ThreatQuotient

ThreatQ Action for Microsoft Entra

Version 1.0.0

September 16, 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.

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 Microsoft Entra integration allows a ThreatQ user to interact with the Microsoft cloud-based identity and access management service. This can be used to control access to external Microsoft resources and applications.

The integration provides the following action:

- **Microsoft Entra Conditional Access Policy** - creates or updates a Microsoft Entra Conditional Access Policy that blocks access to applications based on network locations.

The action is compatible with the following indicator types:

- IP Address
- IPv6 Address
- CIDR Block

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:
  - IP Address
  - IPv6 Address
  - CIDR Block

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:

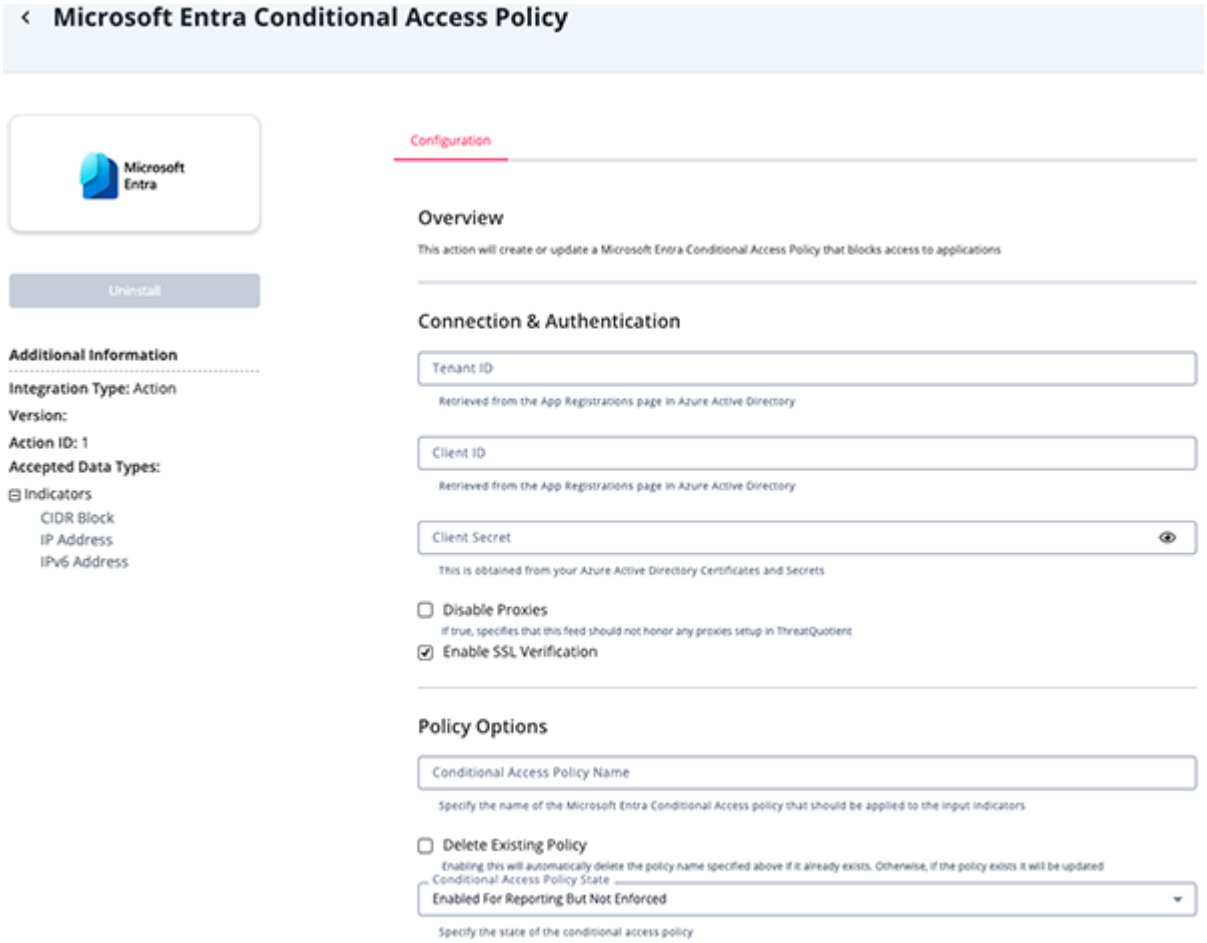
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Actions** option from the *Category* dropdown (optional).
3. Click on the action entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

