

Single Sign-On (SSO) Implementation Guide

Introduction to SSO and Guide for Microsoft Azure Active Directory

June 2025

BrandShelter

222 Catoctin Circle Suite 225, Leesburg, VA 20175 Phone: +1 703 574 3831 Fax: +1 201 596 1433 info@brandshelter.com

www.brandshelter.com



Table of Contents

1	Inti	roduction to Single Sign-On (SSO)4
	1.1	What is Single Sign-On?
	1.2	When is SSO a good fit for my company?
	1.3	How does SSO work?
2	Pre	-work checklist for a successful SSO Implementation
3	Ste	ps to enabling SSO for Microsoft Azure Active Directory
	3.1	Create an Azure AD enterprise application6
4	Set	ting Up SSO
	4.1	Required Setup at the IdP 12
	4.1.1	Microsoft Entra ID (formerly Azure AD)
	4.1.2	For the BrandShelter demo environment demo.brandshelter.com
	4.1.3	For the BrandShelter production environment secure.brandshelter.com
	4.2	Okta (SAML) 13
	4.2.	For the BrandShelter demo environment demo.brandshelter.com
	4.2.	2 For the BrandShelter production environment secure.brandshelter.com 13
	4.3	Okta (OpenID Connect)14
	4.3.	For the BrandShelter demo environment demo.brandshelter.com
	4.3.	2 For the BrandShelter production environment secure.brandshelter.com14
	4.4	Attribute Mapping14
	4.5	Provide federation data to BrandShelter
	4.6	Common Errors
	4.6.	"Required String parameter 'RelayState' is not present" on the Cognito-
	hos	
	4.6.	2 "An error was encountered with the requested page." (no further info) on
	the	Cognito-hosted page
	4.6.	3 "Invalid relayState from identity provider" or "Invalid samlResponse or
	relo	yState from identity provider" on the Cognito-hosted page

Phone: +1 703 574 3831 | Fax: +1 201 596 1433 | info@brandshelter.com | www.brandshelter.com



4.6.4	"Invalid saml response received: client is not enabled for oauth2.0 flows						
" on the	BrandShelter hosted login page						
4.6.5	4.6.5 "Could not authenticate you from OpenIDConnect because "invalid 'state'						
parame	parameter" on the BrandShelter hosted login page						
4.6.6 "Your single sign-on user <email> is not assigned to any <brand> accounted accounter signed to any <brand> accounter signed to any <brand> accounter signed to any <brand <br="" any="" signed="" to=""></brand> <</brand></brand></brand></email>							
	20						



1 Introduction to Single Sign-On (SSO)

1.1 What is Single Sign-On?

Single Sign-On (SSO) enables users to log into multiple independent systems using just one set of login credentials. With SSO, users don't need to sign into each application separately nor maintain distinct login details for every application. They simply enter their login credentials once on a single page and gain access to all connected applications.

BrandShelter provides support for integration with other identity providers through SAML and OpenID Connect. These are two widely used standards for securely exchanging authentication and authorization information.

1.2 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 & loses corporate 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.

1.3 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.

SSO Identity Provider for BrandShelter is AWS Cognito.

2 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.

- Confirm that your organization uses a SAML 2.0 compliant IdP (e.g., Okta, Azure Active Directory).
- 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:
- IdP access: To arrange this, contact your IT or Security department (whoever has IdP admin/manager access), or your IdP service provider.
- Second Shelter 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).
- Solution of the organization of the organizati
- Solution 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.



- **Required Data:** Request the following data from BrandShelter Support:
- ✓ Identifier (Entity ID)
- ✓ Reply URL
- Sommunication: Admins should inform teams about upcoming changes to their BrandShelter log-in. Refer to the sample email for guidance.

3 Steps to enabling SSO for Microsoft Azure Active Directory

3.1 Create an Azure AD enterprise application

- 𝔅 Open the Microsoft Azure portal at https://portal.azure.com
- 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 t find the entry.

