Add Azure AD tenant

Last Modified on 27/11/2023 2:25 pm EET

Azure AD integration allows Carillon to target management rules directly to Azure AD groups and devices. When you create dynamic Azure AD group for your devices and then create Carillon management rules for this Azure AD group, your Azure AD connected devices will automatically receive your management rules when devices are joined to Azure AD and dynamic group memberships have been updated.

You can add multiple Azure AD tenants to single Carillon environment.

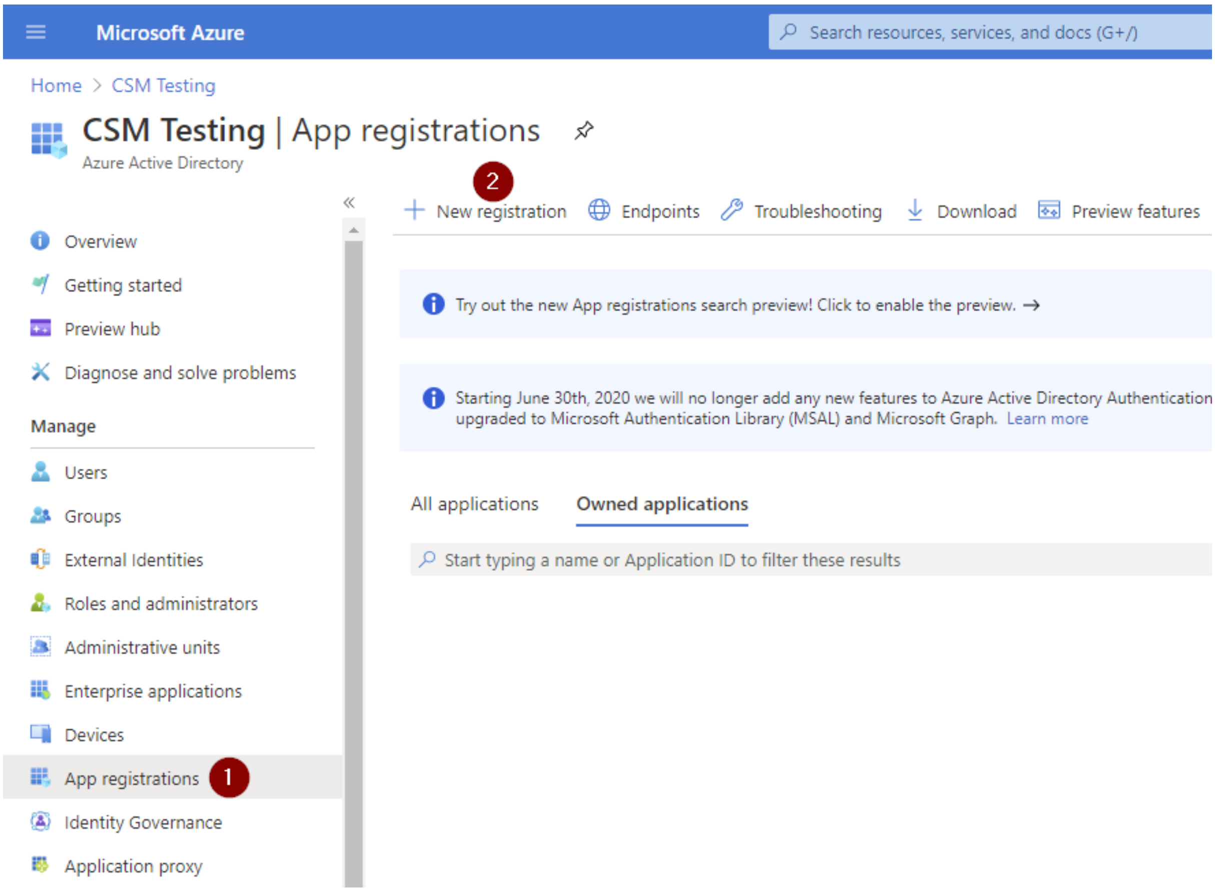
Note!

Azure AD integration can be only used to manage native Azure AD joined devices. For hybrid Azure AD devices (that are joined to both on-premises AD and Azure AD) must be managed as on-premises AD devices.

1. Create Azure AD App Registration

You need to create Azure AD App Registration to the target tenant and you need to have permissions to register new Azure AD Apps. IF you do not have permissions to create Azure AD App Registration, then you need to send these instructions to some one who has permissions to create Azure AD App Registration. Only this step is required to be performed by user who has proper permissions and you will need to receive following information when this step is completed: **Directory ID** (also known as tenant ID), **Application ID** (also known as Client ID) and **Client Secret**

