ThreatQuotient

McAfee MVISION Operation Guide

Version 1.0.0

November 02, 2021

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 `1.0.0`
- Compatible with ThreatQ versions >= `4.35.0`

Introduction

The McAfee MVISION Operation for ThreatQ enables analysts to fetch enrichment context from Insights as well perform actions on their hosts, such as adding or removing tags.

The operation can be run on the following object types:

- Assets (custom object)
- Indicators (all sub-types)

Prerequisites

The following prerequisites are required in order to use the operation.

- Asset Custom Object
- McAfee MVISION Client Credentials
- Appropriate Client ID/Secret Credentials Access

Asset Custom Object Installation

Use the following steps 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. Locate the custom object files in the zip file you downloaded from the ThreatQ Marketplace. Custom Object files include:
   - asset.json
   - asset.svg
2. SSH into your ThreatQ instance.
3. Unzip and then copy the custom objects files to directory of your choice.

   > ThreatQuotient recommends uploading the files to the `/var/www/api/database/seeds/data/custom_objects/`.

4. Navigate to the API directory:

   ```
   cd /var/www/api
   ```

5. Put your ThreatQ instance into maintenance mode:

   ```
   sudo php artisan down
   ```

6. Run the following command to install the Custom Object Definition:

   ```
   sudo php artisan threatq:make-object-set --file=<Path To JSON
   File>

   sudo php artisan threatq:object-settings --code=object --
   ```

```
icon=<Path To Icon Folder>/asset.svg --background-
color='#03ac14'
```

7. Clear the ThreatQ object cache and update permissions:

```
sudo php /var/www/api/artisan cache:clear

sudo php /var/www/api/artisan threatq:update-permissions
```

8. Take your ThreatQ instance out of maintenance mode and restart Dynamo:

```
sudo php artisan up

sudo systemctl restart threatq-dynamo
```

Generating MVISION Client Credentials (API Keys)

Client Credentials (API Keys) are obtained via McAfee's MVISION Marketplace:

https://www.mcafee.com/enterprise/en-us/solutions/mvision/marketplace.html

As of this publication, ThreatQuotient does not have a *configurable* entry in the MVISION Marketplace. You can utilize the **IBM Security App for QRadar** to generate Client Credentials required for this operation.

Perform the following steps to generate Client Credentials:

1. Navigate to the McAfee MVISION Marketplace.
2. Enter `McAfee MVISION App for IBM QRadar` in the search bar and select the auto-completed entry.
3. Click on the **Configure** button for the marketplace entry.
4. Enter a value in the **Instance URL** field.

   > This can be anything you want. You don't need an actual QRadar instance to connect to. Enter `https://127.0.0.1` if you do not have a QRadar instance.

5. Click on the **Refresh** button located above the Client Credential fields.
6. Check the box agreeing to McAfee's user-agreements.
7. Click the **Connect** button to save the configuration.
8. Copy your `McAfee API Key`, `Client ID`, and `Client Secret`, and store them in a safe location.

Client ID/Secret Credentials Access

Confirm that your Client ID/Secret Credentials have access to the following scopes:

- ins.user
- ins.suser
- ins.ms.r
- epo.device.r
- epo.device.w
- epo.tags.r
- epo.tags.w
- epo.evt.r
- epo.taggroup.r

Installation

⚠ The integration requires the installation of a custom object before installing the actual operation. See the Prerequisites chapter for more details before proceeding with installation.

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 feed 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.

6. 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).

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

3. Click on the integration to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
API Key	Your McAfee API Key which is retrieved from the Developer Portal (x-api-token).
McAfee Cloud Client ID	Your McAfee Cloud Client ID to authenticate.
McAfee Cloud Client Secret	Your McAfee Cloud Client Secret to authenticate.

5. Click **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable the operation.

Actions

ACTION	DESCRIPTION	OBJECT TYPES	OBJECT SUB-TYPE
Enrich	Enrich an indicator with context from McAfee MVISION.	Indicators	All
Add Tag	Adds a tag to a device in McAfee MVISION.	Asset	N/A
Remove Tag	Removes a tag from a device in McAfee MVISION.	Asset	N/A

Enrich

This action enriches an indicator with context from McAfee MVISION.

