OS2faktor Login

CoreData API

Version: 2.0.0
Date: 09.04.2023
Author: BSG

1 Formål

Dette dokument beskriver de API snitflader der findes på OS2faktor Login til at vedligeholde stamdata på de personer som har en aktiv konto i OS2faktor Login systemet, herunder hvilke der må få en erhvervsidentitet.

Bemærk at man godt kan indlæse personer i løsningen, som må anvende den til at logge på fagsystemer, uden at disse må få en erhvervsidentitet (og dermed kunne logge på fagsystemer som kræver et NSIS niveau).

2 Data / payloads

Dette afsnit beskriver de forskellige payloads der indgår i de enkelte API operationer

Følgende datastrukturer indgår i API operationerne

2.1 CoreData

Denne datastruktur anvendes når man udfører enten et fuldt load af alle personer der eksisterer indenfor ét domæne, eller hvis man udfører en delta-opdatering af udvalgte personer indenfor ét domæne.

2.1.1 JSON eksempel

```
{
  "domain": "kommune.dk",
  "entryList": [
    {
      "uuid": "1527693d-59f0-4bd0-88fe-408c32e4c0b5",
      "cpr": "1234567890",
      "rid": "78129748",
      "name": "Test Testesen",
      "email": "test@kommune.dk",
      "samAccountName": "ttest",
      "subDomain": "omsorgen",
      "expireTimestamp": "2022-08-01",
      "nsisAllowed": true,
      "transferToNemlogin": true,
      "attributes": {
        "shoesize": "43",
        "eyecolour": "brown"
      }
    }
  ]
}
```

2.1.2 Feltbeskrivelse

Attribut	Obligatorisk	Beskrivelse
uuid	Ja	Et gyldigt UUID, der primært bruges som en ekstern identifikationsnøgle (fx overfor KOMBIT), og dermed en attribut i udstedte claims. Ved reaktivering af deaktivede brugere, så anvendes UUID også som en validering af

		om der er tale om en fysisk ny konto, eller en reaktivering af en eksisterende (nyt UUID betyder at den gamle konto slettes og en ny oprettes, hvor matchede UUID betyder reaktivering)
cpr	Ja	CPR nummeret på personen. Skal være et gyldigt (og korrekt) CPR nummer. Det er kommunens ansvar at sikre at disse CPR numre faktisk matcher de personer man ønsker at indlæse i løsningen.
rid	Nej	Sæt hvilket RID nummer som denne person har ovre i NemLog-ins brugeradministration. Anvendes til en 1-gangs migrering af data, og data kan også leveres som excel eller lignende data til dette formål
name	Ja	Kaldenavn på den person som indlæsning. Personens folkeregisternavn hentes fra CPR registeret, så man kan her udfylde med det navn som personen ønsker at være kendt under
samAccountName	Ja	AD brugernavnet på personen. Hvis personen har flere AD brugernavne, så kan man oprette personen flere gange i payload.
email	Nej	Email adressen på personen, hvis en sådan kendes. Er ikke nødvendig, og anvendes ikke pt af løsningen, men forventes anvendt i fremtiden til ikke-følsom kommunikation
nsisAllowed	Ja	Sættes til ”true” hvis personen må få en erhvervsidentitet, eller ”false” hvis personen ikke må. Hvis der er tale om en opdatering, og personen allerede har en erhvervsidentitet, og værdien sættes til ”false”, så spærres denne erhvervsidentitet (men personen må stadig logge ind i løsninger som IKKE kræver et NSIS niveau)
transferToNemLogin	Ja	Sættes til ”true” for de brugere som skal overføres til NemLog-ins brugeradministration. Bemærk at Digst tager 20 DKK for oprettelsen af en bruger, så der er økonomi forbundet med at sætte dette flag (til Digst, ikke til Digital Identity)
expireTimestamp	Nej	Denne værdi kan udfyldes med en dato-angivelse for hvornår kontoen udløber. En udløben konto kan ikke bruges til login. Hvis værdien sættes til NULL eller udelades, vil udløb blive fjernet på kontoen.
attributes	Nej	Et sæt af ekstra attributter på key/value format. Man kan indlæse alle de attributter man ønsker, og gøre brug af disse til overførsel af data til tjenesteudbydere. Er ikke nødvendigt til STIL, KOMBIT og NemLog-in3, men kan være nødvendigt til

