BrandShelter

Guide zur Implementierung von Single Sign-On (SSO)

Einführung in SSO und Guide für Microsoft Azure Active Directory

Juni 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

Inhaltsverzeichnis

BrandShelter

Einführung in Single Sign-On (SSO)

1.1 Was ist Single Sign-On?

Single Sign-On (SSO) ermöglicht es Benutzern, sich mit nur einem Satz von Anmeldedaten bei mehreren unabhängigen Systemen anzumelden. Mit SSO müssen sich Benutzer nicht mehr separat bei jeder einzelnen Anwendung anmelden oder für jede Anwendung unterschiedliche Zugangsdaten verwalten. Sie geben ihre Anmeldedaten einmal auf einer zentralen Seite ein und erhalten Zugriff auf alle verbundenen Anwendungen.

BrandShelter bietet Unterstützung für die Integration mit anderen Identitätsanbietern über **SAML** und **OpenID Connect**. Dabei handelt es sich um zwei weit verbreitete Standards für den sicheren Austausch von Authentifizierungs- und Autorisierungsinformationen.

1.2 Wann ist SSO eine gute Lösung für mein Unternehmen?

SSO kann eine gute Lösung für Ihr Unternehmen sein, wenn:

- **Erhöhte Sicherheit:** Sie nach einer besonders sicheren Möglichkeit suchen, sich bei BrandShelter anzumelden, bei der Mitarbeiter die etablierten Authentifizierungsprotokolle Ihres Unternehmens verwenden müssen.
- **Vereinfachtes Benutzer-management:** Sie sicherstellen möchten, dass der Zugriff eines Benutzers auf das BrandShelter-Dashboard endet, sobald dieser das Unternehmen verlässt und keinen Zugang mehr zu den Unternehmenssystemen hat.
- **Verbesserte Benutzererfahrung:** Sie den Anmeldeprozess für Benutzer vereinfachen möchten, indem sich diese nur einmal authentifizieren müssen und nicht mehrere Zugangsdaten verwalten müssen.

1.3 Wie funktioniert SSO?

Die SSO-Funktion von BrandShelter nutzt Amazon Cognito als Identitätsanbieter. Externe Identitätsanbieter werden über SAML oder OpenID Connect mit Cognito verbunden. Abhängig von der Cognito-Benutzergruppe und den Ansprüchen (Claims) werden zusammenhängende Benutzer BrandShelter-Konten mit den jeweiligen Berechtigungen zugewiesen. Dies ermöglicht eine nahtlose und sichere Anmeldung für Benutzer und bietet gleichzeitig eine zentrale Verwaltung der Zugriffskontrolle.

Der SSO-Identitätsanbieter für BrandShelter ist AWS Cognito.

Checkliste zur Vorbereitung einer erfolgreichen SSO-Implementierung

WICHTIG: Administrator(en) müssen bestätigen, dass alle Benutzer eine geschäftliche E-Mail-Adresse im Account Center hinterlegt haben. Wenn Benutzer keine geschäftliche E-Mail-Adresse haben, werden sie nach der Aktivierung von SSO ausgesperrt. Die geschäftlichen E-Mail-Adressen müssen mit den IdP-spezifischen E-Mails der Benutzer übereinstimmen.

- **Bestätigen Sie, dass Ihre Organisation einen SAML 2.0-konformen IdP verwendet (z. B. Okta, Azure Active Directory).**
- **Admins identifizieren:** Identifizieren Sie den Account-Center-Administrator für das BrandShelter-Dashboard sowie relevante interne IT-Ansprechpartner. Zur Konfiguration von SSO benötigen Admins sowohl Zugriff auf den IdP als auch auf das BrandShelter-Dashboard:
- **IdP-Zugang:** Wenden Sie sich hierzu an Ihre IT- oder Sicherheitsabteilung (oder wer auch immer Zugriff als IdP-Administrator/-Manager hat) oder an Ihren IdP-Dienstanbieter.

- **Admin-Zugang zum BrandShelter-Dashboard:** Der Admin benötigt eine „Admin Account"-Lizenz, um SSO zu aktivieren. Dies kann auf folgende Weise erfolgen:
- Gewähren Sie die Lizenz Ihrem IdP-Admin oder -Manager im Dashboard.
- Oder übertragen Sie relevante Informationen vom IdP-Admin an einen Dashboard-Admin zur Eingabe im Account Center.

OpenID Connect Integration: BrandShelter integriert sich über OpenID Connect mit Amazon Cognito. Falls die OpenID Connect-Berechtigungen (Scopes) nicht alle erforderlichen Informationen enthalten, werden Benutzer aufgefordert, ein Formular auszufüllen, um fehlende Daten bereitzustellen. Zudem müssen die Nutzer der Datenverarbeitungsvereinbarung zustimmen.