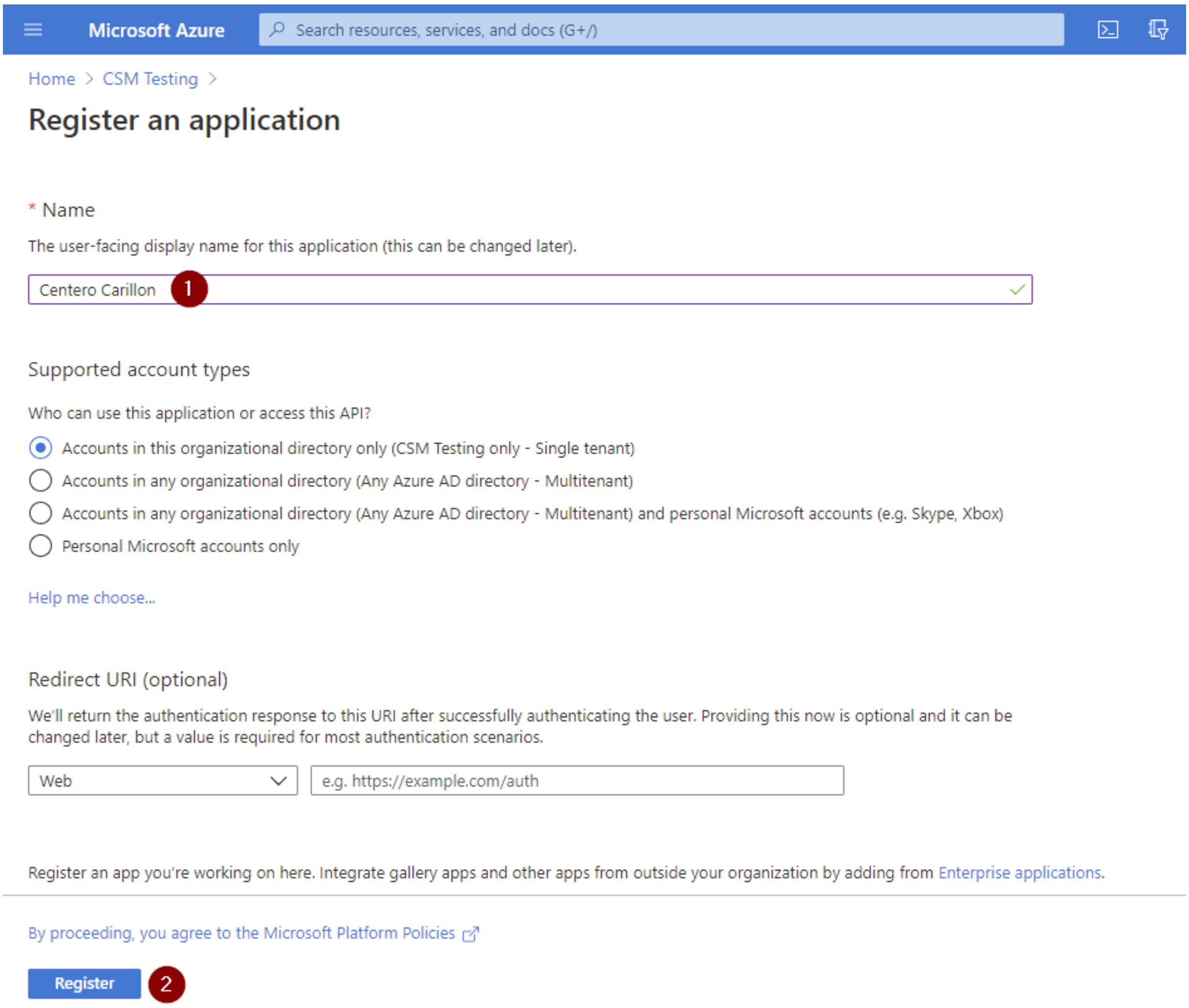
1. Open https://portal.azure.com



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 upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

2. First click **App registrations** and then click **New registration**



Register an application

* Name

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

Centero Carillon

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (CSM Testing 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.

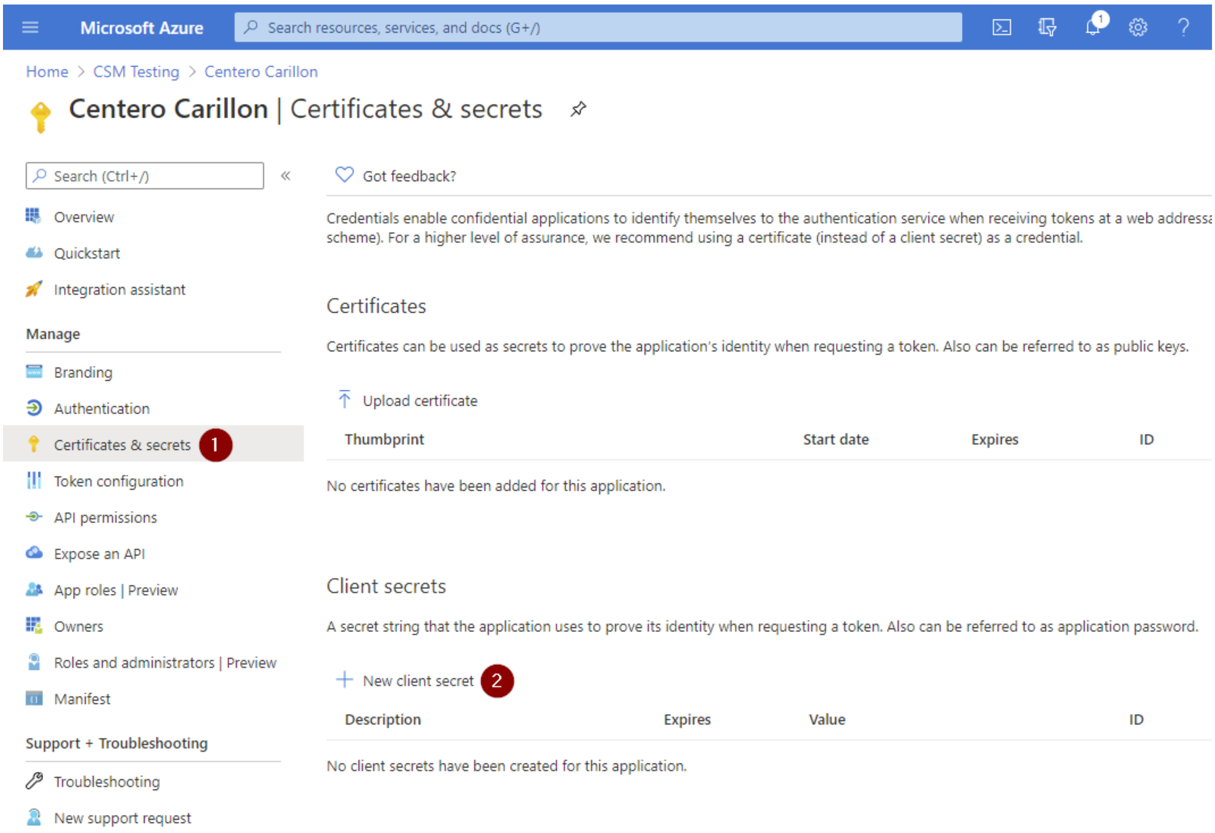
Web | e.g. https://example.com/auth

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

By proceeding, you agree to the Microsoft Platform Policies

Register

3. Specify **name** for the application (for example Centero Carillon) and then click **Register**



Centero Carillon | Certificates & secrets

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressa 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

No certificates have been added for this application.

