ThreatQuotient

MaxMind Action

Version 1.0.0

June 24, 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	>= 5.12.1
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The MaxMind Action integration allows ThreatQ users to enrich IP addresses with geolocation data from MaxMind. This data can be used to better understand the context of an IP address and make more informed decisions.

MaxMind offers both free and paid geolocation services. Their GeoIP service enables users to query the location of an IPv4 or IPv6 address. Context such as an IP's country, continent, city, postal code, and more can be retrieved.

The integration pprovides the following action:

- **MaxMind GeoIP Lookup** - fetches geolocation data for IP addresses from MaxMind's GeoIP service.

The action is compatible with the following object types:

- Indicators
  - IP Address
  - IPv6 Address

The action returns the following enriched system objects:

- Indicators
  - IP Address
  - IPv6 Address
  - FQDN

This action is intended for use with ThreatQ TDR Orchestrator (TQO). An active TQO license is required for this feature.

Prerequisites

- An active ThreatQ TDR Orchestrator (TQO) license.
- A MaxMind account (free or paid)
- A data collection containing the following indicator objects:
  - IP Address
  - IPv6 Address

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

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

You will still need to configure the action.

Configuration

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

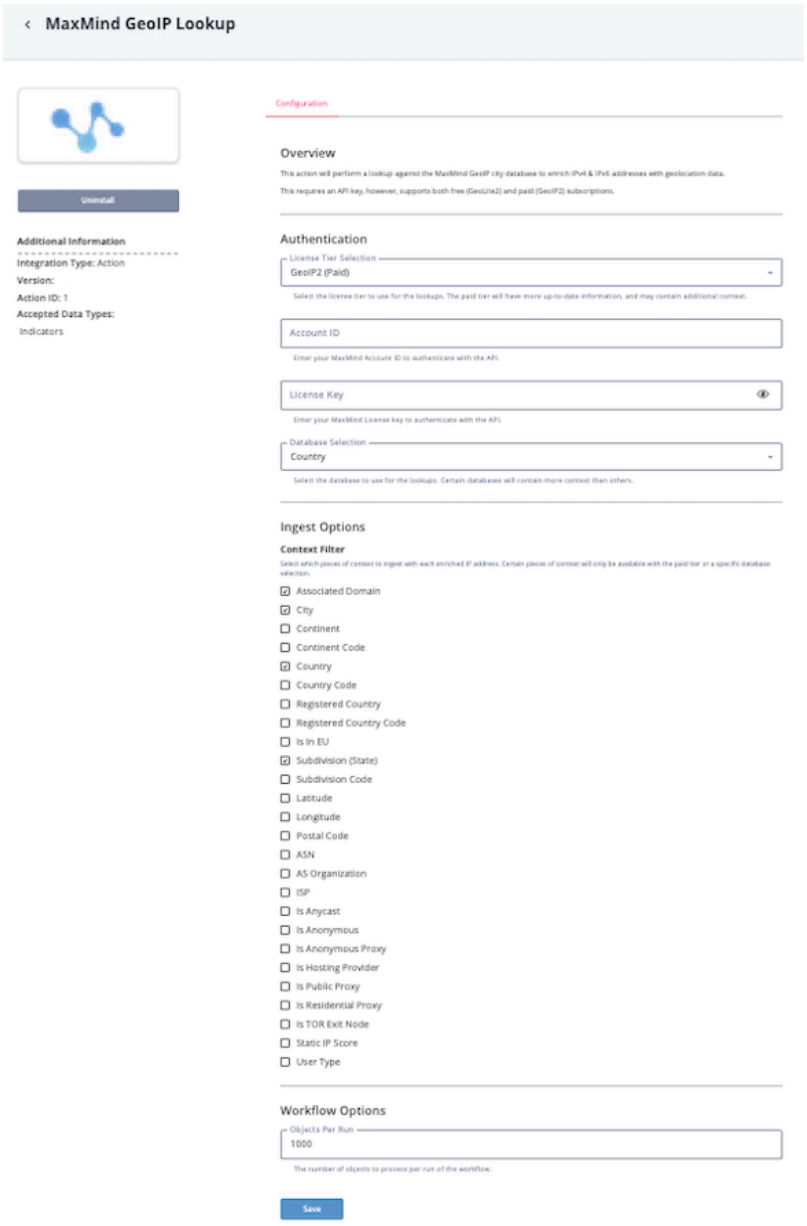
To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Actions** option from the *Category* dropdown (optional).
3. Click on the action entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

> The configurations set on this page will be used as the default settings when inserting this action into a new workflow. Updating the configurations on this page will not update any instances of this action that have already been deployed to a workflow. In that scenario, you must update the action's configurations within the workflow itself.

