Best Practices for Enabling SSL, TLS and Ciphers

Contents

[Disabling Unsecure SSL/TLS on Registry 3](#_Toc37864503)

[Disable SSL 2.0 Protocols 3](#_Toc37864504)

[Disable SSL 3.0 Protocols 3](#_Toc37864505)

[Disable TLS 1.0 Protocols 4](#_Toc37864506)

[Disable TLS 1.1 Protocols 5](#_Toc37864507)

[Enable TLS 1.2 Protocols 5](#_Toc37864508)

[Ciphers 7](#_Toc37864509)

[Key Exchange Algorithms 7](#_Toc37864510)

[Disable TLS/SSL support for static key cipher suites 7](#_Toc37864511)

[Disable RC4 Ciphers 7](#_Toc37864512)

[To Prevent Poodle Attack 8](#_Toc37864513)

[To Prevent BEAST Attack 8](#_Toc37864514)

[Solution: Disable SSLv2, SSLv3, and TLS 1.0. The best solution is to only have TLS 1.2 enabled.” 8](#_Toc37864515)

[To Prevent Birthday attacks on 64-bit block ciphers (SWEET32) 8](#_Toc37864516)

[To Remove Weak Cipher Suites from TLS 9](#_Toc37864517)

[Ensuring the Changes reflects on Server 9](#_Toc37864518)

# Disabling Unsecure SSL/TLS on Registry

## Disable SSL 2.0 Protocols

Below is the set of steps to ensure SSL2.0 is disabled on the Server.

**Step 1 -** Disable SSL 2.0 Protocols

1. Navigate to the below mentioned Path in registry

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0]

1. Check if we already have client key, if yes ignore this step,
2. If no add key and Name it Client - Right Click on SSL 2.0 -> New -> Key and Name it Client
3. Right Click on SSL 2.0 -> Client -> Right Click on Client and Select New -> DWORD (32-Bit) Value

Name: DisabledByDefault

Value Data: 1

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Client]

"DisabledByDefault"=dword:00000001

1. Add key and Name it Server - Right Click on SSL 2.0 -> New -> Key and Name it Server
2. Right Click on SSL 2.0 -> Server -> Right Click on Server and Select New -> DWORD (32-Bit) Value

Name: Enabled

Value Data: 0

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server]

"Enabled"=dword:00000000

## Disable SSL 3.0 Protocols

Below is the set of steps to ensure SSL3.0 is disabled on the Server.

**Step 2 -** Disable SSL 3.0 Protocols

1. Navigate to the below mentioned Path in registry

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols]

1. Add key and Name it SSL 3.0 - Right Click on Protocols -> New -> Key and Name it SSL 3.0
2. Add key and Name it Client - Right Click on SSL 3.0 -> New -> Key and Name it Client
3. Add key and Name it Server - Right Click on SSL 3.0 -> New -> Key and Name it Server
4. Right Click on SSL 3.0 -> Client -> Right Click on Client and Select New -> DWORD (32-Bit) Value

Name: DisabledByDefault

Value Data: 1

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Client]

"DisabledByDefault"=dword:00000001

1. Right Click on SSL 3.0 -> Server -> Right Click on Server and Select New -> DWORD (32-Bit) Value

Name: Enabled

Value Data: 0

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server]

"Enabled"=dword:00000000

## Disable TLS 1.0 Protocols

Below is the set of steps to ensure TLS1.1 is disabled on the Server.

