IT HANDLEIDING · VERSIE 3.2

SSO instellen voor de Attendi App

Stapsgewijze werkwijze voor IT-beheerders, gebaseerd op werkende klantconfiguraties. Beschikbaar voor Microsoft Entra ID, Google Workspace en HelloID.

SAML 2.0 · Augustus 2026

> **Wijzigingen in v3.2:** uitgebreide, stapsgewijze instructies voor het correct instellen van de `team_name`-claim (§2, §3, §4), gebaseerd op terugkerende supportvragen. Nieuwe rijen toegevoegd aan de tabel met veelvoorkomende fouten (§6) en de go-live checklist (§7) is uitgebreid met losse verificatiepunten voor de teamnaam-claim.

Inhoudsopgave

1. Hoe werkt SSO bij Attendi?

Attendi gebruikt SAML 2.0 voor Single Sign-On. Jullie organisatie fungeert als Identity Provider (IdP) en Attendi is de Service Provider (SP). Gebruikers loggen in met hun bestaande organisatieaccount. Een apart Attendi-wachtwoord is niet nodig.

SAML 2.0 Login Flow
Gebruiker opent Attendi (SP) → Attendi stuurt AuthnRequest naar jullie IdP → IdP authenticeert de gebruiker → SAML Assertion wordt teruggestuurd → **Gebruiker is ingelogd**

⚠ **Altijd SP-initiated inloggen**

Gebruikers starten altijd vanuit Attendi zelf (SP-initiated), op één van twee manieren:
(1) ga direct naar zorgorganisatie.app.attendi.nl, of
(2) ga naar app.attendi.nl, voer het werk-e-mailadres in en word automatisch doorgestuurd.

Inloggen via app-tegels of het dashboard van de IdP (IdP-initiated) wordt afgeraden: bij Google wordt dit expliciet geweigerd, en bij Entra en HelloID ontbreekt dan de SP-sessie/-status, waardoor gebruikers op /acs/finish/ belanden en een inlogfout zien.

⚠ **Gebruik exact het subdomein dat je hebt opgegeven in het SSO-aanvraagformulier**

Vervang zorgorganisatie in alle SAML-URL's door het subdomein dat je zelf hebt ingevuld bij de Sign-on URL in het SSO-aanvraagformulier.
Dit komt meestal overeen met het deel vóór .nl in je e-maildomein, maar niet altijd — gebruik exact wat je in het formulier hebt opgegeven.
Een verkeerd subdomein leidt tot problemen, vooral in de mobiele app.

ⓘ **Meerdere locaties of vestigingen onder één e-maildomein**

Attendi bepaalt op basis van het e-maildomein naar welke omgeving een gebruiker wordt gestuurd. Wanneer meerdere locaties hetzelfde e-maildomein delen, kan Attendi niet bepalen naar welke vestiging een gebruiker hoort.
De aanbevolen oplossing is één gedeelde Attendi-omgeving voor de hele organisatie, waarbij elke locatie als aparte groep in de IdP wordt ingericht.
Bespreek deze situatie vóór de onboarding met je contactpersoon bij Attendi.

2. Microsoft Entra ID — stap voor stap

Log in als **Global Administrator** of **Application Administrator** op entra.microsoft.com.

Stap 1 — Maak een nieuwe Enterprise Application aan

Ga naar Identiteit → Toepassingen → Enterprise-toepassingen → + Nieuwe toepassing → Uw eigen toepassing maken. Kies „Integreer een andere toepassing die niet in de galerie staat", geef de naam **Attendi App** in en klik op Maken.

Stap 2 — Open de SAML-configuratiepagina

Ga in de Attendi App naar Eenmalige aanmelding → SAML. Je ziet de pagina met drie genummerde kaarten.

Stap 3 — Vul de SP-gegevens in (Kaart 1) en stel claims in (Kaart 2)

Klik op ✏ Bewerken bij Kaart 1. Vervang zorgorganisatie door het subdomein dat je hebt opgegeven in het SSO-aanvraagformulier. De Aanmeldings-URL is verplicht.

