BrandShelter

Guide de mise en œuvre de l'authentification unique (SSO)

Introduction à la connexion SSO et guide pour Microsoft Azure Active Directory

Juin 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

BrandShelter

Table des matières

1 Introduction à l'authentification unique (SSO)

1.1 Qu'est-ce que l'authentification unique (SSO) ?

L'authentification unique (SSO) permet aux utilisateurs de se connecter à plusieurs systèmes indépendants en utilisant un seul ensemble d'identifiants. Avec la connexion SSO, les utilisateurs n'ont pas besoin de se connecter à chaque application séparément ni de gérer des identifiants distincts pour chaque application. Il leur suffit de saisir leur identifiant une seule fois sur une page unique pour accéder à toutes les applications connectées.

BrandShelter prend en charge l'intégration avec d'autres fournisseurs d'identité via SAML et OpenID Connect. Il s'agit de deux normes largement utilisées pour l'échange sécurisé d'informations d'authentification et d'autorisation.

1.2 Quand l'authentification unique (SSO) est-elle adaptée à mon entreprise ?

La connexion SSO peut être adaptée à votre entreprise si :

- **Sécurité renforcée :** Vous recherchez le moyen le plus sécurisé de vous connecter à BrandShelter en exigeant que les employés utilisent les protocoles d'authentification établis par votre entreprise.
- **Gestion simplifiée des utilisateurs :** Vous souhaitez que l'accès d'un utilisateur au portail BrandShelter soit automatiquement révoqué lorsqu'il quitte l'entreprise et perd l'accès à vos systèmes internes.
- **Expérience utilisateur améliorée :** Vous cherchez à simplifier le processus de connexion pour les utilisateurs, en leur permettant de s'authentifier une seule fois et en réduisant la nécessité de gérer plusieurs ensembles d'identifiants.

1.3 Comment fonctionne la connexion SSO ?

La fonctionnalité SSO de BrandShelter utilise Amazon Cognito comme fournisseur d'identité. Les fournisseurs d'identité externes sont fédérés avec Cognito via SAML ou OpenID Connect. Selon le groupe d'utilisateurs Cognito et les demandes spécifiques, les utilisateurs fédérés sont affectés aux comptes BrandShelter avec les permissions correspondantes. Cela permet une expérience de connexion fluide et sécurisée pour les utilisateurs, tout en offrant une gestion centralisée du contrôle d'accès.

Le fournisseur d'identité SSO pour BrandShelter est AWS Cognito.

2 Liste de vérification préalable pour une mise en œuvre réussie de la connexion SSO

IMPORTANT : Les administrateurs doivent confirmer que tous les utilisateurs ont une adresse e-mail professionnelle dans le Centre d'Administration (*Account Center*). Si les utilisateurs n'ont pas d'e-mail professionnel, ils seront bloqués après l'activation du SSO. Les adresses e-mails professionnelles doivent correspondre aux e-mails spécifiques des utilisateurs dans le fournisseur d'identité (IdP).

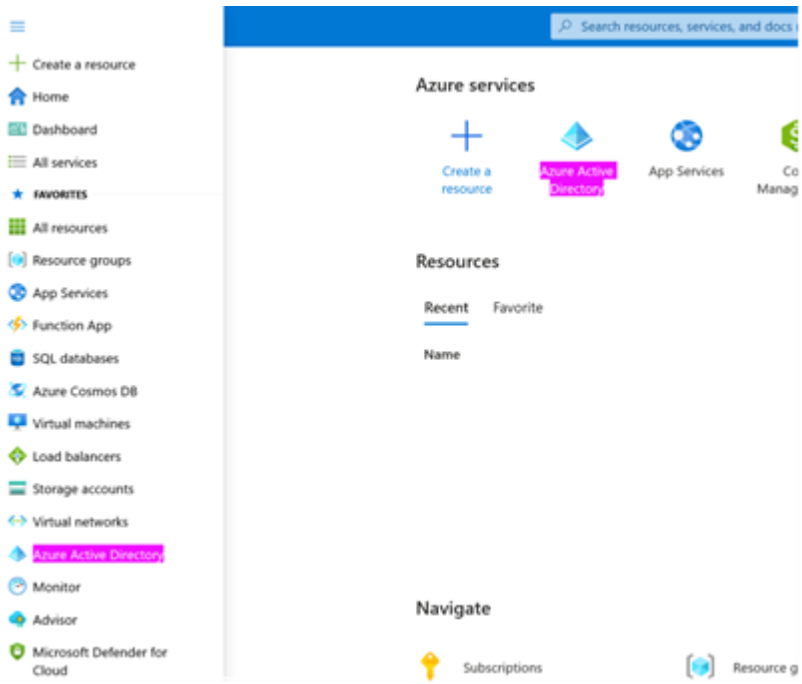
- Confirmez que votre organisation utilise un IdP conforme à la norme SAML 2.0 (par exemple, Okta, Azure Active Directory).
- **Identifier les administrateurs :** Identifiez l'administrateur de l'Account Center pour le portail BrandShelter ainsi que tout point de contact IT interne pertinent. Pour configurer le SSO, les administrateurs doivent avoir accès à la fois à l'IdP et au portail BrandShelter :

