Image not found or type unknown

SSL Manager - Certificate Authorities

PUQcloud Panel

Order Now | Download | FAQ

Overview

Certificate Authorities (CA) are provider profiles the panel uses to issue and renew SSL/TLS certificates via ACME. PUQcloud follows a simple rule: **one module per CA**.
Currently supported modules:

- **Let’s Encrypt** (plus **Let’s Encrypt Staging** for safe testing)
- **ZeroSSL**

Where to find it: Settings → SSL Manager → Certificate Authorities

---

What you can do here

- Create and configure CA profiles (ACME account, technical DNS zone, timeouts).
- Test connectivity to the CA (**Save and Test**) and see the CA directory endpoints.
- Keep multiple profiles (e.g., Production vs Staging) and select them per-certificate.

Create a CA Profile (step-by-step)

1. Go to **Settings → SSL Manager → Certificate Authorities** and click **+ Create**.
2. Enter **Name** and choose **Module = PUQ ACME (active)** → **Save**.

3. Click **Edit** on the new CA profile and fill in the fields (see the Field Reference below).
4. Click **Save and Test**. A modal should show **API is available** plus a dump of **ACME directory endpoints**.
5. Click **Save**.

Field Reference (when & why)

Field	What it is	When / Why
Name	Internal display name	Use meaningful names like `LE PROD`, `LE STAGING`, `ZeroSSL`.
Description	Short profile note	Note target usage: “production issuance”, “sandbox”, or project scope.
Certificate Authority	Selected CA directory	Use **Let’s Encrypt Staging** for tests, **Let’s Encrypt** or **ZeroSSL** for production.
Email address for the ACME account	Email used to register/manage the ACME account	Required. Prefer a shared ops mailbox (e.g., `it@company.tld`) for continuity.
EAB Key ID / EAB HMAC Key	External Account Binding	Needed by some providers/plans (e.g., ZeroSSL). Leave empty if not required.
DNS Zone	**Technical zone** where TXT records are actually created	Example: `acme.puqcloud.com`. The target domain’s `_acme-challenge` will **CNAME** to this zone.
Allow wildcard certificates	Allows `*.domain`	Enable if you plan wildcard issuance (DNS-01 only).
DNS Record TTL (seconds)	TTL for created DNS records	30–60 speeds up DCV; raise slightly if your DNS is slow to propagate.
API Timeout (seconds)	Max wait for ACME API responses	Increase (e.g., 20–30) on flaky networks/CI bursts.
Save and Test (button)	Connectivity check	Opens a modal with **API is available** and the list of ACME endpoints. Investigate if it fails.

Provider specifics

Let’s Encrypt (incl. Staging)

- Uses **DNS-01 via a technical zone**:
  1. On the **target domain** you create a **CNAME** for `_acme-challenge.domain` pointing into your technical zone (e.g., `_acme-challenge.domain CNAME <token>.acme.puqcloud.com`).
  2. Let's Encrypt queries `_acme-challenge` on the target domain, **follows the CNAME** into the tech zone, and reads the TXT value there.
- **Let's Encrypt Staging** is ideal for testing without spending production rate limits.
- Wildcards (`*.domain`) require DNS-01 and the **Allow wildcard** flag.

ZeroSSL

- Supports **account API keys** so that **issued certificates appear in your ZeroSSL account**.
- If you **don't** provide keys, the system will create **temporary keys per certificate** automatically.
- With a paid ZeroSSL plan (~$12/month), generate API keys and add them to PUQcloud so all certs are visible/manageable in your ZeroSSL panel.

Good practices

- Start with **Let's Encrypt Staging** to validate your flow, then enable **Let's Encrypt** (production).
- Keep **DNS TTL** low (30–60s) in the CA profile to speed up challenges.
- For ZeroSSL at scale, use **account keys** for visibility and auditing.

Migration cheat-sheet (e.g., from Let's Encrypt to ZeroSSL)

1. **Create** a new CA profile (add EAB/API keys if required by your ZeroSSL plan).
2. **Save and Test** to confirm directory endpoints.
3. Check/update your **technical DNS zone** if it differs from previous setup.
4. **Issue a test cert** on a non-critical domain to validate DCV.
5. For **new** certs, select the new CA in the creation form. For **existing** certs, you cannot "switch issuer"; **issue a new** certificate under the new CA and deploy it.
6. Verify **Days Remaining / Auto Renew** behavior on new certs (and, with ZeroSSL keys, that issues appear in the ZeroSSL account).

Troubleshooting

- **“Save and Test” doesn’t show “API is available”**
  - Check selected CA, network access, EAB keys (if required), and **API Timeout**.
- **LE DNS validation fails**
  - Confirm the **CNAME** is correct and already resolves to the tech zone; wait for **TTL**.
- **Wildcard fails**
  - Ensure **Allow wildcard** is enabled and you are using **DNS-01**.
- **ZeroSSL certificates don’t show in the ZeroSSL dashboard**
  - Add **account API keys** to the CA profile (temporary per-certificate keys don’t link certs to your account).

Related

- **SSL Certificates** — issuance workflow (Draft → CSR → Pending (CNAME) → Active), auto-renew, metadata.
- **DNS Manager** — managing your technical zone and verifying `_acme-challenge` records.
- **Email & Notifications** — reminders for expiry and operational alerts.

Revision #7
Created 6 November 2025 13:35:56 by Yuliia Noha
Updated 13 November 2025 13:43:49 by Yuliia Noha