> 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
Tenant ID	Enter your Microsoft Tenant ID. This is retrieved from the App Registrations page in the Azure Active Directory.
Client ID	Enter your Microsoft Client ID. This is retrieved from the App Registrations page in the Azure Active Directory.
Client Secret	Enter your Microsoft Tenant ID. This is obtained from your Azure Active Directory Certificates and Secrets.
Disable Proxies	Enable this option to have the action ignore proxies set in the ThreatQ UI.
Enable SSL Verification	Enable this option if the action should verify the SSL certificate.
Conditional Access Policy Name	Specify the name of the Microsoft Entra Conditional Access policy that should be applied to the input indicators.

PARAMETER	DESCRIPTION
Delete Existing Policy	Enabling this option to automatically delete the policy name specified above if it already exists. Otherwise, if the policy exists, it will be updated.
Conditional Access Policy State	Specify the state of the conditional access policy. Options include: ◦ Enabled ◦ Disabled ◦ Enabled for Reporting But Not Enforced
Sign-in Risk Level (Optional)	Sign-in risk levels included in the policy. Options include: ◦ Low ◦ Medium ◦ High
Applications Excluded From The Policy	Select an application suite from this list that should be excluded from the policy. Options include: ◦ Office 365 Applications Suite ◦ Microsoft Admin Portals
Client IDs (appId) Explicitly Excluded From The Policy	To exclude particular apps enter a comma-separated list of app Ids that should be excluded from the policy.
Applications Included In The Policy	Select an application suite from this list that should be included in the policy. Options include: ◦ All ◦ Office 365 Applications Suite ◦ Microsoft Admin Portals
Client IDs (appId) Explicitly Included In The Policy	To include particular apps enter a comma-separated list of app Ids that should be included in the policy.
Client Application Types (Optional)	Select the client application types included in the policy. If All is selected the other enabled types are ignored. Options include: ◦ All ◦ Browser

PARAMETER	DESCRIPTION
	◦ Mobile Apps And Desktop Clients ◦ Exchange Active Sync ◦ Other
Network Location Name	Specify the name of the network location where the input indicators are uploaded to.
Clear Network Location on Manual Run	Enabling this will clear the existing values in the network location specified above. This is done to ensure that the location is always up-to-date with the ThreatQ data collection.
Network Location Is Trusted	Enabled this option if this network location is explicitly trusted.
Exclude Network Location	Enable this option if this network location should be excluded from the policy.
Platforms excluded from the policy scope	Select the platforms excluded from the policy scope. Options include: ◦ All ◦ Android ◦ iOS ◦ Windows ◦ Windows Phone ◦ Mac OS ◦ Linux
Platforms included in the policy scope	Select the platforms included in the policy scope.Options include: ◦ All ◦ Android ◦ iOS ◦ Windows ◦ Windows Phone ◦ Mac OS ◦ Linux
Objects per run	Maximum number of objects to process 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
Microsoft Entra Conditional Access Policy	Creates a conditional access policy that blocks access to applications based on IP Addresses	Indicators	IP Address, IPv6 Address, CIDR Block

Microsoft Entra Conditional Access Policy

The Microsoft Entra Conditional Acccess Policy action creates a network location using the input indicators.

> The network location allows only IP Ranges.

Indicators of type IP Address are converted to IP range using /32 mask. IPv6 Addresses are converted to IP range using /128 mask. This network location can always be re-created or it can be updated at each new run.

After the network location is created the function creates a conditional access policy that blocks access to applications for the IP ranges uploaded to the network location. The policy can be always re-created or it can be updated at each new run.

