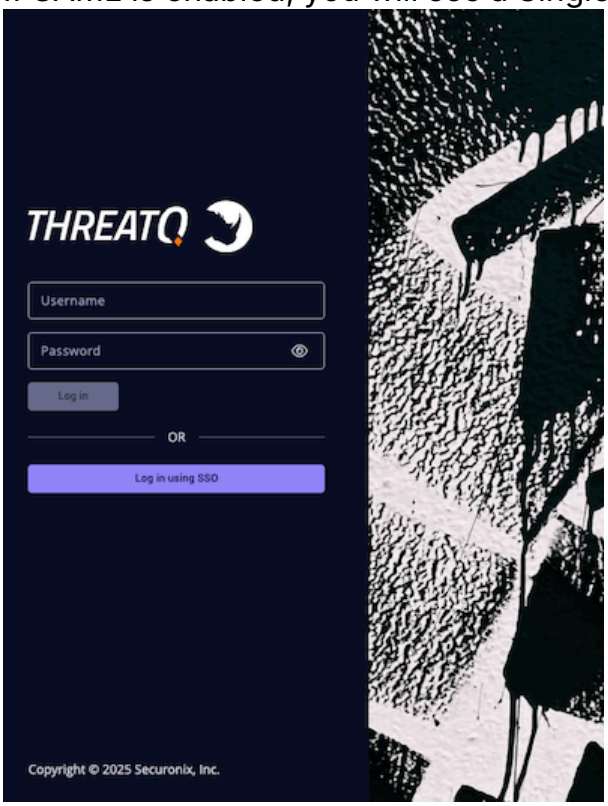
Users using SAML authentication use this log in method.

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.

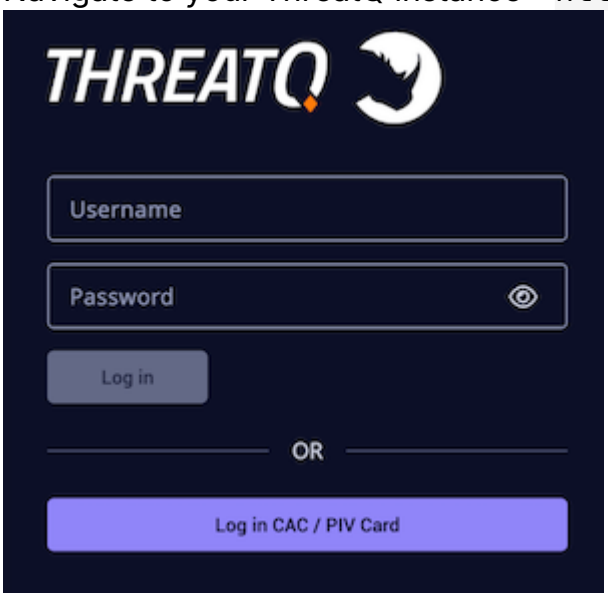
   Navigate to your third-party authenticated site to log in. Once that has been completed, you are automatically sent back to the ThreatQ instance.

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`.



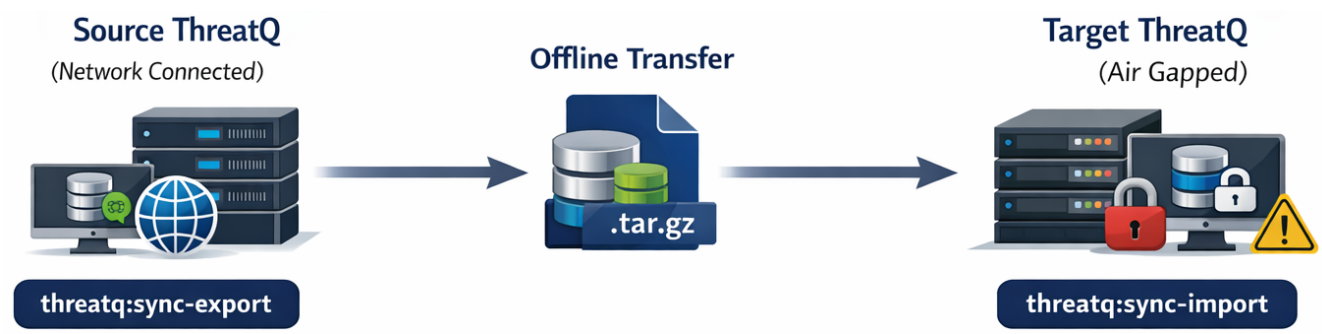
3. Click the **Log in CAC/PIV Card** button.

Air Gapped Data Sync

About Air Gapped Data Sync

Air Gapped Data Sync (AGDS) is the supported mechanism for transferring threat intelligence data from a source ThreatQ instance to a target ThreatQ instance deployed in an air-gapped environment. An air-gapped system is defined as one with no connectivity to public networks, meaning external feed ingestion and direct integrations do not occur.

AGDS operates as a two-stage process: data is first exported from the source system using the `threatq:sync-export` command, which packages selected intelligence objects, related context, metadata, and optional investigations into a portable archive, and is then imported into the air-gapped target system using the `threatq:sync-import` command.



AGDS supports controlled synchronization of selected content between environments, including updates to object names and descriptions and removals of relationships, attributes, tags, and sources, while preserving data integrity, provenance, and repeatable, auditable synchronization workflows.

> ⚠ ThreatQuotient strongly recommends contacting ThreatQ Support or a Threat Intelligence Engineer prior to implementing AGDS in production environments.

AGDS Prerequisites

Before using AGDS, ensure the following requirements are met:

- **ThreatQ Version Parity**: Source and target systems must run the same ThreatQ version.
- **Time Configuration**: All ThreatQ systems must be configured to use UTC.
- **Air Gapped Deployment**: The target system must be installed using the **ThreatQ Air Gapped Installation** process.
- **Kubernetes**: ThreatQ 6 runs on RKE2; Kubernetes must be healthy and fully operational prior to AGDS execution.

Authentication Considerations

It is important to be aware of the following authentication notes:

- **User Accounts and Permissions** - users transferred via AGDS are imported as disabled accounts and exist solely to preserve source attribution. Permissions are not transferred. Upon upgrade to ThreatQ v6.16.0, any user transferred without an account role is assigned a place holder, read-only role.
- **LDAP and SAML Authentication** - if LDAP or SAML authentication is used on the source system and user continuity is required, the same authentication method must be configured on the target before running an import.

Export Data

AGDS exports can include the following data:

DATA	DETAILS
Threat Intelligence Objects	ThreatQ default object types include: • Adversaries • Assets • Attachments (Files) Physical files for all attachments included in the date range are copied into the attachments/files directory of the data tarball. • Attack Patterns • Campaigns • Courses of Actions • Events • Exploit Targets • Identity • Incidents • Indicators • Intrusion Set • Malware • Notes • Report • Signatures • Tasks • Tool • TTPs • Vulnerability **Custom object schemas** must already exist on the target system. If an object type is included in the export data, but is not found on the target, it will be ignored.
Object Context	Tables covered for each object type include: • <object type>_attributes

DATA	DETAILS
	• <object type>_attribute_sources • <object type>_comments • <object type>_sources Not all Objects have all Object Contexts (Attributes, Attribute Sources, Comments, and Sources). Tables are only polled if they exist.
Object relationships and links	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
Metadata	Metadata included in the export: • Attributes • Clients • Connectors • Connector Categories • <Object Type> Statuses • <Object Type> Types • Other Sources • Operations • Sources

DATA	DETAILS	
	• Connector Definitions • Content Types • Groups • Investigation Priorities	• Tags • TLP • Users
Investigations and Tags	Optional and can be included in the export via the addition of a flag parameter. When Investigations are imported, ownership is automatically assigned to the most recently created admin or super user on the target system.	

Excluded or Limited Data

The following data is excluded or limited in ADGS exports:

- **Dashboards** and **Data Collections** are not transferred.
- **Connectors** and **Operations** are not installed on the target system (metadata only).
- **Custom object schemas** must already exist on the target system.
- **Permissions** and **roles** are not transferred.

Storage and Other Data Information

The follow provides additional details on object handling, transfer, and storage.

Storage (Exports)

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

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

ThreatQ 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

Exports

Executing Exports

AGDS manual exports are on-demand executions of the `threatq:sync-export` command used to create an Air Gapped Data Sync export from a source ThreatQ system without relying on automation or scheduling. They are typically used for initial data seeding, one-time transfers, testing, or controlled operational changes where administrators want full visibility into the export process and its results. In workflows that use AGDS synchronization updates, exports can also support changes that are later reflected in the air-gapped environment, including updates to object names and descriptions and removals of supported related data.

The following steps are for manually creating AGDS exports

1. Confirm that the Source and Target ThreatQ instances are running the same version of ThreatQ.
2. Determine what data do you intend to export. At a minimum, decide on the following:
   - Will this be a full export or incremental?
   - Will the export include Investigations?
   - Will the export include Soft Deleted Objects?
   - Will the export exclude large files such as malware samples?
   - How far back do you want export to go or is there a date range?

   See the Export Command Flags topic for a complete list of flags for the AGDS export command.
3. SSH into the network-connected (Source) ThreatQ instance.
4. Run the following command to check the Kubernetes pods' health:

   ```
   kubectl get pods -n threatq
   ```
5. Verify that you have enough disk space for the export in the `/var/lib/threatq/agds_transfer` directory.
6. Create the export file using the following command and Export Flags:

```
kubectl exec --namespace threatq --stdin --tty deployment/
api-schedule-run -- \
./artisan threatq:sync-export --target=<relative_path>
```

> It is highly recommended that you use the `--start-date` flag to determine how far back the export should go. Not using the `--start-date` flag will result in the export using the "Beginning of Time" date of `1970-01-01`.

7. Navigate to the export file once the process has been completed and locate the export tarball file. The file naming convention will be: `tqSync_<timestamp>.tar.gz`.

> This directory was specified in the export command via the `--target` flag and is a relative path to the default ADGS directory: `/var/lib/threatq/agds_transfer`.

8. Open the sync report and confirm that there are no errors, the object count looks correct, and that any other flag additions have been included.

```
tar -xzf tqSync_<timestamp>.tar.gz
cat sync/sync-export.txt
```

9. Transfer the export tarball file to the air-gapped target system using your organization's approved offline method.

Export Flags

AGDS export flags control what data is exported, how much data is included, and how the export behaves operationally. These flags are especially important because some of them directly influence incremental sync behavior when exports are run manually or via scheduled via cron.

> The configuration for the `--target`, `--include_investigations`, and `--include_deleted` flags are used to compute the MD5 hash that drives incremental and cron-based behavior. These flags for each run of the export command are stored in the `config_json` column of the Synchronization record.

Commonly Used Flags

The following is the most commonly used flags with the AGDS export command.

FLAG	DETAILS
`--target`	Target directory where the output file should be placed. This is a relative pathway for `/var/lib/threatq/agds_transfer` directory. The value entered for this flag will tell ThreatQ where inside that directory the export should be placed. If this flag is not used, the default location for the export will be `/var/lib/threatq/agds_transfer/tmp`. The following example will place the export tarball file in `/var/lib/threatq/agds_transfer/export/runs` directory. `kubectl exec --namespace threatq --stdin --tty deployment/api-schedule-run -- ./artisan threatq:sync-export --target=export/runs`
`--start-date`	The start date for data selection. The date format should be: `YYYY-MM-DD HH:MM:SS`. The default setting is `1970-01-01 00:00:00` which will be used if the start date flag is not included.

FLAG	DETAILS

	The start date flag can use either the `touched_at` or `updated_at` column based on the object type.
	
	`touched_at` is used for Adversaries, Attachments, Events, Indicators, Signatures, Custom Objects.
	
	`updated_at` is used for Investigations, Tasks, Object Links, Tagged Objects, Spearphish.
	
	The following is an example of an export with a start date of June 1, 2025.
	
	`kubectl exec --namespace threatq --stdin --tty deployment/api-schedule-run -- ./artisan threatq:sync-export --target=export/runs --start-date="2025-06-01 00:00:00"`
	
	The following is an example of an export with a date range of January 1, 2025 - November 25, 2025.
	
	`kubectl exec --namespace threatq --stdin --tty deployment/api-schedule-run -- ./artisan threatq:sync-export --target=export/runs --start-date="2025-01-01 00:00:00" --end-date="2025-11-25 00:00:00"`

`--end-date`	Specifies the end date for data selection and applies only to objects, not object context or object links. The date format should be: `YYYY-MM-DD HH:MM:SS`. The following is an example of an export with the default start date, January 1, 1970, (since the `--start-date flag` is not used) and an end date of November 1, 2021. `kubectl exec --namespace threatq --stdin --tty deployment/api-schedule-run -- ./artisan`

FLAG	DETAILS
	`threatq:sync-export --target=export/runs --end-date="2021-11-01 00:00:00"`
`--include-deleted`	Determines whether objects that have been soft-deleted are included in the result set. Options are `Y` for **Yes** or `N` for **No**. The default setting for this flag is **No** so the flag is only required if you want to include soft-deleted objects. The following is an example of an export that includes soft-deleted files. `kubectl exec --namespace threatq --stdin --tty deployment/api-schedule-run -- ./artisan threatq:sync-export --target=export/runs --include-investigations=Y`
`--include-investigations`	Determines whether ThreatQ Investigations and Tasks are included in the result set. Options are `Y` for **Yes** or `N` for **No**. The default setting for this flag is **No** so the flag is only required if you want to include ThreatQ Investigations and Tasks. The following is an example of an export that includes ThreatQ Investigations and Tasks. `kubectl exec --namespace threatq --stdin --tty deployment/api-schedule-run -- ./artisan threatq:sync-export --target=export/runs --include-investigations=N`

Other AGDS Export Flags

FLAG	DETAILS
`--ignore-`	Defines a comma-delimited list of ThreatQ File Types for which physical files stored on the source ThreatQ installation should not be

FLAG	DETAILS
`file-types`	transferred to the target air gapped ThreatQ installation. Database records are still included in the export tarball. The following is an example of an export that ignores Malware Analysis Report and Malware Sample types. `kubectl exec --namespace threatq --stdin --tty deployment/api-schedule-run -- ./artisan threatq:sync-export --target=export/runs --ignore-file-types="Malware Analysis Report,Malware Sample"`
`--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. The following is an example of an export that will include all related data for objects with the source of `Black Source`. `kubectl exec --namespace threatq --stdin --tty deployment/api-schedule-run -- ./artisan threatq:sync-export --target=export/runs --sources="Black Source" --include-all-relationships`
`--initial-start-date`	Controls the starting point for data selection during the first run of an AGDS export, particularly in large or long-running environments. It explicitly defines the earliest date from which data should be exported, allowing administrators to avoid exporting the entire historical dataset ("beginning of time") in a single run. This flag is most commonly used when staging large data migrations in multiple, incremental export windows. See the CRON topic for more details. Unlike the `--start-date`, the `--initial-start-date` value is recorded separately in the synchronization record and does not participate in cron hash matching, which prevents it from interfering with ongoing scheduled or incremental exports. After the initial run

FLAG	DETAILS
	completes, subsequent exports can rely on the standard incremental logic (based on prior run timestamps) without needing to reuse the `--initial-start-date` flag. In this example, the initial start date is set to January 1, 2016. `kubectl exec --namespace threatq --stdin --tty deployment/api-schedule-run -- ./artisan threatq:sync-export --initial-start-date="2016-01-01 00:00:00" --target=export/runs --end-date="2024-01-01 00:00:00`
`--memory-limit`	Sets the PHP memory limit in megabytes or gigabytes. The default value is 2G. The following is an example of the export command that sets the PHP memory limit to 4GB. `kubectl exec --namespace threatq --stdin --tty deployment/api-schedule-run -- ./artisan threatq:sync-export --target=export/runs --memory-limit=4G`
`--meta-only`	Tells the export to only pull meta data objects (Attributes, Sources, Object Statuses etc.) from the system. The following export command example only pulls meta data objects. `kubectl exec --namespace threatq --stdin --tty deployment/api-schedule-run -- ./artisan threatq:sync-export --target=export/runs --meta-only`
`--object-limit`	Sets the limit on the number of objects selected at a time. The default value is 50,000. ThreatQuotient recommends that you set the limit to a number smaller than the default value on boxes with very large data sets.

FLAG	DETAILS
	The following is an example of setting object limit to 10,000 for an export. `kubectl exec --namespace threatq --stdin --tty deployment/api-schedule-run -- ./artisan threatq:sync-export --target=export/runs --object-limit=10000`

`--sources`	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.
	The following is an example of filtering down the export to objects with the Abyss source.
	`kubectl exec --namespace threatq --stdin --tty deployment/api-schedule-run -- ./artisan threatq:sync-export --target=export/runs --sources="Abyss"`
	Existing CRON Runs: use the `initial-start-date` flag to avoid pulling all historical data.
	`kubectl exec --namespace threatq --stdin --tty deployment/api-schedule-run -- ./artisan threatq:sync-export --target=export/runs --sources="Abyss" --initial-start-date="2018-11-01 00:00:00"`

Scheduled Exports

You can utilize CRON to run recurring, incremental Air Gapped Data Sync exports from a network-connected source system to support ongoing updates of an air-gapped ThreatQ deployment. Instead of requiring administrators to manually manage dates or track changes, cron for AGDS relies on ThreatQ's internal synchronization records to determine what data should be exported on each run.

When an export is executed via cron, ThreatQ calculates a configuration hash based on a fixed set of command-line flags (such as `--target`, `--include-deleted`, and `--include-investigations`). If a previous successful export exists with the same hash, ThreatQ automatically uses the start time of the last completed run as the starting point for the next export. This allows cron-based exports to behave incrementally, pulling only new or updated data since the last run. If the hash changes, ThreatQ treats the export as a new sequence and resets the incremental cursor.

CRON jobs must be run by a non-root user that installed RKE2.

1. Determine which, if any, CRON configuration flags to use. The CRON configuration flags listed below must be the same for every run, but they only need to be specified if **different** from the defaults.

OPTION	DETAILS	DEFAULT	FLAG	EXAMPLE
Target Directory	The directory where the export tarball file will be placed.	/tmp	`--target`	`--target=export/runs`
Include ThreatQ Investigations and Tasks	Include ThreatQ Investigations and Tasks in the export tarball file.	N	`--include-investigations`	`--include-investigations=Y`
Include Deleted Objects	Include soft-deleted objects in the export tarball file.	N	`--include-deleted`	`--include-deleted=Y`

The example command below includes all three flags as they differ from the default settings

```
kubectl exec --namespace threatq --stdin --tty deployment/
api-schedule-run -- ./artisan threatq:sync-export --
target=export/runs --include-deleted=Y --include-
investigations=Y
```

2. Retrieve the DB password:

```
kubectl get secret mariadb-root --output go-template='{{range
$k,$v := .data}}{{printf " %s: " $k}}{{if not $v}}{{$v}}
{{else}}{{$v | base64decode}}{{end}}{{"\n"}}{{end}}' -n
threatq
```

3. Run the initial export command along with any Export Command Flags needed:

```
kubectl exec --namespace threatq --stdin --tty deployment/
api-schedule-run -- ./artisan threatq:sync-export --
target=export/runs --include-deleted=Y --include-
investigations=Y
```

4. Enter the DB password when prompted.
5. Set up CRON for the non-root user:

```
sudo crontab -u <non-root_user_that_installed_RKE2> -e
```

6. Enter the following command while replacing target placeholder as well as adding any other export flags you need. Remove the `--include-deleted` and `--include-investigations` flags if you do not want to include soft-deleted files and investigations.

```
/var/lib/rancher/rke2/bin/kubectl exec --namespace threatq --
stdin --tty deployment/api-schedule-run -- ./artisan
threatq:sync-export --target=<relative_path> --include-
deleted=Y --include-investigations=Y
```

You can add the following to the end of the command to add logging for a chronological execution history: `>> /var/log/threatq/agds-export.log 2>&1`. The `>>` appends output (does not overwrite), the `2>&1` captures errors (stderr) and normal output (stdout).

Example:

```
/var/lib/rancher/rke2/bin/kubectl exec --namespace threatq --
stdin --tty deployment/api-schedule-run -- ./artisan
threatq:sync-export --target=export/runs --include-deleted=Y
--include-investigations=Y >> /var/log/threatq/agds-
export.log 2>&1
```

Steps for Larger Data Sets

Attempting to perform a full run on larger data sets can result in decrease in system performance.

ThreatQuotient recommends that you use the `--end-date` flag to specify an upper limit on the date range pulled. Multiple runs will be necessary to process all data up to the current date. Once the current date has been reached, the `--end-date` flag is no longer necessary.

Steps for Larger Data Sets Starting at the Beginning of Time

The following example does not use the start-date flag so the command will use the start date default: `1970-01-01 00:00:00`.

```
kubectl exec --namespace threatq --stdin --tty deployment/api-
schedule-run -- ./artisan threatq:sync-export --target=export/
runs --include-investigations=Y --end-date="2017-01-01 00:00:00"
```

Steps for Larger Data Sets Starting at a Specific Start Date

The `--initial-start-date` flag be used for the first run if only a subset of data needs to be processed up to the current date.

```
kubectl exec --namespace threatq --stdin --tty deployment/api-
schedule-run -- ./artisan threatq:sync-export --initial-start-
date="2016-01-01 00:00:00" --target=export/runs --include-
investigations=Y --end-date="2017-01-01 00:00:00"
```

The `--end-date option` flag should be used for each additional run until current date has been reached.

```
kubectl exec --namespace threatq --stdin --tty deployment/api-
schedule-run -- ./artisan threatq:sync-export --target=export/
runs --include-investigations=Y --end-date="2017-01-01 00:00:00"
```

Imports

Executing the AGDS Import Command

The AGDS import process is the write-side operation of ThreatQ's Air Gapped Data Sync (AGDS) service and is responsible for safely applying exported threat intelligence data from a network-connected source system into an air-gapped ThreatQ environment. It is designed to preserve data integrity, avoid duplication, and ensure that incremental updates can be applied repeatedly without corrupting the target system.

At a high level, the import process begins when an operator runs the threatq:sync-import command on the air-gapped target system and points it to an export tarball generated by threatq:sync-export. Before any data is written, ThreatQ validates the export package and prepares the database by using internal synchronization hashes (sync_hash) to uniquely identify records. This allows the import to determine whether each incoming object already exists on the target system or must be created for the first time.

During execution, ThreatQ extracts the CSV dump files from the tarball and loads them into temporary synchronization tables that mirror the structure of the production tables but exclude indexes for performance. Once all data for a table is loaded, ThreatQ performs integrity checks and matches records using their sync_hash values. Existing objects are updated, and supported related data such as relationships, attributes, tags, and sources can also be removed when the source system no longer includes them, while new objects are inserted.

Special handling is applied to related data such as object context, tags, links, attachments, and investigations. Relationships are re-established after object IDs are resolved, ensuring referential integrity even when IDs differ between source and target systems. If physical files were intentionally excluded during export, placeholder files are created on the target system so database references remain valid. Users transferred as part of the import are created in a disabled state and exist only to preserve source attribution, and any imported Investigations are assigned to the most recently created admin or super user on the target system.

When the import completes, ThreatQ finalizes the run by removing all temporary sync tables and writing a synchronization record to the synchronizations database table. This record includes the configuration used, object counts, performance metrics, and timestamps, providing a complete audit trail. If the import fails, no incremental state is advanced and the operation can be safely rerun without risking data duplication. In practice, this design allows organizations to repeatedly and reliably update air-gapped ThreatQ environments while maintaining strict security and operational controls.

Executing the AGDS Import Command

You **must** run the `threatq:fill-sync-hash-column` command prior to running the `threatq:sync-import` command on the air gapped ThreatQ installation. This command prepares the database of an air gapped installation to run the `threatq:sync-import` command.

1. SSH to your target ThreatQ installation.
2. Put the ThreatQ platform into maintenance mode:

```
kubectl exec --namespace threatq --stdin --tty deployment/
api-schedule-run -- ./artisan down
```

3. Run the fill-synch-hash command:

```
kubectl exec --namespace threatq --stdin --tty deployment/
api-schedule-run -- ./artisan threatq:fill-sync-hash-column
```

4. Run the import command:

```
kubectl exec --namespace threatq --stdin --tty deployment/
api-schedule-run -- ./artisan threatq:sync-import --
file=<relative_path/zip_file.tar.gz>
```

The `-file` flag is required when running the import command. This flag specifies the relative path to the export tarball within the default `/var/lib/threatq/agds_transfer` directory. See the Import Command Flags topic for additional information about this flag and other supported import options.

5. Bring ThreatQ out of maintenance mode:

```
kubectl exec --namespace threatq --stdin --tty deployment/
api-schedule-run -- ./artisan up
```

Import Command Flags

AGDS import flags control how exported data is applied to an air-gapped ThreatQ system. They influence data integrity, performance, and overwrite behavior, but do not affect incremental tracking, which is handled entirely on the export side. They are designed to balance performance, data fidelity, and overwrite behavior while maintaining a safe, repeatable import process.

> All flags for the `threatq:sync-import` command, other than the `--file` flag, will use the default value unless otherwise defined by the user.

FLAG	EXPLANATION
`--file`	**This flag is required**. The flag specifies the relative path within the default `/var/lib/threatq/agds_transfer` directory that the export tarball is imported into. The following example will import the export tarball file to `/var/lib/threatq/agds_transfer/import/runs` directory. `kubectl exec --namespace threatq --stdin --tty deployment/api-schedule-run -- ./artisan threatq:sync-import --file=import/runs/tqSync-19-01-16-1547660837-8345.tar.gz`
`--keep-created-at`	This flag controls how `created_at` timestamps are handled for imported objects and uses a Yes/No argument. The default value is Y (Yes) and preserves the earliest created_at time stamp between the source and target ThreatQ instances. Setting the flag to N (No) sets the `created_at` timestamp to the current time for the imported objects. As the default value for the flag is Y, you will only need to include the flag in import commands if you do not want to use the earliest time stamp for imported objects. The command below will use the current date and time for the `created_at` time stamp for imported objects. `kubectl exec --namespace threatq --stdin --tty deployment/api-schedule-run -- ./artisan threatq:sync-import --keep-created-at=N --`

FLAG	EXPLANATION
	`file=import/runs/ tqSync-19-01-16-1547660837-8345.tar.gz`
`--object-limit`	This flag sets the limit for the number of objects updated or inserted at a time. When using this flag, the size of the data sets on both source and target ThreatQ installations should be taken into account. While increasing this value will result in faster imports on larger systems setting it could also hinder performance. The default value is 1000. The example below sets the object limit for the import command to 5000. `kubectl exec --namespace threatq --stdin --tty deployment/api-schedule-run -- ./artisan threatq:sync-import --object-limit=50000 --file=import/runs/ tqSync-19-01-16-1547660837-8345.tar.gz`
`--memory-limit`	This flag sets the PHP memory limit in megabytes or gigabytes. The default value is 2g. Increasing this value is helpful when processing large investigations or the import process originally failed due to memory exhaustion. The example below sets the new memory limit to 4 gibabytes. `kubectl exec --namespace threatq --stdin --tty deployment/api-schedule-run -- ./artisan threatq:sync-import --memory-limit=4G --file=import/runs/tqSync-19-01-16-1547660837-8345.tar.gz`
`--override-description`	This flag determines if descriptions on existing objects on the target ThreatQ installation are be updated using a Yes/No argument. The default value is Yes. This flag is useful if you want to preserve analyst-curated descriptions on the target system.

FLAG	EXPLANATION
	The default value is If an existing object has a NULL description, it will be updated regardless of the use of this flag.

The example below will result in the preserving the existing descriptions when importing.

```
kubectl exec --namespace threatq --stdin --tty
deployment/api-schedule-run -- ./artisan
threatq:sync-import --override-description=N --
file=import/runs/
tqSync-19-01-16-1547660837-8345.tar.gz
```

Reports, Logs, Synchronization

You can review AGDS import and export process details from the following:

- Console Output
- Sync Export Report
- Sync Import Report
- Cron Logs
- Synchronization Database
- Application Logs

Console Output

You can view live statistics of the AGDS process when performing a on-demand export or import. The information will be appear in the same terminal window that you used to enter the command.

The output includes details such as:

- Progress and Phase Transitions
- Object Counts
- File Write Status
- Fatal Errors regarding memory, permissions, and disk.

Sync Export Report

The Sync Export report is generated at the end of the export process and is bundled within the export tarball file. The file name is `sync-export.txt` and is located within the `sync` directory of the tarball.

The report provides information on:

- Flags used
- Object counts
- Files created
- Execution time

Sync Import Report

The Sync Import Report is generated at the end of the import process and uses the following naming format: `<tqSync_filename>-sync.import.txt`.

The report provides information on:

- Flags used
- Object counts
- Files created
- Execution time

AGDS Cron Logs (Export)

Cron-based AGDS logs are only available if cron logging has been enabled. You can enable cron logging by adding the following to the cron command:

```
>> /var/log/threatq/agds-export.log 2>&1
```

Example

```
/var/lib/rancher/rke2/bin/kubectl exec --namespace threatq --
stdin --tty deployment/api-schedule-run -- ./artisan
threatq:sync-export --target=export/runs --include-deleted=Y --
include-investigations=Y >> /var/log/threatq/agds-export.log 2>&1
```

Using the command example above, the logs will be located at: `/var/log/threatq/agds-export.log`.

The AGDS logs allows you to check for the following:

- Command Start and End timestamps
- Run Failures (you should focus on repeated failures)
- Permission or kubectl errors
- Sudden terminations

Recording Handling and Synchronization Tables

The record handling for Air Gapped Data Sync (AGDS) is managed through a dedicated database table called synchronizations, which serves as the authoritative system of record for all AGDS export and import operations. Every time an AGDS export or import

is initiated, ThreatQ creates a synchronization record that tracks the lifecycle, configuration, and outcome of that run.

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

The synchronization table columns are as follows:

COLUMN	DETAILS
`id`	The auto-incremented id for the Synchronization record.
`type`	The Synchronization direction - either **export** or **import**.
`started_at`	The date and time the command run was started.
`finished_at`	The date and time the command run completed. This column will read as `NULL` until the sync action (export or import) has been 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`	A unique identifier for a command run. The Synchronization record hash column is automatically calculated as an MD5 of the `config_json` column on record creation.
`created_at`	The date and time the Synchronization record was created.

COLUMN	DETAILS
`updated_at`	The date and time the Synchronization record was updated.

Application Logs

You can look for issues not present in the console view or AGDS reports in the pod's logs such as:

- Database errors
- PHP exceptions
- Serialization failures
- Sync table errors

To check application logs for AGDS:

1. Access the API pod:

```
kubectl exec -n threatq -it deployment/api-schedule-run --
bash
```

2. Navigate to the logs directory:

```
cd /var/lib/threatq/logs
```

3. Run the following command to show the most recent events (last 200 lines of the log):

```
tail -n 200 laravel.log
```

Installing an Air Gapped ThreatQ Instance

ThreatQuotient supports the deployment of ThreatQ version 6 on an air gapped device. An air gapped device can be defined as a device situated in a location with no or limited public network access.

The standard steps for installing ThreatQ require network access to the ThreatQ repositories to download and install the platform. In an air gapped instance, where the device cannot make that connection, you must download required files from a network-connected device and then transfer those files to the targeted air gapped device. The process is the same when it comes to upgrading an air gapped device.

This document will provide you with the requirements, recommended settings, and the steps for installing a new instance of ThreatQ version 6 on a device in an air gapped environment.

> ThreatQuotient recommends you install the most recent version of ThreatQ 6x for your upgrade.

Operating System and Kubernetes Distribution Maintenance

After upgrading to ThreatQ 6x, customers are responsible for maintaining their RHEL or Ubuntu operating system as well as the RKE2 Kubernetes distribution.
ThreatQ currently supports RHEL 8.10, 9.4, or 9.6, Ubuntu 22.04 LTS, and the latest, stable RKE2 version. Before updating to a different version, please contact ThreatQuotient Support to confirm compatibility.

Supported Hardening Standards by Operating System

ThreatQ v6 supports the following hardening standards for RHEL 8.10, RHEL 9.4, RHEL 9.6, and Ubuntu 22.04 LTS:

	RHEL 8.10	RHEL 9.4	RHEL 9.6	UBUNTU 22.04 LTS
CIS Level 1	X	✓	X	X
CIS Level 2	X	✓	X	X
STIG	✓	✓	✓	X

See the ThreatQ v6 RHEL v9 Hardening guide for more information on implementing CIS Level 1, CIS Level 2, and STIG hardening standards in a RHEL 9.4 or 9.6 environment.

Security Technical Implementation Guide (STIG) Installs

This installation guide includes STIG Install Notes to assist customers performing a STIG install of ThreatQ 6x on RHEL 8.10 , 9.4, or 9.6 instances.

Prerequisites

Review the following requirements before attempting to install the ThreatQ platform on your air gapped device.

System Requirements

> ⚠ Before you begin a ThreatQ install, you must disable any security endpoint tools running on your VM as this may cause the installation to fail.

For the best performance, your system should meet the following requirements. Failing to meet the minimum system requirements can cause serious platform degradation and loss of functionality.

- Ubuntu 22.04 LTS or Red Hat Enterprise Linux (RHEL) 8.10, 9.4, or 9.6 instance that meets ThreatQ System Requirements and is configured to use UTC as the time zone standard.
- The latest stable RKE2 version. See the steps below for information on installing and configuring RKE2.
- The following packages must be installed on your system:
  bash-completion curl gnupg python3 tmux wget zstd
  In addition, software-properties-common is required for Ubuntu. The container-selinux and iptables packages are required for RHEL.
- Your ThreatQ license key.
- Your ThreatQ YUM credentials.
- A static IP address assigned to the new Ubuntu or RHEL instance.
- Firewall access to the following ports:
  ThreatQ Appliance Ports

SOURCE	DESTINATION	PORT	PORT USE
All of the workstations that will be used by security analysts	ThreatQ	443	Open for ThreatQ UI (HTTPS / TLS)
Workstations that will access remotely ThreatQ	ThreatQ	22	Secure shell access. Open for shell access by administrators
All of the workstations that will be used by security analysts	ThreatQ	80	Redirects to 443 to ensure TLS is used
TAXII Clients	ThreatQ	5910	Used by the embedded TAXII server
Other TQX subscribers	ThreatQ Publisher	8883	Used by ThreatQ Exchange (TQX) Broker (opendxl-broker). The port is used for TQX communication. This is the subscriber's incoming connection port

ThreatQ v6 BYOD Partitioning Overview

For BYOD 6x installations, we require the following partition scheme to obtain the best ThreatQ experience.

Specific Sizes Overview

Use the following in the event that your organization requires specific sizes:

FILE SYSTEM	SIZE	NOTES
/	50GB	N/A
/var	120GB/ 200GB	200GB is the recommended size if there are no other partitions under **/var**. 120GB is the recommended size if there are separate log and tmp partitions under **/var**. Images are stored in **/var** in addition to the locations listed below. See the breakdown of the individual locations within **/var** in the Specific Size Breakdown table below.
/opt	>=600GB	The majority of resources should be dedicated to this location. MYSQL and SOLR utilize this mount point. A minimum of 600GB to several TBs is required for optimal performance.

Specific Size Breakdown

The following is a more detailed break down of specific sizes (listed on the overview table above):

FILE SYSTEM	SIZE	NOTES
/boot	1GB	N/A
/home	20GB	N/A
/tmp	20GB	N/A
/var/tmp	5GB	• If your **/var** size is 200GB, the **/var/tmp** size is included in the overall recommended **/var** file system size of 200GB. • If your **/var** size is 120GB, the **/var/tmp** size is not included in the overall recommended **/var** size of 120GB.
/var/log	50GB	All container logs are written to this location. You can increase the size if needed. • If your **/var** size is 200GB, the **/var/log** size is included in the overall recommended **/var** file system size of 200GB. • If your **/var** size is 120GB, the **/var/log** size is not included in the overall recommended **/var** size of 120GB.
/var/log/audit	20GB	• If your **/var** size is 200GB, the **/var/log/audit** size is included in the overall recommended **/var** file system size of 200GB. • If your **/var** size is 120GB, the **/var/log/audit** size is not included in the overall recommended **/var** size of 120GB.
/	>=680GB	All remaining resources should be dedicated to this location.

Dedicated Mount /opt

Use the following sizing, in addition to the Specific Size Breakdown table, if you are required to create a dedicated mount for `/opt`.

FILE SYSTEM	SIZE	NOTES
/	250GB	N/A
/opt	>=600GB	The majority of resources should be dedicated to this location. A minimum of 600GB to several TBs is required for optimal performance.

Before You Begin

Before setting up your new environment, installing ThreatQ 6x, and migrating your ThreatQ 5x data, we recommend the following preparation:

- Create a non-root user for the new ThreatQ 6x environment.
- Determine if you want to use the default IP range for K8s on the new 6x instance or a custom IP range.
- Make sure your YUM credentials are easily accessible. If you do not have them, please reach out to ThreatQ Support.

⚠ The following install steps must be completed using a non-root user account.

Set up Your Ubuntu or RHEL Environment

1. Provision a new amd64 Ubuntu 22.04 LTS or RHEL 8.10, 9.4, or 9.6 instance that meets ThreatQ system requirements.

DEPLOYMENT SIZE	TYPICAL USAGE	REQUIRED HARDWARE SPECIFICATIONS	MINIMUM INSTANCE SIZE FOR AWS DEPLOYMENT
<2M Indicators	Development or PoC (small)	• 4-8 Core CPUs • 64GB RAM • 800GB of provisioned storage	r6i.2xlarge
2 - 10M Indicators	Medium Production	• 8-16 Core CPUs • 128GB RAM • 800GB of provisioned storage	r6i.4xlarge
>10M Indicators	Large Production	• 16-32 Core CPUs • 256GB RAM • 2TB of provisioned storage	r6i.8xlarge

2. Run the following command to set the maximum number of inotify instances for the installing user to 300.

   ⚠ If the inotify instance maximum is already configured for your system, this command will overwrite any existing value with a value of 300.

```
sudo sed -i '/^fs\.inotify\.max_user_instances/d' /etc/
sysctl.conf && printf "fs.inotify.max_user_instances = 300\n"
| sudo tee -a /etc/sysctl.conf >/dev/null && sudo sysctl -p
```

Pin Your RHEL 9 Version

The following steps allow you to pin your current RHEL 9 release so that you cannot inadvertently upgrade your RHEL 9 environment to an unsupported release. See the Red Hat Enterprise Linux 9 Support section for more information on currently supported RHEL 9 versions.

Run the following commands as root or prefix them with sudo.

1. Set release to minor version:

```
subscription-manager release --set=<release number>
```

2. Clean repositories:

```
yum clean all
```

3. Check which release is set locally:

```
subscription-manager release --show
```

Pin Your Ubuntu 22.04 Version

ThreatQ recommends you update the **release-upgrades** file to disable manual Ubuntu upgrades so that you cannot inadvertently upgrade your Ubuntu 22.04 environment to an unsupported release.

1. Use a text editor, such as vi, to access `/etc/update-manager/release-upgrades`.
2. Change the `Prompt=` setting to `Prompt=never`.
3. Save your changes and exit the file.

Configure Internal Networking

With the default configuration, changing the hostname or external IP address of a Kubernetes system can cause unrecoverable errors that require a complete reinstall to resolve. All these commands must be run with root permissions.

3. Create a virtual network interface using an IP address that does not exist on a local subnet.
   For Ubuntu:

```
sudo tee /etc/netplan/99-k8s-dummy.yaml <<EOF > /dev/null
network:
  version: 2
  bridges:
    dummy0:
      interfaces: []
      addresses: [ "<dummy IP>/32" ]
EOF
sudo chmod 0600 /etc/netplan/*.yaml
sudo netplan apply
```

You may receive a warning message. You can ignore this message and proceed to the next step.

For RHEL:

```
sudo nmcli connection add type dummy ifname dummy0
ipv4.method manual ipv4.addresses <dummy IP>/32 ipv6.method
disabled
```

4. Add an entry to the /etc/hosts file mapping the IP address of the dummy network interface to a simple hostname like “node”.
   Example:

```
echo '<dummy IP> node' | sudo tee -a /etc/hosts
```

Prepare the RKE2 Configuration File

5. Add a configuration file for RKE2 **before** installing it so it takes effect when building the initial configuration. This will force the system to use the dummy IP address and hostname for the Kubernetes node, leaving you free to change your system's external IP address and hostname.

```
sudo mkdir -p /etc/rancher/rke2
sudo tee /etc/rancher/rke2/config.yaml <<EOF > /dev/null
node-name: node
node-ip: <dummy IP>
node-external-ip: <dummy IP>
EOF
```

Example:

```
sudo mkdir -p /etc/rancher/rke2
sudo tee /etc/rancher/rke2/config.yaml <<EOF > /dev/null
node-name: node
node-ip: 192.168.199.1
node-external-ip: 192.168.199.1
EOF
```

Further steps require additional changes to the configuration file, so be careful not to overwrite the file if it already exists.

6. **For RHEL only**, enable SElinux in the rke2 config file:

```
echo "selinux: true" | sudo tee -a /etc/rancher/rke2/
config.yaml > /dev/null
```

7. You **must** configure RKE2 to disable the default ingress module **before** installing in an air gapped environment. Failure to do so will result in the ThreatQ installation hanging later.

```
sudo tee -a /etc/rancher/rke2/config.yaml <<EOF> /dev/null
disable:
  - rke2-ingress-nginx
EOF
```

Change the Kubernetes Subnet (Optional)

By default, RKE2 uses the 10.42.0.0/15 subnet for container and service networking. If that subnet is used for your local network, you may want to configure RKE2 to use a different subnet.
See the RKE2 server configuration options for cluster-cidr, service-cidr, and cluster-dns.ptional.

Set Up kubectl

8. Run the following command to add RKE2 and associated utilities:

```
sudo tee /etc/profile.d/rke2.sh <<EOF > /dev/null
export PATH="\$PATH:/var/lib/rancher/rke2/bin"
EOF
source /etc/profile.d/rke2.sh
```

During the installation of RKE2, restart the host system right after you enable the rke2-server.service and before you start it.

9. Install RKE2 as a Server Node on a systemd-based system using the steps in the RKE2 Air-Gap Install guide.

   If you are using RKE2 on a RHEL system with SElinux enabled you MUST install the rke2-selinux package prior to starting the rke2-server service. This is done automatically if RKE2 is installed via RPM but **NOT** if it is installed via tarball.

Verify Your RKE2 Installation

The following steps must be completed using a non-root user account.

10. After the RKE2 installation is complete, copy the RKE2 kubeconfig file to your home directory and set the appropriate permissions. This enhances security by restricting access to the kubeconfig file.
    Example:

```
mkdir -p ~/.kube
sudo cp /etc/rancher/rke2/rke2.yaml ~/.kube/config
sudo chmod 600 ~/.kube/config
sudo chown "$(id -un)":"$(id -ng)" ~/.kube/config
```

11. Run the following command to check the status of your pods:

```
kubectl get pods -A
```

Example - Successful Output:

```
NAMESPACE     NAME                                                READY   STATUS      RESTARTS      AGE
kube-system   cloud-controller-manager-node                       1/1     Running     3 (23m ago)   34m
kube-system   etcd-node                                           1/1     Running     0             34m
kube-system   helm-install-rke2-canal-hfgqz                       0/1     Completed   0             35m
kube-system   helm-install-rke2-coredns-58ssq                     0/1     Completed   0             35m
kube-system   helm-install-rke2-ingress-nginx-8w876               0/1     Completed   0             35m
kube-system   helm-install-rke2-metrics-server-csrnh              0/1     Completed   0             35m
kube-system   helm-install-rke2-snapshot-controller-crd-tcpsx     0/1     Completed   0             35m
kube-system   helm-install-rke2-snapshot-controller-t9x67         0/1     Completed   1             35m
kube-system   helm-install-rke2-snapshot-validation-webhook-qwsxp 0/1     Completed   0             35m
kube-system   kube-apiserver-node                                 1/1     Running     0             34m
kube-system   kube-controller-manager-node                        1/1     Running     3 (23m ago)   35m
kube-system   kube-proxy-node                                     1/1     Running     0             34m
kube-system   kube-scheduler-node                                 1/1     Running     3 (23m ago)   34m
kube-system   rke2-canal-g7mfc                                    2/2     Running     0             34m
kube-system   rke2-coredns-rke2-coredns-84b9cb946c-r79rv          1/1     Running     0             34m
kube-system   rke2-coredns-rke2-coredns-autoscaler-b49765765-8d6k8 1/1    Running     0             34m
kube-system   rke2-ingress-nginx-controller-tph5x                 1/1     Running     0             32m
kube-system   rke2-metrics-server-655477f655-glq7m                1/1     Running     0             33m
kube-system   rke2-snapshot-controller-59cc9cd8f4-s262d           1/1     Running     2 (23m ago)   33m
kube-system   rke2-snapshot-validation-webhook-54c5989b65-mw5hf   1/1     Running     0             33m
root@dc01-threatq-v6-01:~#
```

Air Gapped Installation

The following steps will walk you through how to download all necessary files and install ThreatQ on an air gapped device.

12. Use the following link format to download the appropriate ThreatQ install tarball:

    You will be prompted to enter your YUM credentials.

> **STIG Install Note:**
> Download ThreatQ from another system. FIPS will not allow you to download ThreatQ. After you download ThreatQ from another system, copy it to the /root/ directory.

```
https://install-v6.threatq.com/<version>-platform.tar.gz
```

You can also download the tarball using a curl command:

```
curl https://<YUM_USER>:<YUM_PASSWORD>@install-
v6.threatq.com/<version>-platform.tar.gz -O
```

13. Download the tqadmin file.

> **STIG Install Note:**
> Download TQAdmin from another system. FIPS will not allow you to download TQAdmin. After you download TQAdmin from another system, copy it to the /root/ directory.

Ubuntu:

```
curl -fO -u <YUM_USER> https://install-v6.threatq.com/
tqadmin.deb
```

RHEL:

```
curl -fO -u <YUM_USER> https://install-v6.threatq.com/
tqadmin.rpm
```

14. Open the CLI of the device you will install ThreatQ on and copy the install tarball and tqadmin package to **/root** using the SCP client of your choice.
15. Return to the CLI of the device and confirm that the install tarball and tqadmin package are present.
16. Install TQAdmin:

> **STIG and RHEL 8.10 Install Note:**
> For STIG installs and for non-STIG RHEL 8.10 installs, append `--nodigest` to the end of the TQAdmin install command.

Ubuntu:

```
sudo dpkg -i tqadmin.deb
```

RHEL:

```
sudo rpm -Uvh tqadmin.rpm
```

17. For RHEL installs, run the following command to install iptables:
RHEL:

```
sudo dnf install iptables-nft
```

18. Run the following command to provision your deployment:

```
sudo /usr/local/bin/tqadmin configure
```

PROMPT	DESCRIPTION
Do you want to enable OpenDXL (TQX)? (yes/no)	Enter yes to enable ThreatQ Data Exchange's OpenDXL functionality. Enter no to disable this functionality.
Do you want to enable the embedded TAXII server? (yes/no)	Enter yes to enable ThreatQ Data Exchange's TAXII server functionality. Enter no to disable this functionality.
Do you want to use your own SSL certificate? (yes/no)	Enter yes to configure a custom SSL certification (not self-signed).
Enter the file path for your certificate	Enter the path for your SSL certificate. **example:** /etc/threatq-certs/mycert.pem
Enter the file path for your private key	Enter the path for the SSL certificate's private key. **example:** /etc/threatq-certs/mykey.pem

PROMPT	DESCRIPTION
Do you want to enable CAC/mTLS? (yes/no)	Enter yes to configure SSL Client Certificate Authentication.
Enter the file path for your certificate	Enter the path for your CA Certificate. **example:** /etc/threatq-certs/mycert.pem
Enter the FQDN of the server	Enter the FQDN of the server. **example:** myserver.threatq.com

Enable syslog audit log output?	Enter yes to access the following configuration prompts:
	• Enter the hostname or IP address of the syslog server to send audit log messages:
	• Enter the port number on the syslog server for audit log messages (default 514):
	• Enable TLS with a client certificate for the syslog server? - If you enter yes for this prompt, TQAdmin displays the following three prompts.
	  ▪ Enter the full path to the client certificate file:
	  ▪ Enter the full path to the client private key file:
	  ▪ Enter the path to the trusted root CA certificate for the syslog server (leave empty to disable certificate validation):

STIG Install Notes:
Running the `tqadmin platform install` command may take longer than fifteen minutes and as such may trigger the timeout interval required

by STIG. To prevent process interruption, a user will need to press the spacebar prior to each timeout. If this is not an option, you can use the following command to increase the timeout interval:
RHEL 9.6: `sudo sed -i 's/=600/=60000/g' /etc/systemd/logind.conf`
RHEL 9.4: `sudo sed -i 's/=600/=60000/g' /etc/profile.d/tmout.sh`
RHEL 8.10:
`sudo sed -i 's/600/60000/g' /etc/ssh/sshd_config; sudo systemctl restart sshd.service`
After you run this command, you must log out and log back in. After you complete the install process, run the following command to reinstate the timeout interval:
RHEL 9.6: `sudo sed -i 's/=60000/=600/g' /etc/systemd/logind.conf`
RHEL 9.4: `sudo sed -i 's/=60000/=600/g' /etc/profile.d/tmout.sh`
RHEL 8.10:
`sudo sed -i 's/60000/600/g' /etc/ssh/sshd_config; sudo systemctl restart sshd.service`

19. Run the following command to Install ThreatQ. You will be prompted for the location of the platform bundle if it is not in **/root**.

```
sudo /usr/local/bin/tqadmin platform install -v <ThreatQ version> -z
```

STIG Install Note:
If you disabled the fifteen minute timeout, after the TQAdmin install completes, run the following command to reinstate the timeout interval:
RHEL 9.6: `sudo sed -i 's/=60000/=600/g' /etc/systemd/logind.conf`
RHEL 9.4: `sudo sed -i 's/=60000/=600/g' /etc/profile.d/tmout.sh`
RHEL 8.10:
`sudo sed -i 's/60000/600/g' /etc/ssh/sshd_config; sudo systemctl restart sshd.service`

20. Run the following command to generate the initial password for the ThreatQ Admin user (username = admin):

```
sudo /usr/local/bin/tqadmin password
```

21. To verify your ThreatQ installation, check the status of the pods and services in your Kubernetes cluster.

```
kubectl get pods -A
kubectl get svc -A
```

22. List the ThreatQ pods:

```
kubectl get pods -n threatq
```

Access Your New ThreatQ 6x Instance

23. Connect to the ThreatQ web interface, using the IP/hostname given during the installation.
24. Add the license key provided by ThreatQ Support.
25. Use the username admin and the password you generated.
26. Accept the EULA.
27. Opt in or out of sending analytics.

Upgrading an Air Gapped ThreatQ Instance

If you are upgrading from one 6x 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. Copy the following location to your browser's address bar:

```
https://<YUM_USER>:<YUM_PASSWORD>@install-v6.threatq.com/
<version>-platform.tar.gz
```

2. Open the CLI of the device to upgrade and copy the upgrade file to `/root/` using the SCP client of your choice.
3. 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-
v6.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:

```
sudo /usr/local/bin/tqadmin platform upgrade -v <release
number> -z
```

Example:

```
sudo /usr/local/bin/tqadmin platform upgrade -v 6.2.0 -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.

Troubleshooting

AGDS is designed to be restartable, meaning export and import operations can be safely rerun after interruption or failure without causing data corruption, duplication, or loss.

On the **export** side, restartability is achieved through the use of **synchronization records** and a configuration-based MD5 hash. Each export run creates a synchronization record at start time and only finalizes it when the run completes successfully. If an export fails, the record is left incomplete (`finished_at` remains NULL), and AGDS does not advance the incremental cursor. When the export is rerun with the same hash-affecting flags, ThreatQ automatically resumes from the last successfully completed export, ensuring that previously exported data is not duplicated and no changes are missed.

On the **import** side, restartability is enabled through the use of **temporary synchronization tables** and deterministic record matching via `sync_hash` values. Imported data is first loaded into temporary tables, validated, and then merged into production tables as either updates or inserts. If an import fails, partially written data is safely handled—rerunning the import will update existing records rather than duplicating them, and no destructive operations are performed. The import process never deletes data from the target system, further reducing risk during retries.

This allows administrators to correct the underlying issue (such as memory limits, disk space, or configuration errors) and rerun the same command without manual cleanup or state resets.

Before you Begin

You should confirm the following before proceeding to troubleshoot an AGDS issue:

- Source and target are on the same ThreatQ version.
- System time is set to UTC on both systems.
- Kubernetes pods are healthy:

  ```
  kubectl get pods -n threatq
  ```

- Sufficient disk space exists:

  ```
  df -h /var/lib/threatq/agds_transfer
  ```

- You are using the correct user (non-root RKE2 user).

Troubleshooting Scenarios

SCENARIO	POSSIBLE CAUSES	WHAT TO CHECK
The manual export process fails Immediately and no tarball is created.	• Permission Issues • Invalid Flags • Insufficient Memory	• Export console output • Larvel Logs
The manual export process completes but does not create the tarball.	• CSV generation error • The disk is full • File system permissions	• Export console output • Laravel log • Disk space
Cron-based export runs but does not create the tarball. Additionally, there may be no log output.	• The cron is being run by the wrong user • Cron environmental differences • Cron is missing the kubectl pathway	• Cron logging enabled • Synchronization records • Cron user permissions
Incremental exports are re-exporting all data resulting in large exports every run and no reduction in data volume.	• Changes have been made to the `--target`, `--include-investigations`, and/or `--include-deleted` flags	• `hash` column in synchronizations table • Export flags consistency
Import process fails mid-way resulting in partial data appearing on the target instance.	• Missing sync_hash initialization • Memory constraints	• Import console output • Import sync report

SCENARIO	POSSIBLE CAUSES	WHAT TO CHECK
	• Data integrity issues	• Laravel logs
Import process completes but the target instance is missing data.	• Export flags used (`--sources`, `--include-investigations` etc.) • Custom objects not installed on target instance	• Review Export and Import sync report files • Check synchronization table for the `--include-investigations` flag • If there are custom objects, confirm they have been installed on the target instance

AGDS Recovery Steps

If the AGDS process fails:

1. Do **not** delete synchronization records.
2. Fix the underlying issue (memory, disk, flags)
3. Re-run the same command.
4. Verify a new `finished_at` is populated in the synchronization table.

Audit Log

About the Audit Log

ThreatQ includes comprehensive audit logging that records detailed user, admin, and system actions across the ThreatQ Platform as well as ThreatQ Data Exchange (TQX), and ThreatQ TDR Orchestrator (TQO). This allows you to track activities such as logins/logouts and configuration updates, and to export these logs securely to your SIEM or Syslog Server.

Configuring Audit Log Exports

To begin exporting your audit log to your SIEM or Syslog Server, you must have the following information available: syslog hostname, syslog port, path to client certificate, and path to client private key:

- For hosted customers, open a Support ticket with that information so that ThreatQuotient can configure your system.
- On premise customers will need to upgrade to the latest version of TQAdmin and use TQAdmin to configure Audit Log Exports. See the TQAdmin Configuration section of the Help Center for more details.

Tips and Tricks

- You can access the audit log from **/var/log/threatq/audit.log**.
- For logged password updates, the password value is redacted.
- Audit Log timestamps use the following format: **yyyy-mm-ddThh:mm:ss+z**
- For failed actions, the audit log entry includes the reason for the failure.
- The following information if the source of an action (e.g. ThreatQ user) has been authenticated via HTTP:
    - URL
    - HTTP method
    - Server
    - Referrer
    - XFF IP address

Audit Log Entries

See the Audit Log Entries section for a list of system actions that trigger the creation of a log entry as well as a description of the information logged.

Audit Log Entries

Authentication/User Activity Logging

ACTION	MESSAGE(S)	INFORMATION LOGGED

Local OAuth2 Authentication	• Login Success
	• Login Fail
		• Username (authentication type)
		• Login fail reason:
		  ◦ User credentials are not valid
		  ◦ Account Locked
		  ◦ Account Disabled
		  ◦ Incorrect auth type
		• Timestamp

Client Credential Authentication	• Login Success • Login Fail	• Username (authentication type) • Login fail reason: ◦ Connector is disabled • Timestamp

LDAP Authentication	• Login Success
	• Login Fail
	• User conversion from local to LDAP
		• Username (authentication type)
		• Login fail reason:
		  ◦ User credentials are not valid
		  ◦ Invalid authentication method
		  ◦ User credentials are not valid

ACTION	MESSAGE(S)	INFORMATION LOGGED
		◦ The User Certificate has not been selected ◦ User credentials are not valid ◦ Invalid authentication method ◦ No user groups found in LDAP search ◦ No LDAP to TQ group mappings found ◦ The account has been temporarily locked due to too many consecutive failed login attempts ◦ Maintenance accounts are prohibited to log in using SSO ◦ LDAP User does not belong to any mapped TQ groups • Timestamp
SAML Authentication	• Login Success • Login Fail • User conversion from local to SAML • LDAP maintenance user was converted to SAML • Local login attempt after	• Username (authentication type) • Login fail reason: ◦ SAML Single-Logout-Service error(s) ◦ Invalid authentication method • Timestamp

ACTION	MESSAGE(S)	INFORMATION LOGGED
	conversion to SAML Only allowed for Maintenance users.	

SSL Client Certificate Authentication (CAC)	• Login Success
	• Login Fail
	• User fingerprint saved
		• Username (authentication type)
		• Login fail reason:
		  ◦ User credentials are not valid
		  ◦ The User Certificate has not been selected
		  ◦ The account has been temporarily locked due to too many consecutive failed login attempts
		• Timestamp

Account Lock	• Account Locked • Account Unlocked	• Username • Timestamp
Logout	• Logout Success • Logout Failure	• Username • Timestamp

User Management Logging

ACTION	MESSAGE(S)	INFORMATION LOGGED
Add/Delete User	• New User added to platform • User Deleted	• Username that made the change • User information such as name and role • Timestamp
Updates to User Information	• New Custom Role created • User Role changed by administrator Listed if users were added to the Role as part of the creation process. • Changes have been made to a Custom Role • User Role changed by administrator Listed if users were added to the role as part of the creation process. • Custom Role has been removed • LDAP has been enabled • LDAP has been disabled • LDAP configuration has been updated	• Username that made the change • Username that was changed • User profile changes • Timestamp

ACTION	MESSAGE(S)	INFORMATION LOGGED
	• LDAP connection tested • LDAP Groups listed • LDAP Users listed • SAML has been enabled • SAML has been disabled • SAML configuration has been updated • User profile updated by User	
Updates to Multifactor Authentication (MFA) Settings	• MFA enabled by User • MFA disabled by User	• Username that made the change • Username that was changed • Timestamp

Integration Configuration Logging

Applies to feeds and operations.

ACTION	MESSAGE(S)	INFORMATION LOGGED
Installing/ uninstalling an integration	• <integration type> has been installed • <integration type> has been uninstalled	• Username that made the change • Integration name • Timestamp
Enabling/disabling an integration	• <integration type> has been disabled • <integration type> has been enabled	• Username that made the change • Integration name

ACTION	MESSAGE(S)	INFORMATION LOGGED
		• Timestamp
Updating integration settings	• <integration type> configuration has been updated	• Username that made the change • Integration name • Configuration changes • Timestamp

Data Retention Policy Logging

ACTION	MESSAGE(S)	INFORMATION LOGGED
Enable/Disable Data Retention Policy	• Data Retention Policy has been enabled • Data Retention Policy has been disabled	• Username that made the change • Timestamp
Update Data Retention Policy	• Data Retention Policy has been updated	• Username that made the change • Data collection name • Timestamp

ThreatQ Data Exchange (TQX) Logging

ACTION	MESSAGE(S)	INFORMATION LOGGED
Install a TQX transport via new install or upgrade	• Integration has been installed	• Username • Timestamp
Update a TQX transport	• Integrations setting has been updated	• Username • Feed name • Timestamp
Create/delete an OpenDXL transport node	• TQX - OpenDXL integration configuration has been created • TQX - OpenDXL integration configuration has been removed	• Transport UUID and name • Timestamp
Update an OpenDXL transport node	• TQX - OpenDXL integration configuration has been updated	• Transport UUID and name • Configuration updates • Timestamp
Create/Delete OpenDXL data feed	• TQX - OpenDXL integration configuration has been created • TQX - OpenDXL integration configuration has been removed	• Feed name • Feed settings • Timestamp

ACTION	MESSAGE(S)	INFORMATION LOGGED
Update OpenDXL data feed	• TQX - OpenDXL integration configuration has been updated	• Feed name • Updates to feed settings • Timestamp

TAXII Server Logging

ACTION	MESSAGE(S)	INFORMATION LOGGED
Install a TAXII transport via an install or upgrade that includes a TQX license	• Integration has been installed	• Username that installed the TAXII transport • TAXII Collection Name • Timestamp
Create a TAXII collection	• TQX - TAXII integration configuration has been created	• Username that created the TAXII collection • TAXII Collection Name • Timestamp
Delete a TAXII collection	• TQX - TAXII integration configuration has been removed	• Username that deleted the TAXII collection • TAXII Collection Name • Timestamp
Update a TAXII collection	• TQX - TAXII integration	• Username that updated the TAXII

ACTION	MESSAGE(S)	INFORMATION LOGGED
	configuration has been updated	collection's configuration • Configuration changes • TAXII Collection Name • Timestamp
Create a TAXII user –	• TQX - TAXII integration configuration has been created	• Username that created a TAXII user • TAXII username • Timestamp
Delete a TAXII user	• TQX - TAXII integration configuration has been removed	• Username that removed a TAXII user • TAXII username • Timestamp
Update a TAXI user	• TQX - TAXII integration configuration has been updated	• Username that updated a TAXII user's username, password, and/or TAXII collection access • Configuration changes • TAXII username • Timestamp
Create a TAXII collection user	• TQX - TAXII integration configuration has been created	• Username that added a TAXII user to a TAXII collection • TAXII username

ACTION	MESSAGE(S)	INFORMATION LOGGED
Delete a TAXII collection user	• TQX - TAXII integration configuration has been removed	• Username that removed a TAXII user from a TAXII collection • TAXII username

ThreatQ TDR Orchestrator (TQO) Configuration Logging

Applies to configuration driven workflows (CDWs), TQO workflows, and TQO actions.

ACTION	MESSAGE(S)	INFORMATION LOGGED
TQO Component: CDW		
Install/Uninstall a CDW	• Integration has been installed • Integration has been uninstalled	• Username that made the change • CDW name • Timestamp
Enable/Disable a CDW	• Integration has been enabled • Integration has been disabled	• Username that made the change • CDW name • Timestamp

ACTION	MESSAGE(S)	INFORMATION LOGGED
Update a CDW's configuration	• Integrations setting has been updated	• Username that made the change • CDW name • Configuration changes • Timestamp
Delete a CDW's configuration	• Advanced workflow integration configuration has been removed	• Username that deleted the configuration • CDW name • Timestamp
TQO Component: Workflows		
Install/Uninstall a workflow	• Integration has been installed • Integration has been uninstalled	• Username that made the change • Workflow name • Timestamp
Enable/Disable a workflow	• Integration has been enabled • Integration has been disabled	• Username that made the change • Workflow name • Timestamp
Update a workflow	• Integrations setting has been updated	• Username that made the change • Workflow name • Configuration change

ACTION	MESSAGE(S)	INFORMATION LOGGED
		• Timestamp
Create a workflow	• Workflow builder integration configuration has been created	• Username that created the workflow • Workflow name • Configuration settings • Timestamp
Update a workflow's configuration	• Workflow builder integration configuration has been updated	• Username that updated the workflow's configuration • Workflow name • Configuration changes • Timestamp
Delete a workflow's configuration	• Workflow builder integration configuration has been removed	• Username that deleted the workflow's configuration • Timestamp
TQO Component: TQO Action		
Configure a TQO action	• Workflow builder action integration configuration has been created	• Username that configured the action • TQO action name • Timestamp

ACTION	MESSAGE(S)	INFORMATION LOGGED
Update a TQO action's configuration	• Workflow builder action integration configuration has been updated	• Username that updated the action's configuration • TQO action name • Configuration changes • Timestamp
Delete a TQO action's configuration	• Workflow builder action integration configuration has been removed	• Username that deleted the action's configuration • TQO action name • Configuration changes • Timestamp
Install/Uninstall a TQO action	• Integration has been installed • Integration has been uninstalled • Action integration configuration has been removed	• Username that installed/uninstalled the action • Uninstall - Includes the message and data for an action configuration deletion • TQO action name • Timestamp
Update a TQO action	• Integrations setting has been updated • Action integration configuration has been updated	• Username that updated the action • Configuration settings • TQO action name • Timestamp

ACTION	MESSAGE(S)	INFORMATION LOGGED
Create a TQO action	• Action integration configuration has been created	• Username that updated the action • Configuration settings • TQO action name • Timestamp

Export Audit Log Command

The **Audit Log Export** command allows administrators to export ThreatQ audit logs to a consolidated **CSV** or **JSON** file. Exported audit logs can be archived for long-term retention, imported into external reporting tools, or scheduled to run automatically using operating system schedulers such as **cron**.

The export includes audit records for all supported ThreatQ object types, including custom object types, and automatically includes new object types as they are added to your environment.

Before You Begin

- You must be running ThreatQ v6.20.1 or later.
- You must have command-line access to the ThreatQ application server.
- You must have permission to run ThreatQ Artisan commands.
- Ensure sufficient disk space is available for the exported file. By default the export will be written to the tmp folder. Example: `/tmp/audit_log_export_<timestamp>.csv`. This location can be changed using the `--output` flag - see the Export Audit Log Command Flags section below for more details.

Performance Considerations

The Audit Log Export command is optimized for large environments and enterprise deployments.

The command:

- Streams records directly to disk to minimize memory usage.
- Automatically discovers newly added custom object types.
- Supports configurable batch sizes for large exports.
- Uses non-blocking database reads by default to minimize impact on normal ThreatQ operations.

These optimizations allow the command to export very large audit datasets without requiring significant system memory.

Export Audit Logs Command

Use the following command to export audit logs:

```
php artisan threatq:export-audit-log [object] [options]
```

The **`object`** argument specifies **which audit logs to export**. If you omit it, the command exports audit logs for **all supported object types**.

You can specify one of the following for the object argument:

TARGET	DESCRIPTION	EXAMPLE
`all` (default)	Exports audit logs for all supported object types.	`php artisan threatq:export-audit-log`
Object type	Exports audit logs for one or more object types. Specify multiple object types as a comma-separated list.	`php artisan threatq:export-audit-log indicator,event`
Audit table	Exports records from a specific audit table.	`php artisan threatq:export-audit-log indicator_audit_log`

Export Audit Logs Command Flags

The following flags will allow you to filter an export to your organization's needs.

FLAG	DESCRIPTION
`--discover`	Lists available audit tables without exporting data.
`--from`	Exports records changed on or after the specified date.
`--to`	Exports records changed on or before the specified date.
`--format=csv|json`	Specifies the export format. Default is CSV.
`--output`	Specifies the output file location.
`--limit`	Limits the number of exported records per table.
`--chunk-size`	Sets the number of records processed in each batch.
`--memory-limit`	Overrides the PHP memory limit used during export.
`--no-dirty-read`	Disables the default non-blocking database read mode.

Filtering Scenarios

SCENARIO	COMMAND	DESCRIPTION
Export all audit logs	`php artisan threatq:export-audit-log`	Exports audit logs for all supported object types. By default, the output is written as a CSV file to `/tmp/audit_log_export_<timestamp>.csv`.
Export specific object types	`php artisan threatq:export-audit-log indicator,event`	Exports audit logs for the specified ThreatQ object types. Specify multiple object types as a comma-separated list.

SCENARIO	COMMAND	DESCRIPTION
Export a specific audit table	`php artisan threatq:export-audit-log indicator_audit_log`	Exports records from a single audit table instead of all object types.
Export a date range	`php artisan threatq:export-audit-log --from="2026-01-01" --to="2026-01-31"`	Exports only audit records modified within the specified date range.
Export recent records	`php artisan threatq:export-audit-log --from="30 days ago"`	Exports audit records modified within the last 30 days using a relative date.
Export a sample of records	`php artisan threatq:export-audit-log --limit=1000`	Limits the export to the specified number of records per audit table, which is useful for testing or sampling.
Export as CSV	`php artisan threatq:export-audit-log`	Exports audit logs in CSV format. This is the default output format, so the `--format` option is not required.
Export as JSON	`php artisan threatq:export-audit-log --format=json`	Exports audit logs in JSON format. The JSON output includes export metadata, audit log records, and the total number of exported records.
Save the export to a custom location	`php artisan threatq:export-audit-log --output=/exports/audit_logs.csv`	Writes the exported audit logs to the specified file path instead of the default output location.

SCENARIO	COMMAND	DESCRIPTION
View available audit tables	`php artisan threatq:export-audit-log --discover`	Lists all exportable audit tables that can be used with the command. Tables that do not support exporting, such as `cache_audit_log`, are automatically excluded.

Exported Data

Each export contains normalized audit information from every supported audit table.

Depending on the audit event, exported records may include:

- Object type
- Audit table
- Audit event type
- Object ID
- Object value
- Modified field
- Updated value
- User or integration that made the change
- Date and time of the change
- Relationship source and destination objects (for link events)
- Additional audit metadata

Relationship events include both the source and destination objects, making it easier to identify objects that were linked or unlinked.

Schedule Automatic Exports

Because the Audit Log Export command is a standard Artisan command, it can be scheduled using **cron** or another operating system scheduler.

Example:

```
0 2 * * * cd /opt/threatq && php artisan threatq:export-audit-log
--output=/exports/audit_$(date +\%F).csv
```

This example exports all audit logs every day at **2:00 AM**.

Troubleshooting

ISSUE	RESOLUTION
Invalid object type	Verify the object type or audit table name, or run `--discover` to view available export targets.
Invalid output format	Specify either `csv` or `json`.
Invalid chunk size or limit	Specify a positive integer value.
Command unavailable	Contact your ThreatQ administrator to verify that the Audit Log Export feature is installed and available in your deployment.

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.
- ThreatQuotient recommends you delete any disabled custom objects before running the backup process. If the backup process encounters a disabled custom object, the process stops and you are prompted to delete the object or contact ThreatQuotient Support for assistance.
- Upon upgrade to ThreatQ 6.15.0, credentials for the backup and restore processes are handled automatically. Users are not prompted for MariaDB credentials, and a separate MariaDB user is created as part of the install process.

Backup Options

ThreatQ supports the following backup options:

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

Password Retrieval (ThreatQ v6.14.0 and Prior)

> The backup and restore processes for ThreatQ v6.15.0 or later **do not** require entry of the MariaDB password.

The backup and restore processes for ThreatQ v6.14.0 and prior may require the MariaDB password. You can use the `get secrets` command listed below to retrieve all Kubernetes secrets, including your MariaDB MySQL password, in a human-readable format.

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

```
kubectl get secrets --namespace threatq --output go-
template='{{range $i,$d := .items}}{{print $d.metadata.name
"\n"}}{{range $k,$v := $d.data}}{{printf " %s: " $k}}{{if not
$v}}{{$v}} {{else}}{{$v | base64decode}}{{end}}{{"\n"}}
{{end}}{{"\n"}}{{end}}'
```

ThreatQ Backup Process

1. SSH to the ThreatQ command line.
2. Choose one of the following options:
   - To create a backup that includes the threat intelligence data index, run the following command:

     ```
     kubectl exec --namespace threatq --stdin --tty
     deployment/api-schedule-run -- ./artisan threatq:backup
     ```

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

     ```
     kubectl exec --namespace threatq --stdin --tty
     deployment/api-schedule-run -- ./artisan threatq:backup
     --exclude-solr
     ```

     > To specify the location of your backup, append the following to your backup command:
     > `--destination-path /var/lib/threatq/misc/my-backup-folder`

3. When prompted, provide the **MariaDB** password. See the Password Retrieval section for the steps to retrieve this password.

   > The backup and restore processes for ThreatQ v6.15.0 or later do not require the entry of the MariaDB password.

   For releases prior to ThreatQ v6.15.0, 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.

4. Provide the path to the file location where you want to create the backup.
   The file that you store the backup file must be in the following location: **/var/lib/threatq/misc**
   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 ThreatQ 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.
- You cannot restore an online backup in a ThreatQ 6x instance. ThreatQ returns the following error message if you attempt to restore a ThreatQ 5x online backup in a ThreatQ 6x instance: Online backups are not supported in this version. **Try again using an offline backup.**

ThreatQ Restore Process

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

1. SSH to the command line and elevate your user privileges to root or sudo.
2. Run the following command:

```
kubectl exec --namespace threatq --stdin --tty deployment/
api-schedule-run -- ./artisan threatq:restore </path/to/
backup_file>
```

> If prompted, provide the **MariaDB** password. See the Password Retrieval section for the steps to retrieve this password. The backup and restore processes for ThreatQ v6.15.0 or later do not require the entry of the MariaDB password.

3. 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.

4. After the restore completes, you should reboot the target ThreatQ system to ensure that the system processes start 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

- 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.
- Artisan commands are run in the api-schedule-run pod.

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. Run the following command:

   ```
   kubectl exec --namespace threatq --stdin --tty deployment/
   api-schedule-run -- ./artisan down
   ```

   The platform is now in maintenance mode. When you log into a ThreatQ instance that is in maintenance mode, ThreatQ displays a maintenance notification that includes the following message: **ThreatQ is down for maintenance**.

Taking the ThreatQ Application Out of Maintenance Mode

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

```
kubectl exec --namespace threatq --stdin --tty deployment/
api-schedule-run -- ./artisan up
```

The platform is now out of maintenance mode.

Passwords for Artisan Commands

Some commands, such as the backup command require the MariaDB password. You can use the `get secrets` command listed below to retrieve all Kubernetes secrets, including your MariaDB password, in a human-readable format.

Retrieving Passwords

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

```
kubectl get secrets --namespace threatq --output go-
template='{{range $i,$d := .items}}{{print $d.metadata.name
"\n"}}{{range $k,$v := $d.data}}{{printf " %s: " $k}}{{if not
$v}}{{$v}} {{else}}{{$v | base64decode}}{{end}}{{"\n"}}
{{end}}{{"\n"}}{{end}}'
```

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 - ThreatQ v6

1. SSH to your ThreatQ installation.
2. Place the application into maintenance mode - see the Maintenance Mode section.
3. Run the following command:

```
kubectl exec --namespace threatq --stdin --tty deployment/
api-schedule-run -- ./artisan threatq:feed-install /var/lib/
threatq/misc/<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.
> ```

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

Upgrade a CDF - ThreatQ v6

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

```
kubectl exec --namespace threatq --stdin --tty deployment/
api-schedule-run -- ./artisan threatq:feed-install /var/lib/
threatq/misc/<Feed Definition File> --upgrade
```

4. 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 - ThreatQ v6

```
kubectl exec --namespace threatq --stdin --tty deployment/api-
schedule-run -- ./artisan threatq:feed-install --help
```

View Feed Queues

This command is deprecated in ThreatQ v6

System Object Commands

Delete Adversary Descriptions

This command is deprecated in ThreatQ v6

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.

Merge Attributes - ThreatQ v6

1. SSH to your ThreatQ installation.
2. Place the application into maintenance mode - see the Maintenance Mode topic.
3. Run the following command:

```
kubectl exec --namespace threatq --stdin --tty deployment/
api-schedule-run -- ./artisan 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`.

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

Merge Attribute without using `--source`

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

ThreatQ v6 Example

```
kubectl exec --namespace threatq --stdin --tty deployment/api-
schedule-run -- ./artisan threatq:merge-attributes --old-
name='Cuontry' --merge-name='Country'
```

Merge Attribute using `--source`

The attribute `Cuontry` , 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), `Cuontry: US`, on an object, after running the command, the attribute value appears as `Country: US` on that object.

ThreatQ v6 Example

The attribute `Cuontry` , 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), `Cuontry: US`, on an object, after running the command, the attribute value appears as `Country: US` on that object.

```
kubectl exec --namespace threatq --stdin --tty deployment/api-
schedule-run -- ./artisan threatq:merge-attributes --old-
name='Cuontry' --merge-name='Country' --source='CrowdStrike'
```

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

The attribute `Cuontry` , 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), `Cuontry: US`, on an object, after running the command, the attribute value appears as `Country: US` on that object.

ThreatQ v6 Example

```
kubectl exec --namespace threatq --stdin --tty deployment/api-
schedule-run -- ./artisan threatq:merge-attributes --old-
name='Cuontry' --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.

Source Consolidation - ThreatQ v6

1. SSH to your ThreatQ installation.
2. Place the application into maintenance mode - see the Maintenance Mode topic.
3. Run the following command:

```
kubectl exec --namespace threatq --stdin --tty deployment/
api-schedule-run -- ./artisan threatq:consolidate-sources
```

4. 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 becomes Source B).

The command does not affect date stamps nor does it require a recalculation of scoring.

Source Merge - ThreatQ v6

1. SSH to your ThreatQ installation.
2. Place the application into maintenance mode - see the Maintenance Mode section.
3. Run the following command:

```
kubectl exec --namespace threatq --stdin --tty deployment/
api-schedule-run -- ./artisan threatq:merge-sources --origin-
source="<source a>" --destination-source="<source b>"
```

4. 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. Place the platform into maintenance mode. 2. Run the Source Merge command. 3. From the merge confirmation dialog, confirm the merge. The platform will merge the origin source into the destination source, delete the origin source after completion, and record the source merge in the audit log for affected data. Then, a command success message is displayed. 4. Bring the platform out of maintenance mode.
Merge system source (origin source) with a user-created source (destination source).	1. Place the platform into maintenance mode. 2. Run the Source Merge command. The platform indicates that a system source cannot be merged into another source. 3. Bring the platform out of maintenance mode.
Merge user-created source (origin source) with a system source (destination source) with duplicate records.	1. Place the platform into maintenance mode. 2. Run the Source Merge command. The platform indicates that there are duplicate records between the two sources and prompts you to run the Source Consolidation command before proceeding with the merge. Run the Source Consolidation command. 3. Run the Source Merge command.

EXAMPLE SCENARIO	DETAILS
	4. From the merge confirmation dialog, confirm the merge. The platform merges the origin source into the destination source, deletes the origin source after completion, and records the source merge in the audit log for affected data. Then, a command success message is displayed. 5. Bring the platform out of maintenance mode.
Merge user-created source (origin source) with a system source (destination source) with an assigned TLP.	1. Place the platform into maintenance mode. 2. Run the Source Merge command. 3. From the merge confirmation dialog, confirm the merge. The platform merges the origin source into the destination source, deletes the origin source after completion and applies the destination source's default TLP settings to the merged data and records the source merge in the audit log for affected data. Then, a command success message is displayed. 4. Bring 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.

Convert TLP - ThreatQ v6

1. SSH to your ThreatQ installation.
2. Place the application into maintenance mode - see the Maintenance Mode section.
3. Run the following command:

```
kubectl exec --namespace threatq --stdin --tty deployment/
api-schedule-run -- ./artisan threatq:convert-tlp-attributes
```

4. 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, object attribute source, and object description 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 are prompted to confirm the action after entering the command. All updates are recorded in the audit log.

> The command updates 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 - ThreatQ v6

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

   ```
   kubectl exec --namespace threatq --stdin --tty deployment/
   api-schedule-run -- ./artisan threatq:apply-tlp-defaults
   ```

   The application will warn you that this action is not reversible and will require user confirmation before proceeding.
3. 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 automatically be brought out of maintenance mode.

Update a Specific Source - ThreatQ v6

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

   ```
   kubectl exec --namespace threatq --stdin --tty deployment/
   api-schedule-run -- ./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"

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

3. 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 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 - ThreatQ v6

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

```
kubectl exec --namespace threatq --stdin --tty deployment/api-schedule-run
-- ./artisan threatq:configuration --key consumer.connectors_override_status
--value 1 kubectl exec –n threatq --stdin --tty deployment/api-schedule-run
-- ./artisan cache:clear
```

Disable Indicator and Signature Status Overrides - ThreatQ v6

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

```
kubectl exec --namespace threatq --stdin --tty deployment/api-schedule-run
-- ./artisan threatq:configuration --key consumer.connectors_override_status
--delete kubectl exec --namespace threatq --stdin --tty deployment/api-
schedule-run -- ./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.

Allow Cross-Origin Resource Sharing for Specific Hostnames - ThreatQ v6

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

```
kubectl exec --namespace threatq --stdin --tty deployment/
api-schedule-run -- ./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:

```
kubectl exec --namespace threatq --stdin --tty deployment/
api-schedule-run -- ./artisan threatq:configuration --
key=cors.allowed_hosts --value https://www.example.com
```

Multiple Domains Example:

```
kubectl exec --namespace threatq --stdin --tty deployment/
api-schedule-run -- ./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.

Disable Export Logging - ThreatQ v6

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

```
kubectl exec --namespace threatq --stdin --tty deployment/
api-schedule-run -- ./artisan threatq:configuration --key
exports.disable_logging --value 1
```

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

```
kubectl exec --namespace threatq --stdin --tty deployment/
api-schedule-run -- ./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 - ThreatQ v6

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

```
kubectl exec --namespace threatq --stdin --tty deployment/
api-schedule-run -- ./artisan threatq:ldap-debug
```

To perform basic connect and bind authentication as well as authentication with the test username - ThreatQ v6

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

```
kubectl exec --namespace threatq --stdin --tty deployment/
api-schedule-run -- ./artisan threatq:ldap-debug --test-
user=username
```

Example:

```
kubectl exec --namespace threatq --stdin --tty deployment/
api-schedule-run -- ./artisan threatq:ldap-debug --test-
user=administrator
```

3. 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

This command is deprecated in ThreatQ v6

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 - ThreatQ v6

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

```
kubectl exec --namespace threatq --stdin --tty deployment/
api-schedule-run -- ./artisan threatq:purge-threat-
intelligence
```

4. You will be presented the following prompt: **You are about to erase all of your data, are you sure?**
5. Enter **Yes** or **No**.
6. Bring the application out of maintenance mode - see the Maintenance Mode section.

Reset User Password

You cannot reset a SAML or LDAP user's password from the command line.

Reset User Password - ThreatQ v6

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

