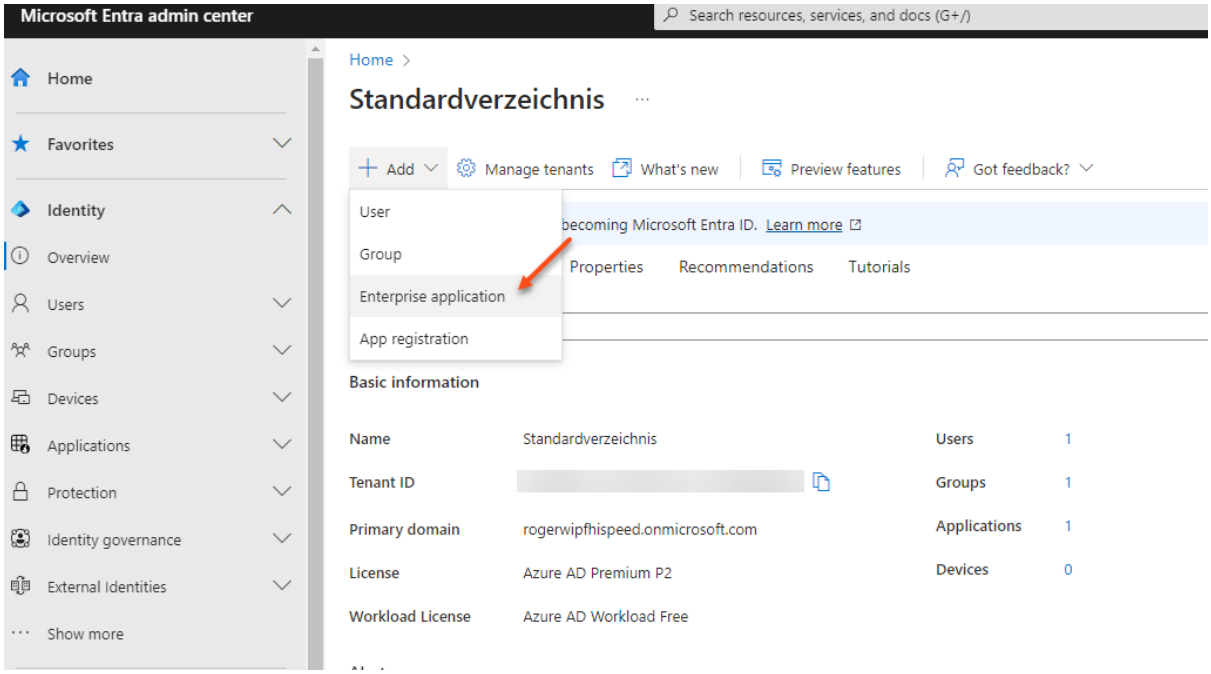
Azure AD (Entra ID) Setup for FNZ Studio

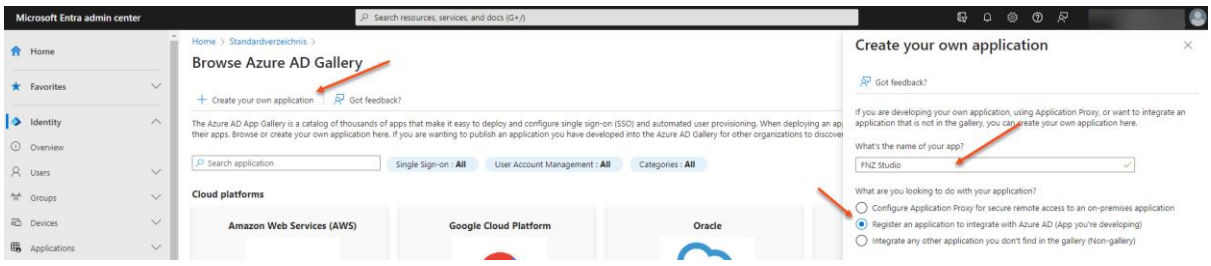
PART 1 – Important for Connectivity Testing

