ThreatQuotient

Forcepoint Action

Version 1.0.0

April 21, 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.

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	>= 5.29.0
Forcepoint Deployments	On Premise, Cloud
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The Forcepoint Action integration allows users to export indicators of compromise to Forcepoint from the ThreatQ platform.

The integration provides the following action:

- **Forcepoint - Manage IP Address Lists -** uploads indicators to an IP Address List in Forcepoint.

The integration is compatible with the following indicator types:

- CIDR Block
- IP Address
- IPv6 Address

> 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 indicator objects:
  - CIDR Block
  - IP Address
  - IPv6 Address
- A Forcepoint instance.
- A Forcepoint Authentication Key - this is generated when the API Client element is configured in the Management Client. See the following for more information: https://help.forcepoint.com/ngfw/en-us/7.0.0/smc_api_ug/GUID-E9FAE543-D857-43F5-BF53-02D0E50A5D7A.html.

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.

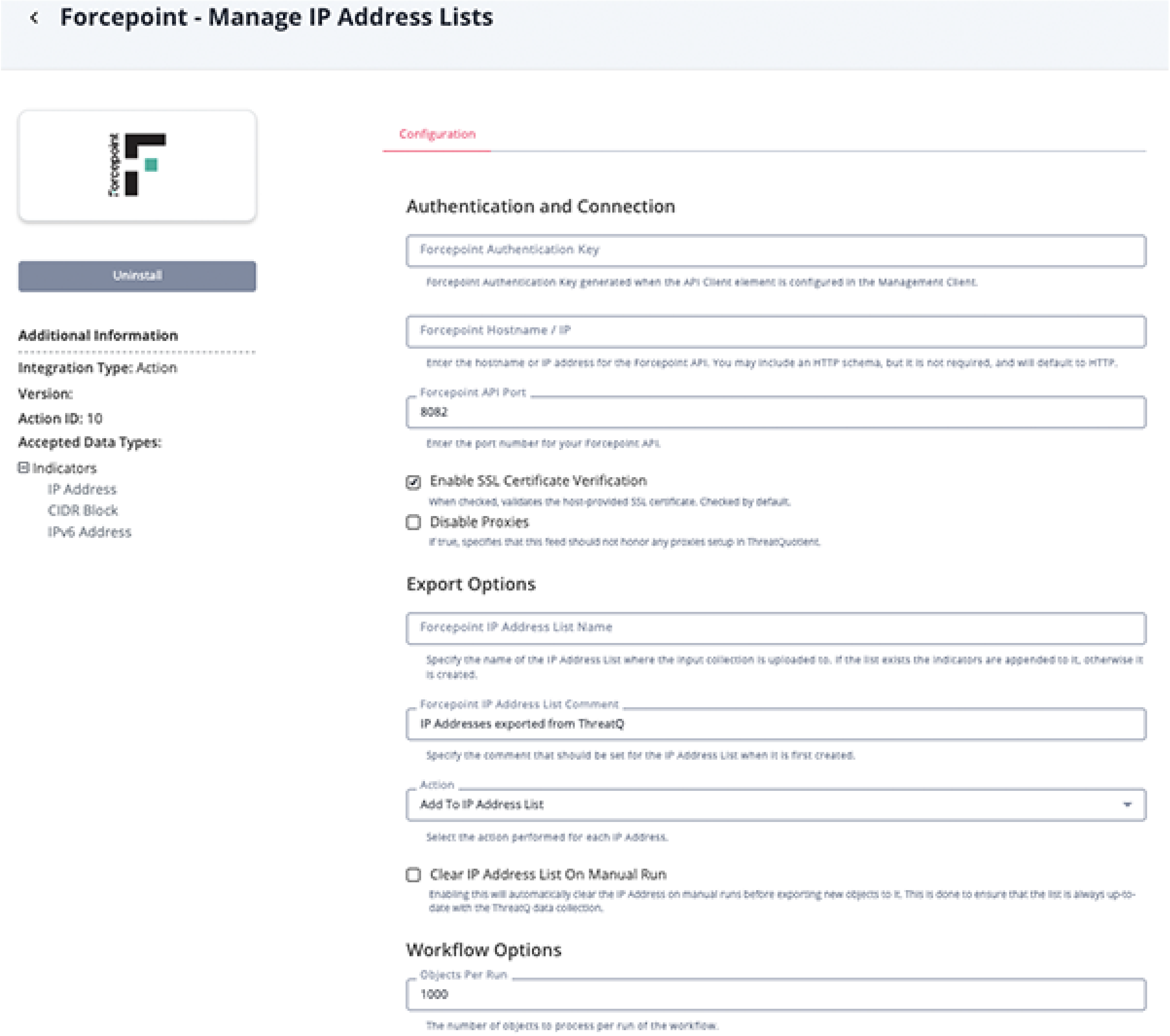
To configure the integration:

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
Forcepoint Authentication Key	Your Forcepoint Authentication Key that is generated when the API Client element is configured in the Management Client.
Forcepoint Hostname / IP	Enter the hostname or IP address for the Forcepoint API. You may include an HTTP schema, but it is not required and will default to HTTP.
Forcepoint API Port	Enter the port number for your Forcepoint API. The default value is 8082.
Enable SSL Certificate Verification	Enable this for the action to validate the host-provided SSL certificate.
Disable Proxies	Enable this option if the action should not honor proxies set in the ThreatQ UI.
Forcepoint IP Address List Name	Specify the name of the IP Address List where the input collection is uploaded to in Forcepoint.

