GRAPHUS

for Office 365

Activation Guide

Table of Contents

1. Graphus Application Activation 1
2. Required Permissions 19
3. Graphus Application Deactivation 21

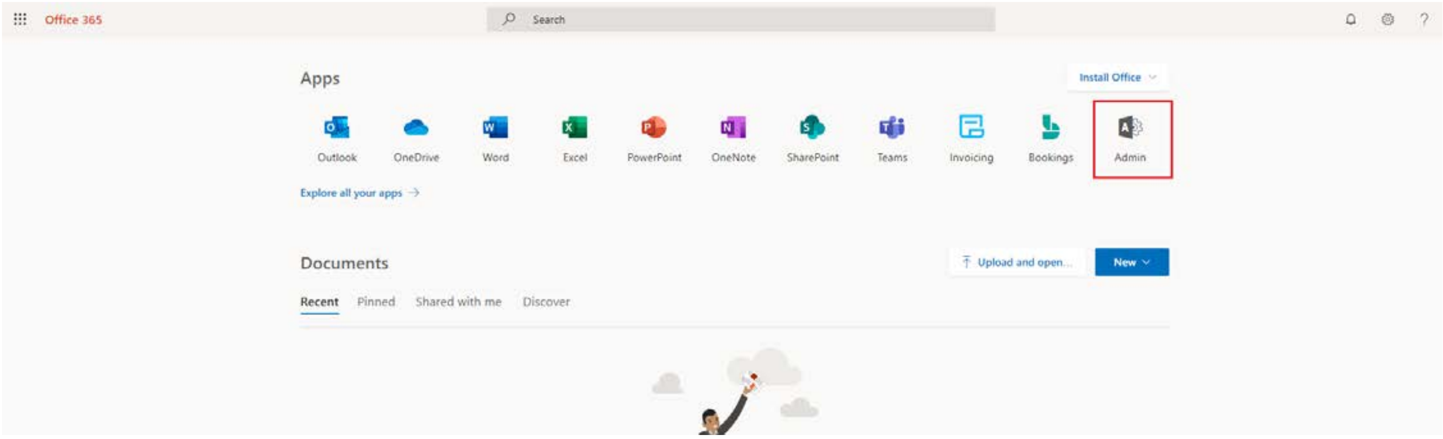
1. Graphus Application Activation

Notes

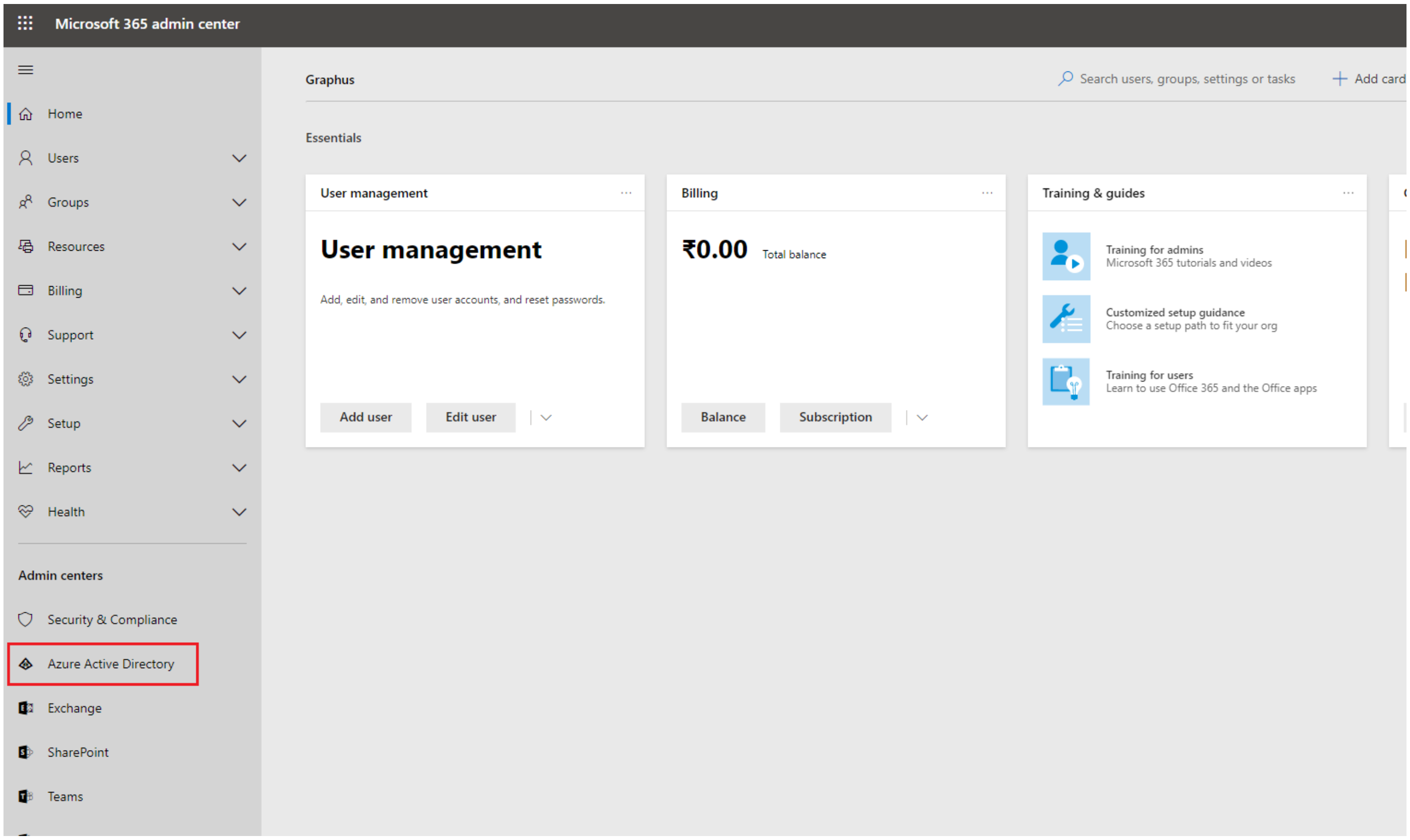
The activation process has to be carried out by the global administrator of Azure AD for your organization.

Steps

1. Login to Office 365 portal and select **Admin**.

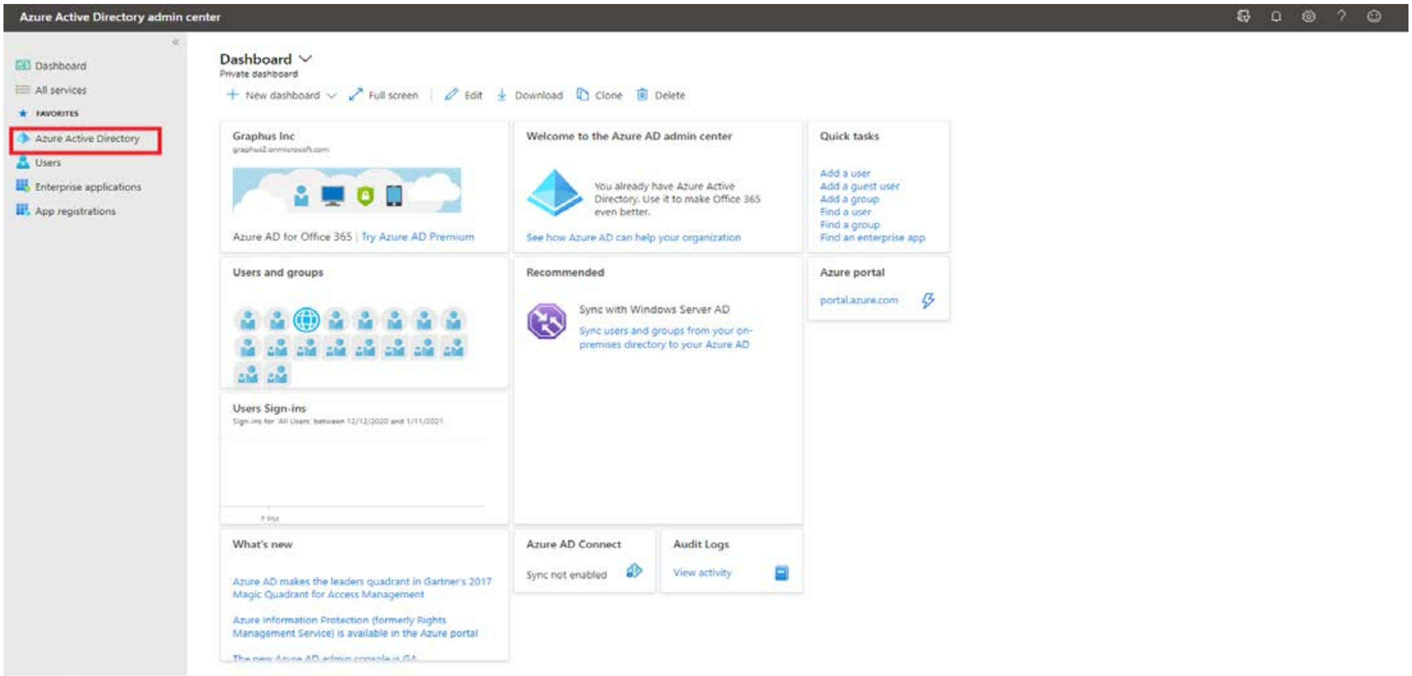


2. Under **Admin centers**, click **Azure Active Directory**.



Add, edit, and remove user accounts, and reset passwords.

3. In the **Azure Active Directory admin center**, click **Azure Active Directory**.



You already have Azure Active Directory. Use it to make Office 365 even better.

Sync users and groups from your on-premises directory to your Azure AD

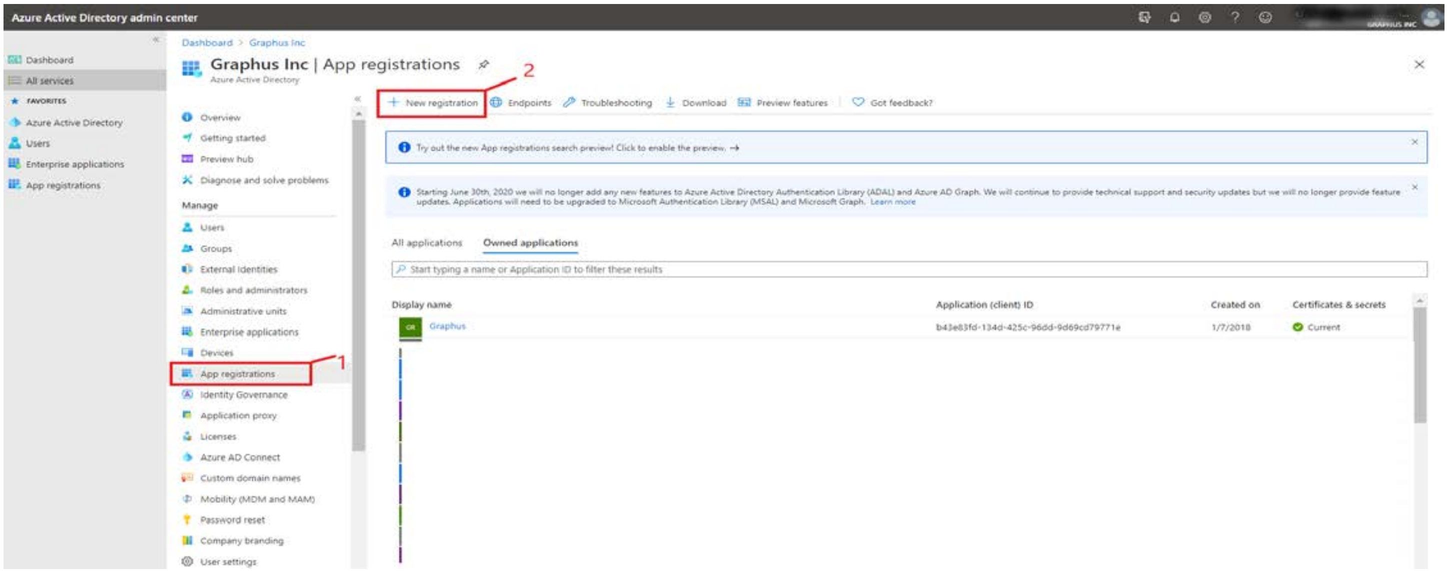
Sign-ins for 'All Users' between 12/12/2020 and 1/11/2021

Azure AD makes the leaders quadrant in Gartner's 2017 Magic Quadrant for Access Management

Azure Information Protection (formerly Rights Management Service) is available in the Azure portal

The new Azure AD admin console is GA

4. Under the **Manage** section, click **App registrations** and then choose **New registration**.

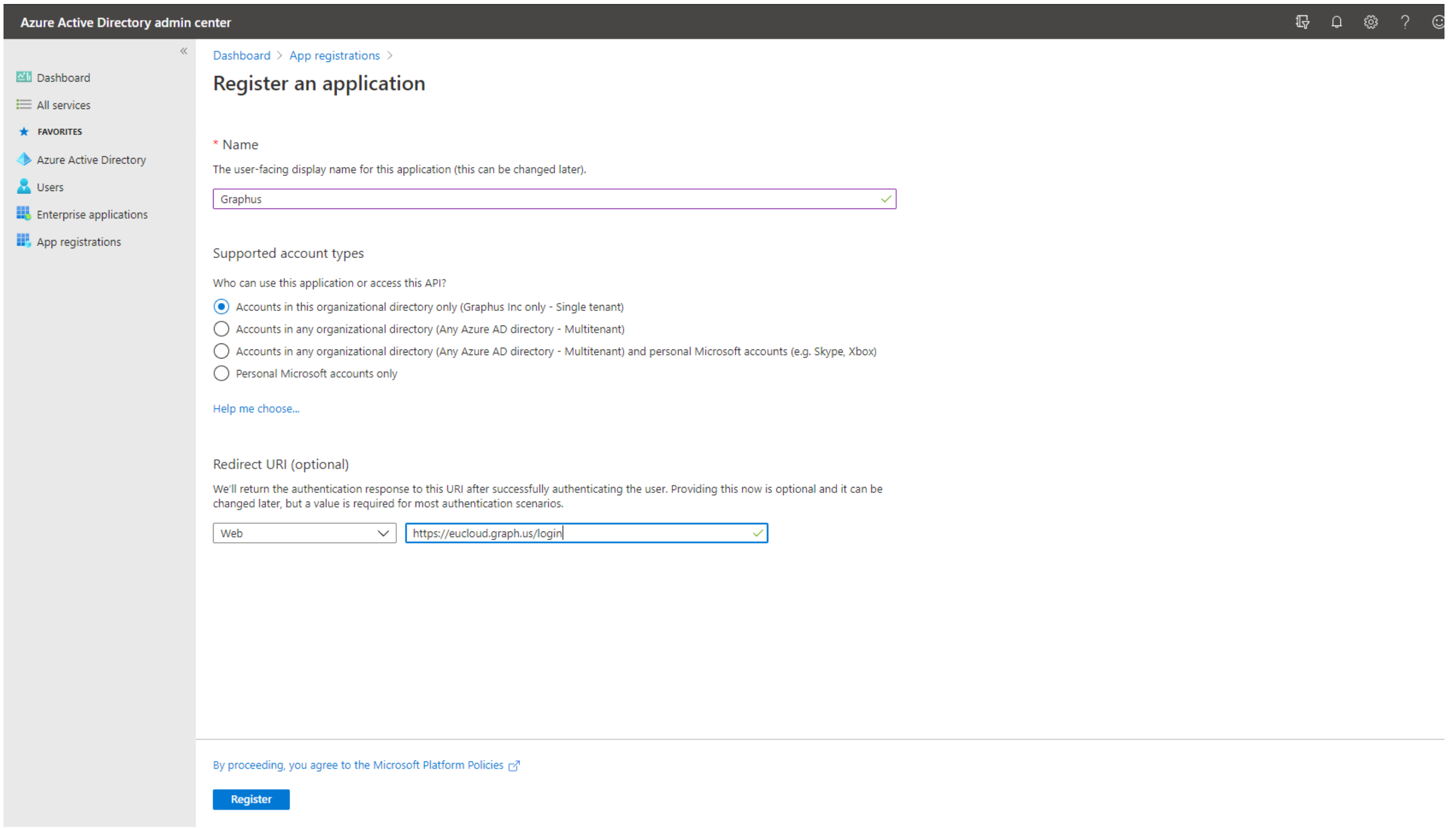


Try out the new App registrations search preview! Click to enable the preview. →

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD 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

Display name	Application (client) ID	Created on	Certificates & secrets
GR Graphus	b43e83fd-134d-425c-96dd-9d69cd79771e	1/7/2018	✓ Current

5. In the **Register an application** page, enter the name as *Graphus* and select Supported account types as **Accounts in this organizational directory only**. In the Redirect URI section, select **Web** and enter *https://eucloud.graph.us/login* as the URL. Then, click **Register**.