- Access Entra ID Admin Center
- Add Enterprise Application



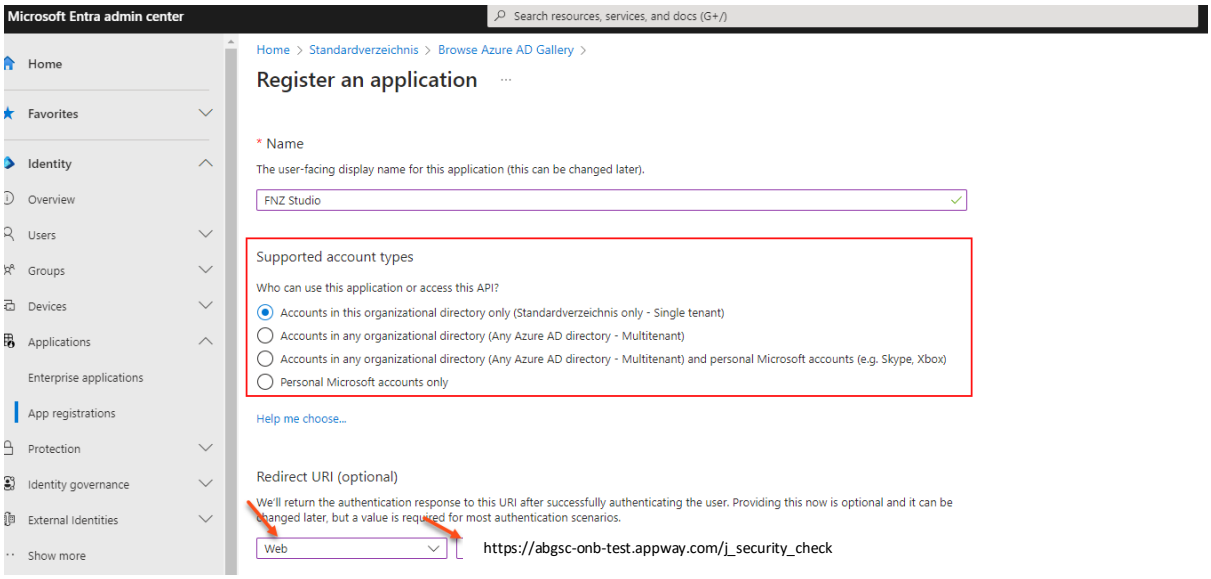
Create own application.

- Give the application a name depending on your requirements.
- Register an application to integrate with Azure AD

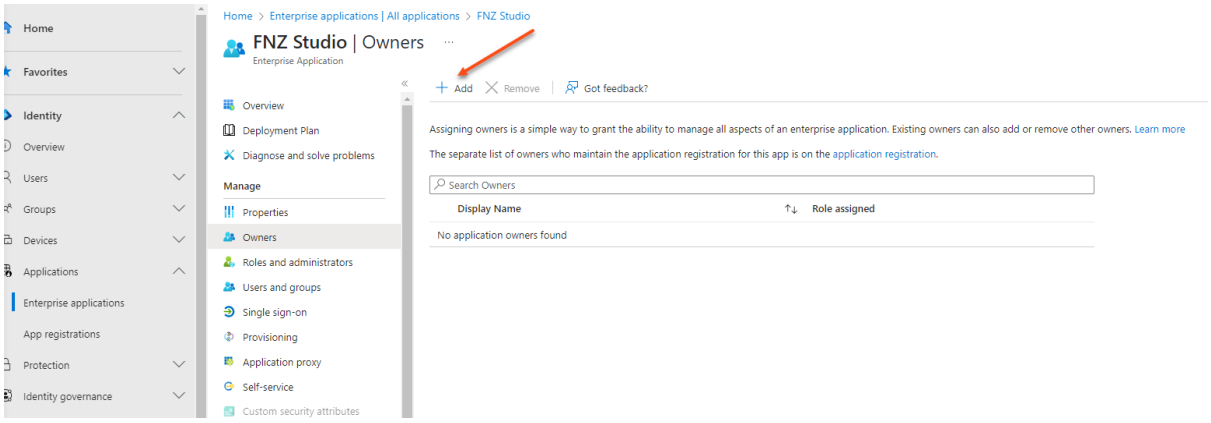


Register the application.

