

Egress blocklist

Policy ? Egress blocklist controls which network destinations the Endpoint Suite allows AI tools to reach directly, outside the Gateway.

Use **Download blocklist** to get the current list, and **Copy** to take it into your own tooling. **Send test** verifies the alerting path end to end.

This is a containment control, not a firewall: it constrains the tools Sentilai manages on machines running the Endpoint Suite. It is not a substitute for network egress controls at your perimeter.

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 section on Policy — generated from your providers and routed endpoints, with Download and Copy for your network team.