

Configuration of Microsoft 365 for Calendars access

You expect to display your meeting rooms planning on your screen running with zebrix signage ?

This guide explains how to register a new application in Microsoft 365 for use with calendar integrations in **zebrix signage**. You will create an app, add a client secret, and assign it the **Calendars.Read** application permission. Then, you'll share the required details to the zebrix technical team and finally a secret UUID will be returned to you to be used in the widget configuration.



Please note that a Microsoft 365 Global Admin account is required to complete this configuration



This tutorial is a straightforward approach that grants application-wide **permissions to all resources and users calendars**. It is the easiest to implement this, using only the Microsoft Entra Admin Center, making it suitable for quick setups. However, **restricting permissions to specific resources** by scoping them to groups is an approach that is **more secured and recommended**. It involves combining the Microsoft Entra Admin Center for initial setup with PowerShell commands to apply scoping that will not be covered in this tutorial.

1. Accessing App Registrations

1. Go to the Microsoft Entra admin center: <https://entra.microsoft.com/>
2. In the left menu, select **"Applications" > "App registrations"**.
3. Click **"New registration"** at the top of the page.



2. Registering the App

1. **Name:** Enter zebrix signage calendars connector (you are free to choose the name you want)
2. **Supported account types:** Choose “Accounts in this organizational directory only” (default).
3. Leave the **Redirect URI** empty.
4. Click “**Register**” to create the application.

Microsoft Entra admin center

Home > Enterprise applications | All applications > Browse Microsoft Entra Gallery > App registrations >

Register an application

Name

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

zebrix signage calendars connector 1

Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory only ☐ only - Single tenant 2

☐ 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...](#)

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.

Select a platform

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

3. Save details and create a Client Secret

1. Save the details that need to be provided to zebrix's technical team:

1. **Application (client) ID**

2. **Directory (tenant) ID**

2. Click on **Add a certificate or secret**.

Microsoft Entra admin center

Home >

zebrix signage calendars connector

Search

Delete Endpoints Preview features

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Essentials

Display name : zebrix signage calendars connector

Application (client) ID : 84204485-2f70 1

Object ID : f93ca51f-968e-4...

Directory (tenant) ID : 35fdbb4d-20f1-4... 2

Client credentials [Add a certificate or secret](#) 3

Redirect URIs : [Add a Redirect URI](#)

Application ID URI : [Add an Application ID URI](#)

Managed application in L... : zebrix signage calendars connector

Supported account types : My organization only

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 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](#)

[Get Started](#) [Documentation](#)

- Add a description, for example zebrix connector secret.
- Set an appropriate expiration (24 months is recommended).



When the secret will expire, zebrix will not have access to your calendars anymore and display their details on screen. You'll have to create a new secret and provide it to zebrix. We invite you to create an event in your personal calendar at



the end of the validity period of the secret.

- Click **“Add”** and copy the generated value immediately. **You will not be able to retrieve it again.**