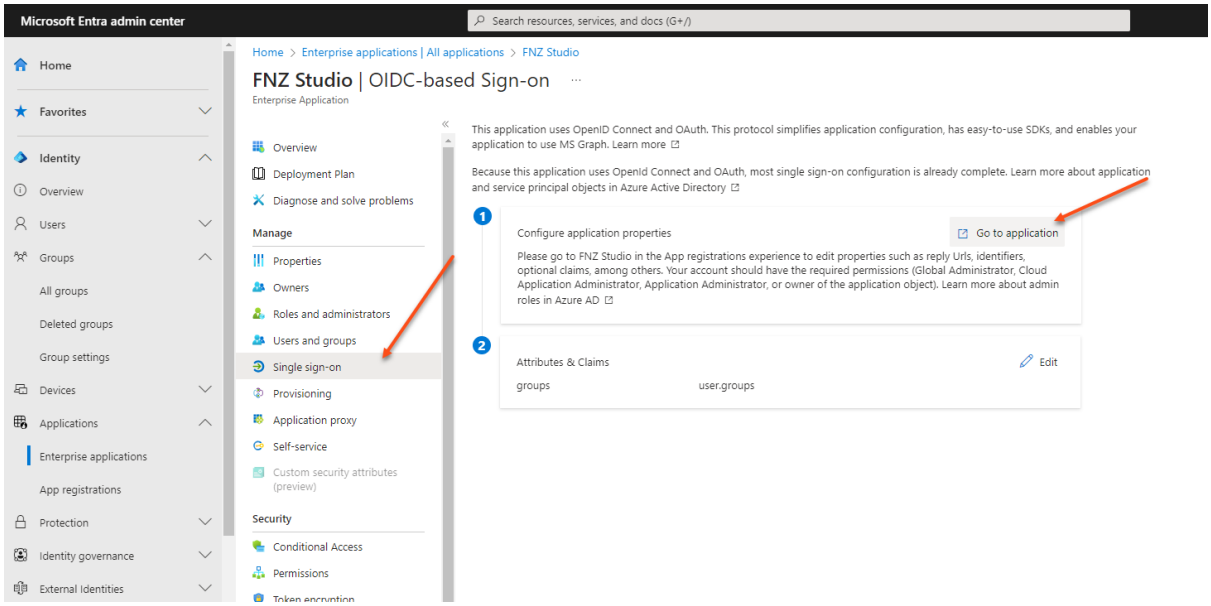
- Select the “Supported account types” based on your requirements and the current setup
- Redirect URL “https://abgsc-onb-test.appway.com/j_security_check”



