

# Configuration of Microsoft 365 for Calendars access

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

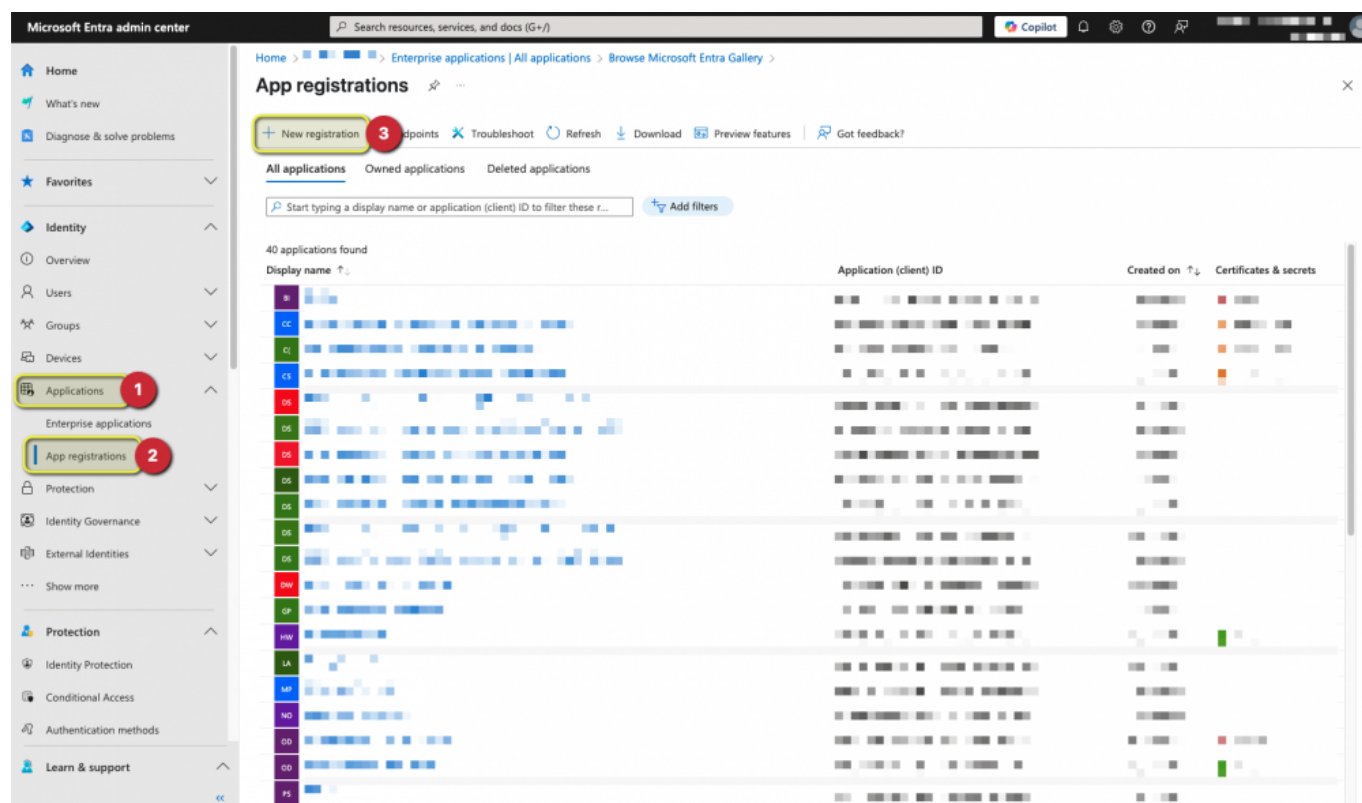
This guide explains how to register a new application in Microsoft 365 for use with calendar integrations in **zebrix signage**. You will create an app, add a client secret, and assign it the **Calendars.Read** application permission. Then, you'll share the required details to the zebrix technical team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

