

# ThreatQuotient



## Trellix ePO Operation Guide

Version 2.0.0

May 22, 2023

**ThreatQuotient**

20130 Lakeview Center Plaza Suite 400  
Ashburn, VA 20147



ThreatQ Supported

### Support

Email: [support@threatq.com](mailto:support@threatq.com)

Web: [support.threatq.com](https://support.threatq.com)

Phone: 703.574.9893

# Contents

- Integration Details..... 5
- Introduction ..... 6
- Prerequisites..... 7
  - Asset Object ..... 7
- Installation..... 9
- Configuration ..... 10
- Actions ..... 12
  - Manage Tags - Apply..... 13
  - Manage Tags - Exclude..... 13
  - Manage Tags - Clear ..... 13
  - Get System Information ..... 13
- Change Log..... 14

# 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 © 2023 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](mailto: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.

# Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	2.0.0
--------------------------------	-------

Compatible with ThreatQ Versions	>= 4.40.0
-------------------------------------	-----------

McAfee ePolicy Orchestrator (ePO) Versions	5.9.0
--	-------

Support Tier	ThreatQ Supported
--------------	-------------------

# Introduction

The Trellix ePolicy Orchestrator (ePO) operation allows users to manage system tags in Trellix ePO.

The operation provides the following actions:

- **Manage Tags Apply** - applies tag(s) to systems in ePO.
- **Manage Tags Exclude** - adds exclude tag(s) to systems in ePO.
- **Manage Tags Clear tags** - removes tag(s) from systems in ePO.
- **Get System Information** - prints the complete information about the endpoint from ePO.

The operation is compatible with the Assets custom object type.


# Prerequisites

The following is required in order to install and run the operation:


- **Assets** object installed on your ThreatQ instance.
- Route between ThreatQ and Trellix ePO.
- Trellix products:
  - ePO with an installed Endpoint Security extension
- Trellix ePO username and password to use with the integration

## Asset Object

The integration requires the Asset object. The Asset installation files are included with the integration download on the ThreatQ Marketplace. The Asset object must be installed prior to installing the integration.

 You do not have to install the Asset object if you are running ThreatQ version 5.10.0 or greater as the object has been seeded as a default system object.

Use the steps provided to install the Asset custom object.

 When installing the custom objects, be aware that any in-progress feed runs will be cancelled, and the API will be in maintenance mode.

1. Download the custom object zip file from the ThreatQ Marketplace and unzip its contents.
2. SSH into your ThreatQ instance.
3. Navigate to tmp directory:

```
<> cd /tmp/
```

4. Create a new directory:

```
<> mkdir trellix_epo
```

5. Upload the **asset.json** and **install.sh** script into this new directory.
6. Create a new directory called **images** within the **trellix\_epo** directory.

```
<> mkdir images
```

7. Upload the asset.svg.
8. Navigate to the `/tmp/trellix_epo`.

The directory should resemble the following:

- tmp
  - trellix\_epo
    - asset.json
    - install.sh
    - images
      - asset.svg

9. Run the following command to ensure that you have the proper permissions to install the custom object:

```
<> chmod +x install.sh
```

10. Run the following command:

```
<> sudo ./install.sh
```



You must be in the directory level that houses the `install.sh` and `json` files when running this command.

The installation script will automatically put the application into maintenance mode, move the files to their required directories, install the custom object, update permissions, bring the application out of maintenance mode, and restart dynamo.

11. Remove the temporary directory, after the custom object has been installed, as the files are no longer needed:

```
<> rm -rf trellix_epo
```



# Installation



The operation requires the installation of a custom object before installing the actual operation if you are on ThreatQ version 5.9.0 or earlier. See the Prerequisites chapter for more details. The custom object must be installed prior to installing the operation. Attempting to install the operation without the custom object will cause the operation install process to fail.

Perform the following steps to install the integration:



The same steps can be used to upgrade the integration to a new version.

1. Log into <https://marketplace.threatq.com/>.
2. Locate and download the integration file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration file using one of the following methods:
  - Drag and drop the file into the dialog box
  - Select **Click to Browse** to locate the integration file on your local machine



ThreatQ will inform you if the operation already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the operation contains changes to the user configuration. The new user configurations will overwrite the existing ones for the operation and will require user confirmation before proceeding.

The operation is now installed and will be displayed in the ThreatQ UI. You will still need to [configure and then enable](#) the operation.

# 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 **Operation** option from the *Type* dropdown (optional).
3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
EPO Hostname	The hostname or IP address for ePO.
ePO Port	The ePO communication port. The default is 8443 and can be changed if needed.
ePO Username	Your username for ePO.
ePO Password	Your password for ePO.
Verify SSL	Check this option to verify your certificate when connecting to Trellix ePO.



Disabled ☒ Enabled

Uninstall

#### Additional Information

Integration Type: Operation

Author: ThreatQ

Description: Manage system tags in Trellix ePO

Version: 2.0.0

Works With:

Asset

#### Configuration

ePO Hostname

Enter the hostname or IP address for ePO

ePO Port

8443

Enter the ePO communication port. The default is 8443, which can be changed if needed

ePO Username

Enter the username for ePO

ePO Password

Enter the password for ePO

☐ Verify  
SSL

Check this box to verify SSL when connecting to Trellix ePO.

☐ Bypass system proxy configuration for this operation

Save

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.

# Actions

The operation provides the following actions:

ACTION	ACTION SUBTYPE	DESCRIPTION	OBJECT TYPE
Manage Tags	<a href="#">Apply</a>	Apply tag(s) to systems in ePO.	Asset
Manage Tags	<a href="#">Exclude</a>	Add exclude tag(s) to systems in ePO.	Asset
Manage Tags	<a href="#">Clear</a>	Remove tag(s) from systems in ePO.	Asset
<a href="#">Get System Information</a>	N/A	Prints the complete information about the endpoint from ePO.	Asset

---

## Manage Tags - Apply

The Manage Tags - Apply action applies tag(s) to systems in ePO.

POST `https://<Trellix ePO Host>/remote/system.applyTag`

## Manage Tags - Exclude

The Manage Tags Exclude action adds excluded tag(s) to systems in ePO.

POST `https://<Trellix ePO Host>/remote/system.excludeTag`

## Manage Tags - Clear

The Manage Tags - Clear action removes tags from systems in ePO.

POST `https://<Trellix ePO Host>/remote/system.clearTag`

## Get System Information

The Get System Information action prints the complete information about the endpoint from ePO.

POST `https://<Trellix ePO Host>/remote/system.find`

# Change Log

- **Version 2.0.0**
  - Rebranded integration from McAfee ePO to Trellix ePO
  - Resolved a bug regarding Asset naming.
- **Version 1.0.0 rev-a (Guide Update)**
  - Updated the Prerequisites chapter regarding the Asset object. ThreatQ version 5.10.0 introduced the Asset object as a seeded default system object. Users on ThreatQ 5.10.0 or later do not have to install the Asset custom object prior to installing the integration.
- **Version 1.0.0**
  - Initial release