Team management and SSO

Admins, developers, seats, invites, enterprise SSO.

Overview

Team management & SSO

Roles

- **Admins** use the Admin Console: policy, inventory, activity, billing.
- **Developers** use the Sentilai Endpoint on their machines; they don't need console access.

Both take a **seat**. Your plan's seat limit and current usage are on the Billing page.

Invites & passkeys

Invite by email: the invitee gets a **passkey setup link** — they register a passkey and are in. No passwords anywhere in Sentilai. A backup passkey can be added from Account settings; admins can issue a new setup link if a device is lost.

Enterprise SSO

Connect your identity provider (Okta, Entra ID, Google Workspace, or any OIDC/SAML IdP) with the guided **SSO wizard**: pick the provider, follow the tailored steps, validate the connection with a live test login, and switch enrollment to SSO. New team members then sign in with your IdP — accounts are provisioned on first login (JIT).

Session security

Sign-ins use phishing-resistant credentials (passkeys or your IdP's own MFA). Device credentials are separate, rotated, and revocable per device from the console.

Invite an admin

Admins manage the organization: policy, providers, people, billing. They do **not** need the Endpoint Suite — that's for developers.

How

1. Go to **Users & Teams ? Admins**.
2. Click **Invite Admin**, enter their name and work email.
3. They receive an email with a **passkey setup link**.

The invite appears under **Pending & past invites** with status `pending`. Once they complete setup it flips to `accepted` and they appear in the admin table above.

What the new admin does

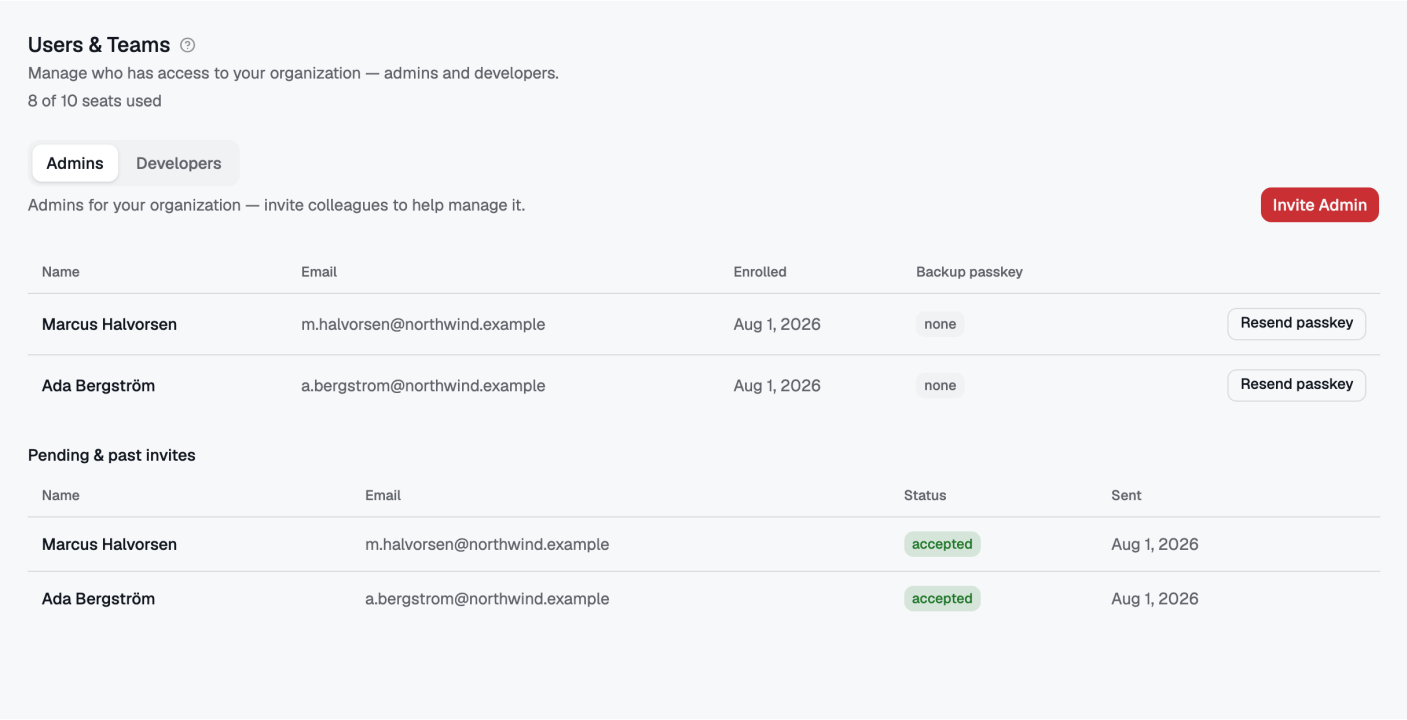
The link opens a short setup page, then asks them to create a passkey (Touch ID, Windows Hello, or a security key). There is no password to choose — Sentilai is passkey-only, so there is no password to phish, reuse or leak.

