SOFD Core

Brugerkonto integration

Version: 2.4.0
Date: 19.04.2022
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 Installation af Windows Service 3
2.1 Download service 3
2.2 Konfiguration af service 3
2.3 Start af service 6
3 Afvikling af powershell 7

1 Indledning

Dette dokument er rettet mod teknikere der skal opsætte og konfigurere kommunens integration fra SOFD Core til Active Directory og Exchange kontobestillinger fra SOFD Core udføres som opsat i SOFD Core.

1.1 Forudsætninger

1.1.1 Windows Server

Servicen skal installeres på en Windows maskine med:

- Netværksmæssig adgang til kommunens AD og Exchange server
- 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.

Kontoen skal ligeledes have lov til at oprette AD konti, sætte kodeord på AD konti, samt oprette Exchange konti via powershell remoting (Enable-Mailbox og Enable-RemoteMailbox kommandoer).

Det sidste kræver at brugerkontoen er medlem af gruppen ”Organization Management”.

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. Det er vigtigt at denne API nøgle tildeles skriveadgang til SOFD Core, da den skal opdatere SOFD Core med status på bestillinger af brugerkonti.

2 Installation af Windows Service

Der skal installeres og konfigureres en Windows Service på en server hvor der er netværksmæssig adgang til kommunens AD og Exchange server 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 User Agent.exe.config** som ligger i roden af installationsmappen (default C:\Program Files (x86)\Digital Identity\SofdCoreAccountAgent).

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
ExchangeCreateEnabled	True	Hvis der løbende skal oprettes nye Exchange konti på baggrund af bestillinger i SOFD, skal denne sættes til "True"
ExchangeDeactivateEnabled	True	Hvis der løbende skal deaktiveres Exchange konti på baggrund af bestillinger i SOFD, skal denne sættes til "True"
ExchangeServer	exchange.kommune.dk	Servernavnet på exchange serveren
ExchangeDefaultMailDomain	@kommune.dk	Mail domæne
ExchangeCustomMailDomains	06e489a4-169f-4242-bb30-41148f0a7c6c=@kommune2.dk;5f447097-a9bd-419a-81c7-00b2b613c8e3=@kommune3.dk	Semikolon-separeret angivelse af hvilke UUID'er (på enheder) der skal have et andet mail domæne. Efterlad blank hvis dette ikke er ønsket.
ExchangeOnline	True	Sættes til "True" hvis der er tale om et hybrid setup, hvor Exchange konti skal oprettes i skyen via en hybrid gateway.
ExchangeOnlineDomain	@kommune.mail.onmicrosoft.com	Udfyldes hvis ovenstående er True, og skal sættes til online domænet
ExchangeUsePSSnapin	False	Sættes til "True" hvis agenten skal anvende "Add-PSSnapin Microsoft.Exchange.Management.powershell" i stedet for "New-PSSession ...". Dette kræver at snap-in er installeret på serveren, men er nødvendigt såfremt man ønsker at afvikle agenten under en managed service account. Kalundborg Kommune har beskrevet installation af Exchange-Snapin her:
ExchangeCreatePowershell	Exchange\createExchange.ps1	Sti til powershell script der afvikles i forbindelse med oprettelse af Exchange konti. Kan sættes til blank hvis man ikke ønsker noget powershell afviklet.

