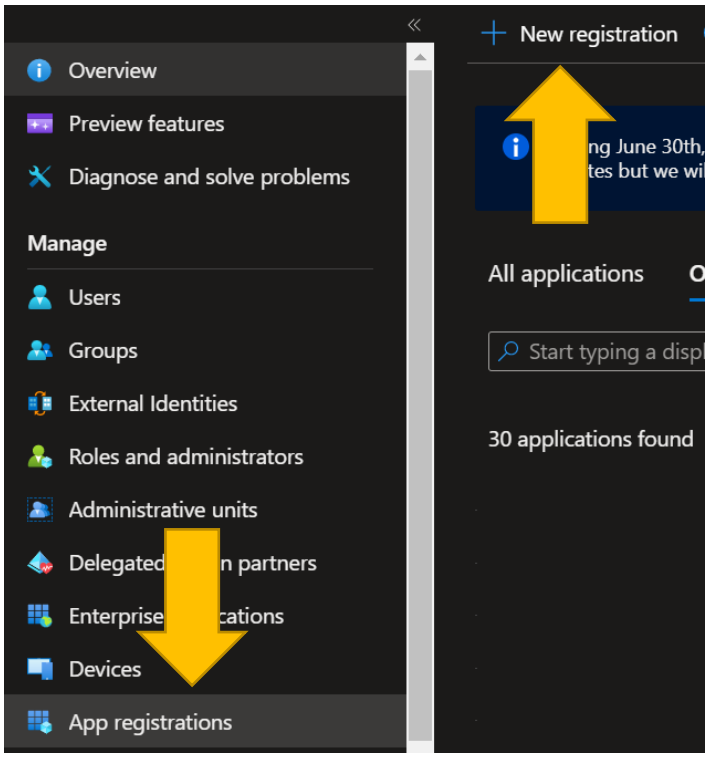
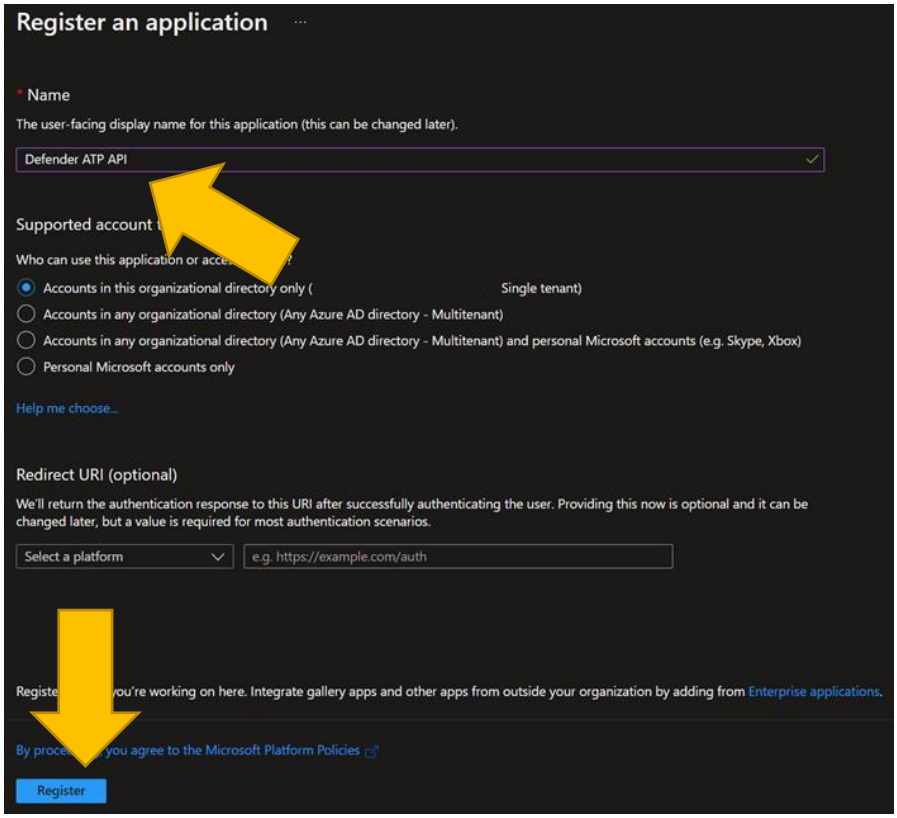
Registering the Defender Application

