ThreatQuotient

Okta CDF Guide

Version 1.0.0

September 20, 2021

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

Not Supported

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 **Not Supported**.

Integrations, apps, and add-ons designated as **Not Supported** are not supported by ThreatQuotient's Customer Support team.

While you can report issues to ThreatQ's Customer Support team regarding the integration/app/add-on, you are solely responsible for ensuring proper functionality and version compatibility of Not Supported designations with the applicable ThreatQuotient software.

If unresolvable functional or compatibility issues are encountered, you may be required to uninstall the integration/app/add-on from your ThreatQuotient environment in order for ThreatQuotient to fulfill support obligations.

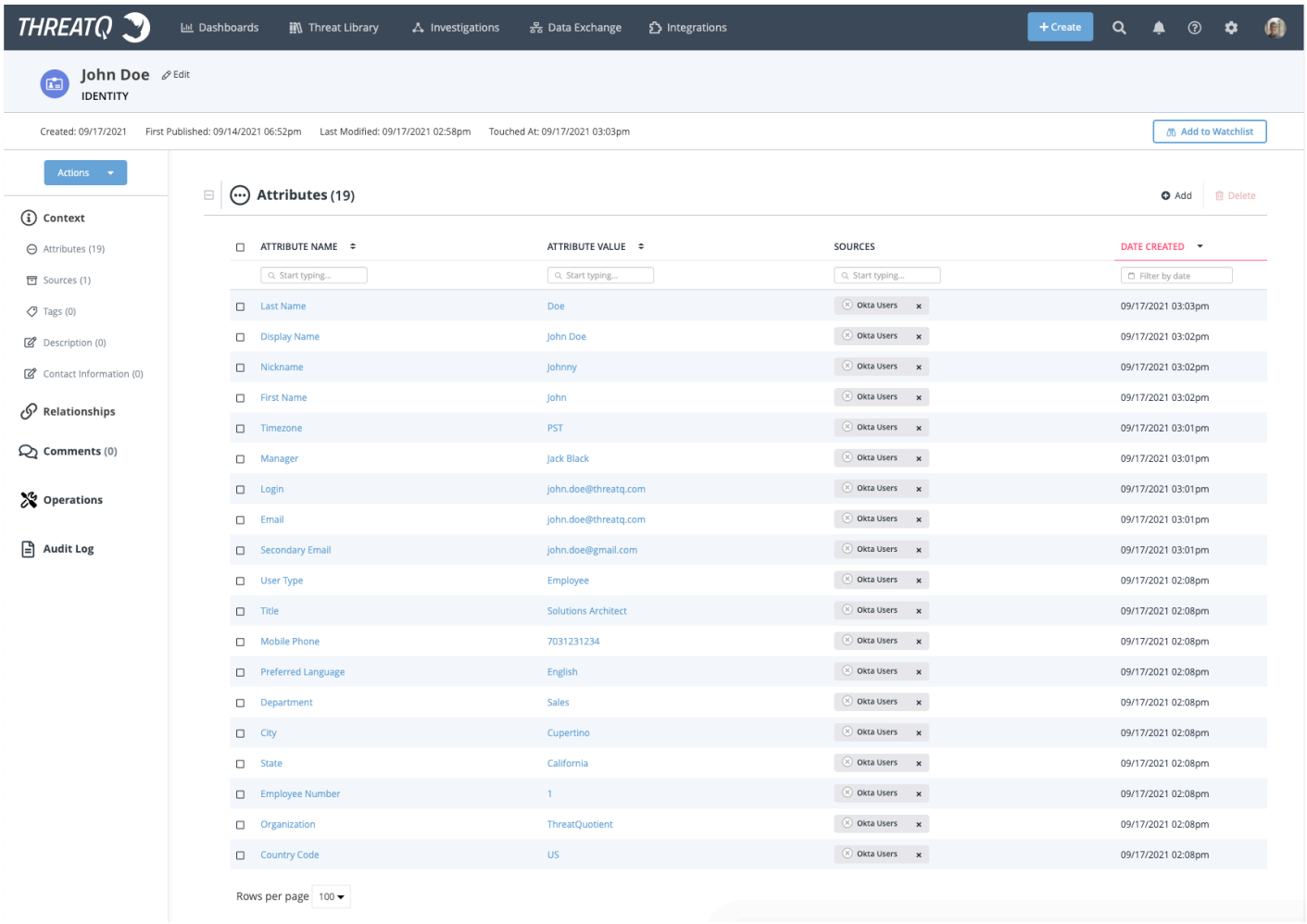
> ⚠ For ThreatQuotient Hosted instance customers, the Service Level Commitment and Service Level Credit in the ThreatQuotient Service Level Schedule will not apply to issues caused by Not Supported integrations/apps/add-ons.

Versioning

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



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 is 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": "00u1t42alzDtDDRNY5d7",
        "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/00u1t42alzDtDDRNY5d7"
            }
        }
    }
]
```


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.secondEmail`	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 1.0.0**
  - Initial Release