



# SNYPR 6.2

OKTA

## Securonix Proprietary Statement

This material constitutes proprietary and trade secret information of Securonix, and shall not be disclosed to any third party, nor used by the recipient except under the terms and conditions prescribed by Securonix.

The trademarks, service marks, and logos of Securonix and others used herein are the property of Securonix or their respective owners.

## Securonix Copyright Statement

This material is also protected by Federal Copyright Law and is not to be copied or reproduced in any form, using any medium, without the prior written authorization of Securonix.

However, Securonix allows the printing of the Adobe Acrobat PDF files for the purposes of client training and reference.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those agreements. Nothing herein should be construed as constituting an additional warranty. Securonix shall not be liable for technical or editorial errors or omissions contained herein. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's internal use without the written permission of Securonix.

Copyright 2018 © Securonix All rights reserved.

## Contact Information

Securonix, Inc.  
14665 Midway Rd. Ste. 100, Addison, TX 75001  
www.securonix.com  
855.732.6649

## Revision History

Date	Product Version	Description
3/13/2018	6.1	First Release
5/21/2018	6.2	Revision

# Table of Contents

---

- 2
- Okta Authentication** ..... 4
- Integration Benefits ..... 4
- Okta Integration ..... 5
  - 1. Create a Token ..... 5
  - 2. Configure the Okta Connector in SNYPR ..... 8
- Supported Collection Methods ..... 11
- Functionality ..... 11
- Taxonomy ..... 11
- Device Event Field Mapping ..... 12
  - Okta Authentication Mappings to SNYPR Fields ..... 12
- Common Events in Okta ..... 12
  - Event Categorization in SNYPR ..... 13
- Available Policies ..... 14
- References ..... 15

# Okta Authentication

Okta Authentication provides operation to authenticate users, perform multi-factor enrollment and verification, recover forgotten passwords, and unlock accounts. It can be used as a standalone API to provide the identity layer on top of your existing application, or it can be integrated with the Okta Sessions API to obtain an Okta session cookie and access apps within Okta.

This data source guide will provide information on how to integrate Okta Authentication and how the data source events are parsed, normalized, and categorized to SNYPR fields. In particular, it provides the following:

- Device event field mapping
- Device event severity mapping
- Device event categorization

To download the Okta Authentication parser from the Securonix Threat Library, search Available Resources Types for Deployment by Vendor name or Functionality. Downloading the resource downloads the parser along with the applicable dashboards, reports, policies and threat models.

## Integration Benefits

Integrating Okta Authentication offers key benefits that help to improve existing infrastructure:

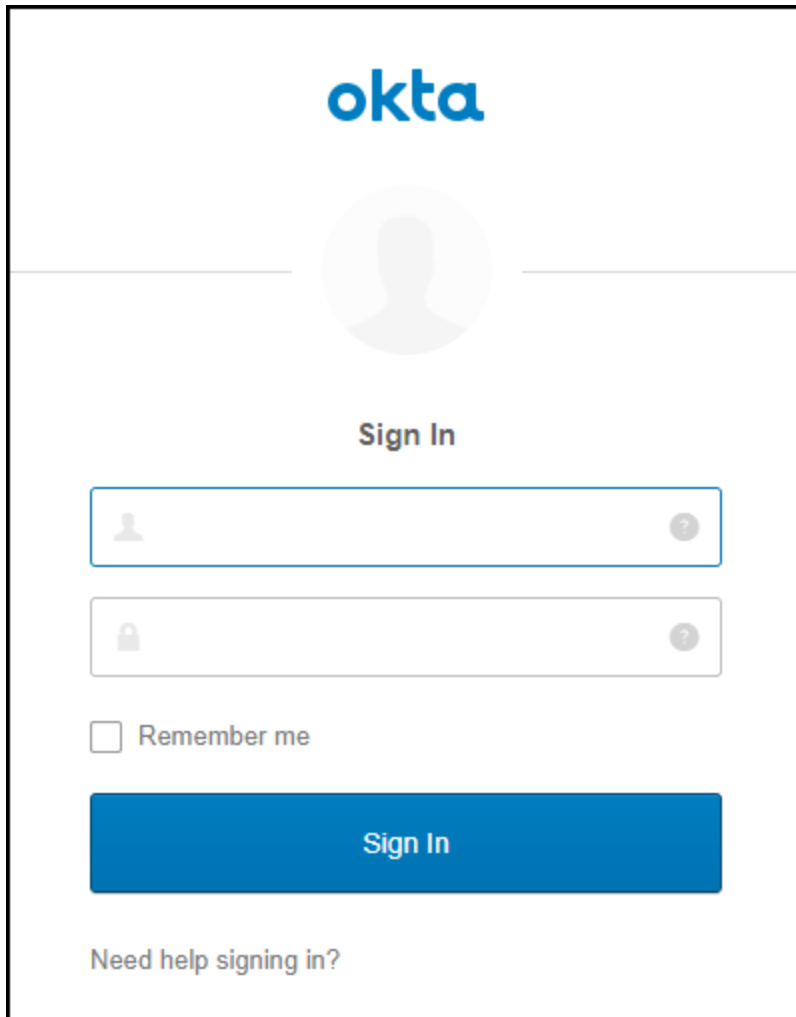
- Detect authentication attempts and password attacks
- Gain insight into user activity across your environment
- Reduce the risk of insider threats and data breach
- Identify suspicious users and compromised accounts
- Take immediate action against user accounts

