Cisco Unified Access CT5760 Controllers, Catalyst 3850 Switches IOS XE Software Release 3.2.2 Web GUI Deployment Guide

Last Updated: August, 2013

351360

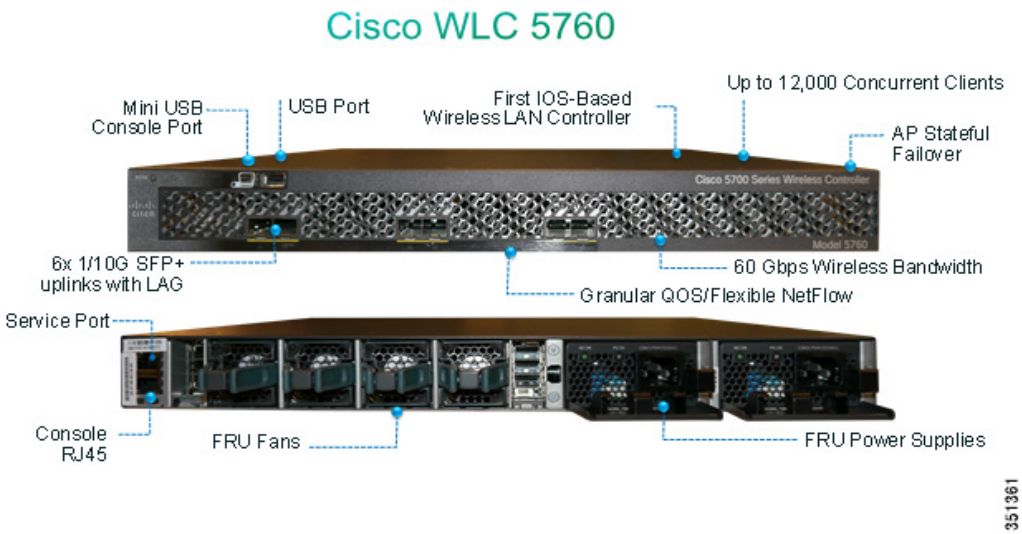
Cisco Systems, Inc.
www.cisco.com

Introduction

This document introduces the Maintenance Release 3.2.2 Web GUI functionality for the Cisco Converged Access CT5760 and Cat3850 products. This guide is designed to help you access, configure and monitor both products using the GUI Web interface.

CT5760 Controller

CT5760 is an innovative UADP ASIC based wireless controller deployed as a centralized controller in the next generation unified wireless architecture. CT5760 controllers are specifically designed to function as the Unified model central wireless controllers. They also support the newer Mobility functionality with Converged Access switches in the wireless architecture.



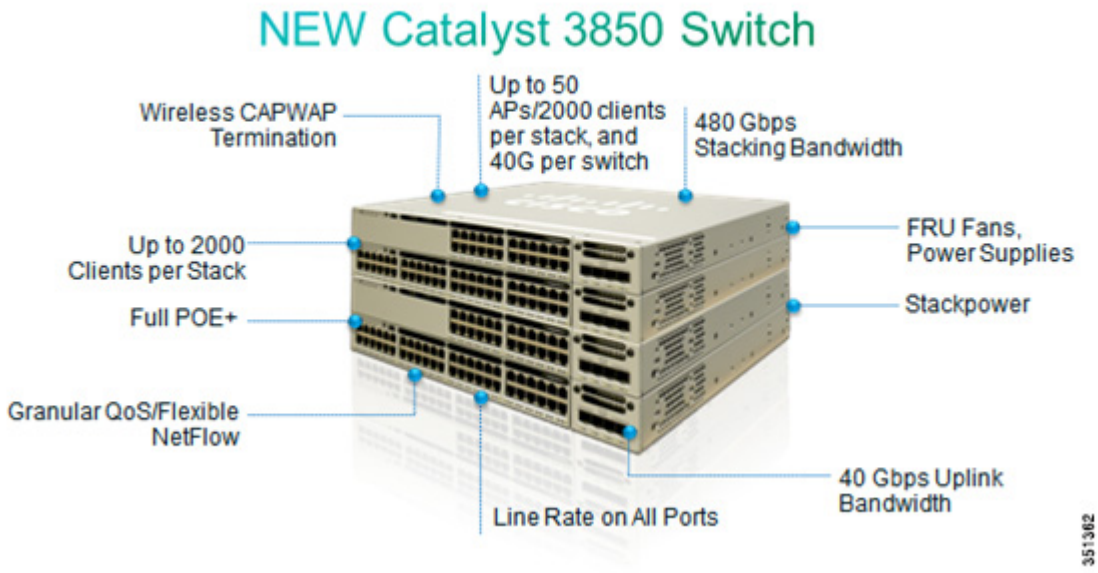
CT5760 controllers will be deployed behind a core switch/router. The core switch/router will be the only gateway into the network for the controller. The uplink ports connected to the core switch will be configured as EtherChannel trunk to ensure port redundancy.

This new controller is an extensible and high performing wireless controller, which can scale up to 1000 access points and 12000 clients. The controller has 6-10 Gbps data ports.

As a component of the Cisco Unified Wireless Network, the 5760 series works in conjunction with Cisco Aironet access points, the Cisco Prime infrastructure and the Cisco Mobility Services Engine to support business-critical wireless data, voice, and video applications.

Catalyst 3850 Controller

Unified Access Catalyst 3850 switches are innovative UADP ASIC hardware that can support multiple protocols and has many advantages over the current hardware platform. CAT3850 switch has an integrated hardware based wireless support with CAPWAP and fragmentation. The CAT3850 switch has 40gig of uplink bandwidth with all port functioning at line rate.



The CAT3850 switches provide Open Service platform. It is a 4 core CPU to leverage the OS and to host various services. The CAT3850 hardware is the Next-Gen switching hardware.

UA CAT3850 switches have unified wired and wireless architecture. The wireless operating system is IOS based. UA CAT3850 switches provide uniform wired and wireless policies. The CAT3850 switch can manage 50 access points-802.11n and support 2000 clients per stack.

Getting Started

Before you get started with enabling the WEB GUI on the Cat3850/CT5760, make sure you have the following:

1. CLI access to the box. Console Access information is shown in the CLI/Console Access section below.
2. Have one of the Supported Browser Version as listed in the section.
3. Go through Release 3.2.2 release notes located at:

http://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2_0_se/release_notes/OL28114.html#wp223882

4. Have access information such as Username/Password and networking access information.

Supported Browser Version

Below is a list of supported browser versions:

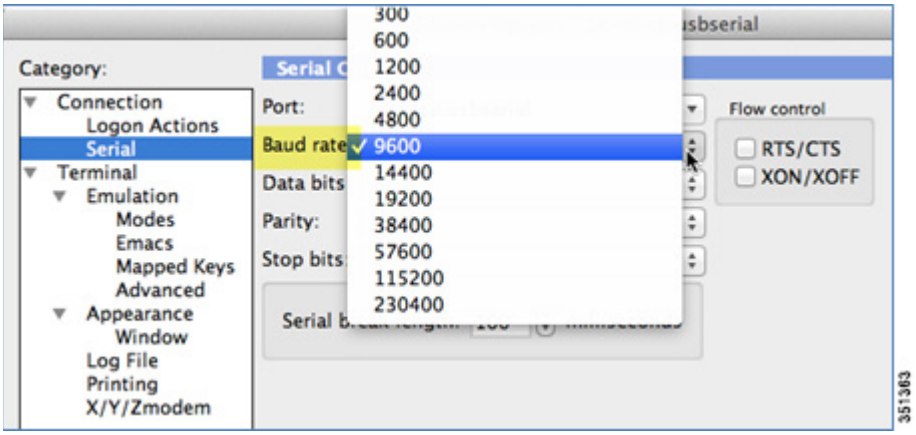
- Chrome – Ver. 26.x
- Mozilla – Ver. 20.x
- IE – Ver. 8.x, 9.x and 10.x

CLI/Console Access

Before you configure the switch or controller for basic operations, you must connect it to a PC that uses a VT-100 terminal emulator (such as HyperTerminal, ProComm, or Putty).

The controller has both EIA/TIA-232 asynchronous (RJ-45) and USB 5-pin mini Type B, 2.0 compliant serial console ports. The default parameters for the console ports are 9600 baud, eight data bits, one stop bit, and no parity. The console ports do not support hardware flow control. Choose the serial baud rate of 9600; if you have issues, try a baud rate of 115200. The figure below shows an example of a Mac Secure CRT; use similar configuration for PC/Windows Putty, and so on.

Figure 1 Mac Secure CRT Example



Enabling WEB GUI on both the 5760 and 3850 Platforms

Both the Cat3850 and CT5760 currently ship with the first release labeled as 3.2.01. If you have an existing CAT3850/CT5760 and want to use GUI to configure/monitor your wireless network, please follow the steps below:

1. Console to the 3850/5760 platform. Save your current configuration and upgrade to 3.2.2 release available on cisco.com. Upgrade procedure can be found in the link below: http://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2_0_se/system_management/appendix/swiosfs.html#wp1311040

Note During the upgrade, firmware will be upgraded and therefore it will take few more additional minutes than the regular upgrade. Please do not turn off the unit during the upgrade.

2. After upgrading to 3.2.2 version, the web GUI functionality will be enabled. By default, https is enabled. You can access the web GUI through https but if you want to enable http access, you can do so by issuing the following command using IOS CLI command: `Controller(config)#ip http server`
3. Using IOS CLI, you will need to create a username and password to access the GUI. You can configure a local username by issuing the following command: `Controller(config)#username admin privilege 15 password Cisco123.` Or you can configure it to use credentials using an authentication server. Make sure the user has privilege 15 access level.

4. In order to access the GUI, you can configure the out of band management port (GigE 0/0) or use existing reachable configured interfaces through the network.
5. Now you will be able to access the Web GUI interface. Open a browser and type your controller/switch IP address. Example: https://10.10.10.5/ . Please refer to the configuration examples below for additional Web GUI access information.

Note If you have an out of the box or brand new 5760 or 3850, please console to the box and go through the Startup Wizard as outline in the deployment guide located at: http://www.cisco.com/en/US/docs/wireless/technology/5760_deploy/Supported_Features.html

Configuration Examples

If you require additional information regarding any of the field while going through the deployment guide, please refer to the GUI online Help available after you have successfully accessed the GUI through the steps below.

GUI access for CT5760/3850 Example

Complete these steps:

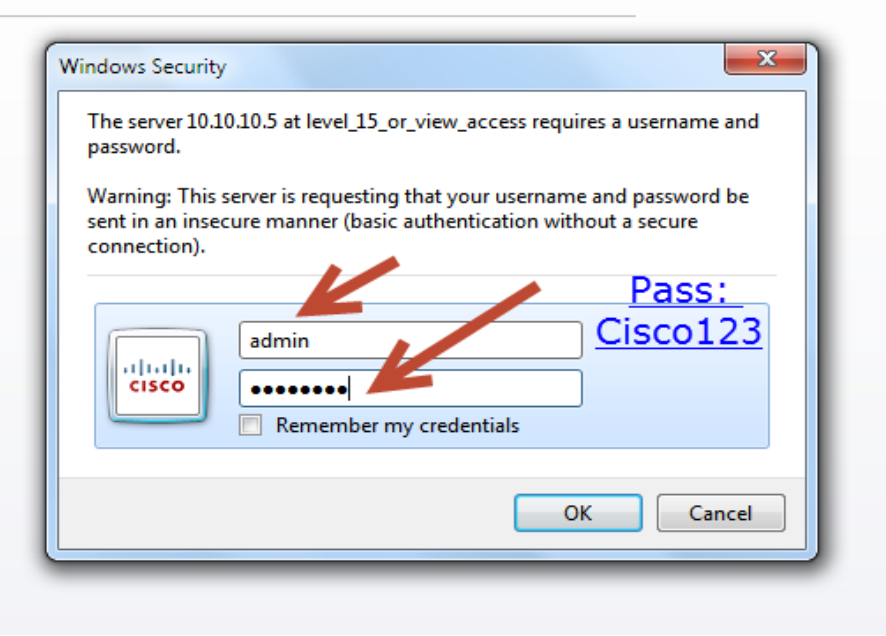
Step 1 For GUI access, open a browser and type your controller IP address. By default https is enabled, for example:

https://10.10.10.5

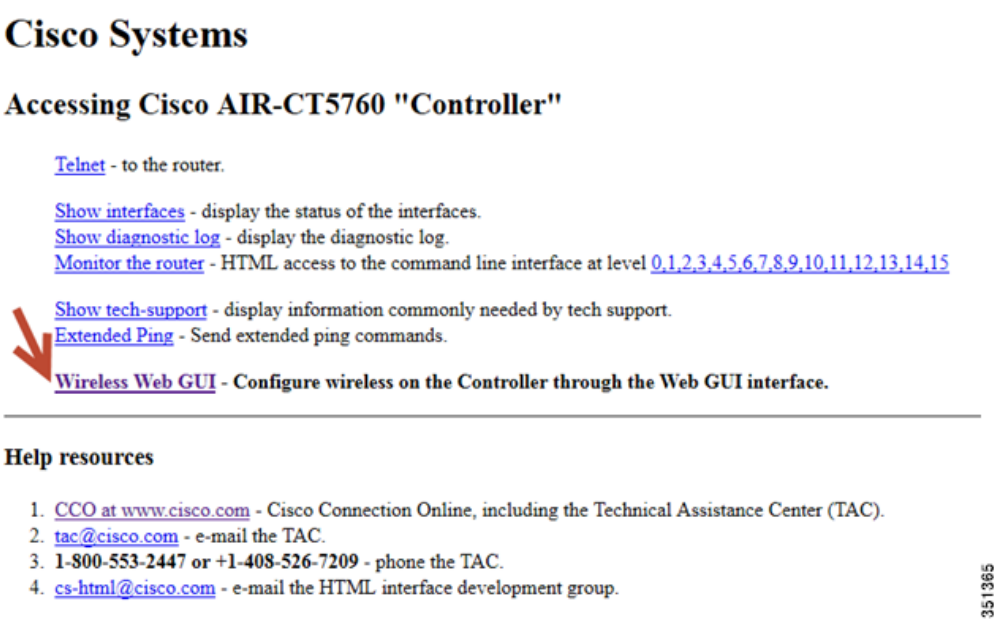
```
username: admin

Password: Cisco123
```

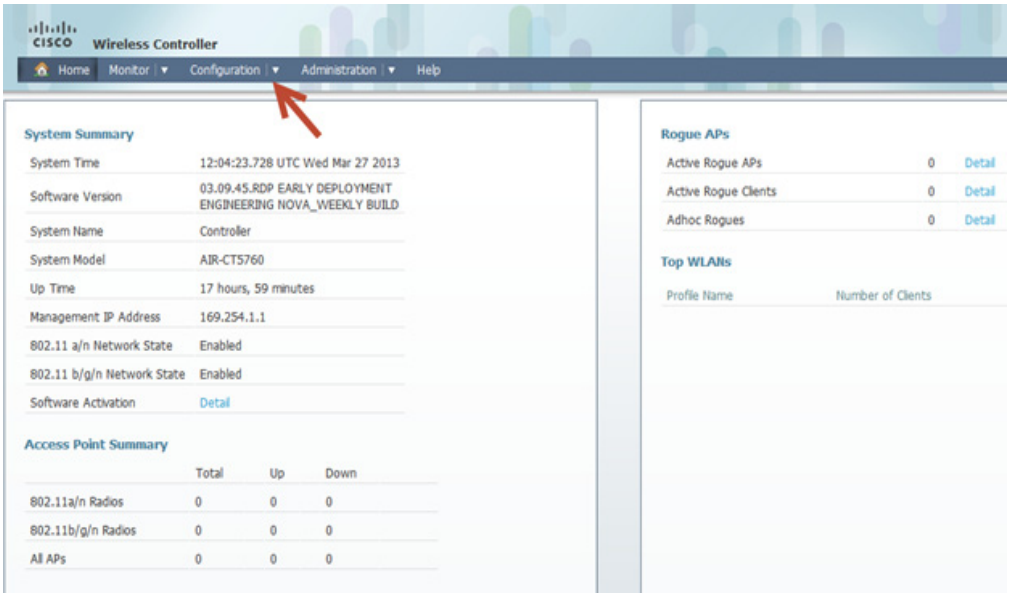
Note You can setup username/password using the following CLI command: `Controller(config)#username admin privilege 15 password Cisco123`. This is an example and not the default username and password.



Once you login, you will be directed to the following page:



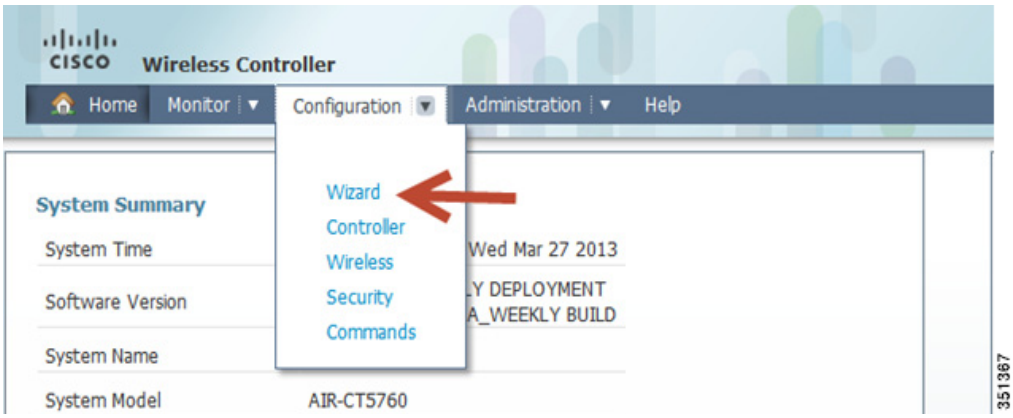
Step 2 Click **Wireless WEB GUI**, this will direct you to the home page shown below:



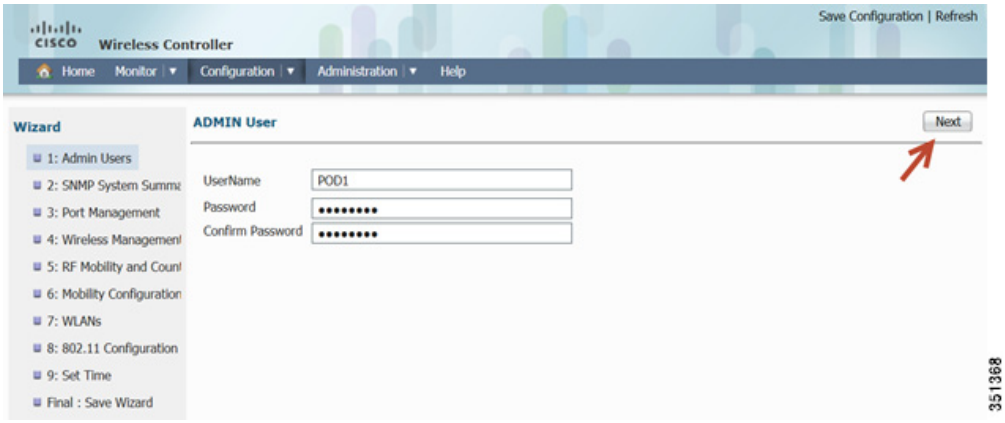
Basic Configuration for the CT5760/3850 Example

In this section you will perform basic controller and management configuration using the GUI Wizard of the CT5760 or CAT 3850.