Register an application

* Name

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

Graphus

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (Graphus Inc 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)

○ Personal Microsoft accounts only

Help me choose...

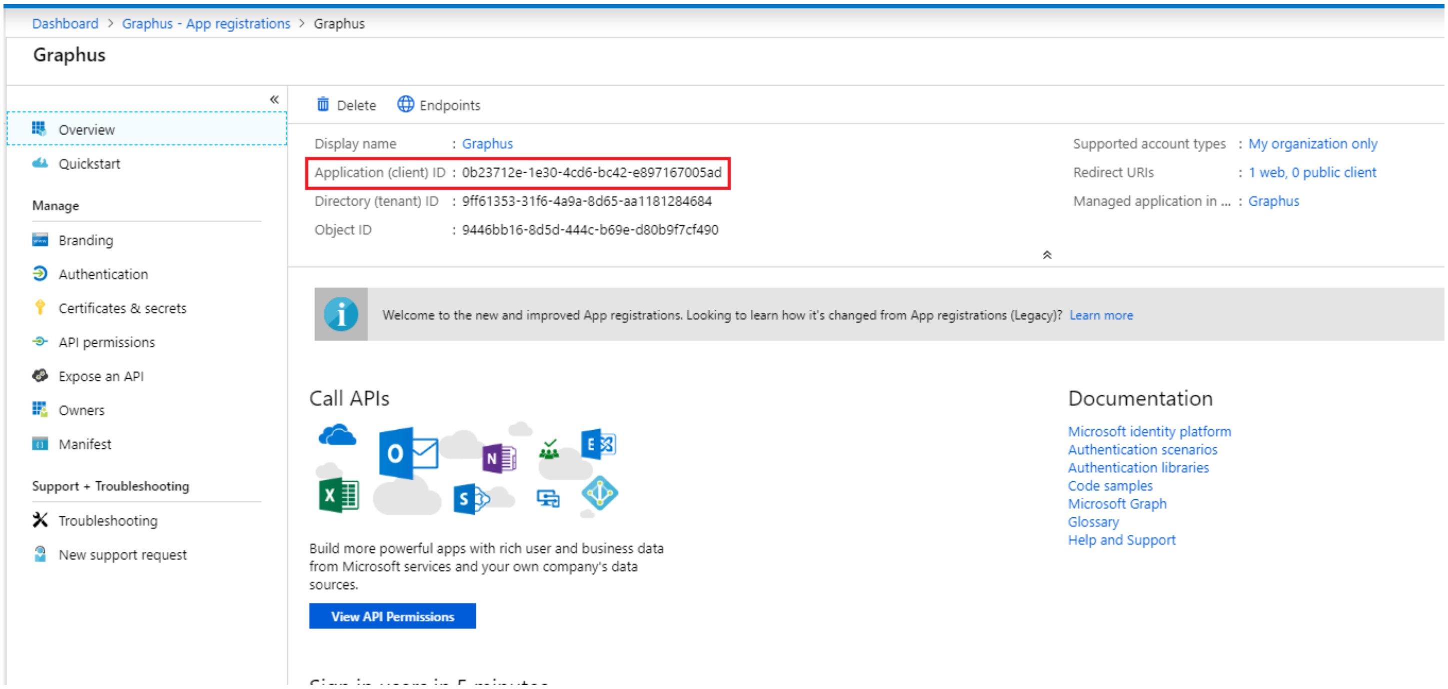
Redirect URI (optional)

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://eucloud.graph.us/login

By proceeding, you agree to the Microsoft Platform Policies

6. Copy and save the Application (client) ID. It will be used in a step later.



Dashboard > Graphus - App registrations > Graphus

Graphus

Display name : Graphus

Application (client) ID : 0b23712e-1e30-4cd6-bc42-e897167005ad

Directory (tenant) ID : 9ff61353-31f6-4a9a-8d65-aa1181284684

Object ID : 9446bb16-8d5d-444c-b69e-d80b9f7cf490

Supported account types : My organization only

Redirect URIs : 1 web, 0 public client

Managed application in ... : Graphus

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? Learn more

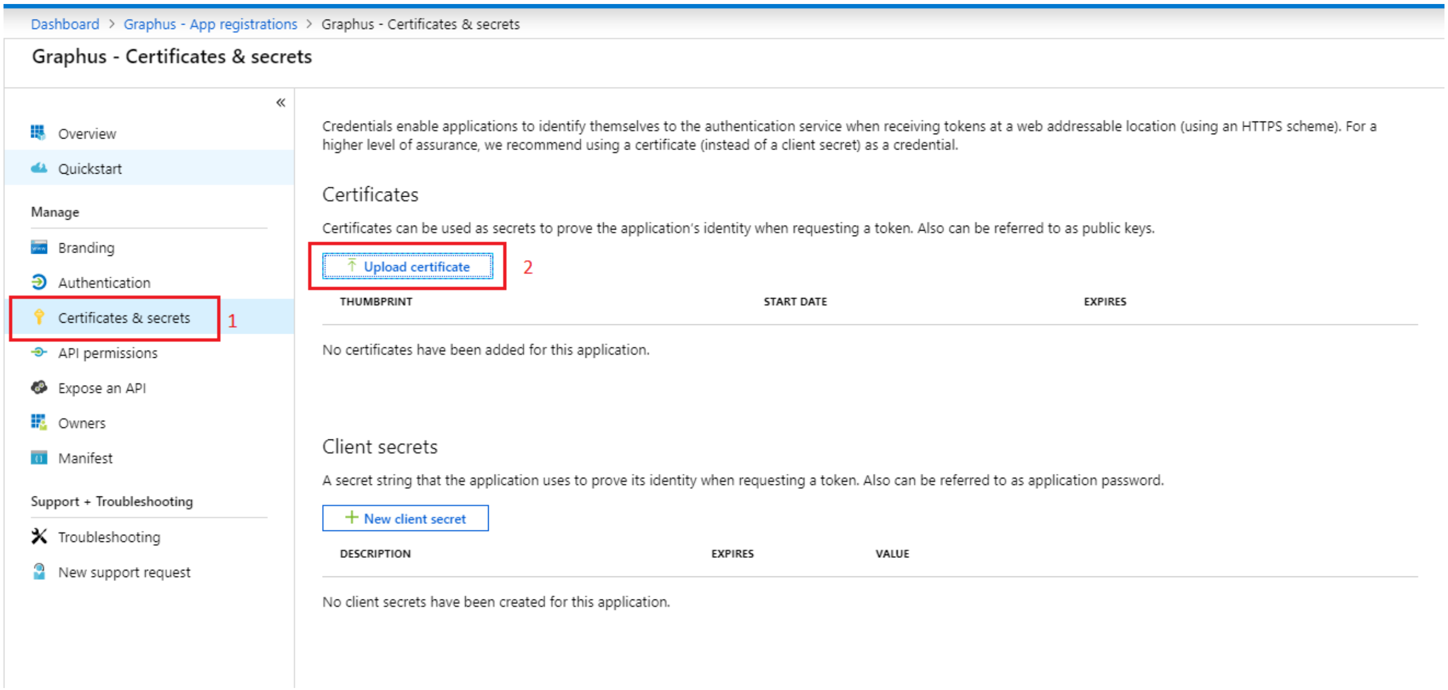
Call APIs

Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

Documentation

Sign in users in 5 minutes

7. In the Manage section, select **Certificates & secrets**. Upload the certificate file generated from Graphus MSP portal.



Dashboard > Graphus - App registrations > Graphus - Certificates & secrets

Graphus - Certificates & secrets

Credentials enable 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.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

THUMBPRINT	START DATE	EXPIRES

No certificates have been added for this application.

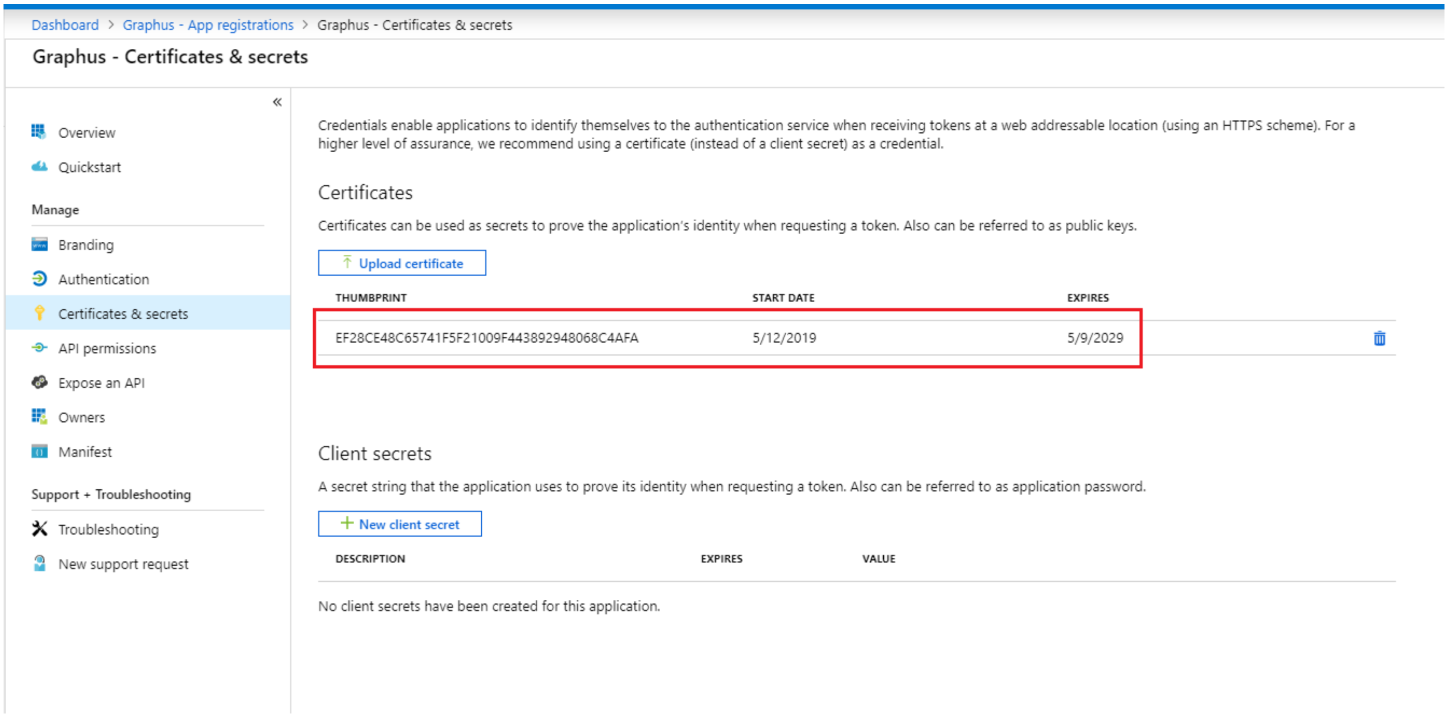
Client secrets

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

No client secrets have been created for this application.

8. The uploaded certificate file should look like the one depicted below in the Certificates section.



Dashboard > Graphus - App registrations > Graphus - Certificates & secrets

Graphus - Certificates & secrets

Credentials enable 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.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

THUMBPRINT	START DATE	EXPIRES
EF28CE48C65741F5F21009F443892948068C4AFA	5/12/2019	5/9/2029

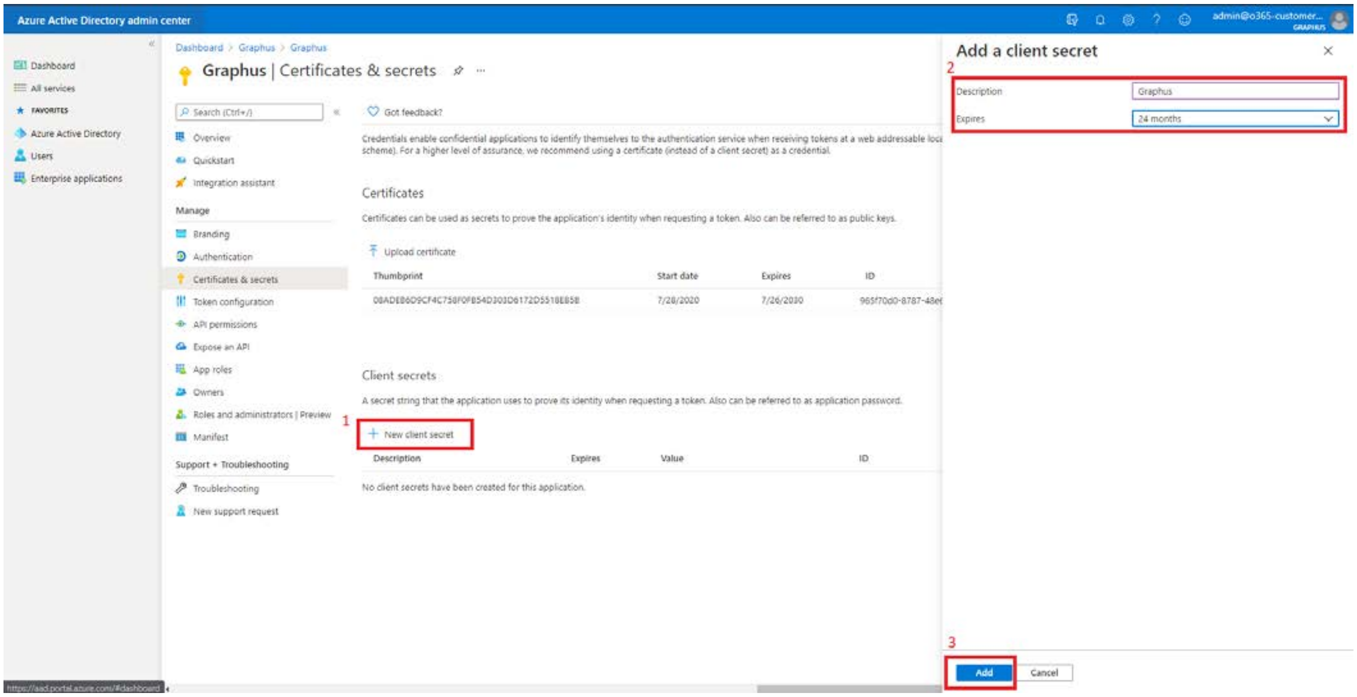
Client secrets

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

No client secrets have been created for this application.

