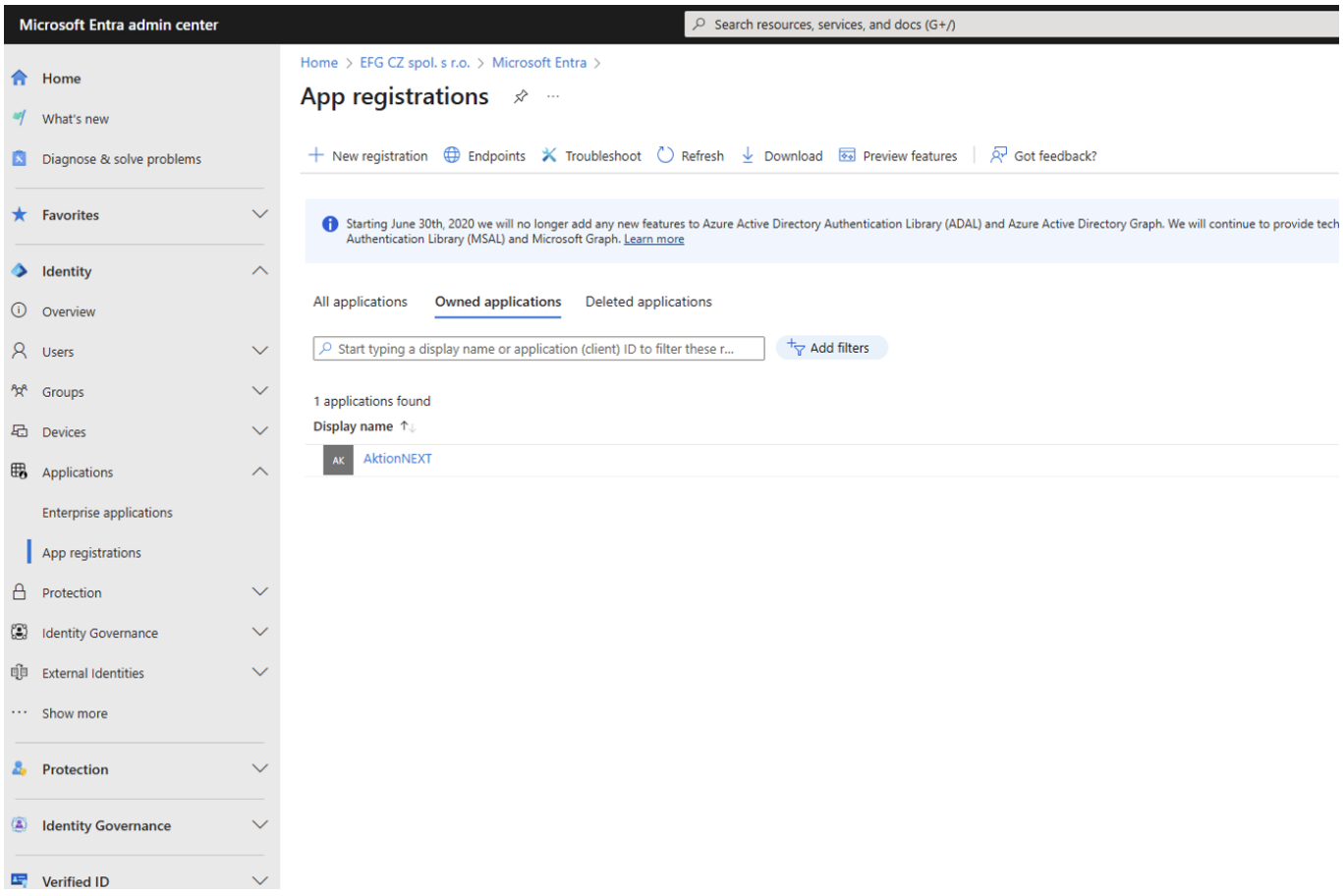
Microsoft Entra ID nastavení (Azure Active Directory)

Konfigurace SW AktionNEXT a Microsoft Entra (dříve Azure Active Directory) pro jednotné přihlašování SSO (revize 5/2025)

Ujistěte se, že máte k dispozici účet Microsoft Entra (AzureAD), ke kterému se můžete přihlásit.

