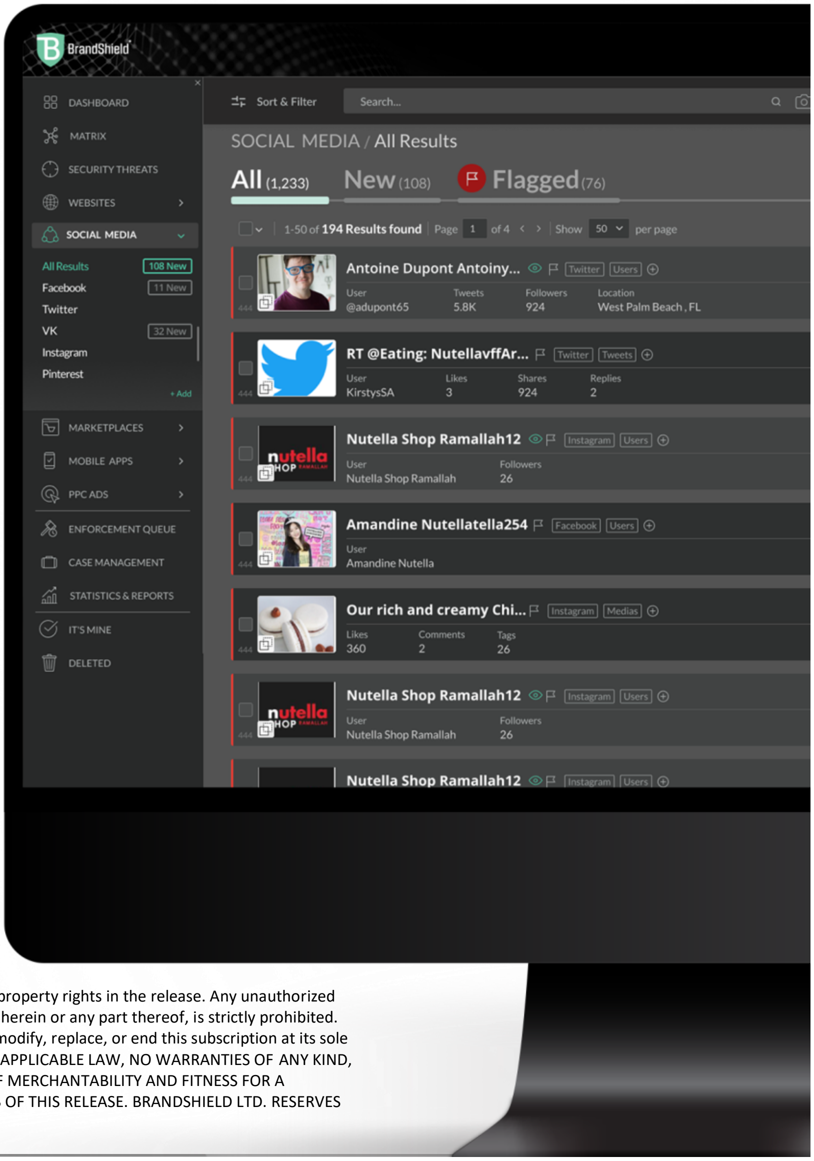
BrandShield 3.0

Okta Single-Sign-On (SSO) - Integration Guide

Published: Mar 1st 2023



BrandShield
DASHBOARD
MATRIX
SECURITY THREATS
WEBSITES
SOCIAL MEDIA
All Results 108 New
Facebook 11 New
Twitter
VK 32 New
Instagram
Pinterest
+ Add
MARKETPLACES
MOBILE APPS
PPC ADS
ENFORCEMENT QUEUE
CASE MANAGEMENT
STATISTICS & REPORTS
IT'S MINE
DELETED
Sort & Filter
Search...
SOCIAL MEDIA / All Results
All (1,233)
New (108)
Flagged (76)
1-50 of 194 Results found
Page 1 of 4
Show 50 per page
Antoine Dupont Antoiny... Twitter Users
User @adupont65 Tweets 5.8K Followers 924 Location West Palm Beach, FL
RT @Eating: NutellavffAr... Twitter Tweets
User KirstysSA Likes 3 Shares 924 Replies 2
Nutella Shop Ramallah12 Instagram Users
User Nutella Shop Ramallah Followers 26
Amandine Nutellatella254 Facebook Users
User Amandine Nutella
Our rich and creamy Chi... Instagram Medias
Likes 360 Comments 2 Tags 26
Nutella Shop Ramallah12 Instagram Users
User Nutella Shop Ramallah Followers 26
Nutella Shop Ramallah12 Instagram Users