9. In the Graphus – Certificates & secrets page, click **New client secret**, enter *Graphus* in the Description field, select **24 months** from the Expires dropdown menu, and click **Add**.



Dashboard > Graphus > Graphus

Graphus | Certificates & secrets

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

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Thumbprint	Start date	Expires	ID
08ADEB6D9CF4C758F0FB54D303D6172D5518EB5B	7/28/2020	7/26/2030	965f70d0-8787-48e

Client secrets

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	ID

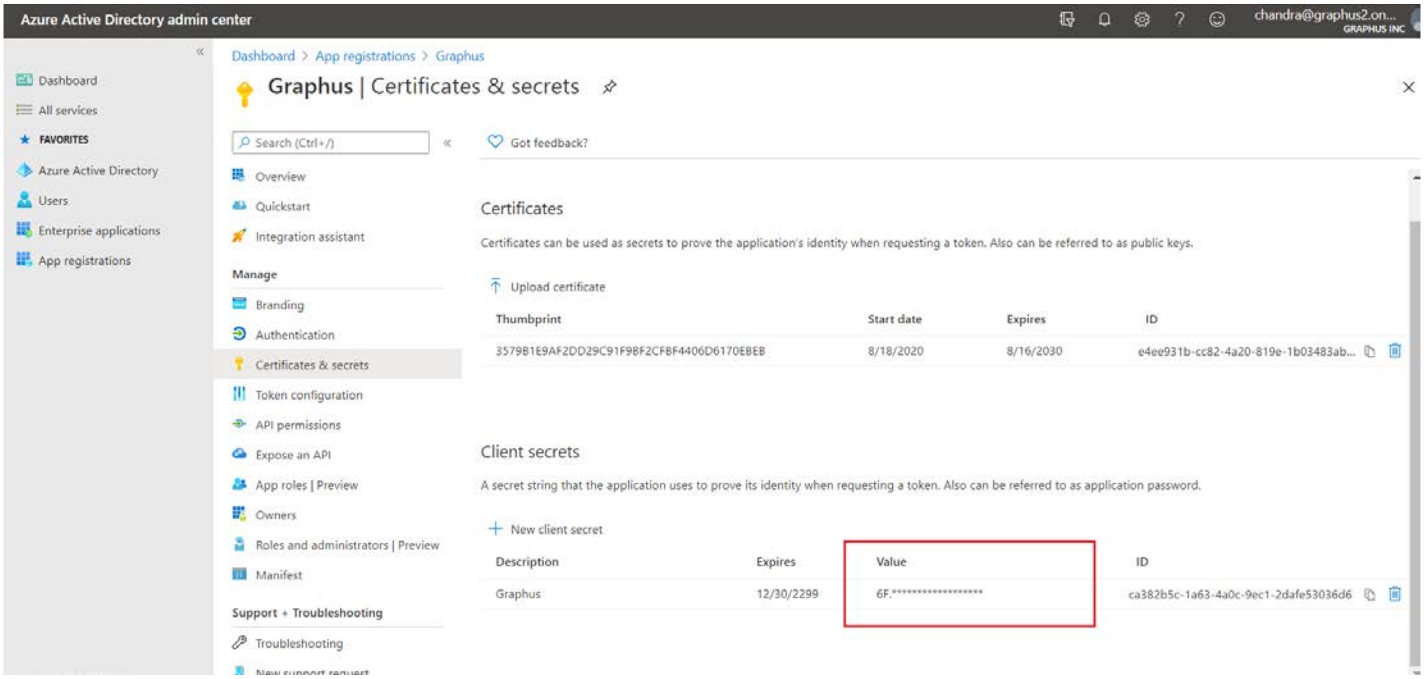
No client secrets have been created for this application.

Add a client secret

Description: Graphus

Expires: 24 months

10. This will automatically generate a value which will be displayed under the **Value** field corresponding to the client secret created in the above step.



Graphus | Certificates & secrets

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Upload certificate

Thumbprint	Start date	Expires	ID
3579B1E9AF2DD29C91F9BF2CFBF4406D6170EBEB	8/18/2020	8/16/2030	e4ee931b-cc82-4a20-819e-1b03483ab...

Client secrets

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

New client secret

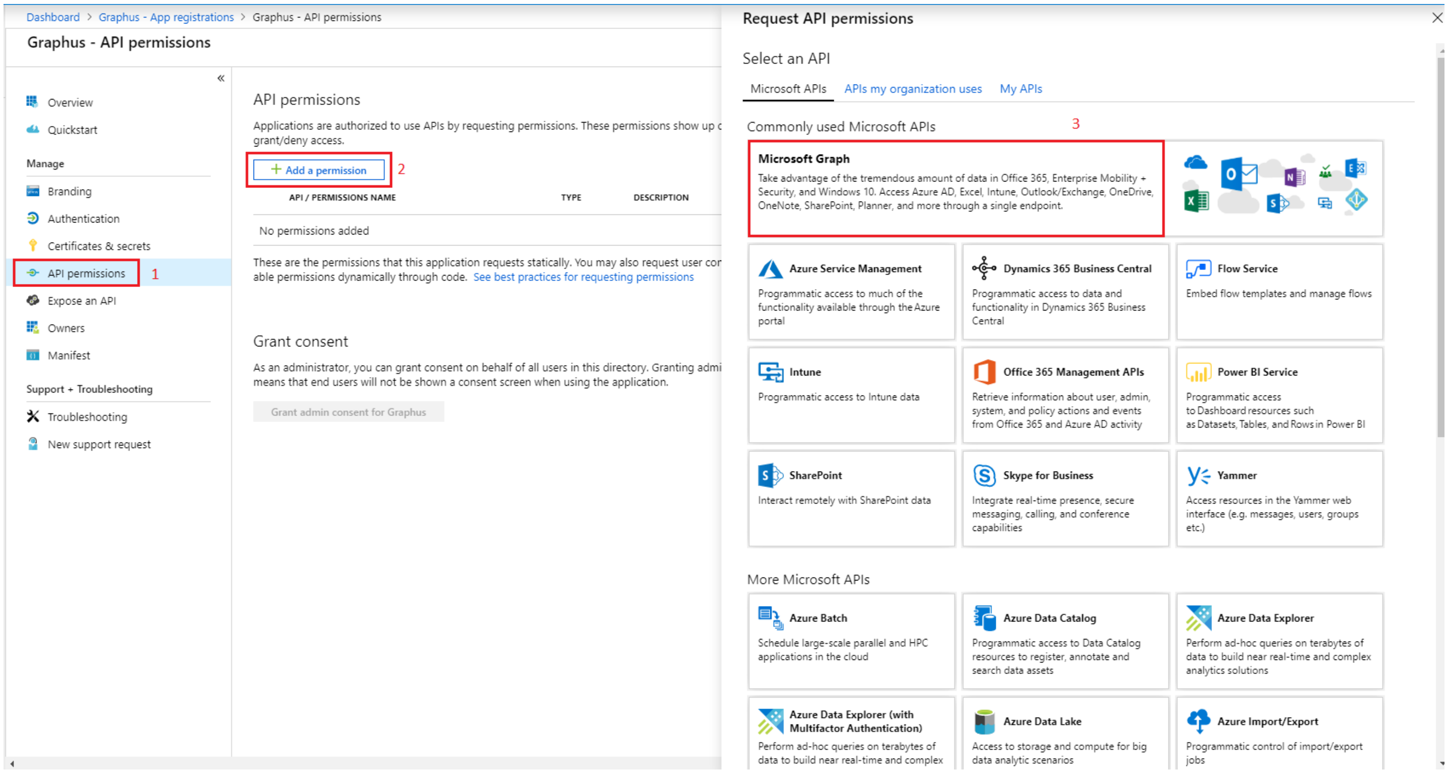
Description	Expires	Value	ID
Graphus	12/30/2299	6F.******************	ca382b5c-1a63-4a0c-9ec1-2dafe53036d6

Copy the value immediately after the creation. Update Application (client) ID (refer step 6) and this client secret value in Graphus MSP portal activation page. Click **Activate organization** on Graphus MSP portal.

Note: This value will no longer be accessible after you leave this blade.

Graphus requires permissions from the APIs provided by Microsoft. To learn more about these permissions, refer to chapter 2 of this guide.

11. In the Manage section, select **API permissions**, click **Add a permission**, then select **Microsoft Graph** from the APIs.



Dashboard > Graphus - App registrations > Graphus - API permissions

Graphus - API permissions

Overview
Quickstart
Manage
Branding
Authentication
Certificates & secrets
API permissions 1
Expose an API
Owners
Manifest
Support + Troubleshooting
Troubleshooting
New support request

API permissions

Applications are authorized to use APIs by requesting permissions. These permissions show up c grant/deny access.

+ Add a permission 2

API / PERMISSIONS NAME | TYPE | DESCRIPTION

No permissions added

These are the permissions that this application requests statically. You may also request user cor 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 admi means that end users will not be shown a consent screen when using the application.

Grant admin consent for Graphus

Request API permissions

Select an API

Microsoft APIs | APIs my organization uses | My APIs

Commonly used Microsoft APIs 3

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

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

Dynamics 365 Business Central
Programmatic access to data and functionality in Dynamics 365 Business Central

Flow Service
Embed flow templates and manage flows

Intune
Programmatic access to Intune data

Office 365 Management APIs
Retrieve information about user, admin, system, and policy actions and events from Office 365 and Azure AD activity

Power BI Service
Programmatic access to Dashboard resources such as Datasets, Tables, and Rows in Power BI

SharePoint
Interact remotely with SharePoint data

Skype for Business
Integrate real-time presence, secure messaging, calling, and conference capabilities

Yammer
Access resources in the Yammer web interface (e.g. messages, users, groups etc.)

More Microsoft APIs

Azure Batch
Schedule large-scale parallel and HPC applications in the cloud

Azure Data Catalog
Programmatic access to Data Catalog resources to register, annotate and search data assets

Azure Data Explorer
Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions

Azure Data Explorer (with Multifactor Authentication)
Perform ad-hoc queries on terabytes of data to build near real-time and complex

Azure Data Lake
Access to storage and compute for big data analytic scenarios

Azure Import/Export
Programmatic control of import/export jobs

12. For **Microsoft Graph** API, choose **Application Permissions**, then select the below 10 permissions and click **Add permissions**.

Contacts

- **Contacts.Read** (Read contacts in all mailboxes)

Directory

- **Directory.Read.All** (Read directory data)

Group

- **Group.Read.All** (Read all groups)

MailboxSettings

- **MailboxSettings.Read** (Read all user mailbox settings)

Mail

- **Mail.Read** (Read mail in all mailboxes)
- **Mail.ReadWrite** (Read and write mail in all mailboxes)

Member

- **Member.Read.Hidden** (Read all hidden memberships)

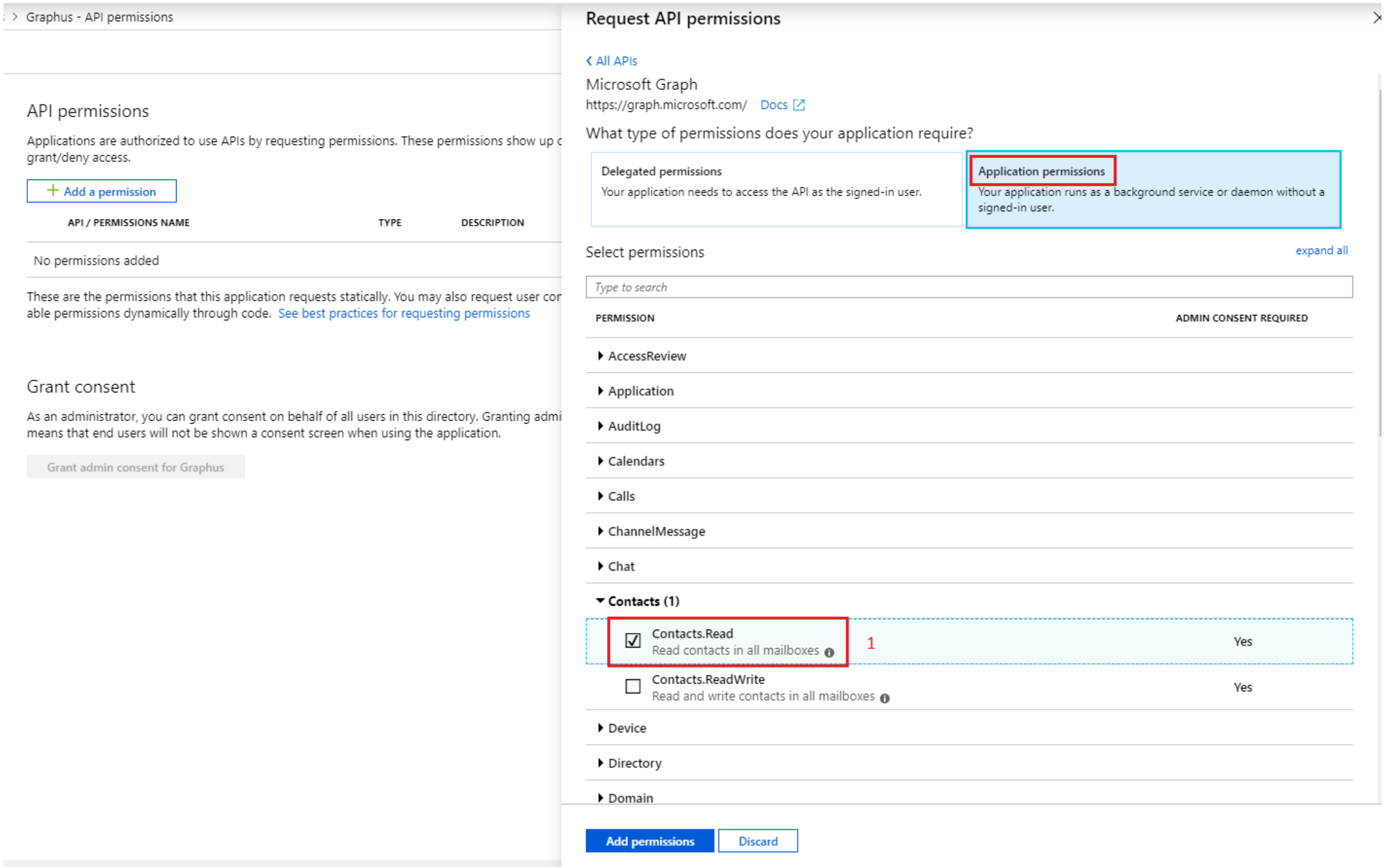
People

- **People.Read.All** (Read all users' relevant people lists)

User

- **User.Export.All** (Export user's data)
- **User.Read.All** (Read all users' full profiles)

Note: None of the DELEGATED PERMISSIONS are required.