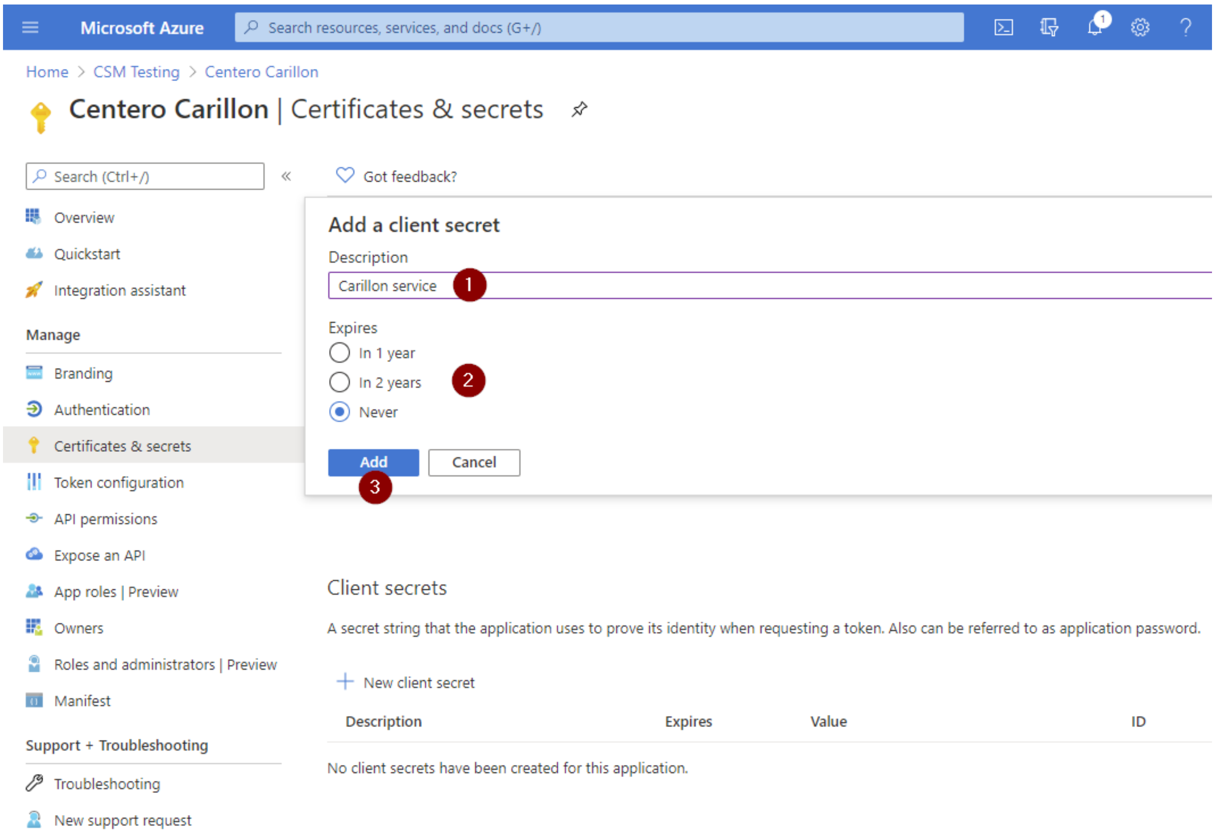
Client secrets

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	ID

No client secrets have been created for this application.

4. After App is registered click **Certificates & secrets** and then click **New client secret**



Centero Carillon | Certificates & secrets

Add a client secret

Description: Carillon service

Expires
○ In 1 year
○ In 2 years
● Never

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

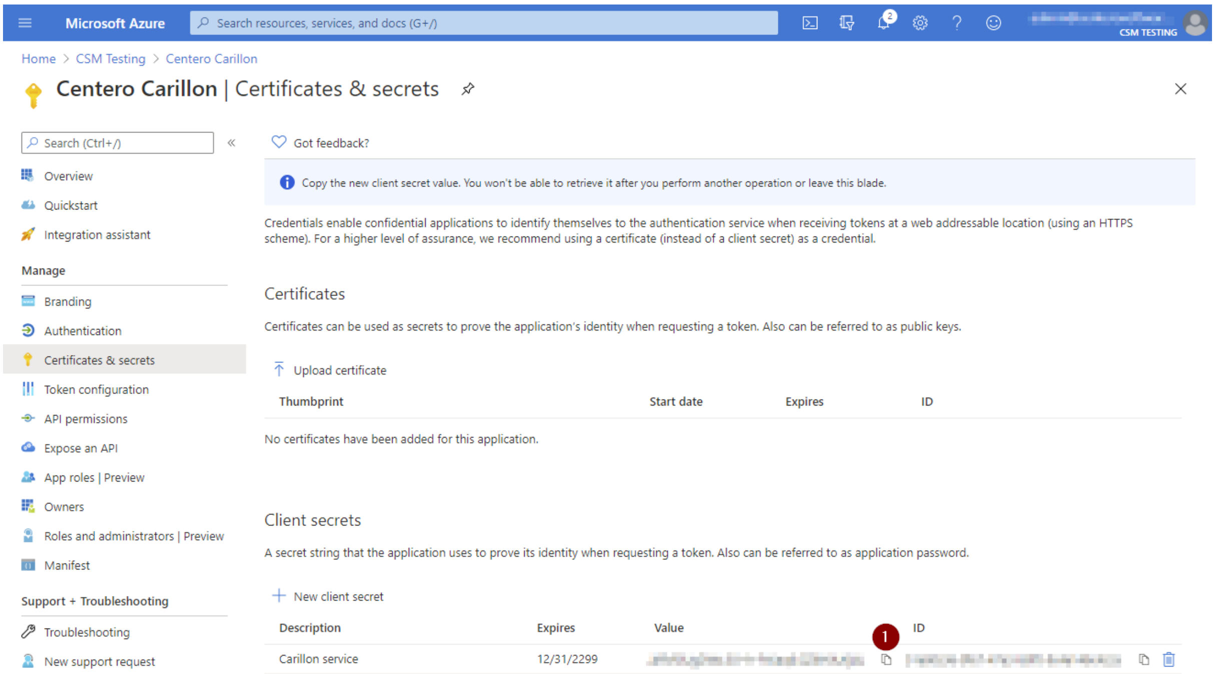
No client secrets have been created for this application.

5. Specify **description** for the secret (for example Carillon service), then **select validity time** for the secret and then click **Add**

Note!

