Secure RealCOM Certificate Deployment for NPort -G2 Models

How to secure serial communication and authenticate Moxa Windows Driver Manager with a self-signed certificate

Moxa Technical Support Team

support@moxa.com

Contents

 Released on Jun 23, 2026

About Moxa

Moxa is a leading provider of edge connectivity, industrial computing, and network infrastructure solutions for enabling connectivity for the Industrial Internet of Things. With over 35 years of industry experience, Moxa has connected more than 111 million devices worldwide and has a distribution and service network that reaches customers in more than 91 countries. Moxa delivers lasting business value by empowering industry with reliable networks and sincere service for industrial communications infrastructures. Information about Moxa's solutions is available at www.moxa.com.

How to Contact Moxa

Tel: 1-714-528-6777
Fax: 1-714-528-6778

1 Purpose and Scope

This guide describes how to encrypt data and command traffic for Secure Real COM communication and how to authenticate Moxa Windows Driver Manager by using a self-signed certificate on NPort -G2 models.

The procedure covers certificate generation on Ubuntu 24.04 LTS Server, equivalent notes for Microsoft Windows 11 PowerShell, and the required import steps on both Moxa Windows Driver Manager and the NPort 6150-G2-T.

IMPORTANT

The backslash or backtick character at the end of a line—Linux / PowerShell command or configuration—indicates that the command continues on the next line.

2 Test Bench Environment

The following environment was used to validate the configuration.

Table 1: Validated test bench

Component	Version/Details
Ubuntu Server	Ubuntu 24.04.4 LTS; Linux kernel 6.8.0-107-generic
OpenSSL on Windows 11	OpenSSL 3.6.2, 7 Apr 2026
OpenSSL on Linux	OpenSSL 3.0.13, 30 Jan 2024
NPort Device	NPort 6150-G2-T; firmware 1.2.0 Build 26042302
Moxa Windows Driver Manager	Version 4.4 Build 25111211

3 Configure the Time Zone on Ubuntu 24.04 LTS Server

3.1 Set the Time Zone

```
$ sudo timedatectl set-timezone Europe/Berlin
```

3.2 Verify the Configured Time Zone

```
$ timedatectl
Local time: Mon 2026-04-20 10:54:09 CEST
Universal time: Mon 2026-04-20 08:54:09 UTC
RTC time: Mon 2026-04-20 08:54:09
Time zone: Europe/Berlin (CEST, +0200)
System clock synchronized: no
NTP service: active
RTC in local TZ: no
```

4 Certificate Creation Process on Ubuntu 24.04 LTS Server

4.1 Create the Working Directory

Create a directory in the home directory for the certificates.

```
$ mkdir CA_NPort_2-05-05-2026
```

Change to the certificate working directory.

```
$ cd CA_NPort_2-05-05-2026/
```

4.2 Create Certificate Extension Configuration

Create the **cert.conf** file.

```
$ nano cert.conf
```

Add the following content, adapting IP addresses to the customer environment.

```
[NPort_ext]
extendedKeyUsage = serverAuth
keyUsage = digitalSignature, keyEncipherment
authorityKeyIdentifier = issuer
subjectKeyIdentifier = hash
subjectAltName = @NPort_alt_names

[NPort_alt_names]
IP.1 = 192.168.127.254 # NPort -G2 IP-Address

[NPortDriverManager_ext]
extendedKeyUsage = clientAuth
keyUsage = digitalSignature, keyEncipherment
authorityKeyIdentifier = issuer
subjectKeyIdentifier = hash
subjectAltName = @NPortDriverManager_alt_names

[NPortDriverManager_alt_names]
IP.1 = 192.168.127.5 # Moxa Windows Driver Manager PC IP-Address
```

4.3 Create the NPort CSR Configuration

Create the **csr_NPort.conf**.

```
$ nano csr_NPort.conf
```

```
[  req  ]
default_bits = 2048
prompt = no
default_md = sha256
distinguished_name = dn

[ dn ]
C = DE
ST = Bayern
L = Frankfurt
O = TS-Frankfurt
OU = TS-Frankfurt-Department
CN = 192.168.127.254 # NPort -G2 IP-Address
emailAddress = Frankfurt@moxa.com
```

4.4 Create the Windows Driver Manager CSR Configuration

Create **csr_NPortDriverManager.conf**.

```
$ nano csr_ NPortDriverManager.conf
```

```
[  req  ]
default_bits = 2048
prompt = no
default_md = sha256
distinguished_name = dn

[ dn ]
C = DE
ST = Bayern
L = Eching
O = TS-Eching
OU = TS-Eching-Department
CN = NPortDriverManager
emailAddress = eching@moxa.com
```

4.5 Prepare the OpenSSL CA Configuration

Copy the default OpenSSL configuration to the working directory.

```
$ cp /etc/ssl/openssl.cnf .
```

