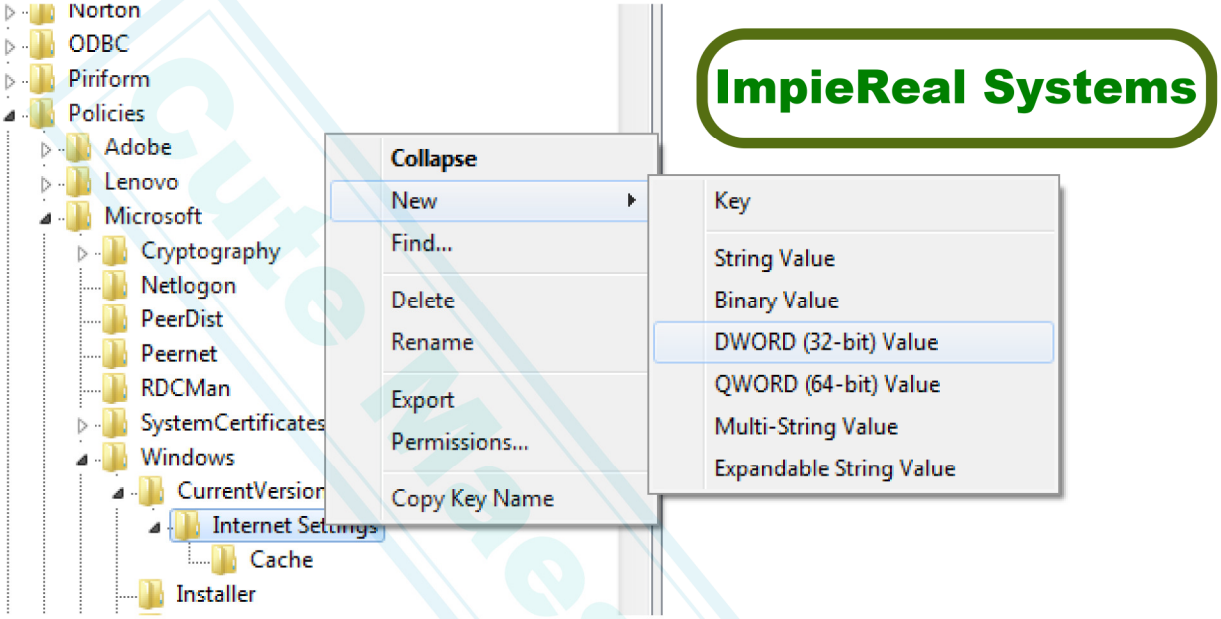
Internet Explorer SSL & TLS Options Advanced Settings Grayed Out

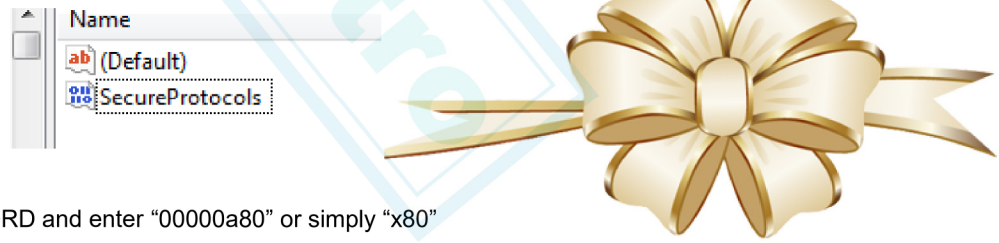
- Log on the same machine as a different user and check Internet Explorer settings
- For Windows domain machines, ask another end user to log on to the domain and check his or her Internet Explorer settings. If all machines seem to be grayed out, there may be Windows security features or Group Policy Objects enforced. Please skip to the bottom.
- Run an antivirus
- Check registry settings

  Just as an example, the following registry setting will disable TLS and SSL options on Internet Explorer

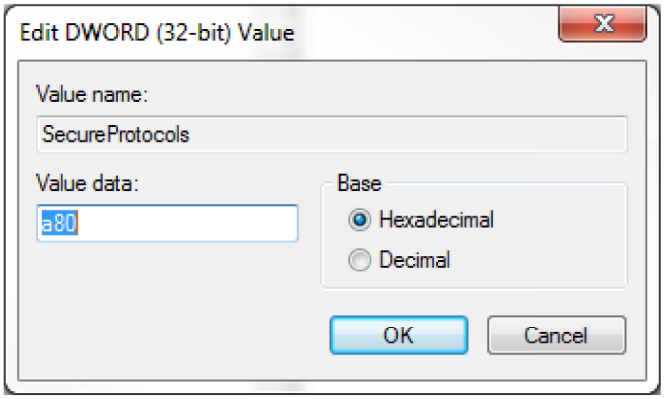
cmd > regedit > HKEY_LOCAL_MACHINE > Software > Policies > Microsoft > Windows > CurrentVersion > Internet Settings > Right click on “Internet Settings “> New > DWORD



> Rename it “SecureProtocols”



> Double click on the DWORD and enter “00000a80” or simply “x80”



This is an example of an attack. Simply delete such corruption from your registry.

Group Policy Objects

- If you are connecting to the network *wirelessly*, try a *wired* connection because Group Policy settings for IE may be bundled with the wireless rules.
- Comb through Group Policy settings
  Just as illustration, this is how the Administrator will *turn off all* SSL and TLS tunneling or encryption via Internet Explorer on Windows 2008 R2. This is the setting to look for in case the “Advanced” tab has SSL & TLS grayed out.

  > [New Group Policy Object] > Edit > User Configuration > Policies > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Advanced Page > “Turn off Encryption Support “

  Important to note that SSL 2.0 is always disabled by default because it is outdated; in fact, enabling SSL 2.0 impairs the performance & functioning of TLS 1.0.

ImpieReal Systems