How to Configure NPort W2x50A/W2x50A-W4 to Connect to a Cisco 2100/2500/4400/5500/Flex 7500 Series Wireless LAN Controller

Moxa Technical Support Team

support@moxa.com

Contents

 Released on Jun 2, 2023

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 35 years of industry experience, Moxa has connected more than 82 million devices worldwide and has a distribution and service network that reaches customers in more than 80 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 Introduction

This application note describes the corresponding settings of connection authentications for Moxa's wireless NPort W2x50A/W2x50A-W4 Series and a Cisco 2100/2500/4400/ 5500/Flex 7500 Series Wireless LAN Controller.

2 Applicable Products

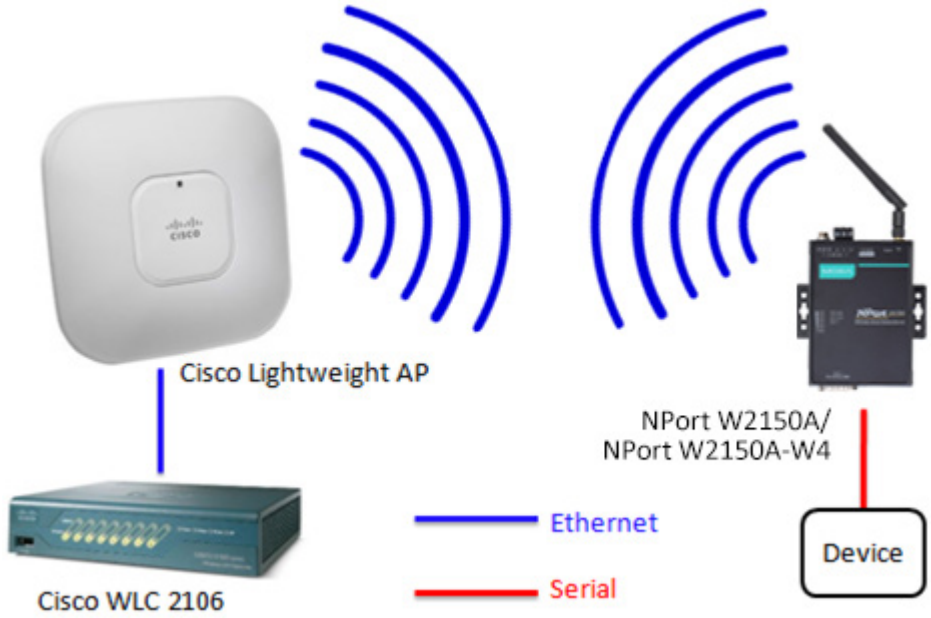
Product Line	Model Names
NPort W2x50A/W2x50A-W4 Series	NPort W2150A, NPort W2250A, NPort W2150A-W4(-T), NPort W2250A-W4(-T)

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/ W2x50A-W4 Series	W2x50A, W2x50A-W4	FW Ver 1.7 or later

4 System Overview

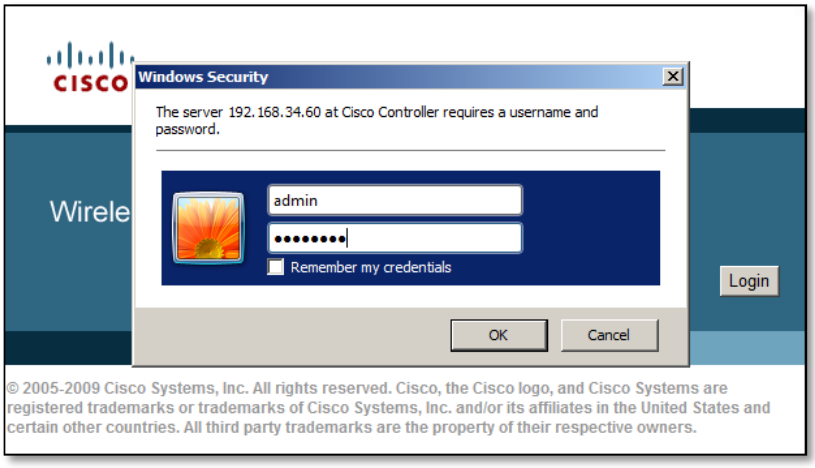
The test system architecture is below.



