# OS2faktor Login

## CoreData AD Integration

**Version**: 2.0.1
**Date**: 17.02.2023
**Author**: BSG

# 1 Formål

Dette dokument er rettet mod teknikere der skal opsætte og konfigurere kommunens integration fra Active Directory til OS2faktor Login, så brugeroplysninger fra Active Directory bliver synkroniseret til OS2faktor Login.

## 1.1 Forudsætninger

### 1.1.1 Windows Server

Servicen skal installeres på en Windows maskine med:

- Netværksmæssig adgang til kommunens AD
- Netværksmæssig adgang til OS2faktor Login via HTTPS.
- .NET Framework 4.7.2 eller nyere

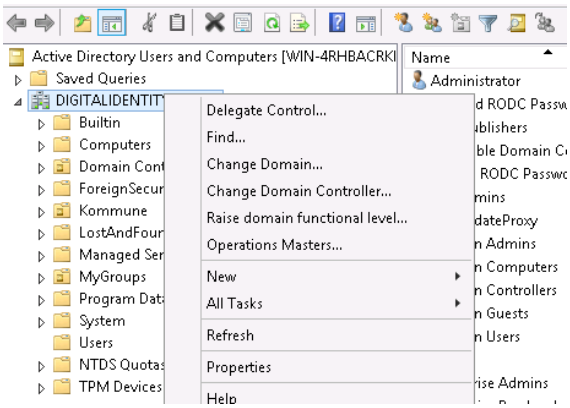
### 1.1.2 Service konto i AD

Der skal oprettes en service konto i kommunes AD.

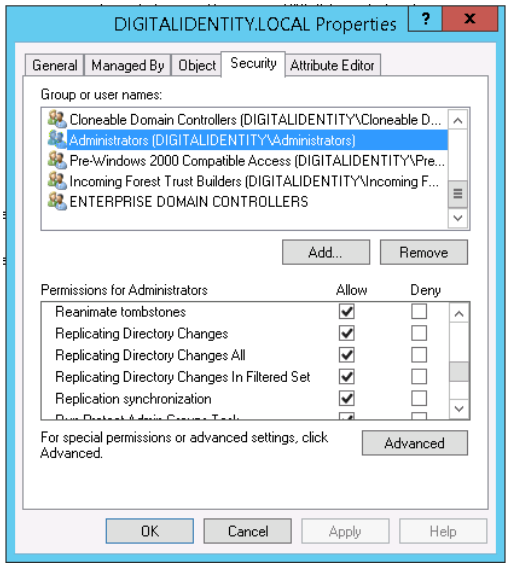
Kontoen skal have læseadgang til alle de bruger-attributer der skal læses fra brugerkonti inkl. den attribut som indeholder brugerens cpr-nummer.

Endelig skal systembrugeren også have rettigheder til at replikere data fra Active Directory. Dette vil brugeren automatisk have hvis denne er domæne administrator, men man kan også nøjes med at tilføje enkelte replikerings-rettigheder til brugeren via nedenstående vejledning

1. Åben "Active Directory Users and Computers" konsollen
2. Vælg domænet, højreklik, og vælg "properties"




3. Gå til security fanen, tilføj systembrugeren, og giv brugeren følgende replikeringsrettigheder (som vist i screenshottet nedenfor). Bemærk at den første formodentligt er den eneste der er nødvendig (alt afhængig af hvilke attributter der skal synkronisers)
    a. Replicating Directory Changes
    b. Replicating Directory Changes All (kun nødvendigt hvis der skal replikeres hemmelige attributter)
    c. Replicating Directory Changes In Filtered Set (kun nødvendigt hvis attributer der skal synkroniseres er beskyttede)




Bemærk at der kan gå nogle minutter fra denne rettighed er sat, til den slår igennem. Hvis man under kørsel af softwaren får "Access Denied" i loggen i kaldet til Active Directory, så er det disse synkroniseringsrettigheder der mangler.

