ThreatQuotient

ThreatQ Google Chrome Extension User Guide

Version 1.1.0

June 22, 2023

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

Developer Supported

Support

Email:	chrome-team@threatq.com
Web:	N/A
Phone:	N/A

Contents

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.

Support

This integration is designated as **Developer Supported**.

Support Email: chrome-team@threatq.com
Support Web: N/A
Support Phone: N/A

Integrations designated as **Developer Supported** are supported and maintained by the developer who submitted the integration to the ThreatQ Marketplace. The developer's contact information can be found on the integration’s download page within the Marketplace as well as in this guide.

You are responsible for engaging directly with the developer of Developer Supported integrations/ apps/add-ons to ensure proper functionality and version compatibility with the applicable ThreatQuotient Software.

If functional or compatibility issues that may arise are not resolved, you may be required to uninstall the app or add-on from their ThreatQuotient environment in order for ThreatQuotient to fulfill support obligations.

For ThreatQuotient Hosted instance customers, the Service Level Commitment and Service Level Credit in the ThreatQuotient Service Level Schedule will not apply for any issues caused by Developer Supported integrations/apps/add-ons.

ThreatQuotient reserves the right to remove the Developer-Supported designation of third-party apps and add-ons if the developer is not, in ThreatQuotient’s determination, fulfilling reasonable obligations for support and maintenance.

> Failure by the developer to update compatibility of an app or add-on within 90 days of the release of a new version of applicable ThreatQuotient Software will result in reclassification to Not Actively Supported.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.1.0
Compatible with ThreatQ Versions	>= 5.6.0
Minimum ThreatQ User Account Role	Primary Contributor
Supported Browsers	Google Chrome
Compatible with Google Chrome Versions	>=87.x.x
Support Tier	Developer Supported
Support Contact	chrome-team@threatq.com
Google Chrome Store	https://chrome.google.com/webstore/detail/threatq-extension/kaoghaifdcjeaabfbdggomcpdgdfdjlm

Introduction

The Chrome Extension to give an analyst integration capabilities on any browser page, with ThreatQ.

The ThreatQ Chrome Extension gives analysts a quick and easy to use assistant while navigating web pages. The extension will allow analysts to perform quick lookups, automatically extract information from web pages, and ultimately, conduct thorough investigations.

Analysts will be able to quickly identify key pieces threat intelligence from web pages, and immediately figure out if they are relevant to their threat hunt or investigation. Additional context can be added to tracked threat objects and can be synced directly with a ThreatQ instance. Reports can be built directly from web pages and imported into ThreatQ, along with any relevant attribution, tags, and relationships.

The extension will be able to assist analysts in numerous ways, making them more efficient by giving them the tools they need to do their work.

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/kaoghaifdcjeaabfbdggomcpdgdfdjlm

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

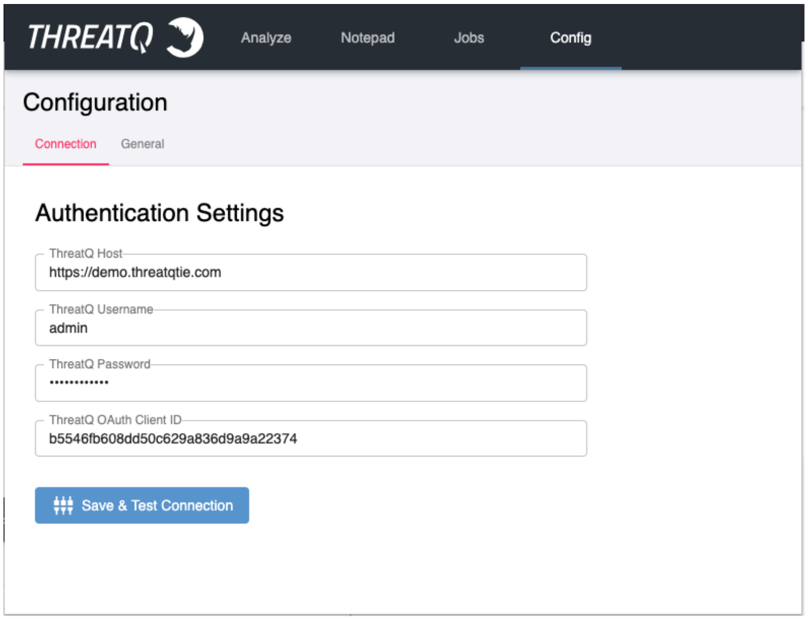
Use the following steps to configure the ThreatQ Chrome Extension. You will first need to pin the extension to your browser's toolbar. Once the extension has been pinned, you will be able to access the extension's UI by clicking on the ThreatQ rhino icon.

