BrandShelter

BrandShelter Single Sign-On (SSO)

Introduction to SSO and implementation guide for Microsoft Azure Active Directory

Azure Active Directory

BrandShelter

Table of Contents

BrandShelter

What is Single Sign-On?

Single Sign-On, or short SSO, allows to sign into independent systems by using a single set of login credentials. With SSO a user no longer needs to sign into every application they use and no longer need separate login credentials for each application. A user enters his login credentials only once at a single page and are then authenticated to all connected applications.

BrandShelter supports connecting to other identity providers via SAML and OpenID Connect, which are two popular standards to exchange authentication and authorization information in a secure way.

When is SSO a good fit for my company?

SSO may be a good fit for your company if:

Increased Security:

You are looking for the most secure way to log into BrandShelter by requiring employees to use your company's established authentication protocols.

Simplified User Management:

You want a user's access to BrandShelter dashboard to cease when a user is terminated & losescorporate system access.

Enhanced User Experience:

You are looking to simplify the login process for users, allowing them to authenticate once and reducing the need for users to manage multiple sets of credentials.

How does SSO work?

BrandShelter's SSO feature works by leveraging Amazon Cognito as the identity provider. External identity providers are federated with Cognito via SAML or OpenID Connect. Depending on the Cognito user group and claims, federated users are assigned to BrandShelter accounts with respective permissions. This enables a seamless and secure login experience for users, while also providing centralized management of user access control.

BrandShelter

SSO Identity Provider for BrandShelter

Pre-work checklist for a successful SSO implementation

IMPORTANT!

Admin(s) to confirm that all users have work emails in Account Center. If users don't have a work email, they will be locked out after SSO is activated. Work emails need to match the users' IdP-specific emails.

1. Confirm that your organization uses a SAML 2.0 compliant IdP (e.g., Okta, Azure Active Directory).

2. Identify Admins: Identify the Account Center admin for the BrandShelter dashboard and any relevant internal IT point of contact. To configure SSO, admins will need both IdP and BrandShelter dashboard access:

   a. IdP access: To arrange this, contact your IT or Security department (whoever has IdP admin/manager access), or your IdP service provider.

   b. BrandShelter dashboard admin access: The admin will need an "Admin Account" license to enable SSO. This can be done by either:

   - Grant the license to your IdP Admin or Manager on the dashboard(s).
   - Or, transfer relevant information from your IdP admin to a Dashboard admin for entry into Account Center.

   Note: Please note that BrandShelter does not support IdP-initiated sign-in. This means certain functionalities, such as the "embed link" provided by Okta, cannot be used for sign-in purposes. All sign-ins must be initiated through the BrandShelter portal to ensure proper authentication and access.

3. OpenID Connect Integration: BrandShelter integrates with Amazon Cognito via OpenID Connect. In cases where OpenID Connect scopes may not contain all required information, users will be prompted to complete a form to provide any missing required information. Users will also be asked to agree to our data processing agreement.

4. Required Data: Request the following data from BrandShelter Support.
    a. Identifier (Entity ID)
    b. Reply URL

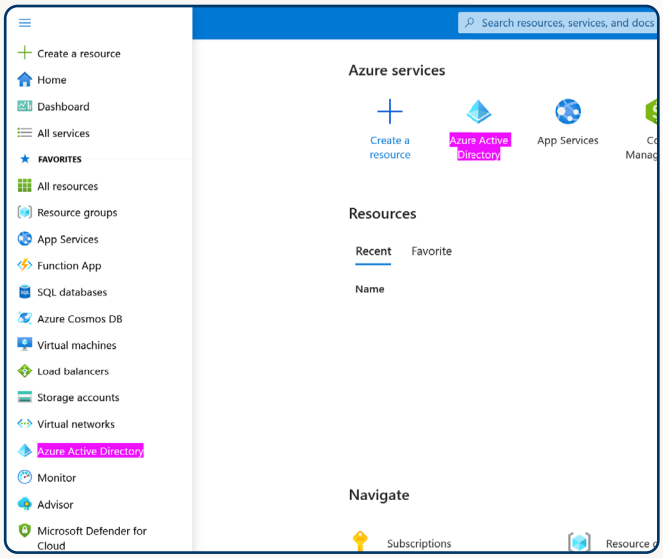
5. Communication:

- Pass on the relevant section of the IdP configuration and the attribute mapping to your internal teams.
- Provide BrandShelter with a metadata URL or document (XML file) and the mail domains used by your users for sign-in.
- Admins should inform teams about upcoming changes to their BrandShelter log-in. Refer to the sample email for guidance.

Steps to enabling SSO for Microsoft Azure Active Directory

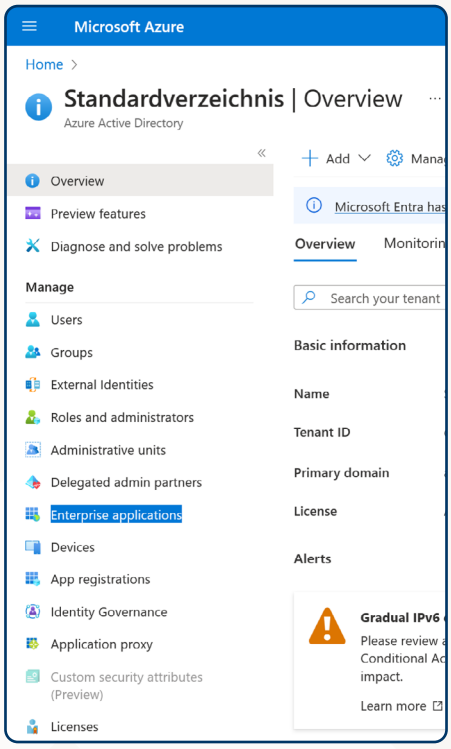
Create an Azure AD enterprise application

1. Open the Microsoft Azure portal at **https://portal.azure.com**
2. Choose **"Azure Active Directory"** in the navigation on the **left side.** If the service is not listed there, choose "All services" and type "Azure Active Directory" in the search bar for find the entry.

