

Azure Portal Guide

Create Client ID, Client Secret, Tenant ID, Subscription ID, and attach the app to the current subscription

Prepared for client sharing

Uses official Microsoft Learn documentation screenshots

Prepared	13 Mar 2026
Portal scope	Microsoft Entra admin center + Azure portal

What this guide covers

Value / task	Where you get it
Application (client) ID	App registration > Overview
Directory (tenant) ID	App registration > Overview or Microsoft Entra ID > Overview
Client secret value	App registration > Certificates & secrets > Client secrets
Subscription ID	Subscription > Overview
Attach app to current subscription	Subscription > Access control (IAM) > Add role assignment

Before you start

- Use a Microsoft Entra account that can register applications. Microsoft's app registration quickstart says at least Application Developer; Microsoft's service principal article uses Cloud Application Administrator for this flow.
- To attach the application to a subscription, your signed-in user must have role-assignment permission at that scope, such as Microsoft.Authorization/roleAssignments/write via Role Based Access Control Administrator, User Access Administrator, or Owner.
- The client secret value is shown only once. Copy the Value immediately after creation and store it securely.

1. Create the app registration

In the Microsoft Entra admin center, go to App registrations and select New registration. Enter the app name, choose the supported account type that matches your use case, and register the app. For most internal single-tenant setups, Accounts in this organizational directory only is the usual choice.

The screenshot shows the 'Register an application' page in the Microsoft Azure portal. The page has a blue header with 'Microsoft Azure' and a search bar. Below the header, there are navigation links for 'Home' and 'App registrations'. The main title is 'Register an application'. The form includes a 'Name' field with the value 'demoapp1-dev' and a green checkmark. Below this is the 'Supported account types' section with four radio button options: 'Accounts in this organizational directory only (Microsoft Customer Led 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)', and 'Personal Microsoft accounts only'. The first option is selected. There is a 'Help me choose...' link. Below that is the 'Redirect URI (optional)' section with a dropdown menu for 'Select a platform' and a text input field containing 'e.g. https://example.com/auth'. At the bottom, there is a 'Register' button and a link to 'Enterprise applications'.

Figure 1. Official Microsoft Learn screenshot of the Register an application page.

Source: Microsoft Learn - Authenticate .NET apps to Azure services during local development using service principals

2. Copy the Client ID and Tenant ID

After registration, Azure opens the app's Overview page. Copy these two values and save them in a secure temporary note:

- Application (client) ID - the client ID used by your app
- Directory (tenant) ID - the tenant ID used for authentication

