# ThreatQuotient

# ThreatQuotient for Report Emailer Operation

Version 1.0.0

August 21, 2019

ThreatQuotient

11400 Commerce Park Dr., Suite 200

Reston, VA 20191

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: + 1 703.574.9893

# 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.

Last Updated: Wednesday, August 21, 2019

# Contents

# List of Figures and Tables

# 1 Introduction

## 1.1 Application Function

The ThreatQuotient Report Emailer Operation allows a ThreatQ user to email a PDF report directly from an object within ThreatQ.

## 1.2 Preface

This guide provides the information necessary to implement the ThreatQuotient Report Emailer Operation. This document is not specifically intended as a site reference guide. It is assumed that the implementation engineer has experience installing and commissioning the ThreatQuotient Apps and integrations covered within the document, as well as the experience necessary to troubleshoot at a basic level.

## 1.3 Audience

This document is intended for use by the following parties:

1. ThreatQ and Security Engineers
2. ThreatQuotient Professional Services Project Team & Engineers

## 1.4 Scope

This document covers the implementation of the ThreatQuotient Report Emailer Operation only.

***Table 1: ThreatQuotient Software & App Version Information***

| Software/App Name | File Name | Version |
|---|---|---|
| ThreatQ | Version 4.20.x or greater | |
| ThreatQuotient Report Emailer Operation | 1.0.0 | |

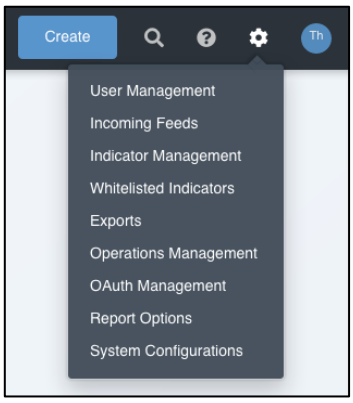
# 2 ThreatQuotient for Report Emailer Operation Installation

## 2.1 Setting up the Integration

Ensure the file `tq_op_report_emailer-1.0.0-py3-none-any.whl` is available on the device being used to administer the ThreatQ instance in which the ThreatQuotient Report Emailer Operation is being installed/upgraded.

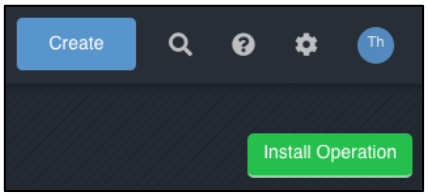
1. Navigate to the **Settings icon** > **Operations Management**.

***Figure 1: Operations Management – Install***




2. Click **Install Operation** in the upper right corner.

***Figure 2: Install Operation***




3. Drag the `tq_op_report_emailer-1.0.0-py3-none-any.whl` to the Add Operation Popup or **Click to Browse** to the required file.
4. Click **Install** or **Upgrade**.

You may be presented with **OPERATION ALREADY INSTALLED** as shown below.

***Figure 3: Add Operation***

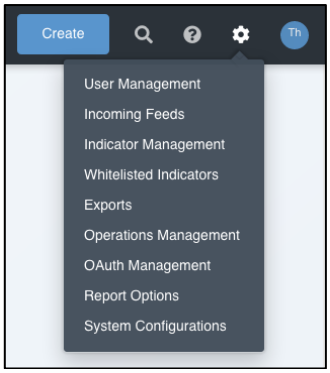

Installation/upgrade is now complete.

## 2.2 Configuring the Operation

The following section covers the configuration of the ThreatQuotient Report Emailer Operation.

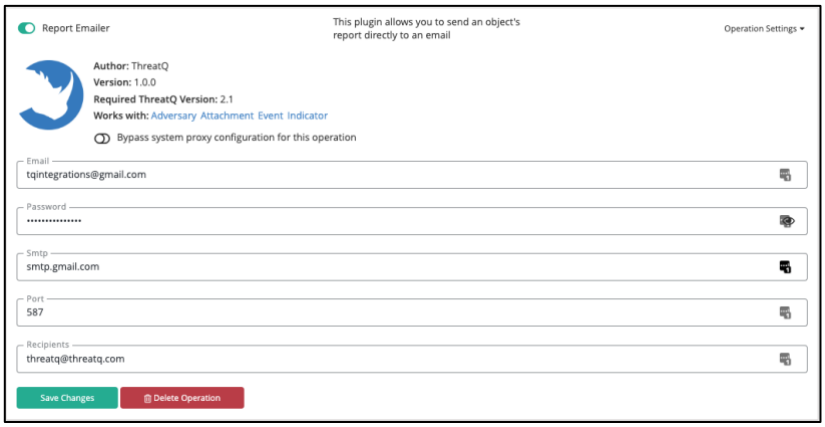
1. Navigate to the **Settings icon > Operations Management.**