Seats

Admins and developers share your plan's seat count. **Users & Teams** shows `X of Y seats used` under the page title. If you're at the cap the invite is refused with a "seat cap reached" message — remove someone who has left, or contact us about a larger band.

If an invite goes wrong

- **Sent to the wrong address** — click **Revoke** on the pending invite. The link stops working immediately.
- **Link expired or lost** — click **Resend**. This issues a fresh link; the old one stops working.
- **They lost their device** — see Resend a passkey link.



Users & Teams — the admin roster, seat usage, and pending invites.

Invite a developer

Developers are the people whose AI tools you're governing. A developer invite grants **no console access** — it exists so their machine can enrol and their name can appear against their AI activity.

How

1. Go to **Users & Teams ? Developers**.
2. Click **Invite Developer**, enter their name and work email.
3. They receive a passkey setup link, exactly like an admin.
4. They install the **Sentilai Endpoint** app and sign in with that passkey.

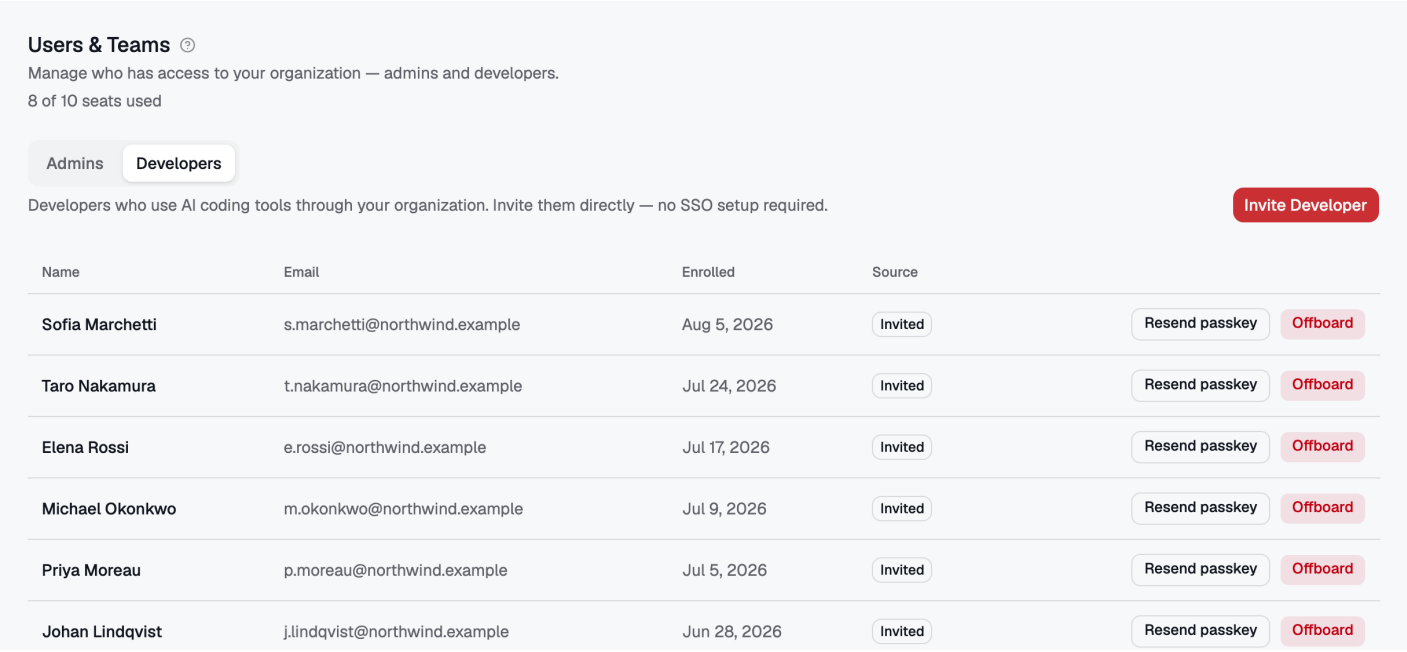
From then on, every AI request from their machine carries their identity — which is what makes the Developer column on **Activity** meaningful.