Introduction

BrandShield

BrandShield Systems PLC (AIM: BRSD) has developed a brand-oriented digital risk protection cloud-based software that revolutionizes the way organizations protect themselves againstonline sams, phishing, impersonation, trademark infringement, counterfeit sales, and other forms of brand abuse. BrandShield’s robust, patented technology detects online scmas, phishing sites, social media impersonation, trademark infringement and brand abuse across multiple platforms, by utilizing artificial intelligence, big data and machine learning technologies to automatically analyze and prioritize online risks, based on various web metrics.

Okta

Okta, Inc. (NASDAQ: OKTA), is the leading independent identity provider that provides a platform for identity and access management (IAM). It offers a range of products that can help an organization manage and secure its digital identities, as well as control access to various applications and resources. Okta's platform includes features such as single sign-on (SSO), multi-factor authentication (MFA), and user provisioning, among others. Okta's products are designed to be flexible and scalable, and can be used by organizations of all sizes, across a variety of industries.

SSO (Single-Sign-On)

Single sign-on (SSO) is a system that allows users to use a single set of login credentials (e.g., username and password) to access multiple applications or resources. The goal of SSO is to reduce the number of times a user has to enter their login information, which can save time and reduce the risk of errors. SSO systems typically use a central authentication server, which is responsible for verifying the user's credentials and granting access to the requested resources. SSO can be used to access both on-premises and cloud-based applications, and can be integrated with a variety of authentication methods, such as passwords, security tokens, and biometric authentication.

OpenID Connect

OpenID Connect (OIDC) is an authentication protocol that is built on top of the OAuth 2.0 framework. It allows users to authenticate with an external identity provider (such as Google, Microsoft, or Salesforce) and then use the resulting authentication token to access protected resources. OIDC provides a secure way for an application to obtain information about the user's identity, without the need to handle the user's credentials directly. OIDC uses JSON Web Tokens (JWTs) to represent the user's identity and other information. The application can use the information contained in the JWT to personalize the user's experience or to enforce access controls.

Index

Supported Features

BrandShield App Integration Supported Features

The BrandShield App integration supports the following features:

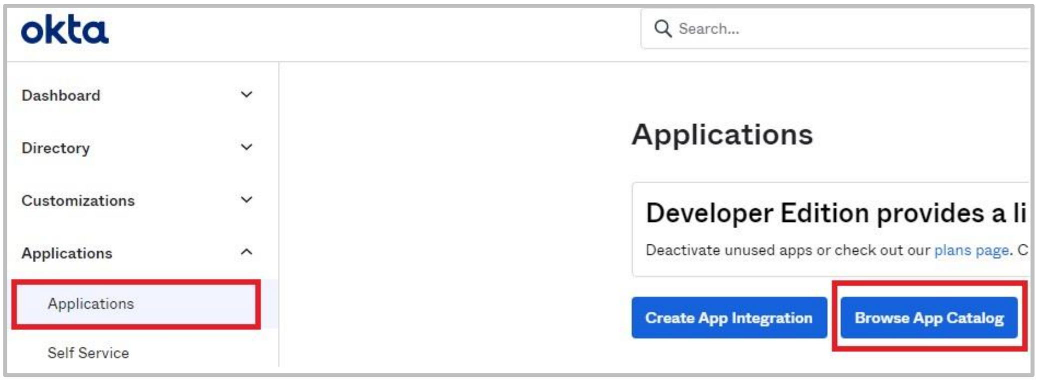
- Service Provider (SP) - Initiated Authentication (SSO) Flow - This authentication flow occurs when the user attempts to log in to the application from BrandShield.