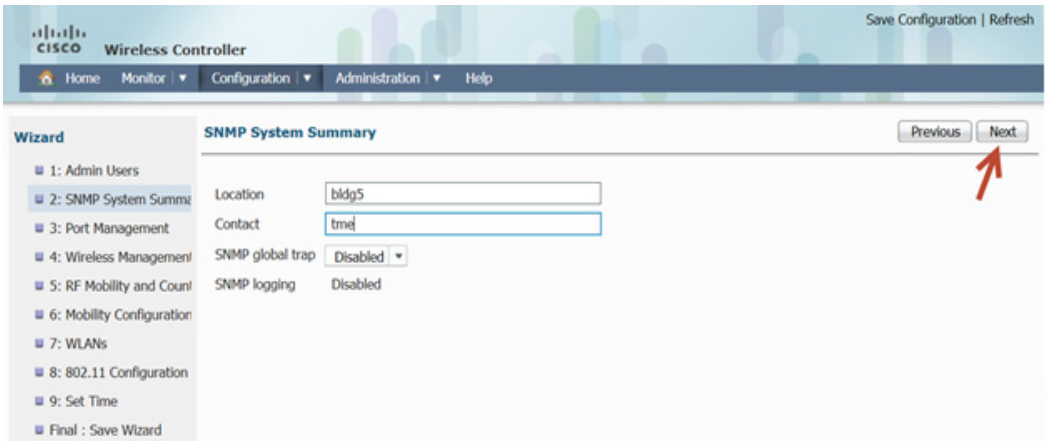
Step 3 Under the Configuration tab, choose the option **Wizard**.



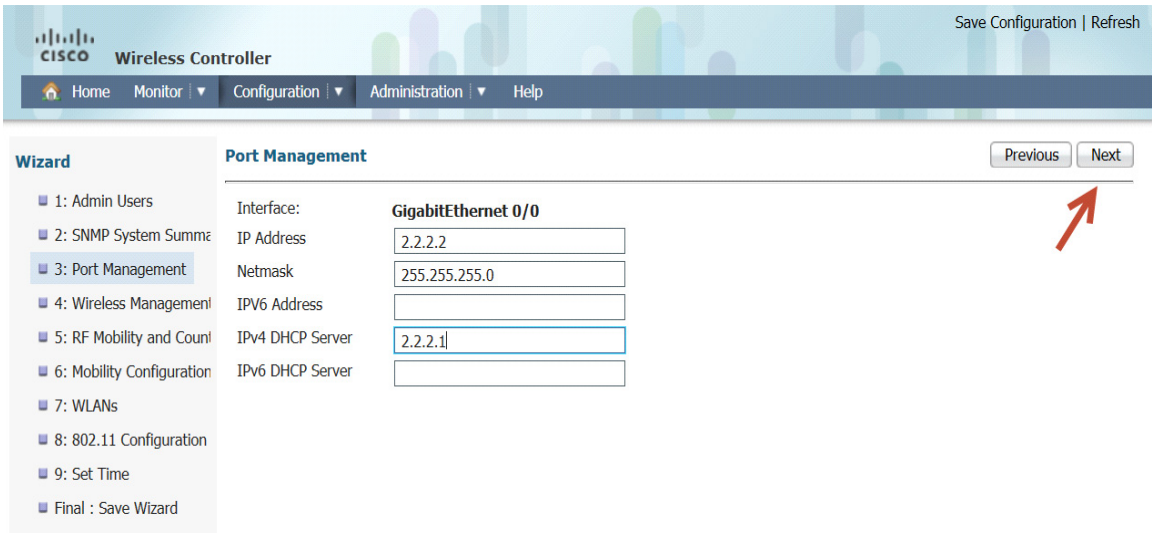
Step 4 Configure Admin username and password.



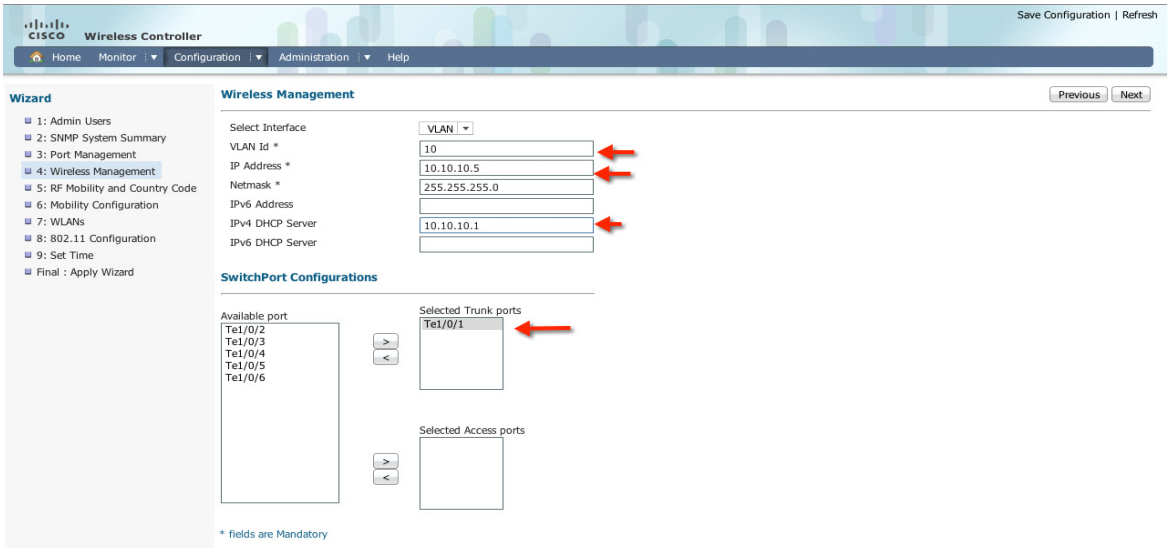
Step 5 Configure SNMP information–SNMP trap can be configured in this section, give a **Location** and **Contact** and proceed to the next step.



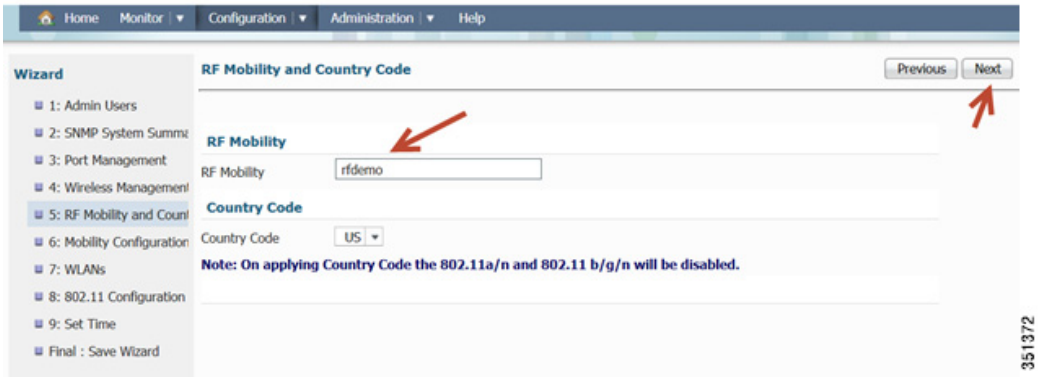
Step 6 Management Interface Configuration–You can use the out of band Management Port to access the controller. Please enter the **IP address/Netmask** and proceed to the next screen for Wireless management configuration.



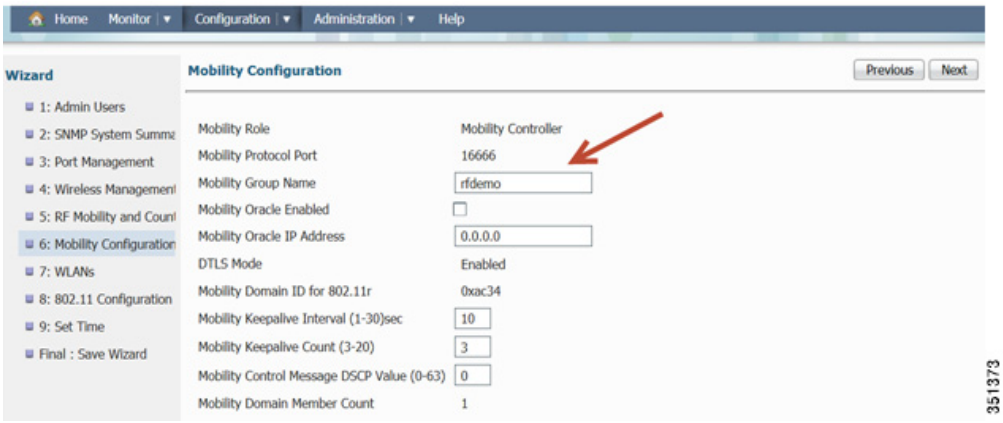
Step 7 Wireless Management Configuration–This is where you can configure Wireless Management interface on the 5760 and assign it for a specific VLAN. Please assign VLAN IP and default gateway.



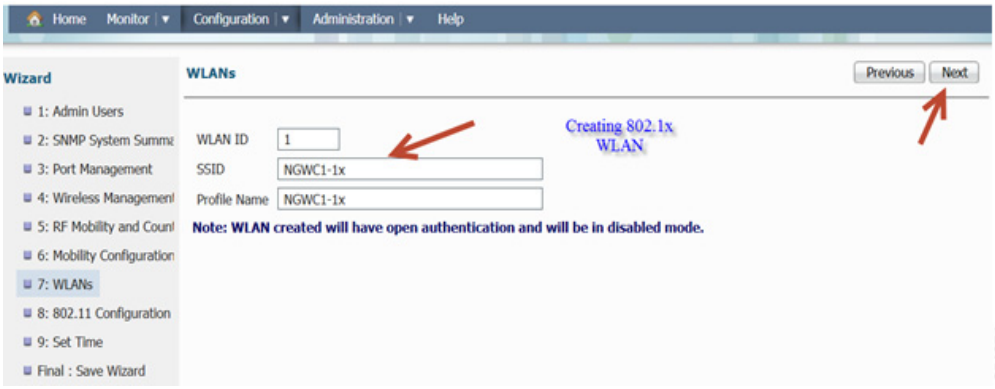
Step 8 RF Mobility and Country Code settings–This is where you can enter RF Mobility config and select a country code. As an example, enter **rfdemo** as the RF mobility name and choose **US** for Country Code.



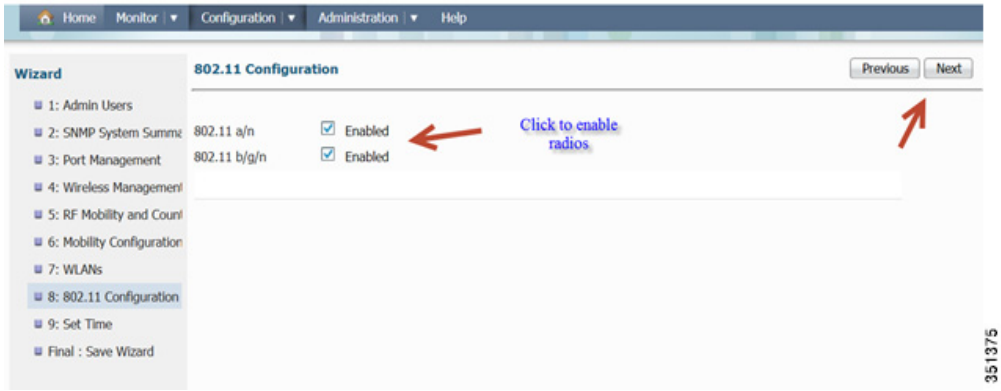
Step 9 Mobility Configuration–Here you can change the Mobility Group Name and other Mobility timers. Please click Next and move to the next screen.



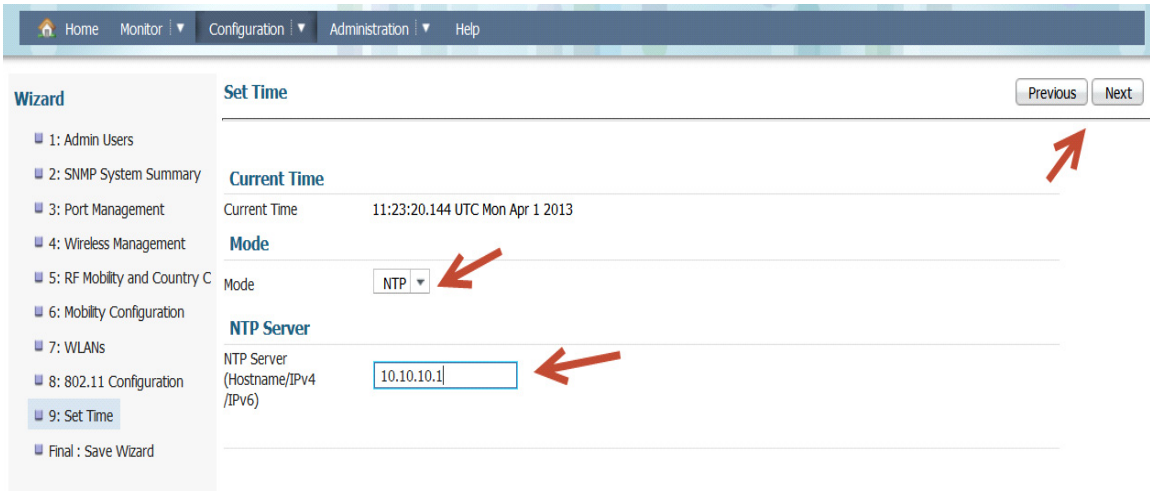
Step 10 Creating a WLAN–You will be able to create a WLAN in this screen. It will be disabled by default. Create an 802.1x WLAN name. In this example, we will use (NGWC1-1x).



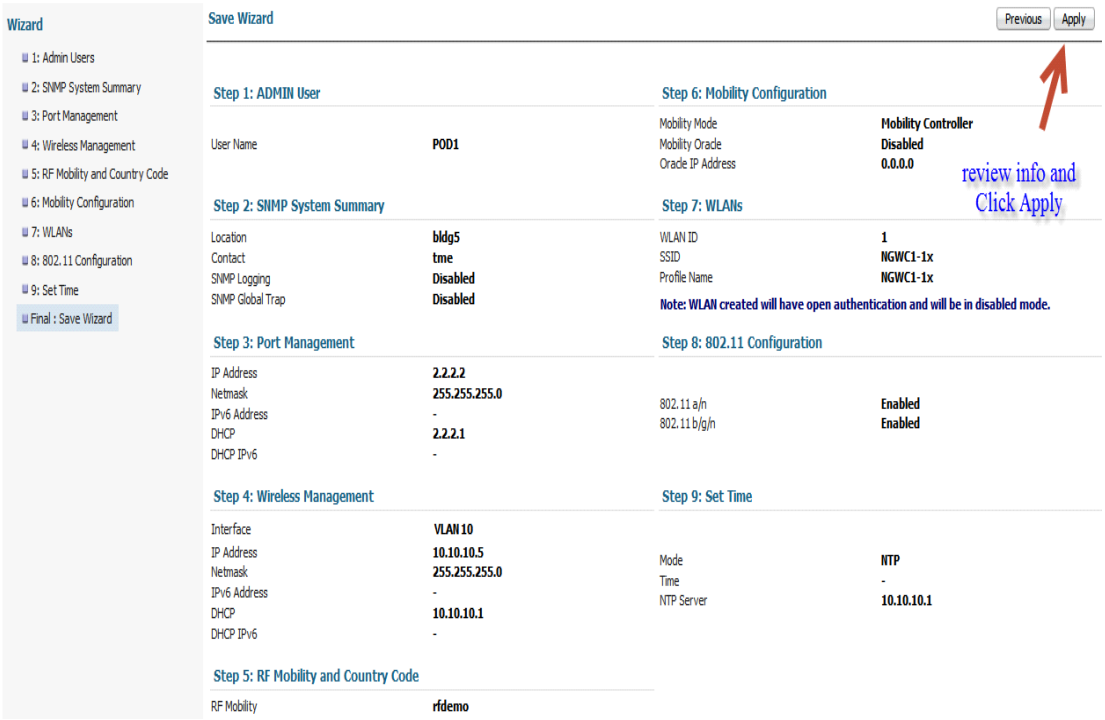
Step 11 Enabling 802.11 Radios–Radios were disabled once we changed the country code in earlier steps. Click on the radio button to Enable the 802.11a/n and 802.11 b/g/n



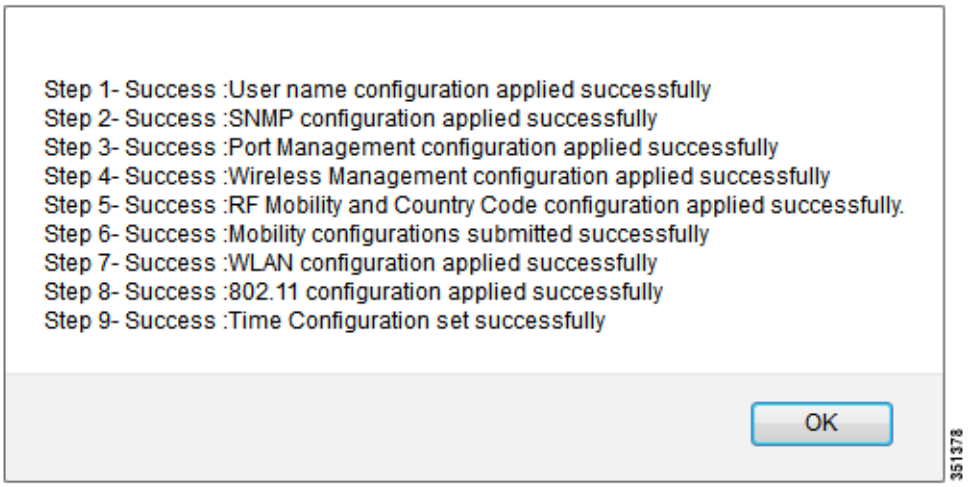
Step 12 Time Settings–You can choose between two modes: Manual and NTP. In this example: we are choosing NTP and using 10.10.10.1 as the NTP Server IP Address.



Step 13 Saving and Applying Wizard



Step 14 Confirmation Message–After pressing apply, please wait few seconds until the configurations have been applied. You should see the success message below. Click **OK** and this should conclude the initial Wizard configuration.

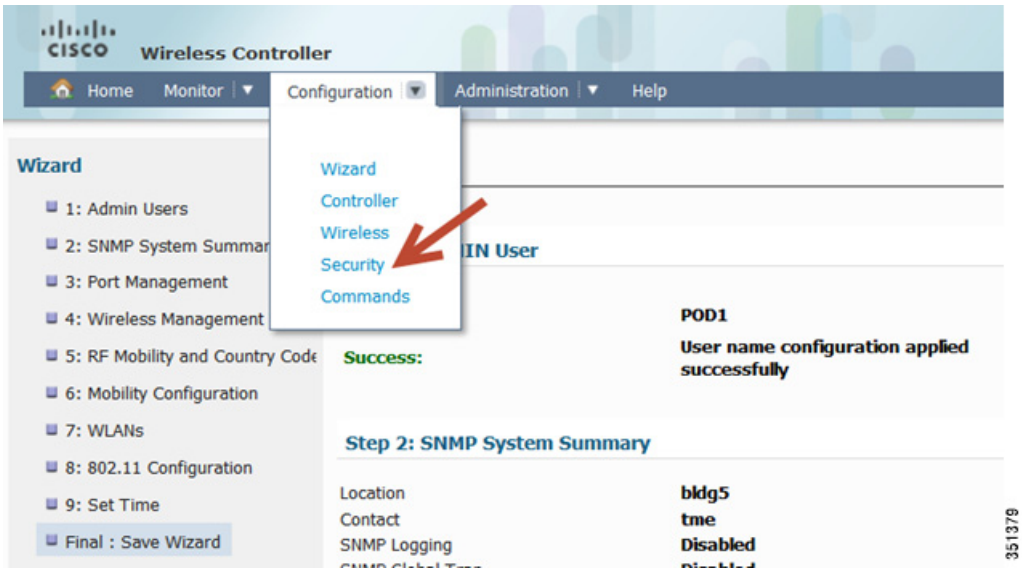


Note This concludes the Initial Wizard setup. Next section describes the AAA configuration.