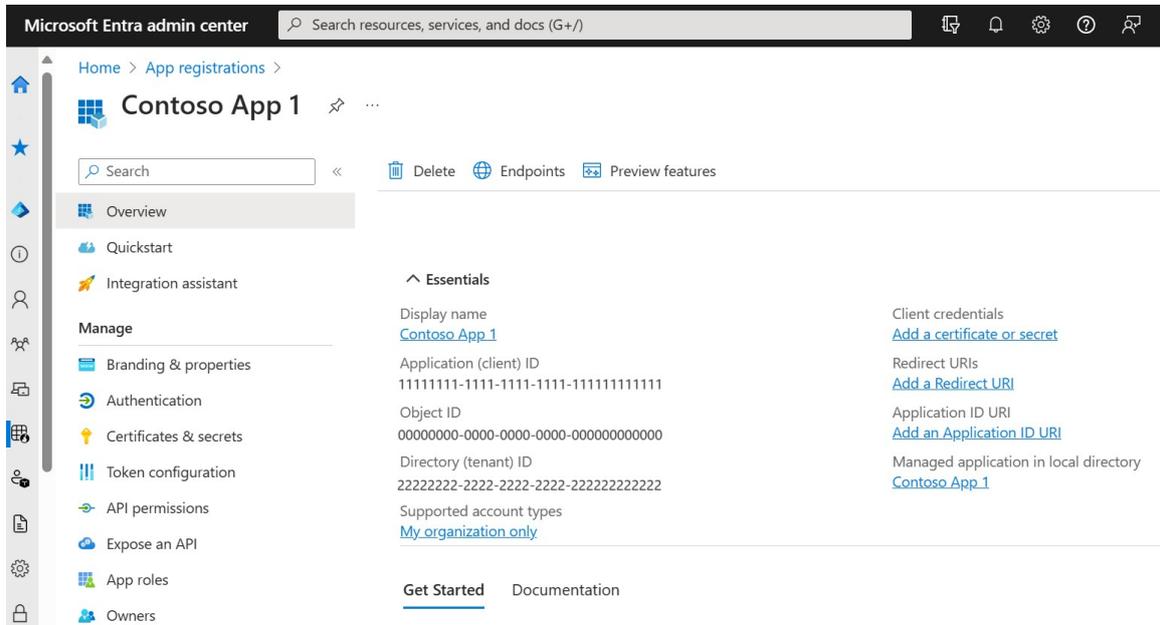


Figure 2. Official Microsoft Learn screenshot of the app Overview page showing Application (client) ID and Directory (tenant) ID.

Source: Microsoft Learn - How to register an app in Microsoft Entra ID

3. Create the client secret

Open the same app registration, then go to Certificates & secrets > Client secrets > New client secret. Add a description, choose the expiry, and select Add.

- Microsoft limits client secret lifetime to two years or less.
- Microsoft recommends an expiry of less than 12 months.

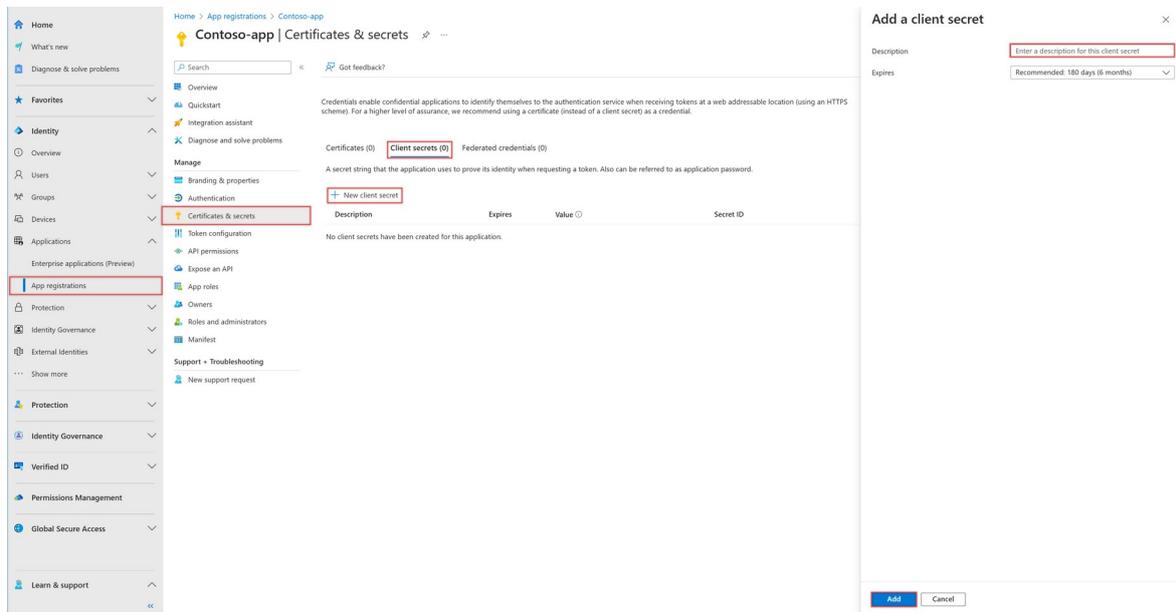


Figure 3. Official Microsoft Learn screenshot showing Client secrets and the Add a client secret panel.

Source: Microsoft Learn - Add and manage application credentials in Microsoft Entra ID

After you select Add, copy the client secret Value immediately. Do not copy Secret ID by mistake - applications use the secret Value.