		lokale tjenesteudbydere som den enkelte kommune kobler på løsningen
subDomain	Nej	Kan udfyldes for at angive at denne person er tilknyttet et underdomæne. Hvis udeladt er personen blot direkte under hoveddomænet. Det anbefales at udelade denne attribut med mindre man har et specifikt behov til at indele brugerne i subdomæner

2.2 CoreDataDelete

Dette payload bruges når der skal udføres en sletning af udvalgte personer fra et domæne.

2.2.1 JSON eksempel

```
{
  "domain": "kommune.dk",
  "entryList": [
    {
      "cpr": "1234567890",
      "samAccountName": "ttest"
    }
  ]
}
```

2.2.2 Feltbeskrivelse

Attribut	Obligatorisk	Beskrivelse
cpr	Ja	CPR på den person der ønskes slettet
samAccountName	Ja	Udfyldes med personens AD brugernavn

2.3 CoreDataStatus

Denne datastruktur anvendes når man udlæser status på alle personer indlæst i OS2faktor Login. Bemærk at dette er et read-only format, og fx kan anvendes til at synkronisere en lokal tilstandsdatabase ud til opslagsformål.

2.3.1 JSON eksempel

```
{
  "domain": "kommune.dk",
  "entryList": [
    {
      "uuid": "1527693d-59f0-4bd0-88fe-408c32e4c0b5",
      "cpr": "1234567890",
      "name": "Test Testesen",
      "samAccountName": "ttest",
      "nsisAllowed": true,
      "nsisLevel": "SUBSTANTIAL",
      "approvedConditions": true,
      "ApprovedConditionsTts": "2022-07-26T06:50:55",
      "lockedAdmin": false,
      "lockedPerson": false,
      "lockedDataset": false,
      "lockedDead": false,
```

```
      "lockedPassword": true,
      "lockedExpired": false,
      "lockedPasswordUntil": "2022-08-01T12:41:27"
    }
  ]
}
```

2.3.2 Feltbeskrivelse

Attribut	Beskrivelse
uuid	UUID på personen
cpr	CPR på personen
name	Navnet på personen (folkeregisternavnet)
samAccountName	AD brugernavn på personen
nsisAllowed	Angiver om personen er tildelt en erhvervsidentitet
nsisLevel	Angiver om personen har fået udstedt en erhvervsidentitet, og kan have værdierne ”NONE”, ”LOW”, ”SUBSTANTIAL” og ”HIGH” (i praksis kun ”NONE” og ”SUBSTANTIAL”)
approvedConditions	Angiver om personen har godkendt vilkår for anvendelse af løsningen
ApprovedConditionsTts	Timestamp på hvornår personen har godkendt vilkår (kan være NULL)
lockedAdmin	Angiver om personen er blevet låst af en administrator
lockedPerson	Angiver om personen har låst sig selv (via selvbetjeningen)
lockedDataset	Angiver om personen er blevet låst via API’ets DELETE operation
lockedDead	Angiver om personen er blevet låst pga en ugyldig status i CPR registeret
lockedPassword	Angiver om personen er låst låst fordi de har indtastet forkert kodeord for mange gange
lockedPasswordTts	Angiver hvornår ovenstående lås fjernes (kan være NULL)
lockedExpired	Angiver om kontoen er udløbet på dato

2.4 CoreDataGroup

Dette payload bruges når der skal udføres vedligehold på gruppe-medlemsskaber for brugere. Opdateringen tager udgangspunkt i grupper (dvs lister af grupper indeholdende liste af brugere)

