

Single Sign On

via Microsoft Entra ID (Azure) en de BHV App van StandBy Solutions

De BHV App van StandBy Solutions heeft ondersteuning voor (interactieve) Single Sign On (SSO) via Microsofts identity platform *Microsoft Entra ID* ([voorheen](#) Azure Active Directory).

Om voor de BHV app en bijbehorende webapplicaties gebruik te maken van SSO via Microsoft zijn er twee hoofdvoorwaarden waaraan moet worden voldaan.

In dit document worden de twee voorwaarden uitgelegd en toegelicht welke stappen u moet nemen om hieraan te voldoen:

Microsoft tenant omgeving	2
Problemen en oplossingen	3
StandBy BHV App omgeving	6
Opvolging	6

Microsoft tenant omgeving

- U dient al in het bezit te zijn van een Microsoft omgeving (Azure/Entra ID)
- Uw medewerkers moeten al zijn opgenomen in deze Microsoft omgeving en **met hun bedrijfsemail adres kunnen inloggen** op Microsoft diensten zoals bijv. Microsoft Outlook voor e-mail.
- De omgeving dient het inloggen (door gebruikers) op externe apps toe te staan:
 - Gebruikers moeten hun account mogen gebruiken om in te loggen op externe apps - zoals 'De BHV App' van StandBy Solutions
 - Indien er gebruik wordt gemaakt van whitelisting van externe apps dient minimaal 'De BHV App' te worden toegestaan:
 - Client ID van 'De BHV App': e238a9ce-375e-430c-b9f1-9cdc1aa50828
 - U dient minimaal 'Cloud Application Administrator' rechten te hebben om apps te mogen installeren binnen de Microsoft omgeving (indien de applicatie expliciet moet worden toegestaan vanwege ingestelde restricties)

U kunt zelf (zonder tussenkomst van uw IT afdeling) controleren of de instellingen al juist staan. Via de volgende pagina kunt u een 'Single Sign On'- test uitvoeren. Indien u een succes melding te zien krijgt, zijn er geen beperkingen op uw Microsoft omgeving ingesteld en kunt u uw Microsoft account gebruiken om in te loggen op de BHV App.

Indien het rode vak (foutmelding zichtbaar is), kunt u bovenstaande (technische) vragen/controles het beste bij uw interne IT beheerder voorleggen (en/of de afdeling verantwoordelijk voor het beheer/configuratie van de interne Microsoft omgeving).

[Test hier zelf de SSO connectie tussen uw Microsoft omgeving en de BHV App van StandBy](#)

- Klik bovenaan op de groene login knop
- Log -via Microsoft- in op uw bedrijfs Microsoft omgeving
- Geef de 'BHV App' Microsoft app toestemming voor toegang tot uw gegevens
- U wordt teruggestuurd naar de testpagina en ziet hier binnen enkele seconden een rood of groen vak verschijnen.
 - Indien het vak groen is, is uw Microsoft omgeving al correct geconfigureerd en kunt u direct door naar de volgende check (zie hieronder het item "*StandBy BHV App omgeving*")
 - Indien het vak rood is, probeer de tweede groene button met de tekst: "Inloggen met Microsoft in consent modus". Deze modus forceert dat u eerst expliciet om toestemming wordt gevraagd om in te mogen loggen.
 - Blijft het niet werken, dan dient u bovenstaande informatie door te geven aan uw interne IT beheerder zodat ze de instellingen in uw Microsoft omgeving kunnen aanpassen zodat het wél toegestaan wordt dat u via SSO kunt inloggen op de

BHV App. Hieronder in dit document treft u een aantal problemen en oplossingen aan die kunnen optreden.

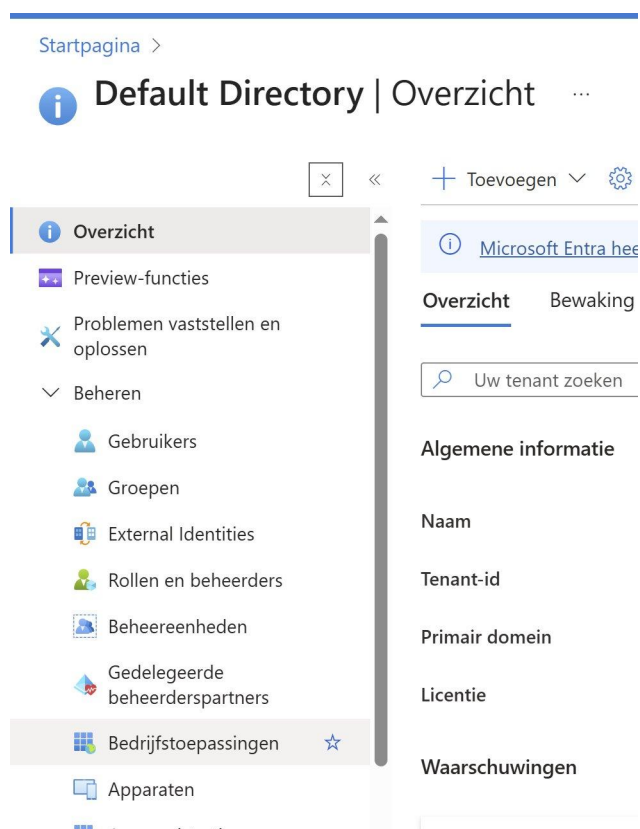
- Indien uw IT beheerder wijzigingen heeft gemaakt, voert u de bovenstaande test nogmaals uit totdat u het groene vak te zien krijgt met een succesvol testresultaat.

