Single Sign-On (SSO) instellen voor de Attendi App

Om medewerkers van jullie zorgorganisatie toegang te geven tot de Attendi App, maken wij gebruik van Single Sign-on (SSO) via een SAML 2.0-koppeling met jullie Identity Provider (IdP). Hierdoor kunnen gebruikers veilig en eenvoudig inloggen met hun bestaande organisatieaccount, zonder aparte inloggegevens voor Attendi.

Wat is SSO (SAML)?

Single Sign-On zorgt ervoor dat gebruikers met één account toegang krijgen tot meerdere applicaties. In deze setup fungeert jullie zorgorganisatie als Identity Provider (IdP) en Attendi als Service Provider (SP). De authenticatie verloopt via het SAML-protocol, waarbij de IdP na een succesvolle login een beveiligde bevestiging (assertion) naar Attendi stuurt.

Werkwijze

1. SAML-applicatie aanmaken in de Identity Provider

Maak binnen jullie Identity Provider (bijv. Azure AD / Entra ID, ADFS, Okta of vergelijkbaar) een nieuwe SAML 2.0-applicatie aan voor Attendi. Bij het aanmaken van deze applicatie worden de Service Provider gegevens van Attendi ingevoerd (zie hieronder).

2. Service Provider gegevens configureren (Attendi)

Gebruik bij het instellen van de SAML-applicatie de volgende onderstaande gegevens. Vul onderstaand voorbeeld in en vervang <zorgorganisatie> door de domein naam van jouw zorgorganisatie. Let op: deze moet gelijk zijn aan het domein in de zorgorganisatie specifieke email adressen.

- Sign-on URL: https://<zorgorganisatie>.app.attendi.nl/
- Entity ID: https://<zorgorganisatie>.app.attendi.nl/accounts/saml/<zorgorganisatie>/metadata/
- ACS URL: https://<zorgorganisatie>.app.attendi.nl/accounts/saml/<zorgorganisatie>/acs/

3. Verplichte SAML-claims (attributen) instellen

De Identity Provider moet bij het inloggen de volgende verplichte claims (attributen) meesturen:

- email – e-mailadres van de gebruiker
- first_name – voornaam
- last_name – achternaam

Deze gegevens gebruikt Attendi om gebruikers te identificeren en correct aan te maken of te koppelen.

Wij ondersteunen daarnaast ook deze **optionele claims (attributen)** in de SAML-assertion:

- team_name
- team_id

Deze attributen worden sterk aanbevolen wanneer jullie het gebruik van de Attendi App op teamniveau willen kunnen inzien.

Belangrijk

Deze claims (attributen) moeten in de SAML-assertion voorkomen met **exact deze namen**: team_name en team_id. Het is aan jullie hoe deze attributen intern worden bepaald en

gemapt (bijvoorbeeld vanuit department, OE-naam of een custom field).

Attendi voert **geen team- of gebruikersmanagement** uit op basis van deze gegevens:
• De aangeleverde waarden worden exact gebruikt zoals ontvangen, uitsluitend voor **analytische doeleinden**.
• Wanneer bij een gebruiker een andere team_name of team_id wordt meegestuurd, wordt de bestaande teaminformatie overgeschreven en alle data gekoppeld aan het nieuwe team.
• team_name en team_id zijn optioneel en kunnen **onafhankelijk van elkaar** worden meegestuurd. Echter, wanneer we deze attributen niet ontvangen, kunnen wij ook geen inzicht geven op teamniveau.

4. Metadata XML-bestand genereren

Zodra de SAML-applicatie is aangemaakt en geconfigureerd, kan vanuit de Identity Provider een metadata XML- bestand worden gegenereerd of gedownload. Dit SML-bestand bevat onder andere: het publieke SAML-certificaat, SSO URL van de IdP en de gebruikte bindings en endpoints. Dit XML-bestand wordt doorgaan automatisch gegeneerd door de Identity Provider en is beschikbaar via een optie zoals “Download metadata XML” of “Federation metadata”.

5. Metadata XML aanleveren bij Attendi

Lever het metadata XML-bestand aan bij Attendi, eventueel aangevuld met specifieke beveiligingsinstellingen. Attendi richt daarna de SSO-koppeling in.

6. Gebruikers toegang geven tot Attendi

Het inrichten van SSO zorg ervoor dat Attendi technisch kan samenwerken met jullie Identity Provider. **Daarna moeten gebruikers nog expliciet toegang krijgen.** Dit gebeurt volledig aan jullie kant, binnen de Identity Provider. Na het aanmaken van de SAML-applicatie in jullie Identity Provider moeten gebruikers (of in groepen) worden toegekend aan deze applicatie. Hoe dit precies werkt verschilt per Identity Provider, maar in de basis geldt:
• Je koppelt individuele gebruikers of gebruikersgroepen aan de Attendi SAML-applicatie
• Alleen gebruikers die zijn toegewezen aan deze applicatie kunnen via SSO inloggen bij Attendi.

7. Mobile Device Management = MDM (Optioneel)

Maken jullie gebruik van Mobile Device Management (MDM)? Dan raden wij sterk aan om dit in te zetten voor het uitrollen van de Attendi-applicatie op de telefoons en tablets van alle eindgebruikers. Hiermee kunnen in korte tijd grote groepen medewerkers worden bereikt. Het beheer van de apparaten verloopt volledig via de zorgorganisatie.

8. Eerste keer inloggen door een gebruiker

Voorwaarde: de gebruiker is toegewezen aan de Attendi SAML-applicatie.
• Gebruiker opent de mobiele applicatie of webomgeving
• Gebruiker kiest ‘Inloggen via SSO’
• Doorverwijzing naar organisatie-login
• Na succesvolle login terug naar Attendi

Bestaat de gebruiker nog niet in Attendi, dan wordt het account automatisch aangemaakt. Bestaat de gebruiker al dan wordt het account gekoppeld aan SSO.