

# ThreatQuotient



## Qualys Scanner Connector Guide

Version 1.2.5 rev-b

March 15, 2023

**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

<b>Integration Details</b> .....	<b>5</b>
<b>Introduction</b> .....	<b>6</b>
<b>Prerequisites</b> .....	<b>7</b>
IP Whitelist .....	7
Time Zone .....	7
Asset Custom Object .....	8
Integration Dependencies .....	9
<b>Installation</b> .....	<b>11</b>
Creating a Python 3.6 Virtual Environment .....	11
Installing the Connector .....	12
<b>Configuration</b> .....	<b>14</b>
<b>Usage</b> .....	<b>16</b>
Command Line Arguments.....	16
CRON.....	18
<b>Change Log</b> .....	<b>19</b>

# Warning and Disclaimer

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

Copyright © 2023 ThreatQuotient, Inc.

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

# 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	1.2.5
Compatible with ThreatQ Versions	>= 4.34.0
Python Version	3.6
Support Tier	ThreatQ Supported
ThreatQ Marketplace	<a href="https://marketplace.threatq.com/details/qualys-scanner">https://marketplace.threatq.com/details/qualys-scanner</a>

# Introduction

The Qualys Scanner connector integrates ThreatQ with a Qualys appliance, either cloud-based or on-prem. The vulnerabilities scanner connector collects information about Qualys scans executed in the past days, collects all CVEs related to those vulnerabilities and ingests them in ThreatQ.

The configuration of the connector in the ThreatQ UI gives the user the ability to define the number of historical days for the first run, and every consecutive run searches only for vulnerabilities in scans executed after the last run of the connector.

Additionally, the user can provide the following parameters to filter down the assets found in Qualys scans; Range or a list of IP addresses to search for, Asset group IDs, and minimum severity of vulnerability scans.

# Prerequisites

The following items are required for the integration:

- A Qualys Knowledgebase account in order to convert QIDs to CVEs.
- The appropriate [IP addresses whitelisted](#) to connect to the cloud platform.
- A dedicated account in Qualys with a Manager role.
- The [Asset object](#) installed on your ThreatQ Instance

## IP Whitelist

The following IP Addresses must be whitelisted in your proxy in order to connect to the Qualys cloud platform:

- 162.159.152.21
- 162.159.153.243

## Time Zone

You should ensure all ThreatQ devices are set to the correct time, time zone, and date (UTC is recommended), and using a clock source available to all.

To identify which time zone is closest to your present location, use the `timedatectl` command with the `list-timezones` command line option.

For example, enter the following command to list all available time zones in Europe:


```
timedatectl list-timezones | grep Europe
Europe/Amsterdam
Europe/Athens
Europe/Belgrade
Europe/Berlin
```

Enter the following command, as root, to change the time zone to UTC:


```
timedatectl set-timezone UTC
```

# Asset Custom Object

The integration requires the Asset object. The Asset installation files are included with the integration download on the ThreatQ Marketplace. The Asset object must be installed prior to installing the integration.

 You do not have to install the Asset object if you are running ThreatQ version 5.10.0 or greater as the object has been seeded as a default system object.

Use the steps provided to install the Asset custom object.

 When installing the custom objects, be aware that any in-progress feed runs will be cancelled, and the API will be in maintenance mode.

1. Download the custom object zip file from the ThreatQ Marketplace and unzip its contents.
2. SSH into your ThreatQ instance.
3. Navigate to tmp directory:

```
<> cd /tmp/
```

4. Create a new directory:

```
<> mkdir qualys_scanner
```

5. Upload the **asset.json** and **install.sh** script into this new directory.
6. Create a new directory called **images** within the **qualys\_scanner** directory.

```
<> mkdir images
```

7. Upload the **asset.svg**.
8. Navigate to the **/tmp/qualys\_scanner**.

The directory should resemble the following:

- tmp
  - qualys\_scanner
    - asset.json
    - install.sh
    - images



- **asset.svg**

9. Run the following command to ensure that you have the proper permissions to install the custom object:

```
<> chmod +x install.sh
```

10. Run the following command:

```
<> sudo ./install.sh
```



You must be in the directory level that houses the install.sh and json files when running this command.

The installation script will automatically put the application into maintenance mode, move the files to their required directories, install the custom object, update permissions, bring the application out of maintenance mode, and restart dynamo.

11. Remove the temporary directory, after the custom object has been installed, as the files are no longer needed:

```
<> rm -rf qualys_scanner
```

## Integration Dependencies



The integration must be installed in a python 3.6 environment.

The following is a list of required dependencies for the integration. These dependencies are downloaded and installed during the installation process. If you are an Air Gapped Data Sync (AGDS) user, or run an instance that cannot connect to network services outside of your infrastructure, you will need to download and install these dependencies separately as the integration will not be able to download them during the install process.



Items listed in bold are pinned to a specific version. In these cases, you should download the version specified to ensure proper function of the integration.