Edit **openssl.cnf**.

```
$ nano openssl.cnf
```

In the **[v3_ca]** section, verify or set the following values.

```
authorityKeyIdentifier=keyid:always,issuer

# Key usage: this is typical for a CA certificate. However since it will
# prevent it being used as an test self-signed certificate it is best
# left out by default.
keyUsage = critical, cRLSign, keyCertSign
```

In the **[CA_default]** section, set the working directory.

```
dir = . # Where everything is kept
```

5 Create the CA, NPort, and Driver Manager Certificates

5.1 Create the CA Certificate and Key

Run the following command and enter the requested Distinguished Name values when prompted.

```
$ openssl req -x509 -sha256 -days 365 \
-nodes -newkey rsa:2048 -keyout CA.key -out CA.pem \
-config openssl.cnf
```

Example prompt values:

```
Country Name (2 letter code) [AU]: DE
State or Province Name (full name) [Some-State]: Bayern
Locality Name (eg, city) []: Munich
Organization Name (eg, company) [Internet Widgits Pty Ltd]: MEU
Organizational Unit Name (eg, section) []: MEU-TS
Common Name (e.g. server FQDN or YOUR name) []: CA-Cert-2-05-05-2026
Email Address []:
```

5.2 Create the NPort Certificate

Generate the NPort private key.

```
$ openssl genrsa -out NPort.key 2048
```

Create the certificate signing request.

```
$ openssl req -new -key NPort.key \
  -out NPort.csr -config csr_NPort.conf
```

Create the NPort certificate.

```
$ openssl x509 -req -in NPort.csr \
  -CA CA.pem -CAkey CA.key -CAcreateserial -out NPort.pem -days 360 \
  -sha256 -extfile cert.conf -extensions NPort_ext
```

Expected result:

```
Certificate request self-signature ok
subject=C = DE, ST = Bayern, L = Frankfurt, O = TS-Frankfurt, OU = TS-
Frankfurt-Department, CN = 192.168.127.254, emailAddress =
Frankfurt@moxa.com
```

5.3 Create the Moxa Windows Driver Manager Certificate

Generate the Driver Manager private key.

```
$ openssl genrsa -out NPortDriverManager.key 2048
```

Create the certificate signing request.

```
$ openssl req -new \
  -key NPortDriverManager.key -out NPortDriverManager.csr \
  -config csr_NPortDriverManager.conf
```

Create the Driver Manager certificate.

```
$ openssl x509 -req \
  -in NPortDriverManager.csr -CA CA.pem -CAkey CA.key -CAcreateserial \
  -out NPortDriverManager.pem -days 360 -sha256 -extfile cert.conf \
  -extensions NPortDriverManager_ext
```

Expected result:

```
Certificate request self-signature ok
subject=C = DE, ST = Bayern, L = Eching, O = TS-Eching, OU = TS-Eching-
Department, CN = NPortDriverManager, emailAddress = eching@moxa.com
```

5.4 Create the Host CA Certificate for Windows Driver Manager

Create a **`Host_CA_Cert.pem`** file by combining the content of **`NPortDriverManager.key`** and **`NPortDriverManager.pem`**.

```
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQE
...
yZpfe2AjT5ObrRURhgVSvFTzFAA
-----END PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIDqTCCApGgAwIBAgIUMMiFnM2
...
QdnZCONaQF1AvvCY7ob3DfLEAEf
-----END CERTIFICATE-----
```

6 Create Certificates on Microsoft Windows 11

6.1 Install OpenSSL for Windows

OpenSSL does not provide official Windows installers. Use a trusted third-party build such as Win64 OpenSSL v3.x Light from Shining Light Productions.

Go to https://slproweb.com/products/Win32OpenSSL.html

Download Win64 OpenSSL v3.x (Light)—recommended for most users—during installation:

- Select **The OpenSSL binaries (/bin) directory** when asked where to copy DLLs.
- Optionally select **Add OpenSSL to the system PATH**, if available.

6.2 Add OpenSSL to PATH

If OpenSSL was not added to PATH automatically:

1. Open **Environment Variables** from the Windows Start menu.
2. Open **Edit the system environment variables**.
3. Select **Environment Variables**.
4. Under **System variables**, select **Path** and **Edit**.
5. Add the OpenSSL binary folder.

```
C:\Program Files\OpenSSL-Win64\bin
```

Restart PowerShell after updating PATH.

6.3 Verify OpenSSL in PowerShell

```
openssl version
```

Expected example output:

```
OpenSSL 3.6.2 7 Apr 2026 (Library: OpenSSL 3.6.2 7 Apr 2026)
```

6.4 Create the Certificate Folder and Configuration Files

```
mkdir CA_NPort_2-05-05-2026
```

Create the same configuration files used in the Linux workflow:

- **cert.conf**
- **csr_NPort.conf**
- **csr_NPortDriverManager.conf**

Example:

```
notepad cert.conf
```

6.5 Copy and Edit openssl.cnf

Check the OpenSSL directory.

```
openssl version -d
OPENSSLDIR: "C:\Program Files\Common Files\SSL"
```

Copy **openssl.cnf** into the certificate folder.

```
copy 'C:\Program Files\Common Files\SSL\openssl.cnf' .
```

Edit **openssl.cnf** using the same settings described in the Linux section.