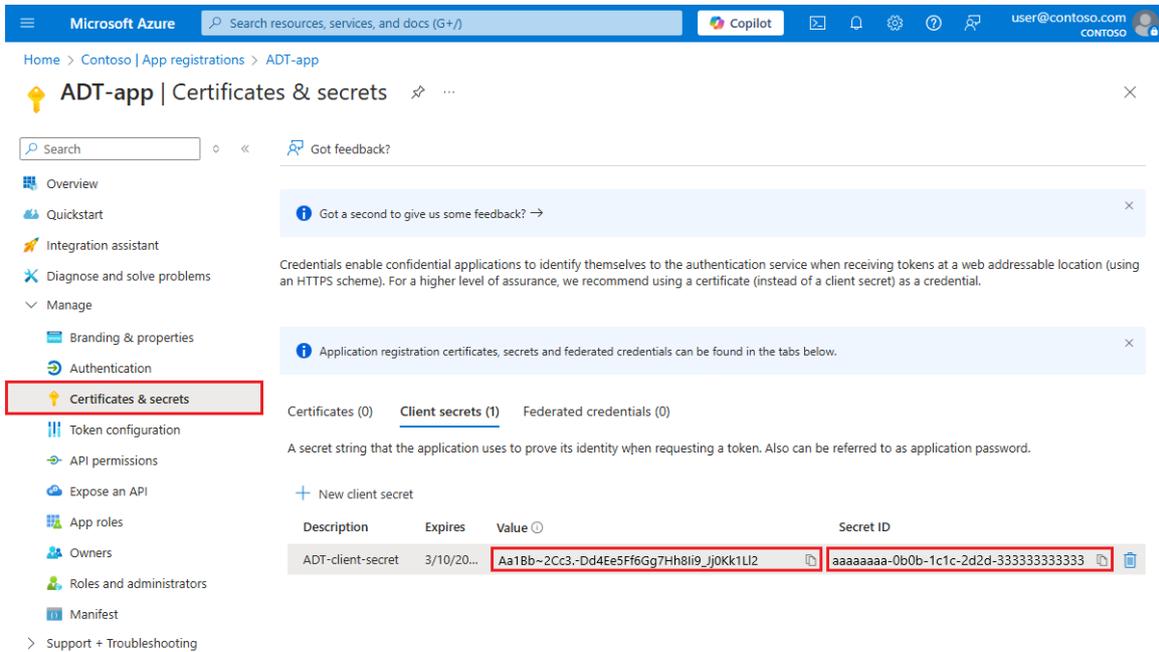


Figure 4. Official Microsoft Learn screenshot showing the client secret Value after creation.

Source: Microsoft Learn - Create an app registration with Azure Digital Twins access

4. Find the Subscription ID

In the Azure portal, search for Subscriptions, open the current subscription, and copy the Subscription ID from the Overview page.

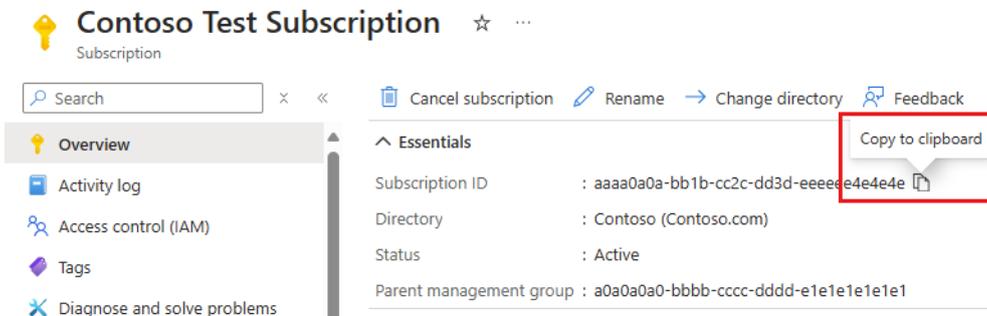


Figure 5. Official Microsoft Learn screenshot showing how to copy the Subscription ID.

Source: Microsoft Learn - Get subscription and tenant IDs in the Azure portal

5. Find the Tenant ID from Azure portal

If you need to verify the tenant directly in Azure portal, open Microsoft Entra ID and copy the Tenant ID from the Overview page.



Figure 6. Official Microsoft Learn screenshot showing how to copy the Tenant ID.

Source: Microsoft Learn - Get subscription and tenant IDs in the Azure portal

6. Attach the app to the current subscription

To let the application access Azure resources in the current subscription, assign an Azure RBAC role to the app's service principal at the subscription scope.

Common role	When to use it
Reader	View-only access to resources
Contributor	Create/update most resources, but not access control
Custom role	When your client needs only specific permissions

Steps in the subscription:

- Open Subscriptions and select the current subscription.
- Open Access control (IAM).
- Select Add > Add role assignment.
- Choose the required role and select Next.
- On Members, choose User, group, or service principal.
- Select Select members, search for the app registration name, select it, then choose Review + assign.