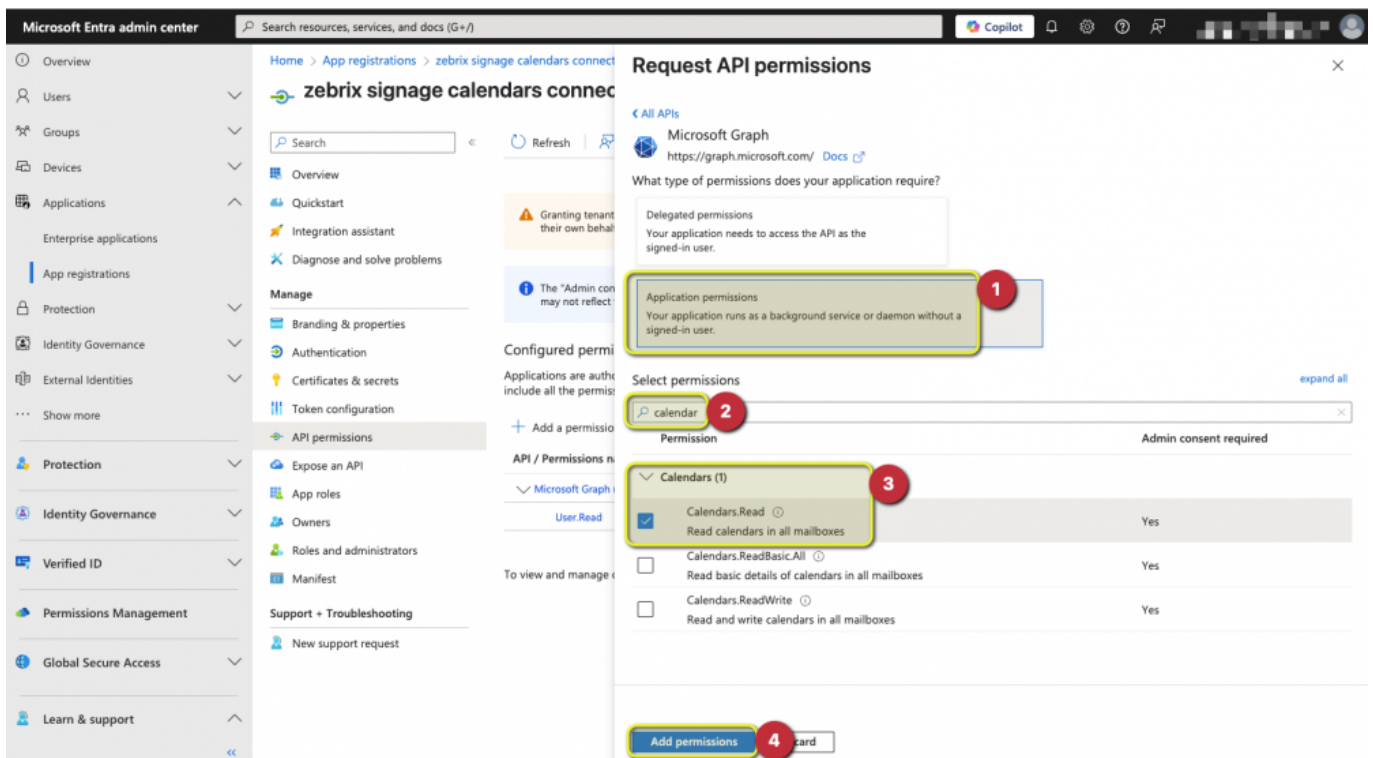
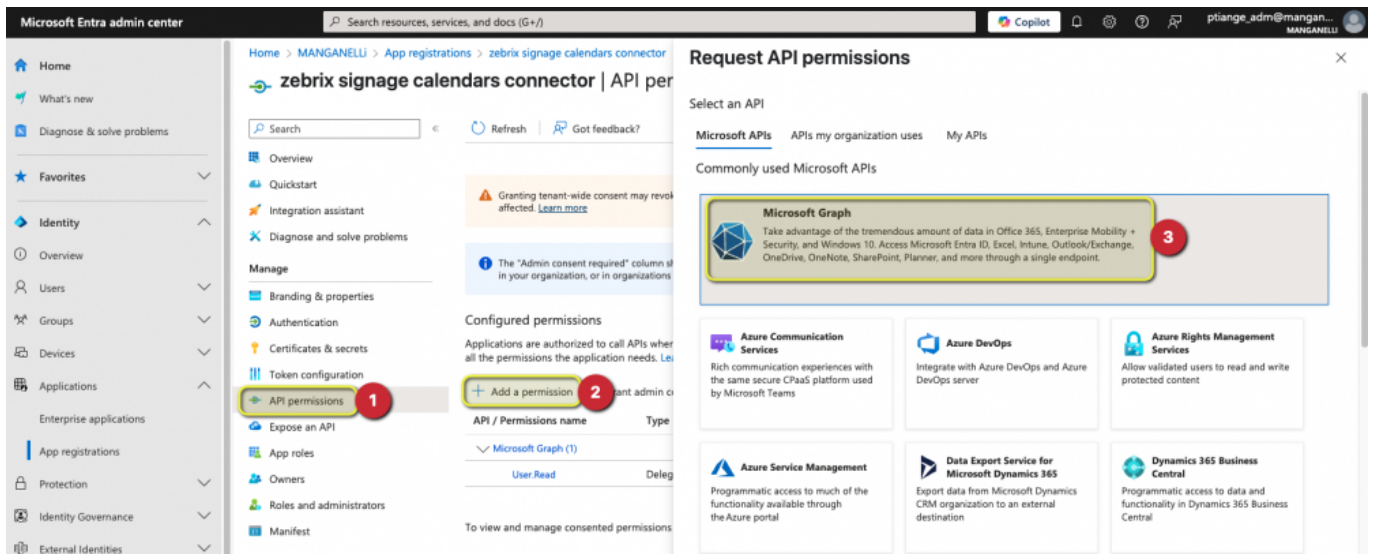
The screenshot shows the Microsoft Entra admin center interface. On the left is the navigation pane with categories like Identity, Protection, and Identity Governance. The main pane shows the 'zebrix signage calendars connector' under 'Certificates & secrets'. A 'Add a client secret' dialog is open on the right. The dialog has two input fields: 'Description' (containing 'zebrix') and 'Expires' (set to '730 days (24 months)'). At the bottom of the dialog are 'Add' and 'Cancel' buttons. Red numbered callouts (1-4) highlight the 'New client secret' button, the 'Description' field, the 'Expires' dropdown, and the 'Add' button respectively.

This screenshot shows the same Microsoft Entra admin center interface, but now the 'Client secrets' tab is active. It displays a table with one client secret. The 'Value' column contains a long alphanumeric string. A red numbered callout (1) highlights this value. The 'Secret ID' column shows a shorter alphanumeric string. The 'Expires' column shows the date '13/06/2027'. The 'Description' column shows 'zebrix'. Above the table, there is a '+ New client secret' button and a message: 'A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.'

4. Adding API Permissions

- Go to **“API permissions”** in the left menu.
- Click **“Add a permission”**.
- Select **Microsoft Graph**.
- Choose **Application permissions**.

5. In the search bar, type **Calendars.Read**.
6. Check **Calendars.Read** under the **Calendars** section.
7. Click **"Add permissions"**.
8. Back on the API permissions page, click **"Grant admin consent"** and confirm.



5. Summary

You now have:

1. Registered an application named **"zebrix signage calendars connector"**.
2. Generated a client secret to authenticate your backend app.
3. Granted **Calendars.Read** application-level permission to access calendars in your organization.

Next Steps

Use the **Application (client) ID**, **Directory (tenant) ID**, and **Client secret** in your integration code to authenticate using the OAuth 2.0 client credentials flow.

From:
<https://documentation.zebrix.net/> - **zebrix documentation**

Permanent link:
https://documentation.zebrix.net/doku.php?id=en:m365_graphapi_calendars_read&rev=1750089241

Last update: **2025/06/16 17:54**