ExchangeDeactivatePowershell	Exchange/deactivateExchange.ps1	Stil til powershell script der afvikles i forbindelse med deaktivering af Exchange konti. Kan sættes til blank hvis man ikke ønsker noget powershell afviklet.
ActiveDirectoryEnableCreation	True	Hvis der løbende skal oprettes nye AD konti på baggrund af bestillinger i SOFD, skal denne sættes til ”True”.
ActiveDirectoryEnableDeactivation	True	Hvis der løbende skal deaktiveres AD konti på baggrund af bestillinger i SOFD, skal denne sættes til ”True”.
ActiveDirectoryEnableDeletion	True	Hvis der løbende skal slettes AD konti på baggrund af bestillinger i SOFD, skal denne sætes til ”True”.
ActiveDirectoryAttributeCpr	employeeNumber	Denne skal udfyldes med navnet på den attribut i AD, hvor medarbejdernes CPR nummer skal sættes ved oprettelse.
ActiveDirectoryAttributeEmployeeId	employeeId	Denne attribute skal KUN udfyldes hvis man kører i det scenarie hvor der oprettes en AD konto per ansættelse. I så fald skal den udfyldes med navnet på den attribut hvor man ønsker at medarbejder ID’et skal skrives til
ActiveDirectoryUserOU	OU=Users,DC=kommune,DC=local	Den OU i AD’et hvor bugerkonti skal oprettes
ActiveDirectoryCreatePowershell	ActiveDirectory\createUser.ps1	Stien til det powershell script der skal afvikles ved oprettelse af nye AD konti. Lad den være blank hvis der ikke ønskes afviklet noget powershell.
ActiveDirectoryDeactivatePowershell	ActiveDirectory\disableUser.ps1	Stien til det powershell script der skal afvikles når en AD konto deaktiveres. Lad den være blank hvis der ikke ønskes afviklet noget powershell.
ActiveDirectoryDeletePowershell	ActiveDirectory\deleteUser.ps1	Stien til det powershell script der skal afvikles når en AD konto slettes. Lad den være blank hvis der ikke ønskes afviklet noget powershell.
ActiveDirectoryEnableAccountExpire	True	Angiver om applikationen må sætte udløbsdato på AD konti

		eller ej. Denne skal være sat til True, hvis man bruger pause-markeringer i SOFD Core.
ActiveDirectoryDeletePowershellBeforeDelete	False	Angiver om det lokalt-tilpassede powershell script ved sletning skal afvikles før sletningen gennemføres i AD (default false).
UploadConfiguration	False	Sæt til ”True” for at den lokale konfiguration bliver uploadet til SOFD Core
UPNChoice	EXCHANGE	Sættes til ”AD”, ”EXCHANGE” eller ”BOTH”, og angiver hvilken kontotype der bestemmer hvad der skrives i UserPrincipalName på brugeren i AD. Ved ”BOTH” anvendes først AD når denne oprettes, og det bliver så overskrevet når/hvis brugeren får en exchange konto.
DefaultUPNDomain	@kommune.dk	Såfremt UPNChoice er ”AD”, anvendes denne som suffix efter samaccountname i UserPrincipalName
AlternativeUPNDomains	185af372-5f79-42f9-8578-b91f20adf6fb=@domain1;a34dc2c4-97bd-42ec-a9fb-42d31c2f21bb=domain2	Semikolonsepareret streng med org-uuid,UPNDomain som kan anvendes hvis UPNChoice er ”AD” og ansatte i nogle enheder skal have et andet UPN domæne i end default (f.eks. @kommunebiblioteker.dk)
ExistingAccountExcludeOUs	OU=Slettede brugere,DC=kommune,DC=dk	Semikolon-separareret liste af Ouer. Brugere under disse OUer vil blive ignoreret når agenten skal afgøre om en eksisterende bruger skal gen-aktiveres, eller om der skal oprettes en ny bruger.
ActiveDirectoryJobCron	0 0-59/5 * ? * *	Cron udtryk til afvikling af oprettelse af AD konto-ordrer.
ExchangeJobCron	0 1-59/5 * ? * *	Cron udtryk til afvikling af oprettelse af Exchange konto-ordrer.

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 Afvikling af powershell

Hvis man har slået afvikling af powershell til, skal man opsætte et powershell script på nedenstående måde. Bemærk det er muligt at slå det til "per hændelse", fx for hhv oprettelse og deaktivere af AD konti og oprettelse af Exchange konti.

For alle hændelsestyper, er det den samme struktur som powershell scriptet skal have

```
function Invoke-Method {
    param(
        [string] $SAMAccountName = $(throw "Please specify a sAMAccountName."),
        [string] $Name = $(throw "Please specify a name."),
        [string] $Uuid = $(throw "Please specify a uuid.")
    )

    $result = "Creating " + $SAMAccountName + ", " + $Name + ", " + $Uuid;

    $result | Out-File 'c:\logs\log.txt'
}
```

Der skal være en funktion i scriptet der hedder "Invoke-Method", som tager 3 argumenter, hhv

- sAMAccountName
- Name
- Uuid

Disse 3 værdier vil indeholder hhv kontonavnet på den AD bruger som hændelsen vedrører, det fulde navn på medarbejeren, samt UUID'et på medarbejderen i SOFD, så man kan lave opslag i SOFD for at hente yderligere oplysninger.

Der følger 3 eksempel-scripts med når man installerer servicen, som man kan rette i. De er alle ens, og skriver blot hændelsen til en logfil.