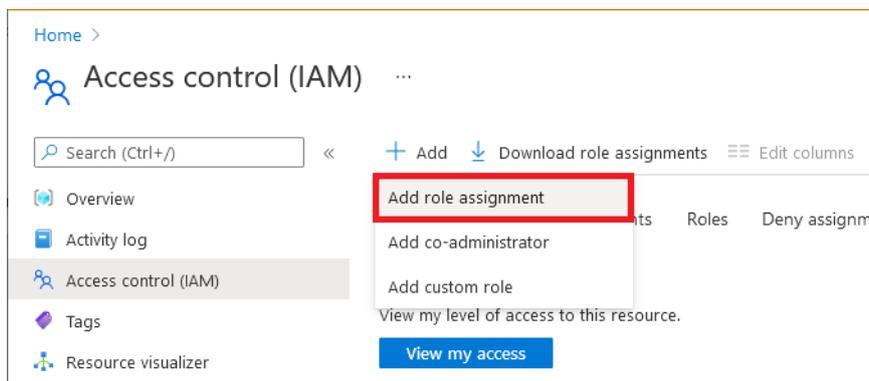


Figure 7. Official Microsoft Learn screenshot showing Add role assignment from Access control (IAM).

Source: Microsoft Learn - Azure RBAC reusable portal content

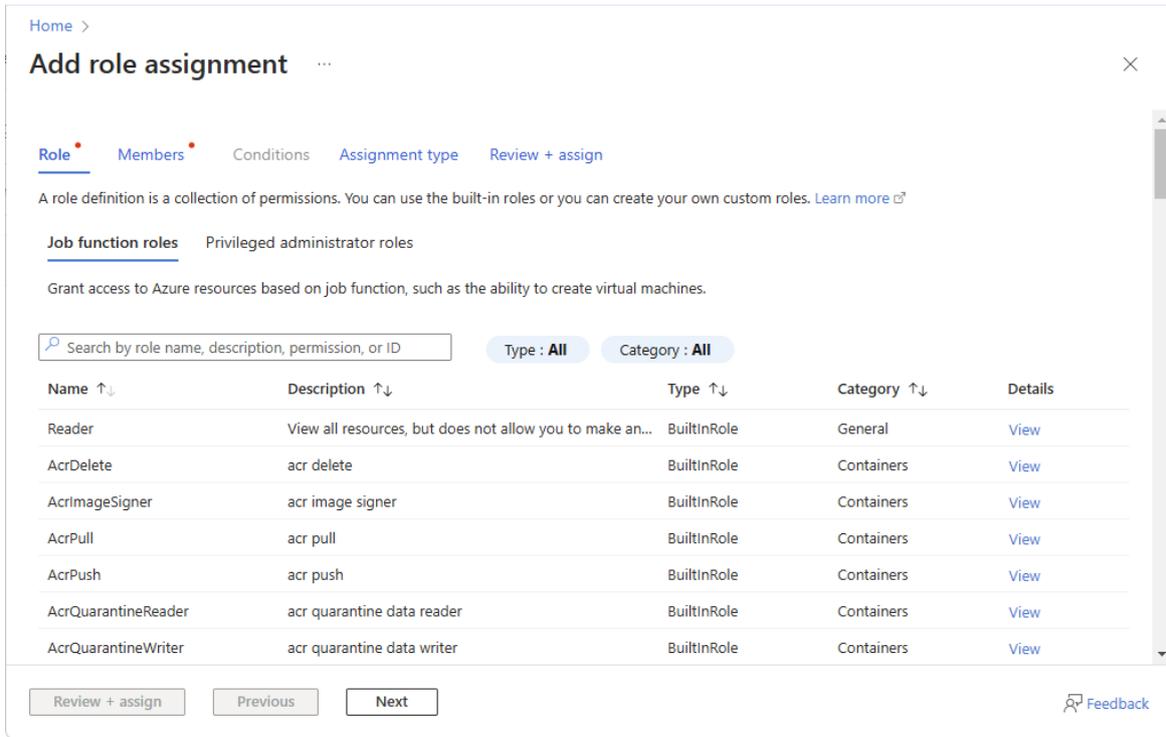


Figure 8. Official Microsoft Learn screenshot showing the Add role assignment page.

