

ThreatQuotient



Infoblox Grid Action Bundle

Version 1.0.0

August 06, 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 3
- Support 4
- Integration Details..... 5
- Introduction 6
- Prerequisites 7
- Installation..... 8
- Configuration 9
- Actions 11
 - Infoblox Grid Add to RPZ 12
 - Infoblox Grid Remove from RPZ 13
- Enriched Data..... 15
 - Infoblox Grid Add to RPZ 15
 - Infoblox Grid Remove from RPZ 15
- Change Log 16

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 © 2024 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	>= 5.25.0
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The Infoblox Grid Action Bundle allows the management of entries in Response Policy Zone (RPZ) zones.

The bundle provides the following actions:

- **Infoblox Grid Add to RPZ** - creates records in an RPZ from ThreatQ indicators of compromise (IP, FQDN and CIDR Block).
- **Infoblox Grid Remove from RPZ** - deletes records from an RPZ that are no longer needed.

The actions enrich indicator type 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 indicator types:
 - CIDR Block
 - FQDN
 - IP Address
- An Infoblox instance, username, and password.

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
6. Select the actions to install, when prompted, and click on Install.



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.

Your actions will now be installed on your instance. You will still need to [configure](#) the action(s).

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
Infoblox Grid URL	Specify full URL to the Infoblox Grid instance.
Infoblox Username	Enter your Infoblox username to authenticate.
Infoblox Password	Enter your Infoblox password to authenticate.
Infoblox RPZ	The name of the Response Policy Zone created on the Infoblox Grid appliance.
DNS View	The name of the DNS view in which the record resides. The default value for DNS view is "default".
Disable Proxies	Enable or disable verification of SSL connections with the provider.
Verify Host SSL	If enabled, the action will not honor proxy settings within ThreatQ.


PARAMETER

DESCRIPTION

Objects per run

Maximum number of objects to send to Infoblox per-run.

< Infoblox Grid Remove From RPZ



Uninstall

Additional Information

Integration Type: Action

Version:

Action ID: 6

Accepted Data Types:

- Indicators
 - CIDR Block
 - FQDN
 - IP Address

Configuration

Infoblox Grid URL

Specify full URL to the Infoblox Grid instance.

Infoblox Username

admin

Enter your Infoblox username to authenticate.

Infoblox Password

Enter your Infoblox password to authenticate.

Infoblox RPZ

test

The name of the Response Policy Zone created on the Infoblox Grid appliance.

DNS View

default

The name of the DNS view in which the record resides. The default value for DNS view is "default".

☐ Disable Proxies

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

☐ Enable SSL Verification

Objects per run

10000

Maximum number of objects per-run

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

Actions

The following actions are available:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Infoblox Grid Add To RPZ	Adds Indicators to a RPZ Zone.	Indicators	IP Address, CIDR Block, FQDN
Infoblox Grid Remove From RPZ	Deletes Indicators from a RPZ Zone.	Indicators	IP Address, CIDR Block, FQDN

Infoblox Grid Add to RPZ

The Infoblox Grid Add to RPZ action uploads the indicators from the selected collection to an existing RPZ Zone from Infoblox Grid. The indicators are added only if they do not have the attribute **Added to Infoblox RPZ** equal to user config **Infoblox RPZ**. The name of the zone must be specified in the action configuration. The action adds the attribute **Added to Infoblox RPZ** to all the exported indicators and it deletes the attribute **Removed From Infoblox RPZ** having the value equal to the specified zone.

POST "{{INFOBLOX_URL}}/wapi/v2.12/record:rpz:cname"

Sample Body:

```
{
  "canonical": "217.60.9.178",
  "name": "217.60.9.178.{{RPZ_NAME}}",
  "rp_zone": "{{RPZ_NAME}}",
  "disable": false,
  "view": "default"
}
```

Sample Response:

```
"record:rpz:cname/
ZG5zLmJpbmRfY25hbWUkLl9kZWZhdWx0LnRocmVhdHEuMTgwLjE2NC43Mi4xNDg:217.60.9.178.
{{RPZ_NAME}}/default"
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
N/A	Indicator.Attribute	Added to Infoblox RPZ	N/A	RPZ Name	The value is the user config Infoblox RPZ



The attribute **Removed From Infoblox RPZ** is removed if it has the value equal to user config **Infoblox RPZ**.

Infoblox Grid Remove from RPZ

The Infoblox Grid Remove from RPZ action deletes the indicators from an existing RPZ Zone from Infoblox Grid. The indicators are removed only if they do not have the attribute `Removed From Infoblox RPZ` equal to `user config Infoblox RPZ`. The name of the zone must be specified in the action configuration. The action adds the attribute `Removed From Infoblox RPZ` to all the indicators from the input collection and it deletes the attribute `Added to Infoblox RPZ` having the value equal to the specified zone.

POST "{{INFOBLOX_URL}}/wapi/v2.12/request"

Sample Body:


```
[
  {
    "method": "GET",
    "object": "record:rpz:cname",
    "data": {
      "name": "217.60.9.178.{{RPZ_NAME}}",
      "view": "default"
    },
    "assign_state": {
      "name_ref": "_ref"
    }
  },
  {
    "method": "DELETE",
    "object": "##STATE:name_ref:##",
    "enable_substitution": true,
    "discard": true
  }
]
```

Sample Response:

```
{
  "result": [
    {
      "_ref": "record:rpz:cname/
ZG5zLmJpbmRfY25hbWUKLl9kZWZhdWx0LnRocmVhdHEuY29tLnhwdG94cA:217.60.9.178.
{{RPZ_NAME}}/default",
      "canonical": "217.60.9.178",
      "name": "217.60.9.178.threatq",
      "view": "default"
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
N/A	Indicator.Attribute	Removed From Infoblox RPZ	N/A	RPZ Name	The value is the user config Infoblox RPZ



The attribute **Added To Infoblox RPZ** is removed if it has the value equal to user config **Infoblox RPZ**.

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.

Infoblox Grid Add to RPZ

METRIC	RESULT
Run Time	1 minute
Indicators	100
Indicator Attributes	100

Infoblox Grid Remove from RPZ

METRIC	RESULT
Run Time	1 minute
Indicators	100
Indicator Attributes	100

Change Log

- Version 1.0.0
 - Initial release