Ciphr HR Sign-In

Entra OpenID (formerly Azure) Tenant configuration for SSO

June 2025 | V2.0

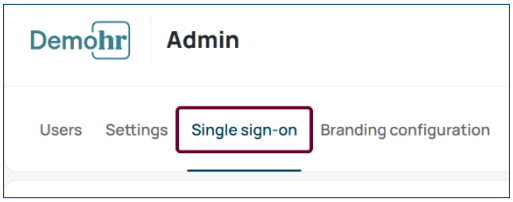
Ciphr Limited
3rd Floor, 33 Blagrave Street, Reading, RG1 1PW | +44 (0)1628 814000 | info@ciphr.com | ciphr.com

Entra OpenID (formerly Azure) Tenant configuration for SSO

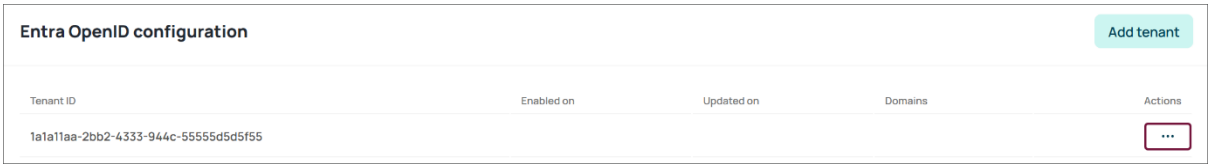
How to set up Entra OpenID Tenant configuration for SSO

Please note before you start, you don't need to create any Azure Enterprise apps of your own as you will be using our enterprise application.

1. Click on the **Single Sign On** tab in CSI

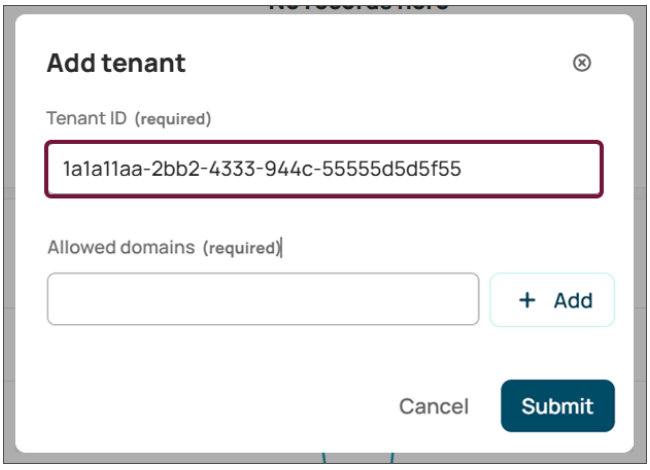


2. If your **Tenant ID** has been added for you, you just need to add your **Domain**. Click on the **...** button and move to step 5



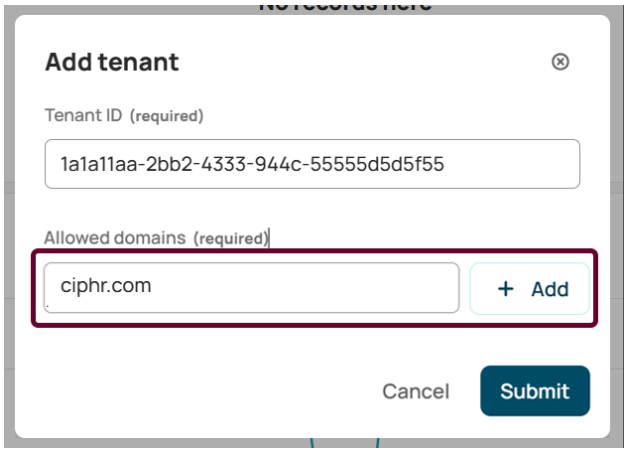
3. To add a new tenant, under **Entra openID tenant configuration** click **Add tenant**

4. A **Tenant ID** is a unique identifier that tells a service or application which organisation's identity system to use for Single Sign-On (SSO). Locate and enter the **Tenant ID** from your Entra (Azure) portal.

