Single Sign-On

De kracht van Single Sign-On is dat een medewerker met één account op verschillende applicaties kan inloggen, mits deze staan ingesteld op de Single Sign-On (SSO) server. Inloggen in OpenWave gebruikmakend van Single Sign-On houdt in dat men met een druk op de knop kan inloggen in OpenWave met een persoonlijk account dat binnen de werkomgeving ook voor andere applicaties gebruikt wordt.

Indien er van deze inlogmethode gebruik gemaakt wordt zal de controle of een medewerker een geldige medewerker is binnen OpenWave naast OpenWave ook plaats vinden op een externe SSO server. Dit betekent dat een medewerker bekend moet zijn in OpenWave en op de SSO server. In OpenWave moeten deze aan elkaar worden gekoppeld.

Waarschuwing

Tenzij anders aangegeven dan gaat het bij configuratie items om items uit *Sectie: SingleSignOn*

(Technische) Opmerkingen vooraf

- OpenWave ondersteunt enkel OpenID Connect (OIDC) als manier van inloggen
- De term ADFS (Active Directory Federation Server) in onderstaande tekst verwijst naar de Microsoft implementatie van een SSO server.
- Wanneer Single Sign-On ingesteld staat dan dient men de geldigheidsduur van een sessie van een gebruiker in te stellen op de Single Sign-On server zelf. Hiermee worden de volgende configuratie instellingen genegeerd:
    - *Getal1* van Sectie: *Sessie* en Item: *MaxUurSindsCreatie*
    - *Getal1* van Sectie: *Sessie* en Item: *MaxUurSindsAanroep*

Stappen

Voor een succesvolle integratie van OpenWave binnen de SSO omgeving dient men de volgende stappen te ondernemen:

- **1. Instellen OpenWave op eigen SSO server**. Als eerste moet **OpenWave ingeregeld/ingesteld worden op de SSO server** die gebruikt gaat worden voor het gebruikersbeheer. Dit valt buiten de scope van Wave support: men dient hiervoor contact op te nemen met de eigen ICT-afdeling.
- **2. OpenWave koppelen aan SSO server**. Wanneer OpenWave is ingesteld op de desbetreffende SSO server dan kan met de verkregen gegevens OpenWave gekoppeld worden met de SSO server. Zie kopje *Koppeling OpenWave met Single Sign-On* op deze pagina hoe dit te doen.
- **3. Gebruikers uit OpenWave koppelen aan de SSO server**. Na het instellen bij stap 1 en 2 kunnen medewerkers uit OpenWave gekoppeld worden aan de SSO server. Vooraleer een

medewerker gekoppeld is, is het belangrijk dat deze medewerker eerst wordt gekoppeld aan OpenWave op de SSO server. Dit is een actie voor uw ICT afdeling. Zie kopje *Koppeling OpenWave gebruiker met Single Sign-On* op deze pagina voor meer informatie.

Waarschuwing

Om Single Sign-On te kunnen testen moet er een medewerker zijn gekoppeld vanuit OpenWave met de SSO server en vice versa moet er een medewerker zijn gekoppeld op de SSO server met OpenWave. Voor deze laatste stap dient men contact op te nemen met de eigen ICT-afdeling.

Koppeling OpenWave met Single Sign-On

Voor de koppeling tussen OpenWave en een SSO server zijn verschillende gegevens nodig. Deze gegevens moeten in de instellingen in OpenWave worden ingevuld en zijn afkomstig van de SSO server. Mocht OpenWave nog niet als applicatie zijn geregistreerd op de SSO server dan moet dit eerst gebeuren door uw ICT-afdeling. De instellingen voor OpenWave staan beschreven op de volgende pagina: Configuratie instellingen Single Sign-On.

Toelichting bij instellen van EndpointAuthorize

Het aanvinkvakje bij instelling *Item: EndpointAuthorize* dient om inloggen via Single Sign-On aan dan wel uit te zetten. In hetzelfde configuratie item kan bij kolom *Tekst* de endpoint URL worden opgegeven.

Indien de *Tekst* kolom van het configuratie item: *EndpointWellKnown* is gevuld met een URL dan kan het tekstveld van *EndpointAuthorize* leeg gelaten worden. In dat geval wordt de *EndpointAuthorize* URL uit het Well Known configuratie document van de Azure gehaald die gekoppeld is aan de *EndpointWellKnown* URL.

De endpoint URL is een link naar de SSO server waarop ingelogd kan worden door de medewerker. Deze URL moet naast het endpoint extra gegevens bevatten waarmee de autorisatieserver op de juiste manier aangeroepen kan worden. Hierdoor weet de autorisatieserver dat het met de juiste instantie/medewerker te maken heeft. Deze gegevens kunnen in de vorm van een JSON worden meegegeven bij kolom *Info*.

