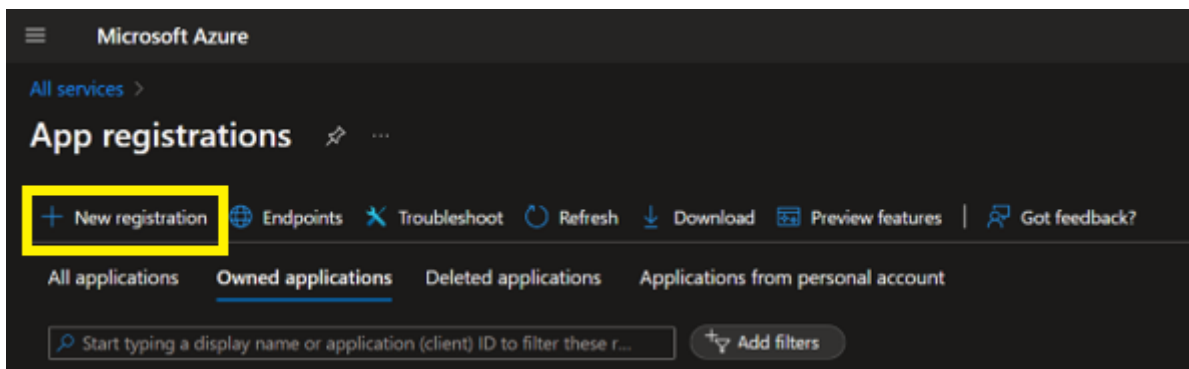
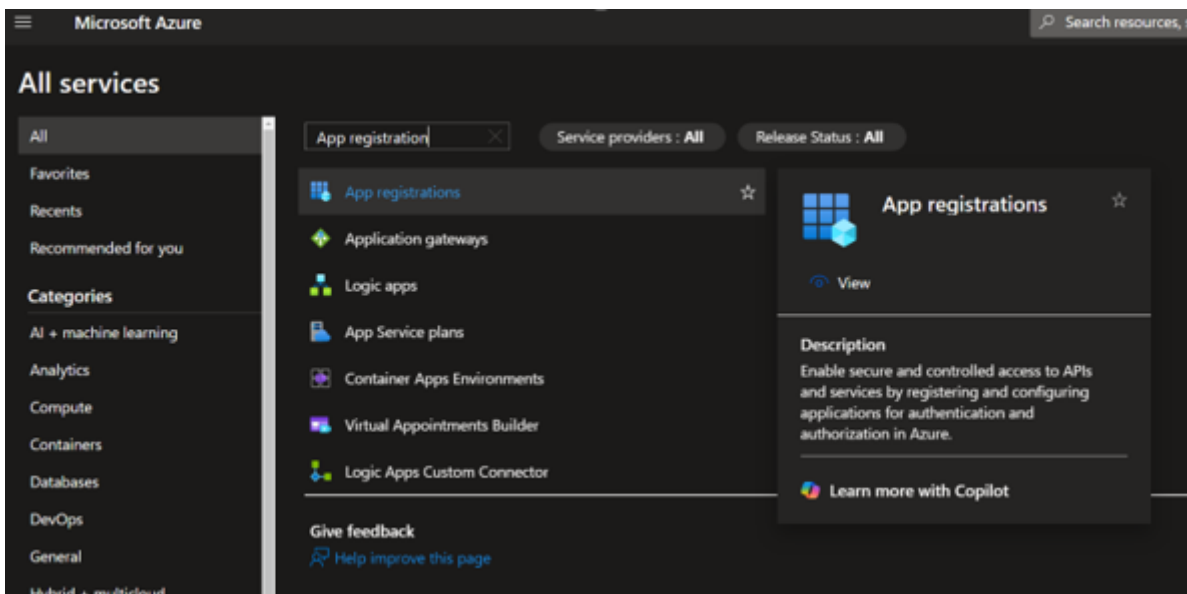


Connecting EaInfoport to Azure EntraID

- First, you need to register the EaInfoport application in Azure. This is done in the "App registration" service.



- by clicking "New registration"
- In the registration process, you only need to fill in the "Name" (for example "Infoport") and complete the registration with the "Register" button.

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

- Basic information about the registered application is displayed as a confirmation.
- The most important information here is the "Application (client) ID". We will enter this information in the Infoport configuration manager under "Client ID" (see later).

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

- If we now go back to the list of registered applications we will see "Infoport" among them (sometimes we need to use the "Refresh" button).
- You can also see the "Application (client) ID" as the primary identifier of the application, which unlike Name cannot be changed after registration.

All services >

App registrations

+ New registration | Endpoints | Troubleshoot | Refresh | Download | Preview features | Got feedback?

All applications | **Owned applications** | Deleted applications | Applications from personal account

Start typing a display name or application (client) ID to filter these r... Add filters

2 applications found

Display name	Application (client) ID	Created on	Certificates & secrets
Infoport	1c0f73b9-9f6e-4806-843d-1c6a1d54c48c	2/20/2025	-
KeyCloak	474d8ea2-54dd-46a3-a72a-2ab07a953c68	12/24/2021	-

- 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“.

- Overview
- Quickstart
- Integration assistant
- Diagnose and solve problems
- Manage
 - Branding & properties
 - Authentication**
 - Certificates & secrets
 - Token configuration
 - API permissions
 - Expose an API
 - App roles

Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.

+ Add a platform

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)

[Help me decide...](#)

- The first thing to do is to add the Infoport application platform using the "Add a platform" button by selecting "Web" from the menu.

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 then asks you to fill in information about two URLs.
- The first of these "Redirect URIs" is the url of the Infoport application where the user will be redirected after logging in with the EntraID.
- Fill in the URI consisting of the server address (where we have Infoport running - in the example it is "http://localhost") and the fixed path "/signin-oidc".
- The second is the "Front-channel logout URL" and is the url of the Infoport application that will be called after the user logs out using single sign-out.
- Fill in the url here consisting of the server address (note: https must be used here) and the fixed path "/Account/Logout".
- It is very important to check the option "ID tokens (used for implicit and hybrid flows)", which selects what type of token will be sent to Infoport after successful authentication in EntraID.
- Confirm the configuration with the "Configure" button.

Configure Web

< All platforms

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](#)

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

- The following is the "Certificates & secrets" setting.

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.			

- Use the "New client secrets" button to add a new "client secret" with the desired expiration date.

Add a client secret

Description

infoport

Expires

Recommended: 180 days (6 months) ▾

Add

Cancel

Note: the value is available for copying (in the Value column) only immediately after the Client Secret is created. If it is not copied immediately, a new Client secret must be created. This will be entered in the Infoport configuration manager under "Client Secret" (see later).

Revision #2

Created 3 March 2025 14:09:44 by Karolína Kavanová

Updated 4 March 2025 08:29:32 by Karolína Kavanová