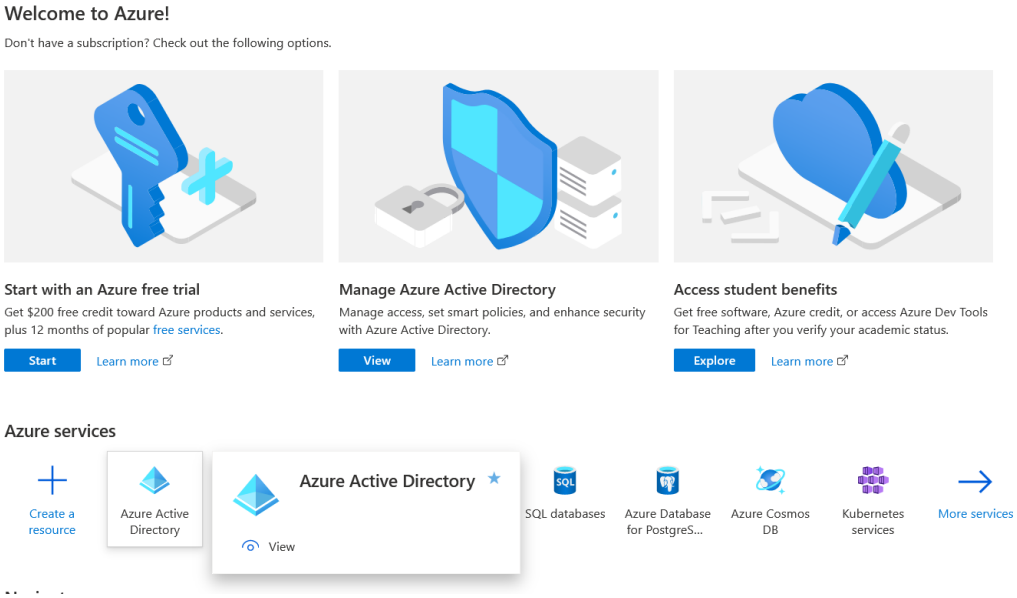
techstep

Integration with Azure ActiveDirectory

Date: 25/04/2023

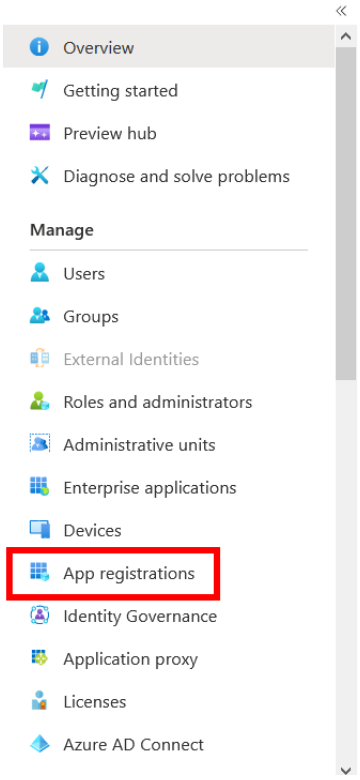
Getting started

The first step to integrate Essentials MDM manage with Azure Active Directory is to register the application in our Azure account. To do this, log in to the portal https://portal.azure.com/ and then from the Azure services we choose Azure Active Directory.