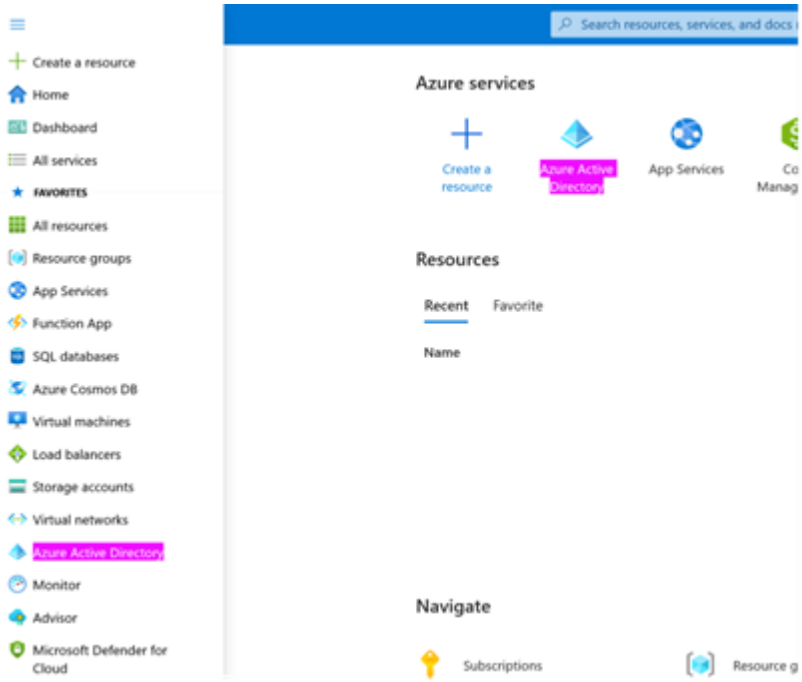
- **Erforderliche Daten:** Fordern Sie folgende Daten vom BrandShelter-Support an:
- Identifier (Entity ID)
- Reply URL

Kommunikation: Admins sollten die Teams über die bevorstehenden Änderungen beim BrandShelter-Login informieren. Nutzen Sie die Mustervorlage für E-Mails als Orientierung.

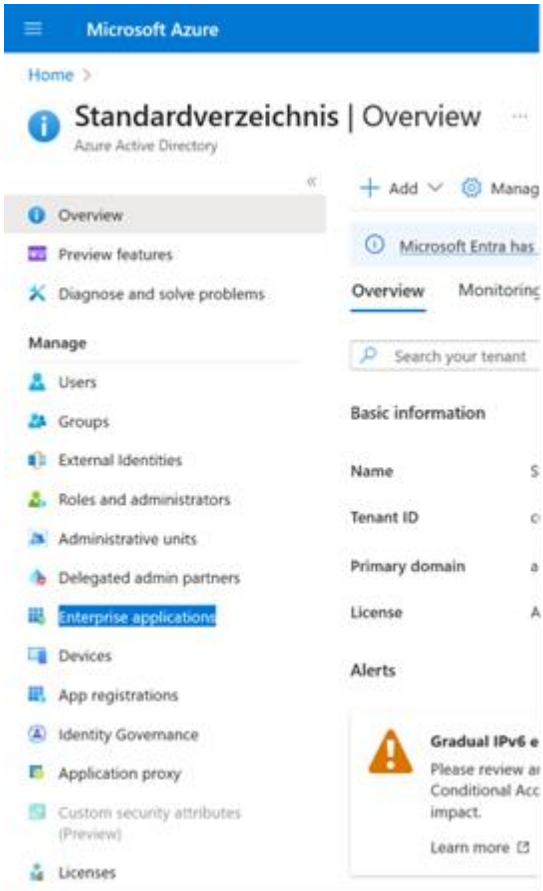
Schritte zur Aktivierung von SSO für Microsoft Azure Active Directory