2.4.1 JSON eksempel

```
{
  "domain": "kommune.dk",
  "groups": [
    {
      "uuid": "1527693d-59f0-4bd0-88fe-408c32e4c0b5",
      "name": "1234567890",
      "description": "ttest",
      "members": [
        "bsg",
        "pso"
      ]
    }
  ]
}
```

2.4.2 Feltbeskrivelse

Attribut	Obligatorisk	Beskrivelse
Uuid	Ja	UUID på gruppen der ønskes indlæst/vedligeholdt. UUID er den unikke nøgle for gruppen. Hvis man fx indlæser fra AD, så kan man bruge ObjectGuid.
Name	Ja	Navnet på gruppen, som den vises i brugergrænsefladen. Kan opdateres ved efterfølgende kald.
Beskrivelse	Nej	Beskrivelse af gruppen, til informationsformål alene.
Members	Ja	En liste af brugere som er tildelt denne gruppe – angivet som deres AD brugernavn (sAMAccountName)

2.5 CoreDataKombitJfrFull

Dette payload bruges når der skal udføres vedligehold på tildelte KOMBIT roller for brugere. Opdateringen tager udgangspunkt i brugere, med en liste af tildelte KOMBIT roller for hver bruger. Alle tildelinger som ikke er nævnt i det indgående payload fjernes i forbindelse med en fuld opdatering.

2.5.1 JSON eksempel

```
{
  "domain": "kommune.dk",
  "entryList": [
    {
      "samAccountName": "ttest",
      "uuid": "1527693d-59f0-4bd0-88fe-408c32e4c0b5",
      "jfrs": [
        {
          "identifier": "http://kommune.dk/roles/jobrole/administrator/1",
          "cvr": "12345678"
        }
      ]
    }
  ]
}
```

2.5.2 Feltbeskrivelse

Attribut	Obligatorisk	Beskrivelse
samAccountName	Delvist	Den primære identifikation af personen – AD brugernavnet (samAccountName). Kan udelades hvis man kun har UUID'et, som så udfyldes i stedet
uuid	delvist	Hvis man kun har UUID'et på personen, kan man sende dette i stedet for sAMAccountName (bruges fx i AzureAD integrationen). Skal bare være tom hvis man har samAccountName

Jfrs.identifier	Ja	Angiver den fulde KOMBIT rolle identifier, også kaldet EntityID i KOMBITs Administrationsmodul
Jfrs.cvr	Ja	Angiver CVR nummeret der ejer rollen (typisk kommunens eget CVR, men kan være forskellig for delegerede roller)

2.6 CoreDataKombitJfrDelta

Dette payload bruges når der skal udføres vedligehold på tildelte KOMBIT roller for brugere. Opdateringen tager udgangspunkt i brugere, med lister af roller der skal fjernes eller tilføjes i forbindelse med denne delta-opdatering.

2.6.1 JSON eksempel

```
{
  "domain": "kommune.dk",
  "entryList": [
    {
      "samAccountName": "ttest",
      "uuid": "1527693d-59f0-4bd0-88fe-408c32e4c0b5",
      "addJfrs": [
        {
          "identifier": "http://kommune.dk/roles/jobrole/administrator/1",
          "cvr": "12345678"
        }
      ],
      "removeJfrs": [
        {
          "identifier": "http://kommune.dk/roles/jobrole/sagsbehandler/1",
          "cvr": "12345678"
        }
      ]
    }
  ]
}
```

2.6.2 Feltbeskrivelse

Attribut	**Obligatorisk**	**Beskrivelse**
samAccountName	Delvist	Den primære identifikation af personen – AD brugernavnet (samAccountName). Kan udelades hvis man kun har UUID'et, som så udfyldes i stedet
uuid	delvist	Hvis man kun har UUID'et på personen, kan man sende dette i stedet for sAMAccountName (bruges fx i AzureAD integrationen). Skal bare være tom hvis man har samAccountName
addJfrs.identifier	Ja	Angiver den fulde KOMBIT rolle identifier, også kaldet EntityID i KOMBITs Administrationsmodul

addJfrs.cvr	Ja	Angiver CVR nummeret der ejer rollen (typisk kommunens eget CVR, men kan være forskellig for delegerede roller)
removeJfrs.identifier	Ja	Angiver den fulde KOMBIT rolle identifier, også kaldet EntityID i KOMBITs Administrationsmodul
removeJfrs.cvr	Ja	Angiver CVR nummeret der ejer rollen (typisk kommunens eget CVR, men kan være forskellig for delegerede roller)