=	P Search resources, services, and docs
+ Create a resource	1 million and an
🟫 Home	Azure services
Dashboard	+ 🚸 🔕 🇯
All services	Create a Acure Active App Services Co
* FAVORITES	resource Directory Manag
All resources	
(Resource groups	Resources
😒 App Services	Recent Favorite
i Function App	
SQL databases	Name
💆 Azure Cosmos DB	
Virtual machines	
Load balancers	
Storage accounts	
Virtual networks	
Azure Active Directory	
Monitor	Navianta
Advisor	Navigate
Microsoft Defender for Cloud	Subscriptions (i) Resource g

BrandShelter 222 Catoctin Circle, Suite 225, Leesburg, VA 20175, USA Phone: +1 703 574 3831 | Fax: +1 201 596 1433 | info@brandshelter.com | www.brandshelter.com



 \odot Choose "Enterprise application" in the navigation on the left side

Home >	
Standardverzeichr Azure Active Directory	nis Overview
	× + Add × () Manag
Overview	
Preview features	Microsoft Entra has
X Diagnose and solve problems	Overview Monitoring
Manage	Search your tenant
L Users	
A Groups	Basic information
External Identities	Name S
Roles and administrators	Tanaat ID
Administrative units	tenant ID c
Delegated admin partners	Primary domain a
Enterprise applications	License A
Devices	Alaste
R App registrations	Aleis
Identity Governance	Gradual IPv6 e
Application proxy	Please review ar
Custom security attributes	impact.
(Preview)	Learn more 🖸
Licenses	



Microsoft Azure								
Home > Standardverzeichnis Enterprise applications > Enterprise application:								
Enterprise applications All applications Standardverzeichnis - Azure Active Directory								
	Hew application Refresh Re							
Overview								
Overview	View, filter, and search applications in y							
X Diagnose and solve problems	The list of applications that are maintain							
Manage	Search by application name or obje							
All applications	2 applications found							
Application proxy	Name							
User settings	TA Test app							
App launchers	8R brandshelter-test							
Custom authentication extensions (Preview)								
Security								
-								

\otimes Choose "Create your own application" from the action menu at the top



The Azure AD App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on

- 𝔅 Enter a name for your application
- Solution Choose "Integrate any other application you don't find in the gallery (Nongallery)"



Create your own application	×
♀ Got feedback?	
f you are developing your own application, using Application Proxy, or want to application that is not in the gallery, you can create your own application here.	integrate an
What's the name of your app?	
Input name	
What are you looking to do with your application?	
Configure Application Proxy for secure remote access to an on-premises a	pplication
Register an application to integrate with Azure AD (App you're developing)
Integrate any other application you don't find in the gallon. (Non-gallon)	

- You should now be on the overview page of your newly created application, choose "Single sign-on" from the navigation on the left
- 𝔄 Choose "SAML"



Microsoft Azure		P. Sear	ch resources, services, and docs (G+/)				
Home > Standardverzeichnis Enterp	orise applicat	tions > Enterprise applications All applications	ons > Test app >				
Test app SAML-base	d Sign-	on					
Noverview	≪ Ť ∪	pload metadata file 🏷 Change single sign-or	a mode 🛛 Test this application 🔰 👰 Got feedback?				
Deployment Plan	Set u	p Single Sign-On with SAML	AMI				
X Diagnose and solve problems	id solve problems An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to						
Manage	more.	ent. Choose SAML single sign-on whenever pos	sible for existing applications that do not use OpenID Connect or OAuth. Lea				
Properties	Read t	he configuration muide 15 for help integration Te	14 ano.				
 Owners Roles and administrators 	0	Basic SAML Configuration	Ø Edit				
Users and groups		Identifier (Entity ID)	Required				
Single sign-on		Reply URL (Assertion Consumer Service URL) Sign on URL	Required Optional				
Provisioning		Relay State (Optional)	Optional				
Application proxy		Logout Un (Optional)	Optional				
G Self-service	0	2 Autobate & Chine					
G Custom security attributes (preview)		Fill out required fields in Step 1					
Security		givenname	user.givenname				
Conditional Access		emailaddress	user.mail				
A Permissions		name Unique User Identifier	user.userprincipalname user.userprincipalname				
a Token encontion		400000000000000000000000000000000000000	2581023328690000				

