



Integrate Azure Active Directory (Entra ID) Employees with VPass





Azure Active Directory (Entra ID) Application Setup







- **1**. Log in to your Microsoft Azure account using valid credentials.
- 2. Search for a *Microsoft Entra ID* in the search box.



3. Click on the *Microsoft Entra ID* displayed below the search box



4. Select App registration.

PART A - (Page 2)

Azure Active Directory (Entra ID) Application Setup (CONTINUED)







5. Click on *New Registration*.



7. Select a platform from drop down list and enter the URL of the application. This varies according to location.

AU/NZ:

https://dashboard.vpass.io/session/signin.

UK, EU, Africa: https://dashboard-uk.vpass.io/session/signin.

Canada: https://dashboard-ca.vpass.io/session/signin.

US, Rest of World: https://dashboard-us.vpass.io/session/signin.

6. Select the Name VPass.



Accounts in this organizational directory only (Default Directory only - Single tenant)

- Accounts in any organizational directory (Any Microsoft Entra ID tenant Multitenant)
- Accounts in any organizational directory (Any Microsoft Entra ID tenant Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

O Personal Microsoft accounts only

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
 https://dathboard.vpass.io/session/signin

 Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from Enterprise application



8. Click on the *Register* button.

PART A - (Page 3)

Azure Active Directory (Entra ID) Application Setup (CONTINUED)







9. Select Expose an API.





R 🖓 🚳

11. Click on the Save button

12. Select *Certificates & Secrets*.

10. Click on Add.

ure 🔎 Se

PART A - (Page 4)

Azure Active Directory (Entra ID) Application Setup (CONTINUED)



Microsoft Azure	$\mathcal P$ Search resources, services, and docs (G+/)			E		P 6			
Home > Default Directory	App registrations > VPass								
🔶 VPass Certi	ficates & secrets 🖉 …								
,₽ Search	« 🔗 Got feedback?								
Overview									
4 Quickstart	Credentials enable confidential applic scheme). For a higher level of assuran	Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTP) scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.							
💉 Integration assistant									
Manage	Application registration certificate	Annipation revisitation certificates servers							
Branding & properties									
Authentication	Certificates (0) Client secret) ederated credentia	ls (0)						
📍 Certificates & secrets		A construction that the construction							
Token configuration	A secret soring that the application	we its identity whe	in requesting a token. Also can be	referred to as ap	pricatio	n password.			
 API permissions 	+ New client secret								
 Expose an API 	Description	Expires	Value 💿		Se	cret ID			
App roles	No cliant secrets have been created	No client carretic hove been created for this annication							
A Owners		the out approximation							
A Roles and administrators									

	Add a client secret	×
	Description	VPass Employee Sync
	Expires	Recommended: 180 days (6 months)
fential applications to identify themselves to the authenticatio el of assurance, we recommend using a certificate (instead of	14	$\mathbf{\Lambda}$
tion certificates, secrets and federated credentials can be found in		Ē
ent secrets (0) Federated credentials (0)		
application uses to prove its identity when requesting a token	16	
Expires Value 🛈		
een created for this application.		
	Add Cancel	

13. Click on *New Client Secret.*

14. Enter a description for this *Client Secret*, (example "VPass Employee Sync") **15**. *Select Expiry* from drop down list and **16**. click on the *Add* button.



17. Copy the value and save it somewhere safe. We will need to use this value in the VPass admin (Step 37).



18. Select API Permissions.

PART A - (Page 5)

Azure Active Directory (Entra ID) Application Setup (CONTINUED)







19. Click on *Add a permission*.

20. Click on *Microsoft Graph*.



21. Click on the Application Permissions.



22. Enter *User* in search box and scroll down the drop down menu.

PART A - (Page 6)

Azure Active Directory (Entra ID) Application Setup (CONTINUED)







24. Select checkbox and **25**... click on *Add Permission* button.

23. Click on User.



26. Check *Grant admin consent for Default Directory* and **27** click on Yes.



Select Overview from the side menu... and copy:**28** Application Client ID**29**. Directory Tenant ID**30**. Application ID URI...

PART A - (Page 7)

Azure Active Directory (Entra ID) Application Setup (CONTINUED)