› Graphus - API permissions

API permissions

Applications are authorized to use APIs by requesting permissions. These permissions show up c grant/deny access.

+ Add a permission

API / PERMISSIONS NAME	TYPE	DESCRIPTION
No permissions added		

These are the permissions that this application requests statically. You may also request user cor 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 admi means that end users will not be shown a consent screen when using the application.

Grant admin consent for Graphus

Request API permissions

‹ All APIs

Microsoft Graph
https://graph.microsoft.com/ Docs

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.

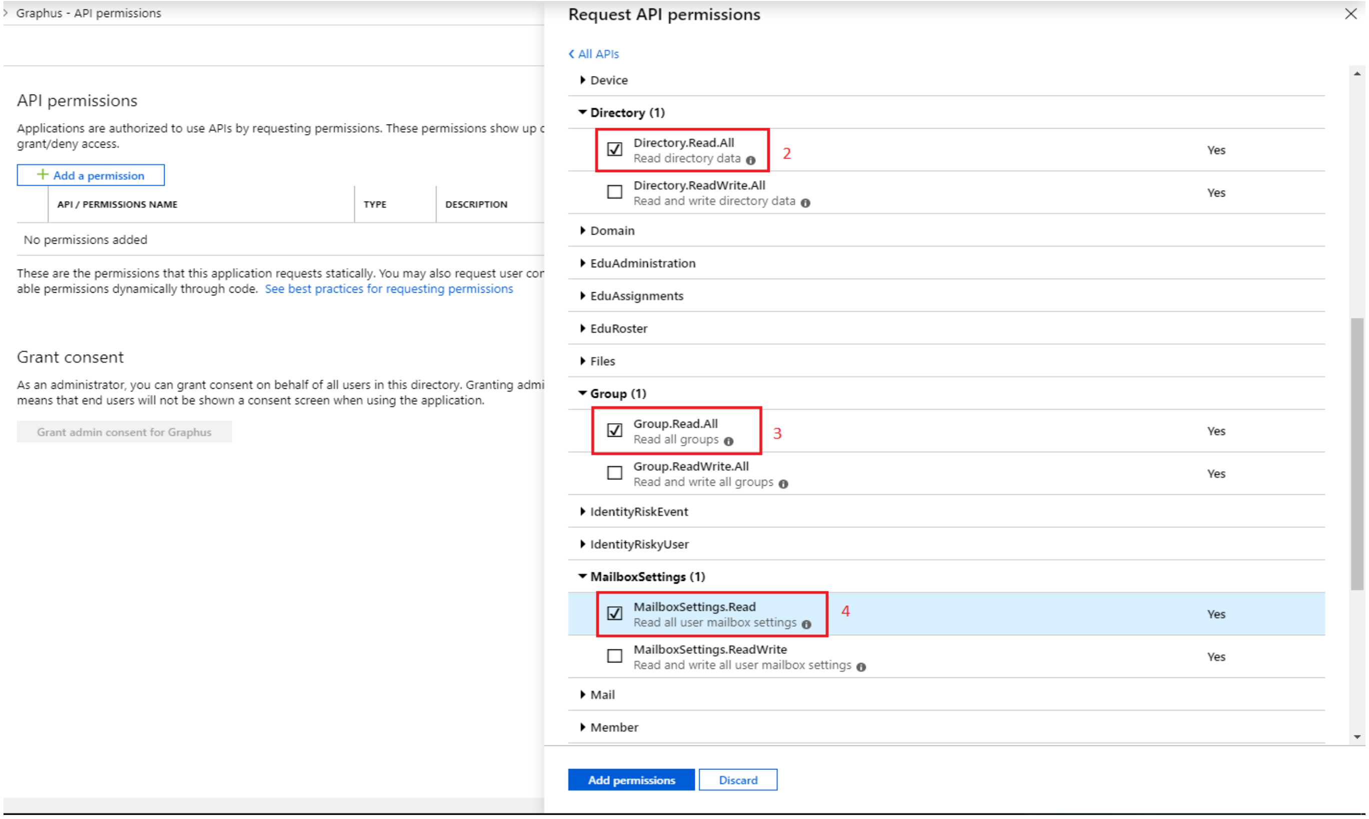
Select permissions

expand all

Type to search

PERMISSION	ADMIN CONSENT REQUIRED
▸ AccessReview	
▸ Application	
▸ AuditLog	
▸ Calendars	
▸ Calls	
▸ ChannelMessage	
▸ Chat	
▾ Contacts (1)	
☑ Contacts.Read Read contacts in all mailboxes ⓘ 1	Yes
☐ Contacts.ReadWrite Read and write contacts in all mailboxes ⓘ	Yes
▸ Device	
▸ Directory	
▸ Domain	

Add permissions Discard



> Graphus - API permissions

API permissions

Applications are authorized to use APIs by requesting permissions. These permissions show up c grant/deny access.

+ Add a permission

API / PERMISSIONS NAME	TYPE	DESCRIPTION
No permissions added		

These are the permissions that this application requests statically. You may also request user cor 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 admi means that end users will not be shown a consent screen when using the application.

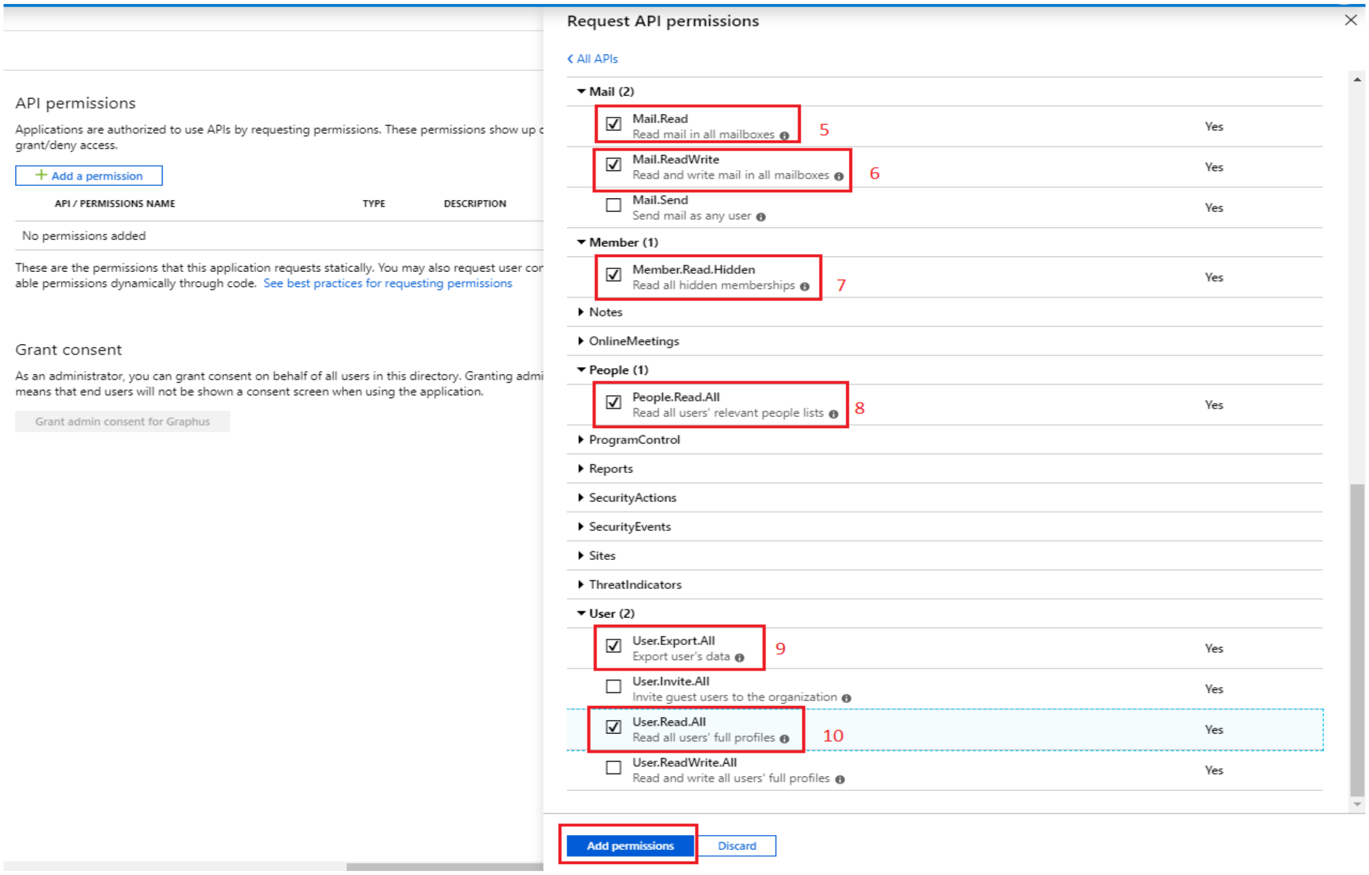
Grant admin consent for Graphus

Request API permissions

< All APIs

- ▸ Device
- ▾ Directory (1)
  - ☑ Directory.Read.All — Read directory data — 2 — Yes
  - □ Directory.ReadWrite.All — Read and write directory data — Yes
- ▸ Domain
- ▸ EduAdministration
- ▸ EduAssignments
- ▸ EduRoster
- ▸ Files
- ▾ Group (1)
  - ☑ Group.Read.All — Read all groups — 3 — Yes
  - □ Group.ReadWrite.All — Read and write all groups — Yes
- ▸ IdentityRiskEvent
- ▸ IdentityRiskyUser
- ▾ MailboxSettings (1)
  - ☑ MailboxSettings.Read — Read all user mailbox settings — 4 — Yes
  - □ MailboxSettings.ReadWrite — Read and write all user mailbox settings — Yes
- ▸ Mail
- ▸ Member

Add permissions | Discard



API permissions

Applications are authorized to use APIs by requesting permissions. These permissions show up c grant/deny access.

+ Add a permission

API / PERMISSIONS NAME	TYPE	DESCRIPTION
No permissions added		

These are the permissions that this application requests statically. You may also request user cor 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 admi means that end users will not be shown a consent screen when using the application.

Grant admin consent for Graphus

Request API permissions

‹ All APIs

▾ Mail (2)

☑ Mail.Read — Read mail in all mailboxes — Yes — 5

☑ Mail.ReadWrite — Read and write mail in all mailboxes — Yes — 6

□ Mail.Send — Send mail as any user — Yes

▾ Member (1)

☑ Member.Read.Hidden — Read all hidden memberships — Yes — 7

▸ Notes

▸ OnlineMeetings

▾ People (1)

☑ People.Read.All — Read all users' relevant people lists — Yes — 8

▸ ProgramControl

▸ Reports

▸ SecurityActions

▸ SecurityEvents

▸ Sites

▸ ThreatIndicators

▾ User (2)

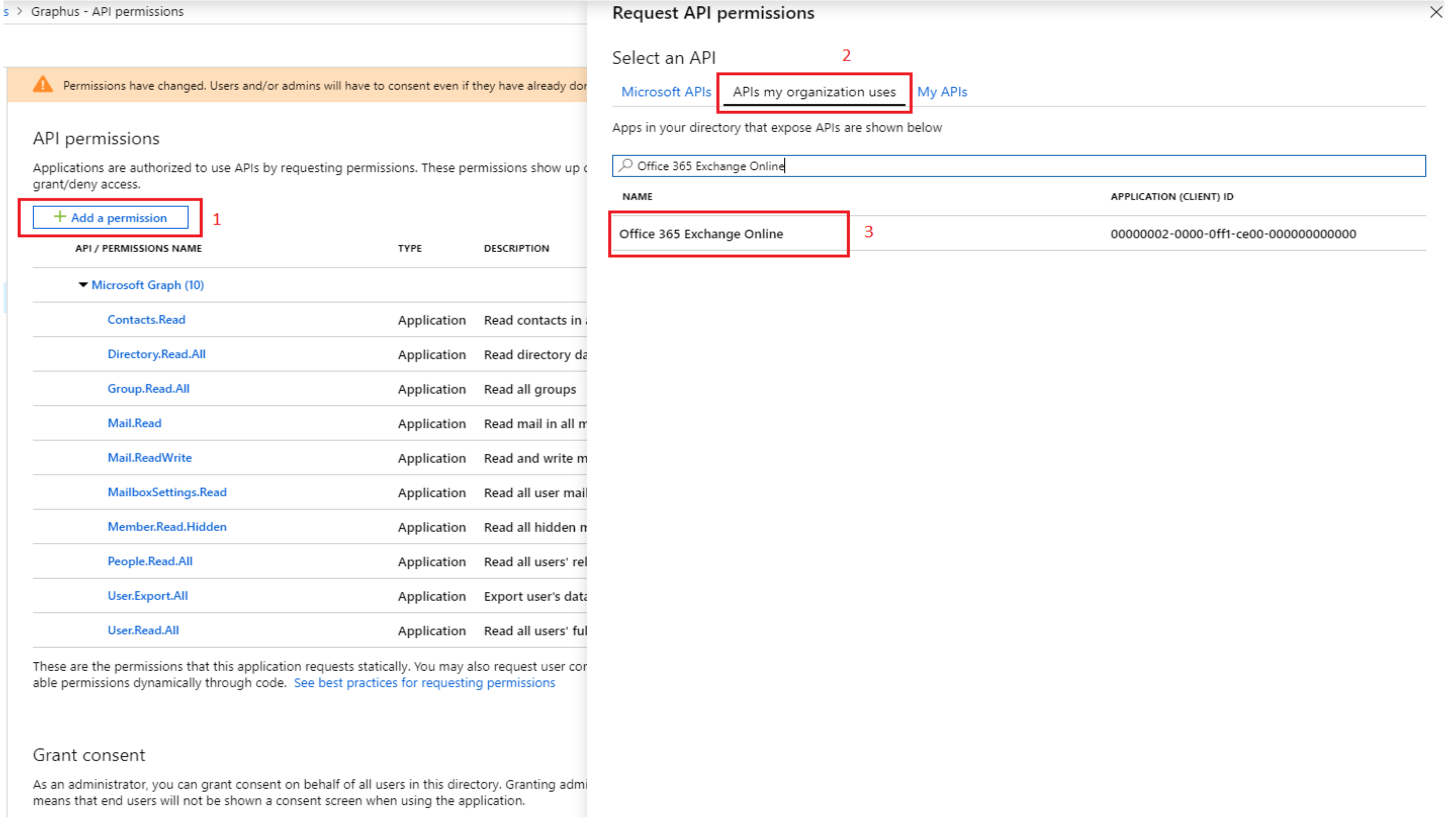
☑ User.Export.All — Export user's data — Yes — 9

□ User.Invite.All — Invite guest users to the organization — Yes

☑ User.Read.All — Read all users' full profiles — Yes — 10

□ User.ReadWrite.All — Read and write all users' full profiles — Yes

13. Click **Add a permission**, select tab **APIs my organization uses**, search for *Office 365 Exchange Online***,** and select **Office 365 Exchange Online** API from the results.



s > Graphus - API permissions

Permissions have changed. Users and/or admins will have to consent even if they have already dor

API permissions

Applications are authorized to use APIs by requesting permissions. These permissions show up c grant/deny access.

