# OS2sync

## Installation Guide

**Version**: 4.3.0
**Date**: 10.06.2024
**Author**: BSG

# Indhold

# 1 Indledning

OS2sync er tilgængelig både som

- Kildekode, så man kan bygge sine egne DLL'er og inkluderer i egne kodeprojekter
- Installerklar Windows Service, der kan anvendes til enten REST eller SQL integration
- Docker Container, der ligeledes kan anvendes til enten REST eller SQL integration

Dette dokument dækker installationen af Windows Service samt Docker Container. For anvendere af kildekoden antages det at man selv henter kildekoden på Github, kompilerer og integrerer ind i eget projekt på egen hånd.

# 2 Forudsætninger

OS2sync er afhængig af en serviceaftale til at kalde FK Organisation. Denne serviceaftatale indgås via KOMBITs administrationsmodul. Denne guide dækker ikke alle detaljer i at blive tilsluttet KOMBITs infrastruktur, og her henvises til KOMBITs egen dokumentation.

Når man er tilsluttet KOMBITs infrastruktur, kan man tilgå Administrationsmodulerne her (de to miljøer hos KOMBIT er helt adskilte, og der er ikke nogen metode til at overføre data fra TEST til PRODUKTION, så opsætningen skal laves forfra i PRODUKTION)

https://admin-test.serviceplatformen.dk/

https://admin.serviceplatformen.dk/

Man skal oprette et såkaldt Anvendersystem, som kræver et OCES 3 certifikat. Certifikatet skal anvendes i OS2sync til at kalde snifladen efterfølgende, så sørg for at gemme p12 filen og det tilhørende kodeord.

I administrationsmodulet skal man indgå en serviceaftale, der giver det Anvendersystem man har oprettet lov til at kalde "Organisation 6" servicen for den kommune hvis data man skal arbejde med.

Serviceaftalen skal godkendes af kommunen før den kan anvendes.

Bemærk at der findes 2 roller til Organisation 6 snitfladen. Begge roller er nødvendige hvis man ønsker at læse/skrive data. Rollen "Udstil" er nødvendig hvis man kun skal læse data. Hvis man skal vedligeholde data er det vigtigt at man angiver "Ja" hvis man spørges om man vil have adgang til navne- og cpr oplysninger.

Endeligt skal man sikre at man har de offentlige certifikater som hhv STS'en (adgangssystemet) og FK Organisation anvender til at digital signere deres svar. Disse certifikater er bundlet sammen med OS2sync, men da de skiftes regelmæssigt hos KOMBIT, bør man sikre at man henter de nyeste udgaver fra KOMBITs digitaliseringskatalog her

https://digitaliseringskataloget.dk/teknik/certifikater

Der er ikke en strengent navngivning i de publicerede certifkater, så brug sund fornuft til at identificere dem/de der skal bruges. Bemærk at der er forskellige pakker til hhv TEST og PROD. Seneste certifikater fra PROD som er relevante hedder

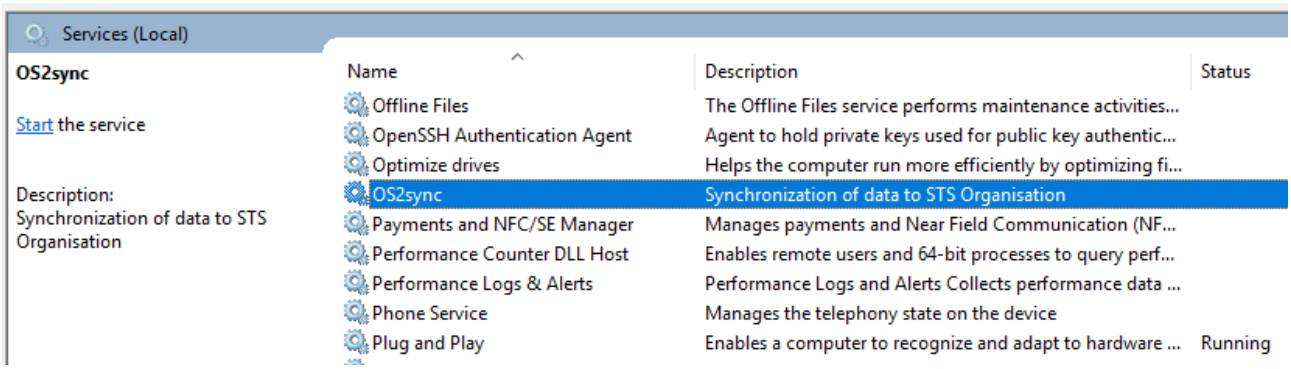
- ADG_PROD_Adgangsstyring_1
- ORG_PROD_Organisation_1