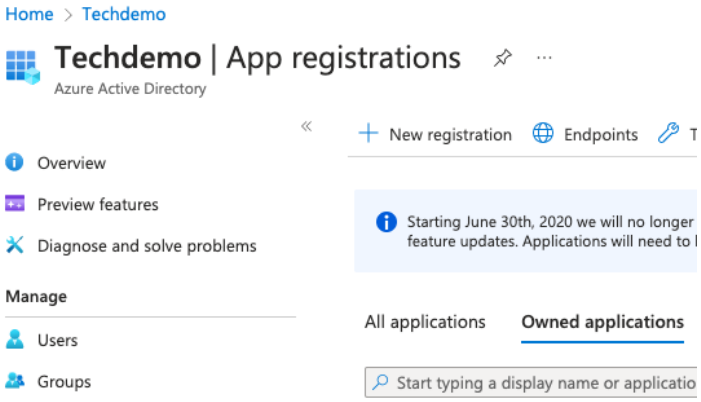


Registering Essentials MDM in Azure

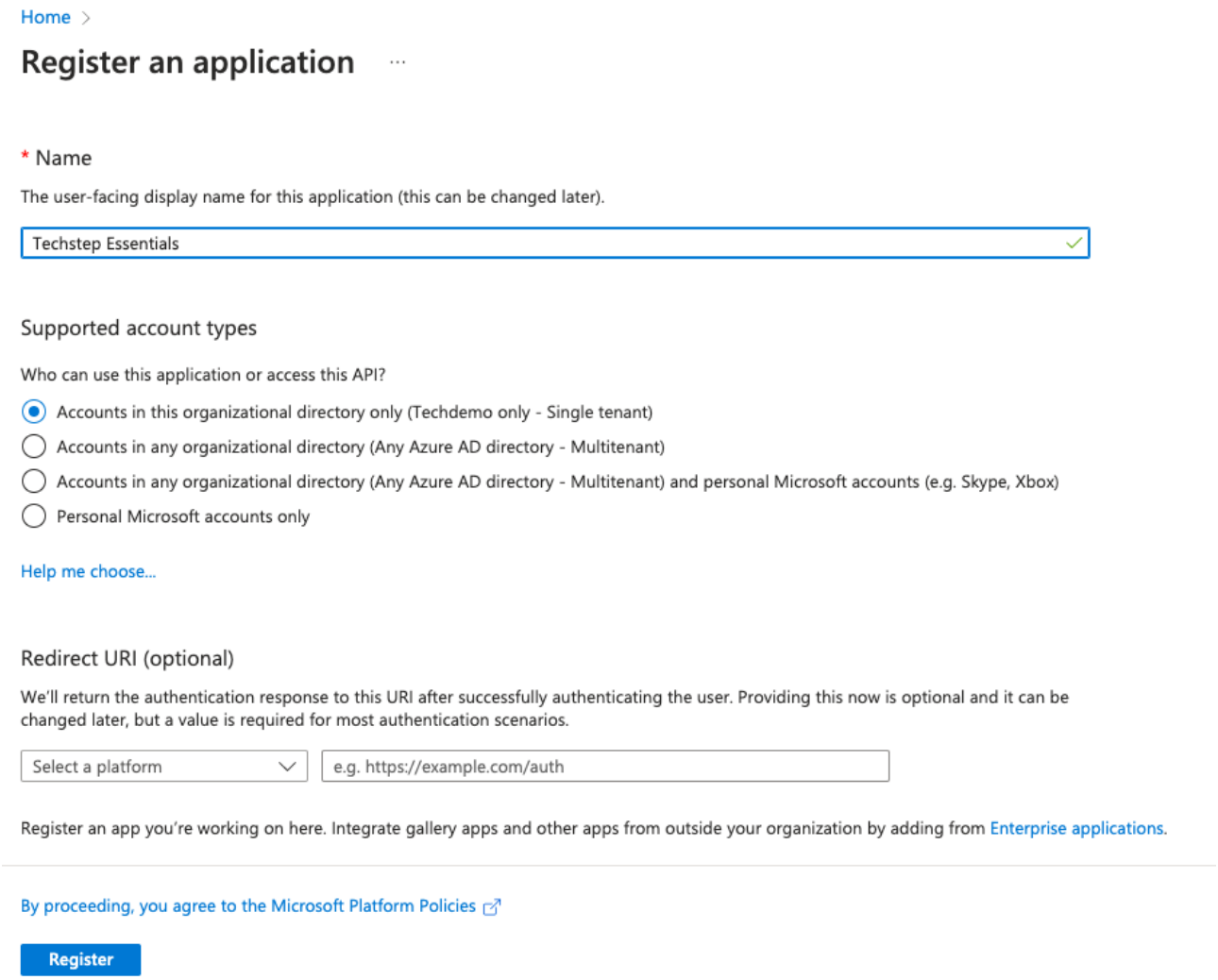
After going to the Azure AD tab, select Application registration from the menu on the left.