## 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.



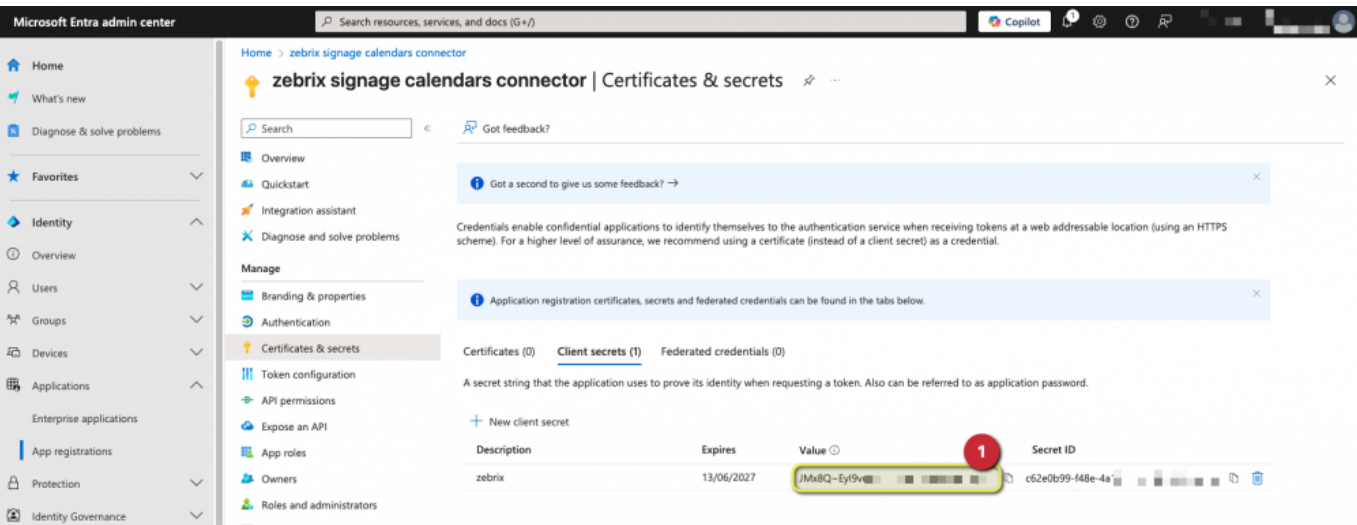
