OS2faktor MFA

Entra ID External Authentication Method

**Version**: 1.0.0

**Date**: 01.12.2024

**Author**: BSG

# Formål

Microsoft EntraID har frigivet External Authentication Method i Public Preview. Det betyder at man kan anvende OS2faktor MFA som step-up/MFA mekanisme til login til applikationer hvor man foretager login via Entra ID / Azure.

Man kan læse mere her hvis man er nysgerrig

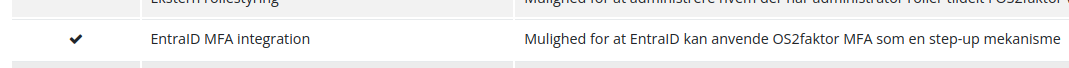
<https://techcommunity.microsoft.com/t5/microsoft-entra-blog/public-preview-external-authentication-methods-in-microsoft/ba-p/4078808>

<https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-external-method-provider>

OS2faktor Login understøtter denne funktionalitet, og kan anvendes som en såkaldt External Authentication Method (EAM) i EntraID.

Dette dokument beskriver hvordan opsætningen skal udføres.

Bemærk at en forudsætning er at funktionen er slået til i OS2faktor Login; dvs der skal være flueben i denne setting under Teknisk Opsætning.



Hvis funktionen ikke er slået til, og man ønsker at anvende den, skal man tage fat i Digital Identity for at få den slået til.

## Forudsætninger

Man skal anvende P1 licenser for at kunne anvende EAM funktionaliteten i Entra. Hvis man ikke har disse, kan man ikke slå External Authentication Methods til inde i Entra. Endeligt er funktionen stadig i Preview, så man skal også have enablet preview features i sit Entra setup.

I OS2faktor er det en forudsætning at man har indlæst UPN på brugerne. Check evt om dette er gjort ved at tage en tilfældig bruger og kigge på denne som administrator/supporter. Hvis man kan se UPN attributten på brugeren, så er UPN indlæst. Hvis ikke, så skal man have tilpasset sin indlæsning, så UPN kommer med.

# Konceptuelt

Når man gennemfører et login via Entra kan man via forskellige conditional access regler, bestemme at en bruger skal lave et 2-faktor login (MFA login). Det første login sker altid i Entra platformen, hvor brugeren anvender brugernavn/kodeord.

Dette første trin identificerer brugeren, og anvendes af Entra til at beregne om brugeren skal lave et MFA login ud fra diverse (og ikke særligt relevante for OS2faktor) regler.

A screenshot of a computer

Description automatically generated

Hvis brugeren skal lave et MFA login, så sender Entra et OpenID Connect login request til OS2faktor, hvor requestet indeholder UPN på brugeren i Entra.

A screenshot of a computer error

Description automatically generated

OS2faktor skal så finde den bruger som har dette UPN registreret i OS2faktor Login brugerdatabasen (så en forudsætning er at man har indlæst UPN på brugerne i OS2faktor), og starte et MFA loginflow (dvs OS2faktor springer brugernavn/kodeord delen af loginflowet over).

A screenshot of a computer

Description automatically generated

OS2faktor skal så svare tilbage på OpenID Connect loginflowet, og fortælle om det gik godt eller skidt.

Entra afslutter så login, baseret på svaret fra OS2faktor Login.

# Opsætning af App i Entra

Der skal oprettes en såkaldt ”app” inde i Entra, og denne ”app” er kommune-specifik, og skal opsættes af kommunen selv i deres Entra Miljø.

**1 – log ind i Entra og gå til ”app registration”**

A screenshot of a computer

Description automatically generated

**2 – Klik på ”new registration” og tildel API rettigheder**

Giv app’en et navn (det vises for brugeren) og vælg ”accounts in this organization”

A screenshot of a computer application

Description automatically generated

**3 – Tildel rettigheder til ”app’en”**

Vælg ”API permissions”, og klik på ”add a permission”. Her vælges ”graph.api” som en delegeret rettighed, og her vælges ”profile” og ”openid”.

A screenshot of a computer

Description automatically generated

Sig ok/gem, og på listen vælg nu at give ”admin consent”. Slutresultatet skal se cirka sådan her ud (flueben ud for status er vigtigt)

A screenshot of a computer

Description automatically generated

**4 – Opret redirect URI’s**

Under ”Authentication” vælges ”Add a platform” og vælg en ”web” platform.

A screenshot of a computer

Description automatically generated

Herefter kan man angive hhv login og logout URL. Den øverste skal pege på /entraMfa/authorize på ens OS2faktor Login installation (IdP’en). Logud adressen kan springes over, den anvendes ikke.

A close-up of a text

Description automatically generated

**4 – Tilføje UPN som et login-hint**

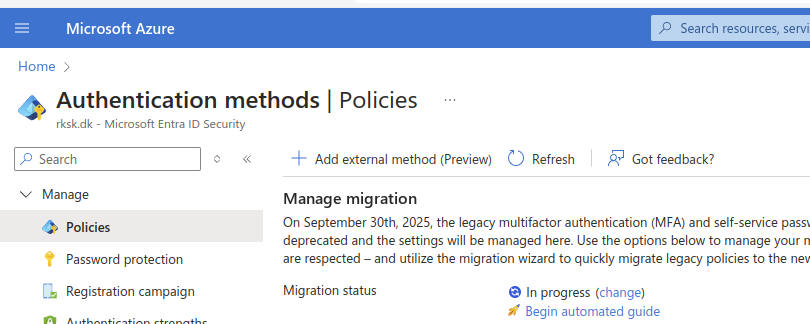
Under Token configuration, kan man angive ekstra claims, der kommer med i beskeden til OS2faktor, og her skal vi tilføje UPN, da det er den eneste nøgle vi nemt kan matche med i OS2faktor Login.

A screenshot of a computer

Description automatically generated

Nu er selve applikationen opsat.

For at anvende den som et MFA login middel, skal man gå til Authentication Methods i Azure, hvor man kan klikke på ”Add external method (preview)”. Hvis man ikke har dette menupunkt, skal man enable preview features (samt sikre at man har en P1 licens på ens Entra AD).



I den dialog der kommer frem, skal man udfylde ClientID og App ID med samme værdi (det App ID som ens app er oprettet med under app registration), og discovery endpoint er /entraMfa/openid-configuration endpointet på ens OS2faktor Login IdP installation.

A screenshot of a computer

Description automatically generated

Husk at enable den oprettede external authentication method.