Configure TLS 1.2 as default secure Protocol On Windows Server 2008 R2 SP1

Let say you are running Exchange Server 2010 installed on Windows Server 2008 R2 SP1 x64(bit), and when you remotely open Outlook Web Access (OWA to the Exchange Server) in your Google Chrome web browser it alerts you that the installed SSL certificate is insecure. When you check the detail about the SSL certificate, the web browser is letting you know that the configured SSL protocols on the server are deprecated.

Get an SSL Report of your Web Server's TLS and SSL configuration

As the Administrator, you first run an SSL Test and analysis of your webserver using the Qualys SSL Labs' SSL test from here: https://ssllabs.com/ssltest/ in order to analyze which Secure Socket Layer (SSL) and Transport Layer Security (TLS) protocols are available, enabled and/or set as default within the registry of your Server. Before inputting your server's web address to run these tests and to obtain a report, it is recommended for the sake of your webserver's privacy that you check the checkbox next to: “Do not show the results on the boards.”

Update to enable TLS 1.1 and TLS 1.2 as default secure protocols in WinHTTP in Windows

This update provides support for Transport Layer Security (TLS) 1.1 and TLS 1.2 in Windows Server 2012, Windows 7 Service Pack 1 (SP1), and Windows Server 2008 R2 SP1.

To obtain the stand-alone package for this update, go to the Microsoft Update Catalog website here: https://www.catalog.update.microsoft.com/search.aspx?q=kb3140245 and download and install the catalog update applicable to your server, such as “Update for Windows Server 2008 R2 x64 Edition (KB3140245).

Prerequisites for your server: To apply this update, you Windows Server 2008 R2 must have installed Service Pack 1 (SP1) for Windows 7 or Windows Server 2008 R2.

To understand why this update is or may be necessary, please review this Microsoft Support article: https://support.microsoft.com/en-us/topic/update-to-enable-tls-1-1-and-tls-1-2-as-default-secure-protocols-in-winhttp-in-windows-c4bd73d2-31d7-761e-0178-11268bb10392

Configuration Information for TLS 1.2.

See: https://support.laserfiche.com/kb/1013919/configuration-information-for-tls-1-2 or

https://support.laserfiche.com/kb/1013919/raw

Before attempting to edit your Windows registry, **MAKE A BACKUP FILE OF YOUR REGISTRY**.

In order to open the Windows Registry in Windows Server 2008 R2 SP1, First click the Windows “Start” button, and in the Run box input 'regeit.exe' (without the single quote marks) and press the enter key on your keyboard.

At the top of the Window's registry tree, select “Computer” right click on “Computer” and left click “Export” and then supply a name to the registry backup file, and save this exported copy of your registry in a folder (directory) where in the future you can locate and import this registry backup if you happen to make a huge mistake while editing the Windows registry.

Configure the Registry to Turn on TLS 1.2

In the registry, browse to
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols

Under the **Protocols** key, create a new Key that you will name as **TLS 1.2**. How? Right click on the **Protocols** key, and left click on **New** and left click on **Key** and input the name of the new key as being **TLS 1.2** and press enter or click on any white space to set the name of the new key.

In the same manner, create two new subkeys under the key that is named **TLS 1.2** and name these two new subkeys as **Client** and **Server** respectively.

In the Registry, browse to:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client and Create a new DWORD value named: **DisabledByDefault** and Set the value to: 0 (hexadecimal)

How? Right click on the **Client** subkey, and left click on new - DWord 32bit and name the Dword as **DisabledByDefault** and right click the new Dword that is named **DisabledByDefault** and select 'Modify' and set the value as **0** with the radio button for **hexadecimal** selected.

Also, under the **Client** subkey, create a new DWORD value named: **Enabled** and set the value to **1** (hexadecimal).

Now, in the Registry, browse to the new subkey named **Server** located at:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server

In the same manner under the **Server** subkey, create a new DWORD (32-bit) value named: **DisabledByDefault** and set its value in hexadecimal to: **0**

In the same manner under the **Server** subkey, create a new DWORD (32-bit) value named: **Enabled** and set its value to **1**

Enable TLS 1.2 by default for WinHTTP

Add the **DefaultSecureProtocols** DWORD value to the: **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp** registry key and

Add the **DefaultSecureProtocols** DWORD value to the: **HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp** registry key.

How? From the Windows search bar, use regedit to open the Window Registry Editor. Browse to **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp**. Create a new DWORD value named: **DefaultSecureProtocols**

and set the value of this new Dword (in hexadecimal) to: **800**

On a 64-bit version of Windows, ALSO browse to **HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp** and repeat the previous step by

Creating a new DWORD value named: **DefaultSecureProtocols**

And set the value of this new Dword (in hexadecimal) to: **800**.

Block RC4 in .NET TLS

If you have .NET Framework 4.x installed on the server, you should:

Add a **SchUseStrongCrypto** DWORD value to the **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319** registry key and also add it to the **HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v4.0.30319** registry key.

From the Windows search bar, use regedit to open the Window Registry Editor. Browse to **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319**. Create a new DWORD value named: **SchUseStrongCrypto**

Set the value to: **1**

On a 64-bit version of Windows, browse to **HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v4.0.30319** and repeat this same procedure by–

Creating a new DWORD value named: **SchUseStrongCrypto**

and setting the value to: **1**

Note: Restart the computer after modifying the registry