

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.

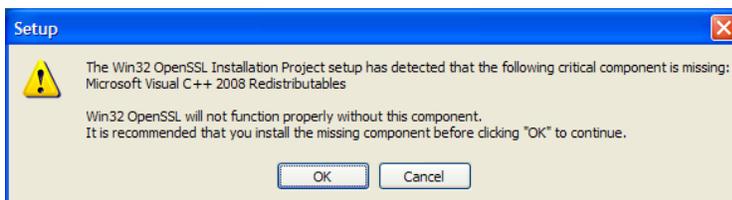
As a result of this, a SSL application will be required. This document will discuss the usage of an open source SSL application.

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.

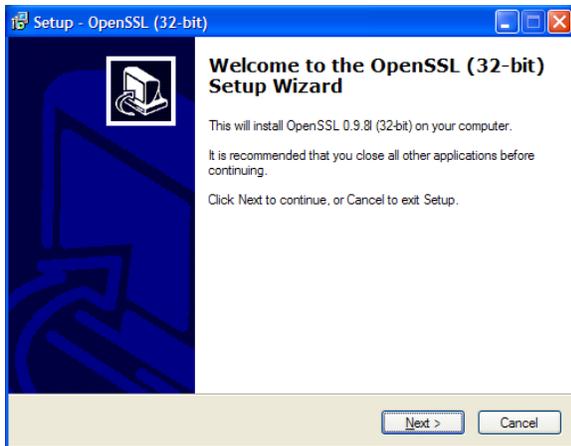
After downloading, execute the file. For this document it will be assumed that the default installation will be used and we will show the paths and instructions based on the default installation.