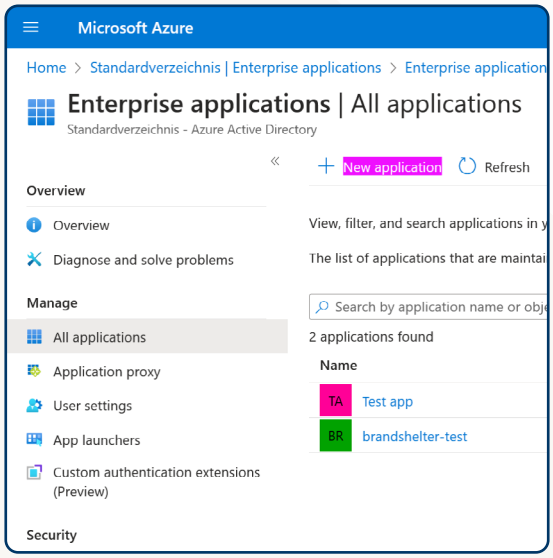


BrandShelter

3. Choose **“Enterprise application”** in the navigation on the **left side.**

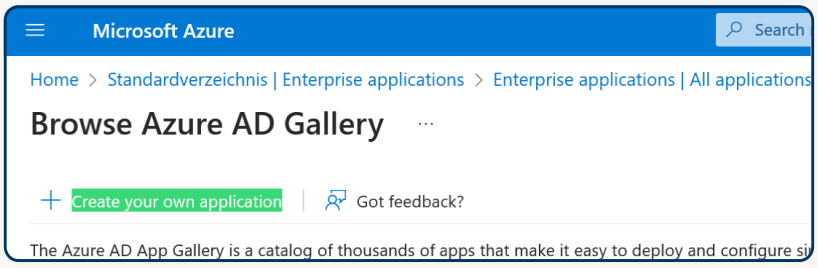


4. Click **“New application”** from the action menu **at the top.**

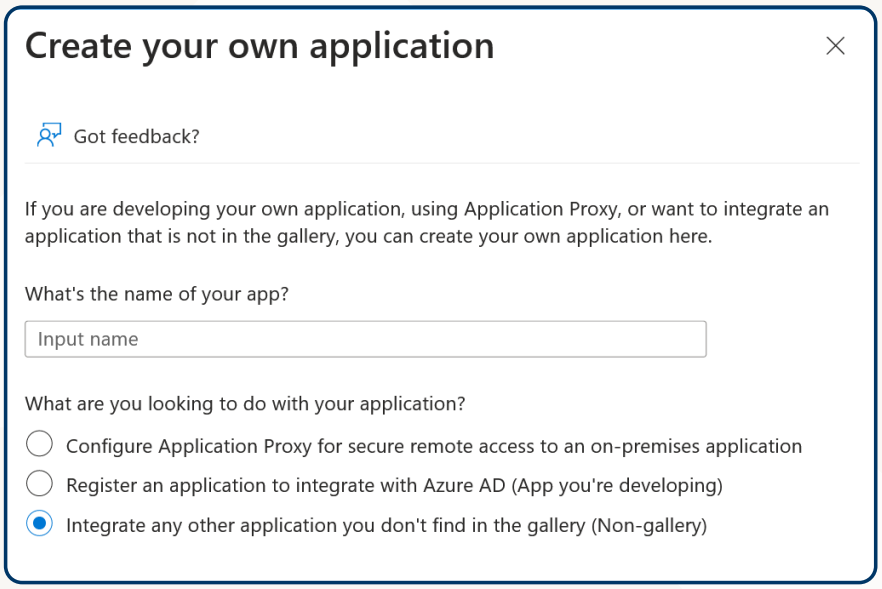


BrandShelter

5. Choose **"Create your own application"** from the action menu **at the top.**



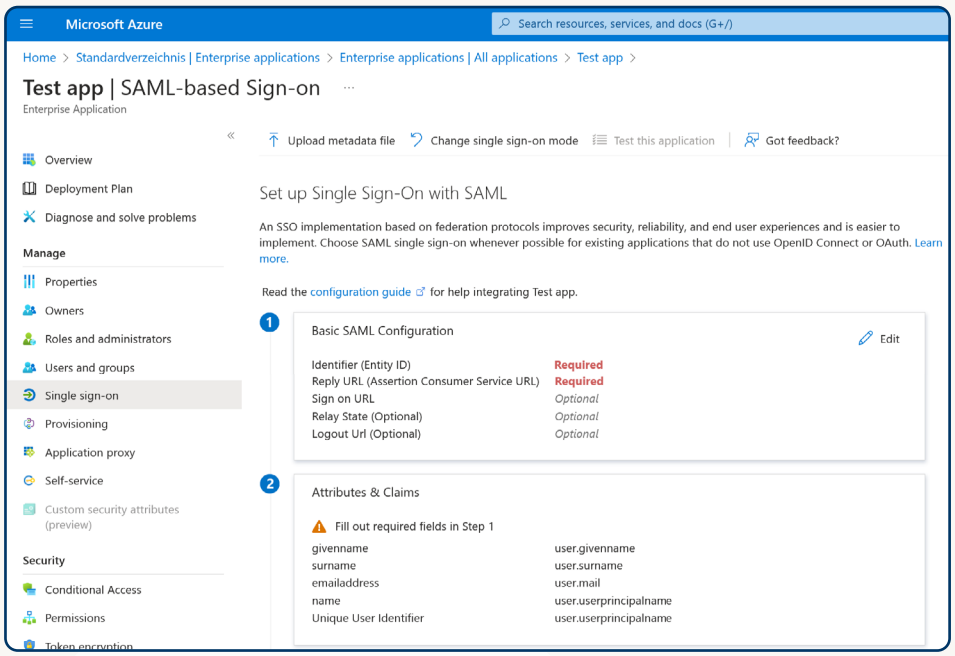
6. **Enter a name** for your application.
7. Choose **"Integrate any other application you don't find in the gallery (Non-gallery)"**



