ThreatQuotient

McAfee Web Gateway Operation Guide

Version 1.0.1

August 09, 2021

ThreatQuotient
11400 Commerce Park Dr., Suite 200
Reston, VA 20191

Support

Email: support@threatq.com
Web: support.threatq.com
Phone: 703.574.9893

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.

Versioning

- Current integration version: `1.0.1`
- Supported on ThreatQ versions >= `4.31.0`
- McAfee ePolicy Orchestrator (ePO) versions >= `5.9.0`
- McAfee Web Gateway versions >= `9.2.11`
- McAfee DXL Client server

Introduction

The McAfee Web Gateway operation enables analysts to query McAfee Web Gateway for reputation information on network indicators (IP Address, FQDN, URL). The search is performed via a McAfee ePO. Any search results can be added as related indicators and/or attributes to the enriched indicator.

Prerequisites

- Route between ThreatQ and McAfee ePO
- McAfee products:
  - ePO with an installed Web Gateway extension
  - Web Gateway server connected to ePO and DXL fabric
- Installed McAfee DXL SDK in ThreatQ

See the Installation section for install instructions.

Installation

The installation process for this operation can be organized into three sets of instructions:

- Install McAfee DXL SDK and Configure Certificates in EPO
- Install the Integration Rule Set (DXL Listener) in Web Gateway
- Install Operation in ThreatQ

Install McAfee DXL SDK and Configure Certificates in ePO

1. Install the McAfee DXL SDK:
    a. SSH to ThreatQ.
    b. Activate Python3.5:

    ```
    source /opt/threatq/python/bin/activate
    ```

    c. Install McAfee DXL SDK:

    ```
    pip install dxlclient
    ```

2. Generate certificates for authenticating the connection between ThreatQ and McAfee ePO. Before executing the commands, confirm that you have the hostname/IP address, username, and password for the ePO available.

    ```
    source /opt/threatq/python/bin/activate

    cd /var/tmp

    python -m dxlclient provisionconfig /var/files/plugin_data/
    tq_op_mcafee_web_gateway <McAfee ePO Hostname or IP Address>
    threatq
    ```

3. Change the owner of the generated files to `apache`. This is the system user that ThreatQ uses to execute the operations in the UI

    ```
    sudo chown -R apache:apache dxl_certs/
    ```

4. Add the generated certificates to the trusted store in McAfee ePO
    a. Log into ePO as an admin via the UI.

b. Navigate to **Server Settings > DXL Topic Authorization**.

c. Click on the **Edit** button in the lower right corner and select the topics:

  - `TIE Server Set Enterprise Reputation`
  - `TIE Server External Reputation Provider Event`
  - `Web Gateway`

d. While the topics are selected, click in the lower left corner on **Actions > Send Certificates**.

e. Select the entry in the certificate list called `threatq` and click **OK**.

f. Click **Save** when you return to the previous page.

g. Log out of ePO.

5. Proceed to the next installation section to install the Integration Rule Set.

Install the Integration Rule Set (DXL Listener) in Web Gateway

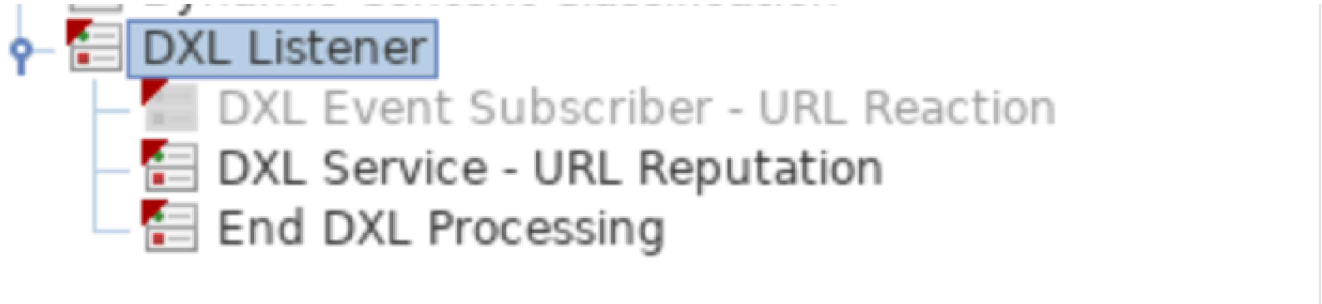
The steps below will show you how to install the Rule Set which will allow the retrieval of reputations from McAfee Web Gateway's servers.