- **Accès IdP :** Pour cela, contactez votre service informatique ou sécurité (celui qui gère l'administration de l'IdP) ou votre fournisseur de service IdP.
- **Accès administrateur au portail et au tableau de bord BrandShelter :** L'administrateur devra disposer d'une licence « Compte administrateur » pour activer le SSO. Cela peut être fait en :
- Attribuant la licence à votre administrateur ou gestionnaire IdP sur le(s) tableau(x) de bord.
- Ou en transférant les informations requises depuis votre administrateur IdP à un administrateur du tableau de bord pour saisie dans l'Account Center.
- **Intégration OpenID Connect :** BrandShelter s'intègre avec Amazon Cognito via OpenID Connect. Dans les cas où les champs OpenID Connect ne contiennent pas toutes les informations requises, les utilisateurs seront invités à compléter un formulaire pour fournir les informations manquantes. Ils devront également accepter notre accord de traitement des données.
- **Données requises :** Récupérez les données suivantes à la section 4.1 Configuration requise chez le fournisseur d'identité (IdP)
- Identifiant (Entity ID)
- URL de réponse (Reply URL)
- **Communication :** Les administrateurs doivent informer les équipes des changements à venir concernant la connexion à BrandShelter. Reportez-vous à l'e-mail type pour vous guider.

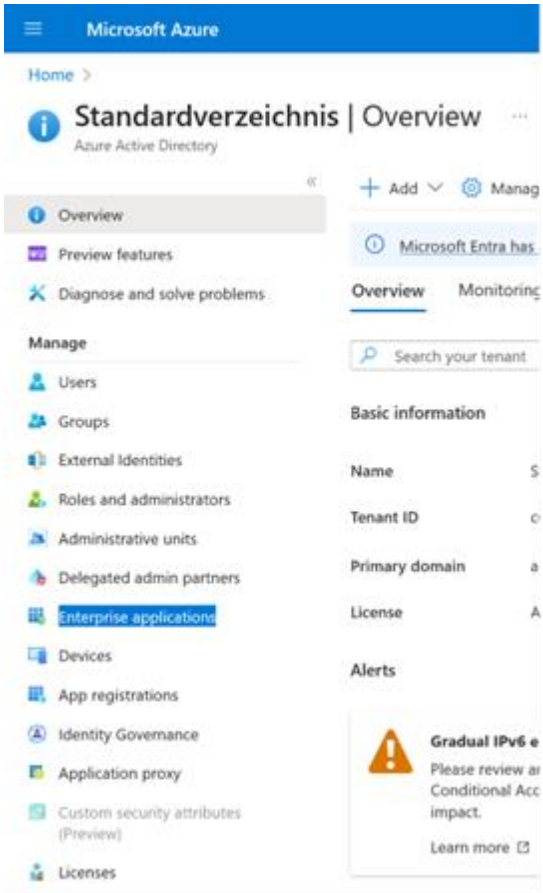
3 Étapes pour activer la connexion SSO avec Microsoft Azure Active Directory

