

# OS2sofd

AD Replikator

**Version:** 1.12.0  
**Date:** 20.05.2025  
**Author:** PSO

# Indhold

1	Indledning .....	3
1.1	Forudsætninger.....	3
1.1.1	Windows Server .....	3
1.1.2	Service konto i AD.....	3
1.1.3	API bruger til SOFD Core backend .....	3
2	Konfiguration .....	3
2.1	Download service .....	3
2.2	Konfiguration af service .....	3
2.2.1	SofdSettings.....	3
2.2.2	ActiveDirectorySettings.....	4
2.3	Start af service .....	6

# 1 Indledning

Dette dokument er rettet mod teknikere der skal opsætte og konfigurere kommunens integration fra OS2sofd til Active Directory, så OU struktur og brugeres indplacering holdes ajour på baggrund af stamdata fra OS2sofd.

## 1.1 Forudsætninger

### 1.1.1 Windows Server

Servicen skal installeres på en Windows maskine med:

- Netværksmæssig adgang til kommunens AD
- Netværksmæssig adgang til SOFD Core via HTTPS

### 1.1.2 Service konto i AD

Der skal oprettes en servicekonto, som har lov til at

- Oprette og redigere OU'ere
- Flytte brugere
- Oprette og vedligeholde sikkerhedsgrupper

### 1.1.3 API bruger til SOFD Core backend

Der skal i konfigurationen tilføjes en API nøgle til OS2sofd. Denne oprettes via OS2sofds administrative brugergrænseflade. Integrationen skal have læseadgang til OS2sofd.

# 2 Konfiguration

Start med at installere servicen, og dernæst opsæt konfigurationen. Endeligt kan der knyttes en servicekonto til servicen og servicen kan startes.

## 2.1 Download service

Download og installér servicen fra <https://www.sofd.io/download.html>

## 2.2 Konfiguration af service

Konfiguration af servicen foretages i filen appsettings.json

### 2.2.1 SofdSettings

Indstilling	Eksempel	Kommentar
BaseUrl	<a href="https://kommune.sofd.io">https://kommune.sofd.io</a>	URL til SOFD installationen
ApiKey	xxx	Nøgle til API'et
OrgUnitPageSize	2000	Max antal enheder der læses ud (sæt til en værdi højere end det samlede antal enheder i OS2sofd)
ExcludeFromSyncTagName		Navnet på det (optionelle) Tag der kan sættes på enheder i OS2sofd, som gør at enheden ikke replikeres til AD
PersonsPageCount	500	Antal brugere der læses af gangen

PersonsPageSize	20	Antal gange der max læses brugere – de to settings til sammen skal være højere end antallet af brugere i OS2sofd
SOFDToADOrgUnitMap	<pre>"SOFDToADOrgUnitMap": {   "sofd_uuid_1":     "ad_dn_1",   "sofd_uuid_2":     "ad_dn_2" }</pre>	Mapning mellem OS2sofd UUIDer og AD OUer (distinguishedName). Der skal minimum angives én mapning her (typisk fra rod-enhed i OS2sofd til en OU i OS2sofd), men det er muligt at splitte op i flere mapninger sådan at organisationen i OS2sofd sendes til forskellige steder i AD.

## 2.2.2 ActiveDirectorySettings

Indstilling	Eksempel	Kommentar
RootOU	https://kommune.sofd.io	DN på den OU som hele strukturen skal bygges i
RootDeletedOusOu	xxx	DN på en OU som integrationen skal flytte slettede enheder til
RequiredOUFields	2000	Vælg en attribut (single-value tekst attribut) som integrationen kan bruge til at gemme UUID på enheden fra OS2sofd. Dette er et krævet felt.
OptionalOUFields		Navnet på de 2 attributter der skal indeholde hhv postadresse og EAN på enheden (de behøves ikke udfyldes)
MoveUsersEnabled	true/false	Sæt til "false" hvis man ikke ønsker at flytte brugere (også en god startværdi, indtil man er sikker på at OU strukturen er på plads)
DontMoveUserRegularExpressions		Hvis der er brugere som aldrig på flyttes, så kan man angive et regex på de brugernavne som skal være undtaget flytning
ExcludeExternalUsers	True/false	Undtager eksterne brugere for flytning. Med eksterne menes de brugerkonti som er direkte knyttet til et eksternt tilhørsforhold, eller brugere ikke knyttet til et tilhørsforhold, men hvor det primære tilhørsforhold er eksternt.
GroupSettings		Se afsnittet nedenfor