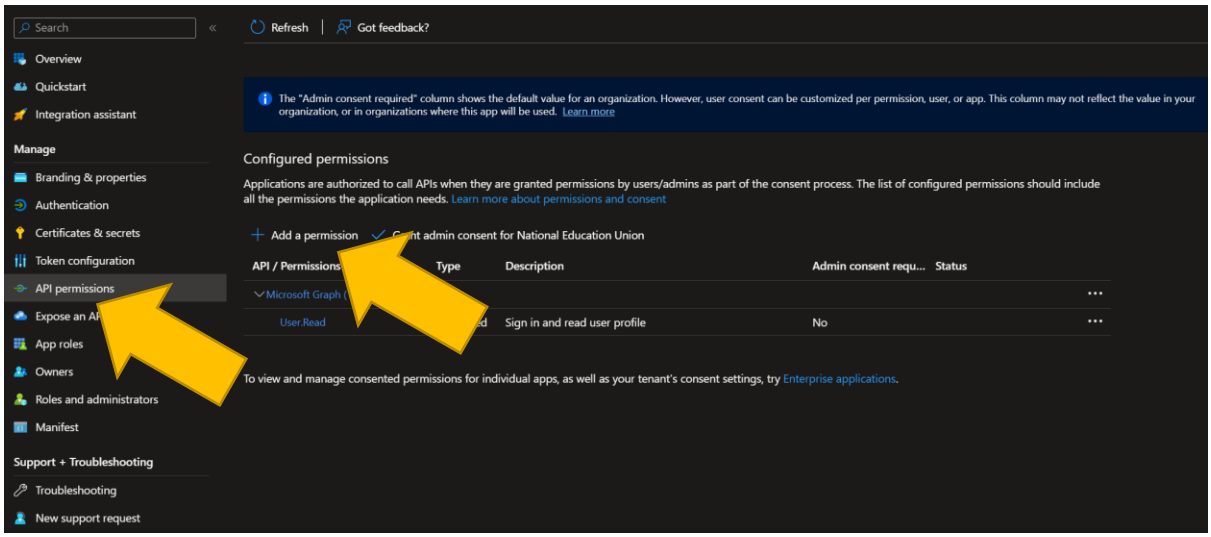
In the Azure portal, go to “App Registrations” and choose “New registration”



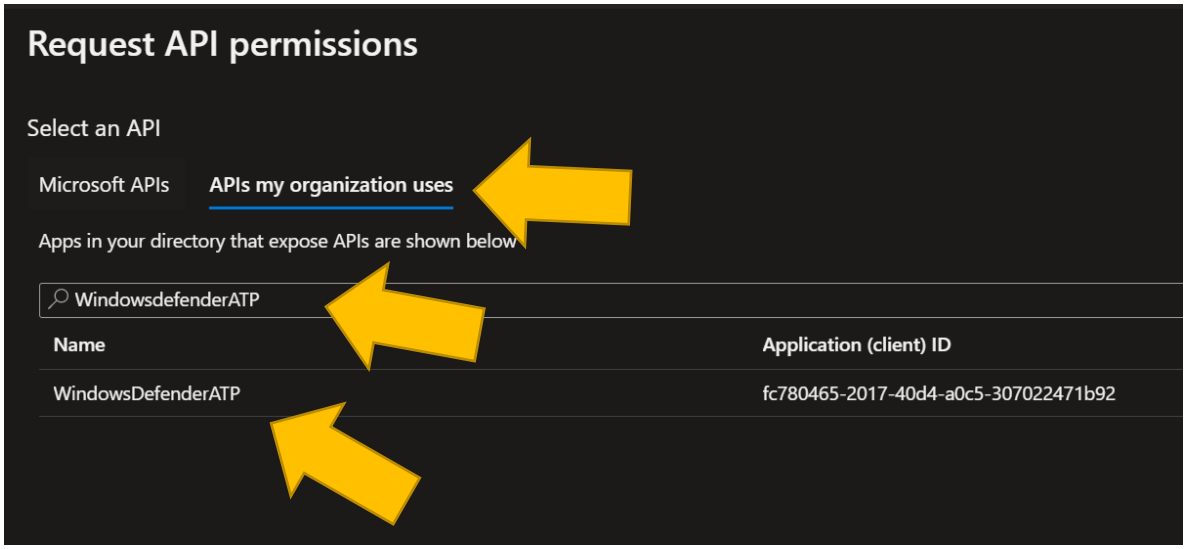
Type a name in for the application (eg “Defender ATP API”) and press “Register”



