TLS Remediation

In case of any OS **BEFORE** Windows Server 2012, you must enable TLS 1.2 as a support server-side protocol. For Windows Server 2008 R2, you MUST apply the patch and merge the .reg file in the file set within Add.TLS.1.2.RDS.Support.zip before ANYTHING ELSE. If you do not, when you configure the crypto settings using the Configure\_Crypto file, you will lock yourself out of the server for RDP since it cannot support TLS 1.2 without the first patch.

**NOTE: Sometimes, the User Access Control settings on the server will be elevated to High. If this is the case, then extracting any .reg files from the .zip archives will fail since the OS regards the .reg file in the .zip as dangerous…and will not extract that particular file. In these cases, you will need to:**

1. **Extract the .zip on another machine.**
2. **Rename from .reg to .re\_**
3. **Copy the .re\_ file to the server**
4. **Rename back to .reg,**
5. **Right click > Merge. If the UAC is elevated…you won’t be able to Merge from the right click menu. You will need to import directly from within Registry Editor (File > Import).**

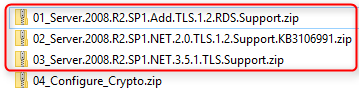
First, make sure that the OS supports TLS 1.2 by default (2008 R2 does not). There is a list of files on the SharePoint site at this location:

<https://skydrive3m.sharepoint.com/sites/IT/cshs/Operations%20Team%20Only/Forms/AllItems.aspx?viewpath=%2Fsites%2FIT%2Fcshs%2FOperations%20Team%20Only%2FForms%2FAllItems%2Easpx&id=%2Fsites%2FIT%2Fcshs%2FOperations%20Team%20Only%2FPrivate%2FTLS>

Depending on the OS that is used here, follow the sub-folder, and run the patches in the numeric prefix on the file names. Some may not apply since they were picked up in a previous patch. Just run through and try to apply them all.

**Step 1:**

For the patching, please apply the patches for the respective OS by extracting the .zip files and running the patches/registry files in them. For example, these are the patches for Windows Server 2008 R2:



For Server 2008 R2 and prior, **MAKE ABSOLUTELY** positive that you apply both the files found in **01\_Server.2008.R2.SP1.Add.TLS.1.2.RDS.Support.zip** before anything else, or you will cut off your RDP connectivity since it will try to use TLS 1.2 but is not configured correctly for it.

After applying the patches and registry fix highlighted above (NOT the Configure\_Crypto yet), reboot the server.

**REBOOT.**

**Step 2:**

**Registry Editor**

**regedit.exe:**

**Correct registry (use Configure\_Crypto.reg):**

**Merge Configure\_Crypto.reg into registry. (If you have issues with merging the .reg files, refer to the notes in the first section of this document.)**

