comnet
Communication Networks

INSTALLATION AND OPERATION MANUAL

CNFE3DOE2/M

RS232/422/485 DATA OVER ETHERNET TERMINAL SERVER

The ComNet CNFE3DOE2/M allows any combination of two RS-232, RS-422, or 2 or 4-wire RS-485 serial data circuits to be inserted onto any 10/100 Mbps Ethernet-based network. The CNFE3DOE2/M units include two serial data input/output ports, and three Ethernet ports featuring two electrical ports and one SFP port. It may be used to tunnel serial data over an IP network or as a media converter, for converting copper transmission media to fiber. Access one serial device from the Internet and another serial device from a local area network (LAN) using SSH or SSL. The CNFE3DOE2/M provides control of the remote hardware, as if it were connected directly to the PC COM port. A USB to serial converter may be required in new PCs without a DB9 serial connection. The CNFE3DOE2/M supports SNMP Version 1, RFC1155, RFC1213 & RFC1215.

Contents

Hardware description 3

Assign IP Address to a Terminal Server 4

Using Terminal Server as a Serial Extender over Ethernet 8

- TCP Transport 8
- UDP Transport 13
- SSL Transport 17
- Creating openssl certificates 23
- SSH Transport 25
- Creating SSH key pairs 29
- Telnet Transport 29

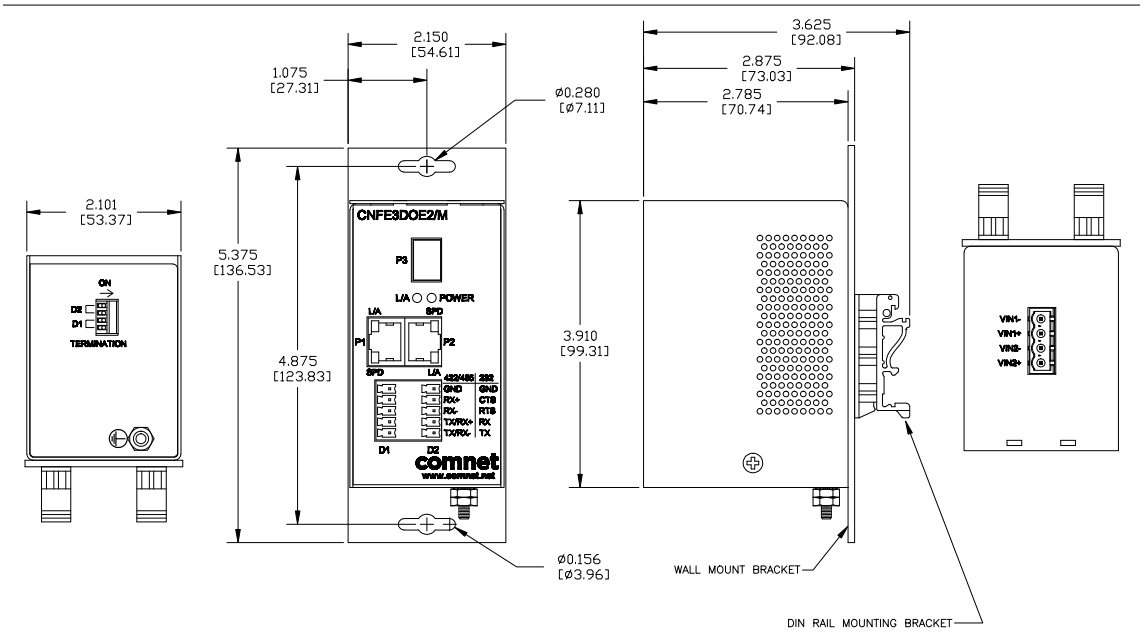
HTTPS Configuration 33

- OpenSSL Certificate, key and CA for HTTPS 39

Console Port Access 40

Hardware description

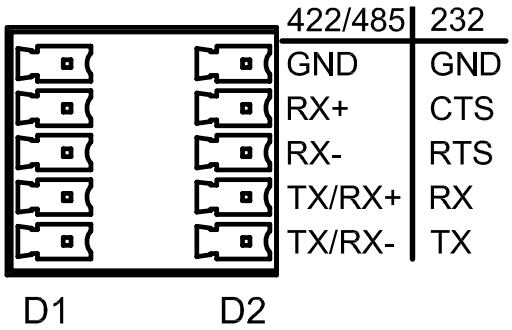
The ComNet CNFE3DOE2/M terminal server supports Ethernet transmission over two copper ports and one fiber port. The server is universally compatible with RS232, RS422, RS485 serial data protocols. All configurations are done through its web server. Distances depend on which SFP (Small Form Pluggable) module is used. The RJ45 Ethernet and SFP interfaces are all enabled. They can function as an Ethernet media converter.



Mechanical Drawing of CNFE3DOE2/M Unit

Switches are used for RS485 Full Duplex mode to terminate Tx+ & Tx- and Rx+ & Rx- with 120 ohms. Both switches should be in the on position. For all other modes, the switches should be in the off position.

The data connector pin-out is as below:



Settings by Data Type (Port 1 or 2)

Assign IP Address to a Terminal Server

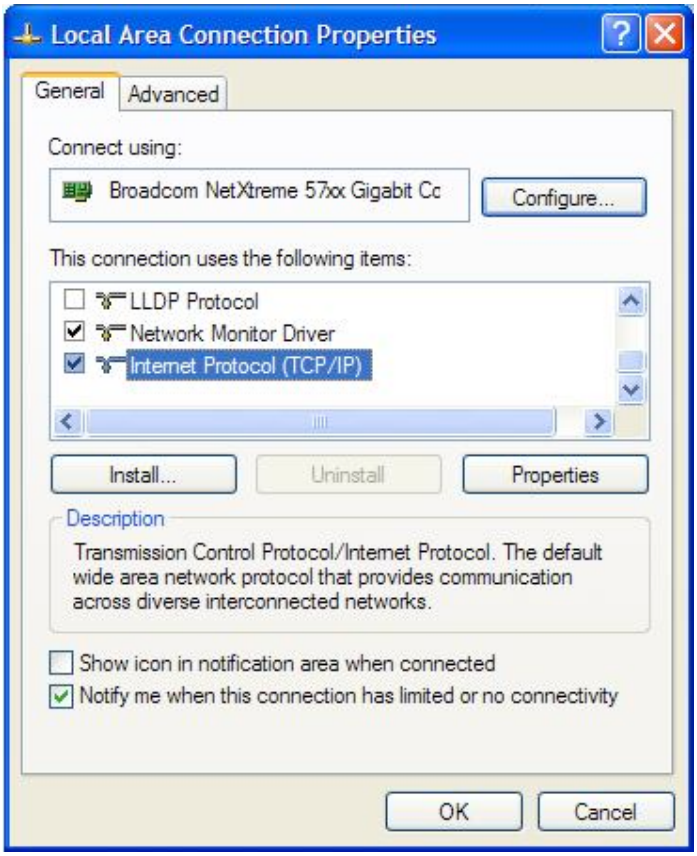
A unique IP address has to be assigned to each terminal server device. You can connect one at a time to change the default IP address. The default IP address of the device is the same: 192.168.10.1.

Connect the terminal server on to your local Ethernet network which your PC is connected to, and power on the unit.

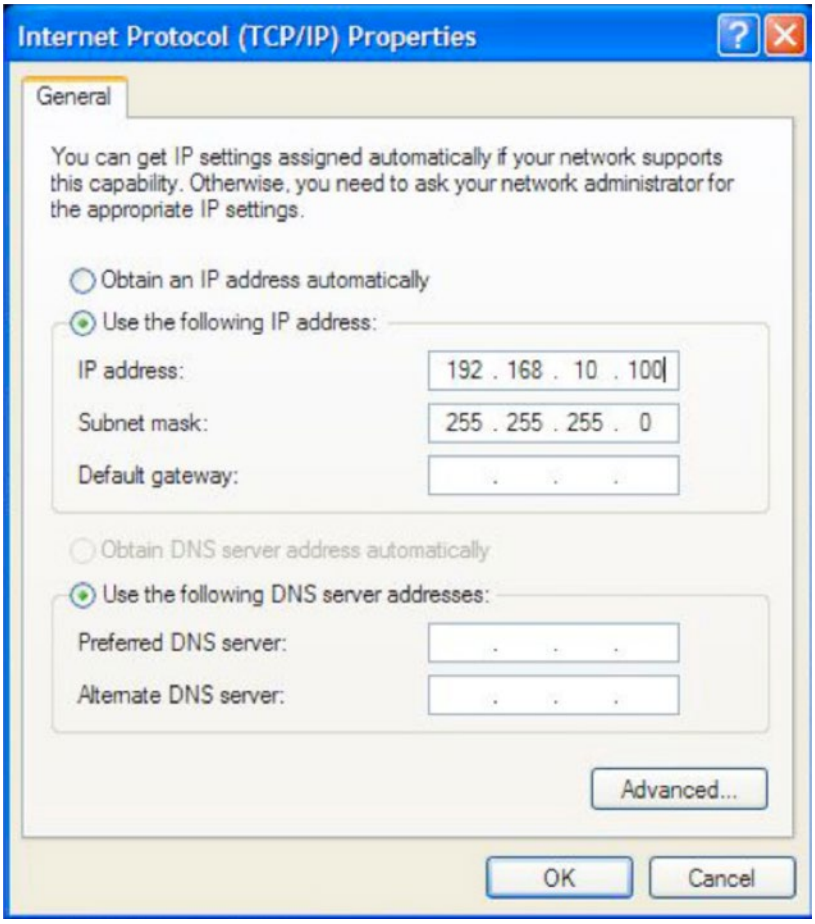
Follow the steps below to set up your PC IP address to the same subnet as the terminal servers.

Disable the machine's wireless network connection and any other internet connections that could interfere with the network being created.

Select the Internet Protocol (TCP/IP) connection within the Local Area Connection Properties from **start -> Control Panel -> Network Connections -> Properties**.



Next, manually set your IP address to **192.168.10.100**, for instance, and your subnet mask to **255.255.255.0**, as shown below.

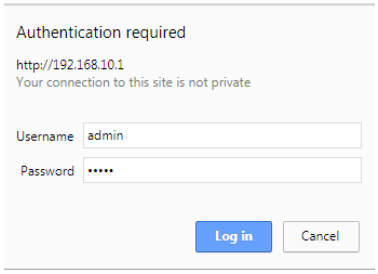


Click **OK** to finish the setting.

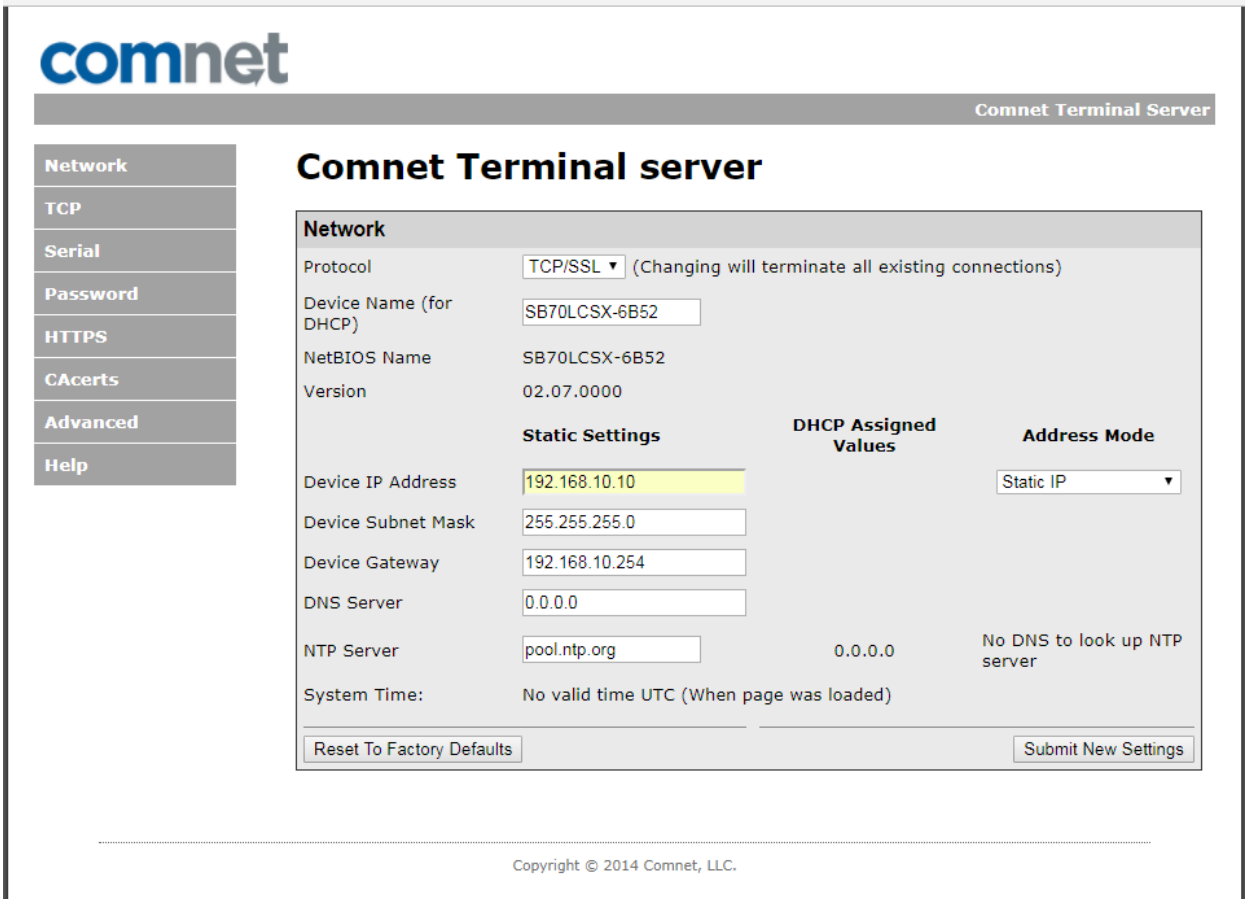
Open the browser on your PC, and type in **192.168.10.1** and open the Terminal Server Log in Page as shown.

The default User Name and Password are both **admin**

Log in to the Terminal Server Home Page as shown.