1.4 Erstellen Sie eine Azure AD Unternehmensanwendung

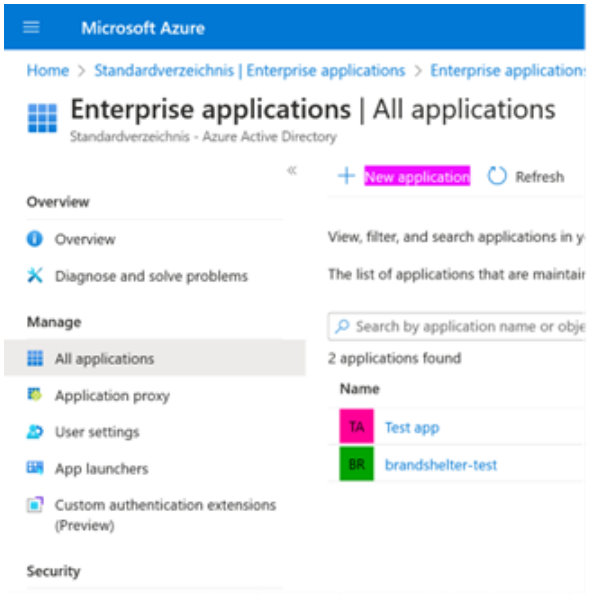
- Öffnen Sie das Microsoft Azure-Portal unter https://portal.azure.com
- Wählen Sie in der linken Navigationsleiste **„Azure Active Directory“** aus. Falls der Dienst dort nicht aufgeführt ist, wählen Sie **„Alle Dienste/All Services“** und geben Sie **„Azure Active Directory“** in die Suchleiste ein, um den Eintrag zu finden.



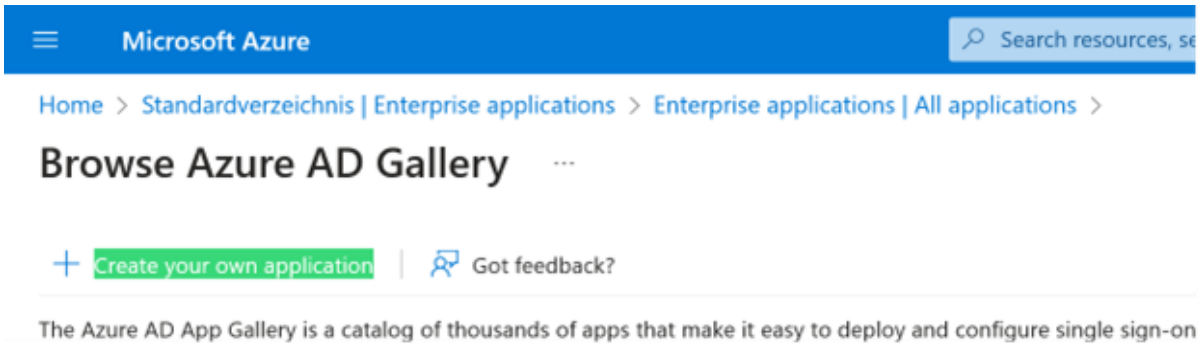
- Wählen Sie in der linken Navigation „Unternehmensanwendung“ oder “Enterprise Applications” aus



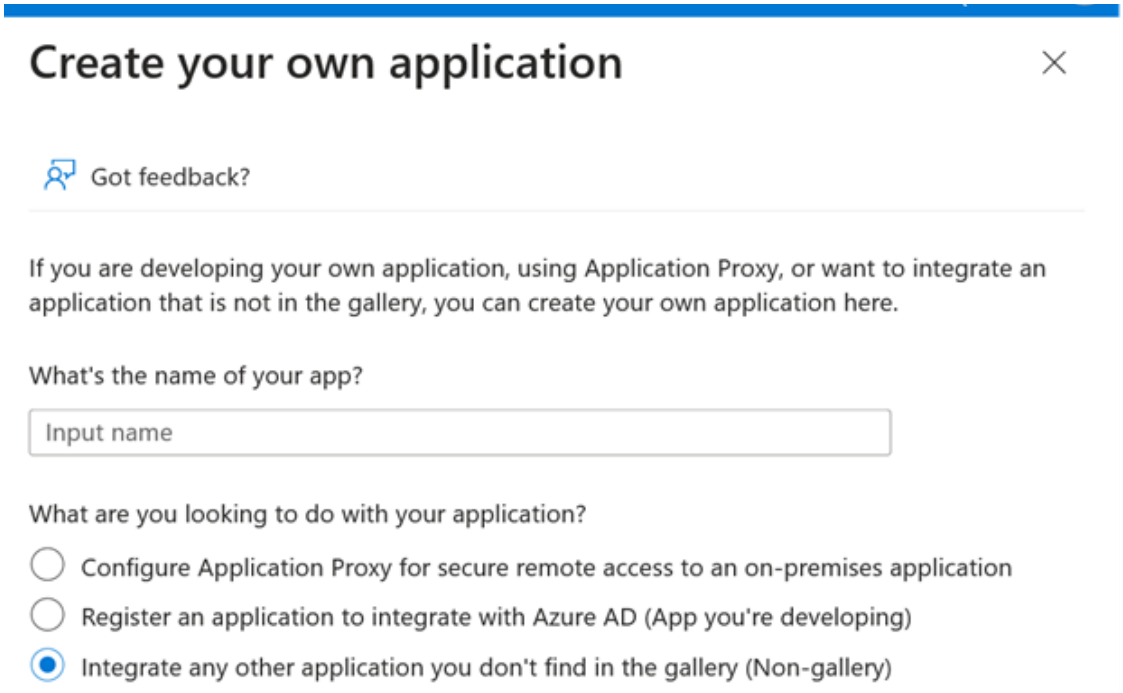
- Klicken Sie im Aktionsmenü oben auf „Neue Anwendung/New Application“