API / PERMISSIONS NAME	TYPE	DESCRIPTION
Microsoft Graph (10)		
Contacts.Read	Application	Read contacts in a
Directory.Read.All	Application	Read directory da
Group.Read.All	Application	Read all groups
Mail.Read	Application	Read mail in all m
Mail.ReadWrite	Application	Read and write m
MailboxSettings.Read	Application	Read all user mail
Member.Read.Hidden	Application	Read all hidden m
People.Read.All	Application	Read all users' rel
User.Export.All	Application	Export user's data
User.Read.All	Application	Read all users' ful

These are the permissions that this application requests statically. You may also request user cor 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 admi means that end users will not be shown a consent screen when using the application.

Request API permissions

Select an API

Apps in your directory that expose APIs are shown below

Office 365 Exchange Online

NAME	APPLICATION (CLIENT) ID
Office 365 Exchange Online	00000002-0000-0ff1-ce00-000000000000

14. For **Office 365 Exchange Online** API, choose **Application Permissions**, then select the below six permissions and click **Add permissions**.

Contacts

- **Contacts.Read** (Read contacts in all mailboxes)

MailboxSettings

- **MailboxSettings.Read** (Read all user mailbox settings)

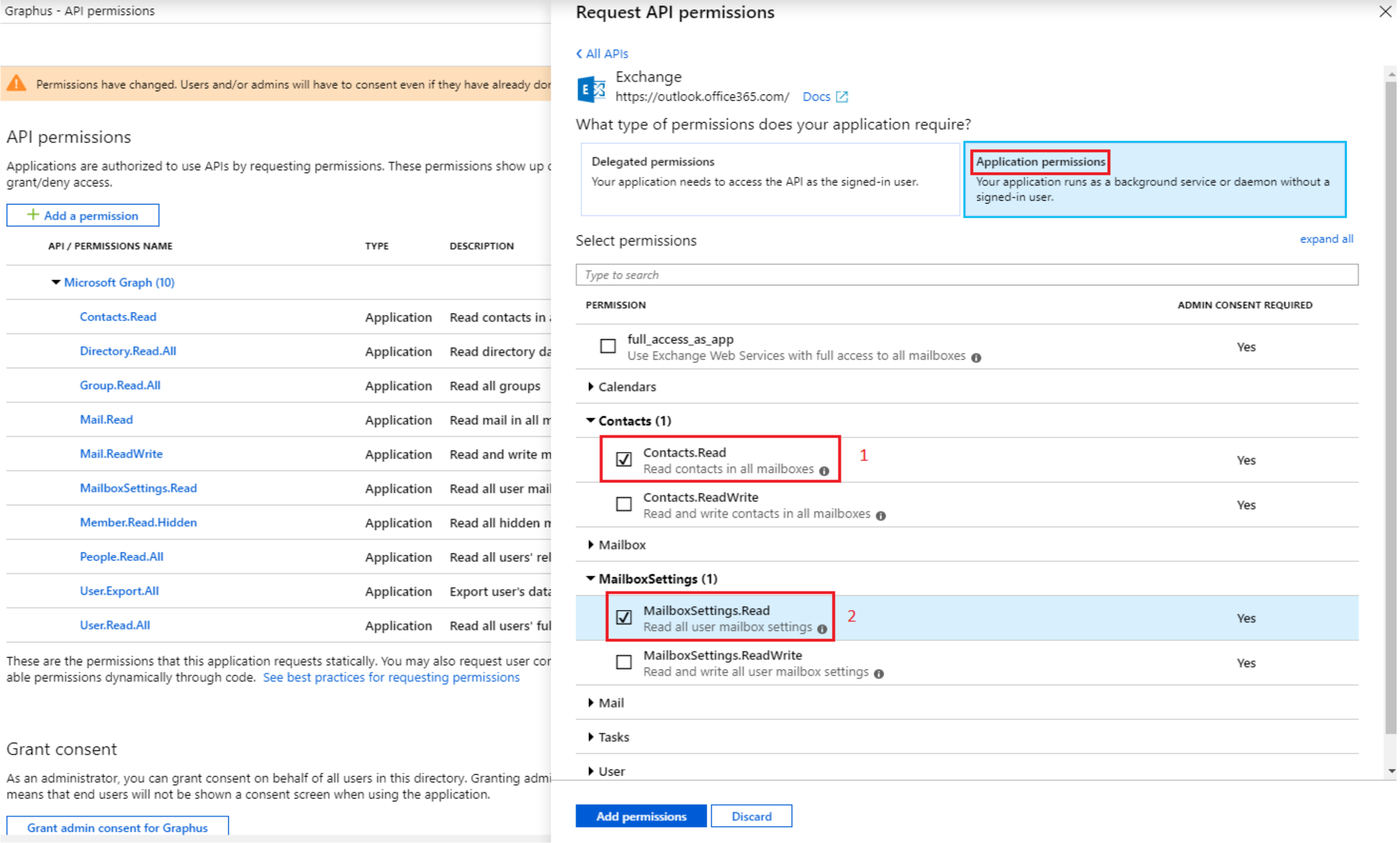
Mail

- **Mail.Read** (Read mail in all mailboxes)
- **Mail.ReadWrite** (Read and write mail in all mailboxes)

User

- **User.Read.All** (Read all users' full profiles)
- **User.ReadBasic.All** (Read all users' basic profiles)

Note: None of the DELEGATED PERMISSIONS are required.



Graphus - API permissions

⚠ Permissions have changed. Users and/or admins will have to consent even if they have already dor

API permissions

Applications are authorized to use APIs by requesting permissions. These permissions show up c grant/deny access.

API / PERMISSIONS NAME	TYPE	DESCRIPTION
▾ Microsoft Graph (10)		
Contacts.Read	Application	Read contacts in a
Directory.Read.All	Application	Read directory da
Group.Read.All	Application	Read all groups
Mail.Read	Application	Read mail in all m
Mail.ReadWrite	Application	Read and write m
MailboxSettings.Read	Application	Read all user mail
Member.Read.Hidden	Application	Read all hidden m
People.Read.All	Application	Read all users' rel
User.Export.All	Application	Export user's data
User.Read.All	Application	Read all users' ful

These are the permissions that this application requests statically. You may also request user cor 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 admi means that end users will not be shown a consent screen when using the application.

Request API permissions

‹ All APIs

Exchange
https://outlook.office365.com/ Docs

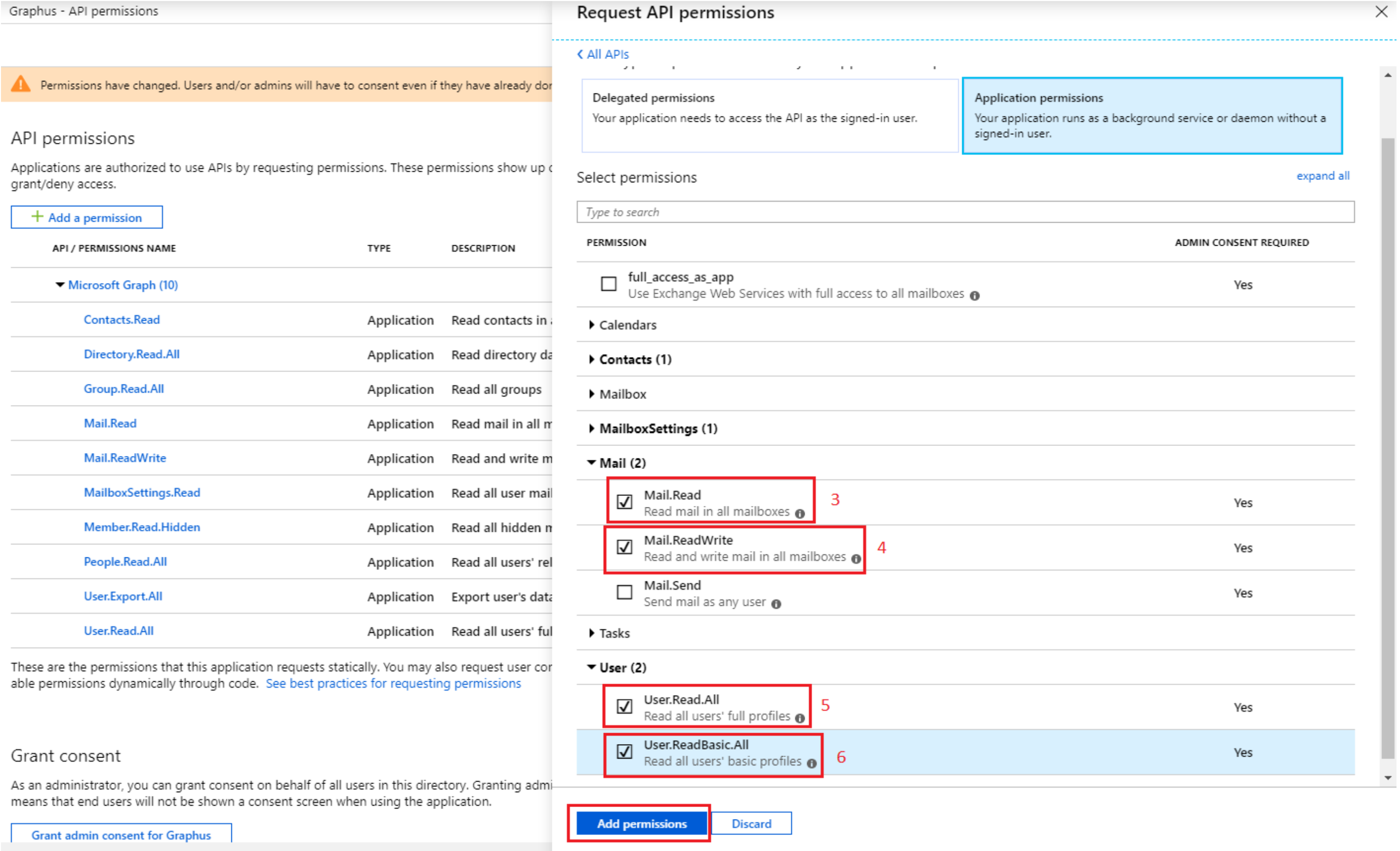
What type of permissions does your application require?

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.

Select permissions

PERMISSION	ADMIN CONSENT REQUIRED
☐ full_access_as_app Use Exchange Web Services with full access to all mailboxes	Yes
▸ Calendars	
▾ Contacts (1)	
☑ Contacts.Read Read contacts in all mailboxes 1	Yes
☐ Contacts.ReadWrite Read and write contacts in all mailboxes	Yes
▸ Mailbox	
▾ MailboxSettings (1)	
☑ MailboxSettings.Read Read all user mailbox settings 2	Yes
☐ MailboxSettings.ReadWrite Read and write all user mailbox settings	Yes
▸ Mail	
▸ Tasks	
▸ User	



Graphus - API permissions

Permissions have changed. Users and/or admins will have to consent even if they have already dor

API permissions

Applications are authorized to use APIs by requesting permissions. These permissions show up c grant/deny access.

API / PERMISSIONS NAME	TYPE	DESCRIPTION
▾ Microsoft Graph (10)		
Contacts.Read	Application	Read contacts in a
Directory.Read.All	Application	Read directory da
Group.Read.All	Application	Read all groups
Mail.Read	Application	Read mail in all m
Mail.ReadWrite	Application	Read and write m
MailboxSettings.Read	Application	Read all user mail
Member.Read.Hidden	Application	Read all hidden m
People.Read.All	Application	Read all users' rel
User.Export.All	Application	Export user's data
User.Read.All	Application	Read all users' ful

These are the permissions that this application requests statically. You may also request user cor 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 admi means that end users will not be shown a consent screen when using the application.