1. Přihlaste se k účtu v roli administrátora (https://entra.microsoft.com/)
2. Vytvoření nové aplikace v Microsoft Entra
   a. Vyhledejte a vyberte službu **Identity.**



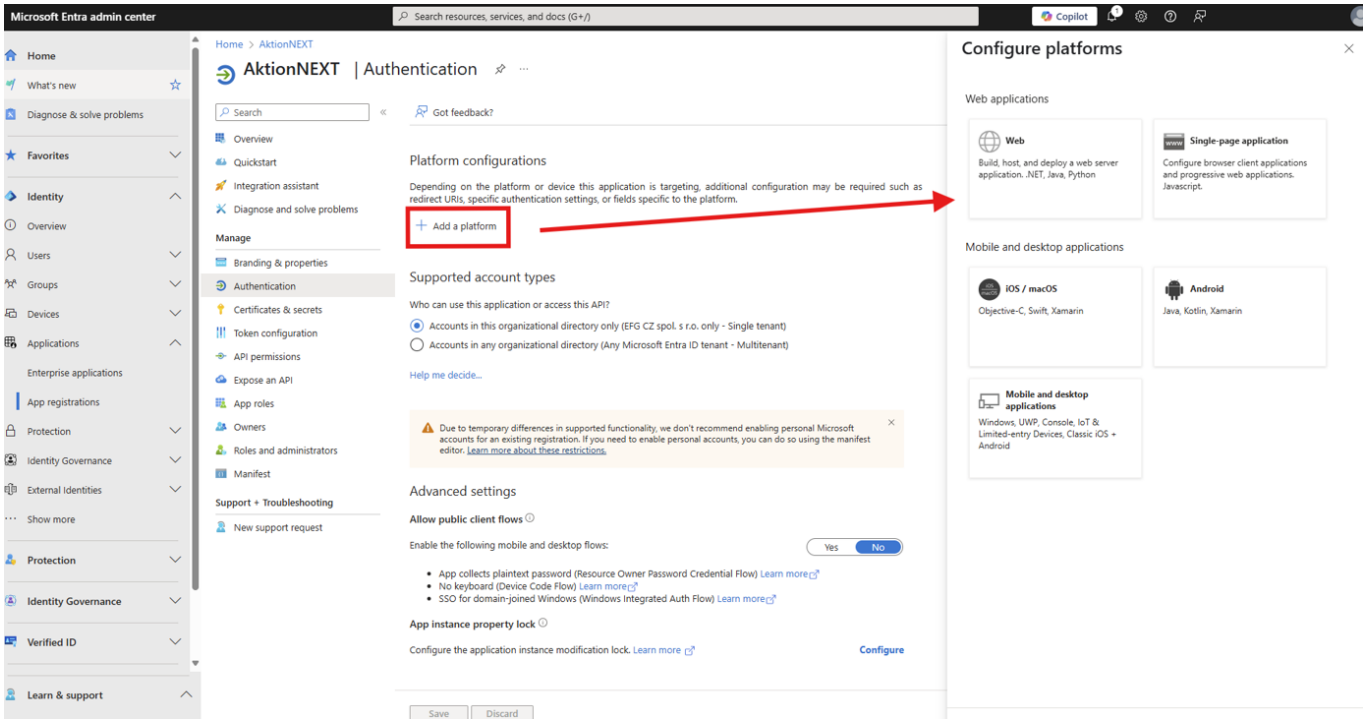
   b. Přejděte do nabídky **Applications – App registration (Registrace aplikací) – Nová registrace (New registration)**. Otevře se obrazovka **Register an application (Zaregistrovat aplikaci).**
   c. V poli **Name (Název)** zadejte název aplikace `AktionNEXT` (dále v textu jen Entra aplikace Aktion).
   d. Vyberte podporované typy účtu, typicky **Account in this organizational directory only – Single tenant (Jen účty v tomto adresáři – jeden tenant)**, pokud máte uživatele z různých tenantů pak vyberte druhou možnost **Account in any organizational directory – Multitenant (Účty v libovolném**

adresáři organizace – více tenantů).

e. Aplikaci uložte **Register (Zaregistrovat)**.

f. Otevřete detail Entra aplikace Aktion v **App registrations – All Applications (Registrace aplikací – Všechny aplikace)**, vyberte aplikaci a přejděte do **Authentication (Ověřování)**.