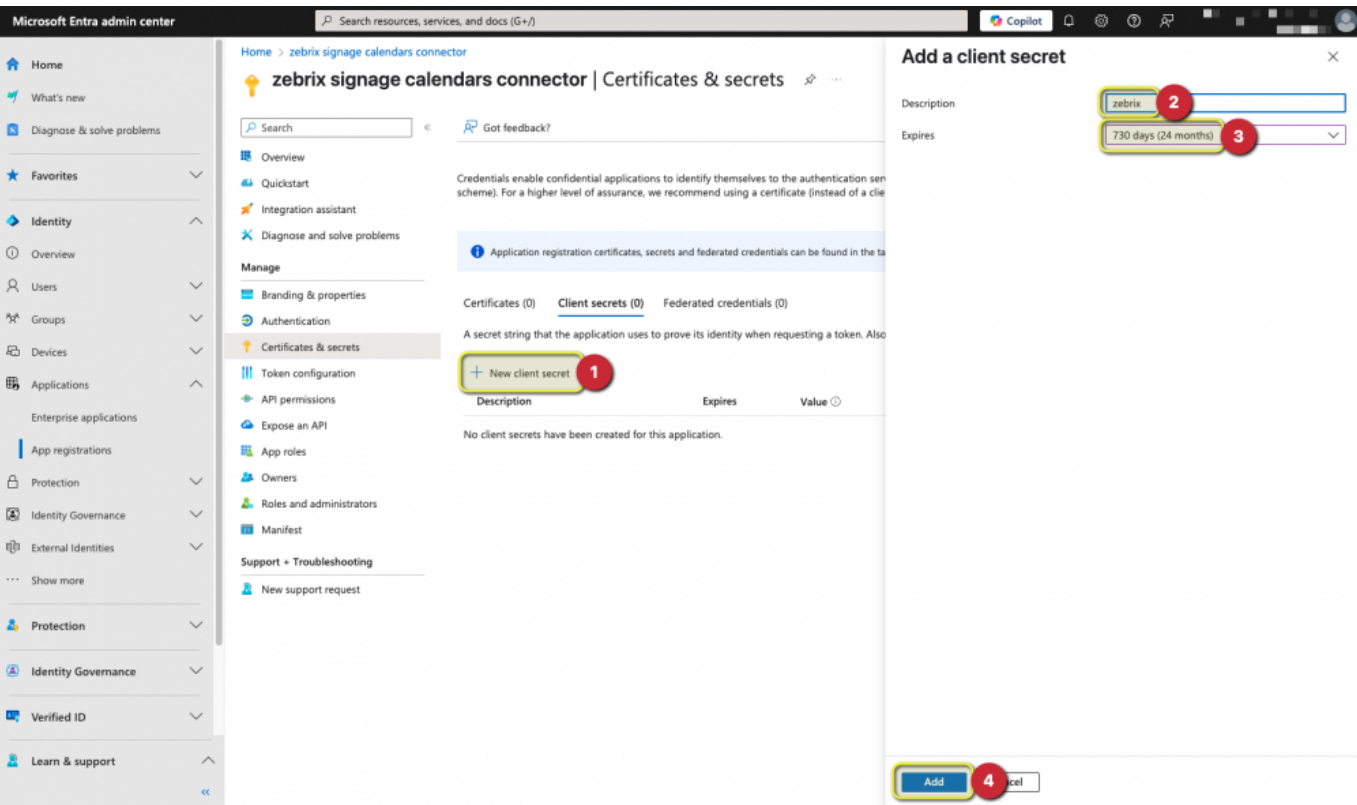
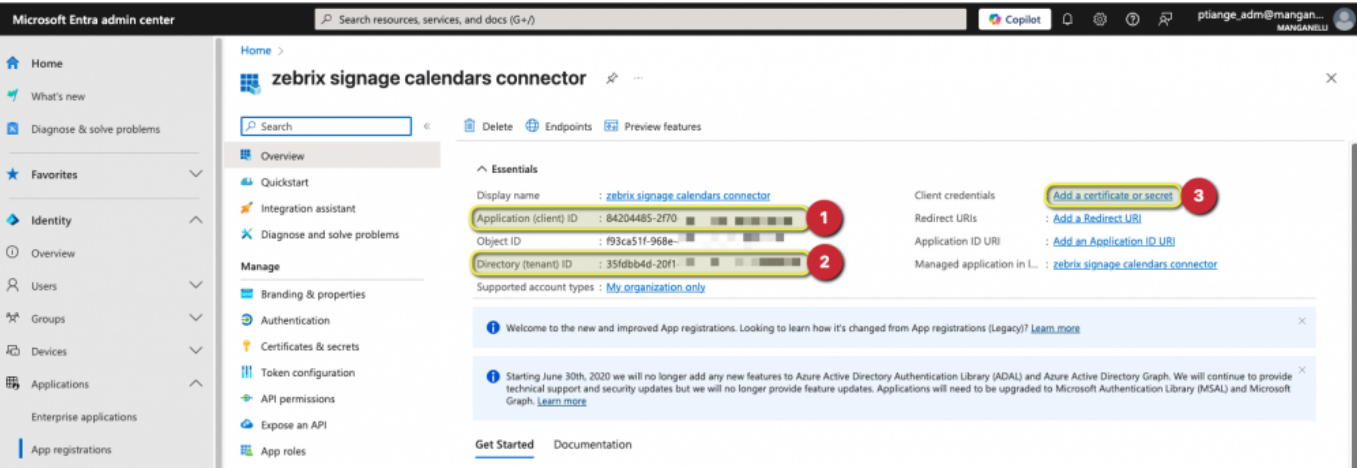
## 2. Registering the App

