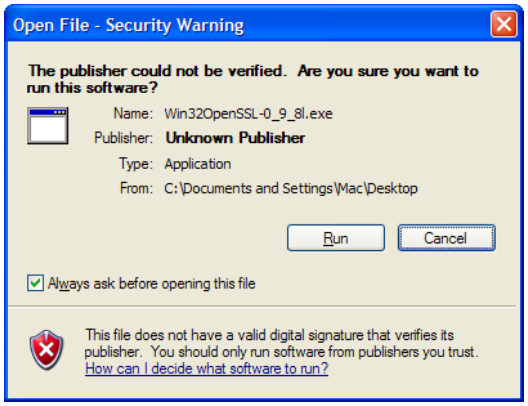
Test Sockets Using Secure Mode

When using secure mode in the DeviceMaster, it is necessary to use a Secure Sockets Layer (SSL) application. Telnet and Secure Shell (SSH) will not transfer data across the socket connections to/from serial ports.

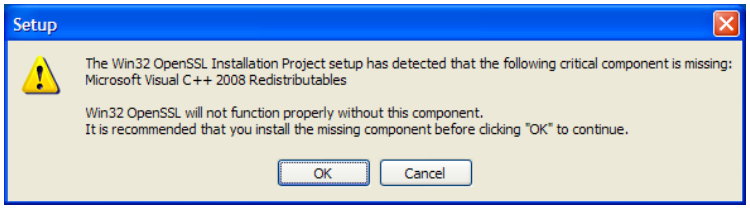
As a result of this, a SSL application will be required. This document will discuss the usage of an open source SSL application.

Download openssl for windows at http://www.slproweb.com/products/Win32OpenSSL.html selecting the appropriate version for your environment. For 32 bit windows select Win32 OpenSSL v0.9.8l. For 64 bit windows select Win64 OpenSSL v0.9.8l.

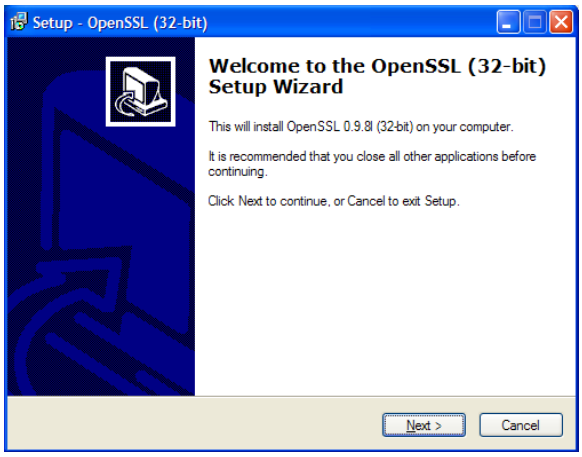
After downloading, execute the file. For this document it will be assumed that the default installation will be used and we will show the paths and instructions based on the default installation.



