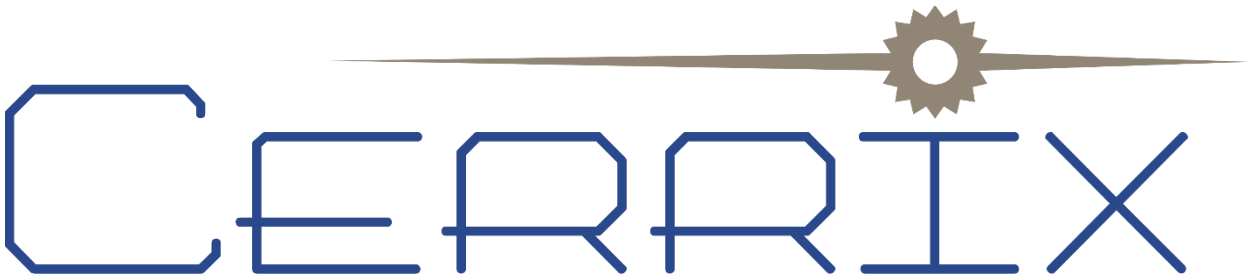
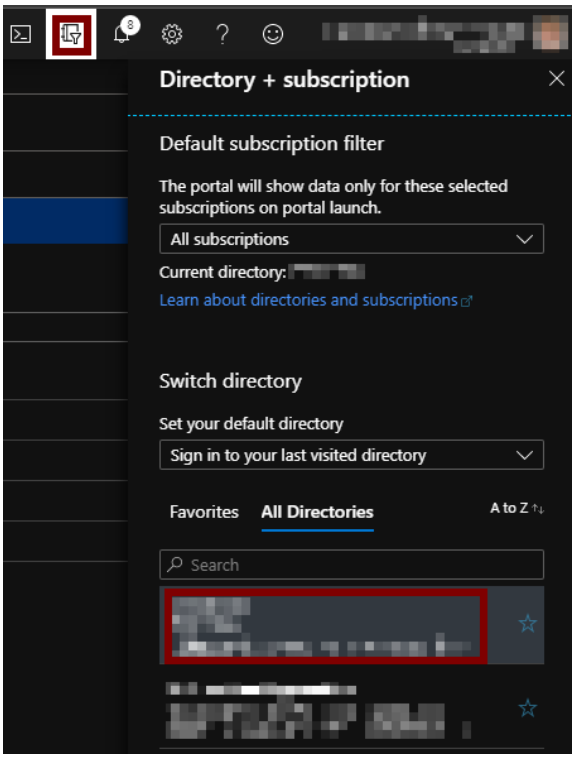


Azure AD Authentication

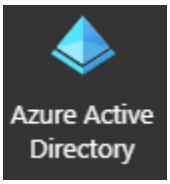
Customer

App Registration

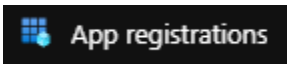
An app registration is needed to allow users to use the companies Azure Active Directory to sign into CERRIX. To do this login at https://portal.azure.com/ and make sure the correct “Directory” is selected:



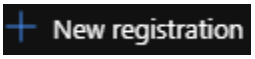
Select “Azure Active Directory” at the home screen:



Select “App registration” in the side menu:

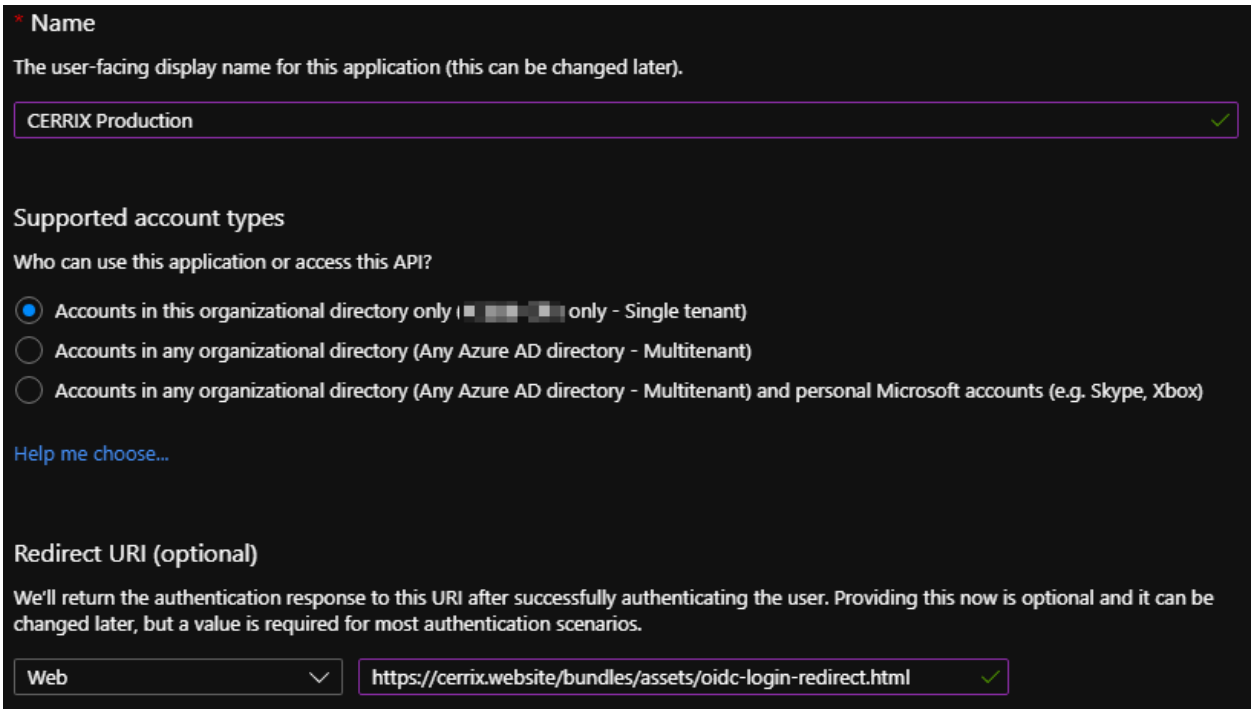


Select “New registration” in the top menu:



Insert the following configuration:

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



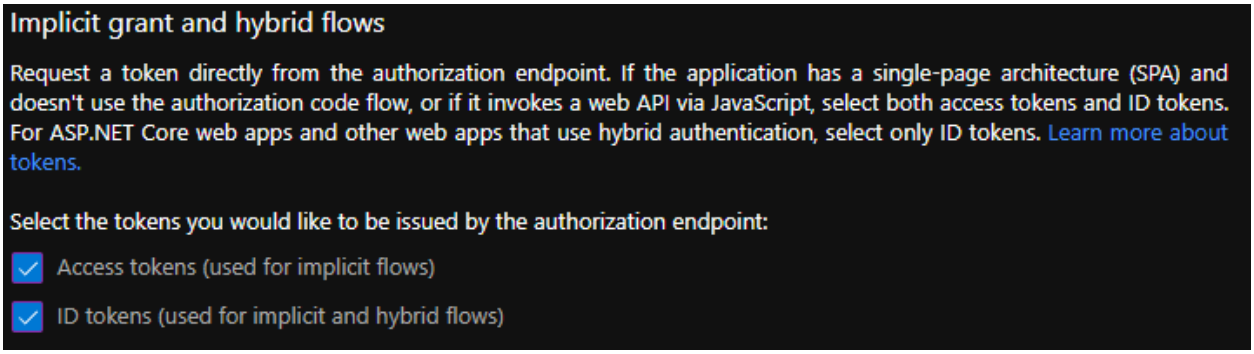
Select “Register” bellow:

You will be redirected to the “App registration”.

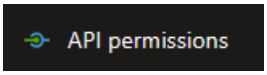
Select “Authentication”:

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

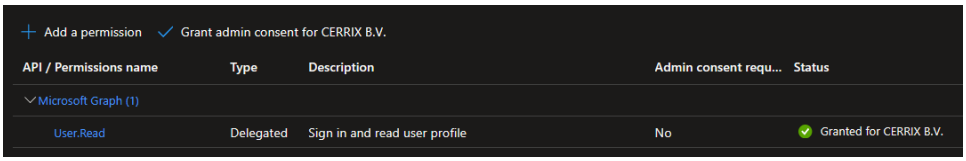


Select “API Permissions” in the left side menu:

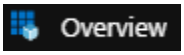


Select “Add a permission” and add the following delegated permission: “Microsoft Graph” -> “User.Read”. (Note: This permission might already exist. If so you can skip this step.)

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



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?