If you select validity time other than **Never**, you must create new client secret before current expires and then change client secret also to Centero Carillon management portal to Azure AD directory

6. After secret is created DO NOT navigate way from the page before you have completed next step!



Centero Carillon | Certificates & secrets

Copy the new client secret value. You won't be able to retrieve it after you perform another operation or leave this blade.

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.

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

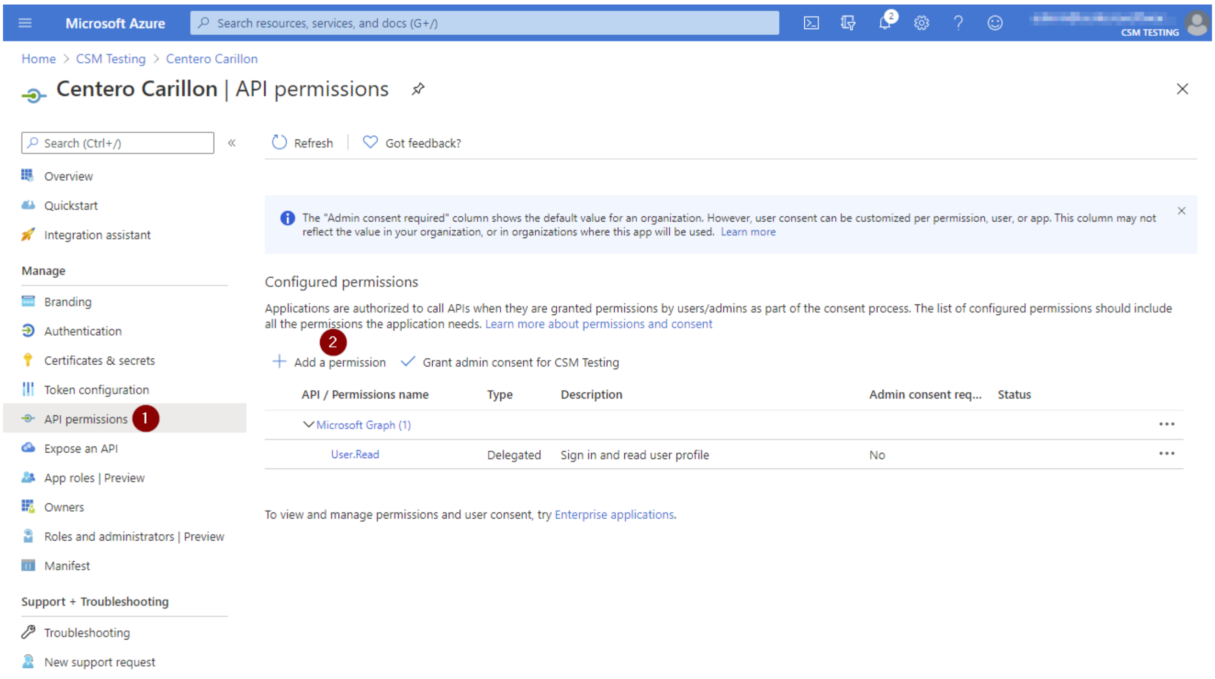
No certificates have been added for this application.

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	ID
Carillon service	12/31/2299	[redacted]	[redacted]

7. **Copy** client secret value to clipboard and save the value to secure location (if you need to access client secret later). You are not able to see client secret after you have navigated away from the page. Also Carillon management portal will not show you the client secret and you will need to specify client secret always when you modify your Azure AD directory in Carillon (for example if you want to change the display name of the Azure AD tenant in Carillon).



Microsoft Azure

Search resources, services, and docs (G+/)

[redacted] CSM TESTING

Home > CSM Testing > Centero Carillon

Centero Carillon | API permissions

Search (Ctrl+/)

- Overview
- Quickstart
- Integration assistant

Manage

- Branding
- Authentication
- Certificates & secrets
- Token configuration
- API permissions 1
- Expose an API
- App roles | Preview
- Owners
- Roles and administrators | Preview
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

Refresh | Got feedback?

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

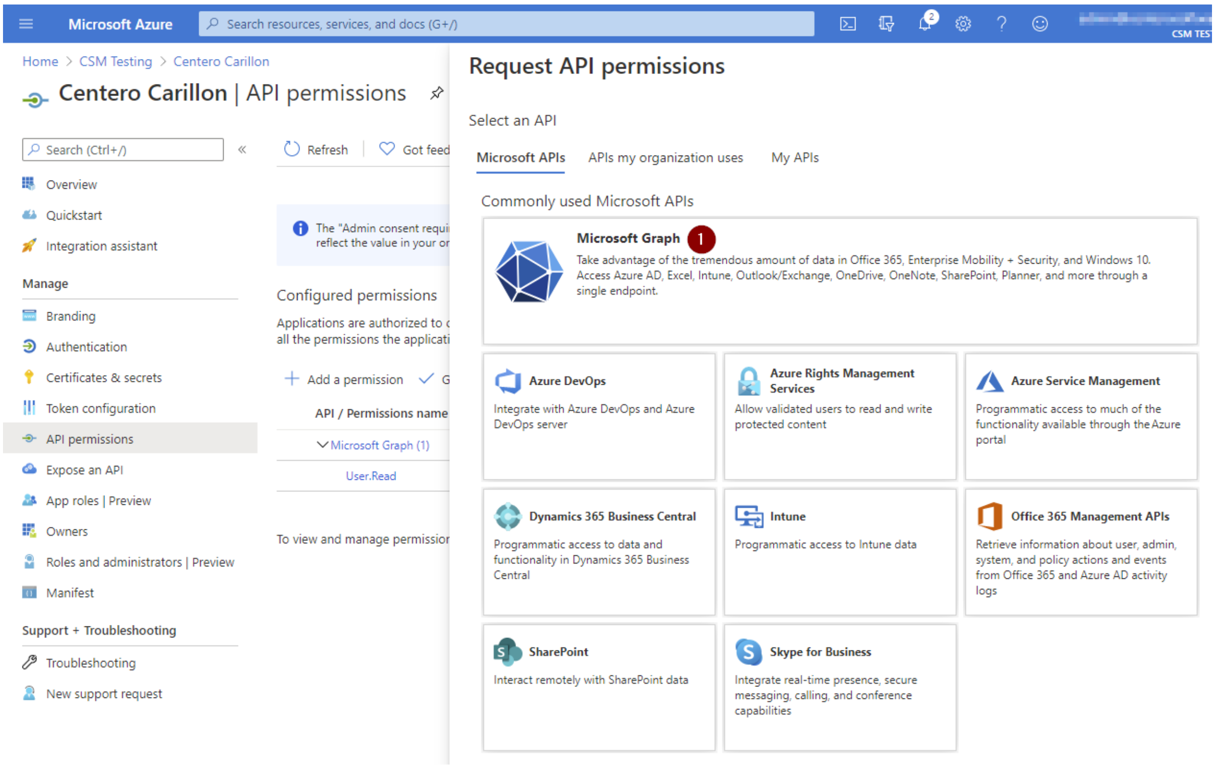
2

+ Add a permission ✓ Grant admin consent for CSM Testing

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 permissions and user consent, try Enterprise applications.

