SSL Manager - SSL Certificates

PUQcloud Panel

Order Now | Download | FAQ

Overview

The **SSL Certificates** section is your single place to issue, renew, import, and store SSL/TLS certificates.

Each certificate page is split into two columns:

- **Left column** — generated by the panel and **identical for all certificates** (fields, statuses, PEM blocks, metadata).
- **Right column** — **module-specific**, driven by the selected CA module (PUQ ACME). It may show provider-specific hints or controls.

Where to find it: Settings → SSL Manager → SSL Certificates

What you can do

- Create a certificate (set the domain, choose a CA profile, add SANs/aliases).
- Generate a **CSR** and a private key.
- Complete domain control validation (DNS-01 via CNAME → tech zone).
- Enable **Auto-renewal** and track **Days Remaining**.
- View/copy **Certificate / Private Key / CSR (PEM)**.
- Change status (Draft → Active via standard actions).
- Delete certificates.
- (Optionally) Import existing certificates.

> “

> The private key is **encrypted in the database** and **visible only on the certificate’s page**.

Certificates list

The list shows:

- **Domain**, **Certificate Authority (PUQ ACME)**
- **Status** (e.g., **ACTIVE**, **“X DAYS”**, **“AUTO RENEW: 7”**)
- Actions: **Edit / Delete**
- **+ Create** to add a new certificate

Create a certificate (step-by-step)

1. Click **+ Create** in **SSL Certificates**.
2. Fill in:
   - **Domain** — primary domain (CN).
   - **Certificate Authority** — select a CA profile (e.g., Let’s Encrypt / ZeroSSL).
   - **Aliases** — SAN domains, one per line (optional).
3. Click **Save** — this **only saves form data** (no keys or certificate yet).
4. Click **Generate CSR**:
   - The system creates the **CSR** and **Private Key** (they **do not exist** before this step).
   - The private key is encrypted in DB; it is **only** visible on this page.
5. Status switches to **Pending**. The panel shows instructions to create a **CNAME** for `_acme-challenge.<domain>` pointing into your **tech zone** (e.g., `acme.puqcloud.com`).
6. Once the CNAME resolves, issuance **starts automatically**. When finished, the card turns **Active** and shows all metadata/PEMs.

Certificate page — left column fields

Top block (editable in Draft)

- **Certificate Status (Draft toggle)** — draft state.
- **Auto Renew Days** — how many days before expiry to auto-renew (typically `7`).
- **Days Remaining** — remaining days until expiry (LE defaults are ~90 days from issue).
- **Email (ACME account email)** and **Agree to Terms of Service** — required by the CA policy.

Domain & Organization

- **Domain** — CN.
- **Aliases (SANs)** — additional domains/subdomains, one per line.
- **Wildcard** — `*.domain` (works with DNS-01 and “Allow wildcard” enabled in the CA profile).
- **Email (contact)** — certificate contact (may differ from ACME account email, if present).
- **Organization / Organizational Unit / Country / State / Locality** — subject fields (as required by policy).

CA / Crypto / Metadata

- **Certificate Authority** — selected profile (read-only once active).
- **Module = PUQ ACME** — issuance module.
- **Key Size**, **Signature Algorithm** — set/visible after CSR/issuance.
- **Issued At / Expires At / CSR Valid From / Renewed At** — lifecycle timestamps.
- **Issuer** — e.g., Let’s Encrypt / Let’s Encrypt Staging.
- **Serial Number (DEC/HEX)**, **Fingerprints (MD5/SHA1/SHA256)** — identifiers.
- **Certificate PEM / Private Key PEM / CSR PEM** — PEM blocks.

Actions

- **Generate CSR** — create CSR + private key (mandatory before issuance).
- **Change Status** — service actions.
- **Save** — persist form changes (no CA interaction).

> In **Draft**, the upper part of the left column is editable; after issuance, many fields become read-only.

Workflow: statuses & transitions

1. **Draft**
   - Edit primary fields (domain, SANs, email, ToS, auto-renew threshold).
   - **Save** only stores data; no key/CSR is created.
2. **Generate CSR**
   - Creates **CSR** and **Private Key** (encrypted; visible only on this page).
   - Crypto fields/PEM blocks appear.
3. **Pending (CNAME → tech zone)**
   - The panel displays the exact **CNAME** instruction for `_acme-challenge.<domain>` → into your tech zone.
   - As soon as the CNAME resolves, the panel continues issuance (DNS-01).
4. **Active**
   - Certificate is issued; **Certificate PEM** is available; a success panel shows **“Certificate is active!”**.

- **Days Remaining** and **Auto Renew** operate; crypto/metadata are filled.

5. **Expired / Error / Revoked**
   - **Expired** — reissue/renew required.
   - **Error** — check logs/CA setup/DNS path.
   - **Revoked** — revoked per CA policy.

Auto-renewal

- Controlled by **Auto Renew Days** (e.g., `7`).
- The panel tracks **Days Remaining** and triggers renewal ahead of expiry.
- For LE/ZeroSSL via DNS-01, ensure your **CNAME** and tech zone remain intact.

Importing an existing certificate (if used)

1. Open **SSL Certificates → + Import** (or equivalent).
2. Paste **CRT / Private Key / CA Bundle** in PEM.
3. **Save** and verify validity/expiry.
4. Configure **Auto Renew** manually if needed (imports are usually not tied to ACME).

Key security

- The private key is created at **Generate CSR**, **encrypted in the database**, and **never shown outside** this certificate page.
- Visibility follows your role-based access.
- Export a secure copy and store it in your organization’s secret vault.

Troubleshooting

Symptom	Likely cause	Fix
Stuck in **Pending**	CNAME not resolving / wrong target	Verify `_acme-challenge.<domain>` name and target in tech zone; wait for **TTL**.
Issuance doesn’t start	CSR not generated	Click **Generate CSR**, then follow CNAME steps.
No **“Certificate is active!”** after CNAME	DCV incomplete / CA error	Check logs; ensure the tech zone is publicly resolvable.
Auto-renew doesn’t trigger	Bad **Auto Renew Days** or broken CNAME	Use a sensible threshold (e.g., 7) and verify CNAME/tech zone.
PEM mismatch on import	Key/cert pair doesn’t match	Import the correct pair or reissue.

Related

- **Certificate Authorities** — profiles, tech zone, TTL, EAB.
- **DNS Manager** — manage your tech zone and verify `_acme-challenge` resolution.
- **Notifications** — expiry and operational alerts.

Revision #4
Created 7 November 2025 08:12:54 by Yuliia Noha
Updated 13 November 2025 06:43:49 by Yuliia Noha