

BEHEERCONSOLE > INLOGGEN MET SSO >

Microsoft Entra ID SAML- implementatie

Weergeven in het Helpcentrum:

<https://bitwarden.com/help/saml-microsoft-entra-id/>

Microsoft Entra ID SAML-implementatie

Dit artikel bevat **Azure-specifieke** hulp voor het configureren van Login met SSO via SAML 2.0. Raadpleeg [SAML 2.0 Configuratie](#) voor hulp bij het configureren van inloggen met SSO voor een andere IdP.

Bij de configuratie wordt tegelijkertijd gewerkt met de Bitwarden webapp en de Azure Portal. We raden u aan om beide documenten bij de hand te hebben en de stappen uit te voeren in de volgorde waarin ze zijn beschreven.

💡 Tip

Bent u al een SSO-expert? Sla de instructies in dit artikel over en download schermafbeeldingen van voorbeeldconfiguraties om te vergelijken met je eigen configuratie.

📄 type: asset-hyperlink id: 7CKe4TX98FPF86eAimKgak

Open SSO in de webapp

Log in op de Bitwarden web app en open de Admin Console met behulp van de product switcher (🗄️):

<input type="checkbox"/>	All	Name	Owner	
<input type="checkbox"/>		Company Credit Card	My Organiz...	⋮
<input type="checkbox"/>		Company Credit Card Visa, *4242	My Organiz...	⋮
<input type="checkbox"/>		Personal Login	Me	⋮
<input type="checkbox"/>		Personal Login myusername	Me	⋮
<input type="checkbox"/>		Secure Note	Me	⋮
<input type="checkbox"/>		Secure Note	Me	⋮
<input type="checkbox"/>		Shared Login	My Organiz...	⋮
<input type="checkbox"/>		Shared Login sharedusername	My Organiz...	⋮

Product switcher

Open het scherm **Instellingen** → **Enmalige aanmelding** van uw organisatie:

bitwarden Admin Console

- My Organization
- Collections
- Members
- Groups
- Reporting
- Billing
- Settings
- Organization info
- Policies
- Two-step login
- Import data
- Export vault
- Domain verification
- Single sign-on**
- Device approvals
- SCIM provisioning

Single sign-on



Use the [require single sign-on authentication policy](#) to require all members to log in with SSO.

Allow SSO authentication

Once set up, your configuration will be saved and members will be able to authenticate using their Identity Provider credentials.

SSO identifier (required)

Provide this ID to your members to login with SSO. To bypass this step, set up [Domain verification](#)

Member decryption options

Master password

Trusted devices

Once authenticated, members will decrypt vault data using a key stored on their device. The [single organization](#) policy, [SSO required](#) policy, and [account recovery administration](#) policy with automatic enrollment will turn on when this option is used.

Type

SAML service provider configuration

Set a unique SP entity ID

Generate an identifier that is unique to your organization

SP entity ID

SAML 2.0 metadata URL

SAML 2.0 configuratie

Als je dat nog niet hebt gedaan, maak dan een unieke **SSO-identificer** aan voor je organisatie en selecteer **SAML** in het keuzemenu **Type**. Houd dit scherm open voor gemakkelijke referentie.

U kunt de optie **Een unieke SP entiteit ID instellen** in dit stadium uitschakelen als u dat wilt. Als u dit doet, wordt uw organisatie-ID verwijderd uit uw SP entiteit-ID waarde, maar in bijna alle gevallen is het aan te raden om deze optie aan te laten staan.



Tip

Er zijn alternatieve **ontcijferingsopties voor leden**. Leer hoe u aan de slag kunt met [SSO met vertrouwde apparaten](#) of [Key Connector](#).

Een bedrijfsapplicatie maken

Navigeer in de Azure Portal naar **Microsoft Entra ID** en selecteer **Enterprise toepassingen** in het navigatiemenu:

Home >

Default Directory | Overview

Microsoft Entra ID

Overview

Preview features

Diagnose and solve problems

Manage

Users

Groups

External Identities

Roles and administrators

Administrative units

Delegated admin partners

Enterprise applications

Devices

App registrations

Identity Governance

Application proxy

Custom security attributes

+ Add Manage tenants What's new Preview features Got feedback?

