ThreatQuotient

Trend Micro Deep Security Action

Version 1.0.0

February 18, 2025

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.

Copyright © 2025 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	1.0.0
Compatible with ThreatQ Versions	>= 6.5.0
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The Trend Micro Deep Security Action integration is designed to export a ThreatQ data collection comprised of IP Addresses, CIDR Blocks, IPv6 Addresses from ThreatQ to a Trend Micro Deep Security on-premise or cloud instance. These data collections are accepted as IP Lists within Trend Micro and are typically used for policies.

The integration provides the following action:

- **Trend Micro Deep Security - Export Indicators -** uploads indicators to an IP List in Trend Micro.

The action is compatible with Asset and Indicator type system objects.

> 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 data collection containing at least one of the following object types:
  - Asset
  - Indicator
- A Trend Micro Deep Security Instance.
- A Trend Micro Deep Security API Key. See the following links, based your environment type, for additional information:
  - **Cloud Instances -** https://cloudone.trendmicro.com/docs/workload-security/api-reference/tag/IP-Lists#operation/createIPList
  - **On-Premise Instance -** https://automation.deepsecurity.trendmicro.com/article/20_0/api-reference

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.

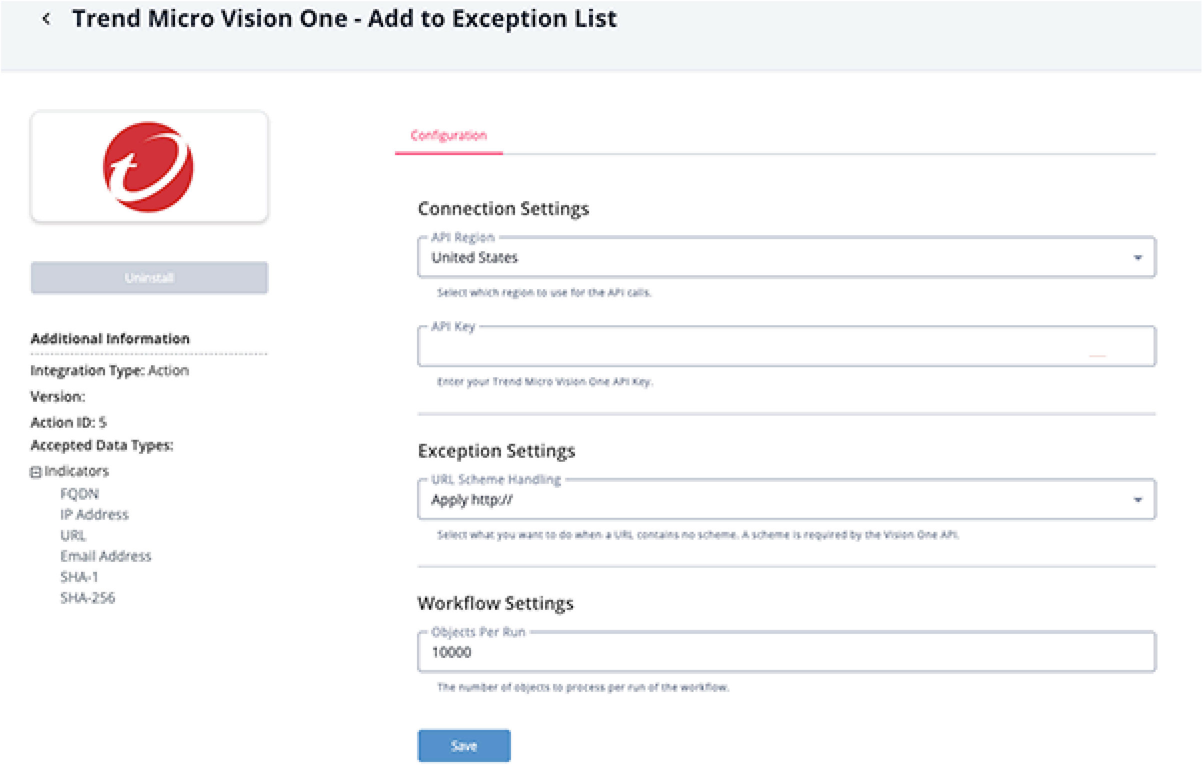
To configure the integration:

