

ThreatQuotient



McAfee MVISION Operation User Guide

Version 1.0.1 rev-a

November 06, 2023

ThreatQuotient

20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147



Support

Email: support@threatq.com

Web: support.threatq.com

Phone: 703.574.9893

Contents

Warning and Disclaimer	3
Support	4
Integration Details.....	5
Introduction	6
Prerequisites	7
Asset Custom Object	7
McAfee MVISION Client Credentials.....	8
Generating MVISION Client Credentials Access (API Keys)	8
Installation.....	10
Configuration	11
Actions	12
Enrich	13
Example Result	15
Add Tag.....	16
Action Parameters.....	16
Example Result	17
Remove Tag	18
Action Parameters.....	18
Example Result	19
Change Log	20

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

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	1.0.1
Compatible with ThreatQ Versions	>= 4.40.0
Support Tier	ThreatQ Supported

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 provides the following actions:

- **Enrich** - enriches an indicator with context from McAfee MVISION.
- **Add Tag** - adds a tag to a device in McAfee MVISION.
- **Remove Tag** - removes a tag from a device in McAfee MVISION.

The operation can be run on the following object types:

- Assets
- Indicators (all sub-types)


Prerequisites

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


- [Asset Object](#)
- [McAfee MVISION Client Credentials](#)
- [Appropriate Client ID/Secret Credentials Access](#)

Asset Custom 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 integration 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 mcafee_mvision
```

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

```
<> mkdir images
```

7. Upload the **asset.svg**
8. Navigate to the **/tmp/mcafee_mvision**.

The directory should resemble the following:

- tmp
 - mcafee_mvision
 - 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 mcafee_mvision
```

McAfee MVISION Client Credentials

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

Generating MVISION Client Credentials Access (API Keys)

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

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



As of the date of this publication, ThreatQuotient does not have a configurable entry on the MVISION Marketplace. You can use the FireEye Helix to generate the Client Credentials that are required to use ThreatQ integrations.

Perform the following steps to generate these Client Credentials using FireEye Helix:

1. Navigate to the McAfee MVISION Marketplace:
<https://www.mcafee.com/enterprise/en-us/solutions/mvision/marketplace.html>.
2. Enter **FireEye Helix** in the search bar and select the auto-completed entry.
3. Click on the **Configure** button for the marketplace entry.
4. Complete the **Instance URL** field.



The URL can be any value as you are not actually connecting to a FireEye Helix instance.

Recommendation: Enter `https://127.0.0.1` if you do not have a FireEye Helix instance.

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

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 zip file.
3. Extract the zip file's contents and install the Asset custom object if you are on ThreatQ version 5.9 or earlier.
4. Navigate to the integrations management page on your ThreatQ instance.
5. Click on the **Add New Integration** button.
6. Upload the integration .whl file using one of the following methods:
 - Drag and drop the .whl file into the dialog box
 - Select **Click to Browse** to locate the .whl 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
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 used to authenticate. See the Generating MVISION Client Credentials (API Keys) section of the Prerequisites chapter for steps to obtain McAfee Cloud credentials.
McAfee Cloud Client Secret	Your McAfee Cloud Client Secret used to authenticate. See the Generating MVISION Client Credentials (API Keys) section of the Prerequisites chapter for steps to obtain McAfee Cloud credentials.

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	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Enrich	Enriches 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

The Enrich action enriches an indicator with context from McAfee MVISION.

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

Sample Response:

```
{
  "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": "imgsrvr.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"
          }
        }
      }
    }
  ]
}

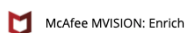
```

ThreatQuotient 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

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.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 Result



McAfee MVISIONs Results

Threat Context

NAME	VALUE
<input type="checkbox"/> Potentially Malicious	True
<input type="checkbox"/> Lethality	30
<input type="checkbox"/> Determinism	10
<input type="checkbox"/> Comment	Ransomware Executable
<input type="checkbox"/> Analyzed by Coat Team	True
<input type="checkbox"/> Category	Payload delivery

Add Selected Indicators

Related Campaigns

CISA-FBI Joint Cybersecurity Advisory On DarkSide Ransomware
Show

Threat Profile: DarkSide Ransomware
Show

Raw Response
Show

Add Tag

The Add Tag 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

Action 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.

Run

Cancel

Example Result

<div>  McAfee MVISION: Remove Tag </div>	<div>McAfee MVISIONs Results</div> <div>Successfully applied tag to Host/Asset, "DESKTOP-RIS67BS" (192.168.15.128)</div>
<div>  McAfee MVISION: Add Tag </div>	<div>Raw Response Show</div>

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`

Action 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.

Run

Cancel

Example Result

 McAfee MVISION: Remove Tag

 McAfee MVISION: Add Tag

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)

Raw Response

Show

Change Log

- **Version 1.0.1 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 1.0.1**
 - Updated operation code to ThreatQuotient-approved standards.
 - Added installation script, `install.sh`, for the Asset custom object and updated the custom object installation steps in the Prerequisites chapter.
 - Upgraded the support tier from Not Support to ThreatQ Supported.
- **Version 1.0.0**
 - Initial Release