PARAMETER	DESCRIPTION
	If a list exists with that name, the indicators are appended to it. If the list does not exist, it will created for you.
Forcepoint IP Address List Comment	Specify the comment that should be set for the IP Address List when it is first created.
Action	Select the action performed for each IP Address. Actions include: ◦ Add to IP Address List *(default)* ◦ Remove from IP Address List
Clear IP Address List On Manual Run	Enable this parameter to automatically clear the IP Address on manual runs before exporting new objects to it. This is done to ensure that the list is always up-to-date with the ThreatQ data collection. This parameter is only accessible if you have selected the `Add to IP Address List` option for the **Action** configuration parameter.
Objects Per Run	Enter the number of objects to process per run of the workflow.



‹ **Forcepoint - Manage IP Address Lists**

Additional Information

Integration Type: Action
Version:
Action ID: 10
Accepted Data Types:
⊟ Indicators
IP Address
CIDR Block
IPv6 Address

Authentication and Connection

Forcepoint Authentication Key
Forcepoint Authentication Key generated when the API Client element is configured in the Management Client.

Forcepoint Hostname / IP
Enter the hostname or IP address for the Forcepoint API. You may include an HTTP schema, but it is not required, and will default to HTTP.

Forcepoint API Port: 8082
Enter the port number for your Forcepoint API.

☑ Enable SSL Certificate Verification
When checked, validates the host-provided SSL certificate. Checked by default.

☐ Disable Proxies
If true, specifies that this feed should not honor any proxies setup in ThreatQuotient.

Export Options

Forcepoint IP Address List Name
Specify the name of the IP Address List where the input collection is uploaded to. If the list exists the indicators are appended to it, otherwise it is created.

Forcepoint IP Address List Comment: IP Addresses exported from ThreatQ
Specify the comment that should be set for the IP Address List when it is first created.

Action: Add To IP Address List
Select the action performed for each IP Address.

☐ Clear IP Address List On Manual Run
Enabling this will automatically clear the IP Address on manual runs before exporting new objects to it. This is done to ensure that the list is always up-to-date with the ThreatQ data collection.

Workflow Options

Objects Per Run: 1000
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
Forcepoint - Manage IP Address Lists	Uploads indicators to an IP Address List in Forcepoint	Indicator	IP Address, CIDR Block, IPv6 Address

Forcepoint - Manage IP Address List

The Forcepoint - Manage IP Address List action exports collection of indicators (IP Address, CIDR Block, IPv6 Address) to a Forcepoint IP Address List. The action will check to see if the IP Address List Name, specified in the action's configuration parameters, already exists Forcepoint IP Address list specified in Forcepoint IP Address List Name exists. If the IP Address List Name does not exist on Forcepoint, one will be created.

After confirming or creating the IP Address List name, the action will perform its designated functions, either appending or remove indicators from the specified Forcepoint IP Address List.

Request to Get all Existing IP Address Lists from Forcepoint

`GET http://{FORCEPOINT_IP}:8082/7.0/elements/ip_list`

Sample Response:

```
{
  "result": [
    {
      "href": "http://{FORCEPOINT_IP}:8082/7.0/elements/ip_list/1117",
      "name": "ThreatQ Integration",
      "type": "ip_list"
    }
  ]
}
```

> The value of the **Forcepoint IP Address List Name** configuration parameter is searched in the list returned by the API (`.result[]`). If the list is found the ID of the list is parsed from the `.href` key.

Request to Create an IP Address List

`POST http://{FORCEPOINT_IP}:8082/7.0/elements/ip_list`

Sample Response:

```
{
  "name": "ThreatQ Action",
  "comment": "ThreatQ Malicious indicators of compromise."
}
```

> The response body is empty. The URL to the new list is added to the header `Location`.

Request to Get the IP Addresses Already Present in the List

`GET http://{FORCEPOINT_IP}:8082/7.0/elements/ip_list/{LIST_ID}/ip_address_list`

Sample Response:

```
{
  "ip": [
    "222.212.94.49/32",
    "20.232.186.34/32",
    "217.113.229.88/32"
  ]
}
```

Request to Set the IP Addresses of a List

`POST http://{FORCEPOINT_IP}:8082/7.0/elements/ip_list/{LIST_ID}/ip_address_list`

Sample Response:

```
{
  "ip": [
    "20.116.63.219/32",
    "69.167.19.32/32"
  ]
}
```

> The response body is empty.

Use Case Example

1. A Threat Analyst identifies a collection of IP Address they would like to upload to Forcepoint.
2. The Threat Analyst adds the **Forcepoint - Manage IP Address Lists** 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 and uploads the input collection to an IP Address List in Forcepoint.

Change Log

- **Version 1.0.0**
    - Initial release