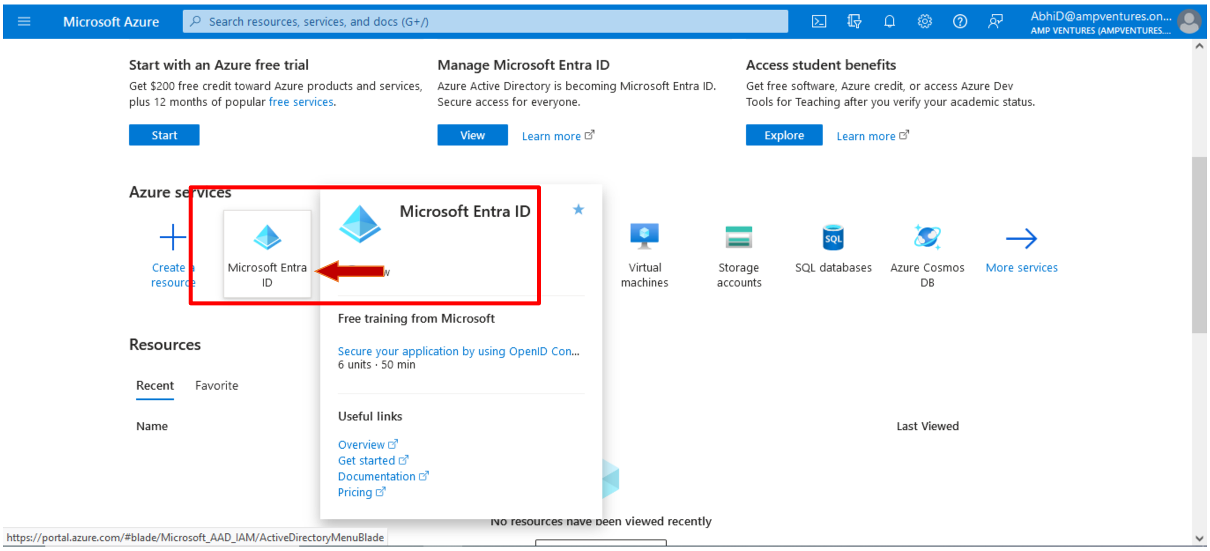
Registering the Microsoft Graph App on the Microsoft Azure Portal

1. Go to the Microsoft Azure portal at https://portal.azure.com/ and sign in with your Microsoft Azure account.

2. Under **Azure services,** select **Microsoft Entra ID**.



Start with an Azure free trial

Get $200 free credit toward Azure products and services, plus 12 months of popular free services.

Manage Microsoft Entra ID

Azure Active Directory is becoming Microsoft Entra ID. Secure access for everyone.

Access student benefits

Get free software, Azure credit, or access Azure Dev Tools for Teaching after you verify your academic status.