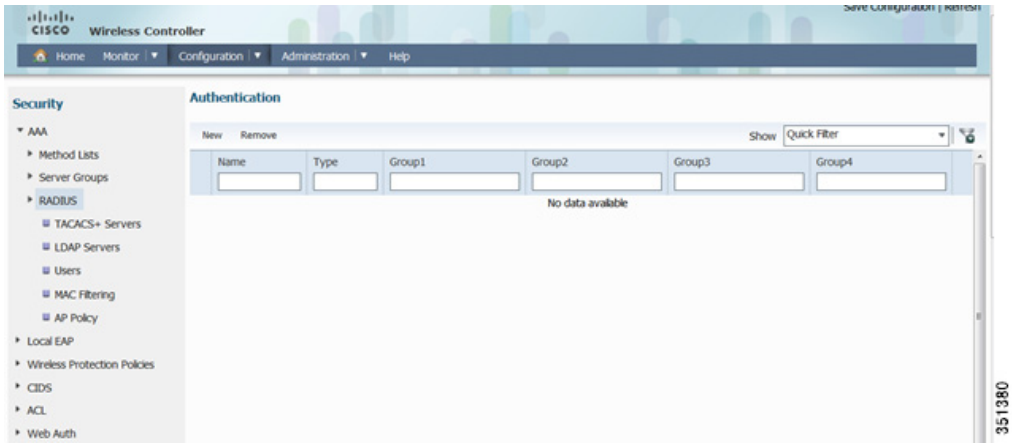
AAA Configuration for 802.1x WLAN Example

In this section you will setup AAA configuration.

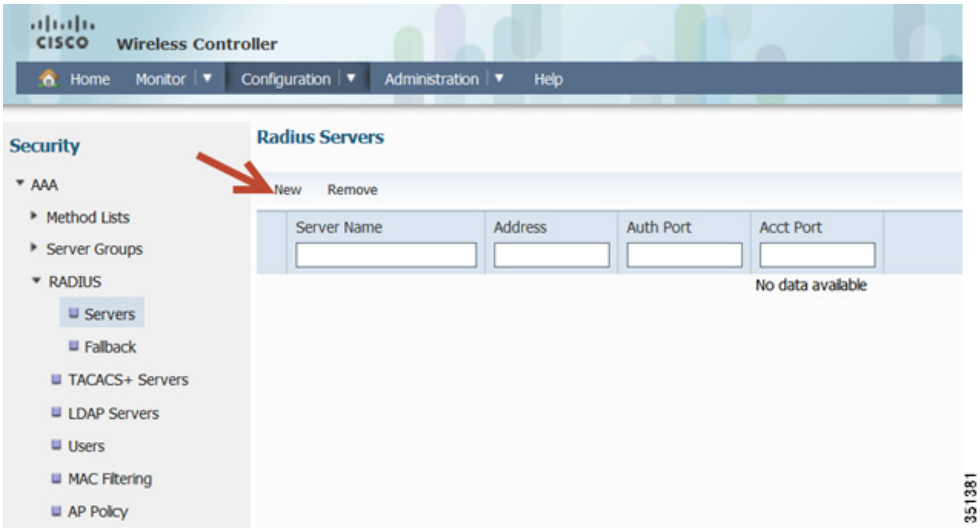
Step 15 Configuring AAA settings for 802.1x WLAN–Under Configuration tab, choose **Security**.



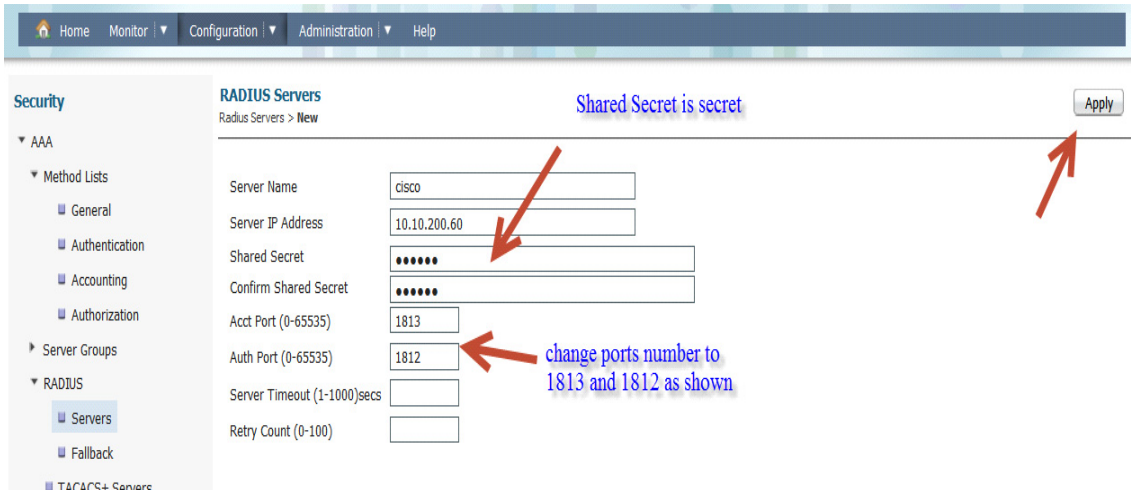
This will take you to the AAA configuration page:



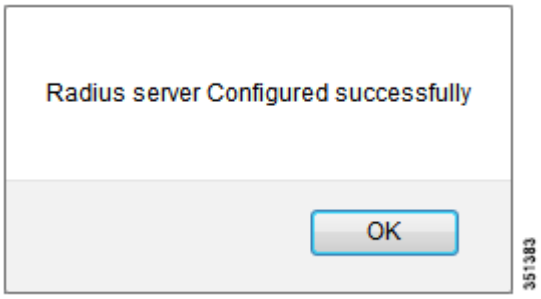
Step 16 Radius Server Configuration–Expand Radius Tab and Click **New**



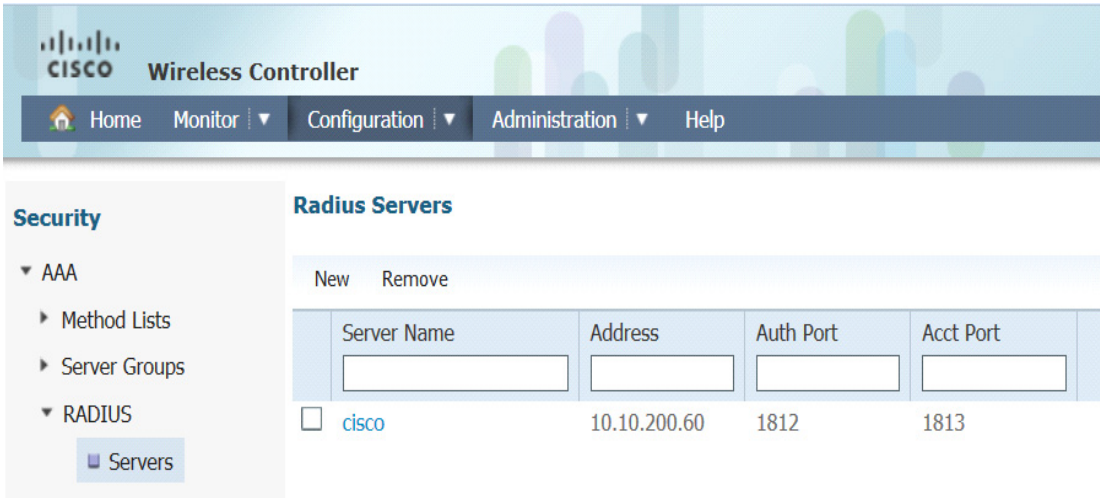
Please enter the ISE/Radius server information as shown below. Once done, Click Apply.



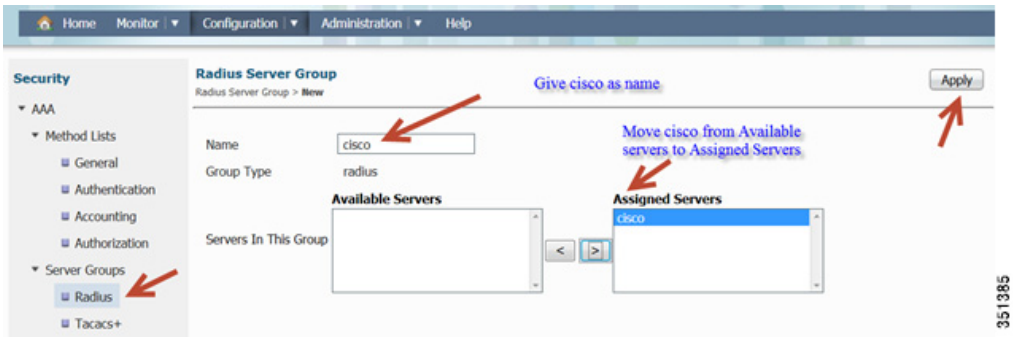
Confirmation message:



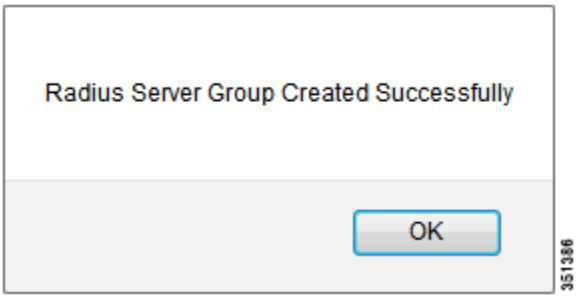
Click **Ok** and you should see the following window.



Step 17 Server Group Creation–Go to **Server Group > Radius > New**

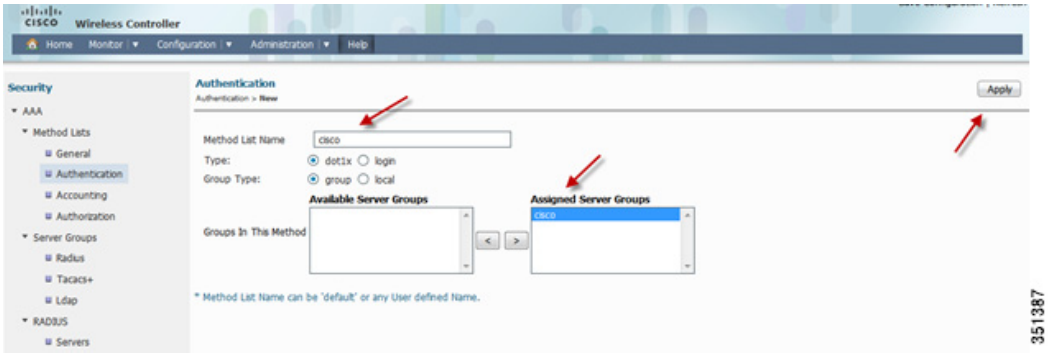


Once you click **Apply**, a confirmation pop-up appears:

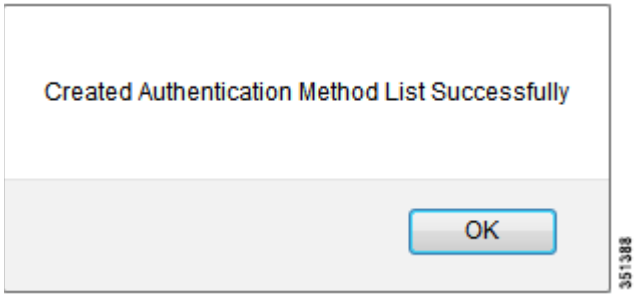


Click **Ok** and confirm the server group cisco is created.

Step 18 Creating AAA Method Lists for Authentication/Accounting/Authorization–Go to **AAA > Method Lists > Authentication > New**



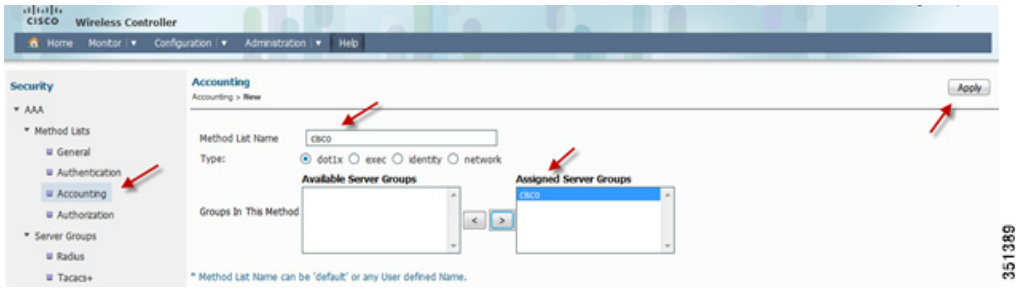
Once you click **Apply**, a confirmation pop-up appears:

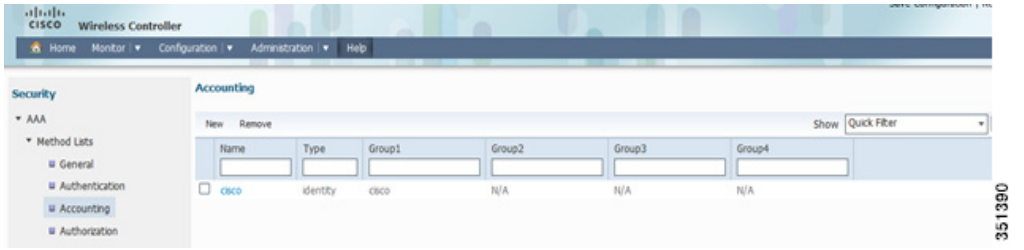


Click **Ok** and confirm the server group cisco is created.

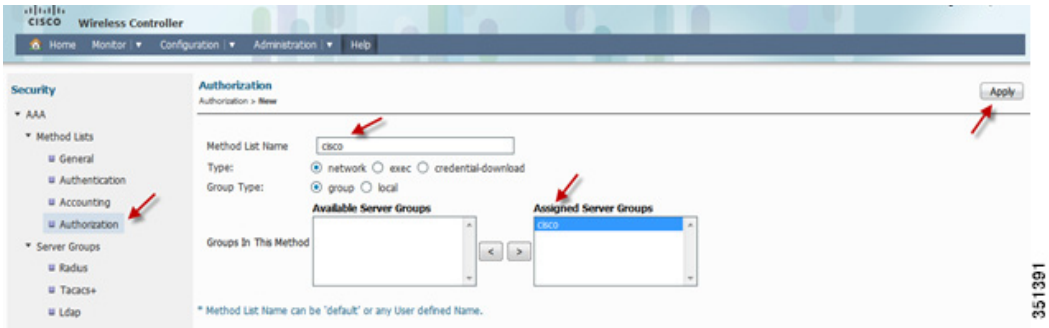
Repeat the same Step for Accounting and Authorization:

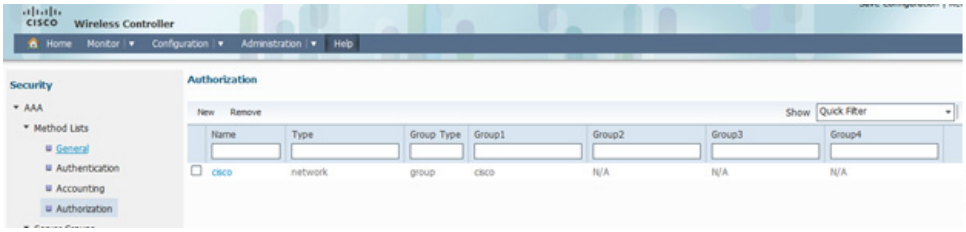
Accounting



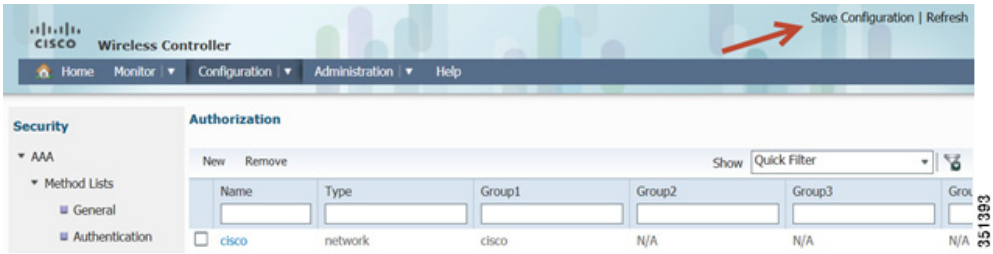


Authorization





This will conclude Radius and AAA configuration. Next section is WLAN settings. Before moving on, please Save your configuration by clicking on **Save Configuration** in the upper right hand side of the GUI.

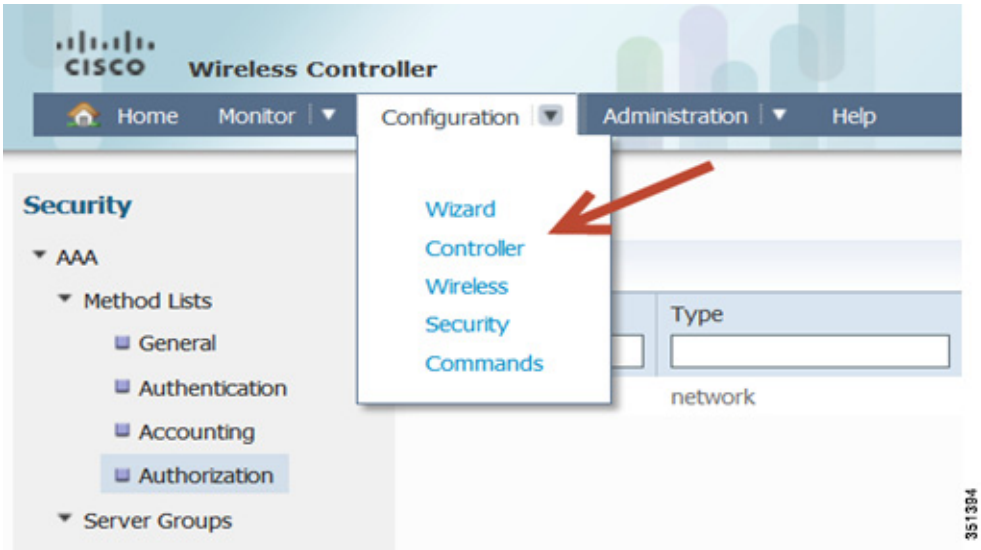


801.1x WLAN Configuration Example

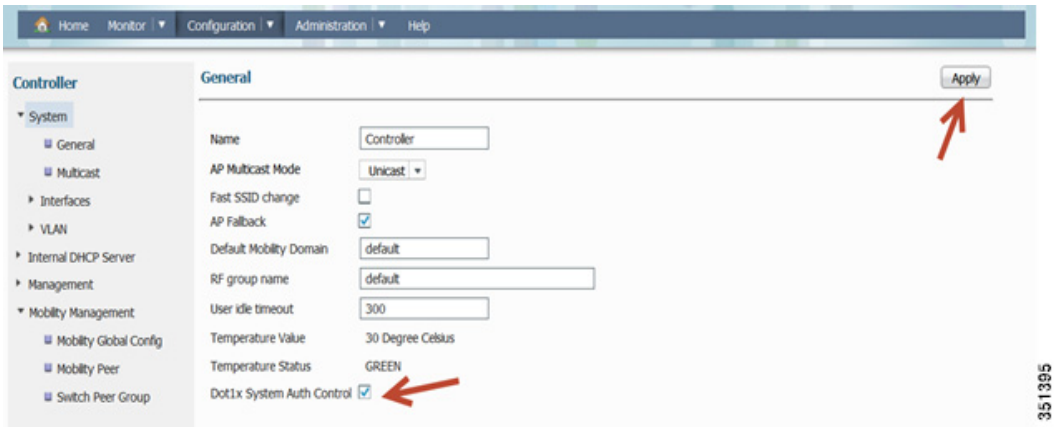
In this section you will perform 802.1x WLAN configuration using ISE as a radius server

Step 19 Enabling 802.1x on the entire system.

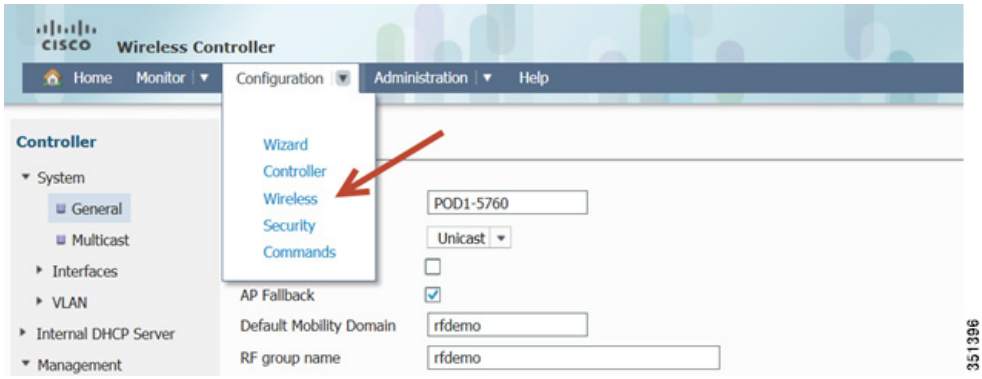
Under Configuration tab, navigate to **Controller > System > General**



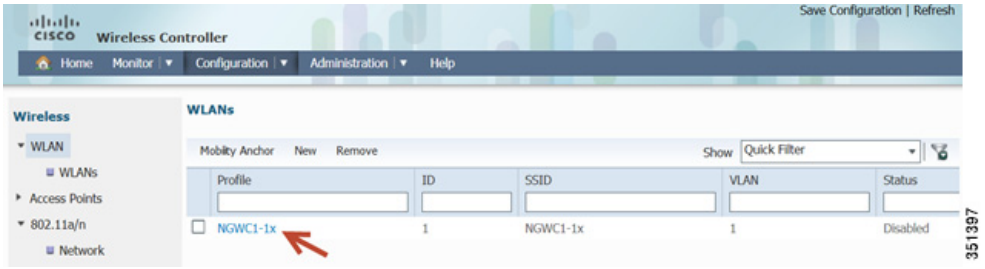
Enable **Dot1x System Auth Control** and click **Apply**. Once you get a confirmation message, move to the next step.



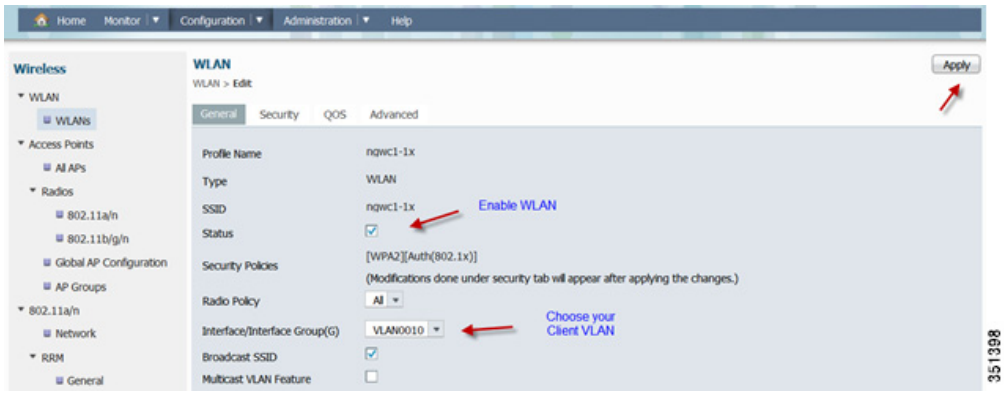
Step 20 Edit WLAN Configuration and Assigning VLAN–Under Configuration tab, choose **Wireless**



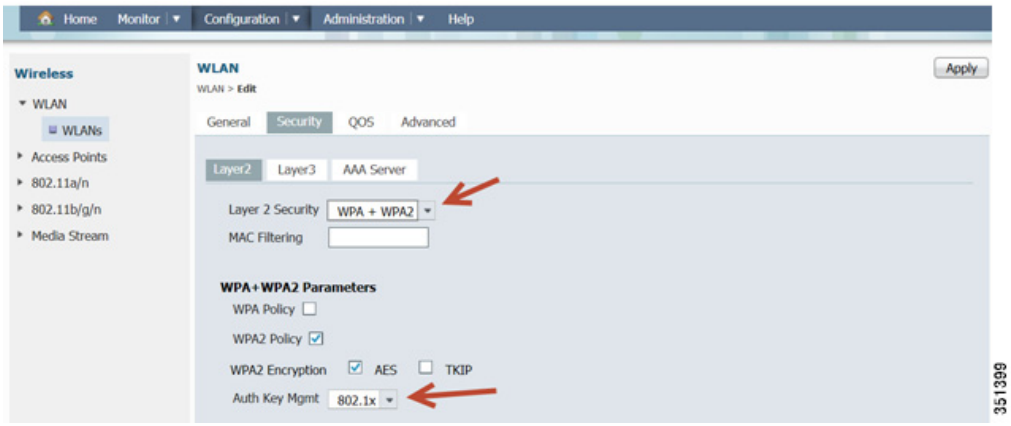
Navigate to **Wireless > WLAN**, you should see the WLAN summary page:



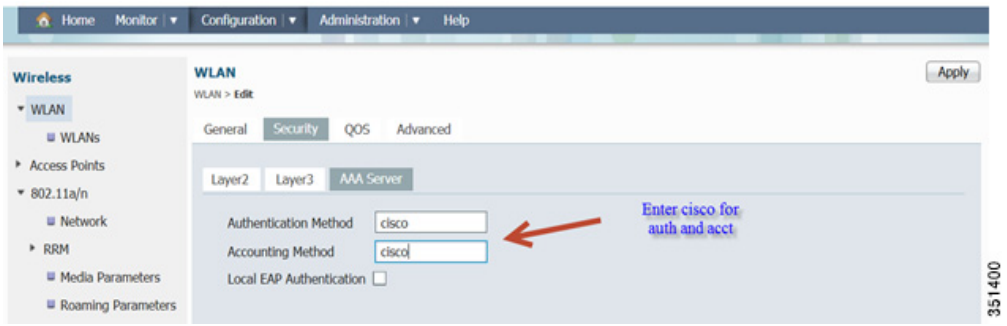
Select WLAN NGWC1-1x and then you will be able to edit its settings.



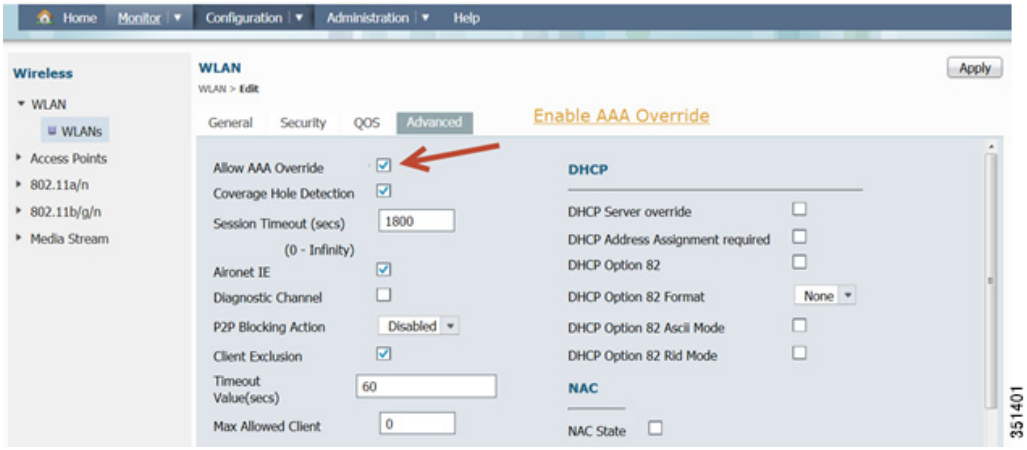
Step 21 Apply Security Settings–Under **Security** tab, **Layer 2**. Make sure WPA+WPA2 is selected as **Layer 2 Security** and 802.1x is selected as an **Auth Key Mgmt**



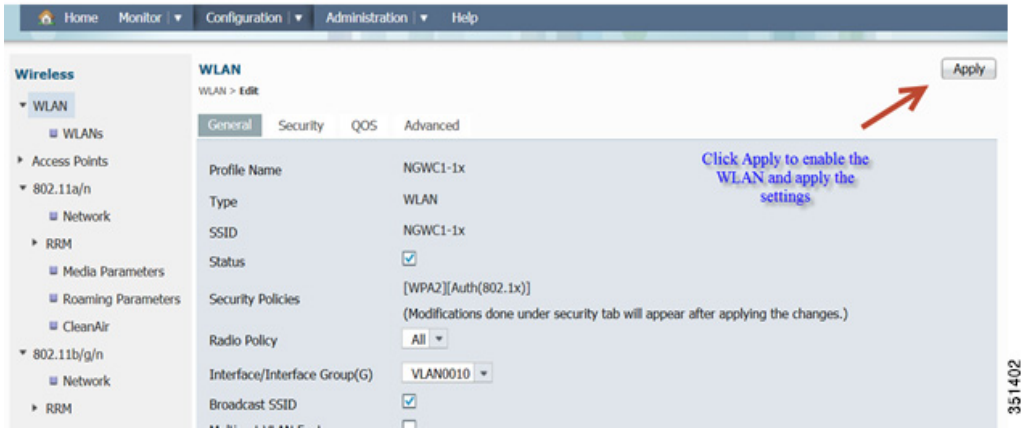
Under **WLAN > Security > AAA Server**, type cisco as the Authentication and Accounting Methods that we have created earlier under AAA.



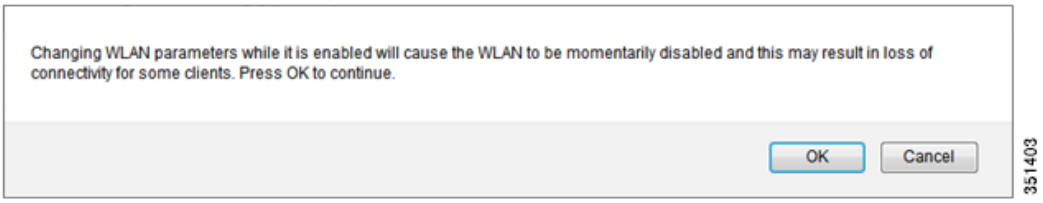
Under **WLAN > Advanced**, Enable **Allow AAA Override**



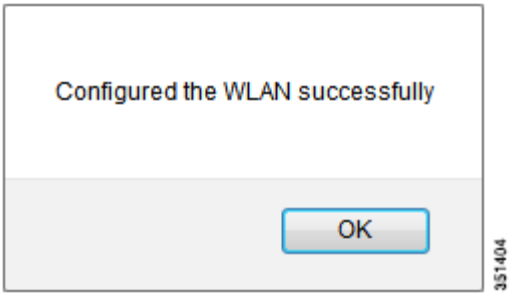
Now Click **Apply** to enable the WLAN and its settings.



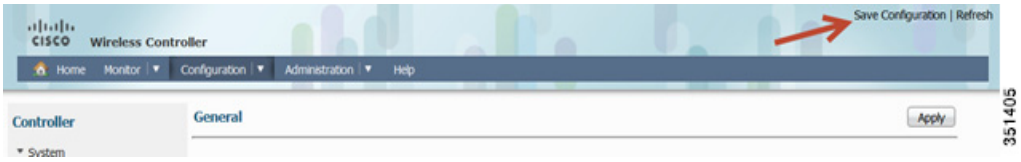
Once you click **Apply**, you will be prompted with the message below. Click **Ok**.



Confirmation message appears. Click **Ok.**



Step 22 Saving Config–Once client verification is done, please save the configuration by selecting **Save Configuration** in the upper right hand side of the screen.

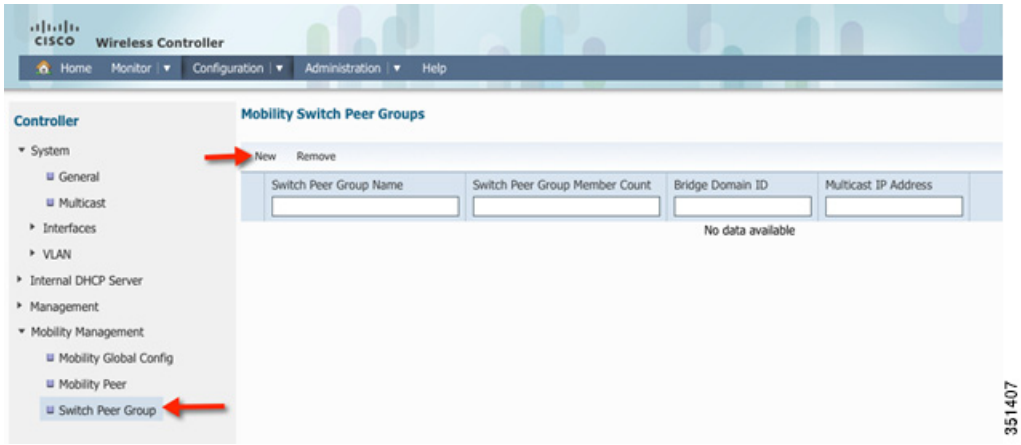


Creating a Switch Peer Group (SPG) on Mobility Controller 5760 Example

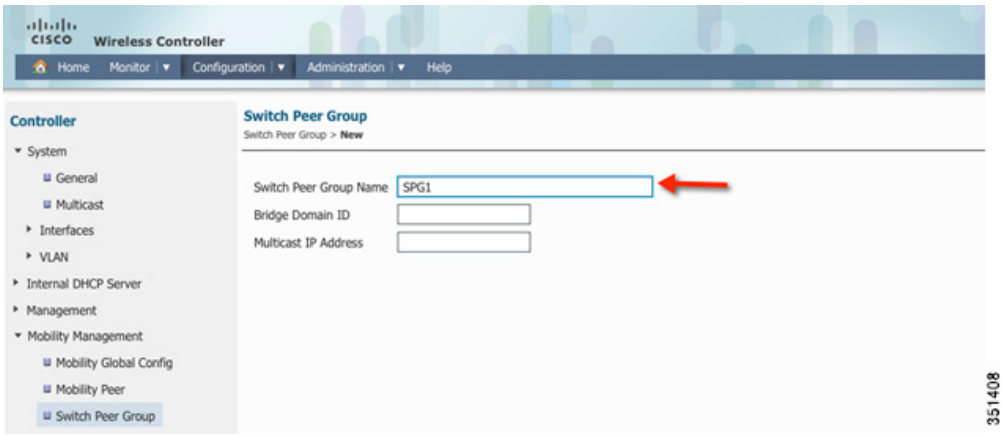
In this section, you will be able to configure Switch Peer Group(SPG) and add members (Mobility Agent) to the Group on the Mobility Controller (MC).

Step 23 On the 5760 controller GUI, navigate to **Configuration > Controller > Mobility Management**

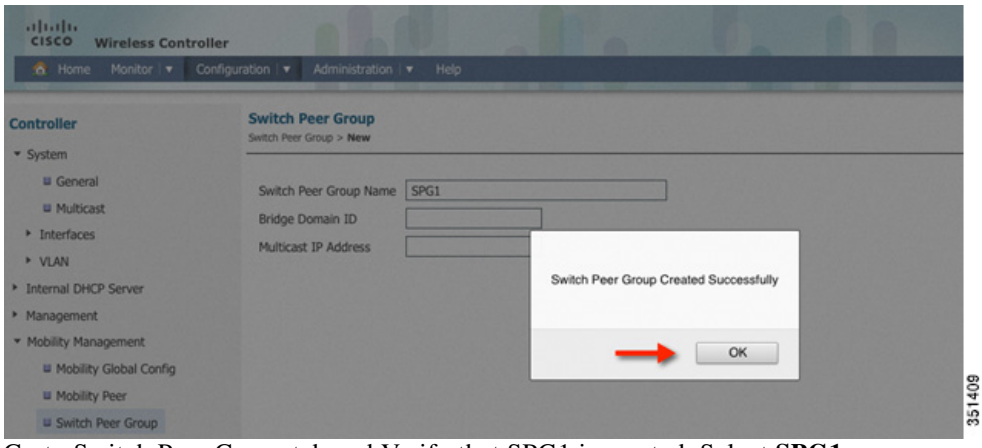
Step 24 Under Mobility Management tab, select **Switch Peer Group** tab. Click **New** and create a new Switch Peer Group (SPG1)



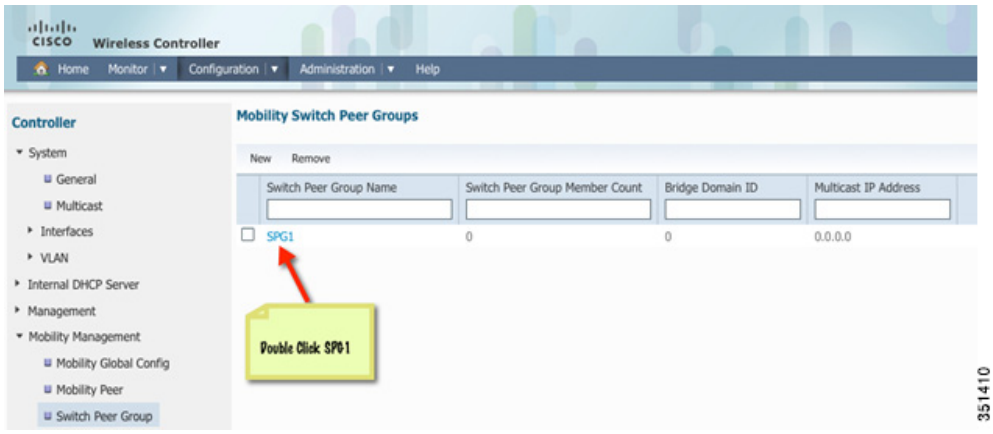
Step 25 Create new Switch Peer Group SPG1 and Click **Apply**



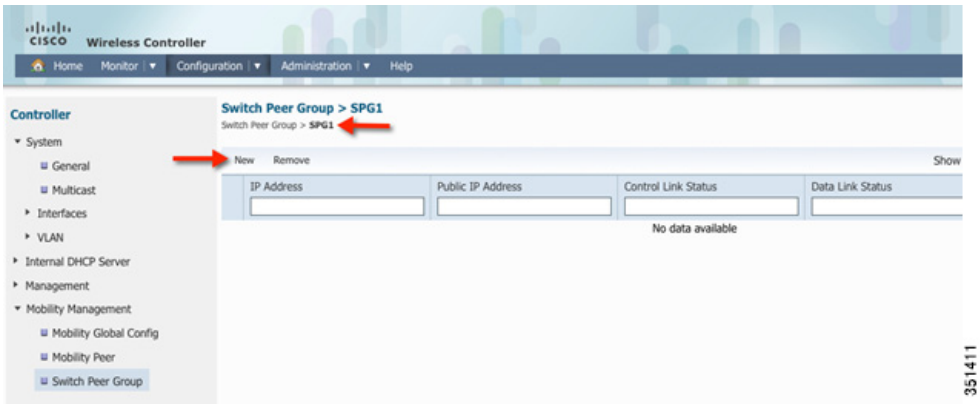
Step 26 Click **OK**



Step 27 Go to Switch Peer Group tab and Verify that SPG1 is created. Select **SPG1**

