SOFD Core

AD Indlæsningsintegration

Version: 1.9.0
Date: 07.03.2022
Author: BSG

Indhold

1 Indledning

Dette dokument er rettet mod teknikere der skal opsætte og konfigurere kommunens integration fra Active Directory til SOFD Core, så brugeroplysninger fra Active Directory bliver synkroniseret til SOFD Core.

1.1 Forudsætninger

1.1.1 Windows Server

Servicen skal installeres på en Windows maskine med:

- Netværksmæssig adgang til kommunens AD (hvis der skal læses direkte fra AD)
- Netværksmæssig adgang til fil-udtrækket fra AD (hvis der skal læses via et AD filudtræk)
- Netværksmæssig adgang til SOFD Core i skyen via HTTPS.
- .NET Framework 4.6.1 eller nyere

1.1.2 Service konto i AD

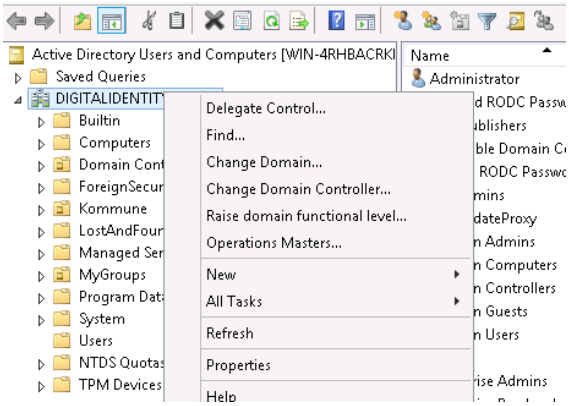
Dette afsnit er kun relevant hvis der skal læses direkte fra AD.

Der skal oprettes en service konto i kommunes AD.

Kontoen skal have læseadgang til alle de bruger-attributer der skal læses fra brugerkonti inkl. den attribut som indeholder brugerens cpr-nummer.

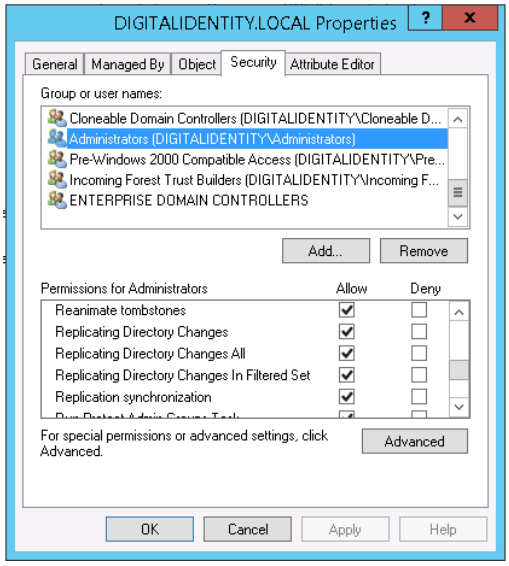
Endelig skal systembrugeren også have rettigheder til at replikere data fra Active Directory. Dette vil brugeren automatisk have hvis denne er domæne administrator, men man kan også nøjes med at tilføje enkelte replikerings-rettigheder til brugeren via nedenstående vejledning

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.

1.1.3 Filudtræk fra AD

Dette afsnit er kun relevant hvis udlæsning fra AD skal ske via et filudtræk. Kommunen skal I så fald selv etablere et dagligt filudtræk fra AD, hvor der skal dannes en fil med følgende navn

SOFD_yyyymmdd.csv

Hvor yyyy er årstal, mm er måned og dd er dagen for filudtrækket. Eksempelvis

SOFD_20200522.csv

Filen skal enkodes i ISO-8859-1 tegnsættet, og skal have følgende struktur

```
cpr,ad-kontonavn,mobilnummer,telefonnummer,kaldenavn,medarbejderid,fornavn,efternavn
0101708091,abcd,30405060,,Hans Hansen,07893,Hans Erik,Hansen
0504698198,efgh,,80807070,,0799,Gitte,Hansen
```

Filen skal indeholde et fuldt udtræk af de brugere som findes i AD, der har et CPR nummer, og som skal indlæses i SOFD Core.

