

Sena Device Server and Serial/IP Application Guide

Version 1.0.0

2005. 3. 7.

Revision History

Revision	Date	Name	Description
V1.0.0	2005-04-21	Kumar	Serial/IP 4.3.2 Guide

Technical Support

Sena Technologies, Inc.

210 Yangjae-dong, Seocho-gu

Seoul 137-130, Korea

Tel: (+82-2) 573-5422

Fax: (+82-2) 573-7710

E-Mail: support@sena.com

Website: <http://www.sena.com>

Table of Contents

1. Serial/IP	5
1.1 Overview.....	5
1.2 Application Diagram	5
1.3 Screenshot	6
1.4 Operation Modes	7
1.4.1 Client Mode.....	7
1.4.2 Server Mode	7
1.4.3 Server & Client Mode	7
2. Serial/IP Client Mode Operation	7
2.1 RawTCP Operation Mode	7
2.1.1 Supported Models	7
2.1.2 Configuration in the Sena Product	7
2.1.3 Configuration in the Serial/IP	8
2.1.4 Operation	10
2.2. VirtualCOM Operation Mode	12
2.2.1 Supported Models	12
2.2.2 Setting in the Sena Device Server	12
2.2.3 Serial/IP Configuration	13
2.2.4 Sample Application.....	13
3. Serial/IP Server Operation Mode.....	15
3.1 RawTCP Operation Mode	15
3.1.1 Supported Products.....	15
3.1.2 Sena Device Server configuration.....	15
3.1.3 Serial/IP setup.....	15
3.1.4 Operation	16
4. SSL Security features	17
4.1 SSL Data Transfer without certificate.....	17
4.1.1 Supported Models	17
4.1.2 Cryptography configuration.....	17
4.1.3 SSL Security configuration options in Serial/IP	18
4.1.4 Operation	18
4.2 SSL Data Transfer using certificate.....	20
4.2.1 Supported Models	20
4.2.2 Sena Device Server Configuration	20

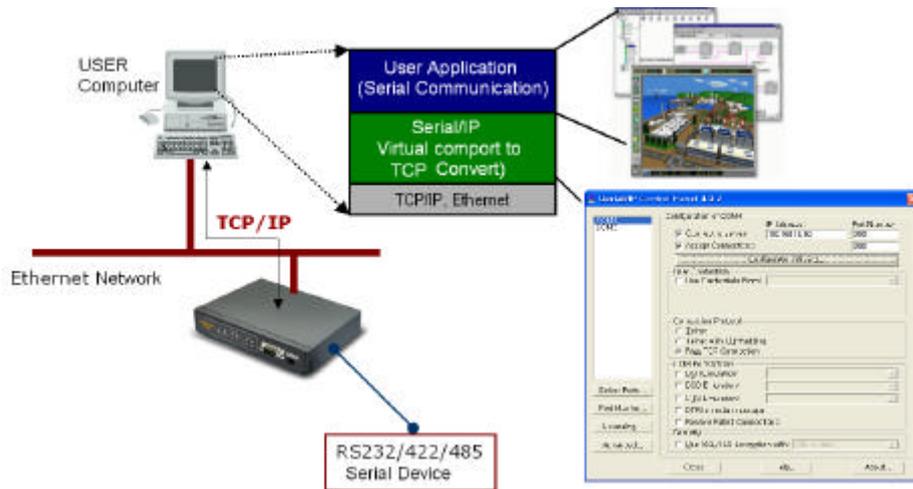
4.2.3 Configuring the Encryption feature.....	21
4.2.4 Operation	25
5. Appendix.....	26

1. Serial/IP

1.1 Overview

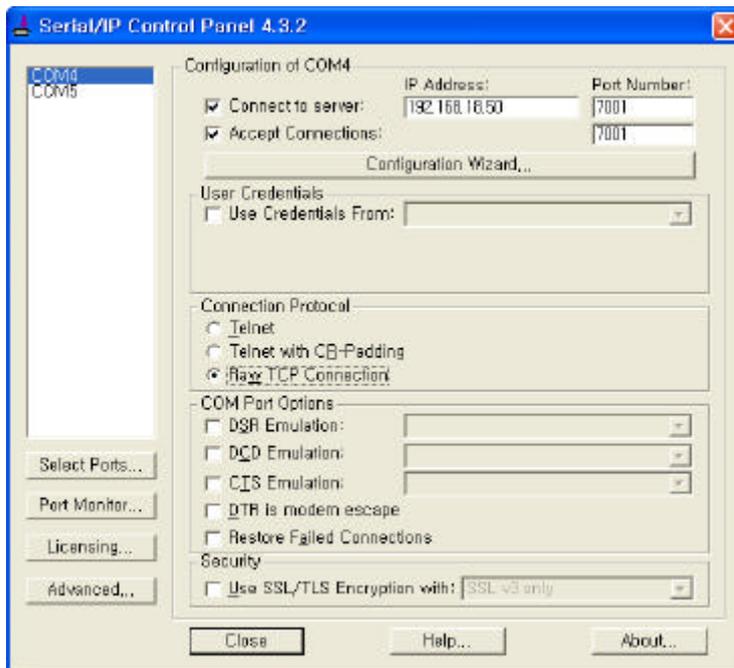
Sena bundles Serial/IP™ from Tactical Software as standard COM Port Redirector software of Sena products. This software enables your existing serial communication programs that use Windows serial port drivers to be used over the network allowing you to keep using your existing program without any modification. It provides access to the serial ports of the Sena Device Servers from multiple PCs over a TCP/IP network. Serial/IP™ Virtual COM port session works either TCP client mode or server mode and communicates with Sena Device Servers accordingly.

1.2 Application Diagram



1. Connect a Sena Device Server and PC on your network.
2. Configure the Sena Device Server to make its serial ports available to the network via TCP/IP.
3. Install the Serial/IP Redirector software on the PC that will use devices attached to the Sena Device Server.
4. Configure the Serial/IP Redirector to create one or more Virtual COM ports.
5. For each Serial/IP COM port, specify the IP address of a Sena Device server and the TCP local port number that provides access to its serial ports.
6. In your PC application, change settings to use Serial/IP COM ports instead of local COM ports.
7. Thereafter, your PC application can use serial ports on the Sena Device server instead of local serial ports.

1.3 Screenshot



- Configuration of COM x: Enter the IP address and Local Port number of Sena Device Server when working in Client mode.
- Accept Connections: Enter the listening port number when working in Server mode.
- Configuration Wizard: The Configuration Wizard determines whether the Serial/IP Redirector can communicate with the Sena Device server using the following settings for a Serial/IP COM port: IP Address of Server, TCP Port Number and Credentials.
- Connection Protocol: Set the TCP/IP protocol that Sena Device Server uses for communication.
- COM port Option: These settings allow control of the respective signals as presented to the user application by the redirector.
- Security: Set the Security protocol
- Select Port: Allows user to create or delete of Virtual COM Ports.
- Port Monitor: User can monitor the data communication between user application and Sena Device Server.
- Licensing: License information of Serial/IP software that Sena bundles.
- Advanced: The Advanced button opens a dialog for settings of specialized features such as SSL Encryption, SSL Authentication, and SSL Certificate.

Note: For more information on Serial/IP installation, please refer the Serial/IP user manual.

1.4 Operation Modes

1.4.1 Client Mode

Check the "Connect to Server" option.

Enter the IP address and Local Port number of the Sena Device Server.

If users open Virtual COM port created and send data, it tries to connect to the specified IP address: TCP port and to transfer data accordingly.

1.4.2 Server Mode

Check the "Accept Connection" option.

Enter the listening TCP port number.

If users open Virtual COM port created, then it waits the incoming connection at TCP port specified listening port.

1.4.3 Server & Client Mode

If the Server & Client Mode is selected in the Sena Device Server, users should input the IP address, Server port number and Listening port number.

If users open Virtual COM port created and send data, it tries to connect to the specified IP address: TCP port and to transfer data accordingly. If users open Virtual COM port created, then it waits the incoming connection at TCP port specified listening port.

2. Serial/IP Client Mode Operation

2.1 RawTCP Operation Mode

Raw TCP Connection is used to communicate with a Sena Device Server without any additional protocols.

2.1.1 Supported Models

LS, NEMO, PS, SS, and STS

2.1.2 Configuration in the Sena Product Example

- Host Mode: TCP Server Mode (Default Port 7001 or 6001)
- In case of the SS/STS products, users don't have to specify the host mode. If it is configured as "TCP", then everything is done accordingly.

Host mode configuration	
Host mode :	TCP
TCP listening port (1024-65535, 0 for only outgoing connections) :	7001
Telnet protocol :	Disabled
Max. allowed connection (1-32) :	32
Cyclic connection to remote hosts (sec, 0 : disable) :	0
Inactivity disconnection timeout (sec, 0 : unlimited) :	0
<input type="button" value="Save to flash"/> <input type="button" value="Save & apply"/> <input type="button" value="Cancel"/>	

2.1.3 Configuration in the Serial/IP Example

Serial/IP Control Panel 4.3.2

Configuration of COM4

IP Address: 192.168.18.50 Port Number: 7001

Connect to server: Accept Connections:

Configuration Wizard...

User Credentials

Use Credentials From: [Dropdown]

Connection Protocol

Telnet
 Telnet with CR-Padding
 Raw TCP Connection

COM Port Options

DSR Emulation: Always High
 DCD Emulation: Always Low
 CIS Emulation: Track Connection
 DTR is modem escape
 Restore Failed Connections

Security

Use SSL/TLS Encryption with: SSL v3 only

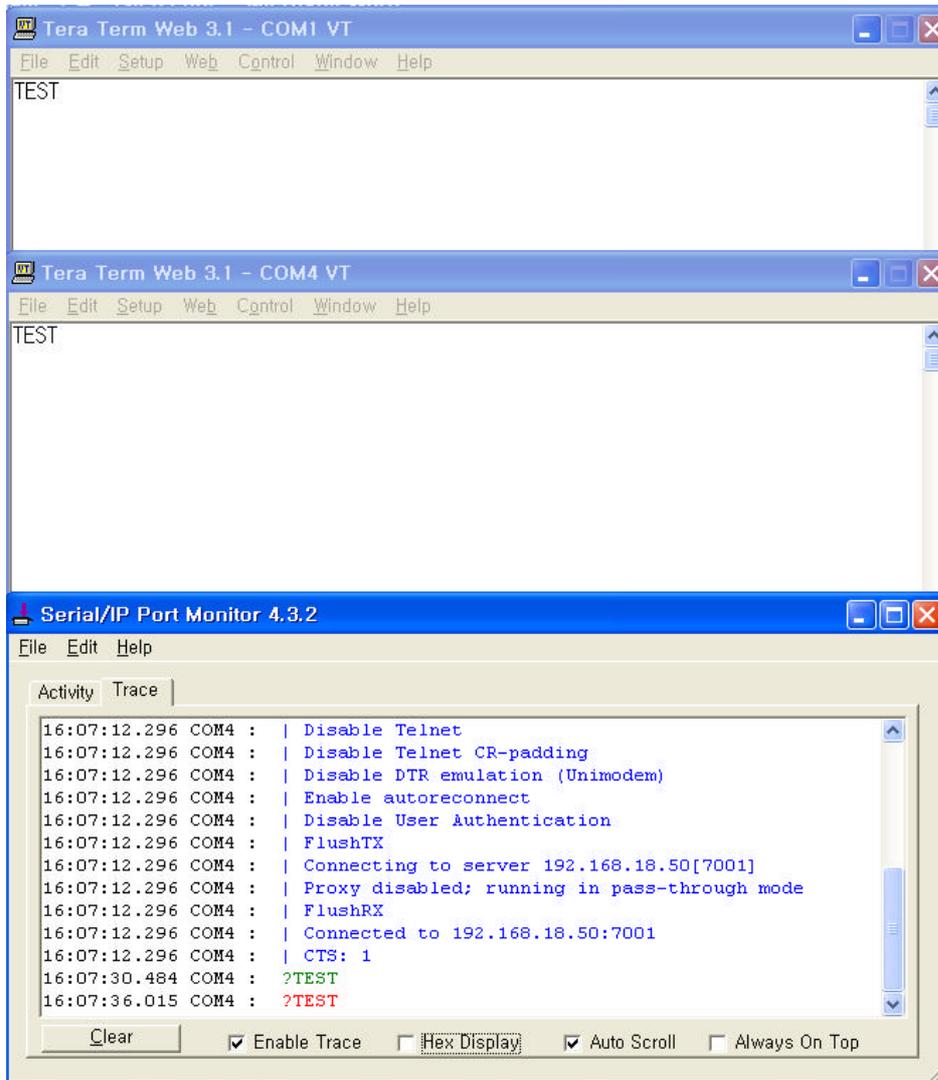
Buttons: Select Ports..., Port Monitor..., Licensing..., Advanced..., Close, Help..., About...