Kaart 1 — Standaard SAML-configuratie

Entity ID *	`https://zorgorganisatie.app.attendi.nl/accounts/saml/zorgorganisatie/metadata/`
ACS URL *	`https://zorgorganisatie.app.attendi.nl/accounts/saml/zorgorganisatie/acs/`
Aanmeldings-URL *	`https://zorgorganisatie.app.attendi.nl/`
Relay State	`– leeg laten –`
Logout URL	`– leeg laten –`

Kaart 2 — Kenmerken en claims

Claim name	Bron / waarde	Naamruimte	Status
`...claims/emailaddress`	`user.mail`	auto	**Verplicht**
`...claims/givenname`	`user.givenname`	auto	**Verplicht**
`...claims/surname`	`user.surname`	auto	**Verplicht**
`team_name`	`user.department`	LEEG	Aanbevolen

2.1 — team_name goed instellen: drie velden, drie veelgemaakte fouten

De `team_name`-claim is degene die in de praktijk het vaakst verkeerd wordt ingesteld — vrijwel altijd door één van de drie fouten hieronder. Klik op **+ Nieuwe eigenschap toevoegen** (Add new claim) onder Kaart 2 en vul de velden exact zo in:

Veld in Entra	Vul in als	Let op
Naam (Claim name)	`team_name`	

		Exact deze naam: kleine letters, underscore. **Niet** de naam van het bronattribuut invullen (dus niet "department" of "afdeling").
Naamruimte (Namespace)	`— leeg laten —`	Typ hier **niets** in, ook geen "http://...". Zodra dit veld gevuld is, plakt Entra een lange URL-prefix vóór de claimnaam en herkent Attendi de claim niet meer.
Bronattribuut (Source attribute)	`user.department`	Of het attribuut waarin bij jullie de team-/afdelingsnaam van de medewerker staat. Controleer dat dit veld voor gebruikers ook daadwerkelijk gevuld is.

De 3 meest gemaakte fouten bij team_name

1. Naamruimte niet leeg. De claim komt dan binnen als bijvoorbeeld `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/team_name` in plaats van kaal `team_name`. Attendi herkent deze sleutel niet en de teamnaam blijft weg.

2. Claim-naam is de naam van het bronattribuut. Bijvoorbeeld de claim heet `department` in plaats van `team_name`. De waarde komt dan wel door, maar onder de verkeerde sleutel — Attendi ziet hem niet.

3. Bronattribuut is leeg voor de gebruiker. De claim heet en staat correct, maar de waarde is leeg omdat het department-veld in Entra ID niet is ingevuld voor die specifieke gebruiker.

Zo controleer je het vóór livegang

Gebruik de knop „Testen door u" / „Test this application" op de SAML-configuratiepagina in Entra (rechtsboven bij Kaart 2 of 3), log in als testgebruiker en bekijk de ontvangen SAML-respons. Controleer dat de claim exact `team_name` heet (dus geen URL-prefix ervoor) én een waarde bevat. Zie je een andere sleutel of een lege waarde, loop dan de tabel hierboven nogmaals langs.

Kopieer deze waarden exact — Entra ID

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

Stap 4 — Download de Federatieve metagegevens-XML en lever aan bij Attendi

Klik op Federatieve metagegevens-XML → Downloaden (Kaart 3). Lever dit bestand aan bij Attendi via het SSO-aanvraagformulier.

Stap 5 — Wijs gebruikers of groepen toe aan de applicatie

Ga naar Gebruikers en groepen → + Gebruiker/groep toevoegen. Alleen toegewezen gebruikers kunnen via SSO inloggen. Zonder toewijzing krijgt de medewerker een 403-foutmelding.

Meest voorkomende fout: gebruiker niet toegewezen

> De foutmelding app_not_configured_for_user of een 403-fout betekent vrijwel altijd dat de medewerker niet is toegewezen. Controleer dit als eerste stap bij elk inlogprobleem.

3. Google Workspace — stap voor stap

Log in als **Super Administrator** op admin.google.com.

Stap 1 — Maak een nieuwe aangepaste SAML-app aan

Ga naar Apps → Web- en mobiele apps → App toevoegen → Aangepaste SAML-app toevoegen. Geef de naam **Attendi** en klik op Doorgaan.

Stap 2 — Download de Google IdP-metadata

Op het scherm „Google-identiteitsprovidergegevens" klik je op METADATA DOWNLOADEN. Bewaar dit XML-bestand — dit lever je aan bij Attendi in stap 5. Klik daarna op Doorgaan.

Stap 3 — Vul de Attendi SP-gegevens in

Vul in het scherm „Gegevens van de serviceprovider" de SP-waarden in. Vervang zorgorganisatie door het subdomein dat je hebt opgegeven in het SSO-aanvraagformulier. Stel de Notatie naam-ID bij voorkeur in op EMAIL (emailAddress) met Primary email als Naam-ID; dit sluit het beste aan op Attendi.