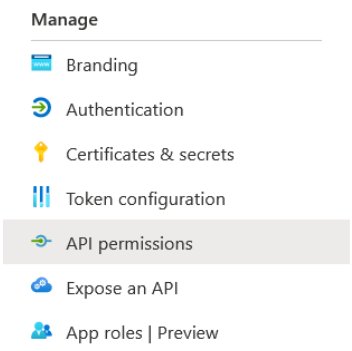
Then select the **New registration** option



In the next step, enter the name of the Application and specify whether accounts from one domain or more domains should have access to it - select single- or multi-tennant. We can also provide the URI to which the user is to be redirected after successful authentication (this is optional and can be done later). Press “Register”.

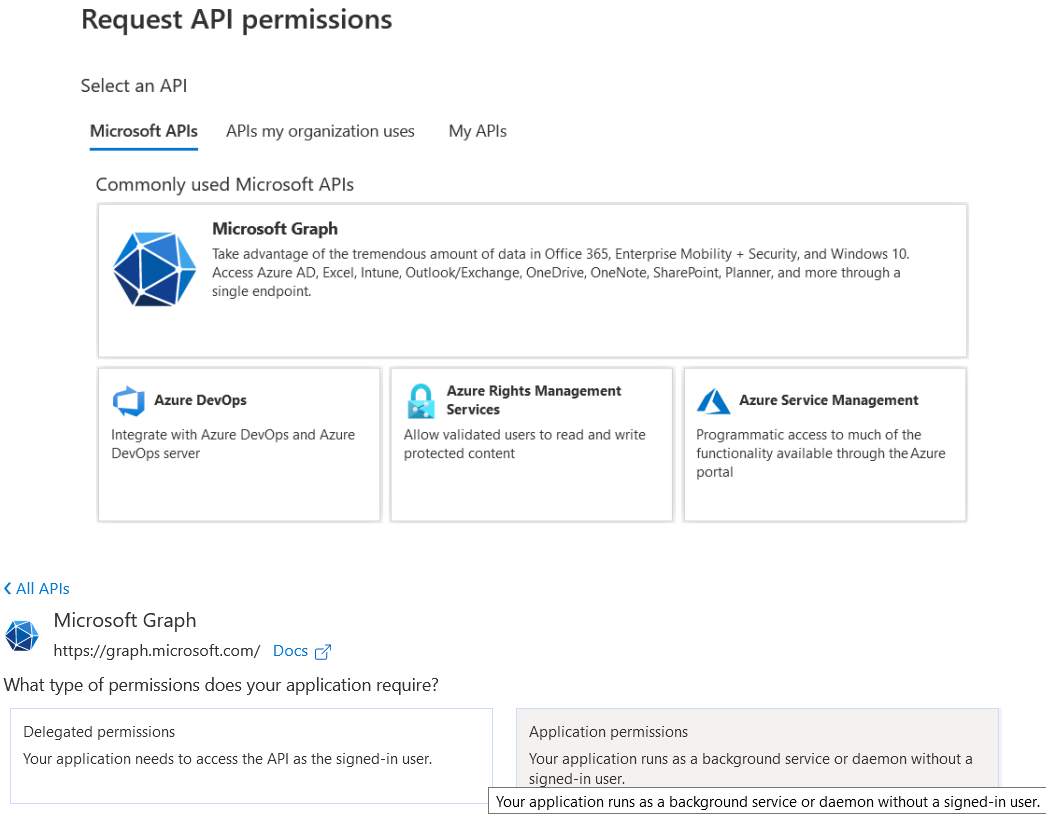


Then configure its permissions. Go to the API permissions tab.



