

SIGN-IN SETUP · FOR IT ADMINS

Okta and other OpenID Connect providers

Okta, JumpCloud, Keycloak, Ping and other OpenID Connect providers, with optional SCIM provisioning.

Last updated 6 October 2026

Overview

Clouddraw connects to any identity provider that supports **OpenID Connect** (OIDC) with the authorization code flow and a client secret. Your people sign in at your provider with the account and MFA you already manage there.

In **Settings** → **Identity & SSO** → **Your identity provider** you can choose:

Choice	Use it for	You enter
Okta	Okta organizations on an <code>okta.com</code> , <code>oktapreview.com</code> or <code>okta-emea.com</code> address	Your Okta org URL, client ID, client secret
JumpCloud	JumpCloud	Client ID, client secret (the issuer is filled in for you)
OpenID Connect	Any other OIDC provider: Keycloak, Ping, Authentik, Okta with a custom domain, and others	Issuer URL, client ID, client secret

What Clouddraw needs from every provider:

- A **confidential web client** (client ID plus client secret) using the **authorization code** flow.
- The scopes `openid`, `profile` and `email`.
- An `https` issuer URL with a working discovery document at `<issuer>/.well-known/openid-configuration`.
- A **verified e-mail address** for every user. Users whose e-mail is not verified at the provider are refused with *"Your email address is not verified with your identity provider"*.

Step 1. Copy the redirect URI from Clouddraw

In the Clouddraw admin console open **Settings** → **Identity & SSO**, turn on **Workspace sign-in** if needed, and copy *Redirect URI (add this at your provider)*. It looks like:

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

Step 2a. Okta: create the app integration

1

Create the integration

In the Okta Admin Console go to **Applications** → **Applications** → **Create App Integration**. Choose **OIDC - OpenID Connect** and **Web Application**.

2

General settings

Name: `Cloudraw`. Grant type: **Authorization Code** only.

3

Sign-in redirect URI

Remove the example and paste the Cloudraw redirect URI. Leave the sign-out redirect empty.

4

Assignments

Choose **Limit access to selected groups** and pick the groups that should use Cloudraw, or assign people later on the *Assignments* tab.

5

Copy the credentials

Save. On the *General* tab, under *Client Credentials*, check that **Client authentication** is *Client secret*. Copy the **Client ID** and the **Client secret**.

6

Note your Okta org URL

It is the address of your Okta sign-in page, for example `https://acme.okta.com`. Use this *without* `-admin` and without a path.

Connect Okta in Cloudraw

1

Choose Okta

In **Settings** → **Identity & SSO** → **Your identity provider** choose **Okta**.

2

Fill in the fields

Okta URL (issuer): `https://acme.okta.com`. Then the client ID and client secret. Optionally set a button label and **Only allow sign-in through the provider**.

3

Save and test

Sign in from Cloudraw Connect on a test computer. You should land on your Okta sign-in page.

NOTE

Using an Okta **custom domain** such as `login.acme.com`? The Okta choice accepts only `okta.com`-style addresses. Choose **OpenID Connect** instead and enter your custom domain as the issuer, exactly as it appears in `https://login.acme.com/.well-known/openid-configuration`.

Step 2b. JumpCloud

1

Create the application

In the JumpCloud Admin Portal go to **SSO Applications** → **Add New Application** → **Custom Application** and choose **OIDC**.

2

Configure it

Redirect URI: the Cloudraw redirect URI. Client authentication type: **Client Secret Basic**.
Login URL: your Cloudraw sign-in, or any URL your portal should open. Include the **Email** and **Profile** standard scopes.

3

Copy the credentials

Activate the app and copy the **Client ID** and **Client Secret**. JumpCloud shows the secret once. Bind the user groups that should use Cloudraw.

4

Connect in Cloudraw

Choose **JumpCloud** and paste the client ID and secret. The issuer

`https://oauth.id.jumpcloud.com` is set for you.

Step 2c. Any other OpenID Connect provider

1

Create a client at your provider

A confidential web client with the authorization code flow, a client secret, the Clouddraw redirect URI as the allowed redirect URI, and the scopes `openid profile email`.

2

Find the issuer URL

Open `<your provider>/.well-known/openid-configuration` in a browser and copy the "issuer" value exactly.

3

Connect in Clouddraw

Choose **OpenID Connect**, enter the issuer, client ID and client secret, and optionally a button label (default "Company sign-in").

