ThreatQuotient

Okta Operation Guide

Version 1.0.0

April 19, 2022

ThreatQuotient
11400 Commerce Park Dr., Suite 200
Reston, VA 20191

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.

Versioning

- Current integration version: `1.0.0`
- Supported on ThreatQ versions >= `4.35`

Introduction

The Okta Operation for ThreatQ enables analysts to execute actions against users in their Okta Directory

The operation provides the following action:

- **Take Action** - take an action on a given user such as Activate, Deactivate, Suspend etc.

The operation is compatible with **Identity** object types.

Prerequisites

The Okta operation requires an Okta API Token. Use the steps provided below to generate the required token.

Generate an Okta API Token

Follow these steps to generate an Okta API Token:

1. Log into your Okta Portal.
2. Using the left navigation, Navigate to to `Security -> API` in the left navigation menu.
3. Select the `Tokens` tab.
4. Click on the `Create Token` button.
5. Enter a name for the token. ThreatQuotient recommends naming it `ThreatQ`.
6. Click on the `Create` button.
7. Copy and save the token to a secure location to reference later.

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 feed 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.

   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 operation:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Operation** option from the **Type** 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 to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Okta Host	Okta Hostname (without HTTP Scheme)
Okta API Token	Okta API Token found under `Security -> API -> Tokens` within your portal

5. Click **Save**.
6. Click on the toggle switch, located above the **Additional Information** section, to enable the operation.

Actions

The operation provides the following action:

ACTION	DESCRIPTION	OBJECT TYPES	OBJECT SUB-TYPES
Take Action	Take an action on a given user such as Activate, Deactivate, Reactivate, Suspend, Unsuspend, Unlock, or Expire Password.	Identity	N/A

Take Action

The **Take Action** action allows you to take an action on a given user such as: Activate, Deactivate, Reactivate, Suspend, Unsuspend, Unlock, or Expire Password.

```
POST https://{okta_host}/api/v1/{user_id}/lifecycle/{action}
```

Due to the nature of this action, there is no API response data or mapping.

Configuration Options

ThreatQ provides the following parameters for the **Take Action** action:

PARAMETER	DESCRIPTION
Action:	Select the type of action to take on the user: Activate (Provision), Deactivate (De-Provision), Reactivate, Suspend, Unsuspend, Unlock, Expire Password
Send Email (Only Activate & Reactivate):	Do you want to send out an email when activating or reactivating the user?

Known Issues / Limitations

- Certain actions can only be taken on a user (identity) if the user is in a certain status.
  - **Example 1**: a user can only be suspended from the `ACTIVE` state.
  - **Example 2**: a user can only be activated from `STAGED` and `DEPROVISIONED` states.

Change Log

- **Version 1.0.0**
  - Initial release