

# ThreatQuotient



## Zscaler Action

Version 1.0.0

July 28, 2024

## ThreatQuotient

20130 Lakeview Center Plaza Suite 400  
Ashburn, VA 20147

 ThreatQ Supported

## Support

Email: [support@threatq.com](mailto:support@threatq.com)

Web: [support.threatq.com](https://support.threatq.com)

Phone: 703.574.9893

# Contents

Warning and Disclaimer ..... 3

Support ..... 4

Integration Details..... 5

Introduction ..... 6

Prerequisites ..... 7

Installation..... 8

Configuration ..... 9

Actions ..... 11

    Zscaler URL Category Export Indicators ..... 12

Known Issues / Limitations ..... 13

Change Log ..... 14

# 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 © 2024 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.

# Support

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

**Support Email:** [support@threatq.com](mailto:support@threatq.com)

**Support Web:** <https://support.threatq.com>

**Support Phone:** 703.574.9893

Integrations/apps/add-ons designated as **ThreatQ Supported** are fully supported by ThreatQuotient's Customer Support team.

ThreatQuotient strives to ensure all ThreatQ Supported integrations will work with the current version of ThreatQuotient software at the time of initial publishing. This applies for both Hosted instance and Non-Hosted instance customers.



ThreatQuotient does not provide support or maintenance for integrations, apps, or add-ons published by any party other than ThreatQuotient, including third-party developers.

# Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.0.0
-----------------------------	-------

Compatible with ThreatQ Versions	>= 6.1.0
-------------------------------------	----------

ThreatQ TQO License Required	Yes
---------------------------------	-----

Support Tier	ThreatQ Supported
--------------	-------------------

# Introduction

The Zscaler Action integration provides ThreatQ users with the ability to export FQDNs, URLs, and IP Addresses in a ThreatQ data collection to a Zscaler URL Category.

The integration provides the following action:

- **Zscaler URL Category Export Indicators** - adds the indicators in a data collection to a predefined Zscaler URL Category.

The action is compatible with the following indicator types:

- FQDN
- IP Address
- URL



This action is intended for use with ThreatQ TDR Orchestrator (TQO). An active TQO license is required for this feature.

# Prerequisites

The following is required in order to install and use the action.

- An active ThreatQ TDR Orchestrator (TQO) license.
- A data collection containing at least one of the following indicator types:
  - FQDN
  - IP Address
  - URL
- Zscaler Username.
- Zscaler Password.
- ZScaler API Key.



See the following link for additional information about the Zscaler API key: <https://help.zscaler.com/zia/managing-cloud-service-api-key>.

# Installation

Perform the following steps to install the integration:



The same steps can be used to upgrade the integration to a new version.

1. Log into <https://marketplace.threatq.com/>.
2. Locate and download the action zip file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the action zip file using one of the following methods:
  - Drag and drop the zip file into the dialog box
  - Select **Click to Browse** to locate the zip file on your local machine



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

You will still need to [configure](#) the action.

# Configuration



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

To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Actions** option from the *Category* dropdown (optional).
3. Click on the action entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:




The configurations set on this page will be used as the default settings when inserting this action into a new workflow. Updating the configurations on this page will not update any instances of this action that have already been deployed to a workflow. In that scenario, you must update the action's configurations within the workflow itself.

PARAMETER	DESCRIPTION
Zscaler URL	Enter the full URL of your Zscaler instance.
Zscaler Username	Enter your Zscaler Cloud (ZIA) username to authenticate.
Zscaler Password	Enter your Zscaler Cloud (ZIA) password to authenticate.
Zscaler ZIA API Key	Enter the API key provided in Zscaler. This can be found under Administration -> Cloud Service API Security in in your Zscaler instance. Additional information can be found at <a href="https://help.zscaler.com/zia/managing-cloud-service-api-key">https://help.zscaler.com/zia/managing-cloud-service-api-key</a> .
Category Name	Enter a name for the category to export IOCs to when using the action.
Category Description	Enter a description for the category to export IOCs to when using the action.

PARAMETER	DESCRIPTION
Automatically Activate Pending Changes	Enable this parameter to automatically activate pending policy/category changes after uploading the indicators.
Verify Host SSL	Enable or Disable Host SSL certificate verification.
Disable Proxies	Enable this option if the action should not honor proxies set in the ThreatQ UI.
Objects Per Run	Enter the max number of objects to send to this action per run.

### < Zscaler URL Category Export Indicators



Uninstall


**Additional Information**  
Integration Type: Action  
Version:  
Action ID: 9  
Accepted Data Types:  
☒ Indicators  
URL  
FQDN  
IP Address

#### Configuration

Zscaler URL

Specify full URL to the Zscaler instance.

Zscaler Username

Zscaler Password 

Zscaler ZIA API Key

Category Name

ThreatQ Blacklist

Enter a name for the category you want to export IOCs to

Category Description

Prioritized IOCs exported from the ThreatQ platform.

Enter a description for the category you want to export IOCs to

☐ Automatically Activate Pending Changes  
Enable this to automatically activate pending policy/category changes

☒ Enable SSL Verification

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

Objects per run

1000

Maximum number of objects to send to Zscaler per-run

Save

5. Review any additional settings, make any changes if needed, and click on **Save**.

# Actions

The following action is available:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
<a href="#">Zscaler URL Category Export Indicators</a>	Adds indicators to a predefined Zscaler URL Category.	Indicator	IP Address, URL, FQDN

## Zscaler URL Category Export Indicators

The Zscaler URL Category Export Indicators action uploads the indicators from the selected collection to a predefined Zscaler URL Category. The name of the predefined category must be specified in the action configuration (**Category Name** parameter). The category will be deleted if it already exists, together with all the associated URLs and IP Addresses. The URLs are upload without the HTTP schema.

POST "{{ZSCALER\_URL}}/api/v1/urlCategories"

### Sample Body:

```
{
  "configuredName": "ThreatQ Blacklist",
  "superCategory": "SECURITY",
  "customCategory": true,
  "description": "Prioritized IOCs exported from the ThreatQ platform.",
  "urls": [
    "217.60.9.178",
    "253.106.205.92.host.secureserver.net/konto-creedentials",
    "vetfashion.xyz/css/10/admin/index.php"
  ]
}
```

### Sample Response:

```
{
  "configuredName": "ThreatQ Blacklist",
  "customCategory": true,
  "customIpRangesCount": 0,
  "customUrlsCount": 3,
  "dbCategorizedUrls": [],
  "description": "Prioritized IOCs exported from the ThreatQ platform.",
  "editable": true,
  "id": "CUSTOM_04",
  "ipRangesRetainingParentCategoryCount": 0,
  "keywords": [],
  "keywordsRetainingParentCategory": [],
  "superCategory": "SECURITY",
  "type": "URL_CATEGORY",
  "urls": [
    "217.60.9.178",
    "vetfashion.xyz/css/10/admin/index.php",
    "253.106.205.92.host.secureserver.net/konto-creedentials"
  ],
  "urlsRetainingParentCategoryCount": 0,
  "val": 131
}
```

## Known Issues / Limitations

- The changes to a URL Category must be activated in the Zscaler Portal. You can either enable the **Automatically Activate Pending Changes** configuration parameter to automatically activate any pending changes or go to the Zscaler Portal to manually activate them.
- Zscaler allows for a maximum of 25,000 values across all Categories.
- Zscaler allows for a maximum of 64 predefined categories.
- Zscaler does not accept URLs longer than 1024 characters. Anything longer than this limit is truncated.

# Change Log

- Version 1.0.0
  - Initial release