1. **Name:** Enter zebrix signage calendars connector
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.

The screenshot shows the 'Register an application' page in the Microsoft Entra admin center. The left sidebar contains navigation links for Home, What's new, Diagnose & solve problems, Favorites, Identity, Overview, Users, Groups, Devices, Applications, Enterprise applications, App registrations, Protection, Identity Governance, External Identities, Show more, Protection, Identity Protection, Conditional Access, Authentication methods, and Learn & support. The main content area is titled 'Register an application'. It has a search bar at the top with the text 'Search resources, services, and docs (G+I)'. Below the search bar, there's a breadcrumb trail: Home > Enterprise applications > All applications > Browse Microsoft Entra Gallery > App registrations. The 'Name' field is labeled 'Name' and has a description: 'The user-facing display name for this application (this can be changed later)'. The value 'zebrix signage calendars connector' is entered in the field. The 'Supported account types' section is titled 'Supported account types' and has a description: 'Who can use this application or access this API?'. There are three radio button options: 'Accounts in this organizational directory only' (selected), 'Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)', and 'Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)'. The 'Redirect URI (optional)' section has a description: '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.' There is a dropdown menu for 'Select a platform' and a text input field with the value 'e.g. https://example.com/auth'. At the bottom of the page, there is a blue button labeled 'Register'.

