

Single sign-on voor Dialog

Online platform - [Click for English](https://www.dialog.nl/wp-content/uploads/2020/10/Dialog-Single-sign-on-english.docx)

# Introductie

Dialog ondersteunt single sign-on (SSO) op basis van OAuth 2.0 en OpenID connect 1.0. Om dit voor jullie organisatie in te kunnen stellen, moeten jullie zelf een aantal acties ondernemen. Daarnaast hebben wij bepaalde informatie nodig om de SSO vanuit onze kant goed in te kunnen stellen.

In dit document vind je alle informatie die nodig is om gebruik te kunnen maken van de SSO. We delen daarnaast een aantal veel gestelde vragen rondom de SSO en de bijbehorende antwoorden. Mochten jullie nog andere vragen hebben, stel die dan gerust door een e-mail te sturen naar support@dialog.nl.

# Acties

Voer de volgende acties uit in jullie identity provider.

1. Controleer of jullie SSO provider de ‘Authorization Code flow’ ondersteunt
2. Controleer of de volgende scopes worden toegestaan: ‘openid’, ‘email’, ‘profile’
3. Sta de volgende redirect urls toe:
	* <https://api.dialog.nl/api/sso/openidconnectcallback>
	* <https://acceptance-api.dialog.nl/api/sso/openidconnectcallback>
4. Stel indien mogelijk de homepage voor de SSO in als: https://app.dialog.nl
5. Stel het volgende icoon in als icoon voor de koppeling:

# Claims

Dialog volgt de OpenID Connect 1.0 standaard en verwacht dat de volgende claims worden meegestuurd in de Identity Token (<https://openid.net/specs/openid-connect-core-1_0.html#Claims>):

* email
* given\_name
* middle\_name
* family\_name
* name
* picture (optioneel)
* gender (optioneel)

De exacte naamgeving, zoals hierboven aangegeven, is essentieel voor het parsen van de token. Bij sommige identity providers moet expliciet aangegeven worden dat de claims ook in de identity token worden gezet.

Naast de bovenstaande acties, is het volgende belangrijk om te regelen:

* Zorg ervoor dat in jullie Identity Provider bij gebruikers zowel de voornaam als achternaam is ingevuld (claims: ‘given\_name’, ‘middle\_name’, ‘family\_name’). Dit wordt overgenomen door Dialog. Als deze velden leeg zijn, wordt de volledige naam (de ‘name’ claim) overgepakt.
* Zorg ervoor dat gebruikers in Dialog worden uitgenodigd op hun originele e-mailadres. Alias e-mailadressen zorgen voor problemen bij het inloggen in Dialog als het Dialog e-mailadres niet gelijk is aan het originele e-mailadres van de gebruiker.

# Benodigde informatie

Na het uitvoeren van de bovenstaande acties, krijg je informatie te zien die wij nodig hebben om de SSO goed in te stellen. Vul de antwoorden in in de kolom ‘Antwoord’.

|  |  |  |
| --- | --- | --- |
| Categorie | Voorbeeld | Antwoord |
| Discovery url | https://login.microsoftonline.com/{Directory/tenant ID}/v2.0/.well-known/openid-configuration |  |
| Client ID |  |  |
| Client secret |  |  |
| Issuer ID  | https://login.microsoftonline.com/{Directory/tenant ID}/v2.0 |  |
| Domain | dialog.nl |  |

# Veel gestelde vragen

## Wat verandert er aan de login flow zodra SSO aan staat in Dialog?

Wanneer de SSO is ingesteld, wordt de standaard login flow vervangen door een SSO login flow. Gebruikers loggen dan in met hun organisatie account, zoals een Office 365 of Google account. Zij blijven dit doen vanaf https://app.dialog.nl/account/login, maar zullen na het invullen van het e-mailadres veld doorgestuurd worden naar de SSO inlog. Na succesvolle login in de SSO omgeving, wordt de gebruiker terug naar Dialog geredirect.

## Moet ik nieuwe gebruikers nog steeds uitnodigen voor Dialog?

Jullie zullen nieuwe gebruikers nog steeds moeten aanmaken in Dialog. De datum die je aan de uitnodiging meegeeft, is de datum waarop het account actief wordt en dus te gebruiken is. De gebruiker ontvangt dan een uitnodigingsmail om te starten met Dialog. Deze nieuwe gebruiker hoeft zich niet te registreren, maar komt in het inlogscherm van Dialog. De gebruiker logt in met zijn SSO account en komt daarna in Dialog terecht.

##  Is twee factor authenticatie mogelijk wanneer we gebruik maken van SSO?

Jullie kunnen bij jullie identity provider zelf instellen dat jullie gebruik willen maken van twee factor authenticatie. Dit is niet iets wat in of door Dialog hoeft te worden geregeld.

## Kan een gebruiker zijn naam, e-mailadres of wachtwoord wijzigen in Dialog na ingelogd te zijn met SSO?

Nee. Wanneer de gebruiker voor het eerst in Dialog inlogt met zijn SSO/company account, worden de velden voor naam, e-mail en wachtwoord vastgezet in Dialog. Gebruikers kunnen deze velden dan ook niet meer aanpassen. De naam van de gebruiker wordt namelijk opgehaald uit jullie identity provider. De wachtwoord reset flow gaat ook via jullie identity provider.