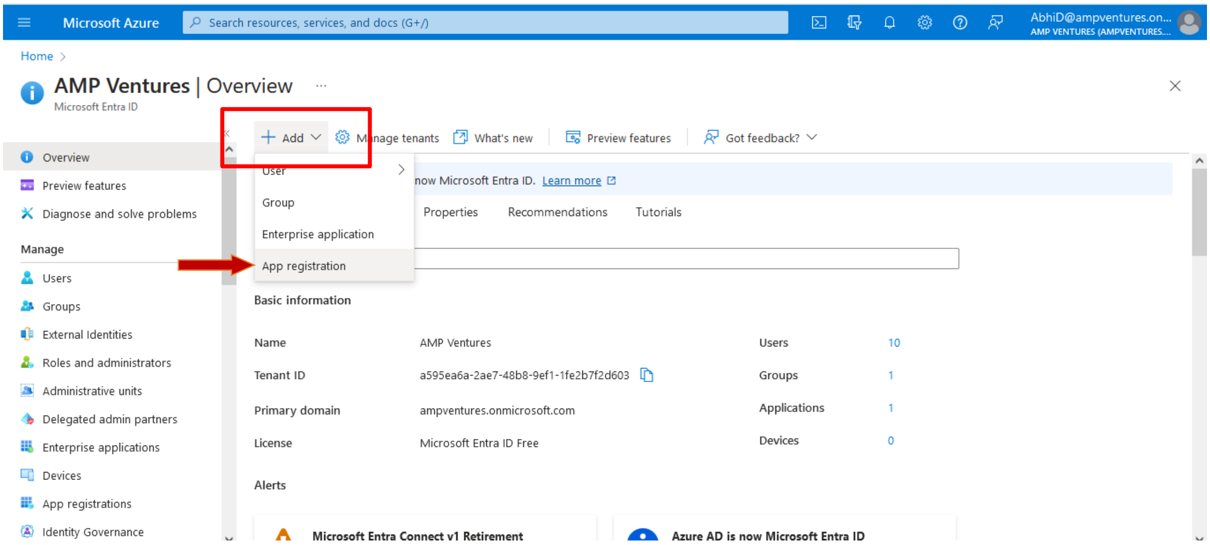
Free training from Microsoft

Secure your application by using OpenID Con...
6 units · 50 min

No resources have been viewed recently

https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade

3. Once the page opens hover on **Add** and click on **App registration** from drop down menu.



AMP Ventures | Overview

Microsoft Entra ID

...now Microsoft Entra ID. Learn more

Basic information

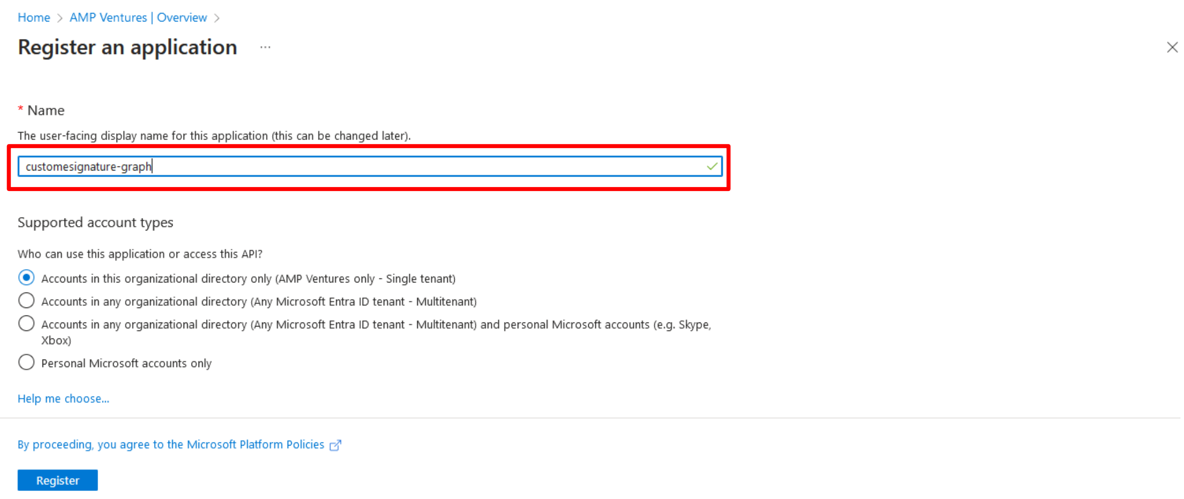
Name	AMP Ventures	Users	10
Tenant ID	a595ea6a-2ae7-48b8-9ef1-1fe2b7f2d603	Groups	1
Primary domain	ampventures.onmicrosoft.com	Applications	1
License	Microsoft Entra ID Free	Devices	0

Alerts

Microsoft Entra Connect v1 Retirement

Azure AD is now Microsoft Entra ID

4. On **Register an application** page enter **Name** of your application (for example **customesignature-graph**)



Home > AMP Ventures | Overview >

Register an application ...

* Name

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

customesignature-graph

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (AMP Ventures only - Single tenant)

○ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)

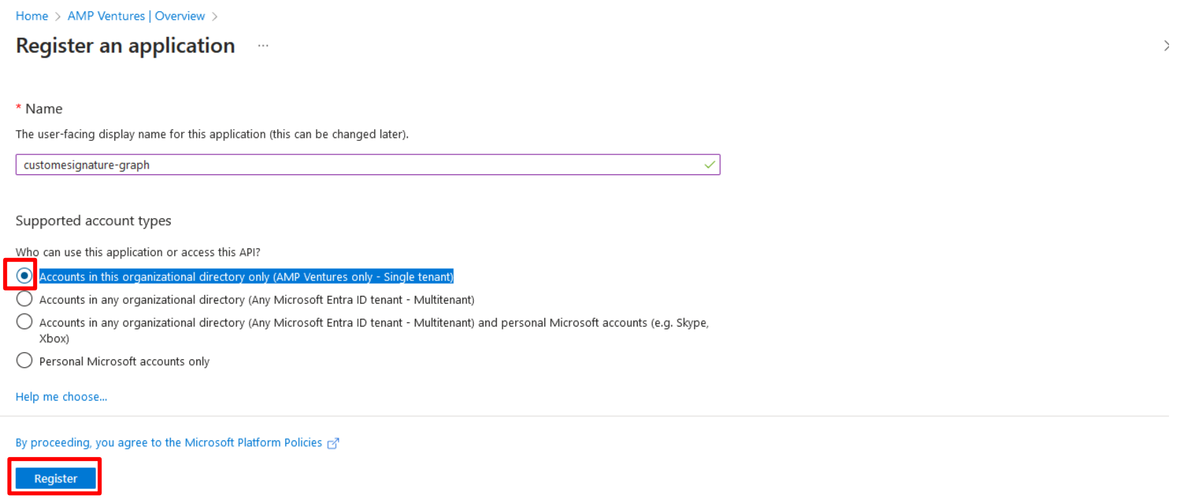
○ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

○ Personal Microsoft accounts only

Help me choose...

By proceeding, you agree to the Microsoft Platform Policies

5. Select Accounts in this organizational directory only (**AMP Ventures only - Single tenant**) option radio button.
   By choosing **Supported account types**, specify who can use the application (sometimes called its *sign-in audience*.). Select the option **Accounts in this organizational directory only**.