3 Adgangskontrol

Når man kalder servicen skal man angive en API nøgle som en HTTP Header. Denne udleveres af Digital Identity når man skal have adgang til API'et. Headeren hedder ApiKey, og API nøglen angives som direkte værdi, fx

```
ApiKey: 09fc50d5-f9f6-44e1-ba63-524c146354ad
```

4 Endpoints

API'et er udstillet under det domæne hvor administratorpotalen er udstillet, fx

https://login.kommune.dk/

De enkelte API endpoints er

4.1 HTTP POST /api/coredata/full

Dette endpoint laver en fuld opdatering for et enkelt brugerdomæne, og tager et **CoreData** payload som input.

Payload kræver altid at "domain" er udfyldt, og at dette angiver ID'et på et domæne som findes i OS2faktor Login løsningen. Hvis man ønsker at oprette nye domæner, skal man kontakte Digital Identity som opretter disse direkte i Løsningens database. Forsøg på at indlæse data under et domæne som ikke findes, vil resultere i en fejl.

Hvis man ønsker at under-opdele brugerne fra ét domæne i underdomæner, så kan man vælge at udfylde feltet "subDomain" på hver enkelt person. Lige som med domæner, skal subdomæner også være oprettet på forhånd, så tag fat i Digital Identity om modelleringen af domæner og underdomæner inden indlæsningen sættes op.

"entryList" er et array af personer som findes undet det angivne domæne. Når man kalder /full endpointet skal man angive ALLE personer som skal eksistere under dette domæne.

- Personer som allerede er indlæst i løsningen, og som ikke findes i det indkommende payload, vil blive spærret.
- Personer som endnu ikke er indlæst i løsningen, og som findes i det indkommende payload, vil blive oprettet.
- Personer som allerede er indlæst i løsningen, og som findes i det indkommende payload, vil blive opdateret.

4.2 HTTP POST /api/coredata/delta

Dette API endpoint fungerer som /full endpointet beskrevet ovenfor, og har samme input format. Men der foretages kun oprettelser og opdateringer. Der foretages ikke nogen spærringer af eksisterende konti som ikke er med i payload.

Dette API endpoint kan bruges til at lave drypvise opdateringer (opret/opdater).

4.3 HTTP DELETE /api/coredata

Dette API endpoint kan bruges i kombination med /delta endpointet beskrevet ovenfor, til at lave drypvise opdateringer med det formål at spærre personer. Som input tages et **CoreDataDelete** payload

Domain skal udfyldes som for de forrige API endpoints, men entryList er lidt simplere, da man blot skal angive de identificerende attributter på de konto man ønsker at spærre.

4.4 HTTP DELETE /api/coredata/cleanup

Dette API endpoint tager samme input (**CoreDataDelete**) som ovenstående DELETE operation, men hvis det kaldes slettes de fysiske data fra OS2faktor databasen, modsat ovenstående hvor brugerkontoen alene spærres.

Man bør ikke anvende dette endpoint som en generel spærre/oprydningsfunktion. OS2faktor har brug for at gemme data på indlæste brugere, også selvom de er spærrede, så fejlsøgning, reaktivering, logsøgning m.m. fungerer optimalt.

Anvend kun dette endpoint til at slette fejlindlæste data.

4.5 HTTP GET /api/coredata/status?domain=xxx

Dette API endpoint udlæser status på alle personer indenfor et angivet domæne. Output har formatet **CoreDataStatus**.

Denne API operation er ikke nødvendig for en integration til OS2faktor, og er alene tilgængelig til fejlsøgningsformål eller informationsudlæsning.

