# OS2syncAD

## Installationsvejledning

**Version**: 2.9.0
**Date**: 11.05.2022
**Author**: BSG

# Indholdsfortegnelse

# 1 Indledning

Formålet med dokument er at dække installation og konfiguration af STS synkroniseringsmodulet, der kan synkronisere organisationsdata fra Active Directory, til støttesystemet Organisation.

# 2 Installation

## 2.1 Forudsætninger

For at kunne anvende softwaren, er der en række forudsætninger der skal være på plads. Disse er

### 2.1.1 Et FOCES certifikat

For at anvende løsningen, skal der bruges et FOCES certifikat, som er krævet for at kalde organisationsservicen. Dette kan være et vilkårligt FOCES certifikat bestilt hos NETS/DanID, men det skal være gyldigt (ikke udløbet, og ikke spærret).

### 2.1.2 Serviceaftale på støttesystemerne

Der skal være oprettet (og godkendt) en serviceaftale på støttesystemet Administrationsmodul, hvor der er givet skriveadgang til støttesystemet Organisation. Denne serviceaftale skal være knyttet til det FOCES certifikat der er nævnt ovenfor.

Serviceaftalen oprettes på følgende måde

1. Log på KOMBITs Adminisrationsmodul (https://admin.serviceplatformen.dk)
2. Opret et nyt it-system af typen Anvendersystem, og upload FOCES certifikatet som en del af registreringen
3. Anmod om en serviceaftale, hvor der vælges ”Organisation v5” (dette tilvælger automatisk organisation2 servicen også)
4. Når der skal vælges roller, så vælges ”dummy” rollen til ”Organisation v5” servicen, og både ”udstil” og ”rediger” skal tilvælges til ”organisation2” servicen.
5. ”udstil” og ”rediger” rollerne skal afgrænses på ”SeNavn” og ”SeCPR” som det eneste, og her skal værdierne ”Ja” angives.

Husk at få godkendt serviceaftalen.

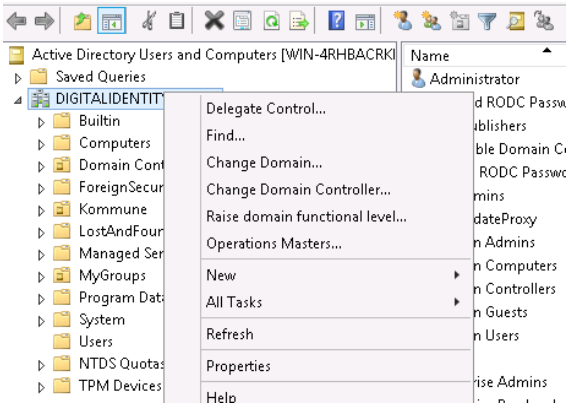
### 2.1.3 Windows Server og systembruger konto

Softwaren skal installeres på en Windows Server (2016 eller nyere), og der skal være oprettet en systembruger der kan afvikle softwaren.

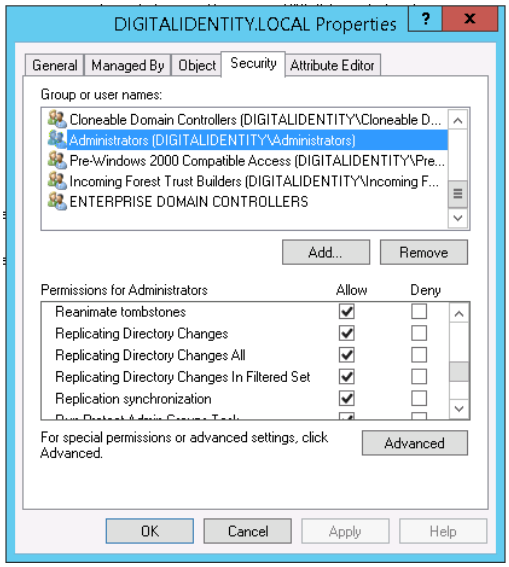
Denne systembruger skal have lokale adminsitratorrettigheder på den server hvor softwaren skal installeres.

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.

## 2.2 Installation

Installationen foretages ved at køre en Windows Installer ved navn

`OS2syncADSetup.exe`

Der opsættes en Service på Windows Serveren, som dog ikke startes automatisk. Dette skal først gøres efter konfigurationen er gennemført.

