

ThreatQuotient



Okta CDF Guide

Version 1.0.1

September 27, 2021

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

Support 4

Versioning..... 5

Introduction 6

Prerequisites 7

 Generating an Okta API Token..... 7

Installation..... 8

Configuration 9

ThreatQ Mapping 11

Average Feed Run..... 14

Known Issues / Limitations 15

Change Log..... 16

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 © 2021 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.

Versioning

- Current integration version 1.0.1
- Supported on ThreatQ versions $\geq$ 4.35.0

Introduction

The Okta CDF for ThreatQ enables analysts to automatically pull back a list of users (and their identity information) from Okta, into ThreatQ.

THREATQ Dashboards Threat Library Investigations Data Exchange Integrations + Create

John Doe IDENTITY Edit

Created: 09/17/2021 First Published: 09/14/2021 06:52pm Last Modified: 09/17/2021 02:58pm Touched At: 09/17/2021 03:03pm Add to Watchlist

Actions

Context

- Attributes (19)
- Sources (1)
- Tags (0)
- Description (0)
- Contact Information (0)
- Relationships
- Comments (0)
- Operations
- Audit Log

Attributes (19) Add Delete

ATTRIBUTE NAME	ATTRIBUTE VALUE	SOURCES	DATE CREATED
Last Name	Doe	Okta Users	09/17/2021 03:03pm
Display Name	John Doe	Okta Users	09/17/2021 03:02pm
Nickname	Johnny	Okta Users	09/17/2021 03:02pm
First Name	John	Okta Users	09/17/2021 03:02pm
Timezone	PST	Okta Users	09/17/2021 03:01pm
Manager	Jack Black	Okta Users	09/17/2021 03:01pm
Login	john.doe@threatq.com	Okta Users	09/17/2021 03:01pm
Email	john.doe@threatq.com	Okta Users	09/17/2021 03:01pm
Secondary Email	john.doe@gmail.com	Okta Users	09/17/2021 03:01pm
User Type	Employee	Okta Users	09/17/2021 02:08pm
Title	Solutions Architect	Okta Users	09/17/2021 02:08pm
Mobile Phone	7031231234	Okta Users	09/17/2021 02:08pm
Preferred Language	English	Okta Users	09/17/2021 02:08pm
Department	Sales	Okta Users	09/17/2021 02:08pm
City	Cupertino	Okta Users	09/17/2021 02:08pm
State	California	Okta Users	09/17/2021 02:08pm
Employee Number	1	Okta Users	09/17/2021 02:08pm
Organization	ThreatQuotient	Okta Users	09/17/2021 02:08pm
Country Code	US	Okta Users	09/17/2021 02:08pm

Rows per page 100

Prerequisites

The Okta CDF requires an Okta API Token. See the section below for steps on generating an Okta API Token.

Generating an Okta API Token

Use the following steps to generate an Okta API Token to use for this integration.

1. Log into your Okta Portal.
2. Click on **Security > API** in the left navigation.
3. Select the **Tokens** tab.
4. Click on the **Create Token** button.
5. Name the token. ThreatQuotient recommends the following name: **ThreatQ**.
6. Click on the **Create** button
7. Copy and save the token to a secure location. This token will be used when [configuring the CDF](#).

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 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.

6. If prompted, select the individual feeds to install and click **Install**. 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 to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Okta Host	Enter your Okta hostname. Do not include the http schema or any trailing slashes.
API Token	Enter your Okta API Token generated at Security > API > Tokens in your Okta portal. See the Prerequisites chapter for more details.
Ingest Users Based on Last Run Timeframe	Enable this option if you don't want the entire user list ingested every time the feed runs. You can use the manual run button to pull historically if this option is enabled.
Custom Search Query (Optional)	Optional. Enter a custom search query to apply to the API requests. See the following Okta reference for more details: https://developer.okta.com/docs/reference/api/users/#list-users-with-search .
Include User Information	Select the pieces of user information that you'd like to be brought into ThreatQ.

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

The feed automatically pulls back a list of Okta users (as Identity objects) into ThreatQ