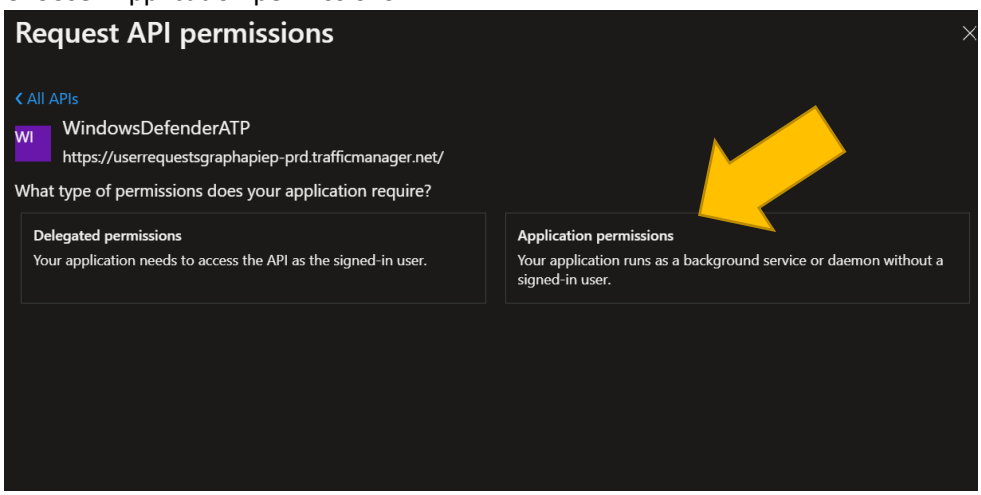
Click on “API Permissions”, then “Add a permission”



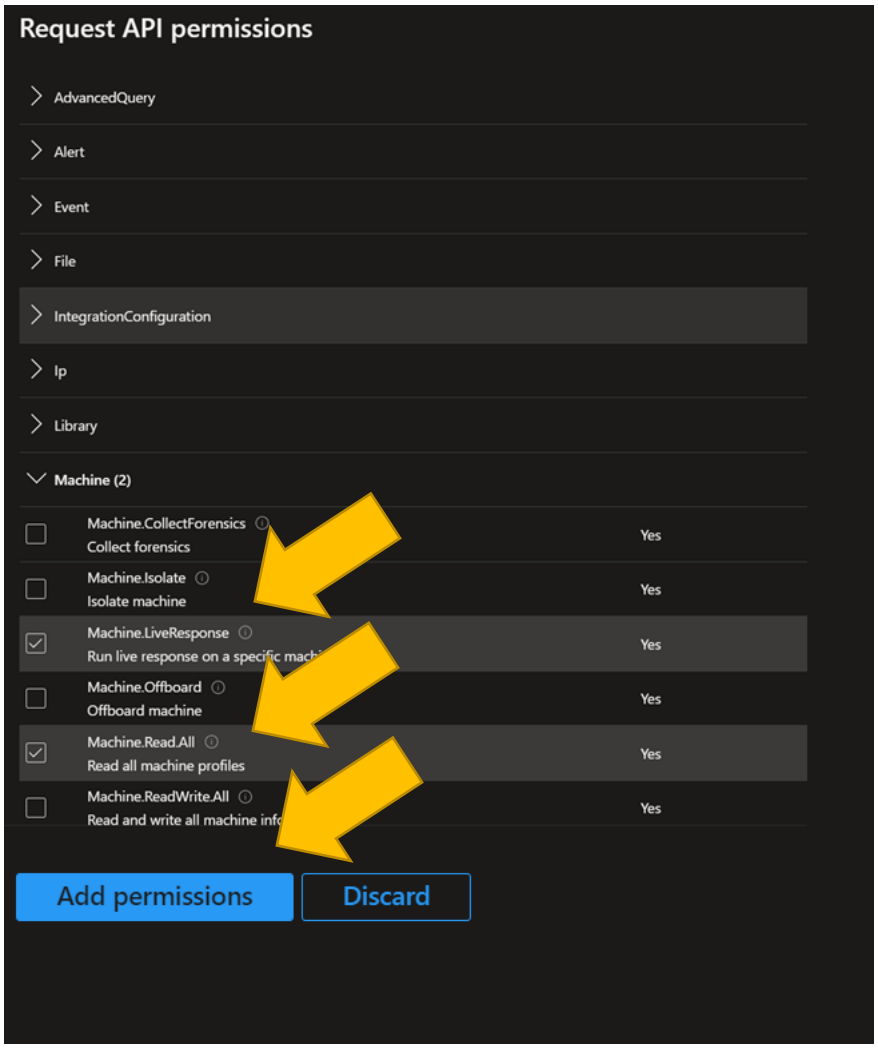
Choose “APIs my organisation uses”, then type “WindowsdefenderATP” in the search bar. Click on the “WindowsDefenderATP” application that it finds



