# TDM5 - How To setup SSO

# Introduction

TDM5 offers the ability to configure authentication through Single Sign-On (SSO).
Enabling SSO offers administrators the ability to manage all their users and roles from their own Azure AD.

# Requirements

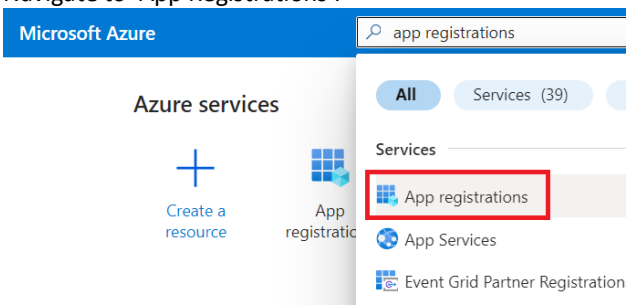
If you want to setup Single Sign-On (SSO) you need to meet the following requirements:

- Have administrator access to your TDM5 environment
- Administrator access to your Azure AD
- Have groups setup in AD to synchronize

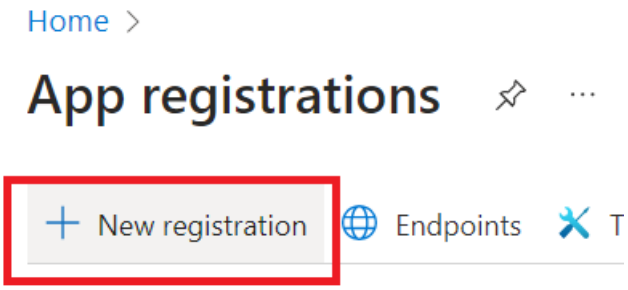
# Create your Azure application

1. Login in as an administrator in your Azure portal: https://portal.azure.com/

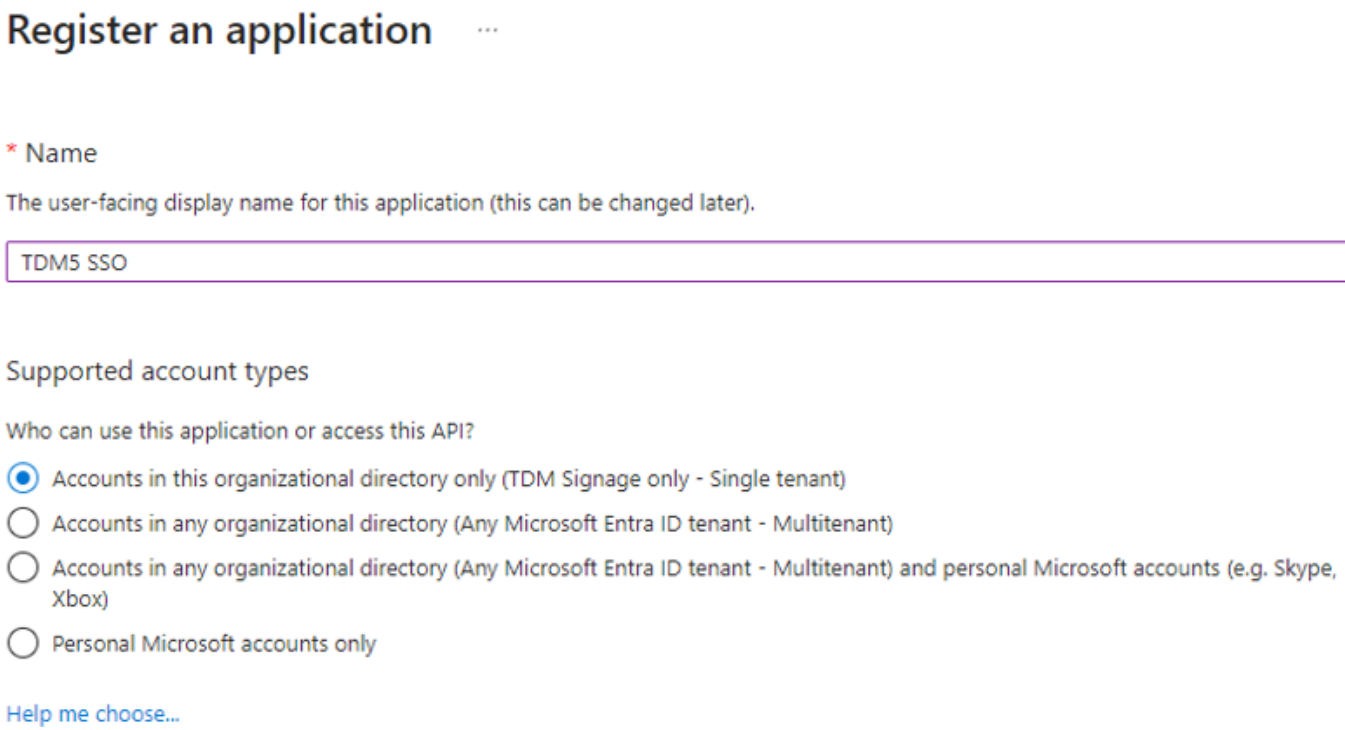
2. Navigate to ‘App Registrations’.