`GET https://api.mvision.mcafee.com/insights/v2/iocs`

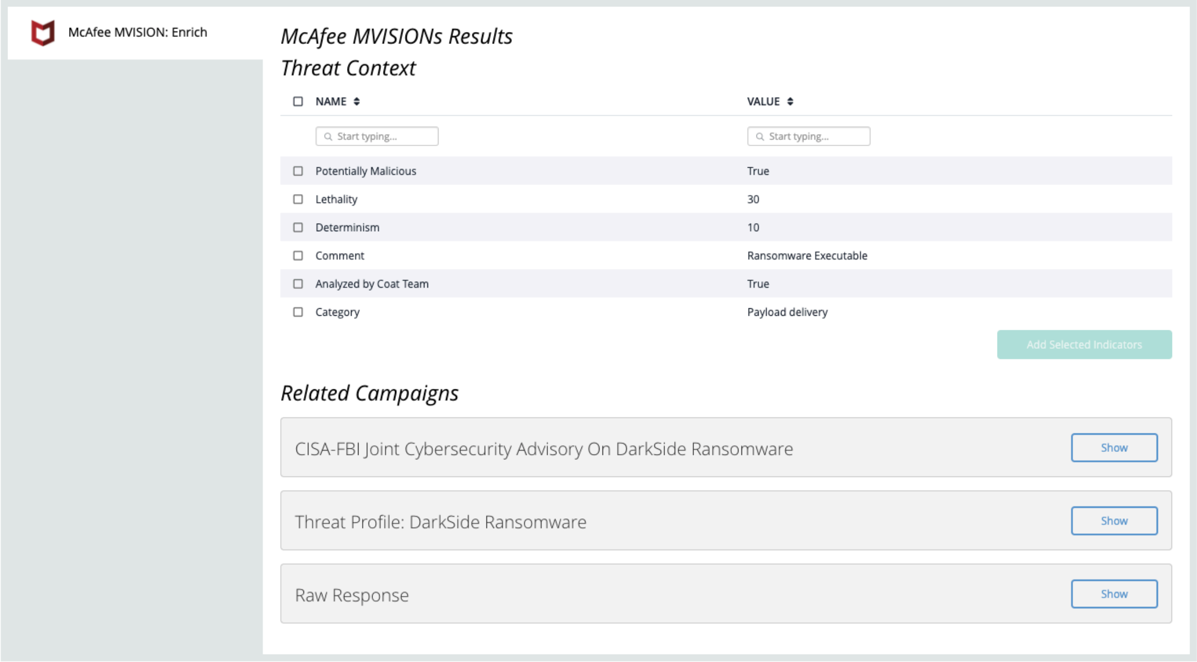
```
{
    "links": {
        "self": "https://api.mvision.mcafee.com/insights/v2/iocs?include=threat&page[limit]=2&page[sort]=updated-on",
        "first": "https://api.mvision.mcafee.com/insights/v2/iocs?include=threat&page[limit]=2&page[sort]=updated-on&page[offset]=0",
        "last": "https://api.mvision.mcafee.com/insights/v2/iocs?include=threat&page[limit]=2&page[sort]=updated-on&page[offset]=169348",
        "prev": null,
        "next": "https://api.mvision.mcafee.com/insights/v2/iocs?include=threat&page[limit]=2&page[sort]=updated-on&page[offset]=2"
    },
    "data": [
        {
            "type": "iocs",
            "id": "00002945-edb8-11ea-9477-02d538d9640e",
            "links": {
                "self": "https://api.mvision.mcafee.com/insights/v2/iocs/00002945-edb8-11ea-9477-02d538d9640e"
            },
            "attributes": {
                "type": "md5",
                "value": "13cddf1941005919220c8eb9846cd170",
                "coverage": {
                    "dat_version": {
                        "min": 3705
                    }
                },
                "uid": "6973ee45-4d39-4d4d-beb1-050434886fc5",
                "is-coat": 1,
                "is-sdb-dirty": 1,
                "category": "Artifacts dropped",
                "comment": "",
                "lethality": null,
                "determinism": null,
                "threat": {
                    "id": "4887026d-881a-e841-6ac9-ebac7ed3f84c",
                    "name": "Generic Trojan-Downloader",
                    "classification": "Trojan",
                    "severity": 1
                }
            },
            "relationships": {
                "campaigns": {
                    "links": {
                        "self": "https://api.mvision.mcafee.com/insights/v2/iocs/00002945-
edb8-11ea-9477-02d538d9640e/relationships/campaigns",
                        "related": "https://api.mvision.mcafee.com/insights/v2/iocs/00002945-
edb8-11ea-9477-02d538d9640e/campaigns"
                    }
                }
            }
        },
        {
            "type": "iocs",
            "id": "000038dd-b04f-11ea-9477-02d538d9640e",
            "links": {
                "self": "https://api.mvision.mcafee.com/insights/v2/iocs/000038dd-b04f-11ea-9477-02d538d9640e"
            },
            "attributes": {
                "type": "domain",
                "value": "imgsrvrer.com",
                "coverage": null,
                "uid": "5662e834-56b5-40ce-8de1-08db575d745b",
                "is-coat": 0,
                "is-sdb-dirty": 1,
                "category": "Network activity",
                "comment": "",
                "lethality": null,
                "determinism": null,
                "threat": {}
            },
            "relationships": {
                "campaigns": {
                    "links": {
                        "self": "https://api.mvision.mcafee.com/insights/v2/iocs/000038dd-
b04f-11ea-9477-02d538d9640e/relationships/campaigns",
                        "related": "https://api.mvision.mcafee.com/insights/v2/iocs/000038dd-
b04f-11ea-9477-02d538d9640e/campaigns"
                    }
                }
            }
        }
    ]
```

```
}
```