3.1 Créer une application d'entreprise Azure AD

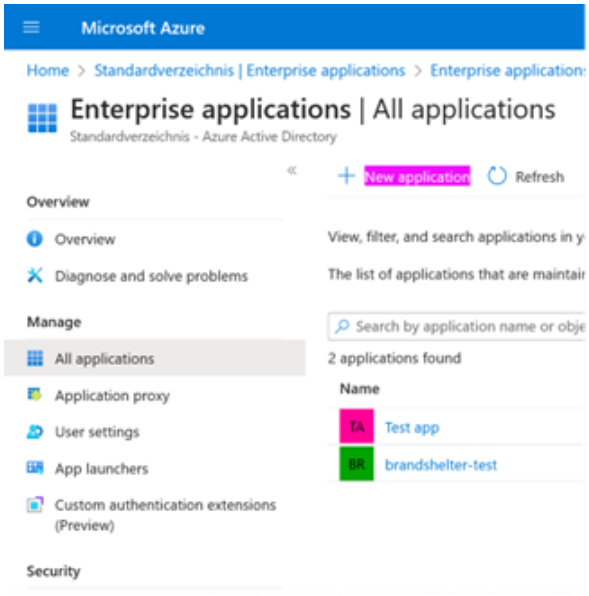
- Ouvrez le portail Microsoft Azure à l'adresse https://portal.azure.com
- Choisissez « Azure Active Directory » dans la navigation à gauche. Si ce service n'apparaît pas, sélectionnez « Tous les services » et tapez « Azure Active Directory » dans la barre de recherche pour trouver l'entrée.



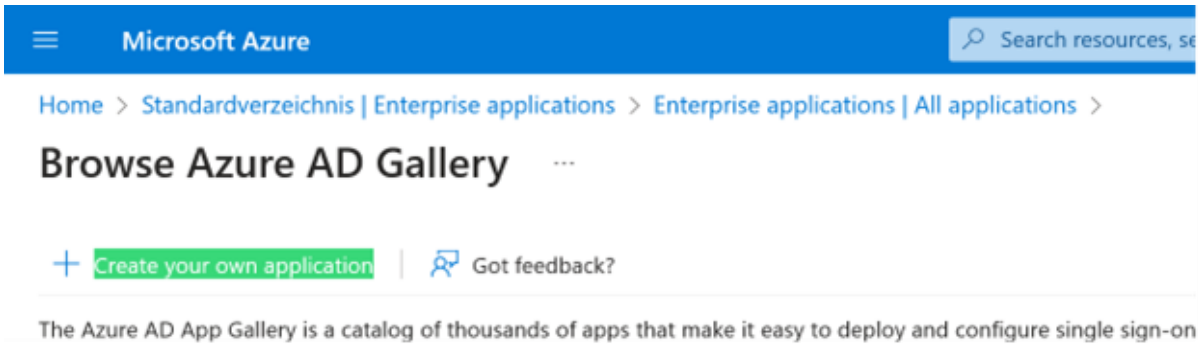
- Choisissez « Application d'entreprise » dans la navigation à gauche



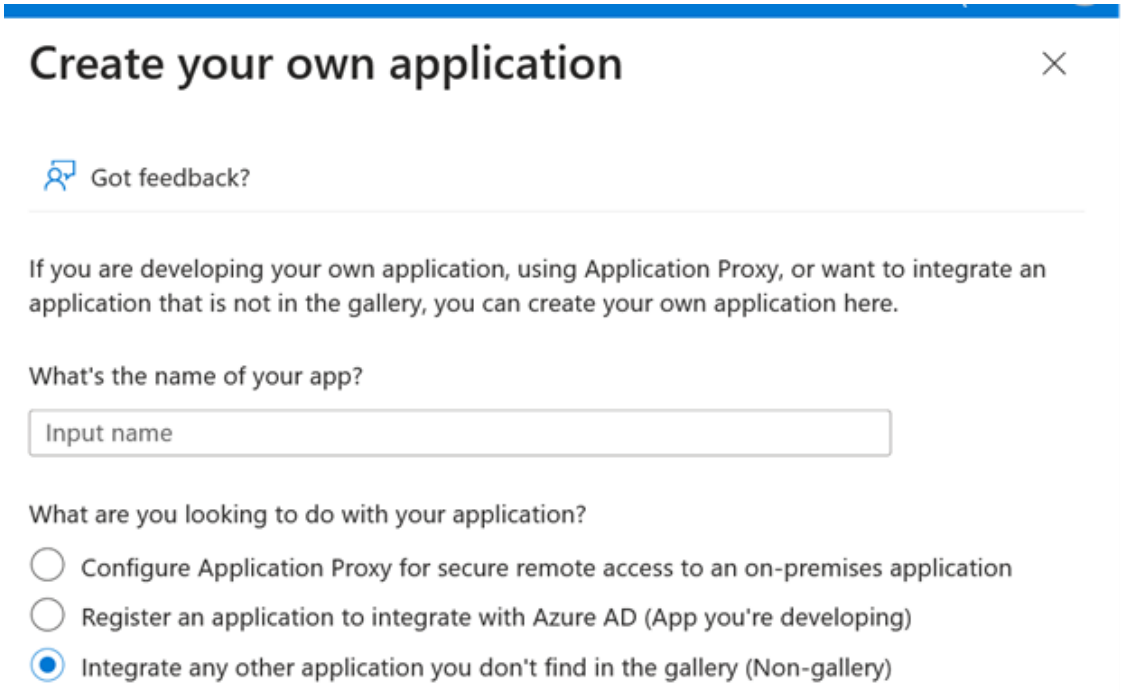
- Cliquez sur « Nouvelle application » dans le menu d'actions en haut