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

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	DESCRIPTION
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.



Configuration

Authentication Settings

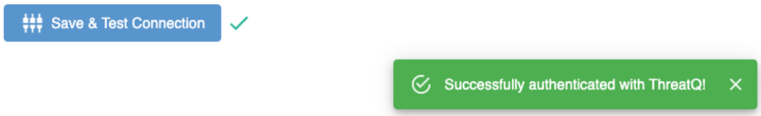
ThreatQ Host: https://demo.threatqtie.com

ThreatQ Username: admin

ThreatQ Password: ············

ThreatQ OAuth Client ID: b5546fb608dd50c629a836d9a9a22374

3. 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 ThreatQ instance.



Successfully authenticated with ThreatQ!

General Options

1. Click on the **Config** tab and select **General**.
2. Enter the following parameters:

PARAMETER	DESCRIPTION
Background Scanning	Enabling this will allow the extension to automatically scan your current browser page for indicators, preloading them into the Analyze page within the extension popup.
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.

PARAMETER	DESCRIPTION
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.
Default Source Name	This field allows you to set a default source name for all objects loaded into the Chrome Extension. Upon uploading selected objects to ThreatQ, this default source name will be applied.

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 following context menu options:

PARAMETER	DESCRIPTION
Highlight Indicators	Selecting this will highlight all indicators on your current web page .
Highlight Threat Actors	Selecting this will highlight all “standardized” Threat Actor names on your current web page. This includes APTs, TEMPs, UNCs, DEVs, TAs, Threat-Groups, and CrowdStrike Actors.
Highlight MITRE Techniques	Selecting this will highlight all MITRE ATT&CK Techniques on your current web page. The techniques must be in their “TID” form.
Highlight MITRE Tactics	Selecting this will highlight all MITRE Tactics on your current web page. **Example:** Exfiltration, Execution, Persistence, etc.
Open ThreatQ	Selecting this will quickly open the linked ThreatQ instance in a new tab.

> All highlight options will modify the HTML of your current web page, adding in a box around each item found. Hovering over an item will show an interactive tool tip that you can use to

> view information about the highlighted item, as well as perform actions on the highlighted item.

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:

PARAMETER	DESCRIPTION
Quick Search	Selecting this perform a quick search against ThreatQ. You will receive an OS-level notification if the selection was found or not. If the selection was found, the result will be added to your Notepad.
Create Report	Selecting this will take all the selected text/HTML, and create a report for it within the extension's Notepad. This will maintain all HTML formatting, which you'll be able to view within the extension's object details popup (eye icon next to each record). A source name will automatically be detected and applied to the Report object. Additional context can be added to the report before upload, such as tags, attributes, sources, etc.
Import Indicators	electing this will take all the selected text and send it to ThreatQ's Indicator Import workflow. This requires the authenticated user in the Chrome Extension to match the user you use to login via the UI.
Add to Notepad	Selecting this will add the selected text to the extension's Notepad page.
Add to Analyze	Selecting this will add the selected text to the extension's Analyze page.