ACS-URL *	`https://zorgorganisatie.app.attendi.nl/accounts/saml/zorgorganisatie/acs/`
Entiteits-ID *	`https://zorgorganisatie.app.attendi.nl/accounts/saml/zorgorganisatie/metadata/`
Start-URL *	`https://zorgorganisatie.app.attendi.nl/`
Ondertekende reactie	`☐ Niet aanvinken`
Notatie naam-ID	`EMAIL (emailAddress) – aanbevolen`
Naam-ID	`Basic Information > Primary email`

> ⊘ **Ongeldige ACS-URL — kopieer nooit uit een e-mail of Word-document**
> Dit leidt tot een ongeldige URL met extra tekens (/acs/finish/%20https:/...). Kopieer de URL altijd direct vanuit onderstaand blok.

> **Kopieer deze waarden exact — Google Workspace**
> ```
> ACS-URL: https://zorgorganisatie.app.attendi.nl/accounts/saml/zorgorganisatie/acs/
> Entiteits-ID: https://zorgorganisatie.app.attendi.nl/accounts/saml/zorgorganisatie/metadata/
> Start-URL: https://zorgorganisatie.app.attendi.nl/
> ```

Stap 4 — Stel de SAML-kenmerktoewijzing in

Ga door naar het scherm „SAML-kenmerktoewijzing". Voeg koppelingen toe via TOEWIJZING TOEVOEGEN.

Claim name	Bron / waarde	Status
`email`	Basic Information > Primary email	**Verplicht**

`first_name`	Basic Information > First name	**Verplicht**
`last_name`	Basic Information > Last name	**Verplicht**
`team_name`	Employee Details > Department	Aanbevolen

> ⚠ **Let op bij team_name in Google Workspace**
>
> Het linker veld (App attribute) is de naam die Attendi ontvangt — deze moet exact `team_name` zijn. Vul hier **niet** de naam van het Google-veld in (zoals "Department"). Controleer daarnaast of het Department-veld daadwerkelijk is ingevuld bij Gebruikersbeheer → gebruiker → Functie-informatie — is dit leeg, dan komt de teamnaam wel aan als claim, maar zonder waarde.

Stap 5 — Lever de metadata aan bij Attendi

Lever het in stap 2 gedownloade XML-bestand aan bij Attendi via het SSO-aanvraagformulier.

Stap 6 — Schakel de app in voor gebruikers of organisatie-eenheden

Klik op het overzichtsscherm van de app op Details tonen bij Gebruikerstoegang. Schakel de app in voor de gewenste organisatie-eenheden of alle gebruikers.

> ⊘ **Meest voorkomende fout: app niet ingeschakeld voor de gebruiker**
>
> De foutmelding app_not_configured_for_user betekent vrijwel altijd dat de Attendi-app niet is ingeschakeld voor de OE van de gebruiker. Controleer dit als eerste bij inlogproblemen.

> ⓘ **Test altijd in een incognitovenster**
>
> Google onthoudt inlogcookies. Test SSO altijd in een privé- of incognitovenster om te voorkomen dat bestaande sessies de test beïnvloeden.

4. HelloID — stap voor stap

> ⓘ **HelloID als tussenschakel**
> HelloID fungeert als SAML IdP richting Attendi, maar authenticeert gebruikers via Microsoft 365 of Google Workspace als achterliggende bron.

Stap 1 — Maak een zelf-ondertekend certificaat aan

Ga naar Instellingen → Certificaten → Zelfondertekend certificaat aanmaken. Bewaar de naam van het certificaat — je selecteert het in stap 3.

Stap 2 — Voeg een Generic SAML-applicatie toe

Ga naar Applicaties → Application Catalog → zoek op „Generic" → Add bij Generic SAML. Geef de naam **Attendi**.

