

SSO - Azure AD

Giúp người dùng có thể truy cập vào những trang web main và web portal mà chỉ cần đăng nhập một lần duy nhất

1. MỤC TIÊU

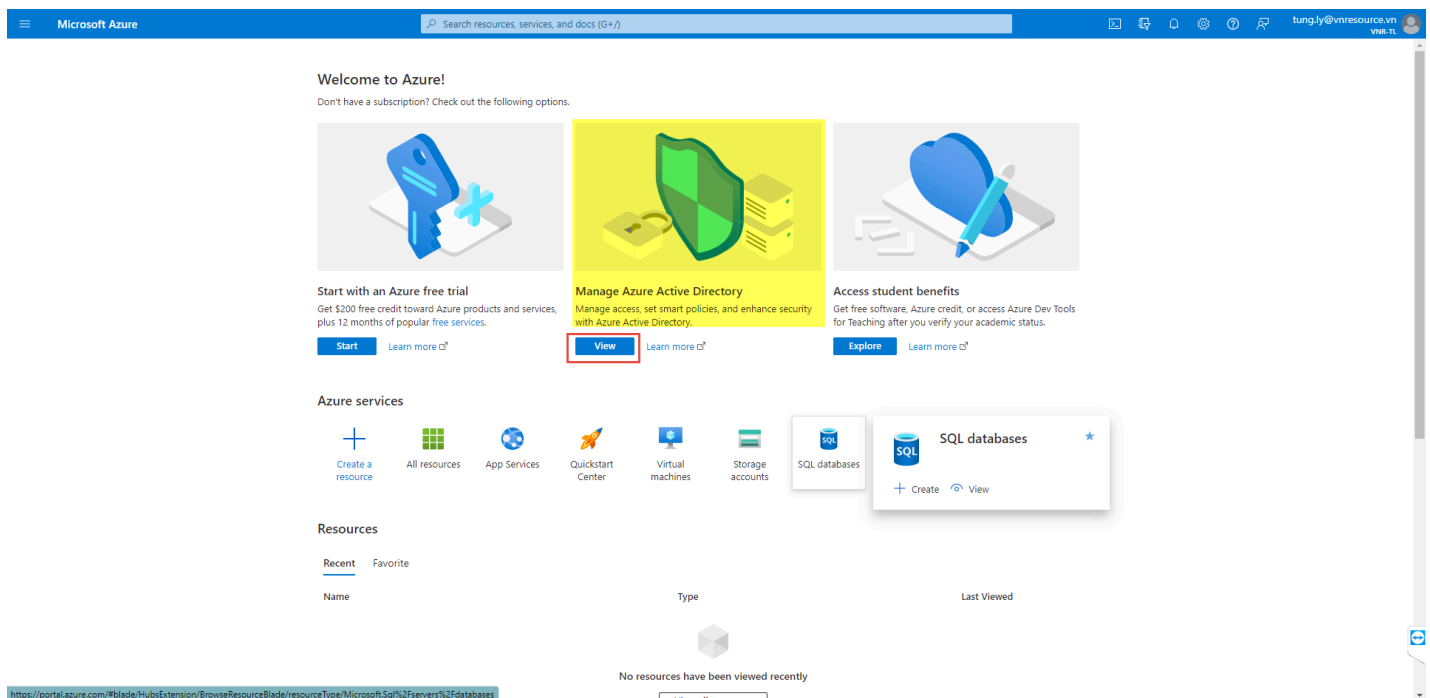
- Cho phép đăng nhập vào web main và web portal Vnr mà không cần biết password của Vnr



Note: Chức năng đăng nhập azure apply từ version : V8.10.32.01 trở về sau


2. ĐĂNG NHẬP VÀO AZURE

- Đăng nhập vào azure vào chọn Manage Azure Active Directory



3. ĐĂNG KÝ WEB APP (WEB MAIN)