Add an owner to the application

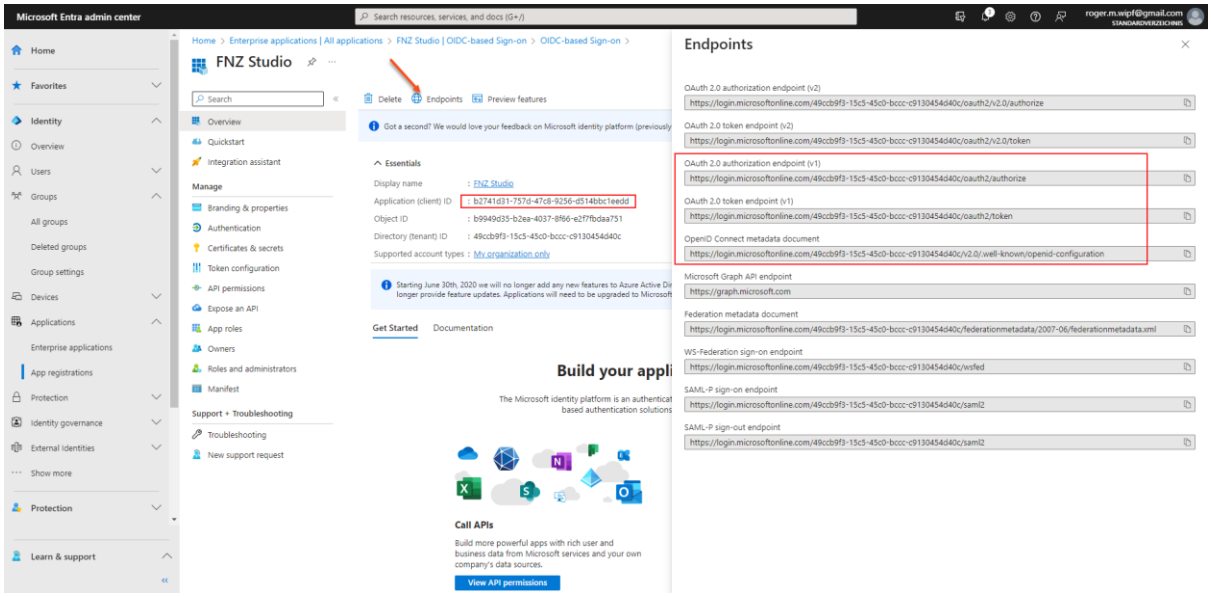


Got to “Single Sign-on”



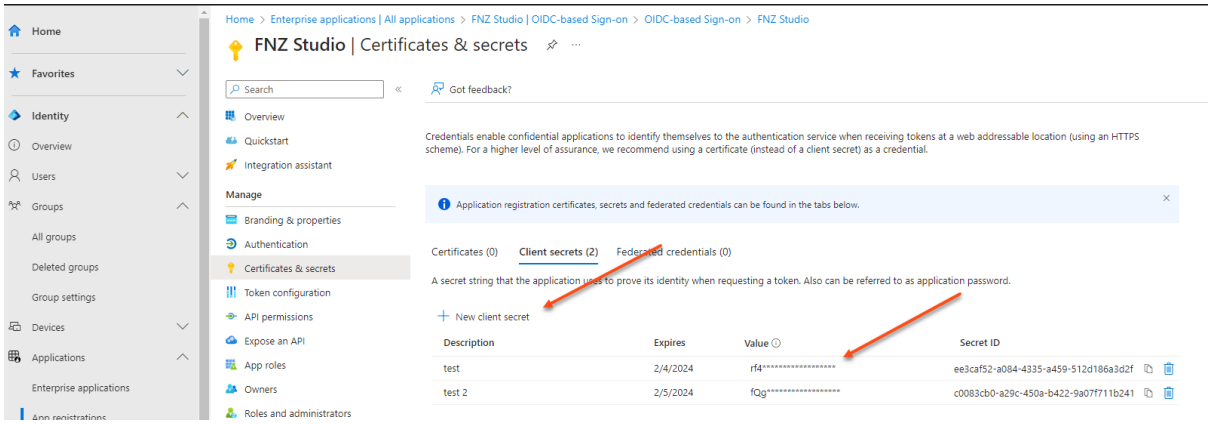
Open “Endpoints” and share the following information

