

Step-CA (Internal Certificate Authority)

Overview

Step-CA is an internal ACME-compatible certificate authority that issues TLS certificates for all `*.home.local` domains. It allows Traefik to provision and auto-renew trusted certificates for internal services without relying on Let's Encrypt or exposing any ports to the internet.

Clients and browsers on the LAN trust `*.home.local` certificates because the Step-CA root certificate has been manually installed as a trusted CA on each device.

Access

Type	URL / Endpoint	Notes
ACME API	<code>https://ca.home.local:9000/acme/acme/directory</code>	Used by Traefik only
Step-CA UI	N/A	No web UI — CLI managed only

Step-CA does not have a browser-accessible dashboard. Management is via the `step` CLI tool.

Configuration

Image: `smallstep/step-ca:latest` **Compose project:** `traefik` (same project as `traefik` container)

Ports

Port	Protocol	Purpose
<code>9000</code>	TCP	ACME API (host-bound: <code>0.0.0.0:9000</code>)

Port 9000 is bound directly to the host so that Traefik (and any other ACME client on the LAN) can reach it at `ca.home.local:9000`.

CA Configuration — `ca.json`

Location: `/home/jeeves/docker/step-ca/config/config/ca.json`

Key settings (secrets redacted):

```
{
  "root": "/home/step/certs/root_ca.crt",
  "crt": "/home/step/certs/intermediate_ca.crt",
  "key": "/home/step/secrets/intermediate_ca_key",
  "address": "0.0.0.0:9000",
  "dnsNames": ["ca.home.local"],
  "db": {
    "type": "badger",
    "dataSource": "/home/step/db"
  },
  "authority": {
    "provisioners": [
      {
        "type": "ACME",
        "name": "acme"
      }
    ]
  }
}
```

Certificate duration for ACME-issued certs is set to **720 hours (30 days)** in Traefik's `step-ca` resolver config. Traefik renews automatically before expiry.

Volumes / Bind Mounts

Host Path	Container Path	Purpose
<code>/home/jeeves/docker/step-ca/config</code>	<code>/home/step</code>	CA configuration, certificates, database

Directory Layout Inside the Volume

```
/home/jeeves/docker/step-ca/config/
├─ config/
│   ├── ca.json          ← Main CA configuration
│   └─ defaults.json    ← Step CLI defaults
├─ certs/
│   ├── root_ca.crt      ← Root CA certificate (install this on client devices)
│   └─ intermediate_ca.crt
├─ secrets/              ← Private keys – never expose these
│   ├── root_ca_key
│   ├── intermediate_ca_key
│   └─ password          ← Key encryption password (REDACTED)
└─ db/                   ← BadgerDB certificate issuance database
```

Dependencies

- AdGuard Home — `ca.home.local` must resolve on the LAN for Traefik to reach the ACME endpoint
- No other service dependencies

Trusting the Root CA on Client Devices

Every device that accesses `*.home.local` URLs in a browser must trust the Step-CA root certificate. The root cert is at:

```
/home/jeeves/docker/step-ca/config/certs/root_ca.crt
```

Also available at `/home/jeeves/docker/traefik/step-ca-root.crt` (Traefik keeps a copy for its own ACME client trust store).

macOS

```
sudo security add-trusted-cert -d -r trustRoot -k /Library/Keychains/System.keychain  
root_ca.crt
```

Windows

```
Import-Certificate -FilePath root_ca.crt -CertStoreLocation Cert:\LocalMachine\Root
```

Ubuntu / Debian

```
sudo cp root_ca.crt /usr/local/share/ca-certificates/step-ca.crt  
sudo update-ca-certificates
```

Notes / Gotchas

- The Step-CA password file (`/home/step/secrets/password`) is read on startup. If the volume is lost, the CA must be re-initialized and all client devices must re-import the new root certificate.
- Do not delete the `db/` directory — it contains the certificate issuance history. Loss means Step-CA cannot check for revoked certificates.
- Step-CA is in the same Portainer compose project as Traefik. Restarting the Traefik stack will also restart Step-CA briefly. Schedule this during off-hours.
- Traefik caches issued certs in its ACME storage file. If Step-CA is temporarily down, Traefik will continue serving existing certs until they near expiry.

Last Updated: 2026-06-16

Revision #1

Created 2026-06-17 00:24:27 UTC by Admin

Updated 2026-06-17 00:24:58 UTC by Admin