4.6 HTTP POST /api/coredata/groups/load/full

Dette API endpoint kan bruges til at indlæse alle grupper for et givent domæne, herunder hvem der er medlem af de enkelte grupper. Data som ikke er med i payloadet nedlægges, hermed forstået at

- Grupper som ikke er i payloadet fjernes helt fra OS2faktor løsningen
- Brugere som ikke længere er i en gruppes liste af brugere, fjernes fra gruppen

Ellers oprettes og opdateres grupperne med de indkommende data.

Operationen tager en **CoreDataGroup** som input.

4.7 HTTP POST /api/coredata/groups/load/delta

Dette API endpoint kan bruges til at indlæse alle grupper for et givent domæne, herunder hvem der er medlem af de enkelte grupper. Grupper som ikke er med i payload forbliver som de er i OS2faktor løsningen. Alle gruppemedlemsskaber opdateres dog, så alle medlemmer af gruppen skal indlæses når en grupper opdateres.

Operationen tager en **CoreDataGroup** som input.

4.8 HTTP POST /api/coredata/jfr/full

Dette API endpoint bruges til at læse KOMBIT roller ind i OS2faktor, inkl hvem der har de enkelte roller tildelt.

Der foretages en fuld indlæsning, og roller samt tildelinger som ikke er inkluderet i payload, bliver fjernet fra OS2faktor løsningen.

Operationen tager en **CoreDataKombitJfrFull** som input.

4.9 HTTP POST /api/coredata/jfr/delta

Dette API endpoint bruges til at læse KOMBIT roller ind i OS2faktor, inkl hvem der har de enkelte roller tildelt.

Der foretages en delta indlæsning, hvor man kan angive ændringer til delinger i form af tilføjelser og fratagelser for enkelte medarbejdere.

Operationen tager en **CoreDataKombitJfrDelta** som input.

4.10 HTTP GET /api/coredata?domain=xxx

Ovenstående API kan bruges til at udlæse alle data der er registreret under et givent domæne. Output er på formen **CoreData**.

4.11 HTTP GET /api/coredata/{cpr}?domain=xxx

Ovenstående API kan bruges til at udlæse alle registrerede oplysninger på ét CPR nummer for ét givent domæne. Output er på formen **CoreData**.

4.12 HTTP GET /api/coredata/jfr?domain=xxx

Dette API endpoint udlæser alle personer der er tildelt KOMBIT roller indenfor et angivet domæne. Output har formatet **CoreDataKombitJfrFull** .

Denne API operation er ikke nødvendig for en integration til OS2faktor, og er alene tilgængelig til fejlsøgningsformål eller informationsudlæsning.

4.13 HTTP GET /api/coredata/jfr/{cpr}?domain=xxx

Ovenstående API kan bruges til at udlæse alle registrerede KOMBIT roller på ét CPR nummer for ét givent domæne. Output er på formen **CoreDataKombitJfrFull** .

Denne API operation er ikke nødvendig for en integration til OS2faktor, og er alene tilgængelig til fejlsøgningsformål eller informationsudlæsning.

4.14 HTTP GET /api/coredata/groups?domain=xxx

Ovenstående API kan bruges til at udlæse alle grupper for et givent domæne, herunder hvem der er medlem af de enkelte grupper. Output er på formen **CoreDataGroup**.

Denne API operation er ikke nødvendig for en integration til OS2faktor, og er alene tilgængelig til fejlsøgningsformål eller informationsudlæsning.

4.15 HTTP GET /api/coredata/groups/{cpr}?domain=xxx

Ovenstående API kan bruges til at udlæse alle grupper for et givent domæne, som er tildelt personer med det givne CPR nummer, herunder hvem der er medlem af de enkelte grupper. Output er på formen **CoreDataGroup**.

Denne API operation er ikke nødvendig for en integration til OS2faktor, og er alene tilgængelig til fejlsøgningsformål eller informationsudlæsning.