ThreatQuotient

Installing Custom Connectors in ThreatQ v6

Version 1.0.1

August 09, 2024

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: support@threatq.com
Web: support.threatq.com
Phone: 703.574.9893

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.

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.

Installing Custom Connectors in ThreatQ v6

Download PDF version

The installation process for custom connectors has changed with ThreatQ version 6 due to architectural changes in the platform.

> Contact ThreatQ Support if you have any questions or issues installing a custom connector on your ThreatQ v6 instance.

Summary of Changes

The following is a list of changes made to the installation process when installing a custom connector on a ThreatQ v6 instance (when compared to ThreatQ v5):

- Custom connectors are now installed in the custom connector container.
- Custom connector logs are now aggregated to an output container opposed to a single file.
- Custom connector configuration files are now automatically housed in the following location: `/etc/tq_labs/`.
- CRONtab is not used when the connector is installed on your ThreatQ instance when using version 6. Users can now generate a cron job using the `--cron flag`. See the CRON section under the Install on ThreatQ Instance tab for more details on using CRON with custom connectors in ThreatQ v6.

Connector Installation

The following steps are for installing the custom connector on a ThreatQ instance.

1. Download the connector integration file from the ThreatQ Marketplace.
2. Transfer the connector whl file to the `/tmp/` directory on your instance.
3. SSH into your instance.
4. Move the connector whl file from its `/tmp/` location to the following directory: `/opt/tqvenv`
5. Navigate to the custom connector container:

   ```
   kubectl exec -n threatq -it deployments/custom-connectors -- /bin/bash
   ```

6. Create your python 3 virtual environment:
7.
   ```
   python3.6 -m venv /opt/tqvenv/<environment_name>
   ```

8. Active the new environment:

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

9. Run the pip upgrade command:

   ```
   pip install --upgrade pip
   ```

10. Install the required dependencies:

    ```
    pip install setuptools==59.6.0 threatqsdk threatqcc
    ```

11. Install the connector:

    ```
    pip install /opt/tqvenv/tq_conn_<wheel_name>-<version>-py3-none-
    any.whl
    ```

12. Perform an initial run of the connector:

    ```
    /opt/tqvenv/<environment_name>/bin/<driver-name> --cron="0 */2 * * *"
    ```

    > The `--cron` argument above is used to generate a cron job for the connector. After running the command above, the cronjob will be created under the /etc/cron.d/ directory. This entry will initially be commented out upon creation - see the CRON chapter for more details.

13. Enter the following parameters when prompted:

PARAMETER	DESCRIPTION
ThreatQ Host	**Leave this field blank as it will be set dynamically.**
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-<driver-name> --cron="0 */2 * * *"
ThreatQ Host:
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. This process is the same as in ThreatQ v5.

Usage

Use the following commands to execute the driver:

```
/opt/tqvenv/<environment_name>/bin/tq-conn-<driver-name>
```

Command Line Arguments

This connector supports the following custom command line arguments:

ARGUMENT	DESCRIPTION
`-h`, `--help`	Review all additional options and their descriptions.
`-v {1,2,3}`, `--verbosity {1,2,3}`	This is the logging verbosity level where **3** means everything.
`-n, --name`	Optional - Name of the connector (Option used in order to allow users to configure multiple connector instances on the same TQ box).
--cron	Creates a CRON entry for the connector based on a pre-loaded ThreatQ template. See the CRON section for more details.

Accessing Connector Logs

ThreatQ version 6 aggregates the logs for all custom connectors to its output container. You can access the container's log using the following command:

```
kubectl logs -n threatq deployments/custom-connectors
```

Accessing Connector Configuration

The custom connector configuration file can be found in the following directory: `/etc/tq_labs/`.

CRON

The addition of the `--cron` argument in the initial run of connector, performed during the install process, resulted in the creation of a cron job file for the connector in the following directory: `/etc/cron.d/`. The contents of the file will resemble the following structure:

```
#{schedule} root /bin/bash -c "source /etc/env-vars.sh; {venv_path}/bin/
{executable} --config=/etc/tq_labs > /proc/1/fd/1 2>/proc/1/fd/2"
```

The `{schedule}` will be replaced with the cron settings you entered with the `--cron` flag and the `{executable}` will be replaced for with the connector's driver command.

You will also see a `#` at the beginning of file. This comments out the job. This allows you to configure the custom connector in the ThreatQ UI first. After you have configured the connector in ThreatQ, you can remove the `#` from the file content's in order to activate the cron job.

To summarize this process:

1. Install the connector and perform an initial run using the `--cron` argument to create the cron job.
2. Complete the connector's configuration settings in the ThreatQ UI.
3. Access the connector's cron file in the `/etc/cron.d/` directory and remove the # from the beginning of the file.

Uninstalling the Connector

Perform the following steps to remove the connector from your ThreatQ v6 instance:

1. SSH into your ThreatQ instance.
2. Navigate to the custom connector pod:

   ```
   kubectl exec -n threatq -it deployments/custom-connectors -- /bin/bash
   ```

3. Activate the python environment:

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

4. Uninstall the connector:

   ```
   pip uninstall <connector-driver-name>
   ```

5. Remove the cron file for the connector:

   ```
   rm /etc/cron.d/<connector-driver-name>
   ```