6.6 PowerShell Line Continuation

In PowerShell, replace the Linux backslash line continuation character with a PowerShell backtick.

```
openssl x509 -req `
  -in NPortDriverManager.csr -CA CA.pem -CAkey CA.key -CAcreateserial `
  -out NPortDriverManager.pem -days 360 -sha256 -extfile cert.conf `
  -extensions NPortDriverManager_ext
```

6.7 Merge Key and Certificate Files in PowerShell

Example for combining **NPort.key** and **NPort.pem** into **NPort_Key_Pem.pem**:

```
Get-Content NPort.key, NPort.pem | Set-Content NPort_Key_Pem.pem
```

7 Configure the NPort 6150-G2-T

7.1 Set System Time and Time Zone

Set the system date, time, time zone, and daylight saving settings before importing certificates.

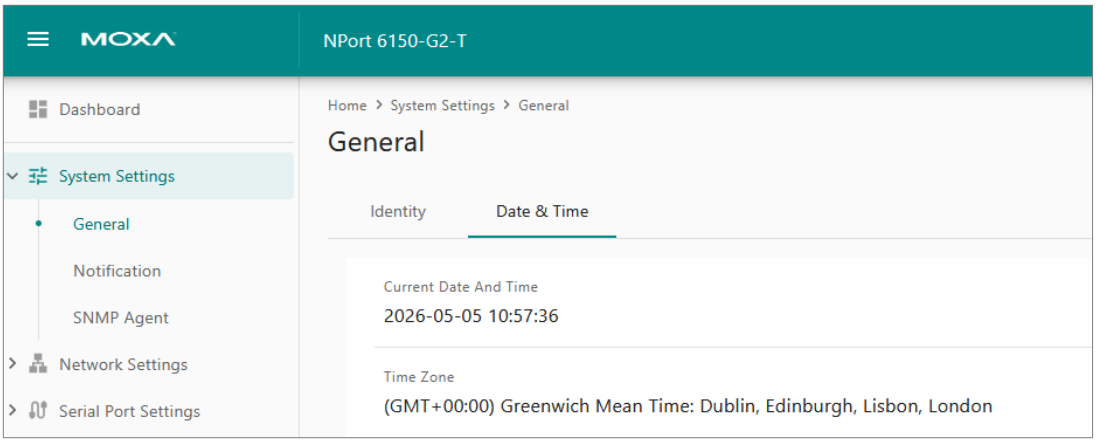


Figure 1: System Settings—General—Date and Time

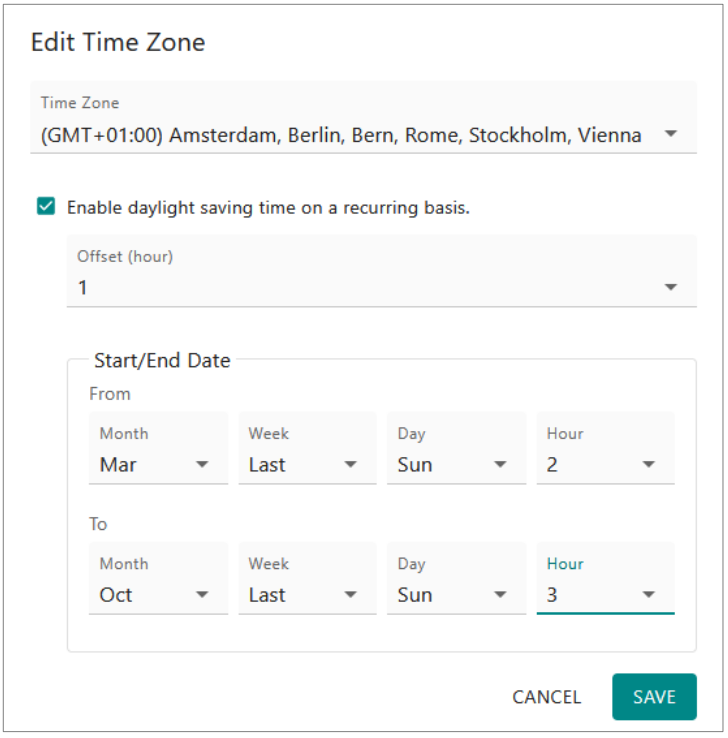