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
Trend Micro Deep Security Instance	The URL to the Trend Micro Deep Security instance. The pattern for cloud instance is as follows: `workload.<region>.cloudone.trendmicro.com`. On-Premise instances should specify the port.
API Key	The API Key generated within your Trend Micro Deep Security Manager instance.
Authentication Header Parameter Name	Select the name of the header used for authentication. Options include: ◦ Authorization ◦ api-secret-key Users should select **api-secret-key** for an on-premise instance. For cloud instances, the selection depends on the API Key type. Select **Authorization** for a Trend Micro

PARAMETER	DESCRIPTION
	Cloud One API Key or **api-secret-key** for a Legacy API Key.
Enable SSL Certificate Verification	Enable this parameter if the action should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the action should not honor proxies set in the ThreatQ UI.
IP List Name	Specify the name of the IP List where the input collection is uploaded to in Trend Micro.
Clear IP List on Manual Run	Enabling this will automatically clear the IP List on manual runs before exporting new objects to it. This is done to ensure that the category is always up-to-date with the ThreatQ data collection.
Objects per run	Maximum number of objects to process per-run.



Trend Micro Vision One - Add to Exception List

Additional Information

Integration Type: Action

Version:

Action ID: 5

Accepted Data Types:

Indicators
- FQDN
- IP Address
- URL
- Email Address
- SHA-1
- SHA-256

Connection Settings

API Region: United States

Select which region to use for the API calls.

API Key:

Enter your Trend Micro Vision One API Key.

Exception Settings

URL Scheme Handling: Apply http://

Select what you want to do when a URL contains no scheme. A scheme is required by the Vision One API.

Workflow Settings

Objects Per Run: 10000

The number of objects to process per run of the workflow.

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

Actions

The following action is available:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Trend Micro Deep Security - Export Indicators	Uploads indicators to an IP List in Trend Micro	Indicator, Asset	IP Address, CIDR Block, IPv6 Address

Trend Micro Deep Security - Export Indicators

The Trend Micro Deep Security - Export Indicators action submits a ThreatQ data collection of indicators and/or assets that have the value equal to a valid private IP Address or private CIDR Block.

> Trend Micro allows IP Lists to have a maximum of 32,000 characters. Due to this limitation, the data from the collection is split in multiples parts. The name of each part is built by appending to the value of the user field `IP List Name` the number of the part from the ThreatQ collection that is uploaded (e.g list_0, list_1 and so on). Even if the ThreatQ collection does not exceed the Trend Micro limit the name of the list will have `_0` appended.

`POST https://workload.us-1.cloudone.trendmicro.com`

Sample Body:

```
{
  "name": "threatq_collection_0",
  "description": "Data Collection sent from ThreatQ at 2025-02-10 10:00:00",
  "items": [
    "1.2.3.4",
    "5.15.134.0/24",
    "2606:4700:4700:0000:0000:0000:0000:1111"
  ]
}
```

Sample Response:

```
{
  "ip_list": {
    "ID": 65,
    "description": "Data Collection sent from ThreatQ at 2025-02-10 10:00:00",
    "items": [
      "1.2.3.4",
      "5.15.134.0/24",
      "2606:4700:4700:0000:0000:0000:0000:1111"
    ]
  }
}
```

Use Case Example

1. A Threat Analyst identifies a collection of IP Address he would like to upload to Trend Micro.
2. The Threat Analyst adds the Trend Micro Deep Security action to a Workflow.
3. The Threat Analyst configures the action with the desired parameters and enables the Workflow.
4. The Workflow executes all actions in the graph, including Trend Micro Deep Security.
5. The uploads the input collection to an IP List in Trend Micro.

Known Issues / Limitations

- Trend Micro allows IP Lists to have a maximum of 32,000 characters. Due to this limitation, the data from the collection is split in multiples parts. The name of each part is built by appending to the value of the user field `IP List Name` the number of the part from the ThreatQ collection that is uploaded (e.g list_0, list_1 and so on). Even if the ThreatQ collection does not exceed the Trend Micro limit the name of the list will have `_0` appended.
- Trend Micro allows a maximum of 5000 IP Lists in their platform.
- The entire batch (100 items) will fail to upload if the input collection contains Assets that are not valid private IP Addresses or CIDR Blocks.

Change Log

- **Version 1.0.0**
  - Initial release