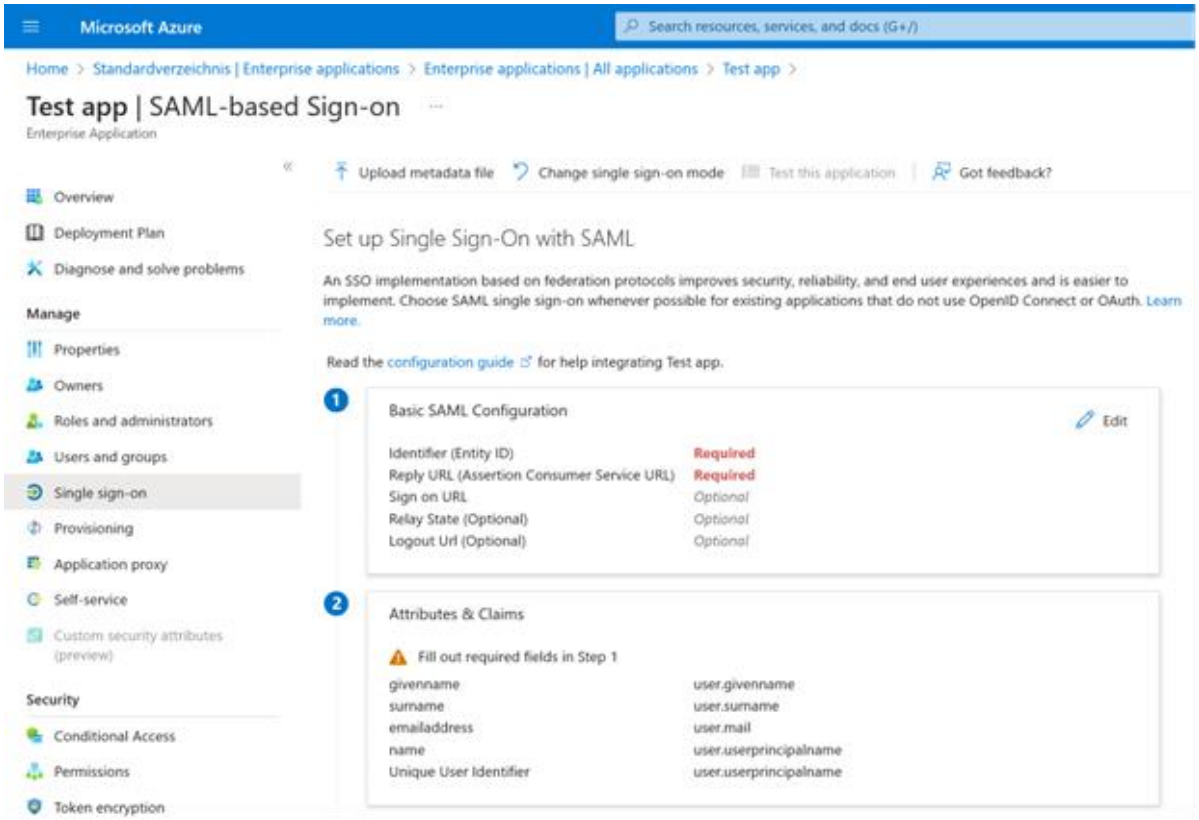
- Wählen Sie im Aktionsmenü oben „Eigene Anwendung erstellen/Create your own application“ aus



- Geben Sie einen Namen für Ihre Anwendung ein.
- Wählen Sie „Integration einer anderen Anwendung, die Sie nicht in der Galerie finden (Nicht-Galerie)/Integrate any other application you don’t find in the gallery (Non-gallery) “ aus.



- Sie sollten sich nun auf der Übersichtsseite Ihrer neu erstellten Anwendung befinden. Wählen Sie in der linken Navigation **„Single Sign-On“** aus.
- Wählen Sie anschließend **„SAML“**.