8. Click **API permissions** and then click **Add a permission**



Microsoft Azure

Search resources, services, and docs (G+/)

[redacted] CSM TEST

Request API permissions

Select an API

Microsoft APIs | APIs my organization uses | My APIs

Commonly used Microsoft APIs

Microsoft Graph 1
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 DevOps
Integrate with Azure DevOps and Azure DevOps server

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

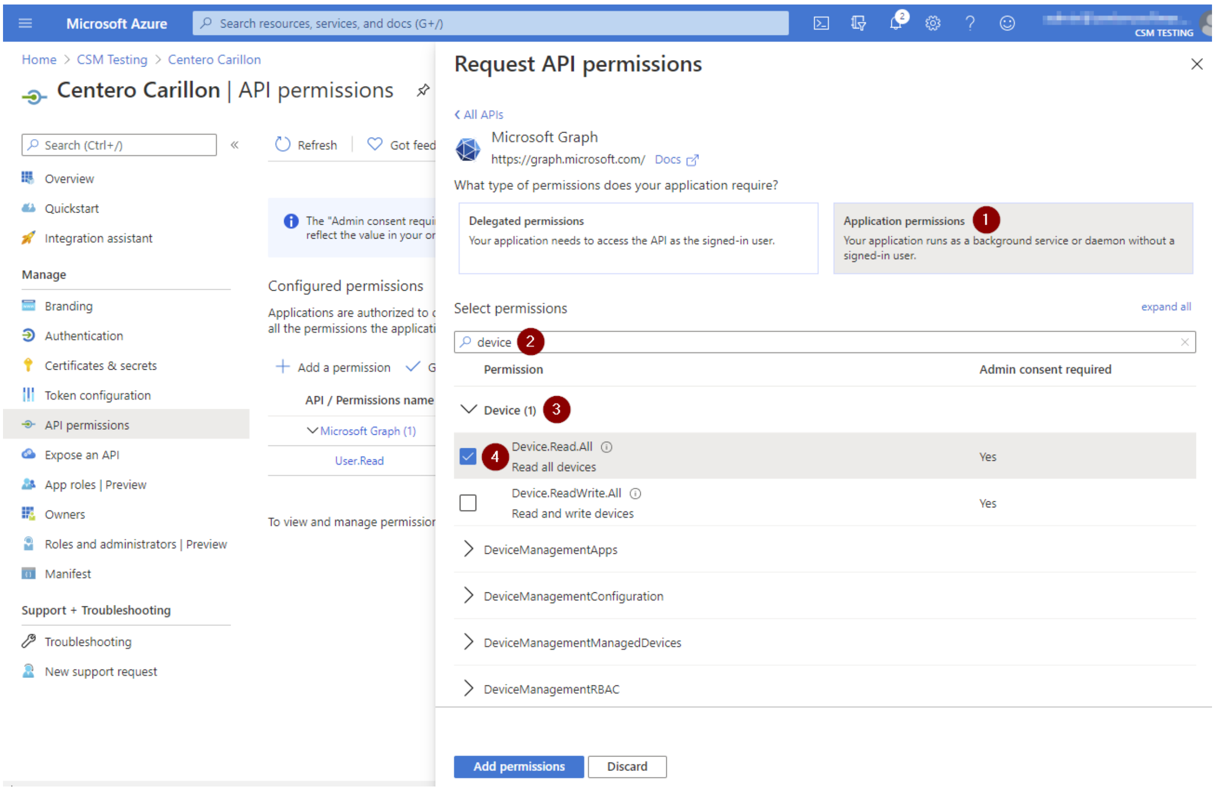
Intune
Programmatic access to Intune data

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

SharePoint
Interact remotely with SharePoint data

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

9. Click **Microsoft Graph**



Centero Carillon | API permissions

The "Admin consent requi… reflect the value in your or…

Configured permissions

Applications are authorized to c… all the permissions the applicati…

To view and manage permission…

Request API permissions

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

What type of permissions does your application require?

