# OS2faktor Login

## RobotMFA

**Version**: 1.0.0
**Date**: 11.01.2025
**Author**: BSG

# 1 Formål

Dette dokument beskriver anvendelsen af MFA klienter for robotter / RPA processer.

# 2 Angivelse af at en bruger er robot

Før en Robot kan tildeles en MFA klient, er det vigtigt at OS2faktor ved at brugeren er en robot. Dette styres fra det kildesystem hvor man læser brugeredata ind i OS2faktor.

Hvis man som kommune har bygget sin egen integration, skal man have tilpasset sin integration til Coredata API'et. Der er tilføjet en "robot" angivelse på brugerstamdataene der indlæses. Se API beskrivelsen for Coredata API'et for detaljer.

Hvis man indlæser stamdata fra sit Active Directory, så skal man oprette en sikkerhedsgruppe i AD, der angiver hvilke brugere der er robotter, og så melde sine robot-brugere ind i denne sikkerhedsgruppe.

I servicen "OS2faktor Coredata Service", som står for indlæsningen fra AD, skal man tilføje denne setting, og udpege sikkerhedsgruppen. Bemærk at denne funktionalitet kræver at man kører mininum version 2.14.0 af Coredata servicen.

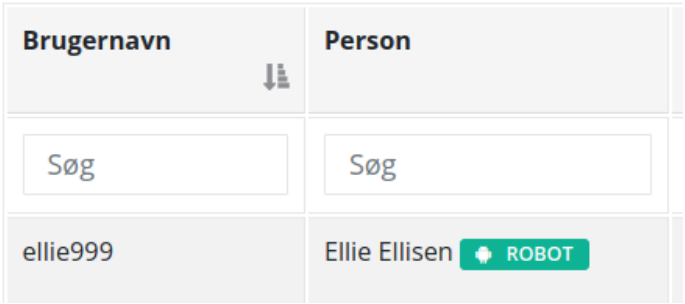
```
<add key="ActiveDirectory.Robot.Group" value="CN=MinGruppe,OU=xxx,DC=yyy,DC=zz" />
```

Dvs man udpeger sikkerhedsgruppen via dennes DistinguishedName, og så genstarter servicen.

Bemærk at robotter ikke kan få en erhvervsidentitet, og hvis en robot allerede har en sådan, så fungerer det ikke at tilføje brugeren til robot-gruppen. Tilsvarende kan en robot aldrig stoppe med at være en robot, så hvis man først har gjort en bruger til en robot, så er de robot for altid.

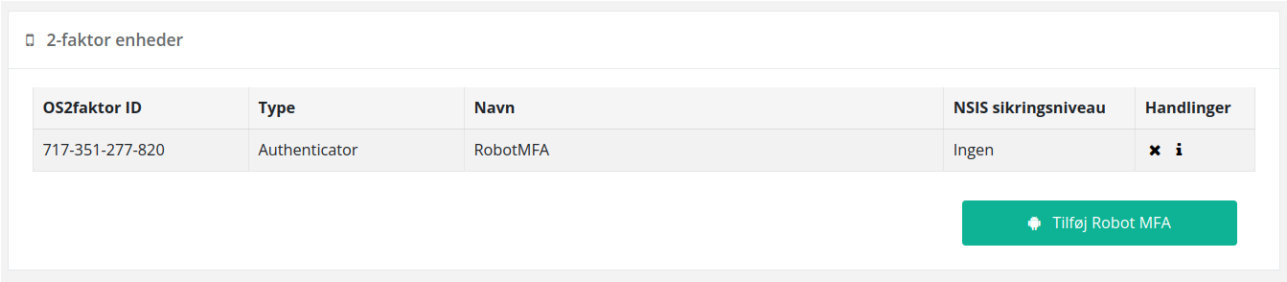
Endeligt kan OS2sofds integration også styre dette. Angivelsen af hvorvidt en bruger er en robot, sættes inde i OS2sofds brugergrænseflade (kræver man kører mindst version 2025 r1 af OS2sofd).

