

ThreatQuotient



ThreatQ Chrome Extension Guide

Version 1.0.0

April 09, 2021

ThreatQuotient

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



Support

Email: support@threatq.com

Web: support.threatq.com

Phone: 703.574.9893

Warning and Disclaimer

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

Copyright © 2021 ThreatQuotient, Inc.

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

Contents

Versioning.....	4
Introduction.....	5
Installation	6
Configuration.....	7
Connection Options	7
General Options.....	9
Usage.....	11
Entry Points	11
Tabs & Layout	12
Analyze.....	12
Notepad	13
Jobs.....	14
Config.....	14
Browser Context Menu Actions	15
No Text Selection.....	15
Text Selected	16
Bulk Actions	17
Analyze Bulk Actions	17
Page Actions.....	17
Indicator Actions.....	18
Table Actions.....	18
Notepad Bulk Actions.....	19
Object Actions	19
Investigation Actions	20
Table Actions.....	20
Filtering	21
Troubleshooting / FAQ	22
Uninstalling the Extension	23
Change Log	24

Versioning

- Minimum ThreatQ Version: v4.25.0
- Minimum ThreatQ User Account Role: Primary Contributor
- Minimum Google Chrome Version: v87.x.x
- Supported Browsers:

BROWSER	SUPPORTED
Google Chrome	✓
Brave	N/A
Firefox	×
Safari	×
Opera	×

Introduction

The ThreatQ Chrome Extension enables analysts to actively interact with ThreatQ while browsing other websites and tools within Google Chrome. The extension provides users with the ability to perform lookups against ThreatQ, interact with their investigations, as well as add context back to their ThreatQ instance.

Installation

1. Navigate to the Chrome Web Store and search for ThreatQ.



You can also navigate directly to the entry using the following link:

<https://chrome.google.com/webstore/detail/threatq-extension/kaoghaifdcjeaabfdbggomcpdgdgfdjlm>

2. Click on the **ThreatQ Extension** listing if you used the Chrome Web Store search method. Otherwise, skip to step 3.
3. Click on the **Add to Chrome** button.

The extension will now be installed on your browser. You will still need to configure the extension.

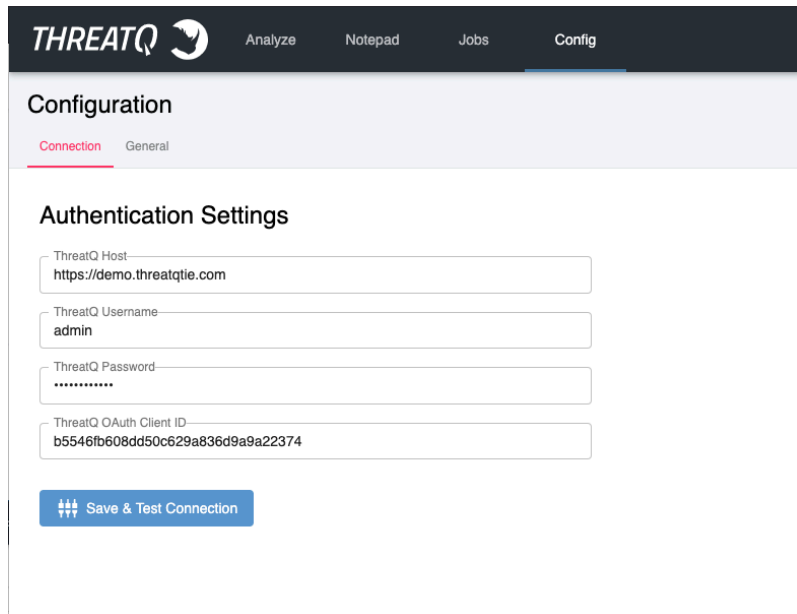
Configuration

Use the following steps to configure the ThreatQ Chrome Extension. You will first need to pin the extension to your browser's toolbar. Once the extension has been pinned, you will be able to access the extension's UI by clicking on the ThreatQ rhino icon.