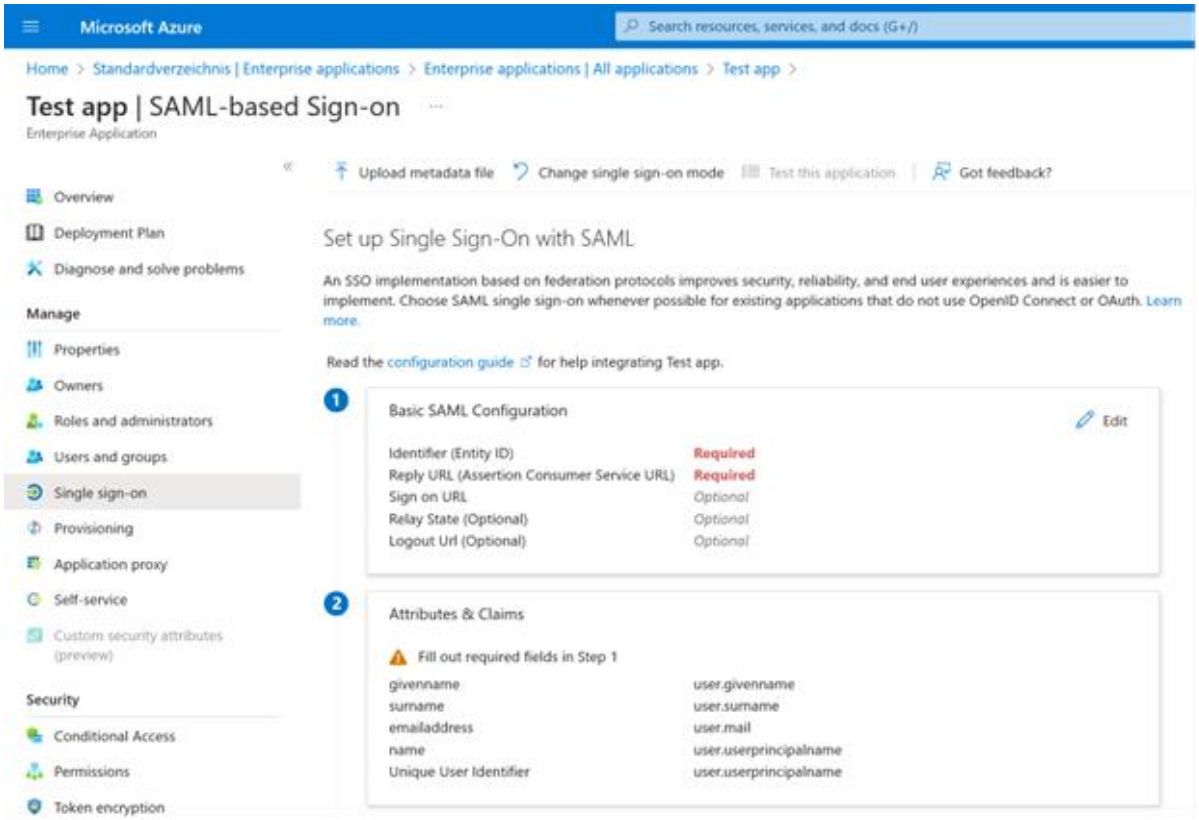
- Choisissez « Créez votre propre application » dans le menu d'actions en haut



- Saisissez un nom pour votre application
- Choisissez « Intégrer toute autre application que vous ne trouvez pas dans la galerie (Non-galerie) »



