Tls1 1 and 1.2

No need to muck about in the registry, just use this tool to do the hard work (and apply best practices with 1 click). You will need to immediately reboot the server after making this change otherwise you will get errors by anything using SSL (like Exchange): �� I love that it's a portable program (no install). I clicked the "Best Practices" button since it seemed to enable what i'm looking for. But it still doesn't show. I'm wondering if i need to clean out my registry changes then run it again. Thoughts? Did you reboot the server after making those changes? This tool should essentially just make those reg changes for you. Sorry, I should have mentioned i did reboot. I just found an article that says TLS 1.1 and 1.2 are available on 2008 R2. I'm running 2008 (non R2) which is probably the issue here. Thanks for the program as i'm sure I can use this elsewhere. the nartac IISCRYPTO program is wonderful I have been doing this with a reg file for a while but the results where not nearly as good as with the app. I have added it to my tool belt thanks again for posting it :-) Does that mean that SBS 2008 does not support TLS 1.1 or 1.2, in which case the only fix is to upgrade? M Boyle is correct. No support for TLS 1.1+ on SBS 2008. To get better TLS you need to upgrade to a newer version of SBS but the writing on the wall points to small business being pushed to cloud for email and servers since the SBS line is now officially dead. So, you can either upgrade to the latest SBS, or to a 2012 server plus exchange, or the cloud with Office 365 (or jump ship to gmail for business). �� I believe one of the optional update KB3080079 provides the functionality to 2008 as well Looks like it's for RDS on Win 7 / Server 2008 r2. I very much doubt that MS will ever introduce support for TLS 1.1 & 1.2 on Server 2008 at this stage in it's life-cycle. Late as it is, TLS 1.1/1.2 support was recently added to Windows Server 2008 (non R2). jonathanlaughery wrote:Late as it is, TLS 1.1/1.2 support was recently added to Windows Server 2008 (non R2).Thank you! I have more than 400 servers all are windows servers(2008,2012),In which i need to check TLS 1.2 is enabled or not. where i have to check about TLS 1.2 is enabled or not? and please letme know have any script to get the output in excel . i know we can check via regedit from the below path and need script to check for 400 servers. HKLM SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols, @ajithsaim, you started TWO other posts in addition to this one with the same question. Don't highjack this old thread, focus on your duplicate new posts instead. jonathanlaughery wrote:Late as it is, TLS 1.1/1.2 support was recently added to Windows Server 2008 (non R2).Fabulous! Thanks TONS! Has anyone got this patch deployed and working? I've tried to deploy the patch to a Wndows Server 2008 SP2, changed the registry settings as described but still my Server application doesn't use TLS 1.2.Is there something else I should be changing? Once the patch is installed and the server rebooted try using this tool rather than setting reg keys manually (as this is fiddly and prone to errors): sure you reboot after making any TLS config changes though I enabled TLS 1.1 and TLS 1.2 in the registry by hand, but it didn't work. I tried the IIS Crypto tool, but I don't see TLS 1.1 and TLS 1.2 listed. We had issues where TLS 1.1/1.2 wasn't working even after doing everything mentioned above. We added additional registry keys (step 4) and it started working! I had to do:1. Discover that Windows 2008 (not R2) is now supported: . Install all windows updates. Reboot.3a. FAIL: IIS Crypto doesn't list TLS 1.2, so I need to manually create the keys...3b. FAIL: Manually create keys by following instructions for enabling TLS 1.2... . PROGRESS: Microsoft's instructions suck! These were much better: this point, IE still wouldn't connect to a URL that only allows TLS 1.2. This was the magic step:4. Update to enable TLS 1.1 and TLS 1.2 as a default secure protocols in WinHTTP in Windows is now able to connect to my URL that only allows TLS 1.2! My .NET 4.x client application using WCF would still not connect over TLS 1.2, this fix for this 5. Registry update...HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319: SchUseStrongCrypto to DWORD 16. Apply missing .NET 4.x updates...and SUCCESS! What version of IE are you using on 2008 SP2? I am using IE 9 using your instructions and it's still not working. Chrome on the same server works fine. I used the IIS Crypto tool and it created the registry keys. But, on TLS 1.0, 1.1 and 1.2 for Client and Server it set the Enabled dword to hexadecimal ffffffff and decimal 4294967295. Isn't it supposed to be 0 or 1? Windows Vista does not properly support TLS 1.1 and TLS 1.2 https connections. This can cause issues not just with