Man kan tydeligt se hvorvidt en bruger er en robot inde i OS2faktor, da der står et "robot mærke" ud for navnet på brugerkontoen når man er inde i adminsitrationsmodulet, som vist nedenfor



# 3 Hvordan får man en MFA klient til en robot

En kommunal ansat der har adgang til administrationsmodulet i OS2faktor, kan tilføje en MFA klient til en robot inde i OS2faktor. Dette gøres ved at tilgå brugerens detaljeside som administrator, og så klikke på knappen "Tilføj Robot MFA". Bemærk at når man tilføje en MFA klient, så vises en hemmelig nøgle på skærmen (eksempel vist nedenfor) som skal kopieres og gives til ens RPA udviklere. Nøglen kan ikke vises igen, så hvis man mister den, er man nødt til at slette MFA klienten, og oprette en ny



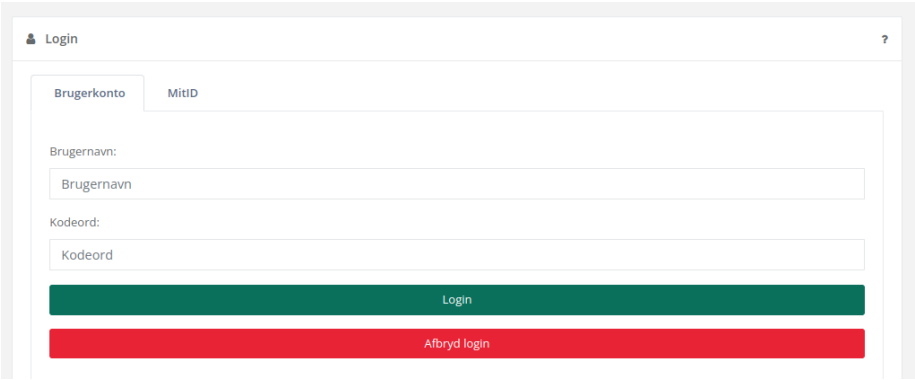


Med den hemmelige nøgle, kan en RPA udvikler gennemføre et MFA loginflow.

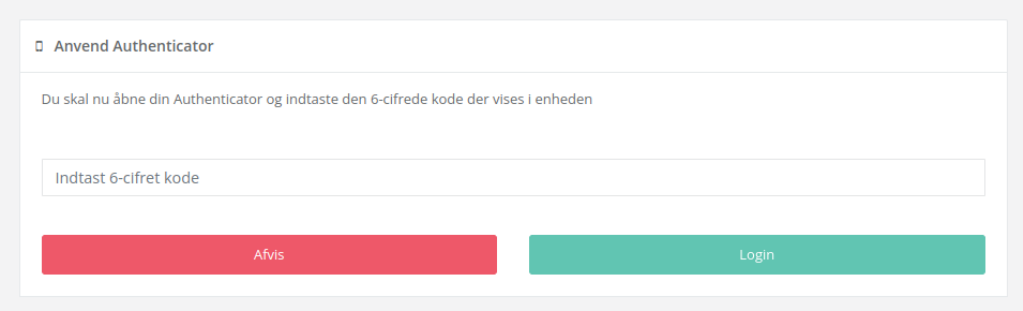
# 4 Hvordan ser loginflowet ud

Loginflowet er identisk med det loginflow som brugere med en kodeviser kommer gennem. Flowet består af 2 trin, som illustreret nedenfor

Først indtastes brugernavn og kodeord



Dernæst indtastes den beregnede 6 cifrede kode (den hemmelige nøgle fra før kan bruges til at beregne en korrekt 6 cifret kode)




Hvorefter login er gennemført.

# 5 Teknik

Med den hemmelige nøgle i hånden, kan man beregne en korrekt 6 cifret kode på nedenstående måde. Selve specifikationen der anvendes er

https://datatracker.ietf.org/doc/html/rfc6238

hvor der som input anvendes den nævnte hemmelige kode, og et timestamp (klokken som den er lige nu, præcist). En simpel matematisk formel beregner så en 6 cifret kode, der kan anvendes til login.

Man kan enten selv implementere beregningen, eller man kan anvende en af de mange frameworks der findes til at beregne værdien korrekt.

Fx findes følgene to frameworks til hhv .NET og Java

https://github.com/kspearrin/Otp.NET

https://github.com/aerogear-attic/aerogear-otp-java

Men der findes mange andre frameworks, herunder også flere til ovenstående 2 sprog.

Hvis man er i tvivl om hvorvidt man danner den 6 cifrede kode korrekt, så kan man anvende en af de mange online værktøjer der findes, der danner koden ud fra hemmeligheden (bemærk at man ikke bør indtaste ens produktions-hemmelighed i et online værktøj).

https://totp.danhersam.com/

https://totp.app/

der findes mange af disse implementationer på nettet, som man kan lade sig inspirere af.

Der anvendes SHA1, 30 sekunders intervaller og 6 cifrede koder. Hvis det framework man anvender har flere konfigurationsmuligheder, skal man anvende disse.