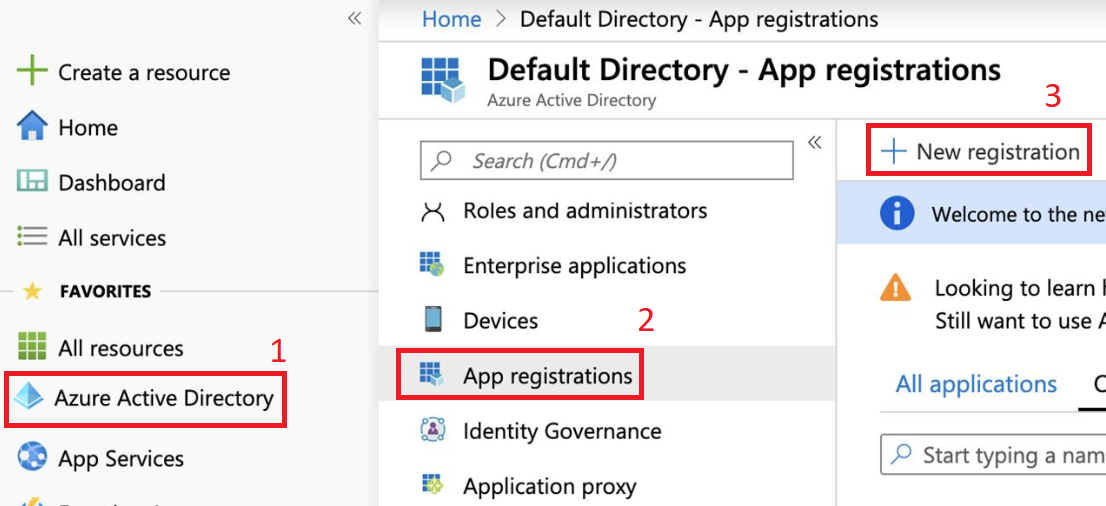
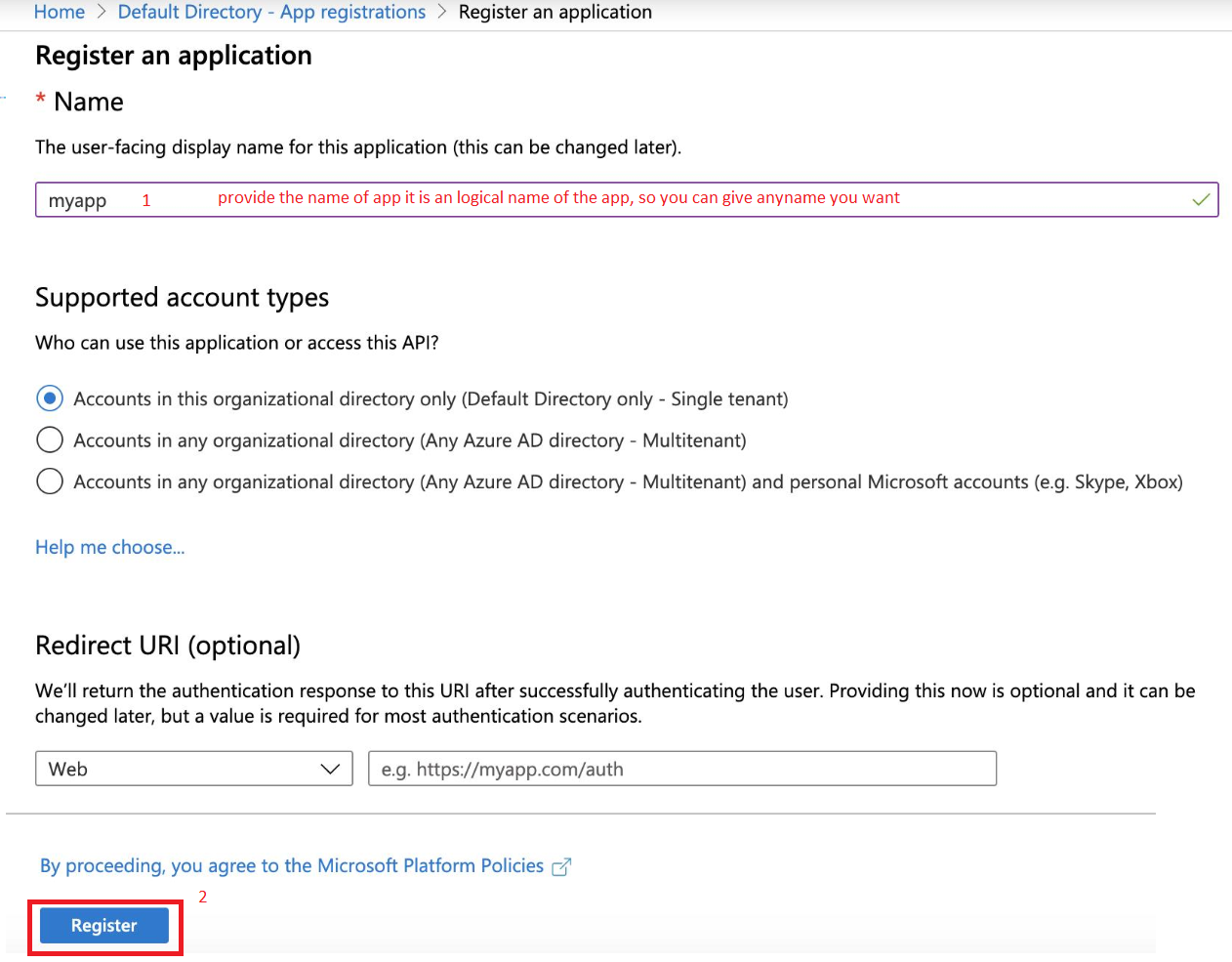
How to register an app in active directory and provide RBAC to clients