Home > AMP Ventures | Overview >

Register an application ...

* Name

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

customesignature-graph

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (AMP Ventures 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)

○ Personal Microsoft accounts only

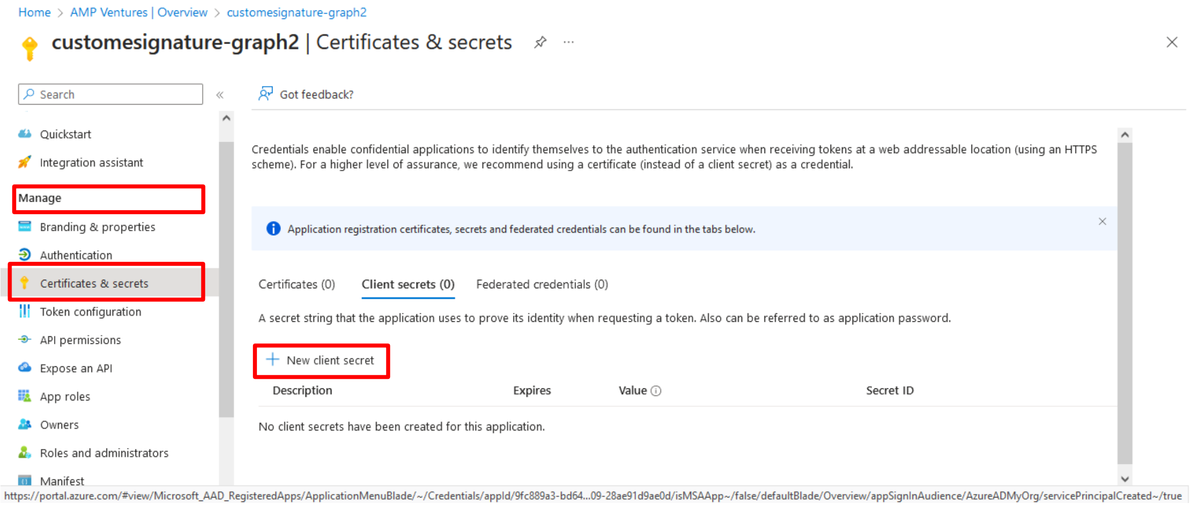
Help me choose...

By proceeding, you agree to the Microsoft Platform Policies

6. Once all above is done, click on **Register**.

7. After redirect Under **Manage** on the left side menu, select **Certificates & secrets**.

8. On the **Certificates & secrets** page that opens, select **Client secrets,** and click **New client secret**.



Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

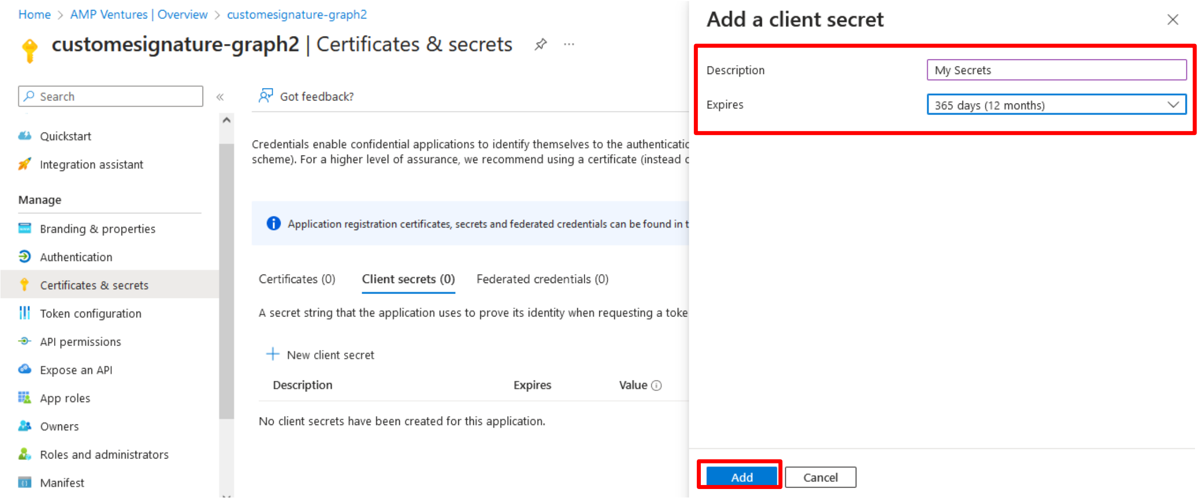
Application registration certificates, secrets and federated credentials can be found in the tabs below.

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

No client secrets have been created for this application.

https://portal.azure.com/#view/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/~/Credentials/appId/9fc889a3-bd64...09-28ae91d9ae0d/isMSAApp~/false/defaultBlade/Overview/appSignInAudience/AzureADMyOrg/servicePrincipalCreated~/true

9. In the dialog that appears, provide a **Description** for the new secret, select the period after which the secret expires, and then click **Add**.



