

Devices and revoking access

Diagnostics lists every machine enrolled in your organization: who it belongs to, when it registered, and when the Gateway last saw it.

Revoking a device

Revoke access on a row kills that machine's gateway tokens. The AI tools on it lose access within seconds — no need to reach the laptop, and it works whether or not the machine is online.

Use it for a lost or stolen laptop, or a machine that shouldn't have been enrolled. For a person who has left, use **Offboard** on Users & Teams instead — it covers every device plus their passkeys in one action.

Revoking is reversible: the same row offers **Restore access** afterwards.

Device identity

Each machine holds a hardware-backed key in the OS keychain (Keychain on macOS, Credential Manager on Windows). The private key never leaves the device, and it is what ties a request in **Activity** to a person and a machine rather than to a shared token.

Diagnostics ⓘ

Request event logs from a device to troubleshoot. Event logs only — never prompt content — and kept 14 days.

Ungoverned AI agents ⓘ

Autonomous AI agents found on your devices that Sentilai can see but does not route or enforce.

Detection only — these devices keep working and stay compliant. Choose what happens on the Policy screen.

User	Device	Agent	Findings	First detected
t.nakamura@northwind.example	nakamura-mbp16	OpenClaw	10 findings	Jul 29, 2026

Recently removed

OpenClaw was removed from okonkwo-xps15 — detected Jul 11, gone Jul 26.

Devices

User	Device	Registered	Last seen		
j.lindqvist@northwind.example	johan-mbp16	Jun 27, 2026	Aug 4, 2026, 11:25 AM	Request logs	Revoke access
p.moreau@northwind.example	priya-mbp14	Jul 4, 2026	Aug 4, 2026, 11:18 AM	Request logs	Revoke access

Diagnostics — enrolled machines, when each was last seen, and per-device revocation.