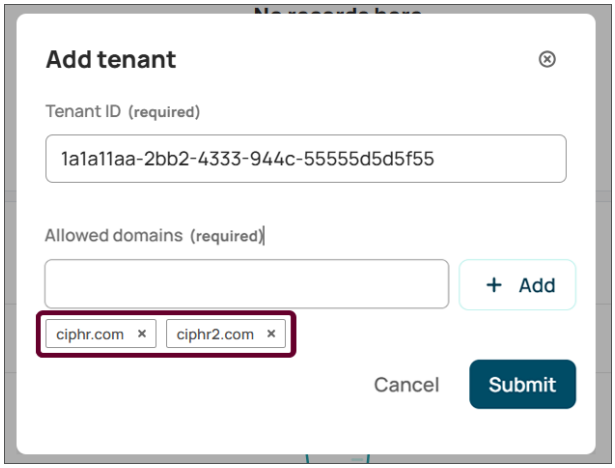


5. Next, add the recognised domains associated with the tenant for SSO. Ciphr recognises which tenant to redirect a user to by that user's email address. Enter any email domains that should be associated with this tenant.

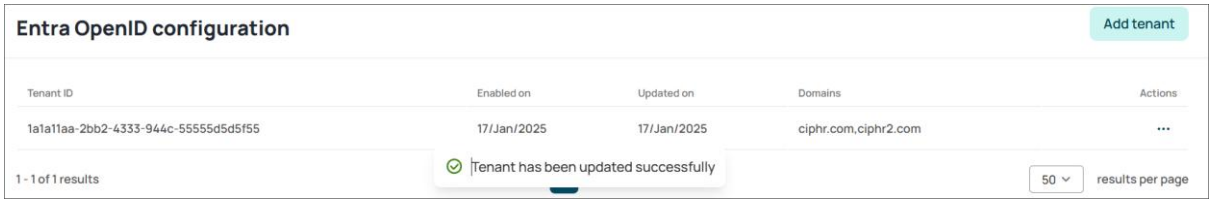
6. Click **+Add**



7. If users need to authenticate with different email domains within this tenant, repeat the last two steps. To remove a domain, click the **x** button next to the domain you wish to delete



8. Click **Submit**



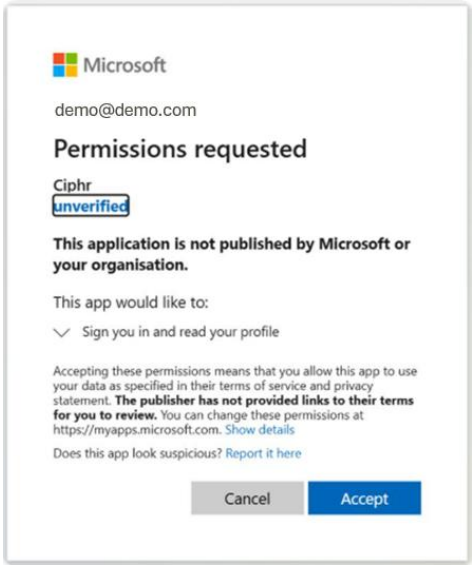
Once activated, users logging in with an email from a previously configured domain will no longer be able to access the system using a username and password. To ensure the setup works correctly, it's good practice to have someone else test it (see next section). This allows the person who configured it to disable or modify the settings if necessary.

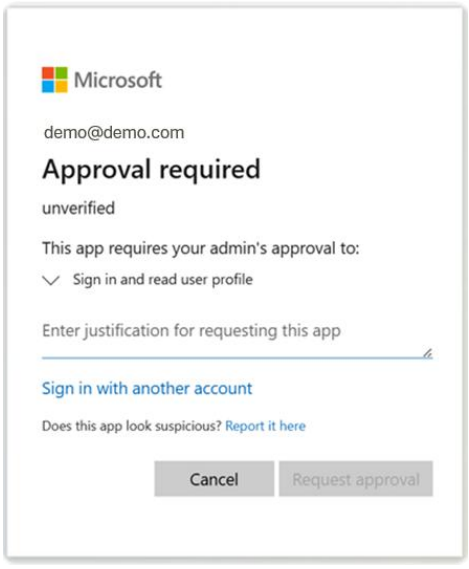
Authorise/Accept App – for IT users only