Source: Microsoft Learn - Azure RBAC reusable portal content

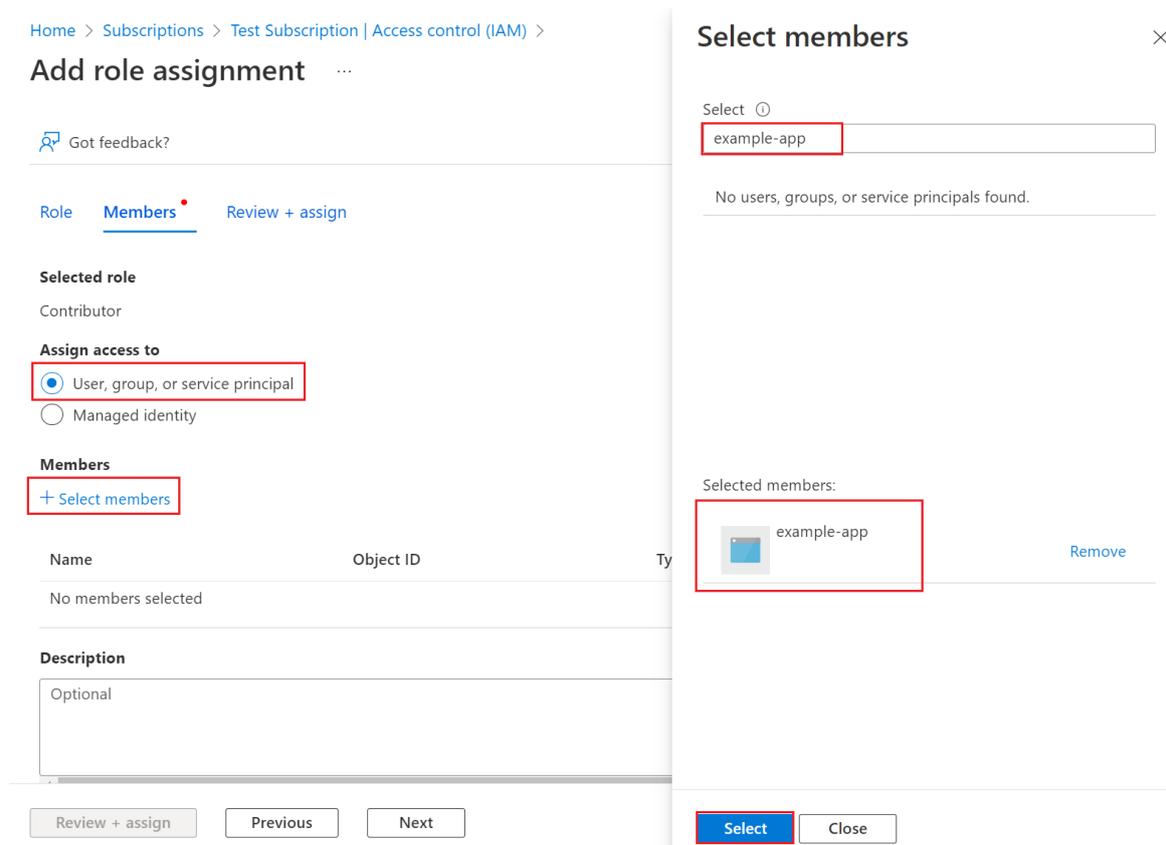


Figure 9. Official Microsoft Learn screenshot showing how to select the application as a member/service principal.

Source: Microsoft Learn - Register a Microsoft Entra app and create a service principal

7. Final handover checklist

Use this table when sharing the completed setup details with your client or project team.

Item	Value / note	Done
App registration name	_____	<input type="checkbox"/>
Application (client) ID	_____	<input type="checkbox"/>
Directory (tenant) ID	_____	<input type="checkbox"/>
Subscription ID	_____	<input type="checkbox"/>
Client secret Value	Store securely - do not email in plain text	<input type="checkbox"/>
Assigned role on subscription	_____	<input type="checkbox"/>

Official Microsoft Learn pages used

- How to register an app in Microsoft Entra ID - <https://learn.microsoft.com/en-us/entra/identity-platform/quickstart-register-app>
- Add and manage application credentials in Microsoft Entra ID - <https://learn.microsoft.com/en-us/entra/identity-platform/how-to-add-credentials>
- Get subscription and tenant IDs in the Azure portal - <https://learn.microsoft.com/en-us/azure/azure-portal/get-subscription-tenant-id>
- Register a Microsoft Entra app and create a service principal - <https://learn.microsoft.com/en-us/entra/identity-platform/howto-create-service-principal-portal>
- Assign Azure roles using the Azure portal - <https://learn.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal>