Key Takeaways

- The **ERR_CERTIFICATE_TRANSPARENCY_REQUIRED** error occurs when Chrome cannot verify that a website's SSL certificate is logged in the Certificate Transparency (CT) system.
- Updating Chrome and checking SSL settings can resolve the issue quickly.
- This guide provides **10 actionable steps** to troubleshoot and fix the error.
- For advanced users, Certificate Transparency Exemption or reissuing the SSL certificate may be necessary.
- Temporarily ignoring the error is **not recommended** unless you're certain the website is safe.

Step-by-Step Guide: Fix the ERR_CERTIFICATE_TRANSPARENCY_REQUIRED Error

Step 1: Update Google Chrome

Outdated browsers can lead to certificate errors due to obsolete security protocols.

Steps:

1. Open Chrome and type `chrome://settings/help` in the address bar.
2. Check if an update is available.
3. Click on **"Update Google Chrome"** and restart the browser.

Pro Tip: Always ensure you're running the latest stable release of Chrome. (Check Chrome's version here).

Step 2: Clear the SSL State

Your system may be holding a cached SSL state that doesn't recognize the updated certificate.

On Windows:

1. Press `Windows + R` and type `inetcpl.cpl`.
2. Under the **"Content"** tab, click **Clear SSL State**.
3. Restart your browser.

On Mac:

1. Clear your browser cache and cookies via Chrome settings.

Step 3: Contact Your Certificate Authority (CA)

If your SSL certificate has not been logged in the **Certificate Transparency** system, it will trigger this error.

1. Identify your CA by checking your certificate details.
2. Contact your CA via their support system and request them to verify the issue.
3. Ask for your certificate to be logged in the CT system or reissued.

Recommended CA Resources:

- **Let's Encrypt** (support)
- **DigiCert** (contact)

Step 4: Apply a Certificate Transparency Exemption Policy (For Businesses Only)

If you manage corporate devices, you can apply policies to bypass Certificate Transparency requirements.

Steps:

1. Deploy the CT exemption policy through the Chrome Enterprise Policy tool.
2. Add trusted certificates to your certificate store.

Resource: Google Policy Reference.

Step 5: Reissue and Reinstall Your SSL Certificate

If your CA cannot resolve the issue, reissue the SSL certificate.

Steps:

1. Log into your CA's portal.
2. Request a certificate reissue.
3. Follow the CA's guide to reinstall the certificate on your website server.

Affiliate Link Tool Recommendation: Use tools like **EaseUS Backup Center** (get it here) to secure your server before making changes.

Step 6: Temporarily Disable Firewall or Antivirus Software

Over-protective security tools can interfere with SSL verifications.

1. Temporarily disable your antivirus or firewall to identify if it’s causing the issue.
2. Allow Chrome through your firewall settings.

Affiliate Link Suggestion: Use trusted VPNs like **NordVPN** (check NordVPN here) for secure browsing while your protection is off.

Step 7: Clear Cookies and Cached Data

Cached website files may conflict with Chrome’s certificate validation.

1. Go to Chrome settings:
   `Menu > More Tools > Clear Browsing Data.`
2. Check **Cookies** and **Cached Images and Files**.
3. Hit **Clear Data**.

Step 8: Disable Chrome Extensions

Extensions interfering with HTTPS connections may cause SSL errors.

Steps:

1. Visit `chrome://extensions/` in Chrome.
2. Toggle **off** all extensions one by one.

3. Recheck if the site loads without errors.

Recommended Management Tool: Safeguard personal data during extensions testing with **NordPass** (learn more).

Step 9: Ignore the Error (Last Resort)

If you're sure that the site is secure, bypass the validation temporarily.

1. Go to `chrome://flags`.
2. Locate **Proceed to SCT Errors**.
3. Enable this flag to bypass certificate checks.

Note: This is highly risky and recommended only for private and trusted websites.

Step 10: Check for Time Zone or System Time Issues

Incorrect device time can often invalidate SSL verification.

1. Open your system's **Date & Time Settings**.
2. Select **Set Time Automatically** based on your location.
3. Sync your system time with an authoritative server, e.g., **time.google.com**.

Advanced Troubleshooting Tips

- For webmasters, inspect your server logs and confirm that the certificate chain contains the correct SCT (Signed Certificate Timestamp).
- Use online tools like SSL Labs tester to validate your certificate's CT compliance.

Backup Tip: Ensure server settings are backed up using **MiniTool ShadowMaker** (get it here).

FAQs

1. What causes the ERR_CERTIFICATE_TRANSPARENCY_REQUIRED error?

This occurs when Chrome detects that an SSL certificate is not logged in a Certificate Transparency log. Chrome uses this method to detect fraudulent certificates.

---

2. Is ignoring the error safe?

Ignoring the error can expose you to security threats. Ensure the site is 100% trusted before bypassing the error.

---

3. What is Certificate Transparency?

It's a public logging system designed by Google and other entities to ensure SSL certificates are valid and trustworthy.

---

4. Which tools can help secure my site from SSL issues?

- **EaseUS Backup Center** (Check it here) for complete server backups.
- **NordVPN** (Visit NordVPN) to ensure secure web traffic during testing.

By following these expert-recommended steps, you'll ensure your site or browsing experience is secure and error-free.