

ThreatQuotient



Infoblox BloxOne Connector User Guide

Version 1.0.0

October 18, 2023

ThreatQuotient

20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147



Support

Email: support@threatq.com

Web: support.threatq.com

Phone: 703.574.9893

Contents

Warning and Disclaimer	3
Support	4
Integration Details.....	5
Introduction	6
Prerequisites	7
Time Zone	7
Integration Dependencies	8
Installation.....	9
Creating a Python 3.6 Virtual Environment	9
Installing the Connector.....	10
Configuration	12
Usage.....	16
Command Line Arguments.....	16
CRON	18
Change Log	19

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

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	>= 4.34.0
-------------------------------------	-----------

Python Version	3.6
----------------	-----

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

Introduction

The Infoblox BloxOne Connector for ThreatQ provides you with the ability to upload IP Address, FQDN, and CIDR Block Indicator types to a Custom List in Infoblox Bloxone.

Prerequisites

Review the following requirements before attempting to install the connector.

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
```

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
threatqcc	>=1.4.1	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 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_infoblox_bloxone-<version>-py3-none-any.whl
```



A driver called `tq-conn-infoblox-bloxone` will be installed. After installing, a script stub will appear in `/opt/tqvenv/<environment_name>/bin/tq-conn-infoblox-bloxone`.

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-infoblox-bloxone -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.
ThreatQ Client ID	This is the OAuth id that can be found at Settings Gear → User Management → API details within the user's details.

PARAMETER	DESCRIPTION
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-infoblox-bloxone -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
API IP/ Hostname	The Hostname or IP address of the Infoblox BloxOne instance.
API Key	The API Key used to connect to your Infoblox BloxOne instance. Your API Key can usually be found under User Preferences (bottom left corner).
Custom List Name	The name of the custom list to add indicators to on Infoblox BloxOne.
Data Collections To Add	A comma-delimited list of data collections containing indicators to add to your specified Infoblox BloxOne custom list. The indicators must be of type IP Address, FQDN, or CIDR Block in order for them to be added to Infoblox BloxOne.
Data Collections To Remove	Optional - A comma-delimited list of data collections containing indicators to remove from your specified Infoblox BloxOne custom list. The indicators must be of type IP Address, FQDN, or CIDR Block in order for them to be added to Infoblox BloxOne.
Historical Timeframe (days)	<p>The number of days worth of indicators the connector will pull from to add to Infoblox BloxOne. This applies to the first time the connector is ran or when the connector is executed with the <code>-hist</code> argument.</p> <p>The default setting is 10 days, i.e. all indicators that were added to, or modified in ThreatQ during the last ten days will be pushed to</p>

PARAMETER	DESCRIPTION
	Infoblox BloxOne. This is also the same date range that will be used when pulling data from InfoBlox BloxOne analytic (Threat Insight) events to upload to ThreatQ. Valid values are integers that are 0 or greater.
Add Analytic Events	Optional - Selecting this option will have the connector upload Infoblox BloxOne analytic (Threat Insight) events to ThreatQ. The data will be uploaded as ThreatQ Events with related Indicators.
Analytic Network	Optional - Enter an Analytic Network : Source Network (NAT case) / On-Prem Host name / AT Endpoint
Analytic Query IP	Optional - Enter a Device IP that sent the DNS query.
Analytic Queried Name/ Domain	Optional - Enter the Name/Domain that was queried by an analytic event.
Analytic Policy Name	Optional - Enter the Policy on Infoblox BloxOne that created an analytic event.
Analytic Threat Level	Optional - Enter the Threat level of an analytic event in Infoblox BloxOne. Options include: <ul style="list-style-type: none"> ◦ Low ◦ Medium ◦ High
Analytic Threat Category	Optional - Enter the Threat Category of an analytic event in Infoblox BloxOne.

Configuration

API IP/Hostname

csp.infoblox.com

Hostname or IP address of the Infoblox BloxOne instance.

API Key

.....

This is the API Key used to connect to your Infoblox BloxOne instance. Your API Key can usually be found under User Preferences (bottom left corner).

Custom List Name

CustomList

This is the name of the custom list you wish to add indicators to on Infoblox BloxOne.

Data Collections To Add

IndsToAdd, MoreIndsToAdd

This is a comma-delimited list of data collections containing indicators you wish to add to your specified Infoblox BloxOne custom list. The indicators must be of type IP Address, FQDN, or CIDR Block in order for them to be added to Infoblox BloxOne.

(Optional) Data Collections To Remove

(Optional) This is a comma-delimited list of data collections containing indicators you wish to remove from your specified Infoblox BloxOne custom list. The indicators must be of type IP Address, FQDN, or CIDR Block in order for them to be added to Infoblox BloxOne.

Historical timeframe (days)

10

This is the number of days worth of indicators the connector will pull from to add to Infoblox BloxOne. This applies to the first time the connector is ran or when the connector is executed with the -hist argument. The default is 10 days, i.e. all indicators that were added to, or modified in ThreatQ during the last ten days will be pushed to Infoblox BloxOne. This is also the same date range that will be used when pulling data from InfoBlox BloxOne analytic (Threat Insight) events to upload to ThreatQ. Valid values are integers that are 0 or greater.

☐ (Optional) Add Analytic Events

Select this box if you want the connector to upload Infoblox BloxOne analytic (Threat Insight) events to ThreatQ. The data will be uploaded as ThreatQ Events with related Indicators.

(Optional) Analytic Network

(Optional) Source Network (NAT case) / On-Prem Host name / AT Endpoint

(Optional) Analytic Query IP

(Optional) Device IP that sent the DNS query

(Optional) Analytic Queried Name/Domain

(Optional) Name/Domain that was queried by an analytic event

(Optional) Analytic Policy Name

(Optional) Policy on Infoblox BloxOne that created an analytic event

(Optional) Analytic Threat Level

- ☐ LOW
- ☐ MEDIUM
- ☐ HIGH

(Optional) Threat level of an analytic event in Infoblox BloxOne

(Optional) Analytic Threat Category

(Optional) Threat category of an analytic event in Infoblox BloxOne

How frequent should we pull information from this feed?

▼

Set indicator status to...

Active

▼

Save

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/tqenv/<environment_name>/bin/tq-conn-infoblox-bloxone -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>-hist, --historical</code>	Adding this flag will enable a historical run. This will allow the integration to pull/pull data from Infoblox BloxOne that has been created or updated in the past X days, where X is the number of days provided in the the ThreatQ config UI.
<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.)
<code>-v {1,2,3}, --verbosity {1,2,3}</code>	This is the logging verbosity level where 3 means everything. The default setting is 1 (Warning).
<code>-ep, --external-proxy</code>	This allows you to use the proxy that is specified in the ThreatQ UI. This specifies an internet facing proxy, NOT a proxy to the TQ instance.

ARGUMENT	DESCRIPTION
<code>-ds, --disable-ssl</code>	Adding this flag will disable SSL verification when contacting the MISP API.

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/tqenv/<environment_name>/bin/tq-conn-infoblox-  
bloxone -c /etc/tq_labs/ -ll /var/log/tq_labs/ -v3
```

4. Save and exit CRON.

Change Log

- Version 1.0.0
 - Initial release