

ThreatQuotient



ThreatQ Operation for Microsoft Active Directory

Version 1.0.0

April 23, 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 3

Support 4

Integration Details..... 5

Introduction 6

Installation..... 7

Configuration 8

Actions 10

 Query 10

 Parameters 10

Change Log 11

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	>= 3.6.0
Support Tier	ThreatQ Supported

Introduction

The ThreatQ Operation for Microsoft Active Directory allows a ThreatQ user to query their Active Directory for identity matches.

The operation provides the following action:

- **Query** - queries your Active Directory for identity matches.

The operation is compatible with Email Address and Username Indicator types.

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 whl file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration whl 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 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
Server	Your Active Directory server. Include ldap:// or ldaps://.
Domain	The domain for your Active Directory Server.
Certificate	<p>If you are using SSL, provide a path to your certificate on your ThreatQ instance.</p> <div>  <p>This file must be accessible by the operation, so it must be placed on the ThreatQ instance in a directory that is accessible.</p> <p>Entering a path here will automatically enable SSL.</p> </div>
Use TLS	Use this parameter if you use TLS to connect to your Active Directory server.
Username	The username to authenticate with the Active Directory server.
Password	The password to authenticate with the Active Directory server.
Groups	A comma-delimited list of groups to perform the query on



It is possible to list multiple groups that are nested within each other.

It is not possible to list multiple groups that are at the same level.

You cannot use groups alongside organizational units.

Organizational Units

A comma-delimited list of organizational units to perform the query on



It is possible to list multiple organizational units that are nested within each other.

It is not possible to list multiple organizational units that are at the same level.

You cannot use organizational units alongside groups.

Version

The version of your Active Directory server.

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 action:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Query	Queries your Active Directory for identity matches.	Indicator	Email Address, Username

Query

The Query action allows you to query your Active Directory server for identity matches.

Parameters



This action allows you to override the settings that are set in the operation's configuration settings.

The Query action has the following parameters:

PARAMETER	DESCRIPTION
Groups (Override)	This allows you to override the Group setting in the operation's configuration.
Organizational Units (Override)	This allows a user to override the Organizational Units setting in the operation's configuration.

Change Log

- Version 1.0.0
 - Initial release