

HTTPS Migration Checklist

A practical, printable checklist for moving a site to HTTPS without breaking it. From sslguides.com — full guides linked below.

Before you start

- ☐ **Confirm the certificate is issued and valid**
Check validity dates and that the SAN list covers every hostname you'll actually serve — including both www and non-www if you use both.
- ☐ **Verify the full chain, not just the leaf certificate**
Missing intermediates are the most common cause of a certificate that works in one browser but fails in another client.
- ☐ **Lower DNS TTL if you'll be changing DNS records**
Gives you a fast rollback path if something goes wrong during the migration window.

Server configuration

- ☐ **Install the certificate and enable HTTPS on port 443**
Confirm the site actually loads over https:// before touching any redirect logic.
- ☐ **Set a modern TLS configuration**
TLS 1.2 and 1.3 only, no legacy cipher suites. Generate one at sslguides.com/tools/tls-config-generator.html.
- ☐ **Enable OCSP stapling**
Lets your server proactively supply its own revocation status, rather than every client checking separately.

Redirects

- ☐ **Force all HTTP traffic to HTTPS with a 301 redirect**
Use a permanent (301), not temporary (302), redirect — this passes SEO signal to the new URL.
- ☐ **Test every entry point, not just the homepage**
www and non-www, deep links, and any subdomain you serve.
- ☐ **Check for redirect loops if you're behind a CDN or proxy**
A common cause: the CDN's SSL mode conflicting with your origin server's own redirect logic.

Content

- ☐ **Scan for mixed content**
Any HTTP resource (image, script, stylesheet) loading on an HTTPS page breaks the padlock.
- ☐ **Update hardcoded HTTP URLs in your database or CMS**
Common on WordPress and similar platforms — a plain find-and-replace often isn't enough due to serialized data.
- ☐ **Update any external services pointing at the old HTTP URL**
Webhooks, embeds, and third-party integrations that reference your site directly.

Search & monitoring

**Add the HTTPS property in Google Search Console**

Treat it as a distinct property from the HTTP version and submit its sitemap.

Set up certificate expiry monitoring

Don't rely on remembering — use an automated alert independent of your renewal automation.

Confirm auto-renewal is actually working

Run a dry-run renewal test rather than assuming a cron job you set up months ago is still firing.

For the full guide behind any item on this list, visit sslguides.com — Start Here, HTTPS Migration, and How-To categories cover each step in depth.