Terminal Server Log in Pop-up



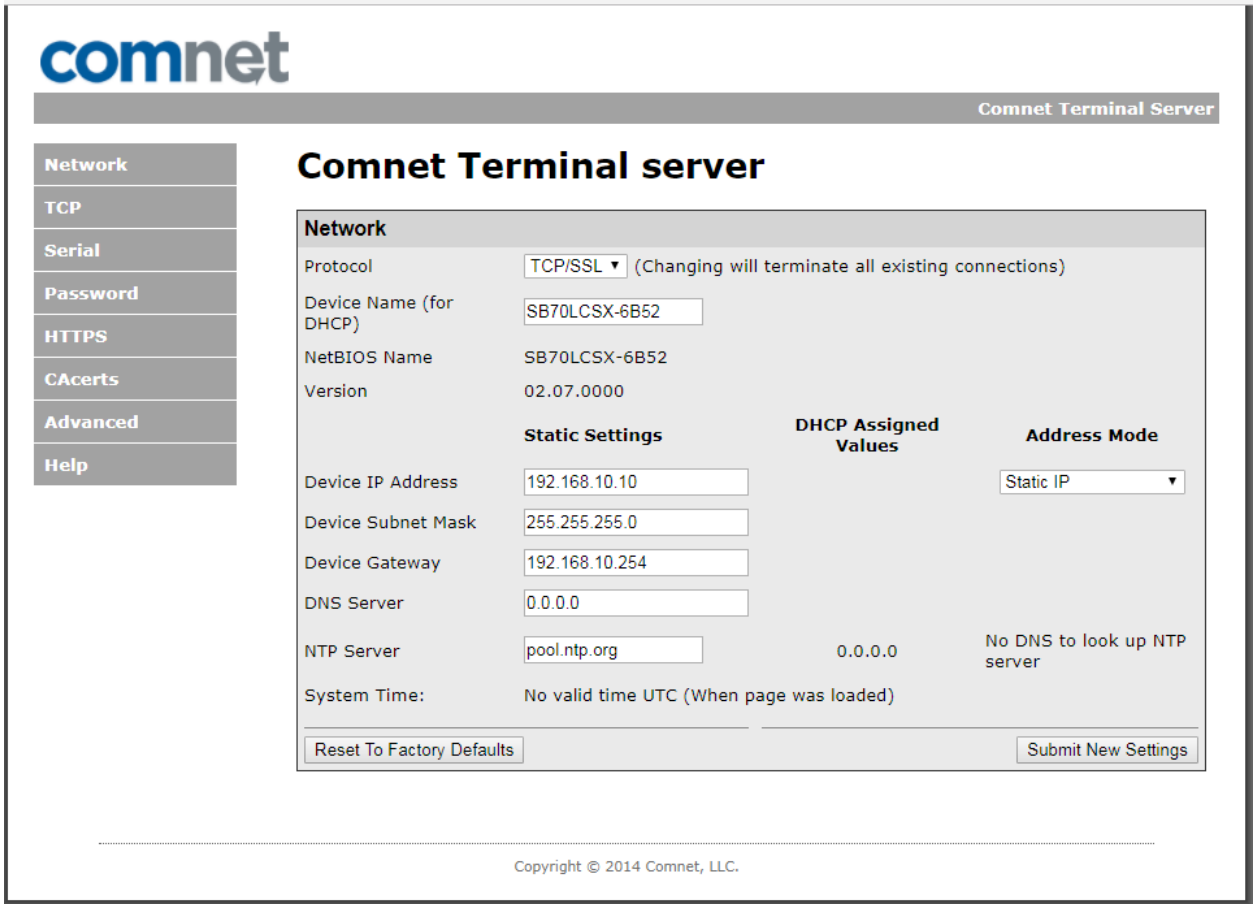
Terminal Server Network Page

Click on the **Device IP Address text box**.

Change the IP address to an IP address with subnet appropriate for your network. In the following examples an IP address in subnet **192.168.10.xxx** will be used.

Configure the IP address to **192.168.10.10** as shown in the Terminal Server Network Page.

Click **Submit New Settings**.



Terminal Server Configuration Page

Log in to the terminal server again using the new IP address.

If an IP address in a different subnet was used, be sure to change the PC's network address to an IP address in the appropriate subnet.

Using Terminal Server as a Serial Extender over Ethernet

TCP Transport

To use the Terminal Server as a serial extender over Ethernet, connect two terminal servers to your local Ethernet network.

Configure Server

Configure the first device as a server:

» Set protocol to TCP/SSL on Network page.

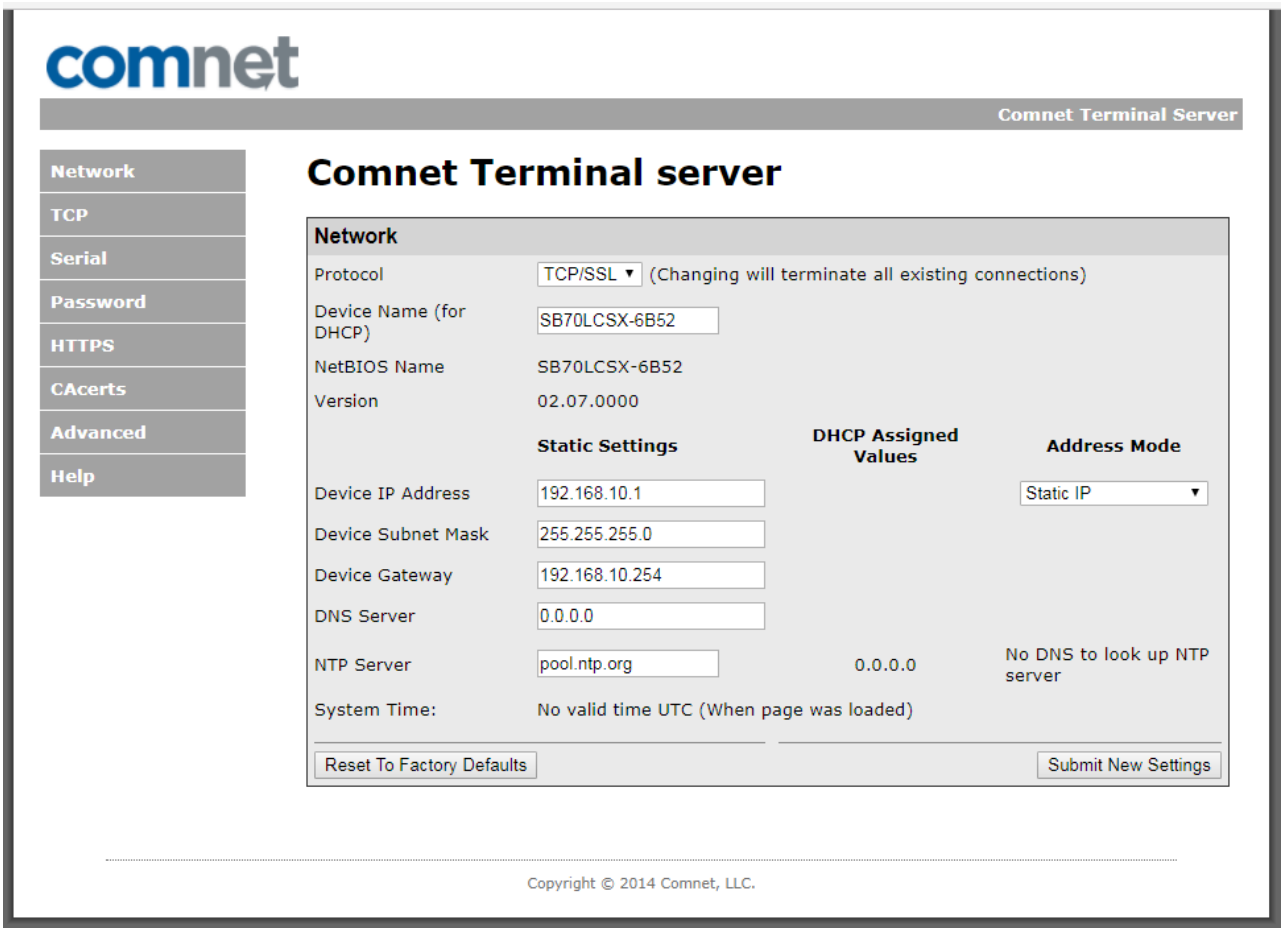


Figure 1 Terminal Server Network Page

» Click TCP link

» Configure Port1 to listen for incoming connections on port 24

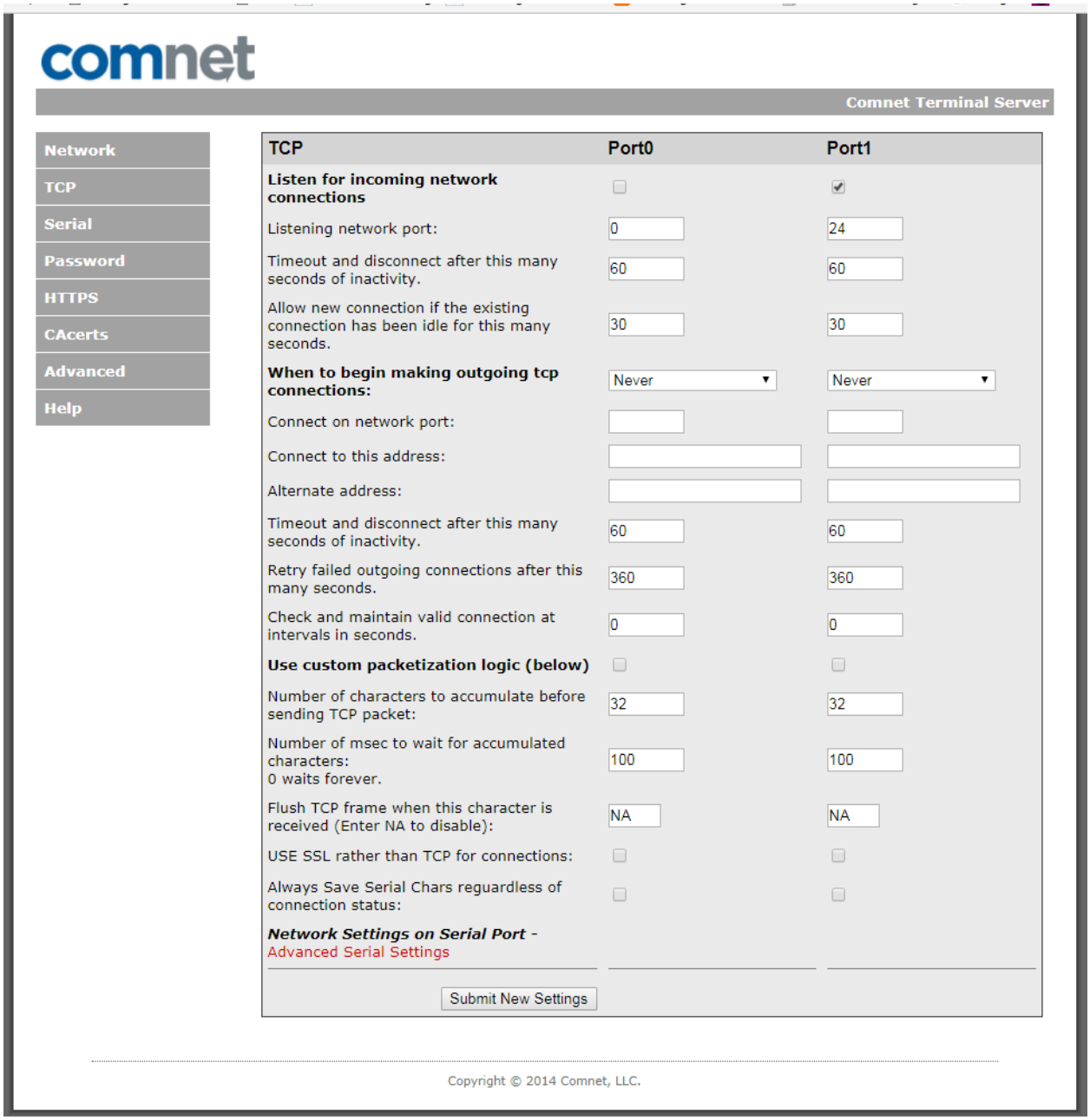


Figure 2 Terminal Server TCP Page

» Click Serial link

» Configure Port1 for RS422

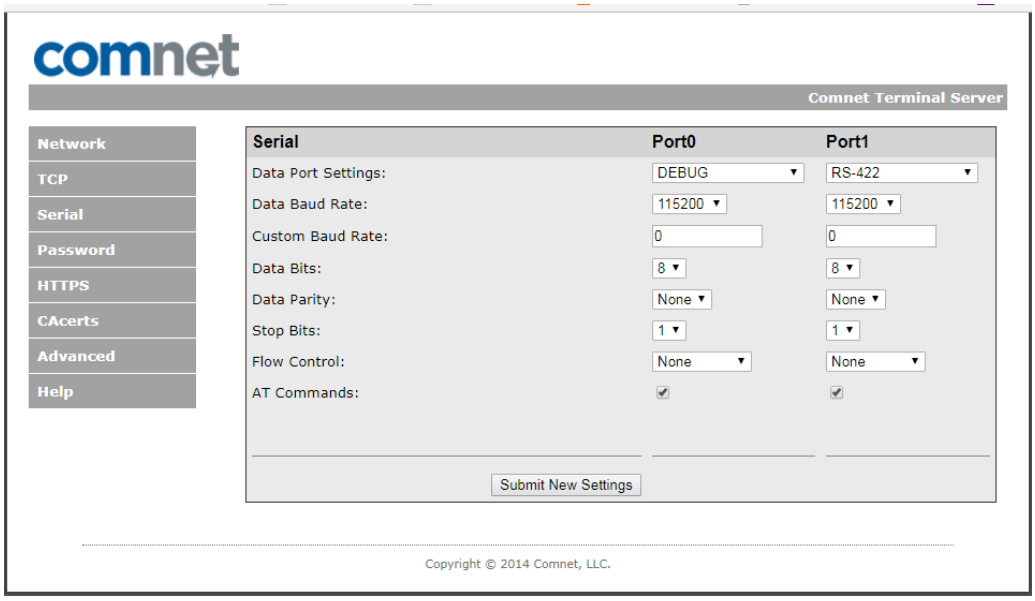


Figure 3 Terminal Server Serial Page

Configure Client

» Configure the second device as a client.

» Set protocol to TCP/SSL on Network page.