Request API permissions

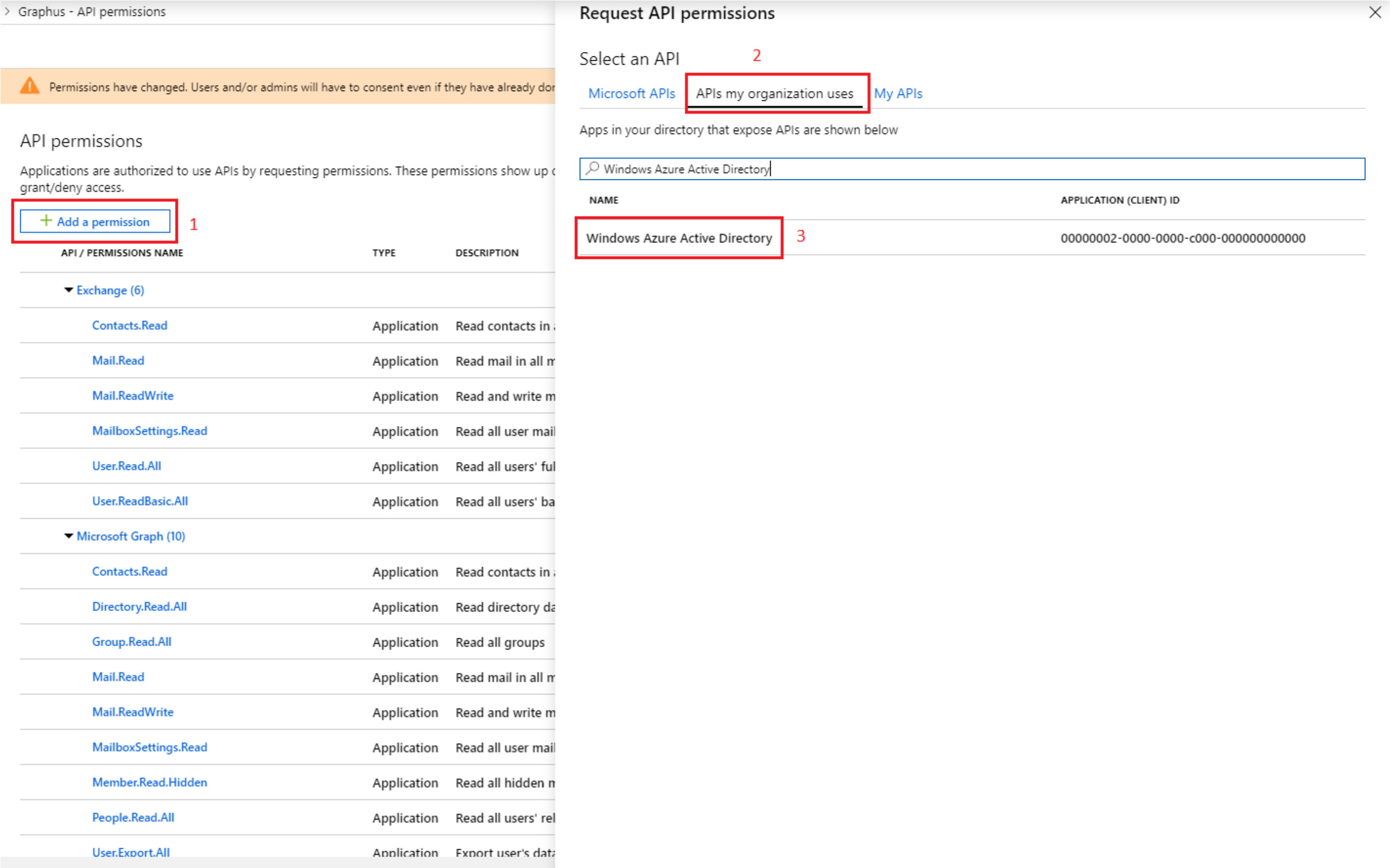
Delegated permissions
Your application needs to access the API as the signed-in user.

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

Select permissions

PERMISSION	ADMIN CONSENT REQUIRED
□ full_access_as_app Use Exchange Web Services with full access to all mailboxes	Yes
▸ Calendars	
▸ **Contacts (1)**	
▸ Mailbox	
▸ **MailboxSettings (1)**	
▾ **Mail (2)**	
☑ Mail.Read Read mail in all mailboxes 3	Yes
☑ Mail.ReadWrite Read and write mail in all mailboxes 4	Yes
□ Mail.Send Send mail as any user	Yes
▸ Tasks	
▾ **User (2)**	
☑ User.Read.All Read all users' full profiles 5	Yes
☑ User.ReadBasic.All Read all users' basic profiles 6	Yes

15. Click **Add a permission**, select the tab **APIs my organization uses**, search for *Windows Azure Active Directory***,** and select **Windows Azure Active Directory** API from the results.



> Graphus - API permissions

Permissions have changed. Users and/or admins will have to consent even if they have already dor

API permissions

Applications are authorized to use APIs by requesting permissions. These permissions show up c grant/deny access.

+ Add a permission 1

API / PERMISSIONS NAME	TYPE	DESCRIPTION
▾ Exchange (6)		
Contacts.Read	Application	Read contacts in a
Mail.Read	Application	Read mail in all m
Mail.ReadWrite	Application	Read and write m
MailboxSettings.Read	Application	Read all user mail
User.Read.All	Application	Read all users' ful
User.ReadBasic.All	Application	Read all users' ba
▾ Microsoft Graph (10)		
Contacts.Read	Application	Read contacts in a
Directory.Read.All	Application	Read directory da
Group.Read.All	Application	Read all groups
Mail.Read	Application	Read mail in all m
Mail.ReadWrite	Application	Read and write m
MailboxSettings.Read	Application	Read all user mail
Member.Read.Hidden	Application	Read all hidden m
People.Read.All	Application	Read all users' rel
User.Export.All	Application	Export user's data

Request API permissions

Select an API 2

Apps in your directory that expose APIs are shown below

Windows Azure Active Directory

NAME	APPLICATION (CLIENT) ID
Windows Azure Active Directory 3	00000002-0000-0000-c000-000000000000

16. For **Windows Azure Active Directory** API, choose **Application Permissions**, then select the below two permissions and click **Add permissions**.

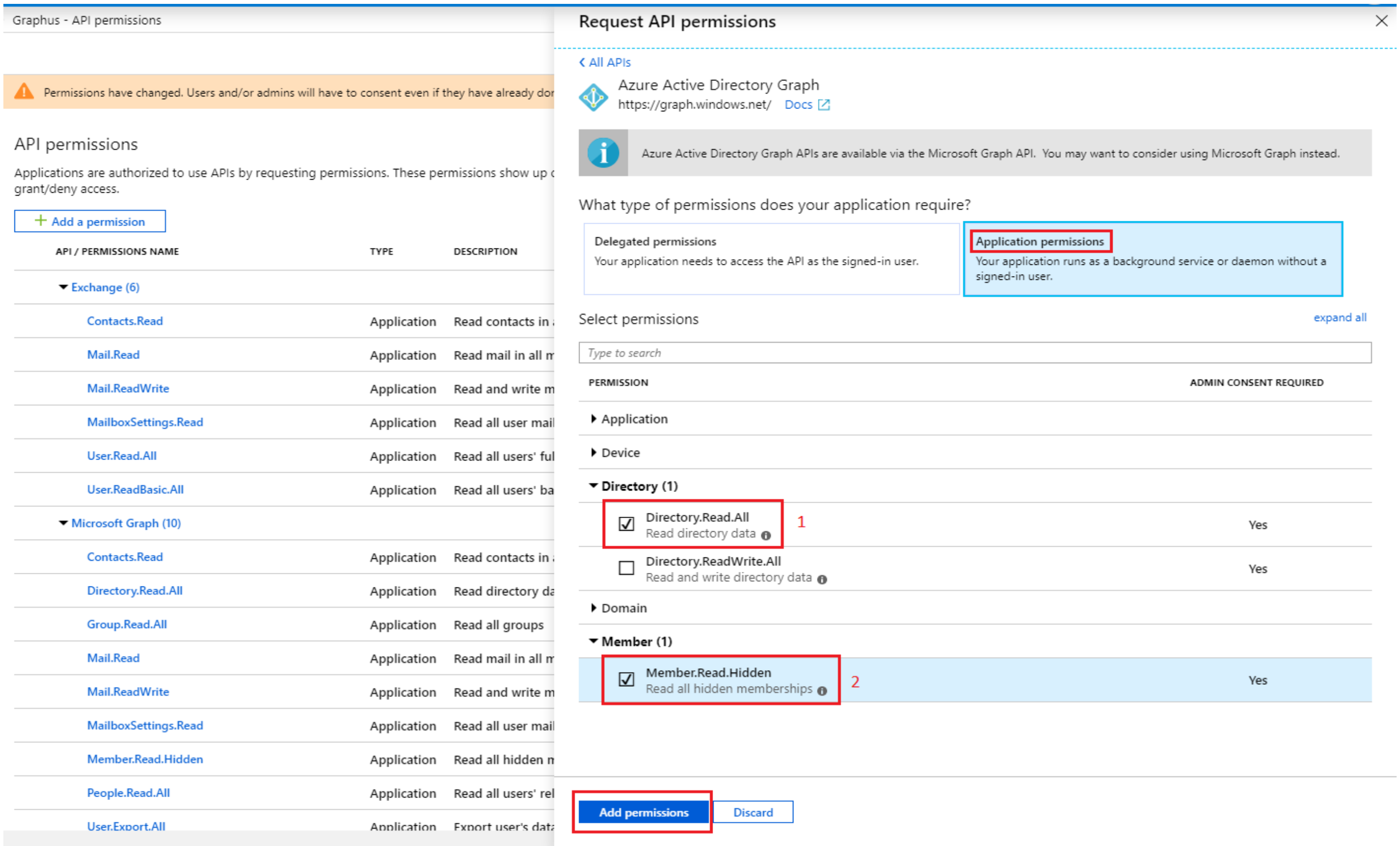
Directory

- **Directory.Read.All** (Read directory data)

Member

- **Member.Read.Hidden** (Read all hidden memberships)

Note: None of the DELEGATED PERMISSIONS are required.



Graphus - API permissions

⚠ Permissions have changed. Users and/or admins will have to consent even if they have already dor

API permissions

Applications are authorized to use APIs by requesting permissions. These permissions show up c grant/deny access.

API / PERMISSIONS NAME	TYPE	DESCRIPTION
▾ Exchange (6)		
Contacts.Read	Application	Read contacts in a
Mail.Read	Application	Read mail in all m
Mail.ReadWrite	Application	Read and write m
MailboxSettings.Read	Application	Read all user mail
User.Read.All	Application	Read all users' ful
User.ReadBasic.All	Application	Read all users' ba
▾ Microsoft Graph (10)		
Contacts.Read	Application	Read contacts in a
Directory.Read.All	Application	Read directory da
Group.Read.All	Application	Read all groups
Mail.Read	Application	Read mail in all m
Mail.ReadWrite	Application	Read and write m
MailboxSettings.Read	Application	Read all user mail
Member.Read.Hidden	Application	Read all hidden m
People.Read.All	Application	Read all users' rel
User.Export.All	Application	Export user's data

Request API permissions

Azure Active Directory Graph
https://graph.windows.net/ Docs

Azure Active Directory Graph APIs are available via the Microsoft Graph API. You may want to consider using Microsoft Graph instead.

What type of permissions does your application require?

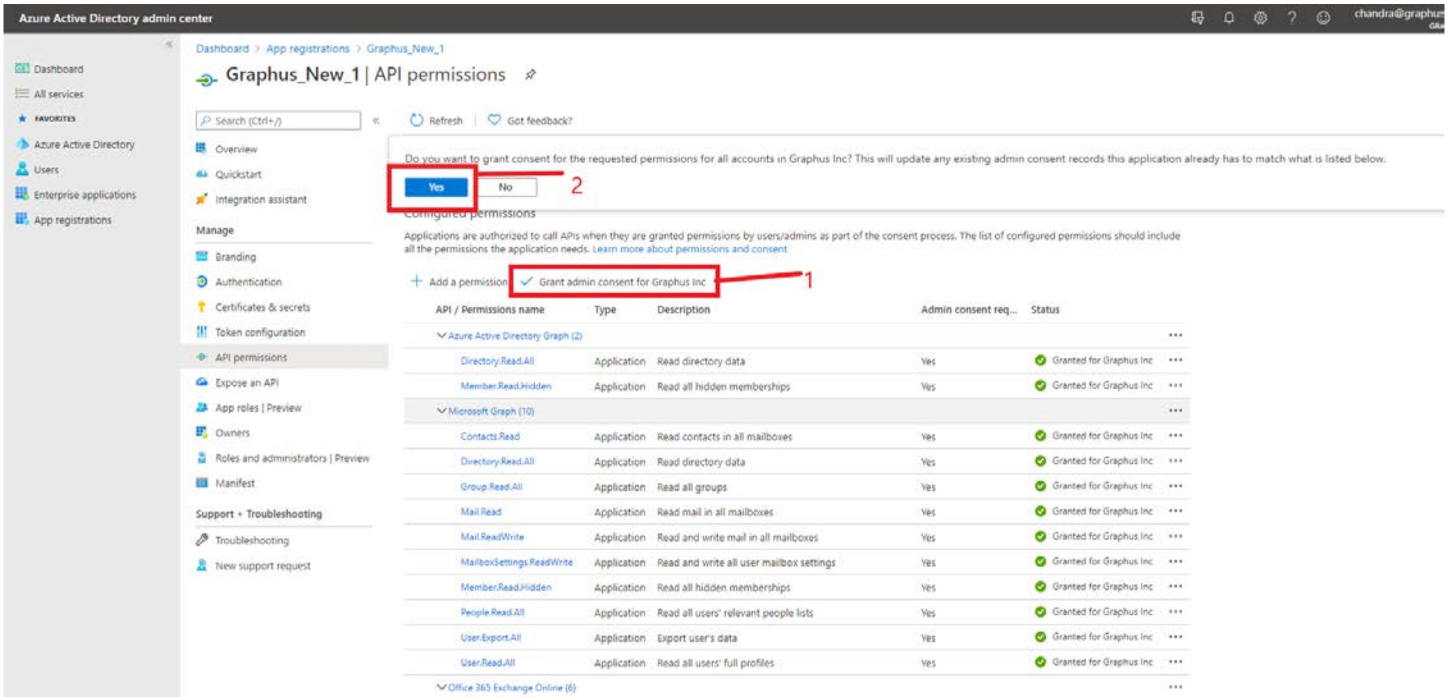
Delegated permissions
Your application needs to access the API as the signed-in user.

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

Select permissions

PERMISSION	ADMIN CONSENT REQUIRED
▸ Application	
▸ Device	
▾ Directory (1)	
☑ Directory.Read.All Read directory data 1	Yes
□ Directory.ReadWrite.All Read and write directory data	Yes
▸ Domain	
▾ Member (1)	
☑ Member.Read.Hidden Read all hidden memberships 2	Yes

17. Click **Grant admin consent for <your organization>** button in Grant Consent section. Then, click **Yes** button on the confirmation popup.

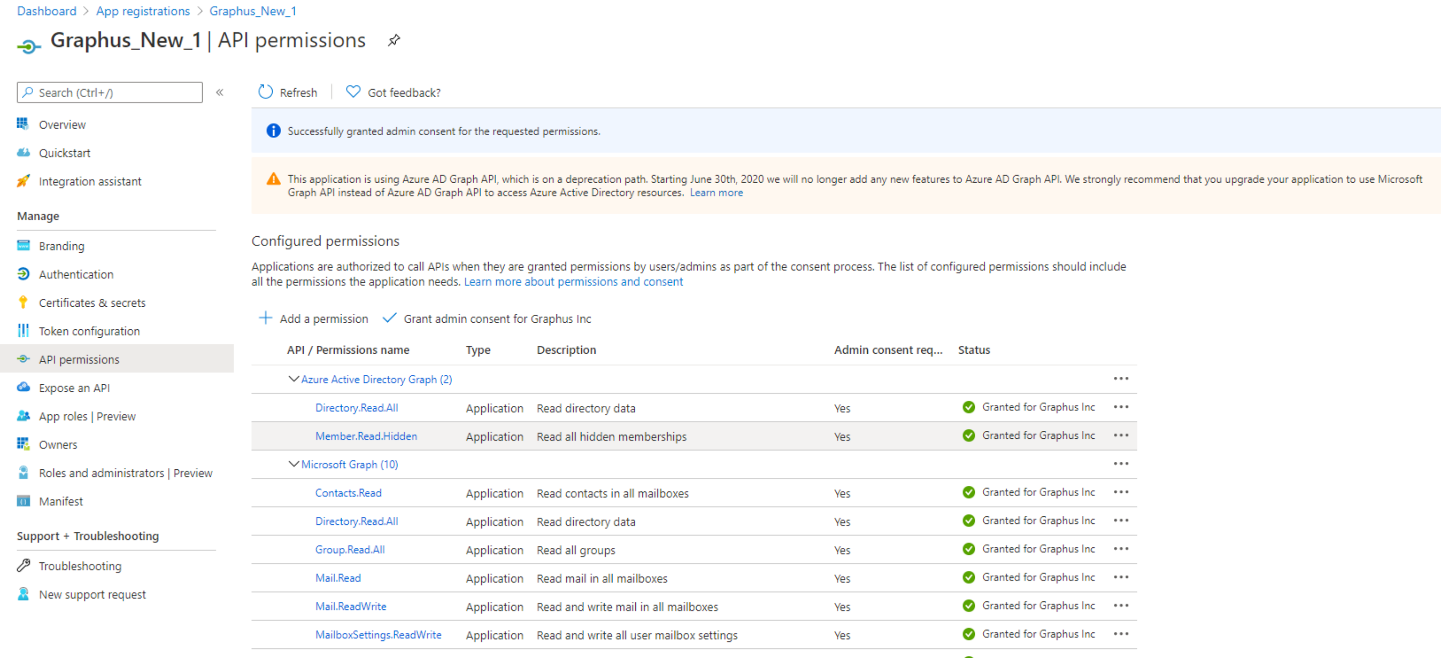


Do you want to grant consent for the requested permissions for all accounts in Graphus Inc? This will update any existing admin consent records this application already has to match what is listed below.