# 3 Windows Service Installation

Windows Servicen kommer som en EXE installer, der bare skal afvikles. Efter den er installeret kan man finde servicen installeret her

C:\Program Files (x86)\Digital Identity\OS2sync

Og under "Services" på windows serveren kan man finde denne service, som skal opsættes med en servicekonto der har de fornødne rettigheder.




## 3.1 Rettigheder

Servicen har brug for begrænsede rettigheder, og det er ikke sikkert det er nødvendigt med en dedikeret servicekonto. Der afhænger af hvor hårdt selve windows serveren er låst ned. Som minimum skal OS2sync kunne

- Kalde KOMBITs webservices over HTTPS/443 (dvs ren udgående netværkstrafik)
- Skrive til en logfil (placeringen er konfigurabel)
- Læse keystore (p12 fil) og certifikater

Hvis OS2sync også anvendes til at skrive data tilbage til FK Organisation skal servicen have adgang til at skrive til en SQL database (da udgående data samles op i en SQL kø, og afvikles så hurtigt som muligt efterfølgende). Man kan enten angive en SQL brugerkonto i konfigurationsfilen, eller man kan anvende Windows Integrated Authentication til at forbinde til SQL databasen – i det sidste tilfælde så er det nødvendigt med en dedikeret servicekonto til at afvikle OS2sync servicen, da rettighederne til SQL databasen i så fald skal knyttes til denne.

## 3.2 Eksempel på appsettings.json til Windows Servicen

Når Windows Servicen er installeret er der en appsettings.json fil, som kan tilpasses med konfigurationsparametre. Nedenfor er vist et eksempel på hvordan en sådan kan udfyldes

```
{
  "AllowedHosts": "*",

  "Environment": "TEST",

  "StsSettings": {
    "StsCertificateLocation": "c:/certifikater/ sts.cer"
  },

  "ServiceSettings": {
    "WspCertificateLocation":  "c:/certifikater/organisation.cer"
  },

  "ClientSettings": {
    "WscKeystoreLocation": "c:/certifikater/keystore.p12",
    "WscKeystorePassword": "HemmeligKode"
  },

  "SchedulerSettings": {
    "Enabled": true,
    "DBConnectionString": "server=127.0.0.1;user
id=SA;password=Test1234;Database=os2sync",
    "DBType": "MSSQL"
  }
}
```

## 3.3 Windows Service specifikke konfigurationsparametre

Der er en enkelt setting, AllowedHosts, som bare skal efterlades med defaultværdien i appsettings.json. Den sikrer at servicen kan tage mod REST kald.

For OS2sync konfiguration henvises til afsnit 5, da den dækker både Windows Service og Docker opsætningen.

# 4 Docker Installation

Det antages at anvenderen er bevendt med Docker. Eksemplet nedenfor baserer sig på anvendelsen af Docker Compose som orkestreringsværktøj – det er på mange måder laveste fællesnævner for okestrering, og anvenderne kan selvfølgelig selv tilpasse deployment til Kubernetes, Docker Swarm eller hvad end orkestreringsværktøj der ønskes anvendt.

Images publiceres på Dockerhub her

https://hub.docker.com/r/os2sync/linux/tags

Og nyeste udgave er på skrivende tidspunkt 4.0.0 – man bør dog altid checke om der er kommet en nyere udgave, og anvende seneste patch-release (fx 4.0.3) af den version man anvender, da evt fejlrettelse vil blive publiceret som patch-release versioner.

