How to Fix NET::ERR_CERT_COMMON_NAME_INVALID Chrome Error?

11 Effective Methods to Fix Net Err_Cert_Common_Name_Invalid Chrome Error

Encountering the NET::ERR_CERT_COMMON_NAME_INVALID error can be frustrating when accessing a website securely. This error indicates an issue with the SSL certificate validation, preventing a proper connection.

Thankfully, multiple solutions are available to help you resolve this error and regain access to the desired website. In this comprehensive troubleshooting guide, we will explore various steps you can take to fix the ERR CERT COMMON NAME INVALID error and browse seamlessly again.

But before we begin exploring the possible solutions to resolve the cert_common_name_invalid error, let's understand what this error is exactly and what causes it.

What is a Cert Common Name Invalid Error?

To understand what a common name invalid error is, let's clarify the concept of the "Common Name" (AKA CN) about SSL certificates. The common name refers to the domain for which the SSL certificate is issued.

This error signifies that the specified common name in the SSL certificate is invalid. In most instances, this occurs when the common name fails to align (does not match) with the domain where the certificate is installed.

What Causes the Net Cert_Common_Name_Invalid Error?

Apart from the common name issue, the NET::ERR_CERT_COMMON_NAME_INVALID error can occur due to n number of other reasons –

One possible cause is when the SSL certificate fails to account for variations between the www and non-www versions of the domain. Another scenario is attempting to enable HTTPS without installing an SSL certificate.

It's also worth noting that utilizing a self-signed SSL certificate, which lacks acknowledgment or is considered secure by the browser, can incite this error.

Furthermore, antivirus software can occasionally interfere with the SSL connection, leading to this error message. Additionally, specific browser extensions might conflict with the site's SSL connection, causing the error to appear. Misconfigured proxy settings can also contribute to the issue.

Lastly, a corrupted browser cache or SSL state can be a factor behind the NET::ERR_CERT_COMMON_NAME_INVALID error. It's essential to consider these different possibilities when troubleshooting the problem.

How to Resolve the Net Err Cert Common Name Invalid Error?

We advise starting with the first method and moving on to the next if the first one doesn't work.

Verify that CN on your SSL certificate matches the site's domain

Inspect for improper redirection

Verify that the addresses (WordPress and website addresses) are the same.

Ensure Siteurl and Home Rows Store Identical URLs

Replace a self-signed certificate with an SSL cert from a trusted CA.

Clear your browser's SSL state

Clear your browser's cache

Enable automatic detection of proxy settings

Disable browser extensions

Deactivate the HTTPS scanning feature

Update the browser and OS

1. Verify that CN on Your SSL Certificate Matches the Website's Domain

Case 1: Using Normal SSL Certificates (DV, OV, or EV)

To resolve the NET::ERR_CERT_COMMON_NAME_INVALID error, verifying that the Common Name on your SSL certificate matches the website domain you're accessing is crucial. The CN serves as an identifier for the certificate and should align with the site's domain name.

Follow the steps given below to verify whether CN on your SSL certificate matches the website's domain or not:

Open a fresh tab in the browser (Google Chrome).

In the URL bar, enter the website's address.

You will see the term "Not Secure" in the URL bar; click on that.

A list will appear.

Verify the value written on the right of the term Certificate. If it shows "Invalid," then it simply means that CN does not match the website's domain.

If there's a mismatch between the CN and the domain, obtaining a new certificate from a trusted CA with the correct CN is recommended.

Case 2: Using Wildcard SSL Certificate

When you utilize a Wildcard SSL Certificate to safeguard a subdomain of a primary domain and encounter this error, it signifies that the SSL certificate doesn't secure the subdomain you're attempting to access.

To illustrate, if you have acquired a wildcard certificate to secure *errorssl.com, it will not extend its protection to *remedies.errorssl.com. This happens because we use the subdomain level instead of a single domain in wildcard certificates.

Case 3: Using Subject Alternative Name SSL Certificate

If you are using a SAN SSL certificate, follow the steps given below:

Open a tab in Chrome.

In the Search Google bar, enter the site's URL.

Click "Not Secure" in the URL bar.

From the list, select Certificate (Invalid).

A new window will appear.

Click on the Details button.

A new window will appear.

The Extension Subject Alternative Name section explores the subdomains, www, non-www, and TDL variations that the cert protects. You will get this error if the domain you are accessing is not listed.

2. Inspect for Improper Redirection

Not all SSL certificates automatically protect your site's www and non-www versions. Thus, redirecting your website from one domain to another without installing an SSL certificate on the initial (original) domain can lead to this error.

For example, assume that you configure www.cheapsslweb.com to redirect to cheapsslweb.com. If you install the SSL certificate only on cheapsslweb.com and neglect www.cheapsslweb.com, you will likely encounter the error in question.

Note: To be 100% sure that redirects are causing the cert_common_name_invalid error, you can employ the Redirect Detective tool that is capable of identifying redirects between HTTP and HTTPS versions, along with redirects between www and non-www variations.

If you are sure that redirects are the reasons behind the mentioned error, then to resolve the issue, you can:

Purchase an SSL cert that includes both variations, or

Configure the redirect settings appropriately to align with the SSL certificate's coverage.

3. Verify that Both the Addresses (WordPress and website addresses) are the Same

Sometimes, website owners manually change the web protocol from HTTP to HTTPS without installing an SSL certificate. However, this can lead to a common name mismatch

error when visitors try to access the website. If you encounter this issue, review and update your WordPress URL settings.

Follow the steps given below to verify that both the addresses are the same:

Open the WordPress dashboard

Under the Settings section, click General.

Verify that WordPress Address (URL) and Site Address (URL) fields contain the same addresses.