Do I have to invite everyone?

Only if you invite people one by one. If you configure **Organization SSO**, developers sign in with your existing identity provider and are provisioned automatically the first time they use the Endpoint Suite. For a team above ~10 people that is the easier path.

Removing a developer

Use **Offboard**, not delete — see Offboard a developer. It revokes their devices and passkeys in one action and leaves a record of what was revoked.



The Developers tab on Users & Teams — invite developers directly, no SSO setup required.

Resend a passkey link

Use this when someone can't sign in because their passkey is gone — a lost or wiped laptop, a replaced phone, or a passkey that was never finished.

How

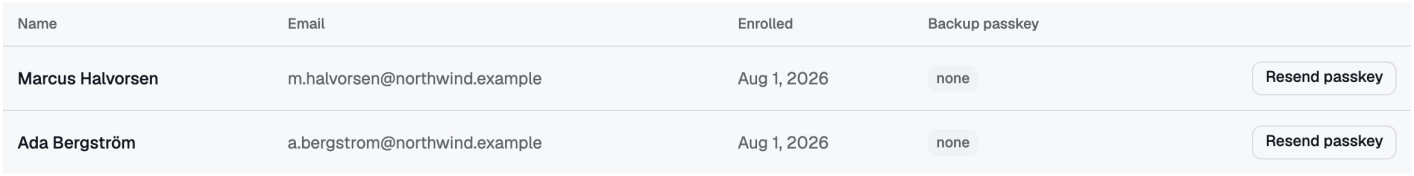
Users & Teams ? find the person in the Admins or Developers table ? **Resend passkey**.

They get a fresh setup link and can register a passkey on their new device. Their old passkey is not automatically removed; if the old device is compromised rather than merely gone, offboard them instead and re-invite.

Backup passkeys

The **Backup passkey** column shows whether that person has more than one passkey registered. `none` is not an error — it's a note that a single lost device will lock them out and need an admin to intervene.

Encourage a second passkey (a phone, or a hardware key kept in a drawer) for anyone whose lockout would be disruptive — especially your own account. You can add yours under **Account & Profile**.



Resend passkey sits on each roster row — for the colleague whose enrollment link expired or never arrived.

Offboard a developer

One action for "this person has left". Classic offboarding checklists cover email and VPN but never reach AI tooling — API keys sitting in tool configs, live logged-in assistants, MCP credentials, gateway tokens.

How

Users & Teams ? Developers ? **Offboard** on their row ? confirm.

What happens, immediately

- **Every device they registered is revoked.** Their gateway tokens stop working, so their AI tools lose access at the Gateway — even if their laptop is offline, off, or never comes back.
- **Every passkey is removed**, so they cannot sign in to enrol a new device.
- A **receipt** is recorded — how many devices and passkeys were revoked, by whom, and when — and the person shows as `Offboarded` in the table.