Integrating Okta

Adding BrandShield App Integration from the Catalog

To add BrandShield SSO App integration from Okta App Integration Catalog: first enter your organization Okta Admin Console and the Application section:

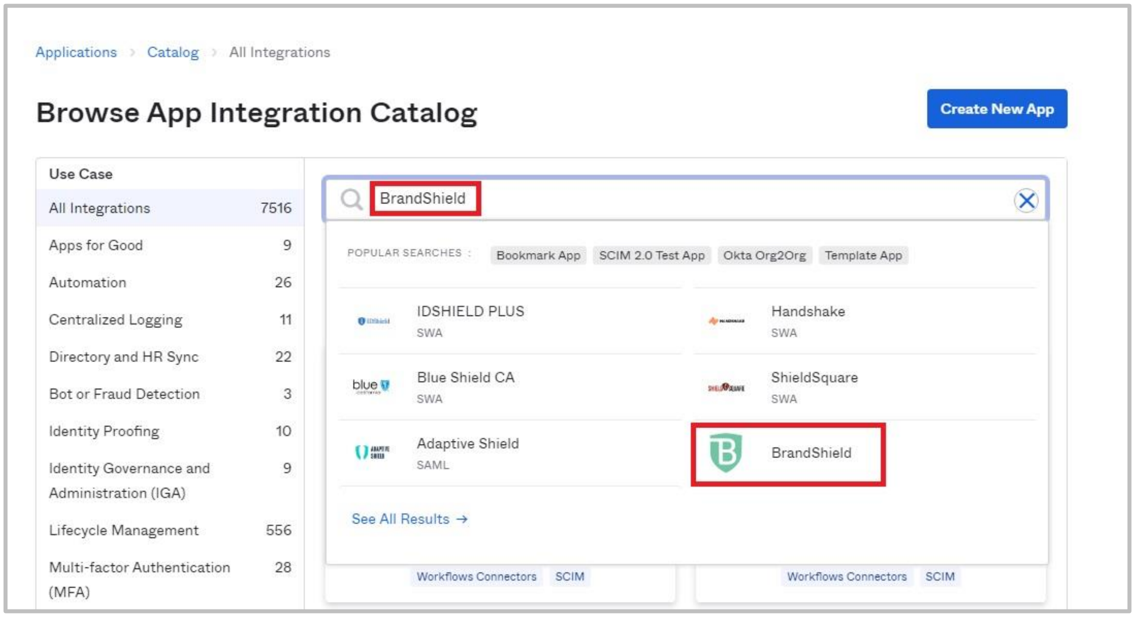
1. Enter your organization Okta Admin Console on https://www.okta.com
2. In the Admin Console, go to Applications > Applications
3. Click Browse App Catalog.



Developer Edition provides a li

Deactivate unused apps or check out our plans page. C

4. On the Browse App Integration Catalog page, search for BrandShield in the search box and select the BrandShield app in the presented applications dropdown.



Applications › Catalog › All Integrations

Browse App Integration Catalog

Create New App

Use Case	
All Integrations	7516
Apps for Good	9
Automation	26
Centralized Logging	11
Directory and HR Sync	22
Bot or Fraud Detection	3
Identity Proofing	10
Identity Governance and Administration (IGA)	9
Lifecycle Management	556
Multi-factor Authentication (MFA)	28

