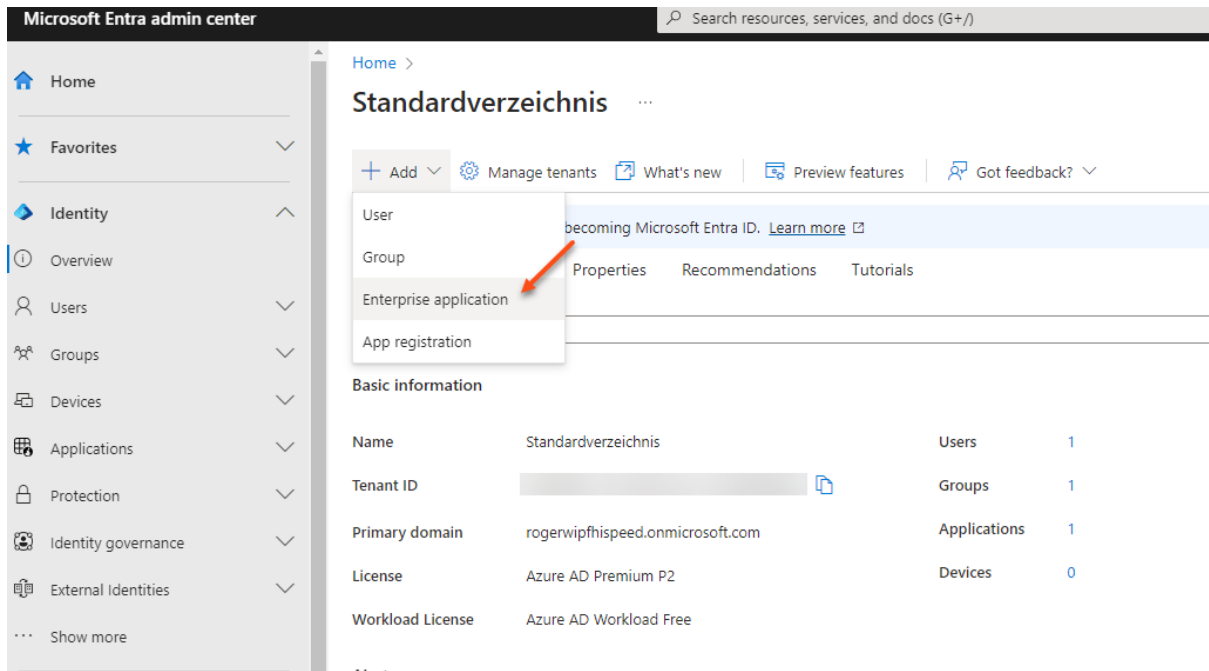


Azure AD (Entra ID) Setup for FNZ Studio

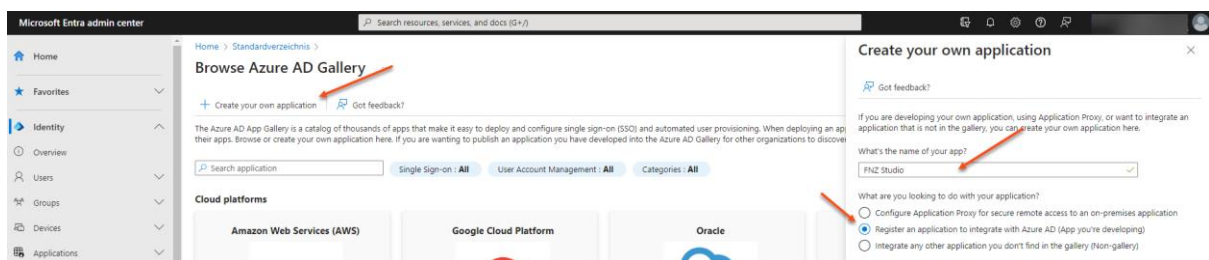
PART 1 – Important for Connectivity Testing

- 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”

Microsoft Entra admin center

Home > Standardverzeichnis > Browse Azure AD Gallery >

Register an application

* Name
The user-facing display name for this application (this can be changed later).
FNZ Studio

Supported account types
Who can use this application or access this API?