PARAMETER	DESCRIPTION
License Tier Selection	Select the license tier to use for the lookups. The paid tier will have more up-to-date information, and may contain additional context.
Account ID	Enter your MaxMind Account ID to authenticate with the API.
License Key	Enter your MaxMind License key to authenticate with the API.
Database Selection	Select the database to use for the lookups. Certain databases will contain more context than others.
Context Filter	Select which pieces of context to ingest with each enriched IP address. Certain pieces of context will only be available with the paid tier or a specific database selection.
Context filter	◦ Associated Domain *(default)* ◦ City *(default)* ◦ Continent ◦ Continent Code ◦ Country *(default)*

PARAMETER	DESCRIPTION
	◦ Country Code ◦ Registered Country ◦ Registered Country Code ◦ Is In EU ◦ Subdivision (State) *(default)* ◦ Subdivision Code ◦ Latitude ◦ Longitude ◦ Postal Code ◦ ASN ◦ AS Organization ◦ ISP ◦ Is Anycast ◦ Is Anonymous ◦ Is Anonymous Proxy ◦ Is Hosting Provider ◦ Is Public Proxy ◦ Is Residential Proxy ◦ Is TOR Exit Node ◦ Static IP Score ◦ User Type
Confidence Threshold (Insights Only)	Set the minimum confidence threshold for the data to be ingested. This will prevent low-confidence data from being ingested. *(default: 50)*
Objects Per Run	The number of objects to process per run of the workflow. *(default: 1000)*



5. Review any additional settings, make any changes if needed, and click on **Save**.

Action

The following action is available:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
MaxMind GeoIP Lookup	Performs look ups against MaxMind's Geolocation API	Indicators	IP Address, IPv6 Address

MaxMind GeoIP Lookup

This action will perform lookups against the MaxMind (GeoIP service) https://www.maxmind.com/en/geoip2-services-and-databases and return geolocation data for the provided IP address.

```
GET https://{{ tier }}/geoip/v2.1/{{ db }}/{{ value }}
```

