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.



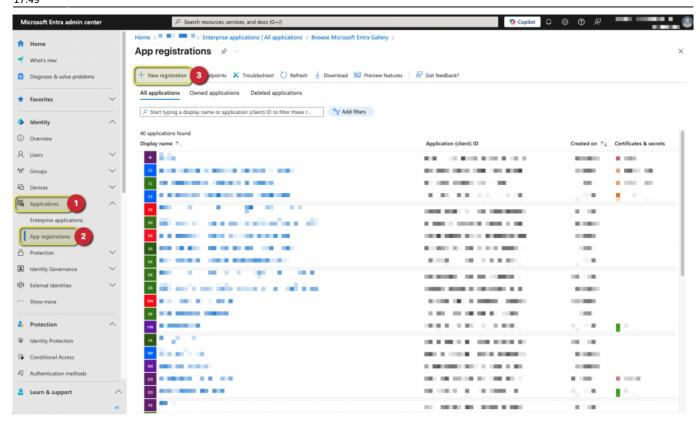
Please note that a Microsoft 365 Global Admin account is required to complete this configuration



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.

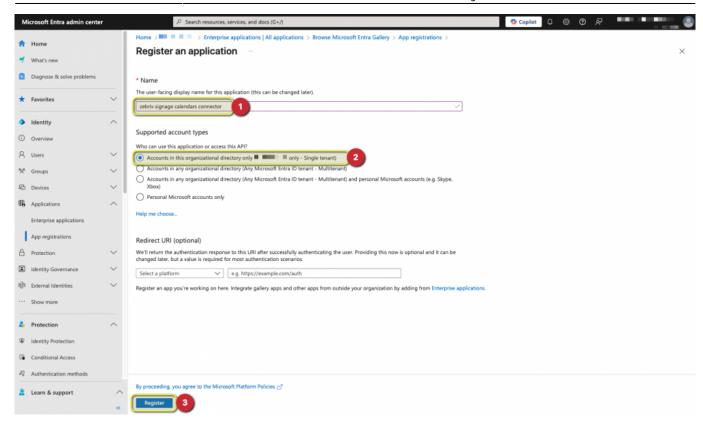
1. Accessing App Registrations

- 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.



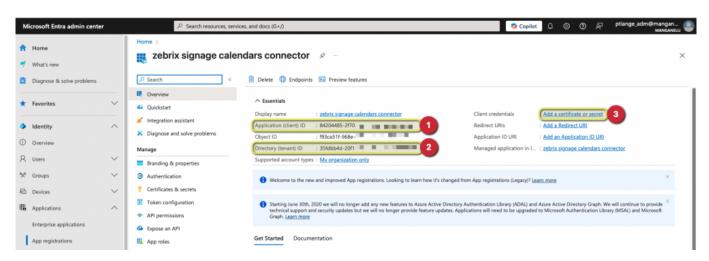
2. Registering the App

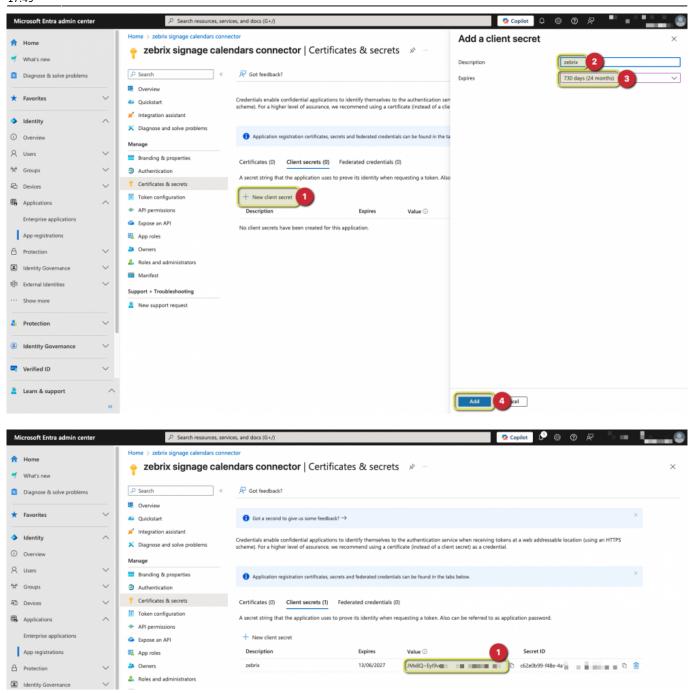
- 1. **Name**: Enter zebrix signage calendars connector (you are free to choose the name you want)
- 2. Supported account types: Choose "Accounts in this organizational directory only" (default).
- 3. Leave the **Redirect URI** empty.
- 4. Click "Register" to create the application.



3. Save details and create a Client Secret

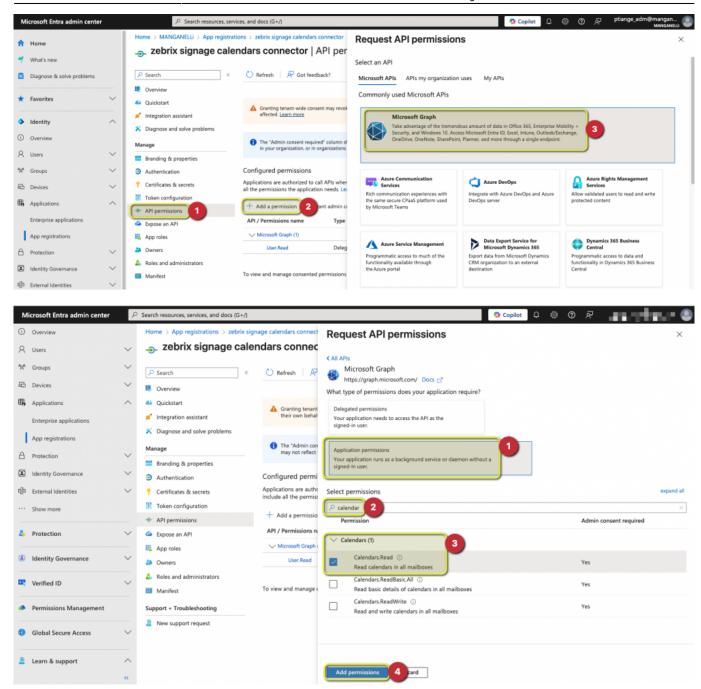
- 1. Save the details that need to be provided to zebrix's technical team:
 - 1. Application (client) ID
 - 2. Directory (tenant) ID
- 2. In the app overview, select "Certificates & secrets".
- 3. Under Client secrets, click "New client secret".
- 4. Add a description, for example zebrix connector secret.
- 5. Set an expiration (recommended: 6 or 12 months).
- 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=1750088976

Last update: 2025/06/16 17:49