```
kubectl exec --namespace threatq --stdin --tty deployment/
api-schedule-run -- ./artisan threatq:password-reset
```

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

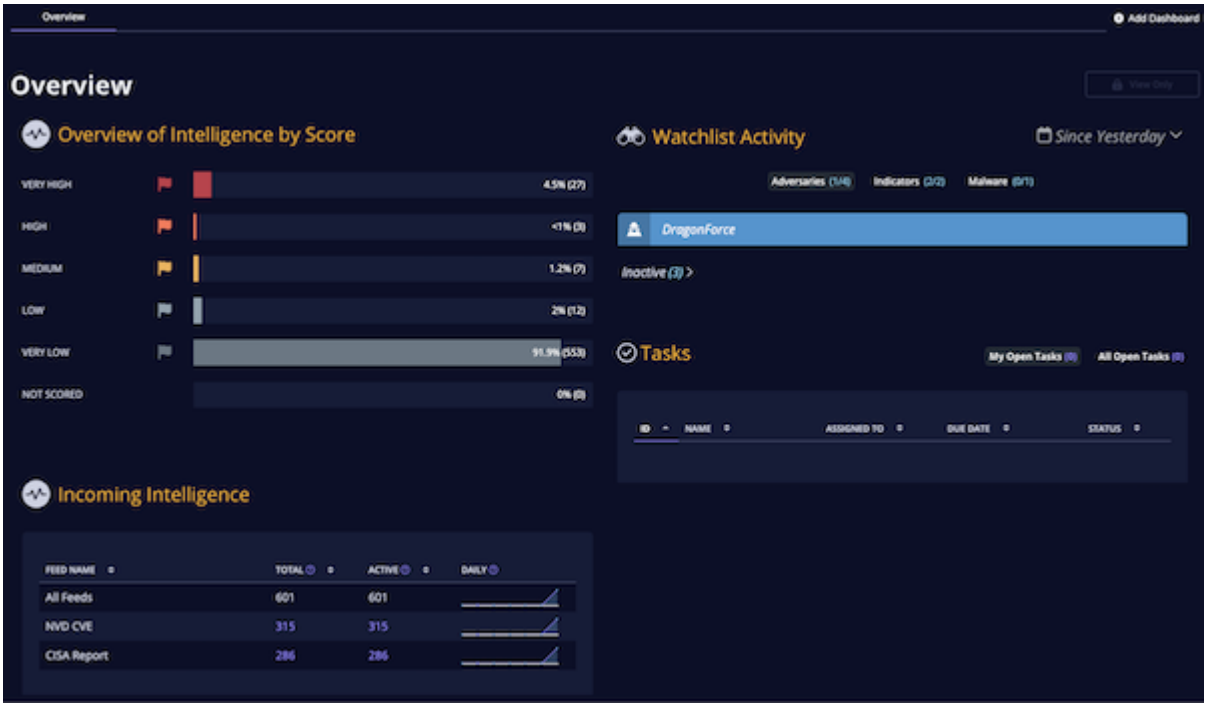
Dashboards

About Dashboards

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role - Action Permissions: Artifact Management - 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.



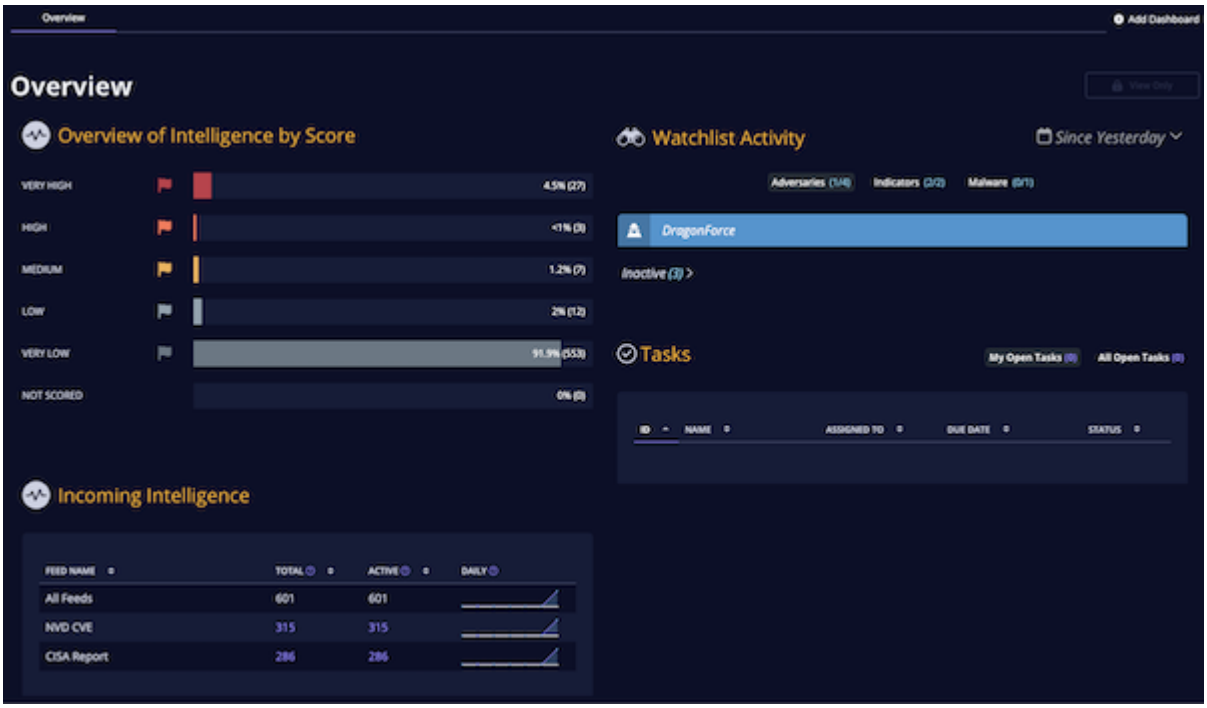
While the Overview dashboard cannot be modified, Primary Contributors, Administrators, and Maintenance users can use ThreatQ widgets to build custom dashboards that can be shared with individual users or all users. These custom dashboards allow you to narrow your focus on threat intelligence trends that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

Default Dashboard

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role - Action Permissions: Artifact Management - Dashboards

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 of Intelligence by Score

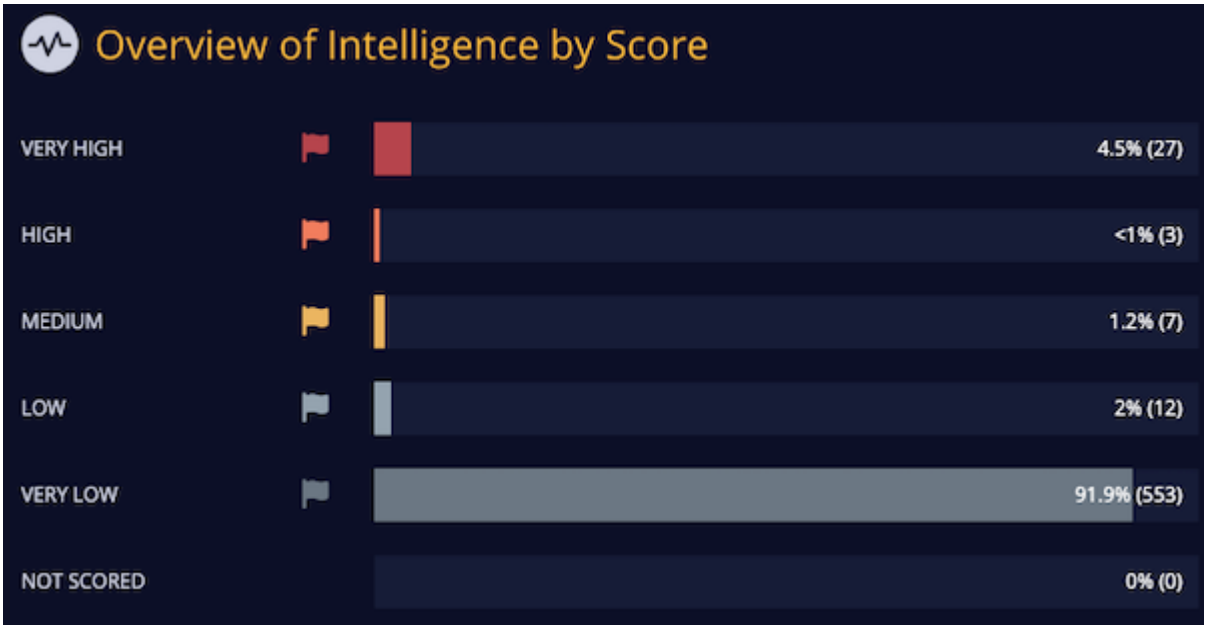
This dashboard graph provides a summary of indicator scoring in the system. It lists total indicators by score in the following order:

- Very High

- High
- Medium
- Low
- Very Low
- Not Scored

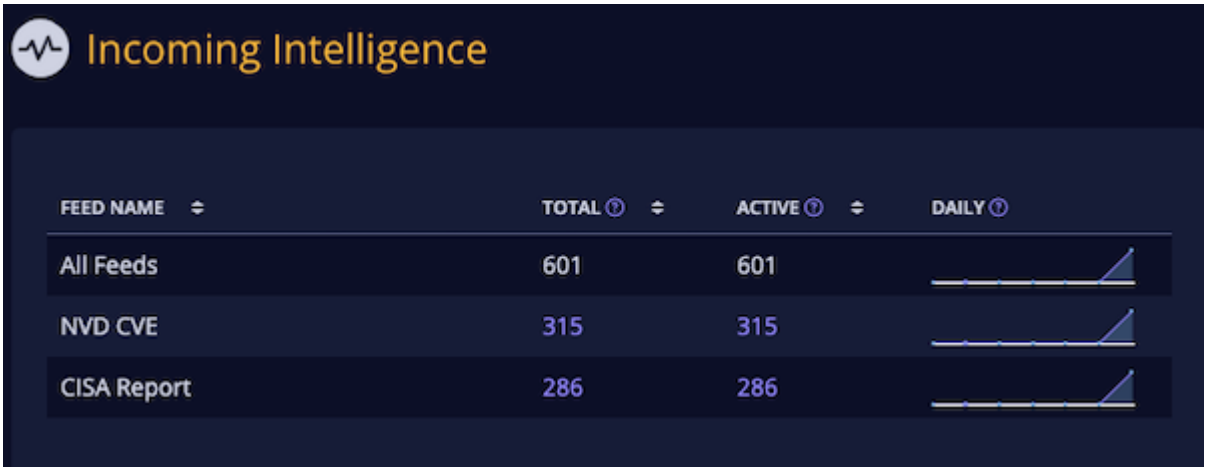
Ideally, this dashboard reflects a small number of **Very High** indicators with the bulk of the remaining indicators scored as **Low** or **Very Low**. This distribution reflects a focus on key threat intelligence. You can use Scoring Algorithms or manually set an object's score to adjust the scores 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:

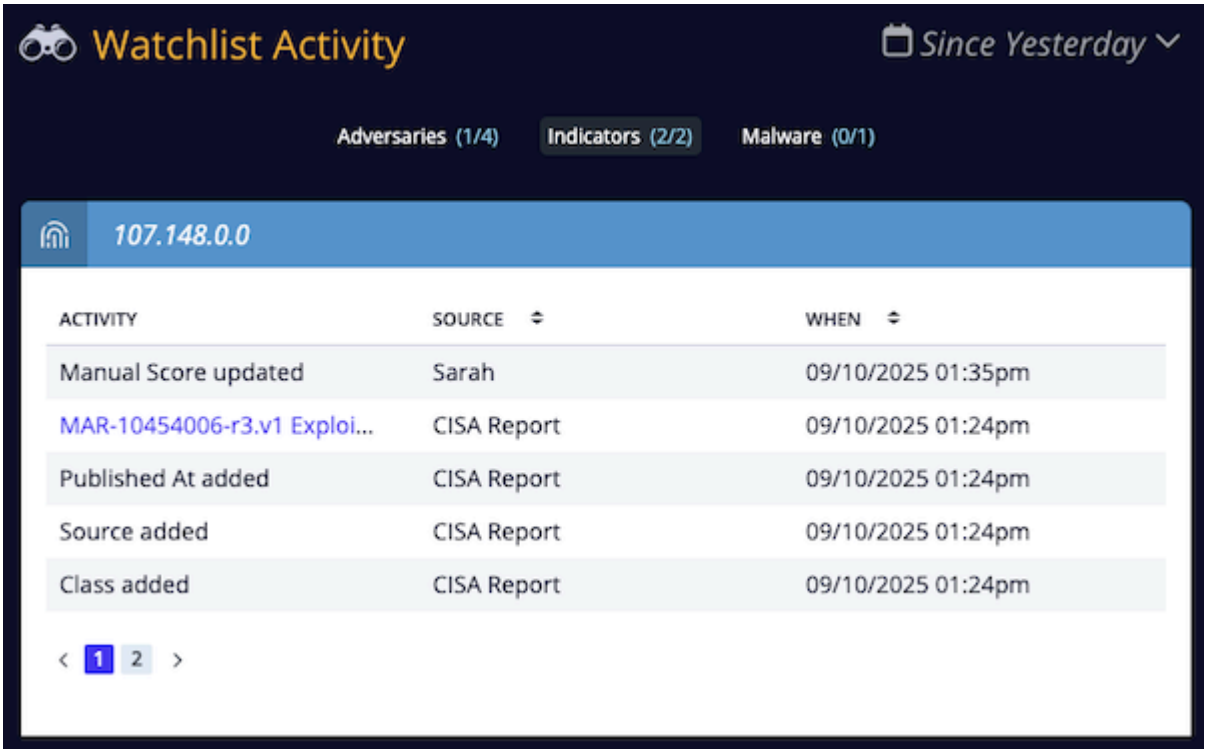
- Feed Name
- Total number of indicators reported by a source
- Indicators reported by a source with a status of active
- All indicators reported by a source per day (includes existing indicators)

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 Watchlist Activity widget is not displayed for Read-Only users.



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

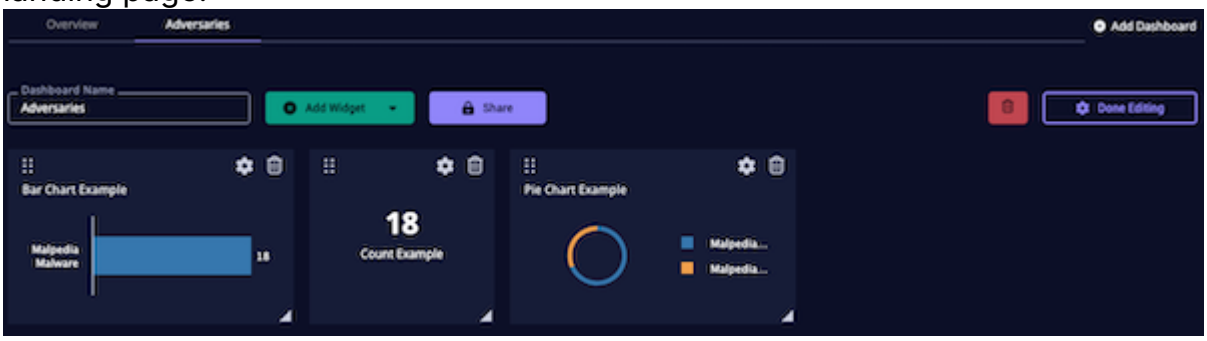
About Custom Dashboards

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role:

- Action Permissions: Objects & Context - Objects (all object types) **OR** Data Access Permissions: object type
- Action Permissions: Artifact Management - 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 About 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

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role:

- Action Permissions: Objects & Context - Objects (all object types) **OR** Data Access Permissions: object type
- Action Permissions: Artifact Management - 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.

Adversary Analytics Dashboard

THREATQ REQUIRED PERMISSIONS

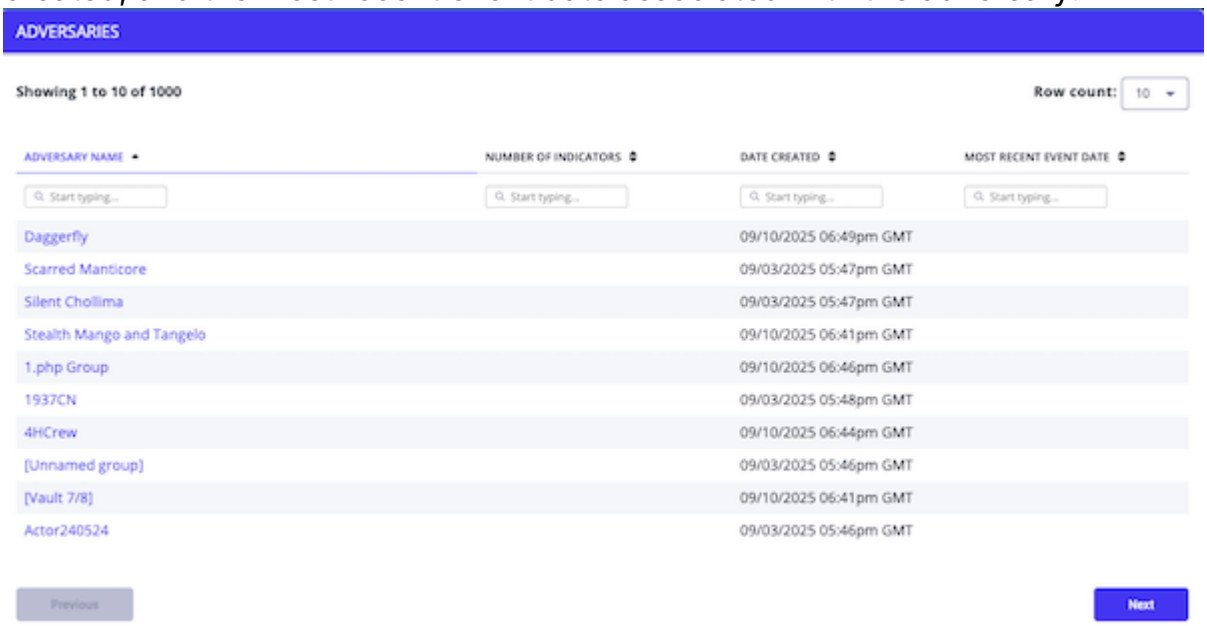
Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role:

- Action Permissions: Objects & Context - Objects (all object types) **OR** Data Access Permissions: Adversary
- Action Permissions: Artifact Management - Dashboards

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.



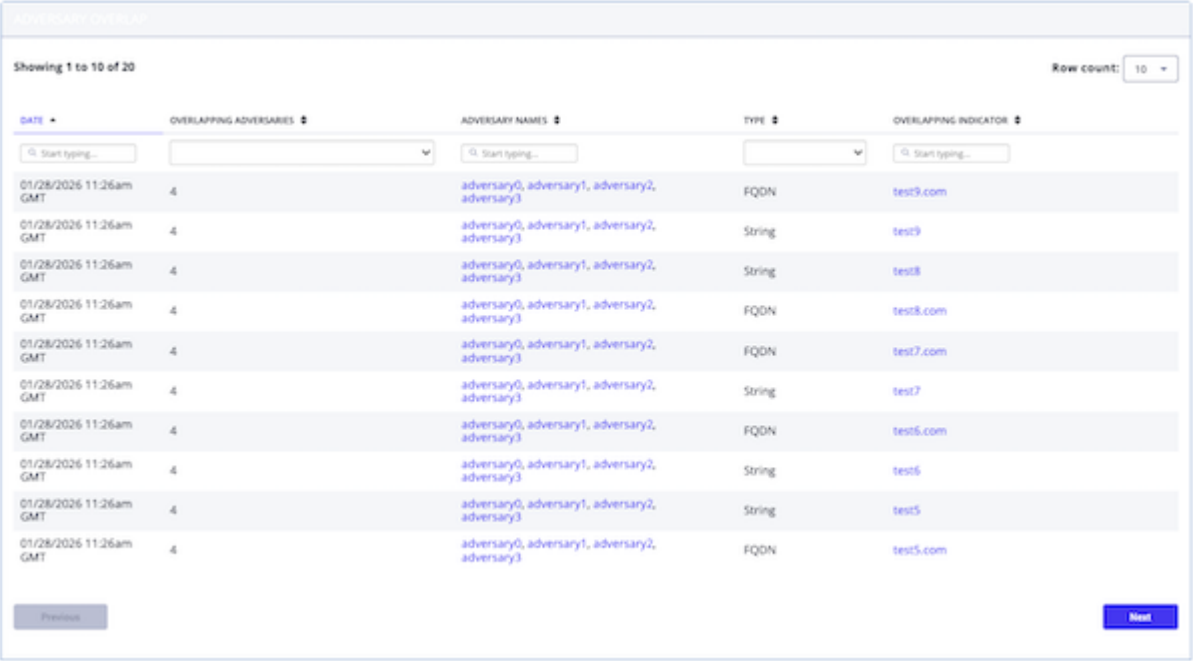
The following functions are available:

FUNCTION	DETAILS
Opening the Adversary Details page for an adversary	Click the name in the Adversary Name column.

FUNCTION	DETAILS
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.
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.

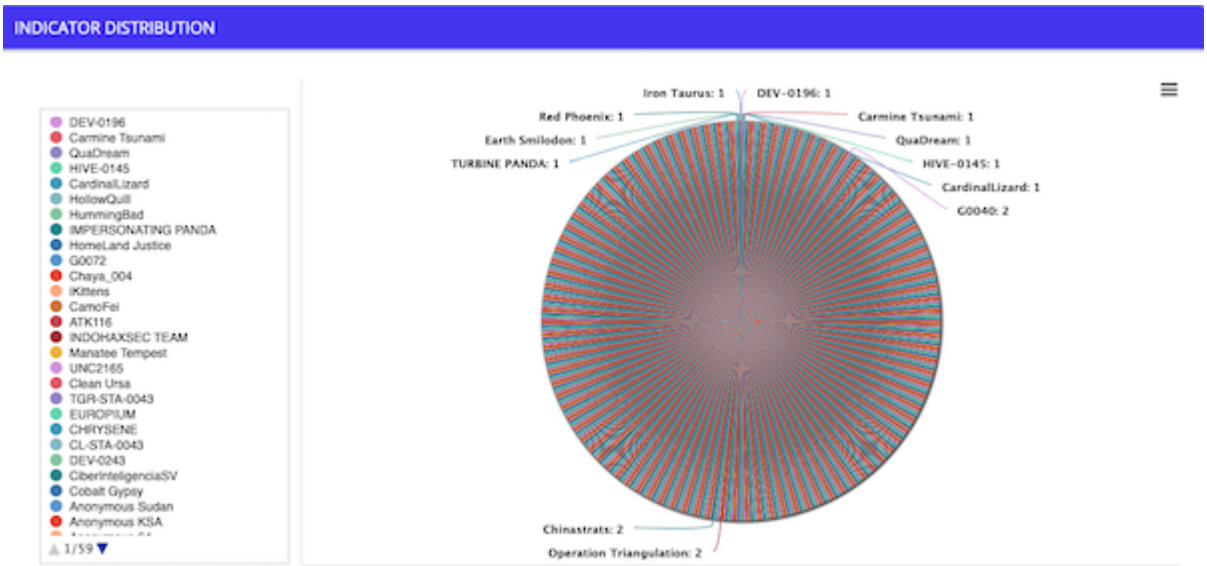


The following functions are available:

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.

Indicator Distribution Pie Chart

The Indicator Distribution pie chart shows you how many indicators are associated with all adversaries.



The following functions are available:

FUNCTION	DETAILS
Viewing more information about a selected value	Hover over a colored section of the pie chart to open a popup identifying the indicator, the number of times the indicator was found and what percentage of the total number of indicators it represents.
Hiding or unhiding one of the values from the pie chart	Click the indicator on the left of the pie chart to remove it; click a second time to reinstate it.
Printing the graph or saving it as a PNG, JPEG, PDF, or SVG	Click the hamburger menu ☰ and select the desired option.

Event Analytics Dashboard

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role:

- Action Permissions: Objects & Context - Objects (all object types) **OR** Data Access Permissions: Event
- Action Permissions: Artifact Management - Dashboards

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.

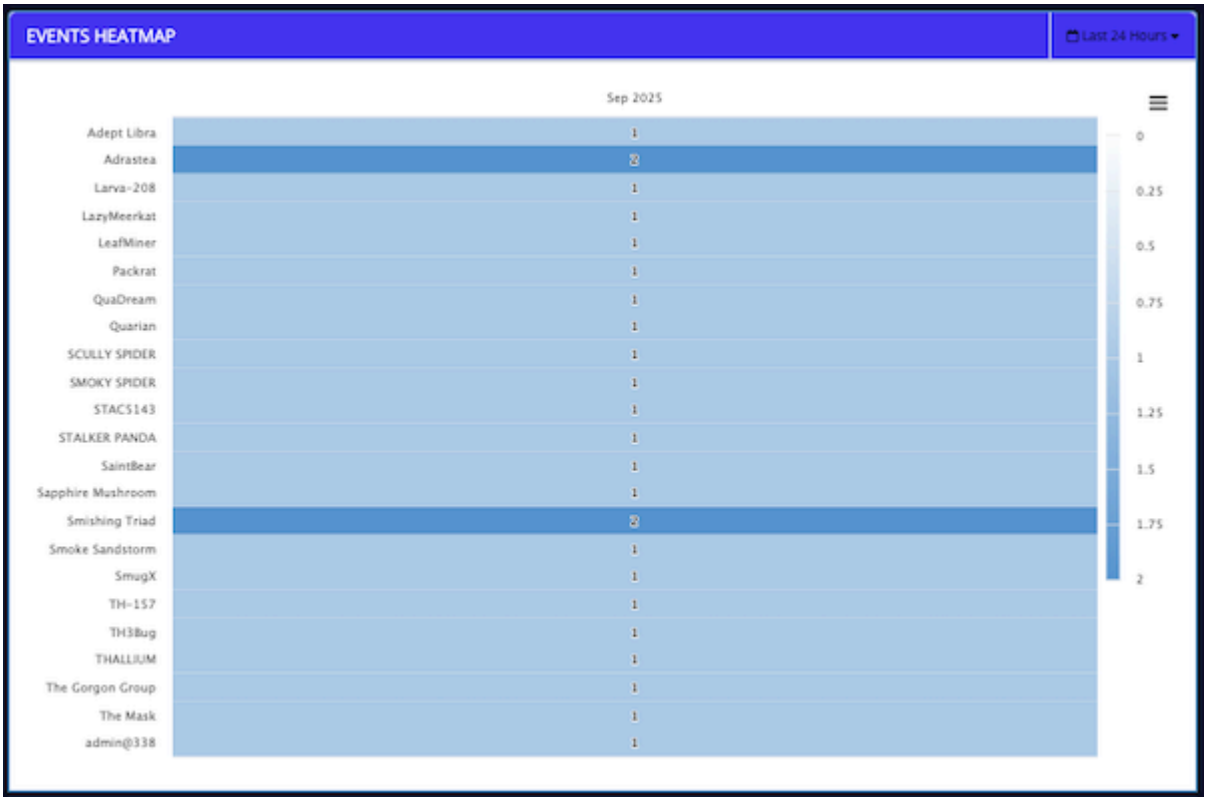
The following functions are available:

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 Page.
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.

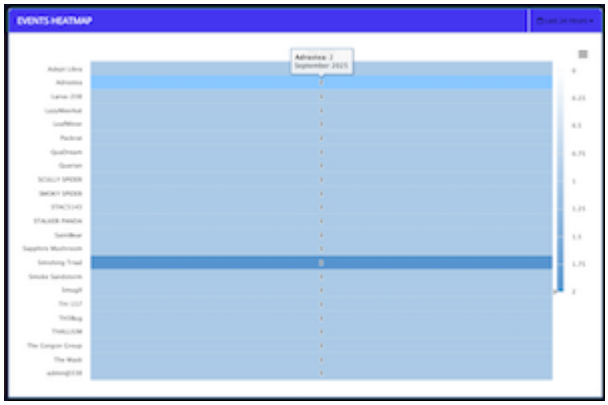
FUNCTION	DETAILS
Adjusting the time frame of the information displayed	Click the dropdown menu at the top right and select the desired time frame. You can select from: • Last 24 Hours • Last 7 Days • Last 30 Days • Last Year • User-set custom range
Printing or downloading the scatter plot as a PNG, JPEG, 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. 

FUNCTION	DETAILS
Adjusting the time frame of the information displayed	1. Click the dropdown menu at the top right and select the desired time frame. You can select from: ◦ Last 24 Hours ◦ Last 7 Days ◦ Last 30 Days ◦ Last Year ◦ User-set custom range
Printing the graph or saving it as a PNG, JPEG, PDF, or SVG	1. Click the hamburger menu ☰ and select the desired option.

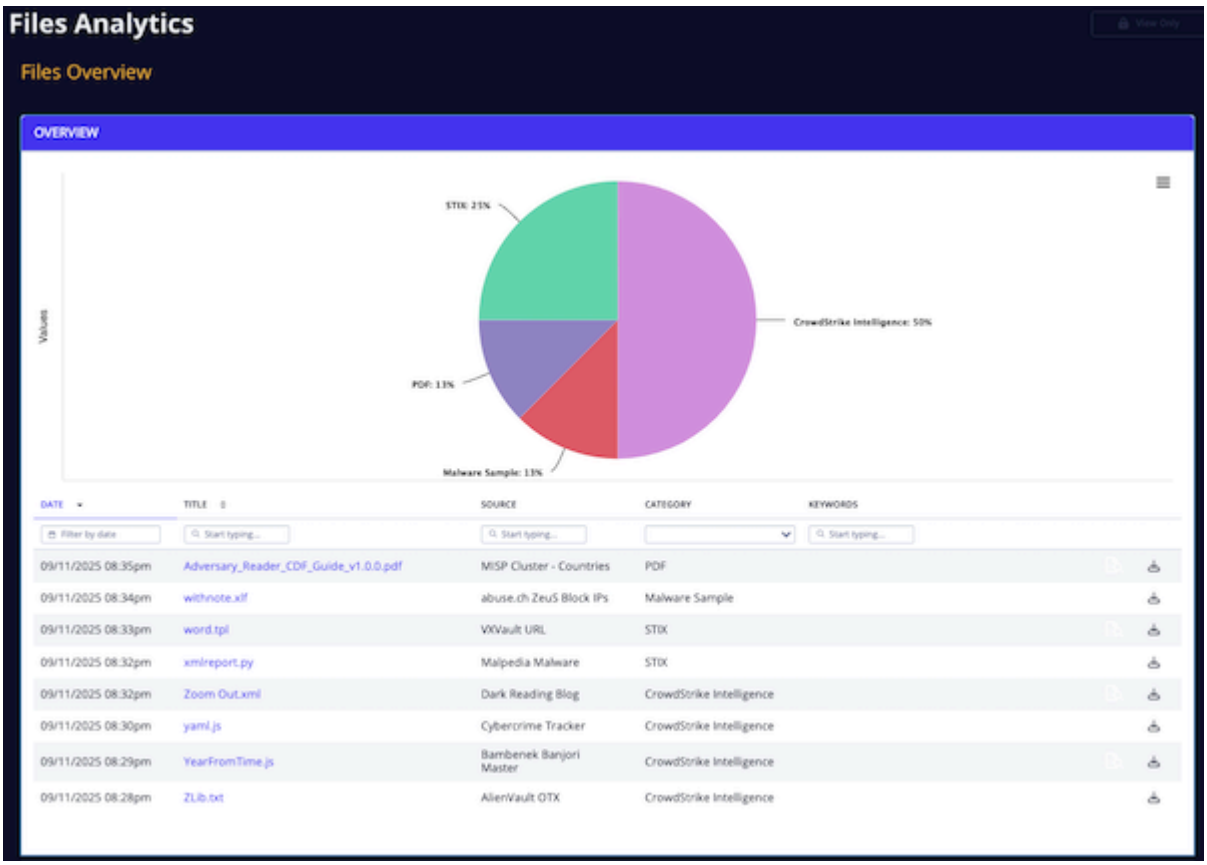
Files Analytics Dashboard

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role:

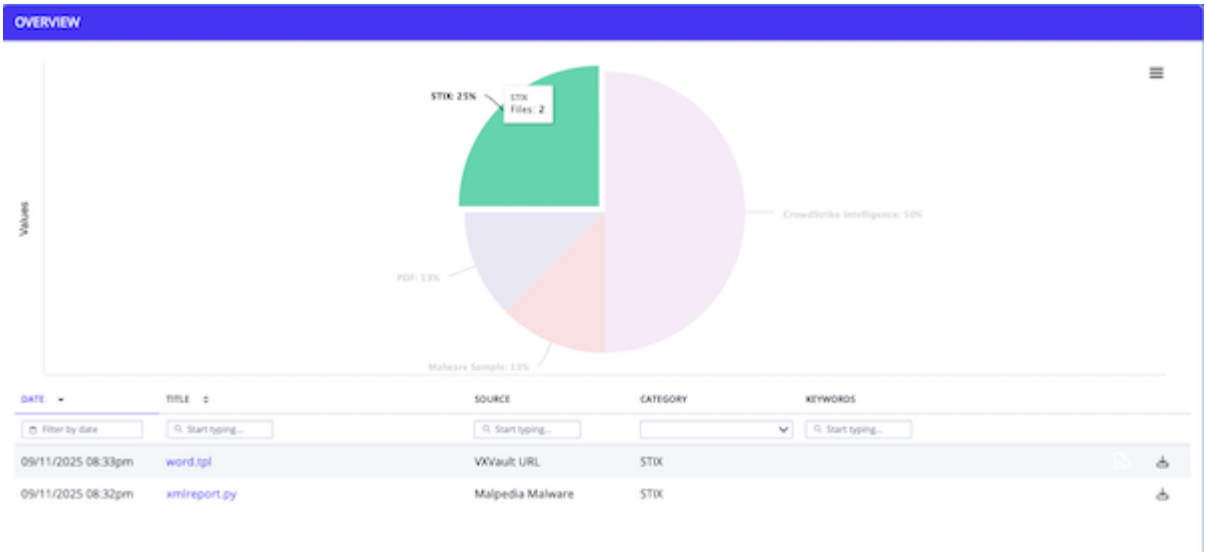
- Action Permissions: Objects & Context - Objects (all object types) **OR** Data Access Permissions: File
- Action Permissions: Artifact Management - Dashboards

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.

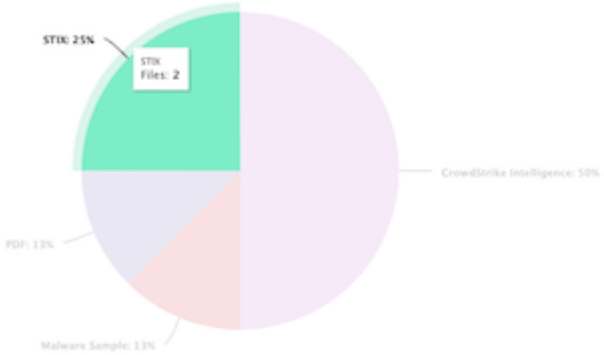


File Type Pie Chart

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

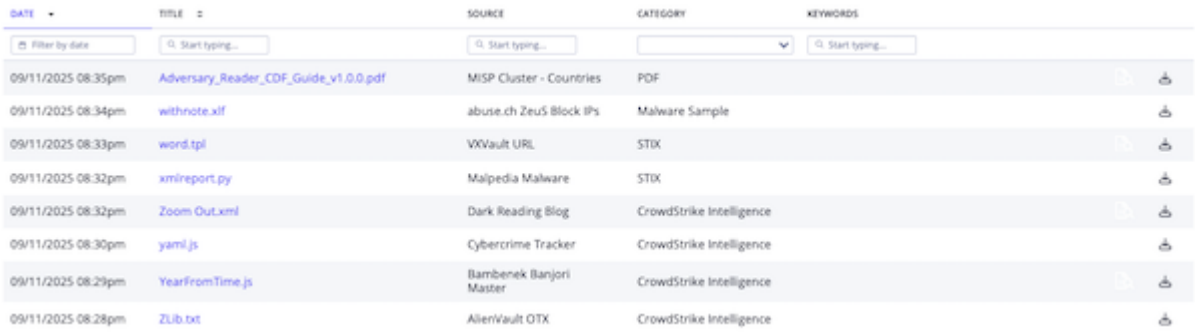


The following functions are available:

FUNCTION	DETAILS
Viewing more information about a selected file	Hover over a colored section of the pie chart to view the number that 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...
09/11/2025 08:35pm	Adversary_Reader_CDF_Guide_v1.0.0.pdf	MISP Cluster - Countries	PDF	
09/11/2025 08:34pm	withnote.xlf	abuse.ch ZeuS Block IPs	Malware Sample	
09/11/2025 08:33pm	word.tpl	VXVault URL	STIX	
09/11/2025 08:32pm	xmlreport.py	Malpedia Malware	STIX	
09/11/2025 08:32pm	Zoom Out.xml	Dark Reading Blog	CrowdStrike Intelligence	
09/11/2025 08:30pm	yaml.js	Cybercrime Tracker	CrowdStrike Intelligence	
09/11/2025 08:29pm	YearFromTime.js	Bambenek Banjori Master	CrowdStrike Intelligence	
09/11/2025 08:28pm	ZLib.txt	AlienVault OTX	CrowdStrike Intelligence	

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. You cannot preview a malware locked file.

Indicator Analytics Dashboard

THREATQ REQUIRED PERMISSIONS

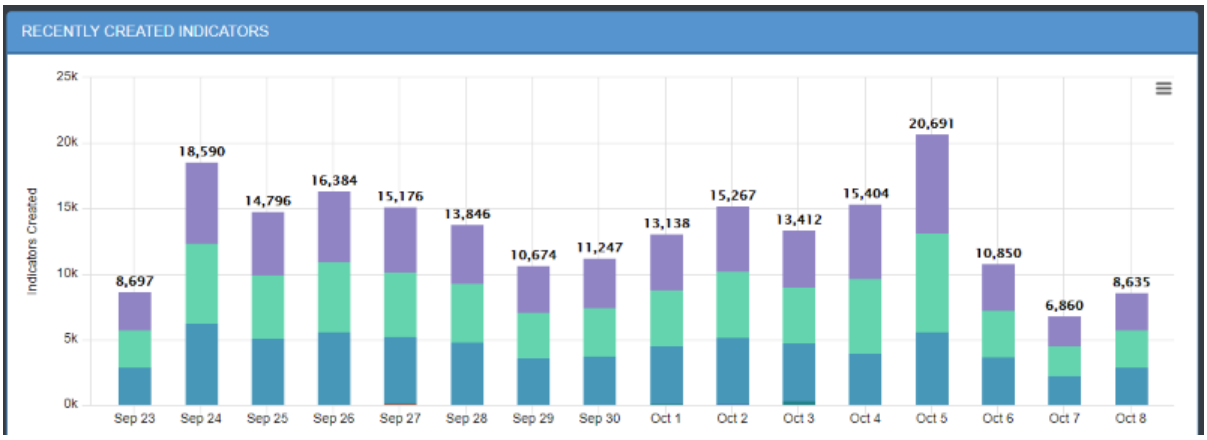
Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role:

- Action Permissions: Objects & Context - Objects (all object types) **OR** Data Access Permissions: Indicator
- Action Permissions: Artifact Management - Dashboards

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.

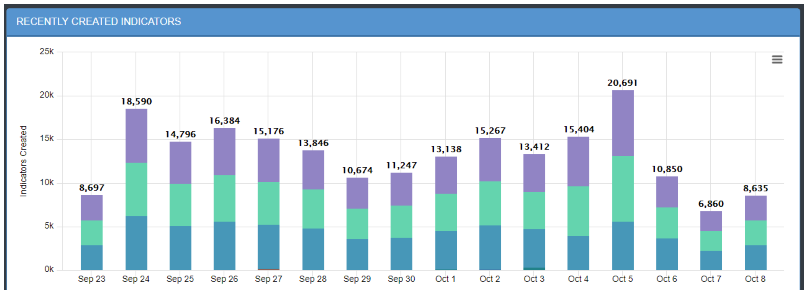
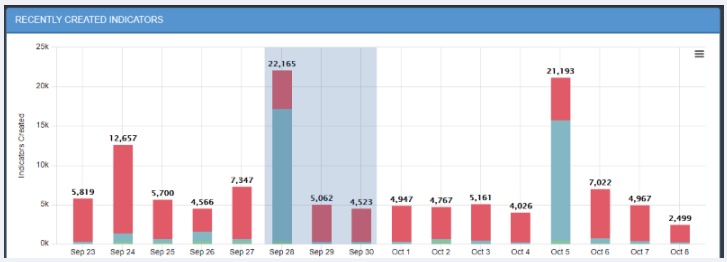
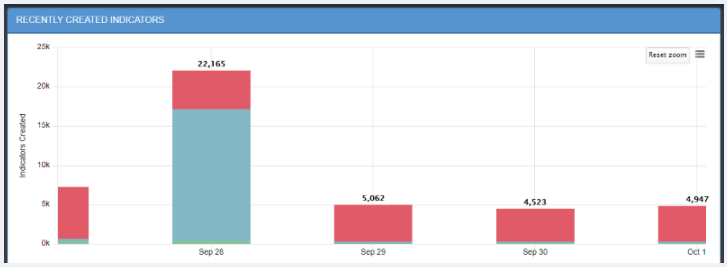
Recently Created Indicators Histogram

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.



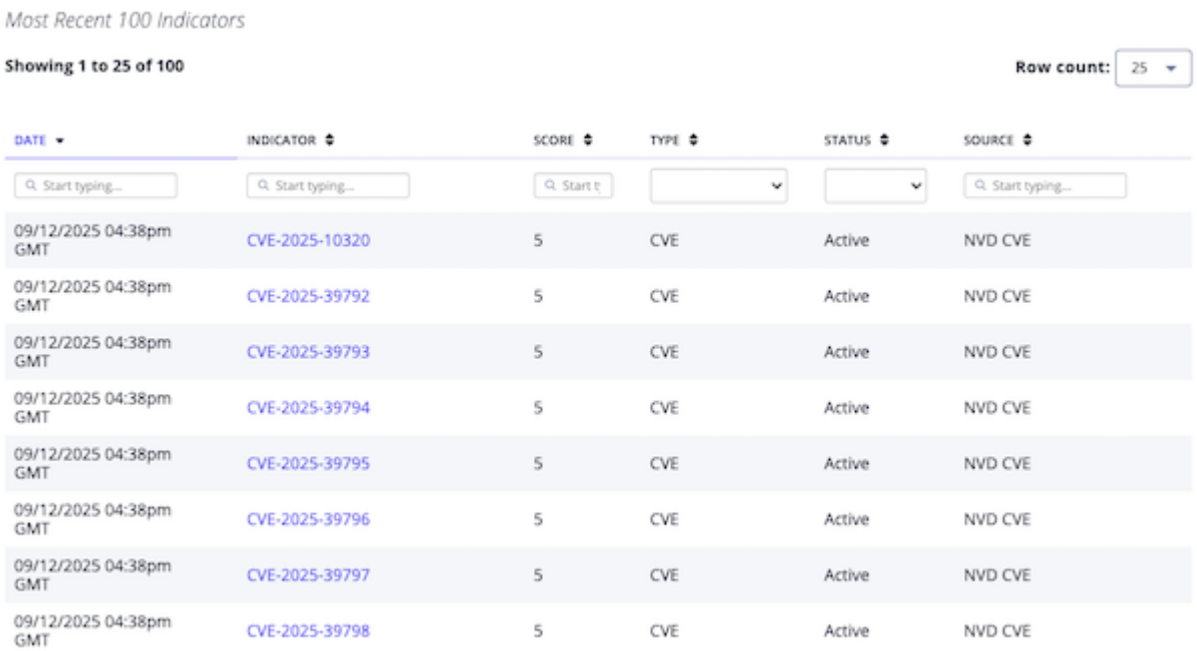
The following functions are available:

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.

FUNCTION	DETAILS
	
Zooming in for a closer view	1. Drag your mouse over a section of the histogram, and your view will be magnified.   2. Click **Reset Zoom** to return to the full histogram.
Printing the histogram or downloading it as a PNG, JPEG, PDF, or SVG file	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.

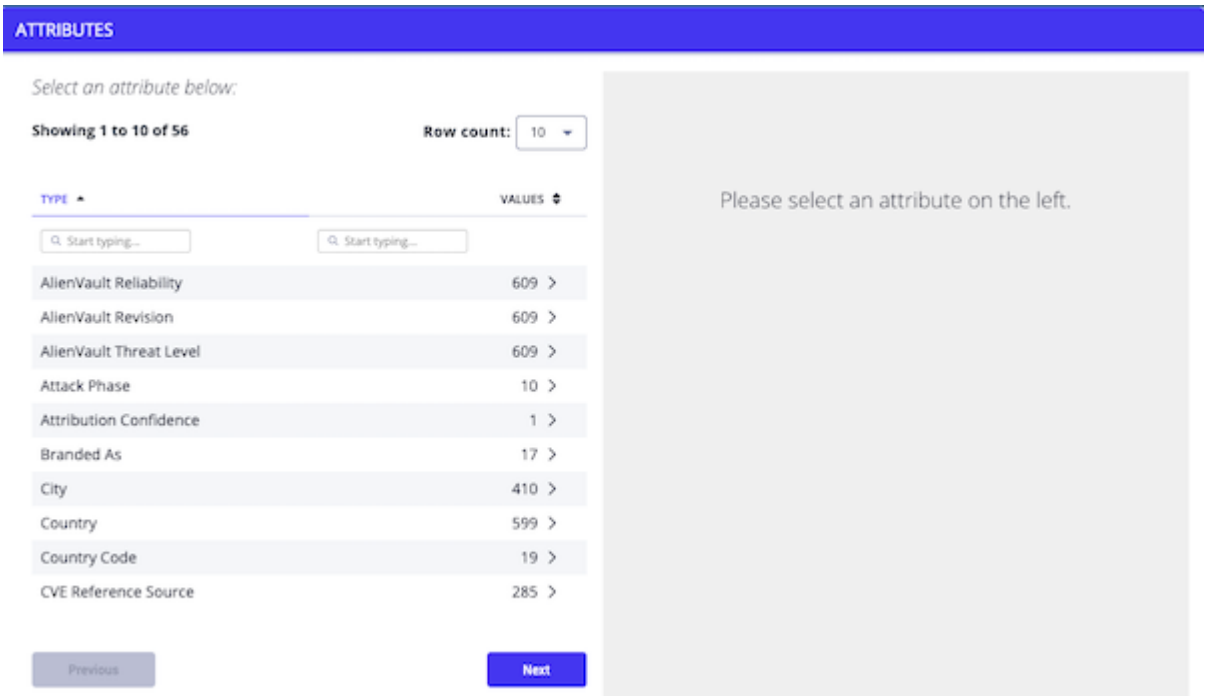


The following functions are available:

FUNCTION	DETAILS
Sort the Table	Click on the different table headings to sort 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

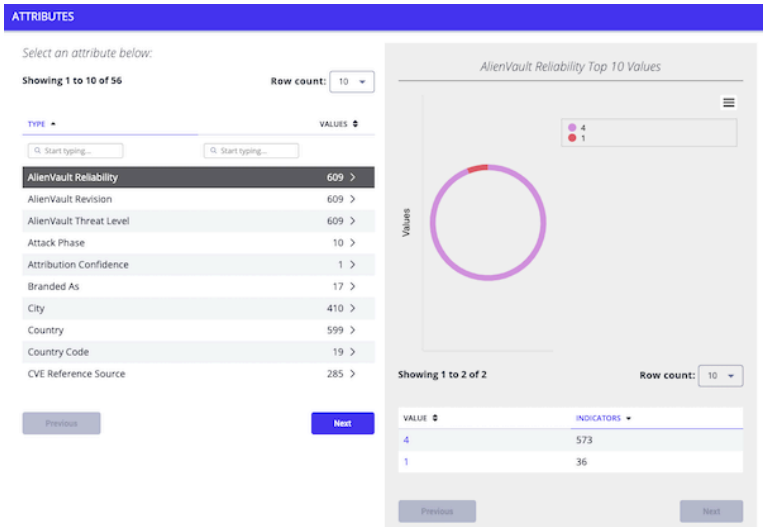
The attributes list on the left side displays attributes related to Indicators in your system.



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.
View More Information About a Selected Attribute	1. Click on an attribute row in the table to view additional information in the right pane. If there are multiple attributes with the same number of indicators, the pie chart key and the table below the pie chart may list attributes in a different order since the

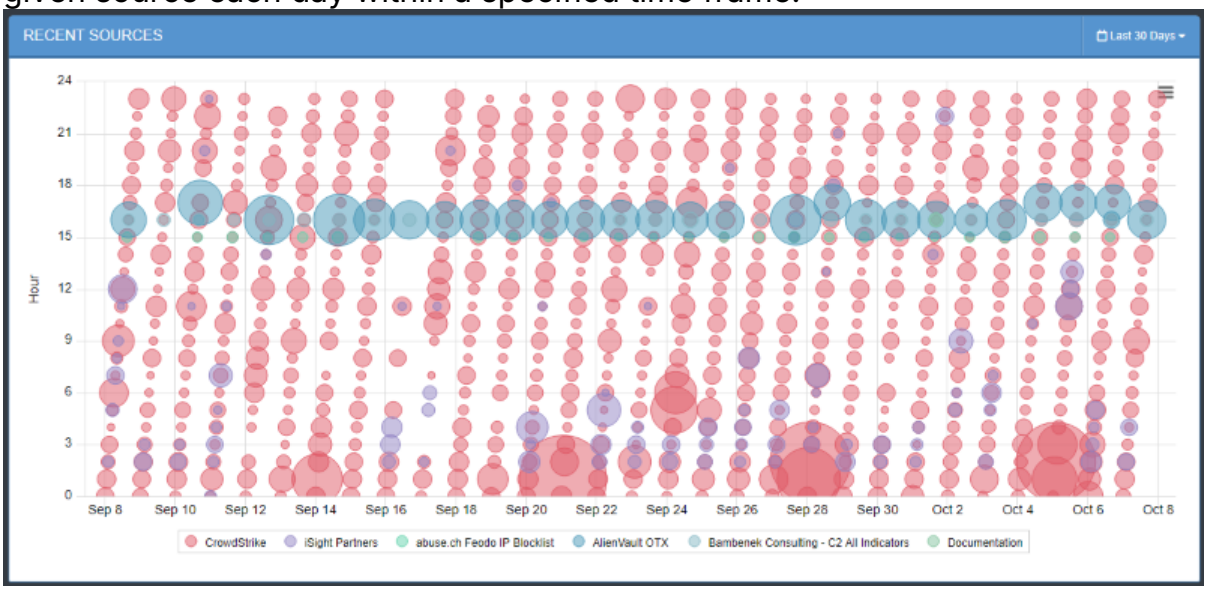
FUNCTION	DETAILS
	key and table use different sorting methods.



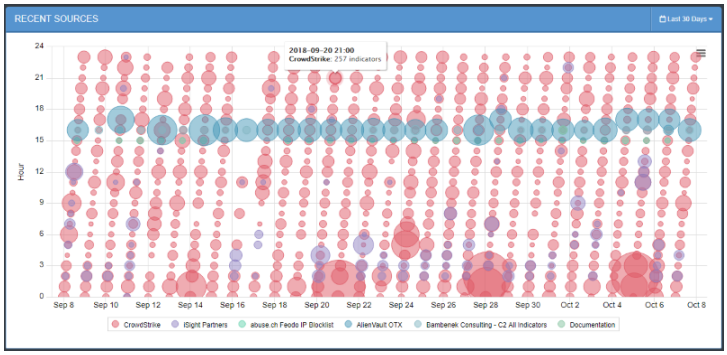
2. Hover the mouse over different portions of the pie chart to reveal the segment's value.
3. Click on an **Attribute Value** in the summary table below the pie chart to open the Advanced Search page with those attribute values applied.

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:

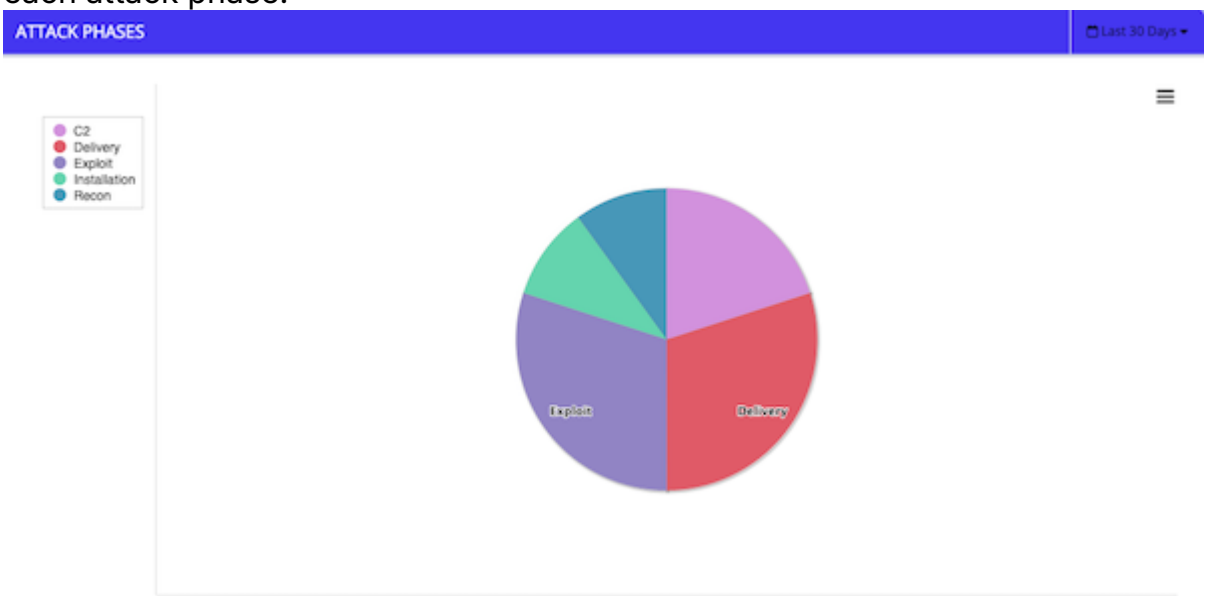
FUNCTION	DETAILS
View the Date and Number of Indicators from a Given Source	1. Hover the mouse over one of the scatter plot circles to view a popup with the Source, Date, Time and Number of Indicators.  2. Click on the one of the scatter plot circles to open the Advanced Search page with the specific filter settings used for that selection.
Adjust the Date Range of the Information Displayed	The default date range is 30 days.

FUNCTION	DETAILS
	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

FUNCTION	DETAILS
	◦ User-set custom range
Hide a Values from the Pie Chart	1. Click on a Attack Phase in the legend to the left of the pie chart to hide it. The Attack Phase will be removed from the pie chart and the source in the legend appear greyed out. 2. Click on the Attack Phase again to add it back to the pie chart.

Dashboard Widgets

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor

Custom Role:

- Action Permissions: Objects & Context - Objects (all object types) **OR** Data Access Permissions: object type
- Action Permissions: Artifact Management - Dashboards

Custom Dashboard Widgets allow you to build interactive dashboards that visualize and monitor threat intelligence data using configurable charts, tables, counters, and descriptive content. Each widget is powered by a data collection and can be customized to present the information most relevant to your analysts and stakeholders.

Available Widget Types

ThreatQ provides the following widget types for custom dashboards:

- **Bar Chart** – Compare objects across categories.
- **Count** – Display the total number of matching objects.
- **Description** – Add formatted text, images, and documentation.
- **Line Chart** – Visualize trends over time.
- **Pie Chart** – Display proportional distribution of objects.
- **Table** – Present detailed object data in tabular format.

Bar Chart Widget

The **Bar Chart** widget displays object counts grouped by a selected field, making it useful for comparing categories such as sources, tags, or object status.

Users can select individual bars to open the corresponding results in the Threat Library. If grouped by a date or time field (for example, **Modified At**), dates are displayed in **UTC**, regardless of the configured user or system time zone.

Objects matching multiple groups are counted once in each applicable group. Objects with scores greater than **10** are included in the **10** score bar.

Widget Parameters

FIELD	DESCRIPTION
Title	The title that will appear above the widget.
Automatically Update	The refresh time for the data. Options include: • every 2 minutes • every 5 minutes • every 15 Minutes • every 30 Minutes • ever 60 Minutes • Off
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. You have the option to group event and custom

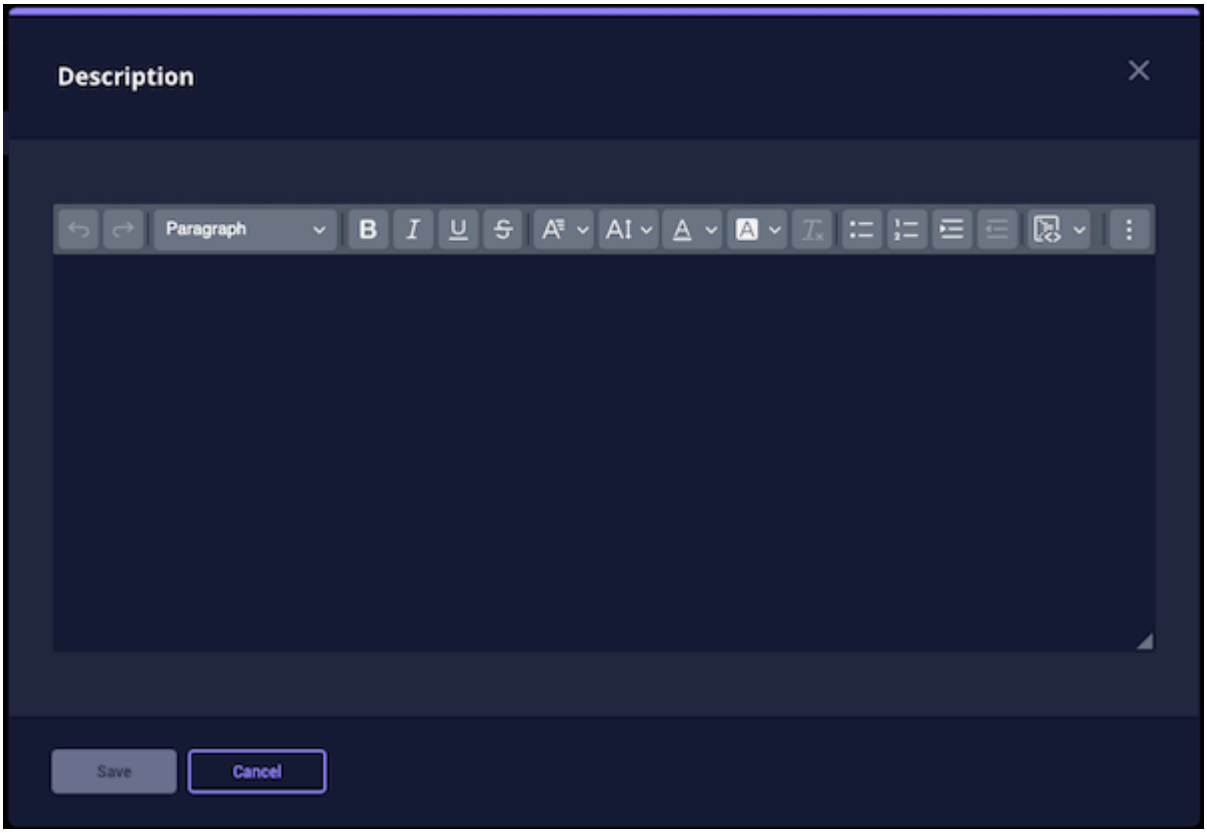
FIELD	DESCRIPTION
	objects by status and/or point of contact in bar chart widgets. The group by status option is displayed only if an Admin or Maintenance user has configured Event Statuses in the Object Management page. If you group your bar chart by a date/time, such as grouping by Modified At, the bar chart displays the time in UTC regardless of currently configured system or user timezone display.
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 Widget

The **Description** widget provides formatted text, images, instructions, or other contextual information that supports the dashboard. It includes a rich text editor for formatting content.

When adding images:

- Add captions after selecting the image alignment.
- Alternative text improves accessibility and is displayed only if the image cannot be loaded.
- Use the editor controls to insert lines above or below an image.
- Resize images to 25%, 50%, 75%, or restore the original size.

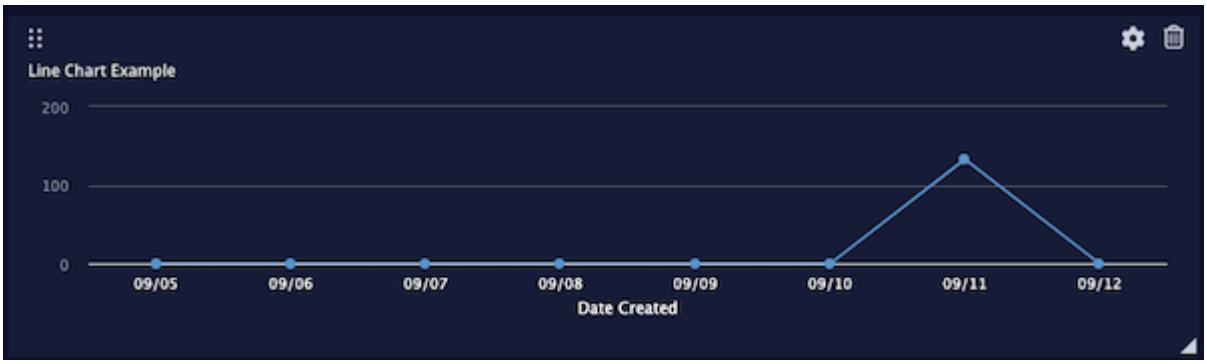


Line Chart Widget

The **Line Chart** widget displays object activity over time using one of the available date metrics.

Supported date metrics include:

- Date Created
- Last Modified
- Expiration Date (Indicators only)



FIELD	DESCRIPTION
Title	The title that will appear above the widget.
Automatically Update	The refresh time for the data. Options include: • every 2 minutes • every 5 minutes • every 15 Minutes • every 30 Minutes • ever 60 Minutes • Off
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)

FIELD	DESCRIPTION

	• 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 Widget

The **Count** widget displays the total number of objects matching the selected data collection and object type.

Optionally, the widget can emphasize results using configurable background colors when the count exceeds or falls below a specified threshold.

FIELD	DESCRIPTION
Title	The title that will appear above the widget.
Automatically Update	The refresh time for the data. Options include: • every 2 minutes

FIELD	DESCRIPTION
	• every 5 minutes • every 15 Minutes • every 30 Minutes • ever 60 Minutes • Off
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 Widget

The **Pie Chart** widget displays the proportional distribution of objects grouped by a selected field.

Users can click individual segments to view matching results in the Threat Library.

> Objects associated with multiple values are counted once in each applicable segment. As a result, the combined percentages may exceed 100%.

FIELD	DESCRIPTION
Title	The title that will appear above the widget.
Automatically Update	The refresh time for the data. Options include: • every 2 minutes • every 5 minutes • every 15 Minutes • every 30 Minutes • ever 60 Minutes • Off
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. You have the option to group event and custom objects by status and/or point of contact in pie chart widgets. The group by status option is displayed only if an Admin or Maintenance user has configured Event Statuses in the Object Management page.

Table Widget

The **Table** widget displays detailed object information in a configurable table.

Users can:

- Open an object by selecting its value.
- Preview object details using the **Preview** icon.
- Preview or download associated files when they are not malware locked.

Files marked as **malware locked** cannot be previewed.

FIELD	DESCRIPTION
Title	The title that will appear above the widget.
Automatically Update	The refresh time for the data. Options include: • every 2 minutes • every 5 minutes • every 15 Minutes • every 30 Minutes • ever 60 Minutes • Off
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. Click the Add Columns option to add more columns to your table.
Sorting	Select the column to sort the table and the order (ascending/ descending).

Widget Behavior Notes

Keep the following behaviors in mind when designing dashboards:

- Widgets automatically refresh based on the configured update interval.
- Interactive charts allow analysts to drill down into Threat Library results by selecting chart elements.
- Objects associated with multiple categories may appear in multiple chart segments, causing totals to exceed 100% for pie and bar chart groupings.
- Time-based bar chart groupings display timestamps in UTC regardless of the user's configured time zone.

Dashboard Management

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor

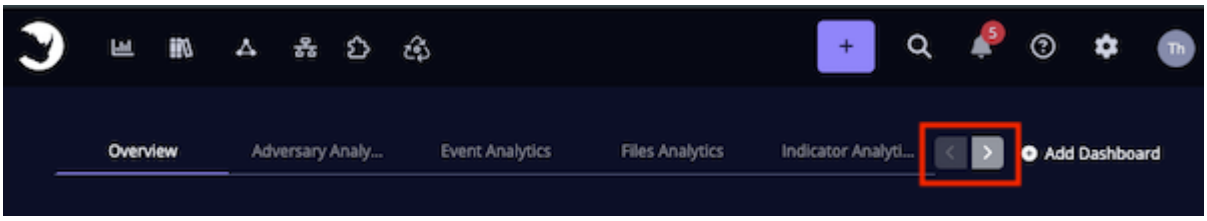
Custom Role:

- Action Permissions: Objects & Context - Objects (all object types) **OR** Data Access Permissions: object type
- Action Permissions: Artifact Management - Dashboards

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

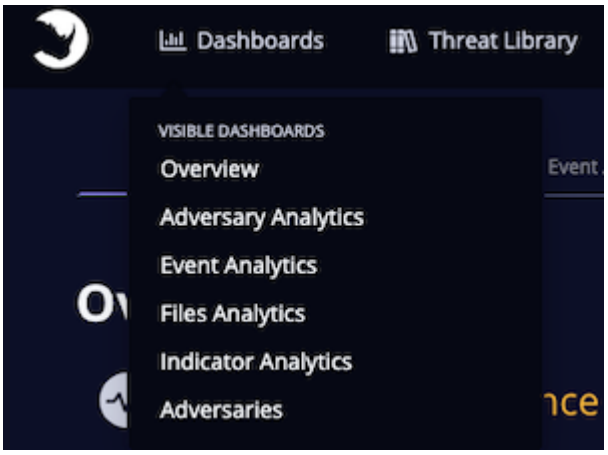
Accessing a Dashboard

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.



- 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:

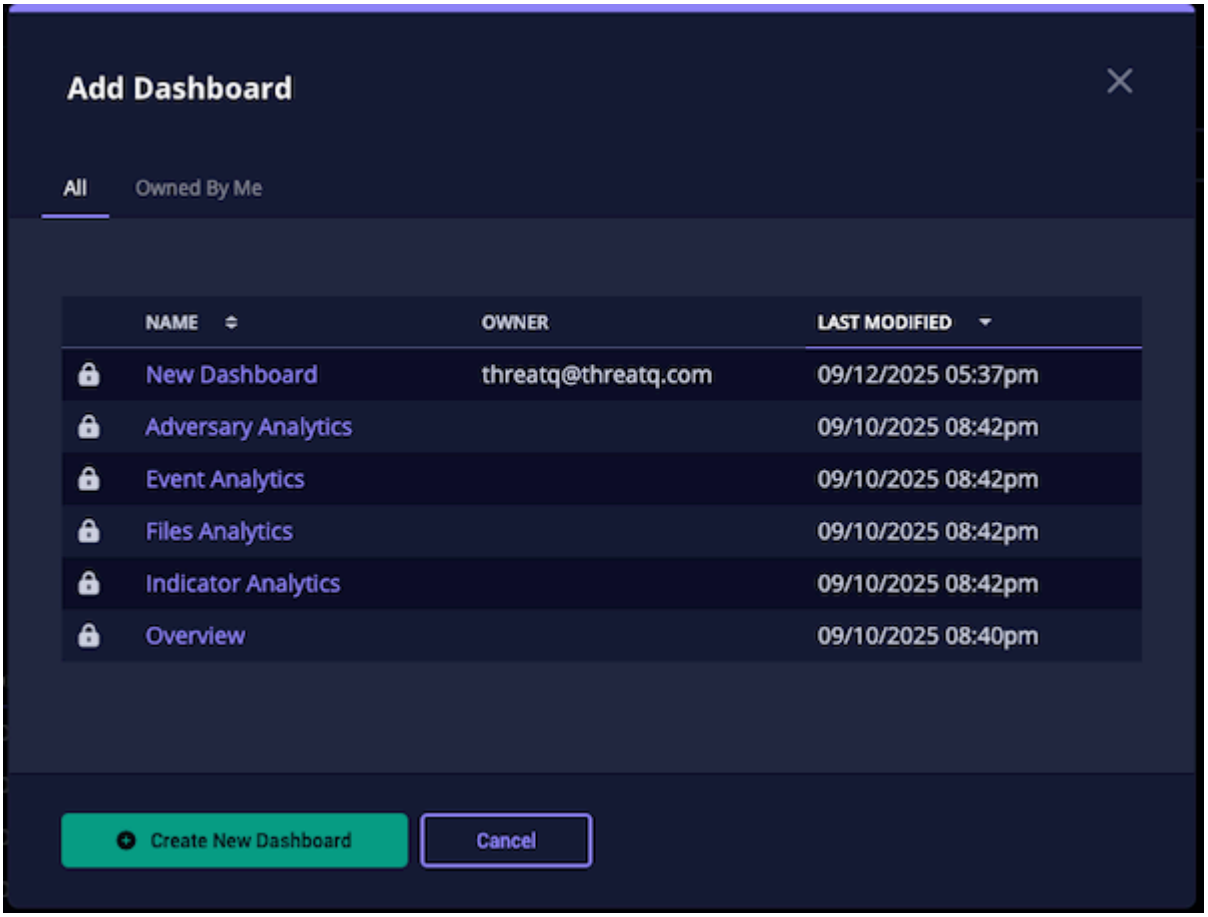
- Dashboard owner
- Date and time of the last change to the dashboard

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.



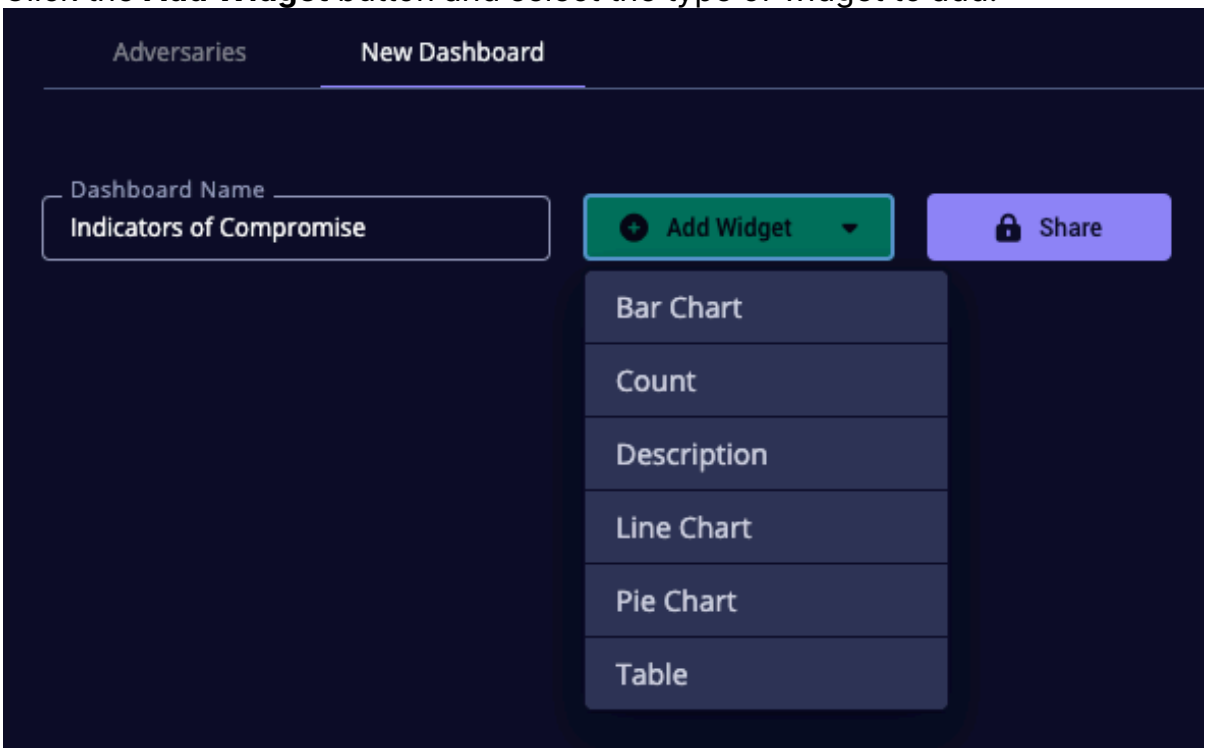
3. Click the dashboard you want to add to your view.

Creating a Dashboard

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

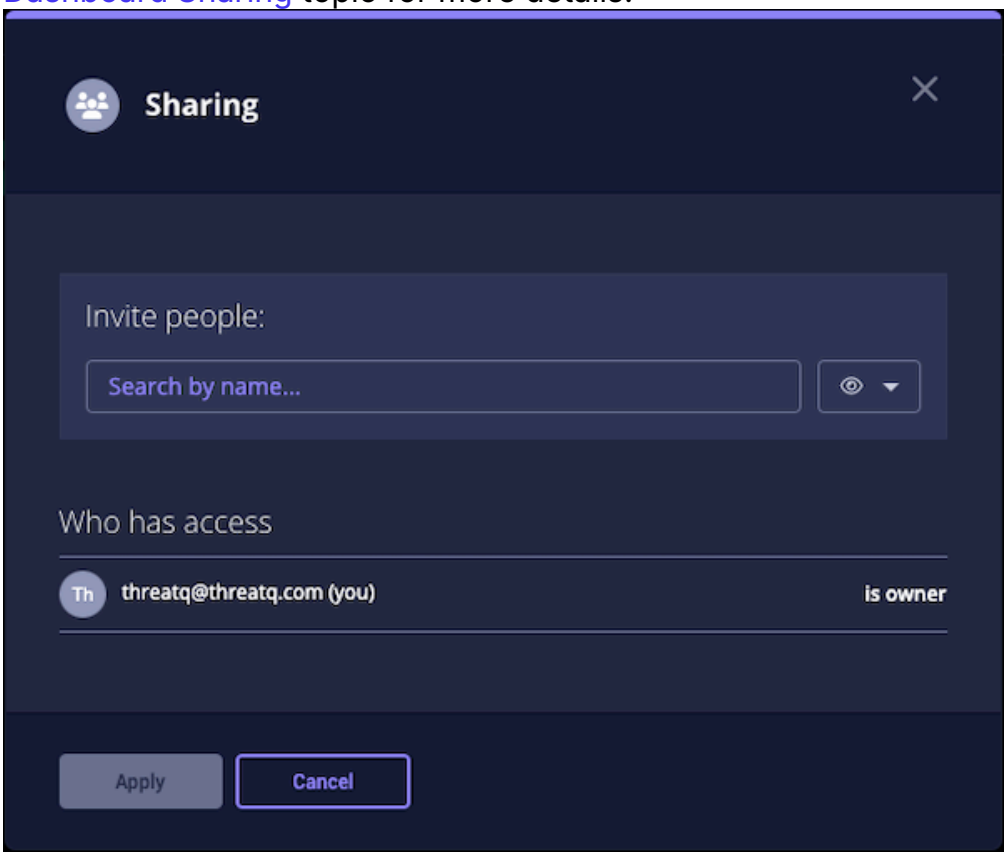
1. Navigate to the ThreatQ landing page.
2. Click one of the following options:
   - **Create New Dashboard** - If your view includes all the dashboards that you created and that are shared with you, click this link to begin creating a new dashboard.
   - **Add Dashboard** - If your view does not include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

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



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

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



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

Editing a Dashboard

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

1. Switch to the custom dashboard you want to edit.
2. Click the **Edit** button.
3. You can click the gear icon in the header of a widget to edit individual widget settings. You can click the delete icon to delete the widget.

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

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

Deleting a Dashboard

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

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

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

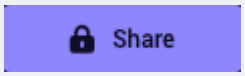
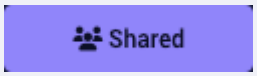
THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor

Custom Role:

- Action Permissions: Objects & Context - Objects (all object types) **OR** Data Access Permissions: object type
- Action Permissions: Artifact Management - Dashboards

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.

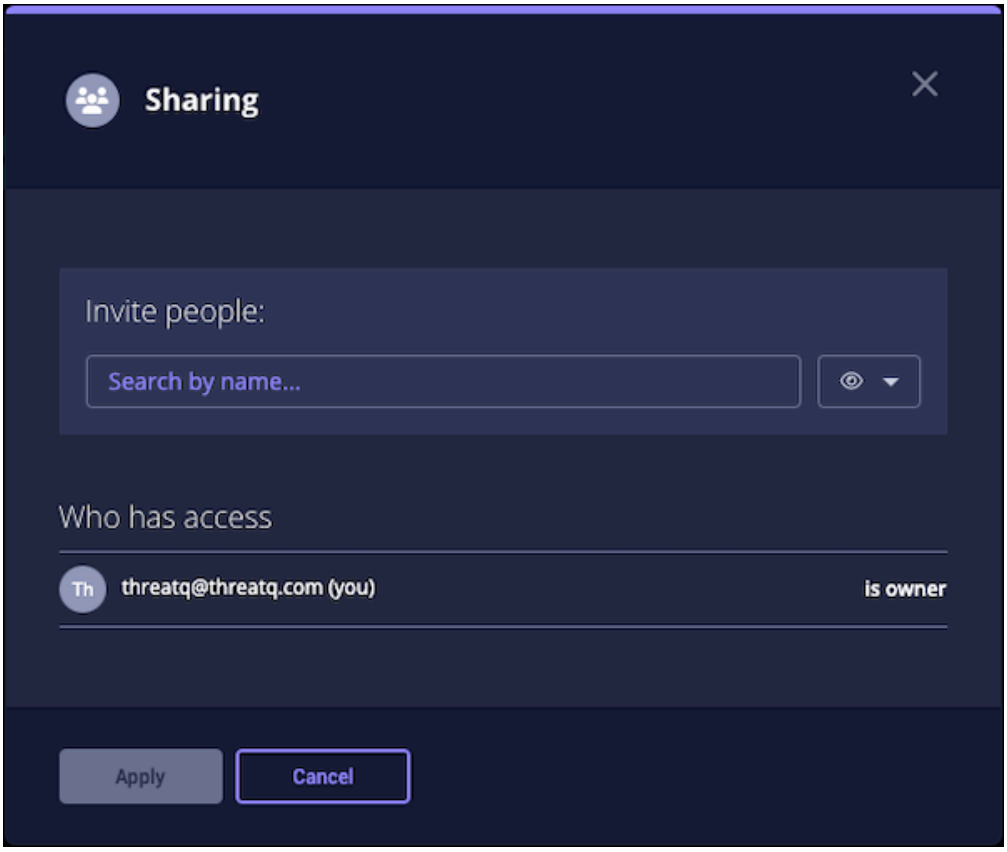
Sharing a Dashboard

Sharing dashboards does not override the Data Access permissions of the user with whom you share the dashboard. For example, if Joe shares an indicator dashboard with Sarah, whose role does not include Data Access permission for Indicators, she cannot view the dashboard.

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

1. Enter a dashboard's **Edit** view.
2. Click the **Share** button.
   The Sharing window allows you to select the user(s) to which you want to grant

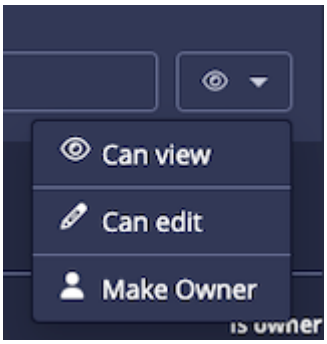
access.



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

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

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



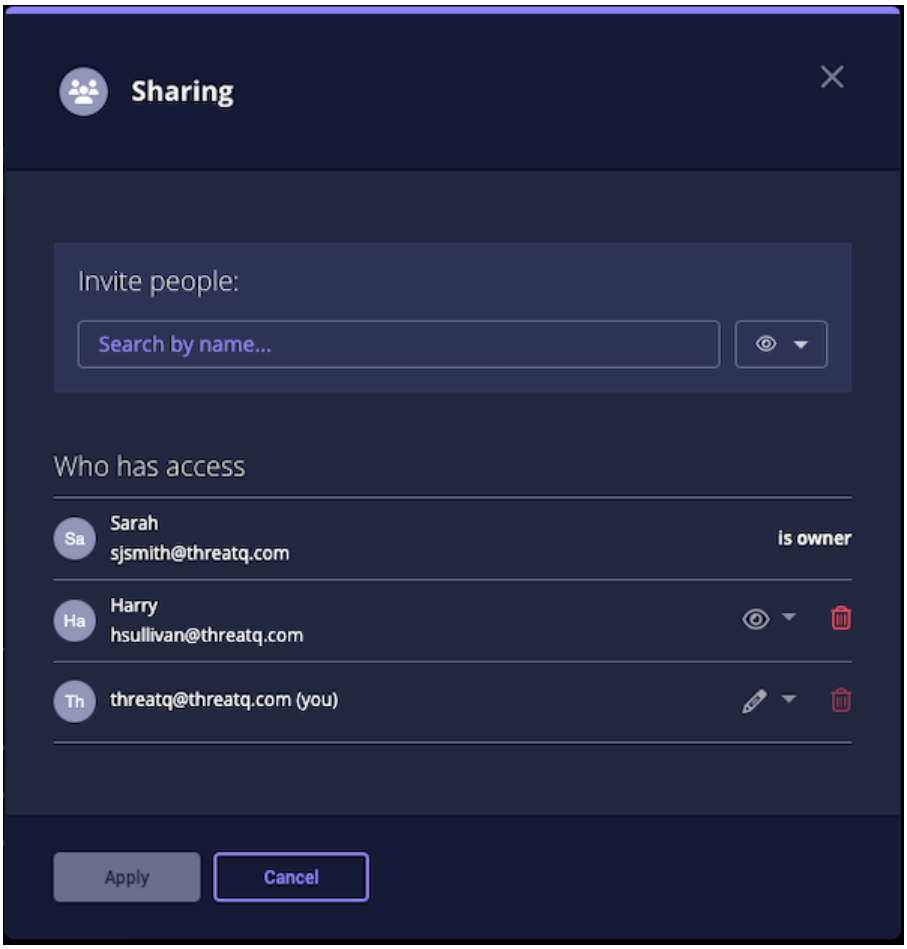
4. Use the search field to locate and select a user's name or the **Everybody (Public)** option. This option grants view-only access to all users.
   The user is now listed in the **Who has access** list. From this listing, you can change or delete the user's permissions.

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

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

Updating Dashboard Permissions

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



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

Shared Dashboards of a Deleted User

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

Dashboard Export

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role:

- Action Permissions: Objects & Context - Objects (all object types) **OR** Data Access Permissions: object type
- Action Permissions: Artifact Management - Dashboards

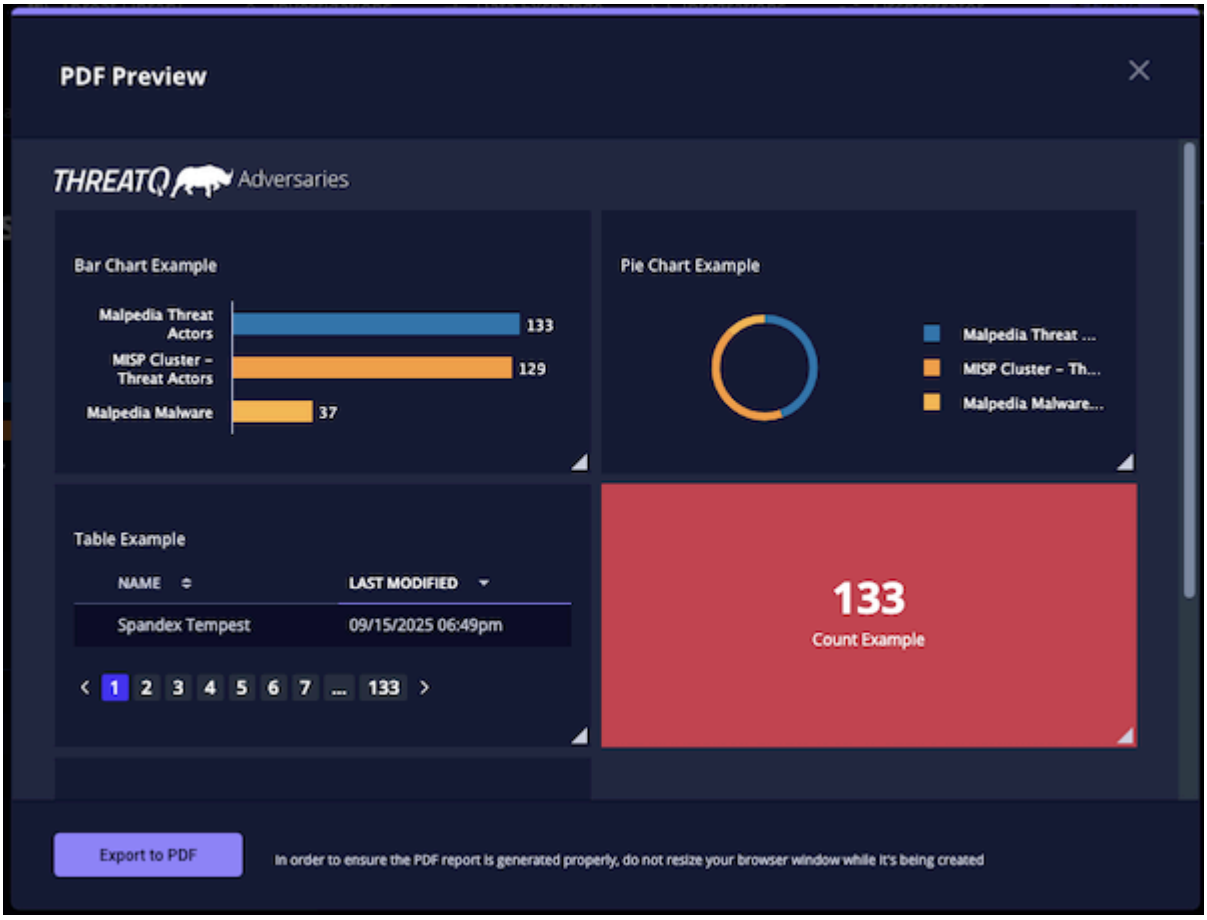
When you select a custom dashboard, the PDF Preview button gives you the option to export a PDF copy of all the widgets in the dashboard. The PDF preview window allows you to rearrange the widget order before you print and/or save the PDF.

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.



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

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

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

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

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

Sample PDF:

THREATQ Adversaries
Bar Chart Example
Malpedia Threat Actors
133
MISP Cluster – Threat Actors
129
Malpedia Malware
37
Pie Chart Example
Malpedia Threat ...
MISP Cluster – Th...
Malpedia Malware...
Table Example
NAME
LAST MODIFIED
Spandex Tempest
09/15/2025 06:49pm
1 2 3 4 5 6 7 ... 133
133
Count Example
Line Chart Example
160
0
09/08
09/09
09/10
09/11
09/12
09/13
09/14
09/15
Date Created

User View Management

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role:

- Action Permissions: Objects & Context - Objects (all object types) **OR** Data Access Permissions: object type
- Action Permissions: Artifact Management - Dashboards

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.

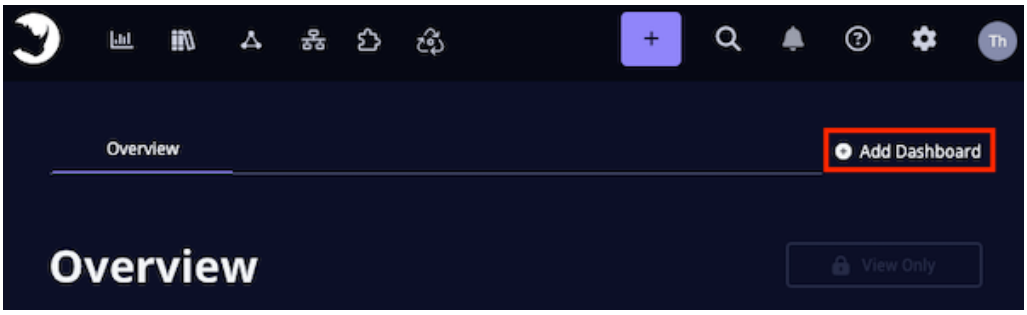
Any dashboard that is part of your User View will also be listed in the Dashboards dropdown menu.

Dashboards may appear empty if your user role's Data Access permissions for all widget object types are set to No Access.

Adding a Dashboard to Your View

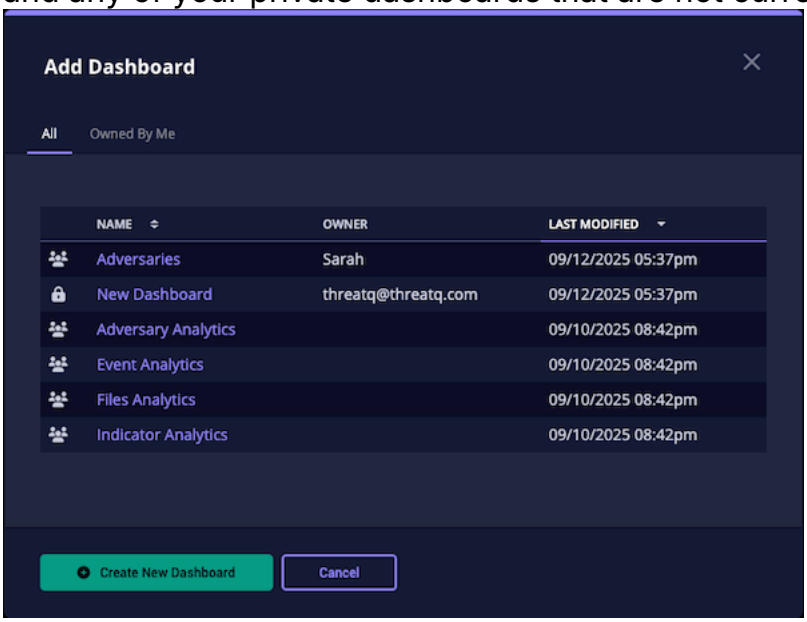
You can add dashboards that have been shared with you as well as your own private dashboards that are not currently part of your view.

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.

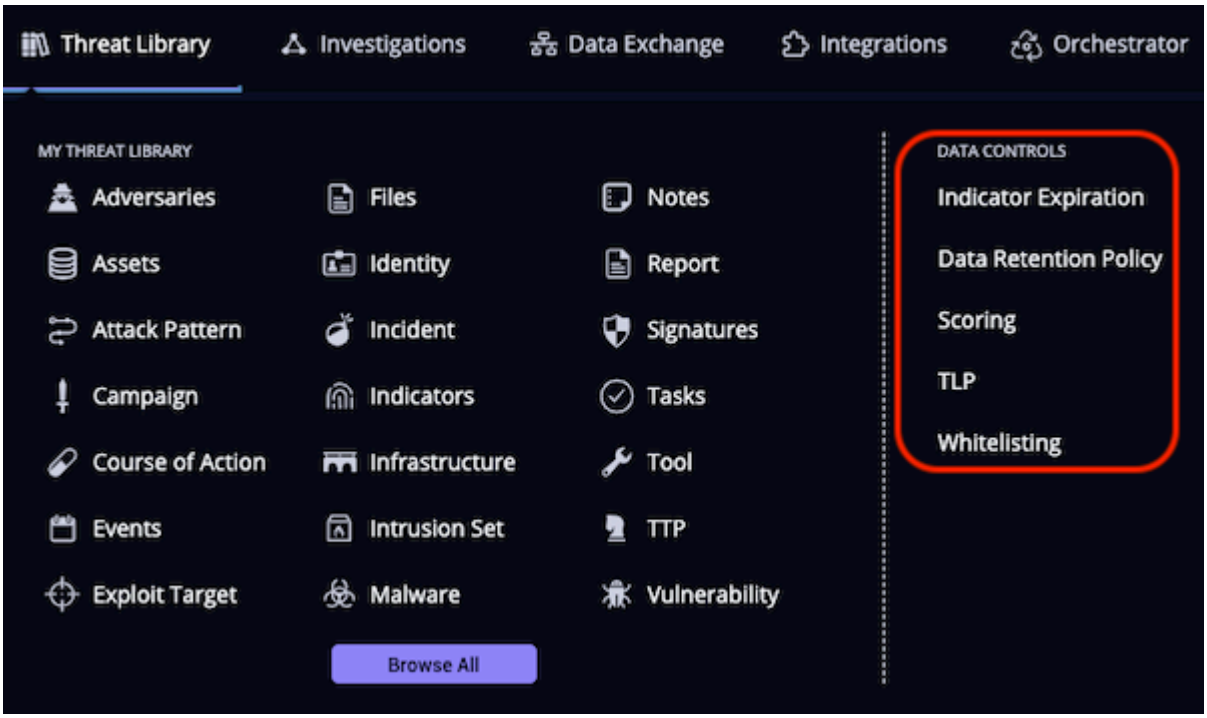
3. Drag the tab to your desired order and release the mouse button.

> 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 dropdown 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

THREATQ REQUIRED PERMISSIONS

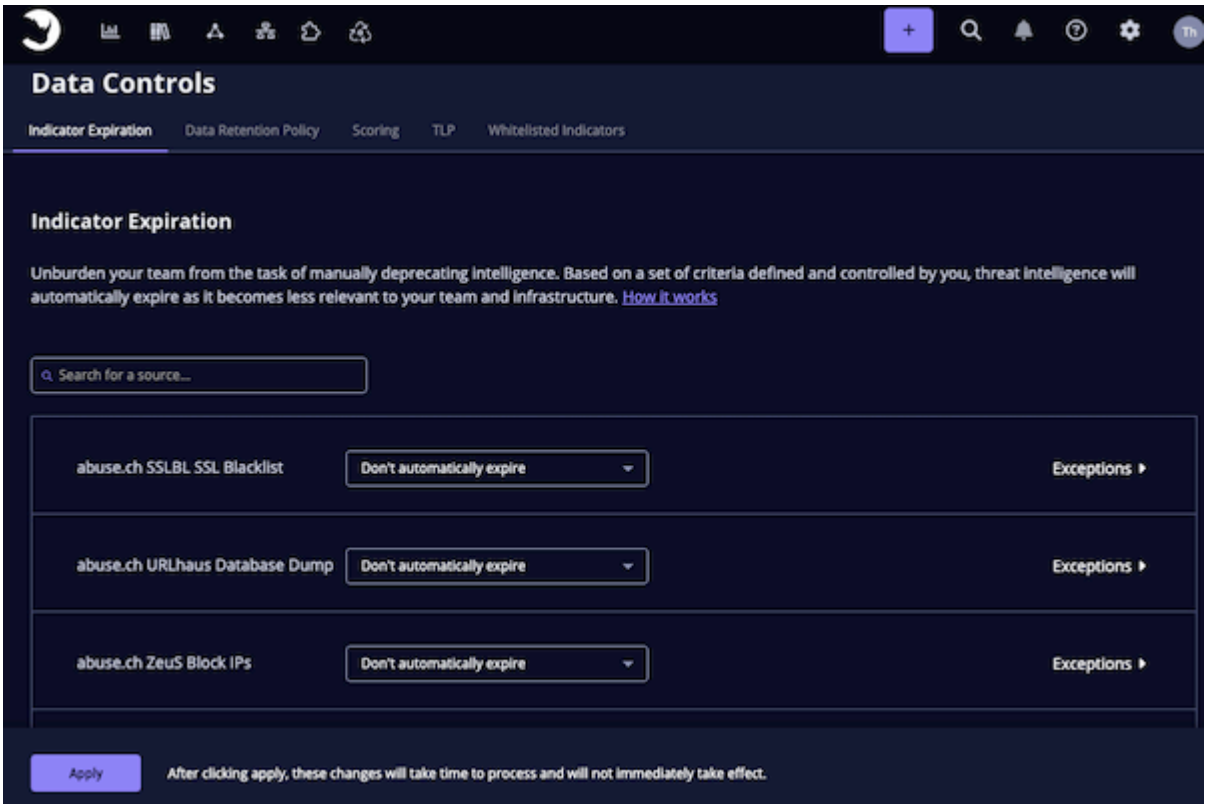
Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role - Action Permissions: Data Controls - Edit Indicator Expiration

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

Accessing the 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.



How ThreatQ Calculates Expiration Dates

SCENARIO	DESCRIPTION
Indicator Reported by Source with an Expiration Policy	If an indicator has an expiration date and it's reported by a new source that has an expiration policy, ThreatQ will set the expiration date using the policy with the greater expiration date.
Indicator Report by a Source with an Expiration Policy of Never Expire	If an indicator has an expiration date and it's reported by a new source that has an expiration policy of Never Expire, ThreatQ sets that indicator to Never Expire.
Indicator Reported by a Source with an Exception for that Indicator	If an indicator is reported by a source that has an exception for the indicator, the exception expiration date will be used regardless of the greater expiration date. An exception takes precedence over the source's expire policy.
Indicator Reported by Two Different Sources	If an indicator is reported by a source with an Expiration Policy and then reported by a second source with another Expiration Policy, the greatest expiration date is selected to set the expiration date. The expiration date will be set based on the date the second source reported the indicator.
Indicator Reported by Two Different Sources, one with an Exception	If an indicator is reported by a source that has an exception for the indicator and then reported by a second source, the greatest expiration date is selected despite the exception. The expiration date will be set based on the date the second source reported the indicator.

Selecting an Expiration Policy per Feed

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

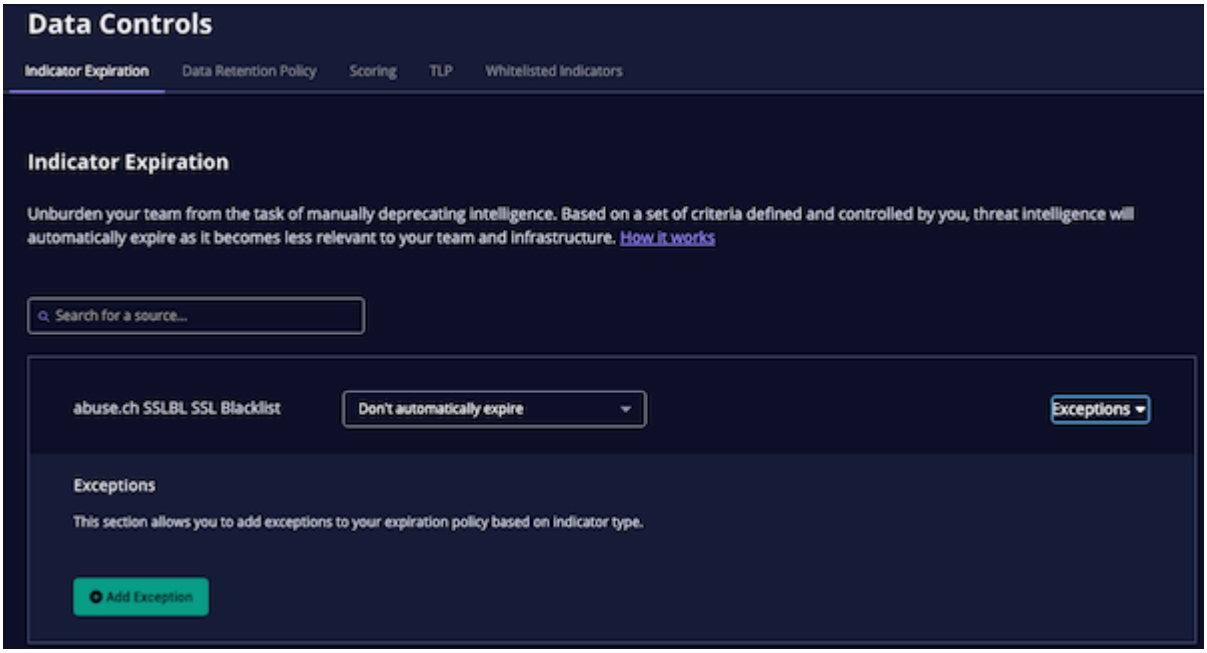
OPTION	DESCRIPTION
Don't automatically expire (No policy set)	ThreatQ sets all feeds to **Don't Automatically Expire** until an analyst decides otherwise. When set, indicators reported from this specific feed do not have an expiration date automatically applied to them. If an indicator is reported by Source A (an intelligence feed without an expiration policy), and is later reported by Source B (an intelligence feed that expires data in 7 days), ThreatQ sets the indicators to automatically expire in 7 days.
Automatically Expire Indicators	When setting a specific intelligence feed to **Automatically Expire Indicators**, ThreatQ requires you to provide a specific number of days. After you configure this setting, it applies to all intelligence currently in the system, as well as new intelligence as it is ingested. ThreatQ calculates the appropriate expiration date based on the number of days from ingestion. Once an indicator's expiration date is met, its status changes to **Expired**.
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 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.
>
> 2 Exceptions

4. Click **Add Exception**.
5. Select the **Indicator Type** from the dropdown.
6. Enter the number of days after the item has been ingested before expiring.

   Repeat steps 4-6 to add multiple

7. Click on **Delete** next to the row to delete an exception.
8. Click on **Save**.

Applying Expiration Policy Changes to Data

When updating an expiration policy, the system now applies the update to all selected existing data in the platform to honor the new policy. This process can take a while based on system resources and the number of indicators in the system.

Refer to the following table for estimates on the total time required for the system to apply the selected policy to existing data, based on the following criteria:

- Dataset: 6 Million Indicators
- System Specifications: 32GB VM 4 vCPU

INDICATORS TO RESET EXPIRATION OUT OF 6M TOTAL INDICATORS	RESET AND RECALCULATE EXPIRATION	EXPIRE INDICATORS	TOTAL TIME FOR RESET
50,000	3 hours and 30 minutes	53 seconds	3 hours 31 minutes
100,000	4 hours and 51 minutes	1.8 minutes	4 hours 53 minutes
200,000	10 hours 20 minutes	3.5 minutes	10 hours 24 minutes
1.2 million	2 days 7 hours 4 minutes	35 minutes	2 days 7 hours 40 minutes
3.1 million	3 days 16 hours 42 minutes	3.5 hours	3 days 20 hours
5.3 million	4 days 7 hours 17 minutes	4.7 hours	4 days 12 hours

Common Expiration Policy Scenarios

SCENARIO	DESCRIPTION
An indicator is reported by a single source (with an expiration policy)	1. On 10/1, Source A reports the indicator and the expiration date is set to 10/8. 2. When the date switches from 10/7 to 10/8, this indicator is queued to have its status changed to **Expired**.

SCENARIO	DESCRIPTION
An indicator is reported by Source A (with an expiration policy of 7 days) and 3 days later is reported by Source B (with an expiration policy of 10 days).	1. On 10/1, Source A reports the indicator and the expiration date is set to 10/8. 2. Source B reports the same indicator 3 days later (10/4). The indicator's expiration date is set using the greatest expiration date between the two sources. In this example, the new expiration date will be 10/14 (10 days from when it was reported by Source B). 3. When the date switches from 10/14 to 10/15, this indicator is queued to have its status changed to **Expired**.
An indicator is reported by Source A (with an expiration policy of 7 days) and is later reported by Source B (with an expiration policy of Never Expire).	1. On 10/1, Source A reports the indicator and the expiration date is set to 7 days. 2. Source B reports the same indicator 3 days later with a policy of **Never Expire**. The indicator’s expiration date is removed and the indicator is now set to **Protect from auto-expiration**.
A FQDN indicator is reported by Source A (with an expiration policy of 10 days with an exception for 5 days for FQDN indicators) and is later reported by Source B (with an expiration policy of 15 days).	1. On 10/1, Source A reports the FQDN indicator and the expiration date is set to 10/6. An exception takes precedence over the source’s expire policy. 2. Source B reports the same indicator 1 day later (10/2). The indicator's expiration date is set using the greatest expiration date between the two sources. In this example, the new expiration date will be 10/17 (15 days from when it was reported by Source B).

SCENARIO	DESCRIPTION
	3. 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).**	1. On 10/1, an indicator is in ThreatQ with a status of **Expired**. 2. On 10/1, Source A reports the indicator. The status of the indicator does not change.
• **An indicator is currently set to Expired and is reported by Source A (with an expiration policy of Never Expire).**	1. An indicator is in ThreatQ with a status of Expired. 2. Source A, with an expiration policy of Never Expire, reports the indicator. The 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).**	1. On 10/1, an indicator is in ThreatQ with a status of **Expired**. 2. On 10/1, Source A reports the indicator. The status of the indicator changes to whatever the default status is for Source A and the expiration date is set to 10/8.

SCENARIO	DESCRIPTION
	3. When the date switches from 10/7 to 10/8, this indicator is queued to have its status changed to **Expired**.
• **An indicator is currently set to Expired and is reported by Source A (with an expiration policy of Never Expire).**	1. An indicator is in ThreatQ with a status of Expired. 2. Source A, with an expiration policy of Never Expire, reports the indicator. The expiration of that indicator changes to Protect from auto-expiration.

Data Retention Policy

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role - Action Permissions: Data Controls - Edit Data Retention Policy

The ThreatQuotient team strongly recommends that you disable your DRP when making changes to an associated data collection and then reviewing the Calculate Impact option before re-enabling DRP to prevent the unintended deletion of system objects. See the Data Retention Policy Bug product alert for more details. It is also 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.

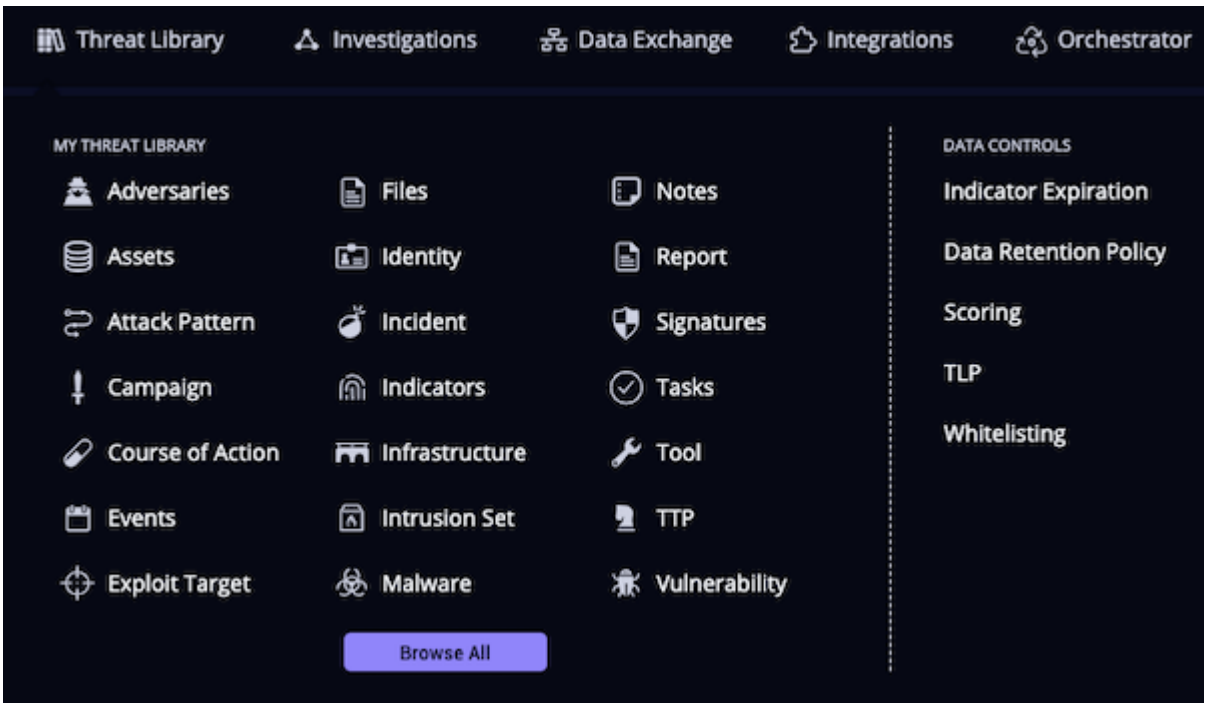
After you enable your data retention policy, ThreatQ provides updates on the associated object deletions through system notifications and the Job Management page.

Tips and Tricks

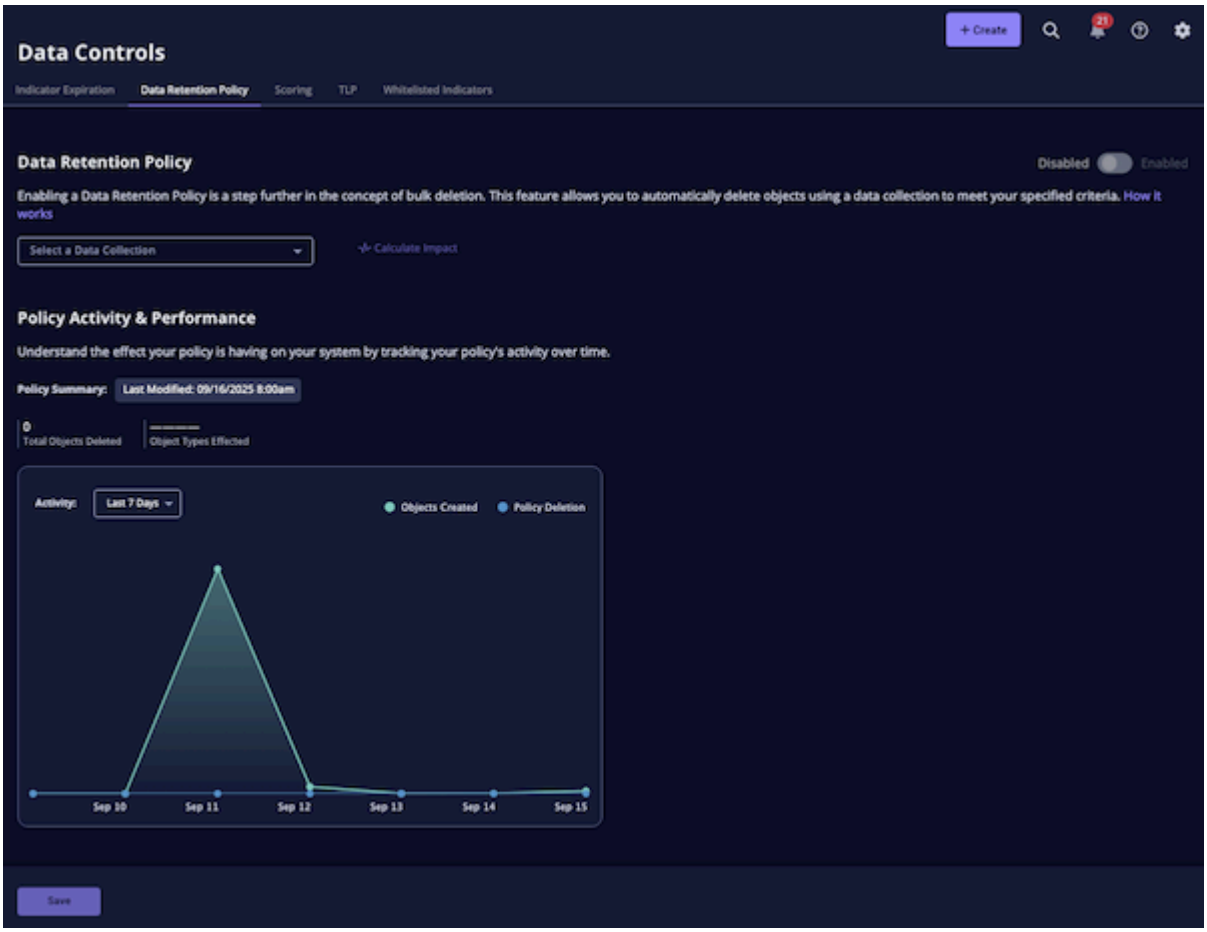
- If you assign an unshared data collection to the data retention policy, all users are automatically granted view-only permissions for the data collection.
- If you disable the data retention policy, the Policy Activity & Performance graph continues to track created objects.

Accessing the Data Retention Policy Page

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



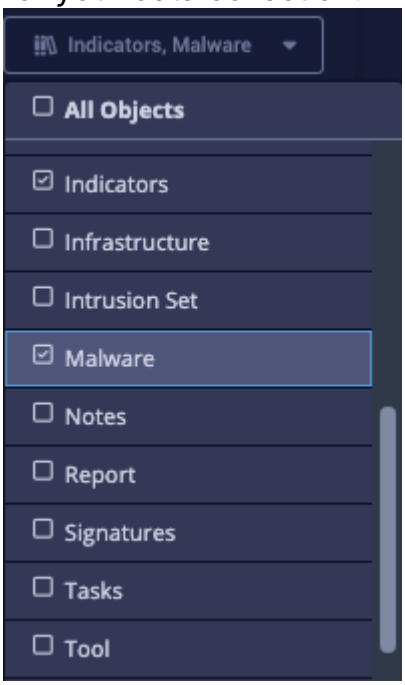
The Data Controls page is displayed with the Data Retention Policy tab selected.



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 you assign an unshared data collection to the data retention policy, all users are automatically granted view-only permissions for the data collection.

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:
   - The system creates and begins processing the first job to apply the data retention policy you configured.
   - 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.

Scoring Algorithms

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role - Action Permissions: Data Controls - Edit Scoring, See the Interdependent Permissions topic.

ThreatQ scoring algorithms automatically assign and update scores for supported objects based on criteria defined by your organization. Scoring helps analysts prioritize the threat intelligence most relevant to their environment. For stops on manually setting an object's score, see the Manually Setting an Object's Score topic.

Scoring algorithms can apply to the following object types:

- Indicators
- Adversaries
- Vulnerabilities

Scoring algorithms for adversaries and vulnerabilities can only be configured using attribute-based criteria on the **Attributes** tab.

How Scoring Works

Scores indicate the relative priority of an object. The scoring scale ranges from -10 to 10:

- 10 represents Very High priority.
- 0 represents a neutral score and is the default for indicators.
- -10 represents Very Low priority.

A higher score increases the priority of an object.

When you configure or update a scoring algorithm, ThreatQ recalculates the scores of applicable objects. Processing may take time, so changes might not appear immediately in the Threat Library.

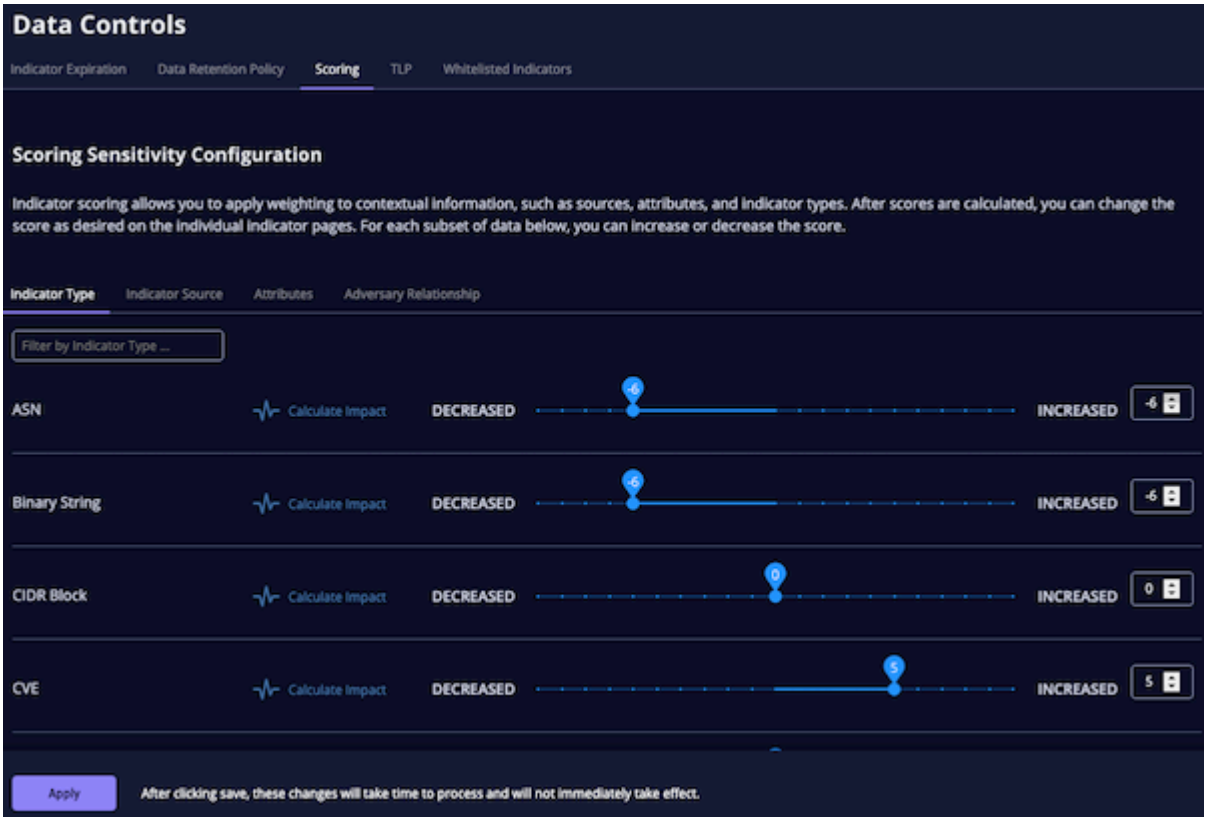
Scoring Criteria

The Scoring Sensitivity Configuration page provides the following criteria sorted by tabs:

CRITERIA	DESCRIPTION	SUPPORT OBJECT TYPES
Indicator Tab	Assigns scores based on the indicator type.	Indicators
Indicator Source	Assigns scores based on the source of the indicator.	Indicators
Attributes	Assigns scores based on an attribute key and value associated with an object.	Adversaries, Indicators, and Vulnerabilities
Adversary Relationships	Assigns scores to indicators based on their relationships with adversaries.	Indicators

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.



Configure Scoring by Indicator Type

Indicator type scoring allows you to prioritize indicators based on their usefulness to your organization.

For example, if your organization cannot process or does not use Fuzzy Hash indicators, you can assign the Fuzzy Hash indicator type a lower score, such as -3.

1. Select the **Indicator Type** tab.
2. Locate the indicator type by scrolling through the list or filtering by name.
3. Adjust the score using one of the following methods:
   - Drag the scoring slider to the required value.
   - Click the up or down arrow next to the current score.
4. Optionally, click **Calculate Impact** to determine how many indicators will be affected.
5. Click **Apply** to save the configuration.

Configure Scoring by Indicator Source

Indicator source scoring allows you to prioritize indicators based on your confidence in the source of the data.

For example, if your organization has greater confidence in intelligence from a paid feed, you can assign indicators from that source a higher score, such as 3.

1. Select the **Indicator Source** tab.
2. Locate the source by scrolling through the list or filtering by source name.
3. Adjust the score using one of the following methods:
   - Drag the scoring slider to the required value.
   - Click the up or down arrow next to the current score.
4. Optionally, click **Calculate Impact** to determine how many indicators will be affected.
5. Click **Apply** to save the configuration.

Configure Scoring by Attribute

Attribute scoring assigns scores based on an attribute key and value associated with an object. It can be used for indicators, adversaries, and vulnerabilities.

You can use attributes supplied by an intelligence provider or custom attributes added by internal users. For example, if your organization applies a `Department` attribute to identify the team targeted by a threat, you can assign a higher score to objects with the attribute `Department - Finance`.

1. Select the **Attributes** tab.
2. Click **Add**.
3. Specify the attribute key using one of the following methods:
   - Open the Key dropdown and select an attribute.
   - Enter the attribute key in the Key field.
4. In the Value field, enter one of the following: o The specific attribute value to which the score applies.

   > An asterisk (*) to apply the score to every value associated with the selected attribute key.

5. Adjust the score using one of the following methods:
   - Drag the scoring slider to the required value.

    - Click the up or down arrow next to the current score.
6. To configure additional attribute criteria, click **Add** and repeat the preceding steps.
7. Optionally, click **Calculate Impact** to determine how many objects will be affected.
8. Click **Apply** to save the configuration.
9. The new scoring criterion appears on the Attributes tab in the following format: `<Key> is <Value>`.

Configure Scoring by Adversary Relationship

Adversary relationship scoring allows you to prioritize indicators associated with adversaries that target your industry or organization.

The Any Adversary option applies the configured score to any indicator with a positive adversary attribution.

1. Select the **Adversary Relationship** tab.
2. Click **Add**.
3. Open the **Select Adversary** dropdown.
4. Locate and select an adversary using the scroll bar or search field.

   To apply the score to indicators with a positive attribution to any adversary, select Any Adversary.

5. Adjust the score using one of the following methods:
    - Drag the scoring slider to the required value.
    - Click the up or down arrow next to the current score.
6. To configure additional adversary relationship criteria, click **Add** and repeat the preceding steps.
7. Optionally, click **Calculate Impact** to determine how many indicators will be affected.
8. Click **Apply** to save the configuration.

Update a Scoring Algorithm

Review scoring configurations periodically to ensure that they reflect changes in your organization's threat environment and priorities, including:

- Changes to the organization's risk profile
- Organizational or geopolitical changes

- New adversaries
- New adversary tactics
- New tools and techniques

To update a scoring algorithm:

1. Open the appropriate tab:
    - Indicator Type
    - Indicator Source
    - Attributes
    - Adversary Relationship
2. Locate the scoring criterion that you want to update.
3. Adjust the score using one of the following methods:
    - Drag the scoring slider to the required value.
    - Click the up or down arrow next to the current score.
4. Optionally, click **Calculate Impact** to determine how many objects will be affected.
5. Click **Apply** to save the changes.

Scoring Considerations

- Use **Calculate Impact** before applying a change to identify how many objects the configuration will affect.
- Allow time for ThreatQ to process scoring configuration changes. Updated scores might not appear in the Threat Library immediately.
- A manually assigned object score overrides the score calculated by a scoring algorithm.
- Adversary and vulnerability scoring must be configured on the **Attributes** tab.
- Review scoring algorithms regularly to ensure that they continue to represent your organization's intelligence priorities and risk profile.

Traffic Light Protocol (TLP)

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role - Action Permissions: Data Controls - Edit TLP, See the Interdependent Permissions topic.

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 the following light icons 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):

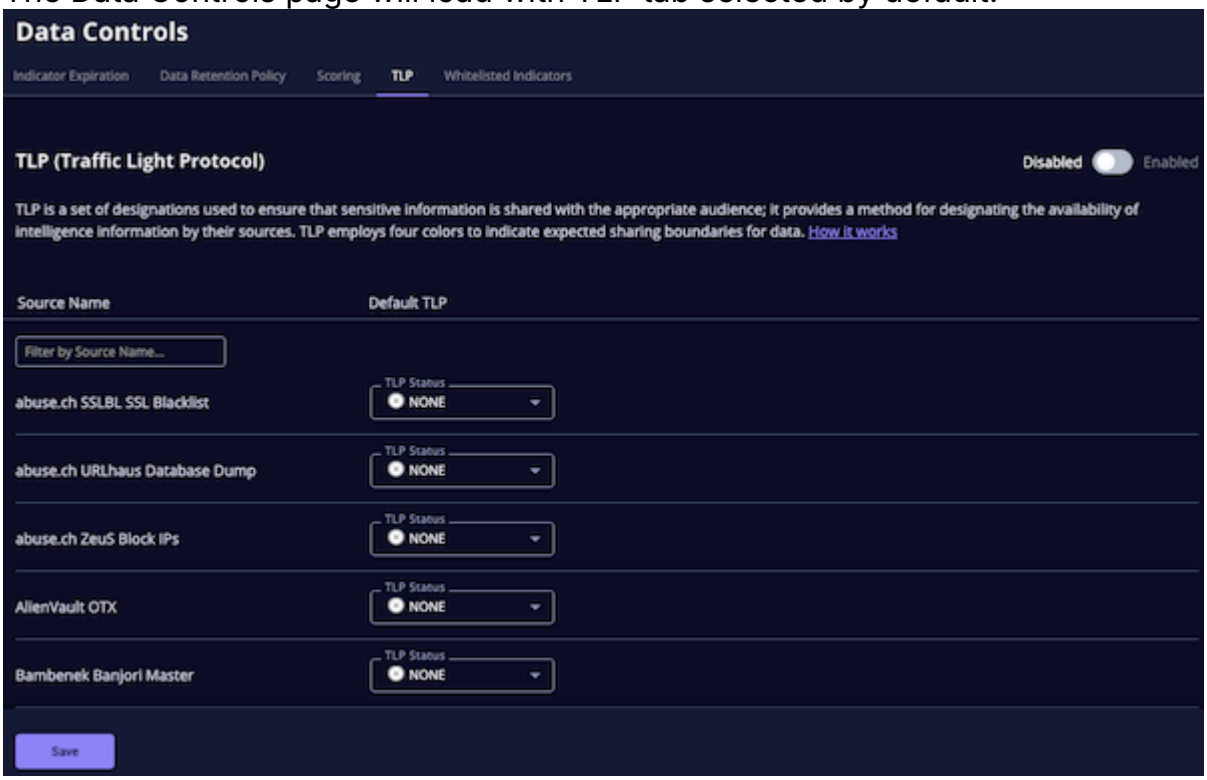
METHOD	DETAILS
Manually Set	Using the Add New Source option when creating an object will allow you to select a TLP label.
Source Provided Data	TLP label received from ingested data.
Source Default	Administrators can set a source's default TLP label. See the Add TLP to Source section.
No TLP	A TLP label 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.

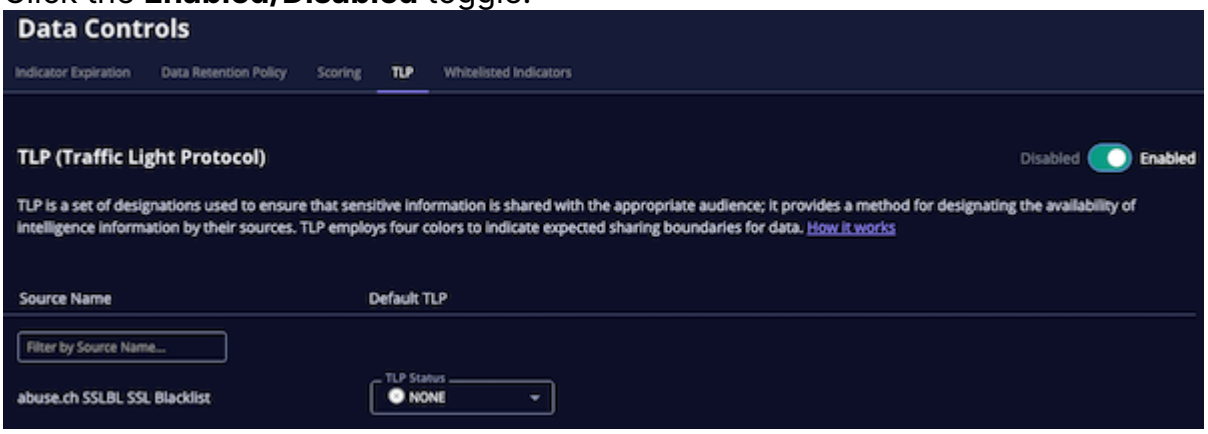
   The Data Controls page will load with TLP tab selected by default.



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.

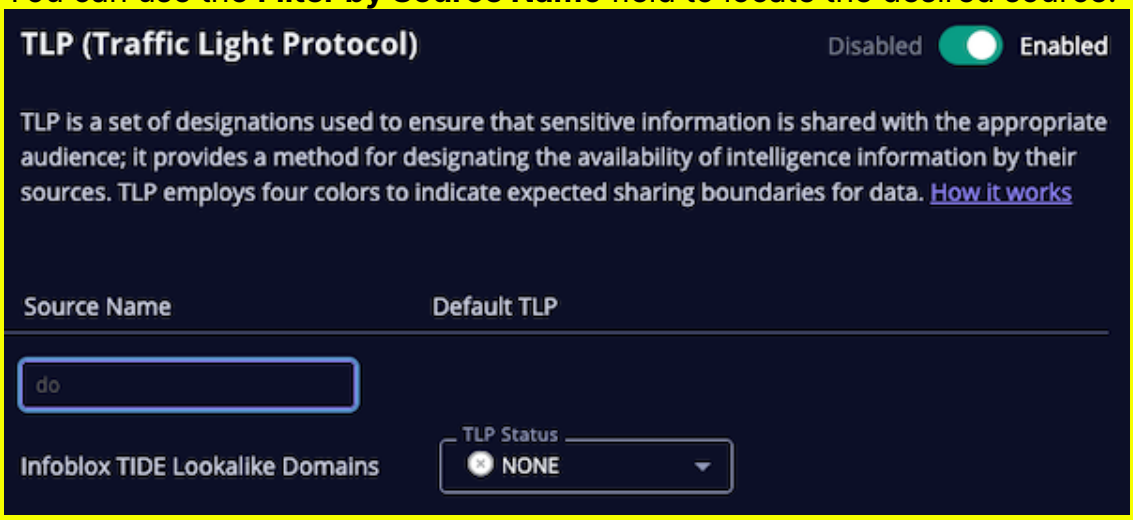


   You do not need to click the **Save** button. Changes to the Enabled/Disabled status are made immediately.

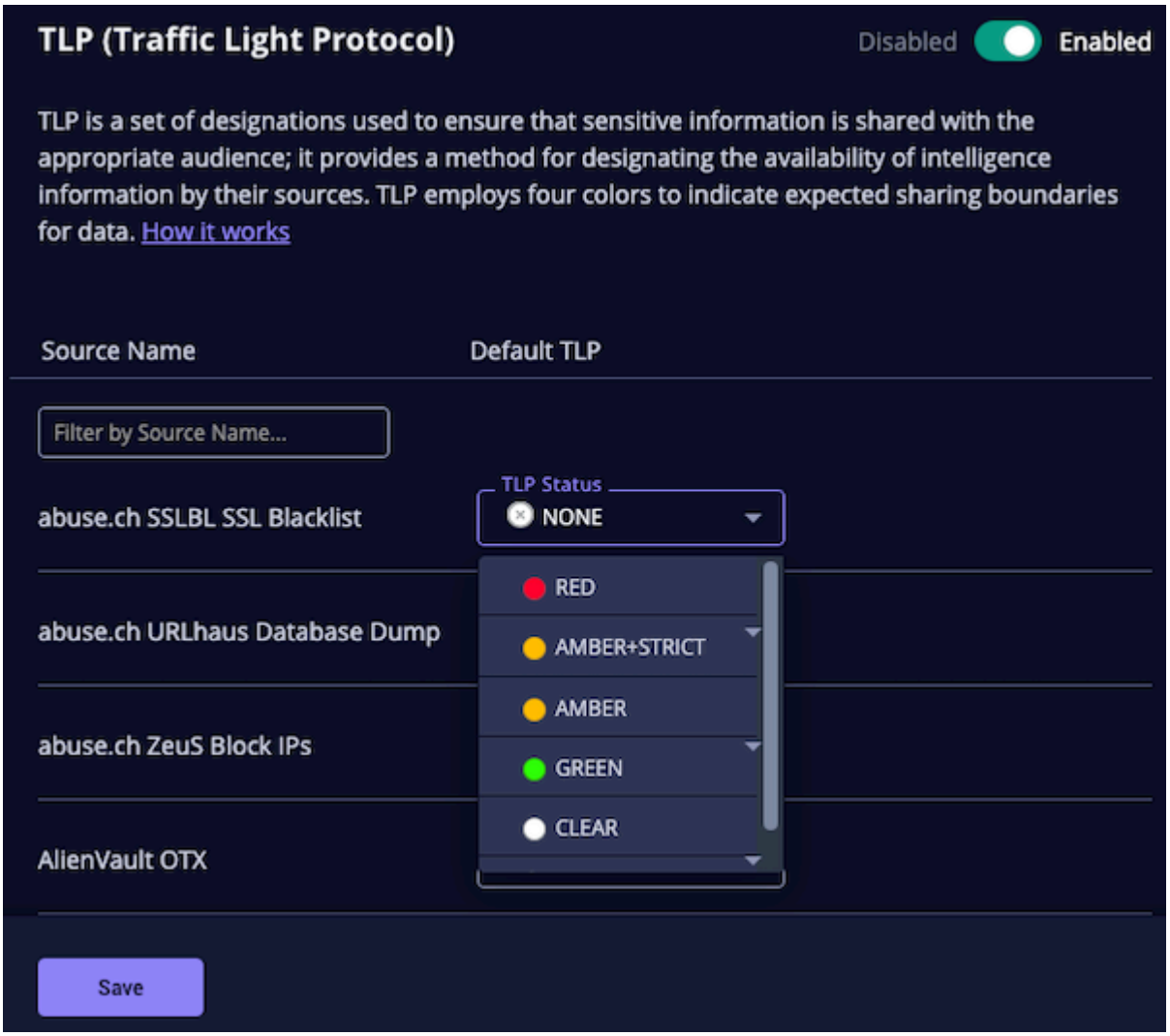
Apply a TLP Label to Source

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

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



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



3. Click **Save**.

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

Whitelisted Indicators

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role - Action Permissions: Data Controls - Edit Whitelisting

There are some Indicators that should be considered to be non-malicious and eligible for whitelisting. As such, you would not want those indicators going out to other systems. For example, a company's own domain name would never need to be blocked.

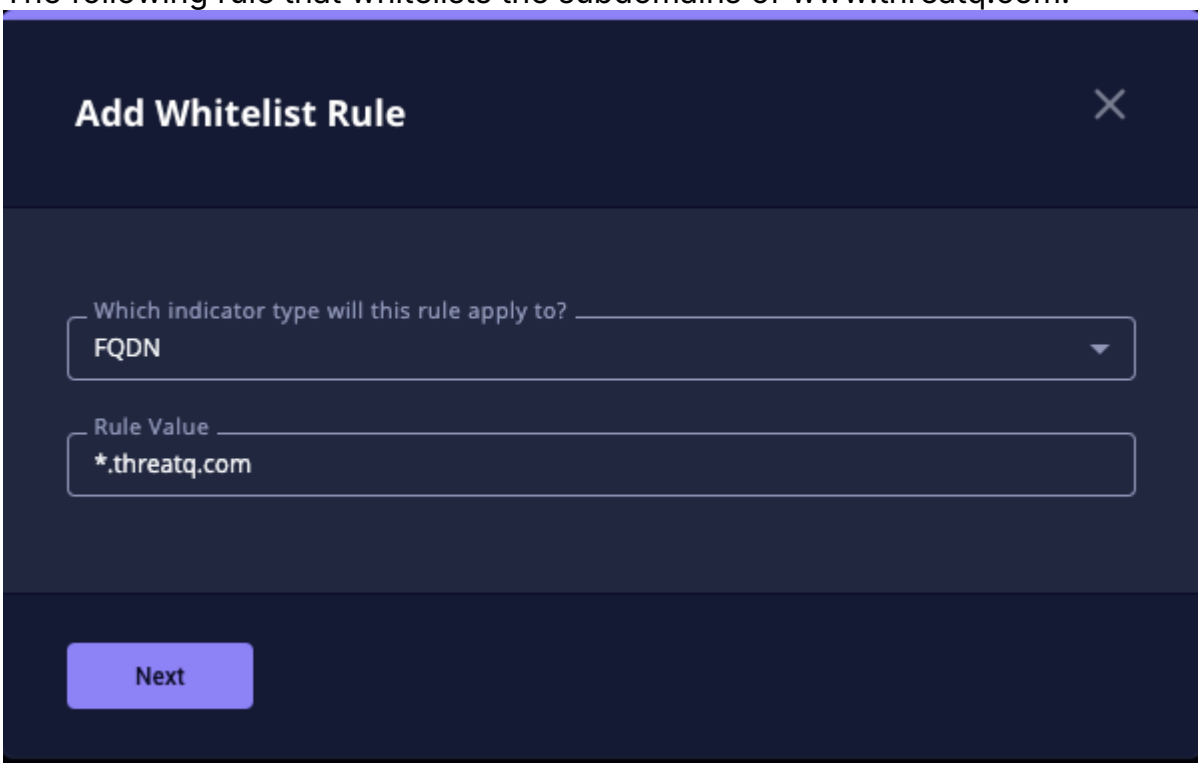
The Whitelisting process creates rules for specific indicators, so that when those indicators come in in the future, they are automatically whitelisted.

Wildcard Options

ThreatQ whitelist rules support the use of wildcard characters. Wildcard characters allow you to create a single rule that applies to multiple indicator values. For example, you can use a site's domain coupled with a wildcard (*) to whitelist all of its subdomains. This saves the step of creating a rule for each existing subdomain or the need to enter new rules as a site adds subdomains.

Example: Whitelisting FQDNS

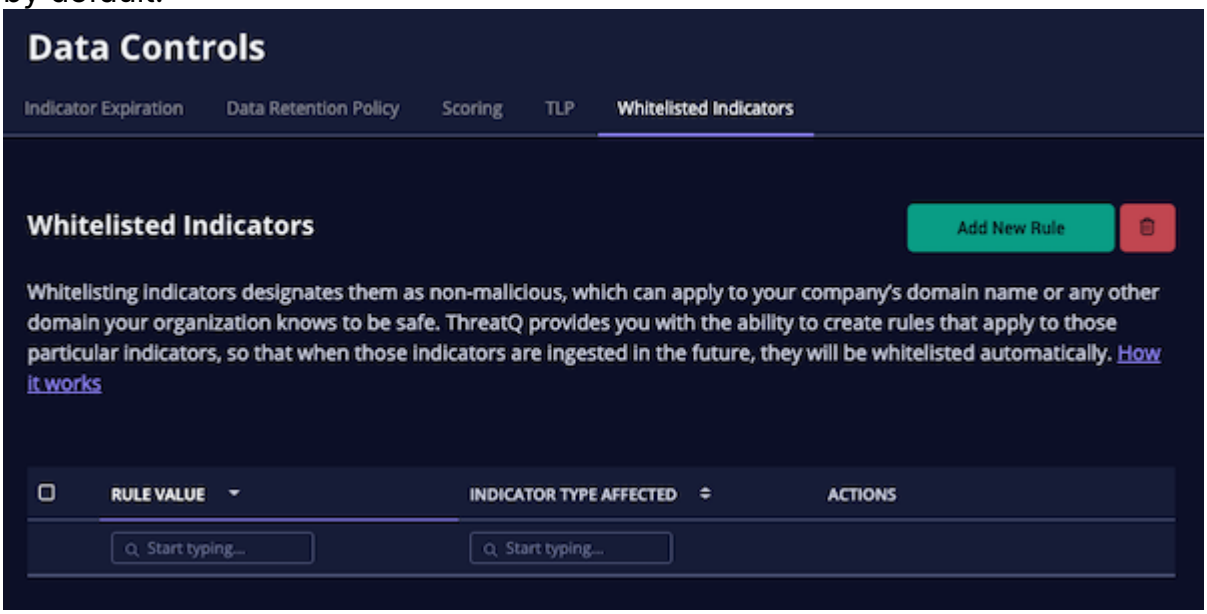
The following rule that whitelists the subdomains of www.threatq.com:



Accessing the Whitelisted Indicator Rules

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

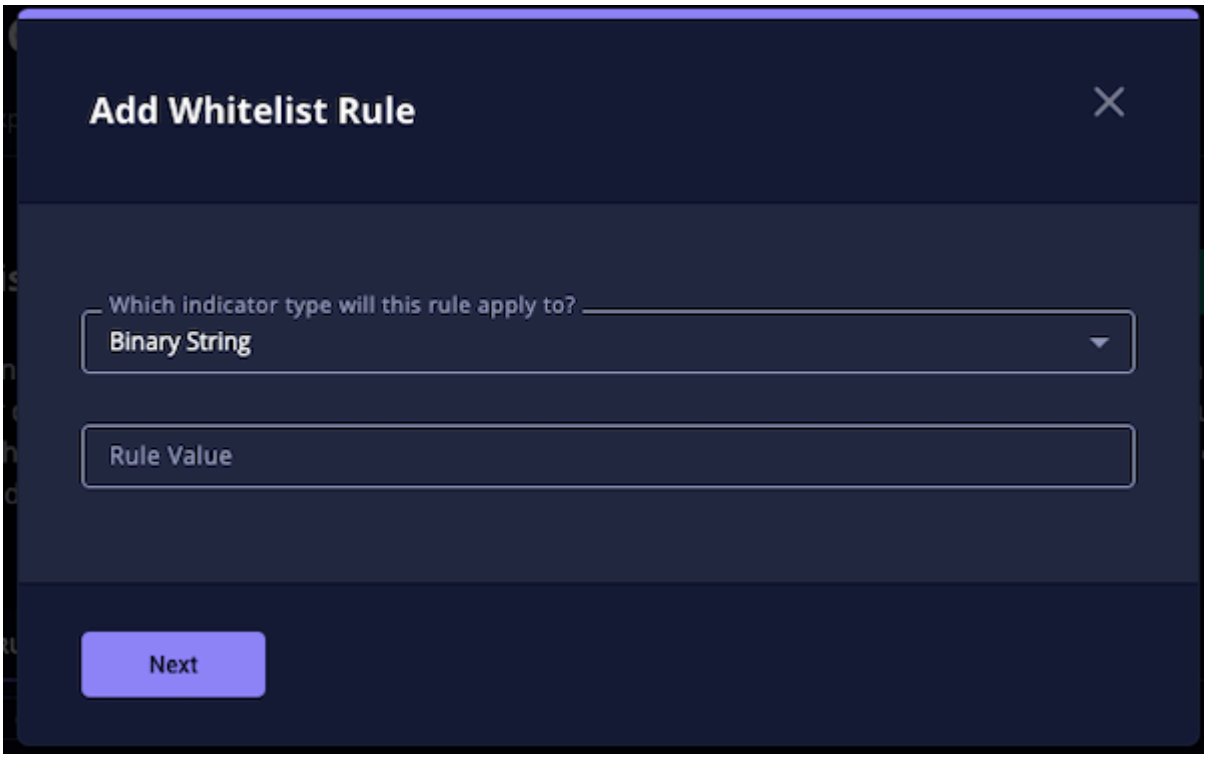
   The Data Controls page is displayed with the Whitelisted Indicators tab selected by default.



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.

1. From the Whitelisted Indicators tab, click the **Add New Rule** button to access the Add Whitelist Rule window.



2. Select the indicator type to which the rule applies.
3. Add a Rule Value.

   The Rule Value field supports the use of wildcards. See the Wildcard Options section for more information on creating whitelist rules with wildcard characters.

4. Click **Next**.

Affected indicators are listed in the dialog box.

5. Review the affected indicators.

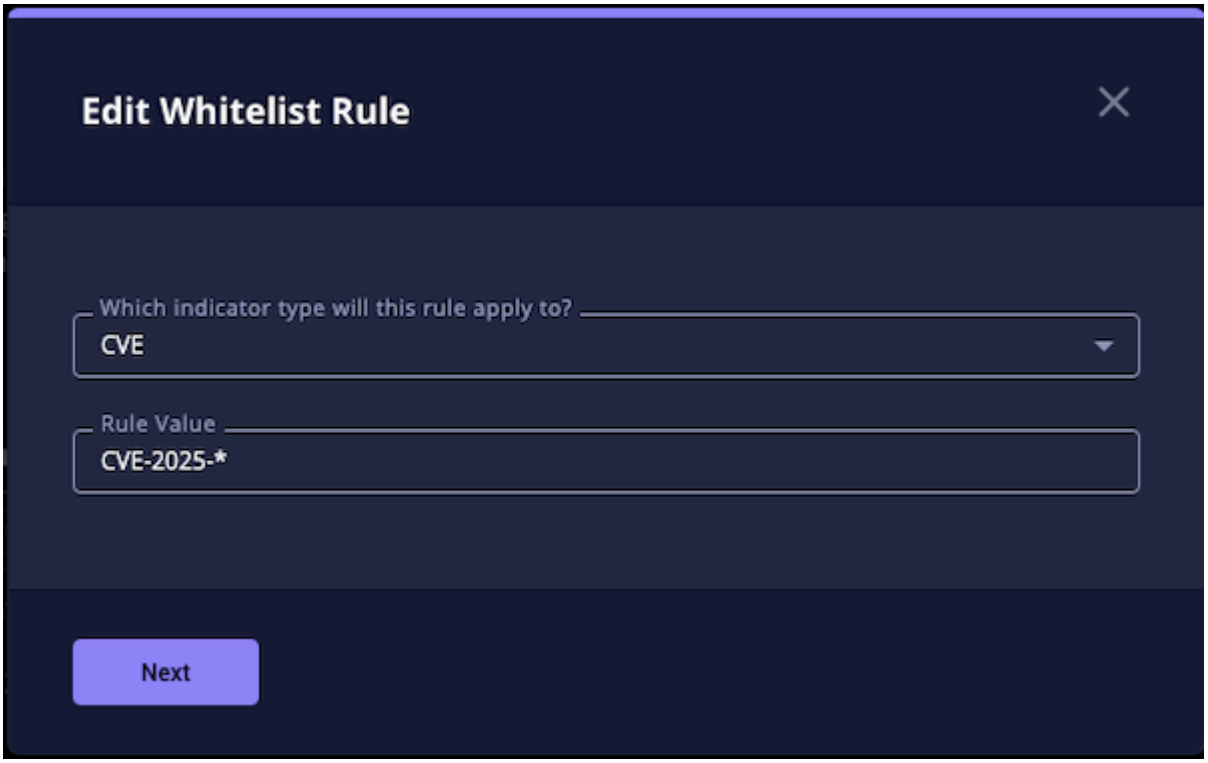
> The rule has not been applied yet, so you still have time to edit it based on whether you are satisfied with how it affects the indicators.

6. To make changes to the rule before saving it, 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. This rule will apply to any new indicators as they enter the system.

Editing a Whitelisted Rule

1. Click the **Edit** option to the right of the rule you want to update.In the Whitelisted Rules table, locate the rule you wish to edit.
   The Edit Whitelist Rule window is displayed.



2. Enter your changes and click the **Next** button.

   The Edit Whitelist Rule window displays the number of affected indicators.

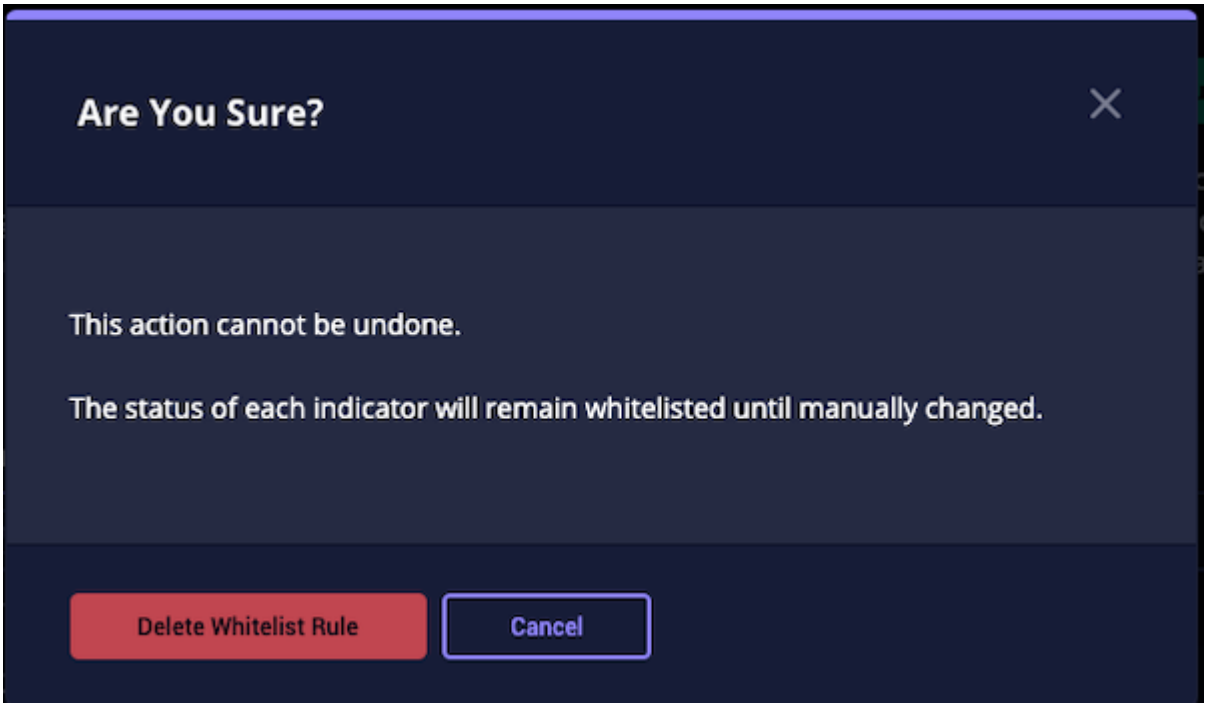
   The rule change has not been applied yet, so you still have time to edit it based on whether you are satisfied with how it affects the indicators.

3. To make changes to the rule before saving it, click **Continue Editing this Rule**.
4. 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. This rule will apply to any new indicators 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. You can use the checkboxes located to the left of each rule to select multiple rules for deletion.
2. Click the delete icon .
3. From the Are You Sure window, click the **Delete Whitelist Rule** button to confirm the deletion.


Are You Sure?
This action cannot be undone.
The status of each indicator will remain whitelisted until manually changed.
Delete Whitelist Rule
Cancel

Exports

About Exports

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative or Maintenance
Custom Role:

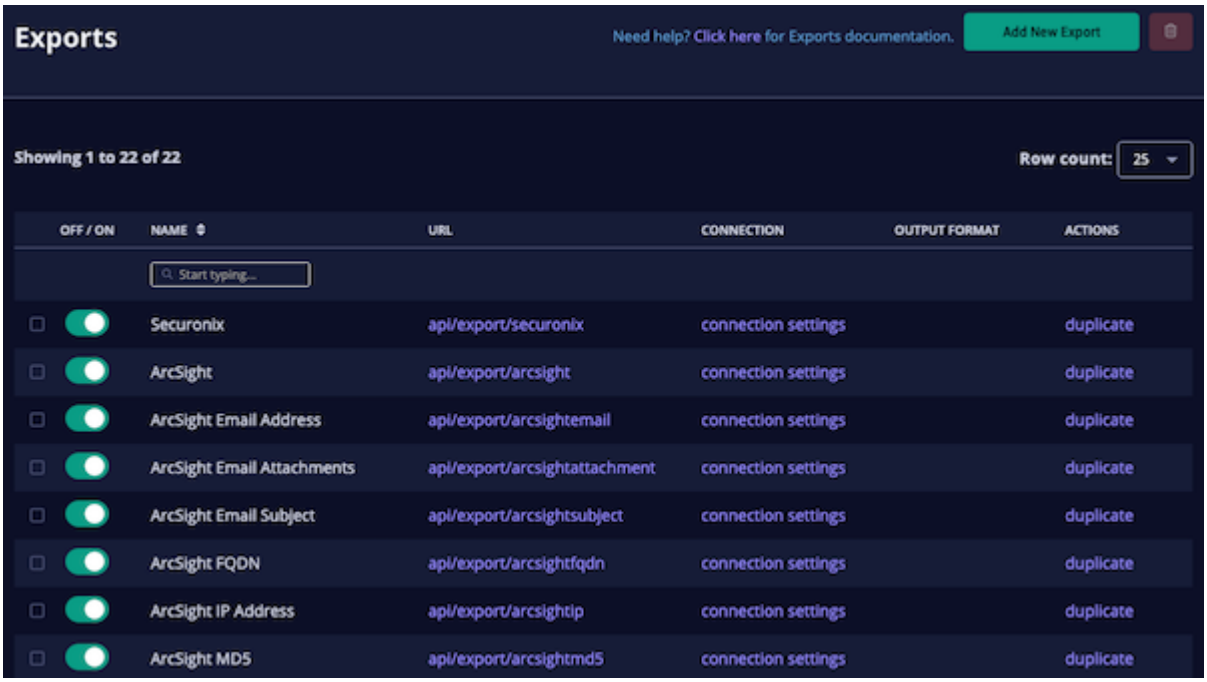
- Action Permissions: Objects & Context - Objects (all object types) **OR** Data Access Permissions: object type
- Action Permissions: Administrative Functions - Edit Exports

Notes:

- Authenticated exports are filtered based on the user's Data Access permissions. Anonymous exports generated via access tokens return full results.
- Export configurations include only object types the user can access.

Exporting is one of the most important ThreatQ features, as it allows you to output non-whitelisted Indicators and other system object types to an external threat detection system.

The Export page allows you to view, update, or delete the exports you have created as well as to view the standard system exports seeded in the ThreatQ. You can also copy a standard export to use it as the basis for a new export.



ThreatQ Exports are built on the Smarty PHP Template Engine; see https://www.smarty.net/ which provides an easy to understand syntax that simplifies export creation and updates.

Managing Exports

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative or Maintenance
Custom Role:

- Action Permissions: Objects & Context - Objects (all object types) **OR** Data Access Permissions: object type
- Action Permissions: Administrative Functions - Edit Exports

Notes:

- Authenticated exports are filtered based on the user's Data Access permissions. Anonymous exports generated via access tokens return full results.
- Export configurations include only object types the user can access.

Excessively large exports of threat intelligence data can cause system performance degradation and prevent the export from completing successfully. It is important to note that practical export limits will vary based on your deployment size, underlying hardware resources, overall structure of data, and active ingress activity.

The Exports page lists all existing exports in ascending, alphabetical order by export name. You can easily identify active exports by the green toggle in the Off/On column. In addition, all seeded exports have a blank Output Format field and all exports created in your instance, have an output format link.

To customized the Export page display, you can change the number of rows displayed from the default of 25 to 10, 50, or 100. You can change the sort order to descending alphabetical by clicking the Name column.

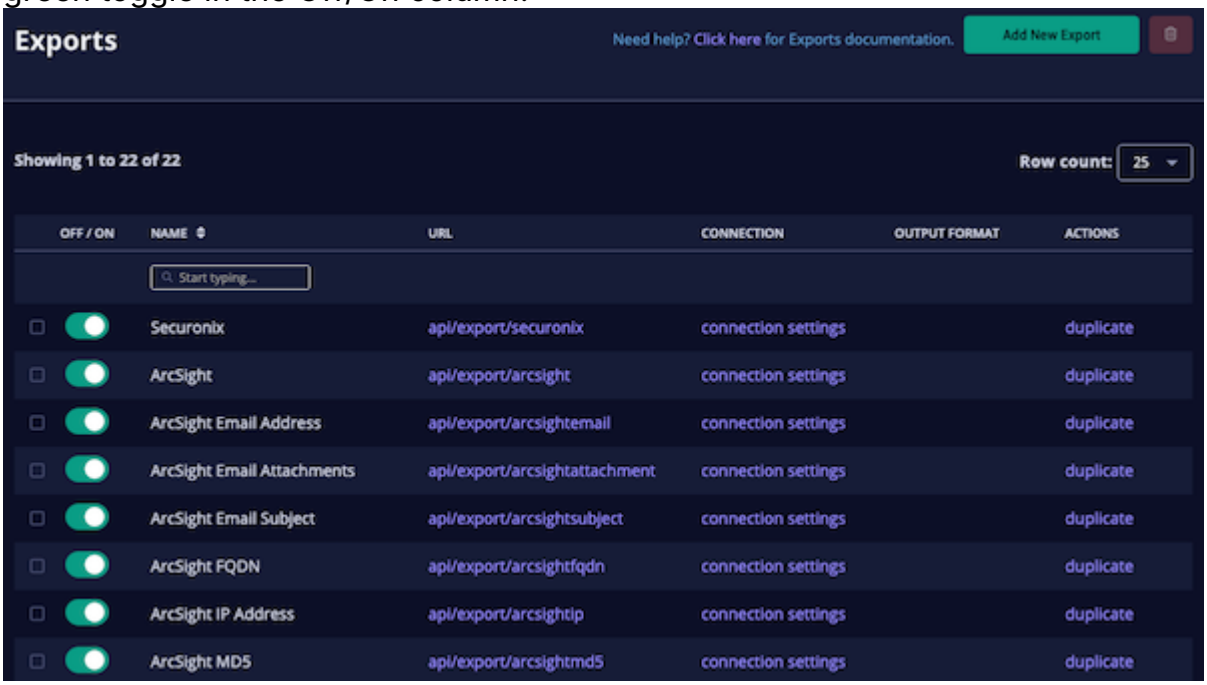
Tips and Tricks

- Use the seeded exports or output format template examples provided by ThreatQuotient as building blocks for new exports.
- Give each new export a descriptive name.
- 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.

Accessing the Exports List

1. Select the **Settings** **icon >Exports**.
   The Exports page lists all exports in alphabetical order. Active exports display a

green toggle in the Off/On column.



Viewing an Export

1. From the Exports page, click the export's URL.
   A new tab opens in your browser and displays the data returned from the export. By default, this tab displays up to ten objects. To increase the number of objects included in your export, you can update the limit value in the export's URL.

   Original URL - Default 10 Objects:

   https://te-28440.threatq.com/api/export/b98c62268ac80754e3e0e774afafc639/?limit=**10**&token=49vx259akYhOgvaJ2Fa8

   New URL - 300 Objects:

   https://te-28440.threatq.com/api/export/b98c62268ac80754e3e0e774afafc639/?limit=**300**&token=49vx259akYhOgvaJ2Fa8

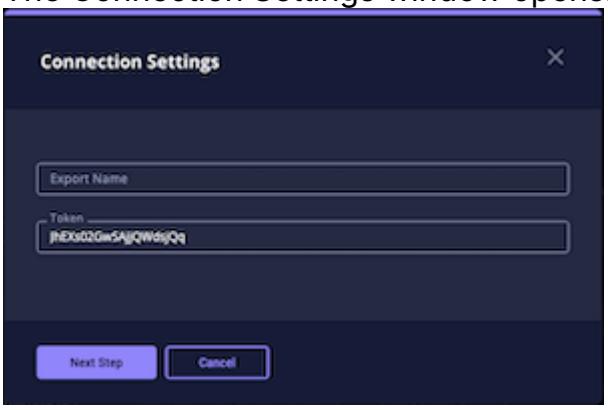
   The load time may be lengthy depending on the amount of data returned.

Enabling/Disabling Exports

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

Adding an Export

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



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
Custom

Filter by TLP

- [x] **Red**
- [x] **Amber+Strict**
- [x] **Amber**
- [x] **Green**
- [x] **Clear**
- [x] **Not Specified**

Provide an output type here

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?	This field defaults to a value of Indicators. Click the field to select from a list of object types.
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 of 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 source, attribute source, or description source 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.
Output Format Template	(Optional) See the Output Format Templates topic for more information.

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.
7. To begin exporting data, click the export's Off/On toggle to On.

Duplicating an Export

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

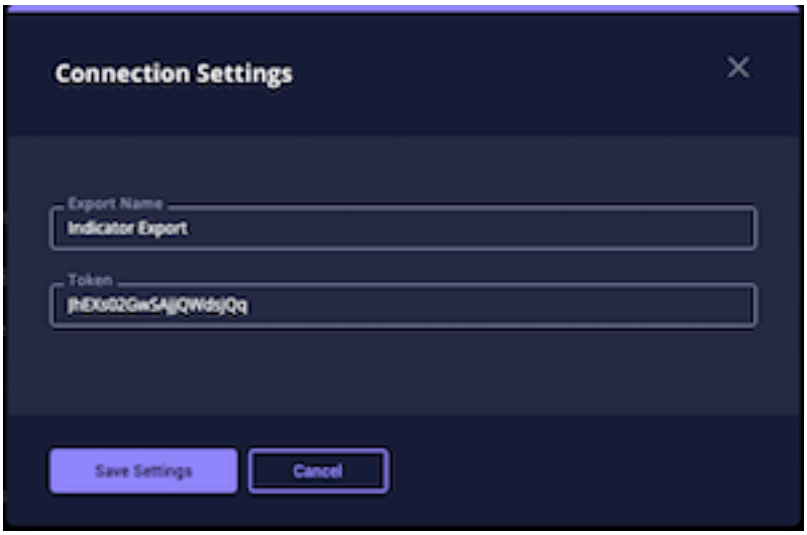
1. From the Exports page, locate the Export you want to duplicate.
2. Click the **duplicate** option in the Actions column.
   The duplicate appears at the bottom of the Exports table. By default, the copy you just created is toggled to Off.

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.



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. For each export you want to delete, check the box next to the export's off/on toggle.
3. Click the delete icon next to the **Add New Export** button.

Output Format Options

The Special Parameters and Output Format Template fields allow you to control the data included in your exports. The Special Parameters field allows you filter the data included in the export and the Output Format Template field allows you to specify which data points are included in the export.

You can customize these fields for an custom or duplicated export but not for the seeded exports supplied by ThreatQ.

Special Parameters Field

The Special Parameters field allows you to filter 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

You can add the following parameters to an export's Special Parameters field to filter the data included in the export:

Assets

```
assets.value
assets.status
assets.point_of_contact
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
```

Attack Pattern

```
attack_pattern.value
attack_pattern.status_id
attack_pattern.status
attack_pattern.point_of_contact
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
```

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
```

Event

```
event.type_id
event.status
event.point_of_contact
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
```

Exploit Target

```
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
```

Identity

```
identity.value
identity.status_id
identity.status
identity.point_of_contact
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
```

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
```

Indicator

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

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

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

Intrusion Set

```
intrusion_set.value
intrusion_set.status_id
intrusion_set.status
intrusion_set.point_of_contact
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.status
malware.point_of_contact
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.status
report.point_of_contact
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
```

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
```

Tag

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`)

Tool

```
tool.value
tool.status_id
tool.status
tool.point_of_contact
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
```

TTP

```
ttp.value
ttp.status_id
ttp.status
ttp.point_of_contact
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
```

Vulnerability

```
vulnerability.value
vulnerability.status_id
vulnerability.status
vulnerability.point_of_contact
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
```

Filtering by Attribute Value

You can filter your export results by a specific attribute name and value. You can view all attribute names and values in the Attribute Management tab within the Object Management page.

Example:

To create an export that only includes objects with a Confidence attribute value of High, you would add the following to the Special Parameters field:

```
indicator.Attributes[attribute key]=attribute value
```

Example:

This example restricts your export to objects with a Confidence attribute set to High.

```
indicator.Attributes[Confidence]=High
```

Adding Differential Flags

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

Include the following to limit exports to new data only:

```
differential=1
```

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

external system 1
https://{tq-host}/api/export/c2ab6df72e67ee13cef90f0e00981b62/?token=npc6z01pFXwfHYb5tm51hMvKQJNYecTG& **differential=1**

external system 2
https://{tq-host}/api/export/c2ab6df72e67ee13cef90f0e00981b62/?token=npc6z01pFXwfHYb5tm51hMvKQJNYecTG& **differential=2**

Adding Parameters to the End of the URL

You can append the 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 Export Filters

You can configure exports to output objects matching filter conditions based on comparisons such as greater than (>) or less than (<) as well as logical operators such as AND. You can add these filters to the export's Special Parameters field (Output Format window) or append the filter criteria to the export's URL. Use the following examples as guidelines for creating your own export filters.

1. Searching using greater than, less than, or equal to
   The first example captures indicators with a score greater than or equal to 5. The second example captures indicators with a score less than or equal to 5.
   - Special Parameters field:

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

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

   - Appended to Export URL:

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

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

2. Adding multiple criteria for a single field using an AND comparison
   The following example captures indicators with a score of 5 and indicators with a score of 8.
   - Special Parameters field:

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

   - Appended to Export URL:

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

3. Adding a criteria range for a single field using an AND comparison
   The following example captures indicators with a score of 5, 6, 7 and 8.
   - Special Parameters field:

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

   - Appended to Export URL:

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

4. Adding criteria for a multiple fields using an AND comparison
   The following example captures indicators with a score of 8 AND a status of indirect.
   - Special Parameters field:

     ```
     indicator.score>=8&indicator.status=indirect
     ```

   - Appended to Export URL:

     ```
     &indicator.score[]=>=8&indicator.status[]=indirect
     ```

Output Format Template Field

You can use the template examples provided by ThreatQuotient as a baseline for your exports or you can add your own export parameters to the Output Template field.

Inserting Variables

The **Insert Variable** button above the field allows you to select from a drop down list of variables based on the object type included in the export. To insert a variable, click the location for the variable, click the **Insert Variable** button, and select the variable from the dropdown list.

Template Format

This Output Format Template field allows you to control 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 as shown in the following example:

```
{foreach $data as $indicator}

Your variables go here

{/foreach}
```

Output Format Template Examples

ThreatQuotient provides output format template examples that you can use as a starting point for a new export. You can copy and paste these examples to the Output Format Template field and make changes based on the data you want to export.

Export Template Examples by Object Type

Each of these examples includes the following placeholder text to clarify where you can add additional variables to customize your export:

- *Your variables go here*

In addition, these examples include text labels to clarify the data included in the export. For example, the output of the Indicators example, list of the name of each variable separated from the value by a colon as in **Type: IP Address**.

```
1.33.5.232
ID: 1
Value: 1.33.5.232
Type: IP Address
Status: Active
Class: network
Description:
Score: 0
Hash: a53a6ec8cd0ae6af7d0469daeac5574d
Source Count: 1
Whitelisted: N
Last Detected At:
Created At: 2023-10-04 14:28:40
Updated At: 2023-10-04 14:28:41
Touched At: 2023-10-04 17:56:20
Since Deleted: Y
Deleted At:
Deleted: N
```

Adversaries Template

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

{foreach $adversary.Descriptions item=description
```

```
name=Descriptions}
Source: {$description.source}
Description: {$description.value}
{/foreach}

Your variables go here

{/foreach}
```

Assets Template

```
{foreach $data as $asset}
ID: {$asset.id}
Name: {$asset.value}
Status:  {$asset.status}
Point of Contact:  {$asset.point_of_contact}
Created At: {$asset.created_at}
Updated At: {$asset.updated_at}
Deleted At: {$asset.deleted_at}

{foreach $asset.Descriptions item=description name=Descriptions}
Source: {$description.source}
Description: {$description.value}
{/foreach}

Your variables go here

{/foreach}
```

Attack Pattern Template

```
{foreach $data as $attack_pattern}
ID: {$attack_pattern.id}
Name: {$attack_pattern.value}
Status:  {$attack_pattern.status}
Point of Contact:  {$attack_pattern.point_of_contact}
Created At: {$attack_pattern.created_at}
Updated At: {$attack_pattern.updated_at}
Deleted At: {$attack_pattern.deleted_at}
```

```
{foreach $attack_pattern.Descriptions item=description
name=Descriptions}
Source: {$description.source}
Description: {$description.value}
{/foreach}

Your variables go here

{/foreach}
```

Campaign Template

```
{foreach $data as $campaign}
ID: {$campaign.id}
Name: {$campaign.value}
Status:  {$campaign.status}
Point of Contact:  {$campaign.point_of_contact}
Objective:  {$campaign.objective}
First Seen: {$campaign.started_at}
Last Seen:  {$campaign.ended_at}
Created At: {$campaign.created_at}
Updated At: {$campaign.updated_at}
Deleted At: {$campaign.deleted_at}

{foreach $campaign.Descriptions item=description
name=Descriptions}
Source: {$description.source}
Description: {$description.value}
{/foreach}

Your variables go here

{/foreach}
```

Course of Action Template

```
{foreach $data as $course_of_action}
ID: {$course_of_action.id}
Name: {$course_of_action.value}
Status:  {$course_of_action.status}
```

```
Point of Contact:  {$course_of_action.point_of_contact}
Created At: {$course_of_action.created_at}
Updated At: {$course_of_action.updated_at}
Deleted At: {$course_of_action.deleted_at}

{foreach $course_of_action.Descriptions item=description
name=Descriptions}
Source: {$description.source}
Description: {$description.value}
{/foreach}

Your variables go here

{/foreach}
```

Events Template

```
{foreach $data as $event}

{$event.title} ID: {$event.id}
Title: {$event.title}
Type: {$event.type}
Status:  {$event.status}
Point of Contact:  {$event.point_of_contact}
Happened: {$event.happened_at}
Created At: {$event.created}
Updated At: {$event.updated_at}
Deleted At: {$event.deleted_at}
Deleted: {$event.deleted}

{foreach $event.Descriptions item=description name=Descriptions}
Source: {$description.source}
Description: {$description.value}
{/foreach}

Your variables go here

{/foreach}
```

Exploit Target Template

```
{foreach $data as $exploit_target}
ID: {$exploit_target.id}
Name: {$exploit_target.value}
Status:  {$exploit_target.status}
Point of Contact:  {$exploit_target.point_of_contact}
Created At: {$exploit_target.created_at}
Updated At: {$exploit_target.updated_at}
Deleted At: {$exploit_target.deleted_at}

{foreach $exploit_target.Descriptions item=description
name=Descriptions}
Source: {$description.source}
Description: {$description.value}
{/foreach}

Your variables go here

{/foreach}
```

Identity Template

```
{foreach $data as $identity}
ID: {$identity.id}
Name: {$identity.value}
Status:  {$identity.status}
Point of Contact:  {$identity.point_of_contact}
Contact Information:  {$identity.contact_information}
Created At: {$identity.created_at}
Updated At: {$identity.updated_at}
Deleted At: {$identity.deleted_at}

{foreach $identity.Descriptions item=description
name=Descriptions}
Source: {$description.source}
Description: {$description.value}
{/foreach}

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}
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: {$indicator.updated_at}
Since Deleted: {$indicator.sincedeleted}
Deleted At: {$indicator.deleted_at}
Deleted: {$indicator.deleted}

{foreach $indicator.Descriptions item=description
name=Descriptions}
Source: {$description.source}
Description: {$description.value}
{/foreach}

Your variables go here

{/foreach}
```

Intrusion Set Template

```
{foreach $data as $intrusion_set}
ID: {$intrusion_set.id}
Name: {$intrusion_set.value}
Status:  {$intrusion_set.status}
```

```
Point of Contact:  {$intrusion_set.point_of_contact}
First Seen: {$intrusion_set.started_at}
Last Seen:  {$intrusion_set.ended_at}
Created At: {$intrusion_set.created_at}
Updated At: {$intrusion_set.updated_at}
Deleted At: {$intrusion_set.deleted_at}

{foreach $intrusion_set.Descriptions item=description
name=Descriptions}
Source: {$description.source}
Description: {$description.value}
{/foreach}

Your variables go here

{/foreach}
```

Malware Template

```
{foreach $data as $malware}
ID: {$malware.id}
Name: {$malware.value}
Status:  {$malware.status}
Point of Contact:  {$malware.point_of_contact}
Created At: {$malware.created_at}
Updated At: {$malware.updated_at}
Deleted At: {$malware.deleted_at}

{foreach $malware.Descriptions item=description
name=Descriptions}
Source: {$description.source}
Description: {$description.value}
{/foreach}

Your variables go here

{/foreach}
```

Report Template

```
{foreach $data as $report}
ID: {$report.id}
Name: {$report.value}
Status:  {$report.status}
Point of Contact:  {$report.point_of_contact}
Created At: {$report.created_at}
Updated At: {$report.updated_at}
Deleted At: {$report.deleted_at}

{foreach $report.Descriptions item=description name=Descriptions}
Source: {$description.source}
Description: {$description.value}
{/foreach}

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}
Hash: {$signature.hash}
Detected At: {$signature.last_detected_at}
Created At: {$signature.created}
Updated At: {$signature.updated_at}
Deleted At: {$signature.deleted_at}
Deleted: {$signature.deleted}

{foreach $signature.Descriptions item=description
name=Descriptions}
Source: {$description.source}
Description: {$description.value}
```

```
{/foreach}

Your variables go here

{/foreach}
```

Tool Template

```
{foreach $data as $tool}
ID: {$tool.id}
Name: {$tool.value}
Status:  {$tool.status}
Point of Contact:  {$tool.point_of_contact}
Created At: {$tool.created_at}
Updated At: {$tool.updated_at}
Deleted At: {$tool.deleted_at}

{foreach $tool.Descriptions item=description name=Descriptions}
Source: {$description.source}
Description: {$description.value}
{/foreach}

Your variables go here

{/foreach}
```

TTP Template

```
{foreach $data as $ttp}
ID: {$ttp.id}
Name: {$ttp.value}
Status:  {$ttp.status}
Point of Contact:  {$ttp.point_of_contact}
Created At: {$ttp.created_at}
Updated At: {$ttp.updated_at}
Deleted At: {$ttp.deleted_at}

{foreach $ttp.Descriptions item=description name=Descriptions}
Source: {$description.source}
Description: {$description.value}
```

```
{/foreach}

Your variables go here

{/foreach}
```

Vulnerability Template

```
{foreach $data as $vulnerability}
ID: {$vulnerability.id}
Name: {$vulnerability.value}
Status:  {$vulnerability.status}
Point of Contact:  {$vulnerability.point_of_contact}
Created At: {$vulnerability.created_at}
Updated At: {$vulnerability.updated_at}
Deleted At: {$vulnerability.deleted_at}

{foreach $vulnerability.Descriptions item=description
name=Descriptions}
Source: {$description.source}
Description: {$description.value}
{/foreach}

Your variables go here

{/foreach}
```

Template Variables

The following is a list of commonly used Adversary and Indicator variables that you can add to the above template examples to expand the data included in an export.

Adversary Examples

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}
```

Attribute Variable

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

Attribute Variable with Attribute Source and Update At Timestamp

```
{* $adversary.Attributes $attribute.Sources $attribute.updated_at
*}
[
{foreach $adversary.Attributes item=attribute}
  Name: {$attribute.name}
  Updated_at: {$attribute.updated_at}
{foreach $attribute.sources item=source}
  Attr Source: {$source.name}
{/foreach}

{/foreach}
]
```

Any TLP filters specified for the export apply to the attribute source's TLP label as well as the system object source's TLP label.

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}
```

Source Variable

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

Tag Variable

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

Task Variable

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

Indicator Examples

Adversary Variable

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

Attachment Variable

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

Attack Pattern Variable

```
{foreach $indicator.Attack_pattern item=attack_pattern
name=Attack_pattern}
Name: {$attack_pattern.name}
Value: {$attack_pattern.value}
{/foreach}
```

Attribute Variable

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

Attribute Variable with Attribute Source and Update At Timestamp

```
{* $indicator.Attributes $attribute.Sources $attribute.updated_at
*}
[
{foreach $indicator.Attributes item=attribute}
  Name: {$attribute.name}
  Updated_at: {$attribute.updated_at}
{foreach $attribute.sources item=source}
```

```
  Attr Source: {$source.name}
{/foreach}

{/foreach}
]
```

Any TLP filters specified for the export apply to the attribute source's TLP label as well as the system object source's TLP label.

Campaign Variable

```
{foreach $indicator.Campaign item=campaign name=Campaign}
Name: {$campaign.name}
Value: {$campaign.value}
{/foreach}
```

Course of Action Variable

```
{foreach $indicator.Course_of_action item=course_of_action
name=Course_of_action}
Name: {$course_of_action.name}
Value: {$course_of_action.value}
{/foreach}
```

Event Variable

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

Exploit Target Variable

```
{foreach $indicator.Exploit_Targets item=exploit_target
name=Exploit_Target}
Name: {$exploit_target.name}
Value: {$exploit_target.value}
{/foreach}
```

Identity Variable

```
{foreach $indicator.Identity item=identity name=Identity}
Name: {$identity.name}
Value: {$identity.value}
{/foreach}
```

Incident Variable

```
{foreach $indicator.Incident item=incident name=Incident}
Name: {$incident.name}
Value: {$incident.value}
{/foreach}
```

Indicator Variable

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

Intrusion Set Variable

```
{foreach $indicator.Intrusion_set item=intrusion_set
name=Intrusion_set}
Name: {$intrusion_set.name}
Value: {$intrusion_set.value}
{/foreach}
```

Investigation Variable

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

Malware Variable

```
{foreach $indicator.Malware item=malware name=Malware}
Name: {$malware.name}
Value: {$malware.value}
{/foreach}
```

Report Variable

```
{foreach $indicator.Report item=report name=Report}
Name: {$report.name}
Value: {$report.value}
{/foreach}
```

Signature Variable

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

Task Variable

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

Tool Variable

```
{foreach $indicator.Tool item=tool name=Tool}
Name: {$tool.name}
Value: {$tool.value}
{/foreach}
```

TTP Variable

```
{foreach $indicator.Ttp item=ttp name=Ttp}
Name: {$ttp.name}
```

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

Vulnerability Variable