Stap 3 — Configureer het tabblad Single Sign On

Vervang zorgorganisatie overal door het subdomein dat je hebt opgegeven in het SSO-aanvraagformulier. Vul alle velden exact in zoals hieronder:

Name ID format	`emailAddress`
Issuer	`— leeg laten —`
Endpoint / ACS URL *	`https://zorgorganisatie.app.attendi.nl/accounts/saml/zorgorganisatie/acs/`
Validate and use ACS URL	`Aan`
ACS validation list	`https://zorgorganisatie.app.attendi.nl/accounts/saml/zorgorganisatie/acs/`
Binding	`HTTP-Post`
SP-initiated URL	`https://zorgorganisatie.app.attendi.nl/`
RelayState	`— leeg laten —`
Sign Assertion	`Aan`
Sign Response	`Aan`
Use DS Prefix	`Uit`
X509 Certificate *	`zorgorganisatie.helloid.com certificaat`
Overwrite Audience	`Uit`
Extra audience(s)	`https://zorgorganisatie.app.attendi.nl/accounts/saml/zorgorganisatie/metadata/`
Encrypt Assertion	`Uit`

> **Kopieer deze waarden exact — HelloID**

```
ACS URL: https://zorgorganisatie.app.attendi.nl/accounts/saml/zorgorganisatie/
acs/
ACS validation: https://zorgorganisatie.app.attendi.nl/accounts/saml/
zorgorganisatie/acs/
SP-initiated URL: https://zorgorganisatie.app.attendi.nl/
Extra audience: https://zorgorganisatie.app.attendi.nl/accounts/saml/
zorgorganisatie/metadata/
```

Stap 4 — Stel attribuutkoppelingen in (tabblad Credentials)

Ga naar tabblad Credentials. Stel NameID in op EmailAddress en voeg de extra SAML-attributen toe. Let op: voor HelloID verwacht Attendi de attribuutnamen **emailaddress**, **givenname** en **surname** — deze wijken af van de Google-namen (email, first_name, last_name).

Claim name	Bron / waarde	Status
`emailaddress`	EmailAddress	**Verplicht**
`givenname`	GivenName	**Verplicht**
`surname`	Surname	**Verplicht**
`team_name`	Department of custom	Aanbevolen

> ⚠ **Let op bij team_name in HelloID**
>
> De naam van het attribuut die je hier instelt (linkerkolom, Claim name) moet exact `team_name` zijn — niet "Department" of de naam van het HelloID-veld dat je als bron kiest. Controleer daarnaast of de bronwaarde (Department of het gekozen custom-attribuut) voor de gebruiker daadwerkelijk gevuld is; anders komt de teamnaam wel aan als claim, maar leeg.

Stap 5 — Download de metadata en lever aan bij Attendi

Klik rechtsboven op Download metadata. Lever het XML-bestand aan via het SSO-aanvraagformulier.

Stap 6 — Koppel groepen voor toegang

Ga terug naar de Attendi-applicatie in HelloID en koppel de juiste gebruikersgroepen. Alleen leden van gekoppelde groepen kunnen via SSO inloggen bij Attendi.

5. Eerste keer inloggen

De stappen zijn identiek voor alle providers. Gebruikers hoeven zelf niets in te stellen.

Stap 1	App openen (mobiel of browser)
Stap 2	E-mailadres invoeren (werk-e-mailadres)
Stap 3	Doorverwijzing naar IdP (MS / Google / HelloID)
Stap 4	Inloggen bij IdP met bestaand account
Stap 5	Ingelogd in Attendi — account is actief

ⓘ **Mobiele app — geen extra IdP-configuratie nodig**

De Attendi mobiele app opent een browser voor de SAML-flow. Er is geen aparte OAuth- of app-registratie nodig in de IdP.
Als de app na het inloggen niet terugkeert, wordt de deep link waarschijnlijk geblokkeerd door een MDM-beveiligingslaag — vraag IT de Attendi deep link te whitelisten.

ⓘ **Gebruik geen www. vóór de inlog-URL**

Open de app altijd via app.attendi.nl of via zorgorganisatie.app.attendi.nl, zonder www. ervoor.
Een adres met www. (zoals www.app.attendi.nl) wordt doorgestuurd naar een niet-bestaande omgeving. Dit toont zich vaak als een „onjuist wachtwoord"-fout terwijl het wachtwoord correct is.

