

SECURITY · FOR IT ADMINS

Two-factor authentication

How the second sign-in step works in Clouddraw, and how it combines with your provider's own MFA.

Last updated 6 October 2026

Which second step applies to whom

Every sign-in to Clouddraw Connect has two steps. Something the person *knows* (a password), then proof that they can reach something they *have*. Which second step is used depends on your sign-in method:

Sign-in method	Second step	Managed in
Clouddraw accounts	Clouddraw e-mail code, on every sign-in	Clouddraw (always on)
Active Directory	Clouddraw e-mail code, sent to the user's AD e-mail address	Clouddraw (always on)
Microsoft Entra ID	Entra MFA: Microsoft Authenticator, FIDO2 keys, Windows Hello, and so on	Entra (Security Defaults or Conditional Access)
Google Workspace	Google 2-Step Verification	Google Admin console
Okta, JumpCloud, other OIDC	The provider's MFA, for example Okta Verify	Your provider

NOTE

For Entra, Google, Okta and other providers, Clouddraw relies on your provider's MFA and does not add its own e-mail code. The exception: if your workspace sent Clouddraw invitations *before* you connected the provider, the Clouddraw e-mail code stays on as well, after the provider sign-in. If you are unsure which applies to you, sign in once on a test computer, or ask support@clouddraw.com (mailto:support@clouddraw.com).

SMS codes are not supported. Codes go by e-mail, or through your provider's own methods.

The Cloudraw e-mail code

When it is on

The e-mail code is the second step for **every sign-in** to a workspace that uses Cloudraw accounts or Active Directory. It is turned on automatically: when you send the first invitation, and for Active Directory sign-in. There is no switch to turn it off, so a stolen password alone is never enough to get in.

What your people see

1 Password first

In the sign-in window that Cloudraw Connect opens, they enter their username or e-mail address and their password.

2 A code by e-mail

Cloudraw sends an e-mail with the subject "**Your sign-in code for *your workspace***". It reads *"Use this one-time code to finish signing in"*, followed by the code.

3 Type the code

They type the code in the sign-in window. The code works once and **expires after a few minutes**. If it has expired, they start the sign-in again and a new code is sent.

The e-mail also says: *"If you did not try to sign in, ignore this e-mail and tell your IT team."* Ask your people to do exactly that. An unexpected code means someone knows their password, so reset it.

TIP

Tell your people in advance that the e-mail comes from `noreply@cloudraw.com`, or from your own sender address if you set one up below. They then know it is genuine.

Who sends it

- **By default:** `Cloudraw <noreply@cloudraw.com>`, in Cloudraw's branded template, with your workspace name in the subject.
- **From your own domain:** once you have verified your own sender (see below), codes and invitations come from that address, for example `Acme IT <it@acme.com>`.
- If your own sender stops working, for example because a DNS record was removed, Cloudraw sends from `noreply@cloudraw.com` instead, so codes still arrive.

Asking people to sign in again

A sign-in is not forever. In **Settings** → **Identity & SSO** → **Re-authentication** choose how often people must sign in again on each device: **Off**, **every 8 hours**, **every 24 hours**, **every 7 days**, or a

custom interval. Each new sign-in includes the second step. Until the person signs in again, the device is treated as untrusted. Cloudraw Connect shows a **Sign in again** button.

You can also make one device sign in again right away, for example after a suspected theft, from that device's page under **Devices**.

Provider MFA: quick reference

Microsoft Entra ID

- **Small tenants:** turn on *Security Defaults* (**Entra admin center** → **Identity** → **Overview** → **Properties** → **Manage security defaults**). This requires Microsoft Authenticator for everyone.
- **With Entra ID P1/P2:** create a Conditional Access policy that targets the *Cloudraw* app with *Grant: Require multifactor authentication*, or better, an authentication strength such as *Phishing-resistant MFA*.
- Details: [Microsoft Entra ID guide, MFA section](#).

Google Workspace

- **admin.google.com** → **Security** → **Authentication** → **2-step verification**: allow it, set Enforcement to On, and prefer security keys or the Google prompt over text messages.
- Details: [Google Workspace guide, 2-Step Verification](#).

Okta

- Set up Okta Verify under **Security** → **Authenticators**, then assign an authentication policy that requires two factors to the Cloudraw app.
- Details: [Okta guide, MFA section](#).

JumpCloud, Keycloak and others

- Turn on MFA for the users or the application in your provider. Cloudraw applies whatever your provider requires at sign-in.

Send codes from your own domain

Optional. Your people then receive sign-in codes, invitations and alerts from an address on your company's domain, which they already trust and which spam filters know.

1 Open the setting

In the Cloudraw admin console open **Settings** → **E-mail sender**. You need the *Owner* or *Security admin* role.

2 Enter the address

From name (optional, for example *Acme IT*) and **From address** (for example `it@acme.com`). The address must be on your company's own domain, not Gmail, Outlook or similar. Click **Save and show DNS records**. It can take 10 to 20 seconds.

3 Add the DNS records

Cloudraw shows a table with each record's type, host and value. Copy them into your DNS provider exactly:

- **Ownership** (TXT): proves you own the domain.
- **SPF** (TXT): allows Cloudraw to send for your domain. A domain can have only *one* SPF record. If you already have one, Cloudraw shows the merged record to *replace* it with. Do not add a second one.
- **DKIM**: signs the messages.
- **Return path** (CNAME): handles bounces.
- **DMARC** (TXT): recommended, not required.

4 Verify

Click **Verify now**, or just wait. Cloudraw checks by itself every 10 minutes for 3 days, so you can add the records and come back later. Each record gets a status and, if something is wrong, a hint.

Status	Meaning
Waiting for DNS	Not all required records are found yet. DNS changes can take from minutes to a few hours to appear.
DNS verified, activating	Your records are correct. Cloudraw is finishing the setup on its mail service.
Active	Mail now goes out from your address.
DNS broken	A record that used to be correct is missing or changed. Mail goes out from the Cloudraw sender until you fix it.

To go back to the Cloudraw sender, remove your own sender on the same page.

Troubleshooting: "I didn't get the code"

1 Check spam, junk and quarantine

Look in the junk folder first. In Microsoft 365 also check the *Quarantine* in the Defender portal. In Google Workspace check the *Email log search* in the Admin console.

2 Allow the sender

Add `noreply@cloudraw.com`, or your own sender address, to your mail filter's allow list.

3 Check the address

Is the person's e-mail address correct? For Active Directory users the code goes to the AD `mail` attribute, or the attribute you configured. An empty or old address is the most common cause.

4 Check your own sender

If you set up your own sender, look at **Settings** → **E-mail sender**. If the status is *DNS broken*, codes come from `noreply@cloudraw.com` instead, so check for that address too. Fix the records the table marks as missing or wrong.

5 Make sure the code is fresh

A code works once and expires after a few minutes. Start the sign-in again to get a new one, and use the newest e-mail.

6 Still nothing?

E-mail support@cloudraw.com (<mailto:support@cloudraw.com>) with the person's address, your workspace name and the approximate time. We can see whether the message was sent and what the receiving server answered.

IMPORTANT

Never ask people to forward their codes to IT or to anyone else. Cloudraw support will never ask for a sign-in code.

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