g. Přidejte platformy **Add platform (Přidat platformu)**

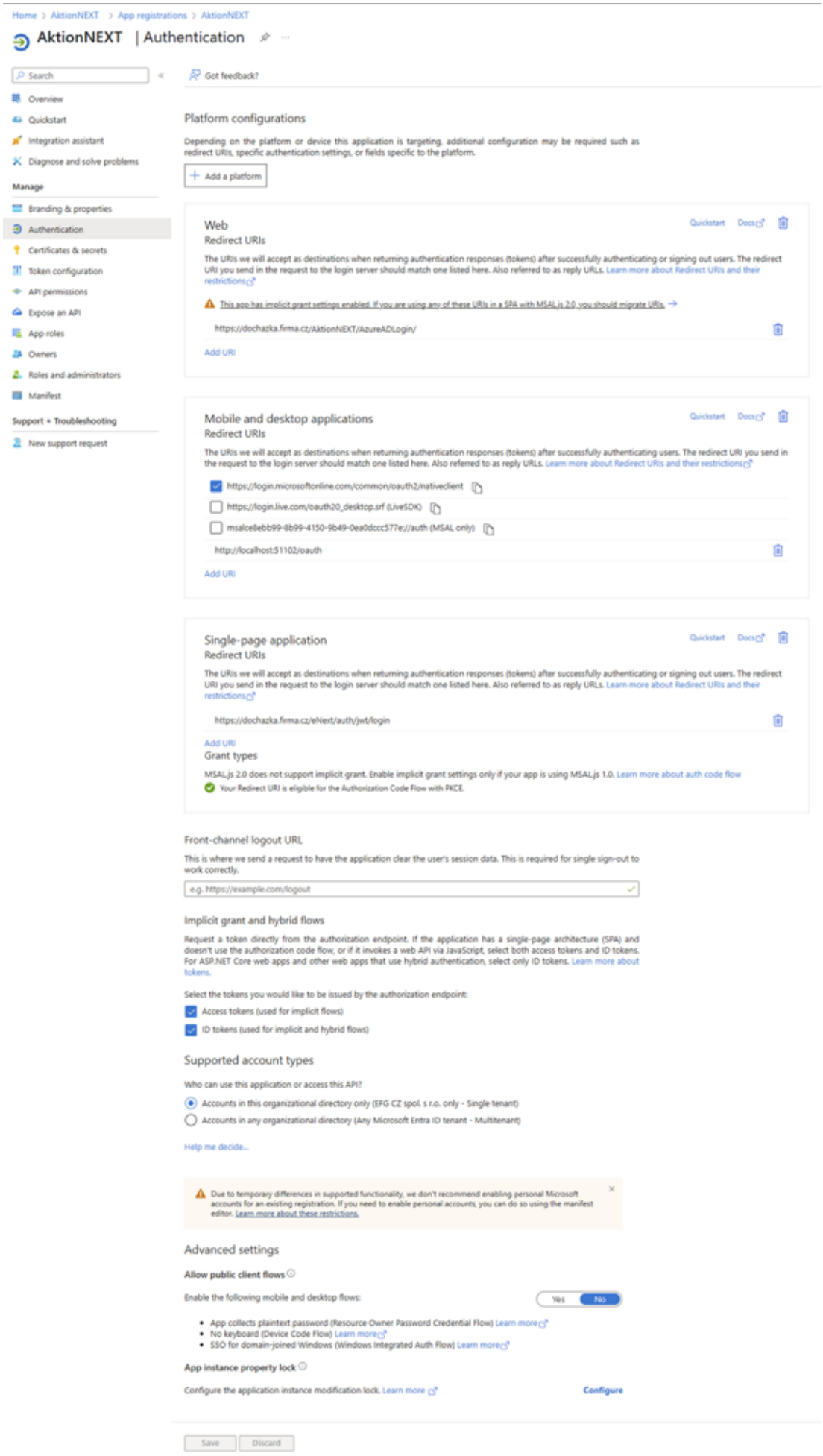


I. Pro ověřování v desktopové (Windows) aplikaci AktionNEXT a v Mobilní aplikaci Aktion zvolte **Mobile and Desktop applications (Mobilní a desktopové aplikace)**. Zde vyberte první **Redirect URIs (Identifikátory URI pro přesměrování)** (`https://login.microsoftonline.com/common/oauth2/nativeclient`) pro desktopovou aplikaci a dále do **Custom redirect URIs (Vlastní identifikátory URI)** zadejte přesně tuto `http://localhost:51102/oauth` adresu pro mobilní aplikaci. Nakonec uložte pomocí **Configure (Konfigurovat).**