- 𝔅 In the "Basic SAML Configuration" section
- 𝔄 Click "Edit"
- ⊗ Enter the "Identifier (Entity ID)" you got from BrandShelter

- ♂ Click "Add a new claim"
- Senter <u>http://schemas.xmlsoap.org/ws/2005/05/identity/claims/workphone</u> as "Name"
- 𝔅 Choose "user.mobile phone" as the "Source attribute"
- 𝔄 Click "Save"



Microsoft Azure	,₽ s	earch resources, services, and	d doci				
Home > Standardverzeichnis Enterprise applications > Enterpri	se applications All applic	ations > brandshelter-test	SAJ				
Attributes & Claims							
+ Add new claim + Add a group claim EE Columns R	Got feedback?						
had the carts had a group carts in contras C	and he append						
equired claim							
Claim name	Туре	Value					
Unique User Identifier (Name ID)	SAML	user.userprincipalname [
Additional claims							
Claim name	Туре	Value					
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd	SAML	user.mail					
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	SAML	user.givenname					
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SAML	user.userprincipalname	•••				
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	SAML	user.sumame					
	C + + + +	user mehilenhene					

- Solution SAML Certificates Section € 10 Section
- Copy the "App Federation Metadata URL" and provide this URL to BrandShelter
- S Choose "Users and groups" in the navigation on the left
- ♂ Add users and groups as you see fit
- 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.

4 Setting Up SSO

To integrate Single Sign-On (SSO) between your identity provider (e.g., Microsoft Entra ID [formerly Azure Active Directory] or Okta) and BrandShelter, we support a standard SSO federation setup. Please note the following key points:

Sign-In Flow: BrandShelter currently supports only *service providerinitiated* sign-in. This means users must start the sign-in process from the



BrandShelter portal. Features like Okta's "embed link" for IdP-initiated signin are not supported.

- Setup Requirements: You'll need to provide your IdP metadata (either as a URL or XML file). Share the email domains your users will use to sign in.
- Configuration Support: We'll provide the necessary configuration details and attribute mapping to help you complete the setup in your IdP.

4.1 Required Setup at the IdP

4.1.1 Microsoft Entra ID (formerly Azure AD)

The following data needs to be configured on Azure AD:

- ⊗ Identifier (Client ID) (mandatory)
- ♂ Reply URL (mandatory)
- Sign on URL (mandatory)
- ♂ Relay State (optional)

4.1.2 For the BrandShelter demo environment demo.brandshelter.com

Client id: urn:amazon:cognito:sp:eu-central-1_ieAQ8aVrs

Reply URL: <u>https://bs-ote-auth.auth.eu-central-</u>

1.amazoncognito.com/saml2/idpresponse

Sign on URL: <u>https://demo.brandshelter.com/users/sign_in</u>

Relay State (Optional): <u>https://demo.brandshelter.com/</u>



4.1.3 **For the BrandShelter production environment** secure.brandshelter.com

Client id: urn:amazon:cognito:sp:eu-central-1_FmcrLjcuB

Reply URL: <u>https://bs-live-auth.auth.eu-central-</u> <u>1.amazoncognito.com/saml2/idpresponse</u>

Sign on URL: <u>https://secure.brandshelter.com/users/sign_in</u>

Relay State (Optional): <u>https://secure.brandshelter.com/</u>

4.2 Okta (SAML)

4.2.1 For the BrandShelter demo environment demo.brandshelter.com

- Single Sign On URL: <u>https://bs-ote-auth.auth.eu-central-</u>
 <u>1.amazoncognito.com/saml2/idpresponse</u>
- S Audience restriction: urn:amazon:cognito:sp:eu-central-1_ieAQ8aVrs
- ♂ Default Relay State: leave blank
- In Security/API/Trusted Origins, add <u>https://bs-ote-auth.auth.eu-central-</u>
 <u>1.amazoncognito.com</u> as a permitted "redirect"