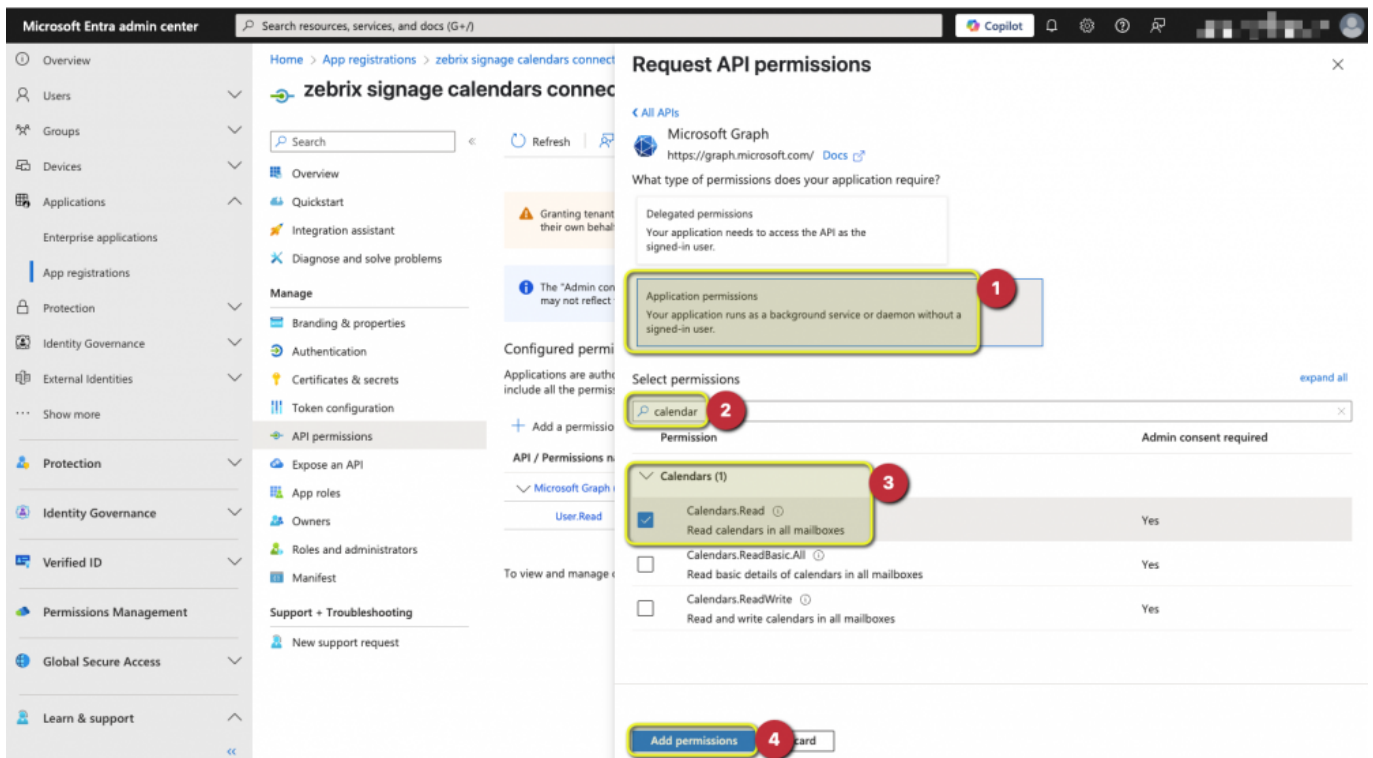
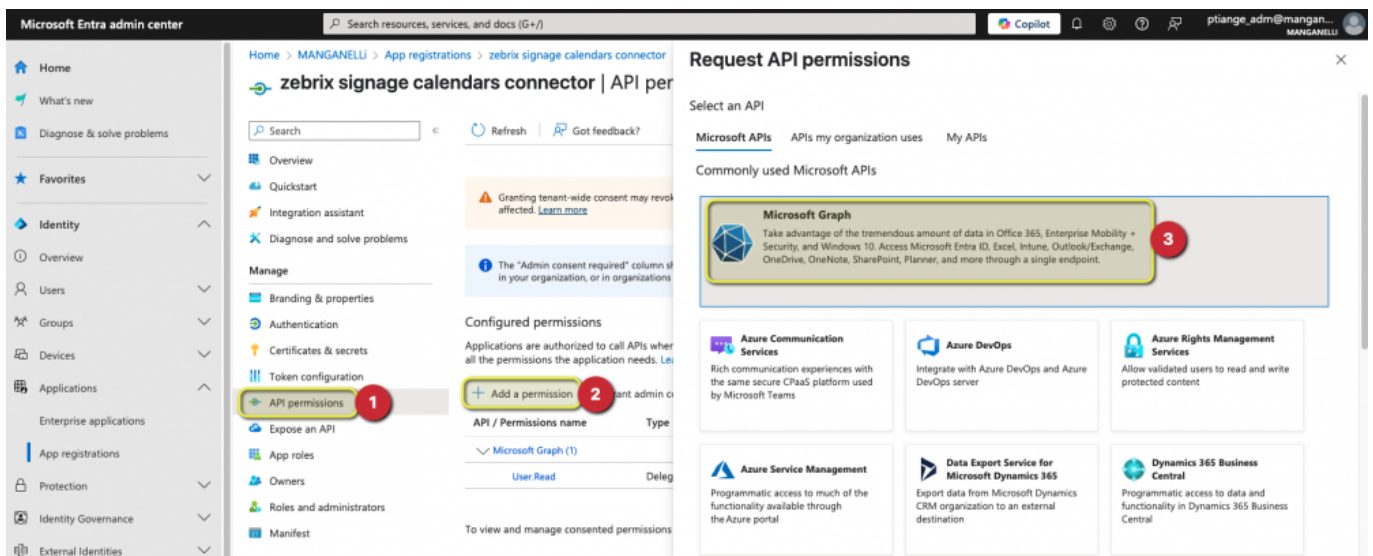
## 3. Creating a Client Secret

1. In the app overview, select “**Certificates & secrets**”.
2. Under **Client secrets**, click “**New client secret**”.
3. Add a description, for example zebrix connector secret.
4. Set an expiration (recommended: 6 or 12 months).
5. Click “**Add**” and copy the generated value immediately. **You will not be able to retrieve it again.**



## 4. Adding API Permissions

1. Go to **"API permissions"** in the left menu.
2. Click **"Add a permission"**.
3. Select **Microsoft Graph**.
4. 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=1750088439](https://documentation.zebrix.net/doku.php?id=en:m365_graphapi_calendars_read&rev=1750088439)

Last update: **2025/06/16 17:40**

