

ThreatQuotient

A Securonix Company



Imperva Action

Version 1.0.0

August 05, 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	3
Support	4
Integration Details.....	5
Introduction	6
Prerequisites	7
Installation.....	8
Configuration	9
Actions	12
Imperva - WAF Policy Management	13
Imperva - Search Policy (supplemental).....	14
Imperva - Create Policy (supplemental)	15
Imperva - Add IPs to Policy (supplemental).....	17
Imperva - Delete Policy (supplemental)	19
Known Issues / Limitations	20
Change Log	21

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	>= 5.26.0
----------------------------------	-----------

ThreatQ TQO License Required	Yes
------------------------------	-----

Support Tier	ThreatQ Supported
--------------	-------------------

Introduction

The Imperva Action integration for ThreatQ enables the automatic export of IP Addresses from ThreatQ to an Imperva WAF Policy.

The integration provides the following action:

- **Imperva - WAF Policy Management** - exports IP Addresses from the ThreatQ platform to Imperva.

The action 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 if the following indicator types:
 - CIDR Block
 - IP Address
 - IPv6 Address
- An Imperva API ID and 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
Imperva API ID	Enter your Imperva API ID used to authenticate.
Imperva API Key	Enter Your Imperva API Key used to authenticate.
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.
Imperva WAF Policy Name	Enter a name for an existing policy. <div>  If the policy does not exist on Imperva, a new policy will be created. </div>
Policy Description	Enter a description to be added when a policy is created.

PARAMETER	DESCRIPTION
Action	<p>Select the action performed on the requests arriving from each IP Address. Options include:</p> <ul style="list-style-type: none"> ◦ Block (<i>default</i>) ◦ Allow <div>  <p>Modifying the action for an existing policy necessitates the recreation of that policy and all the existing IP Addresses are deleted.</p> </div>
Clear IP Address List on Manual Run	<p>Enable this parameter to automatically delete and recreate the policy 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 enabled by default.</p>
Objects Per Run	<p>Enter the number of objects to process per run of the workflow.</p>

< Imperva - WAF Policy Management



Uninstall

Additional Information

Integration Type: Action

Version:

Action ID: 1

Accepted Data Types:

Indicators

IP Address

IPv6 Address

CIDR Block

Configuration

Authentication and Connection

Imperva API ID

Enter the Imperva API ID to authenticate.

Imperva API Key

Enter your Imperva API Key to authenticate.

☒ Enable SSL Certificate Verification

When checked, validates the host-provided SSL certificate.

☐ Disable Proxies

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

Export Options

Imperva WAF Policy Name

ThreatQ Blocklist

Enter a name for an existing policy, or a new policy to be created.

Policy Description

ACL Policy created by ThreatQ

Enter a description to add in case the policy is created.

Action

Block

Select the action performed on the requests arriving from each IP Address. Modifying the action for an existing policy necessitates the recreation of that policy and all the existing IP Addresses are deleted.

☒ Clear IP Address List on Manual Run

Enabling this will automatically delete and recreate the policy before exporting new objects to it. This is done to ensure that the list is always up-to-date with the ThreatQ data collection.

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
Imperva - WAF Policy Management	Exports IP Addresses from a ThreatQ data collection to Imperva.	Indicator	IP Address

Imperva - WAF Policy Management

The Imperva - WAF Policy Management action exports IP Addresses from a ThreatQ data collection to Imperva.

The action utilizes four supplemental feeds:

- [Imperva - Search Policy](#)
- [Imperva - Create Policy](#)
- [Imperva - Add IPs to Policy](#)
- [Imperva - Delete Policy](#)

Imperva - Search Policy (supplemental)

The Imperva - Search Policy supplemental feed returns all the WAF policies from Imperva and searches for the name supplied in the user configuration **Imperva WAF Policy Name** parameter.

GET <https://api.imperva.com/policies/v2/policies?extended=true>

Sample Response:

```
{
  "value": [
    {
      "defaultPolicyConfig": [],
      "policySettings": [
        {
          "id": 8178855,
          "policyId": 1943815,
          "settingsAction": "BLOCK",
          "policySettingType": "IP",
          "data": {
            "ips": [
              "5.15.134.0/24",
              "2606:4700:4700:0000:0000:0000:1111",
              "1.0.0.1"
            ]
          },
          "policyDataExceptions": []
        }
      ],
      "id": 1943815,
      "name": "ThreatQ Blocklist",
      "description": "ACL Policy created by ThreatQ",
      "enabled": true,
      "accountId": 2359055,
      "policyType": "ACL",
      "lastModified": "Aug 1, 2025, 7:13:50 AM",
      "lastModifiedBy": 2689953,
      "blockRoute": true
    }
  ],
  "isError": false
}
```



ThreatQuotient does not provide a mapping for this function. If a policy is found the keys `.id` and `.policySettings.id[policySettingType=IP]` are used in the next requests as `POLICY_ID` and `POLICY_IP_SETTING_ID`.