4.2.2 For the BrandShelter production environment

secure.brandshelter.com

- Single Sign On URL: <u>https://bs-live-auth.auth.eu-central-</u>
 <u>1.amazoncognito.com/saml2/idpresponse</u>
- S Audience restriction: urn:amazon:cognito:sp:eu-central-1_FmcrLjcuB
- 𝔄 Default Relay State: leave blank



In Security/API/Trusted Origins, add <u>https://bs-live-auth.auth.eu-central-</u>
 <u>1.amazoncognito.com</u> as a permitted "redirect"

4.3 Okta (OpenID Connect)

- 4.3.1 For the BrandShelter demo environment demo.brandshelter.com
 - Single Sign On URL: <u>https://bs-ote-auth.auth.eu-central-</u>
 <u>1.amazoncognito.com/oauth2/idpresponse</u>
 - In Security/API/Trusted Origins, add <u>https://bs-ote-auth.auth.eu-central-</u>
 <u>1.amazoncognito.com</u> as a permitted "redirect"
- 4.3.2 For the BrandShelter production environment secure.brandshelter.com
 - Single Sign On URL: <u>https://bs-live-auth.auth.eu-central-</u>
 <u>l.amazoncognito.com/oauth2/idpresponse</u>
 - In Security/API/Trusted Origins, add <u>https://bs-live-auth.auth.eu-central-</u>
 <u>1.amazoncognito.com</u> as a permitted "redirect"

4.4 Attribute Mapping

Solution By default, we process the following assertions to onboard users:

For SAML:

- ⊗ http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
- ⊗ http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
- <u>http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname</u>
- ⊗ <u>http://schemas.xmlsoap.org/ws/2005/05/identity/claims/workphone</u>



Scopes and attributes OIDC:

- 𝔅 "profile" scope for given_name and family_name
- 𝔄 "email" scope for email

We are using the "URI Reference" name format ; and we assign user.email to both "name" and "emailaddress" attributes, but other mapping can work as well.

Example:

Name	Name Format	Value
http://schemas.xmlsoap.org/ ws/2005/05/identity/claims/ emailaddress	URI Reference	user.email
http://schemas.xmlsoap.org/ ws/2005/05/identity/claims/ givenname	URI Reference	user.firstName
http://schemas.xmlsoap.org/ ws/2005/05/identity/claims/ name	URI Reference	user.email
http://schemas.xmlsoap.org/ ws/2005/05/identity/claims/ surname	URI Reference	user.lastName

Other attributes can be mapped on request.

The above attributes are required, and we cannot change those requirements without recreating the user pool and breaking all existing federations.



Additionally, <u>Cognito requires</u> phone numbers to be given in a very specific format:

"Phone numbers must follow these format rules: A phone number must start with a plus (+) sign, followed immediately by the country code. A phone number can only contain the + sign and digits. Remove any other characters from a phone number, such as parentheses, spaces, or dashes (-) before you submit the value to the service. For example, a phone number based in the United States must follow this format: +14325551212."

If a client is unable to provide that format, please advise to map a blank attribute so users can enter that information during the onboarding process. For example in Okta, an administrator can simply map the empty string to the phone_number attribute for their BrandShelter application:

user.countryCode == null ? "en_US" : user.countryCod	•	→ •	locale	string
	•	→ •	phone_number	string
user.streetAddress	•	→ •	street_address	string

4.5 Provide federation data to BrandShelter

You must provide us with a metadata URL or document (XML file), as well as the mail domains used by their users for sign-in.

And specify the protocol used for the SSO federation, i.e. SAML or OIDC.

IMPORTANT: You can choose between 2 possible configurations for access to the BrandShelter portal after SSO activation.

1) Default Configuration 1 - BrandShelter + SSO Connection

The 2 connection methods coexist, direct connection and SSO:



- or by using the SSO login which requires entering only your email address (or SSO username) in the "Username" field, then clicking on "Login" without entering the password to be redirected to the SSO form.

