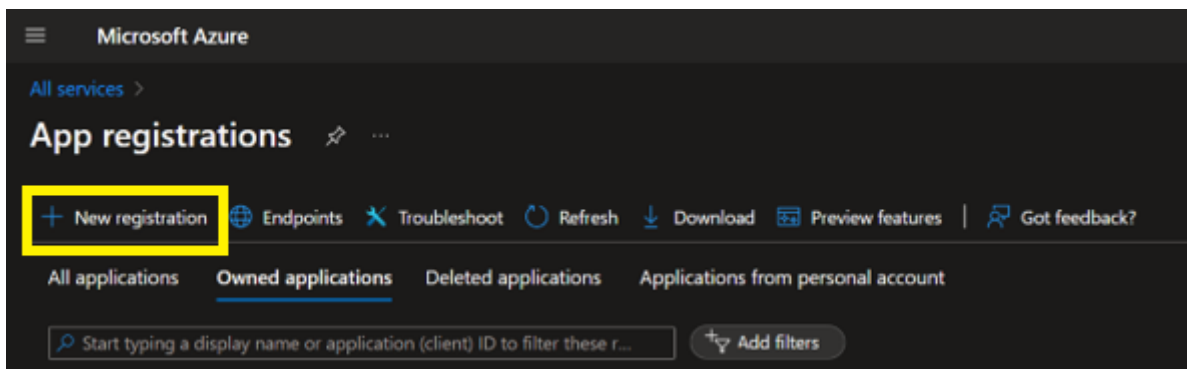
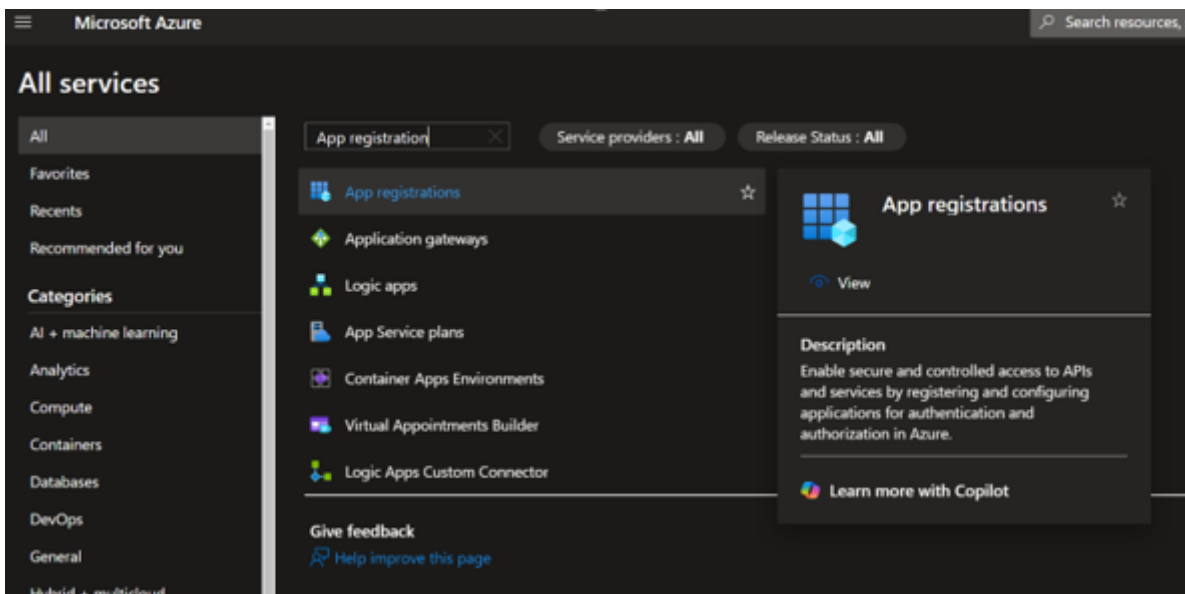


Připojení EaInfoportu k Azure EntraID

- Nejprve je potřeba v Azure zaregistrovat aplikaci EaInfoport. To se provádí v servise „App registration“.



- tlačítkem „New registration“
- V rámci registrace je v tuto chvíli potřeba vyplnit jen „Name“ (například „Infoport“) a registraci dokončit tlačítkem „Register“.
-

Register an application ...

Name

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

Infoport



Supported account types

Who can use this application or access this API?