***Figure 4: Operations Management – Configuration***




2. Expand the **Report Emailer** Operation Settings configuration.

***Figure 5: Operation Configuration***




3. **Sender Email:** The email you want to use to send the reports
4. **Sender Password:** The password associated with the sender email
5. **SMTP Server:** The SMTP server used by your email provider
    - See below for some common SMTP servers (and ports)
6. **SMTP Port:** The port associated with the SMTP server
    - See below for some common SMTP servers (and ports)
7. **Default Recipients:** A comma-delimited list of email addresses to receive the reports
    - This can be overridden when running the operation
8. Click the toggle in next to the **Report Emailer** name to enable the operation.

**Common SMTP Configurations:**

- **Gmail:** smtp.gmail.com:587
- **Office 365:** smtp.office365.com:587
- **Outlook:** smtp-mail.outlook.com:587

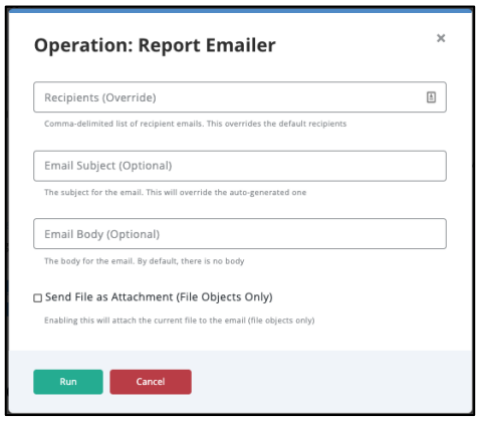
## 2.3 Using the Operation

The following section covers the use of the ThreatQuotient for Report Emailer Operation.

### 2.3.1 Send

This action will send an email (with the PDF attachment) to the specified recipients.

***Figure 6: Report Emailer Send Submit Example***




1. **Recipients (Override):** If needed, you can override the default recipients that were specified in the configuration page.
2. **Email Subject (Optional):** You can override the auto-generated subject using this input.
3. **Email Body (Optional):** You can set a body for the email here. By default, there is no body.
4. **Send File as Attachment (*File Objects Only*):** Enabling this option will attach the current file object to the email.
    - This will only work for File objects.

**Results**
Example result of running the operation:

***Figure 7: Report Emailer Response Example***


Here is what the email will look like in your inbox (for Gmail). The look will vary depending on your email provider.

***Figure 8: Report Emailer Received Email Example***

### 2.3.2 Supplemental

The operation can only be run from the following ThreatQ Base Objects:

- Indicators
- Adversaries
- Events
- Attachments
- STIX 1.2 Objects
    - TTPs
    - Campaigns
    - Courses of Action
    - Exploit Target
    - Incident

# Trademarks and Disclaimers

THE SUBJECT AND SPECIFICATIONS INCLUDING ALL INFORMATION REGARDING THE PRODUCTS IN THIS DOCUMENT ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENT ARE BELIEVED TO BE ACCURATE AT THE TIME OF WRITING BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE TERMS AND CONDITIONS WHEN PURCHASED. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR THREATQUOTIENT REPRESENTATIVE FOR A COPY.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THIRD PARTY SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. THREATQUOTIENT AND THIRD-PARTY SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL THREATQUOTIENT OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF THREATQUOTIENT OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

It is wholly the customers responsibility for any design requirements and the utilization of any recommendations provided by ThreatQuotient. ThreatQuotient recommendations are based upon customer information provided to ThreatQuotient at the time of the services. ThreatQuotient shall not be liable for the accuracy or completeness of the customer information contained in the ThreatQuotient recommendations.

All documentation and deliverables shall be provided in the English language, unless specifically stated otherwise. or agreed before the commencement of any services in writing.
Any costs incurred by ThreatQuotient as a result of translations requested by Customer shall be Customer’s responsibility.
In the event of any conflict between this English version and the translation(s), the English version will prevail.

ThreatQuotient and the ThreatQuotient Rhino Logo are trademarks of ThreatQuotient, Inc.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.