Depending on your IT configuration for Azure there are two routes to authorise the app. Follow the relevant option below related to which pop-up image is displayed upon initial login:

Option 1 (default permission settings)

Option 2 (enhanced consent permissions)

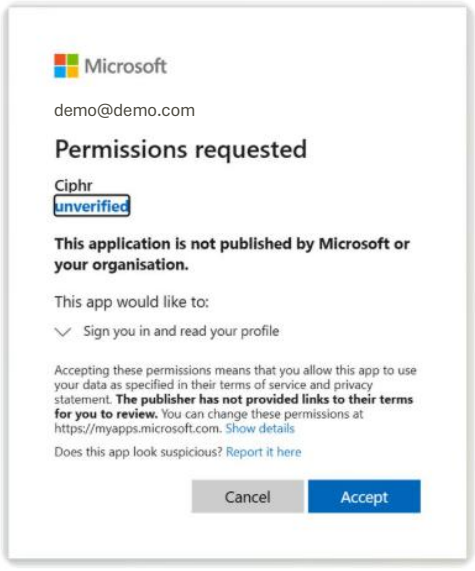




Option 1 (default Azure permission settings)

To authorise the app and prevent all users receiving a permission message follow the steps below:

1. One user on the relevant domain should log into the app and **accept** the app as per the image below:

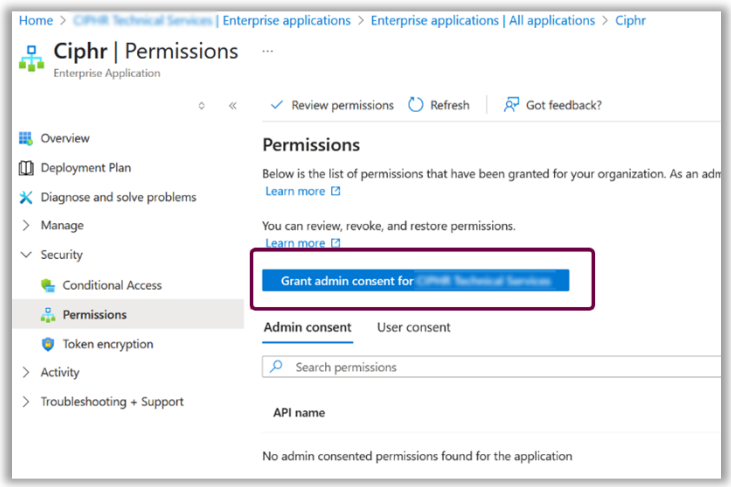


2. Once one person has logged in, your IT Team may now (as an Azure Admin) authorise all users, so that they do not get this prompt.

   This step is vital otherwise all users will receive the above prompt

3. To accept this permission request for all users, an Admin user can manage the app's consent settings within Azure Active Directory (AAD) following the steps below:

   a. Go to the Azure portal and sign in with an account that has the necessary admin rights in your organisation's Azure AD
   b. In the left pane, select **Azure Active Directory**
   c. Under the **Manage** section, click on Enterprise applications
   d. Search for the application ('Ciphr' in this case) in the list of enterprise applications
   e. Select the app, and in the app's pane, go to the "Permissions" section
   f. Click on **Grant admin consent** for [Organisation] to approve the permissions for everyone



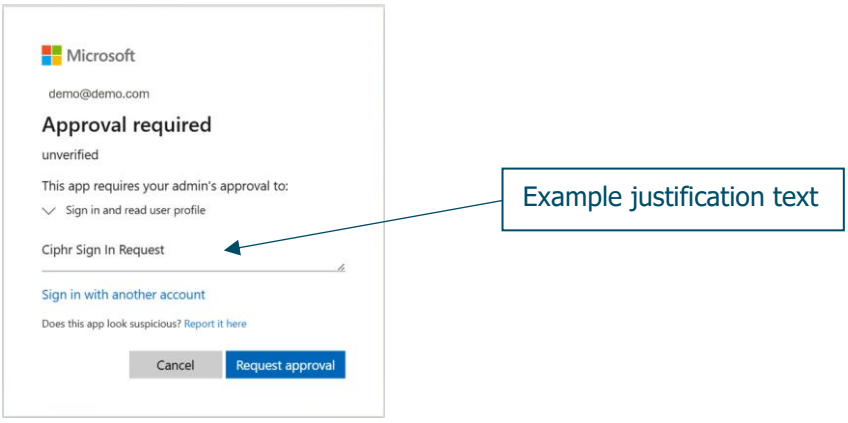
After you've granted the consent, all users in the organisation should automatically be able to accept the app's permissions without the prompt.