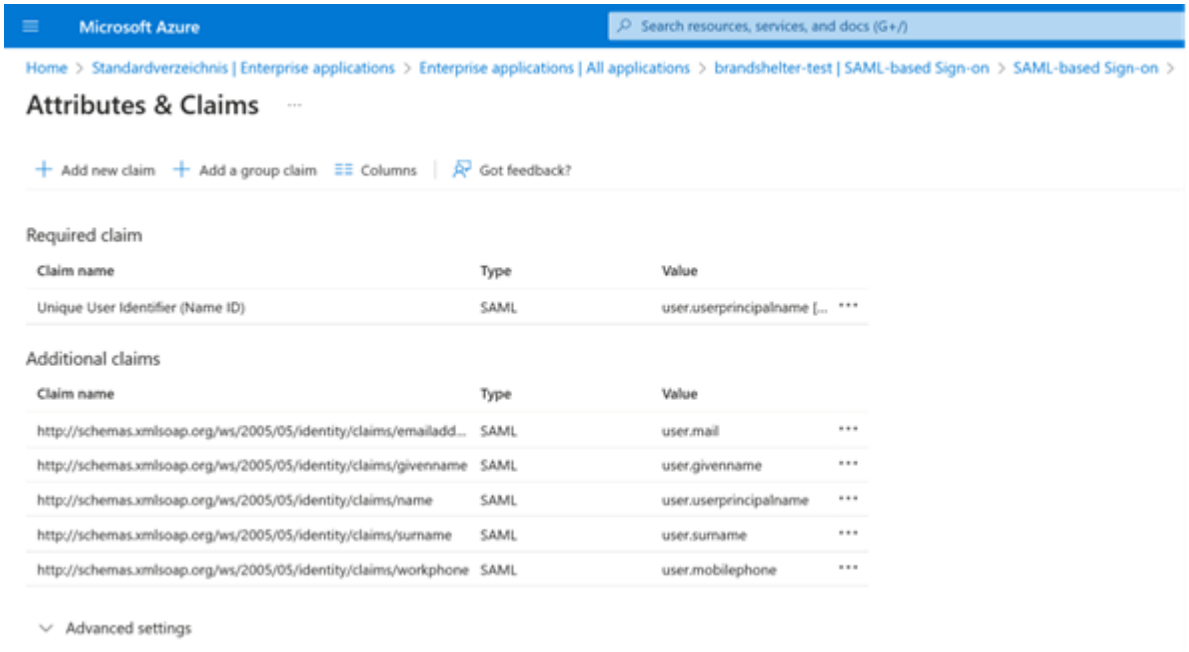
- Vous devriez maintenant être sur la page d'aperçu de votre application nouvellement créée, choisissez « Authentification unique » dans la navigation à gauche.
- Choisissez « SAML »



Dans la section **« Configuration SAML de base »**

- Cliquez sur **« Modifier »**
- Saisissez l'**« Identifiant (Entity ID) » (à récupérer dans la section 4.1 Configuration requise chez le fournisseur d'identité (IdP))**
- Saisissez l'**« URL de réponse (Reply URL / Assertion Consumer Service URL) » (à récupérer dans la section 4.1 Configuration requise chez le fournisseur d'identité (IdP))**

- Dans la section **« Attributs et spécifications »**
- Cliquez sur **« Modifier »**
- Cliquez sur **« Ajouter une nouvelle demande spécifique »**
- Saisissez **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/workphone** comme **« Nom »**
- Choisissez **user.mobilephone** comme **« Attribut source »**
- Cliquez sur **« Enregistrer »**



Dans la section **« Certificats SAML »**

- Copiez l'**« URL des métadonnées de fédération de l'application »** et fournissez cette URL à BrandShelter
- Choisissez **« Utilisateurs et groupes »** dans la navigation à gauche

- Ajoutez les utilisateurs et groupes selon vos besoins
- Fournissez les données de fédération à BrandShelter : À la fin de la configuration, vous devez disposer de l'URL des métadonnées de fédération. BrandShelter a besoin de cette URL pour finaliser la configuration de leur côté. Une fois cela fait, la fédération peut être testée.

4 Configuration de la connexion SSO

Pour intégrer l'authentification unique (SSO) entre votre fournisseur d'identité (par exemple, Microsoft Entra ID [anciennement Azure Active Directory] ou Okta) et BrandShelter, nous supportons une configuration standard de fédération SSO. Veuillez noter les points clés suivants :

- **Flux de connexion :** BrandShelter prend actuellement en charge uniquement la connexion initiée par le fournisseur de service. Cela signifie que les utilisateurs doivent obligatoirement initier le processus de connexion depuis le portail BrandShelter. Les fonctionnalités comme le « lien intégré » d'Okta pour une connexion initiée par l'IdP ne sont pas prises en charge.
- **Exigences de configuration :** Vous devrez fournir les métadonnées de votre IdP (soit sous forme d'URL, soit sous forme de fichier XML). Communiquez les domaines de messagerie que vos utilisateurs utiliseront pour se connecter.
- **Assistance à la configuration :** Nous vous fournirons les détails nécessaires pour la configuration et le mapping des attributs afin de vous aider à compléter la configuration dans votre IdP.