De JSON/ waarde van kolom *Info* kan bestaan uit de volgende velden:

- **state**: Geeft aan of er een unieke code meegestuurd moet worden met de eerste request richting de SSO server. Deze kan worden toegevoegd om cross-site attacks te voorkomen. Wanneer de state in de tussentijd verandert dan mislukt het inloggen. Het wordt sterk aangeraden om deze variabele op true te zetten. Waarde is **true** of **false**. Dit veld is niet verplicht, indien niet opgegeven dan wordt er standaard wél een state meegestuurd.
- **client_id**: Dit zal vervangen worden met de waarde van kolom *Tekst* bij *Item: ClientID*. De waarde van dit veld is **%CLIENTID%**. Dit veld is **verplicht**
- **redirect_uri**: Dit zal vervangen worden met de waarde van kolom *Tekst* bij *Item: EndpointRedirect*. De waarde van dit veld is **%ENDPOINTREDIRECT%**. Dit veld is **verplicht**
- **scope**: Hiermee wordt aangegeven middels openid te willen autoriseren en dat met behulp van

profile extra gegevens opgevraagd worden om de medewerker te kunnen identificeren in OpenWave. Indien niets wordt ingevuld dan wordt standaard de waarde met *openid profile* gevuld. Indien wel ingevuld maar het bevat niet de waardes *openid* en *profile* dan worden deze automatisch toegevoegd aan de waarde. De waarde van dit veld is **openid profile** met spatie tussen beide woorden.

- **response_type**: Hiermee wordt aan de autorisatieserver aangegeven dat OpenWave om een code zal vragen waarmee vervolgens een token kan worden opgevraagd. De waarde van dit veld is **code**. Dit veld is **verplicht**
- **nonce**: Middels een nonce wordt een extra beveiliging laag toegevoegd in de vorm van een unieke id per login request. Hiermee kunnen replay attacks worden voorkomen. Het wordt sterk aangeraden om deze variabele op true te zetten. Waarde is **true** of **false**. Dit veld is niet verplicht, indien niet opgegeven dan wordt er standaard wél een nonce meegestuurd.

Een voorbeeld van de configuratie JSON wordt daarmee als volgt:

```
{
   "state": true,
   "client_id": "%CLIENTID%",
   "redirect_uri": "%ENDPOINTREDIRECT%",
   "scope":"openid profile",
   "response_type": "code",
   "nonce": true
  }
```

Een voorbeeld van een volledig opgebouwde endpoint URL zoals die in de adresbalk is te zien: https://ditiseenadfsserver.nl/adfs/oauth2/authorize/v2.0?client_id=1111111-2222-3333-4444-55555555&response_type=code&scope=openid_profile&state=123456789&redirect_uri=https://www.open-wave.nl

Waarschuwing

Aangeraden wordt om metjsonlint.com te controleren of de configuratie JSON valide is. Wanneer de JSON niet valide is dan wordt de knop: “Inloggen met Single Sign On” onzichtbaar en kan niet worden ingelogd via Single Sign-On.

Waarschuwing (2)

Met uitzondering van de parameters: state en nonce staan alle sleutels én de bijbehorende waardes (key/value paren) tussen dubbele aanhalingstekens. De waarden van state en nonce zijn in dit geval een boolean (true/false) en behoeven geen aanhalingstekens.

Waarschuwing (3)

In de Authorisatie endpoint URL staat veelal aangegeven met welke versie van een endpoint men te maken heeft. Een server biedt veelal v1.0 en v2.0 endpoints aan. Echter gaat het bij ADFS 2016 en 2019 servers evenwel vaak om een v1.0 implementatie van Single Sign-On, hoewel de endpoint URL anders zou doen vermoeden. De versienummering is van invloed op de manier hoe een medewerker wordt geautoriseerd. Zie *Koppeling OpenWave gebruiker met Single Sign-On* voor meer informatie

hierover.

Bij een Azure AD (Cloud) oplossing kan men er vanuit gaan dat dit altijd een versie 2.0 implementatie betreft. Een voorbeeld van een endpoint URL met versienummering: https://ditiseenadfsserver.nl/adfs/oauth2/authorize/v2.0

Waarschuwing (4)

Indien er een nonce wordt meegestuurd dan dient de volgende instelling te bestaan: *Sectie: PreInlog, Item: TussenMapSSO* met in kolom *Tekst* de waarde van de tussenmap (/tmp/openwave/sso/).

