

SSL & HTTPS Troubleshooting Guide

Common checks when a website shows certificate or HTTPS problems.

Certificate Not Issuing

- Confirm the domain points to the server where the certificate is being requested.
- Make sure HTTP validation is not blocked by a firewall, redirect loop or inaccessible document root.
- Check that the domain name is spelled correctly and exists in the Plesk subscription.
- Review the Plesk/Let's Encrypt error message for the exact validation failure.

Certificate Name Mismatch

- Confirm the certificate includes the exact hostname being opened.
- If users visit www, ensure www is covered.
- If using mail.yourdomain.com, that hostname needs a matching certificate.
- Do not assume a certificate for one hostname automatically covers every subdomain.

Mixed Content

- Open browser developer tools and look for HTTP assets loaded from an HTTPS page.
- Update hard-coded image, CSS, JavaScript and API URLs to HTTPS.
- For WordPress, check Site URL, plugins and cached content.
- Clear application/CDN caches after correcting URLs.

Redirect Problems

- Avoid stacking multiple competing HTTP-to-HTTPS redirects.
- Choose one canonical hostname, such as www or non-www.
- Check .htaccess, application rules, CDN settings and Plesk forwarding.
- Test with a clean browser session after making changes.

Final Verification

- Confirm the certificate is valid and not expired.
- Test root domain and important subdomains.
- Verify forms and login pages work over HTTPS.
- Check that HTTP requests redirect once to the intended HTTPS URL.

HTTPS Checklist

- ✓ DNS correct
- ✓ Certificate covers hostname

- | |
|--------------------------|
| ✓ Certificate valid |
| ✓ No mixed content |
| ✓ Redirects clean |
| ✓ www/non-www consistent |
| ✓ Forms tested |