How to Configure OAuth 2.0 for Azure DevOps

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

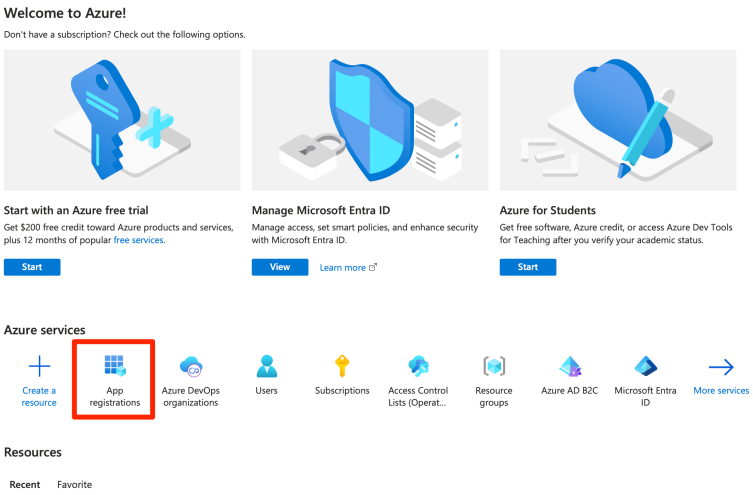
The guide is specifically designed for organizations that manage their identities and access through **Microsoft Entra ID** (formerly Azure Active Directory). This article will walk you through the essential steps for configuring your Exalate node with OAuth 2.0.

Register a New App

1. Navigate to Azure Portal

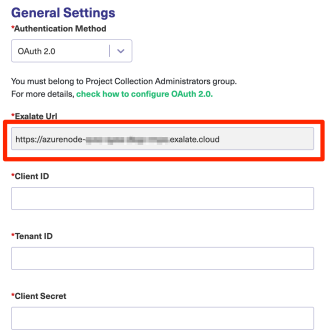
2. Sign in using an organizational account that has sufficient permissions to register applications within your Microsoft Entra ID tenant

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

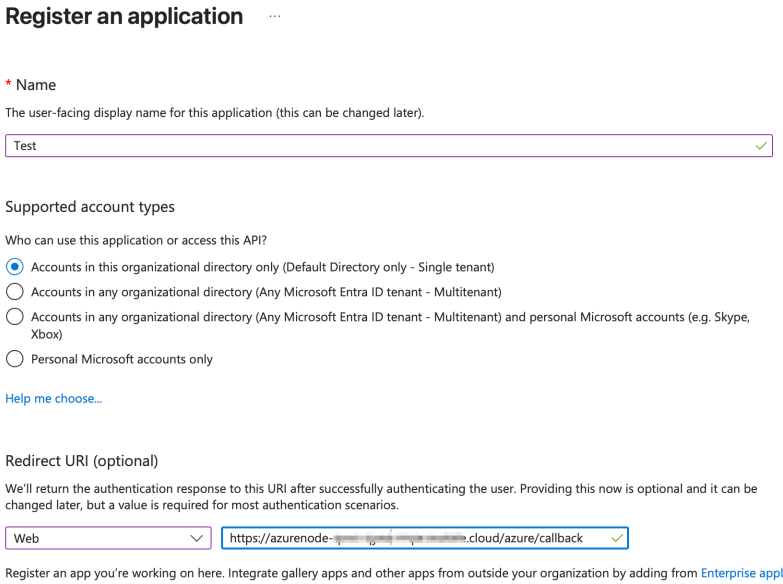


4. Fields to fill:

- **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)