# Okta Integration

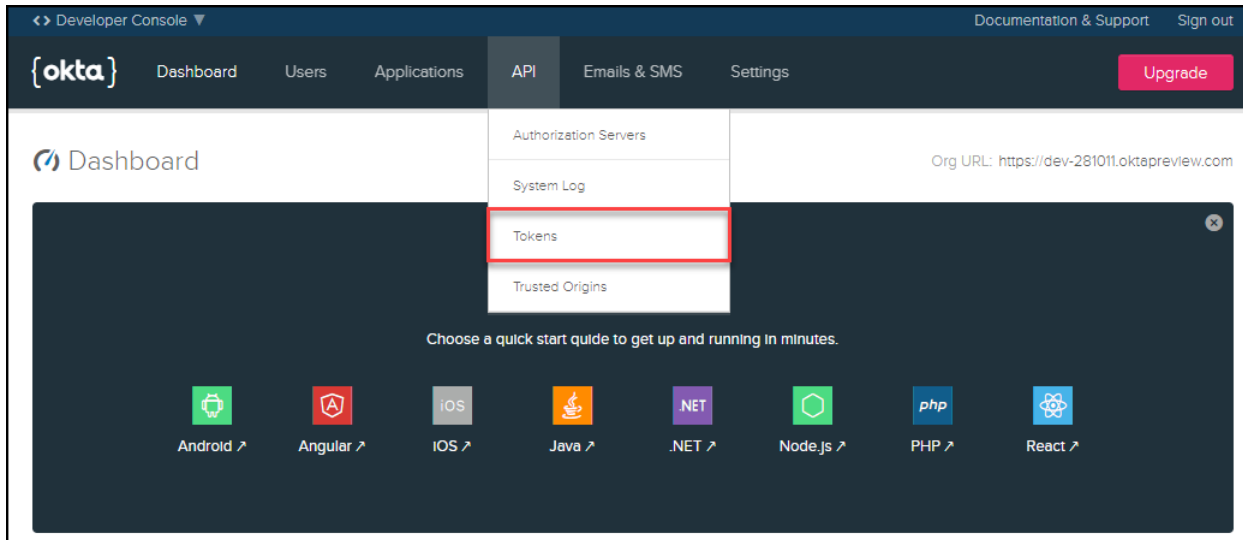
Follow the steps below to integrate Okta into SNYPR.

