CLI commands

security

Security tools (audit + optional fixes).

Related:

- Security guide: Security

Audit

```
openclaw security audit
openclaw security audit --deep
openclaw security audit --fix
openclaw security audit --json
```

The audit warns when multiple DM senders share the main session and recommends **secure DM mode**: `session.dmScope="per-channel-peer"` (or `per-account-channel-peer` for multi-account channels) for shared inboxes. It also warns when small models (`<=300B`) are used without sandboxing and with web/browser tools enabled. For webhook ingress, it warns when `hooks.defaultSessionKey` is unset, when request `sessionKey` overrides are enabled, and when overrides are enabled without `hooks.allowedSessionKeyPrefixes`. It also warns when sandbox Docker settings are configured while sandbox mode is off, when `gateway.nodes.denyCommands` uses ineffective pattern-like/unknown entries, when global `tools.profile="minimal"` is overridden by agent tool

profiles, and when installed extension plugin tools may be reachable under permissive tool policy.

JSON output

Use `--json` for CI/policy checks:

```
openclaw security audit --json | jq '.summary'
openclaw security audit --deep --json | jq '.findings[] | select(.severity=="crit
```

If `--fix` and `--json` are combined, output includes both fix actions and final report:

```
openclaw security audit --fix --json | jq '{fix: .fix.ok, summary: .re
```

What `--fix` changes

`--fix` applies safe, deterministic remediations:

- flips common `groupPolicy="open"` to `groupPolicy="allowlist"` (including account variants in supported channels)
- sets `logging.redactSensitive` from `"off"` to `"tools"`
- tightens permissions for state/config and common sensitive files (`credentials/*.json`, `auth-profiles.json`, `sessions.json`, session `*.jsonl`)

`--fix` does **not**:

- rotate tokens/passwords/API keys
- disable tools (`gateway`, `cron`, `exec`, etc.)
- change gateway bind/auth/network exposure choices

remove or rewrite plugins/skills

‹ Sandbox CLI › sessions ›