- Application (client) ID
- And the endpoints marked

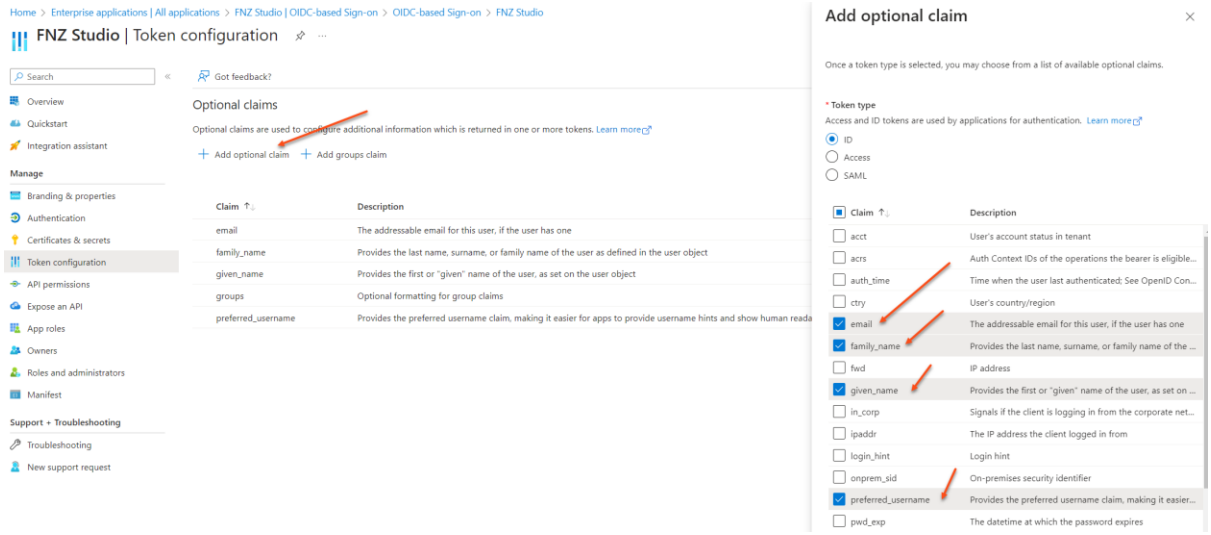


Go to “Client Credentials”

Add new client secret and share the secret value with us (let us know how to securely exchange this)