## 4.1 Eksempel docker-compose.yml fil

```
version: "2.0"
services:
  os2sync:
    image: os2sync/linux:4.0.0
    ports:
      - 5000:5000
    environment:
      Environment: "TEST"

      StsSettings:StsCertificateLocation: "/home/trust/sts.cer"

      ServiceSettings:WspCertificateLocation:  "/home/trust/organisation.cer"

      ClientSettings:WscKeystoreLocation: "/home/cert/keystore.pfx"
      ClientSettings:WscKeystorePassword: "TopHemmeligt"

      SchedulerSettings:Enabled: "true"
      SchedulerSettings:DBConnectionString: "server=127.0.0.1;user
id=root;password=Test1234;Database=os2sync"
      SchedulerSettings:DBType: "MYSQL"
    volumes:
      - /path/to/keystore:/home/cert
      - /path/to/trusttore:/home/trust
```

## 4.2 Docker specifikke konfigurationsparametre

OS2sync udstiller en REST snitflade på port 5000, som evt kan mappes via Docker til en anden port. Man kan også udelade at mappe porten hvis man ikke skal bruge REST snitfladen.

Det anbefales at man placerer keystore (.p12 filen) og trusttore (.cer filer) filerne i en folder som mappes ind i Docker containeren som vist ovenfor. Det kan sagtens være samme folder, eksemplet viser blot at man også kan adskille dem hvis man ønsker.

For OS2sync konfiguration henvises til afsnit 5, da den dækker både Windows Service og Docker opsætningen.

Bemærk at sub-konfigurationer er adskilt med ":", fx er SchedulerSettings -> Enabled angivet som SchedulerSettings:Enabled.

# 5 Konfiguration

Nedenstående tabel indeholder de tilgængelige konfigurationsparametre, som skal indarbejdes enten i ens konfigurationfil til Windows Servicen eller til miljøparametrene til Docker. Bemærk at syntax'en for udfyldelse af de to respektive konfigurationsfiler er forskellig, så tag udgangspunkt i skabelonen til hver af disse, og tilpas efter behov.

| Parameter | Default | Beskrivelse |
|---|---|---|
| `Cvr` | | Hvis denne parameter er udfyldt (ikke krævet), behøves man ikke angive CVR som parameter når man kalder REST snitfladen – så anvendes dette CVR nummer automatisk. |
| `CvrUuid` | | Hvis man ønsker at anvende et CVR nummer som ikke er en af de 98 kommuner i Danmark, så SKAL man angive et UUID her – UUID'et angiver den overliggende organisation som alle data registreres under i FK Organisation. OS2sync har en indbygget tabel med de korrekte UUID'er for alle 98 kommuner, så udfyld kun denne værdi hvis man ønsker at bruge et CVR der ikke tilhører en af disse 98 kommuner. |
| `TrustAllCertificates` | `false` | Som udgangspunkt bruger OS2sync operativsystemet til at foretage certifikat-validering, men hvis man løber ind i udfordringer med manglende tillid til fx STS eller FK Organisations certifikater, kan man slå certifikatvalideringen fra – det anbefales ikke, og man bør i stedet forsøge at få etableret tillid til certifikaterne i stedet. |
| `Environment` | `PROD` | Her kan man angive enten PROD eller TEST. Det påvirker hvilket miljø hos KOMBIT som OS2sync kalder webservices hos. |
| `StsSettings -> StsCertificateLocation` | | Denne setting bruges til at udpege det certifikat som KOMBITs STS bruger til at signere deres svar. Hvis den ikke udfyldes, og peger på det certifikat som KOMBIT anvender på deres STS, så vil forsøg på at få adgang til FK Organisation fejle.<br><br>Der angives en fil-placering på certifikatfilen, fx<br><br>`C:/certifikater/sts.cer` |
| `ServiceSettings -> WspCertificateLocation` | | Denne setting bruges til at udpege det certifikat som KOMBITs FK Organisation service bruger til at signere deres svar. Hvis man ikke udfyldes, og peger på det certifikat som KOMBIT anvender på FK Organisation, så vil forsøg på at kalde FK Organisation servicen fejle.<br><br>Der angives en fil-placering på certifikat-filen, fx<br><br>`C:/certifikater/organisation.cer` |
| `ClientSettings -> WscKeystoreLocation` | | Denne setting bruges til at udpege det certifikat som OS2sync skal anvende til at kalde FK Organisation snitfladen. Her peges på en p12 fil (eller pfx fil) på serveren hvor OS2sync afvikles, fx<br><br>`C:/certifikater/keystore.p12` |