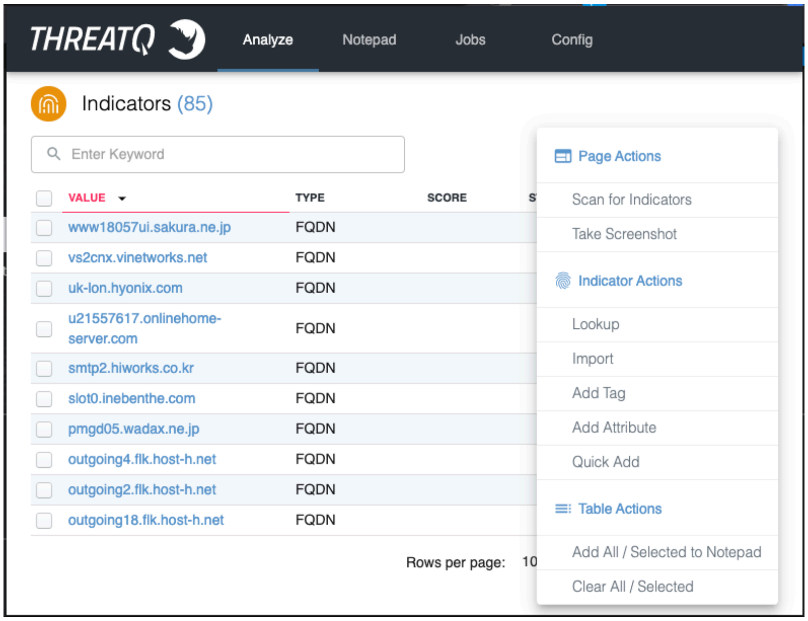
Tabs & Layout

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 **Background Scanning** is enabled. When you change tabs, the extension will automatically scan the webpage for indicators, and present them in the `Analyze` tab to be interacted with. If the Scan for Indicators optionis enabled, those items will persist in the Analyze tab until you manually clear it. On the Analyze page, you will be able to add context back to ThreatQ, perform lookups, or add an indicator to your `Notepad`.



Indicators (85)

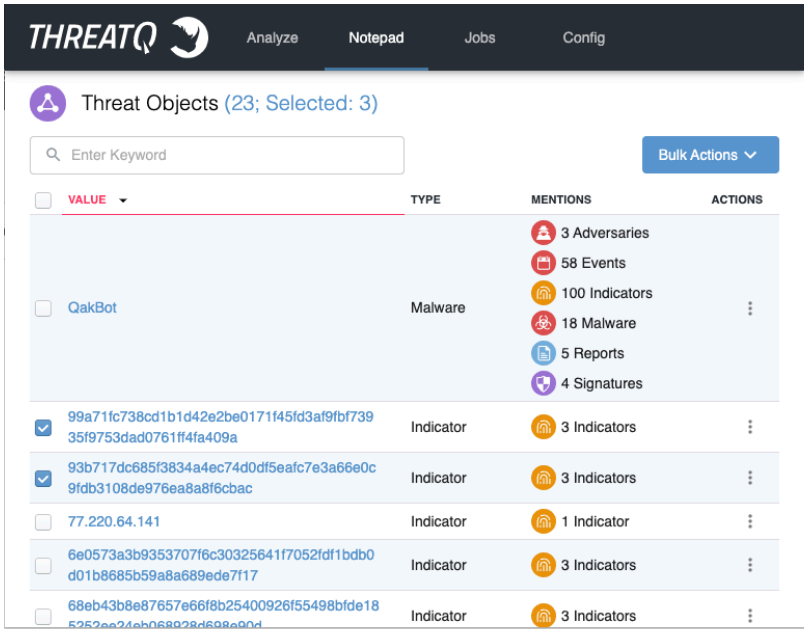
Enter Keyword

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		

Rows per page: 10

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, view the object's details, add relationships, add attributes, and more.