By following these steps, you'll have successfully configured your application for SSO with Entra OpenID using Microsoft accounts.

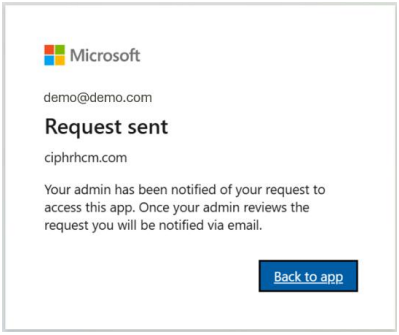
Option 2 (enhanced consent permissions - dedicated admin reviewers)

To authorise the app and prevent all users receiving a permission message follow the steps below:

1. One user on the relevant domain should log into the app to **request approval** for the app, as per the image below:

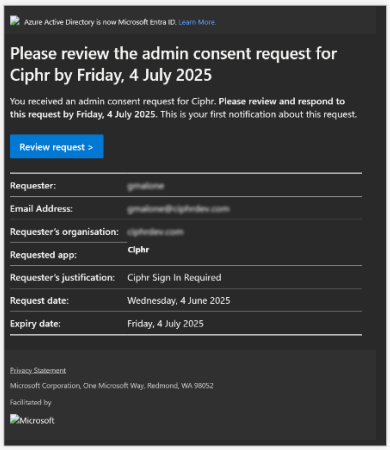


The following pop-up will then display and the request will be sent to your **Azure admin consent reviewer(s)**.



Note: ciphrhcm is the source Azure tenant, not who the request is sent to.

Example email



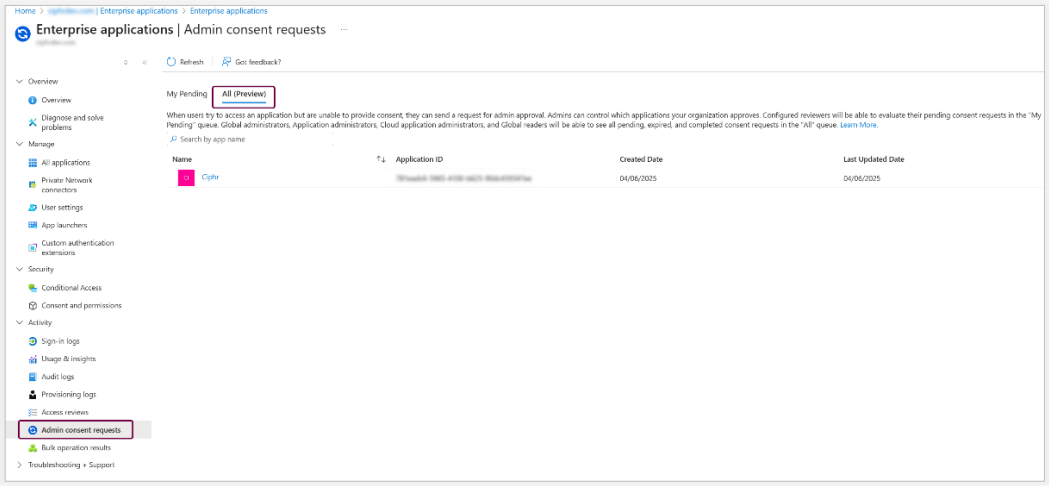
If you don't receive the email request and wish to check where it's been sent, then see the **How to check Azure Admin reviewers** section.

2. Once the request has been sent, your IT Team may now (as an Azure Admin) go to the **Admin consent requests** to authorise the application.