DEPENDENCY	VERSION	NOTES
threatqsdk	>=1.8.0	N/A

---

DEPENDENCY	VERSION	NOTES
threatqcc	>=1.4.1	N/A
urllib3	N/A	N/A
python-dateutil	N/A	N/A
future	N/A	N/A

# Installation

The following provides you with steps on installing a Python 3 Virtual Environment and installing the connector.


## Creating a Python 3.6 Virtual Environment

Run the following commands to create the virtual environment:

```
mkdir /opt/tqvenv/  
sudo yum install -y python36 python36-libs python36-devel python36-pip  
python3.6 -m venv /opt/tqvenv/<environment_name>  
source /opt/tqvenv/<environment_name>/bin/activate  
pip install --upgrade pip  
pip install threatqsdk threatqcc  
pip install setuptools==59.6.0
```

Proceed to [Installing the Connector](#).

# Installing the Connector

 **Upgrading Users** - Review the [Change Log](#) for updates to configuration parameters before updating. If there are changes to the configuration file (new/removed parameters), you must first delete the previous version's configuration file before proceeding with the install steps listed below. Failure to delete the previous configuration file will result in the connector failing.

1. Navigate to the ThreatQ Marketplace and download the .whl file for the integration.
2. Activate the virtual environment if you haven't already:

```
<> source /opt/tqvenv/<environment_name>/bin/activate
```

3. Transfer the whl file to the /tmp directory on your ThreatQ instance.
4. Install the connector on your ThreatQ instance:

```
<> pip install /tmp/tq_conn_qualys_scanner-<version>-py3-none-any.whl
```



A driver called tq-conn-qualys-scanner will be installed. After installing, a script stub will appear in /opt/tqvenv/<environment\_name>/bin/tq-conn-qualys-scanner.

5. Once the application has been installed, a directory structure must be created for all configuration, logs and files, using the `mkdir -p` command. Use the commands below to create the required directories:

```
<> mkdir -p /etc/tq_labs/  
mkdir -p /var/log/tq_labs/
```

6. Perform an initial run using the following command:

```
<> /opt/tqvenv/<environment_name>/bin/tq-conn-qualys-scanner -  
ll /var/log/tq_labs/ -c /etc/tq_labs/ -v3
```

7. Enter the following parameters when prompted:

PARAMETER	DESCRIPTION
ThreatQ Host	This is the host of the ThreatQ instance, either the IP Address or Hostname as resolvable by ThreatQ.

PARAMETER	DESCRIPTION
ThreatQ Client ID	This is the OAuth id that can be found at Settings Gear → User Management → API details within the user's details.
ThreatQ Username	This is the Email Address of the user in the ThreatQ System for integrations.
ThreatQ Password	The password for the above ThreatQ account.
Status	This is the default status for objects that are created by this Integration.

## Example Output

```
/opt/tqvenv/<environment_name>/bin/tq-conn-qualys-scanner -ll /var/log/tq_labs/ -c /etc/tq_labs/ -v3
ThreatQ Host: <ThreatQ Host IP or Hostname>
ThreatQ Client ID: <ClientID>
ThreatQ Username: <EMAIL ADDRESS>
ThreatQ Password: <PASSWORD>
Status: Review
Connector configured. Set information in UI
```

You will still need to [configure and then enable the connector](#).

# 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 **Labs** option from the *Category* dropdown (optional).
3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
IP/Hostname	The Hostname or IP address of Qualys. The following are common Qualys Hostnames that can be used in this field: <ul style="list-style-type: none"><li>◦ <b>Qualys US Platform 1:</b> https://qualysapi.qualys.com</li><li>◦ <b>Qualys US Platform 2:</b> https://qualysapi.qg2.apps.qualys.com</li><li>◦ <b>Qualys US Platform 3:</b> https://qualysapi.qg3.apps.qualys.com</li><li>◦ <b>Qualys EU Platform 1:</b> https://qualysapi.qualys.eu</li><li>◦ <b>Qualys EU Platform 2:</b> https://qualysapi.qg2.apps.qualys.eu</li><li>◦ <b>Qualys India Platform 1:</b> https://qualysapi.qg1.apps.qualys.in</li><li>◦ <b>Qualys Private Cloud Platform:</b> https://qualysapi.&lt;customer_base_url&gt;</li></ul>
Port	The Port for communicating with the Qualys API.
Username	Your Username for logging to Qualys.
Password	The password associated with the account referenced above.

PARAMETER	DESCRIPTION
Number of days for initial run	Enter the number of days of history do you want to search for vulnerability scans for the initial run.
Number of Quality IDs to search at a time	Enter the number of Qualys IDs to search at a time. Consult the administrative setting in Qualys to determine this value. The default value is 1000.
Automate Assets	<p>Select this option if you want to enable the automatic ingestion of assets into you TQ instance.</p> <p>This option requires that you have the <b>Asset</b> custom object installed on your instance.</p>
Unrelate Patched QIDs/ CVEs from Assets	Select this option to delete relationships between assets and patched QIDs/CVEs.
Provide a range of IPs to collect data for	Optional - One or more IPs or ranges may be specified. Multiple entries should be comma-separated.
Enter asset groups	Optional - Collect scan information only for hosts belonging to asset groups with certain IDs. One or more asset group IDs and/or ranges may be specified. Multiple entries should be comma-separated
Collect only scans which have specific severities	Optional - Show only detection records which have certain severities. One or more levels may be specified. Multiple entries should be comma-separated.