## 2.2.3 GroupSettings

Dette afsnit er et optionelt sub-set af ActiveDirectoryConfiguration, og bruges til at oprette og vedligeholde et sæt af AD sikkerhedsgrupper

Indstilling	Eksempel	Kommentar
Enabled	true	Slå hele funktionen til/fra
DryRun	false	Hvis den sættes til TRUE, så logger den alene ændringer til grupper, men udfører dem ikke
GroupOUDN	OU=Groups,OU=Kommune,DC=dk	Den OU i AD'et hvor alle sikkerhedsgrupperne oprettes. Bemærk at der IKKE må ligge andre grupper i denne OU, da integrationen i så fald vil slette dem.
GroupIdField	adminDescription	Den attribut som integrationen bruger til at sætte et unikt ID på gruppen, så den ved hvilken enhed gruppen hører til
ManagerGroup		Struktur der beskriver hvordan grupper med ledere for enheder oprettes og vedligeholdes – se detaljer for opsætningen nedenfor
DirectMemberGroup		Struktur der beskriver hvordan grupper med brugere der har direkte tilhørsforhold i enhederne oprettes og vedligeholdes – se detaljer for opsætningen nedenfor
MemberGroup		Struktur der beskriver hvordan grupper med brugere der har tilhørsforhold til enheder (og alle de underliggende enheder) oprettes og vedligeholdes – se detaljer for opsætningen nedenfor

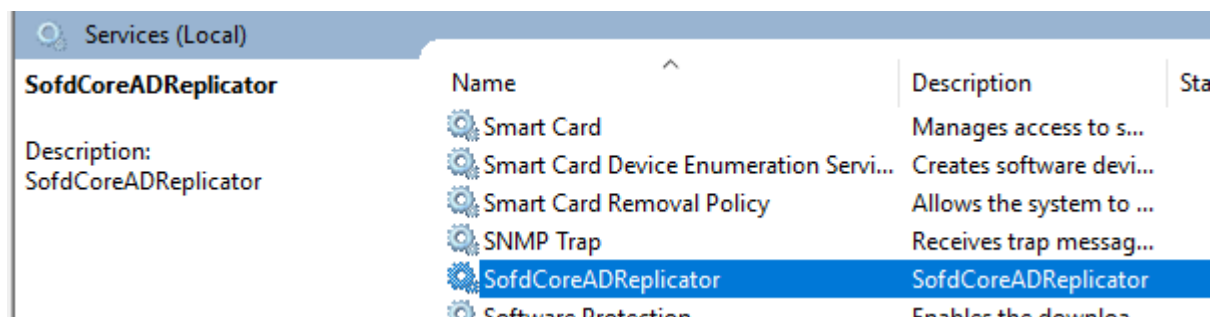
Hver af de 3 typer af grupper har en sektion der angiver hvordan disse skal skabes. Strukturen er ens for hver af disse, og konfigureres på følgende måde

Indstilling	Eksempel	Kommentar
Enabled	true	Slå oprettelsen af denne type af grupper til/fra
Name		Hvad skal der stå i name feltet for gruppen – man kan anvende {NAME} og {ID} som pladsholdere
SAMaccountName		Hvad skal der stå i SAMAccountName feltet for gruppen – man kan anvende {NAME} og {ID} som pladsholdere
DisplayName		Hvad skal der stå i displayName feltet for gruppen – man kan anvende {NAME} og {ID} som pladsholdere
Description		Hvad skal der stå i beskrivelsesfeltet for gruppen –

		man kan anvende {NAME} og {ID} som pladsholdere
--	--	---

## 2.3 Start af service

Efter servicen er konfigureret startes den via Windows Services eller tilsvarende kommandolinjeværktøjer.



Ved start/genstart af servicen foretages altid en fuld synkronisering, og ellers udføres der en fuld synkronisering 2 gange om dagen (lidt før kl 5 om morgenen, og lidt før kl 17 om eftermiddagen).