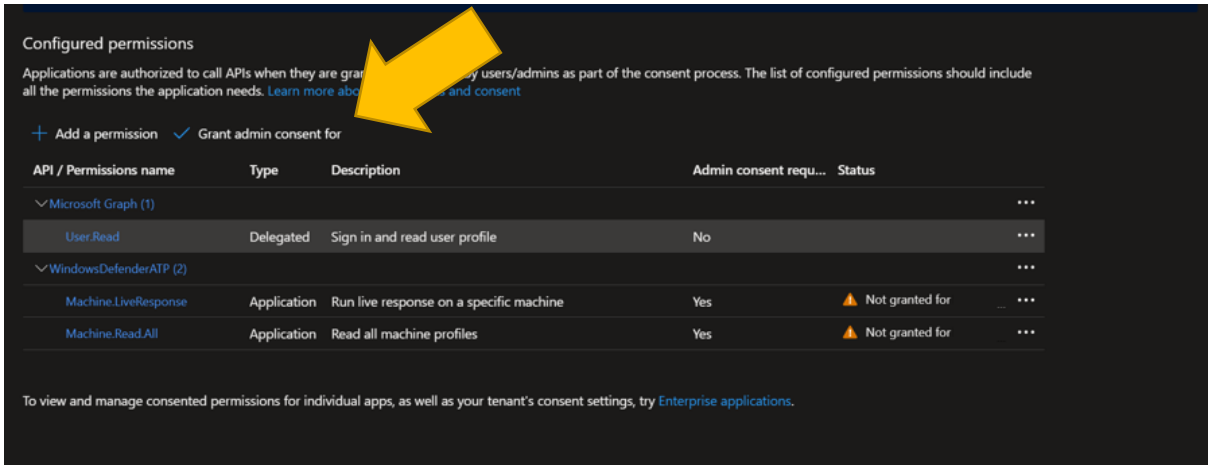
Choose “Application permissions”



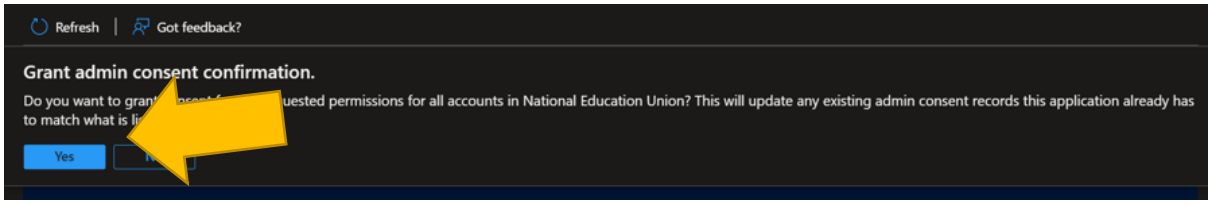
Under “Machine”, choose “Machine.LiveResponse” and “Machine.Read.All”, then click “Add permissions