- Connect to server: IP address and Port number of the connected Sena Device Server is 192.168.18.50: 7001.
- Connection Protocol: Connection Protocol has been set to Raw TCP.

- DSR/DCD/CTS Emulation: These settings allow control of the respective signals as presented to the application by the redirector.
- Restore Failed Connections: When this option is enabled, a dropped TCP connection will cause the Serial/IP Redirector to automatically attempt to reconnect to the Sena Device server.

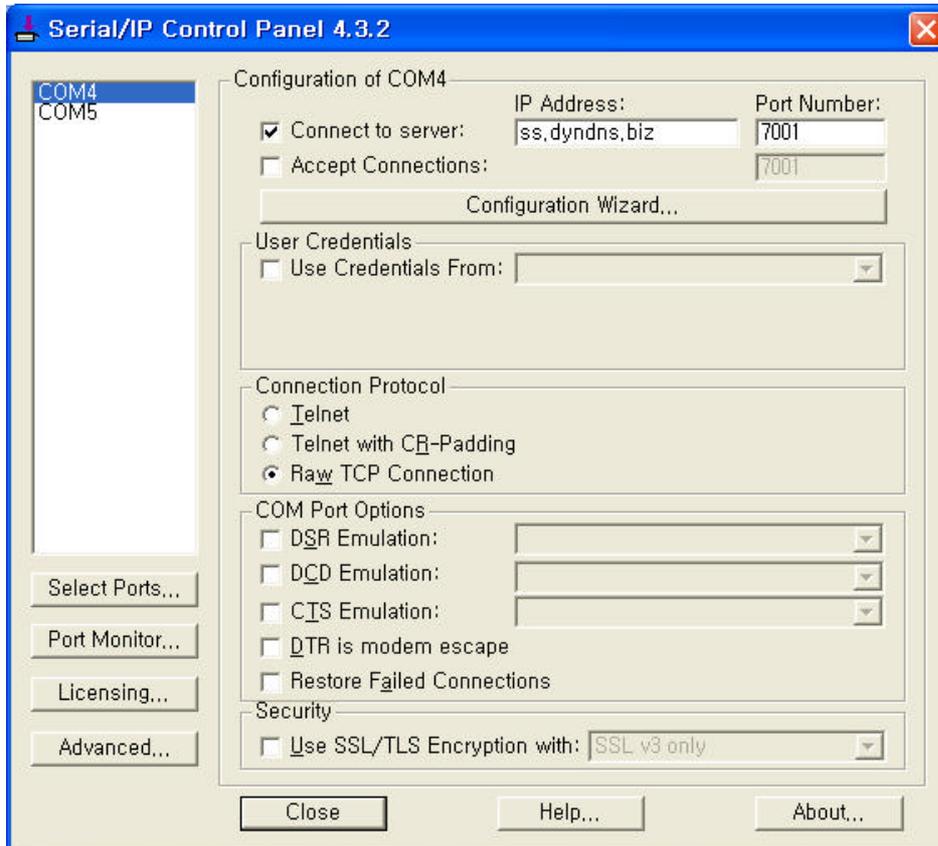
2.1.4 Operation

- After opening a Virtual COM Port in the user application, Serial/IP will start communication with Sena Device Server.
- User can monitor or trace the connection status using Serial/IP Port Monitor or Trace window.
- Client mode is useful when user application is initiating the communication.



Note:

When using the Serial/IP in client mode, user application needs to know the IP of the Sena Device Server. In this scenario, if the users network environment is DHCP, the IP address might be changed whenever it reconnects to the network. Sena Device Server supports Dynamic DNS Protocol that enables user to access the Sena Device Server via a domain name.



2.2. VirtualCOM Operation Mode

Virtual COM Mode of Sena device servers use a driver to create a "Virtual COM Port" so that the software thinks it's talking to a serial port, but it's really talking to a LAN. When working with Serial/IP COM port redirector, Sena device servers transmit all serial signals including DTR, DSR and DCD.

2.2.1 Supported Models

HelloDevice PS110/410/810, Super Series, and STS Series

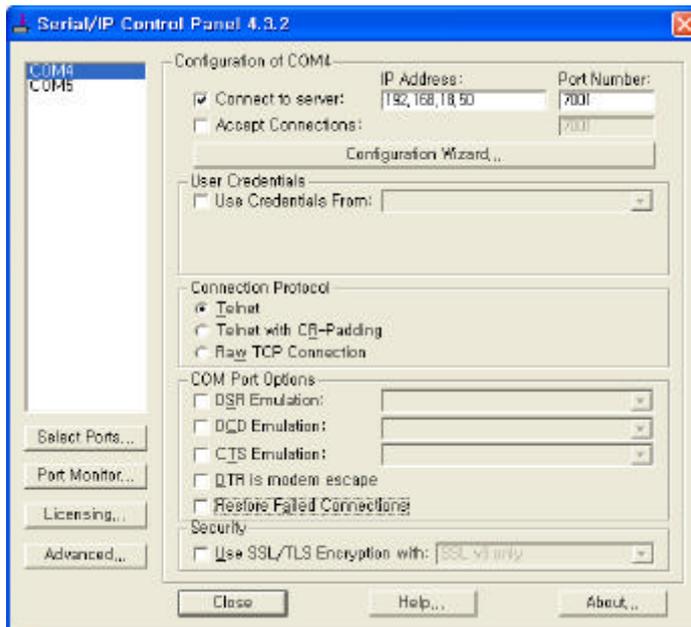
2.2.2 Setting in the Sena Device Server

Configuration Item	Value
Host mode :	TCP
TCP listening port (1024-65535, 0 for only outgoing connections) :	7001
Telnet protocol :	Enabled
Max. allowed connection (1-32) :	32
Cyclic connection to remote hosts (sec, 0 : disable) :	0
Inactivity disconnection timeout (sec, 0 : unlimited) :	0

Buttons: Save to flash, Save & apply, Cancel

- Set the Telnet protocol option enabled.
- The features provided by the COM Port Control protocol support are specified by IETF RFC 2217.