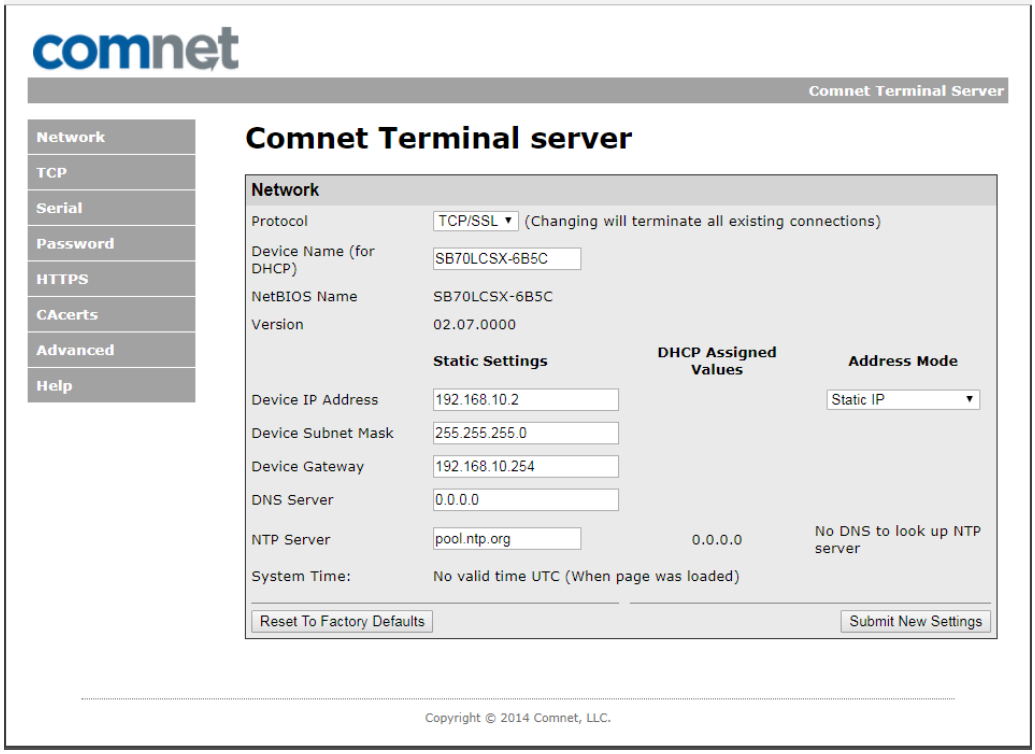


Figure 4 Terminal Client Network Page

» Click TCP link

» Configure Port1 to connect to 192.168.10.1 port 24

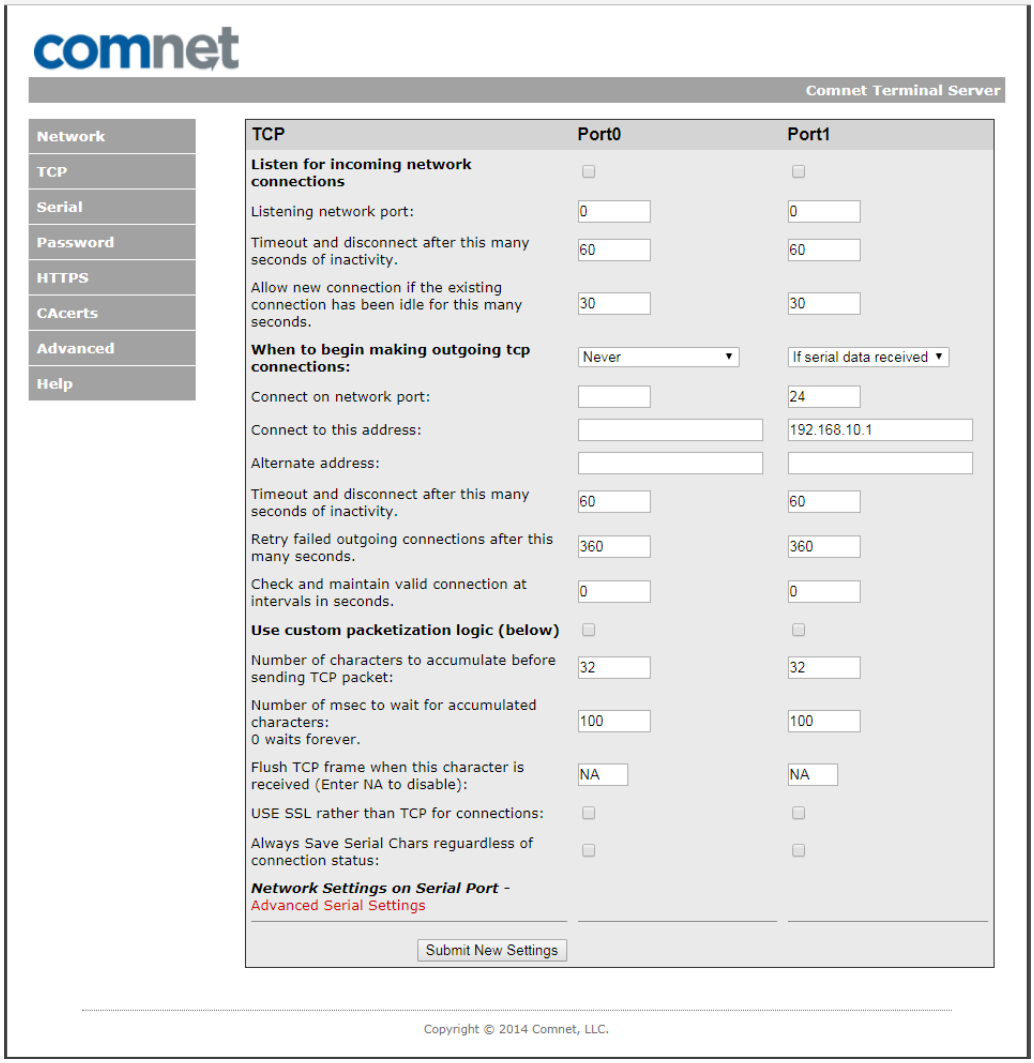


Figure 5 Terminal Client TCP Page

» Click Serial link

» Configure Port1 for RS422

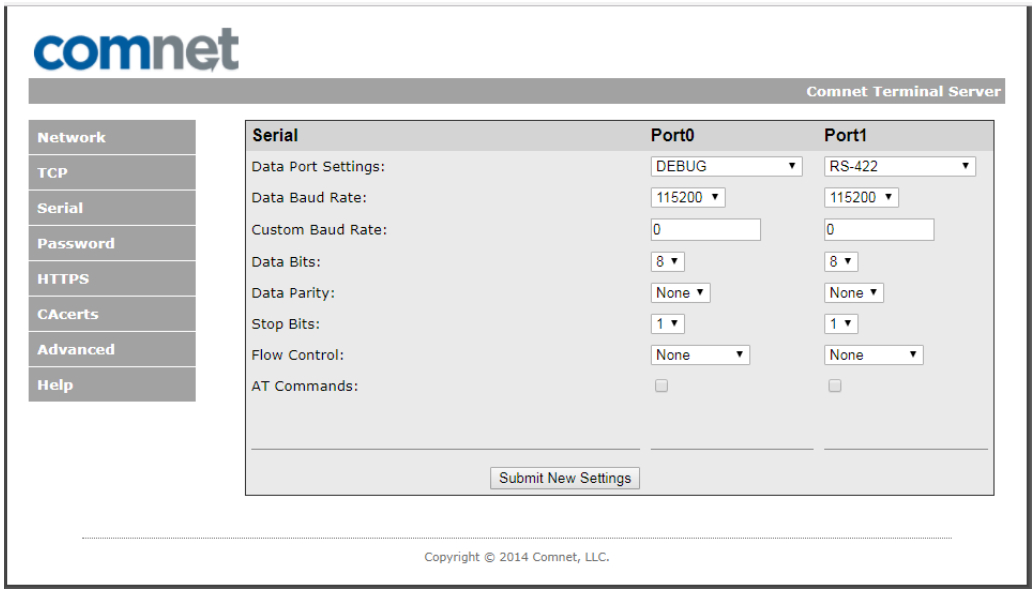


Figure 6 Terminal Client Serial Page

UDP Transport

To use the Terminal Server as a serial extender over Ethernet utilizing UDP, connect two terminal servers to your local Ethernet network and configure devices as a client server connection.

Configure Server

» Set protocol to UDP on Network page.

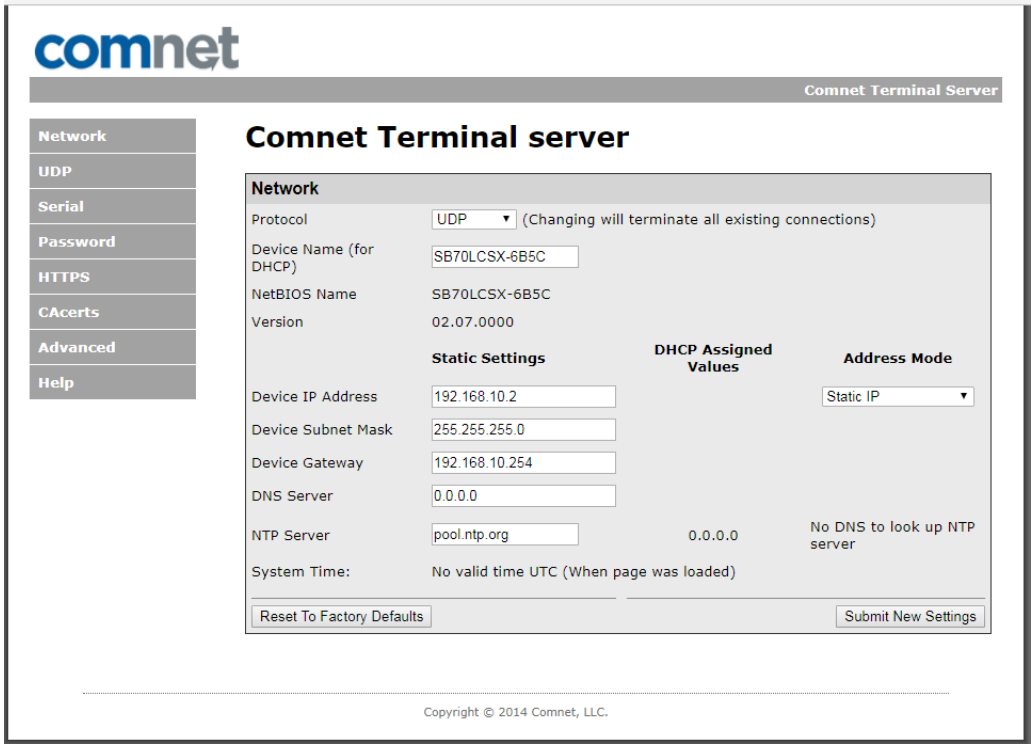


Figure 7 Terminal Server Network Page

» Click UDP link

» Configure Port1 to receive on port 24 & to transmit to 192.168.10.2 on port 25

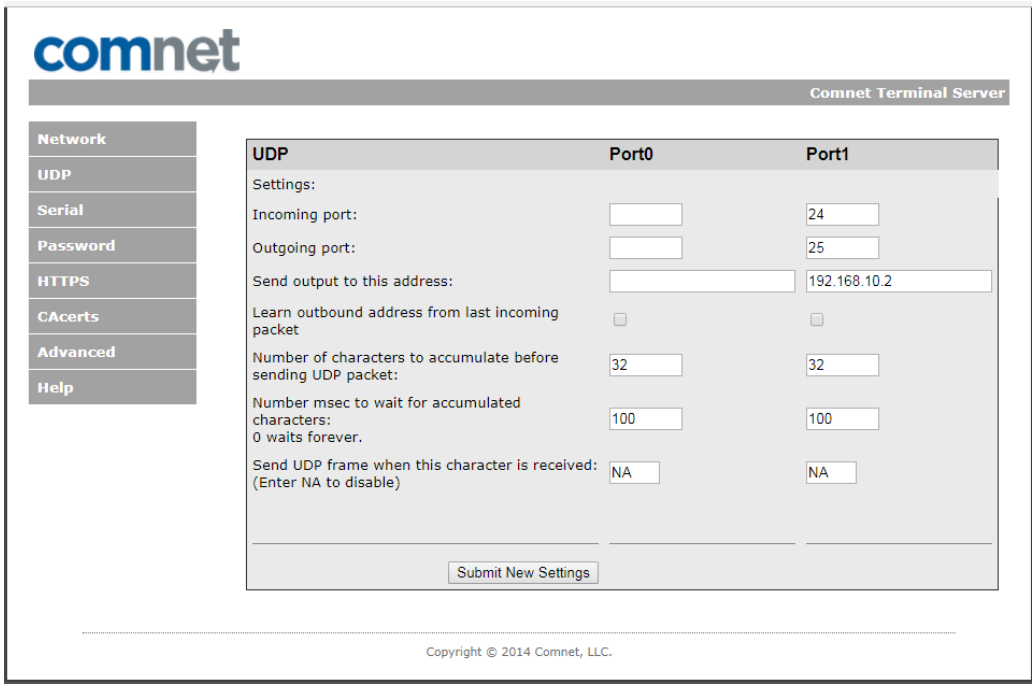


Figure 8 Terminal Server UDP Page

» Click Serial link

» Configure Port1 for RS422

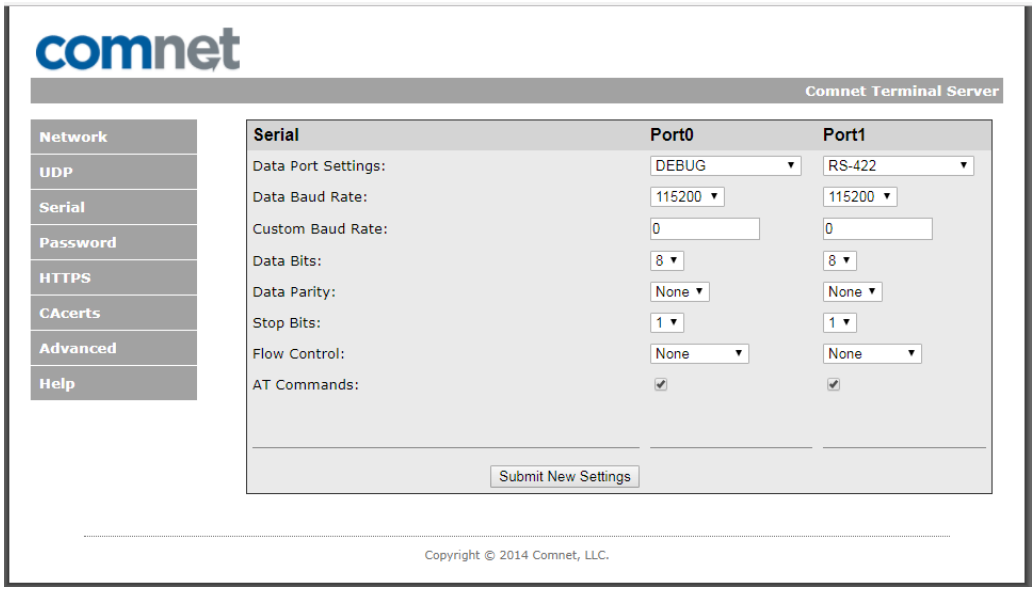


Figure 9 Terminal Server Serial Page

Configure Client

» Set protocol to UDP on Network page.

