SSL Automation

PUQ Web Hosting module **WHMCS**

Order now | Download | Community

SSL is hands-off by default: the module issues and renews **Let's Encrypt** certificates automatically, and gets out of the way when a customer brings their own.

Acquisition

For each role that needs a certificate, an auto-SSL worker:

1. **Checks DNS** — confirms the domain (and `mail.` / `webmail.` for mail) resolves to the right server.
2. **Probes TLS** — checks whether a valid cert is already present.
3. **Issues** — runs the Let's Encrypt request only when the checks pass.

Cadence (Settings → SSL)

The check interval adapts to the situation:

- **Fast mode** — a few quick attempts shortly after provisioning (configurable count + interval), so a new site goes green within minutes of DNS pointing.
- **Normal interval** — the steady-state re-check.
- **Active-cert interval** — the slow re-check once a valid cert exists (renewals).

Rate-limit guard

To respect Let's Encrypt limits, a domain that fails repeatedly is **frozen** for a configurable window (freeze after N fails, for M hours) before trying again. All of these knobs live on **Settings → SSL**.

Custom certificates

When a customer uploads a custom certificate (client **SSL** page), auto-SSL is suspended for that role so the upload isn't overwritten, and a daily **custom-cert expiry** cron warns before it lapses.

> The per-service SSL state, plus manual **Issue** / **Renew now** buttons, are on the admin service panel's **SSL** tab and the client **SSL** page.

Revision #8
Created 4 June 2026 15:12:07 by Ruslan
Updated 7 June 2026 20:54:29 by Ruslan