| | | |
|---|---|---|
| `ClientSettings -> WscKeystorePassword` | | Denne setting bruges til at angive kodeordet til ovenstående p12 fil. |
| `SchedulerSettings -> Enabled` | `false` | Sæt denne værdi til true hvis OS2sync skal bruges til at skrive data til FK Organisation. Hvis den sættes til true så skal der som minimum også angives en ConnectionString til databasen nedenfor |
| `SchedulerSettings -> DBConnectionString` | | Her angives en ConnectionString til den database hvor udgående data skal gemmes kortvarigt (kø-funktionalitet). Formatet på en sådan ConnectionString afhængiger af typen af database, samt sikkerhedsmodellen der anvendes – der henvises til egen database dokumentation for korrekte værdier.<br><br>Som eksempel er vist en ConnectionString til en MySQL database, der kører på localhost nedenfor<br><br>`server=127.0.0.1;user id=os2sync;password=Hemmelig;Database=os2sync` |
| `SchedulerSettings -> DBType` | `MSSQL` | Angiv enten MSSQL (Microsoft SQL Server) eller MYSQL (for MariaDB eller MySQL) – OS2sync tilpasser SQL dialekten der anvendes til håndtering af databasekøen afhængigt af denne parameter |
| `SchedulerSettings -> DisableOpgaver` | | Sættes til værdien ”true” hvis man ønsker at vedligholde KLE opmærkning inde i FK Organisation brugergrænsefladen, og ikke ønsker at OS2sync skal overskrive KLE opmærkningen derinde |
| `SchedulerSettings -> DisableHenvendelsessteder` | `true` | Sættes til værdien ”false” hvis man ønsker at overføre henvendelsessteder fra ens lokale kilde. Som default overfører OS2sync ikke henvendelsesteder, så denne setting skal slås fra for at sikre at OS2sync overfører disse værdier |
| `SchedulerSettings -> DisableUdbetalingsenheder` | `true` | Sættes til værdien ”false” hvis man ønsker at overføre udbetalingsenheder fra ens lokale kilde. Som default overfører OS2sync ikke udbetalingsenheder, så denne setting skal slås fra for at sikre at OS2sync overfører disse værdier |
| `SchedulerSettings -> IgnoredOUAddressTypes` | `SOR` | Her kan angives en kommasepareret liste af adressetyper som OS2sync ikke må overskrive inde i FK Organisation. Som udgangspunkt bruges dette kun til at understøtte sameksistens med et andet system der vedligeholder denne type af adresser (fx SOR værdierne via KOMBITs organisation-synkroniseringssystem).<br><br>Lovlige værdier er<br><br>SOR, EAN, DTRID, PNR, LOCATION, CONTACT |
| `LogSettings -> LogLevel` | `INFO` | Kan sættes til DEBUG, INFO, WARN eller ERROR for at øge/reducere mængden af logs |
| `LogSettings -> LogFile` | | Her kan man angive placeringen på en fil der skal logges til. Hvis man ikke angiver en placering (default) så logges output bare til konsollen. |

