ThreatQuotient

ThreatQ Action for Microsoft Defender

Version 1.1.0

March 17, 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	1.1.0
Compatible with ThreatQ Versions	>= 5.25.0
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The ThreatQ Action for Microsoft Defender integration allows you to export indicators directly to Microsoft Defender via Microsoft's Defender API.

The integration provides the following action:

- **Microsoft Defender Export Collection -** submits the indicators in a ThreatQ data collection to Microsoft Defender.

The action is compatible with the following indicator types:

- FQDN
- IP Address
- IPv6 Address
- MD5
- SHA-1
- SHA-256
- URL

> This action is intended for use with ThreatQ TDR Orchestrator (TQO). An active TQO license is required for this feature.

Prerequisites

The following is required in order the use this integration's actions:

- An active ThreatQ TDR Orchestrator (TQO) license.
- A data collection containing at least one of the following indicator types:
    - FQDN
    - IP Address
    - IPv6 Address
    - MD5
    - SHA-1
    - SHA-256
    - URL
- A ThreatQ App registration in Microsoft Azure - see the following link for more information - https://learn.microsoft.com/en-us/azure/azure-monitor/logs/api/register-app-for-token
- A Microsoft Defender Tenant ID.
- A Microsoft Defender Client ID.
- A Microsoft Defender Client Secret.
- Your Azure Application must have WindowsDefenderATP Permissions.

Azure Application Permissions

Your Microsoft Azure Application must have **WindowsDefenderATP** access for the `Ti.ReadWrite.All` and `Ti.ReadWrite` permissions.

1. Select **Add a Permission** under the API permissions for your Azure Application.
2. Click on the **APIs my organization uses** tab.
3. Search for **WindowsDefenderATP** and select the result.
4. Select the **Application Permissions** box when prompted.
5. Search and enable `Ti.ReadWrite.All` and `Ti.ReadWrite` permissions.
6. Click the **Add permissions** button.
7. Click on **Grant admin consent for <Organization>** button to fully enable the permissions.

> This last step may take several minutes to propagate the permissions to your Application. See the following link for additional information: https://learn.microsoft.com/en-us/defender-endpoint/api/import-ti-indicators.

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:

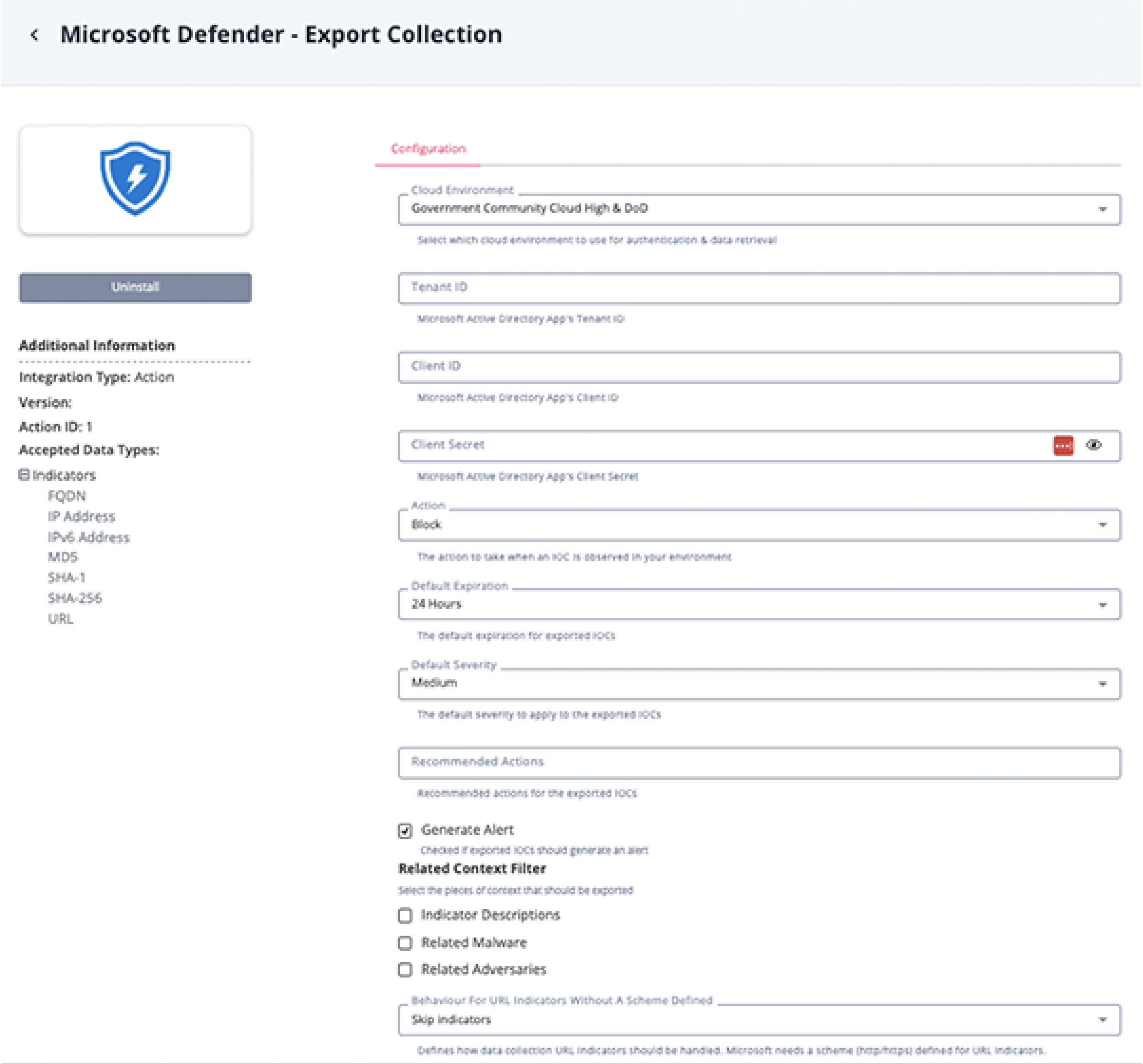
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Actions** option from the *Category* dropdown (optional).
3. Click on the action entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

> 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
Cloud Environment	Select which cloud environment to use for authentication and data retrieval. Options include: ◦ Global (default) ◦ Government Community Cloud ◦ Government Community Cloud High & DoD
Tenant ID	Your Microsoft Active Directory App's Tenant ID.
Client ID	Your Microsoft Active Directory App's Client ID.
Client Secret	Your Microsoft Active Directory App's Client Secret.
Action	The action to take when an IOC is observed in your environment. Options include: ◦ Allow ◦ Warn ◦ Block ◦ Audit ◦ Alert ◦ Alert and Block

PARAMETER	DESCRIPTION
	◦ Block and Remediate
Default Expiration Days	Set the number of days the indicators should remain valid.
Default Severity	Select the default severity to apply to the exported IOCs if attribute `Severity` is not present. Options include: ◦ Informational ◦ Low ◦ Medium ◦ High The default value configured in the UI for `Severity` can be overwritten by adding an indicator attribute whose name is `Severity` and whose value is one of the following: `Informational`, `Low`, `Medium` or `High`.
Recommended Actions	Set the recommended actions for the exported IOCs.
Generate Alert	Enable this parameter if the exported IOCs should generate an alert.
Related Context Filter	Select the pieces of context that should be exported. Options include: ◦ Indicator Descriptions ◦ Related Malware ◦ Related Adversaries
Behaviour for URL indicators without a scheme defined	Define how data collection URL indicators should be handled. Microsoft needs a scheme (http/https) defined for URL indicators. Options include: ◦ Skip Indicators ◦ Add "http" ◦ Add "https"
Hostname	Your ThreatQ Hostname.

PARAMETER	DESCRIPTION
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.
Objects Per Run	The max number of objects to send to this action per run.