**Step 3 -** Disable TLS 1.0 Protocols

1. Navigate to the below mentioned Path in registry

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0]

1. Add key and Name it TLS 1.1 - Right Click on Protocols -> New -> Key and Name it TLS 1.0
2. Add key and Name it Client - Right Click on TLS 1.0 -> New -> Key and Name it Client
3. Add key and Name it Server - Right Click on TLS 1.0 -> New -> Key and Name it Server
4. Right Click on TLS 1.0 -> Client -> Right Click on Client and Select New -> DWORD (32-Bit) Value

Name: Enabled

Value Data: 0

1. Right Click on TLS 1.0 -> Client -> Right Click on Client and Select New -> DWORD (32-Bit) Value

Name: DisabledByDefault

Value Data: 1

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Client]

"Enabled"=dword:00000000

"DisabledByDefault"=dword:00000001

1. Right Click on TLS 1.0 -> Server -> Right Click on Server and Select New -> DWORD (32-Bit) Value

Name: Enabled

Value Data: 0

1. Right Click on TLS 1.0 -> Server -> Right Click on Server and Select New -> DWORD (32-Bit) Value

Name: DisabledByDefault

Value Data: 1

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server]

"Enabled"=dword:00000000

"DisabledByDefault"=dword:00000001

## Disable TLS 1.1 Protocols

Below is the set of steps to ensure TLS1.1 is disabled on the Server.

**Step 4 -** Disable TLS 1.1 Protocols

1. Navigate to the below mentioned Path in registry

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1]

1. Add key and Name it TLS 1.1 - Right Click on Protocols -> New -> Key and Name it TLS 1.1
2. Add key and Name it Client - Right Click on TLS 1.1 -> New -> Key and Name it Client
3. Add key and Name it Server - Right Click on TLS 1.1 -> New -> Key and Name it Server
4. Right Click on TLS 1.1 -> Client -> Right Click on Client and Select New -> DWORD (32-Bit) Value

Name: Enabled

Value Data: 0

1. Right Click on TLS 1.1 -> Client -> Right Click on Client and Select New -> DWORD (32-Bit) Value

Name: DisabledByDefault

Value Data: 1

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Client]

"Enabled"=dword:00000000

"DisabledByDefault"=dword:00000001

1. Right Click on TLS 1.1 -> Server -> Right Click on Server and Select New -> DWORD (32-Bit) Value

Name: Enabled

Value Data: 0

1. Right Click on TLS 1.1 -> Server -> Right Click on Server and Select New -> DWORD (32-Bit) Value

Name: DisabledByDefault

Value Data: 1

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server]

"Enabled"=dword:00000000

"DisabledByDefault"=dword:00000001

## Enable TLS 1.2 Protocols

Below is the set of steps to ensure TLS1.2 is enabled on the Server.

**Step 5 -** Enable TLS 1.2 Protocols

1. Navigate to the below mentioned Path in registry

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2]

1. Add key and Name it TLS 1.2 - Right Click on Protocols -> New -> Key and Name it TLS 1.2
2. Add key and Name it Client - Right Click on TLS 1.2 -> New -> Key and Name it Client
3. Add key and Name it Server - Right Click on TLS 1.2 -> New -> Key and Name it Server
4. Right Click on TLS 1.2 -> Client -> Right Click on Client and Select New -> DWORD (32-Bit) Value

Name: Enabled

Value Data: 1

1. Right Click on TLS 1.2 -> Client -> Right Click on Client and Select New -> DWORD (32-Bit) Value

Name: DisabledByDefault

Value Data: 0

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client]

"Enabled"=dword:00000001

"DisabledByDefault"=dword:00000000

1. Right Click on TLS 1.2 -> Server -> Right Click on Server and Select New -> DWORD (32-Bit) Value

Name: Enabled

Value Data: 1

1. Right Click on TLS 1.2 -> Server -> Right Click on Server and Select New -> DWORD (32-Bit) Value

Name: DisabledByDefault

Value Data: 0

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server]

"Enabled"=dword:00000001

"DisabledByDefault"=dword:00000000

# Ciphers

## Key Exchange Algorithms

Below is the steps to Set Key Exchange Algorithms on the Server.

