

Knowledge Base Index

OClaw Knowledge Base

This book records durable, non-secret knowledge from OpenClaw work. Credentials, API keys, token values, and other sensitive secrets are intentionally excluded.

How this book is maintained

- Add or update pages after meaningful sessions.
- Record decisions, verified procedures, integration status, troubleshooting outcomes, and follow-up actions.
- Keep transient chat noise and secret material out of the knowledge base.
- Prefer one page per system or topic, with this index linking the durable record.

Current integration status

BookStack

- BookStack API access is working.
- Existing books observed before this book was created: **AI** and **OpenClaw**.
- BookStack credentials are configured through protected secret storage.
- The BookStack API token requires **Access System API** permission.

UniFi

- Cloud Site Manager API access through `api.ui.com` was verified read-only.
- Observed environment: one console/site, five networks, eight firewall zones, 145 policies, and zero ACL rules.
- Reverse proxy host: `192.168.1.117`.

- The reverse-proxy port-forward was tightened to expose ports `80` and `443`; port `8080` was removed.
- Port 80 is useful for HTTP-to-HTTPS redirects or certificate validation; 443 is the primary public service port.
- Recommended follow-up: enable logging on the specific WAN-to-reverse-proxy firewall allow rule and keep other administrative ports private.
- A public DNS port-forward and Home-to-Camera/IoT access were flagged for intentionality and least-privilege review.
- No firewall changes were made by the assistant.

Proxmox

- Dedicated page: [Proxmox Read-Only Integration](#).
- Hostname: `pve.stargrid.com.au`, resolving internally to `192.168.1.115`.
- API endpoint: `https://pve.stargrid.com.au:8006/api2/json`.
- API token identity: `oc@pve!oc`; permission: `PVEAuditor` at path `/`.
- Token secret is protected in OpenClaw secret storage as `PROXM0X_API_TOKEN`; no secret is recorded here.
- Direct read-only API validation succeeded and returned node JSON.
- The certificate is issued to the Proxmox hostname by the cluster CA; clients need to trust that CA or explicitly disable TLS verification.
- OpenClaw's protected egress path still returns HTTP 502 for this private-LAN destination; this is separate from Proxmox authentication.

OpenClaw Gateway and secrets

- Gateway was previously inspected as a healthy systemd user service owned by `stark`, listening on localhost port 18789.
- Protected credentials should be stored through OpenClaw secret storage and never pasted into chat.
- Secret allowlists must match the exact destination hostname or IP used by the request.
- Existing troubleshooting lesson: a reachable service with HTTP 401 indicates routing is working and authentication/configuration remains the issue; a 502 may indicate the protected egress path or proxy rather than the target service.

Follow-up queue

1. Enable logging on the UniFi reverse-proxy allow rule.
2. Resolve the OpenClaw protected egress path and retry the read-only Proxmox inventory check.

3. Add focused pages for UniFi firewall review, Proxmox health review, and OpenClaw operations as those topics are revisited.

Last updated: 2026-09-12 UTC.

Revision #3

Created 2026-09-12 16:05:10 UTC by Admin

Updated 2026-09-12 20:03:31 UTC by Admin