

Management Portal Authentication

Last Modified on 02/11/2021 12:02 pm EET

Azure Active Directory authentication should be enabled to Carillon Management portal. Authentication requires a Azure AD App Registration that should be created to Azure AD tenant where users of the Carillon Management portal exists. You can invite external users also but Azure AD App registration should be created to your primary Azure AD tenant.

Instructions how to enable Azure AD authentication can be found from here: [Configure Azure AD authentication - Azure App Service](#)

Self hosted Azure App Service

If you are self-hosting Azure App Service then you can follow option 1 (Create a new app registration automatically) to add Azure AD authentication to Carillon Management portal

Centero hosted Azure App service

If you are using Centero hosted Azure App Service then follow option 2 (Use an existing registration created separately) to create Azure AD App registration. If you have not received value from Centero support (this is required to create Azure AD App registration) then contact tahtipuikko@centero.fi support. After creating Azure AD App registration deliver following information to tahtipuikko@centero.fi support:

- Client ID
- Tenant ID
- Client secret
- Application ID URI

Client secret can be valid only for specific time so you need to remember to create new client secret before old expires and then deliver new client secret information to tahtipuikko@centero.fi support.