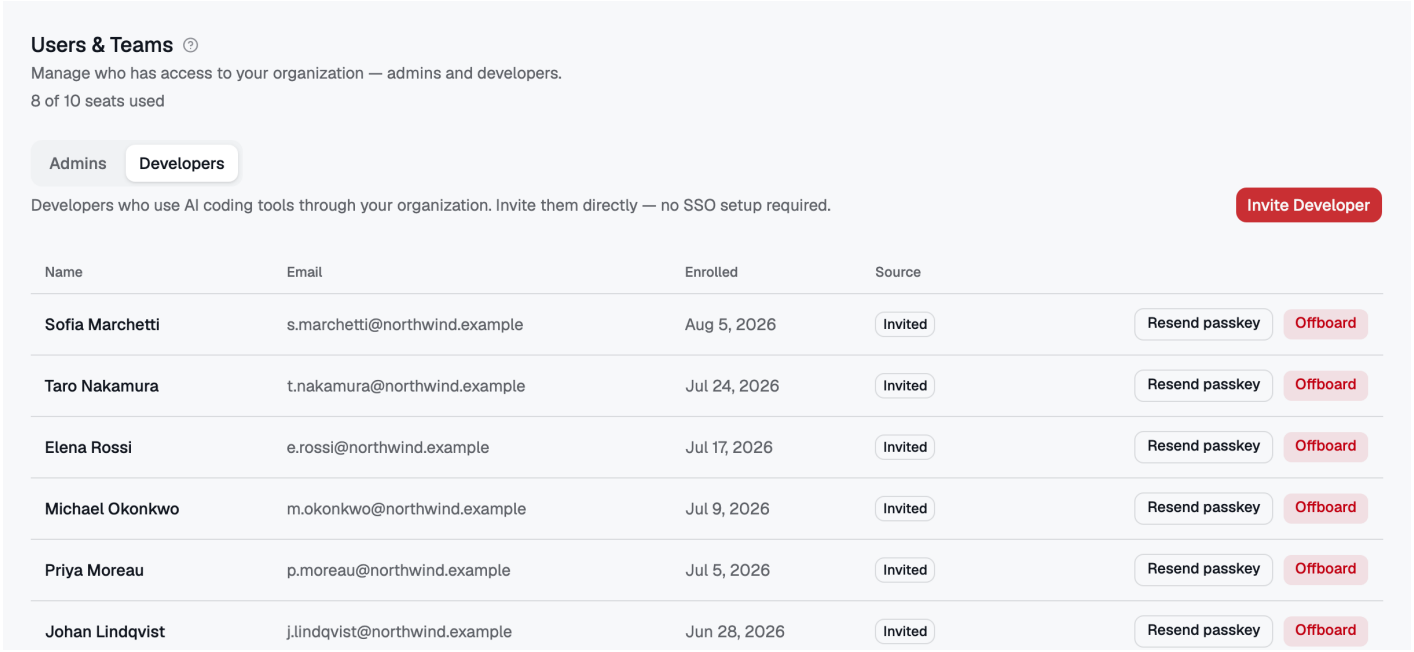
Their seat is freed for someone else.

What it does not do

It does not reach into the laptop and delete files. If the machine is still under your control and online, the Endpoint Suite also removes the Sentilai routing from the tool configs; if it isn't, access is dead at the Gateway regardless, which is the part that matters.

Offboarding an admin

Not a one-click action yet. Revoke their pending invites and remove their passkeys from **Users & Teams**; a dedicated admin offboarding flow is on the roadmap.



Every developer row carries Offboard — one click revokes their AI access and frees the seat.

Set up single sign-on

SSO lets your wider developer team sign in with the identity provider you already run — Google Workspace, Microsoft Entra, or any generic OIDC or SAML provider. Your own admin login is unaffected: admins keep signing in with passkeys.

The wizard

Organization SSO walks through eight steps: **Provider ? Overview ? Configure ? Validate ? Test login ? Provisioning ? Review ? Activate**. You can leave and come back; progress is saved as a draft.

The steps that need attention:

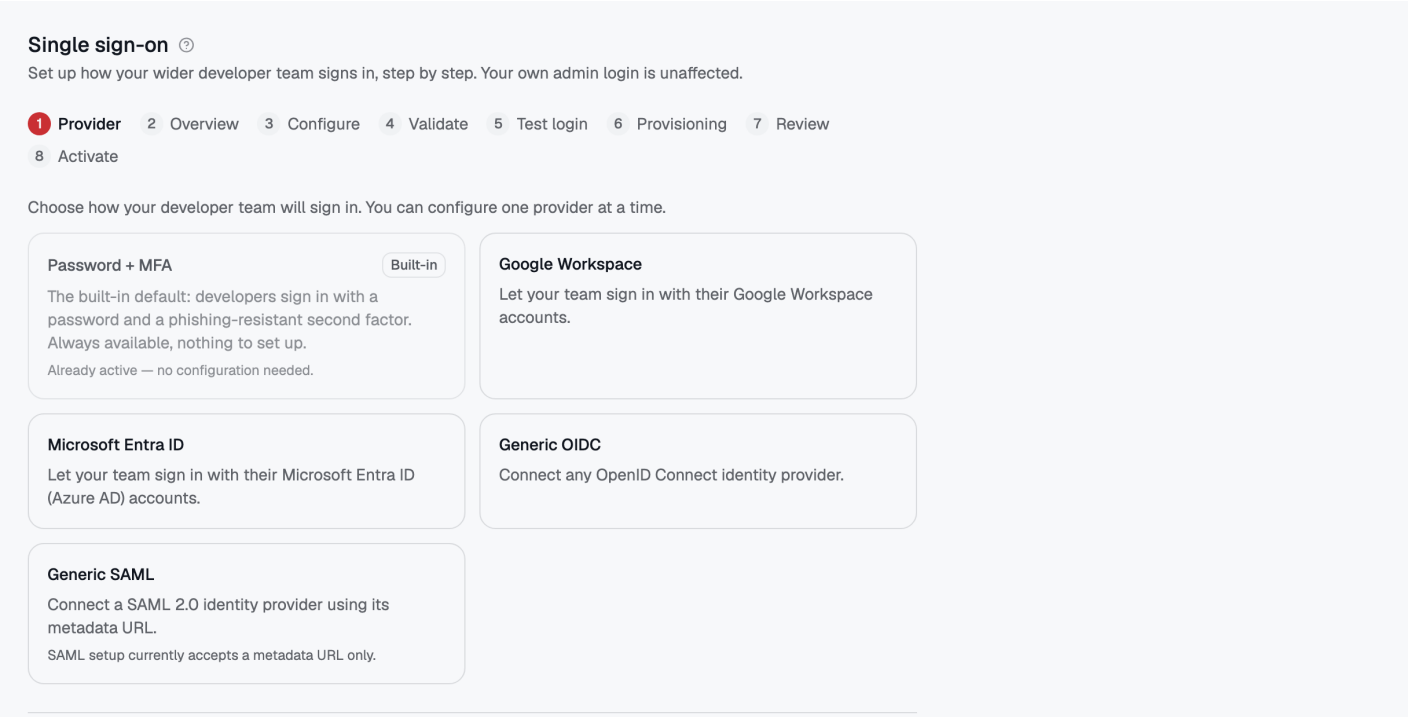
- **Configure** — the values from your IdP (issuer URL, client id and secret, or the SAML metadata). The wizard shows the redirect URL to paste into your IdP.
- **Validate** — a reachability check against the issuer before anything is saved. This catches the common typo class (wrong tenant id, a URL that only resolves inside your network) early rather than at first login.
- **Test login** — you sign in through the provider for real, in a separate window. The wizard refuses to activate until this passes.
- **Provisioning** — decide whether a developer who authenticates successfully is admitted automatically, or waits for an admin to approve them (**Users & Teams ? Developers** shows them as `pending`).

One provider at a time

Configuring a new provider replaces the existing one. The old configuration is removed when the new one activates.

If sign-in starts failing later

The SSO page shows the configuration status (`active`, `testing`, `failing`). A `failing` state usually means a rotated client secret or an expired SAML certificate — re-run **Test login** to see the provider's own error.



Organization SSO — Google, Microsoft, generic OIDC or SAML, one provider at a time.

The SSO enrollment wizard

Connecting your identity provider is eight steps, and the wizard will not let you activate something that has not been proven to work.

The steps

1. **Provider** — Google Workspace, Microsoft Entra ID, generic OIDC, or generic SAML. (Password + MFA is shown for reference; Sentilai itself is passkey-only.)
2. **Overview** — what this provider needs, which permissions you need in it, and a realistic time estimate: 10 minutes for Google, 15 for Entra and generic OIDC, 20 for SAML.
3. **Configure** — the credentials. See Configure your identity provider.
4. **Validate** — Sentilai fetches your provider's discovery document or metadata and runs a checklist. **You cannot continue until it passes**, because every failure here would otherwise become a mysterious login error later.
5. **Test login** — a real login, in a popup, against your real provider. It reports the email it got back, or the error.
6. **Provisioning** — what happens to people who sign in. See Provisioning and approval.
7. **Review** — a read-back of everything, including whether a secret is stored.
8. **Activate** — switch it on.

