Brug af Single-Sign-On (Azure AD-login) i FirstAgenda Prepare

FirstAgenda

Formål

Formålet med at anvende Single-Sign-On (f.eks. AD-login) i FirstAgenda Prepare er at gøre det lettere og mere sikkert at benytte FirstAgenda Prepare. Du kan som organisation benytte det loginsystem (Identity provider), du i forvejen anvender, og brugerne slipper for at huske flere brugernavne og passwords.

Sådan får brugerne adgang med AD-login

Det er muligt at logge på FirstAgenda Prepare med AD-login på alle de klienter, FirstAgenda Prepare i forvejen understøtter – dvs. iPad App og website[1].

”Oprettelse” af brugere

Brugere kan få adgang til FirstAgenda Prepare på 2 måder. Enten ved at blive oprettet på forhånd i administrationsmodulet i FirstAgenda Prepare eller ved automatisk oprettelse i forbindelse med første login.
Alle rettigheder – det vil sige tilknytning til udvalg, angivelse af roller, såsom dagsordensamler eller administrator skal fortsat håndteres i FirstAgendas administrationsmodul. (Medmindre du har valgt at tilkøbe AD Plus, som håndtere ekstern rettighedsstyring))

Brugeren oprettes på forhånd i FirstAgenda Prepares administrationsmodul, ved at administrator angiver brugerens e-mail-adresse. Dernæst kan administrator indstille brugerens rettigheder til de forskellige udvalg. Således har brugeren ved første login adgang til rette udvalg og dokumenter. Så snart administrator har oprettet en bruger, vil brugeren modtage en velkomstmail.

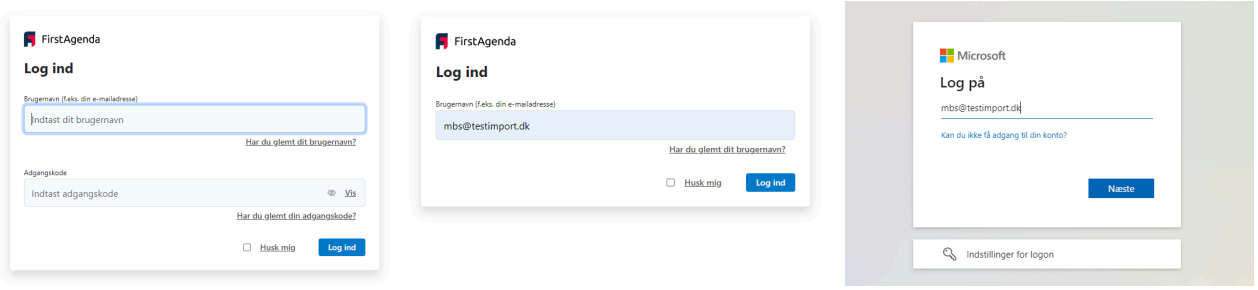
Brugeren kan som nævnt også blive oprettet ved første login i FirstAgenda Prepare. Adgang til bestemte udvalg bliver indstillet efterfølgende af administrator. Administrator får kendskab til en ny brugers adgang via en notifikationsmail, som bliver afsendt ved brugerens første login. I mailen er der et direkte link til opsætning af rettigheder for den nye bruger.

Hvordan logger brugeren på?

Hjemmesiden der benyttes er id.firstagenda.eu.
Så snart din organisation er indstillet til at benytte AD-login, så logger interne brugere ikke længere ind med FirstAgenda Prepare login (brugernavn/password), men med den e-mail-adresse, der hører til den pågældende organisation[2]. Efterfølgende videresendes brugeren til den pågældende login providers loginside (se flow nedenfor).

---

[1] Klienten skal via internettet kunne opnå forbindelse til ADFS-endpoint. Ellers vil det ikke være muligt for brugeren at logge ind. Dette påhviler organisationen at sikre dette og ikke FirstAgenda Prepare.
[2] Denne e-mail-adresse er sat op i forbindelse med den tekniske implementering.



Brugere der i forvejen benytter FirstAgenda Prepare, og som fremover skal benytte AD, men som ikke er registreret med en intern e-mail-adresse (organisationsmail) i FirstAgenda Prepare, skal manuelt have opdateret deres e-mail-adresser i FirstAgenda Prepare. Vi kan hjælpe med denne proces – bl.a. med et udtræk af brugere.

Kan interne brugere benytte FirstAgenda Prepare-login?

Som udgangspunkt vil brugere med en intern e-mail-adresse skulle anvende SSO (AD-login) i FirstAgenda Prepare, så snart organisationen er sat op til at logge på med AD. Men hvis nogle af jeres interne brugere ønsker at benytte FirstAgenda Prepare login i stedet for AD-login, vil det kunne lade sig gøre. Kontakt FirstAgenda Prepare, hvis I ønsker at aktivere funktionen, "Tillad FirstAgenda Prepare login" på jeres AD-brugere. Vær opmærksom på at disse interne brugers adgang til FirstAgenda Prepare ikke længere vil være styret i jeres AD.
Eksterne brugere (med en anden e-mail-adresse end den interne e-mail-adresse) vil fortsat kunne benytte FirstAgenda Prepare uden om AD-login.