`POST https://graph.microsoft.com/v1.0/identity/conditionalAccess/policies`

Sample Body:

```
{
  "conditions": {
    "applications": {
      "excludeApplications": [
        "81fc9bc8-1140-43e1-a525-336e4e654561",
        "a1c1be3d-ca33-4606-a9e6-97fe099e3902",
        "MicrosoftAdminPortals"
      ],
      "includeApplications": [
        "0ed33d48-cb51-4711-953d-4468c52da87d",
        "Office365"
      ]
    },
    "locations": {
      "excludeLocations": [],
      "includeLocations": [
        "028b6391-2bdf-4ea6-b843-52b35d5c0568"
      ]
    },
    "platforms": {
      "excludePlatforms": [
        "iOS"
      ],
      "includePlatforms": [
        "all"
      ]
    },
    "signInRiskLevels": [
      "low"
    ],
    "users": {
```

```
      "includeUsers": [
        "none"
      ]
    }
  },
  "grantControls": {
    "builtInControls": [
      "block"
    ],
    "operator": "OR"
  },
  "state": "enabled"
}
```

Sample Response:

```
{
  "@odata.context": "https://graph.microsoft.com/v1.0/$metadata#identity/
conditionalAccess/policies/$entity",
  "conditions": {
    "applications": {
      "applicationFilter": null,
      "excludeApplications": [
        "81fc9bc8-1140-43e1-a525-336e4e654561",
        "a1c1be3d-ca33-4606-a9e6-97fe099e3902",
        "MicrosoftAdminPortals"
      ],
      "includeApplications": [
        "0ed33d48-cb51-4711-953d-4468c52da87d",
        "Office365"
      ],
      "includeAuthenticationContextClassReferences": [],
      "includeUserActions": []
    },
    "clientAppTypes": [],
    "clientApplications": null,
    "devices": null,
    "insiderRiskLevels": null,
    "locations": {
      "excludeLocations": [],
      "includeLocations": [
        "028b6391-2bdf-4ea6-b843-52b35d5c0568"
      ]
    },
    "platforms": {
      "excludePlatforms": [
        "iOS"
      ],
      "includePlatforms": [
        "all"
      ]
```

```
    },
    "servicePrincipalRiskLevels": [],
    "signInRiskLevels": [
      "low"
    ],
    "userRiskLevels": [],
    "users": {
      "excludeGroups": [],
      "excludeGuestsOrExternalUsers": null,
      "excludeRoles": [],
      "excludeUsers": [],
      "includeGroups": [],
      "includeGuestsOrExternalUsers": null,
      "includeRoles": [],
      "includeUsers": [
        "None"
      ]
    }
  },
  "createdDateTime": "2024-09-11T10:11:30.2438623Z",
  "displayName": "ms_entra_act_policy",
  "grantControls": {
    "authenticationStrength": null,
    "authenticationStrength@odata.context": "https://graph.microsoft.com/
v1.0/$metadata#identity/conditionalAccess/policies('bf70a9a4-
bfdb-469b-8dcb-0c99218a02b0')/grantControls/authenticationStrength/$entity",
    "builtInControls": [
      "block"
    ],
    "customAuthenticationFactors": [],
    "operator": "OR",
    "termsOfUse": []
  },
  "id": "bf70a9a4-bfdb-469b-8dcb-0c99218a02b0",
  "modifiedDateTime": null,
  "sessionControls": null,
  "state": "enabled",
  "templateId": null
}
```

Use Case Example

1. A Threat Analyst identifies a collection of IPs for which they would like to create a Microsoft Entra Conditional Access Policy
2. The Threat Analyst adds the Microsoft Entra Conditional Access Policy action to a Workflow
3. The Threat Analyst configures the action with the desired parameters, and enables the Workflow
4. The Workflow executes all Actions in the graph, including Microsoft Entra Conditional Access Policy
5. The action adds the IPs from the collection to a network location and creates the policy

Known Issues / Limitations

- Not all values specified in `Client Application Types` are compatible with all platforms. Selecting incompatible values throws 400 Bad Request.

Change Log

- **Version 1.0.0**
  - Initial release