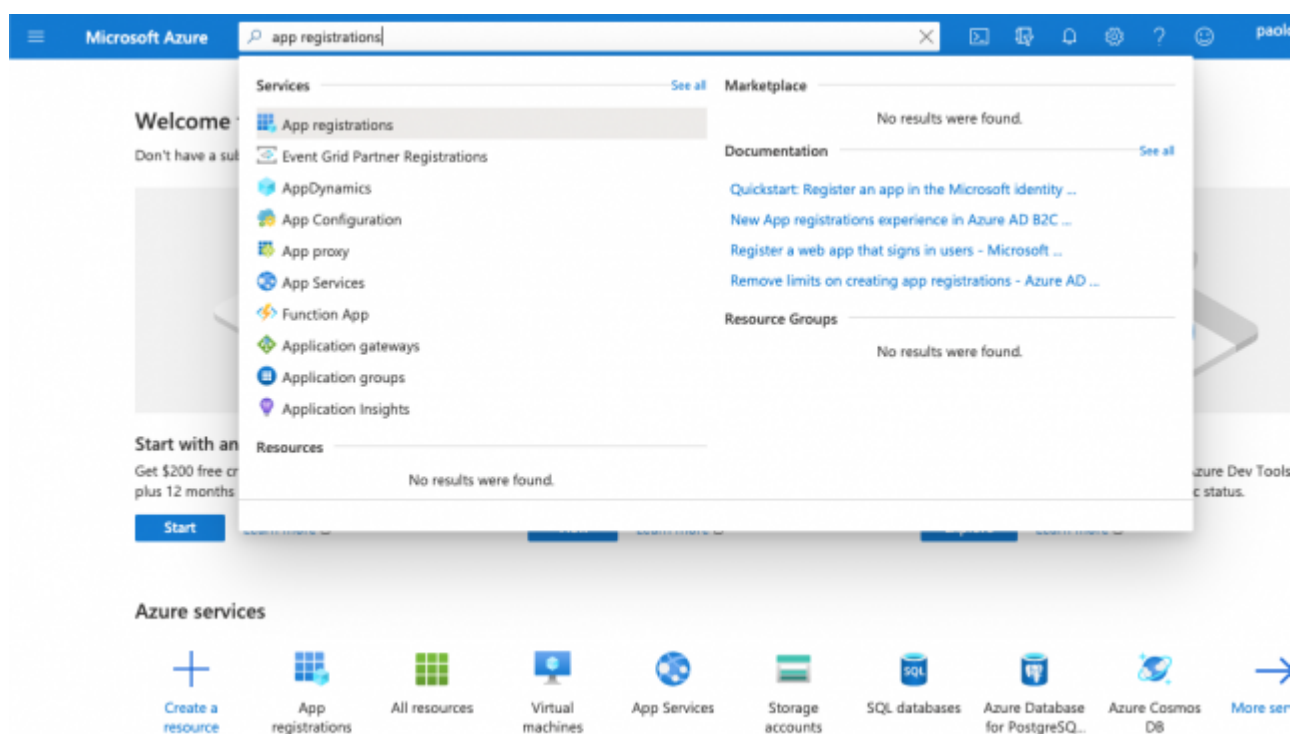


Microsoft Azure AD Libraesva App registration

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.

Home > App registrations >

Register an application

* Name

The user-facing display name for this application (this can be changed later).

LibraesvaESG ✓

Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (365 Demonstration only - Single tenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web ✓

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

Application ID: 21f970b2-3a03-4a71-a711-f439519597b1

Display name	: Archiver	Supported account types	: My organization only
Application (client) ID	: 21f970b2-3a03-4a71-a711-f439519597b1	Redirect URIs	: 1 web, 0 public client
Directory (tenant) ID	: 2c628118-cd58-4659-b317-a0dd31a82837	Managed application in ...	: Archiver
Object ID	: a3b61bd0-e632-49d5-979a-7023ac09490f		

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

Archiver - API permissions

API permissions

Applications are authorized to use APIs by requesting permissions. These permissions show up during the consent process where users are given the opportunity to grant/deny access.

[+ Add a permission](#)

API / PERMISSIONS NAME	TYPE	DESCRIPTION	ADMIN CONSENT REQUIRED
▼ Microsoft Graph (1)			
User.Read	Delegated	Sign in and read user profile	-

These are the permissions that this application requests statically. You may also request user consentable permissions dynamically through code. See [best practices for requesting permissions](#)

- 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**

Read and write devices	✓ Yes
<input checked="" type="checkbox"/> Read all users' full profiles	✓ Yes
Read and write all users' full profiles	✓ Yes
Read and write contacts in all mailboxes	✓ Yes
<input checked="" type="checkbox"/> Read all groups	✓ Yes
Read and write all groups	✓ Yes

- 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

Select permissions

Permission	Admin consent required
<input checked="" type="checkbox"/> Mail (1) <input checked="" type="checkbox"/> Mail.ReadWrite ⓘ Read and write mail in all mailboxes	Yes

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

Do you want to grant consent for the requested permissions for all accounts in 365 Demonstration? This will update any existing admin consent records this application already has to match what is listed below.

grant/deny access.

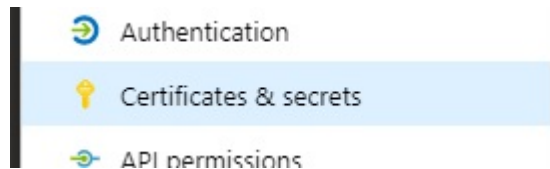
API / PERMISSIONS NAME	TYPE	DESCRIPTION	ADMIN CONSENT REQUIRED
Microsoft Graph (3)			
Group.Read.All	Application	Read all groups	Yes ⚠ Not granted for 365 ...
User.Read	Delegated	Sign in and read user profile	-
User.Read.All	Application	Read all users' full profiles	Yes ⚠ Not granted for 365 ...

These are the permissions that this application requests statically. You may also request user consent-able permissions dynamically through code. See [best practices for requesting permissions](#)

Grant consent

As an administrator, you can grant consent on behalf of all users in this directory. Granting admin consent for all users means that end users will not be shown a consent screen when using the application.

- 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