

# OS2faktor MFA

Entra ID External Authentication Method

**Version:** 1.0.0

**Date:** 01.12.2024

**Author:** BSG

# 1 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.

Erstatningsindstilling	Mulighed for administratoren fremover har administratoren slået OS2faktor
✓ EntralID MFA Integration	Mulighed for at EntralID kan anvende OS2faktor MFA som en step-up mekanisme

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.

## 1.1 Forudsætninger

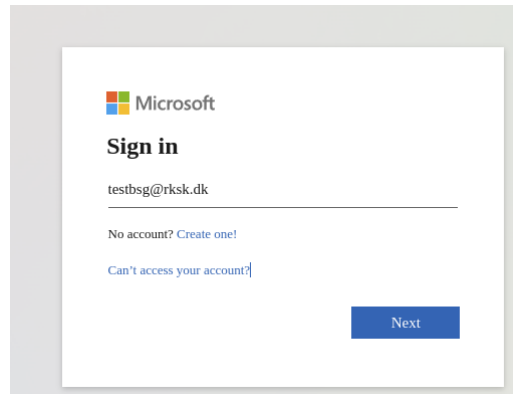
Man skal anvende P1 licenser for at kunne anvende EAM funktionaliteten i Entra. Hvis man ikke har disse, kan man ikke slå External Authentication Methods til inde i Entra. Endeligt er funktionen stadig i Preview, så man skal også have enabled preview features i sit Entra setup.

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.

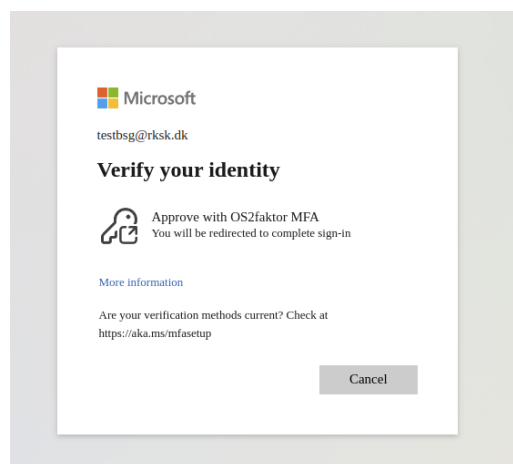
# 2 Konceptuelt

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.

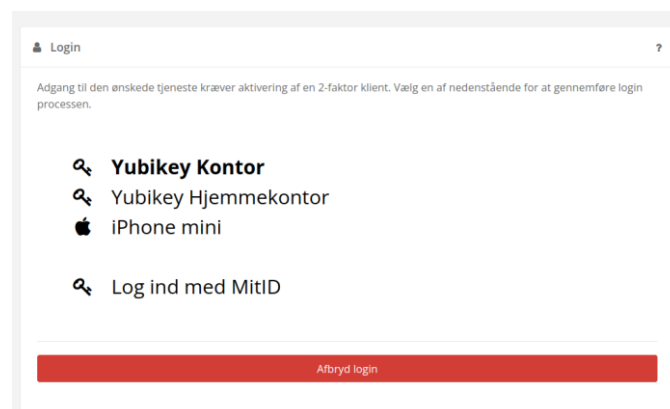
Dette første trin identificerer brugeren, og anvendes af Entra til at beregne om brugeren skal lave et MFA login ud fra diverse (og ikke særligt relevante for OS2faktor) regler.



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.



OS2faktor skal så finde den bruger som har dette UPN registreret i OS2faktor Login brugerdatabase (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).



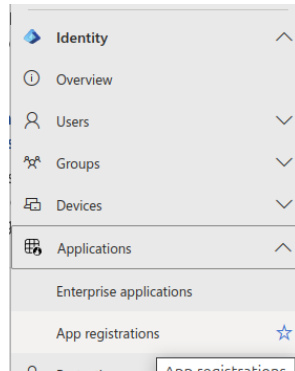
OS2faktor skal så svare tilbage på OpenID Connect loginflowet, og fortælle om det gik godt eller skidt.

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

### 3 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"



#### 2 – Klik på "new registration" og tildel API rettigheder

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

Register an application ...

\* Name  
The user-facing display name for this application (this can be changed later).

OS2faktor MFA ✓

Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (rsk.dk only - Single tenant)
- Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
- Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- Personal Microsoft accounts only

