

Admins, developers and seats

Sentilai has two kinds of people, and they use the product completely differently.

Admins

Admins use the console: policy, providers, people, activity, billing. An admin does **not** need the Endpoint Suite and does not need to be a developer.

Developers

Developers are the people whose AI tools you govern. They never open the admin console — if they try, they get a polite "this account can't open the admin console". What they use is the Endpoint Suite on their machine.

A developer can arrive two ways: invited by an admin, or created automatically the first time they sign in through your identity provider (see [Set up single sign-on](#)).

Seats

Both kinds consume a seat, and they share one pool. The count is on Users & Teams as `X of Y seats used`.

If you hit the cap, invitations are refused with a message naming your limit. Two ways out: offboard people who have left — which frees their seat immediately — or move to a larger plan on **Billing & Plan**.

A common surprise: developers who left the company keep holding seats until somebody offboards them. Offboarding is one click and it also revokes their devices and removes their passkeys, so it is worth doing promptly rather than at renewal time.

What neither role can do

Nobody in your organization can read another organization's data, and Sentilai support cannot read your prompt content. Support can see that a request happened and what the policy decided; the content, when captured at all, is yours.