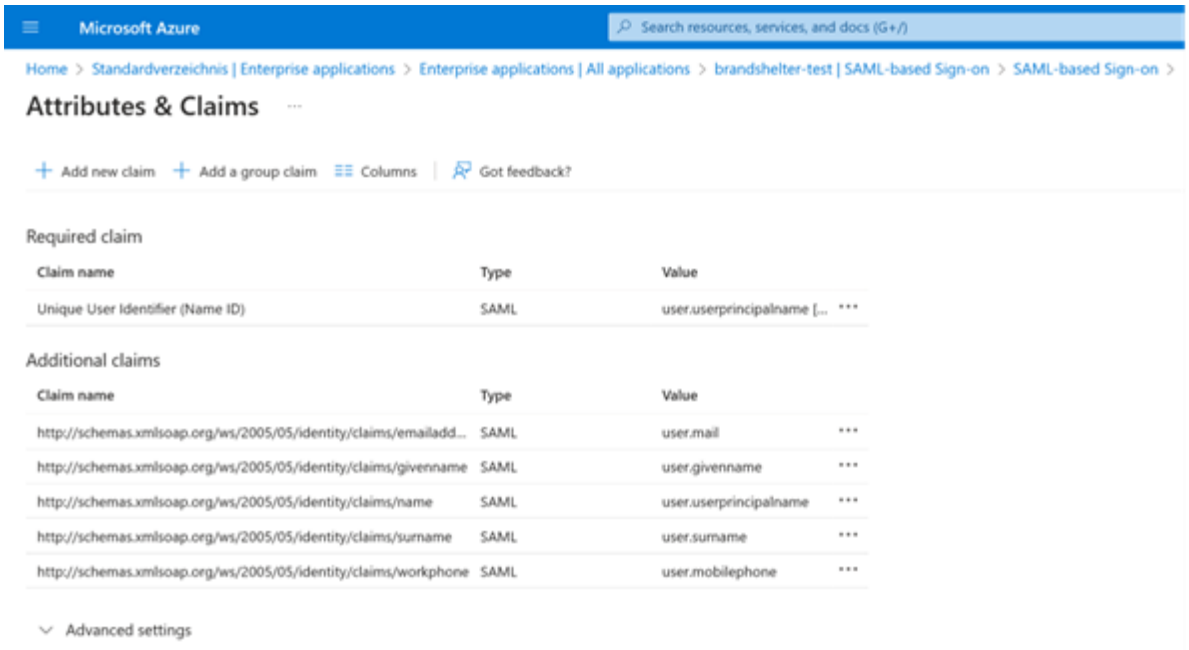


Im Abschnitt **„Basic SAML-Konfiguration“**

- Klicken Sie auf **„Bearbeiten/Edit“**
- Geben Sie die **„Identifier (Entity ID)“** ein, die Sie von BrandShelter erhalten haben.
- Geben Sie die **„Antwort-URL (Reply URL / Assertion Consumer Service URL)“** ein, die Sie von BrandShelter erhalten haben.

Im Abschnitt **„Attribute & Ansprüche/Attributes & Claims“**

- Klicken Sie auf **„Bearbeiten/Edit“**
- Klicken Sie auf **„Neuen Anspruch hinzufügen/Add a new claim“**
- Geben Sie **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/workphone** als **„Name“** ein
- Wählen Sie **„user.mobilephone“** als **„Source attribute“** aus
- Klicken Sie auf **„Speichern/Save“**



Im Abschnitt **„SAML-Zertifikate/SAML Certificates“**

- Kopieren Sie die **„App Federation Metadata URL“** und stellen Sie diese URL BrandShelter zur Verfügung
- Wählen Sie in der linken Navigation **„Benutzer und Gruppen/Users and groups“** aus
- Fügen Sie Benutzer und Gruppen nach Bedarf hinzu.

- **Bereitstellung der Federation-Metadaten an BrandShelter:** Am Ende der Einrichtung sollten Sie die Federation-Metadaten-URL haben. BrandShelter benötigt diese URL, um die Einrichtung auf unserer Seite abzuschließen. Sobald dies erfolgt ist, kann die Federation getestet werden.

Einrichtung von SSO

Um Single Sign-On (SSO) zwischen Ihrem Identitätsanbieter (z. B. Microsoft Entra ID [früher Azure Active Directory] oder Okta) und BrandShelter zu integrieren, unterstützen wir eine standardisierte SSO-Federation. Bitte beachten Sie die folgenden wichtigen Punkte:

- **Anmeldeablauf:** BrandShelter unterstützt derzeit nur die *vom Dienstanbieter initiierte Anmeldung*. Das bedeutet, dass Benutzer den Anmeldevorgang über das BrandShelter-Portal starten müssen. Funktionen wie der „Embed-Link" von Okta für eine vom IdP initiierte Anmeldung werden nicht unterstützt.