8. You should now be on the overview page of your newly created application, choose **"Single sign-on"** from the navigation on the **left.**

BrandShelter

9. Choose **"SAML"**

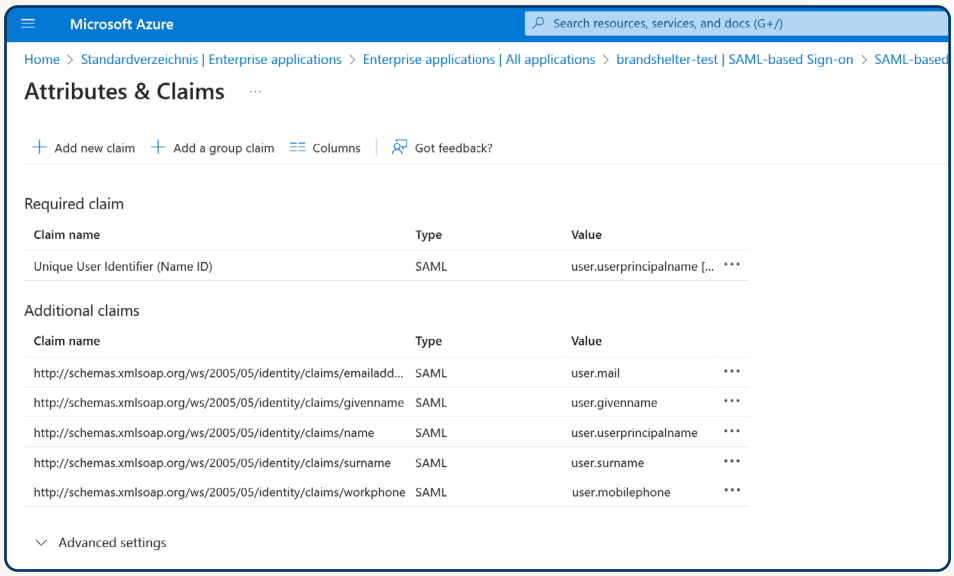


10. In the **"Basic SAML Configuration"** section

a. Click **"Edit"**
b. Enter the **"Identifier (Entity ID)"** you got from BrandShelter
c. Enter the **"Reply URL (Assertion Customer Service URL)"** you got from BrandShelter

11. In the **"Attributes & Claims"** section

a. Click **"Edit"**
b. Click **"Add a new claim."**
c. Enter **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/workphone** as "Name."
d. Choose **"user.mobile phone"** as the "Source attribute"
e. Click **"Save"**



BrandShelter

12. **In the "SAML Certificates" section**

- Copy the **"App Federation Metadata URL"** and provide this URL to BrandShelter

13. Choose **"Users and groups"** in the navigation on the **left**

- **Add** users and groups as you see fit

14. Provide federation data to BrandShelter: At the end of the setup, you should have the **federation metadata URL.** BrandShelter needs this **URL to finish the setup** on their side, once this has been done, **the federation can be tested.**

About BrandShelter

BrandShelter is the world's leading digital brand protection and corporate domain management company. We provide advanced technology and expertise to safeguard the reputation and revenue of leading brands in today's digital world, where new risks arise due to anonymity, global reach, and shifting consumption patterns of digital content, goods, and services. BrandShelter is the preferred choice of customers because of its unparalleled combination of personalized customer service, comprehensive brand protection, and strong industry relationships. We offer our clients effective solutions that mitigate brand infringement risks, safeguard their marketing investments, protect their revenues, and maintain the trust of their customers.