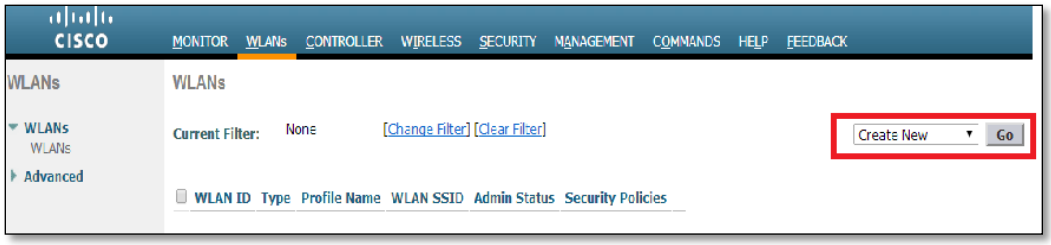
5 Basic Configuration of the Cisco Controller

5.1 Enable the WLAN Function

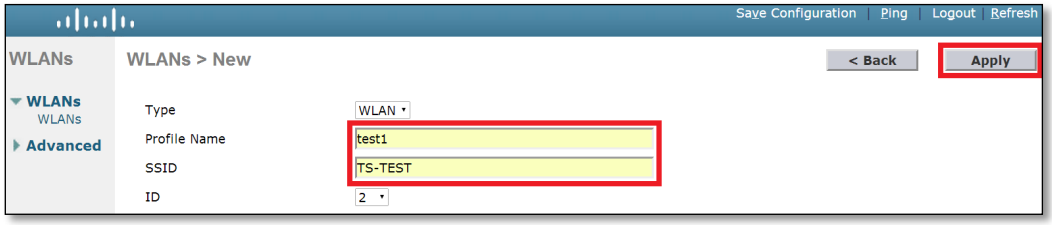
1. Log in to the controller's web GUI.



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



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

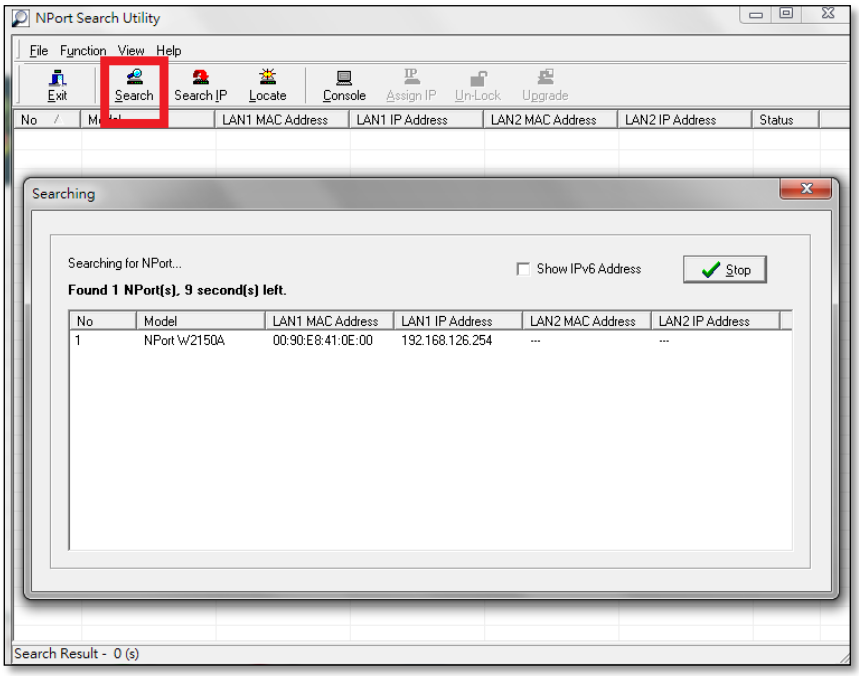


4. Checkmark the "Enabled" checkbox to the right of Status and then click **Apply** to complete the basic wireless settings. At this point, a wireless client should be able to find the AP using SSID TS-TEST.

6 Moxa NPort W2x50A/W2x50A-W4 Configuration

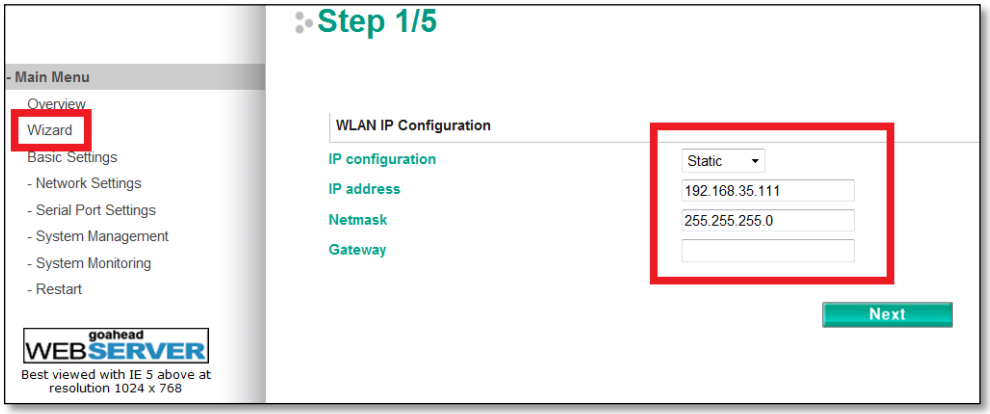
6.1 Configuring the NPort W2x50A/W2x50A-W4 with the Configuration Wizard

1. Connect the NPort W2x50A/W2x50A-W4 to an Ethernet network and then power it on. Use the NPort Search Utility or DSU Utility to locate the NPort W2x50A/W2x50A-W4, and then double click on the selected NPort W2x50A/W2x50A-W4 to enter the web console.