Sample Response:


```
{
  "continent": {
    "code": "NA",
    "geoname_id": 123456,
    "names": {
      "de": "Nordamerika",
      "en": "North America",
      "es": "América del Norte",
      "fr": "Amérique du Nord",
      "ja": "北アメリカ
      "pt-BR": "América do Norte",
      "ru": "Северная Америка",
      "zh-CN": "北美洲
    }
  },
  "country": {
    "geoname_id": 6252001,
    "is_in_european_union": false,
    "iso_code": "US",
    "names": {
      "de": "USA",
      "en": "United States",
      "es": "Estados Unidos",
      "fr": "États-Unis",
      "ja": "アメリカ合衆国
      "pt-BR": "Estados Unidos",
      "ru": "США",
      "zh-CN": "美国
    },
    "confidence": 75
  },
  "maxmind": {
    "queries_remaining": 54321
  },
  "registered_country": {
    "geoname_id": 6252001,
    "is_in_european_union": true,
    "iso_code": "US",
    "names": {
      "de": "USA",
      "en": "United States",
```

```
      "es": "Estados Unidos",
      "fr": "États-Unis",
      "ja": "アメリカ合衆国
      "pt-BR": "Estados Unidos",
      "ru": "США",
      "zh-CN": "美国
    }
  },
  "represented_country": {
    "geoname_id": 6252001,
    "is_in_european_union": true,
    "iso_code": "US",
    "names": {
      "de": "USA",
      "en": "United States",
      "es": "Estados Unidos",
      "fr": "États-Unis",
      "ja": "アメリカ合衆国
      "pt-BR": "Estados Unidos",
      "ru": "США",
      "zh-CN": "美国
    },
    "type": "military"
  },
  "traits": {
    "ip_address": "1.2.3.4",
    "is_anycast": true,
    "network": "1.2.3.0/24",
    "autonomous_system_number": 1239,
    "autonomous_system_organization": "Linkem IR WiMax Network",
    "connection_type": "Cable/DSL",
    "domain": "example.com",
    "isp": "Linkem spa",
    "mobile_country_code": "310",
    "mobile_network_code": "004",
    "organization": "Linkem IR WiMax Network",
    "is_anonymous": true,
    "is_anonymous_vpn": true,
    "is_hosting_provider": true,
    "is_public_proxy": true,
    "is_residential_proxy": true,
    "is_tor_exit_node": true,
    "static_ip_score": 1.5,
    "user_count": 1,
    "user_type": "traveler"
  },
  "city": {
    "confidence": 25,
    "geoname_id": 54321,
    "names": {
```

```
      "de": "Los Angeles",
      "en": "Los Angeles",
      "es": "Los Ángeles",
      "fr": "Los Angeles",
      "ja": "ロサンゼルス市
      "pt-BR": "Los Angeles",
      "ru": "Лос-Анджелес",
      "zh-CN": "洛杉矶
    }
  },
  "location": {
    "accuracy_radius": 20,
    "latitude": 37.6293,
    "longitude": -122.1163,
    "metro_code": 807,
    "time_zone": "America/Los_Angeles",
    "average_income": 128321
  },
  "postal": {
    "code": "90001",
    "confidence": 10
  },
  "subdivisions": [
    {
      "geoname_id": 5332921,
      "iso_code": "CA",
      "names": {
        "de": "Kalifornien",
        "en": "California",
        "es": "California",
        "fr": "Californie",
        "ja": "カリフォルニア
        "ru": "Калифорния",
        "zh-CN": "加州
      },
      "confidence": 50
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.continent.code`	Attribute	Continent Code	N/A	`NA`	If enabled
`.continent.names.en`	Attribute	Continent	N/A	`North America`	If enabled
`.country.iso_code`	Attribute	Country Code	N/A	`US`	If enabled
`.country.names.en`	Attribute	Country	N/A	`US`	If enabled
`.country.is_in_european_union`	Attribute	Is In EU	N/A	`true`	If enabled
`.registered_country.iso_code`	Attribute	Registered Country Code	N/A	`US`	If enabled
`.registered_country.names.en`	Attribute	Registered Country	N/A	`United States`	If enabled
`.traits.is_anycast`	Attribute	Is Anycast	N/A	`true`	If enabled
`.traits.is_anonymous`	Attribute	Is Anonymous	N/A	`true`	If enabled
`.traits.autonomous_system_number`	Attribute	ASN	N/A	`1239`	If enabled
`.traits.autonomous_system_organization`	Attribute	AS Organization	N/A	`true`	If enabled
`.traits.is_hosting_provider`	Attribute	Is Hosting Provider	N/A	`true`	If enabled
`.traits.is_public_proxy`	Attribute	Is Public Proxy	N/A	`true`	If enabled
`.traits.is_anonymous_proxy`	Attribute	Is Anonymous Proxy	N/A	`true`	If enabled
`.traits.is_residential_proxy`	Attribute	Is Residential Proxy	N/A	`true`	If enabled
`.traits.is_tor_exit_node`	Attribute	Is TOR Exit Node	N/A	`true`	If enabled
`.traits.static_ip_score`	Attribute	Static IP Score	N/A	`1.5`	If enabled
`.traits.user_type`	Attribute	User Type	N/A	`traveler`	If enabled
`.city.names.en`	Attribute	City	N/A	`Los Angeles`	If enabled
`.location.latitude`	Attribute	Latitude	N/A	`37.6293`	If enabled
`.location.longitude`	Attribute	Longitude	N/A	`-122.1163`	If enabled
`.postal.code`	Attribute	Postal Code	N/A	`90001`	If enabled

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.subdivisions[].iso_code`	Attribute	Subdivision Code	N/A	`CA`	If enabled
`.subdivisions[].names.en`	Attribute	Subdivision	N/A	`California`	If enabled
`.traits.isp`	Attribute	ISP	N/A	`Linkem spa`	If enabled
`.traits.domain`	Indicator.Value	FQDN	N/A	`example.com`	If enabled

Enriched Data

Object counts and action runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and action runtime may vary based on system resources and load.

METRIC	RESULT
Run Time	1 minute
Indicators	5
Indicator Attributes	15

Use Case Example

As an analyst, I have a list of IP addresses that have accessed compromised account emails. I want to figure out which country these IP addresses are coming from to determine if they are likely to be malicious.

Change Log

- **Version 1.0.0**
  - Initial release