Figure 2: Time zone setting with daylight saving

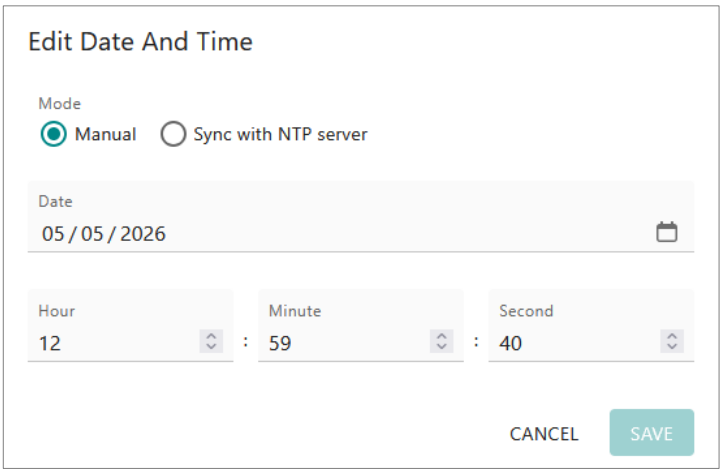


Figure 3: Set the current local date and time

8 Certificate Import Flow

8.1 Import Certificates in Moxa Windows Driver Manager

Import **`Host_CA_Cert.pem`** using **File > Host CA Import**. The file was created in the earlier certificate generation step.

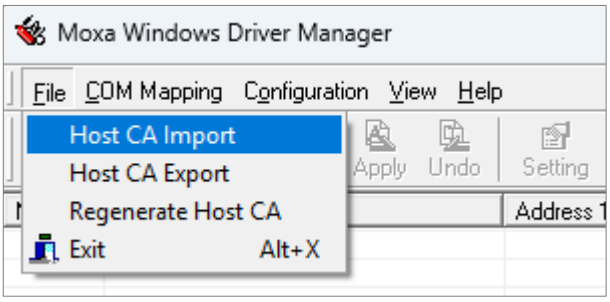


Figure 4: Host CA import in Moxa Windows Driver Manager

Import **`CA.pem`** from the COM port security settings, for example, **COM2 > Security tab > Import Certificate**.

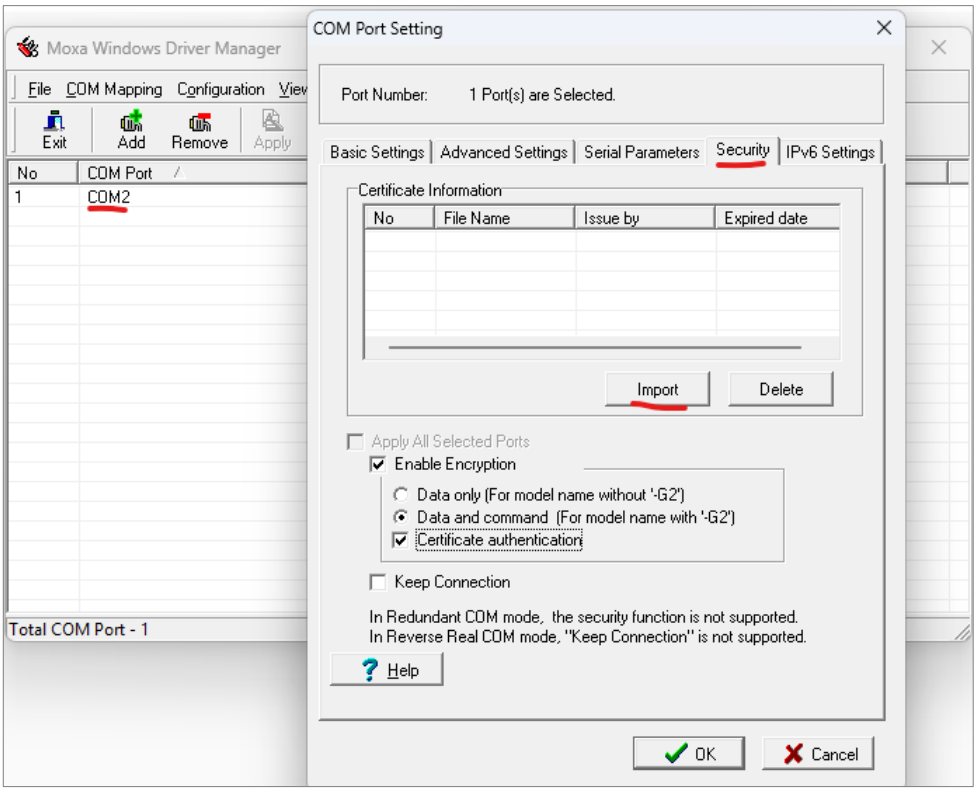


Figure 5: Import CA certificate in the COM port security settings

Note Ensure the following options are selected:

- Enable Encryption
- Data and command (For model name with -G2)
- Certificate authentication

After importing `CA.pem`, select **OK** and then **Apply**.

