ZYXEL

www.zyxel.com

NXC Series

NXC 2500/ 5500

NXC Controllers

Firmware Version 5.40
Edition 11, 06/2019

Handbook

Default Login Details	
LAN Port IP Address	https://192.168.1.1
User Name	admin
Password	1234

Contents

Manage APs through NXC Controller

1.1 How to Manage APs through NXC Controller

This example shows how to use the NXC controller to manage APs via manual setting, DHCP option 138 and broadcast. In this case shown as below, there are two subnets in the environment. The APs can find NXC controller in the same subnet via broadcasting without any settings. The APs in different subnet can find NXC controller by manually setting NXC controller's IP or DHCP option 138 in DHCP server.

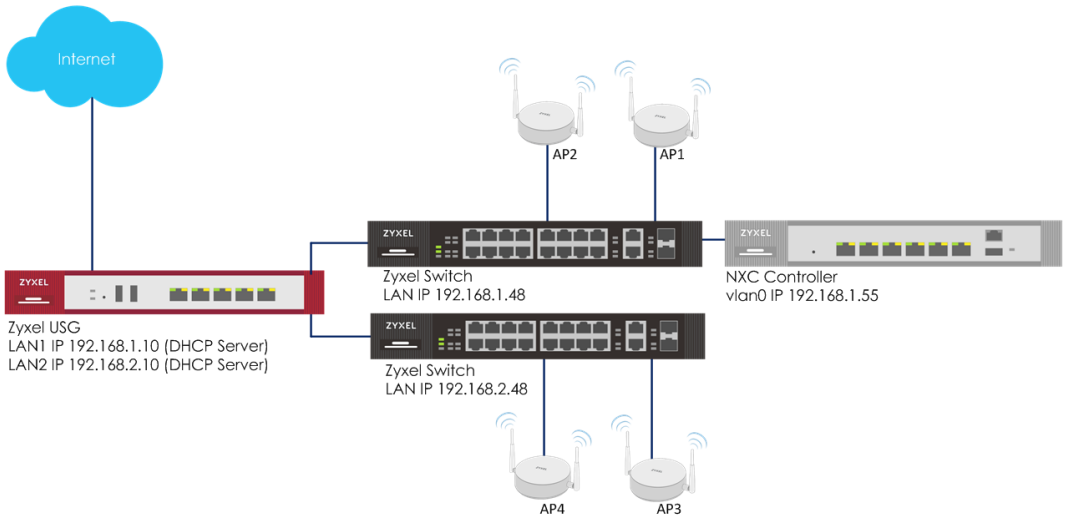


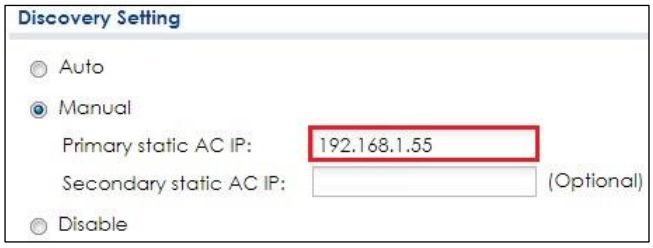
Figure 1.1 Manage APs through NXC Controller

Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC5500 (Firmware Version: 5.40), GS2210-8HP (Firmware Version: V4.30).

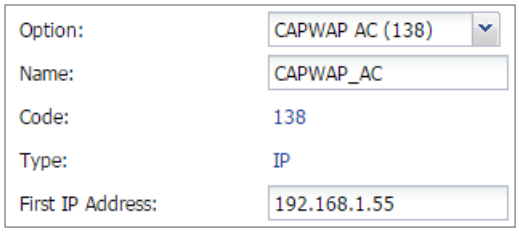
1.1.1 Configuration in the AP

1 In the same subnet (for AP1 and AP2), the APs don't need to do any setting. The APs can find the NXC controller via broadcast and NXC controller always accepts APs to managed list by default. The NXC controller manages the APs without any setting.

2 In the different subnet (for AP3 and AP4), the APs need to set the NXC controller's IP manually. Go to **CONFIGURATION > Network > AC Discovery**, set **Discovery Setting** to **Manual** and set the NXC controller's IP **192.168.1.55** to **Primary static AC IP**. Click **Apply** to apply the setting.



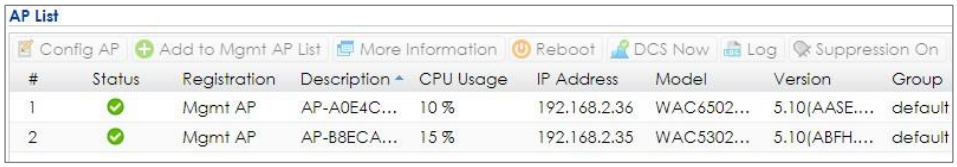
3 Or, you can use DHCP option 138 in the DHCP server for the APs which are in the different subnet from NXC controller.



1.1.2 Test the Result

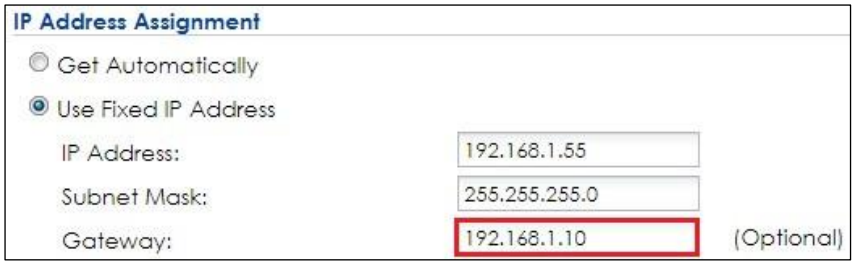
1 When the APs and the NXC controller are in the same subnet, the NXC controller manages the APs without any settings. The result is visible in **MONITOR > Wireless > AP Information > AP List**.

2 When the APs and the NXC controller are in the different subnets, the APs can find NXC controller through manually setting NXC controller's IP or DHCP option 138. After the APs find the NXC controller, the NXC controller can manage the APs. The result is visible in **MONITOR > Wireless > AP Information > AP List**.



1.1.3 What Could Go Wrong?

1 To make sure the NXC controller goes to correct traffic routing, please remember to set up the gateway in NXC controller.



2 When you use the manual NXC controller IP or DHCP option 138, please make sure the NXC controller's IP is correct so that the APs can find the NXC controller.

1.2 How to Enlarge Managed AP Number with License

This example shows how to enlarge managed AP number with license. The default managed AP number for NXC2500 is 8 units and NXC5500 is 64 units. If you want to control more than default managed units, it's necessary to import the license to enlarge managed AP number.

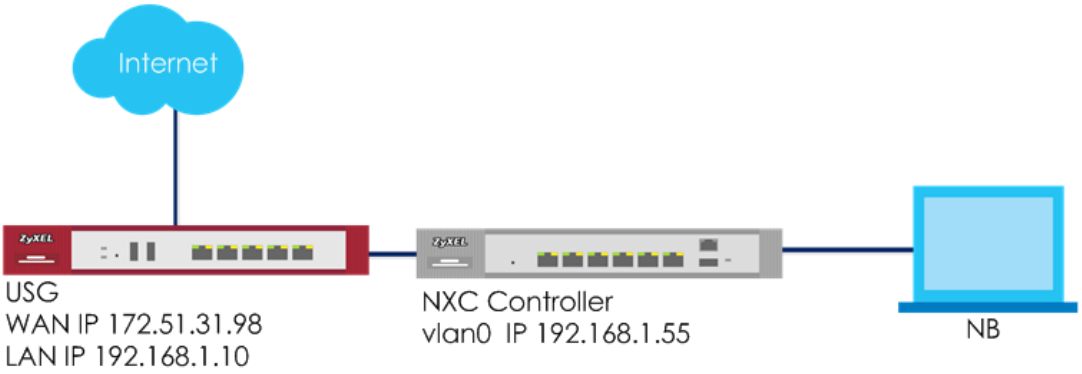
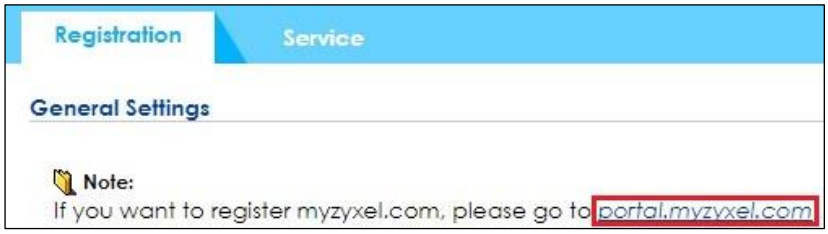


Figure 1.2 Enlarge Managed AP Number

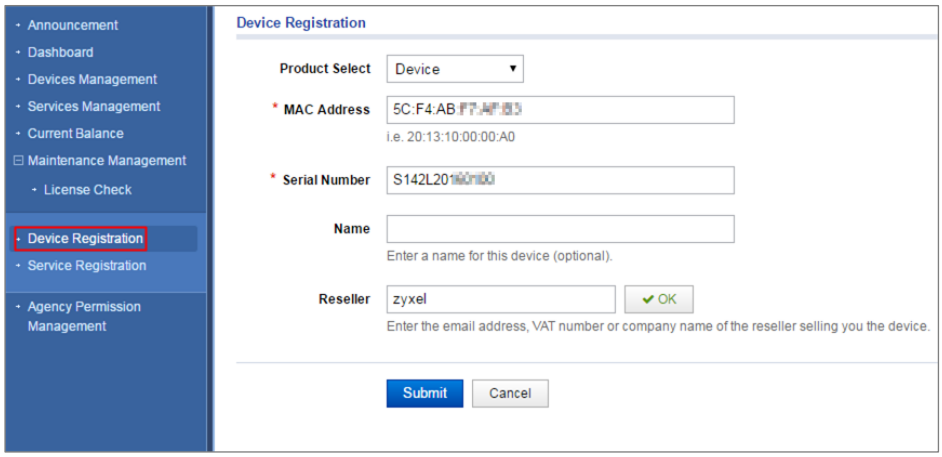
Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC2500 (Firmware Version: 5.40), GS2210-8HP (Firmware Version: V4.30).

1.2.1 Device Registration

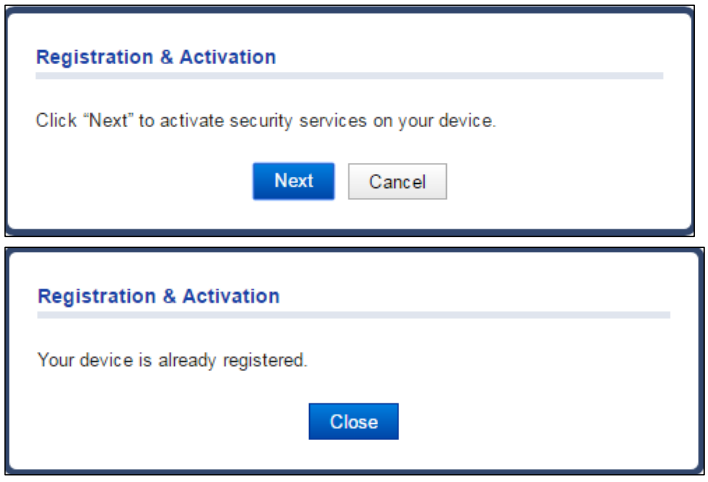
1 Click the hyperlink on NXC controller's GUI to connect portal.myzyxel.com in **CONFIGURATION > Licensing > Registration**.



2 After log in the registration portal, click the **Device Registration** to register a device by filling in the **MAC Address** and **Serial Number**. Click **Submit**.

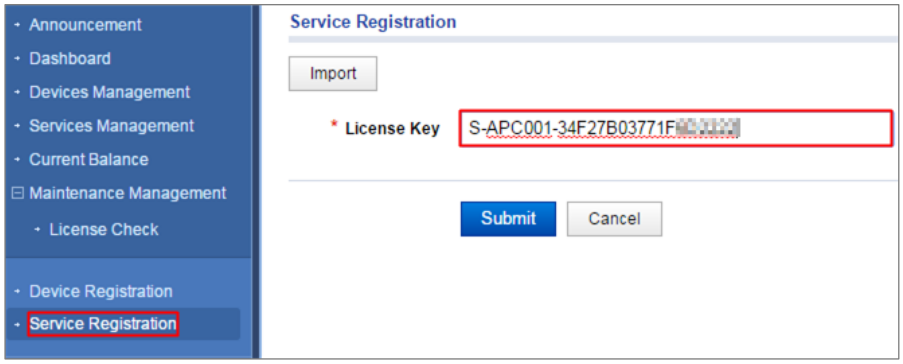


3 Click **Next** to activate security services on the device, and click **Close** in next step.

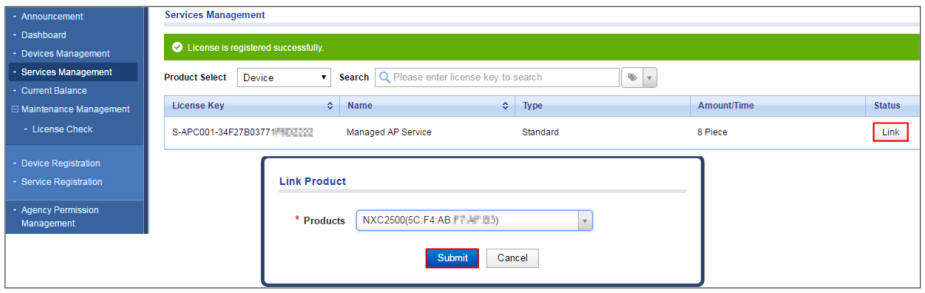


1.2.2 Service Registration

1 Click **Service Registration** and fill in the **License Key**. Click **Submit** to register the license key.

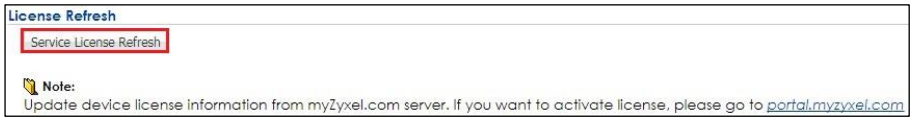


2 Click **Service Management**, and click the **Link**. Select a device, and then click **Submit** to activate the license key for the selected device.



1.2.3 License Refresh

1 Click **Service License Refresh** in below path of NXC controller web GUI. Go to **CONFIGURATION > Licensing > Registration.**



1.2.4 Test the Result

1 The Count of Managed AP number changes from 8 to 16 in **CONFIGURATION > Licensing > Registration**.

License Status

#	Status	Registration Type	Expiration Date	Count	Service
1	Licensed	Standard		16	Managed AP Service

Set up a Wireless Connection Environment

2.1 How to configure with the Wizard Setting.

This example shows how to get start with Wizard. It will be easier to complete the deployment configuration of the AP and the NXC. The Wizard setting includes Uplink Connection, VLAN Setting and AP Profile. The NXC will be the DHCP server for the stations, and all the guest stations must pass the captive portal authentication. NXC5500 does not support Wizard Setting now.

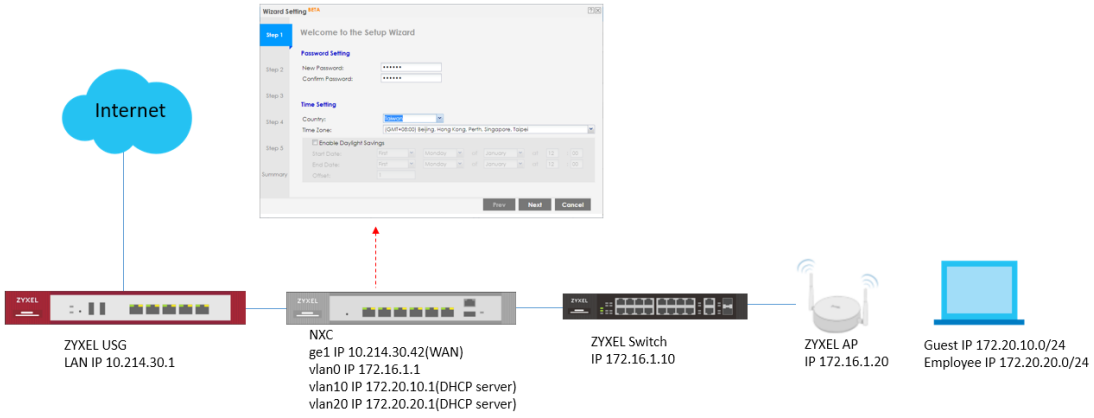
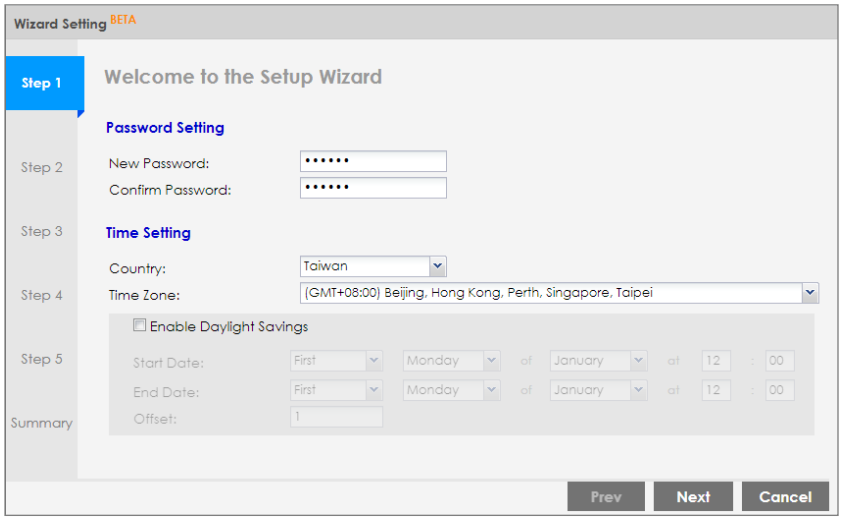


Figure 2.1 Add configuration via Wizard settings.

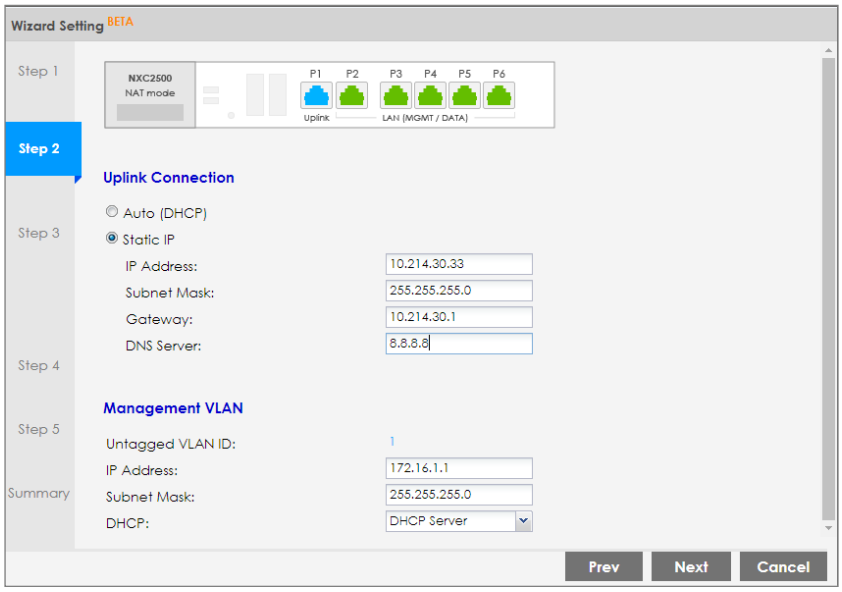
Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG210 (Firmware Version: V4.30), GS2210 (Firmware Version: V4.50), NXC2500 (Firmware Version: 5.40)

2.1.1 How to configure the Wizard Setting with First login?

1 Change the **Password Setting** to the private one. Configure the correct **Time Setting**. Enable **Daylight Saving** if needed. Click **Next**.

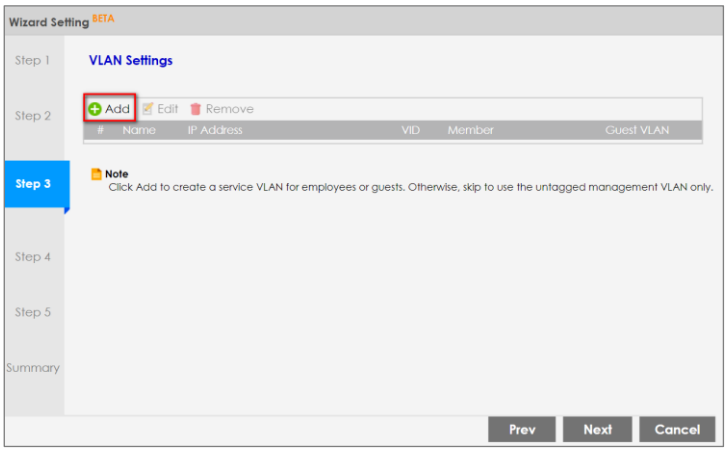


2 Configure the **Uplink Connection** which will be connected to the USG as 10.214.30.33/24, and the gateway is USG LAN IP address 10.214.30.1. Add the DNS server as 8.8.8.8. Configure the **Management VLAN** to manage AP. The default setting IP address is 172.16.1.1/24 and enable DHCP server. Click **Next**.



3 Add VLAN interfaces for Employee and Guest.

a. Add Interface for Guest. Click **Add** to create a service VLAN for guests.



b. Set the configuration as below:

Tagged VLAN ID:**10**,

Guest VLAN is **Enable**. (Guest VLAN: This field displays if this is a guest VLAN and if the captive portal feature is enabled.)

Restrict Intranet Access: Enable

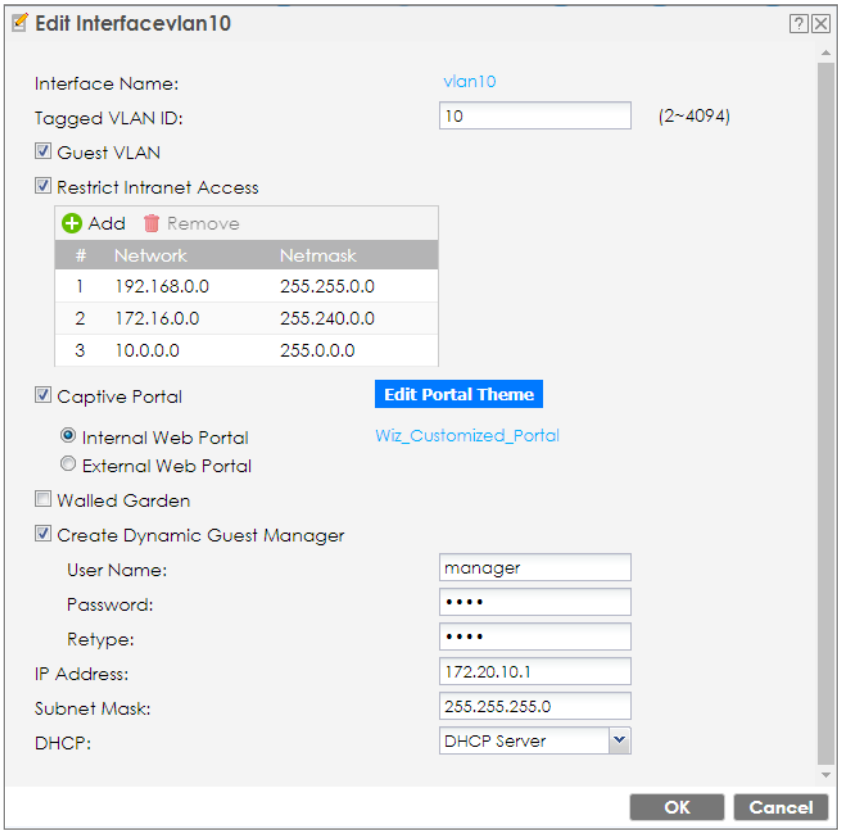
(Restrict Intranet Access: define the local networks to which wireless clients cannot have access)

Captive Portal: Enable.

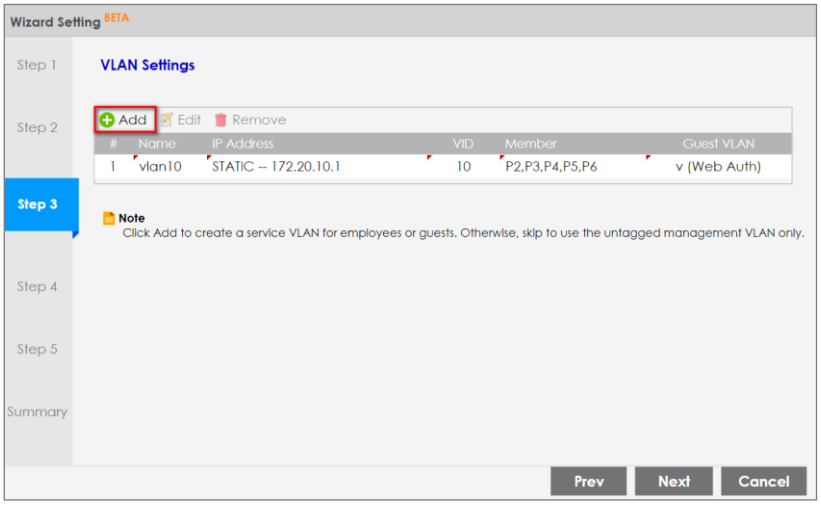
Create Dynamic Guest Manager: fill in the guest manager information.

Fill in the **IP address**, **Subnet Mask**, and **DHCP setting**.

Click **OK**.



c. Add Interface for Employee. Click **Add** to create a service VLAN for guests.

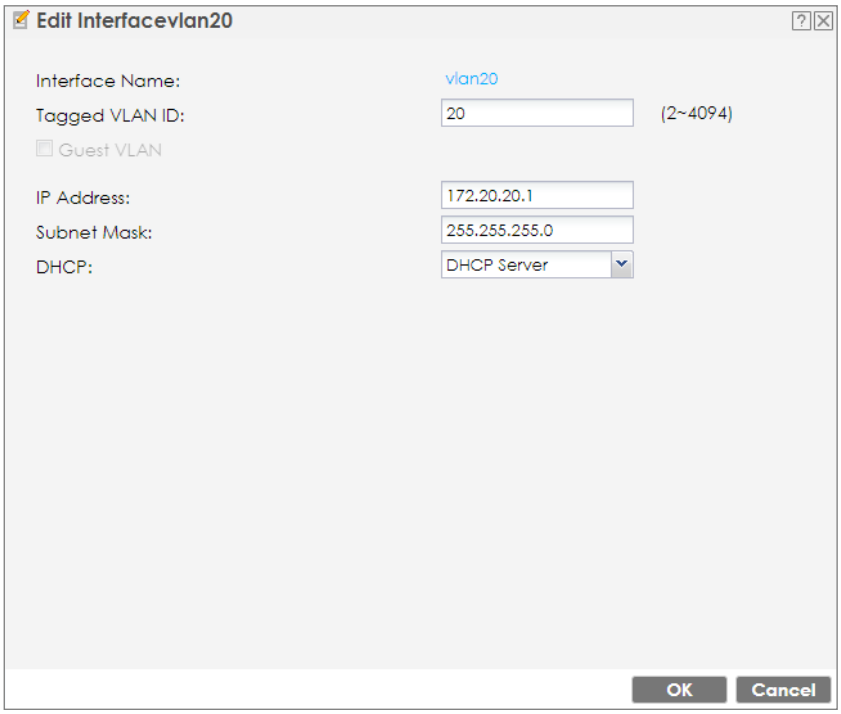


d. Set the configuration as below:

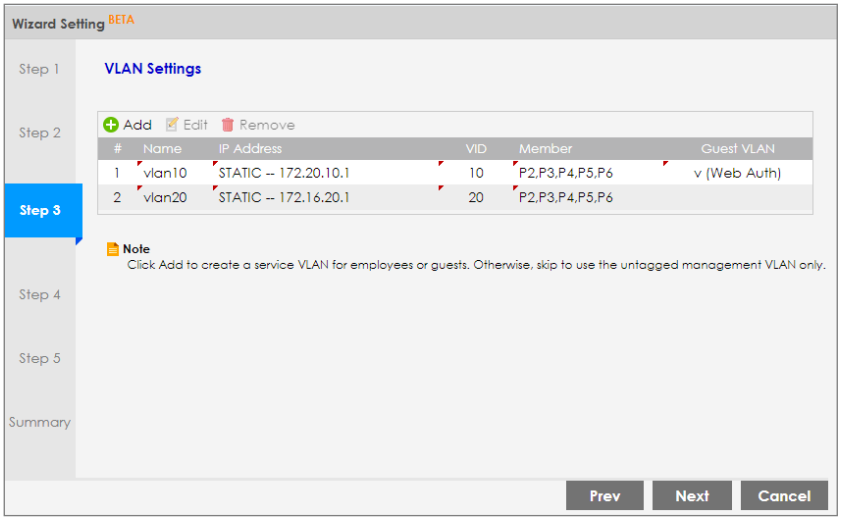
Tagged VLAN ID: 20

Fill in the **IP address**, **Subnet Mask**, and **DHCP setting**.

Click **OK**.



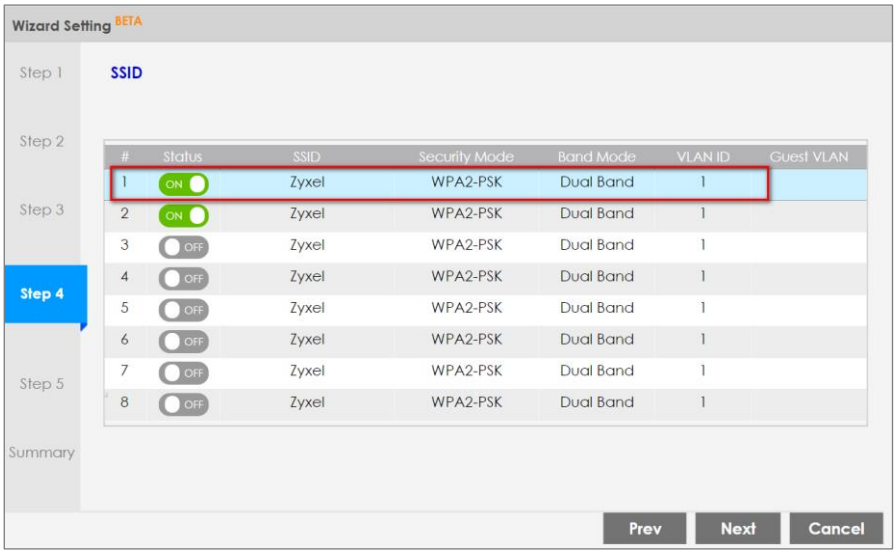
e. Click **Next.**



4 Configure the SSID profile.

a. Edit the SSID profile for Guest

Double click the SSID profile to modify the configuration.



b. Edit the first **SSID Profile** for Guest VLAN.

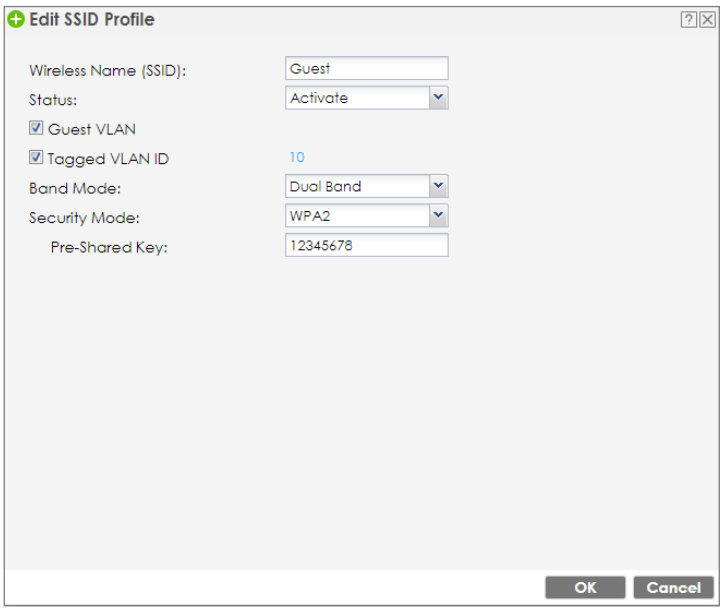
Wireless Name (SSID): Guest

Guest VLAN: Enable (it will fill in the Guest VLAN setting automatically.)

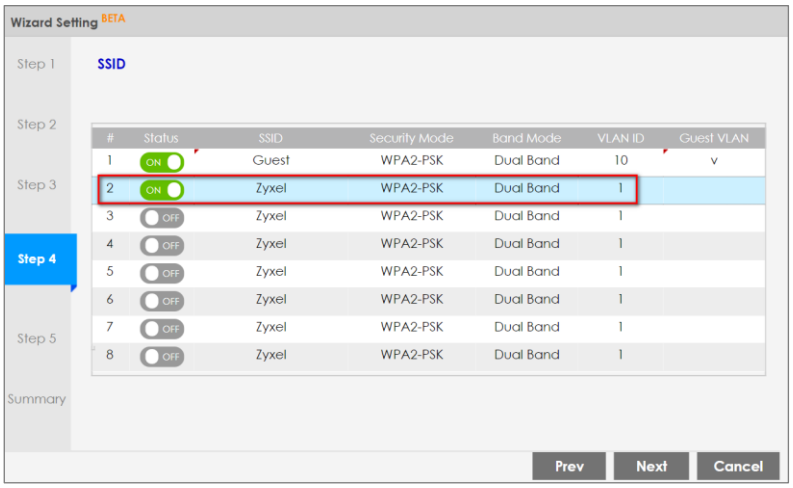
Security Mode: WPA2

Pre-Shared Key: 12345678

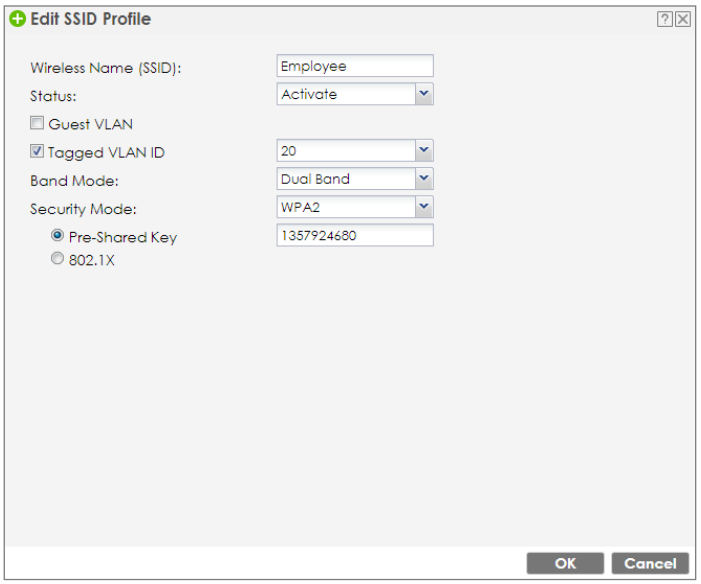
Click **OK**.



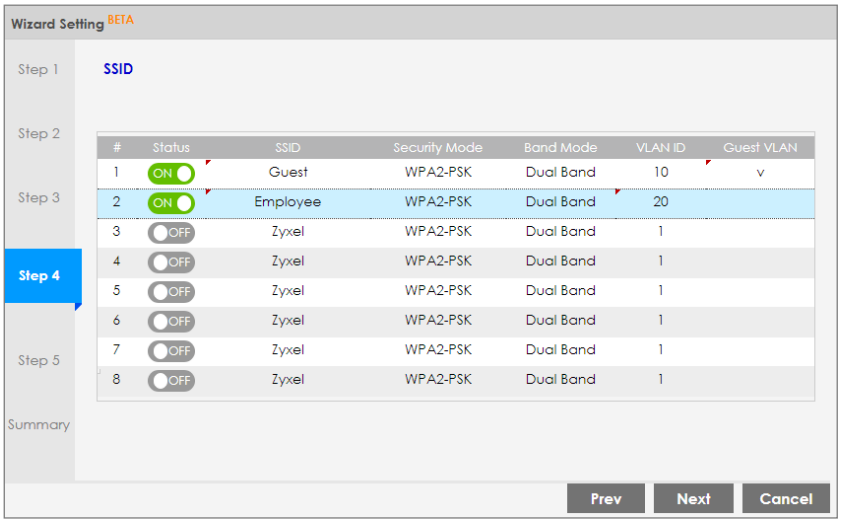
c. Edit the second **SSID Profile** for Employee.
Double click the SSID profile to modify the configuration.



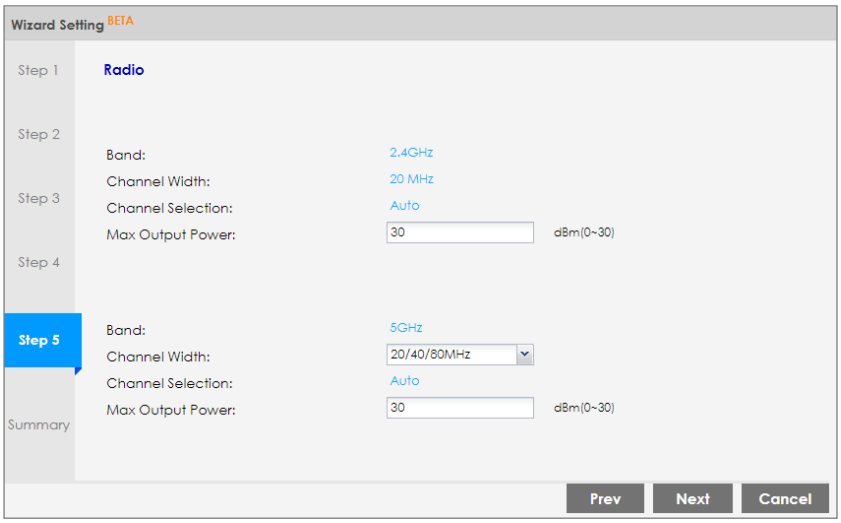
d. Set the configuration as below:
Tagged VLAN ID: 20
Security Mode: WPA2
Pre-Shared Key: 1357924680
Click **OK**.



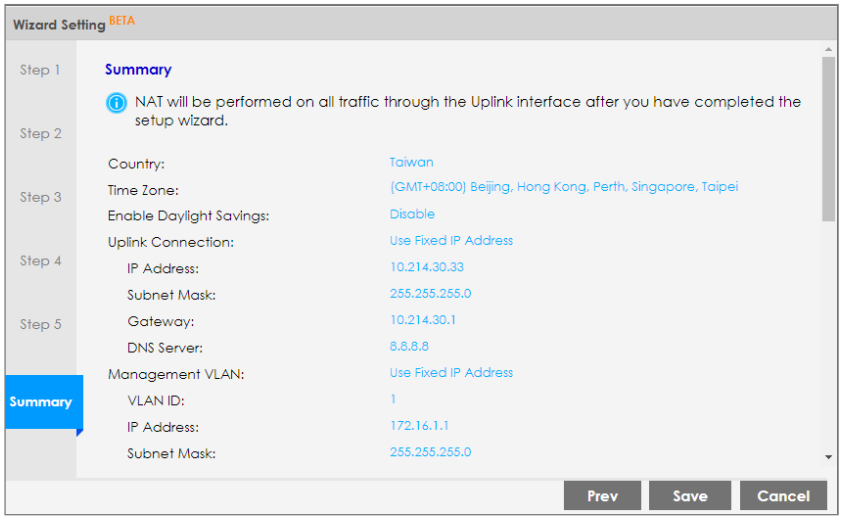
e. Click **Next**.



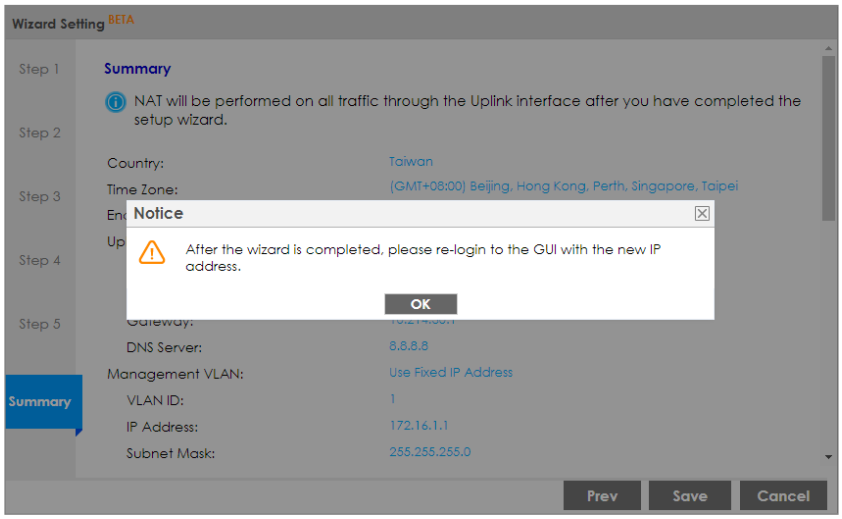
5 Modify the Radio setting for the AP. Adjust the **Output Power** for both of the channels, and **Channel Width** for 5GHz.



6 Get the Summary page and confirm if all of the configurations can match to the environment.
If yes, click **Save**.
If not, click **Prev** to modify the setting.



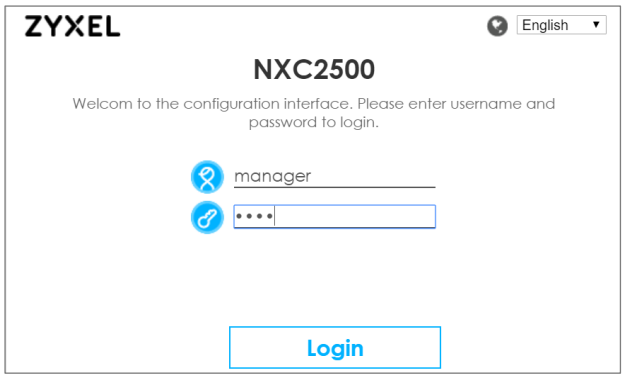
7 Here is the page after click **Save** from item 6.
Click **OK**. And **refresh** the browser to re-login.



2.1.2 Test the Result

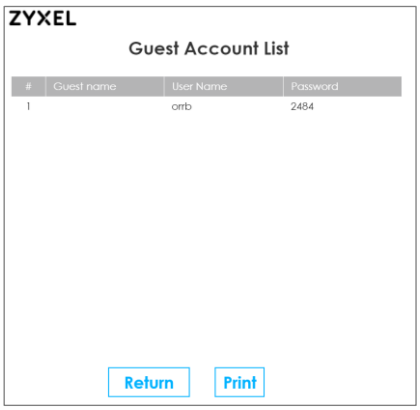
Connect NXC P1 to USG LAN, and NXC P2 to Switch. And connect AP to the Switch.

1 Login with guest-manager account.

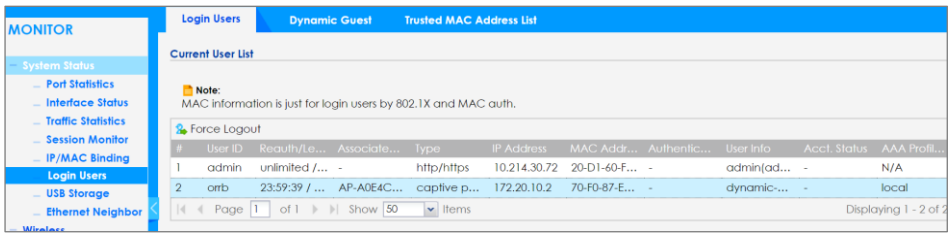


2 **Dynamic Guest User Group**: Wiz_Dynamic_Guest

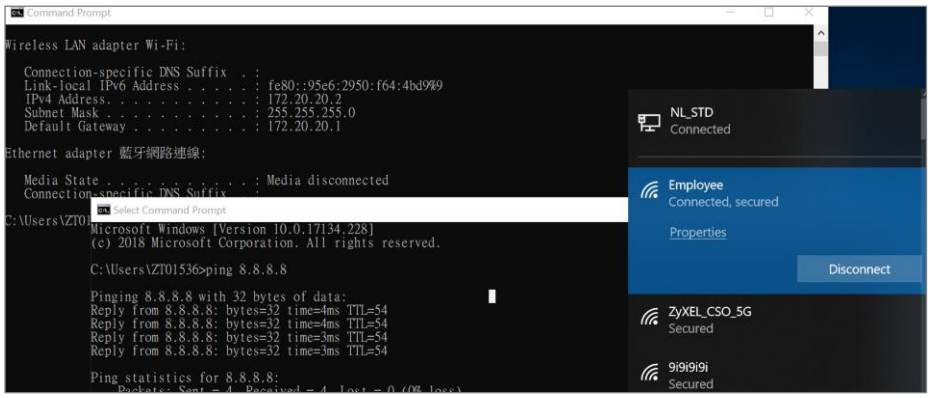
Click **Apply**.



3 User a station connect to the SSID "Guest" and login with the Guest account. Monitor the account via the Monitor > System Status > Login Users > Login Users.



4 Use a station to connect to the SSID “Employee”.



2.1.3 What Could Go Wrong?

1. The object which is created by the Wizard cannot be deleted via the web GUI. It must be modified via the Wizard setting again.
2. If there is VLAN ID for the management VLAN, remember to add VLAN on the switch.

2.2 How to Set WiFi Multiple SSID for Office Environment?

2.2.1 When USG is DHCP Server for VLAN10 and VLAN20

The example instructs how to configure VLANs and set different VLANs for different SSIDs in NXC. In this example, USG is the only DHCP server in the environment, and NXC only needs to set VLAN for passing traffic. In this example, we configure interfaces, set VLANs, create security and SSID profiles, and then configure AP profiles for managed APs.

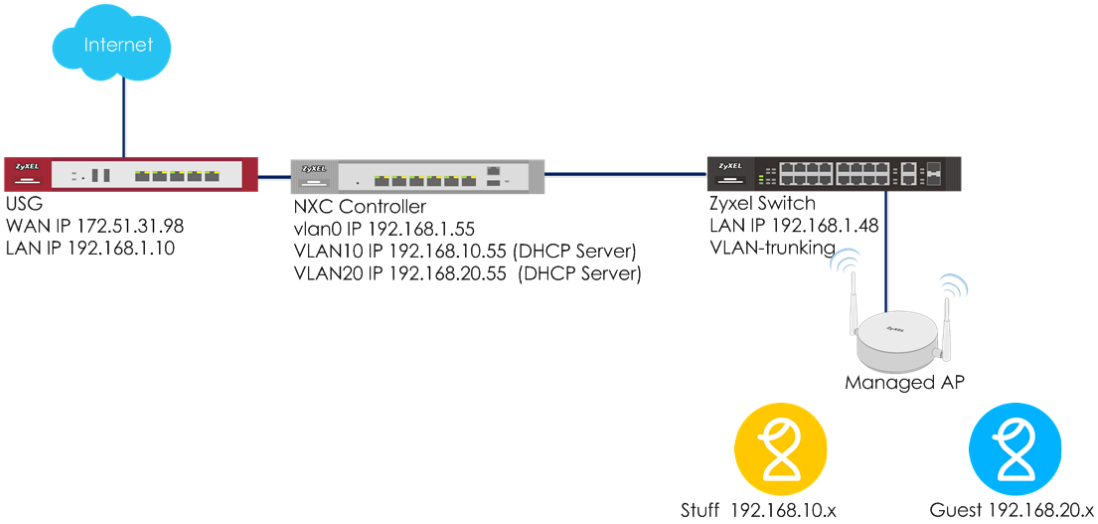


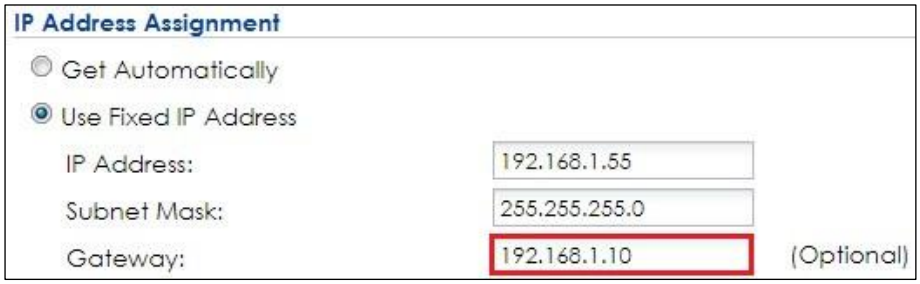
Figure 2.2.1 Set Different VLANs for Different SSIDs When USG is DHCP Server

Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC5500 (Firmware Version: 5.40), GS2210-8HP (Firmware Version: V4.30).

2.2.1.1 Configure NXC's Interface to Go to Internet

1 Connect NXC controller to USG LAN port. In the USG, all LAN ports are DHCP server for interface LAN, VLAN10, VLAN20, and all the stations connected to APs get an IP from the USG.

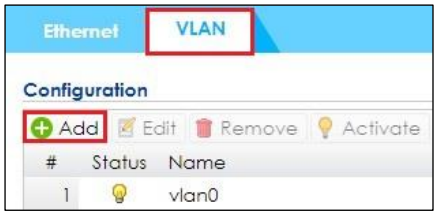
2 In the NXC, go to **CONFIGURATION > Network > Interface > VLAN** to set the NXC's IP address to be in the same subnet as the USG's LAN IP and have the USG act as the gateway. Double click **vlan0** to edit **IP Address Assignment** section. Click **OK**.



2.2.1.2 Configure VLAN

1 Connect Switch to NXC ge2 (P2), and connect all APs to the switch.

2 In the NXC, go to **CONFIGURATION > Network > Interface > VLAN**, Click **Add** to create a new VLAN (VLAN10).

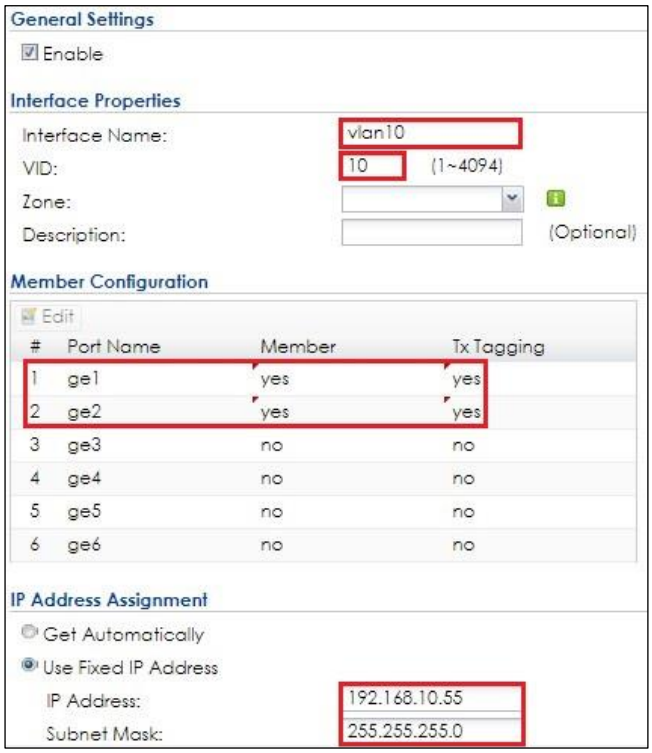


3 In General Settings, check **Enable**.

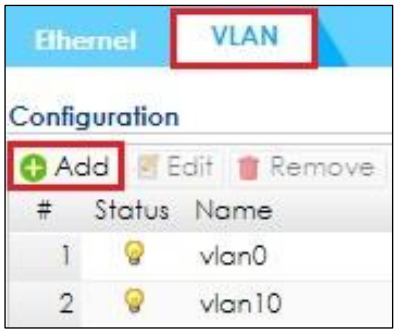
In Interface Properties, key in Interface Name: **vlan10**; set VID: **10**

In Member Configuration, set ge2 to be a **Member** and **Tx Tagging** to **yes**.

In IP Address Assignment, **Use Fixed IP Address** and key in **IP Address**, **Subnet Mask**. Click **OK**.



4 Click **Add** to create VLAN20 configuration in **CONFIGURATION > Network > Interface > VLAN**.

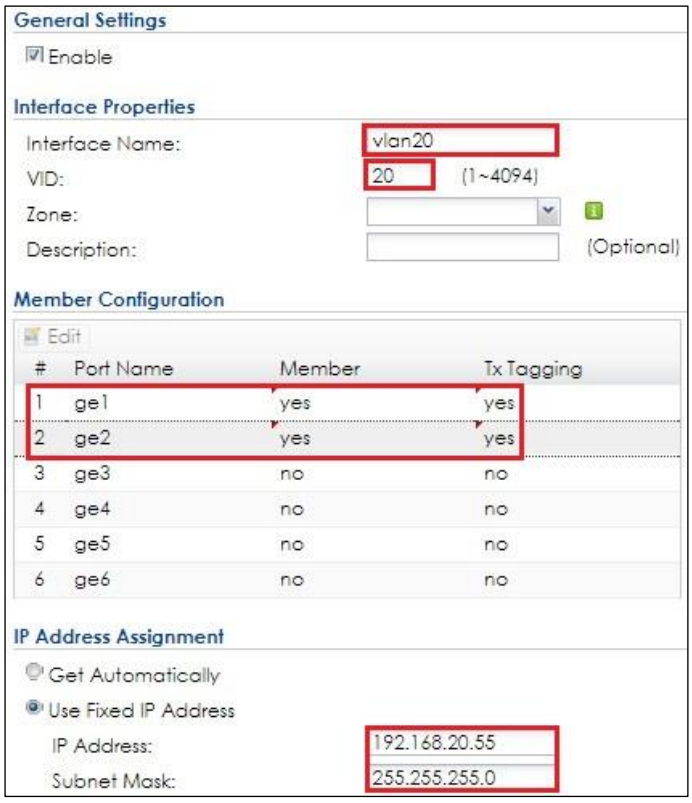


5 In General Settings, check **Enable**.

In Interface Properties, key in Interface Name: **vlan20**; set VID: **20**

In Member Configuration, set ge2 to be a **Member** and **Tx Tagging** to **yes**.

In IP Address Assignment, **Use Fixed IP Address** and key in **IP Address**, **Subnet Mask**. Click **OK**.



2.2.1.3 Configure Security and SSID

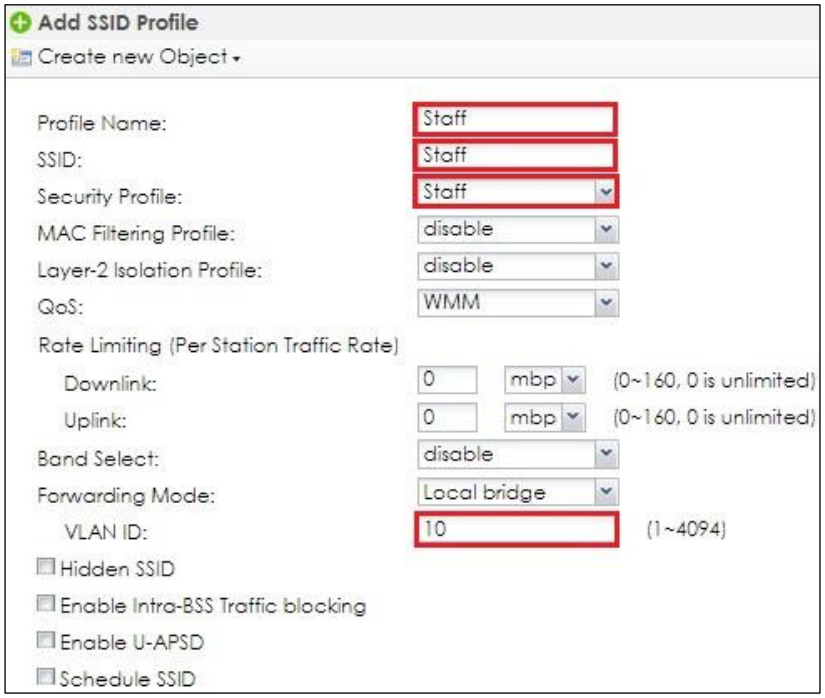
1 Go to **CONFIGURATION > Object > AP Profile > SSID > Security List**, Click **Add** to create a new security profile for staff.

In **General Settings**, key in **Staff** as profile name, and set security mode to **wpa2**.

In **Authentication Settings**, select to **PSK** and key in **Pre-shared Key**. Click **OK.**

2 Click **Add** to create a new security profile for guest.
In **General Settings**, key in **guest** as profile name, and set security mode to **none**. Click **OK**.

3 Go to **CONFIGURATION > Object > AP Profile > SSID > SSID List** and click **Add** to create a SSID for staff.
In **Profile Name** and **SSID**, key in **Staff**.
In **Security Profile**, select **Staff**.
In **VLAN ID**, key in **10**. Click **OK**.

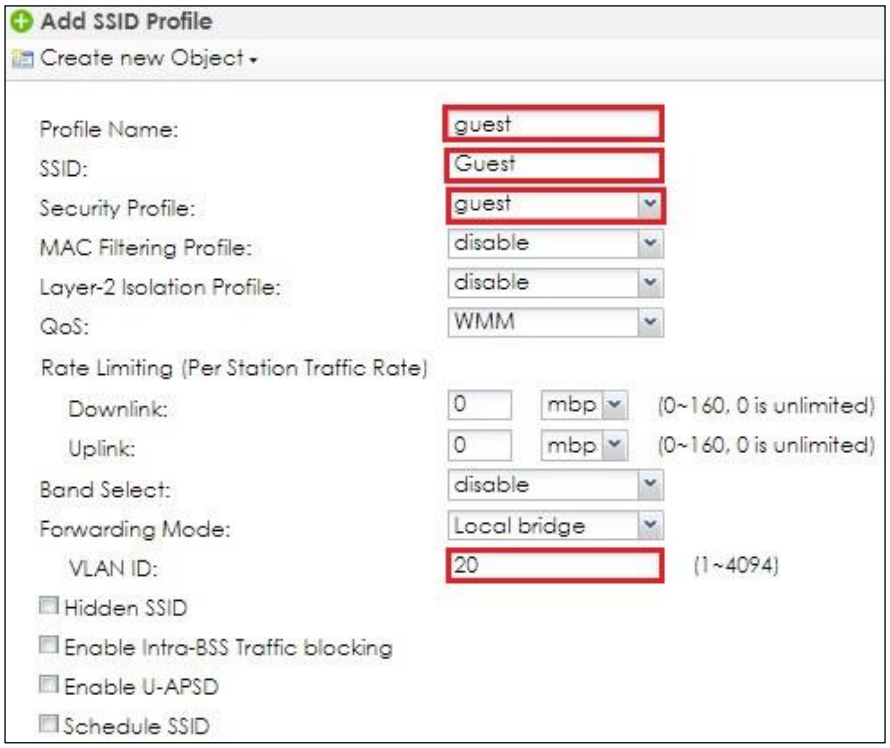


4 Click **Add** to create a SSID for guest in vlan20.

In **Profile Name** and **SSID**, key in **guest**.

In **Security Profile**, select **guest**.

In **VLAN ID**, key in **20**. Click **OK**.

