Troubleshoot SSL connection errors

An SSL connection error occurs if you try to connect to an SSL-enabled website and your browser cannot establish a secure connection with the website's server. In the article below, TipsMake will provide and guide you through several ways to fix SSL connection errors.

SSL certificates are used on millions of websites to provide security for online transactions. However, during SSL implementation , some problems can occur, resulting in error messages appearing on the user's screen when accessing the website.

SSL connection error

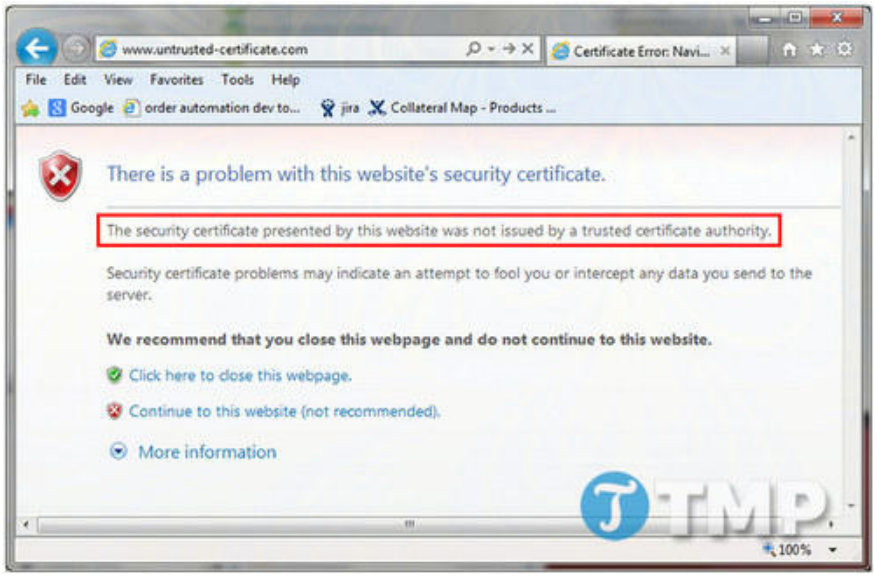
An SSL connection error occurs if you try to connect to an SSL-enabled website and your browser (client) is unable to establish a secure connection with the website's server.

Depending on the cause of the SSL connection error, the browser will display warnings such as ' *This Connection is Untrusted* ', ' *The site's security certificate is not trusted* ', or ' *Your Connection is not private* '.

Below, TipsMake will guide you on how to fix SSL connection errors.

Fix error The SSL certificate for this website is not trusted

Internet browsers will display an error message stating that the website certificate is untrusted if it has not been registered by a trusted Certificate Authority (CA). For the browser to accept the certificate, it must be linked to a 'trusted root certificate'.



Trusted root certificates are embedded in popular browsers such as **Internet Explorer** , **Firefox** , **Chrome** , and **Comodo Dragon** . These root certificates are used as 'trust tools' to verify the validity of all website certificates the browser encounters. If a certificate not signed by one of these root certificates is encountered, the browser will indicate that it is an untrusted certificate, and the visitor will receive the error message above.

Most trusted root certificates in a browser are recognized by a Certificate Authority (CA). When a CA signs a website's certificate, the website's certificate is linked to one of their trusted root certificates in the browser's certificate store.

For security reasons, most Certificate Authorities (CAs) do not register the end-entity directly from the root certificate; instead, they use an Intermediate certificate to create a 'chain of trust' within the root certificate. In this system, the root certificate signs the Intermediate certificate, and the Intermediate certificate is used to sign certificates for individual websites.

Therefore, the 'Untrusted' error is usually caused by one of the following two reasons:

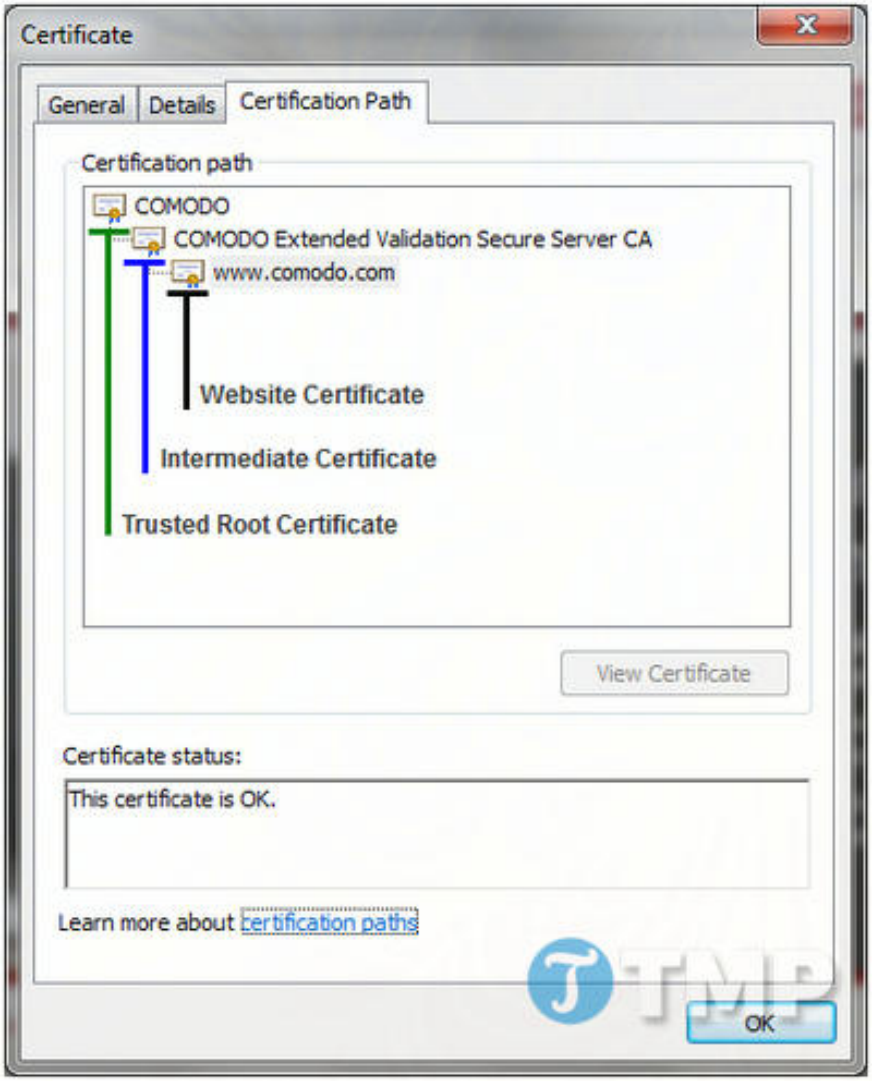
- The website uses a self-signed certificate.

In many cases, the 'Untrusted' error occurs because the website is using a self-signed certificate. As the name suggests, a self-signed certificate is a certificate created and signed by the website owner using their web server software. Therefore, this certificate is not linked to any trusted root certificate in the browser's certificate store, and the browser will display the 'Untrusted' error.

Self-signed certificates offer several advantages. Firstly, they are free to create and work quite well on internal servers. However, these certificates should not be used for deployment on commercial websites.

- Intermediate certificate not installed

Another potential cause of the 'Untrusted' error is that the website administrator has not correctly installed all the intermediate certificates on their web server. Here is an example illustrating this error:



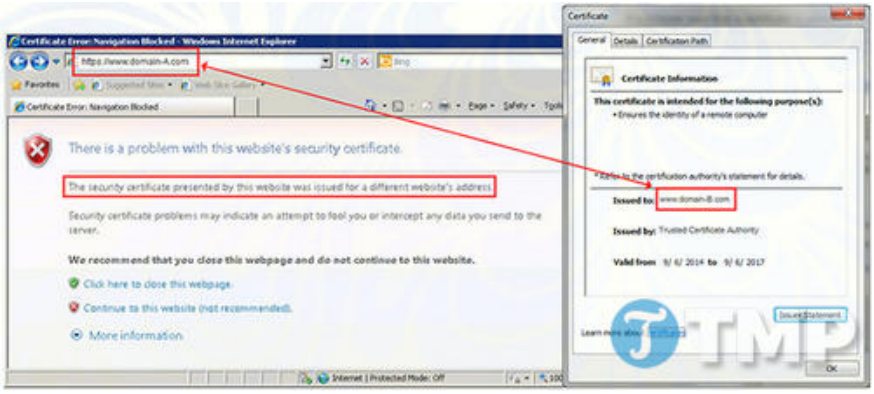
In the diagram above, you can see the certificate for www.comodo.com. **The Certification Path** tab shows the trust chain that the internet browser uses to verify the certificate. The trusted root certificate signs the Intermediate certificate, and then the Intermediate certificate signs the website certificate (in this example, www.comodo.com).

When a visitor establishes a connection to www.comodo.com, the web server must present both the site certificate and the Intermediate certificate to the visitor's browser. The browser then checks all certificates in the trust chain within the root certificate.

Most Certificate Authorities (CAs) will send a CA bundle file containing all the required intermediate certificates along with their end-entity to the website owner. However, if the web server administrator does not install all the intermediate certificates, users will receive an error message: 'certificate not trusted'.

Certificate Name Mismatch error

The 'Certificate Name Mismatch' error occurs when the server displays a domain name listed on the SSL certificate that does not match the domain name the browser is connecting to. To initiate an HTTPS session, the domain name on the certificate must exactly match the domain name in the browser's address bar.



Here are some of the reasons for the error:

- The website/server is accessed using an internal hostname or IP address, but the certificate is only issued with a fully qualified domain name (such as www.domain.com). Accessing the server using the internal hostname or IP address might take you to the same website, but if the certificate only contains the FQDN, it could cause a 'Certificate Name Mismatch' error.

- The certificate issued is domain.com, but the address bar of the browser enters www.domain.com (essentially, www is just a subdomain of domain.com). The 'Certificate Name Mismatch' error can still occur, but it's less common because most major certificate providers, including Comodo, issue a single domain certificate that includes both domain.com and www.domain.com.

However, if you encounter a 'Certificate Name Mismatch' error, this could be the cause. Using a **Wildcard** certificate can help you resolve this SSL connection error because any and all subdomains of domain.com will be automatically protected.

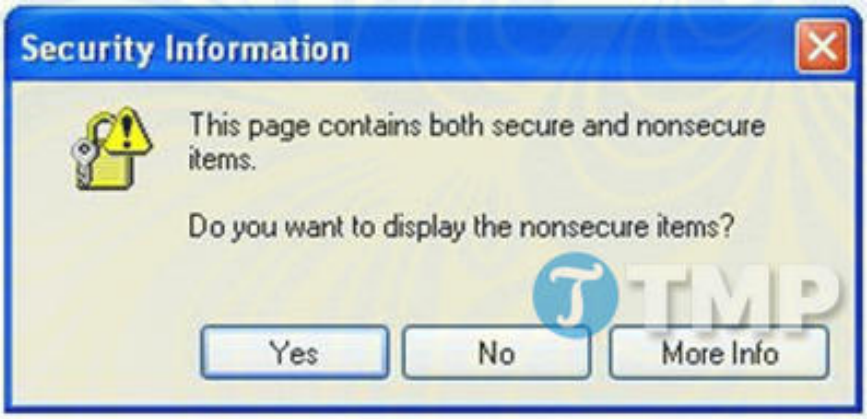
- Certificate Name Mismatch errors can occur when multiple websites are hosted on the same IP address. This is common in shared hosting environments. In a normal HTTP connection, the browser tells the server which domain it wants to connect to in the host header.

However, when an HTTPS connection is established, an SSL handshake means the browser requests a certificate from the server before presenting the host header. As a result, the server lacks the necessary information to decide which certificate to send and will present the wrong certificate.

If there is only one website and one certificate on a single IP address, the cause of the error is not there. However, if multiple websites are on the same IP address, the server may issue a certificate for the wrong domain. To prevent this, users can use a Multi-Domain certificate, which allows the website owner to add all websites and hostnames to the Subject Alternative Name (SAN) field of the certificate.

Mixed content error

For a secure connection, HTTPS is established, and items on the page must be retrieved from a secure source. This means all images, videos, iframes, flash movies, and Javascripts must be from a secure source. If any item is not retrieved from a secure source, website visitors will receive an error message similar to the one below:



If the visitor selects **Yes** , all items will be displayed, but the connection will revert to an insecure HTTP connection. If they select **No** , only secure items will be displayed. This means certain videos and images will not be shown, or the page will not execute important scripts. Either way, this sends a bad signal to your website visitors.

Here's how website administrators can fix the **Mixed Content** SSL connection error :

- Avoid calling any insecure content via HTTP or port 80. Change all references from HTTP to HTTPS. Ensure you have SSL set up at the source location. If using subdomains to host your website elements, a Wildcard certificate may be helpful.

- Use relative links on your website instead of absolute links. For example, instead of using **`src = http://mydomain.com/my-script.js`** , you can use **`src = /my-script.js`** . If your homepage is accessed via HTTPS, the browser will load **`/my-script.js`** via HTTPS. This technique is also useful if your website references external content that is a server via HTTP (e.g., YouTube or Google Analytics).

- Implement SSL across your entire website. This ensures a higher level of security for your website visitors, and it's also a criterion Google uses for website ranking, thus improving SEO to some extent.

Note that implementing SSL across your entire website means you have two copies of your content, so you'll need to 'tell' search engines which version is authoritative. To do this:

+ Inform search engines which HTTPS version is authoritative by updating links to point to the HTTPS version. Update **your XML sitemap** to reference the HTTPS version of your content. Making these changes means search engines will index your website's SSL version and display it in search results.

Ensure that **robots.txt** is available over HTTPS.

+ Redirect all HTTP requests to the HTTPS version using a permanent 301 redirect. This means your search engine ranking will shift to the HTTPS version.

Update your webmaster tools to reference the HTTPS version on your website instead of HTTP.

Above, TipsMake has introduced and guided you through some ways to fix SSL connection errors. If you are facing an SSL connection error, you can apply one of the methods above to resolve the issue.

Besides common SSL errors, you may also encounter this issue when accessing some popular websites like Facebook and Gmail. In this case, TipsMake's guide on how to fix SSL errors when accessing Facebook and

Gmail can help you reconnect.

If you have any questions, please leave your comments below the article!

You finished reading the article "**Troubleshoot SSL connection errors**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.