Credentials enable confidential applications to identify themselves to the authenticatic scheme). For a higher level of assurance, we recommend using a certificate (instead c

Application registration certificates, secrets and federated credentials can be found in t

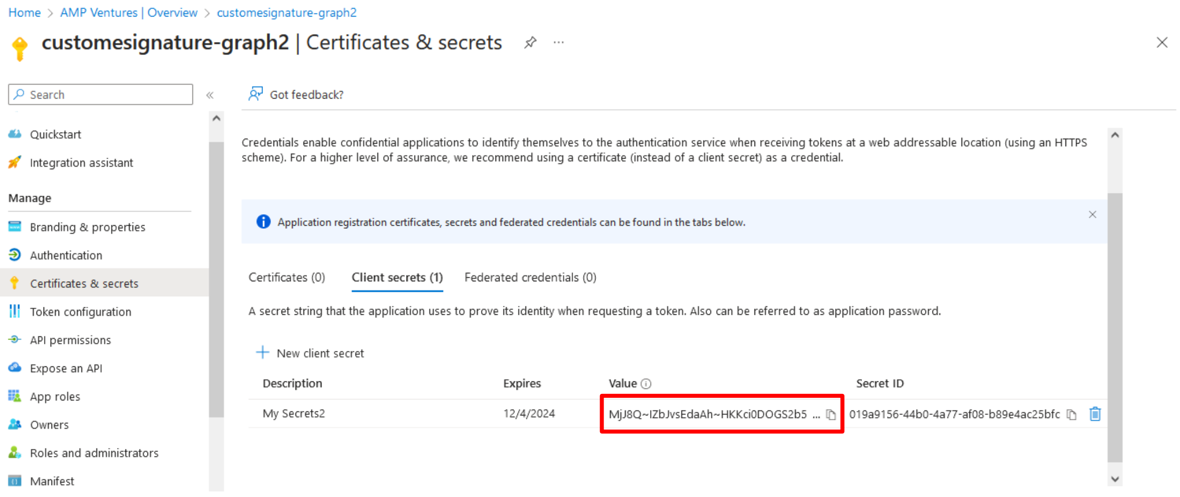
A secret string that the application uses to prove its identity when requesting a toke

No client secrets have been created for this application.

Description: My Secrets

Expires: 365 days (12 months)

10. **Copy the secret value** and **make sure to save it somewhere** to access it later because the secret will not be accessible after you proceed from here.



Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

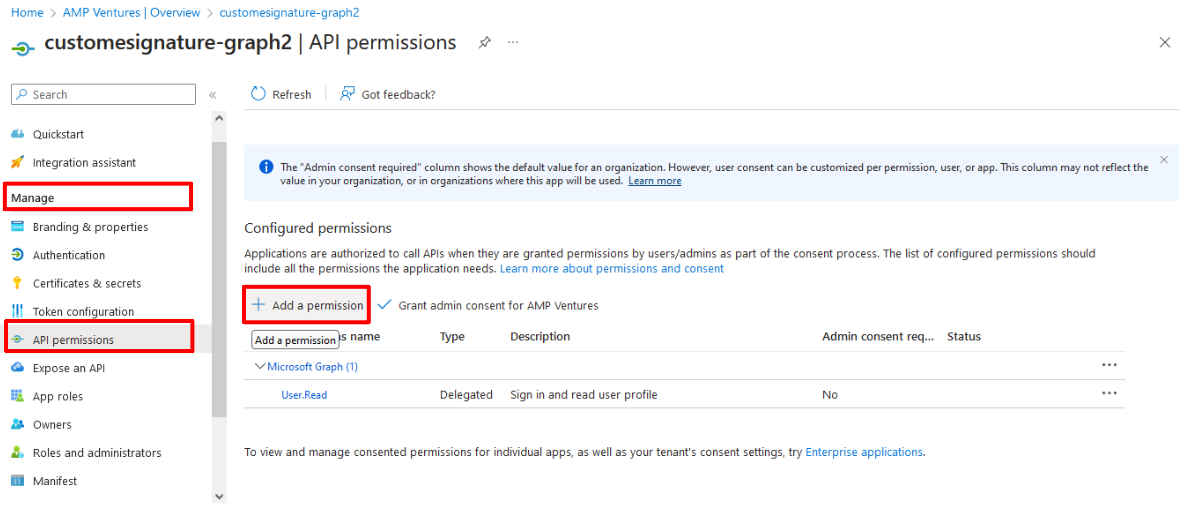
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	Secret ID
My Secrets2	12/4/2024	MjJ8Q~IZbJvsEdaAh~HKKci0DOGS2b5 ...	019a9156-44b0-4a77-af08-b89e4ac25bfc

Note: Copy the secret value on that step because it will not be accessible after you proceed from here.