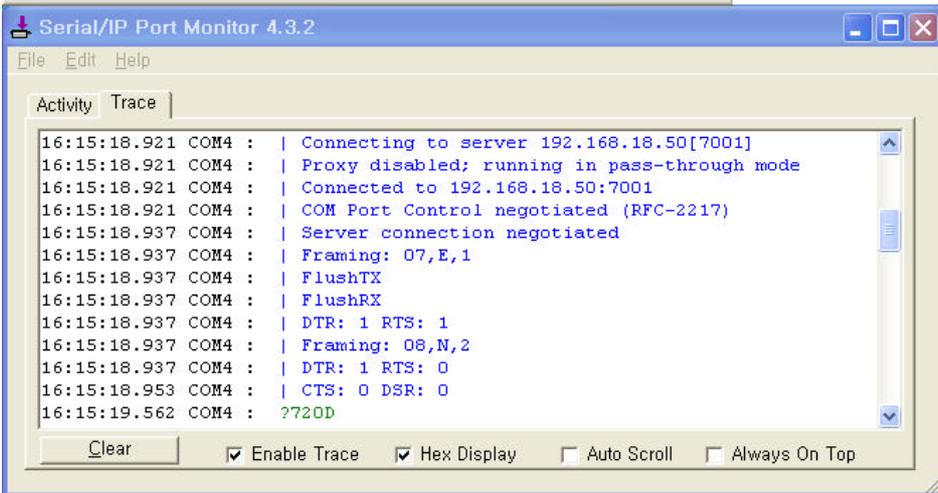
2.2.3 Serial/IP Configuration



- Connection protocol is set to Telnet.

2.2.4 Sample Application

Here is a sample application named "Protek" that changes serial port settings like baud rates and framing automatically. For this kind of applications, Sena's device servers support the COM Port Control protocol.



3. Serial/IP Server Operation Mode

3.1 RawTCP Operation Mode

3.1.1 Supported Products

LS, NEMO, PS, SS, STS

3.1.2 Sena Device Server configuration

TCP Client Mode (Destination IP, Port assignment-LS, PS), and Remote Host assignment (SS, STS)

The screenshot shows a dialog box titled "Remote host configuration". It contains a table with columns: Check, Host #, Primary remote host IP, Port #, Secondary remote host IP, and Port #. The first row has a checked box, Host # 1, Primary remote host IP 192.168.18.10, Port # 7001, and dashes for the secondary fields. Below the table are radio buttons for "Add", "Edit", and "Remove", with "Add" selected. There are input fields for "Primary host address", "Primary host port", "Secondary host address", and "Secondary host port". At the bottom are buttons for "Save to flash", "Save & apply", and "Cancel".

Check	Host #	Primary remote host IP	Port #	Secondary remote host IP	Port #
<input checked="" type="checkbox"/>	1	192.168.18.10	7001	--	--

Action on remote host : Add Edit Remove

Primary host address :

Primary host port :

Secondary host address :

Secondary host port :

Save to flash Save & apply Cancel

3.1.3 Serial/IP setup

The screenshot shows the "Serial/IP Control Panel 4.3.2" dialog box. On the left is a list of COM ports with "COM4" selected. The main area is titled "Configuration of COM4" and includes fields for "IP Address:" (192,168,18,50) and "Port Number:" (7001). There are checkboxes for "Connect to server:" (unchecked) and "Accept Connections:" (checked). Below is a "User Credentials" section with a "Use Credentials From:" dropdown. The "Connection Protocol" section has radio buttons for "Telnet", "Telnet with CR-Padding", and "Raw TCP Connection" (selected). The "COM Port Options" section has checkboxes for "DSR Emulation:", "DCD Emulation:", "CIS Emulation:", "DTR is modem escape", and "Restore Failed Connections". The "Security" section has a checkbox for "Use SSL/TLS Encryption with:" and a dropdown set to "SSL v3 only". Buttons for "Close", "Help...", and "About..." are at the bottom.

Configuration of COM4

IP Address: 192,168,18,50 Port Number: 7001

Connect to server: Accept Connections: 7001

Configuration Wizard...

User Credentials

Use Credentials From: [dropdown]

Connection Protocol

Telnet

Telnet with CR-Padding

Raw TCP Connection

COM Port Options

DSR Emulation: [dropdown]

DCD Emulation: [dropdown]

CIS Emulation: [dropdown]