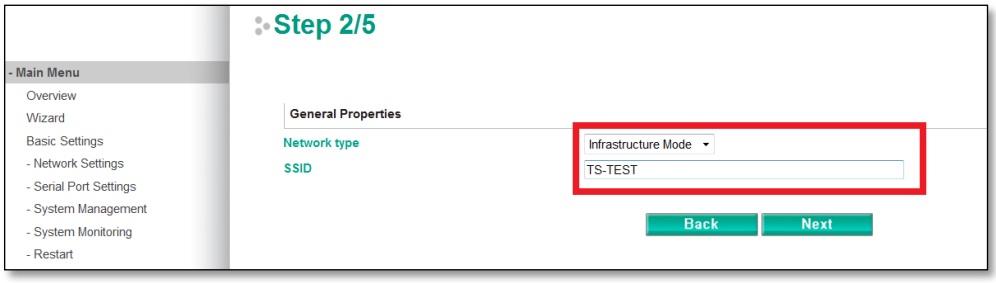


2. Click "Wizard" and then take the following steps to configure the NPort W2x50A/W2x50A-W4's wireless connection.

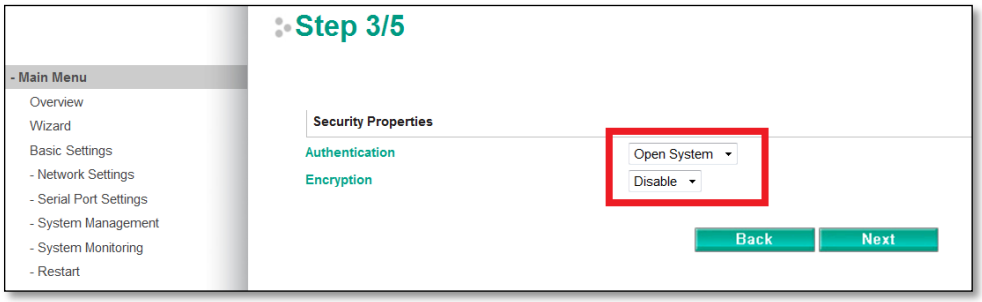
   a. Step 1: Enter the NPort W2x50A/W2x50A-W4's IP settings and then click **Next**.



b. 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.

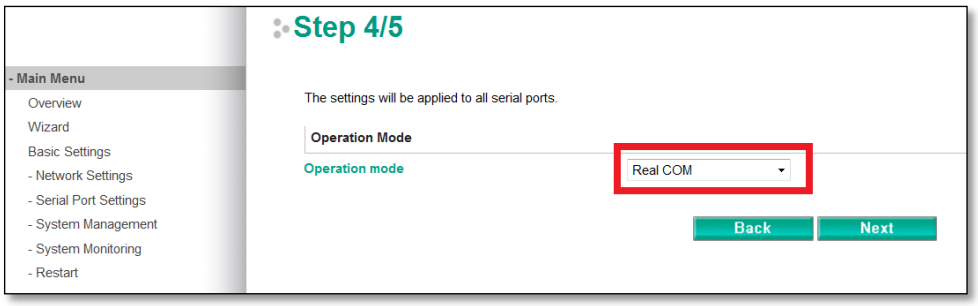


c. Step 3: Choose the authentication and encryption options that match the Cisco Controller settings and then click **Next**.

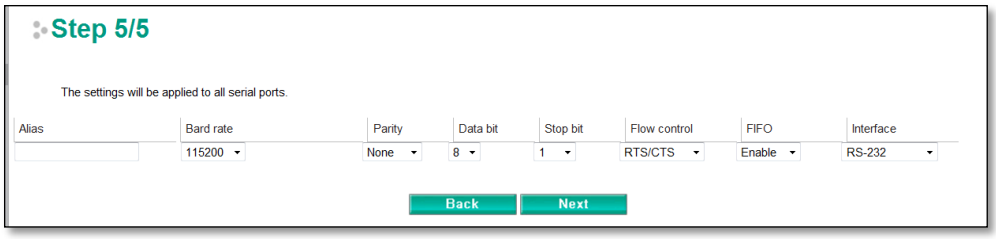


(Since we have not yet set up any authentication options in the Cisco Controller, we use Open System here to illustrate.)

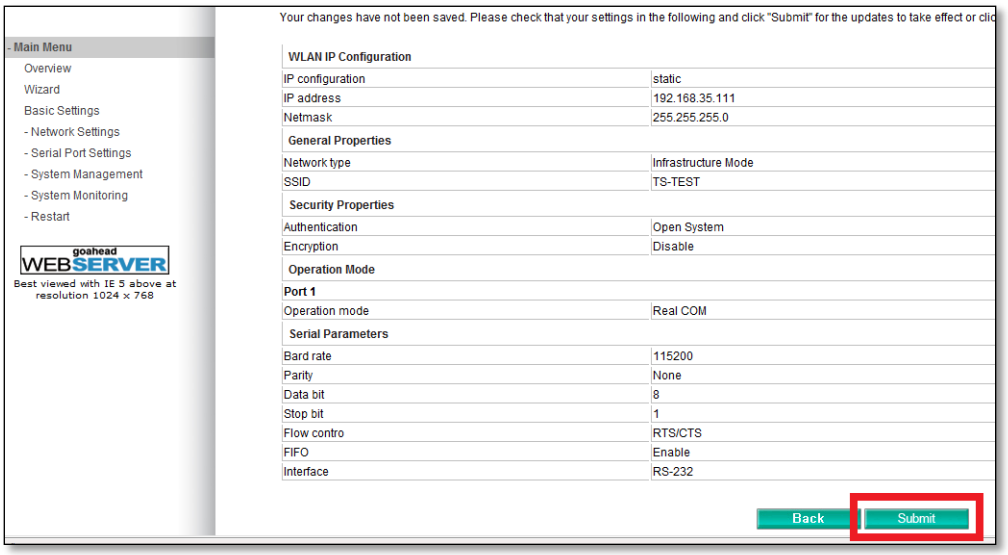
d. Step 4: Choose an operation mode for the W2x50A/W2x50A-W4's serial ports and then click **Next**.



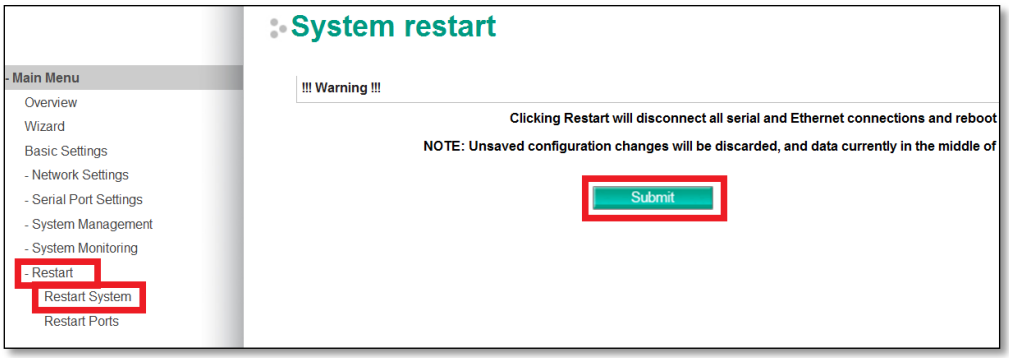
e. Step 5: Configure the parameters for the W2x50A/W2x50A-W4's serial ports and then click **Next**.



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

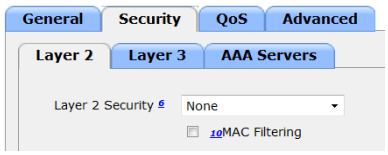
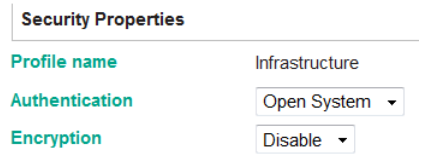
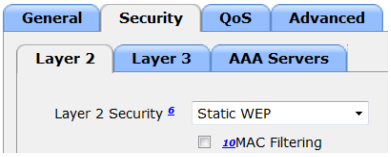
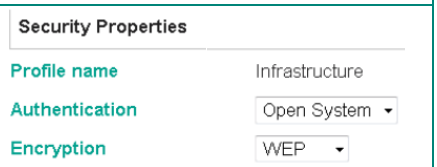
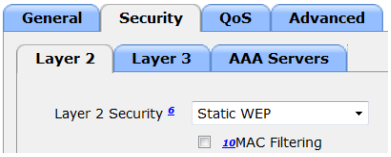
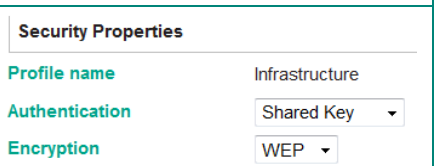
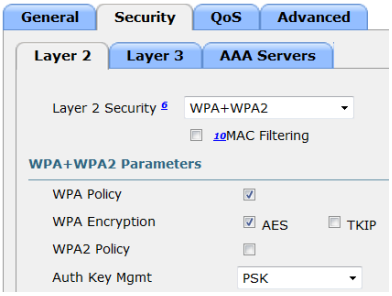
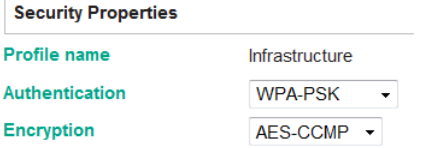
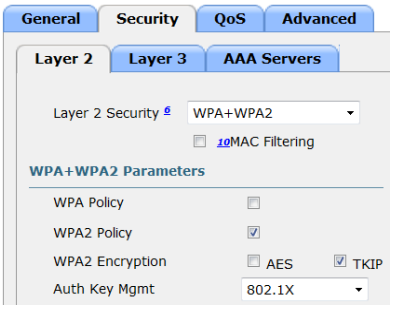
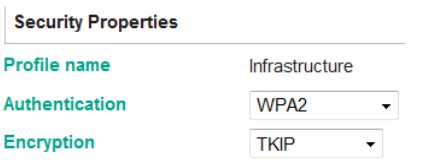


4. Restart the system to activate the settings. Click Restart > Restart System > Submit to perform the reboot. Disconnect the Ethernet cable before booting up to enable the wireless connection.



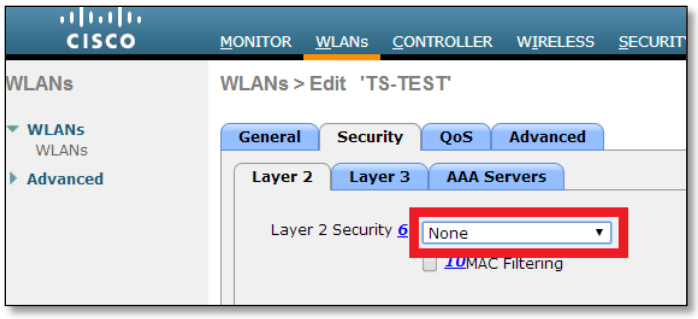
7 Configuring Detailed WLAN Security Settings

The following table shows how to map security settings between the Cisco WLC and Moxa W2x50A/W2x50A-W4 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/W2x50A-W4 Settings
7.1.1 Open System Cisco: None W2x50A/W2x50A-W4: Open System		
7.1.2 Open System Cisco: Stiatic WEP W2x50A/W2x50A-W4: Open System		
7.2 WEP Cisco: Static WEP W2x50A/W2x50A-W4: Shared Key-WEP		
7.3 WPA-PSK/WPA2-PSK Cisco: WPA+WPA2 & PSK W2x50A/W2x50A-W4: WPA-PSK/WPA2-PSK		
7.4 WPA/WPA2 Cisco: WPA+WPA2 & 802.1X W2x50A/W2x50A-W4: WPA/WPA2		

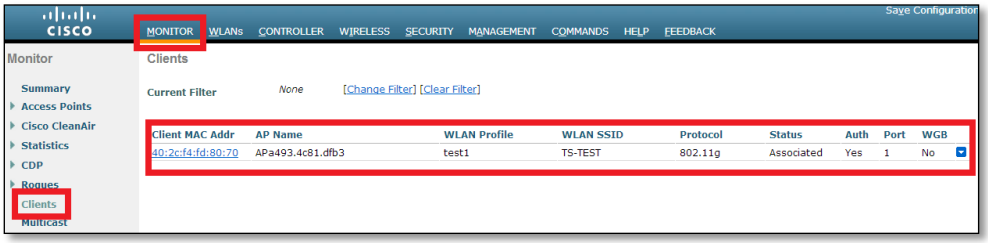
7.1 No Security: Open System

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



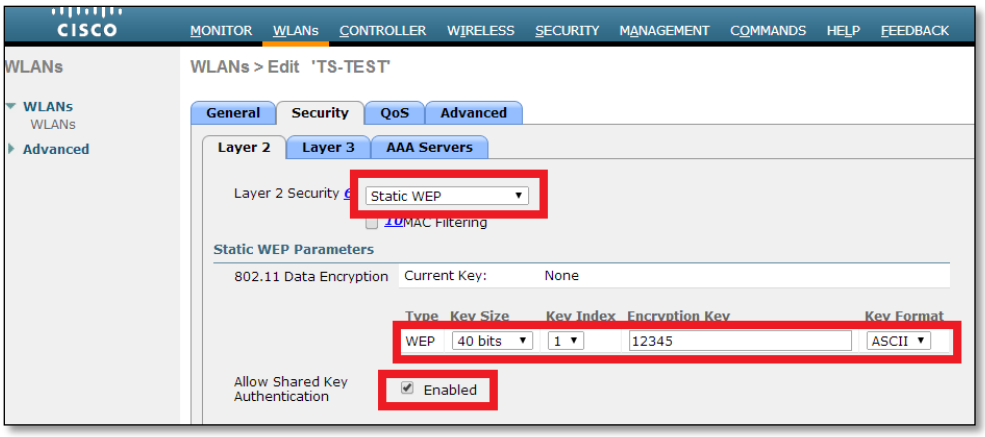
2. Enter the NPort W2x50A/W2x50A-W4's web console and choose Network Settings > WLAN Settings > Profile > Security; select Open System for Authentication and Disable for Encryption.

3. Save all the settings and restart the NPort W2x50A/W2x50A-W4. Disconnect the Ethernet cable before booting up to enable the wireless connection. From the Cisco Controller, check that the NPort W2x50A/W2x50A-W4 has successfully established a connection with the Cisco AP.



7.2 Lowest Security: WEP

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.

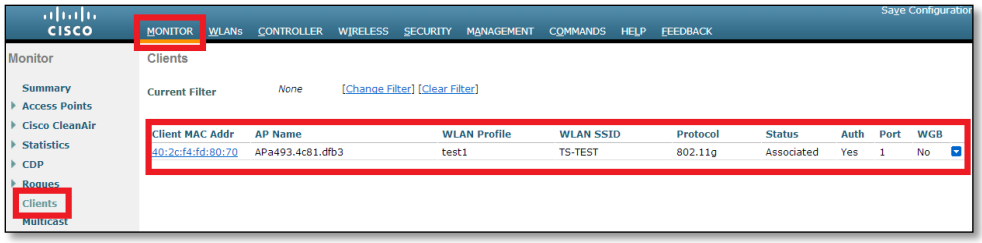


(12345 is an example)

2. Enter the NPort W2x50A/W2x50A-W4'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.

3. Save all the settings and restart the NPort W2x50A/W2x50A-W4. Disconnect the Ethernet cable before booting up to enable the wireless connection. From the Cisco Controller, check that the NPort W2x50A/W2x50A-W4 has successfully established a connection with the Cisco AP.



7.3 Higher Security: WPA-PSK/WPA2-PSK

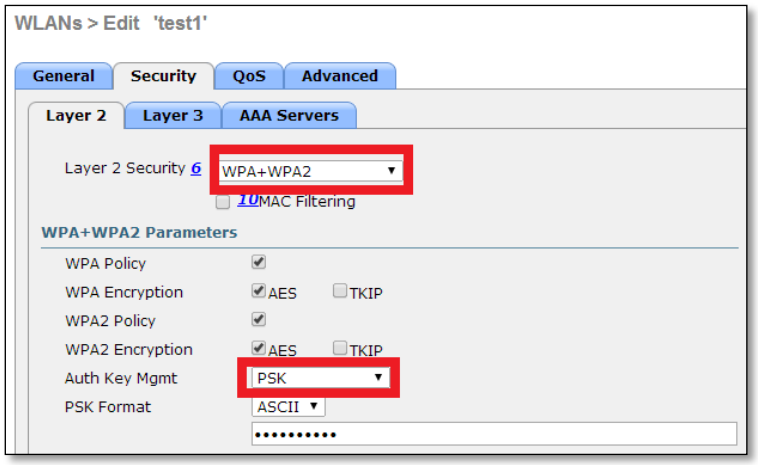
1. Enter the Cisco Controller's web GUI, click WLANs > (WLAN ID) > Security > Layer 2, and select WPA+WPA2 for Layer 2 Security.

   Four types of security can be configured:

Authentication / Encryption	WPA	WPA2
AES	WPA Policy Enable AES Enable	WPA2 Policy Enable AES Enable
TKIP	WPA Policy Enable TKIP Enable	WPA2 Policy Enable TKIP Enable

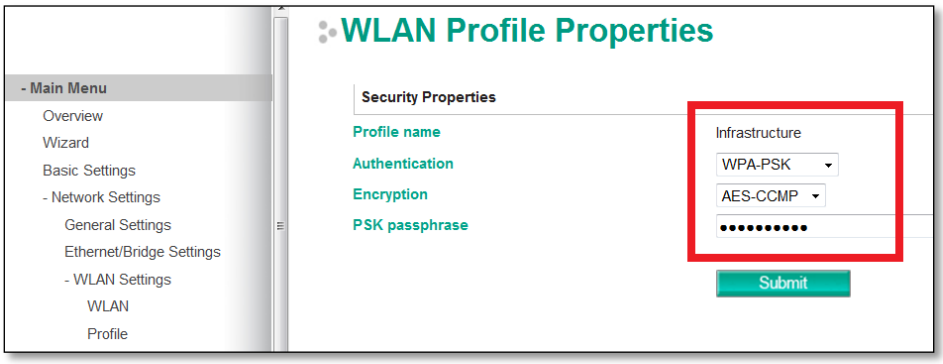
   The Cisco Controller can enable the above four types simultaneously, so if the wireless client supports any of the above and the key is correct, the wireless client can successfully establish a wireless connection. To enable any of the above, check the appropriate checkbox. In the screenshot below, we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

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

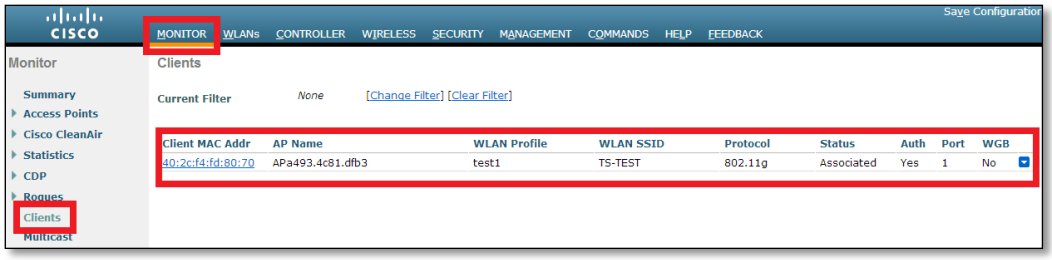


2. For Moxa's NPort W2x50A/W2x50A-W4, we can only enable one of the above four types at a time. In this example, we select WPA-PSK for Authentication and AES-CCMP for Encryption.

   Enter the NPort W2x50A/W2x50A-W4's web console, choose Network Settings > WLAN Settings > Profile > Security, and then select WPA-PSK for Authentication and AES-CCMP for Encryption.



3. Save all the settings and restart the NPort W2x50A/W2x50A-W4. Disconnect the Ethernet cable before booting up to enable the wireless connection. From the Cisco controller, check that the NPort W2x50A/W2x50A-W4 has successfully established a connection with the Cisco AP.



7.4 Highest Security: WPA/WPA2

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.

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

```
#DEFAULT        Group == "disabled", Auth-T
#               Reply-Message = "Your accou
#

moxa_admin     User-Password == "moxa123 "
```

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

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

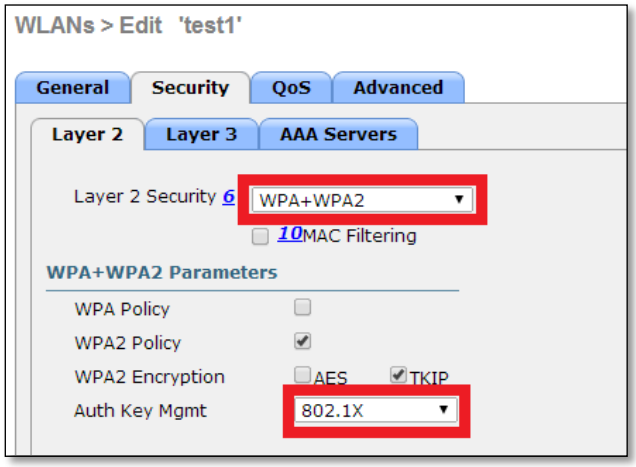
   c. Set the EAP method in file "EAP.conf".

```
    #
    #default_eap_type = md5
    default_eap_type = peap
    #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
```

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.

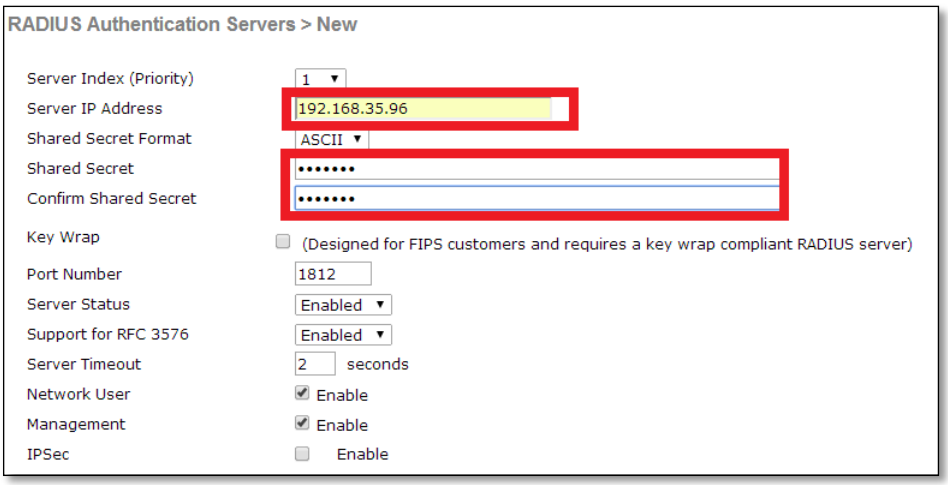
   Here we use WPA2 for Authentication and TKIP for Encryption as an example. Choose "802.1X" for Auth Key Mgmt to select an associate a RADIUS server with the wireless client.



