

# OS2faktor Login

Password AD Integration

**Version:** 1.2.0

**Date:** 29.10.2021

**Author:** BSG

# 1 Formål

Dette dokument er rettet mod teknikere der skal opsætte og konfigurere kommunens integration fra Active Directory til OS2faktor Login, så kodeord kan replikeres mellem de to systemer.

## 1.1 Forudsætninger

### 1.1.1 Windows Server

Servicen skal installeres på en Windows maskine med:

- Netværksmæssig adgang til kommunens AD
- Netværksmæssig adgang til OS2faktor Login via HTTPS.
- .NET Framework 4.7.2 eller nyere

### 1.1.2 Service konto i AD

Der skal oprettes en service konto i kommunes AD.

Kontoen skal have lov til at skifte kodeord på brugerkonti. Dette kan fx gøres ved at give den Account Operator rollen, eller ved at explicit tildele den adgang til at skifte kodeord på brugere.

Bemærk at en servicekonto opsat på denne måde ikke kan skifte kodeord på domæne administratorer, da kun domæne administratorer kan skifte kodeord på andre domæne administratorer. Hvis det er nødvendigt at OS2faktor kan skifte kodeord på domæne administratorer, så skal denne servicekonto være domæne administrator.

### 1.1.3 WebSocket nøgle til OS2faktor Login

Der skal i konfigurationen indtastes en WebSocket nøgle. Denne udleveres af Digital Identity.

## 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 OS2faktor Login via HTTPS.

### 2.1 Download service

Download og installér servicen fra <https://www.os2faktor.dk/download.html>

### 2.2 Konfiguration af service

Konfiguration af servicen foretages i appSettings sektionen i xml-filen **OS2faktor Password Agent.exe.config** som ligger i roden af installationsmappen (default C:\Program Files (x86)\Digital Identity\OS2faktorPasswordAgent).

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

Indstilling	Eksempel	Kommentar
serilog:*		Diverse indstillinger til opsætning af log.
websocketKey	xxxx	Den nøgle der giver adgang til at forbinde til OS2faktor Login. Udleveres af Digital Identity.

WebsocketUrl	wss://kommune.os2faktor.dk/ws	URL adressen på websocket forbindelsen til OS2faktor. Udleveres af Digital Identity
Domain	kommune.dk	Domænenavnet som brugerne er kendt under i OS2faktor Login.  Se CoreData opsætningen for det valgte domænenavn. Det samme navn skal bruges her.
allowValidatePassword	true	Sættes som udgangspunkt til "true".  Hvis man ikke ønsker at integrationen må foretage validering af kodeord op mod AD, kan denne sættes til false
allowChangePassword	true	Sættes som udgangspunkt til "true".  Hvis man ikke ønsker at integrationen må foretage password skifte, kan man sætte værdien til "false".

## 2.3 Start af service

Servicen skal konfigureres til at afvikle under den servicekonto som har de fornødne rettigheder, og herefter kan den startes som en normal service under Services.

Det anbefales at man sætter den til automatisk opstart (gerne med forsinket opstart), så man er sikker på at den kører efter en server genstart.

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**.

## 3 High Availability / Redundans

Hvis denne integration er utilgængelig, kan brugerne ikke skifte kodeord. Det anbefales derfor at man har 2 af disse integrationer kørende på hver deres server, og sikrer at man kun udfører servicevindue/genstart på én af disse servere af gangen.