DTR is modem escape

Restore Failed Connections

Security

Use SSL/TLS Encryption with: SSL v3 only

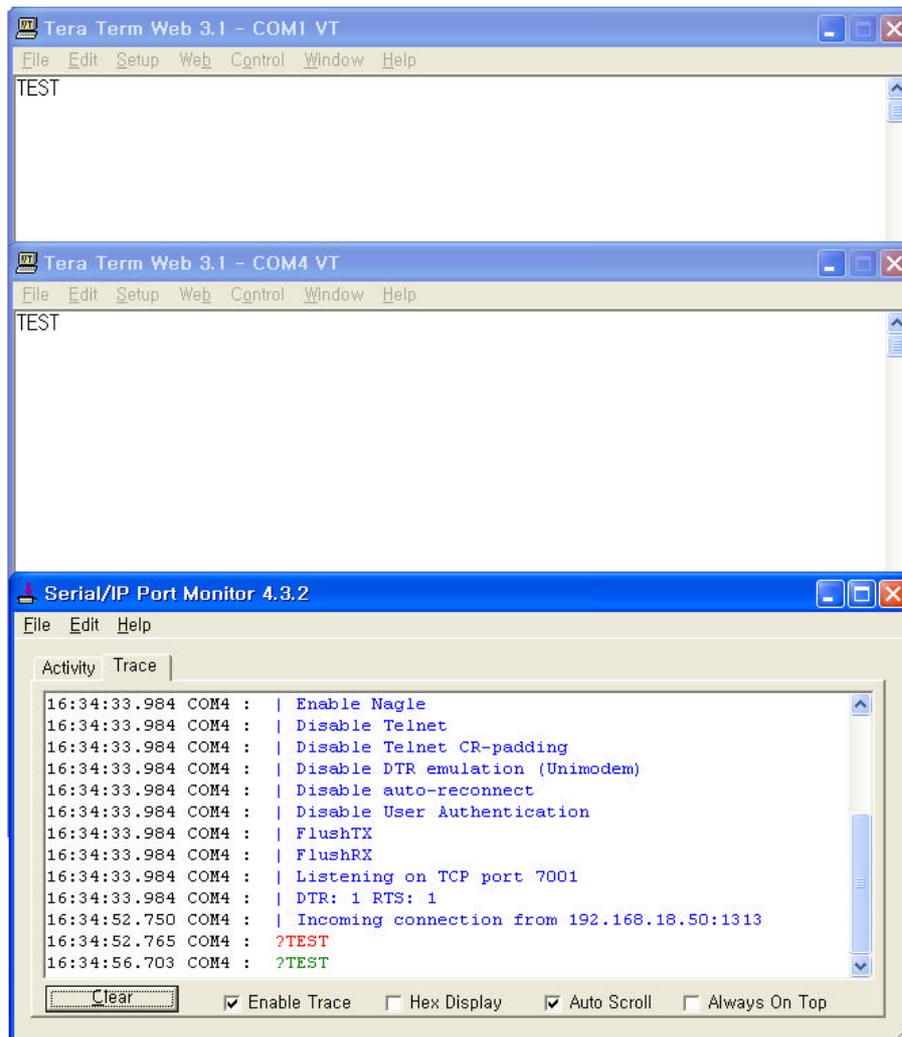
Close Help... About...

- Accept connection: Listening TCP Server Port number

- Connection Protocol: Connection has been set to RawTCP mode.

3.1.4 Operation

- If Virtual COM port is opened, then Serial/IP waits at the listening port until an incoming connection is established.
- Server mode operation is working even when users do not know the IP address of the Sena Device Servers in a dynamic IP environment, since it does not initiate the connection.



4. SSL Security features

Sena now takes COM Port Redirection a step further with encryption features, offering a secure Ethernet connection between the COM port and a Sena device server or terminal server. When working with the Serial/IP COM Port Redirector and OpenSSL Toolkit, the new SSL/TLS Security option offers a selection of five ciphers (including 3-DES and AES) and strengths up to 256 bits, sufficient to meet the tough security requirements encountered in the financial services industry.

4.1 SSL Data Transfer without certificate

4.1.1 Supported Models

HelloDevice PS110/PS410/PS810, SS100/SS110/SS400/SS800, and STS800/STS1600

4.1.2 Cryptography configuration

Cryptography configuration

Encryption method : SSLv3

Enable/Disable cipher suites :

- SSL_DHE_DSS_WITH_RC4_128_SHA
- SSL_DHE_DSS_EXPORT1024_WITH_RC4_56_SHA
- SSL_RSA_EXPORT1024_WITH_RC4_56_SHA
- SSL_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA
- SSL_RSA_EXPORT1024_WITH_RC4_56_MD5
- SSL_DHE_RSA_WITH_3DES_CBC_SHA
- SSL_DHE_RSA_WITH_DES_CBC_SHA
- SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
- SSL_DHE_DSS_WITH_3DES_CBC_SHA
- SSL_DHE_DSS_WITH_DES_CBC_SHA
- SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA
- SSL_RSA_WITH_3DES_CBC_SHA
- SSL_RSA_WITH_DES_CBC_SHA
- SSL_RSA_EXPORT_WITH_DES40_CBC_SHA
- SSL_RSA_WITH_IDEA_CBC_SHA
- SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5
- SSL_RSA_WITH_RC4_SHA
- SSL_RSA_WITH_RC4_MD5
- SSL_RSA_EXPORT_WITH_RC4_40_MD5
- SSL_DH_anon_WITH_3DES_CBC_SHA
- SSL_DH_anon_WITH_DES_CBC_SHA
- SSL_DH_anon_EXPORT_WITH_DES_CBC_SHA
- SSL_DH_anon_WITH_RC4_128_MD5
- SSL_DH_anon_EXPORT_WITH_RC4_40_MD5
- SSL_RSA_WITH_NULL_SHA
- SSL_RSA_WITH_NULL_MD5

Verify client (server mode only) : NO

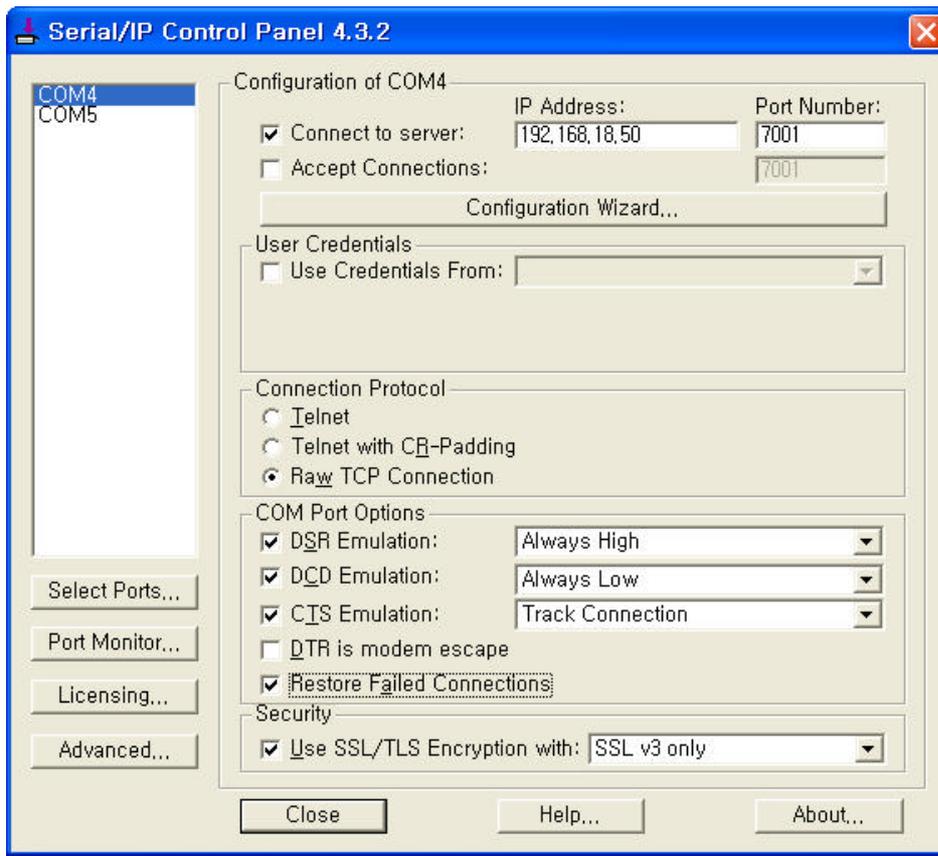
Verify certificate chain depth : 3

Check the certificate CN : NO

Save to flash Save & apply Cancel

- SS and STS support SSLv2, SSLv3, SSLv3 rollback to v2, TLSv1, 3DES, and RC4 Encryption methods.
- Select one of the Encryption methods, SSLv3 rollback to v2, SSLv3 and TLSv1.

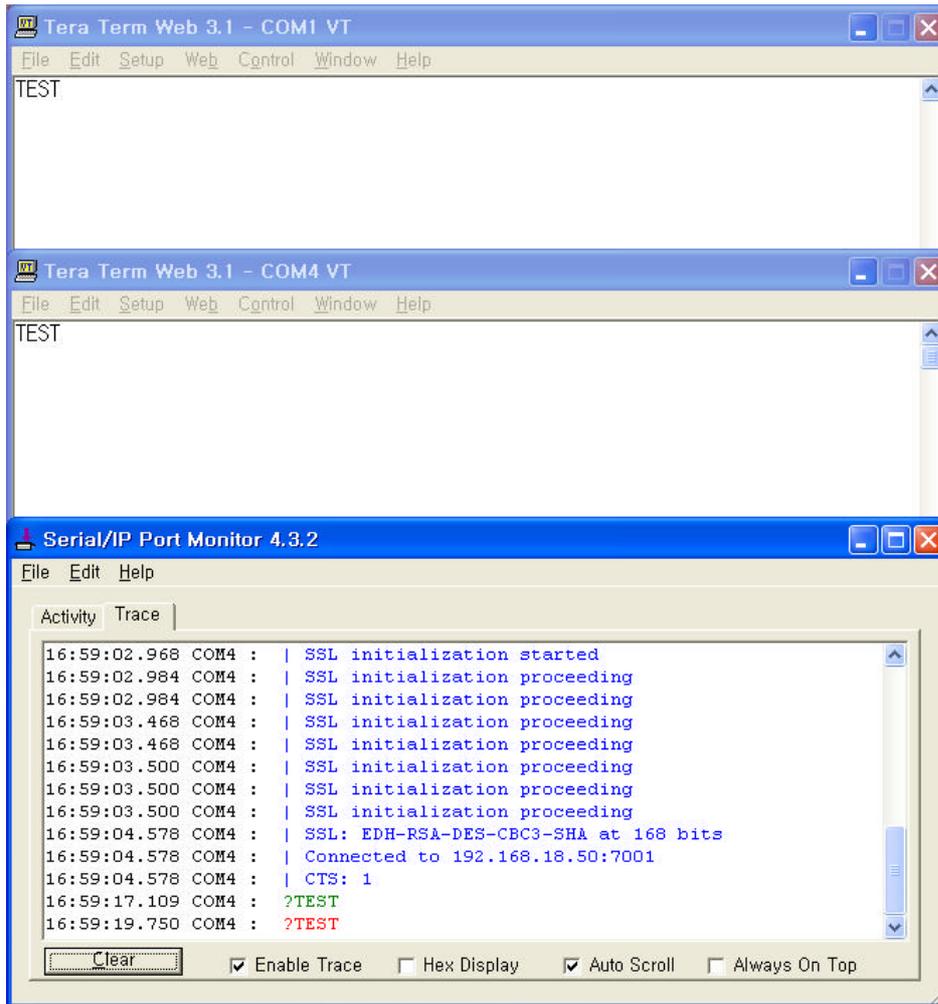
4.1.3 SSL Security configuration options in Serial/IP



- Specify the operation mode according to users' application scenario.
- Check the "Use SSL/TLS Encryption with" option.
- Set the Encryption method in Sena Device Server configuration.

4.1.4 Operation

- When user opens the Virtual COM Port, the TCP connection between the Serial/IP and Sena Device Server is done via SSL Secure encryption.
- If the authentication is completed, then data communication is started.



Note: Serial/IP settings according to the Encryption methods of Sena Device Servers.

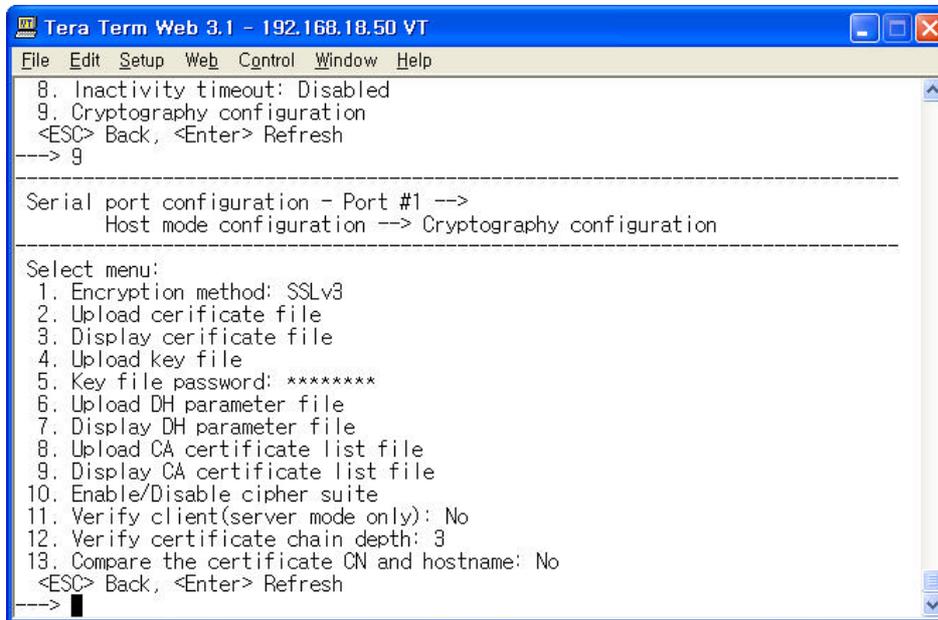
Sena Device Server	Serial/IP	Remarks
SSLv3 Rollback to v2	SSL v3 or TLS v1 SSL v3 Only TLS v1 Only	Serial/IP supports all Encryption methods.
SSLv3	SSL v3 Only	
TLSv1	TLS v1 Only	

4.2 SSL Data Transfer using certificate

4.2.1 Supported Models

HelloDevice PS110/PS410/PS810, SS100/SS110/SS400/SS800, and STS800/STS1600

4.2.2 Sena Device Server Configuration



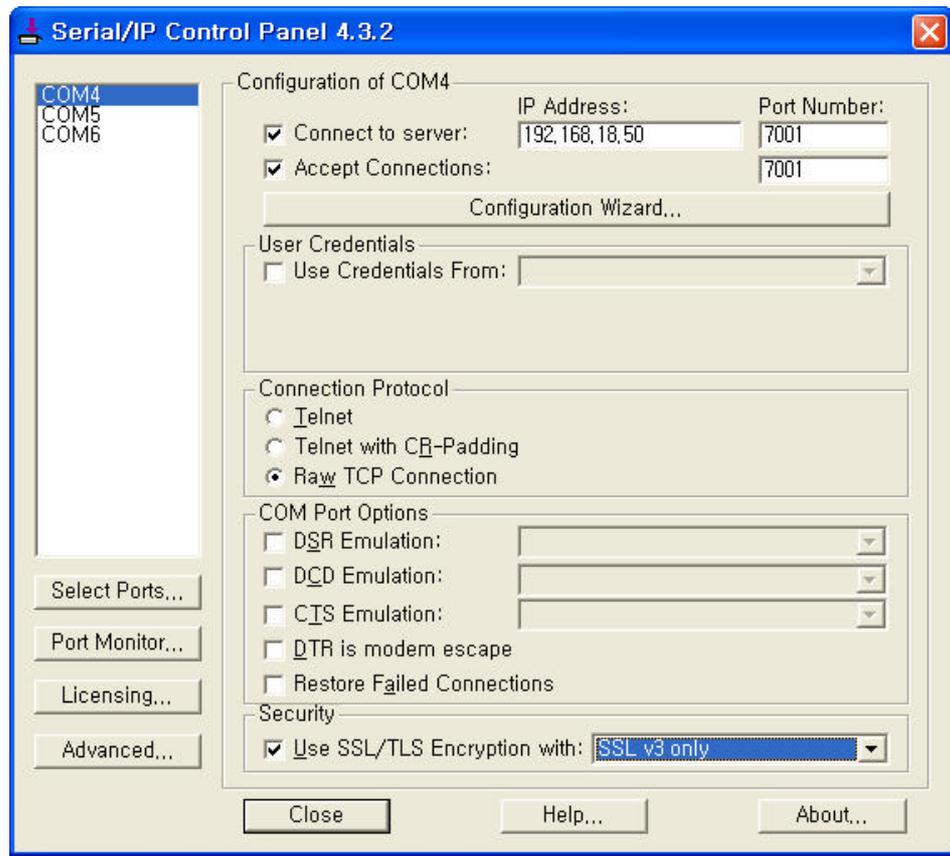
```
Tera Term Web 3.1 - 192.168.18.50 VT
File Edit Setup Web Control Window Help
8. Inactivity timeout: Disabled
9. Cryptography configuration
<ESC> Back, <Enter> Refresh
--> 9

-----
Serial port configuration - Port #1 -->
Host mode configuration --> Cryptography configuration
-----

Select menu:
1. Encryption method: SSLv3
2. Upload certificate file
3. Display certificate file
4. Upload key file
5. Key file password: *****
6. Upload DH parameter file
7. Display DH parameter file
8. Upload CA certificate list file
9. Display CA certificate list file
10. Enable/Disable cipher suite
11. Verify client(server mode only): No
12. Verify certificate chain depth: 3
13. Compare the certificate CN and hostname: No
<ESC> Back, <Enter> Refresh
--> █
```

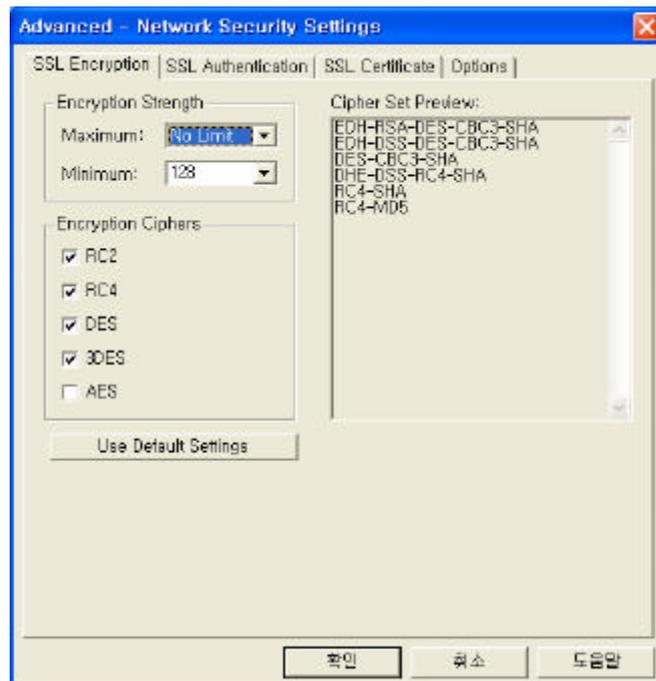
- Set the Encryption method serial port #1 of Sena Device Server as follows
 - ☞ SSL v3, SSLv3 rollback to V2, TLS v1
- Select the "Samplecert.pem" certificate file from Serial/IP folder and upload.
- Select the "Samplecert.pem" Key file from Serial/IP folder and upload.
- Set the Key file password.
- Upload the "Samplecert.pem" CA certificate list file from Serial/IP folder.
- Enable/Disable cipher suite.
- Set the Host mode according to the Server and Client operation modes.
-

4.2.3 Configuring the Encryption feature

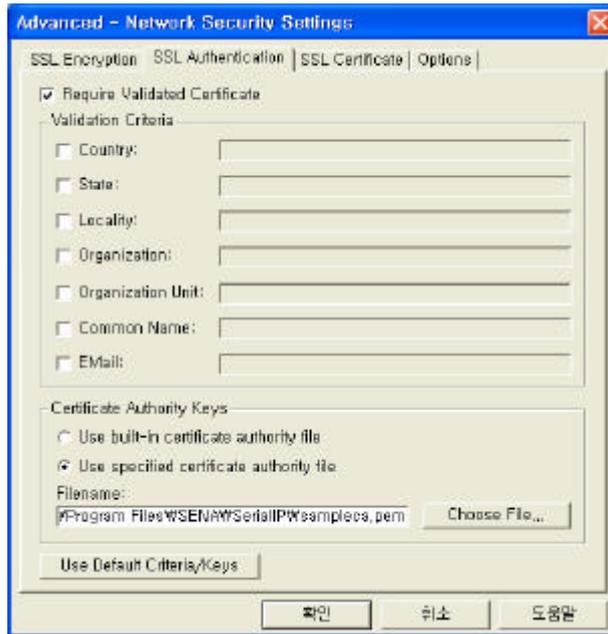


To use SSL encryption:

1. Click the [Advanced] button to get the Advanced Settings dialog window.
2. Select the [Encryption] tab.
3. In the Encryption Strength group, select Minimum and Maximum strengths in their respective dropdown lists.
4. In the Encryption Ciphers group, select one or more cipher suites.
5. Verify that at least one cipher appears in the Cipher Set Preview display.
6. Click [Apply] or [OK] to make the settings effective.



- In the Certificate Authority Keys group, select the radio button that corresponds to the source of the CA keys to be used. Built-in CA keys are those used by Internet Explorer 6, and are summarized in Appendix B. Alternatively, a file containing CA keys can be specified in Filename. A sample CA file named "sampleca.pem" is included with the software and is located in the software installation folder.



- Select the checkbox Supply Certificate. This enables the other controls in the window.
- In the Certificate File field, enter the filename of a certificate file or use Choose File to specify a file.
- A sample certificate file named "samplecert.pem" is included with the Serial/IP package and is located in the same folder as the product software.

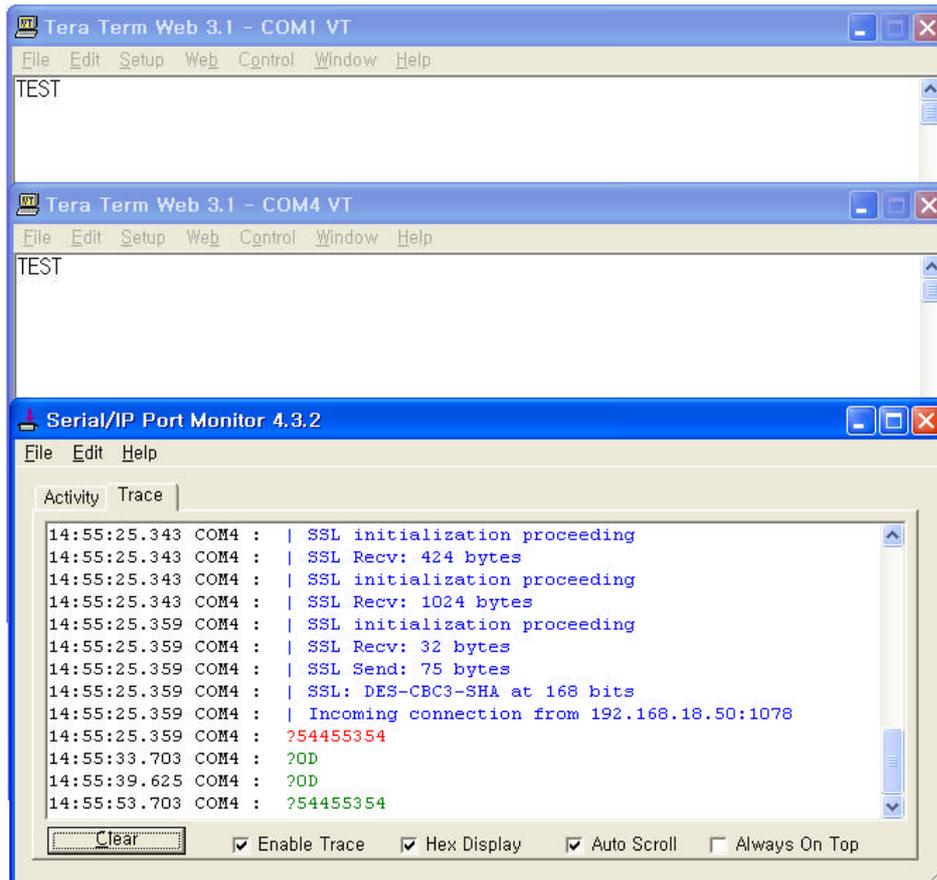


- The password for this certificate is "password".



4.2.4 Operation

- Open the Virtual COM Port COM4 and wait for the incoming connection.
- If the application sends data through COM1 port connected to the Sena Device Server, then the device server tries to connect to the listening port of the Serial/IP.
- If the connection is established, then the data communication is started after the SSL authentication process.



5. Appendix

- Host mode configuration between the Serial/IP and Sena Device server in communication depends on the TCP data initiation.
- Depending upon the application scenario, user should choose the host mode of communication.
- If there is any communication error, please check on the Port Monitor window.
- Below are 3 common causes for errors in communication.
 - ~~///~~ If the timeout is set to less in the user application that it has to be with the program)
 - ~~///~~ If pin information is not matched with the serial device.
 - ~~///~~ If user application does not support the serial software.
 - ~~///~~ If the user has a firewall blocking port communication.

<References>

- Lite Series Manual
- Pro Series Manual
- Super Series Manual
- STS Series Manual
- Serial/IP Manual