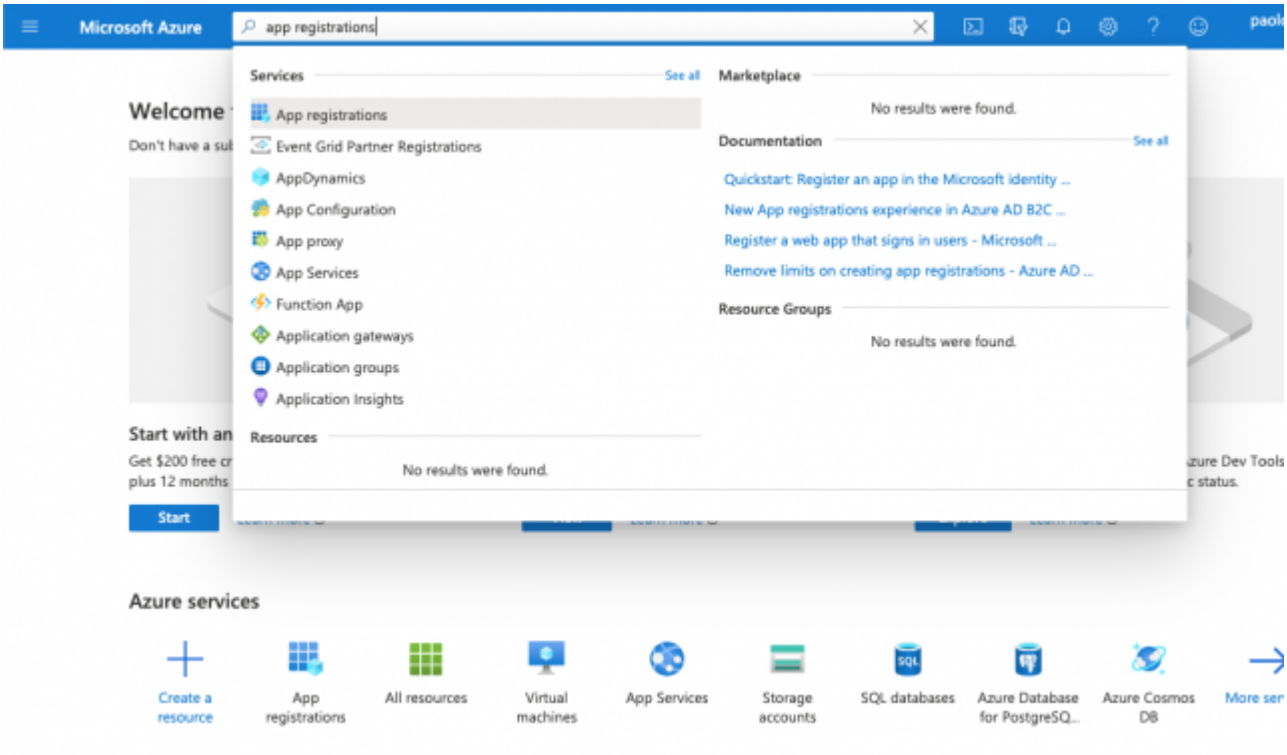
Microsoft Azure AD Libraesva App registration

