Configure Active Directory Authentication

If your company already uses an Active Directory instance for authenticating users, you can configure the Workbench to use this authentication method for your users as well. Note that the user roles and permissions are still administered in the Workbench. So new users have to be created in the Workbench as well.

Active Directory Settings

> ⊘ **Warning**
>
> Please be careful changing any settings for the Active Directory configuration. They will be saved automatically and are immediately active. Your users will not be able to login if the parameters are not correct. It is generally a good idea to test the new settings by opening a separate browser and try to login with another user. So your own session stays open and you are able to make changes if necessary.

- **Enable AD authentication:**
  Switches the Active Directory authentication on/off for the entire account.

- **AD Authentication URL:**
  URL to your Active Directory authentication portal. Please consult your IT department for support.

- **Workbench Callback URL:**
  Callback or redirect URL that will be used by the Active Directory server after successful authentication. This value cannot be changed. Make sure that this URL is **registered as redirect URL** in your Active Directory.

- **Scopes:**
  Comma-separated list of permission sets to use during authentication. E.g. "profile".

- **Tenant ID:**
  Tenant ID of your Active Directory instance. Please consult your IT department for support.

- **Client ID:**
  Client ID of the Workbench application defined in your Active Directory. Please consult your IT department for support.

- **Client Secret:**
  Secret key created in your Active Directory for the Workbench client application. Please consult your IT department for support.

☐ Enable login via Active Directory

AD Authentication URL

Workbench Callback URL
https://workbench.excentos.com/demo/auth/redirect

Scopes

Tenant ID

Client ID

Client Secret