Connection Options

1. Once the extension popup is open, click on the Config tab.
2. In the Connection tab, you will configure your Authentication Settings:

PARAMETER	DETAILS
ThreatQ Host	Enter your ThreatQ host (schema optional). Do not provide any URL paths.
ThreatQ Username	Enter the username for the account you want to use with the extension. To authenticate and act on behalf of the user when executing actions against ThreatQ.
ThreatQ Password	Enter the password associated with the above user account.
ThreatQ OAuth Client ID	Enter your API Credentials found in your user profile within ThreatQ.



The screenshot shows the ThreatQ Configuration page with the 'Connection' tab selected. The 'Authentication Settings' section contains four input fields: 'ThreatQ Host' with the value 'https://demo.threatqtie.com', 'ThreatQ Username' with the value 'admin', 'ThreatQ Password' with masked characters, and 'ThreatQ OAuth Client ID' with the value 'b5546fb608dd50c629a836d9a9a22374'. A blue button labeled 'Save & Test Connection' is at the bottom.

- Once you have entered your credentials, click on the Save & Test Connection button. If everything connects, you will see a green popup message saying you have successfully authenticated with your ThreatQ instance.


Save & Test Connection ✓

Successfully authenticated with ThreatQ! ✕

General Options

1. Click on the Config tab and then select General.
2. In the General tab, you will configure your General Settings:

PARAMETER	DETAILS
Background Scanning	Enabling this will allow the extension to scan your current browser page for indicators. This also allows the extension to highlight indicators on the page. Note, no data will be sent to ThreatQ or anywhere over the internet. The indicator parsing all happens locally, within the extension.
Default Indicator Status	The status to give indicators that are quickly added via the Chrome Extension.
Default Whitelist Status	You can set a custom Whitelist status for indicators that you mark Whitelisted. This can be used if your ThreatQ workflow includes a different status class for Whitelisted indicators.
Investigation Name	This is the name of the investigation that you can sync with your Notepad. If the investigation does not already exist, you will be prompted to create it when you choose to sync your notepad with the investigation.

THREATQ 

AnalyzeNotepadJobsConfig

Configuration

ConnectionGeneral

General Settings

☒ Background Scanning

Enabling this will allow the extension to scan your current browser page for indicators. This also allows the extension to highlight indicators on the page.

Default Indicator Status

Review

Default Whitelist Status

Whitelisted

Investigation Name

Internal Trickbot Sighting - In Progress

Usage

This section will provide you with details on how you can use the ThreatQ Chrome Extension.

Entry Points

Once the ThreatQ Chrome Extension is installed, there are a few entry points to using the extension. Below are the entry points, along with a brief description.

Extensions Toolbar Popup

The extension can be accessed via your Chrome browser's toolbar, to the right of your URL bar. If you do not see a ThreatQ icon, you may need to click the puzzle piece icon and pin the ThreatQ Extension.

Right Click (no selection)

You'll also notice that when you right click a webpage, you now have a new context menu entry for ThreatQ. If nothing is selected when you make the right-click action, you will be given the ThreatQ context menu options to highlight indicators and/or open your configured ThreatQ instance.

Right Click (with selection)

The right-click actions are a bit different if you have actual text selected by your cursor. If text is selected, you will be able to perform actions such as lookup in ThreatQ, as well as import into ThreatQ.