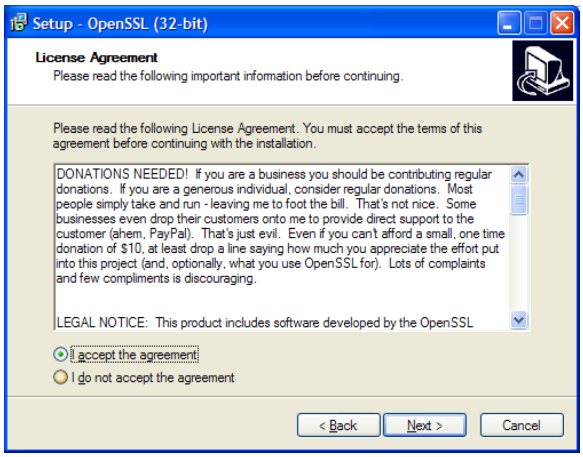
Click Run



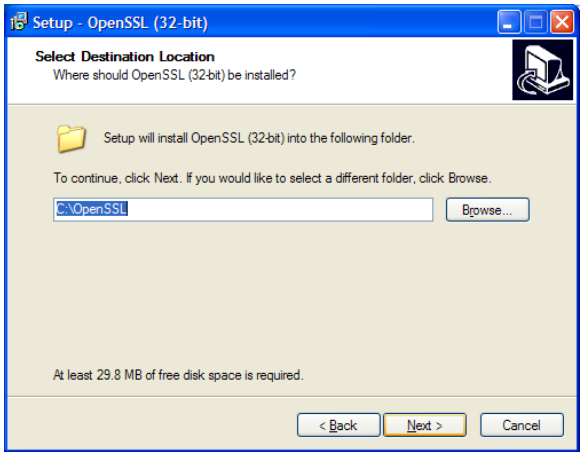
Click OK



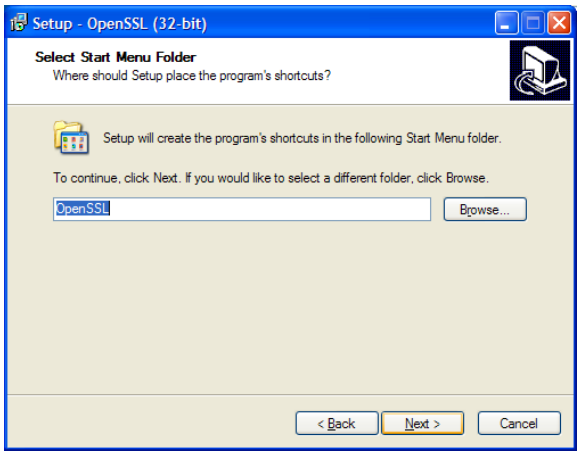
Click Next



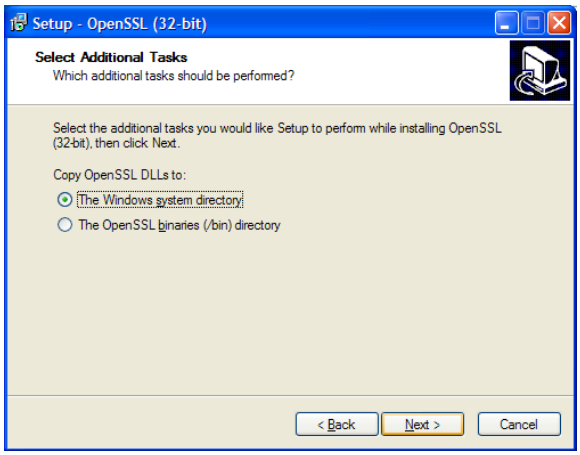
Accept the agreement and click Next



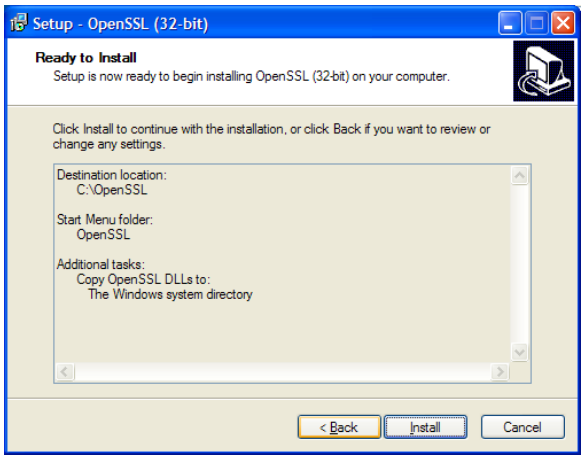
Click Next



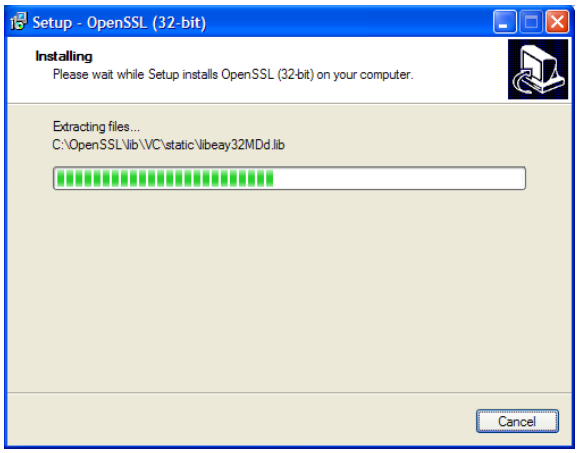
Click Next

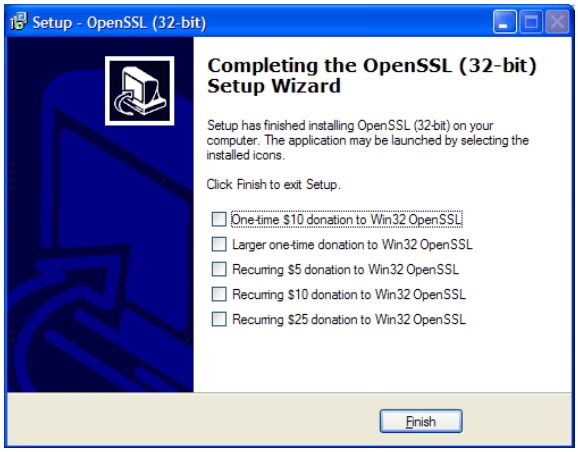


Click Next



Click Install

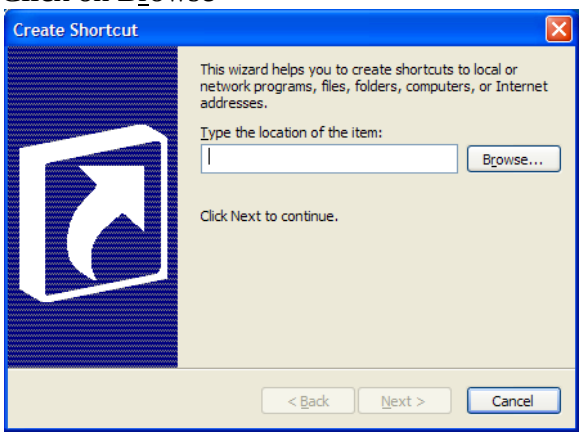




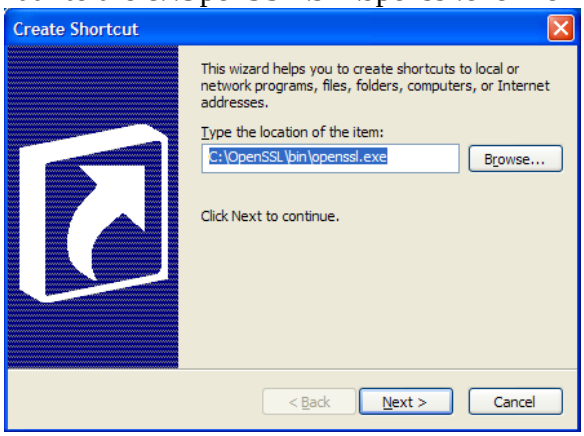
If desired, unselect and select your choice
Click Finish

Create a shortcut on the desktop.
On the desktop right-click and select New>Shortcut from the pop-up menu

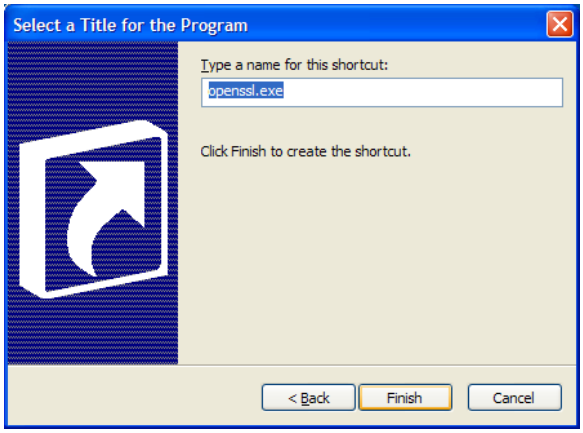
Click on Browse



Path to the c:\OpenSSL\bin\openssl.exe file



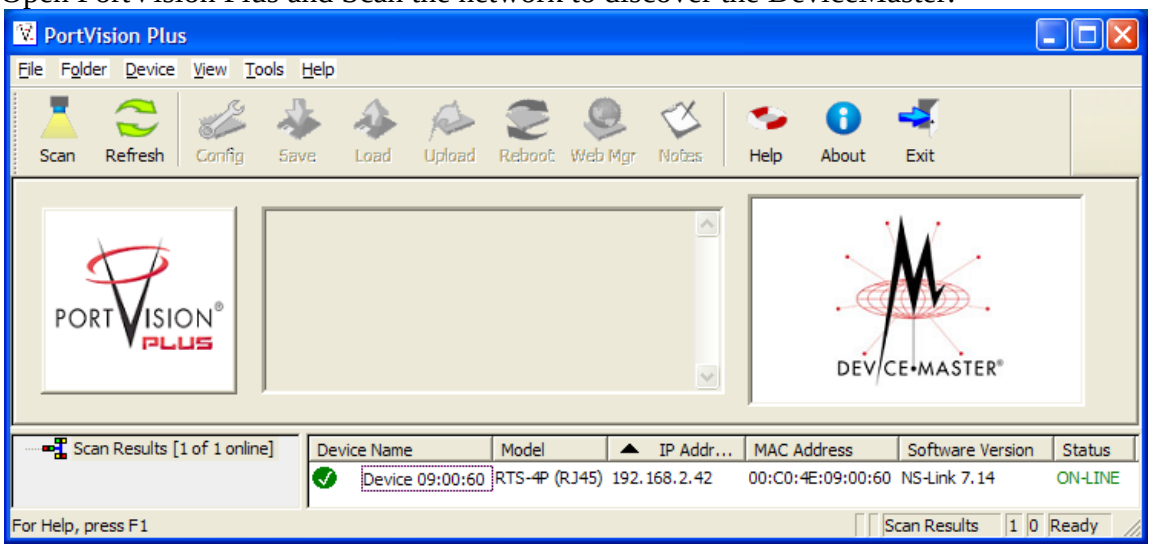
Click Next



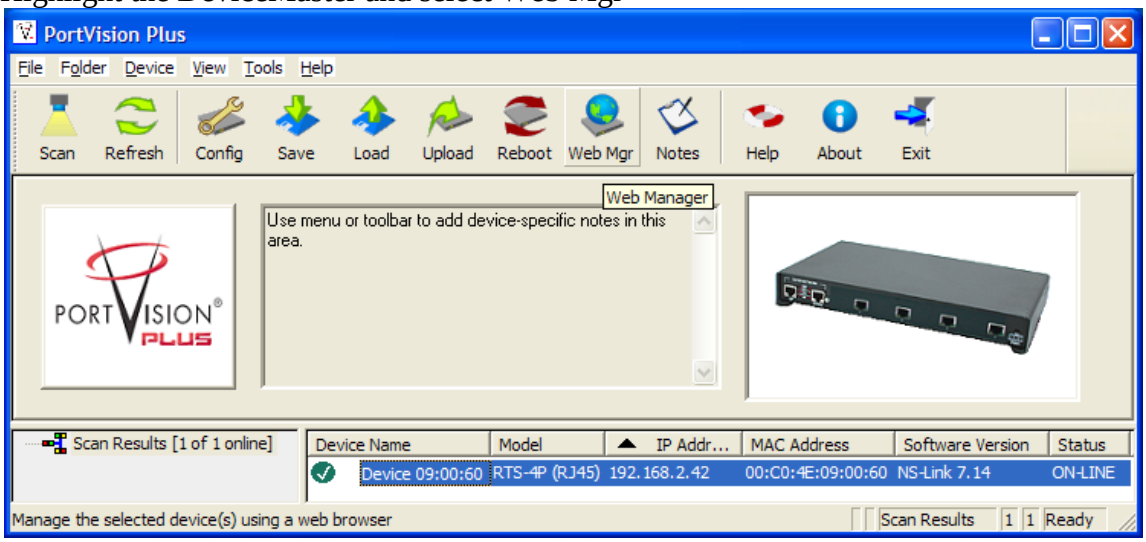
Enter a name to be displayed.
Click Finish

Configure the DeviceMaster for basic security. This document will NOT discuss The configuration or addition of Key and Certificate Management. For this example we will be using the default key in the DeviceMaster.

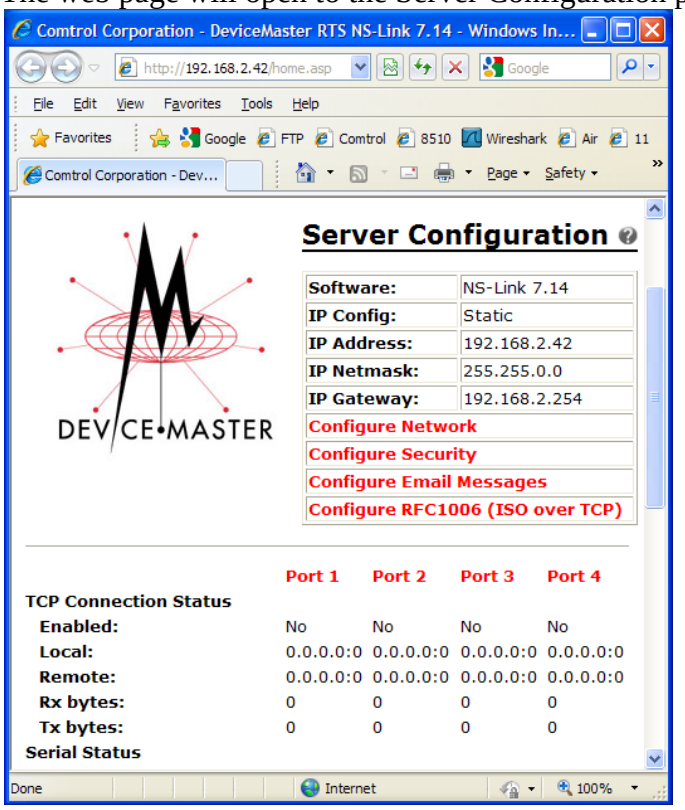
Open PortVision Plus and Scan the network to discover the DeviceMaster.



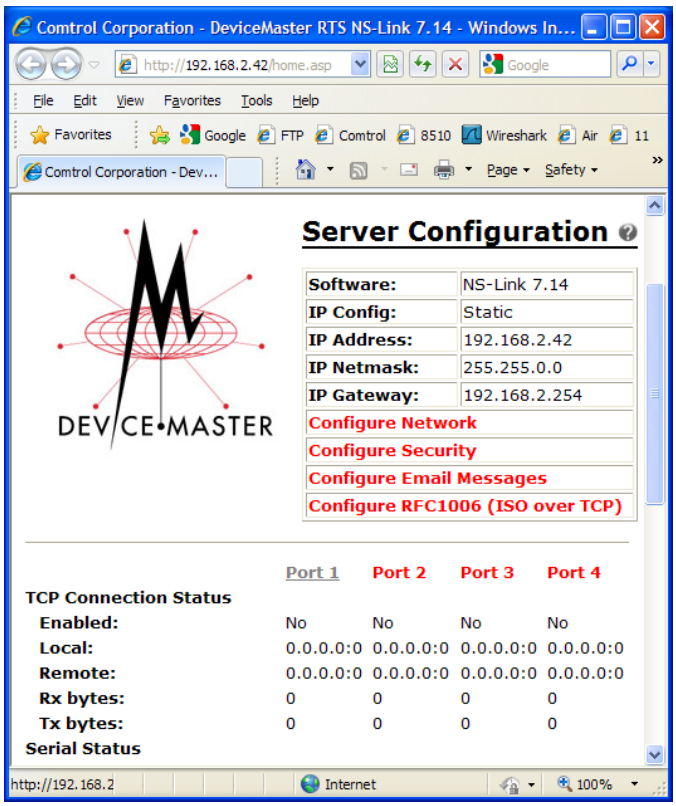
Highlight the DeviceMaster and select Web Mgr



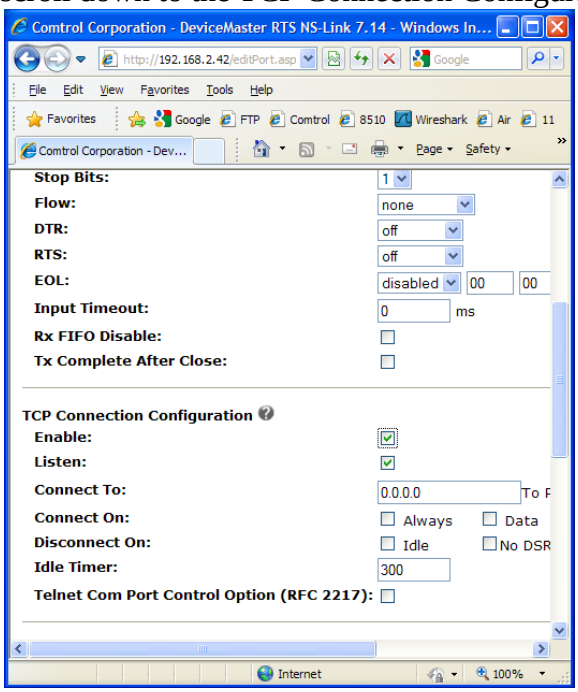
The web page will open to the Server Configuration page



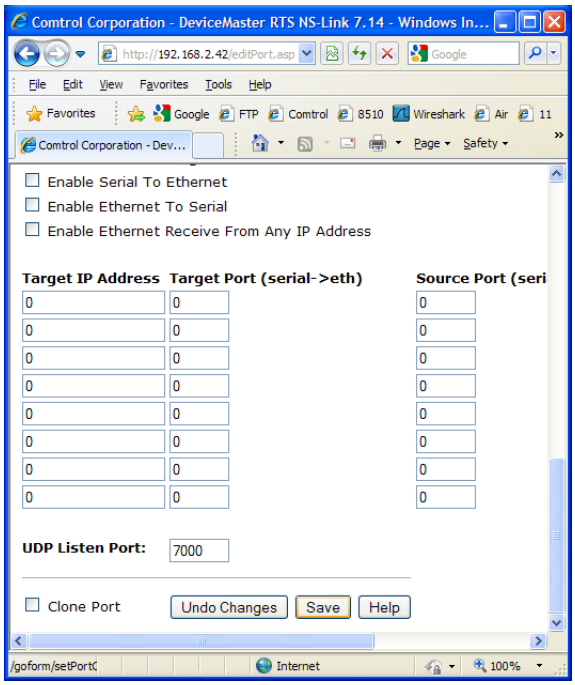
Click on Port 1



Set the serial port to the parameters you wish to use and then scroll down to the TCP Connection Configuration

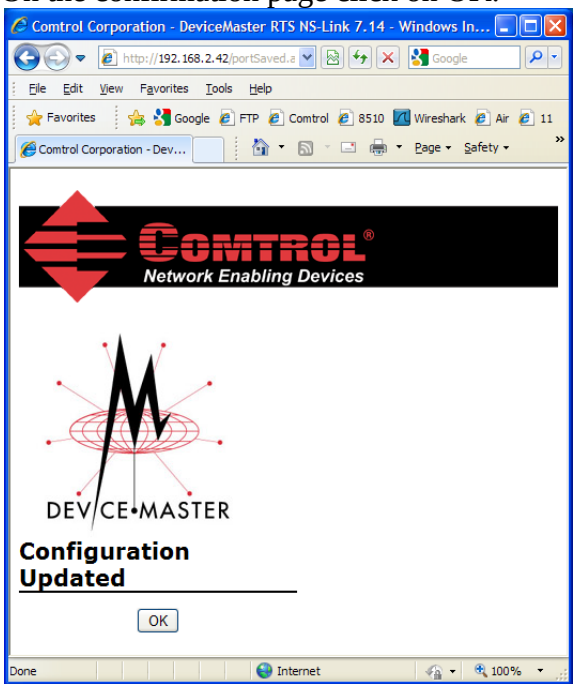


Place a checkmark in the Enable box.

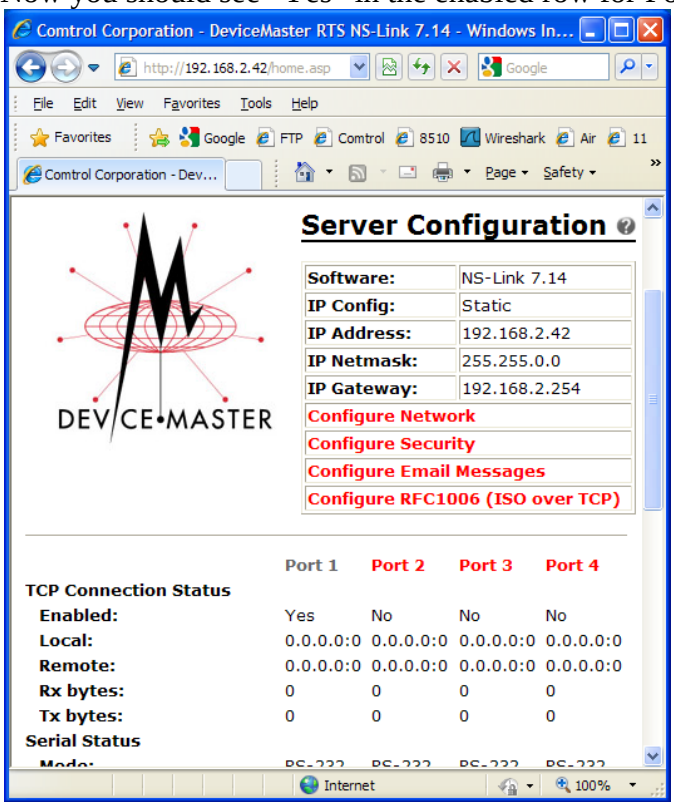


Scroll to the bottom of the page and click on Save/

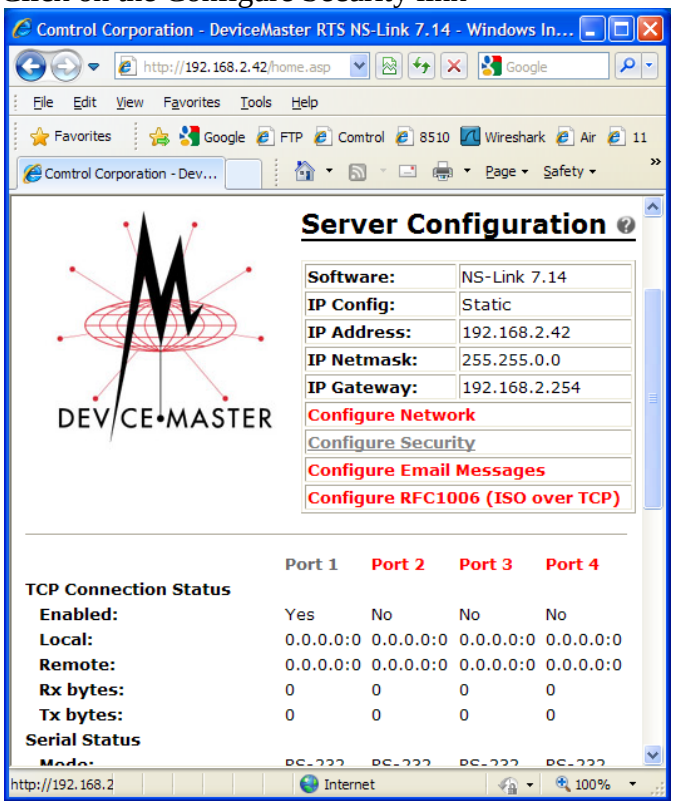
On the confirmation page click on OK.



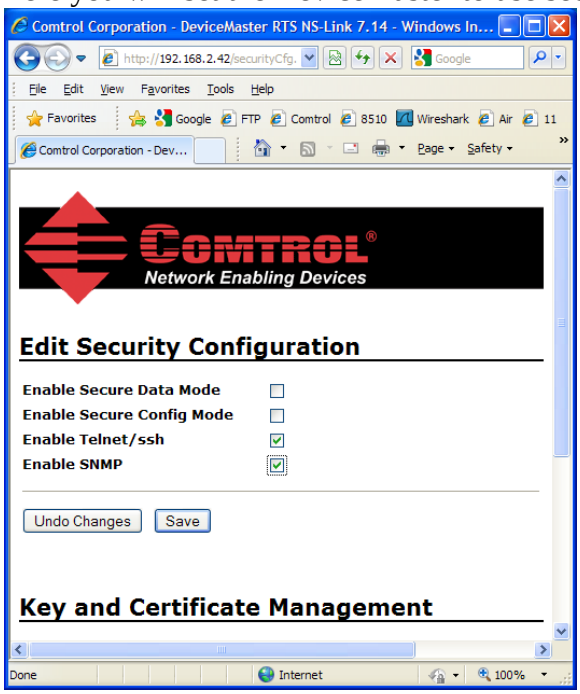
Now you should see “Yes” in the enabled row for Port 1.



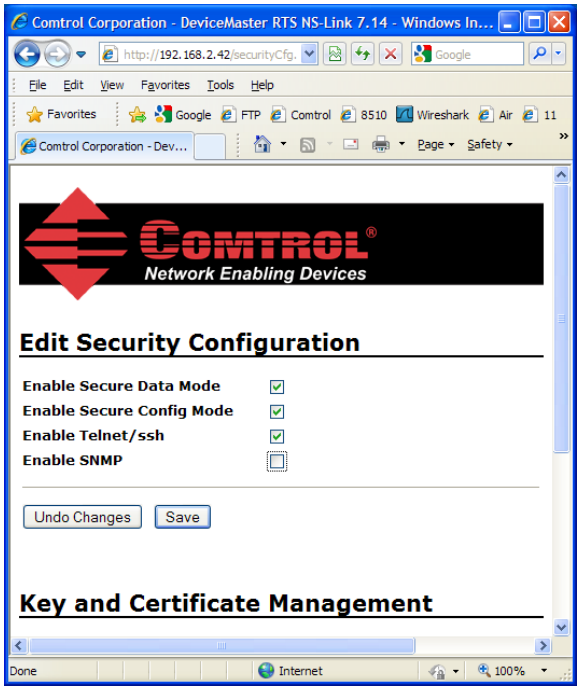
Click on the Configure Security link



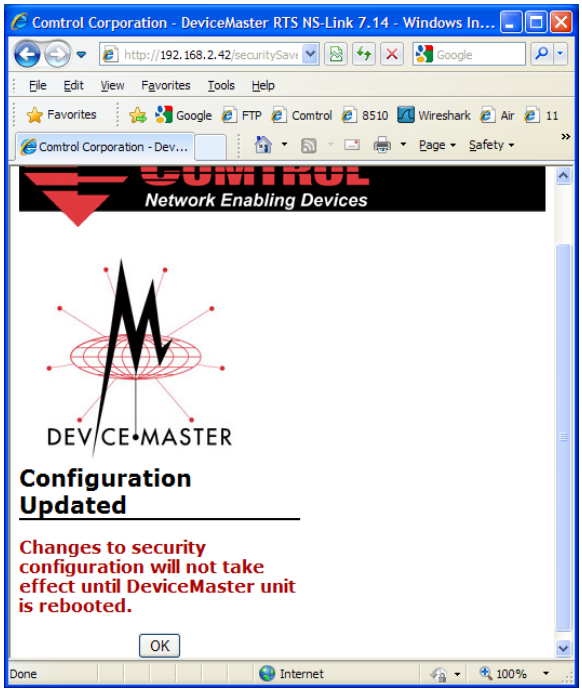
Here you will set the DeviceMaster to use secure modes.



Checkmark “Enable Secure Data Mode”
Checkmark “Enable Secure Config Mode”
Remove the checkmark on “Enable SNMP”

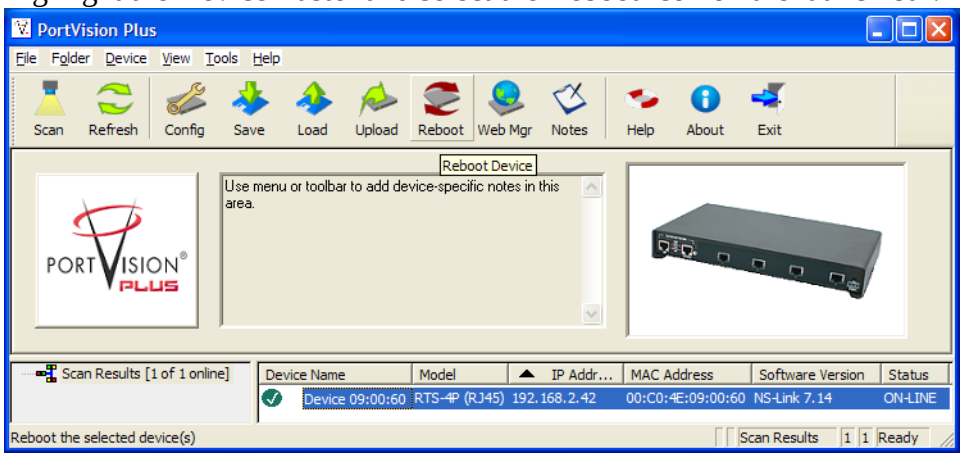


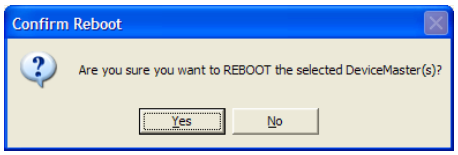
Click Save



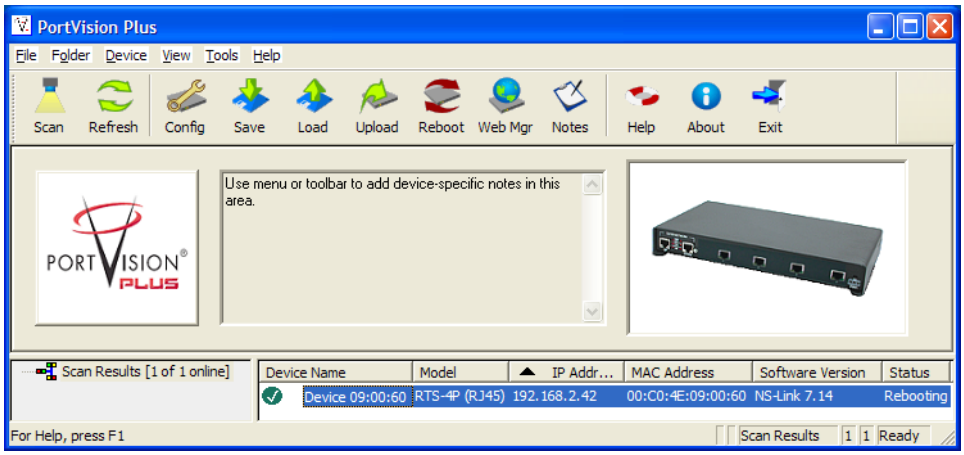
Click OK (which will return you to the previous screen).
Close the web browser.

Back to PortVision Plus.
Highlight the DeviceMaster and select the Reboot icon on the launch bar.



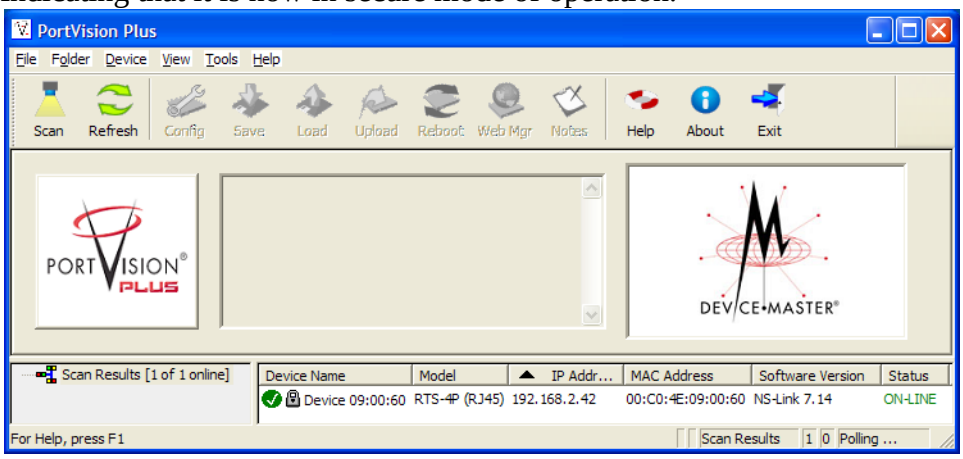


Click Yes to reboot

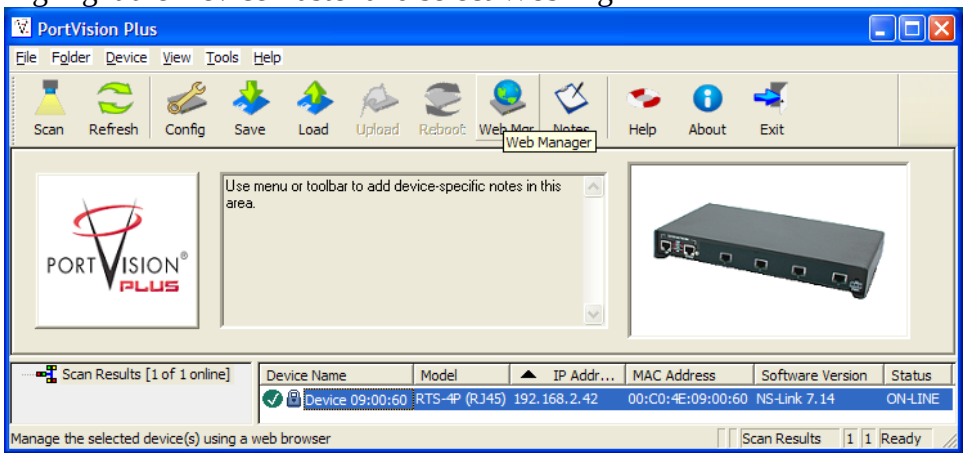


PortVision Plus will show the DeviceMaster as rebooting in the status column.

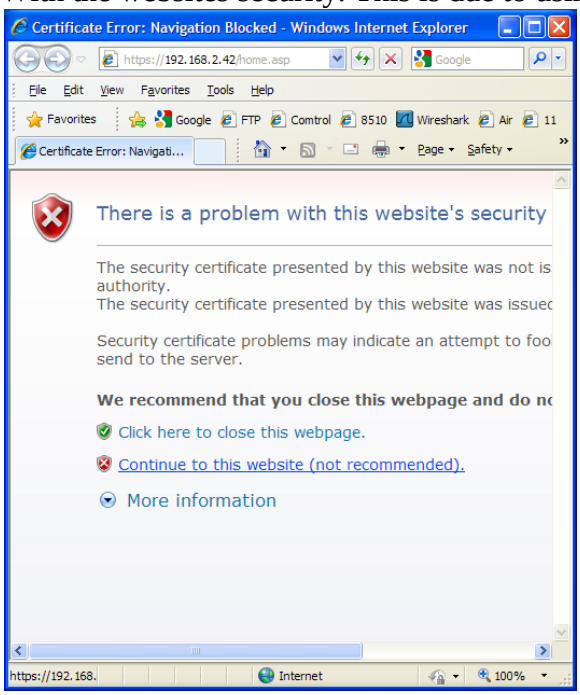
Once back on line you will now notice a “lock” next to the Device Name Indicating that it is now in secure mode of operation.



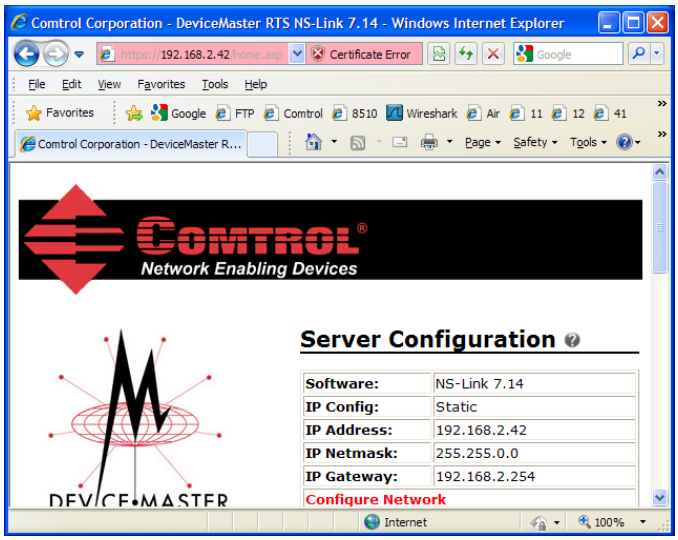
Highlight the DeviceMaster and select Web Mgr



When the browser opens you will receive a notice that there is a problem
With the websites security. This is due to using the default certificate key.

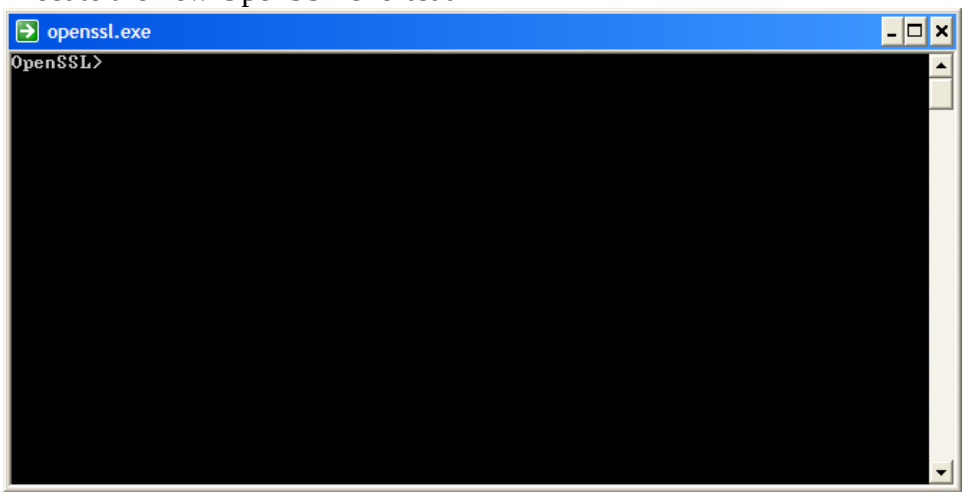


Click on “Continue to website (not recommended)”

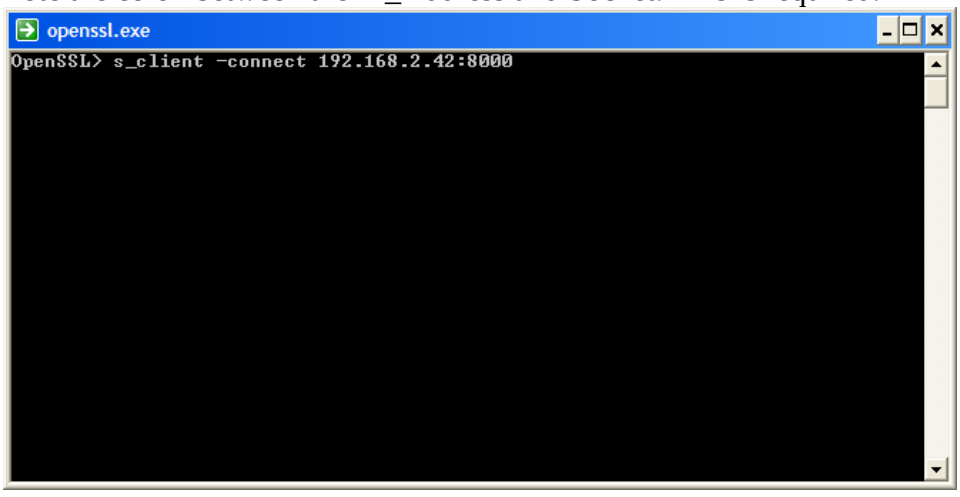


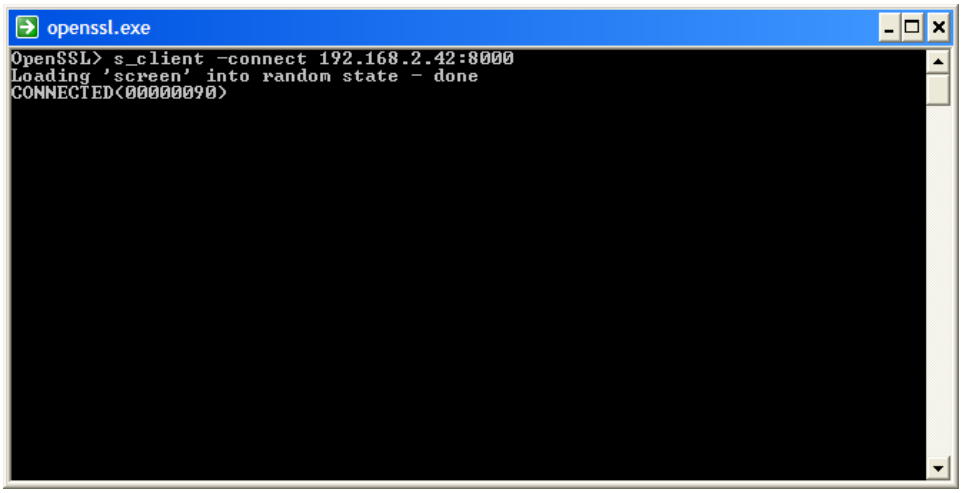
When the web page opens the URL will be in red due to the Certificate error.

Execute the new OpenSSL shortcut



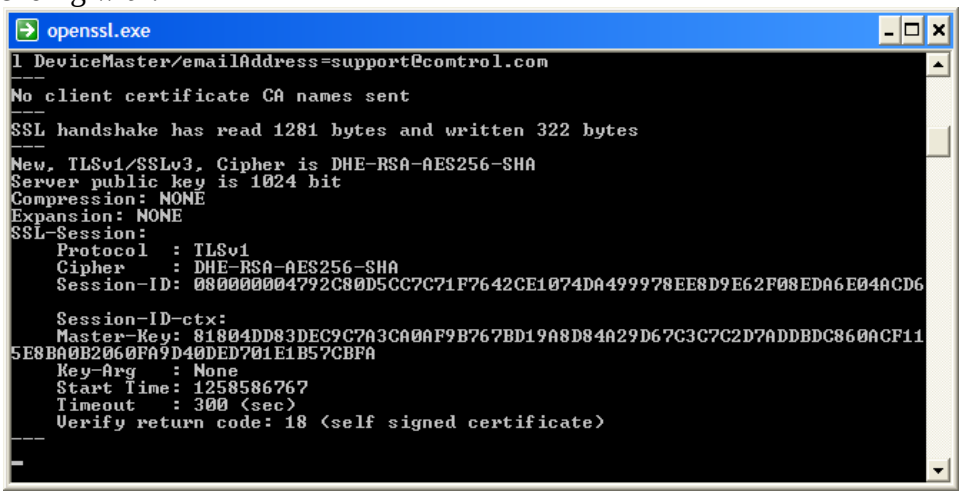
enter “s_client -connect IP_Address:Socket” without quotes and where IP_Address is replaced by the IP Address of the DeviceMaster (in this example 192.168.2.42) and Socket is replaced by the socket number assigned (in this example 8000) to the serial port, then press Enter↵
Note the colon between the IP_Address and Socket. This is required.



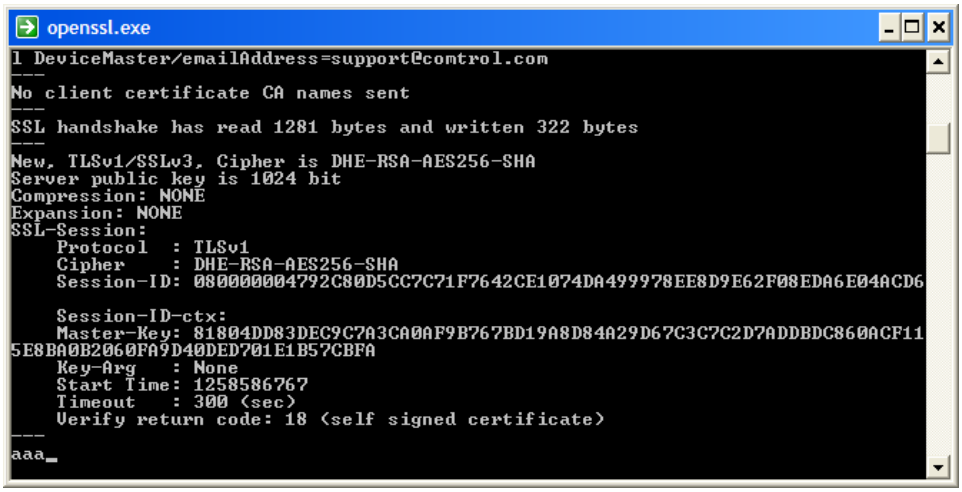


several lines will be displayed

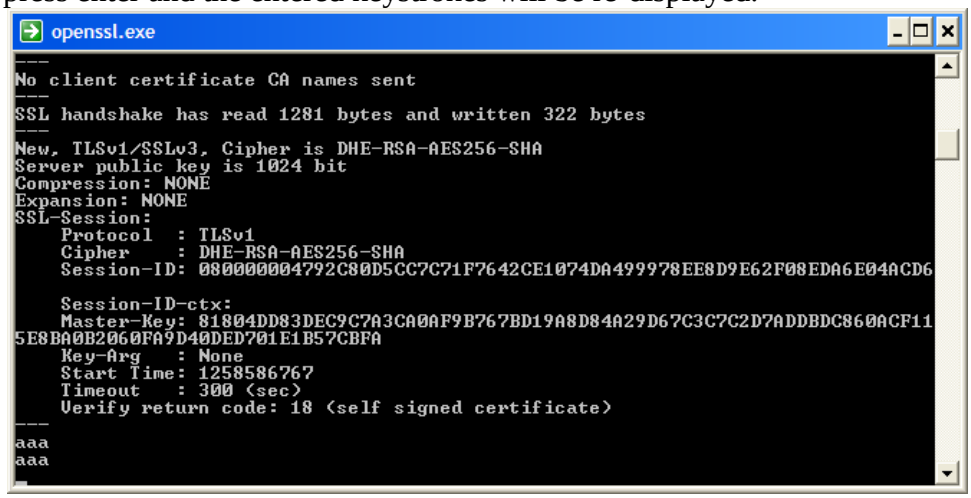
ending with:



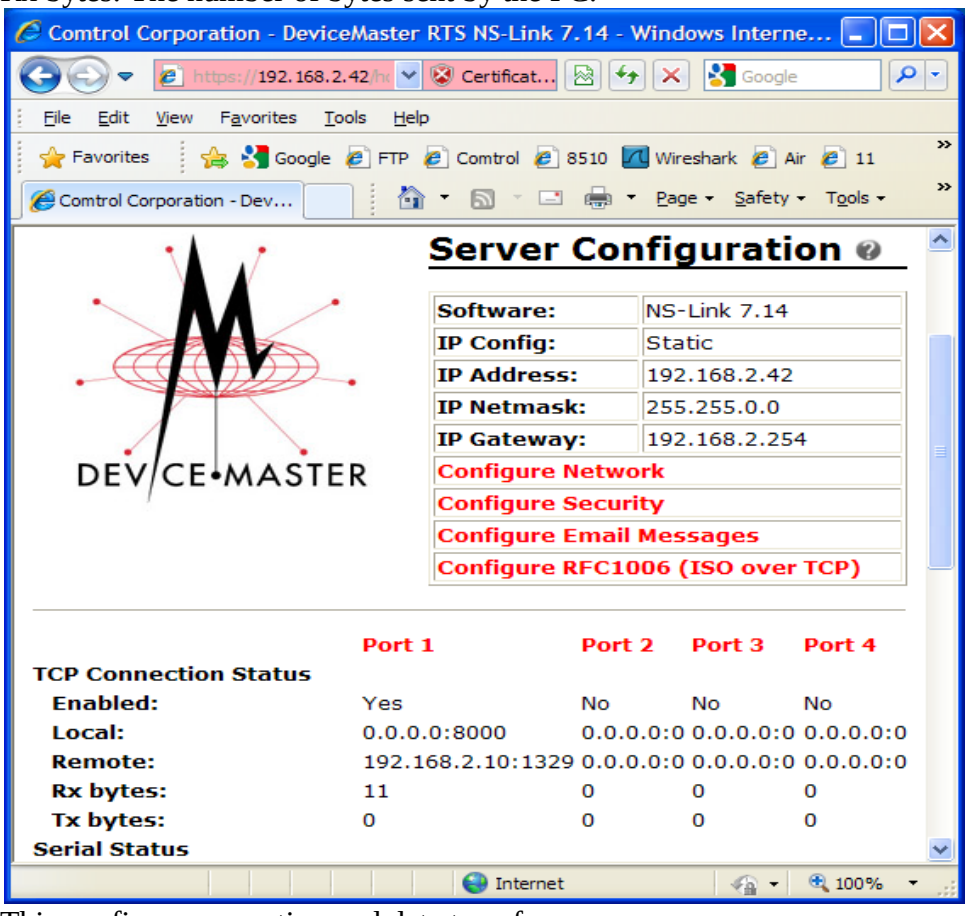
Press any keys and the keystroke should be echoed to the screen.



press enter and the entered keystrokes will be re-displayed.

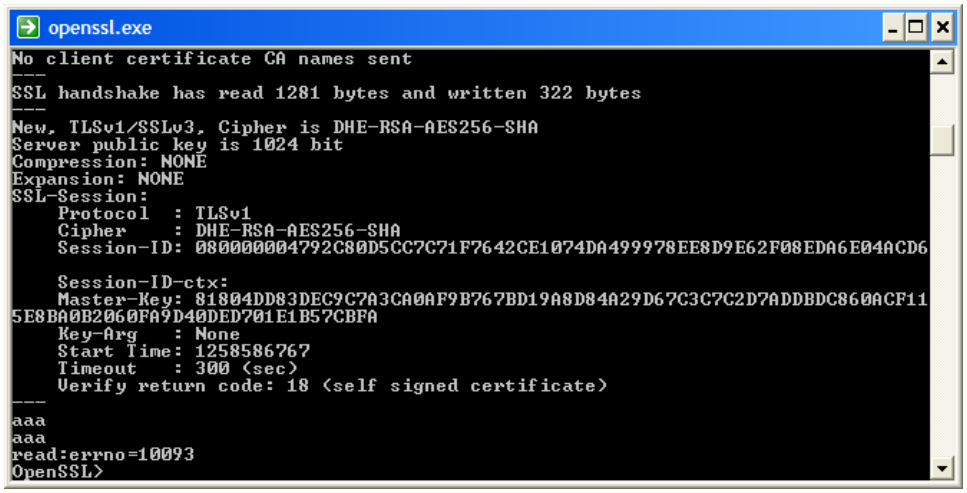


In the web page you should see that Port 1 shows:
Local: 0.0.0.0:8000
Remote: IP_Address:Socket of the connected PC
in this example 192.168.2.10:1329
Rx bytes: The number of bytes sent by the PC.



This confirms connection and data transfer.

Back to OpenSSL
Ctrl-C to disconnect



q (and Enter↵) to quit and close the window.