- Accounts in this organizational directory only (Standardverzeichnis only - Single tenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- Personal Microsoft accounts only

Help me choose...

Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.
Web https://abgsc-onb-test.appway.com/j_security_check

Add an owner to the application

Home > Enterprise applications | All applications > FNZ Studio

FNZ Studio | Owners

Enterprise Application

+ Add Remove Got feedback?

Overview
Deployment Plan
Diagnose and solve problems

Manage
Properties
Owners
Roles and administrators
Users and groups
Single sign-on
Provisioning
Application proxy
Self-service
Custom security attributes

Assigning owners is a simple way to grant the ability to manage all aspects of an enterprise application. Existing owners can also add or remove other owners. [Learn more](#)

The separate list of owners who maintain the application registration for this app is on the [application registration](#).

Search Owners

Display Name	Role assigned
No application owners found	

Got to "Single Sign-on"

Microsoft Entra admin center

Home > Enterprise applications | All applications > FNZ Studio

FNZ Studio | OIDC-based Sign-on

Enterprise Application

This application uses OpenID Connect and OAuth. This protocol simplifies application configuration, has easy-to-use SDKs, and enables your application to use MS Graph. Learn more

Because this application uses OpenID Connect and OAuth, most single sign-on configuration is already complete. Learn more about application and service principal objects in Azure Active Directory

- 1 Configure application properties [Go to application](#)
Please go to FNZ Studio in the App registrations experience to edit properties such as reply URIs, identifiers, optional claims, among others. Your account should have the required permissions (Global Administrator, Cloud Application Administrator, Application Administrator, or owner of the application object). Learn more about admin roles in Azure AD
- 2 Attributes & Claims
groups user.groups [Edit](#)

Open "Endpoints" and share the following information

- Application (client) ID
- And the endpoints marked

Microsoft Entra admin center

Home > Enterprise applications | All applications > FNZ Studio | OIDC-based Sign-on > Endpoints

Endpoints

OAuth 2.0 authorization endpoint (v2)
<https://login.microsoftonline.com/49ccb9f3-15c5-43c0-bccc-c9130454640c/oauth2/v2.0/authorize>

OAuth 2.0 token endpoint (v2)
<https://login.microsoftonline.com/49ccb9f3-15c5-43c0-bccc-c9130454640c/oauth2/v2.0/token>

OAuth 2.0 authorization endpoint (v1)
<https://login.microsoftonline.com/49ccb9f3-15c5-43c0-bccc-c9130454640c/oauth2/authorize>

OAuth 2.0 token endpoint (v1)
<https://login.microsoftonline.com/49ccb9f3-15c5-43c0-bccc-c9130454640c/oauth2/token>

OpenID Connect metadata document
<https://login.microsoftonline.com/49ccb9f3-15c5-43c0-bccc-c9130454640c/v2.0/.well-known/openid-configuration>

Microsoft Graph API endpoint
<https://graph.microsoft.com>

Federation metadata document
<https://login.microsoftonline.com/49ccb9f3-15c5-43c0-bccc-c9130454640c/federationmetadata/2007-06/federationmetadata.xml>

WS-Federation sign-on endpoint
<https://login.microsoftonline.com/49ccb9f3-15c5-43c0-bccc-c9130454640c/wsfed>

SAML-P sign-on endpoint
<https://login.microsoftonline.com/49ccb9f3-15c5-43c0-bccc-c9130454640c/saml2>

SAML-P sign-out endpoint
<https://login.microsoftonline.com/49ccb9f3-15c5-43c0-bccc-c9130454640c/saml2>

Essentials

Display name : FNZ Studio

Application (client) ID : **b2741d31-757d-47c8-9256-d514bbc1eedd**

Object ID : b9949d35-b2ea-4037-8f66-e2f7bd9a751

Directory (tenant) ID : 49ccb9f3-15c5-43c0-bccc-c9130454640c

Supported account types : [My organization only](#)

Go to "Client Credentials"

Microsoft Entra admin center

Home > Enterprise applications | All applications > FNZ Studio | OIDC-based Sign-on > Client Credentials

Client Credentials

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer).