the built in Internet Explorer web browser, but also with any apps that rely on the Windows networking components when connecting to servers configured to only accept TLS 1.1+ connections. These steps will allow you to enable TLS 1.1 and 1.2 on Windows Vista using the KB4056564 update patch for Windows Server 2008 and are an updated version of the steps outlined in this forum post on MSFN.WarningsThese instructions and files are provided without warranty. Use them at your own risk. They may violate your license depending on your local laws..REG files update your Windows registry. Incorrect changes to the registry may damage Windows or other installed software. Be sure you know what a given .REG file contains before merging it into the registry.These instructions and files are unsupported, please do not contact me with questions on their use.Installation and update directionsOpen Windows Update and ensure you have applied all Critical and Important updates for Windows Vista through when it was end of lifed.Visit the KB4056564 page in the Microsoft Update CatalogClick the Download button next to either "2018-05 Security Update for Windows Server 2008 for x86-based Systems (KB4056564)" or "2018-05 Security Update for Windows Server 2008 for x64-based Systems (KB4056564)" depending on whether your copy of Windows Vista is 32-bit or 64-bit. If you are unsure which your version of Windows Vista is, you can right click on My Computer in Windows Explorer and it will show in the details.Run the windows6.0-kb4056564-v2-x86_1cf1b27424b4017e5f1341d88b42c463a62e1ac8.msu (or x64) file that is downloaded and follow along the prompts to install the patch.Restart your computerDownload this .reg key: vista-tls-1.1-1.2-update.reg (Updated 2021-01-05 to support Vista 64-bit)Double click the .reg key and allow it to merge into the Windows registry (For the curious, this will remove version-specific information from the CRYPTO\TLS1.1 and CRYPTO\TLS1.2 keys allowing the options to display in Internet Options)Open up Internet Options from your Control Panel or from within Internet Explorer by clicking the gear icon and selecting Internet OptionsClick the Advanced tabScroll all the way down and check the boxes next to TLS 1.1 and TLS 1.2Click OKYou should now be able to connect to TLS 1.1 and TLS 1.2 secured websites. Note that Internet Explorer will still have issues displaying most modern websites and most are no longer tested for compatibility with Internet Explorer 9.Mozilla Firefox 52.9.0 ESRThe last version of Firefox to support Windows Vista is the 52.9.0 ESR release. Download the 32-bit installer. Note that it has known security issues at this point.K-MeleonK-Meleon uses the older Firefox rendering engine and is still compatible with Windows Vista. Head to the K-Meleon homepage and then click through to the forum thread with the latest Goanna fork build. To enable TLS 1.1 and/or TLS 1.2 protocols on web browsers, see the list below. Microsoft Internet Explorer Open Internet Explorer From the menu bar, click Tools > Internet Options > Advanced tab Scroll down to Security category, manually check the option box for Use TLS 1.1 and Use TLS 1.2   Click OK Close your browser and restart Internet Explorer Google Chrome Open Google Chrome Click Alt F and select Settings Scroll down and select Show advanced settings... Scroll down to the Network section and click on Change proxy settings... Select the Advanced tab Scroll down to Security category, manually check the option box for Use TLS 1.1 and Use TLS 1.2   Click OK Close your browser and restart Google Chrome Mozilla Firefox Open Firefox In the address bar, type about:config and press Enter In the Search field, enter tls. Find and double-click the entry for security.tls.version.max Set the integer value to 3 to force protocol of TLS 1.2 Click OK Close your browser and restart Mozilla Firefox Opera Open Opera Click Ctrl plus F12 Scroll down to the Network section and click on Change proxy settings... Select the Advanced tab Scroll down to Security category, manually check the option box for Use TLS 1.1 and Use TLS 1.2   Click OK Close your browser and restart Opera Apple Safari There are no options for enabling SSL protocols. If you are using Safari version 7 or greater, TLS 1.1 and TLS 1.2 are automatically enabled. Most websites intended for a general audience will want to select TLS versions based on security and browser compatibility. If you have guarantees that the clients used to connect to your website will be reasonably up to date, you may be able to depend on TLS1.3 alone. The optimal configuration for your website will depend on a number of parameters, and the configuration will need to change over time as support for stronger protocols and ciphers is added to browsers. Likewise, you will want to disable less secure protocols and ciphers as