- **Voraussetzungen für die Einrichtung:** Sie müssen Ihre IdP-Metadaten bereitstellen (entweder als URL oder als XML-Datei). Teilen Sie uns zudem die E-Mail-Domains mit, die Ihre Benutzer für die Anmeldung verwenden werden.

- **Unterstützung bei der Konfiguration:** Wir stellen die notwendigen Konfigurationsdetails und Attributzuordnungen zur Verfügung, um Sie bei der Einrichtung in Ihrem IdP zu unterstützen.

1.5 Erforderliche Einrichtung beim IdP

1.5.1 **Microsoft Entra ID (früher Azure AD)**

Die folgenden Daten müssen in Azure AD konfiguriert werden:

- **Identifier (Client ID) (erforderlich)**
- **Reply URL (erforderlich)**
- **Sign on URL (erforderlich)**
- **Relay Status (optional)**

1.5.2 Für die BrandShelter-Demoumgebung demo.brandshelter.com

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

Reply URL: https://bs-ote-auth.auth.eu-central-1.amazoncognito.com/saml2/idpresponse

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

Relay Status (Optional): https://demo.brandshelter.com/

1.5.3 Für die BrandShelter-Produktionsumgebung secure.brandshelter.com

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

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

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

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

1.6 Okta (SAML)

1.6.1 Für die BrandShelter-Demoumgebung demo.brandshelter.com

- Single Sign On URL: https://bs-ote-auth.auth.eu-central-1.amazoncognito.com/saml2/idpresponse
- Audience-Einschränkung: urn:amazon:cognito:sp:eu-central-1_ieAQ8aVrs
- Default Relay State: bitte leer lassen
- Fügen Sie bei Security/API/Trusted Origins https://bs-ote-auth.auth.eu-central-1.amazoncognito.com als erlaubte „Redirect"-URL hinzu.

1.6.2 Für die BrandShelter-Produktionsumgebung secure.brandshelter.com

- Single Sign On-URL: https://bs-live-auth.auth.eu-central-1.amazoncognito.com/saml2/idpresponse
- Audience-Einschränkung: urn:amazon:cognito:sp:eu-central-1_FmcrLjcuB
- Default Relay State: bitte leer lassen
- In Security/API/Trusted Origins, https://bs-live-auth.auth.eu-central-1.amazoncognito.com als erlaubte „Redirect"-URL hinzufügen.

1.7 Okta (OpenID Connect)

1.7.1 Für die BrandShelter-Demoumgebung demo.brandshelter.com

- Single Sign On URL: https://bs-ote-auth.auth.eu-central-1.amazoncognito.com/oauth2/idpresponse

- In Security/API/Trusted Origins, https://bs-ote-auth.auth.eu-central-1.amazoncognito.com als erlaubte „Redirect"-URL hinzufügen.

1.7.2 Für die BrandShelter-Produktionsumgebung secure.brandshelter.com

- Single Sign On-URL: https://bs-live-auth.auth.eu-central-1.amazoncognito.com/oauth2/idpresponse
- In Security/API/Trusted Origins, https://bs-live-auth.auth.eu-central-1.amazoncognito.com als erlaubte „Redirect"-URL hinzufügen.

1.8 Attributzuordnung

- Standardmäßig verarbeiten wir die folgenden Assertions zum Onboarding von Nutzern:

Für 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

Scopes und Attribute OIDC:

- Der „profile"-Scope für given_name und family_name
- Der „email"-Scope für email
- Der „phone"-Scope für phone_number

Wir verwenden das Namensformat „URI Reference“ und weisen user.email sowohl dem Attribut „name“ als auch „emailaddress“ zu, aber auch andere Zuordnungen sind möglich.

Beispiel:

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

Andere Attribute können auf Anfrage hin zugeordnet werden.

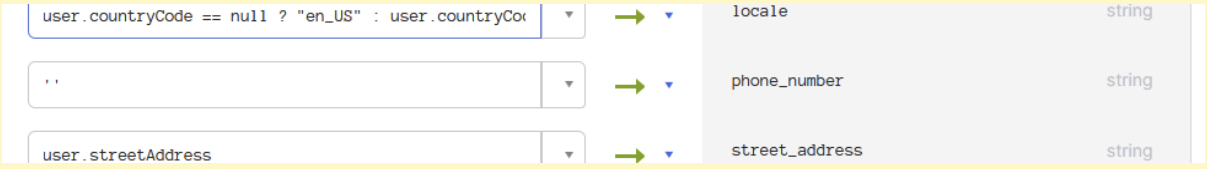
Die oben genannten Attribute sind erforderlich, und wir können diese Anforderungen nicht ändern, ohne den User Pool neu zu erstellen und alle bestehenden Federations-Verbindungen zu unterbrechen.

Zusätzlich verlangt Cognito, dass Telefonnummern in einem sehr spezifischen Format angegeben werden:

„Telefonnummern müssen folgende Formatregeln erfüllen: Eine Telefonnummer muss mit einem Pluszeichen (+) beginnen, unmittelbar gefolgt vom Ländercode.

Eine Telefonnummer darf nur das Pluszeichen (+) und Ziffern enthalten. Entfernen Sie vor dem Übermitteln an den Dienst alle anderen Zeichen wie Klammern, Leerzeichen oder Bindestriche (-). Zum Beispiel muss eine Telefonnummer aus den USA folgendes Format haben: +14325551212."

Wenn ein Client dieses Format nicht bereitstellen kann, empfehlen wir, ein leeres Attribut zuzuordnen, damit die Benutzer diese Information während des Onboarding-Prozesses eingeben können. Beispielsweise kann in Okta ein Administrator einfach den leeren String dem Attribut phone_number für die BrandShelter-Anwendung zuweisen:



1.9 Federationsdaten an BrandShelter bereitstellen

Sie müssen uns eine Metadaten-URL oder ein Metadaten-Dokument (XML-Datei) sowie die von den Benutzern für die Anmeldung verwendeten Mail-Domains bereitstellen.

Außerdem geben Sie bitte das für die SSO-Federation verwendete Protokoll an, also SAML oder OIDC.

WICHTIG: Sie können zwischen zwei möglichen Konfigurationen für den Zugriff auf das BrandShelter-Portal nach der SSO-Aktivierung wählen.

- **Standardkonfiguration 1 – BrandShelter + SSO-Verbindung**

Die beiden Verbindungsarten koexistieren, Direktverbindung und SSO:

- Sie können sich mit dem direkten BrandShelter-Login (Benutzername + Passwort) anmelden

- Oder Sie verwenden die SSO-Anmeldung, bei der Sie nur Ihre E-Mail-Adresse (oder SSO-Benutzername) im Feld „Benutzername“ eingeben und dann auf „Login“ klicken, ohne ein Passwort einzugeben. Dadurch werden Sie zum SSO-Formular weitergeleitet.

Diese Konfiguration ermöglicht die Anmeldung und Hinzufügung von Benutzern, die keine mit SSO verknüpfte E-Mail-Adresse haben und daher eine direkte Verbindung zum Portal benötigen, um auf Ihr Konto zuzugreifen.

- **Konfiguration 2 – auf Anfrage aktivierbar – SSO Single Sign-On**

Die direkte BrandShelter-Verbindung (Benutzername + Passwort) wird deaktiviert und nur die SSO-Methode ist möglich.

Dies macht die SSO-Verbindung für alle Benutzer des Kontos ohne Ausnahme verpflichtend und unvermeidbar.

Hinweis 1: Jeder Benutzer mit einem Benutzernamen, der mit einer der angegebenen Domains übereinstimmt, muss sich über Single Sign-On (SSO) authentifizieren (Konfiguration 2). Jeder Benutzer dieses Kontos mit einem Benutzernamen, der nicht mit einer dieser Domains übereinstimmt, benötigt seine normalen lokalen Anmeldeinformationen und verwendet nicht SSO (Standardkonfiguration 1). Beispiel: Der Hostname example.com stimmt mit Benutzernamen wie name@example.com überein.

Hinweis 2: Bitte beachten Sie, dass BrandShelter keinen IdP-initiierten Login unterstützt. Das bedeutet, dass bestimmte Funktionen, wie der von Okta bereitgestellte „Embed Link“, nicht für Anmeldezwecke verwendet werden können, ebenso wenig wie andere Authentifizierungsplattformen, z. B. das „My Applications“-Portal von Azure. Alle Anmeldungen müssen über das BrandShelter-Portal initiiert werden, um eine korrekte Authentifizierung und den Zugriff zu gewährleisten.

Bitte stellen Sie sicher, dass die Benutzer ihre Anmeldung immer auf unserem Portal starten.

Hinweis 3: Ein neuer Benutzer wird weiterhin zur Kontoerstellungsseite von BrandShelter weitergeleitet, um alle Informationen auszufüllen, die nicht von seinem IdP bereitgestellt werden. Außerdem ist es wichtig zu beachten, dass ein bestehender Portalbenutzer zur Kontoerstellungsseite von BrandShelter weitergeleitet wird, um alle Informationen, die nicht vom IdP bereitgestellt wurden, auszufüllen und/oder zu aktualisieren.