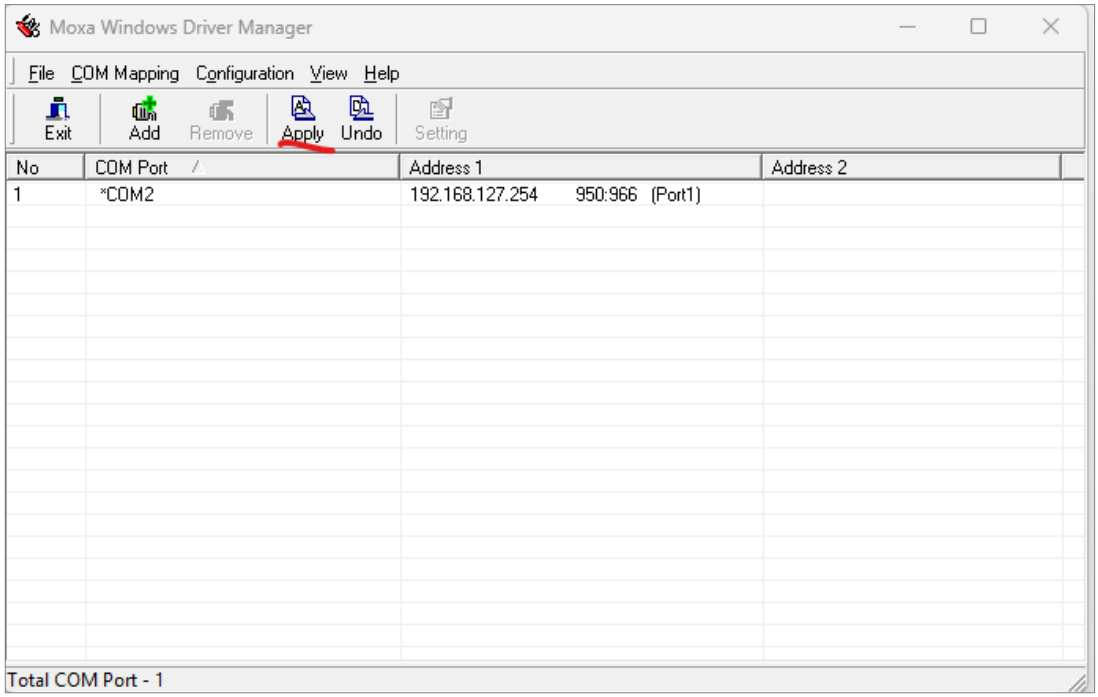


Figure 6: Apply certificate and encryption settings

8.2 Import Certificates on the NPort 6150-G2-T

Import the combined **`NPort.key`** and **`NPort.pem`** file, for example **`NPort_Key_Pem.pem`**, using **Security > Certificate > Import user certificate**.

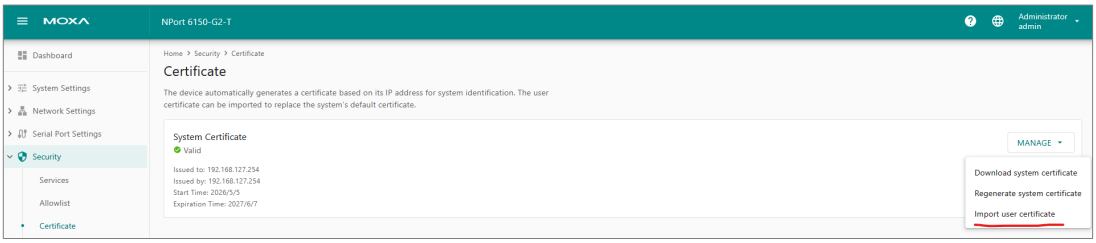


Figure 7: Import user certificate on the NPort device

Import **`CA.pem`** using **Serial Port Settings > Secure Connection > Remote Device Certificate**.

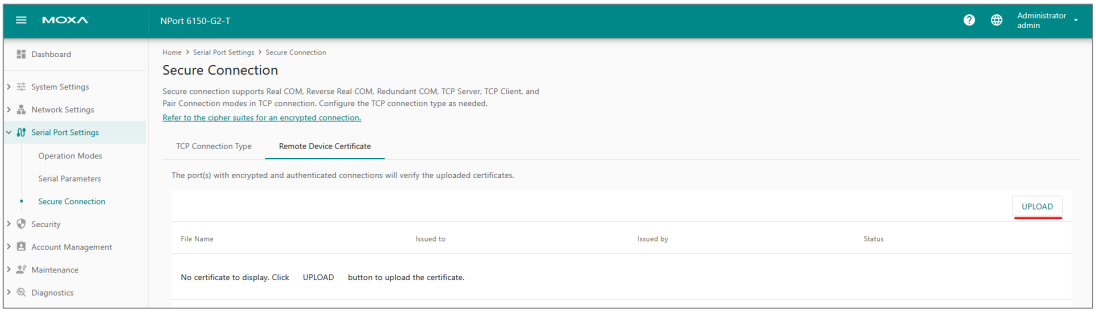


Figure 8: Remote device certificate import location

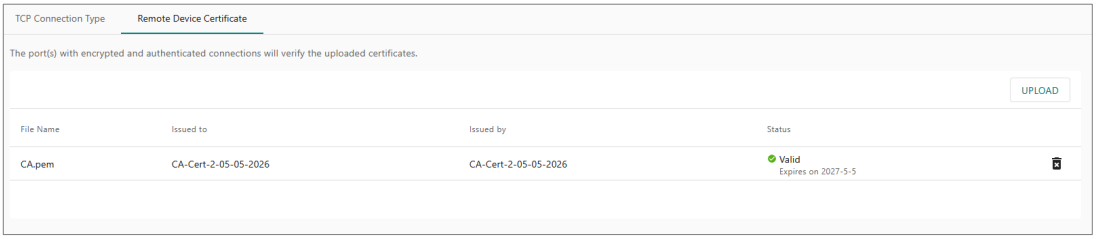


Figure 9: Imported remote device certificate

Set **TCP Connection Type** to **Encrypted and authenticated connection**.

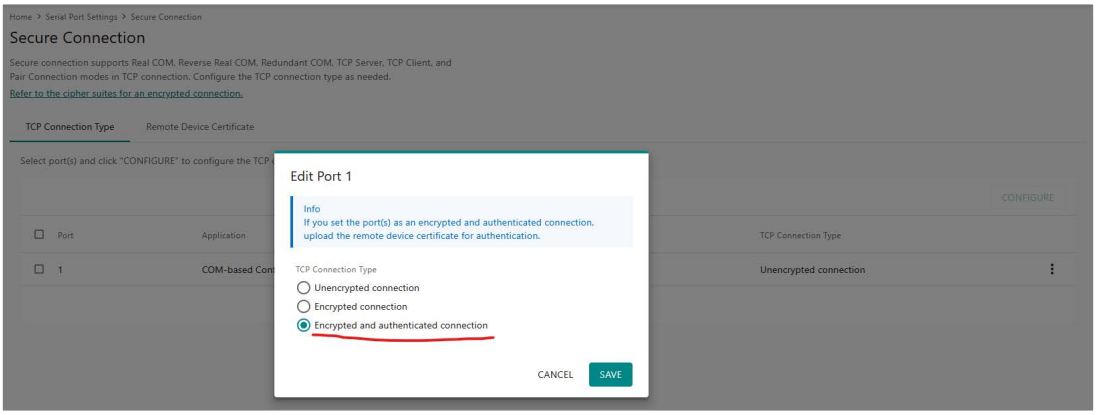


Figure 10: TCP connection type for encrypted and authenticated connections

8.3 Certificate Storage Locations on Windows

After importing, the files are stored by Moxa Windows Driver Manager in the following locations.

Certificate	Windows Location
Host_CA_Cert.pem	`C:\Program Files\Moxa\MoxaWindowsDrvManager\local_cert`
CA.pem	`C:\Program Files\Moxa\MoxaWindowsDrvManager\certificate`

The Host CA certificate is stored in two separate files:

- `local_cert.pem`
- `local_full_cert.pem`

The CA certificate is stored as:

- `CA.pem`

9 NPort Secure Service

The Windows service that drives data and command encryption for Windows Driver Manager is **NPort Secure Service**.