De krævede felter er

- Cpr
- Ad-kontonavn
- Fornavn
- Efternavn

De andre felter kan være tomme

1.1.4 API bruger til SOFD Core backend

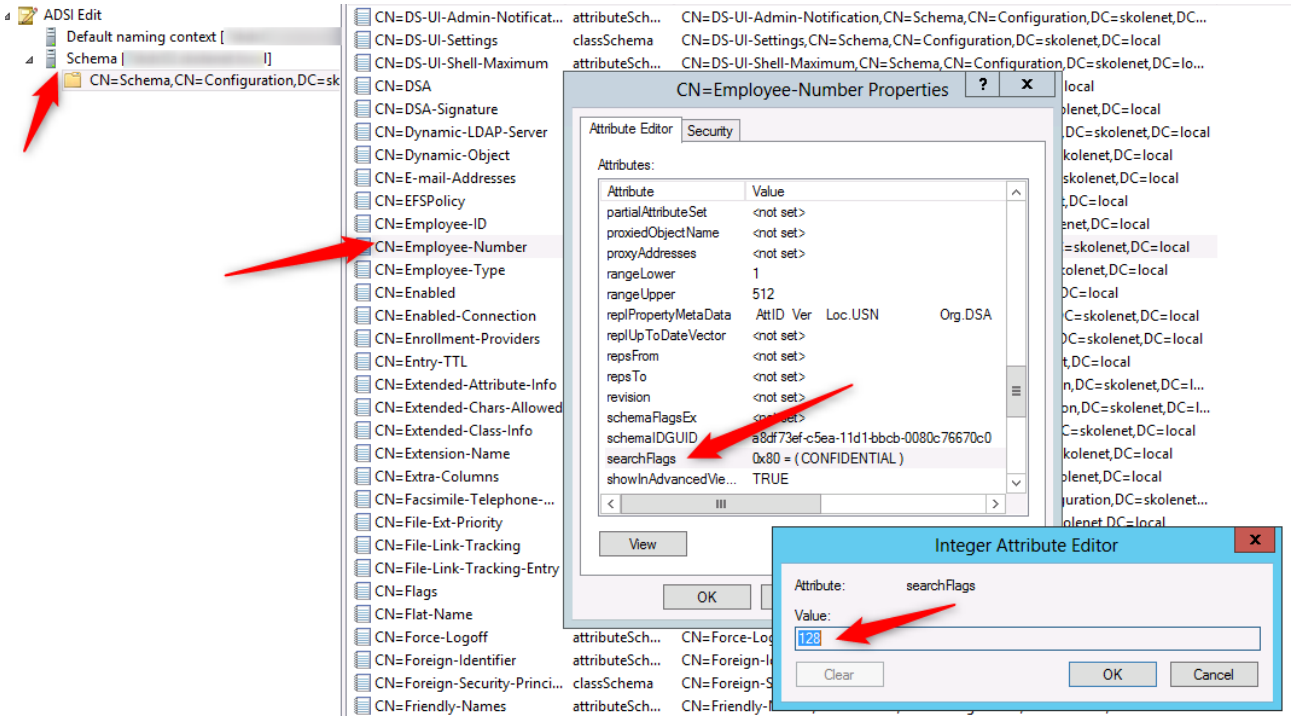
Der skal i konfigurationen indtastes et brugernavn og kodeord. Disse udleveres af Digital Identity.

1.1.5 Afklaring af cpr-attribut

Det skal afklares hvilken attribut i AD der indeholder/skal indeholde brugerens cpr-nummer. Det kan eksempelvis være attributten EmployeeNumber.

Det anbefales at den valgte attribut skjules for almindelige brugere ved at tilføje confidentiality bit på attributten. Bemærk at det ikke er alle felter i AD der understøtter denne mulighed.

Dette kan f.eks. gøres via ADSI Edit MMC snap-in ved at tilføje bit 8 (tal-værdi 128) til searchFlags på attributten. Bemærk at hvis searchFlags har en værdi i forvejen, og den ikke i forvejen har bit 8 sat, skal bit 8 (tal-værdi 128) lægges til denne værdi.



Med dette flag sat er det kun brugere med CONTROL_ACCESS rettighed i AD, der kan læse/skrive attributten (default administratorer).

Den valgte attribut til cpr-nummer angives i indstillingen **ActiveDirectory.Property.Cpr** under konfiguration i det næste afsnit af denne vejledning.

1.1.6 Afklaring af affiliation-attribut

Det er muligt at lade Active Directory være master for et organisatorisk tilhørsforhold til den autoritative organisation i SOFD Core.

Normalt defineres dette tilhørsforhold via en integration til f.eks. lønsystemet, men der kan være brugere som kun findes i Active Directory, men hvor man alligevel ønsker at indplacere dem organisatorisk. Det kan eksempelvis være eksterne konsulenter.

Hvis man ønsker denne funktionalitet, man kan i indstillingen **ActiveDirectory.Property.Affiliation** angive navnet på en AD attribut. Brugere hvor der i denne attribut står en værdi der matcher et masterId fra lønsystemet (LOS ID), vil få oprettet et organisatorisk tilhørsforhold til den tilsvarende organisatoriske enhed i SOFD Core.