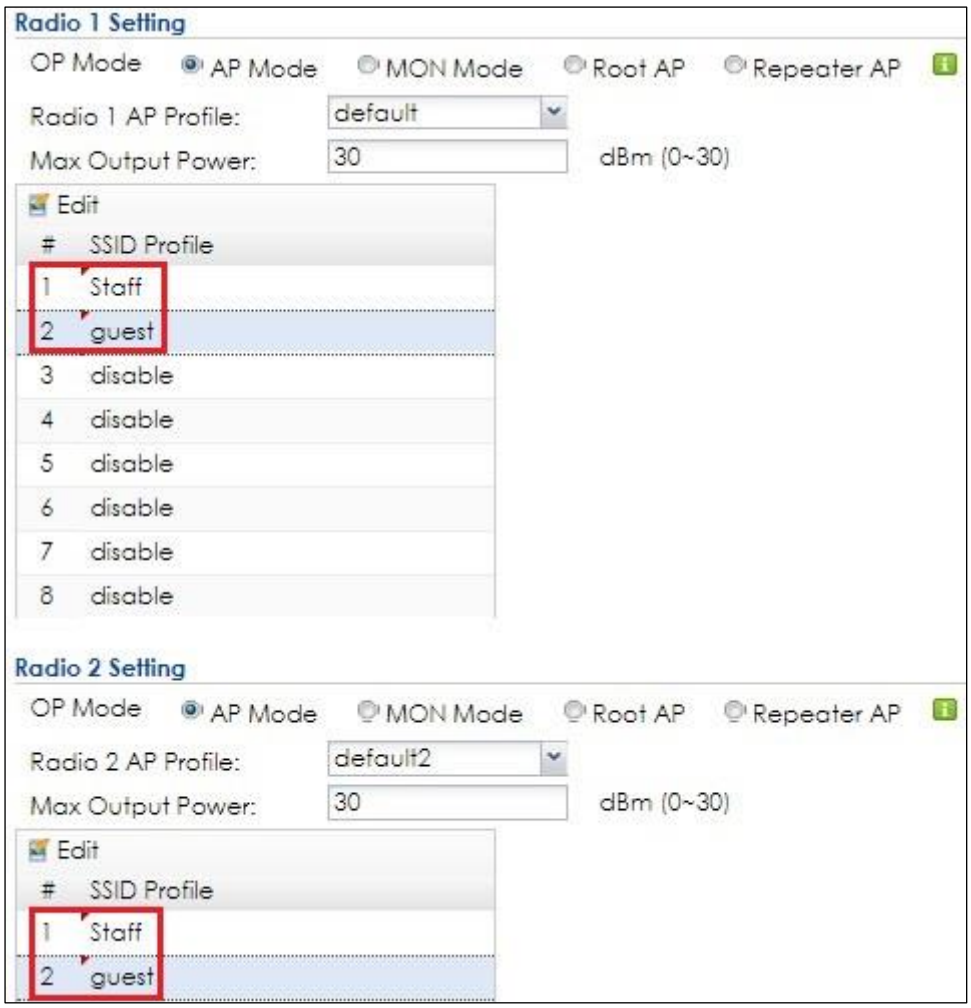


2.2.1.4 Configure AP Profile to Broadcast SSID

1 Go to **CONFIGURATION > Wireless > AP Management > AP Group**, click **Edit** for **default** group.

In Radio 1 and Radio 2, set the SSID profile, **Staff** and **guest**.

Click **OK** to apply the configuration.



2.2.2 When NXC is DHCP Server for VLAN10 and VLAN20

The example instructs how to configure VLANs and set different VLANs for different SSIDs in NXC when NXC is DHCP server for VLANs. The USG does not need to do any other settings when there are different VLANs add to the environment since NXC is a DHCP server for VLANs. In this example, we configure interfaces, set VLANs, create security and SSID profiles, and then configure AP profiles for managed APs.

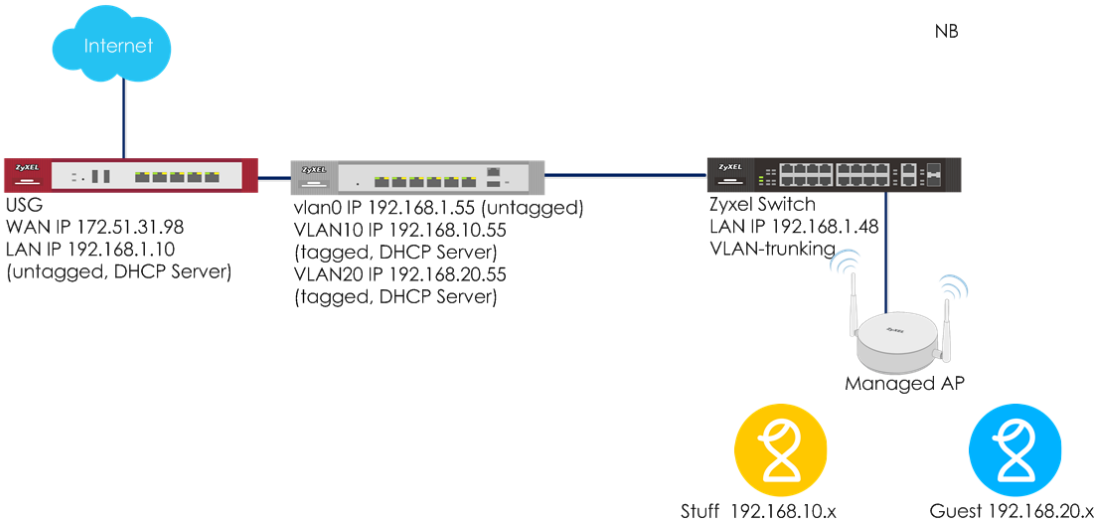


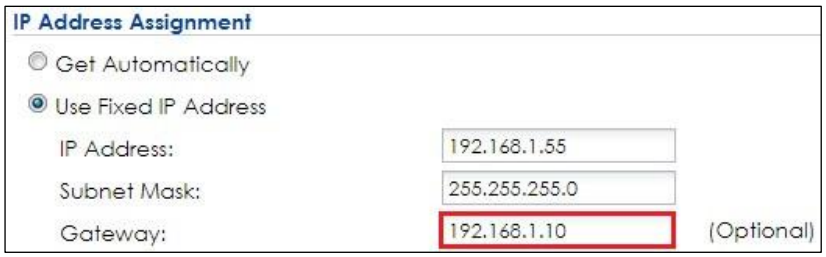
Figure 2.2.2 Set different VLANs for different SSIDs when NXC is DHCP server

Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC5500 (Firmware Version: 5.40), GS2210-8HP (Firmware Version: V4.30).

2.2.2.2 Configure Interface ge1 to Go to Internet

1 Connect ge1 (P1) to USG LAN port. In USG, LAN ports are DHCP server and all APs get IP from LAN.

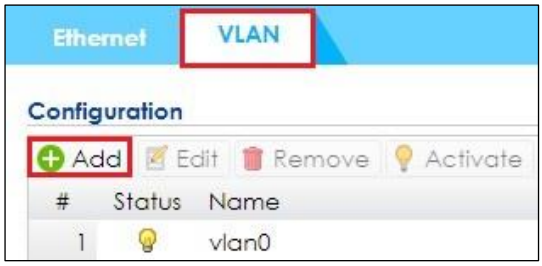
2 In the NXC, go to **CONFIGURATION > Network > Interface > VLAN** to set USG's LAN IP as the gateway. Double click **vlan0** to edit **IP Address Assignment** section. Click **OK**.



2.2.2.2 Configure VLAN

1 Connect Switch to NXC ge2, and connect all APs to the switch.

2 In the NXC, go to **CONFIGURATION > Network > Interface > VLAN**, Click **Add** to create a new VLAN.



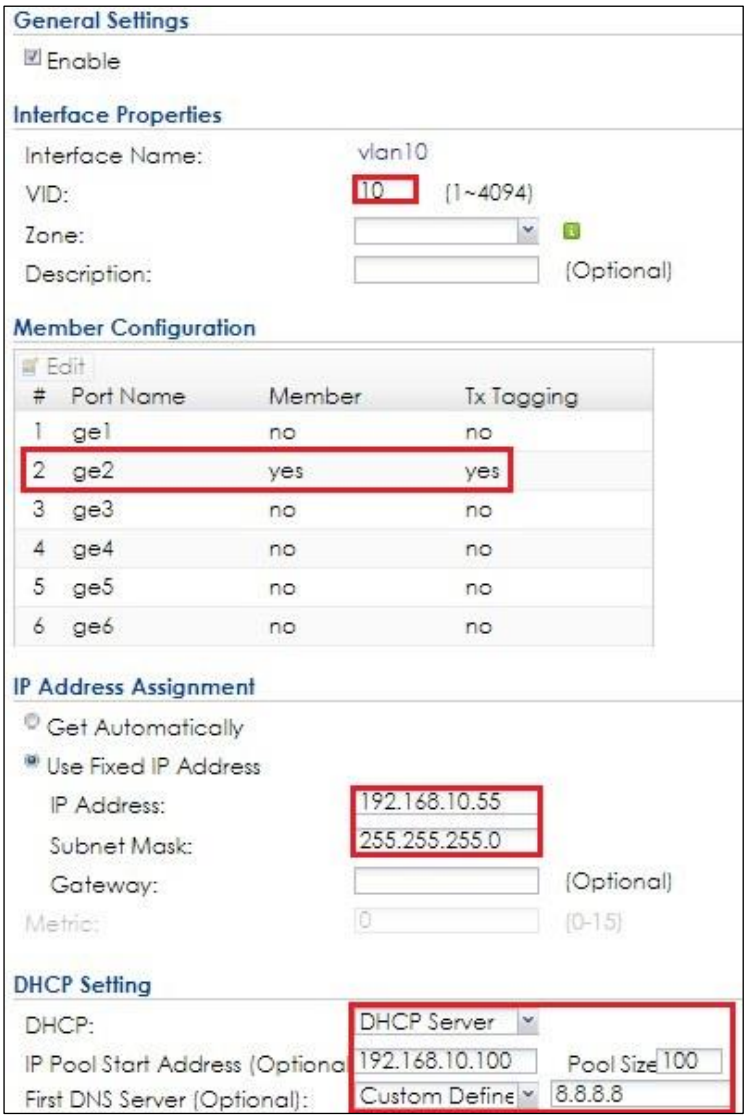
3 In General Settings, check **Enable**.

In Interface Properties, key in Interface Name: **vlan10**; VID: **10**

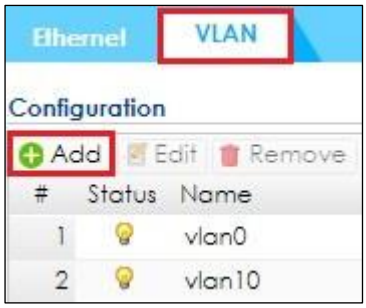
In Member Configuration, set ge2 to be a **Member** and **Tx Tagging**.

In IP Address Assignment, **Use Fixed IP Address** and key in **IP Address**, **Subnet Mask**, **and Gateway**.

In DHCP Setting, select **DHCP server** and key in **IP Pool Start Address** and **Pool Size**. **First DNS serve**r select to **Customer Defined 8.8.8.8**. The users on VLAN 10 get IP from this DHCP server. Click **OK**.



4 Click **Add** to create VLAN20 in **CONFIGURATION > Network > Interface > VLAN**.



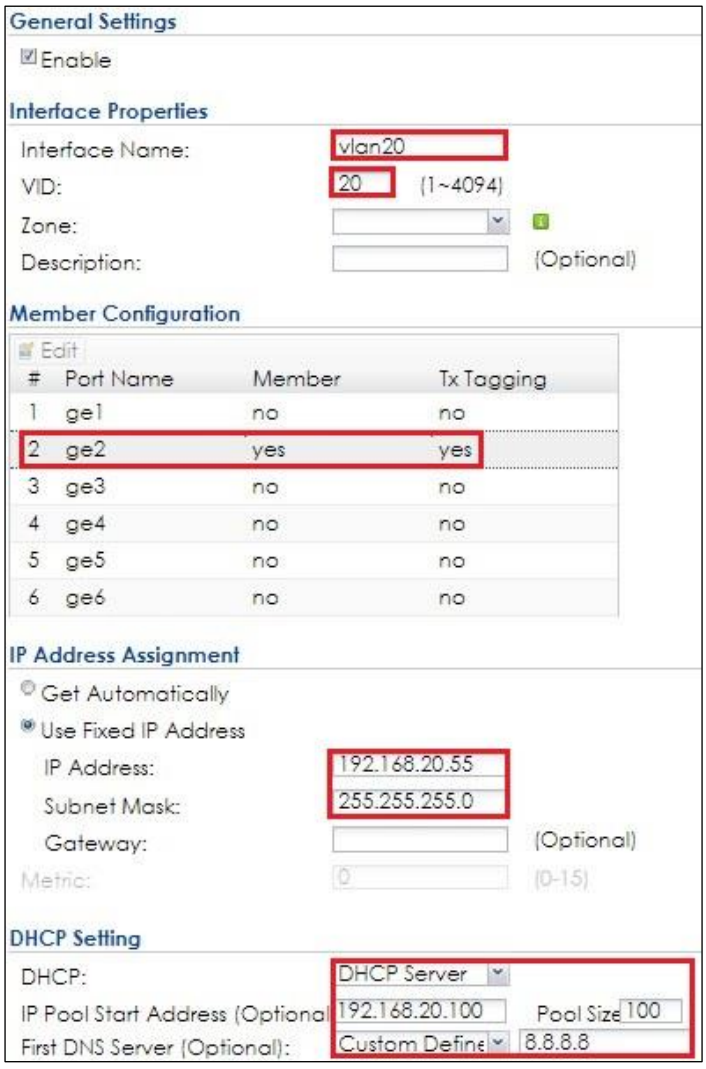
5 In General Settings, check **Enable**.

In Interface Properties, key in Interface Name: **vlan20**; VID: **20**

In Member Configuration, set ge2 are **Member** and **Tx Tagging**.

In IP Address Assignment, **Use Fixed IP Address** and key in **IP Address**, **Subnet Mask**, **and Gateway**.

In DHCP Setting, select **DHCP server** and key in **IP Pool Start Address** and **Pool Size**. **First DNS serve**r select to **Customer Defined 8.8.8.8**. The users on VLAN 20 get IP from this DHCP server. Click **OK**.



2.2.2.3 Set Policy Route

1 Set Policy Route in **CONFIGURATION > Network > Routing > Policy Route** to create new routing rule. Click **Show Advanced Settings**.

In **Configuration**, check **Enable**.

In **Criteria**, select **Incoming** as **Interface** and **Please select one member** is **vlan10**.

In Next-Hop, select **Type** as **Interface** and **Interface** is **vlan0**

In **Address Translation**, select **Source Network Address Translation** to **outgoing-interface** to use the IP address of the outgoing interface as the source IP address of the packet that matches this route. Click **OK**.

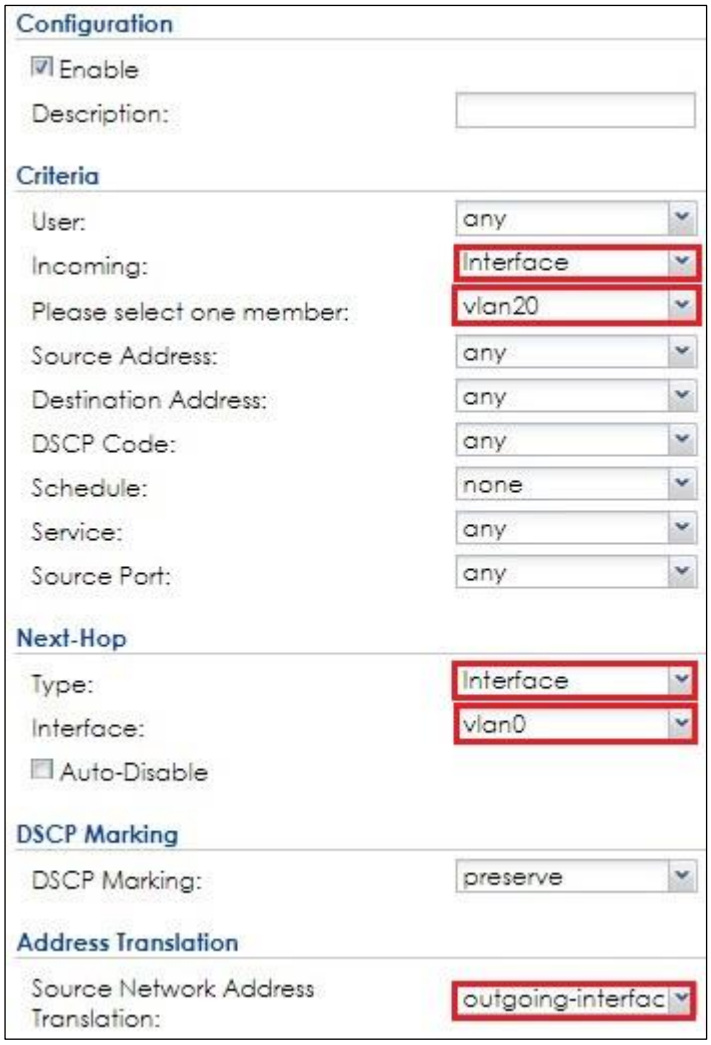
2 Set Policy Route in **CONFIGURATION > Network > Routing > Policy Route** to create new routing rule. Click **Show Advanced Settings**.

In **Configuration**, check **Enable**.

In **Criteria**, select **Incoming** as **Interface** and **Please select one member** is **vlan20**.

In Next-Hop, select **Type** as **Interface** and **Interface** is **vlan0**

In **Address Translation**, select **Source Network Address Translation** to **outgoing-interface** to use the IP address of the outgoing interface as the source IP address of the packet that matches this route. Click **OK**.



2.2.2.4 Configure Security and SSID

1 Go to **CONFIGURATION > Object > AP Profile > SSID > Security List**, Click **Add** to create a new security profile for staff.

In **General Settings**, key in **Staff** as profile name, and set security mode to **wpa2**.

In **Authentication Settings**, select to **PSK** and key in **Pre-shared Key**. Click **OK.**

2 Click **Add** to create a new security profile for guest.

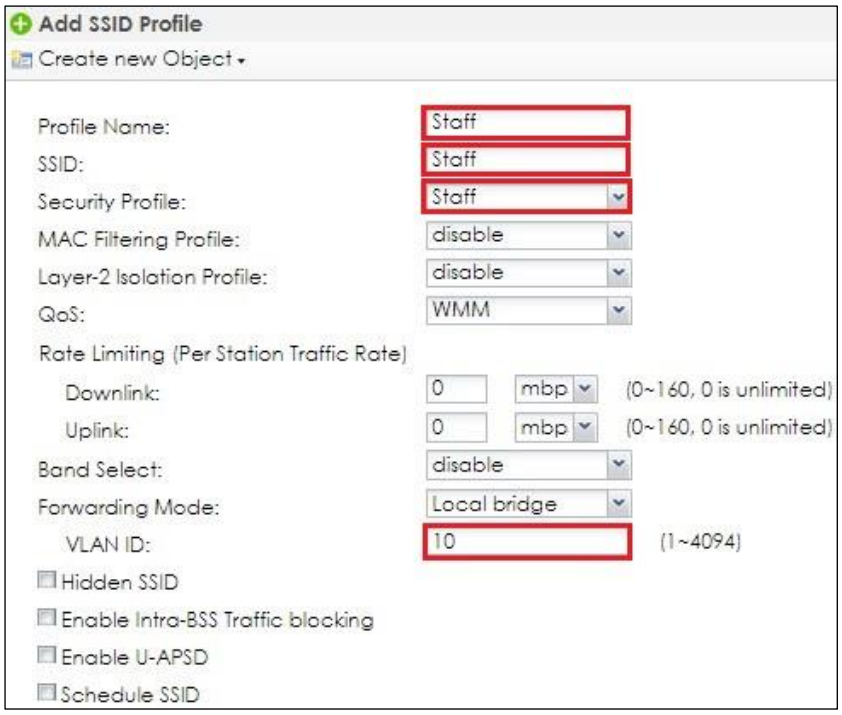
In **General Settings**, key in **guest** as profile name, and set security mode to **none**. Click **OK**.

3 Go to **CONFIGURATION > Object > AP Profile > SSID > SSID List** and click Add to create a SSID for staff.

In **Profile Name** and **SSID**, key in Staff.

In **Security Profile**, select Staff.

In **VLAN ID**, key in 10. Click **OK**.

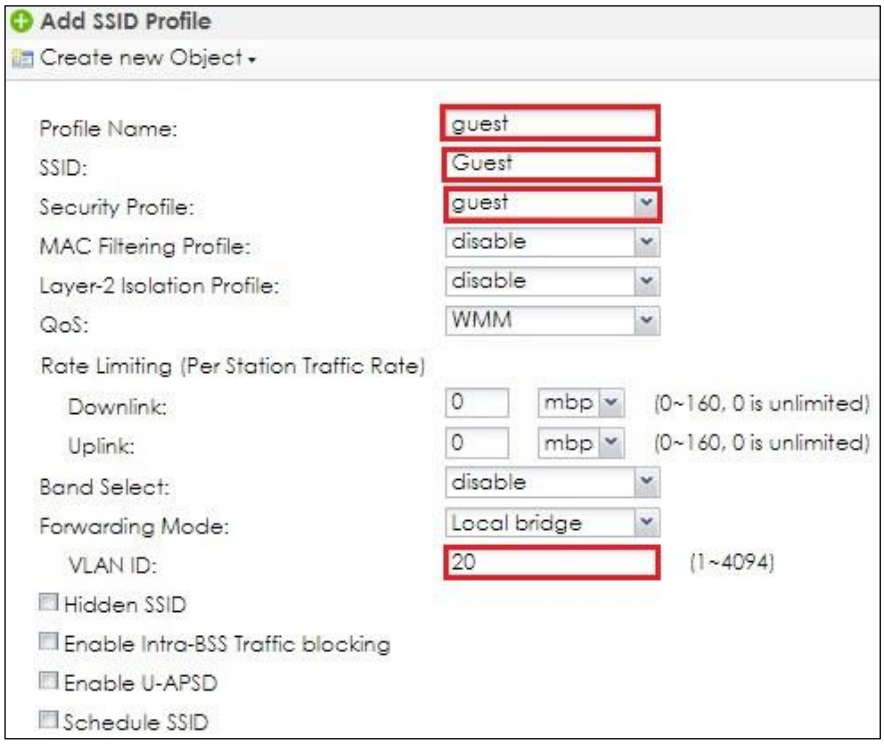


4 Click **Add** to create a SSID for guest in vlan20.

In **Profile Name** and **SSID**, key in **guest**.

In **Security Profile**, select **guest**.

In **VLAN ID**, key in **20**. Click **OK**.

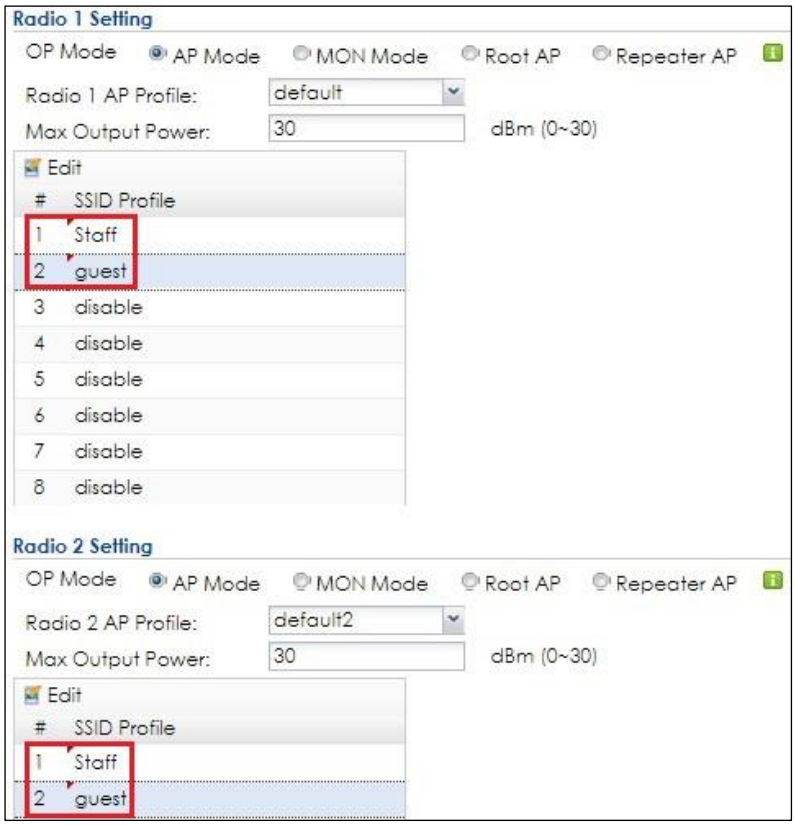


2.2.2.5 Configure AP Profile to Broadcast SSID

1 Go to **CONFIGURATION > Wireless > AP Management > AP Group**, click **Edit** for **default** group.

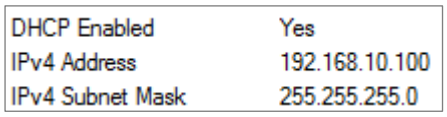
In Radio 1 and Radio 2, set the SSID profile, **Staff** and **guest**.

Click **OK** to apply the configuration.

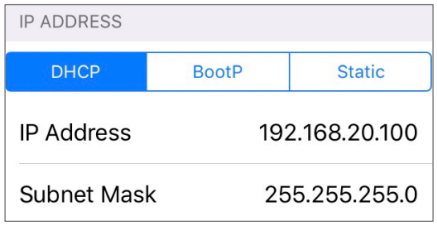


2.2.3 Test the Result

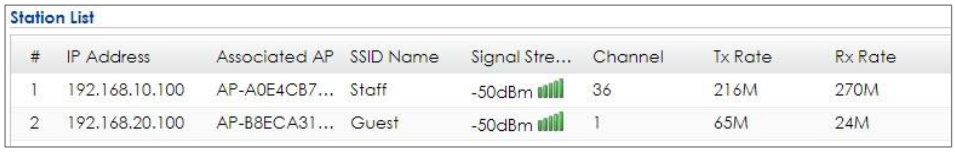
1 Use a laptop to select SSID Staff and key in the security setting for connection. After connection successful, laptop can get an IP in VLAN10.



2 Use a mobile phone to select SSID guest and connect to it. After connection is successful, mobile phone can get an IP in VLAN20.



3 The connected stations are visible in NXC controller **MONITOR > Station Info > Station List**.



2.2.4 What Could Go Wrong?

1. When USG is a DHCP server, users may not get IP if USG and switch do not set VLAN10 and VLAN20.
2. When NXC is a DHCP server, user may not go to Internet if the policy route does not set to outgoing-interface.
3. For the broadcasting the radio, the example only sets radio1 for 2.4GHz. If 5GHz also needs to broadcast the same setting, you can set in radio2 with the same operation steps.

2.3 How to Set up Fail Over/Fall Back?

The example instructs how to set up fail over and fall back. All management APs connect to NXC controller 1 in this example. When the NXC controller 1 fails to connect, all managed APs are controlled by NXC controller 2 by fail over setting. Once NXC controller 1 works again, the APs are back to NXC controller 1 via fall back setting.

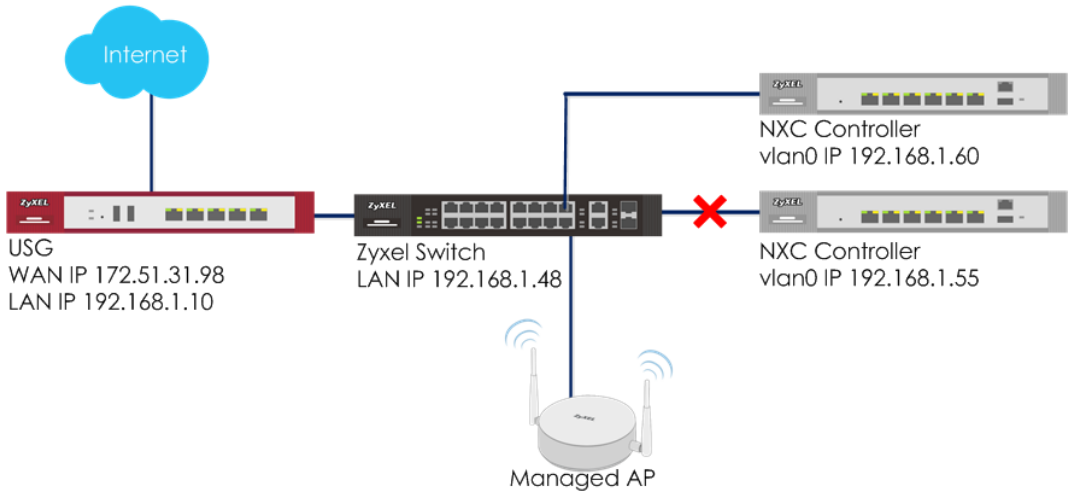
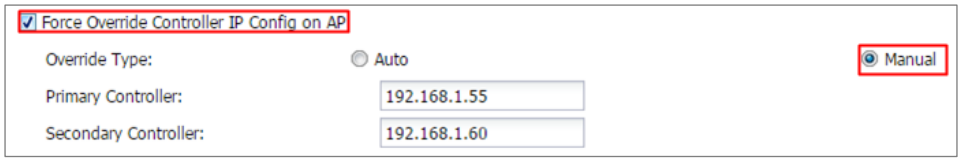


Figure 2.3 Fail Over and Fall Back

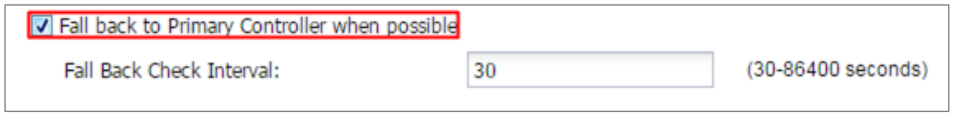
Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC2500 (Firmware Version: 5.40), GS2210-8HP (Firmware Version: V4.30).

2.3.1 Configure Fail Over and Fall Back

1 To set the fail over in **CONFIGURATION > Wireless > AP Management > AP Policy**, enable **Force Override Controller IP Config on AP**. Select **Manual** and set the **Primary Controller**: 192.168.1.55 and **Secondary Controller**: 192.168.1.60

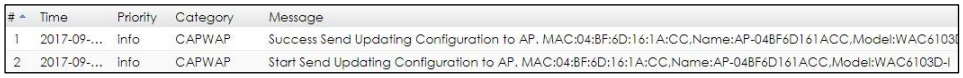


2 To set the fall back in **CONFIGURATION > Wireless > AP Management > AP Policy**, enable **Fall back to Primary Controller when possible**. When the **Fall Back Check Interval** is set to 30 seconds and the APs have transferred to the secondary controller because of the primary one fails to connect, the APs check whether the primary controller works every 30 seconds and change back to associate with the primary one as soon as it's available.



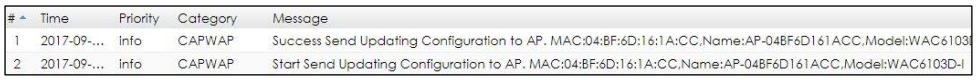
2.3.2 Test the Result

1 In **MONITOR > Log**, check whether the NXC controller 1 sets the configuration for the AP(s). Logs show the messages after the configuration is applied to in the AP.



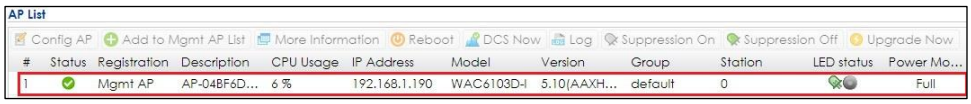
#	Time	Priority	Category	Message
1	2017-09-...	info	CAPWAP	Success Send Updating Configuration to AP. MAC:04:BF:6D:16:1A:CC,Name:AP-04BF6D161ACC,Model:WAC6103
2	2017-09-...	info	CAPWAP	Start Send Updating Configuration to AP. MAC:04:BF:6D:16:1A:CC,Name:AP-04BF6D161ACC,Model:WAC6103D-I

2 Disconnect the NXC controller 1 from switch, and the managed APs go to find NXC controller 2 and get controlled by it. In NXC controller 2, when the AP is controlled by the 2nd NXC, the 2nd NXC also sends configuration to the AP and shows in log.



#	Time	Priority	Category	Message
1	2017-09-...	info	CAPWAP	Success Send Updating Configuration to AP. MAC:04:BF:6D:16:1A:CC,Name:AP-04BF6D161ACC,Model:WAC6103
2	2017-09-...	info	CAPWAP	Start Send Updating Configuration to AP. MAC:04:BF:6D:16:1A:CC,Name:AP-04BF6D161ACC,Model:WAC6103D-I

3 In NXC controller 2, the AP also shows in **MONITOR > Wireless > AP Information > AP List**.

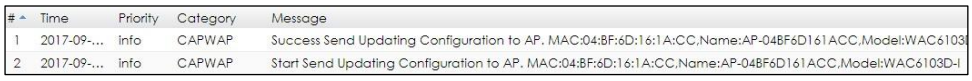


AP List

Config AP | Add to Mgmt AP List | More Information | Reboot | DCS Now | Log | Suppression On | Suppression Off | Upgrade Now

#	Status	Registration	Description	CPU Usage	IP Address	Model	Version	Group	Station	LED status	Power Mo...
1		Mgmt AP	AP-04BF6D...	6 %	192.168.1.190	WAC6103D-I	5.10(AAXH...	default	0		Full

4 When NXC controller 1 links up again, the AP is controlled by NXC controller 1 again after 30 seconds.



#	Time	Priority	Category	Message
1	2017-09-...	info	CAPWAP	Success Send Updating Configuration to AP. MAC:04:BF:6D:16:1A:CC,Name:AP-04BF6D161ACC,Model:WAC6103
2	2017-09-...	info	CAPWAP	Start Send Updating Configuration to AP. MAC:04:BF:6D:16:1A:CC,Name:AP-04BF6D161ACC,Model:WAC6103D-I

2.3.3 What Could Go Wrong?

1. The controllers need to have the same configurations/profiles and firmware, or the AP changes the setting/firmware after doing fail over.
2. If NXC controllers 1 and 2 control different APs, after the APs policy settings are applied, clear the Force Override option on controller 2 via unchecking the **Force Override Controller IP Config on AP** to avoid overriding the setting of APs from NXC controller 1.

2.4 How to Set up Mesh to Extend Wireless Coverage?

The example instructs how to set up ZyMesh. When AP's signal needs to extend, use ZyMesh to set up connection between root AP and repeater AP. Because ZyMesh profile makes the WDS connection, the root AP and repeater AP don't need to use the same SSID for users connecting.

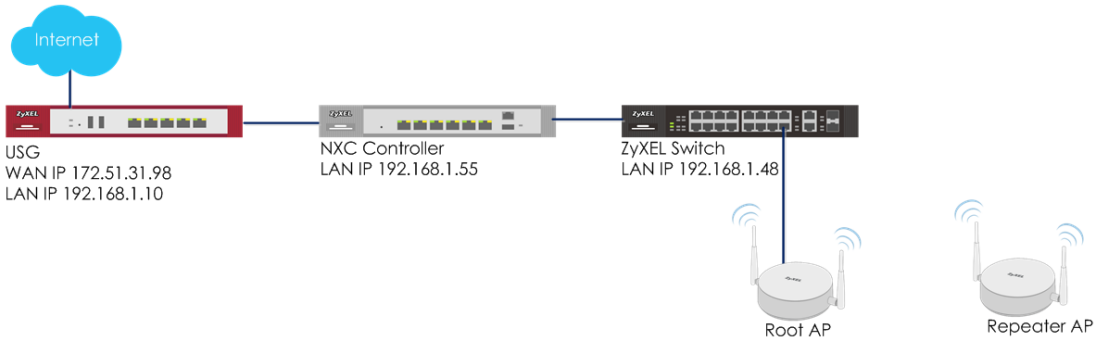


Figure 2.4 Setup ZyMesh for Root AP and Repeater AP

Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC5500 (Firmware Version: 5.40), GS2210-8HP (Firmware Version: V4.30).

2.4.1 Configure ZyMesh Profile

1 Both root AP and repeater AP need to use the same ZyMesh profile to set up connection.

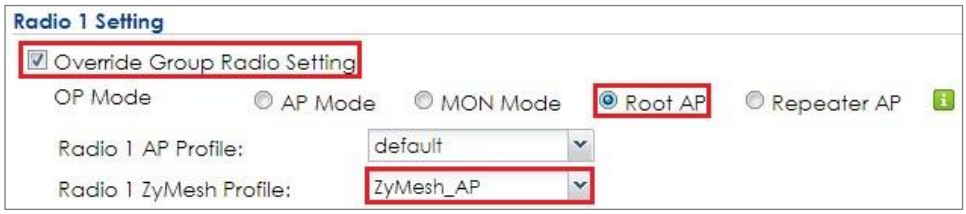
Go to **CONFIGURATION > Object > ZyMesh Profile**, Click **Add** to create a ZyMesh SSID and pre-shared key. The ZyMesh SSID hides and it is not visible.

In **General Settings**, set **Profile Name**, **ZyMesh SSID**, and **Pre-Shared Key**. Click **OK**.

2.4.2 Configure Root AP and Repeater AP

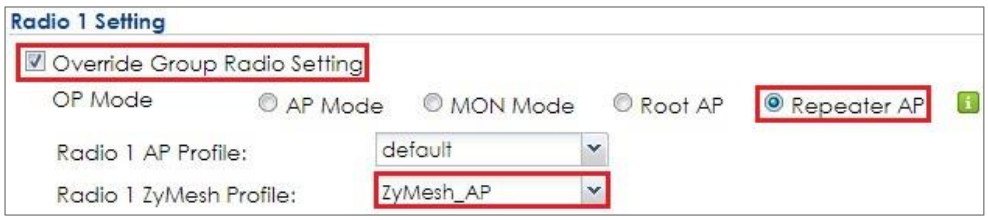
1 In the same AP, radio 2 is not able to work as the repeater when radio 1 is root AP. Select an AP in **CONFIGURATION > Wireless > AP Management > Mgnt. AP List** to edit the selected AP as root AP.

In Radio 1 Setting, check **Override Group Radio Setting**. Select **Root AP** and **ZyMesh_AP** as the Radio 1 ZyMesh Profile. Click **OK**.



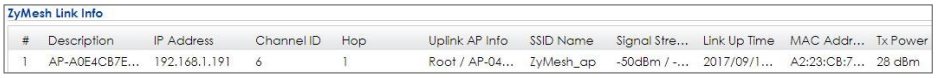
2 Select an AP in the Mngt. AP List and configure the AP as repeater in **CONFIGURATION > Wireless > AP Management > Mgnt. AP List**.

In Radio 1 Setting, check **Override Group Radio Setting**. Select **Repeater AP** and **ZyMesh_AP** as the Radio 1 ZyMesh Profile. Click **OK**.



2.4.3 Test the Result

1 Check ZyMesh Link Info in **MONITOR > Wireless > ZyMesh > ZyMesh Link Info**. When the ZyMesh sets up successfully, root AP and repeater AP information shows in the ZyMesh link info.

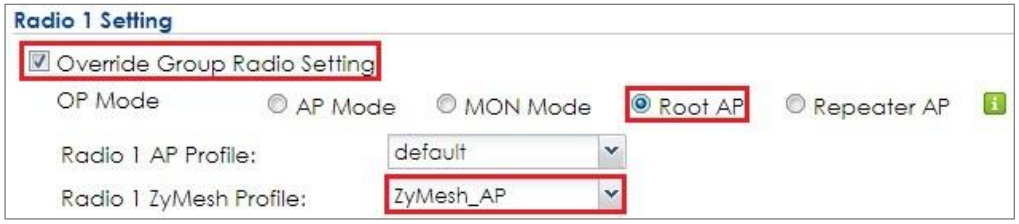


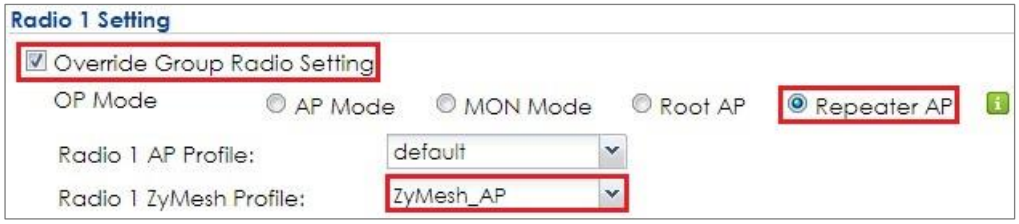
ZyMesh Link Info

#	Description	IP Address	Channel ID	Hop	Uplink AP Info	SSID Name	Signal Stre...	Link Up Time	MAC Addr...	Tx Power
1	AP-A0E4CB7E...	192.168.1.191	6	1	Root / AP-04...	ZyMesh_ap	-50dBm / -...	2017/09/1...	A2:23:CB:7...	28 dBm

2.4.4 What Could Go Wrong?

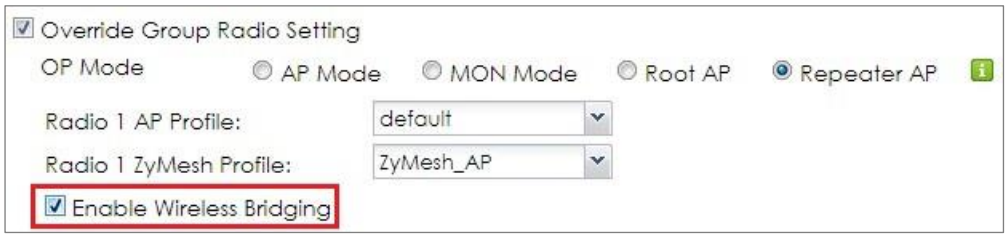
1 If the ZyMesh profiles are not the same on root AP and repeater AP, it's not able to connect using ZyMesh successfully. Go to **CONFIGURATION > Wireless > AP Management > Mgnt. AP List** to make sure root AP and repeater AP's ZyMesh profile are the same.





2 When ZyMesh set up, the repeater AP's throughput is lower due to path loss.

3 When ZyMesh set up, the repeater AP's uplink port is down to avoid loop. It is able to bridge via uplink port by checking **Enable Wireless Bridging** in repeater AP's setting. The repeater AP can still transmit data through its Ethernet port.



4 The APs' country code must be the same for setting up ZyMesh connection. You can check the country code in **CONFIGURATION > Wireless > Controller**

5 DCS on root and repeater AP will cause the ZyMesh disconnected when the AP change to the other change. So, please disable DCS or set longer time for doing DCS when building up a ZyMesh deployment.

2.5 How to Set up Seamless Wireless Roaming?

The example instructs how to configure two APs profile and topology for roaming. These two APs need to use the same SSID, security, DHCP server, and signal overlap. The two APs have the same DHCP server from USG, and this example shows how to configure APs in the same SSID and security.

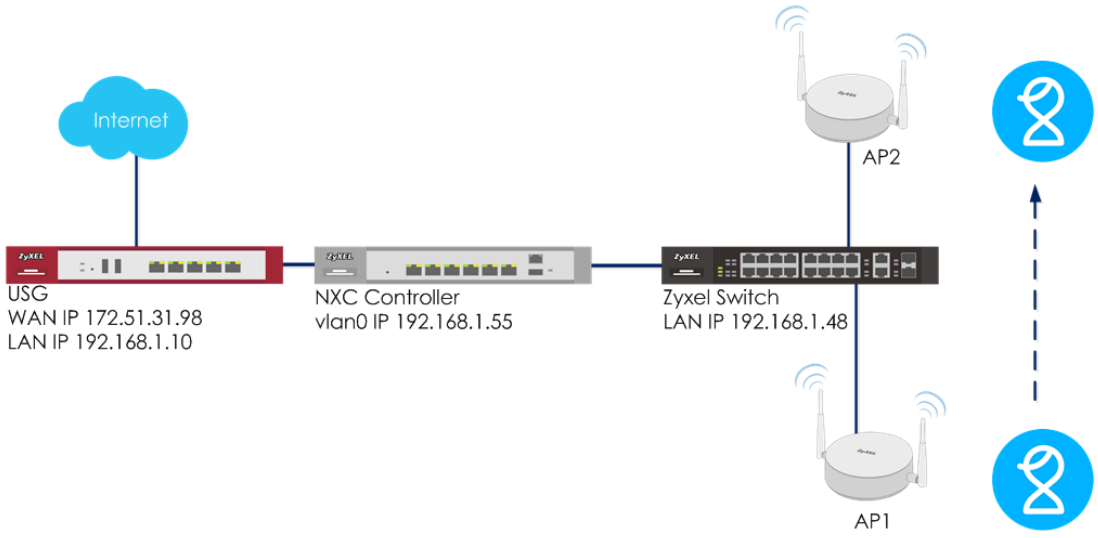


Figure 2.5 Roaming from AP1 to AP2

Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC5500 (Firmware Version: 5.40), GS2210-8HP (Firmware Version: V4.30).

2.5.1 Configure APs via AP Group

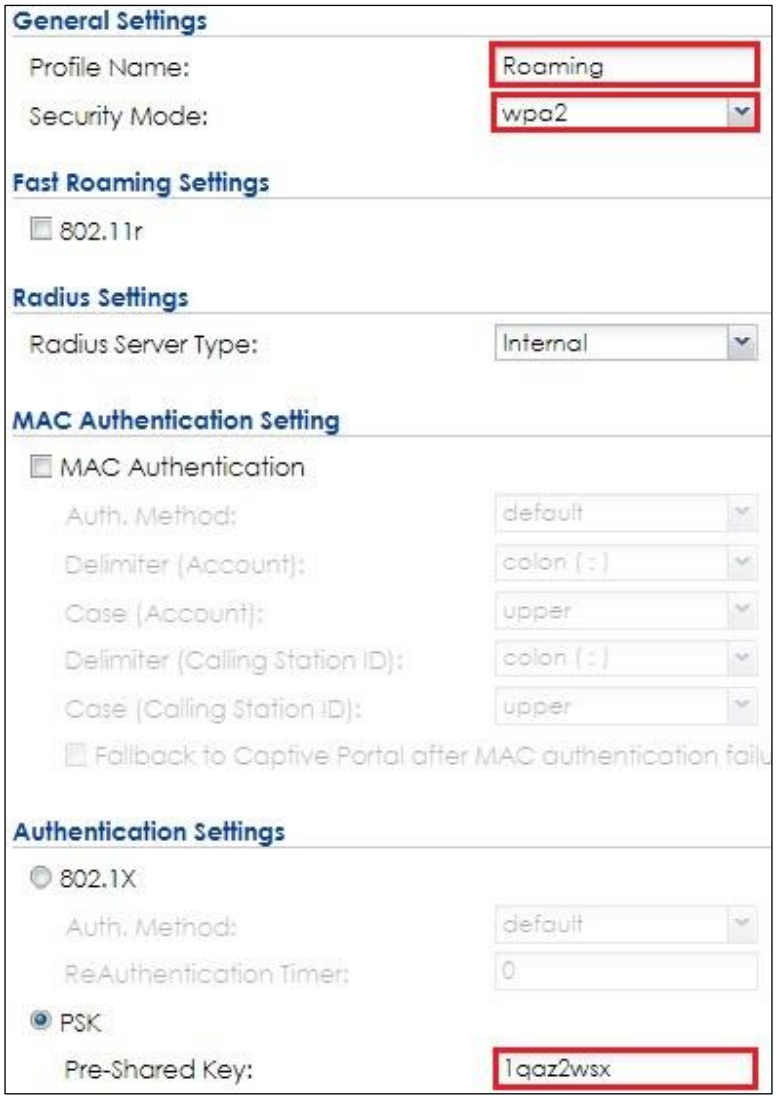
1 Roaming needs to use the same SSID and security. AP group can assign APs' configuration, so that APs have the same SSID and security.

Create a new security profile for roaming.

Go to **CONFIGURATION > Object > AP Profile > SSID > Security List**, Click **Add**.

In **General Settings**, key in **Roaming** as profile name, and set security mode to **wpa2**.

In **Authentication Settings**, select to **PSK** and key in **Pre-shared Key**. Click **OK**



2 Create a new SSID for roaming.

In **Profile Name** and **SSID**, key in **Roaming**.

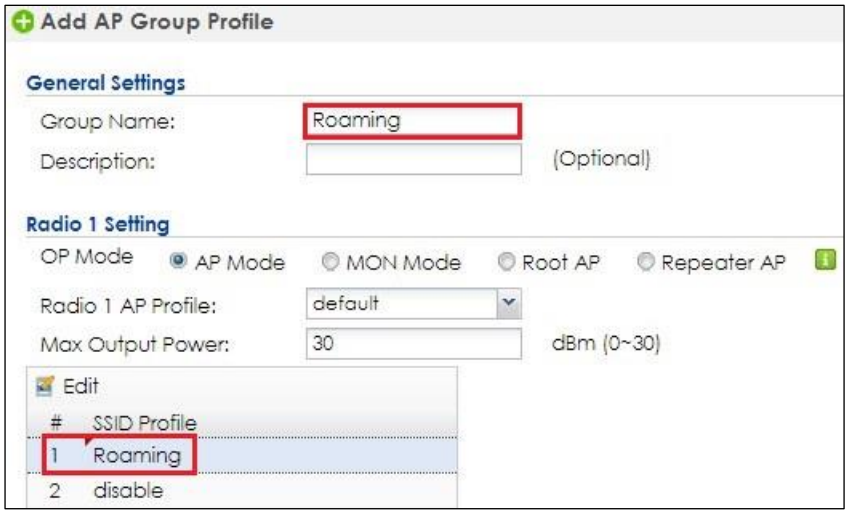
In **Security Profile**, select **Roaming.** Click **OK**

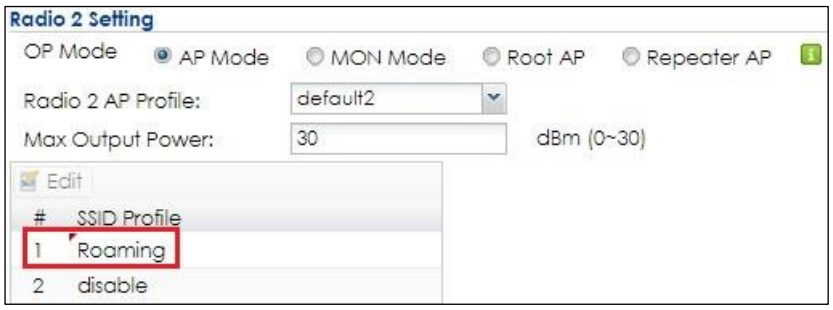
3 Create a new AP group for roaming, and select AP1 and AP2 as member of the AP group.

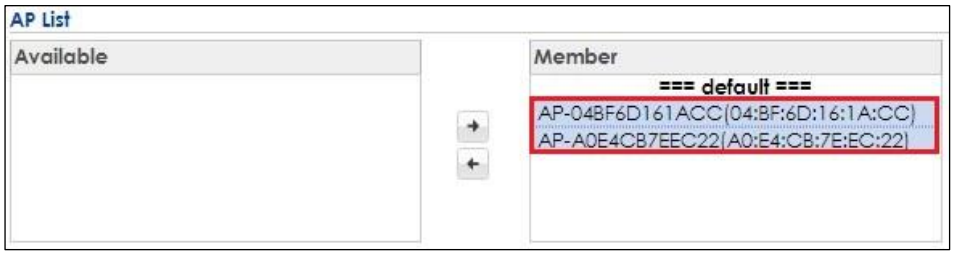
In **Profile Name**, key in **Roaming**.

In **Radio1 Setting and Radio 2 Setting**, change SSID profile to **Roaming.**

In **AP List**, move two APs from **Available** to **Member**. Click **OK**.

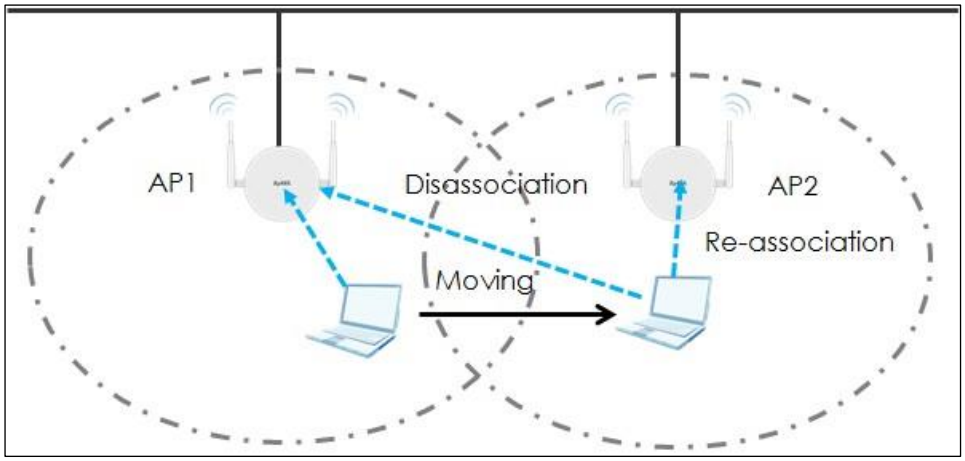






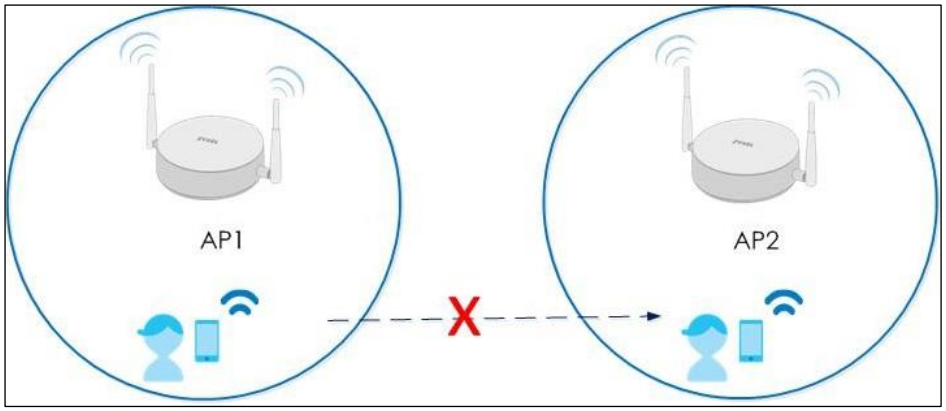
2.5.2 Test the Result

1. User connects to the SSID and make sure the user can access the Internet without any problem.
2. When user is roaming from AP1 to AP2, the connection is not interrupted because of reconnection from AP1 to AP2.

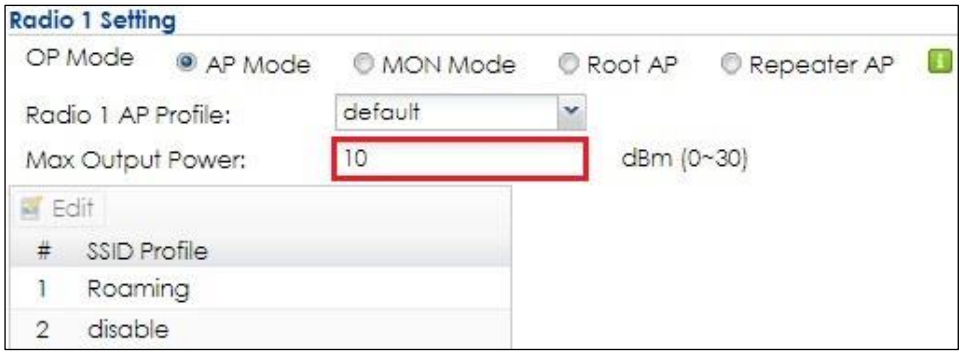


2.5.3 What Could Go Wrong?

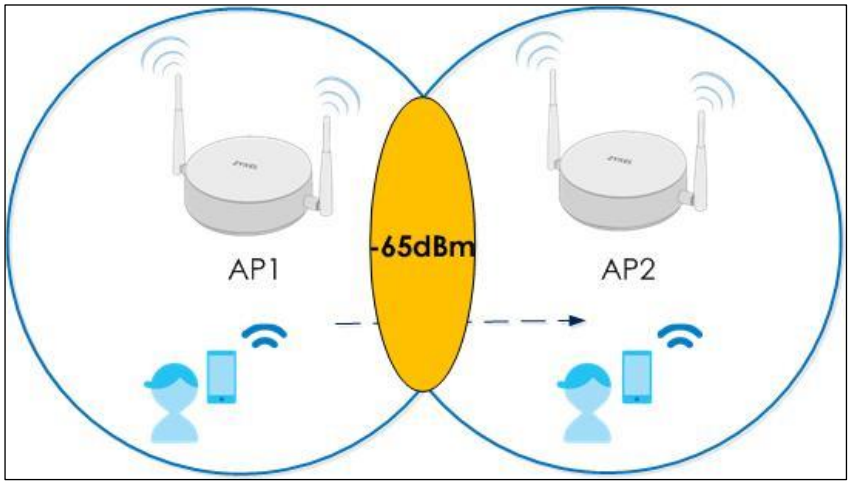
1 User may disconnect when AP1 and AP2's signal is not overlapping. If the Max out power is 30 and two APs still don't overlap, please move these two APs closer to make signal overlap.

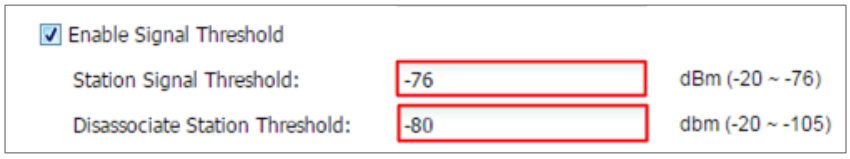


2 When AP1 and AP2 overlapping is too large, the AP1 and AP2's signal are interference to each other. Here are two ways for solving this issue. One is to make these two APs more far away from each other; the other is to decrease Max output power.



3 Enable threshold in radio might cause disconnection between AP and station. When the overlap area RSSI is lower than threshold value, station is not able to connect to AP. The **Station Signal Threshold** and **Disassociation Station Threshold** should be lower than the overlapping area's RSSI.





4 "Band Select" may potentially cause interruptions for time-sensitive applications because of roaming delays. So, it's suggested disabling band select.

5 The connection might not be stable if the "Load Balance" is enabled and the maximum station number is reached. The roaming station may connect to the AP and disconnect soon.

6 It's up to station to roam or not. The roaming tendency is able to modify in computer's setting.

2.6 How to implement Wireless VoIP Best Practice (VoWiFi)?

This guide provides several recommendations to optimize the quality of VoIP and mitigate the latency when mobile devices roaming between APs. For the roaming, the two APs have the same DHCP server from USG, and this example shows how to configure APs in the same SSID, security and enable important features.