4.1 Configuration requise chez le fournisseur d'identité (IdP)

4.1.1 Microsoft Entra ID (anciennement Azure AD)

Les données suivantes doivent être configurées sur Azure AD :

- Identifiant (Client ID) (obligatoire)
- URL de réponse (Reply URL) (obligatoire)
- URL de connexion (Sign on URL) (obligatoire)
- Relay State (facultatif)

4.1.2 Pour l'environnement de démonstration BrandShelter demo.brandshelter.com

- **Client ID :** urn:amazon:cognito:sp:eu-central-1_ieAQ8aVrs
- **URL de réponse (Reply URL) :** https://bs-ote-auth.auth.eu-central-1.amazoncognito.com/saml2/idpresponse
- **URL de connexion (Sign on URL) :** https://demo.brandshelter.com/users/sign_in
- **Relay State (facultatif) :** https://demo.brandshelter.com/

4.1.3 Pour l'environnement de production BrandShelter secure.brandshelter.com

4.1.4 **Client ID :** urn:amazon:cognito:sp:eu-central-1_FmcrLjcuB

4.1.5 **URL de réponse (Reply URL) :** https://bs-live-auth.auth.eu-central-1.amazoncognito.com/saml2/idpresponse

4.1.6 **URL de connexion (Sign on URL) :** https://secure.brandshelter.com/users/sign_in

4.1.7 **Relay State (facultatif) :** https://secure.brandshelter.com/

4.2 Okta (SAML)

4.2.1 Pour l'environnement de démonstration BrandShelter demo.brandshelter.com

- **URL de connexion unique (Single Sign On URL) :** https://bs-ote-auth.auth.eu-central-1.amazoncognito.com/saml2/idpresponse
- **Restriction d'audience :** urn:amazon:cognito:sp:eu-central-1_ieAQ8aVrs
- **Relay State par défaut :** laisser vide
- Dans **Security/API/Trusted Origins**, ajoutez https://bs-ote-auth.auth.eu-central-1.amazoncognito.com comme redirection autorisée (« redirect »)

4.2.2 Pour l'environnement de production BrandShelter secure.brandshelter.com

- **URL de connexion unique (Single Sign On URL) :** https://bs-live-auth.auth.eu-central-1.amazoncognito.com/saml2/idpresponse
- **Restriction d'audience :** urn:amazon:cognito:sp:eu-central-1_FmcrLjcuB
- **Relay State par défaut :** laisser vide
- Dans **Security/API/Trusted Origins**, ajoutez https://bs-live-auth.auth.eu-central-1.amazoncognito.com comme redirection autorisée (« redirect »)

4.3 Okta (OpenID Connect)

4.3.1 Pour l'environnement de démonstration BrandShelter demo.brandshelter.com

- **URL de connexion unique (Single Sign On URL) :** https://bs-ote-auth.auth.eu-central-1.amazoncognito.com/oauth2/idpresponse
- Dans **Security/API/Trusted Origins**, ajoutez https://bs-ote-auth.auth.eu-central-1.amazoncognito.com comme redirection autorisée (« redirect »)

4.3.2 Pour l'environnement de production BrandShelter secure.brandshelter.com

- **URL de connexion unique (Single Sign On URL) :** https://bs-live-auth.auth.eu-central-1.amazoncognito.com/oauth2/idpresponse
- Dans **Security/API/Trusted Origins**, ajoutez https://bs-live-auth.auth.eu-central-1.amazoncognito.com comme redirection autorisée (« redirect »)

4.4 Mappage des attributs

- Par défaut, nous traitons les assertions suivantes pour l'intégration des utilisateurs :

Pour SAML:

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

NB : Il s'agit d'identificateurs de nom fixes. Ces URI utilisent exclusivement le schéma HTTP, et non HTTPS ! La saisie d'URI HTTPS ici entraînera des revendications ou claims vides.

Champs et attributs OIDC :

- Scope « profile » pour given_name et family_name
- Scope « email » pour email
- Scope « phone » pour phone_number

Nous utilisons le format de nom « URI Reference » ; nous attribuons user.email aux attributs « name » et « emailaddress », mais d'autres mappages sont également possibles.