Softwaren installeres som default til følgende folder (alternativ folder kan vælges under installationen)

```
C:\Program Files (x86)\Digital Identity\OS2syncAD
```

## 2.3 Konfiguration

Konfiguration af løsningen sker via filen appsettings.json, der ligger i installationsfolderen. Følgende indstillinger er nødvendige at tilpasse inden softwaren kan startes

- **ClientCertPath**. Denne skal pege på en PFX/P12 fil, der indeholder det FOCES
- **ClientCertPassword**. Denne skal indeholde kodeord til PFX/P12 filen.
- **Municipality.** Denne skal indeholde kommunens CVR nummer
- **DBConnectionString**. Dette skal være en connection string til en SQL Server, hvor den bruger der afvikler servicen skal have adgang til database schemaet. OS2sync opretter selv tabellerne, men selve schemaet skal være oprettet på forhånd.
- **AD.RootOU**. Dette skal være distinguishedName (DN) på den OU i AD'et hvorfor der skal replikeres data.

Herudover er det muligt at konfigurere yderligere mapningsparametre. Der er opsat fornuftige startværdier, som man kan tilpasse. Disse ligger alle under "AD" indstillingerne i filen

- **AD.OrgUnitAttributes**. Dette er de attributter på OU'ere i AD der skal sendes til STS Organisation. Hvis man fx har EAN stående i extensionAttribute7, så udfylder man med

```
"Ean": "extensionAttribute7"
```

- **AD.OrgUnitAttributes.Filtered**. Denne værdi er speciel, og anvendes til at udvælge en "filtrerings"-attribut på OU'ere. Hvis man ønsker at udvalgte OU'ere ikke skal replikeres til STS Organisation, så skal man vælge en attribut (fx extensionAttribute12), og så sætte den i konfigurationsfilen. Alle OU'ere der har værdierner "1" eller "2" indsat i netop denne attribut vil blive fjernet fra replikeringen til STS Organisation. Hvis man sætter "2" så ryger alle enheder under den filtrede enhed også, hvor "1" blot betyder at det er denne ene enhed der filtreres bort.
- **AD.UserAttributes**. Dette er de attributter på brugere der skal sendes til STS Organisation. Hvis man fx har e-mail adressen på brugere stående i "mail" attribut, så skriver man

```
"Mail": "mail"
```

- **AD.OrgUnitNameMap**. Denne værdi indeholder alternative navne for enheder. Hvis man har en eller flere enheder som skal have et andet navn i Organisation end det som det har i AD, så kan man indtaste ObjectGUID for enheden, og det navn som det faktisk skal have

```
"OrgUnitNameMape": {

  "8ec9698d-8bb4-497b-833d-4e87986cde73": "Nyt navn"

}
```

## 2.4 Automatisk OU oprydning

Servicen fanger automatisk når man nedlægger en OU, så denne nedlukning replikeres til STS Organisation. Men, skulle servicen være slukket i en længere periode, så kan nogle af disse

hændelser gå tabt. For at sikre at enheder lukkes korrekt, selv hvis servicen har været slukket i en længere periode, er det muligt at opsætte et oprydningsjob, der afvikles på et bestemt tidspunkt.

Dette gøres via følgende indstillinger i konfigurationsfilen

```
"CleanupOUJobEnabled": "true",
"CleanupOUJobCron": "0 30 3 ? * SAT",
```

Den første værdi skal sættes til "true" for at slå jobbet til, og den anden værdi angiver hvornår det skal køre. Default kører den kl 03:30 om lørdagen. Man kan øge intervallet, eller sætte den til at køre på et andet tidspunkt. Der anvendes CRON udtryk til styringen af dette.

## 2.5 Håndtering af disabled brugere

Som default behandles AD konti ens, uagtet om de er disabled eller ej. Det betyder at en bruger først fjernes fra FK Organisation når brugeren slettes, eller flyttes udenfor det område af AD som OS2sync overvåger.

Hvis man ønsker at en bruger skal fjernes fra FK Organisation når denne disables, kan man slå følgende setting til

```
"TerminateDisabledUsers":  "true",
```

Hvis man ændrer denne setting efter at servicen har kørt, så er det vigtigt at man sletter den cookie som ligger i databasen, da man ellers ikke udlæser oplysninger om disablet flagget fra AD.

Se afsnit 4 for detaljer om konfigurationsændringer.

## 2.6 Opstart

Når konfiguration er gennemført, åbnes Windows Services, og servicen OS2syncAD findes. På fanen "Log on" vælges den systembruger der er oprettet til at køre servicen, og på fanen "General" skifter man servicens "startup type" fra "Manuel" til "Automatisk".

Herefter starter man servicen.