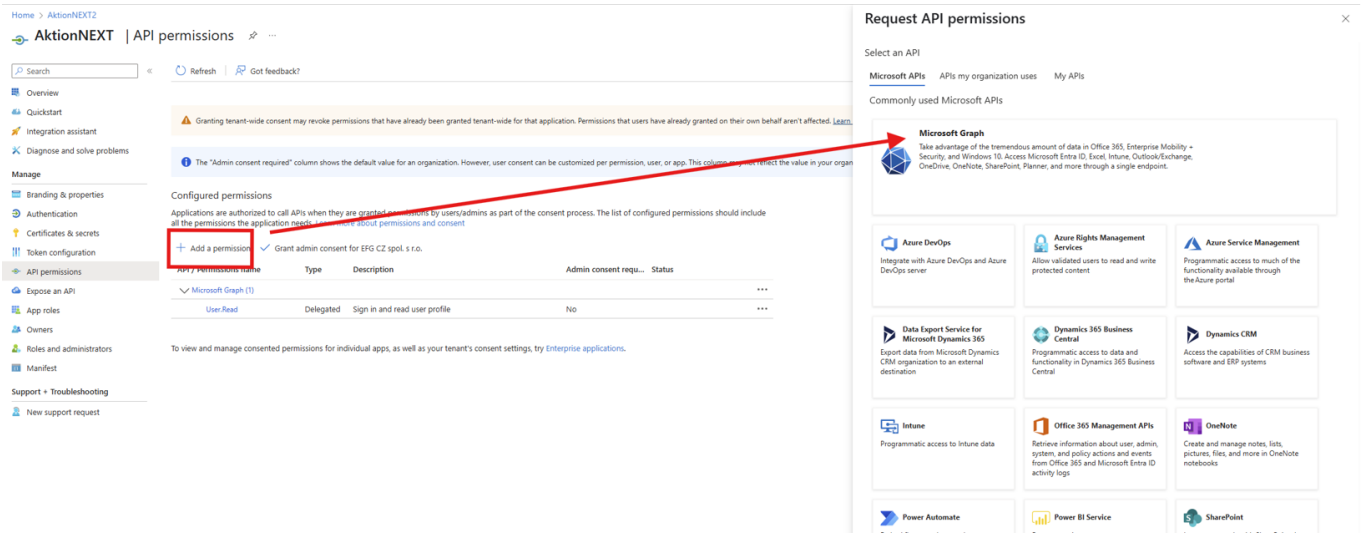
II. Pro ověřování ve webové aplikaci AktionNEXT přidejte platformu **Web** a do **Redirect URIs (Identifikátory URI pro přesměrování)** zadejte adresu vašeho AktionNEXT webu ve formátu `https://dochazka.firma.cz/AktionNEXT/AzureADLogin/` a zaškrtněte **Access tokens (used for implicit flows)** a také **ID tokens (used for implicit and hybrid flows)**. Nakonec uložte pomocí **Configure (Konfigurovat).**

III. Pro ověřování ve webové aplikaci eNEXT přidejte platformu **Single-page application (Jednostránková aplikace)** a do **Redirect URIs (Identifikátory URI pro přesměrování)** zadejte adresu vašeho AktionNEXT webu ve formátu `https://dochazka.firma.cz/eNext/auth/jwt/login`. Nakonec uložte pomocí **Configure (Konfigurovat).**

IV. Všechny přidané platformy by měly vypadat takto:


Home > AktionNEXT > App registrations > AktionNEXT
AktionNEXT | Authentication
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
New support request
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
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
This app has implicit grant settings enabled. If you are using any of these URIs in a SPA with MSALjs 2.0, you should migrate URIs.
https://dochazka.firma.cz/AktionNEXT/AzureADLogin/
Add URI
Mobile and desktop applications
Quickstart
Docs
Redirect URIs
The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating 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://login.microsoftonline.com/common/oauth2/nativeclient
https://login.live.com/oauth20_desktop.srf (LiveSDK)
msalce8ebb99-8b99-4150-9b49-0ea0dccc577e://auth (MSAL only)
http://localhost:51102/oauth
Add URI
Single-page application
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://dochazka.firma.cz/eNext/auth/jwt/login
Add URI
Grant types
MSALjs 2.0 does not support implicit grant. Enable implicit grant settings only if your app is using MSALjs 1.0. Learn more about auth code flow
Your Redirect URI is eligible for the Authorization Code Flow with PKCE.
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.
e.g. https://example.com/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)
Supported account types
Who can use this application or access this API?
Accounts in this organizational directory only (EFG CZ spol. s r.o. only - Single tenant)
Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
Help me decide...
Due to temporary differences in supported functionality, we don't recommend enabling personal Microsoft accounts for an existing registration. If you need to enable personal accounts, you can do so using the manifest editor. Learn more about these restrictions.
Advanced settings
Allow public client flows
Enable the following mobile and desktop flows:
Yes
No
App collects plaintext password (Resource Owner Password Credential Flow) Learn more
No keyboard (Device Code Flow) Learn more
SSO for domain-joined Windows (Windows Integrated Auth Flow) Learn more
App instance property lock
Configure the application instance modification lock. Learn more
Configure
Save
Discard