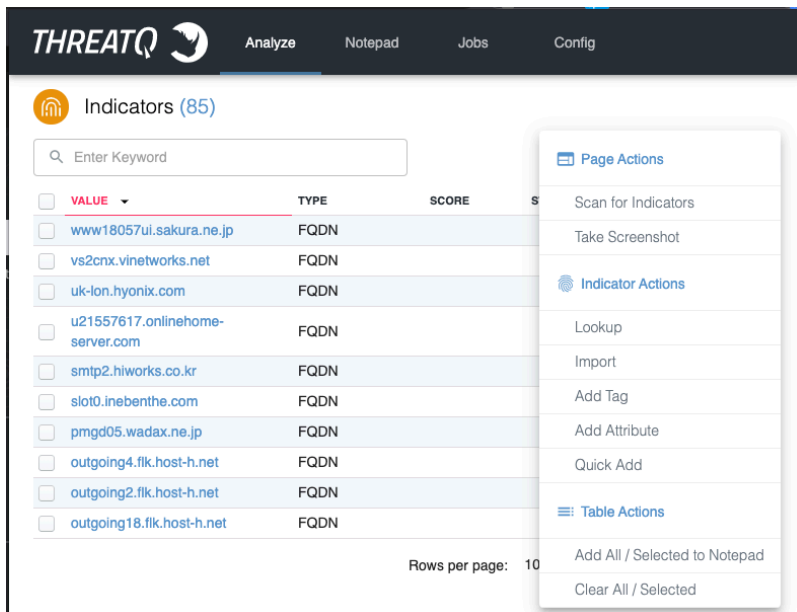
Tabs & Layout

There are four main tabs in the extension:

- [Analyze](#)
- [Notepad](#)
- [Jobs](#)
- [Config](#)

Analyze

The Analyze tab will reflect your *current* browser tab, and the data in it only persists while you stay in the same browser tab. When you change browser tabs, the data in the extension's Analyze tab will get reset. If you have Background Scanning enabled, when you change tabs, the extension will automatically scan the webpage for indicators, and present them in the Ana1yze tab to be interacted with. On this page, you will be able to add context back to ThreatQ, perform lookups, or add an indicator to your Notepad.

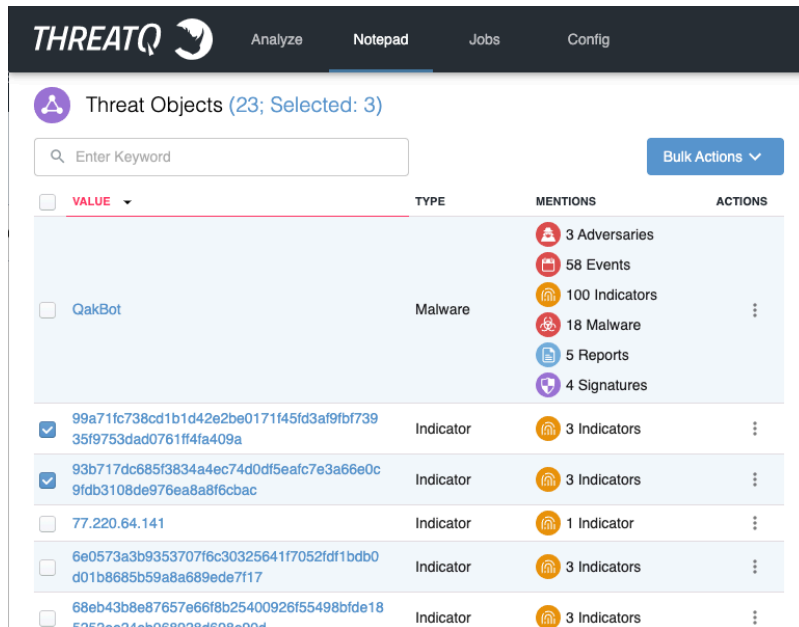


The screenshot displays the ThreatQ Analyze tab interface. At the top, there's a navigation bar with tabs: Analyze, Notepad, Jobs, and Config. Below the navigation bar, the main content area shows a table of indicators. The table has columns for VALUE, TYPE, SCORE, and S. A dropdown menu is open over the table, showing Page Actions (Scan for Indicators, Take Screenshot) and Indicator Actions (Lookup, Import, Add Tag, Add Attribute, Quick Add). Table Actions (Add All / Selected to Notepad, Clear All / Selected) are also visible. The table lists several FQDN indicators like www18057ui.sakura.ne.jp, vs2cnx.vinetworks.net, etc.