## 1. Create a Token

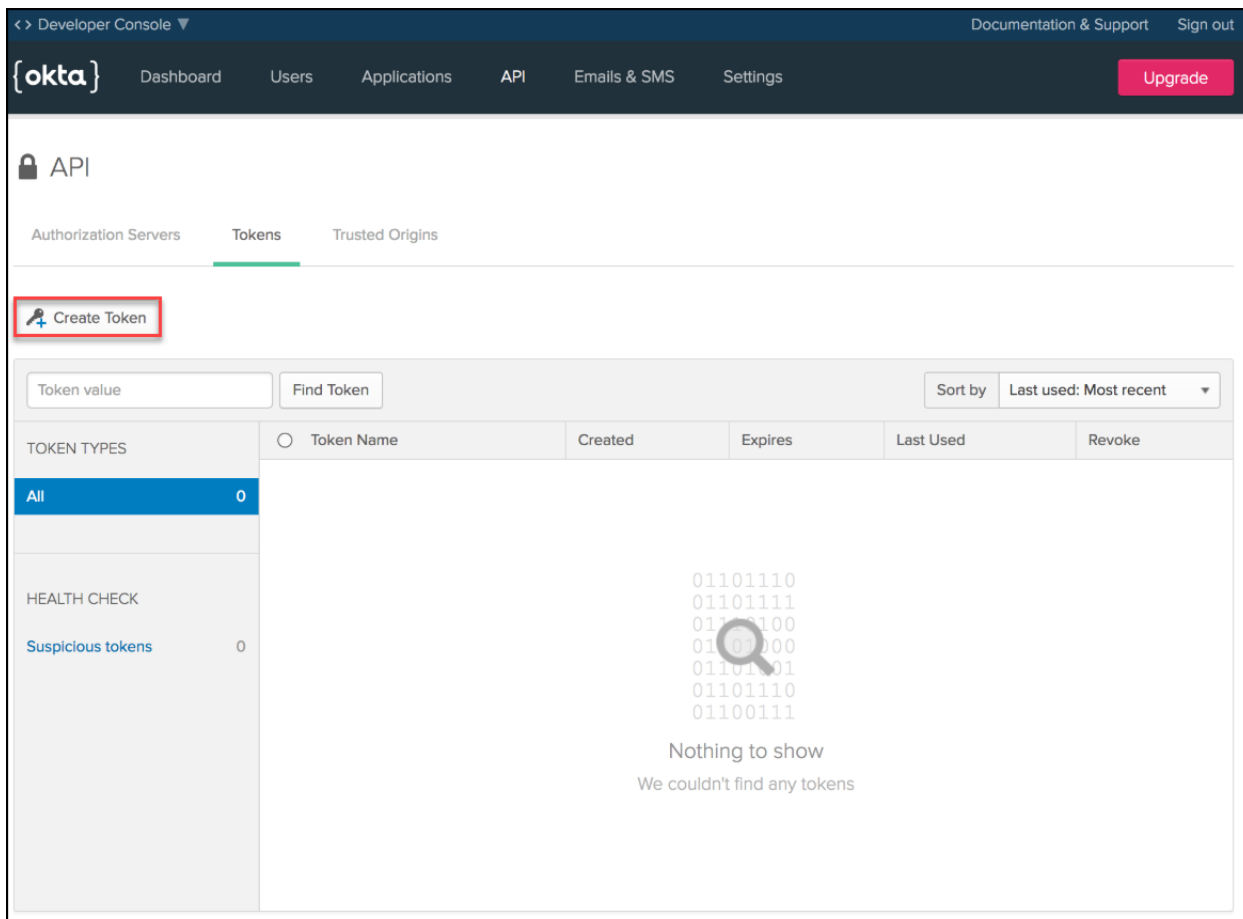
Navigate to <https://login.okta.com> and sign in with your credentials.

A screenshot of the Okta Sign In page. At the top center is the 'okta' logo in blue. Below the logo is a circular placeholder for a user profile picture. Underneath the placeholder is the text 'Sign In'. There are two input fields: the first is for the username, containing a person icon and a question mark icon; the second is for the password, containing a lock icon and a question mark icon. Below the password field is a checkbox labeled 'Remember me'. At the bottom of the form is a large blue button with the text 'Sign In'. Below the button is the text 'Need help signing in?'.

