OS2faktor Login

Windows Credential Provider

Version: 3.3.0
Date: 19.06.2025
Author: MPO

1 Formål

Der er udarbejdet en såkaldt Windows Credential Provider (WCP) til OS2faktor Login løsningen. Denne WCP understøtter følgende funktionalitet

- Mulighed for at etablere en NSIS login session helt fra Windows login skærmen. Ved at anvende denne WCP vil brugerens initielle windows login blive brugt til at skabe single-signon sessionen, og brugeren slipper da for at anvende sit brugernavn/kodeord til at foretage det første web-baserede login
- Muligheden for at brugerne selv kan skifte kodeord via Windows, uden at dette kræver at de skal gennem en re-aktiveringsproces i forhold til deres erhvervsidentitet.
- Muligheden for at brugerne kan genskabe et glemt kodeord direkte fra Windows Login siden

1.1 Forudsætning

WCP'en skal installeres på brugernes PC. Hvis der anvendes Citrix eller en anden form for fjernskrivebord, så skal WCP'en installeres på Citrix serverne.

Funktionaliteten til at etablere single-signon sessionen helt fra windows login skærmbilledet, fungerer ved at sessionen overdrages fra windows login skærmbilledet til browseren.

WCP'en kan rulles ud på brugernes PC centralt, og kræver ikke at brugerne skal foretage nogen efterfølgende opsætning.

2 Opdatering af WCP fra v2.x.x til v3.x.x

Tidligere har opdatering været uden nogen ekstra trin men i skiftet fra en v2 til v3 WCP har programmet ændres sig teknisk, derfor kan de kræve nogle yderlige handlinger for at sikre at slutbrugerne får den bedste oplevelse.

2.1 Policy (GPO)

Hvis i gør brug af den policy der sætter en default credential provider (System > Logon > Assign a default credential provider) så vil det være nødvendigt at ændre denne.

Vi udstiller ikke længere den credential provider som er ansvarlig for login, men skaber i stedet en Single Sign-on forbindelse efter en vilkårlig WCP har udført login. Derfor er skal denne policy ændres til en anden WCP, evt. Jeres VPN WCP hvis i gør brug af en. Alternativt kan denne policy slås fra så Windows bruger sin egen WCP som standard.

Det er anbefalet at opdatere GPO'en først for at sikre sig at den er rullet ud på alle computere før der opdateres til en v3.x.x WCP.

2.2 Nulstil bruger præferencer for WCP

Når en bruger foretager et login husker Windows hvilken credentials provider, der blev brugt og gemmer den som den enkelte brugers præference. Det betyder at Windows allerede har gemt den credentials provider som er valgt i ens GPO (afsnit 2.1) som eksisterende brugeres præference.

Derfor kan man nulstille denne præference så et skifte i GPO betyder at de enkelte brugere bliver ført over til den nye standard.

Dette gør man ved at enten slette eller blanke alle key/value par under Windows registry nøglen:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI\UserTile

Det er anbefalet at lave denne ændring i forbindelse med opdatering til en v3 credentials provider.

Hvis man tidligere har haft OS2faktor WCP sat som standard WCP og senere ændret det i forbindelse med en opdatering vil denne nulstilling flytte brugerne over på den nyligt opdaterede WCP

2.3 Fjern filterede WCP'er

Hvis man tidligere har gjort brug af OS2faktor WCP'en eller en anden metode til at fjerne eller filtrere andre WCP'er skal man sørge for at der er mindst én tilgængelig WCP som ikke er OS2faktor WCP.

Dette vil oftest være Windows indbyggede WCP som er blevet filteret fra og derfor skal slås til igen.

Det er anbefalet at lave dette skifte samtidigt eller lige før man opdaterer til en v3 WCP

3 Installation af WCP

MSI pakken til at installere WCP'en kan hentes på OS2faktor hjemmesiden

https://www.os2faktor.dk/

Under Download findes et område til OS2faktor Login Agenter. Her ligger den seneste WCP samt tilhørende dokumentation (dette dokument).

WCP'en forudsætter at man har installeret den nyeste VC Redist pakke fra Microsoft. Der ligger en sådan på samme website, som kan downloades, så man er sikker på at denne også er installeret.