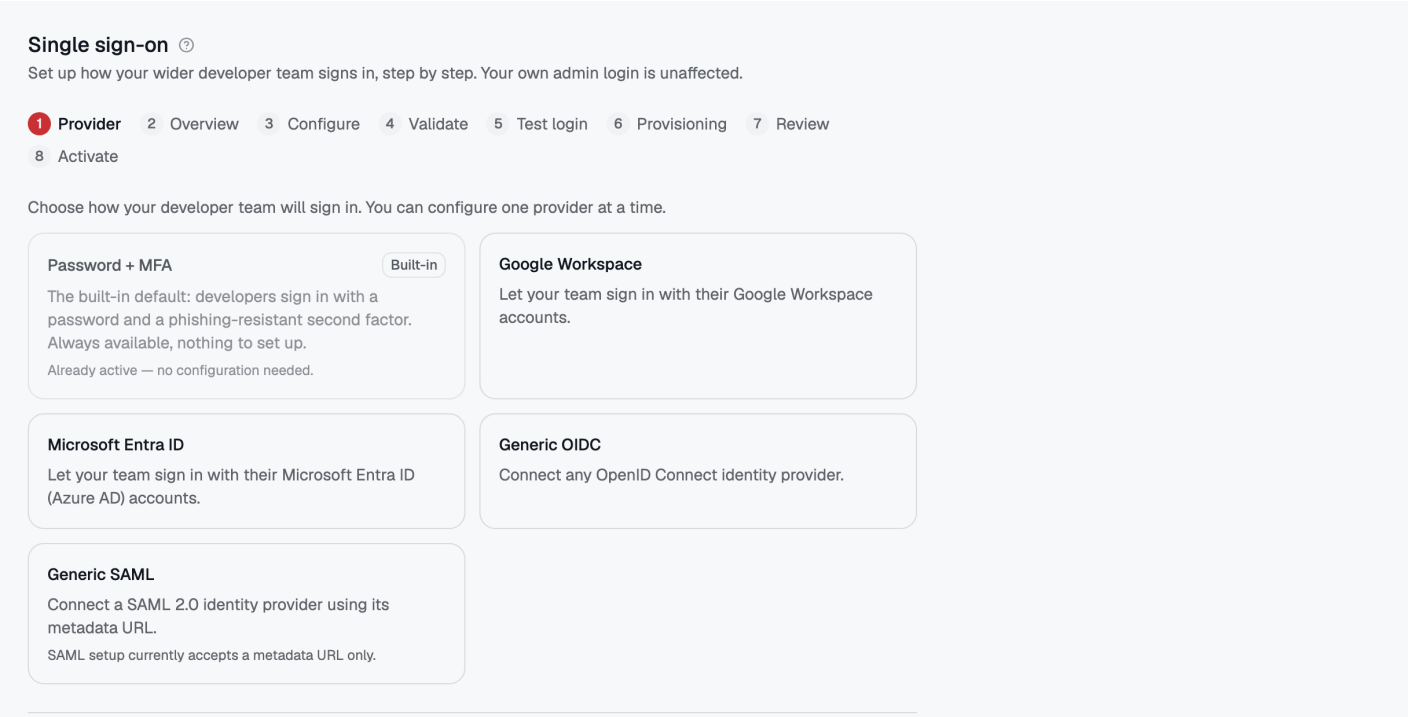
You must test before you activate

Activating without a successful test login is refused, with a message telling you to run the test first. This is not bureaucracy: an SSO configuration that looks right and does not work locks out everyone who depends on it, and the person best placed to notice is you, one minute earlier.

Afterwards

The landing view shows the provider, its status — Draft, Testing, Active or Failing — and a **configuration quality score** out of five with specific recommendations. It is worth reading once; it tends to catch the things that work today and cause trouble later.

You can **Edit configuration**, **Deactivate**, or **Remove**. Removing it means anyone who signs in this way can no longer do so, and the confirmation says exactly that.



The eight steps, always visible — the wizard saves progress, so Configure can wait for your IdP admin.

Configure your identity provider

What step 3 of the wizard needs, by provider.

Google Workspace

Client ID and client secret from a Google Cloud OAuth client. Roughly ten minutes if you already have a project.

Microsoft Entra ID

Client ID and client secret, plus two decisions:

- **Account types** — organizations only, or also personal Microsoft accounts. Almost everyone wants organizations only.
- **Treat emails from Microsoft as verified** — whether to trust the email claim Entra returns without further checking. Correct for a tenant you control; think twice if you have allowed personal accounts.

