



Opsætning af jobfunktionsrolle og lokal IdP

Dokument

Emne: [Implementering](#)

Adgangs- og rettighedsstyring til den administrative hjemmeside styres ved hjælp af [Fælleskommunal Adgangsstyring for brugere](#) (også kendt som Context Handler). Det er altså kommunens egen opsætning af brugere og jobfunktionsroller, som styrer, hvilke medarbejdere der kan få adgang.

OS2valghalla benytter Context Handler 2 og kræver som udgangspunkt, at brugere er godkendt til NSIS sikringsniveau 'Betydelig'. Det er derfor en forudsætning, at kommunens IdP har etableret trust til Context Handler 2, og der er angivet NSIS assurance level for IdP'en i Fælleskommunalt Administrationsmodul.

Opsætning af jobfunktionsrolle

Der skal oprettes en jobfunktionsrolle i kommunens Fælleskommunale Administrationsmodul.

Den skal tilknyttes systemet OS2valghalla og brugersystemrollen **Administrator**'.

Der skal ikke tilknyttes dataafgrænsning via KLE-numre eller lignende.

Hvis du ikke er bekendt med opsætning af jobfunktionsroller, har KOMBIT lavet en [Brugervejledning til Administrationsmodulerne for myndigheder](#).

Find vejledning til jobfunktionsroller i afsnit 7.10

Opsætning af lokal IdP

Kommunens lokale IdP skal være sat op til at kunne fungere med Context Handler 2. Desuden skal NSIS assurance level være angivet.

1. Etablering af trust til Context Handler 2

Kommunerne modtog 31. maj 2022 en KLIK-opgave om hvordan, de tilslutter deres IdP til den nye version af Context Handler (Context Handler 2). Kort fortalt, kan en kommune tage Context Handler 2 i brug ved at oprette den som relying party i kommunens IdP (etablere trust), så kommunens IdP stoler på både den gamle Context Handler (Context Handler 1) og den nye Context Handler 2.

Opgaven har deadline 22. januar 2024.

Kilde: https://digitaliseringskataloget.dk/I%C3%B8sninger/adgangsstyring-brugere#Ny_Context_Handler

2. Angivelse af NSIS assurance level

For at få kommunens IdP til at kunne sende NSIS-sikringsniveauer via Context Handler 2, skal kommunen sende en mail til leverandøren af Fælleskommunalt Administrationsmodul (helpdesk@serviceplatformen.dk), hvor kommunen beder om, at der i Fælleskommunal Administrationsmodul bliver registreret det NSIS-sikringsniveau, som kommunens IdP er anmeldt til.

Inden da skal IdP'en være sat op til at kunne håndtere NSIS, og kommunen skal have etableret to faktor-godkendelse. Læs mere i KOMBIT's [Vejledning til opsætning af Identity Provider](#).

Kommunens IdP skal desuden NSIS-anmeldes til Digitaliseringsstyrelsen, som skal godkende den: Læs

Ejer:
Godkender:

Version:
Godkendelsesdato:
Revisionsdato:

mere på [Digitaliseringsstyrelsens hjemmeside](#).

Kilde: https://digitaliseringskataloget.dk/l%C3%B8sninger/adgangsstyring-brugere#Ny_Context_Handler

3. Ikke muligt at gøre IdP NSIS klar nu

Hvis I ikke har mulighed for at gøre kommunens IdP klar til at levere et NSIS assurance level, skal I tage kontakt til [driftsleverandøren Precio Fishbone](#).

Det er muligt at omkonfigurere OS2valghalla til at benytte NIST sikringsniveau, indtil IdP'en bliver NSIS klar.

Det er dog ikke muligt at undgå kravet om at benytte Context Handler 2.