h. Dále nastavte oprávnění. Přejděte do **sekce API permissions (Oprávnění rozhraní API)** a zvolte **Add permission (Přidat oprávnění).** Otevře se obrazovka **Request API permissions (Požádat o oprávnění rozhraní API).**



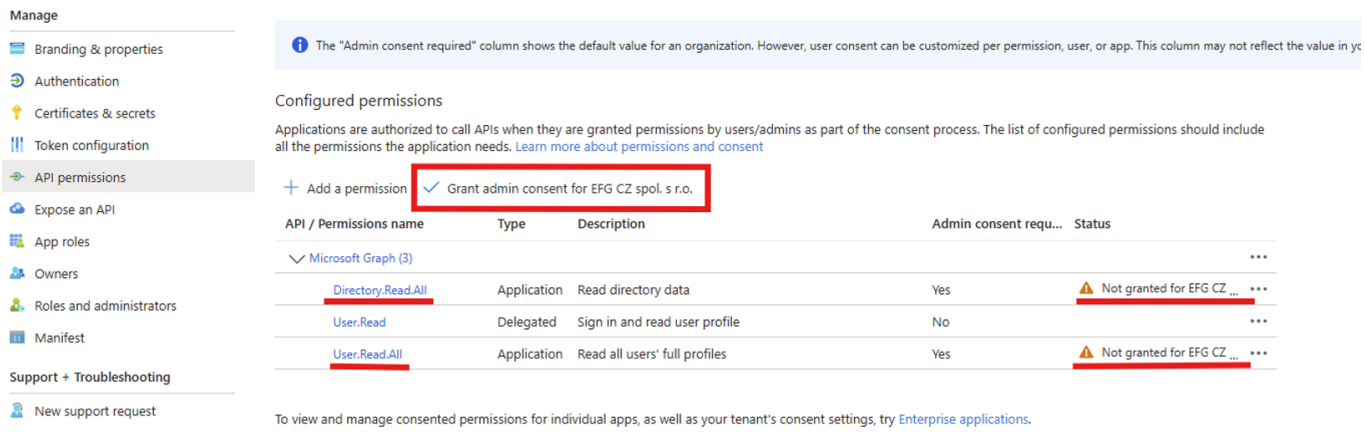
I. Klikněte na možnost **Microsoft Graph** a jako typ oprávnění pro vaši aplikaci vyberte možnost **Application permissions (Oprávnění aplikace).**