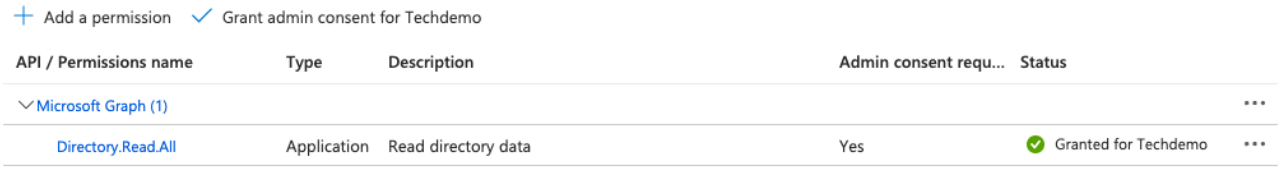
We can remove the default User delegated permissions by clicking the three dots icon, and then Remove permissions.

Then, we click Add a permission. We select Microsoft Graph and then Application permissions.

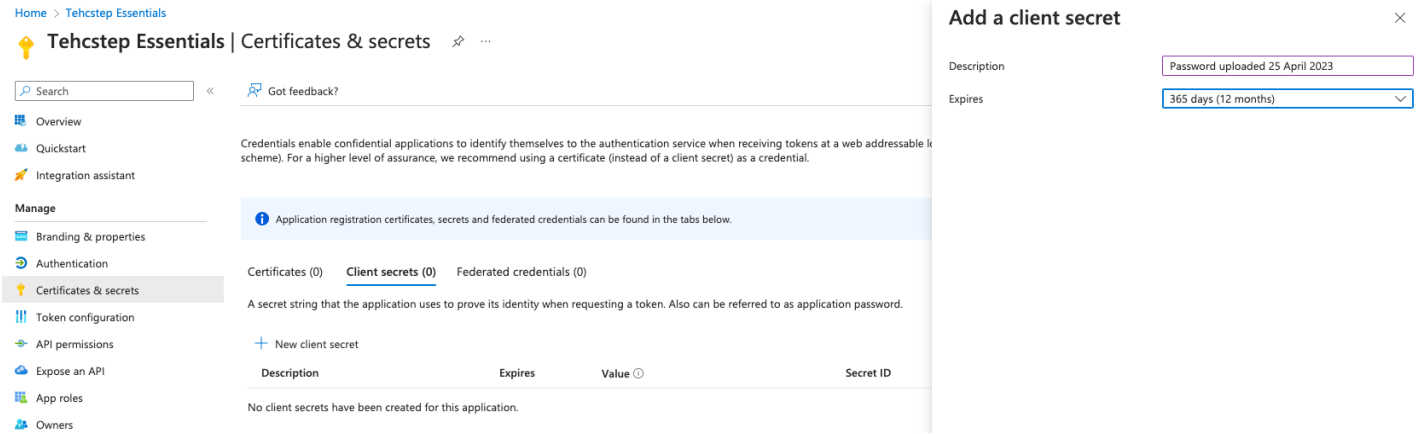


In the Directory section, select directory.read.all and confirm by clicking Add permissions.

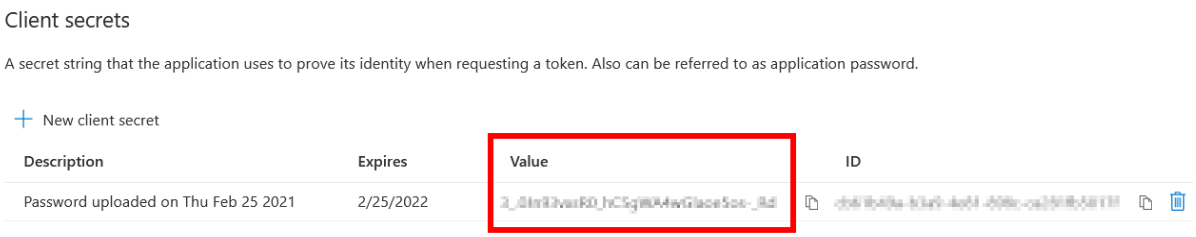
In the API permissions section it is also required to Grant Admin consent for created app.