### 1.1.3 API bruger til OS2faktor Login

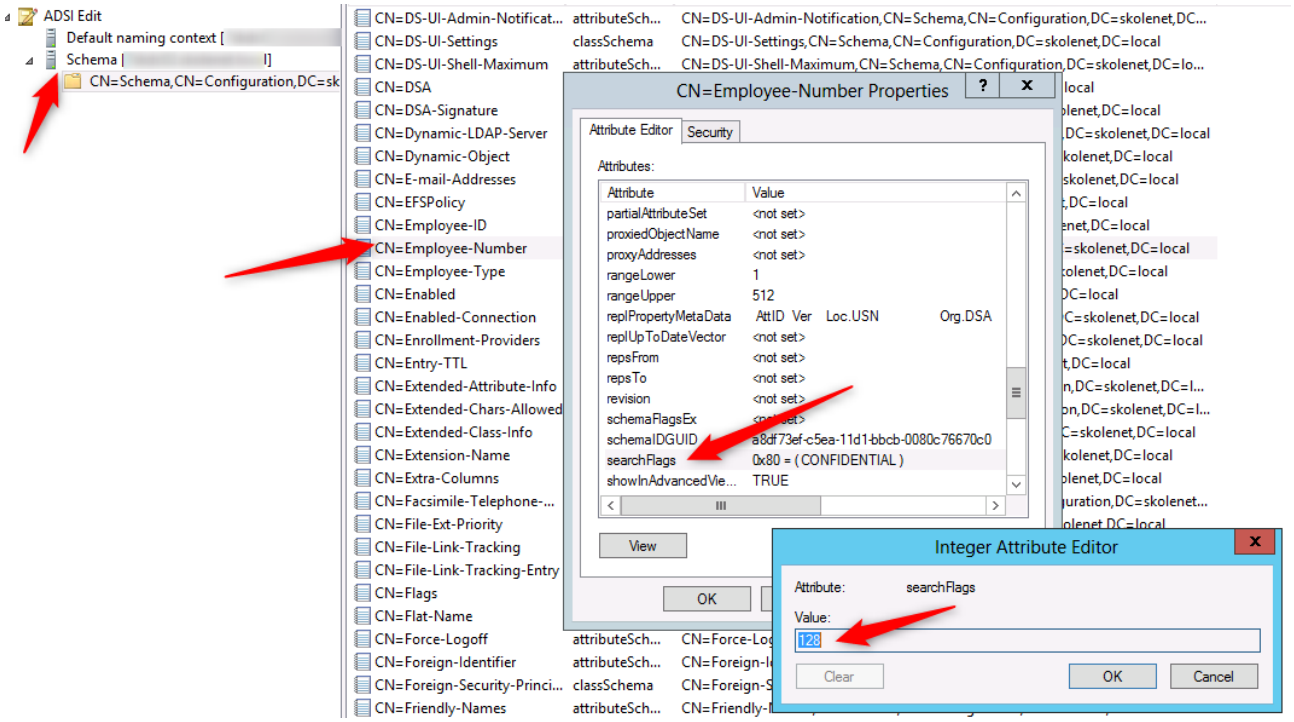
Der skal i konfigurationen indtastes en API nøgle. Denne udleveres af Digital Identity.

### 1.1.4 Afklaring af cpr-attribut

Det skal afklares hvilken attribut i AD der indeholder/skal indeholde brugerens cpr-nummer. Det kan eksempelvis være attributten EmployeeNumber.

Det anbefales at den valgte attribut skjules for almindelige brugere ved at tilføje confidentiality bit på attributten. Bemærk at det ikke er alle felter i AD der understøtter denne mulighed.

Dette kan f.eks. gøres via ADSI Edit MMC snap-in ved at tilføje bit 8 (tal-værdi 128) til searchFlags på attributten. Bemærk at hvis searchFlags har en værdi i forvejen, og den ikke i forvejen har bit 8 sat, skal bit 8 (tal-værdi 128) lægges til denne værdi.