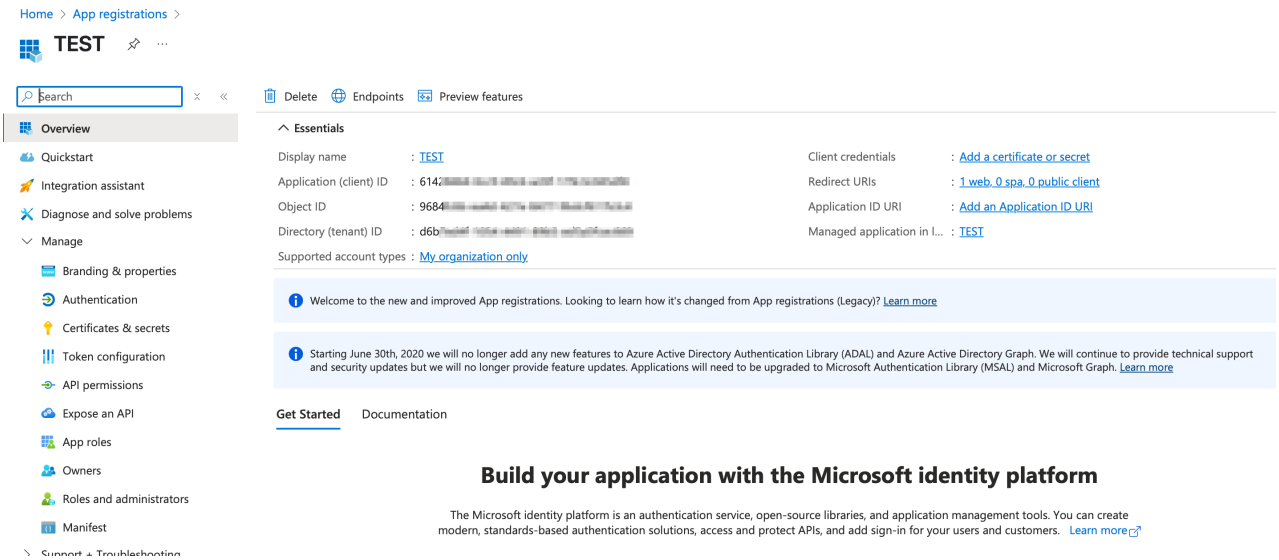


Example: https://azurenode-xxxx-xxxx-xxxx-xxxx.exalate.cloud/azure/callback



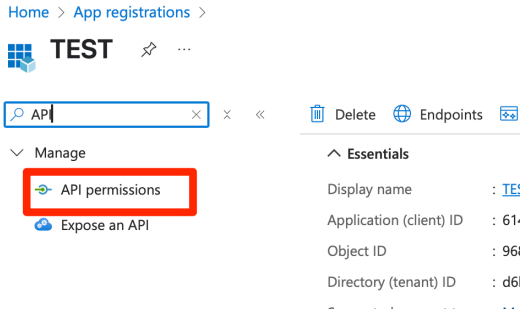
5. After filling in all the required fields, click the **Register** button at the bottom of the page to create your application registration.

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



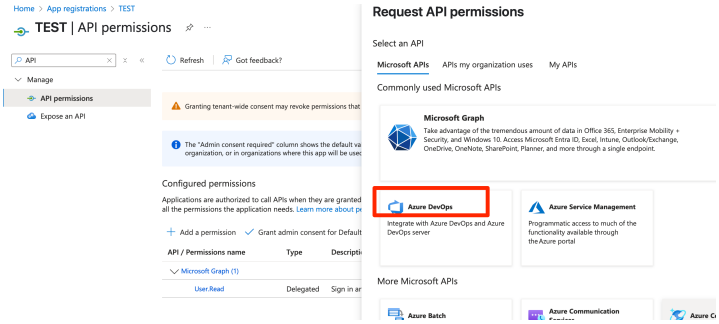
Add the API Permissions in the App

1. Search for **API**

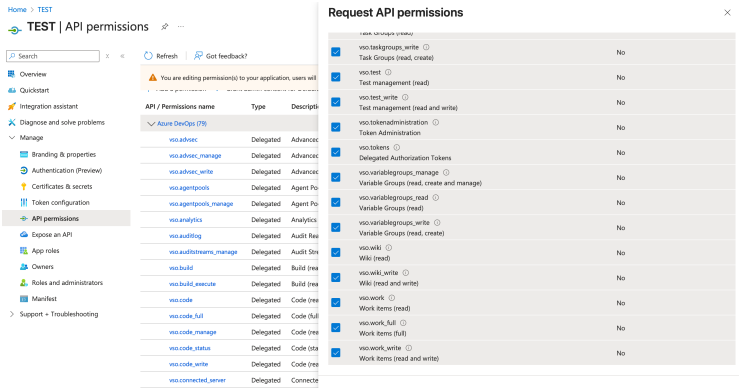


2. Click on **Add permission**

- 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

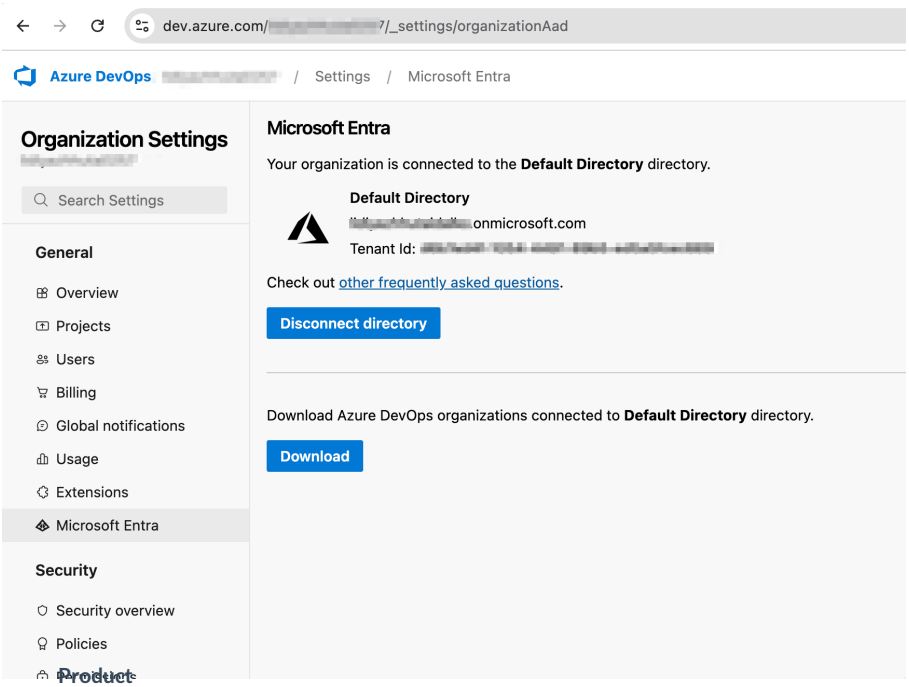
Add a permission | Grant admin consent for Default Directory

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