‹ Microsoft Defender - Export Collection

Uninstall

Additional Information

Integration Type: Action

Version:

Action ID: 1

Accepted Data Types:

⊟ Indicators

- FQDN
- IP Address
- IPv6 Address
- MD5
- SHA-1
- SHA-256
- URL

Configuration

Cloud Environment: Government Community Cloud High & DoD

Select which cloud environment to use for authentication & data retrieval

Tenant ID

Microsoft Active Directory App's Tenant ID

Client ID

Microsoft Active Directory App's Client ID

Client Secret

Microsoft Active Directory App's Client Secret

Action: Block

The action to take when an IOC is observed in your environment

Default Expiration: 24 Hours

The default expiration for exported IOCs

Default Severity: Medium

The default severity to apply to the exported IOCs

Recommended Actions

Recommended actions for the exported IOCs

☑ Generate Alert

Checked if exported IOCs should generate an alert

Related Context Filter

Select the pieces of context that should be exported

☐ Indicator Descriptions

☐ Related Malware

☐ Related Adversaries

Behaviour For URL Indicators Without A Scheme Defined: Skip indicators

Defines how data collection URL indicators should be handled. Microsoft needs a scheme (http/https) defined for URL indicators.

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
Microsoft Defender Export Collection	Add Indicators to Microsoft Defender.	Indicators	IP Address, IPv6 Address, URL, FQDN, MD5, SHA-256, SHA-1

Microsoft Defender Export Collection

The Microsoft Defender Export Collection action submits the indicators in a ThreatQ data collection to Microsoft Defender.

Cloud Environment Endpoints

- **Global**
    - Login - `https://login.microsoftonline.com`
    - Resource - `https://api.securitycenter.microsoft.com`
- **Government Community Cloud**
    - Login - `https://login.microsoftonline.com`
    - Resource - `https://api-gcc.securitycenter.microsoft.us`
- **Government Community Cloud High & DOD**
    - Login - `https://login.microsoftonline.us`
    - Resource - `https://api-gov.securitycenter.microsoft.us`

`POST "https://{{ cloud_environment }}/api/indicators/import"`

Sample Body:

```
{
  "Indicators": [
    {
      "action": "Allowed",
      "description": "IOC exported from ThreatQ.\nDetails page: https://
{{TQ_HOSTNAME}}/indicators/7284/details",
      "expirationTime": "2024-04-15T08:58:22Z",
      "generateAlert": false,
      "indicatorType": "FileMd5",
      "indicatorValue": "f4c3fa43b5bdfaa0205990d25ce51c5f",
      "recommendedActions": null,
      "severity": "Low",
      "title": "f4c3fa43b5bdfaa0205990d25ce51c5f"
    }
  ]
}
```

Sample Response:

```
{
  "@odata.context": "https://api.securitycenter.microsoft.com/api/
$metadata#Collection(microsoft.windowsDefenderATP.api.ImportIndicatorResult)",
  "value": [
    {
      "id": "102149",
      "indicator": "f4c3fa43b5bdfaa0205990d25ce51c5f",
      "isFailed": false,
      "failureReason": null
    }
  ]
}
```

Microsoft Defender Indicator Type Mapping

The following table illustrates the Microsoft Defender to ThreatQ indicator type mapping.

MICROSOFT DEFENDER INDICATOR TYPE	THREATQ INDICATOR TYPE
FileMd5	MD5
FileSha1	SHA-1
FileSha256	SHA-256
IpAddress	IP Address
IpAddress	IPv6 Address
DomainName	FQDN
Url	URL

Change Log

- **Version 1.1.0**
    - Added support for Gov-Cloud and DoD environments.
    - Added the following new configuration parameters:
        - **Cloud Environment -** allows you to select the cloud environment.
        - **Enable SSL Certificate Verification -** enable or disable verification of the server's SSL certificate.
        - **Disable Proxies -** determines if the action should honor proxy settings set in the ThreatQ UI.
    - Renamed the integration and provided action to reflect current vendor branding:
        - **ThreatQ Action for Microsoft 365 Defender** is now **ThreatQ Action for Microsoft Defender**.
            - **Microsoft 365 Defender - Export Collection** is now **Microsoft Defender - Export Collection**.
- **Version 1.0.0 rev-b**
    - Guide Update - updated the requirements and permission sections in the **Prerequisites** chapter.
- **Version 1.0.0**
    - Initial release