vulnerabilities are discovered or they become disused. Security Considerations Newer versions of TLS provide fixes for known vulnerabilities in older TLS versions. Specific vulnerabilities in TLS1.1 have already been discussed. For instance, a countermeasure to the Lucky13 attack is to use AEAD ciphers which became available in TLS1.2. TLS1.3 removes support for a number of weaker ciphers and hash algorithms while adding stronger ciphers. Compatibility Considerations At this time, TLS1.3 is supported by the browsers of ~81% of global users, which is likely not enough to rely solely on TLS1.3. You will likely want to additionally enable support for TLS1.2, which is currently supported by over 97% of global users. Depending on the specific demographics and requirements of your websites, you may want to disable support for TLS1.0 and TLS1.1 at this time (as many websites have already done). Client Support According to Can I Use, current global support as a percentage of users (as of January 2020): | Version | Global Support | | ------- | ------------- | | TLS 1.0 | virtually all | | TLS 1.1 | 97.43% | | TLS 1.2 | 97.35% | | TLS 1.3 | 81.08% | Most popular browsers are phasing out support of TLS1.0 and TLS1.1 in 2020. (Source) Server Support Server support, as measured by Qualys SSL Labs (as of December 3, 2019): | Version | Server Support | | ------- | ------------- | | TLS 1.0 | 63.4% | | TLS 1.1 | 73.7% | | TLS 1.2 | 96.2% | | TLS 1.3 | 17.0% | Many websites have already disabled support for TLS1.0 and TLS1.1. Some users with outdated clients that do not support TLS1.2 are likely receiving error messages when viewing such websites. Other Notes Newer TLS versions also add features that you may want to take advantage of. TLS1.2: HTTP/2: TLS1.2 is the minimum TLS version for HTTP/2, which provides additional features to speed up page load time. TLS1.3: Faster handshakes: TLS1.3 will reduce latency in establishing a secure connection. Forward Secrecy: In TLS1.3, all ciphers support ephemeral key exchange. This helps to maintain security of previous connections even if your server is compromised (or, in this case, your CDN is compromised). For optimal security, you will want to tune additional parameters for your websites. Qualys SSL Labs can help you discover and tune these settings for additional security. To name a few, consider configuring HSTS, downgrade prevention via TLS Fallback SCSV, and forward secrecy. You may not be able to control all of these settings via your CDN - some may need to be configured on your servers. Also, do not neglect the TLS configuration of your own servers as your CDN will establish an independent TLS connection to your servers. WildTangent uses Internet Explorer to display game details and app content. TLS is the latest standard of security that ensures your information stays safe, but older versions of Internet Explorer may not support this. You'll want to first update your version of Internet Explorer to Internet Explorer 11. You can download IE 11 from Microsoft here: For more information about TLS Updates from Microsoft: If you already have Internet Explorer 11 installed, then all you need to do ensure TLS 1.1 and 1.2 are enabled. To check these settings: Go to Tools and select Internet Options Select the Advanced tab in Internet Options Enable(check) TLS 1.1, TLS 1.2 and also disable (uncheck) SSL 3.0 for additional security Click on Apply and OK to complete the procedure Skip to content In the Windows start menu, type regedit and open it We strongly recommend backing up your current registry before making any changes. This can be done by clicking File, then Export and the save the backup at a safe location Go to the following path: Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols Right-click on the empty space in the pane on the right side and choose New > Key Name the new key TLS 1.2 Right-click the empty space on the right side again and add two new keys named Client and Server Select the Client key, right-click on the right side, and select New -> DWORD (32-bit) Value Name the DWORD DisabledByDefault, right-click on it, and select Modify. The base should be set to Hexadecimal and the value set to 0: Create a new DWORD with the name Enabled. The base should be set to Hexadecimal and the value set to 1 Repeat the process for the Server key, creating the same DWORDS with the same values Exit the registry and reboot your server If anything goes wrong, you can revert to your initial registry settings by double-clicking your registry backup file created in step 2. You can check if your configuration is correct by looking up your site in our SSL Labs checker: In the Configuration section, you can see the protocols enabled for your site. You can check which protocols are supported on a different version of Windows by following this link: ��schannel-ssp-