BrandShield

POPULAR SEARCHES : Bookmark App SCIM 2.0 Test App Okta Org2Org Template App

IDSHIELD PLUS
SWA

Handshake
SWA

Blue Shield CA
SWA

ShieldSquare
SWA

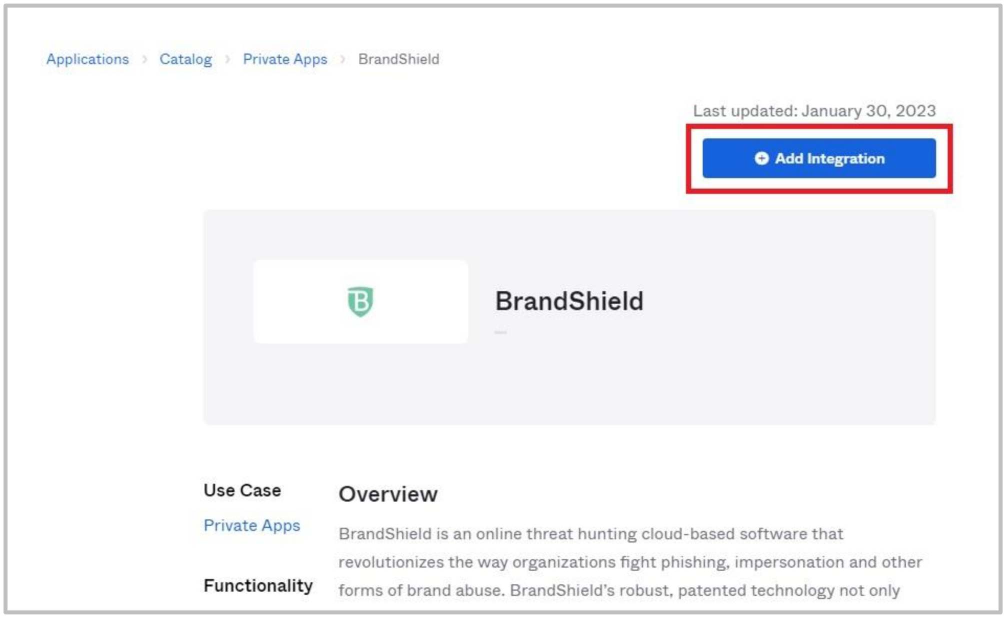
Adaptive Shield
SAML

BrandShield

See All Results →

Workflows Connectors SCIM Workflows Connectors SCIM

5. Click the 'Add Integration' button in order to add the application integration.



Applications › Catalog › Private Apps › BrandShield

Last updated: January 30, 2023

Add Integration

BrandShield

Use Case

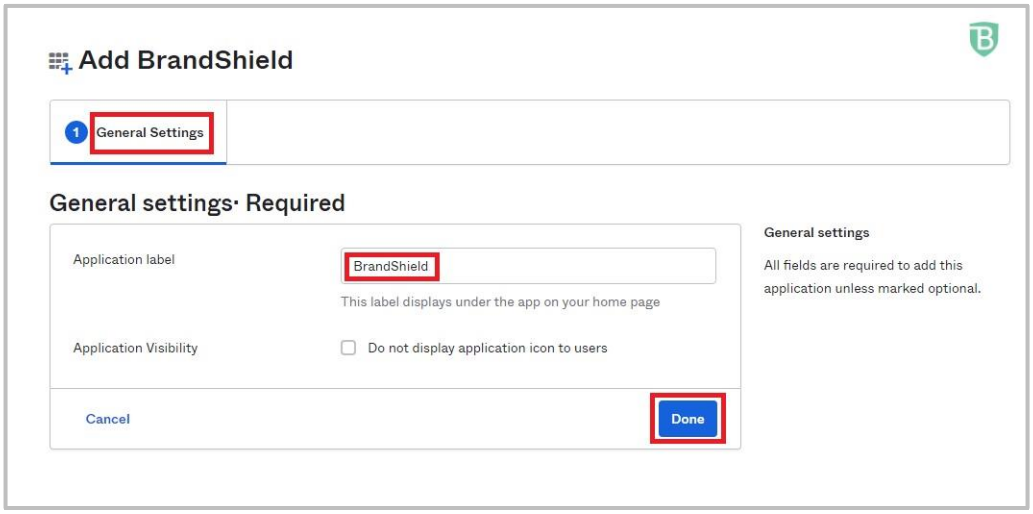
Private Apps

Functionality

Overview

BrandShield is an online threat hunting cloud-based software that revolutionizes the way organizations fight phishing, impersonation and other forms of brand abuse. BrandShield's robust, patented technology not only

6. In the 'Add BrandShield' page, under the 'General Settings' tab, enter a name for the new integration (preferably BrandShield) and click the 'Done' button.



Add BrandShield

1 General Settings

General settings· Required

Application label: BrandShield

This label displays under the app on your home page

Application Visibility: □ Do not display application icon to users

General settings

All fields are required to add this application unless marked optional.

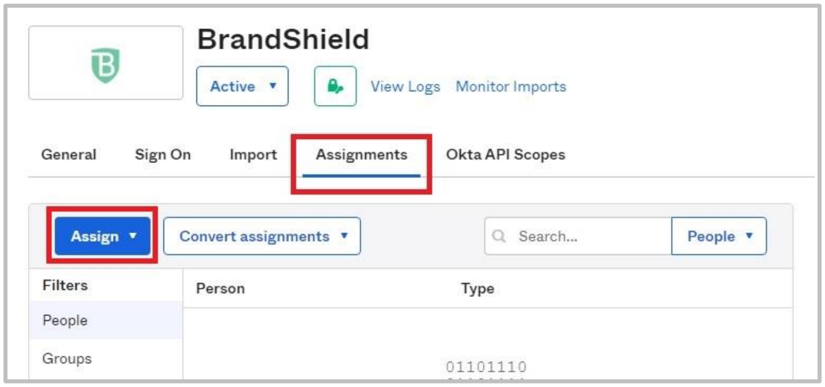
7. After the BrandShield integration app is installed, you'll be redirected to the app 'Assignments' tab where you should assign the relevant people or groups that are allowed to use the app integration. For more information about how to assign the relevant users, please read the 'Assigning Users' below.