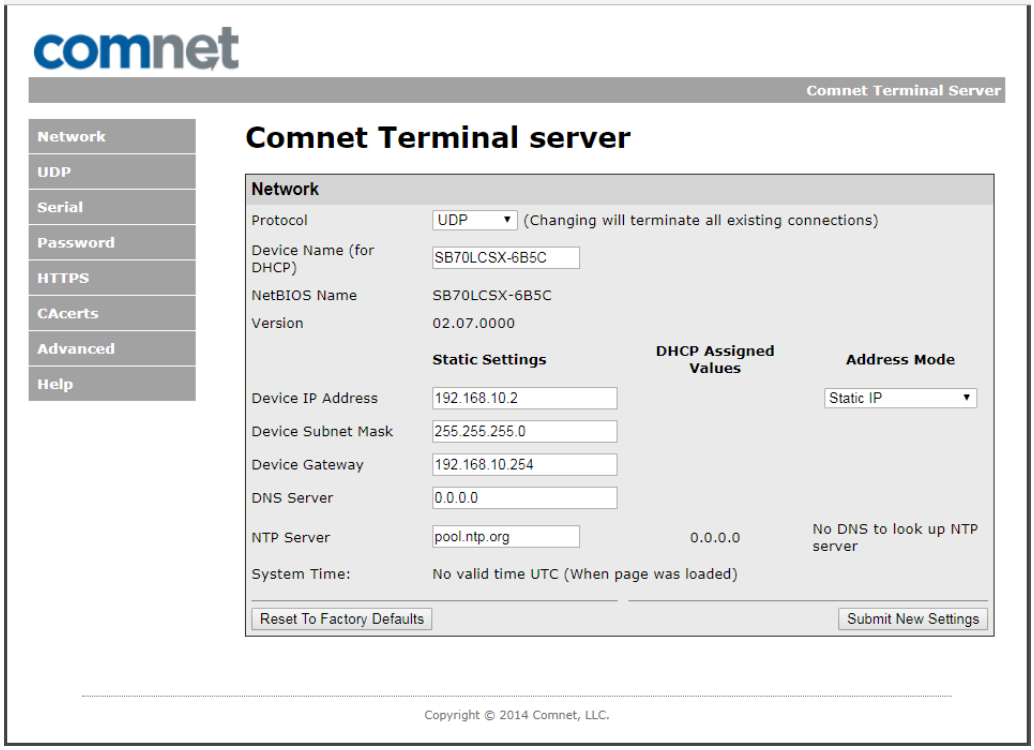


Figure 10 Terminal Client Network Page

» Click UDP link

» Configure Port1 to receive on port 25 & to transmit to 192.168.10.1 on port 24

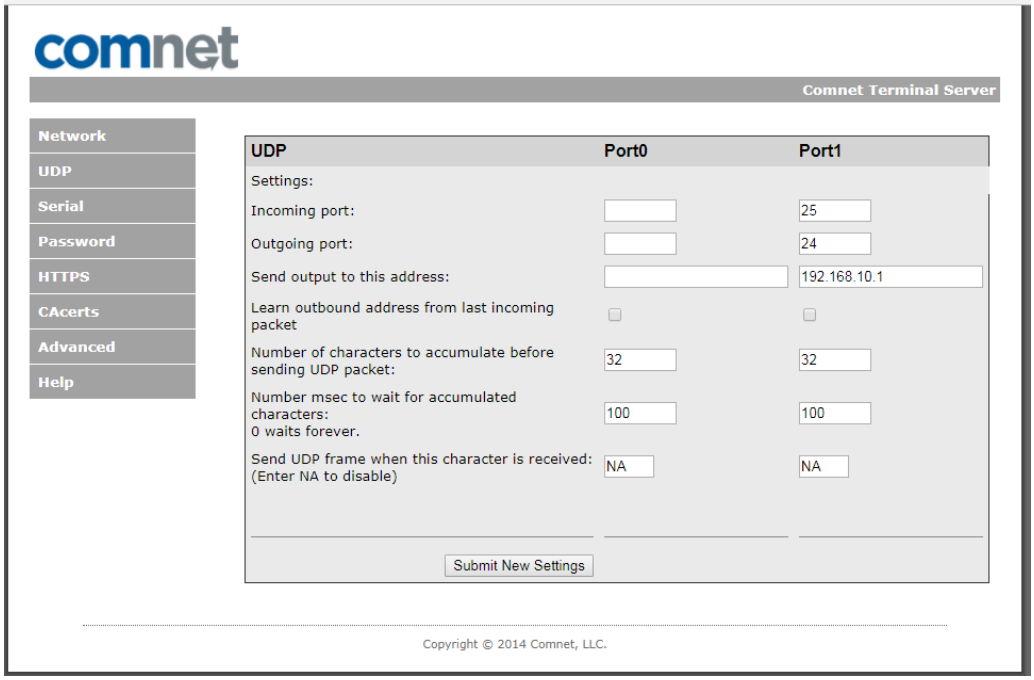


Figure 11 Terminal Client UDP Page

» Click Serial link

» Configure Port1 for RS422

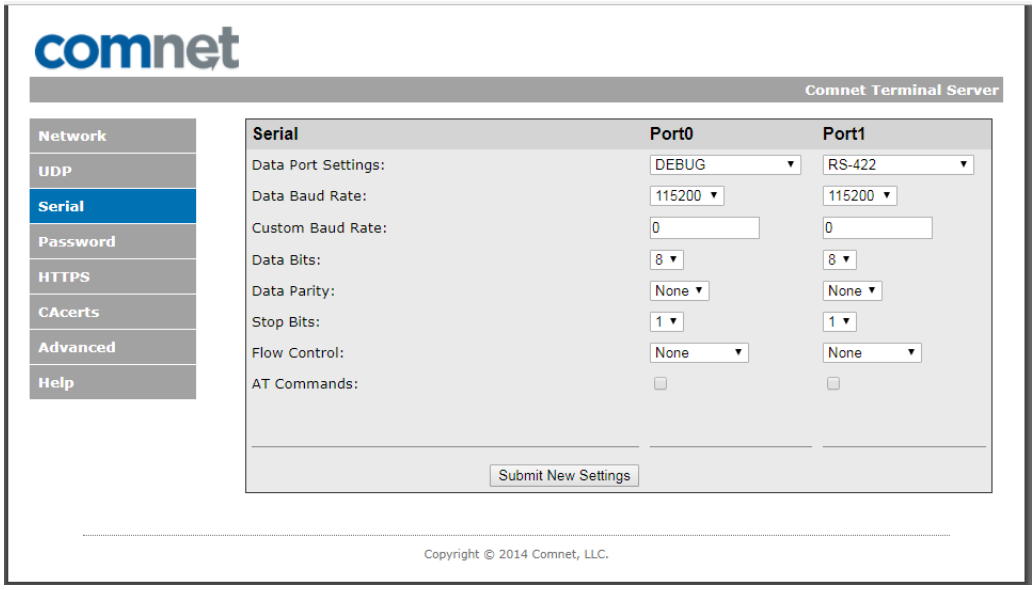


Figure 12 Terminal Client Serial Page

SSL Transport

To use the Terminal Server as a serial extender over Ethernet utilizing SSL, connect two terminal servers to your local Ethernet network and configure devices as a client server connection.

Configure Server

» Set protocol to TCP/SSL on Network page.

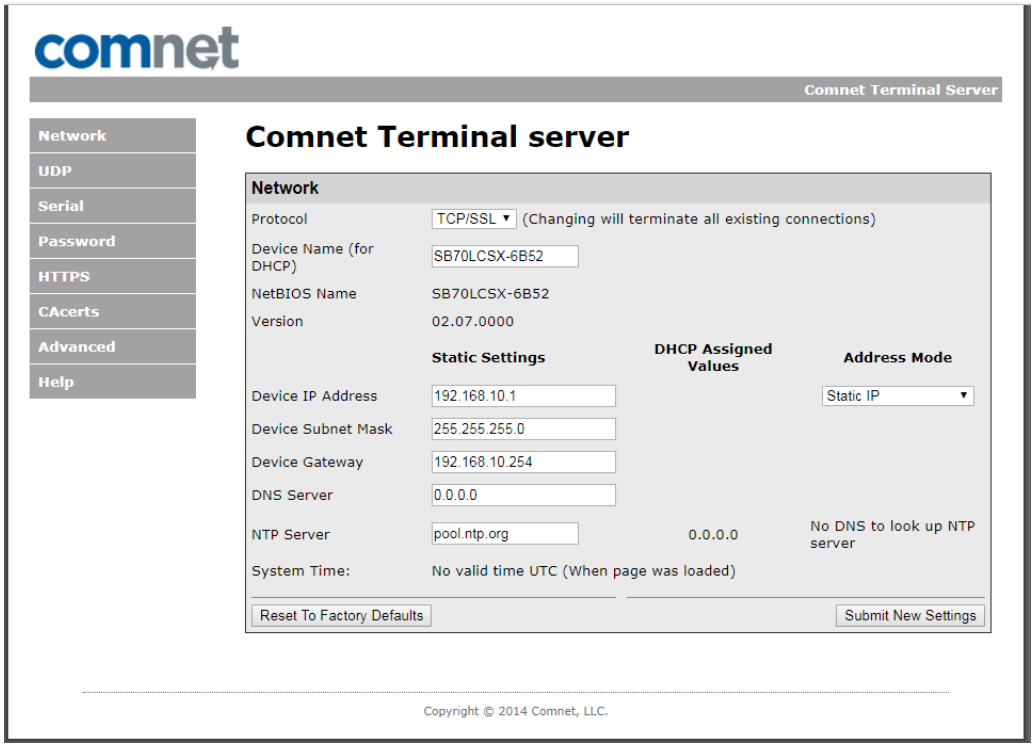


Figure 13 Terminal Server Network Page

» Click TCP link

» Configure Port1 to listen for incoming connections on port 24

» Check “USE SSL rather than TCP for connection”

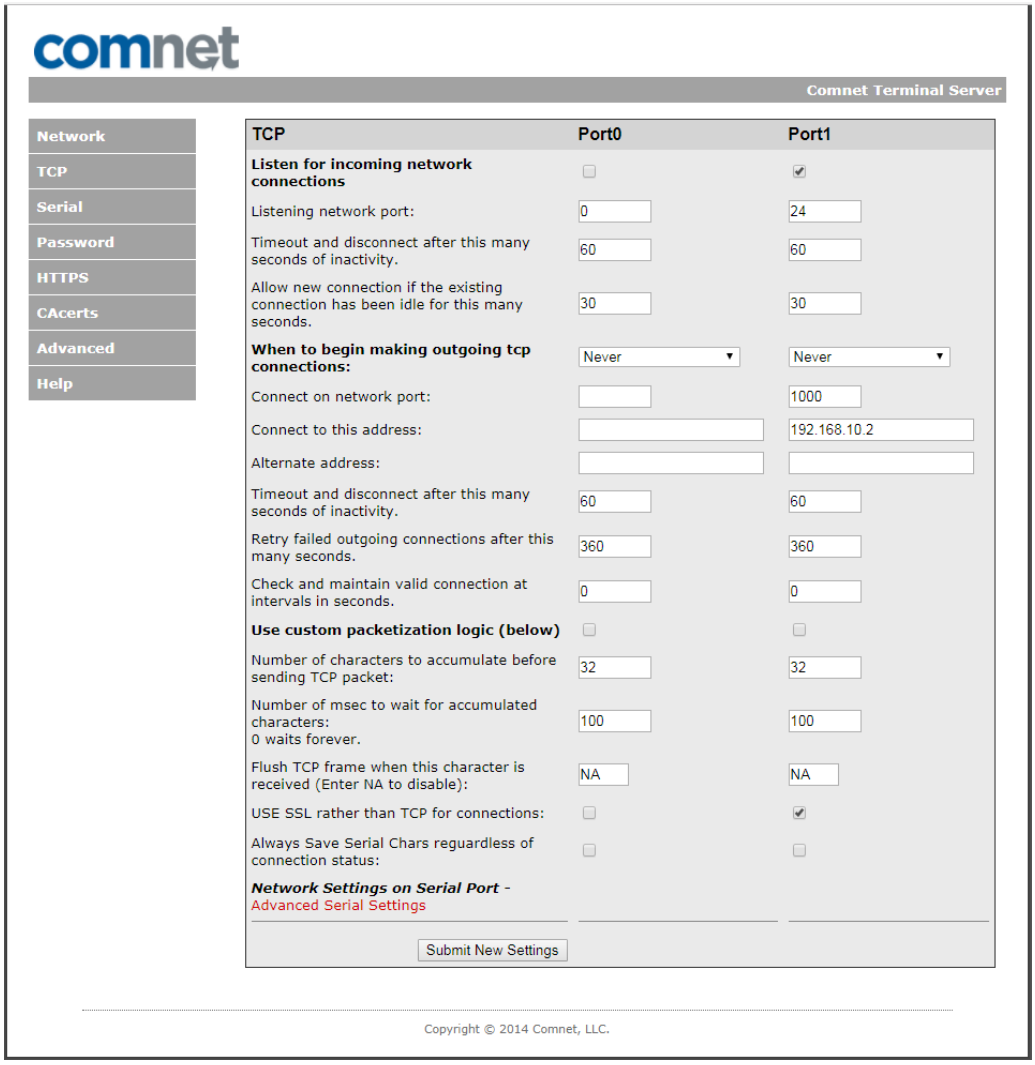


Figure 14 Terminal Server TCP Page

» Click Serial link

» Configure Port1 for RS422

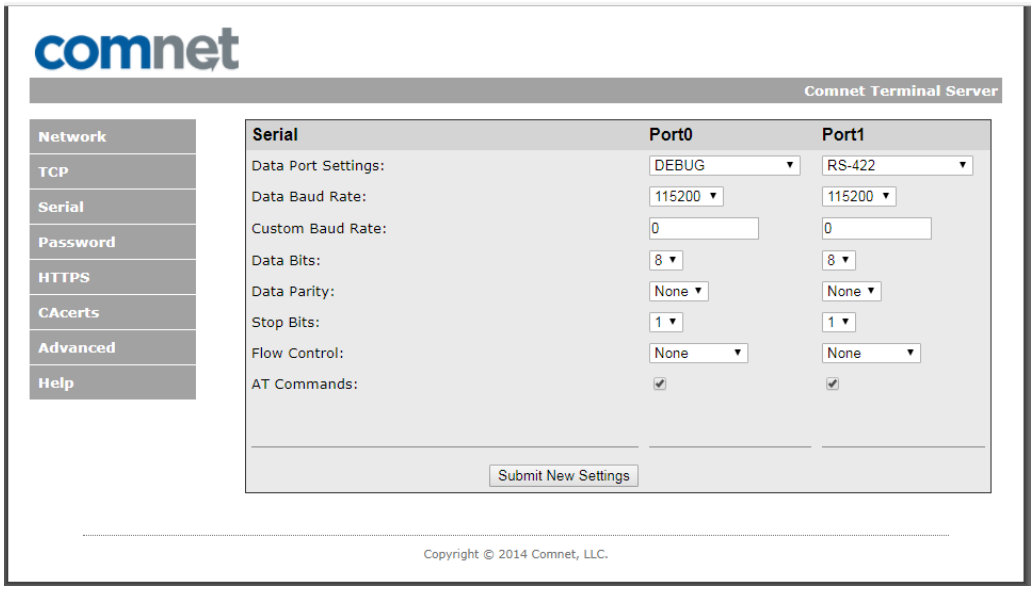


Figure 15 Terminal Server Serial Page

» Click HTTPS link

» Select Choose File and load Certificate "device.crt"

» Select Choose File and load Certificate key "device.key"

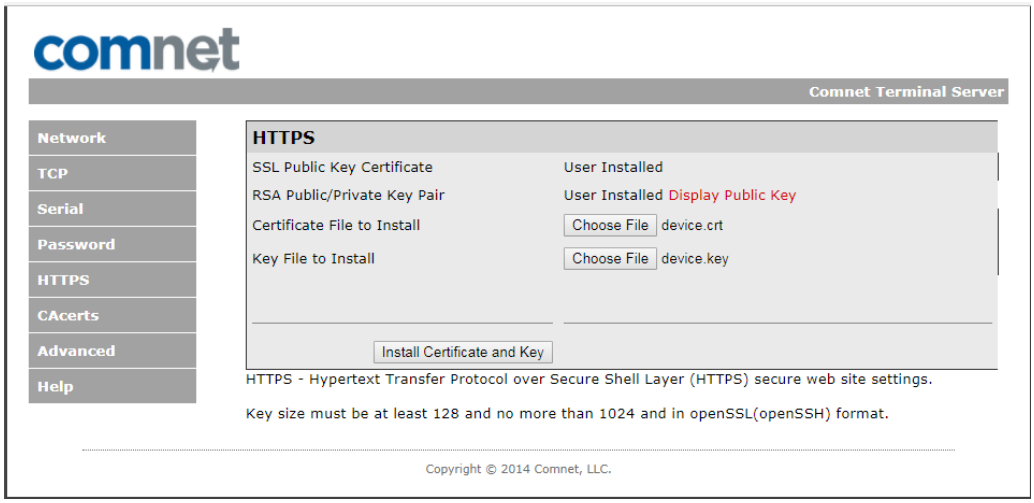


Figure 16 Terminal Server Certificate and key files

» Select Install Certificate and Key

Configure Client

» Set protocol to TCP/SSL on Network page.