Exemple :

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

D'autres attributs peuvent être mappés sur demande.

Avertissement

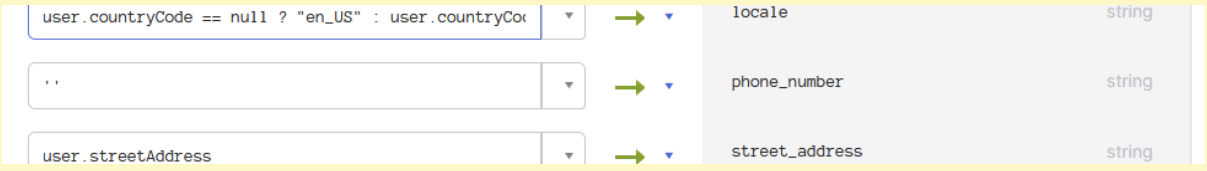
IMPORTANT :
Les attributs ci-dessus sont obligatoires, et nous ne pouvons pas modifier ces exigences sans recréer le pool d'utilisateurs, ce qui casserait toutes les fédérations existantes.

De plus, Cognito exige que les numéros de téléphone soient fournis dans un format très précis :

« Les numéros de téléphone doivent respecter les règles de format suivantes : un numéro de téléphone doit commencer par un signe plus (+), immédiatement

suivi de l'indicatif pays. Un numéro de téléphone ne peut contenir que le signe + et des chiffres. Supprimez tout autre caractère du numéro de téléphone, tels que parenthèses, espaces ou tirets (-), avant de soumettre la valeur au service. Par exemple, un numéro de téléphone basé aux États-Unis doit suivre ce format : +14325551212. »

Si vous n'êtes pas en mesure de fournir ce format, nous vous conseillons de mapper un attribut vide afin que les utilisateurs puissent saisir ces informations lors du processus d'intégration. Par exemple, dans Okta, un administrateur peut simplement mapper la chaîne vide à l'attribut / fonction phone_number pour son application BrandShelter :



4.5 Fournir les données de fédération à BrandShelter

Vous devez nous fournir une URL de métadonnées ou un document (fichier XML), ainsi que les domaines de messagerie utilisés par vos utilisateurs pour la connexion.

Et préciser le protocole utilisé pour la fédération SSO, c'est-à-dire SAML ou OIDC.

IMPORTANT : Vous pouvez choisir entre 2 configurations possibles pour l'accès au portail BrandShelter après l'activation de la SSO.

1) Configuration par défaut 1 – BrandShelter + connexion SSO

Les deux méthodes de connexion coexistent, connexion directe et SSO :

- vous pouvez vous connecter en utilisant la connexion directe BrandShelter (nom d'utilisateur + mot de passe)

- et.ou en utilisant la connexion SSO, qui nécessite uniquement de saisir votre adresse e-mail (ou nom d'utilisateur SSO) dans le champ « Nom d'utilisateur », puis de cliquer sur « Connexion » sans entrer de mot de passe pour être redirigé vers le formulaire SSO.

Cette configuration est conçue pour permettre l'ajout et la connexion des utilisateurs qui ne disposent pas d'une adresse e-mail liée au SSO et qui auraient donc besoin d'un accès direct au portail pour accéder à votre compte.

2) Configuration 2 à activer sur demande – Connexion unique (SSO)

Nous désactivons la connexion directe BrandShelter (nom d'utilisateur + mot de passe) et seule la méthode SSO est possible.

Cela rend la connexion SSO obligatoire et incontournable pour se connecter, pour tous les utilisateurs du compte sans exception.

Note 1 : Chaque utilisateur dont le nom d'utilisateur correspond à l'un de ces domaines de messagerie devra s'authentifier via le Single Sign-On (SSO) (configuration 2). Tout utilisateur de ce compte dont le nom d'utilisateur ne correspond pas à l'un de ces domaines devra utiliser ses identifiants locaux habituels et n'utilisera pas le SSO (configuration par défaut 1). Par exemple, le domaine *example.com* correspondra aux noms d'utilisateur comme nom@example.com.

Note 2 : Veuillez noter que BrandShelter ne supporte pas la connexion initiée par le fournisseur d'identité (IdP-initiated sign-in). Cela signifie que certaines fonctionnalités, comme le « lien intégré » fourni par Okta, ne peuvent pas être utilisées pour la connexion, ni via d'autres plateformes d'authentification, par

exemple le portail « Mes Applications » d'Azure. Toutes les connexions doivent être initiées via le portail BrandShelter pour garantir une authentification et un accès corrects.