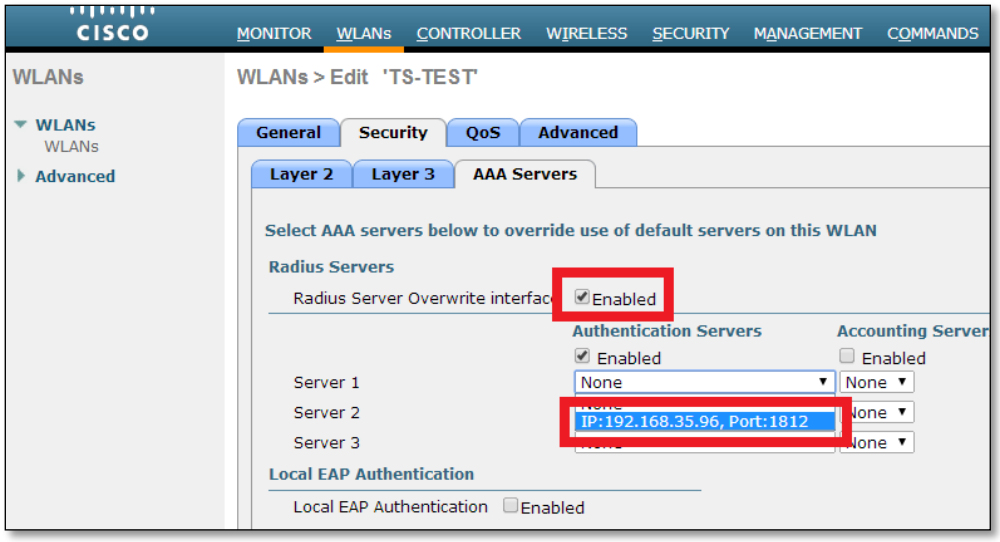
3. Add RADIUS Server in the Cisco controller.

   a. Click SECURITY > RADIUS > Authentication, and then click New…

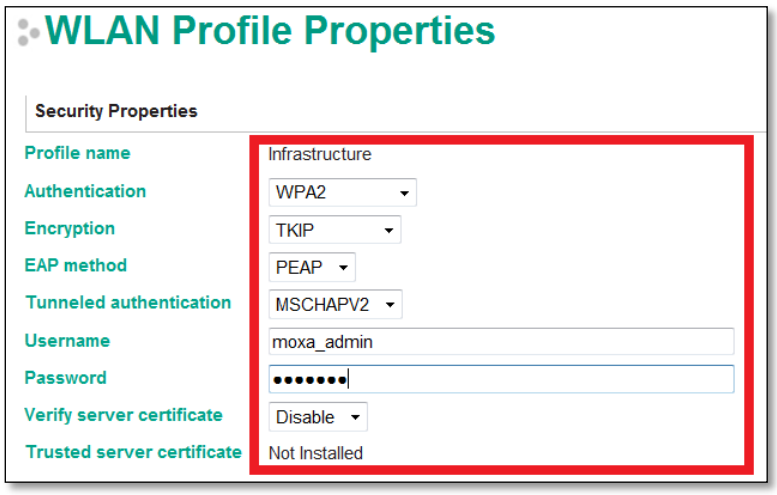
   b. Create a new RADIUS Authentication Server. Enter the RADIUS server's IP Address and RADIUS key (the same key used in step 7.4.1.b; we use 1111111 to illustrate).



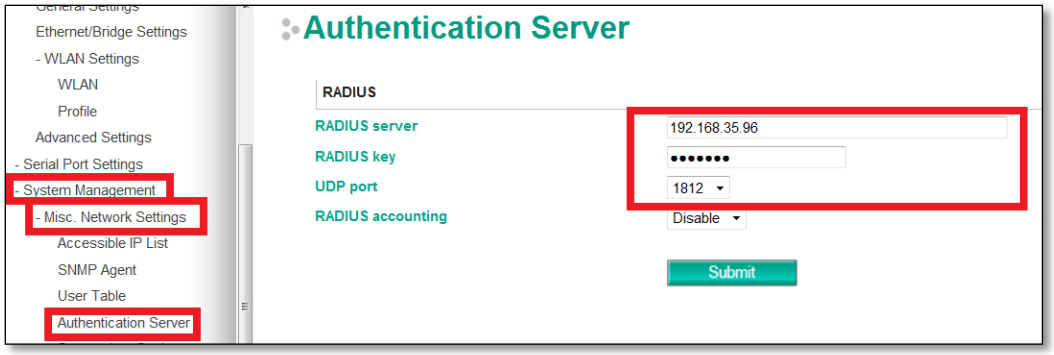
4. Go to WLANs > (WLAN ID) > Security tab > AAA Servers and select which RADIUS server should be used for this WLAN profile.



5. Enter the NPort W2x50A/W2x50A-W4'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.a for the RADIUS server).



6. We also need to add the RADIUS server to the NPort W2x50A/W2x50A-W4. 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.b), and UDP port (default = 1812).



7. Save all the settings and restart the NPort W2x50A/W2x50A-W4. Disconnect the Ethernet cable before booting up to enable the wireless connection. From the Cisco Controller, check that the NPort W2x50A/W2x50A-W4 has successfully established a connection with the Cisco AP.