II. V části **Select permissions (Vybrat oprávnění)** vyhledejte `Directory — Directory.Read.All` a vyberte ho.

III. Dále vyhledejte `User — User.Read.All` a také ho vyberte

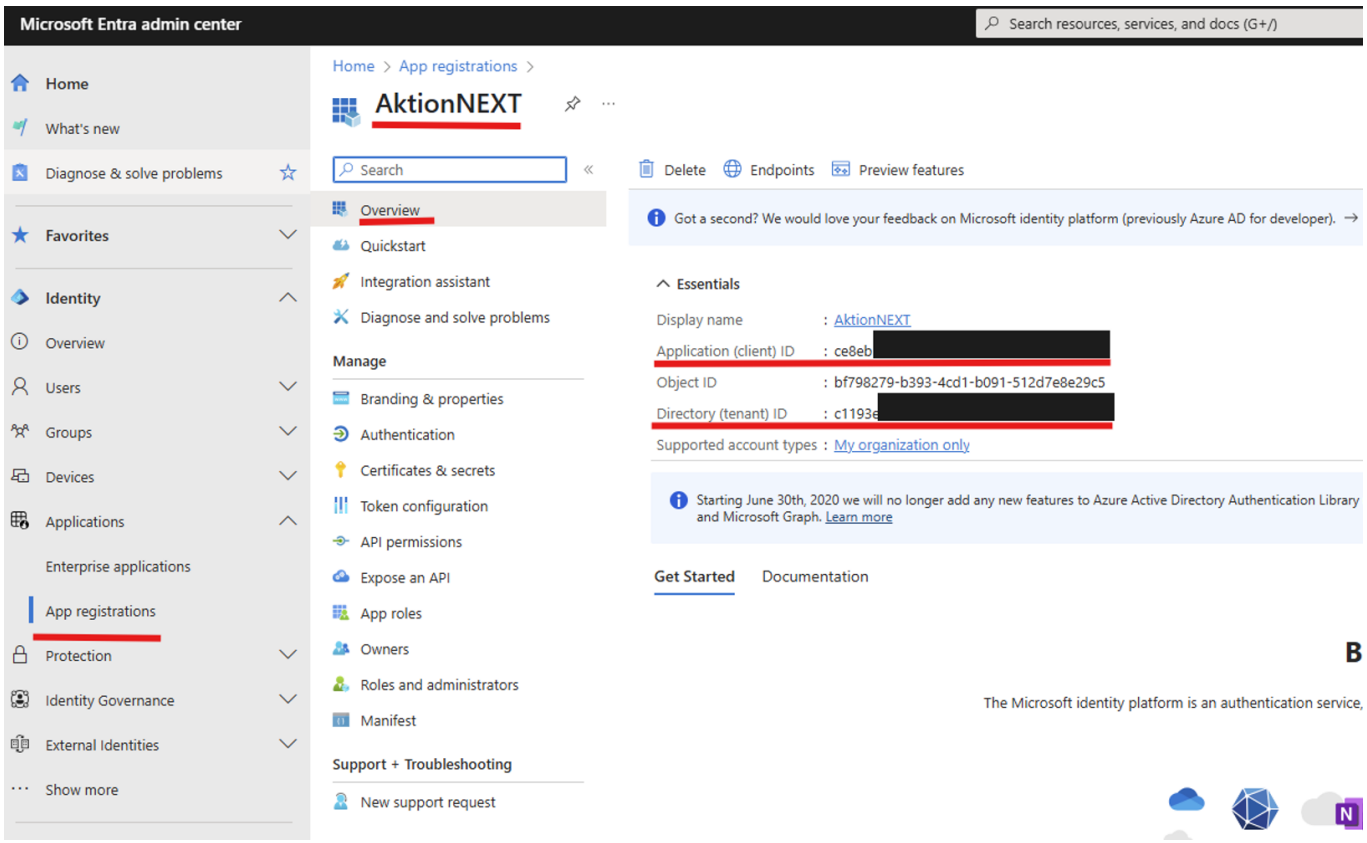
IV. Potvrďte pomocí **Add permissions (Přidat oprávnění)**

i. Přidaná oprávnění schvalte nebo nechte schválit pomocí **Grant admin consent (Udělit souhlas správce)**