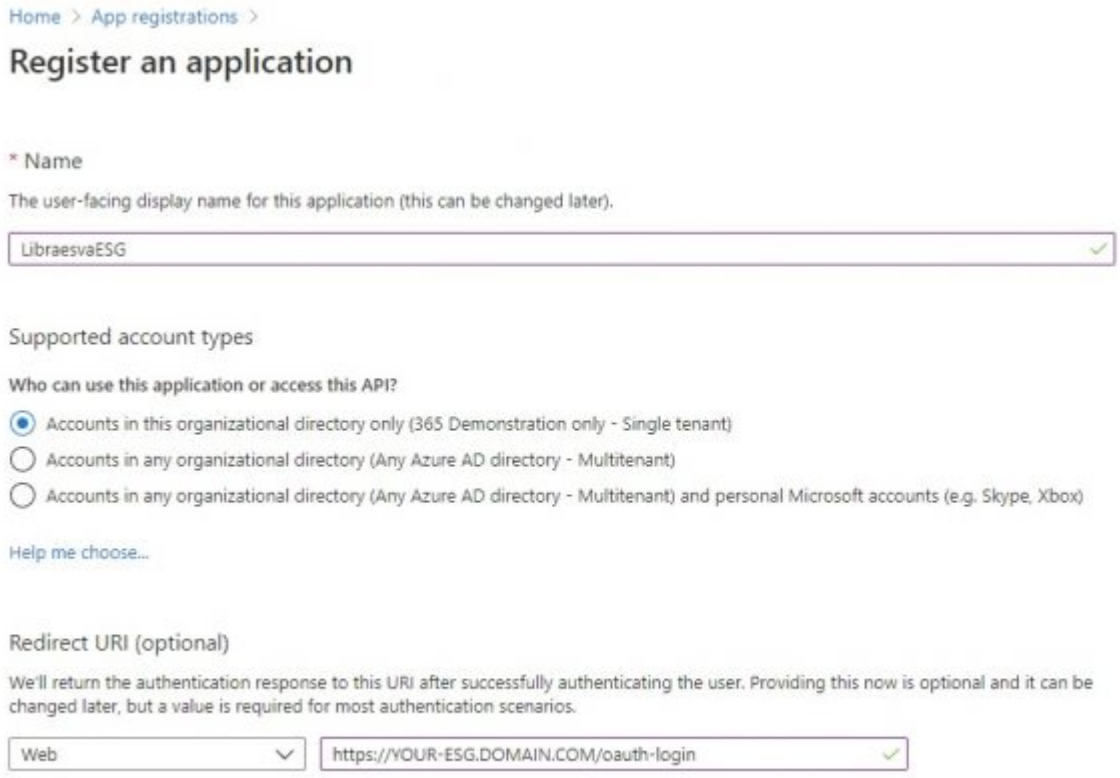
Office 365 relies on Azure Active Directory as directory service. Each Office 365 tenant corresponds to an Azure AD tenant where its user information is being stored. This guide will cover the steps needed to grant your Libraesva Email Security Gateway permissions on your Office 365 tenant. No changes are made to the Office 365 tenant itself by Libraesva Email Security Gateway.

- Navigate to https://portal.azure.com/ and log in using your administrator credentials (NOT FROM https://aad.portal.azure.com/)
- Open the **App registrations** portal as shown:

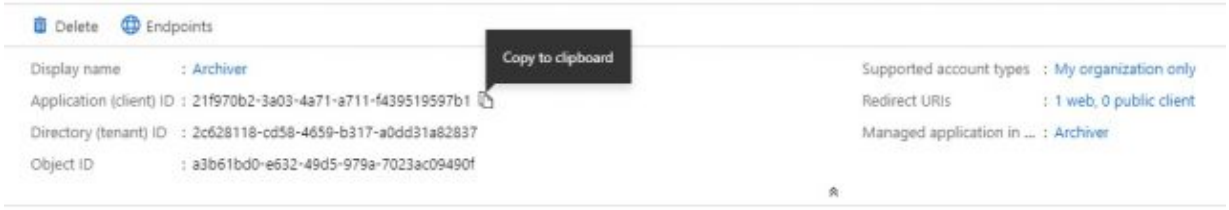


- Click on the **New registration** button
- Insert ESG as the name of the application, choose **Accounts in this organizational directory only** as the supported account type and type **https://your-esg.domain.com/oauth-login** where **esg.domain.com** is the url you use to access the ESG appliance in the **Redirect URL** field.