8. Your new Okta app integration for BrandShield is ready.

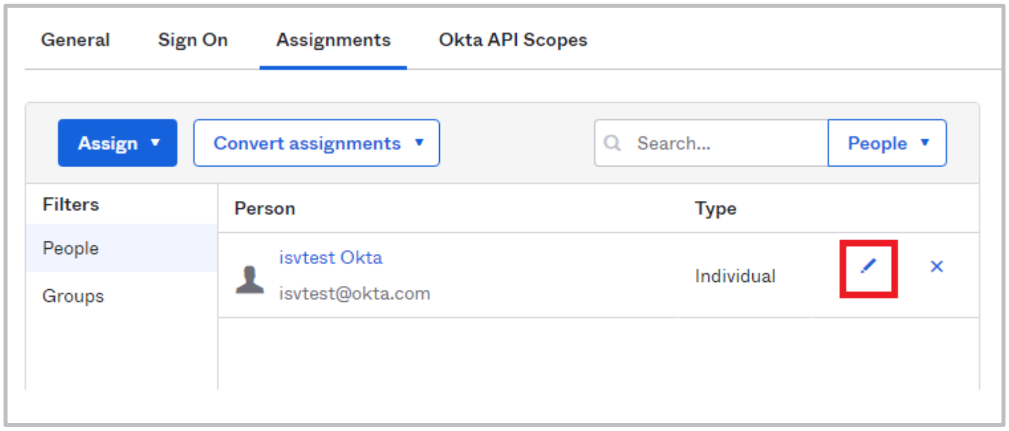
Assigning Users

To assign the Okta SSO integration application for BrandShield to users in your organization:

1. Enter the BrandShield integration application and Click the Assignments tab.



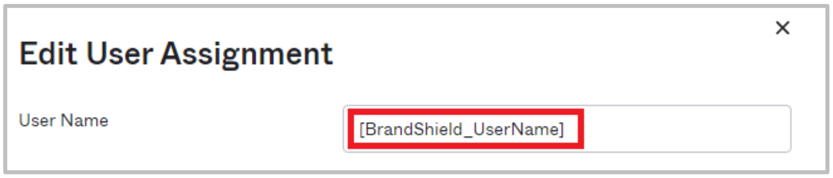
2. Click Assign and then select either Assign to People or Assign to Groups.
3. Enter the appropriate people or groups that you want to have Single Sign-On into your application, and then click Assign for each.
4. For any people that you add, verify the user-specific attributes, and then select Save and Go Back.
5. Important note: While Okta requires its usernames to be email, BrandShield allow its username to be created in different formats. Therefore, in order to correlate Okta user with the relevant BrandShield user, you should set the preferred username to be the one configured on BrandShield. To do so:
    a. In the Assignment tab, find the relevant user under the People filter and edit the user assignment by clicking on the pen icon:



Person	Type
isvtest Okta isvtest@okta.com	Individual

b. A long popup by the name of 'Edit User Assignment' should appear. The top field is the 'User Name' field. Set the username to be the BrandShield username (replace the BrandShield_UserName placeholder with the

c. original BrandShield username)



Edit User Assignment

User Name [BrandShield_UserName]

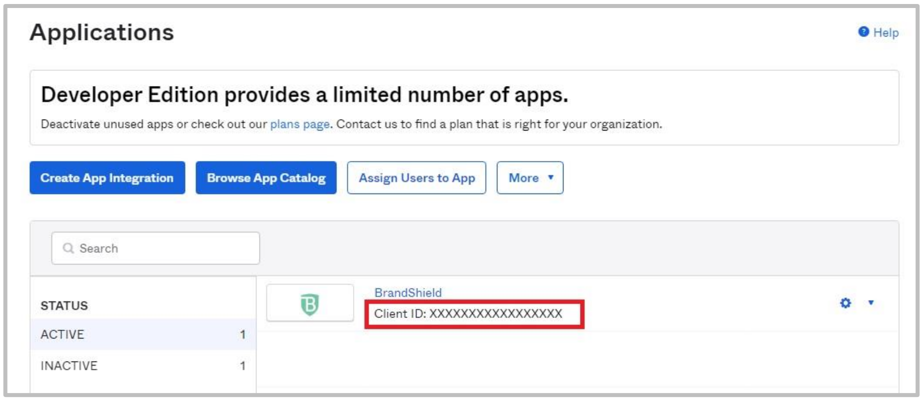
d. Click Save.