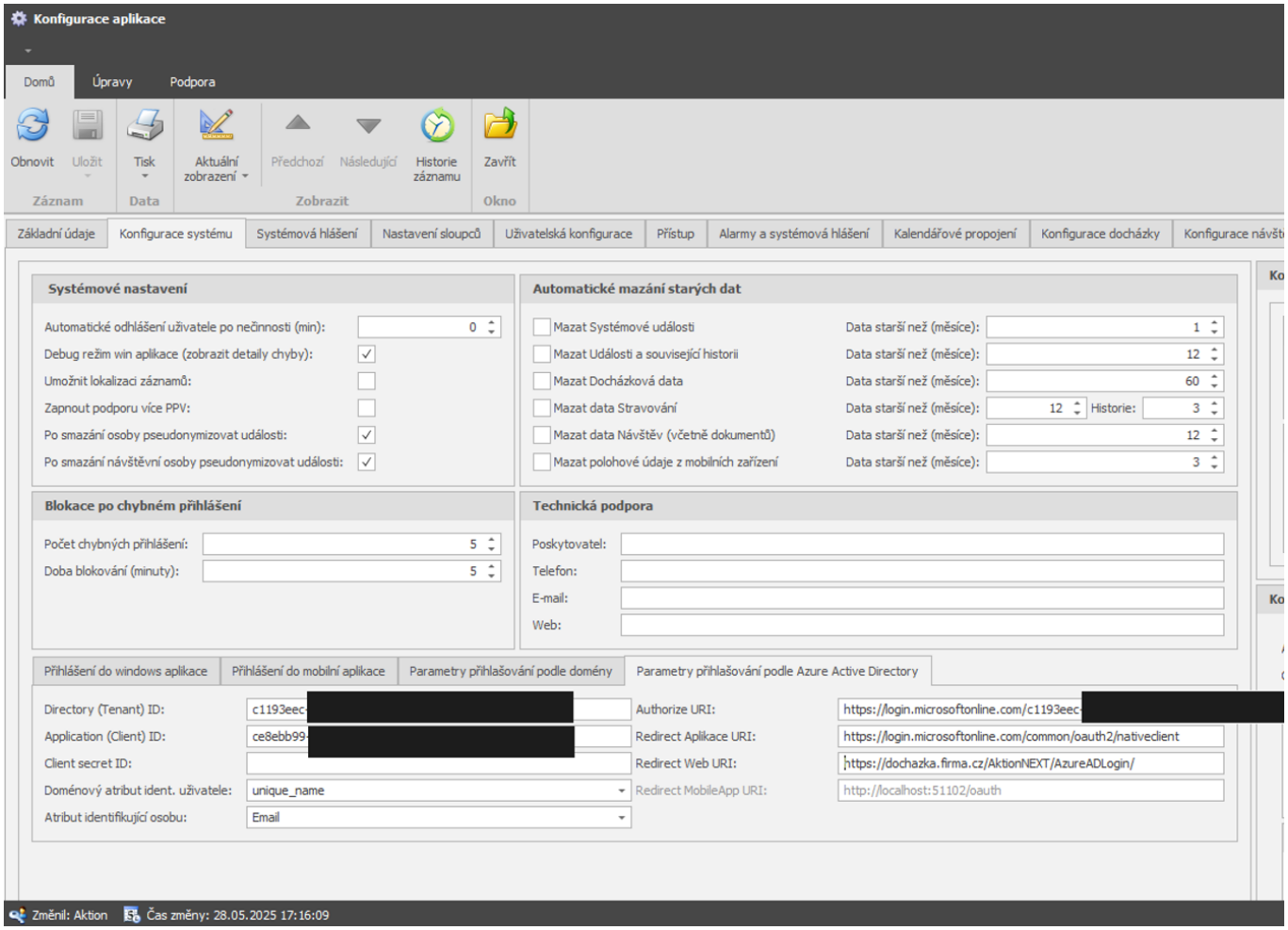
3. Konfigurace SW AktionNEXT

a. Z nastavení Entra aplikace Aktion zjistíme **Directory (tenant ID (ID adresáře (tenanta))** a **Application (client) ID (ID aplikace (tenanta)).**

