

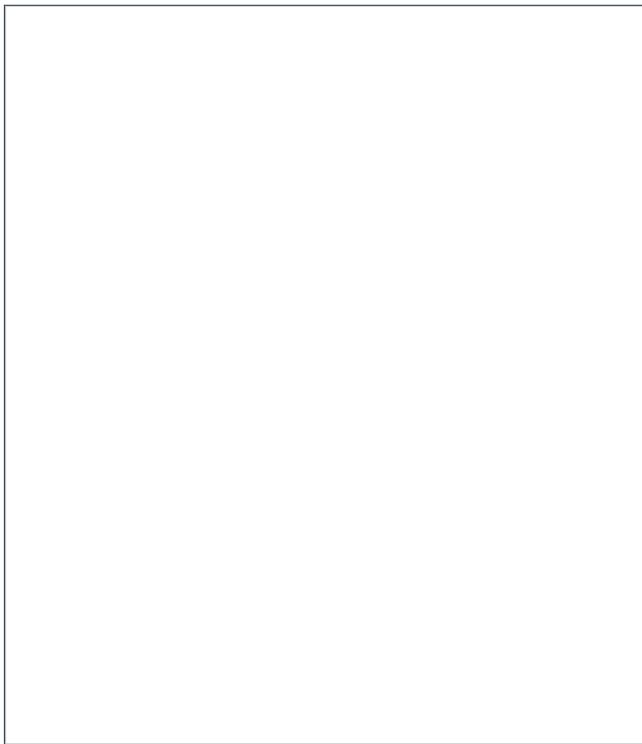


ADAL is an end of life technology which will be out of support on June 30, 2022. Therefore, Centero Portal authentication relies now on Microsoft Authentication Library (MSAL). As the result, registering and authenticating are easier from now on. But the change also have some user impacts in specific scenarios.

### Scenario 1 - Authentication to Centero Portal now requires a consent.

#### Requester point of view

Some organizations have [admin consent workflow](#) enabled which means that the consent request must be forwarded to an administrator. If this is the case, login to our Portal and try to sign in. A request for approval should appear. Input a justification and request for the approval. Also notifying your administrator can speed up the process.



Picture 1. Request without admin consent workflow



Picture 2. Request with admin consent workflow

### Admin point of view

See for the following Microsoft's documentation on [admin consent](#).

After consent, make sure **Assignment required** setting in the enterprise application properties is set to **No**. If assignment required is set to Yes, you need to grant access to Centero Portal users from "Users and groups" tab

The screenshot displays the 'Centero Portal | Properties' page in the Microsoft Azure portal. The breadcrumb trail at the top reads 'Home > Centero Oy > Enterprise applications > Centero Portal'. The page title is 'Centero Portal | Properties' with a three-dot menu icon. Below the title, there are action buttons: 'Save', 'Discard', 'Delete', and 'Got feedback?'. A left-hand navigation pane lists various management options under 'Manage' (Overview, Deployment Plan, Properties, Owners, Roles and administrators (Preview), Users and groups, Single sign-on, Provisioning, Application proxy, Self-service) and 'Security' (Conditional Access, Permissions, Token encryption). Under 'Activity', there are 'Sign-in logs', 'Usage & insights', 'Audit logs', and 'Provisioning logs'. The main content area shows the following settings:

- Enabled for users to sign-in?: Yes (selected), No
- Name: Centero Portal (with a checkmark)
- Homepage URL: https://preview.portal.centero.fi/ (with a copy icon)
- Logo: Centero Portal logo (with a refresh icon)
- Application ID: 16345f31-9803-4809-9f8a-4e5b3e328b76 (with a copy icon)
- Object ID: 3232c91c-d8d7-4b7d-a76e-8085d712cc60 (with a copy icon)
- Assignment required?: Yes, No (selected) (highlighted in yellow)
- Visible to users?: Yes (selected), No
- Notes: (with a checkmark)



# software MANAGER

Scenario: Some Azure AD Directories is different than used in Centro Portal

Some customers enabled a feature to login to Azure AD with the email as an alternate login. At the time of review more using this request can cause a problem when signing in to the Centro Portal. The problem occurs when a user has registered to the Portal with a specific email address and then using different e-mail (usually alternate email) when trying to login.

Make sure that you use the same username while authenticating that you originally registered with. If you know that there is a problem with this feature contact our support.



Picture 3. Email and alternate email of an user object in Azure AD