Sectie SingleSignOn

Hieronder de instellingen uit de configuratietabel (tbinitialisatie) van de *Sectie: SingleSignOn* gerangschikt op item. Zie pagina Single Sign-On voor de volledige beschrijving instellen van Single Sign-On.

Items Configuratietabel

Item	Kolom	Omschrijving
AllowAllHostnameVerifier	Aanvinkvakje	**Zet deze alleen in het uiterste geval aan**. Indien aangevinkt dan wordt er niet gecontroleerd of de hostnaam zoals deze is gespecificeerd in de EndpointToken URL overeenkomt met de hostnaam (dnsName) uit het certificaat van de ADFS/SSO server. Deze kan in het uiterste geval op true worden gezet wanneer de foutmelding: hostname in certificate didn't match:[...] wordt gegeven als Errorcode in de messagelog. **Let op dat dit een mogelijk beveiligingsprobleem kan opleveren** Neem daarom bij voorkeur contact op met de ICT afdeling met de melding dat het certificaat van de ADFS/SSO server niet hoort bij de hostnaam van de EndpointToken URL.
ClientId	Tekst	Dit is de client identificatie, ook wel AppId genoemd. Onder deze identificatie is OpenWave als applicatie op de SSO server geregistreerd.
ClientSecret	Tekst	Dit is een sleutel die alleen bij de SSO server en OpenWave bekend is. **Deel deze sleutel met niemand**. De sleutel is gecrypt en wordt ook als zodanig op de database opgeslagen.
Debuglog	Aanvinkvakje	**Zet deze alleen in het uiterste geval aan**. Kan gebruikt worden om te debuggen. Niet aan laten staan i.v.m. overspoelen van de messagelog.
EndpointAuthorize	Aanvinkvakje	Indien aangevinkt dan kan er via SSO ingelogd worden in OpenWave.
	Tekst	De endpoint URL van de SSO autorisatie server. Indien leeg gelaten dan moet EndpointWellKnown gevuld zijn en wordt de URL hiervandaan verkregen.
	Info	Bevat een JSON string met instellingen voor het opbouwen van een autorisatie URL. Zie Toelichting bij instellen van EndpointAuthorize voor informatie over wat deze JSON kan bevatten/hoe deze op stellen.
EndpointRedirect	Tekst	Het webadres waarnaartoe gegaan moet worden nadat men succesvol is ingelogd met SSO en in het inlogscherm op de SSO knop heeft geklikt. Dit adres moet ook staan ingesteld bij de Client ID op de SSO server.

Item	Kolom	Omschrijving
EndpointToken	Tekst	De endpoint URL waarnaartoe OpenWave een aanvraag doet voor een token. Dit endpoint stuurt een Access token en een ID token terug. Dit zijn tokens in het JWT (JSON Web Token) formaat. Dit token wordt gebruikt om een gebruiker te identificeren en autoriseren in OpenWave. Indien leeg gelaten dan moet EndpointWellKnown gevuld zijn en wordt de URL hiervandaan verkregen.
	Getal1	Met welke versie van het endpoint men te maken heeft. De waarde kan 1.0 of, 2.0 of leeg zijn (leeg betekent default = 2.0). **Let op**: hoewel er in een endpoint 2.0 staat hoeft dit niet te betekenen dat men daadwerkelijk met een 2.0 versie van het endpoint te maken heeft (zie Koppeling OpenWave gebruiker met Single Sign-On voor meer informatie hierover).
	Info	Bevat een JSON string met instellingen voor het opvragen van een JWT token. Zie Toelichting bij instellen van EndpointToken voor informatie over wat deze JSON kan bevatten/hoe deze op te stellen.
EndpointWellKnown	Tekst	De endpoint URL waar de configuratie van de server staat. Hier staat onder andere welke endpoints de server kent en herbergt ook publieke sleutels die gebruikt kunnen worden om de tokens te kunnen valideren. Alleen in het laatste geval is het vullen van dit veld verplicht.
LoginschermLabel	Tekst	Het label op het loginscherm. Dit is het label waarop men kan klikken wanneer men middels SSO wil inloggen. Voeg dit item toe als een andere waarde gewenst is dan de defaultwaarde *Inloggen met Single Sign On*.
TussenMapSSO	Tekst	Moet aanwezig zijn indien men wilt inloggen met Single-Sign-On en bij instelling *EndpointAuthorizeEndpoint* kolom *Info* nonce is true (default). Het tussenstation tussen SSO en de server van OpenWave. De waarde is /tmp/openwave/sso/. Het aanmaken van deze map valt buiten de bevoegdheid van de applicatiebeheerder.
VerifyTokenSignature	Aanvinkvakje	Indien aangevinkt dan moet de signature van een access/ id token worden gecontroleerd of deze valide is. Sterk aangeraden wordt om deze standaard aan te zetten. Hiervoor moet wel het *Item: EndpointWellKnown* zijn ingevuld in deze sectie.
	Tekst	Hier staat welk veld van de header van de JWT token gebruikt moet worden voor verificatie. De waardes *kid* of *x5t* zijn mogelijk. *X5t* is verouderd en altijd in versie 1.0 tokens te vinden. *kid* is niet altijd in versie 1.0 tokens te vinden maar wel altijd in versie 2 tokens. Standaard staat deze op *kid* ingesteld tenzij handmatig anders gespecificeerd.

Inloggen

From:
https://doc.open-wave.nl/ - **Documentatie**

Permanent link:
https://doc.open-wave.nl/doku.php/openwave/1.32/applicatiebeheer/instellen_inrichten/configuratie/sectie_singlesignon

Last update: **2025/07/01 10:59**