

ThreatQuotient



IMAP Connector Guide

Version 4.0.0

October 07, 2021

ThreatQuotient

11400 Commerce Park Dr., Suite 200
Reston, VA 20191

 **ThreatQ Supported**

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: 703.574.9893

Contents

Support	4
Versioning.....	5
Introduction	6
Prerequisites	7
Requirements	7
Timezones	7
Installation	8
Configuration	11
Usage.....	13
Command Line Arguments.....	13
CRON.....	14
Change Log.....	15

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 © 2021 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.

Versioning

- Current integration version: 4.0.0
- Supported on ThreatQ versions \geq 4.0.0

There are two versions of this integration:

- Python 2 version
- Python 3 version

Introduction

The IMAP Connector for ThreatQ enables analysts to use an email inbox for spearphish submissions as well as intelligence sharing. Attachments and forwarded spearphishing emails will automatically be parsed, with the indicators and metadata ingested into ThreatQ.

Notes

- Running the connector will look for all unread emails in the inbox folder. The unread emails will then be marked as read.
- The connector will read the entire email including the attachments. If an attachment is present, it will upload the attachment to ThreatQ as a File. The connector will also attempt to parse the file and the email body looking for indicators. If indicators are found, they will be related to the email's attachment.

Prerequisites

Review the following in order to successfully install and use the integration.

Requirements

The following is required for this connector:

- A Python 2.7 or 3.5 environment to install the custom connector.
 - If you don't have an environment, you can be created by running this command: `/opt/threatq/python/bin/python -m venv /path/to/new/env`
- The ThreatQ PyPi Repository is configured in your `/etc/pip.conf` file

Timezones

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
```

Change Time Zone Example

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

```
timedatectl set-timezone UTC
```

Installation

The connector can be installed from the ThreatQuotient repository with YUM credentials or offline via a .whl file.

⚠ 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. Install the connector using one of the following methods:

ThreatQ Repository

- a. Run the following command:

```
<> pip install tq_conn_imap
```

Offline via .whl file

To install this connector from a wheel file, the wheel file (.whl) will need to be copied via SCP into your ThreatQ instance.

- a. Download the connector whl file with its dependencies:

```
<> mkdir /tmp/tq_conn_imap  
  
pip download tq_conn_imap -d  
/tmp/tq_conn_imap/
```

- b. Archive the folder with the .whl files:

```
<> tar -czvf tq_conn_imap.tgz /tmp/tq_conn_imap/
```

- c. Transfer all the whl files, the connector and all the dependencies, to the ThreatQ instance.
- d. Open the archive on ThreatQ:

```
<> tar -xvf tq_conn_imap.tgz
```

- e. Install the connector on the ThreatQ instance.



The example assumes that all the whl files are copied to `/tmp/conn` on the ThreatQ instance.

```
<> pip install /tmp/conn/ tq_conn_imap-<version>-<python
version>-none-any.whl --no-index --find-links /tmp/conn/
```



A driver called `tq-conn-imap` will be installed. After installing with `pip` or `setup.py`, a script stub will appear in `/usr/bin/tq-conn-imap`.

2. 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
```

3. Perform an initial run using the following command:

```
<> tq-conn-imap -v3 -ll /var/log/tq_labs/ -c /etc/tq_labs/
```

4. 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.
Email Address	This is the User in the ThreatQ System for integrations.
Password	The password for the above ThreatQ account.
Status	This is the default status for objects that are created by this Integration.

PARAMETER	DESCRIPTION
	Your organization SOPs should be respected when setting this field.

Example Output

```
tq-conn-imap -v3 -ll /var/log/tq_labs/ -c /etc/tq_labs/  
ThreatQ Host: <ThreatQ Host IP or Hostname>  
ThreatQ Client ID: <ClientID>  
E-Mail Address: <EMAIL ADDRESS>  
Password: <PASSWORD>  
Status: Active  
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 to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
IMAP Server	The IMAP server associated with the email provider you want to connect with.
IMAP Username	The username/email to log into.
IMAP Password	The password associated with your username/email.
Proxy Address	Optional - Socks proxy address used to connect to the IMAP server. <div> This cannot be a HTTP/HTTPS proxy, which is why the proxy settings within ThreatQ will not be used.</div>
Proxy Port	Optional - The port associated with the proxy address field.
Proxy Type	Optional - The type of proxy that will be used. Options include: <ul style="list-style-type: none">• <i>socks4</i>

PARAMETER

DESCRIPTION

- *socks5*

5. Review any additional settings available, 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:

```
<> tq-conn-imap -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>-ll LOGLOCATION, --loglocation LOGLOCATION</code>	Sets the logging location for the connector. The location should exist and be writable by the current.
<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 oath, etc.)
<code>-v {1,2,3}, --verbosity {1,2,3}</code>	This is the logging verbosity level where 3 means everything.
<code>-n, --name</code>	Name of the connector. This allows you to configure multiple Intelligence Mailbox connector instances on the same TQ instance.

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 hour.

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 Hour Example

```
<> 0 * * * * tq-conn-imap -c /etc/tq_labs/ -ll /var/log/tq_labs/  
-v3
```

4. Save and exit CRON.

Change Log

- **Version 4.0.0**
 - Added python 3 support.
 - Fixed a bug regarding emails and attachments.
- **Version 3.2.0**
 - Fixed a bug with decoding certain attachments that contained ascii characters.
 - Forwarded messages will now be treated as a spearphish to utilize ThreatQ's spearphish parser. eml files that are attached to emails will still be parsed using the ThreatQ spearphish parser