How to Configure OAuth 2.0 for Azure DevOps

Last Modified on 07/24/2025 2:52 am EDT

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.
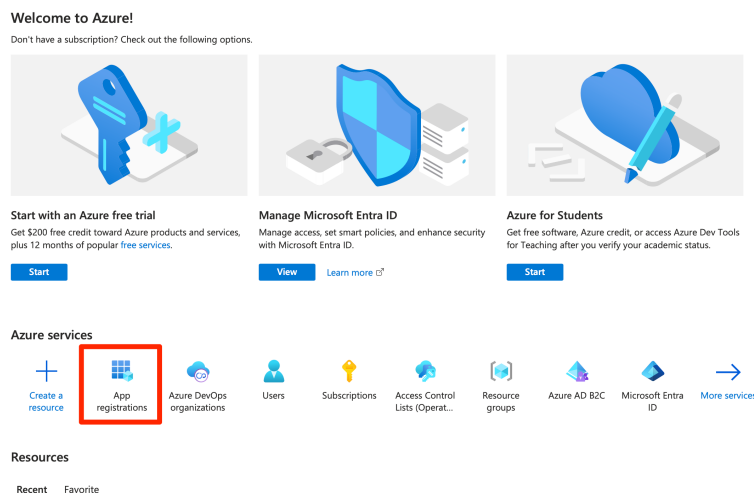
4. Fields to fill:

- **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 Url

https://azurenode-████ ████ ████ ████.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-████ █████ █████ ██████.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 «	🗑 Delete 🌐 Endpoints ▦ Preview features
▦ Overview	^ Essentials
⚡ Quickstart	
🚀 Integration assistant	Display name : **TEST** Client credentials : **Add a certificate or secret**
🔧 Diagnose and solve problems	Application (client) ID : 6142████████████ Redirect URIs : **1 web, 0 spa, 0 public client**
∨ Manage	Object ID : 9684████████████ Application ID URI : **Add an Application ID URI**
░ Branding & properties	Directory (tenant) ID : d6b████████████ Managed application in l... : **TEST**
🔐 Authentication	Supported account types : **My organization only**
🔑 Certificates & secrets	
▦ Token configuration	ⓘ Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? Learn more
◆ API permissions	
🔒 Expose an API	ⓘ 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
🔲 App roles	
👥 Owners	**Get Started** Documentation
👥 Roles and administrators	
▦ Manifest	**Build your application with the Microsoft identity platform**
> Support + Troubleshooting	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

- User.ReadWrite.All

vso.work_write	Delegated	Work items (read and write)	
∨ Microsoft Graph (5)			
Application.Read.All	Delegated	Read applications	
Application.ReadWrite.All	Delegated	Read and write all applications	
Directory.ReadWrite.All	Delegated	Read and write directory data	
User.Read	Delegated	Sign in and read user profile	
User.ReadWrite.All	Delegated	Read and write all users' full profiles	

Grant Admin consent

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The lis
all the permissions the application needs. Learn more about permissions and consent

+ Add a permission   ✓ Grant admin consent for Default Directory

API / Permissions name	Type	Description	Admin consent
∨ Azure DevOps (4)			
vso.project_manage	Delegated	Project and team (read, write and manage)	No
vso.work	Delegated	Work items (read)	No

Generate Client Secret

Note: Check the How to Generate Client Secret for more details.

Note: Make sure your organization is connected to the default directory.

Product

About Us ⧉

Release History ⧉

Glossary ⧉

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 ⧉