11. Under **Manage,** on the left side menu, select **API permissions**.

12. On the **API permissions** page that opens, click **Add permission**.



The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. Learn more

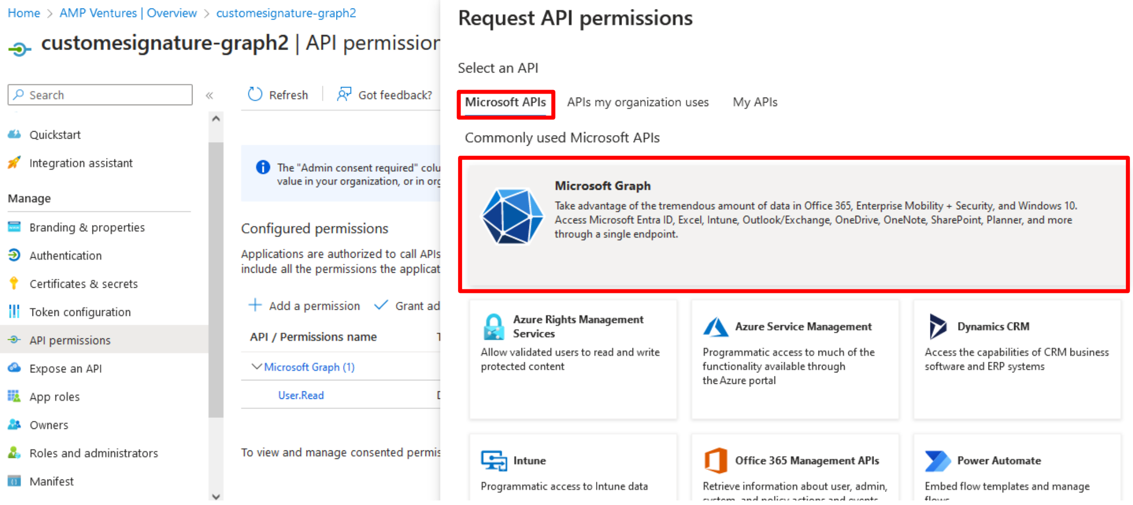
Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	No	

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try Enterprise applications.

13. On the **Request API permissions** window that appears, double click **Microsoft Graph**.



The "Admin consent required" colu value in your organization, or in org

Configured permissions

Applications are authorized to call APIs include all the permissions the applicat

To view and manage consented permis

Microsoft Graph: Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Microsoft Entra ID, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Azure Rights Management Services: Allow validated users to read and write protected content

Azure Service Management: Programmatic access to much of the functionality available through the Azure portal

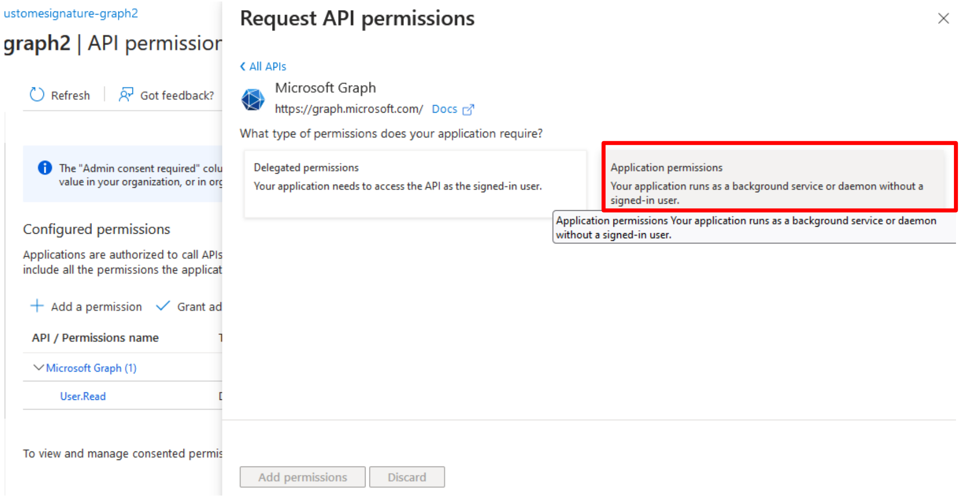
Dynamics CRM: Access the capabilities of CRM business software and ERP systems

Intune: Programmatic access to Intune data

Office 365 Management APIs: Retrieve information about user, admin,

Power Automate: Embed flow templates and manage

14. Select **Application Permissions.**



The "Admin consent required" colu value in your organization, or in org

Configured permissions

Applications are authorized to call APIs include all the permissions the applicat

To view and manage consented permis

What type of permissions does your application require?