Imperva - Create Policy (supplemental)

The Imperva - Create Policy supplemental feed creates a new policy in the event it does exist or it was deleted (the policy type was changed, or it was cleared during a manual run).

POST <https://api.imperva.com/policies/v2/policies>

Sample Body:

```
{
  "name": "ThreatQ Blocklist",
  "description": "ACL Policy created by ThreatQ",
  "enabled": true,
  "policyType": "ACL",
  "policySettings": [
    {
      "settingsAction": "BLOCK",
      "policySettingType": "IP",
      "data": {
        "ips": [
          "1.2.3.4",
          "8.8.8.8"
        ]
      }
    }
  ]
}
```

Sample Response:

```
{
  "value": {
    "defaultPolicyConfig": [],
    "policySettings": [
      {
        "id": 8179147,
        "policyId": 1943865,
        "settingsAction": "BLOCK",
        "policySettingType": "IP",
        "data": {
          "ips": [
            "1.2.3.4",
            "8.8.8.8"
          ]
        },
        "policyDataExceptions": []
      }
    ],
    "id": 1943865,
    "name": "ThreatQ Blocklist",
    "description": "ACL Policy created by ThreatQ",
  }
}
```

```
"enabled": true,  
"accountId": 2359055,  
"policyType": "ACL",  
"lastModified": "Aug 1, 2025, 9:15:51 AM",  
"lastModifiedBy": 2689953,  
"blockRoute": true  
},  
"isError": false  
}
```



ThreatQuotient does not provide a mapping for this function. The keys `.id` and `.policySettings.id[policySettingType=IP]` are used in the next requests as `POLICY_ID` and `POLICY_IP_SETTING_ID`.

Imperva - Add IPs to Policy (supplemental)

The Imperva - Add IPs to Policy supplemental feed appends IP Address to the exiting WAF Policy.

POST https://api.imperva.com/policies/v2/policies/{{POLICY_ID}}

Sample Body:

```
{
  "policySettings": [
    {
      "id": "{{POLICY_IP_SETTING_ID}}",
      "settingsAction": "BLOCK",
      "policySettingType": "IP",
      "data": {
        "ips": [
          "1.2.3.5",
          "8.8.8.9"
        ]
      }
    }
  ]
}
```

Sample Response:

```
{
  "isError": false,
  "value": {
    "accountId": 2359055,
    "defaultPolicyConfig": [],
    "description": "ACL Policy created by ThreatQ",
    "enabled": true,
    "id": 1943815,
    "lastModified": "Aug 1, 2025, 7:13:49 AM",
    "lastModifiedBy": 2689953,
    "name": "ThreatQ Blocklist",
    "policySettings": [
      {
        "data": {
          "ips": [
            "1.2.3.4",
            "8.8.8.8",
            "1.2.3.5",
            "8.8.8.9"
          ]
        },
        "id": 8178855,
        "policyDataExceptions": [],
        "policyId": 1943815,
        "policySettingType": "IP",
        "settingsAction": "BLOCK"
      }
    ]
  }
}
```

```
    }  
  ],  
  "policyType": "ACL"  
}  
}
```



ThreatQuotient does not provide a mapping for this function since it only exports the IOCs.

Imperva - Delete Policy (supplemental)

The Imperva - Delete Policy supplemental feed deletes the WAF Policy if the policy type was changed or the user performs a manual run and the **Clear IP Address List on Manual Run** configuration parameter is enabled.

DELETE `https://api.imperva.com/policies/v2/policies/{{POLICY_ID}}`

Sample Response:

```
{
  "isError": false,
  "value": "Deleted successfully"
}
```



ThreatQuotient does not provide a mapping for this function.

Known Issues / Limitations

- Changing the action for a policy (Allow - Whitelist / Block - ACL) necessitates the recreation of that policy and all the existing IP Addresses are deleted.
- Performing a manual run with the configuration `Clear IP Address List on Manual Run` enabled necessitates the recreation of that policy and all the existing IP Addresses are deleted.

Change Log

- Version 1.0.0
 - Initial release