Enable TLS 1.1 & 1.2  
Then  
Disable SSL & TLS 1.0

Contents

[Information 2](#_Toc102482090)

[1. Documentation to enable TLS 1.1 & 1.2 2](#_Toc102482091)

[OS 2](#_Toc102482092)

[WinHTTP 2](#_Toc102482093)

[.NET Framework 2](#_Toc102482094)

[Determine .NET Version from Powershell with the command: 2](#_Toc102482095)

[Explanation for registry keys. 2](#_Toc102482096)

[MS SQL Server 3](#_Toc102482097)

[MS SQL Server 2012 3](#_Toc102482098)

[WSUS 3](#_Toc102482099)

[2. Procedure to enable TLS 1.1 & 1.2 4](#_Toc102482100)

[Enable OS Schannel 4](#_Toc102482101)

[WinHTTP 4](#_Toc102482102)

[MS Server 2012 R2 or newer 4](#_Toc102482103)

[MS Server 2012 or older 4](#_Toc102482104)

[.NET Framework 4](#_Toc102482105)

[MS SQL server 4](#_Toc102482106)

[2016 or newer 5](#_Toc102482107)

[2012 5](#_Toc102482108)

[References 5](#_Toc102482109)

# Information

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Author | Date | Changes |
| Version 0.1 | Nikola Velichkov | 2021-12-22 | This is the first version of the document. |
|  |  |  |  |
|  |  |  |  |

This document is for MS Windows Server 2012 R2 and newer.

# Documentation to enable TLS 1.1 & 1.2

First enable TLS 1.1 & 1.2 for OS, WinHTTP and .NET Framework.

## OS

For MS Windows Server 2016 and newer OS’s, the protocol TLS 1.2 should be default for SChannel.

“Start with the HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols registry key. Under that key you can create any subkeys in the set SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1, and TLS 1.2. Under each of those subkeys, you can create subkeys Client and/or Server. Under Client and Server, you can create DWORD values DisabledByDefault (0 or 1) and Enabled (0 or 1).”

## WinHTTP

For MS Windows Server 2012 R2 and newer OS’s, natively support protocol TLS 1.2 over WinHTTP.

## .NET Framework

.NET Framework 4.6.2 and later supports TLS 1.1 and TLS 1.2.

### Determine .NET Version from Powershell with the command:

**(Get-ItemProperty "HKLM:SOFTWARE\Microsoft\NET Framework Setup\NDP\v4\Full").Version**

### Explanation for registry keys.

This one configures all .NET applications to use OS settings when it is set to “1”.

"SystemDefaultTlsVersions" = dword:00000001

This one enables TLS 1.0, TLS 1.1 and TLS 1.2 when the value is set to “1”. When value is set to “0” SSL 3.0 and TLS 1.0 can be used.

"SchUseStrongCrypto" = dword:00000001

For 32-bit applications that are running on 32-bit OSs and for 64-bit applications that are running on 64-bit OSs, update the following subkey values:

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\.NETFramework\v2.0.50727]

"SystemDefaultTlsVersions" = dword:00000001

"SchUseStrongCrypto" = dword:00000001

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319]

"SystemDefaultTlsVersions" = dword:00000001

"SchUseStrongCrypto" = dword:00000001

For 32-bit applications that are running on 64-bit OSs, update the following subkey values:

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727]

"SystemDefaultTlsVersions" = dword:00000001

"SchUseStrongCrypto" = dword:00000001

[HKEY\_LOCAL\_MACHINE\SOFTWARE\WOW6432Node\Microsoft\.NETFramework\v4.0.30319]

"SystemDefaultTlsVersions" = dword:00000001

"SchUseStrongCrypto" = dword:00000001

## MS SQL Server

Microsoft SQL Server 2016 and later support TLS 1.1 and TLS 1.2. Earlier versions and dependent libraries might require updates.

### MS SQL Server 2012

<https://social.msdn.microsoft.com/Forums/en-US/1901b1f0-c360-4cd2-aad3-c55a008e0c9d/how-to-enable-tls-12-on-sql-server-2012-sp4?forum=sqlgetstarted>

<https://support.microsoft.com/en-us/topic/kb3135244-tls-1-2-support-for-microsoft-sql-server-e4472ef8-90a9-13c1-e4d8-44aad198cdbe>

## WSUS

For WSUS server that's running Windows Server 2012 R2, install update 4022720 or a later rollup update.

Get-HotFix -Computername COMPUTERNAME -Id KB5008263

# Procedure to enable TLS 1.1 & 1.2

## Enable OS Schannel

Create and/or edit registry keys.

## WinHTTP

### MS Server 2012 R2 or newer

Natively supports TLS 1.2.

### MS Server 2012 or older

Ensure update is installed:  
<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>

Create registry keys:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp\

DefaultSecureProtocols = (DWORD): 0xAA0

HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp\

DefaultSecureProtocols = (DWORD): 0xAA0

Registry keys explanation:

The example above shows the value of 0xAA0 for the WinHTTP DefaultSecureProtocols setting. [Update to enable TLS 1.1 and TLS 1.2 as default secure protocols in WinHTTP in Windows](https://support.microsoft.com/topic/update-to-enable-tls-1-1-and-tls-1-2-as-default-secure-protocols-in-winhttp-in-windows-c4bd73d2-31d7-761e-0178-11268bb10392) lists the hexadecimal value for each protocol. By default in Windows, this value is 0x0A0 to enable SSL 3.0 and TLS 1.0 for WinHTTP. The above example keeps these defaults, and also enables TLS 1.1 and TLS 1.2 for WinHTTP. This configuration ensures that the change doesn't break any other application that might still rely on SSL 3.0 or TLS 1.0. You can use the value of 0xA00 to only enable TLS 1.1 and TLS 1.2. Configuration Manager supports the most secure protocol that Windows negotiates between both devices.

## .NET Framework

Check .NET Framework version if it is >= 4.6.2 . Then it is compliant, else update .NET .

## MS SQL server

Check MS SQL Server version:

### 2016 or newer

They are compliant.

### 2012

Do the following

# References

<https://docs.microsoft.com/en-us/mem/configmgr/core/plan-design/security/enable-tls-1-2-client>

<https://docs.microsoft.com/en-us/dotnet/framework/network-programming/tls#configuring-security-via-the-windows-registry>

<https://docs.microsoft.com/en-us/dotnet/framework/network-programming/tls#configuring-security-via-the-windows-registry>