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

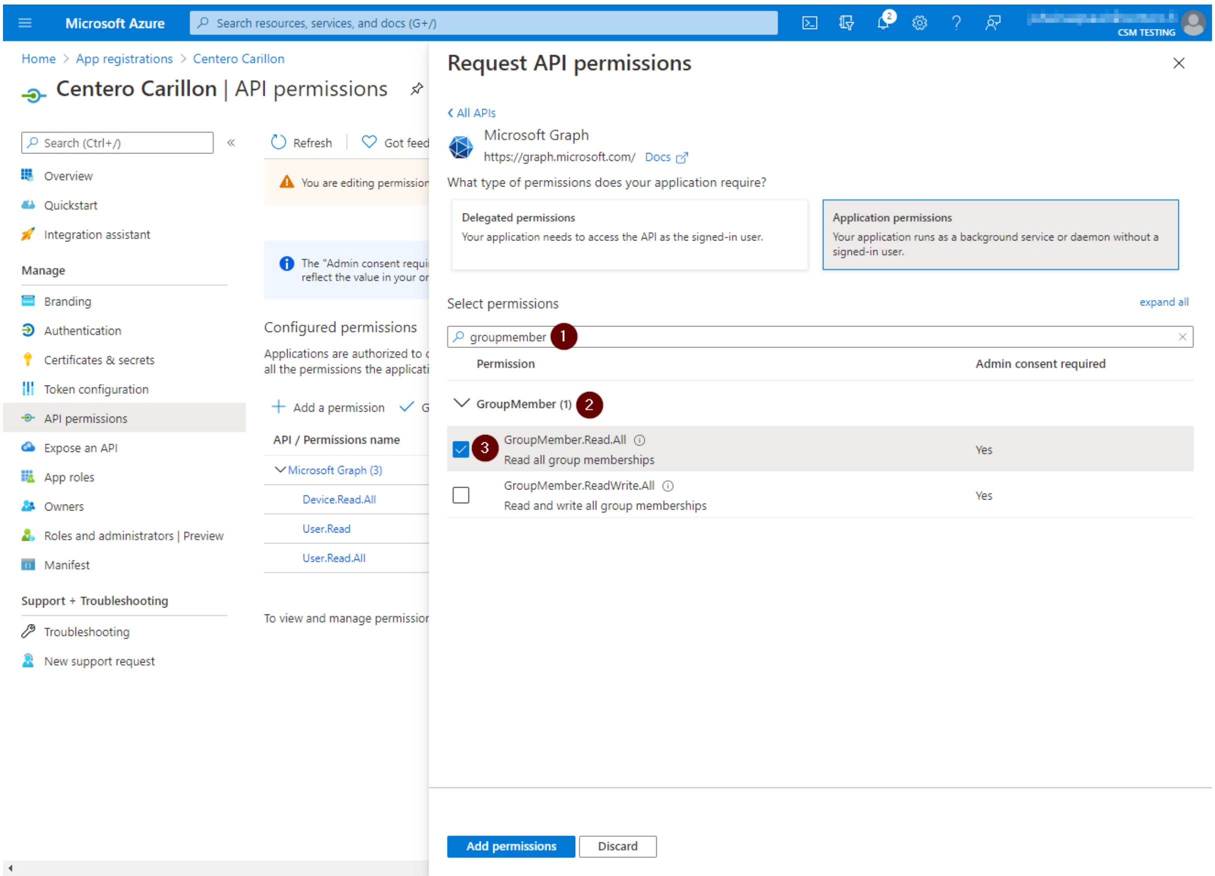
Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions

device

	Permission	Admin consent required
	Device (1)	
☑	Device.Read.All Read all devices	Yes
□	Device.ReadWrite.All Read and write devices	Yes
	DeviceManagementApps	
	DeviceManagementConfiguration	
	DeviceManagementManagedDevices	
	DeviceManagementRBAC	

10. Click **Application permissions**, then type '**device**' in search permissions field, **expand Device** and then select **Device.Read.All**



Centero Carillon | API permissions

You are editing permission…

The "Admin consent requi… reflect the value in your or…

Configured permissions

Applications are authorized to c… all the permissions the applicati…

To view and manage permission…

Request API permissions

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

What type of permissions does your application require?

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

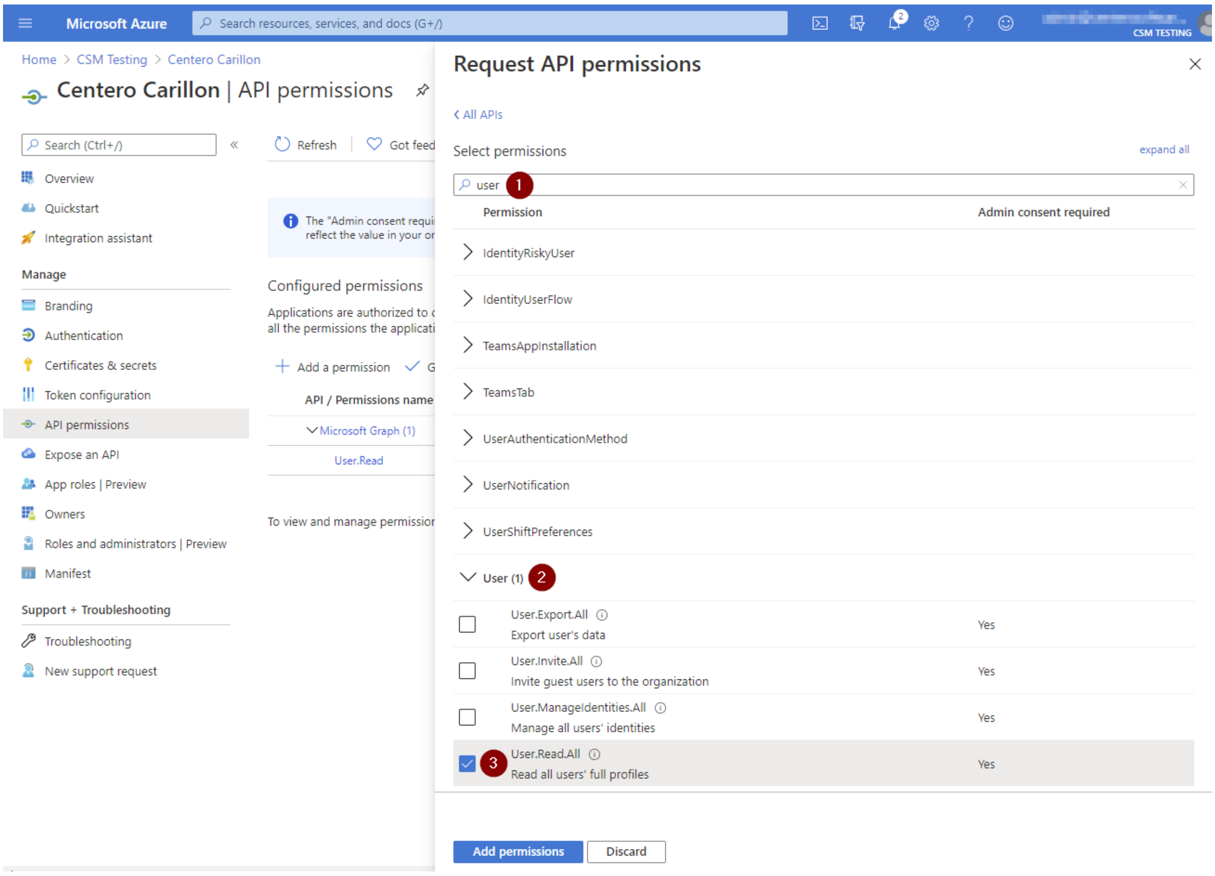
Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions

groupmember

	Permission	Admin consent required
	GroupMember (1)	
☑	GroupMember.Read.All Read all group memberships	Yes
□	GroupMember.ReadWrite.All Read and write all group memberships	Yes