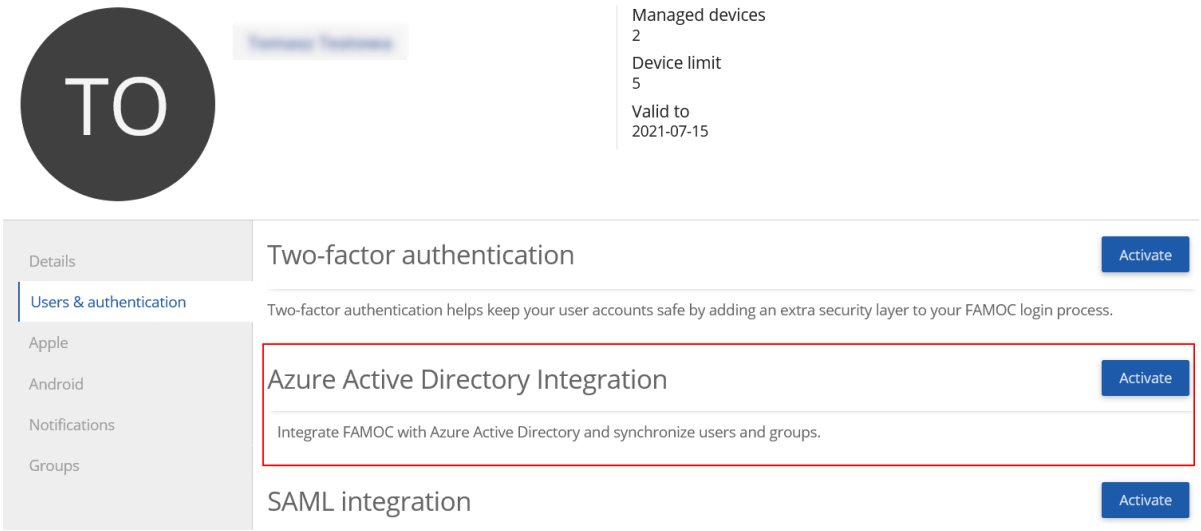
Then go to the **Certificates & secrets** tab to add a new client secret. Click New client secret, enter its description and specify an expiration time.



Then you MUST copy its value (it will not be displayed again).