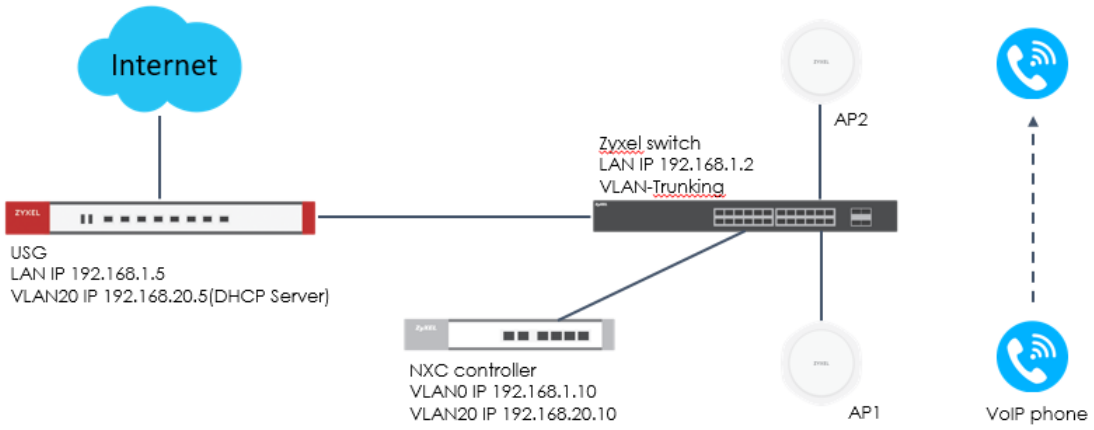


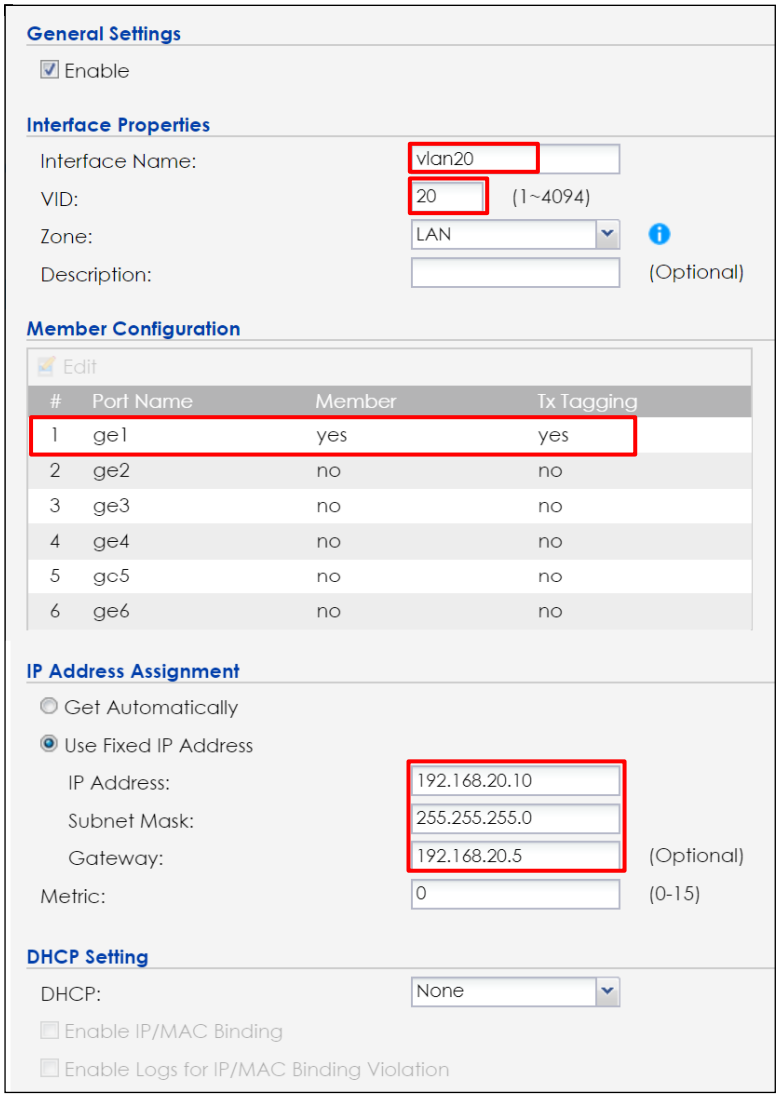
Figure 2.6 VoIP phone roaming from AP1 to AP2

Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.33), NXC5500 (Firmware Version: 5.40), GS2210-8HP (Firmware Version: V4.50).

2.6.1 Configure Interface

1. The USG have a VLAN20 DHCP pool only for Voice phones. Connect Switch to NXC ge1 (P1), and connect all APs to the switch. The switch ports connect all the devices must have in the VLAN 20 with Tx Tagging.
2. In the NXC, go to **CONFIGURATION > Network > Interface > VLAN**, Click **Add** to create a new VLAN (VLAN20).

3 In **General Settings**, check **Enable**. In Interface Properties, key in **Interface Name**, key in **vlan20**; set **VID** with **20.**
In **Member Configuration**, set ge1 to be a **Member** and **Tx Tagging** to **yes**.
In **IP Address Assignment-Use Fixed IP Address** and key in **IP Address, Subnet Mask**. Click **OK**.



2.6.2 Configure AP profile with Security, SSID and radio

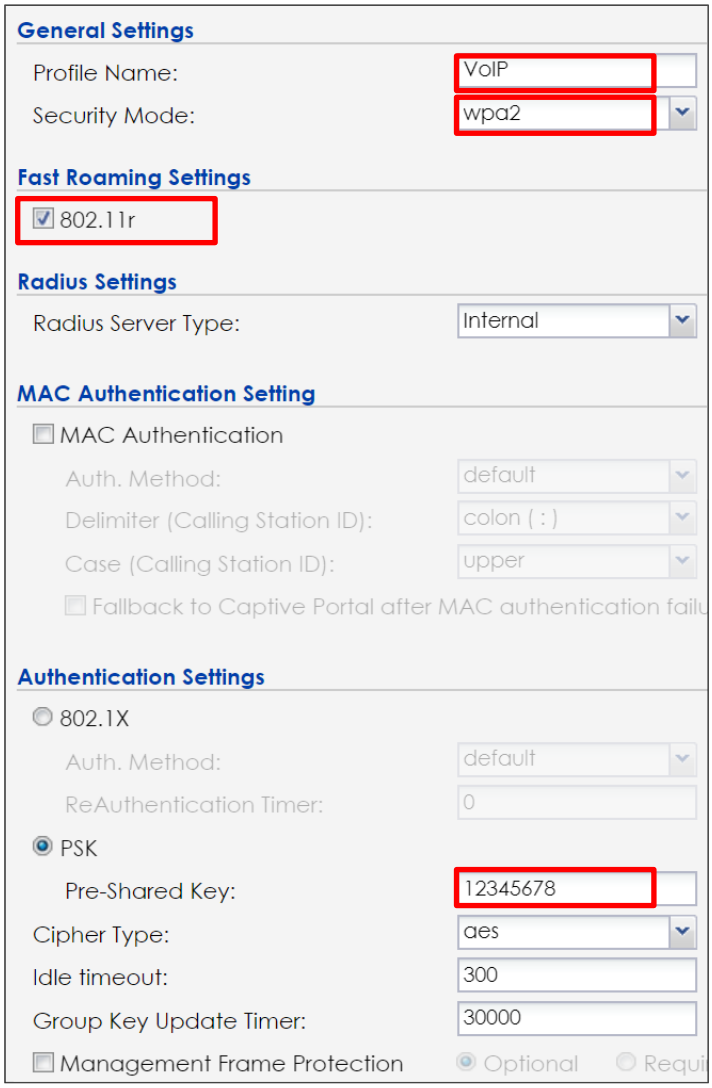
1 Create a new security profile for VoIP phone roaming and must enable 802.11r for fast roaming.

Go to **CONFIGURATION > Object > AP Profile > SSID > Security List**, Click **Add**.

In **General Settings**, key in **VoIP** as profile name, and set security mode to **wpa2**.

In **Fast Roaming Settings**, enable **802.11r**.

In **Authentication Settings**, select to **PSK** and key in **Pre-shared Key**. Click **OK**



2 Create a new SSID for VoIP phone roaming.

In **Profile Name** and **SSID**, key in **VoIP**.

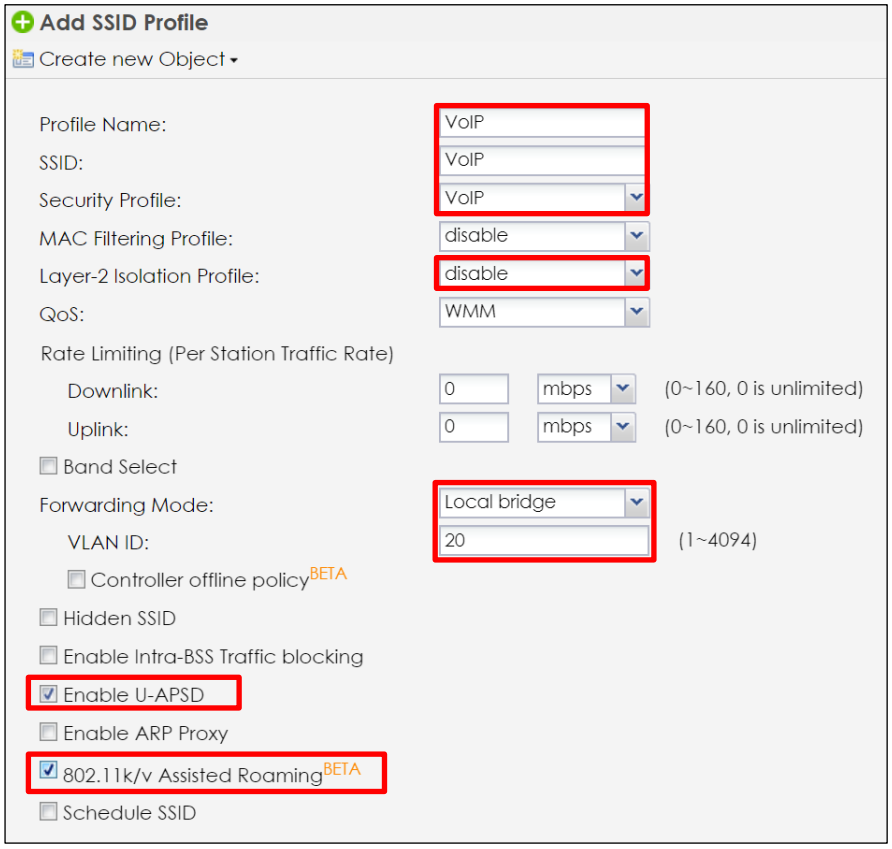
In **Security Profile**, select **VoIP.** Click **OK**.

In **Layer-2 Isolation Profile**, select **disable**.

In **Forwarding Mode** select **Local bridge**.

In **VLAN ID,** key in **20**.

Check the box of **Enable U-APSD** and **802.11k/v Assisted Roaming**.



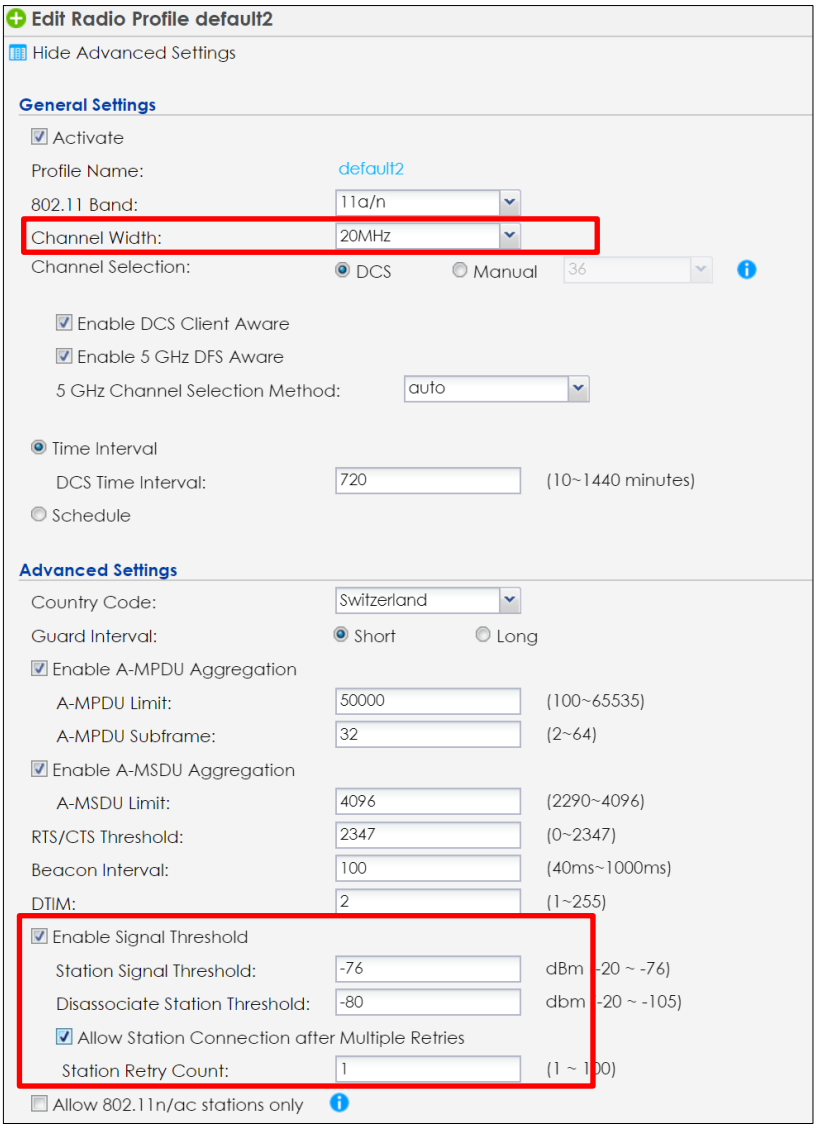
3 Use dedicated SSID for VoWiFi and 5 GHz for the Voice SSID is the best strategy to improve voice quality. Use 20 Mhz channel width for the voice SSID.

Edit the **default2 profile** for 5G radio.

In **channel Width**, select **20MHz**.

Check the box of **Enable Signal Threshold**, key in **-76dBm** for **Station signal Threshold** and key in **-80dBm** for **Disassociate Station Threshold**.

Check the box of **Allow Station Connection after Multiple Retries**.



2.6.3 Configure AP Group

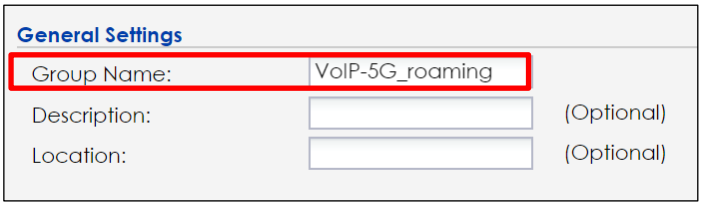
1 Create a new AP group for VoIP Phone roaming, and select AP1 and AP2 as member of the AP group. The maximum 5 GHz power should <18dBm to avoid mismatch capability with client output power.

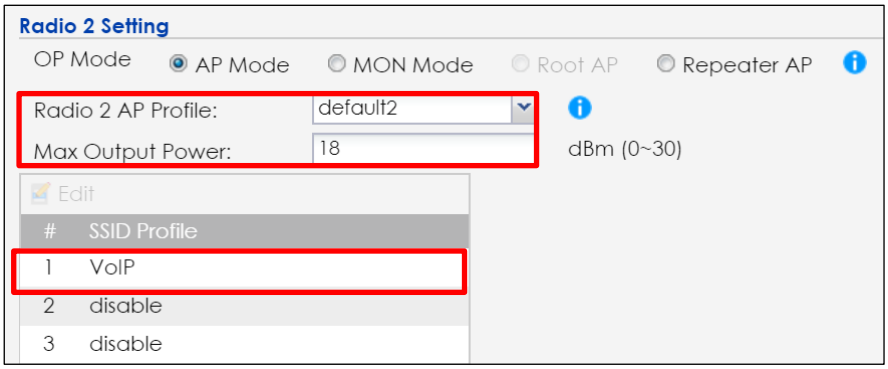
In **Profile Name**, key in **VOIP-5G_roaming**.

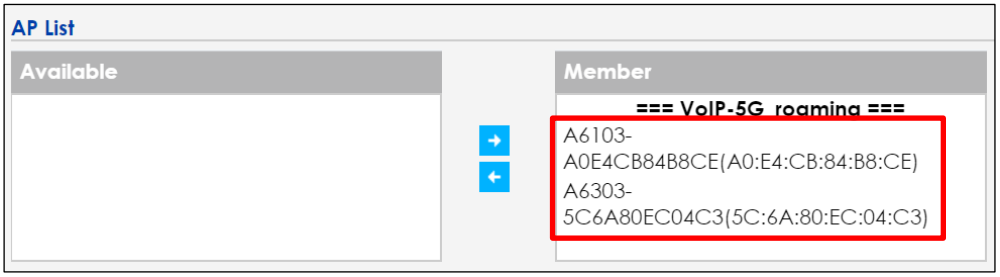
In **Radio 2 Setting**, select **default2** for **Radio 2 AP Profile** and change SSID profile to **VoIP**.

In **Max Output Power**, key in **18dBm**.

In **AP List**, move two APs from Available to Member. Click **OK**.

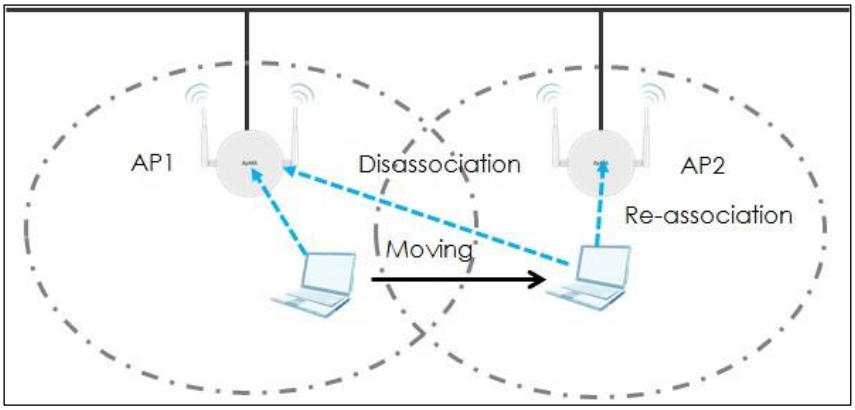






2.6.4 Test the Result

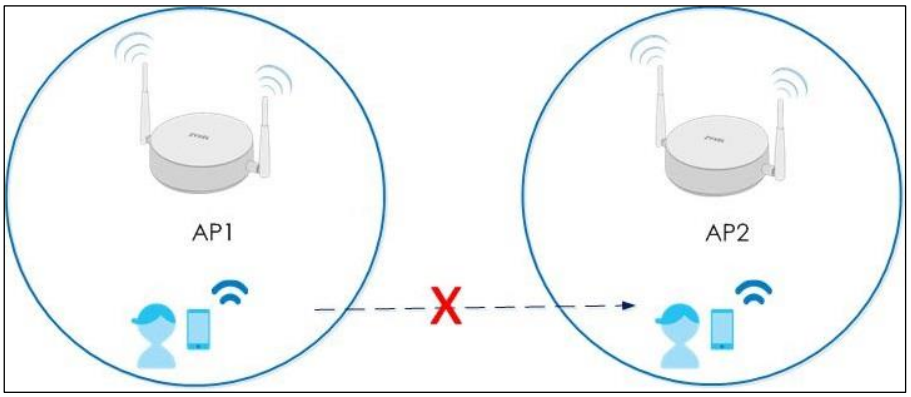
1. User connects to the SSID and make sure the user can access the Internet without any problem.
2. When user is roaming from AP1 to AP2, the connection is not interrupted because of reconnection from AP1 to AP2.



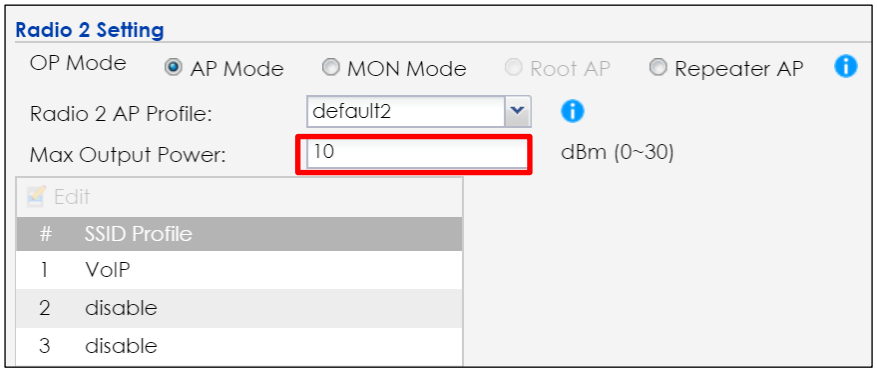
3. The Voice quality is good has not any delay or lose during 1-2 seconds when VoIP phone roaming between AP1 and AP2.

2.6.5 What Could Go Wrong?

1 User may disconnect when AP1 and AP2's signal is not overlapping. Please move these two APs closer or add some APs between two AP to make signal overlap.

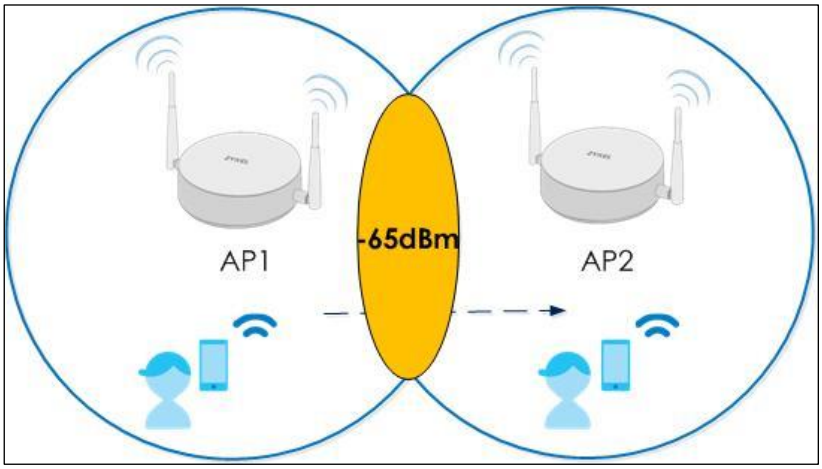


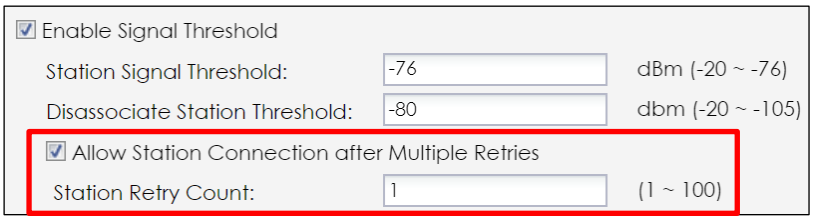
2 When AP1 and AP2 overlapping is too large, the AP1 and AP2's signal are interference to each other. Here are two ways for solving this issue. One is to make these two APs more far away from each other; the other is to decrease Max output power.



3 Enable threshold in radio might cause disconnection between AP and station. When the overlap area RSSI is lower than threshold value, station is not able to connect to AP. The **Station Signal Threshold** and **Disassociation Station Threshold** should be lower than the overlapping area's RSSI and check the box of **Allow Station Connection after Multiple Retries**.

4 Do not suggest aggressive Disassociate Station Threshold (-80 or lower is suggested) as the steering client behavior may cause call-drop.





5 The connection might not be stable if the "Load Balance" is enabled and the maximum station number is reached. The roaming station may connect to the AP and disconnect soon.

6 It's up to station to roam or not. The roaming tendency is able to modify in computer's setting.

7 For RF channel selection, use scheduled DCS channel in off-hours – Voice call is very sensitive to latency and jitter. When AP performs channel scanning, it will cause latency and jitter changes.

8 For all location desired VoWiFi clients, suggest better than -67 dBm signal coverage for 5 GHz. This usually means in one location, there will be at least one good signal AP (>-67dBm) and other 2~3 AP in fair signal (-72~-78dBm).

9 In the case that 2.4 GHz must be enabled for the voice SSID, always set 2.4 GHz power 6~8 dBm lower than 5 GHz. And don't use different SSID for 2.4 GHz and 5 GHz for voice application. It will sometimes confuse the roaming behavior of the phone device.

10 Don't use Band-steering: it could cause interoperability issues with WiFi phone. In the worst case scenario, the WiFi phone determined to use 2.4 GHz only and AP keep trying to steer it to 5 GHz. For data only, that is usually not an issue but could lead to Voice quality issue.

11 No more than 3 SSIDs should be enabled on any single AP.

Optimize the Wireless Environment

3.1 How to Set up User Ratio of 2.4GHz and 5GHz to Avoid WiFi Congestion?

The example instructs how to configure AP profile with band select. When 2.4GHz and 5G capable users connect to the AP, user is easy to connect to 5GHz when enabling band select. This example uses band select to balance wireless band, 2.4GHz and 5GHz.

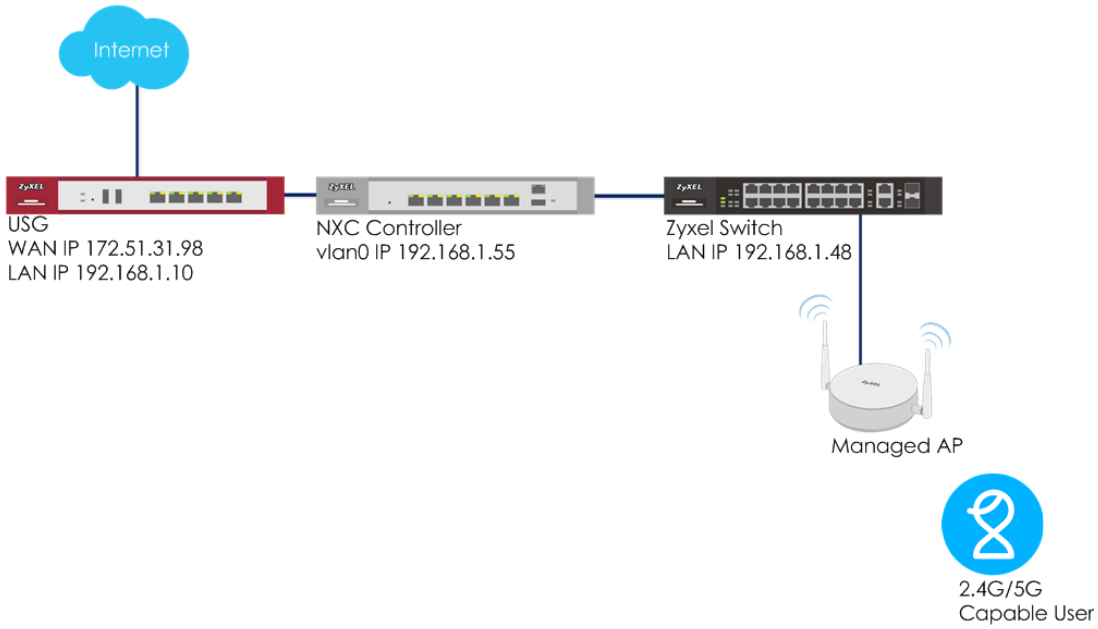


Figure 3.1 Configure AP profile with Band Select

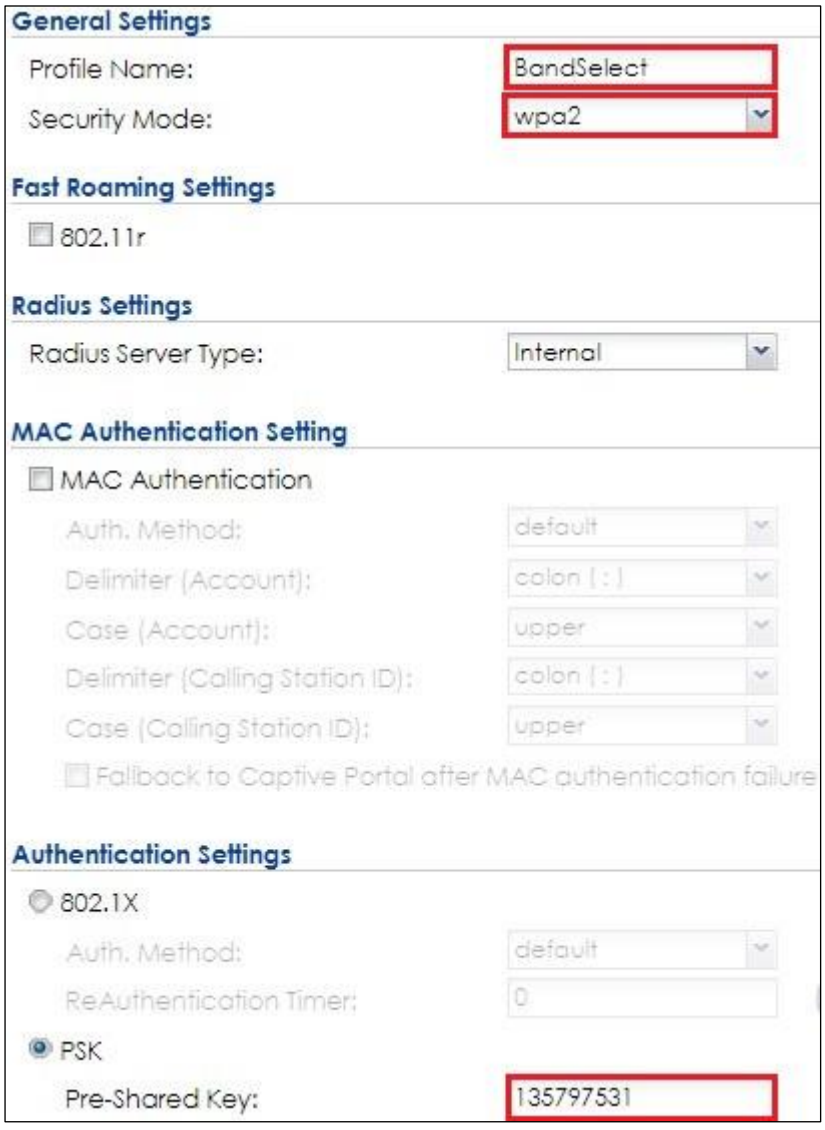
Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC5500 (Firmware Version: 5.40), GS2210-8HP (Firmware Version: V4.30).

3.1.1 Configure Band Select

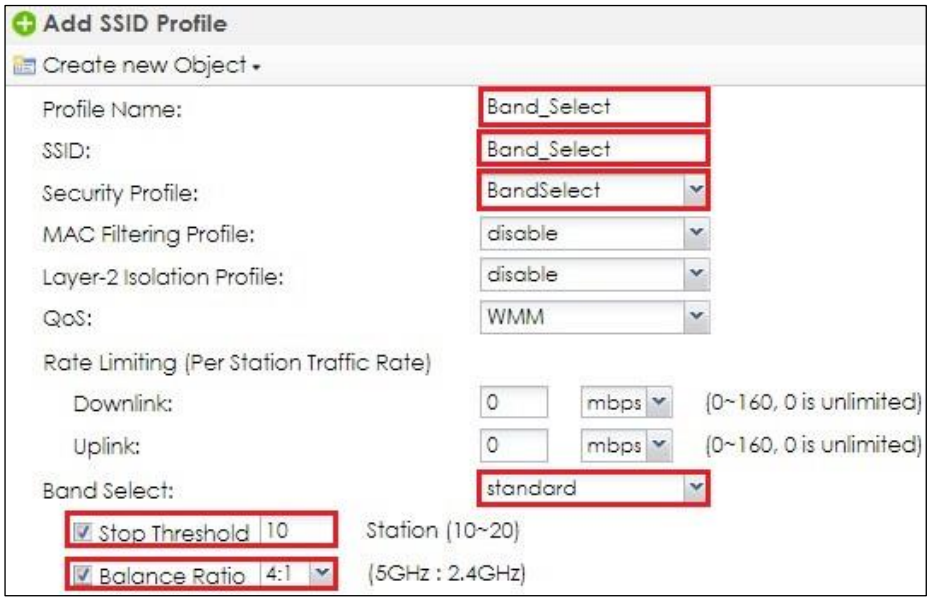
1 Band select setting is in SSID. Before creating a new SSID, security is necessary to create first. Go to **CONFIGURATION > Object > AP Profile > SSID > Security List**, click Add to create a new security rule for band select.

In **General Settings**, use **BandSelect** as the **Profile Name**, and **wpa2** as the **Security Mode**.

In **Authentication Settings**, select **PSK** and make a **Pre-Shared Key**. Click **OK**.



2 Go to **CONFIGURATION > Object > AP Profile > SSID > SSID List**, click Add to create a new SSID for band select.
Use **Band_Select** as the **Profile Name** and **SSID**. Select **BandSelect** as the **Security Profile**.
In **Band Select**, select **standard** to let user easy access to AP via band 5GHz. Check **Stop Threshold** and set station number to **10**. Check **Balance Ratio** and select **4:1**. Click **OK**.

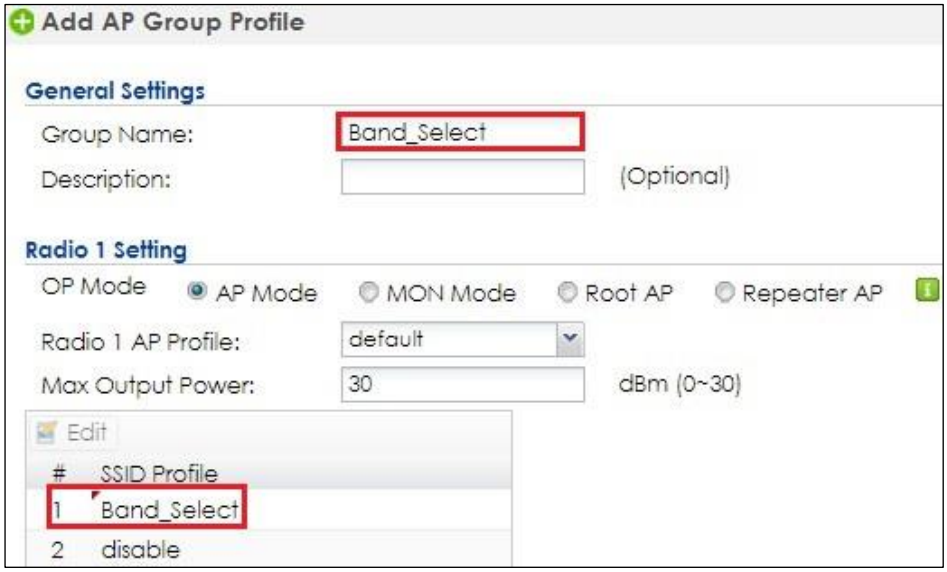


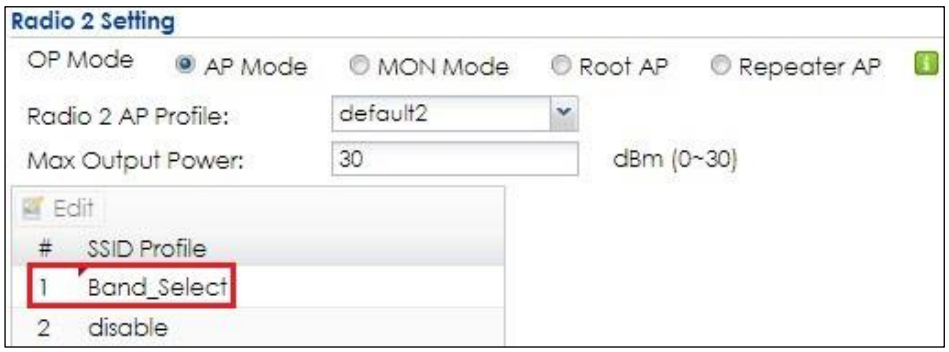
3 Go to **CONFIGURATION > AP Management > AP Group**, click Add to create a new group for band select.

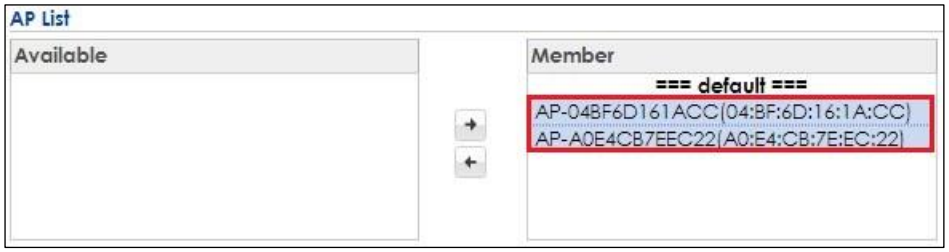
In **General Setting**, set Group Name as **Band_Select**.

In **Radio 1 Setting** and **Radio 2 Setting**, select SSID profile **Band_Select**.

In **AP List**, select APs to **Member**. Click **Override Member AP Setting**. Click **Yes** when window pop up.







3.1.2 Test the Result

1 Use a 2.4GHz and 5GHz supported device (ex. Mobile phone or laptop) to connect with SSID Band_Select. The device connects to 5GHz first when it connects to the SSID.

3.1.3 What Could Go Wrong?

1. If the AP does not support dual band, band select does not work.
2. When the connected station number is greater than stop threshold station number, the band select stops working.
3. Band Select may potentially cause interruptions for time-sensitive applications if the client only has 2.4G ability, like roaming delays.
4. The station connected ratio is approximately the ratio you select in the SSID profile setting.

3.2 How to Set up RSSI Threshold to Avoid Low Rate User Connection Affected Wireless Performance?

The example instructs how to set up RSSI threshold. RSSI threshold ensure wireless clients receive good signal to prevent them from being impacted by the others with poor signal. There are two RSSI value to set. One is station signal threshold which sets a minimum client signal strength to connect with AP; the other is disassociation station threshold to sets a minimum kick-off signal strength.

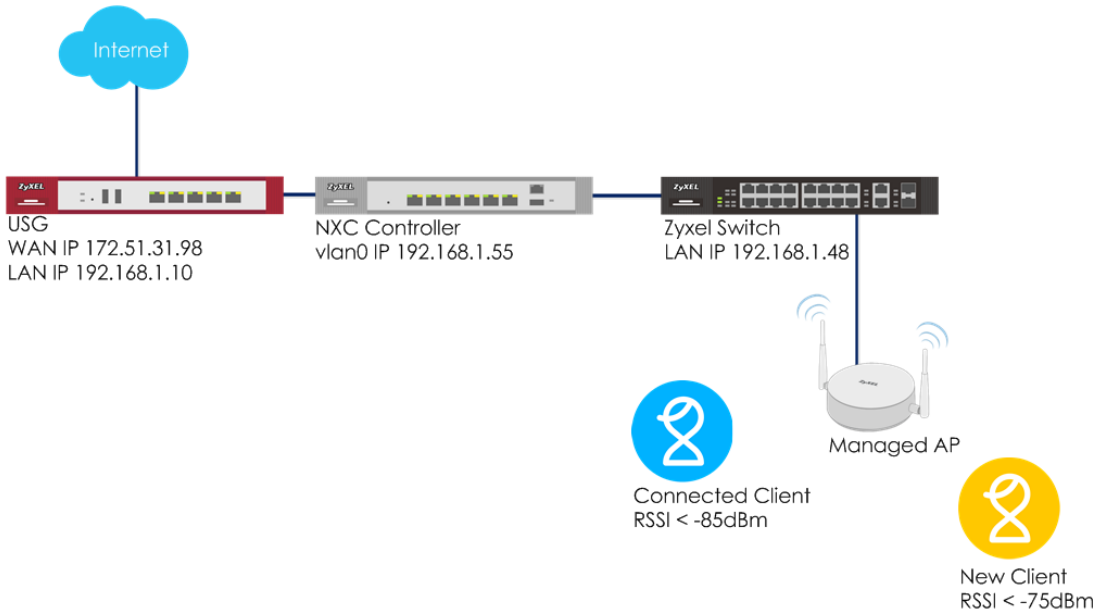
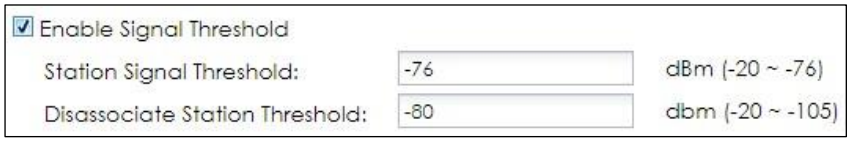


Figure 3.2 RSSI Threshold

Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC5500 (Firmware Version: 5.40), GS2210-8HP (Firmware Version: V4.30).

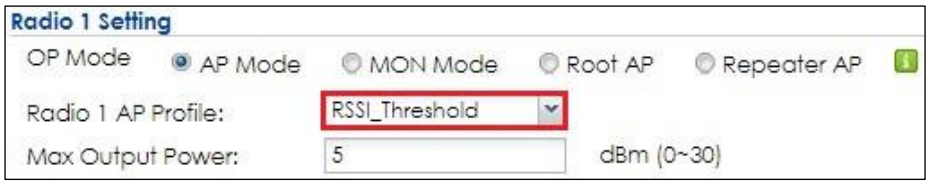
3.2.1 Configure Radio Setting for RSSI Threshold

1 Go to **CONFIGURATION > Object > AP Profile > Radio**, click **Add** to add a new 2.4GHz radio, **RSSI_Threshold**, for setting RSSI threshold. Click **Show Advanced Settings** to check **Enable Signal Threshold**, and edit the value for **Station Signal Threshold** and **Disassociation Station Threshold**. Click **OK**. The station needs signal strength at least -76dBm to make connection with AP, and when the signal is less than -80dBm, the AP disconnects with client.



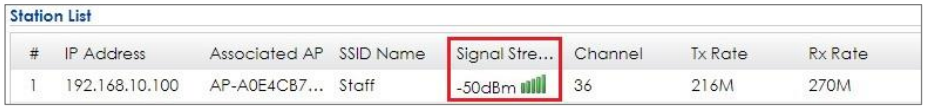
3.2.2 Apply Radio with RSSI Threshold

1 Go to **CONFIGURATION > Wireless > AP Management > AP Group**, click default and **Edit** it. In **Radio 1 Setting**, change **radio 1 AP Profile** to **RSSI_Threshold**. Click **Override Member AP Setting**, and the click **Yes** to apply setting to member APs.



3.2.3 Test the Result

1 In **MONITOR > Station Info > Station List**, check the new connected client's signal strength is stronger than -76dBm.



2 In **MONITOR > Log >View AP Log**, select the AP to which the station is connected and query its log. When the connected client's RSSI is less than -80dBm, the AP kick-out the station because of the RSSI threshold.

3 After modifying the RSSI threshold, it's necessary to check the station's connection status to fine tune the setting value. For example, if the stations don't connect to the nearer AP but the far one, you can adjust the disassociation station threshold to bigger value.

3.3 How to Set up Rate Limiting for Bandwidth Control?

The example instructs how to set up rate limiting for each station traffic rate. In this example, downlink is to set the maximum incoming transmission data rate, and uplinks is to set the maximum outgoing transmission data rate for each client connected to specific SSID.

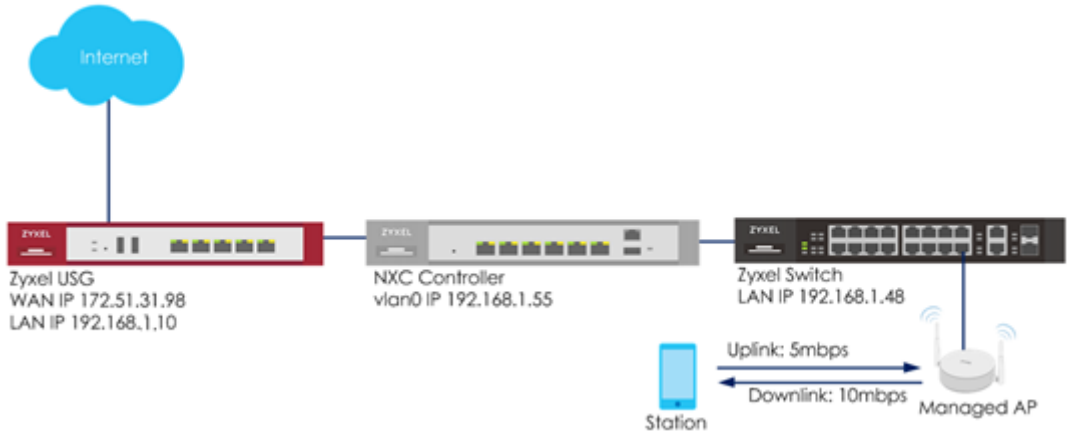
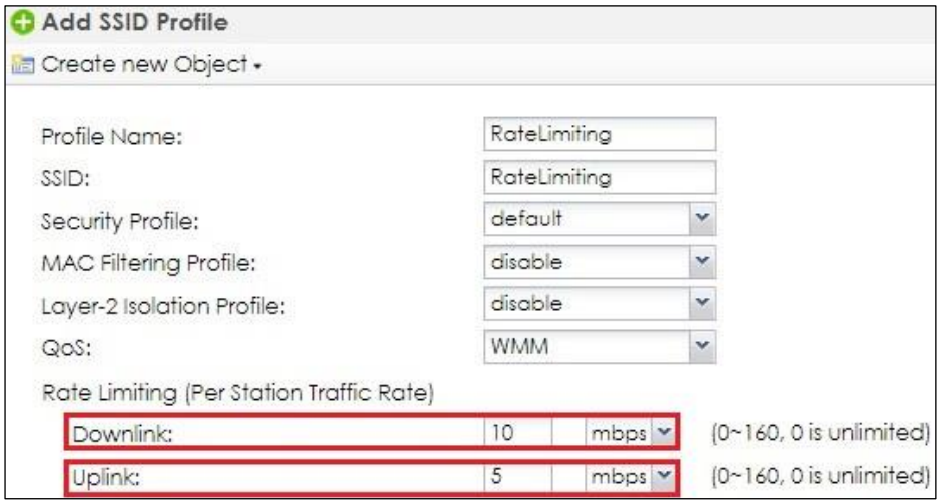


Figure 3.3 Uplink and Downlink Rate Limiting per Station

Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC5500 (Firmware Version: 5.40), GS2210-8HP (Firmware Version: V4.30).

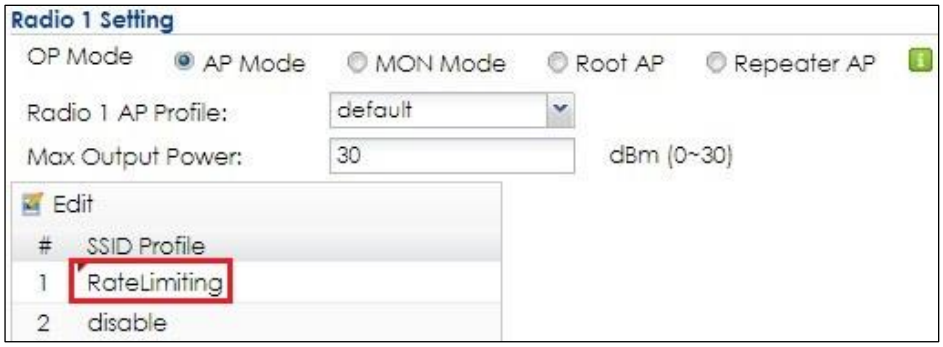
3.3.1 Configure Rate Limiting

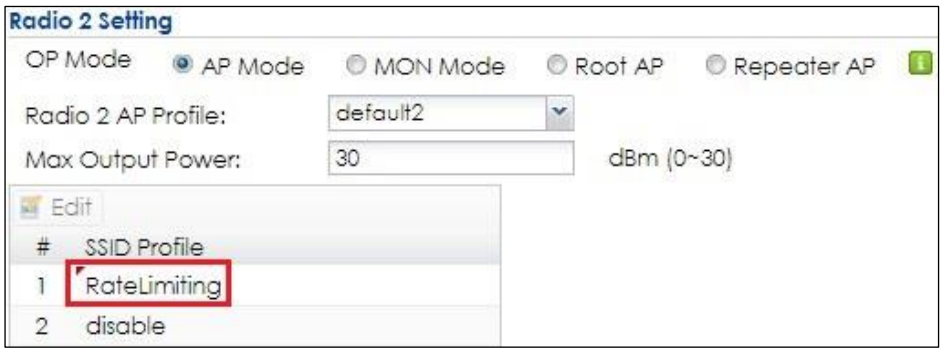
1 Go to **CONFIGURATION > Object > AP Profile > SSID**, click **Add** to add a new SSID, **RateLimiting**. Set the **Downlink** and **Uplink** maximum transmission data rate per station traffic. Click **OK**.



3.3.2 Apply Rate Limiting to Management AP

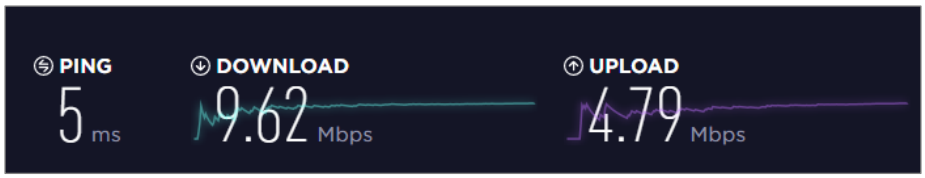
1 Go to **CONFIGURATION > Wireless > AP Management > AP Group**, click default and **Edit** it. In **Radio 1 Setting/Radio 2 Setting**, change **SSID Profile** to **RateLimiting**. Click **Override Member AP Setting**, and the click **Yes** to apply setting to member APs.





3.3.3 Test the Result

1 When the station connected to AP via SSID **RateLimiting**, the maximum incoming transmission data rate is not over 10mbps, and maximum outgoing transmission data rate is not over 5mbps.



3.4 How to Share AP loading to Optimize Wireless Performance?

The example instructs how to set up AP group with load balance. There are three types for load balance, by station number, by traffic level, and by smart classroom. This example shows the configuration of these three kinds of load balance for different scenarios and the load balance is set per radio.

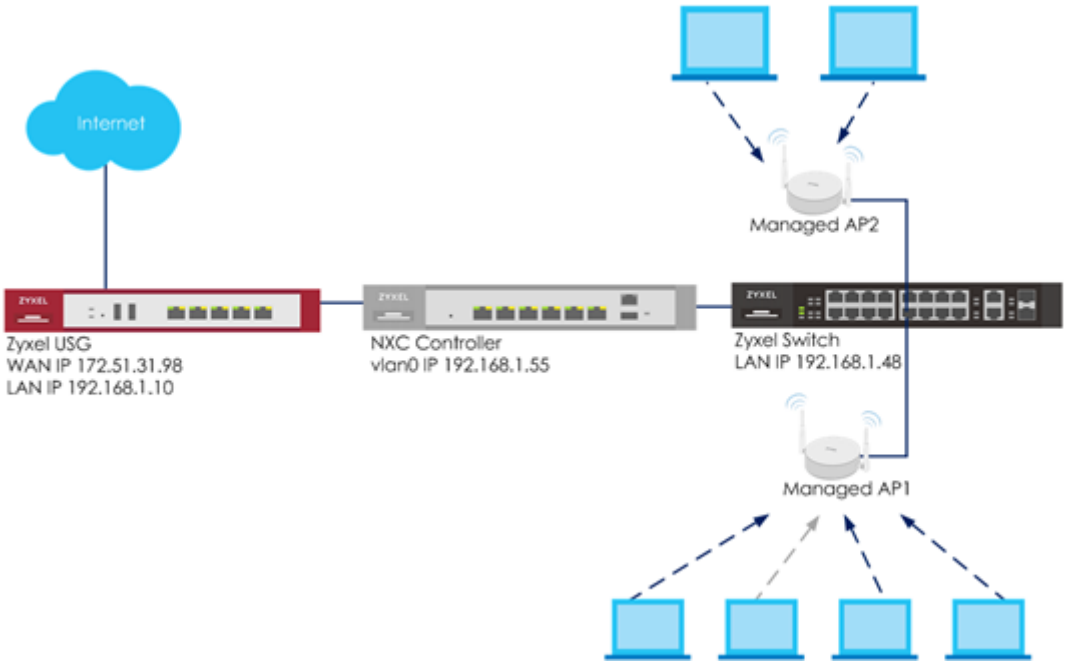


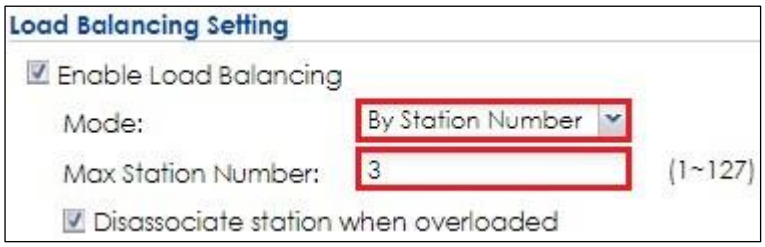
Figure 11 Load Balance

Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC5500 (Firmware Version: 5.40), GS2210-8HP (Firmware Version: V4.30).

3.4.1 Configure Load Balance to “by Station Number”

1 Go to **CONFIGURATION > Wireless > AP Management > AP Group**, click default for editing.

In **Load Balancing Setting**, check **Enable Load Balancing** and **Disassociate station when overloaded**. Change **Mode** to **by Station Number** and set the **Max Station Number**. Click **Override Member AP setting**. Click **Yes**. When the station number is greater than the max station number, AP disconnects clients by the longest idle time first, and then by the poorest signal strength.

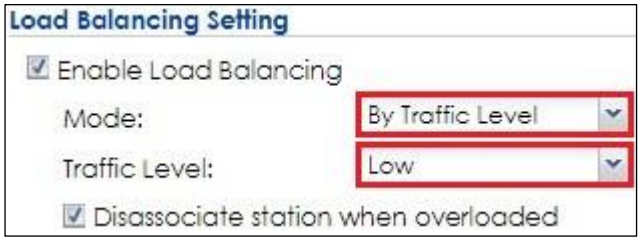


3.4.2 Configure Load Balance to "by Traffic Level"

1 Go to **CONFIGURATION > Wireless > AP Management > AP Group**, click default for editing.

In **Load Balancing Setting**, check **Enable Load Balancing** and **Disassociate station when overloaded**. Select **Mode** to **by Traffic Level** and set the **Traffic Level**. Click **Override Member AP setting**. Click **Yes**.

For load balancing by traffic level, the total throughput is defined as High: 35Mbps; Medium: 23Mbps; Low: 11Mbps. When total throughput of connected stations exceed the selected traffic level, AP disconnects clients with the longest idle time first, and then with the poorest signal strength.



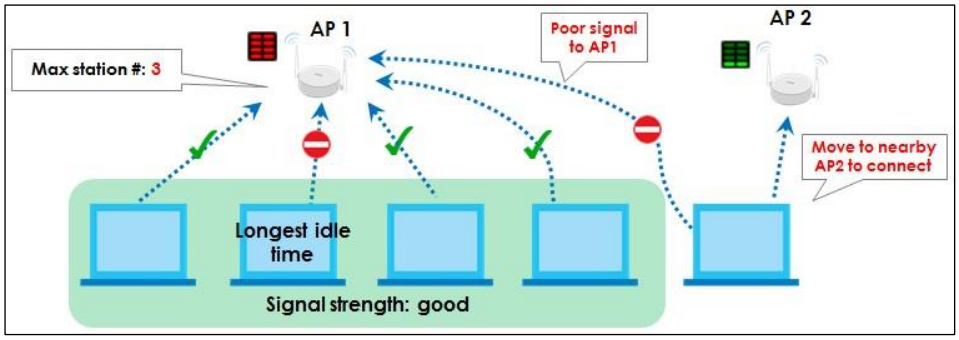
3.4.3 Configure Load Balance to “by Smart Classroom”

1 Go to **CONFIGURATION > Wireless > AP Management > AP Group**, click default for editing.

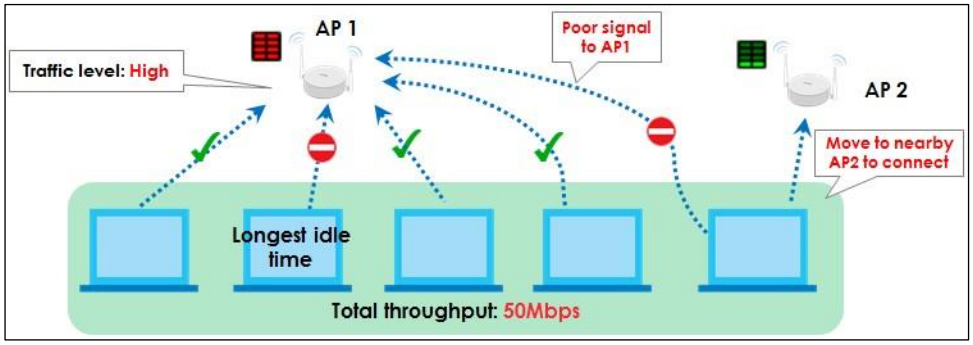
In **Load Balancing Setting**, check **Enable Load Balancing**. Select **Mode** to **by Smart Classroom** and set the **Max Station Number**. Click **Override Member AP setting**. Click **Yes**. When the station number is greater than the max station number, AP disconnects clients with the poorest signal strength.

3.4.4 Test the Result

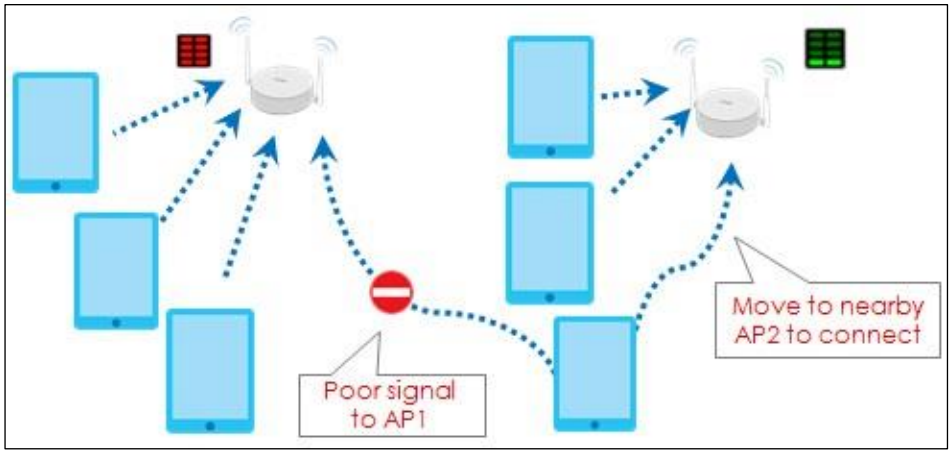
1 When load balancing by station number, the AP disconnects client with the longest idle time first, and then with the poorest signal strength if the client number is greater than setting number.



2 The traffic level is set to low and the maximum bandwidth allowed is 11 Mbps. When total throughput of connected stations exceed the selected traffic level, AP disconnects clients with the longest idle time first, and then with the poorest signal strength.



3 When the station number is greater than the max station number, AP disconnects clients with the poorest signal strength.



3.4.5 What Could Go Wrong?

1. It needs two APs to do the load Balance, or the function is not workable.
2. Load balance's purpose is sharing loading instead of limiting the station numbers.
3. If all APs are over max station number setting/traffic level, the stations still can connect to APs.

Secure the Wireless Environment - 802.1x

4.1 How to Configure 802.1x to Secure the Wireless Environment with an External RADIUS Server?

The example instructs how to set up NXC controller with an external radius server. When station wants to connect with AP, you can use an AAA server to provide access control to your network. In this example, the radius server is external but not embedded in NXC controller, and the Radius server is set ready for authentication.