5. Review any additional settings, make any changes if needed, and click on **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable it.

# Usage

Use the following command to execute the driver:

```
<> /opt/tqvenv/<environment_name>/bin/tq-conn-qualys-scanner -v3  
-ll /var/log/tq_labs/ -c /etc/tq_labs/
```

## Command Line Arguments

This connector supports the following custom command line arguments:

ARGUMENT	DESCRIPTION
<code>-h, --help</code>	Shows this help message and exits.
<code>-n NAME, --name Name</code>	This sets the name for this connector. In some cases, it is useful to have multiple connectors of the same type executing against a single TQ instance. For example, the Syslog Exporter can be run against multiple target and multiple exports, each with their own name and configuration
<code>-d, --no- differential</code>	If exports are used in this connector, this will turn 'off' the differential flag for the execution. This allows debugging and testing to be done on export endpoints without having to rebuild the exports after the test. THIS SHOULD NEVER BE USED IN PRODUCTION.
<code>-ll LOGLOCATION, --loglocation LOGLOCATION</code>	Sets the logging location for the connector. The location should exist and be writable by the current. A special value of 'stdout' means to log to the console (this happens by default).
<code>-c CONFIG, -- config CONFIG</code>	This is the location of the configuration file for the connector. This location must be readable and writable by the current user. If no config file path is given, the current directory will be used. This file is also where some information from each run of the connector may be put (last run time, private oauth, etc.)



---

ARGUMENT	DESCRIPTION
<code>-v {1,2,3}, -- verbosity {1,2,3}</code>	This is the logging verbosity level. The default setting is <b>1</b> (Warning). The recommended value is <b>3</b> (debug).
<code>-ds, --disable_ssl</code>	This allows you to disable SSL verification to all requests to the API.
<code>-ep, -external-proxy</code>	This allows you to use the proxy that is specified in the ThreatQ UI.

## CRON

Automatic CRON configuration has been removed from this script. To run this script on a recurring basis, use CRON or some other jobs scheduler. The argument in the CRON script must specify the config and log locations.

Add an entry to your Linux crontab to execute the connector at a recurring interval. Depending on how quickly you need updates, this can be run multiple times a day (no more than once an hour) or a few times a week.

In the example below, the command will execute the connector every two hours.

1. Log into your ThreatQ host via a CLI terminal session.
2. Enter the following command:

```
<> crontab -e
```

This will enable the editing of the crontab, using vi. Depending on how often you wish the cronjob to run, you will need to adjust the time to suit the environment.

3. Enter the commands below:

### Every 2 Hours Example

```
<> 0 */2 * * * /opt/tqvenv/<environment_name>/bin/tq-conn-qualys-  
scanner -c /etc/tq_labs/ -ll /var/log/tq_labs/ -v3
```

4. Save and exit CRON.

# Change Log

- **Version 1.2.5 rev-b (Guide Update)**
  - Added IP Whitelist section to Prerequisites chapter.
- **Version 1.2.5 rev-a (Guide Update)**
  - Updated the Prerequisites chapter regarding the Asset object. ThreatQ version 5.10.0 introduced the Asset object as a seeded default system object. Users on ThreatQ 5.10.0 or later do not have to install the Asset custom object prior to installing the integration.
- **Version 1.2.5**
  - Fixed an issue where the wrong ID was used when deleting a relationship.
  - Added new configuration option - **Unrelate Patched QIDs/CVEs from Assets**.
  - Updated the connector for improved error catching.
- **Version 1.2.4**
  - Fixed a custom asset error.
- **Version 1.2.3**
  - Improved integration performance by reducing API requests and bulk uploading.
- **Version 1.2.2**
  - Fixed two bugs related to handling API responses.
- **Version 1.2.1**
  - Added the QIDs as Vulnerability objects in TQ.
  - Related the QIDs to CVEs that are ingested.
  - Added IPs as Asset objects to TQ.
  - Related Assets to QIDs and CVEs.
  - Added a checkbox in the TQ UI config allowing users to enable/disable the automated adding of assets.
  - Unrelated Assets from QIDs and corresponding CVEs if QID was patched/fixed.
- **Version 1.2.0**
  - Changed authentication to basic auth with username and password.
  - Modified the the QID to CVE mapping to do it in batches of 1000 QIDs.
- **Version 1.1.1**
  - Added unicode string handling for the response from Qualys.

- 
- **Version 1.1.0**
    - Added Python 3 support.
  - **Version 1.0.0**
    - Initial Release