# 3 Logfiler

Løsningen logger til en logfil der kan findes i c:\logs\OS2syncAD folderen. Logfilen logger ganske få data under normal kørsel (hver gang der synkroniseres data, kommer en række der fortælle hvor mange data der er synkroniseret – hvis der ikke er nogen data, logges intet).

I tilfælde af fejl, logges fejlen til denne fil, og det anbefales at man, i det mindste i starten, holder øje med evt synkroniseringsfejl i denne fil.

Specielt under installationen kan det være nødvendigt at kigge i logfilen hvis der opstår fejl. Man vil typisk kunne se om der er tale om manglende rettigheder, manglende serviceaftale eller lignende ud fra fejlbeskden. En let måde at slippe udenom mange af de rettighedsudfordringer man kan støde på, er at gøre systembrugeren der afvikler servicen til lokal administrator på serveren.

Bemærk at der under den initielle synkronisering af data (første gang man kører), er rigtigt mange data der skal synkroniseres, og man skal forvente at det kan tage 4-8 timer at

gennemføre en fuld synkronisering af data. Hold periodisk øje med logfilen i denne opstartsperiode, for at se om status er som forventet (der synkronisers op til 500 enheder/medarbejdere per log-linje).

# 4 Håndtering af konfigurationsændringer

Hvis man ændrer i konfiguration i registreringsdatabasen, er det nødvendigt at genstarte servicen før disse ændringer slå igennem. Dette gøres via Services på Windows Servicen, hvor man blot trykker på ”restart” ud for OS2syncAD servicen.

Hvis man ændrer i hvilke AD attributter der skal synkroniseres, så er det nødvendig at tvinge en fuld synkronisering igennem. Dette tager igen de 4-8 timer.

En fuld synkronisering kan gennemtvinges på følgende måde

1. stop servicen
2. foretag de ønskede ændringer i konfigurationsfilen
3. find ”records” tabellen i SQL databasen, og slet indholdet af tabellen (slet alle rækker)
4. genstart servicen

# 5 Opdatering til nyere version

I forbindelse med en opdatering fra en ældre version af OS2sync til en nyere udgave, fx fra version 2.0.0 til 2.1.0, kan der være ændringer til konfigurationsfilen som skal behandles. Da konfigurationsfilen ikke overskrives når man opdaterer, skal man sikre at evt ny funktionalitet man ønsker at gøre brug af, bliver tilføjet til konfigurationsfilen i forbindelse med en opdatering.

## 5.1 Opdatering til 2.1.0

I forbindelse med version 2.1.0 er der tilføjet 2 nye indgange i konfigurationsfilen, som man skal tilføje manuelt hvis man ønsker at gøre brug af disse. De to værdier er hhv ”LOSId” og ”RacfID”, som kan tilføjes til de respektive afsnit illustreret nedenfor.

```
"AD": {
  "OrgUnitAttributes": {
    "LOSId": "",
    ....
  },
  "UserAttributes": {
    "RacfId": "",
    ....
```

```
    }
  }
```

Tilføj blot de to fremhævede rækker til den eksisterende konfigurationsfil, og peg dem på de attributter i AD som indeholder hhv LOS-ID'et på en enhed og RacfID'et på en medarbejder.

## 5.2 Opdatering til 2.5.0

Som ved 2.1.0 er der ændringer til konfigurationsfilen. Der er kommet en ny adressetype til dagtilbud (DTR ID), som kan konfigureres på følgende måde

```
"AD": {
  "OrgUnitAttributes": {
    "DtrId": "",
    ....
  },
  ....
}
```

## 5.3 Opgradering til 2.7.0

Der er ændringer til konfigurationsfilen. Hvis man udfører en opdatering, så overskrives den eksisterende konfigurationsfil ikke, og man bør, hvis man ønsker at gøre brug af oprydningsjobbe til OU'ere, tilføje disse indstillinger til konfigurationsfilen under den eksisterende "Environment" indstilling

```
"Environment": …,
"CleanupOUJobEnabled": "true",
"CleanupOUJobCron": "0 30 3 ? * SAT",
```

Dette slår oprydningsjobbet til, og sikrer det afvikles hver lørdag morgen kl 03:30.

## 5.4 Opgradering til 2.8.0

Der er ændringer til konfigurationsfilen – der er tilføjet 7 nye adresse-typer til enheder, som kan opsættes ved at tilføje disse settings

```
  "OrgUnitAttributes": {
    …snip…
    "Location": "",
    "ContactOpenHours": "",
    "EmailRemarks": "",
    "PostReturn": "",
    "PhoneOpenHours": "",
    "Url": "",
    "Landline":  ""
  },
```

De er ikke obligatoriske, og kan udelades.