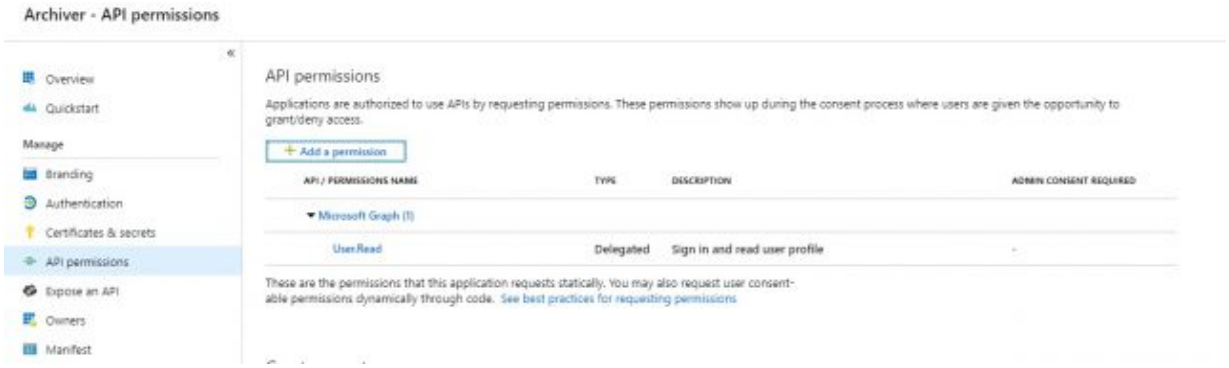
×**NOTE**: If you have a Libraesva ESG Cluster, please add both nodes address under Redirect URL.



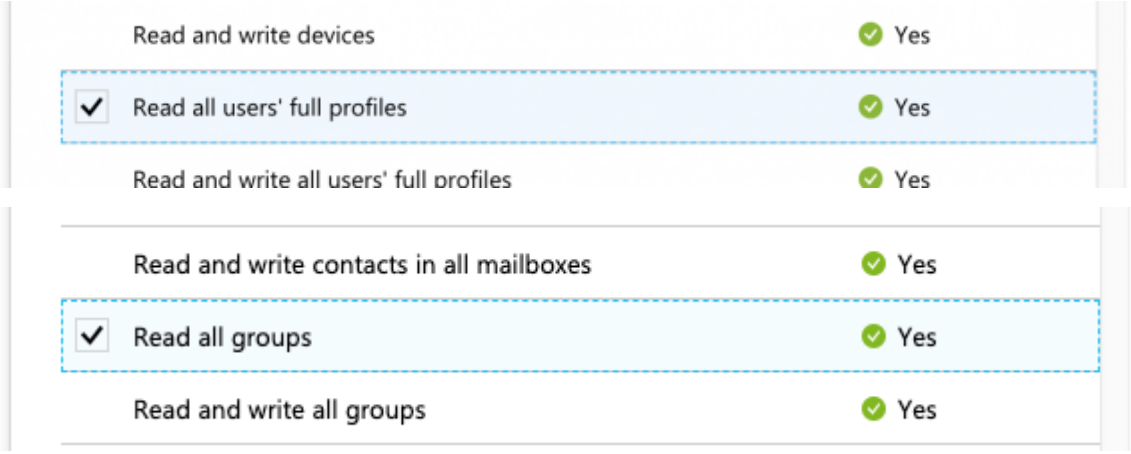
- Take note of the **Application ID** shown in the top right corner:



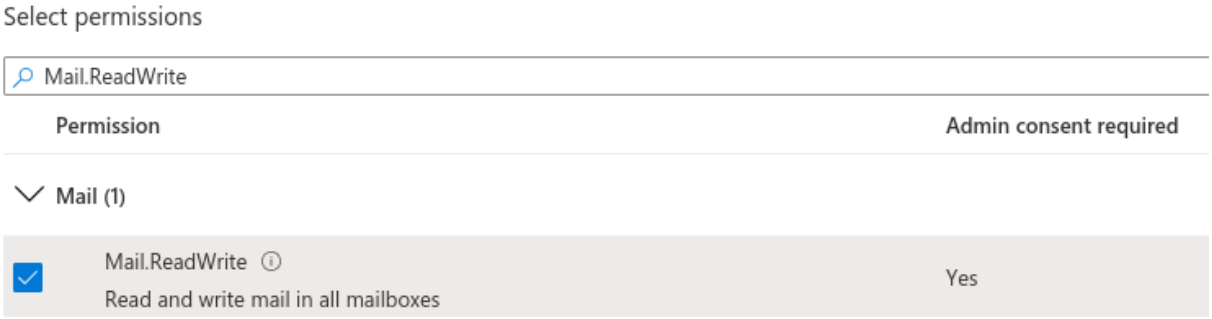
- Click **API Permissions** and in the at the top of the screen select **Add a permission**



