

SIGN-IN SETUP · FOR IT ADMINS

Microsoft Entra ID

Sign in with Microsoft work accounts, with optional automatic provisioning of people and groups.

Last updated 6 October 2026

Overview

With Microsoft Entra ID (formerly Azure AD) your people sign in to Cloudraw Connect with their Microsoft work account. Entra checks the password and applies your MFA and Conditional Access policies. Cloudraw never sees the password.

The setup has two parts. The second is optional:

1. **Sign-in**: an app registration in Entra, connected to Cloudraw. About 15 minutes.
2. **SCIM provisioning (optional)**: Entra creates people and groups in Cloudraw, keeps them up to date, and suspends people you disable in Entra. About 10 minutes.

You need

- An Entra role that can register applications and grant consent, for example *Application Administrator* or *Cloud Application Administrator*. SCIM needs the same role.
- The *Owner* or *Security admin* role in the Cloudraw admin console.
- Every user who will sign in must have an e-mail address in Entra.

Step 1. Copy the redirect URI from Cloudraw

1 Open Identity & SSO

In the Cloudraw admin console go to **Settings** → **Identity & SSO**. If **Workspace sign-in** is not on yet, turn it on. This also sets your workspace name.

2 Copy the redirect URI

In **Your identity provider**, copy the value under *Redirect URI (add this at your provider)*. It looks like this:

```
https://id-stg.cloudraw.com/ui/login/login/externalidp/callback
```

Always copy it from your console rather than from this guide.

Step 2. Register the app in Microsoft Entra

- 1 Open App registrations**
Sign in to the [Microsoft Entra admin center](https://entra.microsoft.com) (<https://entra.microsoft.com>) and go to **Identity** → **Applications** → **App registrations**. Click **New registration**.
- 2 Name and account type**
Name: `Cloudraw`. Supported account types: **Accounts in this organizational directory only (Single tenant)**.
- 3 Redirect URI**
Platform: **Web**. Paste the redirect URI from step 1. Click **Register**.
- 4 Copy two IDs**
On the app's **Overview** page copy the **Application (client) ID** and the **Directory (tenant) ID**.
- 5 Create a client secret**
Go to **Certificates & secrets** → **Client secrets** → **New client secret**. Choose an expiry (Microsoft recommends 180 days or less) and click **Add**. Copy the secret's **Value** right away. Entra shows it only once. You do not need the *Secret ID*.
- 6 Check API permissions**
Under **API permissions**, the app needs these **Microsoft Graph, delegated** permissions: `openid`, `profile`, `email` and `User.Read`. `User.Read` is there by default. Add the other three with **Add a permission** → **Microsoft Graph** → **Delegated permissions**, then click **Grant admin consent for your organization** so users are not asked one by one.

IMPORTANT

Write down when the client secret expires and set a reminder. When it expires, nobody can sign in through Entra. To rotate it, create a new secret in Entra, paste it into Cloudraw (step 3), and delete the old secret only after that.

Step 3. Connect Entra in Cloudraw

- 1 Choose Microsoft**
In **Settings** → **Identity & SSO** → **Your identity provider**, choose **Microsoft**.
- 2 Fill in the fields**
Use the table below.
- 3 Save**
Cloudraw checks the details with Microsoft. If it reports *"The provider could not be configured. Check the client id, secret and issuer"*, check the values for typos and make sure you pasted the secret *Value*, not the *Secret ID*.

4

Test with a real account

On a test computer, open Clouddraw Connect, type your workspace name and click **Sign in**. You should land on the Microsoft sign-in page.

Clouddraw field	Value from Entra	Required
Client ID	Application (client) ID	Yes
Client secret	The client secret Value	Yes
Tenant ID	Directory (tenant) ID, a GUID such as 7f1c2a9e-.... Only accounts from your own Entra tenant can sign in.	Yes
Button label	What the sign-in button says. Default: "Microsoft".	No
Only allow sign-in through the provider	On: people go straight to Microsoft, and Clouddraw passwords are turned off in this workspace. Off: the Clouddraw sign-in page shows a password form and a "Sign in with Microsoft" button.	No

TIP

Turn on **Only allow sign-in through the provider** once your test sign-in works. People then never see a second sign-in page, and every sign-in goes through Entra MFA and Conditional Access. Accounts created with *Add a user* can no longer sign in with a password.

The client secret is sent to the sign-in service and never shown again. The console shows a status line such as *Federated to Microsoft since*

How people get into Clouddraw

- **Without SCIM:** a person who signs in through Entra for the first time is added to **People** automatically. Their seat is used from then on. Put them in Clouddraw groups for access rules. You can also add people in advance under **People** → **Add a person** with the same e-mail address.
- **With SCIM** (step 4): Entra creates the people and their groups in advance and keeps them in sync.

To limit who can sign in, open the app in **Enterprise applications**, set **Assignment required?** to **Yes** under **Properties**, and assign the users or groups who need Clouddraw.