Sådan fjernes adgang

Adgang til FirstAgenda Prepare kan fjernes på to måder:

- Brugeren fjernes fra AD-gruppen i jeres ADFS *eller*
- Brugeren deaktiveres i FirstAgenda Prepare under menuen **Brugere**

Teknisk opsætning

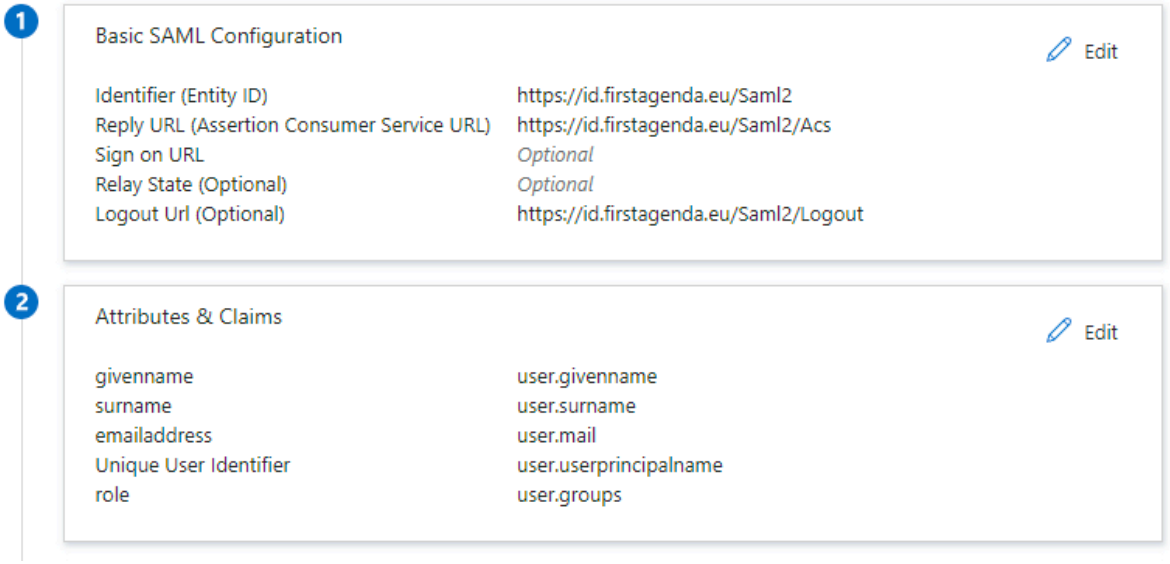
Med henblik på at jeres organisation kan logge på med AD-login i FirstAgenda Prepare er det et ultimativt krav, at jeres metadataurl bliver udstillet eksternt. Derudover er der en række claims, som er nødvendige for at brugerne kan blive oprettet i og få adgang til FirstAgenda Prepare. Læs nærmere nedenfor.

Oplysninger I har brug for fra FirstAgenda Prepare:

- Url'en til vores metadata: https://id.firstagenda.eu/Saml2

- Identifier (Entity ID): https://id.firstagenda.eu/Saml2
- Reply Url (Assertion Consumer Service URL): https://id.firstagenda.eu/Saml2/Acs
- Logout: https://id.firstagenda.eu/Saml2/Logout
- Følgende claims:

  Given Name (fornavn)
  Surname (efternavn)
  E-Mail Address (e-mail-adresse)
  (**Group**) Er ikke nødvendig. Skal bruges for at afgrænse, hvem der kan logge på.



Oplysninger vi skal bruge fra jer:

- Maildomæne
- *Enten* On Premise: Azure enterprise application: federation metadataurl
- *Eller* Cloud: Azure Enterprise non-gallery application: Unik federation metadataurl
- Brugerne, som skal anvende FirstAgenda Prepare skal være en del af **Users and Groups** i Azure AD.
- (Group name) Er ikke nødvendig. Skal bruges til at afgrænse, hvem der kan logge på.

Brugere identificeres ud fra jeres e-mail-adresse = maildomænet. Det kunne eksempelvis være @domain.com eller @subdomain.domain.com. FirstAgenda Prepare skal bruge maildomænet til at konfigurere jeres organisation til at benytte AD-login.

Adgang til flere organisationer

Hvis din virksomhed har flere organisationer i FirstAgenda Prepare, kan I ved hjælp af AD-grupper styre, hvilke organisationer i FirstAgenda Prepare brugeren må få adgang til.

De præcise navne på AD-grupperne – Group claim name – skal FirstAgenda Prepare have oplyst, så vi kan indstille jeres organisationer korrekt. Det er via tilknytningen til AD-grupper, at adgang til de forskellige organisationer i FirstAgenda Prepare kan styres centralt i jeres AD.