This configuration is intended to allow the addition and login of users who do not have an email address linked to SSO and who would therefore need a direct connection to the portal to access your account.

2) Configuration 2 to be enabled on demand - SSO single sign-on

We disable the BrandShelter direct connection (username + password) and only the SSO method is possible.

This makes SSO connection mandatory and inevitable to log in for all users of the account without exception.

Note 1: Each user with a username matching one of these hosts will be required to authenticate through Single Sign-On (SSO) (configuration 2). Any user of this account with a username which does not match one of these hosts will require their normal local credentials and will not be using SSO (default configuration 1). E.g. the hostname example.com will match usernames like name@example.com.

Note 2: 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, or through other authentication platforms, e.g., Azure's "My Applications" portal. All sign-ins must be initiated through the BrandShelter portal to ensure proper authentication and access.

Please ensure then that the users **always start** the login attempt on our portal.

Note 3 : A new user will still be redirected to BrandShelter's account creation page to fill in all the information not provided by their IdP. In addition, it is important to note that an existing portal user will be redirected to the account creation page



on BrandShelter to fill in and/or update all the information not provided by their IdP.

User experience after SSO activation:

A user visit the BrandShelter portal. If he is already authenticated with his corporate identity provider, he's immediately signed into BrandShelter and the process stops here.

If he's not yet authenticated, the user enters his login name into the BrandShelter sign-in form.

The user is redirected to the sign-in form of his company, this could be for example the Microsoft sign-in form. After entering his credentials, the user is redirected back to the BrandShelter portal and is signed-in there.

Additional information link:

Amazon Cognito FAQs

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.

4.6 Common Errors

4.6.1 "Required String parameter 'RelayState' is not present" on the Cognito-hosted page

Wait a few minutes after entering information. We managed to reproduce the error by changing the application in AAD and immediately initiating a sign-in, but did not get a solid reproduction.



4.6.2 "An error was encountered with the requested page." (no further info) on the Cognito-hosted page

This can happen when attempting to use IdP-initiated sign-in, e.g. through the "Test sign in" button in the Azure Portal, or the "My Application" portal. BrandShelter currently does not support this at the moment, but we are working on.

For the time being, please make sure to initiate sign-in through the BrandShelter portal or make sure to enter the correct sign-in URL as indicated in the preamble at the top of the page to make the IdP redirect users to our portal.

4.6.3 "Invalid relayState from identity provider" or "Invalid samlResponse or relayState from identity provider" on the Cognito-hosted page

This is another reaction to IdP-initiated sign-in, observed when attempting to use the Okta Embed Link.

4.6.4 "Invalid saml response received: client is not enabled for oauth2.0 flows " on the BrandShelter hosted login page

This indicates an incorrect reply URL. Make sure to use the URLs given at the top of the page.

This can also be caused by the Cognito client missing the *AllowedOAuthFlowsUserPoolClient* flag in the application client, which was an issue in older versions of the automated setup scripts. To rectify this, a developer can simply enter the application client edit page and save it without changes.

4.6.5 "Could not authenticate you from OpenIDConnect because "invalid 'state' parameter" on the BrandShelter hosted login page

Make sure that the user initiates sign-in on the same host that it will ultimately be forwarded to (and indicated in your SSO settings). A user in an account using, e.g.,



home.safebrands.com cannot initiate sign-in at secure.brandshelter.com. We are working so that this no longer has an impact and that the connection can be initiated from the 2 URLs.

4.6.6 "Your single sign-on user <email> is not assigned to any <brand> account"

Ensure that the user in question is assigned to the appropriate group for the application client in Cognito.

4.6.7 "Could not authenticate you from OpenIDConnect because "Invalid SAML response received: invalid phone number format."

Refer to the warning highlighted in yellow above in this page and check your SSO configuration: this message indicates an error in the attribute mapping of your SSO configuration, specifically on the format of the phone number.