3.1 Lydløs installation af "VC Redistributable"

Microsoft leverer deres VC Redist pakker som EXE installere, der kan installeres uden interaktion via følgende kommando

```
VC_redist.x64.exe /q /norestart
```

3.2 Lydløs installation af WCP

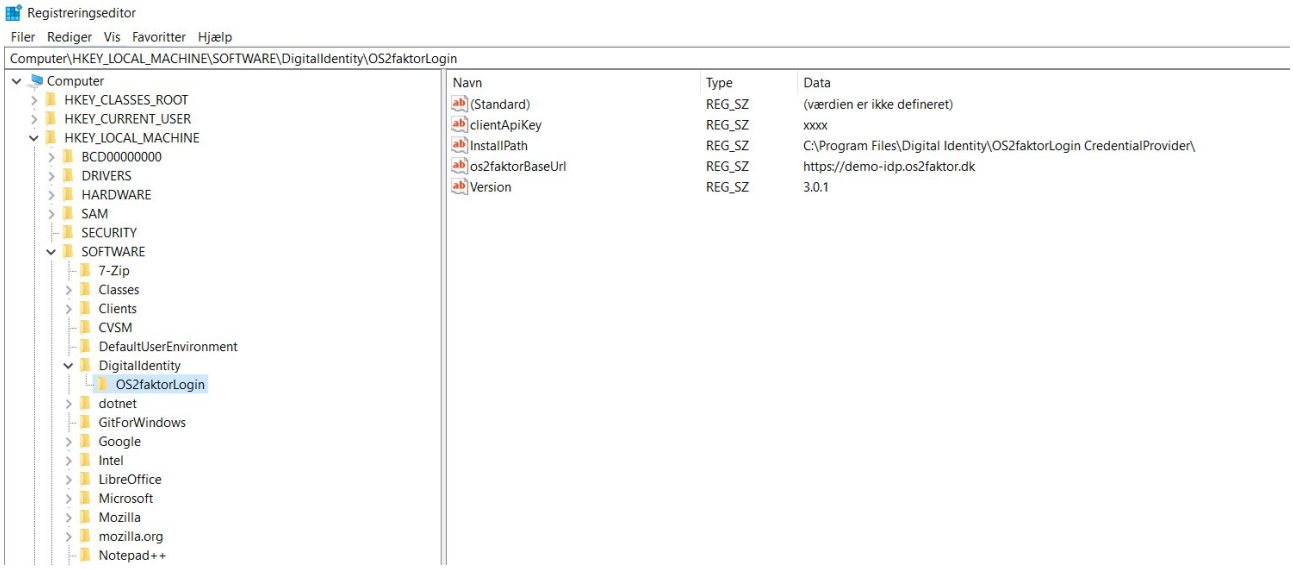
WCP'en leveres som en MSI pakke, der kan installeres lydløst via følgende kommando

```
msiexec /i os2faktor-CredentialProvider.msi /quiet
```

3.3 Konfiguration af WCP

Konfigurationen af WCP'en forefindes i Windows Registry under nøglen HKEY_LOCAL_MACHINE\SOFTWARE\DigitalIdentity\OS2faktorLogin

Registry konfigurationen skal rulles ud på alle maskiner hvor WCP'en installeres, og følgende nøgler er nødvendige for at WCP'en fungerer efter hensigten



WSP'en sætter selv ovenstående nøgler op, men 2 af disse indeholder "dummy-værdier", der skal tilpasses den enkelte kommune der anvender løsningen.

- **clientApiKey**. Denne nøgle skal indeholde en klient nøgle, som kan findes i administratorportalen i OS2faktor Login. Nøglen er specielt hemmelig, men bruges af driftsoperatøren til at spore hvilke WCP'er der laver hvilke kald, samt muligheden for at spærre for en given WCP hvis nødvendigt. Det er samme nøgle der anvendes til alle installationer indenfor et givent domæne i en kommune.
- **os2faktorBaseUrl**. Her skal der peges på kommunens OS2faktor Identity Provider. NB: OS2faktor Selvbetjeningen og Identity Provider er på to forskellige URL, det er vigtigt at det er IdP'en man vælger her.

3.3.1 Tilpasse tekster på login skærmbilledet

Hvis man ønsker at have en bestemt tekst, til "skift kodeord" knappen i Windows login skærmbilledet kan man via en registreringsnøgle ændre denne tekst. Der er sat en standard tekst som vil blive brugt hvis man ikke sætter nogen værdi.

Indstilling	Type	Default	Beskrivelse
ResetPasswordLinkText	REG_SZ (Strengværdi)	Jeg har glemt mit kodeord	Teksten der vises for "skift kode"-knappen. Hvis man ikke sætter denne nøgle vises default teksten.

3.3.2 Understøttelse af Roaming browser profiles

Hvis man gør brug af Roaming browser profiles kan der opstå problemer hvis det drev hvor Chrome eller Edge profilen er gemt først bliver tilgængeligt efter login-tidspunktet.