Med dette flag sat er det kun brugere med CONTROL_ACCESS rettighed i AD, der kan læse/skrive attributten (default administratorer).

Den valgte attribut til cpr-nummer angives i indstillingen **ActiveDirectory.Property.Cpr** under konfiguration i det næste afsnit af denne vejledning.

# 2 Installation af Windows Service

Der skal installeres og konfigureres en Windows Service på en server hvor der er netværksmæssig adgang til kommunens AD samt OS2faktor Login via HTTPS.

## 2.1 Download service

Download og installér servicen fra https://www.os2faktor.dk/download.html

## 2.2 Konfiguration af service

Konfiguration af servicen foretages i appSettings sektionen i xml-filen **OS2faktorADSync.exe.config** som ligger i roden af installationsmappen (default C:\Program Files (x86)\Digital Identity\OS2faktorCoreDataSync).

De indstillinger der skal konfigureres under en standardinstallation er fremhævet med gult.

| Indstilling | Eksempel | Kommentar |
|---|---|---|
| serilog:* | | Diverse indstillinger til opsætning af log. |
| ActiveDirectory.Filter | samaccountname=a* | Angivelse af et ldap-filter til afgrænsning af hvilke AD-konti der skal synkroniseres til OS2faktor Login.<br><br>Kan være blank. |

| | | |
|---|---|---|
| ActiveDirectory.Property.Cpr | EmployeeNumber | Angivelse af hvilken attribut i AD der indeholder cpr-nummer. |
| ActiveDirectory.Property.Rid | | Angivelse af hvilken attribut i AD der indeholder RID nummeret. Er ikke krævet, og skal kun bruge til migrering af eksisterende brugere i NemLog-ins brugeradministration. Kan også klares via en egangs-indlæsning fra fx excel eller lignende. |
| ActiveDirectory.NSISAllowed.Group | CN=nsis,CN=Users,DC=digitalidentity,DC=dk | Angivelse af den AD gruppe der styrer hvilke medarbejdere der må få en erhvervsidentitet |
| ActiveDirectory.TransferToNemlogin.Group | CN=nemlogin,CN=Users,DC=digitalidentity,dc=DK | Angivelse af den AD gruppe der styrer hvilke medarbejdere der skal overføres til NemLog-ins brugeradministration.<br><br>Bemærk at kun brugere i denne gruppe kan logge ind via NemLog-in, og at Digitaliseringsstyrelsen tager 20 DKK (check prisen på digst.dk for evt ændringer) for oprettelse af brugere |
| ActiveDirectory.Attributes.RADIUS | extensionAttribute1 | Der findes en optional styring af hvilke medarbejdere der kan gøre brug af RADIUS baseret login. Her kan man udpege hvilken attribut i AD man ønsker at anvende til denne styring<br><br>Kan være blank |
| Backend.Password | | API-password til OS2faktor Login (udleveres af Digital Identity) |
| Backend.URL.Base | https://login.kommune.dk/api/coredata/ | Sættes til URL'en på CoreData API'et på OS2faktor Login.<br><br>Digital Identity kan hjælpe med denne værdi |
| Backend.Domain | Kommune.dk | Skal udfyldes med navnet på det domæne man indlæser fra. Det er en kombination af et præsentationsnavn (vises i brugergrænsefladen for adminsitratorer) og teknisk ID der skal være ens i alle integrationer der gør brug af domænebegrebet. |