**Step 3:**

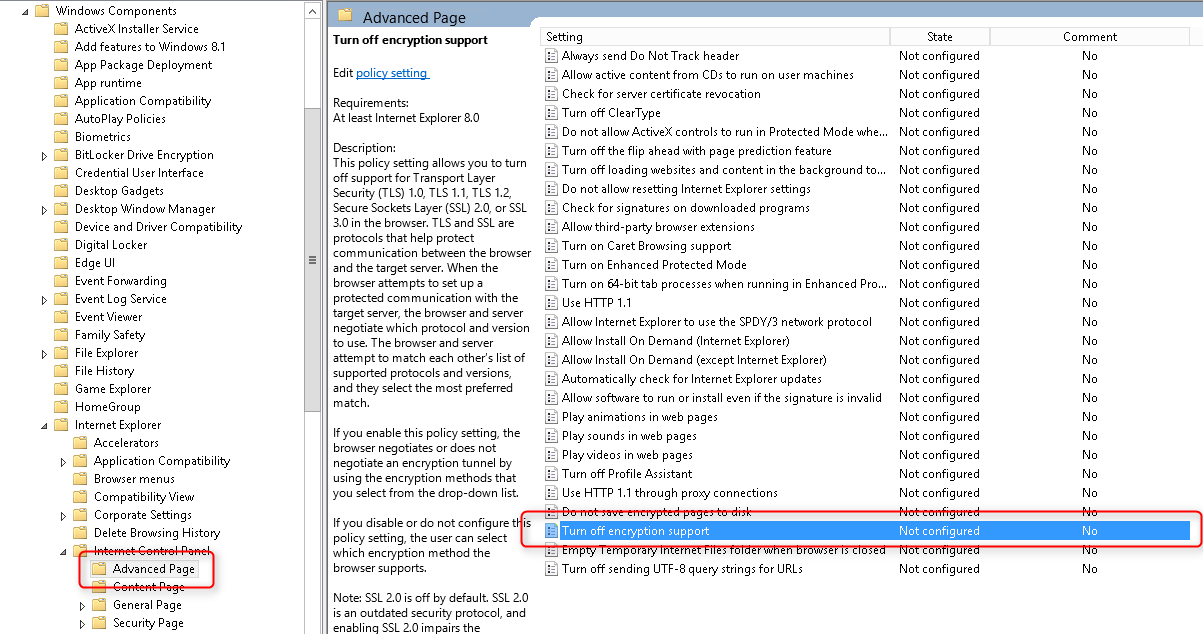
**Group Policy Editor**

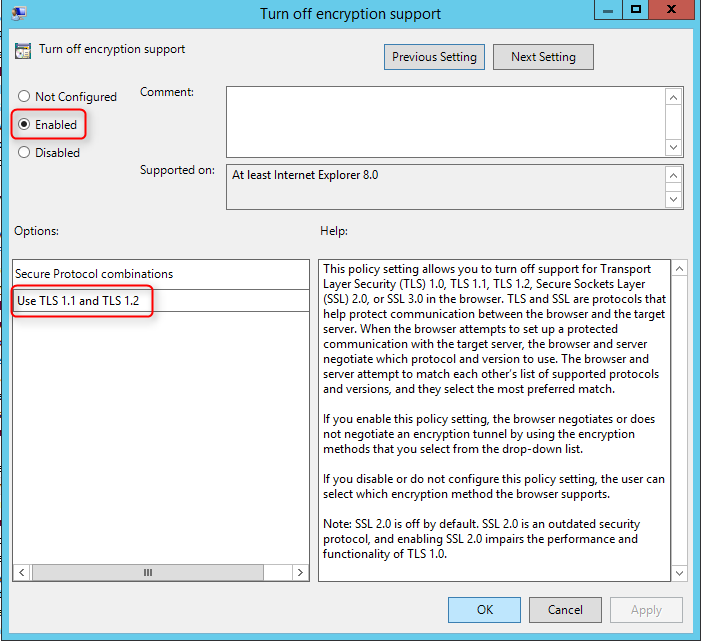
**gpedit.msc:**

Modify local Group Policy (this may have issues later when AD GPO pushes policy to server and resets this configuration setting):

Run > **gpedit.msc**

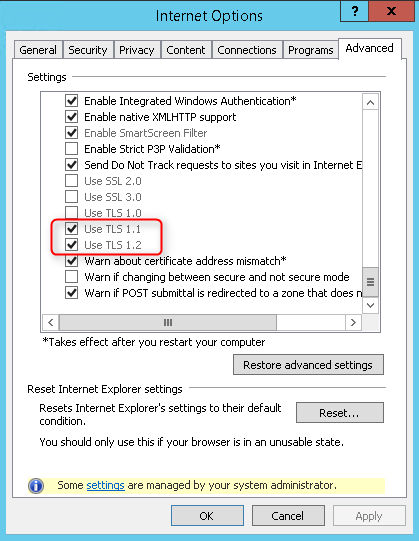
**Computer Configuration > Admin Templates > Windows Components > Internet Explorer > Internet Control Panel > Advanced Page**





**Internet Explorer:**

**Check: Internet Explorer > Internet Options > Advanced:**



**Step 4:**

**REBOOT.**

**Remediation complete.**

**Reference**

**Registry changes**

*(these are the configuration settings for reference)*

Windows Registry Editor Version 5.00

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

"EventLogging"=dword:00000001

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

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

"Enabled"=dword:ffffffff

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\AES 256/256]

"Enabled"=dword:ffffffff

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

"Enabled"=dword:00000000

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

"Enabled"=dword:00000000

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 128/128]

"Enabled"=dword:00000000

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 40/128]

"Enabled"=dword:00000000

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 56/128]

"Enabled"=dword:00000000

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

"Enabled"=dword:00000000

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

"Enabled"=dword:00000000

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

"Enabled"=dword:00000000

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

"Enabled"=dword:00000000

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\Triple DES 168]

"Enabled"=dword:00000000

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

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

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\MD5]

"Enabled"=dword:ffffffff

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\SHA]

"Enabled"=dword:ffffffff

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\SHA256]

"Enabled"=dword:ffffffff

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\SHA384]

"Enabled"=dword:ffffffff

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\SHA512]