11. Replace search permission value to '**groupmember**', **expand GroupMember** and then select **GroupMember.Read.All**



Home > CSM Testing > Centero Carillon

Centero Carillon | API permissions

Refresh | Got feed

The "Admin consent requi
reflect the value in your or

Configured permissions

Applications are authorized to c
all the permissions the applicati

Add a permission ✓ G

API / Permissions name
Microsoft Graph (1)
User.Read

To view and manage permission

Request API permissions

< All APIs

Select permissions

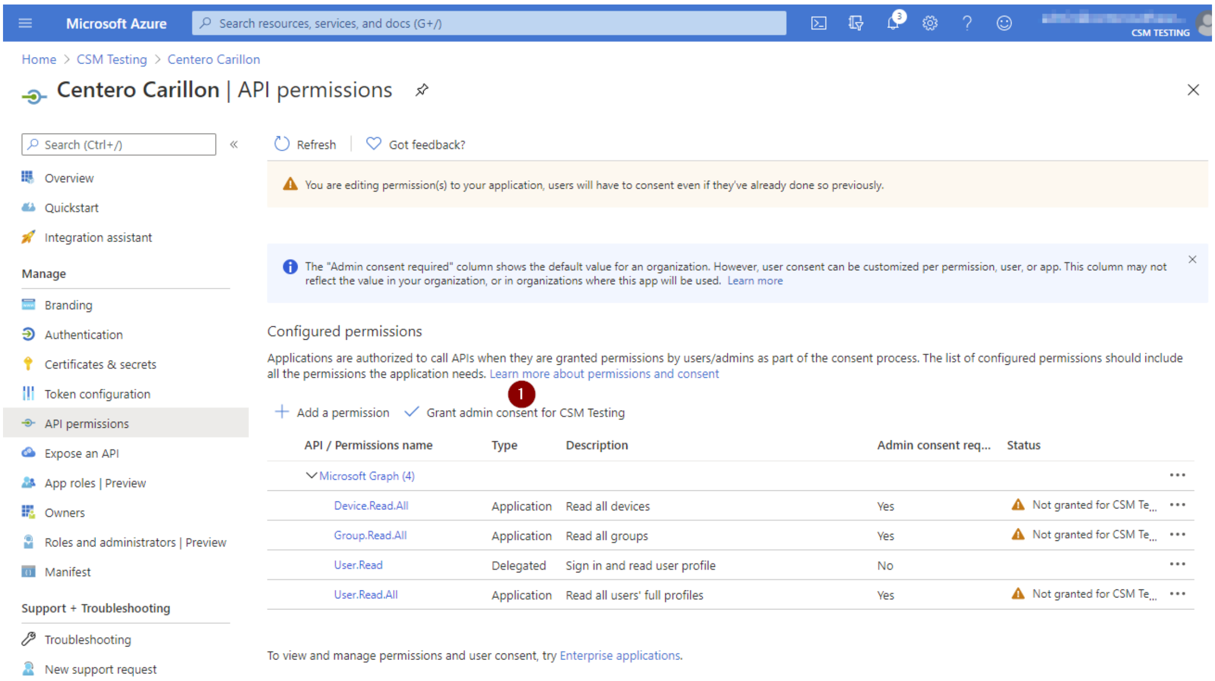
expand all

user 1

Permission	Admin consent required
> IdentityRiskyUser	
> IdentityUserFlow	
> TeamsAppInstallation	
> TeamsTab	
> UserAuthenticationMethod	
> UserNotification	
> UserShiftPreferences	
∨ User (1) 2	
□ 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
☑ 3 User.Read.All ⓘ Read all users' full profiles	Yes

Add permissions | Discard

12. Replace search permission value to '**user**', **expand User**, select **User.Read.All** and then click **Add permissions**



Home > CSM Testing > Centero Carillon

Centero Carillon | API permissions

Refresh | Got feedback?

You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

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

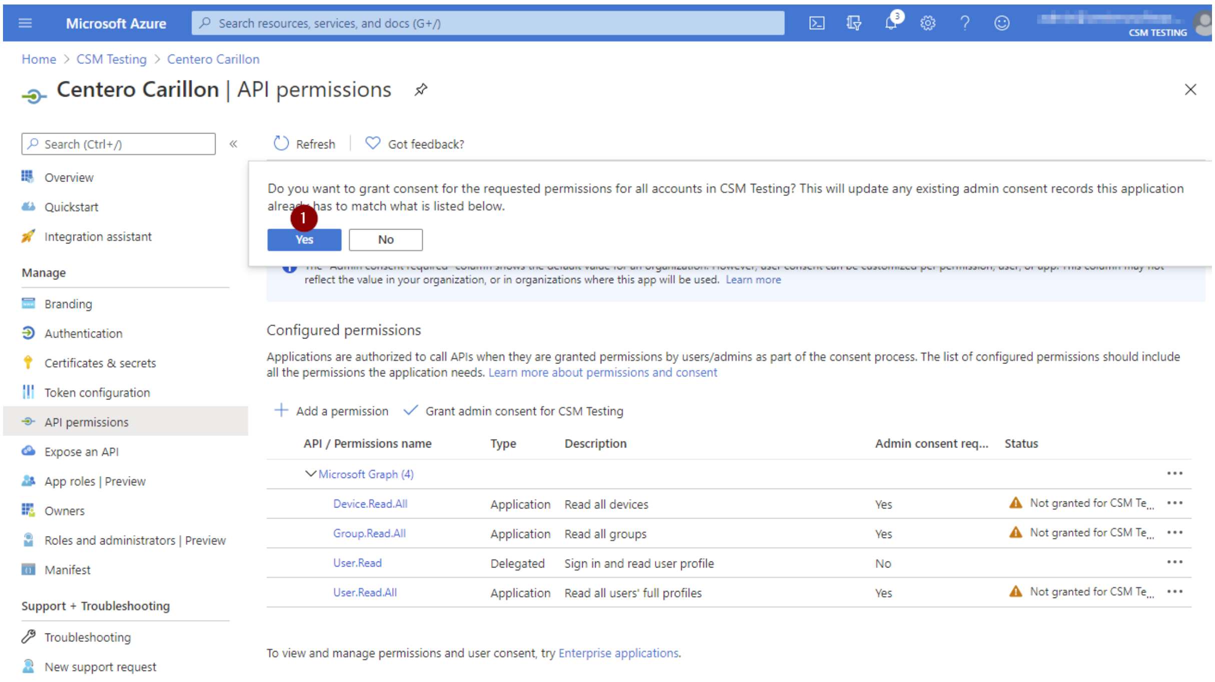
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

