OS2sofd

AD Replikator

Version: 1.14.1
Date: 27.11.2025
Author: PSO

Indhold

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	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",	Mapning mellem OS2sofd UUIDer og AD OUer (distinguishedName). Der

	"sofd_uuid_2": "ad_dn_2" }	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 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

2.2.3 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 OrgUnitTypeField		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.

2.2.4 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
DirectManagerGroup		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
InheritedMemberGroup		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
InheritedManagerGroup		Struktur der beskriver hvordan grupper med ledere for enheder (og alle de underliggende enheder) oprettes og vedligeholdes – se detaljer for opsætningen nedenfor

DirectManagerGroup er bagudkompatible med ManagerGroup og InheritedMemberGroup er bagudkompatible med MemberGroup, således begge navne kan anvendes. Såfremt indstillingen er enablet både med sit nye og bagudkompatible navn, vil indstillingerne med de nye navn blive brugt. Vi anbefaler, at man i videst mulige udstrækning bruger de nyeste navne.

Hver af de 4 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 står i name feltet for gruppen
SAMaccountName		Hvad skal der står i SAMAccountName feltet for gruppen
DisplayName		Hvad skal der står i displayname feltet for gruppen
Description		Hvad skal der står i beskrivelsesfeltet for gruppen

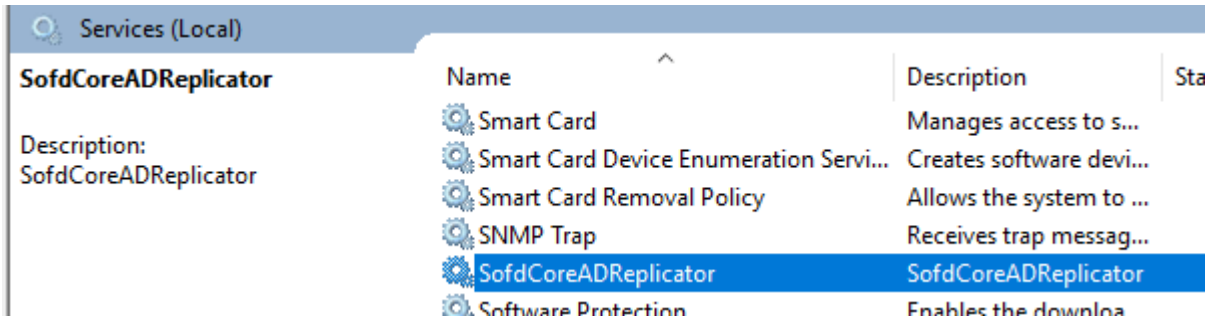
I gruppetypernes indstillinger kan følgende pladsholdere anvendes til at generere gruppens felter.

Pladsholder	**Bør kun anvendes på**	**Forklaring**	**Eksempel**
{ID}	Name, SAMaccountName, DisplayName, Description	Enhedens id i SOFD	1032
{LEVEL}	Name, SAMaccountName, DisplayName, Description	Antal enheder væk fra rod-enheden. Rod-enheden vil returnere 0.	2
{NAME}	Name, SAMaccountName, DisplayName, Description	Enheden navn i SOFD	Børn og Unge
{PATH[X]} – hvor X er et tal 1 eller større	Name, SAMaccountName, DisplayName, Description	Enheden X niveauer over den gældende enhed. Hvis tallet er større end antallet af enheder til	Direktionsområde Velfærd

		roden, returneres en tom streng.	
{PATH[X]} – hvor X ikek er et tal	SAMaccountName, DisplayName, Description	Enhedens fulde sti, separeret af X (så hvis / bruges som separator, vil stien ligne rod-enhed/enhed/enhed) Skal ikke anvendes på Name, da det kan forårsage problemer.	Eksempel Komme/ Direktionsområde Velfærd/ Børn og Unge

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).