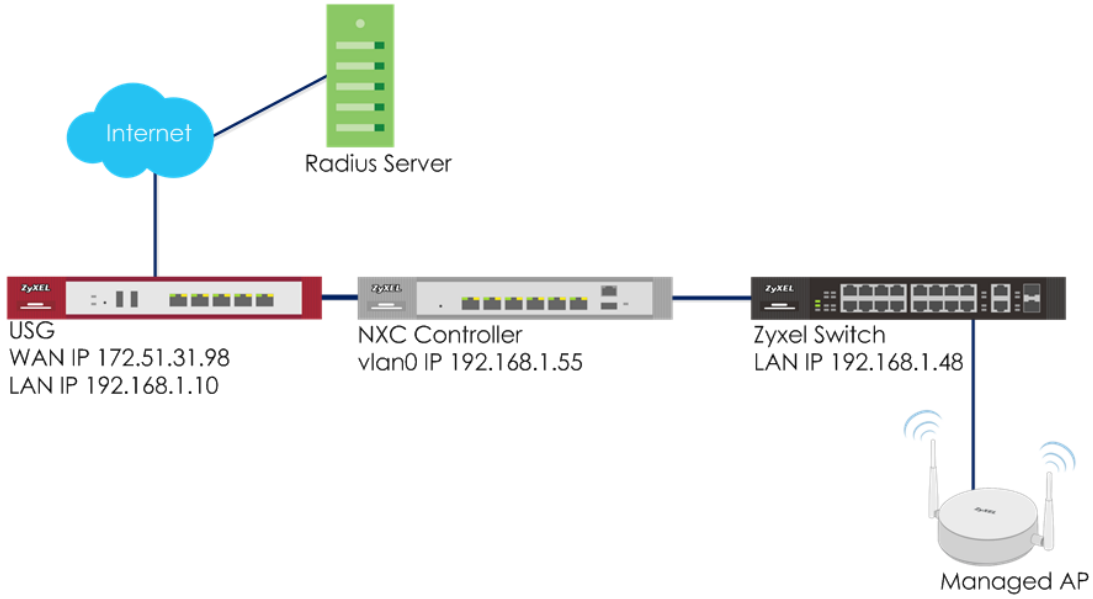
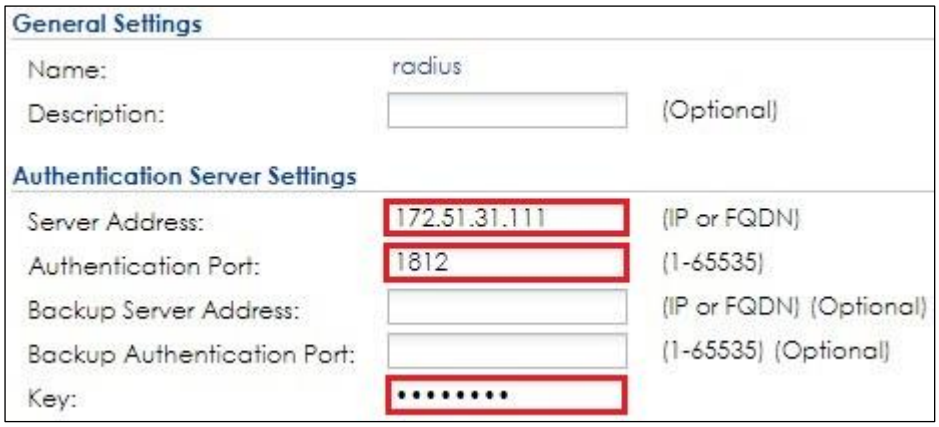


Figure 4.1 Set up AP/NXC with an External Radius Server

Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC5500 (Firmware Version: 5.40), GS2210-8HP (Firmware Version: V4.30).

4.1.1 Configure Radius Server Setting

1 Go to **CONFIGURATION > Object > AAA Server > RADIUS**, click **#1 radius**, and then click **Edit**. Set the **Server Address**, and **Authentication Port** is **1812**. Enter the **Key** for Radius server and click **OK**.



2 Go to **CONFIGURATION > Object > Auth. Method**, click **#1 default**, and then click **Edit**. Change the Method to **group radius**. Click **OK** to save.

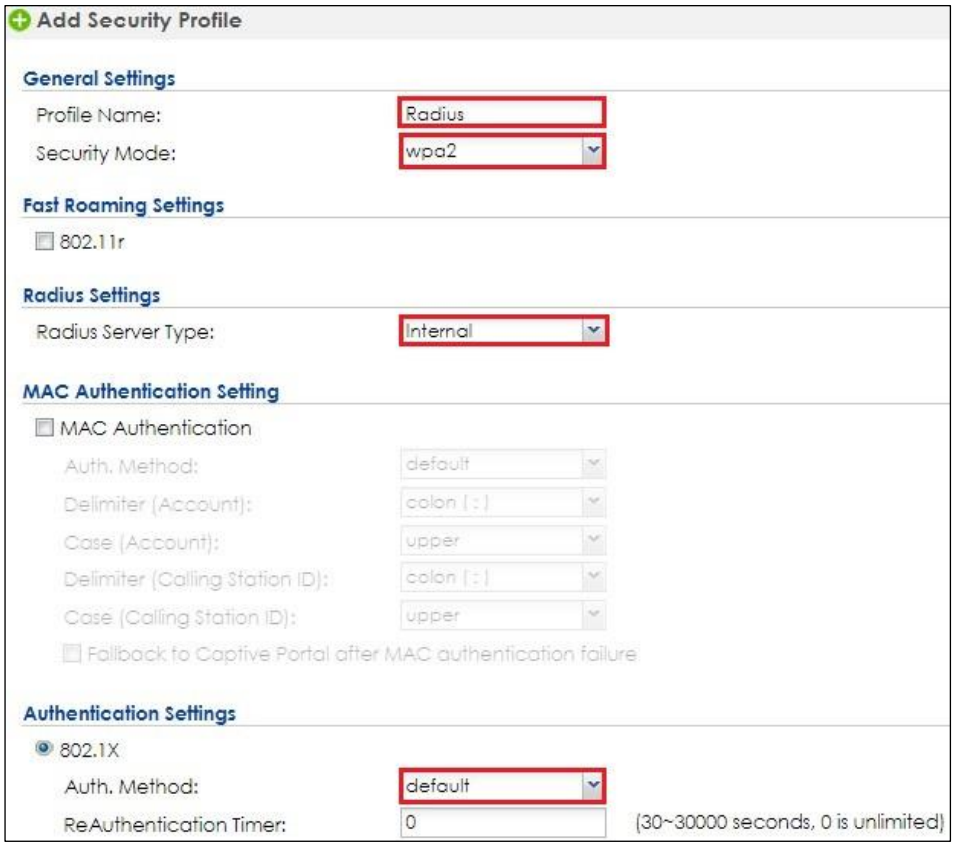
4.1.2 Configure AP Profile

1 Configure AP profile to use 802.1x authentication and user needs to log in with their ID and Password when connecting to AP's SSID. Go to **CONFIGURATION > Object > AP Profile > SSID > Security List**, click **Add** to add security for 802.1x.

In **General Settings**, enter the **Profile Name** and select **Security Mode** to **wpa2**.

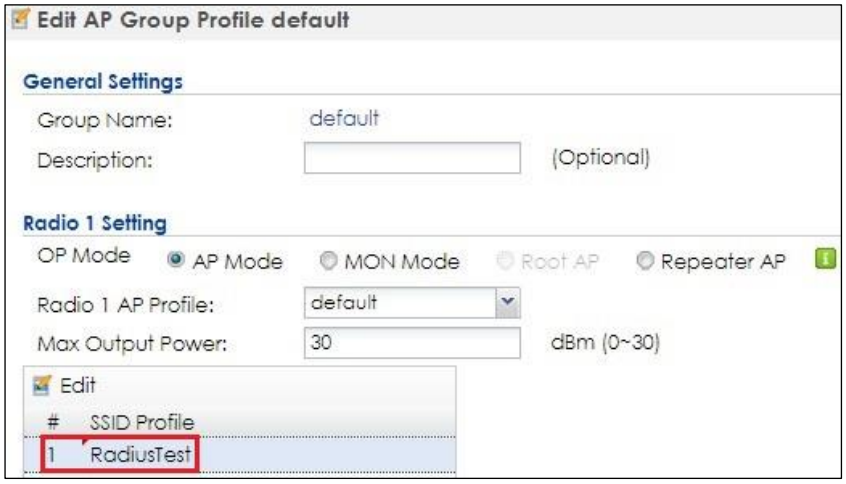
In **Radius Settings**, select **Internal** that means the authentication needs NXC to communicate with external radius server.

In **Authentication Settings**, select **802.1x** and **Auth. Method** is **default**. Click **OK**.



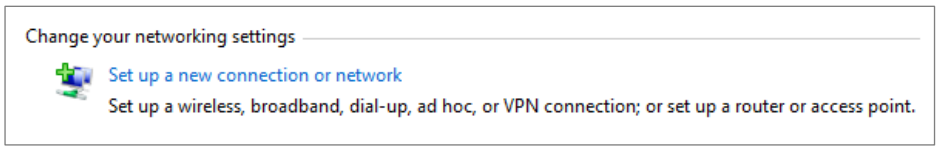
2 Go to **CONFIGURATION > Object > AP Profile > SSID > SSID List**, click **add** to add a SSID for connection with 802.1x security. Key-in the **Profile Name** and **SSID**, and change **Security Profile** to **RadiusTest** which sets in step1. Click **OK** to save.

3 Go to **CONFIGURATION > Wireless > AP Management > AP Group**, click **default** to **Edit**. Change SSID to **RadiusTest** in the SSID Profile. Click **Override Member AP Setting** to apply the SSID to AP and click **Yes** in the pop-up window. Click **OK**.

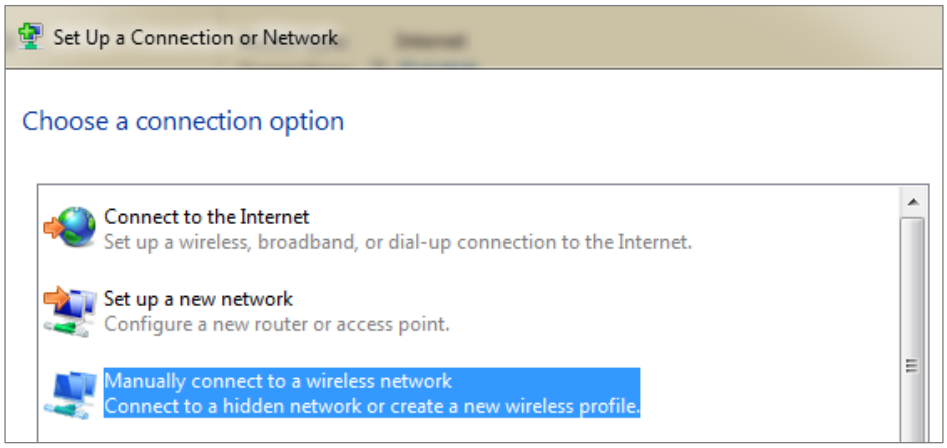


4.1.3 Test the Result

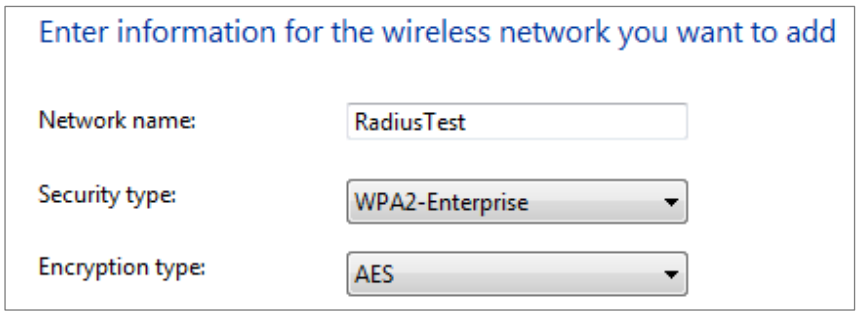
1 Before connecting the SSID, the computer needs to do some settings to make connection successfully.
Opening **Network and Sharing Center** in computer, click **Set up a new connection or network** for building up a new network.



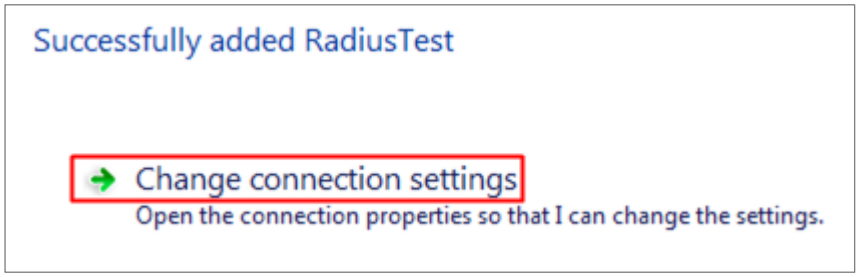
2 Select **Manually connect to a wireless network**. Click **Next**.



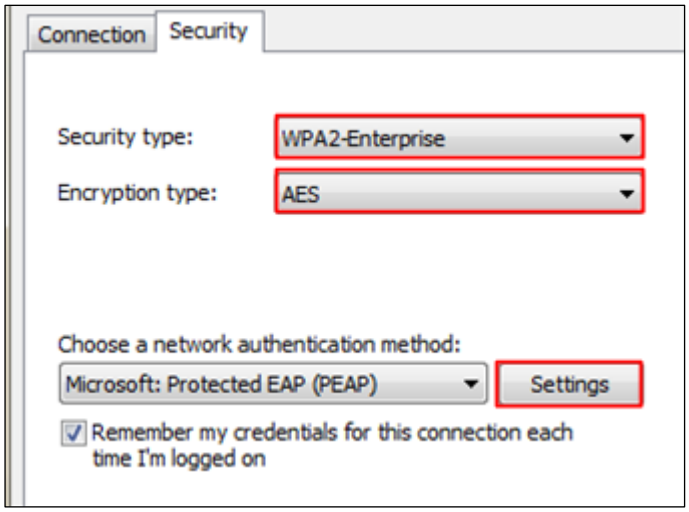
3 Key-in the SSID **Network name** and change the **Security type** to **WAP2-Enterprise**, and the **Encryption type** is **AES**. Click **Next**.



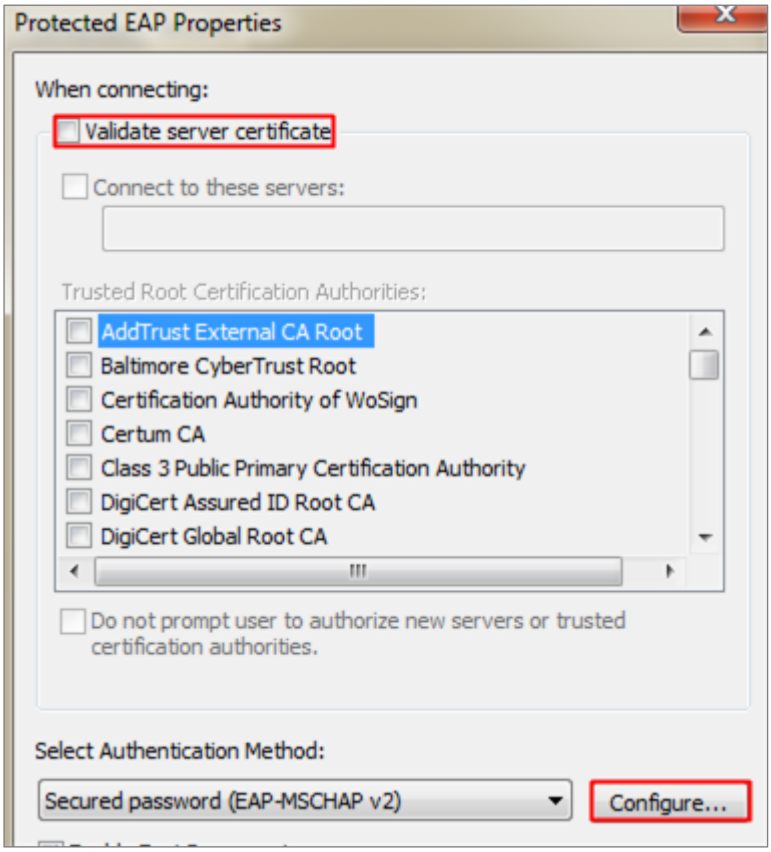
4 Select **Change connection settings**.



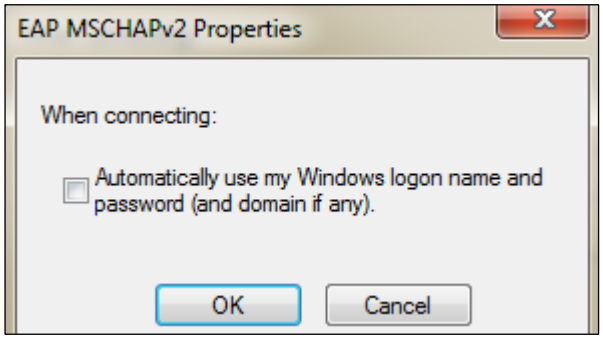
5 Change **Security type** to **WPA2-Enterprise**, **and Encryption type** is **AES**. Click **Settings**.



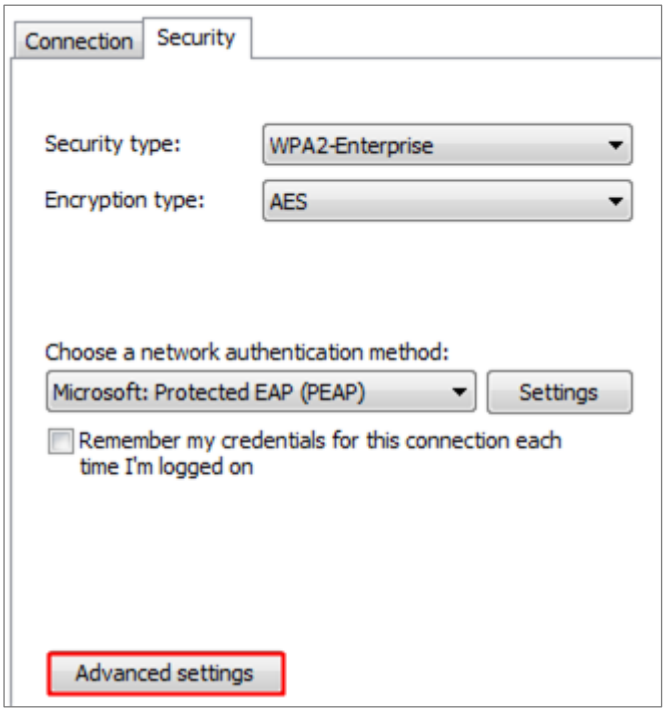
6 Uncheck **Validate server certificate** and click **Configure**.



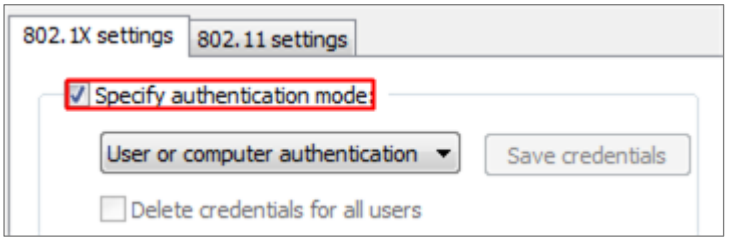
7 Uncheck the checkbox in the pop-up window. Click **OK**.



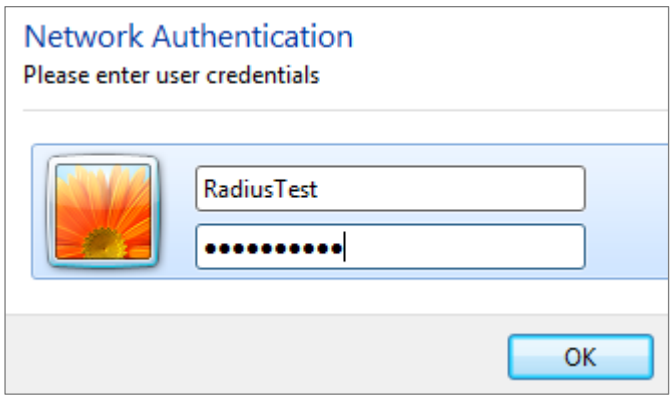
8 Back to the security setting page and click **Advanced settings**.



9 Check **Specify authentication mode**. Click **OK** to save.

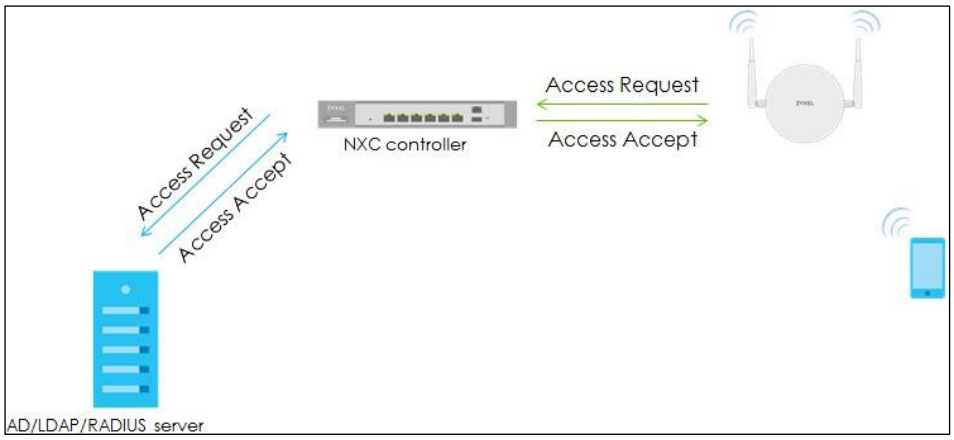


10 Select to the SSID, RadiusTest, for wireless connection. Enter user credentials for authentication. After entering the correct ID and password, the wireless connection is setup successfully.

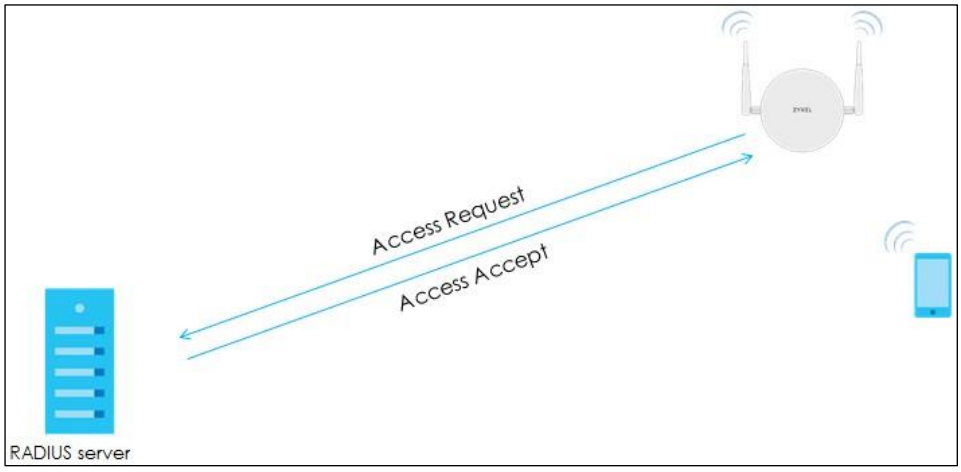


4.1.4 What Could Go Wrong

1 There are two kinds of **Radius Server Types** in security profile setting. **Internal** means the authentication is doing between NXC controller and Radius server. The Radius server needs to add NXC controller as trusted client.



2 **External** means the authentication is doing between Managed AP and Radius server. The Radius server needs to add the managed AP as trusted client.



4.2 How to Configure 802.1x to Secure the Wireless Environment with an External AD Server?

The example instructs how to set up the NXC controller with an external AD server. When the station wants to connect with the AP, you can use an AAA server to provide access control to your network. In this example, the AD server is external but not embedded in the NXC controller, and the controller is already set to use the AD server for authentication.

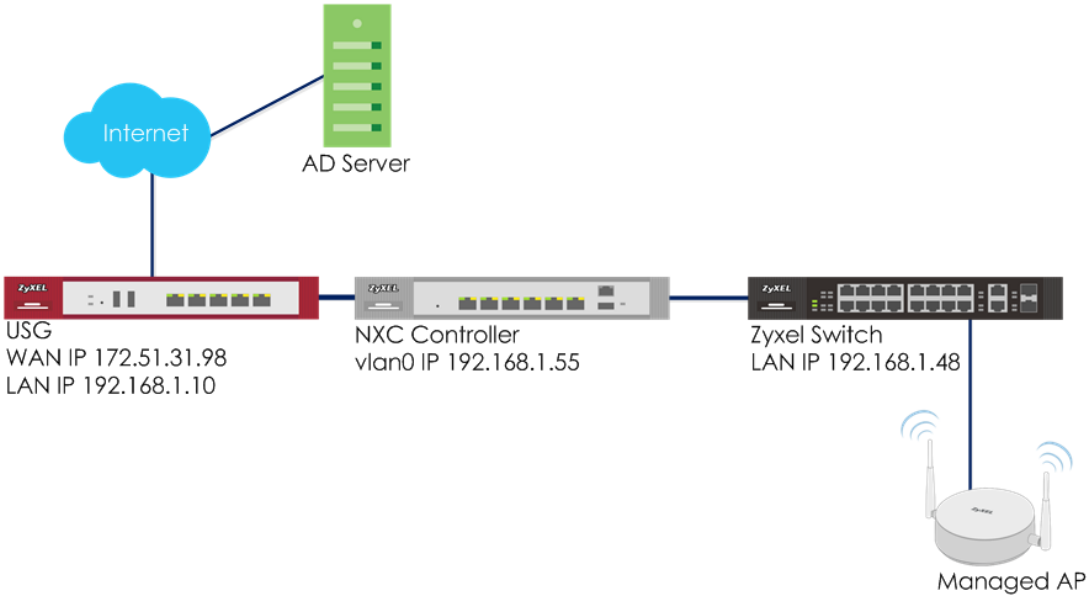


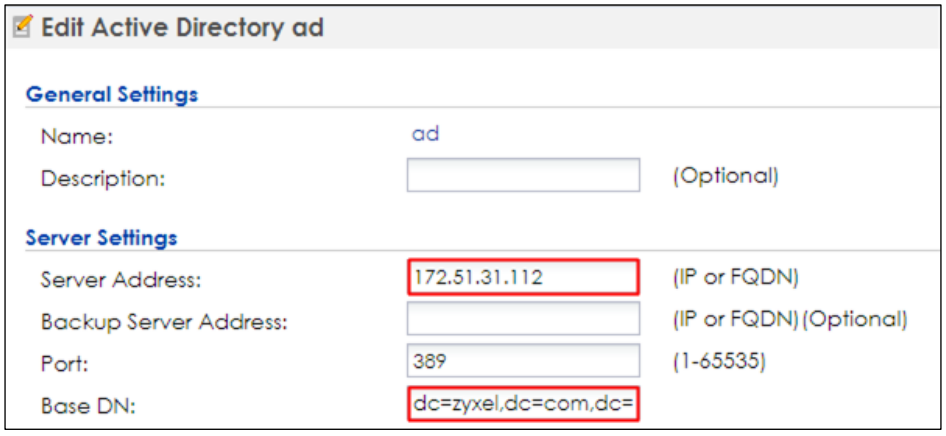
Figure 4.2 Set up AP/NXC with an External AD Server

Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC5500 (Firmware Version: 5.40), GS2210-8HP (Firmware Version: V4.30).

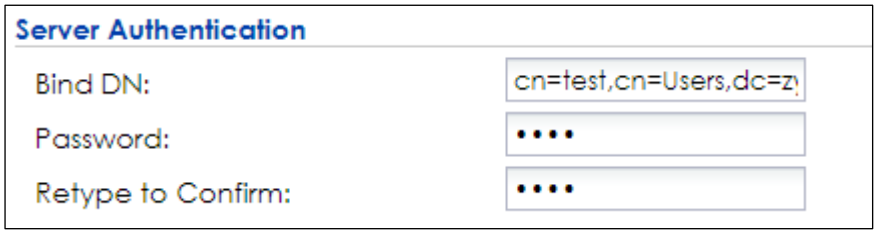
4.2.1 Configure AD Server Setting

1 Go to **CONFIGURATION > Object > AAA Server > Active Directory**, click **#1 ad**, and then click **Edit** to configure AD server's information.

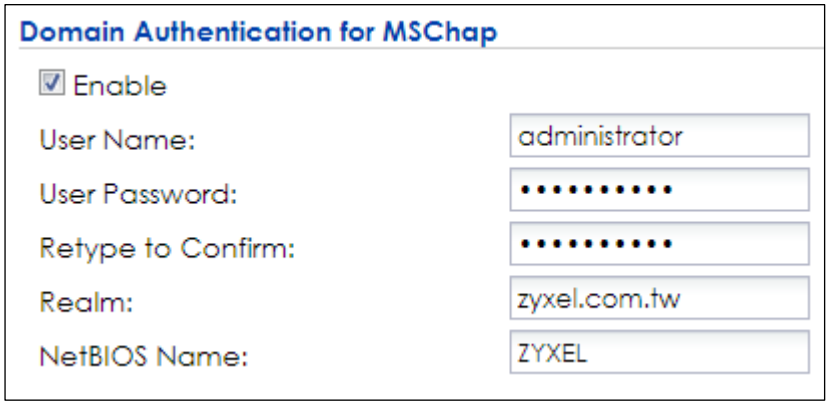
2 In **Server Settings**, enter **Server Address**. Here use **172.51.31.112** as the example. Go to AD server to check Base DN. Here is an example for checking the Base DN on Windows server, and it can be copied from clicking right on the domain name > properties > Attribute Editor> distinguished Name > View.



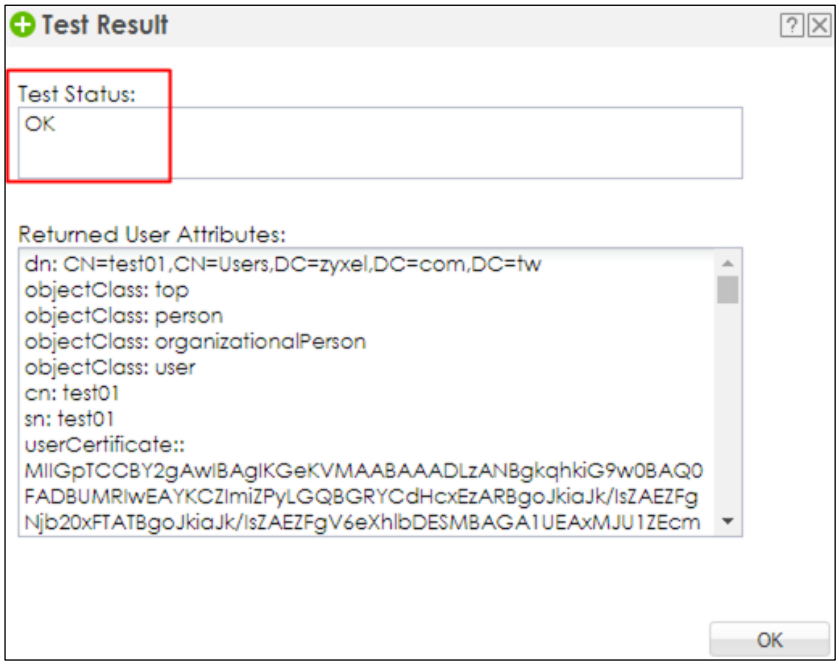
3 In **Server Authentication**, enter **Bind DN** and **Password**. You can check Bind DN in the AD server. In the AD server, clicking right on the Administrator > properties > Attribute Editor > distinguished Name > View. The Password is Administrator's password in the AD server.



4 In **Doman Authentication for MSChap**, check **Enable** and enter the **User Name**, **User Password**, **Realm**, and **NetBIOS Name**. The Realm is the domain name of the AD server.



5 After finishing the configuration, enter **administrator** as the **Username** and click **Test** in **Configuration Validation**.



6 Go to **CONFIGURATION > Object > Auth. Method**. Select to the default method, and click **Edit**. Select the AD server you create. Click **OK**.

7 Go to **CONFIGURATION > System > Date/Time** and check **Current Time and Date**. The date and time must be the same as the date and time of the AD server. If it's different, you can select the correct time zone in **Time Zone Setting**.

8 Go to **CONFIGURATION > System > DNS** for setting domain zone information. In **Domain Zone Forwarder**, click Add to add a new domain zone. Enter the **Domain Zone** and **Public DNS Server** which is the AD server's IP.

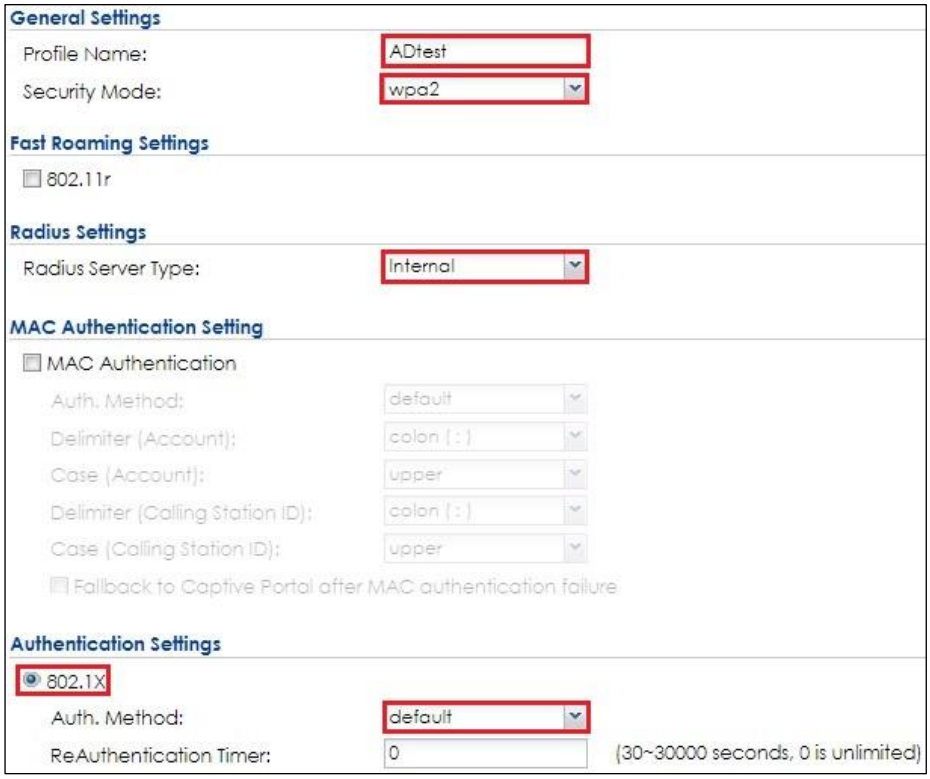
4.2.2 Configure AP Profile

1 Configure AP profile to use 802.1x authentication that the user needs to log in with their ID and Password when connecting to AP's SSID. Go to **CONFIGURATION > Object > AP Profile > SSID > Security List**, click **Add** to add security for 802.1x.

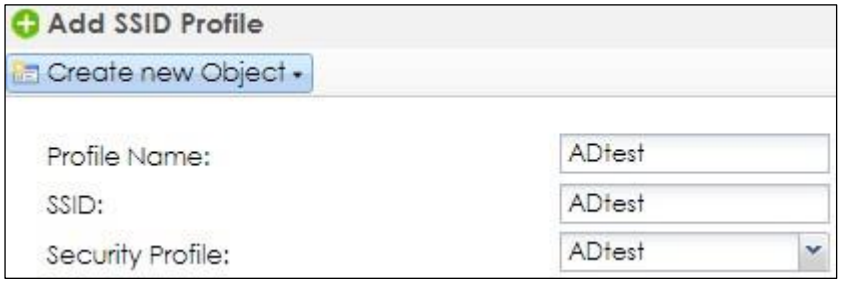
In **General Settings**, enter the **Profile Name** and change **Security Mode** to **wpa2**.

In **Radius Settings**, select to **Internal** and it means the authentication needs NXC to communicate with an external AD server.

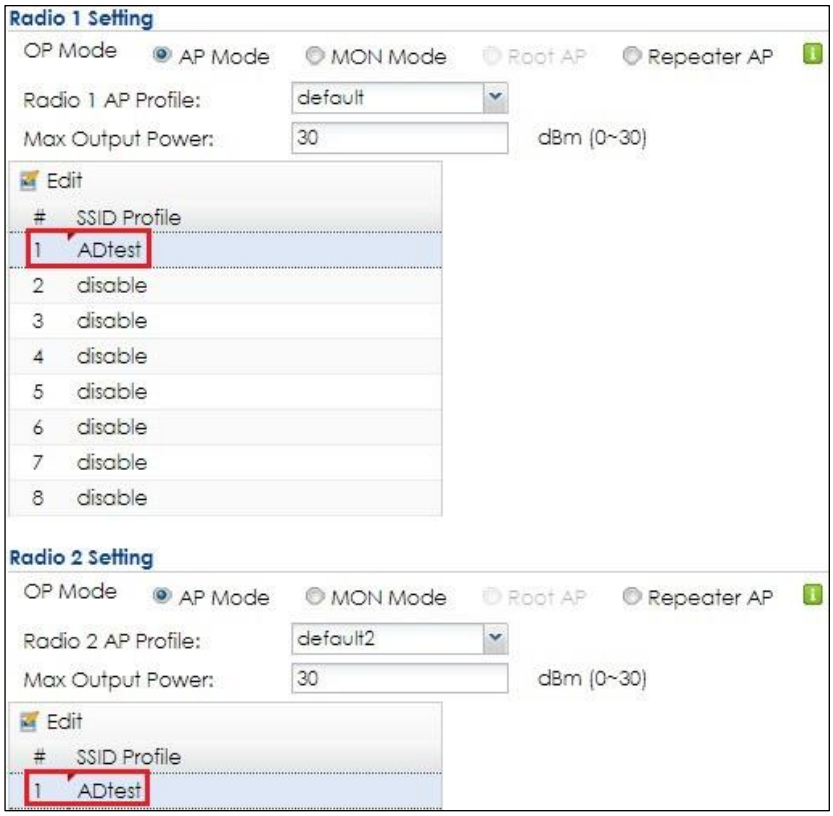
In **Authentication Settings**, select to **802.1x** and **Auth. Method** is **default**. Click **OK**.



2 Go to **CONFIGURATION > Object > AP Profile > SSID > SSID List**, click **add** to add a SSID for the connection with 802.1x security. Key in the **Profile Name** and **SSID**, and change **Security Profile** to **ADtest** which you configured in step1. Click **OK** to save.



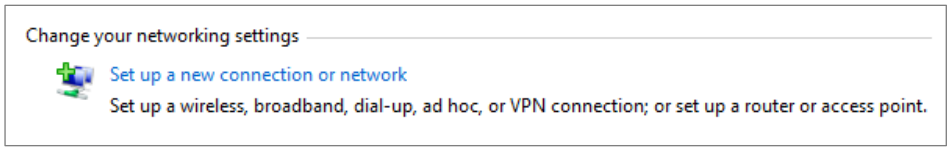
3 Go to **CONFIGURATION > Wireless > AP Management > AP Group**, select the **default** AP profile and edit. Select **ADtest** in the SSID Profile. Click **OK** to apply the SSID to AP.



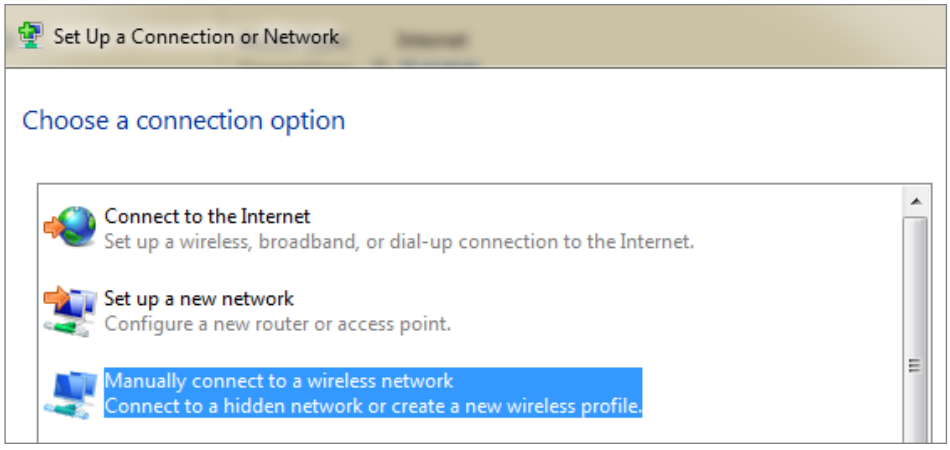
4.2.3 Test the Result

1 Before connecting the SSID, the computer needs to do some settings to make a connection successfully. Here is an example for Windows 7.

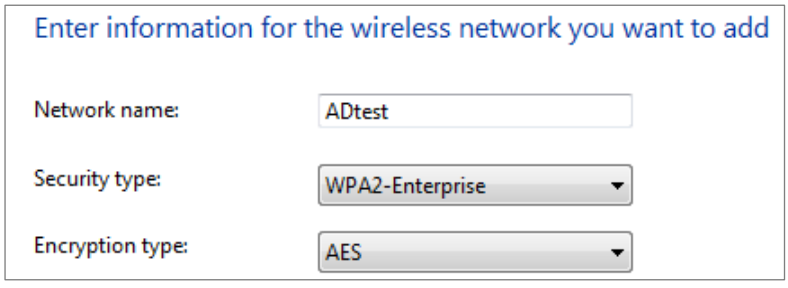
Open **Network and Sharing Center** in the computer, click **Set up a new connection or network** to build up a new network.



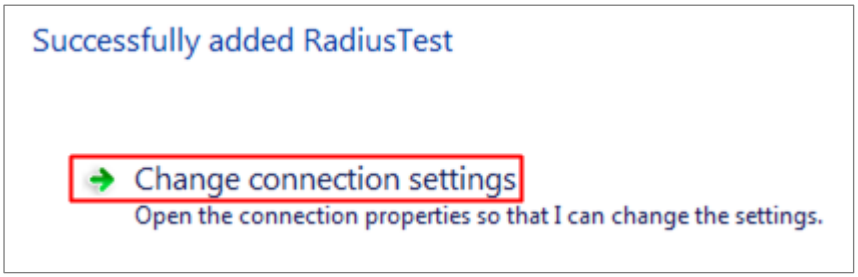
2 Select **Manually connect to a wireless network**. Click **Next**.



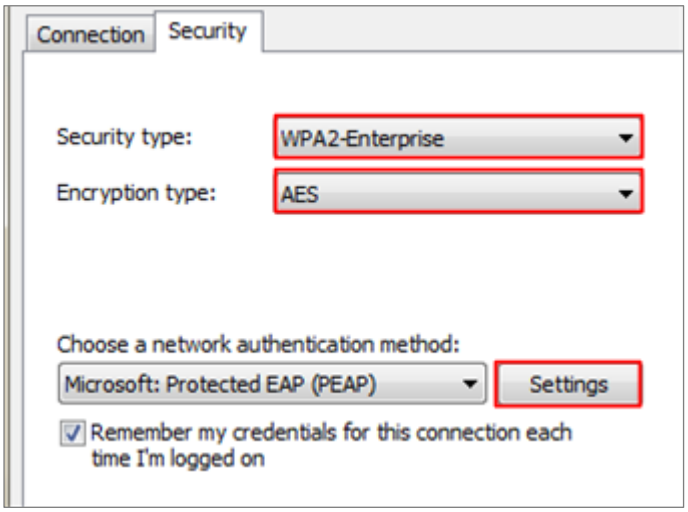
3 Key in the SSID in **Network name**, set the **Security type** to **WAP2-Enterprise**, and the **Encryption type** is **AES**. Click **Next**.



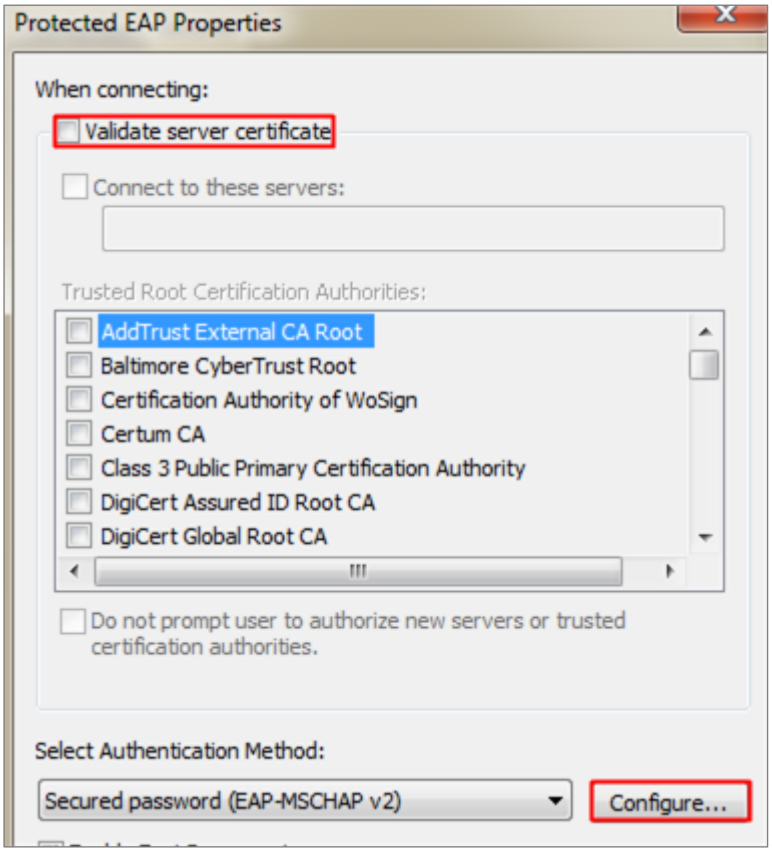
4 Select **Change connection settings**.



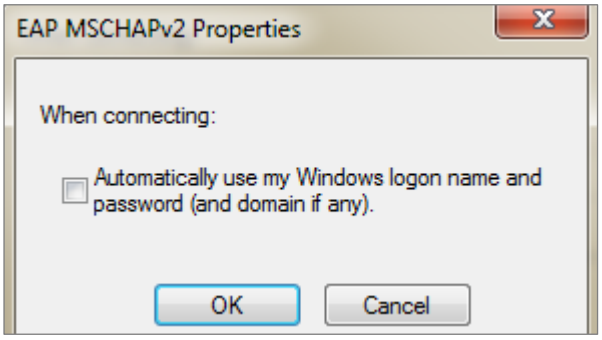
5 Change **Security type** to **WPA2-Enterprise**, **and Encryption type** is **AES**. Click **Settings**.



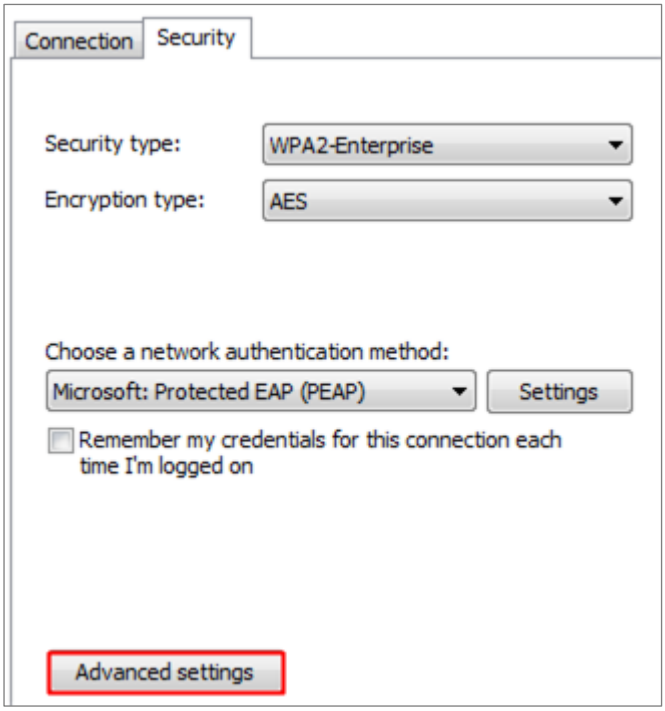
6 Uncheck **Validate server certificate** and click **Configure**.



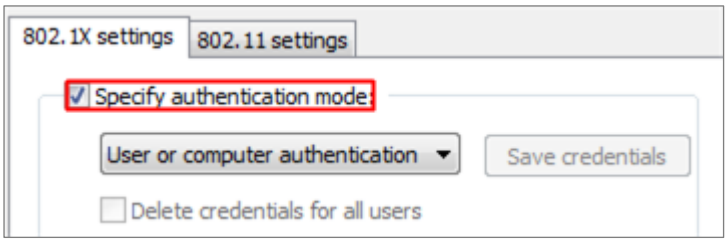
7 Uncheck the selection of the pop-up window. Click **OK**.



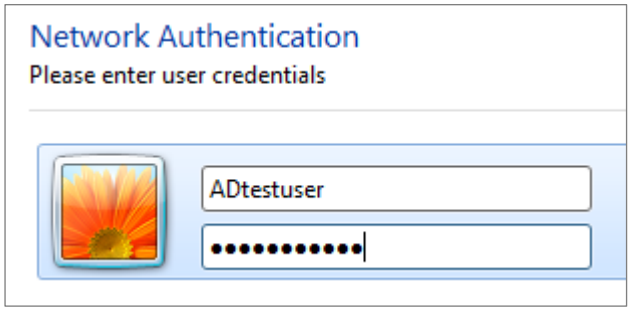
8 Go back to the security setting page and click **Advanced settings**.



9 Check **Specify authentication mode**. Click **OK** to save.

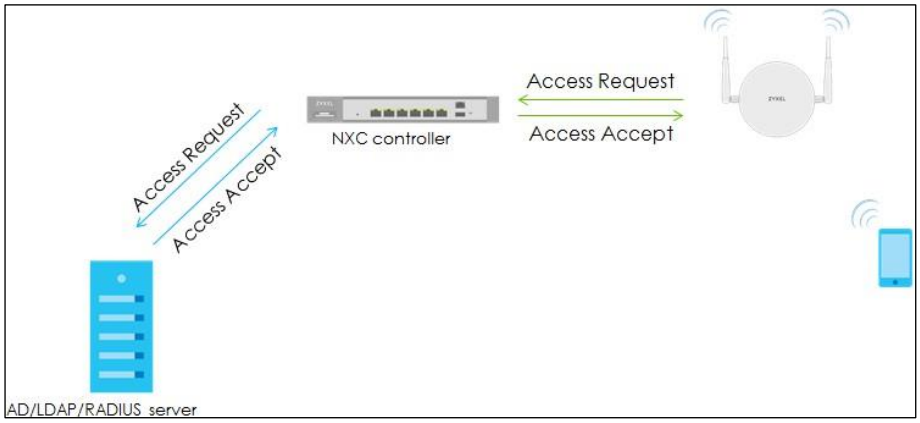


10 Select and connect to the pre-defined SSID "ADTest". Enter user credentials for authentication. After entering the correct ID and password, the wireless connection is set up successfully.



4.2.4 What Could Go Wrong

1 There are two kinds of **Radius Server Types** in security profile setting. **Internal** means the authentication is doing between the NXC controller and the AD server.



2 When the **Radius Server Types** change to **External**, it means the authentication is doing between the Managed AP and the Radius server. However, the AD server does not support EAP protocol, so it's necessary to install IAS or NPS on the AD server for EAP protocol.

4.3 How to Configure 802.1x to Secure the Wireless Environment with an External LDAP Server?

The example instructs how to set up the NXC controller with an external LDAP server. When the station wants to connect with the AP, you can use an AAA server to provide access control to your network. In this example, the LDAP server is external but not embedded in NXC controller, and the controller is already set to use the LDAP server for authentication.

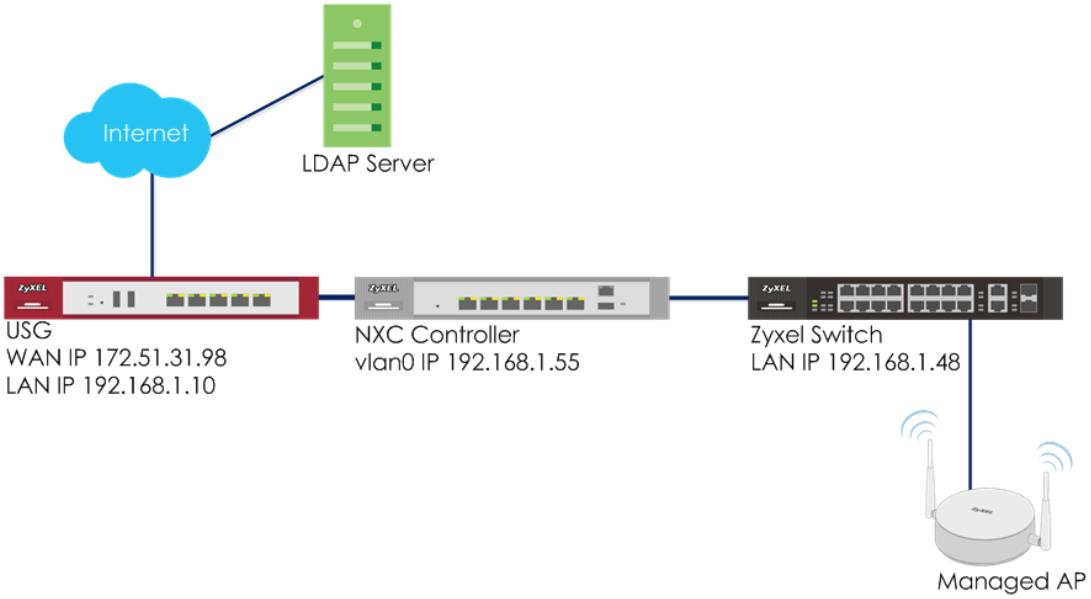


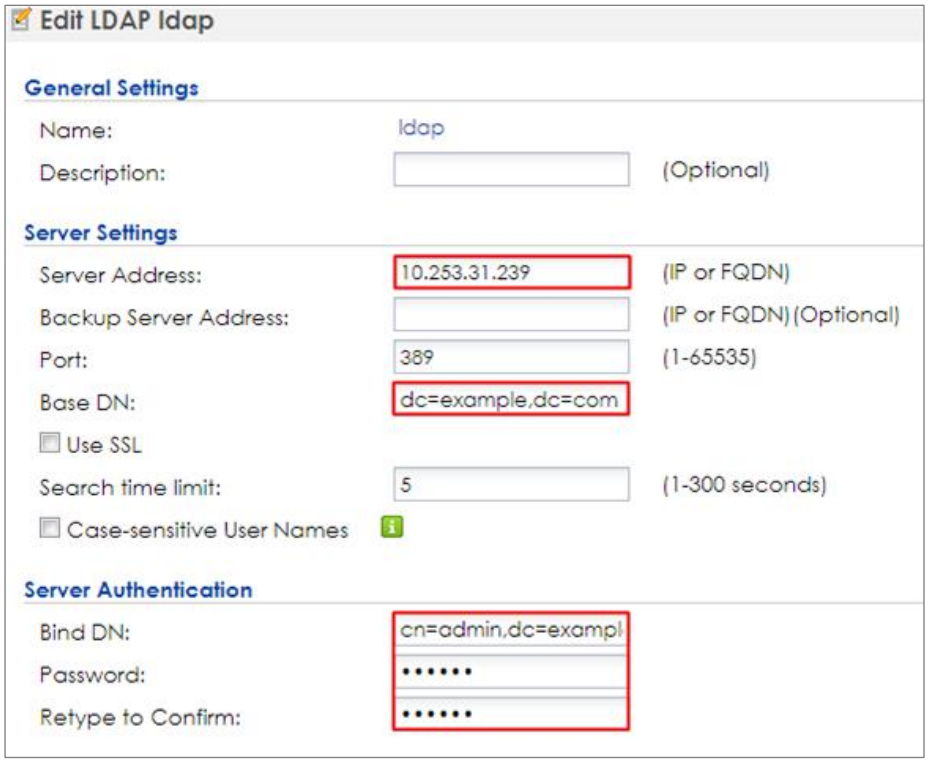
Figure 4.3 Set up AP/NXC with an External LDAP Server

Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC5500 (Firmware Version: 5.40), GS2210-8HP (Firmware Version: V4.30).

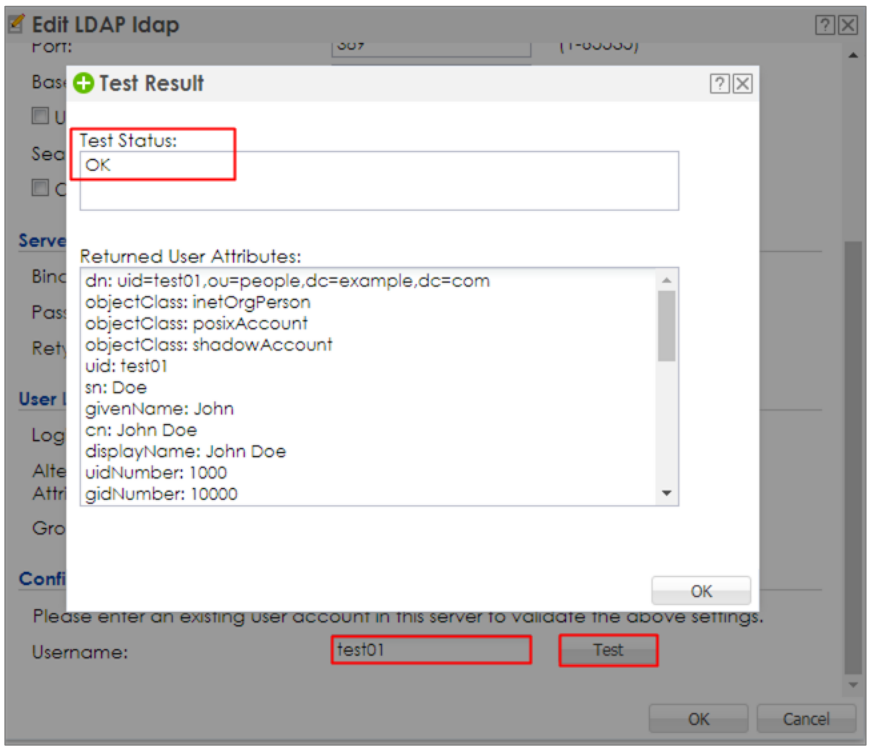
4.3.1 Configure LDAP Server Setting

1 Go to **CONFIGURATION > Object > AAA Server > LDAP**, click **#1 ldap**, and then click **Edit** to edit the LDAP server's information.

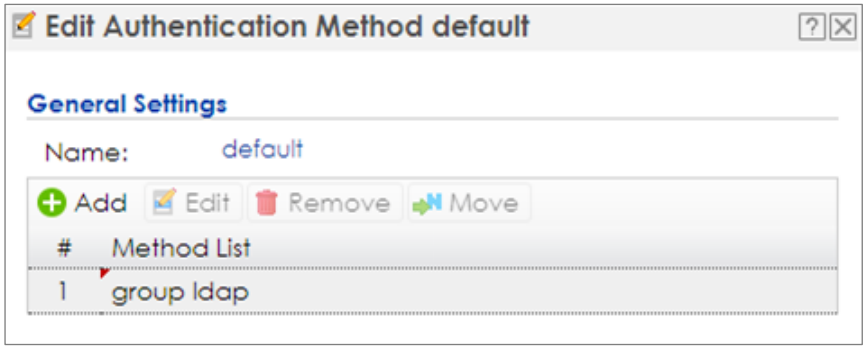
2 In **Server Settings**, enter **Server Address**. Here use **10.253.31.239** as the example. Go to LDAP server to check Base DN and Bind DN.



3 After finishing the configuration, enter **administrator** as the **Username** and click **Test** in **Configuration Validation**.