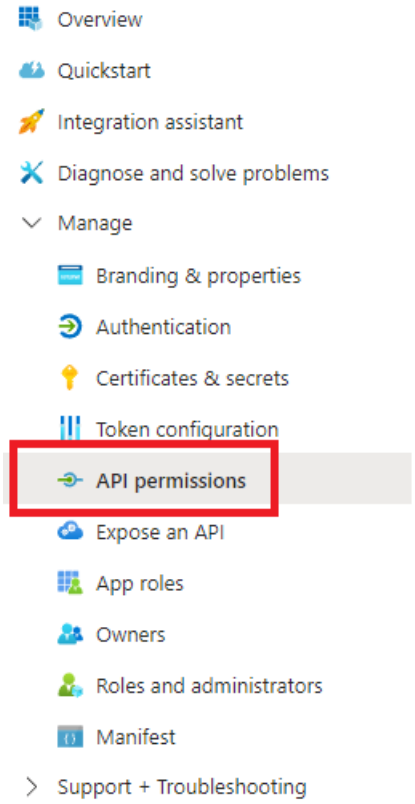

3. Create a new ‘App Registration’.




4. Give your application a name and select that it is available for your Tenant only. Now click ‘Register’.

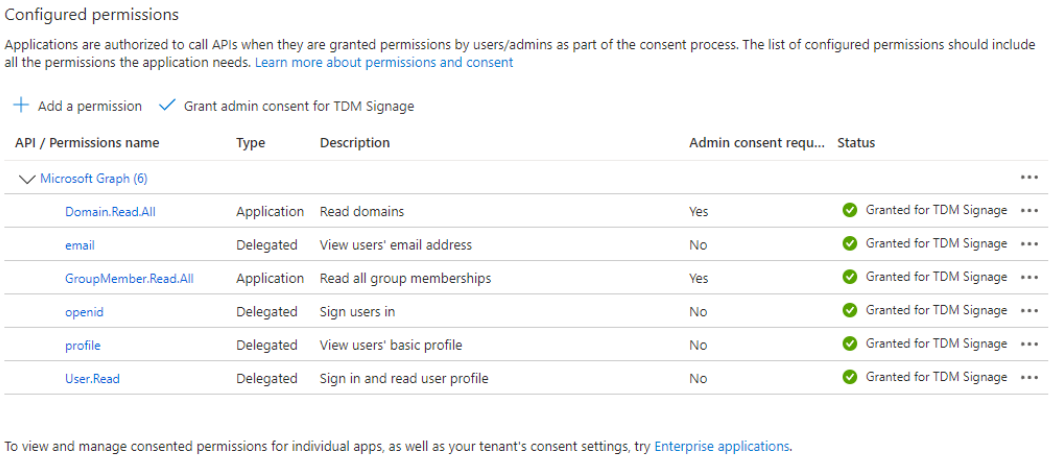


5. After the app is created it opens the ‘App Overview’. Navigate to ‘API Permissions’ in the left bar.

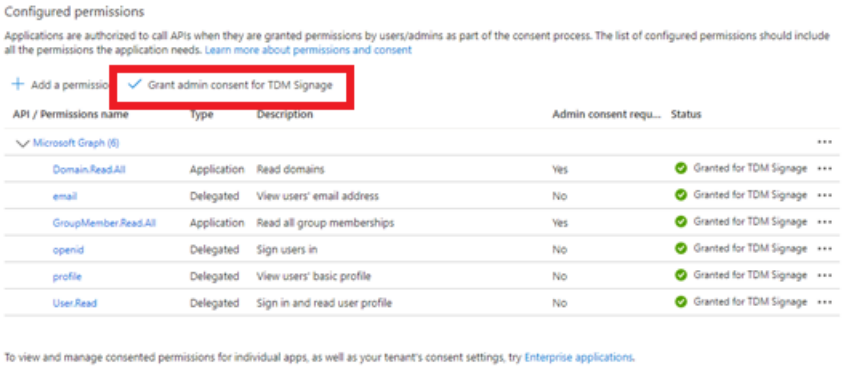



6. Next select “Add a permission”. In the pop-up select “Microsoft Graph”. Next select “Delegated permissions”.