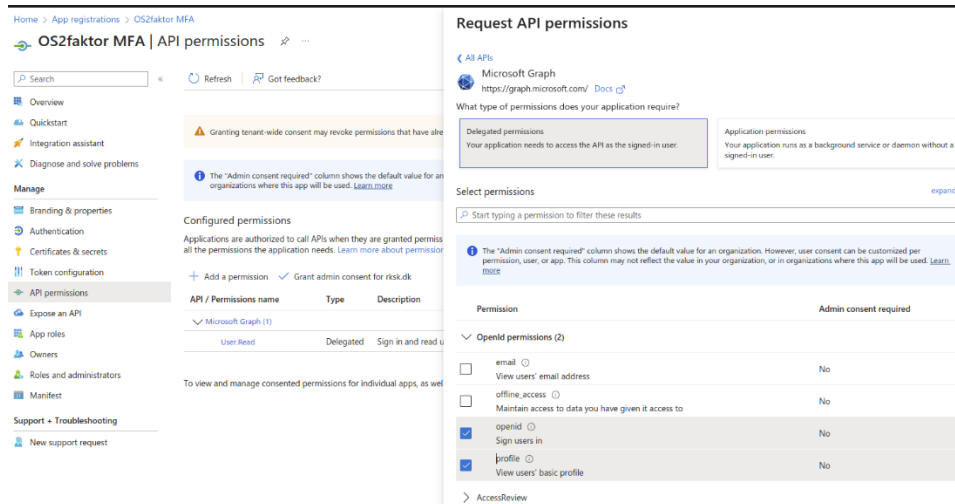
[Help me choose...](#)

Redirect URI (optional)  
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Select a platform ▼ e.g. https://example.com/auth

#### 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".



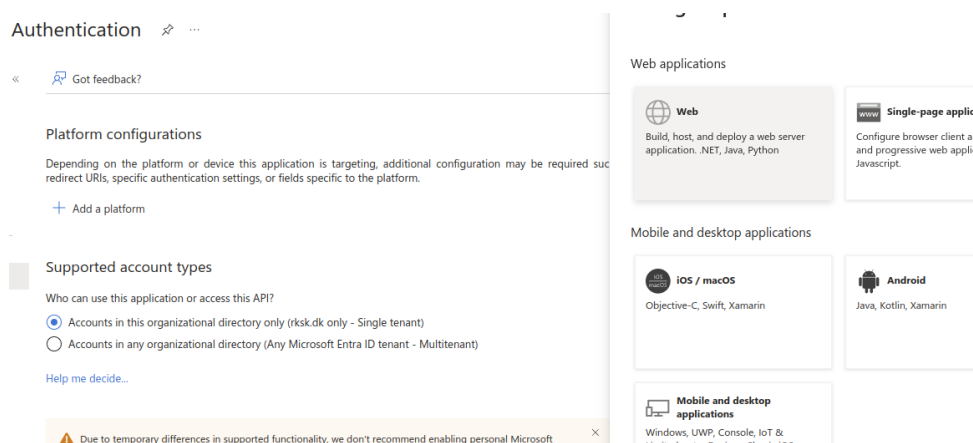
Sig ok/gem, og på listen vælg nu at give "admin consent". Slutresultatet skal se cirka sådan her ud (flueben ud for status er vigtigt)

✓ Grant admin consent for rskk.dk

ne	Type	Description	Admin consent requ...	Status
	Delegated	Sign users in	No	✓ Granted for rskk.dk
	Delegated	View users' basic profile	No	✓ Granted for rskk.dk
	Delegated	Sign in and read user profile	No	✓ Granted for rskk.dk

#### 4 – Opret redirect URI's

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



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.

**Web** Quickstart Docs

**Redirect URIs**

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. The redirect URI you send in the request to the login server should match one listed here. Also referred to as reply URLs. [Learn more about Redirect URIs and their restrictions](#)

https://demo-idp.os2faktor.dk/entraMfa/authorize	
--	--

[Add URI](#)

## 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.

Home > App registrations > OS2faktor MFA

**OS2faktor MFA | Token configuration** ✖

Search  < [Got feedback?](#)

Optional claims

Optional claims are used to configure additional information which is returned in one or more tokens. [Learn more](#)

[+ Add optional claim](#) [+ Add groups claim](#)

Claim ↑↓	Description	Token type ↑↓	Optional settings
upn	An identifier for the user that can be used with the username_hint parameter; not a durable identifier for the user and sho...	ID	Default <span style="float: right;">⋮</span>

**Manage**

- Branding & properties
- Authentication
- Token configuration**
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

Support + Troubleshooting

- [New support request](#)

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).

Microsoft Azure Search resources, servi

Home >

**Authentication methods | Policies** ⋮

rksk.dk - Microsoft Entra ID Security

Search  ⋄ << [+ Add external method \(Preview\)](#) [Refresh](#) | [Got feedback?](#)

**Manage**

- Policies**
- Password protection
- Registration campaign
- Authentication strength

**Manage migration**

On September 30th, 2025, the legacy multifactor authentication (MFA) and self-service pass... are deprecated and the settings will be managed here. Use the options below to manage your n... and utilize the migration wizard to quickly migrate legacy policies to the new

Migration status [In progress \(change\)](#)

[Begin automated guide](#)

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.

Client ID *	<input type="text" value="0a5bfb2f-55e8-41b8-8899-650a98ab88c8"/>
Discovery Endpoint *	<input type="text" value="https://demo-idp.os2faktor.dk/entraMfa/openid-configuration"/>
App ID *	<input type="text" value="0a5bfb2f-55e8-41b8-8899-650a98ab88c8"/>
Request admin consent	<input checked="" type="checkbox"/> Admin consent granted

Husk at enable den oprettede external authentication method.