VALUE	TYPE	SCORE	S
www18057ui.sakura.ne.jp	FQDN		
vs2cnx.vinetworks.net	FQDN		
uk-lon.hyonix.com	FQDN		
u21557617.onlinehome-server.com	FQDN		
smtp2.hiworks.co.kr	FQDN		
slot0.inebenthe.com	FQDN		
pmgd05.wadax.ne.jp	FQDN		
outgoing4.flk.host-h.net	FQDN		
outgoing2.flk.host-h.net	FQDN		
outgoing18.flk.host-h.net	FQDN		

Notepad

The Notepad tab is a cache and storage for indicators and other entities that you have curated and saved, to be investigated. To add an indicator or entity to this extension tab, either use the extension's right-click actions or the Bulk Actions in the AnaLyze tab. Once data is in your notepad, it will persist even when you close your browser. From this tab, you can sync data with your investigations, find mentions using the ThreatQ Threat Library, add relationships, add attributes, and more.

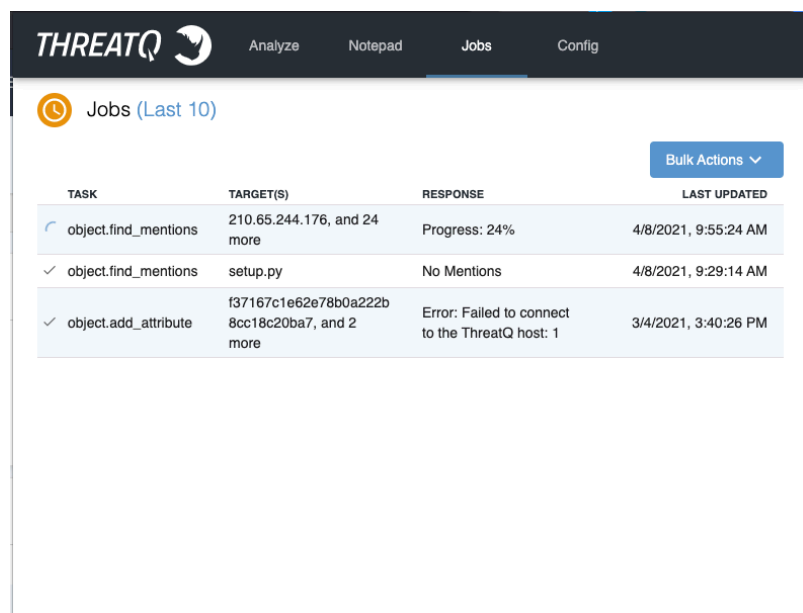


The screenshot displays the ThreatQ Notepad interface. At the top, there is a navigation bar with tabs for 'Analyze', 'Notepad', 'Jobs', and 'Config'. Below the navigation bar, the 'Threat Objects' section shows a count of 23 objects, with 3 selected. A search bar labeled 'Enter Keyword' and a 'Bulk Actions' dropdown menu are present. The main content area is a table with columns: VALUE, TYPE, MENTIONS, and ACTIONS. The table lists several threat objects, including 'QakBot' (Malware) and several indicators (Indicator). The 'MENTIONS' column shows counts for various entities like Adversaries, Events, Indicators, Malware, Reports, and Signatures.


VALUE	TYPE	MENTIONS	ACTIONS
<input type="checkbox"/> QakBot	Malware	3 Adversaries 58 Events 100 Indicators 18 Malware 5 Reports 4 Signatures	⋮
<input checked="" type="checkbox"/> 99a71fc738cd1b1d42e2be0171145d3af9bf73935f9753dad0761ff4fa409a	Indicator	3 Indicators	⋮
<input checked="" type="checkbox"/> 93b717dc685f3834a4ec74d0df5eafc7e3a66e0c9fdb3108de976ea8a8f6cbac	Indicator	3 Indicators	⋮
<input type="checkbox"/> 77.220.64.141	Indicator	1 Indicator	⋮
<input type="checkbox"/> 6e0573a3b9353707f6c30325641f7052df1bdb0d01b8685b59a8a689ede7117	Indicator	3 Indicators	⋮
<input type="checkbox"/> 68eb43b8e87657e66f8b25400926f55498bde185252ee24eb068828d689e90d	Indicator	3 Indicators	⋮

Jobs

The Jobs tab will show any background tasks that are being executed, in the execution queue, or have finished executing. Any bulk action or right click action you take will create a job to handle the action, and you will be able to see them listed in this tab. You will be able to see the status and response for each task, which can give you visibility into what the extension is currently "working on." You are also given Bulk Actions on this page to retry failed jobs or manage the jobs table.