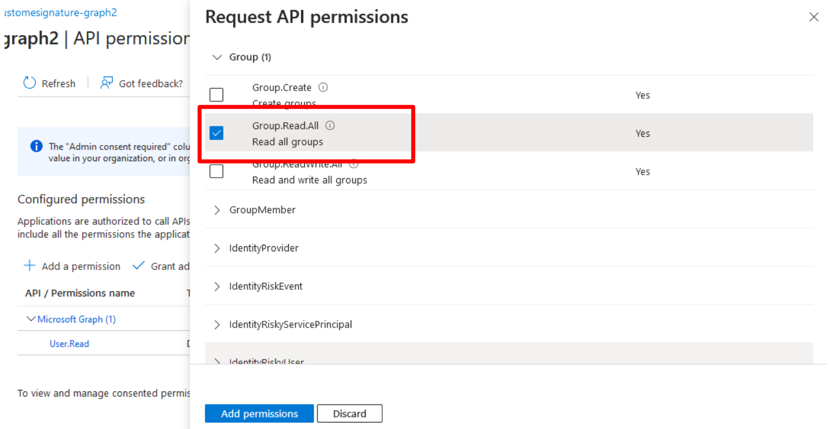
Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Application permissions Your application runs as a background service or daemon without a signed-in user.

15. Then, the **Permission tree** appears below:

- Expand the **Group** node and select **Group.Read.All**



The "Admin consent required" colu value in your organization, or in org

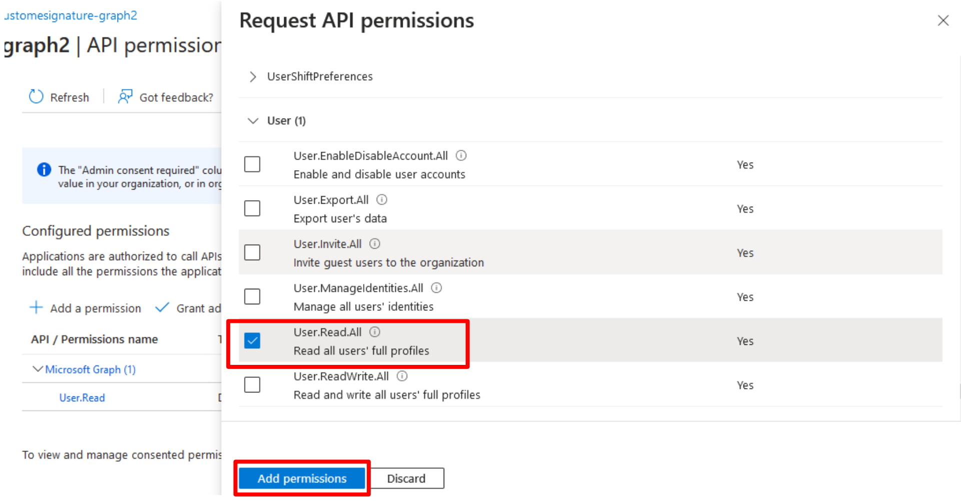
Configured permissions

Applications are authorized to call APIs include all the permissions the applicat

To view and manage consented permis

□	Group.Create Create groups	Yes
☑	Group.Read.All Read all groups	Yes
□	Group.ReadWrite.All Read and write all groups	Yes

- Expand the **User** node and select **User.Read.All**



ustomesignature-graph2

graph2 | API permission

Refresh | Got feedback?

The "Admin consent required" colu value in your organization, or in org

Configured permissions

Applications are authorized to call APIs include all the permissions the applicat

+ Add a permission ✓ Grant ad

API / Permissions name

Microsoft Graph (1)

User.Read

To view and manage consented permis

Request API permissions

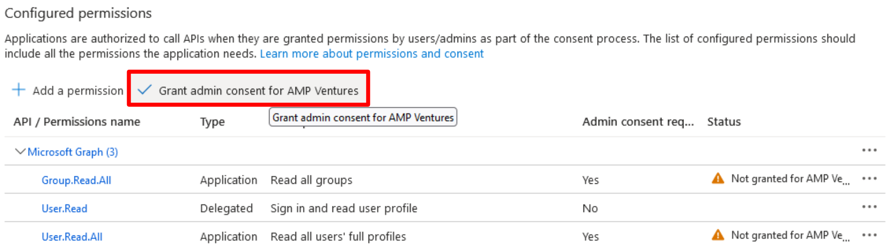
> UserShiftPreferences

User (1)

	Permission	Admin consent required
□	User.EnableDisableAccount.All Enable and disable user accounts	Yes
□	User.Export.All Export user's data	Yes
□	User.Invite.All Invite guest users to the organization	Yes
□	User.ManageIdentities.All Manage all users' identities	Yes
☑	User.Read.All Read all users' full profiles	Yes
□	User.ReadWrite.All Read and write all users' full profiles	Yes

- Click **Add permissions** to confirm the selection.

16. On the **API permissions** page that opens, do the following steps:



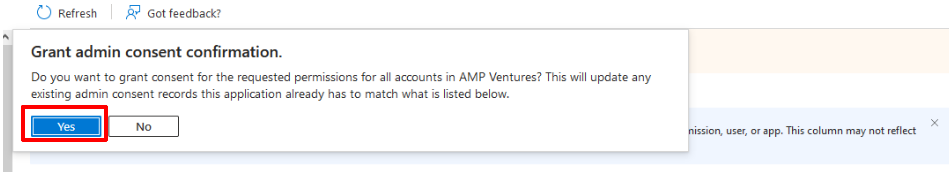
Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

+ Add a permission
✓ Grant admin consent for AMP Ventures
Grant admin consent for AMP Ventures

API / Permissions name	Type		Admin consent req...	Status
Microsoft Graph (3)				
Group.Read.All	Application	Read all groups	Yes	⚠ Not granted for AMP Ve...
User.Read	Delegated	Sign in and read user profile	No	
User.Read.All	Application	Read all users' full profiles	Yes	⚠ Not granted for AMP Ve...