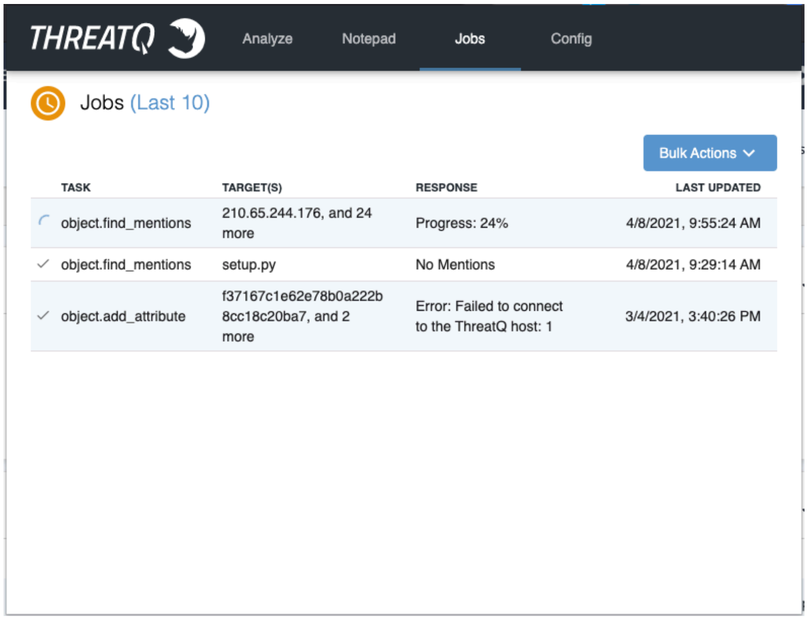


Threat Objects (23; Selected: 3)

☐	VALUE	TYPE	MENTIONS	ACTIONS
☐	QakBot	Malware	3 Adversaries 58 Events 100 Indicators 18 Malware 5 Reports 4 Signatures	⋮
☑	99a71fc738cd1b1d42e2be0171f45fd3af9fbf739 35f9753dad0761ff4fa409a	Indicator	3 Indicators	⋮
☑	93b717dc685f3834a4ec74d0df5eafc7e3a66e0c 9fdb3108de976ea8a8f6cbac	Indicator	3 Indicators	⋮
☐	77.220.64.141	Indicator	1 Indicator	⋮
☐	6e0573a3b9353707f6c30325641f7052fdf1bdb0 d01b8685b59a8a689ede7f17	Indicator	3 Indicators	⋮
☐	68eb43b8e87657e66f8b25400926f55498bfde18 5252ee24eb068928d698e90d	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.



Jobs (Last 10)

	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	f37167c1e62e78b0a222b 8cc18c20ba7, 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.

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` *does not* 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.
Upload	This action will *quickly* upload the indicator. No indicator import workflow. It will use the defaults you set for the status and immediately add the indicator to ThreatQ.
Inter-relate Selected	This action will relate all selected indicators to each other, within ThreatQ.
Create Event with Selected	This action will create an event for the selected indicators, within ThreatQ. You will be prompted for details for the Event.

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.
Upload	This action will *quickly* add the object. No object import workflow. It will use the defaults you set in your configuration.
Inter-Relate Selected	This action will relate all selected objects to each other, within ThreatQ.

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 `Analyze` 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 1.1.0**
    - Updated the extension to Chrome's Manifest v3 Standards.
    - Switched from localStorage to an IndexedDB to allow you to store more information in the extension.
    - Added tooltips to highlighted items.
    - Added an Object Details popup to Analyze/Notepad objects.
    - You can now view tags, sources, attributes, and descriptions.
    - Added additional tags, sources, and attributes.
    - Added improved efficiency of Indicator Highlighting (via right-click).
    - Added MITRE Technique Highlighting (via right-click).
    - Added MITRE Tactic Highlighting (via right-click).
    - Added Threat Actor Highlighting (via right-click).
    - The extension now allows users to re-upload objects if new context has been added to it.
    - Added improved stability of bulk-actions and connection to ThreatQ.
    - Added the ability to inter-relate selected objects.
    - Added the ability to create an event from selected objects.
    - Added the ability to create a report from selected text (via right-click).
    - Added the ability to parse PDFs for Indicators.
    - Added the ability to manually create objects for the Notepad.
    - Added the ability to set a default source name for objects loaded into the extension.
    - Performed various package and dependency upgrades.
- **Version 1.0.0**
    - Initial release