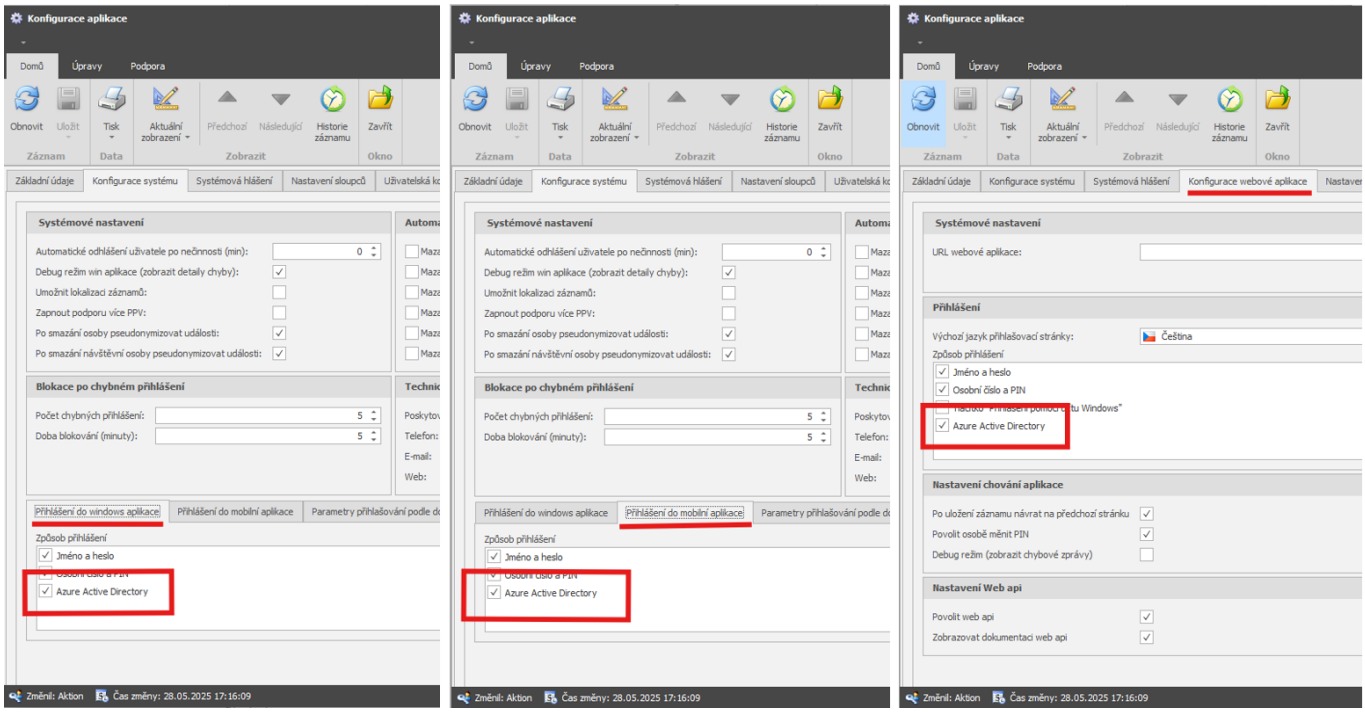


b. V desktopové aplikaci AktionNEXT přejděte do **Konfigurace aplikace**, na záložku **Konfigurace systému**, podzáložka **Parametry přihlašování podle Azure Active Directory**.

c. Zde vyplňte **Directory (tenant) ID** a **Application (client) ID** dle údajů zjištěných v předešlém kroku.



d. **Client secret ID** nevyplňujte.
e. **Autorize URI** vyplňte v případě že jste Entra aplikaci Aktion nastavili jako Single tenant (viz bod 2d.), tak `https://login.microsoftonline.com/directory_tenant_id` bez lomítka na konci, kde `directory_tenant_id` je stejný kód jako v Directory (tenant) ID. V případě Multitenant Entra aplikace Aktion vyplňte `https://login.microsoftonline.com/common`.
f. **Redirect aplikace URI** je adresa přesměrování pro desktopovou aplikaci a bude `https://login.microsoftonline.com/common/oauth2/nativeclient` (viz bod 2gI.).
g. **Redirect Web Uri** zadejte adresu vašeho AktionNEXT webu ve formátu `https://dochazka.firma.cz/AktionNEXT/AzureADLogin/` (viz bod 2gII.), pro eNext webovou aplikaci zadejte `https://dochazka.firma.cz/eNext/auth/jwt/login` (viz bod 2gIII.).
h. **Redirect mobile app** je předvyplněno na `http://localhost:51102/oauth` (viz bod 2gI.).
i. **Doménový atribut identifikující uživatele** vyberte atribut z MS Entra, který je znám na straně MS Entra i v Aktion NEXT, typicky `unique_name` nebo `email`.
j. **Atribut identifikující osobu** vyberte atribut z Aktion NEXTu, pomocí kterého napárujete uživatele z MS Entra, typicky `Email` (Agenda Osoby, doplňující údaje, E-mail).
k. Nakonec je potřeba povolit způsob **přihlášení pomocí Azure Active Directory** pro Windows (desktopovou) aplikaci, pro mobilní aplikaci a pro webovou aplikaci. **V Konfiguraci aplikace**, záložka **Konfigurace systému**, podzáložka **Přihlášení do Windows aplikace** a **Přihlášení do mobilní aplikace**, nebo **Konfigurace aplikace**, záložka **Konfigurace systému**, podzáložka **Konfigurace webové aplikace**.



4. Podmínky pro fungování

a. Přihlašující se klienti musí mít přístup na internet na servery Microsoft Entra ID.
b. Aplikační server Aktion NEXT a webový server aplikace Aktion NEXT (eNext) musí mít přístup na internet na servery Microsoft Entra ID, protože ověřují vystavené přihlašovací tokeny.
c. Webová aplikace Aktion NEXT musí běžet na HTTPS protokolu (platný certifikát), a to i v případě lokálního provozu.

d. Osoby v Aktion NEXTu musí mít vyplněný e-mail nebo jiný atribut pro identifikaci (viz bod 3j), aby bylo možné osobu do systému přihlásit.