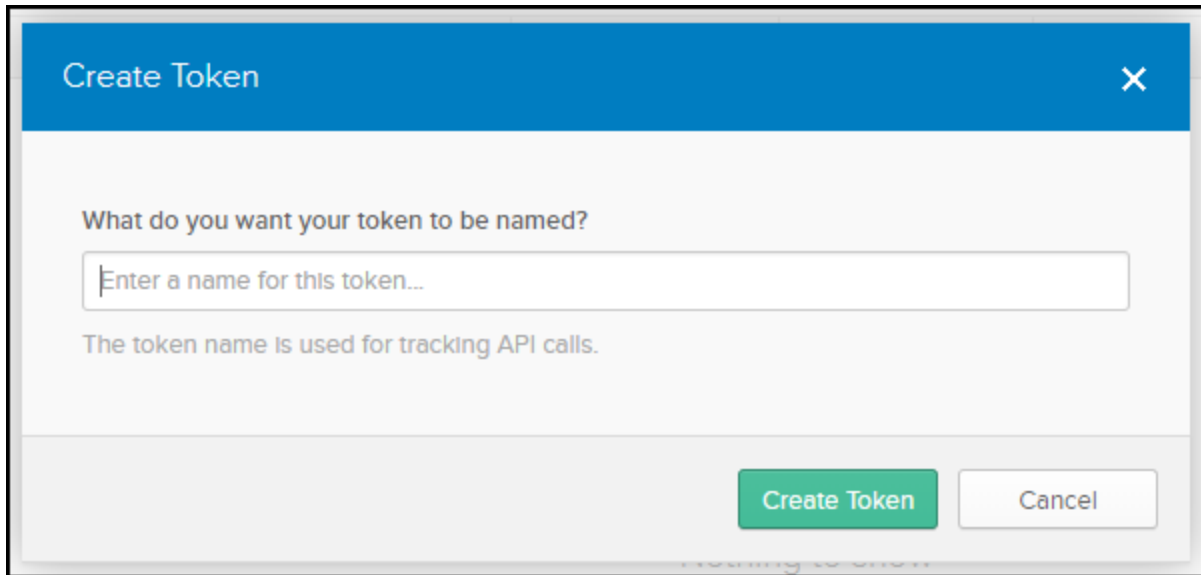
Click **API > Tokens** from the navigation menu.




Click **Create Token**.



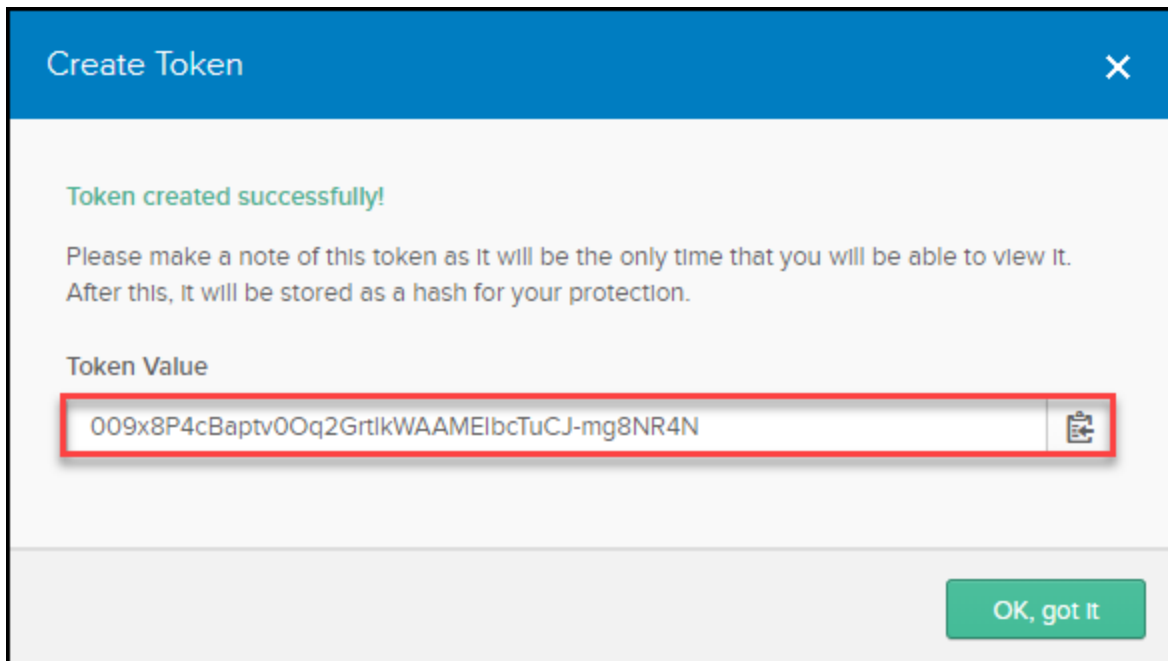
Enter a name for your token, then click **Create Token**.