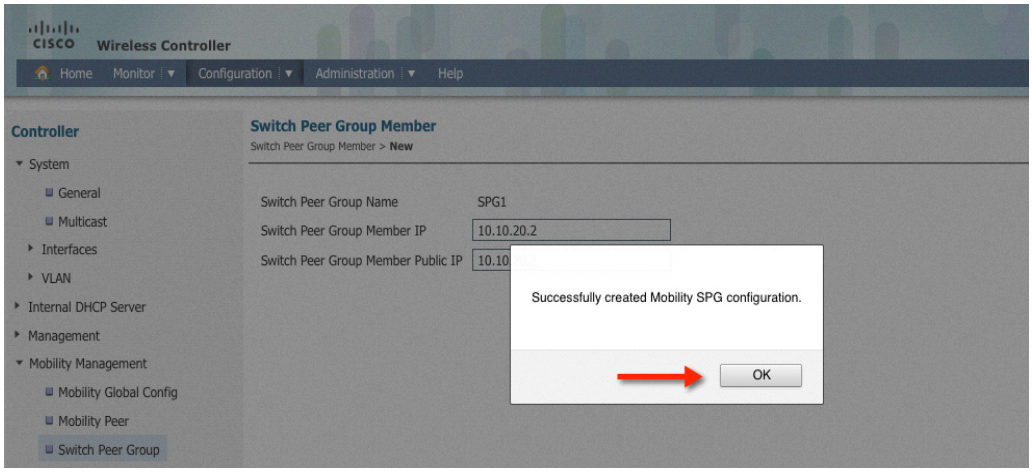


Step 28 Add member in SPG1 by clicking **new**



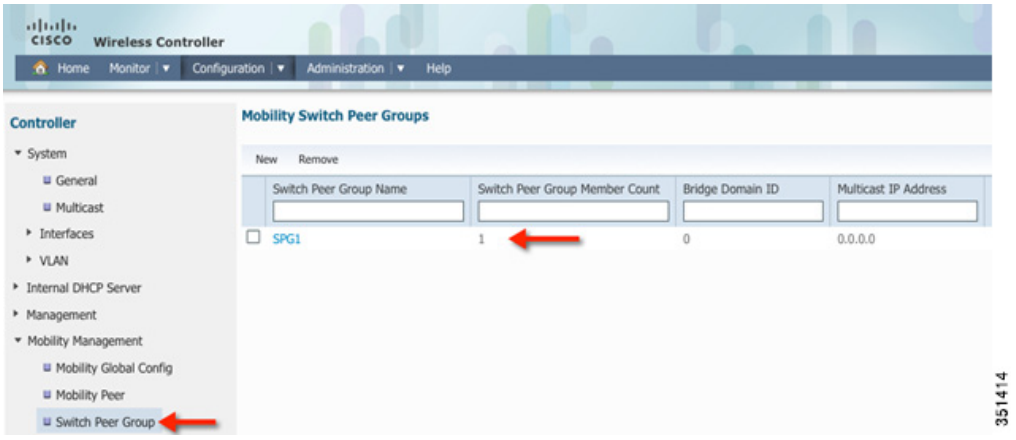
Step 29 Add public and private Mobility Agent (MA) IP address. Example = 10.10.10.2

Step 30 Click **OK**

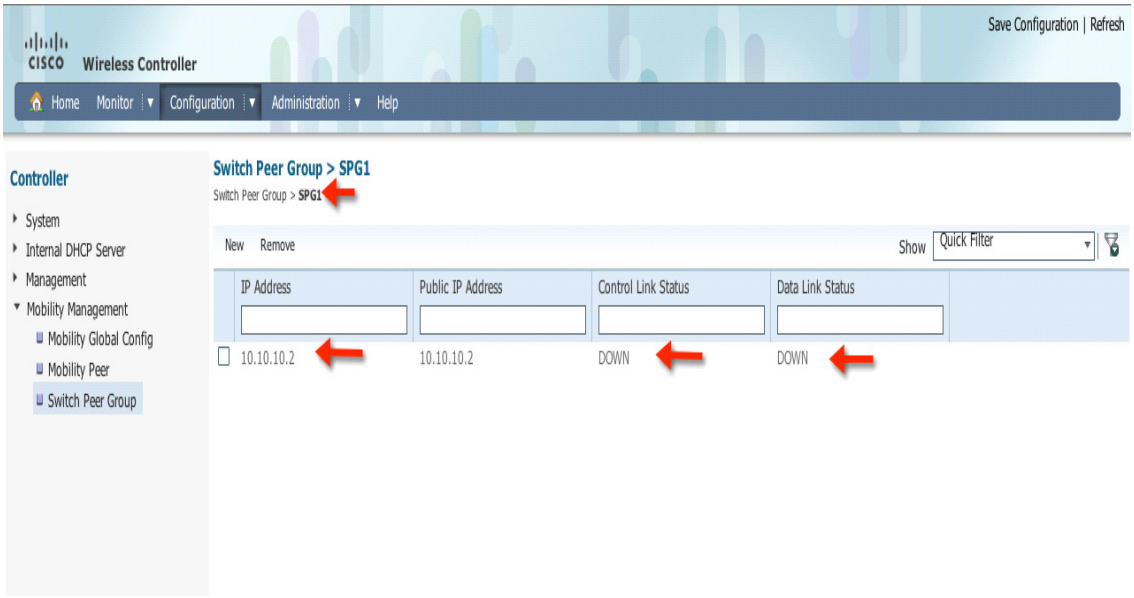


You can repeat this step to additional MA to the switch group or create a different SPG name.

Step 31 Go to **Switch Peer Group** tab and verify that Switch peer group Member Count is 1.



Step 32 Click **SPG1** and verify your MA address and control and data link status as **Down**. That's normal for now since you will be configuring the 3850 (MA) in the upcoming steps.



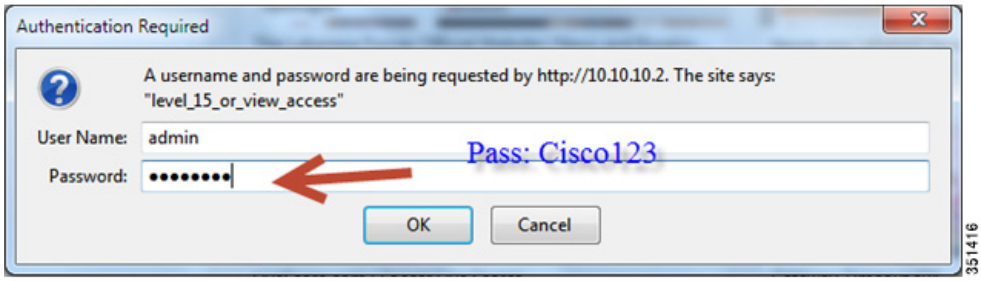
Configuring Mobility between Mobility Agent (3850) and Mobility Controller (5760) Example

Step 33 Follow the same steps outlined in the Basic Configuration for the CT5760/3850 Example to access and configure the 3850 switch. In this example, we will start with the Initial Wizard Configuration. Please note that there are differences between the 3850 and the 5760 Initial Wizard configuration.

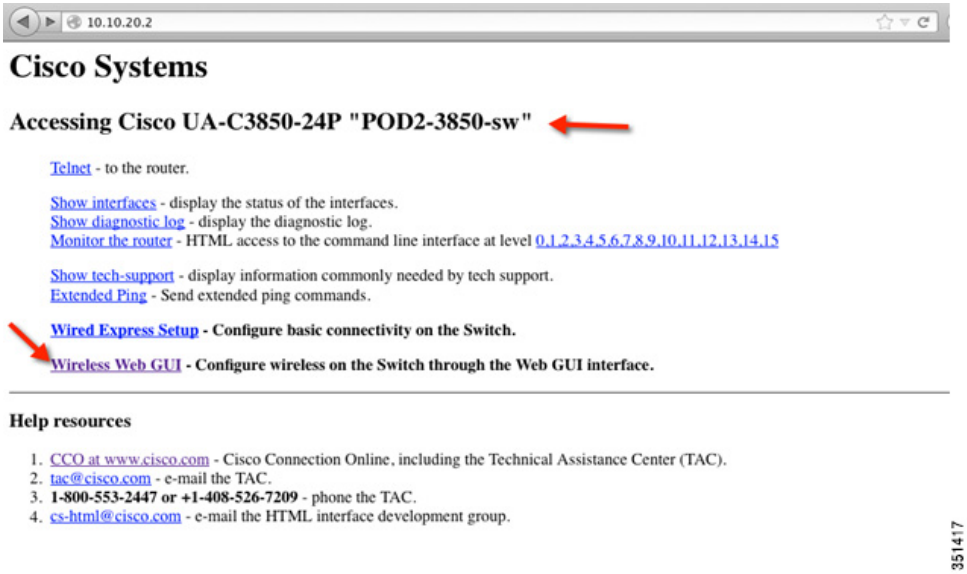
Open a browser and type your 3850 IP address. For example:

```
https://10.10.10.2
Enter username: admin
```

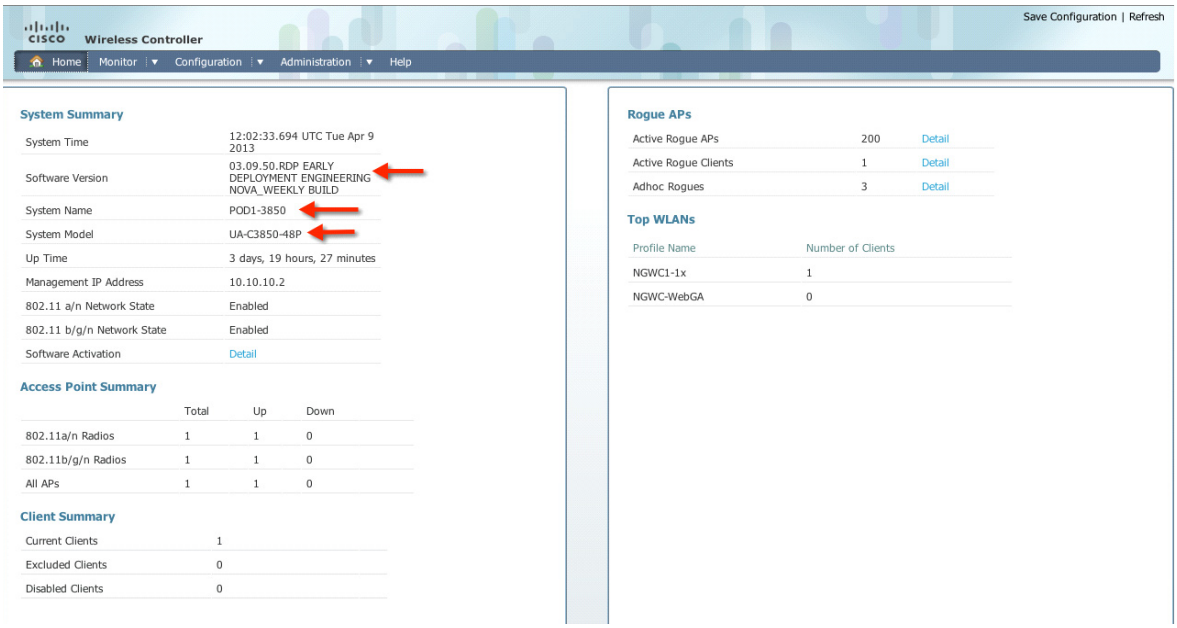
```
Password: Cisco123
```



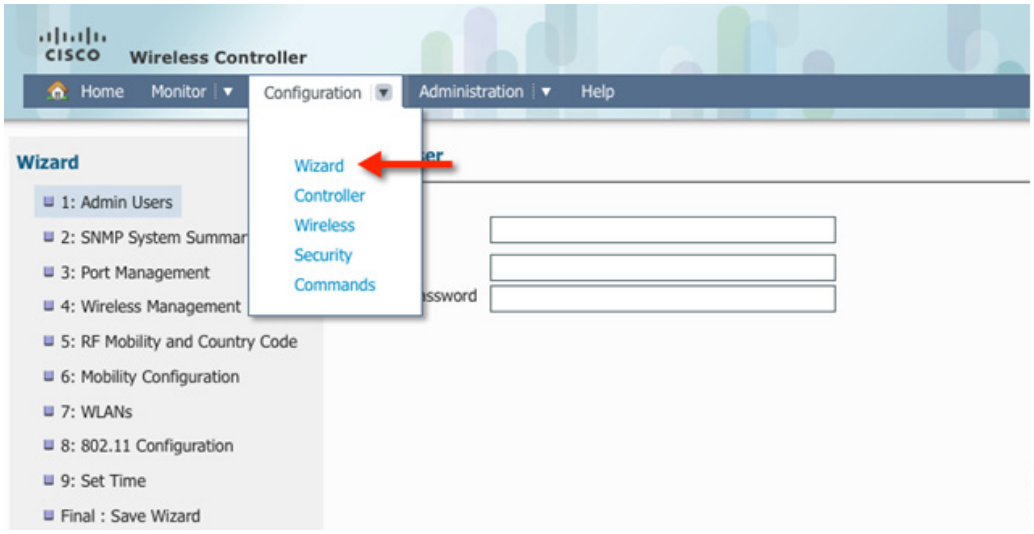
Step 34 Landing Page for MA UA-C3850-24P. Select **Wireless Web GUI**



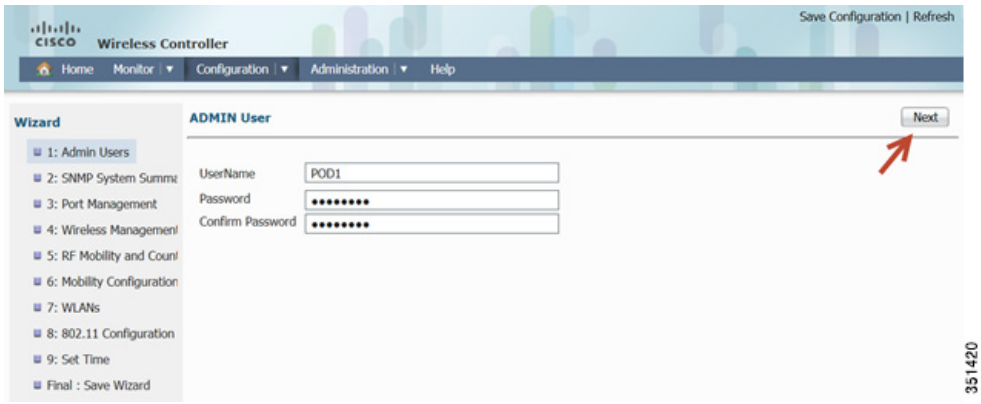
Step 35 Login to the Home page of the 3850 and verify the software version, System model and system name.



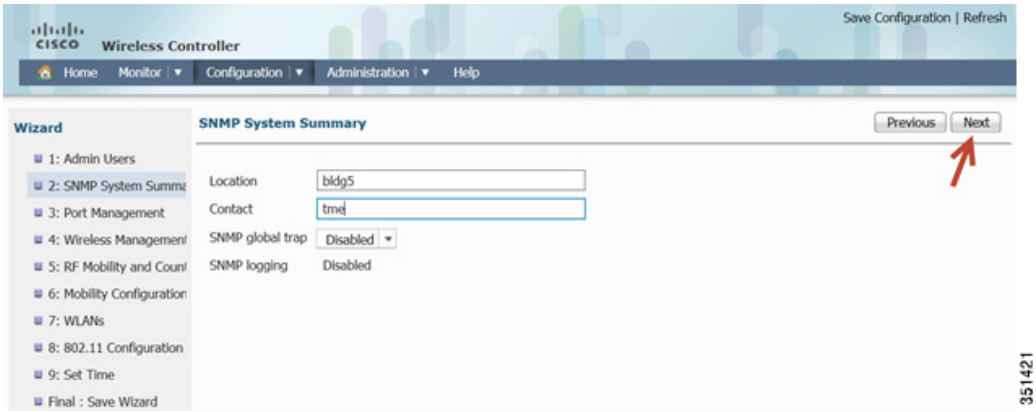
Step 36 Under Configuration Tab, choose Wizard



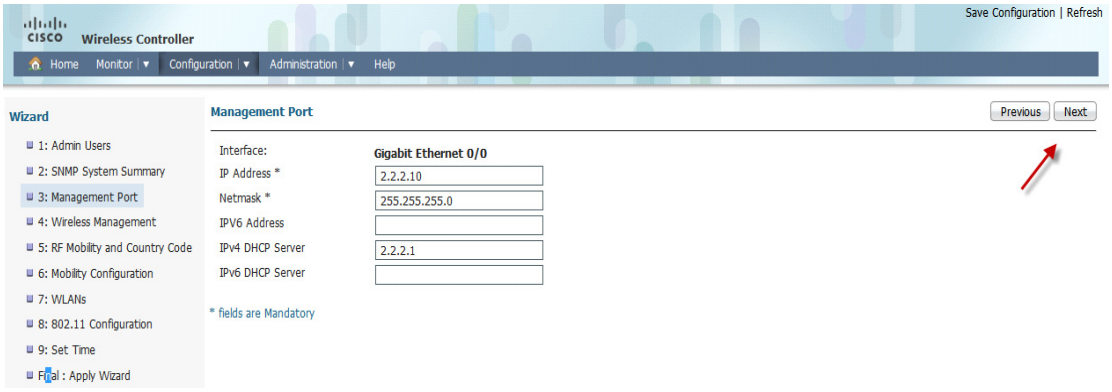
Step 37 Configure admin username and passwords



Step 38 You can configure SNMP trap in this section, give a **Location** and **Contact** to proceed to next step.

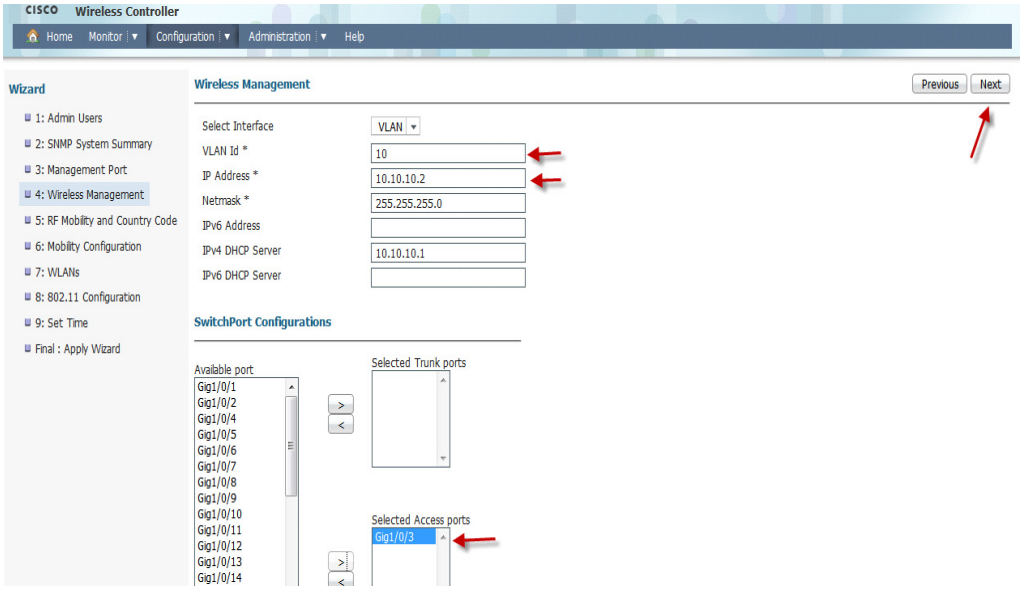


Step 39 Management Interface Configuration–You can use the out of band Management Port to access the switch. Please enter the **IP address/Netmask** shown in the screen below and proceed to next screen for Wireless management configuration.

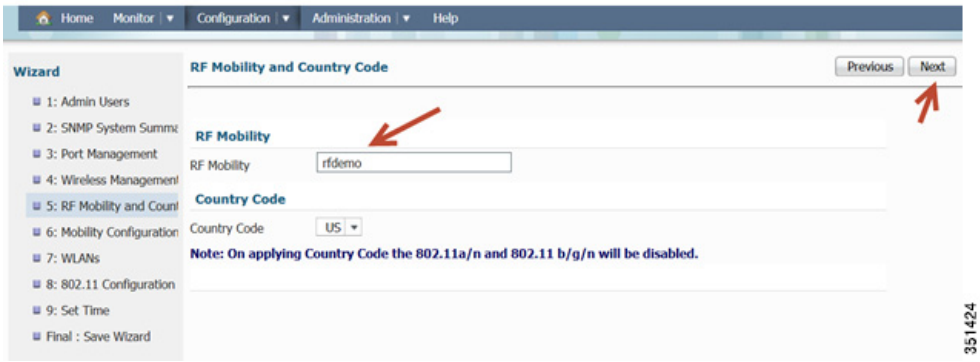


Step 40 Wireless Management Configuration–This is where you can configure Wireless Management interface on the 3850 and assign it for a specific VLAN. Please assign VLAN IP and default gateway.

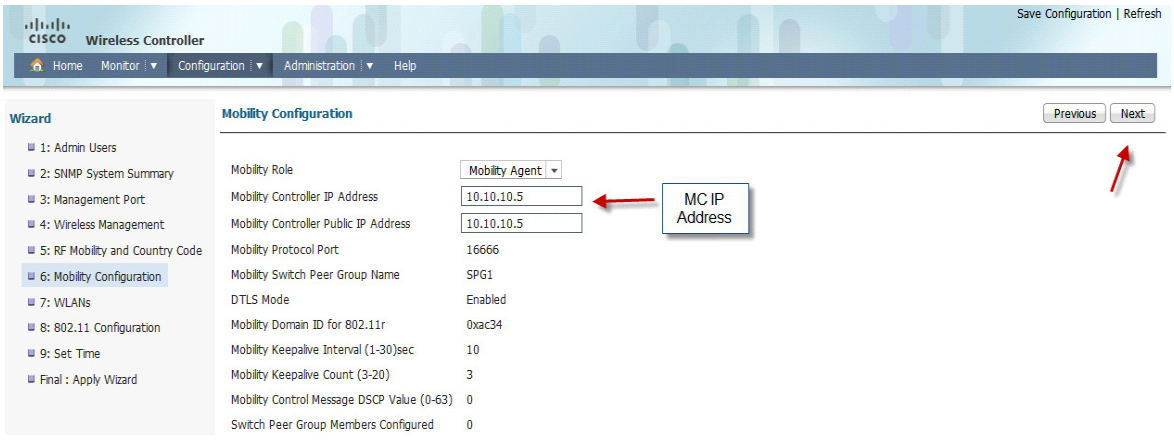
Note AP is connected to Interface Gig1/0/3 marked as access port.



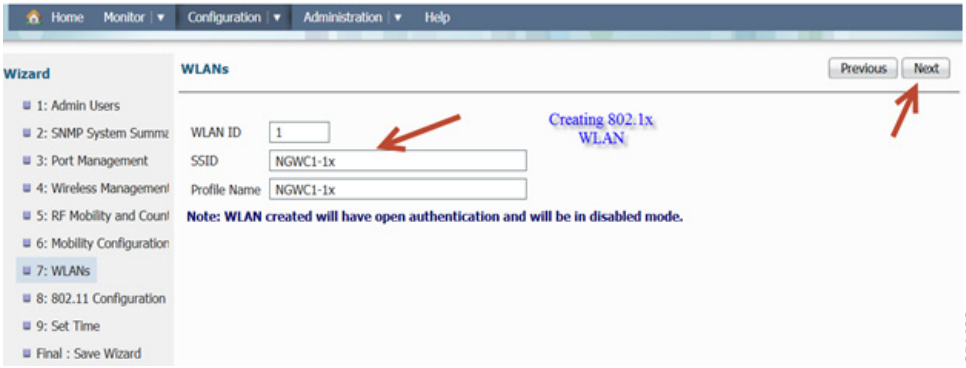
Step 41 Enter RF mobility domain name as **rfdemo** and Country code **US**



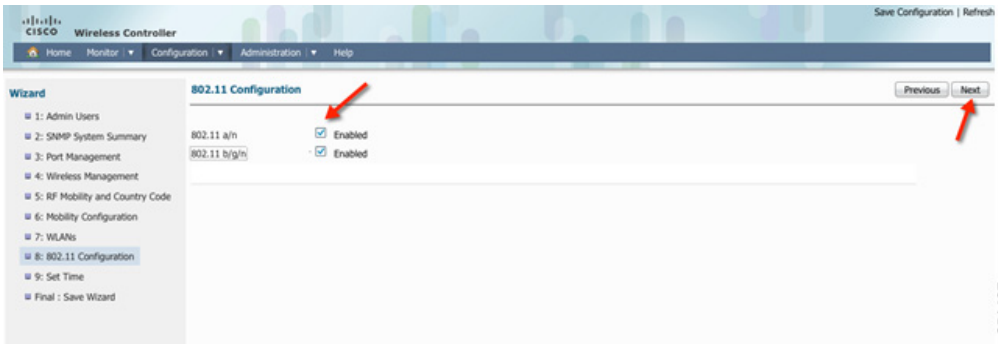
Step 42 Enter Mobility configuration. Define Mobility role as Mobility Agent and enter Mobility Controller public and private IP Address as 10.10.10.5. This is where you point the MA to the MC.



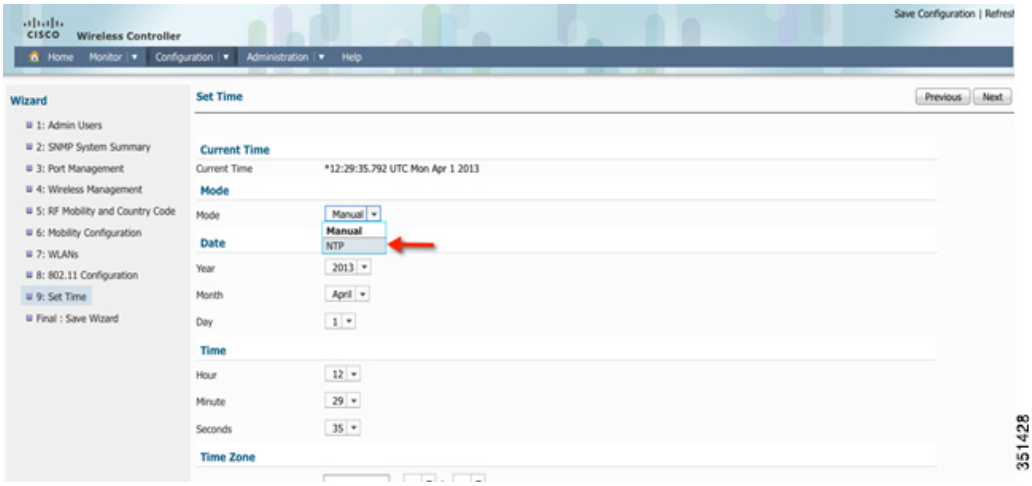
Step 43 Enter WLAN ID as 1 and SSID/Profile information as ngwc1-1x



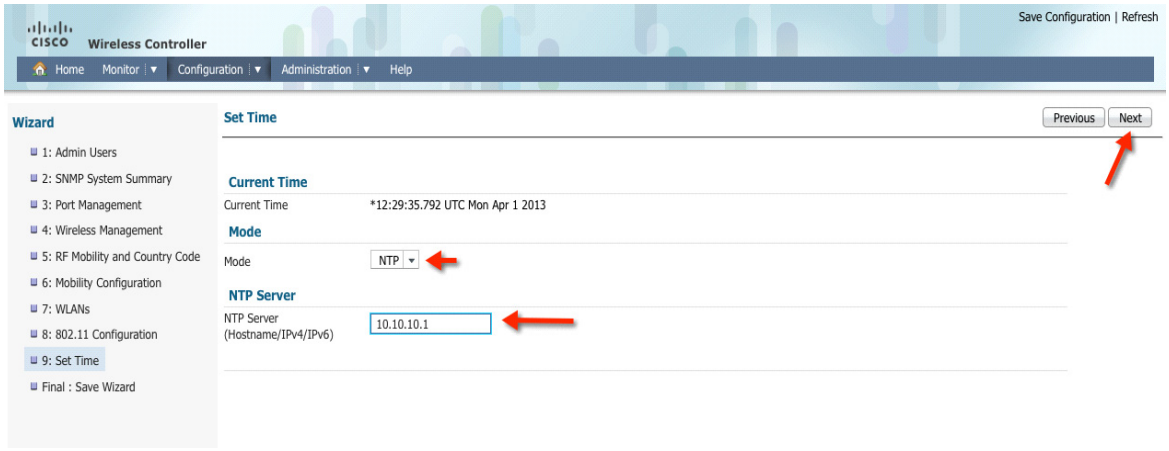
Step 44 Enable Radios as shown below and click **Next**



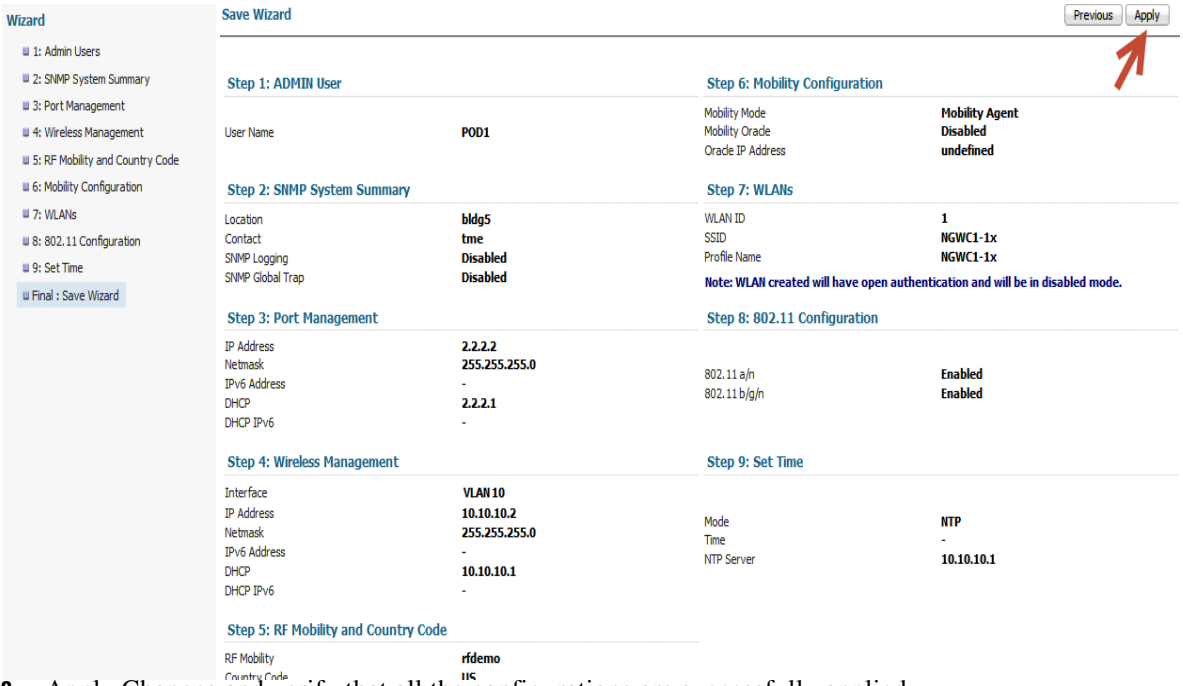
Step 45 Set time as NTP or Manual



Step 46 Enter NTP server as 10.10.10.1 as an example and click **Next**

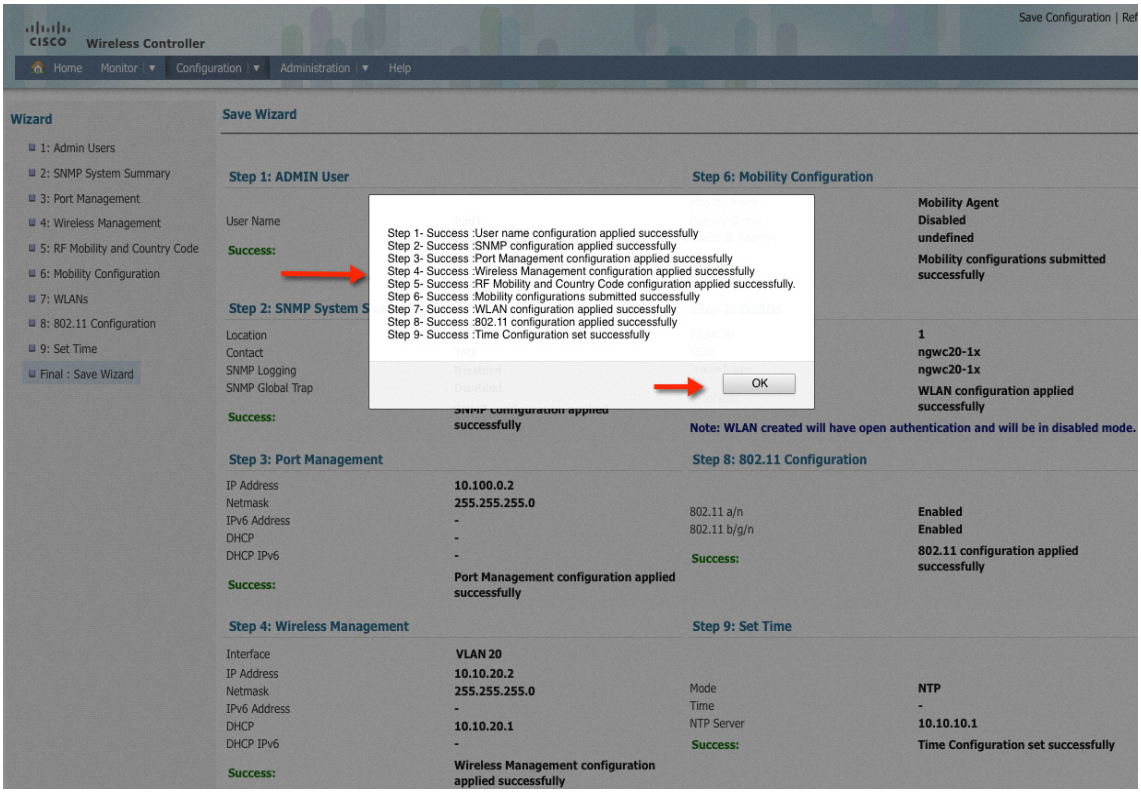


Step 47 At **Save Wizard** page verify Mobility Configuration, WLAN and Wireless Management configuration for your Network

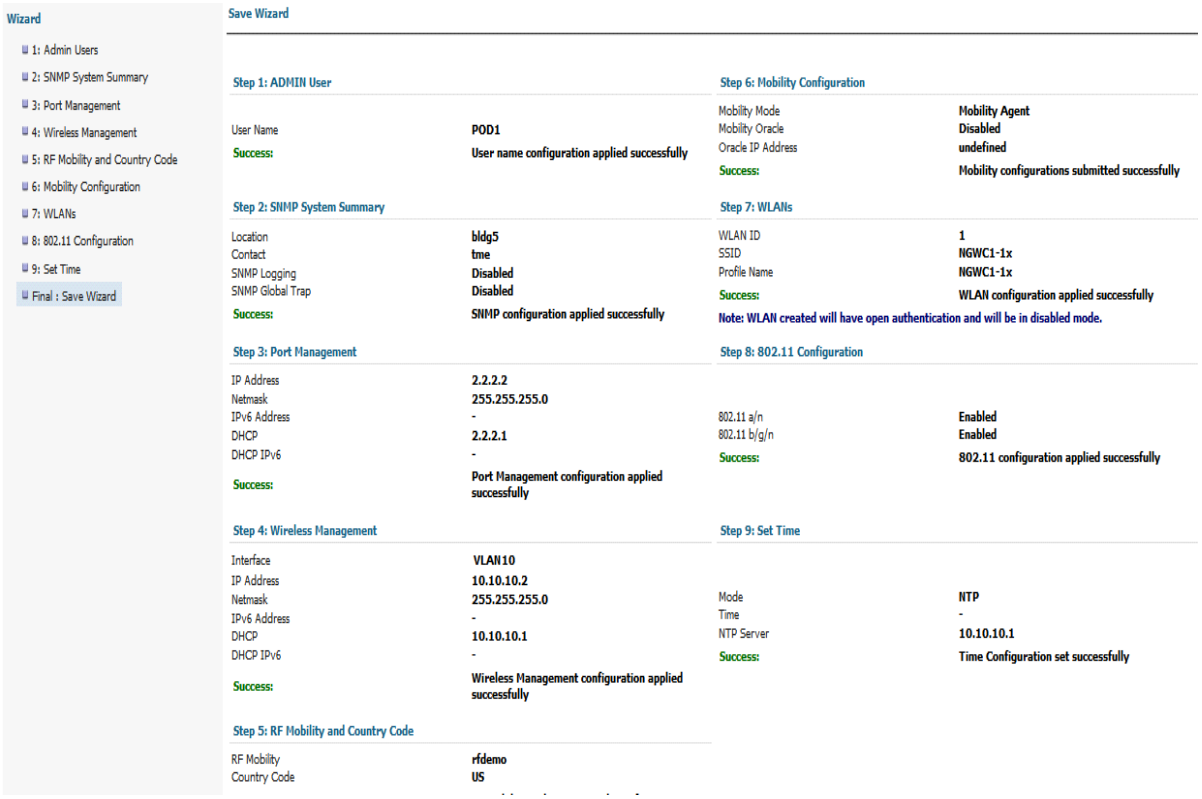


Step 48 Apply Changes and verify that all the configurations are successfully applied.

Note It will take few seconds for the changes to be applied. Do not multiple click.

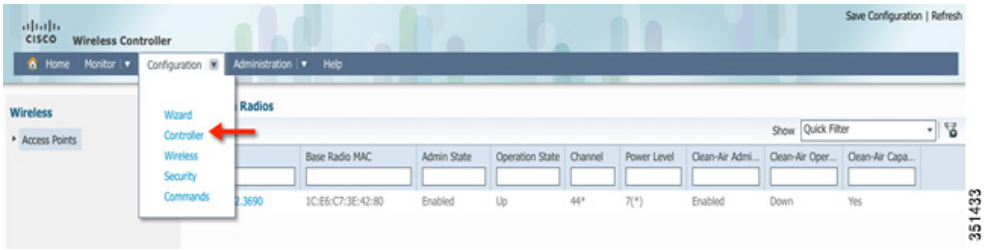


Step 49 The below screenshot displays the final success page where you can verify your configuration changes.