Toelichting bij instellen van EndpointToken

In kolom *Tekst* van configuratie item: *EndpointToken* kan de endpoint URL worden opgegeven om de JWT token op te vragen. In de eerste stap van het inlogproces geeft de autorisatieserver een code terug. Met deze code en enkele andere gegevens kan een toegangstoken worden opgevraagd bij de endpoint URL die gespecificeerd is bij *EndpointToken*.

Indien de Tekst kolom van het configuratie item: *EndpointWellKnown* is gevuld met een URL dan kan het tekstveld van *EndpointToken* leeg gelaten worden. In dat geval wordt de *EndpointToken* URL uit het Well Known configuratie document van de Azure gehaald die gekoppeld is aan de *EndpointWellKnown* URL.

In *Getal1* van dit item kan het versienummer van de SSO server worden opgegeven. Sommige servers waaronder Microsoft ADFS 2016 servers werken met versie 1 tokens. De versie 1 tokens zijn anders opgebouwd dan versie 2 tokens en moeten daarom op een andere manier worden gevalideerd.

De kolom *Info* van *Item: EndpointToken* wordt gebruikt om deze gegevens in JSON formaat naar het token endpoint te sturen. Deze bestaat uit de volgende velden:

- **grant_type**: Het kenbaar maken aan de SSO server op welke manier er geautoriseerd moet worden. De waarde van dit veld is **authorization_code**. Dit veld is **verplicht**
- **client_id**: Dit zal vervangen worden met de waarde van kolom *Tekst* bij *Item: ClientID*. De waarde van dit veld is **%CLIENTID%**. Dit veld is **verplicht**
- **redirect_uri**: Dit zal vervangen worden met de waarde van kolom *Tekst* bij *Item: EndpointRedirect*. De waarde van dit veld is **%ENDPOINTREDIRECT%**. Dit veld is **verplicht**
- **client_secret**: Dit zal vervangen worden met de waarde van kolom *Tekst* bij *Item: ClientSecret*. De waarde van dit veld is **%CLIENTSECRET%**. Indien er op de SSO server een ClientSecret is gespecificeerd dan is dit veld verplicht, anders kan het weggelaten worden.

Een voorbeeld van de configuratie JSON wordt daarmee als volgt:

```
{
   "grant_type":"authorization_code",
   "redirect_uri": "%ENDPOINTREDIRECT%",
   "client_id": "%CLIENTID%",
   "client_secret": "%CLIENTSECRET%"
  }
```

Waarschuwing

Aangeraden wordt om metjsonlint.com te controleren of de configuratie JSON valide is. Wanneer de JSON niet valide is dan wordt de knop: “Inloggen met Single Sign On” onzichtbaar en kan niet worden ingelogd via Single Sign-On.

Waarschuwing (2)

Alle sleutels en bijbehorende waardes (key/value paren) staan tussen dubbele aanhalingstekens.

Waarschuwing (3)

In de EndpointToken URL staat veelal aangegeven met welke versie van een endpoint men te maken heeft. Een voorbeeld van een endpoint URL met versienummering: https://ditiseenadfsserver.nl/adfs/oauth2/token/v2.0 Een SSO server biedt veelal v1.0 en v2.0 endpoints aan. Echter gaat het bij ADFS 2016 en 2019 servers vaak om een v1.0 implementatie van SSO, hoewel het endpoint anders zou doen vermoeden.

De versienummering is dus van invloed op de manier hoe een gebruiker wordt geautoriseerd m.b.t. bepaalde gebruikte parameters die tussen de twee versies verschillen. Zie *Koppeling OpenWave gebruiker met Single Sign-On* voor meer informatie hierover.

Koppeling OpenWave medewerker met Single Sign-On

De volgende stap na het instellen van de instellingen op de SSO server is het koppelen van OpenWave gebruikers aan SSO. De medewerkersnaam / medewerkers ID die ingevuld dient te worden verschilt per serverconfiguratie.

Server	**SSO serverversie**	**Waarde**
ADFS 2016 / 2019	1.0 (soms 2.0)	unique_name of UserPrincipalName (1.0) / oid (2.0)
Azure Active Directory	2.0	oid

Waarschuwing

De SSO gebruikersnaam is hoofdlettergevoelig. In het geval van een oid is dit een string met cijfers en letters.

De SSO serverversie staat gelijk aan de waarde in het configuratie item: EndpointToken (*Getal1*). In sommige gevallen is een ADFS 2019 server een 2.0 versie. Wanneer Single Sign-On niet werkt, probeer dan de serverversie te veranderen van 1.0 naar 2.0 of vice versa. Wanneer geen waarde wordt ingevuld dan wordt uitgegaan van versie 2.0. Vraag dit voor de zekerheid na bij uw ICT afdeling.