Add a permission ✓ Grant admin consent for CSM Testing 1

API / Permissions name	Type	Description	Admin consent req...	Status
∨ Microsoft Graph (4)				
Device.Read.All	Application	Read all devices	Yes	⚠ Not granted for CSM Te...
Group.Read.All	Application	Read all groups	Yes	⚠ Not granted for CSM Te...
User.Read	Delegated	Sign in and read user profile	No	
User.Read.All	Application	Read all users' full profiles	Yes	⚠ Not granted for CSM Te...

To view and manage permissions and user consent, try Enterprise applications.

13. Verify that you have added **three** permissions where type is **Application** and permission values have **Device.Read.All**, **Group.Read.All** and **User.Read.All** and then click **Grant admin consent for <your tenant name>**


Microsoft Azure
Search resources, services, and docs (G+/)
CSM TESTING
Home > CSM Testing > Centero Carillon

Centero Carillon | API permissions

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

reflect the value in your organization, or in organizations where this app will be used. Learn more

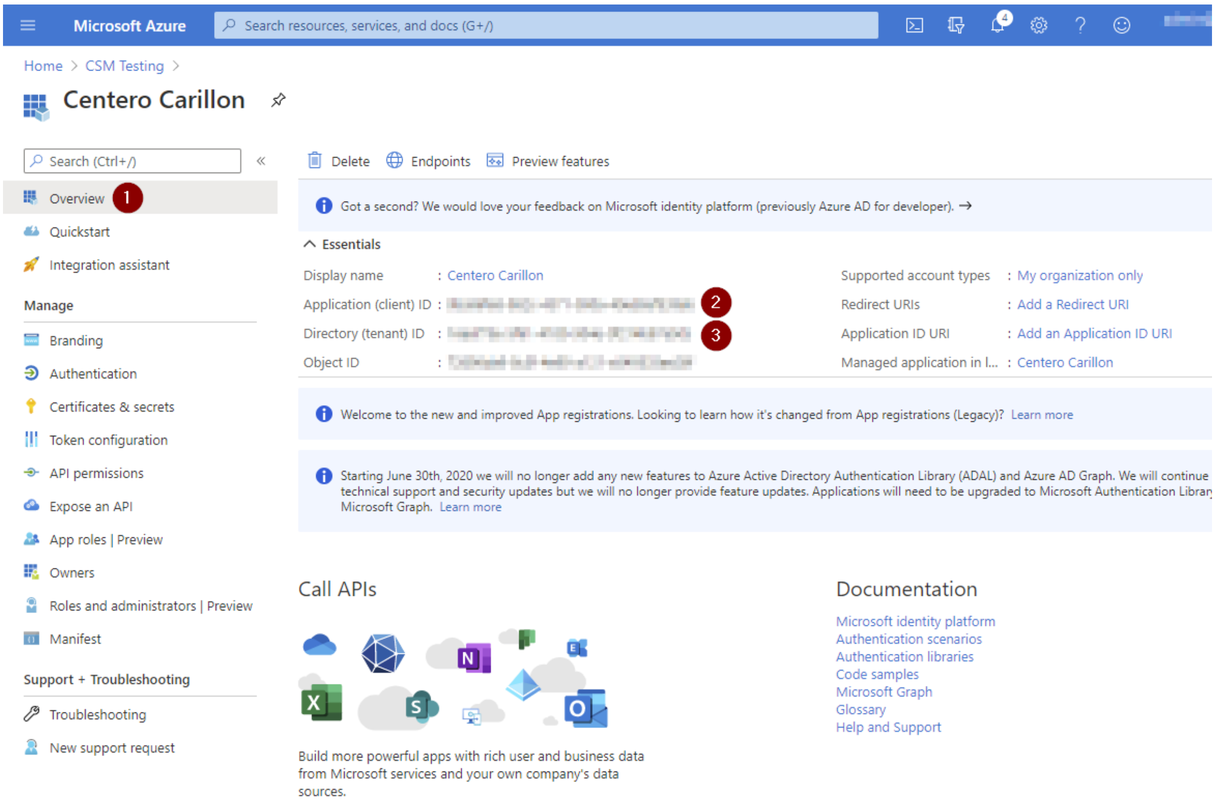
Configured permissions

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 (4)				
Device.Read.All	Application	Read all devices	Yes	Not granted for CSM Te...
Group.Read.All	Application	Read all groups	Yes	Not granted for CSM Te...
User.Read	Delegated	Sign in and read user profile	No	
User.Read.All	Application	Read all users' full profiles	Yes	Not granted for CSM Te...

To view and manage permissions and user consent, try Enterprise applications.

14. Click **Yes**



Centero Carillon

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Essentials

Display name : Centero Carillon
Application (client) ID : [redacted]
Directory (tenant) ID : [redacted]
Object ID : [redacted]
Supported account types : My organization only
Redirect URIs : Add a Redirect URI
Application ID URI : Add an Application ID URI
Managed application in l... : Centero Carillon

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

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 technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Librar Microsoft Graph. 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

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

15. Click **Overview** and take note of **Application (client) ID** and **Directory (tenant) ID**. **Client secret** was noted earlier. These values are required when configuring Centero Carillon

2. Carillon configuration

After Azure AD App Registration is done and you have **Application (client) ID**, **Directory (tenant) ID** and **Client secret** available you can continue to add your Azure AD tenant to Carillon

- Open your Carillon management portal and use these instructions to add new Azure AD

- Create management rules that target Azure AD groups or devices

3. Client update

Make sure that your endpoints are using Centero Carillon client version **3.1.5014** or later