

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 (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: [dropdown] 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)

3. Save details and create a Client Secret

- Save the details that need to be provided to zebrix's technical team:
 - Application (client) ID**
 - Directory (tenant) ID**
- In the app overview, select **"Certificates & secrets"**.
- Under **Client secrets**, click **"New client secret"**.
- Add a description, for example zebrix connector secret.
- 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.**

Microsoft Entra admin center

Home > zebrix signage calendars connector

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

Overview

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-960e- (2)

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

Supported account types: My organization only

Client credentials

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

[Add a Redirect URI](#)

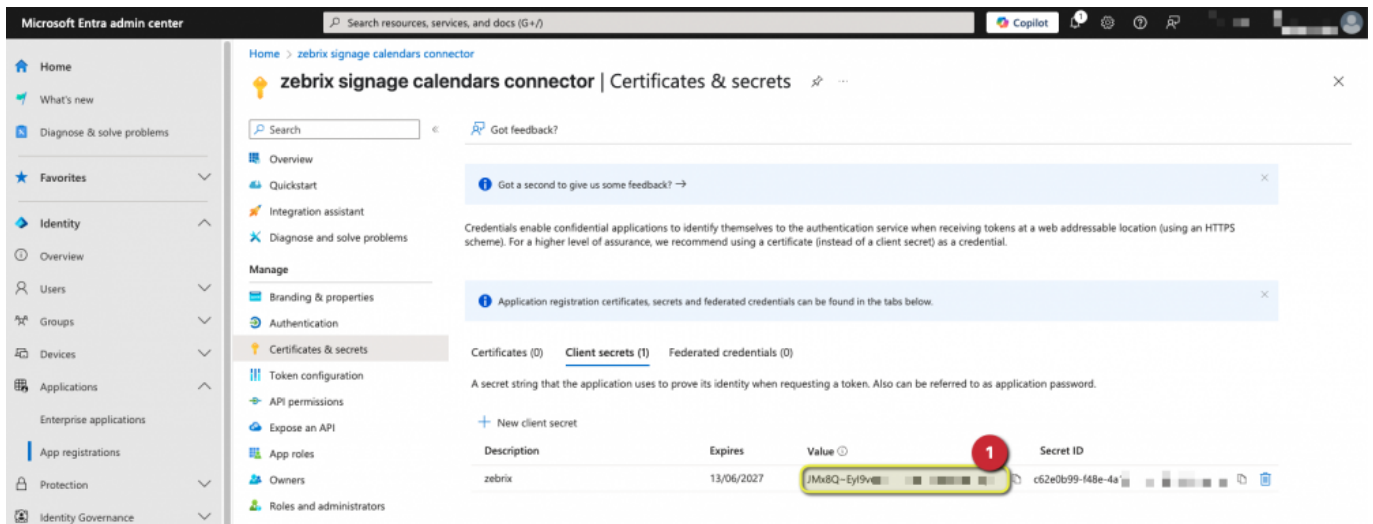
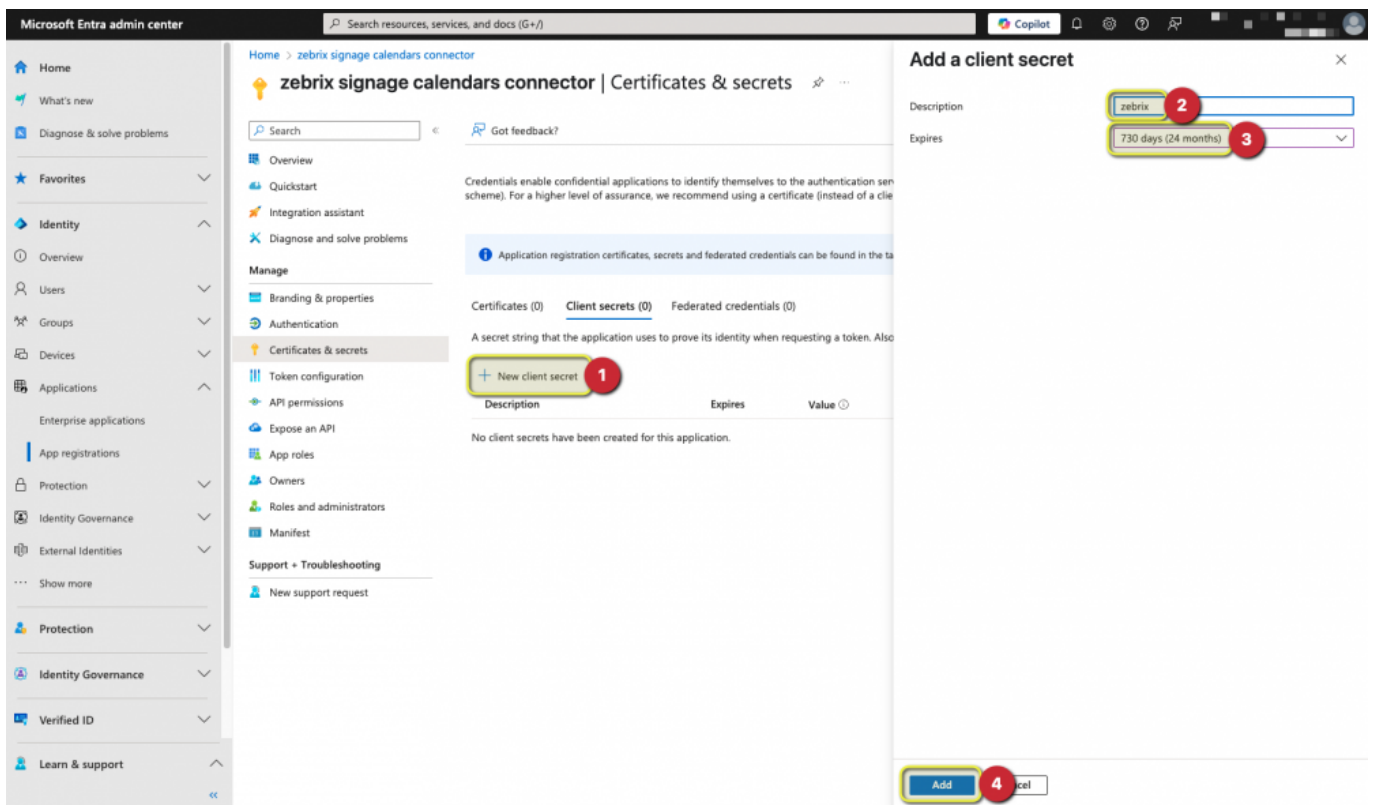
[Add an Application ID URI](#)

Managed application in L: zebrix signage calendars connector

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](#)



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.

The first screenshot shows the 'API permissions' page for the 'zebrix signage calendars connector' application. The 'API permissions' link in the left-hand navigation menu is highlighted with a red circle labeled '1'. The 'Add a permission' button is highlighted with a red circle labeled '2'. The 'Microsoft Graph' API is highlighted with a red circle labeled '3'.

The second screenshot shows the 'Request API permissions' dialog box. The 'Application permissions' tab is selected, highlighted with a red circle labeled '1'. The 'calendar' permission is selected, highlighted with a red circle labeled '2'. The 'Calendars (1)' permission is highlighted with a red circle labeled '3'. The 'Add permissions' button is highlighted with a red circle labeled '4'.

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.

Last
update: en:m365_graphapi_calendars_read https://documentation.zebrix.net/doku.php?id=en:m365_graphapi_calendars_read&rev=1750088976
2025/06/16 17:49

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**