Overview Monitoring Properties Recommendations Tutorials

Search your tenant

Basic information

Name		Users
Tenant ID		Groups
Primary domain		Applications
License		Devices

Alerts

Microsoft Entra Connect v1 Retirement
All version 1.x builds of Microsoft Entra Connect (formerly AAD Connect) will soon stop working between October 2023 – March 2024. You must move to Cloud Sync or Microsoft Entra Connect v2.x.
[Learn more](#)

Azure AD is now Microsoft Entra ID
Microsoft Entra ID is the new name for Azure Active Directory. No action is required from you.
[Learn more](#)

Enterprise applications

Selecteer de knop + **Nieuwe toepassing:**

Home > Enterprise applications

Enterprise applications | All applications

Default Directory - Microsoft Entra ID

+ New application Refresh Download (Export) Preview info Columns Preview features Got feedback?

Overview

Overview View, filter, and search applications in your organization that are set up to use your Microsoft Entra tenant as their Identity Provider. The list of applications that are maintained by your organization are in [application registrations](#).

Manage Search by application name or object ID Application type == Enterprise Applications Application ID starts with Add filters

Create new application

Selecteer op het scherm Browse Microsoft Entra ID Gallery de knop + **Maak uw eigen toepassing:**

Home > Default Directory | Enterprise applications > Enterprise applications | All applications >

Browse Microsoft Entra ID Gallery

+ Create your own application Got feedback?

The Microsoft Entra ID App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user provisioning. When deploying an app from the App Gallery, you leverage prebuilt templates to connect your users more securely to their apps. Browse or create your own application here. If you are wanting to publish an application you have developed into the Microsoft Entra ID Gallery for other organizations to discover and use, you can file a request using the process described in [this article](#).

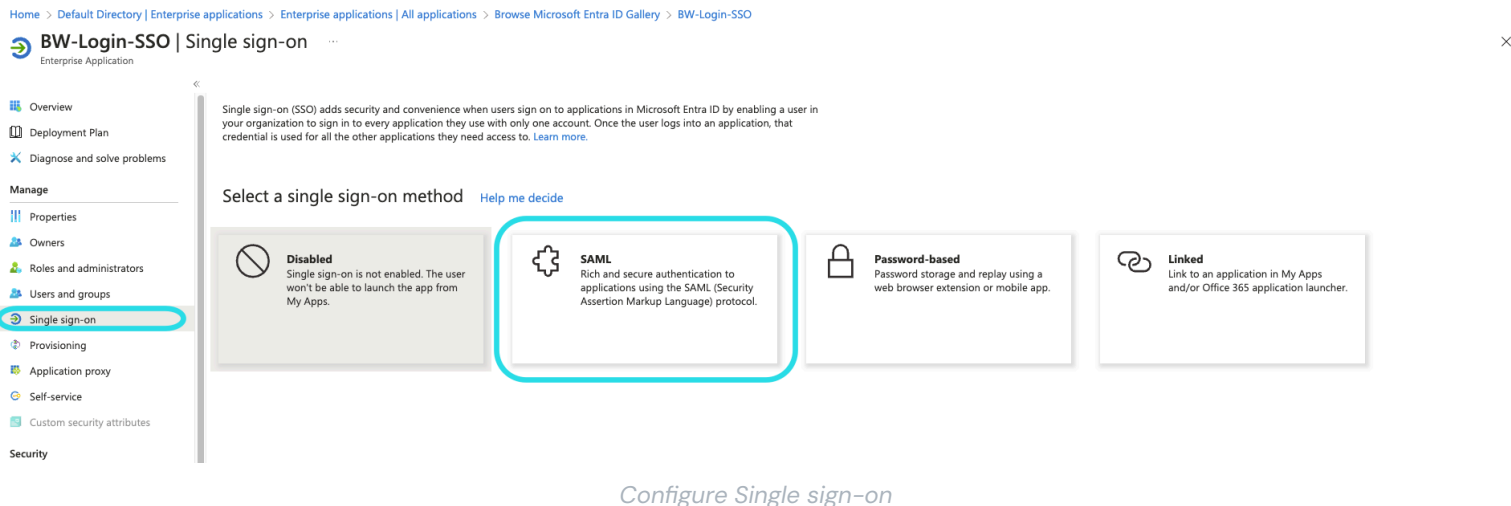
Search application Single Sign-on: All User Account Management: All Categories: All

Create your own application

Geef de applicatie in het scherm Maak uw eigen applicatie een unieke, Bitwarden-specifieke naam en selecteer de optie (Niet-galerij). Klik op de knop **Maken** als je klaar bent.

