

How to register an app in Microsoft Entra ID - Microsoft identity platform

By cilwerner


Archived: 2026-04-05 22:37:39 UTC

In this how-to guide, you learn how to register an application in Microsoft Entra ID. This process is essential for establishing a trust relationship between your application and the Microsoft identity platform. By completing this quickstart, you enable identity and access management (IAM) for your app, allowing it to securely interact with Microsoft services and APIs.

- An Azure account that has an active subscription. [Create an account for free.](#)
- The Azure account must be at least a [Application Developer](#).
- A workforce or external tenant. You can use your **Default Directory** for this quickstart. If you need an external tenant, complete [set up an external tenant](#).

Registering your application in Microsoft Entra establishes a trust relationship between your app and the Microsoft identity platform. The trust is unidirectional. Your app trusts the Microsoft identity platform, and not the other way around. Once created, the application object can't be moved between different tenants.

Follow these steps to create the app registration:

1. Sign in to the [Microsoft Entra admin center](#) as at least an [Application Developer](#).
2. If you have access to multiple tenants, use the **Settings** icon  in the top menu to switch to the tenant in which you want to register the application.
3. Browse to **Entra ID > App registrations** and select **New registration**.
4. Enter a meaningful **Name** for your app, for example *identity-client-app*. App users can see this name, and it can be changed at any time. You can have multiple app registrations with the same name.
5. Under **Supported account types**, specify who can use the application. We recommend you select **Accounts in this organizational directory only** for most applications. Refer to the table for more information on each option.

Supported account types	Description
Accounts in this organizational directory only	For <i>single-tenant</i> apps for use only by users (or guests) in <i>your</i> tenant.
Accounts in any organizational directory	For <i>multitenant</i> apps and you want users in <i>any</i> Microsoft Entra tenant to be able to use your application. Ideal for software-as-a-

Supported account types	Description
	service (SaaS) applications that you intend to provide to multiple organizations.
Accounts in any organizational directory and personal Microsoft accounts	For <i>multitenant</i> apps that support both organizational and personal Microsoft accounts (for example, Skype, Xbox, Live, Hotmail).
Personal Microsoft accounts	For apps used only by personal Microsoft accounts (for example, Skype, Xbox, Live, Hotmail).

6. Select **Register** to complete the app registration.

Register an application

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

Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (Contoso AD (dev) 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://myapp.com/auth

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

7. The application's **Overview** page is displayed. Record the **Application (client) ID**, which uniquely identifies your application and is used in your application's code as part of validating the security tokens it receives from the Microsoft identity platform.

The screenshot shows the Microsoft Azure portal interface for an application registration. The top navigation bar includes the Microsoft Azure logo, a search bar, and the user profile 'meganb@contoso.com'. The breadcrumb trail is 'Home > Contoso AD (dev) | App registrations > Contoso App 1'. The main content area is divided into a left-hand navigation pane and a main configuration area. The navigation pane includes sections for 'Overview', 'Quickstart', 'Integration assistant (preview)', and 'Manage'. The 'Manage' section contains links for 'Branding', 'Authentication', 'Certificates & secrets', 'Token configuration', 'API permissions', and 'Expose an API'. The main configuration area displays the following details for 'Contoso App 1':

Display name Contoso App 1	Supported account types My organization only
Application (client) ID 11111111-1111-1111-1111-111111111111	Redirect URIs Add a Redirect URI
Directory (tenant) ID 00000000-0000-0000-0000-000000000000	Application ID URI Add an Application ID URI
Object ID 22222222-2222-2222-2222-222222222222	Managed application in local directory Contoso App 1

Below the configuration details, there is a warning message: '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 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](#)'

Important

New app registrations are hidden to users by default. When you're ready for users to see the app on their [My Apps page](#) you can enable it. To enable the app, in the Microsoft Entra admin center navigate to **Entra ID > Enterprise apps** and select the app. Then on the **Properties** page, set **Visible to users?** to **Yes**.

Once you register your application, it gets assigned the **User.Read** permission. However, for external tenants, the customer users themselves can't consent to permissions themselves. You as the admin must consent to this permission on behalf of all the users in the tenant:

1. From the **Overview** page of your app registration, under **Manage** select **API permissions**.
2. Select **Grant admin consent for < tenant name >**, then select **Yes**.
3. Select **Refresh**, then verify that **Granted for < tenant name >** appears under **Status** for the permission.

- [Add a redirect URI to your application](#)
- [Add credentials to your application](#)
- [Configure an application to expose a web API](#)
- [Microsoft identity platform code samples](#)
- [Add your application to a user flow](#)