De koppeling met een OpenWave gebruiker vindt plaats op *tbmedewerkers.dvssologinid*. De Single Sign-On gebruikersnaam (*tbmedewerkers.dvssologinid*) is in te stellen in OpenWave via beheertegel *Medewerkers*, blok *SSO* veld **SSO Login ID**.

Bij een gebruiker kan tevens worden aangegeven of een medewerker mag inloggen via SSO middels *tbmedewerkers.dnssologintype*. Deze gegevens (*dnssologintype*) zijn in OpenWave te stellen bij de beheertegel *Medewerkers*, blok *SSO* veld *Inlogmethode*. De keuze bestaat uit:

- **1.** Inloggen enkel via OpenWave
- **2.** Inloggen in zowel Single Sign-On als OpenWave.

Daadwerkelijk inloggen in OpenWave via Single Sign-On en mogelijke foutmeldingen

Hierbij wordt uitgegaan dat binnen de organisatie een SSO server is ingesteld en dat OpenWave aan deze server gekoppeld is.

Indien men klikt op **Inloggen met Single Sign-On** op de inlogpagina van OpenWave wordt de inlogpagina van Single Sign-On geopend. Hier kan volgens op gebruikelijke wijze worden ingelogd. De gevraagde gebruikers-id en wachtwoord staan dus niet in OpenWave opgeslagen, maar enkel op de SSO server. Bij succes retourneert de SSO-server een identifier die OpenWave kan vergelijken met de kolom *tbmedewekers.dvssologinid* zodat ook OpenWave weet wie er ingelogd is.

Mogelijke foutmeldingen:

- *Voer uw gebruikers-id met de indeling* '*domein**gebruiker*' *of* '*gebruiker@domein*' *in*. Dit betekent dat de gebruikersnaam niet correct gevuld is. Het domein ontbreekt of het emailadres is niet goed gevuld.
- *De gebruikers-id of het wachtwoord is onjuist. Voer de gebruikers-id en het wachtwoord opnieuw in*. Gebruikersnaam of wachtwoord is niet correct gevuld. Men dient hier de inloggegevens van Single Sign-On in te vullen .

Wanneer men een gebruikersnaam en wachtwoord op de Single Sign-On inlogpagina heeft ingevuld en men vervolgens op inloggen drukt dan zal men terug genavigeerd worden naar de OpenWave pagina. Indien succesvol aangemeld via Single Sign-On dan verschijnt het openingsportaal van OpenWave zoals men gewend is. Er kan door de gebruiker uitgelogd worden en met de knop *Inloggen met Single Sign-On* opnieuw ingelogd worden, zonder dat men opnieuw inloggegevens hoeft in te vullen.

Mocht het aanmelden niet gelukt zijn dan zal het inlogscherm van OpenWave getoond worden met melding *Er is geen (unieke) medewerker in OpenWave gevonden*.

Dit betekent dat:

- er bij geen enkele medewerker van OpenWave in veld *SSO Login ID* een overeenkomende waarde is gevonden waarmee men heeft proberen in te loggen
- er bij meer dan één medewerker van OpenWave in veld *SSO Login ID* een overeenkomende waarde is gevonden waarmee men heeft proberen in te loggen
- voor de gevonden medewerker in OpenWave de waarde van *Inlogmethode* is ingesteld op NIET inloggen in zowel Single Sign-On als OpenWave

Indien men na het lezen van het bovenstaande nog steeds problemen ervaart dient men contact op te nemen met de eigen ICT-afdeling voor het controleren van het wachtwoord en de gebruikersnaam.

Waarschuwing

Indien men eenmaal succesvol is ingelogd in OpenWave via Single Sign-On dan hoeft men niet meer opnieuw inloggegevens in te vullen. Dit geldt voor zowel het sluiten van alle OpenWave instanties (tabbladen) als de browser. Dit is van toepassing zolang men niet is uitgelogd bij SSO middels de knop afmelden.

Single Sign-Off

Wanneer Single Sign-On aanstaat betekent dit automatisch ook meteen dat Single Sign-Off aanstaat. Een gevolg hiervan is dat wanneer men zich bij OpenWave afmeldt, dit niet enkel bij OpenWave gebeurt maar ook bij alle andere applicaties waarin men met het Single Sign-On account is aangemeld.

Met afmelden wordt hier bedoeld dat een medewerker op de knop: **afmelden** drukt.

Inloggen