1. Download the configuration XML (`2019-08-27_15-13_DXL Listener.xml`) from the ThreatQ Download center (https://download.threatq.com/).
2. Log into your McAfee Web Gateway instance via your browser.
3. Navigate to the **Policy** page by clicking the book icon in the navigation bar. This will navigate you to the **Rule Sets** tab by default.
4. Click on the **Add** button, then select **Rule Set from Library**.

   > 💡 This should show a popup window.

5. Click on the **Import from File** button at the bottom left of the popup
6. Upload the `2019-08-27_15-13_DXL Listener.xml` file to your McAfee Web Gateway instance via the GUI
7. Click **OK** to import the configuration.

   The DXL Listener rule set should now be in your left-side navigator.



DXL Listener
DXL Event Subscriber - URL Reaction
DXL Service - URL Reputation
End DXL Processing

8. Proceed to the next installation section to install the operation in ThreatQ.

ThreatQ UI 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.

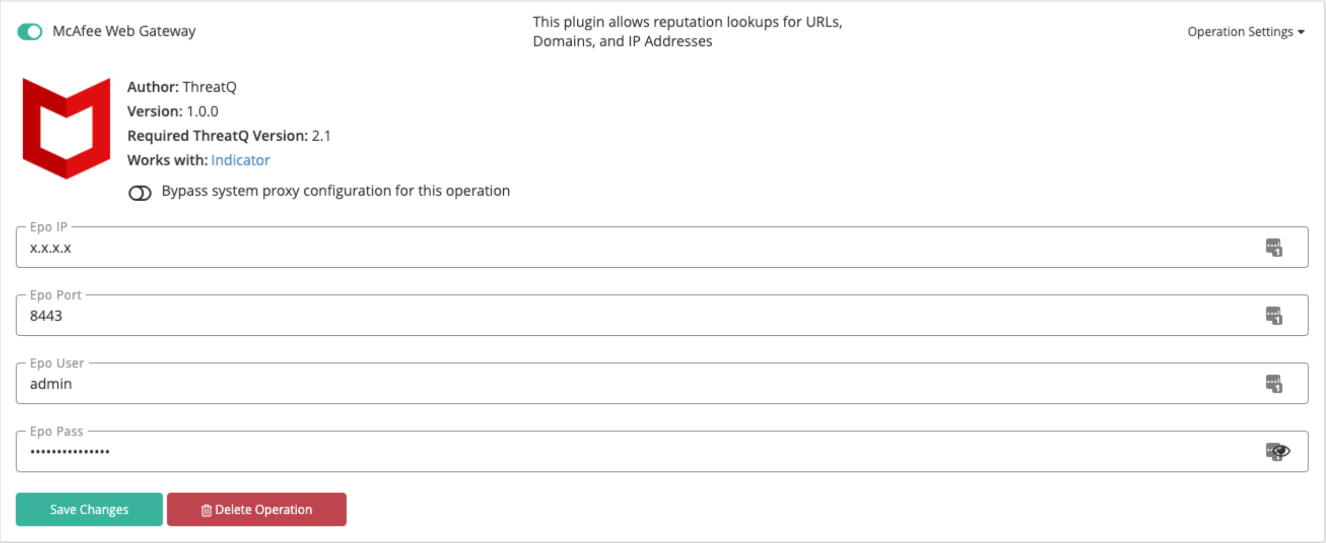
To configure the integration:

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
ePO IP	You hostname or IP address for ePO.
ePO Port	The ePO communication port. The default is 8443, which can be changed if needed.
ePO Username	Your username for ePO.
ePO Password	Your password for ePO.