| | | |
|---|---|---|
| | | Sæt evt til domænenavnet i AD'et, fx "kommune.dk" |
| Scheduled.GroupSyncTask.cron | 0 5/15 5-19 ? * 1-5 * | Et CRON udtryk der angiver hvor ofte der foretages en fuld synkronisering af gruppe-medlemsskaber. Default er en gang i kvarteret |
| Scheduled.NSISAllowedSyncTask.cron | 0 5/15 5-19 ? * * * | Et CRON udtryk der angiver hvor ofte der foretages synkronisering af den gruppe der styrer hvem der må få en erhvervsidentitet. Default er en gang i kvarteret |
| Scheduled.NemLoginAllowedSyncTask.cron | 0 0/15 5-19 ? * * * | Et CRON udtryk der angiver hvor ofte der foretages synkronisering af den gruppe der styrer hvem der skal overføres til NemLog-ins brugeradministration. Default er en gang i kvarteret. |
| Scheduled.Kombit.Cron | 0 5/15 5-19 ? * 1-5 * | Et CRON udtryk der angiver hvor ofte synkroniseringen af KOMBIT jobfunktionsroller afvikles. Default er en gang i kvarteret |
| ActiveDirectory.Group.Root | CN=MainGroup,OU=Grupper,DC=digitalidentity,DC=dk | DistuingishedName på den styrende gruppe, der bestemmer hvilke grupper der synkroniseres til OS2faktor (se mere nedenfor) |
| Kombit.RoleOU | OU=Kombit,DC=digitalidentity,DC=dk | Udfyldes med DN på den OU i AD hvor alle KOMBIT rollerne ligger. Der søges også i alle underliggende mapper |
| Kombit.GroupsInGroups | False | Sættes til "true" hvis man ønsker at understøtte grupper i grupper (dvs rekursivt opslag i AD på gruppemedlemsskaber).<br><br>Dette gør kaldene mod AD tungere og langsommere... |
| Kombit.RoleNameAttribute | extensionAttribute1 | Udfyldes med den attribut på AD gruppen hvor navnet på Jobfunktionsrollen indgår (skal matche KOMBIT rollens ID 100%) |
| Kombit.RoleDomainAttribute | extensionAttribute2 | Udfyldes med den attribut på AD gruppen, hvor man kan angive et alternativt domæne (bruges til delegerede roller) |
| Kombit.RoleCvrAttribute | extensionAttribute3 | Udfyldes med den attribut på AD gruppen, hvor man kan angive et alternativt CVR |

| | | |
|---|---|---|
| | | nummer (bruges til delegerede roller) |
| Kombit.RoleDomainDefault | kommune.dk | Udfyldes med kommunens KOMBIT domæne til jobfunktionsrollerne |
| Kombit.RoleCvrDefault | 12345678 | Udfyldes med kommunens CVR nummer |

### 2.2.1 Håndtering af grupper

Som en optionel feature, kan man vælge at synkronisere AD grupper op i OS2faktor. Dette bør kun gøres for grupper som skal anvendes af OS2faktor til et bestemt formål (fx claims i udgående forbindelse til tjenesteudbydere).

Hvis dette ønskes, skal der oprettes en sikkerhedsgruppe, hvor alle grupper der skal synkronisers skal være medlem. Denne angives i konfigurationen "ActiveDirectory.Group.Root". Efterlad blot denne blank hvis denne funktion ikke ønskes brugt.

Hvis man gør brug af denne funktion, så skal der ligeledes opsættes et CRON udtryk for hvor ofte denne synkronisering skal foregå. Dette gøres i Scheduled.GroupSyncTask.cron.

## 2.3 Start af service

Servicen skal konfigureres til at afvikle under den servicekonto som har de fornødne rettigheder, og herefter kan den startes som en normal service under Services.

Det anbefales at man sætter den til automatisk opstart (gerne med forsinket opstart), så man er sikker på at den kører efter en server genstart.

Ved start/genstart af servicen foretages altid en fuld synkronisering af data, ellers kører den med regelmæssige delta-opdateringer hvert 10. sekund, samt én fuld synkronisering hver nat.

Det er derfor en god idé at kigge i logfilen om alt er gået godt. Logfilens placering kan ses i indstillingen **serilog:write-to:RollingFile.pathFormat**.