MWP - Security & Access - Troubleshooting SSL issues (mixed content, propagation, expired cert)

Article Number: 1977 | Rating: Unrated | Last Updated: Thu, Mar 5, 2026 at 8:32 PM

In this article, we'll cover common SSL issues that you might encounter on your website.Â **Mixed Content** One of reasons an SSL-protected website still shows as â€œNot Secureâ€• is something called mixed content. When an SS installed, your website is expected to load entirely over a secure connection (HTTPS). This means every part of the p delivered securely, not just the main address.Â Mixed content happens when: The website itself loads securely us some parts of the page still load using http://Â Even if only one item on the page is insecure, the browser no longe page fully secure. **Why Mixed Content Causes SSL Warnings** SSL works by encrypting all data sent between your visitors. This encryption only applies to content loaded over HTTPS.Â When insecure (HTTP) content is included on page: That content is not encrypted Browsers cannot guarantee visitor safety The secure connection is considered i Because of this, modern browsers will: Remove the padlock icon Show a â€œNot Secureâ€• warning Block certain website from loadingÂ Â This can make it appear as though SSL is not working, even though the certificate itself is **Important Clarification** Mixed content does not mean your SSL certificate is broken or invalid.Â It means: The SS active The website is partially secure The page fails security checks because not all content is encryptedÂ Browse security of the entire page, not just the certificate.Â **Common Causes of Mixed Content** Mixed content usually ap Themes or plugins load files using HTTP External services or embeds do not use HTTPSÂ Â **How to Fix Mixed C** WordPress Websites If your WordPress website is showing SSL warnings due to mixed content, you can fix it by upd http:// to https://. The easiest way to do this is with the Better Search Replace plugin. **Step 1:** Make a Backup (Import making any changes: Backup your website files and database This ensures you can restore your site if anything goe **2:** Install and Activate Better Search Replace Log in to your WordPress admin dashboard Go to Plugins â†' Add Ne Search ReplaceÂ Click Install Now, then ActivateÂ **Step 3:** Open Better Search Replace Once activated, you can the WordPress menu:Â Go to Tools â†' Better Search ReplaceÂ Â **Step 4:** Update Links: In the Search for field, Replace with field, enter https Select the database tables you want to update (usually all tables are fine) Run a dry ru show how many changes will be made without actually changing anything) If everything looks correct, run the replac **Step 5:** Clear Cache Clear your WordPress cache if you use a caching plugin Clear your browser cache If you use a cache as wellÂ Â For Non-WordPress WebsitesÂ If your site does not use WordPress: Update all website link https:// Check images, scripts, and embedded contentÂ Â **Expired certificate**Â Â Â You can check if your SSL expired by going to your website and clicking on the padlock icon to view the certificate.Â Steps to check the validit **Firefox:** Click on the padlock Click on 'Connection secure'Â Click on 'More Information' Click on 'View Certificate' C periodÂ Â **Chrome:** Click on the settings button Click on 'Connection is secure' Click on 'Certificate is valid'Â Ch periodÂ **For cPanel:** Go to the 'Security' section Click on 'SSL/TLS Status' Check if the Auto-SSL is running and t included Allow a few minutes for Auto-SSL to install a new SSL certificateÂ **For Managed WordPress** The Auto- running constantly in the background making sure that your website is covered by a SSL certificate. If you have any SSL certificate did not renew, please don't hesitate to reach out and we'll gladly assist.Â Â **SSL certificate issuan propagation.** Depending on the type of SSL certificate you choose, the issuance time can vary: Domain Validated (D this category are the Let's Encrypt SSL certificates and our Simple SSL Certificate These can take anywhere from a few hours to be activated and installedÂ Â Organisation Validation (OV) certificate: In this category are our Organ and our Wildcard Organisational Certificates These can take a few days to activate as these require some additional Extended Validation (EV) certificate: In this category are our Extended certificates These certificates take the longes these require even more verifications. You can expect this to take a few days as wellÂ

Posted - Tue, Jan 13, 2026 at 9:52 AM.

Online URL:
https://www.heartinternet.uk/support/article/mwp-security-access-troubleshooting-ssl-issues-mixed-content-propagat