Merci de vous assurer que les utilisateurs initient toujours leur connexion sur notre portail.

Note 3 : Un nouvel utilisateur sera toujours redirigé vers la page de création de compte BrandShelter pour remplir toutes les informations non fournies par leur IdP. De plus, il est important de noter qu'un utilisateur existant du portail sera redirigé vers la page de création de compte BrandShelter pour compléter et/ou mettre à jour toutes les informations non fournies par leur IdP.

Expérience utilisateur après activation du SSO :

Un utilisateur visite le portail BrandShelter. S'il est déjà authentifié auprès de son fournisseur d'identité d'entreprise, il est immédiatement connecté à BrandShelter et le processus s'arrête là.

S'il n'est pas encore authentifié, l'utilisateur saisit son nom de connexion dans le formulaire de connexion BrandShelter.
L'utilisateur est alors redirigé vers le formulaire de connexion de son entreprise, par exemple le formulaire de connexion Microsoft. Après avoir saisi ses identifiants, l'utilisateur est redirigé vers le portail BrandShelter où il est connecté.

Lien d'informations supplémentaires :

FAQ Amazon Cognito

À la fin de la configuration, vous devriez disposer de l'URL des métadonnées de fédération. BrandShelter a besoin de cette URL pour finaliser la configuration de son côté. Une fois cela fait, la fédération peut être testée.

4.6 Erreurs courantes

4.6.1 « Required String parameter 'RelayState' is not present » sur la page hébergée par Cognito

Patientez quelques minutes après avoir saisi les informations. Nous avons réussi à reproduire l'erreur en modifiant l'application dans Azure Active Directory (AAD) et en lançant immédiatement une connexion, mais nous n'avons pas pu reproduire de façon fiable et systématique.

4.6.2 « An error was encountered with the requested page. » (aucune information supplémentaire) sur la page hébergée par Cognito

Cela peut se produire lorsque vous tentez d'utiliser la connexion initiée par l'IdP, par exemple via le bouton « Tester la connexion » dans le portail Azure ou le portail « Mon application ». BrandShelter ne prend pas en charge cela pour le moment, mais nous y travaillons.

Pour l'instant, assurez-vous de lancer la connexion via le portail BrandShelter et depuis l'URL de connexion renseignée dans votre configuration SSO, comme indiqué dans le préambule en haut de page, pour que l'IdP redirige les utilisateurs vers notre portail.

4.6.3 « Invalid relayState from identity provider » ou « Invalid samlResponse or relayState from identity provider » sur la page hébergée par Cognito

Ceci est une autre conséquence de la connexion initiée par le fournisseur d'identité (IdP), observée lors de la tentative d'utilisation du lien intégré (Embed Link) d'Okta.

4.6.4 « Invalid saml response received: client is not enabled for oauth2.0 flows » sur la page de connexion hébergée par BrandShelter

Cela indique que l'URL de réponse est incorrecte. Assurez-vous d'utiliser les URL indiquées en haut de la page.

Cela peut également être dû au fait que le client Cognito n'a pas l'indicateur **AllowedOAuthFlowsUserPoolClient** dans le client d'application, ce qui était un problème dans les anciennes versions des scripts d'installation automatique. Pour résoudre ce problème, un développeur peut simplement entrer dans la page d'édition du client de l'application et l'enregistrer sans modification.

4.6.5 « Could not authenticate you from OpenIDConnect because "invalid 'state' parameter » sur la page de connexion hébergée par BrandShelter

Assurez-vous que l'utilisateur initie bien la connexion depuis le même hôte vers lequel il sera finalement transféré (et renseigné dans votre configuration SSO). Un utilisateur associé à une configuration SSO utilisant, par exemple, home.safebrands.com ne peut pas initier la connexion depuis secure.brandshelter.com. Nous travaillons pour que cela n'ait plus d'impact et que la connexion puisse être initiée depuis les 2 URL.

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

Assurez-vous que l'utilisateur concerné est bien affecté au groupe approprié pour le client d'application dans Cognito.

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

Reportez-vous à l'avertissement surligné en jaune plus haut sur cette page et vérifiez votre configuration SSO : ce message indique une erreur dans le mappage des attributs de votre configuration SSO, spécifiquement sur le format du numéro de téléphone.