Provider	Typical issuer URL	Notes
Keycloak	<code>https://sso.example.com/realms/<realm></code>	Client type OpenID Connect, <i>Client authentication On, Standard flow On</i> . Turn on <i>Email verified</i> for users, or they are refused.
PingOne	<code>https://auth.pingone.com/<environment id>/as</code>	Web app, Authorization Code, token endpoint auth <i>Client Secret Basic</i> or <i>Post</i> .
Authentik	<code>https://auth.example.com/application/o/<slug>/</code>	OAuth2/OpenID provider, client type Confidential.

IMPORTANT

Clouddraw removes a trailing `/` from the issuer you enter. If your provider's "issuer" value ends with a `/` (Authentik and Auth0 do), test a sign-in before you roll out. If it fails, contact support@clouddraw.com (mailto:support@clouddraw.com).

If saving fails with *"The provider could not be configured. Check the client id, secret and issuer"*, check that the issuer opens the discovery document in a browser and that the ID and secret have no extra spaces.

People and groups

A person who signs in through your provider for the first time is added to **People** automatically and uses a seat. To have groups from your provider in Clouddraw, and to suspend people automatically when you deactivate them, set up SCIM below. Otherwise create [Clouddraw groups](#).

Step 3 (optional). SCIM provisioning

In Cloudraw

1 Turn on SCIM

Open **Settings** → **Identity & SSO** → **SCIM provisioning** and click **Turn on SCIM**.

2 Copy the base URL and token

The token starts with `crwscim_` and is shown once. The base URL looks like `https://orchestrator-stg.cloudraw.com/v0/tenants/<workspace id>/scim/v2`.

In Okta

1 Enable SCIM on an app integration

Open the Cloudraw app, then **General** → **App Settings** → **Edit**, and under *Provisioning* select **SCIM**. If your Okta org does not offer SCIM on an OIDC app, create a separate **SWA** app integration called `Cloudraw provisioning` and enable SCIM there.

2 Connection settings

On the new **Provisioning** → **Integration** tab click **Edit**:

- **SCIM connector base URL**: the Cloudraw base URL
- **Unique identifier field for users**: `userName`
- **Supported provisioning actions**: *Push New Users, Push Profile Updates, Push Groups*
- **Authentication Mode**: **HTTP Header**. Paste the `crwscim_...` token as the Bearer token.

Click **Test Connector Configuration**, then **Save**.

3 Turn on actions

Under **Provisioning** → **To App** enable **Create Users**, **Update User Attributes** and **Deactivate Users**.

4 Push groups

On the **Push Groups** tab, push the groups you want to use in Cloudraw access rules.

Okta's `userName` must be the person's e-mail address. That is Okta's default when usernames are e-mail addresses. Deactivating a user in Okta suspends them in Cloudraw, and their devices lose access.

Other providers

Any provider that supports SCIM 2.0 with a bearer token works. Cloudraw supports Users and Groups, filtering by `userName eq "..."`, `externalId` and `displayName`, and PATCH. It does not support bulk operations, sorting or password changes.

MFA: Okta Verify and others

For people who sign in through Okta, JumpCloud or another provider, MFA happens **at your provider**. Clouddraw does not add its own e-mail code, unless the workspace sent Clouddraw invitations before you connected the provider. See [Two-factor authentication](#).

To require **Okta Verify** for Clouddraw:

1 Enroll the authenticator

Under **Security** → **Authenticators**, make sure Okta Verify is set up and an enrollment policy asks users to enroll it.

2 Create an app sign-in policy

Under **Security** → **Authentication Policies**, add a policy, for example *Clouddraw*, with a rule where *User must authenticate with* is **Password + Another factor** or **Any 2 factor types**. Optionally require a phishing-resistant authenticator.

3 Assign the policy

On the policy's *Applications* tab, add the Clouddraw app.

JumpCloud: turn on MFA for users under **User Management**, or with Conditional Access policies on the Clouddraw application. Keycloak: add OTP or WebAuthn to the realm's browser flow.

Troubleshooting

Message or symptom	Cause and fix
Provider says the redirect URI is not allowed	The redirect URI at the provider is not exactly the one Clouddraw shows. Paste it again.
Okta: <i>"User is not assigned to the client application"</i>	Assign the user, or their group, to the Clouddraw app in Okta.
Clouddraw: <i>"issuer must be your Okta org URL"</i>	Use <code>https://<org>.okta.com</code> . For a custom domain choose OpenID Connect.
Clouddraw Connect: <i>"Your email address is not verified with your identity provider"</i>	Mark the user's e-mail as verified at the provider (for example in Keycloak), or make sure the provider sends <code>email_verified</code> .
SCIM test fails with 401	Wrong or rotated token. Generate a new one in Clouddraw and paste it into the provider.
SCIM: <i>"a user with this userName already exists"</i>	A person with that e-mail already exists in Clouddraw, for example added by hand. Remove the duplicate, or let Okta import and match it.