Eenmalige aanmelding inschakelen

Selecteer **Eenmalige aanmelding** in de navigatie van het scherm Toepassingsoverzicht:



Selecteer **SAML** in het scherm Single Sign-On.

SAML instellen

Basis SAML-configuratie

Selecteer de knop **Bewerken** en configureer de volgende velden:

Veld	Beschrijving
Identificatiecode (entiteits-ID)	<p>Stel dit veld in op de vooraf gegenereerde SP entiteit ID.</p> <p>Deze automatisch gegenereerde waarde kan worden gekopieerd vanuit het Instellingen → Enkelvoudige aanmelding scherm van de organisatie en zal variëren afhankelijk van uw instelling.</p>
Antwoord-URL (Assertion Consumer Service URL)	<p>Stel dit veld in op de vooraf gegenereerde URL van de Assertion Consumer Service (ACS).</p> <p>Deze automatisch gegenereerde waarde kan worden gekopieerd vanuit het Instellingen → Enkelvoudige aanmelding scherm van de organisatie en zal variëren afhankelijk van uw instelling.</p>
Aanmelden URL	<p>Stel dit veld in op de aanmeldings-URL van waaruit gebruikers toegang krijgen tot Bitwarden.</p> <p>Voor cloud-hosted klanten is dit https://vault.bitwarden.com/#/sso of https://vault.bitwarden.eu/#/sso. Voor zelf gehoste instanties wordt dit bepaald door je geconfigureerde server URL, bijvoorbeeld https://your-domain.com/#/sso.</p>

Gebruikersattributen & claims

De standaardclaims die Azure maakt zullen werken met inloggen met SSO, maar je kunt dit gedeelte optioneel gebruiken om de NameID-indeling te configureren die Azure gebruikt in SAML-reacties.

Selecteer de knop **Bewerken** en selecteer het item **Unieke gebruikersidentificatie (Name ID)** om de NameID-claim te bewerken:

Attributes & Claims ...

+ Add new claim + Add a group claim ≡ Columns | 🗨️ Got feedback?

Required claim

Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user.userprincipalname [...]

Additional claims

Claim name	Type	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.surname

▼ Advanced settings

Bewerk NaamID Claim

De opties zijn Standaard, E-mailadres, Persistent, Unspecified en Windows gekwalificeerde domeinnaam. Raadpleeg [de Microsoft Azure documentatie](#) voor meer informatie.

SAML ondertekeningscertificaat

Download het Base64-certificaat voor gebruik [tijdens een latere stap](#).

Uw toepassing instellen

Kopieer of noteer de **aanmeldings-URL** en **Microsoft Entra ID Identifier** in dit gedeelte voor gebruik [tijdens een latere stap](#):

4

Set up BW-Login-SSO

You'll need to configure the application to link with Microsoft Entra ID.

Login URL	<input type="text"/>	
Microsoft Entra ID Identifier	<input type="text"/>	
Logout URL	<input type="text"/>	

Azure URLs

Note

If you receive any key errors when logging in via SSO, try copying the X509 certificate information from the Federation Metadata XML file instead.

Gebruikers en groepen

Selecteer **Gebruikers en groepen** in de navigatie:

The screenshot shows the Microsoft Azure portal interface. At the top, there's a navigation bar with 'Microsoft Azure' and a search bar. Below that, the breadcrumb path is 'Home > Default Directory > Enterprise applications > Bitwarden Login with SSO'. The main heading is 'Bitwarden Login with SSO | Users and groups'. On the left, there's a navigation menu with options like 'Overview', 'Deployment Plan', 'Manage', 'Properties', 'Owners', 'Roles and administrators (Preview)', 'Users and groups' (which is selected), 'Single sign-on', 'Provisioning', 'Application proxy', and 'Self-service'. The main content area shows a toolbar with '+ Add user/group', 'Edit', 'Remove', and 'Update Credentials'. Below the toolbar, there's a message: 'The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this.' A search box contains the text 'First 100 shown, to search all users & groups, enter a display name.' Below the search box is a table with columns 'Display Name', 'Object Type', and 'Role assigned'. The table currently shows 'No application assignments found'.

Assign users or groups

Selecteer de knop **Gebruiker/groep toevoegen** om toegang tot de login met SSO-toepassing toe te wijzen op gebruikers- of groepsniveau.

Terug naar de webapp

Op dit punt heb je alles geconfigureerd wat je nodig hebt binnen de context van de Azure Portal. Ga terug naar de Bitwarden web app om de configuratie te voltooien.