6. Click Done.

Configuring BrandShield to Authenticate using Okta

In order to configure BrandShield to authenticate using Okta, the organization must provide BrandShield the following details that will enable BrandShield to validate the authenticating users using the organization authorization server:

1. Okta Integration App Client ID –
    a. Enter your organization Okta Admin Console on https://www.okta.com
    b. In the Admin Console, go to Applications > Applications
    c. Extract the Client ID from the BrandShield App item in the list



Applications

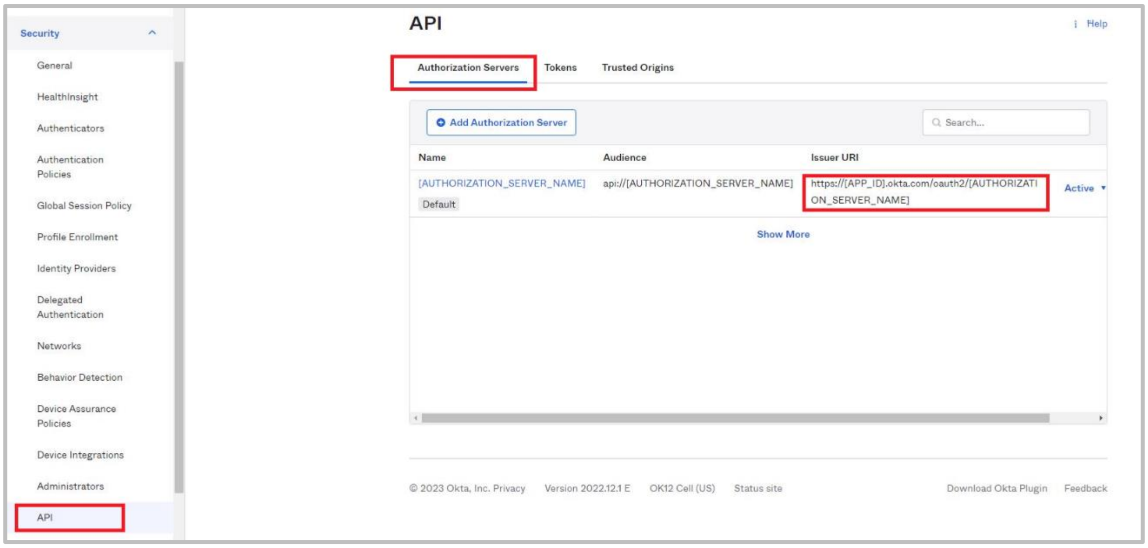
Developer Edition provides a limited number of apps.

Deactivate unused apps or check out our plans page. Contact us to find a plan that is right for your organization.

STATUS	
ACTIVE	1
INACTIVE	1

BrandShield
Client ID: XXXXXXXXXXXXXXXXX

2. Authorization Server Issuer URI –
    a. In the Admin Console, go to Security > API
    b. On the Authorization Servers tab, extract one of the active authorization servers Issuer URI values



API

Name	Audience	Issuer URI	
[AUTHORIZATION_SERVER_NAME] Default	api://[AUTHORIZATION_SERVER_NAME]	https://[APP_ID].okta.com/oauth2/[AUTHORIZATION_SERVER_NAME]	Active ▾

© 2023 Okta, Inc. Privacy Version 2022.12.1 E OK12 Cell (US) Status site Download Okta Plugin Feedback

The Client ID and Issuer URI will be provided to BrandShield's technical team.

Initiating Service Provider (SP) SSO Flow

Service Provider (SP) initiated flow for users

Once BrandShield's technical team configures Okta as the SSO solution for the organization, the organization users will be able to initiate the SSO by:

1. Browsing to https://platform.brandshield.com/

2. Entering the username as defined in Okta. In case an earlier username was provided by BrandShield, verify that the Okta administrator correlated the Okta user with BrandShield user according to the 'Assigning Users' section above.

3. Once the username was entered and verified by BrandShield, users will be redirected to Okta for authentication. In case the user was verified by Okta, he will be automatically redirected into BrandShield application. In case of a failure during authentication, users will be notified and redirected back to BrandShield login screen.