

ThreatQuotient



Email Alerts Connector Guide

Version 1.2.0

December 13, 2022

ThreatQuotient

20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

 Not Actively Supported

Contents

Integration Details	5
Introduction	6
Prerequisites	7
Time Zone	7
ThreatQ Alerts Service Library	7
Integration Dependencies	7
Installation	9
Configuration	11
Usage	13
Command Line Arguments	13
CRON	15
Email Examples	16
ThreatQ Watchlist: Indicator Added	16
ThreatQ Watchlist: Indicator Updated	16
ThreatQ Data Collection Updated: 3 New Items	17
Change Log	18

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 © 2022 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 **Not Actively Supported**.

Integrations, apps, and add-ons designated as **Not Actively 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 Actively Supported integrations/apps/add-ons.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.2.0
Compatible with ThreatQ Versions	>= 4.0.0
ThreatQ Alerts Library Version	1.5.0
Python Version	2.7
Support Tier	Not Actively Supported
ThreatQ Marketplace	https://marketplace.threatq.com/details/email-alerts-connector

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 the ThreatQ Alerts Service Library.

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
```

ThreatQ Alerts Service Library

The Email Alerts Connector requires ThreatQ Alerts Service, with a version equal to or greater than 1.5.0, on your ThreatQ instance.

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

Integration Dependencies

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
requests	N/A	N/A
threatqsdk	=>1.7.0	N/A
threatqcc	=>1.3.0	N/A
tq-alert-server	>=1.5.0	N/A

Installation

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

```
<> pip install /tmp/tq_conn_email_alerts-<version>-py2-none-any.whl
```



A driver called tq-conn-email-alerts will be installed. After installing, a script stub will appear in /usr/bin/tq-conn-email-alerts.

4. 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/
```

5. Perform an initial run using the following command:

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

6. 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

```
tq-conn-email-alerts -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
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.
Recipients	A comma-delimited list of email addresses to receive the notifications.

PARAMETER	DESCRIPTION
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. 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 commands to execute the driver:

Tasks, Watchlists, or Data Collections

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

Send Generic Email with Subject and Body

```
<> tq-conn-email-alerts -ll /var/log/tq_labs/ -c /etc/tq_labs/  
  '{"email_subject": "This is a test subject", "email_body": "Test  
  email body"}' -v3
```

Command Line Arguments

This connector supports the following custom command line arguments:

ARGUMENT	DESCRIPTION
<code>-h, --help</code>	Review all additional options and their descriptions.
<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 oath, etc.)
<code>-v {1,2,3}, --verbosity {1,2,3}</code>	This is the logging verbosity level where 3 means everything.

ARGUMENT	DESCRIPTION
<code>-p, --payload</code>	Provides the option to send free form emails by passing a JSON payload with email subject and body. For example: <i>tq-conn-email-alerts -c /etc/threatq/ -l /var/log/threatq/ -p '{"email_subject": "This is a test subject", "email_body": "Test email body"}' -v3</i>

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
```

Send Generic Email Example

```
<> 0 */3 * * * AGDSFILES=$(ls -Art /opt/tq_labs/agds/
tqSync*.tar.gz | sed "s/.*\//" | sed -e 'H;${x;s/\n/, /g;s/
^, //;p;};d'); if [ $? -eq 0 ]; then /opt/tqvenv/venv27/bin/
tq-conn-email-alerts -c /opt/tq_labs/config/ -ll /opt/tq_labs/
log/ -v3 -p '{"email_subject": "ThreatQ AGDS files are waiting
to be imported", "email_body": "The following files need to be
imported: '"${AGDSFILES}"'"'; else echo 0; fi
```

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 1.2.0**
 - Added the ability to send free form emails by passing a JSON payload to the executable.
 - Updated **Usage** and **CRON** chapters.
- **Version 1.1.2**
 - Updated installation steps. (rev-a)
 - Fixed an issue regarding honoring the configured data collection by name.
- **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