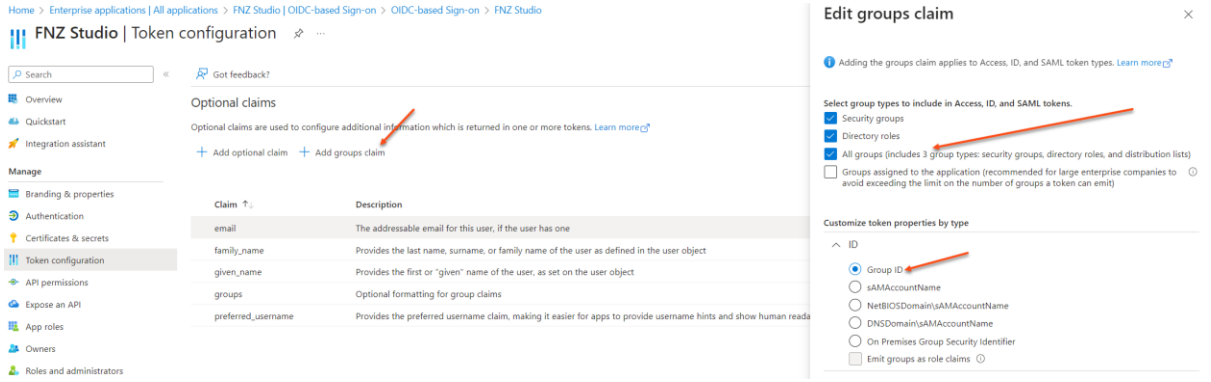


Add optional claims for the ID Token



Add “groups” claim

- All groups
- -> ID -> Group ID

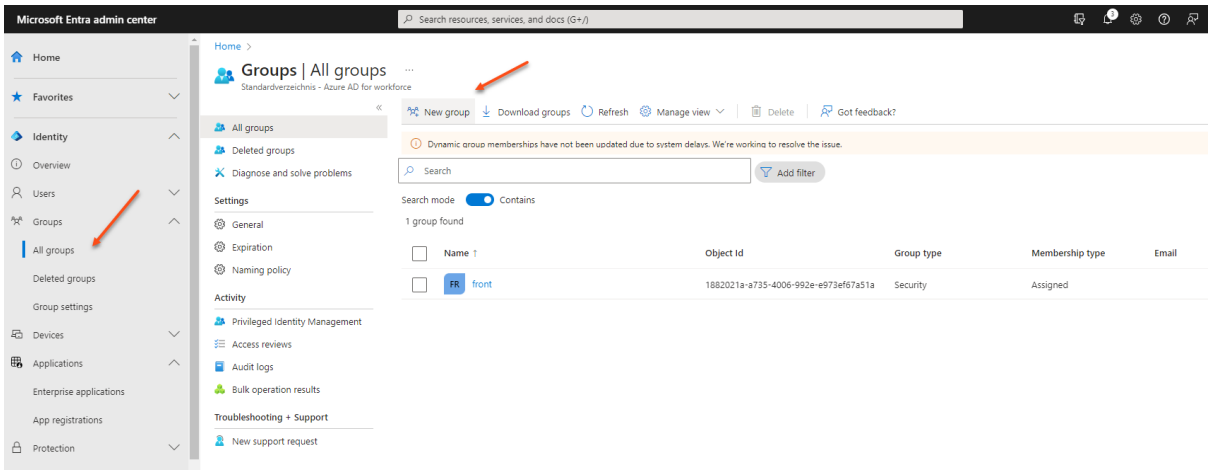


PART 2 – Groups and Roles Setup

This needs ABG input to properly assign the users to the correct roles

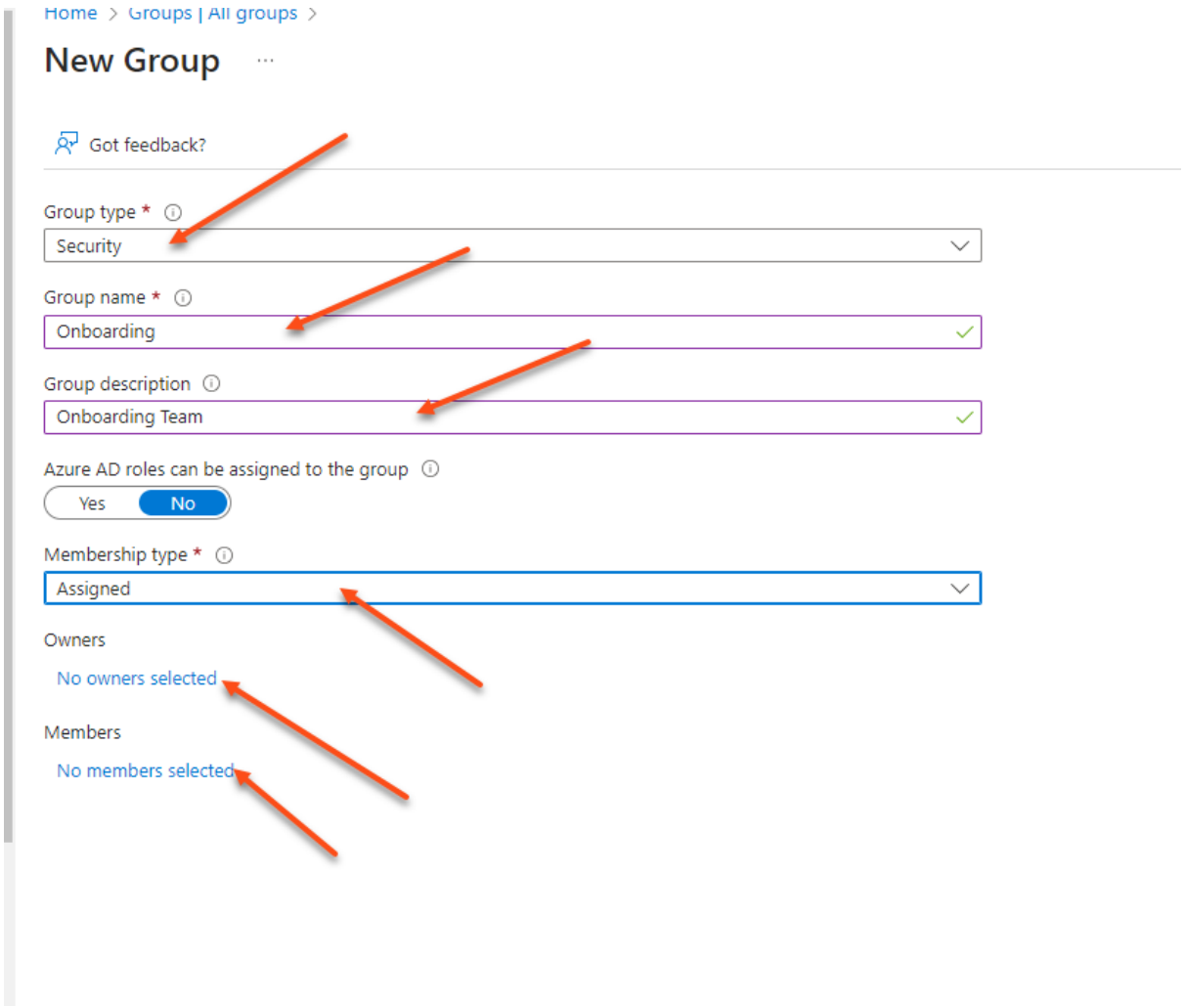
Go to Groups -> All groups

- “New group” (to be done for each required group)

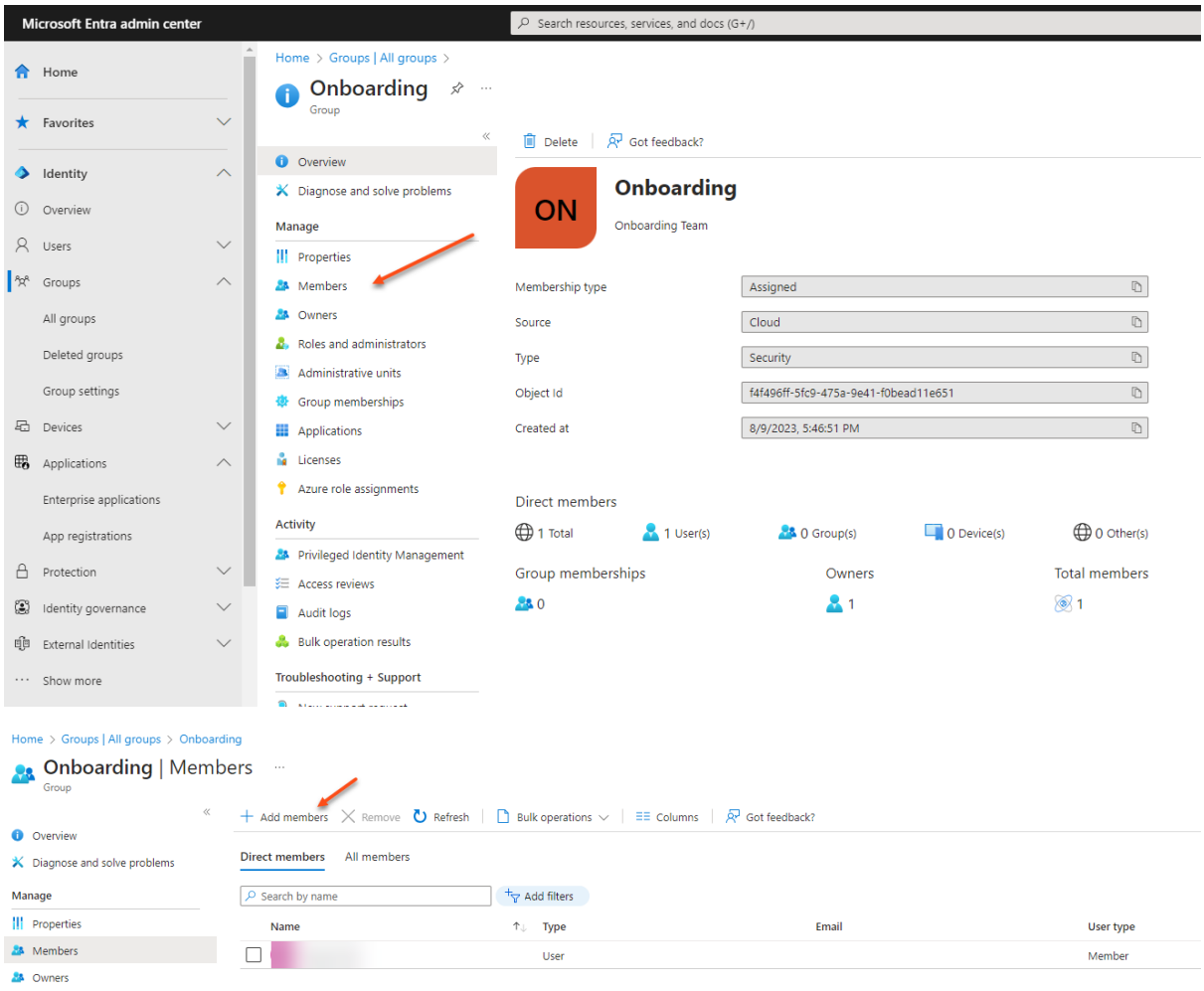


Setup the groups (repeat for each)

- Group type “Security”
- Group name
  - Front
  - OnboardingTeam
  - Compliance
  - ExecutiveCommittee
  - AMLHead

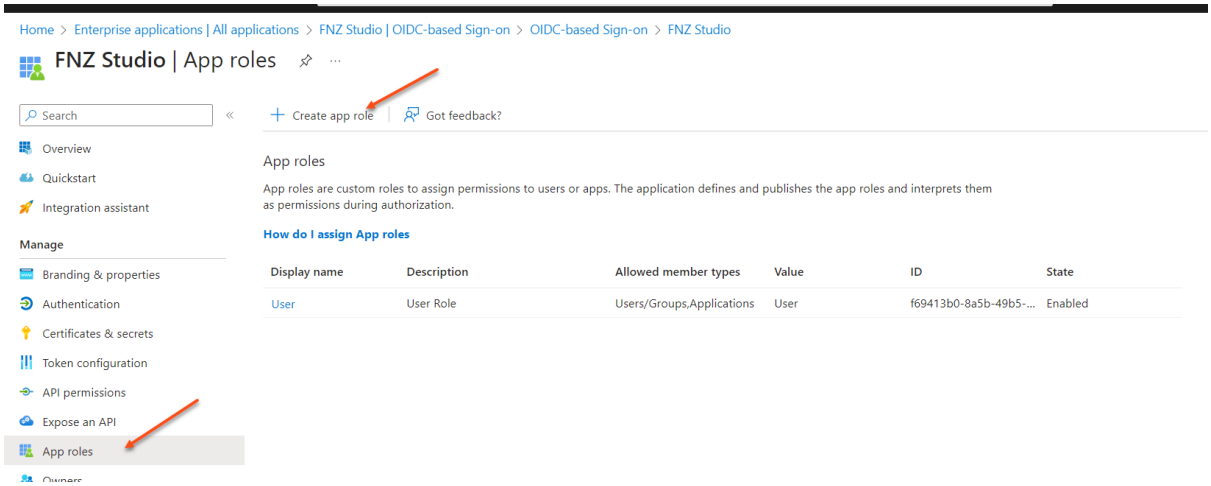


Add Members to the groups [per ABG requirement]



Add “App Roles”

- Create app role



Define the role “User”. This is required as minimum to get access to FNZ Studio processes