# 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-externalauthentication-methods-in-microsoft/ba-p/4078808

https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authenticationexternal-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.

EntraID MFA integration
 Mulighed for at EntraID 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

ERSTER FOR COLUMN

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.

### 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.



Microsoft	
Sign in	
testbsg@rksk.dk	
No account? Create one!	
Can't access your account?	

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.

M	icrosoft
testbsg(	@rksk.dk
Verif	fy your identity
6	Approve with OS2faktor MFA You will be redirected to complete sign-in
More inf	formation
Are your https://ak	verification methods current? Check at ka.ms/mfasetup
	Cancel

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).



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"

٩	Identity ^
0	Overview
8	Users $\checkmark$
25	Groups 🗸
圮	Devices $\checkmark$
₿	Applications ^
	Enterprise applications
	App registrations
0	Ann registrations

#### 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?				
<ul> <li>Accounts in this organizational directory only (rksk.dk only - Single tenant)</li> </ul>				
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)				
O 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				

#### 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".



Home > App registrations > OS2faktor MFA		Request API permissions	
OS2faktor MFA	API permissions 🛷 …		
Search     Search     Overview     Quickstart     Integration assistant	<ul> <li>Refresh Refresh Refresh Cot feedback?</li> <li>Cranting tenure-wide consent may revoke permissions that have already and the second rest of the seco</li></ul>	At APs     Market Corrosoft Graph     Mitro://graph.microsoft.com/ Docs c?     What type of permissions     Delegated permissions     Your application needs to access the API as the signed-in user.	Application permissions Your application runs as a background service or deemon without a signed-n use:
Manage	The "Admin consent required" column shows the default value for an organizations where this app will be used. <u>Learn more</u>	Select permissions	expand al
Branding & properties Authentication Certificates & secrets Token configuration	Configured permissions Applications are authorized to call APIs when they are granted permission all the permissions the application needs. Learn more about permission + Add a permission $\checkmark$ Grant admin consent for risk.dk	Start typing a permission to filter these results     The "Admin consert required" column shows the default value for an or     moster, or app. This column may not reflect the value in your o     motor	rganization. However, user consent can be outomized per $$\times$$ organization, or in organizations where this app will be used $\underline{team}_{\rm c}$
API permissions     Expose an API     App roles	API / Permissions name Type Description	Permission V OpenId permissions (2)	Admin consent required
Owners     Roles and administrators     Manifest	To view and manage consented permissions for individual apps, as we	email  View users' email address offline_access	No
Support + Troubleshooting		Maintain access to data you have given it access to     openid      Sign users in	No
		Profile ①     View users' basic profile     AccessReview	No

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)

🗸 Gra	✓ Grant admin consent for rksk.dk				
ne	Туре	Description	Admin consent requ.	Status	
)					
	Delegated	Sign users in	No	Granted for rksk.dk	
	Delegated	View users' basic profile	No	Granted for rksk.dk	
	Delegated	Sign in and read user profile	No	🥑 Granted for rksk.dk	

#### 4 – Opret redirect URI's

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

Aut	hentication 🖉 …		5 .	
«	₽ Got feedback?	W	eb applications	
	Platform configurations Depending on the platform or device this application is targeting, additional configuration may be required suc redirect URIs, specific authentication settings, or fields specific to the platform.		Build, host, and deploy a web server applicationNET, Java, Python	Single-page applic Configure browser client a and progressive web applic Javascript.
	+ Add a platform	м	lobile and desktop applications	
	Supported account types		iOS / macOS	Android
	Who can use this application or access this API? Accounts in this organizational directory only (rksk.dk only - Single tenant) Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)		Objective-C, Swift, Xamarin	Java, Kotlin, Xamarin
	Help me decide		Mobile and desktop	
	▲ Due to temporary differences in supported functionality, we don't recommend enabling personal Microsoft		Windows, UWP, Console, IoT &	

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 Redirect URIs	Quickstart Docs 🗗 📗
The URIs we will accept as destinations when returning authentication responses (tokens) after successfully auth URI you send in the request to the login server should match one listed here. Also referred to as reply URLs. Lea restrictions c	henticating or signing out users. The redirect arn more about Redirect URIs and their
https://demo-idp.os2faktor.dk/entraMfa/authorize	Î
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 > OS2fa	<sub>aktor MFA</sub> Token configura	ration 🖈 …				×
₽ Search	« 🖗 Got feedback?					
Overview	Optional claims	s				
n Quickstart	Optional claims are u	used to configure additional information which is return	ed in one or more tokens. Learn more 🗗			
<ul> <li>Integration assistant</li> <li>Diagnose and solve problems</li> </ul>	+ Add optional cla	laim + Add groups claim				
Manage	– Claim ↑.	Description		Token type ↑.i.	Optional settings	
Branding & properties	upp	An identifier for the user that can be u	used with the username, hint parameter: not a durable identifier for the user and sho	ID	Default	
Authentication	apri				001001	
Certificates & secrets						
Token configuration						
API permissions						
🗠 Expose an API						
App roles						
2 Owners						
Roles and administrators						
Manifest						
Support + Troubleshooting						

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.

Client ID *	0a5bfb2f-55e8-41b8-8899-650a98ab88c8
Discovery Endpoint *	https://demo-idp.os2faktor.dk/entraMfa/openid-configuration
App ID *	0a5bfb2f-55e8-41b8-8899-650a98ab88c8
Request admin consent	Admin consent granted

Husk at enable den oprettede external authentication method.