ThreatQuotient

ThreatQuotient for McAfee ESM Operation

v.0.4.0

Wednesday, April 1, 2020

ThreatQuotient

11400 Commerce Park Dr., Suite 200

Reston, VA 20191

Support

Email: support@threatq.com

Web: Support.threatq.com

Phone: 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.

Contents

Introduction

Application Function

The ThreatQuotient for McAfee ESM Operation allows a ThreatQ user to add geolocation attributes and related indicators (if available) of IP Addresses within ThreatQ.

Preface

This guide is to provide the information necessary to implement the ThreatQuotient for McAfee ESM Operation. This document is not specifically intended to form a site reference guide.

It is assumed that the implementation engineer has experience installing and commissioning ThreatQuotient Apps and integrations covered within the document, as well as experience necessary to troubleshoot at a basic level.

Audience

This document is intended for use by the following parties:

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

Scope

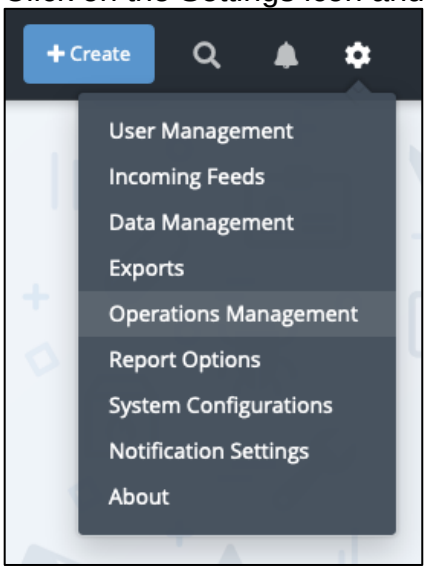
This document covers the implementation of the application only.

Software/App Name	File Name	Version
ThreatQ Platform	Version 4.30.0 or greater	
ThreatQuotient for McAfee ESM Operation	0.0.4	

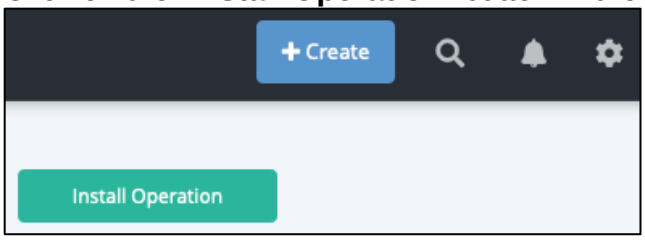
Installation

The following section guides a user through the installation of operations.

1. Ensure the operation file `tq_op_mcafee_esm-<version>-<Python version>-none-any.whl` is available on the device being used to administer the ThreatQ instance and is being installed/upgraded.
2. Navigate to your ThreatQ instance.
3. Click on the Settings icon and select Operations Management.

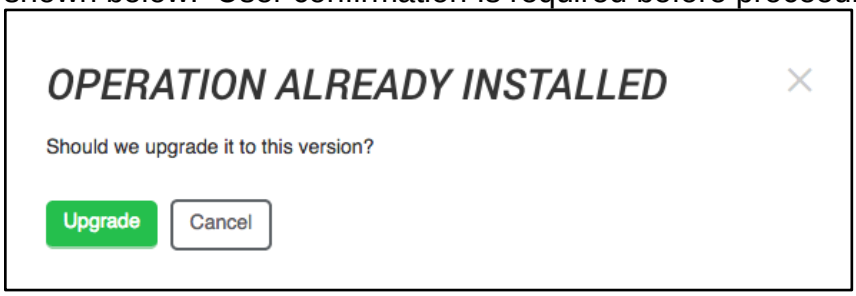


4. Click on the "**Install Operation**" button in the upper right corner.



5. Upload the operation file using one of the following methods:
    - Drag and drop the file into the dialog box
    - Select **Click to Browse** to locate the operation file on your local machine

You may be presented with "**OPERATION ALREADY INSTALLED**" as shown below. User confirmation Is required before proceeding.

