Microsoft Entra ID credentials

# Microsoft Entra ID credentials#

You can use these credentials to authenticate the following nodes:

• Microsoft Entra ID

## Prerequisites#

• Create a Microsoft Entra ID account or subscription.

• If the user account is managed by a corporate Microsoft Entra account, the administrator account has enabled the option “User can consent to apps accessing company data on their behalf” for this user (see the Microsoft Entra documentation).

Microsoft includes an Entra ID free plan when you create a Microsoft Azure account.

## Supported authentication methods#

• OAuth2

## Related resources#

Refer to Microsoft Entra ID's documentation for more information about the service.

## Using OAuth2#

Note for n8n Cloud users

Cloud users don't need to provide connection details. Select Connect my account to connect through your browser.

For self-hosted users, there are two main steps to configure OAuth2 from scratch:

• Register an application with the Microsoft Identity Platform.

• Generate a client secret for that application.

Follow the detailed instructions for each step below. For more detail on the Microsoft OAuth2 web flow, refer to Microsoft authentication and authorization basics.

### Register an application#

Register an application with the Microsoft Identity Platform:

• Open the Microsoft Application Registration Portal.

• Select Register an application.

• Enter a Name for your app.

• In Supported account types, select Accounts in any organizational directory (Any Azure AD directory - Multi-tenant) and personal Microsoft accounts (for example, Skype, Xbox).

• In Register an application:  
Copy the OAuth Callback URL from your n8n credential.  
Paste it into the Redirect URI (optional) field.  
Select Select a platform > Web.

• Copy the OAuth Callback URL from your n8n credential.

• Paste it into the Redirect URI (optional) field.

• Select Select a platform > Web.

• Select Register to finish creating your application.

• Copy the Application (client) ID and paste it into n8n as the Client ID.

Refer to Register an application with the Microsoft Identity Platform for more information.

### Generate a client secret#

With your application created, generate a client secret for it:

• On your Microsoft application page, select Certificates & secrets in the left navigation.

• In Client secrets, select + New client secret.

• Enter a Description for your client secret, such as n8n credential.

n8n credential

• Select Add.

• Copy the Secret in the Value column.

• Paste it into n8n as the Client Secret.

• Select Connect my account in n8n to finish setting up the connection.

• Log in to your Microsoft account and allow the app to access your info.

Refer to Microsoft's Add credentials for more information on adding a client secret.

## Common issues#

Here are the known common errors and issues with Microsoft Entra credentials.

### Need admin approval#

When attempting to add credentials for a Microsoft360 or Microsoft Entra account, users may see a message when following the procedure that this action requires admin approval.

This message will appear when the account attempting to grant permissions for the credential is managed by a Microsoft Entra. In order to issue the credential, the administrator account needs to grant permission to the user (or "tenant") for that application.

The procedure for this is covered in the Microsoft Entra documentation.