Configuring WPA Enterprise Mode Using EAP-TLS Between an AWK-3252A-UN Device as an AP and NPort W2150A-W4-EU (Client)

Moxa Technical Support Team

support@moxa.com

Contents

1 Purpose and Scope 3
2 Testbed Environment 3
3 Prerequisites 4
4 Prepare the Ubuntu Server 4
4.1 Set the Time Zone 4
4.2 Install FreeRADIUS 4
5 Create CA, Server, and Client Certificates 5
5.1 Create the Certificate Working Directory 5
5.2 Create the Certificate Extension File 6
5.3 Create the Server CSR—Certificate Signing Request—Configuration 7
5.4 Create the Client CSR—Certificate Signing Request—Configuration 7
5.5 Create the CA Certificate and Key 8
5.6 Create the FreeRADIUS Server Certificate 8
5.7 Create the NPort Client Certificate 9
6 Configure FreeRADIUS for EAP-TLS 9
6.1 Install Certificates in FreeRADIUS 9
6.2 Replace the EAP Module Configuration 10
6.3 Configure the RADIUS Client Subnet 11
6.4 Start FreeRADIUS in Debug Mode 12
7 Useful OpenSSL Commands 12
8 Configure the AWK-3252A-UN as Access Point 13
8.1 Set Time Zone and System Clock 13
8.2 Set Operation Mode to AP 14
8.3 Create the WPA-Enterprise SSID 15
9 Configure the NPort W2150A-W4-EU 16

Copyright © 2026 Moxa Inc. Released on Oct 28, 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

9.1 Set the Basic Settings 16
9.2 Enable Ethernet Bridge Mode 17
9.3 Check the IP Configuration and IP-Address 17
9.4 Import the WPA Server Certificate 18
9.5 Import the WPA User Certificate 18
9.6 Import the WPA User Key 19
9.7 Set the Wireless LAN Profile 19
9.8 Set the WLAN Profile's General Properties 20
9.9 Set the WLAN Profile's Security Properties 20
9.10 Submit the Wireless LAN Profile Settings 21
9.11 Activating WLAN Log 21
9.12 Checking the Status of the WLAN 22
10 Verify EAP-TLS Authentication 22
10.1 Check the FreeRADIUS Log 22
10.2 Check the AP Device Summary 23
11 Troubleshooting Checklist 23

Copyright © 2026 Moxa Inc.

1 Purpose and Scope

This guide describes how to configure WPA-Enterprise mode using EAP-TLS between an **AWK-3252A-UN** device as an AP and **NPort W2150A-W4-EU** as a client. **FreeRADIUS** on **Ubuntu 24.04 LTS Server** is used as an authentication server.

The procedure includes:

- Preparing the Ubuntu server.
- Creating CA, server, and client certificates with OpenSSL.
- Configuring the FreeRADIUS EAP module for EAP-TLS.
- Configuring the AWK-3252A-UN access point and NPort W2150A-W4-EU client.
- Importing the client certificate and key on the NPort W2150A-W4-EU client.
- Verifying successful authentication in the FreeRADIUS log and AWK device summary.

2 Testbed Environment

The following environment was used to validate the configuration.

Table 1: Validated test bench

Component	Version
Ubuntu server	Ubuntu 24.04.4 LTS
Linux kernel	6.8.0-117-generic
AWK-3252A-UN firmware version	v3.3 Build 2025_0606_1017
NPort W2150A-W4-EU firmware version	v1.5.0 Build 25071608
FreeRADIUS version	3.2.5
OpenSSL	3.0.13 30 Jan 2024
FreeRADIUS Server IP-Address	192.168.127.67/24
AWK-3252A-UN AP IP-Address	192.168.127.253/24
NPort W2150A-W4-EU Client IP-Address	192.168.127.252/24

Copyright © 2026 Moxa Inc.

3 Prerequisites

Before starting, make sure that:

- The Ubuntu server can reach the AWK management network.
- The AWK access point can reach the FreeRADIUS server.
- You have sudo access on the Ubuntu server.
- All devices have their time and date synchronized.
- Certificate validity periods match the system time of the server and AWK/NPort devices.

IMPORTANT

Certificate-based authentication is time-sensitive. Incorrect time, time zone, or date settings can cause certificate validation or EAP-TLS authentication to fail.

4 Prepare the Ubuntu Server

4.1 Set the Time Zone

Set the Ubuntu server's time zone. This example uses Europe/Berlin.

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

Verify the time zone and the current time.

```
$ timedatectl
```

Example output:

```
Local time: Thu 2026-06-25 10:27:48 CEST
Universal time: Thu 2026-06-25 08:27:48 UTC
RTC time: Thu 2026-06-25 08:27:49
Time zone: Europe/Berlin (CEST, +0200)
System clock synchronized: yes
NTP service: active
RTC in local TZ: no
```

4.2 Install FreeRADIUS

Install the FreeRADIUS server and utilities.

```
$ sudo apt install freeradius freeradius-utils
```

Copyright © 2026 Moxa Inc.

5 Create CA, Server, and Client Certificates

5.1 Create the Certificate Working Directory

Create a directory for the certificate files and change into it.

```
$ mkdir CA_Certificates_WiFi_EAP-TLS
$ cd CA_Certificates_WiFi_EAP-TLS/
```

Copy the OpenSSL configuration file to the working directory.

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

Edit the OpenSSL configuration file

```
$ 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
```

Copyright © 2026 Moxa Inc.

5.2 Create the Certificate Extension File

Create **cert.conf** file. The server extension is used for the FreeRADIUS server certificate. The client extension is used for the NPort client certificate.

```
$ nano cert.conf
```

```
[server_ext]
basicConstraints = critical,CA:FALSE
extendedKeyUsage = serverAuth
keyUsage = critical, digitalSignature, keyEncipherment
authorityKeyIdentifier = keyid, issuer
subjectKeyIdentifier = hash
subjectAltName = @alt_names
[alt_names]
DNS.1 = radius.meu-ts.lan
IP.1 = 192.168.127.67           # FreeRADIUS Server IP-Address

[client_ext]
basicConstraints = critical,CA:FALSE
extendedKeyUsage = clientAuth
keyUsage = critical, digitalSignature, keyEncipherment
authorityKeyIdentifier = keyid, issuer
subjectKeyIdentifier = hash
subjectAltName = email:Eching@moxa.com
```

Copyright © 2026 Moxa Inc.

5.3 Create the Server CSR—Certificate Signing Request—Configuration

Create **csr_server.conf**.

```
$ nano csr_server.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 = radius.meu-ts.lan
emailAddress = Frankfurt@moxa.com
```

5.4 Create the Client CSR—Certificate Signing Request—Configuration

Create **csr_client.conf**.

```
$ nano csr_client.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 = NPort-Client-Crt
emailAddress = Eching@moxa.com
```

Copyright © 2026 Moxa Inc.

5.5 Create the CA Certificate and Key

Create the CA certificate and private key.

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

Example input 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
Email Address []:
```

5.6 Create the FreeRADIUS Server Certificate

Generate the server's private key. In this example, the server key is encrypted with passphrase 1111, which must match the FreeRADIUS EAP configuration later.

```
$ openssl genrsa -aes256 -out Server.key 2048
```

Create the certificate signing request.

```
$ openssl req -new -key Server.key -out Server.csr -config csr_server.conf
```

Create the server certificate.

```
$ openssl x509 -req -in Server.csr -CA CA.crt -CAkey CA.key \
-CAcreateserial -out Server.crt \
-days 360 -sha256 -extfile cert.conf \
-extensions server_ext
```

Expected output:

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

Copyright © 2026 Moxa Inc.

5.7 Create the NPort Client Certificate

Generate the client's private key. In this example, the client key is encrypted with passphrase 1111, which must match the password for the private key in the NPort WPA User Key Import later.

```
$ openssl genrsa -aes256 -out Client.key 2048
```

Create the client certificate signing request.

```
$ openssl req -new -key Client.key -out Client.csr -config csr_client.conf
```

Create the client certificate.

```
$ openssl x509 -req -in Client.csr -CA CA.crt -CAkey CA.key \
-CAcreateserial -out Client.crt \
-days 360 -sha256 -extfile cert.conf \
-extensions client_ext
```

Expected output:

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

6 Configure FreeRADIUS for EAP-TLS

6.1 Install Certificates in FreeRADIUS

Copy the CA, server certificate, and server key to the FreeRADIUS certificate directory. Change the owner and the group to **`freerad`** and the privileges to **`640`** for the copied files.

```
# cp CA.crt Server.crt Server.key /etc/freeradius/3.0/certs/
# cd /etc/freeradius/3.0/certs/
# chown freerad:freerad CA.crt Server.crt Server.key
# chmod 640 CA.crt Server.crt Server.key
```

Copyright © 2026 Moxa Inc.

6.2 Replace the EAP Module Configuration

Change to the FreeRADIUS module directory and keep a backup of the original **eap** file.

```
# cd /etc/freeradius/3.0/mods-available/
# mv eap eap_old
```

Create an **eap** file

```
# nano eap
```

Add the following EAP-TLS configuration.

```
eap {
     default_eap_type = tls
     timer_expire = 60
     ignore_unknown_eap_types = no
     cisco_accounting_username_bug = no
     max_sessions = ${max_requests}
     md5 {
     }
     gtc {
          auth_type = PAP
     }
     tls-config tls-common {
          private_key_password = 1111
          private_key_file = /etc/freeradius/3.0/certs/Server.key
          certificate_file = /etc/freeradius/3.0/certs/Server.crt
          ca_file = /etc/freeradius/3.0/certs/CA.crt
          ca_path = ${cadir}
          cipher_list = "DEFAULT"
          cipher_server_preference = yes
          tls_min_version = "1.1"
          tls_max_version = "1.3"
          ecdh_curve = ""
          cache {
                 enable = no
                 store {
                        Tunnel-Private-Group-Id
                 }
          }
          verify {
          }
          ocsp {
                 enable = no
                 override_cert_url = yes
                 url = "http://127.0.0.1/ocsp/"
          }
```

Copyright © 2026 Moxa Inc.

```
            # Optional issuer check. The value depends on the CA issuer.
            check_cert_issuer = "/C=DE/ST=Bayern/L=Munich/O=MEU/OU=MEU-
            TS/CN=CA-Cert"
            # Optional CN check. If Username is configured on the device,
            # it must match the certificate CN of the client certificate.
            check_cert_cn = %{User-Name}
      }
      tls {
            tls = tls-common
      }
      ttls {
            tls = tls-common
            default_eap_type = md5
            copy_request_to_tunnel = no
            use_tunneled_reply = no
            virtual_server = "inner-tunnel"
      }
      peap {
            tls = tls-common
            default_eap_type = mschapv2
            copy_request_to_tunnel = no
            use_tunneled_reply = no
            virtual_server = "inner-tunnel"
      }
      mschapv2 {
      }
}
```

6.3 Configure the RADIUS Client Subnet

Add the subnet where the AWK and NPort devices are deployed to **/etc/freeradius/3.0/clients.conf**.

Add the block after the **IPv6 Client** section.

```
# nano /etc/freeradius/3.0/clients.conf
```

```
client MOXA-Dev {
      ipaddr = 192.168.127.0/24
      secret = "testing1234"
      nas_type = other
}
```

Copyright © 2026 Moxa Inc.

6.4 Start FreeRADIUS in Debug Mode

Stop the FreeRADIUS service and start FreeRADIUS in debug mode.

```
# systemctl stop freeradius.service
# freeradius -X
```

7 Useful OpenSSL Commands

The following OpenSSL commands can help verify certificate files during troubleshooting.

```
# Check a Certificate Signing Request (CSR)
openssl req -text -noout -verify -in CSR.csr

# Check a private key
openssl rsa -in privateKey.key -check

# Check a certificate
openssl x509 -in certificate.crt -text -noout

# Export CRT and key into a PFX/p12 file
openssl pkcs12 -export -inkey Client.key -in Client.crt \
-certfile CA.crt -name "AWK-Client-Crt" \
-out Client.p12 -passout pass:1111

# Export CRT into DER format
openssl x509 -in domain.crt -outform der -out domain.der

# Display the contents of a PFX/P12 file
openssl pkcs12 -in example.pfx -info
```

Copyright © 2026 Moxa Inc.

8 Configure the AWK-3252A-UN as Access Point

Configure the AWK-3252A-UN as an access point with the IP-Address `192.168.127.253/24`.

8.1 Set Time Zone and System Clock

Set the time zone and daylight saving settings in **System > Time > System Time—Time Zone**, then select **Apply**.

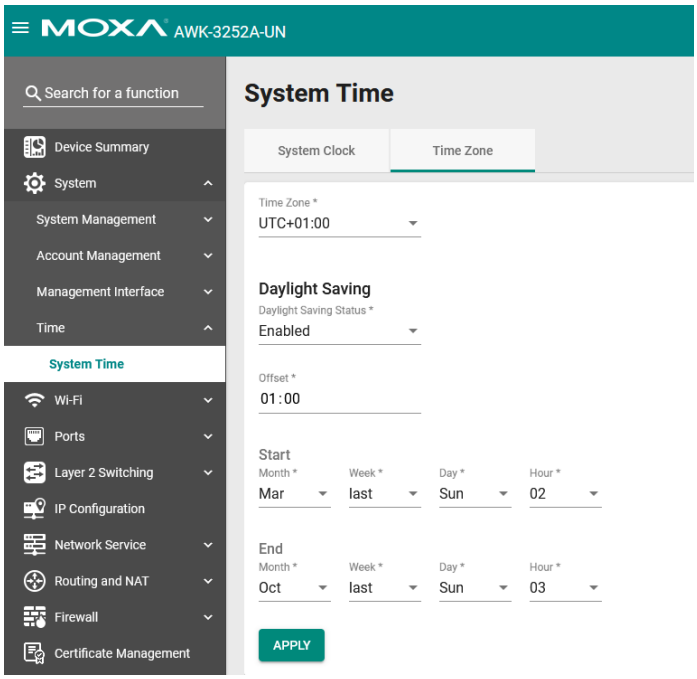


Figure 1: AWK access point time zone configuration

Set the local date and time in **System > Time > System Time - System Clock**. Use **SYNC WITH BROWSER**, then select **Apply**.

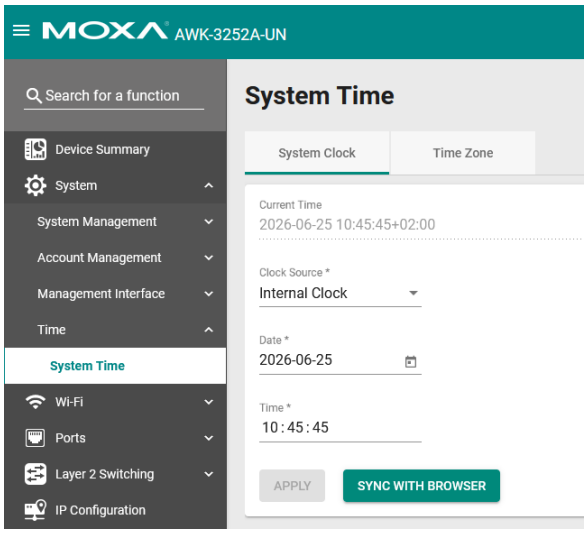


Figure 2: AWK access point system clock configuration

8.2 Set Operation Mode to AP

Set the operation mode to access point in the **Wi-Fi > Wireless Settings - General** tab.

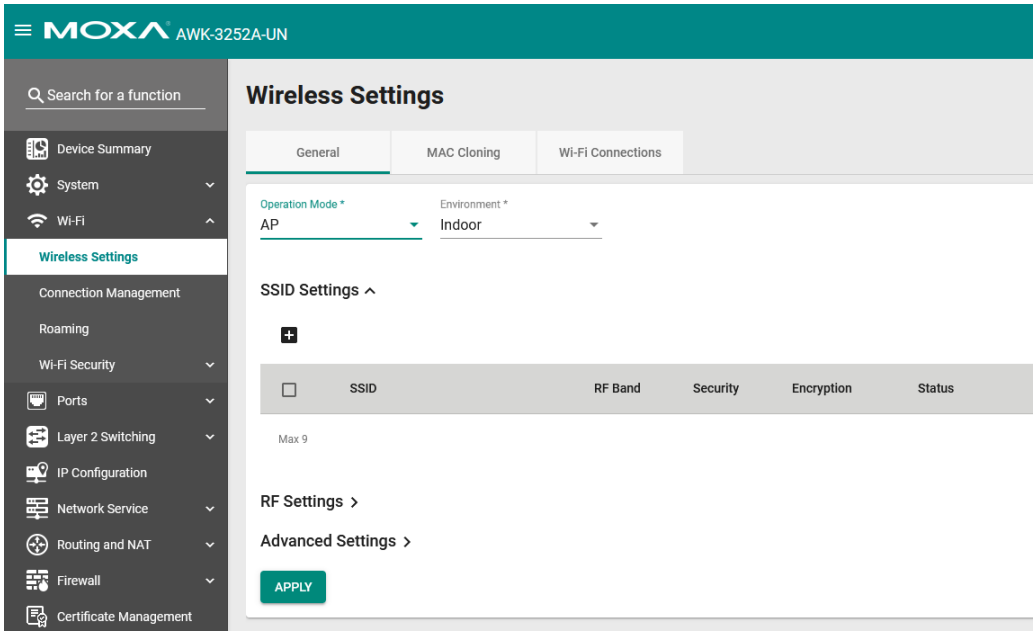


Figure 3: AWK wireless operation mode set to AP

8.3 Create the WPA-Enterprise SSID

Configure the SSID and select **CREATE**.

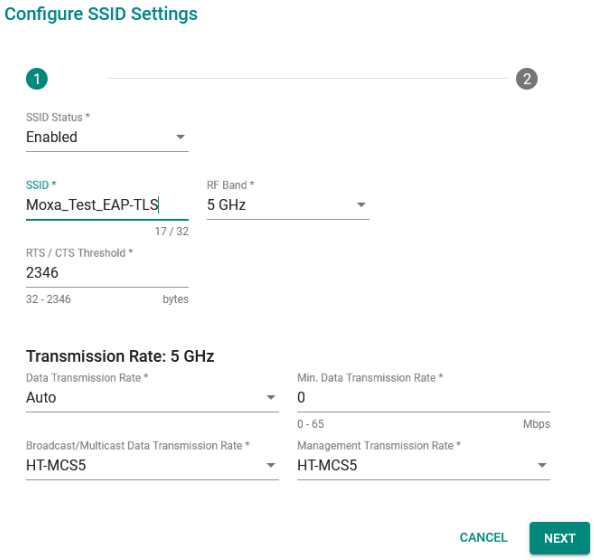


Figure 4: Creating the WPA-Enterprise SSID—Part 1

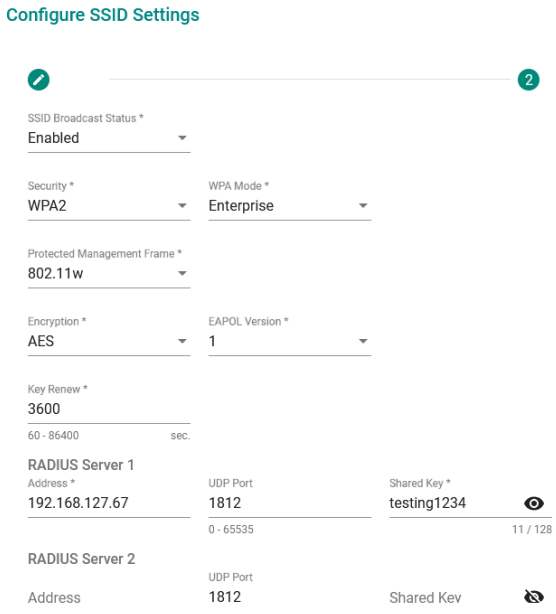


Figure 5: Creating the WPA-Enterprise SSID—Part 2

Copyright © 2026 Moxa Inc.

Select **APPLY** to activate the configuration.

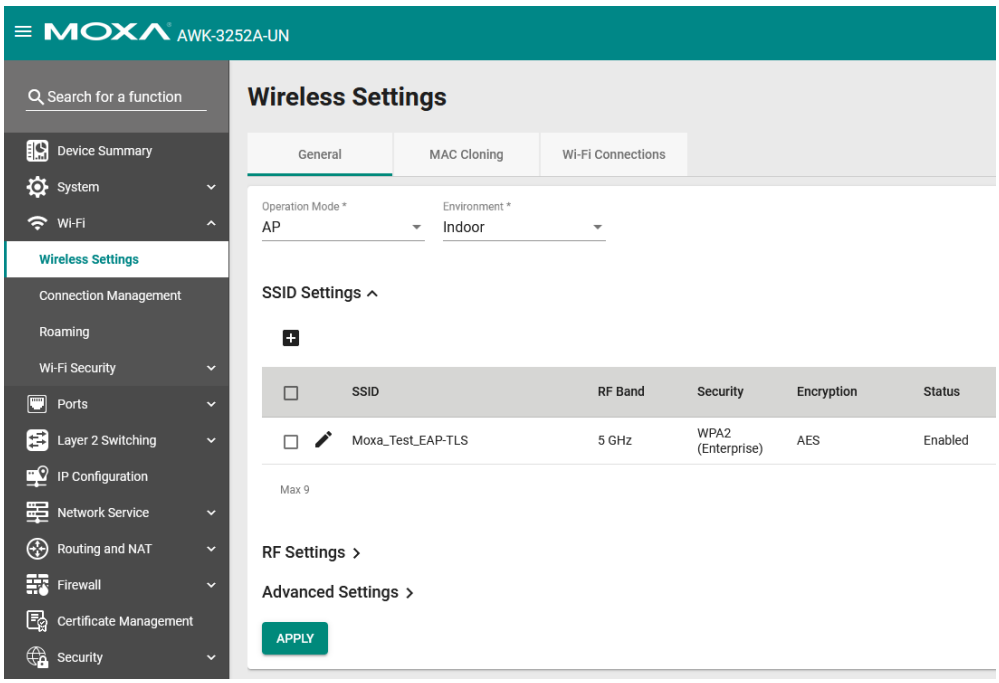


Figure 6: Activate the newly created SSID configuration

9 Configure the NPort W2150A-W4-EU

9.1 Set the Basic Settings

Go to **Main Menu > Basic Settings**.

Set the time zone to your local one. In this example: GMT+01:00 Berlin.

Set the system time/date to your local one. In this example: 2026/06/25 10:32

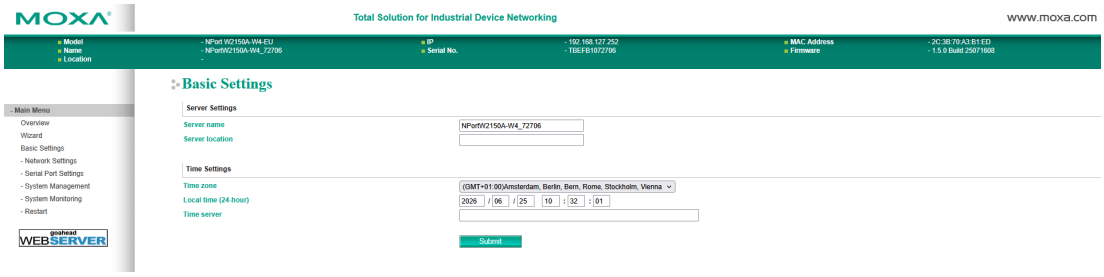


Figure 7: Basic Settings

9.2 Enable Ethernet Bridge Mode

Go to **Main Menu > Network Settings > Ethernet/Bridge Settings**. Select **Enable** from the drop-down menu at **Ethernet bridge** and set the IP-address in the **IP address** textbox for 192.168.127.252, then select **Submit**.

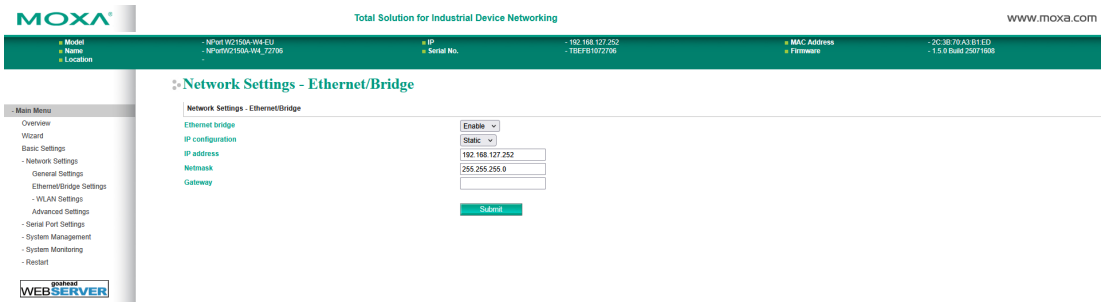


Figure 8: Set the Network Settings and Bridge mode

9.3 Check the IP Configuration and IP-Address

Go to. **Main Menu > Network Settings > WLAN Settings > WLAN.** Check that the IP address is 192.168.127.252.

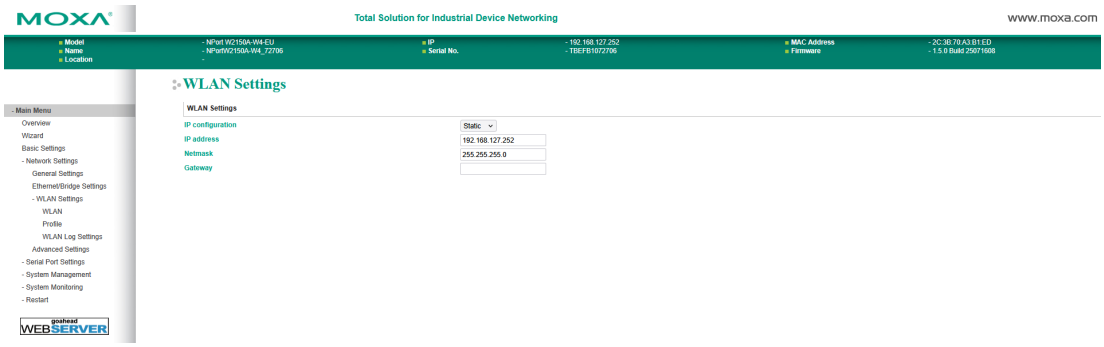


Figure 9: WLAN Settings

9.4 Import the WPA Server Certificate

Go to **Main Menu > System Management > Certificate > WPA Server Certificate Import**, then browse the `CA.crt` and select **Submit**.

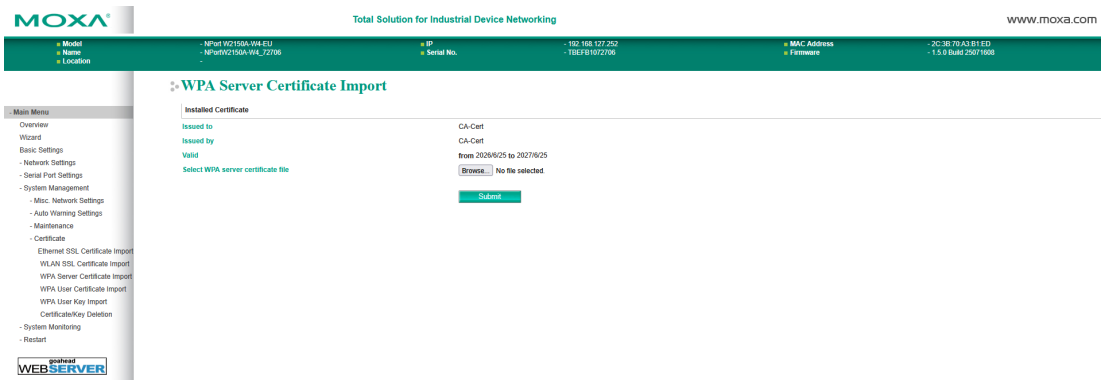


Figure 10: WPA Server Certificate Import

9.5 Import the WPA User Certificate

Go to **Main Menu > System Management > Certificate > WPA User Certificate Import**, then browse the `Client.crt` and select **Submit**.

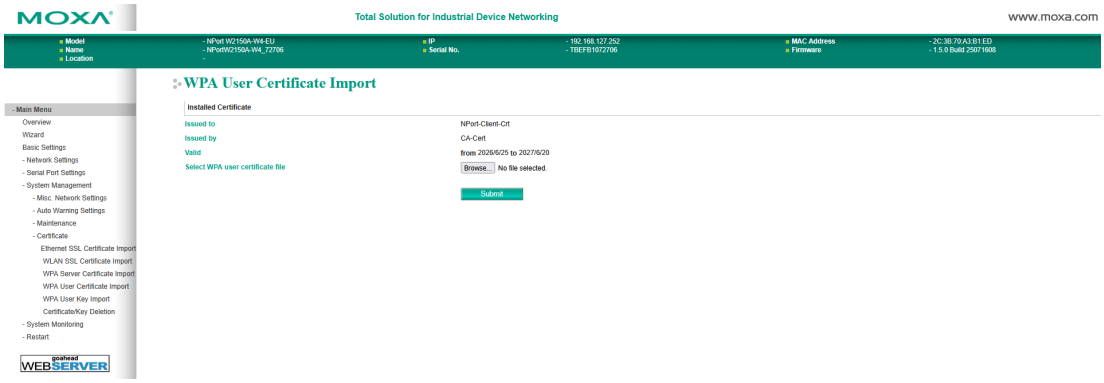


Figure 11: WPA User Certificate

9.6 Import the WPA User Key

Go to **Main Menu > System Management > Certificate > WPA User Key Import**. Browse the **`Client.key`**, type the password 1111 for the key in the **Password for private key** textbox, and select **Submit**.

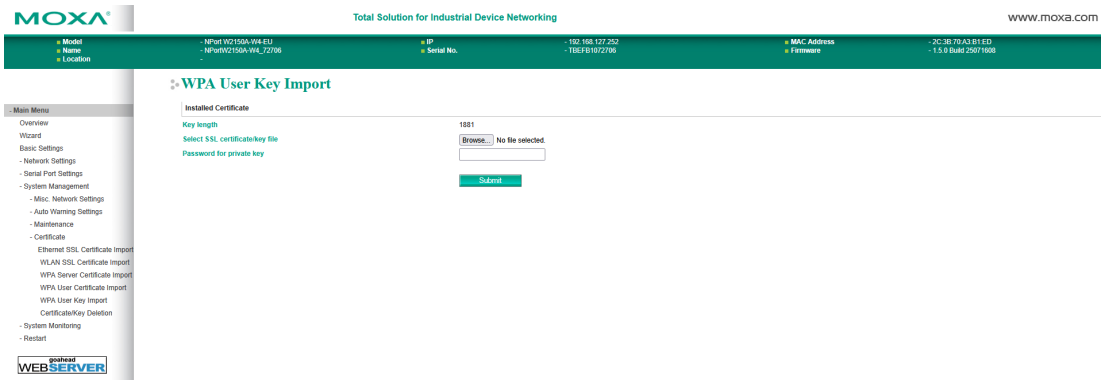


Figure 12: WPA User Key

9.7 Set the Wireless LAN Profile

Go to **Main Menu > Network Settings > WLAN Settings > Profile**. Select **General**.

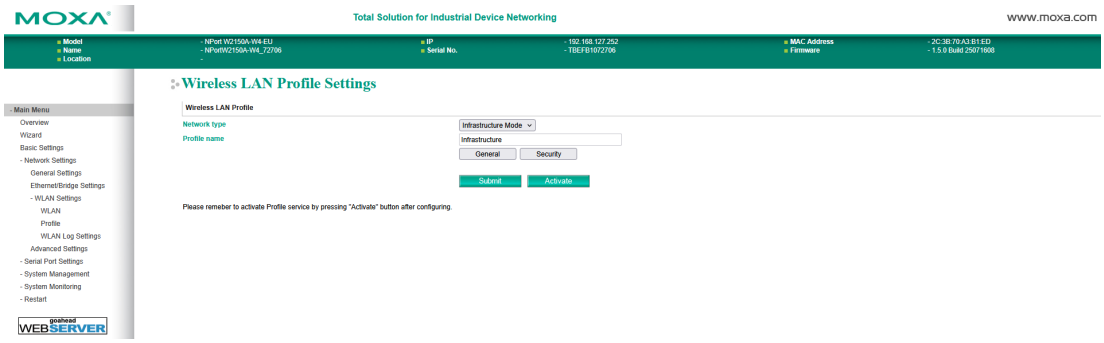


Figure 13: Wireless LAN Profile

Copyright © 2026 Moxa Inc.

9.8 Set the WLAN Profile's General Properties

Select **Site Survey**. Map the **Moxa_Test_EAP-TLS** SSID and select **Submit**.

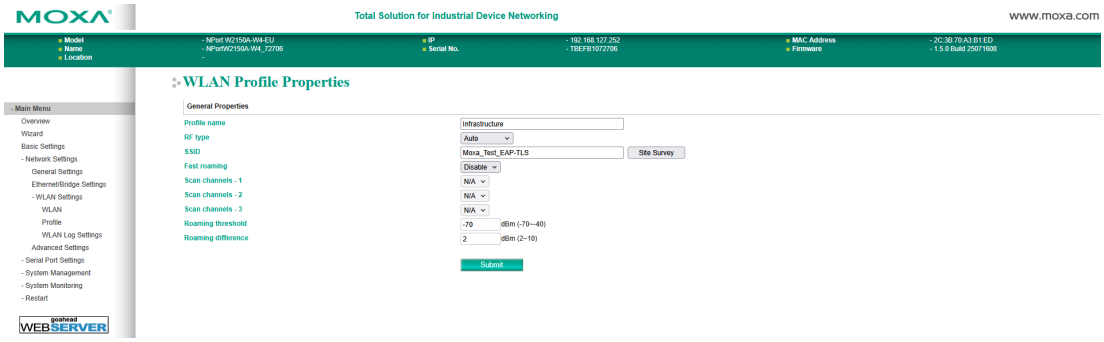


Figure 14: General Properties

9.9 Set the WLAN Profile's Security Properties

In the **Wireless LAN Profile Settings** menu, select **Security**. From the drop-down menu at the **Authentication** select **WPA2**. From the drop-down menu at the **Encryption**, select **AES-CCMP. The EAP method** should be selected as **TLS**. Type the `CN` of the client certificate in the **Username** textbox as `NPort-Client-Crt`, select **Enable** from the drop-down menu at the **Verify server certificate**, and then select **Submit**.

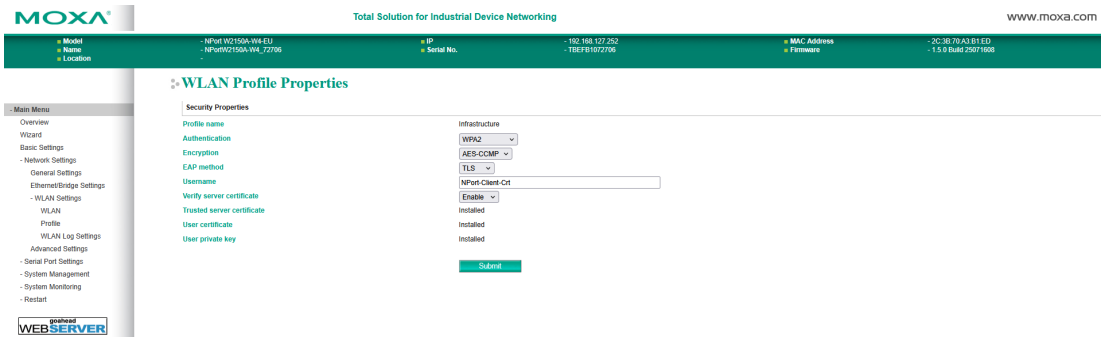


Figure 15: Security Properties

Copyright © 2026 Moxa Inc.

9.10 Submit the Wireless LAN Profile Settings

In the **Wireless LAN Profile Settings,** select **Submit**. Activate the profile by selecting **Activate**.

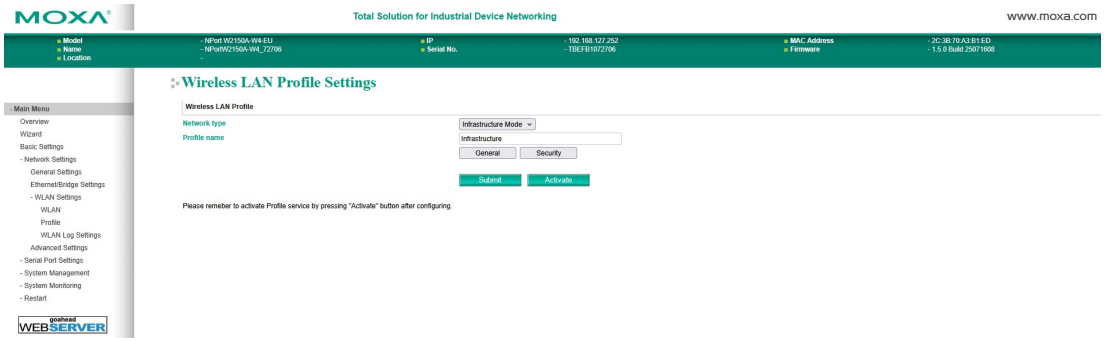


Figure 16: Wireless LAN Profile Settings

9.11 Activating WLAN Log

Go to **Main Menu > Network Settings > WLAN Settings > WLAN Log Settings**. Select **Enable** from the drop-down menu at the **WLAN Log**, and then select **Submit**.

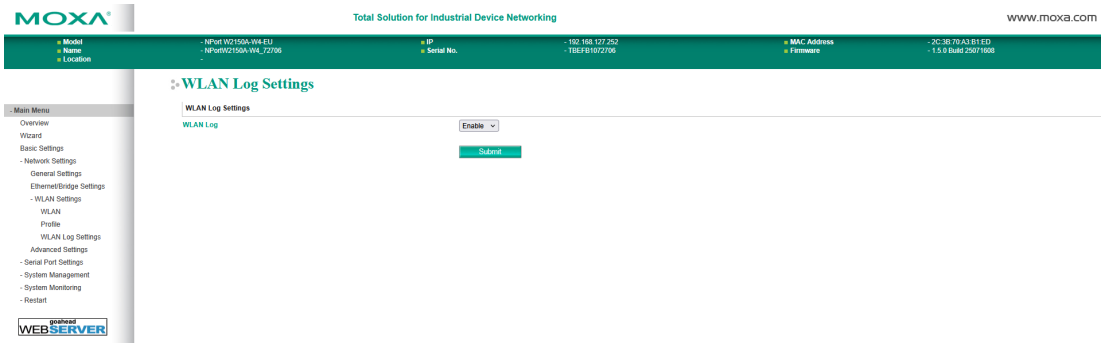


Figure 17: WLAN Log

9.12 Checking the Status of the WLAN

Go to **Main Menu > System Monitoring > System Status > WLAN Status** to check the connection to the AP.

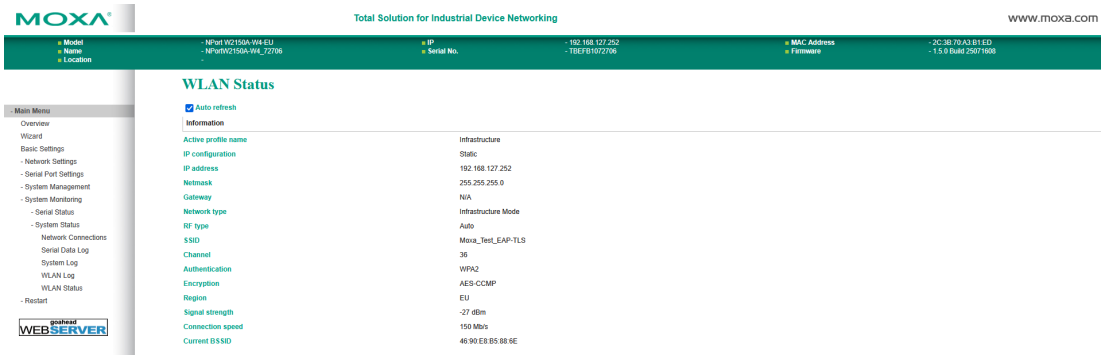


Figure 18: WLAN Status

10 Verify EAP-TLS Authentication

10.1 Check the FreeRADIUS Log

The FreeRADIUS debug log should show an **`Access-Accept`** response for the NPort client.

```
(13) Sent  Access-Accept  Id  27  from  192.168.127.67:1812  to
192.168.127.253:57316  length  184
(13)   MS-MPPE-Recv-Key =
0xb112092aecf40af61e66553feab7d548fb00b52d0393030e4c0ebe6d27961ae7
(13)   MS-MPPE-Send-Key =
0xe20702d7a5a5c50a314a9874365575131589e72085c444fcf2159e46cf5463d4
(13)   EAP-Message = 0x039a0004
(13)   Message-Authenticator = 0x00000000000000000000000000000000
(13)   User-Name = "NPort-Client-Crt"
(13)   Framed-MTU += 994
(13) Finished request
```

10.2 Check the AP Device Summary

The successful wireless client connection can be checked in the device summary of the AP.



Figure 19: AWK AP successful wireless client connection

11 Troubleshooting Checklist

If EAP-TLS authentication fails, verify the following items:

- The FreeRADIUS server certificate and private key are located in **`/etc/freeradius/3.0/certs/`**.
- **`CA.crt`**, **`Server.crt`**, and **`Server.key`** are owned by **`freerad:freerad`** and have permissions **`640`**.
- The **`private_key_password`** in the EAP module matches the passphrase used for **`Server.key`**.
- The NPort client imports the encrypted **`Client.key`** and the matching **`Client.crt`**.
- The RADIUS shared secret in **`clients.conf`** matches the AWK AP RADIUS configuration.
- The time and date, as well as the time zone, are correct on Ubuntu Server, the AWK Access Point, and the NPort Client.
- FreeRADIUS is started in debug mode with **`freeradius -X`** to inspect the exact TLS or certificate error.

Copyright © 2026 Moxa Inc.