Het Single sign-on scherm verdeelt de configuratie in twee secties:

- De **configuratie van de SAML-serviceprovider** bepaalt het formaat van SAML-verzoeken.
- De **configuratie van de SAML identiteitsprovider** bepaalt het formaat dat wordt verwacht voor SAML antwoorden.

Configuratie serviceprovider

Configureer de volgende velden:

Veld	Beschrijving
Naam ID Formaat	Standaard gebruikt Azure het e-mailadres. Als u deze instelling hebt gewijzigd , selecteert u de overeenkomstige waarde. Stel dit veld anders in op Unspecified of Email Address .
Algoritme voor uitgaande ondertekening	Het algoritme dat Bitwarden gebruikt om SAML-verzoeken te ondertekenen.
Ondertekengedrag	Of/wanneer SAML verzoeken ondertekend zullen worden.
Algoritme voor minimale inkomende ondertekening	Standaard ondertekent Azure met RSA SHA-256. Selecteer rsa-sha256 in de vervolgkeuzelijst.
Ondertekende beweringen	Of Bitwarden verwacht dat SAML-asserties worden ondertekend.
Certificaten valideren	Vink dit vakje aan bij gebruik van vertrouwde en geldige certificaten van je IdP via een vertrouwde CA. Zelfondertekende certificaten kunnen mislukken tenzij de juiste vertrouwensketens zijn geconfigureerd met het Bitwarden login met SSO docker image.

Als je klaar bent met de configuratie van de serviceprovider, sla je je werk **op**.

Configuratie identiteitsprovider

Identity provider configuratie vereist vaak dat je terugkeert naar de Azure Portal om applicatiewaarden op te halen:

Veld	Beschrijving
Entiteit ID	Voer uw Microsoft Entra ID Identifier in, die u hebt opgehaald uit de sectie Uw toepassing instellen van de Azure Portal. Dit veld is hoofdlettergevoelig.
Type binding	Stel in op HTTP POST of Redirect .
URL voor service voor eenmalige aanmelding	Voer uw aanmeldings-URL in, opgehaald uit de sectie Uw toepassing instellen van de Azure Portal.
URL voor service voor eenmalig afmelden	Inloggen met SSO ondersteunt momenteel geen SLO. Deze optie is gepland voor toekomstige ontwikkeling, maar u kunt deze desgewenst vooraf configureren met uw URL voor afmelden .
X509 publiek certificaat	<p>Plak het gedownloade certificaat, verwijder</p> <p>-----BEGIN CERTIFICAAT-----</p> <p>en</p> <p>-----END CERTIFICAAT-----</p> <p>De certificaatwaarde is hoofdlettergevoelig, extra spaties, carriage returns en andere vreemde tekens zorgen ervoor dat de certificaatvalidatie mislukt.</p>
Algoritme voor uitgaande ondertekening	Standaard ondertekent Azure met RSA SHA-256. Selecteer rsa-sha256 in de vervolgkeuzelijst.
Uitgaande afmeldverzoeken uitschakelen	Inloggen met SSO ondersteunt momenteel geen SLO. Deze optie is gepland voor toekomstige ontwikkeling.
Authenticatieverzoeken ondertekend willen hebben	Of Azure verwacht dat SAML verzoeken worden ondertekend.

Note

Let bij het invullen van het X509-certificaat op de vervaldatum. Certificaten zullen vernieuwd moeten worden om onderbrekingen in de dienstverlening aan SSO eindgebruikers te voorkomen. Als een certificaat is verlopen, kunnen de accounts Admin en Eigenaar altijd inloggen met e-mailadres en hoofdwachtwoord.