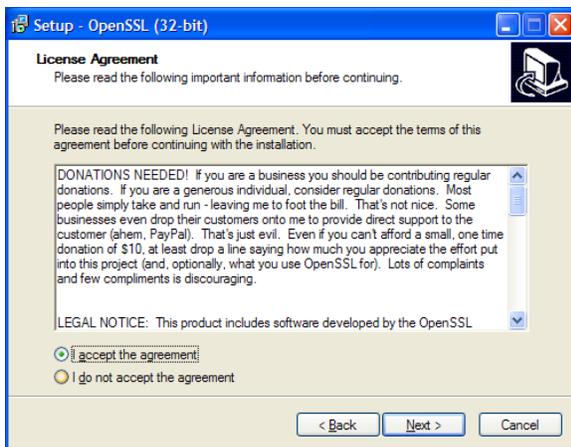
Click Run



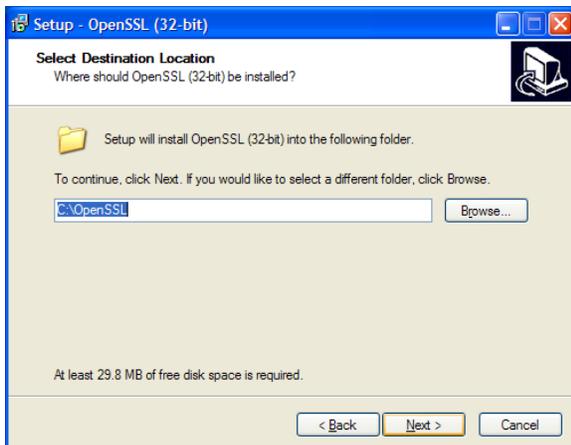
Click OK



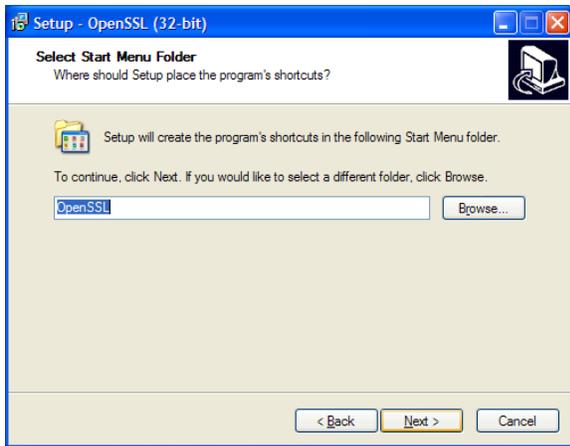
Click Next



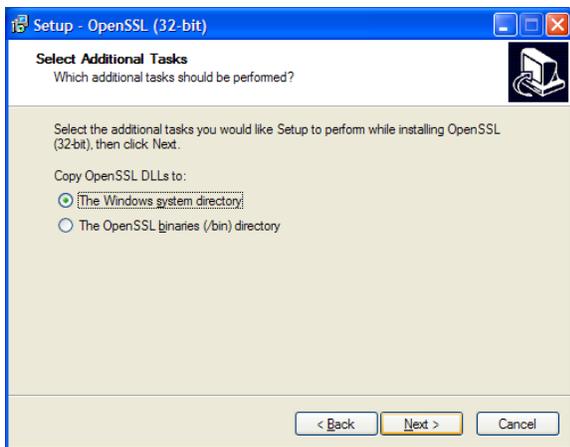
Accept the agreement and click Next



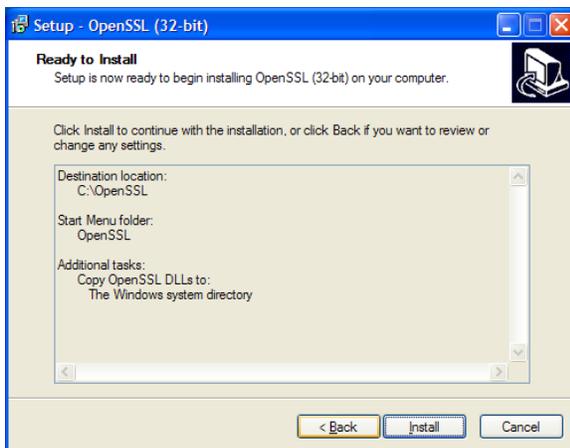
Click Next



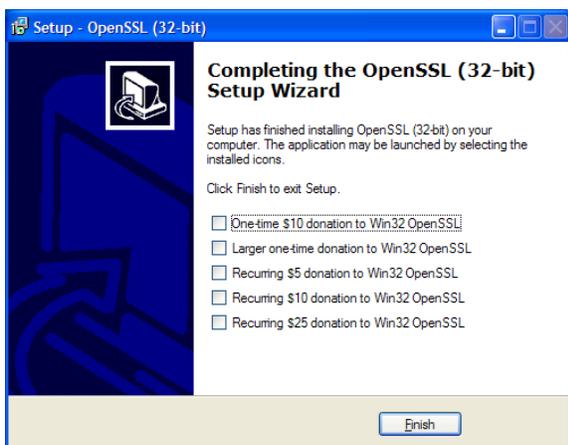
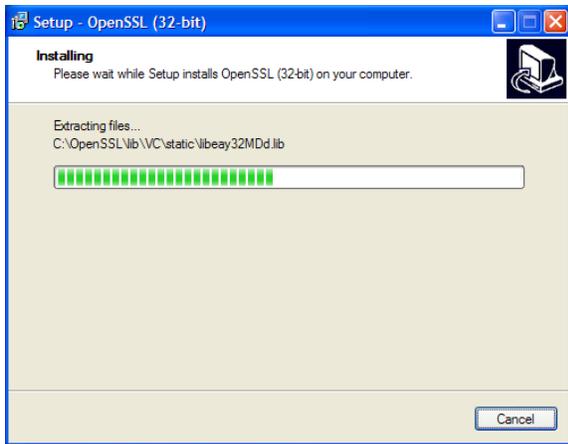
Click Next



Click Next



Click Install

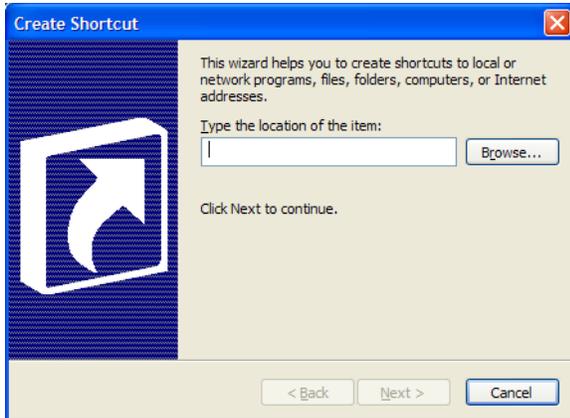


If desired, unselect and select your choice
Click Finish

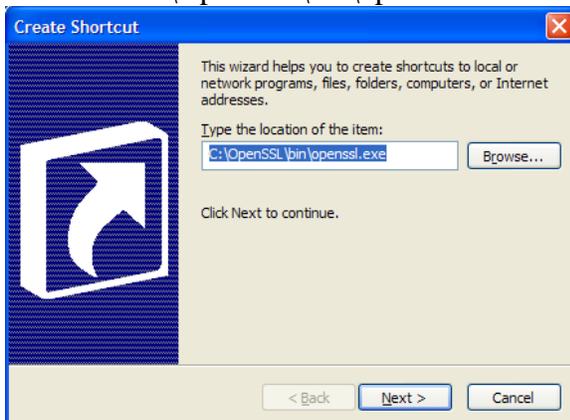
Create a shortcut on the desktop.

On the desktop right-click and select New>Shortcut from the pop-up menu

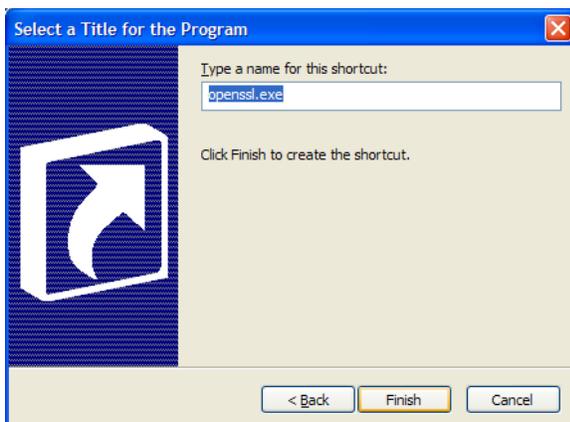
Click on Browse



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



Click Next

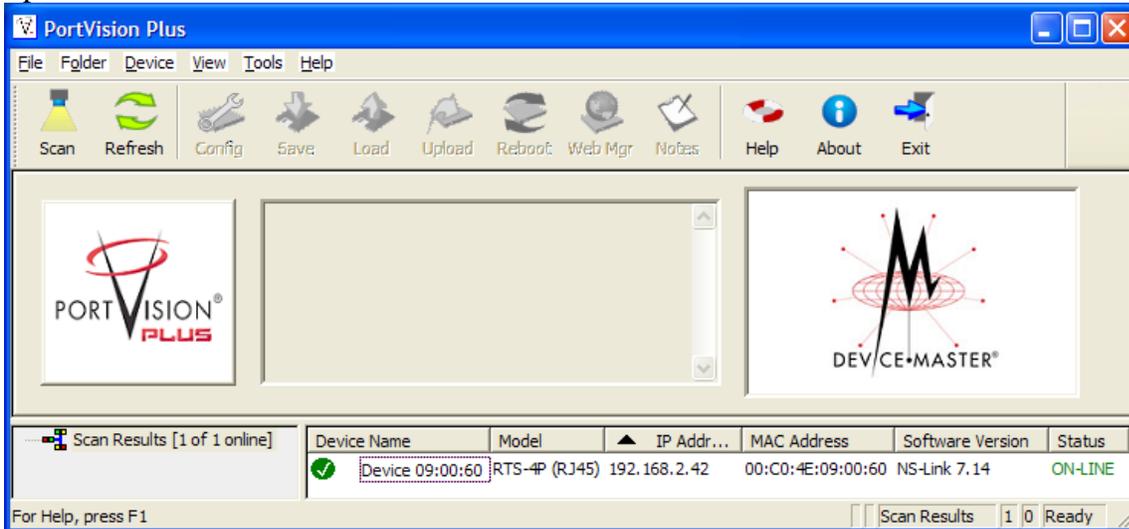


Enter a name to be displayed.

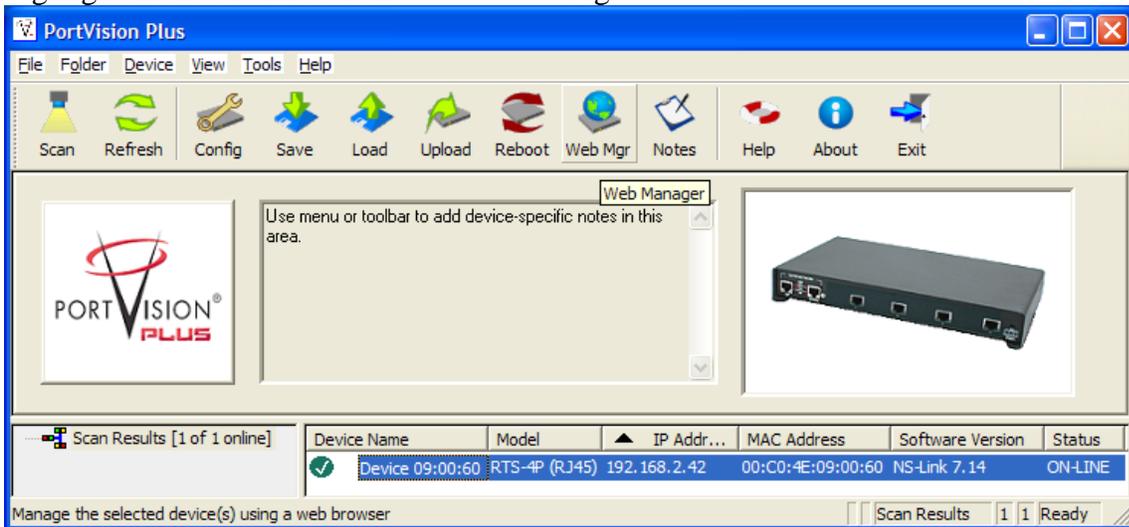
Click Finish

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.

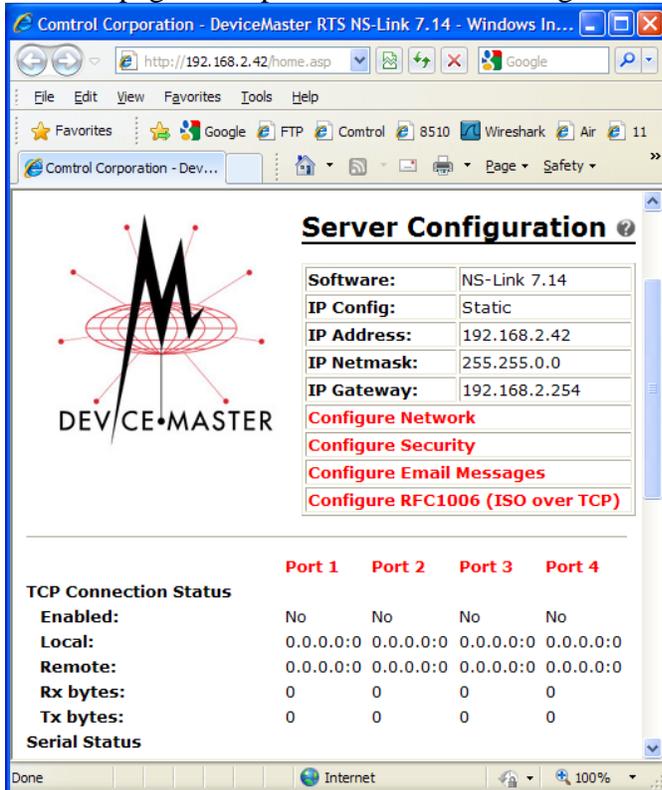
Open PortVision Plus and Scan the network to discover the DeviceMaster.



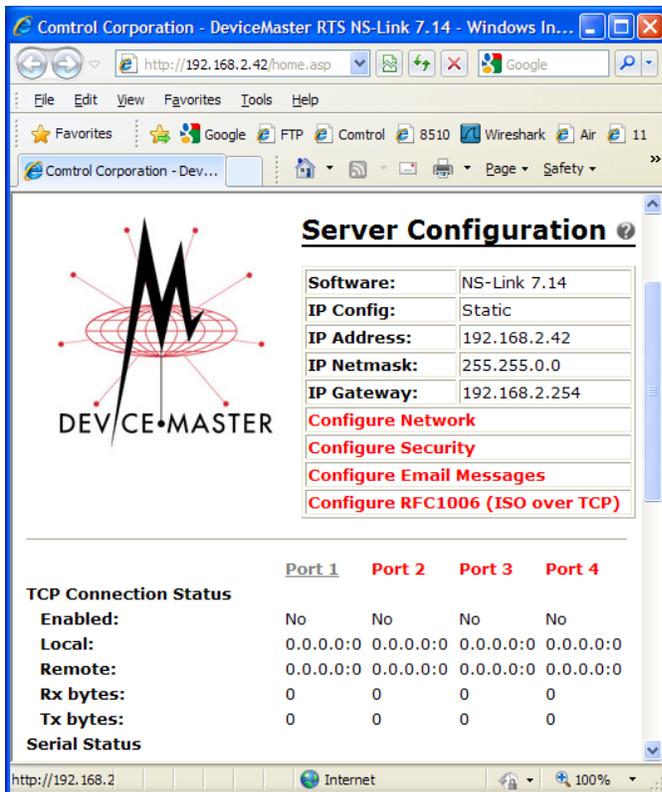
Highlight the DeviceMaster and select Web Mgr



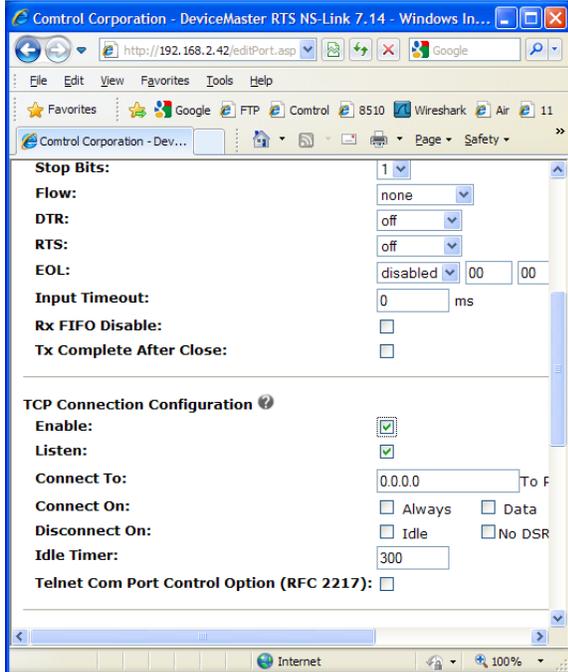
The web page will open to the Server Configuration page



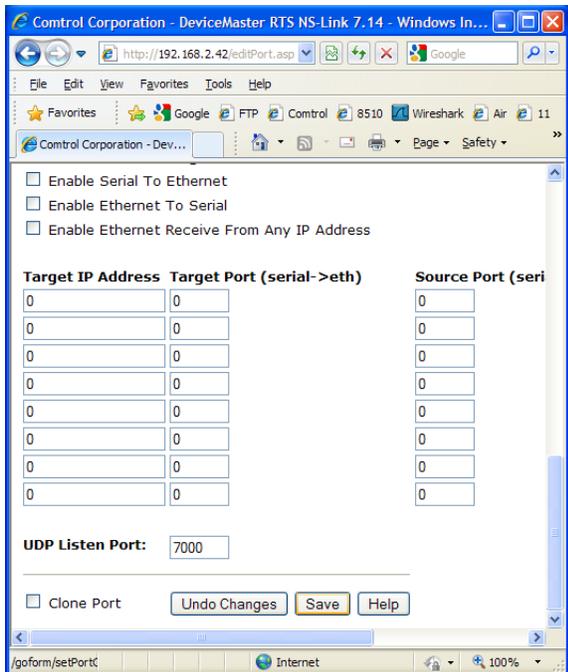
Click on Port 1



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.

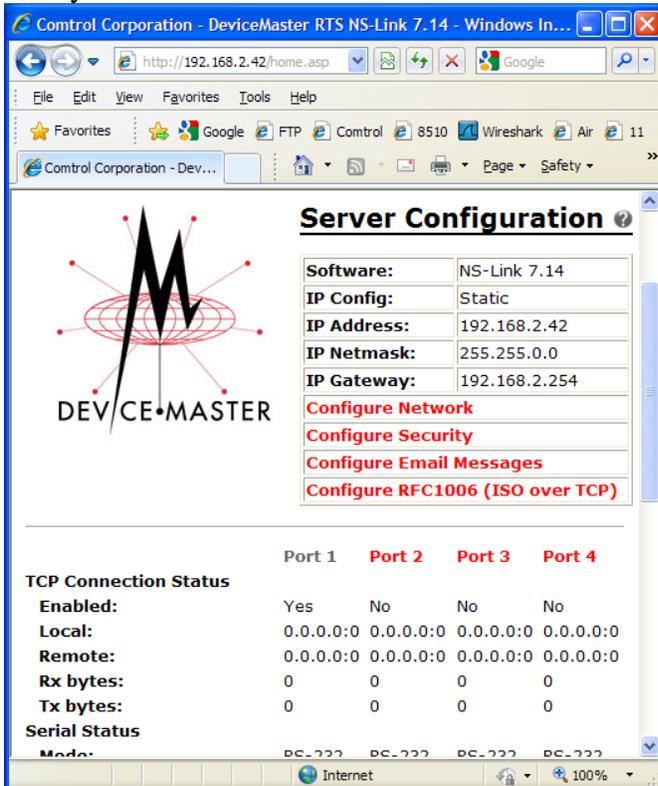


Scroll to the bottom of the page and click on Save/

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

The screenshot shows the DeviceMaster web interface. On the left is the DeviceMaster logo. The main content area is titled "Server Configuration" and contains a table with the following information:

Software:	NS-Link 7.14
IP Config:	Static
IP Address:	192.168.2.42
IP Netmask:	255.255.0.0
IP Gateway:	192.168.2.254

Below the table are four links: "Configure Network", "Configure Security", "Configure Email Messages", and "Configure RFC1006 (ISO over TCP)".

At the bottom, there is a "TCP Connection Status" section with a table:

	Port 1	Port 2	Port 3	Port 4
Enabled:	Yes	No	No	No
Local:	0.0.0.0:0	0.0.0.0:0	0.0.0.0:0	0.0.0.0:0
Remote:	0.0.0.0:0	0.0.0.0:0	0.0.0.0:0	0.0.0.0:0
Rx bytes:	0	0	0	0
Tx bytes:	0	0	0	0

Below this is a "Serial Status" section with a table:

Mode:	PC-222	PC-222	PC-222	PC-222

Here you will set the DeviceMaster to use secure modes.

The screenshot shows the "Edit Security Configuration" page. At the top is the Control logo with the tagline "Network Enabling Devices". Below the logo is the heading "Edit Security Configuration".

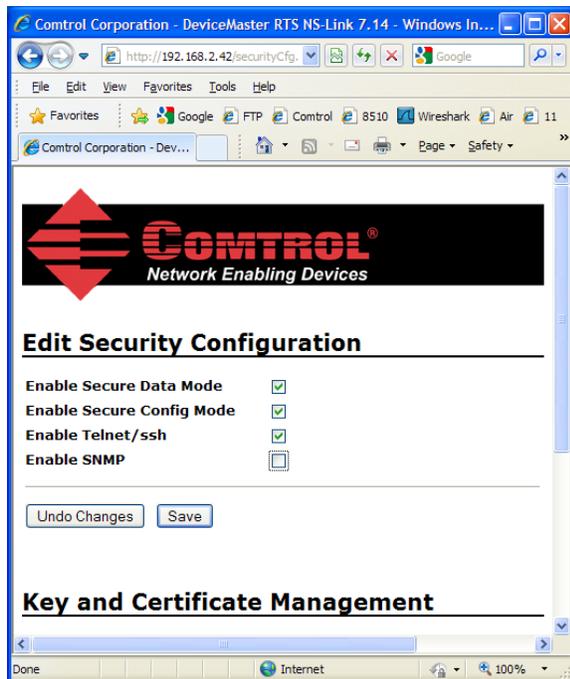
There are four checkboxes for configuration options:

- Enable Secure Data Mode
- Enable Secure Config Mode
- Enable Telnet/ssh
- Enable SNMP

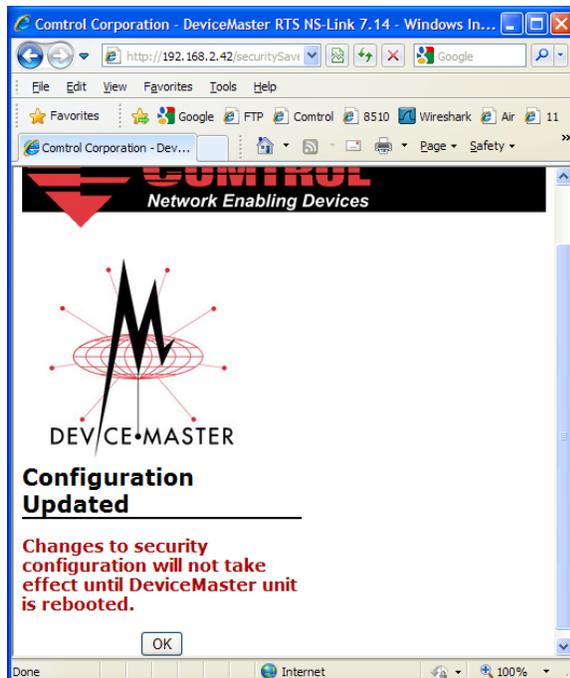
At the bottom of this section are two buttons: "Undo Changes" and "Save".

Below this is the heading "Key and Certificate Management".

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



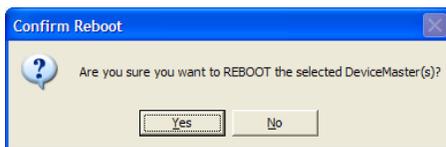
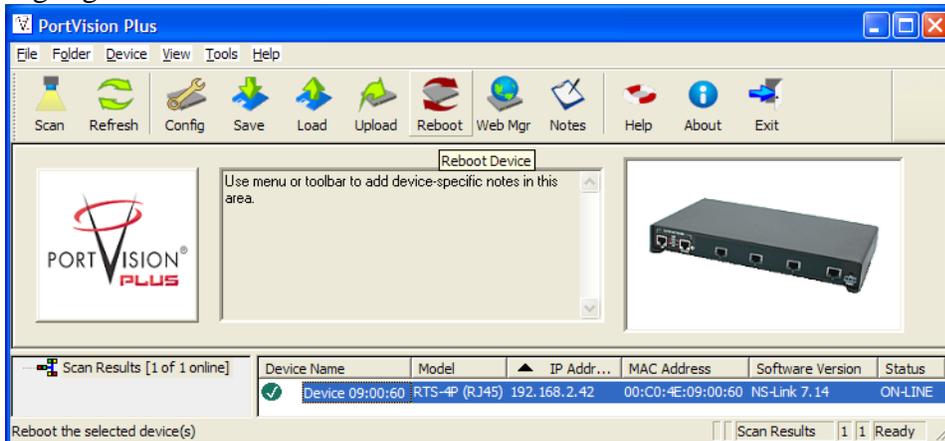
Click Save



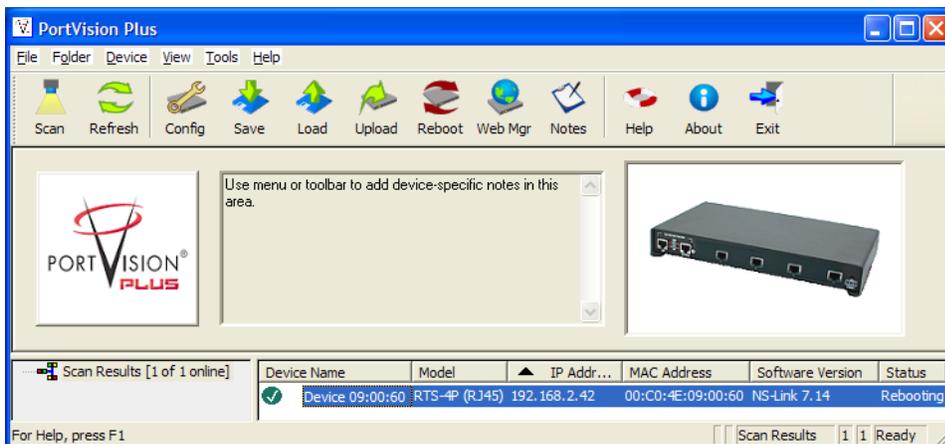
Click OK (which will return you to the previous screen).
Close the web browser.

Back to PortVision Plus.

Highlight the DeviceMaster and select the Reboot icon on the launch bar.

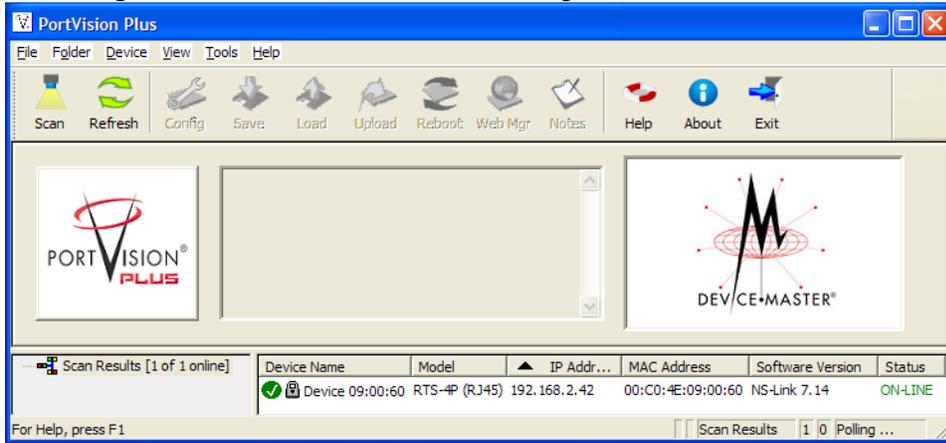


Click Yes to reboot

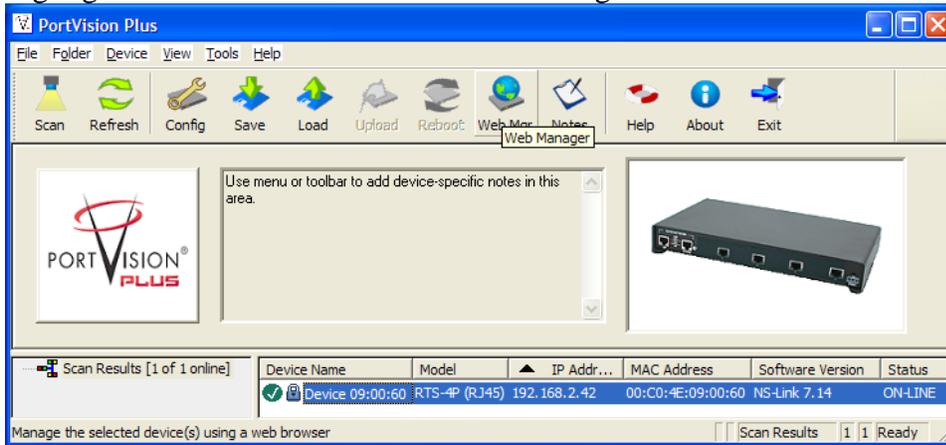


PortVision Plus will show the DeviceMaster as rebooting in the status column.

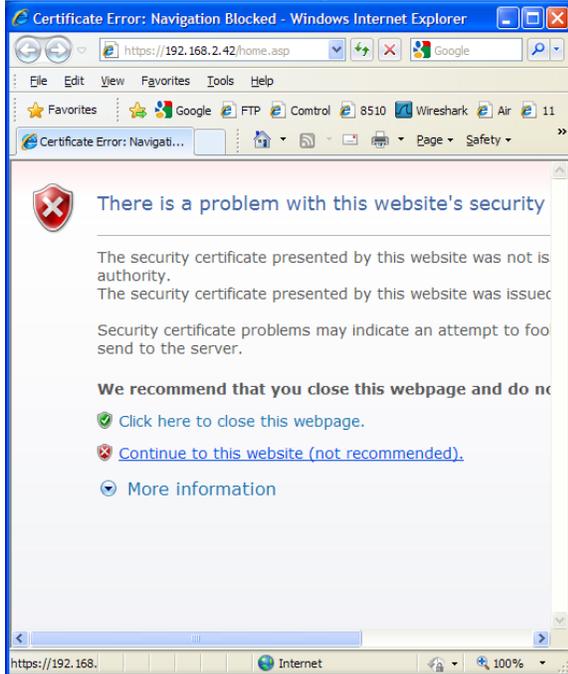
Once back on line you will now notice a “lock” next to the Device Name Indicating that it is now in secure mode of operation.



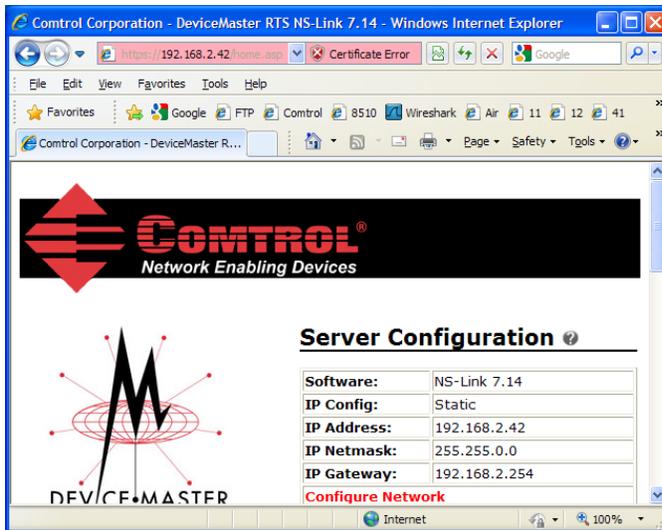
Highlight the DeviceMaster and select Web Mgr



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.

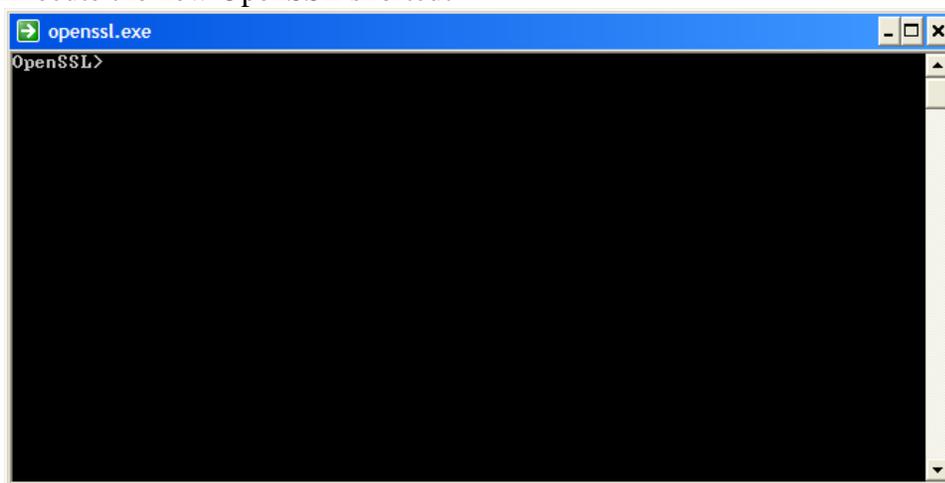


Click on “Continue to website (not recommended)”

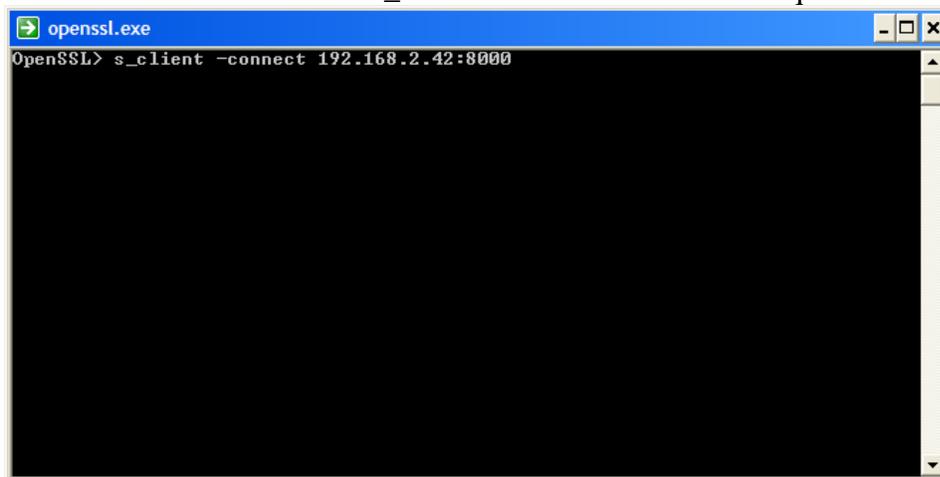


When the web page opens the URL will be in red due to the Certificate error.

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.



```
openssl.exe
OpenSSL> s_client -connect 192.168.2.42:8000
Loading 'screen' into random state - done
CONNECTED(00000090)
```

several lines will be displayed

ending with:

```
openssl.exe
l DeviceMaster/emailAddress=support@control.com
No client certificate CA names sent
SSL handshake has read 1281 bytes and written 322 bytes
New, TLSv1/SSLv3, Cipher is DHE-RSA-AES256-SHA
Server public key is 1024 bit
Compression: NONE
Expansion: NONE
SSL-Session:
  Protocol : TLSv1
  Cipher   : DHE-RSA-AES256-SHA
  Session-ID: 080000004792C80D5CC7C71F7642CE1074DA499978EE8D9E62F08EDA6E04ACD6
  Session-ID-ctx:
  Master-Key: 81804DD83DEC9C7A3CA0AF9B767BD19A8D84A29D67C3C7C2D7ADDBDC860ACF11
5E8BA0B2060FA9D40DED701E1B57CBFA
  Key-Arg  : None
  Start Time: 1258586767
  Timeout  : 300 (sec)
  Verify return code: 18 (self signed certificate)
```

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

```
openssl.exe
l DeviceMaster/emailAddress=support@control.com
No client certificate CA names sent
SSL handshake has read 1281 bytes and written 322 bytes
New, TLSv1/SSLv3, Cipher is DHE-RSA-AES256-SHA
Server public key is 1024 bit
Compression: NONE
Expansion: NONE
SSL-Session:
  Protocol : TLSv1
  Cipher   : DHE-RSA-AES256-SHA
  Session-ID: 080000004792C80D5CC7C71F7642CE1074DA499978EE8D9E62F08EDA6E04ACD6
  Session-ID-ctx:
  Master-Key: 81804DD83DEC9C7A3CA0AF9B767BD19A8D84A29D67C3C7C2D7ADDBDC860ACF11
5E8BA0B2060FA9D40DED701E1B57CBFA
  Key-Arg  : None
  Start Time: 1258586767
  Timeout  : 300 (sec)
  Verify return code: 18 (self signed certificate)
aaa_
```

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

```
openssl.exe
No client certificate CA names sent
SSL handshake has read 1281 bytes and written 322 bytes
New, TLSv1/SSLv3, Cipher is DHE-RSA-AES256-SHA
Server public key is 1024 bit
Compression: NONE
Expansion: NONE
SSL-Session:
  Protocol  : TLSv1
  Cipher    : DHE-RSA-AES256-SHA
  Session-ID: 080000004792C80D5CC7C71F7642CE1074DA499978EE8D9E62F08EDA6E04ACD6
  Session-ID-ctx:
  Master-Key: 81804DD83DEC9C7A3CA0AF9B767BD19A8D84A29D67C3C7C2D7ADDBDC860ACF11
5E8B00B2060FA9D40DED701E1B57CBFA
  Key-Arg   : None
  Start Time: 1258586767
  Timeout  : 300 (sec)
  Verify return code: 18 (self signed certificate)
aaa
aaa
```

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.

The screenshot shows the DeviceMaster web interface in a browser window. The page title is "Control Corporation - DeviceMaster RTS NS-Link 7.14 - Windows Interne...". The address bar shows "https://192.168.2.42/". The page content includes a logo for "DEVICE MASTER" and a "Server Configuration" section with the following details:

Software:	NS-Link 7.14
IP Config:	Static
IP Address:	192.168.2.42
IP Netmask:	255.255.0.0
IP Gateway:	192.168.2.254

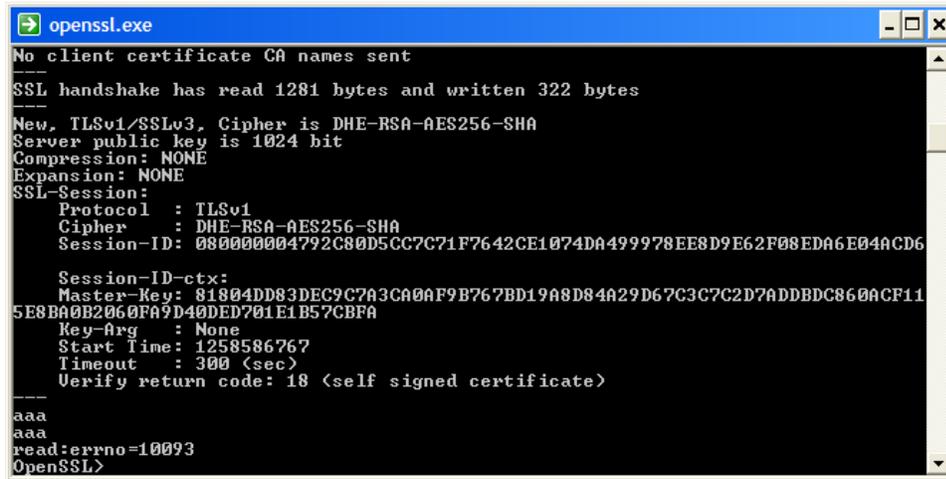
Below the configuration table are links for "Configure Network", "Configure Security", "Configure Email Messages", and "Configure RFC1006 (ISO over TCP)".

The "TCP Connection Status" section shows a table with columns for Port 1, Port 2, Port 3, and Port 4. The "Enabled" row shows "Yes" for Port 1 and "No" for the others. The "Local" row shows "0.0.0.0:8000" for Port 1 and "0.0.0.0:0" for the others. The "Remote" row shows "192.168.2.10:1329" for Port 1 and "0.0.0.0:0" for the others. The "Rx bytes" row shows "11" for Port 1 and "0" for the others. The "Tx bytes" row shows "0" for all ports.

	Port 1	Port 2	Port 3	Port 4
Enabled:	Yes	No	No	No
Local:	0.0.0.0:8000	0.0.0.0:0	0.0.0.0:0	0.0.0.0:0
Remote:	192.168.2.10:1329	0.0.0.0:0	0.0.0.0:0	0.0.0.0:0
Rx bytes:	11	0	0	0
Tx bytes:	0	0	0	0

This confirms connection and data transfer.

Back to OpenSSL
Ctrl-C to disconnect



```
openssl.exe
No client certificate CA names sent
-----
SSL handshake has read 1281 bytes and written 322 bytes
-----
New, TLSv1/SSLv3, Cipher is DHE-RSA-AES256-SHA
Server public key is 1024 bit
Compression: NONE
Expansion: NONE
SSL-Session:
  Protocol  : TLSv1
  Cipher    : DHE-RSA-AES256-SHA
  Session-ID: 080000004792C80D5CC7C71F7642CE1074DA499978EE8D9E62F08EDA6E04ACD6
-----
  Session-ID-ctx:
  Master-Key: 81804DD83DEC9C7A3CA0AF9B767BD19A8D84A29D67C3C7C2D7ADDBDC860ACF11
5E8BA0B2060FA9D40DED701E1B57CBFA
  Key-Arg   : None
  Start Time: 1258586767
  Timeout  : 300 (sec)
  Verify return code: 18 (self signed certificate)
-----
aaa
aaa
read:errno=10093
OpenSSL>
```

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