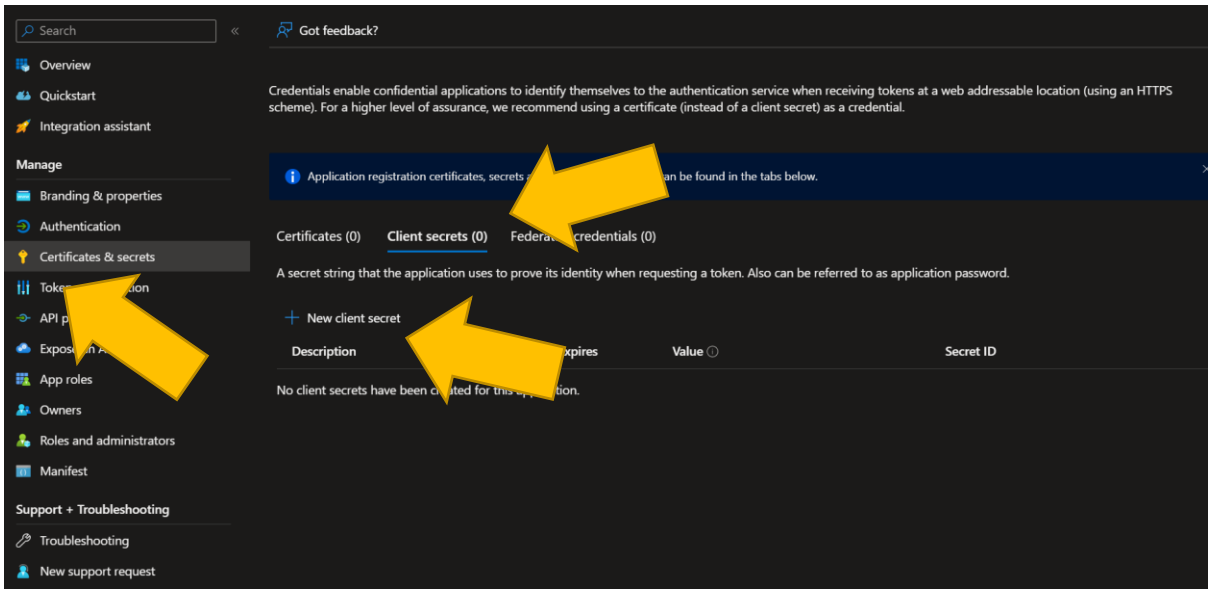
Now press “Grant consent for [Your organisation]”



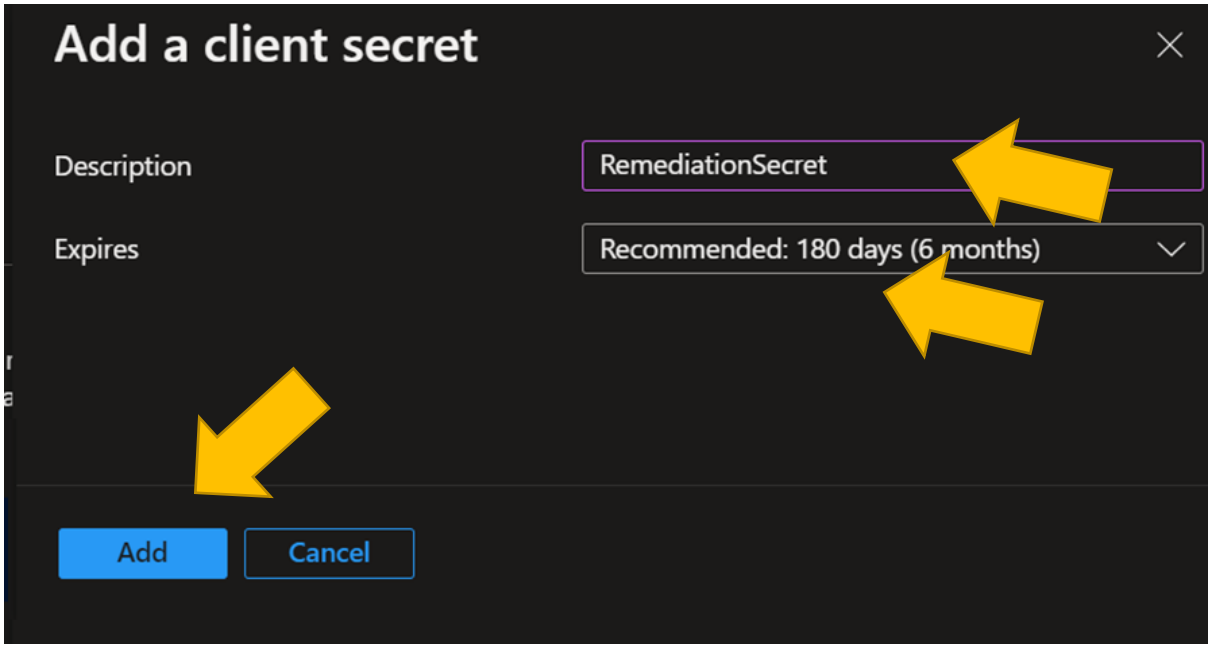
Then click “Yes”



