

How to Configure OAuth 2.0 for Azure DevOps

Last Modified on 01/15/2026 7:37 pm EST

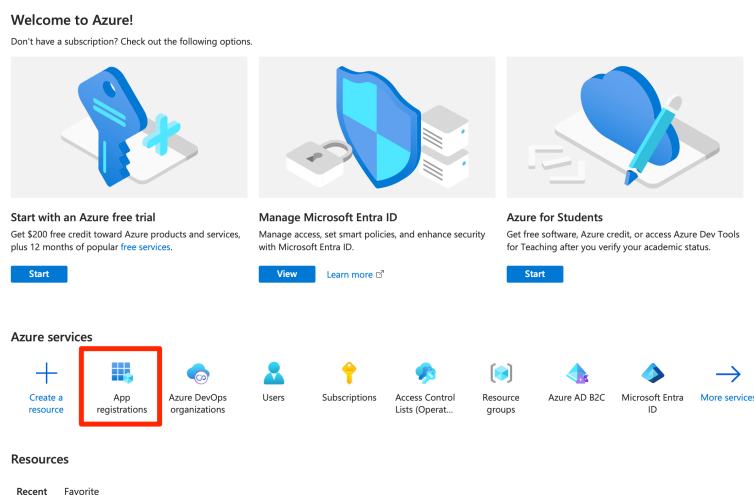
The guide is specifically designed for organizations that manage their identities and access through **Microsoft Entra ID** (formerly Azure Active Directory). This article will walk you through the essential steps for configuring your Exalate node with OAuth 2.0.

Register a New App

1. Navigate to [Azure Portal](#)

2. Sign in using an organizational account that has sufficient permissions to register applications within your Microsoft Entra ID tenant

3. Once signed in, in the Azure portal search bar, type **App registrations** and select the App registrations service.



4. Fields to fill:

- **Name**
- **Who can use this application or access this API?**
 - Accounts in this organizational directory only (Default Directory only - Single tenant)
- **Redirect URI**
 - select Web
 - append `/azure/callback` to your Exalate URL (you can find the Exalate URL on the Registration page)

General Settings

***Authentication Method**

OAuth 2.0

You must belong to Project Collection Administrators group.
For more details, [check how to configure OAuth 2.0.](#)

***Exalate Uri**

<https://azurenode-xxxx-xxxx-xxxx-xxxx.exalate.cloud>

***Client ID**

***Tenant ID**

***Client Secret**

Example: <https://azurenode-xxxx-xxxx-xxxx-xxxx.exalate.cloud/azure/callback>

Register an application

* Name

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

Test

Supported account types

Who can use this application or access this API?

- ☒ Accounts in this organizational directory only (Default Directory only - Single tenant)
- ☐ 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.

Web <https://azurenode-xxxx-xxxx-xxxx-xxxx.exalate.cloud/azure/callback>

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

5. After filling in all the required fields, click the **Register** button at the bottom of the page to create your application registration.

Note: **Client ID** and **Tenant ID** values will be required when you proceed with registering your Exalate node.

[Home](#) > [App registrations](#)

TEST

Search

Overview

- Quickstart
- Integration assistant
- Diagnose and solve problems
- Manage
 - Branding & properties
 - Authentication
 - Certificates & secrets
 - Token configuration
 - API permissions
 - Expose an API
 - App roles
 - Owners
 - Roles and administrators
 - Manifest
- Support & Troubleshooting

Essentials

Display name : TEST

Application (client) ID : 6142xxxx-xxxx-xxxx-xxxx-xxxx

Object ID : 9684xxxx-xxxx-xxxx-xxxx-xxxx

Directory (tenant) ID : d6bxxxx-xxxx-xxxx-xxxx-xxxx

Supported account types : [My organization only](#)

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

Redirect URIs : [1 web, 0 spa, 0 public client](#)

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

Managed application in L... : TEST

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](#)

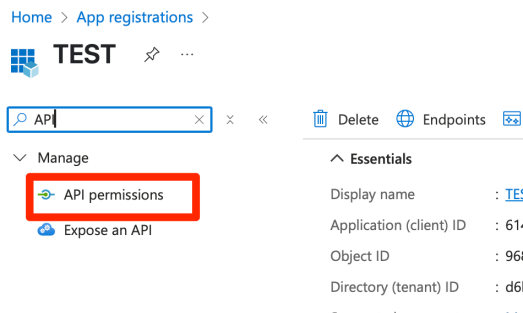
[Get Started](#) [Documentation](#)

Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. [Learn more](#)

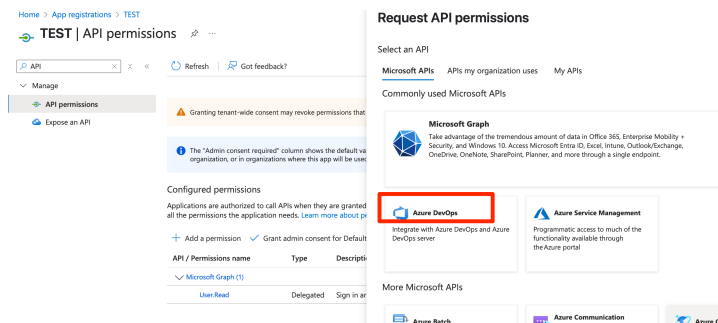
Add the API Permissions in the App

1. Search for **API**

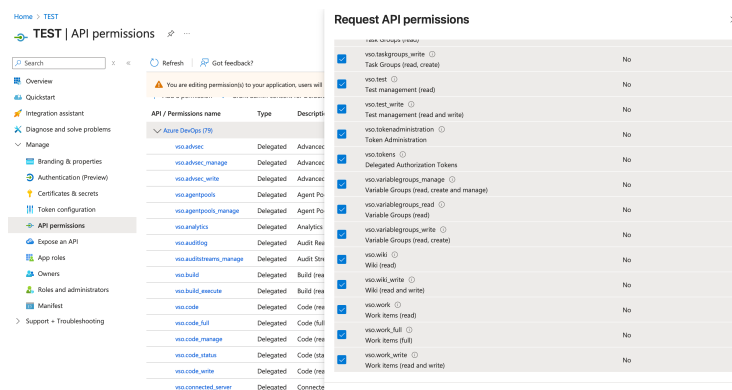


2. Click on **Add permission**

- Click on **Azure DevOps**



- Give all permissions related to **VSO**



- Click on **Microsoft Graph** and give permissions related to Application and User, as shown in the screenshot below.

- Application.Read.All
- Application.ReadWrite.All
- Directory.ReadWrite.All
- User.Read

[API Reference](#)

[Security](#)

[Pricing and Licensing](#)

Resources

[Subscribe for a weekly Exalate hack](#)

[Academy](#)

[Blog](#)

[YouTube Channel](#)

[Ebooks](#)

Still need help?

[Join our Community](#)

[Visit our Service Desk](#)

[Find a Partner](#)