- ☒ Accounts in this organizational directory only (Default Directory 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

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

- Jako potvrzení se zobrazí základní informace o registrované aplikaci.
- Zde je nejdůležitější informace „**Application (client) ID**“. **Tento údaj budeme v konfiguračním manažeru Infoportu zadávat do položky „Client ID“ (viz. později).**

Delete Endpoints Preview features

Essentials

Display name
Infoport

Application (client) ID
1c0f73b9-9f6e-4806-843d-1c6a1d54c48c

Object ID
265a3648-470f-4eef-a017-25c4cdfc25ac

Directory (tenant) ID
ed95c298-30af-448b-be31-512431cb9c00

Supported account types
[My organization only](#)

Client credentials
[Add a certificate or secret](#)

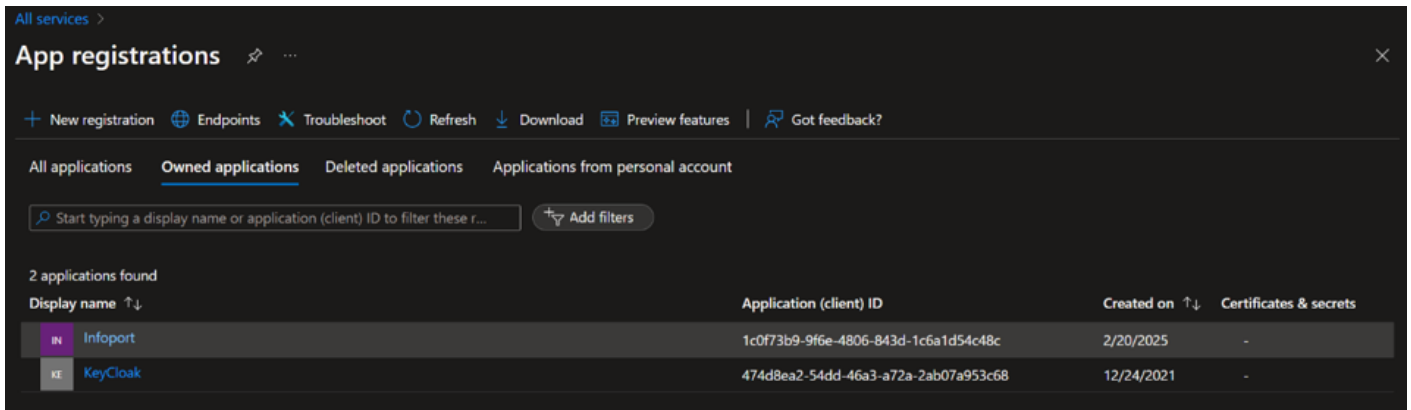
Redirect URIs
[1 web, 0 spa, 0 public client](#)

Application ID URI
[Add an Application ID URI](#)

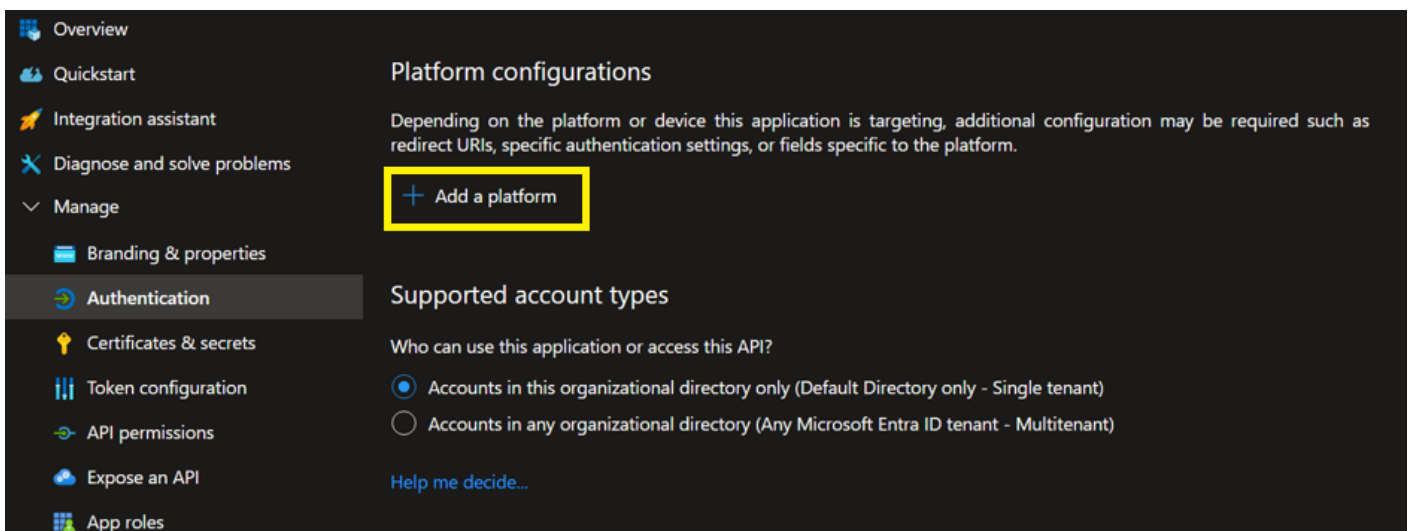
Managed application in local directory
[Infoport](#)

[Get Started](#) [Documentation](#)

- Pokud se nyní vrátíme do seznamu zaregistrovaných aplikací uvidíme „Infoport“ mezi nimi (někdy je potřeba použít tlačítko „Refresh“).
- Je zde také vidět „Application (client) ID“ coby primární identifikátor aplikace, který se na rozdíl od Name nedá po registraci změnit.