[Main_url] : url của web main vd: <https://tl-main.dev.local> 

3.1 Đăng ký App

- Chọn App Registrations bên trái vào chọn New Registrations bên phải

The screenshot shows the Microsoft Azure portal interface. On the left sidebar, under the 'Manage' section, 'App registrations' is highlighted with a red box and a circled '1'. At the top of the main content area, the '+ New registration' button is highlighted with a red box and a circled '2'. Below this, there's a search bar and a table of applications. The table has the following data:

| Display name | Application (client) ID | Created on | Certificates & secrets |
|-----------------|--------------------------------------|------------|------------------------|
| app-test-mail | 59c18be2-7841-45af-a943-2e4bf4c6bb14 | 3/18/2022 | Current |
| app-test02-mail | eb0e6bbb-eeb8-4e2e-91b4-f2250bc19e57 | 3/23/2022 | - |

- Trong trang đăng ký app, nhập vào thông tin

+ Vùng Name : nhập vào tên của app (vd: Vnr SS0 Main - TL)

+ Vùng Supported account types chọn Accounts in this organizational directory only

+ Vùng Redirect URI (optional) chọn Web và điền thông tin web main:
[Main_url]/Home/ExternalLogoutFromIdp

Nhấn vào Register để tiến hành tạo app.

Microsoft Azure

Search resources, services, and docs (G+)

Home > vnr-tl | App registrations >

Register an application

* Name

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

Vnr SSO Main - TL ✓

Supported account types

Who can use this application or access this API?

☐ Accounts in this organizational directory only (vnr-tl only - Single tenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

☒ Accounts in any organizational directory (Any Azure AD directory - 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.

Web https://tl-main.dev.local/Home/ExternalLoginRedirect/Provider-01 ✓

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

3.2 Chỉnh sửa thông tin App

- Vào App vừa tạo

Microsoft Azure

Search resources, services, and docs (G+)

Home > vnr-tl

vnr-tl | App registrations

Azure Active Directory

Overview

Preview features

Diagnose and solve problems

Manage

Users

Groups

External Identities

Roles and administrators

Administrative units

Enterprise applications

Devices

App registrations

Identity Governance

Application proxy

Custom security attributes (Preview)

Licenses

Azure AD Connect

Custom domain names

Mobility (MDM and MAM)

Password reset

User settings

Properties

Security

https://portal.azure.com/#

+ New registration Endpoints Troubleshooting Refresh Download Preview features Got feedback?

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

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

7 applications found

| Display name ↑ | Application (client) ID | Created on ↑ | Certificates & secrets |
|---------------------|---------------------------------------|--------------|------------------------|
| app-OAUTH2 | 48c6c7c-ad54-472c-b0da-0f977d1e4328 | 4/4/2022 | Current |
| app-test-mail | 59c18be2-7841-45af-a943-2e4bf4c0bb14 | 3/18/2022 | Current |
| app-test-mail-v2 | 4cdddec89-d61c-4a9c-8edc-7e3d67aa929d | 8/9/2022 | Current |
| app-test02-mail | eb0e6bbb-eeb8-4e2e-91b4-f2250bc19e57 | 3/23/2022 | - |
| Vnr SSO Main | 19ef47c2-8c02-4d07-a72c-4627984504d7 | 7/11/2022 | - |
| Vnr SSO Main - TL | 95617df1-1cdb-4c18-a679-d6b3c4f81475 | 7/14/2022 | - |
| Vnr SSO Portal - TL | dffa9e52-7d29-4cd0-a04f-c2a62f2e360 | 8/9/2022 | - |

- Chọn direct URIs

- Trong màn hình app, nhập các thông tin url

1. Direct URIs : [Main_url]/Home/ExternalLoginRedirect/Provider-01

2. Direct URIs : [Identity_url]/signin-microsoft

“

3. Front-channel logout URL : [Main_url]/Home/ExternalLogoutFromIdp

4. Select the tokens you would like to be issued by the authorization endpoint : chọn ID tokens

4. Nhấn save

The screenshot displays the Microsoft Azure portal interface for configuring an application registration named 'Vnr SSO Main - TL'. The 'Authentication' tab is active, showing various configuration options. The 'Redirect URIs' section lists two URLs: 'https://ti-main.dev.local/Home/ExternalLoginRedirect/Provider-01' and 'https://ti-ids.dev.local/signin-microsoft'. The 'Front-channel logout URL' is set to 'https://ti-main.dev.local/Home/ExternalLogoutFromIdp'. Under the 'Select the tokens you would like to be issued by the authorization endpoint' section, the 'ID tokens (used for implicit and hybrid flows)' option is selected. The 'Supported account types' section shows 'Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft' as the selected option. The 'Save' button is highlighted in green.