```
{foreach $indicator.Vulnerability item=vulnerability
name=Vulnerability}
Name: {$vulnerability.name}
Value: {$vulnerability.value}
{/foreach}
```

Specific Indicator Exports

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.
Flagged Integrations	Find information on integrations flagged for ingesting a large number of object relationships for a specific system object(s).
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.

TOPIC	DESCRIPTION
Activity Logs (feeds) and Feed Run Activity	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 Operation. 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.

CDFs override indicator statuses to the default status defined in the CDF and override signature statuses to a default value of Active.

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.

> The Threat Research Agent can leverage operations as tools when the agent is enabled and the **Enable this operation for use by your ThreatQ MCP server** setting is configured on the operation's configuration page.

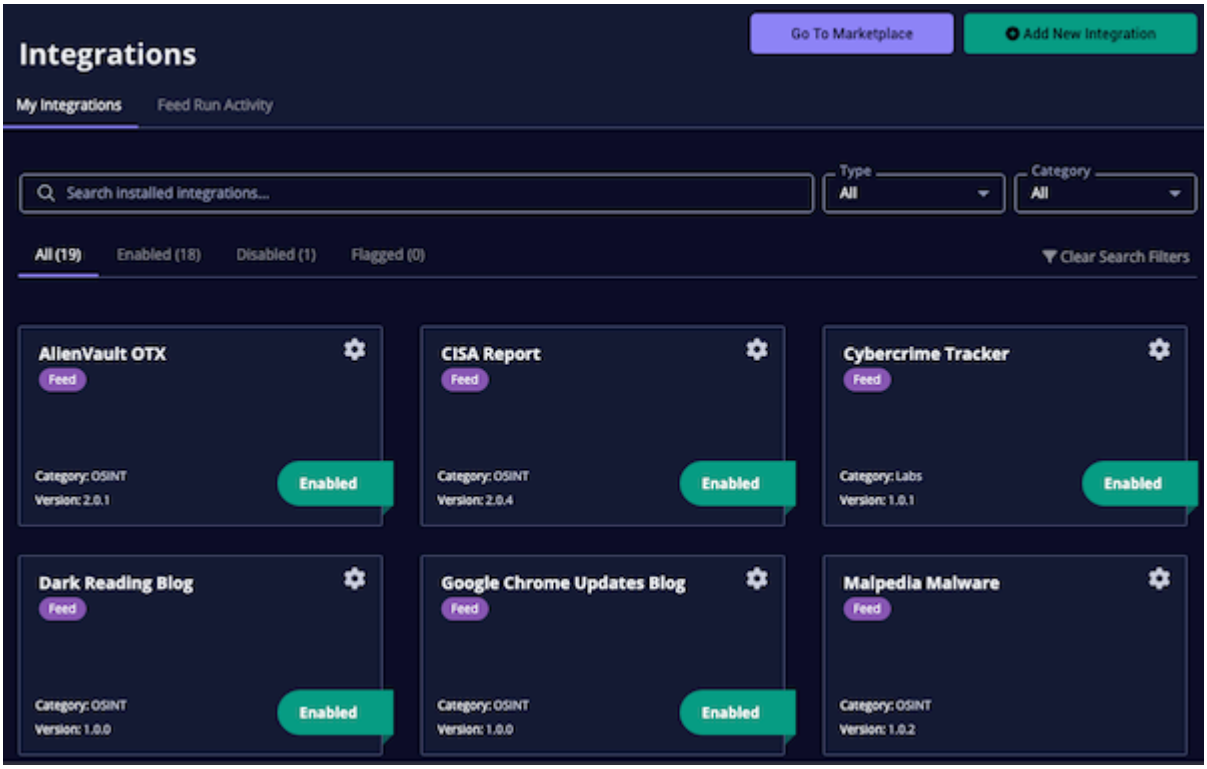
About My Integrations

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative or Maintenance
Custom Role - Action Permissions:

- Orchestration - Edit Orchestration Workflow (required for action type integrations only)
- Integrations - Install & Uninstall Integrations, Edit Integration Configurations

The My Integrations tab within the 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.



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

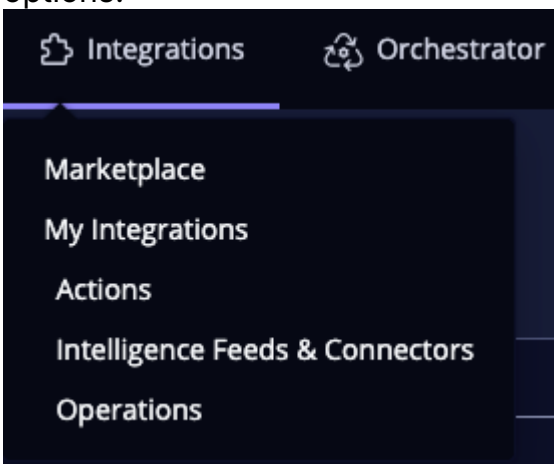
Relationship Limits

When ThreatQ ingests over 10,000 relationships for an object from the integration, the integration's card displays a relationship limit badge and is listed in the Flagged

tab. When you resolve the relationship issue, the relationship limit badge is removed and the integration card is no longer listed in the Flagged tab.

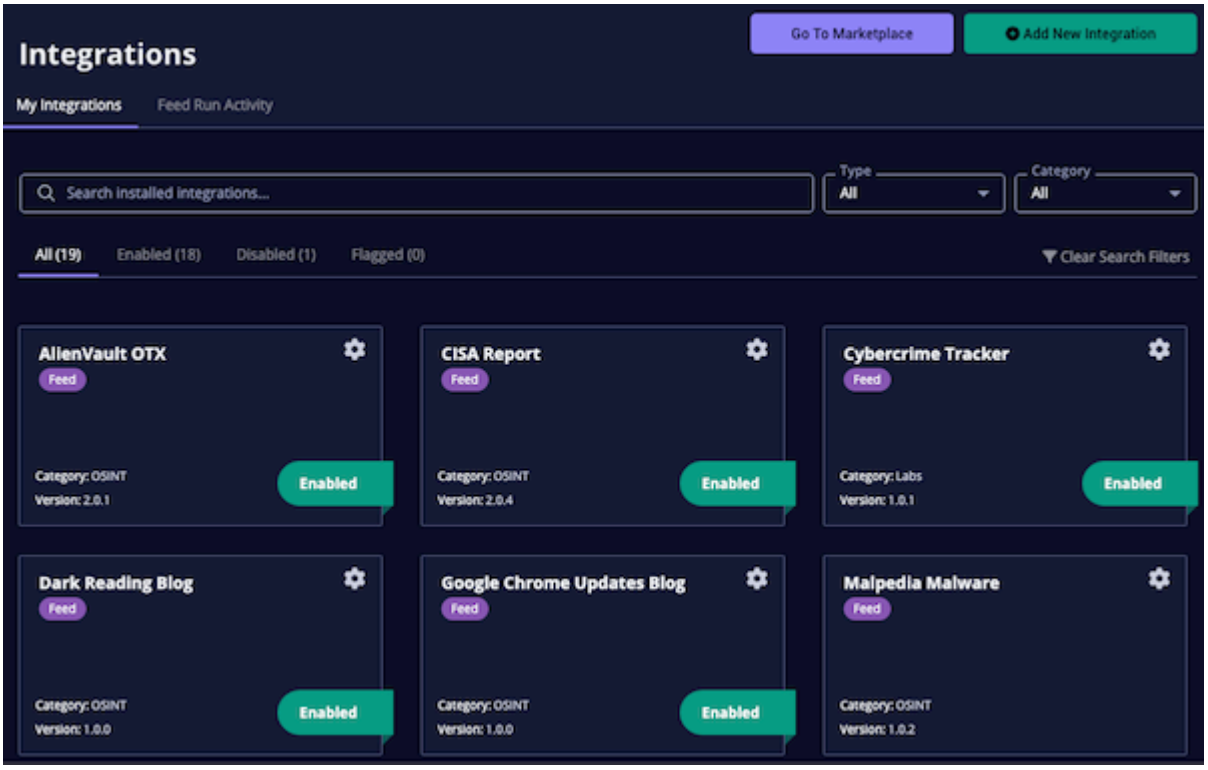
Accessing My Integrations

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 tab within the Integrations page.
Actions	Opens the My Integrations tab filtered to only display actions.
Intelligence Feeds & Connectors	Opens the My Integrations tab filtered to only display feeds and connectors.
Operations	Opens the My Integrations tab filtered to only display operations.

The Integrations page loads and defaults to the My Integrations tab and **All** subtab 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, disabled, or flagged. A count of integrations appears next to each tab and reflects any filter that is selected. The **Flagged** tab lists integrations from which the ThreatQ instance has ingested over 10,000 relationships for an object. ThreatQ will not ingest additional relational data for the object from this feed until the relationship limit issue has been resolved. The **All** tab, which displays both enabled and disabled integrations, is selected by default.
Clear Search Filters	Clears the search filters that are currently in use.

Flagged Integrations

THREATQ REQUIRED PERMISSIONS

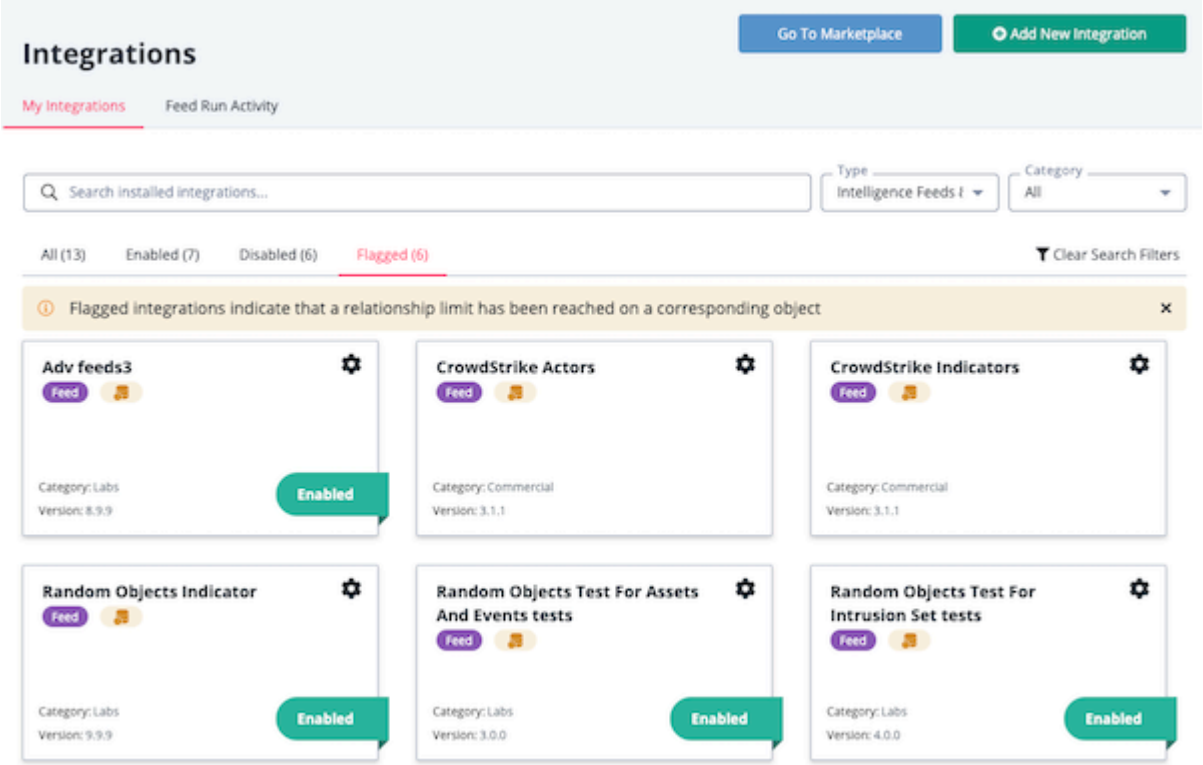
Default ThreatQ Role: Administrative or Maintenance
Custom Role - Action Permissions:

- Orchestration - Edit Orchestration Workflow (required for action type integrations only)
- Integrations - Install & Uninstall Integrations, Edit Integration Configurations

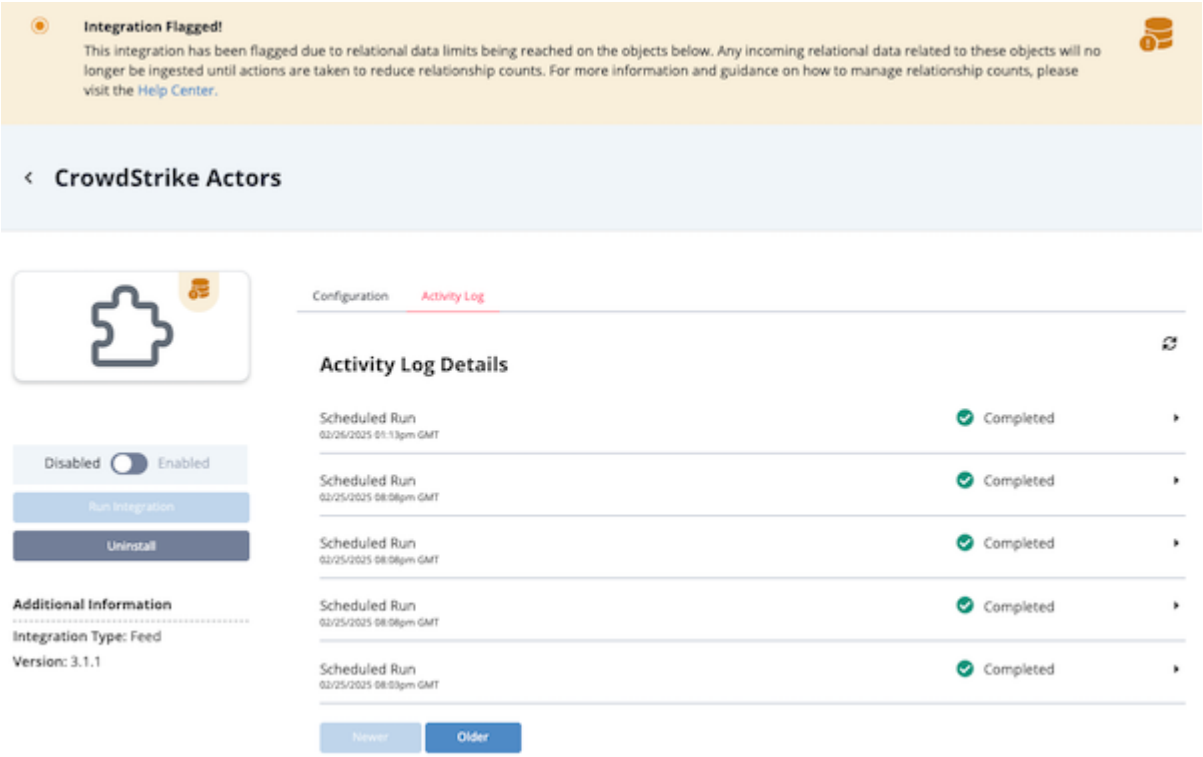
The Flagged tab in the My Integrations page lists all currently flagged integrations and displays a Flagged Integrations banner. An integration's card is added to the Flagged tab when ThreatQ ingests over 10,000 relationships for an object from the integration. The integration is displayed in the Flagged tab until you resolve the relationship issue.

From the Flagged tab, you can:

- Click an integration's card to view its configuration page.
- Close the Flagged Integrations banner by clicking the X in the upper right corner.
- Filter your view by integration type and/or category.
- Use the search field to locate a flagged integration.



The Integration Flagged banner is displayed at the top of the integration details page for each flagged integration. The banner cannot be closed by a user and is displayed until you resolve the relationship issue.



Adding an Integration

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative or Maintenance
Custom Role - Action Permissions:

- Orchestration - Edit Orchestration Workflow (required for action type integrations only)
- Integrations - Install & Uninstall Integrations, Edit Integration Configurations

The steps for upgrading an integration are the same as adding a new integration. You can use the steps below to install CDFs (.yml) and Operations (.whl).

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

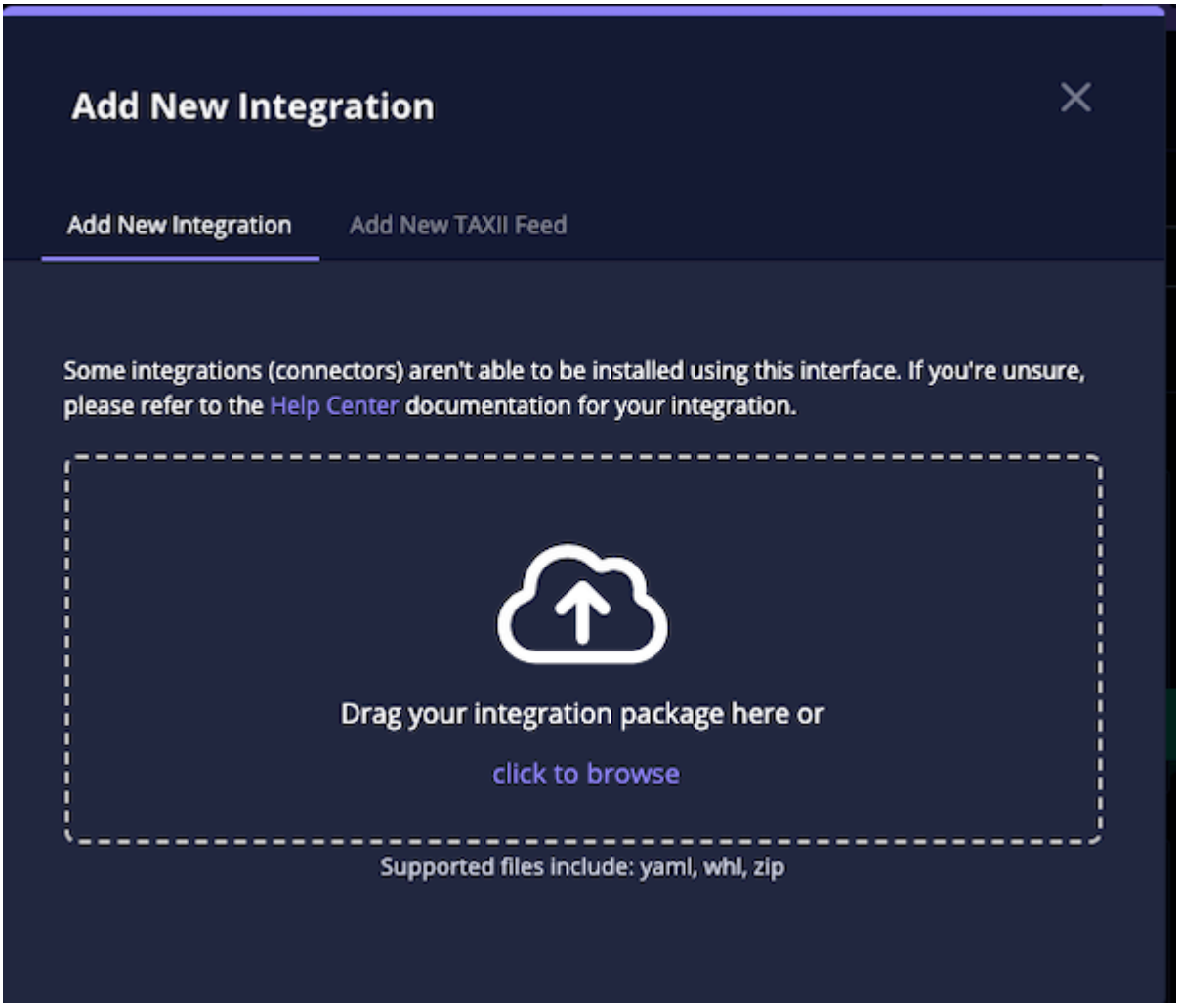
Steps for installing TQO Actions differ slightly in that you can install using a zip file (**actions are the only integration type that can be installed by uploading a zip file**) - see the Installing an Action topic in the ThreatQ Orchestrator guide for more details. Custom connectors and Apps can not be installed using the method described below (UI install) - see the individual user guide for installation steps.

1. Log into https://marketplace.threatq.com.
2. Locate and download the desired integration file.

   CDF or Operation downloads that are in a zip format indicate that additional dependencies, other than the standard whl or yaml, are required. Extract the files from the zip and refer to the integration's individual guide on how to install them.

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

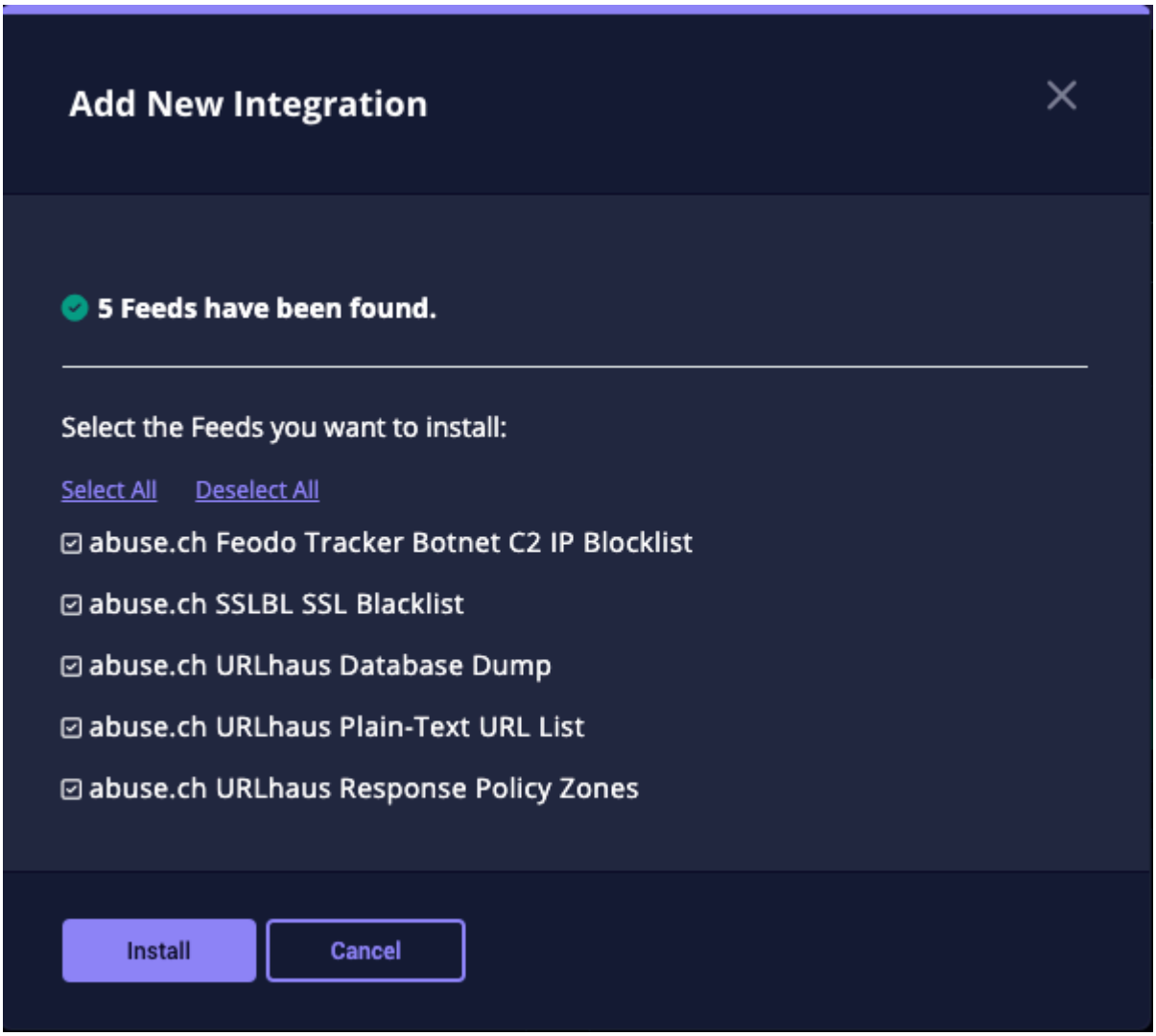
For CDFs, you will upload the yaml file only. For Operations, you will upload the whl file only. Custom connectors, which are typically in a whl format, **cannot** be installed using the UI and require installation via CLI. TQO Actions are the only integrations that support installation using the zip format - see the Installing an Action topic in the ThreatQ Orchestrator guide for more details.

If the ThreatQ Marketplace download for a CDF or Operation is in zip format, a separate dependency or custom object is required by the integration and is included in the download. These additional files cannot be installed via the UI uploader nor can you upload the zip file to install.

See the integration's user guide for steps on how to install these additional files.

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**.



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

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative or Maintenance

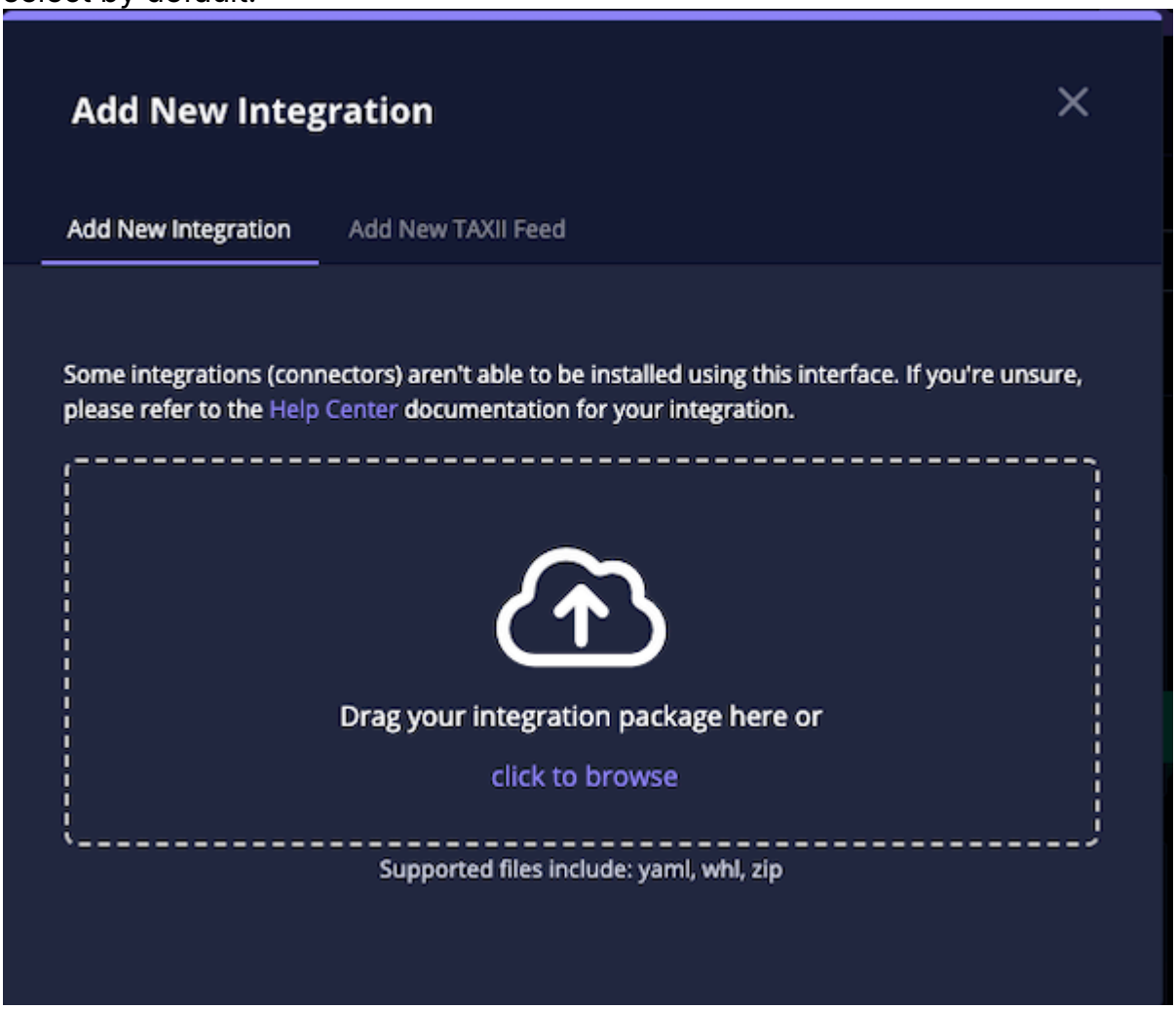
Custom Role - Action Permissions: Integrations - Install & Uninstall Integrations, Edit Integration Configurations

From the My Integrations page:

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

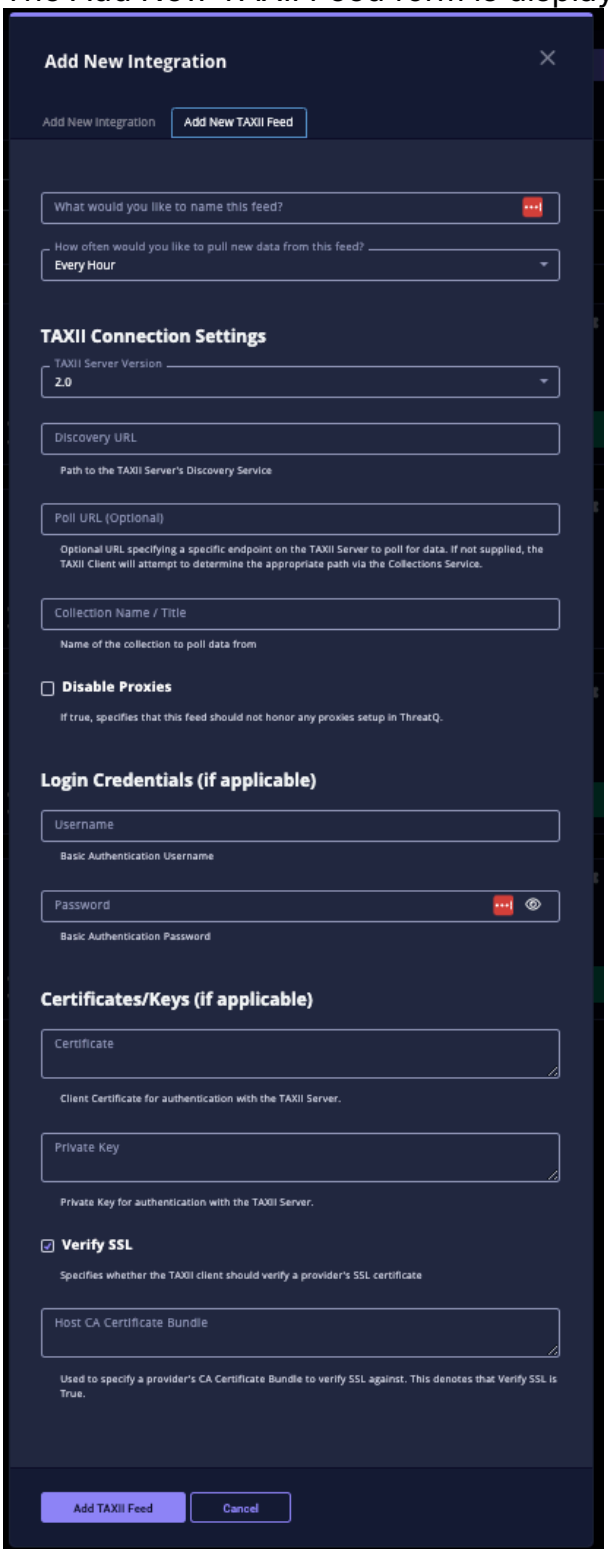
1. Click the **Add New Integration** button.

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



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

   The Add New TAXII Feed form is displayed.



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, 2.1. 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/Title	The name of the collection of data in the feed you will access. This field is required.
Login Credentials	
Username	If required, enter a username for the feed.
Password	If required, enter a password.
Certificates/Keys	
Certificate	If required, enter a certificate if required for the feed.

FIELD	INSTRUCTIONS
Private Key	If required, enter a private key if required for the feed.
Server Authentication	
Verify SSL	Leave the checkbox checked to require that the TAXII client verify the provider's SSL certificate.
Host CA Certificate Bundle	The provider's CA Certificate used to verify SSL. The Host CA Certificate Bundle will not be honored if the Verify SSL option is not selected.

4. Click **Add TAXII** Feed.

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

Configuring an Integration

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative or Maintenance

Custom Role - Action Permissions:

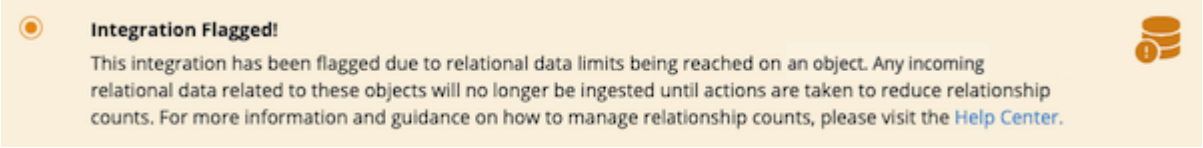
- Orchestration - Edit Orchestration Workflow (required for action type integrations only)
- Integrations - Edit Integration Configurations

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.

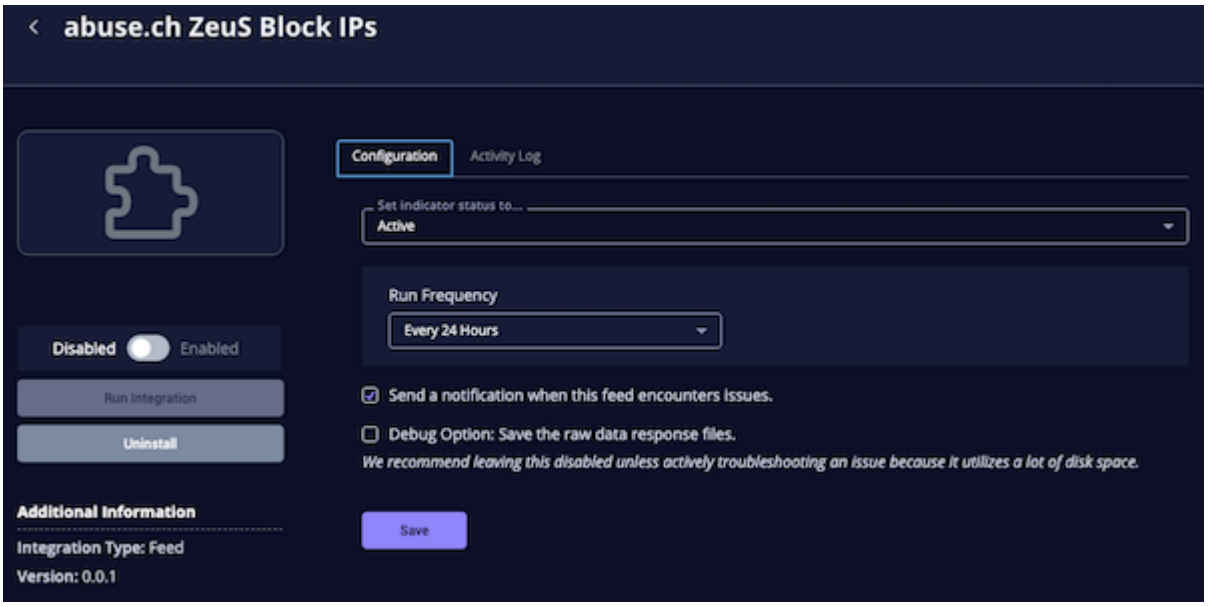
Relationship Limits

When ThreatQ ingests over 10,000 relationships for an object from the integration, integration's configuration page displays an Integration Flagged banner as well as a relationship limit badge above the integration logo.



From the My Integrations page:

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



   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

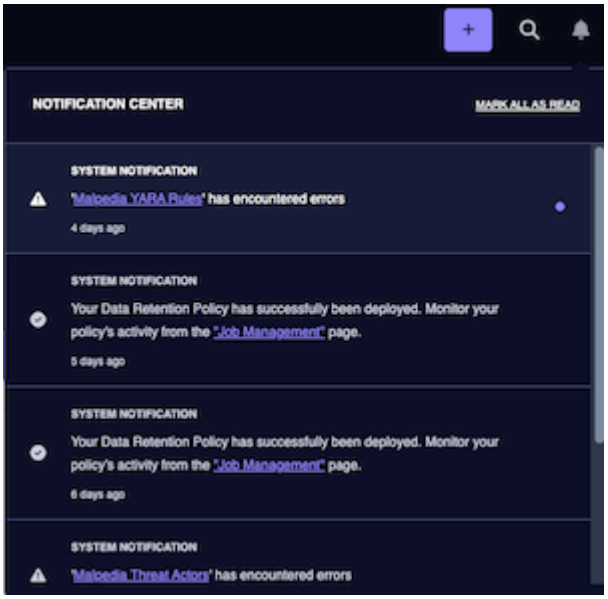
SELECTION	DESCRIPTION
Daily	Allows you to run the integration at a specific time every day.
Weekly	Allows you to run the integration at a specific time, on a specific day, every week.

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

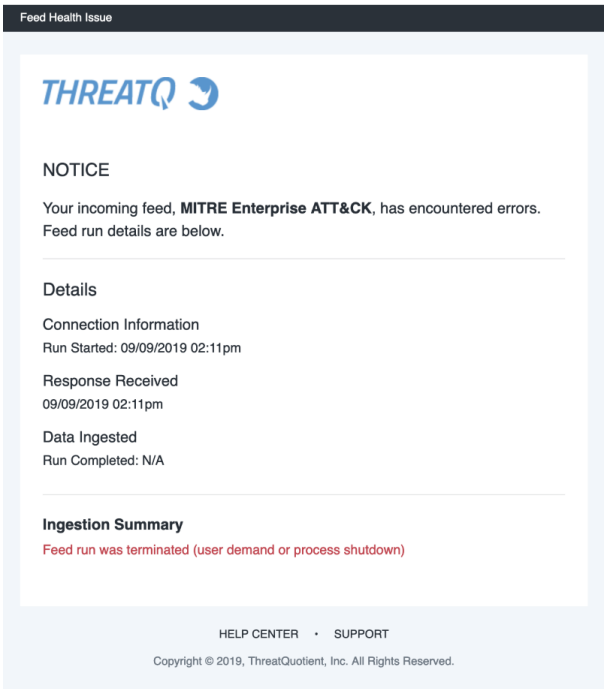
   This configuration option will only be available if the integration ingests indicator or signature types.

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. CDFs Only - Enable or disable the **Debug option**- 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. Operations Only - Enable or disable the **Enable this operation for use by your ThreatQ MCP server** option. Enabling this option allows the Threat Research Agent, when active, to utilize the operation's functions and processes to curate and enrich data.
8. Click **Save**.
9. Click the **Enable/Disable** toggle switch to enable the integration.

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

Triggering a Manual Run

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative or Maintenance

Custom Role - Action Permissions:

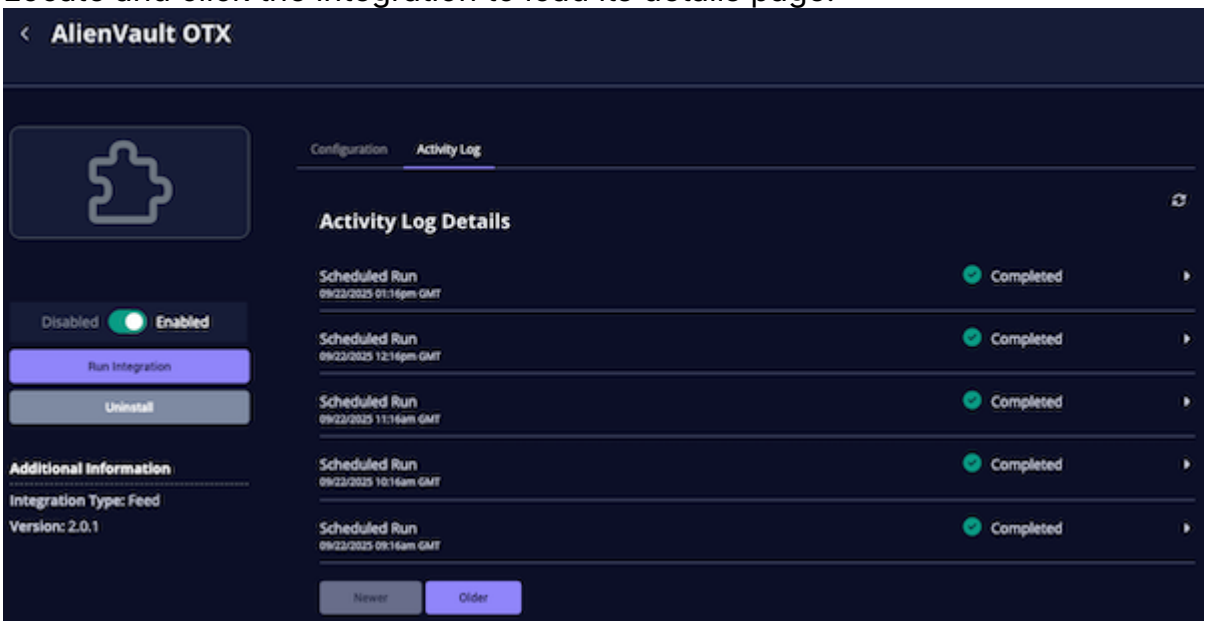
- Orchestration - Edit Orchestration Workflow (required for action type integrations only)
- Integrations - Edit Integration Configurations
- Custom role permissions control access to the pages that allow you to execute manual runs of integrations. However, custom roll permissions do not apply to the objects and object context created/ingested.

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.



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

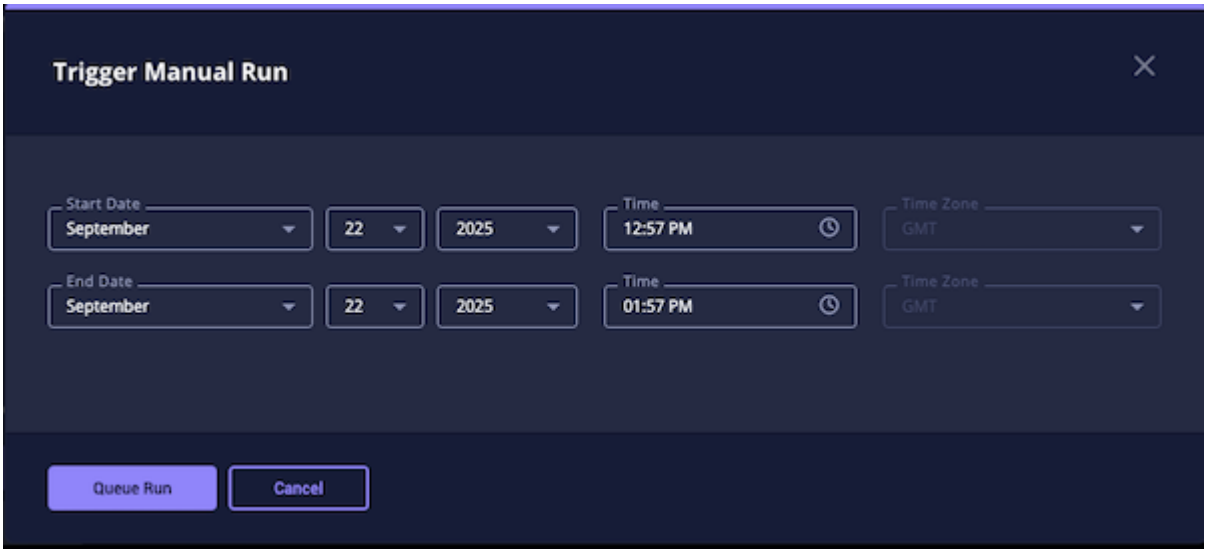
2. Confirm that the integration is enabled.

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, such as TAXII 2.0 and 2.1 feeds, only support a Start Date.

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

Running an Operation

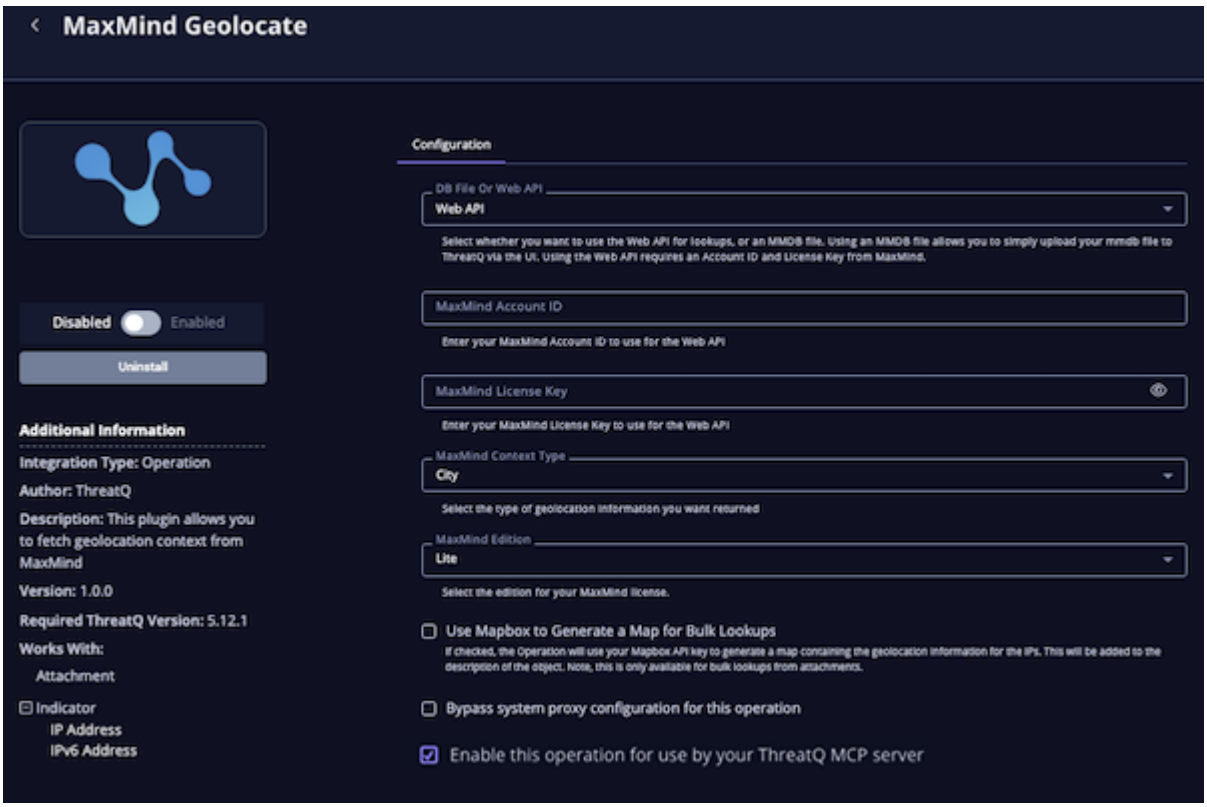
THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Primary Contributor or Administrative or Maintenance

Custom Role - Action Permissions: Integrations - Run Operations

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

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



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)

THREATQ REQUIRED PERMISSIONS

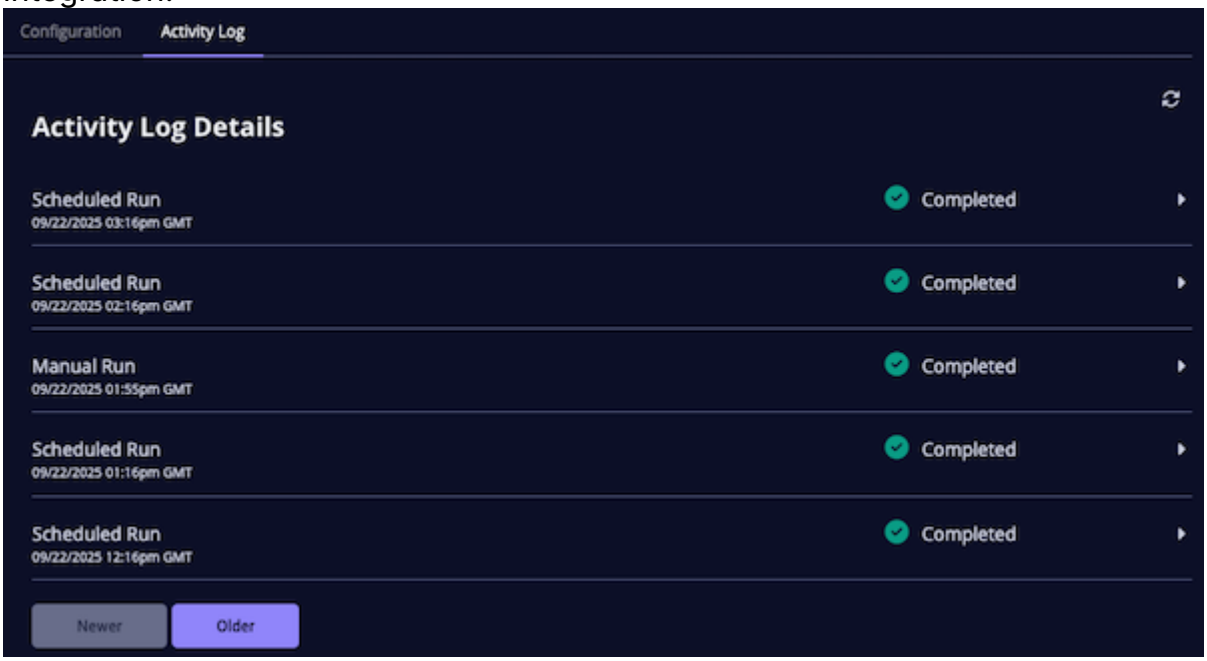
Default ThreatQ Role: Administrative or Maintenance

Custom Role - Action Permissions: Integrations - Edit Integration Configurations, Run Operations

ThreatQ allows you to view feed run activity for individual CDFs from the Activity Log in a CDF's configuration page and to access information on all feed runs over the past ninety days from the Feed Run Activity tab in the Integrations page.

Activity Log Details

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

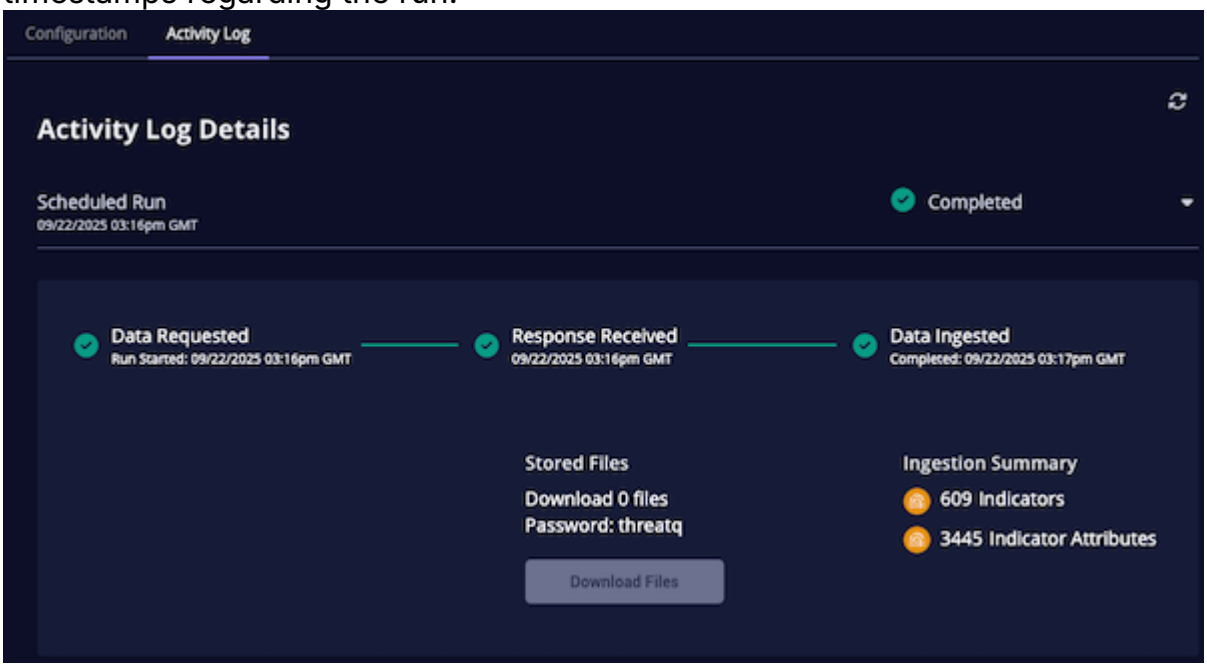


The Log Details section displays run details that include:

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.

LOG DATA	DETAILS
Outcome	Whether the run completed successfully or if it encountered errors.

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



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

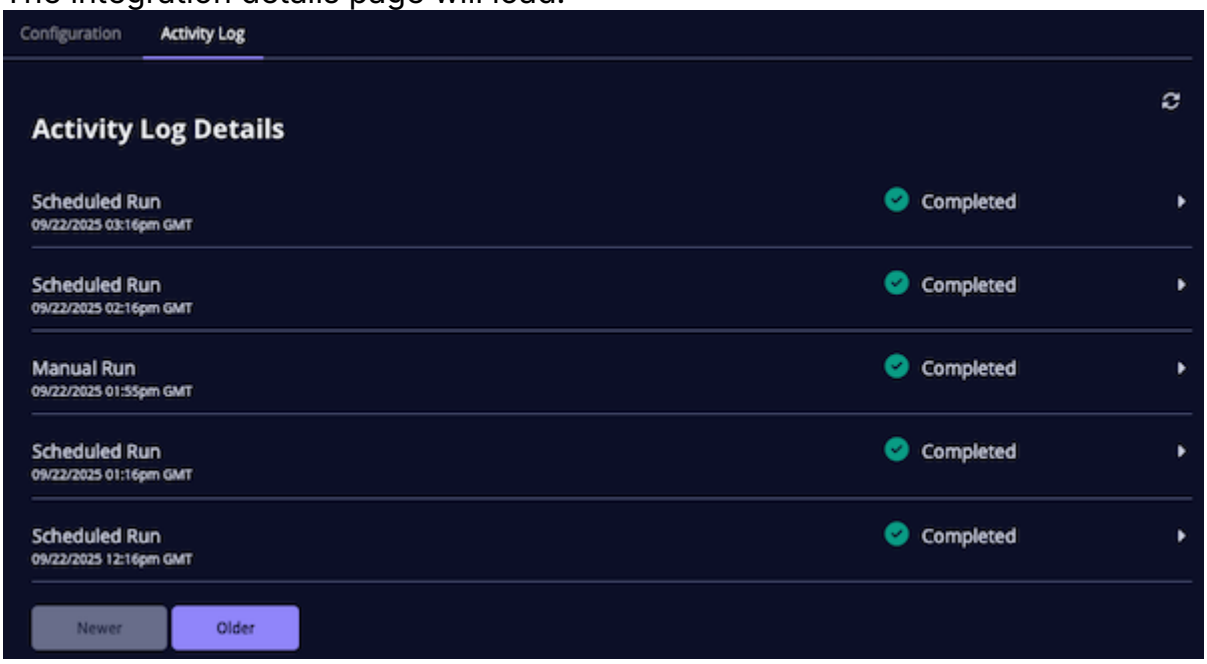
FIELD	DESCRIPTION
Ingested Summary	A summary of ingested object types.

Accessing a CDF's Activity Log

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

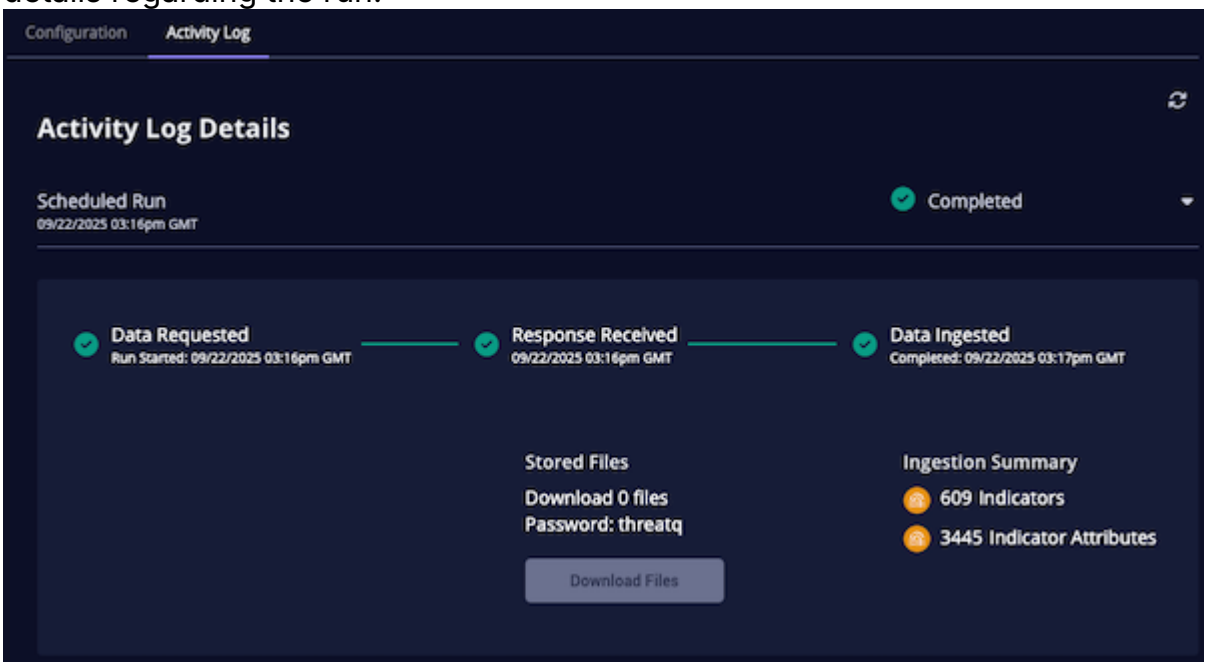
1. Locate and click on the integration to load its details page.

   The integration details page will load.



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.



Feed Run Activity

THREATQ REQUIRED PERMISSIONS

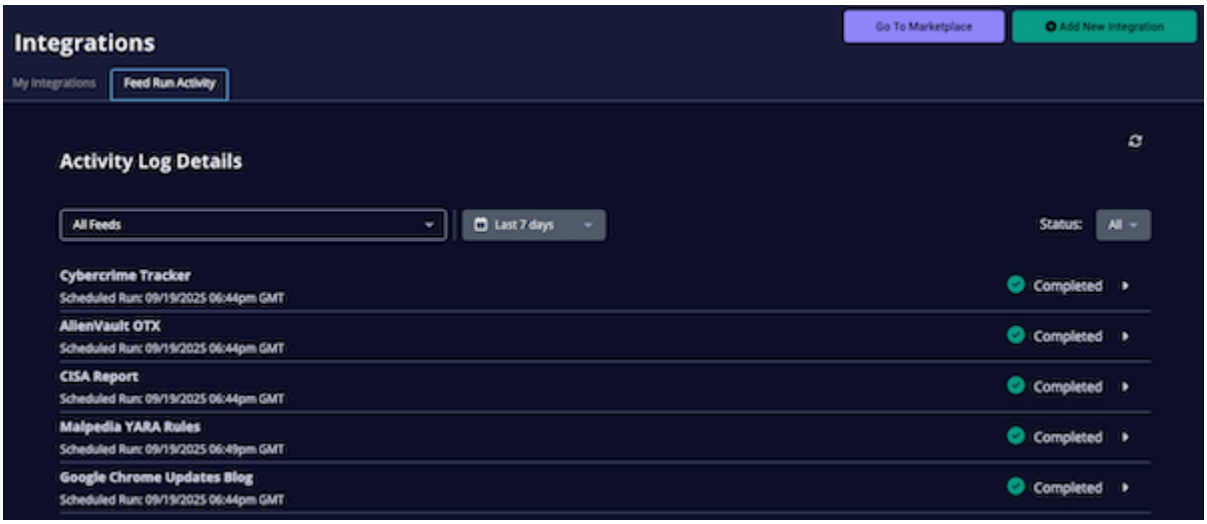
Default ThreatQ Role: Administrative or Maintenance

Custom Role - Action Permissions: Integrations - Install & Uninstall Integrations

ThreatQ allows you to view feed run activity for individual CDFs from the Activity Log in a CDF's configuration page and to access information on all feed runs over the past ninety days from the Feed Run Activity tab in the Integrations page.

Feed Run Activity Details

The Feed Run Activity tab lists feed run activity for all installed feeds on the ThreatQ instance within the last ninety days. By default, this tab lists the last seven days of activity but can be updated to display the last twenty four hours, thirty days, or ninety days of activity. You can also filter the display by feed name, feed run status, or view all feeds. You can click a feed run to view more information on it or to run the feed again.

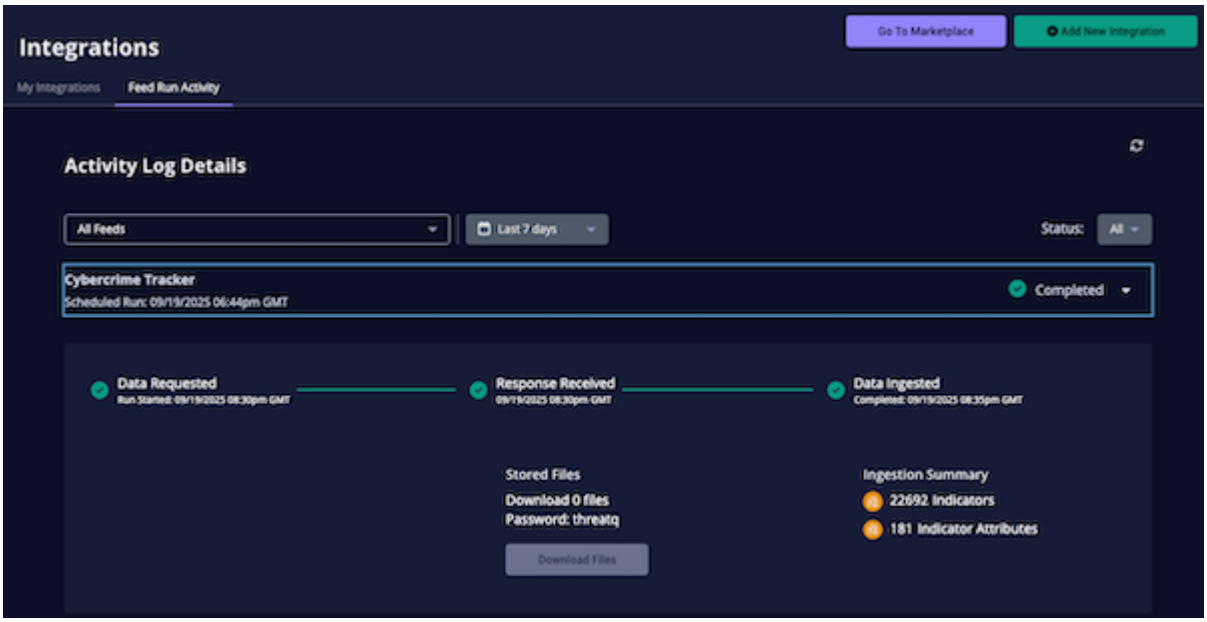


The feed run list displays run details that include:

FIELD	DESCRIPTION
Feed Name	The integration name.
Type of Run	Whether the run was scheduled or triggered manually.

FIELD	DESCRIPTION
Date and Time	When the run, data and time, was initiated.
Feed Run Status	Whether the run completed, completed with errors, or failed.

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.



Accessing Feed Run Activity

1. Navigate to your ThreatQ instance.
2. Click the **Integrations** option in the main navigation
3. Click the Feed Run Activity tab.
   By default, this tab lists all feed runs within the last seven days.
4. From this tab you can:
   - **Select a new feed run timeframe** - Click the calendar field to select the last twenty four hours, thirty days, or ninety days of activity.
   - **Filter the list by feed name** - Click the feed field to view all feed runs for a specific feed within the selected timeframe.
   - **Filter the list by feed run status** - Click the Status field to limit the list to feed runs with a status of Completed, Completed with errors, or Run failed.

- **View feed run details** - Click on the arrow icon located next to a run's outcome status to view additional details regarding the run.
- **Refresh the feed run list** - Click the refresh button in the upper right corner.

Removing an Integration

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative or Maintenance

Custom Role - Action Permissions:

- Orchestration - Edit Orchestration Workflow (required for action type integrations only)
- Integrations - Install & Uninstall Integrations

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.

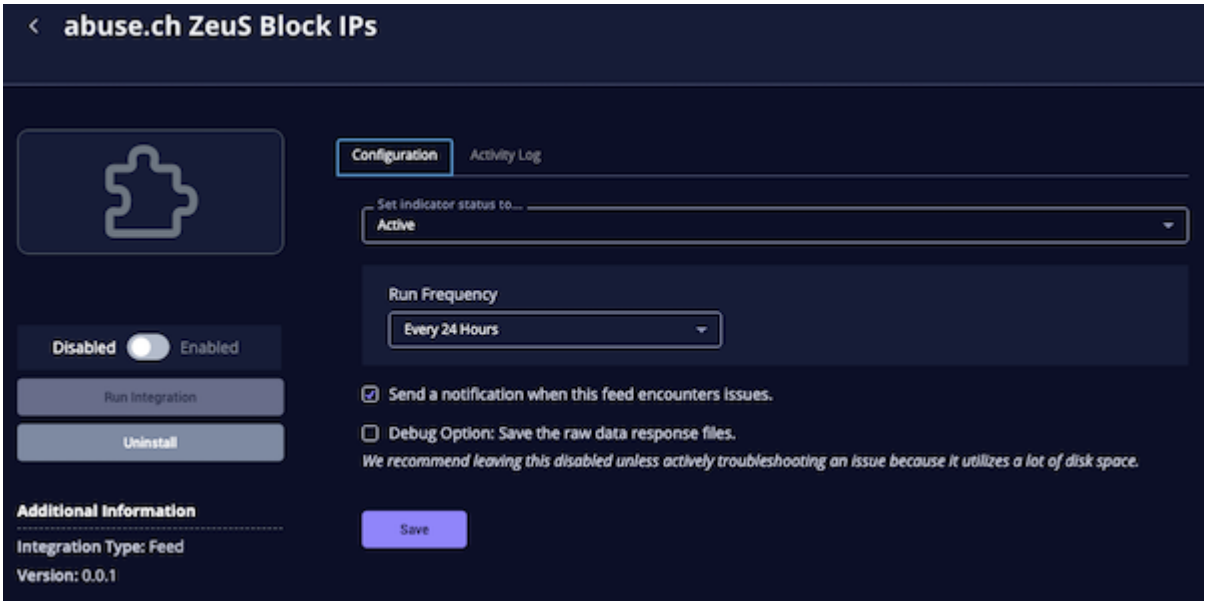
Neither action will affect the threat data that you have already ingested into your ThreatQ instance.

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.



> 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.

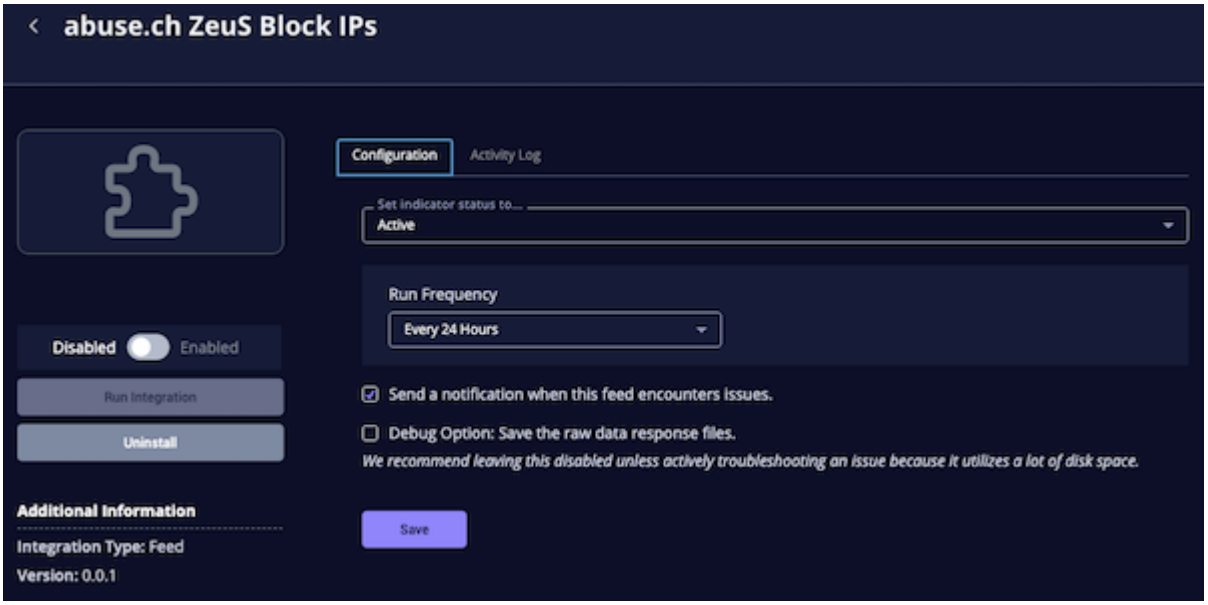
3. Click **Uninstall** to confirm and remove the integration.

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.



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

Job Management

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative or Maintenance
Custom Role - Action Permissions: Administrative Functions - View 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:

  If a Delete, Update, or Relationship job includes system objects filtered by TLP, the job details view includes a Global filters section in the Search Criteria column.

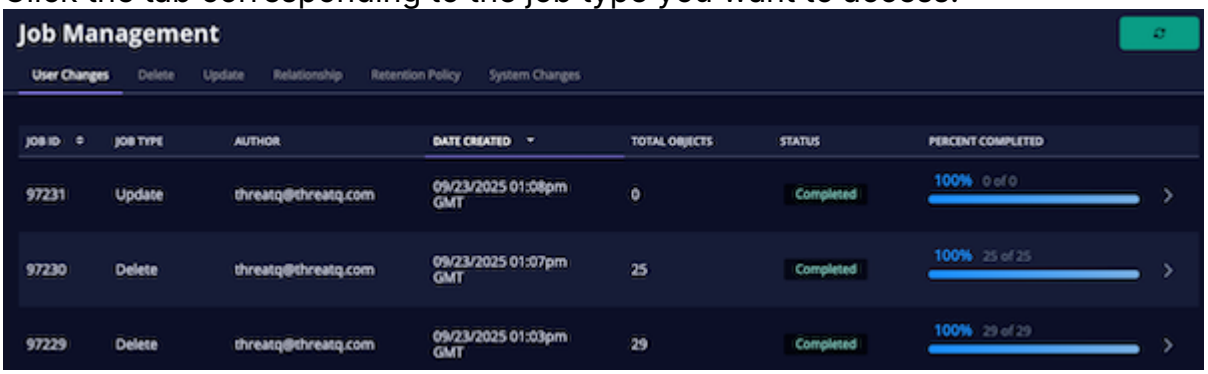
JOB TYPE	DETAILED VIEW INCLUDES...
Delete	• **Object Type** • **Search Criteria** • **Activity** - Lists Start Time and Completed or Failed At timestamps • **Error Message**

Update	• **Object Type** • **Search Criteria** • **Update -** Attribute names displayed in this field are truncated after fifty characters. • **Activity** - Lists Start Time and Completed or Failed At timestamps • **Error Message**
Relationship	
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 Changes	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 User Changes tab is displayed. This tab lists all bulk action jobs. Click the tab corresponding to the job type you want to access.



   The Job Management page allows you to view the following details about Bulk Action, Data Retention, and System Change 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. • **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

FIELD	DESCRIPTION
	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 About Installing ThreatQ. Any subsequent license updates can be applied in the ThreatQ user interface.

Access to additional ThreatQ products, such About 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.

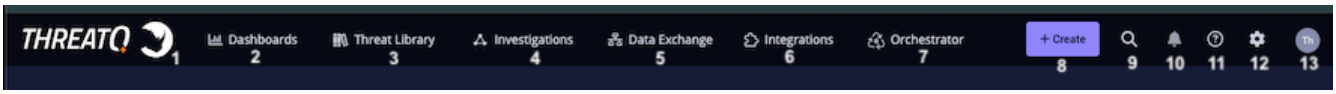
Updating a License

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 Page • Bulk Actions • About Data Controls
4	Investigations	Navigates to ThreatQ Investigations (TQI), a cybersecurity situation room that enables collaborative threat	• About ThreatQ Investigations

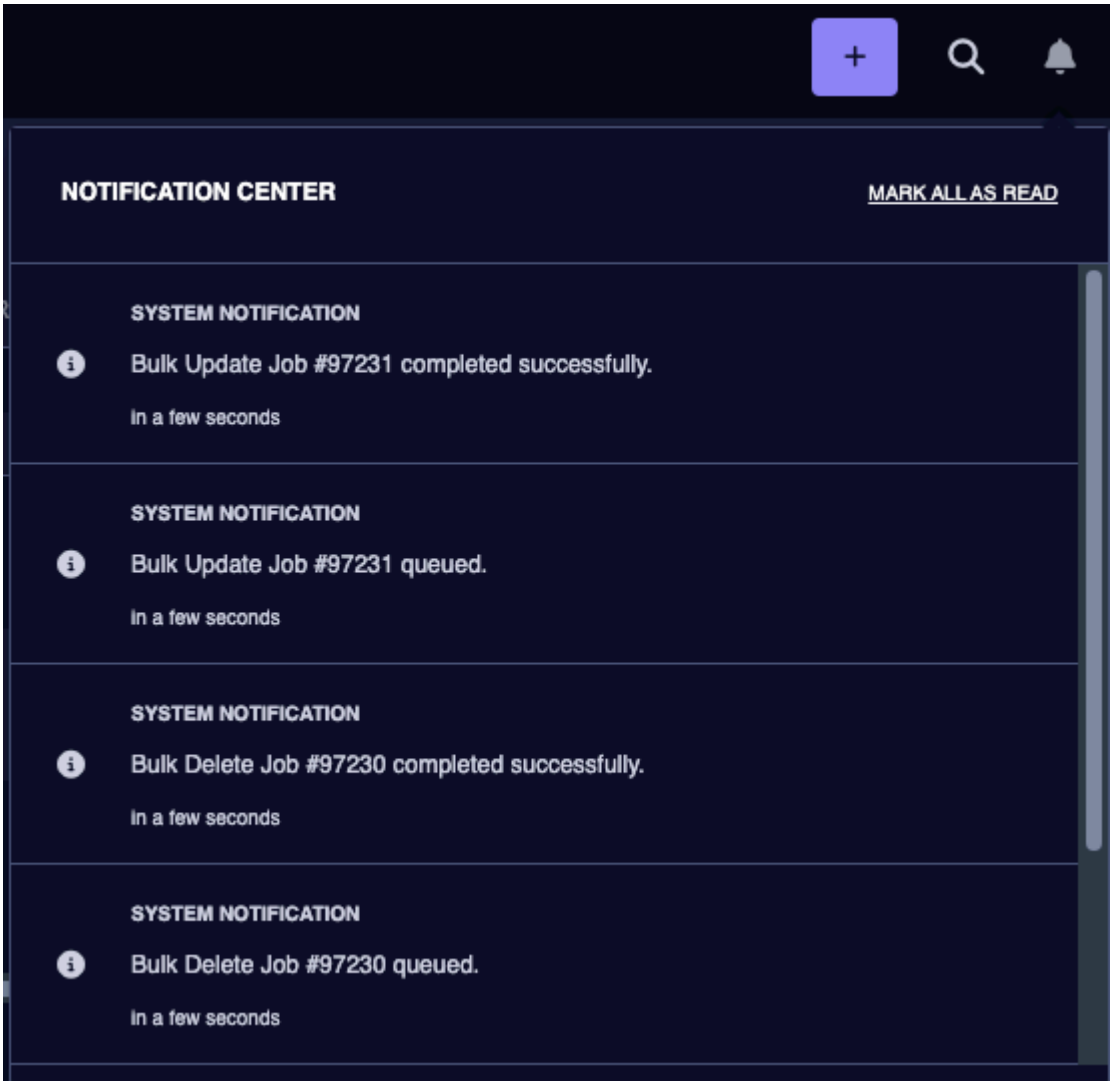
#	NAME	DESCRIPTION	REFERENCES
		analysis, investigation, and coordinated response.	
5	Data Exchange	Allows the bi-directional sharing of threat intelligence across multiple ThreatQ instances.	• About ThreatQ Data Exchange
6	Integrations	Allows you to access the Marketplace as well as you integrations.	• 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 ThreatQ Orchestrator
8	Create Button	Create system objects.	• About System Objects
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

#	NAME	DESCRIPTION	REFERENCES
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.	• About Product Updates • About Installing ThreatQ • All Videos
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

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
- User role permission 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 preforming a run.

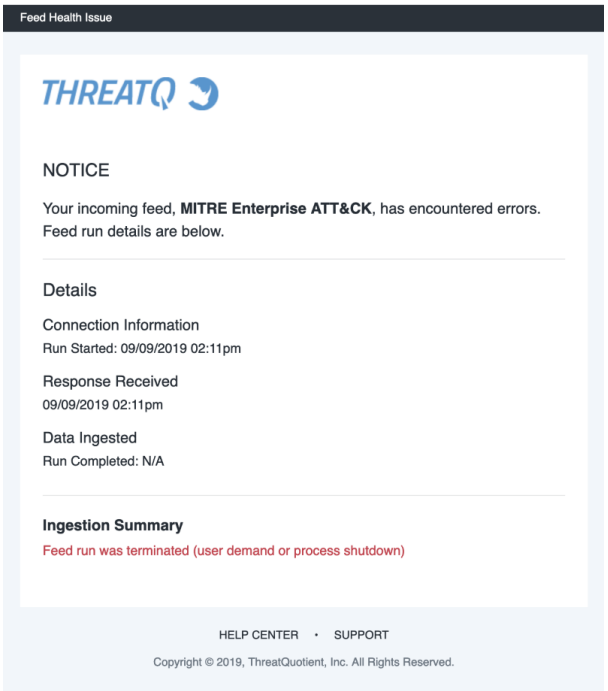
Feed Health Email Notifications

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative or Maintenance
Custom Role - Action Permissions: Administrative Functions - Edit System Configurations, Edit Notification Settings, Edit Integration Configurations, See the Interdependent Permissions topic.

Feed Health Notifications allow 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.

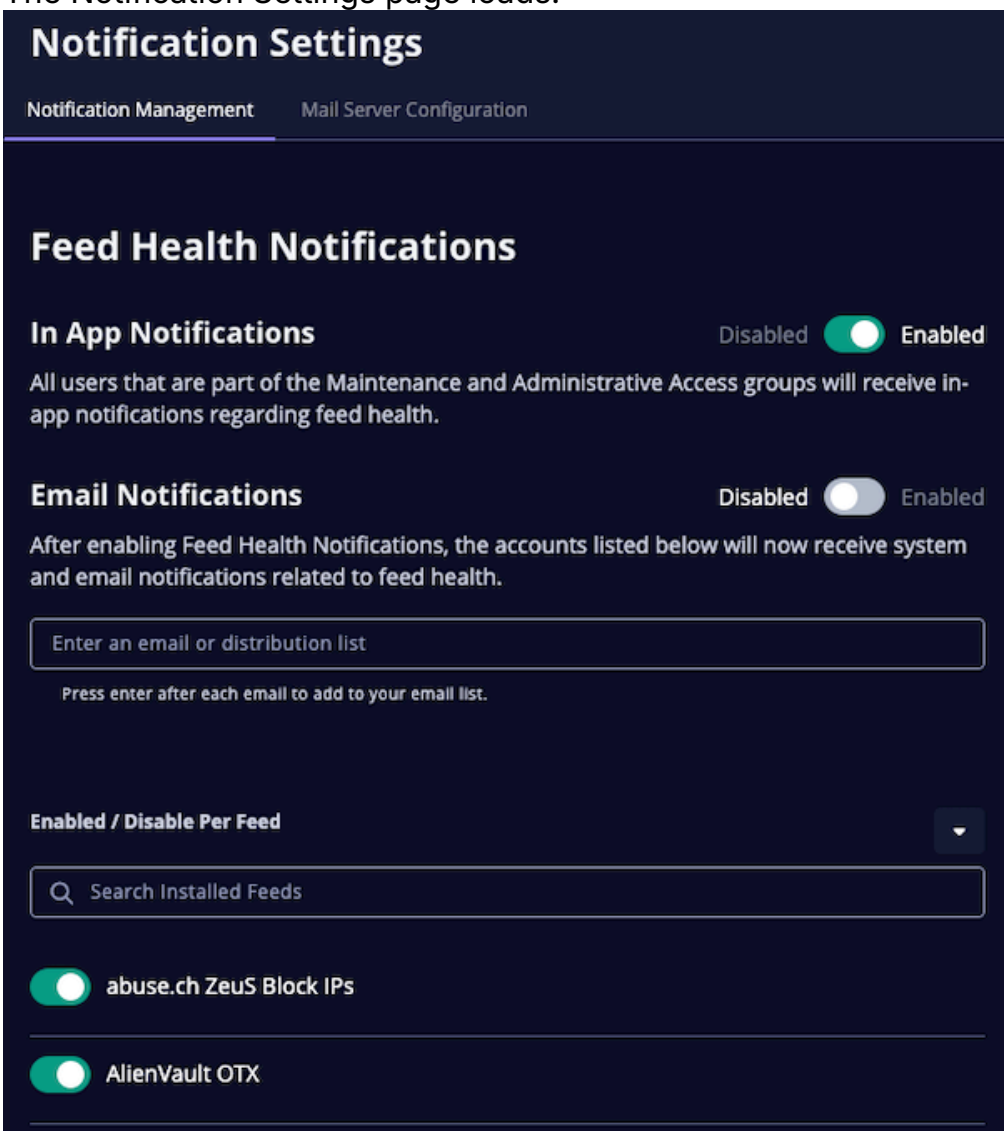
In the event that you have completed the mail server configuration and are still not receiving emails, your email provider may have marked the activity as suspicious. Some services, such as Gmail, will require you to confirm the activity, via an email message, before allowing the ThreatQ application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

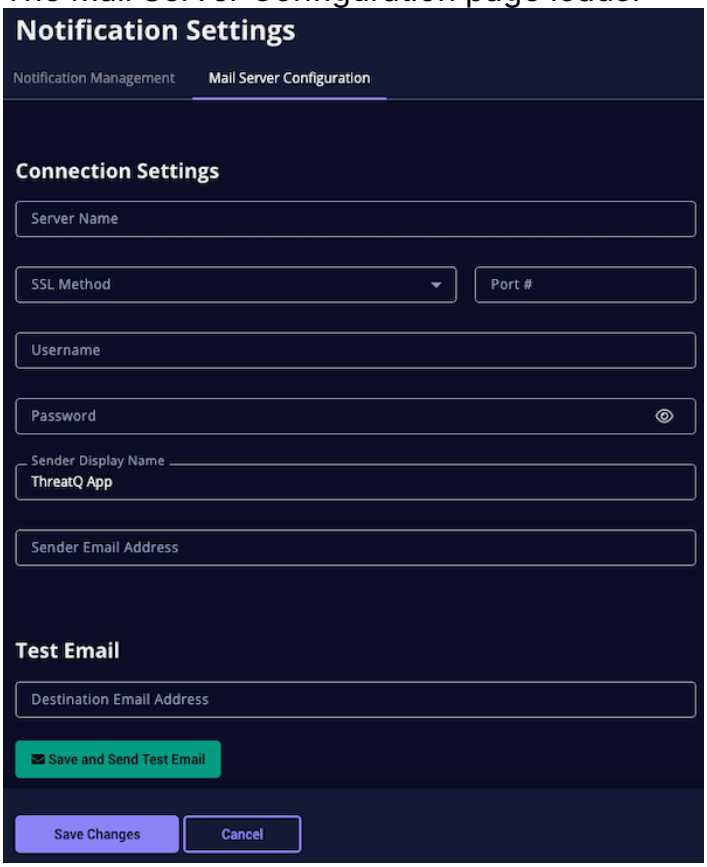
1. Click on the **System Settings** gear icon and select the **Notification Settings** option.

   The Notification Settings page loads.



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

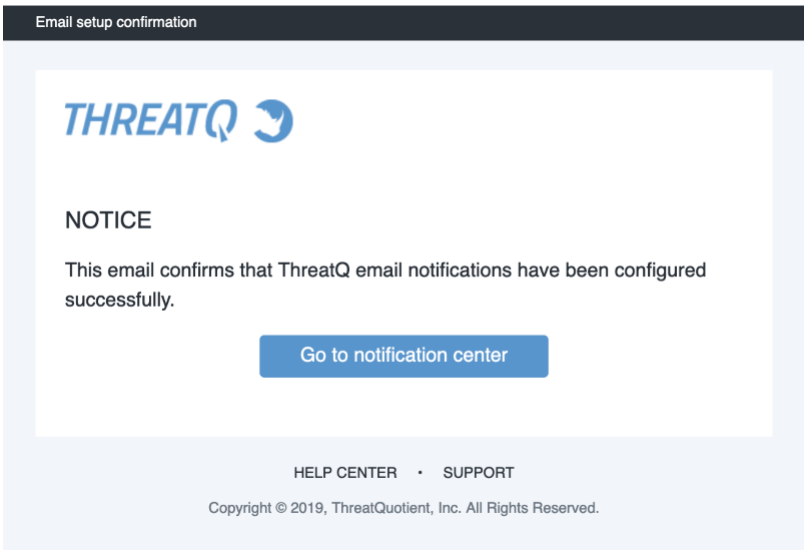
The Mail Server Configuration page loads.



3. Complete the following fields:

FIELD	DESCRIPTION
Server Name	The address of your mail server.
SSL Method	The SSL method used. There are three options: ◦ 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.

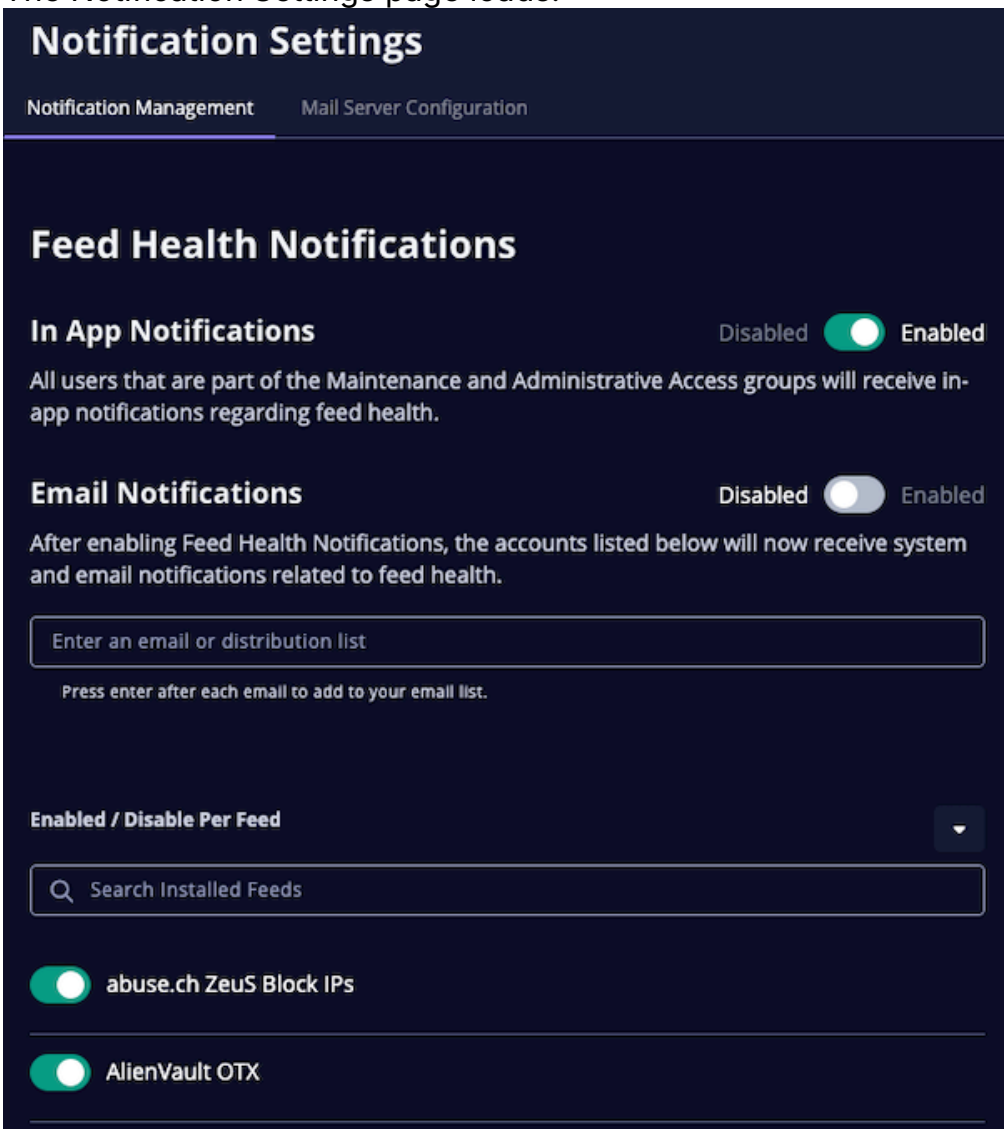
If using Email Notifications, the Mail Server Configuration tab must completed before you enable the feature.

> In the event that you have completed the mail server configuration and are still not receiving emails, your email provider may have marked the activity as suspicious. Some services, such as Gmail, will require you to confirm the activity, via an email message, before allowing the ThreatQ application to continue to use the server to send emails. A common symptom found in the error log is that you will receive an “incorrect password” error. If you are certain that the password you provided is correct, your mail service is likely blocking the service and requires your confirmation to proceed.

To Enable Feed Health Notifications:

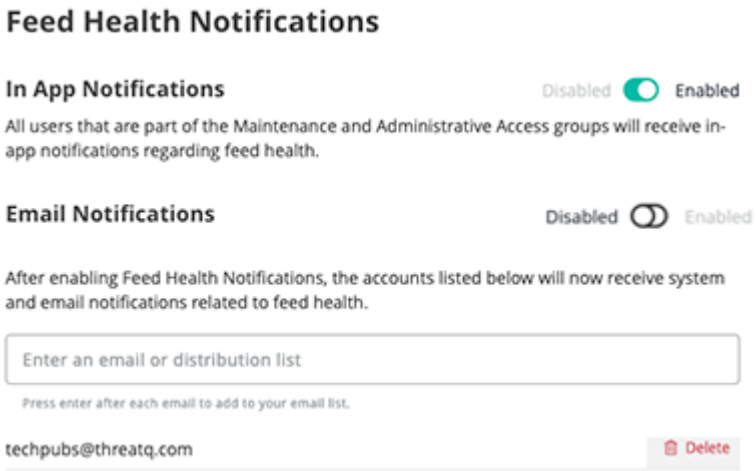
1. Click on the **System Settings** gear icon and select the **Notification Settings** option.

The Notification Settings page loads.



2. Perform the following steps to enable email and in-app notifications:
   - *Enable In-App 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.



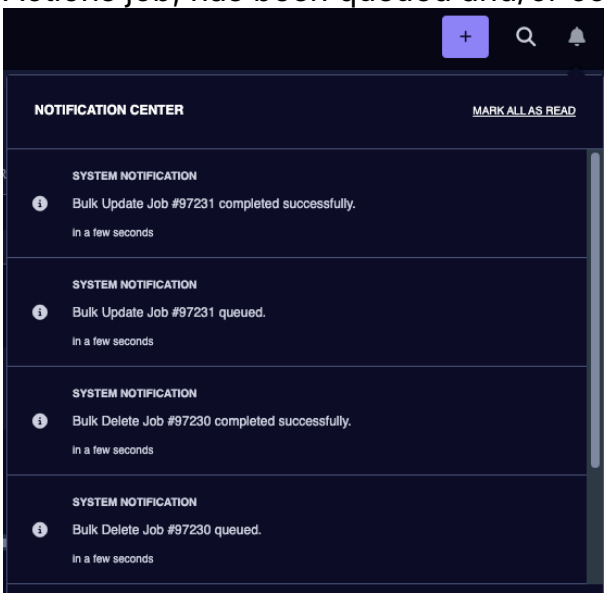
2. Click on the **Enable** toggle switch for **Email Notifications**.

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

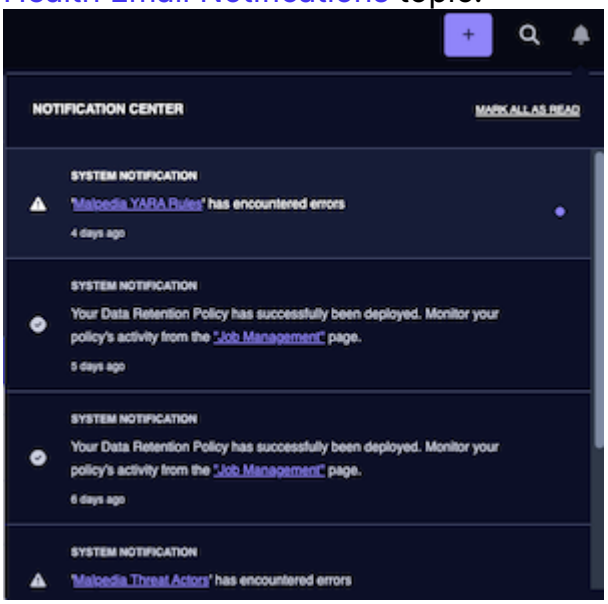
> You can also enable/disable individual CDF feed notifications by clicking on the feed under Integrations and checking/unchecking the notifications checkbox.

Notification Center

The notification 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.

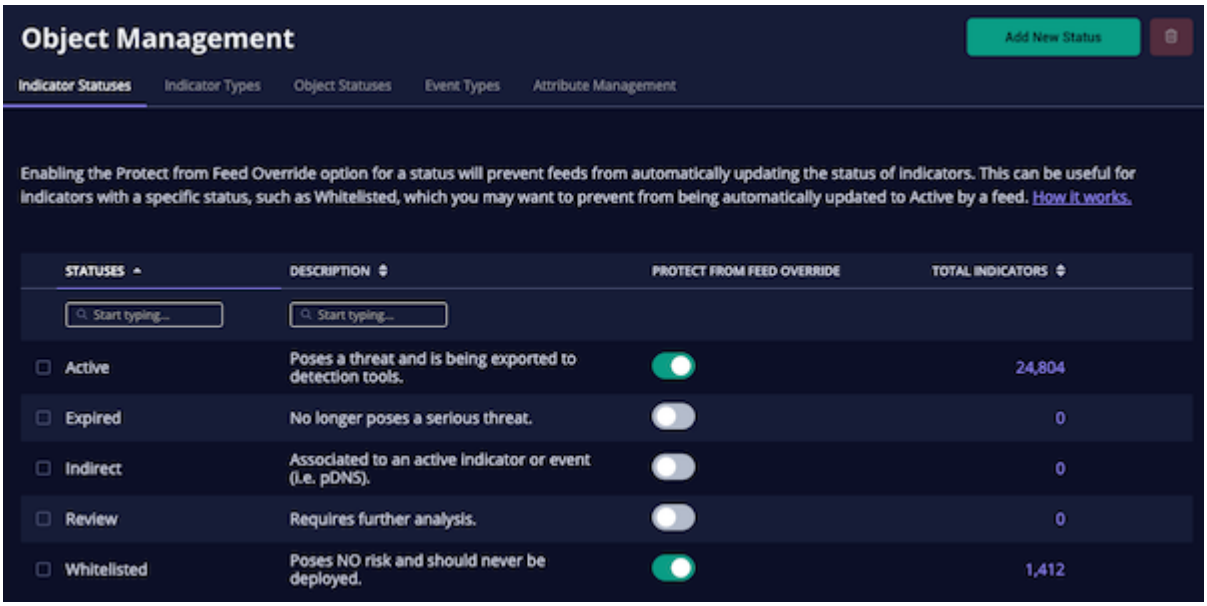
SCENARIO	VIEWER	EDITOR	OWNER
A user shares a data collection, dashboard, or investigation with you.	`You have been added as a Viewer to` ***`<Name>`***	`You have been added as an Editor to` ***`<Name>`***	N/A
A user changes your permissions to editor or viewer.			
A user changes your permissions to owner.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

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

Object Management

About Object Management

The Object Management page consists of five tabs, Indicator Statuses, Indicator Types, Object Statuses, Event Types, and Attribute Management. These tabs allow you to create and manage data points used to enrich system objects.



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.
Object Statuses	Create and edit custom and seeded object statuses.
Event Types	Create and edit custom event types.
Attribute Management	Update attribute keys and values associated with system objects.

Indicator Statuses Management

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role - Action Permissions: Objects & Context - Manage Object Statuses

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

Indicator Status Assignment

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

Indirect Indicator Status

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

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

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

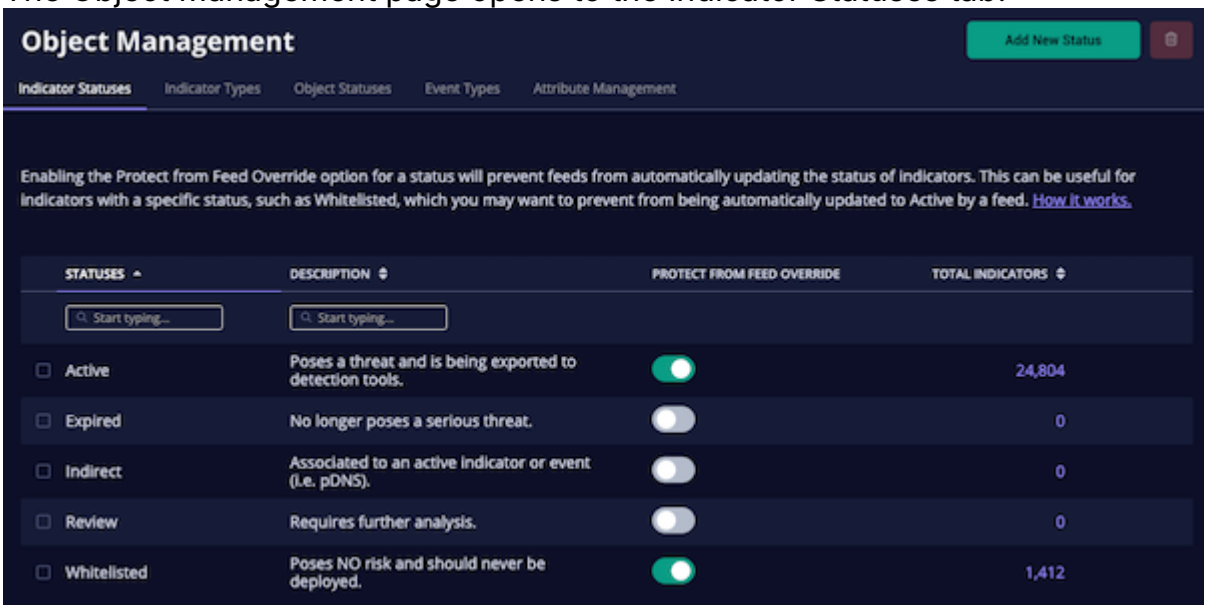
Protected Indicator Statuses

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

Viewing Indicator Statuses

1. Navigate to Settings ⚙ > Object Management.

The Object Management page opens to the Indicator Statuses tab.



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

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

Indicator Statuses Table Functions:

FUNCTION	DESCRIPTION
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.

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

Suppressing Indicator Status Updates

Enabling the **Protect from 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.

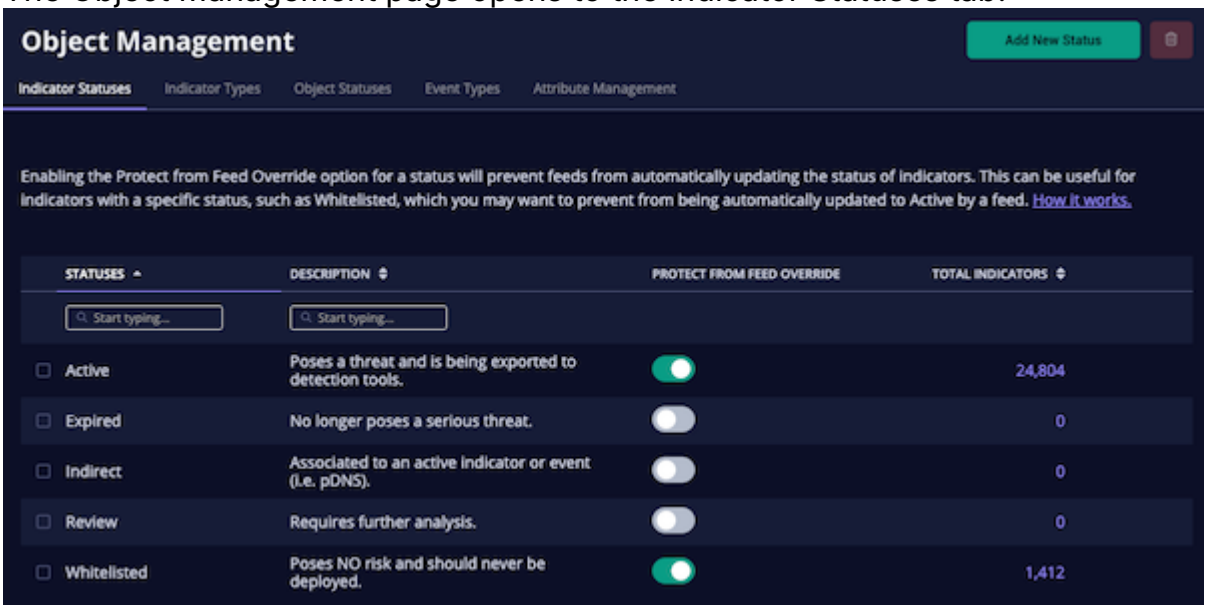
   The Object Management page opens to the Indicator Statuses tab.

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

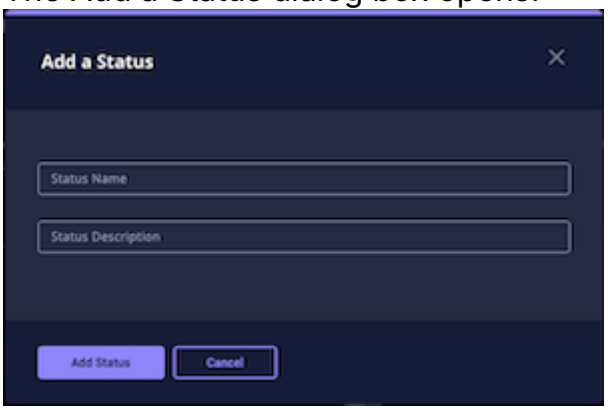
1. Navigate to Settings > Object Management.

The Object Management page opens to the Indicator Statuses tab.



2. Click **Add New Status**.

   The Add a Status dialog box opens.



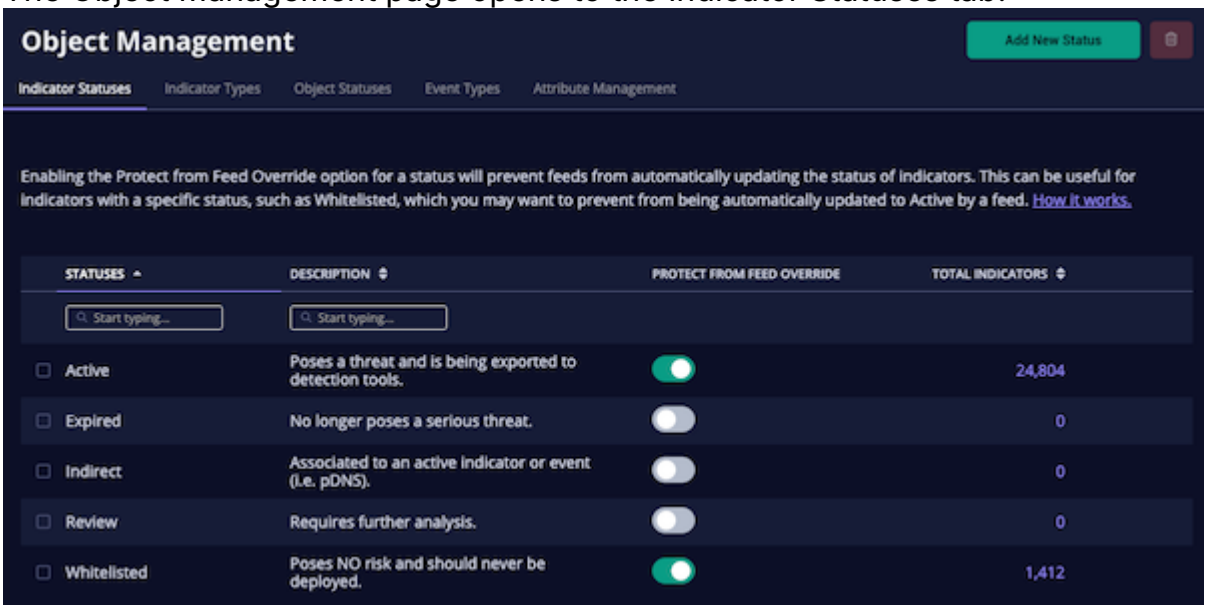
3. Enter a **Status Name**.
4. Optionally, enter a **Status Description**.
5. Click **Add Status**.

Editing an Indicator Status

You cannot edit an indicator status provided by ThreatQ.

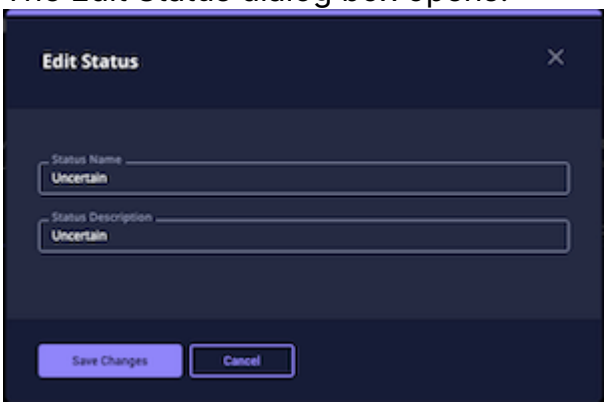
1. Navigate to Settings ⚙ > Object Management.

The Object Management page opens to the Indicator Statuses tab.



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

   The Edit Status dialog box opens.



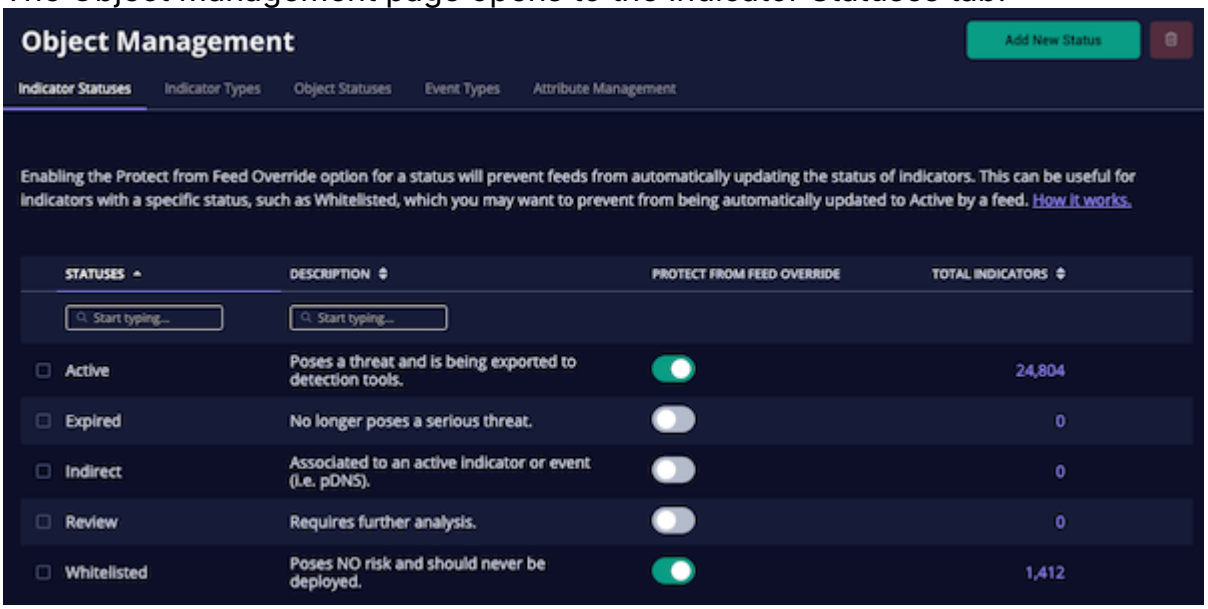
3. Optionally, enter a new **Status Name**.
4. Optionally, enter a new **Status Description**.
5. Click **Save Changes**.

Deleting an Indicator Status

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

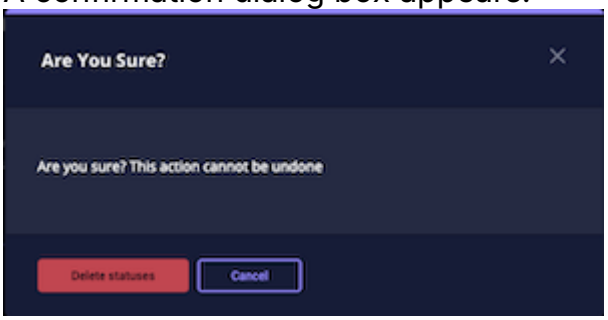
1. Navigate to Settings ⚙ > Object Management.

The Object Management page opens to the Indicator Statuses tab.



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

   A confirmation dialog box appears.



4. Click **Delete Statuses**.

Indicator Types

THREATQ REQUIRED PERMISSIONS

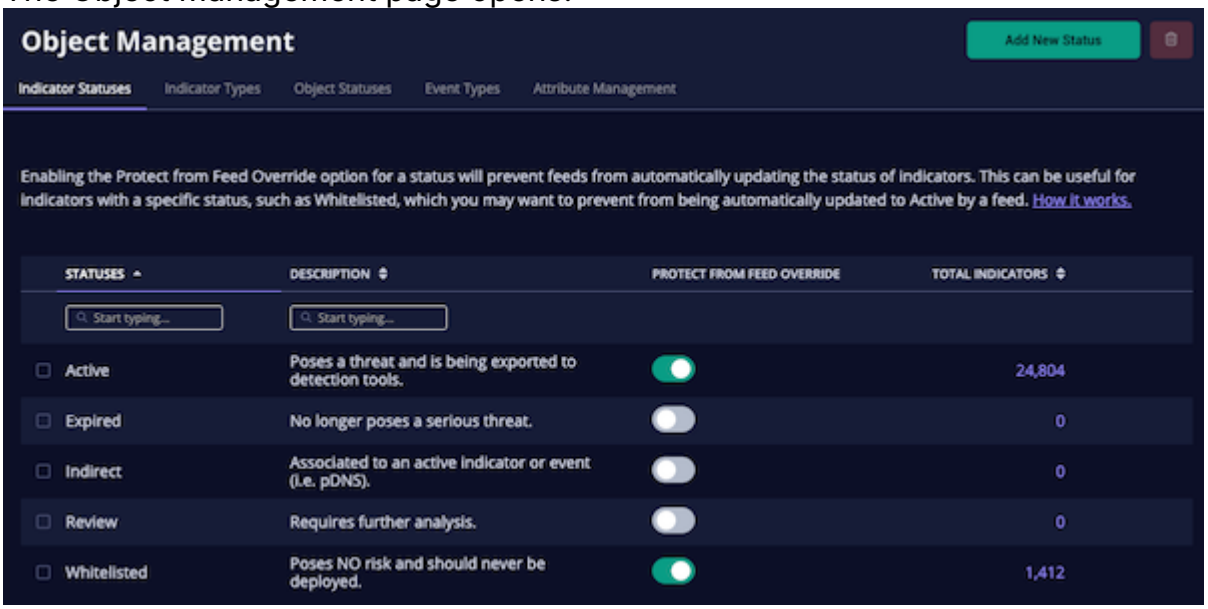
Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role - Action Permissions: Objects & Context - Manage Object Sub-types

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:

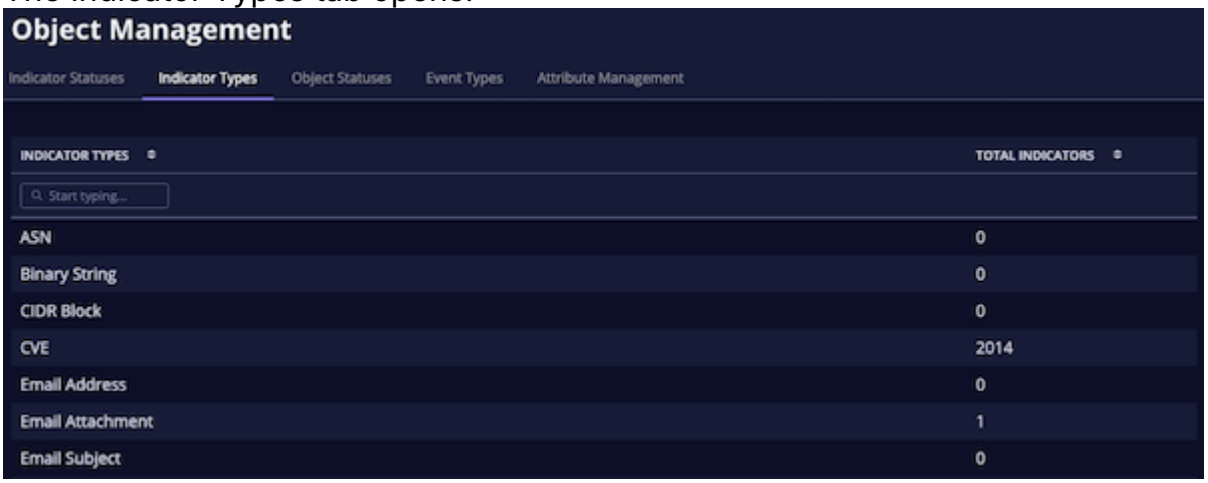
1. Navigate to Settings > Object Management.

   The Object Management page opens.



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

The Indicator Types tab opens.



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.

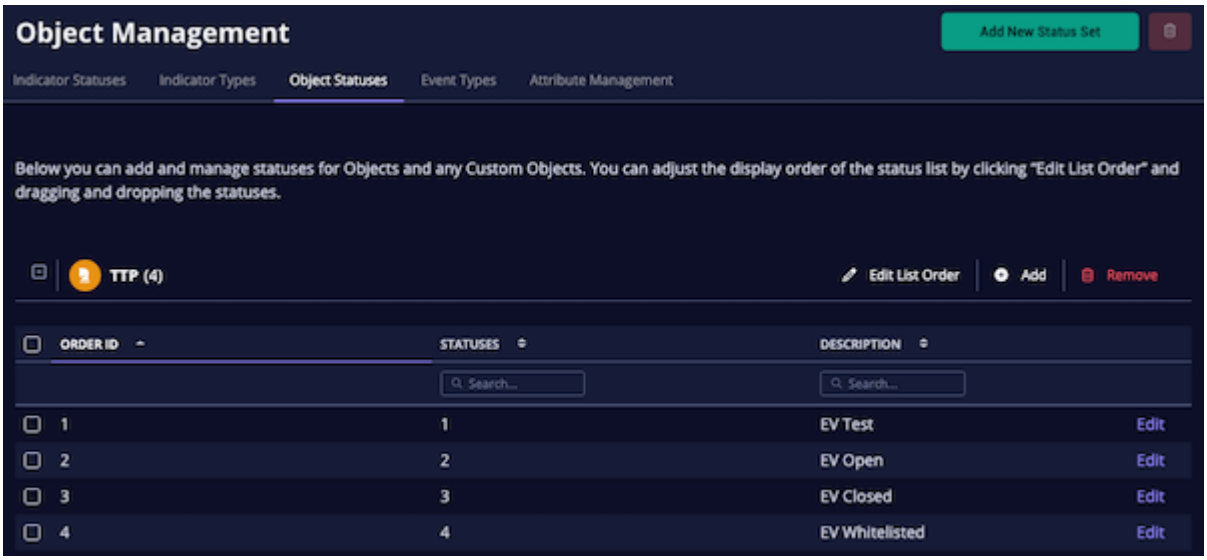
Object Statuses

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role - Action Permissions: Objects & Context - Manage Object Statuses

The Object Statuses tab allows you to create and maintain statuses for custom objects and all seeded system objects except for Adversaries, Files, Signatures, and Tasks objects.

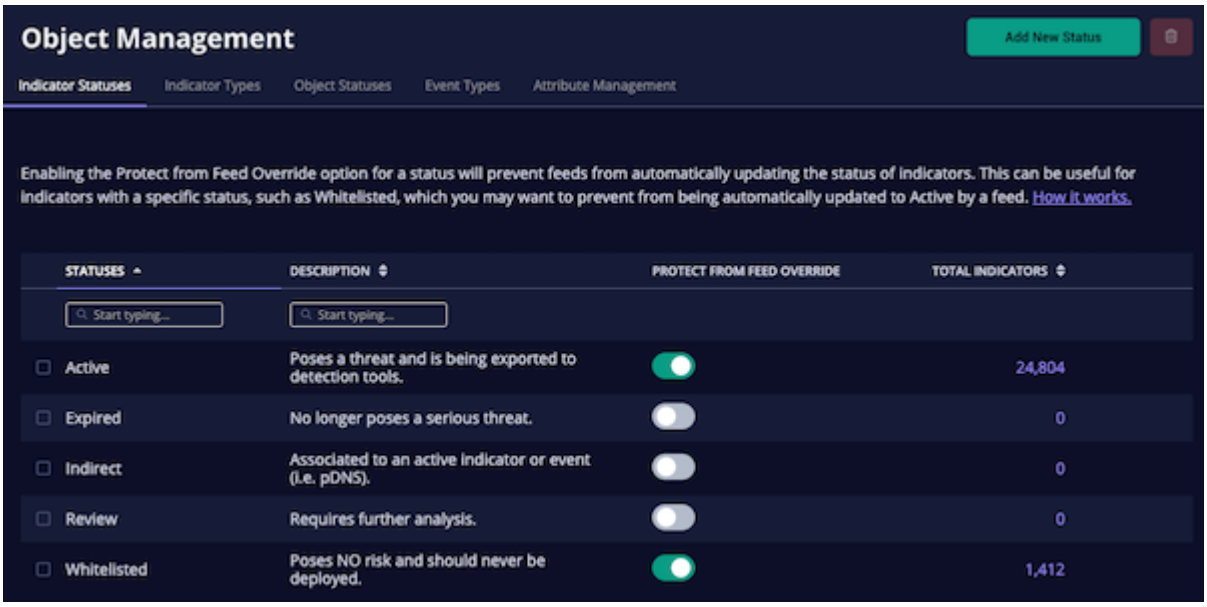
The display of the status field in an object's add modal, object details page, and preview panel is triggered by the creation of at least one status for the object type.



Viewing Object Statuses

1. Navigate to Settings > Object Management.

The Object Management page opens.



2. Click the **Object Statuses** tab.

   The Object Statuses tab opens.

The Object Statuses tab contains a section for each object type. Within each section, you can use the following functions to locate a status:

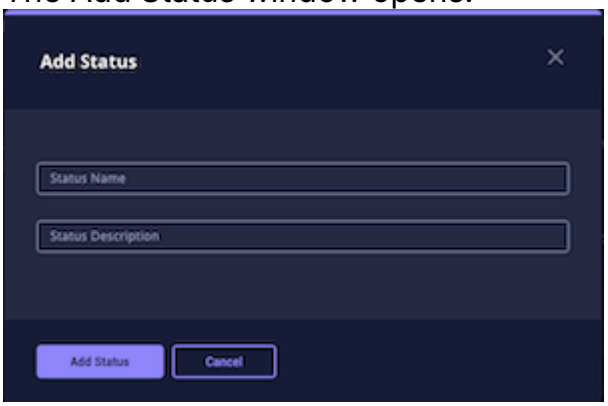
FUNCTION	DESCRIPTION
Filter table by Object Status	Enter a keyword in the Statuses search field to filter by status.
Filter list by Description	Enter a keyword in the Description search field to filter by status description.
Sort table by Order ID, Status name, or Description	Click the arrow to the left of a column to sort the status list by that column. For instance, click the arrow next to the Statuses column to sort the list of statuses alphabetically (ascending/descending) by status name.

Adding an Object Status

The Object Statuses tab gives you the option to add a single status at a time or to add multiple statuses at a time.

To add a single status for an object type:

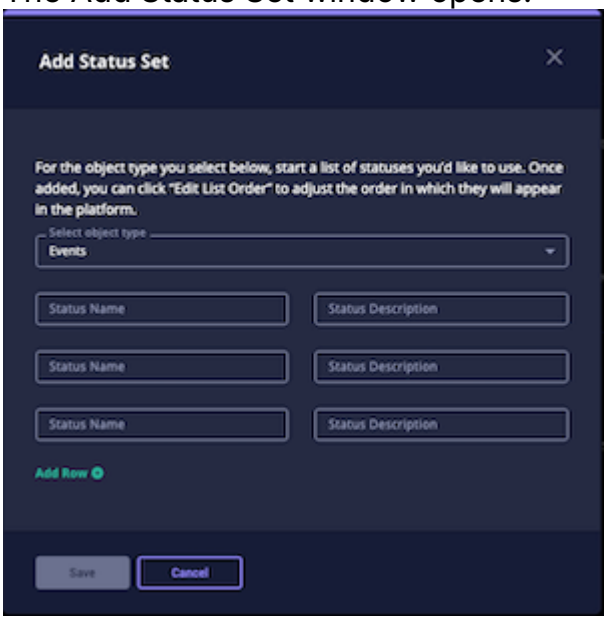
1. In the **Object Statuses** tab, locate the object type to which you want to add a status.
2. Click the Add option located above the object type section.
   The Add Status window opens.



3. Enter the status name and description (optional).
4. Click the **Add Status** button.

To add multiple statuses for an object type:

1. From **Object Statuses** tab, click the **Add New Status Set** button.
   The Add Status Set window opens.



4. Select the object type for which you want to add statuses.
5. Enter the name and description (optional) for each status.
6. To enter more than three statues, click the Add Row option to display additional fields.
5. Click the **Save** button.

Editing an Object Status

1. From the **Object Statuses** tab, click the **Edit** option next to the status you want to update.
2. The Edit Status window opens.
3. Enter your changes.
4. Click the **Save** button.

Editing Object Status Order

Status order controls the order in which statuses are displayed in drop down fields such as the Status field on the object details page. The **Edit List Order** option allows you to modify this order.

1. In the Object Statuses tab, locate the object type status you want to update.
2. Click the **Edit List Order** option for the object type.

3. From the Edit List Order window, drag and drop status names to change the order in which they are displayed in ThreatQ.
4. Click the **Save** button.

Deleting an Object Status

> You cannot delete a status that is currently assigned to an object. You must remove the status from all objects before you can delete it.

The Object Statuses tab allows you to delete a single status as well as multiple statuses associated with the same object type, or multiple statuses associated with different object types.

1. In the **Object Statuses** tab, check the box next to the status you want to delete.
2. If you are deleting a single status or a group of statuses associated with the same object type, you can click the Remove option above the object type section or you can click the Delete icon in the upper right corner.
   If you are deleting statuses for more than one object type, click the Delete icon in the upper right corner.
   A confirmation window prompts you to confirm the deletion.
3. Click the **Delete statuses** button.

Event Types

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role - Action Permissions: Objects & Context - Manage Object Sub-types

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

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

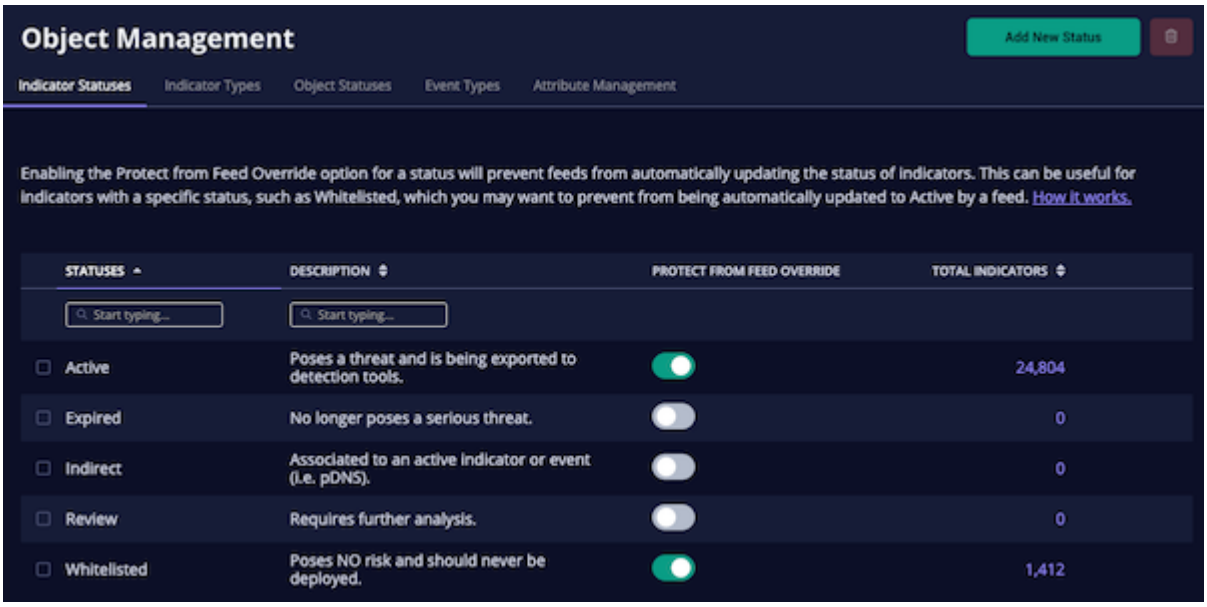
System provided Event Types include:

- Anonymization
- Command and Control
- Compromised PKI Certificate
- DoS Attack
- Exfiltration
- Host Characteristics
- Incidents
- 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.



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

   The Event Types tab opens.

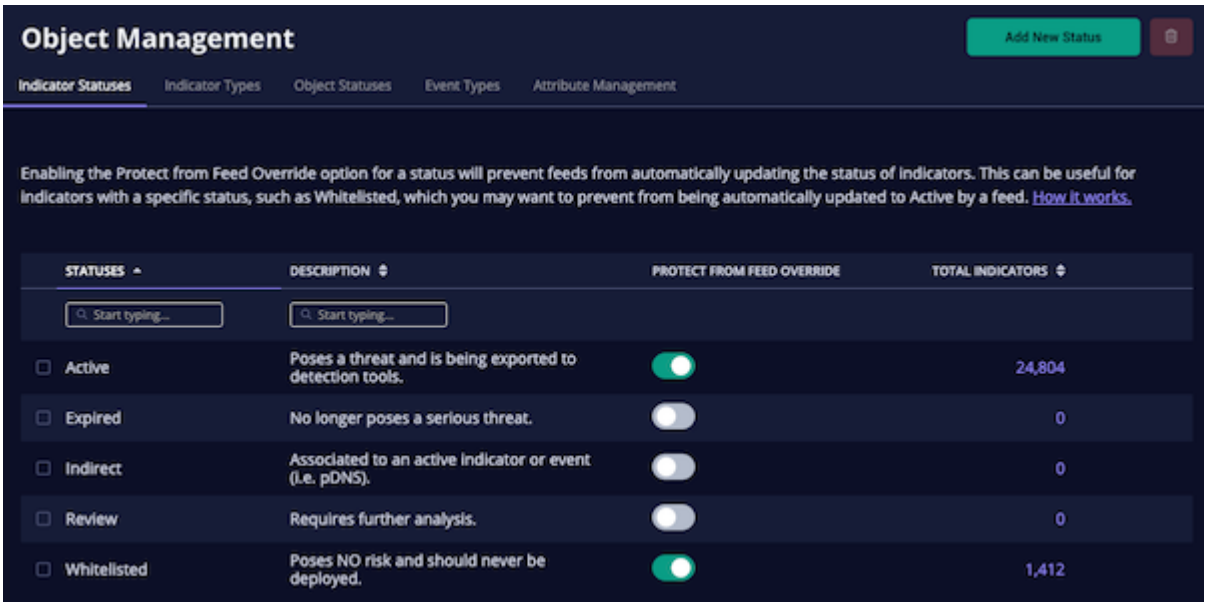
Event Types Table Functions:

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

Adding an Event Type

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

The Object Management page opens to the Indicator Statuses tab.

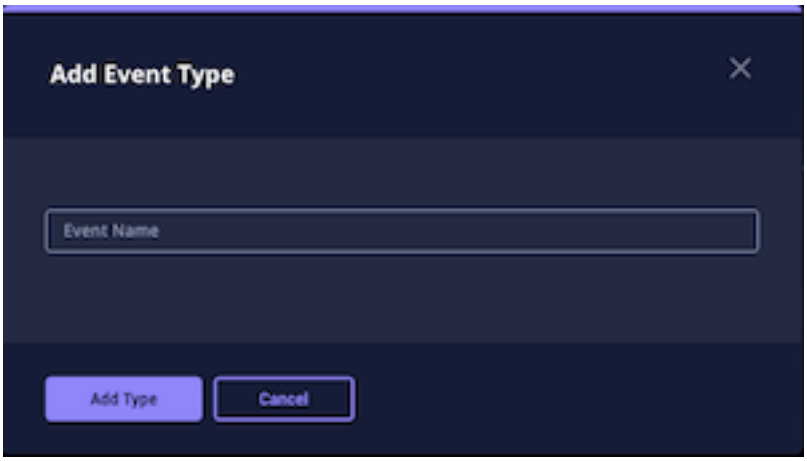


2. Click the **Event Types** tab.

   The Event Types tab opens.

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

The Add Event Type dialog box opens.



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

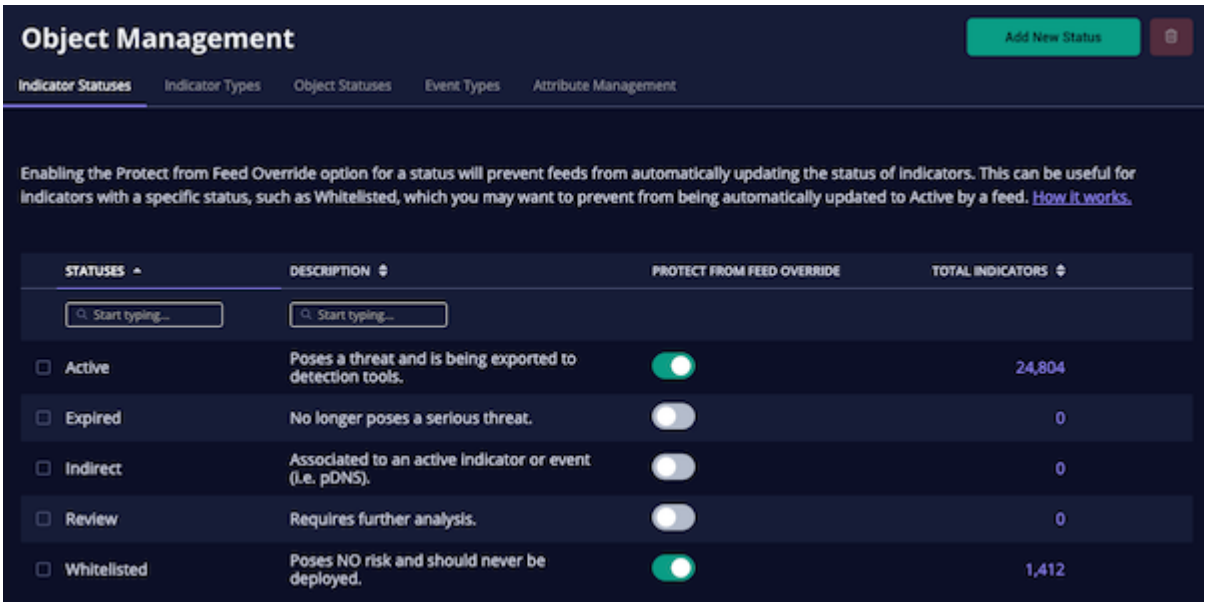
Editing an Event Type

You can edit user-generated event types.

You cannot edit an Event Type provided by ThreatQ.

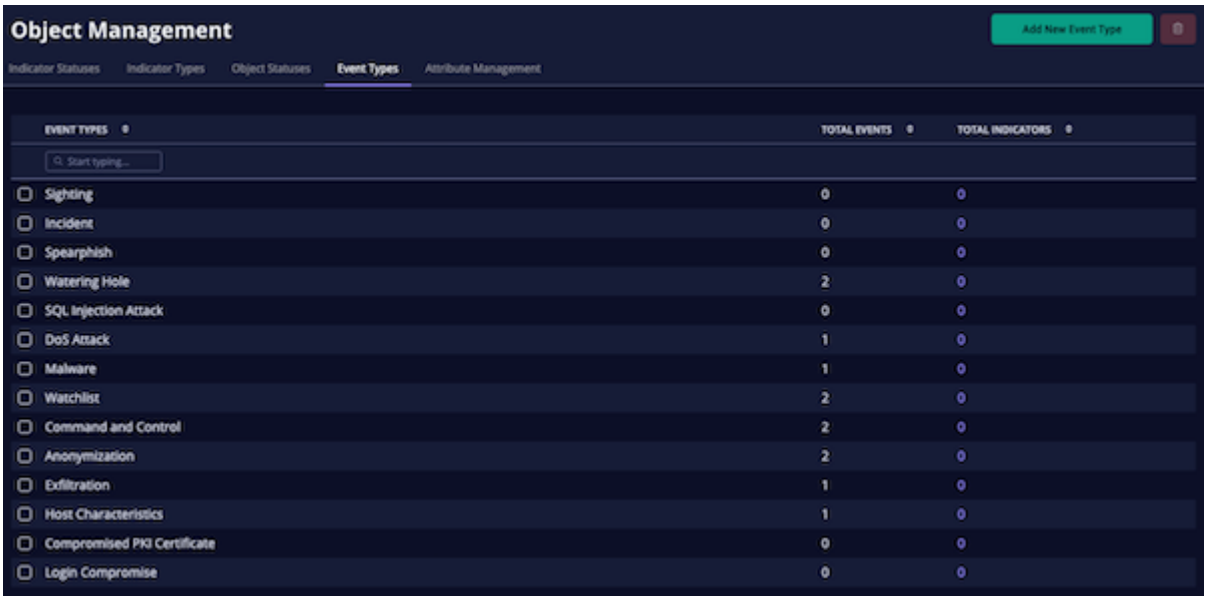
1. Navigate to Settings > Object Management.

   The Object Management page opens to the Indicator Statuses tab.



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

The Event Types tab opens.



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

   The Edit Event Type dialog box opens.

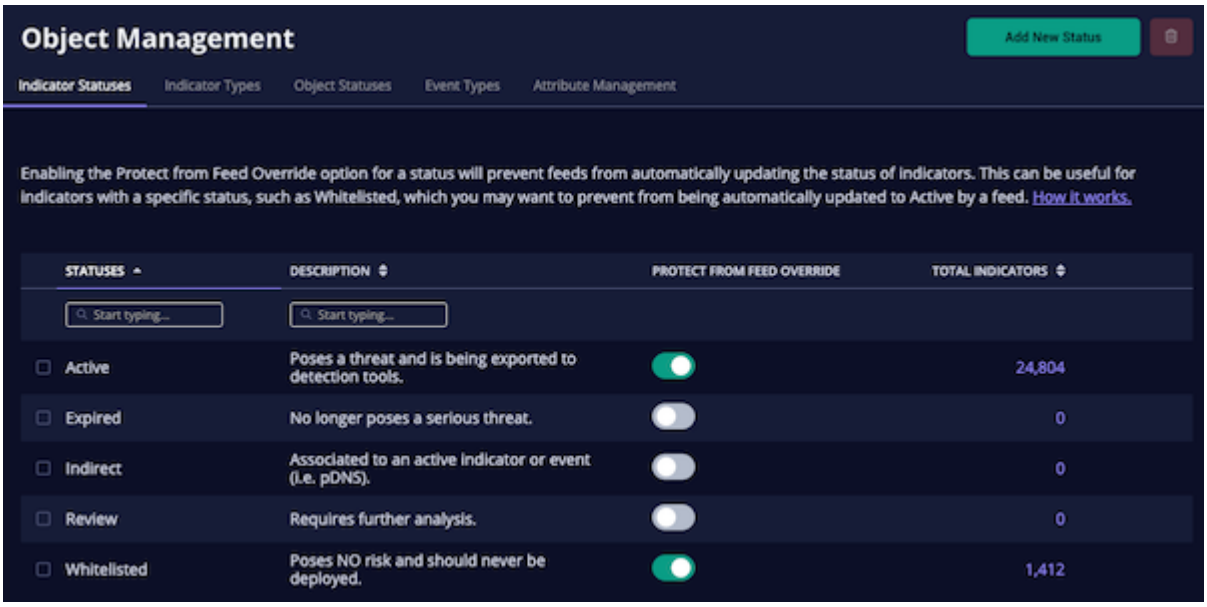
4. Enter a new **Event Name**.
5. Click **Save Changes**.

Deleting an Event Type

> 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.



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

   The Event Types tab opens.

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

   A confirmation dialog box appears.

5. Click **Delete Types**.

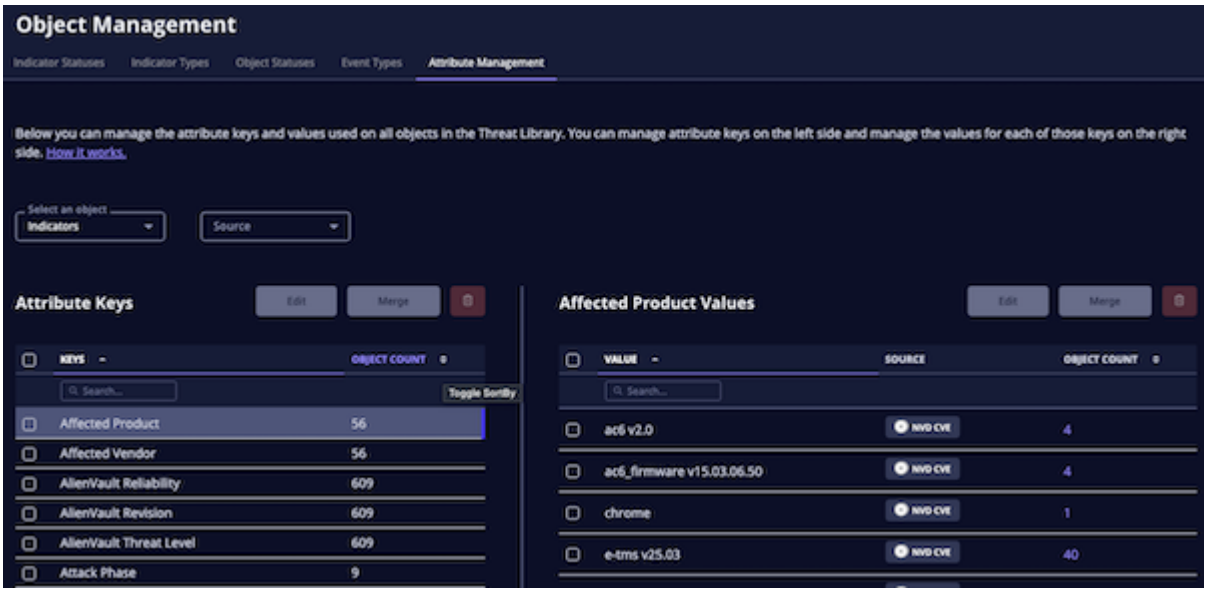
Attribute Management

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative or Maintenance
Custom Role - Action Permissions: Objects & Context - Manage System Attributes

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.



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.

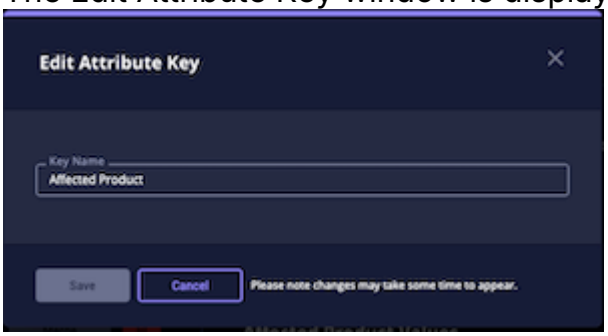
- Browse the list of attribute values and click the attribute key.
- Begin typing the attribute value in the Search box and click it when it is displayed below the field.

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.

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

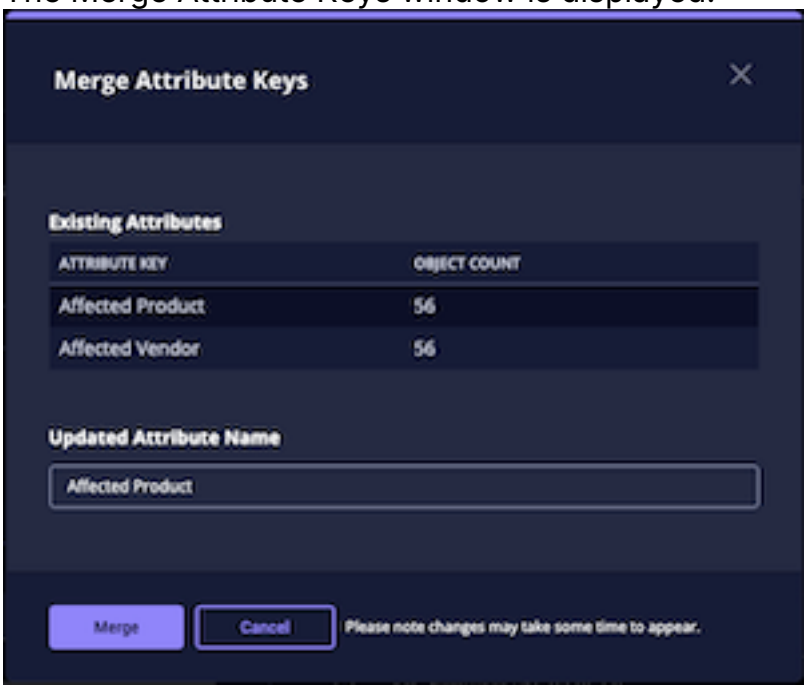


3. Enter your changes to the attribute key.
4. Click the Save button.

Merging Attribute Keys

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

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



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

Deleting Attribute Keys

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

Editing Attribute Values

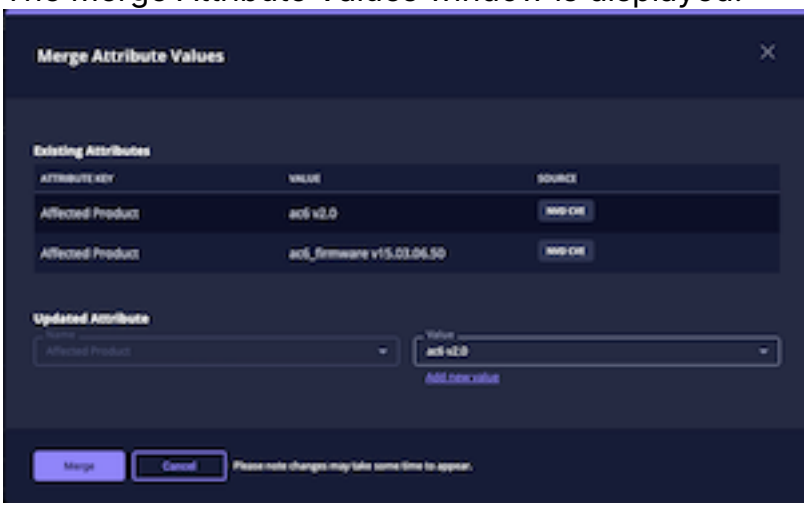
1. From the attribute values list, click the checkbox next to the attribute value you want to edit.

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

2. Click the Edit button.
   The Edit Attribute Value window is displayed.
3. Enter your changes to the attribute value.
4. Click the Save button.

Merging Attribute Values

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



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.
4. Click the Delete button.

Relationships

Relationship Limits

> Please contact ThreatQuotient Support, if you have questions or concerns about the impact of relationship limits on your ThreatQ instance.

ThreatQ provides a relationship limit system to assist you in managing the object relationship volume that ThreatQ ingests.

For a smaller subset of ThreatQ objects, some feed providers may include a very large number of relationships in their feeds. In some cases, these large relationship counts may have performance impacts on Threat Library queries and other ThreatQ capabilities. This feature allows you to balance the impact of excluding data that may be of limited intelligence value with the benefits of improved system performance.

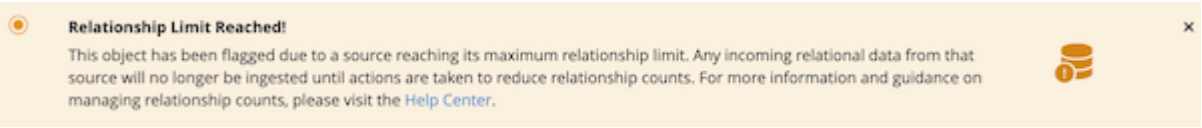
Functionally, relationship limits prevent a source from adding more than a configured number of relationships to an object via an integration, bulk update, manual at the object level, import, or parser. The default limit setting is 10,000 relationships, and generally applies to a small percentage of the overall objects in most ThreatQ systems.

Example: Exceeding the Relationship Limit

If you ingest the UNC5174 adversary object from Malpedia and the feed data for this object includes 10,001 related objects, the source (Malpedia) has exceeded the 10,000 related object limit for the system object (UNC517). As a result, ThreatQ will prevent the ingestion of any additional relationships from Malpedia for UNC5174 and flag the object and integration as follows:

> In this example, Malpedia has only exceeded the relationship limit for UNC5174. As such, ThreatQ will no longer ingest data from Malpedia for UNC5174 but will continue to ingest data for other system objects.

- The UNC5174 object details page and preview panel display a Relationship Limit Reached banner.



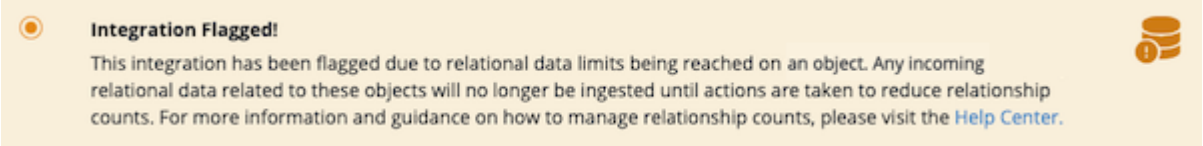
- The Sources pane in the UNC5174 object details page and object preview pane displays a relationship limit badge with a tooltip listing the source(s) that exceeded the limit. Within the tooltip, you can click the offending source(s) to

access a Threat Library view filtered by the Related To (object name) and Relationship Criteria (offending source).

> If the offending source is not a feed, the Threat Library view does not list related objects. For example, if the offending source is a user (such as threatq@threatq.com) that added the relationships, when you click it, the Threat Library view does not list any related objects.

- The new Flagged tab within the My Integrations tab displays a flagged integration banner.

- The Malapedia integration card displays a relationship limit badge .
- The Malpedia configuration page displays an Integration Flagged banner as well as a relationship limit badge above the integration logo.



> Any banner that displays an X in the upper right corner can be closed so that it does not display for the user in the current or future sessions. In addition, the above banners and badges are automatically removed when you resolve the relationship limit issue.

You can use the Flagged Objects filter in the Threat Library to review a list of objects that have exceeded the relationship limit.

What to Do When an Object Exceeds the Relationship Limit

Once an object and source have been flagged as reaching the relationship limit, ThreatQ prevents the ingestion/addition of additional related objects on that object from the feed. You can use the following methods to reduce the number of object relationships:

- **Object details page or object preview pane** - From the object details page/object preview panel, use the Unlink option to unlink related objects from the offending source.
- **Bulk action** - Filter your Threat Library view using the Flagged Objects filter. Then, click the Bulk Actions button and select the Bulk Delete option to delete the objects.
- **Data retention policy** - Use the Flagged Objects filter to create a data collection you can add to your data retention policy.

Once the relationship limit is no longer exceeded, the offending objects and feed no longer display relationship limit banners or badges.

Tips and Tricks

- Relationship limits are applied based on object and source. For example, an object can have 10,000 related objects from Malpedia and 10,000 related objects from NVD. Although the total number of related objects exceeds 10,000, the total per source does not so the object/source is not flagged as exceeding the relationship limit.
- If a source exceeds the relationship limit for one object, ThreatQ halts the ingestion of data for that specific object but continues to ingest data from this source for other objects.
- Since object relationships from the same source can be added by multiple processes, you may encounter situations in which an object's relationship count exceeds 10,000.
  For example, if your instance ingests 9,999 object relationships from a feed in the first run and then it ingests an equal number of additional relationships in the second run, ThreatQ may allow the object relationships to exceed 10,000 due to a slight delay in incrementing the relationship count. However, once the relationship count is updated, the object and source are flagged and you can no longer add relationships to the flagged object from the flagged source.

Reports

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

> Regardless of the alignment you select in the Descriptions pane, images in an object's description PDF report are displayed as left aligned.

Tips and Tricks

- If your object has multiple descriptions, you can select all descriptions by checking the Descriptions checkbox or select specific descriptions by checking the checkbox next to the corresponding description source(s). If the object does not have a description, the Descriptions section is not displayed.
- The Generate PDF modal only displays sections that have contents. For instance, if an object does not have any comments, the Comments section is not displayed.
- When you generate a PDF that includes only the system object's description(s), the Description section header text is omitted as is the last modified date and divider line. If the PDF export includes only a single description, the description source is also omitted.

Generating Reports

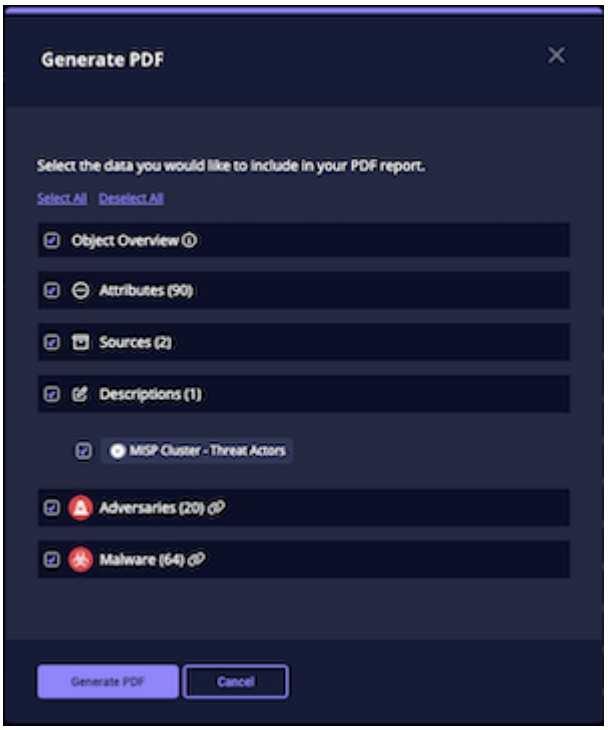
THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative or Maintenance
Custom Role - Action Permissions: Objects & Context - Individual Object Context & Actions - Generate PDF

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

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative or Maintenance
Custom Role - Action Permissions: Administrative Functions - Edit 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.

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

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.

Default 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.

Custom User Roles

Action permissions defined in a custom user role influence sharing permission options for dashboards, data collections, and investigations:

- If your custom role specifies view-only access to dashboards, you can only be added to a dashboard as a viewer.

- If your custom role specifies view-only access to data collections, you can only be added to a data collection as a viewer.
- If your custom role specifies view-only access to investigations, you can only be added to a data investigation as a viewer.

In addition, the Sharing modal lists a view-only icon next to your name and only includes your name in searches with the Viewer filter enabled.

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.

View-only sharing permissions for all users take precedence over action permissions defined in a custom user role. For example, even if your custom user role gives you Create, Edit, Delete permissions for data collections, you cannot edit or delete a data collection with a permission level of **Everybody (Public).**

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.

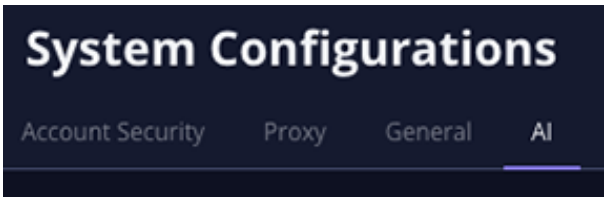
System Configuration

About System Configuration

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative or Maintenance
Custom Role - Action Permissions: Administrative Functions - Edit System Configurations

The System Configurations page consists of the Proxy, Account Security, General Settings, and AI tabs. These tabs allow you to enable, disable, and update multiple system-level settings. When you access the System Configurations page, the Account Security tab is displayed by default.



TAB	DESCRIPTION
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.
AI	Enable, disable, and configure the Threat Research Agent for use on the platform.

TQAdmin Configuration Options

The TQAdmin `configure` parameter allows you to customize your ThreatQ instance during the initial install as well as update these options after the initial install. You can use the configure parameter to specify which ThreatQ Data Exchange modules you use, OpenDXL and/or TAXII, as well as adding SSL certificate or enabling SSL Client Certificate Authentication.

Account Security Tab

Setting Account Lockout

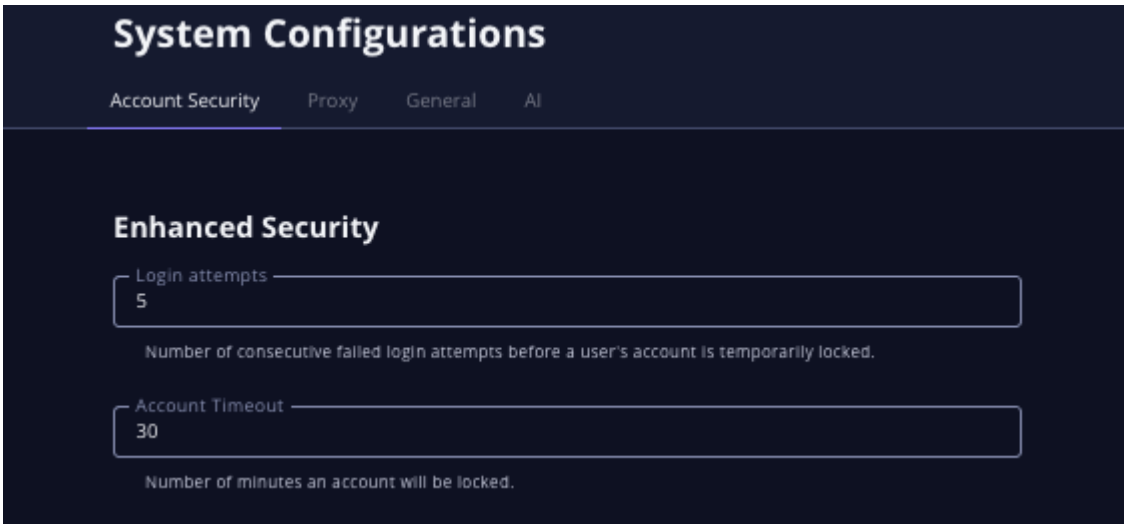
THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative or Maintenance
Custom Role - Action Permissions: Administrative Functions - Edit System Configurations

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.



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

THREATQ REQUIRED PERMISSIONS

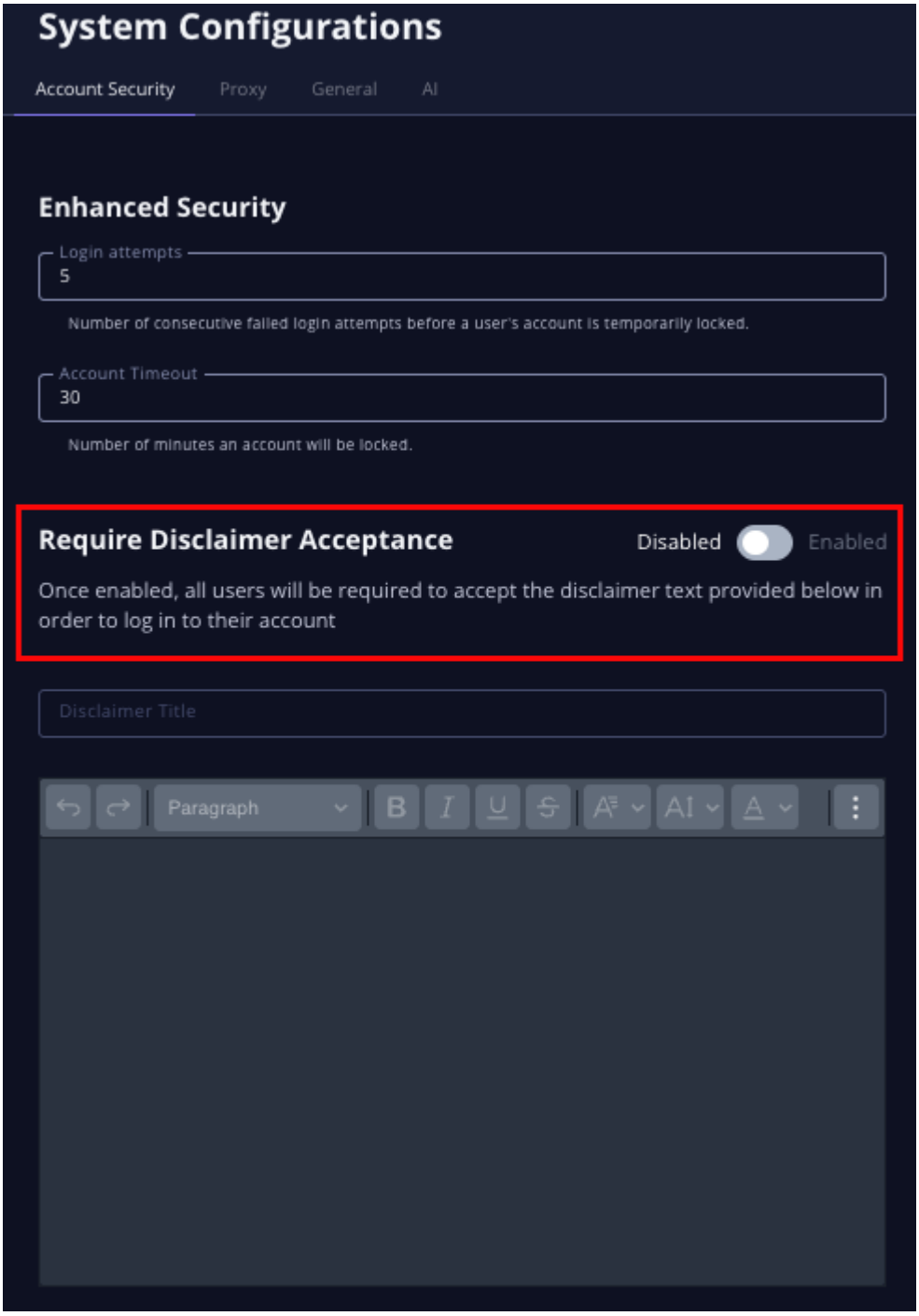
Default ThreatQ Role: Administrative or Maintenance
Custom Role - Action Permissions: Administrative Functions - Edit System Configurations

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.



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.

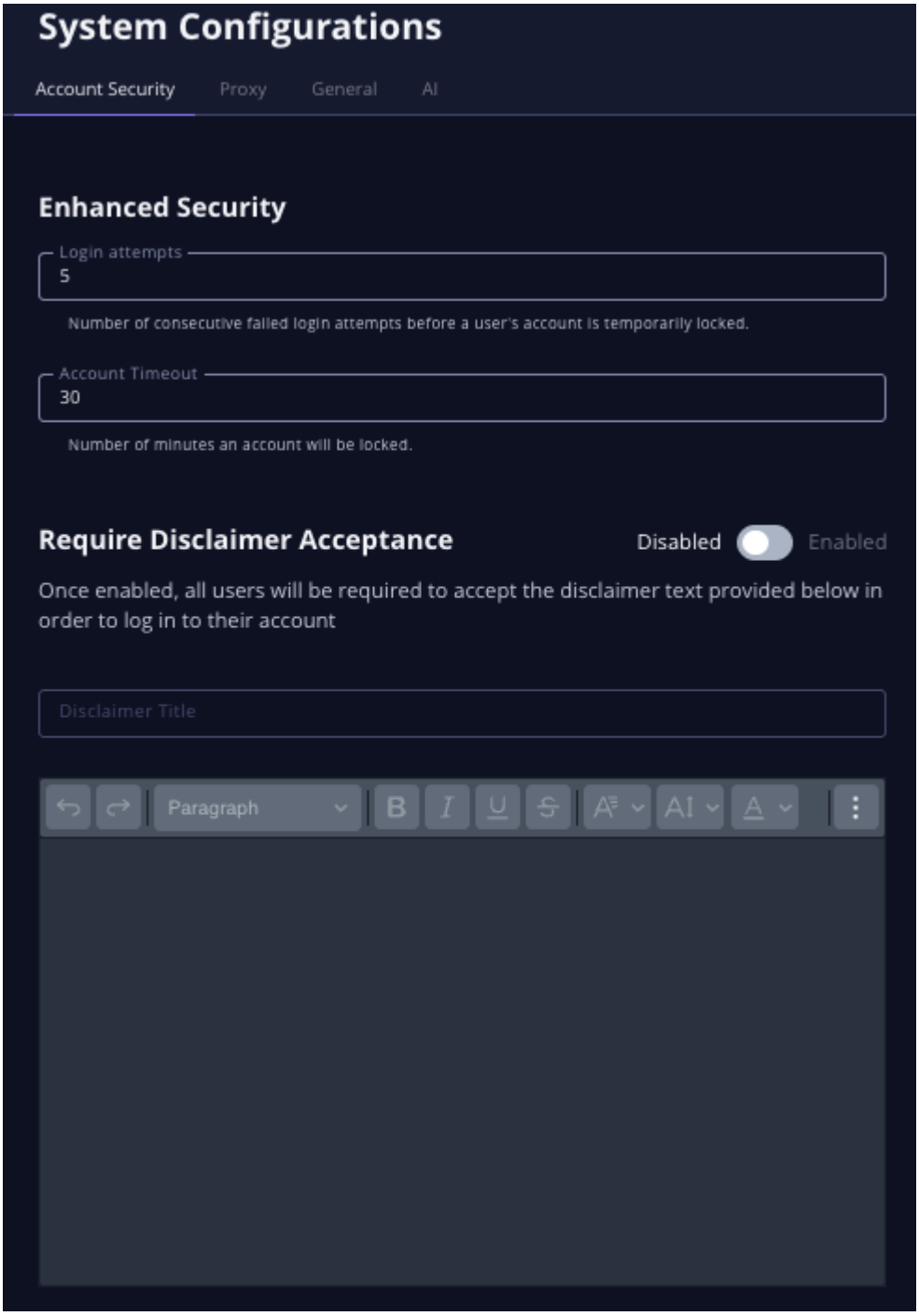
- If a user is logged out and enters a URL for a specific page in the platform, the custom banner is displayed and he must click the **Accept and Continue** button to access the specified page.

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.



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

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative or Maintenance
Custom Role - Action Permissions: Administrative Functions - Edit System Configurations

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.

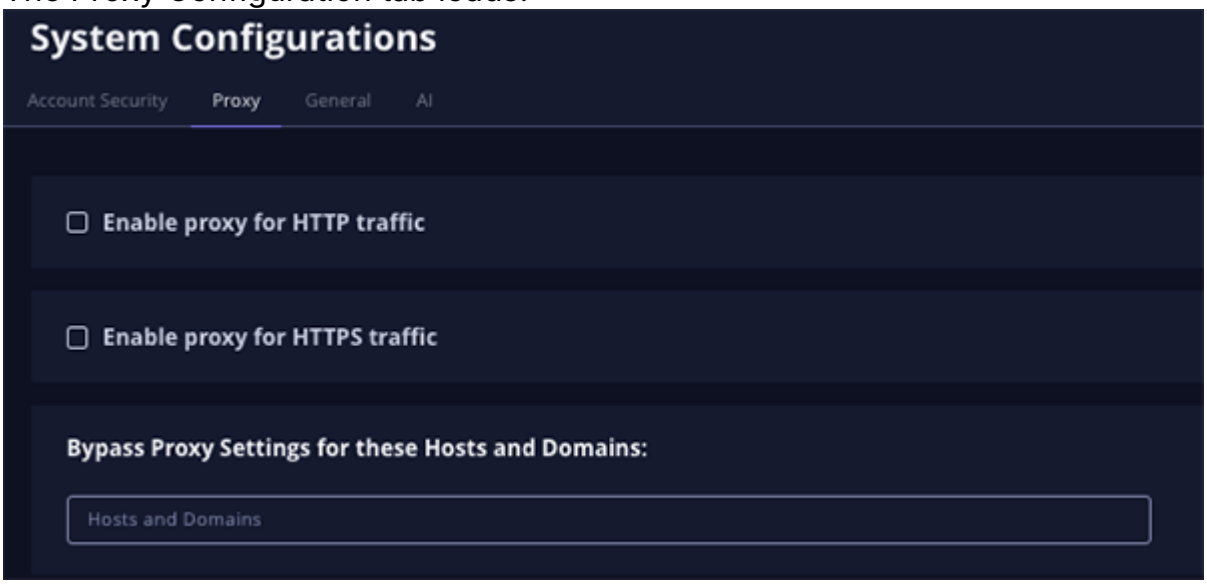
Accessing Proxy Configuration

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

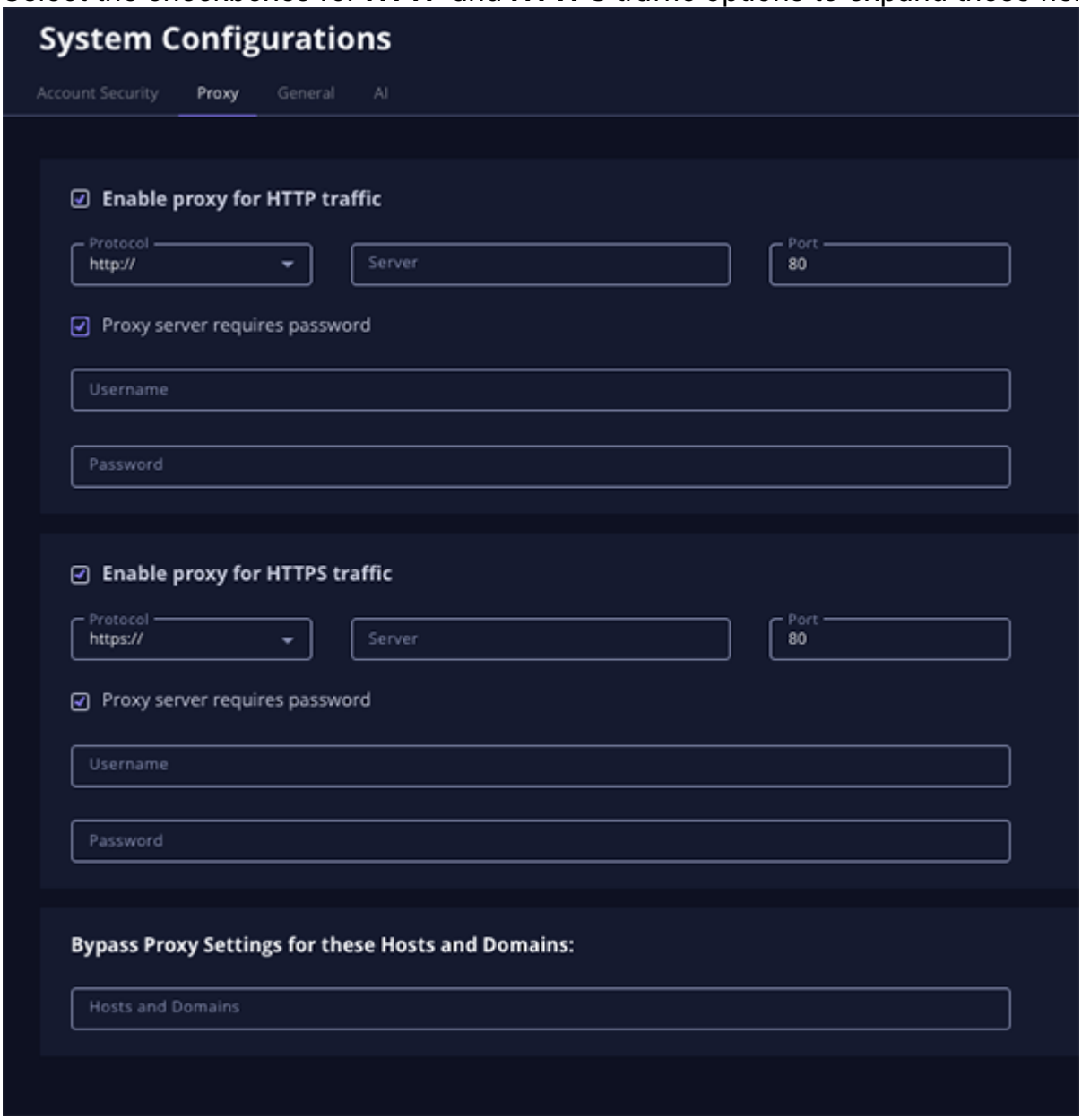
   The System Configurations page opens to the Account Security tab selected by default.

2. Click the **Proxy** tab.

   The Proxy Configuration tab loads.



3. Select the checkboxes for **HTTP** and **HTTPS** traffic options to expand those fields.



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 the **Save** button. ThreatQ saves the proxy information you added as a Kubernetes secret.

No_Proxy Setting

ThreatQ uses the values you add to the Bypass Proxy Setting for these Hosts and Domains field to bypass the proxy for operations, CDFs, and ThreatQ TDR Orchestrator in addition to custom connectors.

> If using IP Addresses values in the No_Proxy field, users are required to use the same IP Address format, and not their hostname, when configuring proxy bypass settings for their ThreatQ feeds. Example: entering 10.0.0.1 in the No_Proxy field and then using my-domain-local in your individual integration's proxy parameters will not result in the feed bypassing the proxy.

> Integration-level proxy configurations take priority over the ThreatQ system-level 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.

3. Add any no_proxy settings to the **Bypass Proxy Settings for these Hosts and Domains** field in the following format:
   <address or hostname of server for the setting>

   > If adding multiple no_proxy settings, use a comma-separated format.

4. Click the Save button.

General Tab

Configuring Time and Date Settings

THREATQ REQUIRED PERMISSIONS

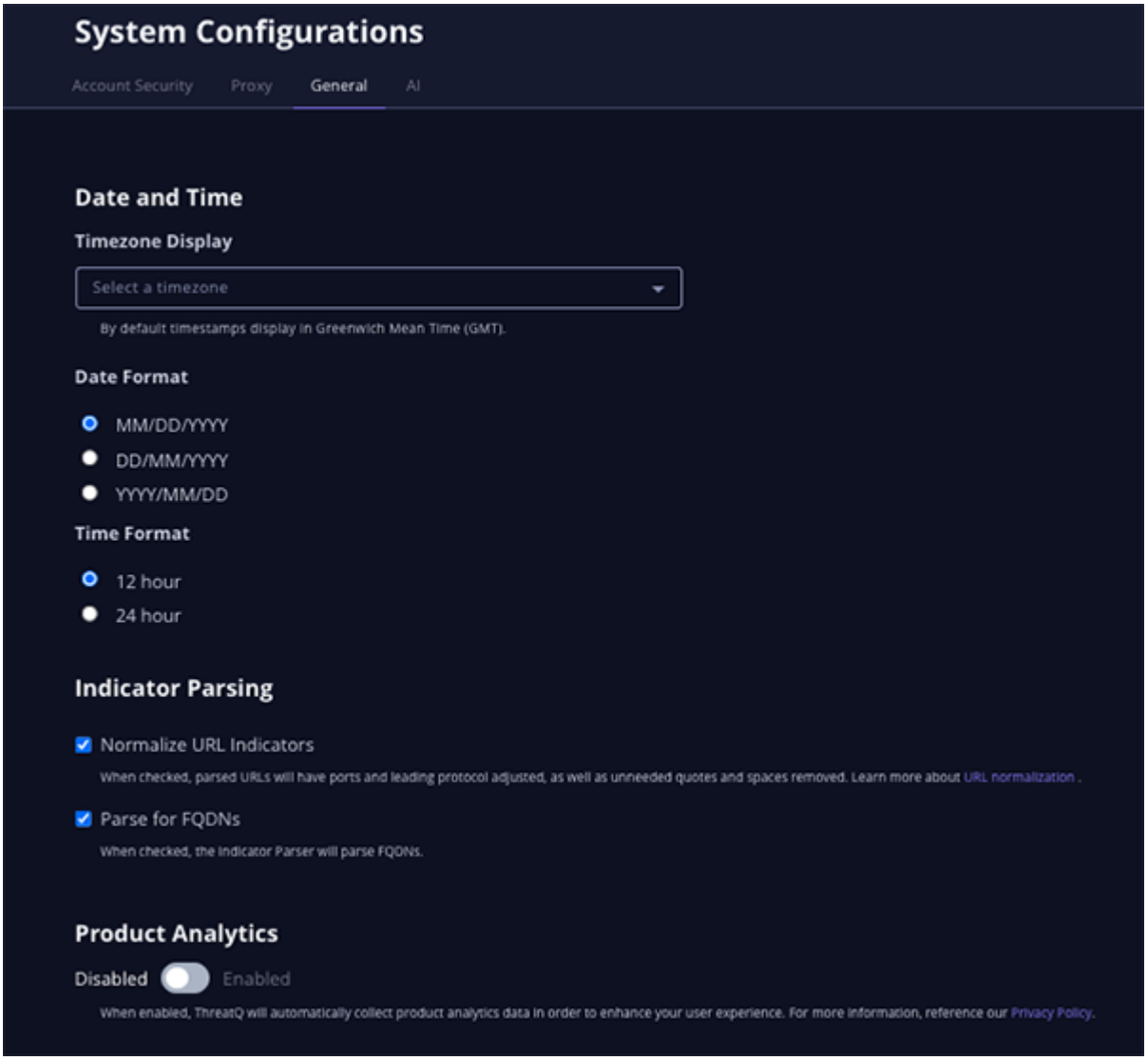
Default ThreatQ Role: Administrative or Maintenance
Custom Role - Action Permissions: Administrative Functions - Edit System Configurations

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.

Tips and Tricks

- The Suggested option in the Timezone Display field is based on your browser timezone.
- The Timezone Display field allows you to scroll through a list of timezones in alphabetical order by continent/region and city or search for a timezone by city, region or timezone abbreviation or name.
- After you select a timezone, the Reset option allows you to reset your timezone display to Greenwich Mean Time (GMT).

1. Click the Settings icon and select the System Configurations option.
2. Click the **General** tab.



3. Click the Timezone display field to select the default timezone used to display times in ThreatQ. Users can select a different timezone to display in their ThreatQ sessions. See the Managing User Accounts section for more details.

> The system timezone setting only affects the display of timestamps in the user interface and PDFs. ThreatQ continues to store timestamps in UTC and share UTC timestamps with resources such as ThreatQ Data Exchange (TQX), ThreatQ TDR Orchestrator (TQO), exports, and TAXII.

4. Select the desired **Date Format**. Options include: MM/DD/YYYY, DD/MM/YYYY, YYYY/MM/DD
5. Select the desired **Time Format**. Options include: 12 hour, 24 hours.
6. Click the **Save** button.

Configuring Indicator Parsing Presets

THREATQ REQUIRED PERMISSIONS

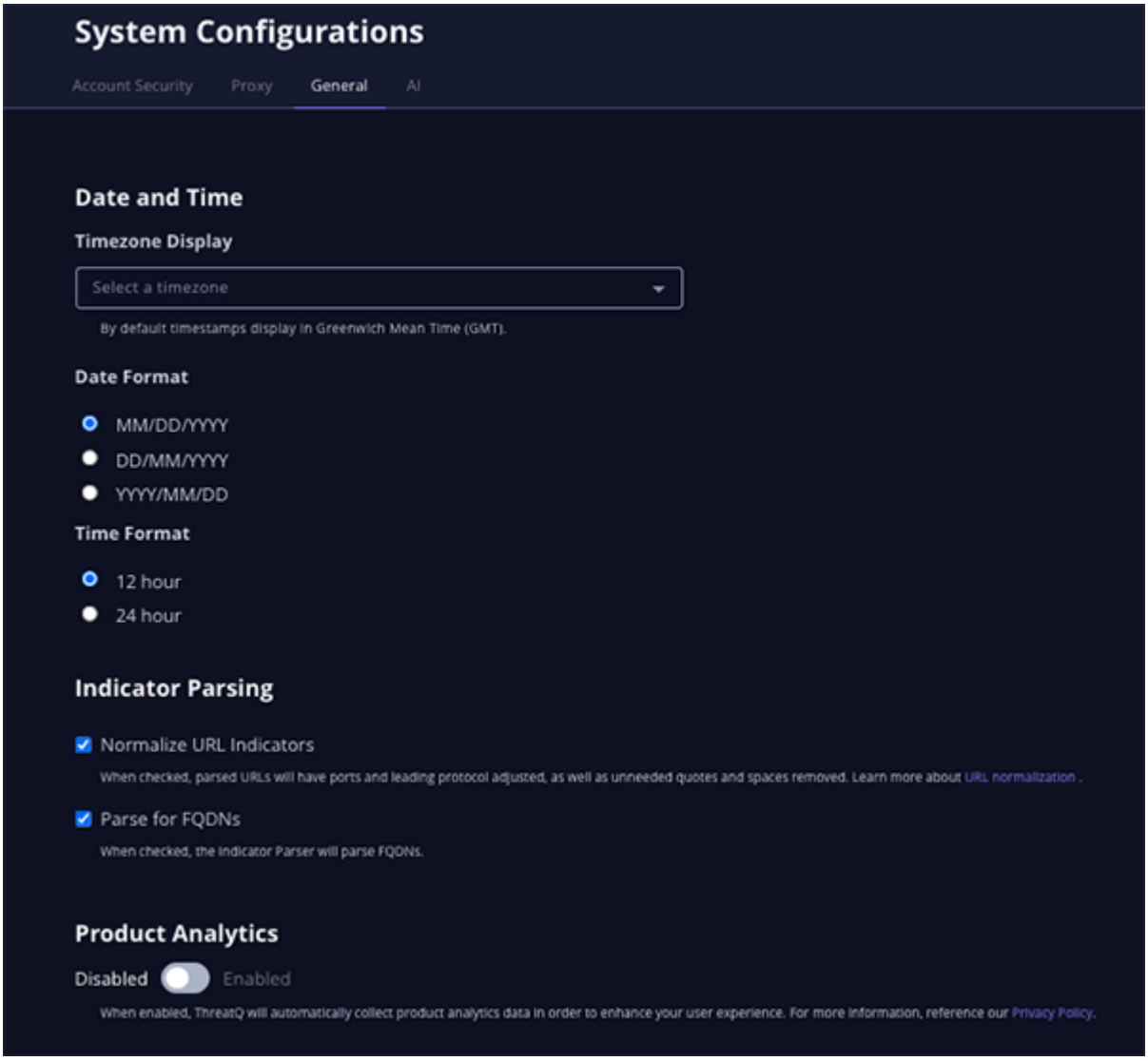
Default ThreatQ Role: Administrative or Maintenance
Custom Role - Action Permissions: Administrative Functions - Edit System Configurations

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.



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:

OPTION	DESCRIPTION
	◦ 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.

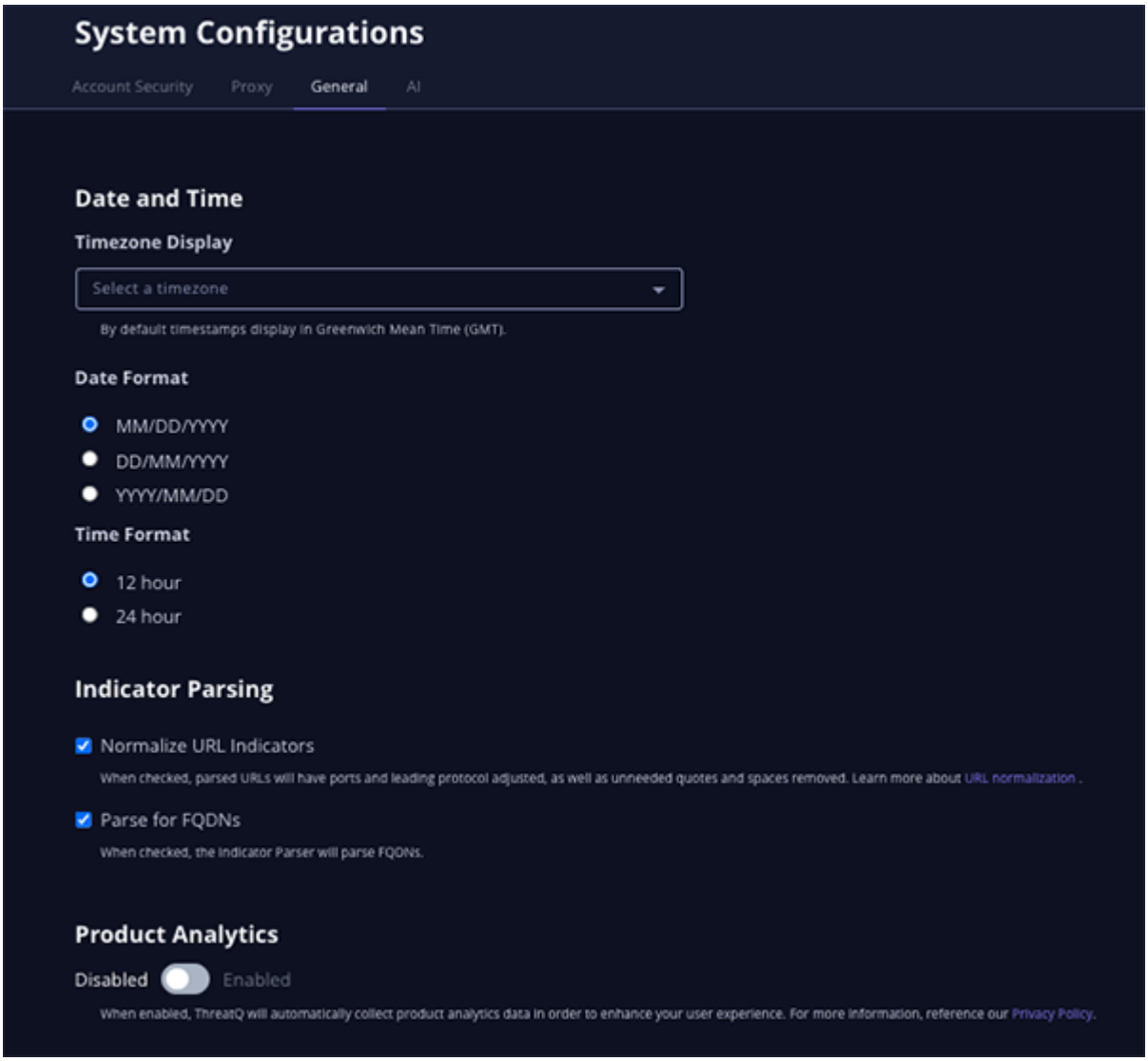
Opt In/Out of Product Analytics

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative or Maintenance
Custom Role - Action Permissions: Administrative Functions - Edit System Configurations

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.



3. In the Product Analytics section, click the toggle button to change the setting from Disabled to Enabled or vice versa.

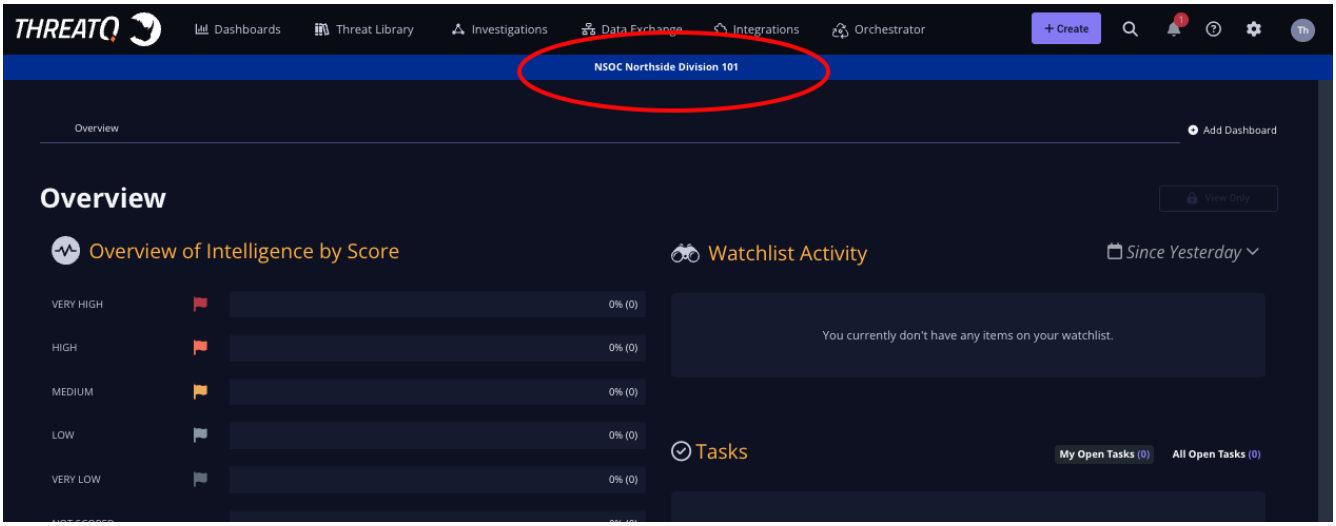
4. Click the **Save** button.

System Banner Display Settings

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative or Maintenance
Custom Role - Action Permissions: Administrative Functions - Edit System Configurations

The System Banner Display Settings feature enables administrators to configure customizable banner messages within the ThreatQ platform to clearly identify the classification, purpose, or operational role of a ThreatQ instance. Banner messaging can be displayed in configurable header and/or footer locations, providing users with immediate visual awareness of the environment they are currently accessing.

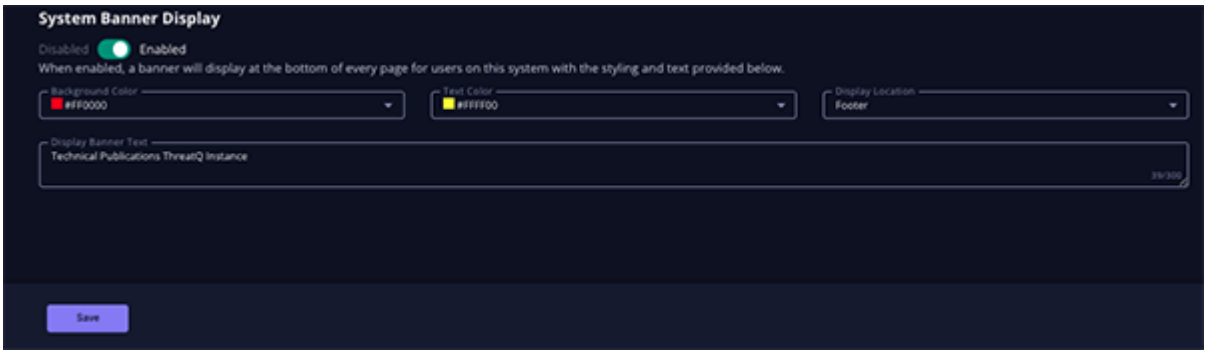


This feature is especially valuable for organizations managing multiple ThreatQ environments, such as development, testing, staging, or production systems, helping reduce user confusion and supporting safer operational workflows across platform instances. In addition to operational awareness, the feature also supports organizational branding, compliance, and system marking requirements through flexible display customization options.

System Banner Display Settings are located under the **General** tab and support plain-text banner messages up to 300 characters in length. Banner text is center-aligned by default. Administrators can customize the banner using four background color options, three text font color options, and two display location settings.

1. Navigate to **Settings** > **System Configurations**.
2. Click the **General** tab.

3. Scroll down the page to the **System Banner Display** section.

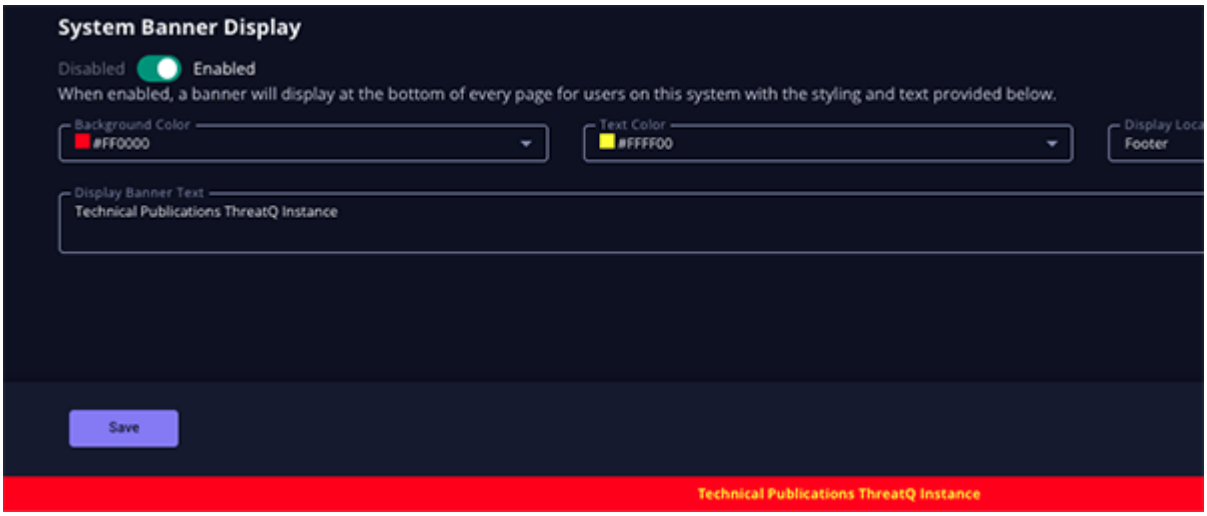


4. Select a background color from the **Background Color** dropdown provided. Hex color options include:
   - blue #0033A0
   - grey #767676
   - black #000000
   - red #FF0000
5. Select your color of your banner text from the **Text Color** dropdown provided. Hex color options include:
   - white #FFFFFF
   - black #000000
   - yellow #FFFF00
6. Select a display location for the banner from the **Display Location** dropdown. Options include:
   - header
   - footer
7. Enter your banner message in the **Display Banner Text** field. This plaintext field supports 300 characters and will default to a centered position in the banner.

   Text entered in this field will appear in a single line. Any returns and line breaks added in the text box will be ignored.

8. Click on the **Save** button to save your changes.
9. Click on the **Enable/Disable toggle switch** to enable the banner.

The banner will now be displayed for all platform users.



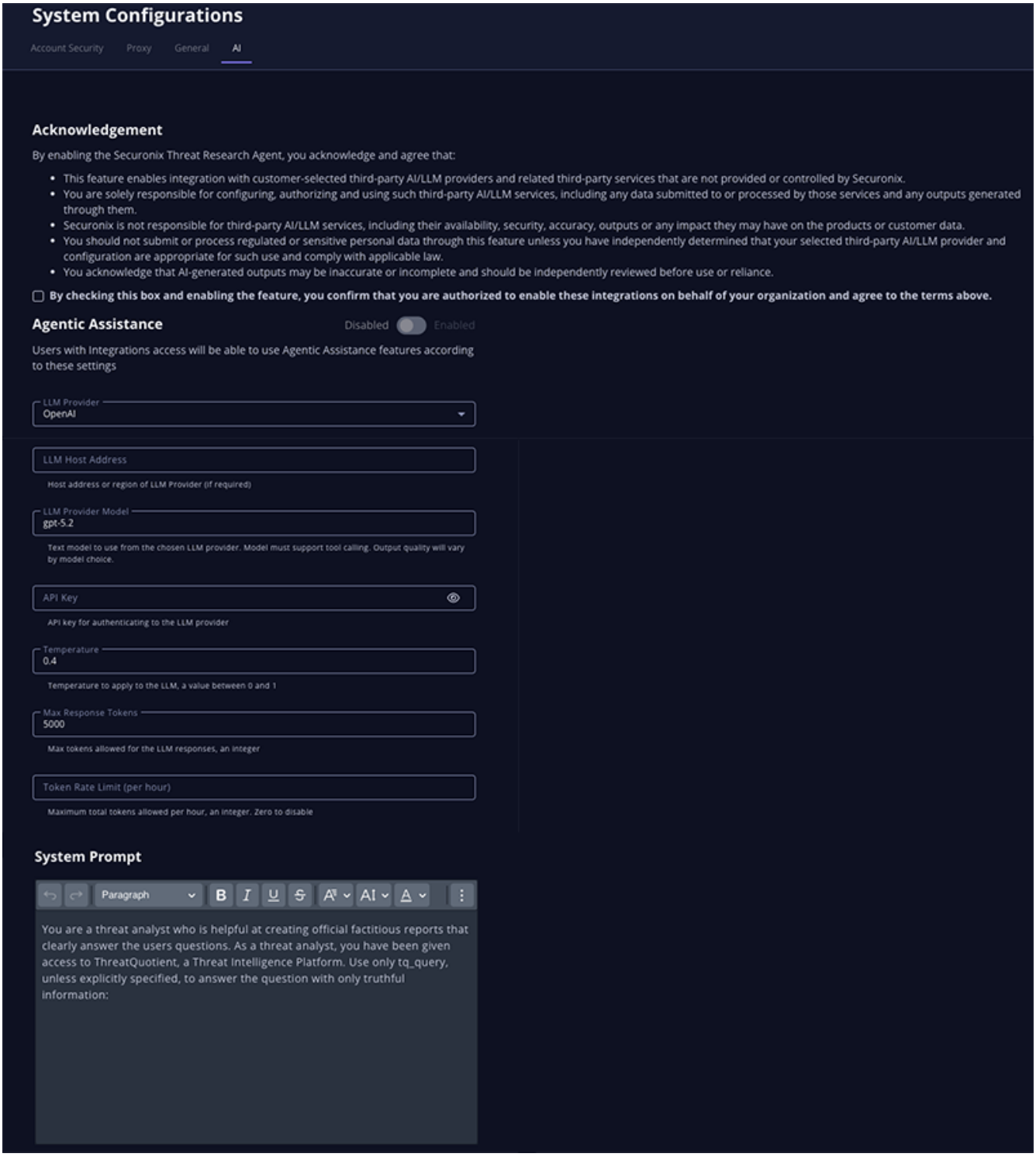
About the AI Tab

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative or Maintenance
Custom Role - Action Permissions: Administrative Functions - Edit System Configurations

The AI tab allows you access the configuration settings for ThreatQ's agentic AI offering: the ThreatQ Research Agent.

See the Threat Research Agent section for complete configuration and operation details.


System Configurations
Account Security
Proxy
General
AI
Acknowledgement
By enabling the Securonix Threat Research Agent, you acknowledge and agree that:
This feature enables integration with customer-selected third-party AI/LLM providers and related third-party services that are not provided or controlled by Securonix.
You are solely responsible for configuring, authorizing and using such third-party AI/LLM services, including any data submitted to or processed by those services and any outputs generated through them.
Securonix is not responsible for third-party AI/LLM services, including their availability, security, accuracy, outputs or any impact they may have on the products or customer data.
You should not submit or process regulated or sensitive personal data through this feature unless you have independently determined that your selected third-party AI/LLM provider and configuration are appropriate for such use and comply with applicable law.
You acknowledge that AI-generated outputs may be inaccurate or incomplete and should be independently reviewed before use or reliance.
By checking this box and enabling the feature, you confirm that you are authorized to enable these integrations on behalf of your organization and agree to the terms above.
Agentic Assistance
Disabled
Enabled
Users with Integrations access will be able to use Agentic Assistance features according to these settings
LLM Provider
OpenAI
LLM Host Address
Host address or region of LLM Provider (if required)
LLM Provider Model
gpt-5.2
Text model to use from the chosen LLM provider. Model must support tool calling. Output quality will vary by model choice.
API Key
API key for authenticating to the LLM provider
Temperature
0.4
Temperature to apply to the LLM, a value between 0 and 1
Max Response Tokens
5000
Max tokens allowed for the LLM responses, an integer
Token Rate Limit (per hour)
Maximum total tokens allowed per hour, an integer. Zero to disable
System Prompt
Paragraph
You are a threat analyst who is helpful at creating official factitious reports that clearly answer the users questions. As a threat analyst, you have been given access to ThreatQuotient, a Threat Intelligence Platform. Use only tq_query, unless explicitly specified, to answer the question with only truthful information:

TQAdmin Configuration

TQAdmin allows you to configure the following options during your initial ThreatQ install and to update these options after the initial install:

- OpenDXL (requires a ThreatQ Data Exchange license)
- TAXII (requires a ThreatQ Data Exchange license)
- Threat Research Agent (requires a Threat Research Agent license)

> ThreatQ Versions <= 6.20.1 - the activation requires editing the **threatq.tfvars** file prior to running TQAdmin. See the Threat Research Agent Requirements topic for more details.
>
> ThreatQ Versions >= 6.21.0 - the activation can be performed using the TQAdmin prompts.

- SSL Certificate
- CAC/mTLS
- Audit log exports

Upgrading TQAdmin

In some instances, you may need to download and install the most recent version TQAdmin to ensure that you have access to all configuration options.

1. Log into your Ubuntu or RHEL instance.
2. Download the most recent version of TQAdmin, using your YUM credentials:
   Ubuntu:

   ```
   curl -fO -u <YUM_USER> https://install-v6.threatq.com/
   tqadmin.deb
   ```

   RHEL:

   ```
   curl -fO -u <YUM_USER> https://install-v6.threatq.com/
   tqadmin.rpm
   ```

3. Run the following command to verify the TQAdmin download:
   Ubuntu:

```
ls -ltr tqadmin.deb
```

RHEL:

```
ls -ltr tqadmin.rpm
```

4. Install TQAdmin:
   Ubuntu:

```
sudo dpkg -i tqadmin.deb
```

RHEL:

```
sudo rpm -Uvh tqadmin.rpm
```

Configuring OpenDXL

The ThreatQ Data Exchange (TQX) product license provides access to both OpenDXL and TAXII server functionality. For those customers who do not wish to use both, TQAdmin allows you to enable/disable OpenDXL and TAXII separately. This allows you to focus your system resources on the functionality you want to use.

1. Access the ThreatQ host command line via SSH or console.
2. Run the following command:

```
sudo /usr/local/bin/tqadmin configure
```

The TQadmin configure command displays a series of prompts.

> ⚠ To prevent undesired changes to your system, you must enter a response for each prompt based on your current system configuration. For example, if your organization uses ThreatQ Data Exchange'sTAXII functionality you must enter "yes" for the **Do you want to enable TAXII** prompt.

3. To use your own SSL certificate for the ThreatQ interface, populate the following:

PROMPT	DESCRIPTION
Do you want to enable OpenDXL (TQX)? (yes/no)	Enter yes to enable ThreatQ Data Exchange's OpenDXL functionality. Enter no to disable this functionality.

4. When prompted, enter your YUM username and password.
5. Run the following command to save and apply your changes:

```
sudo /usr/local/bin/tqadmin reapply
```

Configuring TAXII

1. Access the ThreatQ host command line via SSH or console.
2. Run the following command:

```
sudo /usr/local/bin/tqadmin configure
```

The TQadmin configure command displays a series of prompts.

> ⚠ To prevent undesired changes to your system, you must enter a response for each prompt based on your current system configuration. For example, if your organization uses ThreatQ Data Exchange's OpenDXL functionality you must enter "yes" for the **Do you want to enable OpenDXL** prompt.

3. To use your own SSL certificate for the ThreatQ interface, populate the following:

PROMPT	DESCRIPTION
Do you want to enable the embedded TAXII server? (yes/no)	Enter yes to enable ThreatQ Data Exchange's TAXII server functionality. Enter no to disable this functionality.

4. When prompted, enter your YUM username and password.
5. Run the following command to save and apply your changes:

```
sudo /usr/local/bin/tqadmin reapply
```

Configuring a Web Server Certificate

The following steps allow you to update the SSL certificate from the default self-signed certificate used for the ThreatQ user interface.

1. Move your SSL certificate file to a directory on your ThreatQ instance.
2. Access the ThreatQ host command line via SSH or console.
3. Run the following command:

   ```
   sudo /usr/local/bin/tqadmin configure
   ```

   The TQadmin configure command displays a series of prompts.

   > To prevent undesired changes to your system, you must enter a response for each prompt based on your current system configuration. For example, if your organization uses ThreatQ Data Exchange's OpenDXL functionality you must enter "yes" for the **Do you want to enable OpenDXL** prompt.

4. To use your own SSL certificate for the ThreatQ interface, populate the following:

PROMPT	DESCRIPTION
Do you want to use your own SSL certificate? (yes/no):	Enter yes.
Enter the file path for your certificate	Enter the path for your SSL certificate. **example:** /etc/threatq-certs/mycert.pem
Enter the file path for your private key	Enter the path for the SSL certificate's private key. **example:** /etc/threatq-certs/mykey.pem

5. When prompted, enter your YUM username and password.
6. Run the following command to save and apply your changes:

   ```
   sudo /usr/local/bin/tqadmin reapply
   ```

Configuring SSL Client Certificate Authentication

1. Move your CA certificate file to a directory on your ThreatQ instance.
2. Access the ThreatQ host command line via SSH or console.
3. Run the following command:

```
sudo /usr/local/bin/tqadmin configure
```

The TQadmin configure command displays a series of prompts.

To prevent undesired changes to your system, you must enter a response for each prompt based on your current system configuration. For example, if your organization uses ThreatQ Data Exchange's OpenDXL functionality you must enter "yes" for the **Do you want to enable OpenDXL** prompt.

4. To enable SSL Client Certification, populate the following:

PROMPT	DESCRIPTION
Do you want to enable CAC/mTLS? (yes/no):	Enter yes.
Enter the file path for your certificate:	Enter the path for your CA Certificate. **example:** /tmp/mycert.pem
Enter the FQDN of the server:	Enter the FQDN of the server. **example**: myserver.threatq.com

5. When prompted, enter your YUM username and password.
6. Run the following command to save and apply your changes:

```
sudo /usr/local/bin/tqadmin reapply
```

7. After your changes are saved, the CAC/PV SSL tab in the User Management page displays a status of Currently Enabled.
8. 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.

9. 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.

Configuring Audit Log Exports

1. Access the ThreatQ host command line via SSH or console.
2. Run the following command:

```
sudo /usr/local/bin/tqadmin configure
```

The TQAdmin configure command displays a series of prompts.

> To prevent undesired changes to your system, you must enter a response for each prompt based on your current system configuration. For example, if your organization uses ThreatQ Data Exchange's OpenDXL functionality, you must enter "yes" for the **Do you want to enable OpenDXL prompt**.

3. Populate the following prompts:
   - **Enable syslog audit log output?** Type yes to access additional configuration prompts.
   - **Enter the hostname or IP address of the syslog server to send audit log messages:**
   - **Enter the port number on the syslog server for audit log messages (default 514):**
   - **Enable TLS with a client certificate for the syslog server?** - If you enter yes for this prompt, TQAdmin displays the following three prompts.
     - Enter the full path to the client certificate file:
     - Enter the full path to the client private key file:
     - Enter the path to the trusted root CA certificate for the syslog server (leave empty to disable certificate validation):

4. When prompted, enter your YUM username and password.
5. Run the following command to save and apply your changes:

```
sudo /usr/local/bin/tqadmin reapply
```

System Objects

About System Objects

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role - Action Permissions: Objects & Context - Objects (all object types), Individual Object Context & Actions
Custom Role - Data Access Permissions: Specific object types

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.	About Events

SYSTEM OBJECT	DESCRIPTION	RELATED TOPICS
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 Indicators, Adversaries, and Malware samples.	Files
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
Infrastructure	Information that describes any systems, software services and associated physical or virtual resources intended to support a specific purpose.	Infrastructure
Intrusion Sets	Grouped sets of adversarial behaviors and resources, sometimes referred to as attack packages, used to target an individual organization.	Intrusion Sets

SYSTEM OBJECT	DESCRIPTION	RELATED TOPICS
Malware	Targets devices, services, and networks with the intent to gain unauthorized access or damage a network or programmable device.	Malware
Notes	STIX 2.1 objects that provide further context and/or additional analysis.	Notes
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
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

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role:

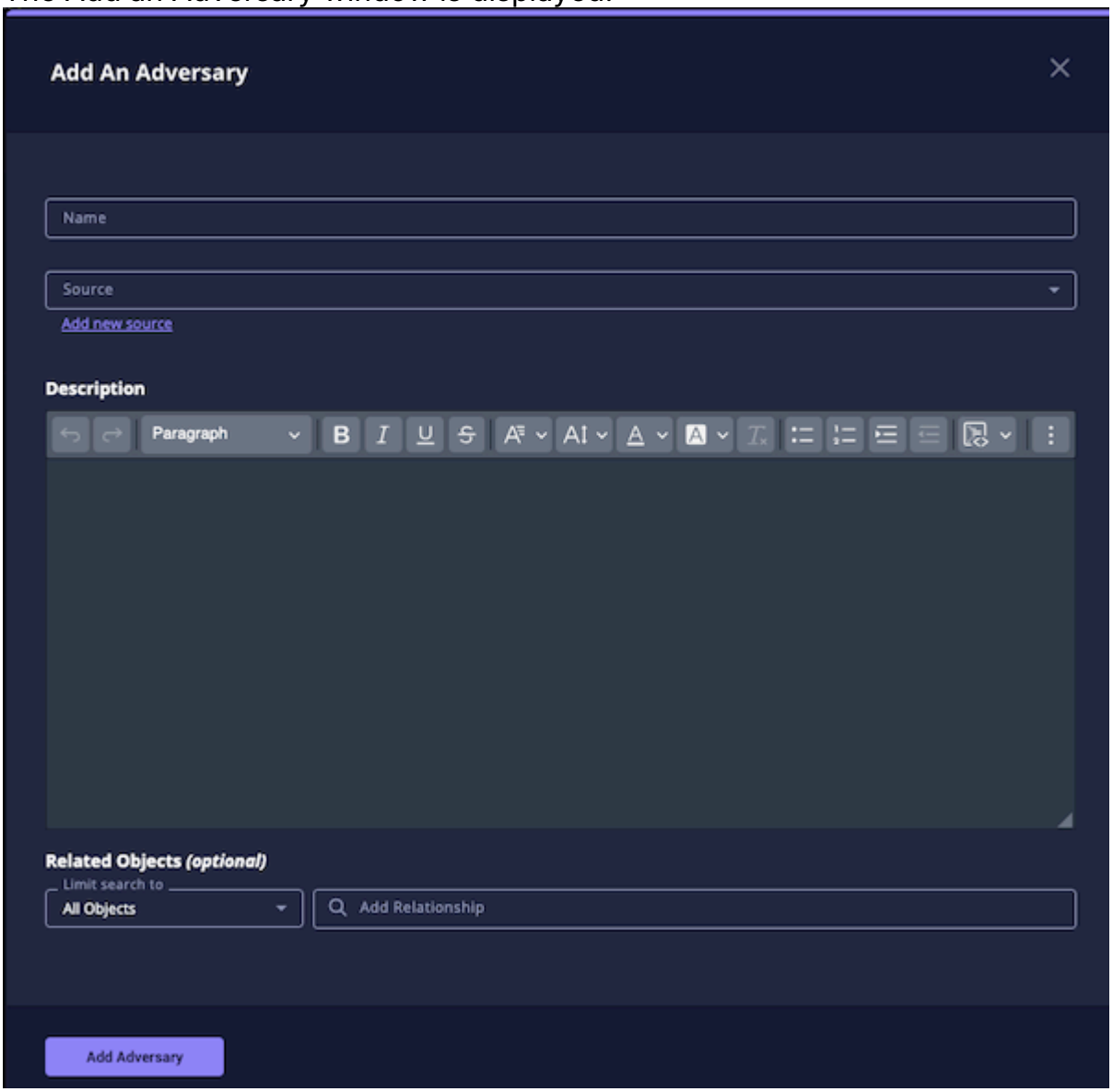
- Action Permissions: Objects & Context - Objects (all object types) **OR** Data Access Permissions: Adversaries
- Action Permissions: Individual Object Context & Actions
  Note: If a user has View Only permission for Sources, system object creation modals default to the user's login as the object source.

An Adversaries 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 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.
4. Enter a description.

> Any description you add during object creation defaults to a Source value of ThreatQ System.

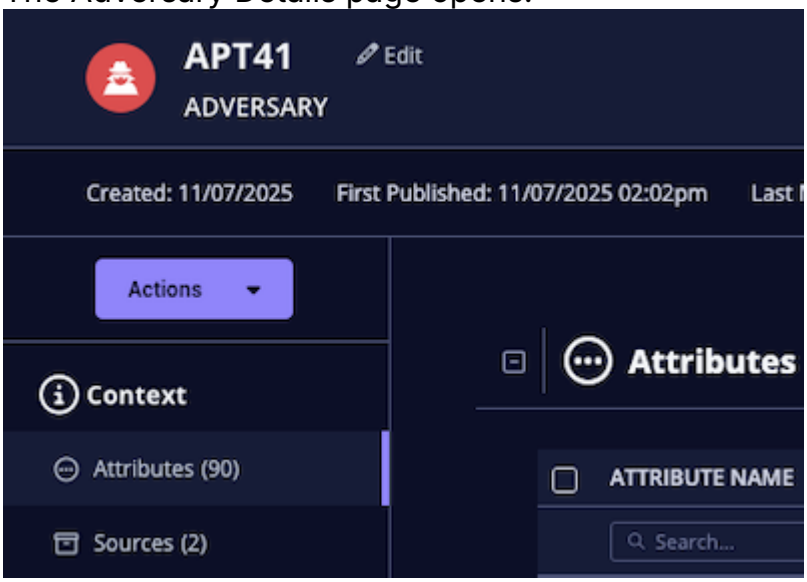
5. Select any **Related Objects** you need to link to the adversary. This field is optional.
6. Click the **Add Adversary** button.

Adding Context

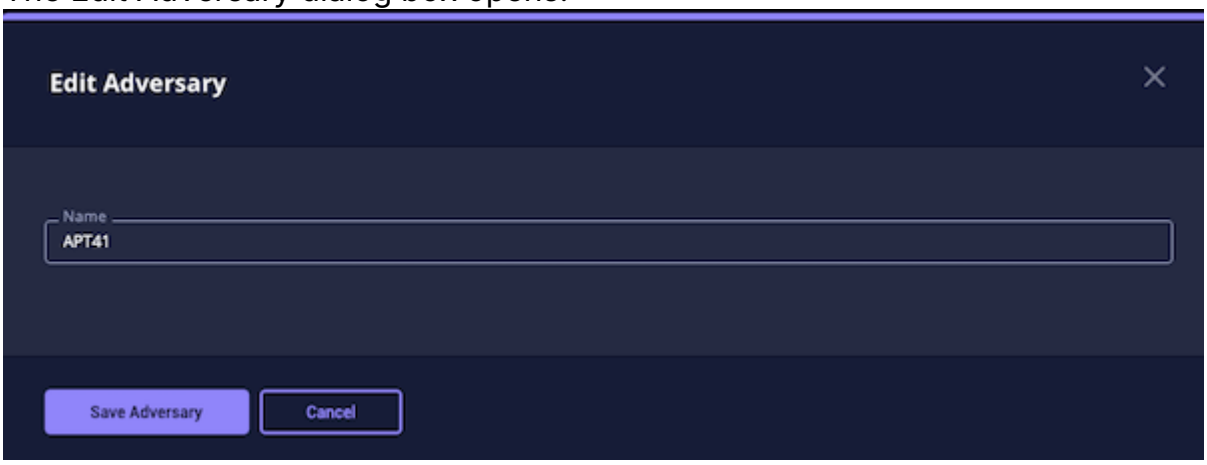
See the About Object Details Page section and its topics for details on adding context to an object such as adding sources, attributes, and related objects.

Editing Adversaries

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



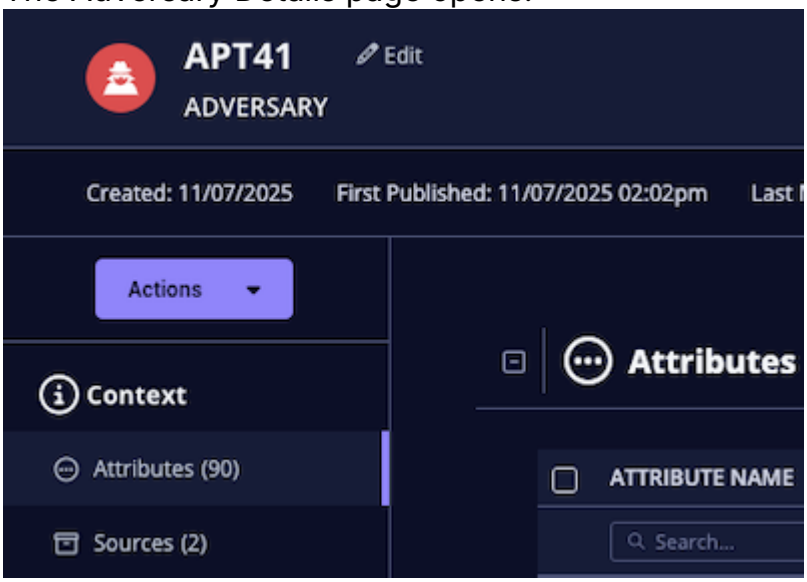
2. Click on **Edit** next to the Adversary name.
   The Edit Adversary dialog box opens.



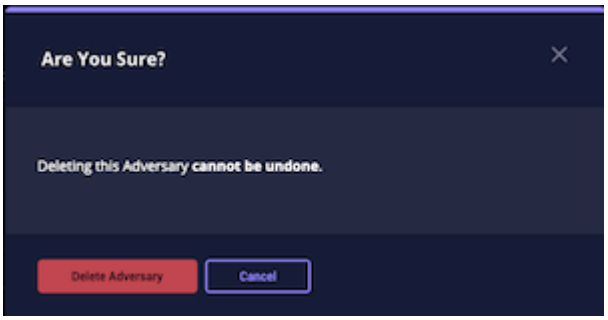
3. Make the desired change to the Adversary name.
4. Click the **Save Adversary** button.

Deleting Adversaries

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



2. Click the **Actions** menu and select **Delete Adversary**.
   A confirmation dialog box appears.



3. Click the **Delete Adversary** button.

Assets

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor

Custom Role:

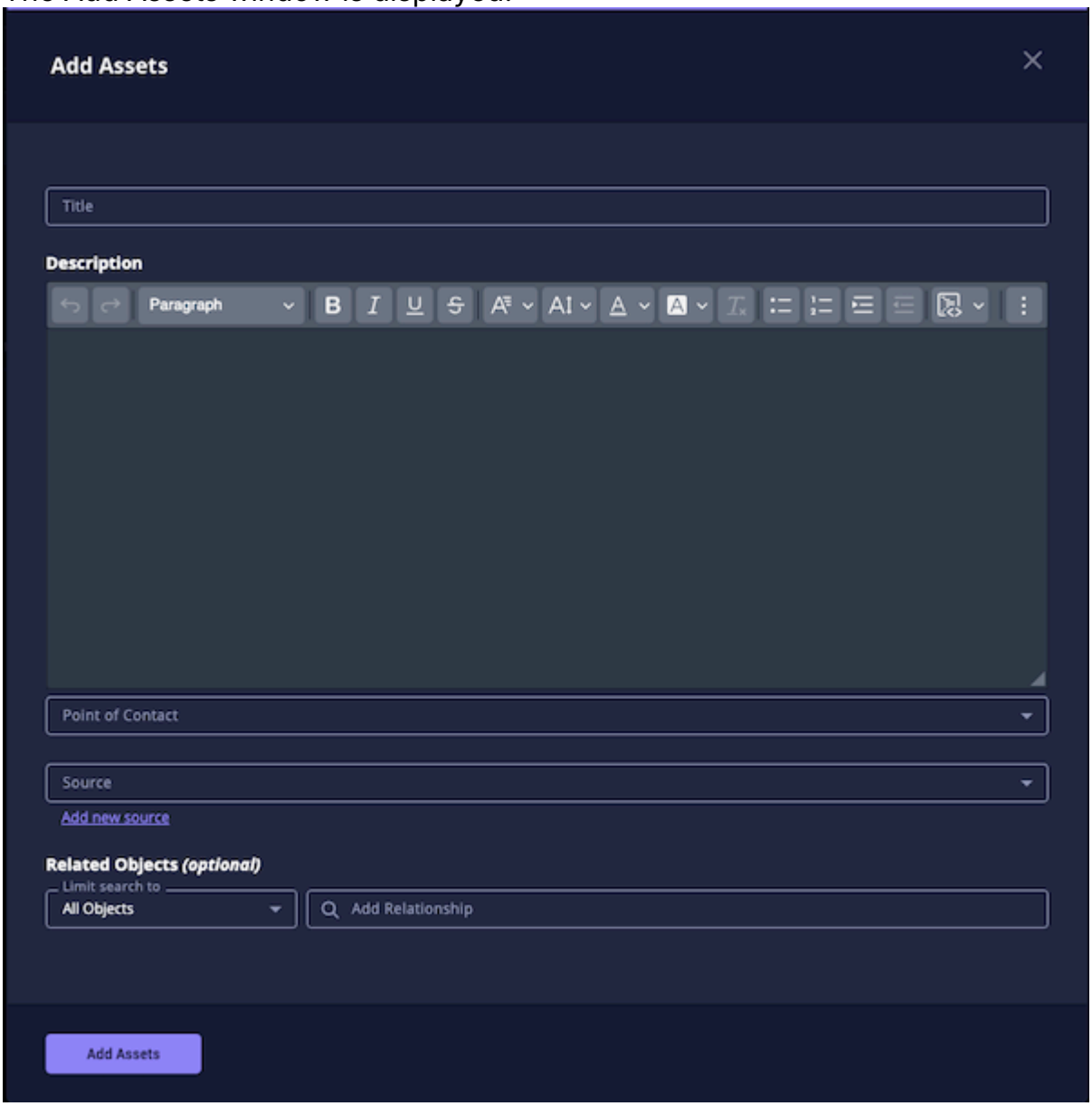
- Action Permissions: Objects & Context - Objects (all object types) **OR** Data Access Permissions: Assets
- Action Permissions: Individual Object Context & Actions
  Note: If a user has View Only permission for Sources, system object creation modals default to the user's login as the object source.

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. Populate the following fields:

FIELD	DESCRIPTION
Title	Add an asset title.
Description	Enter a brief description of the asset.

FIELD	DESCRIPTION
	Any description you add during object creation defaults to a Source value of ThreatQ System.
Status	Optional field. Click the Status field to assign a status to the assets object. Asset statuses are configured in the Object Statuses tab in the Object Management page. If none are configured, this field is not displayed.
Point of Contact	Optional field. Click the field to select the ThreatQ display name of the point of contact for the asset.
Source	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.

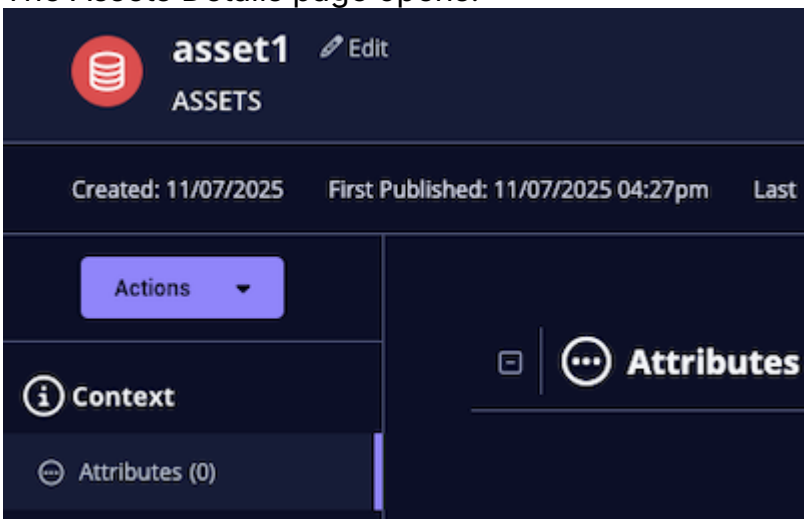
3. Select any **Related Objects** you need to link to the asset. This field is optional.
4. Click **Add Assets**.

Adding Context

See the About Object Details Page 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 Asset name.
4. Click the **Save Assets** button.

Changing the Point of Contact

THREATQ REQUIRED PERMISSIONS

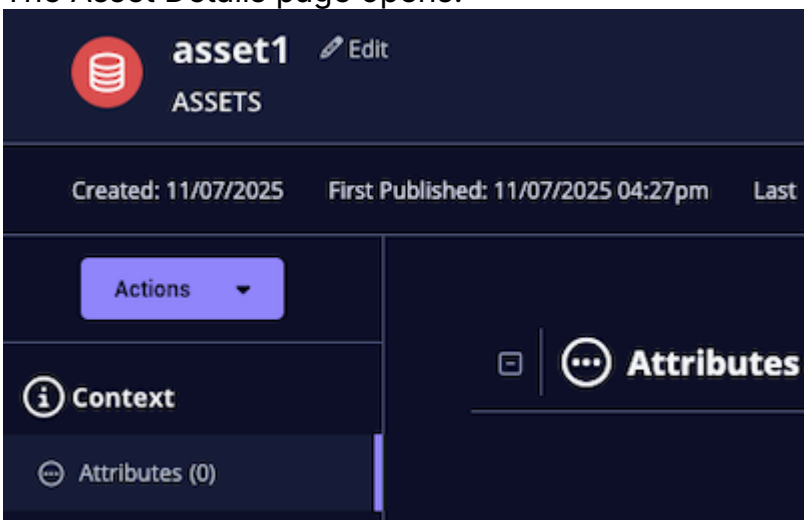
Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role - Action Permissions: Objects & Context - Objects, Individual Object Context & Actions - Point of Contact

1. Locate and click the system object.

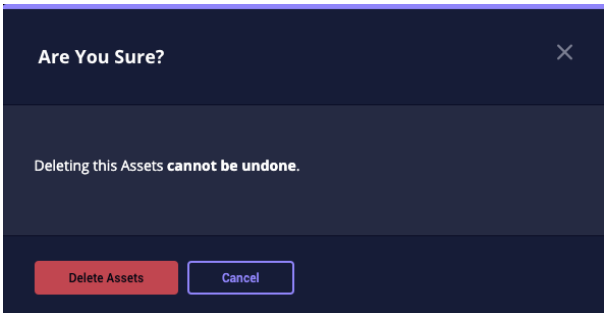
2. From the object details page, click the Point of Contact field.
3. Use the field's scroll or search option to locate and select a new user as the object's point of contact or to change the point of contact to Unassigned.

Deleting Assets

1. Locate and click the assets object.
   The Asset Details page opens.



2. Click 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

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor

Custom Role:

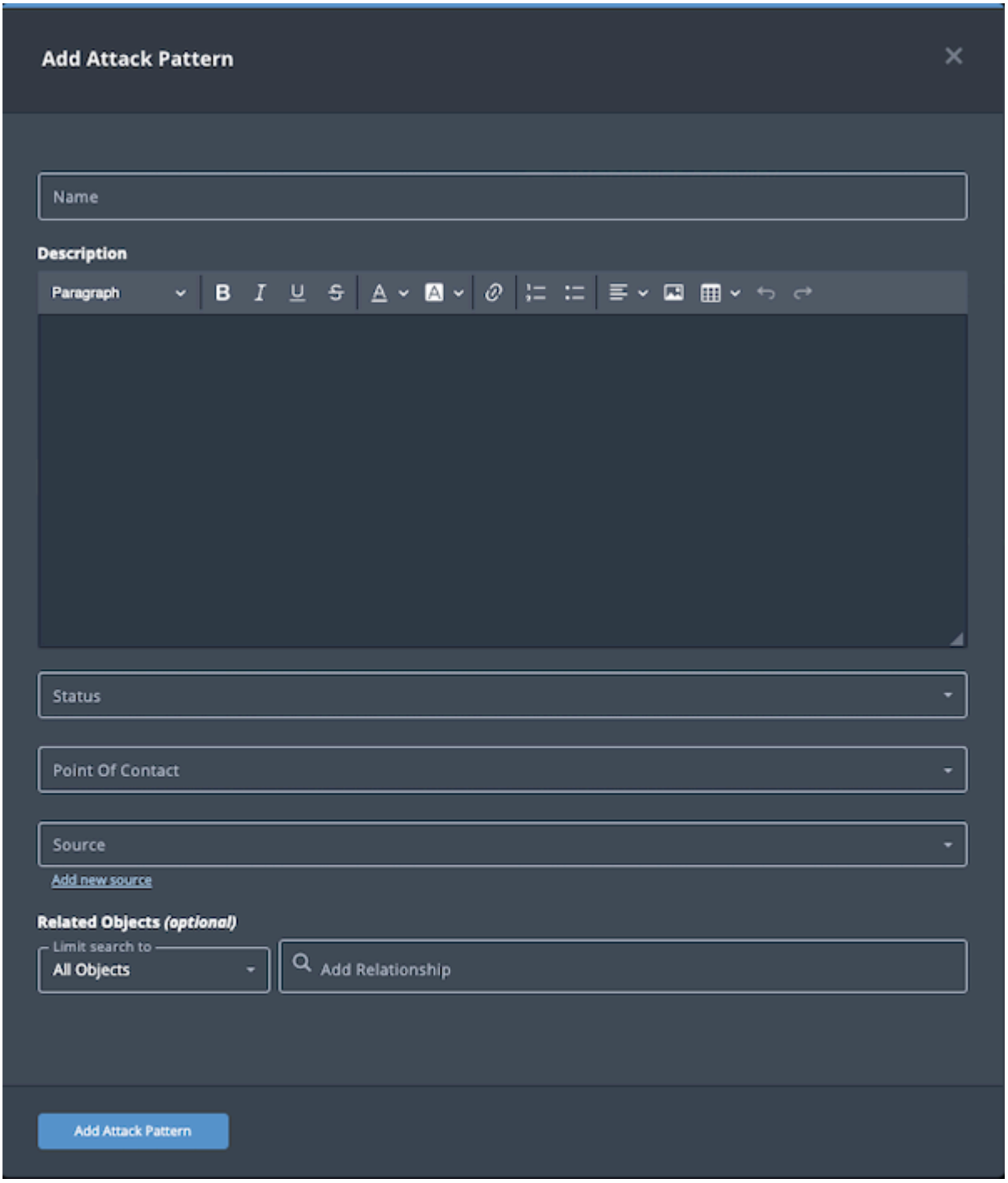
- Action Permissions: Objects & Context - Objects (all object types) **OR** Data Access Permissions: Attack Pattern
- Action Permissions: Individual Object Context & Actions
  Note: If a user has View Only permission for Sources, system object creation modals default to the user's login as the object source.

Attack Patterns 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 window is displayed



2. Populate the following fields:

FIELD	DESCRIPTION
Name	Add an attack pattern name.

FIELD	DESCRIPTION
Description	Enter a brief description of the attack pattern. Any description you add during object creation defaults to a Source value of ThreatQ System.
Status	Optional field. Click the Status field to assign a status to the attack pattern object. Attack pattern statuses are configured in the Object Statuses tab in the Object Management page. If none are configured, this field is not displayed.
Point of Contact	Optional field. Click the field to select the ThreatQ display name of the point of contact for the attack pattern.
Source	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.

3. Select any **Related Objects** you need to link to the attack pattern. This field is optional.
4. Click **Add Attack Pattern**.

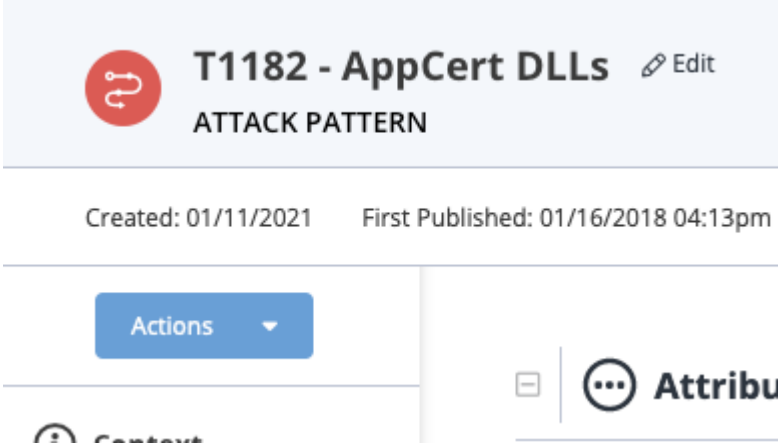
Adding Context

See the About Object Details Page section and its topics for details on adding context to an object such as adding sources, attributes, and related objects.

Editing an Attack Pattern

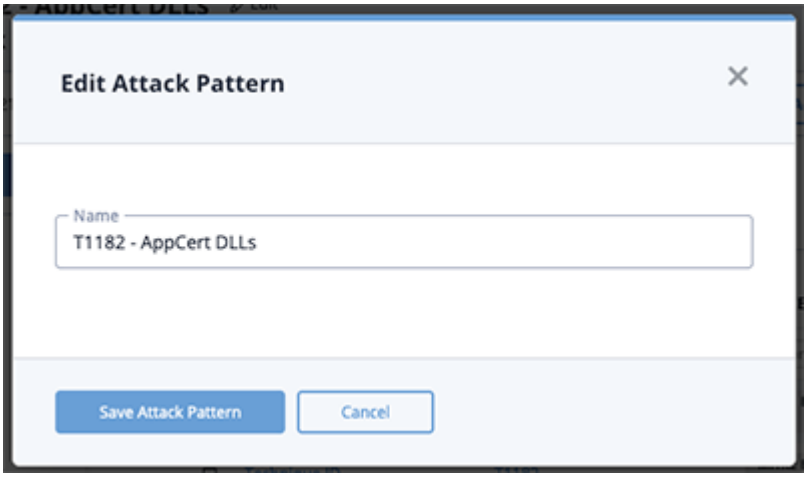
1. Locate and click on the attack pattern.

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**.

Changing the Point of Contact

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role - Action Permissions: Objects & Context - Objects, Individual Object Context & Actions - Point of Contact

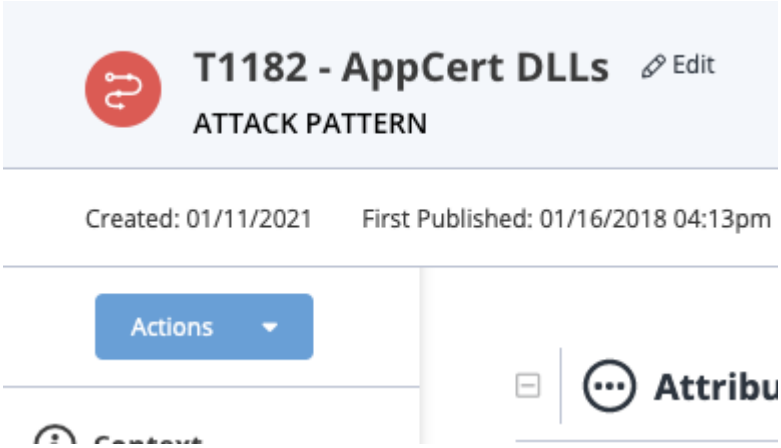
1. Locate and click the system object.
2. From the object details page, click the Point of Contact field.

3. Use the field's scroll or search option to locate and select a new user as the object's point of contact or to change the point of contact to Unassigned.

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

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor

Custom Role:

- Action Permissions: Objects & Context - Objects (all object types) **OR** Data Access Permissions: Campaign
- Action Permissions: Individual Object Context & Actions
  Note: If a user has View Only permission for Sources, system object creation modals default to the user's login as the object source.

A Campaigns is a group of behaviors that describes 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 window is displayed.

Add Campaign

Name

Description

Paragraph

Status

Objective

Paragraph

First Seen
November 13 2023 Time 08:36 PM Time Zone UTC

Last Seen
November 13 2023 Time 08:36 PM Time Zone UTC

Point Of Contact

Source

Add new source

Related Objects *(optional)*

Limit search to
All Objects

Add Relationship

2. Populate the following fields:

FIELD	DESCRIPTION
Name	Add a campaign name.
Description	Enter a brief description of the campaign. Any description you add during object creation defaults to a Source value of ThreatQ System.
Status	Optional field. Click the Status field to assign a status to the campaign object. Campaign statuses are configured in the Object Statuses tab in the Object Management page. If none are configured, this field is not displayed.
Objective	Add a summary of the campaign's objective.
First Seen/ Last Seen	Select the first and last seen dates and times.
Point of Contact	Optional field. Click the field to select the ThreatQ display name of the point of contact for the campaign.
Source	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.

3. Select any **Related Objects** you need to link to the campaign. This field is optional.
4. Click the **Add Campaign** button.

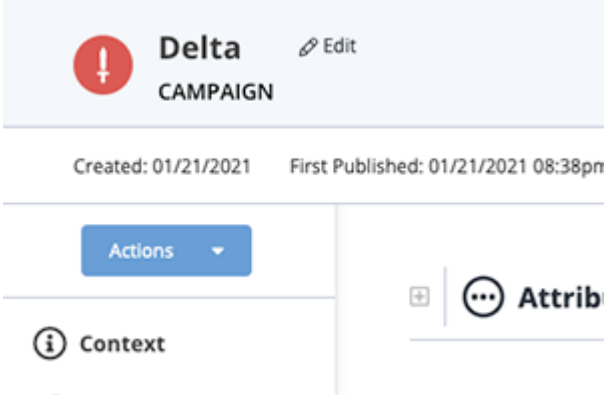
Adding Context

See the About Object Details Page section and its topics for details on adding context to an object such as adding sources, attributes, and related objects.

Editing a Campaign

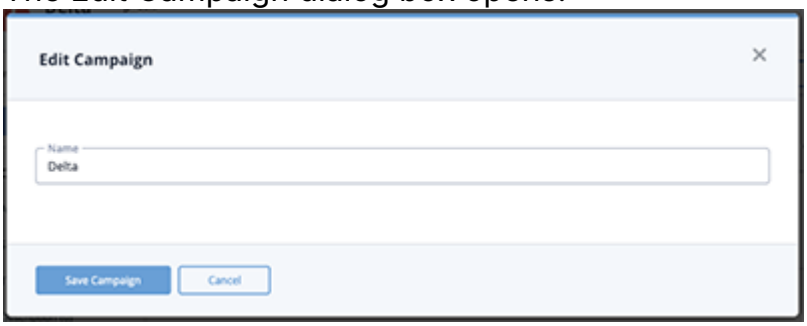
1. Locate and click on the Campaign.

   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**.

Changing the Point of Contact

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role - Action Permissions: Objects & Context - Objects, Individual Object Context & Actions - Point of Contact

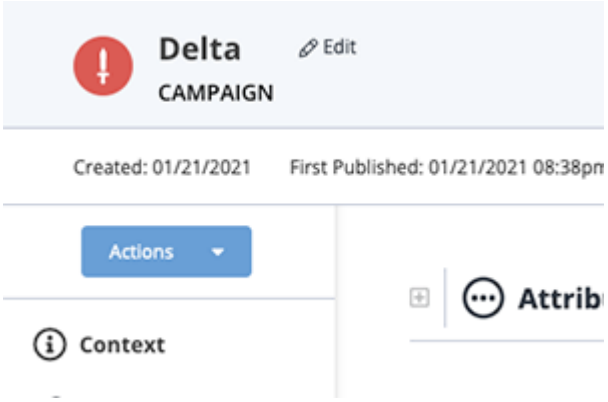
1. Locate and click the system object.
2. From the object details page, click the Point of Contact field.

3. Use the field's scroll or search option to locate and select a new user as the object's point of contact or to change the point of contact to Unassigned.

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

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor

Custom Role:

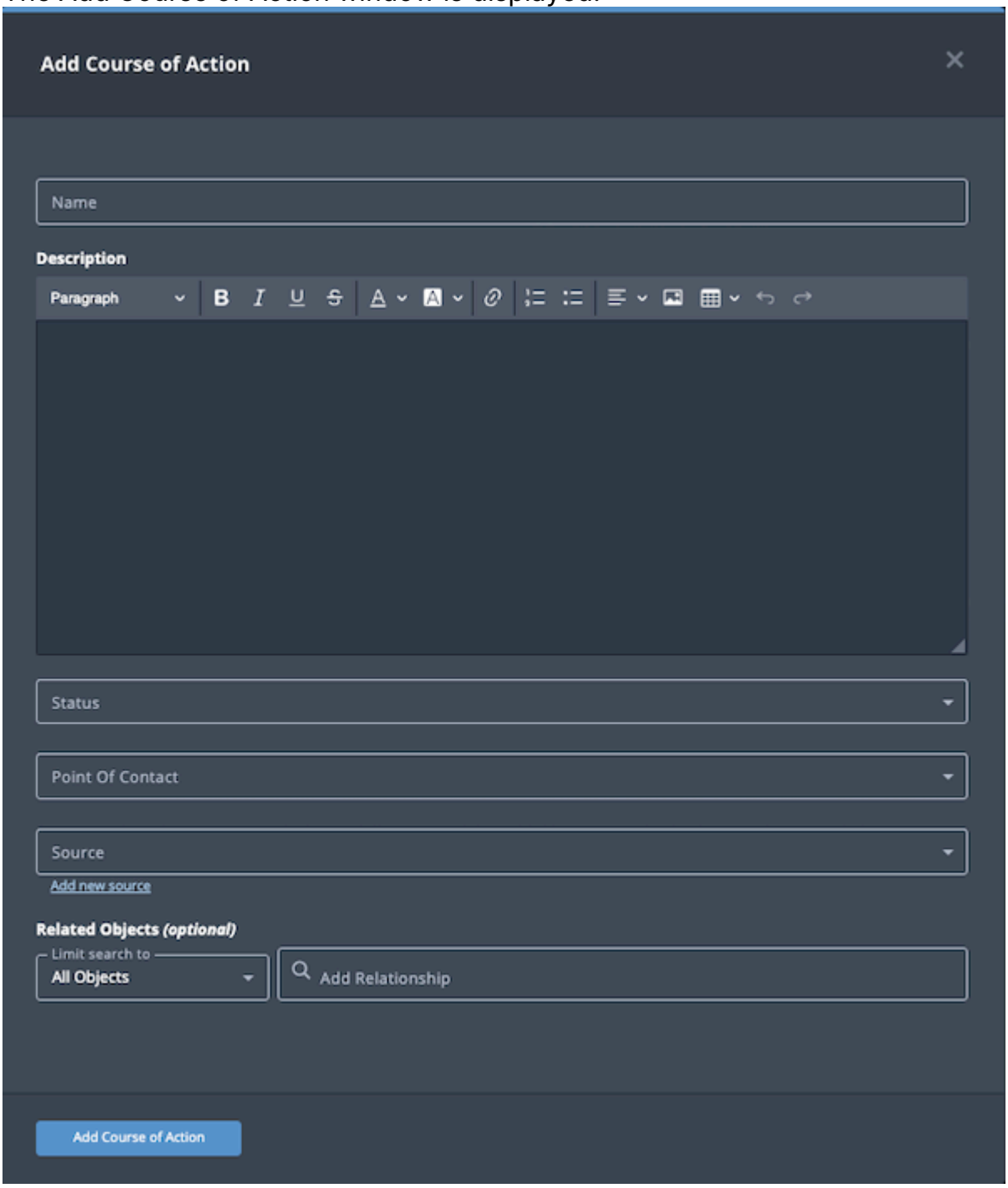
- Action Permissions: Objects & Context - Objects (all object types) **OR** Data Access Permissions: Course of Action
- Action Permissions: Individual Object Context & Actions
  Note: If a user has View Only permission for Sources, system object creation modals default to the user's login as the object source.

Courses of Actions 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 window is displayed.



2. Populate the following fields:

FIELD	DESCRIPTION
Name	Add the course of action's name.
Description	Enter a brief description of the course of action. Any description you add during object creation defaults to a Source value of ThreatQ System.
Status	Optional field. Click the Status field to assign a status to the course of action. Course of action statuses are configured in the Object Statuses tab in the Object Management page. If none are configured, this field is not displayed.
Point of Contact	Optional field. Click the field to select the ThreatQ display name of the point of contact for the course of action.
Source	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.

3. Select any **Related Objects** you need to link to the Course of Action. This field is optional.
4. Click **Add Course of Action**.

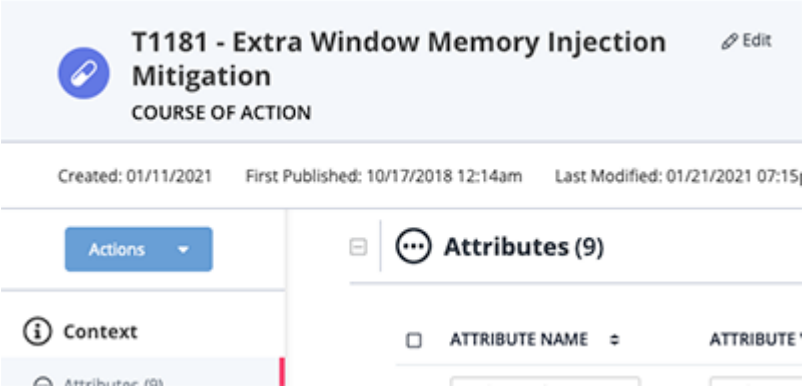
Adding Context

See the About Object Details Page 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

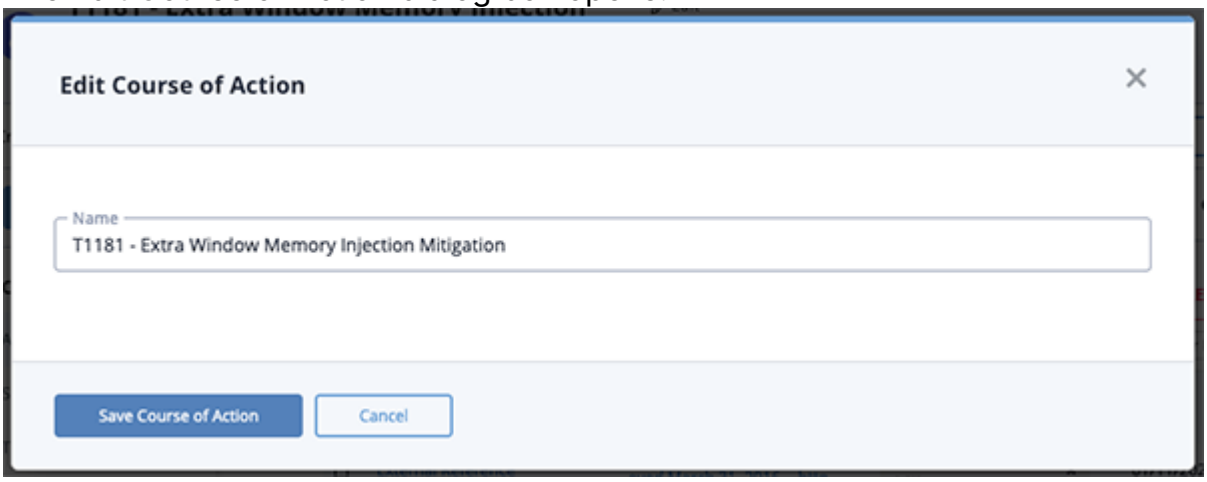
1. Locate and click on the Course of Action.

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.



3. Make the desired change to the Course of Action's name and click **Save Course of Action**.

Changing the Point of Contact

THREATQ REQUIRED PERMISSIONS

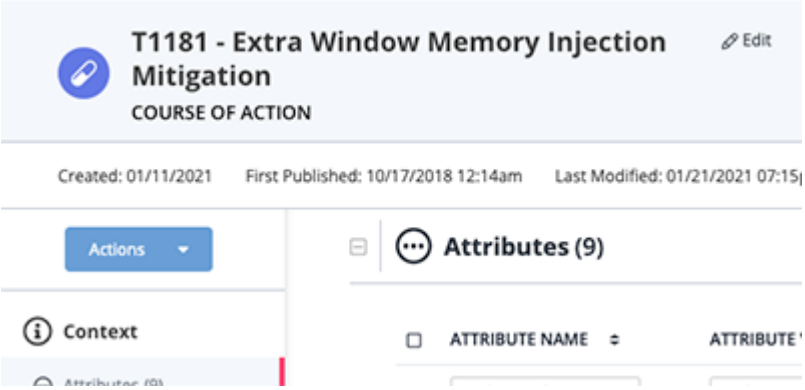
Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role - Action Permissions: Objects & Context - Objects, Individual Object Context & Actions - Point of Contact

1. Locate and click the system object.
2. From the object details page, click the Point of Contact field.
3. Use the field's scroll or search option to locate and select a new user as the object's point of contact or to change the point of contact to Unassigned.

Deleting a Course of Action

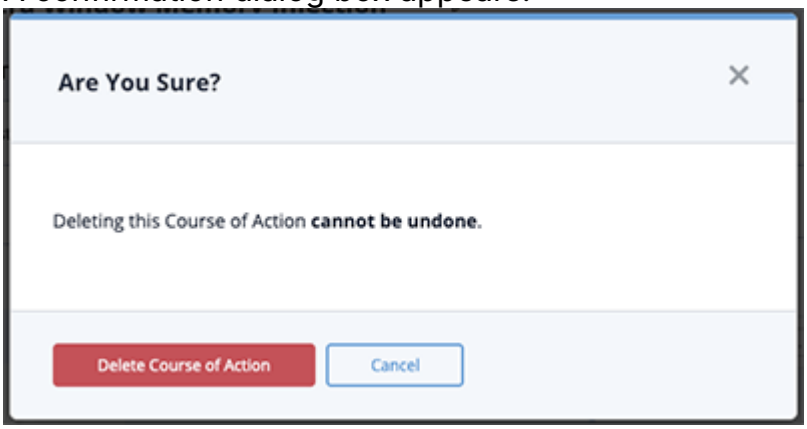
1. Locate and click on the Course of Action.

   The Course of Action's details page opens.



2. Click on the **Actions** menu and select **Delete Course of Action**.

   A confirmation dialog box appears.



3. Click on **Delete Course of Action**.

Events

About 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

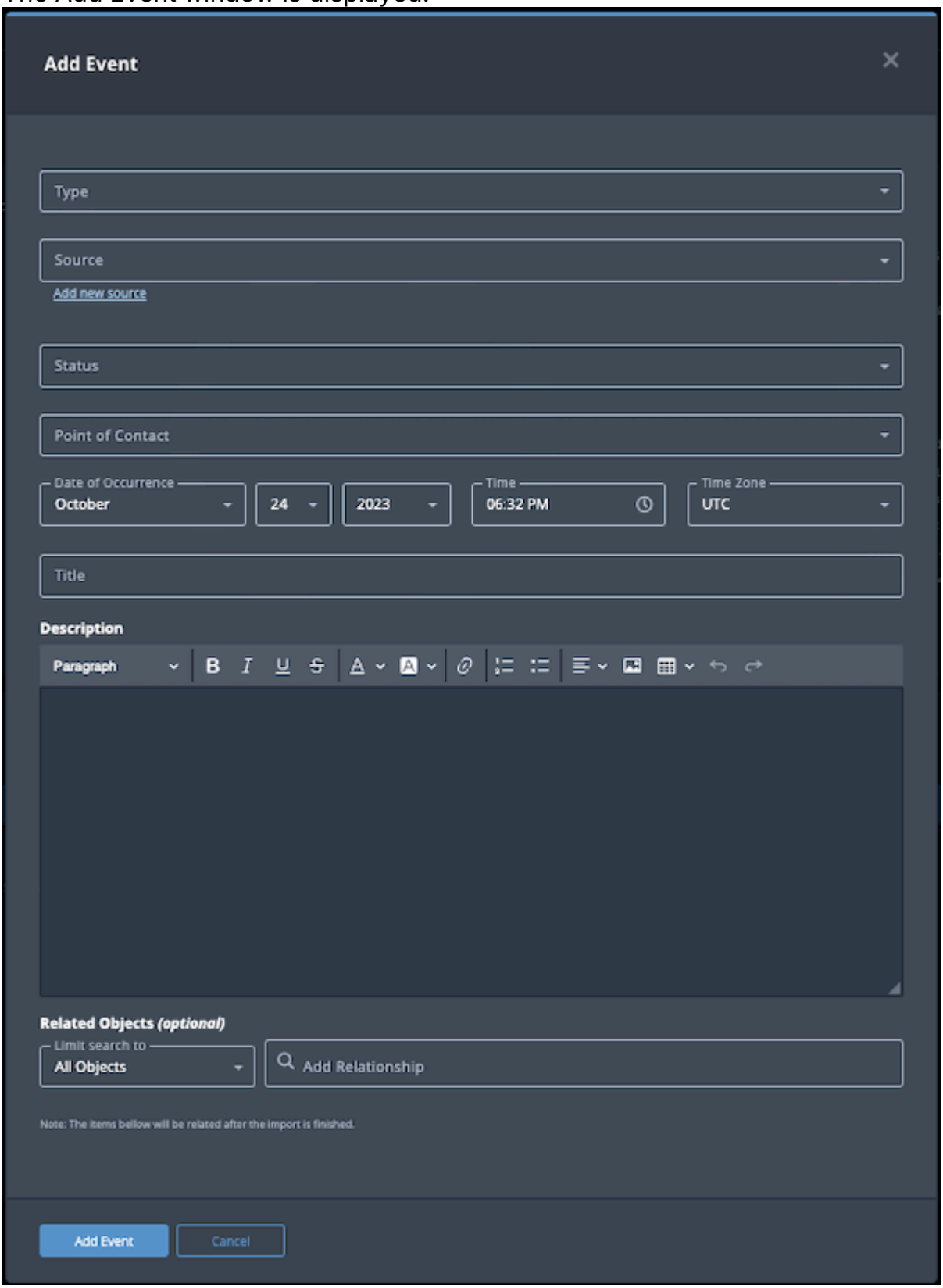
THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor

Custom Role:

- Action Permissions: Objects & Context - Objects (all object types) **OR** Data Access Permissions: Event
- Action Permissions: Individual Object Context & Actions, Perform Bulk Manual Import
  Note: If a user has View Only permission for Sources, system object creation modals default to the user's login as the object source.

1. Go to **Create > Event**.
   The Add Event window is displayed.



2. Populate the following fields:

FIELD	DESCRIPTION
Type	Click this field to select the event type from the dropdown list.
Source	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.
Status	Optional field. Click the Status field to assign a status to the event. Event statuses are configured in the Object Statuses tab in the Object Management page. If none are configured, this field displays a value of None.
Point of Contact	Optional field. Click the field to select the ThreatQ display name of the point of contact for the event.
Date of Occurrence/ Time/Time Zone	Use these fields to add the date and time of the event.
Title	Add an Event Title.
Description	Enter a brief description of the event. Any description you add during object creation defaults to a Source value of ThreatQ System.

3. Select any **Related Objects** you need to link to the event. This field is optional.
4. Click **Add Event**.

Adding Context

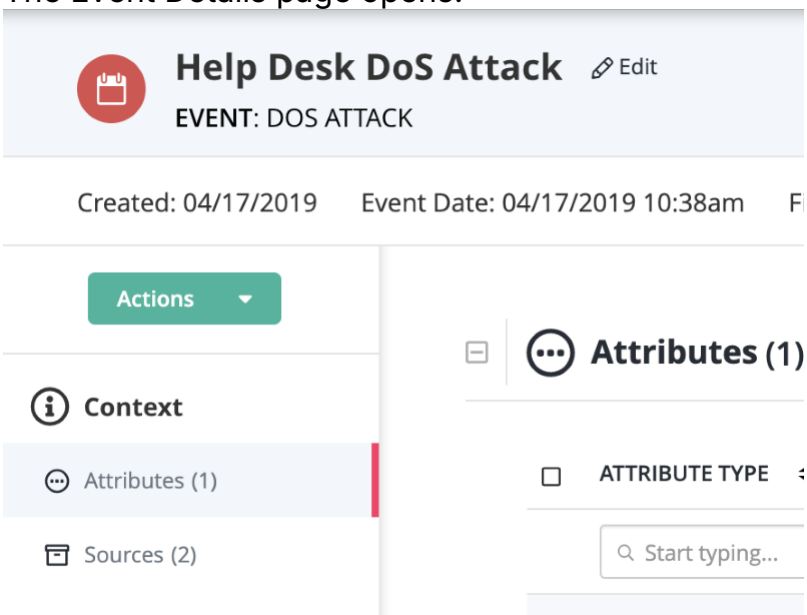
See the About Object Details Page section and its topics for details on adding context to an object such as adding sources, attributes, and related objects.

Editing Events

The Edit Even window allows you to update an Event's title, type and date. You can also update the Event's point of contact, status and type by clicking the corresponding fields located in the top-right of the Event's Object Details page.

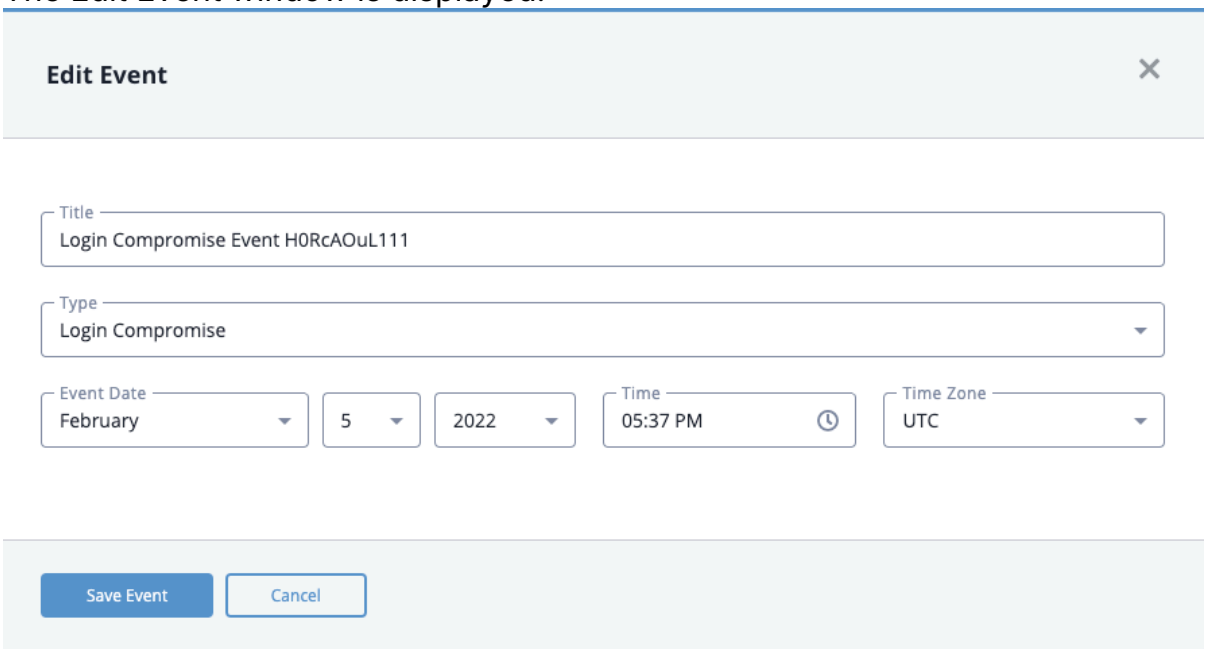
1. Locate and click on the event.

   The Event Details page opens.



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

The Edit Event window is displayed.



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

Changing the Point of Contact

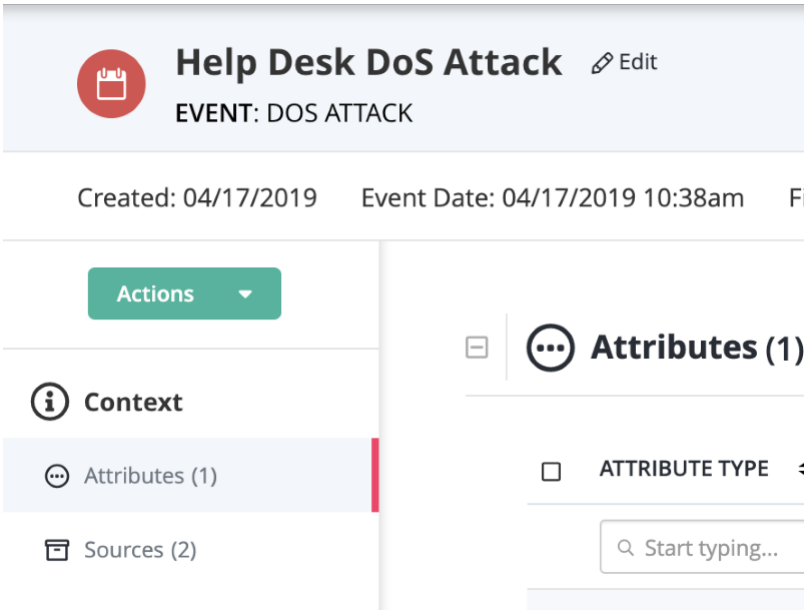
THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role - Action Permissions: Objects & Context - Objects, Individual Object Context & Actions - Point of Contact

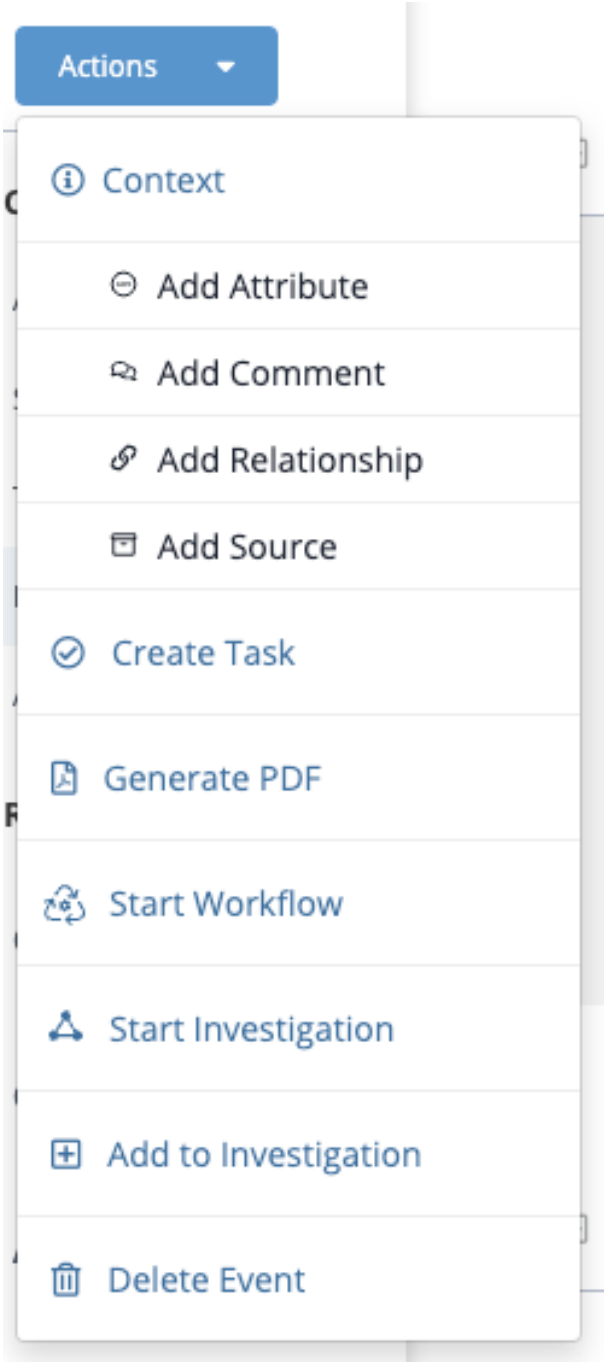
1. Locate and click the system object.
2. From the object details page, click the Point of Contact field.
3. Use the field's scroll or search option to locate and select a new user as the object's point of contact or to change the point of contact to Unassigned.

Deleting Events

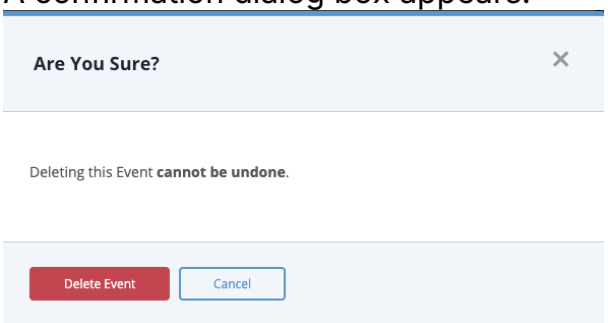
1. Locate and click the event.
   The Events Details page opens.


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

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



A confirmation dialog box appears.



3. Click the **Delete Event** button.

Parsing for Events

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role - Action Permissions: Objects & Context - Perform Bulk Manual Import, Create, Edit, Delete Objects, Create, Edit, Delete Attributes, Create, Edit, Delete Relationships. See the Interdependent Permissions topic.
Notes:

- If a user's role has View Only permission for Sources, system object parsers default to the user's login as the object source.
- If a user's role does not include permission to Edit or delete an object's Status, system object parsers apply the default status to seeded system objects and the first status option for custom objects.

Custom Role - Data Access Permissions: Events

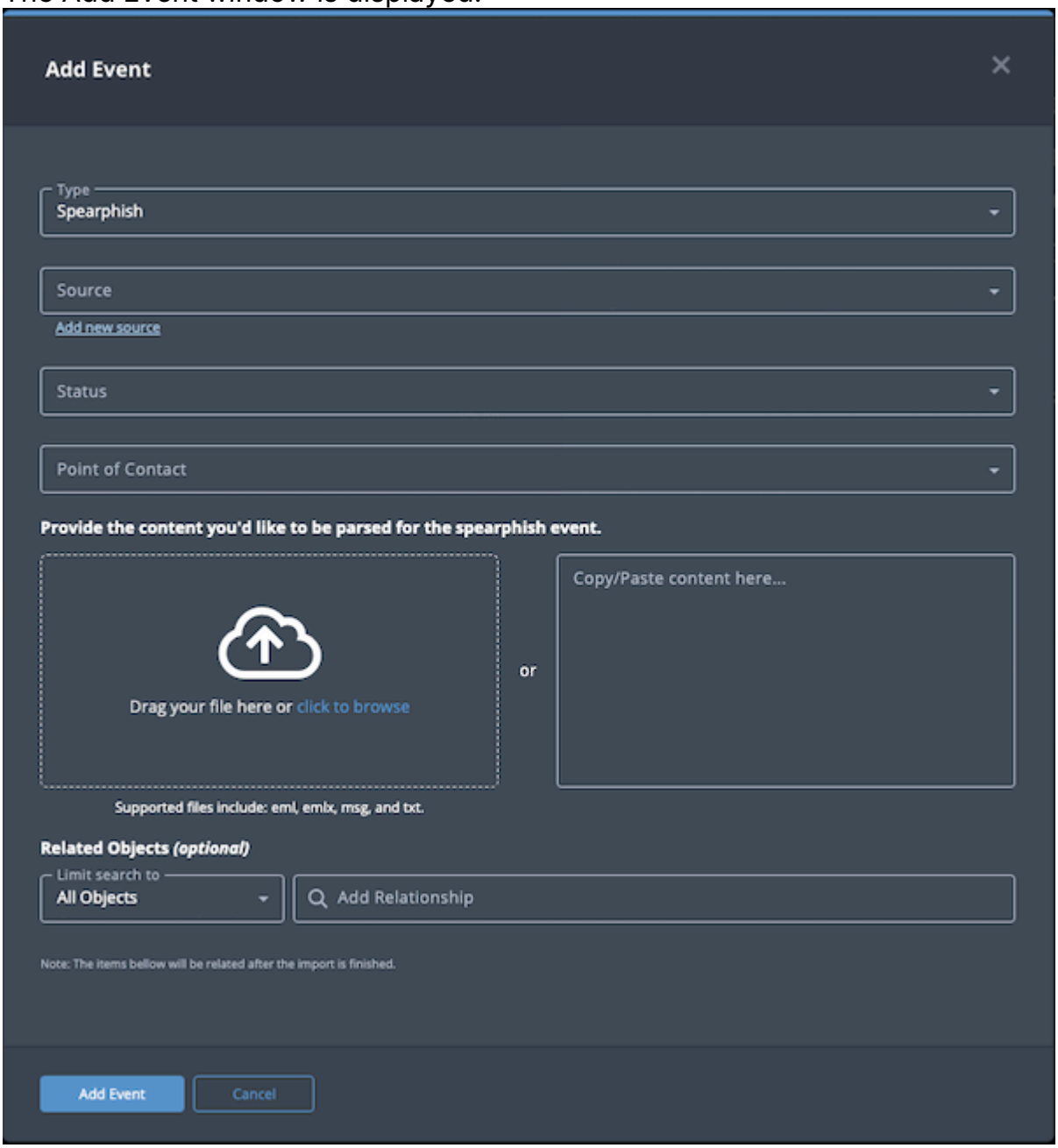
Note:: If an import contains object types or context you lack Create/Edit/Delete permission for, the import fails.

ThreatQ gives you the option to import a file, parse it for events, and add those events to your Threat Library. During the import process you can assign a source, status, point of contact and a relationship to the imported events.

Importing Events with the Spearphish Parser

During the import process you can click the **Abandon this Import** button to stop the import process without adding any of the import file data.

1. Go to **Create > Spearphish Parser**.
   The Add Event window is displayed.



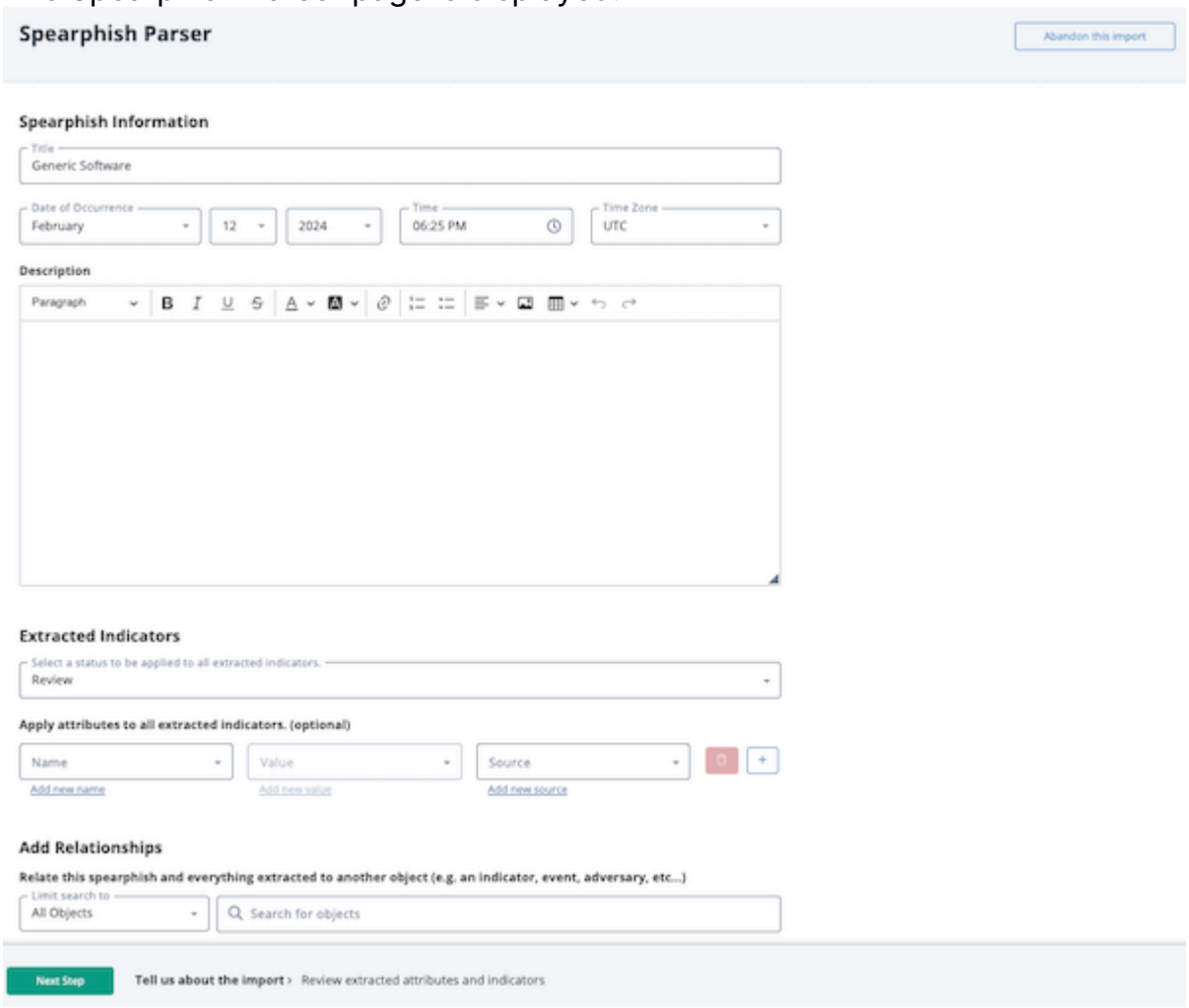
2. Populate the following fields:

FIELD	DESCRIPTION
Type	This field defaults to a value of Spearphish.
Source	Select a **Source** from the dropdown list provided.

FIELD	DESCRIPTION
	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.
Status	Optional field. Click the Status field to assign a status to the event. Event statuses are configured in the Object Statuses tab in the Object Management page. If none are configured, this field is not displayed.
Point of Contact	Optional field. Click the field to select the ThreatQ display name of the point of contact for the event.

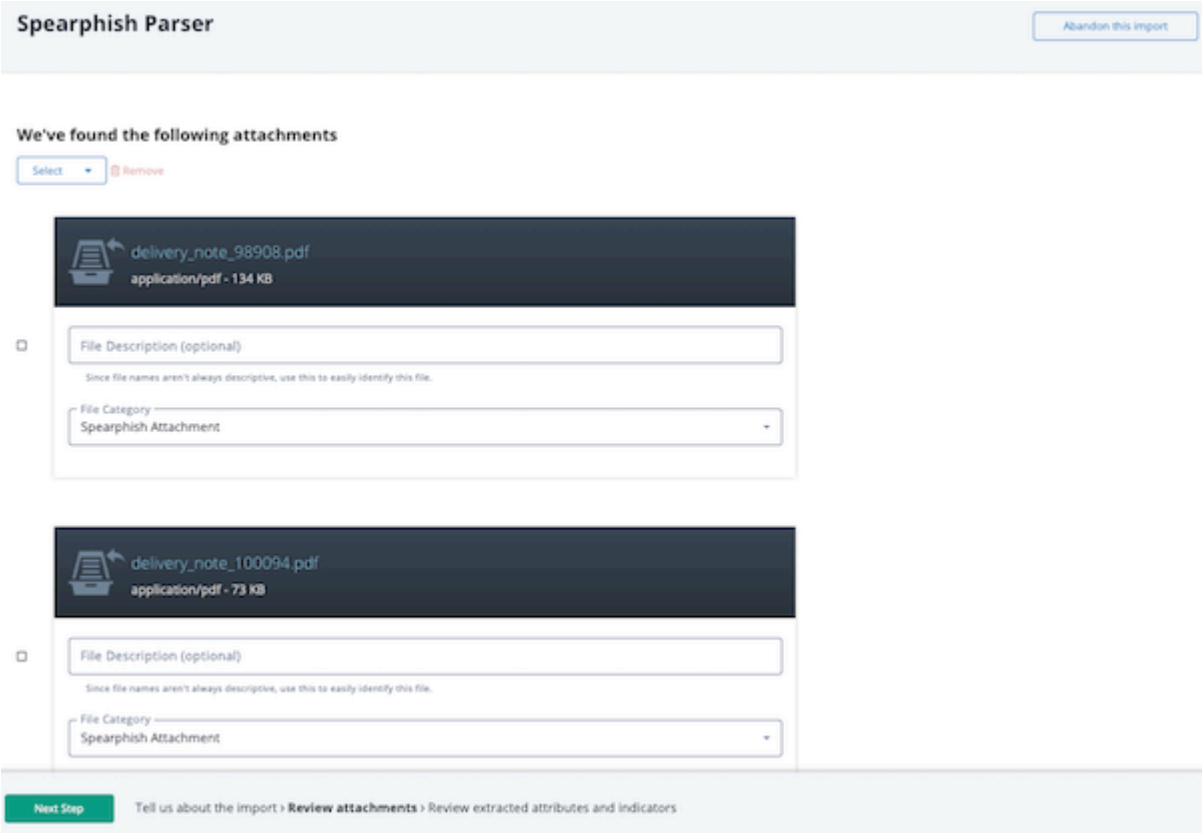
3. Use one of the following methods to upload the file to be parsed:
   - Drag the file to the window.
   - Click the click to browse link to access your File Finder/File Explorer and select the file.
   - Paste the email content into the text box on the right.
4. Select any **Related Objects** you need to link to the event. This field is optional.

5. Click **Add Event**.
   The Spearphish Parser page is displayed.

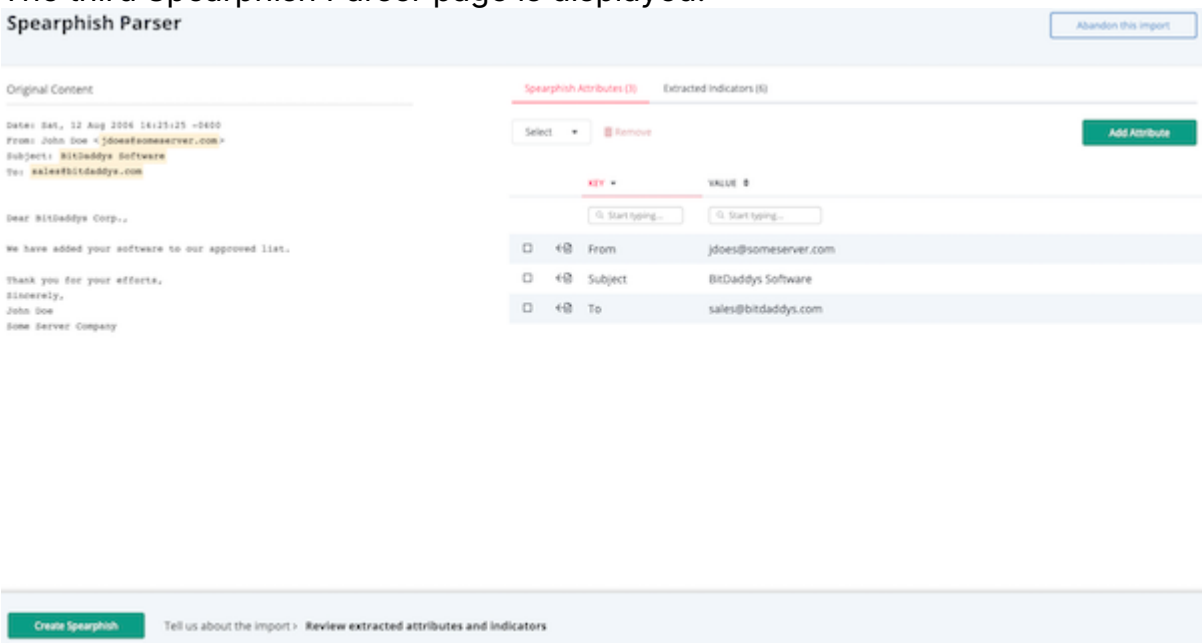


6. The Spearphish Parser page consists of three sections that allow you to review and update the following information:
   - **Spearphish Information** - Allows you to review and update the event information extracted from the file you uploaded.
   - **Extracted Indicators** - Allows you to specify the status and attributes to be applied to all extracted indicators.
   - **Add Relationships** - Allows you to add relationships to the spearphish event and any other extracted object.
7. Click the **Next Step** button.
   The second Spearphish Parser screen displays any attachments associated with the imported email. You can import these attachments or remove them from the import by checking the checkbox to the left of the attachment and clicking the Remove option.

If the imported email did not include attachments, ThreatQ bypasses this screen and takes you directly to the third Spearphish Parser page.



8. Click the **Next Step** button.
   The third Spearphish Parser page is displayed.



9. The third Spearphish Parser page allows you to review the attributes and indicators to be imported. From this page, you can:
    - **Add/remove an attribute** - From the Spearphish Attributes tab, click the **Add Attribute** button and enter the attribute details in the Add Attribute window. To remove an attribute, check the checkbox located to the left of the attribute key. Then, click the **Remove** option.
    - **Add/remove an indicator** - From the Extracted Indicators tab, click the **Add Indicator** button and enter the indicator details in the Add Indicator window. To remove an indicator, check the checkbox located to the left of the indicator value. Then, click the **Remove** option.
    - **Add information to an indicator** - Check the checkbox located to the left of the indicator you want to update. Then, click the Add Info option to access the Add Info window. Enter your changes in the Set Status or Add Comment tab and click the **Add Attributes** button.
10. Click the **Create Spearphish** button.
    The spearphish event is ingested into the Threat Library.

Exploit Targets

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor

Custom Role:

- Action Permissions: Objects & Context - Objects (all object types) **OR** Data Access Permissions: Exploit Target
- Action Permissions: Individual Object Context & Actions
  Note: If a user has View Only permission for Sources, system object creation modals default to the user's login as the object source.

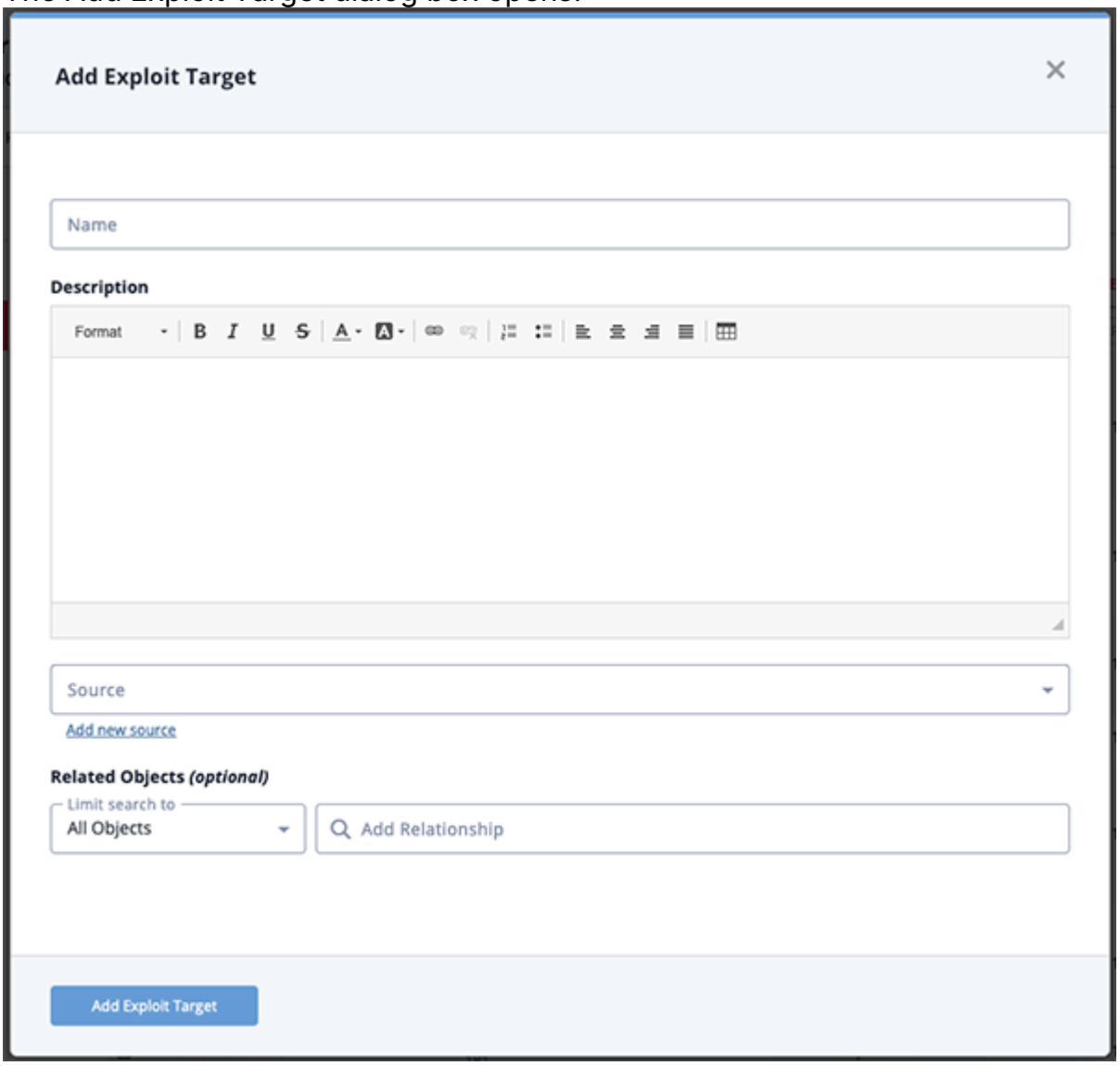
An Exploit Target is an identified vulnerability in a system, software, or network that can be targeted by tactics, techniques, and procedures (TTP).

Use the steps below to create, edit and delete an Exploit Target.

Adding a Exploit Target

1. Go to **Create > Exploit Target**.

The Add Exploit Target 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 Exploit Target. This field is optional.

6. Click **Add Exploit Target**.

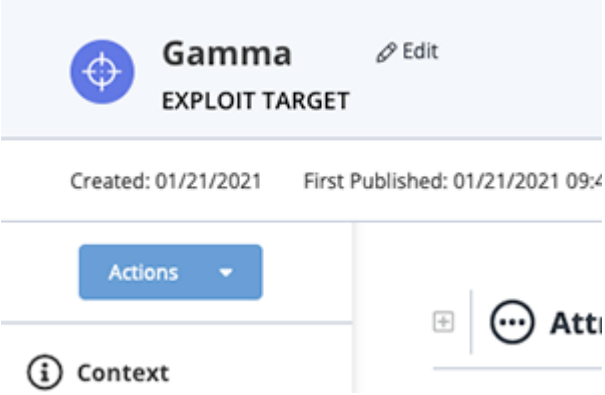
Adding Context

See the About Object Details Page section and its topics for details on adding context to an object such as adding sources, attributes, and related objects.

Editing a Exploit Target

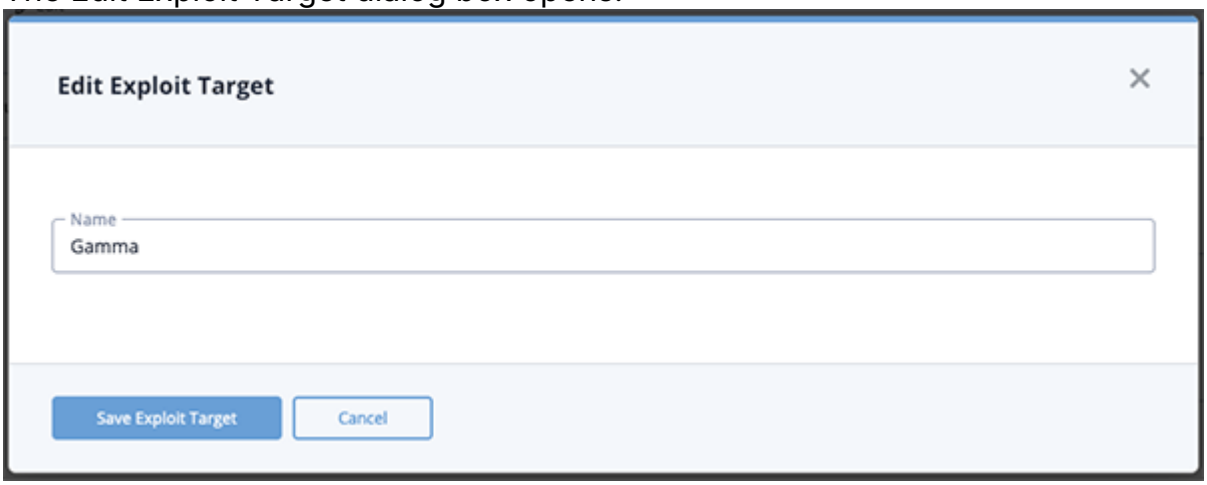
1. Locate and click on the Exploit Action.

   The Exploit Target's detail page opens.



2. Click on **Edit** next to the Exploit Target's name.

   The Edit Exploit Target dialog box opens.

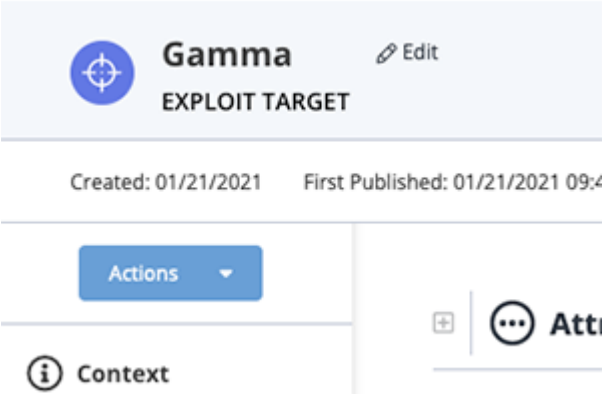


3. Make the desired change to the Exploit Target's name and click **Save Exploit Target**.

Deleting a Exploit Target

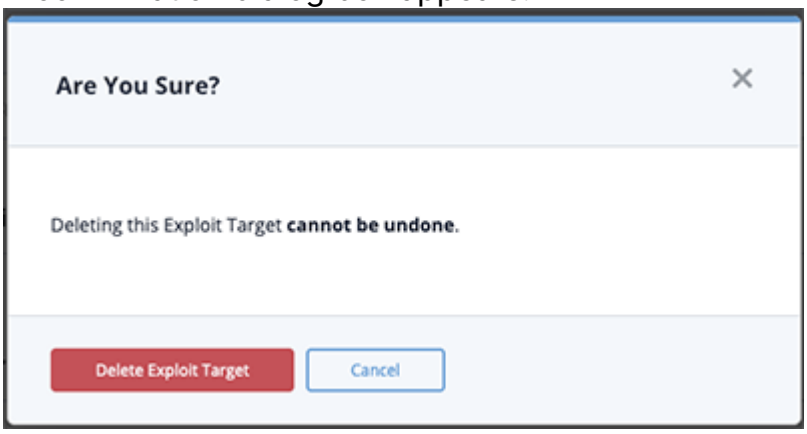
1. Locate and click on the Exploit Target.

The Exploit Target's details page opens.



2. Click on the **Actions** menu and select **Delete Course of Action**.

   A confirmation dialog box appears.



3. Click on **Delete Course of Action**.

Files

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor

Custom Role:

- Action Permissions: Objects & Context - Objects (all object types) **OR** Data Access Permissions: Course of Action
- Action Permissions: Individual Object Context & Actions
  Note: If a user has View Only permission for Sources, system object creation modals default to the user's login as the object source.

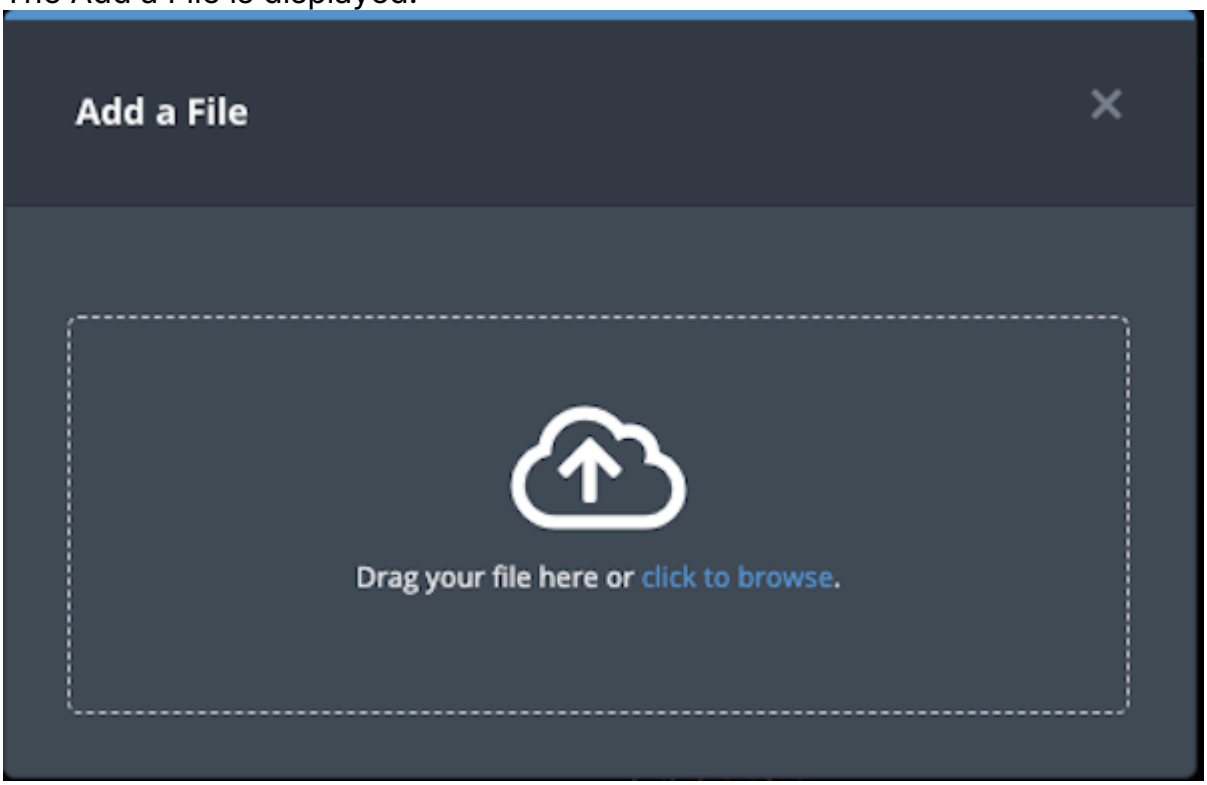
Files are received from various intelligence providers and may contain technical cybersecurity data such as Indicators, Adversaries, and Malware samples.

Use the steps below to create, edit and delete a File.

Adding Files

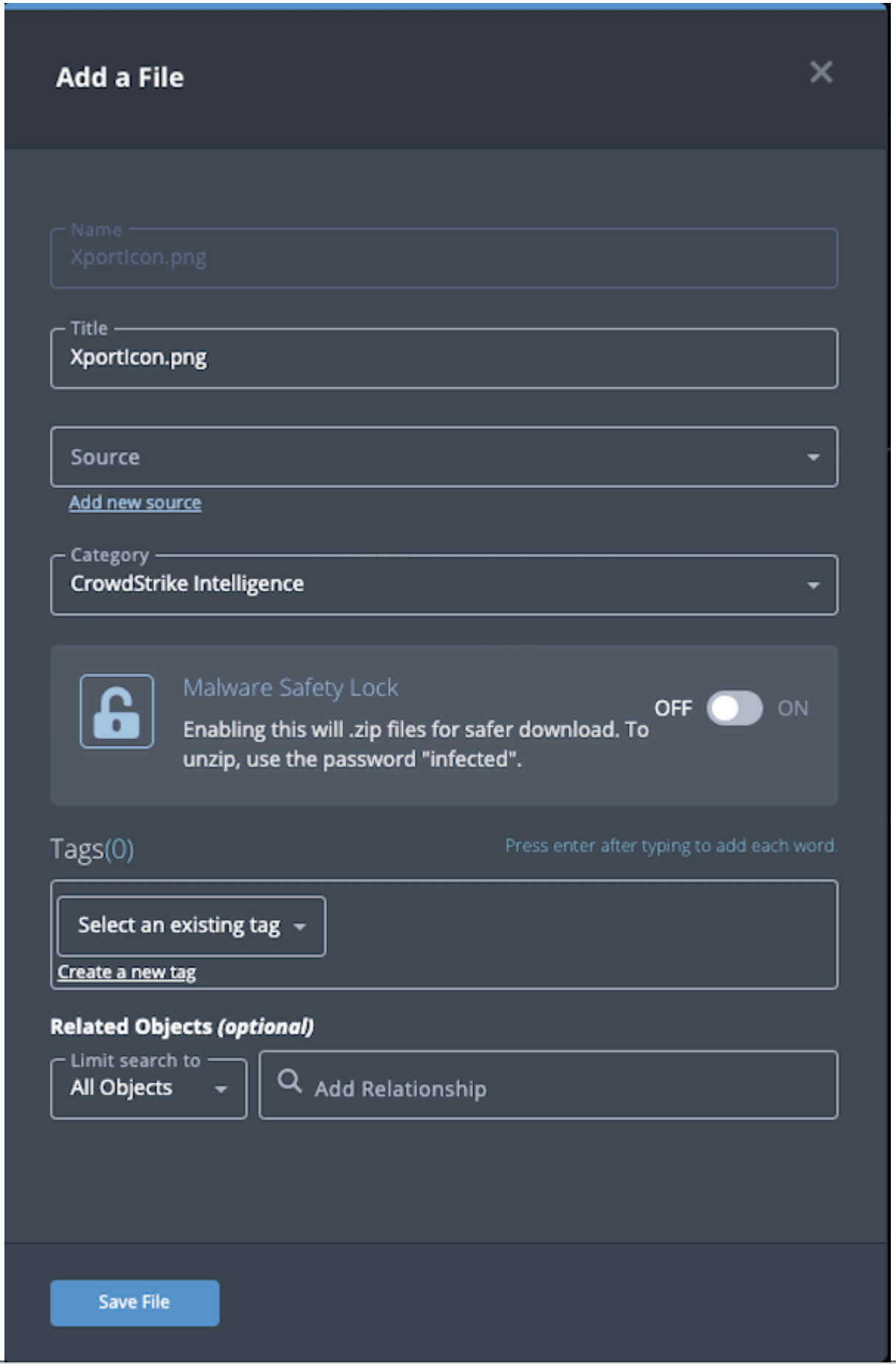
1. Click **Create > File**.

   The Add a File is displayed.



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

The Add a File window displays additional fields.


Add a File
Name
XportIcon.png
Title
XportIcon.png
Source
Add new source
Category
CrowdStrike Intelligence
Malware Safety Lock
Enabling this will .zip files for safer download. To unzip, use the password "infected".
OFF
ON
Tags(0)
Press enter after typing to add each word.
Select an existing tag
Create a new tag
Related Objects (optional)
Limit search to
All Objects
Add Relationship
Save File

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**.

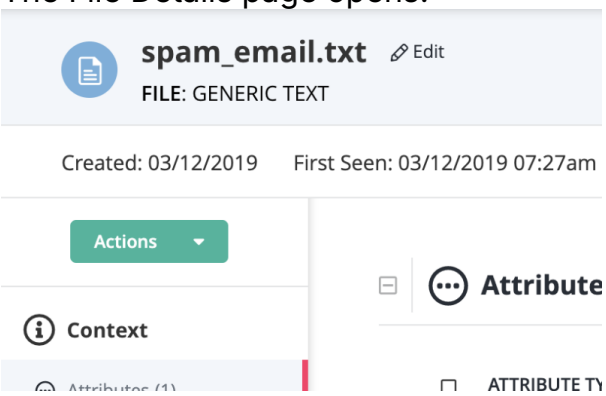
Adding Context

See the About Object Details Page 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.

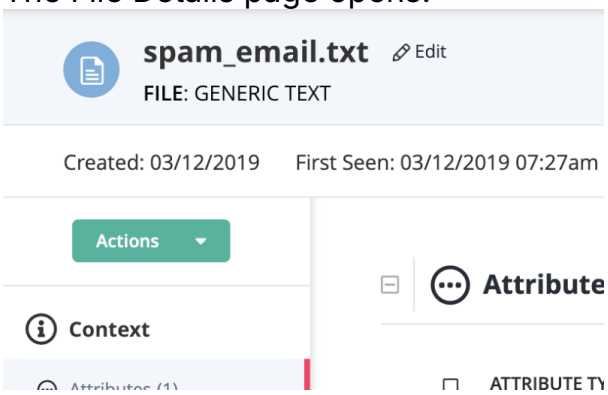
The Edit File dialog box opens.

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

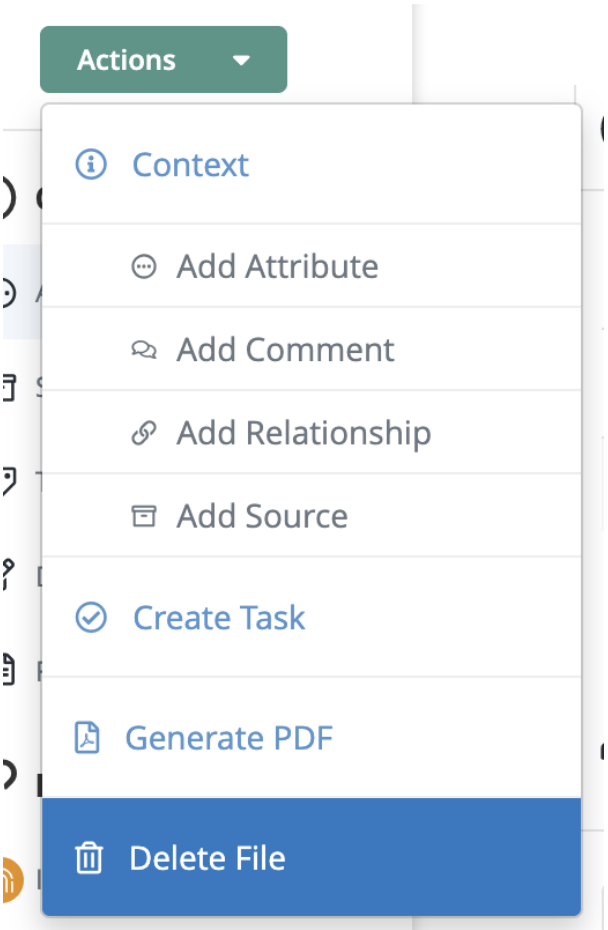
Deleting Files

1. Locate and click on the file.

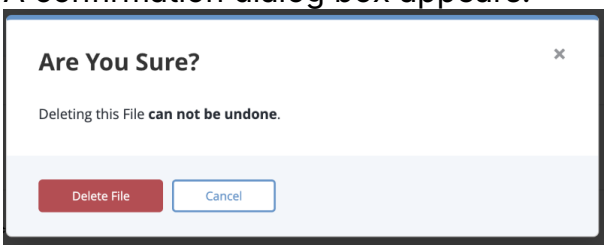
   The File Details page opens.



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



A confirmation dialog box appears.



3. Click on **Delete File.**

Identities

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor

Custom Role:

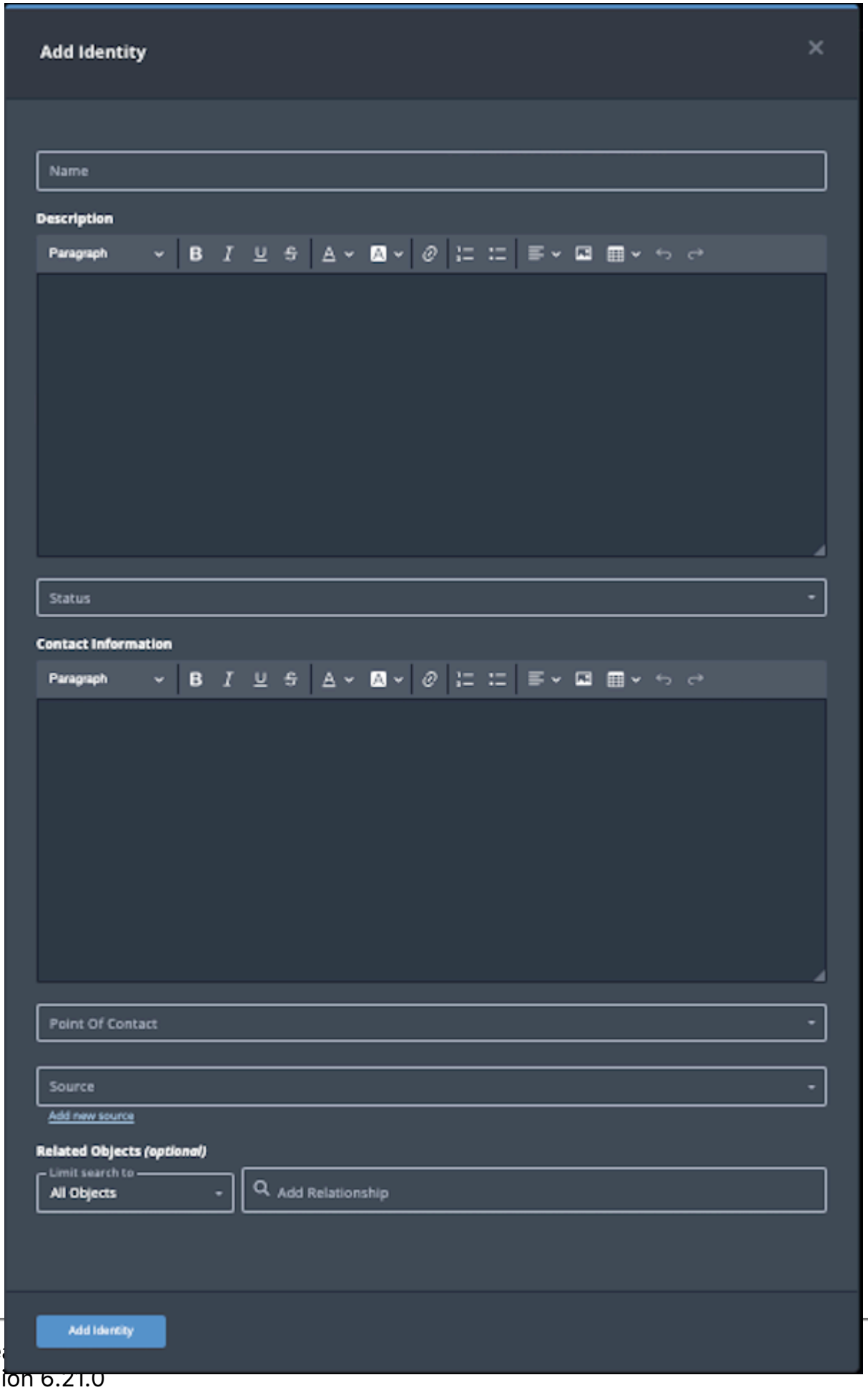
- Action Permissions: Objects & Context - Objects (all object types) **OR** Data Access Permissions: Identity
- Action Permissions: Individual Object Context & Actions
  Note: If a user has View Only permission for Sources, system object creation modals default to the user's login as the object source.

An Identity contains 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 window is displayed.


Add Identity
Name
Description
Paragraph
Status
Contact Information
Paragraph
Point Of Contact
Source
Add new source
Related Objects (optional)
Limit search to
All Objects
Add Relationship
Add Identity

2. Populate the following fields:

FIELD	DESCRIPTION
Name	Add an identity name.
Description	Add a brief description of the identity object.
Status	Optional field. Click the Status field to assign a status to the identity. Indentity statuses are configured in the Object Statuses tab in the Object Management page. If none are configured, this field is not displayed.
Contact Information	Enter any contact information for the identity.
Point of Contact	Optional field. Click the field to select the ThreatQ display name of the point of contact for the identity.
Source	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.

3. Select any **Related Objects** you need to link to the Identity. This field is optional.
4. Click the **Add Identity** button.

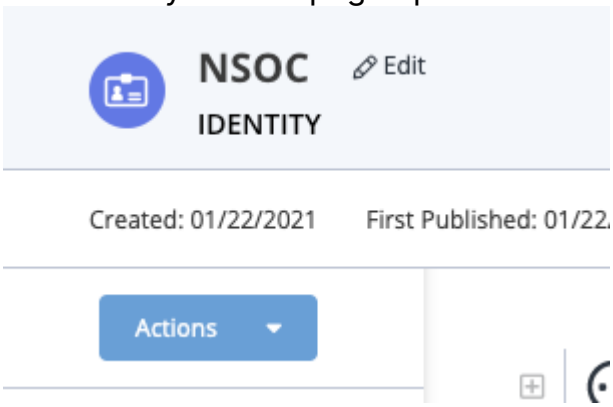
Adding Context

See the About Object Details Page section and its topics for details on adding context to an object such as adding sources, attributes, and related objects.

Editing an Identity

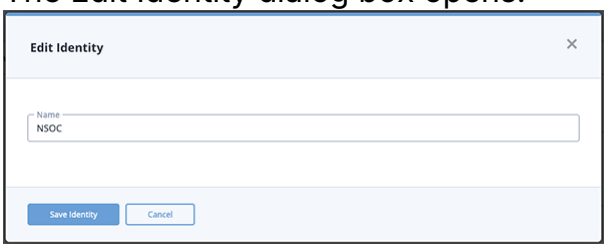
1. Locate and click on the Identity.

The Identity's detail page opens.



2. Click on **Edit** next to the Identity's name.

   The Edit Identity dialog box opens.



3. Make the desired change to the Identity's name and click **Save Identity**.

Changing the Point of Contact

THREATQ REQUIRED PERMISSIONS

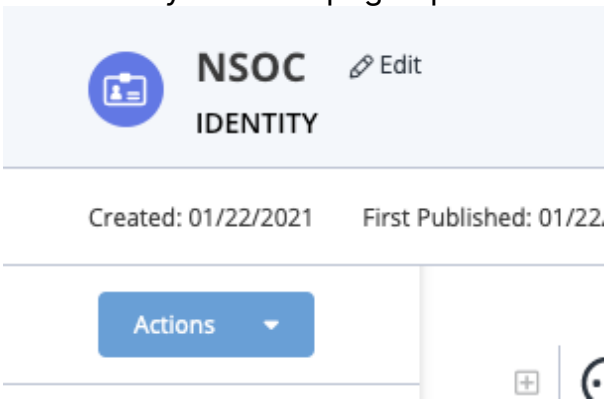
Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role - Action Permissions: Objects & Context - Objects, Individual Object Context & Actions - Point of Contact

1. Locate and click the system object.
2. From the object details page, click the Point of Contact field.
3. Use the field's scroll or search option to locate and select a new user as the object's point of contact or to change the point of contact to Unassigned.

Deleting an Identity

1. Locate and click on the Identity.

The Identity's details page opens.



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

   A confirmation dialog box appears.

3. Click on **Delete Identity**.

Incidents

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor

Custom Role:

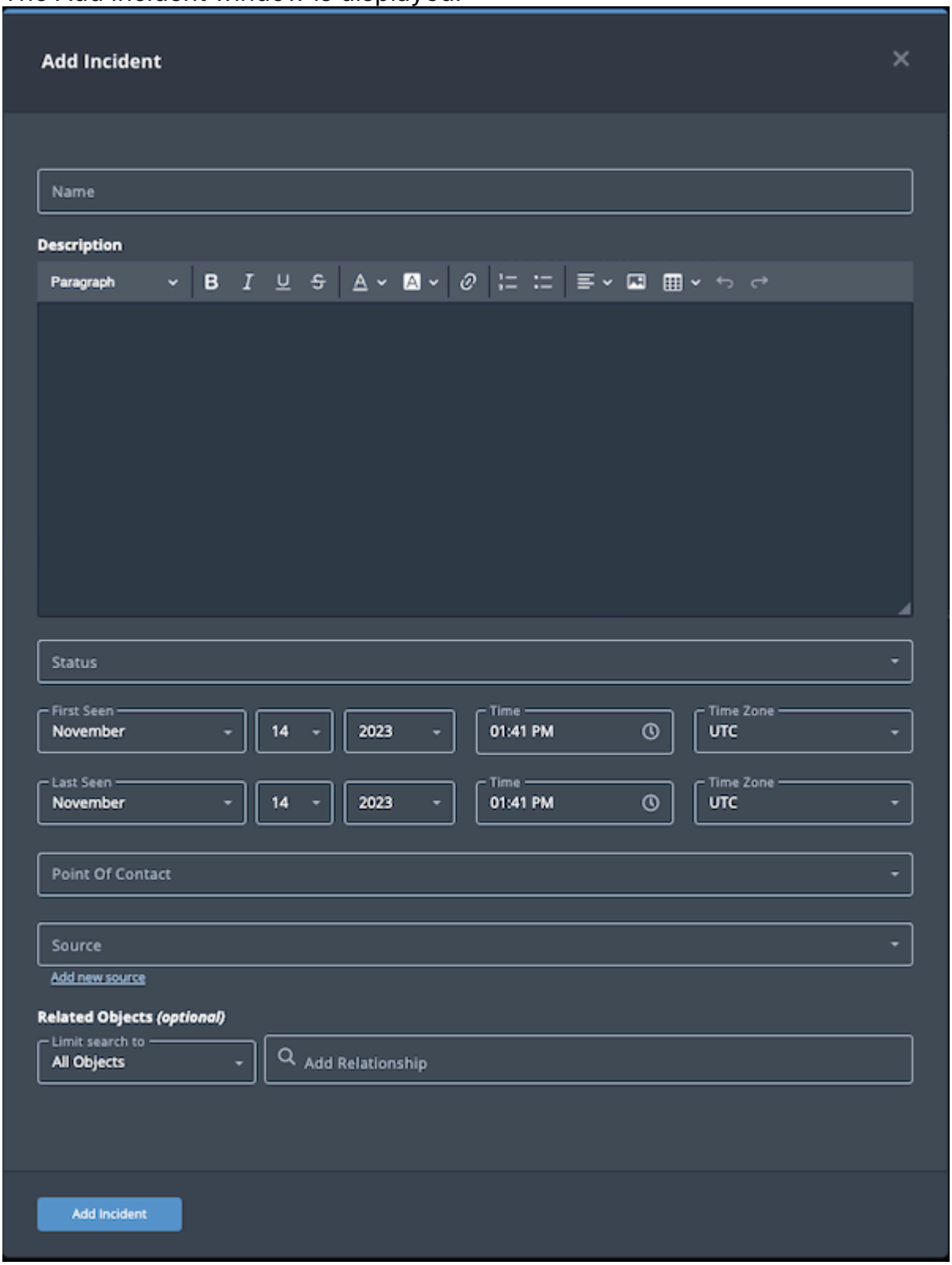
- Action Permissions: Objects & Context - Objects (all object types) **OR** Data Access Permissions: Incident
- Action Permissions: Individual Object Context & Actions
  Note: If a user has View Only permission for Sources, system object creation modals default to the user's login as the object source.

Incidents are records of any violation of an organization's established security/network policy that may compromise security, integrity, or general access.

Use the steps below to create, edit and delete an Incident.

Adding an Incident

1. Go to **Create > Incident**.
   The Add Incident window is displayed.



2. Populate the following fields:

FIELD	DESCRIPTION
Name	Add an incident name.
Description	Enter a brief description of the incident. Any description you add during object creation defaults to a Source value of ThreatQ System.
Status	Optional field. Click the Status field to assign a status to the status object. Incident statuses are configured in the Object Statuses tab in the Object Management page. If none are configured, this field is not displayed.
First Seen/ Last Seen	Select the first and last seen dates and times.
Point of Contact	Optional field. Click the field to select the ThreatQ display name of the point of contact for the incident.
Source	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.

3. Select any **Related Objects** you need to link to the Incident. This field is optional.
4. Click **Add Incident**.

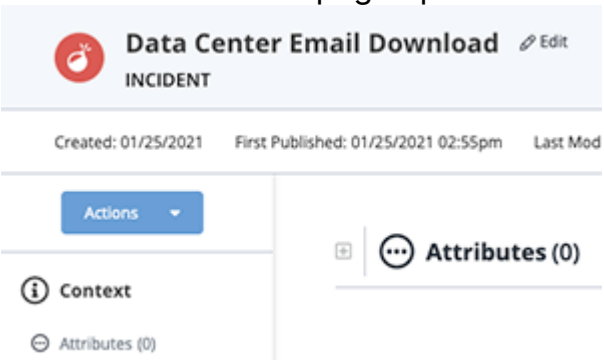
Adding Context

See the About Object Details Page section and its topics for details on adding context to an object such as adding sources, attributes, and related objects.

Editing an Incident

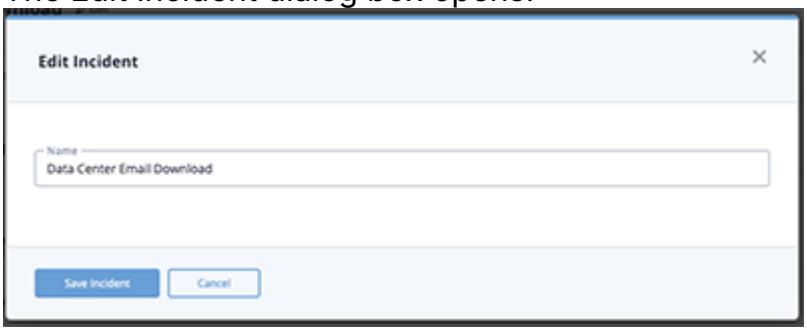
1. Locate and click on the Incident.

   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**.

Changing the Point of Contact

THREATQ REQUIRED PERMISSIONS

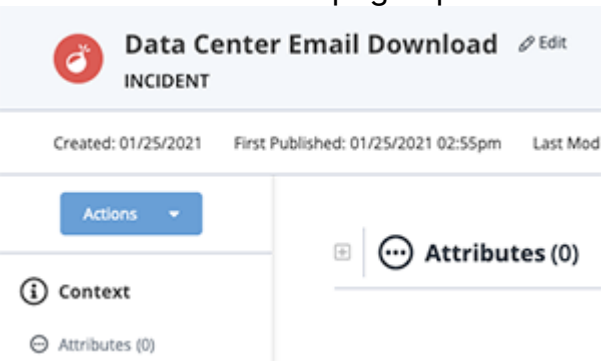
Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role - Action Permissions: Objects & Context - Objects, Individual Object Context & Actions - Point of Contact

1. Locate and click the system object.
2. From the object details page, click the Point of Contact field.
3. Use the field's scroll or search option to locate and select a new user as the object's point of contact or to change the point of contact to Unassigned.

Deleting an Incident

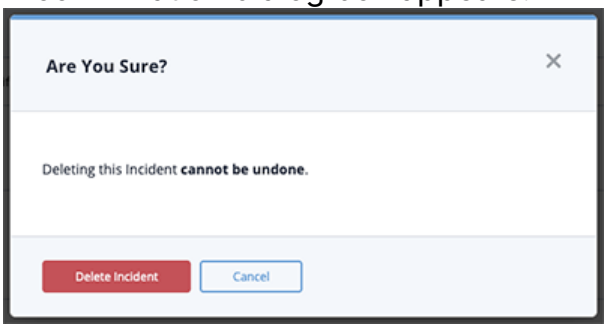
1. Locate and click on the Incident.

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

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role - Action Permissions: Objects & Context - Objects, Individual Object Context & Actions

Note: If a user has View Only permission for Sources, system object creation modals default to the user's login as the object source.

An Indicators 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.

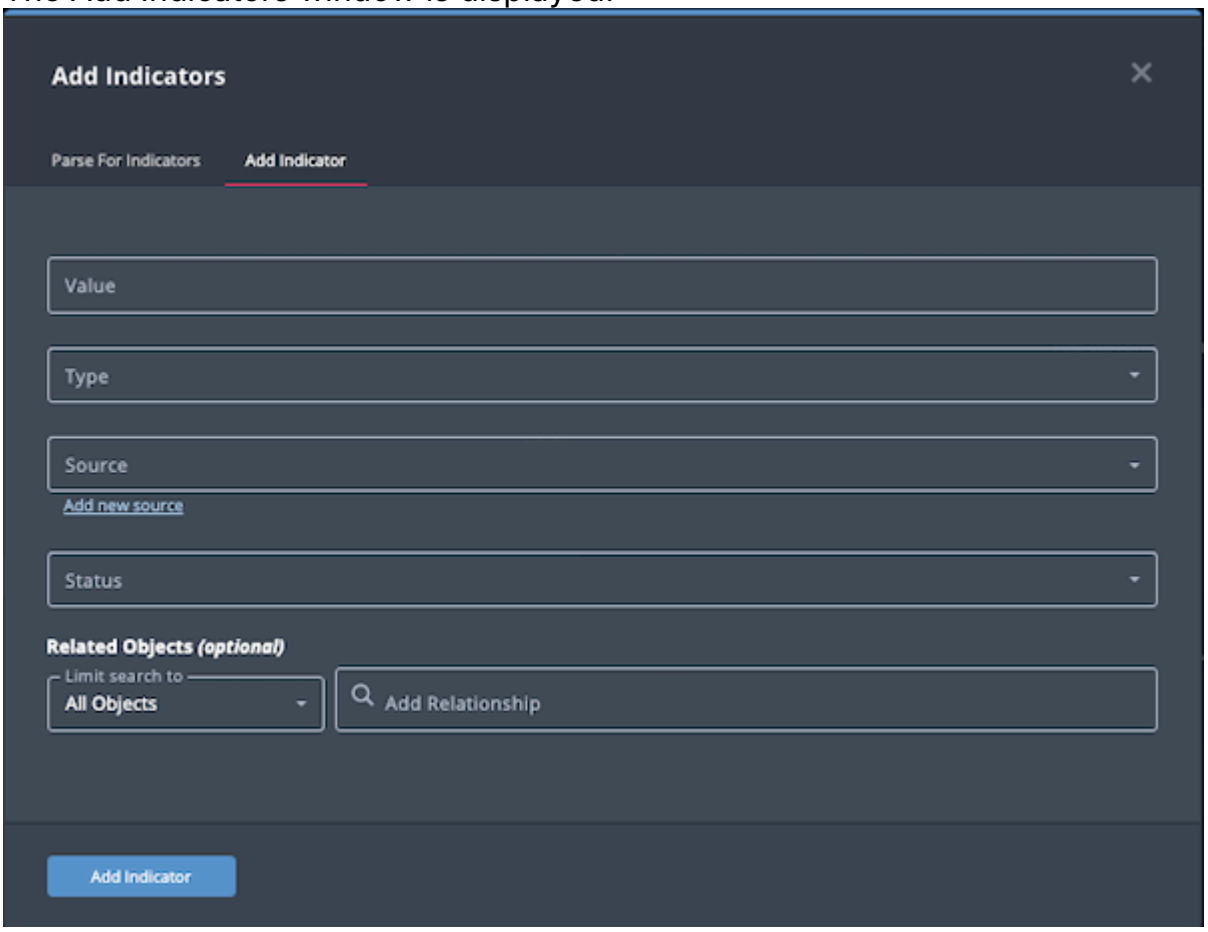
The ThreatQ platform performs validation on all indicators during both ingestion and parsing to ensure data quality and integrity. Indicators containing obvious formatting errors, such as email addresses missing an @ symbol, are automatically rejected. The platform also validates indicators against logical and technical standards; for example, IP addresses containing invalid byte values greater than 255 will fail validation.

In addition, ThreatQ does not support the ingestion of private internal network addresses defined by RFC1918, as these addresses are not considered meaningful or actionable indicators of compromise for threat intelligence sharing and tracking purposes.

Adding an Indicator

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

The Add Indicators window is displayed.



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**.

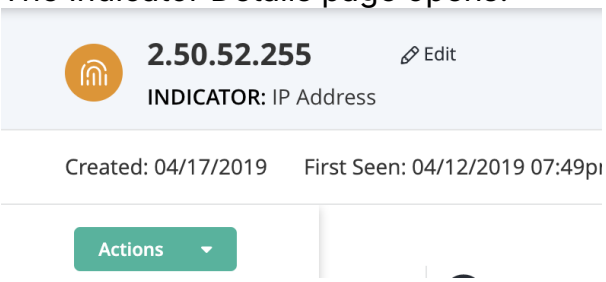
Adding Context

See the About Object Details Page section and its topics for details on adding context to an object such as adding sources, attributes, and related objects.

Editing Indicators

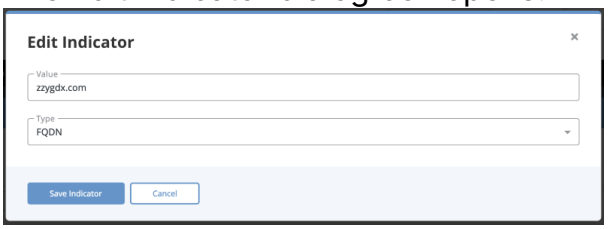
1. Locate and click on the indicator.

   The Indicator Details page opens.



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

   The Edit Indicator dialog box opens.

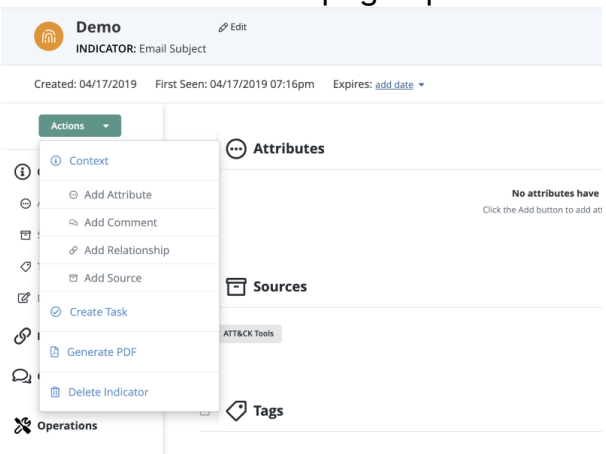


3. Make the desired change to the indicator **Value** and **Type**.
4. Click on **Save Indicator**.

Deleting an Indicator

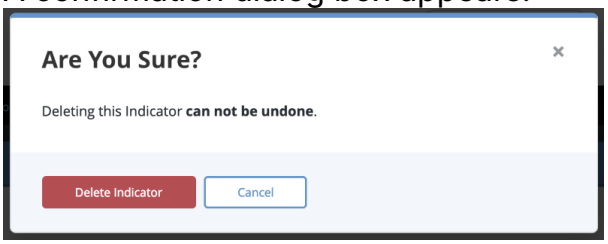
1. Locate and click on the Indicator.

   The Indicator Details page opens.



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

A confirmation dialog box appears.



3. Click on **Delete Indicator**.

Parsing for Indicators

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role - Action Permissions: Objects & Context - Perform Bulk Manual Import, Create, Edit, Delete Objects, Create, Edit, Delete Attributes,Create, Edit, Delete Relationships. See the Interdependent Permissions.

Notes:

- If a user's role has View Only permission for Sources, system object parsers default to the user's login as the object source.
- If a user's role does not include permission to Edit or delete an object's Status, system object parsers apply the default status to seeded system objects and the first status option for custom objects.

Custom Role - Data Access Permissions: Indicators

Note:: If an import contains object types or context you lack Create/Edit/Delete permission for, the import fails.

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.

Indicator Parsers and Permissions

In addition to permission to Perform Bulk Manual Import, users with custom roles must have permissions for the indicator context included in the files they parse. For example, if you use the ThreatQ CSV file parser to parse a file that includes indicator statuses, your role must have Perform Bulk Manual Import permission and Edit/Delete permissions for Status.

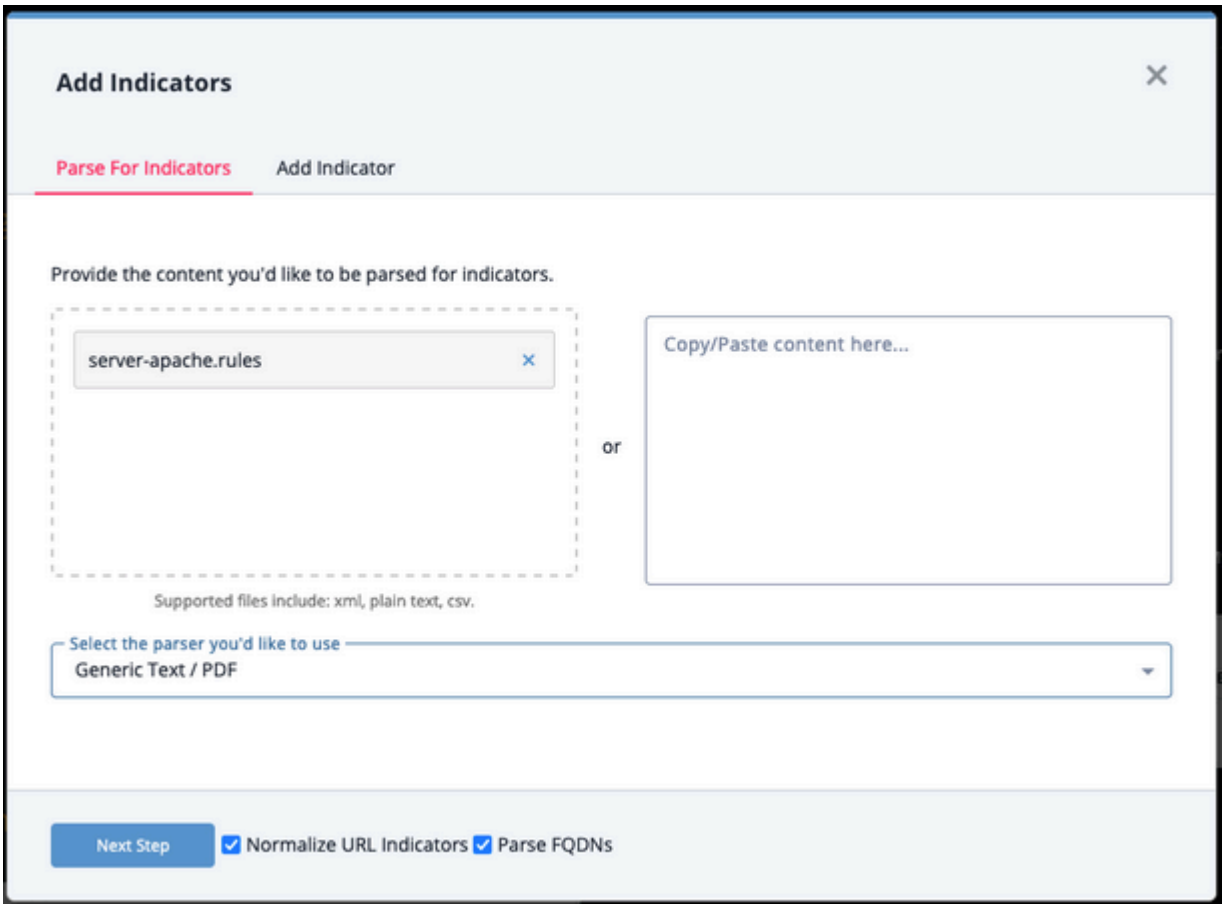
These permission requirements apply to all indicator parsers except ThreatQ's Generic Text/PDF parser. For this parser, ThreatQuotient requires that the parsed file only includes the indicator and its value. As such, no additional object context permissions are required.

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
   - Trellix Analysis
   - Generic Text / PDF - These files must contain only Indicators and their values.
   - Palo Alto Networks WildFire XML
   - ThreatAnalyzer Analysis
   - ThreatQ CSV File - see the Importing Indicators via CSV topic for specific instructions on using this parser.

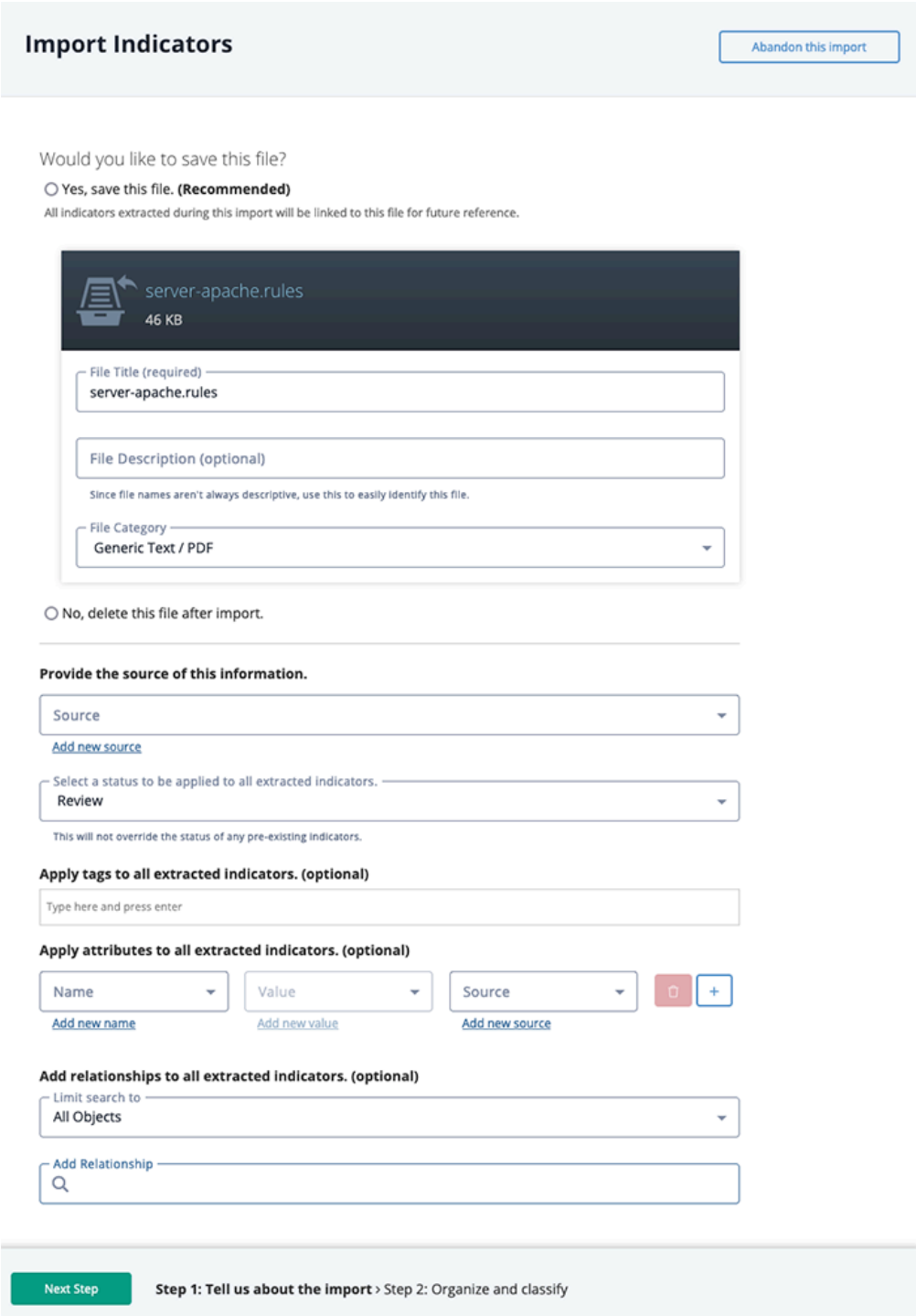
4. Use the checkboxes to select your parsing options:

OPTION	DESCRIPTION
Normalize URL Indicators	When checked, parsed URLs will have ports and leading protocol adjusted, as well as unneeded quotes and spaces removed. Query strings will also be removed when URL normalization is enabled. See the Indicator URL Normalization topic for more details.
Parse FQDNs	When checked, the Indicator Parser will parse FQDNs from the text and derive FQDN indicators from URLs in the text. **Example (checked)**: URL: https://tqexample.com/table.jspa?query_string_example Indicators created: ◦ tqexample.com/table.jspa (the URL) ◦ tqexample.com (the derived FQDN from the URL) When unchecked, the Indicator Parser will not generate FQDN indicators from the parsed text. **Example (unchecked)**: URL: https://tqexample.com/table.jspa?query_string_example Indicator created: ◦ tqexample.com/table.jspa (the URL)

Administrators can configure the default setting for these options under the General Tab on the System Configurations page. See the Indicator Parsing Presets topic for more details.

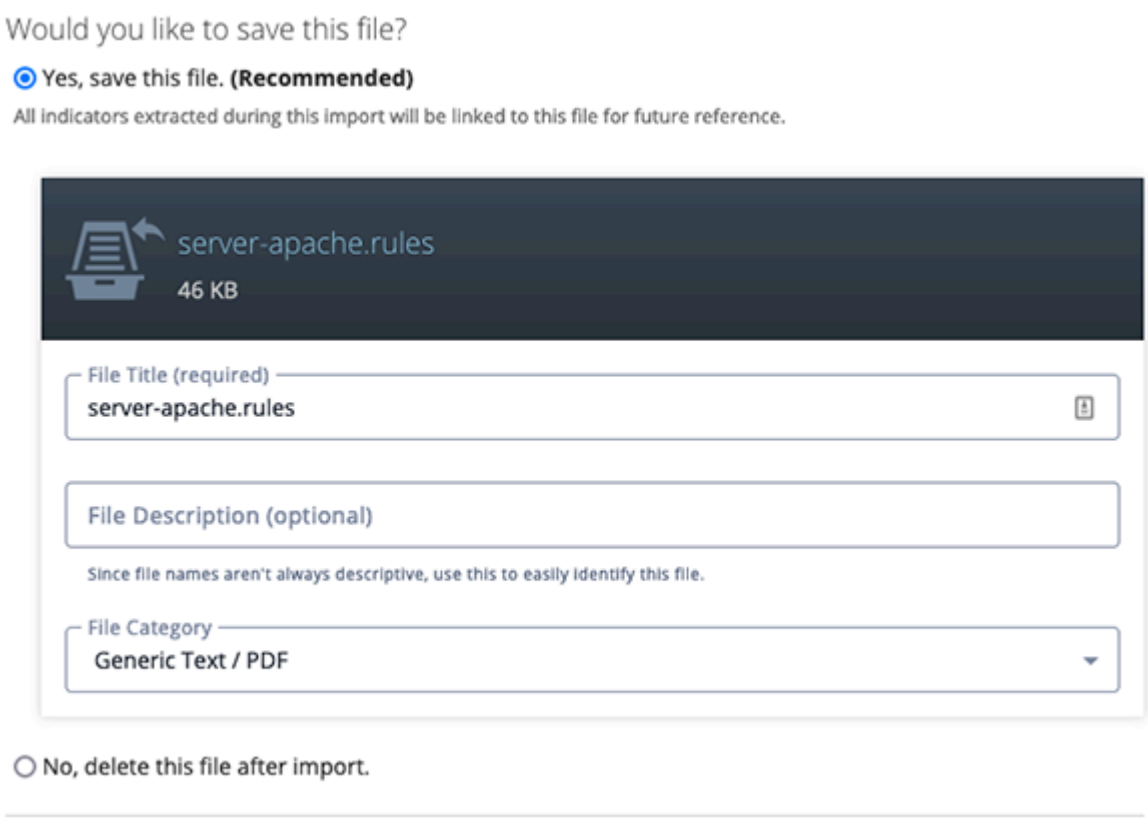
5. Click on **Next Step**.

   The Step 1 - Import Indicators form will load.

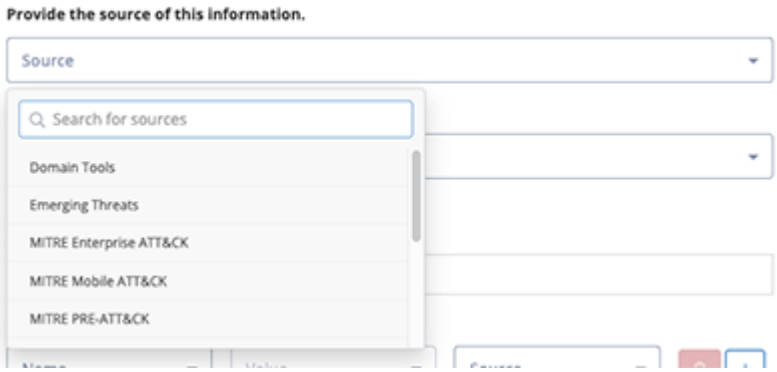


Step 1 - Import Indicators Settings

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**.



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.



8. Select a **Status** for the extracted indicators.

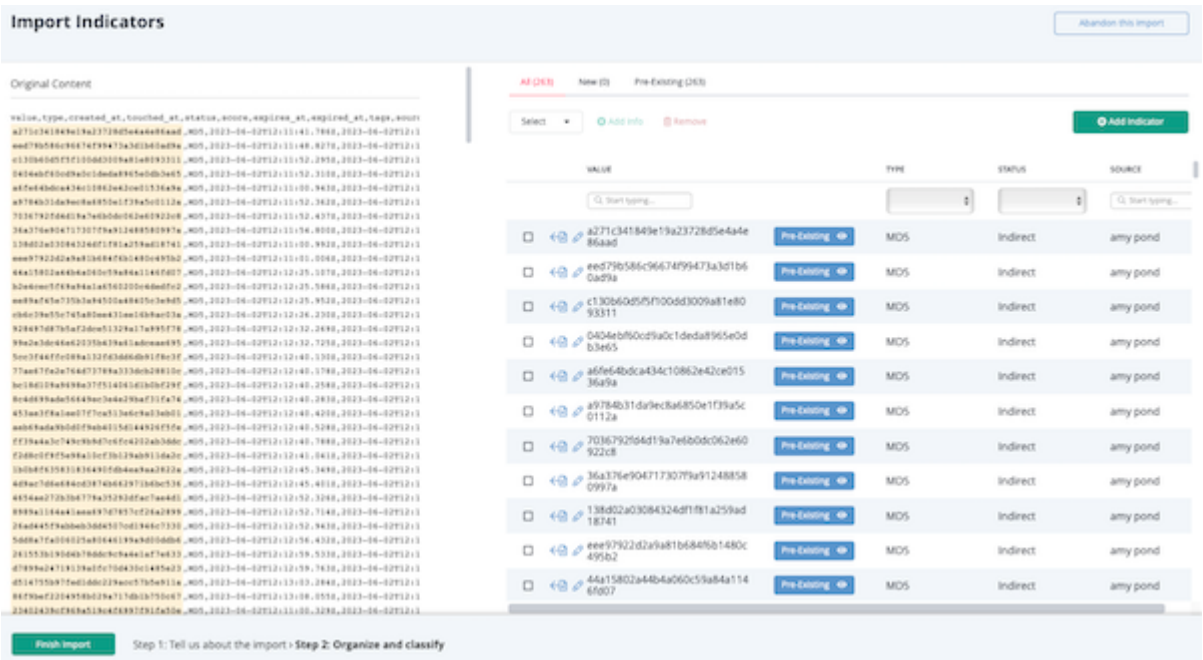
9. Enter any **Tags** to apply to the extracted indicators. This field is optional.

10. Select any attribute, attribute value, and attribute source to apply to the extracted indicators.
11. Add **Relationships** for the extracted indicators.

> If you enter an object name that is not found, you can click the **Create** link to add the new object. If you limited your search to a specific object type, you are linked to the corresponding form. For example, if you limit your search to Adversaries, the **Create** link opens the Add An Adversary form. If you leave the **Limit search to** field set to All Objects, you can select the object type you want to create from a drop-down list.

12. Click on **Next Step**.

    The Organize and Classify form will load.

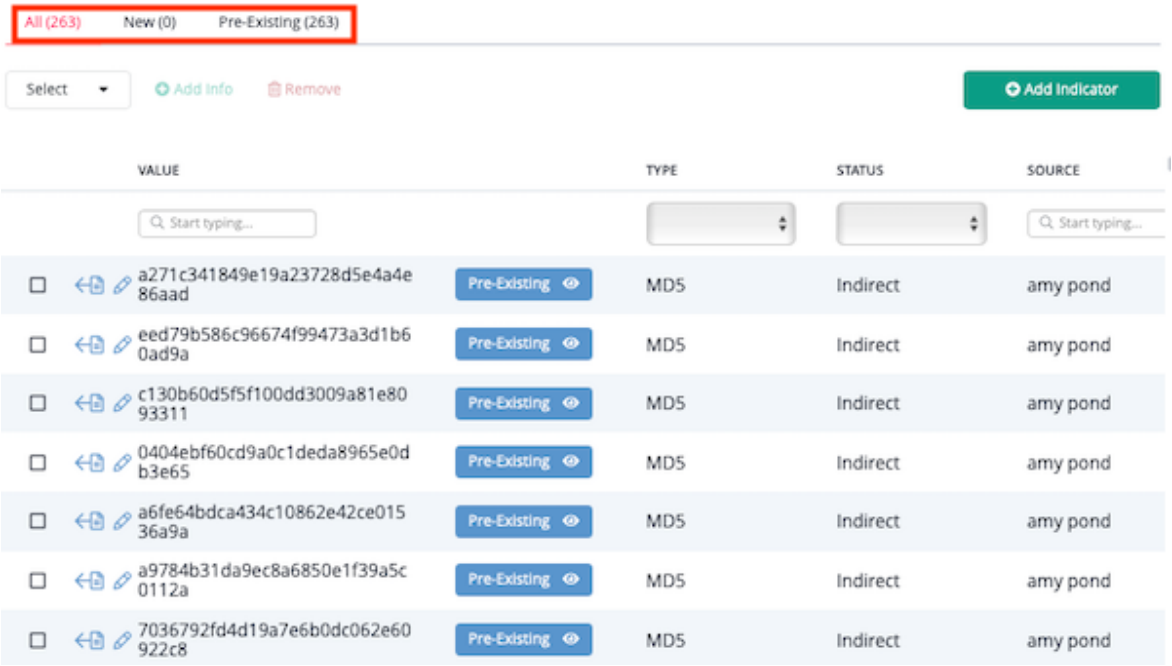


Step 2 - Organize and Classify

13. You can review the original content of the file and the extracted indicators' information.

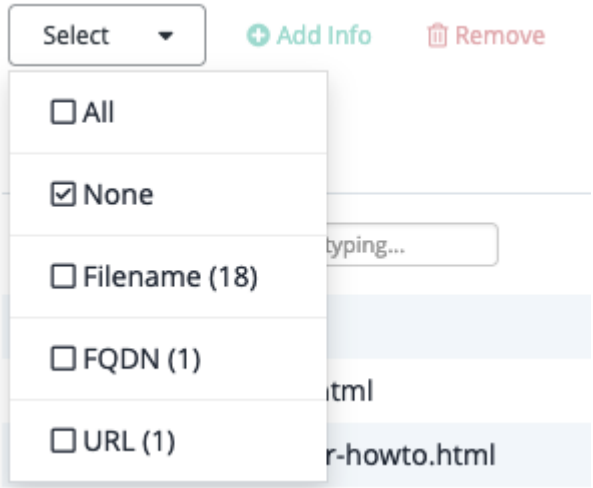
    ### Filtering Extracted Indicators List

    - The top tabs allow you to filter the list of indicators by New and Pre-existing. This allows you to isolate any indicators that already exist in the platform.



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.

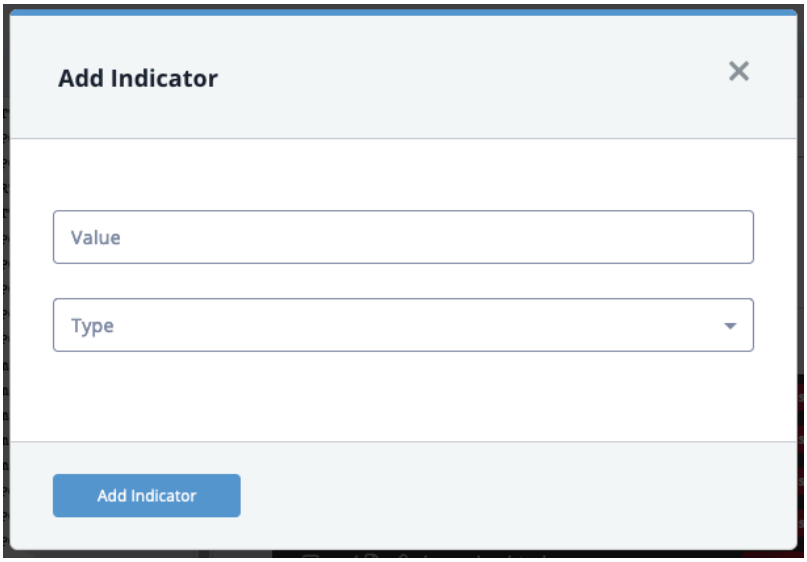
- You can click on the **Select** dropdown to automatically select indicators by sub-type.



> ⚠ Selecting **All** will select all extracted indicators, not just the ones in your current filtered view (New, Pre-Existing).

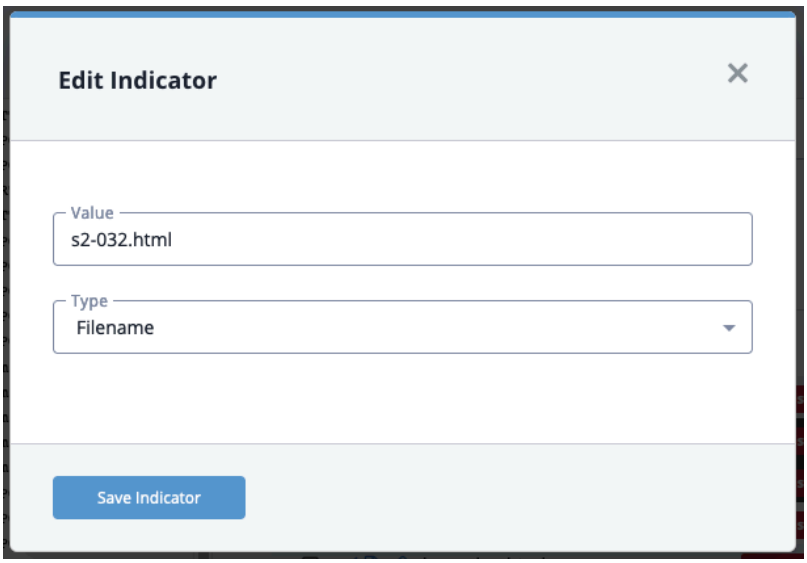
Adding Indicators

- You can click on the **Add Indicator** option, located to the top-right of the list, to add an indicator to the extracted list. You can add further context to the new indicator using the Editing Extracted Indicators actions listed below.



Editing Extracted Indicators

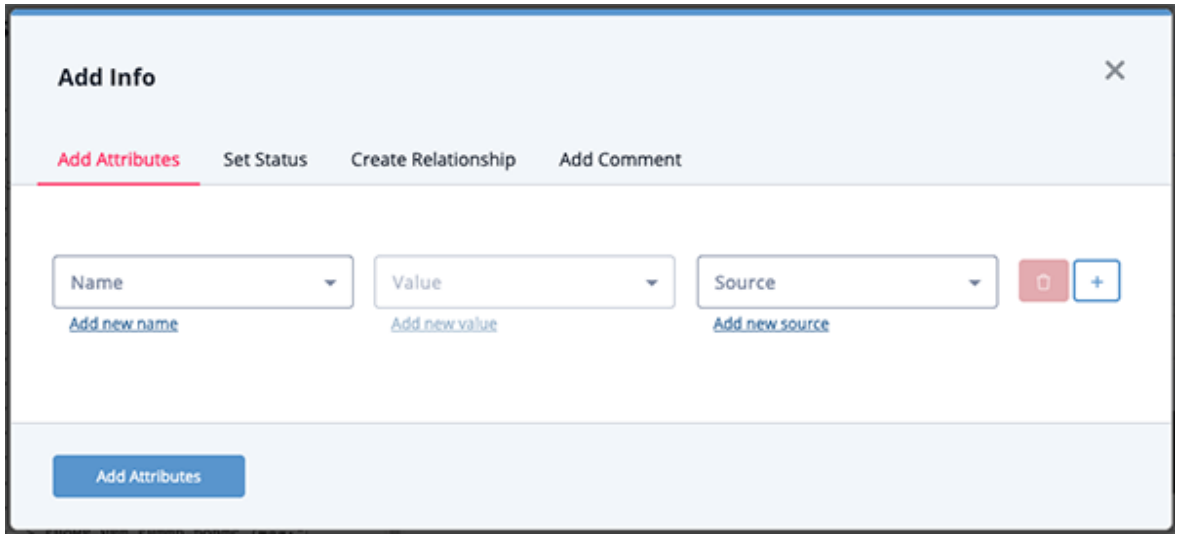
- Clicking on the icon will show you where the indicator appeared in the Original Content window.
- Clicking on the icon will open the **Edit Indicator** dialog box and allow you to edit the indicator value and indicator sub-type.



- Selecting one or more indicators and clicking on **Add Info** option allows you to perform the following actions:

ACTION	DETAILS

ACTION	DETAILS
Add Attribute	You can add an attribute to one or more extracted indicators. Select the checkbox next to the indicator(s) to update and then click on the **Add Info** option. The Add Attributes tab will be selected by default. Select an **Attribute Name**, **Value**, and **Source** to apply to the selected indicator(s).
Set/Update Status	You can update the status of one or more extracted indicators. Select the checkbox next to the indicator(s) to update and then click on the **Add Info** option. Click on the **Set Status** tab and select your new status.
Create Relationship	You can link one or more extracted indicators to another system object. Select the checkbox next to the indicator(s) to update and then click on the **Add Info** option. Click on the **Set Relationship** tab and set the relationship. When you add a relationship, it is displayed in the indicator list and you can click it to view its details in a preview panel. If the object you want to link is not found, you can 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

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role - Action Permissions: Objects & Context - Perform Bulk Manual Import, Create, Edit, Delete Objects, Create, Edit, Delete Attributes, Create, Edit, Delete Relationships. See the Interdependent Permissions topic.

Note: If a user has View Only permission for Sources, system object parsers default to the user's login as the object source.

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	Fradulant robocall
4	6c277b5ea26178c5	MD5	Review	USA	CA	
5	172.54.542.236	IP Address	Active	USA	CO	
6	39.38.116.53	IP Address	Active	USA	FL	

***Type**

This field identifies the indicator type.

ThreatQ requires that the Type column be included in the CSV file and that each entry have a value.

> You must use a type that already exists in your ThreatQ instance. If you are unable to provide an Indicator Type for each indicator, you can use the **Generic Text/ PDF** parsing option that attempta to identify indicator type values automatically.

Example

	A	B	C	D	E	F
1	Indicator	Type	Status	Attribute::Country	Attribute::State	Comments
2	trustme@refundszus.com	Email Address	Active	USA	MA	Phishing attempt
3	officer@irspolice.com	Email Address	Active	USA	MD	Fradulant robocall
4	6c277b5ea26178c5	MD5	Review	USA	CA	
5	172.54.542.236	IP Address	Active	USA	CO	
6	39.38.116.53	IP Address	Active	USA	FL	

***Status**

The Status column is required. You 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@refundszus.com	Email Address	Active	USA	MA	Phishing attempt
3	officer@irspolice.com	Email Address	Active	USA	MD	Fradulant robocall
4	6c277b5ea26178c5	MD5	Review	USA	CA	
5	172.54.542.236	IP Address	Active	USA	CO	
6	39.38.116.53	IP Address	Active	USA	FL	

Attribute

The Attribute columns are optional. You can apply one or more attributes to an indicator by adding an Attribute column.

Attribute keys are **case** and **space** sensitive, 'MalwareFamily' and 'malware family' will generate a separate key in ThreatQ. In order to map to an existing Attribute Key in ThreatQ, you must match 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.

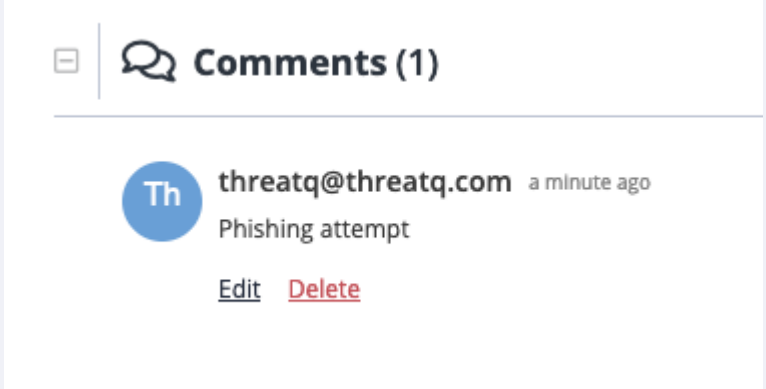
Example

	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	Fradulant robocall
4	6c277b5ea26178c5	MD5	Review	USA	CA	
5	172.54.542.236	IP Address	Active	USA	CO	
6	39.38.116.53	IP Address	Active	USA	FL	

Comments

The optional Comments 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.



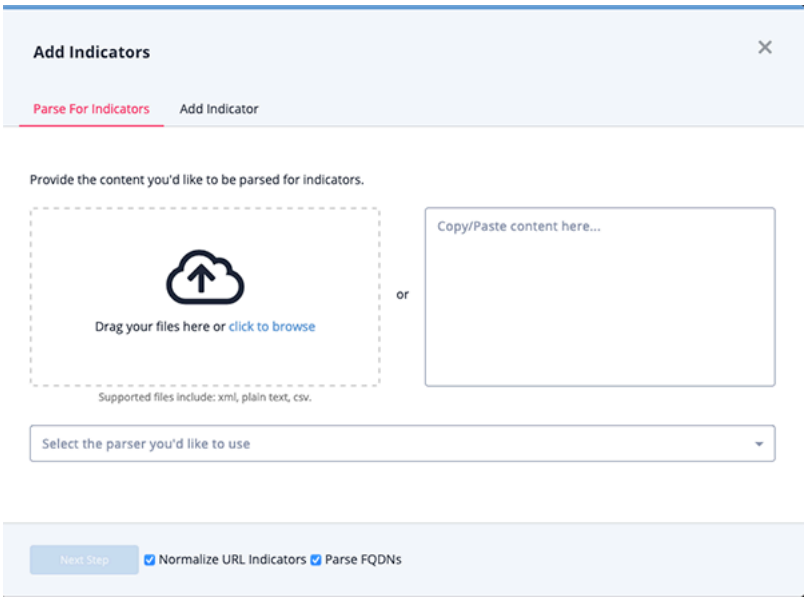
Example

	A	B	C	D	E	F
1	Indicator	Type	Status	Attribute::Country	Attribute::State	Comments
2	trustme@refundszus.com	Email Address	Active	USA	MA	Phishing attempt
3	officer@irspolice.com	Email Address	Active	USA	MD	Fradulant robocall
4	6c277b5ea26178c5	MD5	Review	USA	CA	
5	172.54.542.236	IP Address	Active	USA	CO	
6	39.38.116.53	IP Address	Active	USA	FL	

Parsing a ThreatQ CSV File and Adding Context

1. Click the **Create** button and select **Indicator Parser** under the *Import* heading.

   The Add Indicators dialog box opens with the Parse for Indicators tab selected.



2. Upload your CSV file by either:
   - Dragging and dropping your file into the window

- Clicking the Click to Browse option and uploading your file

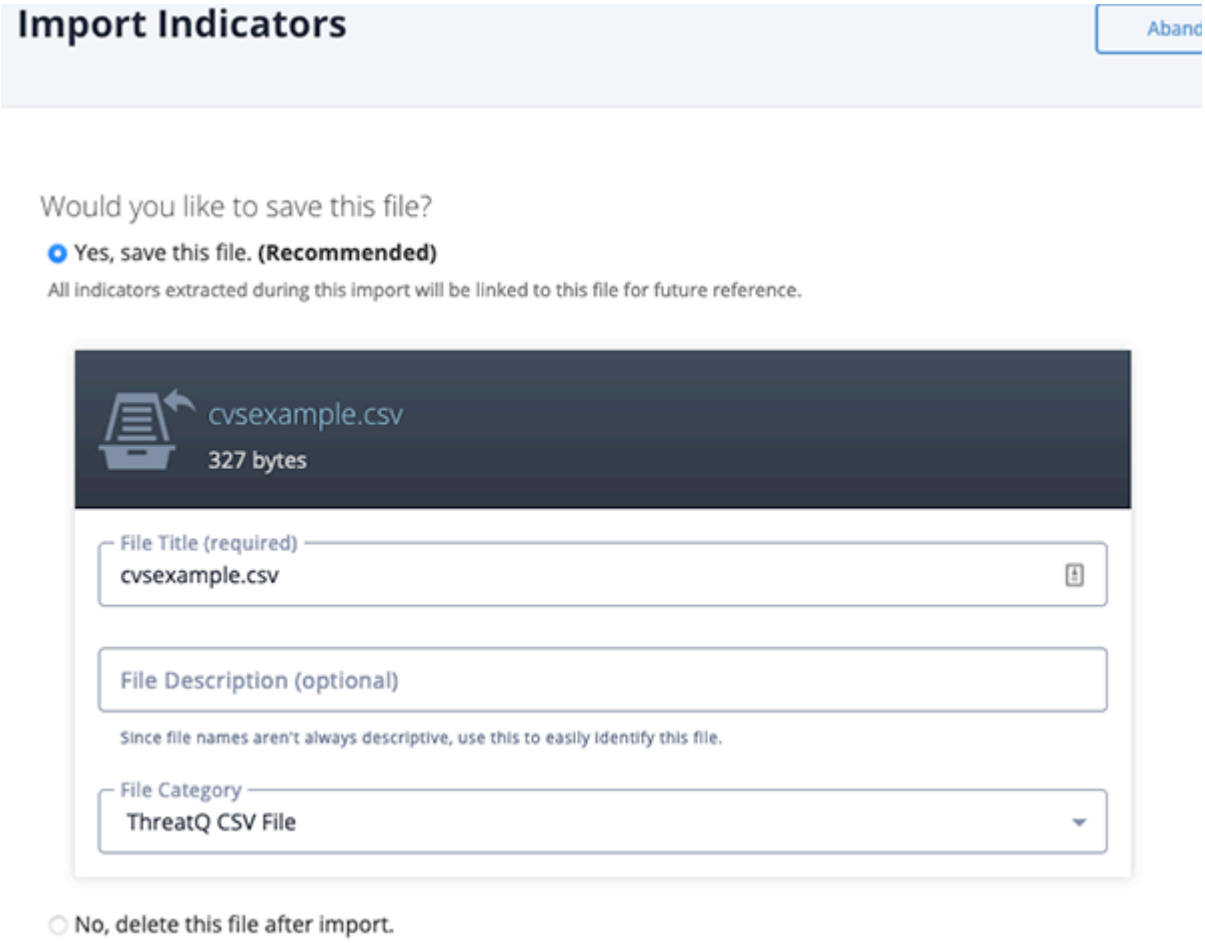
3. Select **ThreatQ CSV File** as the parser to use.
4. Use the checkboxes to select your parsing options:

OPTION	DESCRIPTION
Normalize URL Indicators	When checked, parsed URLs will have ports and leading protocol adjusted, as well as unneeded quotes and spaces removed. Query strings will also be removed when URL normalization is enabled. See the Indicator URL Normalization topic for more details.
Parse FQDNs	When checked, the Indicator Parser will parse FQDNs from the text and derive FQDN indicators from URLs in the text. **Example (checked)**: URL: https://tqexample.com/table.jspa?query_string_example Indicators created: ◦ tqexample.com/table.jspa (the URL) ◦ tqexample.com (the derived FQDN from the URL) When unchecked, the Indicator Parser will not generate FQDN indicators from the parsed text. **Example (unchecked)**: URL: https://tqexample.com/table.jspa?query_string_example Indicator created: ◦ tqexample.com/table.jspa (the URL)

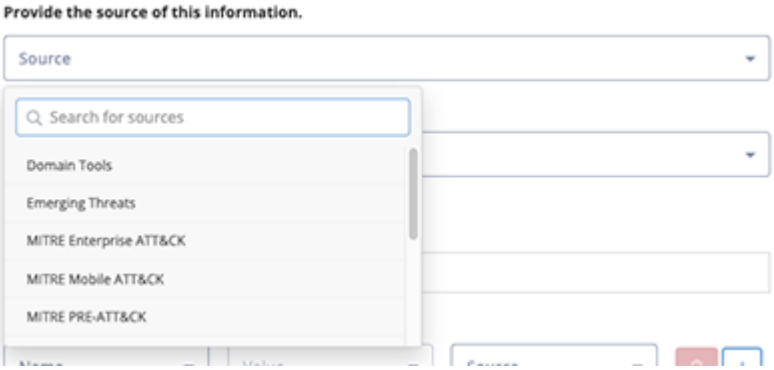
Administrators can configure the default setting for these options under the General Tab on the System Configurations page. See the Indicator Parsing Presets topic for more details.

5. Click **Next Step**.

6. Select whether or not to save the CSV file. Saving the file will result in all extracted indicators being linked to the file for reference.



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.



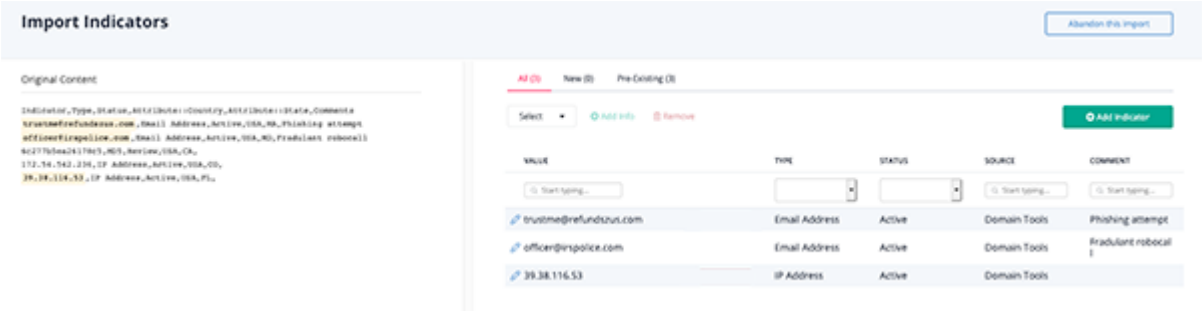
8. Select a **Status** for the extracted indicators. The indicator's Status value supplied in the CSV overrides this value.

9. Enter any **Tags** to apply to the extracted indicators. This field is optional.
10. Select any attribute, attribute value, and attribute source to apply to the extracted indicators.
11. Add **Relationships** for the extracted indicators.

> If you enter an object name that is not found, you can click the **Create** link to add the new object. If you limited your search to a specific object type, you are linked to the corresponding form. For example, if you limit your search to Adversaries, the **Create** link opens the Add An Adversary form. If you leave the **Limit search to** field set to All Objects, you can select the object type you want to create from a drop-down list.

12. Click on **Next Step**.

    The Step 2: Organize and Classify page will load.



13. You can review the extracted indicators' information and attributes.

    You can perform the following actions:

ACTION	DETAILS
Add Indicator	You can add additional indicators by clicking on the Add Indicator button.
Edit Indicator Type and Value	You can edit the Indicator Type by clicking on the Pencil icon next to the indicator name. The Edit Indicator screen will load. You can edit the extracted indicator's value and type from this box.

Set/Update Status	You can update the status of one or more extracted indicators. Select the checkbox next to the indicator(s) to update and then click on the **Add Info** option. Click on the **Set Status** tab and select your new status.
Add Attribute	You can add an attribute to one or more extracted indicators. Select the checkbox next to the indicator(s) to update and then click on the **Add Info** option. The Add Attributes tab will be selected by default. Select an **Attribute Name**, **Value**, and **Source** to apply to the selected indicator(s).
Create Relationship	You can link one or more extracted indicators to another system object. Select the checkbox next to the indicator(s) to update and then click on the **Add Info** option. Click on the **Set Relationship** tab and set the relationship. When you add a relationship, it is displayed in the indicator list and you can click it to view its details in a preview panel. If the object you want to link is not found, you can you can click the **Create** link to add the new object. If you limited your search to a specific object type, you are linked to the corresponding form. For example, if you limited your search to Adversaries, the **Create** link opens the Add An Adversary form. If you leave the **Limit search to** field set to All Objects, you can select the object type you want to create from a drop-down list. In the Add form, the indicators you selected in the second step of the import process are listed in the Create Relationship section.
Add Comment	You can add a comment to one or more extracted indicators. Select the checkbox next to the indicator(s) to update and then click on the **Add Info** option. Click on the **Set Comment** tab and enter your comment.
Delete Extracted Indicator	You can delete one or more extracted indicators. Select the checkbox next to the indicator(s) to delete and then click on the **Remove** icon.

14. Click **Finish Export**.

Troubleshooting

If the CSV fails to parse please review the following points:

- Verify that the file is a CSV.
- Verify that column headers are spelled exactly as they are listed, the parser is case sensitive.
- Verify that all rows have a value for Indicator and Type.
- Verify that all Type and Status values are valid and exist in ThreatQ.

> If you have previously hit a failed parse run and believe you have fixed the error but the file will still not parse, logout of TQ, log back in and attempt to parse again.

Indicator URL Normalization

Remove Quotes from the Beginning and/or End of an Indicator

Single and double quote characters are removed if they are the first or last character of an indicator.

Remove Unneeded Spaces found within an Indicator

All spaces irrelevant of their position in the Indicator value are removed (when applicable).

Adjust Leading Protocol from Indicators

Indicators with a leading protocol [http://, https://, ftp://, or ftps://] are extracted and included as an attribute. When applicable, this indicator adjustment could change the indicator type from URL to FQDN.

> Original URL indicator of http://evilsubdomain.no-ip.biz/ would convert to a FQDN = evildomain.no-ip.biz.

Adjust the Port from an IP Address

An IP address with a port [ex. 199.7.136.88:8143] will be truncated to the IP address and the port assignment will be added as an attribute.

Using the previous example the following indicator/attribute will be created:

FIELD	VALUE
URL	199.7.136.88
Attribute > Port	8143

Adjust Defanged/Neutered Indicators

Indicators that have been defanged/neutered in order to “safely” share them (i.e. www [dot] 3322 [dot] org or badguy [at] gmail.com) need to be adjusted during import in order to ensure the indicators are properly deployed.

Create an IP Address from a URL (when applicable)

Using the previous example the following indicators will be created:

FIELD	VALUE
URL	51.255.131.66/civis/viewforum.php
IP Address	51.255.131.66

Create a FQDN from a URL (when applicable)

When a URL contains a domain [ex. bat99-11611.co/gate777.php] a second indicator will be created for the domain [bat99-11611.co].

Using the previous example, the following indicators will be created:

FIELD	VALUE
URL	bat99-11611.co/gate777.php
FQDN	bat99-11611.co

Query Strings in a URL Indicator

URL query strings are important but can significantly limit pattern-matching detection capabilities due to the likelihood of deviations, as well as, hamper the volume of URL indicators being deployed.

As such, the normalization process discards query strings.

Maintain "WWW" on FQDN Indicators

When parsing or importing an 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

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role - Action Permissions: Objects & Context - Individual Object Context & Actions - Expiration Date

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**

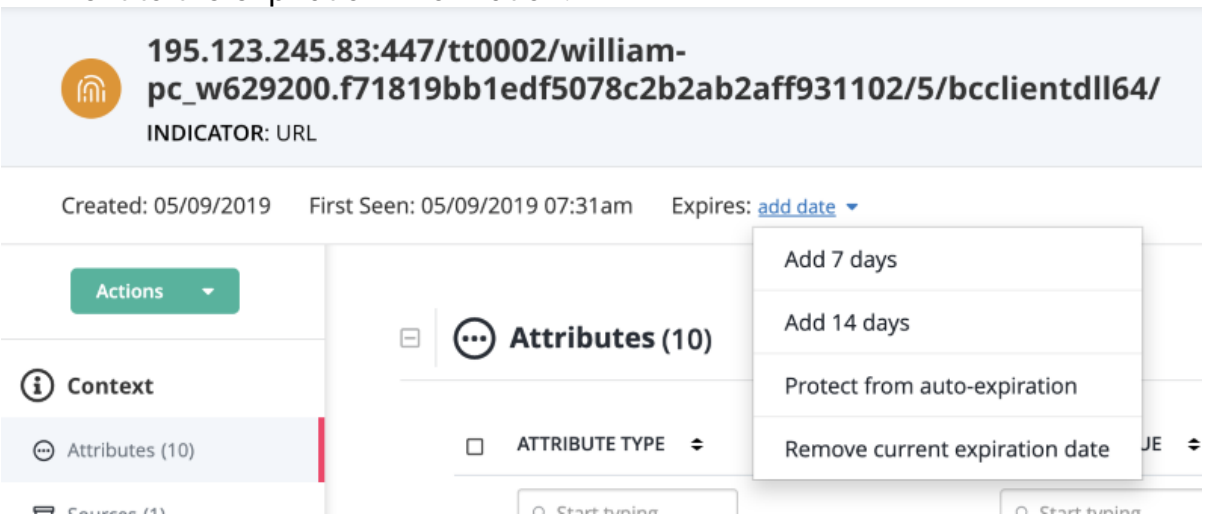
  Each indicator has the option to have an expiration date set, which once past, will toggle the status of that indicator from it's current status to "Expired".

- **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.



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 Status

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role - Action Permissions: Objects & Context - Individual Object Context & Actions - Status

All Indicators in the system have statuses.

Most exports in ThreatQ are configured to use the **Active** status to signal deployment to external devices. However this can be modified and each status can be used however your organization sees fit.

Default Statuses

The default statuses that ship with a standard installation of ThreatQ are as follows:

STATUS	DESCRIPTION
Active	Poses a threat and is being exported to detection tools.
Indirect	Associated to an active indicator or event (i.e. pDNS).
Review	Requires further analysis.
Whitelisted	Poses NO risk and should never be deployed.
Expired	Indicator has reached its expiration and has been is deemed by an analyst to pose less of a threat to their infrastructure than other indicators.

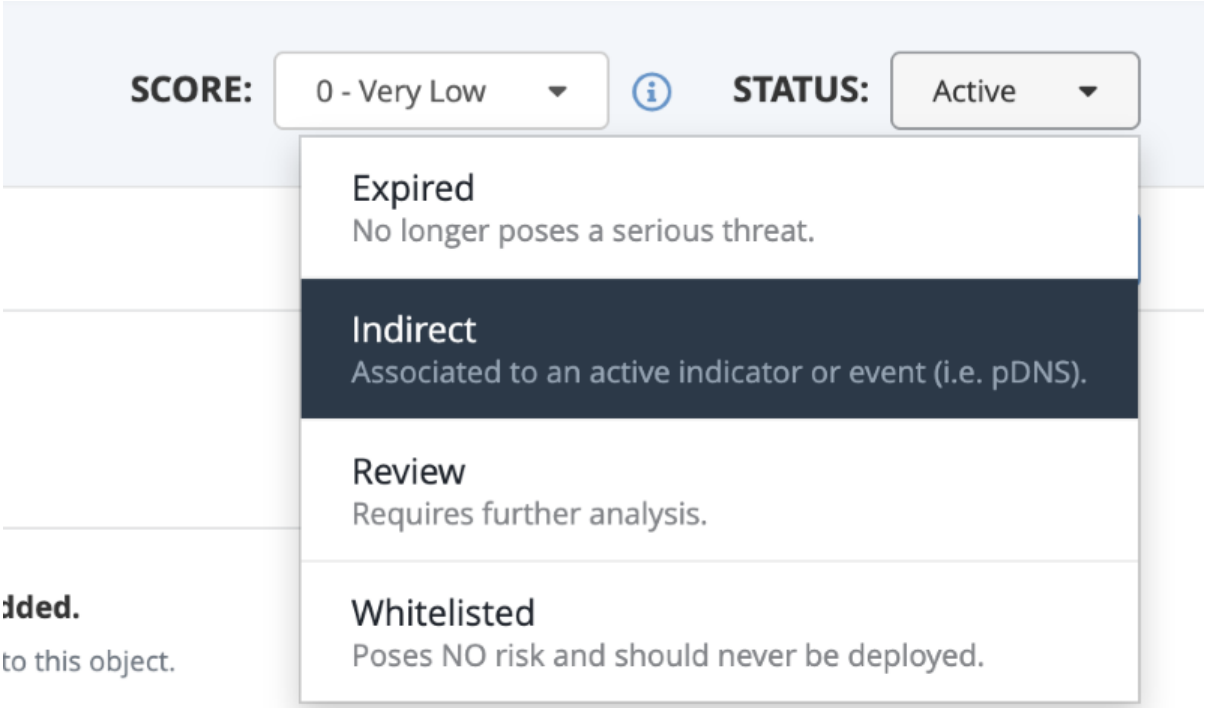
Custom Statuses

You can create custom statuses for use in your ThreatQ instance. See the Indicator Statuses topic for more details.

Changing the Status of an Individual Indicator

Changing an indicator's status is straightforward, except in the case of whitelisting CIDR Block indicators. When Whitelisting a CIDR Block indicator, this process generates a whitelisting rule. See the Whitelisted Indicators topic for more information.

1. Locate and click the indicator to open its details page.
2. Click the status dropdown menu, and select the desired status.



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.

Infrastructure

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor

Custom Role:

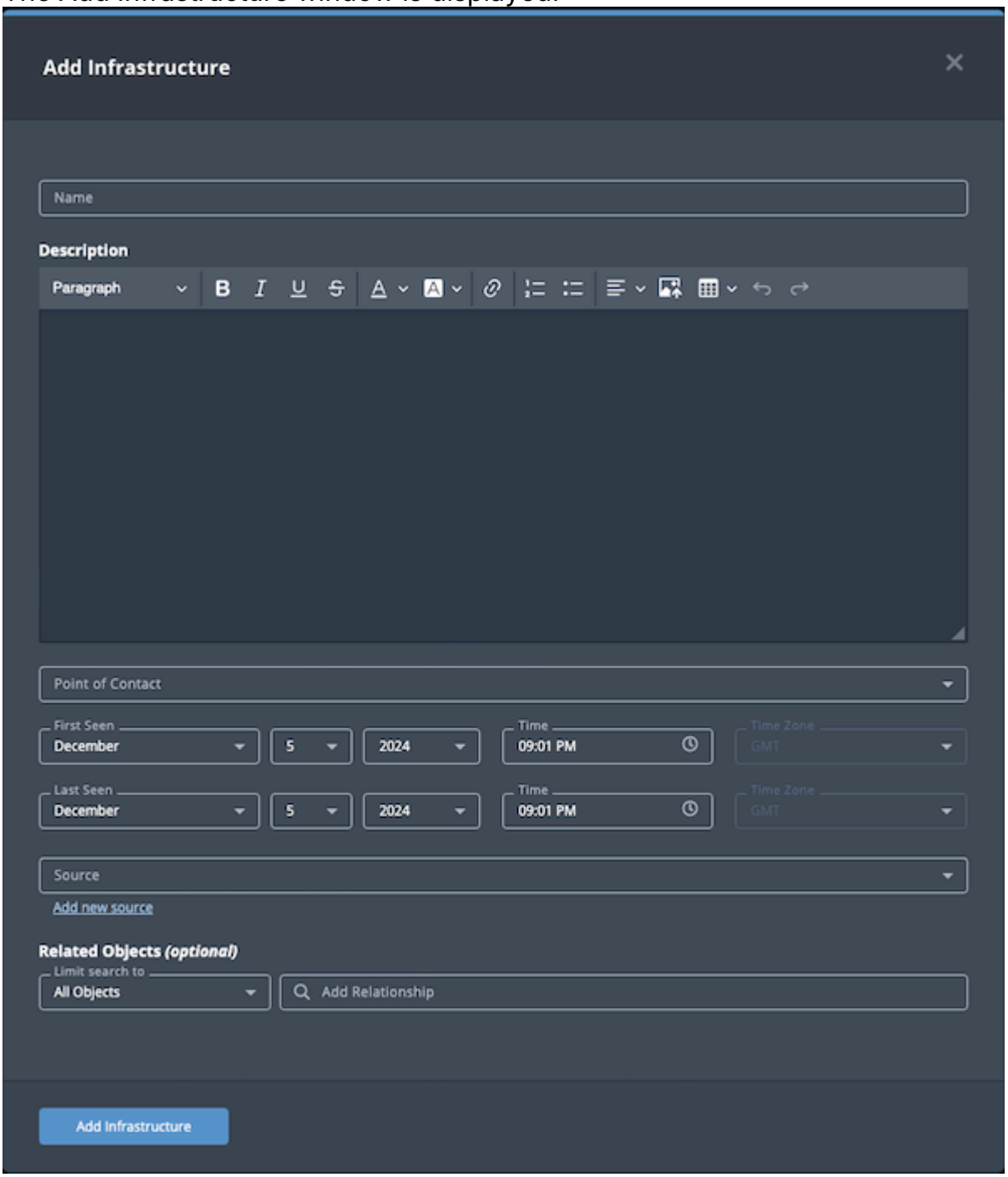
- Action Permissions: Objects & Context - Objects (all object types) **OR** Data Access Permissions: Infrastructure
- Action Permissions: Individual Object Context & Actions
  Note: If a user has View Only permission for Sources, system object creation modals default to the user's login as the object source.

Infrastructure objects are STIX 2.1 objects that provide further context and/or additional analysis. For these objects, ThreatQ stores infrastructure type and kill chain phase information as attributes.

ThreatQ supports STIX exports/imports of infrastructure objects via the Threat Library, object details and preview pages, and the ThreatQ Data Exchange (TQX) TAXII server. When you import an infrastructure object that includes Kill Chain Phase information from a STIX file, this information is imported as attributes with the attribute name prefaced with the "Kill Chain:". For example, if you import the InfraOne infrastructure item, it has an attribute of Kill Chain: mitre-attack. When you export an infrastructure object that includes Kill Chain: attributes to a STIX file, these attributes are exported as Kill Chain Phase information.

Adding Infrastructure Objects

1. Go to **Create > Infrastructure**.
   The Add Infrastructure window is displayed.



2. Populate the following fields:

FIELD	DESCRIPTION
Name	Add a descriptive name for the infrastructure object.
Description	Enter the infrastructure object's description. If you do not select a source during object creation, the description source defaults to ThreatQ System.
Point of Contact	Optional field. Click the field to select the ThreatQ display name of the point of contact for the infrastructure object.
First Seen/ Last Seen	Select the first and last seen dates and times.
Source	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.

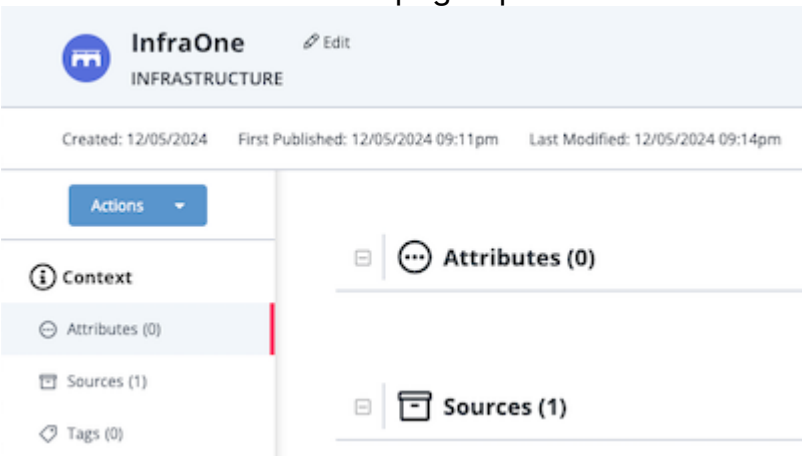
3. Select any **Related Objects** you need to link to the infrastructure object. This field is optional.
4. Click **Add Infrastructure**.

Adding Context

See the About Object Details Page section and its topics for details on adding context to an object such as adding sources, attributes, and related objects.

Editing Infrastructure Objects

1. Locate and click the Infrastructure object.
   The Infrastructure Details page opens.



2. Click the **Edit** option next to the Notes object name.
   The Edit Infrastructure window is displayed.
3. Enter your changes.
4. Click the **Save Infrastructure** button.

Changing the Point of Contact

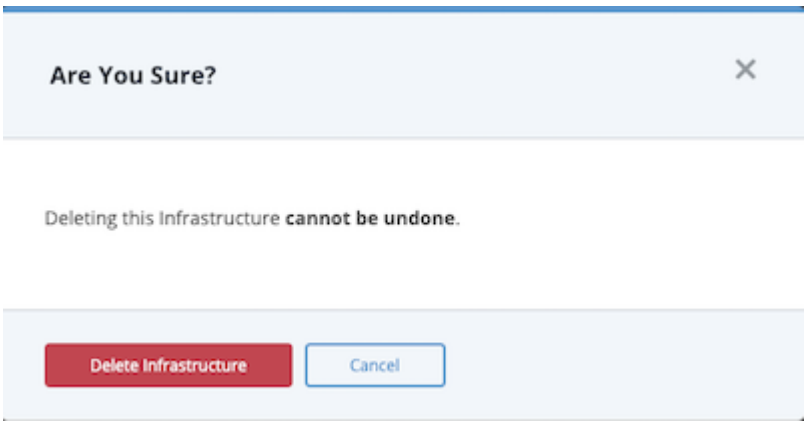
THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role - Action Permissions: Objects & Context - Objects, Individual Object Context & Actions - Point of Contact

1. Locate and click the system object.
2. From the object details page, click the Point of Contact field.
3. Use the field's scroll or search option to locate and select a new user as the object's point of contact or to change the point of contact to Unassigned.

Deleting Infrastructure Objects

1. Locate and click the Infrastructure object.
   The Infrastructure Details page opens.
2. Click the **Actions** menu and select **Delete Infrastructure**.
   The Are You Sure window prompts you to confirm the deletion.



3. Click the **Delete Infrastructure** button.

Intrusion Sets

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor

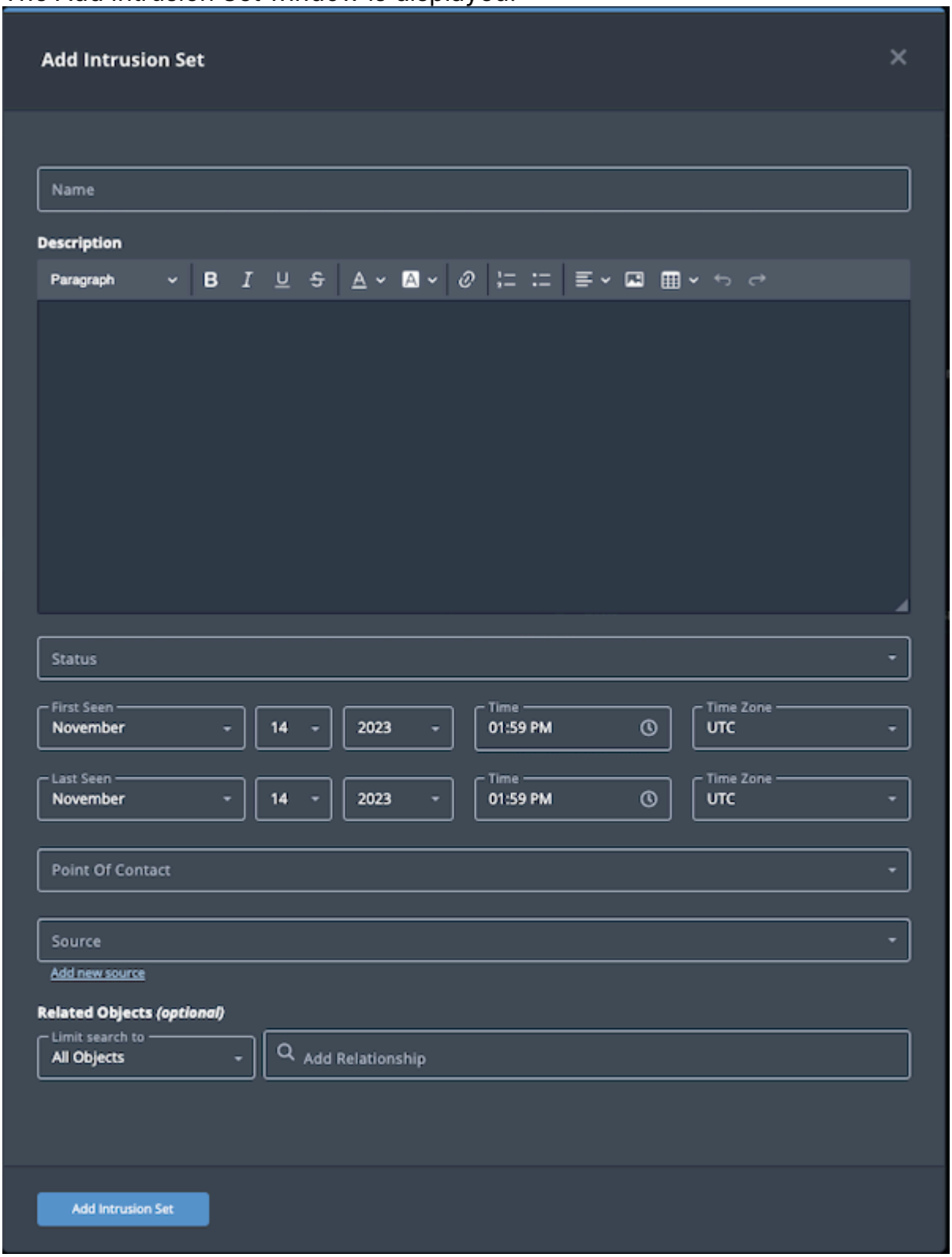
Custom Role:

- Action Permissions: Objects & Context - Objects (all object types) **OR** Data Access Permissions: Intrusion Set
- Action Permissions: Individual Object Context & Actions
  Note: If a user has View Only permission for Sources, system object creation modals default to the user's login as the object source.

An Intrusion Sets 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 window is displayed.



2. Populate the following fields:

FIELD	DESCRIPTION
Name	Add an intrusion set name.
Description	Enter a brief description of the intrusion set. Any description you add during object creation defaults to a Source value of ThreatQ System.
Status	Optional field. Click the Status field to assign a status to the intrusion set. Intrusion set statuses are configured in the Object Statuses tab in the Object Management page. If none are configured, this field is not displayed.
First Seen/ Last Seen	Select the first and last seen dates and times.
Point of Contact	Optional field. Click the field to select the ThreatQ display name of the point of contact for the intrusion set.
Source	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.

3. Select any **Related Objects** you need to link to the Intrusion Set. This field is optional.
4. Click **Add Intrusion Set**.

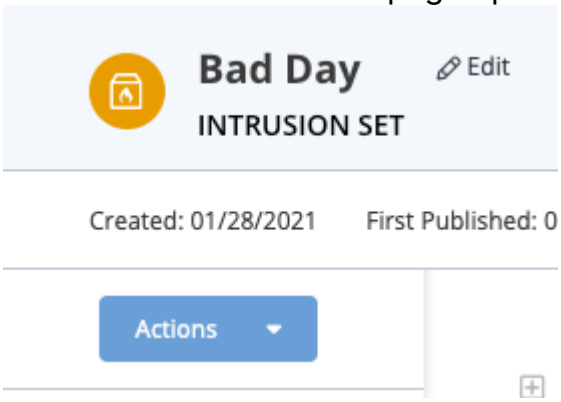
Adding Context

See the About Object Details Page section and its topics for details on adding context to an object such as adding sources, attributes, and related objects.

Editing an Intrusion Set

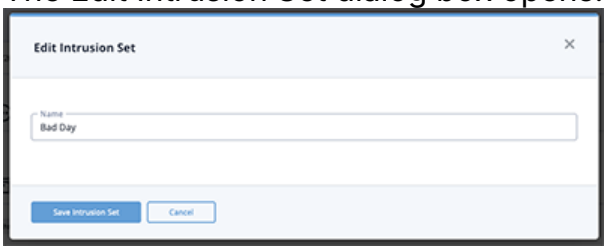
1. Locate and click on the Intrusion Set.

   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.



3. Make the desired change to the Intrusion Set's name and click **Save Intrusion Set**.

Changing the Point of Contact

THREATQ REQUIRED PERMISSIONS

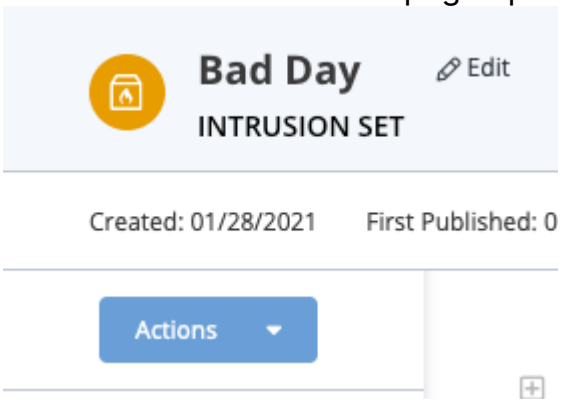
Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role - Action Permissions: Objects & Context - Objects, Individual Object Context & Actions - Point of Contact

1. Locate and click the system object.
2. From the object details page, click the Point of Contact field.
3. Use the field's scroll or search option to locate and select a new user as the object's point of contact or to change the point of contact to Unassigned.

Deleting an Intrusion Set

1. Locate and click on the Intrusion Set.

The Intrusion Set's details page opens.



2. Click on the **Actions** menu and select **Delete Intrusion Set**.

   A confirmation dialog box appears.

3. Click on **Delete Intrusion Set**.

Malware

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor

Custom Role:

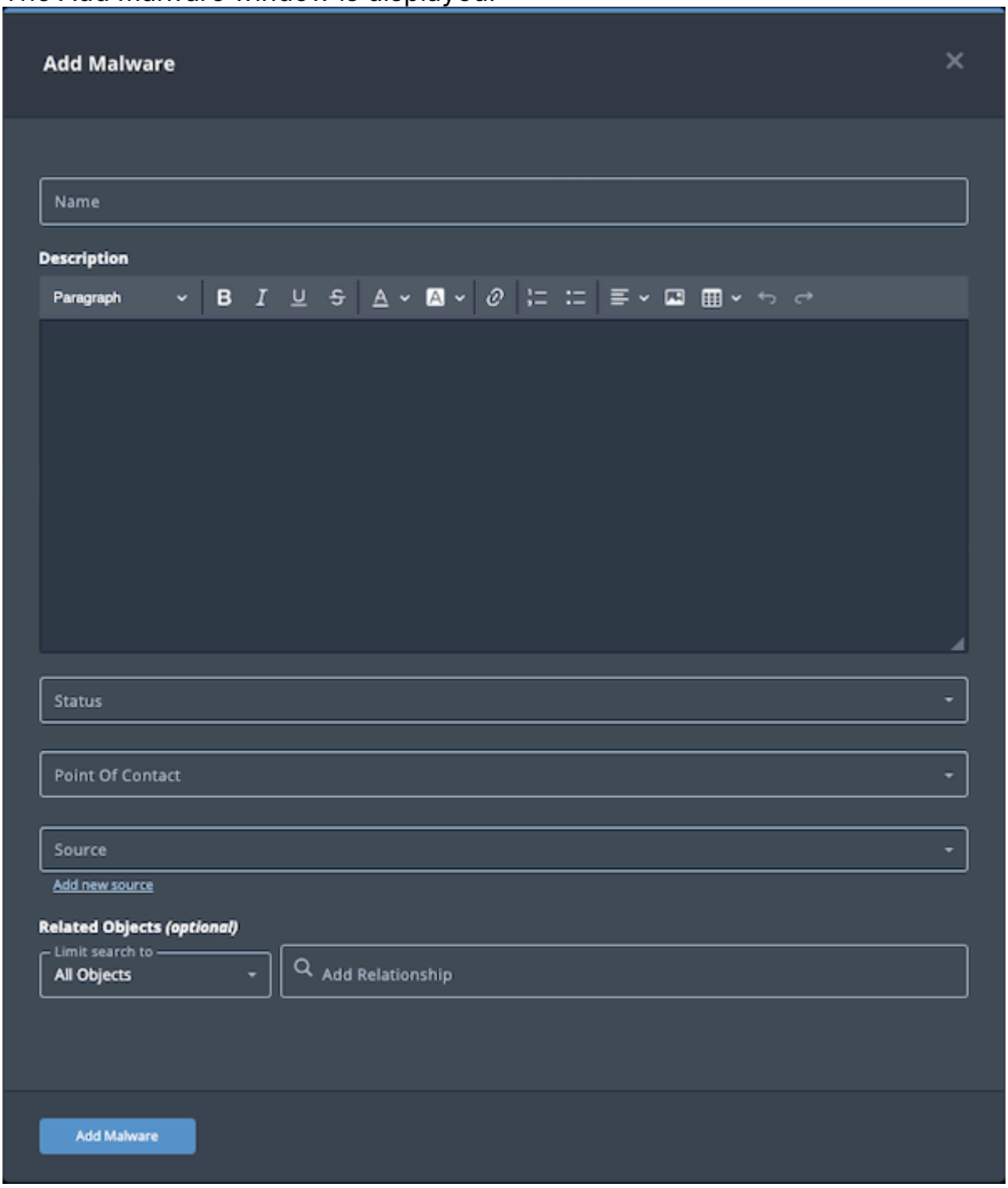
- Action Permissions: Objects & Context - Objects (all object types) **OR** Data Access Permissions: Malware
- Action Permissions: Individual Object Context & Actions
  Note: If a user has View Only permission for Sources, system object creation modals default to the user's login as the object source.

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 window is displayed.



2. Populate the following fields:

FIELD	DESCRIPTION
Name	Add a malware name.
Description	Enter a brief description of the malware object. Any description you add during object creation defaults to a Source value of ThreatQ System.
Status	Optional field. Click the Status field to assign a status to the malware object. Malware statuses are configured in the Object Statuses tab in the Object Management page. If none are configured, this field is not displayed.
Point of Contact	Optional field. Click the field to select the ThreatQ display name of the point of contact for the malware object.
Source	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.

3. Select any **Related Objects** you need to link to the Malware. This field is optional.
4. Click **Add Malware**.

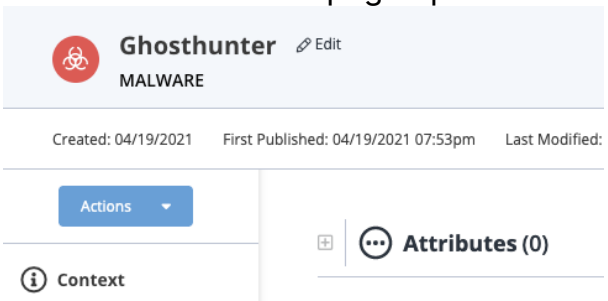
Adding Context

See the About Object Details Page section and its topics for details on adding context to an object such as adding sources, attributes, and related objects.

Editing a Malware Object

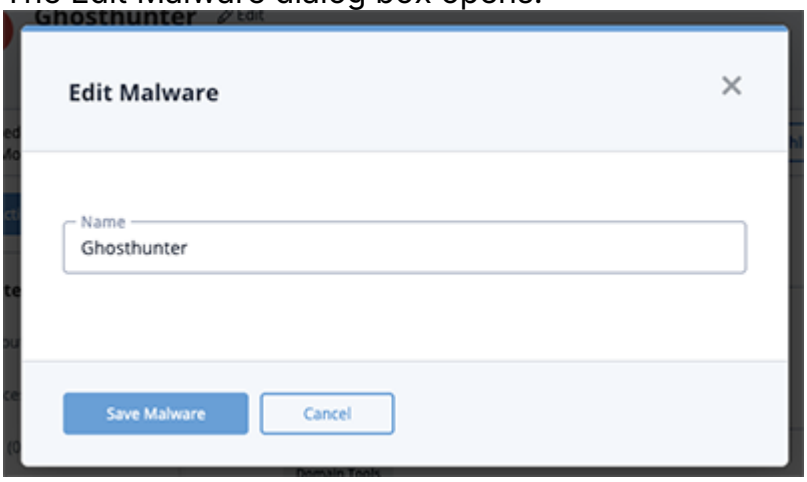
1. Locate and click on the Malware.

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**.

Changing the Point of Contact

THREATQ REQUIRED PERMISSIONS

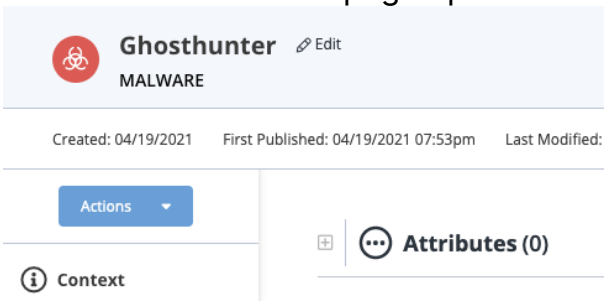
Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role - Action Permissions: Objects & Context - Objects, Individual Object Context & Actions - Point of Contact

1. Locate and click the system object.
2. From the object details page, click the Point of Contact field.
3. Use the field's scroll or search option to locate and select a new user as the object's point of contact or to change the point of contact to Unassigned.

Deleting a Malware Object

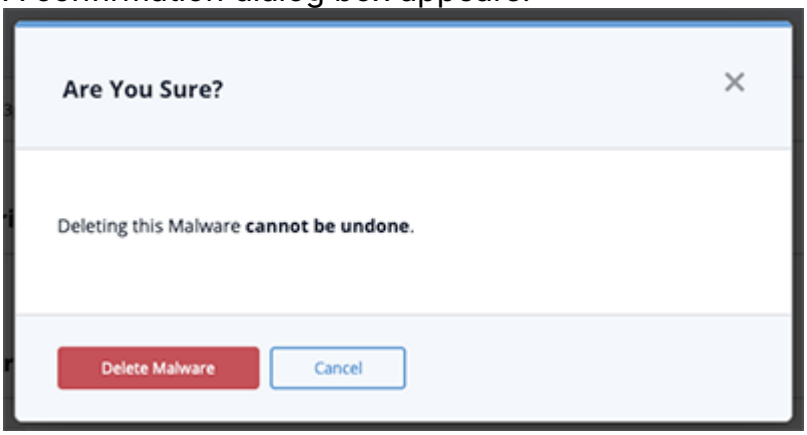
1. Locate and click on the Malware.

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**.

Notes

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor

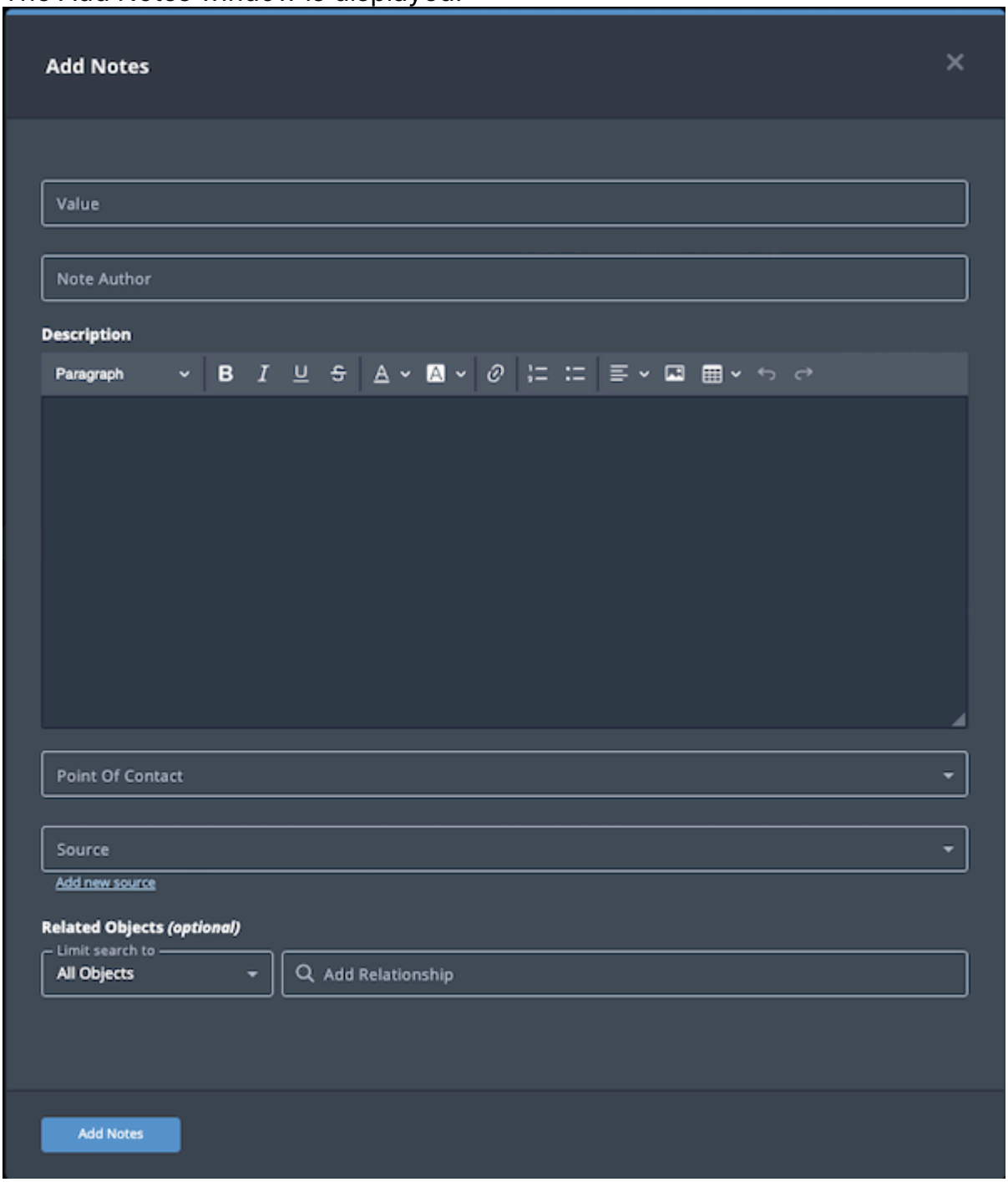
Custom Role:

- Action Permissions: Objects & Context - Objects (all object types) **OR** Data Access Permissions: Notes
- Action Permissions: Individual Object Context & Actions
  Note: If a user has View Only permission for Sources, system object creation modals default to the user's login as the object source.

Notes objects are STIX 2.1 objects that provide further context and/or additional analysis. You can export a Note object to PDF, CSV, or STIX.

Adding Notes

1. Go to **Create > Notes**.
   The Add Notes window is displayed.



2. Populate the following fields:

FIELD	DESCRIPTION
Value	Add a descriptive name for the note.
Note Author	Optional field. Enter the name of the note author.
Description	Enter the note's description. If you do not select a source during object creation, the description source defaults to ThreatQ System.
Point of Contact	Optional field. Click the field to select the ThreatQ display name of the point of contact for the note.
Source	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.

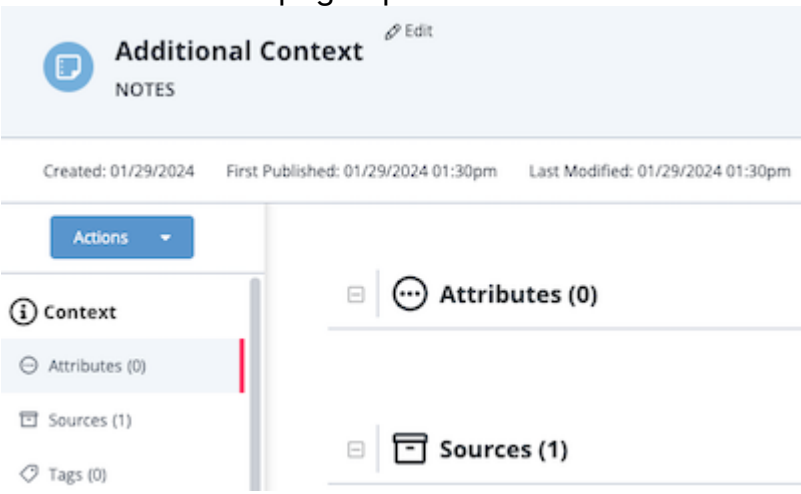
3. Select any **Related Objects** you need to link to the note. This field is optional.
4. Click **Add Notes**.

Adding Context

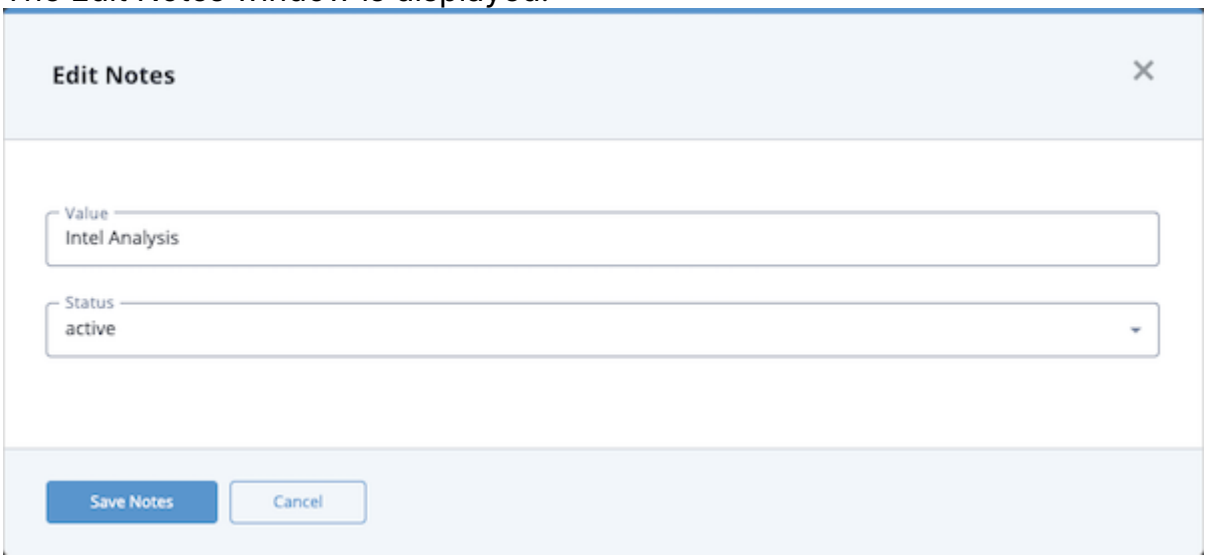
See the About Object Details Page section and its topics for details on adding context to an object such as adding sources, attributes, and related objects.

Editing Notes

1. Locate and click the Notes object.
   The Notes Details page opens.



2. Click the **Edit** option next to the Notes object name.
   The Edit Notes window is displayed.



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

Changing the Point of Contact

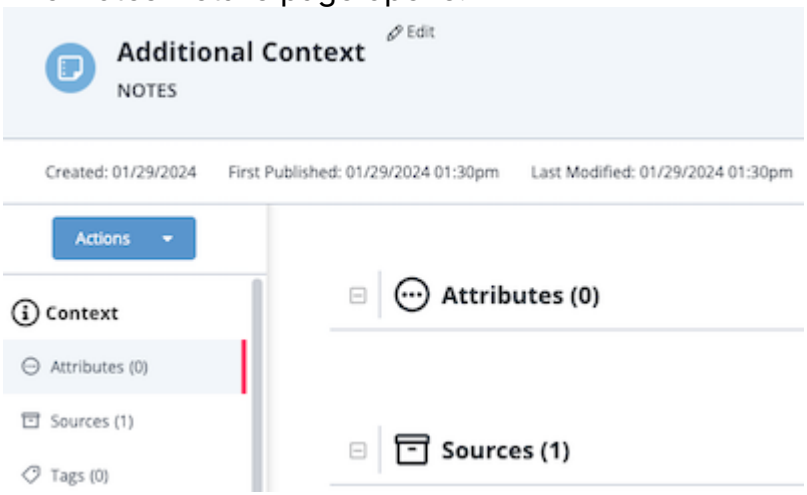
THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role - Action Permissions: Objects & Context - Objects, Individual Object Context & Actions - Point of Contact

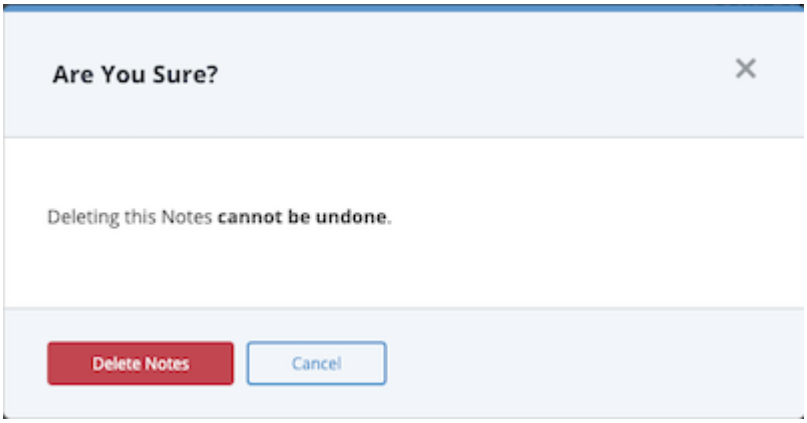
1. Locate and click the system object.
2. From the object details page, click the Point of Contact field.
3. Use the field's scroll or search option to locate and select a new user as the object's point of contact or to change the point of contact to Unassigned.

Deleting Notes

1. Locate and click the Notes object.
   The Notes Details page opens.



2. Click the **Actions** menu and select **Delete Notes**.
   The Are You Sure window prompts you to confirm the deletion.



3. Click the **Delete Notes** button.

Reports

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor

Custom Role:

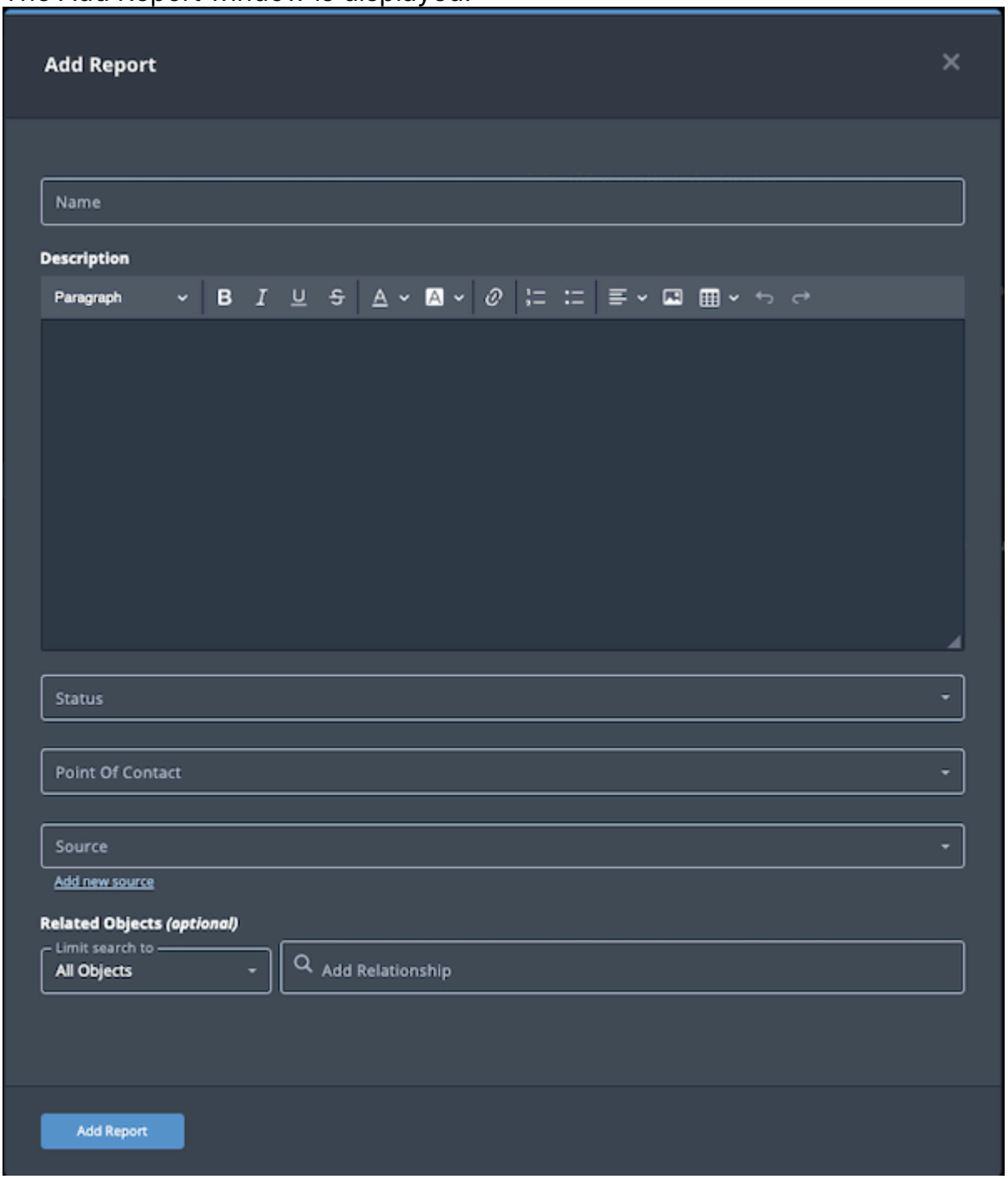
- Action Permissions: Objects & Context - Objects (all object types) **OR** Data Access Permissions: Report
- Action Permissions: Individual Object Context & Actions
  Note: If a user has View Only permission for Sources, system object creation modals default to the user's login as the object source.

Reports 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 window is displayed.



2. Populate the following fields:

FIELD	DESCRIPTION
Name	Add a report name.
Description	Enter a brief description of the report. Any description you add during object creation defaults to a Source value of ThreatQ System.
Status	Optional field. Click the Status field to assign a status to the report. Report statuses are configured in the Object Statuses tab in the Object Management page. If none are configured, this field is not displayed.
Point of Contact	Optional field. Click the field to select the ThreatQ display name of the point of contact for the report.
Source	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.

3. Select any **Related Objects** you need to link to the Report. This field is optional.
4. Click **Add Report**.

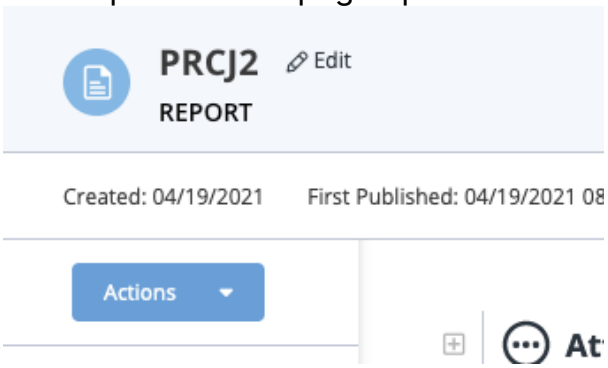
Adding Context

See the About Object Details Page section and its topics for details on adding context to an object such as adding sources, attributes, and related objects.

Editing a Report

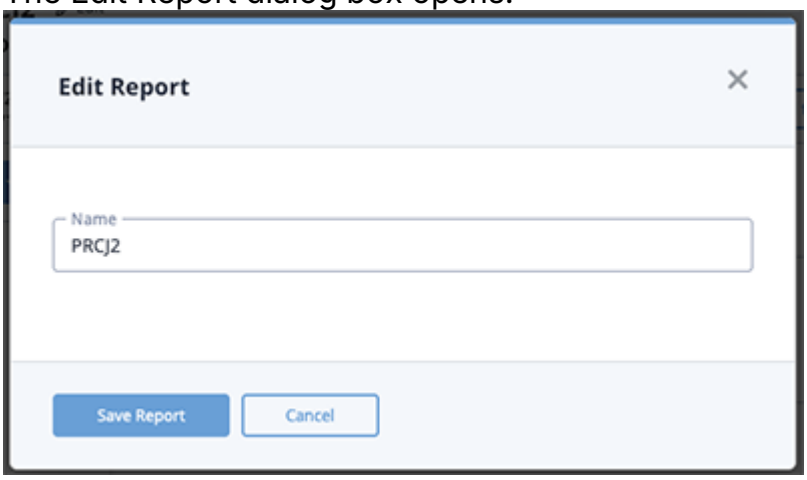
1. Locate and click on the Report.

The Report's detail page opens.



2. Click on **Edit** next to the Report's name.

   The Edit Report dialog box opens.



3. Make the desired change to the Report name and click **Save Report**.

Changing the Point of Contact

THREATQ REQUIRED PERMISSIONS

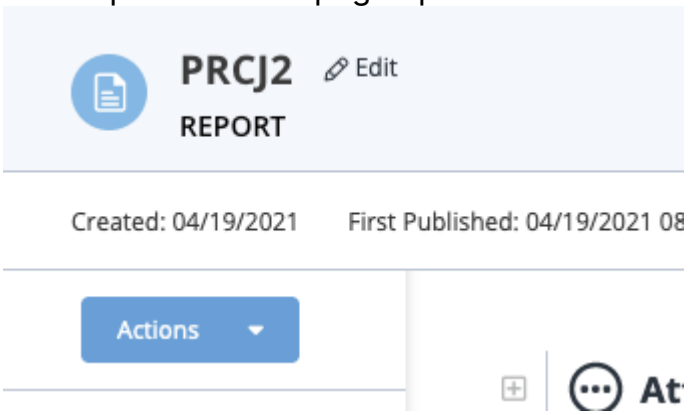
Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role - Action Permissions: Objects & Context - Objects, Individual Object Context & Actions - Point of Contact

1. Locate and click the system object.
2. From the object details page, click the Point of Contact field.
3. Use the field's scroll or search option to locate and select a new user as the object's point of contact or to change the point of contact to Unassigned.

Deleting a Report

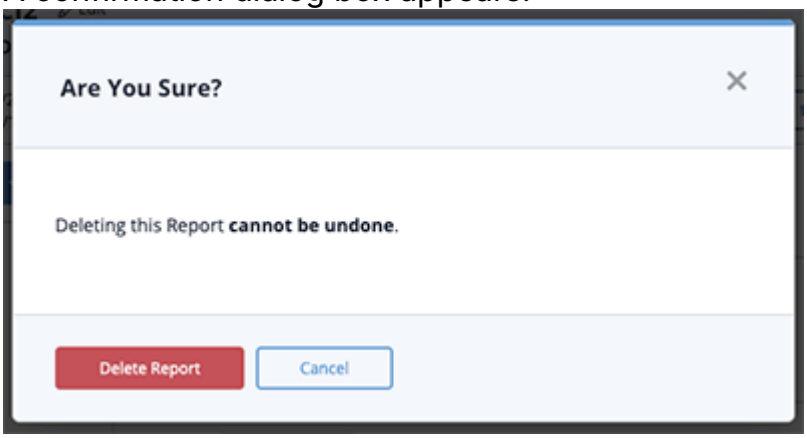
1. Locate and click on the Report.

The Report's details page opens.



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

   A confirmation dialog box appears.



3. Click on **Delete Report**.

Signatures

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor

Custom Role:

- Action Permissions: Objects & Context - Objects (all object types) **OR** Data Access Permissions: Signature
- Action Permissions: Individual Object Context & Actions. Perform Bulk Manual Import

Notes:

- If a user's role has View Only permission for Sources, system object parsers default to the user's login as the object source.
- If a user's role does not include permission to Edit or delete an object's Status, system object parsers apply the default status to seeded system objects and the first status option for custom objects.
- If an import contains object types or context you lack Create/Edit/Delete permission for, the import fails.

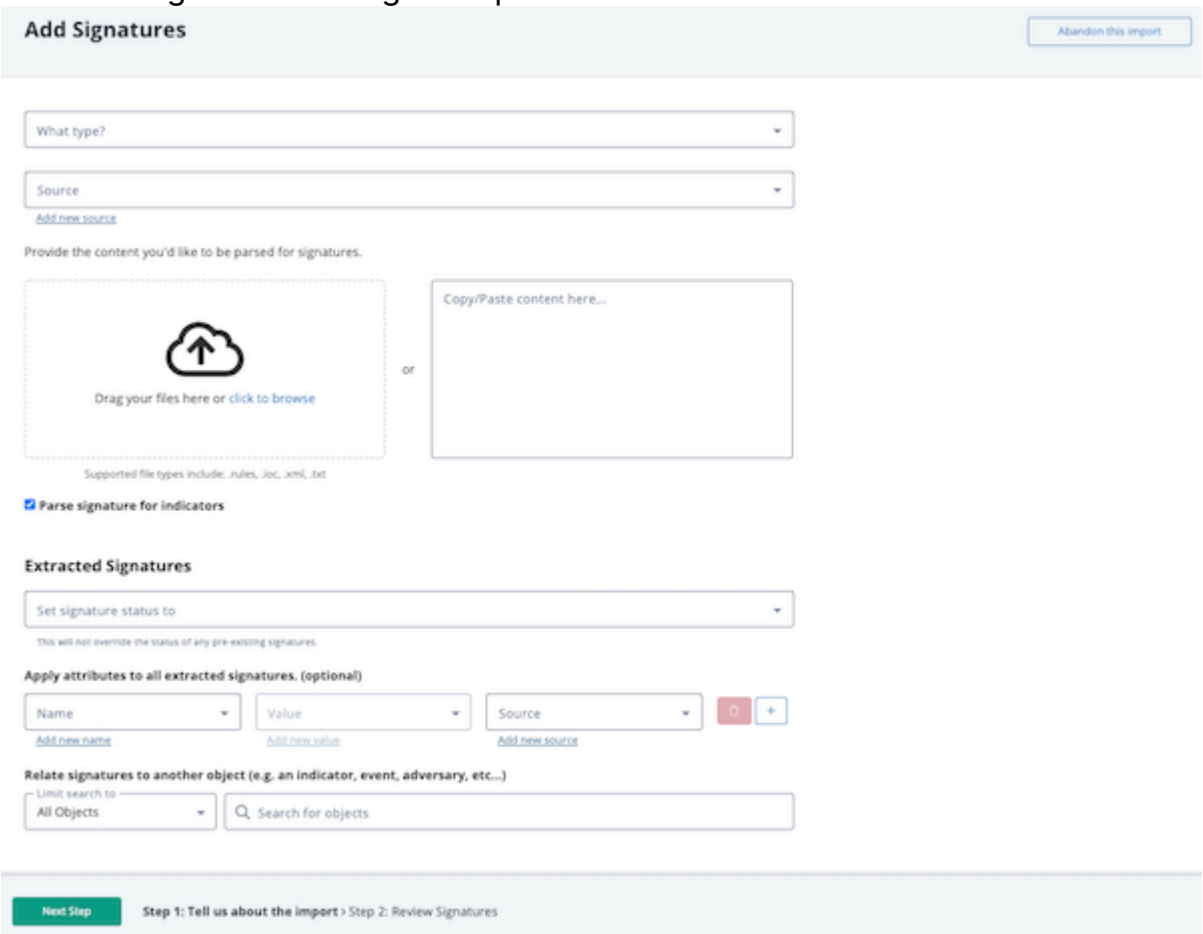
Signatures contain the blueprints or patterns associated with a malicious attack on a network or system.

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 Indicators, Events, Adversaries, 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**.

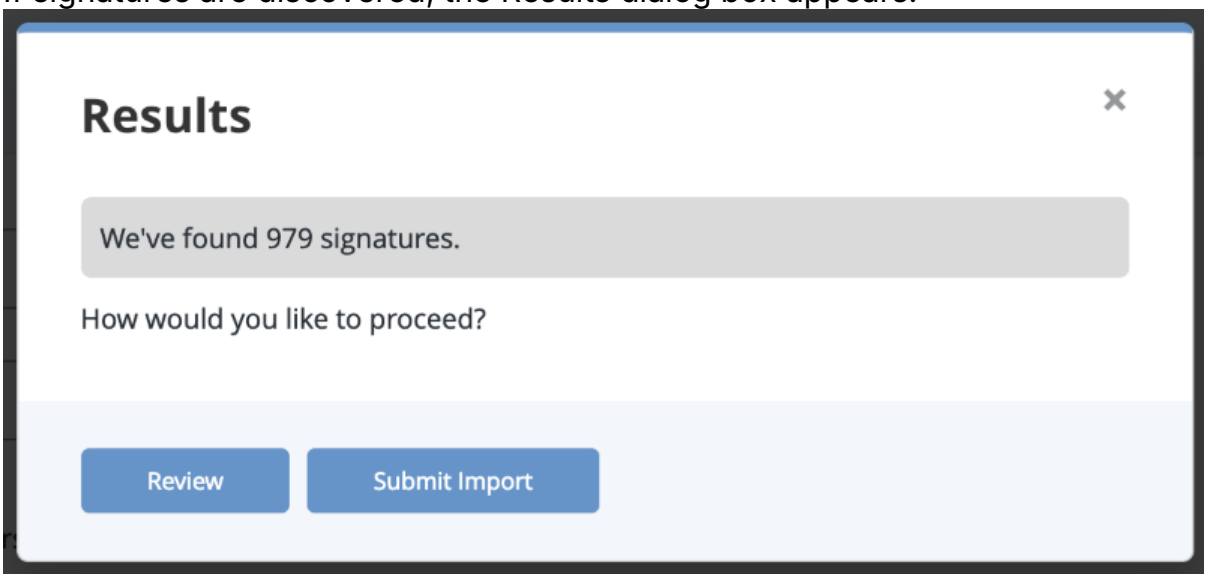
You can click on the **Add** icon for additional attributes.

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.

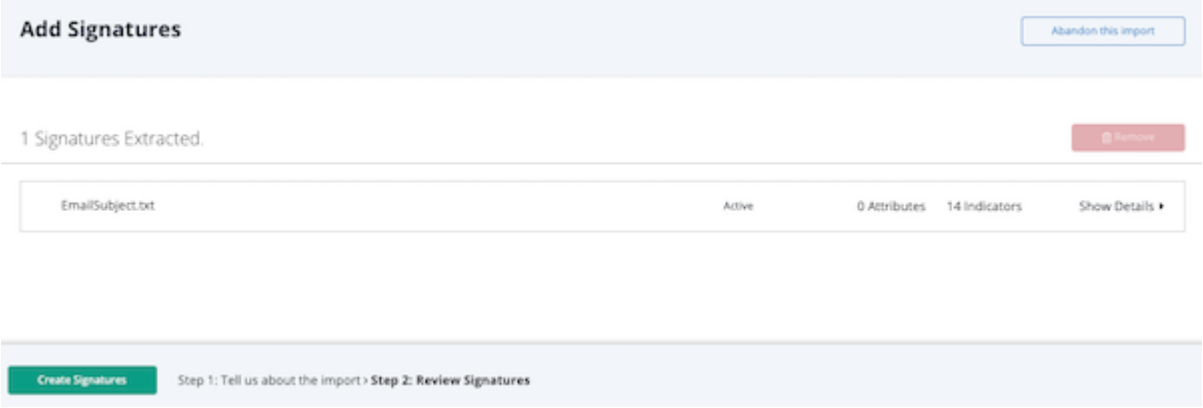
9. Click **Next Step**.

   If signatures are discovered, the Results dialog box appears.



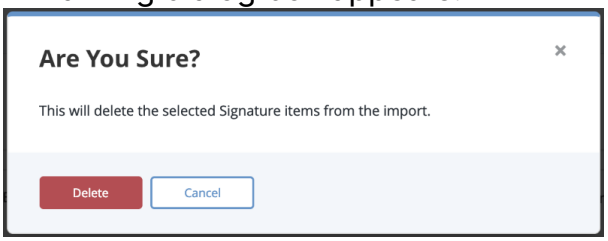
10. You can either select **Submit Import** to finish adding the signatures or **Review** to customize what data is imported.

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 REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role - Action Permissions: Objects & Context - Perform Bulk Manual Import, Create, Edit, Delete Objects, Create, Edit, Delete Attributes,Create, Edit, Delete Relationships. See the Interdependent Permissions topic.

Notes:

- If a user's role has View Only permission for Sources, system object parsers default to the user's login as the object source.
- If a user's role does not include permission to Edit or delete an object's Status, system object parsers apply the default status to seeded system objects and the first status option for custom objects.

Custom Role - Data Access Permissions: Create, Edit, Delete permission for at least one STIX object type.

ThreatQ supports STIX 1.1.1, STIX 1.2, STIX 2.0, and STIX 2.1.

ThreatQ allows you to ingest and manage STIX files. You can ingest STIX data in two ways:

- You can set up a STIX/TAXII Feed.
- You can upload a STIX file or insert STIX data to parse for indicators.

ThreatQ STIX Object Types

STIX integration provides ThreatQ with the following additional object types.

- Campaigns
- Courses of Actions
- Exploit Targets
- Incidents
- TTPs objects
- Identity (STIX 2.0)
- Reports (STIX 2.0)
- Vulnerabilities (STIX 2.0)
- Notes (STIX 2.1)

These objects enable better understanding and communication of STIX data. STIX data will be mapped to these objects and existing objects in the system.

Attribute Updates

When you import a STIX 2.0 or 2.1 object attribute update for the following attributes and from the same TAXII feed, the attribute value is updated in ThreatQ:

- administrative_area
- city
- county
- country
- identity_class
- last_seen
- latitude
- longitude
- number_observed
- postal_code
- precision
- primary_motivation
- region
- resource_level
- sophistication
- street_address
- tool_version
- valid_from
- valid_until

For example, the CAR54 object has a valid_until attribute of 04/02/2025 with a source of YellowCab. When you import an updated valid_until attribute of 05/02/2025 from the YellowCab feed, ThreatQ updates the valid_until attribute to 05/02/25.

Same-source updates to attributes types not listed above as well as attribute updates from a different source are stored as new attributes in ThreatQ.

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. You can select a status for any object for which an Admin or Maintenance user has configured object statuses. See the Object Statuses topic for more information.
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

STIX FIELD	THREATQ FIELD MAPPING	THREATQ NAME
	Indicator.value	
	Indicator.type	File Path
	Indicator.value	
	Indicator.attribute	File Size
	Indicator.attribute	File Format
	Indicator.attribute	Packer
	Indicator.type	MD5
	Indicator.type	SHA-256
	Indicator.type	SHA-1
	Indicator.type	SHA-512
	Indicator.value	
	Indicator.type	SSDEEP
	Indicator.value	
	Indicator.type	FQDN
	Indicator.value	
	Indicator.type	URL
	Indicator.value	

STIX FIELD	THREATQ FIELD MAPPING	THREATQ NAME
	Indicator.type	Email Subject
	Indicator.value	
	Indicator.type	Email Address
	Indicator.value	
	Indicator.type	IP Address
	Indicator.value	
	Indicator.type	User-agent
	Indicator.value	
	Indicator.type	Filename
	Indicator.value	
	Indicator.type	Mutex
	Indicator.value	
	Indicator.attribute	Port
	Indicator.attribute	Protocol
	Object.Description	
	Spearphish.value	
	Indicator.type	Registry Key

STIX FIELD	THREATQ FIELD MAPPING	THREATQ NAME
	Indicator.value	
	Indicator.attribute	Hive

- *Campaigns Mapping*

STIX FIELD	THREATQ FIELD MAPPING	THREATQ NAME
Title	Campaign.value	
ID	Campaign.attribute	STIX Reference ID
Description	Campaign.attribute	Description
Short Description	Campaign.attribute	Short Description
Timestamp	Campaign.started_at	
Names	Campaign.attribute	Alias
Status	Campaign.attribute	Status
Intended_Effect	Campaign.attribute	Intended Effect
Confidence	Campaign.attribute	Confidence
Activity	Campaign.attribute	Activity
Related TTPs	TTP	
Related Incidents	Incident	
Attribution	Adversary	

STIX FIELD	THREATQ FIELD MAPPING	THREATQ NAME
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
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

STIX FIELD	THREATQ FIELD MAPPING	THREATQ NAME
Incident_Closed		
Coordinator	Incident.attribute	Coordinator
	Incident.attribute	Coordinator
Reporter	Incident.attribute	Reporter
	Incident.attribute	Reporter
Responder	Incident.attribute	Responder
	Incident.attribute	Responder
Victim	Incident.attribute	Victim
	Incident.attribute	Victim
Related Indicators	Indicator	
Related Observables	Indicator	
Leveraged_TTPs	TTP	
Intended_Effect	Incident.attribute	Intended Effect
COA_Requested	Course of Action	
COA_Taken	Course of Action	
Confidence	Incident.attribute	Confidence

STIX FIELD	THREATQ FIELD MAPPING	THREATQ NAME
Attributed_Threat_Actors	Adversary	
Discovery_Method	Incident.attribute	Discovery Method
Related_Incidents	Incident	

- *TTP Mapping*

STIX FIELD	THREATQ FIELD MAPPING	THREATQ NAME
Title	TTP.value	
ID	TTP.attribute	STIX Reference ID
Description	TTP.attribute	Description
Handling	TTP.tlp	
Kill_Chain_Phases	TTP.attribute	Kill Chain Phase
Intended_Effect	TTP.attribute	Intended Effect
	TTP.attribute	CAPEC ID
Behavior	TTP.attribute	Attack Pattern
	TTP.attribute	Attack Pattern Description
	TTP.attribute	Attack Pattern Short Description
	TTP.attribute	Malware Type

STIX FIELD	THREATQ FIELD MAPPING	THREATQ NAME
	TTP.attribute	Malware Name
	TTP.attribute	Malware Description
	TTP.attribute	Malware Short Description
	TTP.attribute	Malware Detection Vendor
	TTP.attribute	Malware Family
	TTP.attribute	Exploit
	TTP.attribute	Exploit Description
	TTP.attribute	Exploit Short Description
Exploit_Targets	Exploit Target	
Related_TTPs	TTP	
Resources	TTP.attribute	Tool
	TTP.attribute	Tool
	TTP.attribute	Tool Type
	TTP.attribute	Tool Description
	TTP.attribute	Tool Short Description
	TTP.attribute	Infrastructure Type

STIX FIELD	THREATQ FIELD MAPPING	THREATQ NAME
	TTP.attribute	Infrastructure
	TTP.attribute	Infrastructure Short Description
	TTP.attribute	Infrastructure Description
	Indicator	
	TTP.attribute	Persona
Victim Targeting	TTP.attribute	Victim Name
	TTP.attribute	Victim <CIQ Identity Name>
	TTP.attribute	Targeted Systems
	TTP.attribute	Targeted Information
	Indicator	

- *CIQ Identity Mapping*

STIX FIELD	THREATQ FIELD MAPPING	THREATQ NAME
Party Name	Object.attribute	Name
Organization Name	Object.attribute	Organization
Industry Sector	Object.attribute	Industry
Nationality	Object.attribute	Nationality

STIX FIELD	THREATQ FIELD MAPPING	THREATQ NAME
Languages	Object.attribute	Language
Address	Object.attribute	Country
Email Address	Object.attribute	E-Mail Address
Chat Handle	Object.attribute	Chat Handle
Phone	Object.attribute	Phone

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, except for Notes objects.

You can click on the expand icon located to the 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

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
		Adversaries will be inter-related
created	Adversary.Published_At	
goals	Adversary.Attribute	Goal
labels	Adversary.Attribute	Label
modified	Adversary.Attribute	Modified At
name	Adversary.Value	
primary_motivation	Adversary.Attribute	Primary Motivation
resource_level	Adversary.Attribute	Resource Level
roles	Adversary.Attribute	Role
secondary_motivation	Adversary.Attribute	Secondary Motivation
sophistication	Adversary.Attribute	Sophistication
revoked (if revoked == true)	Adversary.Attribute	Revoked
external_references[]	See External References	
personal_motivations	Adversary.Attribute	Personal Motivation

- *Indicators Mapping*

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
created	Signature.Published_at	
description	Signature.Description	
external_references[]	See External References	
labels	Signature.Attribute	Label
modified	Signature.Attribute	Modified At
name	Signature.Name	ThreatQ will default to using Indicator Pattern as the signature name if a name is not provided.
pattern	Signature.Value	
	Signature.Type	Indicator Pattern
valid.from	Signature.Attribute	Valid From
valid.until	Signature.Attribute	Valid Until
revoked (if revoked == true)	Signature.Attribute	Revoked
kill_chain_phases.[]	See Kill Chain Table	

ThreatQ Indicator and / or Event objects based on the Observables Mapping may be derived from the `pattern` field and related back to the resulting Signature.

- *Identities Mapping*

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
contact_information	Identity.Contact_Information	
created	Identity.Published_at	
description	Identity.Description	
external_references[]	See External References	
identity_class	Identity.Attribute	Identity Class
modified	Identity.Attribute	Modified At
name	Identity.Value	
sectors	Identity.Attribute	Sector
labels	Identity.Attribute	Label
revoked (if revoked == true)	Identity.Attribute	Revoked

- *Observables Mapping*

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
created	Observable.Published_at	
modified	Observable.Attribute	Modified At
revoked (if revoked == true)	Observable.Attribute	Revoked

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
external_references	Observable.Attribute	External Reference See External References.
number_observed	Observable.Attribute	Number Observed
objects[]		Specifies Cyber Observable Objects representing this observation. See the tables below for parsing details.

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. *Automous System Mapping*

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
type: autonomous-system	Indicator.Type	ASN
number	Indicator.Value	
name	Indicator.Attribute	Name
rir	Indicator.Attribute	Regional Internet Registry

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	

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
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
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

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
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
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 pai of the additional_header_field 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** fiel

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
*** If an object in body_multipart has a body field (body_multipart[].body), an attribute is created. The attribute's name is "Body Multipart" and the attribute's value is in the format "Content Type: {body_multipart[].content_type}, Content Disposition: {body_multipart[].content_disposition}, Body: {body_multipart[].body}". Note: Parsing both an indicator and event from an email message will relate the two objects .		

7. *File Mapping*

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREA NAM
type: file	Indicator.Type	Filename
size	Indicator.Attribute	File Size
hashes{}		
hashes{}.key	Indicator.Type	MD5 / SH SHA-256 SHA-384 SHA-512 / Fuzzy Has
hashes{}.value	Indicator.Value	
name	Indicator.Value	
name_enc	Indicator.Attribute	File Name Encoding
magic_number_hex	Indicator.Attribute	Magic Nu Hex
mime_type	Indicator.Attribute	MIME Typ

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREAT NAM
created	Indicator.Attribute	Created A
accessed	Indicator.Attribute	Last Acce
parent_directory_ref	Indicator.Relationship	
is_encrypted	Indicator.Attribute	Encrypted
encryption_algorithm	Indicator.Attribute	Encryptio Algorithm
decryption_key	Indicator.Attribute	Decryptio 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 Fi Comment
extensions.ntfs-ext.sid	Indicator.Attribute	Security I
extensions.ntfs-ext.alternate_data_streams[].hashes{}		
extensions.ntfs-ext.alternate_data_streams[].hashes{}.key	Indicator.Type	MD5 / SH SHA-256 SHA-384

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREAT NAM
		SHA-512 / Fuzzy Has
extensions.ntfs-ext.alternate_data_streams[].hashes{}.value	Indicator.Value	
extensions.ntfs-ext.alternate_data_streams[].name	Indicator.Attribute	Alternate Stream Na
extensions.ntfs-ext.alternate_data_streams[].size	Indicator.Attribute	Alternate Stream Si
extensions.pdf-ext.version	Indicator.Attribute	PDF Specificat Version
extensions.pdf-ext.is_optimized	Indicator.Attribute	PDF Is Optimized
extensions.pdf-ext.document_info_dict{}.key/value	Indicator.Attribute	Formatted 'PDF {key.title()
extensions.pdf-ext.pdfid0	Indicator.Attribute	PDF First Identifier
extensions.pdf-ext.pdfid1	Indicator.Attribute	PDF Seco File Identi
extensions.raster-image-ext.image_height	Indicator.Attribute	Image Hei
extensions.raster-image-ext.image_width	Indicator.Attribute	Image Wi
extensions.raster-image-ext.bits_per_pixel	Indicator.Attribute	Image Bits Pixel

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREAT NAM
extensions.raster-image-ext.image_compression_algorithm	Indicator.Attribute	Image Compress Algorithm
extensions.raster-image-ext.exif_tags{}.key/value	Indicator.Attribute	Formatted 'Image EX {key.title(
extensions.windows-pebinary-ext.pe_type	Indicator.Attribute	Executabl Extension Type
extensions.windows-pebinary-ext.imphash	Indicator.Attribute	Executabl Imphash
extensions.windows-pebinary-ext.machine_hex	Indicator.Attribute	Target Machine H
extensions.windows-pebinary-ext.number_of_sections	Indicator.Attribute	PE Binary Section C
extensions.windows-pebinary-ext.time_date_stamp	Indicator.Attribute	PE Binary Created D
extensions.windows-pebinary-ext.pointer_to_symbol_table_hex	Indicator.Attribute	Symbol Ta Hex Offse
extensions.windows-pebinary-ext.number_of_symbols	Indicator.Attribute	PE Binary Symbol Ta Size
extensions.windows-pebinary-ext.size_of_optional_header	Indicator.Attribute	PE Binary Optional Header Si

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREAT NAM
extensions.windows-pebinary-ext.characteristics_hex	Indicator.Attribute	PE Binary Character Hex
extensions.windows-pebinary-ext.file_header_hashes{}		
extensions.windows-pebinary-ext.file_header_hashes{}.key	Indicator.Type	MD5 / SH SHA-256 SHA-384 SHA-512 / Fuzzy Has
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 Link Version
extensions.windows-pebinary-ext.optional_header.minor_linker_version	Indicator.Attribute	PE Binary Minor Link 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 Size

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREAT NAM
extensions.windows-pebinary-ext.optional_header.size_of_uninitialized_data	Indicator.Attribute	PE Binary Uninitializ Data Size
extensions.windows-pebinary-ext.optional_header.address_of_entry_point	Indicator.Attribute	PE Binary Memory Address E Point
extensions.windows-pebinary-ext.optional_header.base_of_code	Indicator.Attribute	PE Binary Code Mer Address
extensions.windows-pebinary-ext.optional_header.base_of_data	Indicator.Attribute	PE Binary Data Mem Address
extensions.windows-pebinary-ext.optional_header.image_base	Indicator.Attribute	PE Binary Image Me 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 Major Ver
extensions.windows-pebinary-ext.optional_header.minor_os_version	Indicator.Attribute	Windows Minor Ver

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREAT NAM
extensions.windows-pebinary-ext.optional_header.major_image_version	Indicator.Attribute	Image Ma Version
extensions.windows-pebinary-ext.optional_header.minor_image_version	Indicator.Attribute	Image Mir Version
extensions.windows-pebinary-ext.optional_header.major_subsystem_version	Indicator.Attribute	Subyster Major Ver
extensions.windows-pebinary-ext.optional_header.minor_subsystem_version	Indicator.Attribute	Subyster Minor Ver
extensions.windows-pebinary-ext.optional_header.win32_version_value_hex	Indicator.Attribute	Win32 Ve Hex
extensions.windows-pebinary-ext.optional_header.size_of_image	Indicator.Attribute	Image Byt Size
extensions.windows-pebinary-ext.optional_header.size_of_headers	Indicator.Attribute	PE Binary Combined Header Si
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 Subyster Hex
extensions.windows-pebinary-ext.optional_header.dll_characteristics_hex	Indicator.Attribute	DLL Character Hex

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREAT NAM
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 Com Size
extensions.windows-pebinary-ext.optional_header.size_of_heap_reserve	Indicator.Attribute	Heap Spa Reserve S
extensions.windows-pebinary-ext.optional_header.size_of_heap_commit	Indicator.Attribute	Heap Spa Commit S
extensions.windows-pebinary-ext.optional_header.loader_flags_hex	Indicator.Attribute	Loader Fla Hex
extensions.windows-pebinary-ext.optional_header.number_of_rva_and_sizes	Indicator.Attribute	Number o RVA and S
extensions.windows-pebinary-ext.optional_header.hashes{}		
extensions.windows-pebinary-ext.optional_header.hashes{}.key	Indicator.Type	MD5 / SHA SHA-256 SHA-384 SHA-512 / Fuzzy Has
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 SHA-256 SHA-384

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREAT NAM
		SHA-512 / Fuzzy Has
extensions.windows-pebinary-ext.sections[].hashes{}.value	Indicator.Value	
extensions.windows-pebinary-ext.sections[].name	Indicator.Attribute	PE Binary Section N
extensions.windows-pebinary-ext.sections[].size	Indicator.Attribute	PE Binary Section Si
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
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

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
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	

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
created	Campaign.Published_at	
description	Campaign.Description	
first_seen	Campaign.Started_at	
last_seen	Campaign.Ended_at	
modified	Campaign.Attribute	Modified At
name	Campaign.Value	
objective	Campaign.Objective	
revoked (if revoked == true)	Campaign.Attribute	Revoked
external_references[]	See External References	
labels	Campaign.Attribute	Label

- *Courses of Action Mapping*

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
created	Course of Action.Published_at	
modified	Course of Action.Attribute	Modified At
name	Course of Action.Value	
description	Course of Action.Description	
action		

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
revoked (if revoked == true)	Course of Action.Attribute	Revoked
external_references[]	See External References	
labels	Course of Action.Attribute	Label

- *Intrusion Sets Mapping*

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
aliases	Intrusion Set	
created	Intrusion Set.Published_at	
description	Intrusion Set.Description	
first_seen		
goals	Intrusion Set.Attribute	Goal
modified	Intrusion Set.Attribute	Modified At
name	Intrusion Set.Value	
primary_motivation	Intrusion Set.Attribute	Primary Motivation
resource_level	Intrusion Set.Attribute	Resource Level
secondary_motivations	Intrusion Set.Attribute	Secondary Motivation
external_references[]	See External References	

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
revoked (if revoked == true)	Intrusion Set.Attribute	Revoked

- *Malware Mapping*

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
created	Malware.Published_at	
description	Malware.Description	
kill_chain_phases.[]	See Kill Chain Table	
labels	Malware.Attribute	Label
modified	Malware.Attribute	Modified At
name	Malware.Value	
external_references[]	See External References	
revoked (if revoked == true)	Malware.Attribute	Revoked

- *Tools Mapping*

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
created	Tool.Published_at	
modified	Tool.Attribute	Modified At
labels	Tool.Attribute	Label
name	Tool.Value	

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
revoked (if revoked == true)	Tool.Attribute	Revoked
external_references[]	See External References	
description	Tool.Description	
kill_chain_phases.[]	See Kill Chain Table	
tool_version	Tool.Attribute	Tool Version

- *Reports Mapping*

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
created	Report.Published_at	
modified	Report.Attribute	Modified At
name	Report.Value	
description	Report.Description	
labels	Report.Attribute	Label
object_refs	Report.Relationship.Link	
external_references[]	See External References	
revoked (if revoked == true)	Report.Attribute	Revoked

- *Sightings Mapping*

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
count	Event.Attribute	Count
created	Event.published_at	
first_seen	Event.happened_at	
last_seen	Event.Attribute	Last Seen
observed_data_refs	Event.relationship.link	
sighting_of_ref	Event.relationship.link	
where_sighted_refs	Event.relationship.link	
revoked (if revoked == true)	Object.attribute	Revoked
	Event.name	STIX Sighting
	Event.type	Sighting
external_references[]	See External References	
modified	Event.Attribute	Modified

External References

STIX 2.0 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
Object.external_references[].source_name	Object.Attribute	External Reference*
Object.external_references[].external_id	Object.Attribute	External Reference*
Object.external_references[].description	Object.Attribute	External Reference*
Object.external_references[].url	Object.Attribute	External Reference*

* Formatted as: {source_name} ({external_id}): {description} - {url}

Kill Chain Phases

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 Phase

STIX 2.1 Data Mapping

- *Notes Mapping*

STIX 2.1 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
abstract		Object Value
type		"note"
external_references[]	See External References	External Reference
content		Description
authors		Note Author
created	Notes.Published_At	
modified	Notes.Attribute	Modified At
object_refs	object_marking_refs	

- *Incident Mapping*

STIX 2.1 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
name		Object Value
type		"incident"
external_references[]	See External References	External Reference
description		Description
created	Incident.Published_At	

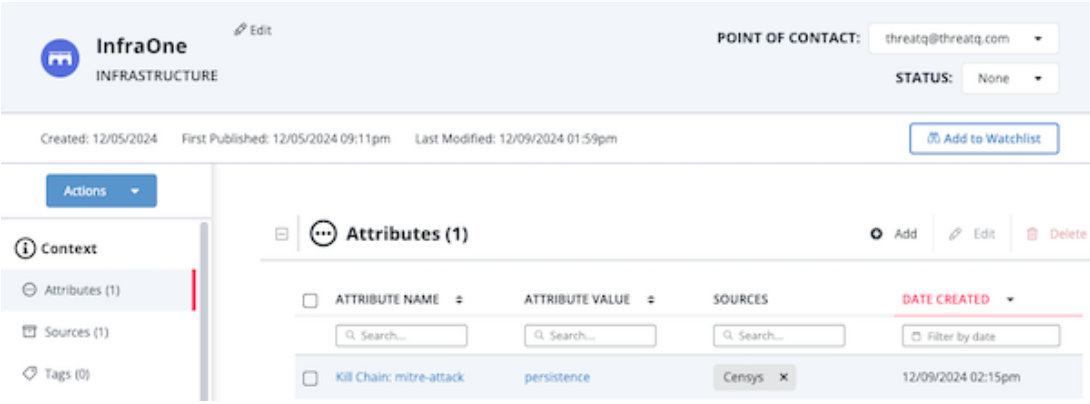
STIX 2.1 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
modified	Incident.Attribute	Modified At
object_refs	object_marking_refs	

- *Infrastructure Mapping*

STIX 2.1 FIELD	THREATQ FIELD MAPPING	THREATQ NAME
name		value
type		"infrastructure"
id		TQUUID
description		Description
created	Infrastructure.Created_At	
modified	Infrastructure.Attribute	Modified At
infrastructure_types		infrastructure_type
kill_chain_phases.[]	See Kill Chain Table	

  - Kill Chain Phase:
    - When you import an infrastructure object that includes Kill Chain Phase information from a STIX file, this information is imported as attributes with the attribute name prefaced with the “Kill Chain:”. For example, if you import the InfraOne infrastructure item, it has an attribute of

KillChain: mitre-attack.



- When you export an infrastructure object that includes Kill Chain: attributes to a STIX file, these attributes are exported as Kill Chain Phase information.

- Infrastructure Types:
  - When you importing an infrastructure object, we convert the list infrastructure_types from the STIX field into attributes with the name infrastructure_type (singular) and setting their respective values.
  - When you export an infrastructure object, these attributes are exported as infrastructure_types information.

External References

STIX 2.1 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*

STIX 2.1 FIELD	THREATQ FIELD MAPPING	THREATQ NAME

* Formatted as: {source_name} ({external_id}): {description} - {url}

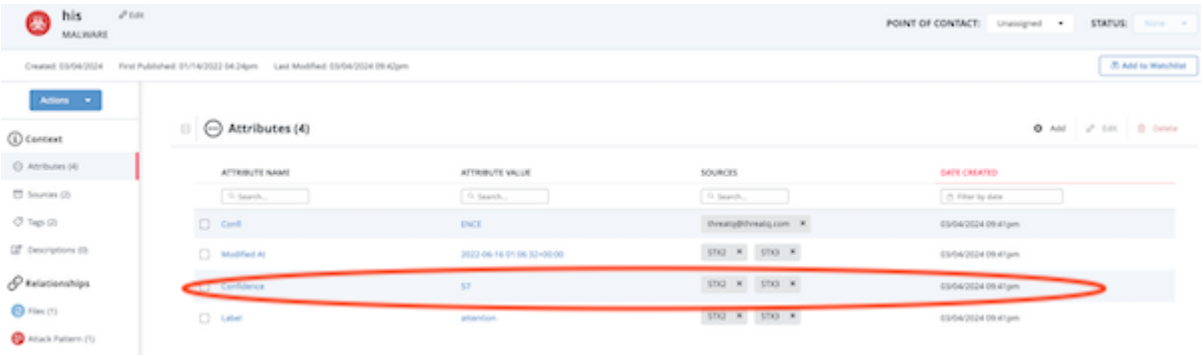
Kill Chain Phases

STIX 2.1 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

Common Properties

Confidence Values:

ThreatQ allows you to import system object Confidence values from STIX 2.1 files as attributes. Confidence is an optional value that specifies the confidence of the object creator in their data on a scale from zero to one hundred.



Location Keys:

When you export system objects with the following location keys as attributes to a STIX file, the export process converts these attributes to STIX location objects: latitude,

region, city, longitude, country, street address, precision, administrative area, postal code. STIX imports of location objects convert these objects to attributes.

Tasks

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor

Custom Role:

- Action Permissions: Objects & Context - Objects (all object types) **OR** Data Access Permissions: Task
- Action Permissions: Individual Object Context & Actions

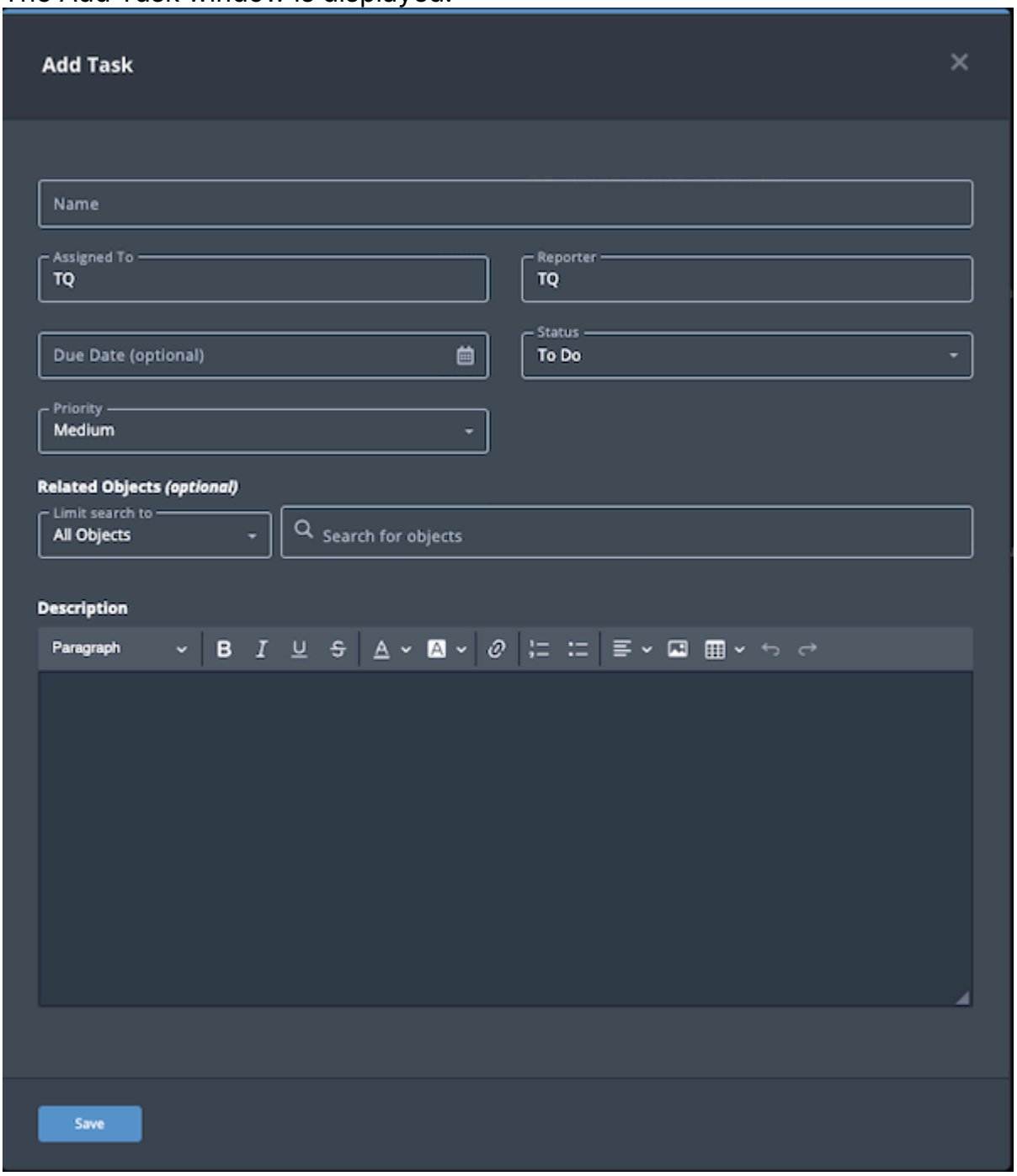
ThreatQ allows you to create and assign tasks to yourself or other users in the platform.

Once tasks are included in your deployment, you can add contextual information and correlate them with Indicators, Events, Adversaries, Signatures, and Files. You can also add comments, change the task priority, change the task status, and delete the task.

Assigning a Task

Complete the following steps to assign a task in ThreatQ.

1. From the main menu, choose **Create > Task**.
   The Add Task window is displayed.



2. Populate the following fields:

FIELD	DESCRIPTION
Name	Add a task name.

FIELD	DESCRIPTION
Assigned To	Enter the person to which the task is assigned. This field defaults to your ThreatQ display name.
Reporter	Enter the person who reported the task. This field defaults to your ThreatQ display name.
Due Date	Use the date picker to select a due date
Status	Select one of the following statuses: ◦ To Do ◦ In Progress ◦ Review ◦ Done
Priority	Select one of the following task priorities: ◦ Low ◦ Medium ◦ High
Related Objects	Optional. Select any related objects you need to link to the Task.
Description	Enter a brief description of the task object. Any description you add during object creation defaults to a Source value of ThreatQ System.

3. Click **Save**.
   The assignee receives a Notification Center alert about the task. This alert includes a link to the assigned task.

Managing Tasks

After a task is created, you can manage it on the task's Details page.

The following table describes the actions you can take to manage your tasks on a Task Details page.

TO	YOU CAN...
Change task priority	Choose the **Priority** drop-down and select a new priority.
Change task status	Choose the **Status** drop-down and select a new status.
Add Attributes, Comments, Relationships, and Sources	Choose the **Add Context** drop-down and select an item.
View and Add Comments	Choose **Comments**.
View the Audit Log	Choose **Audit Log**.
Request Investigation Access	1. Choose **Investigations**. 2. Click the related investigation to open the Access Denied window. 3. Click the **Request Access** button. When you click this button, the investigation owner receives a Notification Center alert indicating you have requested access to the investigation.

Tools

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor

Custom Role:

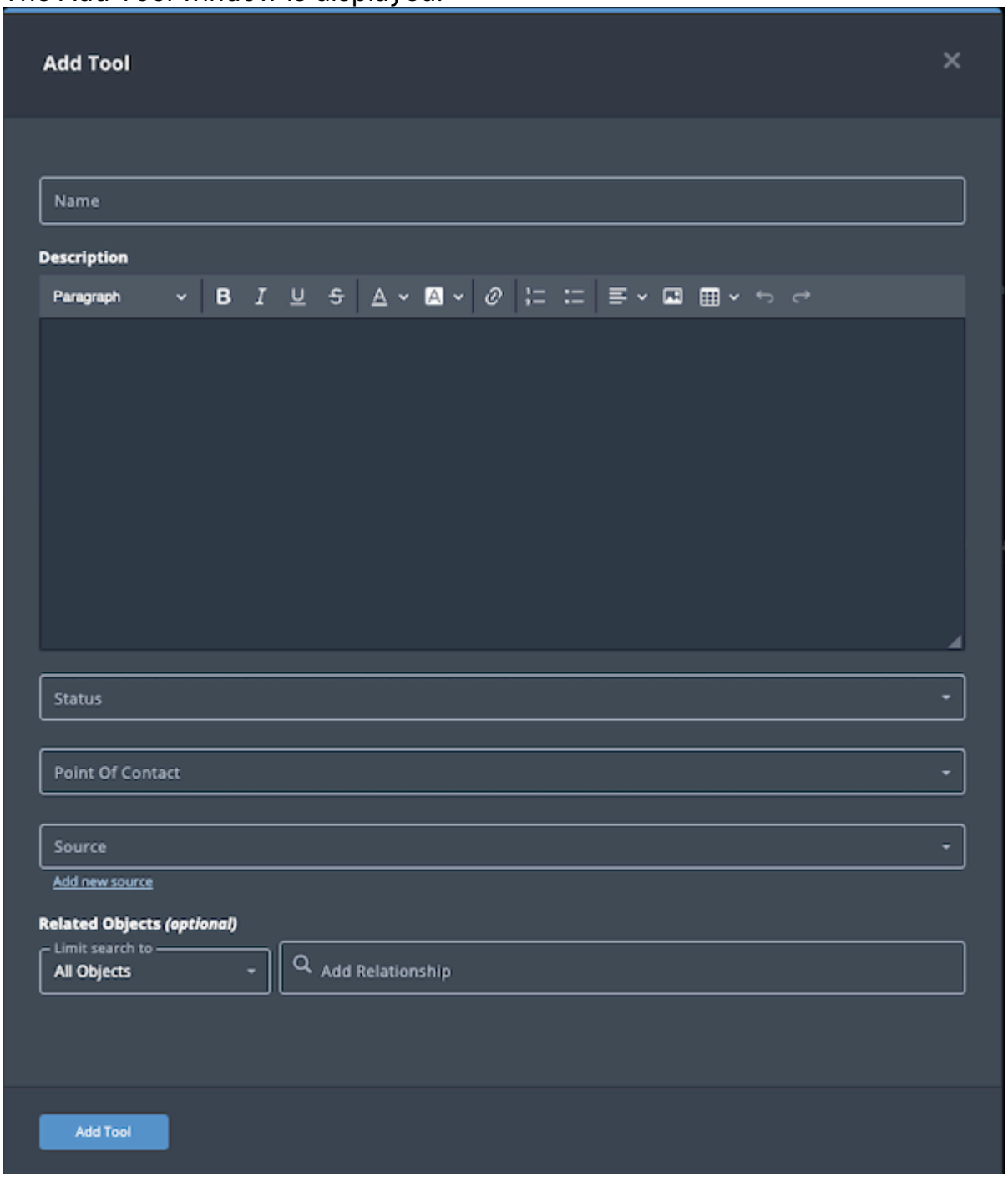
- Action Permissions: Objects & Context - Objects (all object types) **OR** Data Access Permissions: Tool
- Action Permissions: Individual Object Context & Actions
  Note: If a user has View Only permission for Sources, system object creation modals default to the user's login as the object source.

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 window is displayed.



2. Populate the following fields:

FIELD	DESCRIPTION
Name	Add a tool name.
Description	Enter a brief description of the tool. Any description you add during object creation defaults to a Source value of ThreatQ System.
Status	Optional field. Click the Status field to assign a status to the tool. Tool statuses are configured in the Object Statuses tab in the Object Management page. If none are configured, this field is not displayed.
Point of Contact	Optional field. Click the field to select the ThreatQ display name of the point of contact for the tool.
Source	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.

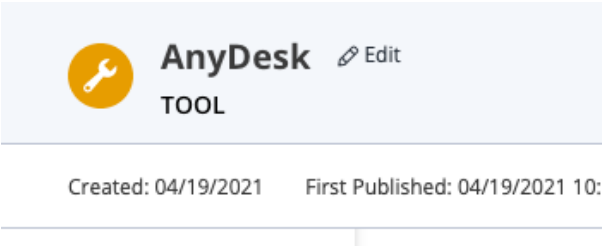
3. Select any **Related Objects** you need to link to the Tool. This field is optional.
4. Click **Add Tool**.

Adding Context

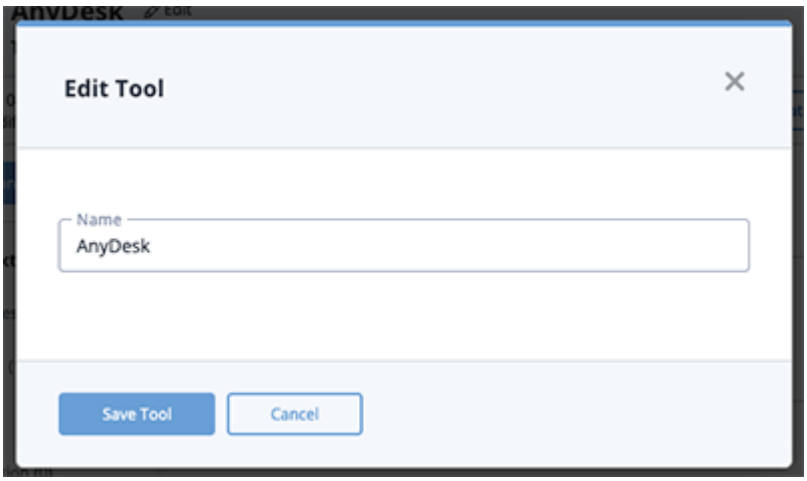
See the About Object Details Page section and its topics for details on adding context to an object such as adding sources, attributes, and related objects.

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**.

Changing the Point of Contact

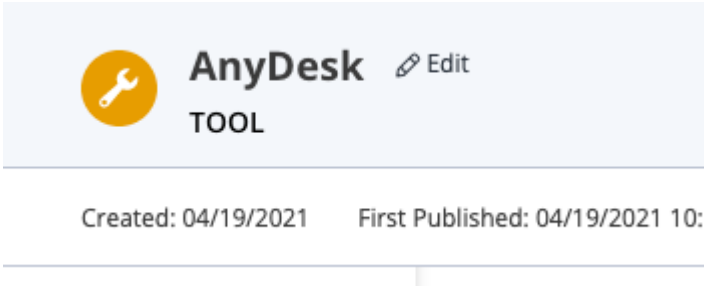
THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role - Action Permissions: Objects & Context - Objects, Individual Object Context & Actions - Point of Contact

1. Locate and click the system object.
2. From the object details page, click the Point of Contact field.
3. Use the field's scroll or search option to locate and select a new user as the object's point of contact or to change the point of contact to Unassigned.

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**.

TTPs

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor

Custom Role:

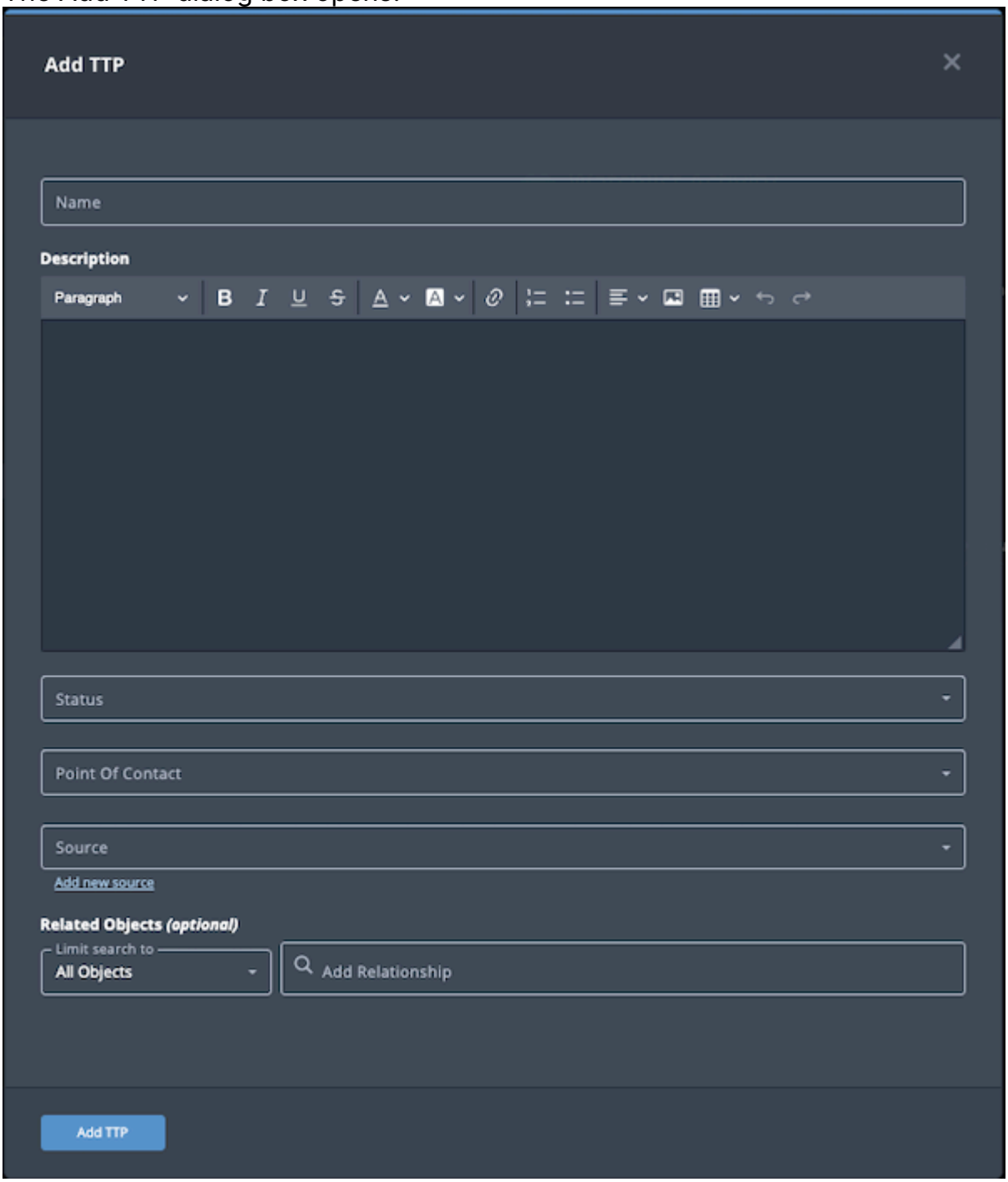
- Action Permissions: Objects & Context - Objects (all object types) **OR** Data Access Permissions: TTP
- Action Permissions: Individual Object Context & Actions
  Note: If a user has View Only permission for Sources, system object creation modals default to the user's login as the object source.

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. Populate the following fields:

FIELD	DESCRIPTION
Name	Add a TTP name.
Description	Enter a brief description of the TTP. Any description you add during object creation defaults to a Source value of ThreatQ System.
Status	Optional field. Click the Status field to assign a status to the TTP. TTP statuses are configured in the Object Statuses tab in the Object Management page. If none are configured, this field is not displayed.
Point of Contact	Optional field. Click the field to select the ThreatQ display name of the point of contact for the TTP.
Source	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.

3. Select any **Related Objects** you need to link to the TTP. This field is optional.
4. Click **Add TTP**.

Adding Context

See the About Object Details Page section and its topics for details on adding context to an object such as adding sources, attributes, and related objects.

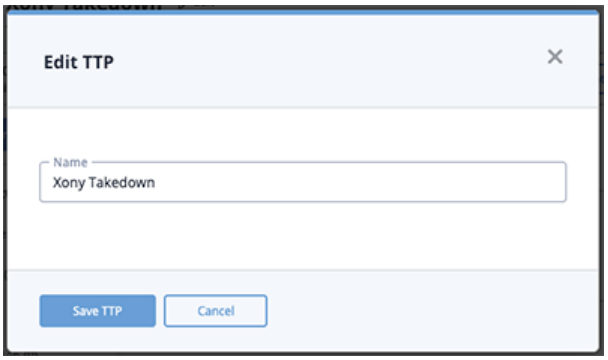
Editing a TTP

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.



3. Make the desired change to the TTP name and click **Save TTP**.

Changing the Point of Contact

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role - Action Permissions: Objects & Context - Objects, Individual Object Context & Actions - Point of Contact

1. Locate and click the system object.
2. From the object details page, click the Point of Contact field.
3. Use the field's scroll or search option to locate and select a new user as the object's point of contact or to change the point of contact to Unassigned.

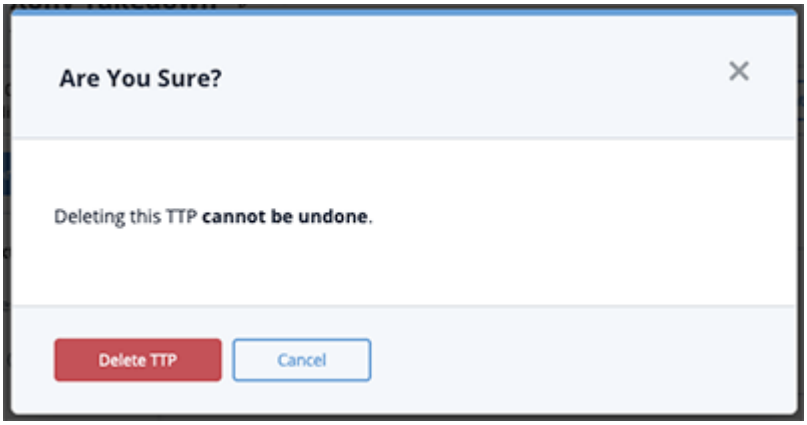
Deleting a TTP

1. Locate and click on the TTP.

The TTP's details page opens.

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

   A confirmation dialog box appears.



3. Click on **Delete TTP**.

Vulnerabilities

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor

Custom Role:

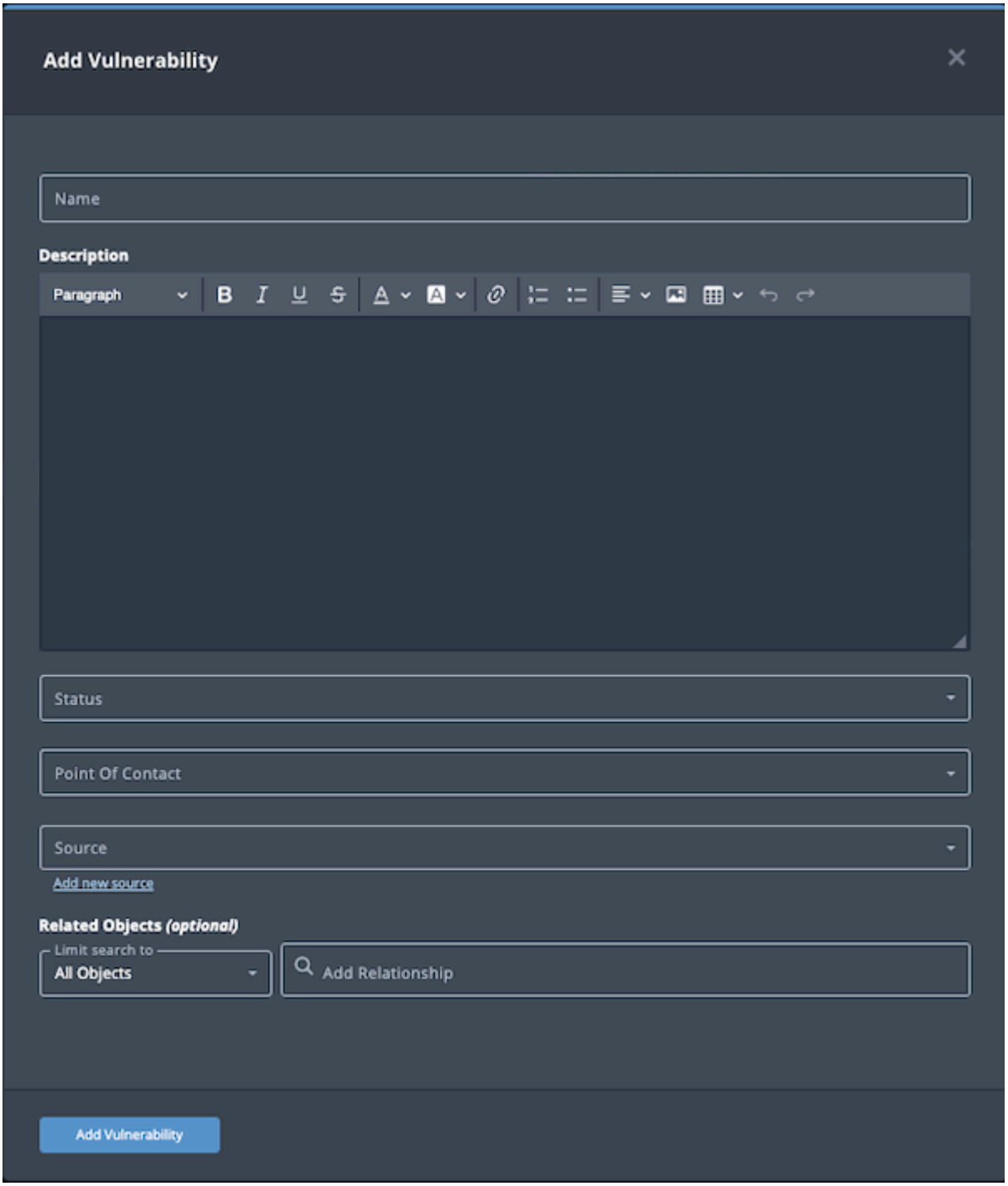
- Action Permissions: Objects & Context - Objects (all object types) **OR** Data Access Permissions: Vulnerability
- Action Permissions: Individual Object Context & Actions
  Note: If a user has View Only permission for Sources, system object creation modals default to the user's login as the object source.

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. Populate the following fields:

FIELD	DESCRIPTION
Name	Add a vulnerability name.

FIELD	DESCRIPTION
Description	Enter a brief description of the vulnerability. Any description you add during object creation defaults to a Source value of ThreatQ System.
Status	Optional field. Click the Status field to assign a status to the vulnerability. Vulnerability statuses are configured in the Object Statuses tab in the Object Management page. If none are configured, this field is not displayed.
Point of Contact	Optional field. Click the field to select the ThreatQ display name of the point of contact for the vulnerability.
Source	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.

3. Select any **Related Objects** you need to link to the vulnerability. This field is optional.
4. Click **Add Vulnerability**.

Adding Context

See the About Object Details Page section and its topics for details on adding context to an object such as adding sources, attributes, and related objects.

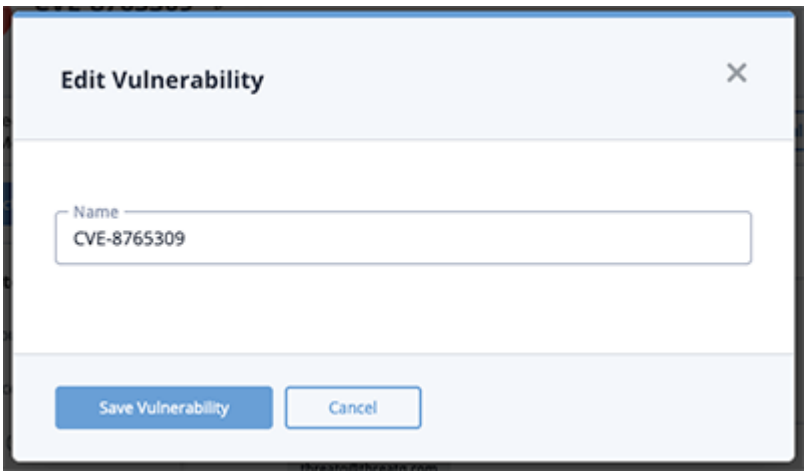
Editing a Vulnerability

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**.

Changing the Point of Contact

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role - Action Permissions: Objects & Context - Objects, Individual Object Context & Actions - Point of Contact

1. Locate and click the system object.
2. From the object details page, click the Point of Contact field.
3. Use the field's scroll or search option to locate and select a new user as the object's point of contact or to change the point of contact to Unassigned.

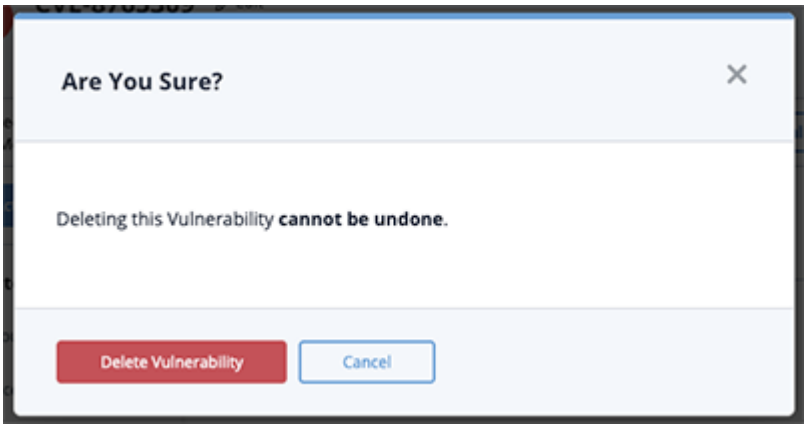
Deleting a Vulnerability

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.

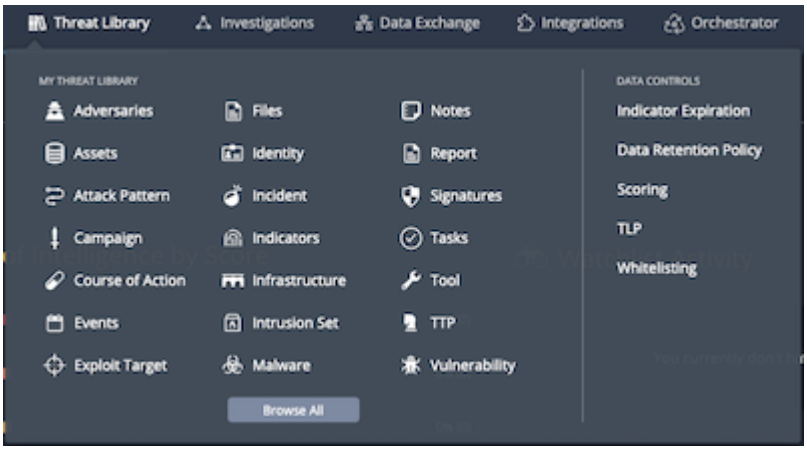


3. Click on **Delete Vulnerability**.

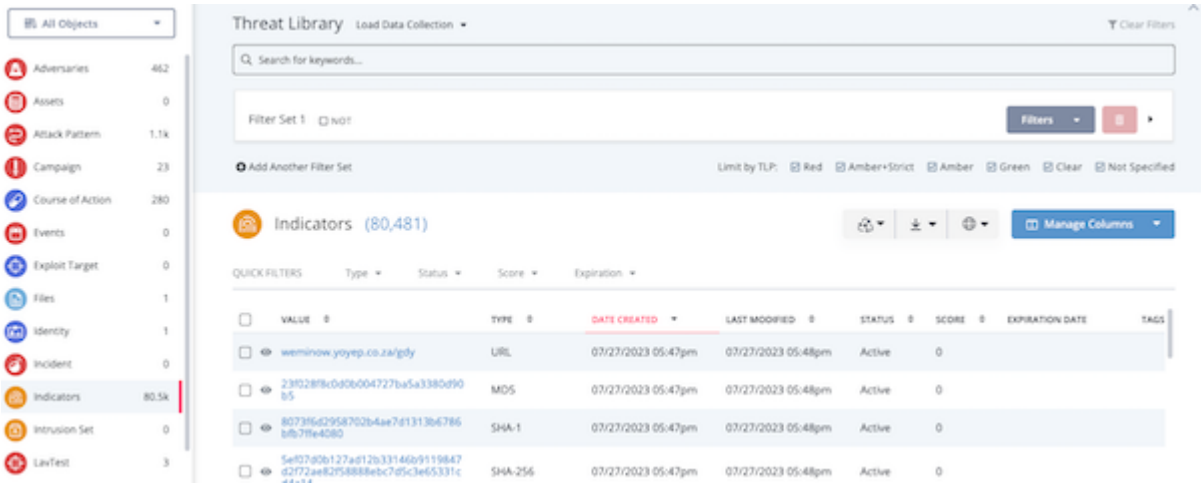
Threat Library

About Threat Library

The Threat Library is your interactive hub for managing the threat intelligence ingested into the 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.

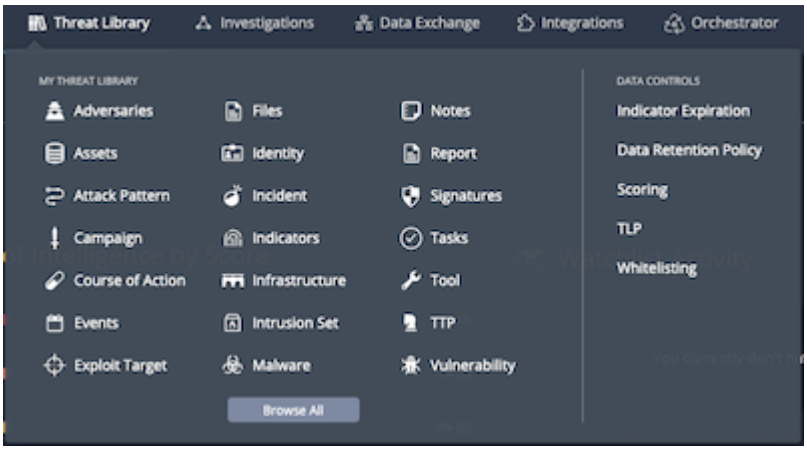
Selecting Object Type View

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**.



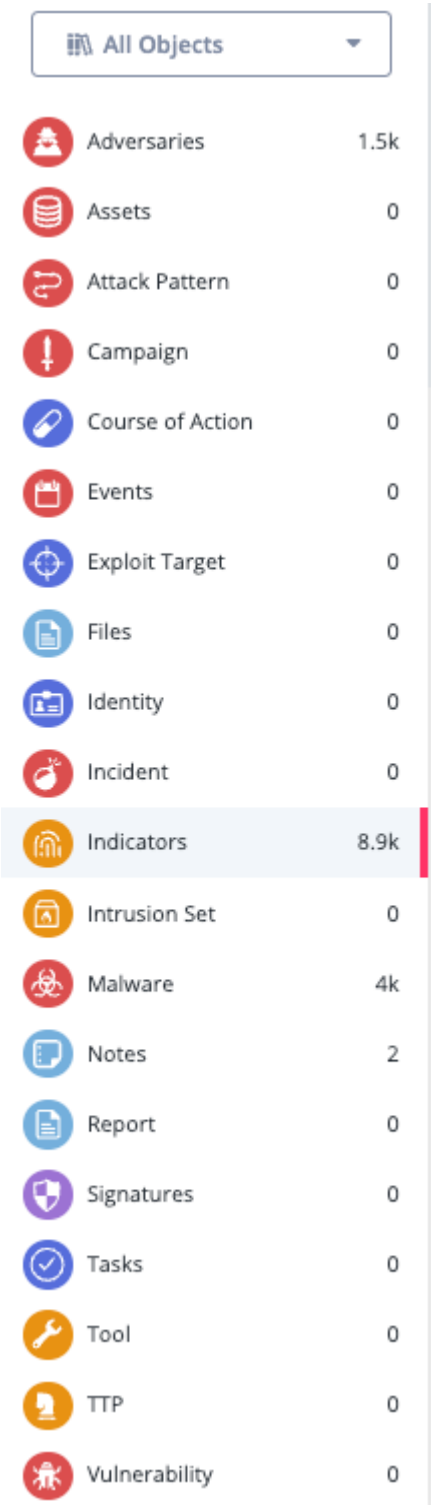
The Advanced Results page opens with the applied object type filter.

> 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.

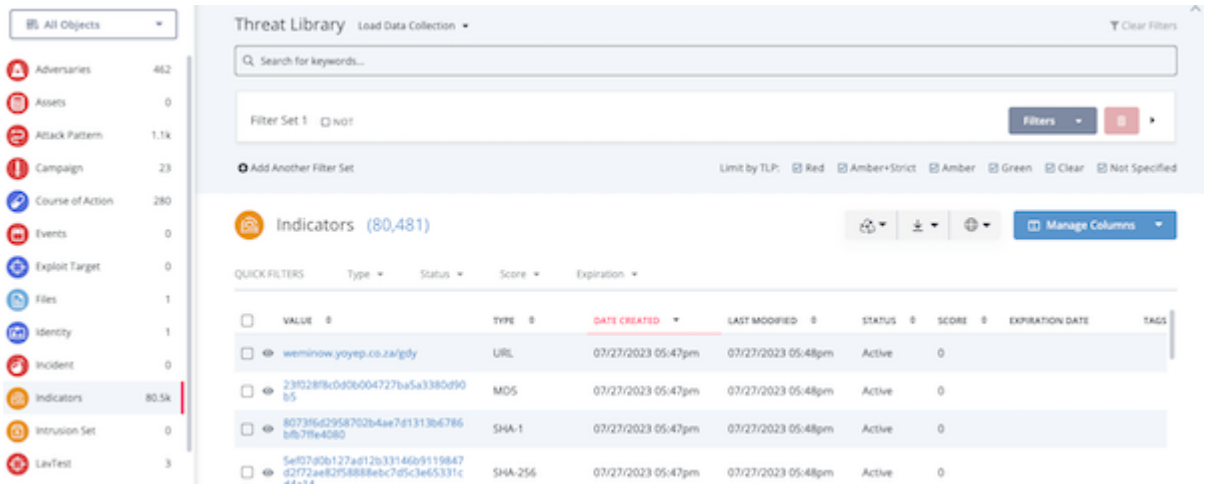
You can either use the **Object Type** dropdown list or click directly on a object type listed in the menu.



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.

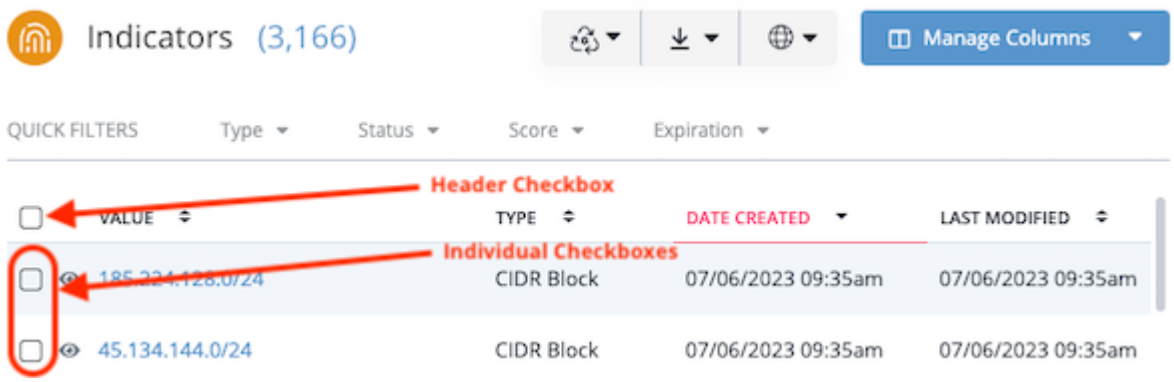


2. Click the **Manage Columns** button.
3. Use one of the following methods to locate the columns you want to display/hide:
   - Scroll through the list of column options.
   - Begin typing the column name until it is displayed below the search field.
4. To display a column, check the checkbox next to the column name.
5. To hide a column, uncheck the checkbox next to the column name.

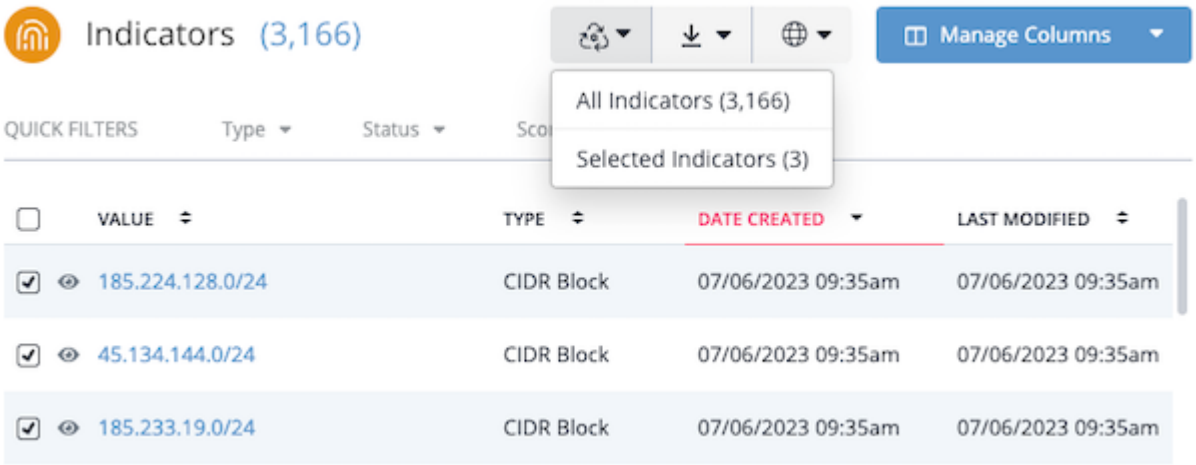
> You can click the values in related object columns to view a list of the related objects. For instance, if the Related Adversaries column lists a value of 10, you can click the 10 to view a list of the ten related adversaries. To return from this list to your original review, use your browser back 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.



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.



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

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role - Data Access Permissions: Search results include only object types for which the user has Create, Edit, Delete, or View Access Only. The Create *<object type>* link appears only if the user has Create, Edit, Delete permission for that object type.

The ThreatQ Basic Search feature provides a fast, intuitive way for users to locate objects across the ThreatQ platform without navigating through multiple modules or object lists. Positioned prominently in the ThreatQ navigation bar next to the Create button, Basic Search is designed to accelerate investigations, improve analyst efficiency, and surface relevant intelligence with minimal friction .

Basic Search operates across **all core ThreatQ object types**, including but not limited to Indicators, Events, Adversaries, Files, and Signatures. Rather than performing deep field-level queries, it focuses on high-level object attributes, enabling broad discovery and quick pivots during triage and analysis workflows.

What Basic Search Can Match

When a query is submitted, ThreatQ evaluates multiple top-level data points across objects, including:

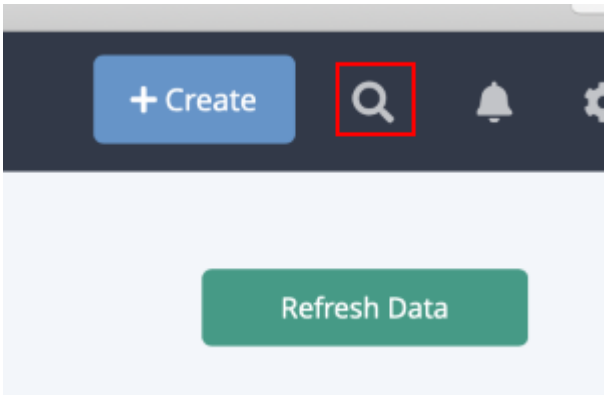
- Network and host-based indicators
- Attachment titles, hashes, and keywords
- Object attributes
- Adversary names
- Event titles

For example, searching for google.com does not only return an exact FQDN match. It also surfaces related objects such as subdomains, URLs, and even email indicators associated with the same root domain, providing immediate contextual breadth .

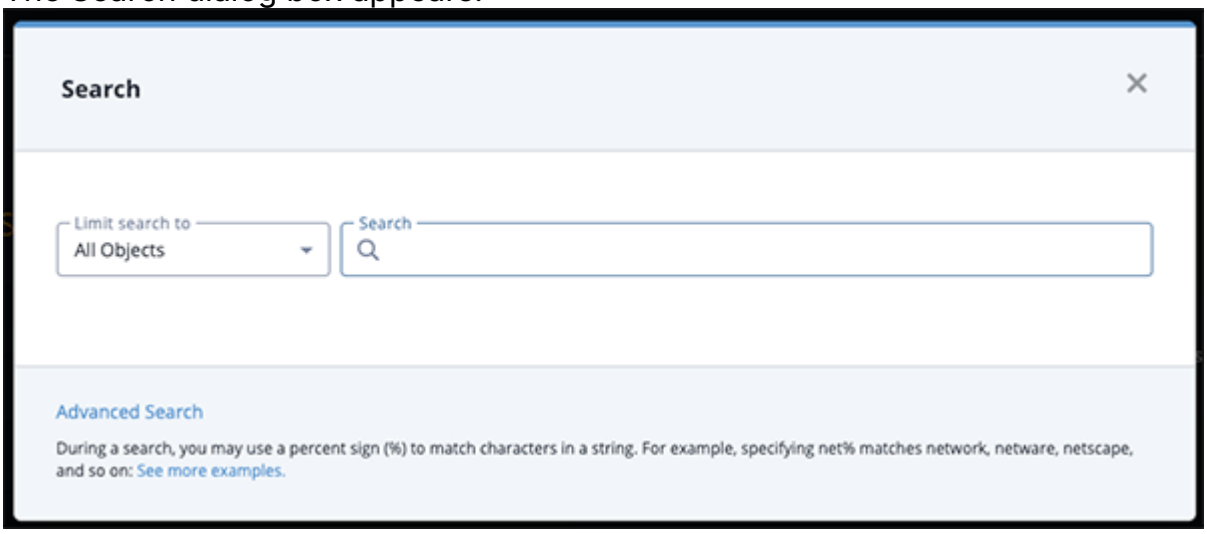
Performing a Basic Search

The Basic Search workflow is intentionally streamlined:

1. Select the Search icon in the ThreatQ navigation.

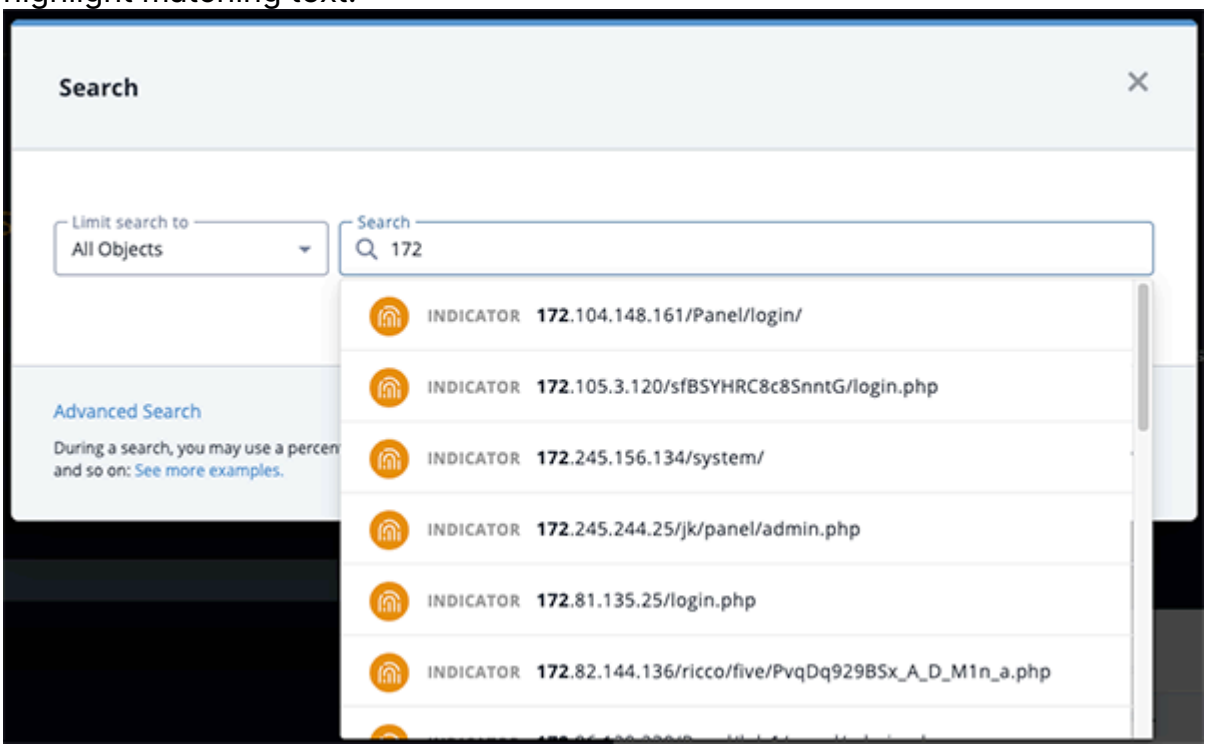


The Search dialog box appears.



2. (Optional) Use the Limit search to dropdown to constrain results to a specific object type.
3. Enter search criteria into the search field.

4. Review type-ahead suggestions, which dynamically appear as you type and highlight matching text.



5. Select a result to navigate directly to the object's details page.

> If a single match is found, ThreatQ automatically opens the corresponding object. If no results are returned, users are guided to leverage Threat Library Advanced Search for more granular querying.

Search Scope and Object Filtering

The **Limit Search** dropdown allows users to narrow results to a specific object class, such as Adversaries or Indicators. This is particularly useful in environments with large data volumes, where the same term may exist across multiple object types.

Limiting the search also affects object creation behavior. If a search term yields no results and the search is constrained to a specific object type, the **Create** option automatically routes users to the appropriate object creation form, streamlining data entry workflows.

Wildcards and Search Types

ThreatQ Basic Search supports flexible pattern matching through the use of the percent sign (%) wildcard. Wildcards allow users to control how strictly or broadly their search terms are evaluated, making the feature effective for both precise lookups and exploratory analysis .

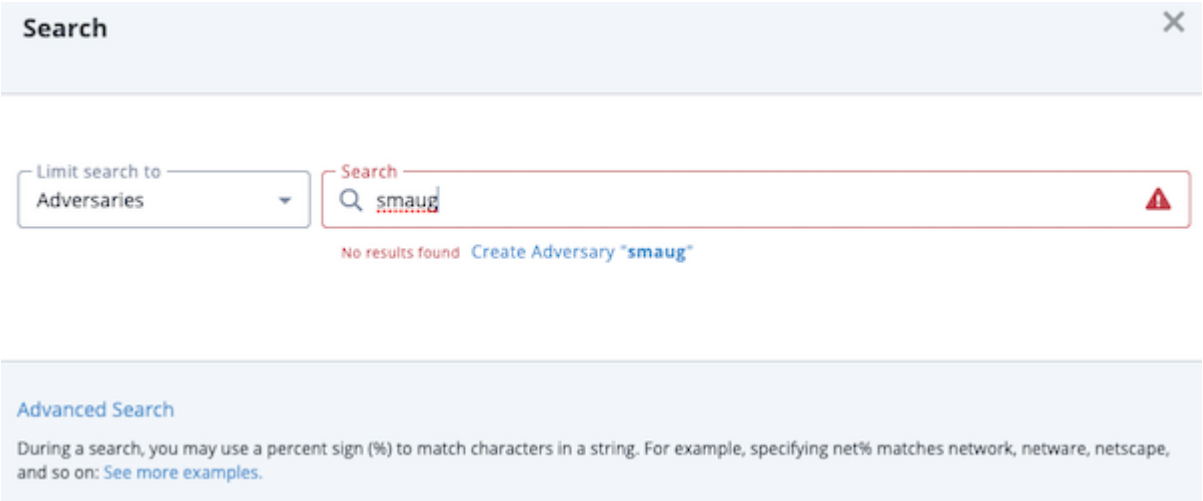
SEARCH TYPE	PATTERN	BEHAVIOR	EXAMPLES	NOTES
Exact Term Match	`TERM`	Matches only the exact term or phrase.	Searching for the term `target german` will result in the application only finding `target german`. It will not find similar results like `targeting german` or `retarget german`.	Best used when the exact object name or phrase is known.
Starts with Search	`TERM%`	Matches any value that begins with the specified term.	Searching for `target%` will return results such as `target`, `targeting`, and `targets`. It will not find not find results that do not begin with the search term like `retarget`.	This is useful for discovering naming variations or object families that share a common prefix.
Ends with Search	`%TERM`	Matches any value that ends with the specified term.	Searching for `%german` will return results such as `german`, `target  german`, and `east german`. It will not find not find results that do not end with the search term like `germanic`.	Common use cases include suffix-based searches such as file extensions or domain endings.

SEARCH TYPE	PATTERN	BEHAVIOR	EXAMPLES	NOTES
Ends with Term Search	`% TERM`	Matches any value preface by another word.	Search for `% bear` will result in the application returning results such as `red bear`, `black bear`, and `brown bear`. It will not find terms such as `bear blue`.	This is useful for discovering variations that utilize the search term in its naming convention.
Contains Search	`%TERM%`	Matches the term anywhere within the value.	Search for `%target%` will return results such as `target`, `targeting`, and `retarget`.	This is the most flexible and expansive option, well-suited for exploratory searches where the exact structure of the data is unknown.
Character Search	`T%M`	Matches any term that contains both characters.	Searching `b%r` will return results such as `black bear`, `black rust`, and `blue rubber`.	This is useful for narrowing down the search for objects without knowing the exact name.

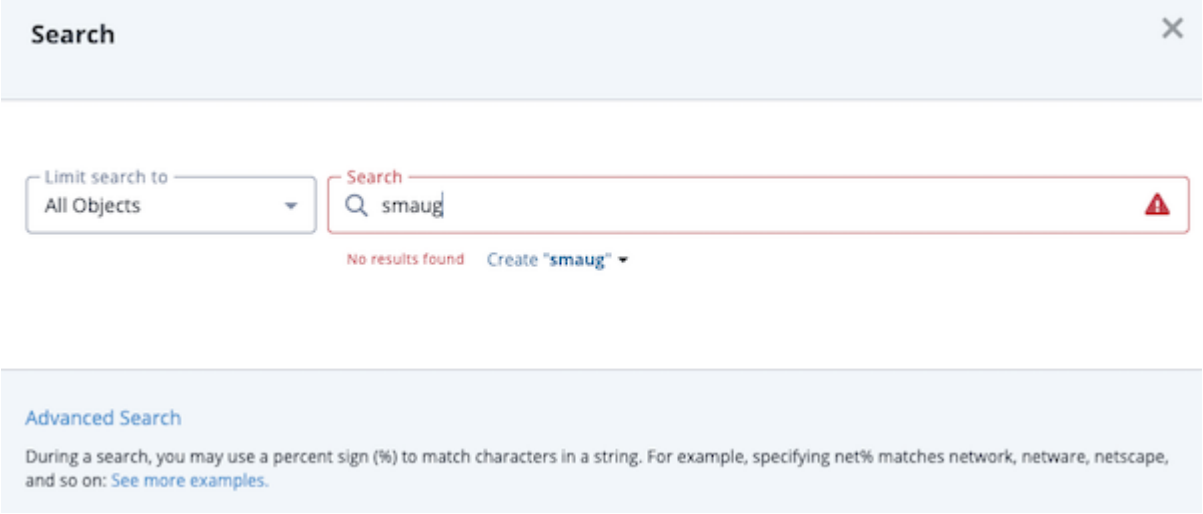
Creating an Object During a Basic Search

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.

You cannot use the **Create** link to add a new investigation.



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.



Best Practices and Usage Guidance

- Start with an exact search and progressively broaden using wildcards if results are too limited.
- Use Starts With or Ends With searches to manage large result sets more effectively.
- Apply Contains searches sparingly for very short terms, as they may return excessive matches.
- Leverage object type filtering to improve relevance and reduce noise in mature ThreatQ environments.

- Contact ThreatQuotient Support for any additional search questions or issues.

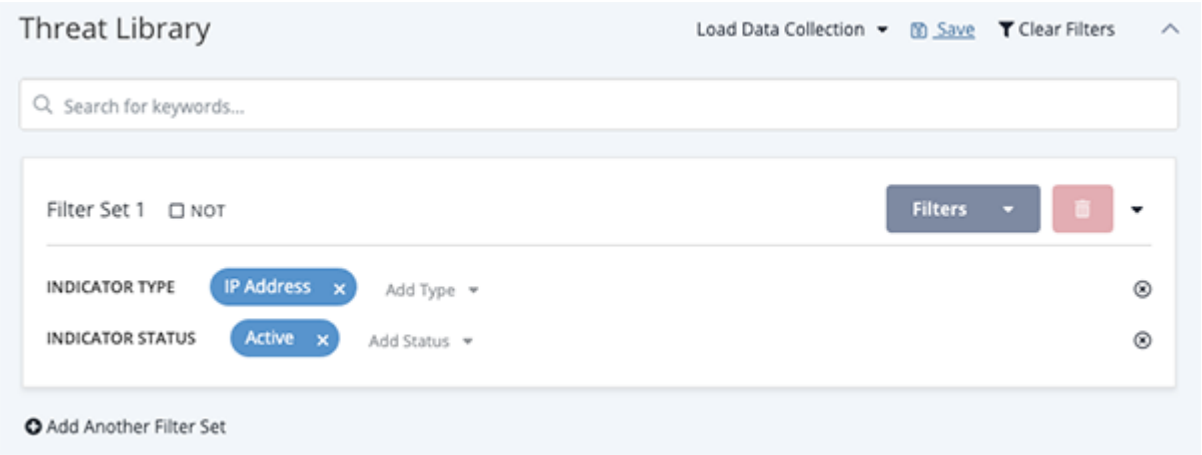
Building Searches with Filter Sets

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 About Managing Search Results topic for more details.

Adding Filter Sets

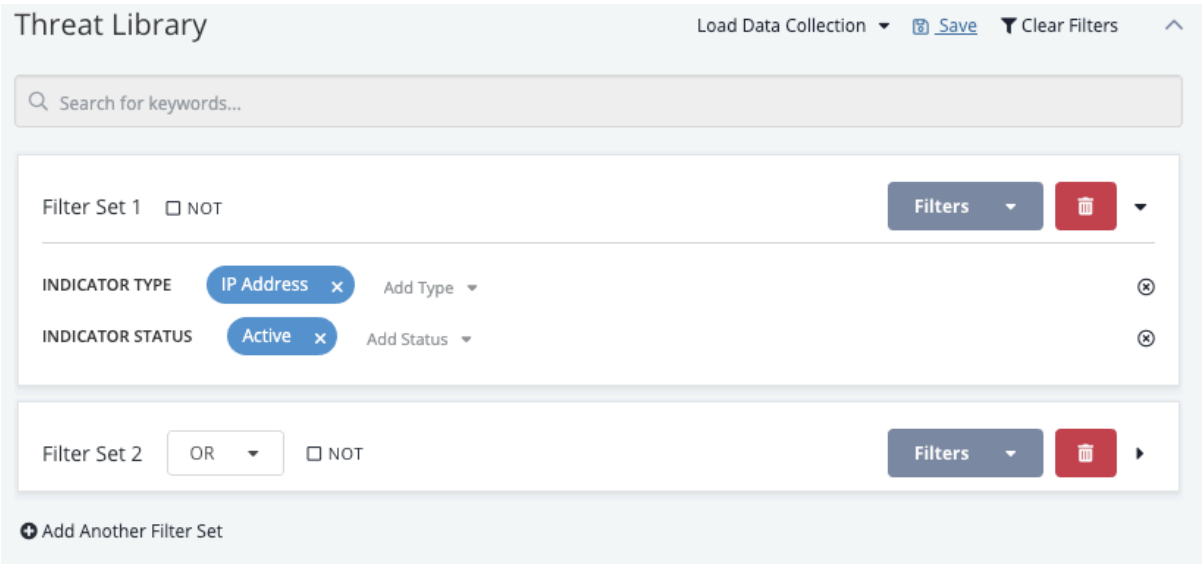
1. Use the **NOT** checkbox to determine if the filters in the initial filter set will be used to include or exclude Threat Library objects.
2. Select one or more filters for the search.



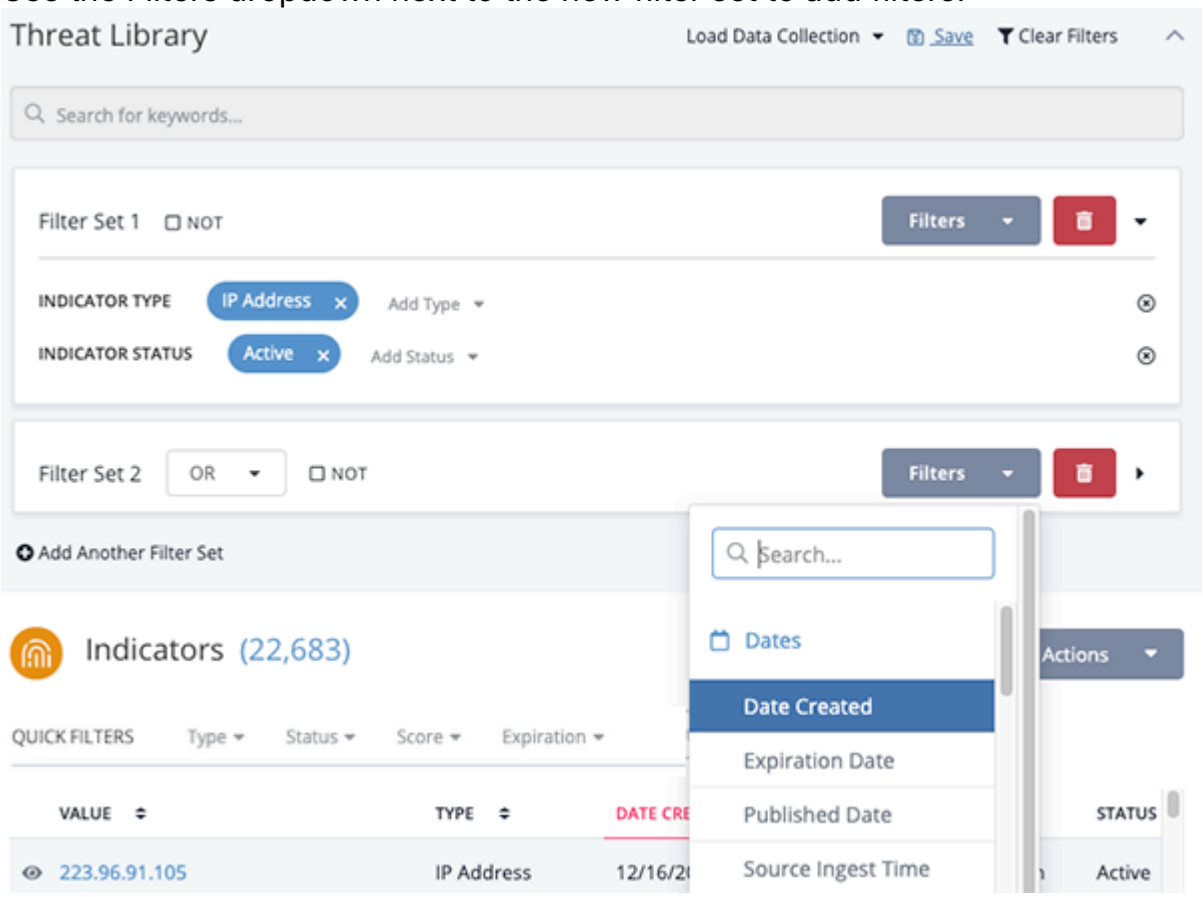
   You can use the search box provided at the top of the filters dropdown to narrow down the list of available filters.

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

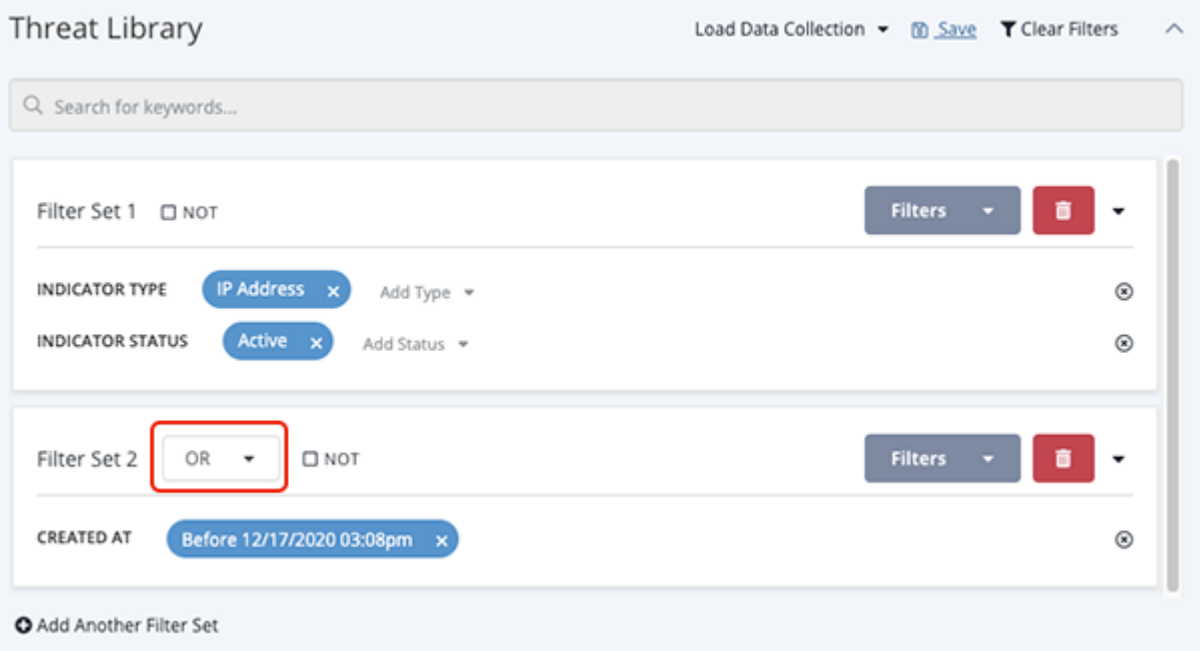
A new Filter Set table will load below the first set.



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



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

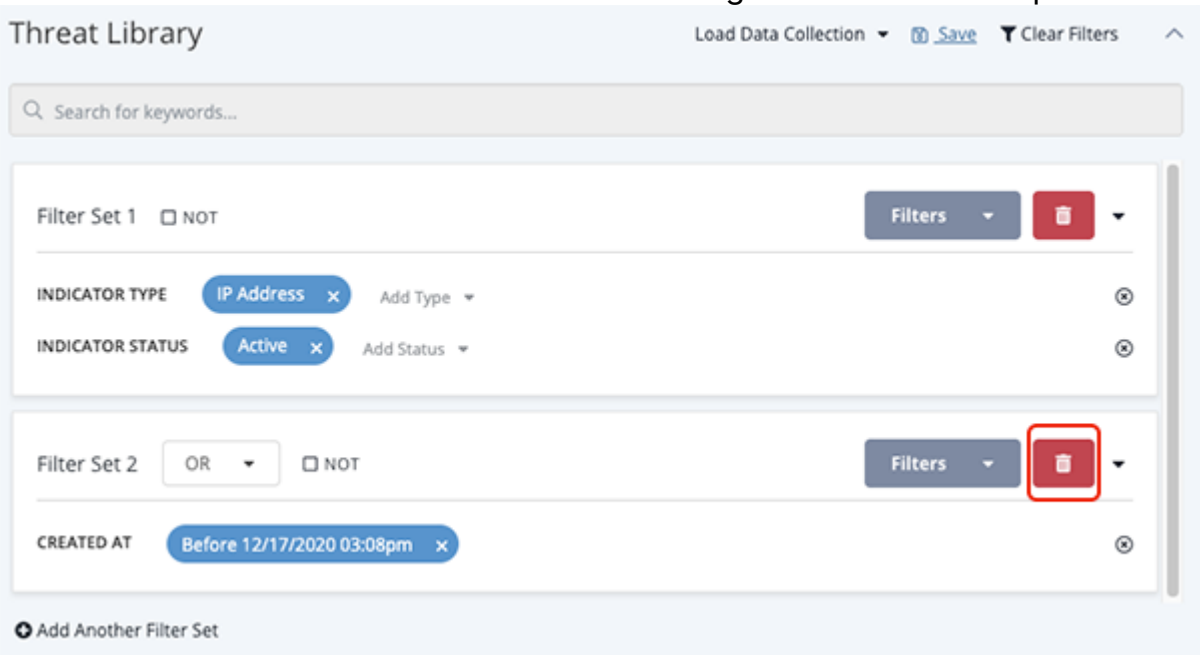


Repeat steps 3-6 to add additional filter sets.

Deleting Filter Sets

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

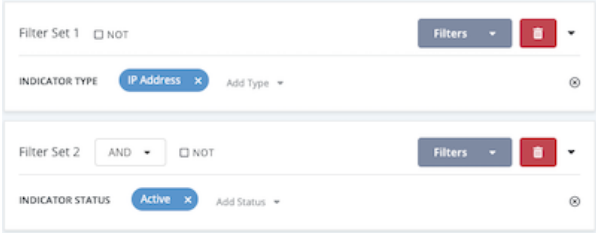
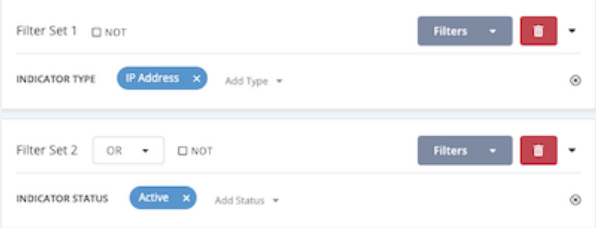
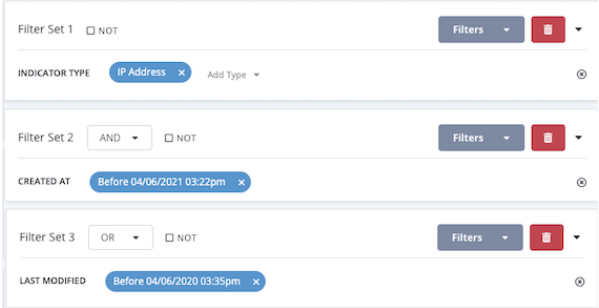
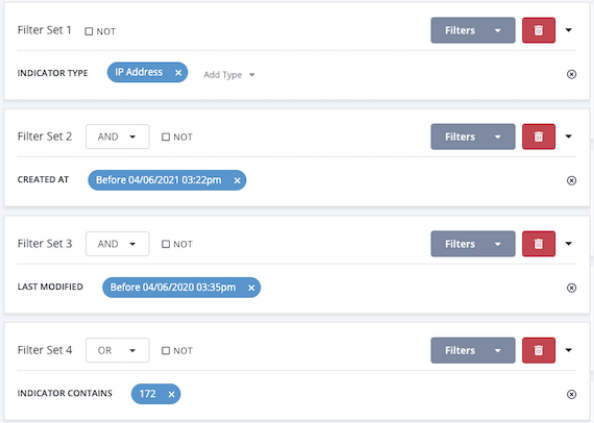
1. Click on the delete icon located next to the right of the Filters dropdown.

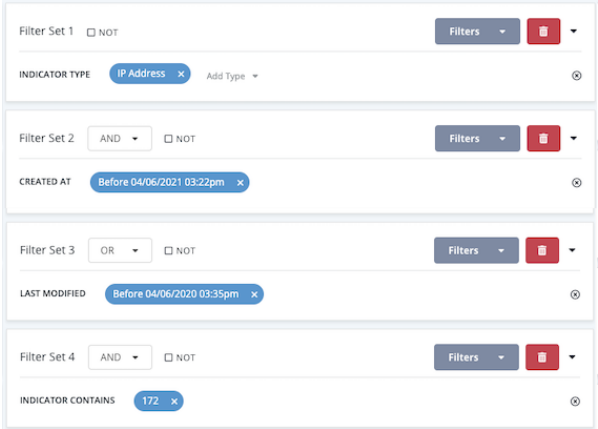


You can click on **Clear Filters**, located above the filter sets, to remove all filter sets from the current search.

And/Or Order of Operations

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

SCENARIO	ORDER	EXAMPLE
Single AND	Filter 1 AND Filter 2	
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)	

Context Filters

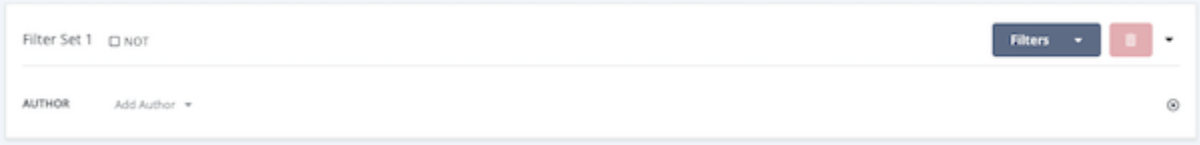
Context filters allow you to filter advanced search results by specific details associated with an object.

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.

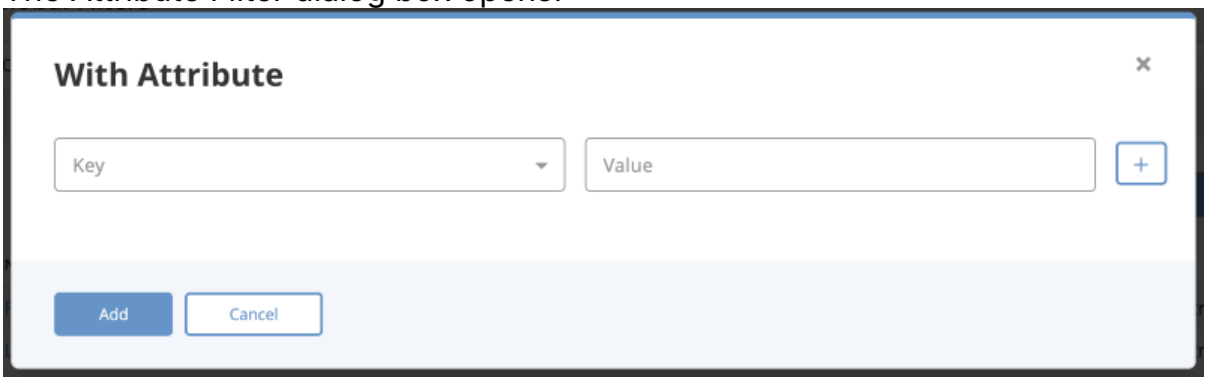
   > The Author column only lists an object's source author(s). It does not list an object's attribute source author(s). If your author filter only matches an object's attribute source author, the column is blank.

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:
   - 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**.

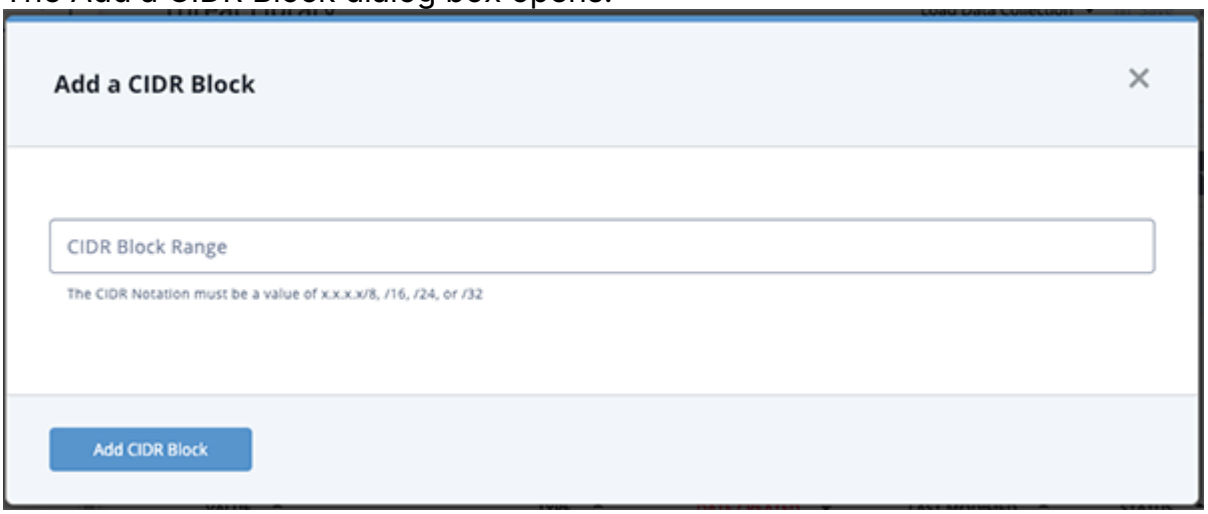
   The filtered results will display any indicator that has both of those attributes

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.



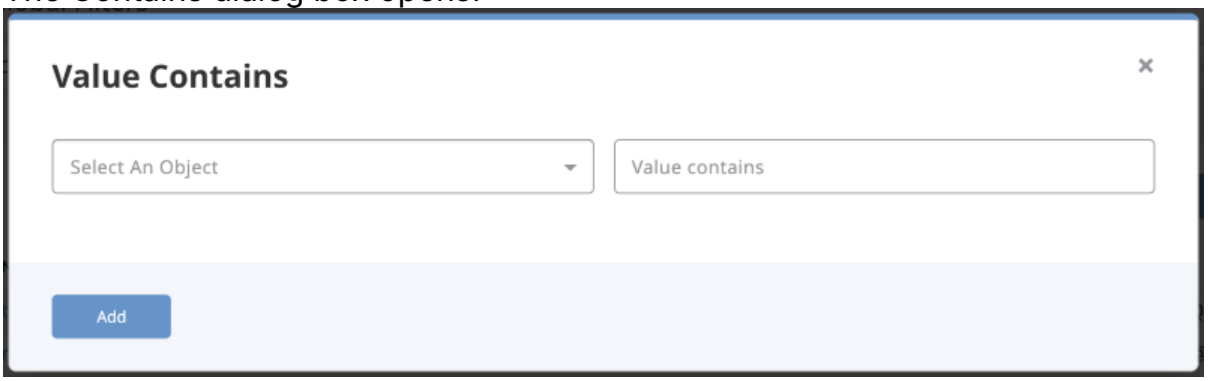
2. Enter the CIDR block in one of the following formats:
   - x.x.x.x/8
   - x.x.x.x/16
   - x.x.x.x/24
   - x.x.x.x/32
3. Click **Add CIDR Block** to apply the filter.

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.



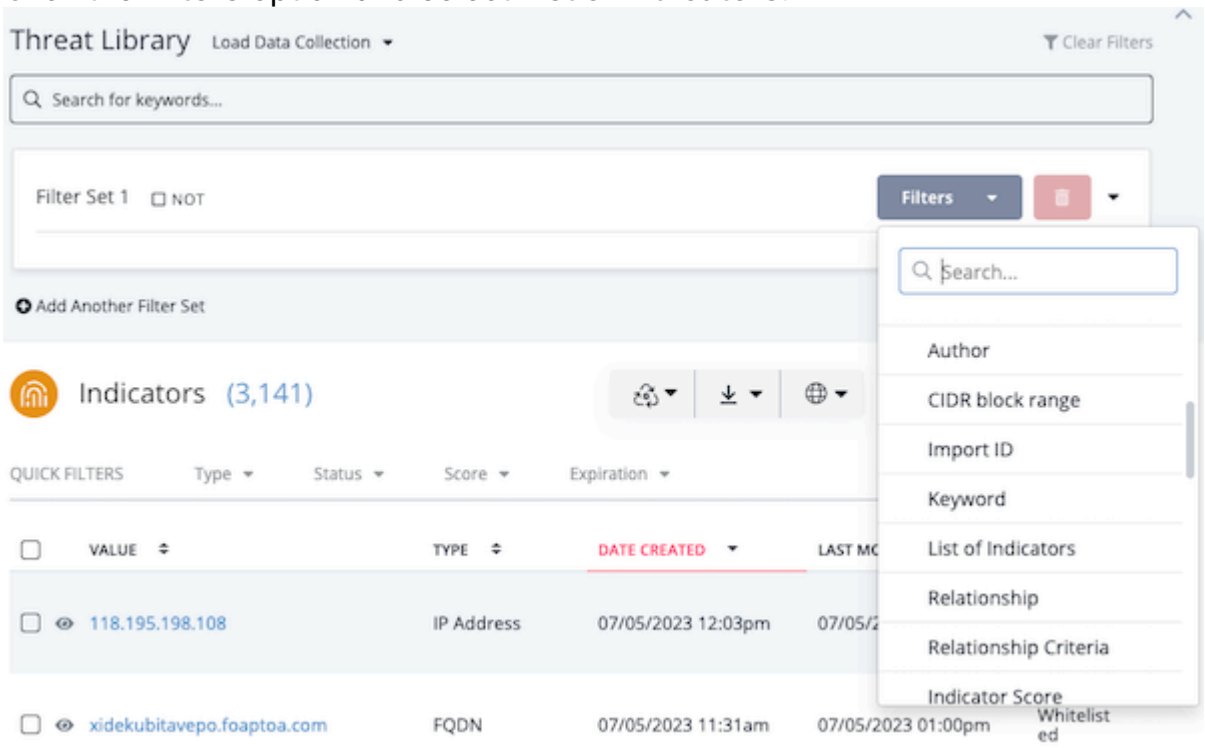
2. Select an **Object**, enter a **Value**, and click **Add** to apply the filter.

Filtering by List of Indicators

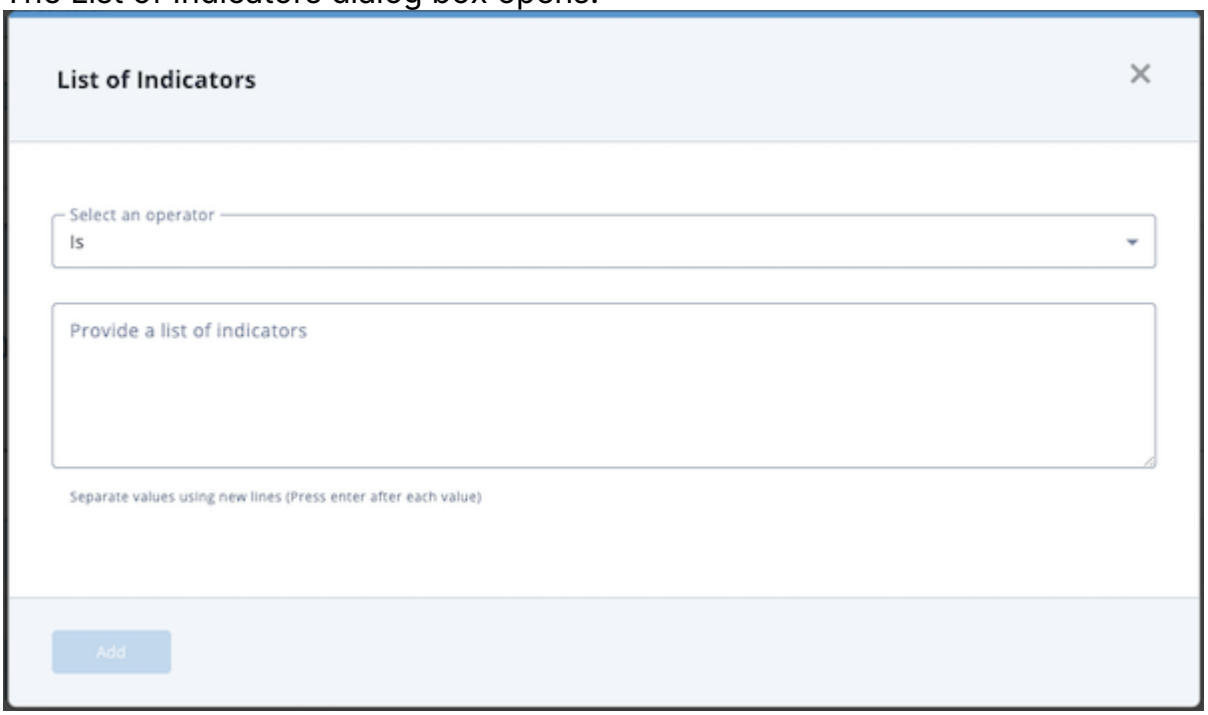
The List of Indicators Filter option allows you to filter the Threat Library by pasting a list of indicators, in raw text.

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

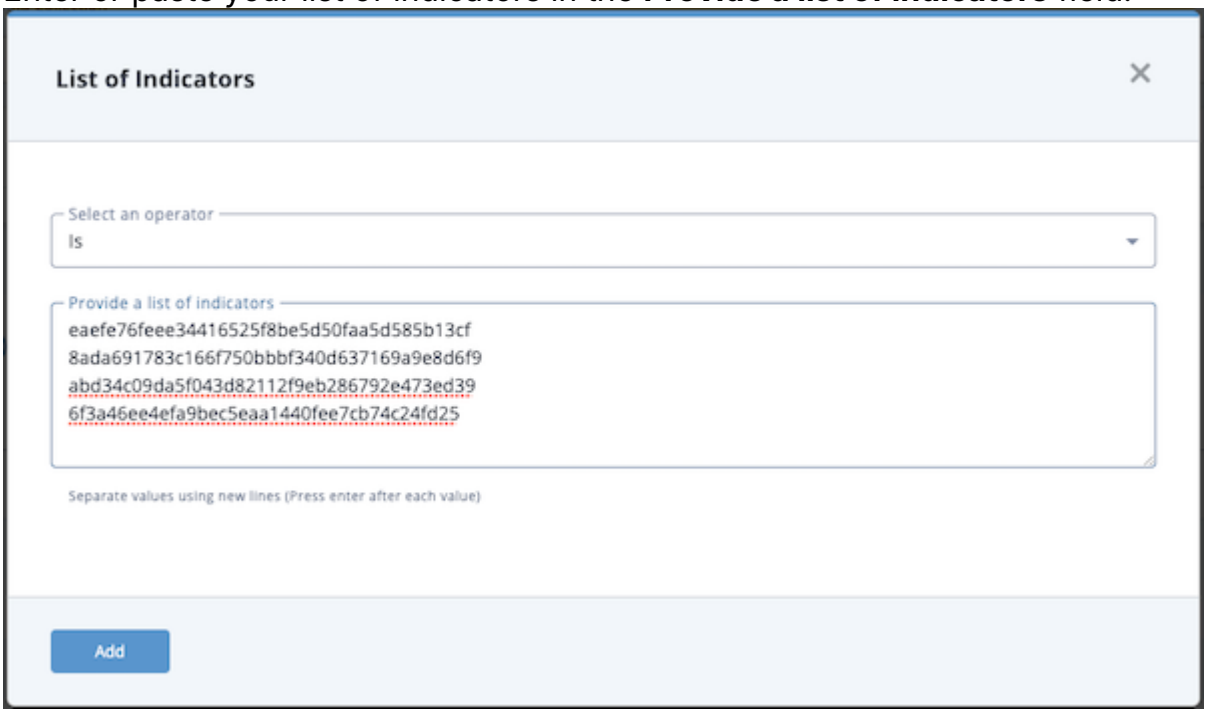
1. Click the **Filters** option and select **List of Indicators**.



The List of Indicators dialog box opens.



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

Keyword searches for phrases return objects that include all the terms in the phrase. For instance, a search for “united kingdom” returns objects that include “united kingdom” instead of objects that include “united” and “kingdom” or “united” or “kingdom”. By default, searches return instances where the search term or phrase is a standalone prefaced by and appended by a space. For instance, a search for “panda” **does not** return “pandas” or “expandability”.

To search for characters in a string, you can use a percent sign (%) or asterisk (*) to specify that characters appear in the position represented by the wildcard. For example, specifying “net%” matches “**net**work” and “**net**ware”. Specifying “%net” matches “bot**net**” and “inter**net**”. Specifying “%net%” matches “ni**net**y” and “hor**net**s”. See the Wildcards and Symbols in Searches section for more examples.

ThreatQ keyword searches apply to different fields based on system object type.

SYSTEM OBJECT/OBJECT CONTEXT	FIELDS SEARCHED
Adversary	• name • tags
Attachment	• content_type_name • hash • name • tags • text • title • type_name
Attribute	• name • value
Comment	• value

SYSTEM OBJECT/OBJECT CONTEXT	FIELDS SEARCHED
Custom Object	• tags • value
Description	• value
Event	• spearphish_subject • spearphish_value • tag • title • type_name
Indicator	• class • status_name • tags • type_name • value
Object Status	• status_name
Point of Contact	• point_of_contact_name
Signature	• hash • name • status_name • tags • type_name

SYSTEM OBJECT/OBJECT CONTEXT	FIELDS SEARCHED
	• value
Source	• name
Task	• assignee_source_name • creator_source_name • name • status_name • tags

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

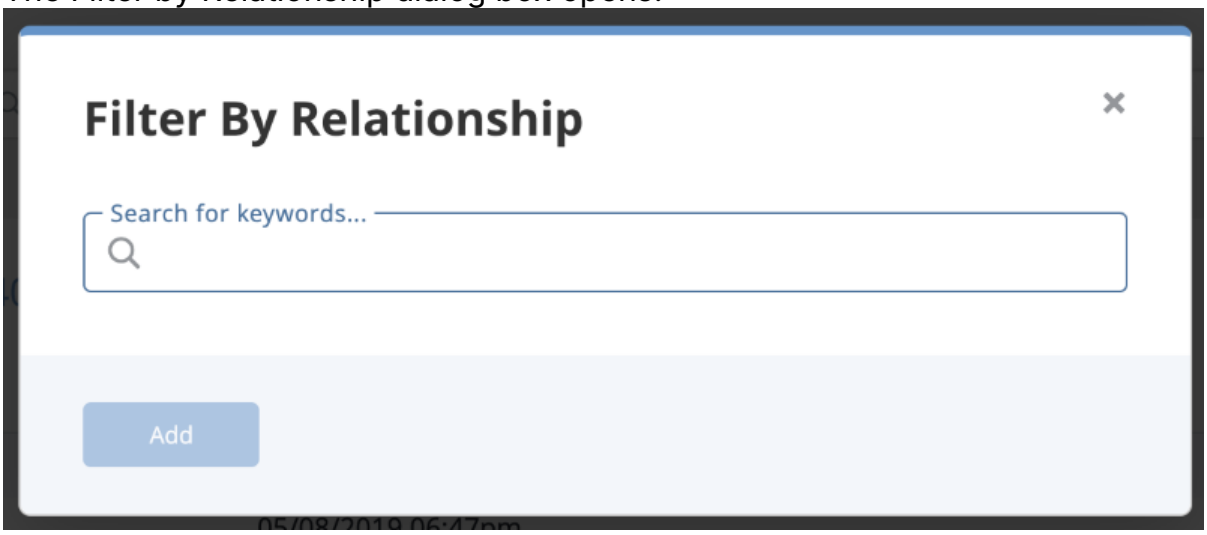
Filtering by Relationship

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

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

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

The Filter by Relationship dialog box opens.



2. Use the text box provided to select an object.
3. Click **Add** to apply the filter.

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

Filtering by Relationship ANY - Match Toggle Selection Example

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

Filtering by Relationship ALL - Match Toggle Selection Example

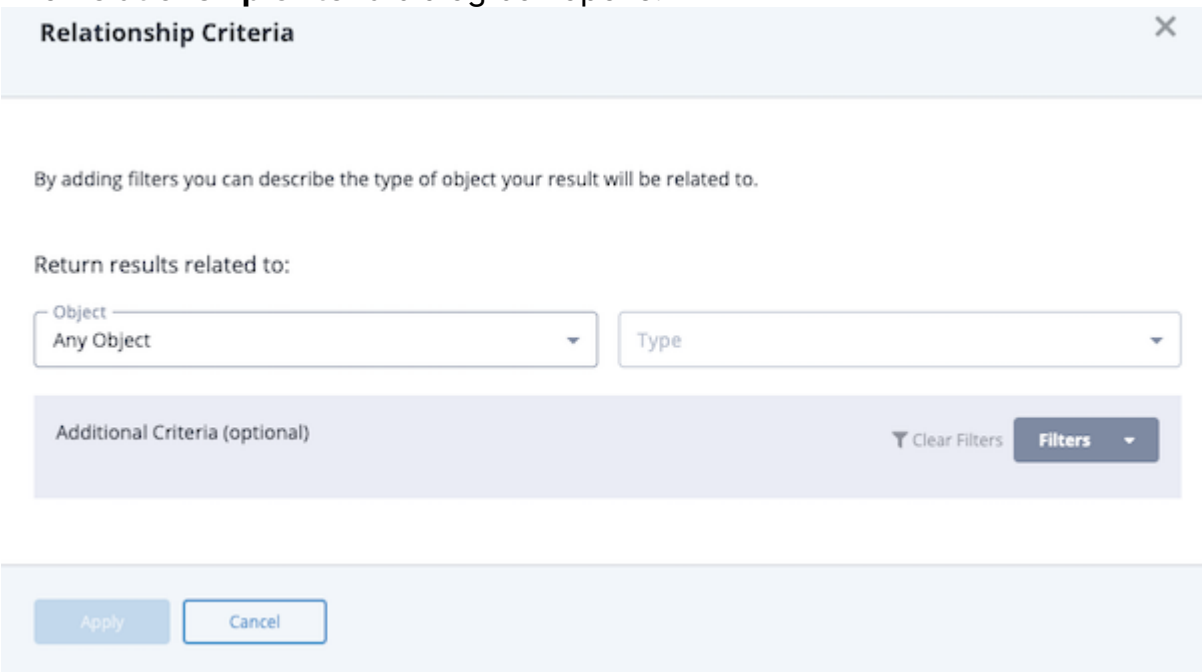
SETTING	RELATED OBJECT
Filter A	ABC Indicator
Filter B	DEF Event
Filter Option	All
Result	Search Results are filtered to include objects related to the ABC Indicator **AND** the DEF Event.

Filtering by Relationship Criteria

The Relationship Criteria filter allows you to filter system objects based on the characteristics of their related objects. For instance, you can filter a list of indicators to include only those with related login compromise event objects.

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

   The **Relationship Criteria** dialog box opens.



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.

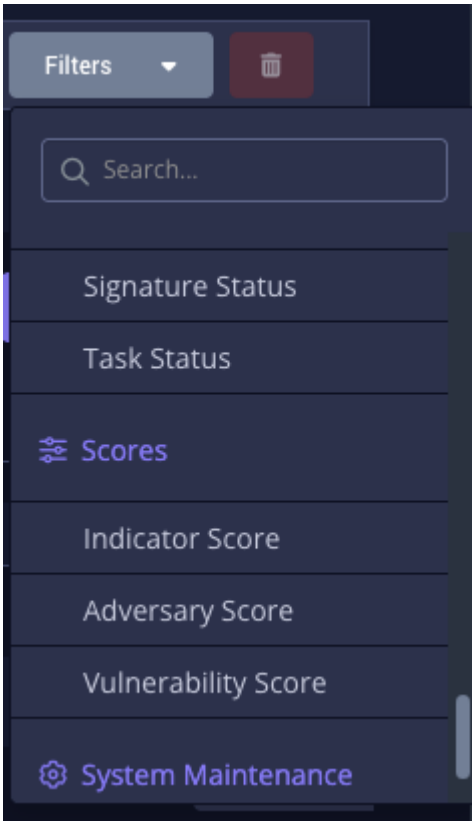
4. After you select all of your filter options, click **Apply** to filter your Threat Library results.

Filtering by Score

You can filter threat library objects in the advanced search results by score.

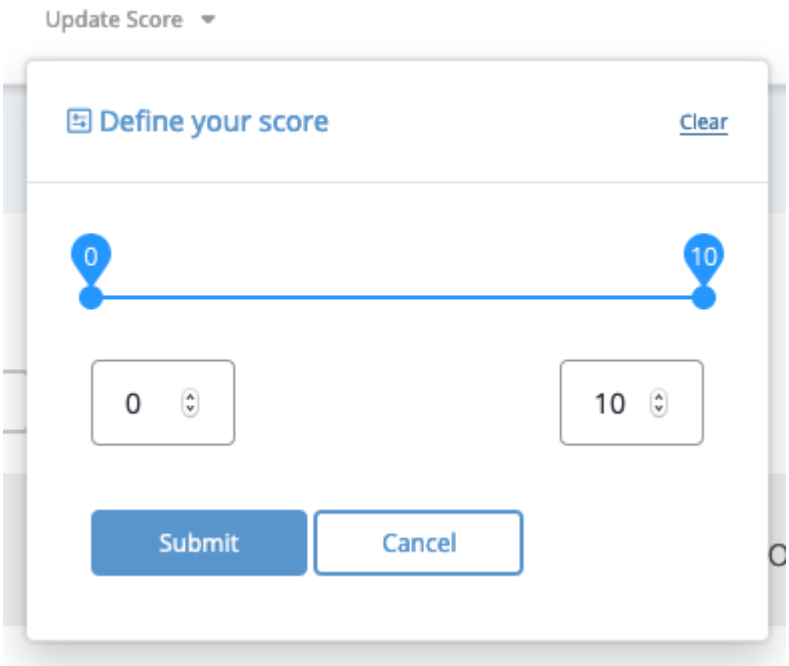
> This option is only available for adversaries, indicators, and vulnerabilities.

1. Navigate to the Advanced Search results page by selecting **Search > Advanced Search** then selecting **<your object> Score** under the Scores heading in the left-hand object type menu.



You can also select **Threat Library > <your object type>** from the main menu for filter criteria narrowed down to a specific object type.

2. Click the **Filters** dropdown and select the **<your object> Score** filter option. The Score dialog row will load in the filter set.



The scale offers a range of 1-10.

3. Adjust the score scale to filter the results.

   Filtering by Scoring Range

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

   Move the left marker to 6 and the right marker to 8 to filter the search results to include objects 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 objects with a score of 8.

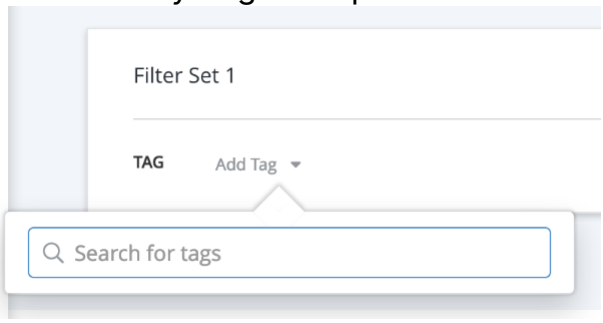
   Select the **Update Score** filter again or select **Clear** to remove the filter.

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, attribute, or description 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

> TLP visibility must be enabled to use the TLP filter in the Threat Library search. See the Configure TLP Visibility section for more details.

The Threat Library allows you to filter your search results based on the TLP label assigned to the object sources, attributes, or description sources. By default, all TLP filter options are checked so that your Threat Library view includes all objects. To exclude objects by TLP, you can uncheck the box to the left of the label name. For example, to omit objects with object and/or description sources assigned a Red TLP label, uncheck the Red box.

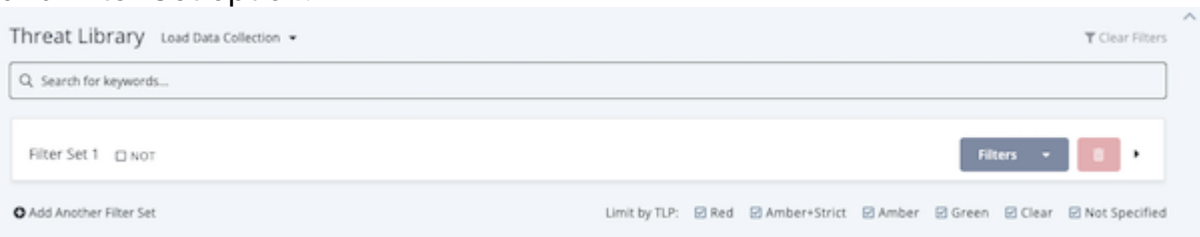
When you apply a TLP filter, the Sources, attribute, and description columns only display data that matches the TLP filter.

Tips and Tricks

- TLP filters can be stored as part of data collections, similar to other filter types.
- The TLP filter is a global filter that 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 in that CSV results output will match those in the Threat Library results.

1. Navigate to Threat Library.

   The option to filter by TLP color designation will be located under the search bar and Filter Set option.

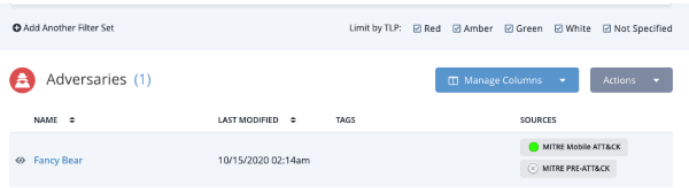
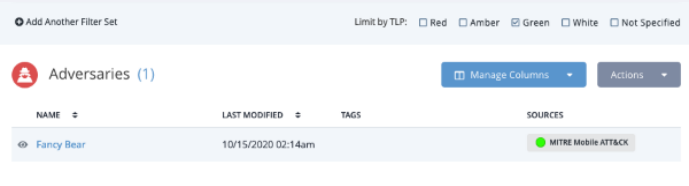


2. Use the **Limit by TLP** filter check boxes to select which TLP designations to apply to your search results.

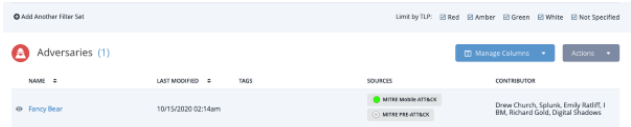
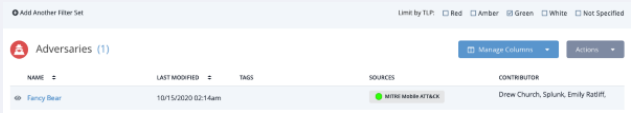
   > If TLP Green is checked, only objects with any source of TLP Green will be returned in the search results.

The TLP filter also impacts the information returned in search results columns, including Sources, attributes, and descriptions.

Sources - In the Sources column of the search results, only sources that match the selected TLP labels are displayed.

SCENARIO	RESULTS DISPLAY
Sources displayed before applying the TLP filter	
Sources displayed after applying the TLP filter	

Attributes - In any displayed attribute column, only attribute values with sources that match the selected TLP labels are displayed.

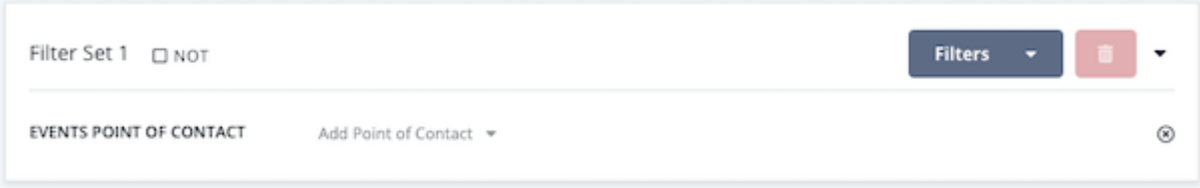
SCENARIO	RESULTS DISPLAY
Attribute Contributors displayed before applying the TLP filter	
Attribute Contributors displayed after applying the TLP filter	

Descriptions - In any displayed description column, only descriptions with sources that match the selected TLP labels are displayed.

Filtering by Point of Contact

The Point of Contact filter allows you to filter objects by the ThreatQ user display name of the person assigned as the object's point of contact. You can filter by multiple user names as well as include objects that do not have a point of contact (Unassigned).

1. Click the **Filters** option and select **Point of Contact**.
   The Point of Contact row is displayed under the filter set name.



2. Click the **Add Point of Contact** option to access a drop-down list of user names.

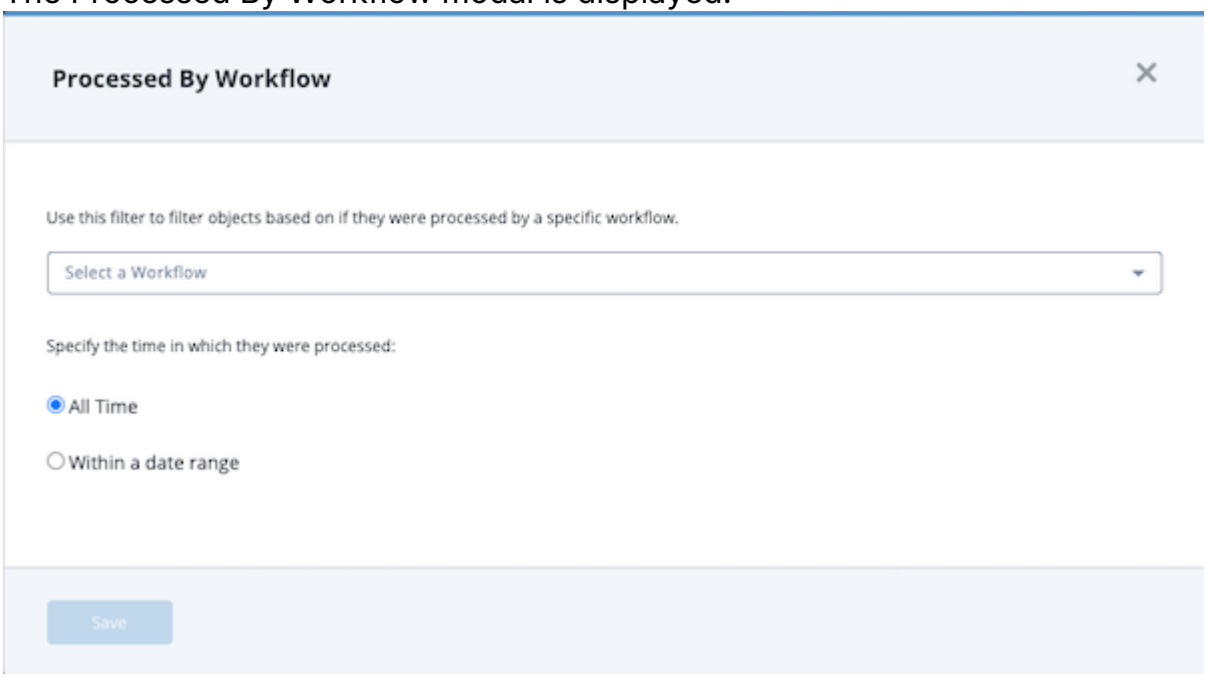
> The point of contact list includes all ThreatQ user names even those not currently assigned as a point of contact for an object. In addition, this list contains an Unassigned option that allows you to include objects with a blank Point of Contact field.

3. Locate and click the checkbox next to the user name for your filter by scrolling through the drop-down list or entering the name in the Search field. You can select one or more user names at a time from this list.

Filtering by Workflow

The Processed by Workflow filter allows you to filter Threat Library results by the TQO workflow that processed the objects and the time period during which the objects were processed.

1. Click the **Filters** option and select **Processed by Workflow**.
   The Processed By Workflow modal is displayed.



2. Select the TQO workflow.

3. Select a time range option:
    - **All Time** - Returns all system objects processed by the workflow.
    - **Within a date range**:
        - **Processed On** - Returns system object processed by the workflow on a specific date.
        - **Processed Before** - Returns system object processed by the workflow before a specific date.
        - **Processed After** - Returns system object processed by the workflow after a specific date.
        - **Processed Between** - Returns system object processed by the workflow within a date range.
        - **Processed Within the Last** - Returns system object processed by the workflow within a specific number of days prior to the current date.
4. Click the Save button to apply the filter criteria.

Date Filters

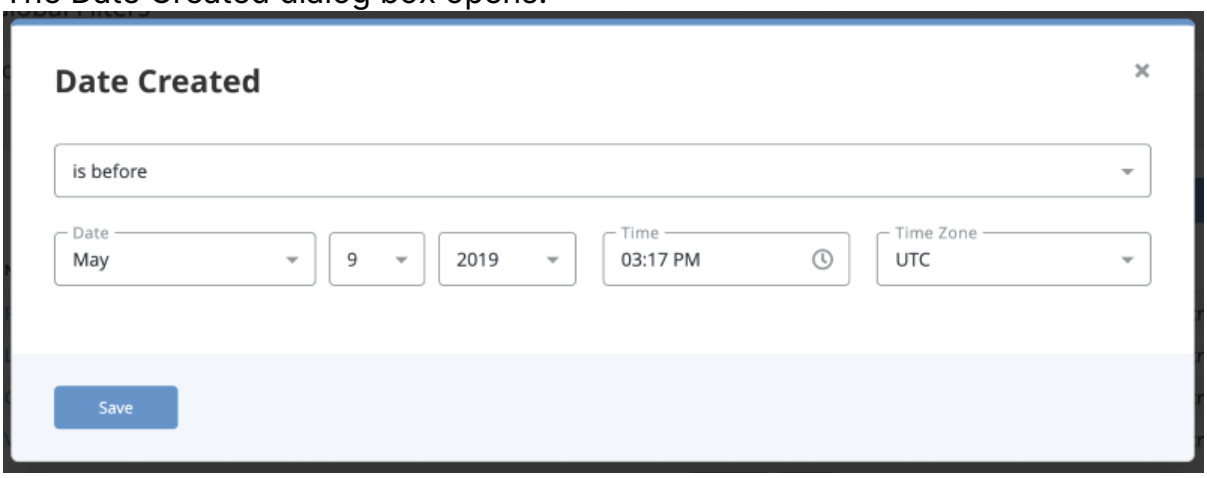
Date filters allow you to filter advanced search results by date-related values.

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	Search results include the specified date.
is not	Search results exclude items from a range of dates.
is before	Search results include items before a selected date
is after	Search results include items after 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.

OPTION	RESULT
is within the last	Search results include items within the selected number of days.

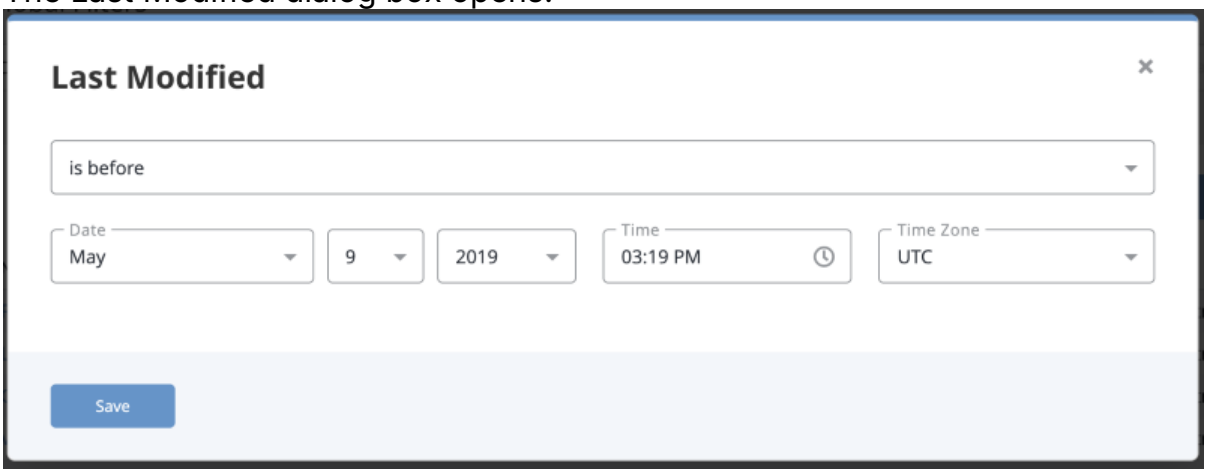
3. Use the controls to select date options based upon the selection in step 2.
4. Click **Save**.

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	Search results include the specified date.
is not	Search results exclude items from a range of dates.
is before	Search results include items before a selected date
is after	Search results include items after a selected date

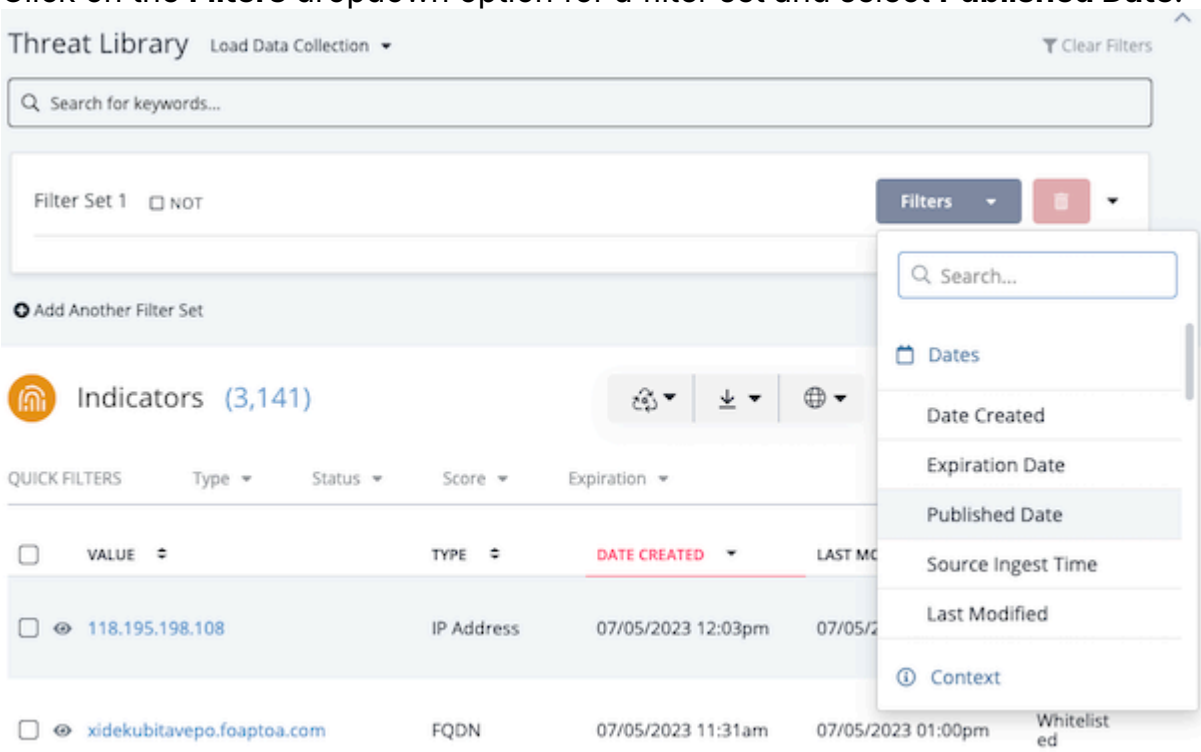
OPTION	RESULT
is between	Search results include items in a selected range of dates
is greater than	Search results include items have exceeded their expiration date by a selected number of days.
is within the last	Search results include items within the selected number of days.

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:

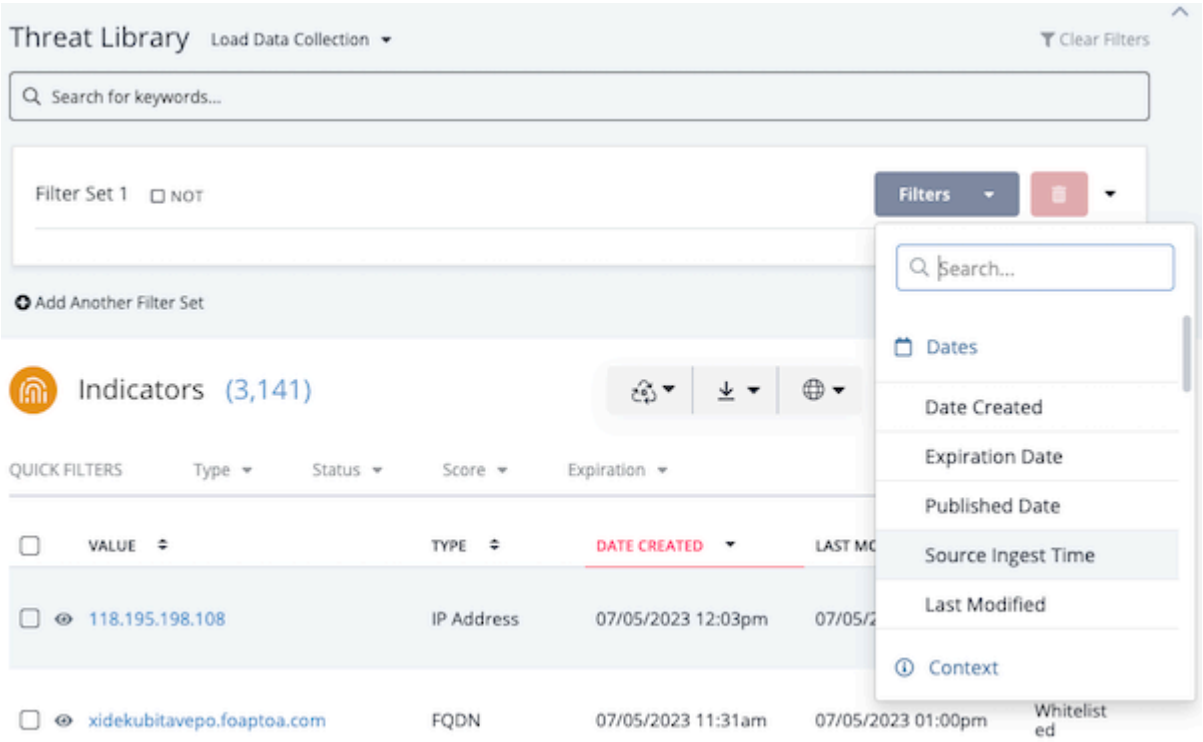
OPTION	RESULT
is	Search results include the specified date.
is not	Search results exclude items from a range of dates.
published before	Search results include items before a selected date
published after	Search results include items after a selected date
published between	Search results include items in a selected range of dates
is greater than	Search results include items have exceeded their expiration date by a selected number of days.
published within the last	Search results include items within the selected number of days.

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

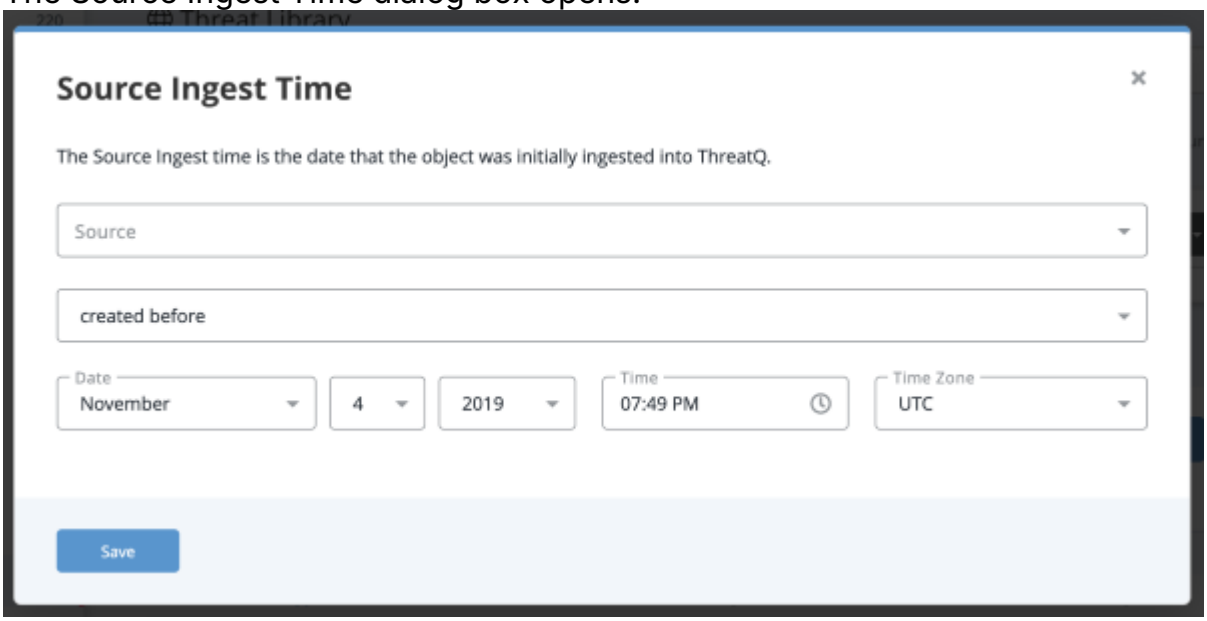
Filtering by Source Ingest Time

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

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



The Source Ingest Time dialog box opens.



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
is	Search results include the specified date.
is not	Search results exclude items from a range of dates.
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
is greater than	Search results include items have exceeded their expiration date by a selected number of days.
created within the last	Search results include items within the selected number of days.

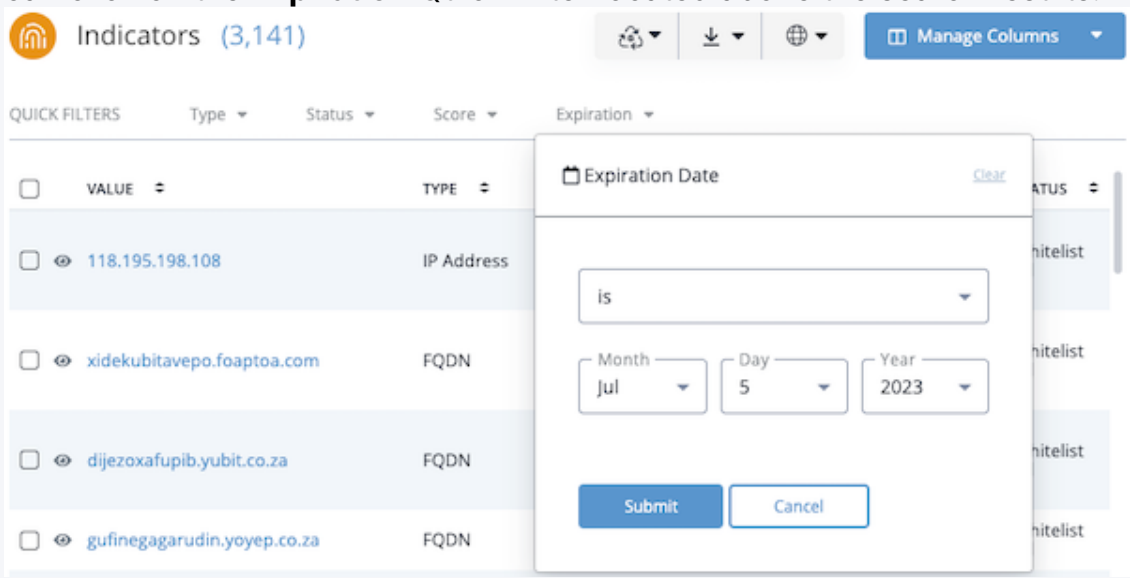
4. Select **Date**, **Time**, and **Time Zone** for the filter to use.
5. Click **Save**.

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.



The Expiration Date dialog box opens.

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

OPTION	RESULT
is	Search results include the specified date.
is not	Search results exclude items from a range of dates.
is after	Search results include items after a selected date.
is before	Search results include items before a selected date.
is between	Search results include items in a selected range of dates.

OPTION	RESULT
is greater than	Search results include items have exceeded their expiration date by a selected number of days.
is within the last	Search results include items within the selected number of days.
is within the next	Search results include items within a range of future dates.
is protected from auto-expiration	Search results include items that are protected from auto-expiration.

3. Based on the filter option you selected, select the date, date range, or number of days for the filter to use.
4. Click **Submit**.

Status Filters

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

> Only Events, Indicators, Signatures, and Tasks can be filtered by their Status. In addition, the Event Status filter is displayed only if an administrator has configured Event Statuses in the Object Management page.

Filtering by Status

1. Click the Filters dropdown and select **<Object Type>Status**.
   The <Object Type> Status filter row is displayed under the filter set name.
2. Click the **Add Status** option to access a drop-down list of statuses.
2. Locate and click the checkbox next to the status for your filter by scrolling through the drop-down list or entering the status in the Search field. You can select one or more user names at a time from this list.

   > The Event Status filter gives you the option to include events without an status by selecting the None option.

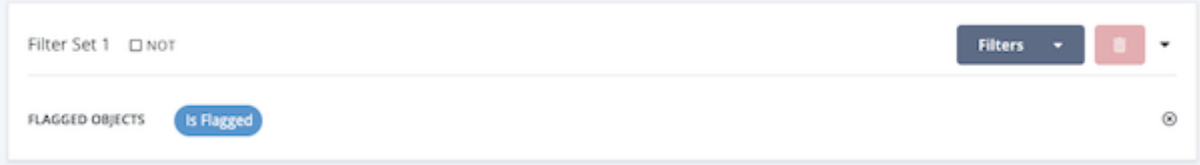
   The search results update with the applied filter.

System Maintenance Filters

The Flagged Object filter allows you to filter Threat Library search results to display objects flagged as exceeding the relationship limit of 10,000 relationships with the same source.

Filtering by Flagged Objects

1. Click the Filters dropdown and select Flagged Objects.
   The Flagged Objects filter row is displayed under the filter set name. This filter row displays the Is Flagged pill. In addition, your Threat Library view lists system objects that have been flagged as exceeding the relationship limit of 10,000 relationships per object/source.



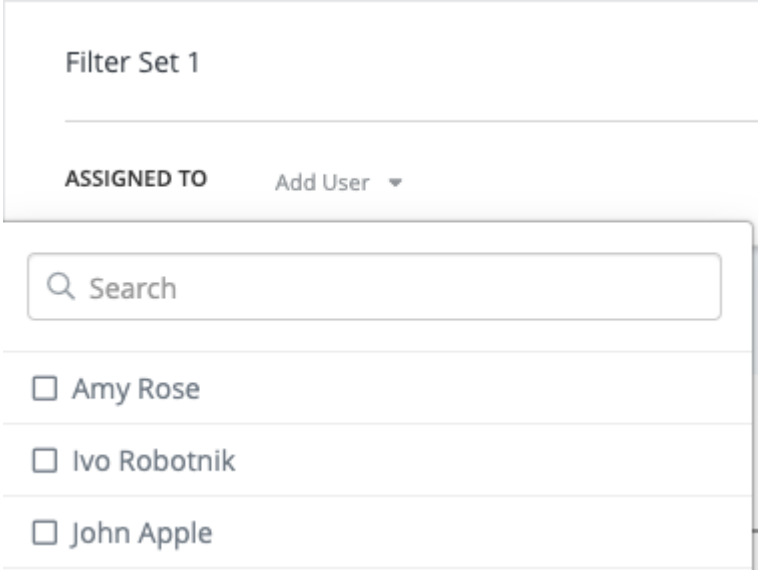
Tasks Filters

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

Filtering Tasks by Assignment

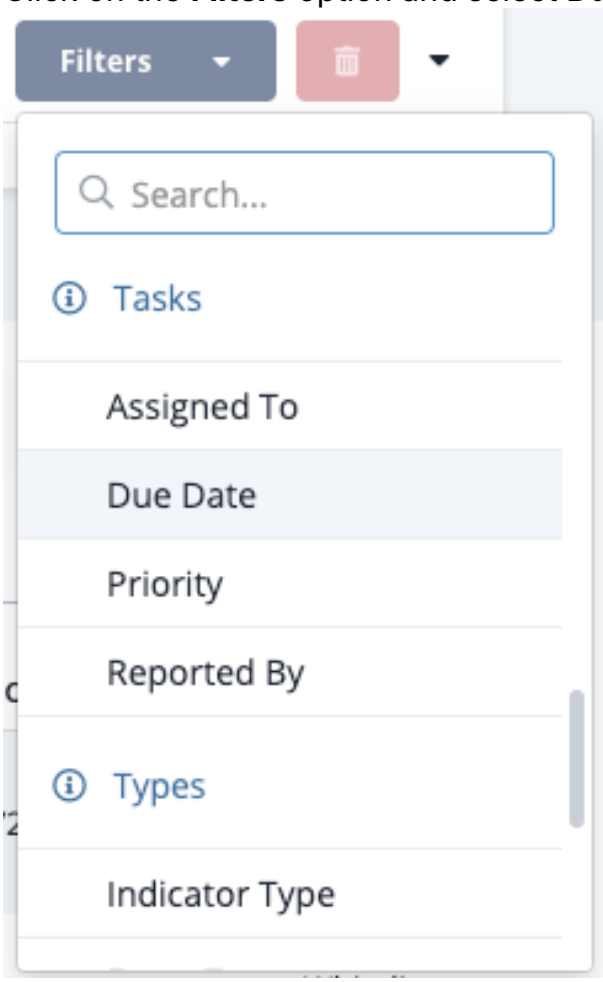
You can filter tasks based on whom they are assigned to.

1. Click on the **Filters** option and select **Assigned To**.
2. Use the **Add User** dropdown to select the user.

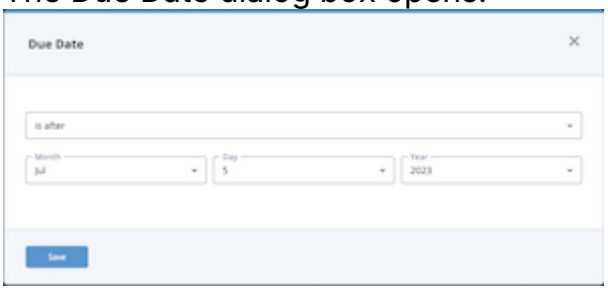


Filtering Tasks by Due Date

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



The Due Date dialog box opens.



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

OPTION	RESULT
is	Search results include the specified date.
is not	Search results exclude items from a range of dates.

OPTION	RESULT
is after	Search results include tasks with a due date after a selected date.
is before	Search results include tasks with a due date before a selected date.
is between	Search results include tasks with a due date that set between the selected range of dates.
is greater than	Search results include items have exceeded their expiration date by a selected number of days.
Is within the last	Search results include tasks with a due date within the last user-specified number of days.
Is within the next	Search results include tasks with a due date within the next user-specified number of days.

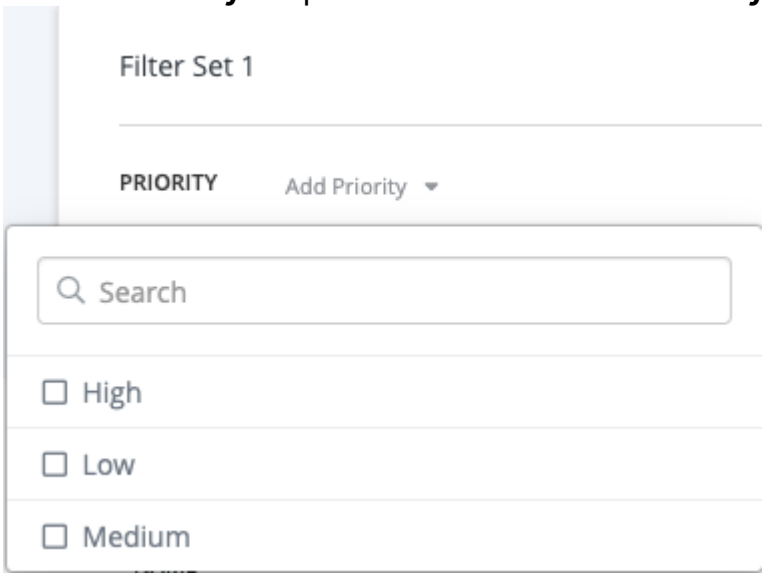
3. Click **Save**.

Filtering Tasks by Priority

You can filter tasks based on their priority.

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

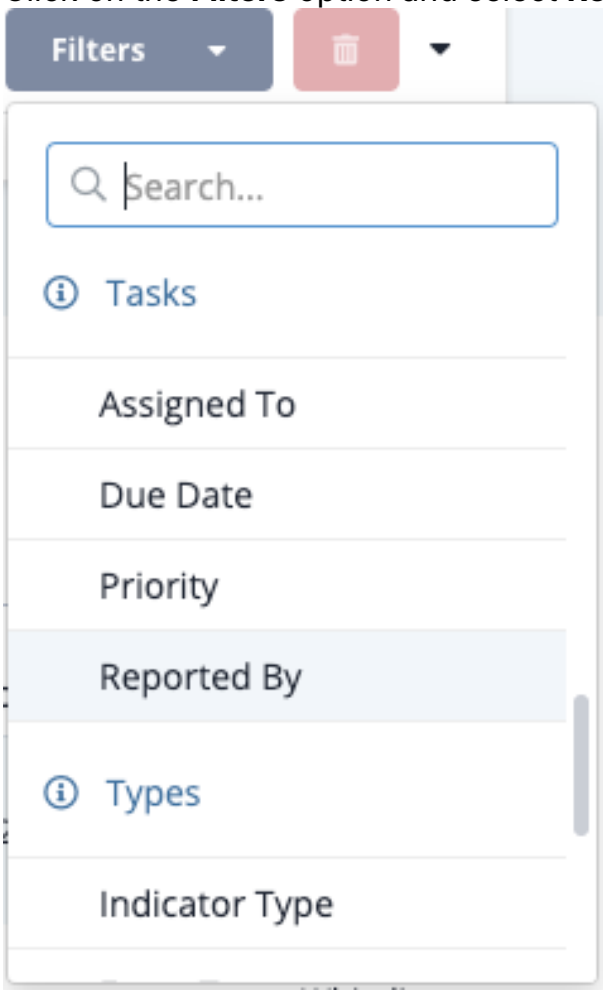
2. Use the **Priority** dropdown and select **Add Priority.**



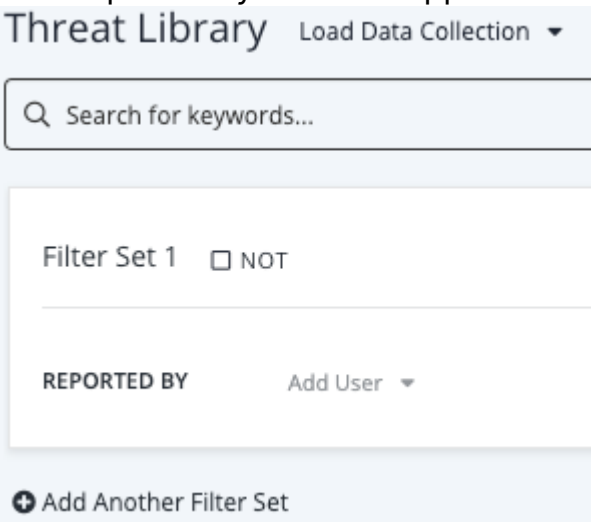
Filtering Tasks by Reported By

You can filter tasks based on who created them.

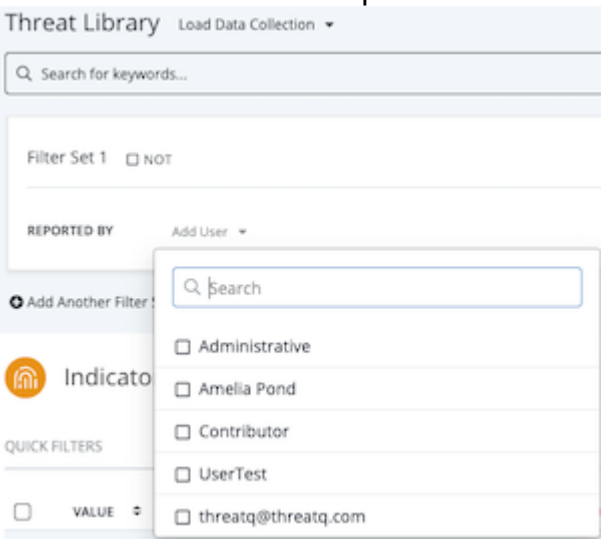
1. Click on the **Filters** option and select **Reported By**.



The Reported By Filter will appear in the filter set.



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



Type Filters

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

Filtering by Object Type

Filter the Signature list to include YARA types only.

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

   The Type filter row will appear in the filter set.

2. Click on **Add Type**.

   You can select multiple types using the check boxes.

   The search results will update with the applied filter.