Problemen en oplossingen

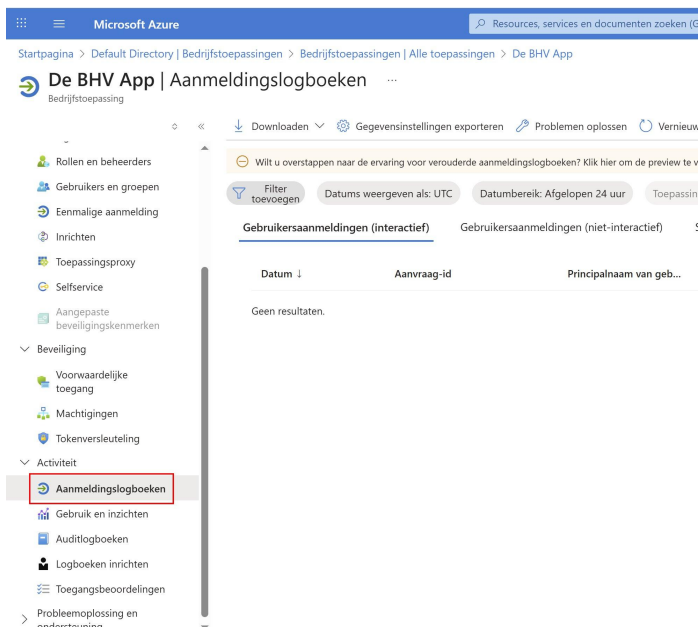
Indien het niet mogelijk is om met uw Microsoft account in te loggen (SSO) op de BHV App test link, zijn er een aantal oorzaken mogelijk. Deze oorzaken zijn hoofdzakelijk technisch van aard, deze kunt u het beste delen met uw IT beheerder als u zelf geen controle heeft over uw Microsoft Azure/Entra ID omgeving:

Volg de volgende stappen om iedere oorzaak te kunnen vinden indien een login wordt geblokkeerd (dit zijn generiek stappen om ieder onderliggend login probleem te kunnen traceren):

[1] Nadat [de test URL is geopend en er een login poging heeft plaatsgevonden](#), kun je binnen de Azure omgeving naar "De BHV App"-applicatie gaan (de app waarvoor Admin consent is gegeven): Entra ID > Bedrijfstoeepassingen > De BHV App:



[2] In het menu kies je vervolgens onder "Activiteit" voor "Aanmeldingslogboeken". Hier verschijnen alle recente login (pogingen). Controleer eerst op het (standaard getoonde) tabblad: "Gebruikersaanmeldingen (interactief)" of de login zelf in orde is:



Let op: Het kan een aantal minuten duren voordat nieuwe logins hier worden getoond. (bovenstaand screenshot laat geen login pogingen zien)

[3] Daarna klik je op het tabblad ernaast: "Gebruikersaanmeldingen (niet-interactief)". Zoek hier dezelfde login(poging) op. Hier zul je een "Status: Fout" zien staan bij een mislukte login.

[4] Klik op de registratie om te zien welke *permission policy* precies ervoor zorgt dat de login wordt geblokkeerd. In het getoonde side-panel zie je bovenaan een tabblad "Voorwaardelijke toegang", klik hierop.

[5] Hier kun je exact zien welke interne Azure policy het probleem is. Als één van de de policy items in de lijst "Geblokkeerd" toont, heb je het probleem gevonden. Dit is precies die policy de reden dat de login vanuit Azure wordt geblokkeerd.

Oplossing: De exacte oplossing is afhankelijk van welke permission policy precies de reden van de blokkade is. Over het algemeen heb je een aantal opties: De policy aanpassen om minder beperkende eisen te hebben voor de (groep van) personen (bijv. meer login locaties toestaan) - of je kunt de policy volledig uitschakelen voor de (group van) personen.