The image shows a 'Create Token' dialog box with a blue header and a close button (X) in the top right. The main content area is white and contains the question 'What do you want your token to be named?'. Below this is a text input field with the placeholder text 'Enter a name for this token...'. Underneath the input field is a note: 'The token name is used for tracking API calls.' At the bottom right of the dialog are two buttons: a green 'Create Token' button and a white 'Cancel' button with a grey border.

 **Note:** The token name above will be used within SNYPR when you set up the Okta connector.

Make a note of the **Token Value** then click **OK, got it**.

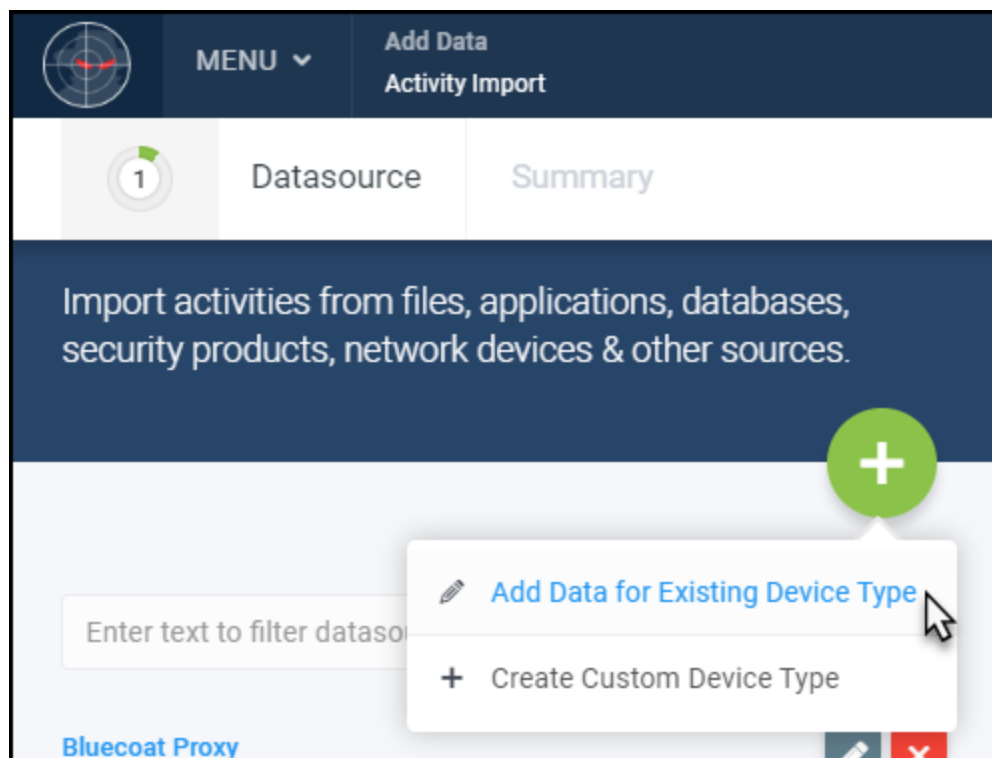


The image shows the 'Create Token' dialog box after successful creation. The header and close button remain. The main content area now displays a green message: 'Token created successfully!'. Below this is a warning: 'Please make a note of this token as it will be the only time that you will be able to view it. After this, it will be stored as a hash for your protection.' Underneath is the label 'Token Value' followed by a text field containing the token value '009x8P4cBaptv0Oq2GrtkWAAMEIbcTuCJ-mg8NR4N'. The text field has a red border and a copy icon on the right. At the bottom right is a green 'OK, got it' button.

 **Note:** This is the only time that you will be able to view your **Token Value**. Once you click **OK, got it**, the **Token Value** will be stored as a hash for your protection.