Managing Search Results

About 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.

Data Collections

THREATQ REQUIRED PERMISSIONS

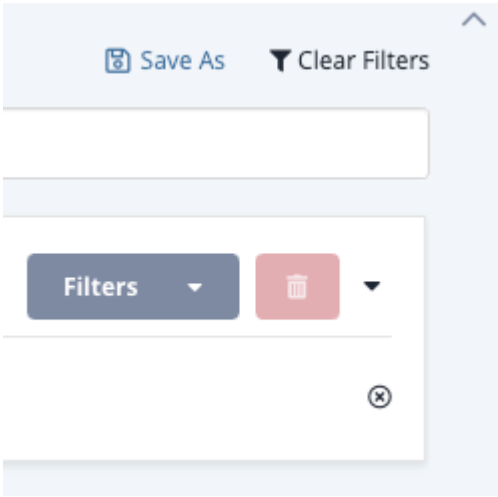
Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role - Action Permissions: Artifact Management - Data Collections - Create. Edit Delete OR View Only

Once saved, a Data Collection can be used by dashboard widgets, integrations, TQO actions, TAXII collections, and other workflows.

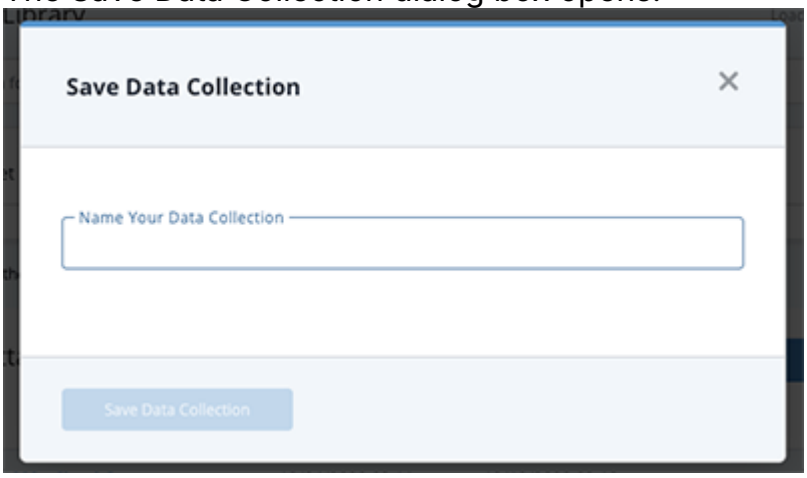
Use caution when deleting a data collection as it could be associated with integrations, custom dashboards, TAXII collections, and other workflows in use with your organization.

Saving Searches as Data Collections

1. Perform a search on the Threat Library.
2. Click the **Save As** link.

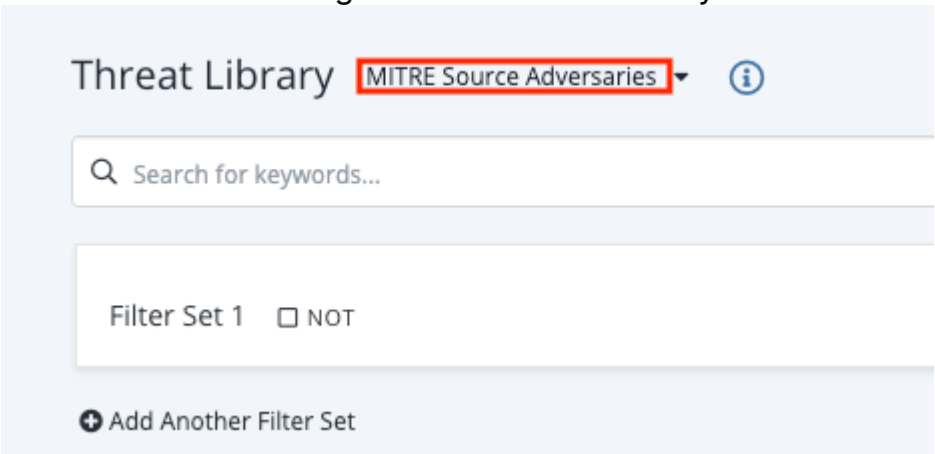


The Save Data Collection dialog box opens.



3. Enter a name for the search in the Data Collection dialog box.
4. Click the **Save Data Collection** button.

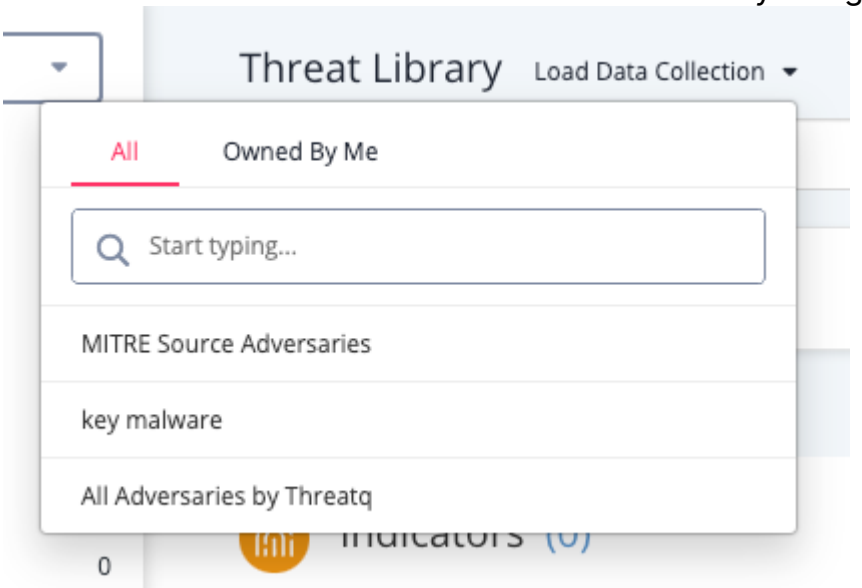
   The name of the data collection is displayed at the top of the page. As the data collection creator, you have owner-level permissions and are the only user who can view or edit the data collection. See the Sharing Data Collections section for information on allowing other users to access your data collection.



Loading Data Collections

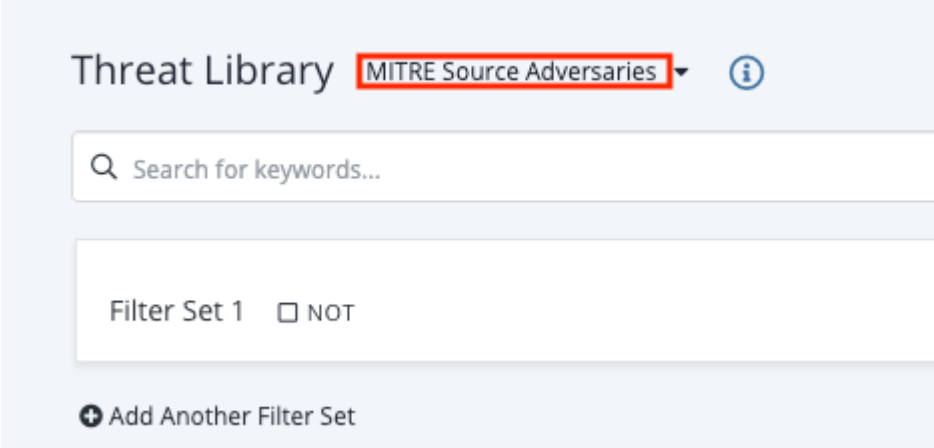
1. Navigate to the Threat Library page.
2. Click the **Load Data Collection Search** option. The data collection window defaults to the All tab that lists all the data collections you own or to which you have view or edit access. The Owned By Me tab lists the data collections for which you are

the owner. You can also locate a data collection by using the search field.

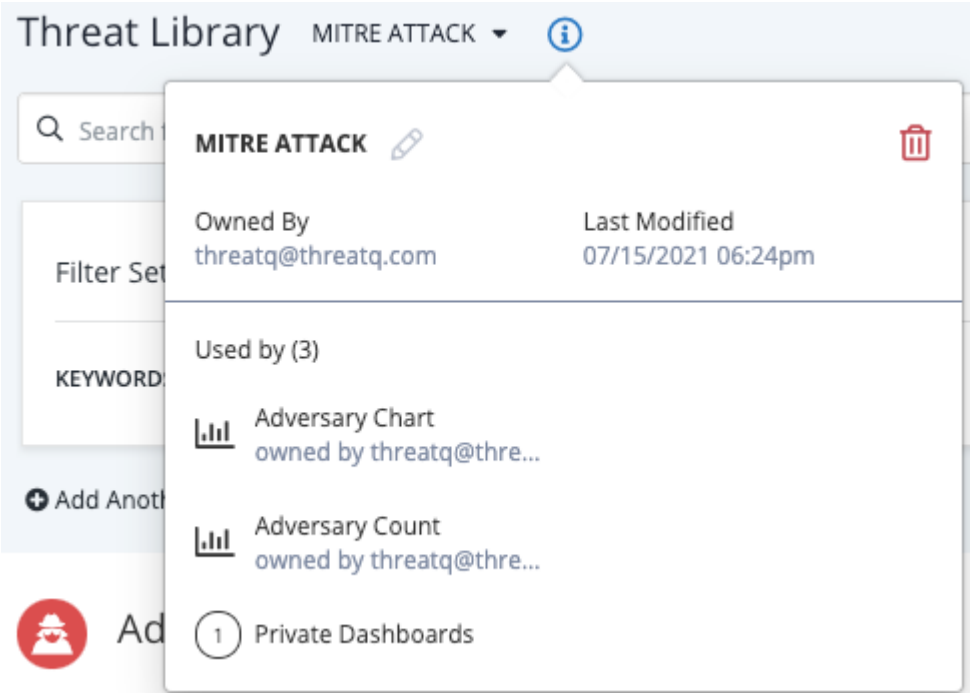


3. Select the data collection.
   The data collection is displayed in the Threat Library page. The name of the data collection is listed at the top of the page.

   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, TAXII collections, and workflows that use the data collection. You can click these items to access the corresponding dashboard or data feed.
   - The number of private dashboards that use the data collection



Modifying a Data Collection

Users with owner or editor permissions for a data collection can make changes to it.

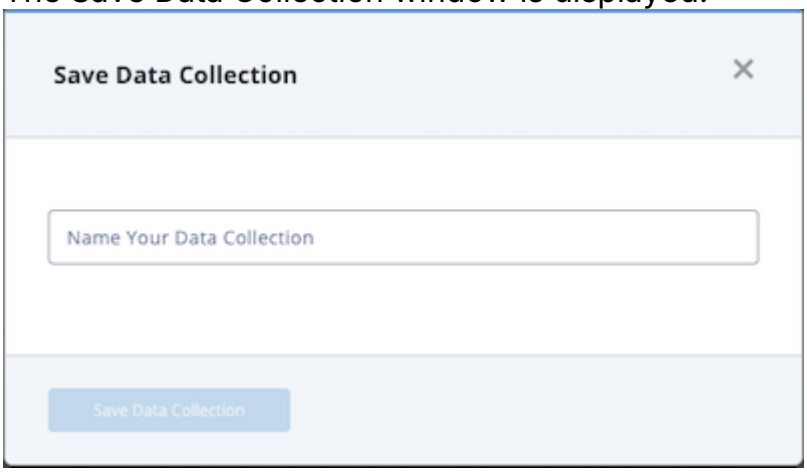
1. Navigate to the Threat Library.
2. Load the data collection you want to change.
3. Enter your changes to the data collection.
4. Click the Save link.

Copying a Data Collection

When an owner or editor makes changes to a data collection, the Save As link allows the creation of a new data collection that reflects these changes and leaves the original data collection unchanged. For example, you can add a filter to an existing Adversaries data collection to include only MITRE Enterprise ATT&CK sources, then save the new data collection as Adversaries - MITRE Enterprise.

1. Navigate to the Threat Library.
2. Load the data collection you want to copy.
3. Enter your changes to the data collection.

4. Click the **Save As** link.
   The Save Data Collection window is displayed.



5. Enter the name of the new data collection.
6. Click the Save Data Collection button.
   ThreatQ creates your new data collection and displays it in the Threat Library page.

Renaming a Data Collection

Only the owner of a data collection can change its name.

1. Navigate to the Threat Library.
2. Load the data collection whose name you want to change.
3. Click the icon.
4. Click the icon next to the data collection's name.
5. Enter the new name.
6. Click the to save your change.

Sharing Data Collections

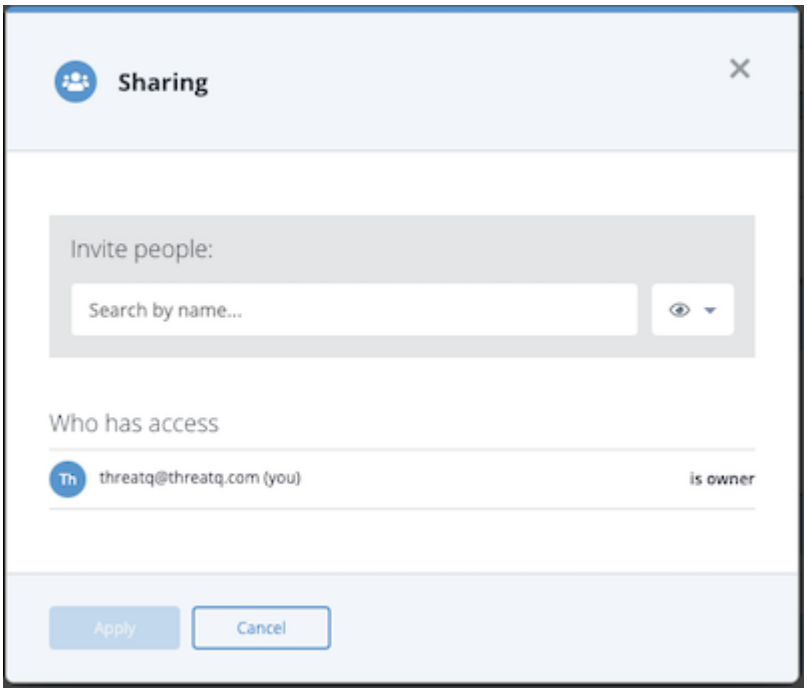
Owners and editors have the option to share a data collection with other users. However, only the data collection owner can remove a user's permissions. In addition, the Share(d) button displayed depends on your permission level and the sharing status of the data collection.

PERMISSION LEVEL	SHARED WITH OTHERS?	SHARE(D) BUTTON

Owner	No	Share
Owner, Editor	Yes	Share
Viewer	Yes	Shared

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

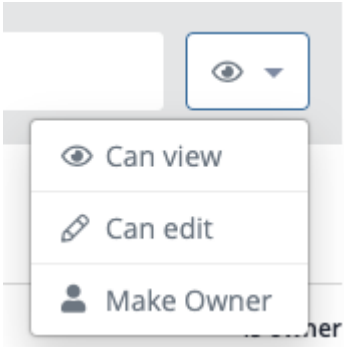
1. Navigate to the Threat Library.
2. Load the data collection you want to share.
3. Click the **Share** button.
   The Sharing window allows you to select the user to which you want to grant access.



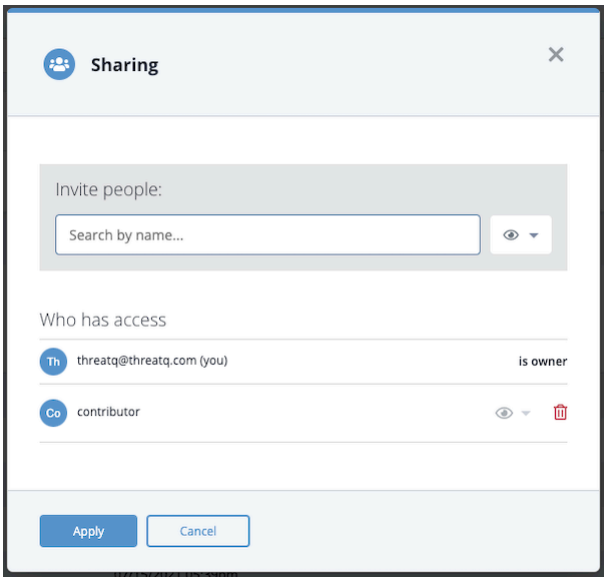
4. Click the arrow next to the icon to select the user's permission level.

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

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



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



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

Removing a User's Access to a Data Collection

Only the data collection owner can remove a user's permissions.

1. Navigate to the Threat Library.
2. Load the data collection to which you want to remove a user's access.
3. Click the Share button.
4. Click the icon next to the user's name.

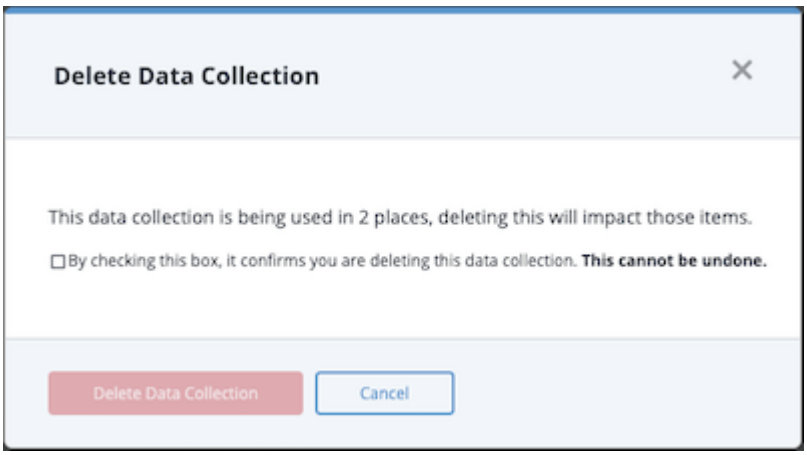
Deleting a Data Collection

To delete a data collection, you must have owner-level permissions for the data collection.

> ⚠ Deletion of a data collection cannot be undone. Exercise caution before deleting a data collection as it could be associated with integrations, custom dashboards, TAXII collections, 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.

CSV Exports

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.

Exporting Search Results to CSV

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.

STIX Exports

You can export ThreatQ-supported STIX objects to STIX files from the object details and object preview pages as well as Threat Library search results. Exports from the object details and object preview pages include object relationships. However, exports from the Threat Library do not.

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.

ThreatQ supports STIX exports for the following seeded objects:

- Adversaries
- Attack Pattern
- Campaign
- Course of Action
- Identity
- Incident
- Indicators
- Infrastructure
- Intrusion Set
- Malware
- Note*
- Report*
- Tool
- Vulnerability

Note and Report objects can only be exported to STIX from the object details and object preview pages or TQX, not from Threat Library search results.

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

Tips and Tricks

- STIX exports:
  - Include an object's confidence value as an attribute as long as the confidence value falls within the range from zero to one hundred.

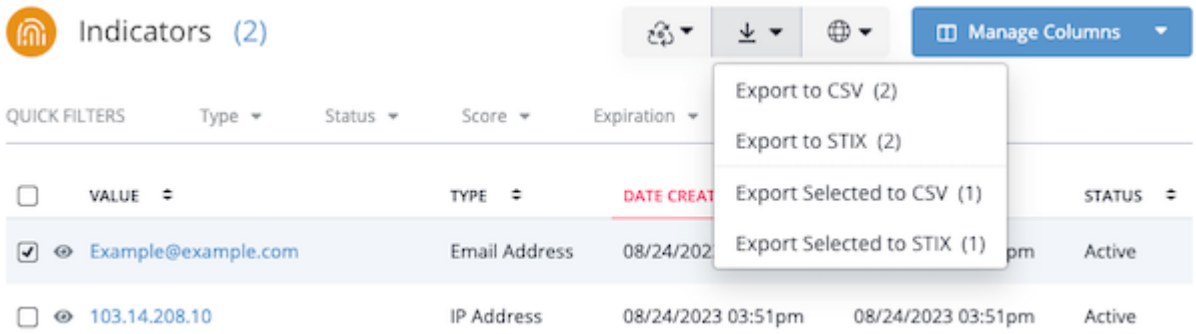
  - Include an object's primary description only. If an object has multiple descriptions, only the primary description is included.
  - Include indicator expiration timestamps in the **valid_until** field.
  - From the object details and object preview pages include object relationships. However, exports from the Threat Library do not.
- When you export system objects with the following location keys as attributes to a STIX file, the export process converts these attributes to STIX location objects: latitude, region, city, longitude, country, street address, precision, administrative area, postal code. STIX imports of location objects convert these objects to attributes.
- When you export an infrastructure object that includes Kill Chain: attributes to a STIX file, these attributes are exported as Kill Chain Phase information.

Exporting Threat Library Search Results to STIX

STIX exports generated from Threat Library search results do not include object relationships.

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.
4. Click the **Export** button and select the option to export all objects or the option to select only checked objects.



The STIX file downloads to your desktop.

Exporting Object Details to STIX

You can export ThreatQ supported STIX objects to STIX files from the object details and object preview pages as well as Threat Library search results. Exports from the object details and object preview pages include up to 1,000 relationships per object. Exports from the Threat Library do not include related objects.

Objects with more than 1,000 relationships return them in an indeterminate order. As a result, there is no sort method available to determine which of the relationships are included in the STIX export.

1. Access the system object's details or preview page.
2. Click the **Actions** button.
3. Click the Export to STIX option.

Bulk Actions

THREATQ REQUIRED PERMISSIONS

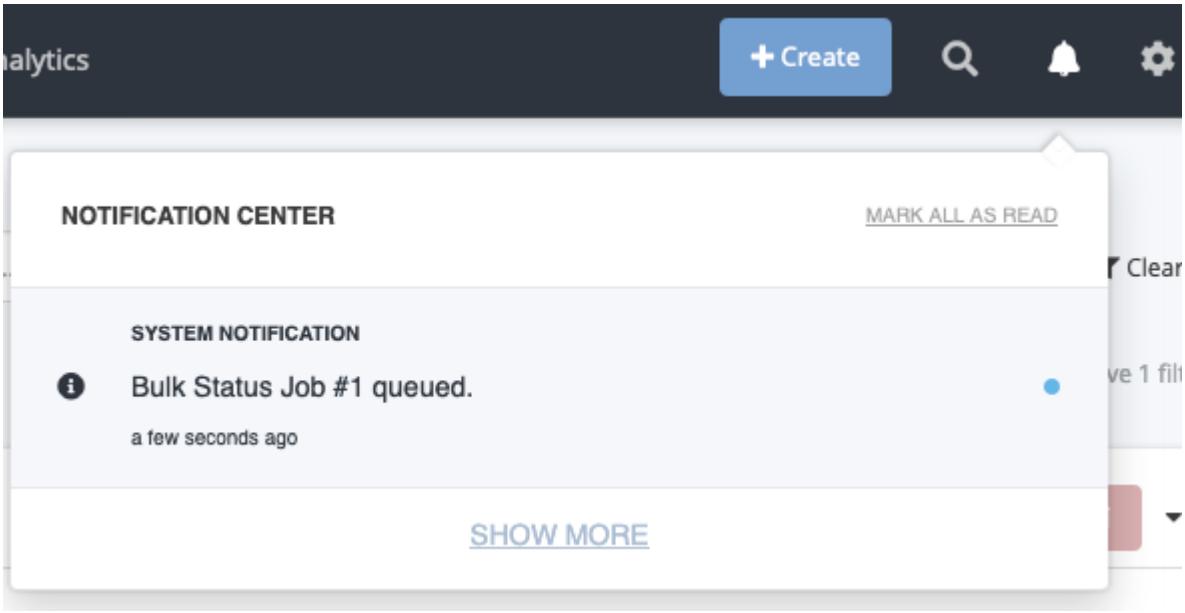
Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role - Action Permissions: See the Interdependent Permissions topic.

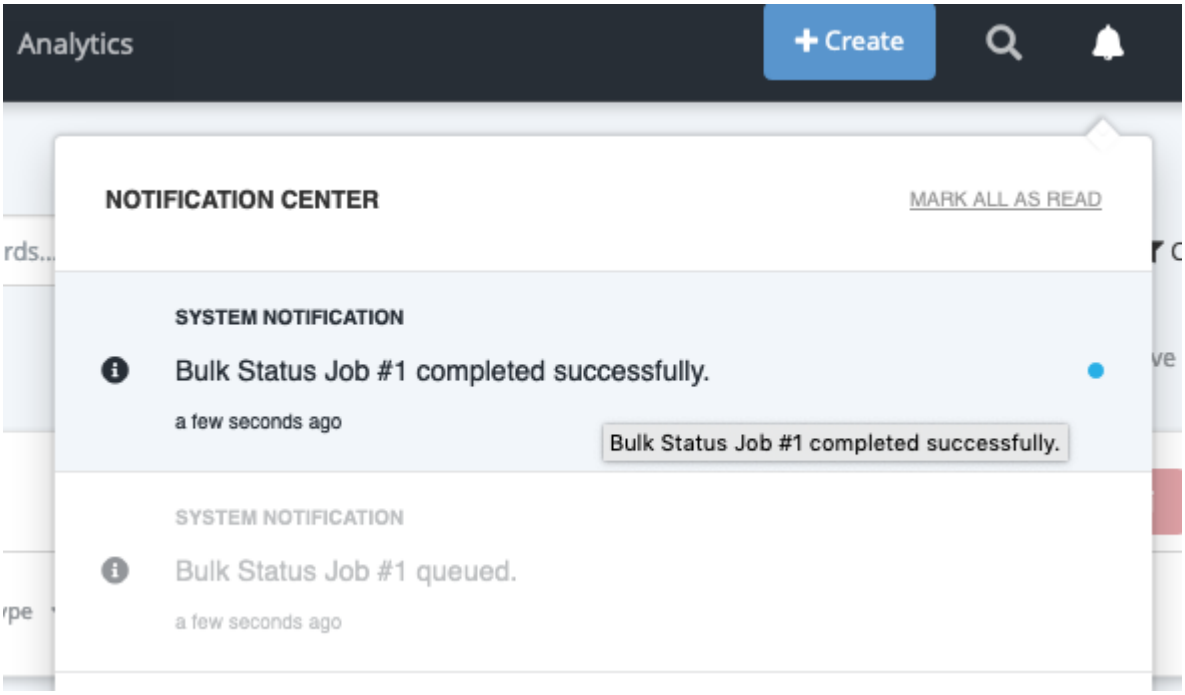
Custom Role - Data Access Permissions: Bulk changes require Create, Edit, Delete permission for the object type(s). Exports require Create, Edit, Delete or View Only Access for the object type(s).

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.



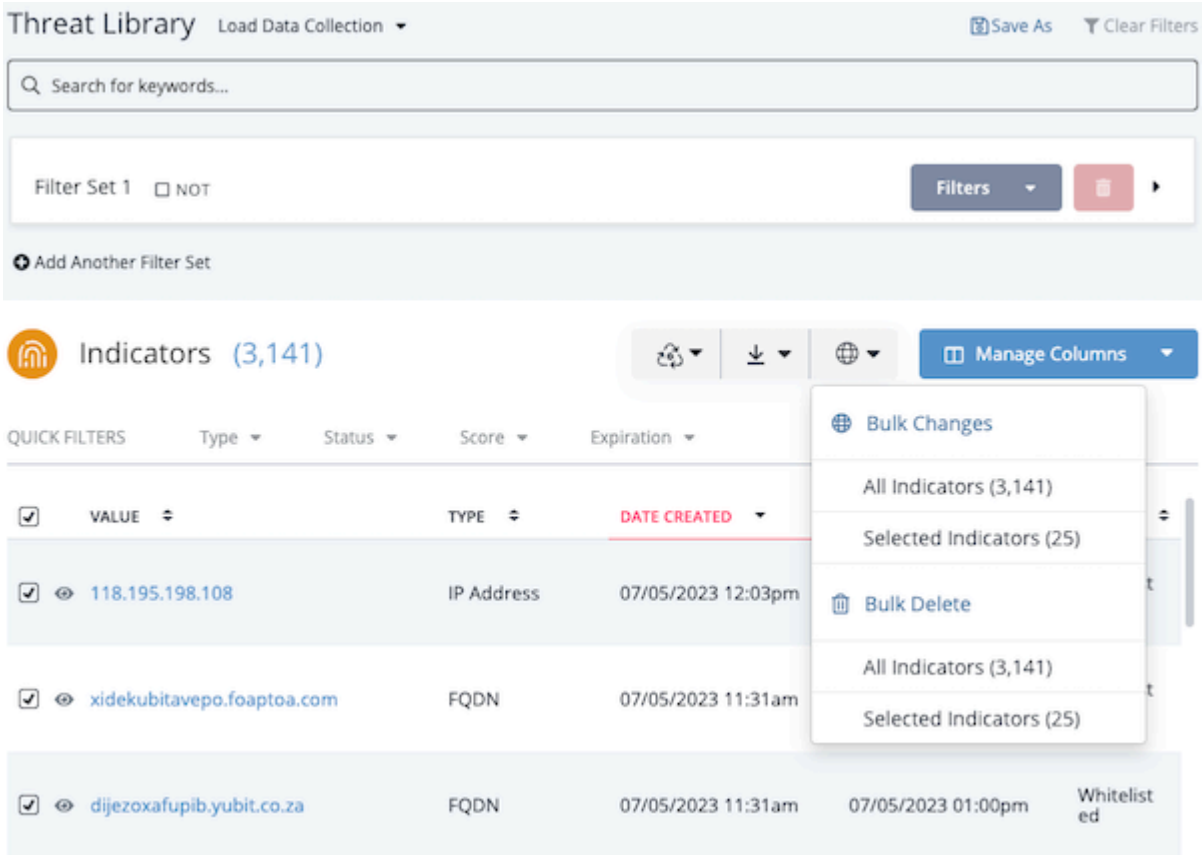


Bulk Add Source

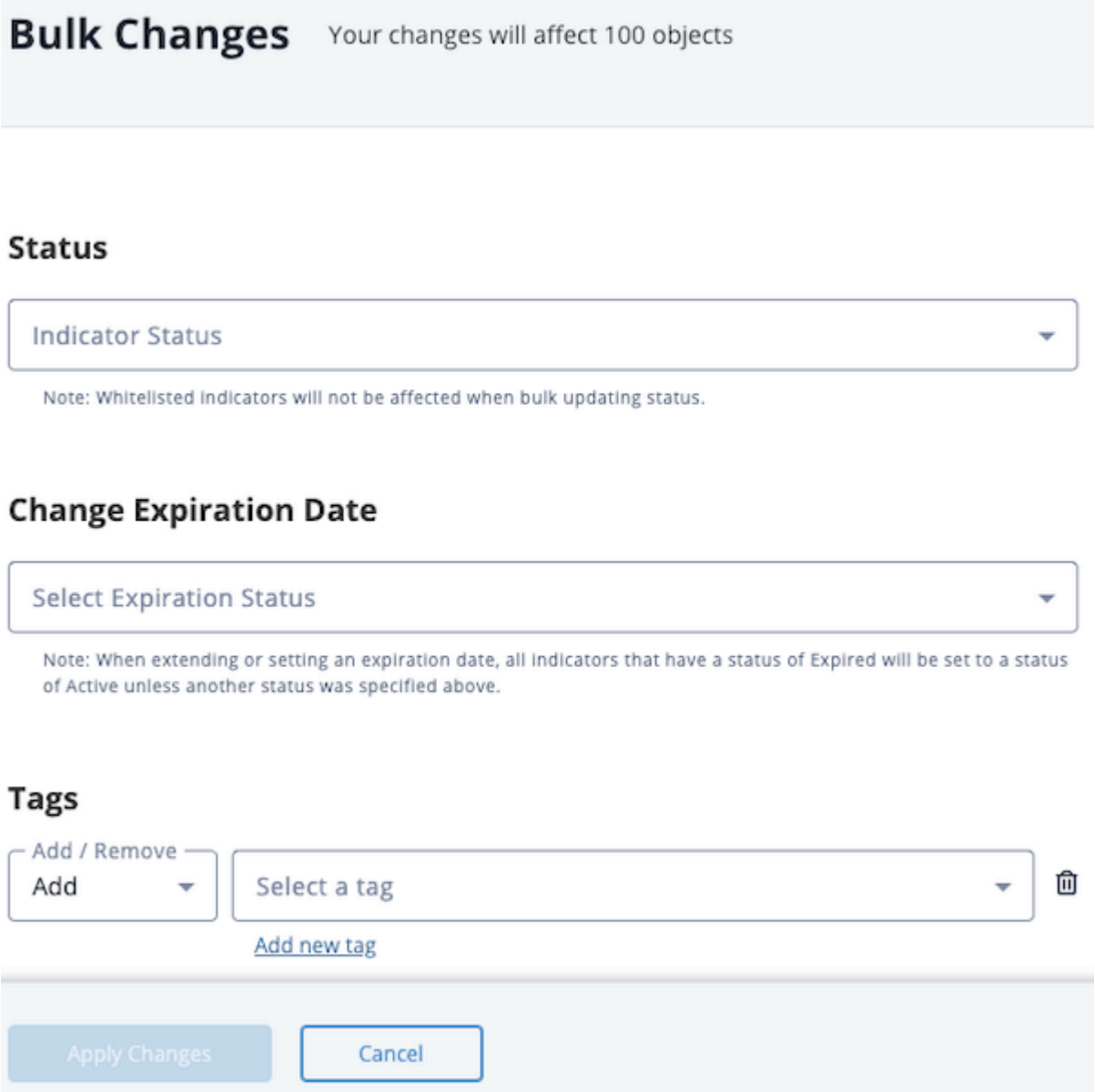
> If an object is already associated with the source selected for the Bulk Add Sources action, the object is skipped during the bulk process.

1. Perform a search on the Threat Library.

2. Click the **Bulk Actions** button .



3. Click the **All *<System Object>*** or **Selected *<System Object>*** option under the *Bulk Changes* heading.

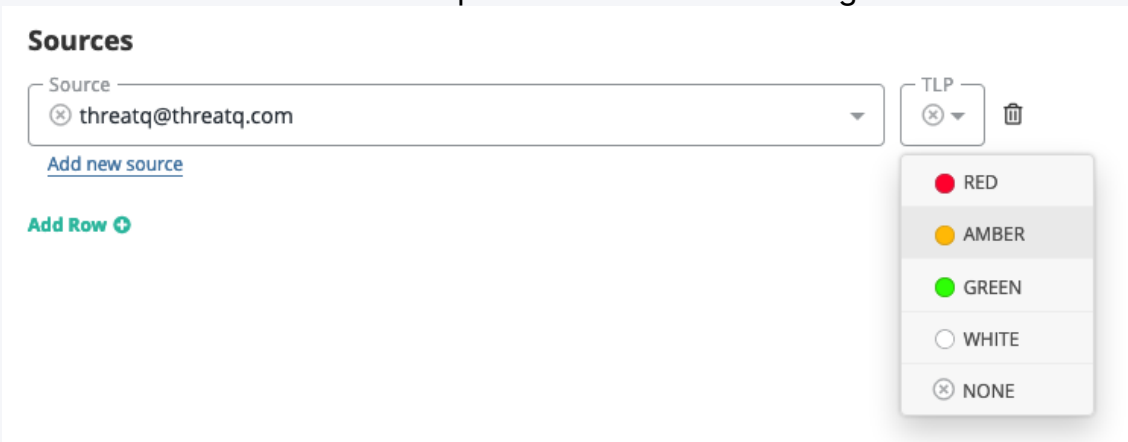


4. Click **Add Row** under the **Source** heading.

   A new row with a dropdown option is displayed.

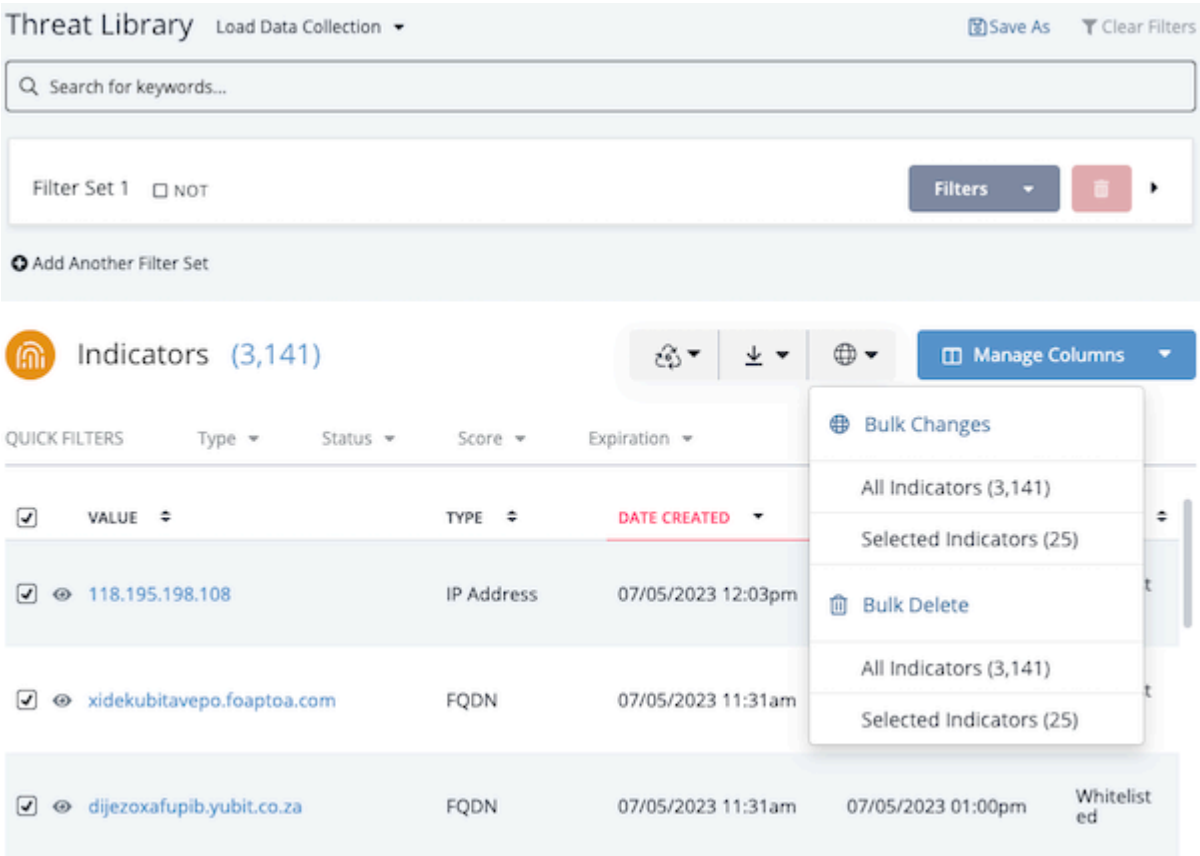
5. Use the dropdown to select the source to add to the selected objects. You can also use the **Add New Source** link to add a source that is not listed in the dropdown.

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

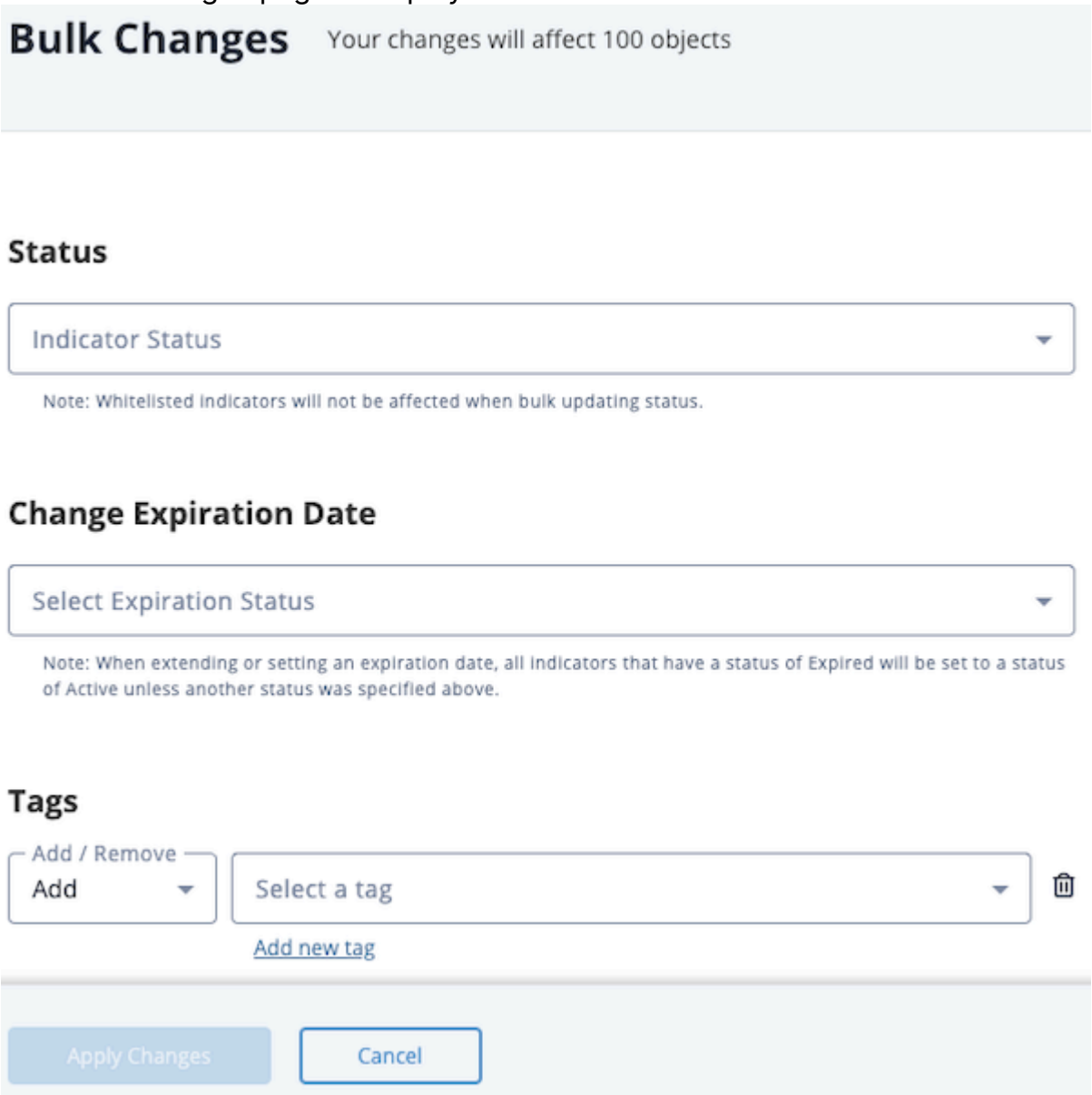


Bulk Add/Remove Attributes

1. Perform a search on the Threat Library.
2. Click the **Bulk Actions** button .

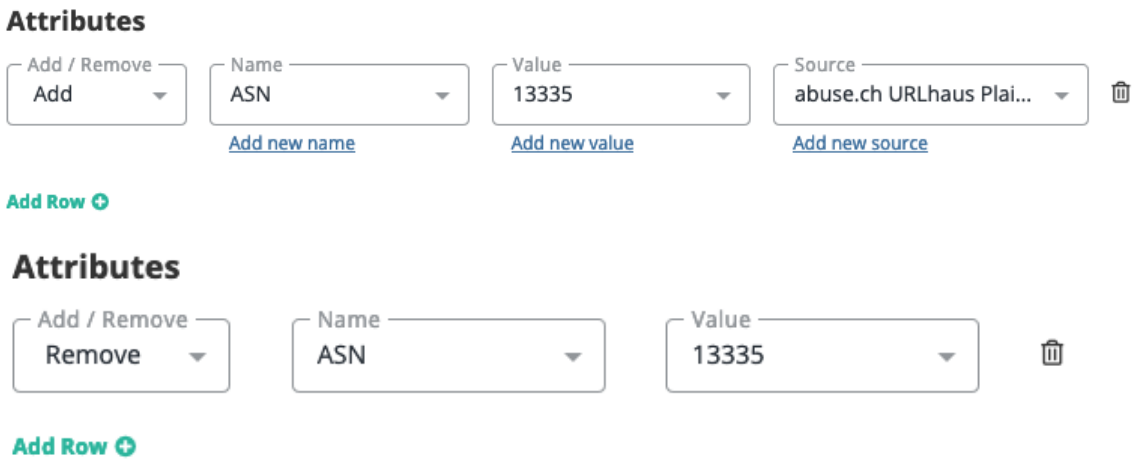


3. Click the **All <System Object>** or **Selected *<System Object>*** option under the *Bulk Changes* heading.
   The Bulk Changes page is displayed.



> 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.



Click **Add Row** and repeat steps 4-5 to add/remove multiple attributes. See the Scenarios section below for more details.

6. Click the **Apply Changes** button located at the bottom of the form.

Bulk Add/Remove Attribute Scenarios

Add Multiple Attributes

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

   Results

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

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

Remove Multiple Attributes

1. The user narrows down the Threat Library using advanced search filters.
2. The user selects **Bulk Changes** from the **Actions** dropdown.

3. The user selects **Remove** from the dropdown in the *Attributes* section and then enters the **Attribute Name**, **Value**, and **Source** for the first row.
4. The user clicks on **Add Row**.
5. The user selects **Remove** from the dropdown and then enters the **Attribute Name**, **Value**, and **Source** for the second row.
6. The user clicks on **Apply Changes**.

   Results

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

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

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

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

Add and Remove Attributes

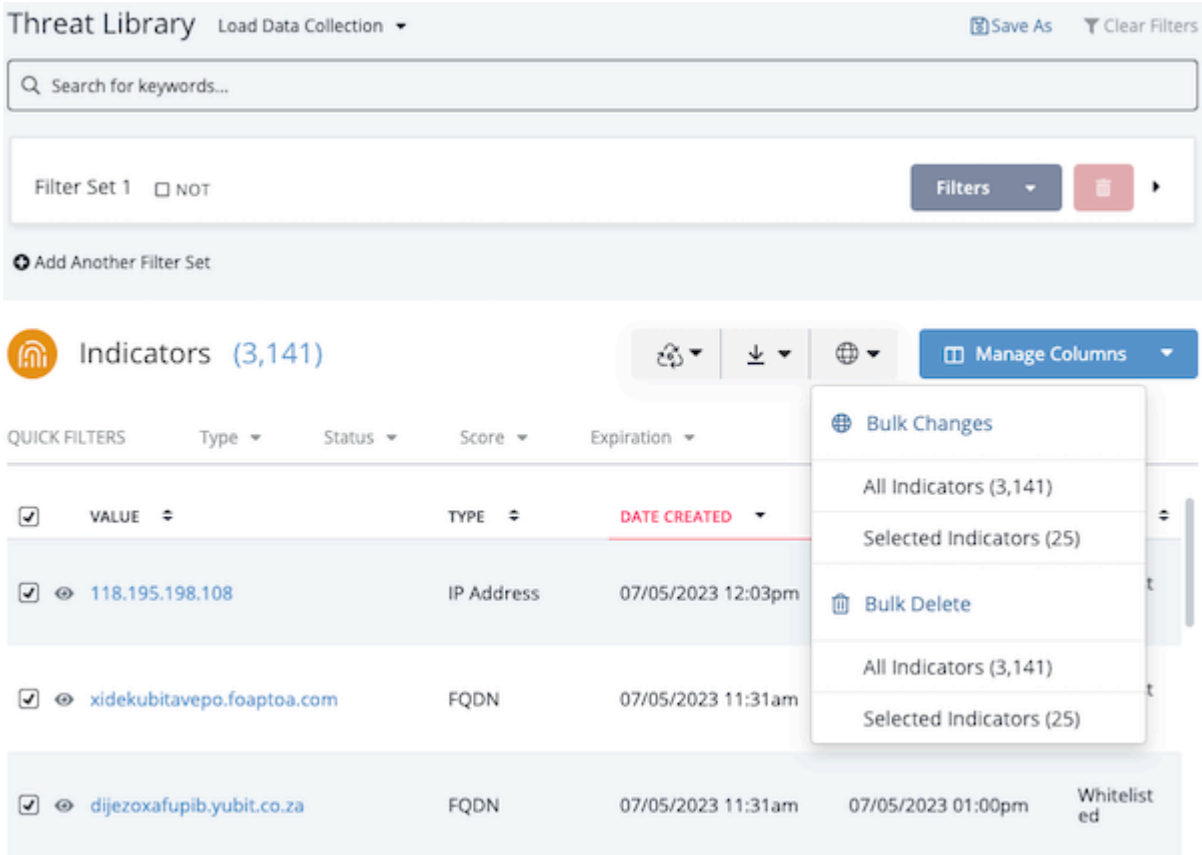
In this scenario, the platform will execute the Bulk Changes in the following order:

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

Bulk Add/Remove Tags

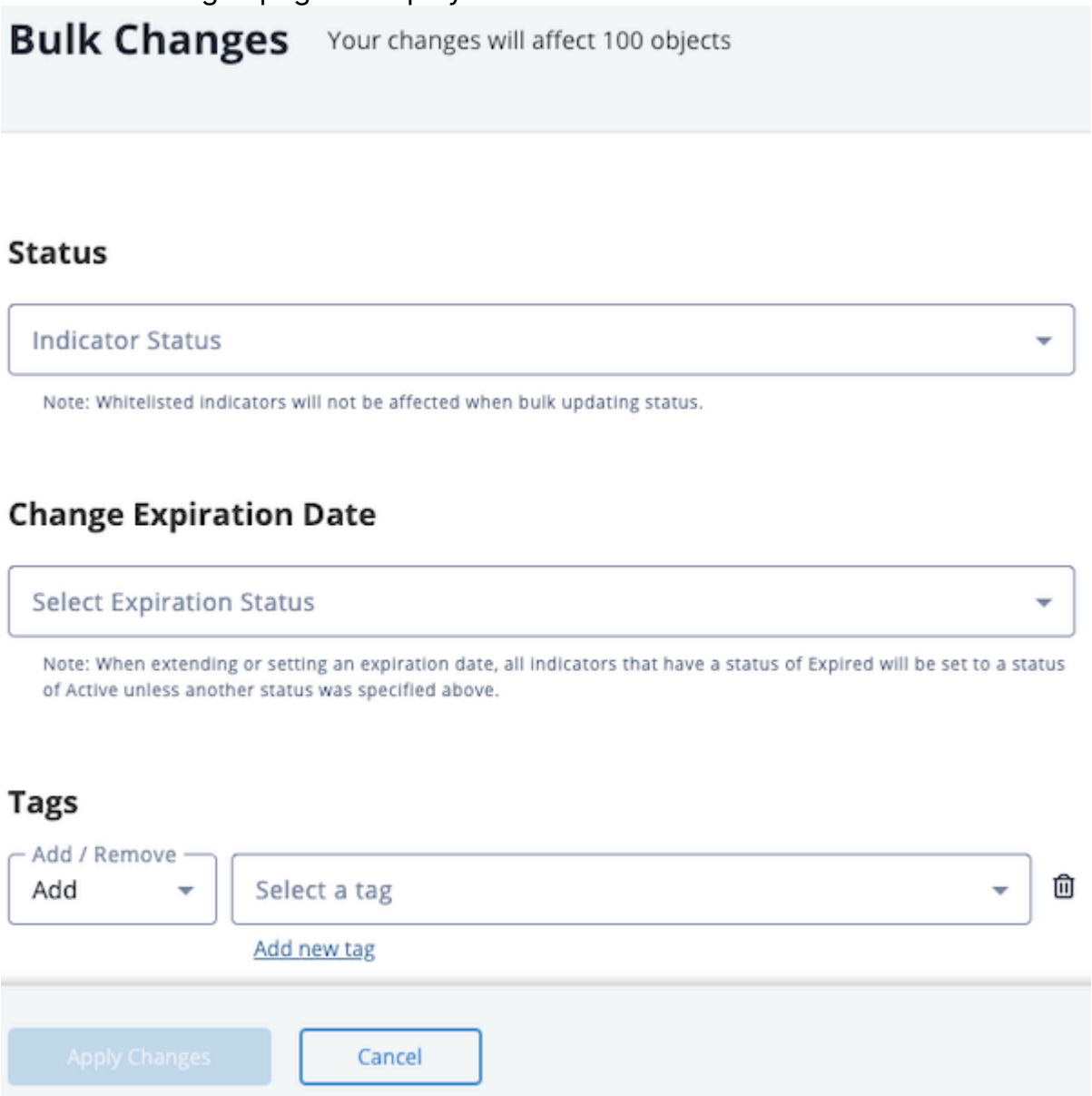
1. Perform a search on the Threat Library.

2. Click the **Bulk Actions** button .

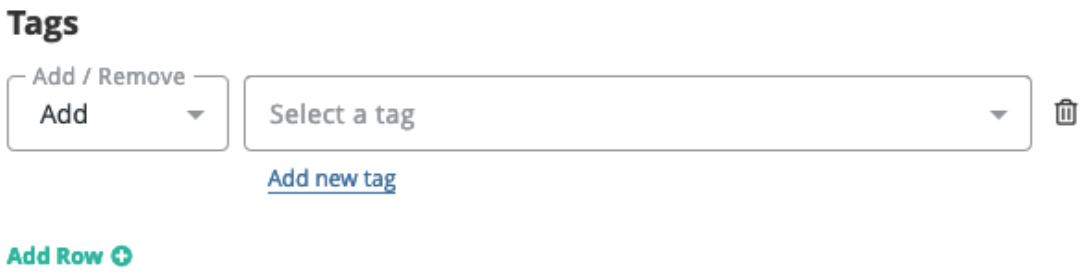


3. Click the **All <System Object>** or **Selected *<System Object>*** option under the *Bulk Changes* heading.

The Bulk Changes page is displayed.



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.



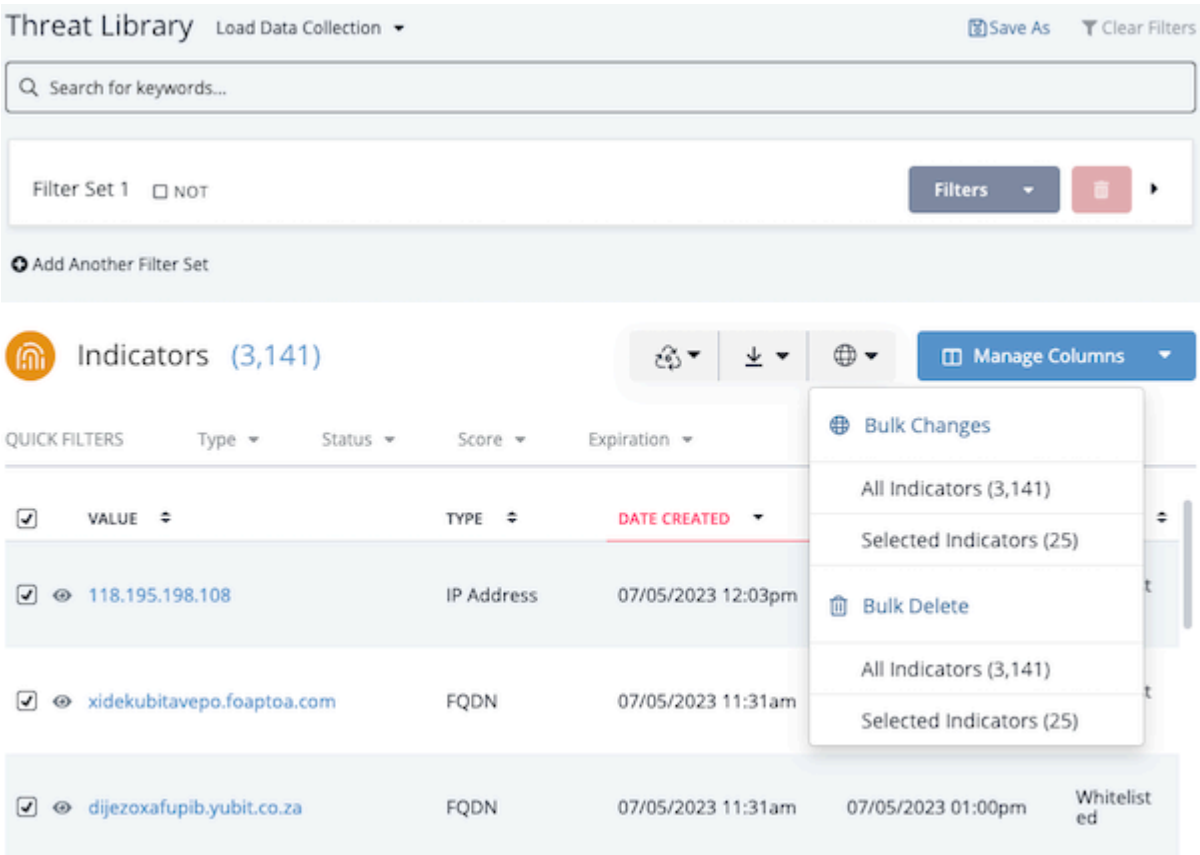
Click on **Add Row** and repeat step 3 to add/remove multiple tags.

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

Bulk Change Expiration Date

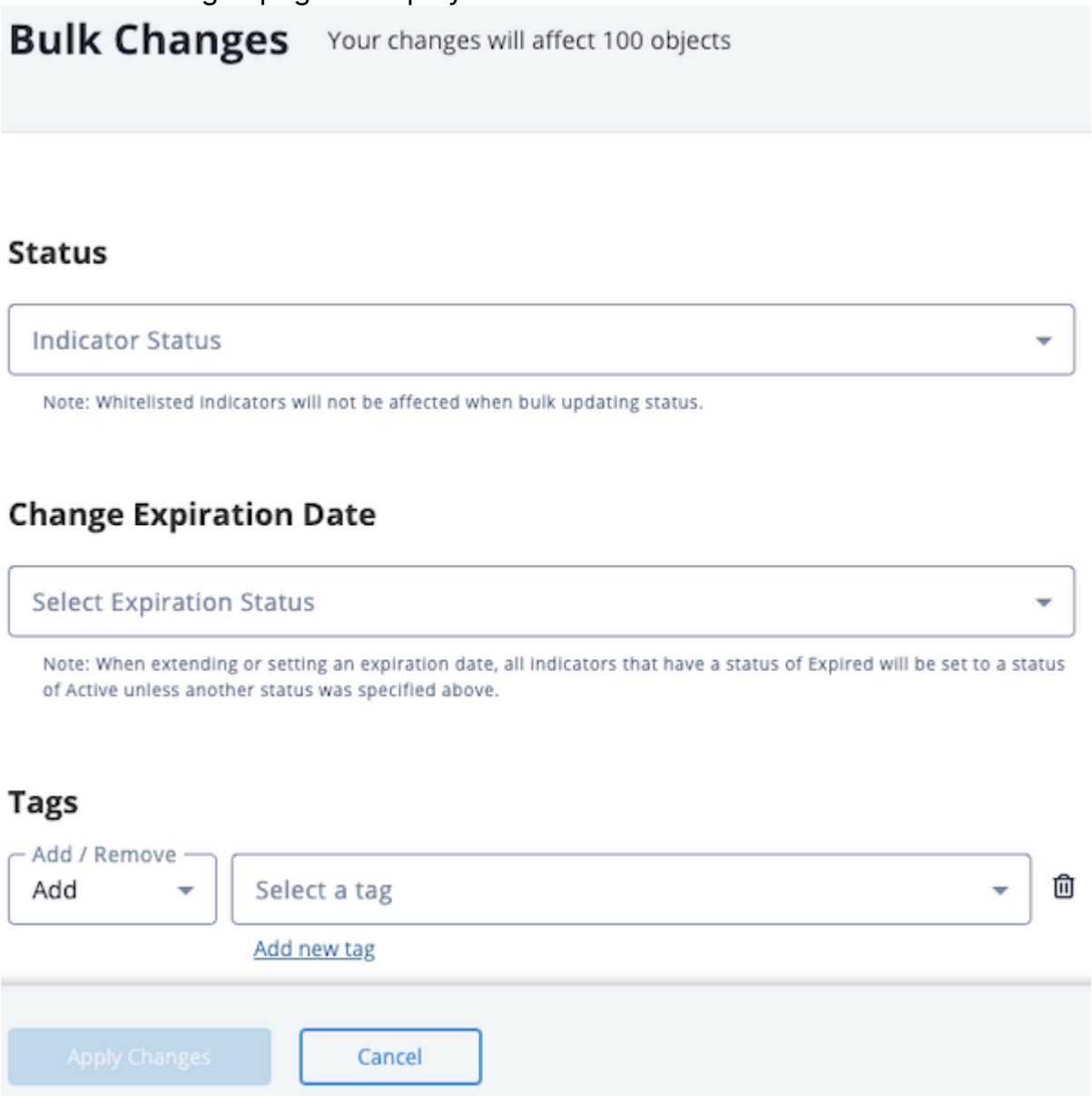
This function can only be performed on Indicators.

1. Perform a search on the Threat Library.
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.



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.

5. 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

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

Setting Expiration policy to a specific day

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

   > The date selected must be a future date.

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

Extending the expiration policy by a number of days

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

Remove an expiration policy

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

Protecting items from auto-expiration

1. The user selects a set of indicators using the advanced search.
2. The user selects **Protect from Auto-Expiration** from the Change Expiration option.

3. After submitting the request, all indicators in that record set will have the **protect from auto-expiration** expiration policy applied.

Extending/Setting an expiration date of an indicator with a status of Expired

1. The user selects a set of expired indicators using the advanced search.
2. The user selects **Set a New Expiration Date** from the Change Expiration option.
3. The users selects a day using the date picker.
   The date selected must be a future date.
4. After submitting the request, the expired indicators in that record set are then changed to a status of Active and the expiration date is set to the date indicated with the date picker.

Extending/Setting an expiration date of an indicator with a status of Whitelisted

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

Removing an expiration date on a previously expired indicator

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

Bulk Delete

The Bulk Delete feature offers users with Maintenance and Administrative roles the ability to select and delete system objects of all types, excluding Files and Tasks, from the Advanced Search page. In addition to the system object, bulk delete will also delete all child records such as attributes and relationships.

> Individual Tasks and Files can be deleted by accessing the object's details page and selecting Delete Task/File from the Actions menu.

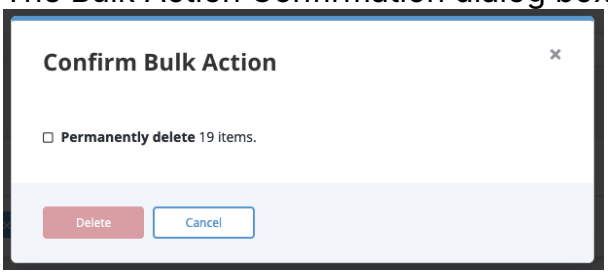
Once selected, the job process will run in the background and allow you to continue working within ThreatQ. An in-app notification will alert you when a Bulk Delete job has been queued and when it has been completed. You can also view the status and outcome of the job from the Job Management page.

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

Based on the size of your bulk delete job and the system resources available, you may find that the estimated job duration is quite long. In these rare instances, contact ThreatQ support to explore your other options for deleting a large number of objects.

1. Perform a search on the Threat Library.
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.



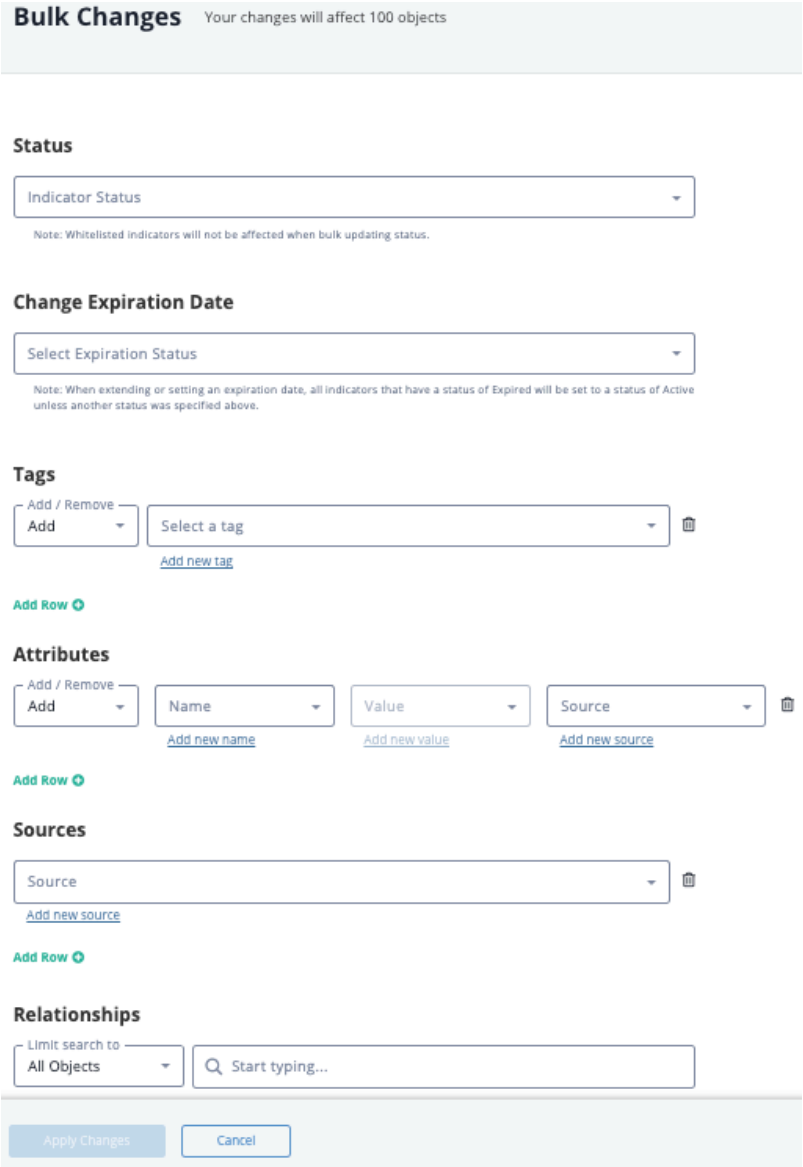
3. Click the checkbox to confirm deletion and then click the **Delete** button.

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.

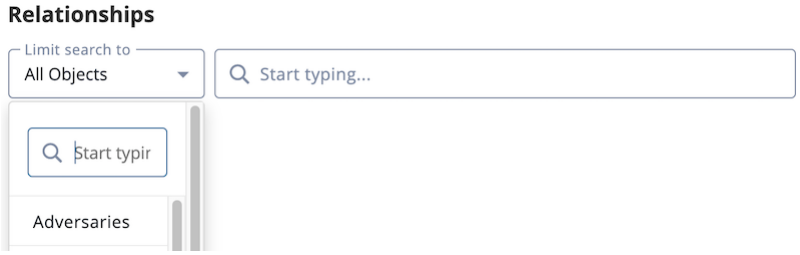
If an object is already associated with the source selected for the Bulk Add Relationships action, the object will be skipped during the bulk process.

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.



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.



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 **US**Bferry and **US**BStealer.
> 2. When you enter "%us" or "*us", your search returns Aquari**us**, Lazar**us** Group, D**us**t Storm, **US**Bferry, and **US**BStealer.

6. After you select an object, the Add/Remove option appears.

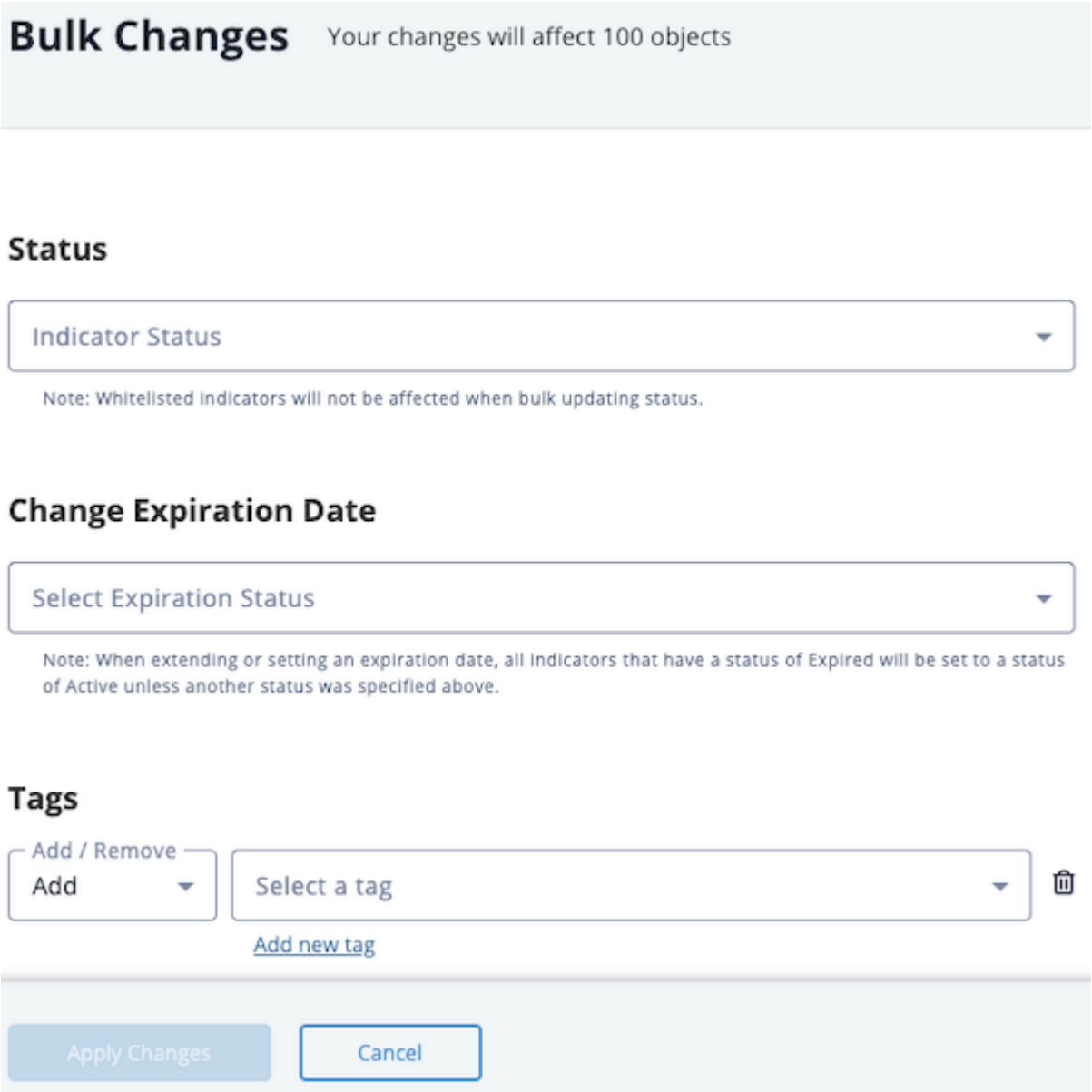
7. Select either **Add** or **Remove**.
8. Use the dropdown to select the source to add to the selected objects. You can also use the **Add New Source** link to add a source that is not listed in the dropdown.
9. Click the **Apply Changes** button located at the bottom of the form.

Bulk Status Change

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



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

> If you no status types are configured for an object, the Status field is not displayed.

> For Event and custom objects, you can select the None option to remove the statuses assigned to the objects.

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

Object Details Page

About Object Details Page

THREATQ REQUIRED PERMISSIONS

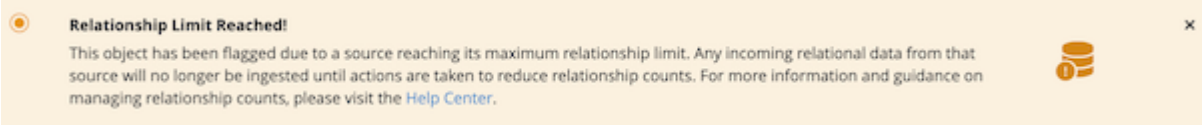
Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role - Action Permissions: Objects & Context - Individual Object Context & Actions

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.

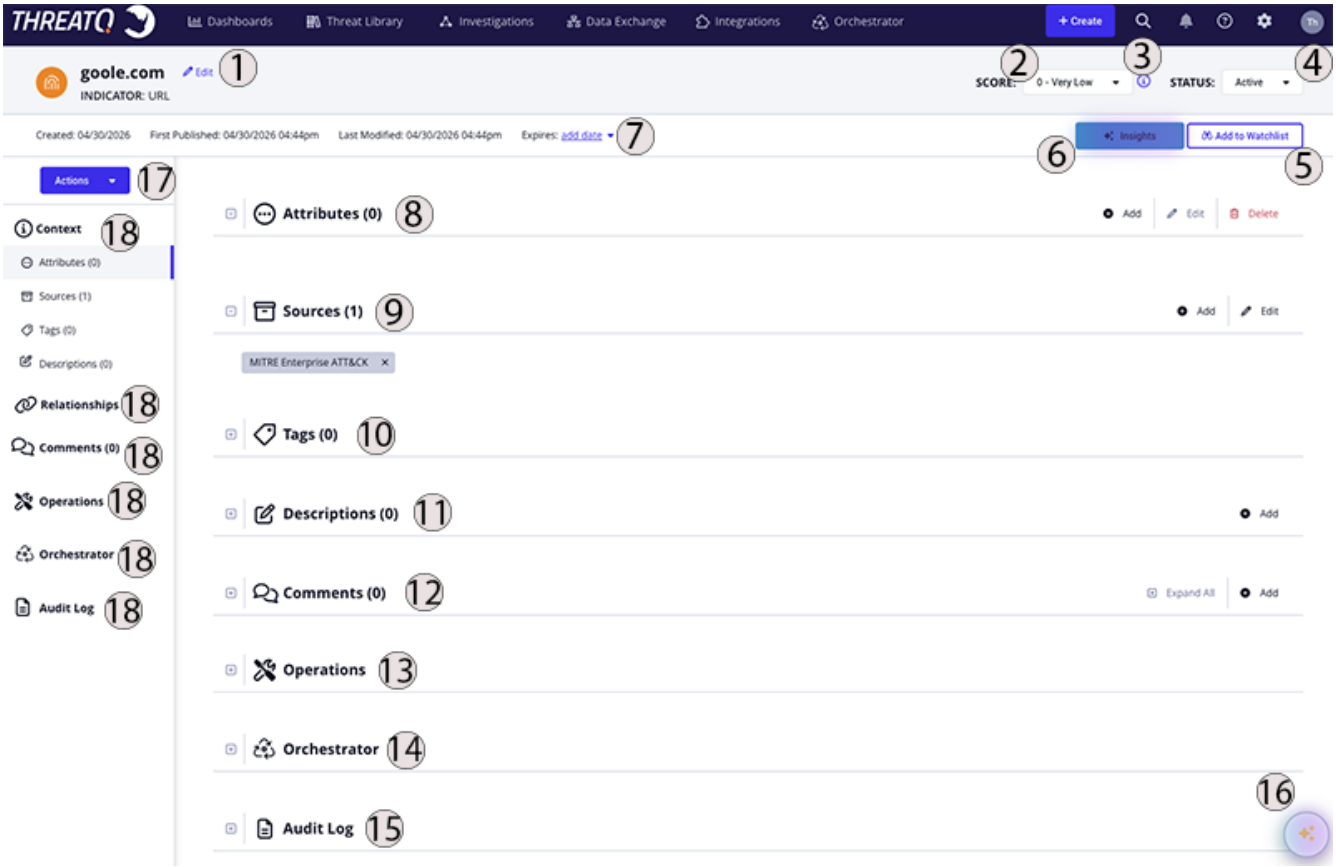
Specific objects, such as Indicators, display additional information such as score, and expiration data.

Relationship Limits

If an object has more than 10,000 relationships from the same source, the Relationship Limit Reached banner is displayed at the top of the object details page until you close by clicking the X in the upper right corner or until you resolve the relationship limit issue.



In addition, the object's Sources pane displays a relationship limit badge with a tooltip listing the source that exceeded the limit. Within the tooltip, you can click the source to access a Threat Library view filtered by the related to (object name) and relationship criteria (offending source).



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	The Score Selection dropdown allows you to override an indicator's score set by the scoring algorithm. This applies to indicators, adversaries, and vulnerabilities.	• Manually Setting an Object's Score • Scoring Algorithms

OBJECT DETAILS PAGE LEGEND

3	Score Summary	You can click on the icon to review the criteria utilized by the application's scoring algorithm to generate the Indicator's score. This applies to indicators, adversaries, and vulnerabilities.	• Scoring Algorithms
	Point of Contact* Does not apply to Adversaries, Files, Indicators, Signatures, and Tasks	The Point of Contact menu allows you to select the ThreatQ display name of the point of contact for the object.	
4	Status* Does not apply to Adversaries, Files, Signatures, and Tasks	The Status dropdown menu allows you to manually set the status of an object.	• Indicator Status • Indicator Statuses Management (Object Management) • Object Statuses (Object Management)
5	Add to Watchlist	The Watchlist toggle button allows you to add and remove the object from the Watchlist widget.	• Add/Remove an Object to the Watchlist
6	Insights	**ThreatQ v6.20.0 and later:** Hovering over the **Insights** button displays two options:	• About the Threat Research Agent

OBJECT DETAILS PAGE LEGEND

		• **Quick** – Opens the Threat Research Agent and generates an AI-powered summary of the selected object directly in the chat. • **Full** – Opens the **Generate AI-Assisted Report** dialog to create a comprehensive AI-generated report for the selected object. **ThreatQ v6.19.x and earlier:** Selecting the **Insights** button opens the Threat Research Agent and automatically submits the selected object as context, allowing the agent to generate information related to that object. The **Insights** button is available only when the Threat Research Agent has been configured and enabled.	• Using the Agent
7	Expiration* Applies to Indicators Only	The Expire link allows you to set an expiration date for the indicator, protect from auto-expiration policies, and remove an existing set expiration date.	• Indicator Expiration • Indicator Expiration Policies (Data Controls)

Details Section

Any related or linked object types will be displayed in this section, organized by type. Only sections corresponding to object types associated

OBJECT DETAILS PAGE LEGEND

with the selected object will be shown. See the About Relationships Panes topic for more details.

Number	Pane	Description	Reference
8	Attributes	The Attributes pane displays attributes associated with the object. You can Add, Edit, and Delete attributes found in this section.	• Attributes Pane
9	Sources	The Sources pane displays sources associated with the object. You can Add, Edit, or Remove sources.	• Sources Pane
10	Tags	The Tags pane displays tags associated with the object. You can Add and Delete tags found in this section.	• Tags Pane
11	Descriptions	The Descriptions pane allows you to add, update, or delete object information.	• Descriptions Pane
12	Comments	The Comments pane allows you to record comments about the object for other users to read and reference.	• Comments Pane
13	Operations	The Operations pane allows you to associate third-party attributes and related indicators to the indicator. This option requires the installation of Operations. See the Managing	• About Integrations Management

OBJECT DETAILS PAGE LEGEND

		Integrations topic for more details.	
14	Orchestrator	Requires ThreatQ TDR Orchestrator. The Orchestrator pane lists the name of each TQO workflow that has processed the object and the workflow run timestamp.	• Orchestrator Pane
15	Audit Log	The Audit Log panel displays all actions and changes made to an Object.	• Audit Log
16	Threat Research Agent Bubble	Opens the Threat Research Agent window from the bottom-right corner of the platform to begin a manual query	• About the Threat Research Agent • Using the Agent

Left-Hand Navigation

Number	Field	Description	Reference
17	Actions Menu	The Actions menu lists the following options: • Add Attribute • Add Comment • Add Relationship • Add Source • Create Task • Generate PDF	• Actions Menu

OBJECT DETAILS PAGE LEGEND

		• Start Workflow (requires ThreatQ TDR Orchestrator) • Start Investigation (requires ThreatQ Investigations) • Add to Investigation (requires ThreatQ Investigations) • Delete	
18	Object Details Navigation Tabs	This allows you to jump to a particular pane on the Object Details page.	N/A

**** Indicates the object details page option is only available for specific object types.***

Manually Setting an Object's Score

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role - Action Permissions: Individual Object Context & Actions - Score

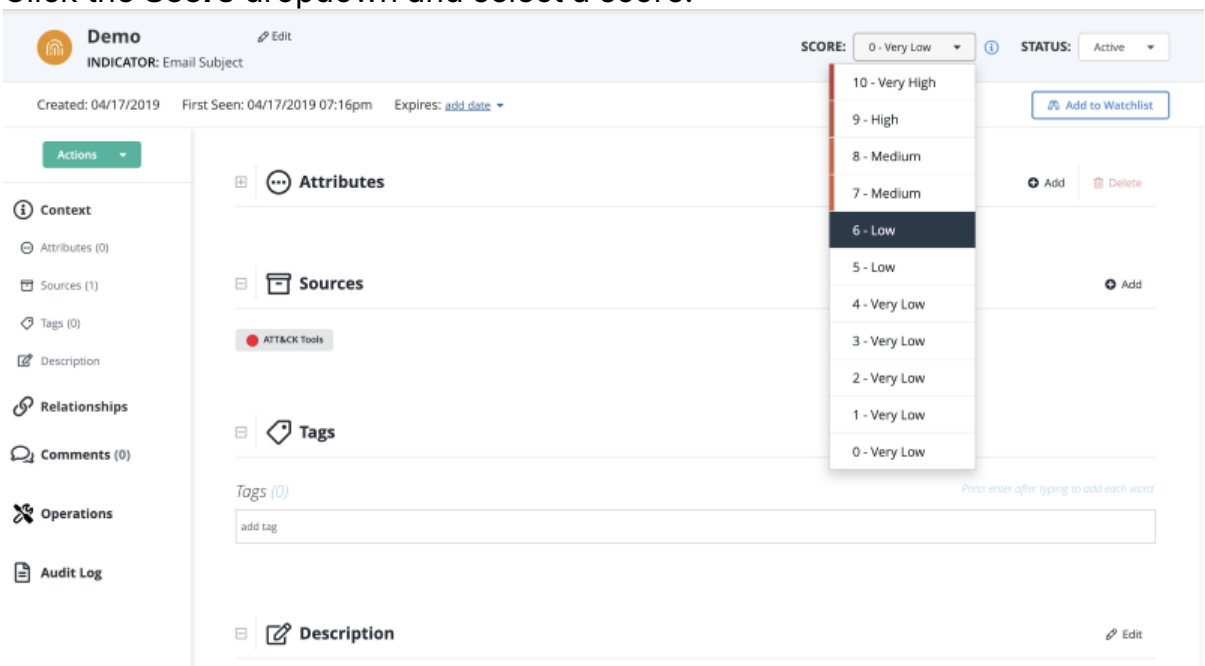
ThreatQ scoring allows you to apply weighting to indicators, adversaries, and vulnerabilities along with their contextual information, such as sources, types, and attributes as they are added to ThreatQ.

See the Scoring Algorithms topic for further details on configuring scoring algorithms.

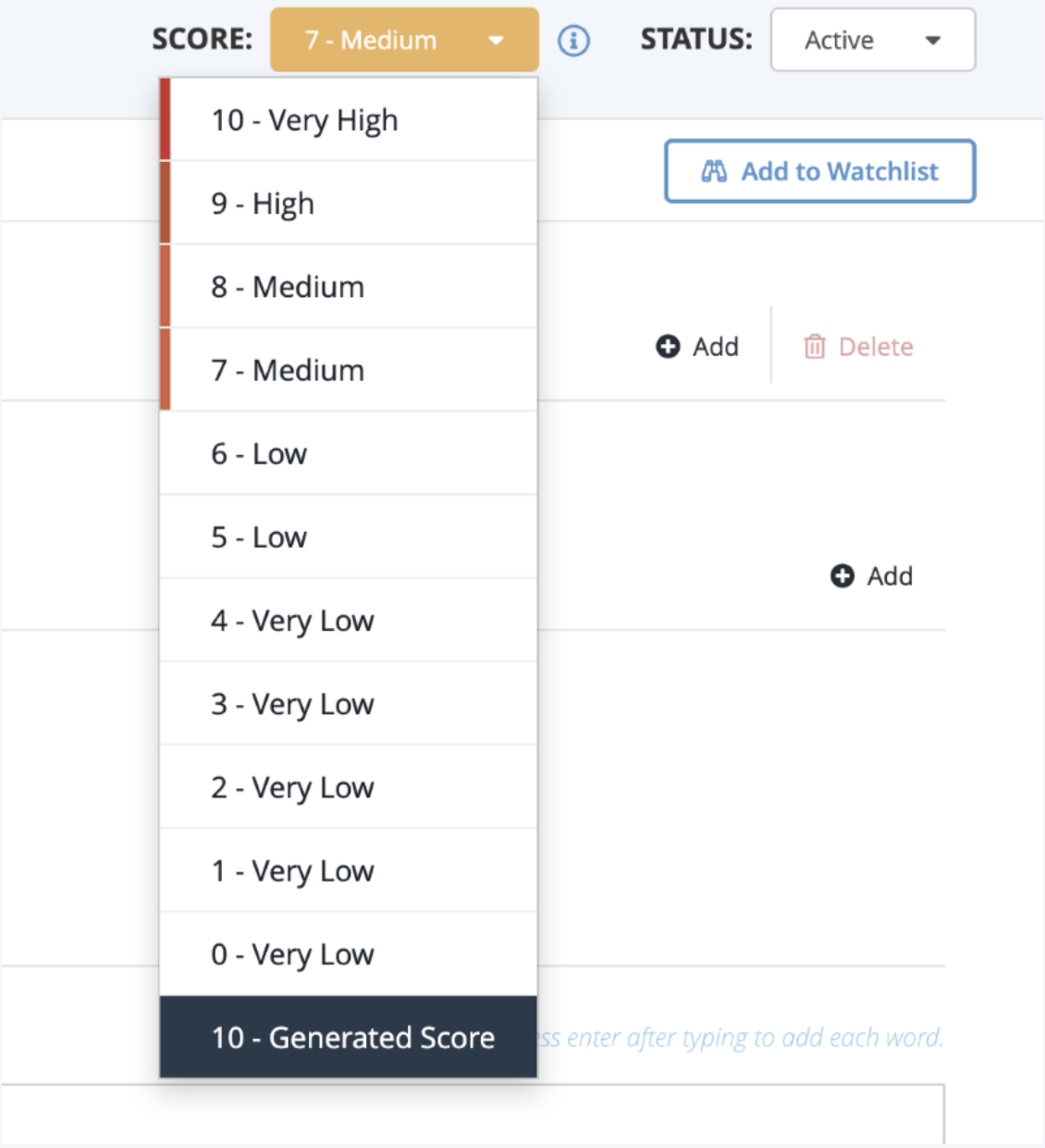
Setting a Manual Score for an Object

You can use this process to override an individual object score set by the scoring algorithm.

1. Navigate to an objects's Details page.
2. Click the **Score** dropdown and select a score.



Optionally, you may revert to the calculated score by clicking on the Score dropdown and selecting **Generated Score**.



Adding/Removing an Object to the Watchlist

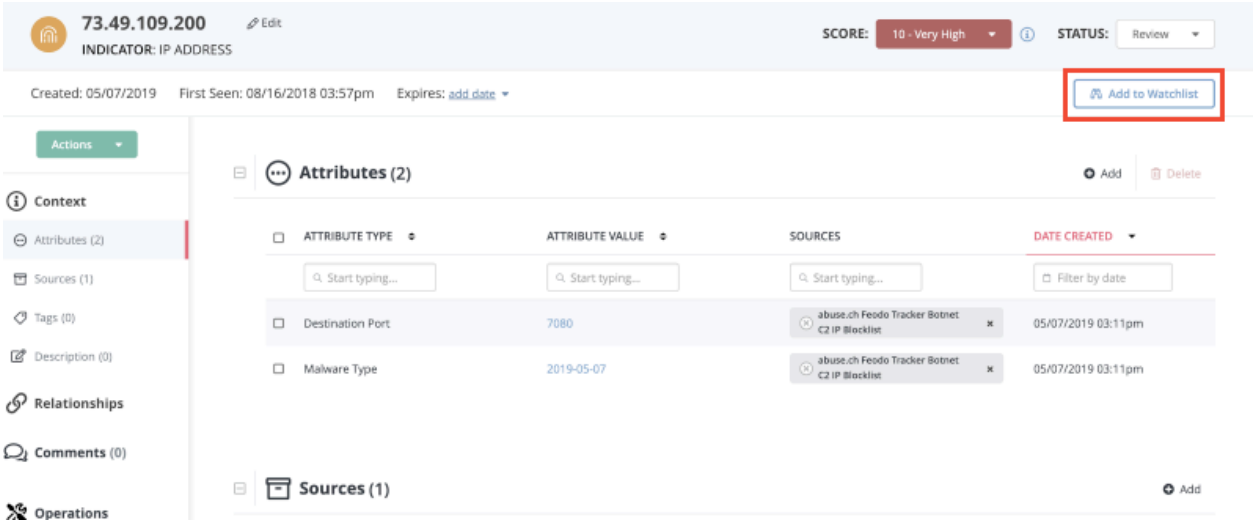
THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role - Action Permissions: Administrative Functions - View Audit Log, Objects & Context - Individual Object Context & Actions - Add to Watchlist, See the Interdependent Permissions topic.

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.



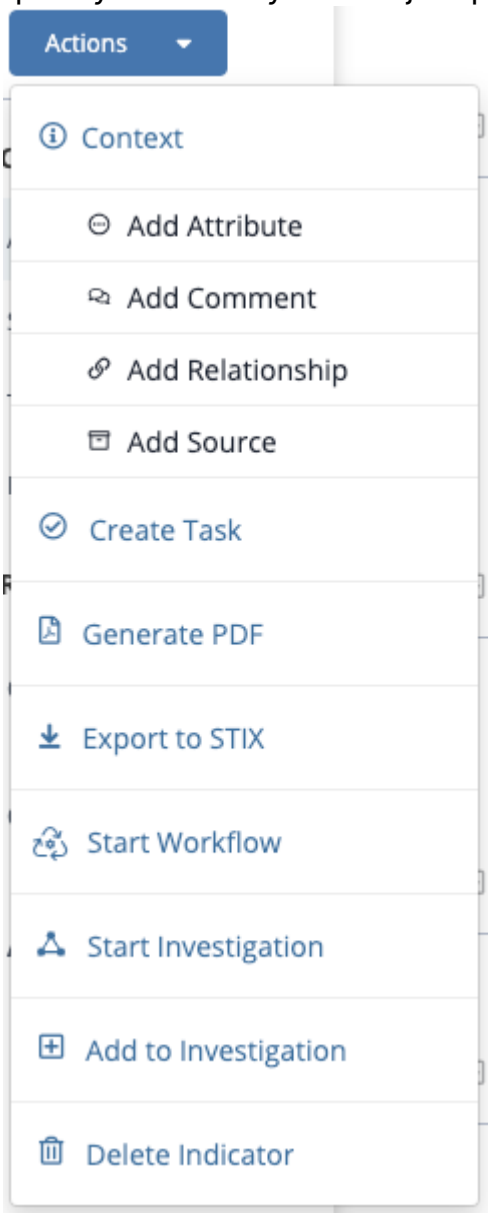
Depending on your selection, the object is added to/removed from the Watchlist on the system default dashboard.

Actions Menu

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role - Action Permissions: Objects & Context - Individual Object Context & Actions

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
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
Export to STIX	Exports the object's details to a STIX file.	• STIX Exports
Start Workflow	Applies a TQO workflow to the object.	• About Manually Triggered Workflows
Start Investigation	Opens the Create Investigation window so that you can create a new investigation to which the object is automatically added.	• Managing Investigations

ACTION	FUNCTION	REFERENCE
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

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role - Action Permissions: Objects & Context - Individual Object Context & Actions

Based on the system object type, the Context section of the object details page displays:

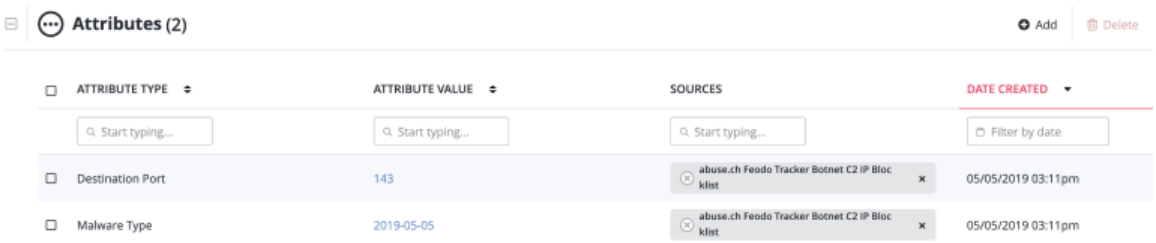
- Attributes
- Sources
- Tags
- Descriptions
- Spearphish Details

Attributes Pane

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role - Action Permissions: Objects & Context - Individual Object Context & Actions - Attributes

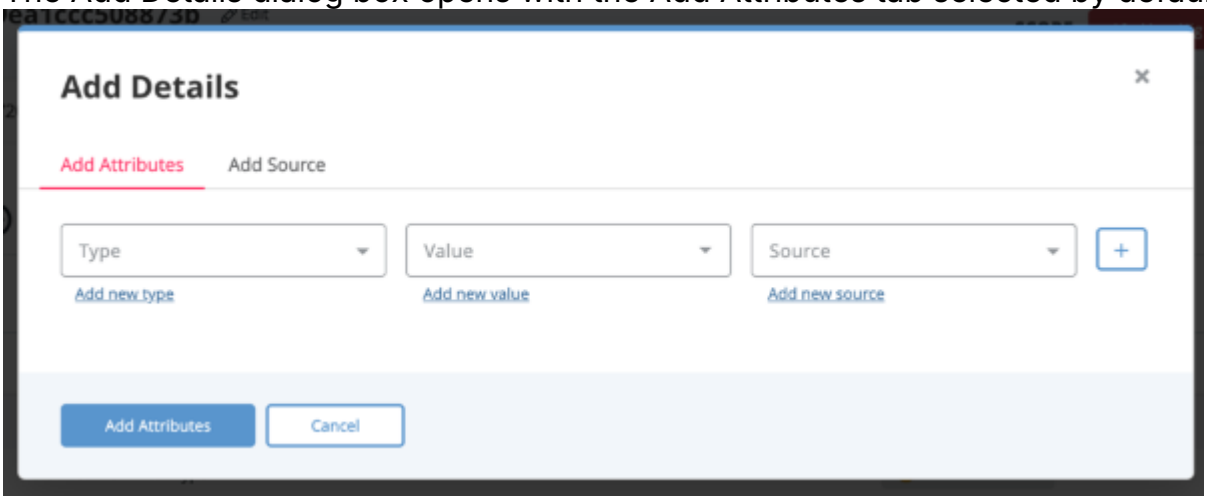
The Context section of the object details page displays attributes, sources, and tags associated with the system object.



Adding an Attribute to an Object

You can link attributes to a system object.

1. Locate the Attributes pane on the object details page.
2. Click on the **+ Add** link located to the top-right.
2. The Add Details dialog box opens with the Add Attributes tab selected by default.



3. Select an **Attribute Type** from the Attributes dropdown or enter a new type.
4. Select an existing **Attribute Value** from the dropdown or enter a new value.
5. Select a **Source** from the dropdown or enter a new source.

You can select the **+** icon to add additional attributes.

6. Select **Add Attributes**.

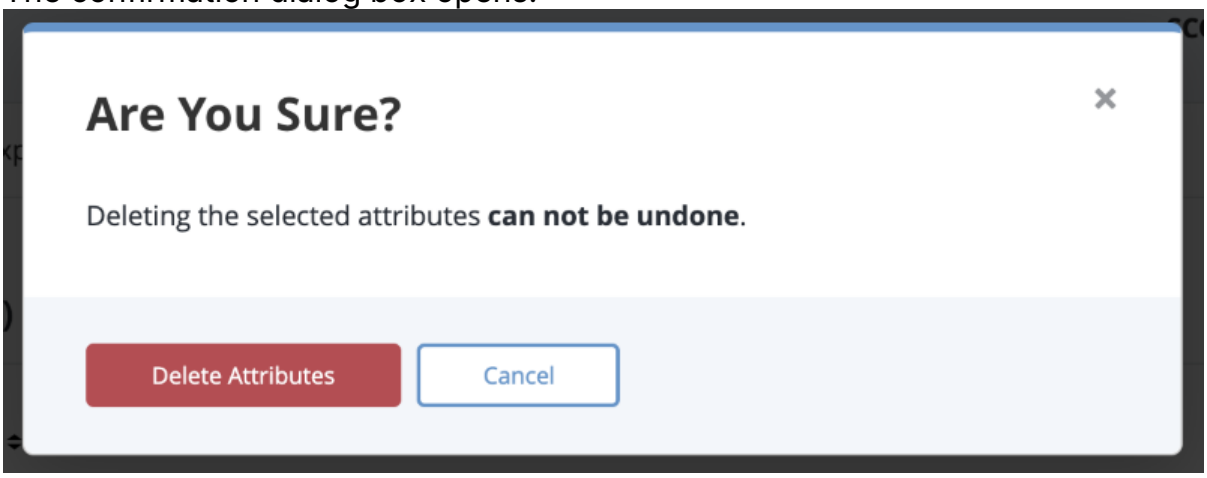
Deleting an Attribute from an Object

You can delete an attribute from the object details page.

1. Locate the Attributes pane on the object details page.
2. Select the checkbox next to the attribute you want to delete.

   You can select more than one attribute to delete

3. Select **Delete**.
   The confirmation dialog box opens.



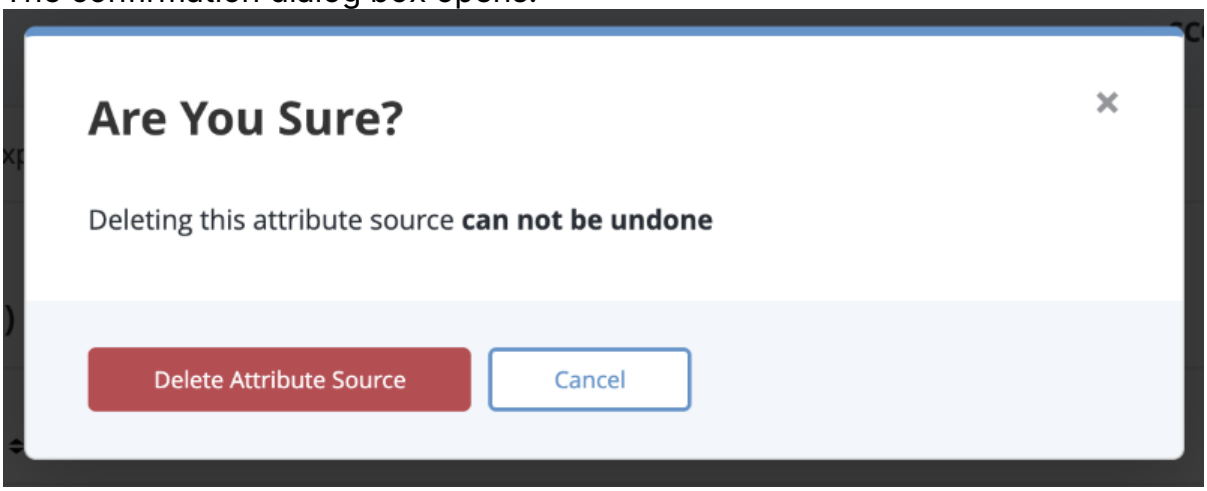
4. Select **Delete Attributes**.

Deleting an Attribute Source from an Object

You can delete an attribute's source from the object details page.

1. Locate the Attributes pane on the object details page.

2. Select the **X** next to the attribute's source.
   The confirmation dialog box opens.



3. Select **Delete Attribute Source**.

Editing an Object's Attribute

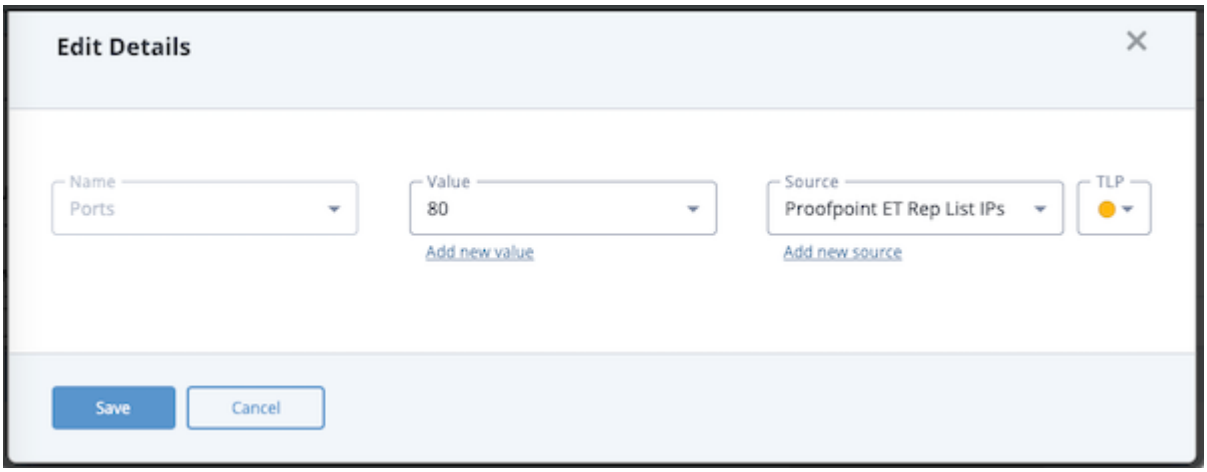
The Edit attribute option allows you to change an attribute's value and source as well as the source's TLP label.

1. Click the checkbox next to the attribute.

   > You can only edit one attribute at a time. If you check the box next to more than one attribute, the Edit option is disabled.

2. Click the **Edit** option in the Attributes pane to access the Edit Details window.

   > If an attribute has multiple sources, the Edit Details window displays a row for each source so that you can update each attribute as needed.



3. From the Edit Details window, you can:

- **Update the attribute's value** - Select a new value from the dropdown list or click the **Add new value** link to enter a new value.
- **Add an attribute's source** - Select the source you want to add from the dropdown list or click the **Add new source** link to enter a new source. The source you select/enter is added to the sources associated with the attribute. It does not replace the source originally associated with the attribute.
- **Select a new TLP label for the attribute's source** - When you add a new source to an attribute, you can use the TLP field to change the default TLP label associated with the source. If you did not add a new source, you can use the TLP field to change the TLP label assigned to the existing source. To select a new TLP label, click the arrow next to the current TLP label and select a new one.

4. After you make your changes, click the **Save** button.

Sources Pane

THREATQ REQUIRED PERMISSIONS

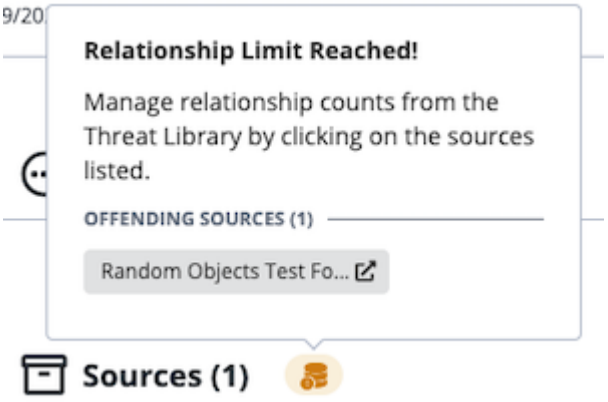
Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role - Action Permissions: Objects & Context - Individual Object Context & Actions - Sources

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.

Relationship Limits

If an object has more than 10,000 relationships from the same source, the Sources pane displays a relationship limit badge with a tooltip listing the source that exceeded the limit.

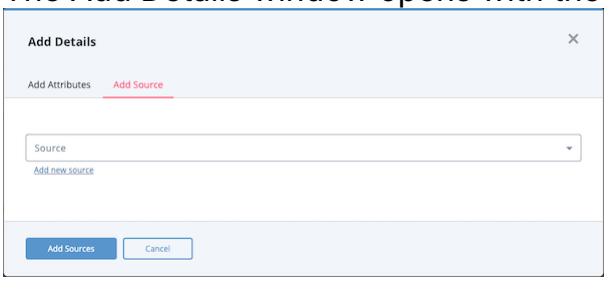


Within the tooltip, you can click the source to access a Threat Library view filtered by the related to (object name) and relationship criteria (offending source).

> If the offending source is not a feed, the Threat Library view does not list related objects. For example, if the offending source is a user (such as threatq@threatq.com) that added the relationships, when you click it, the Threat Library view does not list any related 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.



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.

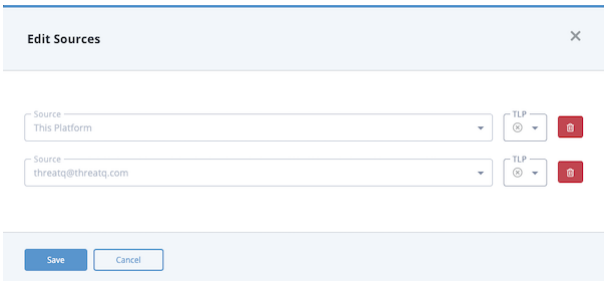
   > Even though the Source drop-down lists displays all sources, you cannot add a source to an object if it has already been added.

4. Click the **Add Sources** button.

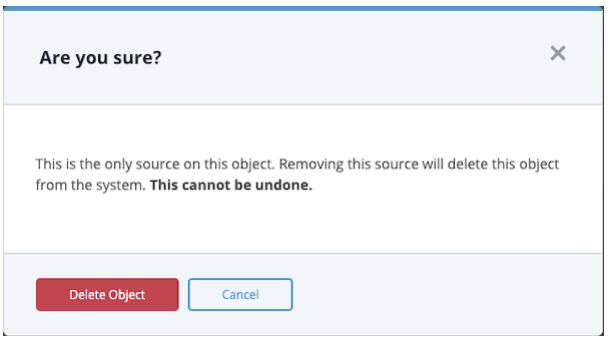
Editing a Source

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.

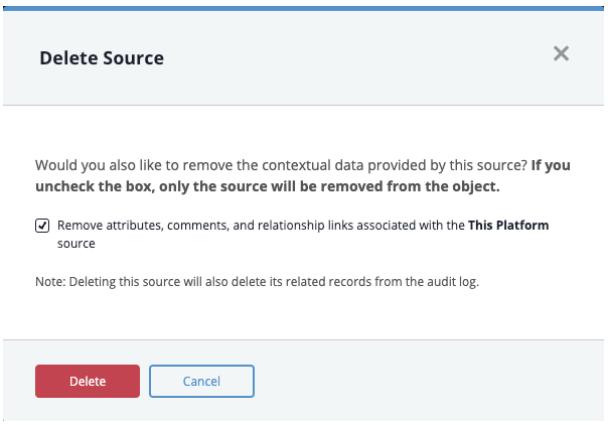
1. Locate the Sources pane on the object details page.
2. Click the Edit option.
   This Edit Sources window lists all the sources associated with the system object.



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.

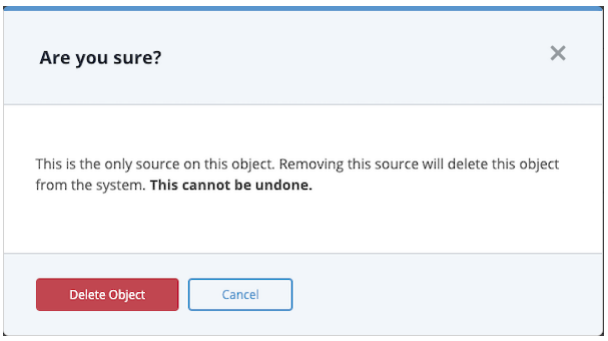
   Removing a relationship link does not delete the linked object. It only removes the link between the objects.

   To remove the source but retain its related context, uncheck the option.

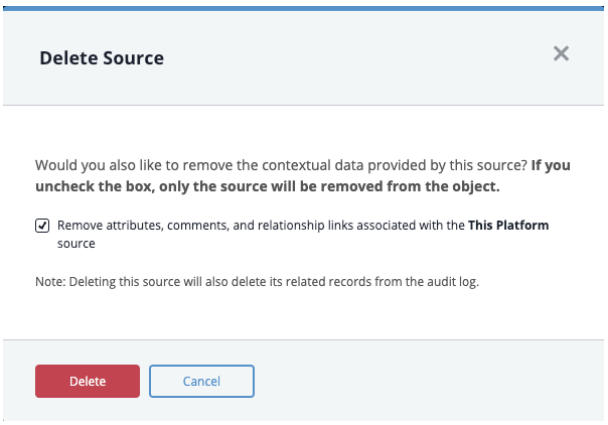
6. Click the **Delete** button.
   Deleted sources are recorded in the audit log as Removed. Removed contexts such as attributes, comments, or relationships are not recorded in the audit log.

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.



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.

Tags Pane

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role - Action Permissions: Objects & Context - Individual Object Context & Actions - Tags

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

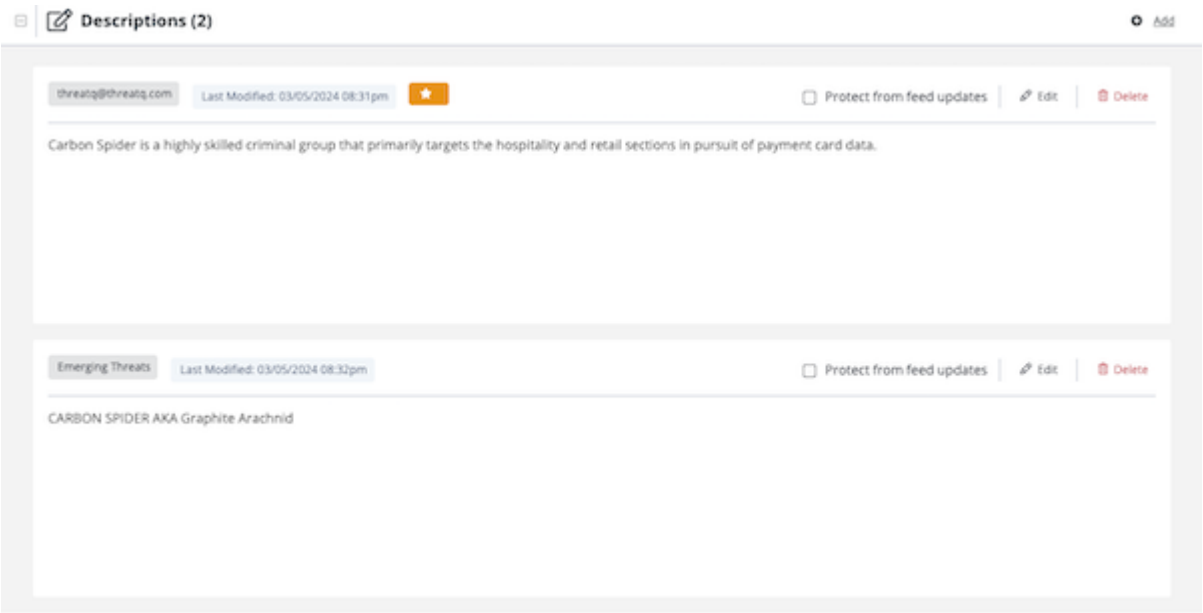
1. Locate the Tags pane on the object details page.
2. Select the **X** next to the tag name.

Descriptions Pane

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role - Action Permissions: Objects & Context - Individual Object Context & Actions - Descriptions

The Descriptions pane displays descriptions associated with a system object. The first description listed is the object's primary description and is identified with a white star on an orange background.



Primary Descriptions

For all new and existing system objects, one description is labeled as the primary description. In the object details page and object preview panel, this primary description is listed first and identified with a white star on an orange background as well as a hover tooltip that displays the Primary Description label.

STIX exports include an object's primary description only. If an object has multiple descriptions, only the primary description is included in the STIX export.

After upgrading to ThreatQ v5.28, the first description added to an object is designated as the primary description by default. For existing objects, the oldest description is the primary description. For objects with multiple descriptions, you can change which description is the primary description.

Description Header and Body

Each description consists of a header and a body. The description header lists the description source's TLP label, source name, last modified timestamp, feed update setting, as well as Edit and Delete options. The **Protect from feed updates** checkbox allows you to specify whether the description is updated when you ingest a description change from the integration source. This checkbox is not displayed for descriptions with internal sources since these description do not come from feeds and cannot be updated by feeds.

> The Descriptions pane truncates description source names that are over thirty characters long. You can view the full source name by hovering on the truncated version.

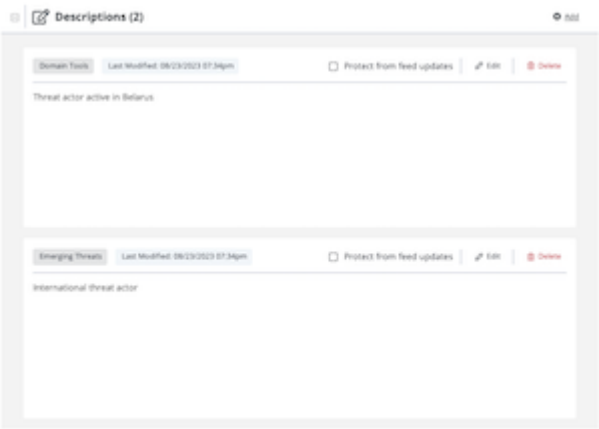
The description body can include text, tables, and images.

Description Guidelines

- An object can only have one primary description and one description per source.
- ThreatQ System Descriptions:
  - When you create an object and do not specify a source for the object, the description is assigned a source of ThreatQ System.
  - If a description's source is ThreatQ System, the **Protect from feed updates** option is not displayed.
  - If present, an object's ThreatQ System description is the first description listed in the Descriptions pane.
- If TLP functionality is enabled, you can view/update the TLP labels associated with description sources.
- When an existing indicator which already has a description is consumed with a new description with a different source, the new description is added. However, if the source is already associated with an existing object description and the description is not protected from feed updates, the ingested description updates the existing one.

Example - New Description and Source

	DESCRIPTION	SOURCE
Original	International threat actor	Domain Tools
Ingested	Threat actor active in Belarus	Emerging Threats

	DESCRIPTION	SOURCE
New		

Example - New Description, Same Source, Protect from feed updates Unchecked

	DESCRIPTION	SOURCE
Original	International threat actor	Domain Tools
Ingested	Threat actor active in Belarus	Domain Tools
New		

Tips and Tricks

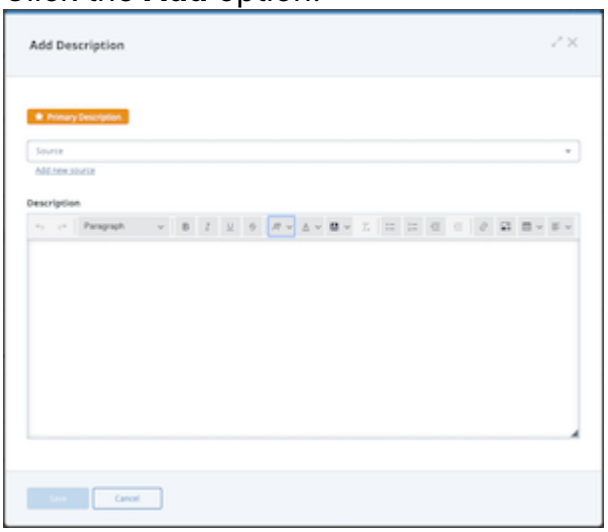
- **Images:**
  - **Image alignment** - Images in an object's description are displayed in the PDF report for the object as left aligned regardless of the alignment you select in the Description pane.
  - **Image captions** - Add your image captions after you select your image alignment. If you change 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.
- **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.

- **Formatting:**
  - **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.
  - **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.
  - **Text formatting** - To apply the HTML <pre> tag to text, click the heading field and select the Formatted option.
- **Navigation:**
  - The Add Description and Edit Description windows include an expand view option in the upper right corner. Click this option to access a full page view which reduces the need for scrolling when adding or updating a description. Click the minimize view option to return to the original window size.

Adding a Description to an Object

1. Locate the Description pane on the object details page.
2. Click the **Add** option.



3. From the Add Description window, populate the following fields:

- **Source** - Required field. Click the Source field to select the description's source from the dropdown list. Or, click the Add new source option to create a new source for the description. The source name cannot exceed 255 characters in length.

  > If you type the name of a source already associated with one of the object's descriptions, ThreatQ returns the following error: **A description with this source already exists.**
  > You must enter or select a different source before you can add the description.

- **Description** - Enter the object description. See the Tips and Tricks section for more information on your description options.
- **Mark as primary description** - Since an object's first description is its primary description by default, this field is not displayed when you add the first description to an object. For subsequent descriptions, you can check this box to select the description as the object's primary description.

4. Click the **Save** button.
5. To view the new description, expand the Descriptions pane.
6. Optional step. To prevent feed updates from updating the description, click the Protect from feed updates checkbox. If this box is unchecked, the following rules apply when an existing indicator with description is consumed with a new description:
   - If the new description has a different source, then the new description is added to the object.
   - If the new description has the same source, then the existing description is updated.

   > The Protect from feed updates field is not displayed for descriptions with a source of ThreatQ System.

Updating the Description of an Object

1. Locate the Description pane on the object details page.
2. Locate the description you want to update.
3. Click the **Edit** option for the description to add/update the object description's text, tables, or images. You can also use check the Mark as primary description box to identify a new Primary Description.
4. Enter your changes and click the **Save** button.

Deleting a Description

1. Locate the Description pane on the object details page.

2. Locate the description you want to delete.
3. Click the **Delete** option for the description.
   The Are You Sure? window prompts you to confirm the deletion. If you are deleting a primary description, the Are You Sure? window also indicates that the oldest description will become the new primary description.
4. Click the **Delete Description** button.

Spearphish Details Pane

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role - Action Permissions: Objects & Context - Objects

You can update spearphish file details as well as add or delete recipients from the Spearphish Details pane in a Spearphish event's object details page.

Adding a Recipient

1. Locate the Spearphish Details pane on the object details page.
2. Click the Add Recipients option.
   The Add Recipients window is displayed.
3. Populate the following fields:
   - **Recipient type** - This field defaults to a value of To. Use this field to specify whether the email was sent directly to the recipient (To) or the recipient received it as a carbon copy (CC) or blind carbon copy (BCC).
   - **Email address** - Enter the email address that received the spearphish file.
   - **Link all emails as related indicators** - This field defaults to checked. Leave this box checked to add a releated indicator record to the system object for each email address.
4. To add another recipient, click the + button and repeat step 3.
5. 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.
3. Enter your changes in the Email Content field.

4. Click the Save button.

Comments Pane

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role - Action Permissions: Objects & Context - Individual Object Context & Actions - Comments

The Comments pane allows you to add comments about the system object for other users to see.

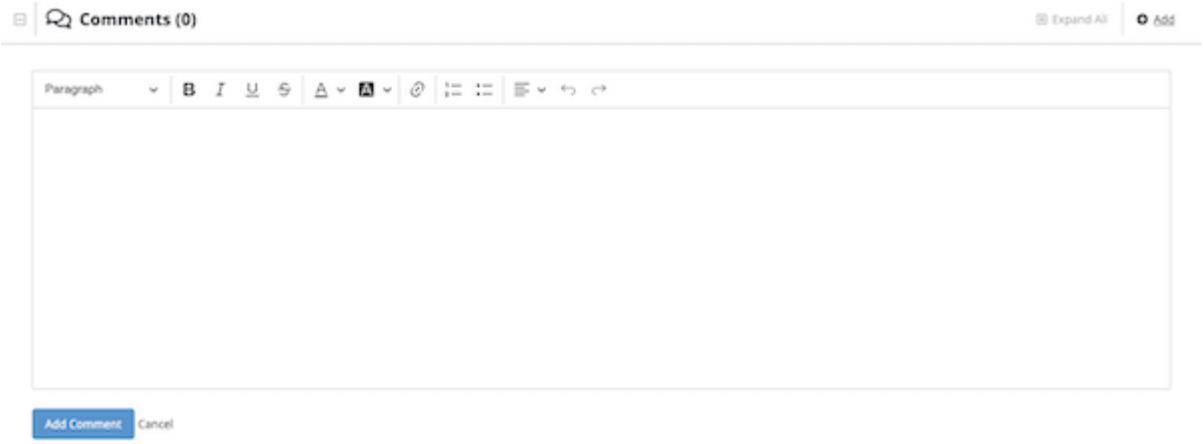
Tips and Tricks

- **Comment Display:**
  - By default, each comment displays up to four lines of text. For longer comments, you can click the **Show More** option to view the full details. You can then click the **Show Less** option to return to the truncated view.
  - The **Expand All/Collapse All** option in the Comments pane header allows you to expand/collapse all of an object's comments. If an object does not have any comments, this option is grayed out.
- **Formatting:**
  - The comment toolbar gives you the option to:
    - Apply styles to comment text.
    - Apply inline formatting such as bold, italics, underline, or strikethrough to comment text.
    - Select a font color and font background color.
    - Insert a link.
    - Add a numbered or bulleted list.
    - Specify text alignment.
    - Undo or redo a text change.
  - The formatting in the comment field is reflected in the PDF export of the system object.

Adding Comments to an Object

Users can also click on the **Actions** menu and select the **Comment** option.

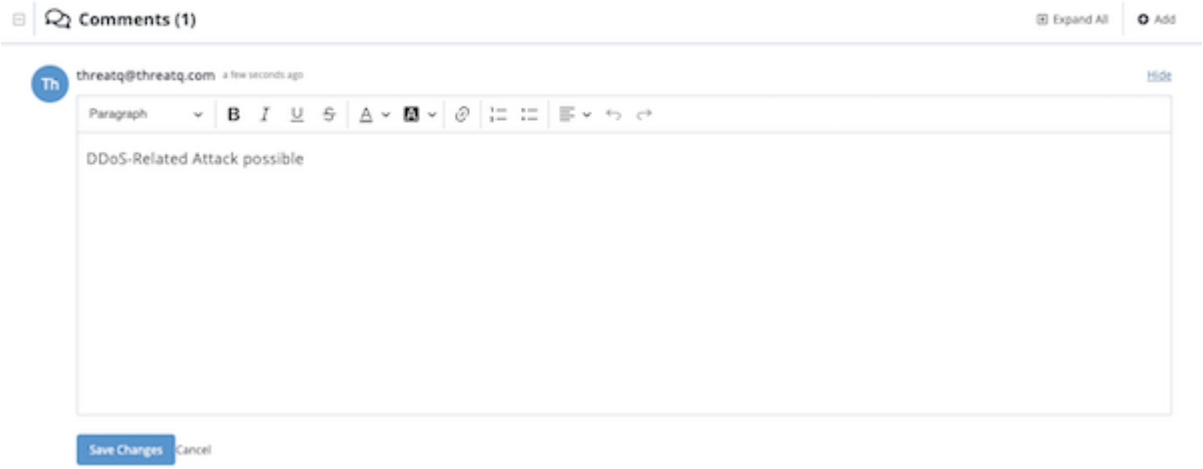
1. Click the **Add** link located at the top-right of the pane.
   The new comment text box opens.



2. Enter a comment.
3. Click the **Add Comment** button.

Editing Comments for an Object

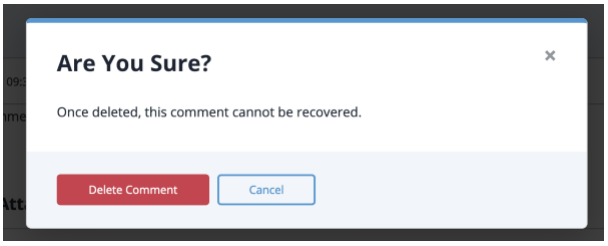
1. Click the **Edit** link located beneath the comment you want to update.
   The edit comment text box opens.



2. Edit the comment.
3. Click the **Save Changes** button.

Deleting Comments from an Object

1. Click on the **Delete** link located beneath the comment to update.
   The delete confirmation dialog text box opens.



2. Click the **Delete Comment** button.

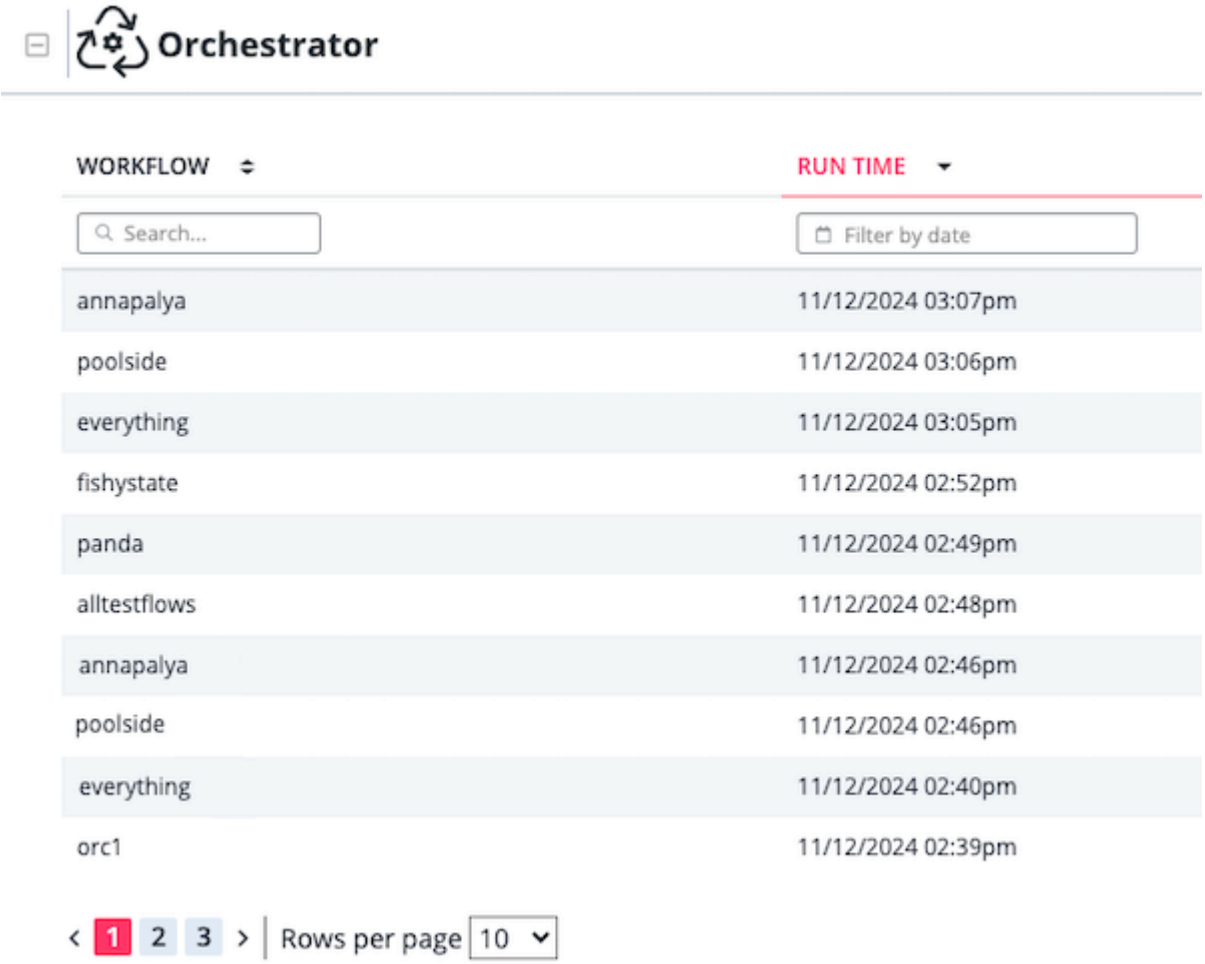
Orchestrator Pane

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role - Action Permissions: See the Interdependent Permissions topic.

To view the Orchestrator pane, your ThreatQ instance must have an active ThreatQ TDR Orchestrator license.

In an object's detail page, the Orchestrator pane lists the name of each TQO workflow that processed the object and the workflow run timestamp.



Tips and Tricks

- You can sort the list of workflows by workflow name or timestamp.

- The Rows per page field allows you to control the number of records, 10, 25, 50, or 100, displayed in each page of the Orchestrator pane.
- The Orchestrator pane lists deleted as well as enabled/disabled workflows.
- The Workflow column displays "Deleted Workflow" for any workflow deleted from ThreatQ after processing the object.
- The Orchestrator pane lists the last ninety days or last 10,000 workflow runs applied to the object, whichever is greater.
- The Orchestrator pane lists entries for all objects included in a workflow run even if the workflow does not support enrichment of the object type. For example, if Workflow A only enriches indicators and the associated data collection includes the Spider1 adversary, the Orchestrator pane lists Workflow A for Spider1.

Audit Log

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor
Custom Role - Action Permissions: Administrative Functions - View Audit Log

The ThreatQ Audit Log tracks every change made to every object in the system. If there is a change to an object, that change is displayed in the audit log. The audit log is only updated if the data itself changes, not just the updated_at value.

The following questions below address further details about the audit logging process.

In the case where an activity is triggered (with nothing updated), where will the activity be logged?
The activity will not show in the audit log, as there were no changes to report. While ThreatQ does not track duplicate objects that enter the application, there is a touched_at date field on primary objects (Adversaries, Files, Events, Indicators, and Signatures) that indicates when a relation of the object has been changed.

Is there another raw audit log within the system where events are logged?
No, there are no other raw audit logs where events are logged.

Is there an option in the User Interface to enable all activities to be shown in the Audit Log?
There is no option in the User Interface to limit or expand the audit log. All entries are pulled for an object when the Audit Log panel is opened. The audit log displays changes to the individual fields of an object; object comments, sources, attributes, and tags; as well as to object links, object link comments, and object link attributes. Additionally, any changes to the score of an Indicator are included.

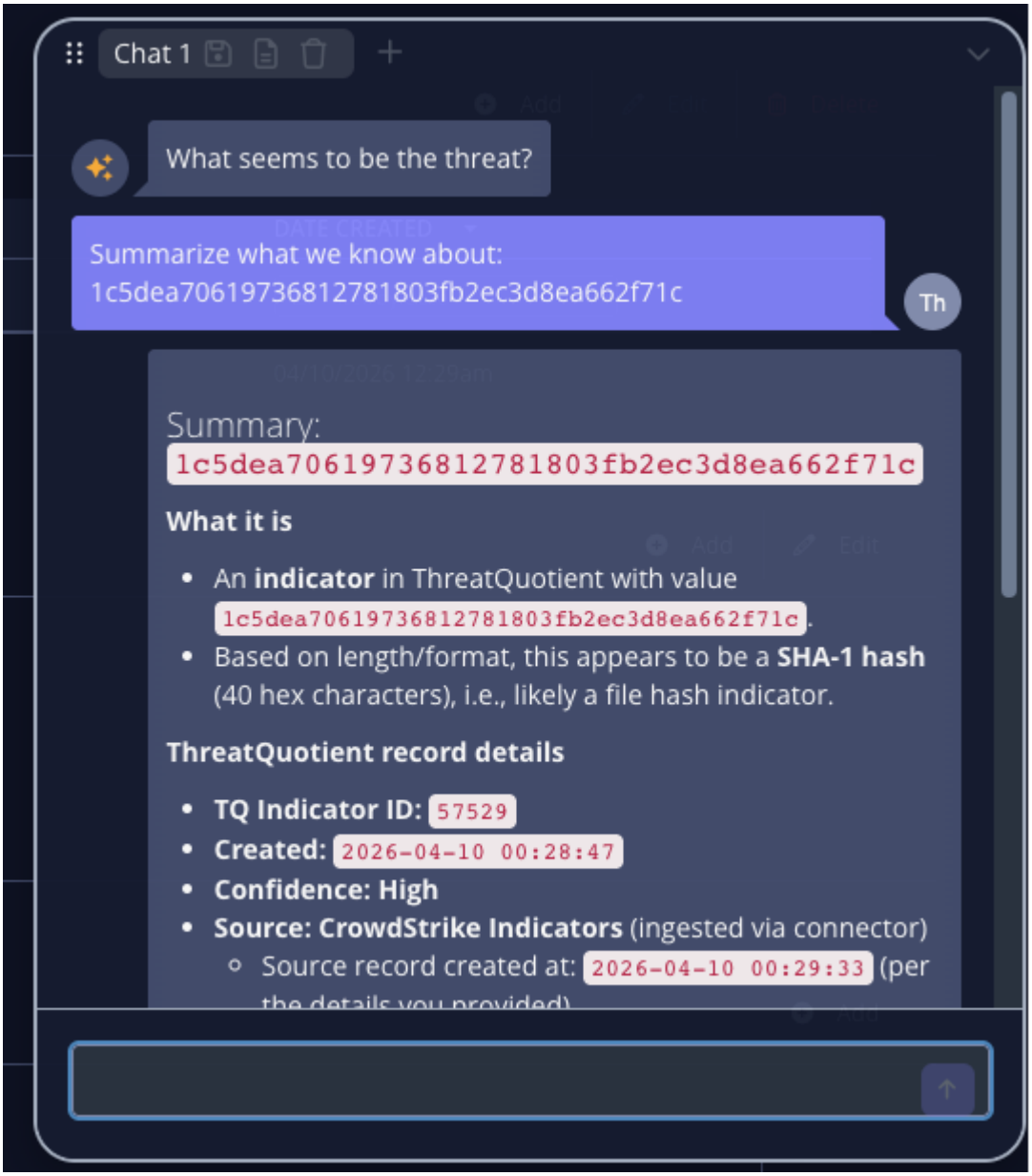
Threat Research Agent

About the Threat Research Agent

The Threat Research Agent is an AI-powered capability within the ThreatQ platform that enhances how you interact with and analyze threat intelligence. By combining natural language processing with ThreatQ's data and operations, the agent enables you to quickly query information, generate insights, and perform enrichment tasks without relying on manual workflows.

Built on a dual-service architecture, the agent integrates a customer-supplied large language model (LLM) with ThreatQ's operational framework to deliver intelligent, context-aware responses. Customers must provide and configure an LLM from one of the supported providers: OpenAI, Anthropic, Google Gemini, or Ollama. The agent then leverages this model to interpret user intent, retrieve relevant data from the Threat Library, and utilize configured operations as tools to automate analysis and enrichment.

The Threat Research Agent is designed to operate securely within your environment, inheriting user roles and permissions while ensuring that data is only shared with the configured LLM after the feature is explicitly enabled. This provides organizations with a controlled and flexible way to incorporate AI-driven capabilities into their threat intelligence processes while maintaining full control over their AI provider and configuration.


Chat 1
What seems to be the threat?
Summarize what we know about:
1c5dea70619736812781803fb2ec3d8ea662f71c
Th
Summary:
1c5dea70619736812781803fb2ec3d8ea662f71c
What it is
An indicator in ThreatQuotient with value 1c5dea70619736812781803fb2ec3d8ea662f71c.
Based on length/format, this appears to be a SHA-1 hash (40 hex characters), i.e., likely a file hash indicator.
ThreatQuotient record details
TQ Indicator ID: 57529
Created: 2026-04-10 00:28:47
Confidence: High
Source: CrowdStrike Indicators (ingested via connector)
Source record created at: 2026-04-10 00:29:33 (per

Requirements

The following is required in order to configure, enable, and use the Threat Research Agent.

- ThreatQ version 6.18.0 or later.
- A Threat Research Agent license - contact ThreatQ Sales or your Technical Account Manager (TAM) for more details.
- The Threat Research Agent's Framework components services enabled:

  > ThreatQuotient will perform this task for ThreatQ hosted customer instances.

  - **ThreatQ versions >= 6.21.0** - on-premise customers will need to enable the mcp and agent services by running TQAdmin and entering **yes** to the the enable `mpc` and `agent` services prompts.
  - **ThreatQ versions <=6.20.1** - on-premise customers will need to enable the `mcp` and `agent` services in their **threatq.tfvars** file after applying the Threat Research Agent license to their ThreatQ instance using the steps below.

    1. Open the **threatq.tfvars** file located at: `/opt/threatq/threatq.tfvars`.
    2. Set the `enable_mcp` and `enable_agent` entries to `true`. The file should resemble:

       ```
       enable_mcp = true
       enable_agent = true
       ```

    3. Save the file and run TQAdmin to apply the changes to your ThreatQ instance.
- A tool-capable model from one of the following LLM providers listed below. The LLM provider token will be system-wide and can be utilized by all users with the appropriate roles/permissions.
  - OpenAI
  - Anthropic
  - Google Gemini
  - Ollama
  - LiteLLM

    > The quality of results will depend on the selected LLM model.

- The appropriate ThreatQ roles/permissions needed to access the agent and its tools. The agent will inherit the role/permissions of the user using it. For example, if you have an Administer role, the agent will have those permissions during that session.
  - Configuring and Enabling the Agent
    - Default Roles Required: Maintenance or Administrator
    - Custom Role: Administrative Functions - Edit System Configurations
  - Using the Agent
    - Default Roles Required: Maintenance, Administrator, or Primary Contributor
    - Custom Role: Agentic Assistance - Access MCP Server and Use Agentic Chat
  - Running Tools to Enrich Data
    - Default Roles Required: Maintenance, Administrator, or Primary Contributor
    - Custom Role: Integrations - Run Operations and Edit Integration Configurations

> Read Only roles will only have access to the MCP service. This will allow them to query data within ThreatQ but they will not have access to the Agent Service that uses the LLM models.

Services

The Threat Research Agent framework in ThreatQ enables AI-driven agentic workflows by connecting large language models (LLMs) with platform capabilities. It is composed of two primary services, the MCP Service and the Agent Service, which work together to provide intelligent automation, enrichment, and analysis.

MCP Service (/api/mcp)

The MCP Service serves as the execution layer and functions as the tool provider for the agent. It exposes ThreatQ operations and capabilities as structured, callable tools that the agent can invoke. Acting as a bridge between the Agent Service and the ThreatQ platform, it enables access to Threat Library queries as well as configured operations.

This service does not interact with a large language model (LLM). Instead, it is responsible for executing requests in a controlled and deterministic manner, ensuring consistent and secure interaction with ThreatQ functionality.

Agent Service (/api/agent)

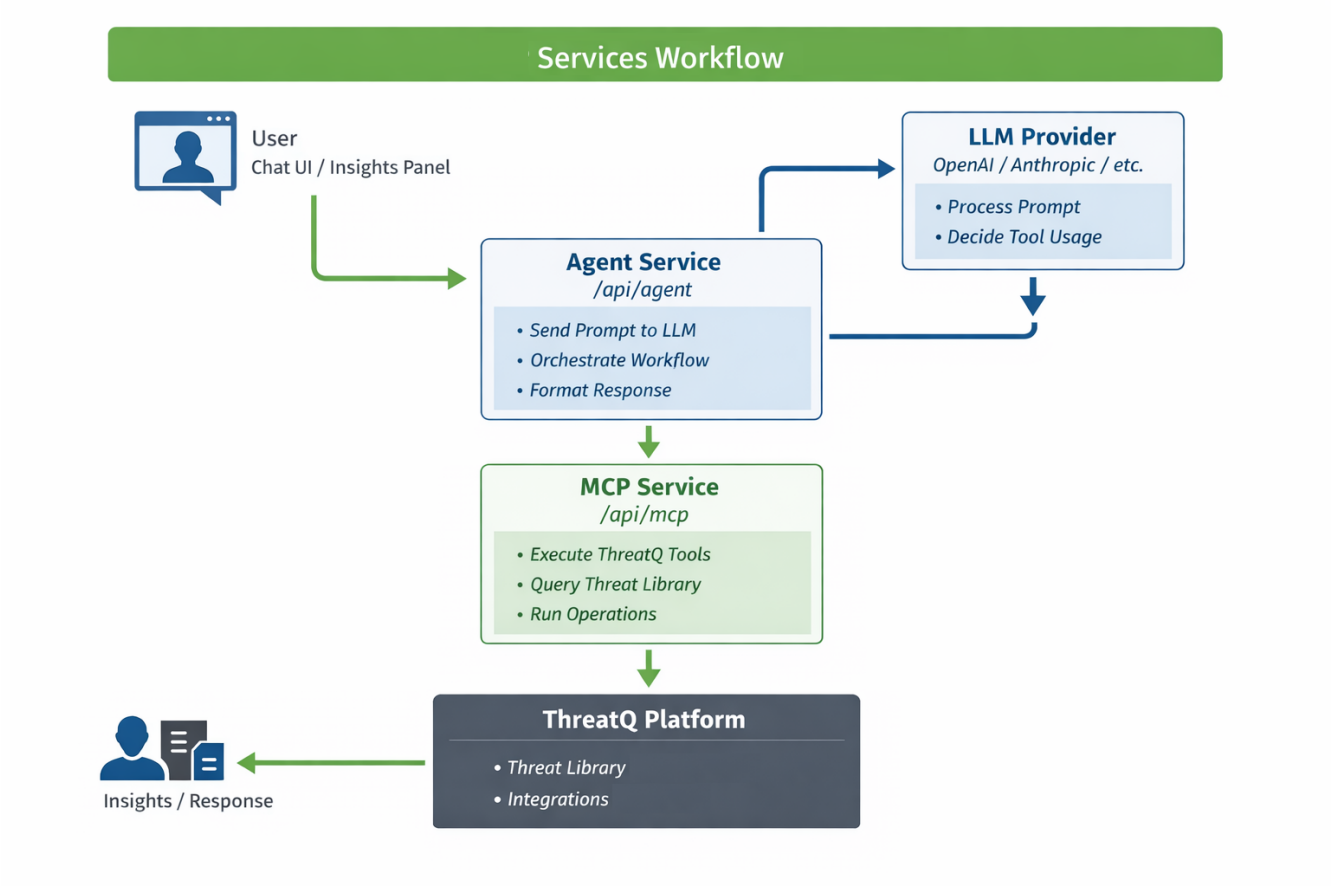
The Agent Service interfaces with a configured LLM provider such as OpenAI, Anthropic, Gemini, or Ollama. It serves as the reasoning engine that processes natural language input, determines appropriate actions, and orchestrates the use of MCP tools to execute tasks within the ThreatQ platform.

Powered by an LLM, the Agent Service interprets user intent, decides when and how to invoke available tools, and can autonomously execute multi-step workflows. It then returns structured, human-readable insights and results.

How the Services Work Together

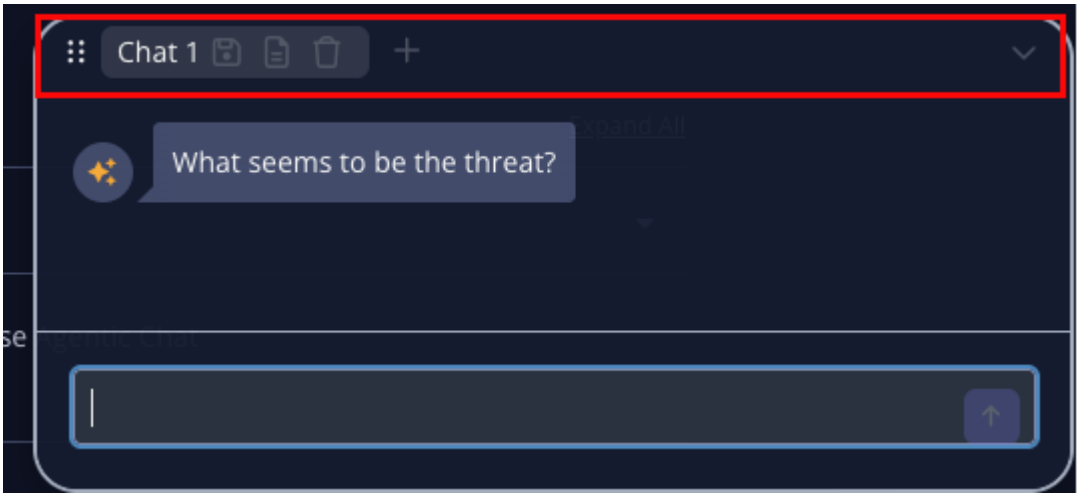
A typical workflow looks like this:

- User submits a prompt via the Agent UI (chat or operation)
- Agent Service sends the prompt to the LLM
- LLM determines that a tool/action is needed
- Agent calls the MCP Service with the appropriate tool
- MCP Service executes the tool in ThreatQ
- Results are returned to the Agent
- Agent formats and presents the final response to the user


Services Workflow
User
Chat UI / Insights Panel
LLM Provider
OpenAI / Anthropic / etc.
• Process Prompt
• Decide Tool Usage
Agent Service
/api/agent
• Send Prompt to LLM
• Orchestrate Workflow
• Format Response
MCP Service
/api/mcp
• Execute ThreatQ Tools
• Query Threat Library
• Run Operations
ThreatQ Platform
• Threat Library
• Integrations
Insights / Response

Agent Toolbar

The Agent Toolbar provides quick access to key functions that enhance how users interact with the Threat Research Agent. It enables users to manage chat sessions, generate and download reports, organize multiple conversations, and control the agent interface. This section outlines each toolbar option and its functionality, helping users efficiently navigate and utilize the agent during their workflow.



ICON	FUNCTION	DESCRIPTION
	Move Agent Widget	Click on the move icon to move the agent on your screen. The agent will automatically snap to the closest corner.
	Download Chat	This function downloads the chat to your local machine in markdown format.
	Generate Report	This function leverages ThreatQ to generate a PDF report of the chat conversation. See the Generating Chat Reports topic for details.
	Delete/Clear Report	The function of this button will differ based on the number of chat tabs opened. If there is only one chat tab, the button will clear the chat. If there are more than one chat tabs, the button will close the current tab open.

ICON	FUNCTION	DESCRIPTION
		The agent does not save chat history at the end of a session or when closing a chat tab.
	Open New Chat Tab	This button opens a new chat tab within the agent. You can have up to five different chat tabs open at one time.
	Minimize Agent Window	This button will minimize the agent.

Enable and Configure Agent

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative or Maintenance
Custom Role - Action Permissions: Administrative Functions - Edit System Configurations

This topic provides step-by-step instructions for configuring and enabling the Threat Research Agent within the ThreatQ platform. This guide walks you through selecting an LLM provider, defining required settings, and activating the agent, as well as enabling ThreatQ operations as tools so the agent can effectively query, enrich, and analyze data within your environment.

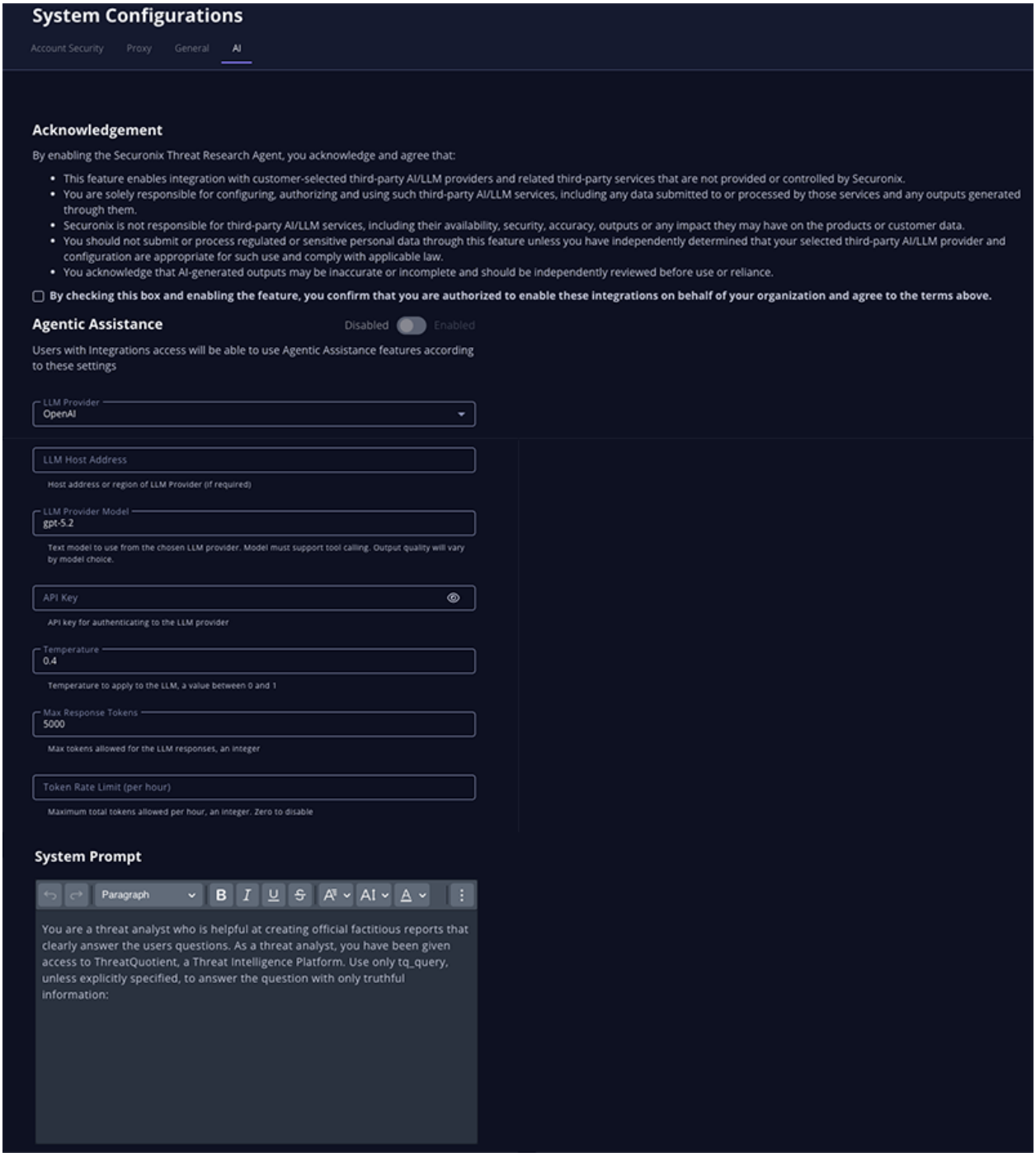
By default, no data is shared with any LLM provider; data is only transmitted after the agent is properly configured and enabled.

Configuring and Enabling the Agent

1. Click on the Settings gear icon and select **System Configurations**.

   The System Configurations page will load.

2. Click on **AI** tab to open the AI configuration page.

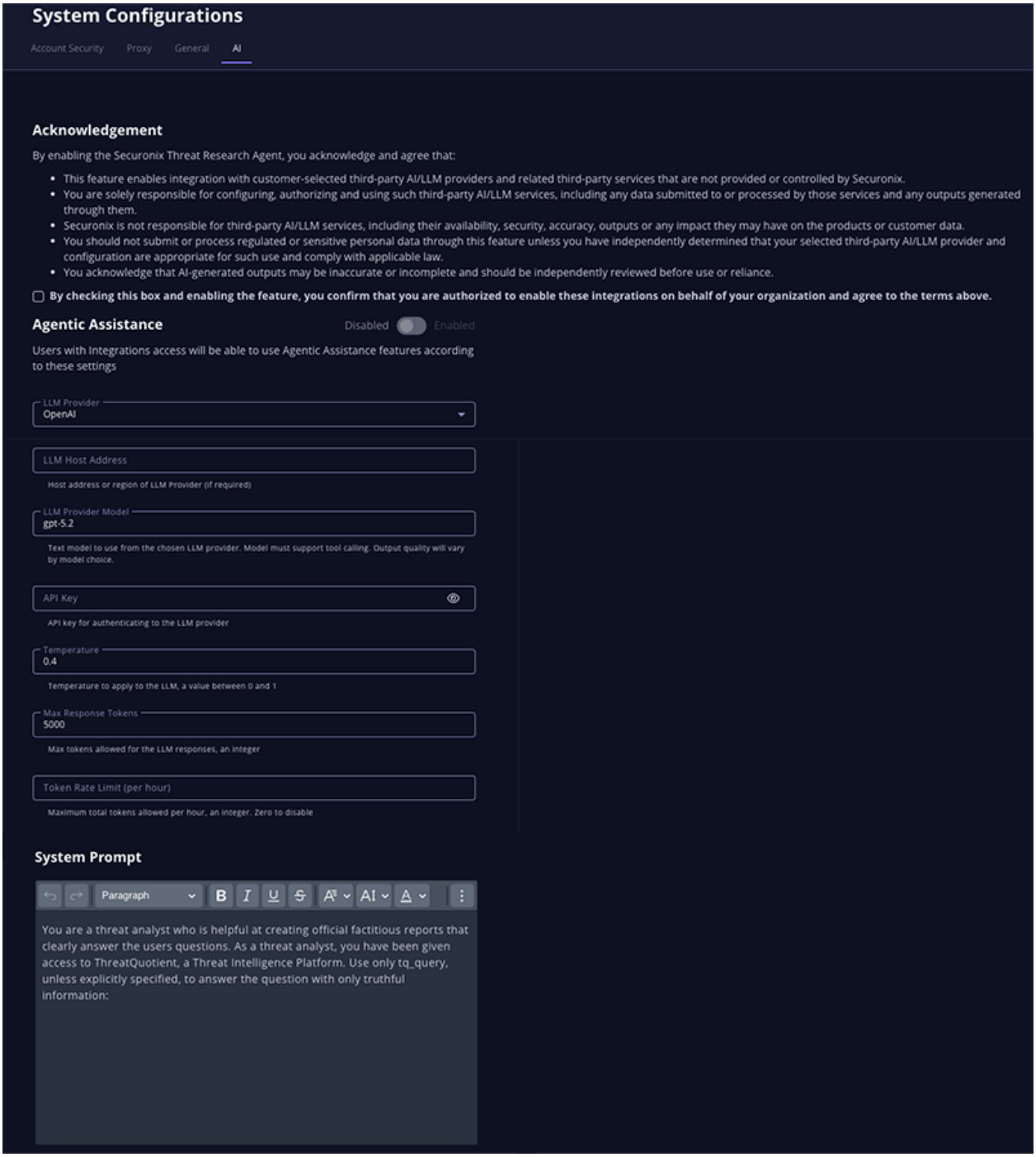


3. Review and accept the **Artificial Intelligence Terms and Conditions**.
4. Complete the following parameters:

PARAMETER	DESCRIPTION
LLM Provider	Select your LLM Provider. Options include:

PARAMETER	DESCRIPTION
	• OpenAI • Anthropic • Gemini • Ollama • LiteLLM
LLM Host	Enter the LLM host address if required by the LLM provider. Only Ollama requires this parameter at the time of this publication.
LLM Provider Model	Enter the model to use for the selected provider. An example for OpenAI would be `gpt-5.2`. The selected model must support tool-calling and the quality of the output will depend on the capabilities of the chosen model.
API Key	Enter the API Key for the LLM provider. The API key is configured at the system level and is shared across all users.
Temperature	Enter a temperature setting, between 0 and 1, to set the randomness, creativity, and predictability of text generated. Lower values will produce more consistent and deterministic responses while higher values generate more varied and creative results. The ThreatQuotient team recommends starting with `.4` and adjusting based on your requirements.

PARAMETER	DESCRIPTION
Max Response Tokens	Enter the max number of tokens the LLM can use in its responses.
Token Rate Limit (per hour)	Enter the maximum total tokens that can be used per hour. Enter 0 to disable the rate limit.
System Prompt	This parameter contains the instructions to the agent on how to operate. A recommended prompt is already populated in the parameter by default. You can edit this prompt as needed by your organization. `You are a threat analyst who is helpful at creating official factitious reports that clearly answer the users questions. As a threat analyst, you have been given access to ThreatQuotient, a Threat Intelligence Platform. Use only tq_query, unless explicitly specified, to answer the question as best you can.`

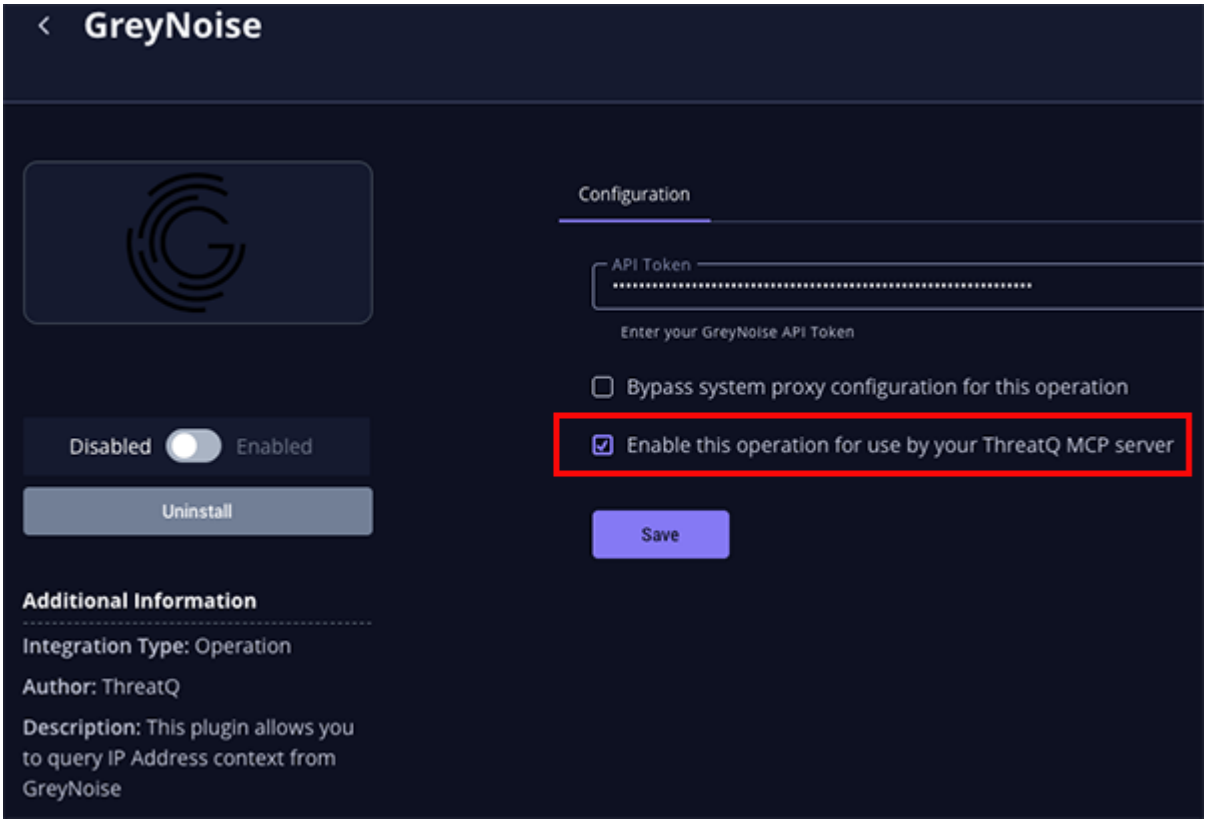


5. Click on the **Save** button and then click on the **Enable** toggle switch to enable the Threat Research Agent.
6. The agent will now be enabled and connected to your selected LLM. Proceed with enabling tools for the agent to utilize.

Enabling Tools

The Threat Research Agent uses ThreatQ operations as tools to enrich and curate data. The agent analyzes the selected object and autonomously determines the appropriate tool to use when additional information or enrichment is requested. The operation must be fully configured (API keys, settings etc.) and enabled in ThreatQ.

1. Click on the **Integrations** menu heading and select **Operations**.
2. Click on the tile card for the operation to be included as an agent tool to load its details page.
3. Check the **Enable this operation for use by your ThreatQ MCP server** configuration option.



4. The operation will now be accessible as a tool by the agent.

Using the Agent

THREATQ REQUIRED PERMISSIONS

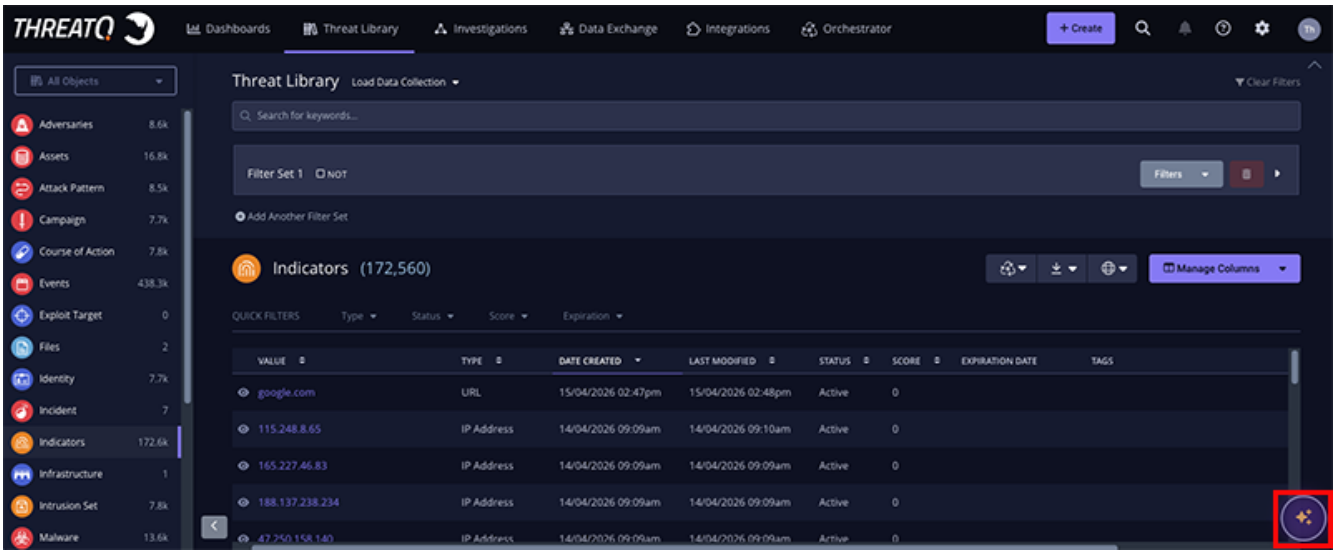
Default ThreatQ Role: Administrative, Maintenance, or Primary Contributor.
Custom Role - Action Permissions: Agentic Assistance - Access MCP Server and Use Agentic Chat

The Threat Research Agent enables you to interact with your ThreatQ data using natural language, allowing you to quickly query threat intelligence, retrieve object details, and enrich information using integrated tools. The agent leverages both your Threat Library and configured ThreatQ operations to provide contextual insights and actionable results.

You can launch the Threat Research Agent from two locations within the ThreatQ platform.

Agent Bubble

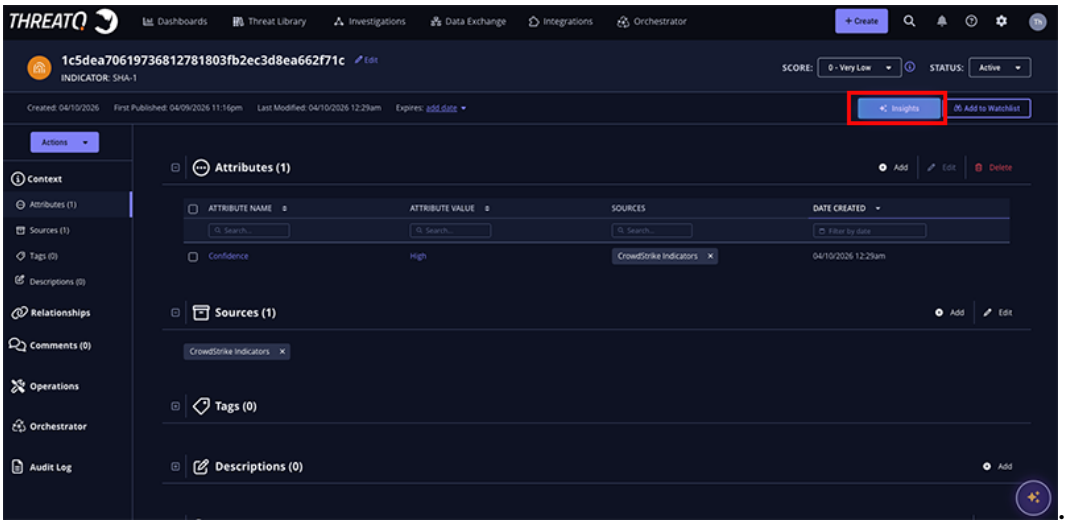
Select the Agent icon located in the lower-right corner of the ThreatQ interface to open the chat window and begin a new conversation. This entry point is intended for general research, ad hoc questions, and investigations that are not tied to a specific ThreatQ object.

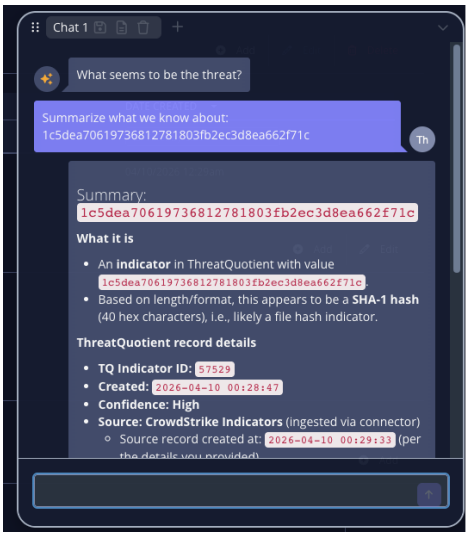


Insights Button

The Insights button is available on an object's details page and provides contextual access to the Threat Research Agent. When launched from an object, the agent automatically receives the selected object as context, allowing it to generate responses

that are specific to the object being analyzed.





ThreatQ v6.20.0 and Later

Beginning with ThreatQ v6.20.0, the **Insights** button provides two analysis options.

- **Quick** – Generates an AI-powered summary of the selected object and displays the results directly in the chat.
- **Full** – Opens the Report Generation interface to create a comprehensive AI-generated report for the selected object.

Working with the Agent

After you submit a prompt, the Threat Research Agent analyzes the request and returns a contextual response. The agent may also suggest follow-up prompts to help you continue your investigation, explore related intelligence, or gather additional information without needing to reformulate your query.

The quality and relevance of responses are enhanced by the context available to the agent, including ThreatQ objects, relationships, and intelligence stored within your Threat Library.

Using ThreatQ Operations as Agent Tools

The Threat Research Agent can invoke configured ThreatQ Operations as AI tools to enrich objects, retrieve external intelligence, and perform investigative actions during a conversation. These tools allow the agent to extend its analysis beyond the information currently stored in your Threat Library.

To be available to the agent, Operations must be properly configured, authenticated, and enabled within the ThreatQ platform.

Unlike manually executed Operations, the Threat Research Agent can use these tools against both:

- Existing ThreatQ objects stored in the Threat Library.
- External indicators or intelligence that have not yet been ingested into ThreatQ.

This capability enables analysts to perform contextual enrichment and research on demand, reducing manual effort while expanding the scope of available intelligence during an investigation.

Generating Chat Reports

You can quickly turn Agent conversations into structured ThreatQ reports by selecting the most relevant chat interactions. This allows you to compile key insights, customize report details, and generate polished, shareable reports directly within the platform.

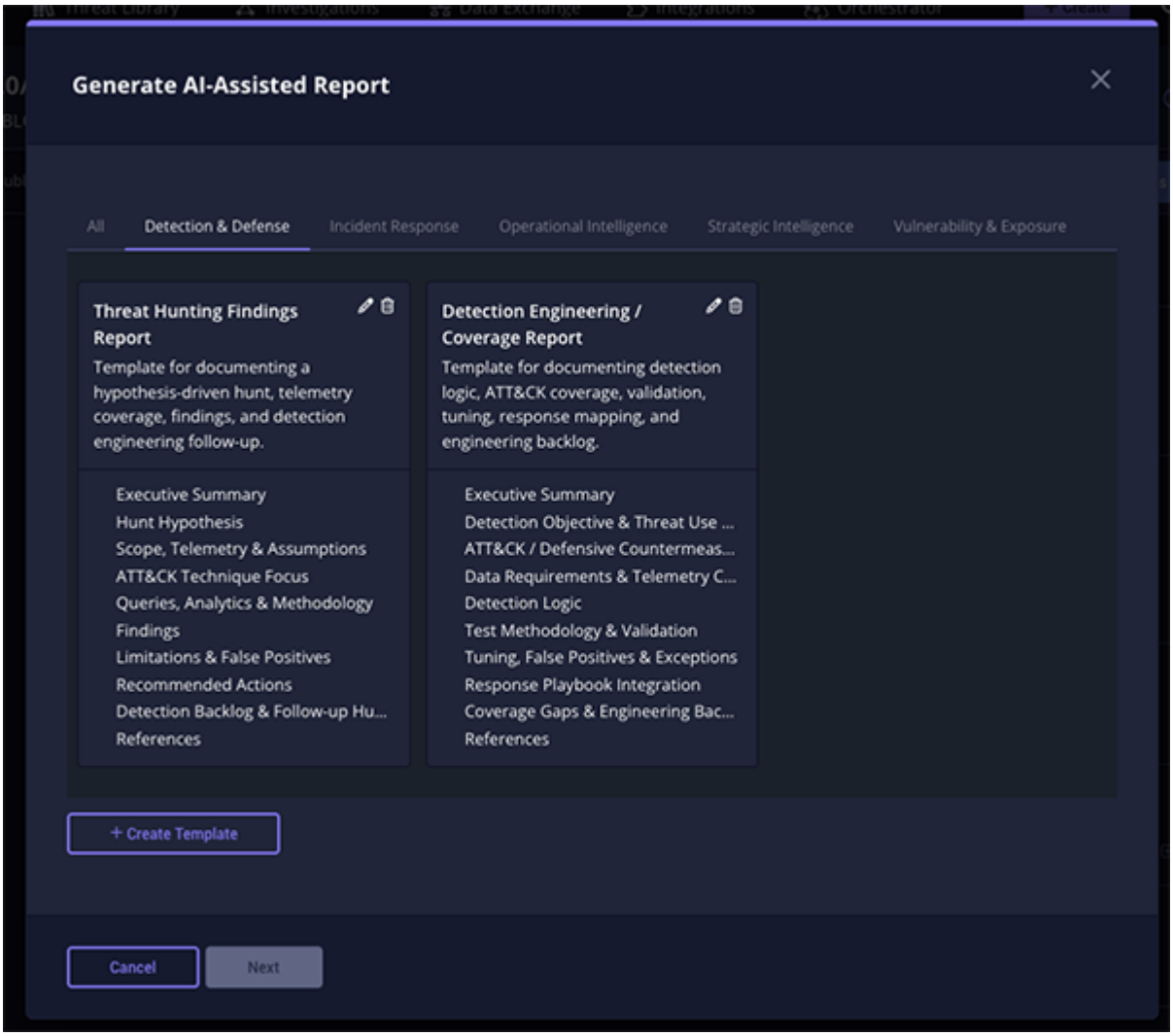
> ThreatQ version 6.20.0 introduced report templates for agent chat reports. Steps to generate will differ based on which ThreatQ version you are currently on.

Generate Report (ThreatQ 6.20.0 and later)

You can begin the report process from either an object's details page or from the chat agent.

1. Perform one of the following:
    - From an object's details page - hover your mouse over the Insights button and select **Full**.
    - From the agent chat modal - click on the checkboxes to include those conversation segments in the report. Next, click on the report icon on the agent toolbar and then click on **Generate** in the lower-left corner of the chat window.

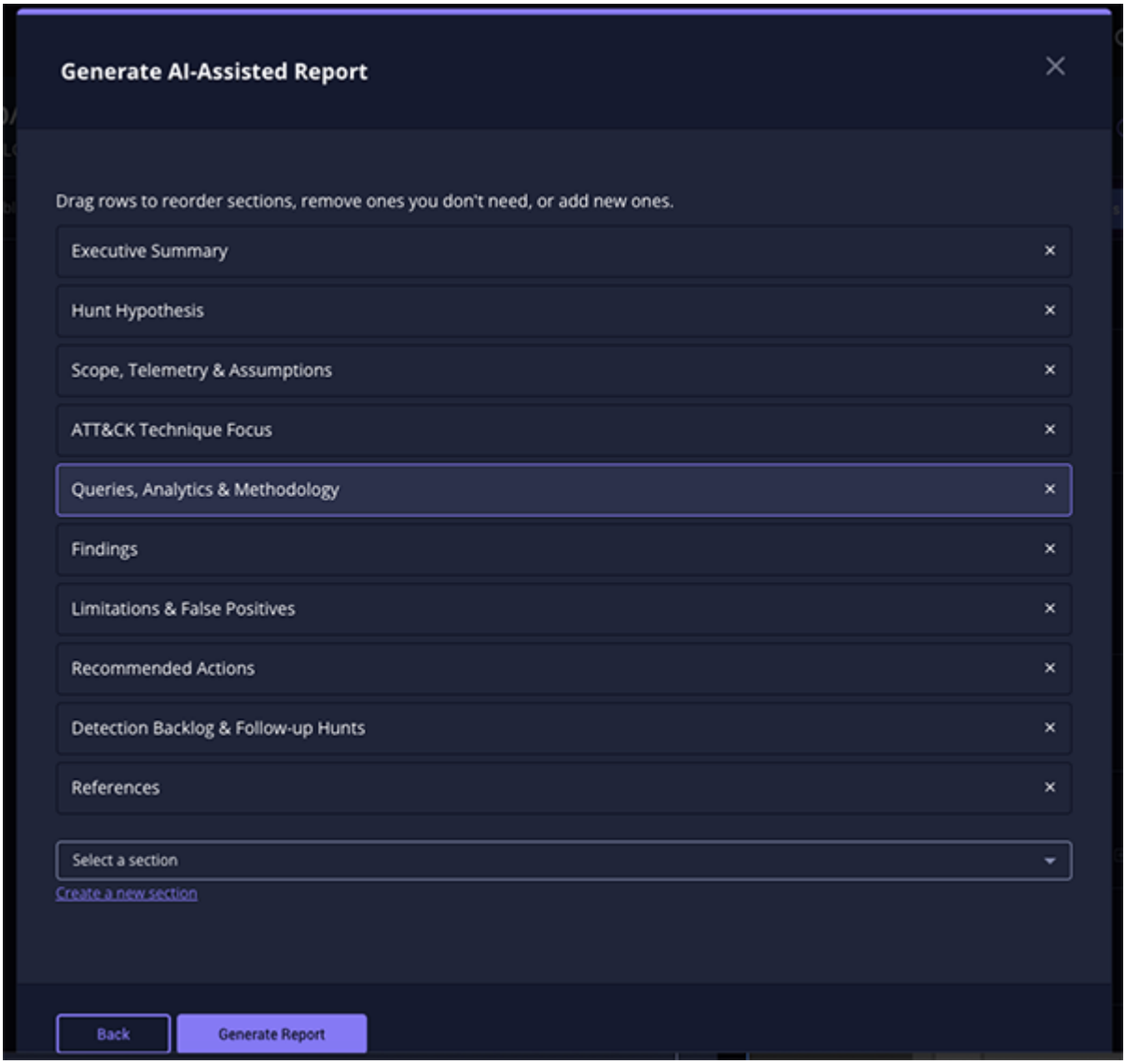
The Generate AI-Assisted Report modal will load.



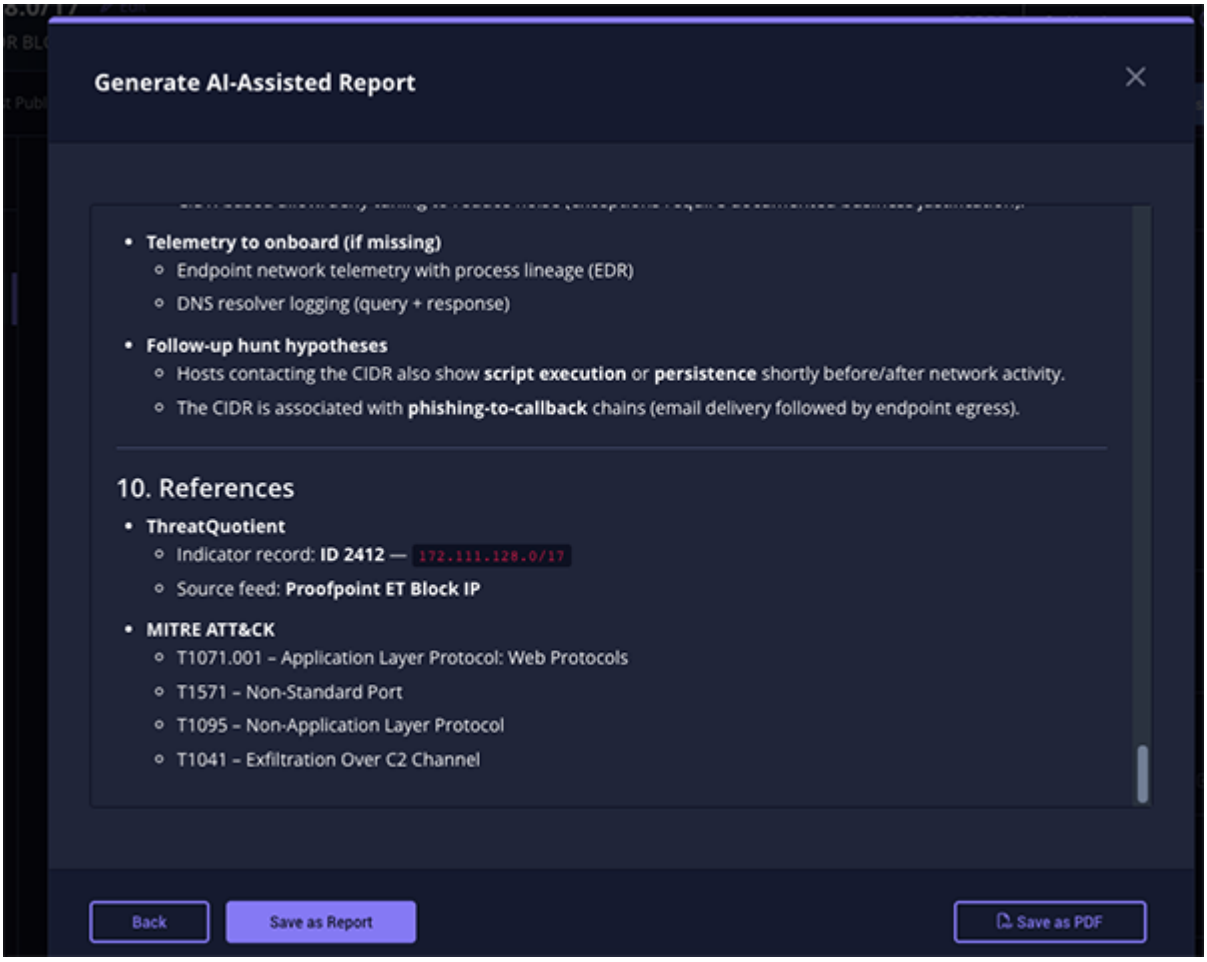
2. Select a saved report template and click **Next**.

   You can also or create your own report template.

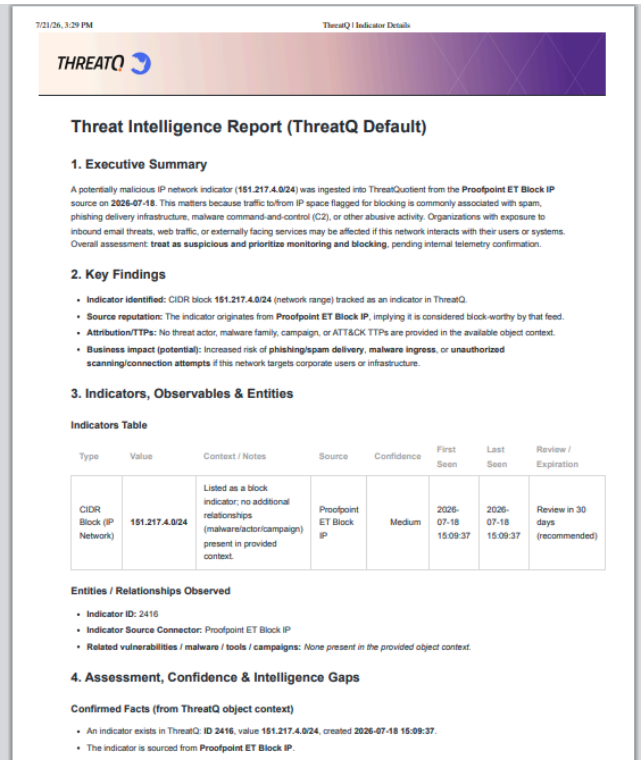
3. Drag and drop report sections to change their order, remove sections that are not needed, or add additional sections to customize the report layout. It is important to note that these sections come from the template you selected. Click on **Generate Report** to proceed.



4. The agent will generate a report in the modal using the sections you have selected and display it for review.



5. Decide how to save the report after you have finishing reviewing it. You can either save it as a report object in ThreatQ or save it as a PDF.



7/21/26, 3:29 PM ThreatQ | Indicator Details

THREATQ

Threat Intelligence Report (ThreatQ Default)

1. Executive Summary

A potentially malicious IP network indicator (**151.217.4.0/24**) was ingested into ThreatQuotient from the **Proofpoint ET Block IP** source on **2026-07-18**. This matters because traffic to/from IP space flagged for blocking is commonly associated with spam, phishing delivery infrastructure, malware command-and-control (C2), or other abusive activity. Organizations with exposure to inbound email threats, web traffic, or externally facing services may be affected if this network interacts with their users or systems. Overall assessment: **treat as suspicious and prioritize monitoring and blocking**, pending internal telemetry confirmation.

2. Key Findings

- **Indicator identified:** CIDR block **151.217.4.0/24** (network range) tracked as an indicator in ThreatQ.
- **Source reputation:** The indicator originates from **Proofpoint ET Block IP**, implying it is considered block-worthy by that feed.
- **Attribution/TTPs:** No threat actor, malware family, campaign, or ATT&CK TTPs are provided in the available object context.
- **Business impact (potential):** Increased risk of **phishing/spam delivery**, **malware ingress**, or **unauthorized scanning/connection attempts** if this network targets corporate users or infrastructure.

3. Indicators, Observables & Entities

Indicators Table

Type	Value	Context / Notes	Source	Confidence	First Seen	Last Seen	Review / Expiration
CIDR Block (IP Network)	**151.217.4.0/24**	Listed as a block indicator; no additional relationships (malware/actor/campaign) present in provided context.	Proofpoint ET Block IP	Medium	2026-07-18 15:09:37	2026-07-18 15:09:37	Review in 30 days (recommended)

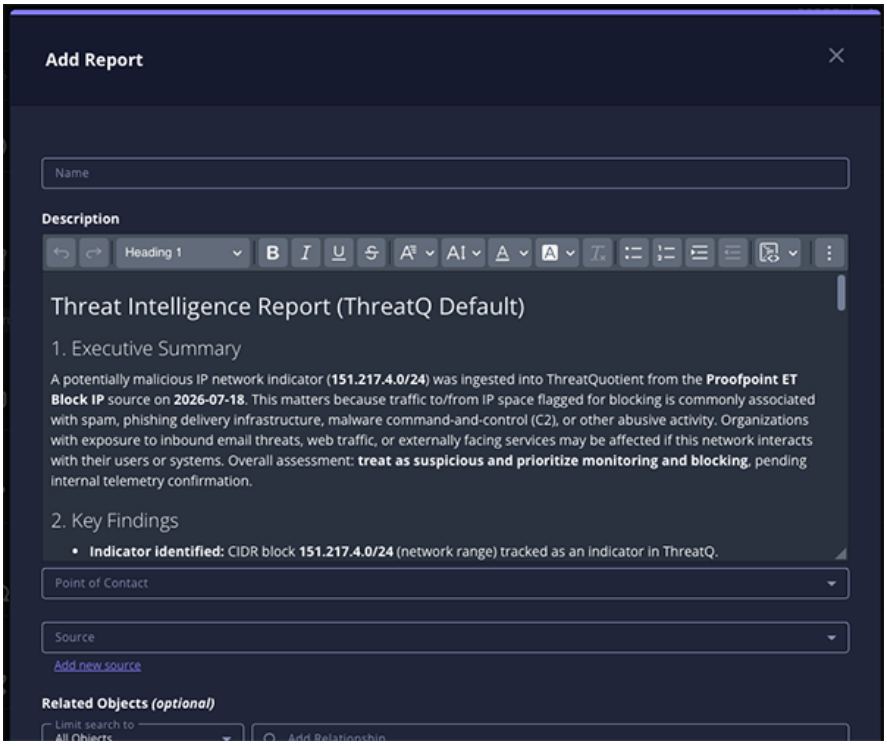
Entities / Relationships Observed

- **Indicator ID:** 2416
- **Indicator Source Connector:** Proofpoint ET Block IP
- **Related vulnerabilities / malware / tools / campaigns:** *None present in the provided object context.*

4. Assessment, Confidence & Intelligence Gaps

Confirmed Facts (from ThreatQ object context)

- An indicator exists in ThreatQ: **ID 2416**, value **151.217.4.0/24**, created **2026-07-18 15:09:37**.
- The indicator is sourced from **Proofpoint ET Block IP**.

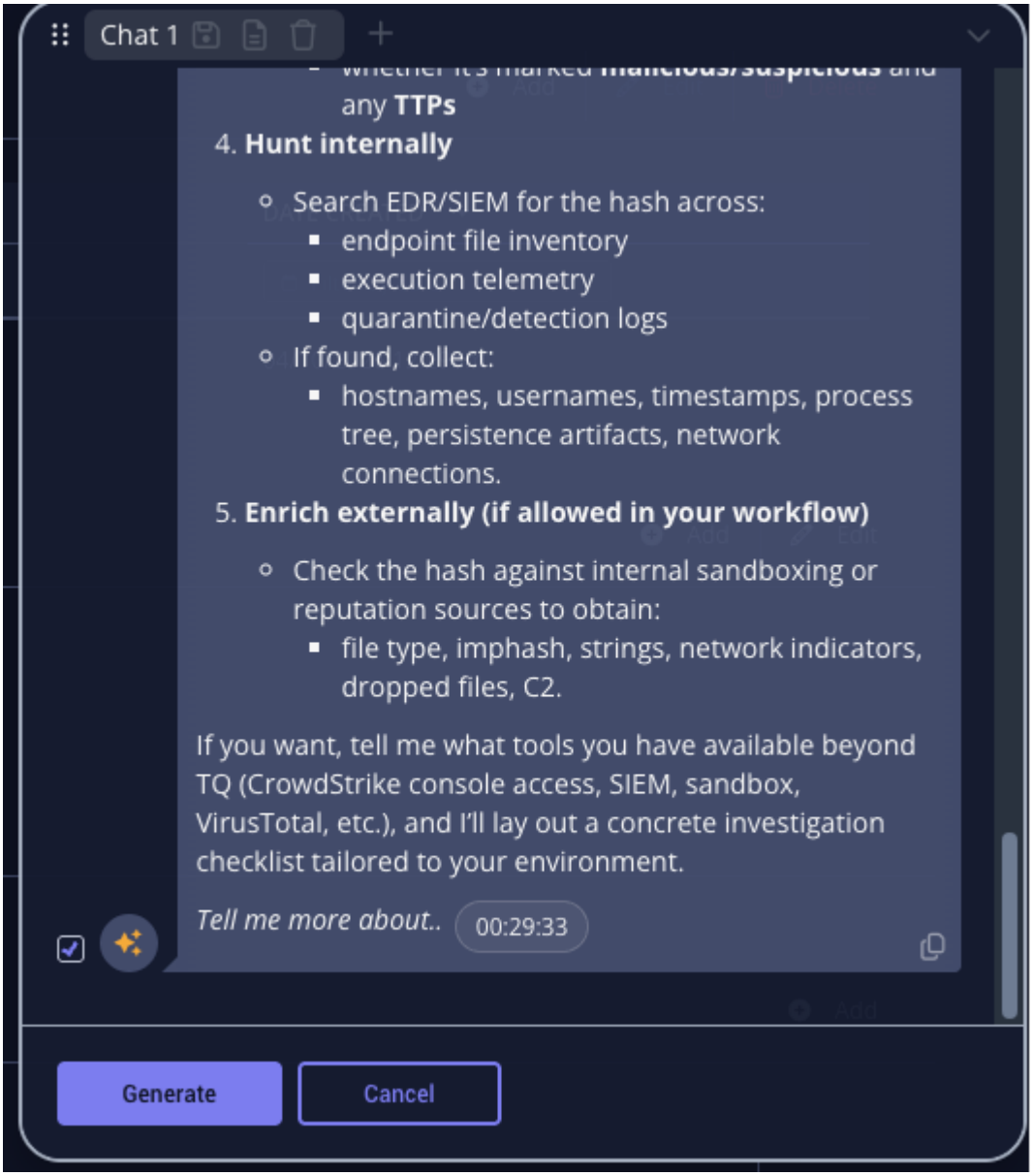


Saving the report to PDF will utilize your PDF settings set under the Report Options page. See the Reports Options section in the topic for more information about PDF styling.

Generate Report (ThreatQ 6.19.1 and earlier)

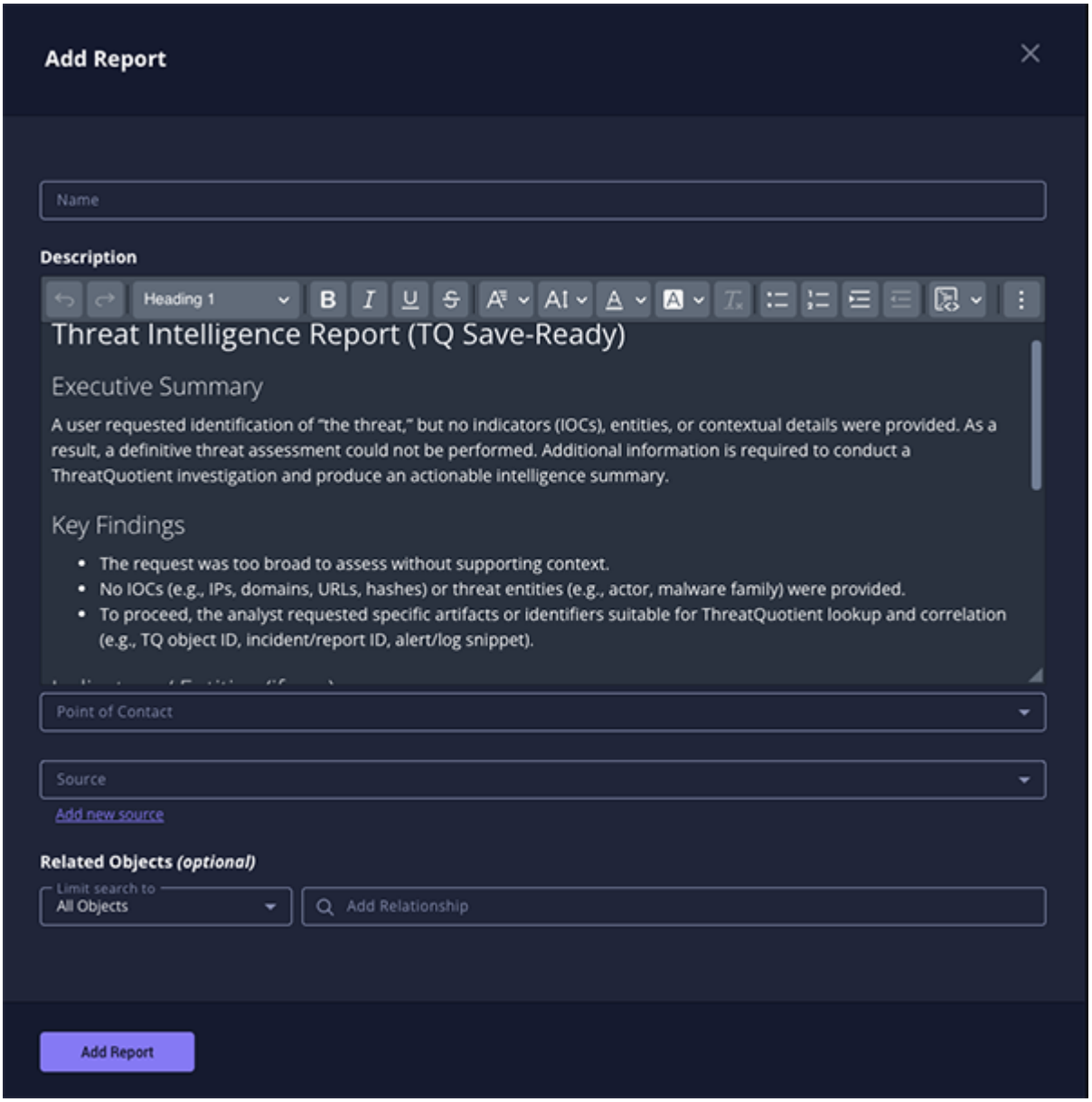
From the Agent chat window:

1. Click on the **Generate Report** button on the agent toolbar.
2. Checkboxes will load next to each interaction of your conversation.



3. Click on the checkboxes to include those conversation segments in the report.
4. Click on the **Generate** button.

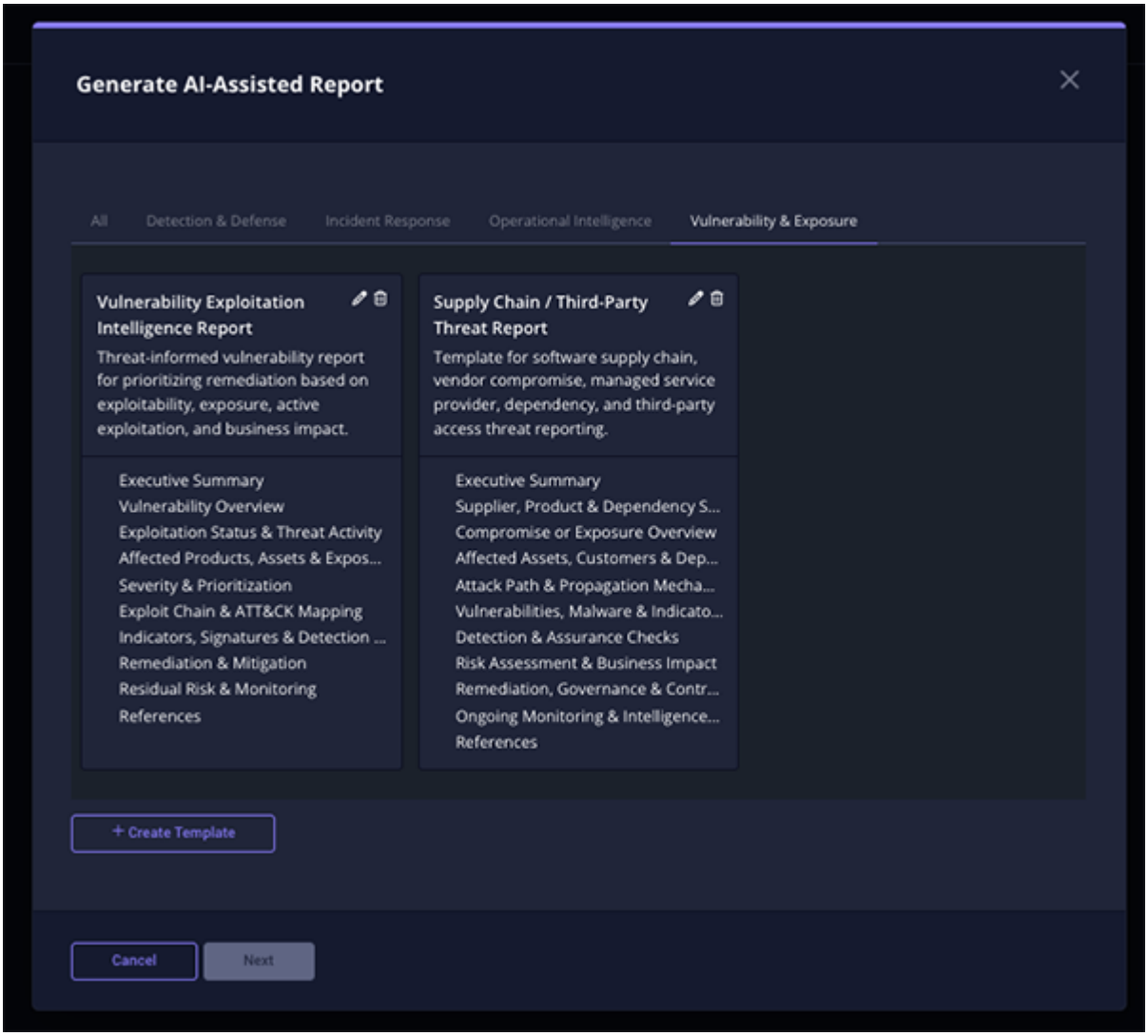
   The Add Report dialog box will load with the selected conversation segments loaded in the Description field.



5. Enter a name for the report and add any additional required information.
6. Click on **Add Report** to finish generating the report.

AI-Assisted Report Templates

Introduced in ThreatQ v6.20.0, AI-Assisted Report Templates enable you to create standardized, reusable report structures for the Threat Research Agent. Templates define the sections and prompts that guide the AI when generating reports, helping ensure reports are consistent, comprehensive, and tailored to your organization's reporting requirements.



Report templates are organized into user-defined categories, making it easy to manage templates for different use cases, such as malware analysis, threat actor profiles, vulnerability assessments, or executive summaries. Users can create, organize, and delete categories as needed.

When generating a report, select a report template as the starting point. Before submitting the report for generation, you can customize the template by adding new sections, removing sections that are not needed, or rearranging the order of existing

sections. This flexibility allows you to adapt reusable templates to meet the requirements of a specific investigation while maintaining a consistent reporting framework.

After the report is generated, you can review the AI-generated content and choose one of the following actions:

- **Create a ThreatQ Report** to save the report as a Report object within the Threat Library.
- **Export as PDF** to generate a portable document that can be shared outside the ThreatQ platform.

By providing reusable report structures and allowing last-minute customization, Chat Report Templates help standardize AI-assisted reporting, reduce the time required to produce detailed intelligence reports, and enable analysts to consistently generate high-quality documentation across investigations.

Default Categories and Reports

The following report template categories and templates are included with the ThreatQ platform by default. You can modify or delete seeded report templates to meet your organization's requirements. You can remove a category by deleting all the reports within it.

The **ThreatQ Default** report template cannot be deleted.

Deleting any other category or report template is permanent and cannot be undone. If a seeded category or report template is deleted, it must be recreated manually.

CATEGORY	REPORT	DESCRIPTION
Detection & Defense	Threat Hunting Findings Report	Template for documenting a hypothesis-driven hunt, telemetry coverage, findings, and detection engineering follow-up.
Detection & Defense	Detection Engineering/ Coverage Report	Template for documenting detection logic, ATT&CK coverage, validation, tuning, response mapping, and engineering backlog.
Incident Response	Ransomware Incident / Campaign Report	Template for ransomware intrusions, extortion campaigns, and ransomware readiness findings.

CATEGORY	REPORT	DESCRIPTION
Incident Response	Cloud & Identity Threat Report	Template for cloud control plane, SaaS, identity provider, and credential-centric threat analysis.
Operational Intelligence	ThreatQ Default	Standard threat intelligence summary used by ThreatQ agentic assistance. Optimized for mixed executive and analyst audiences.
Operational Intelligence	MITRE ATT&CK Campaign Report	Structured analysis of a threat campaign mapped to MITRE ATT&CK, with explicit evidence, versioning, confidence, and defensive recommendations.
Operational Intelligence	MITRE ATT&CK Incident Report	Post-incident report documenting an intrusion through the MITRE ATT&CK lens and incident response lifecycle.
Operational Intelligence	MITRE CTI Threat Actor Profile	Deep-dive profile of a threat actor or intrusion set using CTI conventions, ATT&CK mapping, and explicit confidence language.
Operational Intelligence	Malware Analysis Report	Static and dynamic malware analysis template connecting sample behavior, capabilities, indicators, ATT&CK techniques, and defensive actions.
Operational Intelligence	Phishing / BEC Campaign Report	Template for analyzing phishing, business email compromise, credential theft, and email-borne malware campaigns.
Operational Intelligence	Tactical IOC Enrichment Report	Fast-turn report for validating, enriching, contextualizing, and operationalizing indicators and observables.

CATEGORY	REPORT	DESCRIPTION
Strategic Intelligence	Strategic Sector Threat Landscape Report	Executive and board-oriented threat landscape report for a sector, geography, technology stack, or business line.
Vulnerability & Exposure	Vulnerability Exploitation Intelligence Report	Threat-informed vulnerability report for prioritizing remediation based on exploitability, exposure, active exploitation, and business impact.
Vulnerability & Exposure	Supply Chain / Third-Party Threat Report	Template for software supply chain, vendor compromise, managed service provider, dependency, and third-party access threat reporting.

Sections

Report Sections are the reusable building blocks that define the content of an AI-assisted report. Each section contains a prompt that instructs the Threat Research Agent what information to generate for a specific portion of the report, such as an executive summary, threat actor analysis, malware behavior, indicators of compromise, or recommended mitigations.

Unlike report templates, which define the overall structure of a report, sections define the individual content areas within that structure. Because sections are reusable, a section created once can be used across multiple report templates, ensuring consistent AI instructions while eliminating the need to recreate commonly used report content.

When a report is generated, the AI processes each section independently using its associated prompt and assembles the results into a complete report. Multiple sections can be combined in any order to create reports tailored to different use cases. If a section is updated, the changes are automatically reflected the next time it is used in any report template, allowing organizations to maintain standardized reporting practices while managing common content from a single location.

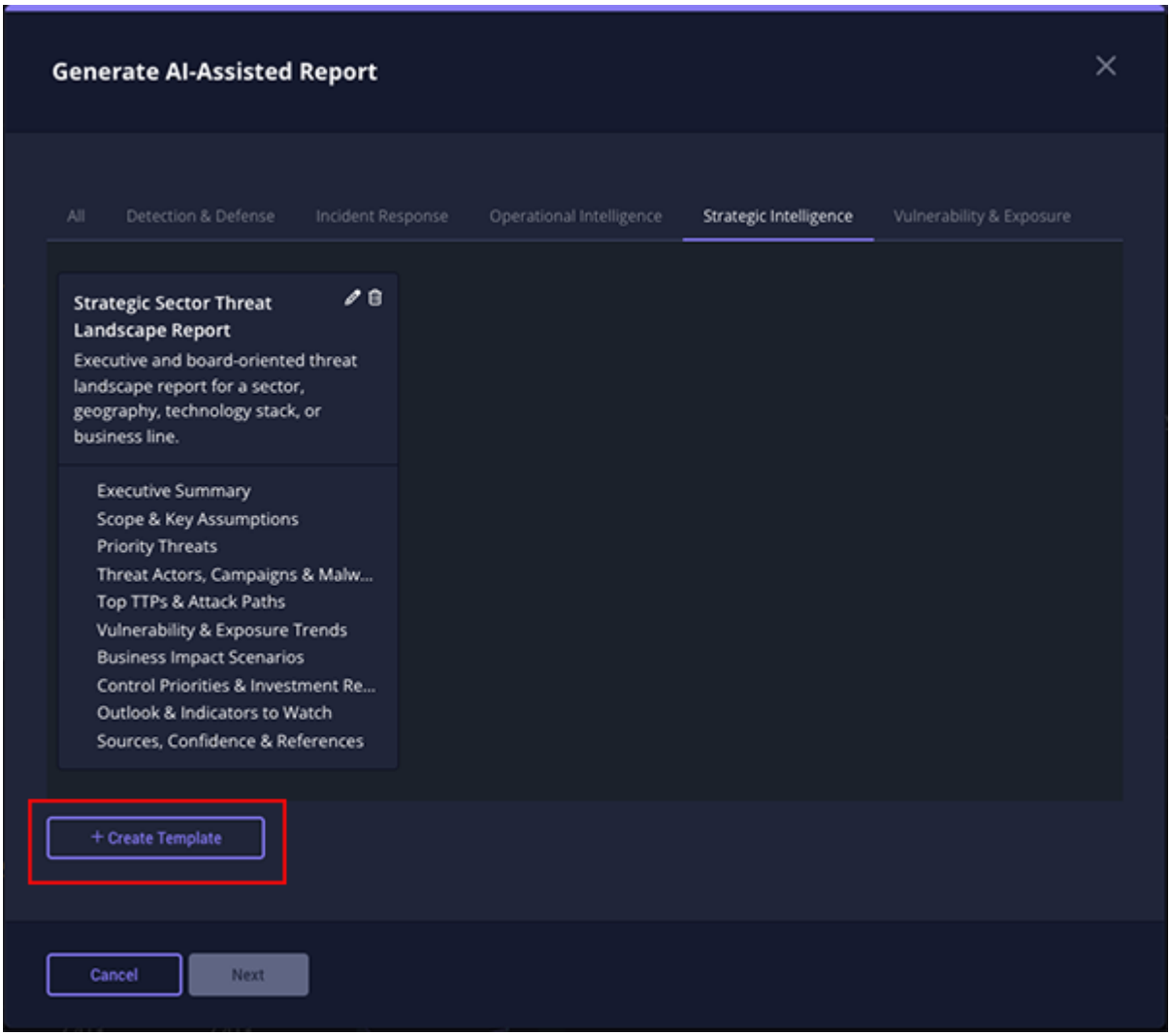
This modular approach enables organizations to standardize report content, maintain consistency across investigations, and quickly build new report templates from a library of reusable sections.

Creating a New Report Template

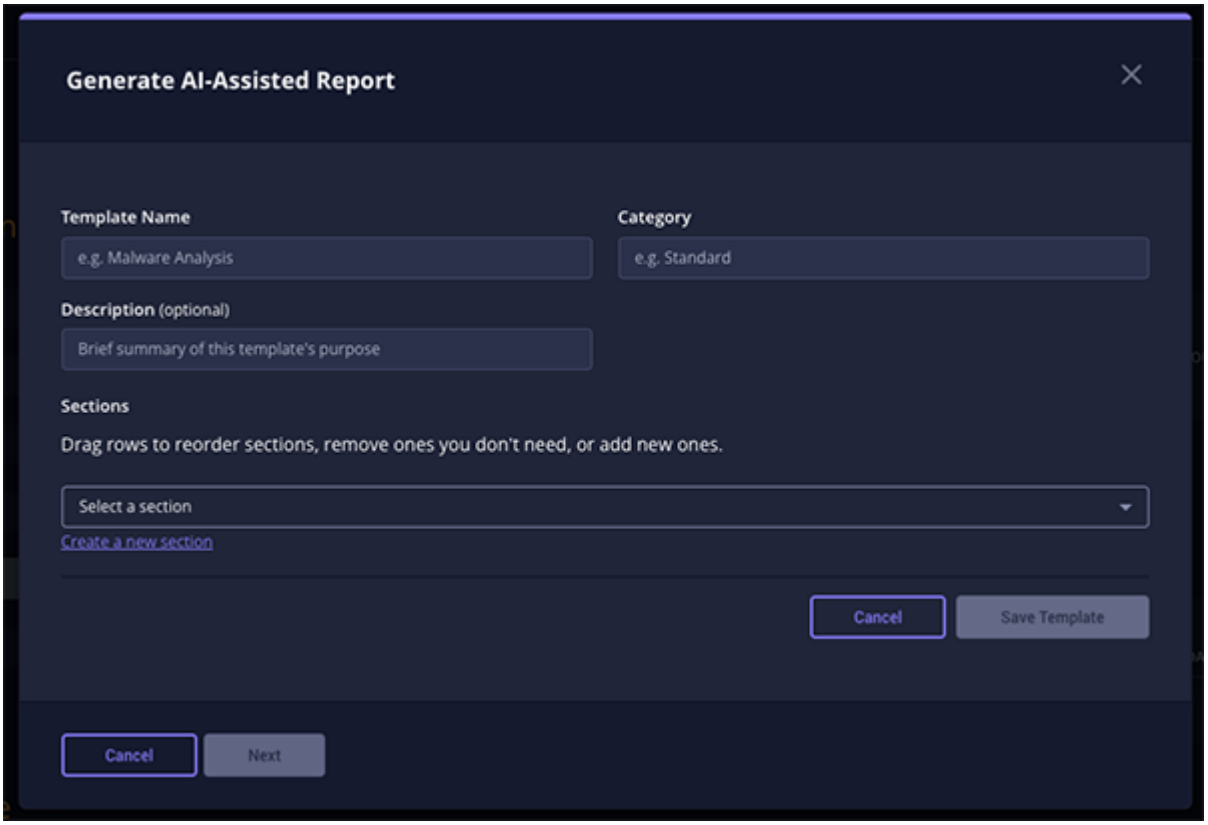
You can create a new chat report template from the Generate AI-Assisted Report modal. This can be access by clicking on the report icon in the agent chat or by clicking on the **Full** option for the **Insights** button on an object's details page.

From the Generate AI-Assisted Report Modal:

1. Click on the **+ Create Template** button.



The new template form will load.



2. Complete the following fields:

FIELD	DESCRIPTION
Template Name	Enter the name for the report template.
Category	Enter the category that the template will be listed under. Categories are listed as tabs on the Generate AI-Assisted Report modal. If the category does not exist, it will be created when you finish the report template setup.
Description	Optional - enter a description about the report template that will help users understand what the template's purpose.

3. Select the report sections to include using the **Select a Section** dropdown. Each section serves as an instruction that guides the AI when generating the report. The dropdown lists all existing sections available across report templates, allowing you to reuse standardized content.

> You can also create new sections for the report using the **Create a New Section** option. Once saved, new sections will be available for use with all reports.

4. Click on **Save Template**.
5. The report will now be available under the category you entered in step 2.

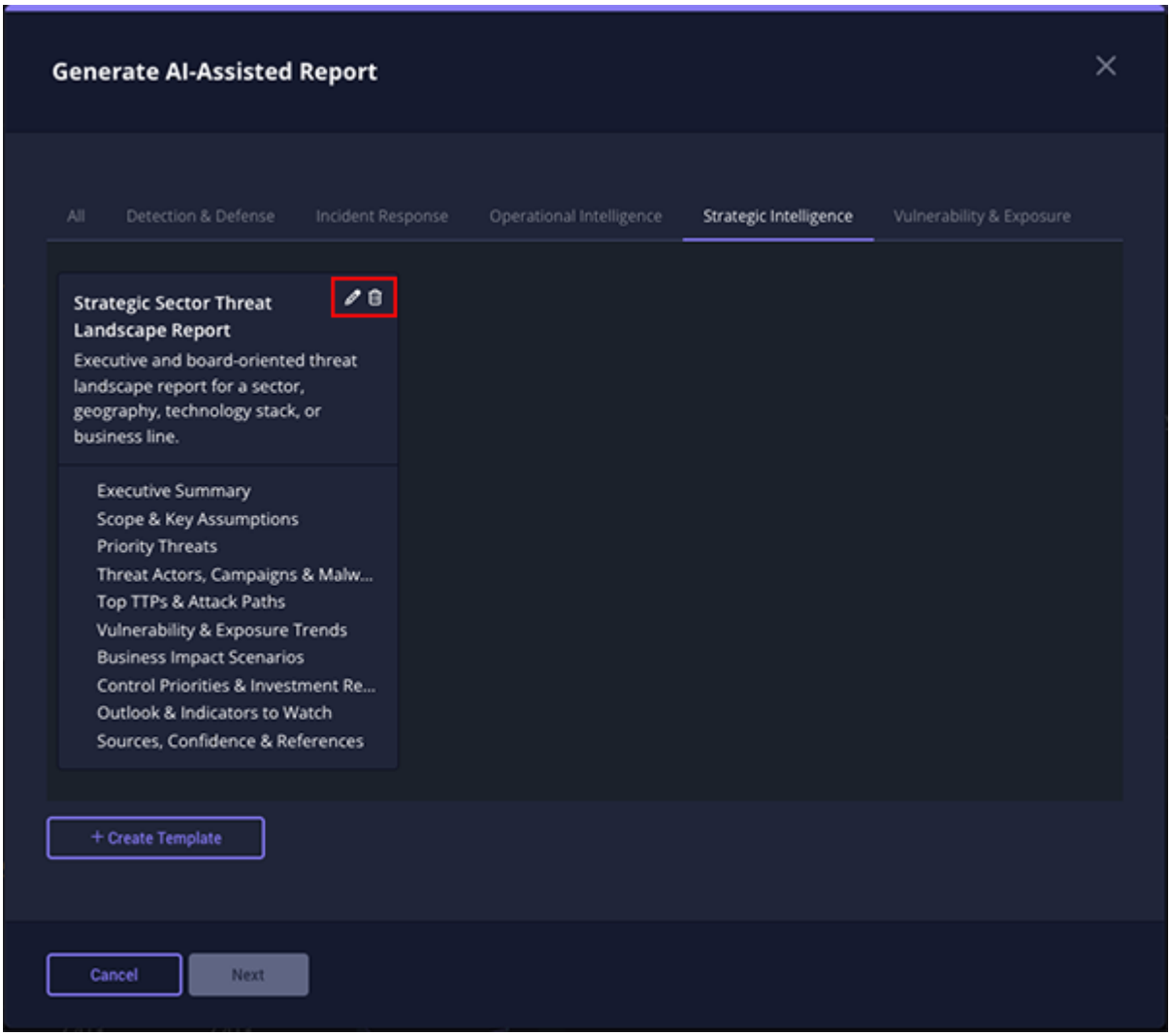
Editing / Deleting a AI-Assisted Report Template

You can edit or delete a chat report template from the Generate AI-Assisted Report modal.

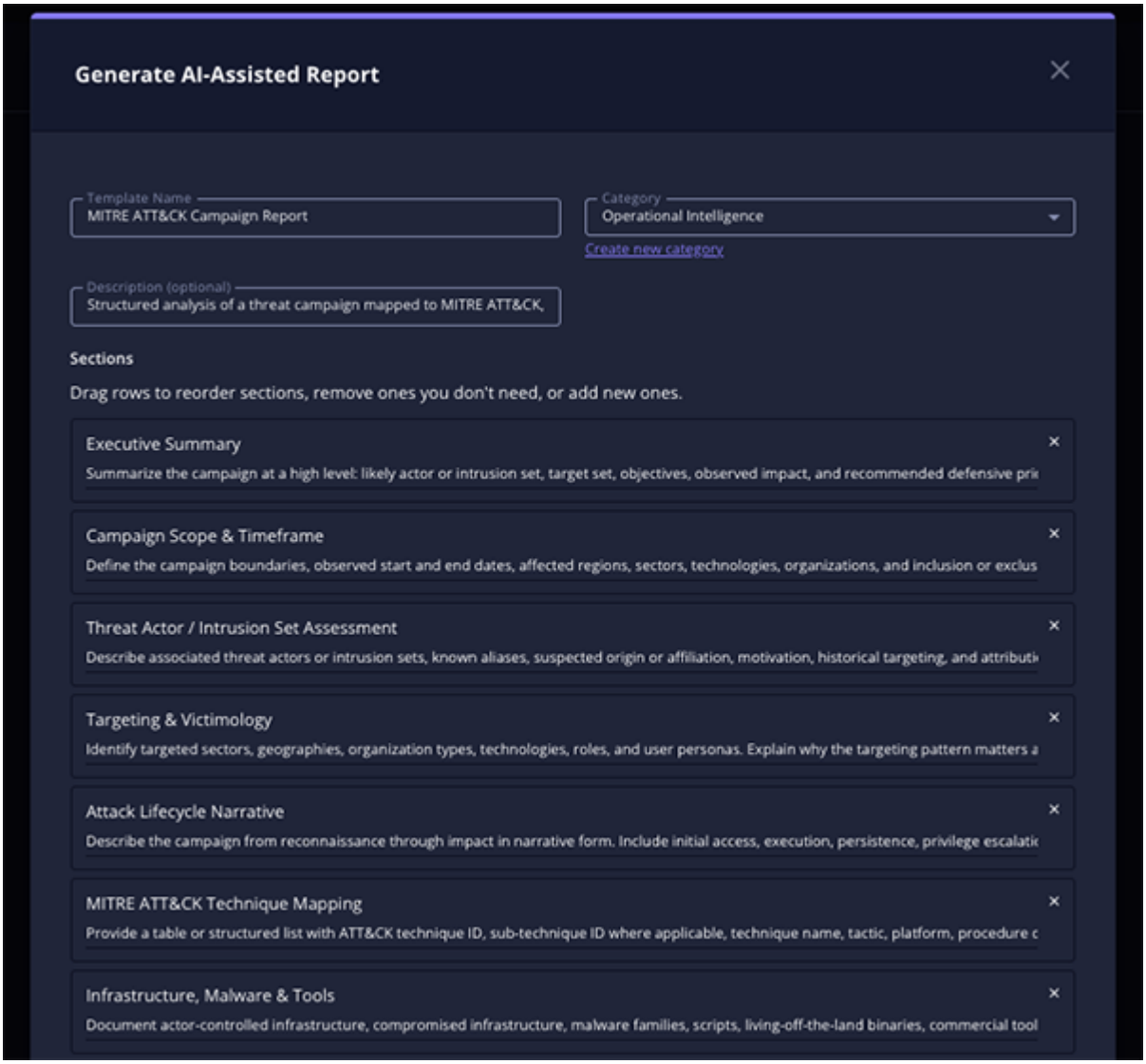
> Deleting a report template is permanent and cannot be undone.

1. Open the Generate AI-Assisted Report modal by clicking on the report icon in the agent chat or by clicking on the **Full** option for the **Insights** button on an object's details page.

2. Click on edit or delete icon, located to the top-right of the individual report's card.



3. If clicked on the delete icon, you will prompted to confirm deletion.
4. If you clicked on the edit icon, the report template builder will load. You can now:
    - Edit the report template name.
    - Change or create a new category for it.
    - Update the report template's description.
    - Reorder, add (new and existing), and delete report sections.



5. Click on **Save Changes** at the bottom of the form once you have completed your updates.

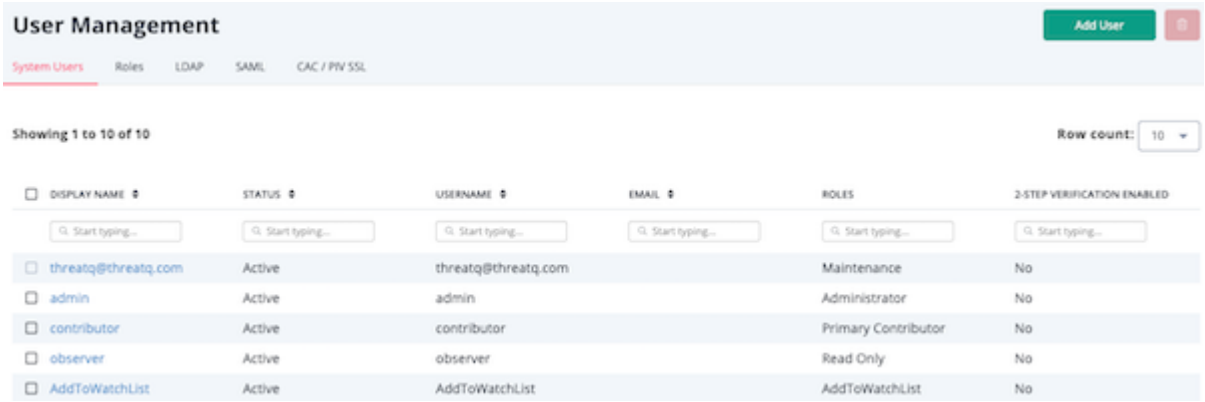
User Management

About User Management

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative or Maintenance
Custom Role - Action Permissions: Administrative Functions - Edit User Management

The User Management page allows you to manage user logins and permissions as well as configure authentication methods.



ThreatQ provides several default user roles, each containing a set of permissions for accessing system functionality. In addition you can create custom roles which allow more granular control over action-level permissions. For each user account you create, you can:

- Assign a default user role which defines the user's permissions.
  OR
- Assign a custom role which specifies action-level permissions.

Example: User Account with Default User Role

User Account = Jane_Smith

Default Role = Administrator

Example: User Account with Custom Role

User Account = Jane_Doe

Custom Role = TQX Restricted

Action Permissions = No permission to edit Data Exchange feeds

After you create a user account, you can use the Edit User screen to further customize its account maintenance and display settings.

User Roles

ThreatQ provides four user roles: Maintenance, Administrator, Primary Contributor, and Read Only. Maintenance and Administrator user roles provide access to the entire ThreatQ user interface as well as the ability to edit all data. The Primary Contributor role provides limited editing capabilities. And, the Read Only role allows users to view but not edit data.

See the Default User Roles section for more information on each user role.

Custom Roles

You can use action permissions to create custom roles that customize user access and provide more robust role-based action control (RBAC). This approach to managing user access allows you to ensure that users have the access they need and to minimize their exposure to data and functions to which they do not require access.

See the Custom User Roles topic for more information on creating and updating custom roles.

Action Permissions

Action permissions allow you to customize a user's ThreatQ permissions by enabling or blocking certain actions. ThreatQ provides action permissions for: Administrative Functions, Artifact Management, Objects & Context, Data Controls, Integrations, Orchestration, and Data Exchange.

> Access to any area of ThreatQ not covered by Action Permissions defaults to the access level defined for the Primary Contributor default role.

See the Action Permissions section for more information on each permission's options.

Custom Roles and Sharing Permissions

- Action permissions defined in a custom user role influence sharing permission options for dashboards, data collections, and investigations:

  - If your custom role specifies view-only access to dashboards, you can only be added to a dashboard as a viewer.
  - If your custom role specifies view-only access to data collections, you can only be added to a data collection as a viewer.
  - If your custom role specifies view-only access to investigations, you can only be added to an investigation as a viewer.
    In addition, the Sharing modal lists a view-only icon next to your name and only includes your name in searches with the Viewer filter enabled.
- View-only sharing permissions for all users take precedence over action permissions defined in a custom user role For example, even if your custom user role gives you Create, Edit, Delete permissions for data collections, you cannot edit or delete a data collection with a permission level of **Everybody (Public)**.

Custom Roles and API Updates

ThreatQ enforces the action permissions associated with the user's custom role when the user account sends a write request via the API.

For example, tquser1 does not have Create/Edit/Delete permission for object attributes and sends a write request that includes attributes. As a result, ThreatQ returns an error.

Custom Roles and Integrations/TQO Workflows

Custom role permissions control access to the pages that allow you to execute manual runs of integrations or TQO workflows. However, custom roll permissions do not apply to the objects and object context created/ingested. A manual feed or workflow run can ingest system objects and any type of associated context regardless of the permissions of the authenticated user who initiated the run.

ThreatQ License Updates

When you update an instance's ThreatQ license, each user account that has permission to access the User Management page will receive the following in-app notification to update all roles to include newly available permissions:

Due to a recent upgrade, some role permission configuration options for users may have changed. Visit the User Management page to update your settings.

This notification includes a link to the Role tab in the User Management page. The notification is sent for every license update, regardless of whether features were added or removed.

If your license update involves removing a product, any action permissions defined in custom user roles are also removed and must be manually added if you add the product at a later date. For instance, if your current license

includes ThreatQ Investigations and you update to a new license that does not, any investigation action permission defined in a custom user role is removed.

Managing User Accounts

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative or Maintenance
Custom Role - Action Permissions: Administrative Functions - Edit User Management

The Edit User page allows you to customize each user account's account maintenance and display settings.

Account Maintenance Settings

SECTION/FIELD	DESCRIPTION
Profile Information	Allows you to specify a display name and title for each user. These settings are independent of the username required for logging into ThreatQ. In addition, you can update a user's permissions by changing the user role group assigned during login creation.
Change Password	Allows you to change the user's current password.
Role Assignment	Allows you to select the user role assigned to the user account. The user role controls the user's access to the ThreatQ user interface and ability to edit ThreatQ data. You can also use the **View all roles** and **View permissions** links to access a list of user roles and permissions in the User Management page. You can also add/update a user account's user role via the Roles tab in the User Management page. You cannot update your role assignment when accessing your own account by clicking the avatar icon.
API Credentials - Client ID	Displays the user's unique client ID. This ID can be used to connect with ThreatQ's API or by external scripts and integrations that authenticate with ThreatQ.

SECTION/FIELD	DESCRIPTION
Session Timeout	Allows you to disable session timeouts for the user or change the inactivity duration that triggers a session timeout. By default, the user's session times out after sixty minutes of inactivity.
Enable 2-Step Verification	Optional. 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.
Account Status	Allow you to enable/disable the user account.
Account Activity	You can click the Account 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.

Display Settings

SECTION/ FIELD	DESCRIPTION
User Avatar	Allows you to upload an image file that displays in the following locations: • Upper right corner of each ThreatQ page • Next to the user name when displayed in the Role Assignment section of the Roles tab (User Management page) . ThreatQ provides a default avatar based on the user's initials.
Screen Display	Allows you to specify dark or light mode display for ThreatQ pages.

SECTION/ FIELD	DESCRIPTION
Timezone Display	Allows you to override the system default timezone and select the timezone displayed in the ThreatQ user interface and PDFs. This selection only affects the display of timestamps in the user interface and PDFs. ThreatQ continues to store timestamps in UTC and share UTC timestamps with resources such as ThreatQ Data Exchange (TQX), ThreatQ TDR Orchestrator (TQO), exports, and TAXII.

While all users can update their own accounts, only users with access to the User Management page through a Maintenance Account or Administrative Access default user role or a custom user role with permission to edit User Management can access the User Management page and add new or update existing 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

Click your avatar icon, located in the top right corner and select the My Account option. The Edit User screen allows you to review and update your Account Maintenance and Display settings.

You **cannot** update your role assignment from this page.

If your user role provides edit access to the User Management page, you can view all user roles, view your user role's permissions, and update your session time out settings.

Accessing Other User Accounts

To add, edit, and delete user accounts, you must have either a Maintenance or Administrative default user role or a custom user role that includes permission to edit user management.

1. Click the Settings icon and select the User Management option. 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. Based on your permissions, you can also click a display name to access the User Profile and Account Activity tabs for the user account:
    - **User Profile tab** - Lists the Account Maintenance and Display settings for the user.
    - **Account Activity tab** - Lists the last date and time the user logged in, the IP Address where the user logged in, and whether the login was successful or not.

Adding a User

To add, edit, and delete user accounts, you must have either a Maintenance or Administrative default user role or a custom user role that includes permission to edit user management.

1. Click the Settings icon and select the User Management option.
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 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.

- **User Role** - *Required.* Select the user role for the user account. The View permissions link below this field allows you to view the default user role, action permissions, and assigned user accounts for the user role you select.
- **Password** - *Required.* Enter the user's password.
- **Retype Password** - *Required.* Re-enter the user's password.

4. Click the **Add User** button.
   The System Users tab displays the new user. See the Editing a User topic for information on further customizing the user profile.

Editing a User

To add, edit, and delete user accounts, you must have either a Maintenance or Administrative default user role or a custom user role that includes permission to edit user management.

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

Tips and Tricks

- The Suggested option in the Timezone Display field is based on your browser timezone.
- The Timezone Display field allows you to scroll through a list of timezones in alphabetical order by continent/region and city or search for a timezone by city, region or timezone abbreviation or name.
- After you select a timezone, the Reset option allows you to reset your timezone display to Greenwich Mean Time (GMT).

1. Click the Settings icon and select the User Management option.

   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.
3. Enter your updates to the user's Account Maintenance and Display settings.
4. Click the **Save** button.

Resetting a User Password from the Command Line

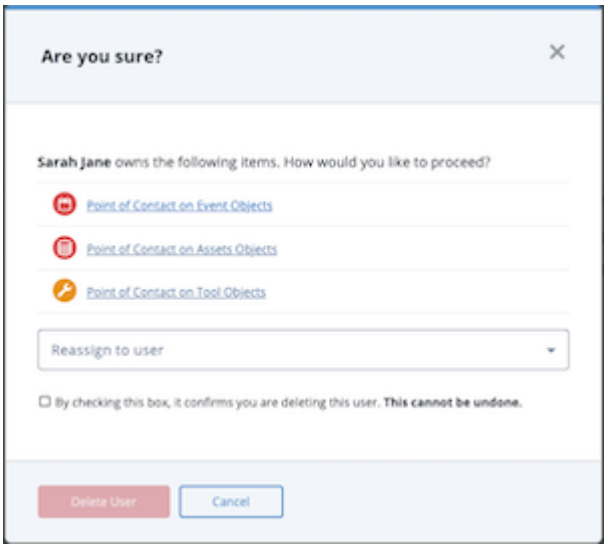
If you have root access to your ThreatQ installation, you can reset any user's password from the command line. See the Reset User Password section in the Commands topic.

Deleting a User

Deleting a user cannot be undone. In addition, you cannot delete the user account you are currently logged in with.

1. Click the Settings icon and select the User Management option.
2. In the System Users tab, click the checkbox next to each user you want to delete.
3. Click the trashcan icon.
   ThreatQ reviews the user ID to determine if it has any shared data collections, data feeds, dashboards, or investigation. In addition, it determines if the user is listed as point of contact on any system object or is assigned with a task. If so, the **Are you sure?** window displays and prompts you to select a new user to replace the deleted user.

   To view more information on the items a user is linked to, you can click the corresponding link on the item name. For instance, click the **Point of Contact on Event Objects** link to view a Threat Library listing of all event objects for which the user is a point of contact.



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. This user will also replace the deleted user as an object's point of contact and/or a task's assignee.

     The new owner must have permission to access the resource type. For instance, to assign John as the new owner of a data collection, he must have permission to create, edit, or delete data collections.

- **Delete** - Select the **Do not reassign. Delete these items and remove users from objects.** option to delete all of the user's data collections, data feeds, dashboards, and/or investigations. In addition, the user is removed as a point of contact or task assignee.

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.

Default User Roles

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative or Maintenance
Custom Role - Action Permissions: Administrative Functions - Edit User Management

The following table lists the default user roles seeded in each ThreatQ instance and details their permissions. You can assign these default user roles to user accounts as is.

A user account's access to dashboards, data collections, and investigations can be further customized by the Sharing permissions assigned to them.

DEFAULT USER ROLE	BASE-LEVEL PERMISSIONS	ACTION PERMISSIONS
Maintenance	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 Functions • Artifact Management • Objects & Context • Data Controls • Integrations • Orchestration • Data Exchange • Agentic Assistance
Administrator	Members have access to the entire ThreatQ user interface and can edit all data.	• Administrative Functions • Artifact Management • Objects & Context • Data Controls • Integrations

		• Orchestration • Data Exchange • Agentic Assistance

Primary Contributor	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.
		• Administrative Functions
		  ◦ View Audit Log
		• Artifact Management
		• Objects & Context
		  ◦ Objects
		  ◦ Individual Object Context and Actions
		  ◦ Bulk Object Management
		  ▪ Perform Bulk Changes
		  ▪ Perform Bulk Manual Import
		  ▪ Manage Object Statuses
		  ▪ Manage Object Sub-types
		• Data Controls
		  ◦ Edit Indicator Expiration
		  ◦ Edit Scoring
		  ◦ Edit Whitelisting
		• Integrations
		  ◦ Run Operations

		• Orchestration ◦ Run Manual Workflows
Read Only	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.	• Administrative Functions ◦ View Audit Log • Artifact Management - View Only • Objects & Context - View Only/No Access

Viewing Default User Roles

You can view default user roles in the Roles tab of the User Management page. Default user role permissions are view-only and cannot be changed. However, you can use the Roles tab to assign default user roles to user accounts.

1. From the User Management page, click the Roles tab.

   Default user roles are listed with a person icon instead of a checkbox.

2. Browse the Roles list or use the Search field to locate the default user role.
3. Click the default user role to view its permissions in the right pane. This pane lists:
   - **Role Name**
   - **Action Permissions** - You can expand the Action Permission sections to view the default user role's permissions.
   - **Role Assignment** - This section lists the user accounts currently assigned to the default user role and gives you the option to add a user to the role or reassign an existing user to a new role.

Adding User Accounts to a Default User Role

1. From the User Management page, click the Roles tab.
2. Browse the Roles list or use the Search field to locate the default user role you want to add to the user account.

3. Click the user role to view its details in the right pane.
4. To assign the default role to a user account, use the **Search to add** field to locate the user account.
    - Begin typing the name of the user account to which you want to assign the role. The field displays the user accounts that match your entry.
    - Click the user account to which you want to assign the role.

    > Until you save your changes, a **Remove** option is displayed to the left of the user name. This option allows you to remove the user account from the custom role before saving your changes.

5. Repeat step 4 to continue adding the user role to multiple user accounts.
6. Click the **Save Changes** button. The new user role is assigned to the user account whether the user account does or does not have a custom or default user role already.

Custom User Roles

About Custom User Roles

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative or Maintenance
Custom Role - Action Permissions: Administrative Functions - Edit User Management

A custom role consists of the role name and action permissions. While creating a custom user role, you can also assign the custom user role to user accounts.

Tips and Tricks

- To view all action permission options, click the **Expand All** option to the left of the Action Permissions section name. Click the **Collapse All** option to display only the action permission section names.
- To view all permission options within a section, click the arrow located to the right of the section name.
- To view and enable all permissions within a section, click the toggle to the left of the section name to change it to green. To disable all permissions within a section, click the toggle to change it to grey.
- When you enable at least one option within an action permission section, the section's toggle changes to green.

Creating a Custom User Role

1. From the User Management page, click the Roles tab.
2. Click the **Create Role** button.
3. Enter a name for the custom role in the Role Name field.
4. Select the action permissions for the custom role.
   See the Action Permissions and Interdependent Permissions topics for more information on each permission option.
5. Select the system-object level permission for the custom role.
   See the Data Access Permissions topic for more information.
6. To assign the default role to a user account, use the **Search to add** field to locate the user account.

- Begin typing the name of the user account to which you want to assign the role.
  The field displays the user accounts that match your entry.
- Click the user account to which you want to assign the role.

7. Repeat step 5 to continue adding the custom user role to multiple user accounts.
8. Click the **Save** button.

Assigning a User Role to a User Account

You can use the following methods to assign a user role to a user account:

- Access the desired user role and use the Search to add field in the Role Assignment section.
- Access the current user role and use the Reassign option in the Role Assignment section.
- Access the user profile and select a new user role.
- Assign a custom role to the user account during the process of creating a custom role.

> When you assign a new user role to a user account that already has a user role, the existing user role is replaced with the new user role.

Assign a User Role From the Desired User Role

1. From the User Management page, click the Roles tab.
2. Browse the Roles list or use the Search field to locate the user role you want to add to the user account.
3. Click the user role to view its details in the right pane.
4. To assign the default role to a user account, use the **Search to add** field to locate the user account.
   - Begin typing the name of the user account to which you want to assign the role. The field displays the user accounts that match your entry.
   - Click the user account to which you want to assign the role.

     > Until you save your changes, a Remove option is displayed to the left of the user name. This option allows you to remove the user account from the custom role before saving your changes.

5. Repeat step 4 to continue adding the custom user role to multiple user accounts.
6. Click the **Save Changes** button.

> The new user role is assigned to the user account whether the user account does or does not already have a custom or default user role.

Assign a User Role from the Current User Role

1. From the User Management page, click the Roles tab.
2. Browse the Roles list or use the Search field to locate the user account's current user role.
3. Click the user role to view its details in the right pane.
4. In the Role Assignment section, locate the user account.
5. Click the **Reassign** option next to the user account.
6. In the Reassign to New Role window, select the desired user role.
7. Click the **Reassign** button.
8. Click the **Save Changes** button.

Updating a Custom User Role

1. From the User Management page, click the Roles tab.
2. Browse the Roles list or use the Search field to locate the user role you want to update.
3. Click the user role to view its details in the right pane.
4. Enter your changes to the role's name and/or action permissions. You can also update the user accounts to which the user role is assigned.

> If you remove an action permission that disables a related permission, ThreatQ displays an Additional Updates Required prompt window that guides you through the changes. See the Interdependent Permissions topic for more information.

5. Click the **Save Changes** button.

> When you update a role's permissions, the users assigned to the role must log out and log in for the permission changes to take effect.

Deleting a Custom User Role

1. From the User Management page, click the Roles tab.
2. Browse the Roles list or use the Search field to locate the user role you want to delete.
3. Check the checkbox next to the user role to view its details in the right pane.
4. Click the delete/trashcan button.
5. If user accounts are assigned to the user role:
    - The Reassign Users & Remove Role window prompts you to select a new user role for the user accounts and click the **Reassign & Remove** button to save your selection.
6. If no user accounts are assigned to the user role:
    - The **Are you sure?** window prompts you to click the **Remove** button to confirm the deletion.

Action Permissions

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative or Maintenance
Custom Role - Action Permissions: Administrative Functions - Edit User Management

Each custom role consists of action permissions which allow you to control access to:

- **Administrator Functions** - Controls access to the options on the settings menu such as Exports, Job Management, Notification Settings, Report Options, System Configuration, and User Management as well at the Audit Log pane in the object details page.
- **Artifact Management** - Controls access to custom dashboards, data collections, and TQI investigations.

  A user account's access to dashboards, data collections, and investigations can be further customized by the Sharing permissions assigned to them.

- **Objects & Context** - Controls the ability to update system objects individually as well as through bulk processes.
- **Data Controls** - Controls access to the Indicator Expiration, Data Retention Policy, Scoring, TLP, and Whitelisted Indicators tabs in the Data Controls page.
- **Integrations** - Controls the ability to add, remove, or configure integrations as well as the ability to run operations.
- **Orchestration** - Controls access to ThreatQ TDR Orchestrator including the ability to edit an advanced workflow or run a manual workflow.
- **Data Exchange** - Controls access to ThreatQ Data Exchange including the ability to edit data exchange feeds.
- **Agentic Assistance** - Controls access to the MCP and Agentic AI services for the Threat Reasearch Agent.

Interdependent Permissions

Some action permissions require related permissions. For example, a user role that includes the Edit TLP permission also requires the Edit Sources permission. When you add or remove action permissions that require related permissions, ThreatQ guides you through adding or removing the related permissions. See the Interdependent Permissions section for more information.

Object Creation and Object Context Permissions

When you create an object through an object modal or an object parser/import, you can update only the context fields for which you have permission. For example, if tquser has View Only permission for Descriptions, the editable Description field is not displayed in the Add An Adversary modal or any other object creation modal.

> If a user has View Only permission for Sources, system object parsers and system object creation modals default to the user's login as the object source.

Navigating the Action Permissions Section

The Action Permissions sections in the Roles tab and the Create Role page allow you to view or update a custom role's permissions:

- **View permission options** - Click the arrow located to the right of a permission section to view the options for that section. Or, click the **Expand All** option to view the options for all sections.
- **Update permissions** - Within an expanded permission section, check or uncheck the checkbox next to a permission option to enable or disable it. Or, you can enable/disable all the permission options within a section, by clicking the toggle to the right of the permission section name.

Administrative Functions Permission Group

PERMISSION OPTION	PERMISSION SETTINGS
Edit Exports	Controls the ability to add, edit, enable or disable exports. A user without this permission can view the Exports page and access export URLs but cannot add or change exports.
View Job Management	Controls access to the Job Management page.
Edit Notification Settings	Controls access to the Notification Settings page as well as the ability to edit Notification Management and Mail Server Configuration settings.
Edit Report Options	Controls access to the Report Options page as well as the ability to update report format settings.

PERMISSION OPTION	PERMISSION SETTINGS
Edit System Configurations	Controls access to the System Configurations page as well as the ability to edit Account Security, Proxy, and General settings.
Edit User Management	• **User Management Page** - Controls access to the page as well as the ability to edit user accounts, custom user roles, and authentication settings (LDAP, SAML, and CAC/PIV SSL). • **User Profile** - Controls the display of the **View all roles** and **View permissions** options in the Role Assignment section. Also, controls the option to change your Session Timeout settings.
View Audit Log	Controls the ability to view the Audit Log pane in the object details page.

Artifact Management Permission Group

PERMISSION OPTION	PERMISSION SETTINGS
Dashboards	Controls the ability to view, create, edit, or delete custom dashboards. A user's access to dashboards, data collections, and investigations can be further customized by the Sharing permissions assigned to them.
Data Collections	Controls the ability to view, create, edit, or delete data collections.

PERMISSION OPTION	PERMISSION SETTINGS
Investigations	This option is displayed only if your ThreatQ instance has a ThreatQ Investigations (TQI) license. Controls the ability to view, create, edit, or delete investigations.

Object & Context Permission Group

PERMISSION OPTION	PERMISSION SETTINGS
Objects	Controls the ability to: • Create system objects (including investigations) by clicking the **Create** button or by clicking the **Create <object type>** link in the object Search window. • Delete system objects from the Threat Library. • Edit an object's Value/Name and Type fields in the object details page. These permissions apply to all seeded and custom objects. Users with Create, Edit, Delete permissions can update only the context fields for which they have permission. See the Object Creation and Object Context Permissions section for more details. Users can only add Signature objects via a manual import. As a result, the Create menu only displays the Signature option for users whose role includes Create, Edit, Delete permissions for **Objects** and permission to **Perform Bulk Manual Import**.

PERMISSION OPTION	PERMISSION SETTINGS
Individual Object Context and Actions	Controls the ability to create, edit, and delete the following information: • **Attributes** - Object details page, object preview panel • **Sources** - **Add <object type>** modal, object details page, object preview panel, Bulk Changes If a user has View Only permissions for Sources, system object parsers and system object creation modals default to the user's login as the object source. • **Tags** - Object details page, object preview panel • **Descriptions** - Add object type modal, object details page, object preview panel • **Comments** - Object details page, object preview panel • **Relationships** - Add object type modal, object details page, object preview panel, Bulk Changes In addition, these permissions determine the user's ability to perform the following tasks in the object details page and object preview panel: • **Create and edit PDF extracts of system object details** • **Add or remove a system object from the Watchlist** • **Edit or delete an object's Point of Contact** • **Edit or delete an object's Status** If your role does not include this permission, the Indicator, Signature, Spearphish, and STIX parsers apply the default status to seeded system objects and the first status option for custom objects. • **Edit the Score assigned to an object** • **Edit or delete an object's Expiration Date**

PERMISSION OPTION	PERMISSION SETTINGS
Bulk Object Management	Controls the ability to change groups of objects through the Threat Library and the Object Management page: • Threat Library: ◦ Bulk Changes using the Threat Library Bulk Changes option. ◦ Bulk Manual Imports using the Indicator, Signature, Spearphish, or STIX parsers. Users can only add Signature objects via a manual import. As a result, the Create menu only displays the Signature option for users whose role includes Create, Edit, Delete permissions for **Objects** and permission to **Perform Bulk Manual Import**. ◦ Bulk Deletes using the Threat Library Bulk Delete option. • Object Management Page: ◦ Editing Indicator and Object Statuses via the Indicator Statuses and Object Statuses tabs (Manage Object Statuses). ◦ Editing Indicator and Event object types via the Indicator Types and Event Types tabs (Manage Object Sub-types). ◦ Update System Attributes via the Attribute Management tab (Manage System Attributes)

Data Control Permission Group

PERMISSION OPTION	PERMISSION SETTINGS
Edit Indicator Expiration	• Controls the ability to view or edit the Indicator Expiration tab in the Data Controls page. This permission **does not** control the ability to update expiration in the object details page or through a bulk update.
Edit Data Retention Policy	• Controls the ability to view or edit the Data Retention Policy tab in the Data Controls page. • Gives users access to the data collection currently assigned to the data retention policy.
Edit Scoring	• Controls the ability to view or edit the Scoring tab in the Data Controls page. This permission **does not** control the ability to update scoring in the object details page or through a bulk update. To edit indicator scoring, you must also have permission to Manage Object Sub-types.
Edit TLP	Controls the ability to view or edit the TLP tab in the Data Controls page. This permission **does not** control the ability to add a TLP during manual creation of an object or through a bulk update.

PERMISSION OPTION	PERMISSION SETTINGS
Edit Whitelisting	• Controls the ability to view or edit the Whitelisted Indicators tab in the Data Controls page. This permission **does not** control the ability to whitelist an object through the object details page or through a bulk update.

Integrations Permissions Group

PERMISSION OPTION	PERMISSION SETTINGS
Install & Uninstall Integrations	Controls a user's ability to: • Use the **Add New Integration** button in the Integrations page to install integrations. • Use the **Uninstall** button in the integration configuration page to remove an integration.
Edit Integration Configurations	• Controls a user's ability to access an integration's configuration page and update an integration's configuration options.
Run Operations	• Controls a user's ability to view the Operations pane in the object details page and apply an operation to the object. • To view the Activity Log tab in the integrations configuration page, you must have the Run Operations permission. • This permission is required to run operations as tools via the Threat Research Agent AI.

Orchestration Permissions Group

This option is displayed only if your ThreatQ instance has a ThreatQ TDR Orchestrator (TQO) license.

Custom role permissions control access to the pages that allow you to execute manual runs of TQO workflows. However, custom roll permissions do not apply to the objects and object context created/ingested.

PERMISSION OPTION	PERMISSION SETTINGS
Edit Orchestration Workflows	• Controls the ability to view TQO pages, create, edit, or delete TQO workflows, and configure Action integrations. • To make full use of TQO, a user's role must include additional permissions. See the Interdependent Permissions section for more information.
Run Manual Workflows	• Controls the ability to run a manual workflow from the object details page or the Threat Library. • Gives the user access to all **existing** workflow data collections.

Data Exchange Permissions Group

This option is displayed only if your ThreatQ instance has a ThreatQ Data Exchange (TQX) license.

PERMISSION OPTION	PERMISSION SETTINGS
Edit Data Exchange Feeds	• Controls the ability to view, create, or edit ThreatQ Data Exchange's OpenDXL transports or TAXII server pages.

- Gives the user access to all **existing** TAXII data collections.

Agentic Assistance Permissions Group

PERMISSION OPTION	PERMISSION SETTINGS
Access MCP Server	• Gives user access to the MCP service which allows them to query data within ThreatQ but they will not have access to the Agent Service that uses the LLM models.
Use Agentic Chat	• Gives user access to the Agent Service that uses the LLM models.

Data Access Permissions

Data Access Permissions work in conjunction with the Objects action permission to control access by object type (for example, Indicator, Adversary, Event, Campaign).

For each object type, you can assign one of the following permission levels:

- Create, Edit, Delete
- View Access Only
- No Access

Object-type permissions override the Objects permission assigned to the role. For example, you can create a role with Create, Edit, Delete permissions for Objects but specify a View Only data access permission for event objects.

Availability and Scope

Data Access Permissions:

- Apply only to custom roles
- Are not available for default roles (Administrator, Maintenance, Primary Contributor, Read Only)

ThreatQ allows you to assign data access permissions for seeded and custom system object types.

How the Objects Permission and Object-Type Permissions Interact

The available object-type permission options depend on the role's Objects permission:

OBJECTS PERMISSION	AVAILABLE OBJECT-TYPE PERMISSIONS
View Only	No Access, Create, Edit, Delete
Create, Edit, Delete	No Access, View Access Only

Tips and Tricks

- Object-type permissions override the Objects permission.
- If an object-type permission is removed, the Objects permission applies to that object type. For example, if you remove View Access Only permission for

adversary objects, the Object permission of Create, Edit, Delete now applies to adversary objects.

- If an object-type permission is set to the same level as the Objects permission, the object-type entry is removed because it is redundant. For example, if you change the Objects permission to Create, Edit, Delete, ThreatQ removes Create, Edit, Delete permission for indicators.

> If most object types are set to the same permission level, ThreatQ prompts you to update the Objects permission to match. Example: If the Objects permission is set to Create, Edit, Delete but most object types are View Access Only, ThreatQ prompts you to switch Objects to View Access Only and retain exceptions.

Permission Conflicts

If an object-type permission conflicts with an Action Permission, ThreatQ resolves the conflict and notifies you.

Examples:

- If Indicator access is set to View Access Only, related permissions (such as Expiration Date or Score) are downgraded to View Only.
- If Indicator access is set to No Access, related permissions are disabled.
- Increasing an Action Permission (for example, Expiration Date from View Only to Create/Edit/Delete) automatically updates the related object-type permission.

System Object Access Rules

Basic Search

Search results include only object types for which the user has:

- Create, Edit, Delete, or
- View Access Only

The Create <object type> link appears only if the user has Create, Edit, Delete permission for that object type.

Object Details and Relationships

An object's Details page is accessible only if the user has Create, Edit, Delete or View Access Only permission for that object type.

An object type appears in the Relationships section only if the user has access to that object type.

System Object Imports

ThreatQ allows you to parse files to import system objects. You must have Create, Edit, Delete permission for the object type to import it or create relationships via import. If an import contains object types or context you lack Create/Edit/Delete permission for, the import fails.

Examples:

- **Signatures** - Adding a signature object to ThreatQ requires a manual import. As a result, the Create menu only displays the Signature option if your user role includes:
  - Create, Edit, Delete Action permissions for Objects OR Create, Edit, Delete
  - Data Access Permissions for Signatures Permission to Perform Bulk Manual Import.
- **Events** - You can add event objects via the spearphish parser. To do so, your user roles must include the Perform Bulk Manual Import permission.
- **STIX Objects** - For STIX imports, you must have Create, Edit, Delete permission for at least one STIX object type.

Threat Library

You can perform bulk changes only for object types for which you have Create, Edit, Delete permission. You can export Threat Library search results sets only for object types for which you have Create, Edit, Delete or View Only Access.

Feature-Specific Behavior

Dashboards

Your data access permissions control the display of object types in dashboard widgets as well as the display of default and custom dashboards.

Custom Dashboard Examples:

- If you have No Access to Events, you cannot view the Event Analytics dashboard.
- If you have No Access to Adversary objects, you cannot view the Adversary Analytics dashboard.
- If you have No Access to, Files you cannot view the Files Analytics dashboard.
- If you have No Access to indicators you cannot view the Indicator Analytics dashboard

Dashboard Widget Examples:

- If you have No Access to Tasks, you cannot view the Tasks widget in the Overview dashboard.
- If you have No Access to Indicators you cannot view the following Overview dashboard widgets:
  - Overview of Intelligence by Score
  - Incoming Intelligence
  - Watchlist Activity
  - Tasks

Dashboards may appear empty if all widget object types are set to No Access.

Sharing dashboards does not override data access permissions.

Exports

Authenticated exports are filtered based on the user's data access permissions. Anonymous exports generated via access tokens return full results.

Export configurations can include only object types the user can access.

Imports

Adding a signature object to ThreatQ requires a manual import. As a result, the Create menu only displays the Signature option if your user role includes:

- Create, Edit, Delete permissions for Objects
- Create, Edit, Delete Data Access Permissions for Signatures
- Permission to Perform Bulk Manual Import.

Similarly, you can add event objects via the spearphish parser. To do so, your user roles must include the Perform Bulk Manual Import permission

ThreatQ Investigations (TQI)

Data Access Permissions also control your access to object types in TQI. For example:

- Evidence boards show only object types the user can access.
- Objects with No Access can be added to an investigation but cannot be committed or removed.
- Related objects appear only if the user has access to them.

Integrations

Feeds and workflows ingest objects regardless of user permissions.

Interdependent Permissions

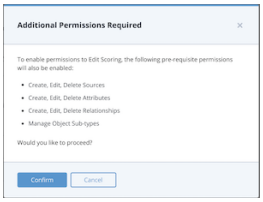
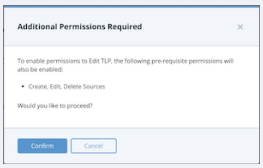
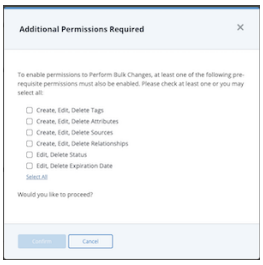
THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative or Maintenance
Custom Role - Action Permissions: Administrative Functions - Edit User Management

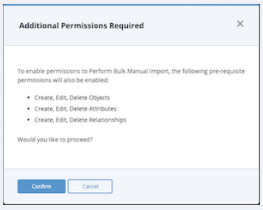
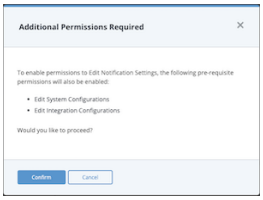
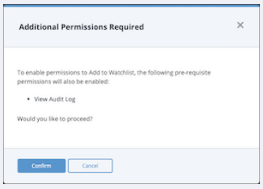
When you add or remove action permissions that require related permissions, ThreatQ guides you through adding or removing the related permissions.

The following action permissions require you to enable other related action permissions:

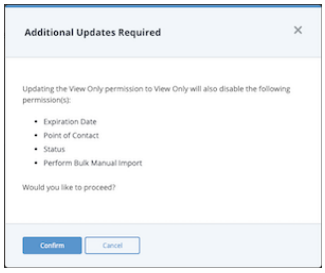
ADDED PERMISSION	ADDITIONAL REQUIRED PERMISSION(S)	PROMPT WINDOW EXAMPLE
Orchestration	To make full use of TQO, a user's role must include: • **All Integrations permissions** - Install & Uninstall Integrations, Edit Integration Configurations, Run Operations • **All Orchestration permissions** - Edit Orchestration Workflow, Run Manual Workflows • **Artifact Management** - Create, Edit, Delete permissions for Data Collections. • **Administrative Functions** - View Audit Log	N/A
Edit Indicator Expirtion	• Requires Action Permissions for all Objects OR Data Access Permissions for Indicators.	

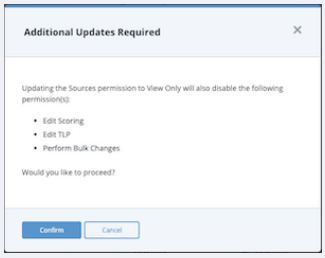
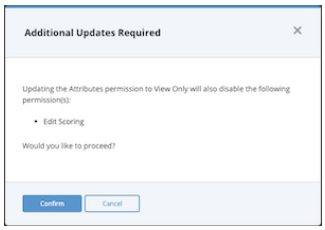
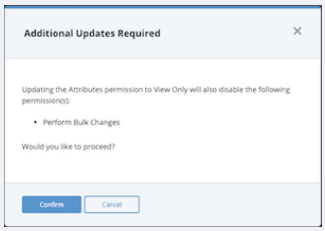
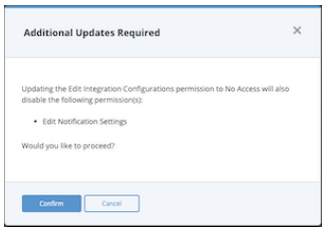
Edit Scoring	• Manage Object Sub-Types • Create, Edit, Delete Sources • Create, Edit, Delete Attributes • Create, Edit, Delete Relationships • Requires Action Permissions for all Objects OR Data Access Permissions for Indicators and Adversaries.	
Edit Whitelisting	• Requires Action Permissions for all Objects OR Data Access Permissions for Indicators.	
Edit Data Retention Policy	• Requires Action Permissions for all Objects.	
Edit TLP	• Create, Edit, Delete Sources	
Perform Bulk Changes	The role must have permissions for **at least one** of the following: • Create, Edit, Delete Attributes • Create, Edit, Delete Sources • Create, Edit, Delete Tags • Create, Edit, Delete Relationships • Edit, Delete Status - Also requires **Create, Edit, Delete Objects** permission • Edit, Delete Expiration Date - Also requires **Create, Edit, Delete Objects** permission	

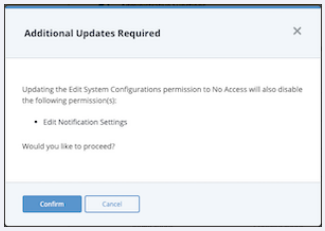
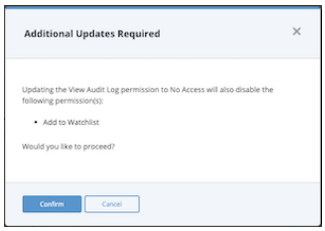
Click the **Select All** option to select all of the above permissions.

Perform Bulk Manual Import	• Create, Edit, Delete Objects • Create, Edit, Delete Attributes • Create, Edit, Delete Relationships	
Edit Notification Settings	• Edit System Configurations • Edit Integration Configurations	
Add to Watchlist	• View Audit Log	
Edit Data Exchange Feeds	• Requires Action Permissions for all Objects.	N/A

Removing the following permissions will disable related permissions:

REMOVED PERMISSION	DISABLED PERMISSION(S)	PROMPT WINDOW EXAMPLE
Create, Edit, Delete Objects	• Expiration Date • Point of Contact • Status • Perform Bulk Manual Import	

Create, Edit, Delete Sources	• Edit Scoring • Edit TLP • Perform Bulk Changes	
You change **any** of the following to View Only: • Create, Edit, Delete Attributes • Create, Edit, Delete Relationships • Manage Object Sub-Types	• Edit Scoring	
Only one of the following is currently enabled and you change it to View Only: • Create, Edit, Delete Attributes • Create, Edit, Delete Sources • Create, Edit, Delete Tags • Create, Edit, Delete Relationships • Edit, Delete Status • Edit, Delete Expiration Date	• Perform Bulk Changes	
Edit Integration Configurations	• Edit Notification Settings	

Edit System Configurations	• Edit Notification Settings	
View Audit Log	• Add to Watchlist	

2-Step Verification

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative or Maintenance
Custom Role - Action Permissions: Administrative Functions - Edit User Management

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.

LDAP Authentication

About LDAP Authentication

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative or Maintenance
Custom Role - Action Permissions: Administrative Functions - Edit User Management

Lightweight Directory Access Protocol (LDAP) authentication verifies a user's identity by validating credentials against a centralized directory service. ThreatQ supports the following LDAP connection options:

- **Anonymous Bind** – enables the application to connect to the LDAP directory without providing credentials. Access is restricted to directory information explicitly configured for anonymous use. See the Anonymous Bind topic for more details.
- **Authenticated Bind** – requires valid LDAP credentials to establish a connection, granting access based on the authenticated account's permissions and group memberships. See the Authenticated Bind topic for more details.

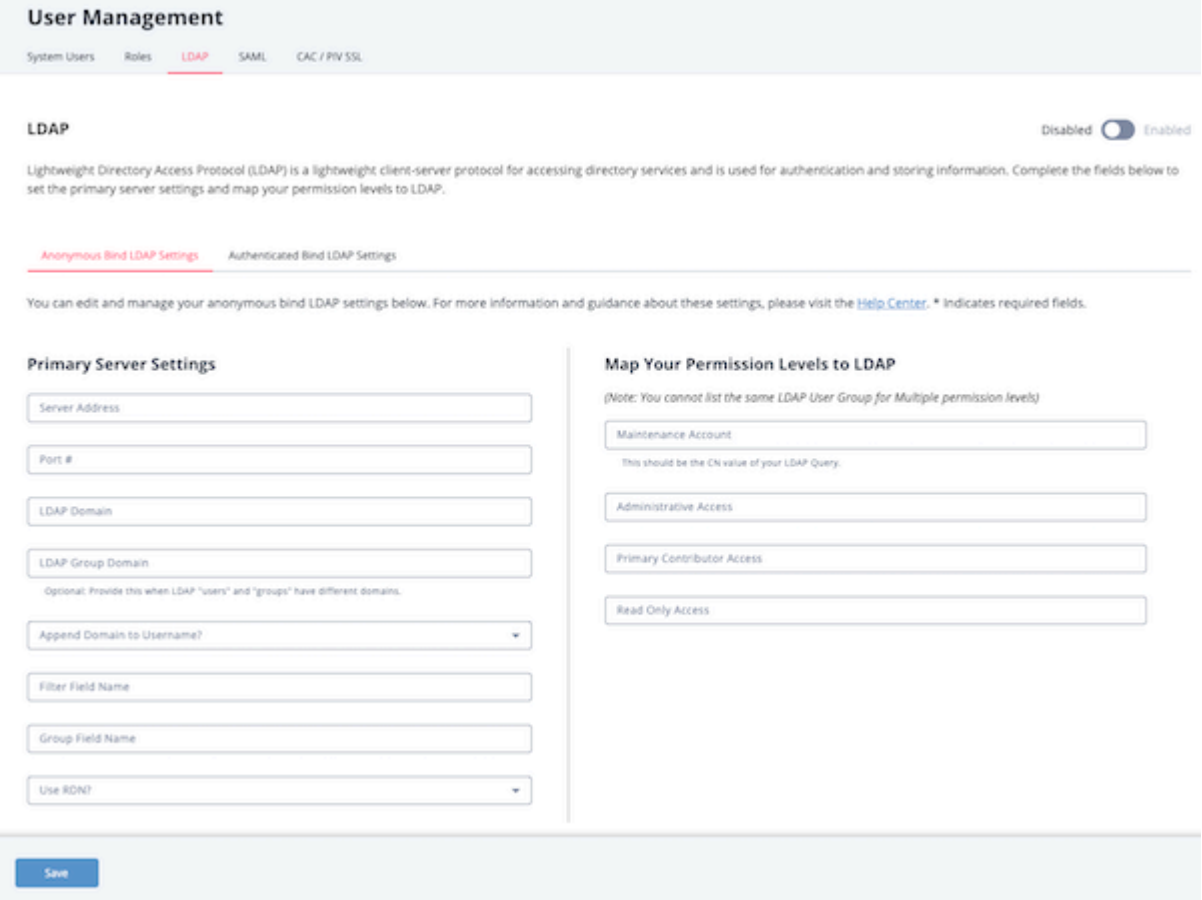
Before configuring LDAP settings, review the following important considerations:

- **LDAP Requirements** - it is highly recommended that you review the LDAP Connection Requirements topic before configuring your LDAP settings.
- **Switching from SSL Client Certificate to LDAP** – if SSL Client Certificate Authentication is enabled, the LDAP configuration tab will display a warning indicating that SSL Client Certificate Authentication (CAC) must be disabled before LDAP can be enabled.
- **Air Gapped Data Sync (AGDS) users** – when LDAP or SAML authentication is enabled on a source ThreatQ instance and users are transferred via import, the same authentication method must be enabled on the target ThreatQ instance prior to the import to ensure continued authentication access for transferred users.

Accessing 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.



LDAP Connection Requirements

Before configuring a connection to your LDAP server, coordinate with your LDAP administrator to obtain, at a minimum, the following required information:

Anonymous Bind

The following information is required for the LDAP Anonymous Bind connection. See the Anonymous Bind topic for full details.

- LDAP Server URL
- LDAP Port
- LDAP Group Field Name
- LDAP Filter Field Name
- * LDAP group mappings for:
    - Super
    - Maintenance
    - Analyst
    - Observer
    - Any custom user roles

Authenticated Bind

The following is required for the LDAP Authenticated Bind connection. See the Authenticated Bind topic for more details.

- LDAP Server URL
- LDAP Port
- LDAP Group Field Name
- LDAP Filter Field Name
- * LDAP group mappings for:
    - Super
    - Maintenance
    - Analyst
    - Observer
    - Any custom user roles

*** Important Note for both Anonymous and Authenticated Bind Group Mappings**

To ensure successful authentication, each LDAP user should belong to only one (1) LDAP user group. If this is not feasible, new LDAP groups should be created with mutually exclusive user membership.

LDAP user groups require careful planning to avoid permission conflicts caused by overlapping group memberships. For example, when a user inherits read/write permissions from one group but is denied write access through another.

It is recommended to implement a clear hierarchy of group memberships for each security device instance, with an administrative group at the top and a standard user group at the bottom. Multi-group membership should be avoided in favor of a least-privilege approach, and group nesting should be kept as shallow as possible.

Permissions should be assigned through group membership rather than individual user roles to maintain consistency and simplify access management.

LDAP Support for Custom Roles

Upon upgrade to v6.16.0, ThreatQ sends the following system notification to all Admin users:

- LDAP Authentication can now map Custom Roles to LDAP User Groups to enable authentication for users in these roles. Your existing group mappings have been migrated. Custom Roles can now be mapped using LDAP User Management

If LDAP is enabled and you create a new custom role, ThreatQ sends the following notification to the Notifications menu:

- Additional LDAP configurations are available due to the creation of a new role. Please map the <role name> role to a user group on the LDAP settings page to complete setup.

Switching LDAP Connections

You can switch between using the Anonymous and Authenticated Bind LDAP connections via the ThreatQ UI.

1. Navigate to **User Management** option page from the Settings dropdown.
2. Click the **LDAP** tab to load the LDAP page.
3. Click on connection type to use and confirm that the required parameters for your selected connection type have been completed.

   See the Anonymous Bind or Authenticated Bind topic for more details on the connection parameters.

4. Click save while under the connection type you intend to use. ThreatQ will now use the selected connection type and settings.
5. You can switch back to the other configured connection (Anonymous > Authenticated or Authenticated > Anonymous) by selecting the desired bind type and clicking **Save**. ThreatQ will use the bind connection that is selected in the ThreatQ UI at the time the save action is performed.

Anonymous Bind

THREATQ REQUIRED PERMISSIONS

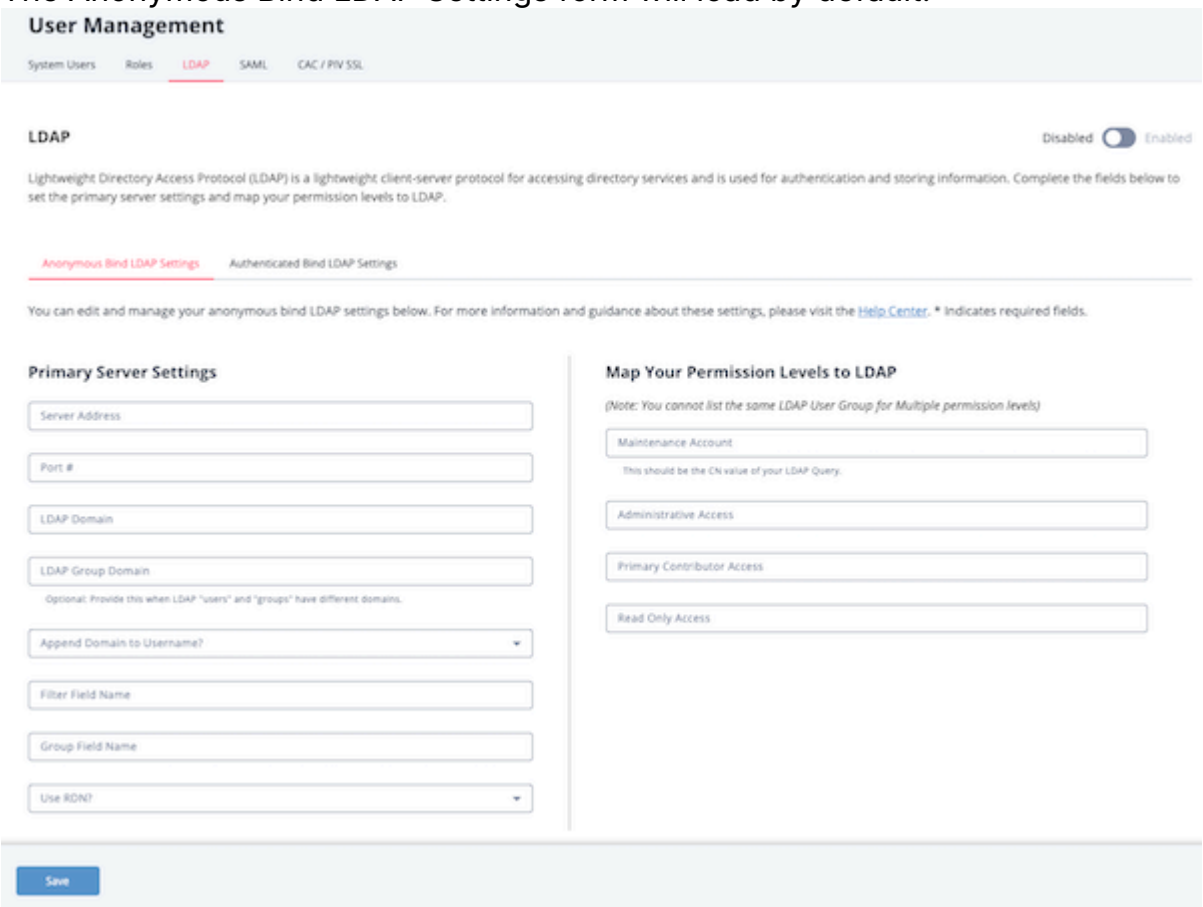
Default ThreatQ Role: Administrative or Maintenance
Custom Role - Action Permissions: Administrative Functions - Edit User Management

Anonymous Bind LDAP refers to an LDAP connection in which a client accesses an LDAP directory without providing authentication credentials.

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.
LDAP Domain	Enter the domain for which LDAP is configured to authenticate. **Example:** threatq.com
LDAP Group Domain	Optional - provide this when LDAP "users" and "groups" have different domains.
Append Domain to Username?	Choose from the following options: ◦ Yes for most Active Directory servers ◦ No for most Open LDAP servers
Filter Field Name	This field is specific to your LDAP directory configuration. **AD Example:** memberuid **OpenLDAP Example:** uid
Group Field Name	This field is specific to your LDAP directory configuration. **AD Example:** memberof **OpenLDAP Example:** cn
Use RDN?	Choose from the following options: ◦ Yes to use Relative Distinguished Names. When you select this option, the Organization Unit (OU) and User Lookup Name fields are displayed. ◦ No to use full Distinguished Names

FIELD	DESCRIPTION
Organizational Unit (OU)	This field is specific to your LDAP directory configuration. Your LDAP administrator should provide the correct value for this field.
User Lookup Name	This field is specific to your LDAP directory configuration. **AD Example:** memberUid **OpenLDAP Example:** uid

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

> To ensure successful authentication, each LDAP user should belong to only one (1) LDAP user group. If this is not feasible, new LDAP groups should be created with mutually exclusive user membership.
>
> LDAP user groups require careful planning to avoid permission conflicts caused by overlapping group memberships. For example, when a user inherits read/write permissions from one group but is denied write access through another.
>
> It is recommended to implement a clear hierarchy of group memberships for each security device instance, with an administrative group at the top and a standard user group at the bottom. Multi-group membership should be avoided in favor of a least-privilege approach, and group nesting should be kept as shallow as possible.
>
> Permissions should be assigned through group membership rather than individual user roles to maintain consistency and simplify access management.
>
> You cannot save the configuration without entering a value in each field. For roles not mapped, you should enter a hyphen: `-`.

FIELD	EXAMPLE
Maintenance Account	**OpenLDAP Example:** ldapSuper **AD Example:** CN=tq-maintenance,CN=Builtin,DC=yourdomain,DC=com

FIELD	EXAMPLE
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
<custom user role>	**OpenLDAP Example:** ldapAnalystPlus **AD Example:** CN=analystplus,CN=Builtin,DC=yourdomain,DC=com

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

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

Configuring Secure LDAP

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

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

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

1. Enter your LDAP settings in the ThreatQ user interface. See the Anonymous Bind steps above for more details.
2. Access the ThreatQ appliance command line as root and edit and navigate to the following directory: /etc/openldap/.
3. Use vi to edit ldap.conf and update/confirm that your settings are as follows:

```
#
# LDAP Defaults
#
# See ldap.conf(5) for details
# This file should be world readable but not world writable.
BASE dc=[your domain],dc=com
URI ldap://[your servername]:389 ldaps://[your servername]:636
#SIZELIMIT 12
#TIMELIMIT 15
#DEREF never
TLS_CACERTDIR /etc/openldap/certs
# Turning this off breaks GSSAPI used with krb5 when rdns = false
SASL_NOCANON on
TLS_REQCERT allow
```

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

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

Authenticated Bind

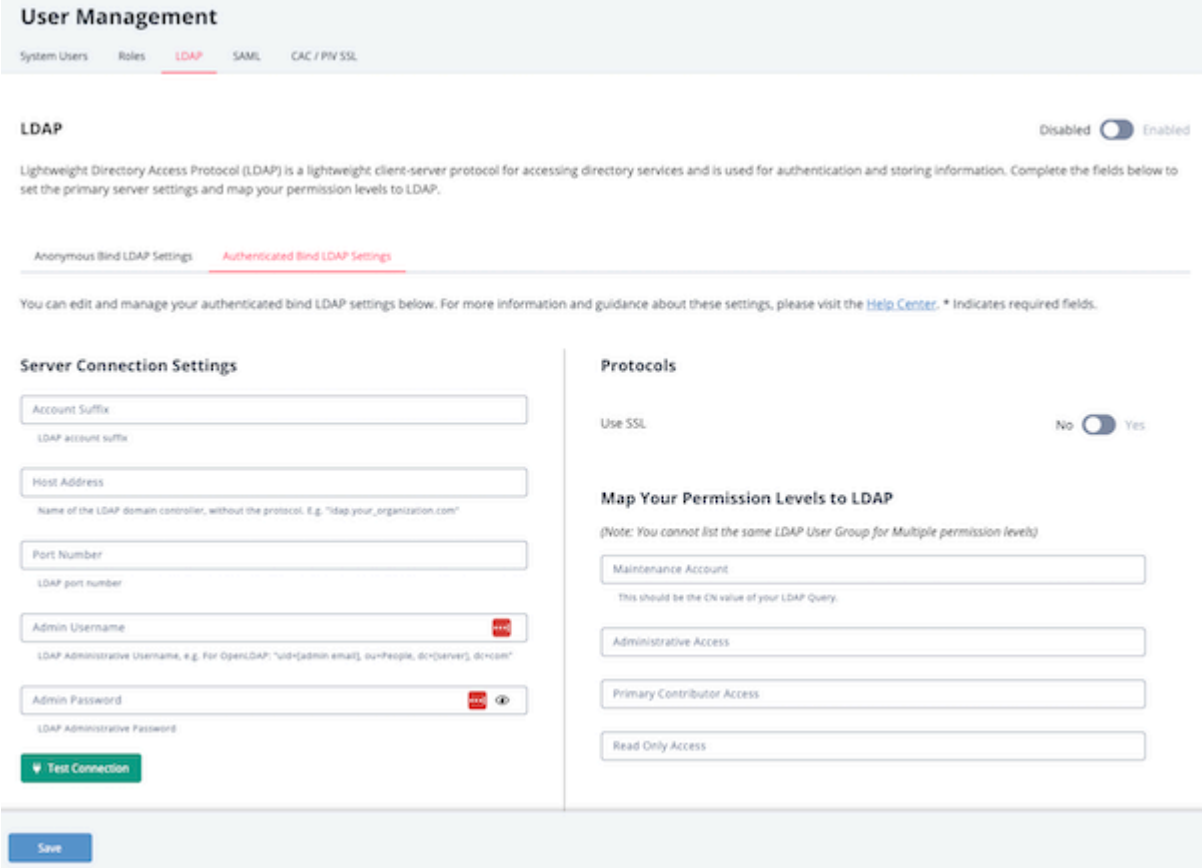
THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative or Maintenance
Custom Role - Action Permissions: Administrative Functions - Edit User Management

An authenticated bind LDAP is an LDAP connection in which a client provides valid credentials, such as a username and password, to authenticate against an LDAP directory service. Follow the steps below to configure your ThreatQ instance for an authenticated bind LDAP connection.

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

1. Navigate to Settings > User Management.
2. Click on the **LDAP** option and select the **Authenticated Bind LDAP Settings** tab.



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

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

4. After you populate the Server Connections Settings fields, click the **Test Connections** button to verify the settings are correct.
5. Complete the **LDAP Schema** section:

FIELD	DESCRIPTION
Base DN	The Base DN of the LDAP server connection. **Example:** DC=[server], DC="com"
DN Field Name	The field used to retrieve the DN or users and groups. This field should be **DN** for both OpenLDAP and Active Directory.
User Search Filter	The field to search for users. For **OpenLDAP**: objectClass=posIxAccount For **Active Directory**: objectClass=user
Group Search Filter	The field to search for grpups. For **OpenLDAP**: objectClass=posIxGroup For **Active Directory**: objectClass=group

FIELD	DESCRIPTION
Primary Group Name	The primary group name.
Group Member Field Name	This field is used to search for groups that a user belongs to. For **OpenLDAP**: cn For **Active Directory**: memberof
User ID Key Field Name	Field used to search for users based on email. For **OpenLDAP**: uid For **Active Directory**: sAMAccountName
User Group Member Key Field Name	Field used to search for groups that user belongs to. For **OpenLDAP**: memberUid For **Active Directory**: uid

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

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

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

   To ensure successful authentication, each LDAP user should belong to only one (1) LDAP user group. If this is not feasible, new LDAP groups should be created with mutually exclusive user membership.

   LDAP user groups require careful planning to avoid permission conflicts caused by overlapping group memberships. For example, when a user inherits read/write permissions from one group but is denied write access through another.

   It is recommended to implement a clear hierarchy of group memberships for each security device instance, with an administrative group at the top and a standard user group at the bottom. Multi-group membership should be avoided in favor of a least-privilege approach, and group nesting should be kept as shallow as possible.

   Permissions should be assigned through group membership rather than individual user roles to maintain consistency and simplify access

management.

You cannot save the configuration without entering a value in each field. For roles not mapped, you should enter a hyphen: `-`.

FIELD	DESCRIPTION
Maintenance Account	The LDAP account the ThreatQ Maintenance group will map to for permissions. **Open LDAP Example:** ldapSuper **Active Directory 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 **Active Directory 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 **Active Directory Example:** CN=linux-admins,CN=Builtin,DC=yourdomain,DC=com
Read-Only Access	The LDAP account the ThreatQ Read-Only group will map to for permissions. **Open LDAP Example:** ldapObserver **Active Directory Example:** CN=read-onlyCN=Builtin,DC=yourdomain,DC=com
<custom user role>	**Open LDAP Example:** ldapAnalystPlus **Active Directory Example:** CN=analystplus,CN=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

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative or Maintenance
Custom Role - Action Permissions: Administrative Functions - Edit User Management

If SSL Client Certificate Authentication is enabled, the SAML tab displays a warning message indicating that SSL Client Certificate Authentication/CAC must be disabled before you can enable SAML.

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.

SAML Support for Custom Roles

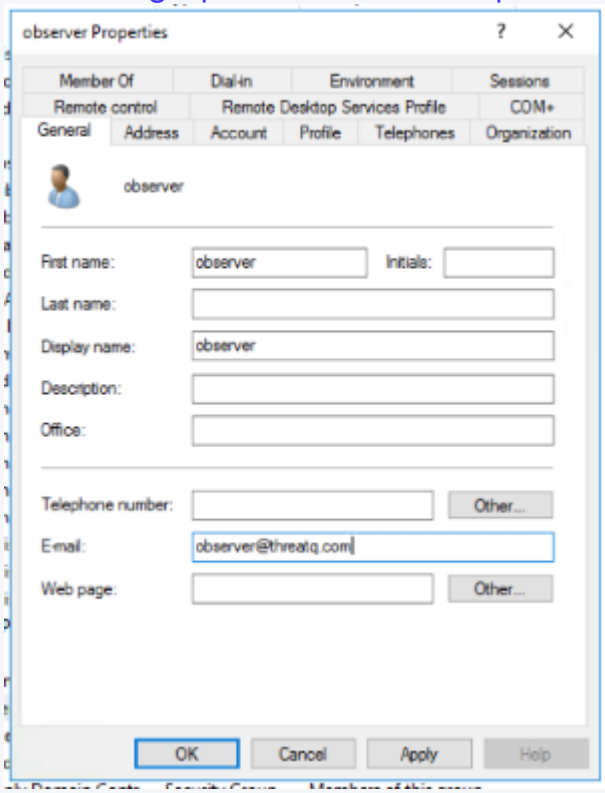
If SAML is enabled and you create a new custom role, ThreatQ sends the following notification to the Notifications menu:

- Additional SAML configurations are available due to the creation of a new role. Please map the *<role name>* role to a user group on the SAML settings page to complete setup.

Configuring SAML

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

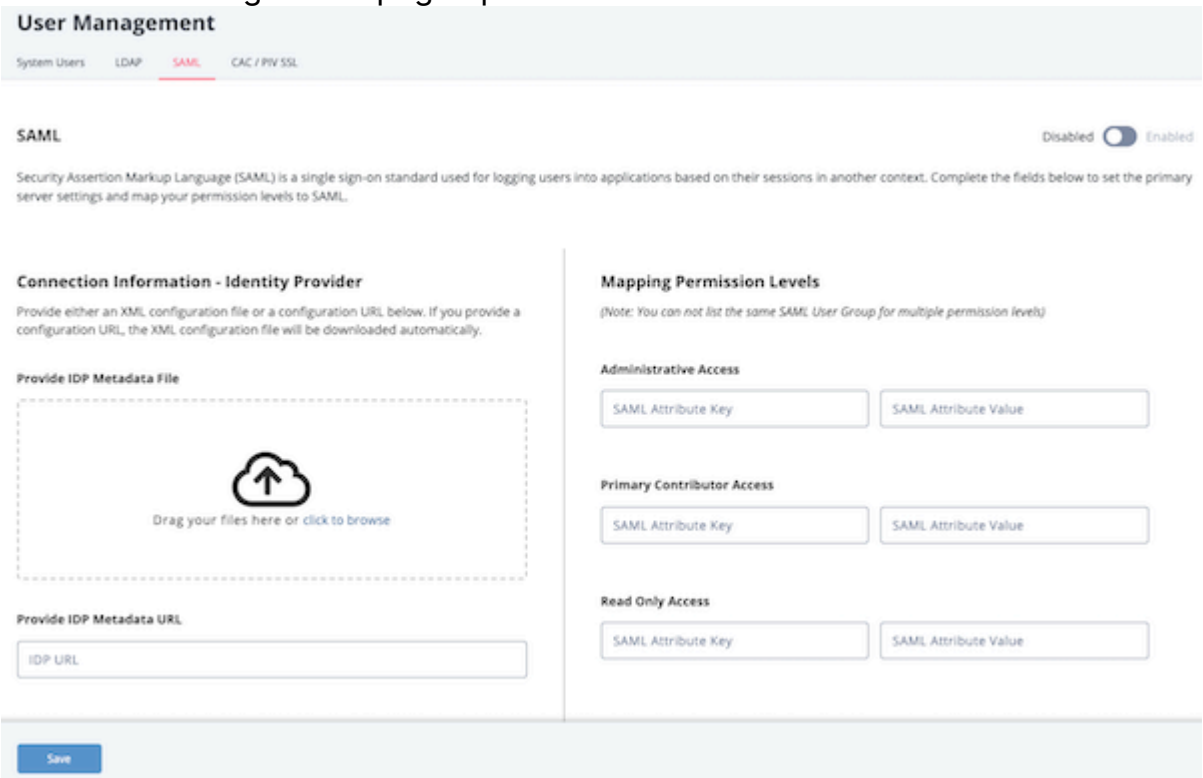
SAML users are required to add their email address to their user profiles in order to use the SSO. As part of the integration process, the ThreatQ platform expects that the user's email address has already been added to their IdP. See the Setting Up LDAP Users/Groups for SAML topic for more details.



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.

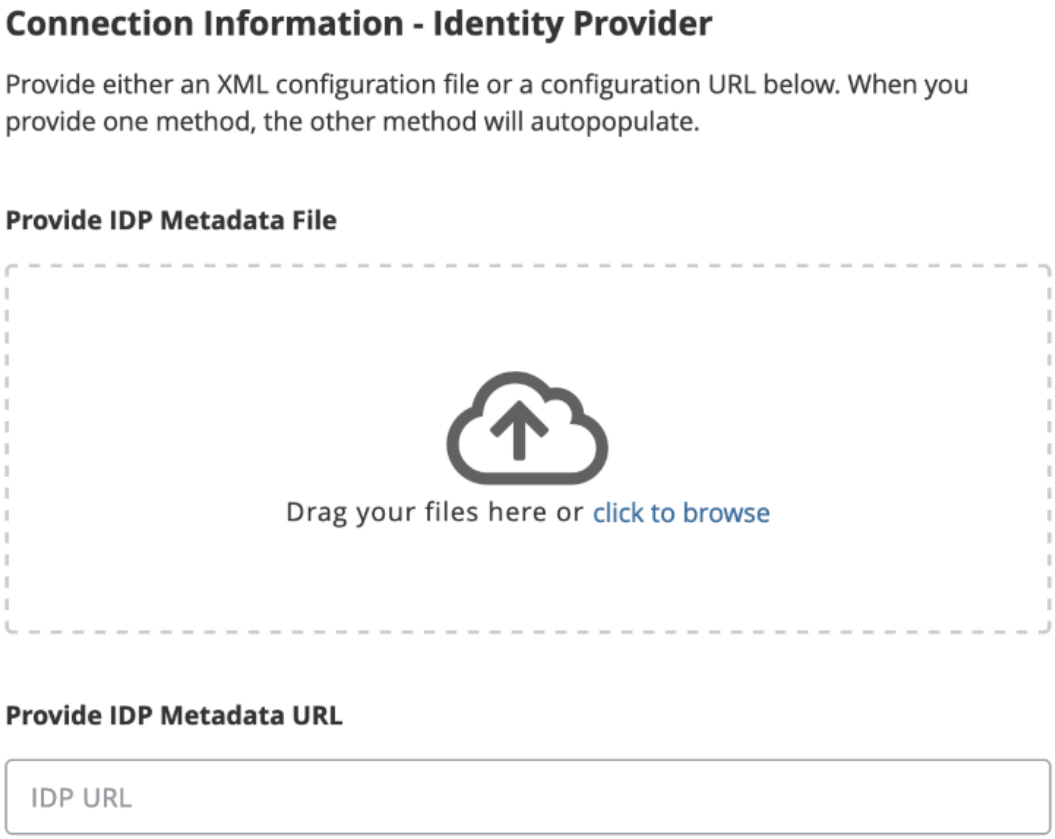
1. From the main menu, select Settings > User Management.
2. From the User Management page, click the **SAML** tab.

The SAML configuration page opens.



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

- Entering your IdP metadata file's URL in the **Provide IdP Metadata URL** field.



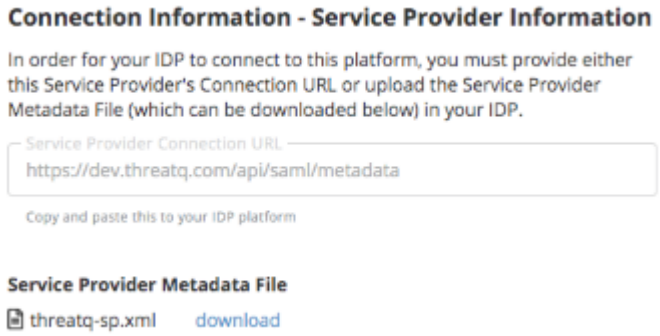
  Whichever method you choose to use will result in the auto-completion of the other field. **Example:** Uploading a metadata file will result in the IdP Metadata URL being populated with data parsed from the file.

4. The Connection Information - Service Provider Information section gives you two options for providing your ThreatQ platform metadata to you network administrator:
   - **Service Provider Connection URL** - Copy the URL listed in the Service Provider Connection URL field.
   - **Service Provider Metadata File** - After you save your SAML configuration, you can download a copy of the Service Provider Metadata file from the Connection Information - Service Provider Information section as shown in the **Example: After Saving Configuration** image below.

   The steps to add ThreatQ as a Service Provider may differ based on your environment - see the Adding ThreatQ as a Service Provider topic.

   Example: Before Saving Configuration

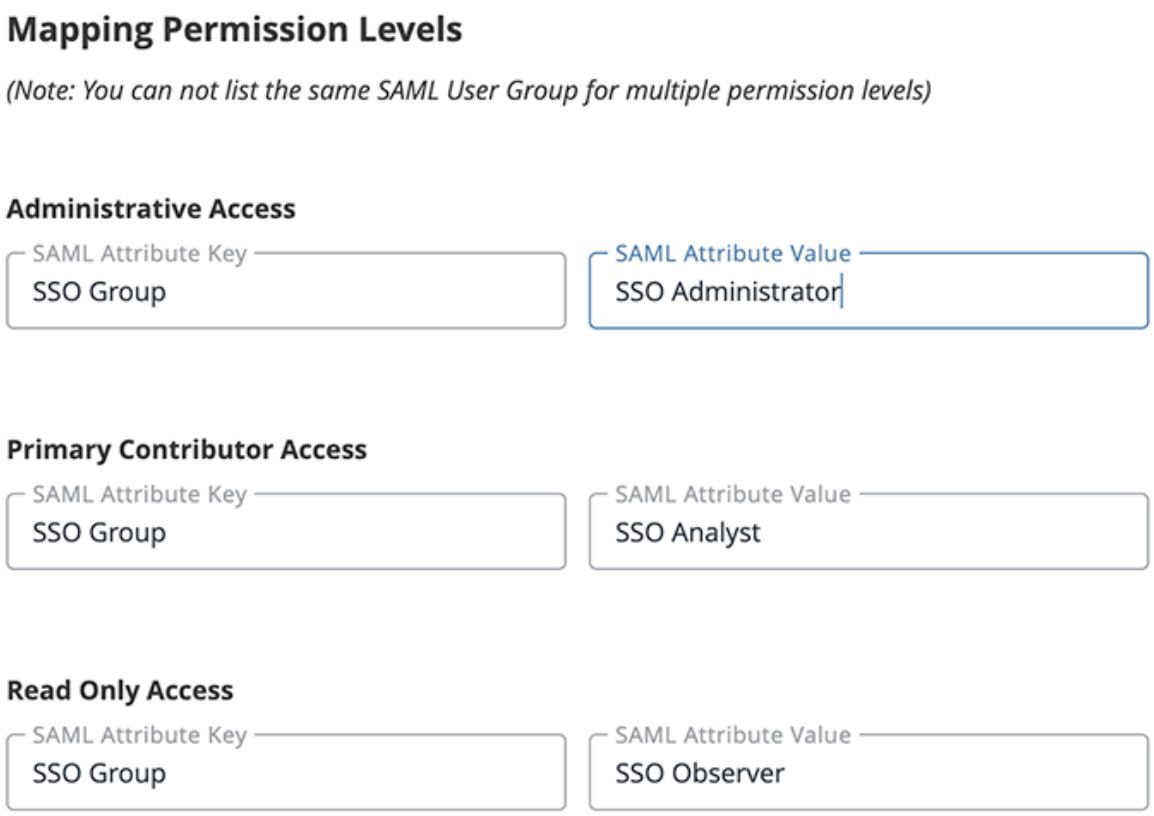
Example: After Saving Configuration



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.

     Your 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 or custom user role. See the Setting Up LDAP Users/Groups for SAML topic for information on how to setup

LDAP users and groups for SAML integration.



Mapping Notes:

- SAML cannot be used for Maintenance Accounts.
  - Local Maintenance Accounts cannot be mapped when enabling SAML.
  - If converting from LDAP authentication, LDAP groups that were mapped to the ThreatQ Maintenance role will have to be mapped to another user role.
- You cannot use the same SAML Key and Values for multiple roles.
- You do not have to map all ThreatQ roles but at least one role has to be mapped to use SAML. **Example:** Administrator and Primary Contributor will be mapped but the Read Only Access role will be blank.
- You must map every custom role before you can enable SAML.
- SAML accounts imported with the same user name and email as a local account will be converted.

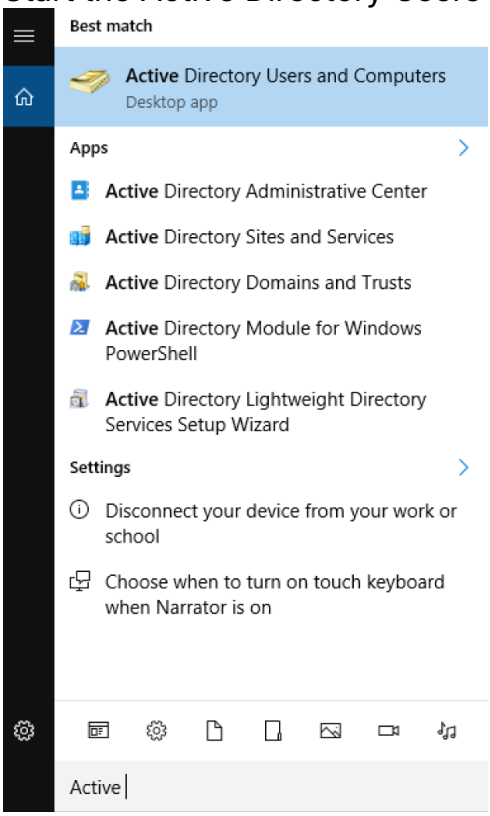
7. Click on **Save** located at the bottom of the page.
8. Confirm that your network administrator has completed Adding ThreatQ as a Service Provider before proceeding with the final steps listed below.

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.

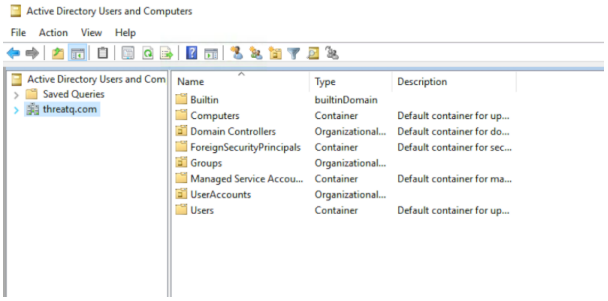
Setting Up LDAP Users/Groups for SAML

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

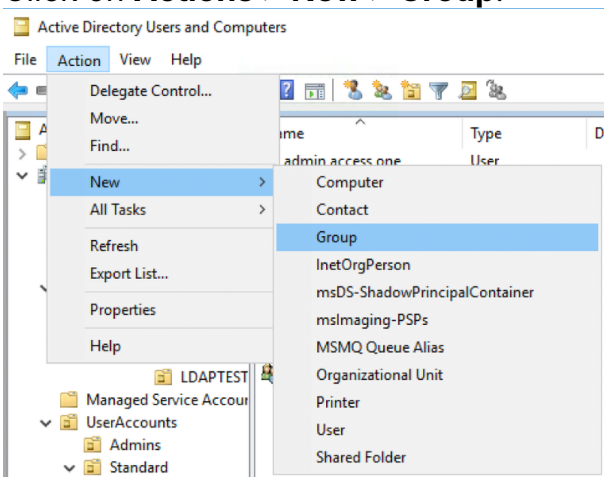
1. Log into the Windows Server.
2. Start the Active Directory Users and Computers application from the Start Menu.



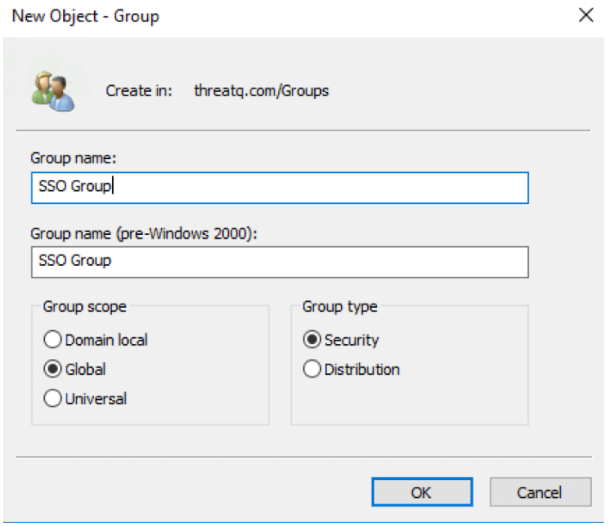
3. Navigate to and select the **Groups** folder under your LDAP domain.



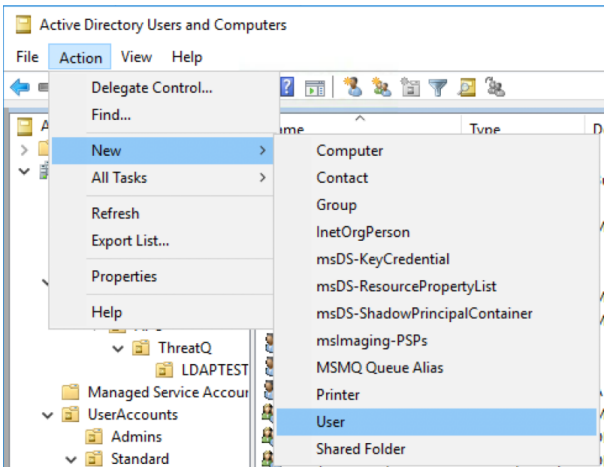
4. Click on **Actions > New > Group**.



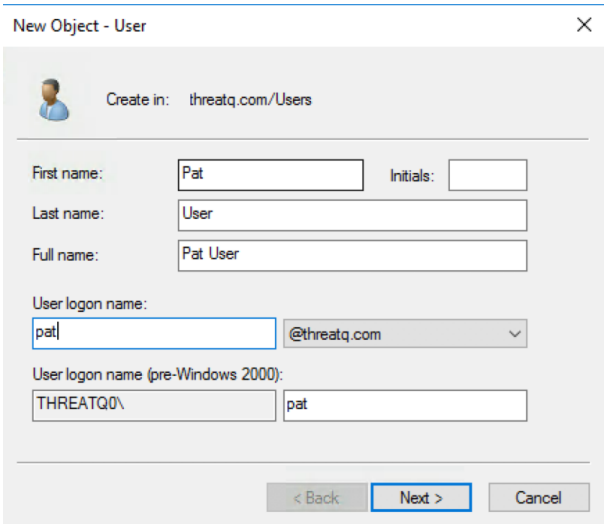
5. Enter in the **Group name** and click on **OK**.



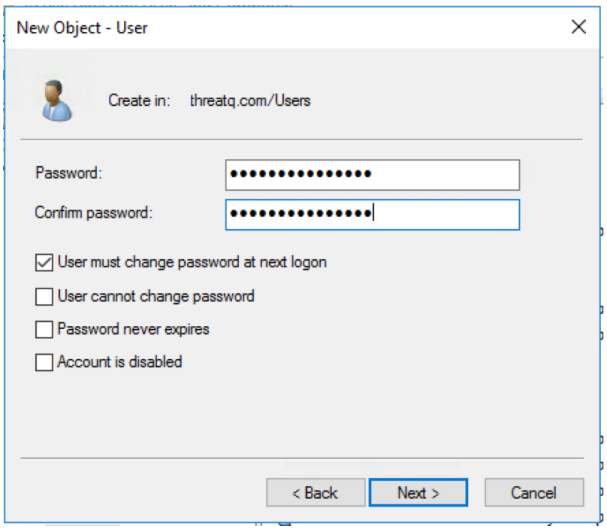
6. Select the **Users** folder and click on **Actions > New > User**.



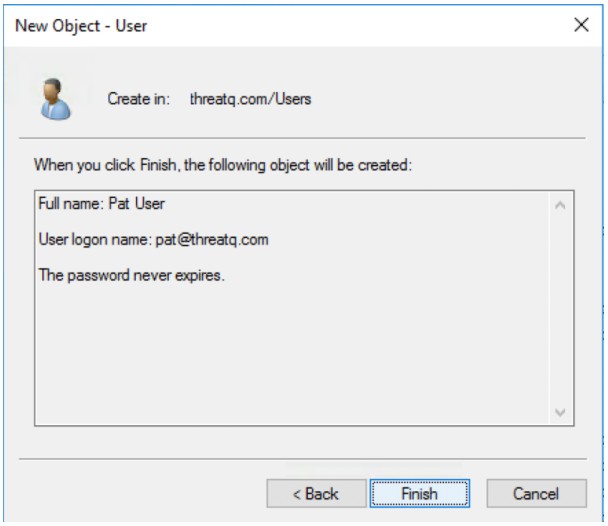
7. Enter in the **User Information** and click on **Next**.



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

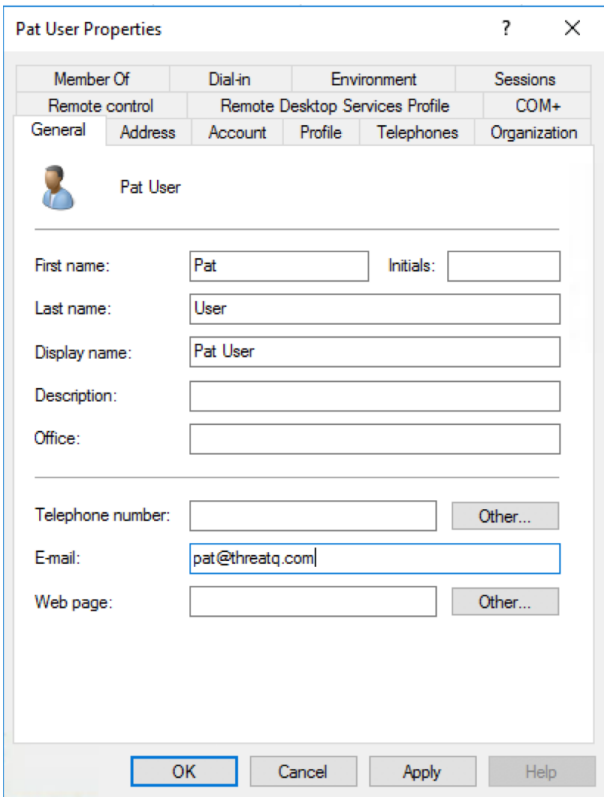


9. Confirm that the details are correct an then click on **Finish**.



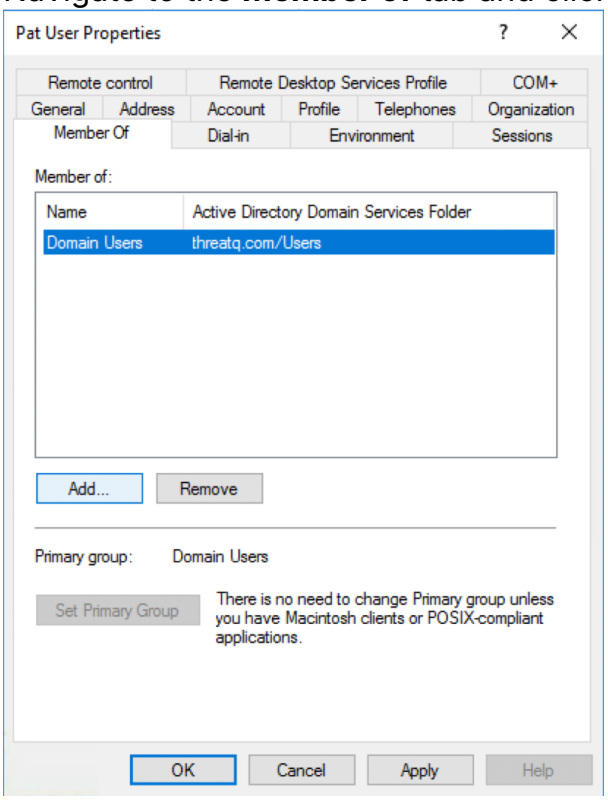
10. Find and double-click on the newly created user to edit the **User Properties**.

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

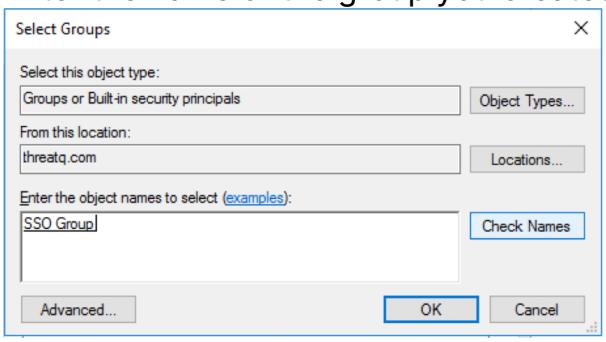


It is important that the E-mail field be filled in order for the SSO integration to work with this user.

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

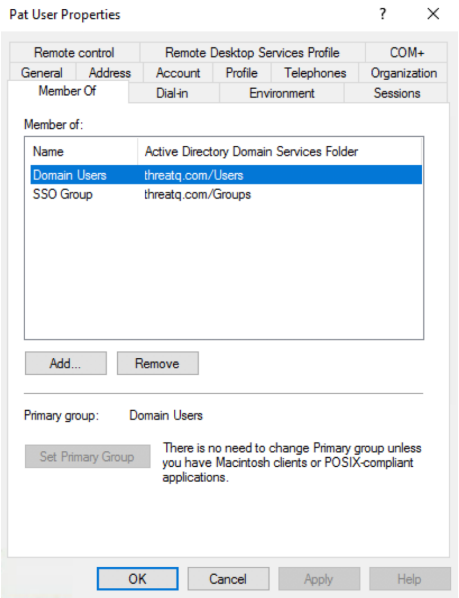


13. Enter the name of the group you created earlier in steps 4-5 in the field provided.



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

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



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

Adding ThreatQ as a Service Provider

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.

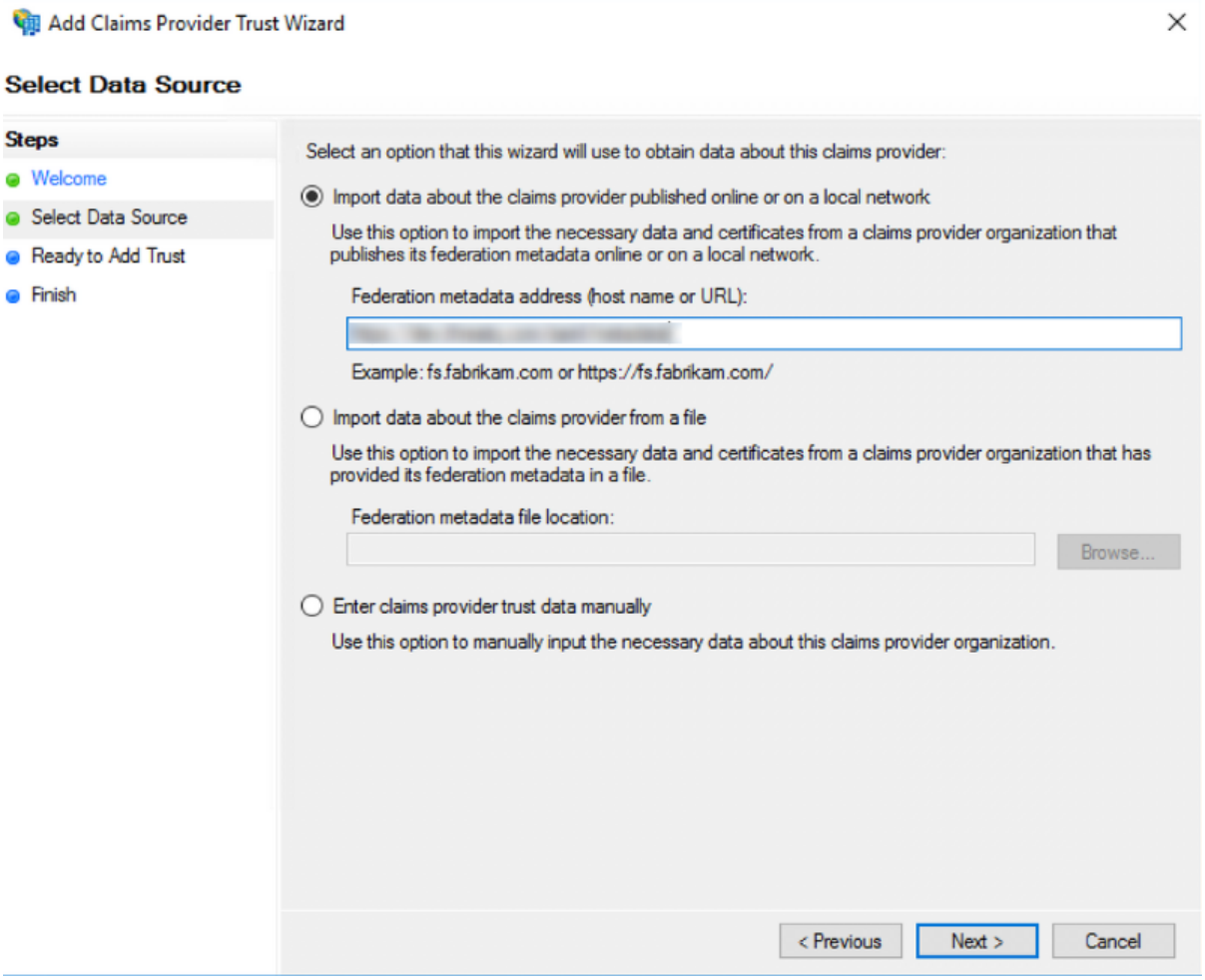
ADFS 2016

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.

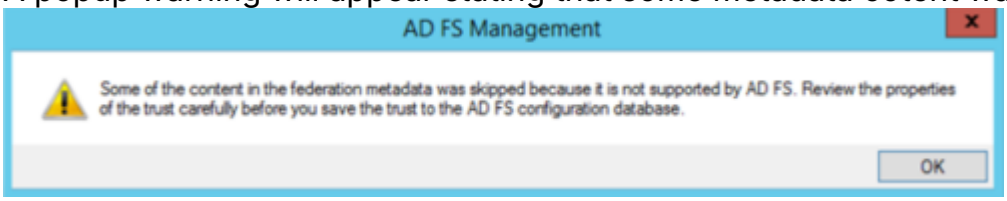


6. Confirm that the first radio option, **Import data about the claims provider published online...**, is selected.
7. Paste the **Platform Connection URL** located on the ThreatQ SAML page, step 4 on the Configuring SAML topic, into the Federation Metadata Address field in the following format:

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

8. Click **Next**.

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



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

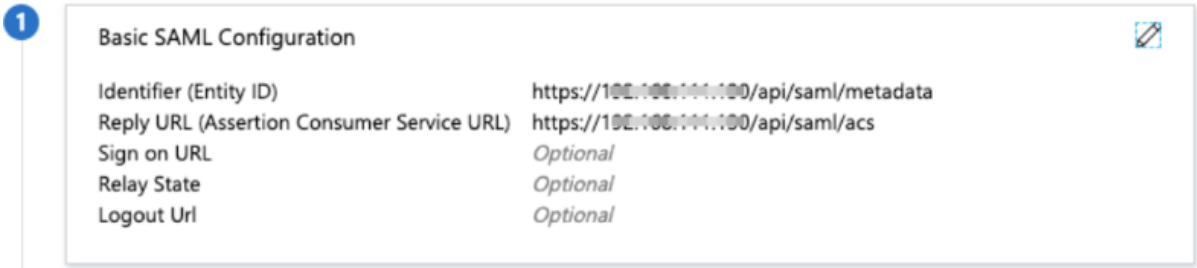
35. Select the **Pass through all claim value** radio option.
36. Click on **OK** to create the rule.
37. Click **OK** to close the Issuance Transform Rules dialog box.

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:

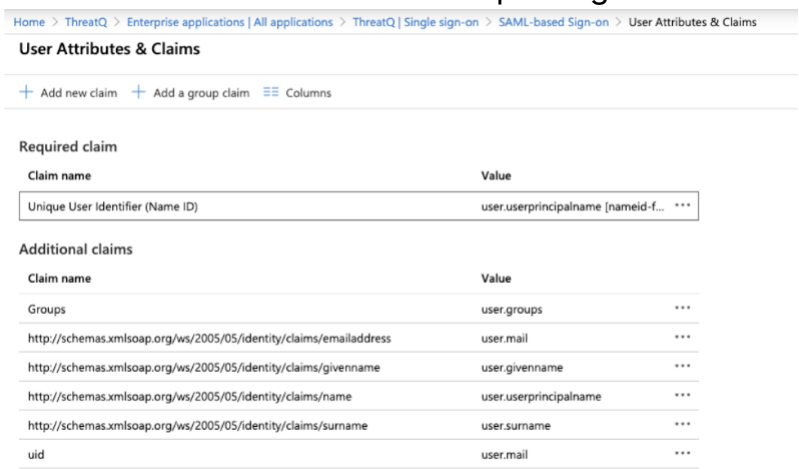


FIELD	VALUE	DESCRIPTION
ACS / Single Sign on URL	https://threatq.example.com/api/saml/acs	Assertion Consumer Service (ACS) is the ThreatQ URL + appended the “/api/saml/acs” string.
SP Entity ID	https://threatq.example.com/api/saml/metadata	This is the ThreatQ entity ID which is the ThreatQ URL + appended 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`.

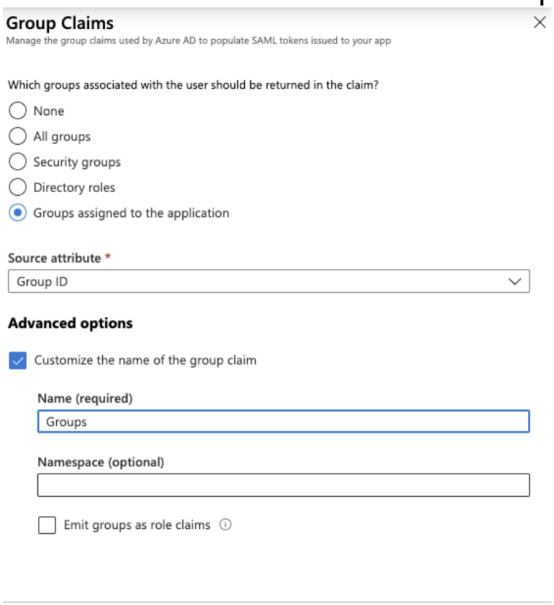
Both the username and uid attributes are **required** and must be mapped to the user's Email address.

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.



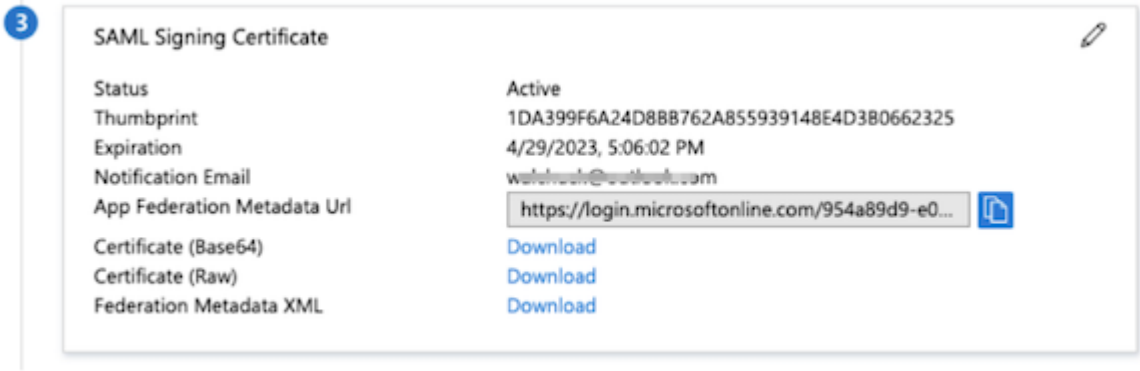
When adding a group claim it is recommended to customize name as this is what is required to be entered on the ThreatQ side as the SAML Attribute Key. This should not contain a namespace otherwise the full claim name will need to be entered - see http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname

for more information. See the example below:



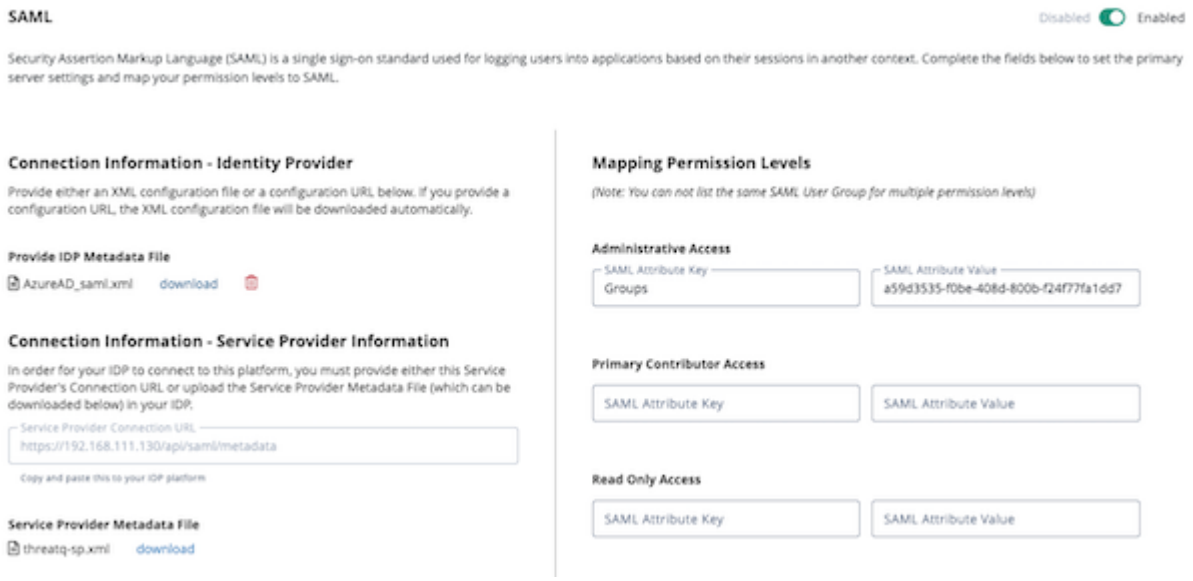
> In the example above, **Groups** would be entered as the Attribute Key in ThreatQ. The Attribute Value would be one of the Group IDs (Group Object ID) assigned to the application in Step 9.

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



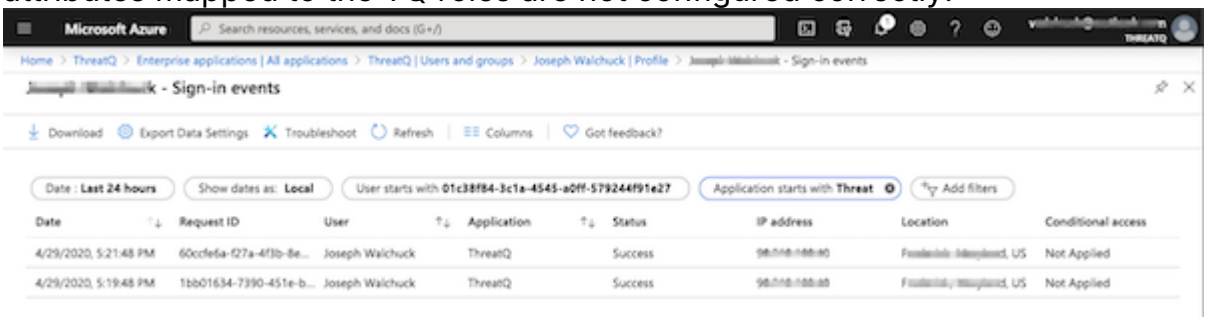
14. After you complete the Configuring SAML process, add the SAML Attribute Key and SAML Attribute Value for each ThreatQ user role to the Mapping Permissions section.
    In the example below, we mapped an Azure AD Group to the Administrative

Access using the group's Object ID as the SAML attribute value.



> 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.



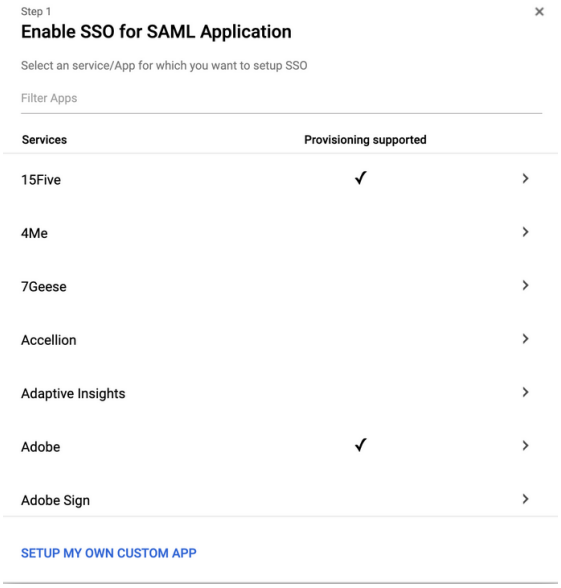
Google G Suite

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

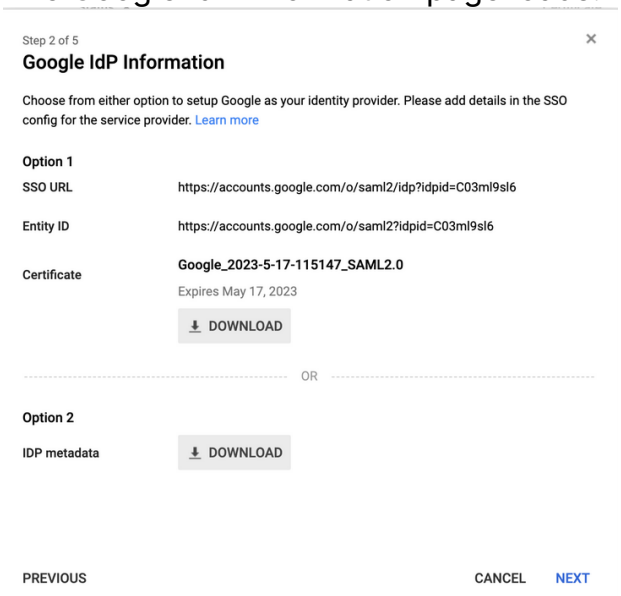
Setting Up the SAML App

1. Log into your **Google Administrative Console**.
2. Navigate to **Apps > SAML Apps**.

3. Click on the **+** icon located at the bottom-right on the page.
4. Select the **Setup my own custom app** option.



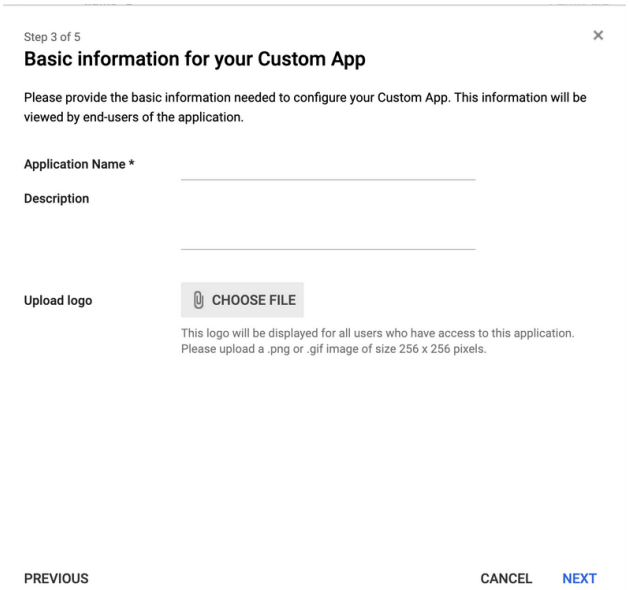
The Google IdP information page loads.



5. Click on **Next**.
6. Complete the *Basic Information for Your Custom App* fields:

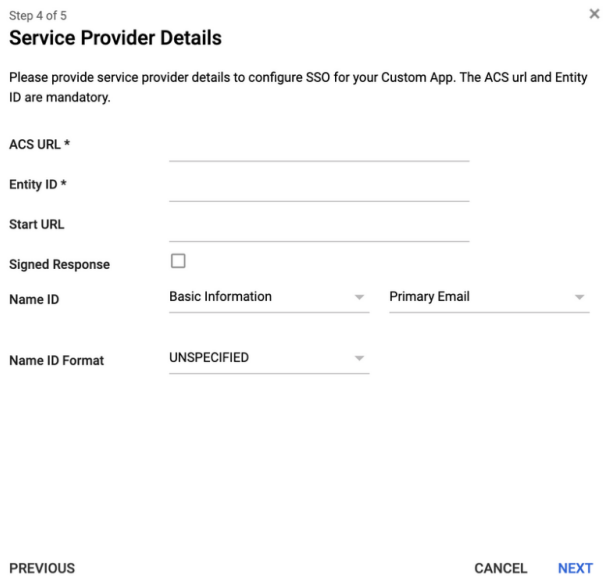
>FIELD	DESCRIPTION	EXAMPLE
Application Name	The name of the application.	ThreatQ

>FIELD	DESCRIPTION	EXAMPLE
Description	What function the app will serve.	SSO for ThreatQ Platform



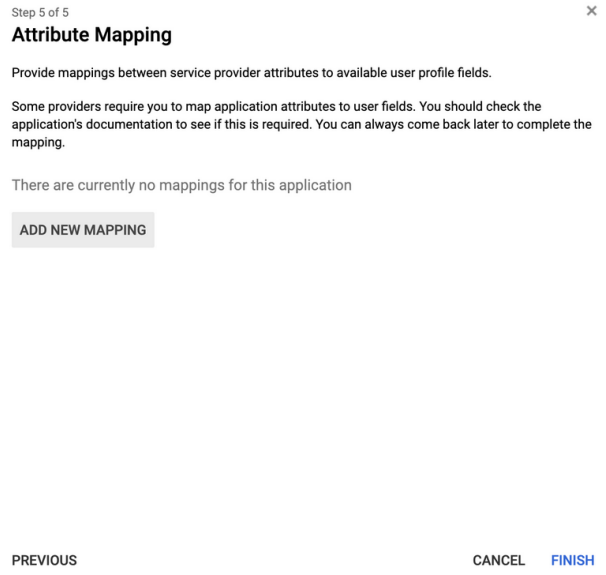
7. Click on **Next**.
8. Complete the *Service Provider Details* fields:

FIELD	DESCRIPTION	EXAMPLE
ACS URL	Assertion Consumer Service is your ThreatQ URL + appended the "/api/saml/acs" string.	https://threatq.example.com/api/saml/acs
Entity ID	The Entity ID is your ThreatQ URL + appended with the "/api/saml/metadata" string.	https://threatq.example.com/api/saml/metadata
Name ID Format	Set this field to **Email**.	N/A



9. Click on **Next**.

   The Attribute Mapping page loads.



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

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

11. Create the **email** mapping:

ATTRIBUTE	TYPE	GOOGLE DATA FIELD
email	Basic Information	Primary Email

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

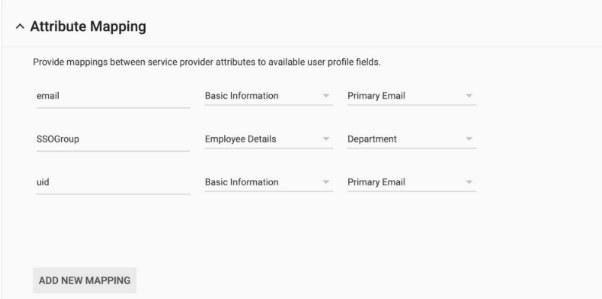
ATTRIBUTE	TYPE	GOOGLE DATA FIELD
uid	Basic Information	Primary Email

14. Click on **Add New Mapping**:
15. Create the **SSOGroup** mapping for ThreatQ roles:

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

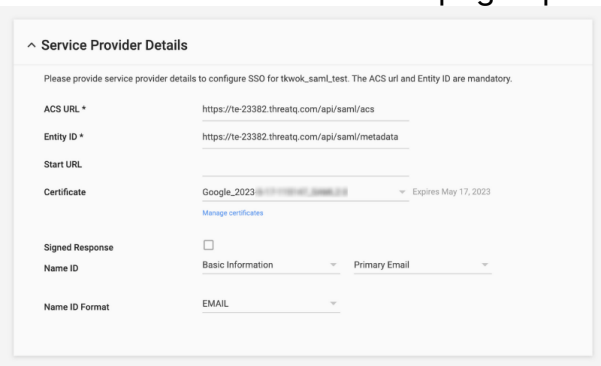
> Any attribute can be used for this mapping other than **Employee ID**. See the Creating custom attributes using the user schema Google support article for instructions on creating custom attributes to use for role mapping.

16. Your setup should now resemble the following screenshot:



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

The Service Provider Details page opens.



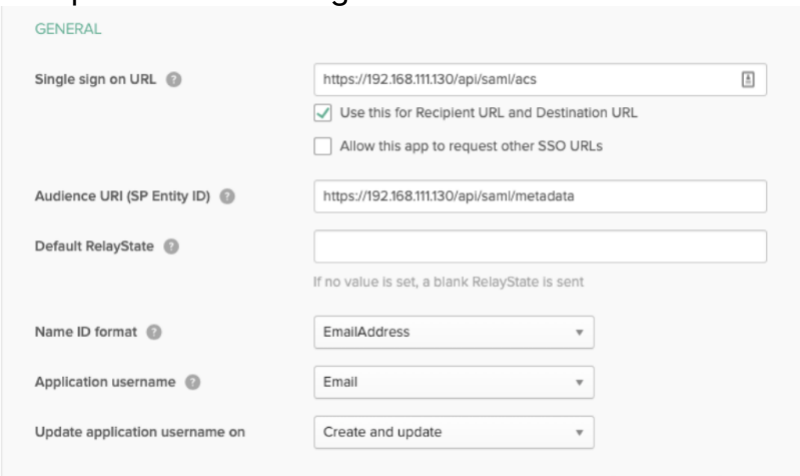
21. Click on **Manage Certificates**.
22. Download the **certificate** and the **IdP Metadata** files that are required in steps 4 and 5 in the *Configuring SAML* section in the About SAML Authentication topic.

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.

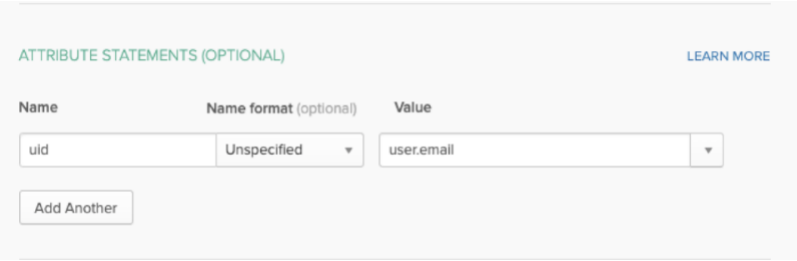
1. Log into the Okta web application.
2. Click on the **Admin** button located to the top-right of the screen.
   The Dashboard page loads.
3. Click on the **Applications** tab.
   The Application page loads.
4. Click on **Add Application**.
5. The Add Applications page loads.
6. Click on **Create New 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:



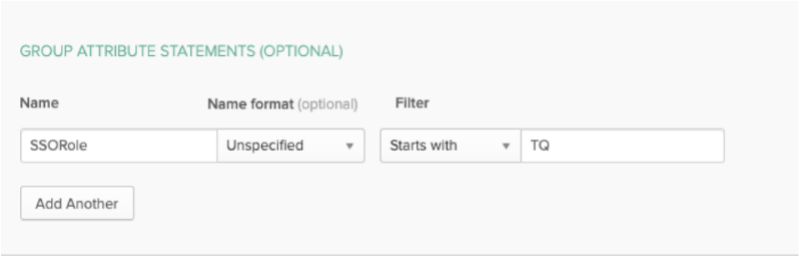
FIELD	ENTRY/SELECTION	NOTES
Single sign on URL	https://< Host-name >.com/api/saml/acs	The Assertion Consumer Service (ACS) is your ThreatQ URL + appended the "/api/saml/acs" string.
Audience URI (SP Entity ID)	https://< Host-name >/api/saml/metadata	The Audience URI is your ThreatQ URL + appended with 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:



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 REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative or Maintenance
Custom Role - Action Permissions: Administrative Functions - Edit User Management

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 6x
- PEM-encoded, X.509 CA certificate file
- CAC, PIV card, Smart card, or SSL client certificate
- Administrative or maintenance login
- List of your current TQAdmin configuration settings

Configuring SSL Client Certificate Authentication

1. Move your CA certificate file to a directory on your ThreatQ instance.
2. Access the ThreatQ host command line via SSH or console.
3. Run the following command:

```
sudo /usr/local/bin/tqadmin configure
```

The TQadmin configure command displays a series of prompts.

> To prevent undesired changes to your system, you must enter a response for each prompt based on your current system configuration. For example, if your organization uses ThreatQ Data Exchange's OpenDXL functionality you must enter "yes" for the **Do you want to enable OpenDXL** prompt.

4. To enable SSL Client Certification, populate the following:

PROMPT	DESCRIPTION
Do you want to enable CAC/mTLS? (yes/no):	Enter yes.
Enter the file path for your certificate:	Enter the path for your CA Certificate. **example:** /tmp/mycert.pem
Enter the FQDN of the server:	Enter the FQDN of the server. **example**: myserver.threatq.com

5. When prompted, enter your YUM username and password.
6. Run the following command to save and apply your changes:

```
sudo /usr/local/bin/tqadmin reapply
```

7. After your changes are saved, the CAC/PV SSL tab in the User Management page displays a status of Currently Enabled.
8. 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.
9. 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.

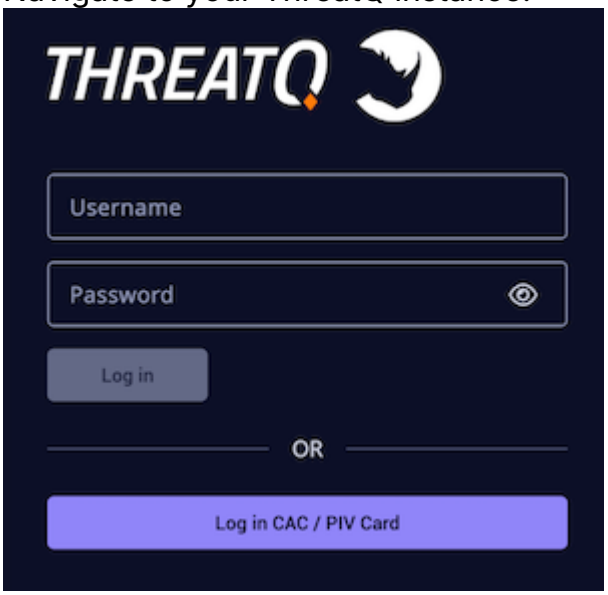
Adding a User's Certificate Fingerprint - User Profile

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.
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

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative or Maintenance
Custom Role - Action Permissions: Administrative Functions - Edit User Management

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.

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. Access the ThreatQ host command line via SSH or console.
2. Run the following command:

   ```
   sudo /usr/local/bin/tqadmin configure
   ```

   The TQadmin configure command displays a series of prompts.
3. To disable SSL Client Certification, populate the following:

PROMPT	DESCRIPTION
Do you want to enable CAC/mTLS? (yes/no):	Enter no.

4. When prompted, enter your YUM username and password.
5. Run the following command to save and apply your changes:

   ```
   sudo /usr/local/bin/tqadmin reapply
   ```

6. After your changes are saved, the CAC/PV SSL tab in the User Management page displays a status of Currently Disabled.

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.

The process for replacing a CA certificate is the same as the process for Configuring SSL Client Certificate Authentication.

Managing Certificate Fingerprints

THREATQ REQUIRED PERMISSIONS

Default ThreatQ Role: Administrative or Maintenance
Custom Role - Action Permissions: Administrative Functions - Edit User Management

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.

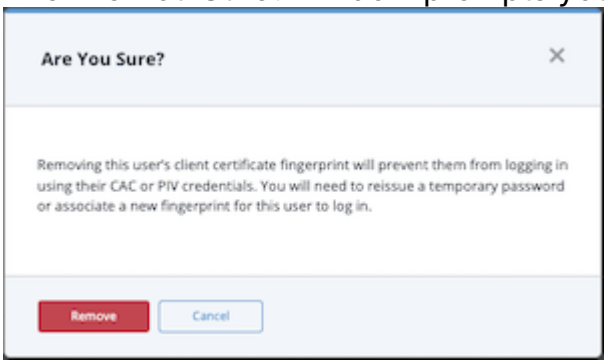
Updating Certificate Fingerprints

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 date prior to the current date.	Upload a certificate file with an expiration date after than the current date.

A

Adversaries 399, 401, 400

Audit Log 715

Authentication 35, 36

Automatic Expiration 193

B

Bulk Actions 662, 665, 675, 668, 674, 671, 677

C

Command Line Interface 120

Commands 122

D

Dashboard (default) 139, 137, 140, 139

Dashboards (custom) 143, 189, 165, 189, 181

Data Collections 647, 657, 648, 658

Data Controls 191

E

Events 424, 428, 427

Expiration 194, 671, 489, 195, 488, 196, 194, 488

Exports 227, 231, 232, 231, 232, 226, 233, 254, 271

F

Feed Health Notifications 317, 324

Files 442, 446, 445

Filter Sets 602, 640, 607, 612, 630, 641, 636, 615, 631, 642, 632, 619, 617, 643, 621, 634, 638, 623, 612

I

Indicator Defanging 486

Indicator Scoring 686

Indicator Status 491, 491, 327

Indicators 460, 462, 462, 464, 161

J

Job Management 307

L

Licensing 311, 311

Logging In 39, 40

N

Navigation 312

Notifications 315

O

Object Details 692, 689, 693, 710, 697, 708, 701

Object Management 326

P

Proxy 373

R

Reports 358, 357, 357, 357, 358

S

SAML 804, 817

Scoring 686

Scoring Algorithms 206

Search Filters 607, 630, 638, 639, 640, 646

Search Results 657, 649, 648

Searches 602

Signatures 517

STIX 521, 522, 525, 539, 565

T

Tasks 570, 573

Threat Library 589

ThreatQ Backup/Restore 116

Traffic Light Protocol (TLP) 214, 212, 212, 214

U

User Accounts 756, 0, 757, 759, 758, 758

User Roles 761, 761, 762, 763

W

Whitelisting 216