- Trong màn hình đăng ký app

- Ghi nhận client ID để cấu hình vào web HRM cho những bước sau.

Microsoft Azure

Home > vnr-tl | App registrations > Vnr SSO Main - TL

Search (Ctrl+/)

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

Troubleshooting

New support request

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Essentials

Display name : Vnr SSO Main - TL

Application (client) ID : 95617df1-1c0b-4c18-a679-d6b3c4f81475

Object ID : fec7bd4e-1947-44ee-9d3a-50dec4fc74e

Directory (tenant) ID : e356ae7e-75ca-4103-8edf-6371e8ef968f

Supported account types : All Microsoft account users

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 L... : Vnr SSO Main - TL

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) for .NET. We will continue to provide technical support and security updates but we will no longer provide feature updates. [Learn more](#)

Starting November 9th, 2020 end users will no longer be able to grant consent to newly registered multitenant apps without verified publishers. [Add MPN ID to verify publisher](#)

Get Started Documentation

Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. [Learn more](#)

- Trong màn hình app, chọn **Token configuration** và chọn **Add optional claim**

Microsoft Azure

Home > vnr-tl | App registrations > Vnr SSO Main - TL

Vnr SSO Main - TL | Token configuration

Search (Ctrl+/)

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

Troubleshooting

New support request

Optional claims

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

2 + Add optional claim + Add groups claim

| Claim | Description | Audience |
|-------------|-------------|----------|
| No results. | | |

3 ID

4 sid

5 Add Cancel

Once a token type is selected, you may choose from a list of available optional claims.

* Token type

Access and ID tokens are used by applications for authentication. [Learn more](#)

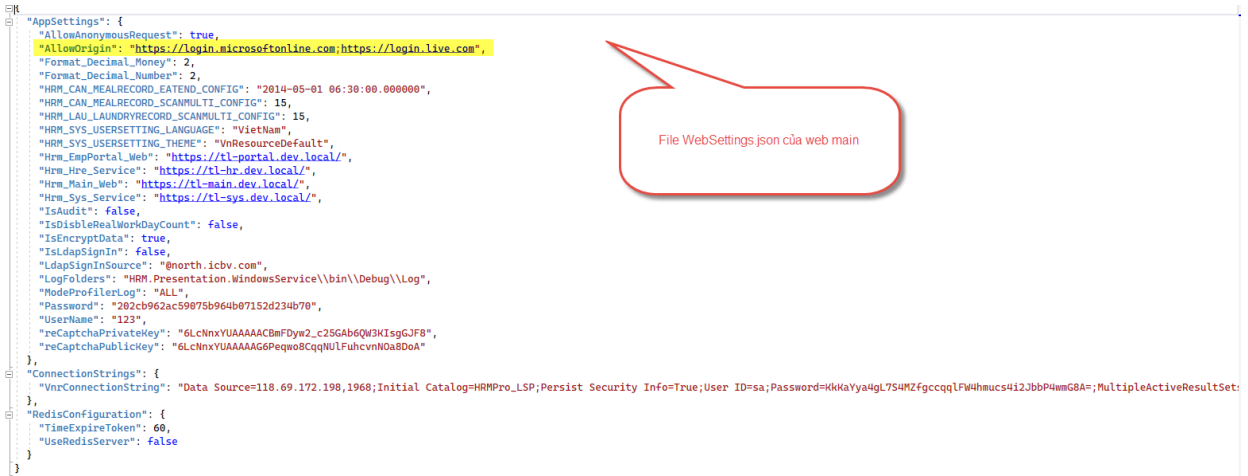
Access

| Claim | Description | Audience |
|--------------------------|---|---------------|
| preferred_username | Provides the preferred username c... | Azure AD only |
| pwd_exp | The datetime at which the passwor... | Azure AD only |
| pwd_url | A URL that the user can visit to ch... | Azure AD only |
| sid | Session ID, used for per-session us... | All users |
| tenant_ctry | Resource tenant's country/region | Azure AD only |
| tenant_region_scope | Region of the resource tenant | Azure AD only |
| upn | An identifier for the user that can ... | Azure AD only |
| verified_primary_email | Sourced from the user's PrimaryAu... | Azure AD only |
| verified_secondary_em... | Sourced from the user's Secondar... | Azure AD only |
| vnet | VNET specifier information | Azure AD only |
| xms_pdl | Preferred data location | Azure AD only |
| xms_pl | User-preferred language | Azure AD only |
| xms_tpl | Tenant-preferred language | Azure AD only |
| xtid | Zero-trust Deployment ID | Azure AD only |