17. Select **Grant admin consent for <Organization>**, read the confirmation dialog that opens, and then click **Yes**.

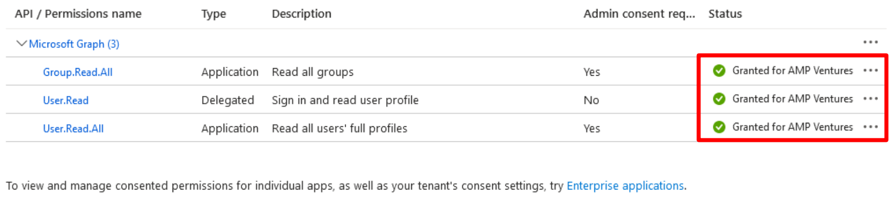


Grant admin consent confirmation.

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

nission, user, or app. This column may not reflect

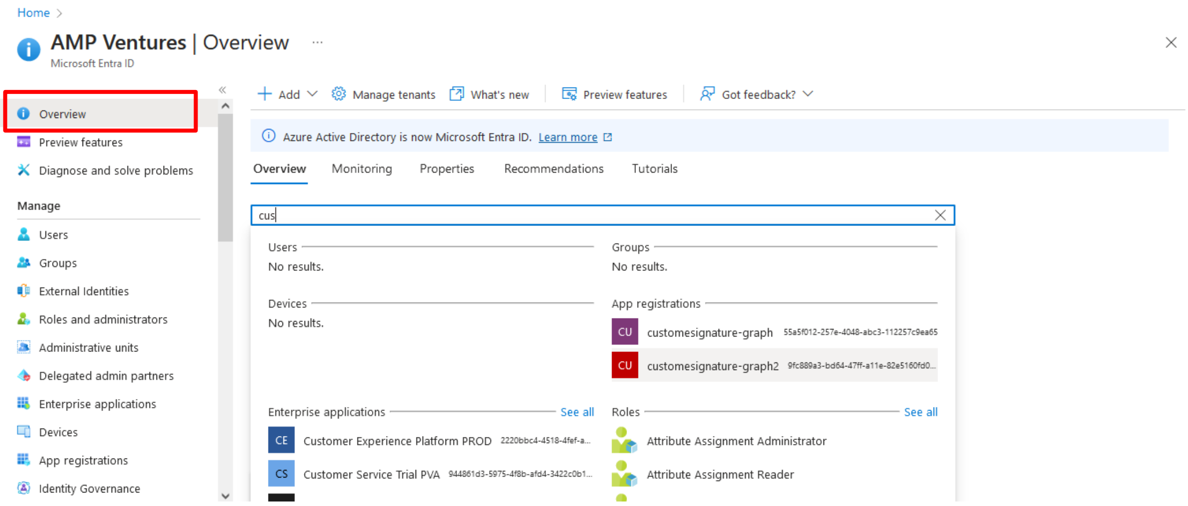
- The **Status** value should now be **Granted for <Organization>**



API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (3)				···
Group.Read.All	Application	Read all groups	Yes	Granted for AMP Ventures ···
User.Read	Delegated	Sign in and read user profile	No	Granted for AMP Ventures ···
User.Read.All	Application	Read all users' full profiles	Yes	Granted for AMP Ventures ···

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try Enterprise applications.

18. Once Granted go to back to **Microsoft Entra ID** And search your newly created application



Azure Active Directory is now Microsoft Entra ID. Learn more

cus

Users
No results.

Groups
No results.

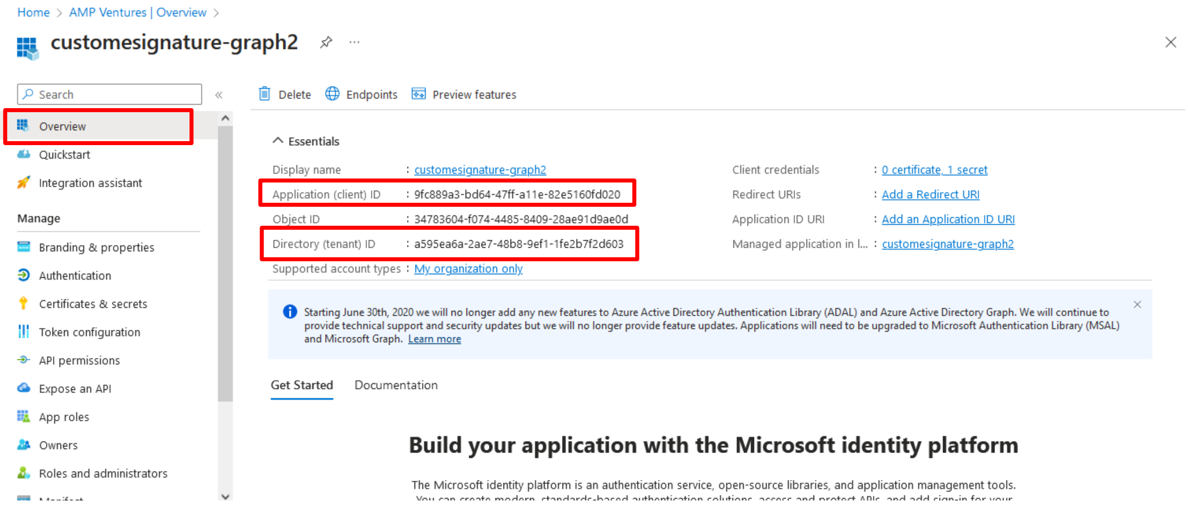
Devices
No results.