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 **SOFDCoreAD.Service.exe.config** som ligger i roden af installationsmappen (default C:\Program Files (x86)\Digital Identity\SofdCoreADEventDispatcher).

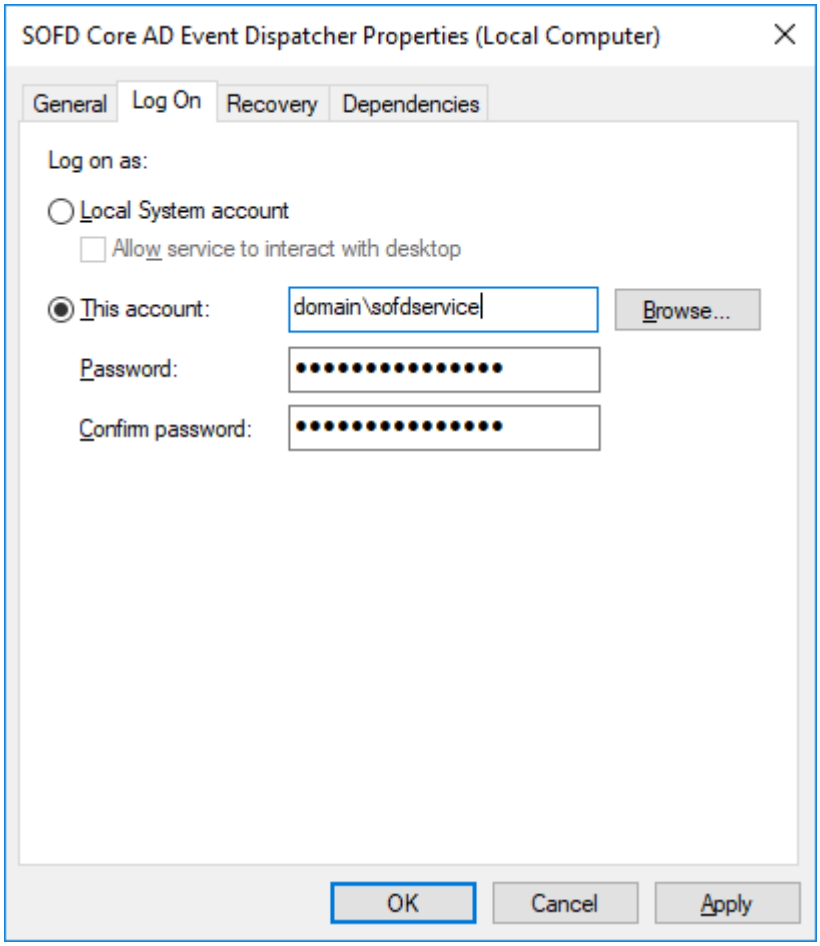
De indstillinger der skal konfigureres under en standardinstallation er fremhævet med gult.

Indstilling	Eksempel	Kommentar
DataSource	AD	Sættes til værdien "AD" eller "FILE" alt efter om der skal læses direkte fra AD, eller om der skal læses fra en fil.
File.Location	c:/tmp	Kun relevant hvis der er valgt "FILE" ovenfor. Skal pege på den folder hvor udtrækket fra AD ligger
File.HeaderRow	true	Sæt til "true" hvis ovenstående fil har en "header" række som den første række i filen, ellers "false"
SOFDCoreAD.FullSyncSchedule	0 0 6 ? * * *	Angiver hvor ofte der foretages en fuld synkronisering af alle brugere. Indstillingen angives som et cron udtryk. Se evt. http://www.freeformatter.com/cron-expression-generator-quartz.html
SOFDCoreAD.SyncIntervalSeconds	10	Angiver hvor mange sekunder der går imellem delta-synkronisreinger.
serilog:*		Diverse indstillinger til opsætning af log.
ActiveDirectory.AllowMultipleUsers	False	Angivelse af om synkroniseringen skal understøtte at synkronisere flere brugere med samme cpr-nummer.
ActiveDirectory.TreatDisabledAsEnabled	False	Angivelse af om disablede AD-brugere skal synkroniseres til SOFD Core.
ActiveDirectory.IntegratedSecurity	False	Angivelse af om servicen skal afvikles i kontekst af servicens logon-bruger.