3.3 Cấu hình trong Web main HRM

- Trong WebSettings.json của web main, cấu hình key **AllowOrigin**

```
vd: "AllowOrigin":
"https://login.microsoftonline.com;https://login.live.com"
```



- Tạo file auth.config của thư mục HRM.Presentation.Main

[BaseUrl] : url của web main

[ClientId] : clientid đã ghi nhận ở những bước trước

[Id] : "Provider-01" (lấy thông tin provider từ bước đăng ký app)

[Tenant] : "common" (Nếu là common thì tài khoản doanh nghiệp hoặc tài khoản cá nhân đều vào được, nếu là 1 id cụ thể thì chỉ tài khoản thuộc tenant mới vào được)

```
1 //Tên file : auth.config
2 {
3     "UseExternalLogin": true,
4     "BaseUrl": "https://tl-main.dev.local",
5     "RedirectSignIn": "/Home/ExternalLoginRedirect",
6     "SignInUrl": "/Home/Login",
7     "SignOutUrl": "/Home/Logout",
8     "RedirectSignoutFromIdp": "/Home/ExternalLogoutFromIdp",
9     "ProviderConfiguration": [
10         {
11             "Id": "Provider-01",
12             "Enabled": true,
13             "ProviderName": "AzureOpenIdConnect",
14             "DisplayName": "Vnr SSO Main - TL",
15             "Tenant": "common",
16             "ClientId": "95617df1-1cdb-4c18-a679-d6b3c4f81475"
17         }
18     ]
19 }
```

4. ĐĂNG KÝ WEB APP (WEB PORTAL)



[Portal_url] : url của web portal vd: <https://tl-portal.dev.local>

4.1 Đăng ký App

- Chọn **App Registrations** bên trái vào chọn **New Registrations** bên phải

Microsoft Azure

Home > vnr-tl | App registrations

+ New registration

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

All applications Owned applications Deleted applications Applications from personal account

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

2 applications found

| Display name | Application (client) ID | Created on | Certificates & secrets |
|-----------------|--------------------------------------|------------|------------------------|
| app-test-mail | 59c18be2-7841-45af-a943-2e4bf4c6bb14 | 3/18/2022 | Current |
| app-test02-mail | eb0e6bbb-eeb8-4e2e-91b4-f2250bc19e57 | 3/23/2022 | - |

- Trong trang đăng ký app, nhập vào thông tin

+ **Vùng Name** : nhập vào tên của app (vd: Vnr SSO Portal - TL)

+ **Vùng Supported account types** chọn **Accounts in this organizational directory only**

+ **Vùng Redirect URI (optional)** chọn **Web** và điền thông tin web main:
[Portal_url]/Portal/ExternalLoginRedirect

Nhấn vào **Register** để tiến hành tạo app.

Microsoft Azure Search resources, services, and docs (G+)

Home > vnr-tl | App registrations >

Register an application

* Name

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

Vnr SSO Portal - TL ✓

Supported account types

Who can use this application or access this API?

☐ Accounts in this organizational directory only (vnr-tl only - Single tenant)
☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
☒ Accounts in any organizational directory (Any Azure AD directory - 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.

Web https://tl-portal.dev.local/Portal/ExternalLoginRedirect ✓

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

4.2 Chỉnh sửa thông tin App

- Vào App vừa tạo

Microsoft Azure Search resources, services, and docs (G+)

Home > vnr-tl

vnr-tl | App registrations Azure Active Directory

Overview Preview features Diagnose and solve problems

Manage

- Users
- Groups
- External Identities
- Roles and administrators
- Administrative units
- Enterprise applications
- Devices
- App registrations**
- Identity Governance
- Application proxy
- Custom security attributes (Preview)
- Licenses
- Azure AD Connect
- Custom domain names
- Mobility (MDM and MAM)
- Password reset
- User settings

+ New registration Endpoints Troubleshooting Refresh Download Preview features Got feedback?

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

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

7 applications found

| Display name | Application (client) ID | Created on | Certificates & secrets |
|---------------------|--------------------------------------|------------|------------------------|
| app-OAUTH2 | 48c6cf7c-ad54-4f2c-b0da-0f977d1e4328 | 4/4/2022 | Current |
| app-test-mail | 59c18be2-7841-45af-a943-2e4bf4c6bb14 | 3/18/2022 | Current |
| app-test-mail-v2 | 4cddec89-d61c-4a9c-8edc-7e3d67aa929d | 8/9/2022 | Current |
| app-test02-mail | eb0e6bbb-eeb8-4e2e-91b4-f2250bc19e57 | 3/23/2022 | - |
| Vnr SSO Main | 19ef47c2-8c02-4d07-a72c-4627984504d7 | 7/11/2022 | - |
| Vnr SSO Main - TL | 95617df1-1cdb-4c18-a679-d6b3c4f81475 | 7/14/2022 | - |
| Vnr SSO Portal - TL | dfda9e52-7d29-4cd0-a04f-c2a62f2e360 | 8/9/2022 | - |

- Chọn direct URIs

- Trong màn hình app, nhập các thông tin url

1. Direct URIs : [Portal_url]/Portal/ExternalLoginRedirect/Provider-01

2. Direct URIs : [Identity_url]/signin-microsoft



3. Front-channel logout URL :

[Portal_url]/Portal/ExternalLogoutBackChannel

4. Select the tokens you would like to be issued by the authorization endpoint : chọn ID tokens

4. Nhấn save

Home > vnr-tl | App registrations > Vnr SSO Portal - TL

Search (Ctrl+/) Delete Endpoints Preview features

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

Troubleshooting

New support request

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Essentials

Display name : Vnr SSO Portal - TL

Application (client) ID : ddfa9e52-7d29-4cd0-a04f-c2a62ff2e360

Object ID : dcf71fa-4edb-48bd-8ce6-12cb35c1bfc7

Directory (tenant) ID : e356ae7e-75ca-4103-8edf-6371e8ef968f

Supported account types : All Microsoft account users

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 L... : Vnr SSO Portal - TL

Microsoft Azure

Home > vnr-tl | App registrations > Vnr SSO Portal - TL

Vnr SSO Portal - TL | Authentication

Provider-01

Got feedback?

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://tl-portal.dev.local/Portal/ExternalLoginRedirect/Provider-01

Add URI

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://tl-portal.dev.local/Portal/ExternalLogoutBackChannel

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 any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft

Save Discard

- Trong màn hình đăng ký app

- Ghi nhận client ID để cấu hình vào web HRM cho những bước sau.

- Trong màn hình app, chọn **Token configuration** và chọn **Add optional claim**

4.3 Cấu hình trong Web portal HRM

- Trong WebSettings.json của web portal, cấu hình key **AllowOrigin**

```
vd: "AllowOrigin":  
"https://login.microsoftonline.com;https://login.live.com"
```

