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/)
- $\circ\,$ Open the $App\,\,registrations\,$ portal as shown:

Microsoft Azure	₽ app registratio	ns				×	2.	Ð	Ф.	۲	?	🙂 🕫	ok
	Services			See all	Marketplace								
Welcome ·	🔣 App registrati	ons				No results w	ere fou	ind.					
Don't have a sub	Event Grid Pa	rtner Registrations			Documentation					Se	e al		
	🮯 AppDynamics	1			Quickstart: Registe	r an app in the M	licroso	ft identit	у				
	App Configur	ation			New App registrati	ions experience in	n Azun	AD B2C					
	App proxy				Register a web app	o that signs in use	ers - M	icrosoft .	-			1	
	App Services				Remove limits on o	creating app regis	tration	ns - Azure	e AD				
-	Function App				Resource Groups								
	Application g	ateways				No results w	ere fou	ind.					
	Application g	roups											
	Application Ir	nsights											
Start with an	Resources												
Get \$200 free cr plus 12 months		No results we	re found.									zure Dev To c status.	ols
Start			_		_	_					_		
Azure servic	es												
+	Ш,			۲		sqL		Ŧ		8	0	_)
Create a resource	App registrations	All resources	Virtual machines	App Services	Storage accounts	SQL databases	Az for	ure Datal r Postgre	base SQ	Azure (Cosmo DB	as More s	ier

- 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

LibraesvaESG		پ ۲
Supported accou	int types	
Who can use this ap	plication or acces	s this API?
Accounts in this	organizational di	ectory only (365 Demonstration only - Single tenant)
Accounts in any	organizational di	rectory (Any Azure AD directory - Multitenant)
Accounts in any	organizational di	rectory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
Help me choose		
Redirect URI (op	ional)	
We'll return the auth changed later, but a	entication respon value is required f	se to this URI after successfully authenticating the user. Providing this now is optional and it can be or most authentication scenarios.
and a	~	https:///OLIB-ESG.DOMAIN.COM/oauth-login

 \circ Take note of the Application ID shown in the top right corner:

🗊 Delete 🌐	Endpoints	
Display name	: Archiver Copy to clipbe	ard Supported account types : My organization only
Application (clien	t) 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	
		A

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

Overview	« API permissions			
4 Quickstart	Applications are authorized to use APIs by re grant/deny access.	questing permissions. These pe	missions show up during the consent process w	here users are given the opportunity to
Aanage	+ Add a permission			
Branding	API / PERMISSIONS NAME	1995	DESCRIPTION	ADMIN CONSENT REQUIRED
3 Authentication	Threeworth Grands (1)			
Certificates & secrets				
API permissions	UterRead	Delegated	Sign in and read user profile	2
Expose an API	These are the permissions that this application able permissions dynamically through code.	on requests statically. You may a See best practices for requestir	lso request user consent-	
Cowners				
Manifest				

- $\circ\,$ 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	0	Yes
~	Read all users' full profiles	0	Yes
	Read and write all users' full profiles	Ø	Yes
	Read and write contacts in all mailboxes	ø	Yes
✓	Read and write contacts in all mailboxes Read all groups	0	Yes 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	
🔎 Ma	ail.ReadWrite	
P	ermission	Admin consent required
\vee M	1ail (1)	
~	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

ent vianu arrado				
the data as a second second				
API / PERMISSIONS NAME	TYPE	DESCRIPTION	ADMIN CONSENT REQUIRED	
• Microsoft Graph (3)				
Group.Read.All	Application	Read all groups	Yes 🔺 Not granted for 365	
UserRead	Delegated	Sign in and read user profile		
User.Read.All	Application	Read all users' full profiles	Yes 🛕 Not granted for 365	
ese are the permissions that this application e permissions dynamically through code. 1	n requests statically, You may a See best practices for requestin	lio request user consent- g permissions		
ant consent				

• 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.

$\circ~$ Click \boldsymbol{Add}

 $\circ\,$ 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