ActiveDirectory.Username	username@domain	Angivelse af brugernavn til opslag i AD såfremt servicen ikke afvikles i kontekst af servicens logon-bruger jf. ovenstående indstilling. Kan være blank.
ActiveDirectory.Password		Angivelse af password til AD-bruger såfremt servicen ikke afvikles i kontekst af servicens logon-bruger. Kan være blank.
ActiveDirectory.Filter	samaccountname=a*	Angivelse af et ldap-filter til afgrænsning af hvilke AD-konti der skal synkroniseres til SOFD Core. Kan være blank.
ActiveDirectory.Property.Cpr	EmployeeNumber	Angivelse af hvilken attribut i AD der indeholder cpr-nummer.
ActiveDirectory.Property.EmployeeId		Angivelse af hvilken attribut i AD der indeholder medarbejderens medarbejdernummer.
ActiveDirectory.Property.Mobile	mobile	Angivelse af hvilken attribut i AD der indeholder medarbejderens mobilnummer
ActiveDirectory.Property.SecretMobile	pager	Angivelse af hvilken attribut i AD der indeholder et mobilnummer som medarbejderen ønsker at holde hemmeligt
ActiveDirectory.Property.Phone		Angivelse af hvilken attribut i AD der indeholder medarbejderens telefonnummer
ActiveDirectory.Property.DepartmentNumber		Angivelse af hvilken attribut i AD der indeholder afdelingsnummeret
ActiveDirectory.Property.FaxNumber		Angivelse af hvilken attribut i AD der indeholder faxnummeret
ActiveDirectory.Property.Photo		Angivelse af hvilken attribut i AD der indeholder medarbejderens billede
ActiveDirectory.Property.Affiliation	extensionAttribute1	Angivelse af hvilken attribut i AD der angiver organisatorisk tilhørsforhold. Kan være blank.
ActiveDirectory.LocalExtention.* (* angiver hvad feltet skal hedde i SOFD Core)	wWWHomePage	Man kan tilføje et vilkårligt antal af indstillinger med dette prefix for at læse værdien fra denne AD-attribut ind i et custom felt i SOFD Core. Kan undlades.

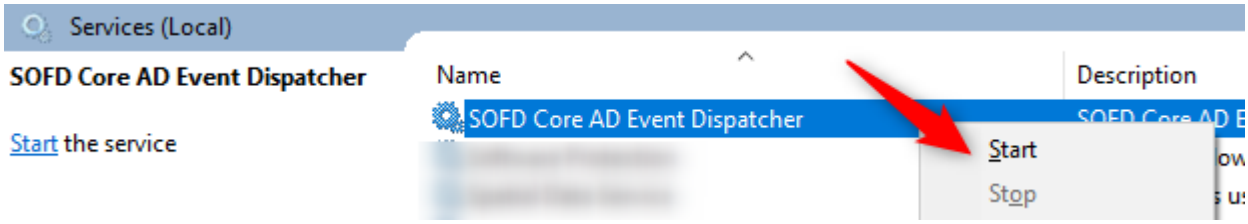
ActiveDirectory.Cron	0/10 * 5-22 ? * * *	Cron-udtræk der angiver hvor ofte der læses ændringer fra AD. Default er hvert 10. sekund hvis ikke der angives en værdi i konfigurationen.
ActiveDirectory.ExcludeOUs	"OU=old users,OU=testkøbing,DC=test,DC=dk; OU=old users 2,OU=testkøbing,DC=test,DC=dk"	En ;-separeret liste af enheders distinguished name. Brugere i enhederne, der listes her, bliver ikke synkroniseret.
Backend.Password		API-password til SOFD Core backend API (udleveres af Digital Identity)
UploadConfig.Enabled	False	Sæt til "True" hvis man ønsker at konfigurationsfilen uploades til SOFD Core
UploadConfig.SofdCoreUrl	https://kommune.sofd.io	Skal udfyldes hvis ovenstående er sat til True. Her skal stå URL'en på SOFD Core
UploadConfig.SofdCoreApiKey	Xxxx	Skal udfyldes ovenstående er sat til True. Skal udfyldes med ApiKey for AD Dispatcher agenten. Bemærk denne er forskellige fra Backend.Password

Såfremt **ActiveDirectory.IntegratedSecurity** er sat til "true" I xml-konfigurationen skal service kontoen angives på "Log On" fanen i Windows Services.



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 uanset hvad **SOFDCoreAD.FullSyncSchedule** indstillingen er konfigureret til.

Det er derfor en god idé at kigge i logfilen om alt er gået godt. Logfilens placering kan ses i indstillingen **serilog:write-to:RollingFile.pathFormat**.

Logfilen bør få sekunder efter opstart indeholde 3 linjer der ser nogenlunde sådan her ud:

2019-09-04 06:00:04 [Information] [SOFDCoreAD.Service.Job.SynchronizeJob] Performing full sync

2019-09-04 06:00:06 [Information] [SOFDCoreAD.Service.ActiveDirectory.ActiveDirectoryService] Found 4860 users in Active Directory

2019-09-04 06:00:12 [Information] [SOFDCoreAD.Service.Job.SynchronizeJob] Full sync complete