

SIGN-IN SETUP · FOR IT ADMINS

Active Directory (on-premises)

Let people sign in with their existing Windows domain account, reached privately through the Clouddraw connector.

Last updated 6 October 2026

How it works

People sign in to Clouddraw Connect with their normal Windows domain username and password. Clouddraw checks the password against your domain controller (DC) through the **Clouddraw connector** that already runs in your network. The connector only makes outbound connections, so you do not open any port to the internet and your DC is never exposed.

After the AD password, Clouddraw sends a **one-time code** to the e-mail address in the user's AD account. The user types it to finish signing in. See [Two-factor authentication](#).

TIP

Domain-joined and workgroup computers both work. Sign-in happens in a browser window with the domain username and password, so the computer does not need to be joined to the domain. A home laptop, a workgroup PC in a branch office and a domain-joined desktop all sign in the same way.

Before you start

You need	Details
A Clouddraw connector that can reach a DC	A Windows or Linux machine (or Docker) inside your network with the Clouddraw connector installed and shown as <i>connected</i> in Connectors . It needs outbound TCP 443 to <code>*.clouddraw.com</code> , and it must reach a domain controller on TCP 636 (LDAPS) or TCP 389 (StartTLS or plain LDAP). Any machine that can reach the DC works. It does not have to be the DC.
The DC's address	As the connector machine sees it, for example <code>dc01.corp.local</code> or <code>10.0.0.5</code> . With LDAPS the name must match the DC's certificate, so use the DNS name rather than the IP.

You need	Details
A read-only service account	A normal domain user with no admin rights, used only to look users up. See Create the service account .
Your base DN	The top of your directory, for example <code>DC=corp,DC=local</code> .
An AD group for Cloudraw users	Only its members can sign in, for example <code>CN=Cloudraw Users,OU=Groups,DC=corp,DC=local</code> .
An e-mail address on every user	The sign-in code is sent to the AD <code>mail</code> attribute (or another attribute you choose). A user without an e-mail address cannot complete sign-in.
An admin role	You need the <i>Owner</i> or <i>Security admin</i> role in the Cloudraw admin console.

TIP

Don't have a connector yet? In the admin console open **Connectors** (or step 2 of onboarding, *Connect your network*), download the connector and run the install command on a machine in your network. A second connector keeps things working if one machine goes down.

Prepare Active Directory

1. Create the service account

1 Create a dedicated user

In *Active Directory Users and Computers*, create a user such as `svc-cloudraw`. Give it a long random password (25+ characters).

2 Keep it unprivileged

Leave it only in *Domain Users*. It needs to read users and groups, which every authenticated domain user can do by default. Do **not** add it to Domain Admins or any admin group.

3 Lock it down

Tick *Account is sensitive and cannot be delegated*. Optionally use *Log On To* to stop it from signing in to workstations interactively.

4 Note its name

Cloudraw accepts a DN (`CN=svc-cloudraw,OU=Service Accounts,DC=corp,DC=local`), a UPN (`svc-cloudraw@corp.local`) or `CORP\svc-cloudraw`.

2. Create the sign-in group

Create a security group such as **Cloudraw Users** and add the people who should use Cloudraw. Copy its distinguished name. In *Active Directory Users and Computers*, turn on **View** → **Advanced Features**, open the group, and copy `distinguishedName` from the *Attribute Editor* tab. In PowerShell you can run:

```
Get-ADGroup "Cloudraw Users" | Select-Object -ExpandProperty DistinguishedName
```

3. Check that LDAPS works (recommended)

LDAPS needs a certificate on the DC, usually issued by your AD Certificate Services or another CA. From the connector machine you can test the port:

```
Test-NetConnection dc01.corp.local -Port 636
```

If the DC's certificate comes from your own internal CA, export that CA's certificate in Base-64 (PEM) format. You will paste it into Cloudraw so it can verify the DC.

Connect Active Directory in Cloudraw

1 Open the settings

In the Cloudraw admin console go to **Settings** → **Active Directory**. You can also get there from onboarding step 3, *Sign-in for your users*, by choosing Active Directory.

2 Fill in the form

Use the table below.

3 Save

Click **Save**. The service account password is stored encrypted and is never shown again.

4 Test

Run the connection test and read the result. See [The connection test](#).

Field	What to enter	Example
Connector	The connector that can reach your DC.	office-connector-1
Domain controller address	The DC's name or IP as the connector machine sees it. With LDAPS use the name on the certificate.	dc01.corp.local
Connection security	LDAPS (port 636) is recommended. StartTLS (port 389) also encrypts. None — plain LDAP (port 389) is not encrypted and should be used only for a first test.	LDAPS (port 636)
Port	Filled in from the connection security. Change it only if your DC listens elsewhere.	636
CA certificate	Only if the DC's certificate comes from your own CA. Paste it in PEM format (starts with -----BEGIN CERTIFICATE-----).	
Base DN	The top of your directory.	DC=corp,DC=local
Service account	The read-only account: a DN, user@domain or DOMAIN\user .	svc-cloudraw@corp.local1
Service account password	Its password. Required the first time. Leave it empty later to keep the stored one.	

