

Re: What version of SSL in 5.0 Web Server

Source:

<http://www.tech-archive.net/Archive/WindowsCE/microsoft.public.windowsce.platbuilder/2007-02/msg00642.html>

- *From:* "Tom" <tomkuhn@xxxxxxxxxx>
 - *Date:* 20 Feb 2007 12:43:05 -0800
-

Ok,

Here is what is happening so far. I disabled SSL 3.0 on the device. TLS is still enabled. I rebooted the device so the Web server is restarted. On my machine, I am running Ethereal and have turned off SSL in Firefox so that only TLS is running. When I try to connect to the web server <https://137.51.25.230>. In firefox I get "Firefox can't connect securely to 137.51.25.230 because the SSL protocol has been disabled."

When I try it in IE...

Holy smokes!! It worked! I am quite surprised. It seems that this only works in IE though. Quite strange. With Firefox I see the TLS Client Hello packet in ethereal going to the server, but no Server hello back. In IE I see the hello and server hello response, along with the rest of the TLS packets. Interesting???

On Feb 19, 5:37 pm, "Dylan DSilva \ (MS\)" <ddsi...@xxxxxxxxxxxxxx> wrote:

Do you have network packet traces for the successful case and for the failure? Packet traces will be useful in isolating the cause of the failure. Also make sure you're restarting the webserver and opening a new instance of your browser after changing the settings for them to take effect.

Dylan DSilva
Software Development Engineer
Microsoft Corporation

This posting is provided "AS IS" with no warranties, and confers no rights. You assume all risk for your use. © 2007 Microsoft Corporation. All rights reserved.

"Tom" <tomk...@xxxxxxxxxx> wrote in message

<news:1171899774.002211.136730@xx>

Re: What version of SSL in 5.0 Web Server

Currently, the registry keys have SSL 3.0 client/Server Enabled and TLS client/Server enabled. In IE or Firefox, SSL 3.0 and TLS 1.0 are checked. Everything works fine when hitting the web page on the web server. If I change the registry settings for SSL 3.0 client/Server to disabled, and unselect the SSL 3.0 in the web browser, I can not longer get to the web page. To me it seems in this case that the TLS is not working on the web server.

Tom

On Feb 16, 1:25 pm, "Dylan DSilva \ (MS\)" <ddsi...@xxxxxxxxxxxxxx> wrote:

CE 5.0 supports SSL 2.0, SSL 3.0 and TLS 1.0 (a.k.a SSL 3.1) which are collectively referred to as SSL protocols. What difficulties are you seeing with TLS connections to the webserver? By default all protocols including TLS should be enabled. The registry keys under HKLM\Comm\SecurityProviders\SCHANNEL\Protocols are only used to modify this default behavior.

Dylan DSilva
Software Development Engineer
Microsoft Corporation

This posting is provided "AS IS" with no warranties, and confers no rights.
You assume all risk for your use. © 2007 Microsoft Corporation. All rights reserved.

"Tom" <tomk...@xxxxxxxxxx> wrote in message

news:1171570708.208108.57200@xx

I must admit I am quite confused on the issue of SSL and TLS

Re: What version of SSL in 5.0 Web Server

versions. I know there was a SSL 2.0, SSL 3.0, and TLS 1.0. Our requirements for encryption (See Below) state that we need TLS or SSL 3.1. CE 5.0 specifies that the web server supports SSL, but I am not seeing anything for TLS. The web server is currently not working over a TLS connection. It will work over a SSL 3.0 connection though. I have been setting these in the HKLM\Comms\SecurityProviders\SChannel\Protocols. Does CE support TLS or SSL 3.1 for the Web Server?

Requirements:

SSL/TSL v3.0 and its successor SSL/TLS v3.1 are protocols that provide data security between application protocols such as HTTP (the protocol used by the Web) and the networking protocol TCP/IP. TLS establishes a secure, encrypted connection between the server and a TLS-capable browser, and then encrypts and decrypts information as it is sent and received. SSL v3.0 and earlier versions are not NIST FIPS 140-2 validated for FIPS mode use. TLS or SSL v3.1 is NIST validated for FIPS Mode use; therefore, TLS or SSL v3.1 is the required protocol for encrypting HTTP sessions. The TLS protocol does provide a mechanism that allows for backward compatibility.

Thanks,

Tom- Hide quoted text -

- Show quoted text -

Re: What version of SSL in 5.0 Web Server