

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

Article Number: 1976 | Rating: Unrated | Last Updated: Thu, Mar 5, 2026 at 8:31 PM

In this article, we'll cover common SSL issues that you might encounter on your website. **Mixed Content** is one of the most common reasons an SSL-protected website still shows as "Not Secure" is something called mixed content. When a website is installed, your website is expected to load entirely over a secure connection (HTTPS). This means every part of the website is delivered securely, not just the main address. Mixed content happens when: The website itself loads securely using HTTPS, but some parts of the page still load using http://. Even if only one item on the page is insecure, the browser no longer considers the page secure. **Why Mixed Content Causes SSL Warnings** SSL works by encrypting all data sent between your website and the browser. Encryption only applies to content loaded over HTTPS. When insecure (HTTP) content is included on a secure (HTTPS) connection, content is not encrypted. Browsers cannot guarantee visitor safety. The secure connection is considered incomplete. Modern browsers will: Show a "Not Secure" warning, Block certain parts of the website, and 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. It means: The website is partially secure. The page fails security checks because not all content is encrypted. Browsers evaluate the entire page, not just the certificate. **Common Causes of Mixed Content** Mixed content usually appears when you load files using HTTP. External services or embeds do not use HTTPS. **How to Fix Mixed Content** For WordPress websites, if your WordPress website is showing SSL warnings due to mixed content, you can fix it by updating old links from http:// to https://. The easiest way to do this is with the Better Search Replace plugin. **Step 1:** Make a Backup (Important) Before making any changes, backup your website files and database. This ensures you can restore your site if anything goes wrong. **Step 2:** Install Better Search Replace Log in to your WordPress admin dashboard. Go to Plugins > Add New > Search for Better Search Replace. Install Now, then Activate. **Step 3:** Open Better Search Replace Once activated, you can find the plugin in the WordPress admin. Go to Tools > Better Search Replace. **Step 4:** Update Links: In the Search for field, enter http://. In the Replace with field, enter https://. Select the database tables you want to update (usually all tables are fine). Run a dry run first (this will show how many links will be made without actually changing anything). If everything looks correct, run the replacement for real. **Step 5:** Clear Cache Clear your WordPress cache if you use a caching plugin. Clear your browser cache. If you use a CDN, clear that cache as well. **Non-WordPress Websites** If your site does not use WordPress: Update all website links from http:// to https://. Check for external scripts and embedded content. **Expired certificate** You can check if your SSL certificate has expired by going to the browser's address bar and clicking on the padlock icon to view the certificate. Steps to check the validity period: **Firefox:** Click on the padlock icon > 'Connection secure' > Click on 'More Information' > Click on 'View Certificate' > Check the validity period. **Chrome:** Click on the padlock icon > settings button > Click on 'Connection is secure' > Click on 'Certificate is valid' > Check the validity period. **For cPanel:** Go to the 'Security' section > Click on 'SSL/TLS Status' > Check if the Auto-SSL is running and the domains are included. Allow a few minutes for Auto-SSL to install a new SSL certificate. **For Managed WordPress** The Auto-SSL feature is running constantly, making sure that your website is covered by an SSL certificate. If you have any concerns that your SSL certificate is expired, please don't hesitate to reach out and we'll gladly assist. **SSL certificate issuance and propagation** The type of SSL certificate you choose, the issuance time can vary: Domain Validated (DV) certificate: In this category, the issuance time is the shortest, typically taking a few minutes to a few hours. **Encrypt SSL certificates and our Simple SSL Certificate** These can take anywhere from a few minutes to a few hours to be installed. **Organisation Validation (OV) certificate:** In this category are our Organisational certificates and our Organisation Validation Certificates. These can take a few days to activate as these require some additional checks. **Extended Validation (EV) certificate:** In this category are our Extended certificates. These certificates take the longest to activate and require even more verifications. You can expect this to take a few days as well.

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>