DCB, Inc.
2949 CR 1000 E
Dewey, Illinois
61840

217.897.6600
800.432.2638 Toll Free
217.897.1331 Fax
www.dcbnet.com

DCB TLS Version Change Issues

4/11/2022

Microsoft recently pushed out a patch that remove all support for TLS v1.0 and v1.1. The result is that customers running older firmware on their ET or UT device will be unable to start a web session with the device for device management and configuration. The messages report that there is no common security protocol or encryption algorithm.

The problem is likely due to the TLS version. Older firmware only supported TLS 1.0 and 1.1. In 2018, we released new firmware that added support for TLS 1.2 and removed TLS 1.0. Web browsers are dropping support for TLS 1.0 and apparently 1.1. If the unit in question is running old firmware, then you will see the error message indicating that there is no common security protocol or encryption algorithm.
The solution is to upgrade the firmware. The problem is that if you can not web browse to the unit, you can't upgrade the firmware.

While the best option is to always use the latest firmware, if you didn't upgrade your unit's firmware before older versions of TLS were deprecated, the best viable option going forward is to find an old version of your favorite web browser. Use that to update the firmware to the latest version. Or, you can use version 99.01 of Firefox and enable TLS 1.x, which is still there, but disabled. Instructions are below, but be aware that Firefox may totally remove this option in the future.

Firefox:
Within the Firefox browser, make the following changes to the about:config section:
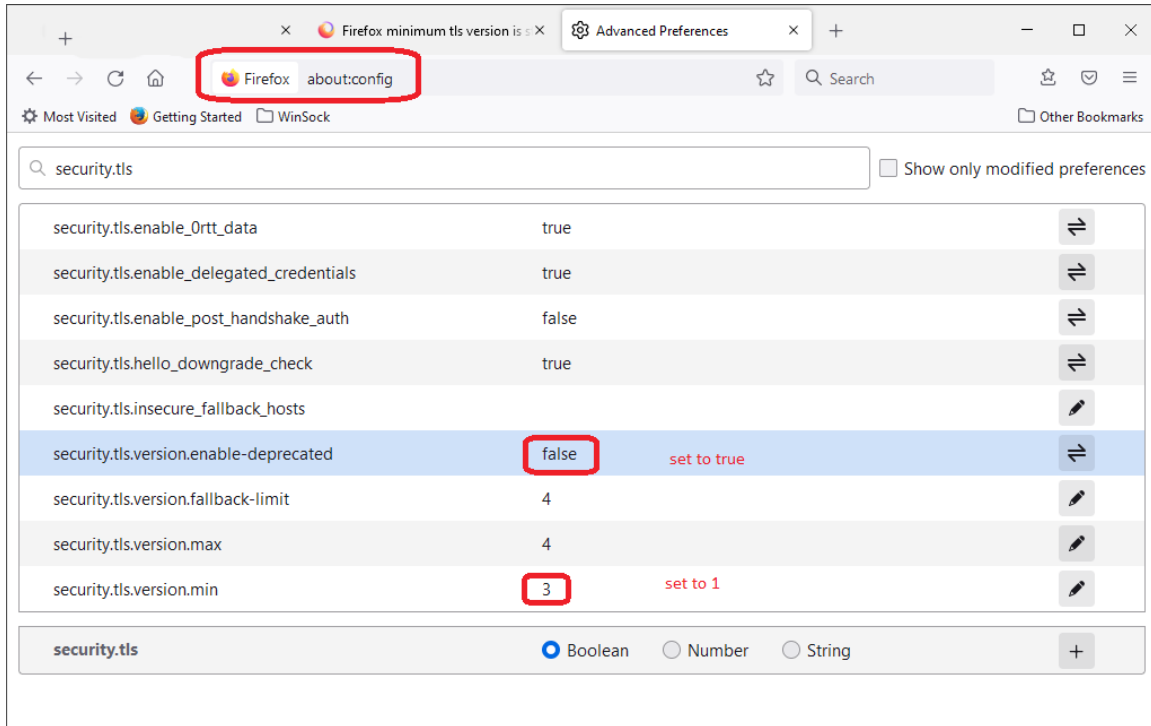
This should let you connect. After you upgrade the firmware, it is recommended to repeat the above process and disable TLS 1.0 and 1.1.

If you have any problem upgrading the firmware or connecting to the units, please email or call for support.