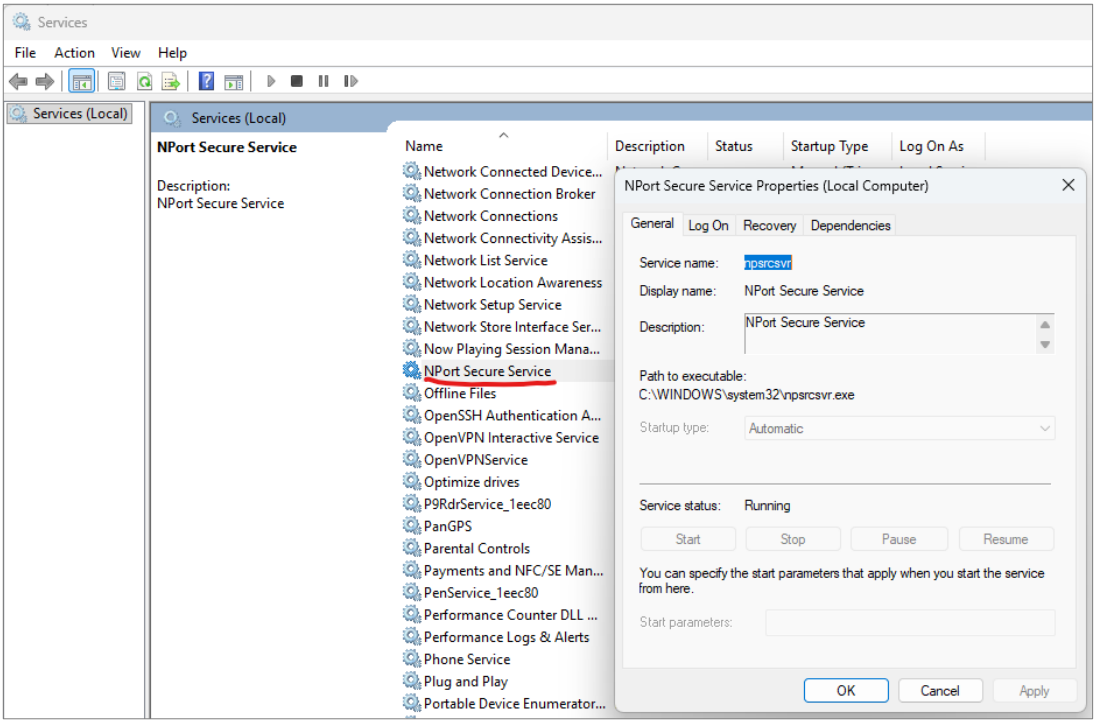


Figure 11: NPort Secure Service in Windows Services

10 Test the Encrypted Data and Command Flow

1. Open a terminal, for example, Tera Term, for COM Port 2 for Real COM.

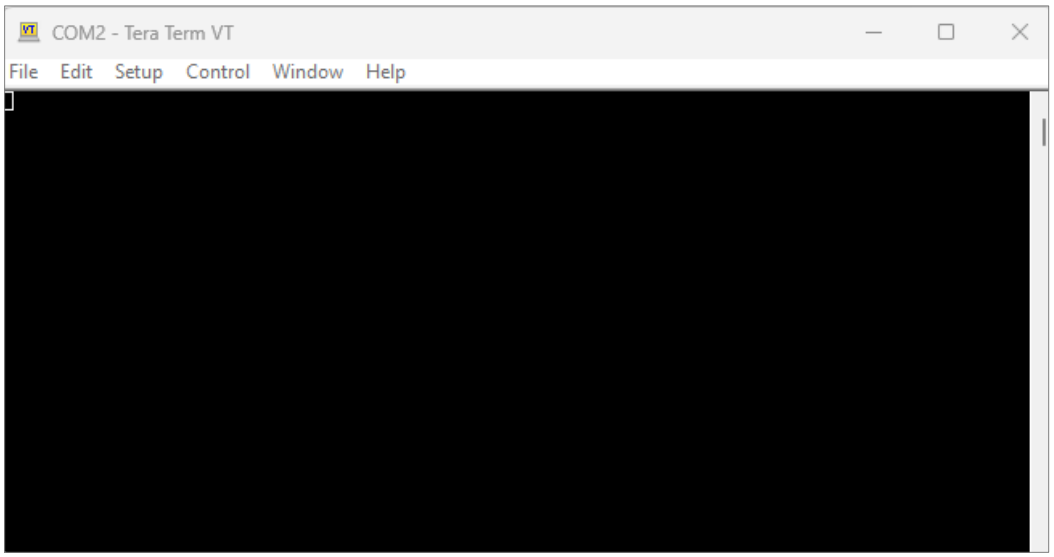


Figure 12: Tera Term session for RealCOM COM port

2. Open a terminal for the RS-232 serial connection to the NPort -G2 model.

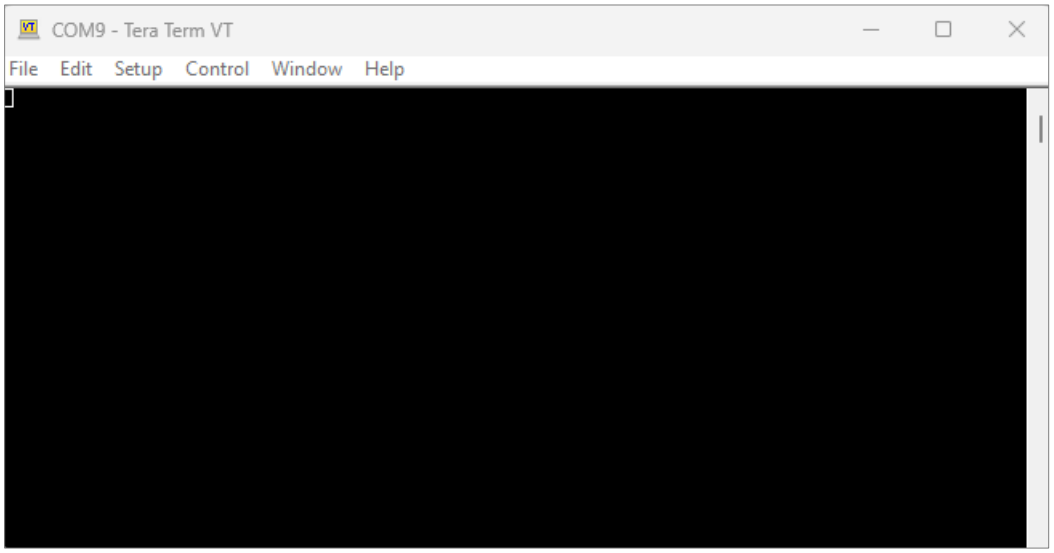
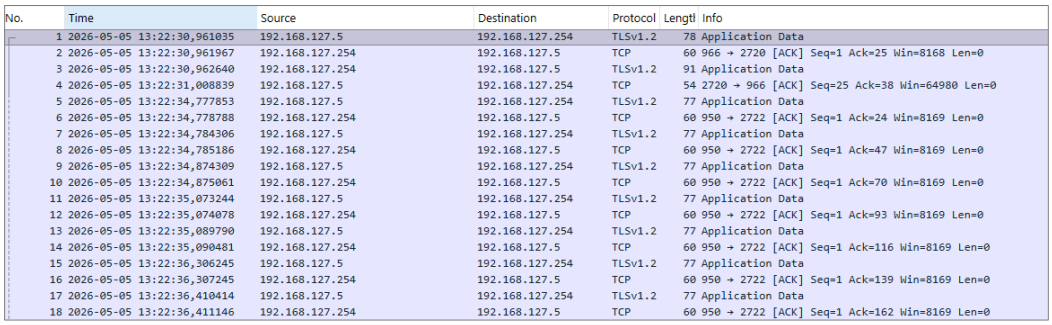