Step 4 (optional). SCIM provisioning from Entra

4a. Turn on SCIM in Cloudraw

1 Turn on SCIM

In **Settings** → **Identity & SSO** → **SCIM provisioning**, click **Turn on SCIM**.

2 Copy both values

Copy the **base URL** and the **token**. The token starts with `crwscim_` and is shown **once**. The base URL looks like:

```
https://orchestrator-stg.cloudraw.com/v0/tenants/<your workspace id>/scim/v2
```

4b. Create the provisioning app in Entra

1 New enterprise application

In the Entra admin center go to **Identity** → **Applications** → **Enterprise applications** → **New application** → **Create your own application**. Name it `Cloudraw provisioning` and choose **Integrate any other application you don't find in the gallery (Non-gallery)**.

2 Open Provisioning

In the new app open **Provisioning**, click **Get started** or **New configuration**, and set **Provisioning Mode** to **Automatic**.

3 Admin credentials

- **Tenant URL:** the Cloudraw base URL followed by `?aadOptscim062020`, for example `https://orchestrator-stg.cloudraw.com/v0/tenants/<id>/scim/v2?aadOptscim062020`. This Microsoft option makes Entra follow the SCIM standard, so disabling a user in Entra suspends them in Cloudraw correctly.
- **Secret Token:** the `crwscim_...` token.

Click **Test Connection**. It should succeed.

4 Check the attribute mappings

Under **Mappings** → **Provision Microsoft Entra ID Users**, `userName` must be each person's e-mail address. The default maps `userPrincipalName`. If your UPNs are not the same as people's e-mail addresses, map `userName` to `mail` instead. Cloudraw matches the people Entra creates to the people who sign in by e-mail address.

5 Choose who is provisioned

Under **Settings** → **Scope** choose **Sync only assigned users and groups**, then assign the users and groups under **Users and groups**.

6

Start

Set **Provisioning Status** to **On** and save. Entra's first cycle can take up to 40 minutes. After that, changes sync about every 40 minutes. Use **Provision on demand** to test one user right away.

What SCIM does in Cloudraw

In Entra	In Cloudraw
User assigned	Person created in People (uses a seat)
User changed (name, e-mail)	Person updated
User disabled or unassigned	Person suspended , so their devices lose access
User deleted	Person removed, and the seat is freed
Group assigned	Group created, members kept in sync. Ready to use in access rules.

NOTE

Groups that come from SCIM are managed by Entra and are read-only in Cloudraw. To rotate the SCIM token, click to generate a new one in Cloudraw and paste it into Entra right away, because the old token stops working at once. Turning SCIM off disables the token.

MFA and Conditional Access

Multi-factor authentication for Entra users happens **at Microsoft**. Whatever your Entra MFA, Security Defaults or Conditional Access policies require for this app (Microsoft Authenticator, FIDO2 keys, compliant device, trusted locations) applies when people sign in to Cloudraw Connect. To target Cloudraw in Conditional Access, choose the *Cloudraw* app registration under **Target resources**.

Cloudraw does not add its own e-mail code for Entra users, with one exception: a workspace that sent Cloudraw invitations *before* Entra was connected keeps the Cloudraw e-mail code as an extra step after the Microsoft sign-in. See [Two-factor authentication](#).

On top of sign-in, Cloudraw can ask people to sign in again on each device at a set interval. Set it in **Settings** → **Identity & SSO** → **Re-authentication** (every 8 hours, 24 hours, 7 days, or a custom interval). Each new sign-in goes through Entra again, MFA included.

Troubleshooting

Message or symptom	Cause and fix
Microsoft shows <code>AADSTS50011</code> (redirect URI mismatch)	The redirect URI in the app registration is not exactly the one in Cloudraw. Copy it again. It must be under the Web platform, not SPA or mobile.
Microsoft shows <code>AADSTS7000215</code> (invalid client secret)	You pasted the Secret ID instead of the Value, or the secret has expired. Create a new secret and paste its Value into Cloudraw.
Microsoft shows <code>AADSTS50105</code> (user not assigned)	Assignment is required and the user is not assigned to the app. Assign them or their group.
Cloudraw Connect: <i>"Your email address is not verified with your identity provider" or "did not share an email address"</i>	The user has no e-mail address in Entra. Add one (the <i>Email</i> field on the user).
Cloudraw Connect: <i>"This account does not match the person registered with that email"</i>	A person with that e-mail address already exists in Cloudraw with a different sign-in account, for example from before you connected Entra. Contact support to re-link.
Cloudraw Connect: <i>"seat quota reached"</i>	All seats on your plan are used. Remove people you no longer need or upgrade your plan.
SCIM Test Connection fails with 401	Wrong or rotated token. Generate a new one in Cloudraw and paste it.

Need help? E-mail support@cloudraw.com

Last updated 6 October 2026

© 2026 Cloudraw