

ThreatQuotient



ThreatQ CDF for Microsoft Entra

Version 1.0.0

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 3

Support 4

Integration Details..... 5

Introduction 6

Prerequisites 7

 Microsoft Graph Required Permissions 7

Installation..... 8

Configuration 9

ThreatQ Mapping..... 12

 Microsoft Entra Users..... 12

Average Feed Run..... 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	>= 5.29.0
Compatible Third-Party Environment	Microsoft Azure Cloud
Support Tier	ThreatQ Supported

Introduction

The ThreatQ CDF for Microsoft Entra integration provides users with the ability to import Microsoft Entra Users into the ThreatQ platform.

The integration provides the following feed:

- **Microsoft Entra Users** - ingests users from a Microsoft Azure Organization into ThreatQ as Identity objects.

The integration ingests Identity and Identity Attribute system object types.

Prerequisites

The following is required to run the integration:

- Azure Tenant ID
- Azure Client ID
- Azure Client Secret
- A Microsoft Azure Application with Microsoft Graph access for the User.ReadWrite.All permission.

Microsoft Graph Required Permissions

Your Microsoft Azure Application must have Microsoft Graph access for the User.ReadWrite permission.

1. Navigate to the **API Permissions** for your Azure Application.
2. Click on **Add a Permission**.
3. Click on **Microsoft Graph > Application Permissions**.
4. Search and enable the User.ReadWrite.All permission.
5. Click on the **Add permissions** button.
6. 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/graph/api/user-list>

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



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

The feed will be added to the integrations page. You will still need to [configure and then enable](#) the feed.

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 **Commercial** option from the *Category* dropdown (optional).



If you are installing the integration for the first time, it will be located under the **Disabled** tab.

3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Azure Tenant ID	<p>Enter your Azure Tenant ID.</p> <p> This can be obtained from the Azure Active Directory App Registrations page.</p>
Azure Client ID	<p>Enter your Azure Client ID.</p> <p> This can be obtained from the Azure Active Directory App Registrations page.</p>
Azure Client Secret	<p>Enter your Azure Client Secret.</p> <p> This can be obtained from the Azure Active Directory Certificates and Secrets page.</p>
Enable SSL Certificate Verification	<p>Enable or disable verification of the server's SSL certificate.</p>

← Microsoft Entra Users

-
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.

ThreatQ Mapping

Microsoft Entra Users

The Microsoft Entra Users feed ingests as ThreatQ Identity objects the users from a Microsoft Azure Organization using Microsoft Entra. The feed can be configured to ingest all the users or only those from a specific domain via the **Domain** configuration parameter.

GET <https://graph.microsoft.com/v1.0/users>

Sample Request Parameters:

```
{
  "$select":
  "displayName,businessPhones,jobTitle,officeLocation,userPrincipalName,streetAddress,city,state,country,accountEnabled,createdDateTime",
  "$filter": "endsWith(userPrincipalName,threatq.com)",
  "$count": "true"
}
```

Sample Response:

```
[
  {
    "@odata.context": "https://graph.microsoft.com/v1.0/$metadata#users(displayName,businessPhones,jobTitle,officeLocation,userPrincipalName,streetAddress,city,state,country,accountEnabled,createdDateTime)",
    "value": [
      {
        "accountEnabled": true,
        "businessPhones": [
          "3046169799"
        ],
        "city": "Martinsburg",
        "country": "US",
        "createdDateTime": "2020-11-24T15:50:56Z",
        "displayName": "threatq",
        "jobTitle": "Threat Intelligence Engineer Intern",
        "officeLocation": "3046169773",
        "state": "West Virginia",
        "streetAddress": "171 ABC",
        "userPrincipalName": "threatq@threatq.com"
      }
    ]
  }
]
```

ThreatQuotient provides the following default mapping for this feed based on fields within each of the value:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.displayName	Identity.Value	Identity	.createdDateT ime	threatq	N/A
.userPrincipalName	Identity.Attribute	User Principal Name	.createdDateT ime	threatq@threatq.com	User-configurable.
.businessPhones	Identity.Attribute	Business Phone	.createdDateT ime	3046169799	User-configurable.
.jobTitle	Identity.Attribute	Job Title	.createdDateT ime	Threat Intelligence Engineer Intern	User-configurable.
.accountEnabled	Identity.Attribute	Is Enabled	.createdDateT ime	True	User-configurable. Updatable.
.officeLocation	Identity.Attribute	Office Location	.createdDateT ime	3046169773	User-configurable.
.streetAddresses	Identity.Attribute	Street Address	.createdDateT ime	171 ABC	User-configurable.
.city	Identity.Attribute	City	.createdDateT ime	Martinsburg	User-configurable.
.state	Identity.Attribute	State	.createdDateT ime	West Virginia	User-configurable.
.country	Identity.Attribute	Country	.createdDateT ime	US	User-configurable.

Average Feed Run



Object counts and Feed runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and Feed runtime may vary based on system resources and load.

METRIC	RESULT
Run Time	1 minute
Identities	82
Identity Attributes	400

Change Log

- Version 1.0.0
 - Initial release