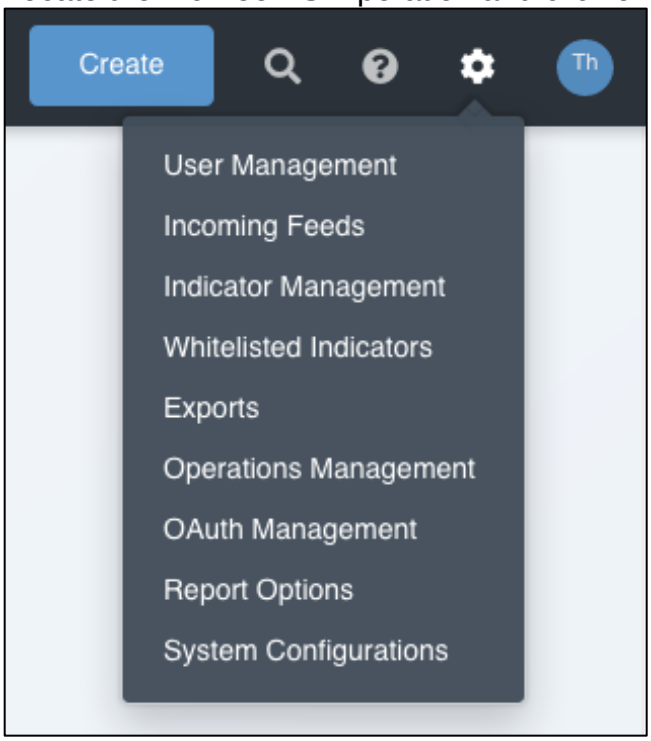


Installation/Upgrade is now complete. You will still need to configure and then enable the operation.

Configuring the Operation

The following section covers the configuration of the ThreatQuotient for McAfee ESM Operation.

1. Click on the Settings icon and select Operations Management.
2. Locate the McAfee ESM peration and click on **Operation Settings**.

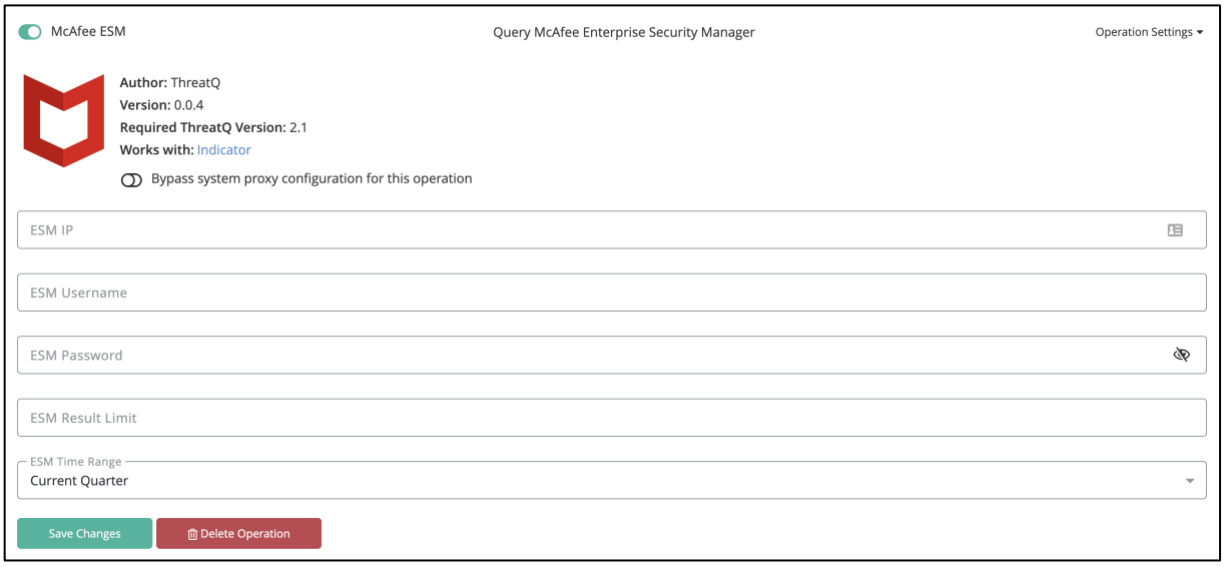


3. Enter the following parameters for the operation:
   - **ESM IP:** IP or Hostname of the McAfee ESM instance
   - **ESM Username:** Username for logging to ESM
   - **ESM Password:** Password for logging to ESM
   - **ESM Result Limit:** The maximum number of sightings to show
   - **ESM Time Range:** The historical time period on which to perform the query (default value is Current Quarter).
     - The possible Time Range Values are:

Last Minute	Previous Day	Previous Week
Last 10 Minutes	Last 24 Hours	Current Month
Last 30 Minutes	Last 48 Hours	Previous Month
Last Hour	Last 72 Hours	Current Quarter
Current Day	Current Week	Previous Quarter

Current Year Previous Year All

Figure 1: Operation Configuration



4. Click on **Save Changes**.
5. Click the toggle in next to the "**McAfee ESM**" name to enable the operation

Document Change Log

Version	Details
1.0.0	Initial Document Release