ThreatQ provides the following default mapping for this Action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].attributes.coverage.dat_version.min	Attribute	Minimum DAT Version	N/A	N/A	N/A
.data[].attributes.is-coat	Attribute	Analyzed by Coat Team	N/A	True	Bool -> True/False
.data[].attributes.is-sdb-dirty	Attribute	Potentially Malicious	N/A	True	Bool -> True/False
.data[].attributes.category	Attribute	Category	N/A	Network activity	N/A
.data[].attributes.comment	Attribute	Comment	N/A	N/A	N/A
.data[].attributes.lethality	Attribute	Lethality	N/A	N/A	N/A
.data[].attributes.determinism	Attribute	Determinism	N/A	N/A	N/A
.data[].attributes.threat.name	Attribute	Threat Name	N/A	N/A	N/A
.data[].attributes.threat.name	Attribute	Threat Name	N/A	N/A	N/A
.data[].attributes.threat.classification	Attribute	Classification	N/A	N/A	N/A
.data[].attributes.threat.severity	Attribute	Severity	N/A	N/A	Mapped from integer to string value (Unverified, Low, Medium, High, Very High)

Example



McAfee MVISIONs Results

Threat Context

NAME	VALUE
Potentially Malicious	True
Lethality	30
Determinism	10
Comment	Ransomware Executable
Analyzed by Coat Team	True
Category	Payload delivery

Related Campaigns

CISA-FBI Joint Cybersecurity Advisory On DarkSide Ransomware

Threat Profile: DarkSide Ransomware

Raw Response

Add Tag

This action adds a tag to a device in McAfee MVISION.

`GET https://api.mvision.mcafee.com/epo/v2/devices`

`GET https://api.mvision.mcafee.com/epo/v2/tags`

`GET https://api.mvision.mcafee.com/epo/v2/tagGroups`

`POST https://api.mvision.mcafee.com/epo/v2/tags`

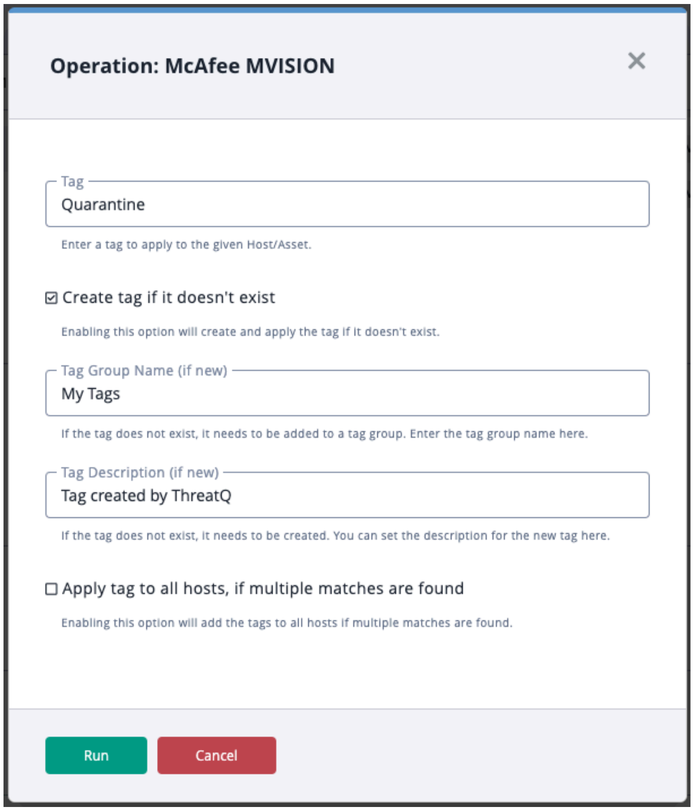
`POST https://api.mvision.mcafee.com/epo/v2/devices/{device_id}/relationships/assignedTags`

There is no sample API response to show

Parameters

ThreatQ provides the following parameters for this Action:

PARAMETER	DESCRIPTION
Tag	Enter a tag to add to the given Host/Asset.
Create tag if it doesn't exist	Enabling this option will create and apply the tag if it doesn't exist.
Tag Group Name (if new)	If the tag does not exist, it needs to be added to a tag group. Enter the tag group name here.
Tag Description (if new)	If the tag does not exist, it needs to be created. You can set the description for the new tag here.
Apply tag to all hosts, if multiple matches are found	Enabling this option will remove the tag from all hosts if multiple matches are found.



