Network and deployment

Hostnames, firewalls, regions and rolling the Endpoint Suite out at scale.

Hostnames and firewall rules

What your network needs to allow for Sentilai to work.

What the Endpoint Suite reaches

- **Your regional Gateway** — where all governed AI traffic goes. The exact hostname depends on your region and is resolved when the device registers, so you do not have to configure it by hand.
- **The platform API** — sign-in, device registration, policy, log upload.
- **The download host** — update checks.

The app tells you when something is unreachable: the tray icon gains an amber badge and a banner names the host it cannot reach. That banner is the fastest way to give your network team a precise answer.

Everything is TLS

There is no plaintext path. If your network does TLS inspection with an internal certificate authority, the machines need to trust that CA the same way they do for any other service.

Egress from the Gateway

The Gateway itself reaches the AI providers you have configured — Anthropic, OpenAI, Azure OpenAI, Gemini — and any **routed remote MCP endpoints** you have registered. That traffic leaves Sentilai's infrastructure, not your network.

The blocklist you can hand over

Policy ? Egress blocklist generates a list derived from your configured providers and registered MCP endpoints, with **Download** and **Copy** buttons. See *Use the egress blocklist*.

Use the egress blocklist

Governance at the Gateway only helps for traffic that reaches the Gateway. A developer can always point a tool straight at `api.openai.com`. Your network is where you close that door.

What Sentilai gives you

Policy ? Egress blocklist produces a list built from what you have actually configured: your provider endpoints, and the MCP endpoints you have registered. Download it as a text file or copy it.

Because it is generated, it stays in step with your configuration — add a provider and the list changes.

What to do with it

Hand it to whoever runs your egress filtering. The rule you want is roughly:

- **Block** direct access from developer machines to the AI provider APIs.
- **Allow** the Sentilai Gateway.

The effect is that the governed path is the only path. A tool that has drifted out of governance stops working visibly, rather than working invisibly ungoverned — which is by far the better failure.

Do it in stages

Blocking provider APIs organization-wide on a Monday morning will break something you did not know existed — a CI job, a data pipeline, someone's script.

Run it in monitor mode first, see what talks directly, decide case by case, then enforce.

The limit

This covers machines on your network. A laptop on a home connection or a phone tether is outside it. Combine egress control with the **Non-compliant** flag in Diagnostics, which catches drift wherever the machine happens to be.

Egress blocklist

Give this generated list to your network team: block the direct provider hosts and allow only the Sentilai Gateway, so AI traffic can't bypass governance at the network layer. It is derived from your configured providers and registered MCP endpoints.

Allow	gateway-dev.sentilai.com	Sentilai Gateway (eu region) — all AI traffic ro…
Block	api.anthropic.com	Anthropic API (governed via the Gateway's /v1/mes…
Block	api.openai.com	OpenAI API (governed via the Gateway's /v1/chat/compl…
Block	generativelanguage.googleapis.com	Google Gemini API (govern…

Download blocklist Copy

The egress blocklist, generated from your own providers and routed endpoints — hand it to your network team.

Rolling out to the team

A sequence that has fewer surprises than doing it all at once.

1. One machine, yours

Install, sign in, govern one tool, watch the request appear in Activity. Everything else depends on this working, so prove it once, slowly.

2. A friendly pilot, three to five people

Pick developers who will tell you when something is odd. Nothing pinned, no restrictions — they should be able to disconnect a tool and tell you why they had to.

Watch for a week. What you are looking for: tools that will not stay governed, MCP servers you did not expect, and requests failing for reasons that turn out to be a missing provider key.

3. Set policy before you widen

Use what the pilot showed you. Approve the MCP servers that turned out to be legitimate. Decide about prompt capture and **tell people the answer**.

4. Roll out

Send the installer, or push it through your MDM. If you are using managed configuration, start with **start at login** and **automatic governing** pinned, and leave the restrictions off until your policy has stopped changing.

5. Close the direct path

Once most machines are governed, apply the egress blocklist. Do this last: applying it first means the tools break before the alternative exists.

Two things to say out loud

Subscription mode does not change who pays — developers keep their own plans. And **say whether prompt capture is on**. Both rumours spread quickly and both are corrosive if they are wrong.

Regions

Your organization belongs to a region — **EU** or **US** — shown in the header on the Overview screen.

What it determines

Which Gateway your developers' tools talk to, and where your audit data, findings and any captured prompt content are stored.

The Endpoint Suite resolves the right Gateway automatically when a device registers. There is a compiled-in fallback, but it is only used if the backend did not supply one — you do not need to configure regional hostnames per machine.

Where the boundary is not

Two honest caveats.

AI providers are outside it. When a request leaves the Gateway for Anthropic or OpenAI, it goes wherever that provider processes it. Sentilai governs and records the request in your region; it cannot make a US provider process data in the EU.

Azure OpenAI keys carry their own region, which you set yourself. If it does not match your organization's region, the console shows a warning badge on the key — it warns rather than blocks, because it is sometimes deliberate, but it should never be accidental.

Choosing

Regions are set when your organization is created. Moving between them is not self-service — open a ticket and we will talk through what is involved.