Account and security

Your own passkeys, sign-in and console preferences.

- Manage your passkeys
- Console preferences
- How Sentilai protects your data

Manage your passkeys

Account & Profile is where your own credentials live.

Your profile

Name and email, read-only. They come from the identity that signed you in, so they are changed where that identity lives rather than here.

Add a second passkey

The single most important thing on this page.

Add a passkey registers another one — a different laptop, a phone, a hardware key. **Set up for new sign-in** registers one directly in the page for the on-host sign-in flow, without leaving the console.

Until you have two, the console warns you on Overview. With one passkey and one lost device, there is no password to fall back on: another admin has to send you a new setup link, and if you are the only admin, that becomes a support ticket.

The passkey list

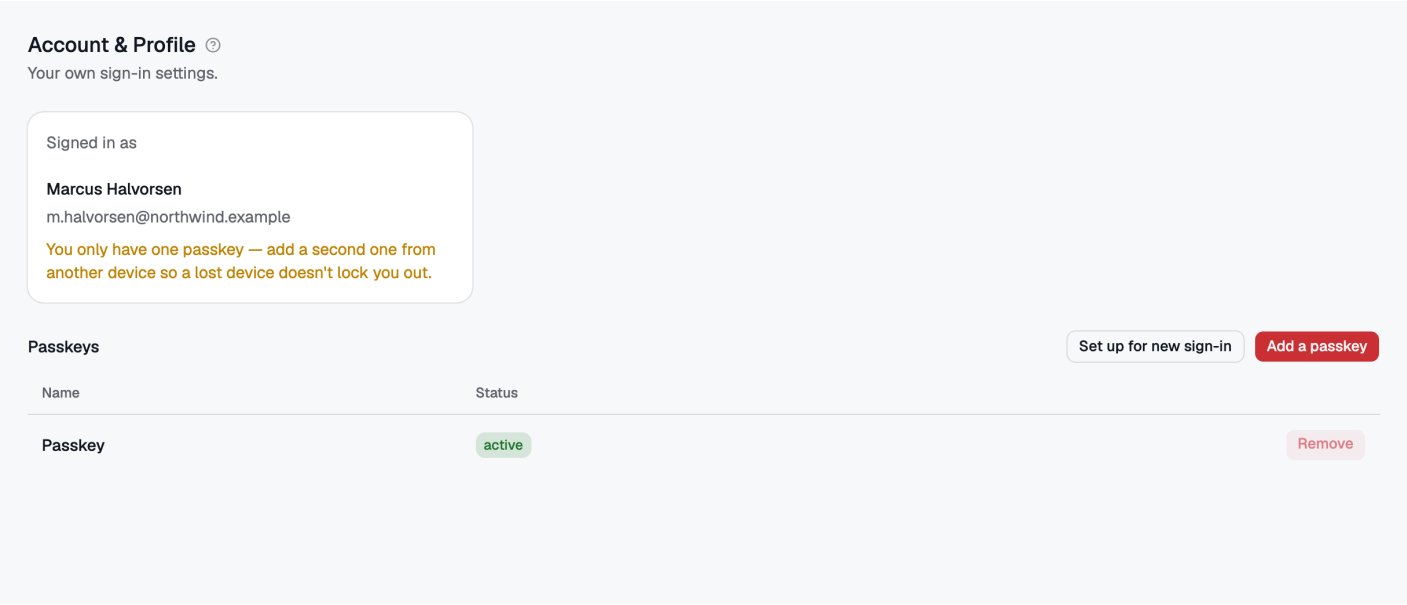
Each with a name — or "Unnamed passkey", which is what you get when the browser did not supply one — and a status of active or pending.

Remove deletes one, after a confirmation. **You cannot remove your last passkey**; that request is refused with an explicit message rather than a generic error.

Remove the passkeys of devices you no longer have. A passkey on a laptop you returned to a previous employer is still a working credential.

What "pending" means

A passkey that was created but whose registration has not completed. If one sits pending, remove it and register again.



Account & Profile — your own passkeys. The last one cannot be removed, which is what stops a self-lockout.

Console preferences

Small things, in the sidebar.

Language

The console is available in five languages, switched from the sidebar. The choice applies to your current session and is not stored on the server — switching machines starts from your browser's preference again.

Only the tenant admin console and the Endpoint Suite are translated. The documentation and Sentilai's support correspondence are in English.

Theme

Light, dark, or follow the operating system. It applies immediately and is remembered in that browser.

The "?" buttons

Small question marks sit beside settings whose consequences are not obvious. Each gives a sentence in place and a link to the article that explains it properly. They are buttons rather than hover tooltips deliberately: hover does not exist on a touch screen and cannot be reached from a keyboard.

Signing out

At the bottom of the sidebar. It ends your console session only — it does not affect any developer's governed tools, and it does not affect your own machine if you also have the Endpoint Suite installed.

How Sentilai protects your data

The honest version, for the security review that will ask.

Tenant isolation

Every query is scoped to your organization in the application layer, and that is the control the isolation rests on today.

We are additionally rolling out **database row-level security** as a second line of defence, so that a bug in application code would not by itself be enough to cross organizations. At the time of writing it covers the policy-rule tables rather than the whole schema. We would rather tell you the current state than describe the finished one — ask us for the up-to-date coverage if this matters to your review.

Credentials at rest

Provider API keys are encrypted and never shown again after saving — only the last four characters. Webhook URLs are write-only for the same reason. API credential secrets are displayed exactly once, at creation.

Findings never contain the finding

A risk finding records the **kind and the count**, never the matched value, its offset, or a preview. A product that detects secrets and then stores them would be a more attractive target than the systems it protects.

Prompt content

Not stored unless you turn on **prompt capture**. When it is on, secrets are redacted before storage, the content follows your retention setting, and **Sentilai support cannot read it**.

Authentication

Passkeys only. No passwords exist to be phished, reused or leaked. Device identity is an ECDSA P-256 key pair in the machine's secure hardware storage — Keychain or Credential Manager — that cannot be exported.

Transport and region

TLS everywhere. Your organization has a region — EU or US — which determines which Gateway your developers reach and where your data lives. If you configure an Azure OpenAI key in a different region, the console flags it, because that would send your traffic outside the region you chose.

What we have not claimed

We do not currently hold SOC 2 or ISO 27001. When we do, it will be stated here with the report available — not before. Ask us for the current status and we will tell you plainly.