ThreatQuotient

Infoblox BloxOne Action

Version 1.0.0

June 03, 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	>= 5.29.0
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The Infoblox BloxOne Action allows users to upload or delete indicators to/from a custom list on the Infoblox BloxOne Cloud platform.

The integration provides the following action:

- **Infoblox BloxOne Action** - uploads or deletes indicators from a BloxOne custom list.

The integration is compatible with the following indicator types:

- CIDR Block
- FQDN
- Indicators
- IP 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 types:
  - CIDR Block
  - FQDN
  - Indicators
  - IP Address
- An InfoBlox BloxOne instance.
- An InfoBlox BloxOne API Key.

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

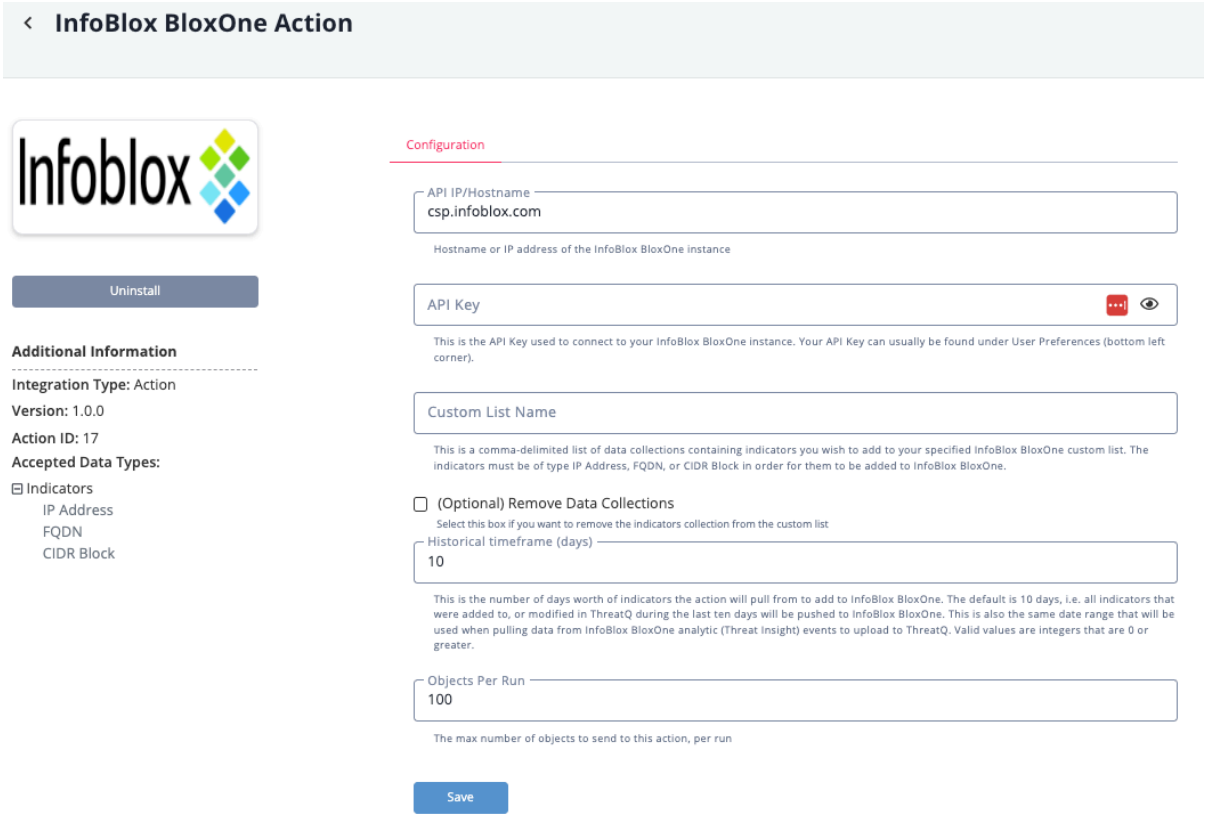
> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

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
Hostname	The Hostname or IP address of your InfoBlox BloxOne instance.
API IP	The API Key used to connect to your InfoBlox BloxOne instance. Your API Key can usually be found under User Preferences (bottom left corner).
Custom List Name	Enter a comma-delimited list of data collections containing indicators you wish to add to your specified InfoBlox BloxOne custom list. The indicators must be of type IP Address, FQDN, or CIDR Block in order for them to be added to InfoBlox BloxOne.
(Optional) Remove Data Collections	Enable this parameter to remove the indicators collection from the custom list.
Historical timeframe (days)	This is the number of days worth of indicators the action will pull from to add to InfoBlox BloxOne.
Objects Per Run	The max number of objects to send, per run.



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
Infoblox BloxOne Action	Upload or Delete indicators	Indicators	IP Address, FQDN, and CIDR Block

Infoblox BloxOne Action

The Infoblox BloxOne action can be used to upload indicators of type IP Address, FQDN, and CIDR Block to a custom list in Infoblox BloxOne, and to retrieve events.

`GET https://{{hostname}}/api/atcfw/v1/named_lists`

This endpoint is utilized to locate the ID of the list that will be used.

Sample Response:


```
{
    "results": [
        {
            "confidence_level": "HIGH",
            "created_time": "2023-10-30T16:36:12Z",
            "description": "",
            "id": 771314,
            "item_count": 1,
            "name": "00020177",
            "policies": [],
            "tags": null,
            "threat_level": "LOW",
            "type": "custom_list",
            "updated_time": "2023-10-30T16:41:39Z"
        },
        {
            "confidence_level": "HIGH",
            "created_time": "2023-07-27T14:42:54Z",
            "description": "Auto-generated",
            "id": 754580,
            "item_count": 0,
            "name": "Default Allow",
            "policies": [
                "Default Global Policy"
            ],
            "tags": null,
            "threat_level": "MEDIUM",
            "type": "default_allow",
            "updated_time": "2023-07-27T14:42:54Z"
        }
    ]
}
```


`POST/DELETE https://{{hostname}}/api/atcfw/v1/named_lists/{{id}}/items`

This endpoint used to add or remove indicators from the specific list. No data is return from the endpoint.

Use Case Example

- A Threat Analyst identifies a collection of supported objects they would like to enrich.
- The Threat Analyst adds the InfoBlox BloxOne Action to a Workflow
- The Threat Analyst configures the action with the desired parameters, and enables the Workflow
- The Workflow executes all Actions in the graph, including InfoBlox BloxOne Action
- The Workflow Upload or Delete the objects to InfoBlox BloxOne

Change Log

- **Version 1.0.0**
  - Initial release