If you notice any discrepancies between the two URLs, make the necessary adjustments to align them.

4. Ensure Siteurl and Home Rows Store Identical URLs

If the error hasn't been resolved, you need to ensure that the URL mentioned in the option_value in siteurl and home rows of your website's database is the same. Follow the steps given below to ensure the same:

Log in to your hosting account.

Open the phpMyAdmin app and select the website's database.

Click on the wp_options table to open it.

Verify that the rows "siteurl" and "home," store identical URLs. If they have different values, edit them to reflect the correct URL.

Save the changes you made to the wp_options table.

5. Replace a Self-Signed Certificate With an SSL Cert From a Trusted CA

Almost all web browsers widely acknowledge and support SSL certificates from trusted CAs. They are recognized and ensure website visitors do not encounter compatibility issues or security warnings when accessing your site.

Whereas using a self-signed certificate for your domain can lead to the occurrence of the net err_cert_common_name_invalid error. To fix it, you can either authenticate the self-signed SSL certificate with your browser (not recommended) or install a new SSL cert issued by a trusted CA.

Follow the steps given below to replace a self-signed certificate with an SSL cert from a reliable certificate authority:

Purchase an SSL certificate from a reliable CA (Comodo, Sectigo, or Certera) by submitting a certificate signing request.

Access your hosting account and locate the directory storing the self-signed certificate files for your website.

Replace the current self-signed certificate on the server with the new, trusted SSL certificate.

Retrieve the SSL certificate files from the trustworthy CA and upload them to the appropriate location in your hosting environment.

Configure your hosting environment to utilize the new SSL certificate to enhance website security effectively.

Verify the installation and functionality of the new SSL certificate by accessing your website using the secure HTTPS protocol.

You can also explore: SSL Certificates Installation Tutorials and Guides

6. Clear your Browser's SSL State

Browsers tend to cache SSL certificates to expedite page loading. But sometimes, because of these cached SSL certificate data, the browser cannot fetch the updated certificates – resulting in this error.

Follow the steps given below to clear your browser's SSL State:

Click on the Search button placed on the taskbar.

Type Internet Options and press Enter.

Navigate to the Content tab.

Under the Certificates section, click the Clear SSL Slate button.

7. Clear the Browser's Cache

One solution to this problem involves clearing your browser's cache. By doing so, you can eliminate any stored data occupying space on your browser and contribute to the connection issues mentioned earlier.

Follow the steps given below to clear the browser's cache:

Open a fresh tab in Chrome.

Click on Customize and Control Google Chrome icon (three vertical dots).

From the list, select More Tools, and click Clear browsing data.

In the Clear browsing data dialog box, select the Time range from the list, and click Clear data.

8. Enable Automatic Detection of Proxy Settings

Verifying and adjusting your proxy settings is essential to ensure seamless web browsing, as it allows your browser to connect to the internet and retrieve web content efficiently.

By enabling automatic detection of proxy settings, you can achieve the same and resolve the invalid issue of the common name.

Follow the steps given below to enable the automatic detection of proxy settings:

Click on the Search button placed on the taskbar.

Type Internet Properties and press Enter.

On the Connections tab, click LAN settings.

In the Local Area Network (LAN) Settings window, check the checkbox under the Automatic Configuration section before the Automatically Detect settings option.

Click OK.

9. Disable Browser Extensions

Sometimes, browser extensions can cause the net to err cert common name invalid error. However, it's difficult to determine which extension interferes with the website's HTTPS connection.

So, to pinpoint the exact extensions responsible for the problem, you can try removing each of the extensions individually and checking whether the error persists or vanishes (after removing that extension).

If the error disappears after removing a specific extension, it indicates that the removed extension was indeed the cause of the issue.

Follow the steps given below to remove extensions individually:

Open a fresh tab in Google Chrome.

Click the Extension icon.

Click on three vertical lines placed adjacent to any extension of your choice (that you want to disable), and click Remove from Chrome.

Click Remove again.

Reload the website and verify whether the error exists or not. If it does, repeat the process from step 2.

1. 10. Deactivate the HTTPS Scanning Feature

Many security software (third-party) offers a helpful functionality known as HTTPS scanning, which involves intercepting and examining encrypted connections.

Unfortunately, this feature occasionally generates conflicts, resulting in the frustrating cert_common_name_invalid error message.

Follow the steps given below to disable the HTTPS scanning feature in Avast antivirus software:

Open the Avast dashboard.

From the Menu list, select Settings.

Click Protection.

In the center pane, click Core Shields.

Under the Configure Shield settings section, click Web Shield.

Uncheck the checkbox next to the Enable HTTPS Scanning option.

If you use Windows antivirus software, turning off the Real-time protection feature is recommended.

Follow the steps given below to disable Windows antivirus software:

Click on the Search button placed on the taskbar.

Type Virus & Threat Protection and press Enter.

Toggle off the switch placed under the Real-time protection option.

2. 11. Update the Browser and OS

Maintaining up-to-date applications and an updated OS ensures a seamless digital experience. Disregarding these updates can result in software instability, which can cause many website errors, including the one under consideration.

Follow the steps given below to update the browser (Chrome):

Open a fresh tab in Chrome.

Click on Customize and Control Google Chrome icon (three vertical dots).

From the list, select Help, and click About Google Chrome.

The update will start automatically if it’s not the latest version.

Follow the steps given below to update the Windows OS:

Click on the Search button placed on the taskbar.

Type Windows Update settings and press Enter.

Click on the Check for updates button.

Conclusion

In conclusion, encountering the frustrating “NET::ERR_CERT_COMMON_NAME_INVALID” error when accessing a website can be resolved through various methods.

By taking these proactive measures, users can overcome the net err cert common name invalid error and browse the web confidently.