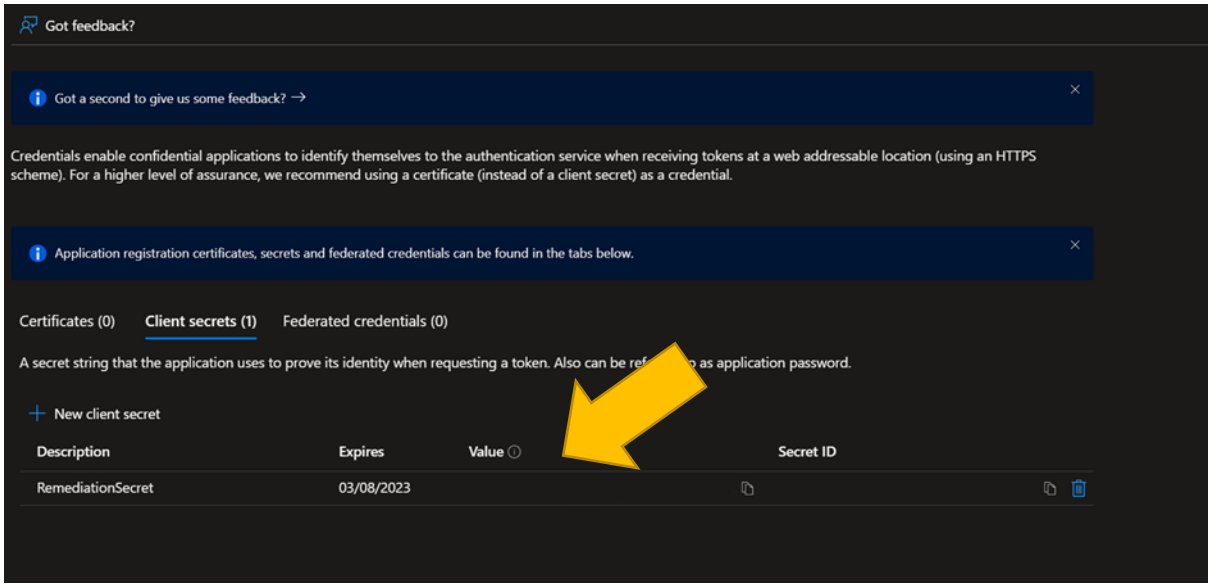
Go to “Certificates & Secrets”, choose “Client secrets” and press “New client secret”



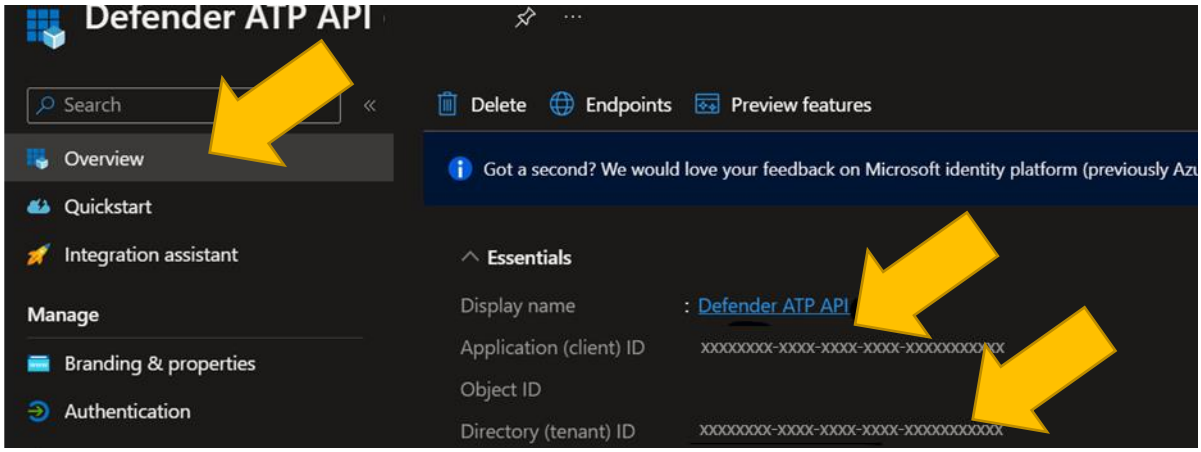
Give the secet a name and an expiration period, then click “Add”



Make a note of the secret value – you will need this every time you connect to the API – you should store this securely – KeyVault is recommended!



On the “overview” note the “Application (client) ID” and your “Directory (tenant) ID” – you will also need these every time you connect ot the API



You now have set up everything you need to run the scripts.