I dette tilfælde kan man konfigurere indstillingen: **WaitForDiskAccess** samme sted som de andre os2faktor indstillinger i registry.

Indstilling	Type	Beskrivelse
WaitForDiskAccess	REG_SZ (Strengværdi)	Sti som session etablering venter på er tilgængelig før programmet kører.

WaitForDiskAccess er en streng værdi der for eksempel kan se således ud: ”G:\”

Dette vil gøre at sessionsetableringen venter på at G drevet bliver tilgængeligt da det er der hvor brugerens Chrome browser profil er lagt i dette eksempel.

3.3.3 Slå sessionsetablering til/fra individuelt pr. browser

Det er muligt at slå sessionsetablering til eller fra for de forskellige browsere. Dette giver mening hvis man for eksempel ikke gør brug af en af de understøttede browsere. Ved kun at have de nødvendige browsere slået til vil man undgå unødig skærmflimmer for brugeren i forbindelse med login.

Session etablering kan slås til/fra via registry, og ligger samme sted som de andre indstillinger:

Indstilling	Type	Default	Beskrivelse
EstablishSessionChrome	DWORD	1 = Slået til	Værdien sættes til 1 eller 0 for at slå Chrome til/fra
EstablishSessionEdge	DWORD	1 = Slået til	Værdien sættes til 1 eller 0 for at slå Edge til/fra
EstablishSessionFirefox	DWORD	0 = Slået fra	Værdien sættes til 1 eller 0 for at slå Firefox til/fra

3.3.4 Tilpas browserens opstartsparametre individuelt for hver browser

Det er muligt at tilpasse de opstartsparametre som en browser startes med. Dette kan være nyttigt for at undgå opstarts popups og valg som en bruger skal foretage sig første gang efter installation eller opdatering af en browser.

Indstilling	Type	Beskrivelse
CustomParametersChrome	REG_SZ (Strengværdi)	Opstartsparametre til Chrome fx. --no-first-run
CustomParametersEdge	REG_SZ (Strengværdi)	Opstartsparametre til Edge
CustomParametersFirefox	REG_SZ (Strengværdi)	Opstartsparametre til Firefox

3.3.5 Ved brug af WCP'en sammen med Windows11 24H2 eller senere

I nyere Windows versioner er der blevet ændret på de standard policies. Der er især én policy som kan medvirke at WCP'en ikke virker.

GPO'en kan findes under:

Windows Components\Windows Logon Options

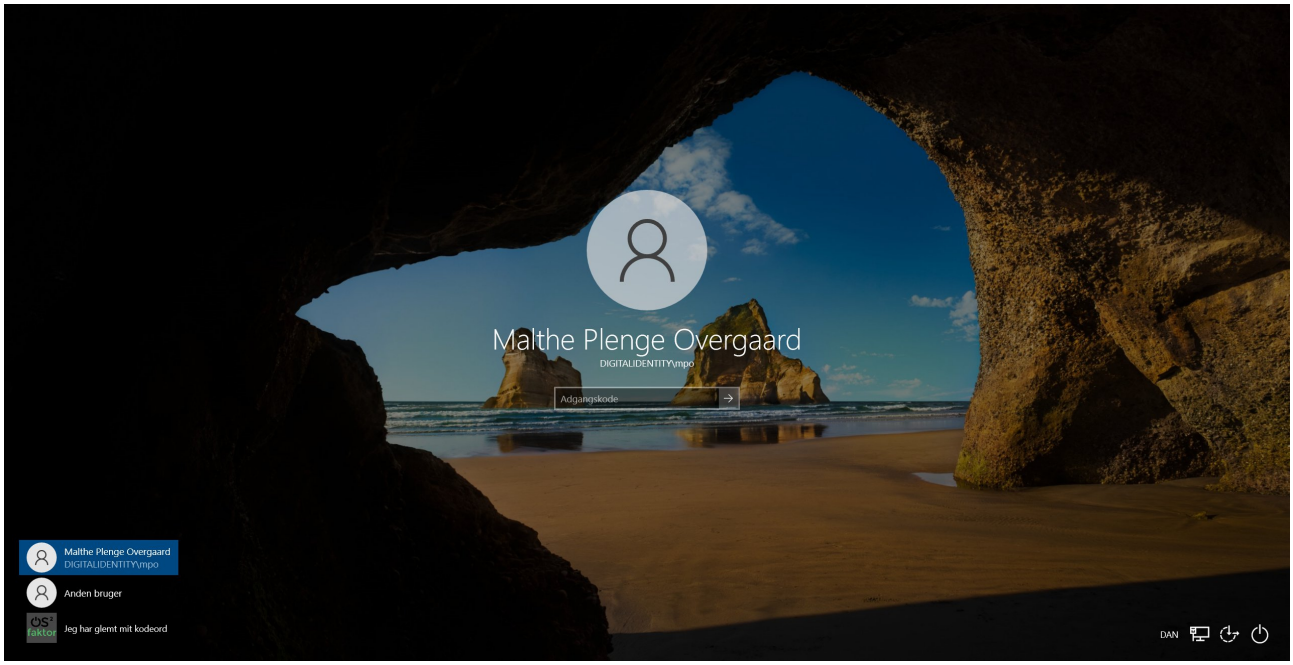
Og hedder:

Enable MPR notification for the system

Denne GPO er i nyere Windows versioner automatisk slået fra hvis man ikke eksplicit har taget stilling til denne policy. For at få WCP'en til at virke korrekt, både i forbindelse med Single Sign-On og kodeord-sskifte er det vigtigt at denne policy bliver eksplicit sat til **enabled**

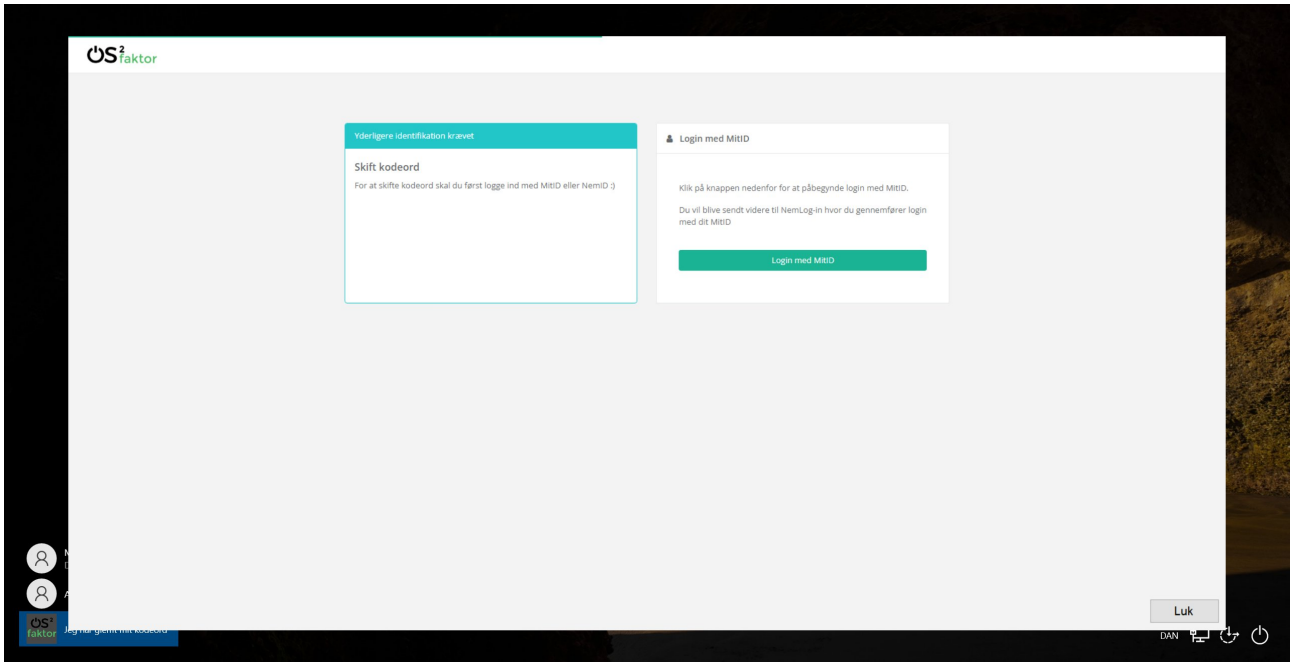
4 Afprøvning af funktionalitet

Når WCP'en er installeret (og korrekt konfigureret), vil login skærmbilledet se cirka ud som nedenfor:

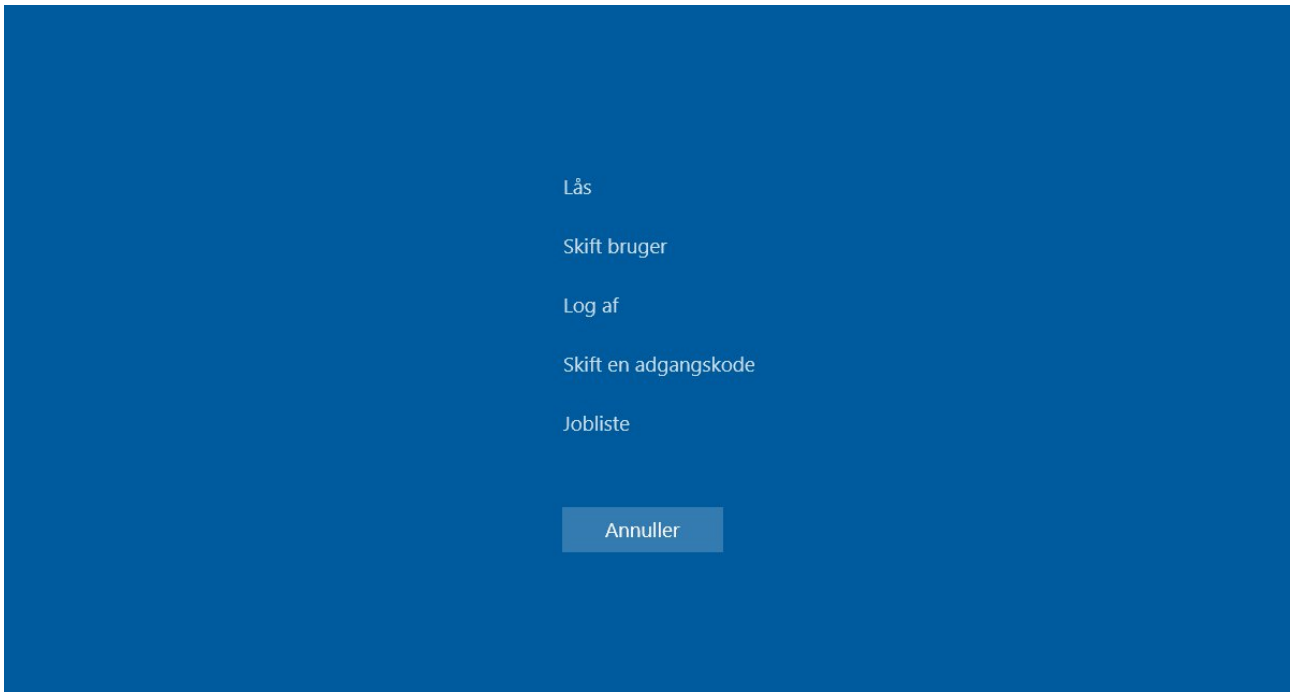


Nederst i venstre side vil man se et OS2faktor logo og teksten "Jeg har glemt mit kodeord". Denne tekst kan ændres se afsnittet "3.3.1 Tilpasse tekster på login skærmbilledet". Hvis man kan se linket, så er WCP'en korrekt opsat.

Hvis man klikker på linket "Jeg har glemt mit kodeord", åbner følgende skærmbillede, hvor man kan foretage login med MitID og derefter vælge et nyt kodeord.



Endeligt kan man foretage et almindeligt password skifte som bruger, som vist nedenfor. Dette gøres ved at trykke Ctrl+Alt+Del og derefter vælge Skift en adgangskode.



Og dette kodeordsskifte vil så skifte brugerens kodeord både i OS2faktor og på Windows.

5 Fejlsøgning

Til fejlsøgningsformål kan man slå logning til på WCP'en. Dette gøres via windows registry (samme placering som de normale indstillinger). Her kan man tilføje en eller flere af nedenstående nøgler, for at tilføje logning på de enkelte funktioner.

Det anbefales ikke at have logning slået til under normal drift, da det kan påvirke både logintiden, samt introducerer udfordringer med store logfiler over tid.

I alle indstillingerne man man angive den fulde sti til en logfil, hvor man ønsker den givne log skal skrives til.

Indstilling	**Beskrivelse**
CredentialManagerLogPath	Generelle logs i forbindelse med etablering af Single Sign-On. Dette program starter CreateSession og SessionEstablisher.
CredentialProviderLogPath	Logger WCP delen af programmet, som har ansvar for at vise skift kodeord knappen i login skærmbilledet. Dette program starter ResetPassword.
CreateSessionLogPath	Logs omhandlende sessions-overdragelse, mere specifikt token modtagelse.

SessionEstablisherLogPath	Logs omhandlende sessions-overdragelse, mere specifikt udveksling af token til sessioner i browserne.
ResetPasswordLogPath	Logs omhandlende skift kodeord fra windows login skærmbilledet.
ChangePasswordLogPath	Logs omhandlende skift kodeord i forbindelse med Ctrl+Alt+Del i Windows, udløbet kodeord og tvunget kodeordsskifte.