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	
∨ Azure Active Directory Graph (2)					•••
Directory.Read.All	Application	Read directory data	Yes	✓ Granted for Graphus Inc	•••
Member.Read.Hidden	Application	Read all hidden memberships	Yes	✓ Granted for Graphus Inc	•••
∨ Microsoft Graph (10)					•••
Contacts.Read	Application	Read contacts in all mailboxes	Yes	✓ Granted for Graphus Inc	•••
Directory.Read.All	Application	Read directory data	Yes	✓ Granted for Graphus Inc	•••
Group.Read.All	Application	Read all groups	Yes	✓ Granted for Graphus Inc	•••
Mail.Read	Application	Read mail in all mailboxes	Yes	✓ Granted for Graphus Inc	•••
Mail.ReadWrite	Application	Read and write mail in all mailboxes	Yes	✓ Granted for Graphus Inc	•••
MailboxSettings.ReadWrite	Application	Read and write all user mailbox settings	Yes	✓ Granted for Graphus Inc	•••
Member.Read.Hidden	Application	Read all hidden memberships	Yes	✓ Granted for Graphus Inc	•••
People.Read.All	Application	Read all users' relevant people lists	Yes	✓ Granted for Graphus Inc	•••
User.Export.All	Application	Export user's data	Yes	✓ Granted for Graphus Inc	•••
User.Read.All	Application	Read all users' full profiles	Yes	✓ Granted for Graphus Inc	•••
∨ Office 365 Exchange Online (6)					•••

If the action is successful, the confirmation message will be displayed as below.



Successfully granted admin consent for the requested permissions.

This application is using Azure AD Graph API, which is on a deprecation path. Starting June 30th, 2020 we will no longer add any new features to Azure AD Graph API. We strongly recommend that you upgrade your application to use Microsoft Graph API instead of Azure AD Graph API to access Azure Active Directory resources. Learn more

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	
∨ Azure Active Directory Graph (2)					•••
Directory.Read.All	Application	Read directory data	Yes	✓ Granted for Graphus Inc	•••
Member.Read.Hidden	Application	Read all hidden memberships	Yes	✓ Granted for Graphus Inc	•••
∨ Microsoft Graph (10)					•••
Contacts.Read	Application	Read contacts in all mailboxes	Yes	✓ Granted for Graphus Inc	•••
Directory.Read.All	Application	Read directory data	Yes	✓ Granted for Graphus Inc	•••
Group.Read.All	Application	Read all groups	Yes	✓ Granted for Graphus Inc	•••
Mail.Read	Application	Read mail in all mailboxes	Yes	✓ Granted for Graphus Inc	•••
Mail.ReadWrite	Application	Read and write mail in all mailboxes	Yes	✓ Granted for Graphus Inc	•••
MailboxSettings.ReadWrite	Application	Read and write all user mailbox settings	Yes	✓ Granted for Graphus Inc	•••

Note: It usually takes 5 -10 minutes for the changes to take effect in Azure AD.

2. Required Permissions

For the seamless integration of Graphus application with your organization and detection and remediation of various kinds of email attacks, a set of permissions is required for following Microsoft APIs.

- Microsoft Graph
- Office 365 Exchange Online
- Windows Azure Active Directory

The following table describes why certain permissions are needed by Graphus.

Microsoft Graph	
Permission	Required for
User.Export.All	Required to fetch the email address, first name and last name of the users in an organization to detect the impersonation.
People.Read.All	Required to fetch the shared contacts of a user in an organization to build the Trust Graph.
MailboxSettings.Read	Required to get the current status of a mailbox.
Member.Read.Hidden	Required to get the information of all the groups (public and private) that a user belongs to. It is used by Graphus to detect mails sent to group email addresses.
Mail.Read	Required by Graphus for the detection of email attacks.
Mail.ReadWrite	Required by Graphus for detection of email attacks and insertion of EmployeeShield in an email. This is also required to delete mail from a user's inbox when an email attack needs to be quarantined.
Contacts.Read	Required to fetch the email addresses, first name and last name of the users in an organization to detect user impersonation.
Group.Read.All	Required to get the information of all the groups that a user belongs to. It is used by Graphus to detect mails sent to group email addresses. This is also needed when only a subset of users belonging to a group is required to be protected.
Directory.Read.All	Required to fetch detailed attributes of all the users and groups in an organization for detection of email attacks.
User.Read.All	Required to make a decision to either process the user's mailbox by Graphus or not. This information is also required in the oAuth flow.

Office 365 Exchange Online	
Permission	Required For
User.Read.All	Required to make a decision to either process the user's mailbox by Graphus or not. This information is also required in the oAuth flow.
User.ReadBasic.All	Required to make a decision to either process the user's mailbox by Graphus or not. This information is also required to fetch the email address, first name and last name of the users in an organization to detect user impersonation.
MailboxSettings.Read	Required to get the current status of a mailbox.
Contacts.Read	Required to fetch the email addresses, first name and last name of users in an organization to detect user impersonation.
Mail.Read	Required by Graphus for the detection of email attacks.
Mail.ReadWrite	Required by Graphus for detection of email attacks and insertion of EmployeeShield in a mail. This is also required to delete mail from a user's inbox when an email attack needs to be quarantined.

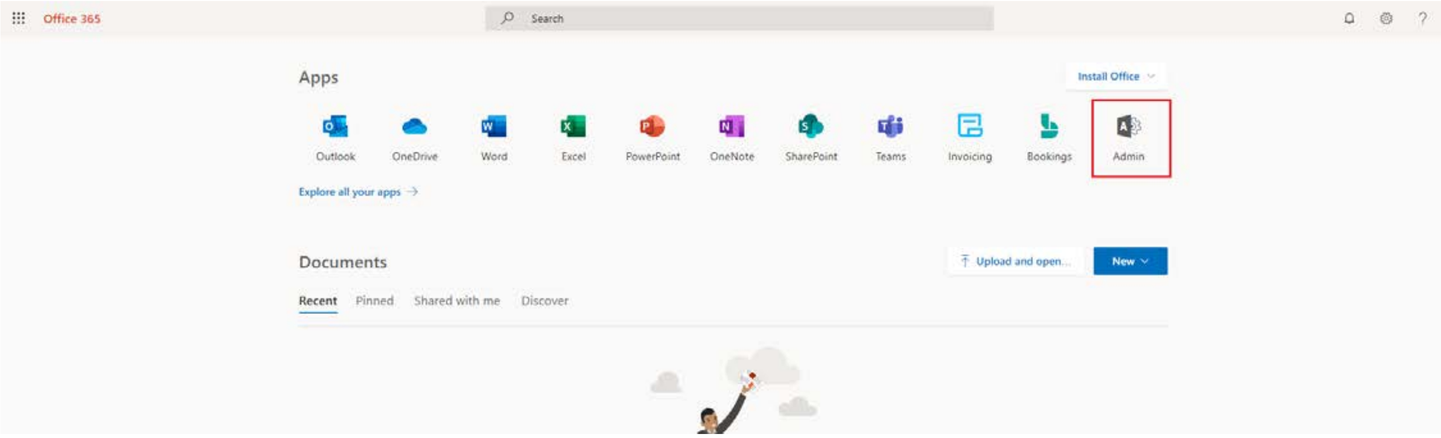
Windows Azure Active Directory	
Permission	Required For
Member.Read.Hidden	Required to get the information of all the groups (public and private) that a user belongs to. It is used by Graphus to detect mails sent to group email addresses
Directory.Read.All	Required to fetch deep-level information of all users and groups in an organization for detection of email attacks

3. Graphus Application Deactivation

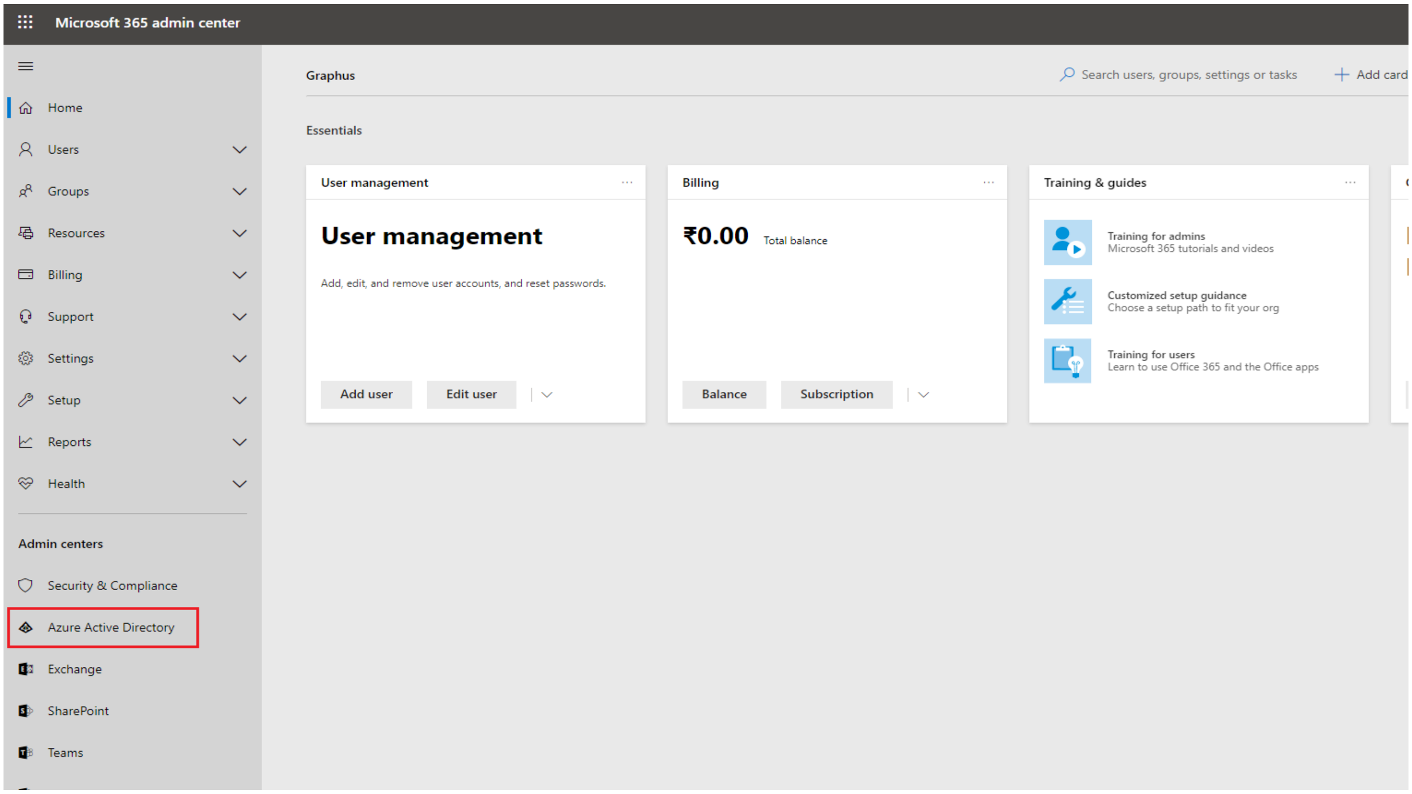
If, for any reason, you want to deactivate Graphus application from your environment, then please follow the below steps.

Steps

1. Login to Office 365 portal and select **Admin**.

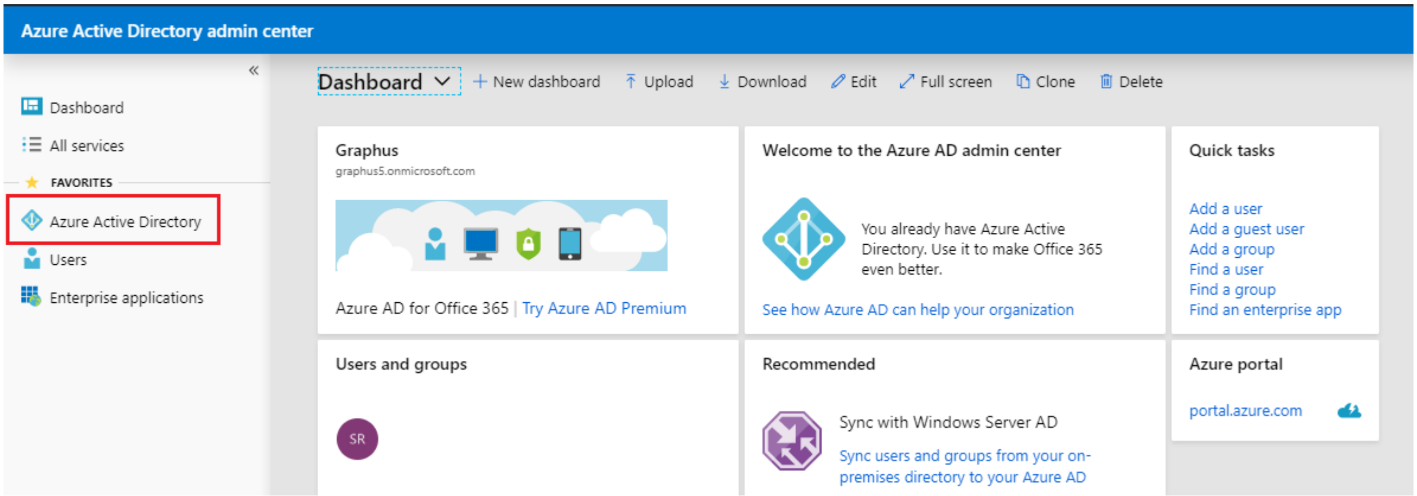


2. Expand **Admin centers** and choose **Azure Active Directory**.



Add, edit, and remove user accounts, and reset passwords.

