Enable TLS 1.2 on Windows 7 Pro

After updating to Greencube Terminal 1.0.0.85 (GC-T), my call on the map at https://oscarwatch.org/greencube/ was still showing up red as a “Transmitting station” and not as a “Greencube Terminal User.”

My call being on the map was from others reporting hearing my signals but in order for it to turn green my station has to also report data and apparently was not doing this. Reviewing a packet capture taken while starting GC-T I noticed the lotw.arrl.com and other connection attempts on start were failing due to protocol errors.

Windows 7 is end of life and by default uses only TLS1.0. As of 2018 the ARRL disabled support for TLS1.0 and this prevents LoTW data, along with other API’s being used by GC-T, from working as expected.

Check if TLS 1.1 and 1.2 are available to turn on by going to

Control Panel > Internet Options > Advanced (tab)

Near the bottom of the Settings window you may have the ability to simply check TLS 1.1 and TLS 1.2. If you can do this check them and reboot. In my case they did not exist.

1) Run Windows Update and reboot until it shows no additional updates required. This wasn’t an easy process as a few of the updates did not download and install from Windows Updates automatically. Follow the process outlined at this Microsoft support link to manually download and install them.

https://support.microsoft.com/en-us/topic/how-to-download-a-windows-update-manually-9f939f2d-c136-8533-cf83-39292c44bffa

Copy the Kbxxxxxx ID that’s failing, search for it on the Update Catalog site, download and install.

2) Download and manually install update KB3140245 from Microsoft Update Catalog

https://www.catalog.update.microsoft.com/search.aspx?q=kb3140245

3) Download and install MicrosoftEasyFix51044.msi

https://download.microsoft.com/download/0/6/5/0658B1A7-6D2E-474F-BC2C-D69E5B9E9A68/MicrosoftEasyFix51044.msi

4) Restart computer

5) Manually add keys to the windows registry to force TLS1.2 to become a default option.

This step requires using regedit.exe to make changes to the windows registry. Using this tool is outside the scope of this document and if you're not sure how to add keys or don't feel comfortable doing this be advised you could render your machine inoperable if things are not done properly. If you're concerned be sure to have proper backups before making changes.

Using the search bar (START > Search programs and files) search for "**regedit**", click it to run and click **Yes** to allow it to make changes to the computer.

Add the following eight DWORD's with HEX values. Before adding the DWORD's you may need to add **TLS 1.1\Client** and **TLS 1.2\Client** keys, if they do not exist. They did not exist on my system and had to be created.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Client

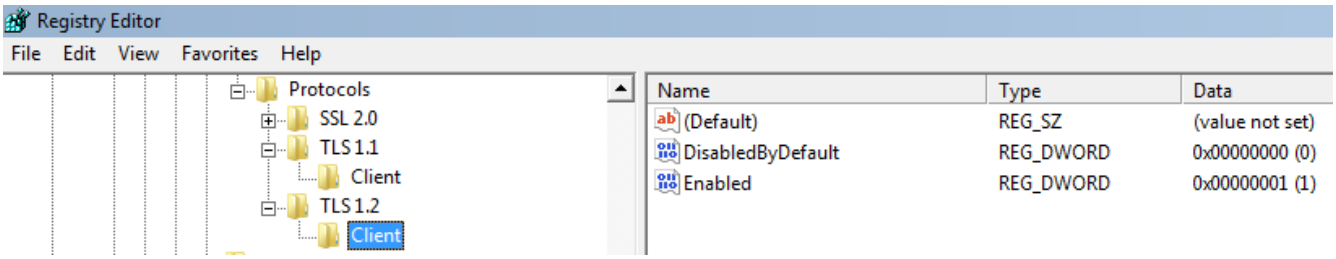
DWORD name: DisabledByDefault
DWORD value: 0

DWORD name: Enabled
DWORD value: 1

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client

DWORD name: DisabledByDefault
DWORD value: 0

DWORD name: Enabled
DWORD value: 1



HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319

DWORD name: SystemDefaultTlsVersions

DWORD value: 1

DWORD name: SchUseStrongCrypto

DWORD value: 1

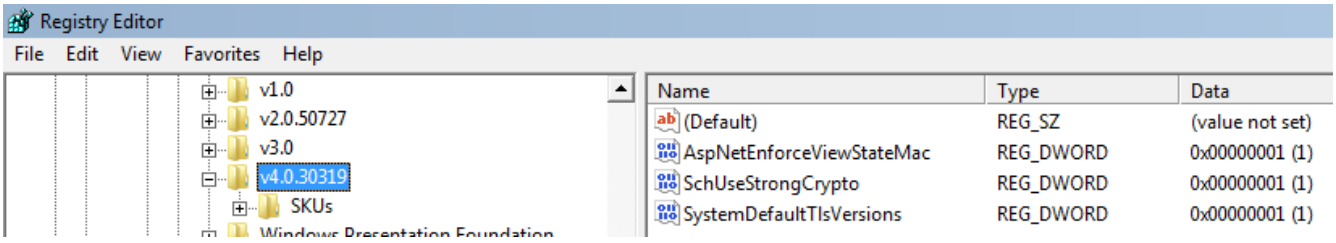
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\ v4.0.30319

DWORD name: SystemDefaultTlsVersions

DWORD value: 1

DWORD name: SchUseStrongCrypto

DWORD value: 1



6) Restart computer

7) Check that TLS 1.1 and TLS 1.2 are now checked in Internet Properties

Control Panel > Internet Options > Advanced (tab)