

Ciphr HR Sign-In Entra OpenID (formerly Azure) Tenant configuration for SSO

June 2025 | V2.0

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

Demo	hr A	dmin	
Users	Settings	Single sign-on	Branding configuration
			-

 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

Entra OpenID configuration				Add tenant
Tenant ID	Enabled on	Updated on	Domains	Actions
1a1a11aa-2bb2-4333-944c-55555d5d5f55				

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

Entra OpenID configuration			Add tenant	
Tenant ID	Enabled on	Updated on	Domains	Actions

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.

Add tenant		\otimes
Tenant ID (required)		
1a1a11aa-2bb2-4333-944c-5555	55d5d5f55	
Allowed domains (required)		
Allowed domains (required)		+ Add
Allowed domains (required)		+ Add
Allowed domains (required)		+ Add

- 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

Norecordshere	
Add tenant	8
Tenant ID (required)	
1a1a11aa-2bb2-4333-944c-55555d5d5f55	
Allowed domains (required)	+ Add
Cancel	Submit

 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

Ne ve se ve la bava	
Add tenant	×
Tenant ID (required)	
1a1a11aa-2bb2-4333-944c-55555d5d5f55	
Allowed domains (required)	
	+ Add
ciphr.com × ciphr2.com ×	
Cancel	Submit

8. Click Submit

Entra OpenID configuration				Add tenant
Tenant ID	Enabled on	Updated on	Domains	Actions
1a1a11aa-2bb2-4333-944c-55555d5d5f55	17/Jan/2025	17/Jan/2025	ciphr.com,ciphr2.com	
1 - 1 of 1 results	⊘ Tenant has been up	odated successfully		50 v results per page

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:

Microsoft	Microsoft
demo@demo.com	
Permissions requested	demo@demo.com
inhr	Approval required
inverified	unverified
This application is not published by Microsoft or	This app requires your admin's approval to:
our organisation.	✓ Sign in and read user profile
his app would like to:	
 Sign you in and read your profile 	Enter justification for requesting this app
Accepting these permissions means that you allow this app to use	Sign in with another account
tatement. The publisher has not provided links to their terms or you to review. You can change these permissions at	Sign in with another account
attps://myapps.microsoft.com. Show details	Does this app look suspicious? Report it here
loes this app look suspicious? Report it here	
Connect	Cancel Request approval

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

Home > CPHR Inclusion Services Enter	rprise applications > Enterprise applications All applications > Ciphr	
Ciphr Permissions		
0 «	✓ Review permissions 💍 Refresh 🛛 🔗 Got feedback?	
Overview	Permissions	
Deployment Plan	Below is the list of permissions that have been granted for your organization. As an add	
🗙 Diagnose and solve problems	Learn more 🗹	
> Manage	You can review, revoke, and restore permissions.	
✓ Security		
👇 Conditional Access	Grant admin consent for	
Permissions	Admin consent User consent	
Token encryption		
> Activity	Search permissions	
> Troubleshooting + Support	API name	
	No admin consented permissions found for the application	

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)**.

Microsoft
demo@demo.com
Request sent
ciphrhcm.com
Your admin has been notified of your request to access this app. Once your admin reviews the request you will be notified via email.
Back to app

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**

Details		×
 Review permissions and cons 	ent 🛇 Block 🗙 Deny 🌉 Review Application 💍 Refresh	
App details Requested by	Help	
Application name	Reply URL	How to enable access
Ciphr Homepage URL	Mga Cash ago oph orreflederation accessible prin	This application requires an administrator to consent. Select Review permissions and consent to see what permissions are being requested and grant admin 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.

Home > Enterprise applic	cations > Enterprise applications Consent and permissions >
Consent and permis	sions User consent settings
× «	🔚 Save 🗙 Discard 🔗 Got feedback?
∨ Manage	Control when and wave and group gupper are allowed to grant concent to applications, and when they will be convired to request
 User consent settings Admin consent settings 	administrator review and approval. Allowing users to grant apps access to data helps them acquire useful applications and be productive, but can represent a risk in some situations if it's not monitored and controlled carefully.
Permission classifications	User consent for applications Configure whether users are allowed to consent for applications to access your organization's data. Learn more Denot allow user consent An administrator will be required for all apps. Allow user consent for apps from verified publishers, for selected permissions (Recommended) All users can consent for permissions classified as "low impact", for apps from verified publishers or apps registered in this organization.
	All users can consent for any app to access the organization's data.
	When user consent for applications is disabled, users may still be able to connect their work or school accounts with Linkedin. You can manage Linkedin account connects in <u>User Settings</u> .
	A Group owner consent settings have been removed and replaced with Team owner consent settings. Learn more

To check the reviewers, click Admin consent settings

X	« 🔄 Save 🗙 Discard	
Manage User consent settings Admin consent settings	Admin consent requests Users can request admin consent to apps they are unable to consent to O	
Permission classifications	Who can review admin consent requests ① Reviewer type	Reviewers
	Users Crowner (Previous)	3 users selected.
	Roles (Preview)	+ Add gloups + Add roles
	Selected users will receive email notifications for requests () Ves No Selected users will receive request expiration reminders () Ves No Consent remust envires after (rbss) ()	

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

onsent and perm	nissions Admin consent settings			Select	admin consent	request reviewe	rs	102
a se 🖾 for X 7000				O type	Solected rationers (J) 9 met 2 met 2 met met			
 More and edge More counts attitige 	Admin consert repend: Les non-part also conserts log retuge as outputs () The consert of the conserts log retuge () Part conserts of the consert of the consert () Part conserts of the consert of the consert () Part conserts of the co		The tables of products and at physical bits, which we derive a structure of parameters of the second bits are consended on the second bits of the second bits are consended on the second bits are conservation are consended on the second bits are conservation are conservationare conservation are conservationare conservation are conservationare conservation are conservationare conservation					
	0.05	5 store solutions					6	
	Notes (Procine)	 And others 		-	rune	Pase .	URUS .	
	Selected uses to interview end testifications for requests ()			-		Cher		
	Selected across with receive request exploration remine as: (2)			U		Liver		
	Conset requer squee we dep $\subset \bigcirc$	0	10	ш 🥻	- August - 100	Unix		
						Our		
						Liver		
						User		
						Unit		
						Univ		
				Π	-	User		
					-	Unit		
						the		
					Annual Marca	User		
				-		Unar		
				-	-	200		*

Example email that will be sent:

Azure Active Directory is now Microsoft Entra ID. Learn More.							
Please review the admin consent request for Ciphr by Friday, 4 July 2025							
You received an admin consent request for Ciphr. Please review and respond to this request by Friday. 4 July 2025. This is your first notification about this request.							
Review request >							
Requester:	gnatore						
Email Address:	gmalone@ciphedex.com						
Requester's organisation:	ciphedex.com						
Requested app:	Ciphr						
Requester's justification:	Ciphr Sign In Required						
Request date:	Wednesday, 4 June 2025						
Expiry date:	Friday, 4 July 2025						
Privacy Statement							
	ft Way. Redmond, WA 98052						
Microsoft							