ThreatQuotient

MaxMind Geolocate Operation

Version 1.0.0

October 01, 2024

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

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.

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	1.0.0
Compatible with ThreatQ Versions	>= 4.35.0
Support Tier	ThreatQ Supported

Introduction

The MaxMind Geolocate Operation for ThreatQ enables analysts to fetch geolocation information from a MaxMind database or the web API.

The operation provides the following actions:

- **Lookup** - performs a Geolocation lookup for the given IP Address.
- **Lookup All Related IPS** - performs a look up of related IPs and adds the results to the description.

The operation is compatible with the following system objects:

- Files (Attachments)
- Indicators:
  - IP Address
  - IPv6 Address

Prerequisites

The following is required by the integration:

- A paid plan MaxMind account.

  > The free account credentials will not work with this integration. You must generate the License Key from a paid MaxMind Account.

  - A MaxMind Account ID
  - A MaxMind License Key
- A Mapbox API Key (optional)
- A MaxMind database file has been downloaded (City, Country, Enterprise, ISP, etc.). This is needed if you plan to use a DB file opposed the Web API (**DB File or Web API** parameter in the operation's configuration page).

  > The database file must be transferred to a persistent location on your ThreatQ instance.

Integration Dependencies

The following is a list of required dependencies for the integration. These dependencies are downloaded and installed during the installation process. If you are an Air Gapped Data Sync (AGDS) user, or run an instance that cannot connect to network services outside of your infrastructure, you will need to download and install these dependencies separately as the integration will not be able to download them during the install process.

> Items listed in bold are pinned to a specific version. In these cases, you should download the version specified to ensure proper function of the integration.

DEPENDENCY	VERSION	NOTES
threatq-pynoceros	>=5.12.1	N/A
maxminddb	==1.5.4	Pinned
geoip2	==3.0.0	Pinned
Jinja1	==2.11.3	Pinned

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 .whl file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration .whl file using one of the following methods:
    - Drag and drop the file into the dialog box
    - Select **Click to Browse** to locate the 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

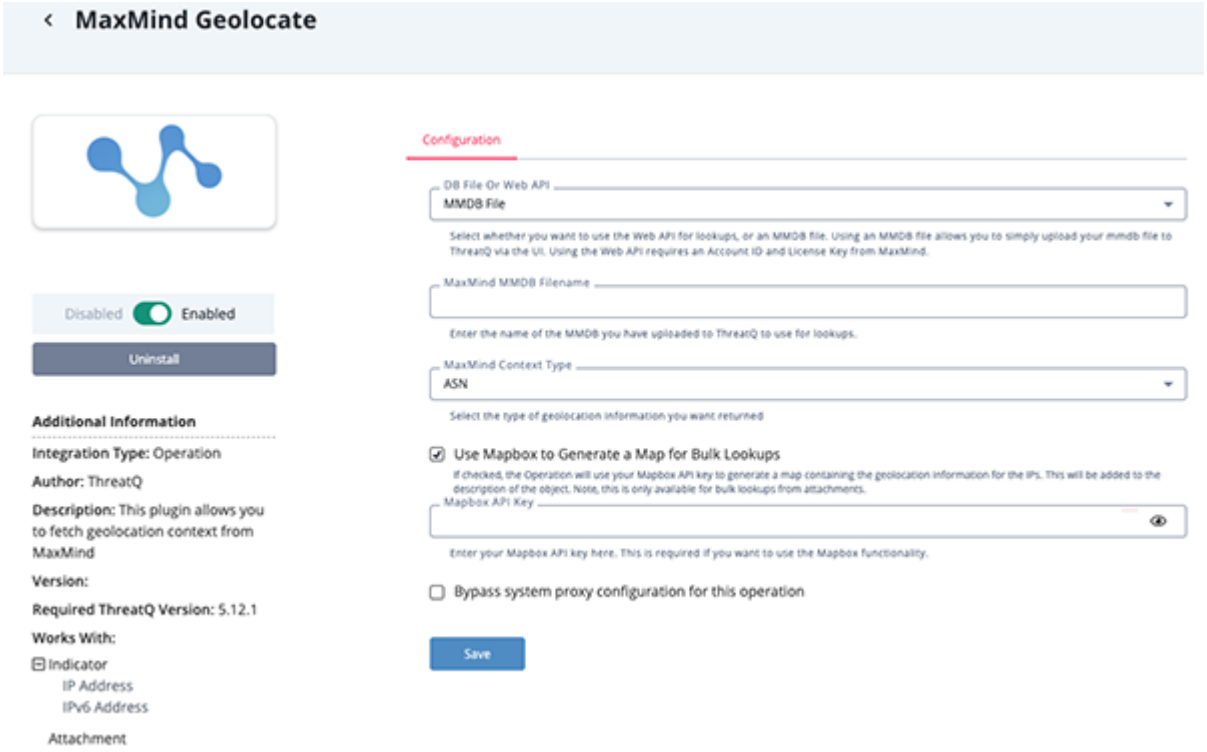
> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

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
DB File or Web API	Select whether you want to use the Web API for lookups, or an MMDB file
MaxMind MMDB Filename	Enter the name of the MMDB you have uploaded to ThreatQ to use for lookups. This field will only load if you selected **DB File** for the **DB File or Web API** field.
MaxMind Account ID	Enter your MaxMind Account ID to use for the Web API. This field will only load if you selected **Web API** for the **DB File or Web API** field.
MaxMind License Key	Enter your MaxMind License Key to use for the Web API. This field will only load if you selected **Web API** for the **DB File or Web API** field.
MaxMind Context Type	Select the type of geolocation information you want returned. Options include: ◦ City ◦ Country ◦ ASN
MaxMind Edition	Select the edition for your MaxMind license. This field will only load if you selected **Web API** for the **DB File or Web API** field.

PARAMETER	DESCRIPTION
Use Mapbox to Generate a Map for Bulk Lookups	Enable this option to use your Mapbox API key to generate a map containing the geolocation information for the IPs. This will be added to the description of the object. This option is only available for bulk lookups from files (attachments).
Mapbox API Key	Enter your Mapbox API key. This is required if you want to use the Mapbox functionality



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
Lookup	Performs a Geolocation lookup for the given IP Address	Indicators	IP Address, IPv6 Address
Lookup All Related IPS	Lookup related IP's and adds to the description	Files (attachments)	N/A

Lookup

The Lookup action performs a Geolocation lookup for the given IP Address. This action utilizes MaxMind's `geoip2` library to perform IP lookups. Depending on your Operation configuration for `MaxMind Context Type`, the Operation will return slightly different results.

Sample Response:


```
{
    "postal": {
        "code": "27403"
    },
    "traits": {
        "ip_address": "173.95.88.48",
        "prefix_len": 29
    },
    "city": {
        "names": {
            "de": "Greensboro",
            "ru": "\u0413\u0440\u0438\u043d\u0441\u0431\u043e\u0440\u043e",
            "en": "Greensboro",
            "pt-BR": "Greensboro",
            "fr": "Greensboro",
            "ja": "\u30b0\u30ea\u30fc\u30f3\u30ba\u30dc\u30ed",
            "zh-CN": "\u683c\u6797\u65af\u4f2f\u52d2"
        },
        "geoname_id": 4469146
    },
    "subdivisions": [
        {
            "names": {
                "ru": "\u0421\u0435\u0432\u0435\u0440\u043d\u0430\u044f
\u041a\u0430\u0440\u043e\u043b\u0438\u043d\u0430",
                "en": "North Carolina",
                "pt-BR": "Carolina do Norte",
                "es": "Carolina del Norte",
                "fr": "Caroline du Nord",
                "ja": "\u30ce\u30fc\u30b9\u30ab\u30ed\u30e9\u30a4\u30ca\u5dde",
                "zh-CN": "\u5317\u5361\u7f57\u6765\u7eb3\u5dde"
            },
            "iso_code": "NC",
            "geoname_id": 4482348
        }
    ],
    "registered_country": {
        "names": {
            "de": "USA",
            "ru": "\u0421\u0428\u0410",
            "en": "United States",
            "fr": "\u00c9tats-Unis",
```

```
            "es": "Estados Unidos",
            "pt-BR": "Estados Unidos",
            "ja": "\u30a2\u30e1\u30ea\u30ab\u5408\u8846\u56fd",
            "zh-CN": "\u7f8e\u56fd"
        },
        "iso_code": "US",
        "geoname_id": 6252001
    },
    "location": {
        "latitude": 36.0617,
        "longitude": -79.8239,
        "time_zone": "America/New_York",
        "metro_code": 518,
        "accuracy_radius": 100
    },
    "continent": {
        "code": "NA",
        "names": {
            "de": "Nordamerika",
            "ru": "\u0421\u0435\u0432\u0435\u0440\u043d\u0430\u044f
\u0410\u043c\u0435\u0440\u0438\u043a\u0430",
            "en": "North America",
            "fr": "Am\u00e9rique du Nord",
            "es": "Norteam\u00e9rica",
            "pt-BR": "Am\u00e9rica do Norte",
            "ja": "\u5317\u30a2\u30e1\u30ea\u30ab",
            "zh-CN": "\u5317\u7f8e\u6d32"
        },
        "geoname_id": 6255149
    },
    "country": {
        "names": {
            "de": "USA",
            "ru": "\u0421\u0428\u0410",
            "en": "United States",
            "fr": "\u00c9tats-Unis",
            "es": "Estados Unidos",
            "pt-BR": "Estados Unidos",
            "ja": "\u30a2\u30e1\u30ea\u30ab\u5408\u8846\u56fd",
            "zh-CN": "\u7f8e\u56fd"
        },
        "iso_code": "US",
        "geoname_id": 6252001
    }
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.postal.code	Attribute.Value	Postal Code	N/A	21401	N/A
.city.names.en	Attribute.Value	City	N/A	Miami	N/A
.subdivisions[].names.en	Attribute.Value	Subdivision	N/A	Florida	N/A
.subvisions[].iso_code	Attribute.Value	N/A	N/A	FL	N/A
.registered_country.names.en	Attribute.Value	Country	N/A	United States	N/A
.registed_country_names.iso_code	Attribute.Value	Country Code	N/A	US	N/A
.country.names.en	Attribute.Value	Country	N/A	United States	N/A
.country.iso_code	Attribute.Value	Country Code	N/A	US	N/A
.represented_country.names.en	Attribute.Value	Country	N/A	United States	N/A
.represented_country.iso_code	Attribute.Value	Country Code	N/A	US	N/A
.location.latitude	Attribute.Value	Latitude	N/A	0.1234	N/A
.location.longitude	Attribute.Value	Longitude	N/A	1.564	N/A
.location.time_zone	Attribute.Value	Timezone	N/A	America/New York	N/A
.location.metro_code	Attribute.Value	Metro Code	N/A	N/A	N/A
.continent.code	Attribute.Value	Continent Code	N/A	NA	N/A
.continent.names.en	Attribute.Value	Continent	N/A	North Ameria	N/A
.autonomous_system_number	Indicator.Value	ASN	N/A	123456	N/A
.autonomous_system_organization	Attribute.Value	ASN Organization	N/A	N/A	N/A
.is_anonymous	Attribute.Value	Is Anonymous	N/A	True	N/A
.is_anonymous_vpn	Attribute.Value	Is Anonymous VPN	N/A	True	N/A
.is_hosting_provider	Attribute.Value	Is Hosting Provider	N/A	True	N/A
.is_public_proxy	Attribute.Value	Is Public Proxy	N/A	True	N/A
.is_residential_proxy	Attribute.Value	Is Residential Proxy	N/A	True	N/A
.is_tor_exit_node	Attribute.Value	Is TOR Exit Node	N/A	True	N/A
.connection_type	Attribute.Value	Connection Type	N/A	True	N/A
.domain	Indicator.Value	FQDN	N/A	N/A	N/A
.isp	Attribute.Value	ISP	N/A	Comcast	N/A
.organization	Attribute.Value	Organization	N/A	N/A	N/A

Lookup All Related IPs

The Lookup All Related IPs action performs a look up of related IPs and adds that information to the description.

Sample Response:


```
{
    "173.95.88.48": {
        "country": {
            "iso_code": "US",
            "names": {
                "de": "USA",
                "pt-BR": "EUA",
                "ru": "\u0421\u0428\u0410",
                "en": "United States",
                "zh-CN": "\u7f8e\u56fd",
                "fr": "\u00c9tats Unis",
                "ja": "\u30a2\u30e1\u30ea\u30ab",
                "es": "Estados Unidos"
            },
            "geoname_id": 6252001
        },
        "location": {
            "latitude": 36.1053,
            "accuracy_radius": 10,
            "longitude": -79.8762,
            "metro_code": 518,
            "time_zone": "America/New_York"
        },
        "subdivisions": [
            {
                "iso_code": "NC",
                "names": {
                    "de": "North Carolina",
                    "es": "Carolina del Norte",
                    "ru": "\u0421\u0435\u0432\u0435\u0440\u043d\u0430\u044f
\u041a\u0430\u0440\u043e\u043b\u0438\u043d\u0430",
                    "en": "North Carolina",
                    "pt-BR": "Carolina do Norte",
                    "ja":
"\u30ce\u30fc\u30b9\u30ab\u30ed\u30e9\u30a4\u30ca\u5dde",
                    "fr": "Caroline du Nord",
                    "zh-CN": "\u5317\u5361\u7f57\u6765\u7eb3\u5dde"
                },
                "geoname_id": 4482348
            }
        ],
        "postal": {
            "code": "27410"
```

```
        },
        "maxmind": {
            "queries_remaining": 74931
        },
        "registered_country": {
            "iso_code": "US",
            "names": {
                "de": "USA",
                "es": "Estados Unidos",
                "ru": "\u0421\u0428\u0410",
                "en": "United States",
                "pt-BR": "EUA",
                "zh-CN": "\u7f8e\u56fd",
                "fr": "\u00c9tats Unis",
                "ja": "\u30a2\u30e1\u30ea\u30ab"
            },
            "geoname_id": 6252001
        },
        "traits": {
            "autonomous_system_organization": "TWC-11426-CAROLINAS",
            "isp": "Spectrum Business",
            "organization": "Spectrum Business",
            "connection_type": "Corporate",
            "domain": "spectrum.com",
            "autonomous_system_number": 11426,
            "network": "173.95.88.48/29",
            "ip_address": "173.95.88.48"
        },
        "city": {
            "names": {
                "de": "Greensboro",
                "pt-BR": "Greensboro",
                "ru": "\u0413\u0440\u0438\u043d\u0441\u0431\u043e\u0440\u043e",
                "en": "Greensboro",
                "ja": "\u30b0\u30ea\u30fc\u30f3\u30ba\u30dc\u30ed",
                "fr": "Greensboro",
                "zh-CN": "\u683c\u6797\u65af\u4f2f\u52d2"
            },
            "geoname_id": 4469146
        },
        "continent": {
            "code": "NA",
            "names": {
                "de": "Nordamerika",
                "es": "Norteam\u00e9rica",
                "ru": "\u0421\u0435\u0432\u0435\u0440\u043d\u0430\u044f
\u0410\u043c\u0435\u0440\u0438\u043a\u0430",
                "en": "North America",
                "pt-BR": "Am\u00e9rica do Norte",
                "ja": "\u5317\u30a2\u30e1\u30ea\u30ab",
```

```
                "fr": "Am\u00e9rique du Nord",
                "zh-CN": "\u5317\u7f8e\u6d32"
            },
            "geoname_id": 6255149
        }
    }
}
```

Action Run Parameters

The following parameter is available when you select the Lookup All Related IPs action:

PARAMETER	DETAILS
Apply Lookup Results to Description	Enable this option to add the results of the lookup to the description of the object.

Change Log

- **Version 1.0.0**
  - Initial release