Een aantal vaker voorkomende problemen waardoor SSO wordt geblokkeerd door een organisatie:

- Uw beheerder heeft de optie om uw login via SSO te gebruiken expliciet uitgezet of hanteert een 'allow list' van applicaties waarmee dat mag.

- Om te voorkomen dat gebruikers ongecontroleerd overal in kunnen loggen met hun bedrijfs e-mail adres, kan een beheerder ervoor kiezen om dit alleen toe te staan bij een vooraf gedefinieerde lijst van diensten.
- Om te zorgen dat gebruikers via SSO kunnen inloggen op De BHV App, dient de Microsoft app “De BHV App” te worden toegestaan (‘admin consent’) door een beheerder. Voor info/instructies, zie het hoofdstuk hierboven met de vereisten: “Microsoft tenant omgeving”
- Uw beheerder heeft restricties ingesteld voor callback URL’s van externe applicaties.
 - Het kan voorkomen dat uw omgeving alleen dataverkeer toelaat van/naar Nederlandse servers (of andere geo beperkingen heeft). De Servers van StandBy zijn gehost bij Amazon Web Services en staan in Ierland. U dient te zorgen dat verkeer naar (*).standbysolutions.nl kan worden gebruikt door uw gebruikers. (Achtergrond: Een SSO Login bestaat uit een gebruiker die inlogt (interactief) en onze server die toestemming heeft om namens de gebruiker in te loggen (non-interactieve login). Specifiek dit deel vereist dat Ierland wordt toegestaan als locatie van waar vandaan moet kunnen worden ingelogd).

StandBy BHV App omgeving

Binnen de BHV App omgeving dient u er alleen voor te zorgen dat alle gebruikers **exact hetzelfde e-mail adres (vanuit Microsoft) aan hun BHV app profiel gekoppeld krijgen**. De SSO koppeling werkt namelijk op basis van het e-mailadres waarmee wordt ingelogd binnen Microsoft.

TIP: Single Sign On integreert het beste in combinatie met een automatische gebruikers synchronisatie. U kunt gebruik maken van de aanvullende **Microsoft Azure synchronisatie module** om te zorgen dat nieuwe BHV'ers in uw Microsoft omgeving automatisch een BHV App account krijgen. Zonder de synchronisatie module zult u nieuwe BHV'ers eerst zelf handmatig moeten aanmelden in de BHV App (met het juiste e-mailadres) om te zorgen dat ze SSO kunnen gebruiken met het Microsoft account.

Opvolging

Werkt de test SSO login én heeft u gecontroleerd of de e-mailadressen van alle gebruikers correct zijn?

Koppel dit dan via support@standbysolutions.nl terug aan de BHV App klantenservice (of uw uitrol manager) om te zorgen dat wij SSO inschakelen voor uw BHV App omgeving. Pas nadat wij bevestigen dat SSO is ingeschakeld, kunnen uw gebruikers met een Microsoft account inloggen op de BHV App.

Gebruikers zullen het volgende merken wanneer SSO is ingeschakeld:

- Bestaande gebruikers die al zijn ingelogd met een BHV App gebruikersnaam/wachtwoord blijven ingelogd en hoeven niets te doen.
- Bestaande gebruikers die uitloggen en weer willen inloggen kunnen vanaf nu SSO gebruiken ('Inloggen met Microsoft' knop op het login scherm) of blijven inloggen met hun eerdere BHV App gebruikersnaam/wachtwoord combinatie.
 - Het inloggen via SSO en inloggen met een gebruikersnaam/wachtwoord bestaat naast elkaar en kan afwisselend worden gebruikt.
- Nieuwe gebruikers ontvangen voortaan een e-mail waarin uitgelegd staat waar ze de BHV App kunnen downloaden en hoe ze via SSO (Microsoft) kunnen inloggen. Deze gebruikers hoeven geen BHV App wachtwoord meer in te stellen en kunnen direct inloggen via SSO.
 - Let op: Nieuwe gebruikers die voor het eerst succesvol via SSO inloggen worden op dat moment ook automatisch als 'geactiveerd' geregistreerd in de BHV App. (omdat deze gebruikers geen BHV App wachtwoord hoeven in te stellen om hun account te activeren)

- Alle gebruikers, met of zonder SSO ingeschakeld, blijven de mogelijkheid behouden om een BHV App specifiek wachtwoord in te stellen/resetten. Dit kan door wachtwoordherstel aan te vragen via help.standbysolutions.nl.