   In the next menu select the following permissions, and after press “Add Permissions”:
   - Email
   - Openid
   - Profile
   - User.read

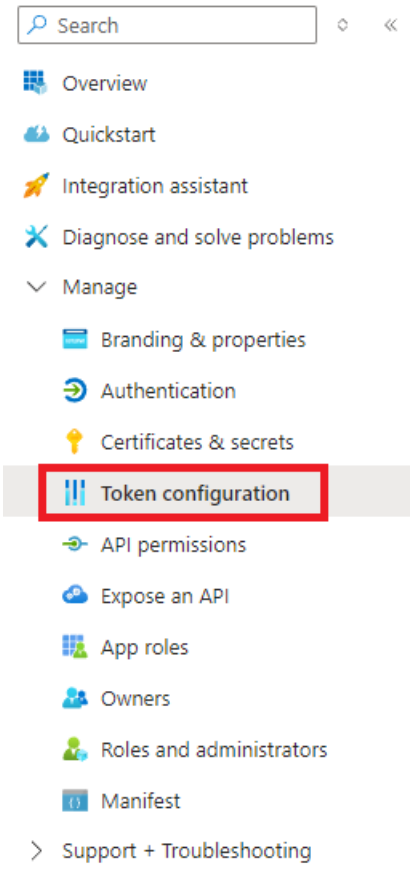
   Now Press “Add a permission” again, select “Microsoft Graph” and now choose “Application Permissions”.
   In the next menu choose the following permissions and press “Add Permissions”:
   - Domain.Read.All
   - GroupMember.Read.All



7. Finally press on “Grant admin consent for <Tenant Name>” to grant permissions for your tenant.

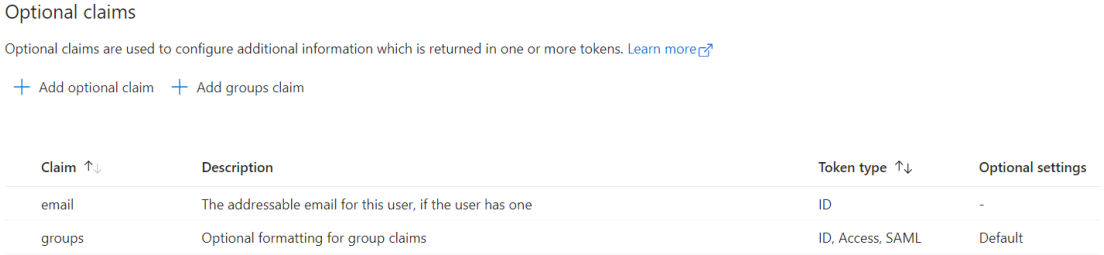



8. Now navigate to “Token configuration” in the left bar.

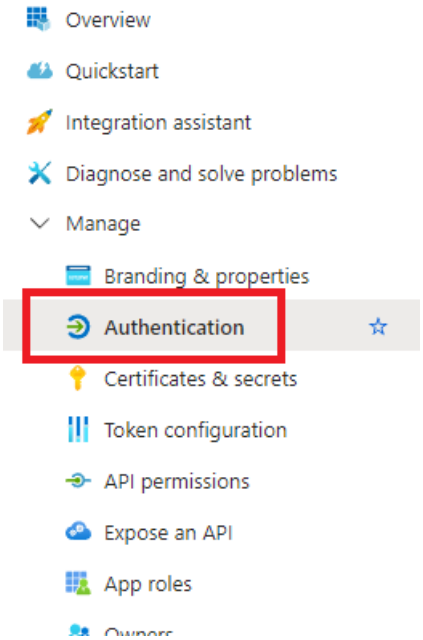



9. Select “Add optional claim”, in the pop-up choose for token type “ID”, claim “email”. Next press ‘Add’.

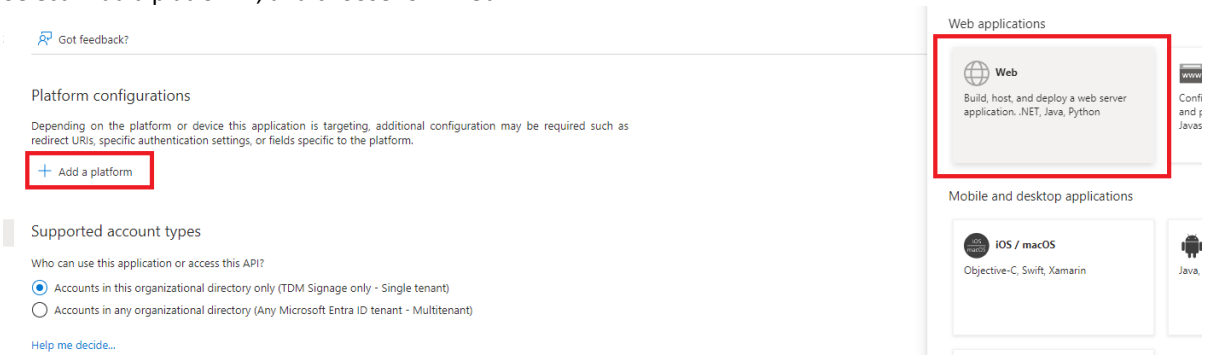
10. Now select “Add groups claim”, in the pop-up select “Security Groups”, and below SAML make sure this is set to “Group ID”. Now press Add to add the claim.
This should now look like below:



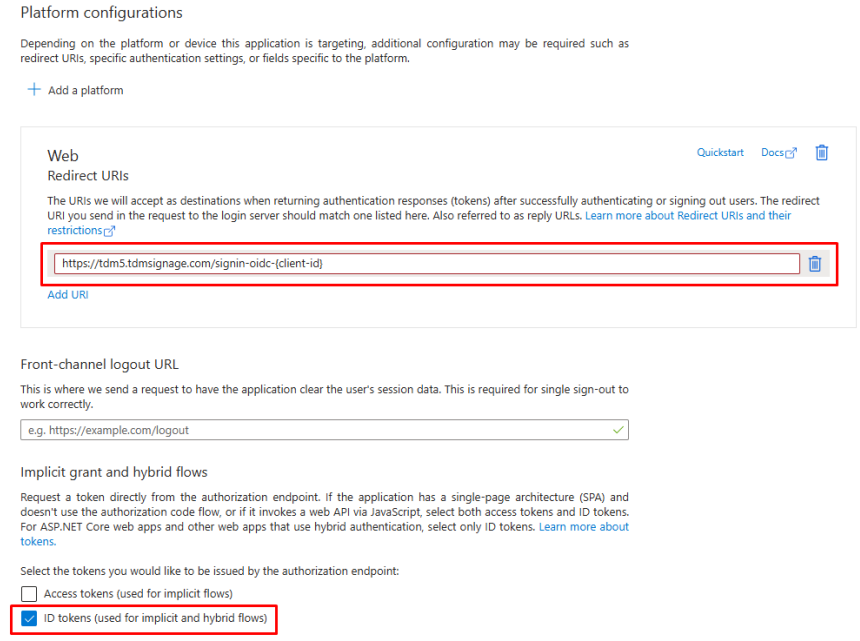
11. For the next step we navigate to ‘Authentication’.



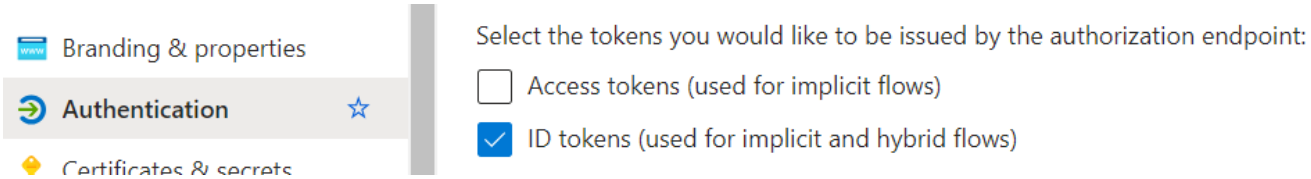

12. Select “Add a platform”, and choose for “Web”.



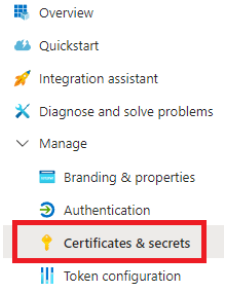

13. Enter the Redirect URL: https://tdm5.tdmsignage.com/signin-oidc-{client-id}.
The client-id can be found on the ‘Overview’ page of the Azure application. Make sure the checkbox for ID tokens is also enabled.



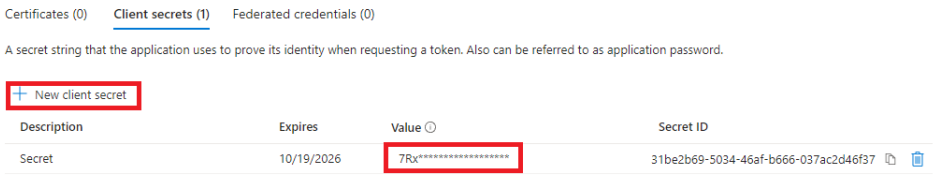
14. In case you forgot to enable the ID Tokens in the previous step, you can still enable this in the ‘Authentication‘ menu.



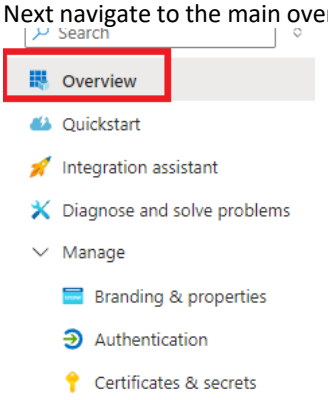

15. Next Navigate to the menu “Certificates & Secrets”.



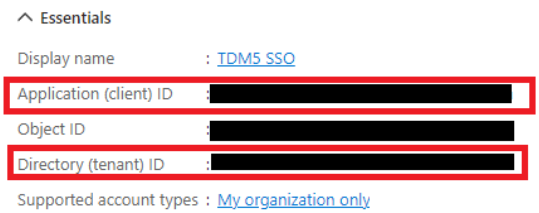

16. Select the “Client secrets” submenu, and choose to create a new client secret. Give your secret a description, and choose an expiration date and press “Add”. The shorter the date, the faster you will need to create a new secret, and update your configuration in TDM.
After creation, copy down the key in the “Value” column. You can only see this value now, on later visits you can only see the first three characters to help identity your secret.




17. Next navigate to the main overview.

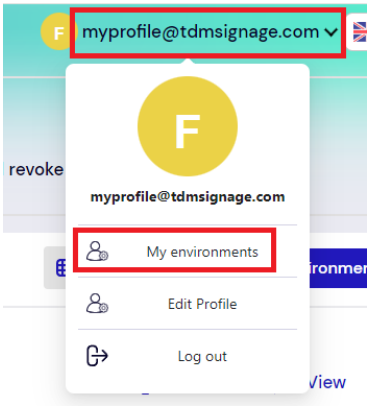



18. Note down your Application (client) ID and your Directory (tenant) ID as we will need these, together with the client secret, to configure SSO in TDM5.



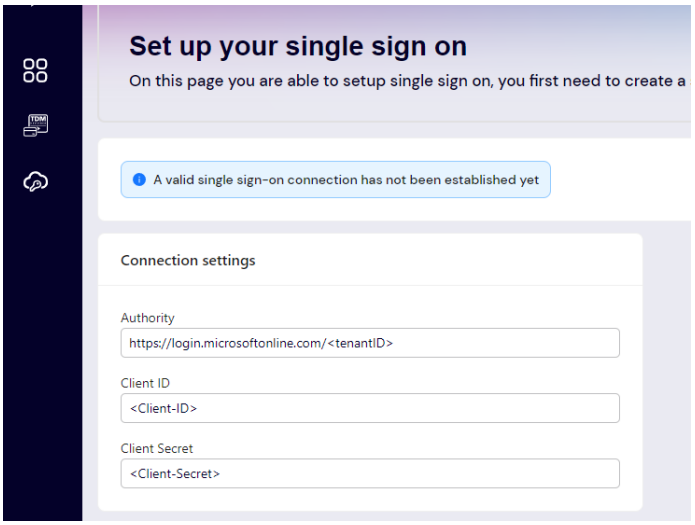
# How To configure SSO in TDM5:

1. Login in as an administrator in your TDM5 portal and go to your ‘My Environments’ page.



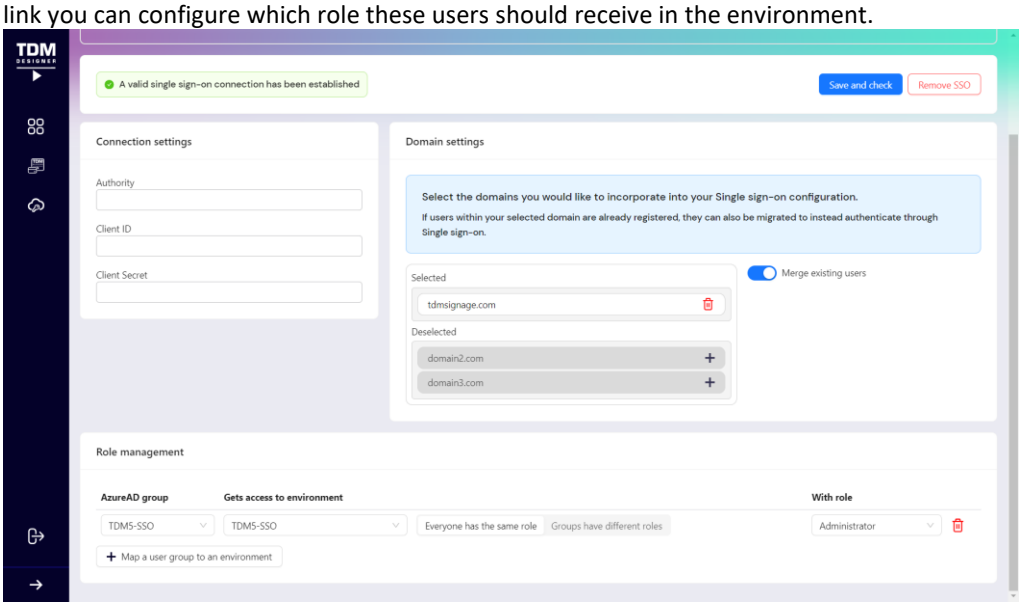

2. Select the SSO configuration menu in the sidebar.


3. Next fill in the Client ID and Secret from the App which we created in Azure. For the authority fill in the following URL: “https://login.microsoftonline.com/<tenantID>” where <tenantID> is the ID of your Azure tenant which we also found during the creation of the Azure application. Afterwards press ‘Save and Check’.



4. If all credentials are correct, the settings will be saved and there will be SSO options to configure.
   - In the domain settings, you can add or remove the domains of the users you would like to be able to login with SSO.
     The domains configured here are used to determine if a login attempt should use SSO or not.

   - In Role management you can select the role from Azure AD which you would like to link to TDM5. The following field determines to which environment these users should have access too. At the end of the link you can configure which role these users should receive in the environment.




   Finally press ‘Save and check’. Your SSO configuration is now set up.