How to Fix the SSL Handshake Failed Error Code 525?

SSL-enabled websites are essential for cybersecurity; SSL Handshake plays a key role. The SSL Handshake establishes a secure connection between a web client and a web server to protect sensitive information from malicious actors intercepting or tampering with it.

However, users might encounter an SSL handshake failed error message during this process.

To understand the SSL handshake fail error message, it is important to examine the SSL handshake process thoroughly.

What is an SSL Handshake?

SSL Handshake is a process that involves three essential functions- algorithm agreement, certificate exchange, and the exchange of cryptographic keys with the help of a shared algorithm.

The server and client agree on one of the two shared algorithms and exchange cryptographic keys using an SSL certificate to encrypt client-server communication.

It also authenticates the server by checking the SSL certificates. Thus, it helps ensure the client is a server, not an imposter. However, often, a glitch happens during this handshake, resulting in an 'SSL handshake failed' error message.

Let us discuss the error message in detail.

What is the 'SSL Handshake Failed' Error Message?

An error message comes up when a client or server cannot establish a secure convention. It is called the SSL Handshake 525 Failed. It can happen for multiple reasons- sometimes due to some issue at the client's end and sometimes from the server's end.

This error message might come up for different reasons based on the client application users use or the server they are trying to connect with. For example, an error in GitHub looks like this:

However, an error 525 on Cloudflare will look something like this:

So what are the reasons that result in the error? Let's find out.

What Causes SSL Handshake Failure?

There are multiple reasons, here are some of the most common ones:

The Local Device has the Wrong Date or Time

One of the steps in the SSL/TLS Handshake process is for the browser to verify the validity of the SSL certificate. To check the certificate's validity period, a web browser or server needs to define the "valid from" and "valid until" fields in the certificate.

If the date and time on the device are incorrect, the browser may incorrectly determine that the certificate is invalid, causing the SSL/TLS Handshake to fail.

It is because the client cannot verify the validity of the certificate. The validity period of the certificate enables its use.

The certificate has a validity period during which it can be used. If the purchased SSL certificate is expired or invalid, the client will reject it. Thus, SSL Handshake will fail.

The issuing certificate authority (CA) creates and signs a timestamp in an SSL certificate. If the date and time on the client device are incorrect, it will not match the timestamp, causing the SSL Handshake to fail.

The Browser doesn't Support the Latest SSL Protocol

It occurs when the browser and server cannot negotiate a standard SSL protocol. This issue can occur if the browser does not support the latest SSL protocol and the server only allows connections using the latest protocol.

In this scenario, the browser cannot establish a connection and displays the error message.

The error message can also pop up if the SSL certificate is invalid or not trusted by the main server or if there is a problem with the SSL/TLS configuration on the server.

Your SSL Certificate is Invalid

The central server verifies the SSL certificate before establishing a secure, encrypted connection.

It will not establish a secure connection with the server if it does not recognize the certificate as valid. For example, A self-signed certificate will not be trusted because a trusted certificate authority does not sign it. A secure connection cannot be established if the certificate has expired.

Issue with the Server Name Identification (SNI) Configuration

SNI is an SSL protocol extension that allows a web server to host multiple SSL-enabled websites with different domain names on the same IP address. When the Browser sends the requested domain name during the Handshake process, the server uses this information to select the correct SSL certificate to present to the Browser.

Improper server configuration to use SNI may prevent it from matching the requested domain name to the correct SSL/TLS certificate, resulting in a failed SSL handshake.

If the web browser does not support SNI, the SSL Handshake may fail even if the server is configured to use it.

Issue with Content Delivery Network (CDN)

A CDN is a distributed server system that delivers web content to a user based on their geographic location.

So when a user tries to access a website via a CDN, the handshake process occurs between the edge server of the CDN and the user's Browser. If there is an issue with the CDN's SSL configuration, the SSL Handshake will fail, and the user will see an SSL Handshake error message.

The issue could arise from an incorrect certificate, an incorrect SSL certificate chain, or a certificate that the browser does not trust.

If we don't configure the CDN correctly to forward the Handshake to the origin server, it will show an error message.

These are some common reasons why error 525 come up. Let us discuss how to fix it.

How to Fix the 'TLS/SSL Handshake Failed' Error?

You can fix the SSL Handshake 525 Error in different ways. Here are some of them.

Update Your System Date and Time

Correcting the date and time on a device could fix an SSL Handshake error if the error is related to the certificate validation process, specifically if the browser is incorrectly determining that the certificate is not valid due to the incorrect date and time.

While this solution may not guarantee a fix, investigators should also examine other causes of the error.

Check if the SSL Certificate Is Valid, Configure the Browser for the Latest SSL Protocol Support

Checking if your SSL certificate is valid and configuring your browser for the latest SSL protocol support can fix this error and establish a secure connection with the server. However, the error must be related to the certificate validation process or the SSL protocol version.

Ensure that your Server is properly Configures to Support SNI

You need to ensure your server is appropriately config to support SNI. The SNI configuration involves some major issues, such as incorrect SNI configuration, missing SNI configuration, or missing domain names in the SNI configuration.

You also have to check that both your client-server and central server support SNI, as sometimes the latter do not support it.

Fixing Protocol Mismatch

The web server administrators can fix the protocol mismatch by configuring the web server and the client server to use the same SSL protocol. It allows them to establish a secure connection.

Web server admin can configure the browser to support the latest SSL protocol or configure the server to support older SSL protocols that it supports.

Check that your CDN or load balancer forwards the SSL protocol version your browser and server agree on.

These are some ways to fix the TLS handshake failed cloudflair error message.

Conclusion

As SSL Handshake plays a crucial role in keeping data in transit secure, users must understand what the SSL Handshake fail 525 error means and how to fix it. By following the fixes we have mentioned, you should be able to resolve the issue and establish a secure connection.