SOFD Core

AD Attribut integration

Version: 2.6.3
Date: 21.01.2022
Author: PSO

Indhold

1 Indledning

Dette dokument er rettet mod teknikere der skal opsætte og konfigurere kommunens integration fra SOFD Core til Active Directory med henblik på at AD konti attributter holdes opdateret med data fra SOFD Core.

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 i skyen via HTTPS.
- .NET Framework 4.6.1 eller nyere

1.1.2 Service konto i AD

Der skal oprettes en service konto i kommunes AD.

Kontoen skal have skriveadgang til alle de bruger-attributer der skal opdateres fra SOFD Core, inkl CPR nummer attributten.

Bemærk at kontoen skal være medlem af Domain Admins hvis den skal kunne opdatere oplysninger på brugere som er eller har været medlem af en beskyttet gruppe (f.eks. andre domain admins).
En konto som "kun" er Account Operator kan ikke opdatere oplysninger på en bruger som har attributten AdminCount sat til 1.

1.1.3 API bruger til SOFD Core backend

Der skal i konfigurationen indtastes en API nøgle til SOFD Core. Denne kan oprettes i SOFD Cores administrative brugergrænseflade. Agenten kan nøjes med læseadgang.

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 SOFD Core i skyen via HTTPS.

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 appSettings sektionen i xml-filen **SOFD Core AD Writeback Agent.exe.config** som ligger i roden af installationsmappen (default C:\Program Files (x86)\Digital Identity\SofdCoreAdWritebackAgent).

Indstilling	Eksempel	Kommentar
SofdUrl	https://kommune.sofd.io	Peger på SOFD installationen for kommunen
SofdApiKey	xxxxxx	Det kodeord som er valgt til klienten i SOFD

ActiveDirectoryWritebackExcludeOUs	OU=Kultur,OU=Administration,OU=Kommune,DC=digitalidentity,DC=dk; OU=IT og Digitalisering,OU=Administration,OU=Kommune,DC=digitalidentity,DC=dk	Ansatte i dises enheder samt underenheder undtages for løbende vedligehold fra SOFD core. Flere OUer kan angives adskilt med semikolon
ActiveDirectoryEnableManagerUpdate	False	Hvis True og ActiveDirectoryEnableAttributeUpdate også er sat til True, bliver "manager" attributten på brugernes AD-konti opdateret med lederen for den primære ansættelse i SOFD Core.
ActiveDirectoryManagerUpdateMasters	OPUS	Hvis angivet, vedligeholder agenten kun manager feltet på brugere som har en primær affiliation fra denne master. Flere værdier kan angives adskilt med semicolon. Kan anvendes hvis man f.eks. ikke ønsker at manager feltet skal udfyldes for eksterne brugere som er oprettet direkte via SOFD Core.
ActiveDirectoryManagerUpdateOnlyPrimes	True	Hvis denne er sat til true (default), bliver manager kun påført primære AD-konti. Ønskes manager også opdateret på øvrige konti, skal denne sættes til False
ActiveDirectoryManagerUpdateNoClear	False	Kun relevant hvis ActiveDirectoryEnableManagerUpdate er sat til true. Hvis denne sættes til true, bliver manager attributten ikke ryddet, selv om den burde blive det jf. data.
ActiveDirectoryUserType	ACTIVE_DIRECTORY	Skal sættes til værdien "ACTIVE_DIRECTORY". Anvendes til at styre hvilke kontotyper der replikeres data fra.
ActiveDirectoryEnablePowershell	False	Hvis denne sættes til "True" afvikles et custom powershell script hver gang agenten laver en ændring på en bruger i AD. Script sti: ./CustomPowershell/UserChanged.psm1

UploadConfiguration	False	Sæt til ”True” for at den lokale konfiguration bliver uploadet til SOFD Core
EnableFallbackToPrimeAffiliation	True	Default True. Sæt denne til False hvis der skal være en hård kobling til den ansættelse der er opmærket direkte på brugerkontoen.
FullSyncCron	0 30 3 ? * *	Cron udtryk, der angiver hvornår der skal køres en fuld synkronisering. Default er hver nat kl. 03:30 som i eksemplet til venstre.

2.3 Start af service

Efter servicen er konfigureret startes den via Windows Services eller tilsvarende kommandolinjeværktøjer. Her er det vigtigt at servicen konfigureres til at starte med den AD konto som har de fornødne rettigheder.

3 Konfiguration af attribute-opdatering

Konfigurationen af hvilke attributter der skal holdes opdateret hedder

ad-mapping.xml

Denne fil indeholder en konfiguration af hvilke felter fra SOFD der skal kopieres til hvilke felter i AD.

Der følger en eksempelfil med, som man bør tilrette. Eksempelfilen ser sådan her ud

```
<?xml version="1.0" encoding="utf-8" ?>
<mappings>
  <mapping sofd="firstname" ad="givenName" />
  <mapping sofd="affiliation.positionName" ad="title" />
  <mapping sofd="affiliation.orgUnit.ean" ad="extensionattribute4" />
</mappings>
```

For hver attribut fra SOFD man ønsker kopieret til en attribut i AD, skal der være en <mapping> i filen. Denne peger på hhv en attribut i SOFD, og en attribut på bruger-objekterne i AD.

Attributnavnene i AD kan man finde i sit AD, og attributterne i SOFD kan man finde ved at lave API opslag i SOFD (det er API attribut-navnene der skal anvendes).

Digital Identity kan også hjælpe med udfyldelsen af filen.

Hvor der er flere mulige værdier i SOFD, vælges altid den primære at kopiere til AD. Fx den tredje mapping i eksempelfilen, hvor der står

```
  <mapping sofd="affiliation.orgUnit.ean" ad="extensionattribute4" />
```

En ”affiliation” er et tilhørsforhold, og en medarbejder kan have flere tilhørsforhold (fx flere ansættelser). Når man laver en mapning på denne måde, så vælges det tilhørsforhold som er opmærket som det primære i SOFD.

”affiliation.orgUnit.ean” fortolkes som

- Vælg det primære tilhørsforhold for brugeren
- Find den enhed som tilhørsforholdet er knyttet til
- Udlæse EAN nummeret på den enhed
- Kopier værdien over i extensionattribute4 på bruger-objektet i AD

Bemærk det er kun muligt at kopiere enkelt-attributter **fra** SOFD Core **til** AD via denne mekanisme. Man kan ikke flette flere SOFD Core attributter og kopiere dem til ét felt i AD, og man kan ikke flette attributter fra SOFD Core med attributter i AD, og kopiere dem til et nyt felt i AD.