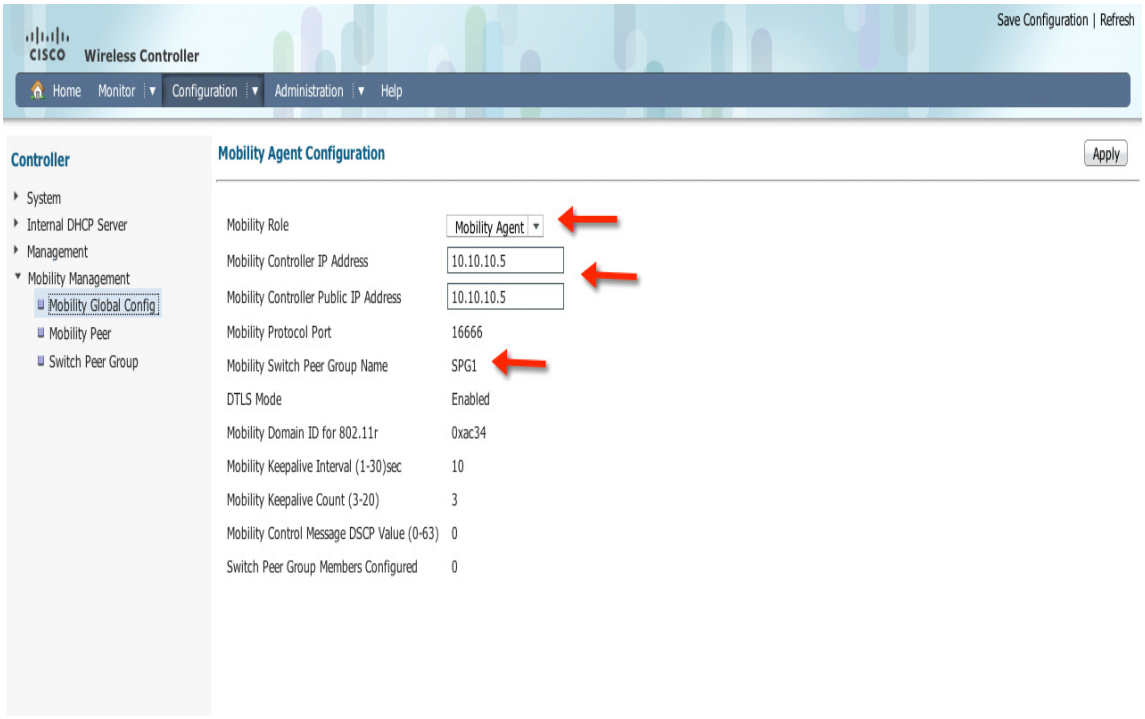


Exercise – Verify New Mobility on MA 3850 and MC 5760

Step 50 Now on Mobility Agent 3850, navigate to **Configuration > Controller > Mobility Management**



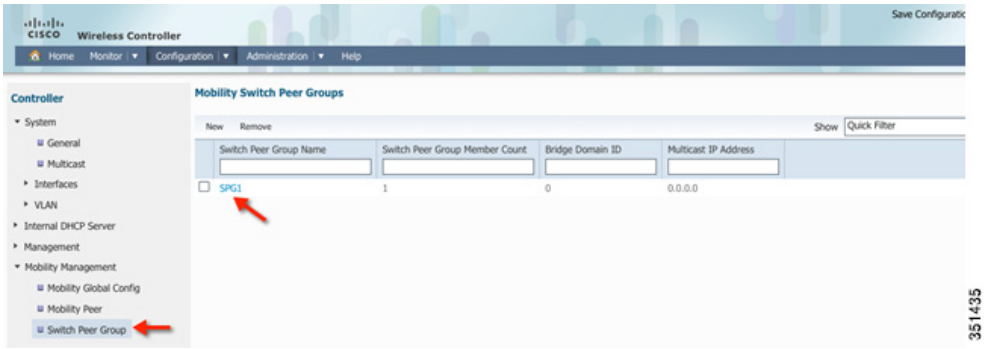
Step 51 Select Mobility Global Config and verify the Mobility role as Mobility Agent and Mobility Controller IP address as your MC 10.10.10.5



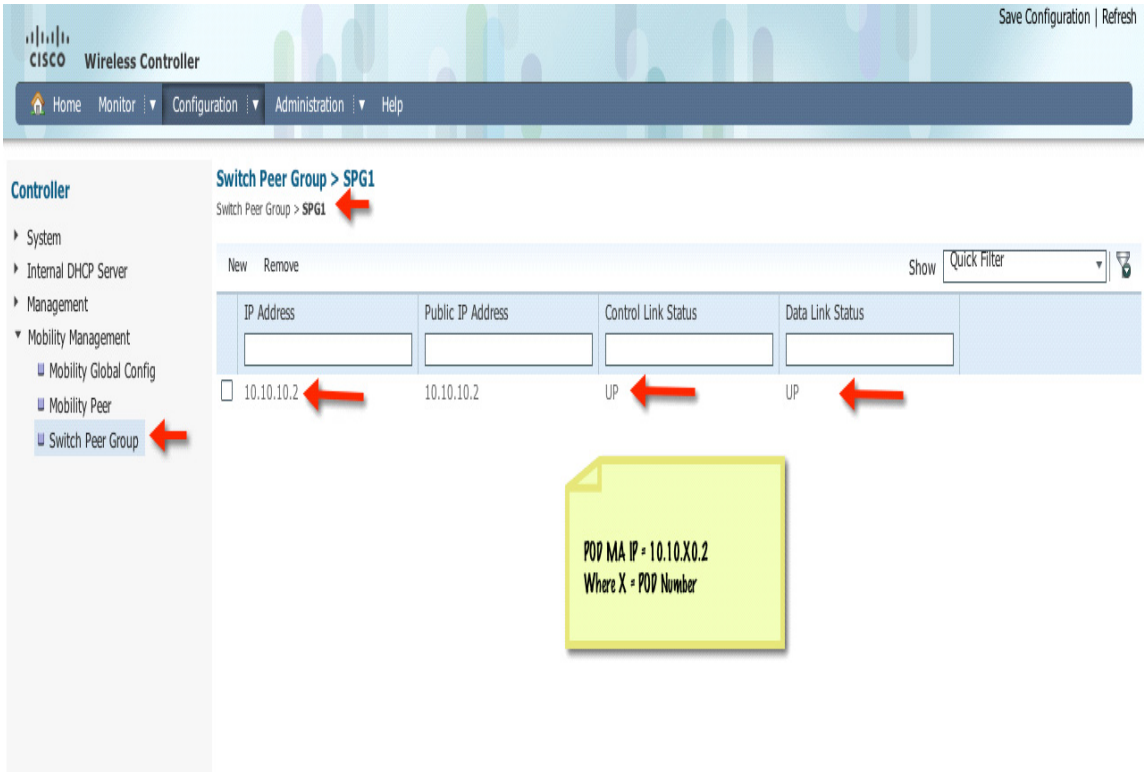
Step 52 Now switch back to you Mobility Controller

https://10.10.10.5

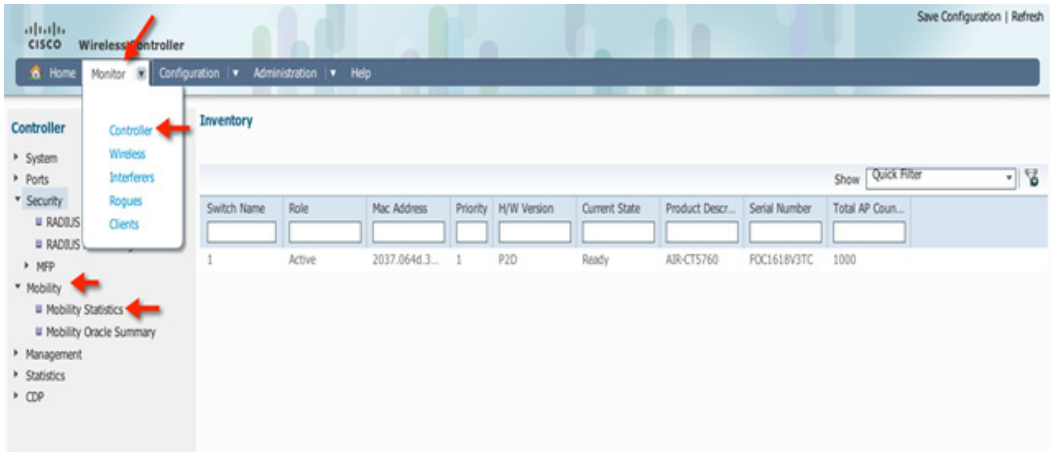
Step 53 Go to **Configuration > Controller > Mobility Management > Switch Peer Group** and then Click SPG1



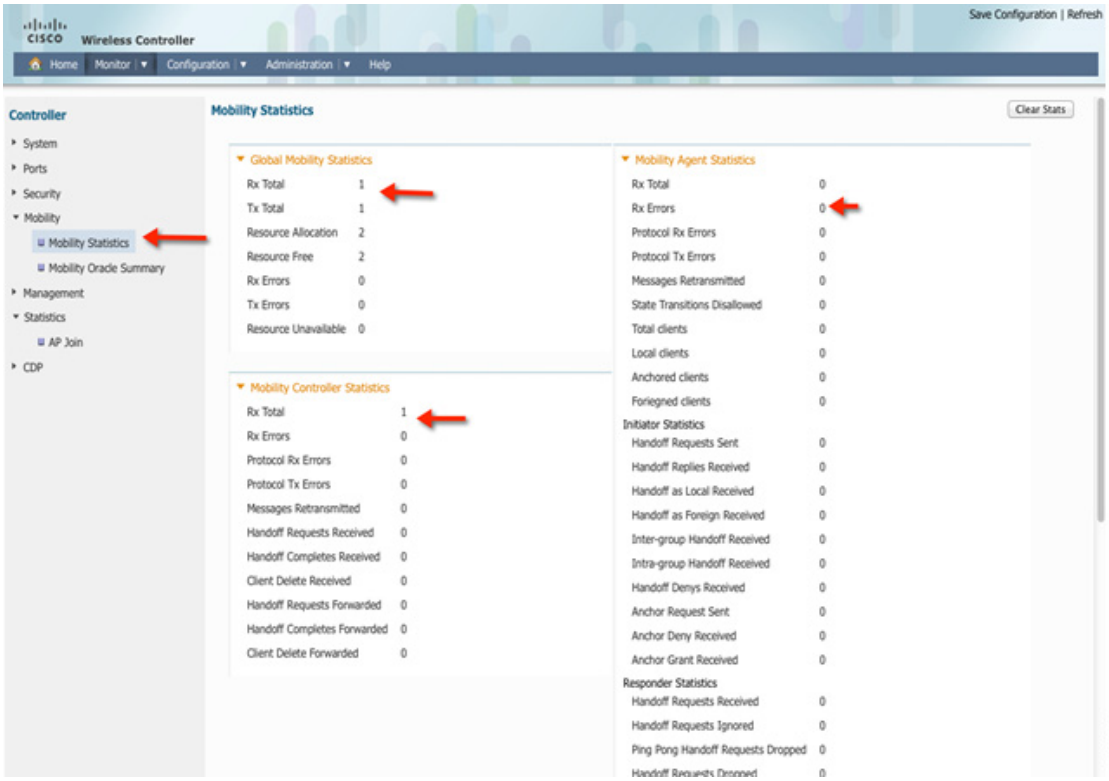
Step 54 Check you MA IP Address 10.10.10.2 and verify that control link status and data link status is UP. If link is still showing down then refresh page. It usually takes around a minute for the link to show as Up.



Step 55 Now go to **Monitor > Controller > Mobility > Mobility Statistics**



Step 56 Verify Mobility statistics

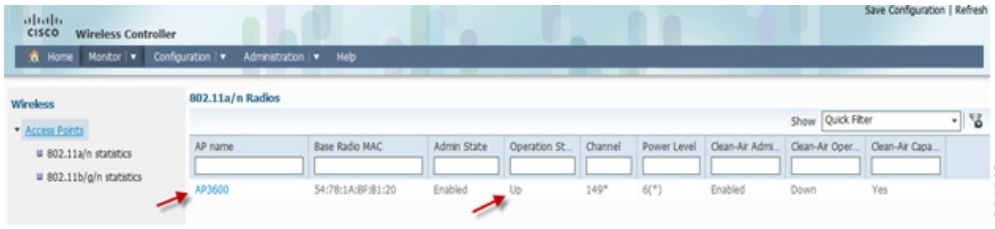


Monitoring: Verify AP Registration Example

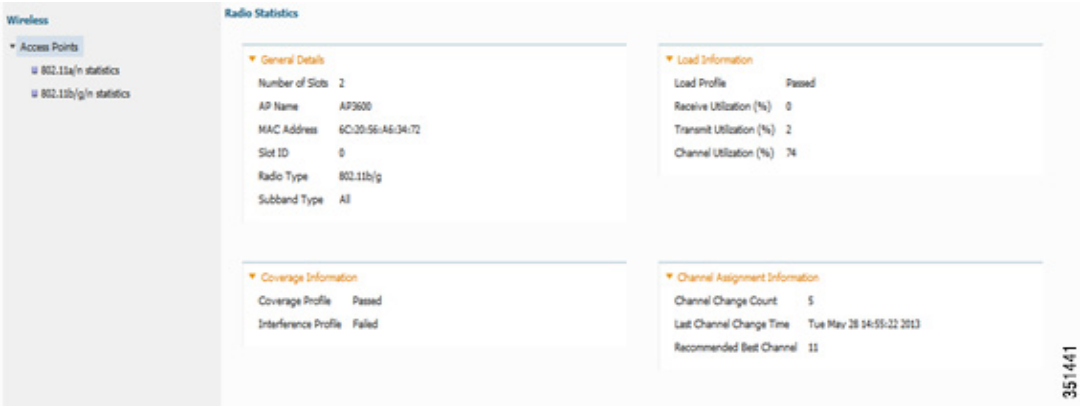
In this section, you monitor and verify AP and Client connectivity.

Step 57 Go to **Monitor > Wireless > Access Points**

Step 58 Verify at **Access Point tab > All APs** that you see your AP connected and it's operationally UP.

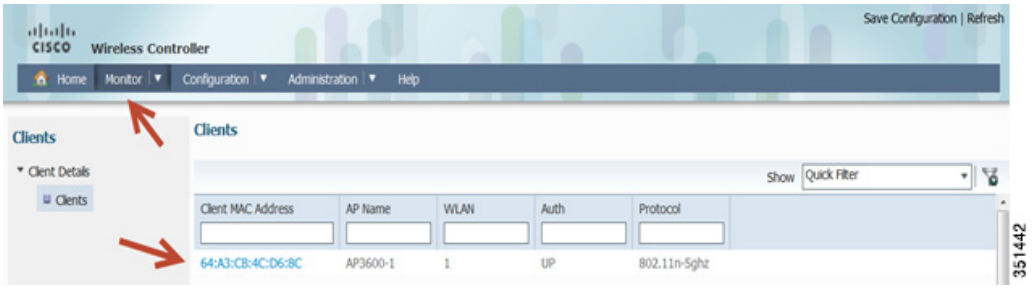


Click the AP and you can check the radio stats, Channel assignment and RF Parameters

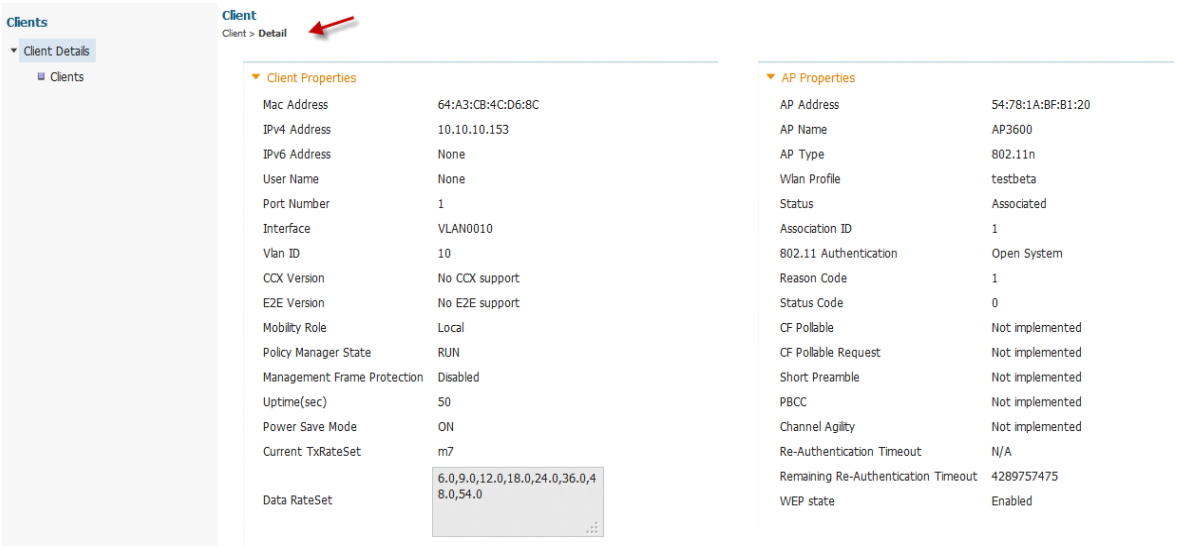


Monitoring: Verify Client Connectivity Example

Step 59 Connecting a Client to your 802.1x WLAN–Go to **Monitor > Clients** and check that the client is connected.

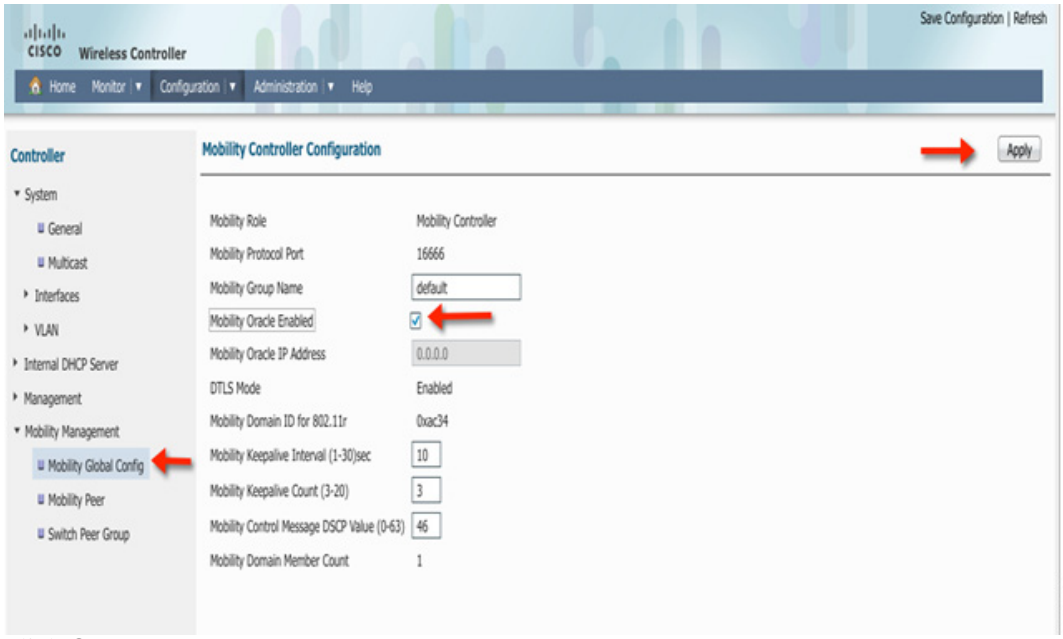


Client Details

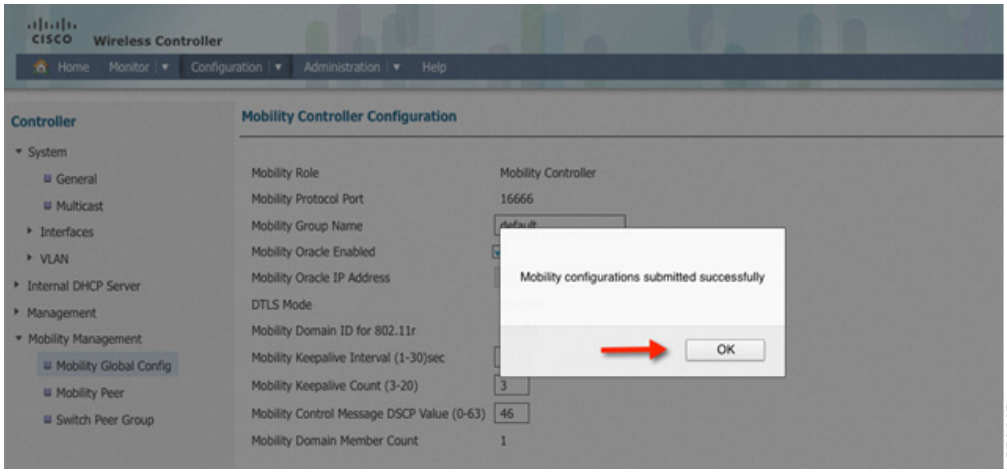


Configure Mobility Oracle, Mobility Peer and Verify Statistics on MC 5760 Example