Essentials

Display name : FNZ Studio

Application (client) ID : b2741d31-757d-47c8-9256-d514bbc1eedd

Object ID : b9949d35-b2ea-4037-8f66-e2f7bd9a751

Directory (tenant) ID : 49ccb9f3-15c5-43c0-bccc-c9130454640c

Supported account types : [My organization only](#)

Client credentials : **0 certificate_2 secret**

Redirect URIs : [1 web_0 spa_0 url](#) 0 certificate_2 secret

Application ID URI : [api://b2741d31-757d-47c8-9256-d514bbc1eedd](#)

Managed application in L... : FNZ Studio

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

The screenshot shows the 'Certificates & secrets' page for the 'FNZ Studio' application. The left sidebar contains navigation options like Home, Favorites, Identity, Overview, Users, Groups, etc. The main content area shows a table of client secrets. A red arrow points to the 'New client secret' button, and another red arrow points to the 'Value' column of the 'test' secret.

Description	Expires	Value	Secret ID
test	2/4/2024	r14*****	ee3caf52-a084-4335-a459-512d106a3d2f
test 2	2/5/2024	fQg*****	c0083cb0-a29c-450a-b422-9a07f7711b241

Add optional claims for the ID Token

The screenshot shows the 'Token configuration' page for the 'FNZ Studio' application. The 'Optional claims' section is visible, and the 'Add optional claim' dialog is open. The dialog shows a list of available claims, with 'email', 'family_name', 'given_name', and 'preferred_username' selected. The 'Token type' is set to 'ID'.

Claim	Description
email	The addressable email for this user, if the user has one
family_name	Provides the last name, surname, or family name of the user as defined in the user object
given_name	Provides the first or "given" name of the user, as set on the user object
groups	Optional formatting for group claims
preferred_username	Provides the preferred username claim, making it easier for apps to provide username hints and show human readable names

Add "groups" claim

- All groups
- -> ID -> Group ID

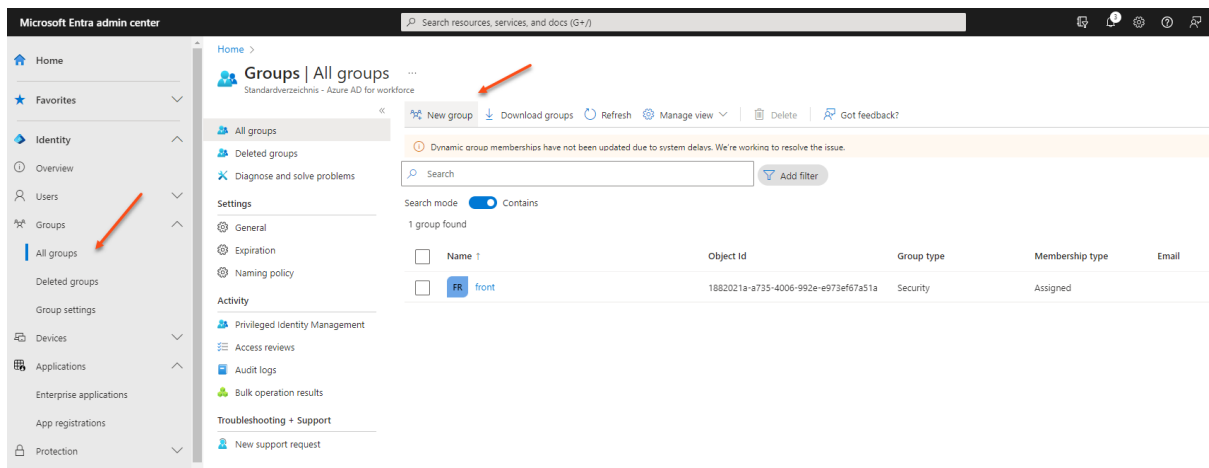
The screenshot shows the 'Token configuration' page for the 'FNZ Studio' application. The 'Optional claims' section is visible, and the 'Edit groups claim' dialog is open. The dialog shows a list of group types to include in Access, ID, and SAML tokens. 'Security groups', 'Directory roles', and 'All groups' are selected. The 'Customize token properties by type' section is also visible, with 'Group ID' selected for the ID token type.

