

ThreatQuotient



ThreatQ Operation for Microsoft 365 Defender

Version 1.0.0 rev-a

March 06, 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
 - Azure Application Permissions 7
- Installation..... 8
- Configuration 9
- Actions 10
 - Create Policy 11
 - Action Run Parameters 12
- Revoke Policy 13
- Known Issues/Limitations 14
- Change Log 15

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	>= 4.30.0
Support Tier	ThreatQ Supported

Introduction

The ThreatQ Operation for Microsoft 365 Defender enables analysts to export IOCs to Microsoft 365 Defender and set actions and expirations.

The operation provides the following actions:

- **Create Policy** - Whitelist or blacklist IOCs from ThreatQ in Microsoft 365 Defender.
- **Revoke Policy** - Remove a policy from Microsoft 365 Defender that had previously been sent from ThreatQ.

The operation is compatible with the following indicator types:

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

Prerequisites

The following is required to run the operation:

- 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 365 Defender Tenant ID.
- A Microsoft 365 Defender Client ID.
- A Microsoft 365 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 integration file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration file using one of the following methods:
 - Drag and drop the file into the dialog box
 - Select **Click to Browse** to locate the integration file on your local machine



ThreatQ will inform you if the operation already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the operation contains changes to the user configuration. The new user configurations will overwrite the existing ones for the operation and will require user confirmation before proceeding.

The operation is now installed and will be displayed in the ThreatQ UI. You will still need to [configure](#) and then [enable](#) the operation.

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 **Operation** option from the *Type* dropdown (optional).
3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Microsoft 365 Defender Tenant ID	Enter your Microsoft 365 Defender Tenant ID.
Microsoft 365 Defender Client ID	Enter your Microsoft 365 Defender Client ID to authenticate.
Microsoft 365 Defender Client Secret	Enter your Microsoft 365 Defender Client Secret to authenticate.

Configuration



☐ Bypass system proxy configuration for this operation

Save

5. Review any additional settings, make any changes if needed, and click on **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable it.


Actions

The operation provides the following actions:

ACTION	DESCRIPTION	OBJECT TYPES	OBJECT SUBTYPE
Create Policy	Whitelist or blacklist IOC's from ThreatQ in Microsoft 365 Defender	Indicators	SHA-1, SHA-256, MD5, FQDN, IP Address, URL
Revoke Policy	Remove a policy from Microsoft 365 Defender that had previously been sent from ThreatQ	Indicators	SHA-1, SHA-256, MD5, FQDN, IP Address, URL

Action Run Parameters

This Action has the following Configuration options:

PARAMETER	DESCRIPTION
Action	The action that will be taken if the indicator is discovered in the organization.
Severity	<p>Selects the severity of the indicator.</p> <div>  <p>This setting is required for Audit, Block and Remediate and Block Execution actions.</p> </div>
Recommended Actions	Describe the recommended action to take if the indicator is discovered in the organization. Only used for 'Audit' action or when generating an alert.
IOC Expiration	An expiration to be set for the IOC within Microsoft 365 Defender.
Description	A description of the indicator. If left blank, it will try to use the description within ThreatQ.
Generate Alert	Generate an alert in Microsoft 365 Defender.

Revoke Policy

The Revoke Policy action revokes a policy from Microsoft 365 Defender that was created from this operation. The action also removes the attribute that showed that the IOC had been sent.

DELETE <https://api.securitycenter.microsoft.com/api/indicators/{id}>



There is no API response for this action.

Known Issues/Limitations

- The operation does not update the same indicator if changes are made when operation is rerun. Instead, it deletes the old indicator and creates a new one.
- Microsoft 365 Defender API parameters and UI parameters have changed slightly and may do so again in the future. Future updates of the operation will address these changes as they are made by Microsoft.

Change Log

- **Version 1.0.0 rev-a**
 - Guide Update - updated the requirements and permission sections in the Prerequisites chapter.
- **Version 1.0.0**
 - Initial release