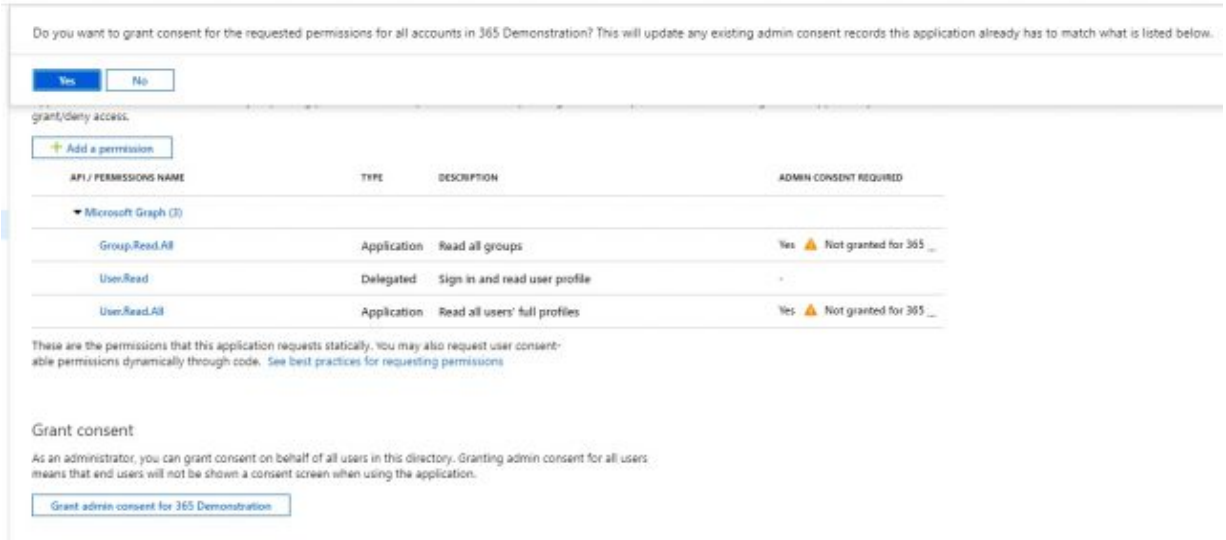
- Select **Microsoft Graph** API on the right side
- Select the **Read all users' full profiles** (search for *user.read.all*) and **Read all groups** (search for *group.read.all*) under **Application permissions**



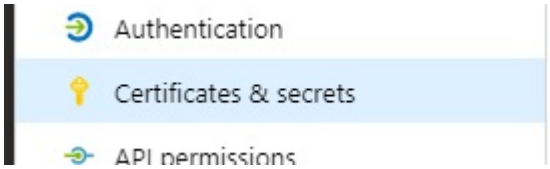
- Select **Read organizational contacts** (search for *OrgContact.Read.All*) **only** if you use Distribution Lists
- Select **Read and write mail in all mailboxes** (search for *Mail.ReadWrite*) **only** if you want to use the Threat Remediation



- Click **Add Permissions** at the bottom of the page
- Click **Grant admin consent for Your Company** and click **Yes** in the dialog



- Now select **Certificates and Secrets:**



- Add a new **Client Secret,** choose a description, choose **a date** from the **Expiry options** dropdown list
  With the latest update of Microsoft security policies it is no longer possible to generate a perpetual certificate.

- Click **Add**
- Now copy the newly generated **key value** you will need this for the next step.

×**WARNING**: Be advised that you won't be able to retrieve the **key value** at a later stage!

×**NOTE**: If you get error "Authorization_RequestDenied: Insufficient privileges to complete the operation", make sure you created all permission, and that permission type is "Application" (not "Delegate", or other). Also remember that permission propagation will take some time on Microsoft server