Generic OIDC

Issuer URL, client ID, client secret, and the scopes to request. The issuer must serve a standard discovery document — the validate step fetches it and tells you precisely what is missing.

Generic SAML

Metadata URL only. Sentilai does not accept a pasted certificate or hand-entered endpoints; if your provider cannot publish metadata at a URL, SAML will not work here today.

Editing later

Leaving the client secret **blank** when editing keeps the stored one. You never have to find the original secret again just to change an unrelated field.

A display name

Whatever you put here is what your developers see on the sign-in screen. "Acme SSO" is kinder than "oidc-prod-2".

Provisioning and approval

Step 6 of the wizard, and the decision that determines who can walk in.

Default role for new sign-ins

- **Developer** — the person is immediately a developer and can use the Endpoint Suite.
- **Pending approval** — they exist but can do nothing until an admin approves them.

Require admin approval for every new user

Same effect, stated as a switch. With it on, every first-time sign-in waits for a human.

Allowed email domains

A list. Only people whose email is in one of these domains can provision an account at all.

Set this. Without it, the gate is only whatever your identity provider allows, and identity providers are frequently configured to allow more than you think — guest accounts, contractors, personal accounts if you enabled them in Entra.

Approving people

Pending users appear on **Users & Teams ? Developers** with a **Pending** badge and an **Approve** button. Nothing else about them changes on approval; they simply become able to work.

Seats

An SSO-provisioned developer consumes a seat exactly like an invited one. If your identity provider hands you a hundred people on day one, they will consume a hundred seats — which is another reason to start with pending

approval rather than automatic developer.

SSO people and passkeys

Developers who arrive through SSO show "Signs in via SSO" instead of a resend-passkey action. Their credentials live in your identity provider; Sentilai does not manage them.

Passkeys explained

Sentilai has no passwords. Not "passwords plus MFA" — no password field exists anywhere. This surprises people, so here is the reasoning and the practical consequence.

Why

A password can be phished, reused, guessed or leaked from somewhere else. A passkey is a key pair: the private half stays in your device's secure hardware and never travels, and the authentication is bound to the site it was created for. A convincing fake login page gets nothing, because there is nothing to type.

For a product whose whole purpose is controlling access to your organization's AI traffic, anything weaker would be inconsistent.

What it looks like

Touch ID, Windows Hello, a hardware security key, or your phone. Whatever your device offers.

The one real risk: losing your only device

There is no password to fall back on. If your only passkey lives on a laptop and the laptop is gone, an admin must send you a new setup link — and if *you* are the only admin, that becomes a support ticket.

So register a second passkey, on a different device, from **Account & Profile**. The console nags you about this on the Overview screen until you do, which is deliberate.

Removing passkeys

You can remove any passkey except your last one — that request is refused. Removing the last one would lock you out permanently, and no amount of confirmation dialog makes that a good outcome.

For developers

Same thing, from the Endpoint Suite's browser sign-in. Their passkey is what ties a device to a person, which is what makes the Activity feed's Developer column meaningful.

When someone cannot sign in

The common cases, in the order they actually occur.

"This account can't open the admin console"

The identity is valid but has no admin record. Nearly always **passkey autofill picked the wrong saved account** — someone with both a personal and a work identity on the same machine. Sign out, sign in again, and choose deliberately.

The other possibility is that they are a developer, not an admin. Developers do not use the console.

The invite link does not work

Invites are single-use and they expire. **Users & Teams ? Pending & past invites** shows the status: `pending`, `accepted`, `expired` or `revoked`. **Resend** issues a fresh link and invalidates the old one.

They lost the device with their passkey

Resend passkey on their row in the admin table. They get a new setup link and can register a passkey on a new device. Their old passkey stays registered until they remove it — worth cleaning up if the device is genuinely gone rather than merely replaced.

SSO worked yesterday and does not today

Check **Organization SSO**: the status badge shows **Failing** when validation against your provider stops succeeding. The usual cause is an expired client secret. Edit the configuration, put in the new secret, re-run the

test login.

Nobody can get in at all

If every admin has lost access, open a ticket from any other channel you have with us. This is exactly why the console asks you to have a second admin and a second passkey — please do both before you need them.