Benutzererlebnis nach der SSO-Aktivierung:

Ein Benutzer besucht das BrandShelter-Portal. Wenn er bereits mit seinem unternehmensweiten Identitätsanbieter authentifiziert ist, wird er sofort bei BrandShelter angemeldet und der Prozess endet hier.

Ist er noch nicht authentifiziert, gibt der Benutzer seinen Benutzernamen im BrandShelter-Anmeldeformular ein.

Der Benutzer wird zum Anmeldeformular seines Unternehmens weitergeleitet, zum Beispiel zum Microsoft-Anmeldeformular. Nach Eingabe seiner Zugangsdaten wird der Benutzer zurück zum BrandShelter-Portal geleitet und dort angemeldet.

Link für weitere Informationen: **Amazon Cognito FAQs**

Am Ende der Einrichtung sollten Sie die Federation-Metadaten-URL vorliegen haben. BrandShelter benötigt diese URL, um die Einrichtung auf ihrer Seite abzuschließen. Sobald dies erledigt ist, kann die Federation getestet werden.

1.10 Häufige Fehler

1.10.1 „Erforderlicher String-Parameter 'RelayState' fehlt“ auf der von Cognito gehosteten Seite

Warten Sie nach der Eingabe der Informationen ein paar Minuten. Wir konnten den Fehler reproduzieren, indem wir die Anwendung in AAD geändert und sofort eine Anmeldung initiiert haben, jedoch war die Reproduktion nicht zuverlässig.

1.10.2 „Bei der angeforderten Seite ist ein Fehler aufgetreten.“ (keine weiteren Informationen) auf der von Cognito gehosteten Seite

Dies kann auftreten, wenn versucht wird, einen IdP-initiierten Login zu verwenden, z. B. über die Schaltfläche „Testanmeldung“ im Azure-Portal oder das „My Applications“-Portal. BrandShelter unterstützt dies derzeit nicht, arbeitet jedoch daran.

Bitte stellen Sie vorerst sicher, dass die Anmeldung über das BrandShelter-Portal initiiert wird oder dass die korrekte Anmelde-URL verwendet wird, wie im einleitenden Text oben auf der Seite angegeben, damit der IdP die Benutzer auf unser Portal weiterleitet.

1.10.3 „Ungültiger RelayState vom Identitätsanbieter“ oder „Ungültige SAMLResponse oder RelayState vom Identitätsanbieter“ auf der von Cognito gehosteten Seite

Dies ist eine weitere Reaktion auf einen IdP-initiierten Login, beobachtet beim Versuch, den Okta Embed Link zu verwenden.

1.10.4 „Ungültige SAML-Antwort erhalten: Client ist nicht für OAuth 2.0-Flows aktiviert“ auf der von BrandShelter gehosteten Login-Seite

Dies weist auf eine falsche Reply-URL hin. Stellen Sie sicher, dass Sie die oben auf der Seite angegebenen URLs verwenden.

Dies kann auch dadurch verursacht werden, dass beim Cognito-Client das Flag **AllowedOAuthFlowsUserPoolClient** im Anwendungsklienten fehlt, was ein Problem bei älteren Versionen der automatisierten Einrichtungsskripte war. Um dies zu beheben, kann ein Entwickler einfach die Bearbeitungsseite des Anwendungsklienten aufrufen und ohne Änderungen speichern.

1.10.5 „Authentifizierung über OpenID Connect nicht möglich wegen ‚ungültigem State-Parameter‘“ auf der von BrandShelter gehosteten Login-Seite

Stellen Sie sicher, dass der Benutzer die Anmeldung auf dem Host startet, zu dem er letztendlich weitergeleitet wird (und der in Ihren SSO-Einstellungen angegeben ist). Ein Benutzer in einem Konto, das z. B. home.safebrands.com verwendet, kann sich nicht bei secure.brandshelter.com anmelden. Wir arbeiten daran, dass dies künftig keine Auswirkungen mehr hat und die Verbindung von beiden URLs aus initiiert werden kann.

1.10.6 „Ihr Single Sign-On-Benutzer <email> ist keinem <brand>-Konto zugewiesen.“

Stellen Sie sicher, dass der betreffende Benutzer der passenden Gruppe für den Anwendungsklienten in Cognito zugewiesen ist.

1.10.7 „Authentifizierung über OpenID Connect nicht möglich wegen ‚Ungültige SAML-Antwort erhalten: ungültiges Telefonnummernformat.'"

Beziehen Sie sich auf die oben auf dieser Seite gelb hervorgehobene Warnung und überprüfen Sie Ihre SSO-Konfiguration: Diese Meldung weist auf einen Fehler in der Attributzuordnung Ihrer SSO-Konfiguration hin, insbesondere beim Format der Telefonnummer.