McAfee Web Gateway

This plugin allows reputation lookups for URLs, Domains, and IP Addresses

Author: ThreatQ
Version: 1.0.0
Required ThreatQ Version: 2.1
Works with: Indicator

Bypass system proxy configuration for this operation

Epo IP: x.x.x.x
Epo Port: 8443
Epo User: admin
Epo Pass: •••••••••••••••

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

Actions

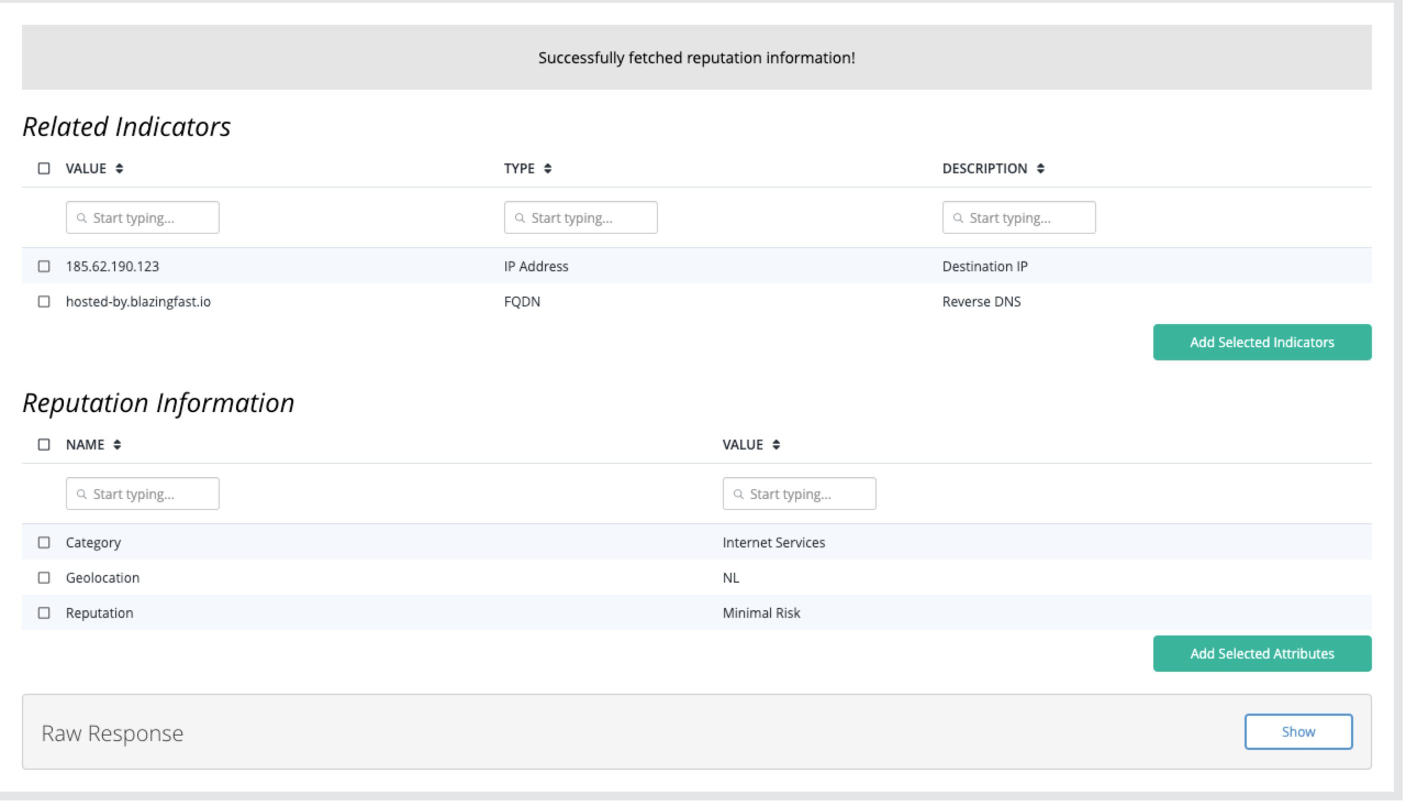
The operation provides the following action:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Get Reputation	Performs a reputation lookup on a network indicator.	Indicators	IP Address, FQDN, URL

Get Reputation

This action queries McAfee Web Gateway and returns reputation for network indicators.

> The operation uses the McAfee SDK to execute the search actions via ePO.



Successfully fetched reputation information!

Related Indicators

□	VALUE	TYPE	DESCRIPTION
	Start typing...	Start typing...	Start typing...
□	185.62.190.123	IP Address	Destination IP
□	hosted-by.blazingfast.io	FQDN	Reverse DNS

Reputation Information

□	NAME	VALUE
	Start typing...	Start typing...
□	Category	Internet Services
□	Geolocation	NL
□	Reputation	Minimal Risk

Change Log

- **Version 1.0.1**
  - Updated dependencies.
- **Version 1.0.0**
  - Initial release