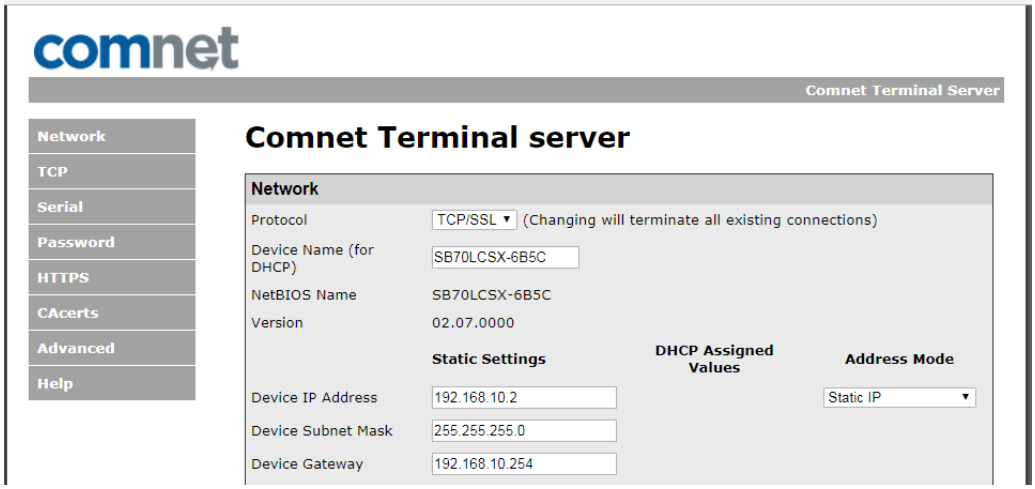


Figure 17 Terminal Client Network Page

» Click TCP link

» Configure Port1 to connect to 192.168.10.1 port 24

» Check "USE SSL rather than TCP for connection"

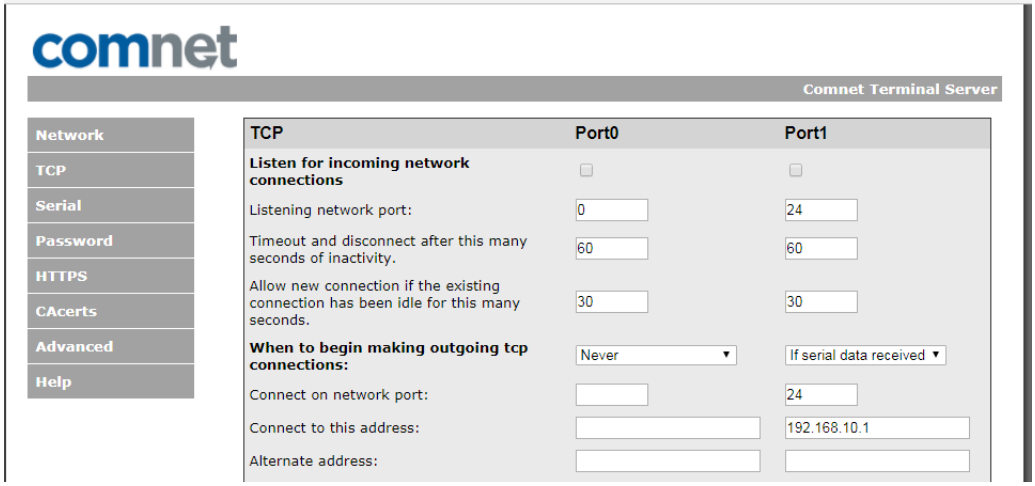


Figure 18 Terminal Client TCP Page

» Click Serial link

» Configure Port1 for RS422

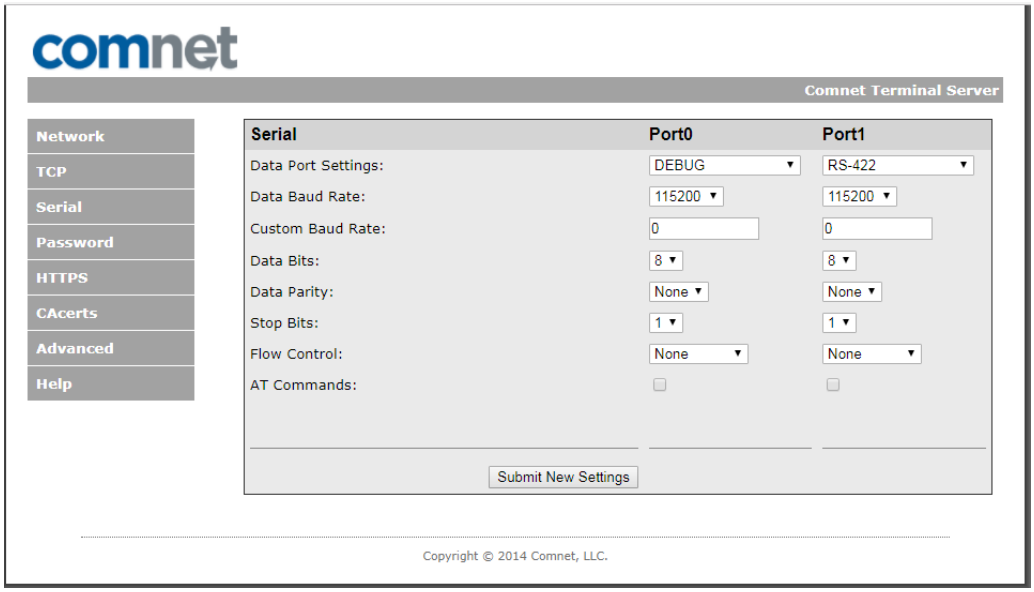


Figure 19 Terminal Client Serial Page

» Click CAcerts link

» Select Choose File and load Certificate "CA.crt"

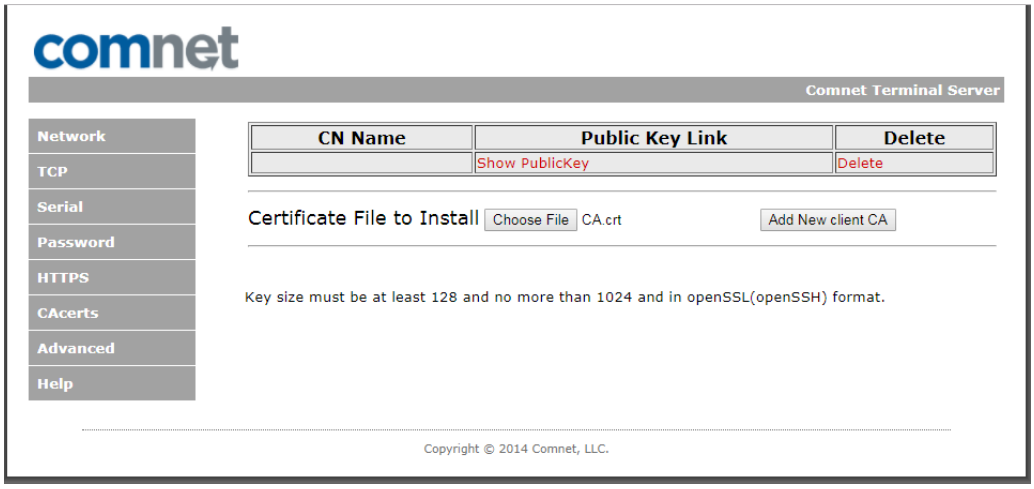


Figure 20 Terminal Client Certificate Authority certificate file

» Select Add New client CA

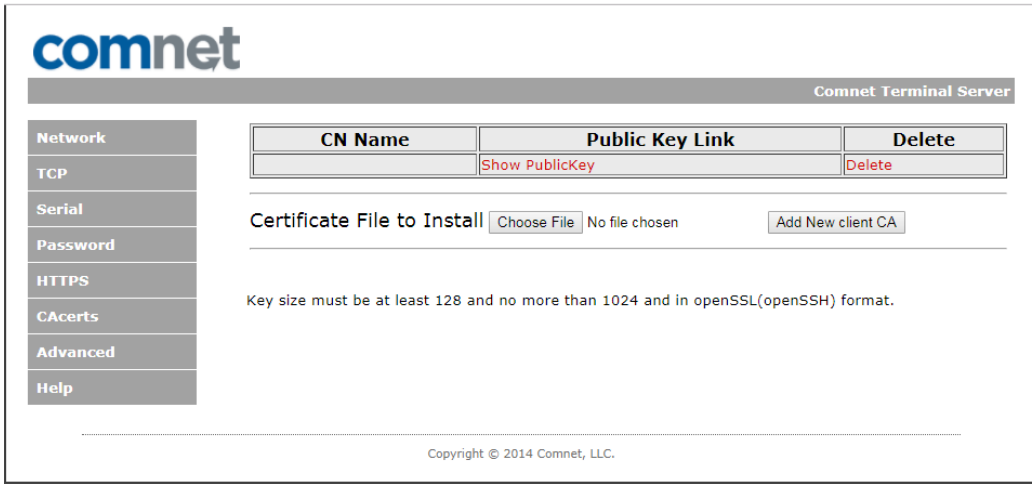


Figure 21 Terminal Client CA Certificate add

Creating openssl certificates

» Open terminal on a Linux machine

Client Certificate

```
development@ubuntu:~/ssl$
development@ubuntu:~/ssl$
development@ubuntu:~/ssl$ openssl genrsa -out CA.key 1024
Generating RSA private key, 1024 bit long modulus
.....................................................................................++++++
.....................++++++
e is 65537 (0x10001)
development@ubuntu:~/ssl$ openssl req -new -key CA.key -x509 -days 365 -out CA.crt
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:California
Locality Name (eg, city) []:SanDiego
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Comnet
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:192.168.10.2
Email Address []:
development@ubuntu:~/ssl$ ls -l
total 8
-rw-rw-r-- 1 development development 940 Feb  6 09:29 CA.crt
-rw-rw-r-- 1 development development 887 Feb  6 09:26 CA.key
development@ubuntu:~/ssl$
```

Figure 22 Client Self Signed Certificate

Server Certificate

```
development@ubuntu:~/ssl$
development@ubuntu:~/ssl$ openssl genrsa -out device.key 1024
Generating RSA private key, 1024 bit long modulus
......++++++
...++++++
e is 65537 (0x10001)
development@ubuntu:~/ssl$
development@ubuntu:~/ssl$ openssl req -new -key device.key -out device.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:California
Locality Name (eg, city) []:San Diego
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Comnet
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:192.168.10.1
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
development@ubuntu:~/ssl$
development@ubuntu:~/ssl$ openssl x509 -req -days 365 -in device.csr -CA CA.crt -CAkey CA.key -CAcreateserial -out device.crt
Signature ok
subject=/C=US/ST=California/L=San Diego/O=Comnet/CN=192.168.10.1
Getting CA Private Key
development@ubuntu:~/ssl$
```

Figure 23 Server Self Signed Certificate

```
development@ubuntu:~/ssl$
development@ubuntu:~/ssl$ ls -l
total 24
-rw-rw-r-- 1 development development 940 Feb  6 09:29 CA.crt
-rw-rw-r-- 1 development development 887 Feb  6 09:26 CA.key
-rw-rw-r-- 1 development development  17 Feb  6 09:39 CA.srl
-rw-rw-r-- 1 development development 822 Feb  6 09:39 device.crt
-rw-rw-r-- 1 development development 639 Feb  6 09:36 device.csr
-rw-rw-r-- 1 development development 887 Feb  6 09:34 device.key
development@ubuntu:~/ssl$
development@ubuntu:~/ssl$
```

Figure 24 Client and Server Certificates & keys

SSH Transport

To use the Terminal Server to connect a serial device over Ethernet utilizing SSH, connect a terminal server and a laptop to your local Ethernet network configuring both devices as a client server connection.

Configure Server

» Set protocol to SSH on Network page.

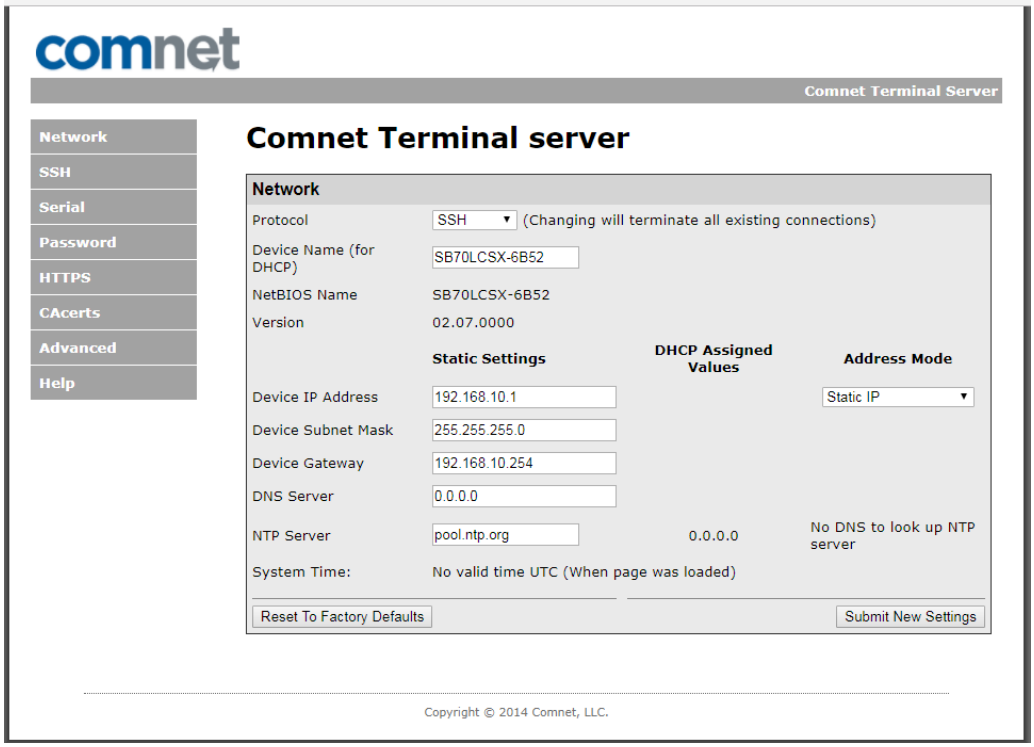


Figure 25 Terminal Server Network Page

» Click SSH link

» Configure Port1 to listen for incoming connections on port 22

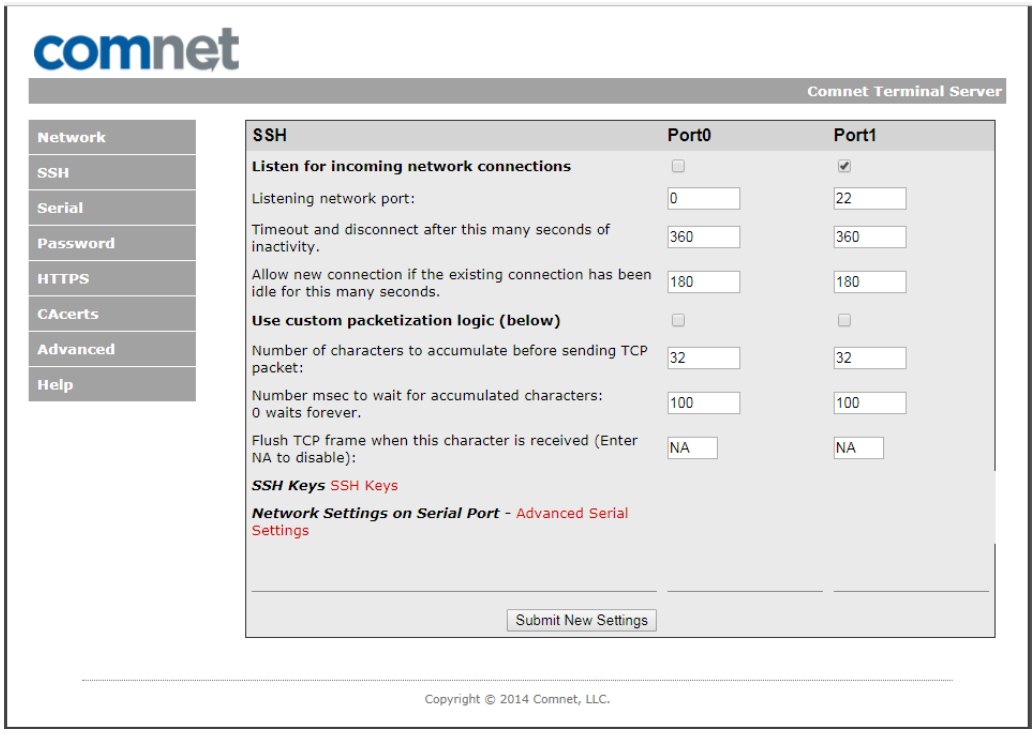


Figure 26 Terminal Server SSH Page

» Click SSH Keys link

» Click Choose File and select ssh rsa key pair "id_rsa"