Field	What to enter	Example
AD group allowed to sign in	The full DN of the group. Only its members can sign in.	CN=Cloudraw Users,OU=Groups,DC =corp,DC=local
Users sign in with	Username (sAMAccountName, <code>jsmith</code>), UPN (<code>jsmith@corp.local</code>) or E-mail address .	Username (jsmith)
User search DN	Optional. Where users are looked up, if you want to limit it to one OU. Blank means the base DN.	OU=Staff,DC=corp, DC=local
E-mail attribute	Optional. The AD attribute that holds the address the sign-in code goes to. Blank means <code>mail</code> .	mail

IMPORTANT

A DN must be written in full, for example `OU=Staff,DC=corp,DC=local`, not `corp.local/Staff`. If a value is not valid, the form names the field and says what it expects.

The connection test

The test runs step by step and stops at the first problem. Each step reports *passed*, *failed* or *not run*. You can run it up to 20 times an hour.

Step	What it checks	If it fails
Connector	The connector you chose is online.	<i>The selected connector is offline.</i> Check the connector machine is running and the service is started. Look at its status under Connectors .
Private path	The connector has picked up the private path to your DC.	<i>The connector has not picked up the directory path yet.</i> This usually clears by itself within a minute after saving. Wait and test again.
Reach	The connector can open a connection to the DC address and port.	Wrong address or port, a firewall between the connector and the DC, or a DNS name the connector machine cannot resolve. Test from the connector machine with <code>Test-NetConnection <dc> -Port 636</code> .
TLS	The encrypted connection is set up and the DC's certificate is trusted.	No certificate on the DC (LDAPS not enabled), a certificate name that does not match the address you typed, or a private CA that you have not pasted in <i>CA certificate</i> .
Bind	The service account can sign in to the directory.	Wrong service account name or password, or the account is disabled, locked or has an expired password.
User search	Users can be found under the base DN or user search DN.	Wrong base DN or user search DN, or the "Users sign in with" attribute does not match your accounts.
Sign-in group	The AD group exists and has members.	Wrong group DN (copy it again from the Attribute Editor), or the group is empty.

NOTE

If the result says *"Not run – the directory sign-in test is being enabled on the Cloudraw side; your settings are saved"*, the first two steps passed and your settings are kept. Nothing is wrong on your side. Contact support@cloudraw.com (mailto:support@cloudraw.com) and we will finish enabling Active Directory sign-in for your workspace.

When all steps pass, the status changes to **Connected** and Active Directory sign-in is ready for your users.

How your users sign in

- 1 Open Cloudraw Connect**
They choose **Sign in** and type your workspace name.
- 2 Enter the AD username and password**
A browser window opens. They enter the username in the form you chose (for example `jsmith`) and their normal Windows password.
- 3 Enter the e-mail code**
Cloudraw e-mails a one-time code to the address in their AD account. They type it in the browser.
- 4 Done**
The computer is registered to that person. Depending on your device trust settings it may have to be trusted before it can reach anything. See [Install Cloudraw Connect](#).

Send your users the guide [Install Cloudraw Connect and enroll your computer](#) together with your workspace name.

Domain and workgroup computers in access rules

Every computer running Cloudraw Connect reports whether it is joined to an AD domain. In an access rule you can use this as a device condition:

- **Any:** the computer type does not matter.
- **Domain computers:** only computers joined to your domain.
- **Workgroup computers:** only computers that are *not* joined to a domain. Computers joined only to Microsoft Entra ID or managed only by an MDM count as workgroup computers.
- **Domain or workgroup:** either kind, as long as the computer has reported it.

For example, allow the accounting app only from domain computers, and allow the file share from both.

NOTE

A computer that has not reported its status recently matches neither "domain" nor "workgroup", so a rule that requires one of them does not let it in until it reports again.

Security recommendations

- **Use LDAPS (port 636), or at least StartTLS.** Plain LDAP sends the service account and user passwords unencrypted between the connector and the DC. The traffic stays inside your network, but it should still be encrypted.
- **Least privilege.** The service account only reads. Keep it out of every admin group and use it for nothing else.
- **Rotate the service account password** on your normal schedule, for example every 6 to 12 months, and when an admin who knew it leaves. Change it in AD first, then enter the new password in **Settings** → **Active Directory**, save, and run the test.
- **Keep the sign-in group small.** Add only people who need remote access, and remove leavers as part of offboarding.
- **Make sure every user has a correct e-mail address in AD.** The sign-in code goes there. A wrong address means someone else's inbox receives the code.
- **Run two connectors** that can reach a DC, so sign-in keeps working when one machine is down for maintenance.

Troubleshooting

Problem	What to check
A user's password is rejected	Is the user a member of the sign-in group? Is the account enabled, not locked, with a valid password? Does the username match the "Users sign in with" setting?
The e-mail code never arrives	The user's AD account needs an e-mail address in the attribute you configured. See Two-factor authentication: troubleshooting .
Sign-in stopped working for everyone	Is the connector online? Did the service account password expire or change? Run the test again.
Saving says the settings were changed elsewhere	Someone else, or you in another tab, changed the settings in the meantime. Reload the page, check the values and save again.

To disconnect Active Directory, remove the configuration in **Settings** → **Active Directory**. Cloudraw deletes the private path through your connector.

Need help? E-mail support@cloudraw.com Last updated 6 October 2026 © 2026 Cloudraw