## 2. Configure the Okta Connector in SNYPR

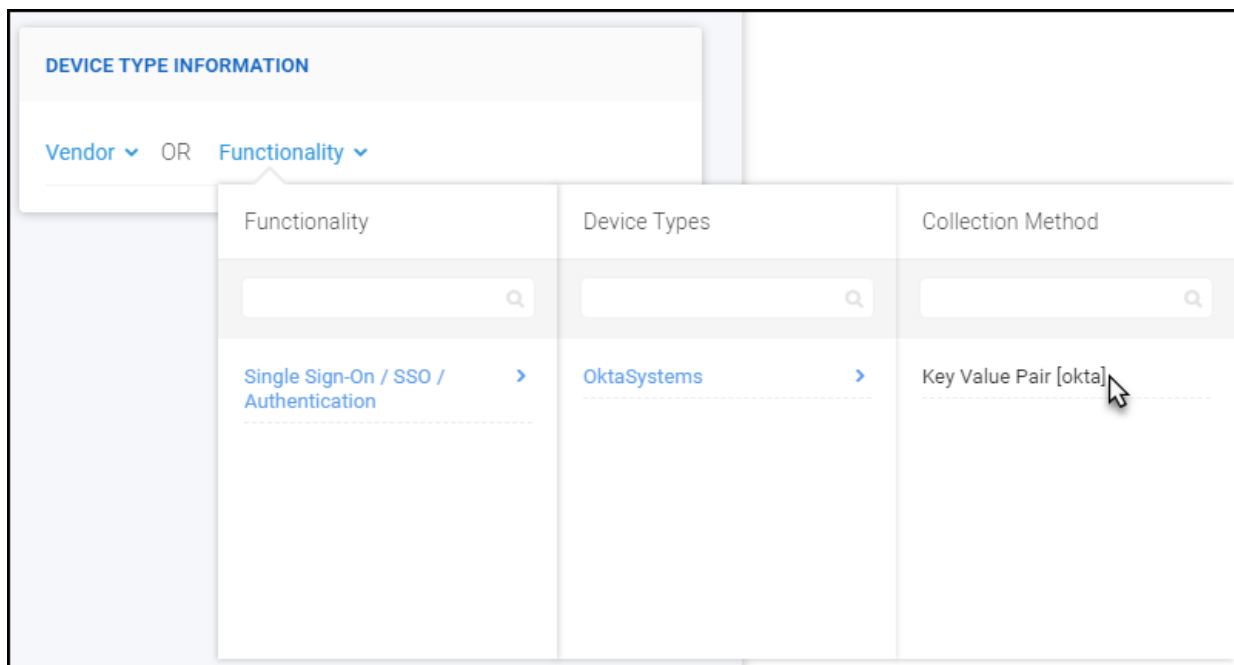
Navigate to **Menu > Add Data > Activity** then click **+ > Add Data for Existing Device Type**.



Click **Functionality** and select the following values in the dialog box:

- **Functionality:** Single Sign-On / SSO / Authentication
- **Device Types:** OktaSystems
- **Collection Method:** Key Value Pair [okta]





Enter a **Datasource Name** in the **Device Information** section.

The screenshot shows a form titled "DEVICE INFORMATION". The "Datasource Name" field is highlighted with a red border and contains the text "OktaSystems". Below it is the "IP Address Or Host Name" field, which is empty. At the bottom is the "Specify timezone for activity logs" field, which is a dropdown menu currently set to "EDT".

Enter the **URL** and **Token** value within the **Connection Properties** section.

### COLLECTION METHOD

**URL**

**Token**

**Import Events From**

**Batch Size**

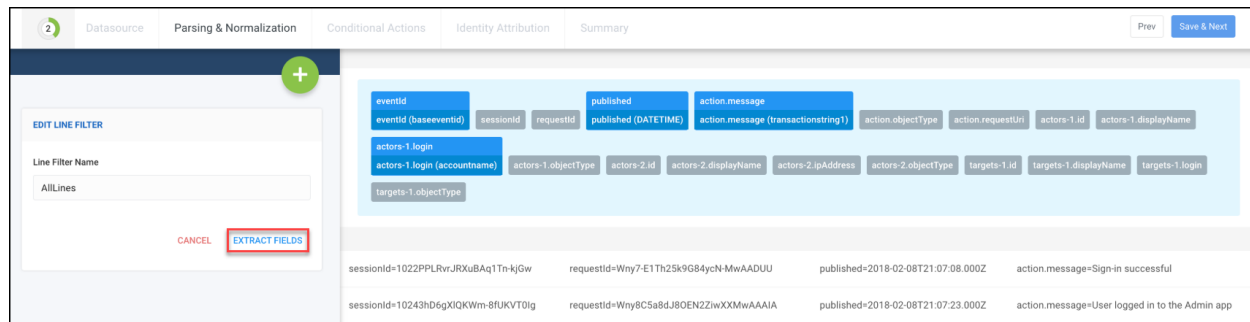
**Polling Interval (In Seconds)**

**Filters to pull data from Okta**

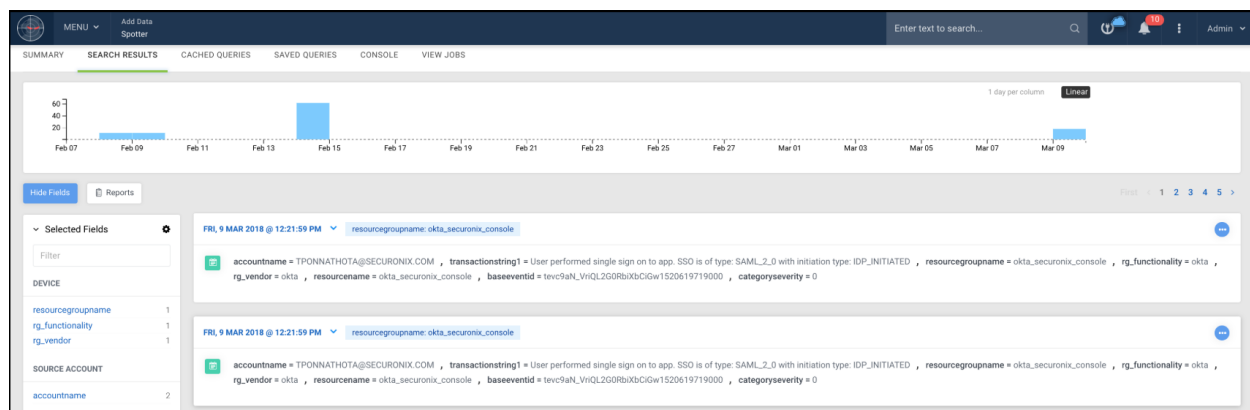
**Parsing Technique**

Key Value Pair

Click **Save & Next**, then click **EXTRACT FIELDS** to parse the fields and map them to corresponding SNYPR attributes.



You can now find events from this datasource in spotter using the syntax `resourcegroupname=<datasource name>`. Example: `resourcegroupname=okta_securonix_console`.



## Supported Collection Methods

The method of collection is API.

## Functionality

The functionality of Okta Authentication is **Single Sign-On / SSO / Authentication**. See Use Cases by Functionality for a complete list of policies for this functionality.

## Taxonomy

Securonix Open Event Format (OEF) 1.0 is used. OEF is an event interoperability standard/schema. It provides a set of standardized attributes (fields) for consistent representation of logging output from disparate security and non-security devices and applications. For additional information, refer to the [Data Dictionary](#) section on the Securonix documentation portal.

## Device Event Field Mapping

This section lists the mappings of SNYPR fields to the device fields.

### Okta Authentication Mappings to SNYPR Fields

Okta Authentication Field	SNYPR Field
eventId	baseeventid
sessionId	sessionid
published	DATETIME
action.message	message
action.objectType	resourcetype
action.requestUri	requesturl
actors-1.id	customstring1
actors-1.displayName	accountowner
actors-1.ipAddress	sourceaddress
actors-1.objectType	sourceuserprivileges
actors-1.login	sourceusername
actors-2.id	requestclientapplication
targets-1.displayName	destinationusername
targets-1.objectType	destinationuserprivileges
requestId	AlertId
targets-1.login	destinationuserid
targets-2.displayName	additionaldetails1
targets-2.objectType	additionaldetails2
actors-2.ipAddress	translatedipaddress

## Common Events in Okta

This section provides common successful events, common failure events, and other notable events that appear in Okta's corpus of data.

