OS2sofd

AD Replikator

**Version**: 1.14.0

**Date**: 23.10.2025

**Author**: PSO

Indhold

[1 Indledning 3](#_Toc212110568)

[1.1 Forudsætninger 3](#_Toc212110569)

[1.1.1 Windows Server 3](#_Toc212110570)

[1.1.2 Service konto i AD 3](#_Toc212110571)

[1.1.3 API bruger til SOFD Core backend 3](#_Toc212110572)

[2 Konfiguration 3](#_Toc212110573)

[2.1 Download service 3](#_Toc212110574)

[2.2 Konfiguration af service 3](#_Toc212110575)

[2.2.1 SofdSettings 3](#_Toc212110576)

[2.2.2 PAMSettings 4](#_Toc212110577)

[2.2.3 ActiveDirectorySettings 4](#_Toc212110578)

[2.2.4 GroupSettings 5](#_Toc212110579)

[2.3 Start af service 7](#_Toc212110580)

# 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.

## Forudsætninger

### Windows Server

Servicen skal installeres på en Windows maskine med:

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

### 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

### 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.

# Konfiguration

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

## Download service

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

## Konfiguration af service

Konfiguration af servicen foretages i filen appsettings.json

### SofdSettings

|  |  |  |
| --- | --- | --- |
| Indstilling | Eksempel | Kommentar |
| BaseUrl | https://kommune.sofd.io | 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 |
| PersonsPageSize | 1000 | Antal gange der max læses brugere – de to settings til sammen skal være højere end antallet af brugere i OS2sofd |
| SOFDToADOrgUnitMap | "SOFDToADOrgUnitMap": {  "sofd\_uuid\_1": "ad\_dn\_1",  "sofd\_uuid\_2": "ad\_dn\_2"  } | 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. |

### PAMSettings

|  |  |  |
| --- | --- | --- |
| Indstilling | Eksempel | Kommentar |
| Enabled | true/false | Angiver om PAM er slået til |
| CyberArkAppId |  | AppId til CyberArk api-kald |
| CyberArkSafe |  | Safe til CyberArk api-kald |
| CyberArkObject |  | Object til CyberArk api-kald |
| CyberArkAPI |  | Base url til CyberArk api |

### ActiveDirectorySettings

|  |  |  |
| --- | --- | --- |
| Indstilling | Eksempel | Kommentar |
| RootOU |  | DN på den OU som hele strukturen skal bygges i. **Indstillingen udfases: Anvend SofdSettings.SOFDToADOrgUnitMap** |
| RootDeletedOusOu | OU=Slettede enheder,DC=kommune,DC=dk | DN på en OU som integrationen skal flytte slettede enheder til |
| RequiredOUFields.OUIdField | adminDescription | 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.  EanField  EanFieldInherit  StreetAddressField  CityField  PostalCodeField  LosIDField |  | Valgfri angivelse af AD attributnavne hvor yderligere oplysninger om enheden skal skrives til. |
| TestOURun | true/false | Afvikler OU oprettelse/flytning/omdøbning mv. i test-tilstand hvor der ikke ændres i AD, men kun logges hvad der vil ske. |
| 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) |
| DryRunMoveUsers | true/false | Afvikler flytning af brugere i test-tilstand vhor der ikke ændres i AD, men kun logges hvad der vil ske. |
| DontMoveUserRegularExpressions |  | Hvis der er brugere som aldrig på flyttes, så kan man angive et regex på de brugernavne som skal være undtaget flytning |
| DontMoveUserFromTheseOUs | true/false | Liste af DN på OUer som der ikke må flyttes brugere fra. |
| 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 |
| OUNameReplaceRegexes | [”s/,//”,”s/[;:]/-/”] | Liste af regulære udtræk i sed-replace-syntaks til at erstatte tegn i OU-navnet. Eksemplet til venstre erstatter alle kommaer med en tom streng samt alle semikoloner og koloner med en bindestreg. |
| OURunScriptOnCreate | C:/scripts/OnOUCreate.ps1 | Sti til script der afvikles efter OU oprettelse. |
| OURunScriptOnDelete | C:/scripts/OnOUDelete.ps1 | Sti til script der afvikles efter OU sletning (flytning til slettet OU). |
| OURunScriptOnMove | C:/scripts/OnOUMove.ps1 | Sti til script der afvikles efter OU flytning. |
| UserRunScriptOnMove | C:/scripts/OnUserMove.ps1 | Sti til script der afvikles efter bruger flytning. |

### 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 |
| UseFastMethod | true/false | Kan sættes til true for at anvende en hurtigere metode til at læse gruppemedlemskaber fra AD. |
| DaysBeforeFirstWorkday | 14 | Angiver hvor mange dage før første arbejdsdag at brugere meldes ind i grupper svarende til deres afdeling. |
| 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 konfigueres på følgende måde

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

## Start af service

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

Graphical user interface, text, application, chat or text message

Description automatically generated

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).