The screenshot shows the ThreatQ interface with the 'Jobs' tab selected. The header bar includes the ThreatQ logo and navigation links for 'Analyze', 'Notepad', 'Jobs', and 'Config'. Below the header, there is a section titled 'Jobs (Last 10)' with a clock icon. A 'Bulk Actions' button with a dropdown arrow is located in the top right of the table area. The table itself has four columns: 'TASK', 'TARGET(S)', 'RESPONSE', and 'LAST UPDATED'. It contains three rows of job data.

TASK	TARGET(S)	RESPONSE	LAST UPDATED
 object.find_mentions	210.65.244.176, and 24 more	Progress: 24%	4/8/2021, 9:55:24 AM
✓ object.find_mentions	setup.py	No Mentions	4/8/2021, 9:29:14 AM
✓ object.add_attribute	f37167c1e62e78b0a222b8cc18c20ba7, and 2 more	Error: Failed to connect to the ThreatQ host: 1	3/4/2021, 3:40:26 PM

Config

This extension tab is where you will configure your connection to ThreatQ, as well as setup some general configuration options. For more information, see the [Configuration](#) section.

Browser Context Menu Actions

The Context menu actions change based on if text is selected or not. Below are the options you will be given based on whether or not text is selected.

No Text Selection

ACTION	DETAILS
Open ThreatQ	This will open your ThreatQ instance in a new tab.
Highlight Indicators	This will attempt to highlight indicators on your current webpage. The Background Scanning must be enabled.
Highlight Threat Objects	You can set a custom Whitelist status for indicators that you mark Whitelisted. This can be used if your ThreatQ workflow includes a different status class for Whitelisted indicators.

Text Selected

ACTION	DETAILS
Quick Search	This will perform a quick search using the highlighted text. If results are found, the user is prompted with the results, and asked if they want to go to the results (in ThreatQ) or stay where they are.
Import Indicators	This will import the selected text into ThreatQ using the Indicator Import workflow within ThreatQ.
Find Mentions	This will run a Threat Library "mentions" search. If results are found, the user is prompted with the results, and asked if they want to go to the results (in ThreatQ) or stay where they are.
Add to Notepad	This will add the selected text to the notepad. If no indicator is detected, the user will be prompted to enter the object type. The object type does not need to be exact, but should align with the object names from ThreatQ (indicator, adversary, malware, etc.).
Add to Analyze	This will add the selected text to the analyze tab of the extension. If no indicator could be automatically parsed, the user will get a popup prompt where they can enter in the indicator type.

Bulk Actions

Throughout the extension's popup window, you will see a drop-down called, Bulk Actions. These are actions you can execute in bulk, either on the selected items from the table, or all of the items from the table. The following Bulk Actions are available:

- [Analyze Bulk Actions](#)
- [Indicator Actions](#)
- [Table Actions](#)

Analyze Bulk Actions

Page Actions

ACTION	DETAILS
Scan for Indicator	This will scan your current page for indicators and place anything found into the Analyze tab's table. Background Scanning <i>does not</i> need to be on for this feature.

Indicator Actions

ACTION	DETAILS
Lookup	This will perform a lookup for the selected (or all) indicators. If found, the score and status will be added to the entry within the table.
Import	This action is the same as the Import Indicator(s) right-click action. It will take all the selected (or all) indicators, and run them through the ThreatQ Indicator Import workflow in a new tab.
Add Tag	This action will allow you to bulk add tags to indicators within the analyze tab.
Add Attribute	This action will allow you to bulk add attributes to indicators within the analyze tab.
Quick Add	This action will <i>quickly</i> add the indicator. No indicator import workflow. It will use the defaults you set for the status and immediately add the indicator to ThreatQ.