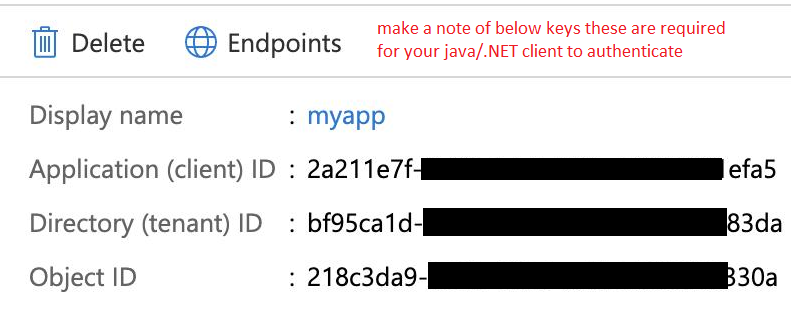
1. Go to Azure Active Directory



1. Register an app

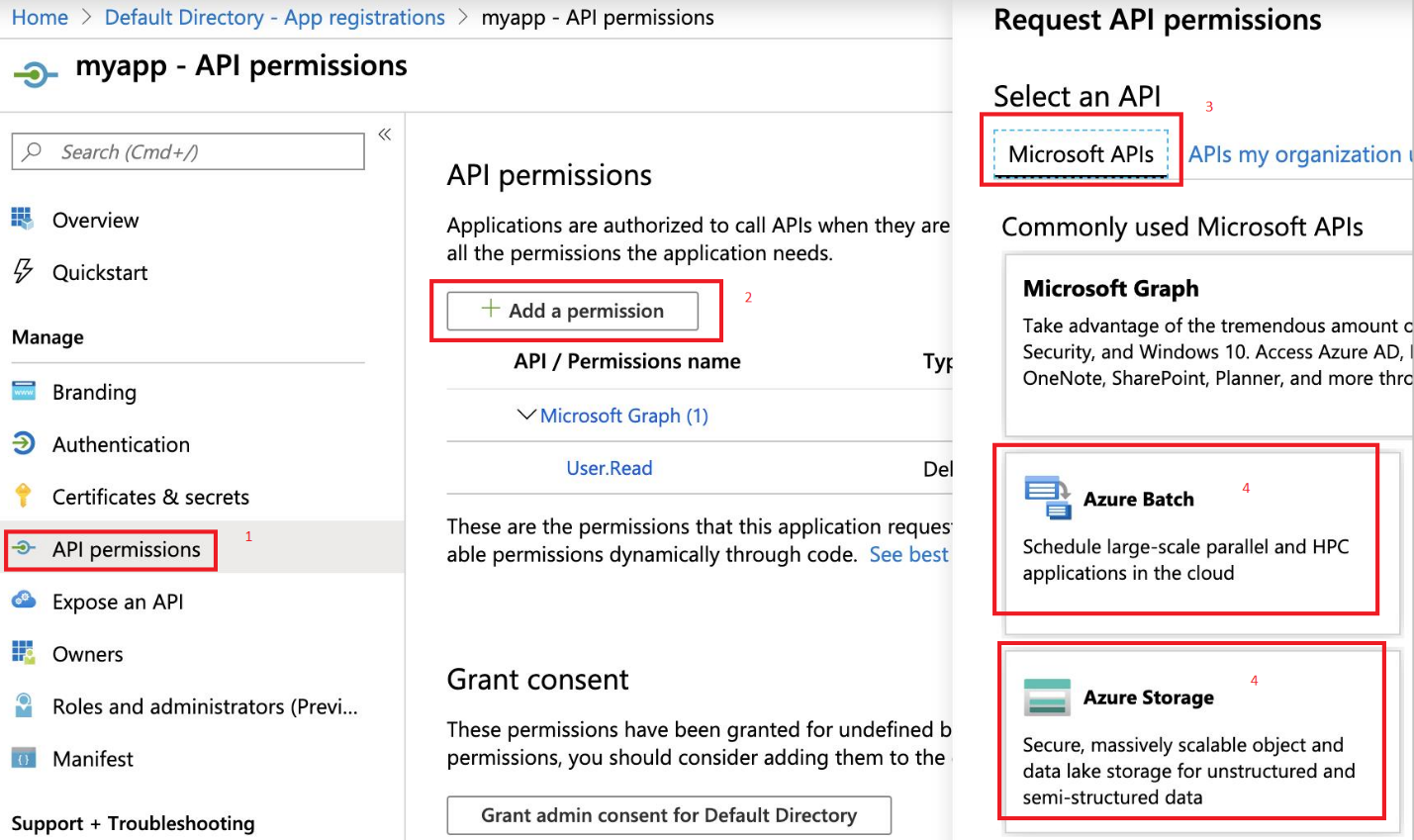


1. Once app is registered

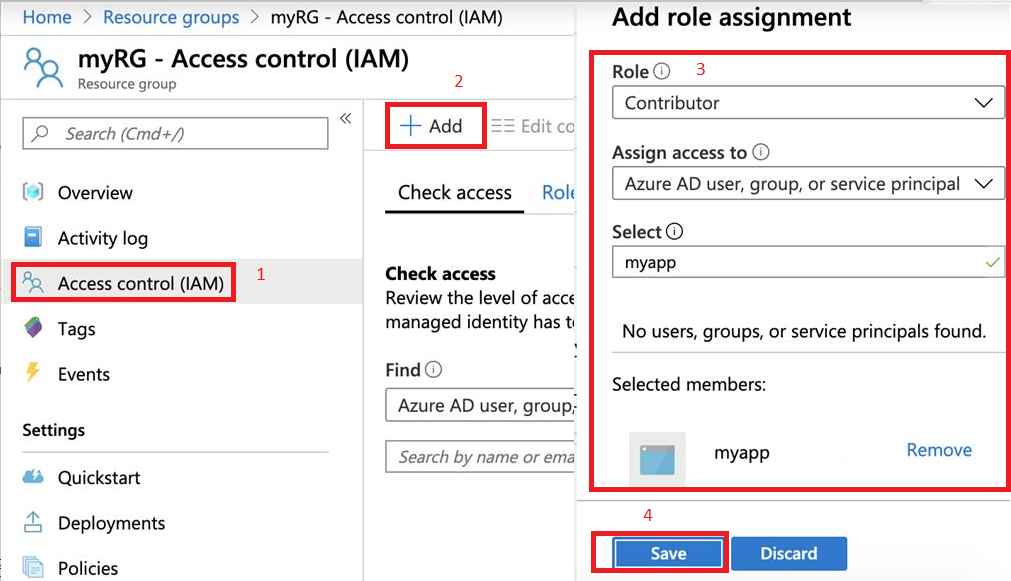


1. Now click on view API Permission button to add required permission
2. In API permission blade click on add a permission button
3. In “Request API permission button” in Microsoft APIs tab select Azure Batch for this example or you can add more as we need to access storage account as well so we add both Azure Batch and Storage account.

**Note: you can use this method for your other clients as well i.e. which is not related to Azure Batch or Storage account**



1. Click on Azure Batch a new blade will open select user\_impersonation and then click on Add Permission button. Repeat this process for adding storage account as well.
2. Now click on “Grant admin consent for Default Directory” without this your changes will not work. And then click “Yes” in the pop p blade.
3. Once successful navigate to your resource group and then click on Access control (IAM) option for the resource group.
4. Click on the “+ Add” button



1. Now Click on the Certificates & Secrets and generate a secret copy the secret key this will go in your azure auth file in parameter “key”

For Creating all the resources from your java client you have to follow below steps:

1. GO to your Azure Active Directory
2. Click on Groups
3. Click “+ New Group”
4. Select the group type “Security”
5. Enter group name (any name you want)
6. Select Membership type “Assigned”
7. In the owner select the owner of the application
8. In the members select the application that you created/registered in the active directory.
9. Now you are able to create your resources directly from your java client.