

# How to Configure NPort W2x50A to Connect to a Cisco 2100/2500/4400/5500/Flex 7500 Series Wireless LAN Controller

Moxa Technical Support Team  
[support@moxa.com](mailto:support@moxa.com)

## Contents

- 1. Introduction..... 2
- 2. Applicable Products ..... 2
- 3. System Requirements ..... 2
- 4. System Overview ..... 2
- 5. Basic Configuration of the Cisco Controller ..... 3
  - 5.1. Enable the WLAN Function..... 3
- 6. Moxa NPort W2x50A Configuration ..... 4
  - 6.1. Configuring the NPort W2x50A with the Configuration Wizard ..... 4
- 7. Configuring Detailed WLAN Security Settings ..... 7
  - 7.1. No Security: Open System ..... 8
  - 7.2. Lowest Security: WEP ..... 9
  - 7.3. Higher Security: WPA-PSK/WPA2-PSK..... 10
  - 7.4. Highest Security: WPA/WPA2 ..... 11

---

Copyright © 2014 Moxa Inc.

Released on July 1, 2014

### About Moxa

Moxa is a leading manufacturer of industrial networking, computing, and automation solutions. With over 25 years of industry experience, Moxa has connected more than 30 million devices worldwide and has a distribution and service network that reaches customers in more than 70 countries. Moxa delivers lasting business value by empowering industry with reliable networks and sincere service for automation systems. Information about Moxa’s solutions is available at [www.moxa.com](http://www.moxa.com). You may also contact Moxa by email at [info@moxa.com](mailto:info@moxa.com).

### How to Contact Moxa

Tel: +886-2-8919-1230  
Fax: +886-2-8919-1231



# Moxa Tech Note Connecting NPort W2x50A to a Cisco WLC

## 1. Introduction

This application note describes the corresponding settings of connection authentications for Moxa's wireless NPort W2x50A series and a Cisco 2100/2500/4400/5500/Flex 7500 Series Wireless LAN Controller.

## 2. Applicable Products

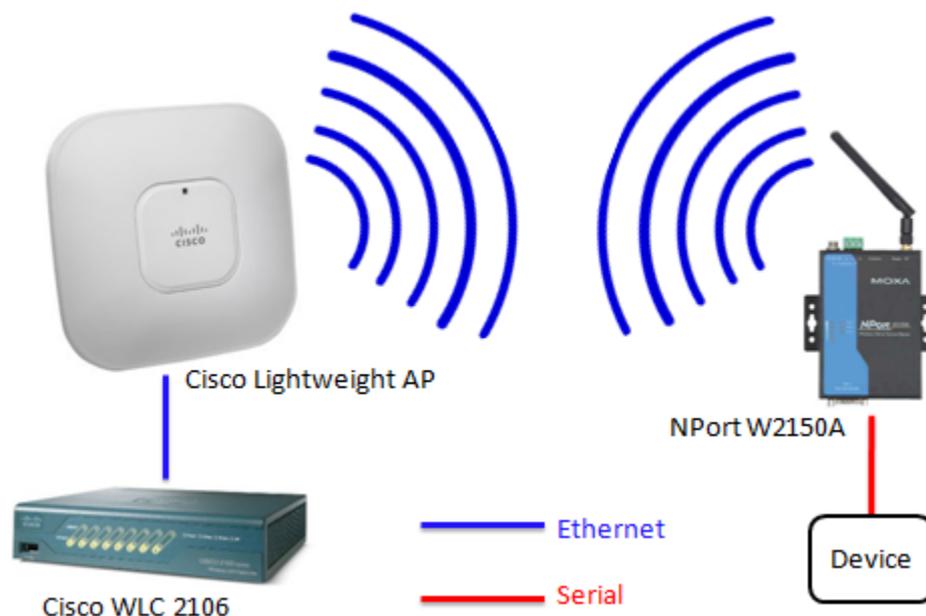
Product Line	Model Names
NPort W2x50A Series	NPort W2150A, NPort W2250A

## 3. System Requirements

Description	Model / File Name	S/W Ver.
Cisco WLC	WLC 2100/2500/4400/ 5500/Flex 7500 Series	7.0.235.0 or later
Cisco Lightweight AP	AIR-LAP1141N-A-K9 (Boot Version) (IOS Version) (Mini IOS Version)	12.4.23.3 12.4(23c)JA5 3.0.51.0
Moxa NPort W2x50A series	W2x50A	FW Ver 1.7 or later

## 4. System Overview

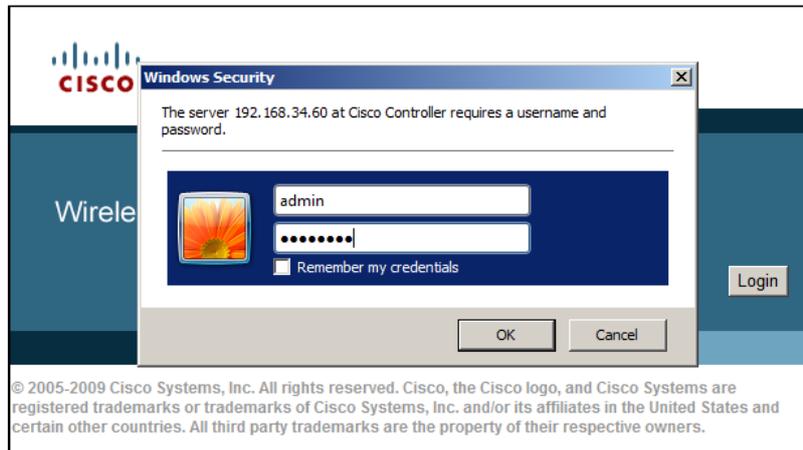
The test system architecture is shown below.



## 5. Basic Configuration of the Cisco Controller

### 5.1. Enable the WLAN Function

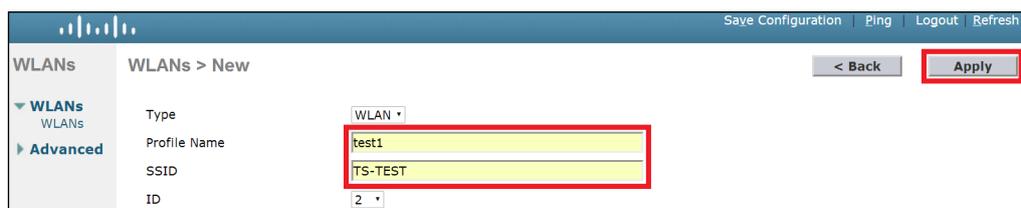
5.1.1. Log in to the controller's web GUI.



5.1.2. Click the WLANs tab. Select "Create New" to create a new profile for the wireless connection and then click **Go**.

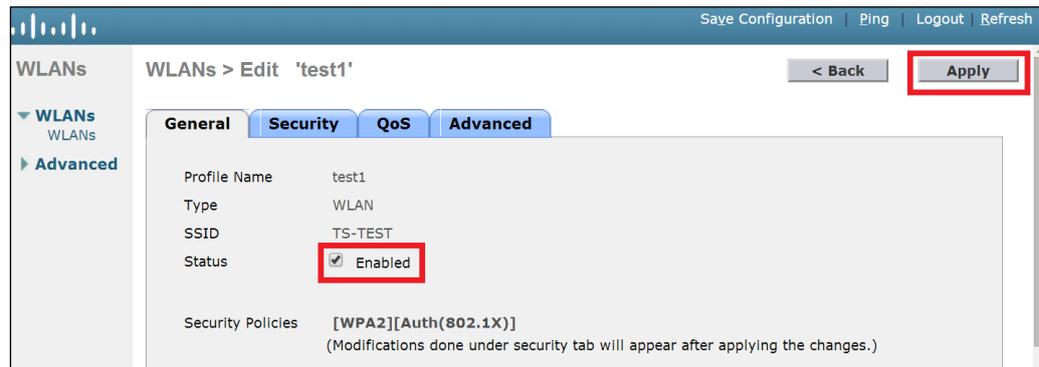


5.1.3. Fill in the Profile Name and SSID and then click **Apply**.



5.1.4. Checkmark the "Enabled" checkbox to the right of Status and then click **Apply** to complete the basic wireless settings. At this point, a wireless client should be able to find the AP using SSID TS-TEST.

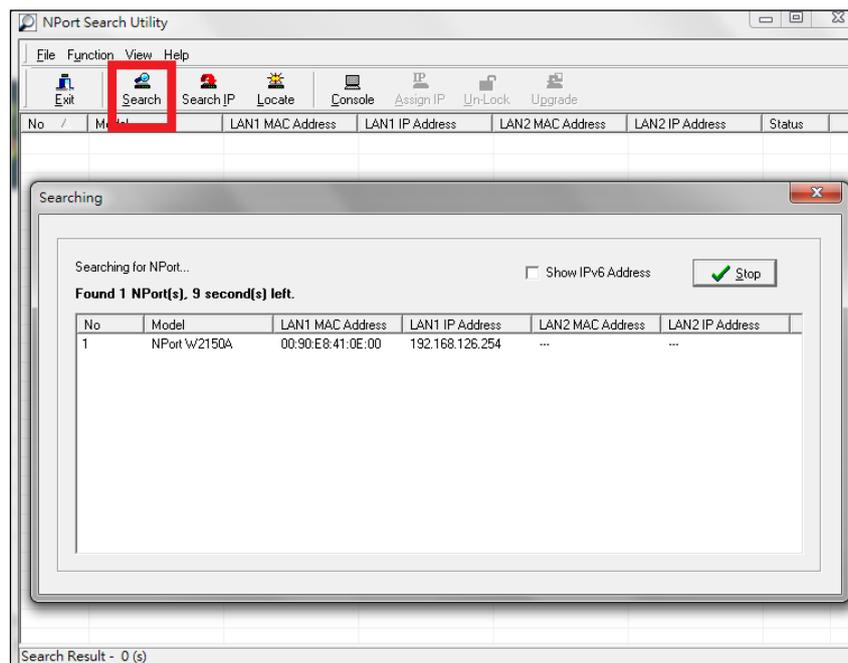
## Moxa Tech Note Connecting NPort W2x50A to a Cisco WLC



## 6. Moxa NPort W2x50A Configuration

### 6.1. Configuring the NPort W2x50A with the Configuration Wizard

6.1.1. Connect the NPort W2x50A to an Ethernet network and then power it on. Use the NPort Search Utility to locate the NPort W2x50A, and then double click on the selected NPort W2x50A to enter the web console.



6.1.2. Click "Wizard" and then take the following steps to configure the NPort W2x50A's wireless connection.

6.1.2.1. Step 1: Enter the NPort W2x50A's IP settings and then click **Next**.

## Moxa Tech Note Connecting NPort W2x50A to a Cisco WLC

Step 1/5

WLAN IP Configuration

IP configuration

IP address

Netmask

Gateway

Static

192.168.35.111

255.255.255.0

Next

goahead  
WEB SERVER  
Best viewed with IE 5 above at resolution 1024 x 768

- 6.1.2.2. Step 2: Enter the SSID for the WLAN setup. This should be the same SSID we configured in the Cisco Controller in Step 5.1.3. Click **Next** to continue.

Step 2/5

General Properties

Network type

SSID

Infrastructure Mode

TS-TEST

Back Next

- 6.1.2.3. Step 3: Choose the authentication and encryption options that match the Cisco Controller settings and then click **Next**.

Step 3/5

Security Properties

Authentication

Encryption

Open System

Disable

Back Next

*(Since we have not yet set up any authentication options in the Cisco Controller, we use Open System here to illustrate.)*

- 6.1.2.4. Step 4: Choose an operation mode for the W2x50A's serial ports and then click **Next**.

## Moxa Tech Note Connecting NPort W2x50A to a Cisco WLC

**Step 4/5**

The settings will be applied to all serial ports.

Operation Mode

Operation mode

Real COM

Back Next

6.1.2.5. Step 5: Configure the parameters for the W2x50A's serial ports and then click **Next**.

**Step 5/5**

The settings will be applied to all serial ports.

Alias	Baud rate	Parity	Data bit	Stop bit	Flow control	FIFO	Interface
	115200	None	8	1	RTS/CTS	Enable	RS-232

Back Next

6.1.3. The wizard will show the settings summary. Click **Submit** to continue.

Your changes have not been saved. Please check that your settings in the following and click "Submit" for the updates to take effect or click "Cancel" to discard.

WLAN IP Configuration	
IP configuration	static
IP address	192.168.35.111
Netmask	255.255.255.0

General Properties	
Network type	Infrastructure Mode
SSID	TS-TEST

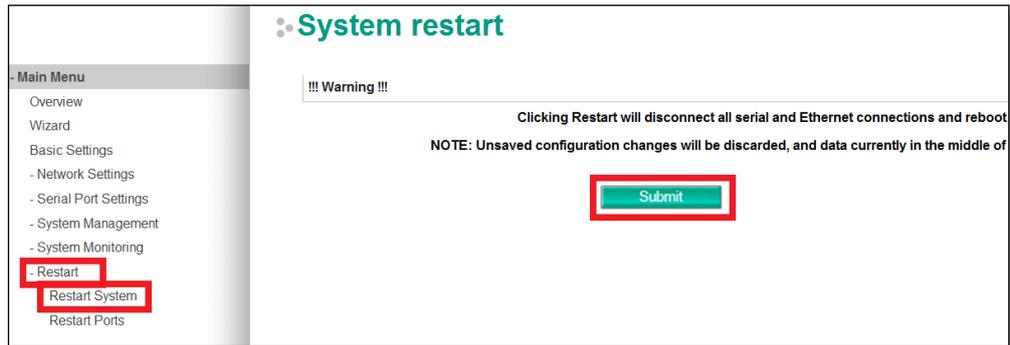
Security Properties	
Authentication	Open System
Encryption	Disable

Port 1	
Operation Mode	
Operation mode	Real COM
Serial Parameters	
Baud rate	115200
Parity	None
Data bit	8
Stop bit	1
Flow contro	RTS/CTS
FIFO	Enable
Interface	RS-232

Back Submit

6.1.4. Restart the system to activate the settings. Click Restart → Restart System → **Submit** to perform the reboot. Disconnect the Ethernet cable before booting up to enable the wireless connection.

# Moxa Tech Note Connecting NPort W2x50A to a Cisco WLC



## 7. Configuring Detailed WLAN Security Settings

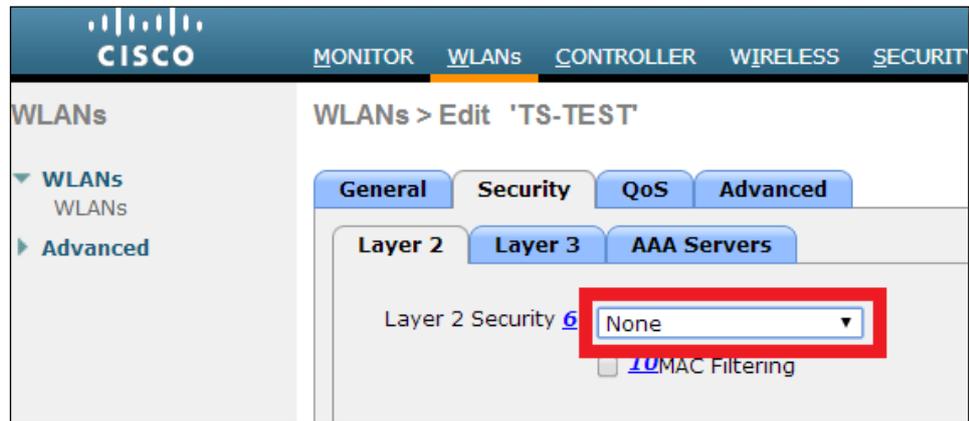
The following table shows how to map security settings between the Cisco WLC and Moxa W2x50A series. Match Moxa's Authentication with Cisco's Layer 2 security for basic settings. For more details, refer to the information in the first column of the table.

	Cisco WLC Settings	W2x50A Settings
<b>7.1 Open System</b> Cisco: None W2x50A: Open System		Security Properties Profile name: Infrastructure Authentication: Open System Encryption: Disable
<b>7.2 WEP</b> Cisco: Static WEP W2x50A: Shared Key-WEP		Security Properties Profile name: Infrastructure Authentication: Shared Key Encryption: WEP
<b>7.3 WPA-PSK/WPA2-PSK</b> Cisco: WPA+WPA2 & PSK W2x50A: WPA-PSK/WPA2-PSK		Security Properties Profile name: Infrastructure Authentication: WPA-PSK Encryption: AES-CCMP
<b>7.4 WPA/WPA2</b> Cisco: WPA+WPA2 & 802.1X W2x50A: WPA/WPA2		Security Properties Profile name: Infrastructure Authentication: WPA2 Encryption: TKIP

## Moxa Tech Note Connecting NPort W2x50A to a Cisco WLC

### 7.1. No Security: Open System

7.1.1. Enter the Cisco Controller's web GUI and click WLANs → (WLAN ID) → Security → Layer 2, select None for Layer 2 Security.



7.1.2. Enter the NPort W2x50A's web console and choose Network Settings → WLAN Settings → Profile → Security; select Open System for Authentication and Disable for Encryption.



7.1.3. Save all the settings and restart the NPort W2x50A. Disconnect the Ethernet cable before booting up to enable the wireless connection. From the Cisco Controller, check that the NPort W2x50A has successfully established a connection with the Cisco AP.



## Moxa Tech Note Connecting NPort W2x50A to a Cisco WLC

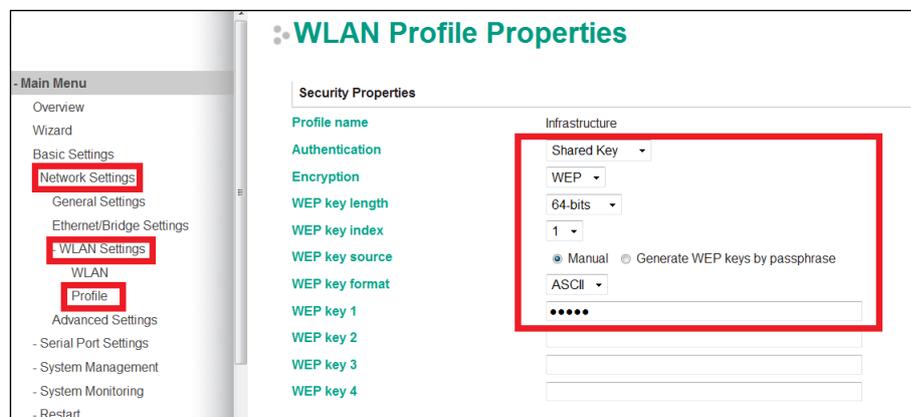
### 7.2. Lowest Security: WEP

- 7.2.1. Enter the Cisco Controller's web GUI and click WLANs → (WLAN ID) → Security → Layer 2, and select Static WEP. Select Key Size, enter the Encryption Key, and checkmark Enabled to the right of Allow Shared Key Authentication.



(12345 is an example)

- 7.2.2. Enter the NPort W2x50A's web console, choose Network Settings → WLAN Settings → Profile → Security; select Shared Key for Authentication and WEP for Encryption.



Note: Choose 64-bit length to match the 40-bit setting in the Cisco Controller.

- 7.2.3. Save all the settings and restart the NPort W2x50A. Disconnect the Ethernet cable before booting up to enable the wireless connection. From the Cisco Controller, check that the NPort W2x50A has successfully established a connection with the Cisco AP.

## Moxa Tech Note Connecting NPort W2x50A to a Cisco WLC



### 7.3. Higher Security: WPA-PSK/WPA2-PSK

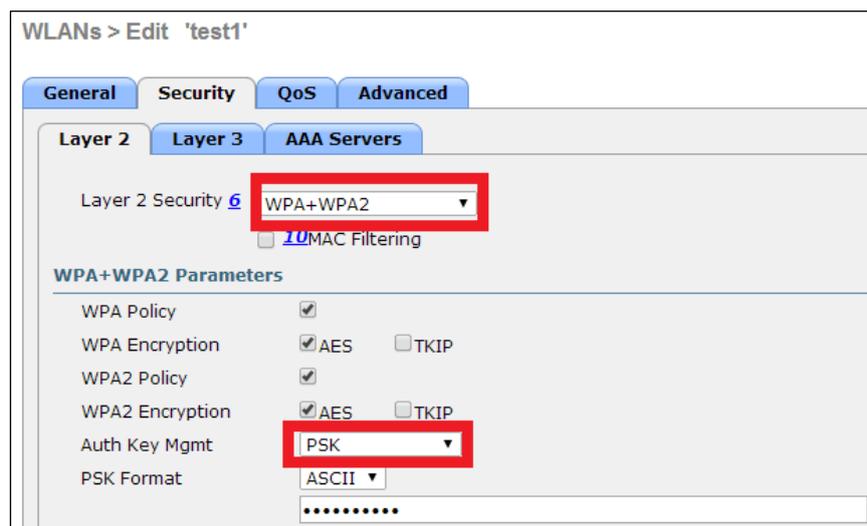
7.3.1. Enter the Cisco Controller's web GUI, click WLANs → (WLAN ID) → Security → Layer 2, and select WPA+WPA2 for Layer 2 Security.

Four types of security can be configured:

Authentication \ Encryption	WPA	WPA2
<b>AES</b>	WPA Policy Enable AES Enable	WPA2 Policy Enable AES Enable
<b>TKIP</b>	WPA Policy Enable TKIP Enable	WPA2 Policy Enable TKIP Enable

The Cisco Controller can enable the above four types simultaneously, which means that if the wireless client supports any of the above and the key is correct, the wireless client can successfully establish a wireless connection. To enable any of the above, check the appropriate checkbox. In the screenshot below, we illustrate enabling Authentication with WPA and WPA2, and Encryption mode with AES.

Choose "PSK" for Auth Key Mgmt to use Pre-Shared Key security.



## Moxa Tech Note Connecting NPort W2x50A to a Cisco WLC

7.3.2. For Moxa's NPort W2x50A, we can only enable one of the above four types at a time. In this example, we select WPA-PSK for Authentication and AES-CCMP for Encryption.

Enter the NPort W2x50A's web console, choose Network Settings → WLAN Settings → Profile → Security, and then select WPA-PSK for Authentication and AES-CCMP for Encryption.



7.3.3. Save all the settings and restart the NPort W2x50A. Disconnect the Ethernet cable before booting up to enable the wireless connection. From the Cisco controller, check that the NPort W2x50A has successfully established a connection with the Cisco AP.



Client MAC Addr	AP Name	WLAN Profile	WLAN SSID	Protocol	Status	Auth	Port	WGB
40:2c:f4:fd:80:70	APa493.4c81.dfb3	test1	TS-TEST	802.11g	Associated	Yes	1	No

### 7.4. Highest Security: WPA/WPA2

7.4.1. Using a RADIUS server for the wireless client can provide greater security on the wireless network. We use a FreeRADIUS server under Linux to illustrate; the main settings are shown below.

7.4.1.1. Add Username and User-Password in the file "users"

```
#DEFAULT          Group == "disabled", Auth-T
#                  Reply-Message = "Your accou
#
moxa_admin        User-Password == "moxa123 "
```

## Moxa Tech Note Connecting NPort W2x50A to a Cisco WLC

- 7.4.1.2. Add RADIUS server client(AP) & RADIUS key(secret) in the file "clients.conf"

```
client 192.168.34.41 {  
    secret      = 1111111  
    shortname   = cisco_ap  
}
```

- 7.4.1.3. Set the EAP method in file "EAP.conf"

```
#  
#default_eap_type = md5  
#default_eap_type = tls  
default_eap_type = peap  
#default_eap_type = tls  
#default_eap_type = leap
```

```
peap {  
    private_key_password = subca1234  
    private_key_file = ${raddbdir}/subca/private/cakey.  
  
    certificate_file = ${raddbdir}/subca/cacert.pem  
    CA_file = ${raddbdir}/myca/demoCA/cacert.pem  
    dh_file = ${raddbdir}/certs/dh  
    random_file = ${raddbdir}/certs/random  
  
    # The tunneled EAP session needs a default  
    # EAP type which is separate from the one for  
    # the non-tunneled EAP module. Inside of the  
    # PEAP tunnel, we recommend using MS-CHAPv2,  
    # as that is the default type supported by  
    # Windows clients.  
    default_eap_type = mschapv2  
    #default_eap_type = gtc  
    #default_eap_type = md5
```

- 7.4.2. Enter the Cisco controller's web GUI, click WLANs → (WLAN ID) → Security tab → Layer 2, and select WPA+WPA2 for Layer 2 Security. A more detailed explanation is given in step 7.3.1.

Here we use WPA2 for Authentication and TKIP for Encryption as an example. Choose "802.1X" for Auth Key Mgmt to select a associate a RADIUS server with the wireless client.

## Moxa Tech Note Connecting NPort W2x50A to a Cisco WLC

WLANs > Edit 'test1'

General Security QoS Advanced

Layer 2 Layer 3 AAA Servers

Layer 2 Security **WPA+WPA2**

10MAC Filtering

**WPA+WPA2 Parameters**

WPA Policy

WPA2 Policy

WPA2 Encryption  AES  TKIP

Auth Key Mgmt **802.1X**

### 7.4.3. Add RADIUS Server in the Cisco controller.

7.4.3.1. Click SECURITY → RADIUS → Authentication, and then click **New...**

CISCO MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK Save Configuration Ping Logout Refresh

Security RADIUS Authentication Servers Apply **New...**

AAA  
General  
**RADIUS Authentication**  
Accounting  
Fallback  
TACACS+  
LDAP  
Local Net Users  
MAC Filtering

Call Station ID Type **IP Address**

Use AES Key Wrap  (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

MAC Delimiter **Hyphen**

Network User Management Server Index Server Address Port IPsec Admin Status

7.4.3.2. Create a new RADIUS Authentication Server. Enter the RADIUS server's IP Address and RADIUS key (the same key used in step 7.4.1.2; we use 1111111 to illustrate).

RADIUS Authentication Servers > New

Server Index (Priority) **1**

Server IP Address **192.168.35.96**

Shared Secret Format **ASCII**

Shared Secret **.....**

Confirm Shared Secret **.....**

Key Wrap  (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

Port Number **1812**

Server Status **Enabled**

Support for RFC 3576 **Enabled**

Server Timeout **2** seconds

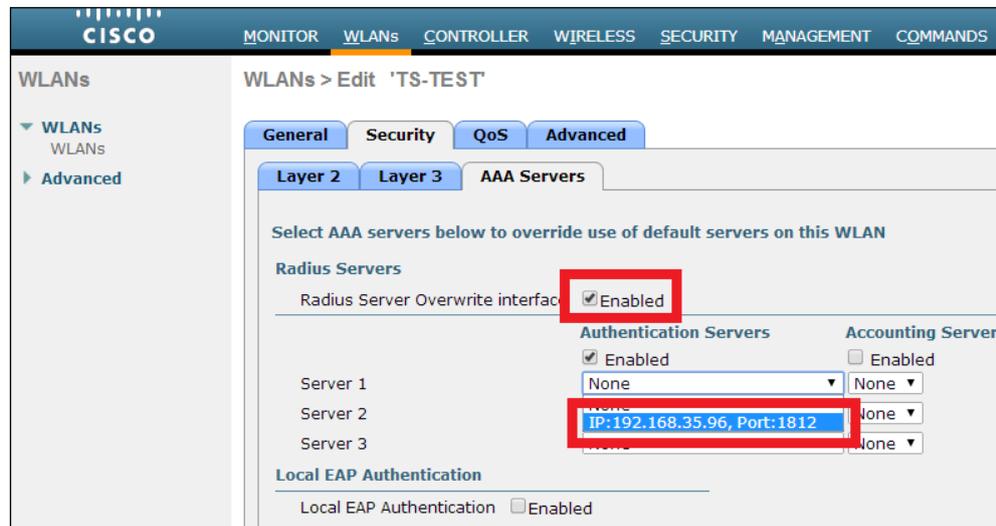
Network User  Enable

Management  Enable

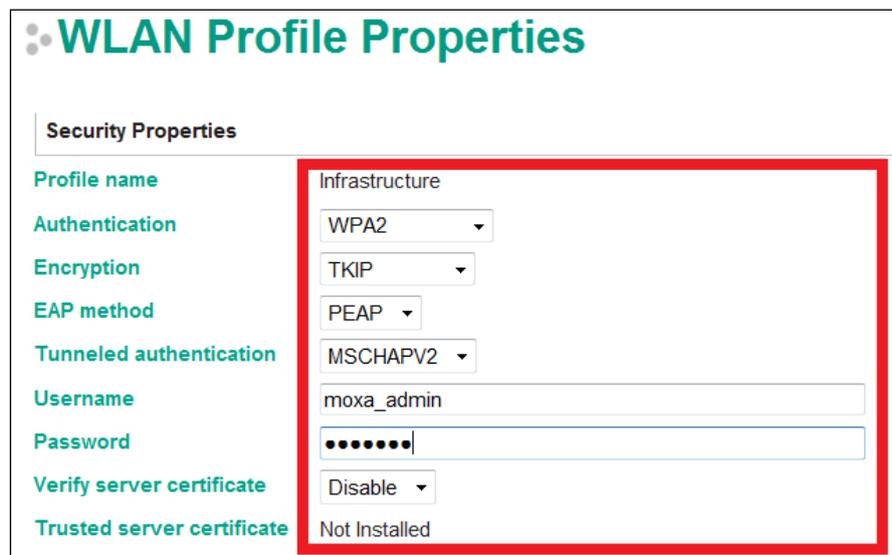
IPsec  Enable

## Moxa Tech Note Connecting NPort W2x50A to a Cisco WLC

- 7.4.4. Go to WLANs → (WLAN ID) → Security tab → AAA Servers and select which RADIUS server should be used for this WLAN profile.

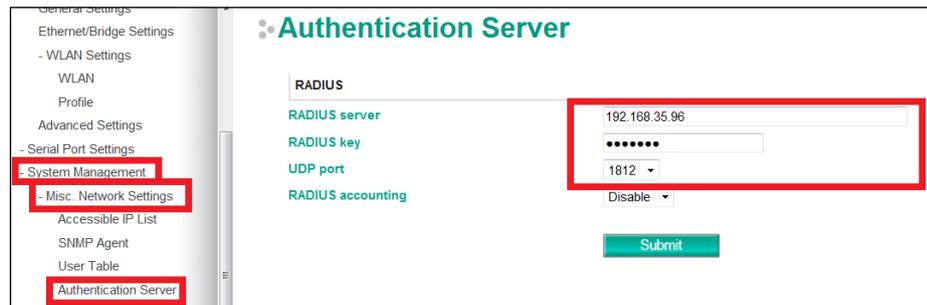


- 7.4.5. Enter the NPort W2x50A's web console, choose Network Settings → WLAN Settings → Profile → Security, and select WPA2 for Authentication and TKIP for Encryption (the same settings as step 7.4.2 for the Cisco Controller). Next configure EAP method as PEAP and Tunneled authentication as MSCHAPV2 (the same settings as step 7.4.1.3 for the RADIUS server). Finally, input the Username moxa\_admin and password moxa123 (the same settings as step 7.4.1.1 for the RADIUS server).



## Moxa Tech Note Connecting NPort W2x50A to a Cisco WLC

7.4.6. We also need to add the RADIUS server to the NPort W2x50A. Choose System Management → Misc. Network Settings → Authentication Server and add relative information, and then configure IP address, RADIUS key (also called secret key, which is configured in step 7.4.1.2.), and UDP port (default = 1812).



The screenshot shows the 'Authentication Server' configuration page. The left sidebar has 'System Management', 'Misc. Network Settings', and 'Authentication Server' highlighted with red boxes. The main content area has a 'RADIUS' section with the following fields: 'RADIUS server' (192.168.35.96), 'RADIUS key' (masked with dots), 'UDP port' (1812), and 'RADIUS accounting' (Disable). A 'Submit' button is at the bottom right.

7.4.7. Save all the settings and restart the NPort W2x50A. Disconnect the Ethernet cable before booting up to enable the wireless connection. From the Cisco Controller, check that the NPort W2x50A has successfully established a connection with the Cisco AP.



The screenshot shows the Cisco WLC Monitor page. The 'MONITOR' tab is selected. The 'Clients' section is active, showing a table of connected clients. The table has columns for Client MAC Addr, AP Name, WLAN Profile, WLAN SSID, Protocol, Status, Auth, Port, and WGB. A red box highlights the first row of data.

Client MAC Addr	AP Name	WLAN Profile	WLAN SSID	Protocol	Status	Auth	Port	WGB
40:2c:f4:fd:80:70	APa493.4c81.dfb3	test1	TS-TEST	802.11g	Associated	Yes	1	No