"Enabled"=dword:ffffffff

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

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

"Enabled"=dword:00000000

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

"Enabled"=dword:ffffffff

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

"Enabled"=dword:ffffffff

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

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\Multi-Protocol Unified Hello]

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\Multi-Protocol Unified Hello\Client]

"Enabled"=dword:00000000

"DisabledByDefault"=dword:00000001

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\Multi-Protocol Unified Hello\Server]

"Enabled"=dword:00000000

"DisabledByDefault"=dword:00000001

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

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

"Enabled"=dword:00000000

"DisabledByDefault"=dword:00000001

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

"Enabled"=dword:00000000

"DisabledByDefault"=dword:00000001

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

"DisabledByDefault"=dword:00000001

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

"DisabledByDefault"=dword:00000001

"Enabled"=dword:00000000

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

"DisabledByDefault"=dword:00000001

"Enabled"=dword:00000000

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

"DisabledByDefault"=dword:00000001

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

"Enabled"=dword:00000000

"DisabledByDefault"=dword:00000001

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

"Enabled"=dword:00000000

"DisabledByDefault"=dword:00000001

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

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

"Enabled"=dword:00000000

"DisabledByDefault"=dword:00000001

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

"Enabled"=dword:00000000

"DisabledByDefault"=dword:00000001

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

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

"Enabled"=dword:ffffffff

"DisabledByDefault"=dword:00000000

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

"Enabled"=dword:00000000

"DisabledByDefault"=dword:00000001

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

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

"Enabled"=dword:ffffffff

"DisabledByDefault"=dword:00000000

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

"Enabled"=dword:ffffffff

"DisabledByDefault"=dword:00000000

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

"SchUseStrongCrypto"=dword:00000001

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

"SchUseStrongCrypto"=dword:00000001

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

"SchUseStrongCrypto"=dword:00000001

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

"SchUseStrongCrypto"=dword:00000001

**Additional notes:**

**Server 2008 R2 SP1 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

Update to add RDS support for TLS 1.1 and TLS 1.2 in Windows 7 or Windows Server 2008 R2:

<https://support.microsoft.com/en-us/help/3080079/update-to-add-rds-support-for-tls-1.1-and-tls-1.2-in-windows-7-or-wind>

**All servers \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

Support for TLS System Default Versions included in the .NET Framework 3.5 on Windows 8.1 and Windows Server 2012 R2:

<https://support.microsoft.com/en-us/help/3154520/support-for-tls-system-default-versions-included-in-the-.net-framework>

SchUseStrongCrypto:

<http://www.diaryofaninja.com/blog/2016/02/28/pci-compliant-web-deploy-getting-webdeploy-working-after-disabling-insecure-ciphers-like-ssl-30-and-tls-10>

SchUseStrongCrypto - .NET 2.0:

<https://technet.microsoft.com/en-us/library/security/2960358.aspx>

IISCrypto:

<https://www.nartac.com/Products/IISCrypto>

TLS/SSL Settings:

<https://technet.microsoft.com/en-us/library/dn786418(v=ws.11).aspx#bkmk_schanneltr_tls12>

Differences in the Schannel SSP by OS:

<https://technet.microsoft.com/en-us/library/dn786433(v=ws.11).aspx>

On Server 2008 R2 (work in progress):

<https://social.technet.microsoft.com/Forums/ie/en-US/aaced205-b0ec-4874-b440-8075dd74d8df/a-fatal-error-occurred-while-creating-an-ssl-client-credential-the-internal-error-state-is-10013?forum=exchangesvradmin>

( no effect - but see this about the Local Security Policy: )

<https://technet.microsoft.com/en-us/library/dd560644(v=ws.10).aspx>

**SQL Server 2008 R2 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

TLS 1.2 support for SQL server blog:

<https://blogs.msdn.microsoft.com/sqlreleaseservices/tls-1-2-support-for-sql-server-2008-2008-r2-2012-and-2014/>

TLS 1.2 support for SQL server KB:

<https://support.microsoft.com/en-us/help/3135244/tls-1.2-support-for-microsoft-sql-server>

Patches for TLS 1.2 support by OS:

KB3154518 – Reliability Rollup HR-1605 – NDP 2.0 SP2 – Win7 SP1/Win 2008 R2 SP1

KB3154519 – Reliability Rollup HR-1605 – NDP 2.0 SP2 – Win8 RTM/Win 2012 RTM

KB3154520 – Reliability Rollup HR-1605 – NDP 2.0 SP2 – Win8.1RTM/Win 2012 R2 RTM