4 Go to **CONFIGURATION > Object > Auth. Method**. Select default method, and click **Edit**. Select the LDAP server you create. Click **OK**.



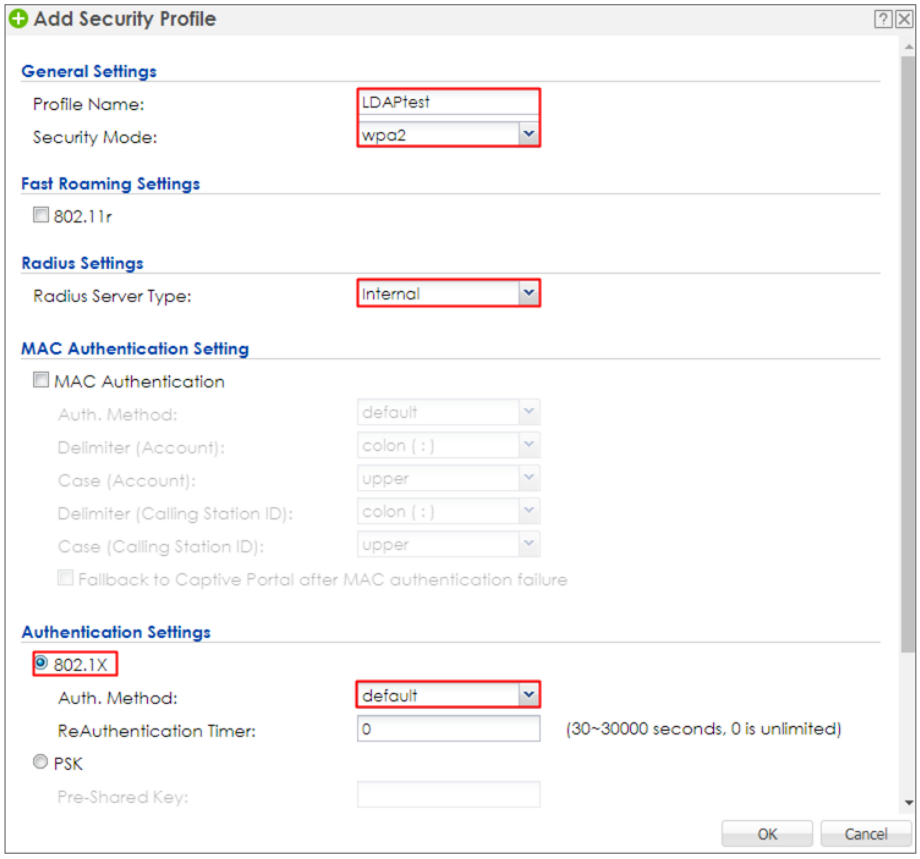
4.3.2 Configure AP Profile

1 Configure AP profile to use 802.1x authentication that user needs to log in with their ID and Password when connecting to AP's SSID. Go to **CONFIGURATION > Object > AP Profile > SSID > Security List**, click **Add** to add security for 802.1x.

In **General Settings**, enter the **Profile Name** and change **Security Mode** to **wpa2**.

In **Radius Settings**, select **Internal** and it means the authentication needs NXC to communicate with external LDAP server.

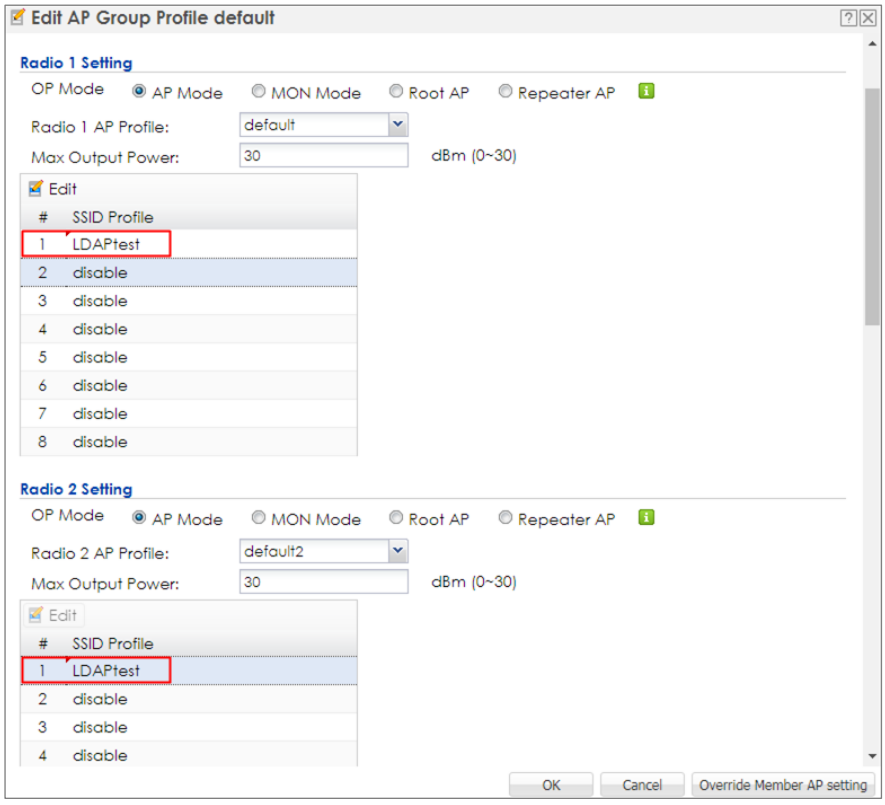
In **Authentication Settings**, select **802.1x** and **Auth. Method** is **default**. Click **OK**.



2 Go to **CONFIGURATION > Object > AP Profile > SSID > SSID List**, click **add** to add a SSID for the connection with 802.1x security. Key in the **Profile Name** and **SSID**, and change **Security Profile**

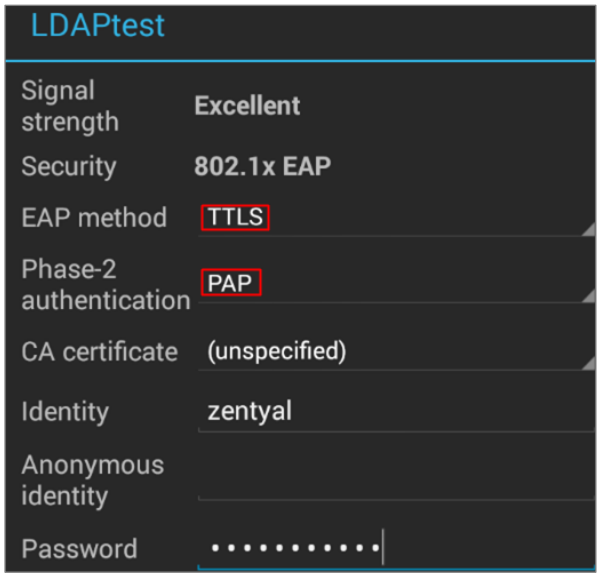
to **LDAP** which you configured in step1. Click **OK** to save.

3 Go to **CONFIGURATION > Wireless > AP Management > AP Group**, select the **default** AP profile and edit. Select **LDAPtest** in the SSID Profile. Click **Override Member AP Setting** to apply the SSID to the AP and click **Yes** in the pop-up window. Click **OK**.



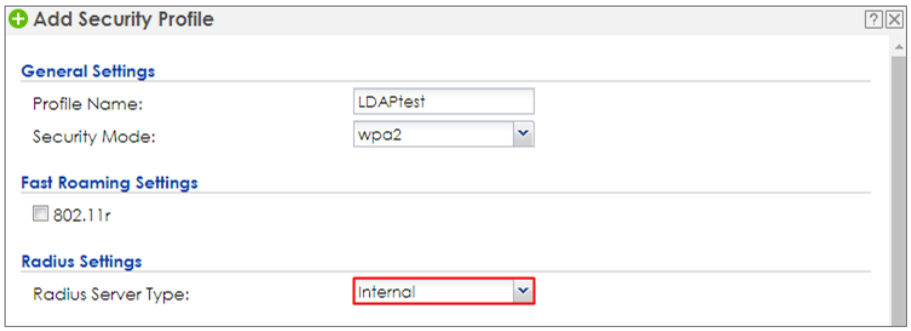
4.3.3 Test the Result

1 The LDAP can be use in Android phone for authentication. When connecting to the SSID, the **EAP method** is set to **TTLS**, and **Phase-2 authentication** is **PAP**. Enter the user ID and password to connect. The station and AP connected with correct ID and password.



4.3.4 What Could Go Wrong

1 The Radius server type is always **internal** in **CONFIGURATION > Object > AP Profile > SSID > Security List** because LDAP is not able to be used as the authentication server. It does not support **external** for LDAP server.



4.4 How to Configure 802.1x to Secure the Wireless Environment with an Internal RADIUS in NXC?

The example instructs how to set up NXC controller and let users do local authentication without external radius server. The user data base is set up in the NXC controller and the client can enter the username and password to do authentication via 802.1x.

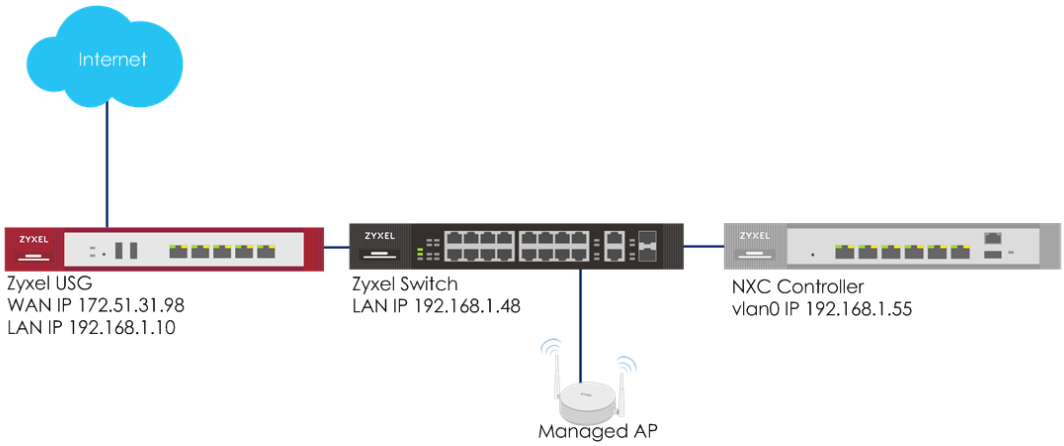
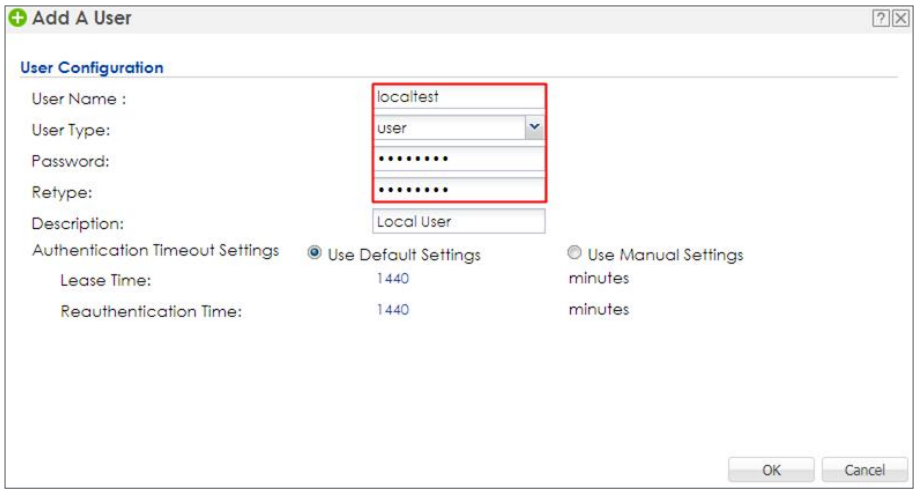


Figure 4.4 Local Authentication

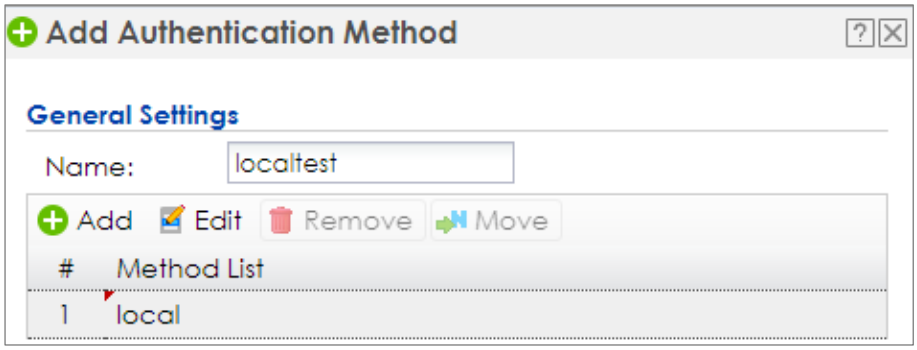
Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC2500 (Firmware Version: 5.30), GS2210-8HP (Firmware Version: V4.30).

4.4.1 Configure Authentication Method Setting

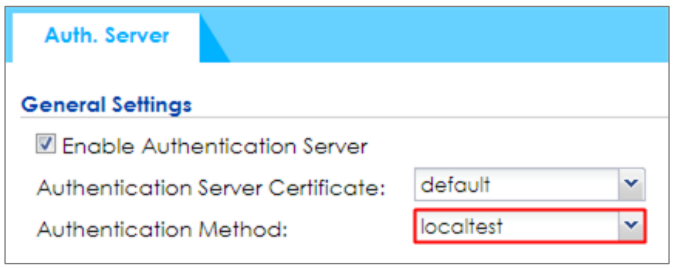
1 Go to **CONFIGURATION > Object > User/Group**, and click **add** to create a new user ID and password. Stations can log in to connect with the AP to access the Internet via this account.



2 Go to **CONFIGURATION > Object > Auth. Method**, and click **add** to create an authentication method. Enter the **Name** of this authentication method and select to local in the **Method List**.



3 Go to **CONFIGURATION > System > Auth. Server**, and set **Authentication Method** to **localtest** which is created in step 2.



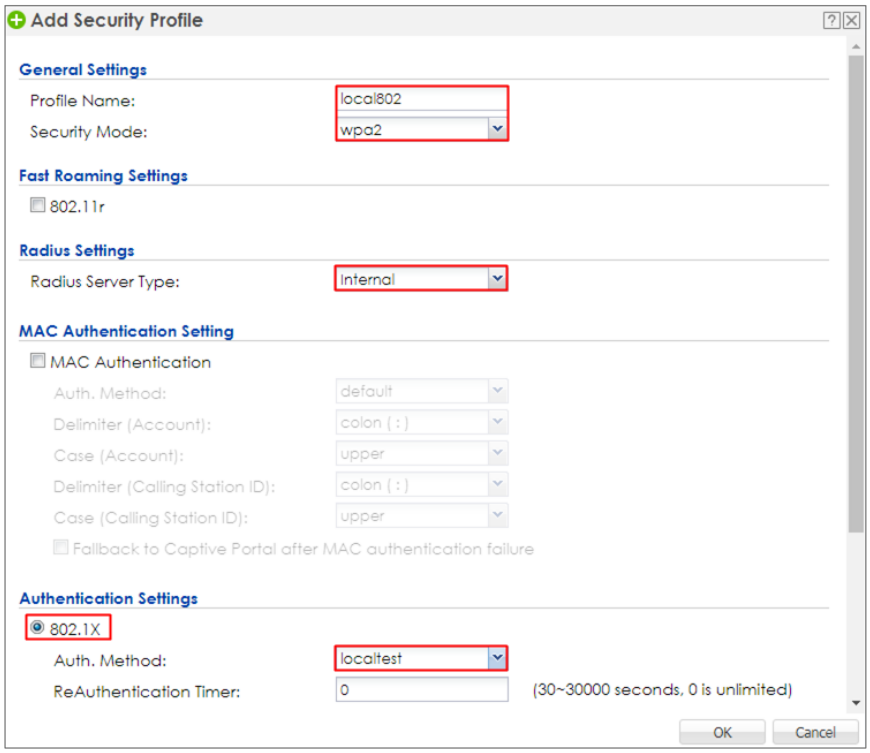
4.4.2 Configure AP Profile

1 Configure the AP profile to use 802.1x authentication that user needs to log in with their ID and Password when connecting to the AP's SSID. Go to **CONFIGURATION > Object > AP Profile > SSID > Security List**, and click **Add** to add security for 802.1x.

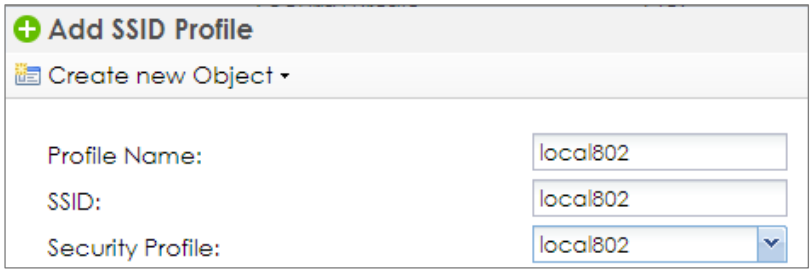
In **General Settings**, enter the **Profile Name** and change **Security Mode** to **wpa2**.

In **Radius Settings**, select to **Internal** and it means the authentication needs NXC to communicate with external LDAP server.

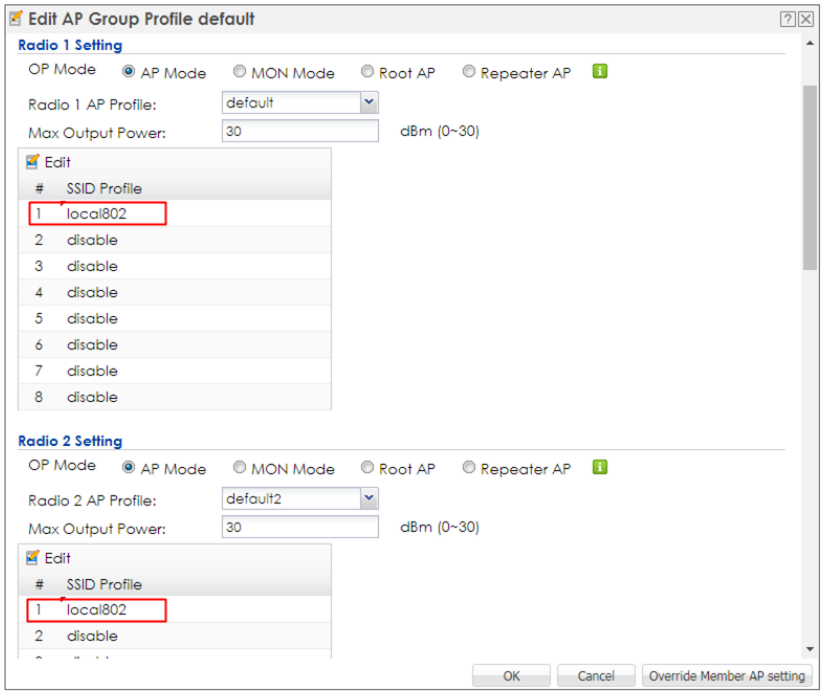
In **Authentication Settings**, select **802.1x** and **Auth. Method** is **localtest**. Click **OK**.



2 Go to **CONFIGURATION > Object > AP Profile > SSID > SSID List**, click **add** to add a SSID for the connection with 802.1x security. Key in the **Profile Name** and **SSID**, and change **Security Profile** to **local802** which is created in step1. Click **OK** to save.



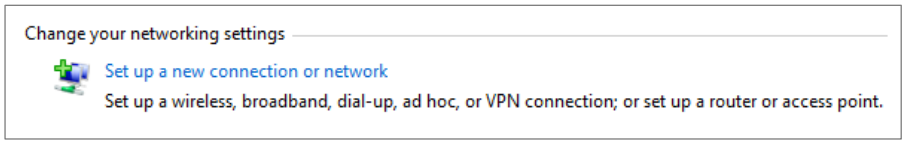
3 Go to **CONFIGURATION > Wireless > AP Management > AP Group**, select the **default** AP profile and edit. Select **local802** in the SSID Profile. Click **Override Member AP Setting** to apply the SSID to the AP and click **Yes** in the pop-up window. Click **OK**.



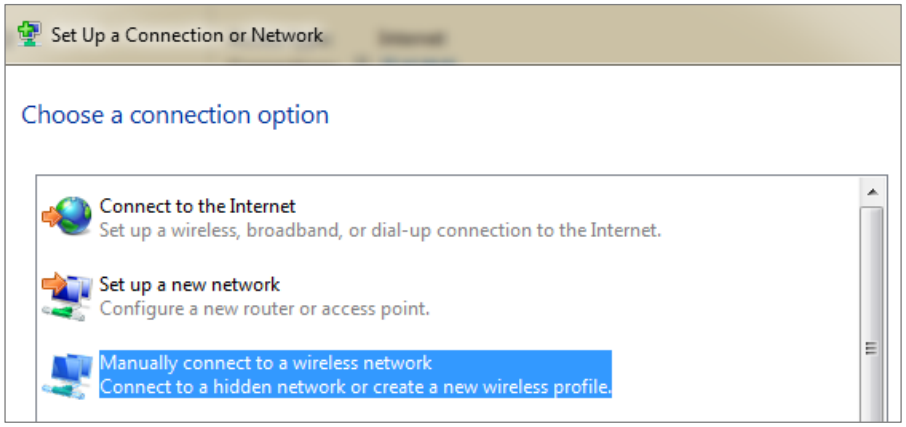
4.4.3 Test the Result

1 Before connecting the SSID, the computer needs to do some settings to make the connection successfully. Here is an example for Windows 7.

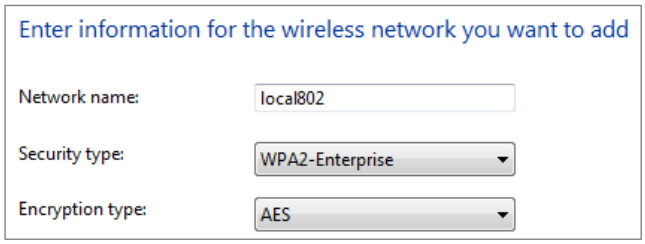
Opening **Network and Sharing Center** in computer, click **Set up a new connection or network** to build up a new network.



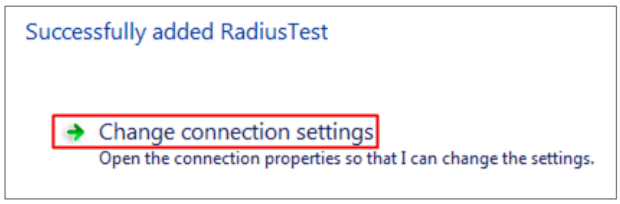
2 Select **Manually connect to a wireless network**. Click **Next**.



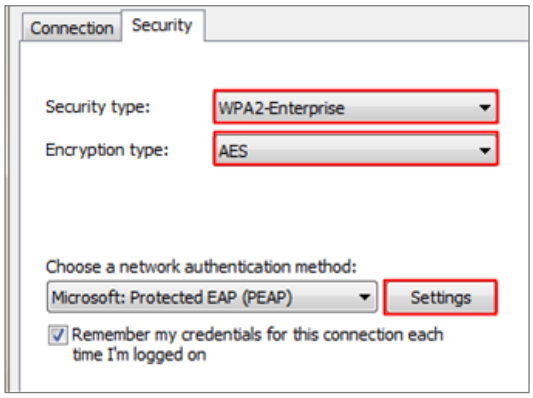
3 Key in the SSID to **Network name** and change the **Security type** to **WAP2-Enterprise**, and the **Encryption type** is **AES**. Click **Next**.



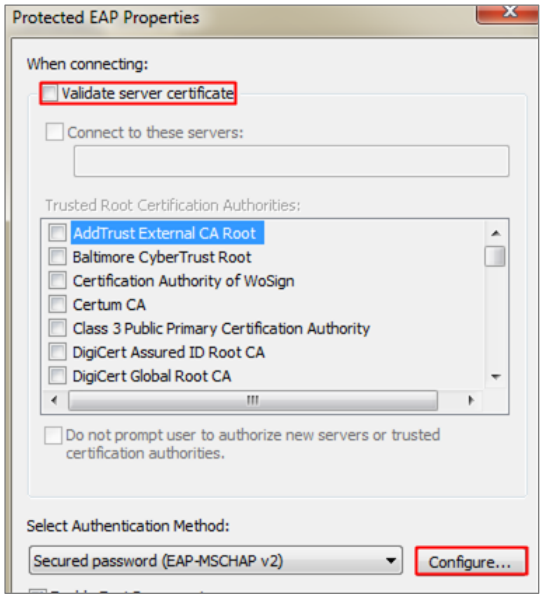
4 Select **Change connection settings**.



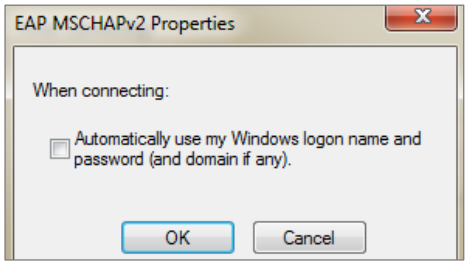
5 Select **Security type** to **WPA2-Enterprise**, **and Encryption type** is **AES**. Click **Settings**.



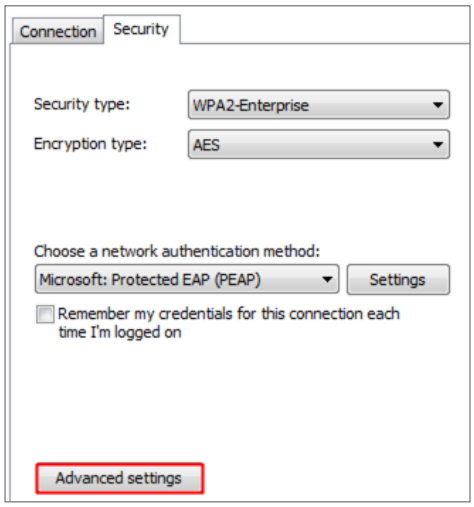
6 Uncheck **Validate server certificate** and click **Configure**.



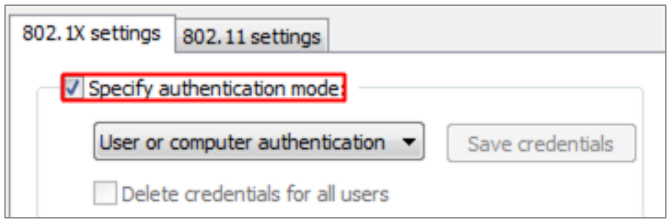
7 Uncheck the selection of pop-up window. Click **OK**.



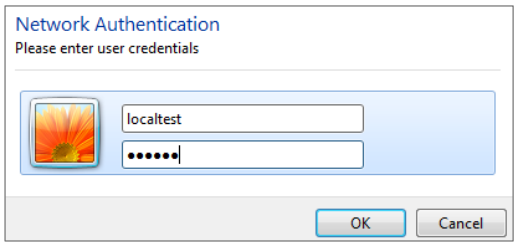
8 Go back to the security setting page and click **Advanced settings**.



9 Check **Specify authentication mode**. Click **OK** to save.



10 Select and connect to the pre-defined SSID "ADTest". Enter user credentials for authentication. After entering the correct ID and password, the wireless connection is set up successfully.



4.5 How to Configure 802.1x to secure the Wireless Environment with Dynamic VLAN by Using External AAA server?

When the station wants to connect with the AP, you can use an AAA server to provide access control to your network. In this example, assuming there are two stations in different groups and they can connect to the same SSID for accessing the Internet, but get IPs in different subnets because of the dynamic VLAN settings.
There are two ways for dynamic VLAN settings. One is to use the radius server attribute, and the other is to use the NXC controller external user group with radius or AD server. The example instructs how to set up dynamic VLAN by using external AAA servers with these two ways.

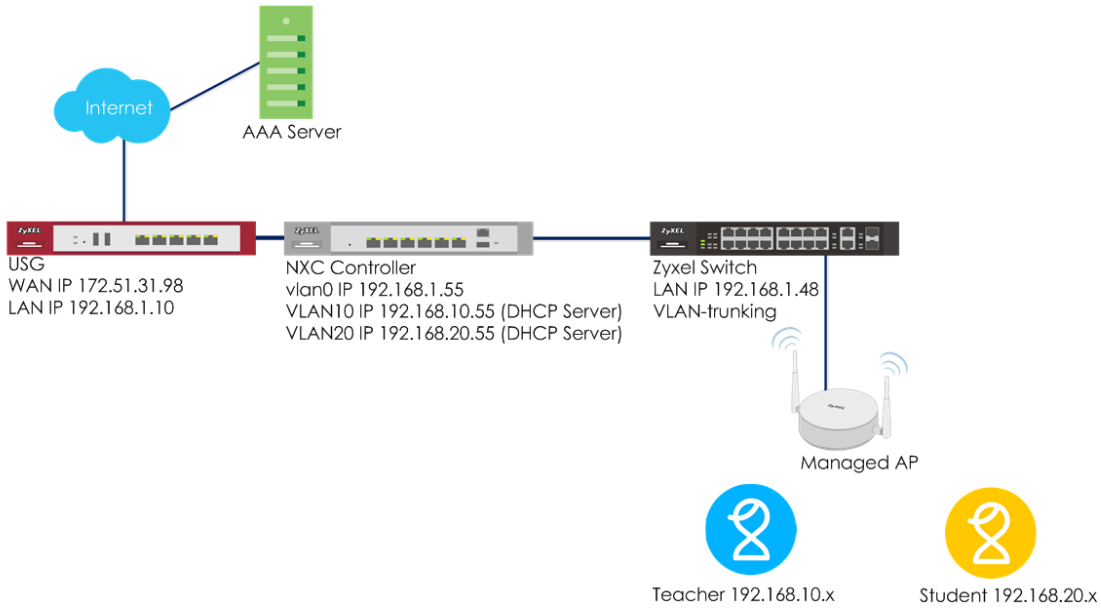
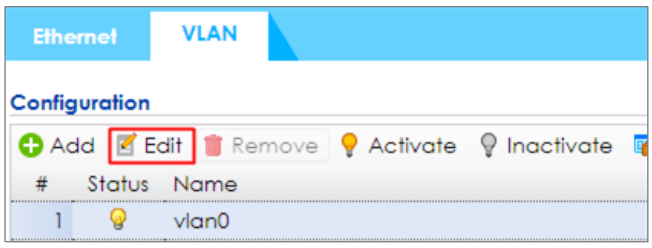


Figure 4.5 Dynamic VLAN with NXC controller using external Radius Server

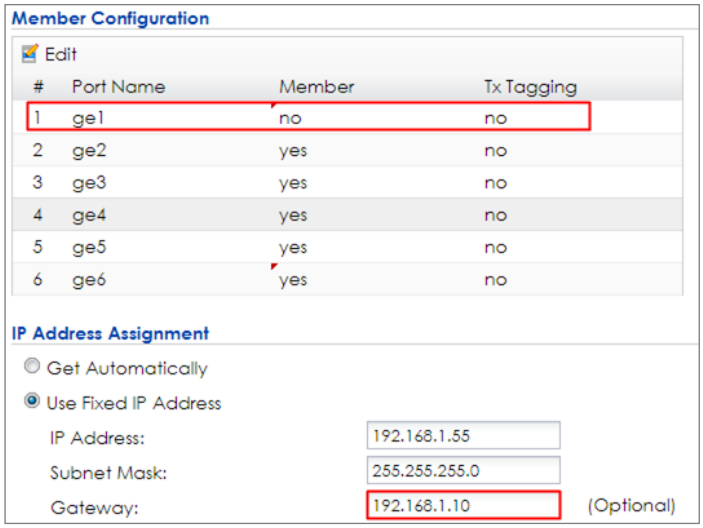
Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC2500 (Firmware Version: 5.30), GS2210-8HP (Firmware Version: V4.30).

4.5.1 Configure Interface

1 Go to **CONFIGURATION > Network > Interface > VLAN**, click **vlan0** and **Edit** it.

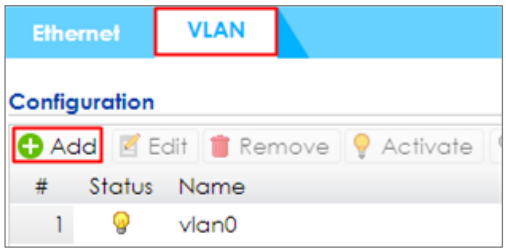


2 Set **ge1** (P1) to not be vlan0's member by selecting no in **Member Configuration**. Set the gateway IP in **IP Address Assignment**. Click **OK** to save. Connect ge1 (P1) to the USG's LAN port.



3 Connect Switch to NXC ge2 (P2), and APs all connect to the switch.

4 In the NXC, go to **CONFIGURATION > Network > Interface > VLAN**. Click **Add** to create a new VLAN configuration.



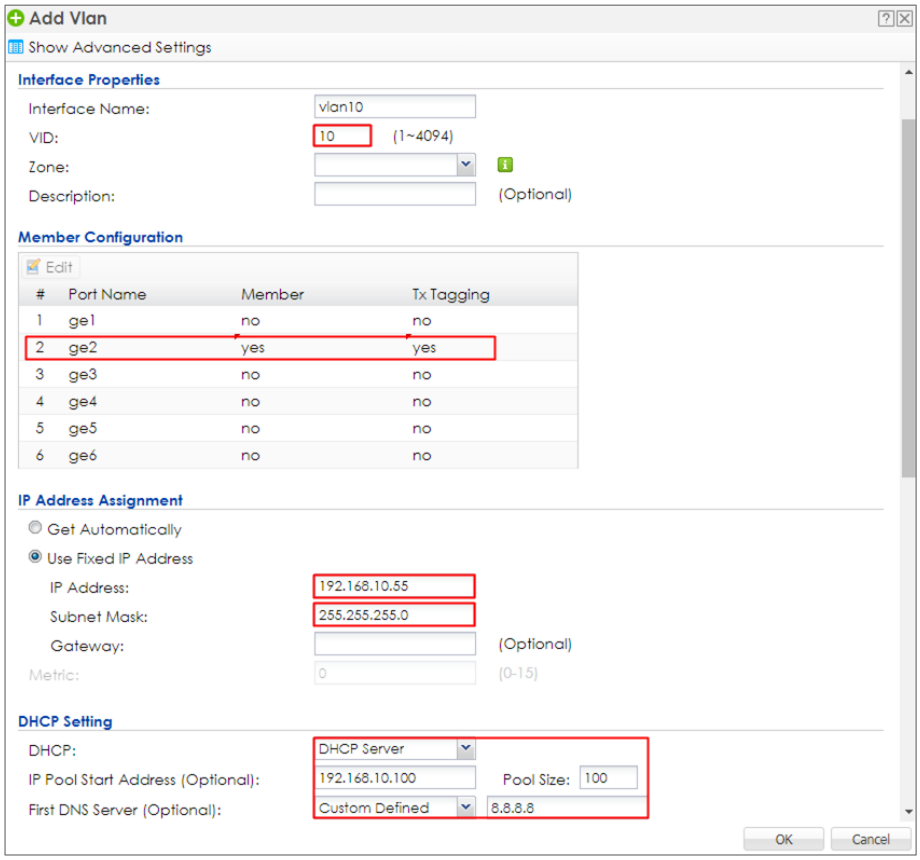
5 In General Settings, check **Enable**.

In Interface Properties, key in Interface Name: **vlan10**; VID: **10**

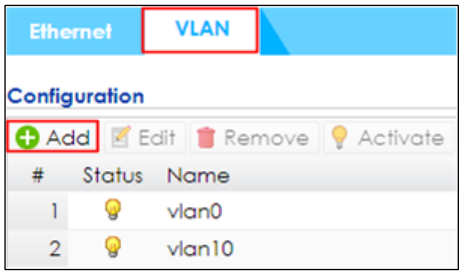
In Member Configuration, set ge2 to be **Member** and **Tx Tagging**.

In IP Address Assignment, **Use Fixed IP Address** and key in **IP Address**, **Subnet Mask**, **and Gateway**.

In DHCP Setting, select **DHCP server** and key in **IP Pool Start Address** and **Pool Size**. **First DNS server** change to **Customer Defined 8.8.8.8**. The users in VLAN 10 get an IP from this DHCP server. Click **OK**.



6 Click **Add** to create vlan20 in **CONFIGURATION > Network > Interface > VLAN**.



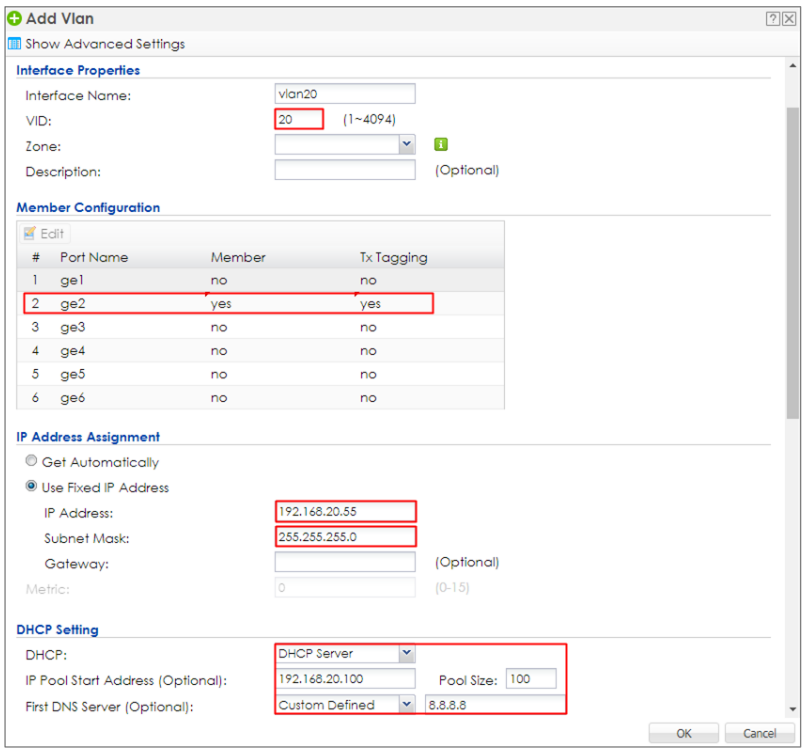
7 In General Settings, check **Enable**.

In Interface Properties, key in Interface Name: **vlan20**; VID: **20**

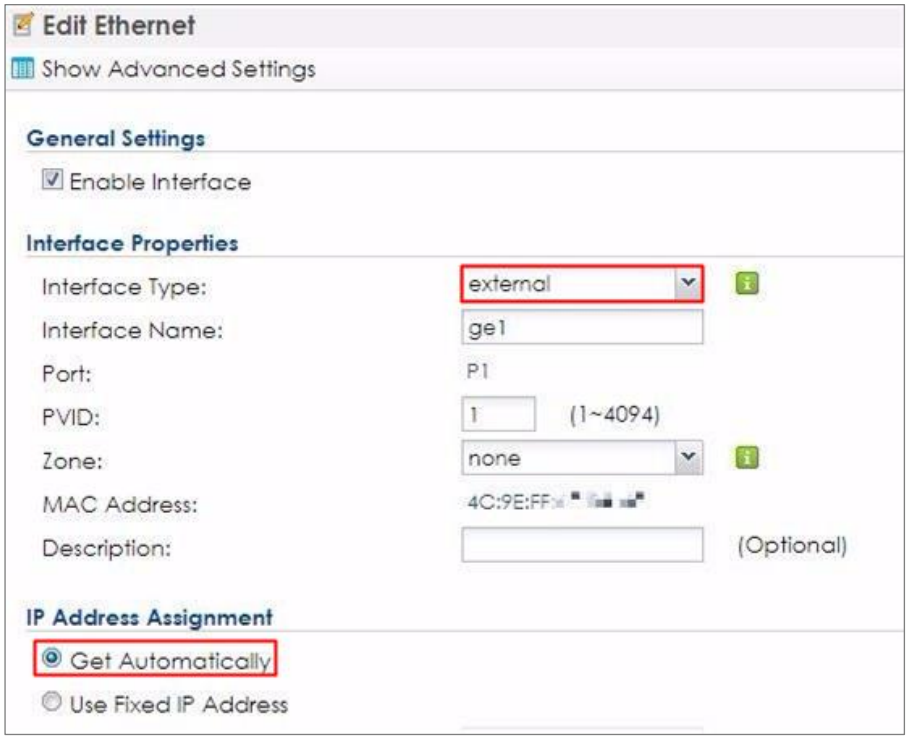
In Member Configuration, set ge2 to be **Member** and **Tx Tagging**.

In IP Address Assignment, **Use Fixed IP Address** and key in **IP Address**, **Subnet Mask**, **and Gateway**.

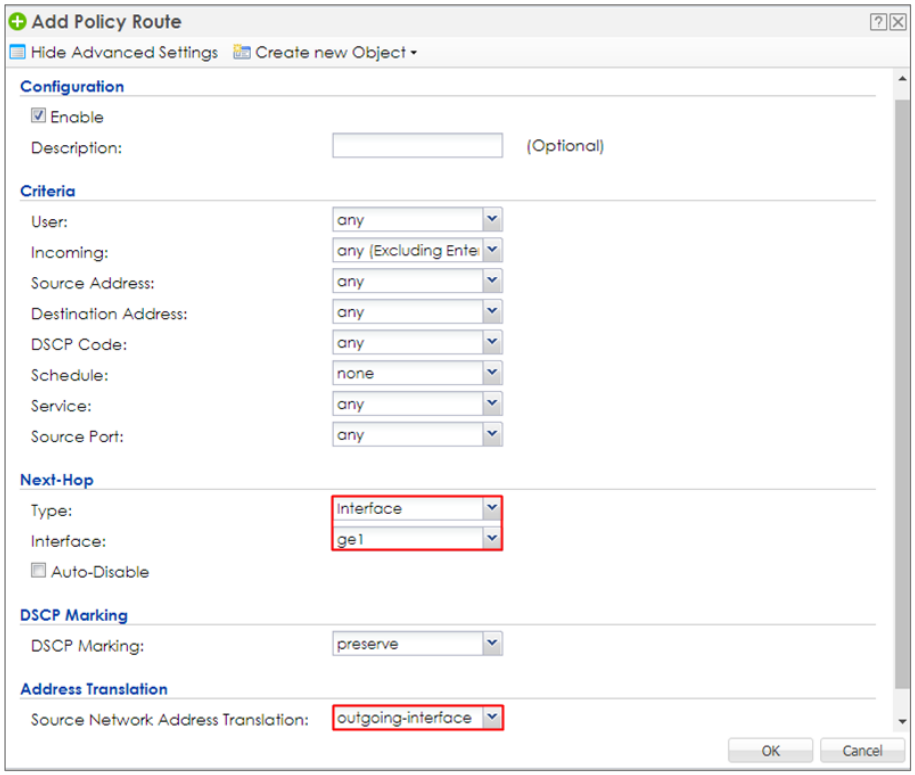
In DHCP Setting, select **DHCP server** and key in **IP Pool Start Address** and **Pool Size**. **First DNS server** change to **Customer Defined 8.8.8.8**. The users in VLAN 20 get an IP from this DHCP server. Click **OK**.



8 Go to **CONFIGURATION > Network > Interface > Ethernet**, select **ge1** and **Edit** it. Change the **Interface Type** to **external** and **Get Automatically** in **IP Address Assignment**.



9 Go to **CONFIGURATION > Network >Routing > Policy Route** and click **Add** to add a policy route. Select **Interface ge1** in **Next-Hop**, and **outgoing-interface** in **Address Translation** after clicking **Show Advanced Settings**.



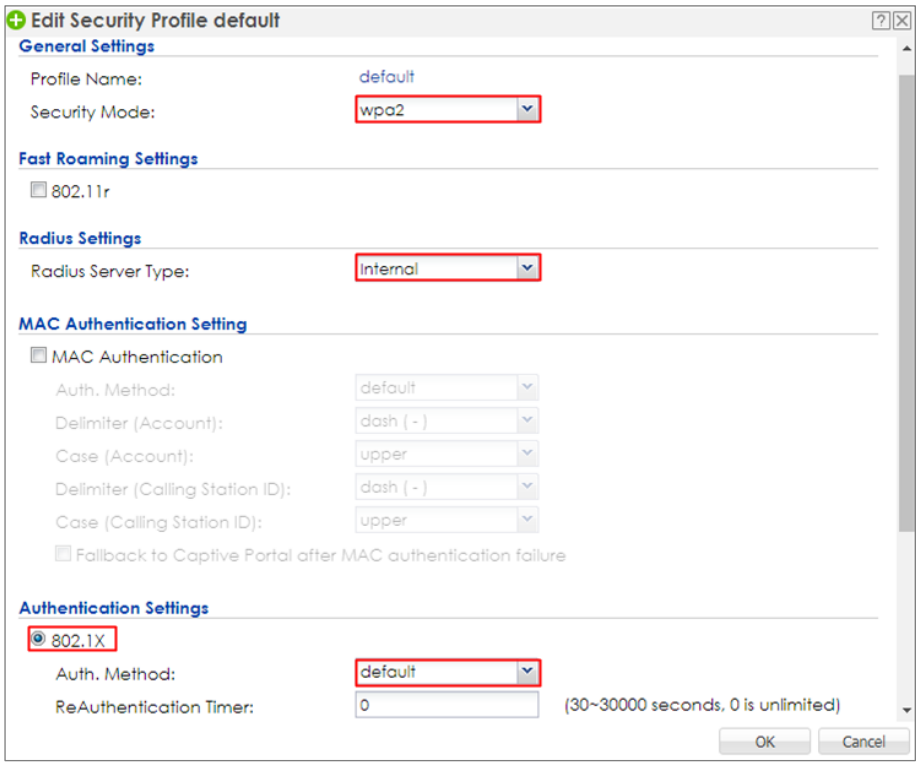
4.5.2 Configure AP Profile

1 Configure the AP profile to use 802.1x authentication that the user needs to log in with their ID and Password when connecting to the AP's SSID. Go to **CONFIGURATION > Object > AP Profile > SSID > Security List**, select the **default** AP profile and edit.

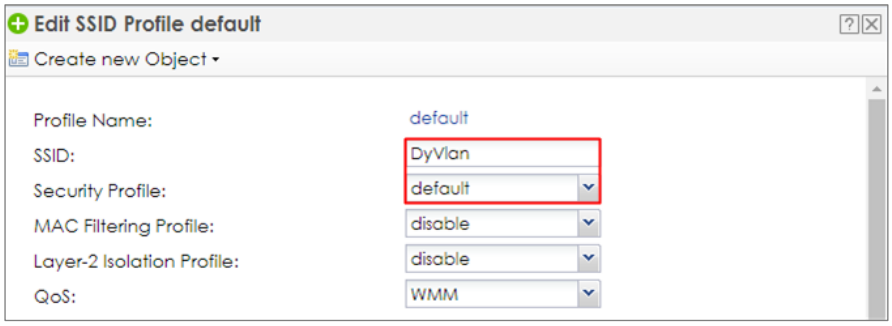
In **General Settings**, enter the **Profile Name** and change **Security Mode** to **wpa2**.

In **Radius Settings**, change to **Internal** and it means the authentication needs NXC to communicate with external radius server.

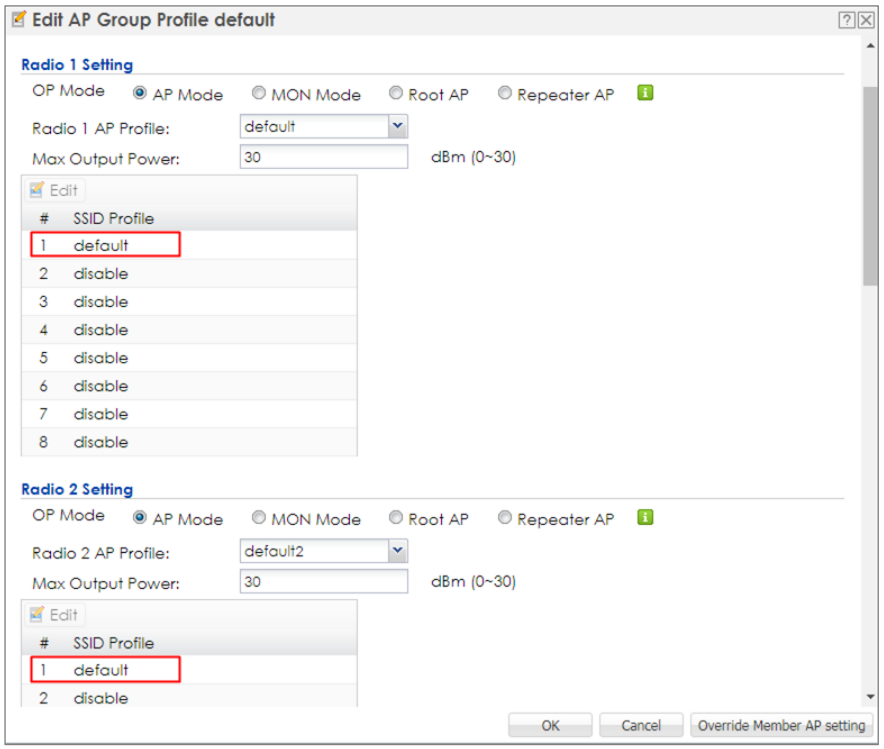
In **Authentication Settings**, change to **802.1x** and **Auth. Method** is **default**. Click **OK**.



2 Go to **CONFIGURATION > Object > AP Profile > SSID > SSID List**, and select the **default** AP profile and edit. Key in the **Profile Name** and **SSID**, and change **Security Profile** to **default** which is created in step1. Click **OK** to save.



3 Go to **CONFIGURATION > Wireless > AP Management > AP Group**, select the **default** AP profile and edit. Select **default** in the SSID Profile #1 in both radio1 and radio2. Click **OK** to apply the settings.



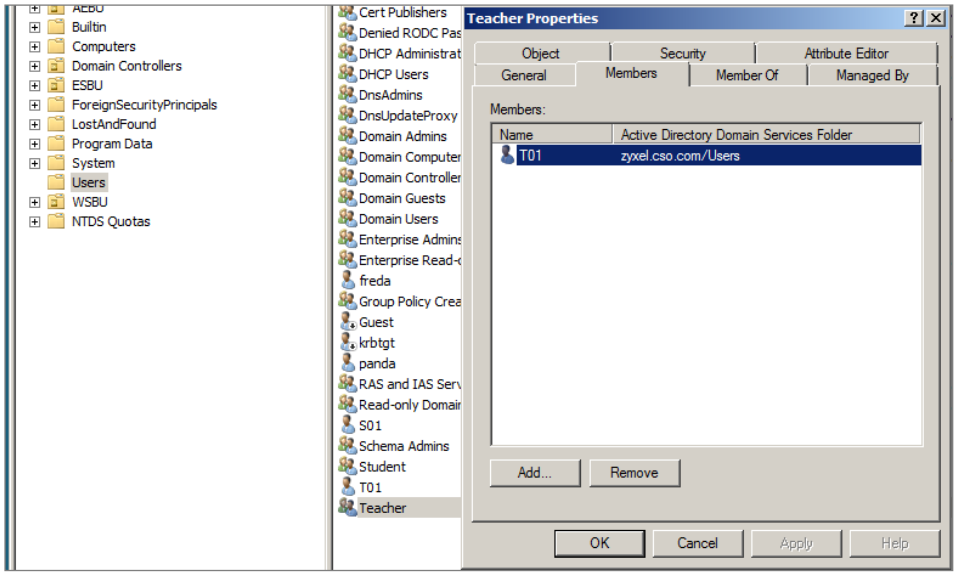
4.5.3 Configure AAA Server Setting

4.5.3.1 Dynamic VLAN by radius server attribute

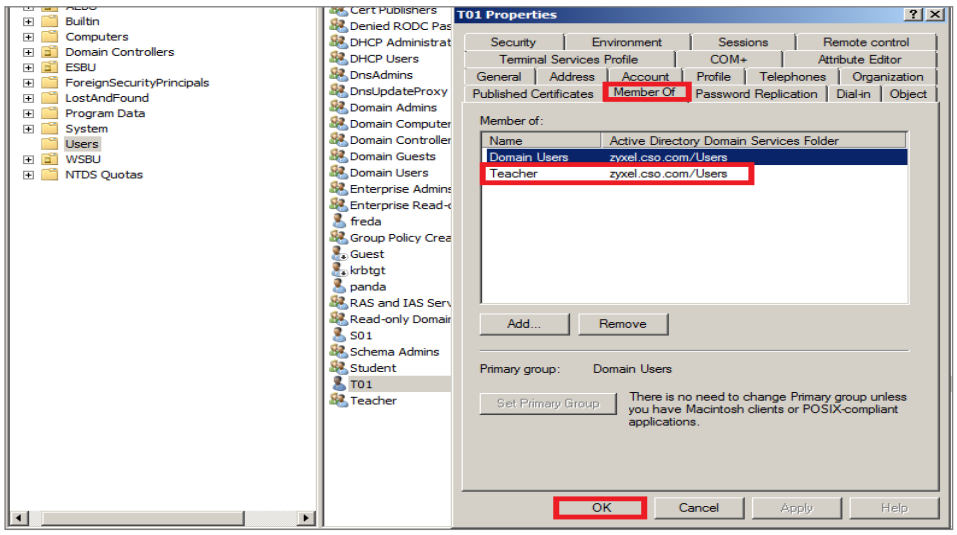
A. Settings on Radius Server

Here is an example by using Windows 2008 server with NPS and AD server.

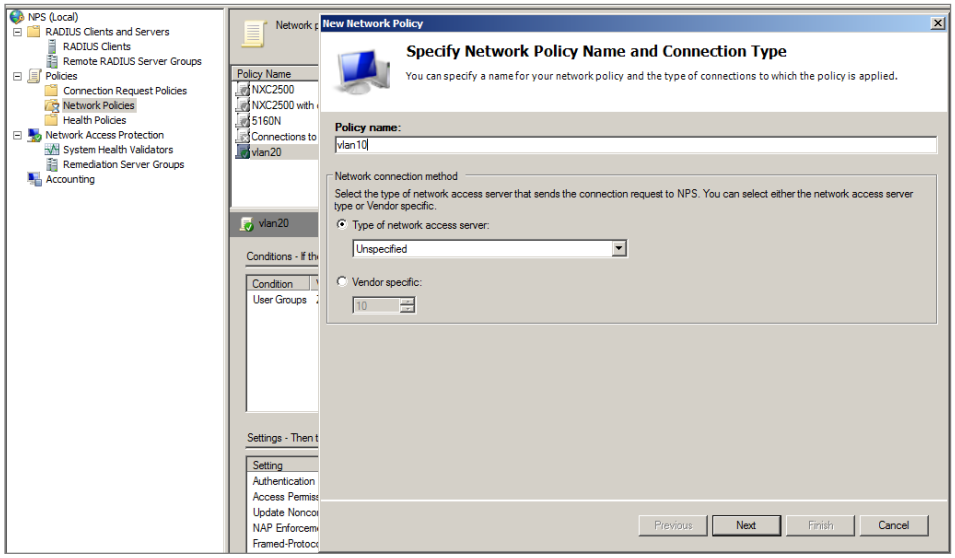
1 Add the user to a group in AD server.



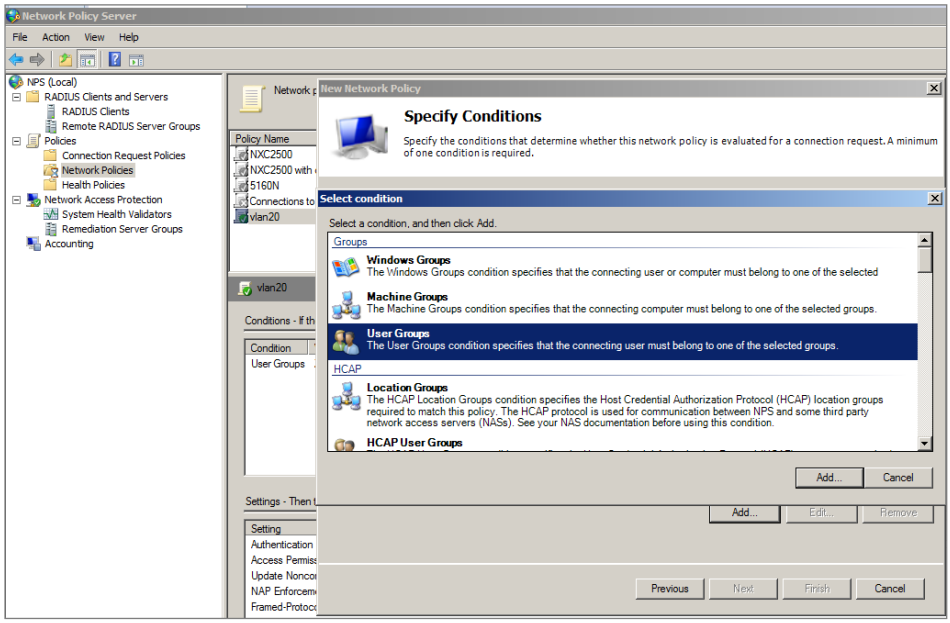
2 Go to **Member Of** to check if the member, **Teacher**, is added successfully in the group.



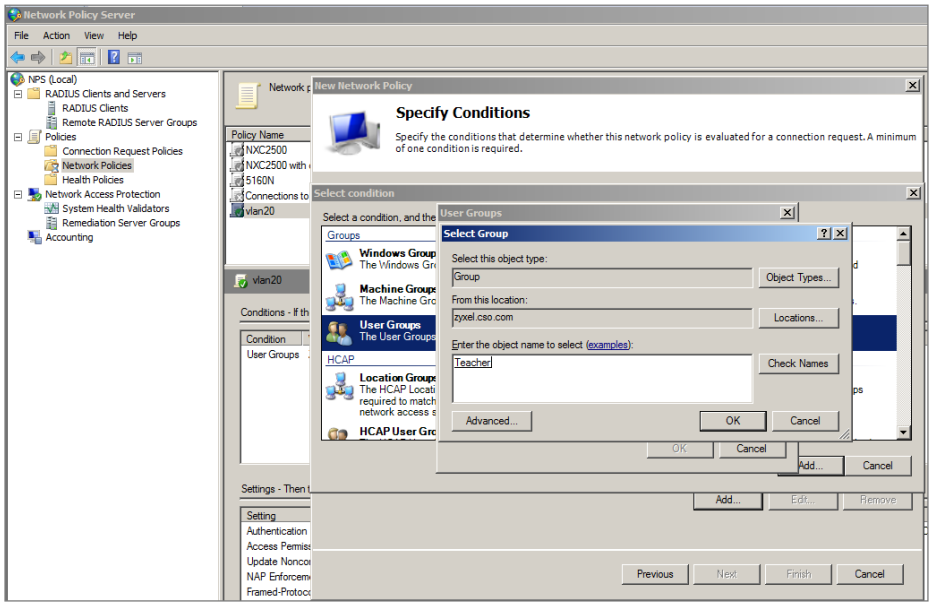
3 Add a new Network Policy of NPS server for a group and then click '**Next**'.