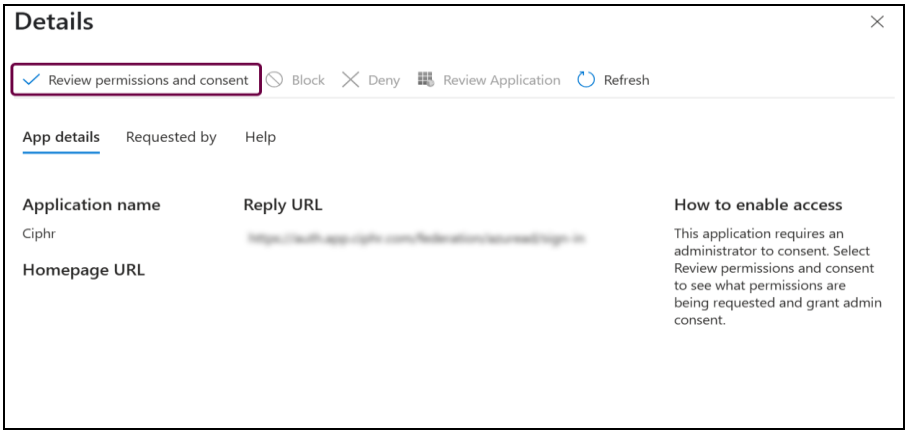
   This step is vital otherwise all users will receive the above prompt

3. To accept this permission request for all users, an Admin user can manage the app's consent settings within Azure Active Directory (AAD) following the steps below:

   a. Go to the Azure portal and sign in with an account that has the necessary admin rights in your organisation's Azure AD
   b. In the left pane, select **Azure Active Directory**
   c. Under the **Manage** section, click on Enterprise applications
   d. Go to **Admin consent requests > All (preview) tab**



   e. Click on the Ciphr app > **Review permissions and consent**

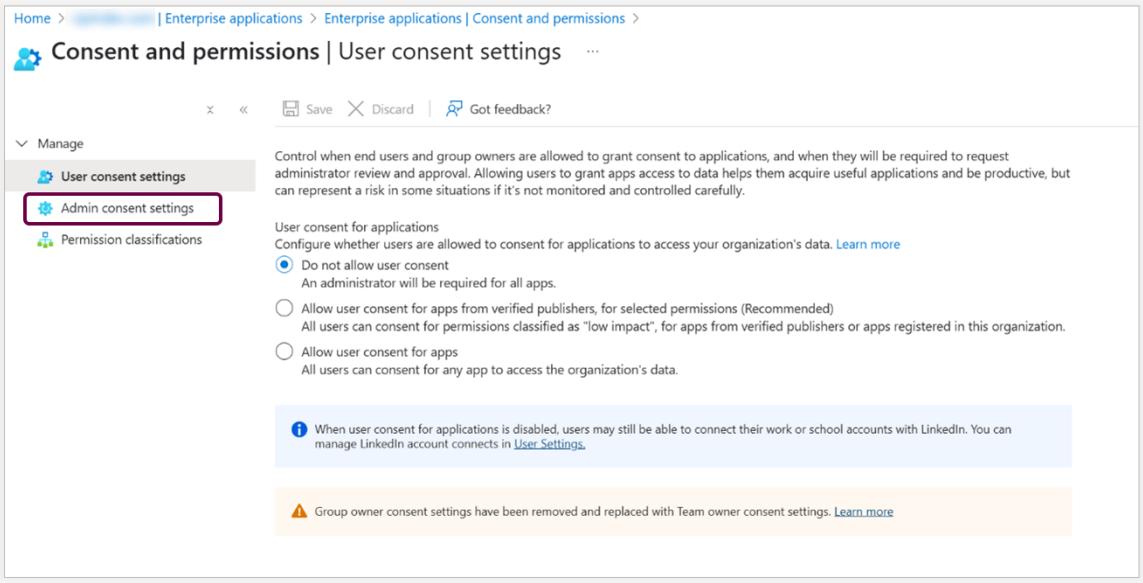


After you've granted the consent, all users in the organisation should automatically be able to accept the app's permissions without the prompt.