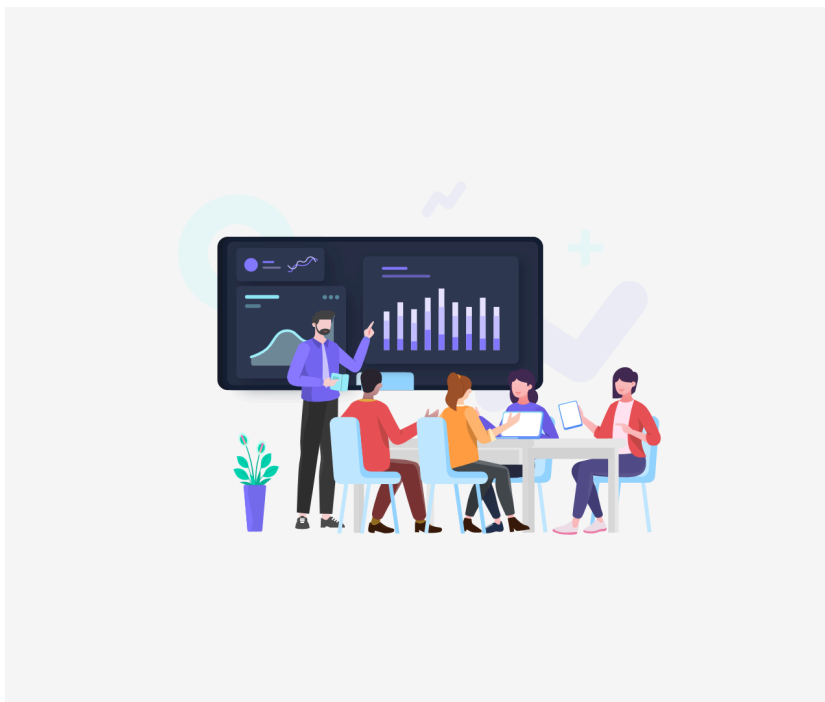
```

{
  "AppSettings": {
    "AllowAnonymousRequest": true,
    "AllowOrigin": "https://login.microsoftonline.com;https://login.live.com",
    "GoogleClientID": "520218699955-1pq0n2q1jmrccchahmr0bnLcu0m7tk0.apps.googleusercontent.com",
    "Hrm_EmpPortal_Web": "https://tl-portal.dev.local/",
    "Hrm_Hr_Service": "https://tl-hr.dev.local/",
    "Hrm_Main_Web": "https://tl-main.dev.local/",
    "Hrm_Sys_Service": "https://tl-sys.dev.local/",
    "IsAudit": false,
    "IsEncryptData": true,
    "IsGoogleSignIn": false,
    "IsIdapSignIn": false,
    "IdapSignInSource": "@north.icbv.com",
    "ModeProfilerLog": "ALL",
    "NewPortal": "true",
    "Password": "202cb962ac59075b964b07152d234b70",
    "SuperAdmin": "khang.nguyen",
    "UseLanguage": "VN, EN",
    "UserName": "khang.nguyen",
    "reCaptchaPrivateKey": "6LcNnxYUAAAAACBmFdyw2_c25GAb6Qh3VIsGcJF8",
    "reCaptchaPublicKey": "6LcNnxYUAAAAAG6Peqwo8CqqNUIFuhcvnNOa8DoA",
    "IsLoadIframeNewLayout": "true"
  },
  "ConnectionStrings": {
    "VnrConnectionString": "Data Source=118.69.172.198,1968;Initial Catalog=HRMPro_LSP;Persist Security Info=True;User ID=sa;Password=k0iaYya4gLT54M2fgccqqlFWHmucs412JbbP4umG8A;MultipleActiveResultSet:
  }
}

```

WebSetting.json của portal

Nếu cấu hình key **"UsingADFS_Azure":true** trong **webSettings.json** thì trên trang đăng nhập portal sẽ ẩn đi **userName** và **Password**.



Đăng nhập với

Chọn phương thức đăng nhập portal

Azure-[ADD - VL][VL - Test - 02]

ADFS-[fs.dev.local][VL-PORTAL]

Azure-[qByc][VL - Portal - WSFED]

hoặc

Đăng nhập với tài khoản Portal

🇻🇳 🇺🇸 🇬🇧

- Tạo file **auth.config** của thư mục **HRM.Presentation.EmpPortal**

[BaseUrl] : url của web portal

[ClientId] : clientid đã ghi nhận ở những bước trước

[Id] : "Provider-01" (lấy thông tin provider từ bước đăng ký app)

[Tenant] : "common" (Nếu là common thì tài khoản doanh nghiệp hoặc tài khoản cá nhân đều vào được, nếu là 1 id cụ thể thì chỉ tài khoản thuộc tenant mới vào được)

```

1 //Tên file : auth.config
2 {
3   "UseExternalLogin": true,
4

```

```
5  "BaseUrl": "https://tl-portal.dev.local",
6  "RedirectSignIn": "/Portal/ExternalLoginRedirect",
7  "SignInUrl": "/Portal/Login",
8  "SignOutUrl": "/Portal/New_Logout",
9  "RedirectSignoutFromIdp": "/Portal/ExternalLogoutFromIdp",
10 "ProviderConfiguration": [
11   {
12     "Id": "Provider-01",
13     "Enabled": true,
14     "ProviderName": "AzureOpenIdConnect",
15     "DisplayName": "Vnr SSO Portal - TL",
16     "Tenant": "common",
17     "ClientId": "dfda9e52-7d29-4cd0-a04f-c2a62ff2e360"
18   }
19 ]
}
```