| | | |
|---|---|---|
| | | Logfilen ruller når den bliver 1 MB stor, og de sidste 10 logfiler gammes, så max logstørrelse er 10 MB. |
| `LogSettings -> LogRequestResponse` | `false` | Hvis man ønsker at ALLE requests logges i rå XML format, så kan man slå denne setting til. Bemærk at det giver enorme mængder logs, og kun bør være slået til under evt fejlsøgning |
| `ReadSettings -> UserGrouping` | `50` | Hvis man har brug for at læse store mængder data ud fra FK Organisation, og oplever timeouts, så kan man reducere dette tal. Så laves flere kald, men med færre data af gangen. Samlet vil det tage længere tid at udlæse data, men de enkelte kald har mindre sandsynlig for at give timeout.<br><br>Dette tal angiver hvor mange brugere der læses på én gang. Værdier mellem 10 og 100 er lovlige, 50 er et godt valg til performance/timeout håndtering. |
| `ReadSettings -> OrgUnitGrouping` | `7` | Hvis man har brug for at læse store mængder data ud fra FK Organisation, og oplever timeouts, så kan man reducere dette tal. Så laves flere kald, men med færre data af gangen. Samlet vil det tage længere tid at udlæse data, men de enkelte kald har mindre sandsynlig for at give timeout.<br><br>Dette tal angiver hvor mange enheder der behandles af gangen (bemærk at alle data for en enhed læses ud, hvilket er en noget tungere operation end det er for brugere). Værdier mellem 3 og 10 er lovlige, og 7 er et godt kompromis mellem performance og timeout håndtering. |
| `ReadSettings -> HierarchyGrouping` | `500` | Hvis man har brug for at læse store mængder data ud fra FK Organisation, og oplever timeouts, så kan man reducere dette tal. Så laves flere kald, men med færre data af gangen. Samlet vil det tage længere tid at udlæse data, men de enkelte kald har mindre sandsynlig for at give timeout.<br><br>Dette tal angiver hvor stor en del af hierarkiet der udlæses på én gang, max værdien er 500, og man kan reducere den helt ned til 50 hvis man har behovet. Typisk har man ikke brug for at reducere denne værdi, men hvis man har, så forsøg med 200-300 stykker. |

## 5.1 Problemer med timeouts

Hvis man oplever problemer med timeouts under udlæsningen af HELE organisationen fra FK Organisation så kan man reducere mængden af data der udlæses af gangen. Det er typisk ikke nødvendigt når man læser data IND i FK Organisation, men hvis man anvender OS2sync til udlæsning af data, så kan man løbe ind i disse problemer).

Ovenstående tabel angiver ReadSettings, som normalt ikke skal sættes (så anvendes default værdier), men hvis man oplever Timeout på udlæsning af data, så kan man prøve med disse settings (og evt tilpasse dem til man får den bedste mulige performance)

```
ReadSettings:UserGrouping: "30"
ReadSettings:OrgUnitGrouping: "5"
ReadSettings:HierarchyGrouping: "250"
```

# 6 Database opsætning

Hvis OS2sync skal skrive data til FK Organisation skal den have adgang til en SQL database, hvor den midlertidigt kan gemme de udgående data.

OS2sync opretter selve de nødvendige tabeller, men der skal være oprettet et tomt database-skema, som OS2sync kan oprette tabellerne i. Det betyder også at OS2sync skal have lov til at oprette tabeller.

Rettighedsstyring i SQL databaser liggende udenfor scope af denne vejledning.

# 7 Migrering fra OS2sync 2/3

Der er ikke nogen migrering af eksisterende installation af OS2sync vesrsion 2.x eller 3.x. Version 4 af OS2sync er en selvstændig applikation, og evt databaseopsætning, certifikater, konfiguration kan ikke genbruges.

# 8 Problemer med p12 filer på Windows Servere

De OCES3 certifikater der udstedes via MitID Erhverv virker ikke på alle Windows Servere. Hvis man oplever problemer med at få p12 filen til at fungere med OS2sync, kan man bruge et trick til at ”rense” p12 filen for de data som Windows ikke kan håndtere.

Importer p12 filen ind i Firefox browseren, og træk derefter filen ud af Firefox igen (via Firefox certifikat backup funktion). Dette danner en ny p12 fil, som ikke indeholder de extensions som MitID Erhverv har lagt i filen, og som Windows kan have problemer med at håndtere.