Table Actions

ACTION	DETAILS
Add All / Selected to Notepad	This will add the selected (or all) indicators to your notepad. The indicators will not be removed from the Analyze page until you change tabs.
Clear All / Selected	This will clear the selected (or all) indicators in your analyze table.

Notepad Bulk Actions

You can perform the following Note Bulk Actions:

- [Object Actions](#)
- [Investigation Actions](#)
- [Table Actions](#)

Object Actions

ACTION	DETAILS
Find Mentions	This action will perform a Threat Library mentions lookup, and return a list of object counts for the given indicator or other threat object.
Add Tag	This action will allow you to bulk add tags to objects within the notepad tab.
Add Relationship	This action will allow you to bulk add relationships to objects within the notepad tab.
Add Attribute	This action will allow you to bulk add attributes to objects within the notepad tab.
Quick Add	This action will <i>quickly</i> add the object. No object import workflow. It will use the defaults you set in your configuration.

Investigation Actions

ACTION	DETAILS
Sync	This will sync your configured investigation with your notepad. Anything in the notepad and not in the investigation will get added to the investigation. Anything in the investigation and not in your notepad will get added to your notepad.
Reset	This action will reset your investigation by removing all nodes, and then adding only the nodes from your notepad.
Open	This action will open your investigation's workbench in a new tab.
Add Selected	This action will add the selected objects to your configured investigation.

Table Actions

ACTION	DETAILS
Clear All / Selected	This will clear the selected (or all) objects in your notepad table.

Filtering

After intelligence is added to either your Ana1yze tab or Notepad tab, you will be able to filter the data down using the search box above the tables. Click on the search bar and type in a term to use to search your table.



This search field persists when you close the extension. If you notice object counts are off, it could be because you still have a search term entered.

Troubleshooting / FAQ

- **Save & Text Connection fails**

If your connection fails when saving your ThreatQ connection configuration, it is most likely due to the host not being reachable. Confirm that your hostname is reachable from your local machine. To test this, you can open up terminal or command prompt and try to ping the hostname. If it fails, that is why the extension cannot connect. If it succeeds, the issue may lie elsewhere. If that is the case, try to configure the ThreatQ Host with the IP for your ThreatQ instance instead of the hostname. Sometimes that may solve the connection issues.

- **The extension is not parsing indicators**

If indicators are not being parsed, it might be because the Background Scanning option in the extension's Config -> General tab is turned off. For indicators to be parsed, that option must be turned on. If indicators are still not being parsed, it could be an unsupported indicator type. If that is the case, please contact our support team so we can add the new type to be parsed.

- **The Highlight Indicators button doesn't work**

In order for this to work, Background Scanning needs to be turned on as well. If it is not, nothing will be highlighted. It is also worth noting that the size of the page you are looking at does effect how long it takes to scan and highlight the indicators. If the page is exceptionally long (i.e. a Cisco Talos Threat Roundup blog), this can take a long time. On the contrary, a smaller blog or website may only take a second to parse and highlight the indicators.

- **How do I import a large block of text?**

To import indicators in bulk into ThreatQ, you can use the right-click actions from the extension. Simply select the text you want to import/parse. Then right click the selection and click ThreatQ -> Import Indicator(s). Doing so should redirect you to ThreatQ, where you can use the Indicator Import workflow to parse and import the indicators. This is done in order to leverage the existing workflow and features of the indicator import, so you can do things such as add related context, tags, and relationships.

Uninstalling the Extension

To uninstall the extension, follow these steps:

1. Open your Chrome Browser
2. Click on the puzzle piece icon to the right of your browser's URL bar
3. Select the button at the bottom labelled, Manage Extensions
4. When on the extensions page, you can uninstall the extension by clicking the Remove button within the extension's card entry.



An alternative to would be to right click the ThreatQ rhino icon and selecting the Remove from Chrome... option.

Change Log

- Version 1.0.0
 - Initial Release