

Multifactor Authentication and User Access Guide

Version: 1.2

Configure Multifactor Authentication

Eiendomsverdi requires users to be authenticated with Multifactor Authentication. For Federation to work, the following prerequisites must be in place:

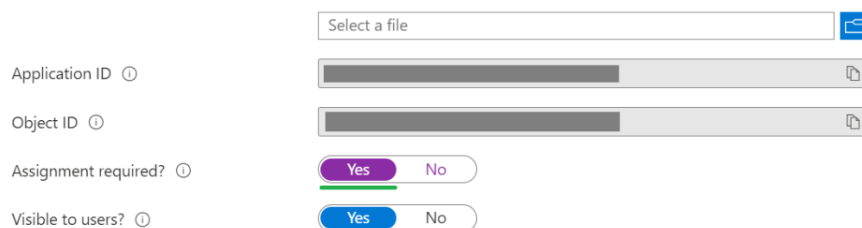
1. All users must have Multifactor Authentication enabled in Azure Entra ID
2. A Conditional Access Policy must be created for the Eiendomsverdi App Registration to enforce Multifactor Authentication

For setting up a Conditional Access Policy for the App Registration, see the following guide:

<https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-enable-azure-mfa>

Configure User Access

To restrict user access to Eiendomsverdi the “Assignment required” property should be set to “Yes” under “Properties” of the Enterprise Application for Eiendomsverdi in Azure Entra ID:



	<input type="text" value="Select a file"/>	
Application ID ⓘ	<input type="text"/>	
Object ID ⓘ	<input type="text"/>	
Assignment required? ⓘ	<input checked="" type="radio"/> Yes	<input type="radio"/> No
Visible to users? ⓘ	<input checked="" type="radio"/> Yes	<input type="radio"/> No

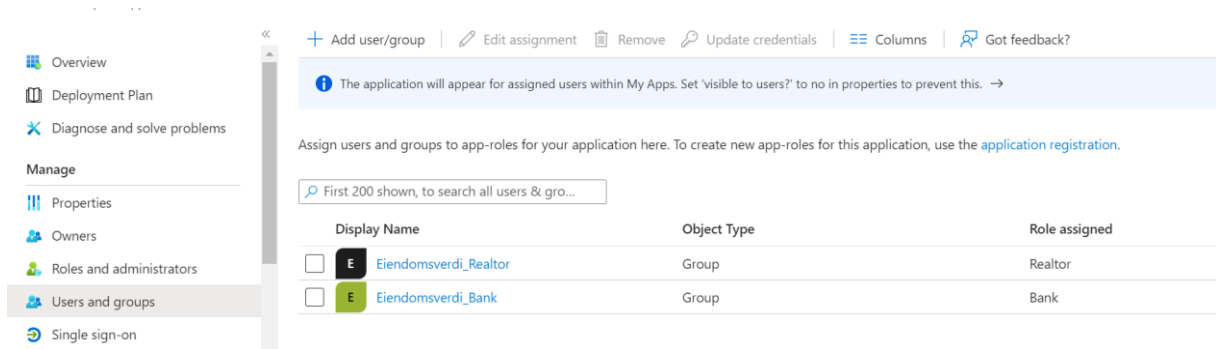
Users and groups can then be assigned under the “Users and groups” tab of the Enterprise Application.

Role Based Access Control

If needed, we can further divide user access based on different groups of users like Bank and Realtor, using Role Based Access Control. See the following guide for details:

<https://learn.microsoft.com/en-us/entra/external-id/customers/how-to-use-app-roles-customers>

The recommended approach is to create App Roles on the App Registration, and then assign the roles to groups on the Enterprise App Registration:



Then, pass this information to Eiendomsverdi so that we can configure the assigned roles appropriately.

Important! Note, that a user should only be assigned one role. If more than one role is assigned, the the first entry in the roles list will get picked.