» Click Install Key

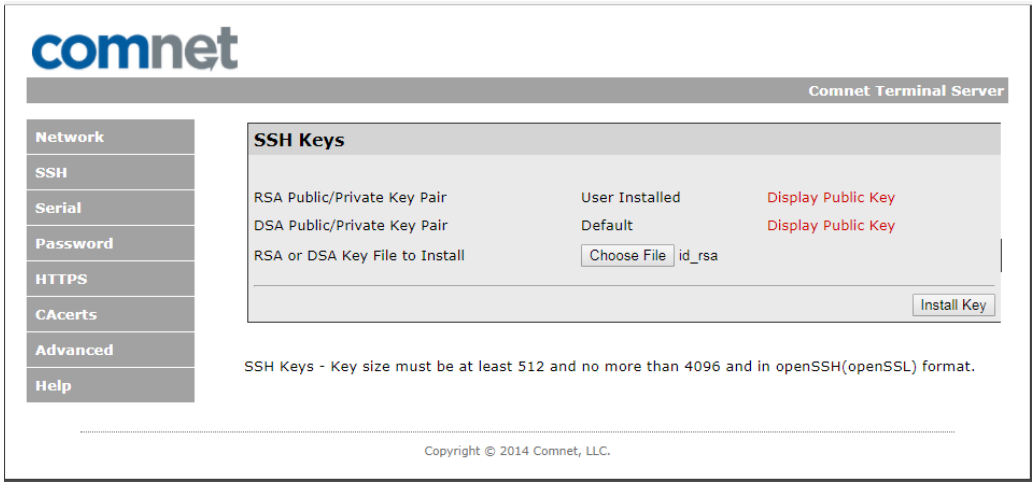


Figure 27 Terminal Server Keys Page

» Click Serial link

» Configure Port1 for RS422

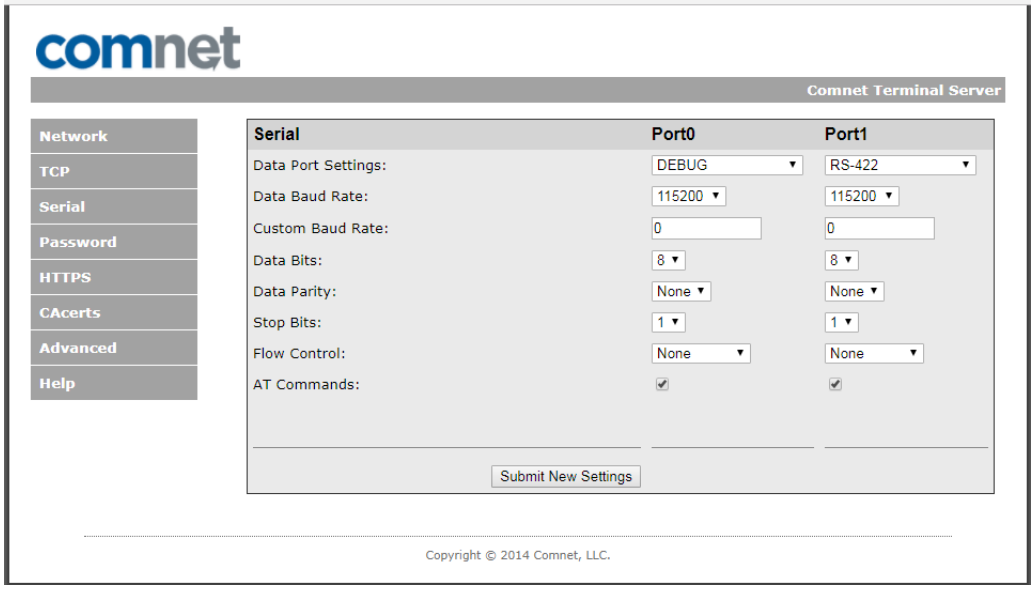


Figure 28 Terminal Server Serial Page

Configure Client Laptop

» Open Tera Term and select SSH and TCP port 22

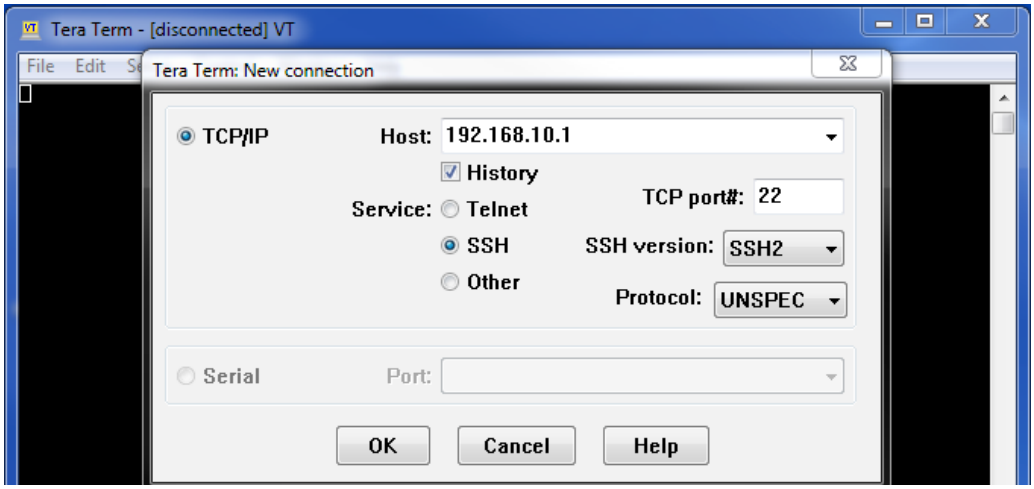


Figure 29 Terminal Client Tera Term

» On SSH Authentication Pop Up click RSA and select Private key file id_rsa

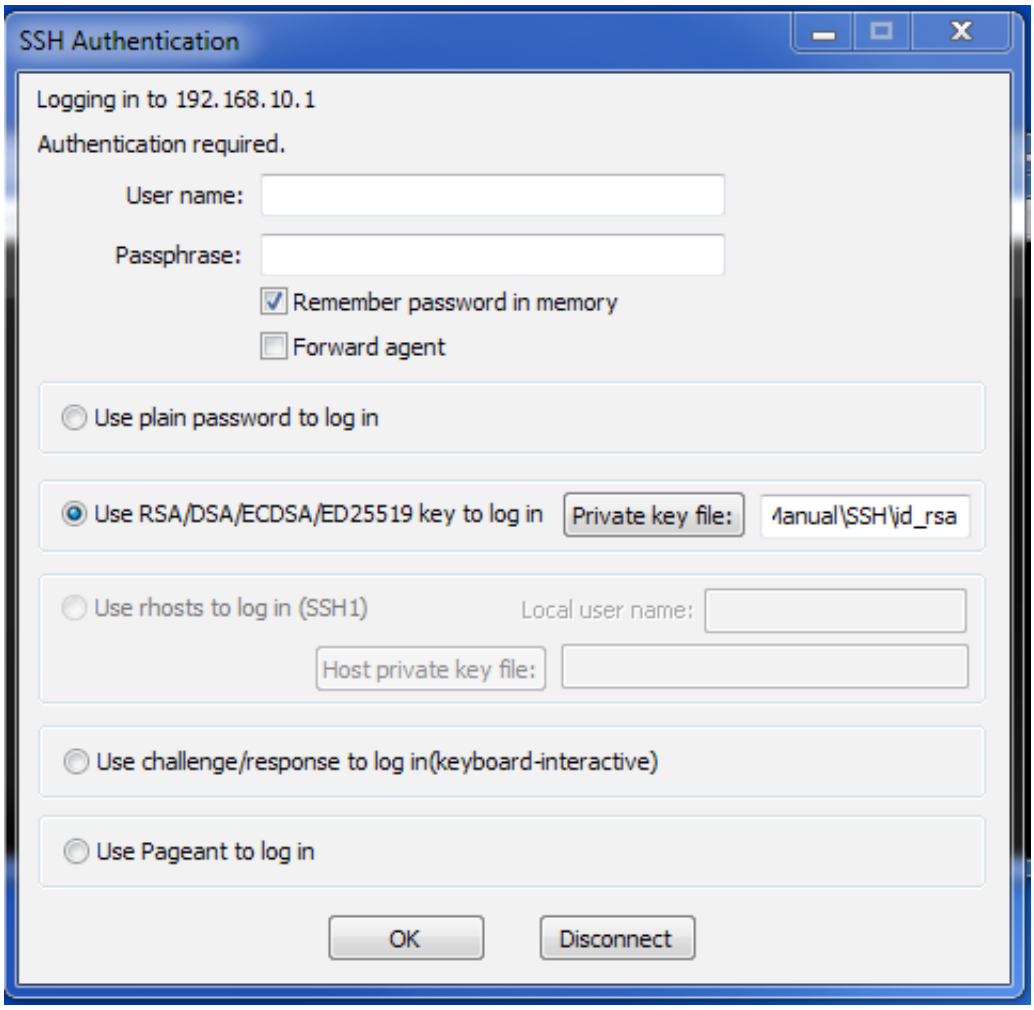


Figure 30 Terminal Client Tera Term SSH Authentication

Creating SSH key pairs

Open terminal on a linux machine

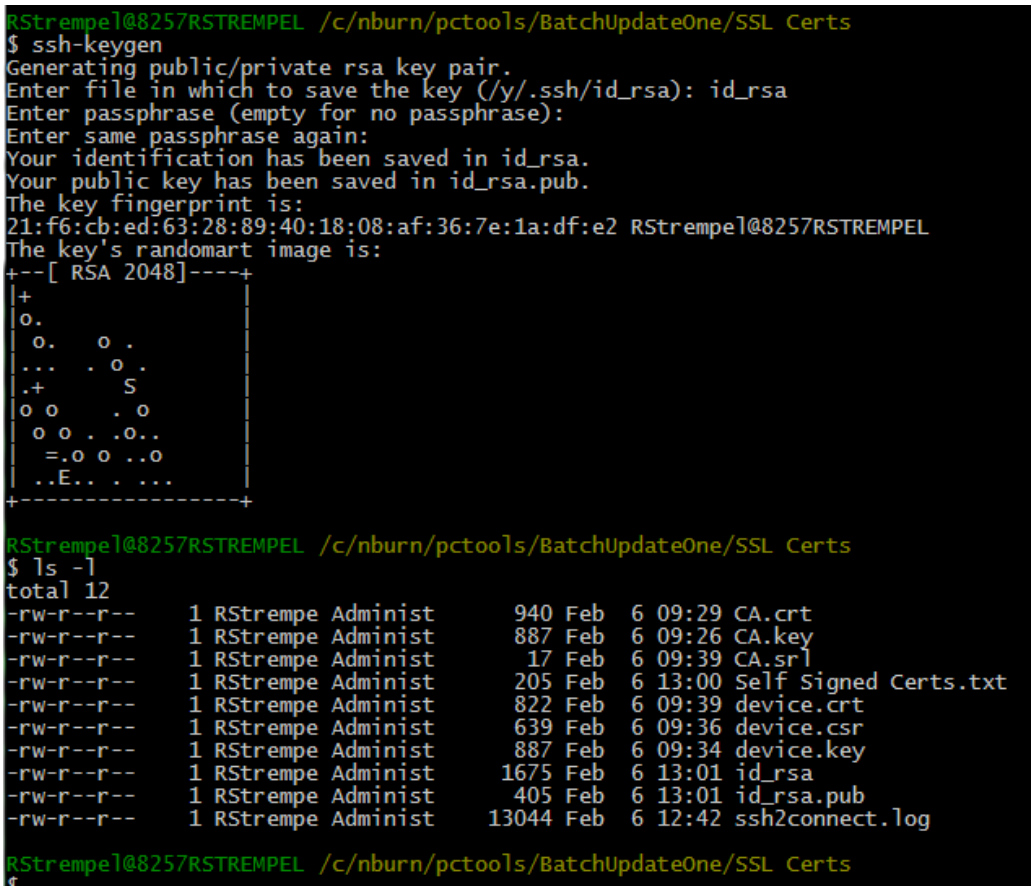


Figure 31 Creating SSH key pairs

Telnet Transport

To use the Terminal Server to connect a serial device over Ethernet utilizing Telnet, connect a terminal server and a laptop to your local Ethernet network configuring both devices as a client server connection.

Configure Server

» Set protocol to TCP on Network page.

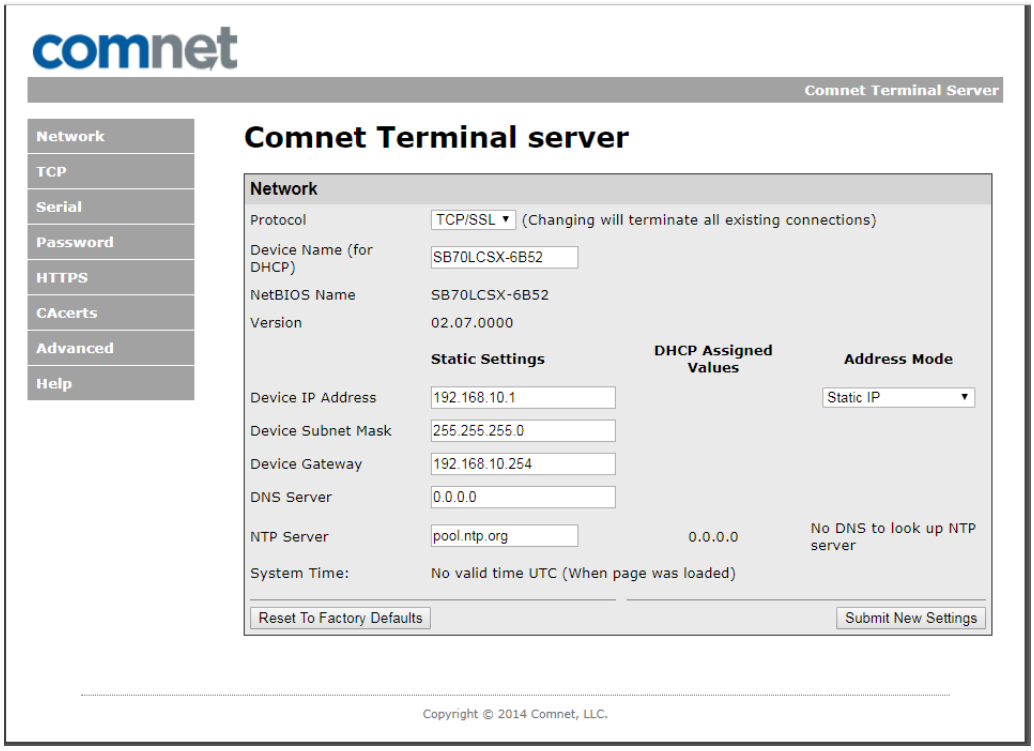


Figure 32 Terminal Server Network Page

» Click TCP link

» Configure Port1 to listen for incoming connections on port 24

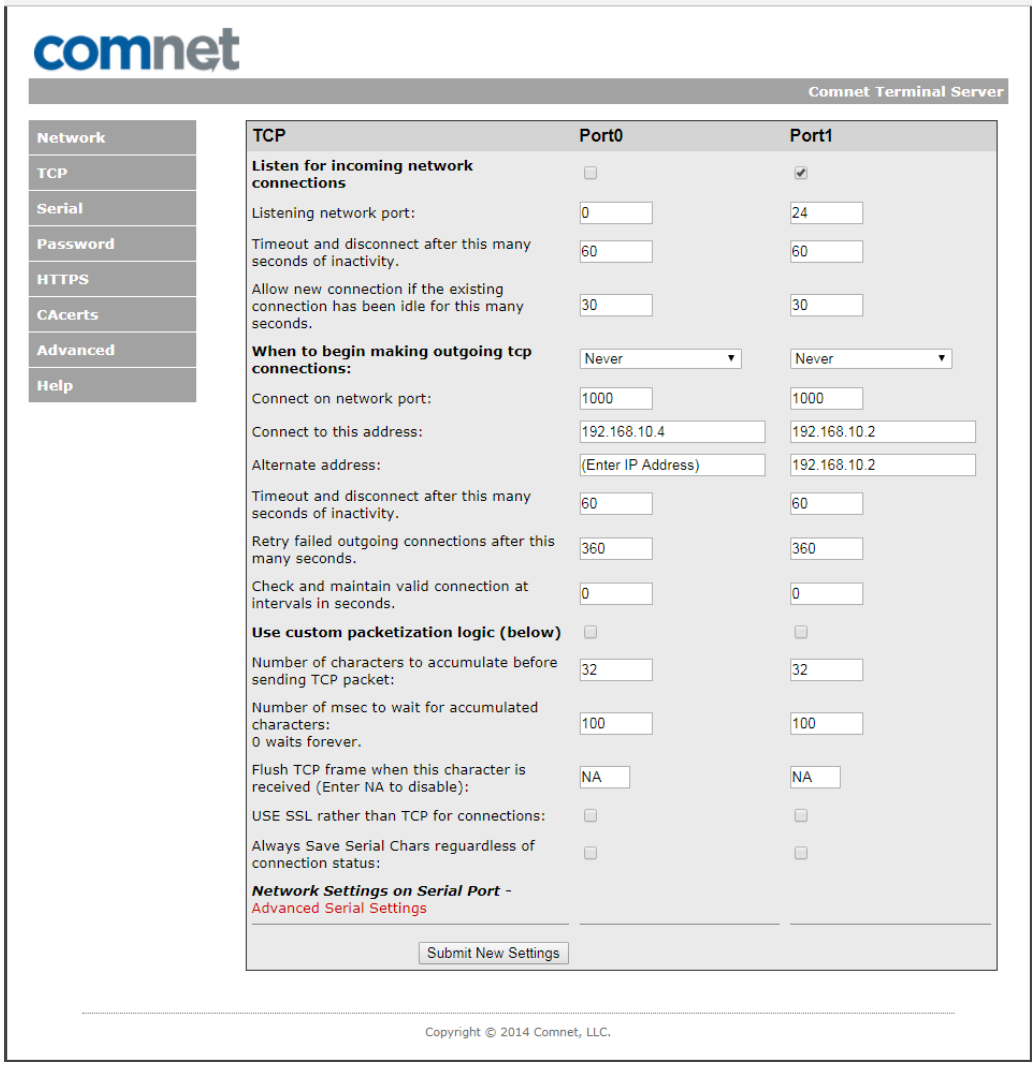


Figure 33 Terminal Server TCP Page

» Click Serial link

» Configure Port1 for RS422

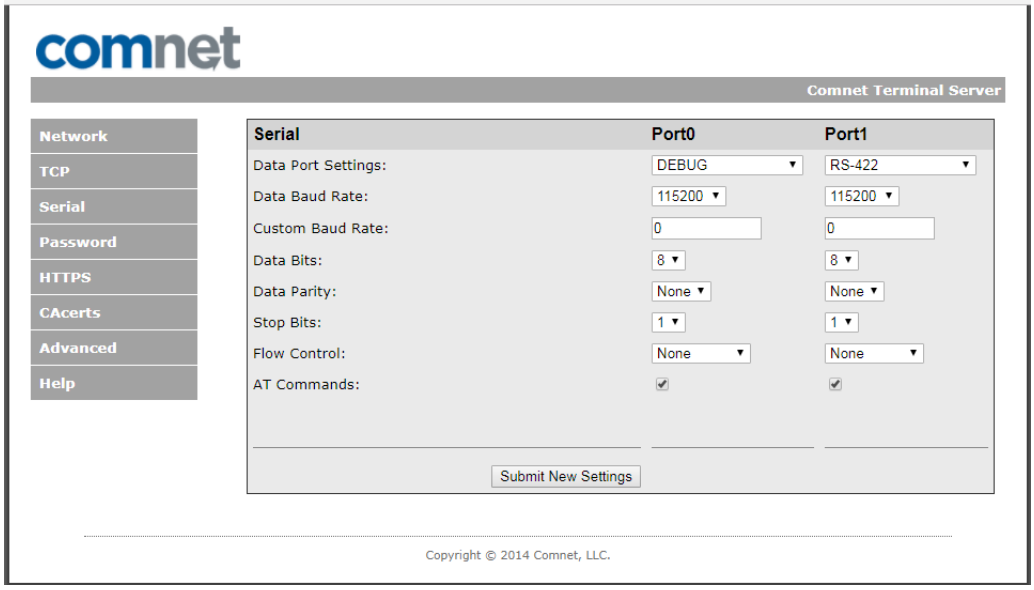


Figure 34 Terminal Server Serial Page

Configure Client Laptop

» Open Tera Term and select Telnet and TCP port 24

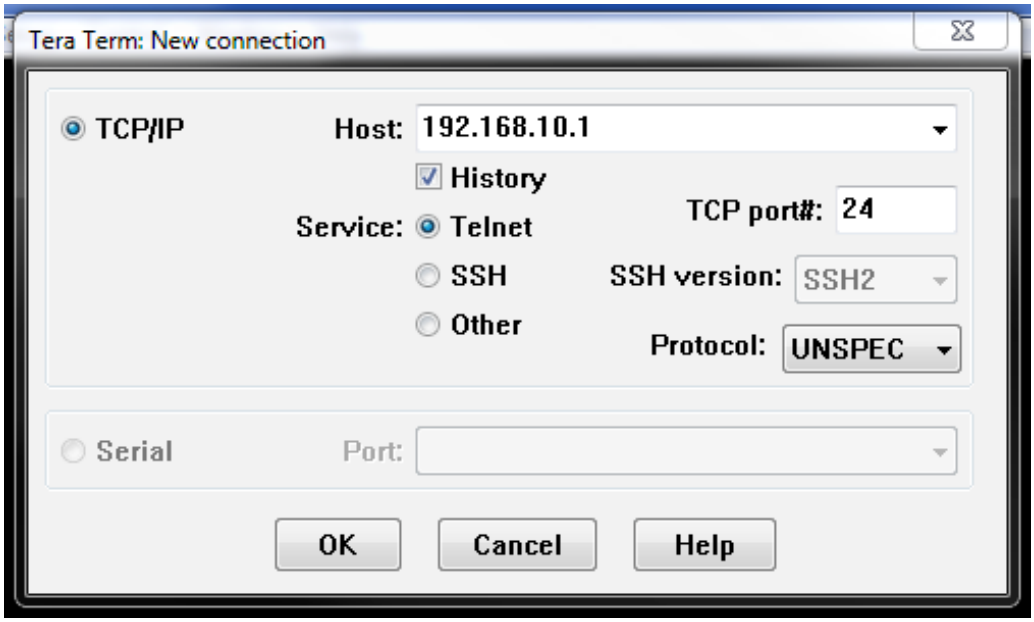


Figure 35 Terminal Client Tera Term

HTTPS Configuration

» Click HTTPS
» Select Certificate File to Install Choose File “device.crt”
» Select Key File to Install. Choose File “device.key”
» Click Install Certificate and Key

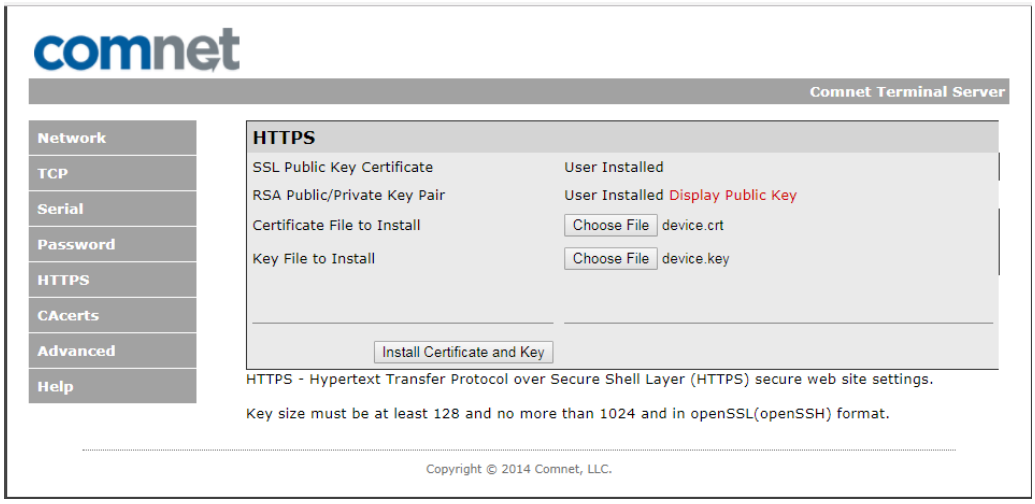


Figure 36 Terminal Server Certificate and Key files

Internet Explorer Configuration

» Click on tools and select Internet options

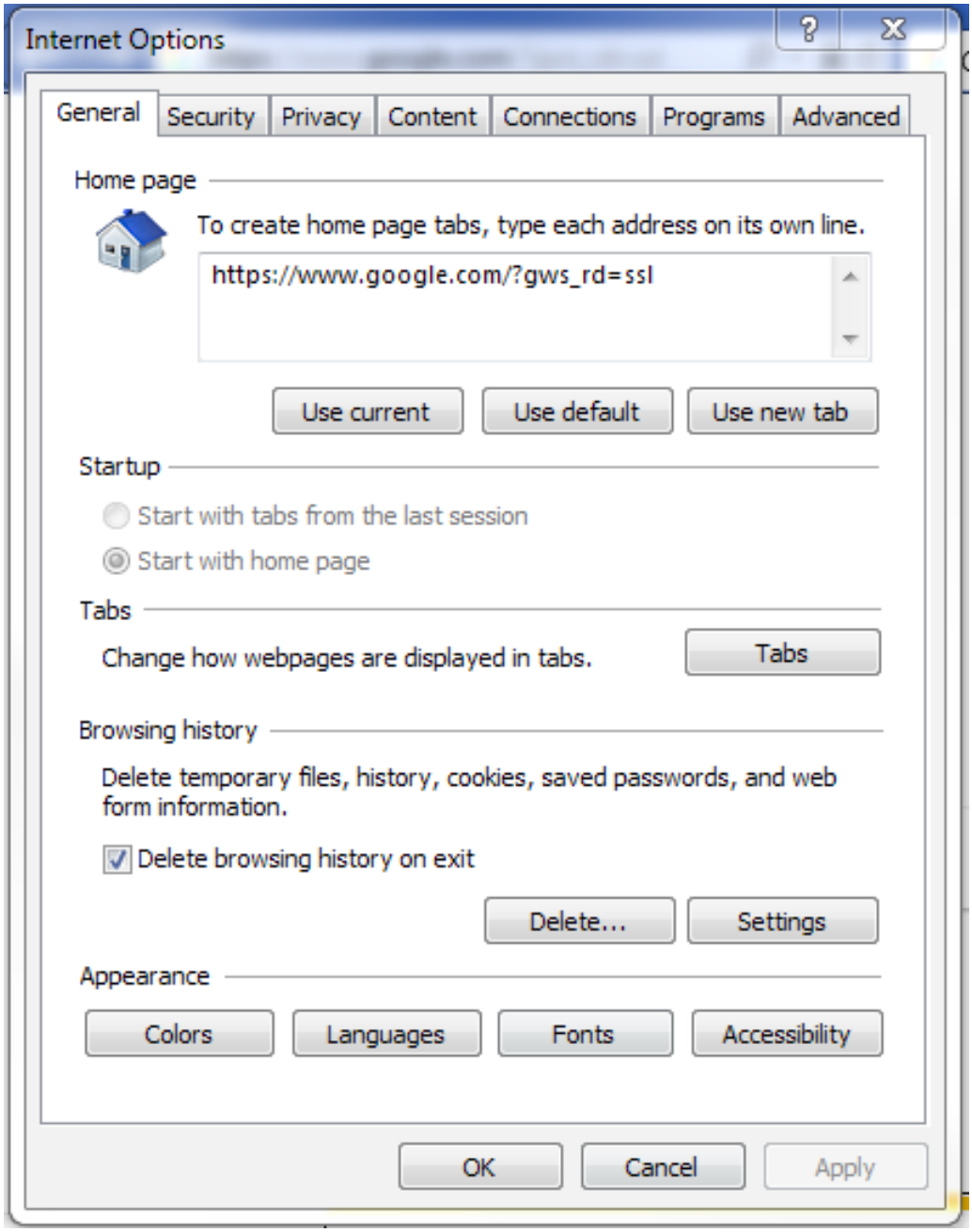


Figure 37 Terminal Client IE Options

» Click Content tab and click Certificates

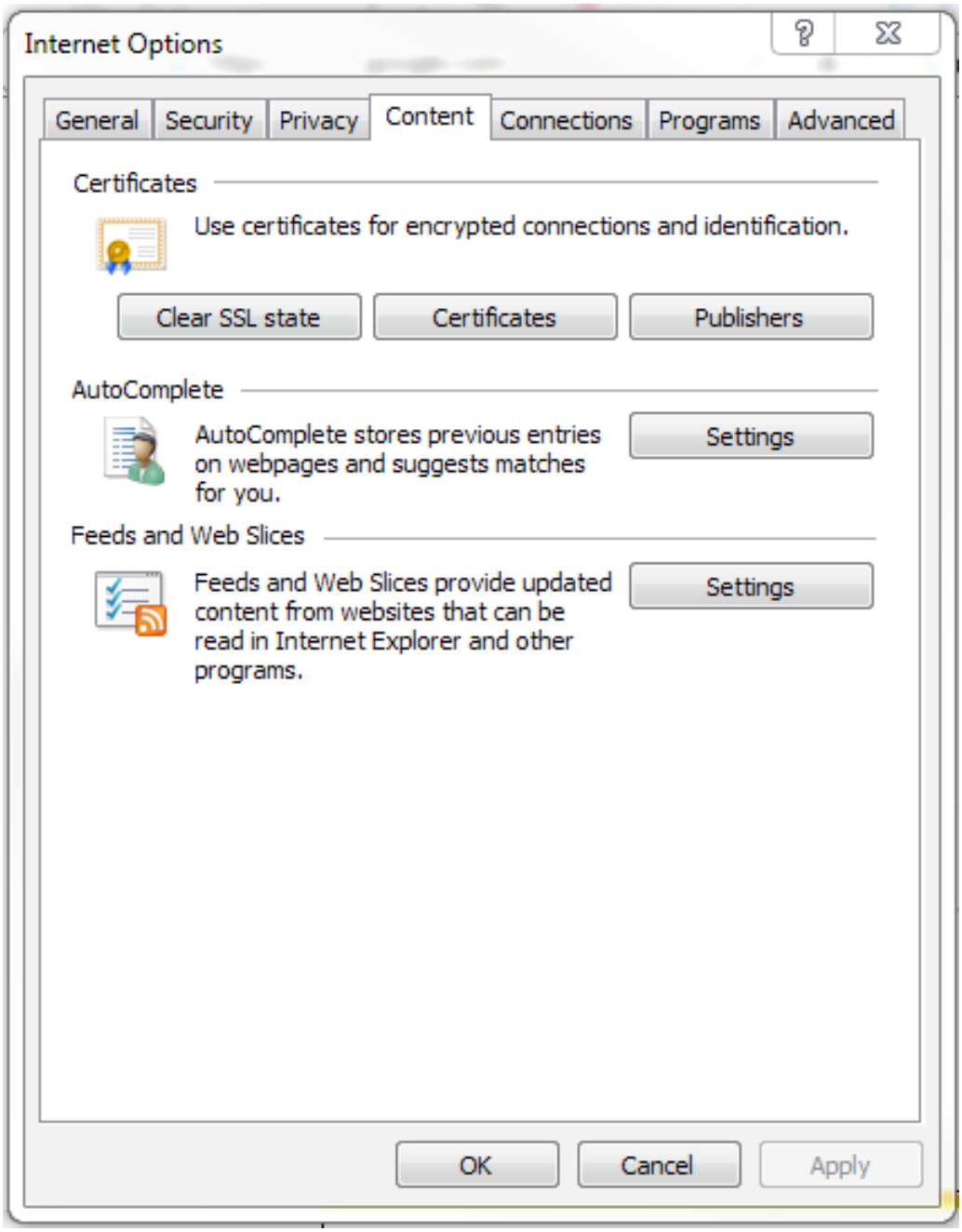


Figure 38 Terminal Client IE Certificates

» Click Trusted Root Certifications Authority tab

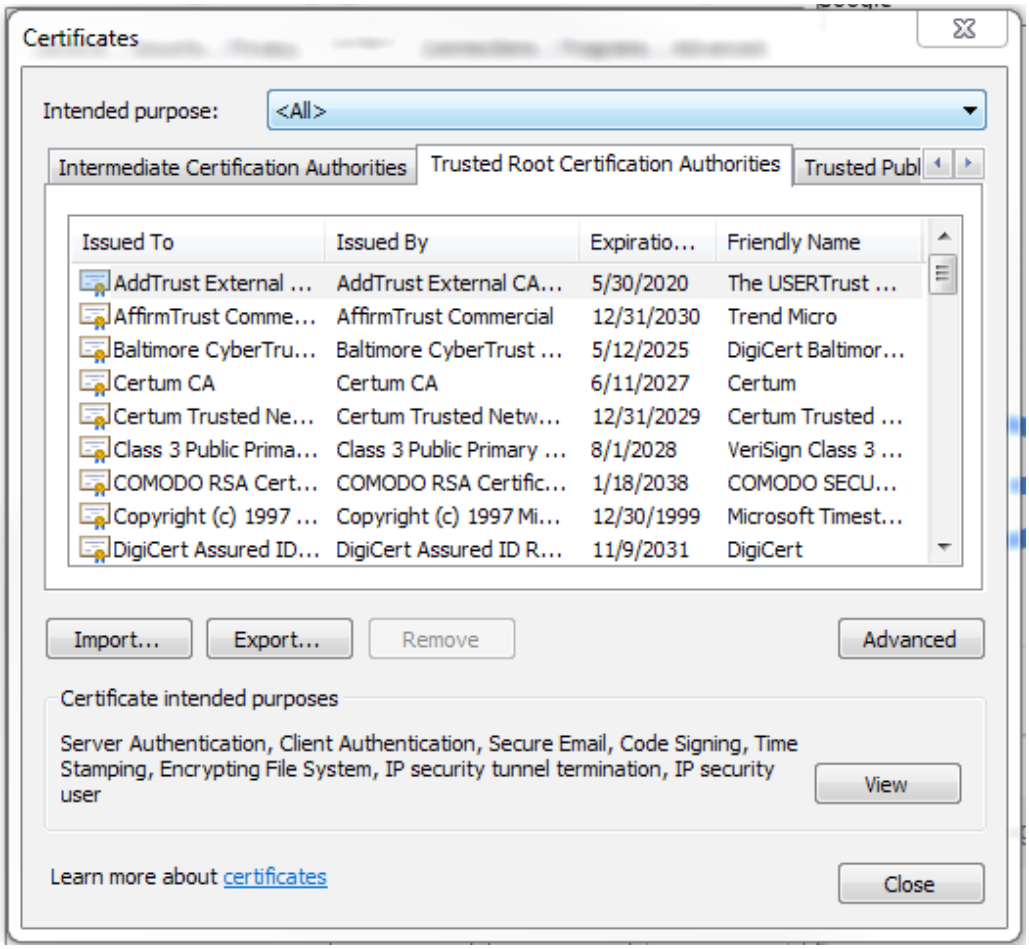


Figure 39 Terminal Client IE Root CA

» Click Import…

» Use wizard to load CA certificate “CA.crt”

» Place in Trusted Root Certification Authorities

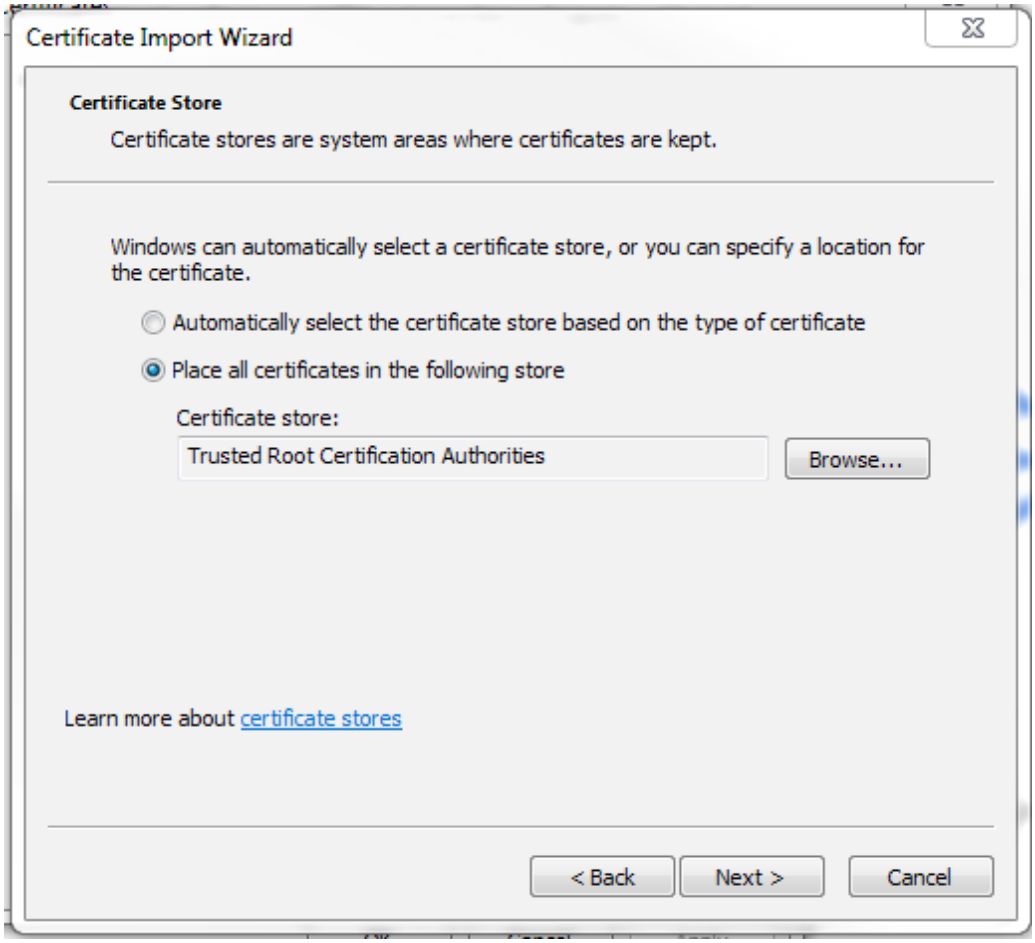


Figure 40 Terminal Client IE Certificate Store

» Finish wizard and close Internet Explorer

» Terminal Server is now accessible using HTTPS with Internet Explorer

FireFox Configuration

» Click on tools and select options

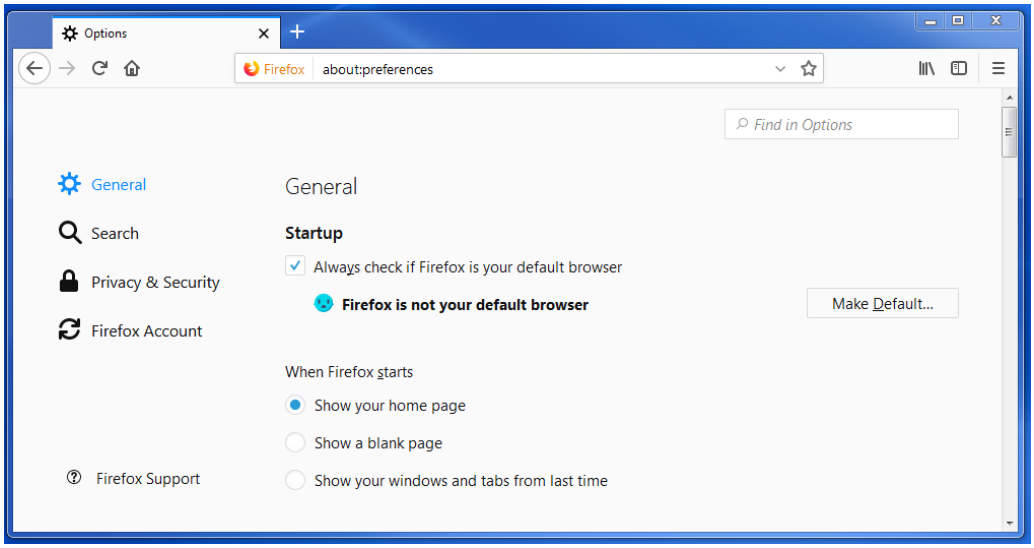


Figure 41 Terminal Client FireFox Options

» Click Privacy & Security

» Click View Certificates

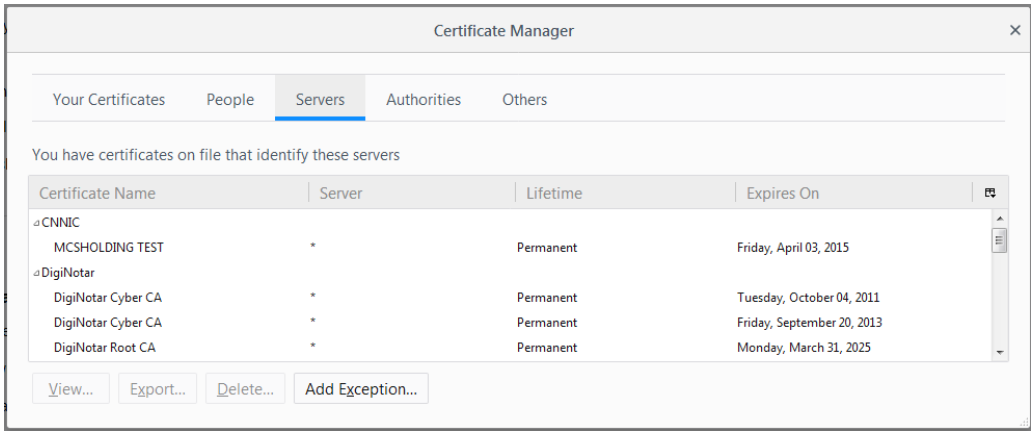


Figure 42 Terminal Client FireFox Certificate MGR

» Click Servers and Add Exception

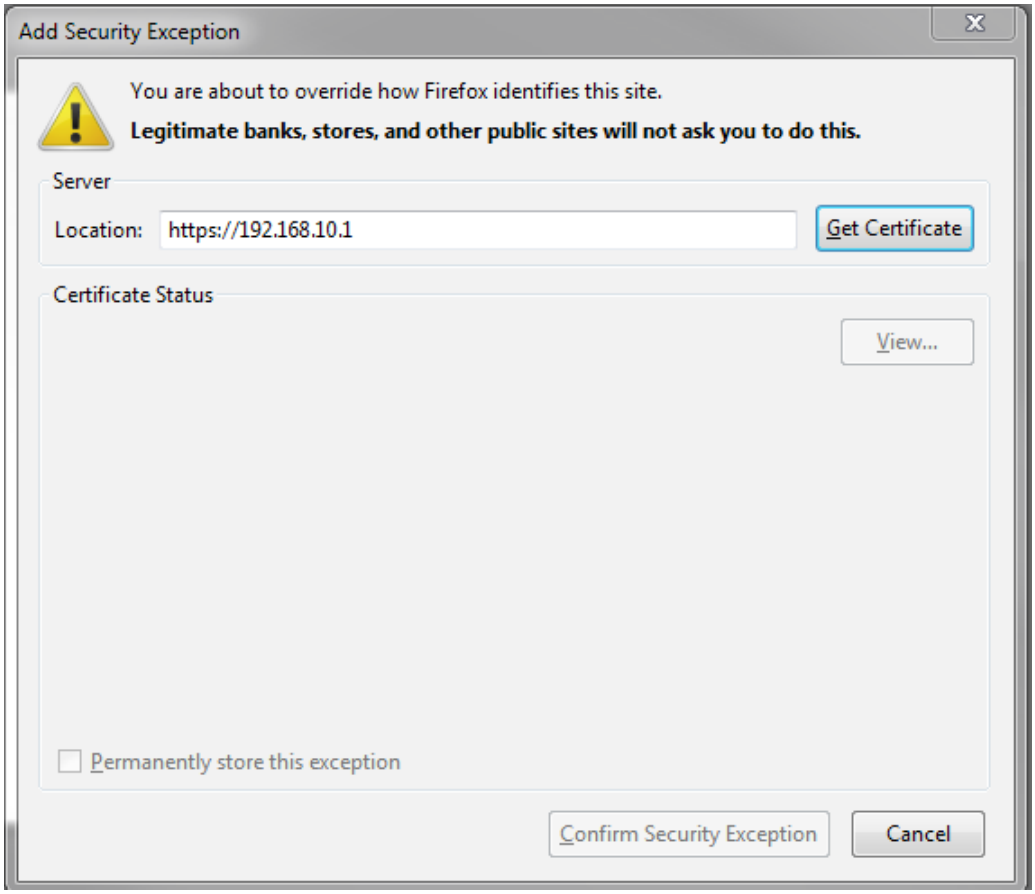


Figure 43 Terminal Client FireFox Exception

» Click Get Certificate

» Click Confirm Security Exception

» Close FireFox

» Terminal Server is now accessible using HTTPS with FireFox

OpenSSL Certificate, key and CA for HTTPS

» Use same SSL certificates

Console Port Access

One serial port may be designated as a console port using USB to RS232 cable. The console port may be used to view and change the IP address as well as access other system information. Debug mode will not forward any serial data but is only used to access the terminal server host.

» Click Serial Link

» Configure Port0 for Debug

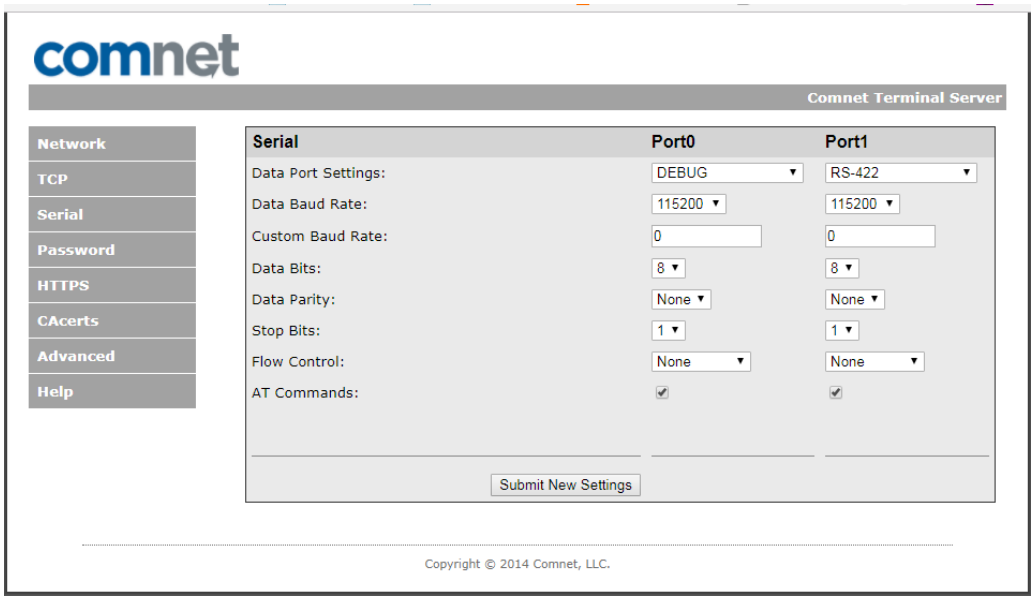


Figure 44 Terminal Server Serial Page

ComNet Customer Service
Customer Care is ComNet Technology's global service center, where our professional staff is ready to answer your questions at any time.

Email ComNet Global Service Center: customercare@comnet.net

comnet
Communication Networks

3 CORPORATE DRIVE | DANBURY, CT 06810 | USA
T: 203.796.5300 | F: 203.796.5303 | TECH SUPPORT: 1.888.678.9427 | INFO@COMNET.NET

8 TURNBERRY PARK ROAD | GILDERSOME | MORLEY | LEEDS, UK LS27 7LE
T: +44 (0)113 307 6400 | F: +44 (0)113 253 7462 | INFO-EUROPE@COMNET.NET