- Nyní budeme pokračovat v konfiguraci zaregistrované aplikace Infoport tím, že se proklikneme (skrz jméno Infoport) do detailu.
- Zde v menu vybereme „Manage“ a následně „Authentication“.



- Jako první přidáme tlačítkem „Add aplatform“ platformu aplikace Infoport a to tak, že z nabídky vybereme „Web“.

Got feedback?

Platform configurations

Depending on the platform or device this app redirect URIs, specific authentication settings, or

Add a platform

Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory on
 ☐ Accounts in any organizational directory (A

[Help me decide...](#)

Advanced settings

Allow public client flows ⓘ

Enable the following mobile and desktop flows:

- App collects plaintext password (Resource
- No keyboard (Device Code Flow) [Learn m](#)

Save

Discard

Web applications

Web
 Build, host, and deploy a web server application. .NET, Java, Python

Single-page application
 Configure browser client applications and progressive web applications. Javascript.

Mobile and desktop applications

iOS / macOS
 Objective-C, Swift, Xamarin

Android
 Java, Kotlin, Xamarin

Mobile and desktop applications
 Windows, UWP, Console, IoT & Limited-entry Devices, Classic iOS + Android

- Azure si následně vyžádá vyplnit informace o dvou URL.
- První z nich „Redirect URIs“ je url aplikace Infoport, kam bude uživatel po přihlášení v EntraID přesměrován.
- Vyplňte URI složený z adresy serveru (na kterém máme spuštěný Infoport – v ukázce je to „http://localhost“) a fixní cesty „/signin-oidc“.
- Druhý je „Front-channel logout URL“ a je to url aplikace Infoport, která bude zavolána poté, co se uživatel odhlašuje pomocí single sign-out.
- Zde vyplňte url složenou z adresy serveru (pozor: zde musí být použit protokol https) a fixní cesty „/Account/Logout“
- Velmi důležité je zaškrtnutí volby „ID tokens (used for implicit and hybrid flows)“, která vybírá, jaký typ tokenu bude po úspěšné autentizaci v EntraID zaslán programu Infoport.
- Konfiguraci potvrdíme tlačítkem „Configure“.

Configure Web

[All platforms](#)

QuickstartDocs

* 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](#)

http://localhost/signin-oidc

Front-channel logout URL

This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.

https://localhost/Account/Logout

Implicit grant and hybrid flows

Request a token directly from the authorization endpoint. If the application has a single-page architecture (SPA) and doesn't use the authorization code flow, or if it invokes a web API via JavaScript, select both access tokens and ID tokens. For ASP.NET Core web apps and other web apps that use hybrid authentication, select only ID tokens. [Learn more about tokens](#).

Select the tokens you would like to be issued by the authorization endpoint:

☐ Access tokens (used for implicit flows)

☒ ID tokens (used for implicit and hybrid flows)

Configure

Cancel

- Následuje nastavení „Certificates & secrets“.

All services > Infoport

Infoport | Certificates & secrets

Search [Got feedback?](#)

- Overview
- Quickstart
- Integration assistant
- Diagnose and solve problems
- Manage
 - Branding & properties
 - Authentication
 - Certificates & secrets**
 - Token configuration
 - API permissions
 - Expose an API
 - App roles
 - Owners
 - Roles and administrators
 - Manifest
- Support + Troubleshooting

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) **Client secrets (0)** Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value ⓘ	Secret ID
No client secrets have been created for this application.			

- pomocí tlačítka „New client secrets“ přidáme nový "client secret" s požadovanou expirací.

Add a client secret

Description

infoport

Expires

Recommended: 180 days (6 months)

Add

Cancel

Pozor: hodnota je pro zkopírování k dispozici (ve sloupečku Value) pouze bezprostředně po vytvoření Client Secret. Pokud si ji hned nekopírujeme, je nutné založit nový Client secret. Tento údaj budeme v konfiguračním manažeru Infoportu zadávat do položky „Client Secret“ (viz. později).

Revision #2

Created 3 March 2025 10:40:43 by Karolína Kavanová

Updated 3 March 2025 13:48:52 by Karolína Kavanová