**Step 6 -** Disable Ciphers

1. Navigate to the below mentioned Path in registry

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms]

1. Add key and Name it Diffie-Hellman Right Click on KeyExchangeAlgorithms -> New -> Key and Name it Diffie-Hellman
2. Right Click on Diffie-Hellman and Select New -> DWORD (32-Bit) Value

Name: Enabled

Value Data: 0

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\Diffie-Hellman]

"Enabled"=dword: 00000000

## Disable TLS/SSL support for static key cipher suites

1. Right Click on KeyExchangeAlgorithms -> New -> Key and Name it PKCS

Right Click on PKCS and Select New -> DWORD (32-Bit) Value

Name: Enabled

Value Data: 0

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\PKCS]

"Enabled"=dword: 00000000

## Disable RC4 Ciphers

1. Navigate to the below mentioned Path in registry

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers]

1. Add key and Name it RC4 128/128 Right Click on Ciphers -> New -> Key and Name it RC4 128/128

Right Click on RC4 128/128 and Select New -> DWORD (32-Bit) Value

Name: Enabled

Value Data: 0

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 128/128]

"Enabled"=dword:00000000

1. Navigate to the below mentioned Path in registry

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers]

1. Add key and Name it RC4 40/128 Right Click on Ciphers -> New -> Key and Name it RC4 40/128

Right Click on RC4 40/128 and Select New -> DWORD (32-Bit) Value

Name: Enabled

Value Data: 0

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 40/128]

"Enabled"=dword:00000000

1. Navigate to the below mentioned Path in registry

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers]

1. Add key and Name it RC4 56/128 Right Click on Ciphers -> New -> Key and Name it RC4 56/128

Right Click on RC4 56/128 and Select New -> DWORD (32-Bit) Value

Name: Enabled

Value Data: 0

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 56/128]

"Enabled"=dword:00000000

1. Navigate to the below mentioned Path in registry

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers]

Add key and Name it RC4 128/128 - Right Click on Ciphers -> New -> Key and Name it RC4 128/128

Right Click on RC4 128/128 and Select New -> DWORD (32-Bit) Value

Name: Enabled

Value Data: 0

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 128/128]

"Enabled"=dword:00000000

1. Add key and Name it RC4 64/128 Right Click on Ciphers -> New -> Key and Name it RC4 64/128

Right Click on RC4 64/128 and Select New -> DWORD (32-Bit) Value

Name: Enabled

Value Data: 0

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 64/128]

"Enabled"=dword:00000000

## To Prevent Poodle Attack

Solution: Disable SSL3

## To Prevent BEAST Attack

## Solution: Disable SSLv2, SSLv3, and TLS 1.0. The best solution is to only have TLS 1.2 enabled.”

## To Prevent Birthday attacks on 64-bit block ciphers (SWEET32)

Solution: Disable TLS/SSL support for 3DES cipher suite

**Actual solution**: Add this registry key:

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\Triple DES 168\Enabled (DWORD: 0)

## To Remove Weak Cipher Suites from TLS

**Solution 1:**

Step 1: Query the TLS Cipher Suites supported from the machine in Power Shell using below command

Command: Get-TlsCipherSuite | Format-Table Name

Step 2: Identify the Weak Cipher Suites name to remove and use the below command to remove the Cipher Suite.

**Example**: In below command we are just removing weak cipher suite “TLS\_RSA\_WITH\_RC4\_128\_SHA”

Similarly you can use other weak cipher suite **name** to remove in below command.

Command: Disable-TlsCipherSuite -Name “TLS\_RSA\_WITH\_RC4\_128\_SHA“

Step 3: Again query the TLS Cipher suites supported from machine using **Step 1 command** and check the weak cipher is removed from the results.

Step 4: Restart the server to apply the config changes.

**If Solution 1 not works then try Solution 2 to fix.**

**Solution 2:**

Steps 1: Download IISCrypto and install in machine where TLS need to be configured

Steps 2: Launch IISCrypto

Step 3: Click on **Cipher Suites icon** from left menu

Step 4: **Uncheck the checkbox** of the weak ciphers suites shown in window and click on apply button

Step 5: IISCrypto will show **reboot** **prompt** to apply changes and click on **OK** button.

Step 6: Again launch the IISCrypto, select the Cipher Suite menu and we can see that unchecked weak cipher suites are not shown in that window.

## Ensuring the Changes reflects on Server

**Step 7 -** Restart the Server