Scopes and least privilege

Seven scopes, granted per credential.

Scope	What it allows
`audit:read`	Read audit events — the SIEM pull endpoint
`risk:read`	Read risk findings
`policy:read`	Read your policy configuration
`policy:write`	Change your policy configuration
`users:read`	Read admins and developers
`users:write`	Invite, approve and offboard people
`gateway:invoke`	Send AI requests through the Gateway

Choosing

Grant the minimum. Three patterns cover almost everything:

- **A SIEM integration** — `audit:read` only.
- **A compliance or reporting script** — `audit:read`, `risk:read`, `policy:read`.
- **Provisioning automation** — `users:read`, `users:write`.

`policy:write` deserves particular care: a credential holding it can turn your enforcement off. If something needs it, restrict that credential by IP as well.

IP restrictions

The allowlist and denylist are cheap and effective. A credential that only ever calls from your SIEM's egress address should say so — a leaked credential is then also useless.

`gateway:invoke`

This is what a tool needs to send AI requests through the Gateway. The Endpoint Suite manages this for developers automatically; you only need it explicitly for something you are building yourself.

Create a credential

The secret is shown once, right after creation — it can't be retrieved again.

Name

e.g. CI pipeline

Scopes

- [ ] `audit:read`
- [ ] `risk:read`
- [ ] `policy:read`
- [ ] `policy:write`
- [ ] `users:read`
- [ ] `users:write`
- [ ] `gateway:invoke`

Expires in

90 days

IP allowlist (optional — one per line or comma-separated)

e.g. 203.0.113.0/24

IP denylist (optional)

Cancel Create

The seven scopes, chosen per credential at creation. A SIEM integration needs exactly one: audit:read.

Revision #12
Created 2026-08-02 10:19:30 UTC by Sentilai Docs
Updated 2026-09-29 14:39:11 UTC by Sentilai Docs