App registrations
CU customesignature-graph 55a5f012-257e-4048-abc3-112257c9ea65
CU customesignature-graph2 9fc889a3-bd64-47ff-a11e-82e5160fd0...

Enterprise applications
CE Customer Experience Platform PROD 2220bbc4-4518-4fef-a...
CS Customer Service Trial PVA 944861d3-5975-4f8b-afd4-3422c0b1...

Roles
Attribute Assignment Administrator
Attribute Assignment Reader

19. On app registration click on newly created application (**customesignature-graph**).



Display name	: customesignature-graph2	Client credentials	: 0 certificate, 1 secret
Application (client) ID	: 9fc889a3-bd64-47ff-a11e-82e5160fd020	Redirect URIs	: Add a Redirect URI
Object ID	: 34783604-f074-4485-8409-28ae91d9ae0d	Application ID URI	: Add an Application ID URI
Directory (tenant) ID	: a595ea6a-2ae7-48b8-9ef1-1fe2b7f2d603	Managed application in l...	: customesignature-graph2
Supported account types	: My organization only		

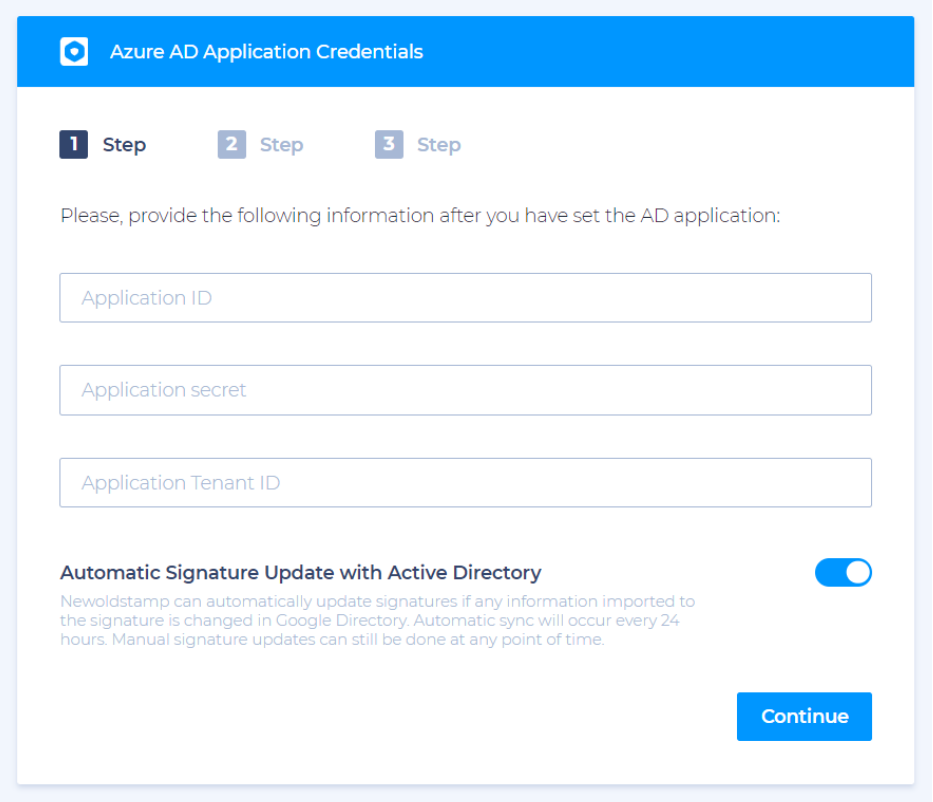
Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools.

- Copy **Application** (Client) ID:
- Copy **Client Secret** (we copied this in Step 10)
- Copy **Directory (tenant) ID**

20. Paste the above copied values and choose if you would like to turn on or off an automatic sync with Active Directory every 24 hours and click Continue:



Azure AD Application Credentials

1 Step 2 Step 3 Step

Please, provide the following information after you have set the AD application:

Automatic Signature Update with Active Directory ●

Newoldstamp can automatically update signatures if any information imported to the signature is changed in Google Directory. Automatic sync will occur every 24 hours. Manual signature updates can still be done at any point of time.

21. Done!