6. Veelvoorkomende fouten

Fout / Symptoom	Provider	Oorzaak	Oplossing
app_not_configured_for_user (403)	Google	App niet ingeschakeld voor de OE van de gebruiker	Admin Console → Apps → Attendi → Gebruikerstoegang → schakel in voor de juiste OE
403 Forbidden	Entra	Gebruiker niet toegewezen aan de Enterprise Application	Entra → Attendi App → Gebruikers en groepen → toevoegen
AADSTS700016 — Application not found in directory	Entra	Entity ID in Entra komt niet overeen of Enterprise App is niet aangemaakt	Controleer of de Entity ID exact overeenkomt inclusief trailing slash
AADSTS50105 — User not assigned to a role	Entra	Gebruiker niet toegewezen aan Attendi Enterprise Application	Entra → Attendi App → Gebruikers en groepen → wijs gebruiker of groep toe
Teamnaam komt helemaal niet door	Entra	Naamruimte-veld niet leeg bij team_name (claim krijgt een URL-prefix)	Kenmerken en claims → Bewerken → open claim → leeg naamruimte-veld
Teamnaam komt helemaal niet door	Alle	Claim-naam is de naam van het bronattribuut (bijv. department) in plaats van team_name	Wijzig de claim-naam naar exact team_name (bron/waarde blijft ongewijzigd)
Teamnaam komt leeg door	Alle	Bronattribuut (department/ afdeling) is niet gevuld voor de gebruiker	Vul het afdelingsveld in bij de gebruiker in de HR-/directorybron
„Er ging iets mis bij het inloggen."	Alle	ACS-URL mist trailing slash (/acs i.p.v. /acs/)	Controleer of de ACS-URL exact eindigt op /acs/ mét trailing slash
Gebruiker belandt op /acs/finish/	Alle	IdP-initiated login (via portaaltegel)	Instrueer gebruikers via zorgorganisatie.app.attendi.nl te starten
Ongeldige ACS-URL	Google	Extra tekens door plakken vanuit e-mail	Herstel ACS-URL in Admin Console. Kopieer direct vanuit dit document.
Inloggen lukt in browser maar niet in mobiele app	Alle	Organisatienaam in SSO-URL komt niet overeen met e-maildomein	Neem contact op met Attendi als deze afwijken.
Mobiele app keert niet terug	Alle	MDM blokkeert Attendi deep link	Vraag IT de Attendi deep link te whitelisten.
„Onjuist wachtwoord" terwijl wachtwoord klopt	Alle	www. in de inlog-URL leidt naar niet-bestaande omgeving	Verwijder www. uit het adres. Gebruik app.attendi.nl.

7. Go-live checklist

Doorloop alle punten vóór de livegang. Elk item moet zijn afgevinkt.

☐	SAML-applicatie aangemaakt in de IdP	Enterprise App (Entra), SAML-app (Google) of Generic SAML (HelloID)
☐	ACS URL, Entity ID en Aanmeldings-URL correct ingevuld	Zonder extra tekens, met de juiste organisatienaam en trailing slashes
☐	Verplichte claims ingesteld: email, first_name, last_name	Entra: standaard URI's gebruiken, naamruimte leeg laten bij custom claims. HelloID gebruikt andere namen: emailaddress, givenname, surname
☐	**team_name — claim-naam is exact team_name**	Geen naamruimte-prefix (Entra), en niet de naam van het bronattribuut (bijv. niet "department")
☐	**team_name — bron correct ingesteld**	Entra: user.department | Google: Employee Details → Department | HelloID: Department
☐	**team_name — bronattribuut gevuld voor (test)gebruiker**	Anders komt de teamnaam leeg door, ook met de juiste claim-naam
☐	**team_name — zichtbaar getest na testlogin**	Zie sectie 5, of gebruik "Test this application" in Entra om de ruwe SAML-respons te bekijken
☐	HelloID: Sign Assertion AAN, Sign Response AAN, Binding HTTP-Post, Extra audience ingesteld	Zie het volledige overzicht van alle HelloID-velden in stap 3
☐	Metadata XML aangeleverd via het SSO-aanvraagformulier	Bevestiging van Attendi ontvangen dat de koppeling is ingericht
☐	Testgebruiker succesvol ingelogd via SP-initiated flow	In incognitovenster via zorgorganisatie.app.attendi.nl, of via app.attendi.nl → e-mailadres invoeren
☐	Alle medewerkers toegewezen aan de applicatie	Individueel of via groep / OE — in Entra, Google of HelloID
☐	Eventuele extra e-maildomeinen doorgegeven aan Attendi	Bijv. @zorgorganisatiewijkzorg.nl naast @zorgorganisatie.nl
☐	Mobiele app getest op Android en iOS	Browser opent, inloggen lukt, app is actief na terugkeer

> **Kom je er niet uit?**
>
> Neem contact op met je contactpersoon bij Attendi. Vermeld: welke IdP je gebruikt, welke foutmelding je ziet, en een screenshot van de SAML-configuratie (inclusief de team_name-claim indien het daarover gaat). Dan kunnen we snel schakelen.