Microsoft credentials

# Microsoft credentials#

You can use these credentials to authenticate the following nodes:

• Microsoft Dynamics CRM

• Microsoft Excel

• Microsoft Graph Security

• Microsoft OneDrive

• Microsoft Outlook

• Microsoft Teams

• Microsoft To Do

## Prerequisites#

• Create a Microsoft Azure account.

• Create at least one user account with access to the appropriate service.

• 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).

## Supported authentication methods#

• OAuth2

## Related resources#

Refer to the linked Microsoft API documentation below for more information about each service's API:

• Dynamics CRM: Web API

• Excel: Graph API

• Graph Security: Graph API

• OneDrive: Graph API

• Outlook: Graph API and Outlook API

• Teams: Graph API

• To Do: Graph API

## 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.

Some Microsoft services require extra information for OAuth2. Refer to Service-specific settings for more guidance on those services.

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.

• If you see other fields in the n8n credential, refer to Service-specific settings below for guidance on completing those fields.

• 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.

### Service-specific settings#

The following services require extra information for OAuth2:

Dynamics OAuth2 requires information about your Dynamics domain and region. Follow these extra steps to complete the credential:

• Enter your Dynamics Domain.

• Select the Dynamics data center Region you're within.

Refer to the Microsoft Datacenter regions documentation for more information on the region options and corresponding URLs.

The general Microsoft OAuth2 also requires you to provide a space-separated list of Scopes for this credential.

Refer to Scopes and permissions in the Microsoft identity platform for a list of possible scopes.

Outlook OAuth2 supports the credential accessing a user's primary email inbox or a shared inbox. By default, the credential will access a user's primary email inbox. To change this behavior:

• Turn on Use Shared Inbox.

• Enter the target user's UPN or ID as the User Principal Name.

SharePoint OAuth2 requires information about your SharePoint Subdomain.

To complete the credential, enter the Subdomain part of your SharePoint URL. For example, if your SharePoint URL is https://tenant123.sharepoint.com, the subdomain is tenant123.

https://tenant123.sharepoint.com

tenant123

## Common issues#

Here are the known common errors and issues with Microsoft OAuth2 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.