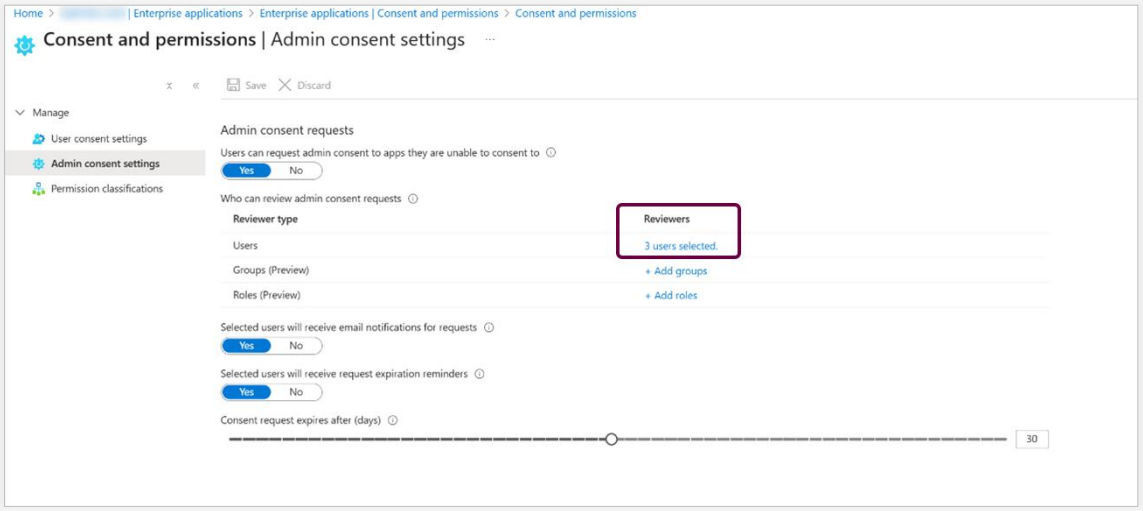
By following these steps, you'll have successfully configured your application for SSO with Entra OpenID using Microsoft accounts.

How to check Azure Admin consent reviewers who will receive the approval email

If you have the following configuration settings then designated reviewers will receive the approval request email.

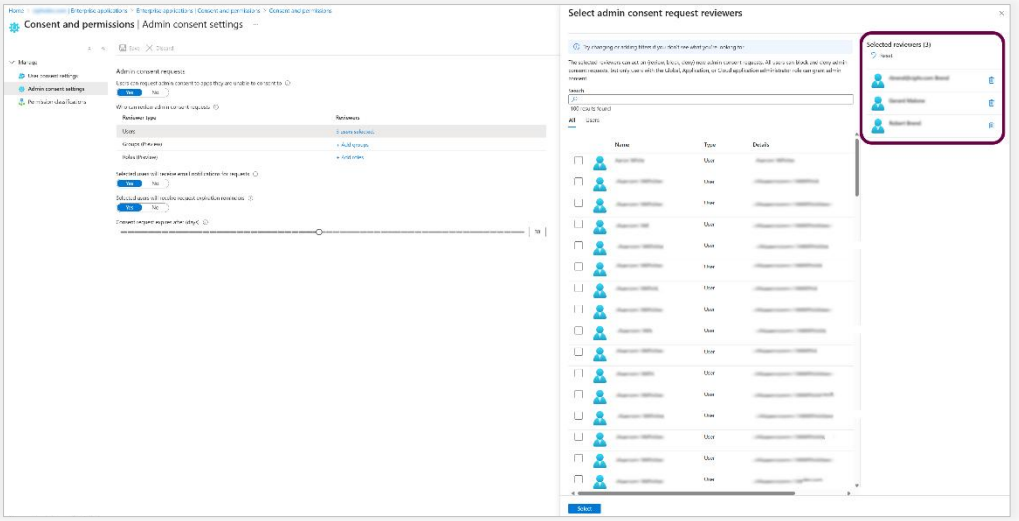


To check the reviewers, click **Admin consent settings**



Click on the **Reviewers** to see who will receive the email.

Entra OpenID (formerly Azure) Tenant configuration for SSO



Example email that will be sent: