ThreatQuotient

Email Alerts Connector Guide

Version 1.1.1

January 10, 2022

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

Not Supported

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.

Support

This integration is designated as **Not Supported**.

Integrations, apps, and add-ons designated as **Not Supported** are not supported by ThreatQuotient's Customer Support team.

While you can report issues to ThreatQ's Customer Support team regarding the integration/app/add-on, you are solely responsible for ensuring proper functionality and version compatibility of Not Supported designations with the applicable ThreatQuotient software.

If unresolvable functional or compatibility issues are encountered, you may be required to uninstall the integration/app/add-on from your ThreatQuotient environment in order for ThreatQuotient to fulfill support obligations.

> ⚠ For ThreatQuotient Hosted instance customers, the Service Level Commitment and Service Level Credit in the ThreatQuotient Service Level Schedule will not apply to issues caused by Not Supported integrations/apps/add-ons.

Versioning

- Current integration version: `1.1.1`
- Compatible with ThreatQ versions >= `4.0.0`
- ThreatQ Alerts Service Library version >= `1.4.1`

Introduction

The Email Alerts Connector for ThreatQ operates as an alert/notification system for ThreatQ. The connector will send emails to a specified email address when the following changes occur:

- Watchlist changes
- Data collection updates

⚠ The Email Alerts Connector requires that the ThreatQ Alerts Service Library.

Prerequisites

The following is required in order to successfully install and run the Email Alerts Connector.

Timezone

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
```

ThreatQ Alerts Service Library

The Email Alerts Connector requires ThreatQ Alerts Service, with a version equal to or greater than 1.4.0, on your ThreatQ instance.

The ThreatQ Alerts Service Library can be downloaded from the ThreatQ Marketplace.

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_email_alerts
   ```

   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_email_alerts

   pip download tq_conn_email_alerts -d

   /tmp/tq_conn_email_alerts/
   ```

   b. Archive the folder with the .whl files:

   ```
   tar -czvf tq_conn_email_alerts.tgz /tmp/
   tq_conn_email_alerts/
   ```

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

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

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-email-alerts -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.
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.

PARAMETER	DESCRIPTION
Status	This is the default status for objects that are created by this Integration. Organization SOPs should be respected when setting this parameter.

Example Output

```
tq-conn-email-alerts -v3 -ll /var/log/tq_labs/ -c /etc/tq_labs/
ThreatQ Host: <ThreatQ Host IP or Hostname>
Client ID: <ClientID>
E-Mail Address: <EMAIL ADDRESS>
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 connector:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Labs** option from the *Category* dropdown (optional).

   > If you are installing the connector for the first time, it will be located under the **Disabled** tab.

3. Click on the connector to open its details page.
4. Enter the following parameters:

PARAMETER	DESCRIPTION
ThreatQ Hostname/IP	The hostname/IP address that you access ThreatQ from in your browser. This is used to link notifications directly to your ThreatQ instance
Email	The email address you want to use to send emails.
Skip Login	Specify if a login to the SMTP server is required to send emails.
Username	The username for the email account if different than the Email parameter.
Password	The password to authenticate with the specified email list in the Username parameter.
Port	The port used by your SMTP server to send emails.
Use SSL	Specify whether use SSL to connect to the SMTP server.

PARAMETER	DESCRIPTION
Recipients	A comma-delimited list of email addresses to receive the notifications.
Enable Watchlist Notifications	Select if you want to enable notifications on your watchlist.
Watchlist Users	A comma-delimited list of users (names or emails) you want to check the watchlist for changes.
Enable Data Collection Notifications	Select if you want to enable notifications on a data collection changes.
Data Collection Name	The name of the Data Collection you want to receive notifications on.
Data Collection Object Selection	Check one or more objects that you want to to be alerted on
Notification Frequency (Saved Search)	Select when you receive notifications on the Saved Search/ Data Collection list in the Saved Search Name parameter. Options include: • Only notify when new items are created. • Notify anytime an item is added or updated with context.

5. 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-email-alerts -v3 -ll /var/log/tq_labs/ -c /etc/tq_labs/
```

Command Line Arguments

ARGUMENT	DESCRIPTION
-v (optional)	Sets the log verbosity (3 means everything).
-c (optional)	The path to the directory where you want to store your config file.
-ll (optional)	The path to the directory where you want to store your logs.
-n, --name (optional)	Name of the connector (Option used in order to allow users to configure multiple McAfee ATD connector instances on the same TQ box)

> All location-based options default to the current working directory if they are not provided. Invoke the program with `-h` to find additional options and option descriptions.

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 * * * tq-conn-email-alerts -c /etc/tq_labs/ -ll /var/log/tq_labs/ -v3
   ```

4. Save and exit CRON.

Email Examples

The following are example emails sent by the connector.

ThreatQ Watchlist: Indicator Added

This message is sent when Enable Watchlist Notifications is enabled and an object is added to the watchlist of one of the Watchlist users

Body

An item in your ThreatQ watchlist has been updated!

Details

Type: Indicator Item: 7.8.9.0 Changed At: 2021-10-28 20:32:57 ThreatQ Link: https://threatq.hostname.com/indicators/8/details

ThreatQ Watchlist: Indicator Updated

This message is sent when Enable Watchlist Notifications is enabled and an object is added to the watchlist of one of the Watchlist users

Body

An item in your ThreatQ watchlist has been updated!

Details

Type: Indicator Item: 7.8.9.0 Changed At: 2021-10-28 20:32:57 ThreatQ Link: https://threatq.hostname.com/indicators/8/details What has changed?

Comment added: 2

ThreatQ Data Collection Updated: 3 New Items

This message is sent when Enable Data Collection Notifications is enabled and a new object matches the filter of the specified data collection. Each item in the list is linked to its object details page in ThreatQ

Body

The following items have been updated in your data collection

Indicators 7.8.9.0 1.2.3.4 5.6.7.8

Change Log

- **Version 1.1.1**
    - Added a new configuration option, **Data Collection Object Selection**, to allow data collection notifications to be sent based on updates to a specific object type. See the Configuration chapter for more details.
    - Added Email examples to the Usage chapter of this guide.
- **Version 1.1.0**
    - Added a configuration option to allow sending emails without a login.
    - Added a configuration parameter, **Username**, to allow specifying a separate username if different from the one supplied in the Email parameter.
    - Added a configuration option to connect to SMTP using SSL (Previously SMTP over SSL was required)
- **Version 1.0.0**
    - Initial Release