## Successful Events

Use the list below to gain a better understanding of the expected messages for successful events:

- Add user to application membership
- User single sign on to app
- Remove users application membership
- User login to Okta
- Push users profile to external application
- Successfully imported new member to an app group
- Sync user in external application
- Updated user application property

## Failure Events

Use the list below to gain a better understanding of the expected messages for failure events:

- User login to Okta
- Perform RealTimeSync by AD agent
- Authenticate user with AD agent
- Authentication of user via Radius
- User reset password for Okta (by Admin)
- User attempted unauthorized access to app
- Connect AD agent to Okta
- Authentication of user via MFA

## Other Notable Events

Events for failed multifactor verification and failed authentication attempts are potential indicators of abuse. Additional context provided in the log will allow for pivoting this information based on things like Target User, Client IP address, User-Agent and more.

## Event Categorization in SNYPR

SNYPR categorizes each event it ingests in order to normalize syntax across multiple functionalities, vendors, and datasources. This section contains the rules used to categorize the events.

Rule	Category Object	Category Behavior	Category Outcome
UserAuthenticationSuccess	User	Authentication	Success
UserAuthenticationFailure	User	Authentication	Failure
AccountAccessAttempt	Account	Access	Attempt

## Available Policies

The following policies are available for Okta:

Name	Description
Abnormally high number of failed logon attempts detected from Network Address	Abnormal high number of failed logon attempts detected from Network Address is an indicative of possible account takeover activity performed from an IP Address. Technique used: Behavior Anomaly for failed login activity
Possible Attempted account enumeration based compromise	Possible Attempted account enumeration based compromise is an indicative of possible account enumeration activity or possible account compromise activity performed from an IP Address. Technique used: Behavior Anomaly for login activity
Activity by Terminated User	Activity by Terminated User is an indicative of possible account misuse activity or possible account compromise activity performed from an account. Technique used: Identity based activity detection
User authenticating from rare geo-location	Account authentication from a rare geolocation may be indicative of a possible account sharing or an account takeover attempt. Technique Used: Behavior anomaly for geolocation associated with an entity
Landspeed Anamolies	Landspeed violation may be indicative of a possible account sharing or an account takeover attempt. Technique Used: Landspeed anomaly detection
Multiple users attempting authentication from IP	Repeated authentication events may be indicative of a malicious entity attempting to communicate to a Command and Control server or to receiving the malicious payload. Technique Used: Aggregated event analysis on multiple authentication events
Spike in account lockouts	Description: Spike in account lockout events could be indicative of a possible bruteforce event. Technique: Behavior anomaly on the account lockout activity for an account
Spike in authentication failures	Abnormal number of logon failures could be indicative of a possible account takeover attempt. Logon failure reason could further indicate the severity of this attack. Technique: Behavior anomaly on the logon failure activity for an account
Spike in password resets	A spike in password reset attempts may be indicative of a possible account takeover attempt. Technique: Behavior anomaly on the password reset activity
Abnormal number of application access attempts	Abnormal number of application access attempts is an indicative of possible application enumeration activity performed from a compromised accounts. Technique used: Behavior Anomaly for login activity

User added and removed	These temporary privilege escalation events may be indicative of a possible backdoor access attempt to use elevated privileges. Technique: Entity attribution
User authenticating from rare useragent	Account authentication from a rare useragent may be indicative of a possible malware. Technique Used: Behavior anomaly for useragent associated with an entity
High number of password reset attempts from an IP	This could indicate a possible account takeover attempt. Unauthorized password changes on multiple accounts could also indicate denial of service.

## References

**Authentication API:** <https://developer.okta.com/docs/api/resources/authn.html>

**Event Information:** [https://developer.okta.com/use\\_cases/isv/isv-syslog-references#event-api-to-system-log-api](https://developer.okta.com/use_cases/isv/isv-syslog-references#event-api-to-system-log-api)