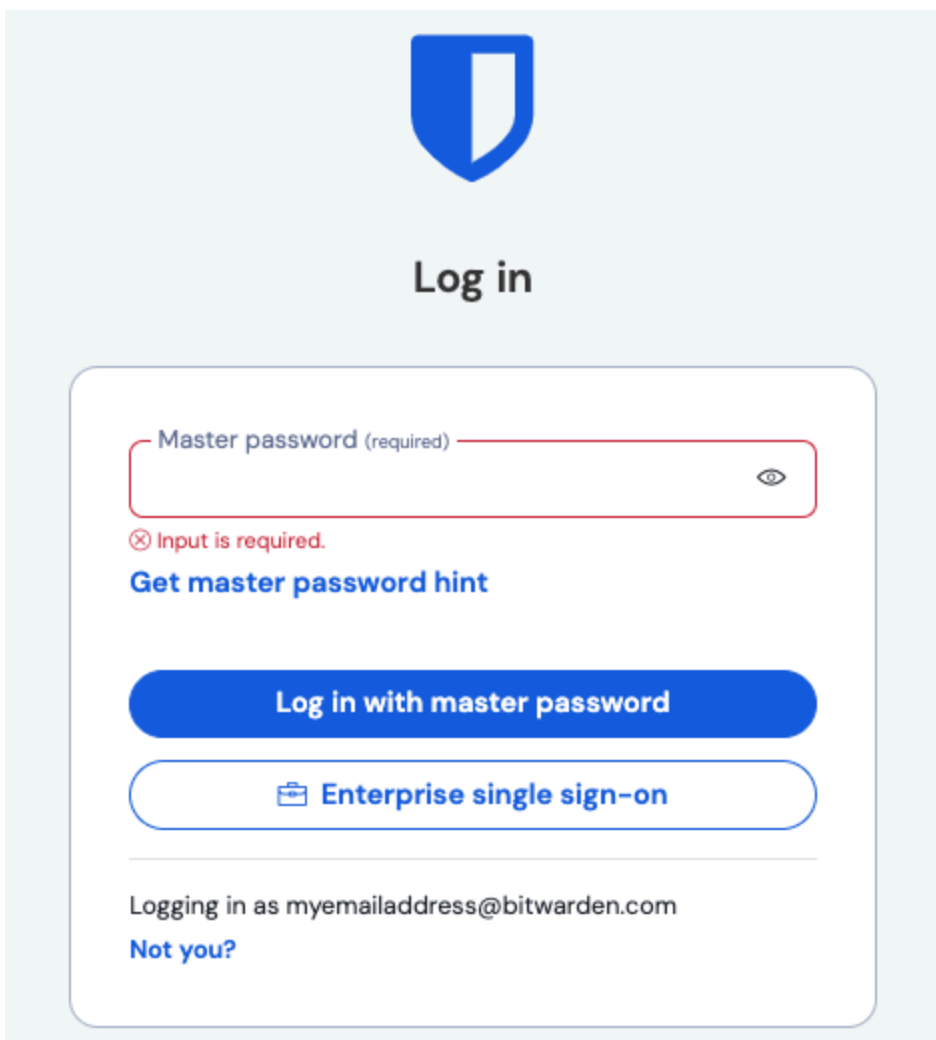
Sla uw werk **op** wanneer u klaar bent met de configuratie van de identity provider.

Tip

Je kunt gebruikers verplichten om in te loggen met SSO door het authenticatiebeleid voor eenmalige aanmelding te activeren. Let op, hiervoor moet ook het beleid voor één organisatie worden geactiveerd. [Meer informatie](#).

De configuratie testen

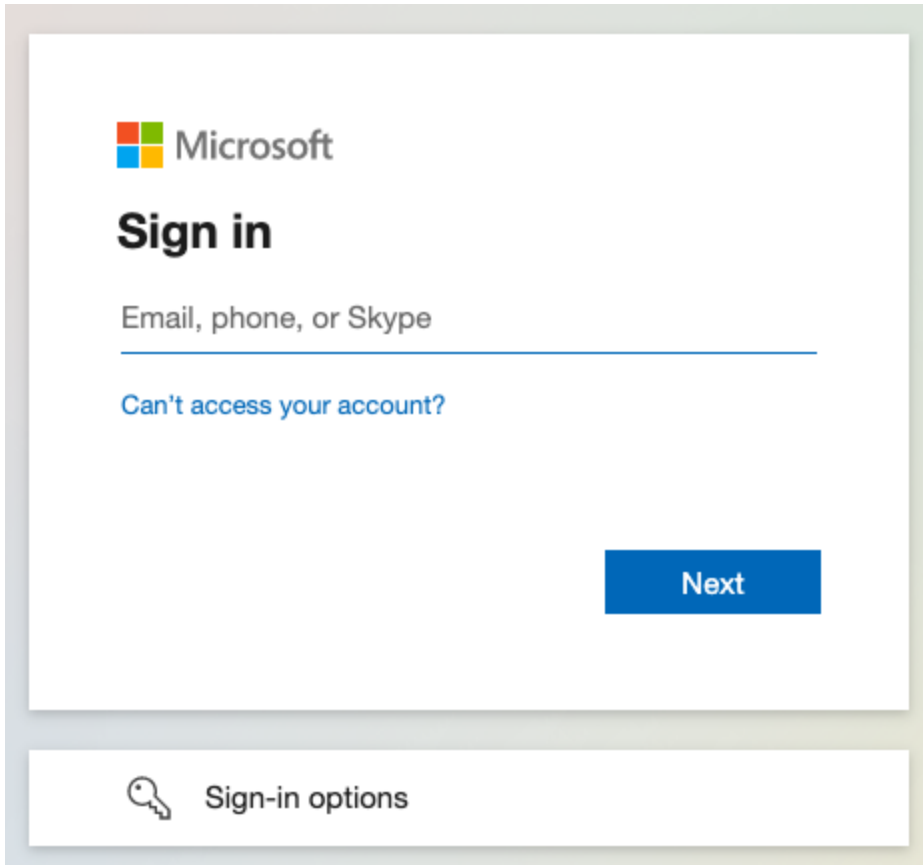
Zodra je configuratie voltooid is, kun je deze testen door te navigeren naar <https://vault.bitwarden.com>, je e-mailadres in te voeren, **Doorgaan** te selecteren en de knop **Enterprise Single-On** te selecteren:



The screenshot shows the Bitwarden login interface. At the top is the Bitwarden logo and the text 'Log in'. Below this is a form with a 'Master password (required)' input field. The field is empty and has a red border, with a red error message 'Input is required.' below it. To the right of the input field is an eye icon. Below the error message is a link 'Get master password hint'. There are two buttons: a blue 'Log in with master password' button and a white 'Enterprise single sign-on' button with a briefcase icon. At the bottom of the form, it says 'Logging in as myemailaddress@bitwarden.com' and a link 'Not you?'.

Enterprise single sign on en hoofdwachtwoord

Voer de [geconfigureerde organisatie-ID](#) in en selecteer **Aanmelden**. Als uw implementatie met succes is geconfigureerd, wordt u doorgestuurd naar het inlogscherf van Microsoft:



The screenshot shows the Microsoft sign-in interface. At the top left is the Microsoft logo. Below it, the text "Sign in" is displayed in a large, bold font. Underneath, there is a text input field with the placeholder text "Email, phone, or Skype". Below the input field is a blue link that says "Can't access your account?". At the bottom right of the main content area is a blue button labeled "Next". At the bottom of the screen, there is a section titled "Sign-in options" with a key icon to its left.

Azure login screen

Nadat u zich hebt geverifieerd met uw Azure-referenties, voert u uw Bitwarden-hoofdwachtwoord in om uw kluis te ontsleutelen!

📌 Note

Bitwarden ondersteunt geen ongevraagde antwoorden, dus inloggen vanuit je IdP zal resulteren in een foutmelding. De SSO-aanmeldingsstroom moet worden geïnitieerd vanuit Bitwarden. Azure SAML-beheerders kunnen een [App-registratie](#) instellen zodat gebruikers worden doorgestuurd naar de inlogpagina voor de Bitwarden-webkuis.

1. Schakel de bestaande Bitwarden-knop uit op de pagina **Alle toepassingen** door te navigeren naar de huidige Bitwarden Enterprise-toepassing en eigenschappen te selecteren en de optie **Zichtbaar voor gebruikers** in te stellen op **Nee**.
2. Maak de App Registratie door te navigeren naar **App Registraties** en **Nieuwe Registratie** te selecteren.
3. Geef een naam op voor de toepassing, zoals **Bitwarden SSO**. Geen omleidings-URL opgeven. Selecteer **Registreren** om het forum te voltooien.
4. Zodra de app is gemaakt, navigeer je naar **Branding & Properties** in het navigatiemenu.
5. Voeg de volgende instellingen toe aan de applicatie:
 1. Upload een logo voor herkenning bij de eindgebruiker. Je kunt het Bitwarden-logo [hier](#) ophalen.
 2. Stel de **URL van de startpagina** in op de inlogpagina van uw Bitwarden-client, zoals <https://vault.bitwarden.com/#/login> of [uw-zelf-gehosteURL.com](#).

Zodra dit proces is voltooid, hebben toegewezen gebruikers een Bitwarden-applicatie die hen rechtstreeks koppelt aan de inlogpagina voor de Bitwarden-webkuis.