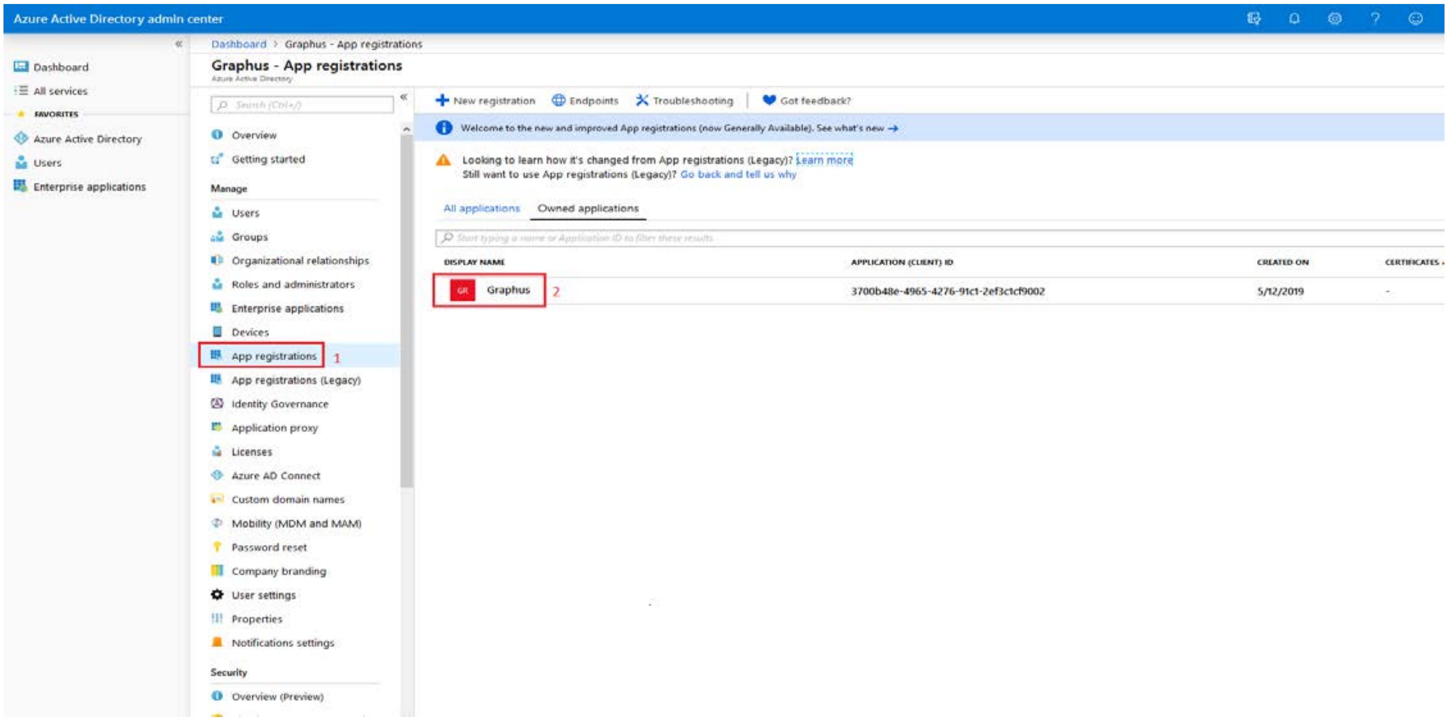
3. Click **Azure Active Directory**.



You already have Azure Active Directory. Use it to make Office 365 even better.

Sync users and groups from your on-premises directory to your Azure AD

4. In the Manage section, click **App registrations** and then choose the Graphus application from the application list.

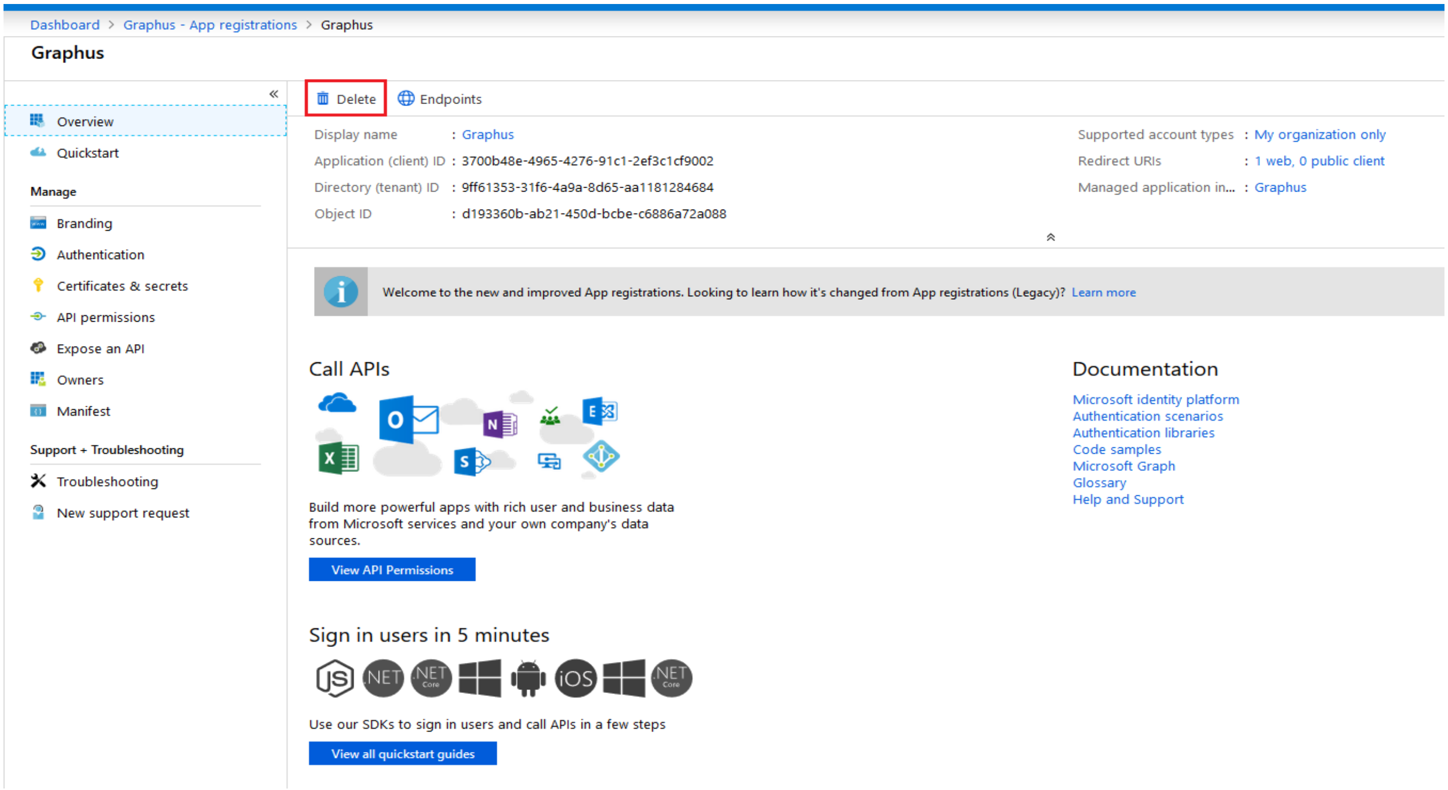


Welcome to the new and improved App registrations (now Generally Available). See what's new →

Looking to learn how it's changed from App registrations (Legacy)? Learn more
Still want to use App registrations (Legacy)? Go back and tell us why

DISPLAY NAME	APPLICATION (CLIENT) ID	CREATED ON	CERTIFICATES
GR Graphus	3700b48e-4965-4276-91c1-2ef3c1cf9002	5/12/2019	-

5. Click the **Delete** button for the Graphus application.



Dashboard > Graphus - App registrations > Graphus

Graphus

Display name	: Graphus	Supported account types	: My organization only
Application (client) ID	: 3700b48e-4965-4276-91c1-2ef3c1cf9002	Redirect URIs	: 1 web, 0 public client
Directory (tenant) ID	: 9ff61353-31f6-4a9a-8d65-aa1181284684	Managed application in...	: Graphus
Object ID	: d193360b-ab21-450d-bcbe-c6886a72a088		

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? Learn more

Call APIs

Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

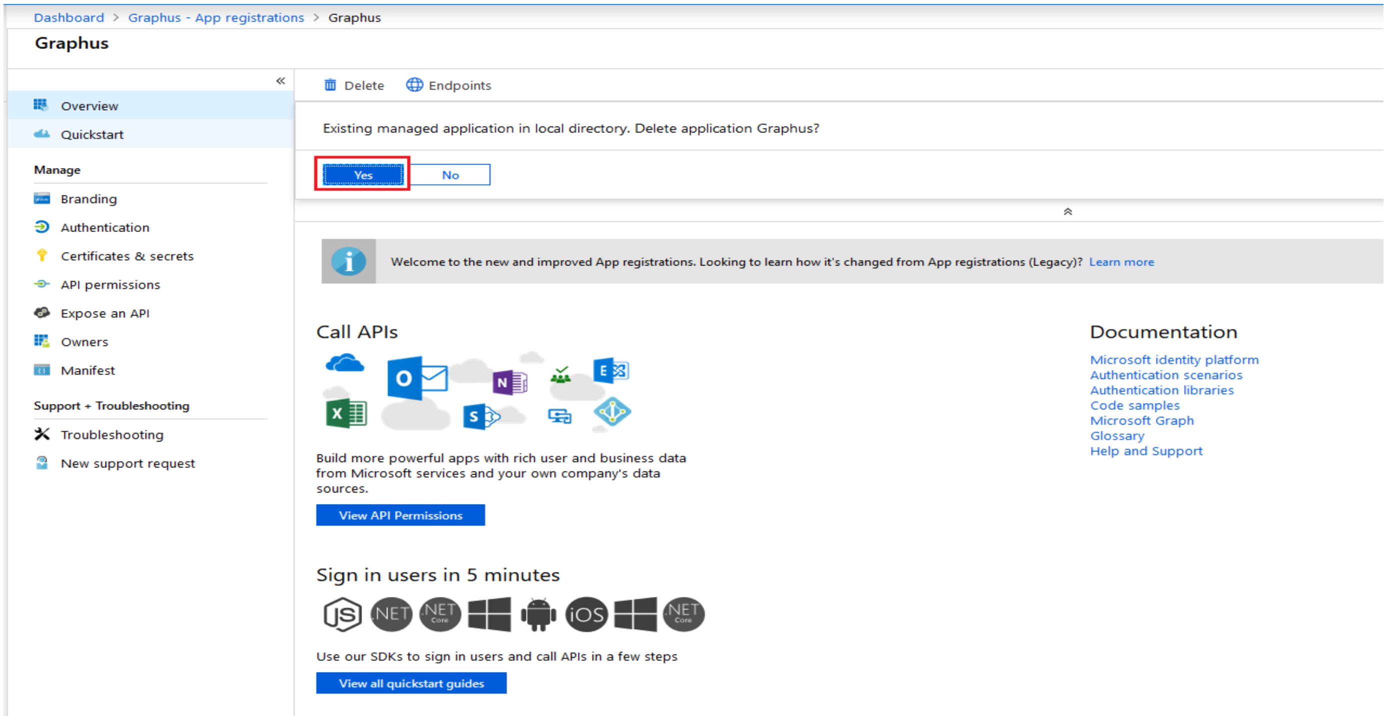
Sign in users in 5 minutes

Use our SDKs to sign in users and call APIs in a few steps

Documentation

Microsoft identity platform
Authentication scenarios
Authentication libraries
Code samples
Microsoft Graph
Glossary
Help and Support

6. Click **Yes** on the confirmation popup.



Dashboard > Graphus - App registrations > Graphus

Graphus

Existing managed application in local directory. Delete application Graphus?

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? Learn more

Call APIs

Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

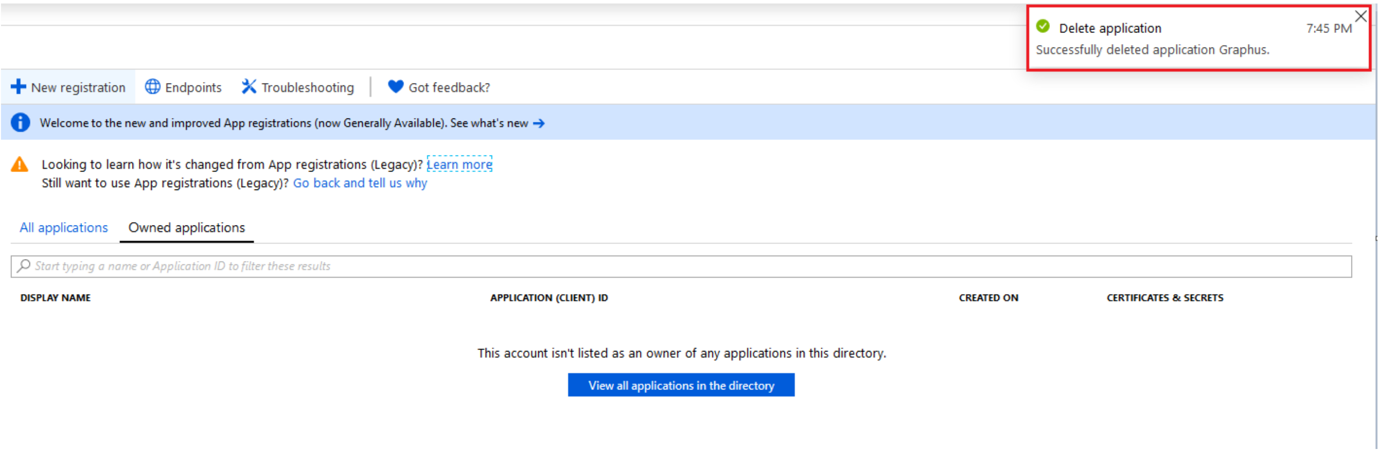
Sign in users in 5 minutes

Use our SDKs to sign in users and call APIs in a few steps

Documentation

Microsoft identity platform
Authentication scenarios
Authentication libraries
Code samples
Microsoft Graph
Glossary
Help and Support

After deletion is successful, a confirmation message will appear as depicted below.



Delete application 7:45 PM
Successfully deleted application Graphus.

Welcome to the new and improved App registrations (now Generally Available). See what's new →

Looking to learn how it's changed from App registrations (Legacy)? Learn more
Still want to use App registrations (Legacy)? Go back and tell us why

All applications
Owned applications
Start typing a name or Application ID to filter these results

DISPLAY NAME	APPLICATION (CLIENT) ID	CREATED ON	CERTIFICATES & SECRETS

This account isn't listed as an owner of any applications in this directory.

After this step, the Graphus application and its associated API permissions will be successfully removed.