# How to create a custom private client app in Azure

Print Director can use Microsoft 365 to sync users from Microsoft Entra ID, send email (reports, PINs and alerts), and receive email for printing. It needs permission from your Microsoft tenant to do this, in one of two ways:

- **A delegated token**, which someone creates by signing in. It is quick to set up, but expires after 90 days at most, and must then be created again.
- **Your own app registration** (a custom private client app) with a **client secret**. The secret lasts up to two years.

This article sets up your own app registration. You need an account that may register applications in Entra ID, and for the email part, the Exchange Administrator role.

## Register the app

1. Sign in to the Azure portal and open **Microsoft Entra ID**.
2. Click **App registrations**, then **New registration**.
3. Enter a name, for example *PD Entra ID integration*.
4. Choose **Accounts in this organizational directory only (Single tenant)**.
5. Leave **Redirect URI** empty. An app that signs in with a client secret does not use one.
6. Click **Register**.

## Create the client secret

Print Director uses the secret to prove it may use the app.

1. In the app, click **Certificates & secrets**, then **New client secret**.
2. Enter a **Description**, for example *Default secret*, and choose how long it lasts in **Expires** (at most two years).
3. Click **Add**.
4. Copy the secret's **Value** (not the **Secret ID**) and keep it somewhere safe, with its expiry date. The portal hides the value later, and you need it in Print Director.

When the secret expires, create a new one the same way, and enter it in Print Director.

# Permissions for the Entra ID Sync

The sync needs two permissions, both with admin consent: **User.Read.All** and **Group.Read.All**. Skip this if you only use the app for email.

1. In the app, click **API permissions**, then **Add a permission**.
2. Click **Microsoft Graph**, then **Application permissions**.
3. Search for *User.Read.All*, expand **User**, and tick **User.Read.All**.
4. Search for *Group.Read.All* and tick **Group.Read.All**.
5. Click **Add permissions**.
6. Click **Grant admin consent for** *(your tenant)*, and click **Yes**.

# Permissions for email

To send and receive email, the app needs **Mail.Send** and **Mail.ReadWrite**. There are two ways to give them:

- **For the whole tenant:** add them as application permissions with admin consent, the same way as the Entra ID Sync permissions above. This is simple, but then the app could read and send email as any user in your organisation.
- **For one mailbox only (recommended):** use Exchange Online role-based access control (RBAC) for applications, as below. The app can then only use the mailbox Print Director sends from.

You can do this with the commands below, or with two ready-made PowerShell scripts that run them for you (see Using the scripts, after step 6).

## What you need

- The **Exchange Administrator** role (or membership of the **Organization Management** role group).
- PowerShell, run as administrator, with the Exchange Online Management module.
- The app's **Application ID** and **Object ID** from **Enterprise applications** (step 3 below).

## Step 1: Connect to Exchange Online

If the Exchange Online Management module is not installed yet, open PowerShell as administrator and run:

```
Install-Module -Name ExchangeOnlineManagement -Force
```

Then connect, and sign in with an account that has the Exchange Administrator role:

```
Connect-ExchangeOnline
```

## Step 2: Turn on organisation customisation

Management scopes need organisation customisation, which is off in new tenants. Check it:

```
Get-OrganizationConfig | Format-List IsDehydrated
```

If the result is **True**, turn it on (this is only ever needed once per tenant, and can take up to 30 minutes):

```
Enable-OrganizationCustomization
```

If you get the error *Resource 'Processor (servername)' is unhealthy and shouldn't be accessed*, the problem is on Microsoft's side. Wait 15 to 30 minutes and try again; it can take up to 24 hours. Check the Microsoft 365 Service health page, and contact Microsoft Support if it lasts longer.

## Step 3: Get the app's IDs

In Entra ID, open **Enterprise applications** (not **App registrations**), and click your app. On the **Overview** page, copy the **Application ID** and the **Object ID**. The Object ID here is different from the one under App registrations, so make sure you use this one.

## Step 4: Create the service principal, scope and roles

Replace the IDs and the mailbox address (here `printdirector@yourdomain.com`) with your own, and run each command.

Create a service principal, which points Exchange Online at the app:

```
New-ServicePrincipal -AppId "<Application-ID>" -ObjectId "<Object-ID>" -DisplayName
"Print Director"
```

Create a management scope that contains only the Print Director mailbox:

```
New-ManagementScope -Name "PrintDirector-Mailbox" -RecipientRestrictionFilter
"PrimarySmtpAddress -eq 'printdirector@yourdomain.com'"
```

Give the app Mail.ReadWrite on that mailbox. This is needed to receive email for printing, and also to send emails with large attachments:

```
New-ManagementRoleAssignment -Name "PD-MailReadWrite" -Role "Application
Mail.ReadWrite" -App "<Application-ID>" -CustomResourceScope "PrintDirector-Mailbox"
```

Give the app Mail.Send on that mailbox:

```
New-ManagementRoleAssignment -Name "PD-MailSend" -Role "Application Mail.Send" -App "
<Application-ID>" -CustomResourceScope "PrintDirector-Mailbox"
```

## Step 5: Make sure the app has no tenant-wide mail permissions

Permissions add up: if **Mail.Send** or **Mail.ReadWrite** were also added under the app's **API permissions** in Entra ID, the app can still use every mailbox. If they are there, remove them. Keep the permissions for the Entra ID Sync.

## Step 6: Test it

This should show **InScope** as **True** for the Print Director mailbox:

```
Test-ServicePrincipalAuthorization -Identity "<Application-ID>" -Resource
"printdirector@yourdomain.com"
```

and **False** for any other mailbox:

```
Test-ServicePrincipalAuthorization -Identity "<Application-ID>" -Resource
"anotheruser@yourdomain.com"
```

The test shows the result straight away, but Exchange Online takes 30 minutes to 2 hours to start using the new permissions. If Print Director reports *Access denied, check credentials* soon after you set this up, wait two hours and try again.

## Using the scripts

Download the Mail RBAC scripts (a zip file with two PowerShell scripts):

- **Setup-MailRBAC.ps1** does steps 1, 2, 4 and 6 for you. It asks for the **Application ID** and **Object ID** from **Enterprise applications** (step 3) and the mailbox address, installs the Exchange Online module if needed, and then tests the result. You still need to do step 5 yourself.
- **Remove-MailRBAC.ps1** removes what the setup made (the role assignments, the management scope and the service principal), so you can start again. It lists what it found and asks you to type *YES* first.

To run one, extract the zip, open PowerShell as administrator in that folder, and run for example:

```
.\Setup-MailRBAC.ps1
```

If PowerShell refuses to run a downloaded script, first run this command, which only affects that PowerShell window:

```
Set-ExecutionPolicy -Scope Process -ExecutionPolicy Bypass
```

## Add the app in Print Director

You add the app in Print Director once, and can then use it for Email Send Accounts, Email Receive Accounts and the Microsoft Entra ID Sync.

First, copy two IDs from Entra ID: open **App registrations**, click **All applications** and your app, and on the **Overview** page copy the **Application (client) ID** and **Directory (tenant) ID**.

For example, for an Email Send Account:

1. In Resource Manager, click **Email Management** > **Email Send Accounts**, then click **Add**.
2. Enter a name for the account, and set **Sending service type** to **MS Graph application authentication**.
3. In **Send as user**, enter the mailbox address, for example `printdirector@yourdomain.com`.
4. In **Client app**, select the app if it is already in Print Director (for example from an Entra ID Sync). Otherwise click the **...** button next to it, and in the **Search for MS confidential app** window click **New**. In the **MS Graph application authentication** window:
   - **Display name:** a name for the app, for example *PD Entra ID integration*.
   - **Application (client) ID**, **Client secret** (the secret's **Value**) and **Directory (tenant) ID:** paste the values you copied.
   - **Client secret expiry:** the date the secret expires, as shown in the Azure portal.
   - Leave **Authority instance** as it is.
   - Click **OK**.
5. Make sure the app is selected in **Client app**, and test the account (see *How to create an Email Send Account*).

For the Microsoft Entra ID Sync, set **MS Graph access type** to **Client secret** and choose the same app in **Private client app secret** (see *How to set up a Microsoft Entra ID Sync*).

## Related articles

- *How to create an Email Send Account*
- *How to set up a Microsoft Entra ID Sync*

Print Director version at time of publish: 2.5.15.3. Publish date: 09/11/2026.