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
 - o Front
 - o OnboardingTeam
 - o Compliance
 - o ExecutiveCommittee
 - o AMLHead

New Group ...

 Got feedback?

Group type * ⓘ

Security 

Group name * ⓘ

Onboarding 

Group description ⓘ

Onboarding Team 

Azure AD roles can be assigned to the group ⓘ

Yes No

Membership type * ⓘ

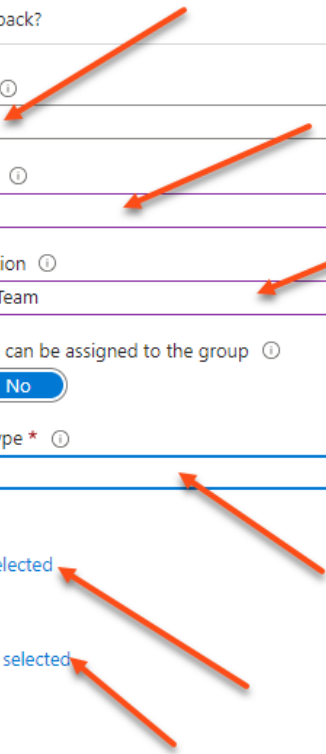
Assigned 

Owners

No owners selected

Members

No members selected



Add Members to the groups [per ABG requirement]

Microsoft Entra admin center

Home > Groups | All groups > Onboarding

Onboarding Group

Overview

Diagnose and solve problems

Manage

- Properties
- Members
- Owners
- Roles and administrators
- Administrative units
- Group memberships
- Applications
- Licenses
- Azure role assignments

Activity

- Privileged Identity Management
- Access reviews
- Audit logs
- Bulk operation results

Troubleshooting + Support

Membership type: Assigned

Source: Cloud

Type: Security

Object id: f4f496ff-5fc9-475a-9e41-f0bead11e651

Created at: 8/9/2023, 5:46:51 PM

Direct members: 1 Total, 1 User(s), 0 Group(s), 0 Device(s), 0 Other(s)

Group memberships: 0

Owners: 1

Total members: 1

Home > Groups | All groups > Onboarding

Onboarding | Members Group

Overview

Diagnose and solve problems

Manage

- Properties
- Members
- Owners

Direct members | All members

Search by name

Add filters

Name	Type	Email	User type
	User		Member

Add "App Roles"

- Create app role

Home > Enterprise applications | All applications > FNZ Studio | OIDC-based Sign-on > OIDC-based Sign-on > FNZ Studio

FNZ Studio | App roles

Search

Create app role

Got feedback?

Overview

Quickstart

Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners

App roles

App roles are custom roles to assign permissions to users or apps. The application defines and publishes the app roles and interprets them as permissions during authorization.

How do I assign App roles

Display name	Description	Allowed member types	Value	ID	State
User	User Role	Users/Groups,Applications	User	f69413b0-8a5b-49b5-...	Enabled

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

Create app role



Display name * ⓘ

User ✓

Allowed member types * ⓘ

- Users/Groups
- Applications
- Both (Users/Groups + Applications)

Value * ⓘ

User ✓

Description * ⓘ

User Role required for general access for FNZ studio processes

Do you want to enable this app role? ⓘ