Figure 13: Terminal for the RS-232 serial connection

3. Launch Wireshark and type text in one of the terminals. The data and command traffic should be encrypted.



No.	Time	Source	Destination	Protocol	Lengtl	Info
1	2026-05-05 13:22:30,961035	192.168.127.5	192.168.127.254	TLSv1.2	78	Application Data
2	2026-05-05 13:22:30,961967	192.168.127.254	192.168.127.5	TCP	60	966 → 2720 [ACK] Seq=1 Ack=25 Win=8168 Len=0
3	2026-05-05 13:22:30,962640	192.168.127.254	192.168.127.5	TLSv1.2	91	Application Data
4	2026-05-05 13:22:31,008839	192.168.127.5	192.168.127.254	TCP	54	2720 → 966 [ACK] Seq=25 Ack=38 Win=64980 Len=0
5	2026-05-05 13:22:34,777853	192.168.127.5	192.168.127.254	TLSv1.2	77	Application Data
6	2026-05-05 13:22:34,778788	192.168.127.254	192.168.127.5	TCP	60	950 → 2722 [ACK] Seq=1 Ack=24 Win=8169 Len=0
7	2026-05-05 13:22:34,784306	192.168.127.5	192.168.127.254	TLSv1.2	77	Application Data
8	2026-05-05 13:22:34,785186	192.168.127.254	192.168.127.5	TCP	60	950 → 2722 [ACK] Seq=1 Ack=47 Win=8169 Len=0
9	2026-05-05 13:22:34,874309	192.168.127.5	192.168.127.254	TLSv1.2	77	Application Data
10	2026-05-05 13:22:34,875061	192.168.127.254	192.168.127.5	TCP	60	950 → 2722 [ACK] Seq=1 Ack=70 Win=8169 Len=0
11	2026-05-05 13:22:35,073244	192.168.127.5	192.168.127.254	TLSv1.2	77	Application Data
12	2026-05-05 13:22:35,074078	192.168.127.254	192.168.127.5	TCP	60	950 → 2722 [ACK] Seq=1 Ack=93 Win=8169 Len=0
13	2026-05-05 13:22:35,089790	192.168.127.5	192.168.127.254	TLSv1.2	77	Application Data
14	2026-05-05 13:22:35,090481	192.168.127.254	192.168.127.5	TCP	60	950 → 2722 [ACK] Seq=1 Ack=116 Win=8169 Len=0
15	2026-05-05 13:22:36,306245	192.168.127.5	192.168.127.254	TLSv1.2	77	Application Data
16	2026-05-05 13:22:36,307245	192.168.127.254	192.168.127.5	TCP	60	950 → 2722 [ACK] Seq=1 Ack=139 Win=8169 Len=0
17	2026-05-05 13:22:36,410414	192.168.127.5	192.168.127.254	TLSv1.2	77	Application Data
18	2026-05-05 13:22:36,411146	192.168.127.254	192.168.127.5	TCP	60	950 → 2722 [ACK] Seq=1 Ack=162 Win=8169 Len=0

Figure 14: Wireshark view showing encrypted traffic

11 Deployment Checklist

Use this checklist before handing over the installation.

- Ubuntu or Windows certificate creation workstation has the correct time and date.
- Certificate Subject Alternative Name entries match the actual NPort and Windows Driver Manager PC IP addresses.
- **`CA.pem`**, **`NPort.pem`**, **`NPort.key`**, and **`NPortDriverManager.pem`** were generated successfully.
- **`Host_CA_Cert.pem`** contains both the Driver Manager private key and certificate.
- The NPort user certificate file combines the NPort private key and certificate.
- Moxa Windows Driver Manager has **Enable Encryption and Certificate authentication** enabled.
- NPort TCP connection type is set to **Encrypted and authenticated connection**.
- The **NPort Secure Service** is running on Windows.
- Wireshark verification confirms that the RealCOM data and command flow is encrypted.