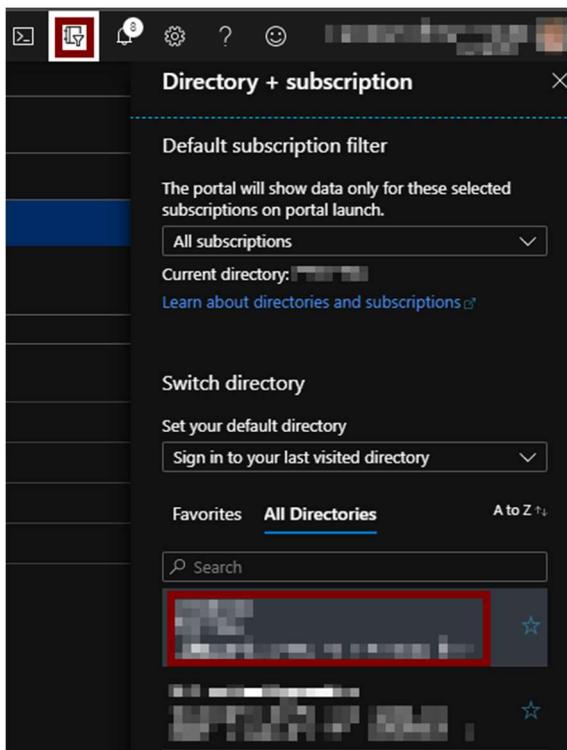


Azure AD Authentication

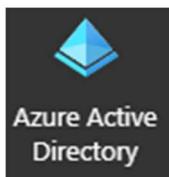
## Customer

### App Registration

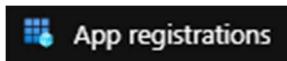
An app registration is needed to allow users to use the companies Azure Active Directory to sign into CERRIX. To do this login at <https://portal.azure.com/> and make sure the correct “Directory” is selected:



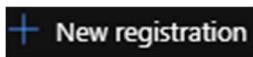
Select “Azure Active Directory” at the home screen:



Select “App registration” in the side menu:



Select “New registration” in the top menu:



Insert the following configuration:

Name	A name for the “App registration” <i>CERRIX [Production, Acceptance, Testing, Development]</i>
Redirect URI	An allowed redirect URL for after a successful login <i>Web</i> <i>https://[URL of the CERRIX website]/bundles/assets/oidc-login-redirect.html</i>

\* Name  
The user-facing display name for this application (this can be changed later).  
CERRIX Production ✓

Supported account types  
Who can use this application or access this API?  
 Accounts in this organizational directory only (■■■■■ 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)  
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://cerrix.website/bundles/assets/oidc-login-redirect.html ✓

Select “Register” bellow:



You will be redirected to the “App registration”. Select “Authentication”:



Select the following configuration for implicit grant flow:

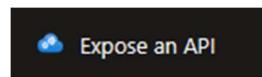
Access tokens	Used to access the CERRIX Web API
ID tokens	Used to prove successful authentication These tokens are returned after successful login

**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)

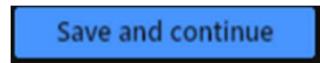
Select “Expose an API” in the left side menu:



Select “Add a scope”:



Keep the “Application ID URI” as is “api://{Client ID GUID}” in the right side menu and select “Save and continue”:



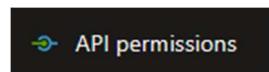
Insert the following configuration:

Scope name	Use “access_as_user” for the scope name
Who can consent?	Admins and users Allow users to consent to using their identity to sign in to CERRIX
Admin/User consent display name	Consent display name like “Access CERRIX as a user”
Admin/User consent description	Consent description like “Access the CERRIX Web API as a user”
State	Enable scope

The screenshot shows a configuration form for a scope named "access\_as\_user". The fields are as follows:

- Scope name \***: access\_as\_user
- Who can consent?**: Admins and users
- Admin consent display name \***: Access CERRIX as a user
- Admin consent description \***: Access the CERRIX Web API as a user
- User consent display name**: Access CERRIX as a user
- User consent description**: Access the CERRIX Web API as a user
- State**: Enabled

Select “API Permissions” in the left side menu:

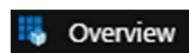


Select “Add a permission” and add the following delegated permission: “Microsoft Graph” -> “User.Read”. (Note: This permission might already exist. If so you can skip this step.)

Once the permission has been added select “Grand admin consent for {Tenant name}” and then select “Yes”

+ Add a permission		Grant admin consent for CERRIX B.V.	
API / Permissions name	Type	Description	Admin consent requ...
▼ Microsoft Graph (1)			
User.Read	Delegated	Sign in and read user profile	No  Granted for CERRIX B.V.

Select “Overview” in the left side menu:



And give the following information to CERRIX so that they can configure the application for Azure AD authentication:

Client/Application ID	Used to specify the app registration
Tenant/Directory URL	Used to redirect the user to the company's Azure AD for authentication
Claim Type	Is your single sign-on username the same as your email address? If no, what claim type can we use to uniquely identify your users?

Application (client) ID : 86e30aa4-5b1d-4f53-a3dc-effa5caf1edd  
Directory (tenant) ID : [REDACTED]