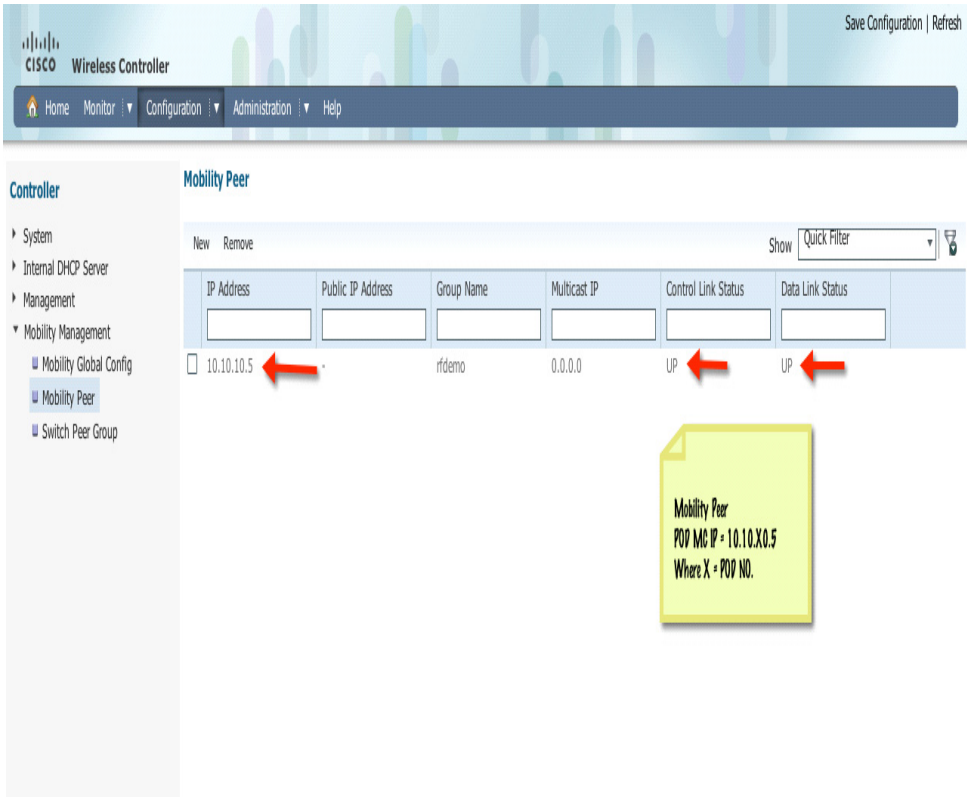
Step 60 Now login back to Mobility Controller 5760 GUI using https://10.10.10.5 and navigate to **Configuration > Controller > Mobility Management** and enable Mobility Oracle as shown below. Click **Apply.**



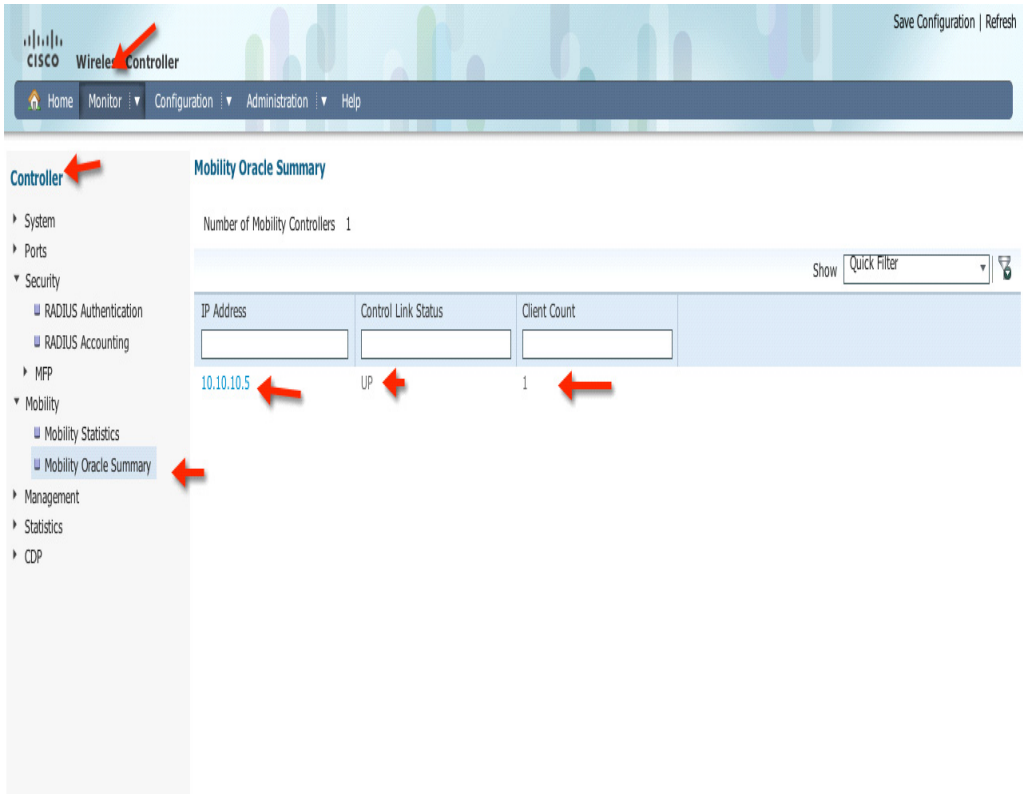
Step 61 Click **OK**



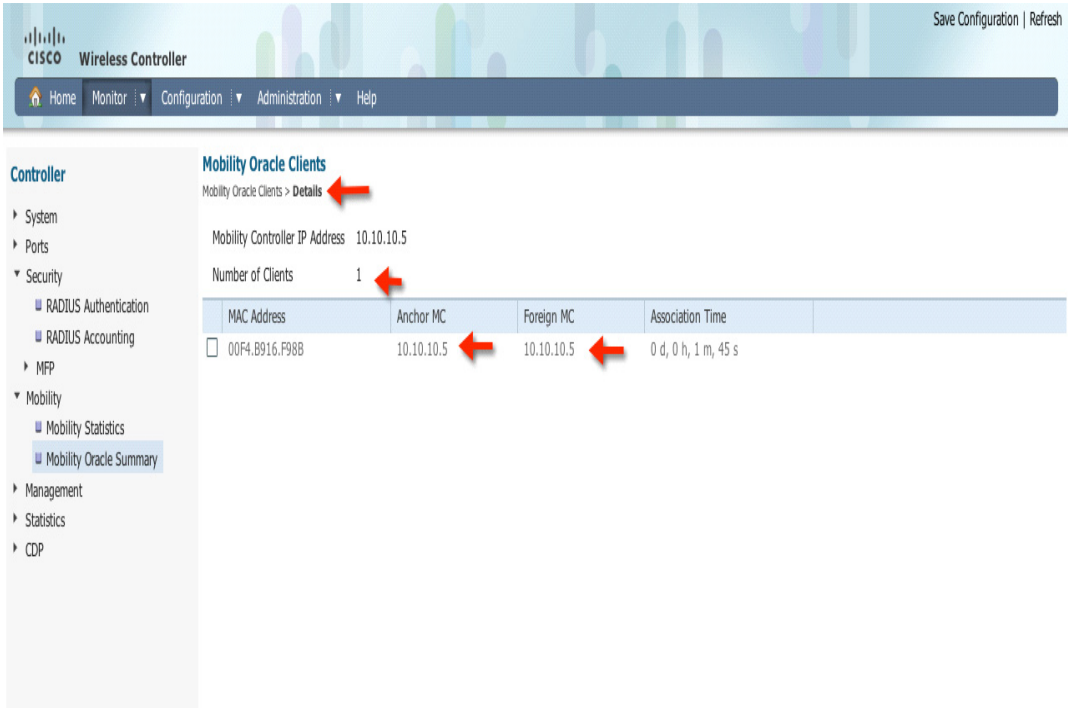
Step 62 Go to Mobility Peer tab and verify that only MC is showing and the link status is shown as **UP**



Step 63 Now navigate to **Monitor > Mobility > Mobility Oracle Summary** and verify client count is showing as 1.



Step 64 Click on IP address and verify your client details on MO as shown below:

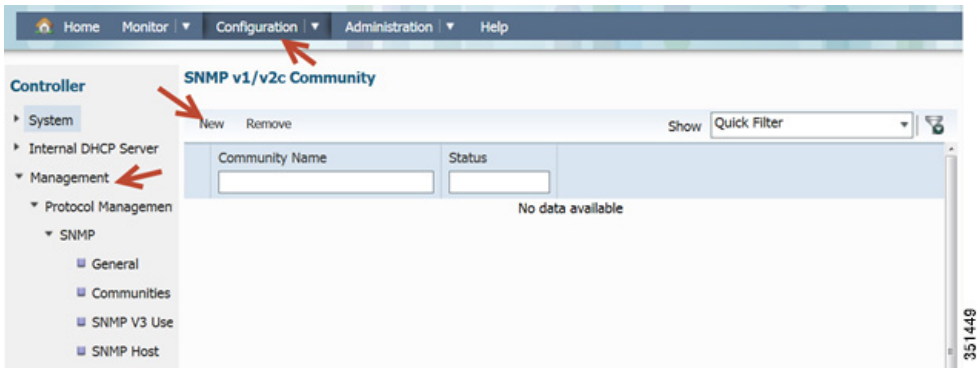


Managing CT5760/Cat3850 with Cisco Prime Infrastructure 2.0 Example

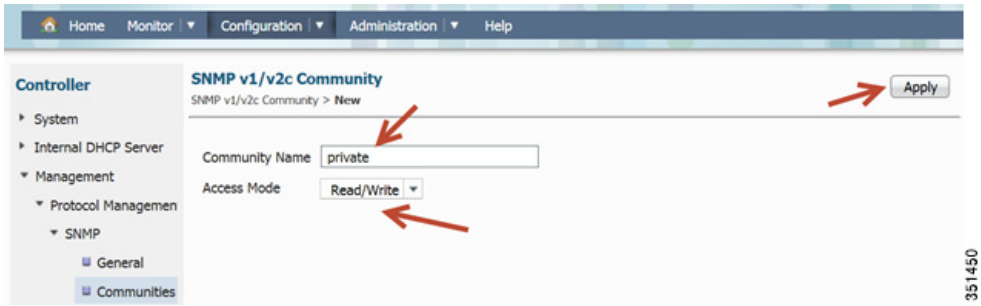
In this section you will:

- Configure SNMP on CT5760
- Add CT5760/Cat3850 to Cisco Prime Infrastructure.
- Manage basic CT5760/Cat3850 functions on Prime Infrastructure.

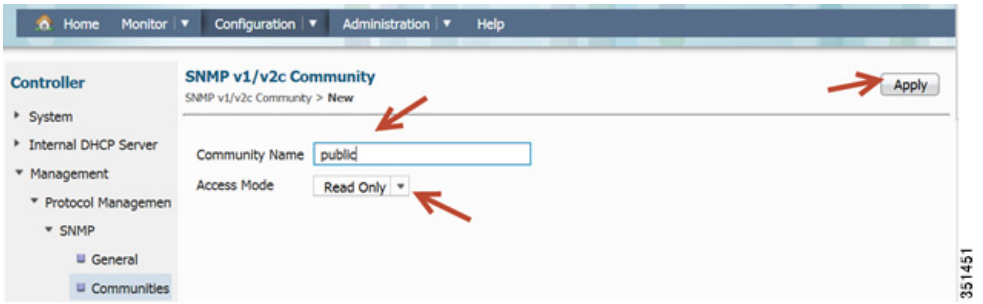
Step 65 SNMP strings Configurations– navigate to 5760 Web GUI: **Configuration > Controller > Management > Protocol Management > SNMP > Communities**



Configure SNMP strings for private and public

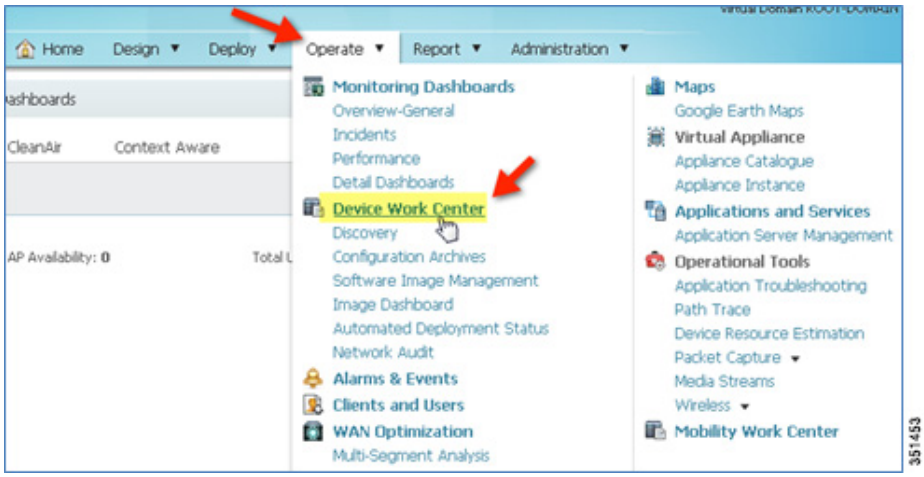


Repeat the same step for a public Community

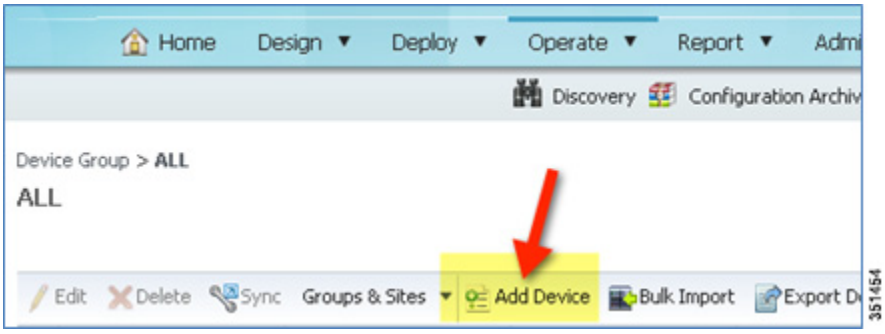


Step 66 Log in to PI 2.0

Step 67 Navigate to **PI > Operate > Device Work Center.**



Step 68 Click ‘Add Device’.



Step 69 Enter CT5760 parameters:

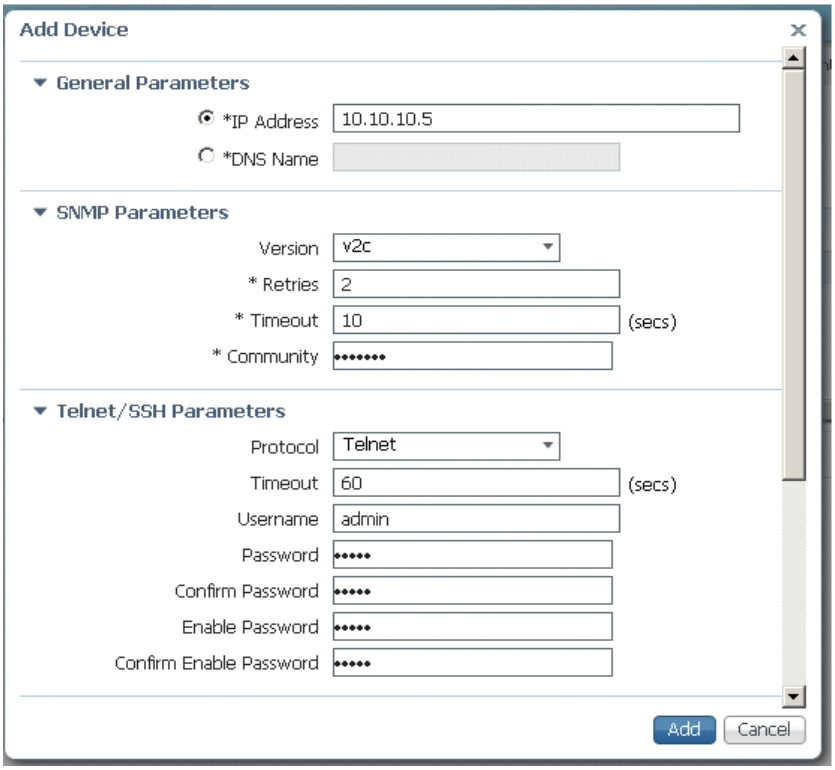
a. IP address – CT5760 mgt IP

b. Read-Write SNMP string (private)

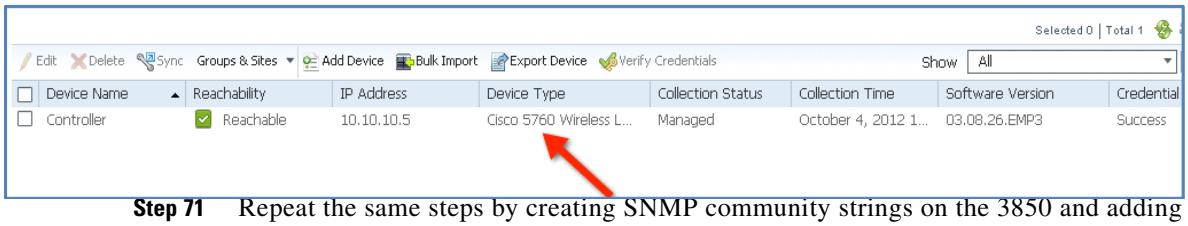
c. Telnet credentials

- Username = admin

- User password = admin
- iEnable password = cisco
- HTTP credentials can be IGNORED

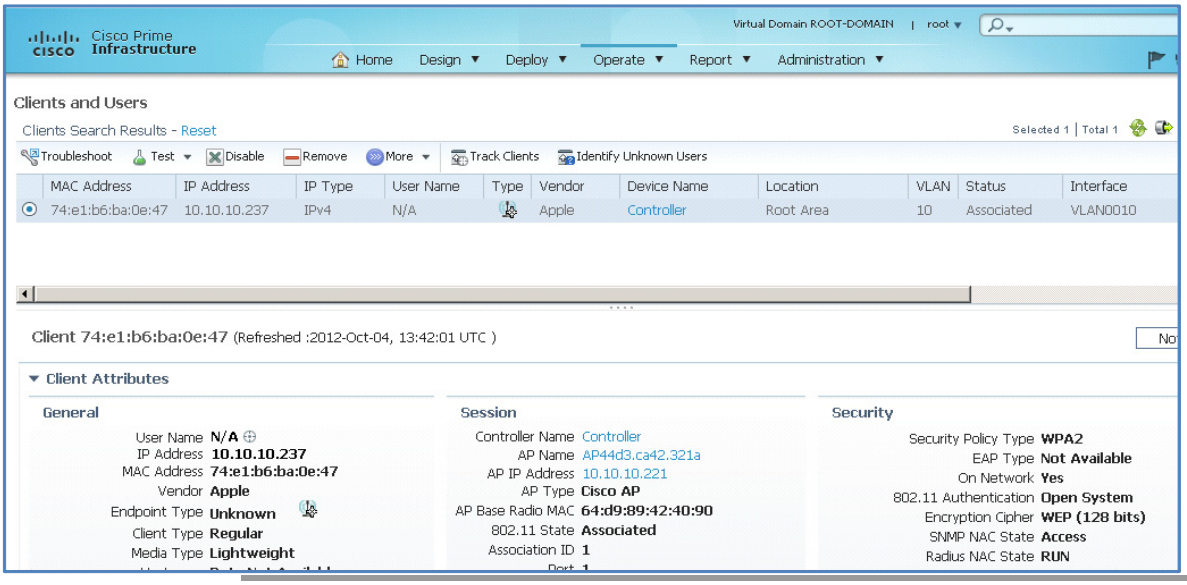


Step 70 Confirm Prime Infrastructure discovery of the CT5760 – if reachable and successful, the status will show as complete with the correct device type.



Step 71 Repeat the same steps by creating SNMP community strings on the 3850 and adding it to Prime Infrastructure.

Step 72 Explore Cisco Prime Infrastructure GUI in management of CT5760, e.g. client statistics, details, reports etc.


Cisco Prime Infrastructure
Virtual Domain ROOT-DOMAIN | root
Home Design Deploy Operate Report Administration
Clients and Users
Clients Search Results - Reset
Selected 1 | Total 1
Troubleshoot Test Disable Remove More Track Clients Identify Unknown Users
MAC Address IP Address IP Type User Name Type Vendor Device Name Location VLAN Status Interface
74:e1:b6:ba:0e:47 10.10.10.237 IPv4 N/A Apple Controller Root Area 10 Associated VLAN0010
Client 74:e1:b6:ba:0e:47 (Refreshed :2012-Oct-04, 13:42:01 UTC)
Client Attributes
General
User Name N/A
IP Address 10.10.10.237
MAC Address 74:e1:b6:ba:0e:47
Vendor Apple
Endpoint Type Unknown
Client Type Regular
Media Type Lightweight
Session
Controller Name Controller
AP Name AP44d3.ca42.321a
AP IP Address 10.10.10.221
AP Type Cisco AP
AP Base Radio MAC 64:d9:89:42:40:90
802.11 State Associated
Association ID 1
Security
Security Policy Type WPA2
EAP Type Not Available
On Network Yes
802.11 Authentication Open System
Encryption Cipher WEP (128 bits)
SNMP NAC State Access
Radius NAC State RUN