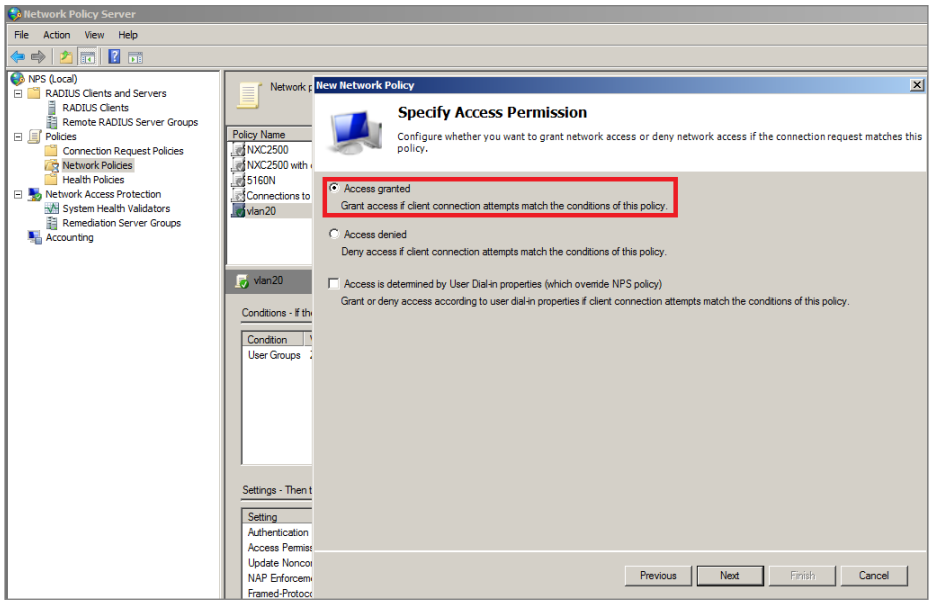
4 Add 'User Group' condition.



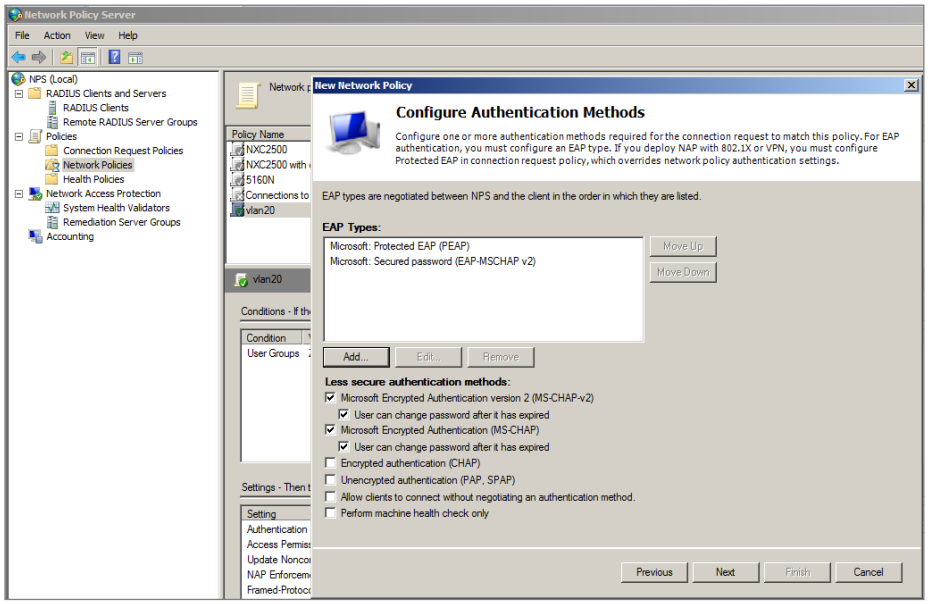
5 Select the group which is set in AD server.



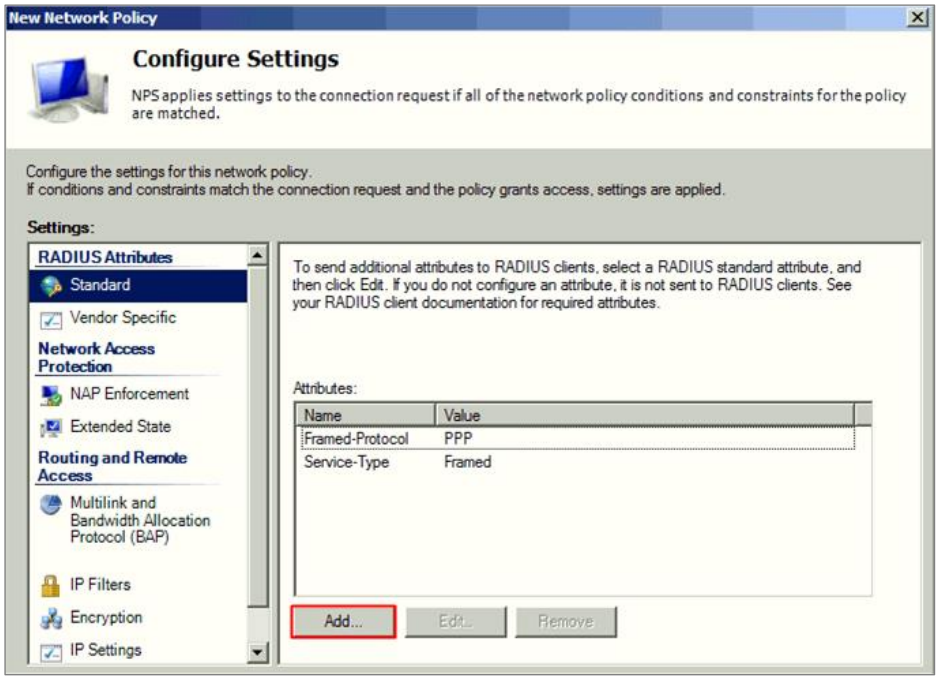
6 Set the access permission and click '**Next**'.

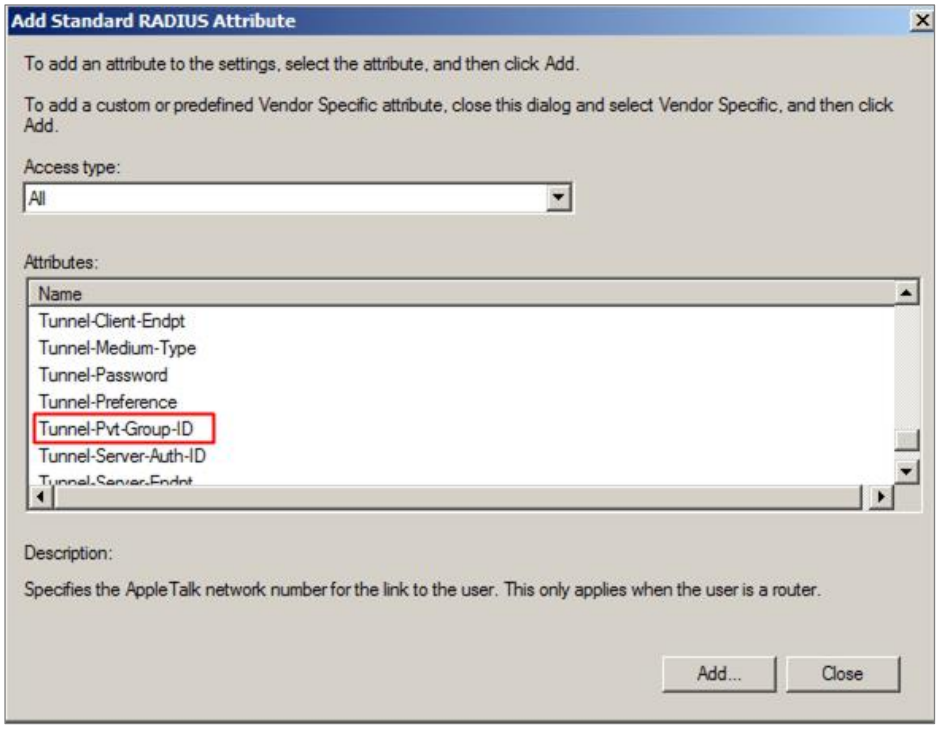


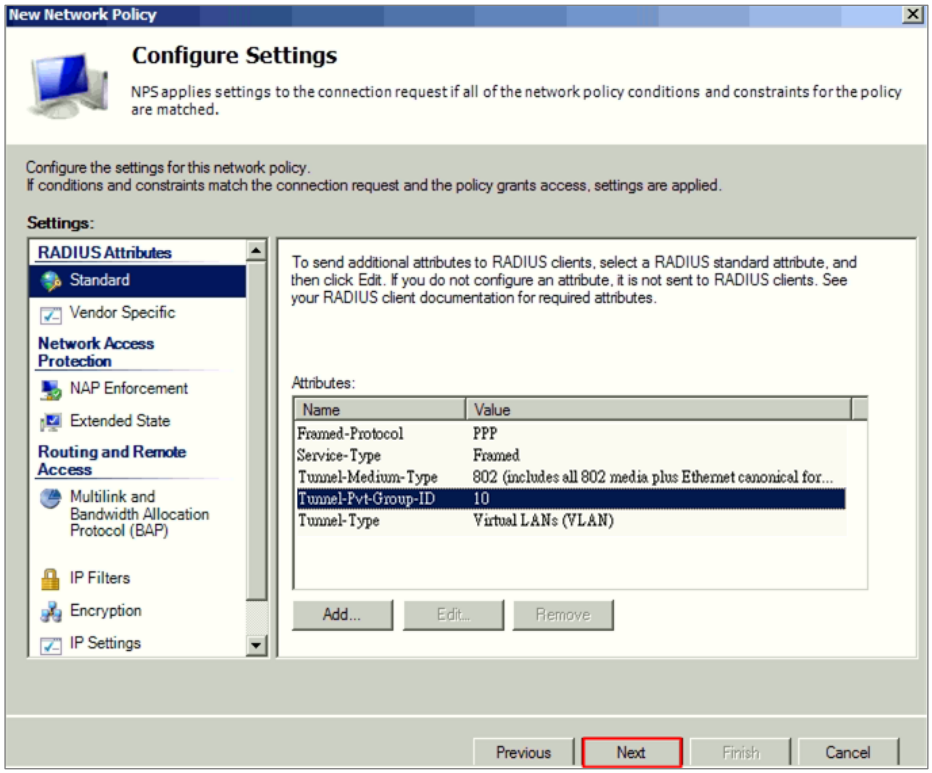
7 Configuration Authentication Methods and click '**Next**'.



8 There are three attribute needed to add, Tunnel-Medium-Type, Tunnel-Pvt-Group-ID, Tunnel Type. Set the attribute configuration and click '**Next**'.

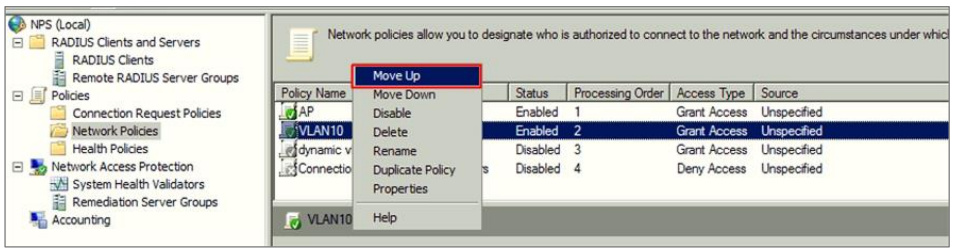



Add Standard RADIUS Attribute
To add an attribute to the settings, select the attribute, and then click Add.
To add a custom or predefined Vendor Specific attribute, close this dialog and select Vendor Specific, and then click Add.
Access type:
All
Attributes:
Name
Tunnel-Client-Endpt
Tunnel-Medium-Type
Tunnel-Password
Tunnel-Preference
Tunnel-Pvt-Group-ID
Tunnel-Server-Auth-ID
Description:
Specifies the AppleTalk network number for the link to the user. This only applies when the user is a router.
Add...
Close


New Network Policy
Configure Settings
NPS applies settings to the connection request if all of the network policy conditions and constraints for the policy are matched.
Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.
Settings:
RADIUS Attributes
Standard
Vendor Specific
Network Access Protection
NAP Enforcement
Extended State
Routing and Remote Access
Multilink and Bandwidth Allocation Protocol (BAP)
IP Filters
Encryption
IP Settings
To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.
Attributes:
Name
Value
Framed-Protocol
PPP
Service-Type
Framed
Tunnel-Medium-Type
802 (includes all 802 media plus Ethernet canonical for...
Tunnel-Pvt-Group-ID
10
Tunnel-Type
Virtual LANs (VLAN)
Add...
Edit...
Remove
Previous
Next
Finish
Cancel

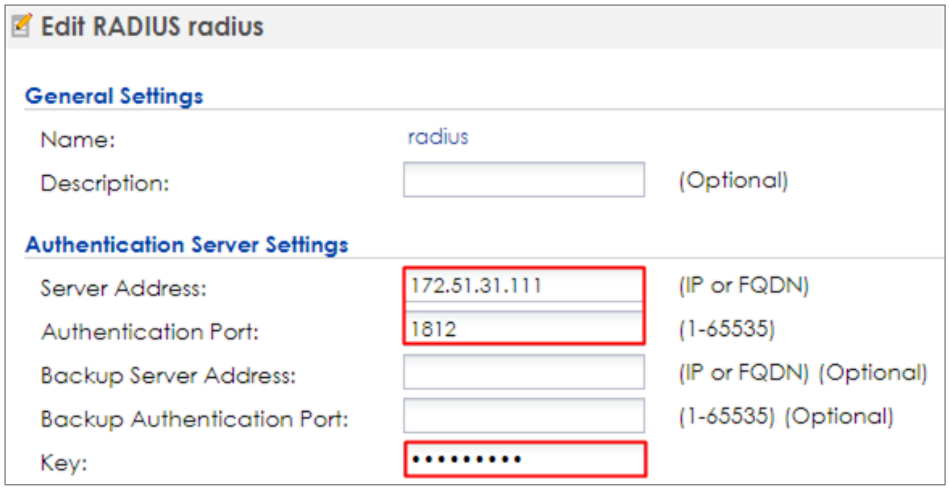
9 Do the same steps to create the other group for other users.

10 Move up the policies to top in Network Policies of NPS to make sure it's the first one to hit when the traffic is come.

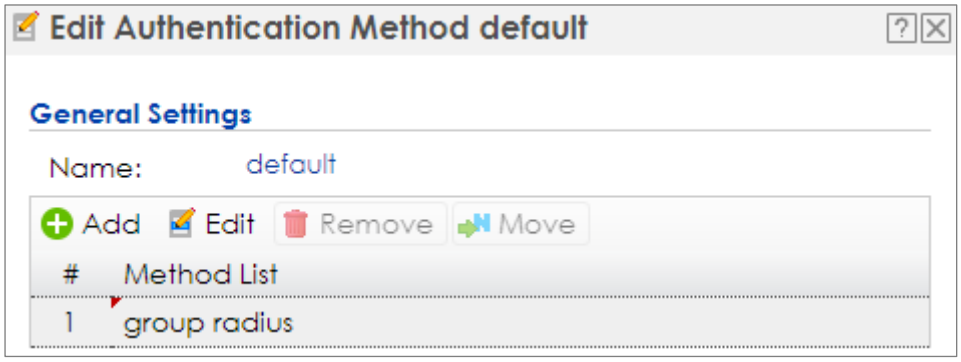


B. Settings on NXC Controller

1 Go to **CONFIGURATION > Object > AAA Server > RADIUS**, click **#1 radius**, and then click **Edit**. Set the **Server Address**, and **Authentication Port** is **1812**. Enter the **Key** for Radius server and click **OK**.



2 Go to **CONFIGURATION > Object > Auth. Method**, click **#1 default**, and then click **Edit**. Change the Method to **group radius**. Click **OK** to save.



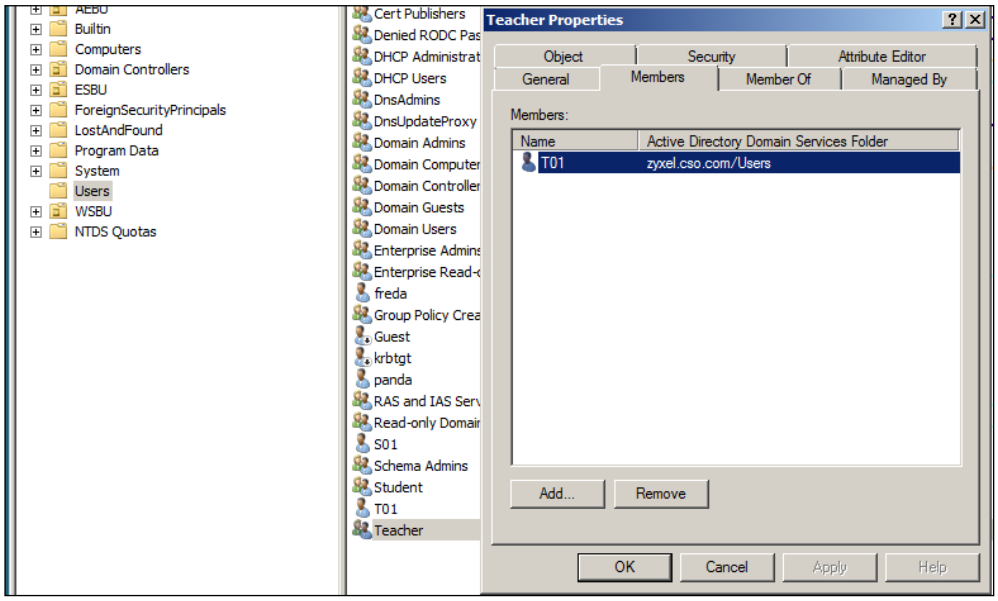
Topic: Dynamic VLAN by radius attribute

4.5.3.2 Dynamic VLAN by External User Group

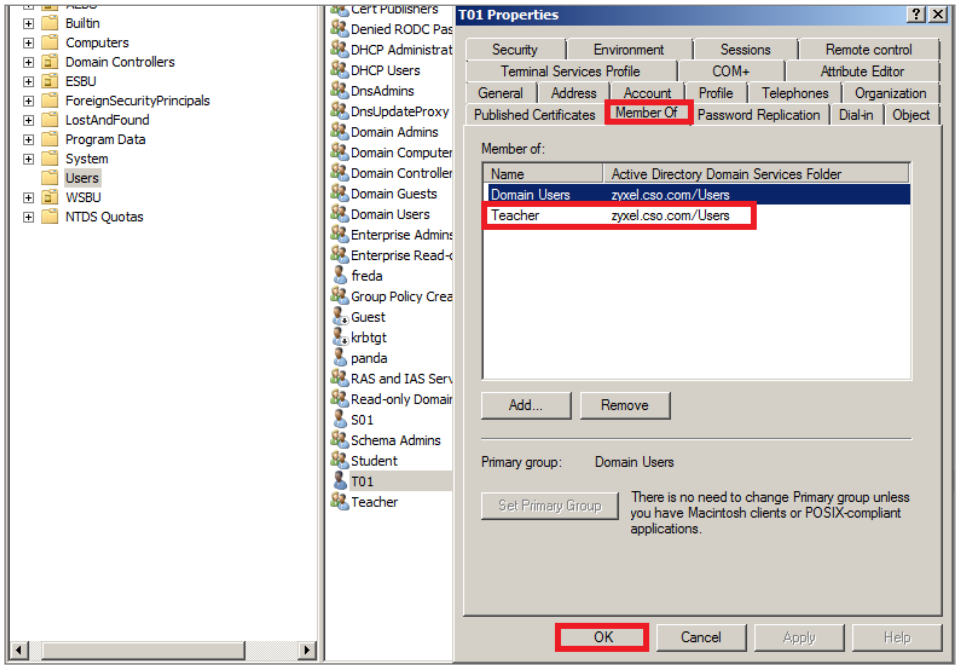
When users use dynamic VLAN by external user group, the radius and AD server are supported. Here are two examples for settings these two servers and NXC controller.

A. Settings on Radius/AD Server

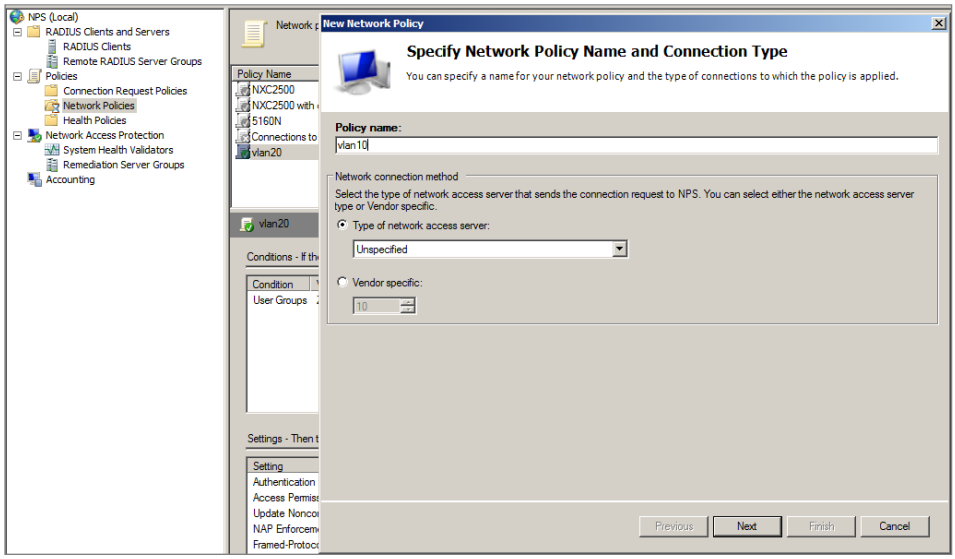
1 Add the user to a group in AD server.



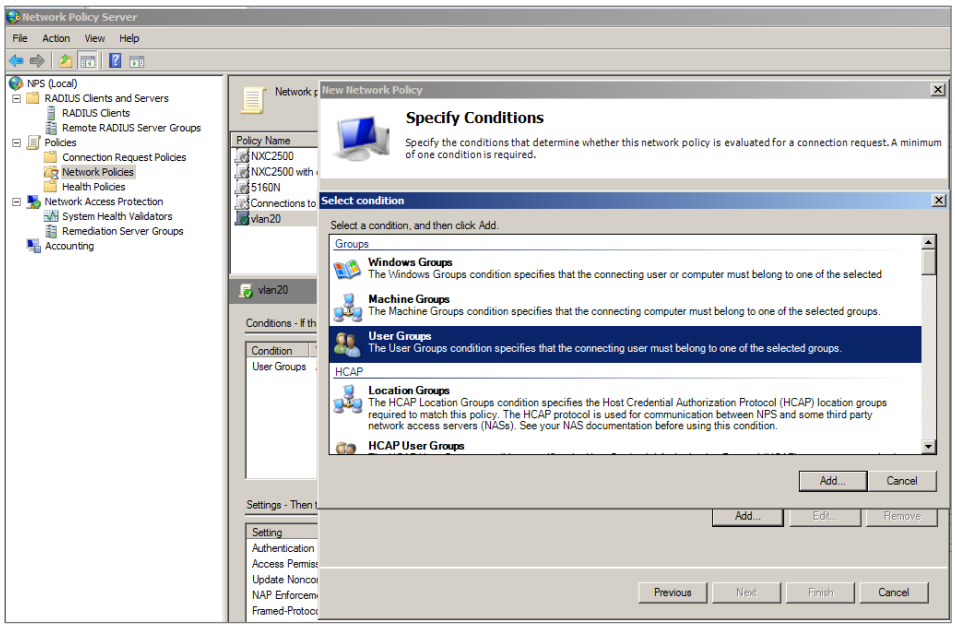
2 Check the user's properties about its group in Member Of.



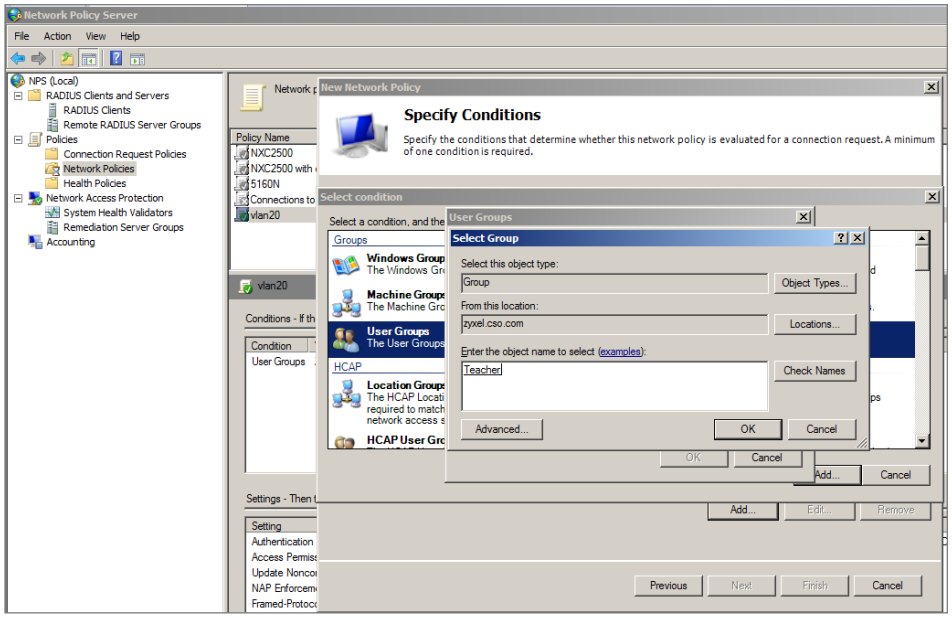
3 Add a new Network Policy of NPS server for a group and then click 'Next'.



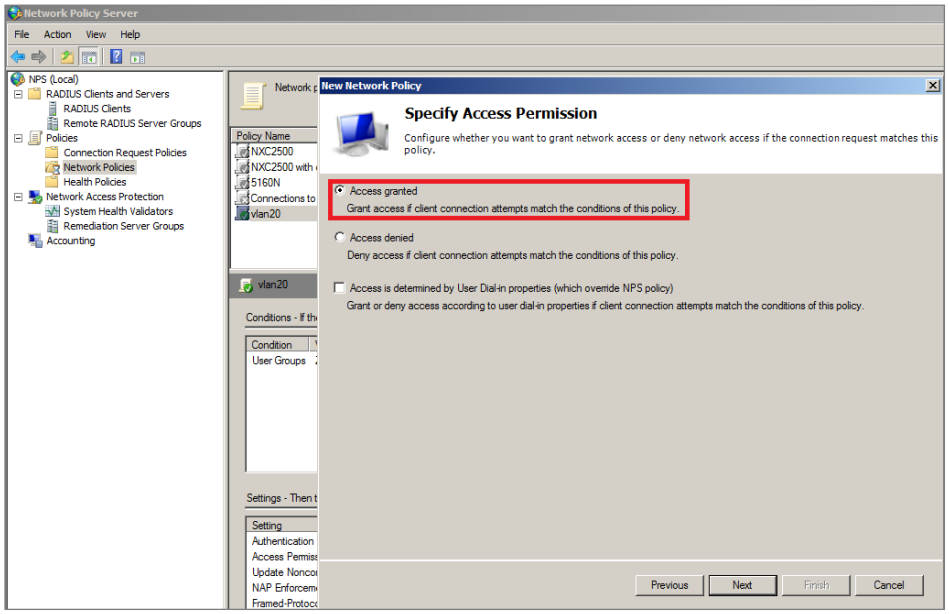
4 Add 'User Group' condition.



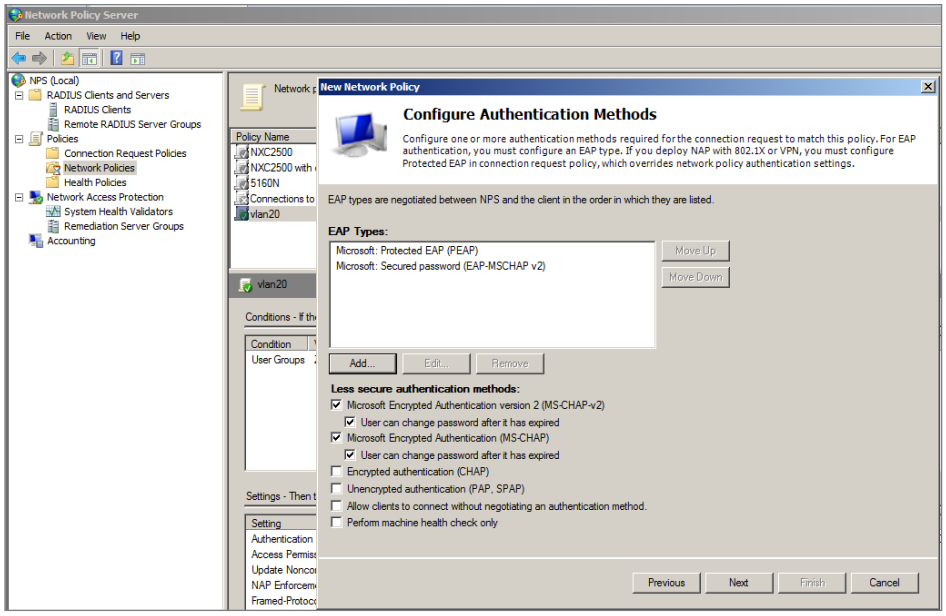
5 Select the group which is set in AD server.



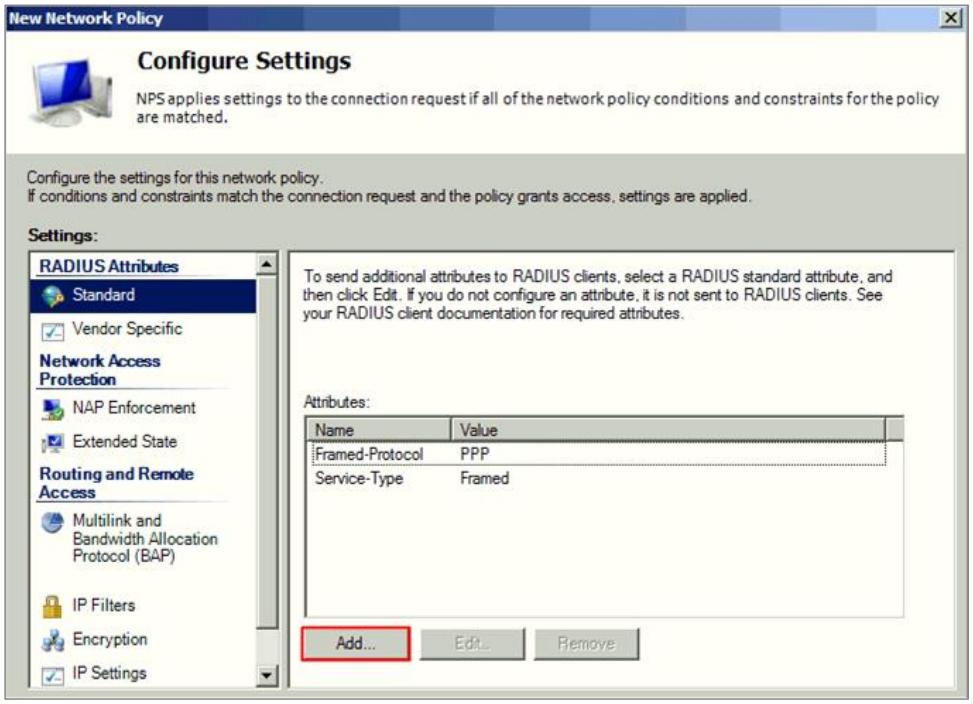
6 Set the access permission and click ‘Next’.

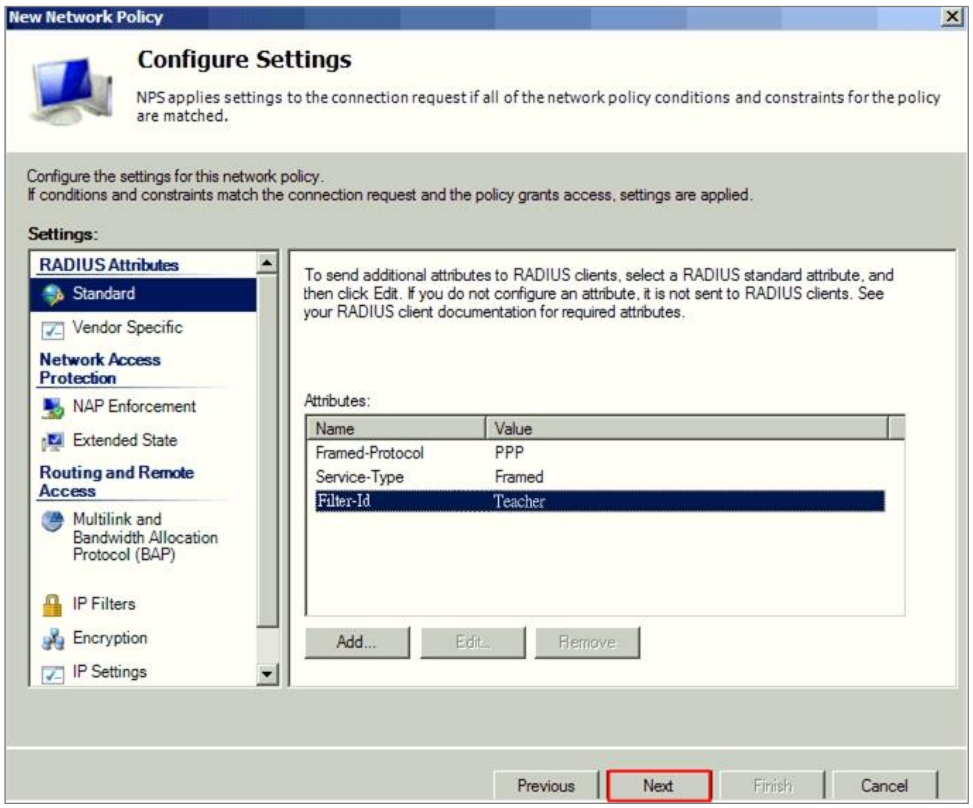


7 Configuration Authentication Methods and click ‘Next’.



8 There are three attribute needed to add Filter-ID as Teacher.



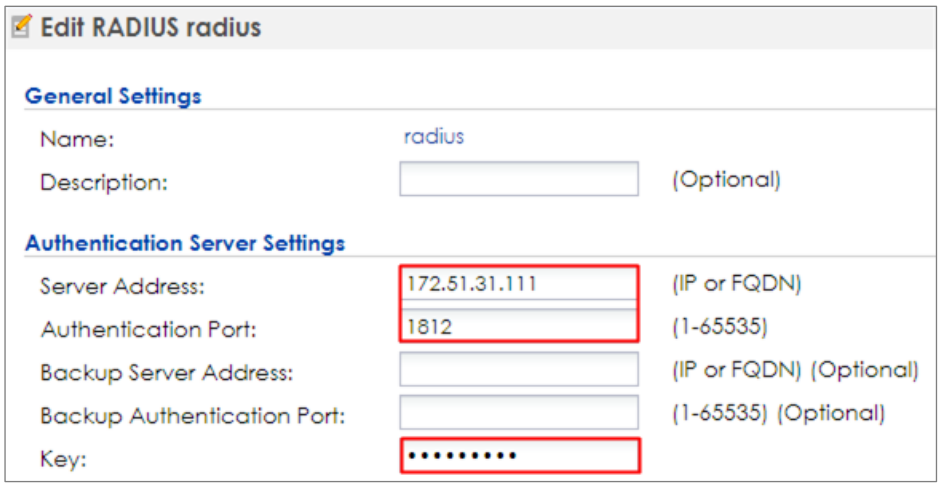


9 Do the same steps to create the other group for other users.

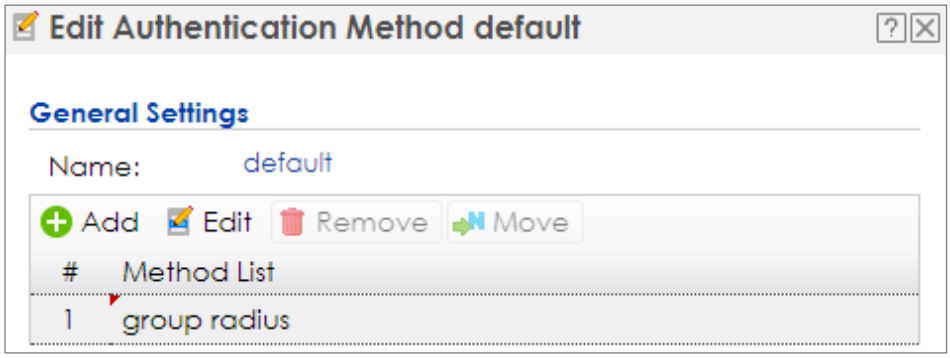
B. Settings on NXC Controller

b1. Using Radius Server

1 Go to **CONFIGURATION > Object > AAA Server > RADIUS**, click **#1 radius**, and then click **Edit**. Set the **Server Address**, and **Authentication Port** is **1812**. Enter the **Key** for Radius server and click **OK**.

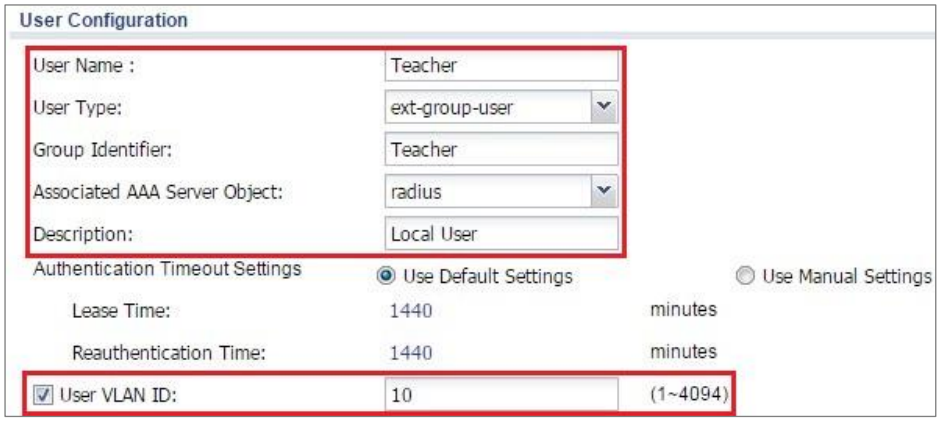


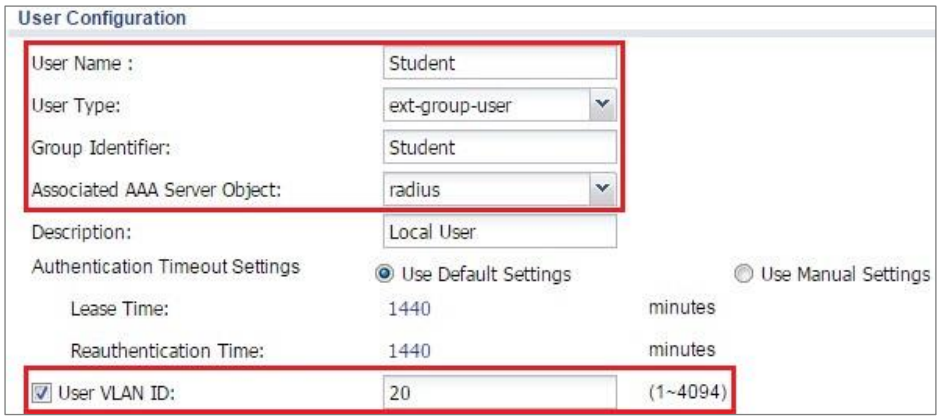
2 Go to **CONFIGURATION > Object > Auth. Method**, click **#1 default**, and then click **Edit**. Change the Method to **group radius**. Click **OK** to save.



3 Go to **Configuration > Object > User/Group > User > Add/Edit**

When user type is 'ext-group-user', set the corresponded value in 'Group Identifier' field, then enable and set the 'User VLAN ID' option.

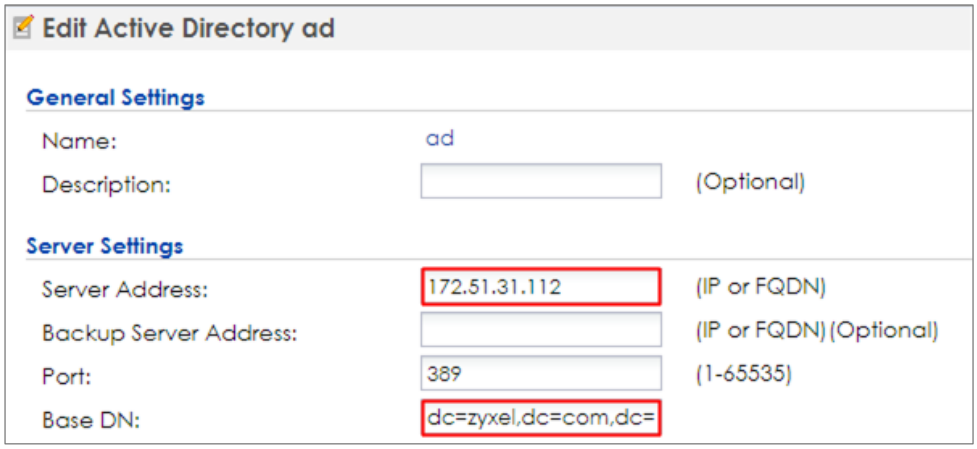




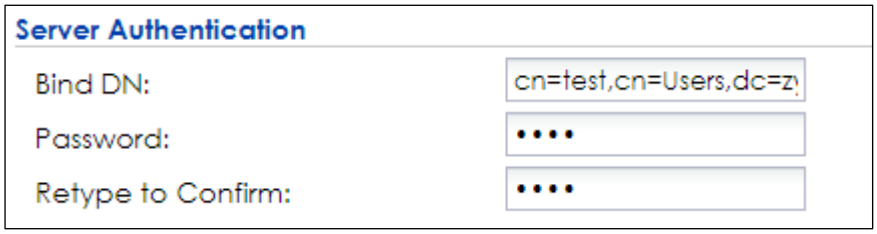
b2. Using AD Server

1 Go to **CONFIGURATION > Object > AAA Server > Active Directory**, click **#1 ad**, and then click **Edit** to configure AD server's information.

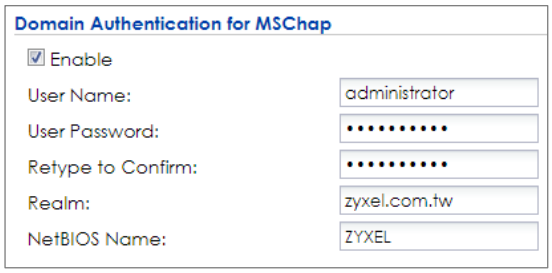
2 In **Server Settings**, enter **Server Address**. Here use **172.51.31.112** as the example. Go to AD server to check Base DN. Here is an example for checking the Base DN on Windows server, and it can be copied from clicking right on the **domain name > properties > Attribute Editor> distinguished Name > View**.



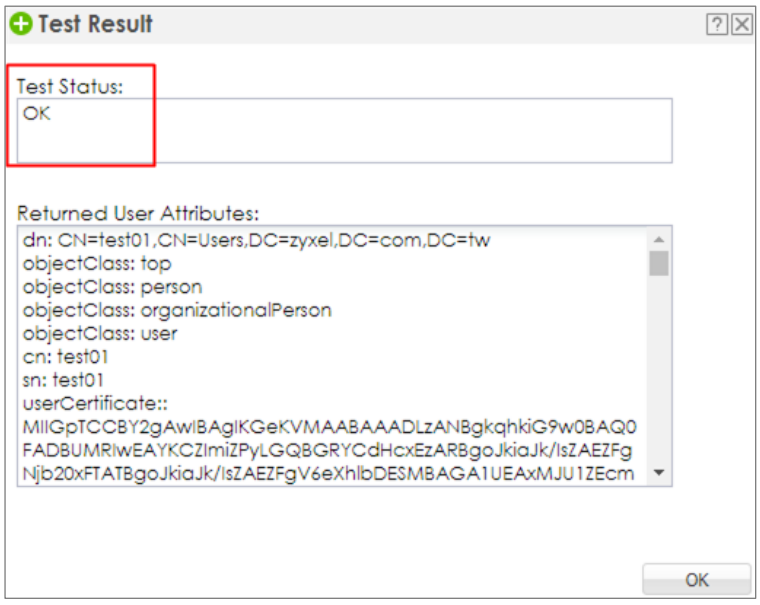
3 In **Server Authentication**, enter **Bind DN** and **Password**. You can check Bind DN in the AD server. In the AD server, clicking right on the Administrator > properties > Attribute Editor > distinguished Name > View. The Password is Administrator's password in the AD server.



4 In **Doman Authentication for MSChap**, check **Enable** and enter the **User Name**, **User Password**, **Realm**, and **NetBIOS Name**. The Realm is the domain name of the AD server.



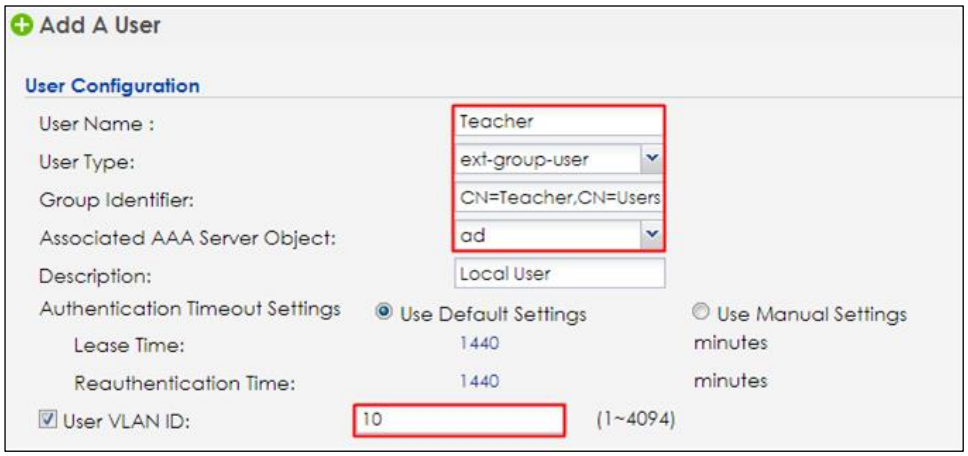
5 After finishing the configuration, enter **administrator** as the **Username** and click **Test** in **Configuration Validation**.



6 Go to **CONFIGURATION > Object > Auth. Method**. Select to the default method, and click **Edit**. Select the AD server you create. Click **OK**.

7 Go to **Configuration > Object > User/Group > User > Add/Edit**. When user type is 'ext-group-user', set the corresponded value in 'Group Identifier' field, then enable and set the 'User VLAN ID' option. There are two Filter-ID in radius server and the 'Group Identifier' of each ext-group-user is the same as the radius server's setting.

The **Group Identifier** is the distinguishedName of the group in AD server.



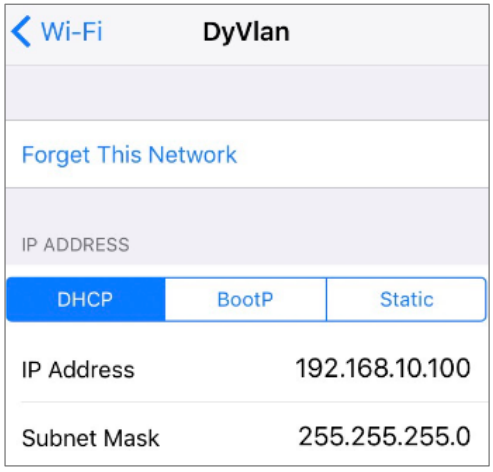
8 Setting the other ext-group-user for student group as the step 4.

4.5.4 Test the Result

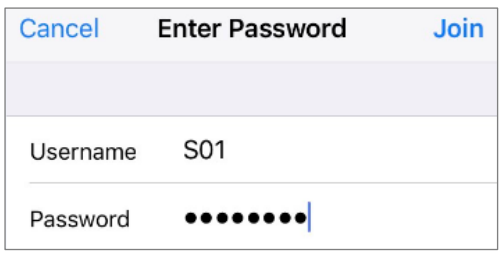
4.5.4.1 Dynamic VLAN by radius server attribute

1. Use mobile phone to connect with SSID **DyVlan**. Enter the Username and Password which are in VLAN 10 group, and then click Join to connect with the AP.

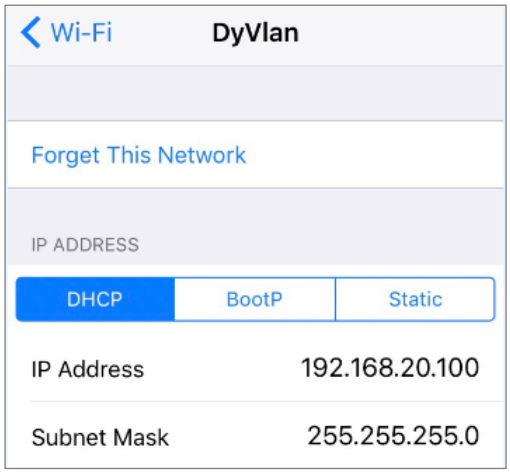
2. The logged-in client gets an IP in VLAN10.



3. Use the mobile phone to connect with SSID **DyVlan**. Enter the Username and Password which is in VLAN 20 group, and then click Join to connect with the AP.



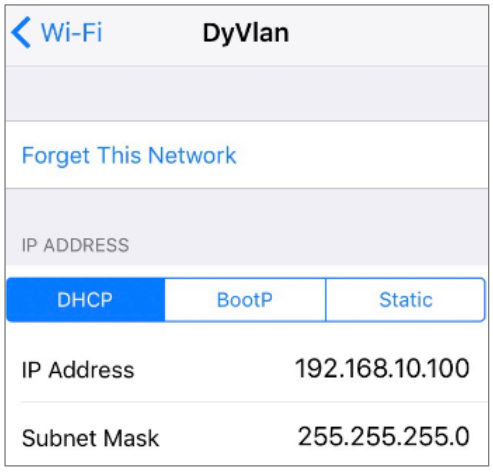
4 The logged-in client gets an IP in VLAN20.



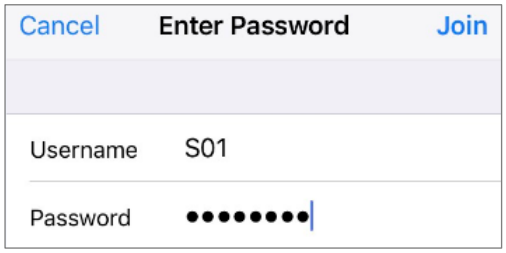
4.5.4.2 Dynamic VLAN by External User Group

1 Use mobile phone to connect with SSID **DyVlan**. Enter the Username and Password which are in VLAN 10 group, and then click Join to connect with the AP.

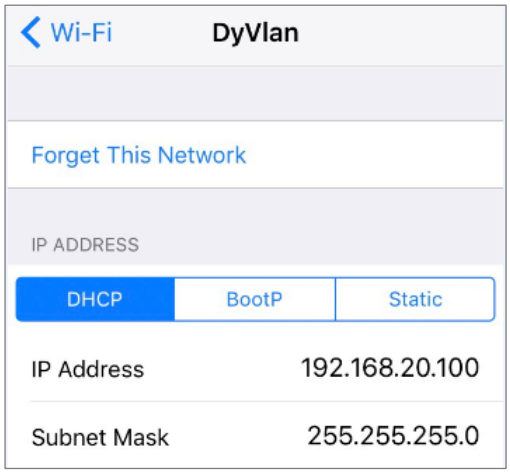
2 The logged-in client gets an IP in VLAN10.



3 Use the mobile phone to connect with SSID **DyVlan**. Enter the Username and Password which is in VLAN 20 group, and then click Join to connect with the AP.



4 The logged-in client gets an IP in VLAN20.



4.5.5 What Could Go Wrong

1. When you set the dynamic VLAN in the NXC controller, the radius server needs to set the corresponding VLAN groups for authentication.
2. Because the dynamic VLAN setting is in the NXC controller, it only supports radius server type "**Internal**" in **CONFIGURATION > Object > AP Profile > SSID > Security List**.

4.6 How to Configure 802.1x EAP-TLS to Secure the Wireless Environment with Self-Signed Certificate?

This example shows how to use Android/iOS phone import the self-sign certificate from NXC to get the wireless connection with 802.1x EAP-TLS protected. We need a certificate which is generated by the NXC.

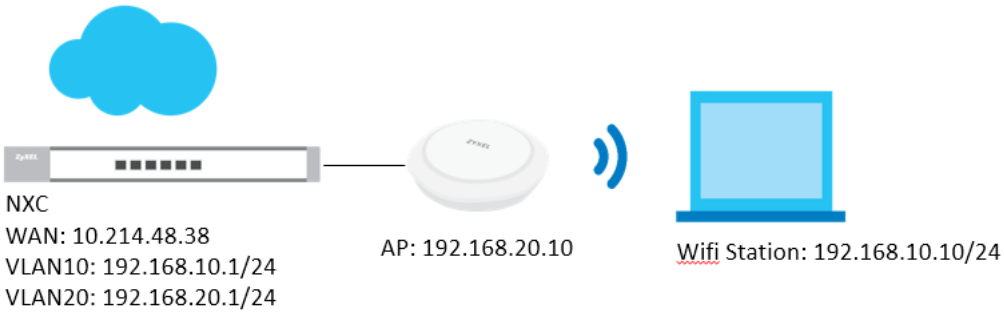


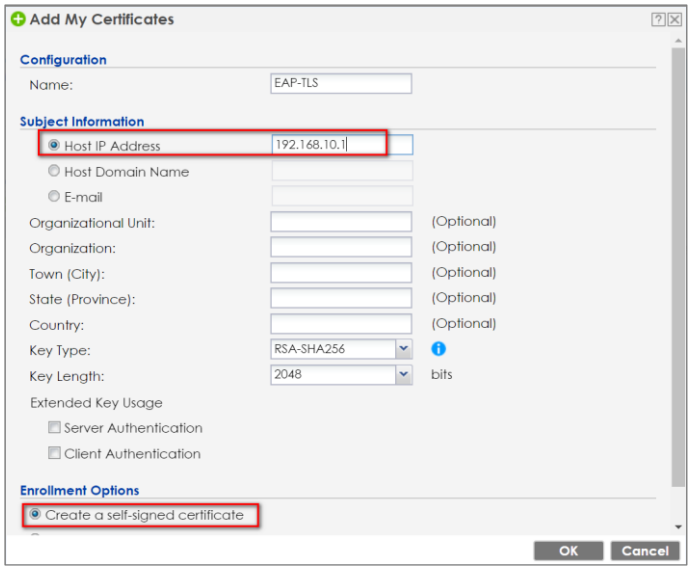
Figure 4.6 Use 802.1x with EAP-TLS

Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using NXC2500 (Firmware Version: 5.40)

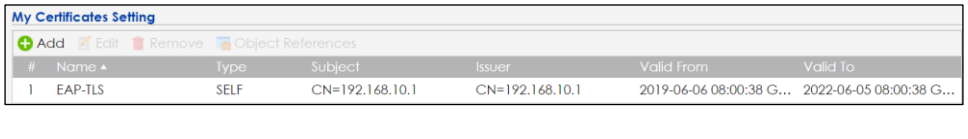
4.6.1 Configure Certificate

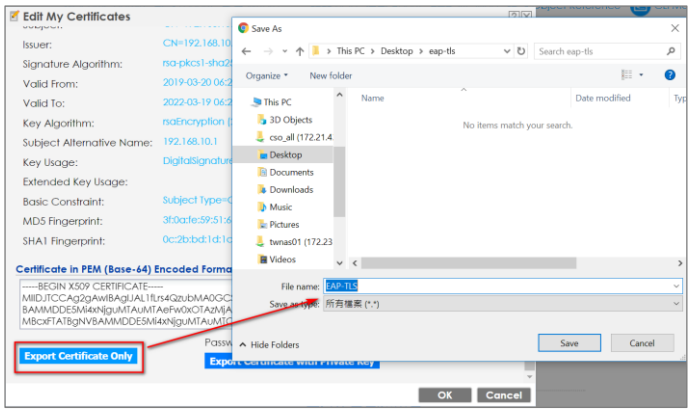
1 Go to **CONFIGURATION > Object > Certificate > My certificates**, and **add** a self-signed certificate. In **Subject Information**, Set the **NXC's IP** in the **Host IP Address**.

In **Enrollment Options**, select **Create a self-signed certificate**

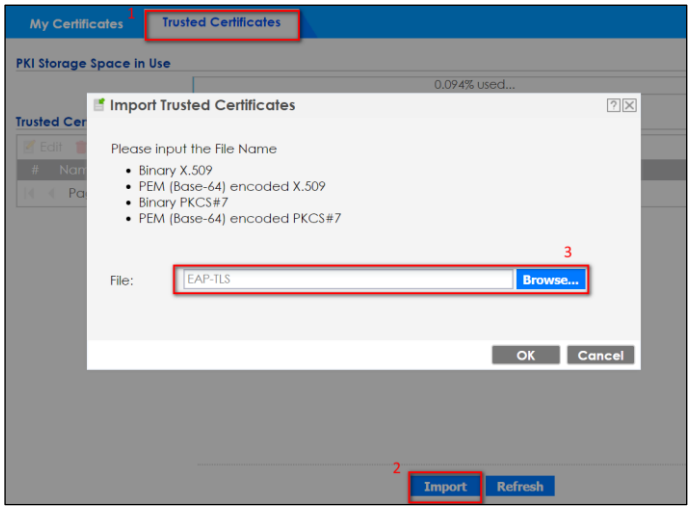


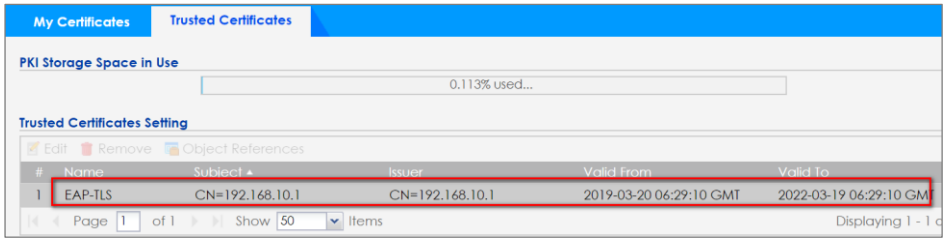
2 Export the self-signed certificate from My certificates. **Double click** the self-signed certificate and scroll down the page to press **Export Certificate Only**. **Save** the certificate.



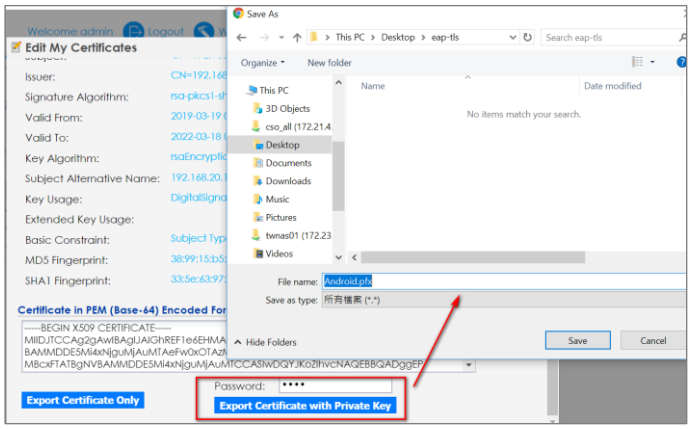


3 Go to **Trusted Certificate** and **import** the self-signed certificate.



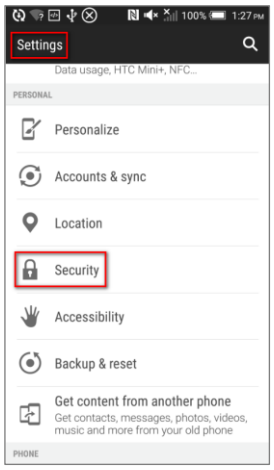


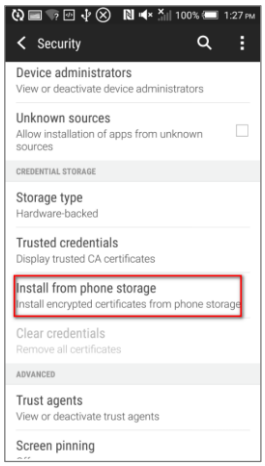
4 Go to **My certificate** and Export the "Self-signed certificate with Private Key". **Double click** the self-signed certificate and scroll down the page to press **Export Certificate with Private Key**. **Save** the certificate and add file extension(*.pfx, *.p12 or *.crt).

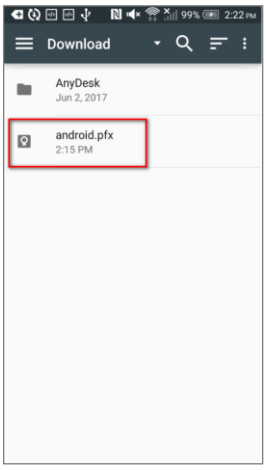


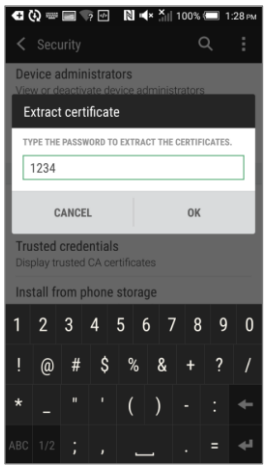
5 Import the self-signed certificate into Android phone. (Here I copied the certificate to the Android phone storage then import them. I send the mail with certificate to iPhone and install it.)

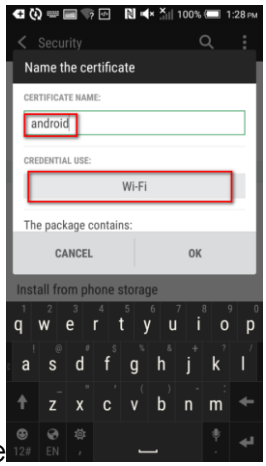
Android: In step "e", the "CREDENTIAL USE" must select as "Wi-Fi"

a 

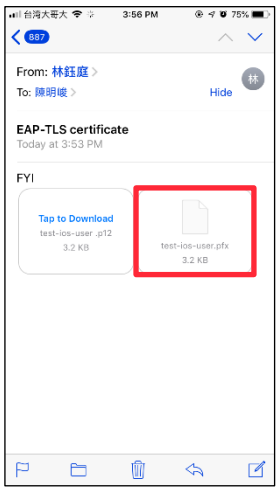
b 

c 

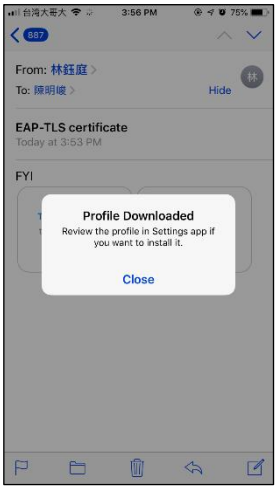
d 

e 

iOS:

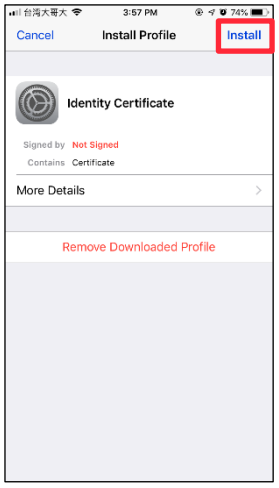


a

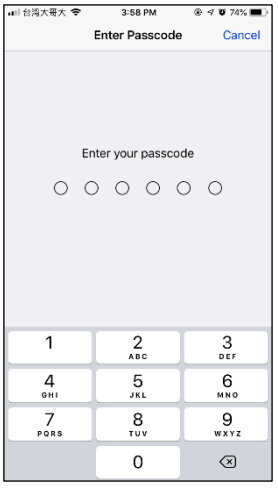


b

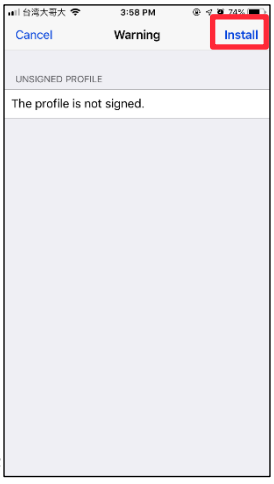
c



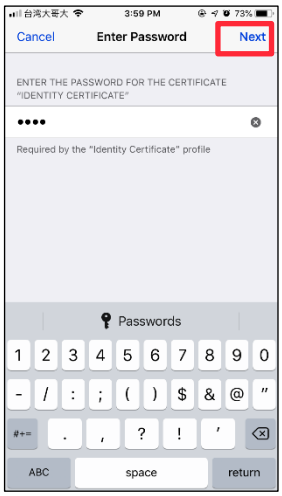
d



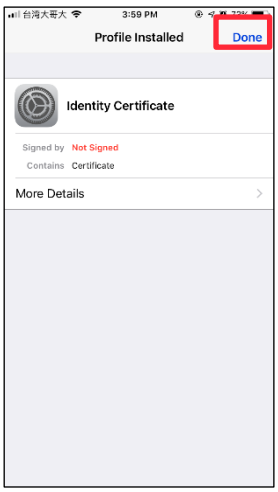
e



f



g

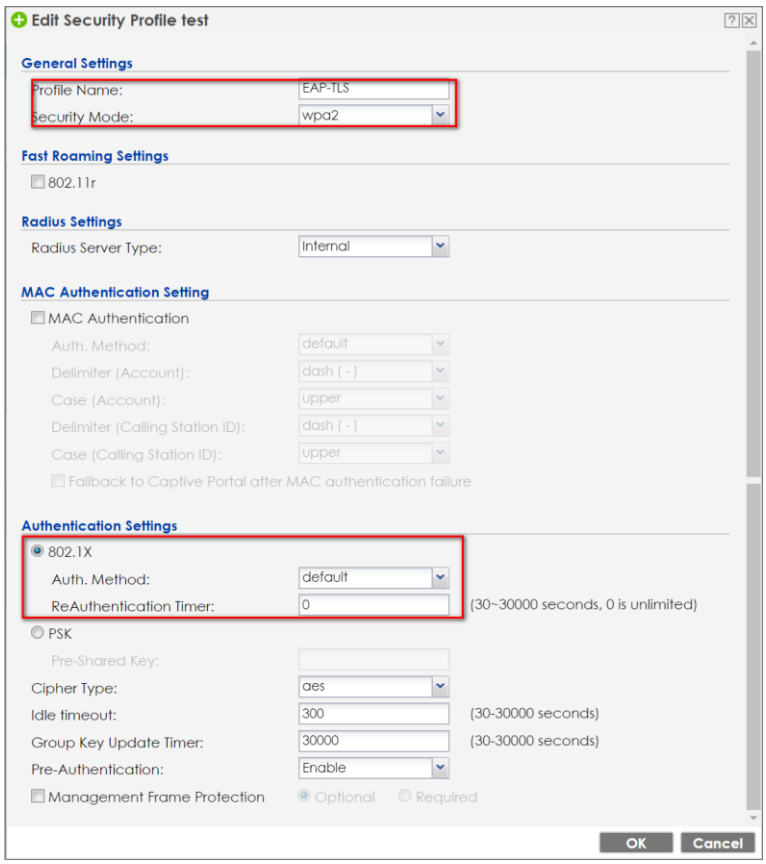


h

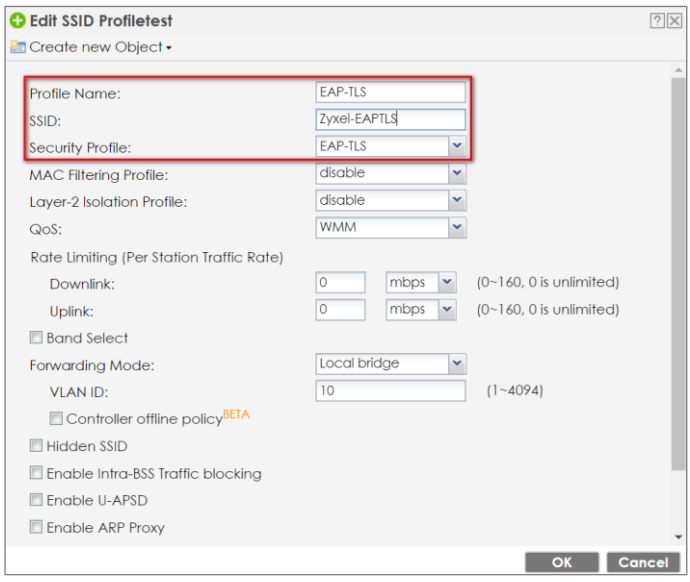
i

4.6.2 Configure AP profile

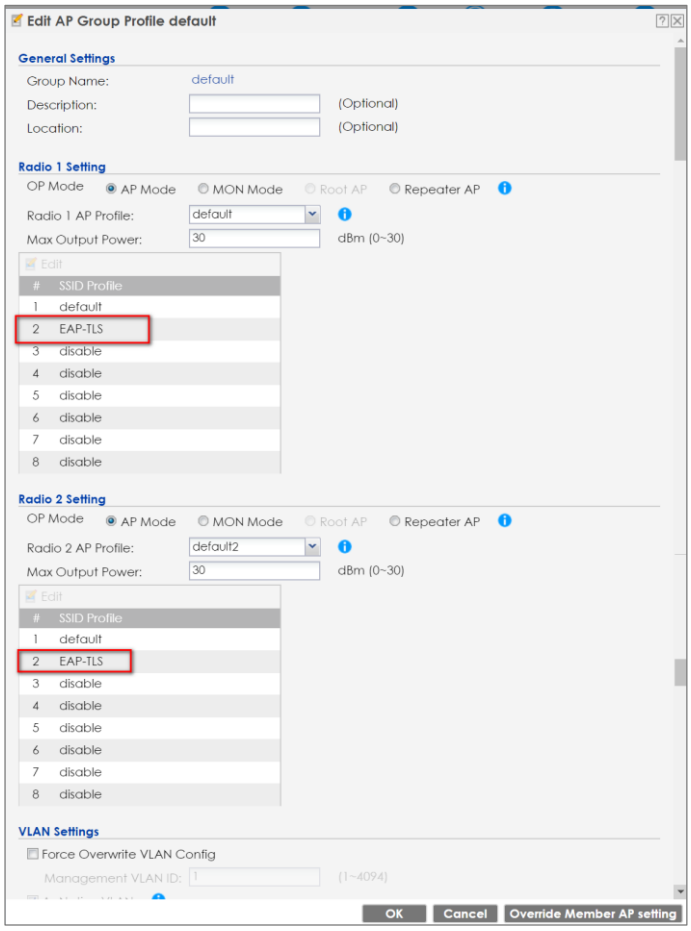
1 Go to **CONFIGURATION > Object > AP Profile > SSID> Security List**, and **add** a Security profile



2 Go to **CONFIGURATION > Object > AP Profile > SSID> SSID List**, and **add** an SSID profile.



3 Go to **CONFIGURATION > Wireless > AP Management > AP Group**, and **add** this SSID into the default group.



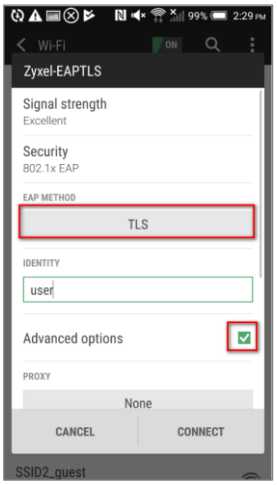
4.6.3 Test the Result

1 Use Android/iOS phone and connect to the SSID Zyxel-EAPTLS.

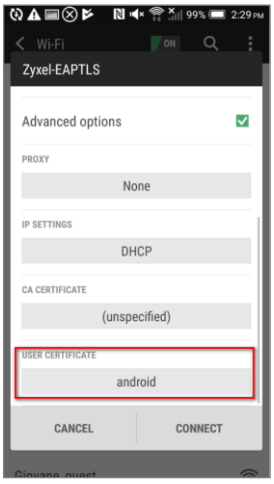
Android:

a

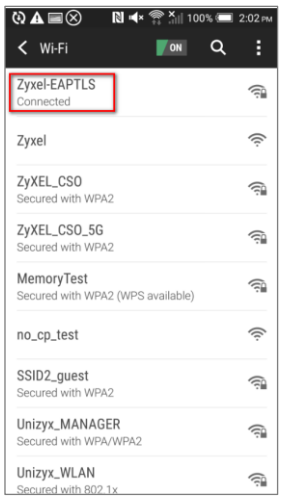
b



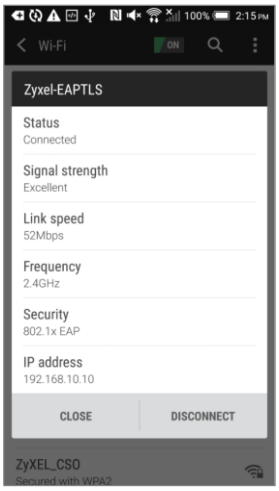
c



d

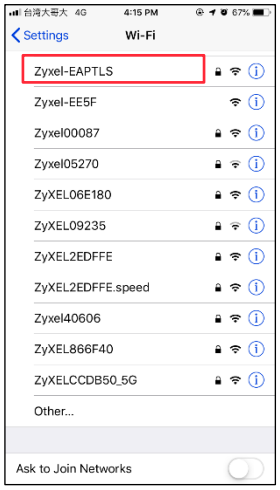


e

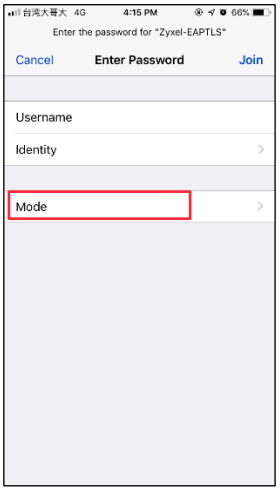


iOS:

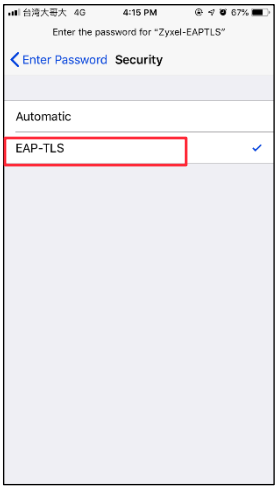
a



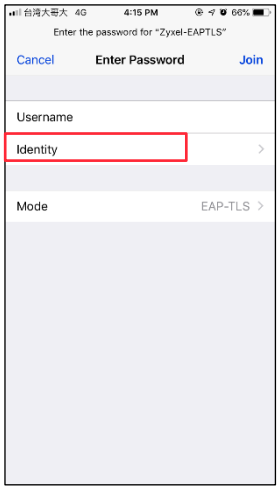
b



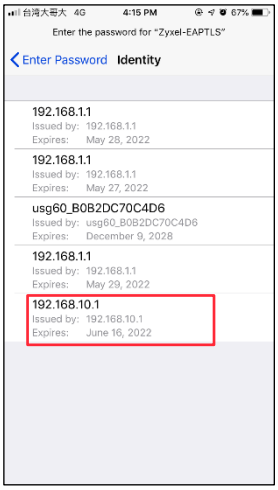
c



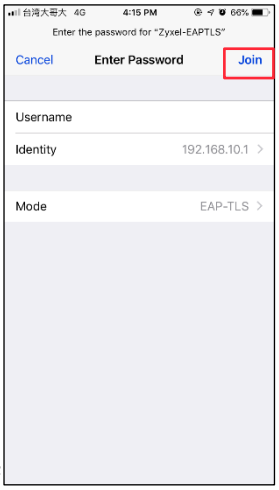
d



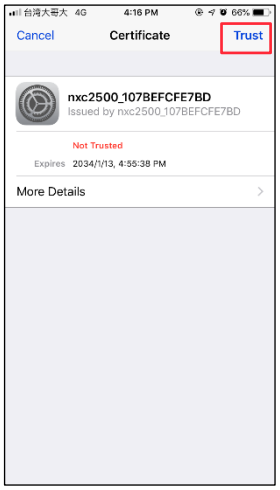
e



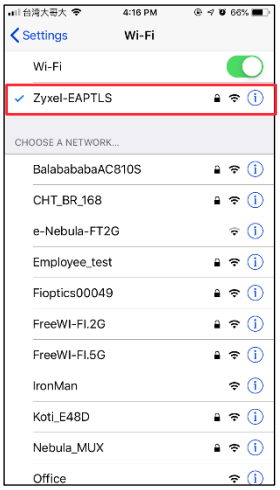
f



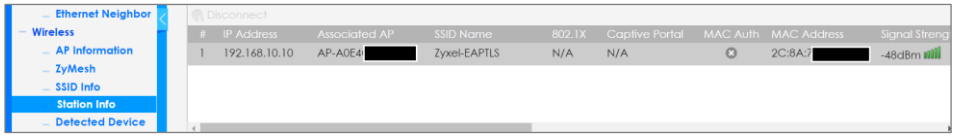
g



i

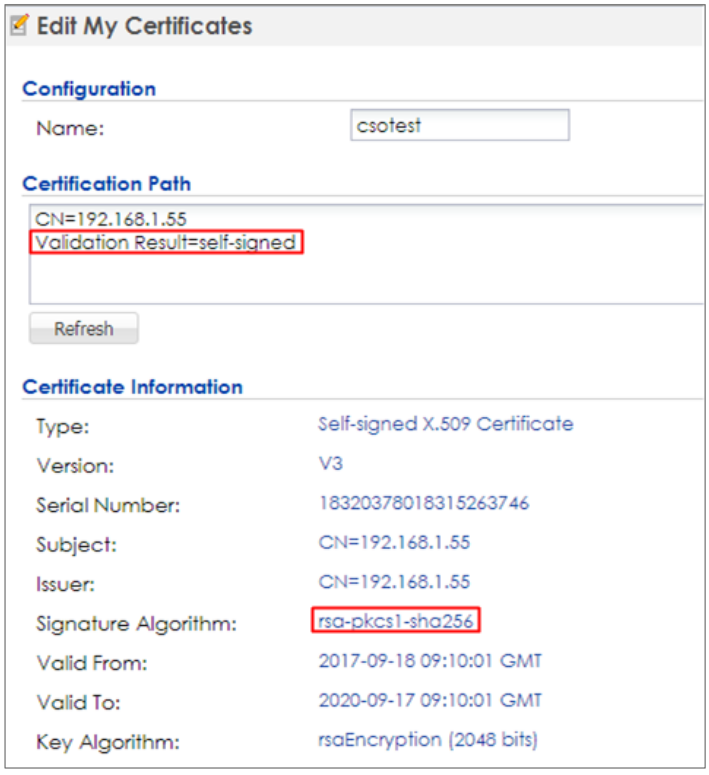


2 Check the station information On NXC station info. Go to **Configuration > Wireless > Station info**.



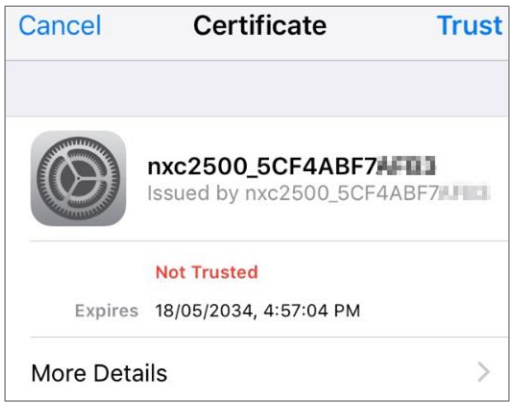
4.6.4 What Could Go Wrong?

1. Users must import the certificate which is signed by NXC, and credential use must select Wi-Fi.
2. When pressing disconnecting on the Android phone, we might need to import the certificates again.
3. Different Android/iOS firmware versions may have different certificate importing behavior. Please ensure the certificates are imported successfully.
4. The Windows PC doesn't support self-signed certificate.
5. Go to **CONFIGURATION > Object > Certificate > My Certificates**, click the self-signed certificate and click edit. It shows **validation result=self-signed** in certification path.



6. When the customer connects to a SSID with 802.1x security, there is a certificate trust request pop-up screen with the

detailed information of the certificate in iOS.



4.7 How to Configure 802.1x EAP-TLS to Secure the Wireless Environment with Third-party CA Certificate?

This example shows how to use Android/iOS phone import the third-party certificate to get the wireless connection with 802.1x EAP-TLS protected. We need a certificate which is purchasing by the third-party CA.

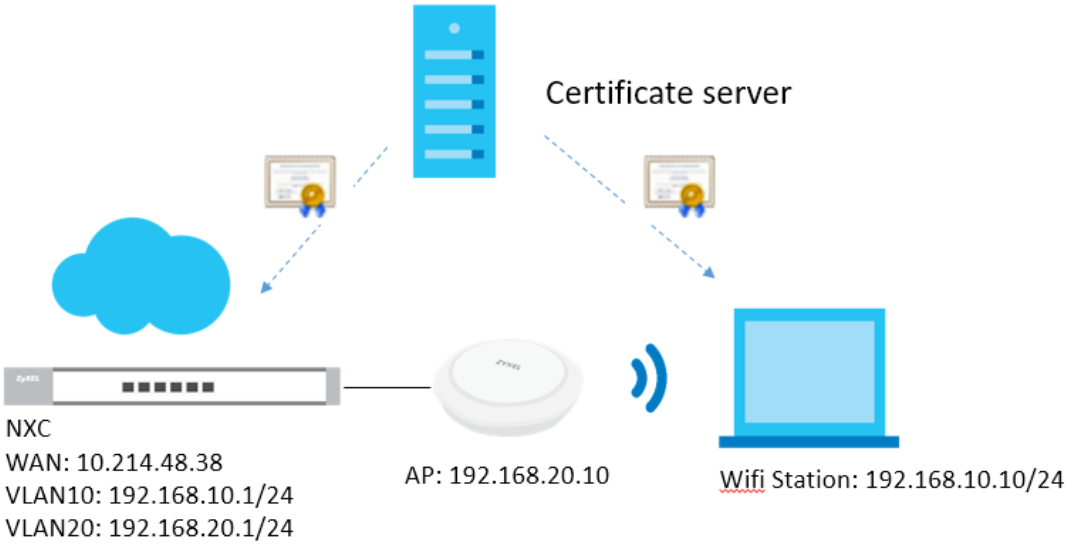


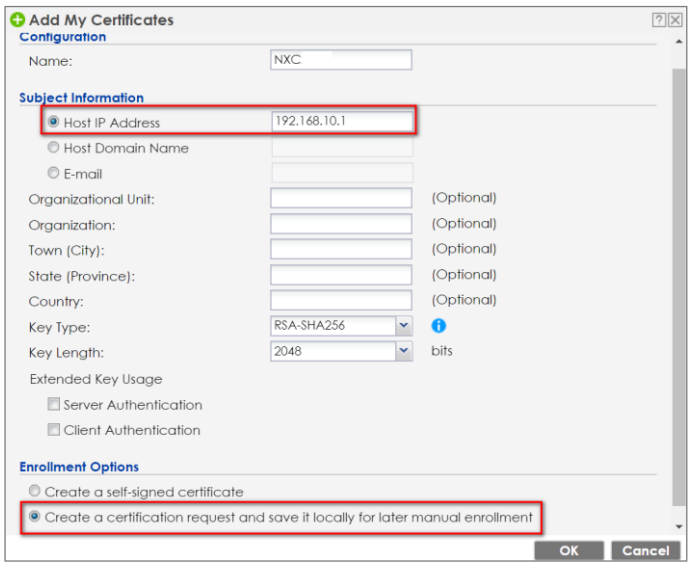
Figure 4.7 Use 802.1x with EAP-TLS

Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using NXC2500 (Firmware Version: 5.40)

4.7.1 Configure Certificate

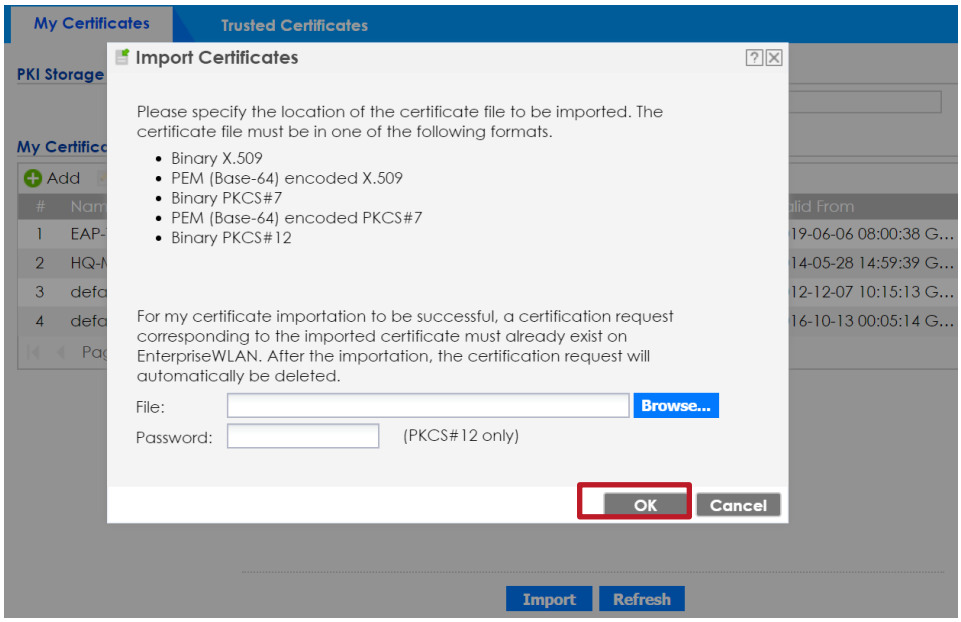
1 Generate certificate request on the NXC. Go to **CONFIGURATION > Object > Certificate > My certificates**, and **add** a request certificate. In **Subject Information**, Set the **NXC's IP** in the **Host IP Address**.

In **Enrollment Options**, select **Create a certification request and save it locally for later manual enrollment**.

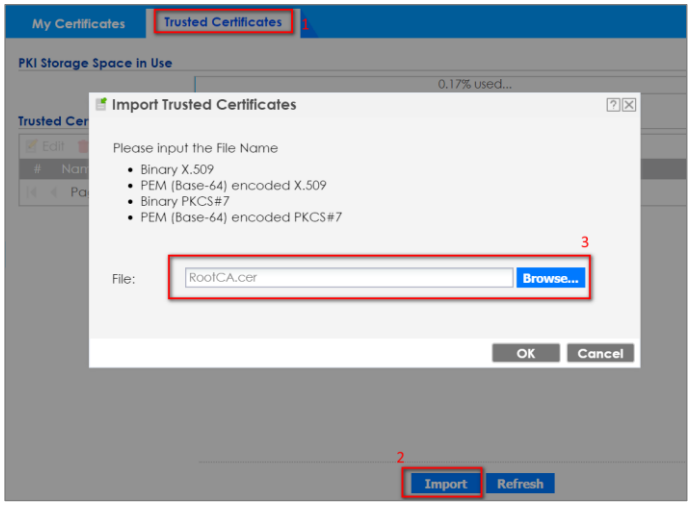


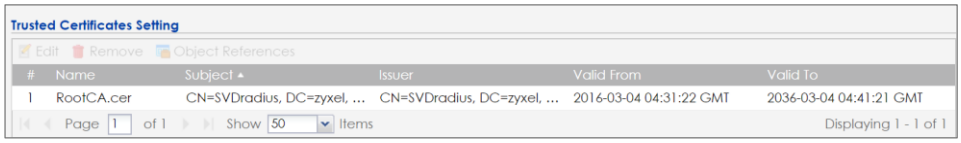
2 **Double click** the certificate and scroll down the page to **copy** the **Base-64 code**, then provide it to the third-party certificate company.

3 After receiving the certificate, import the NXC identity certificate into "My Certificates", and the REQ certificate will be changed to CERT automatically. Go to **CONFIGURATION > Object > Certificate > My Certificates > Import.**



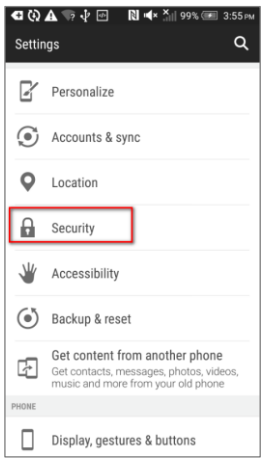
4 Import the root CA and Intermediate CA's certificate (if exits) into "Trusted Certificate". Go to **CONFIGURATION > Object > Certificate > Trusted Certificates > Import.**

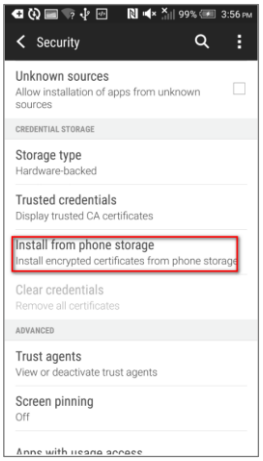


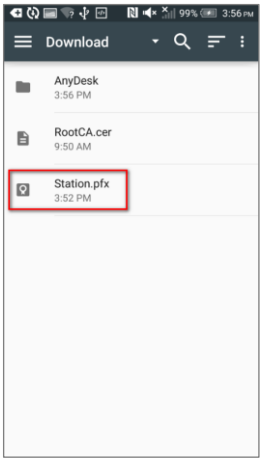


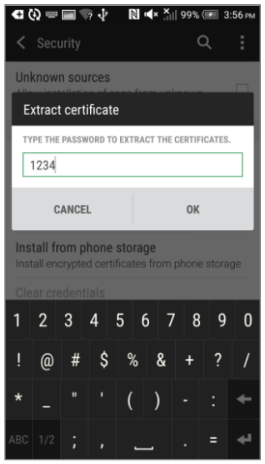
5 Import the station identity certificate, root CA and Intermediate CA's certificate (if exits) into the Android/iOS phone. (The station could download the certificates from email, dropbox or a cloud storage space).

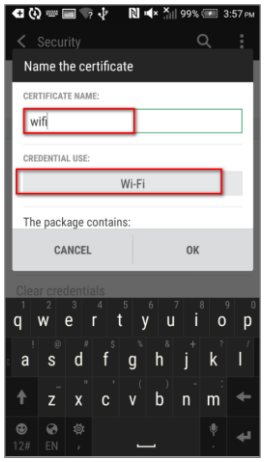
Andriod: In step "e", the Credential use must select Wi-Fi.

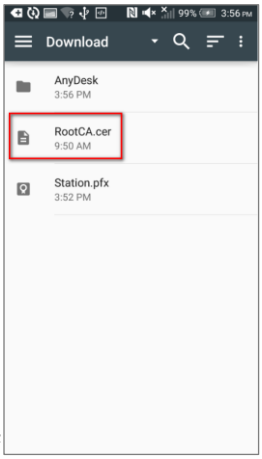
a 

b 

c 

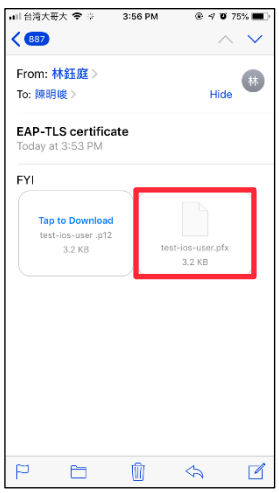
d 

e 

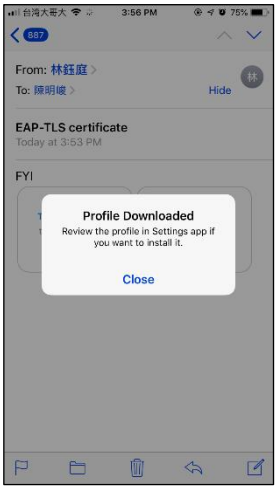
f 

g 

iOS: The way is same as import self-signed certificate.

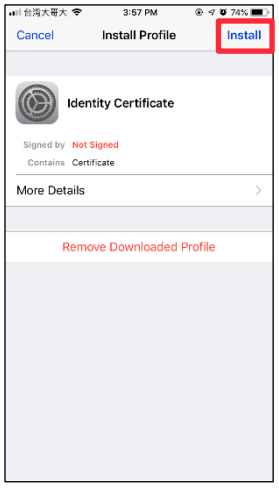


a

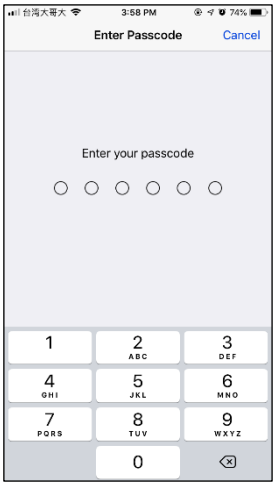


b

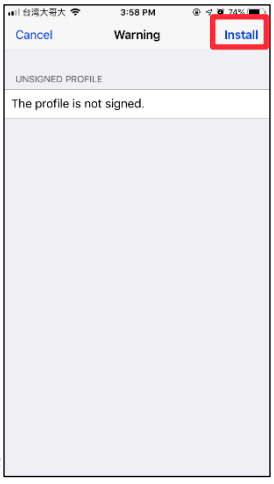
c



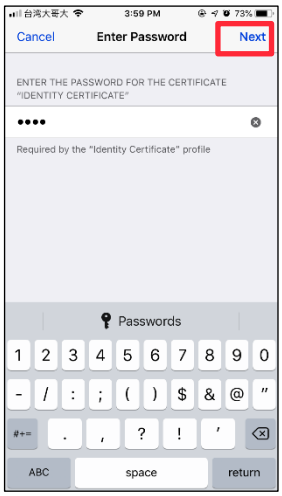
d



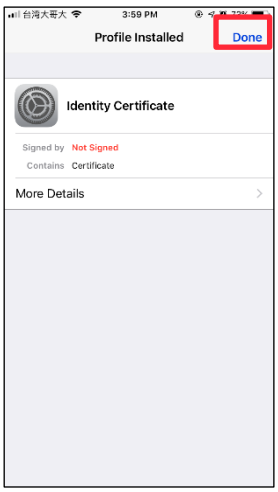
e



f



g

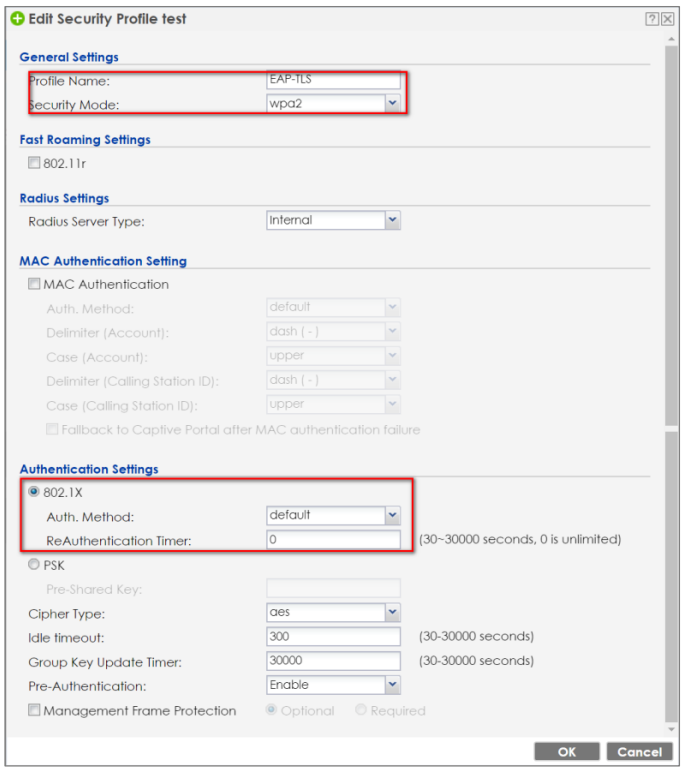


h

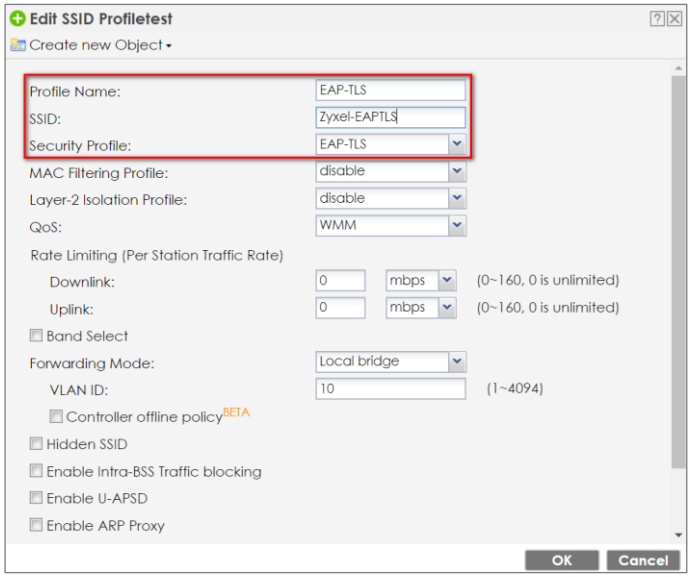
i

4.7.2 Configure AP profile

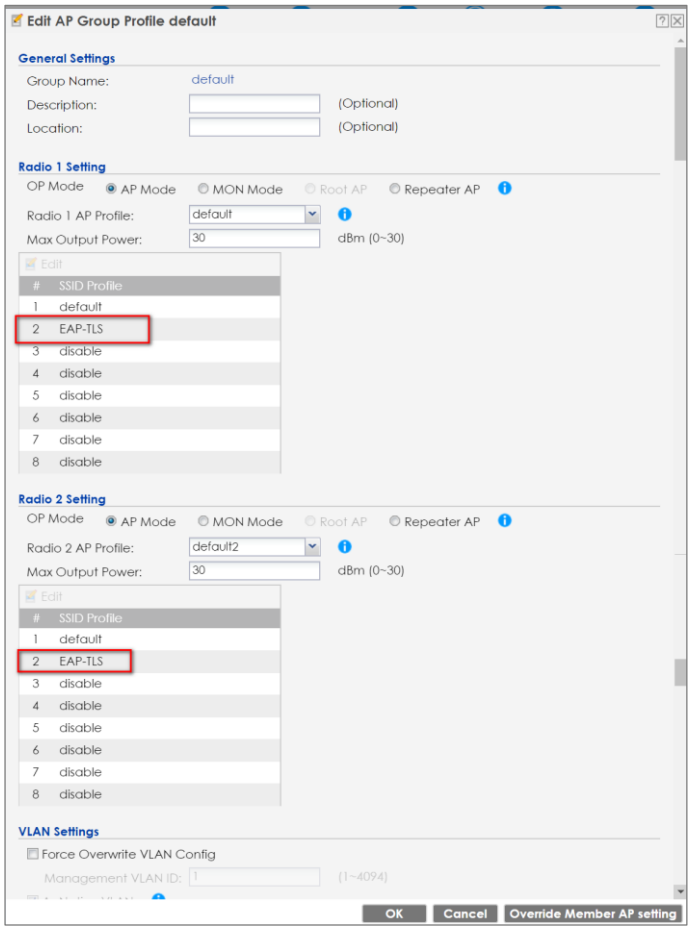
1 Go to **CONFIGURATION > Object > AP Profile > SSID> Security List**, and **add** a Security profile.



2 Go to **CONFIGURATION > Object > AP Profile > SSID> SSID List**, and **add** an SSID profile.

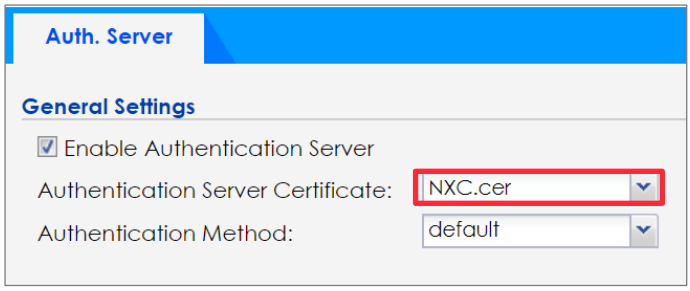


3 Go to **CONFIGURATION > Wireless > AP Management > AP Group**, and **add** this SSID into the default group.



4.7.3 Configure Auth. Server

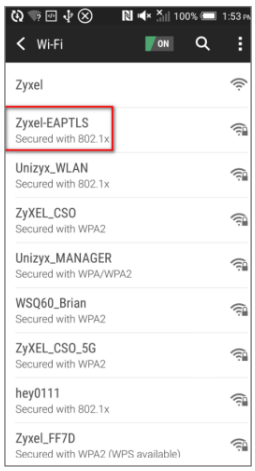
1 Change the certificate to NXC identity certificate from third-party CA. Go to **CONFIGURATION > System > Auth. Server > Auth. Server**, and the **Authentication Server Certificate** select **NXC.cer**.



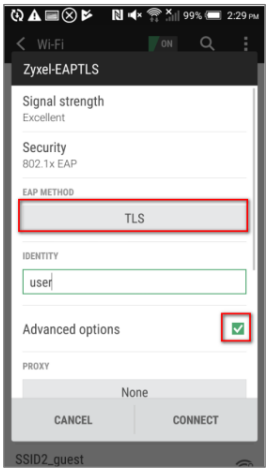
4.7.4 Test the Result

1 Use Android/iOS phone and connect to the SSID Zyxel-EAPTLS.

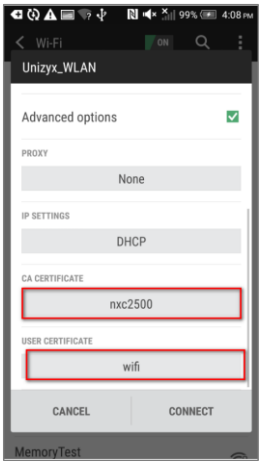
Android: In step "c", please select root CA's certificate in "CA CERTIFICATE" Column and select station identity certificate in "USER CERTIFICATE"



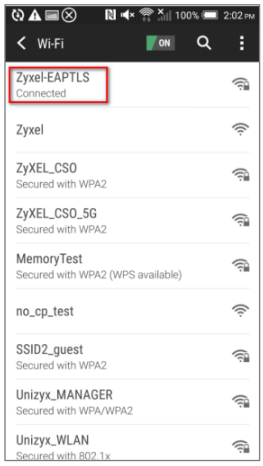
a



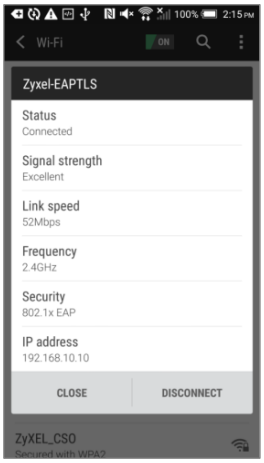
b



c



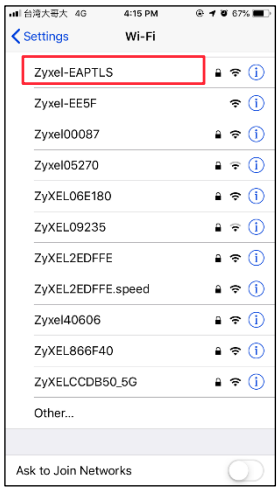
d



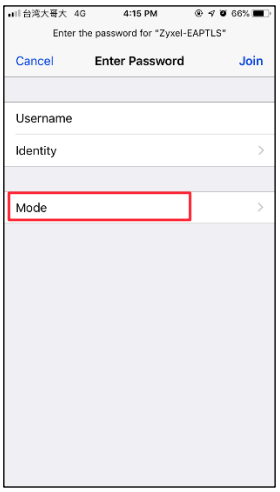
e

iOS: In step “e”, please select the station personal certificate from CA.

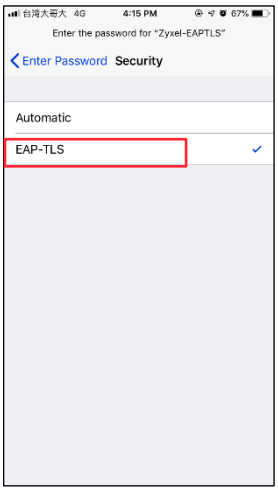
a



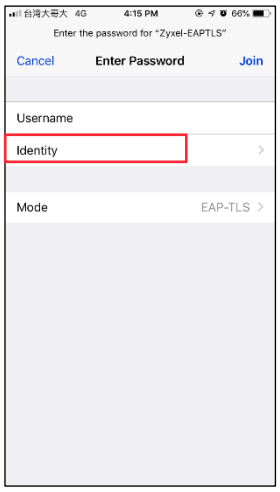
b



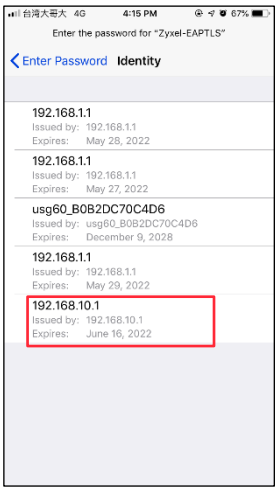
c



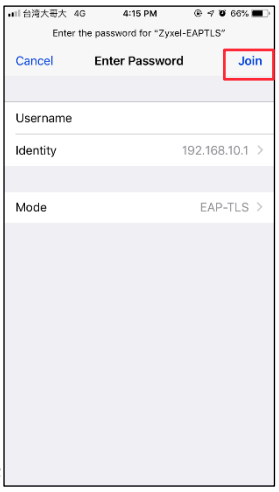
d



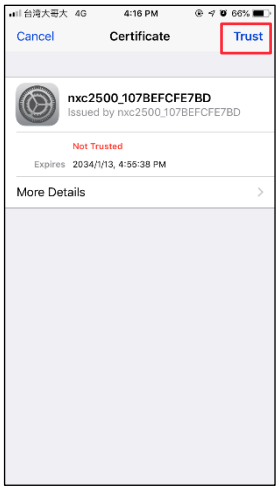
e



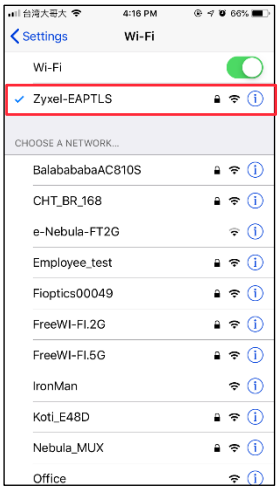
f



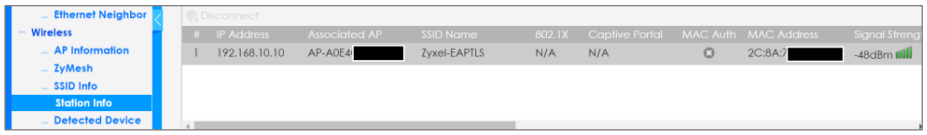
g



i



2 Check the station information On NXC station info. Go to **Configuration > Wireless > Station info**.



4.7.5 What Could Go Wrong?

1. User must import the certificate correctly on each device.
   NXC: Root/Intermediate CA's certificate > Trust Certificate; NXC's certificate > My Certificate;
   Station: Root/Intermediate CA's Certificate > Trusted CA list; Stations' personal certificate > Personal Certificate.
2. When pressing disconnecting on the Android phone, we might need to import the certificates again.
3. Different Android firmware versions may have different certificate importing behavior. Please ensure the certificates are imported successfully.

Secure the Wireless Environment – Captive portal

5.1 How to Configure Captive Portal Redirect on Controller?

The example instructs how to set up captive portal redirect on the controller. A captive portal can intercepts network traffic, according to the authentication policies, until the user authenticates his or her connection, usually through a specifically designated login web page. Typically, you often find captive portal pages in public hotspots. There are two kinds of the topologies for captive portal redirect on the controller: one is to set USG as the gateway; the other is to set NXC controller as the gateway. The configurations of these two kinds of topologies show in below procedures.

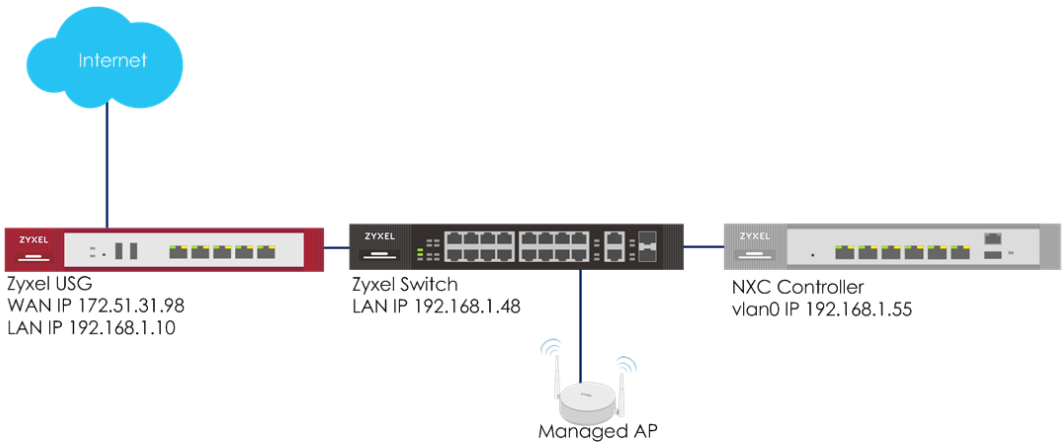


Figure 5.1.a Captive portal redirect on controller (USG is gateway)

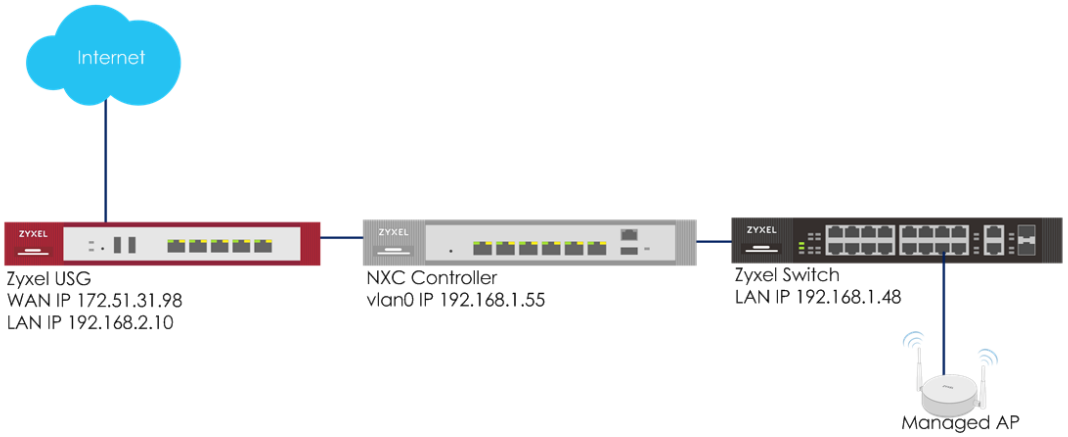
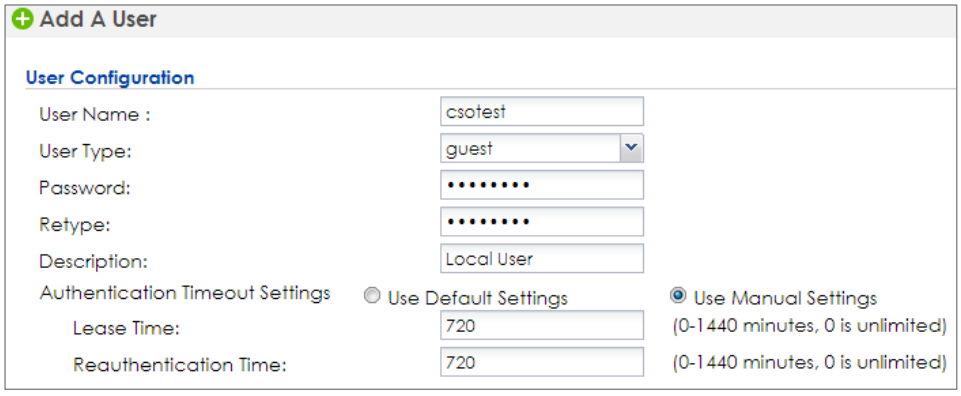


Figure 5.1.b Captive portal redirect on controller (NXC is gateway)

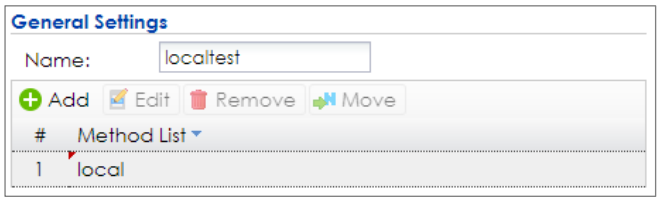
Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC2500 (Firmware Version: 5.30), GS2210-8HP (Firmware Version: V4.30).

5.1.1 Configure Authentication Method Setting

1 Go to **CONFIGURATION > Object > User/Group**, click **add** to create a new user ID and password. Stations can log in captive portal to access the Internet via this account. Enter the **User Name** as login ID for captive portal and **User Type** is **guest**. Enter the **Password** as the login password. The default of **Authentication Timeout Setting** is 1440 minutes, and usually it's shorter for guests. Select to **Use Manual Settings** to set **Lease Time** and **Reauthentication Time**. Click **OK** to save.

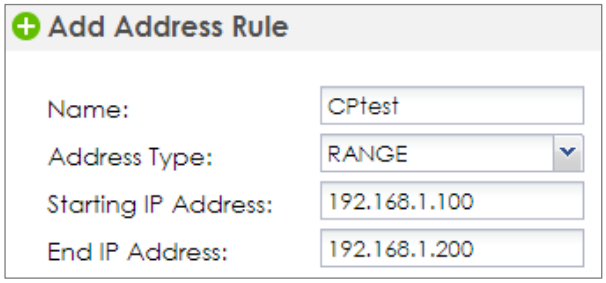


2 Go to **CONFIGURATION > Object > Auth. Method**, click **add** to create an authentication method. Enter the **Name** of this authentication method and select to local in the **Method List**.



5.1.2 Configure Captive Portal

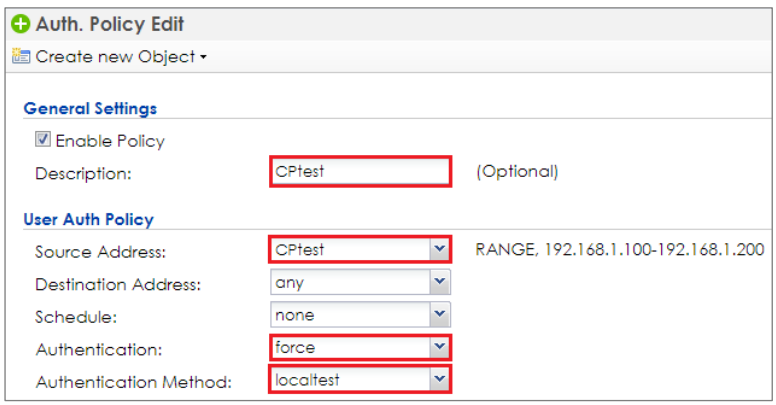
1 Go to **CONFIGURATION > Object > Address > Address**, click **add** to create an address range which needs to do captive portal authentication before accessing to the Internet. Enter profile **Name** and change **Address Type** to **RANGE**. In this example, the IP range for guest is **192.168.1.100** to **192.168.1.200** on DHCP server (USG). Click **OK** to save.



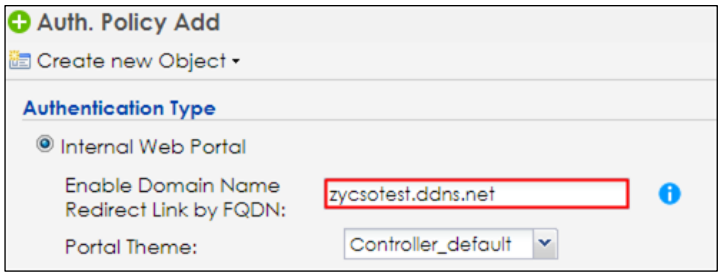
2 Go to **CONFIGURATION > Captive Portal > Redirect on Controller > Authentication Policy Rule**, click **add** to create a policy rule for stations which get an IP range from 192.168.1.100 to 192.168.1.200.

In **General Settings**, check **Enable Policy** and enter the **Description** of this policy.

In **User Auth Policy**, change **Source Address** to **CPtest** and **Authentication** is **required**. Check **Force User Authentication**, and change the **Authentication Method** to **localtest**. Click **OK** to save.

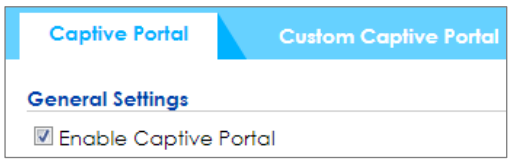


3 If you want to use the domain name instead of an IP address, you can set it in the Authentication Type. (If you don't have FQDN, please skip this step)



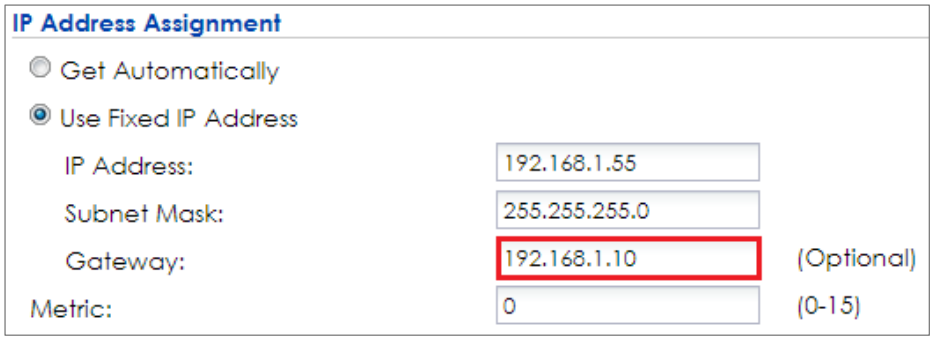
4 Go to **CONFIGURATION > System > WWW** and enable **Redirect HTTP to HTTPS.** Click **Apply** to apply the settings.

5 Go to **CONFIGURATION > Captive Portal > Captive Portal**, check **Enable Captive Portal**. Click **Apply** to apply the settings.