GET `https://{okta_host}/api/v1/users`

Sample Response:

```
[
  {
    "id": "00u1t42a1zDtDDRNY5d7",
    "status": "RECOVERY",
    "created": "2021-09-14T18:52:11.000Z",
    "activated": null,
    "statusChanged": "2021-09-14T19:31:35.000Z",
    "lastLogin": "2021-09-17T13:03:41.000Z",
    "lastUpdated": "2021-09-17T13:44:52.000Z",
    "passwordChanged": "2021-09-14T19:31:37.000Z",
    "type": {
      "id": "oty1t42agnkjSIFX55d7"
    },
    "profile": {
      "lastName": "Doe",
      "zipCode": "22066",
      "preferredLanguage": "English",
      "city": "Cupertino",
      "displayName": "John Doe",
      "timezone": "EST",
      "title": "Solutions Architect",
      "locale": "",
      "login": "john.doe@threatq.com",
      "employeeNumber": "1",
      "division": "Sales Engineering",
      "countryCode": "US",
      "state": "California",
      "department": "Sales",
      "email": "john.doe@threatq.com",
      "manager": "Jack Black",
      "nickName": "John",
      "secondEmail": "john.doe@gmail.com",
      "firstName": "John",
      "primaryPhone": "7031231234",
      "postalAddress": "22066",
      "mobilePhone": "7031231234",
      "streetAddress": "1 Cupertino Road",
      "organization": "ThreatQuotient",
      "middleName": "L",
      "userType": "Employee"
    },
    "credentials": {
      "password": {},
      "emails": [
        {
          "value": "john.doe@threatq.com",
```

```
[{"status": "VERIFIED",
  "type": "PRIMARY",
},
{
  "value": "john.doe@gmail.com",
  "status": "VERIFIED",
  "type": "SECONDARY"
}
],
"provider": {
  "type": "OKTA",
  "name": "OKTA"
}
},
"_links": {
  "self": {
    "href": "https://dev-15613756.okta.com/api/v1/users/00u1t42a1zDtDDrNY5d7"
  }
}
}
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	NORMALIZATION	PUBLISHED DATE	EXAMPLES	NOTES
data.profile.[firstName/lastName]	Object Value	Identity	First and last name concatenated	data.created	N/A	N/A
data.profile.firstName	Attribute	First Name	N/A	data.created	N/A	Conditionally set, if enabled
data.profile.lastName	Attribute	Last Name	N/A	data.created	N/A	Conditionally set, if enabled
data.profile.zipCode	Attribute	Zip Code	N/A	data.created	N/A	Conditionally set, if enabled
data.profile.preferredLanguage	Attribute	Preferred Language	N/A	data.created	N/A	Conditionally set, if enabled
data.profile.city	Attribute	City	N/A	data.created	N/A	Conditionally set, if enabled
data.profile.displayName	Attribute	Display Name	N/A	data.created	N/A	Conditionally set, if enabled
data.profile.timezone	Attribute	Timezone	N/A	data.created	N/A	Conditionally set, if enabled
data.profile.title	Attribute	Title	N/A	data.created	N/A	Conditionally set, if enabled
data.profile.locale	Attribute	Locale	N/A	data.created	N/A	Conditionally set, if enabled
data.profile.login	Attribute	Login	N/A	data.created	N/A	Conditionally set, if enabled
data.profile.employeeNumber	Attribute	Employee Number	N/A	data.created	N/A	Conditionally set, if enabled
data.profile.division	Attribute	Division	N/A	data.created	N/A	Conditionally set, if enabled

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	NORMALIZATION	PUBLISHED DATE	EXAMPLES	NOTES
data.profile.countryCode	Attribute	Country Code	N/A	data.created	N/A	Conditionally set, if enabled
data.profile.state	Attribute	State	N/A	data.created	N/A	Conditionally set, if enabled
data.profile.department	Attribute	Department	N/A	data.created	N/A	Conditionally set, if enabled
data.profile.email	Attribute	Email	N/A	data.created	N/A	Conditionally set, if enabled
data.profile.manager	Attribute	Manager	N/A	data.created	N/A	Conditionally set, if enabled
data.profile.nickName	Attribute	Nickname	N/A	data.created	N/A	Conditionally set, if enabled
data.profile.secondaryEmail	Attribute	Secondary Email	N/A	data.created	N/A	Conditionally set, if enabled
data.profile.primaryPhone	Attribute	Primary Phone	N/A	data.created	N/A	Conditionally set, if enabled
data.profile.postalAddress	Attribute	Postal Address	N/A	data.created	N/A	Conditionally set, if enabled
data.profile.mobilePhone	Attribute	Mobile Phone	N/A	data.created	N/A	Conditionally set, if enabled
data.profile.streetAddress	Attribute	Street Address	N/A	data.created	N/A	Conditionally set, if enabled
data.profile.organization	Attribute	Organization	N/A	data.created	N/A	Conditionally set, if enabled
data.profile.middleName	Attribute	Middle Name	N/A	data.created	N/A	Conditionally set, if enabled
data.profile.userType	Attribute	User Type	N/A	data.created	N/A	Conditionally set, if enabled

Average Feed Run

METRIC	RESULT
Run Time	1 minute
Identities	2
Identity Attributes	23



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.

Known Issues / Limitations

- If the `Ingest Users Based on Last Run Timeframe` is enabled, users will only be pulled back when they have been last updated within the feed run timeframe. Disable this option to always pull back the full list of users, or keep it enabled and utilize the manual `Run Integration` button to pull a list of users, historically.

Change Log

- Version 1.0.1
 - CDF optimization by ThreatQuotient Engineering.
 - Updated Support tier from **Not Supported** to **ThreatQ Supported**.
- Version 1.0.0
 - Initial Release