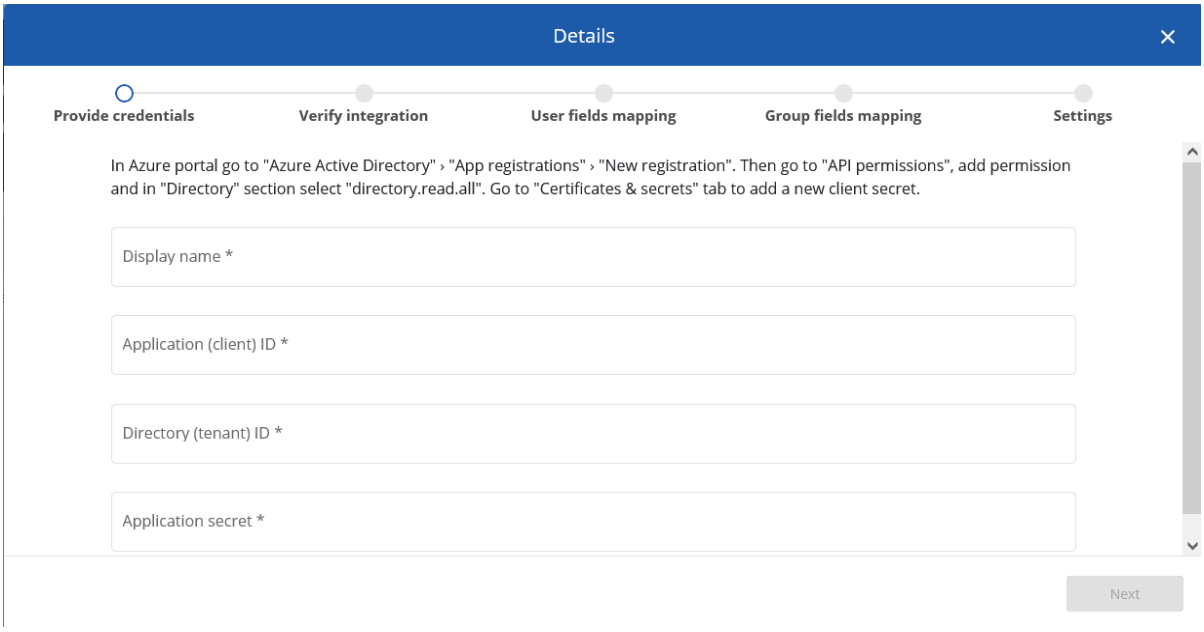


Then log in to the Essentials console. Go to your organization's settings, Users & Authorization section and then find the Azure Active Directory integration section. Click Activate.

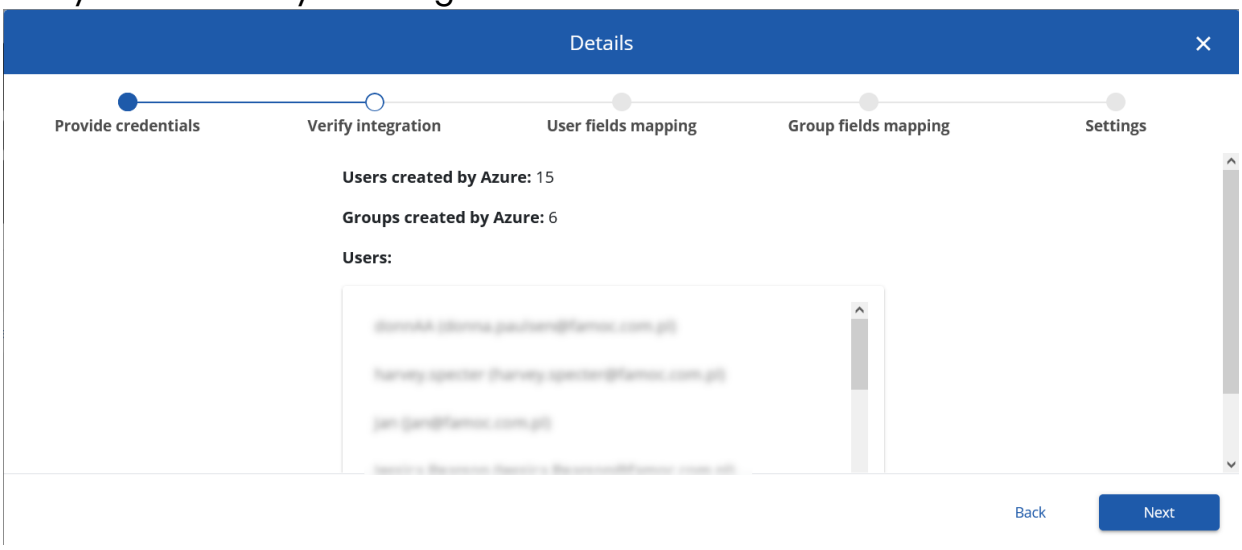


In the next step, enter the following data downloaded from the Azure portal:

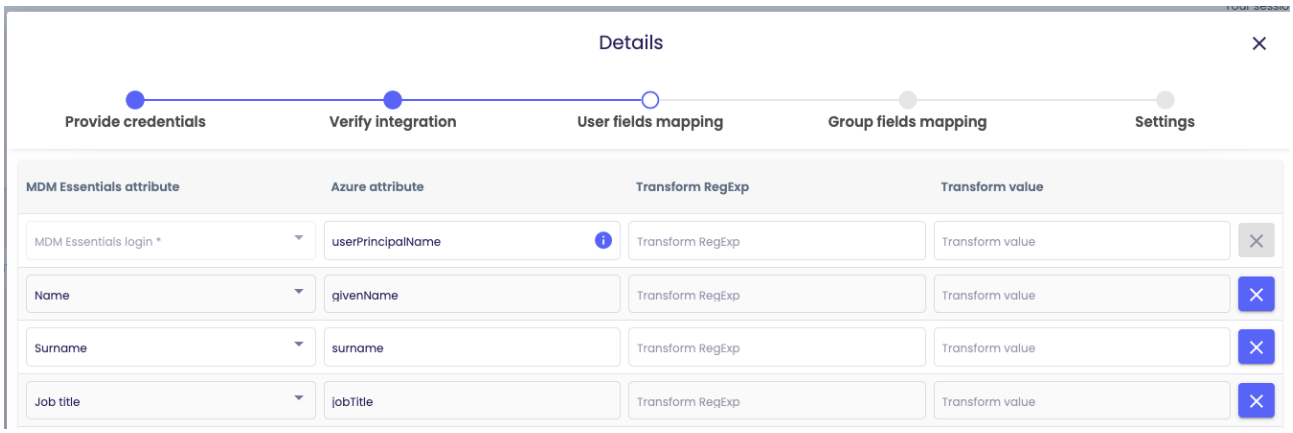
- **Display name** (can be any)
- **Application (client) ID**
- **Directory (tenant) ID**
- **Application secret**



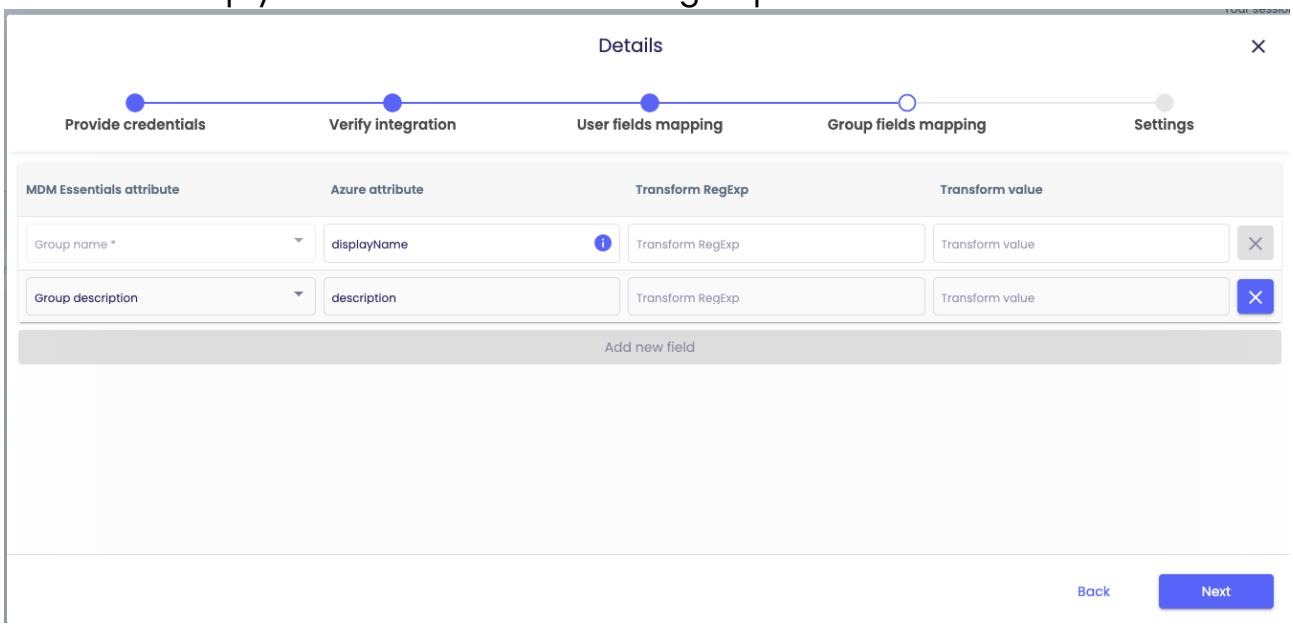
Once you click next your integration will be verified.



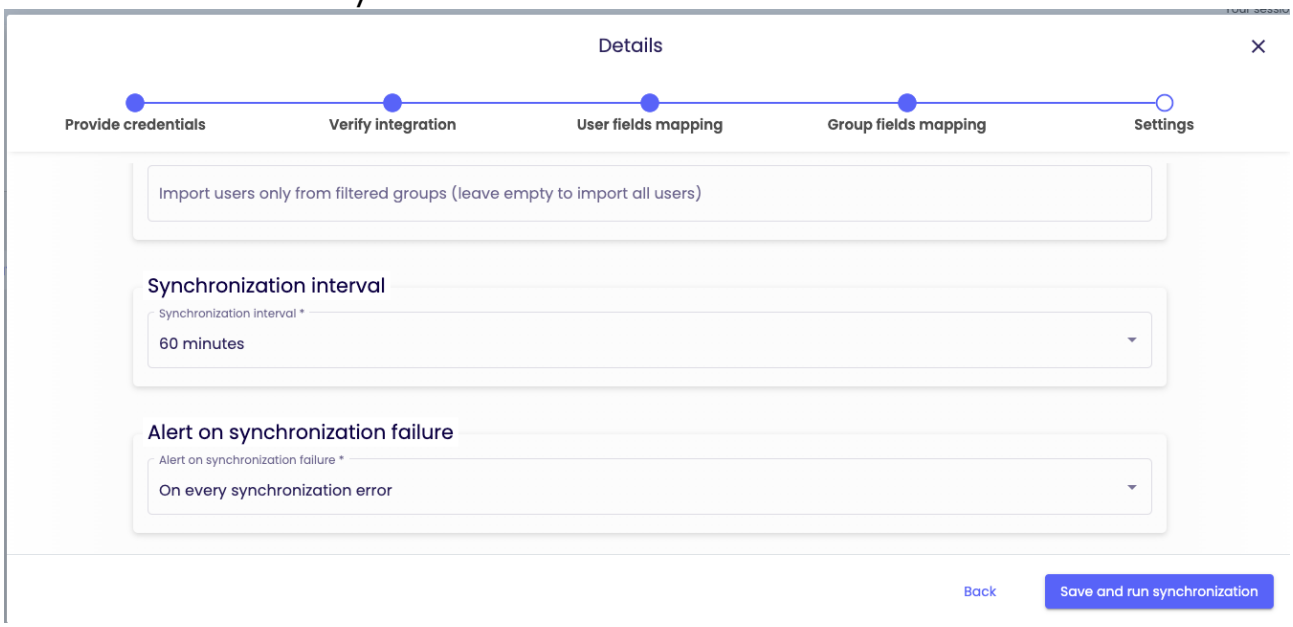
In the last step you can define the integration settings. First, you can assign attributes from Azure AD to automatically match them with the corresponding values in Essentials MDM (e.g. e-mail address, first name, last name, phone number or job title).



In the next step you can do the same with group attributes.



In the last step, you can also define filters to limit the imported data according to specific parameters for Users and/or Groups. You can also define the synchronization interval (by default 60 minutes, the maximum is 24 hours) and the desired “Alert on synchronization failure”.



A detailed description of the filter syntax can be found in the Microsoft documentation:
https://docs.microsoft.com/en-us/graph/query-parameters#filter-parameter
Additionally, it is also possible to use advanced queries:
https://docs.microsoft.com/en-us/graph/aad-advanced-queries
Microsoft provides a tool to validate the entered filters:
https://developer.microsoft.com/en-us/graph/graph-explorer

To finish the process, click Save and run synchronization.
If everything went ok you will see a short summary of imported users as shown in the image below. You can make changes to the integration by clicking "Edit".