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

Article Number: 1976 | Rating: Unrated | Last Updated: Wed, Jan 21, 2026 at 8:48 PM

In this article,Â we'llÂ cover common SSL issues that you mightÂ encounterÂ on your website.Â **Mixed Content** common reasons an SSL-protected website still shows as â€œNot Secureâ€• is something called mixed content. Wh is installed, your website is expected to load entirely over a secure connection (HTTPS). This means every part of th delivered securely, not just the main address.Â Mixed content happens when: The website itself loads securely us parts of the page still load using http://Â Even if only one item on the page is insecure, the browser no longer cons secure. **Why Mixed Content Causes SSL Warnings** SSL works by encrypting all data sent between your website a encryption only applies to content loaded over HTTPS.Â When insecure (HTTP) content is included on a secure (HT content is not encrypted Browsers cannot guarantee visitor safety The secure connection is considered incompleteÂ modern browsers will: Remove the padlock icon Show a â€œNot Secureâ€• warning Block certain parts of the web Â This can make it appear as though SSL is not working, even though the certificate itself is installed correctly.

**Important Clarification** Mixed content does not mean your SSL certificate is broken or invalid.Â It means: The SS The website is partially secure The page fails security checks because not all content is encryptedÂ Browsers eva the entire page, not just the certificate.Â **Common Causes of Mixed Content** Mixed content usually appears when load files using HTTP External services or embeds do not use HTTPSÂ Â **How to Fix Mixed Content**Â For Wo your WordPress website is showing SSL warnings due to mixed content, you can fix it by updating old links from http easiest way to do this is with the Better Search Replace plugin. **Step 1:**Â Make a Backup (Important)Â Before mak Backup your website files and database This ensures you can restore your site if anything goes wrongÂ **Step 2:**Â Better Search Replace Log in to your WordPress admin dashboard Go to Plugins â†' Add New Search for Better Se Install Now, then ActivateÂ **Step 3:**Â Open Better Search Replace Once activated, you can find the plugin in the W Go to Tools â†' Better Search ReplaceÂ Â **Step 4:**Â Update Links: In the Search for field, enter http In the Replac Select the database tables you want to update (usually all tables are fine) Run a dry run first (this will show how man made withoutÂ actually changingÂ anything) If everything looks correct, run the replacement for realÂ **Step 5:**Â Cl WordPress cache if you use a caching plugin Clear your browser cache If you use a CDN, clear that cache as wellÂ Non-WordPress WebsitesÂ If your site does not use WordPress: Update all website links from http:// to https:// Ch and embedded contentÂ Â **Expired certificate**Â Â Â You can check if your SSL certificate has expiredÂ by go and clicking on the padlock iconÂ to view the certificate.Â Steps to check the validity period:Â **Firefox:** Click on t 'Connection secure'Â Click on 'More Information' Click on 'View Certificate' Check the validity periodÂ Â **Chrome** settings button Click on 'Connection is secure' Click on 'Certificate is valid'Â Check the validity periodÂ **For cPane** 'Security' section Click on 'SSL/TLS Status' Check if the Auto-SSL is running and the domains are included Allow a f Auto-SSL to install a new SSL certificateÂ **For Managed WordPress** The Auto-SSL feature is running constantly making sure that your website is covered byÂ aÂ SSL certificate. If you have any concerns that your SSL certificate pleaseÂ don'tÂ hesitate to reach outÂ andÂ we'llÂ gladlyÂ assist.Â Â **SSL certificateÂ issuance and propagatio** type of SSL certificate you choose,Â the issuance time can vary: Domain Validated (DV) certificate: In this category Encrypt SSL certificates and our Simple SSL Certificate These can take anywhere from a few minutes to aÂ few hou installedÂ Â Organisation Validation (OV) certificate: In this categoryÂ are our OrganisationalÂ certificates and ou Organisational Certificates These can take a few days to activate as theseÂ requireÂ someÂ additionalÂ checksÂ Validation (EV) certificate: In this category are our Extended certificates TheseÂ certificates take the longest to activ requireÂ 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/cpanel-security-access-troubleshooting-ssl-issues-mixed-content-propag