Operation: McAfee MVISION

Tag: Quarantine

Enter a tag to apply to the given Host/Asset.

☑ Create tag if it doesn't exist

Enabling this option will create and apply the tag if it doesn't exist.

Tag Group Name (if new): My Tags

If the tag does not exist, it needs to be added to a tag group. Enter the tag group name here.

Tag Description (if new): Tag created by ThreatQ

If the tag does not exist, it needs to be created. You can set the description for the new tag here.

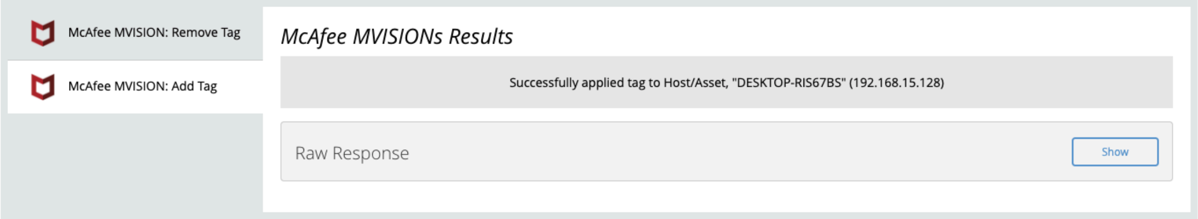
□ Apply tag to all hosts, if multiple matches are found

Enabling this option will add the tags to all hosts if multiple matches are found.

Mapping

There is no mapping for this Action.

Example



McAfee MVISIONs Results

Successfully applied tag to Host/Asset, "DESKTOP-RIS67BS" (192.168.15.128)

Remove Tag

The Remove Tag action removes a tag from a device in McAfee MVISION

```
GET https://api.mvision.mcafee.com/epo/v2/devices
```

```
GET https://api.mvision.mcafee.com/epo/v2/tags
```

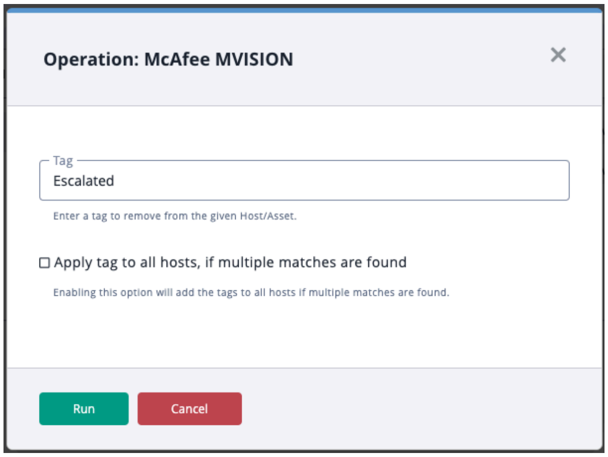
```
DELETE https://api.mvision.mcafee.com/epo/v2/devices/{device_id}/relationships/
assignedTags
```

There is no sample API response to show

Parameters

ThreatQ provides the following parameters for this Action:

PARAMETER	DESCRIPTION
Tag	Enter a tag to remove from the given Host/Asset.
Remove tags from all hosts, if multiple matches are found	Enabling this option will remove the tag from all hosts if multiple matches are found.



Operation: McAfee MVISION

Tag: Escalated

Enter a tag to remove from the given Host/Asset.

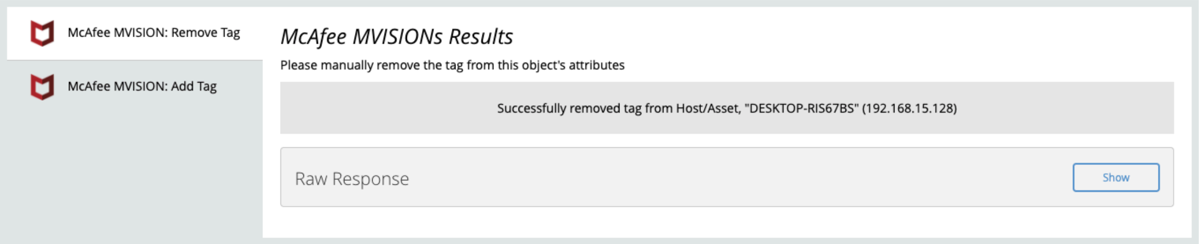
☐ Apply tag to all hosts, if multiple matches are found

Enabling this option will add the tags to all hosts if multiple matches are found.

Mapping

There is no mapping for this Action.

Example



McAfee MVISIONs Results

Please manually remove the tag from this object's attributes

Successfully removed tag from Host/Asset, "DESKTOP-RIS67BS" (192.168.15.128)

Change Log

- **Version 1.0.0**
    - Initial Release