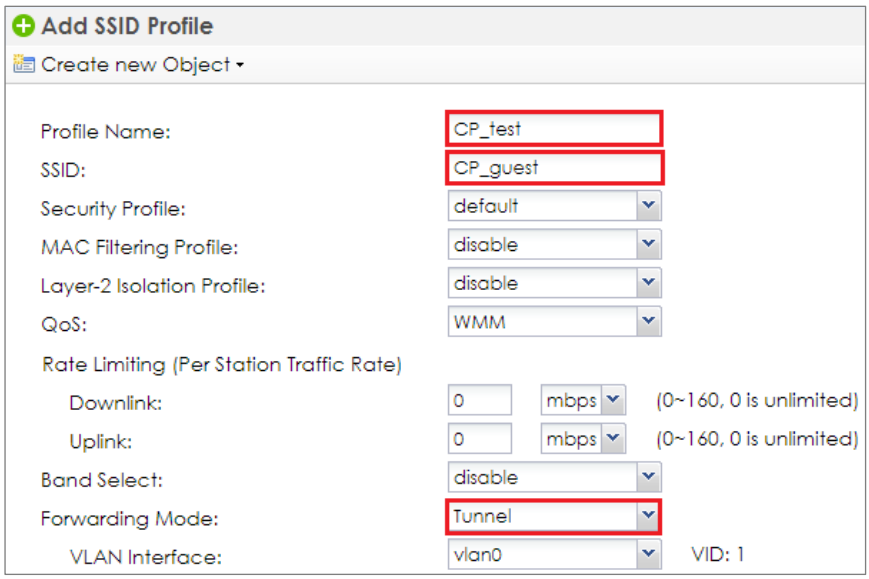


5.1.3 Configure AP Profile when USG is the Gateway

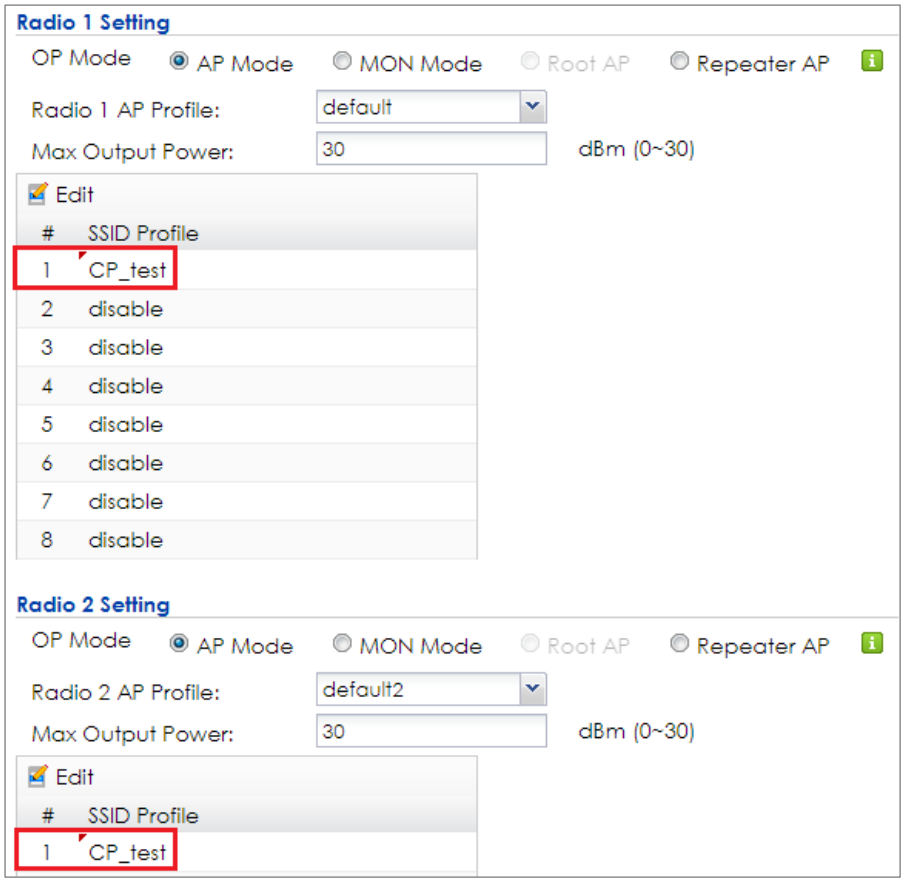
1 To make sure the USG is the gateway for vlan0 interface which is for client accessing the Internet, go to **CONFIGURATION > Network > Interface > VLAN > vlan0 > Edit**, enter USG's IP in **Gateway**. Click **OK** to apply settings.



2 Go to **CONFIGURATION > Object > AP Profile > SSID > SSID List**, click **Add** to add a SSID for captive portal. Key in the **SSID** to **CP_guest**, and change **Security Profile** to **default** which sets none security. Change **Forwarding Mode** to **Tunnel** Mode and click **OK** to save.



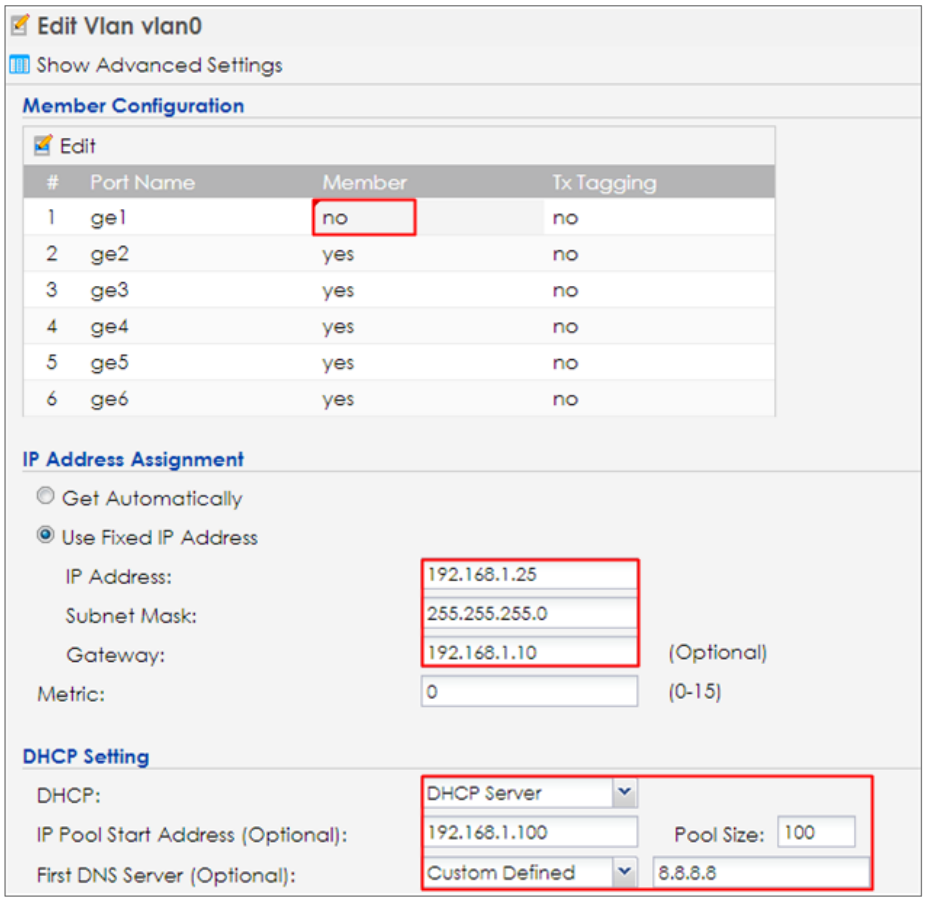
3 Go to **CONFIGURATION > Wireless > AP Management > AP Group**, select the **default** AP profile and edit. Select **#1** to **CP_test** which created in step2. Click **Override Member AP Setting** to apply the SSID to AP and click **Yes** in the pop-up window. Click **OK**.



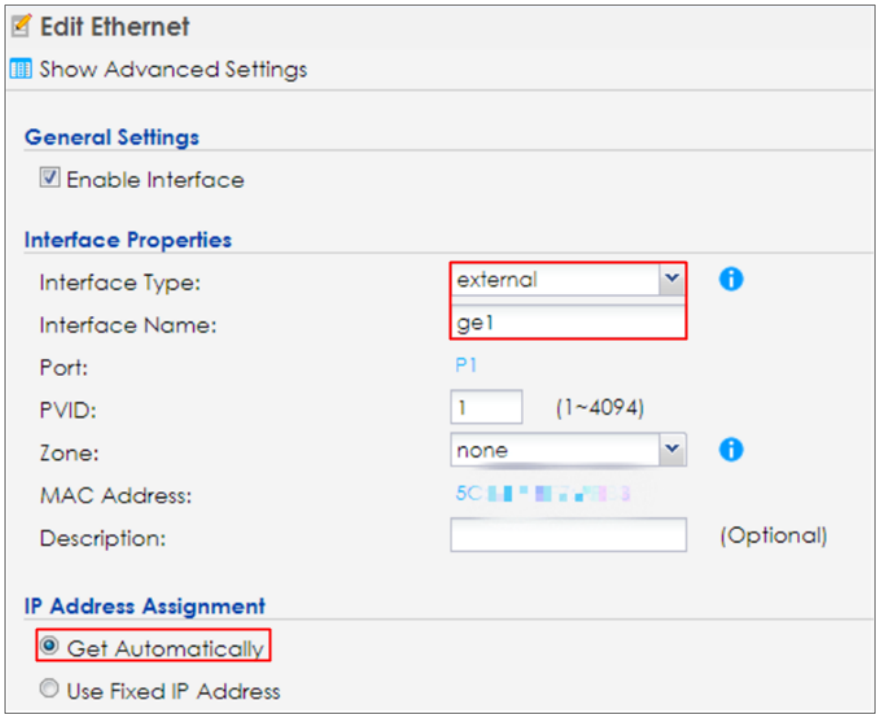
4 **Logout** from NXC controller.

5.1.4 Configure AP Profile when NXC is the Gateway

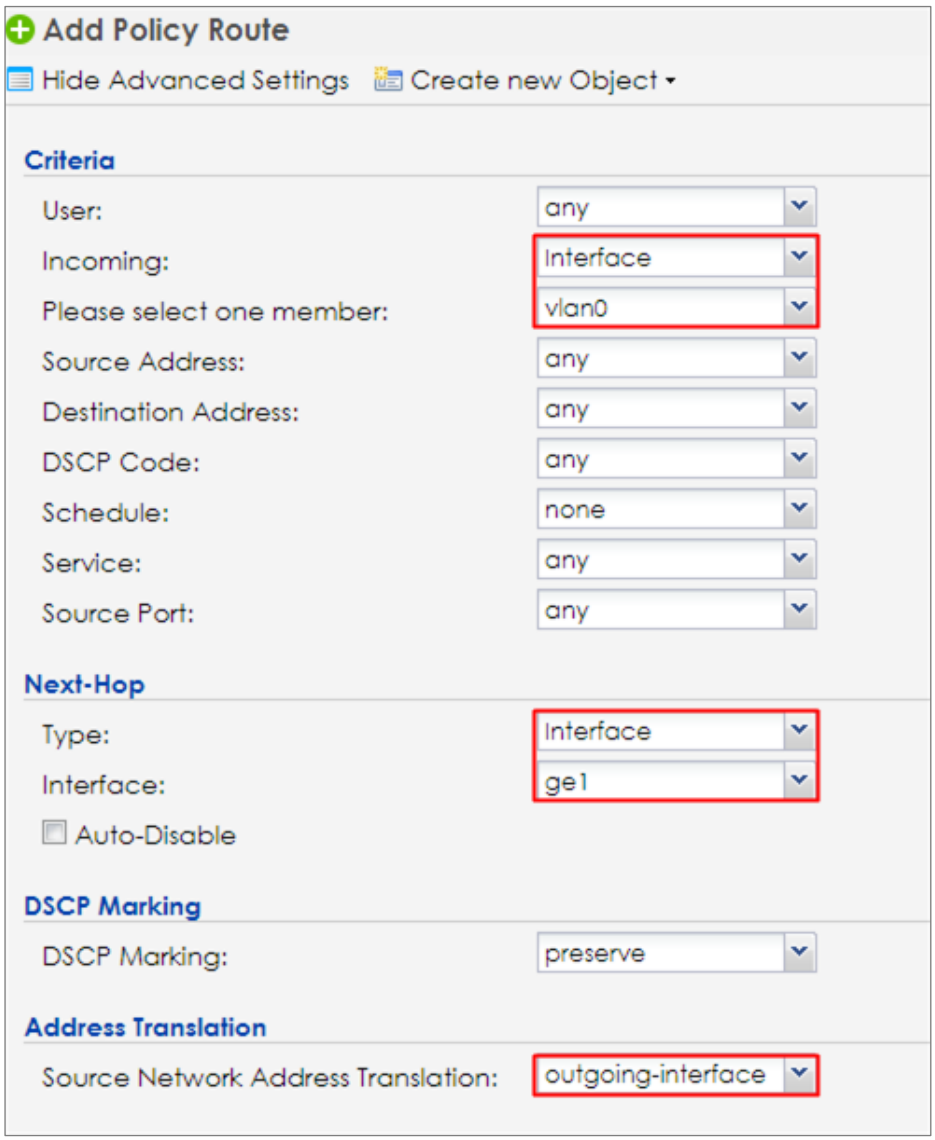
1 Make sure the NXC is the gateway for vlan0 interface which is the captive portal and stations need to connect to. Go to **CONFIGURATION > Network > Interface > VLAN > vlan0 > Edit**, select **no** in Member for ge1 and enter the NXC's IP in **Gateway**. Enable **DHCP server** and set the IP from **192.168.1.100 to 192.168.1.200** (IP pool 100). The **Default Router** is **vlan0**. Click **OK** to apply settings



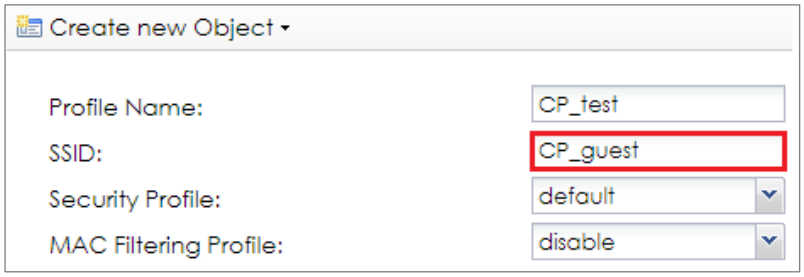
2 Go to **CONFIGURATION > Network > Interface > Ethernet**, click **ge1** and then click **Edit** to make ge1 as the external interface for connecting with the Internet. Change **Interface Type** to **external** and **IP Address Assignment** is **Get Automatically**. Click **OK** to save.



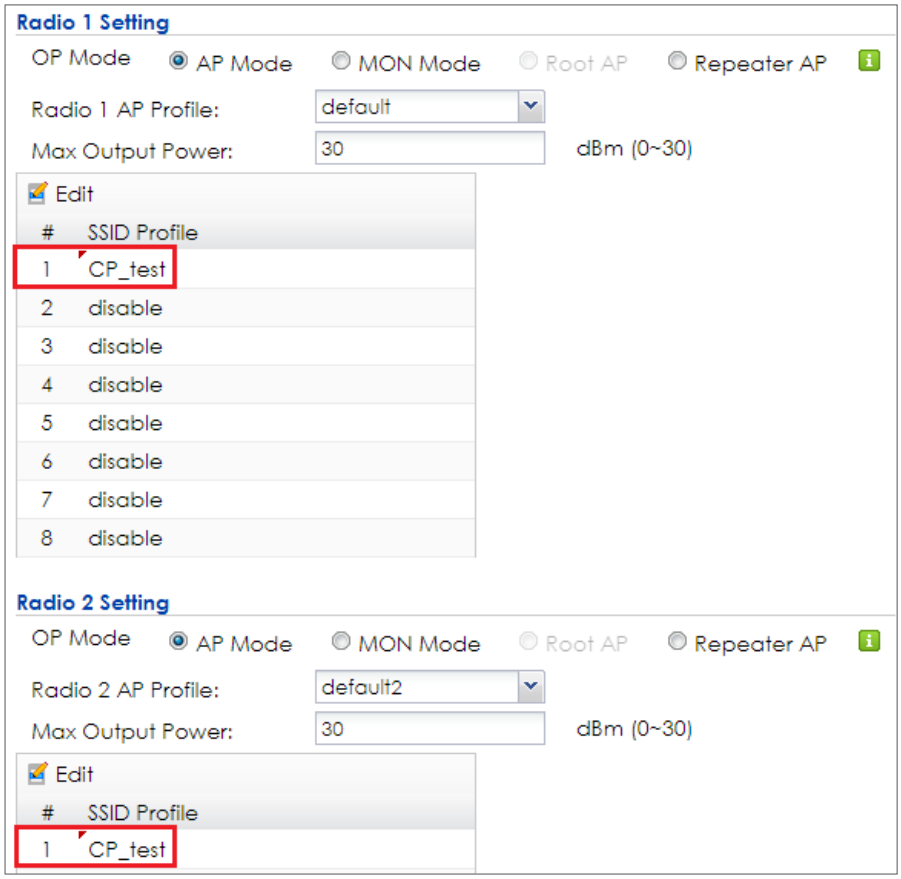
3 Go to **CONFIGURATION > Network > Routing > Policy Route**, and click **Add** to add a routing rule for outgoing traffic. Click **Show Advanced Settings**. Check **Enable** in **Configuration**. Select **Interface** in **Incoming** and select to **vlan0** in **Please select one member**. Change **Type** to **Interface** and select **Interface ge1**. Change **Source Network Address Translation** to **outgoing-interface**. Click **OK**.



4 Go to **CONFIGURATION > Object > AP Profile > SSID > SSID List**, and click **Add** to add a SSID for captive portal. Key in the **SSID** to **CP_guest**, and change **Security Profile** to **default** which sets none security. Click **OK** to save.

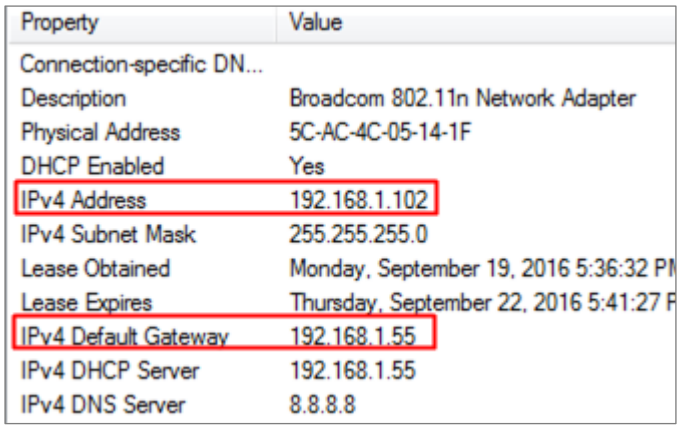


5 Go to **CONFIGURATION > Wireless > AP Management > AP Group**, and click **default** to **Edit**. Change **#1** to **CP_test** which is created in step2. Click **Override Member AP Setting** to apply the SSID to AP and click **Yes** in the pop-up window. Click **OK**

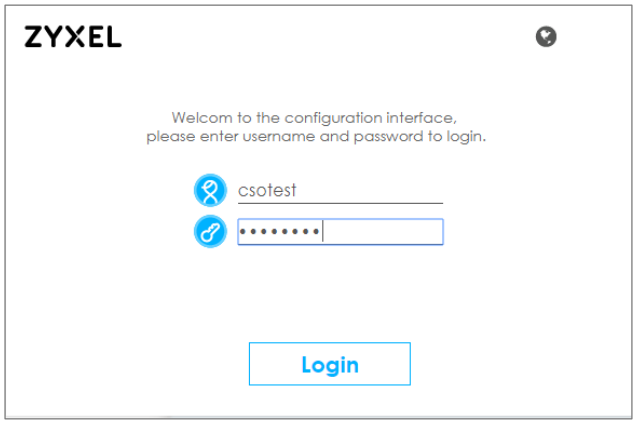


5.1.5 Test the Result

1 Connect to SSID CP_guest from the computer. After the connection is successfully established, check if the IP is in the range from 192.168.1.100 to 192.168.1.200, and the gateway is NXC's IP.

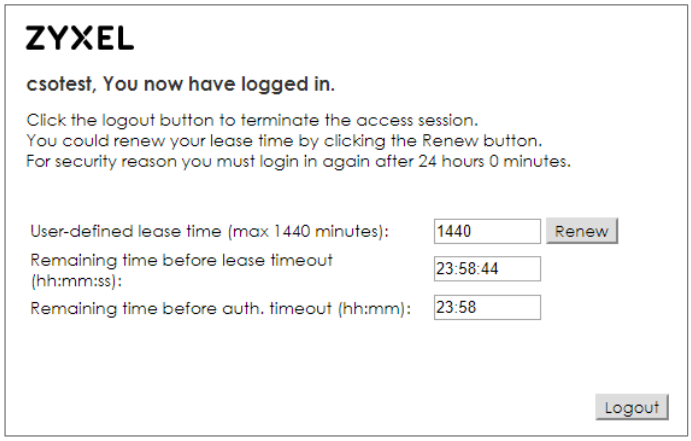


2 Open a browser and visit a website it after the computer connects to the AP successfully. The browser redirects to the captive portal page and needs to enter the username and password for authentication before accessing the Internet.



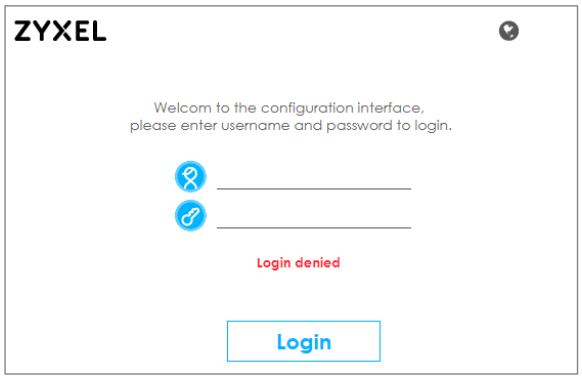
3 If you use redirect by FQDN, the website address shows the domain name you set in captive portal authentication Type.

4 After entering the username and password correctly, the connected station is able to access the Internet now. There is also a pop-window to show the detail information of the renew time and re-authentication time after authentication succeed.

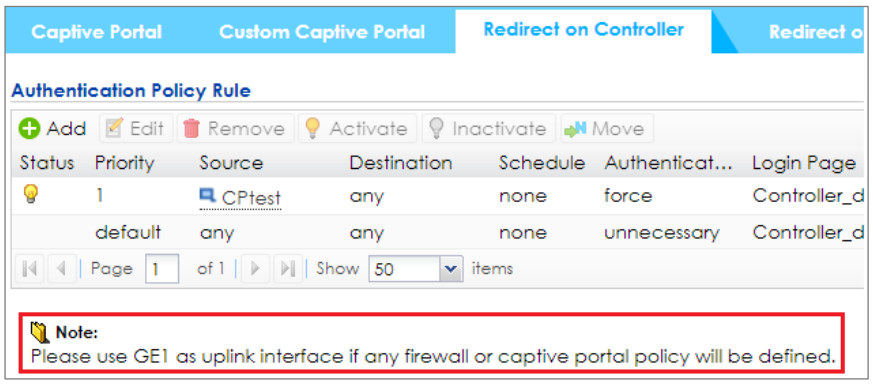


5.1.6 What Could Go Wrong

1. The DNS **MUST** be set in the DHCP setting, or the captive portal might fail to redirect because NXC controller is not able to know the correct IP address of the website which stations access to.
2. The captive portal fails to redirect the webpage if the station logs in to the NXC controller before and does not logout.
3. When USG is the gateway, the **Forwarding Mode** MUST be **Tunnel** mode to make sure the traffic from AP goes to NXC controller.
4. If the user enters an incorrect username or password, there is a login failure webpage. Please use the correct username and password to log in again.



5. When using the NXC2500 as the controller, the uplink port MUST be ge1.



5.2 How to Configure Captive Portal Redirect on AP?

The example instructs how to set up captive portal redirect on the AP. A captive portal can intercepts network traffic, according to the authentication policies, until the user authenticates his or her connection, usually through a specifically designated login web page. Typically, you often find captive portal pages in public hotspots.

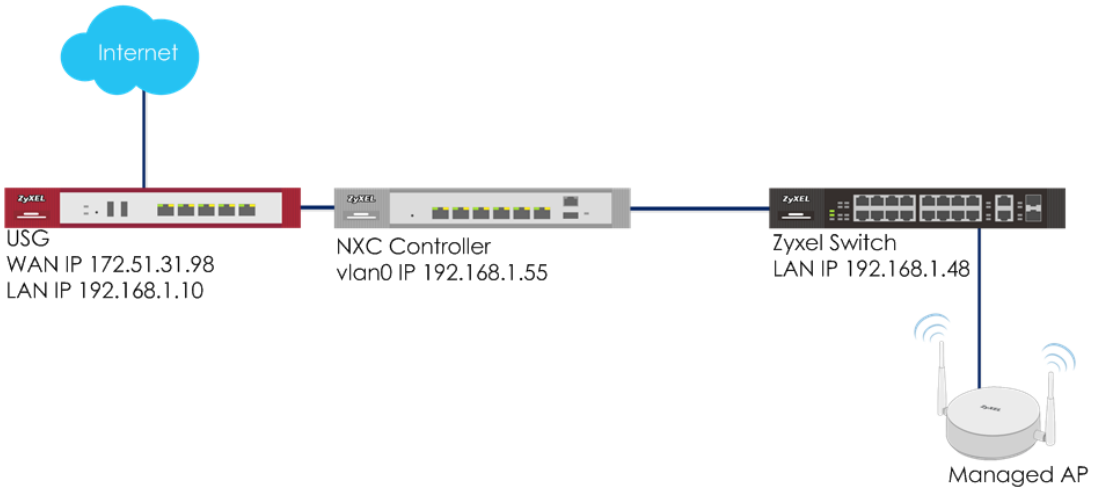


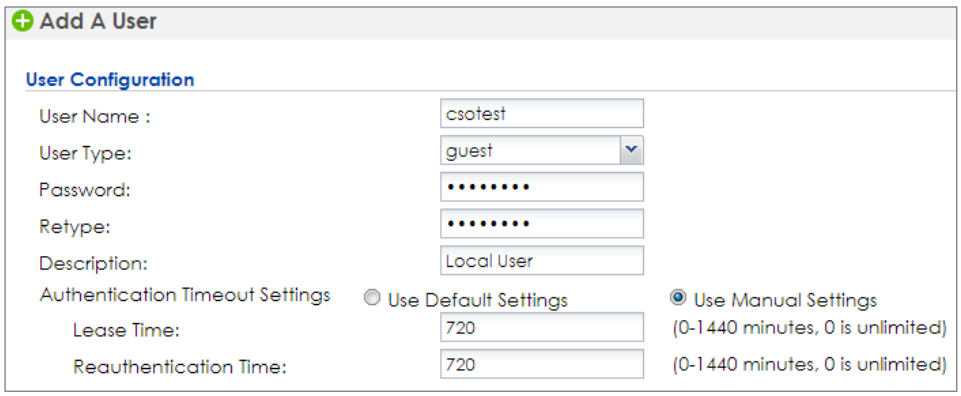
Figure 5.2 Captive portal redirect on AP

Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC5500 (Firmware Version: 5.40), GS2210-8HP (Firmware Version: V4.30).

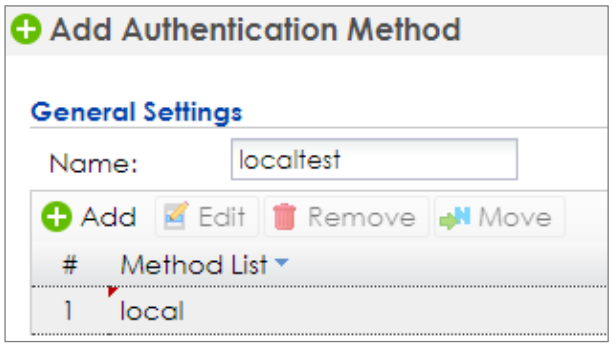
5.2.1 Configure AP Profile and User

1 Go to **CONFIGURATION > Object > AP Profile > SSID > SSID List**, click **Add** to add a SSID for captive portal. Key-in the **Profile Name** is **CP_test** and **SSID** as **CP_guest**, and select **Security Profile** to **default** which sets none security. Click **OK** to save.

2 Go to **CONFIGURATION > Object > User/Group**, and click **add** to create a new user ID and password. Stations can log in captive portal to access Internet via this account. Enter the **User Name** as login ID for captive portal and **User Type** is **guest**. Enter the **Password** as the login password. The default of **Authentication Timeout Setting** is 1440 minutes, and usually it's shorter for guests. Select to **Use Manual Settings** to set **Lease Time** and **Reauthentication Time**. Click **OK** to save.



3 Go to **CONFIGURATION > Object > Auth. Method**,and click **add** to create an authentication method. Enter the **Name** of this authentication method and select to local in the **Method List**.

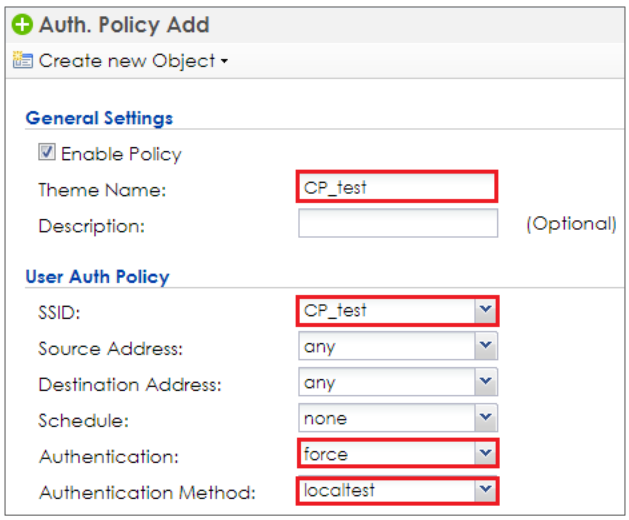


5.2.2 Configure Captive Portal

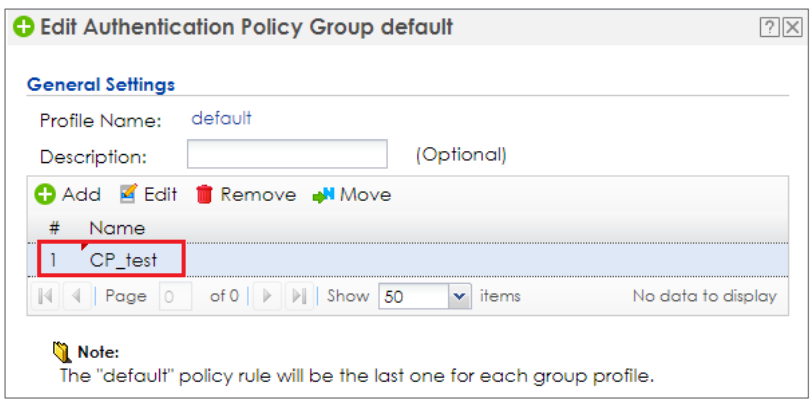
1 Go to **CONFIGURATION > Captive Portal > Redirect on AP > Authentication Policy Rule**, and click **add** to create a policy rule for stations which connect to SSID profile CP_test.

In **General Settings**, check **Enable Policy** and enter the **Profile Name** of this policy.

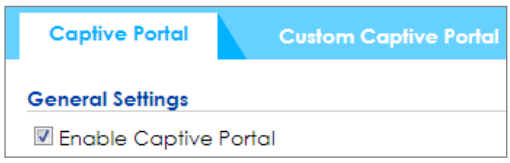
In **User Auth Policy**, change **SSID** to **CPtest** and **Authentication** is **required**. Check **Force User Authentication**, and change the **Authentication Method** to **localtest**. Click **OK** to save.



2 Go to **CONFIGURATION > Captive Portal > Redirect on AP > Authentication Policy Group**, and click **default** to edit. In the setting, click **Add** to add the policy rule which is created in previous step.

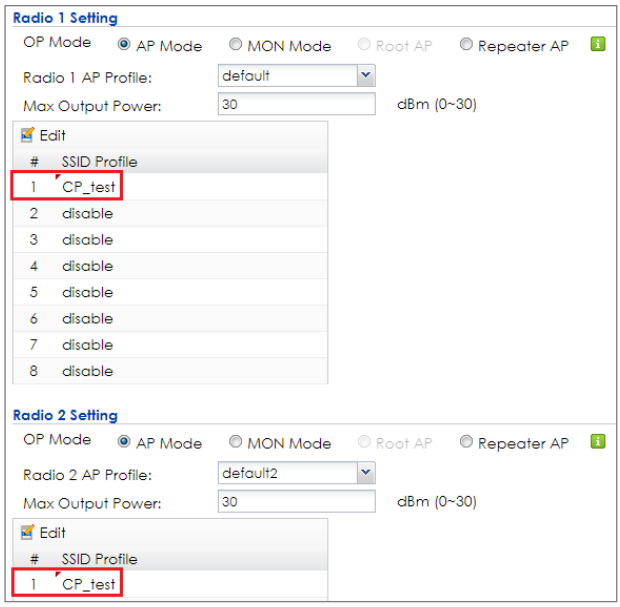


3 Go to **CONFIGURATION > Captive Portal > Captive Portal**, check **Enable Captive Portal**. Click **Apply** to apply the settings

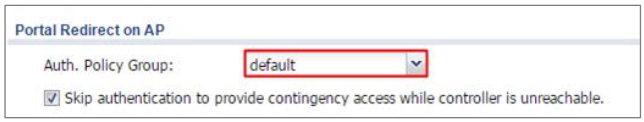


5.2.3 Broadcast SSID

1 Go to **CONFIGURATION > Wireless > AP Management > AP Group**, click **default** to **Edit**. Change **#1** to **CP_test**.



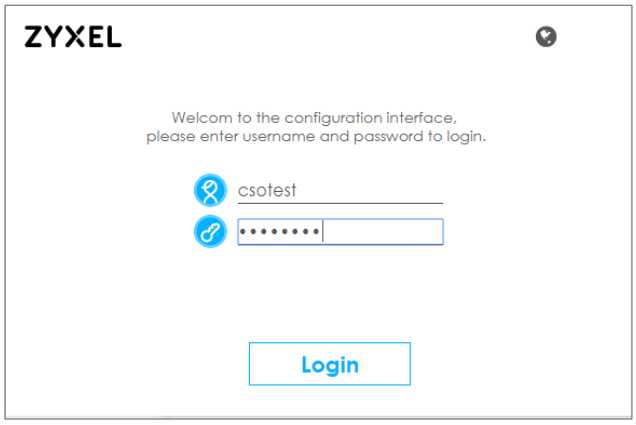
2 In the same setting page as previous step, select **default** for **Auth. Policy Group** in **Poral Redirect on AP**. Click **OK** to save.



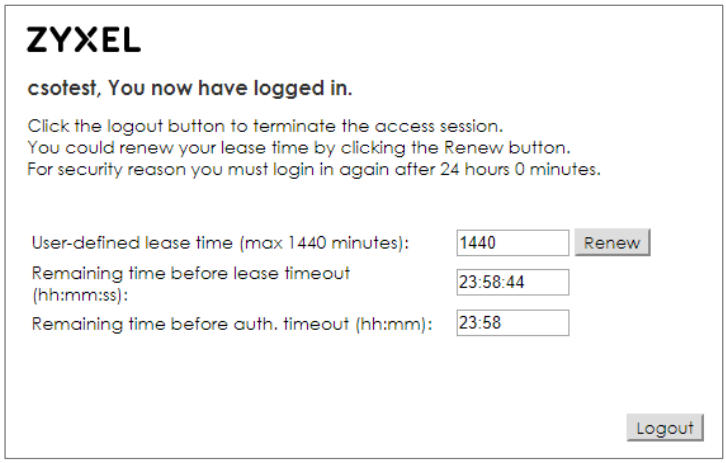
3 **Logout** from NXC controller.

5.2.4 Test the Result

1 Connect the station to the SSID 'CP_guest'. Open a browser and visit a website after the computer and AP connect successfully. The browser redirects the webpage to captive portal page and the user needs to enter the username and password for authentication before accessing the Internet

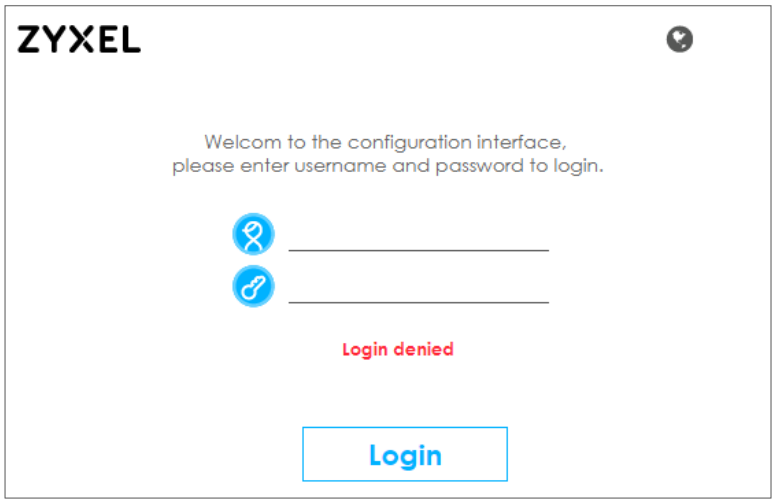


2 After entering the username and password correctly, the connected station is able to access the Internet now. There is also a pop-window to show the detail information of the renew time and re-authentication time after authentication succeed.



5.2.5 What Could Go Wrong

1. The DNS **MUST** be set in the DHCP setting, or the captive portal might fail to redirect because NXC controller is not able to know the correct IP address of the website which stations access to.
2. The captive portal fails to redirect the webpage if the station logs in to the NXC controller before and does not logout.
3. When you use redirect on AP, the **Forwarding Mode** MUST be **Local bridge** mode.
4. If the user enters an incorrect username or password, there is a login failure webpage. Please use the correct username and password to log in again.



5.3 How to Configure Captive Portal with QR Code?

The example instructs how to set up captive portal authentication with QR code. This new feature offers two convenient and fast methods to access the Internet. The first method is authenticator assisted. This means that the employees are the authenticators, who can authenticate the guest to access the Internet. The second method is self-serviced. The guest can use a mobile device to scan the QR code to pass the authentication.

The Captive portal with QR code can be utilized for some applications including private enterprises, schools, seminars, meetings and guests to access the network through the duration of their visit.

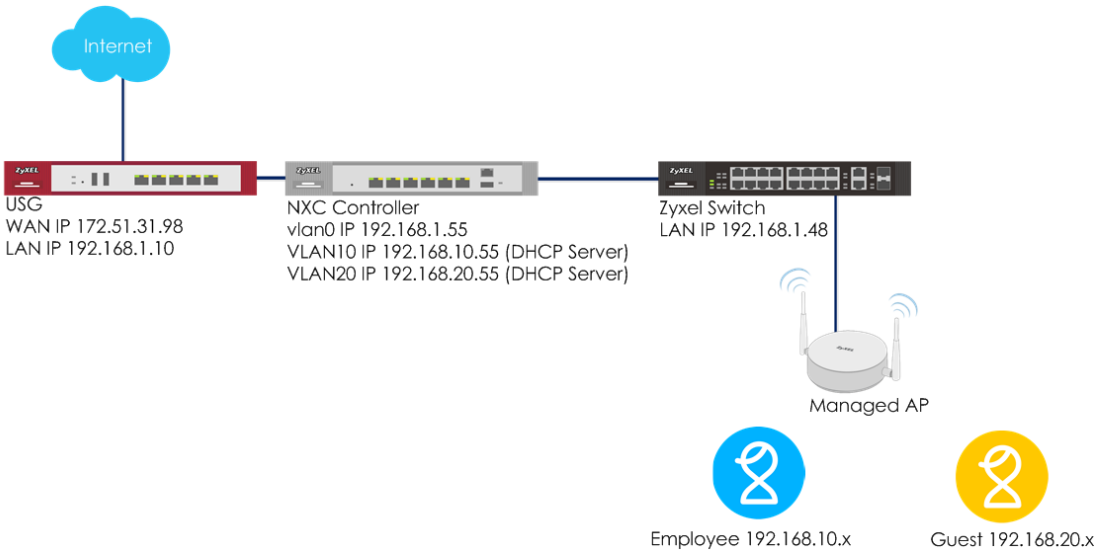
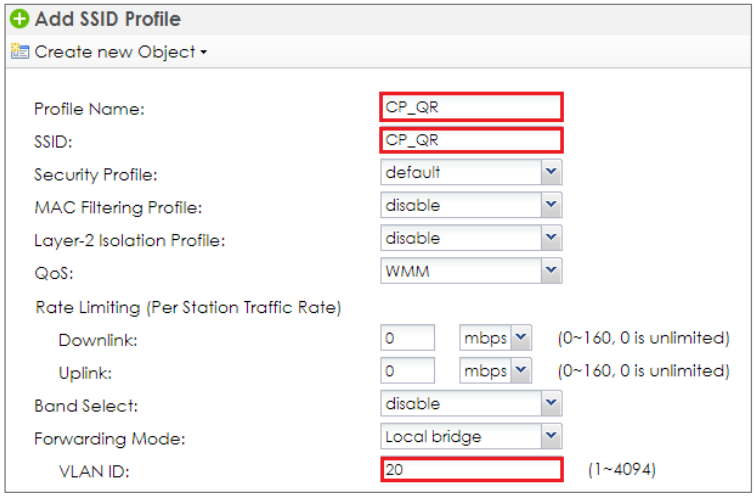


Figure 5.3 Captive portal redirect on AP

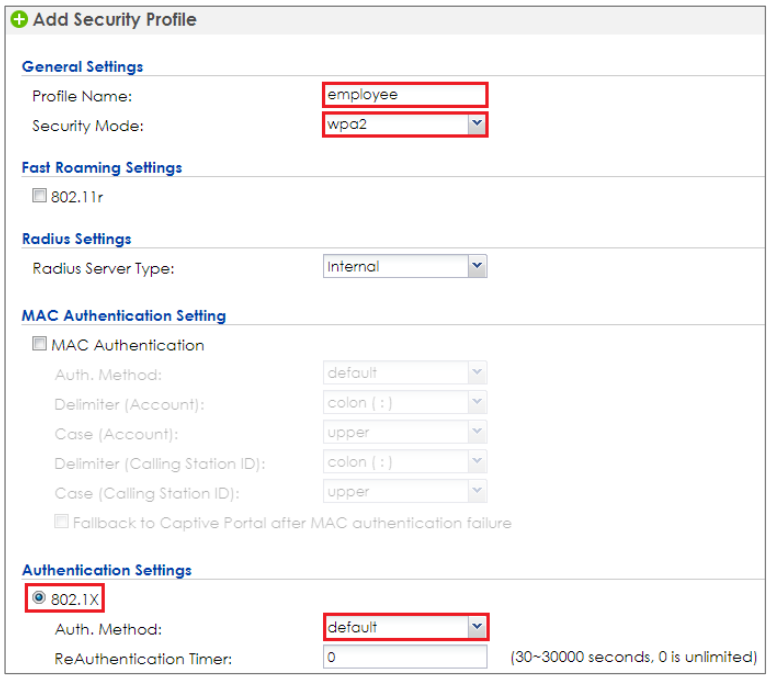
Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC2500 (Firmware Version: 5.30), GS2210-8HP (Firmware Version: V4.30).

5.3.1 Configure AP Profile

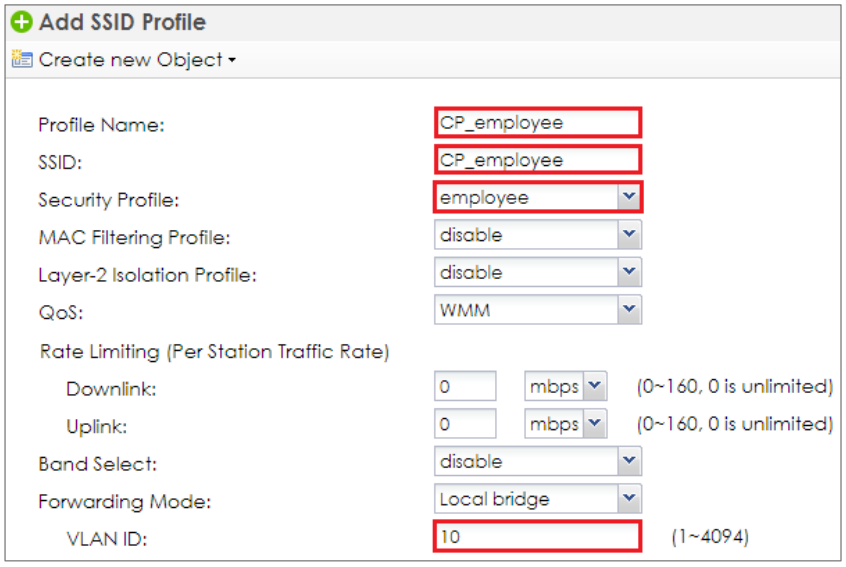
1 Go to **CONFIGURATION > Object > AP Profile > SSID > SSID List**, and double click **default** to modify the SSID for captive portal. Key in the **SSID** to **CP_QR**, and change **Security Profile** to **default** which sets none security. The VLAN ID is set to 20. Click **OK** to save.



2 Go to **CONFIGURATION > Object > AP Profile > SSID > Security List**, Click **Add** to add the security profile for employees. Key in the **Profile Name** and **SSID** to **employee.** Click **OK** to save.

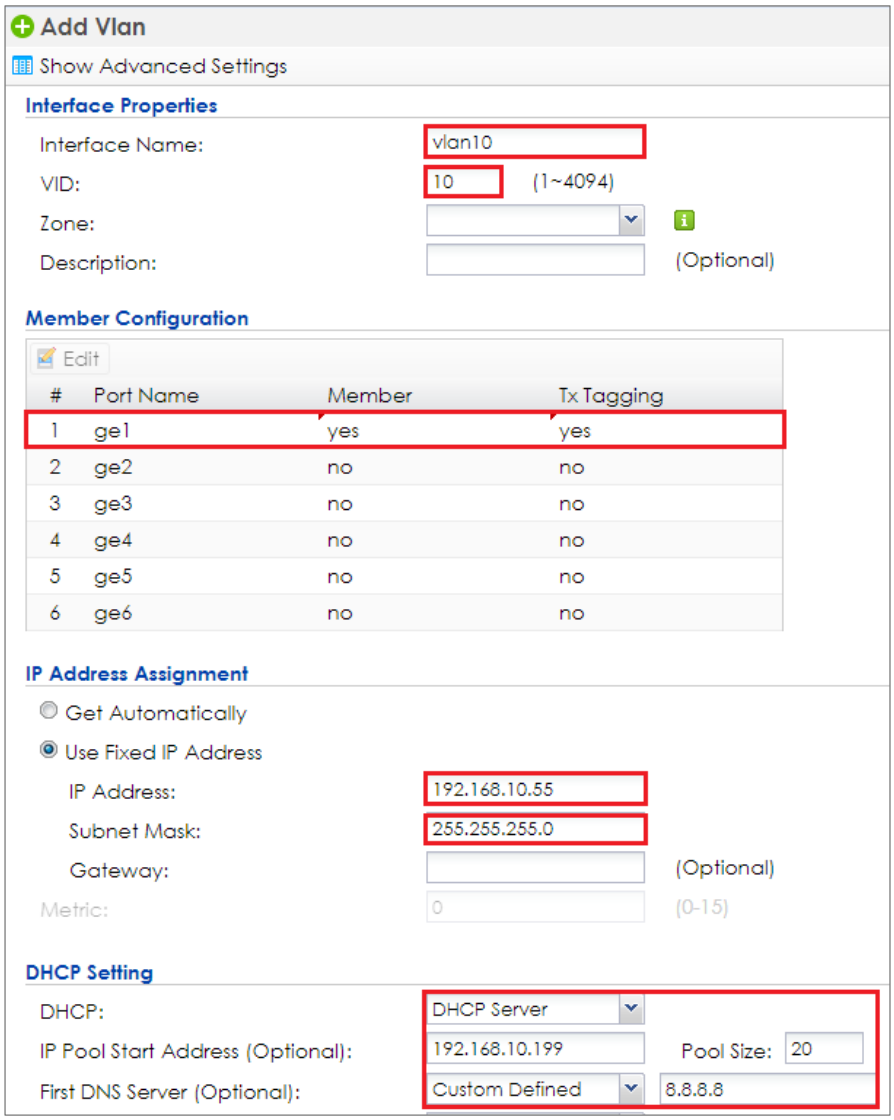


3 Go to **CONFIGURATION > Object > AP Profile > SSID > SSID List**, double click **Add** to add the SSID for employees. Key in the **Profile Name** and **SSID** to **CP_employee** with **VLAN ID 10**, and change **Security Profile** to **employee**. Click **OK** to save.

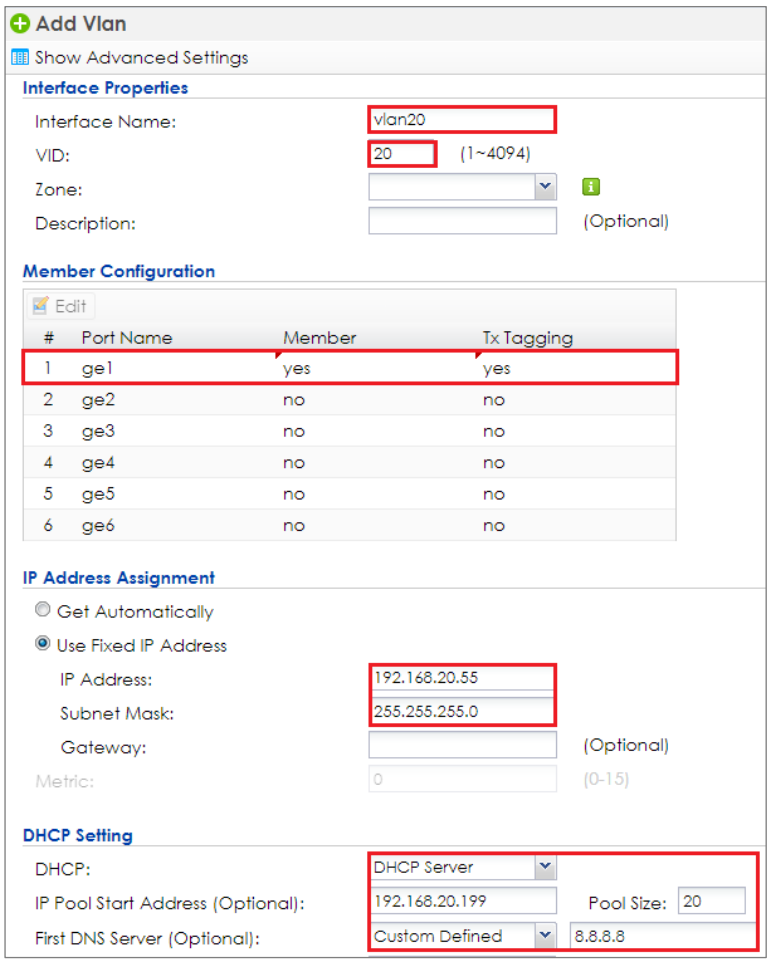


5.3.2 Configure VLAN

1 Go to **CONFIGURATION > Network > Interface > VLAN**, click **Add** to add VLAN 10 and set NXC2500 as the DHCP server of VLAN 10. Click **OK** to save.

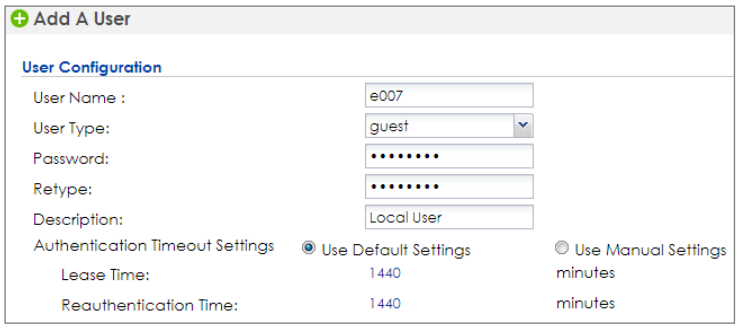


2 Go to **CONFIGURATION > Network > Interface > VLAN**, click **Add** to add VLAN 20 and set NXC2500 as the DHCP server of VLAN 20. Click **OK** to save.

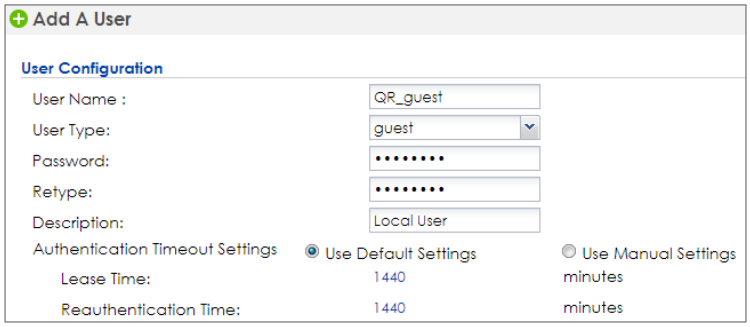


5.3.3 Create Assistance Account

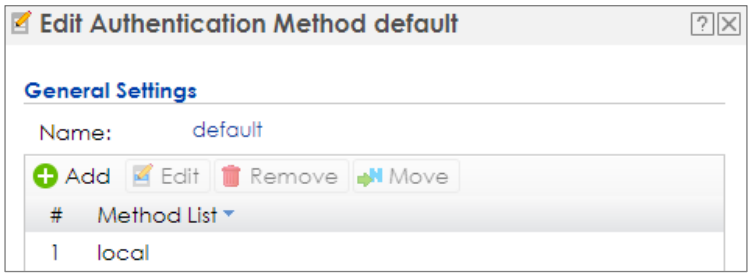
1 Go to **CONFIGURATION > Object > User/Group > User**, and click **Add** to add the user as the assistance account for employees to help the guest pass the authentication when the guest scan the QR code. Click **OK** to save.



2 Go to **CONFIGURATION > Object > User/Group > User**, and click **Add** to add the user as the assistance account to let guest self-authenticate. Click **OK** to save.

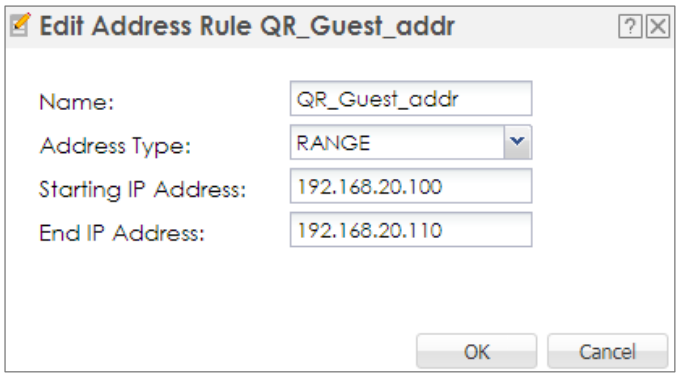


3 Go to **CONFIGURATION > Object > Auth. Method > Authentication Method**, and double click **default** to edit the method as **local**. Click **OK** to save.

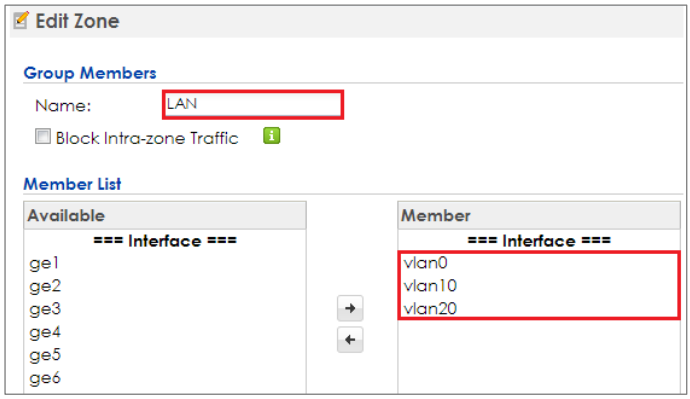


5.3.4 Set Guest Address & Zone

1 Go to **CONFIGURATION > Object > Address > Address**, click **Add** to add the guest address. Change the **Address Type** to **RANGE** and enter the starting and end IP address. Click **OK** to save.



2 Go to **CONFIGURATION > Network > Zone**, click **LAN** to edit. Change **vlan0, vlan10, vlan20** to the same zone and then the employee's account can help to do captive portal authentication. Click **OK** to save.

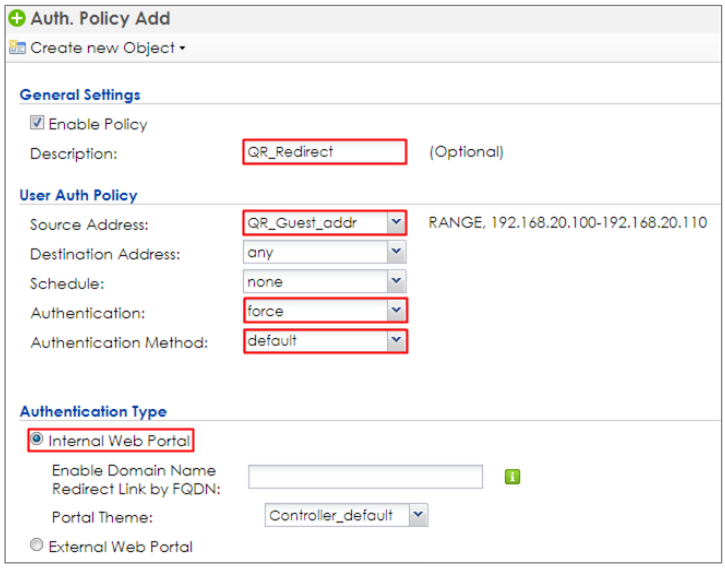


5.3.5 Configure Captive Portal

1 Go to **CONFIGURATION > Captive Portal > Redirect on Controller > Authentication Policy Rule**, click **add** to create a policy rule for guests whose IP addresses are in the setting range.

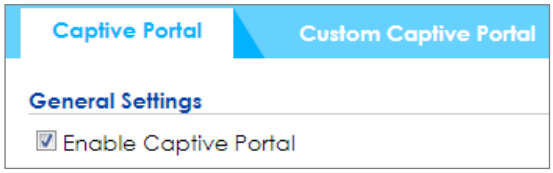
In **User Auth Policy**, change **Source Address** to **QR_Guest_addr** and **Authentication** is **required**. Check **Force User Authentication** to force every connected IP in the range to be redirected to captive portal. Change the **Authentication Method** to **default**.

In **Authentication Type**, use the **Internal Web Portal**.

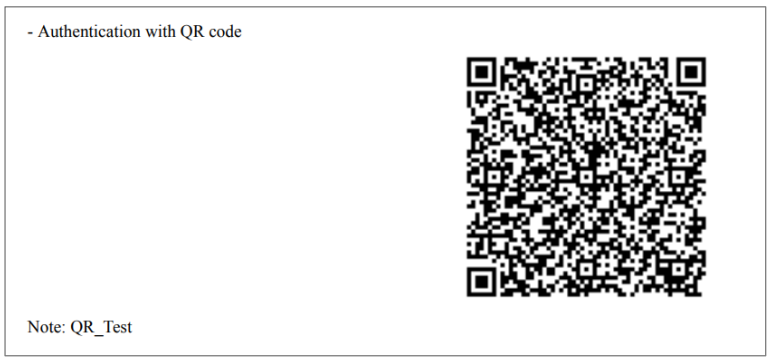


2 In the same page of step 1. Check the Authentication with QR code, and change the Guest Account to QR_Guest. Check **Authenticator-assisted** and the **QR Portal Address** is vlan10 interface IP. The **Authenticator** is the employee account or group. Click **Apply**.

3 Go to **CONFIGURATION > Captive Portal > Captive Portal**. Check **Enable Captive Portal**. Click **Apply**.

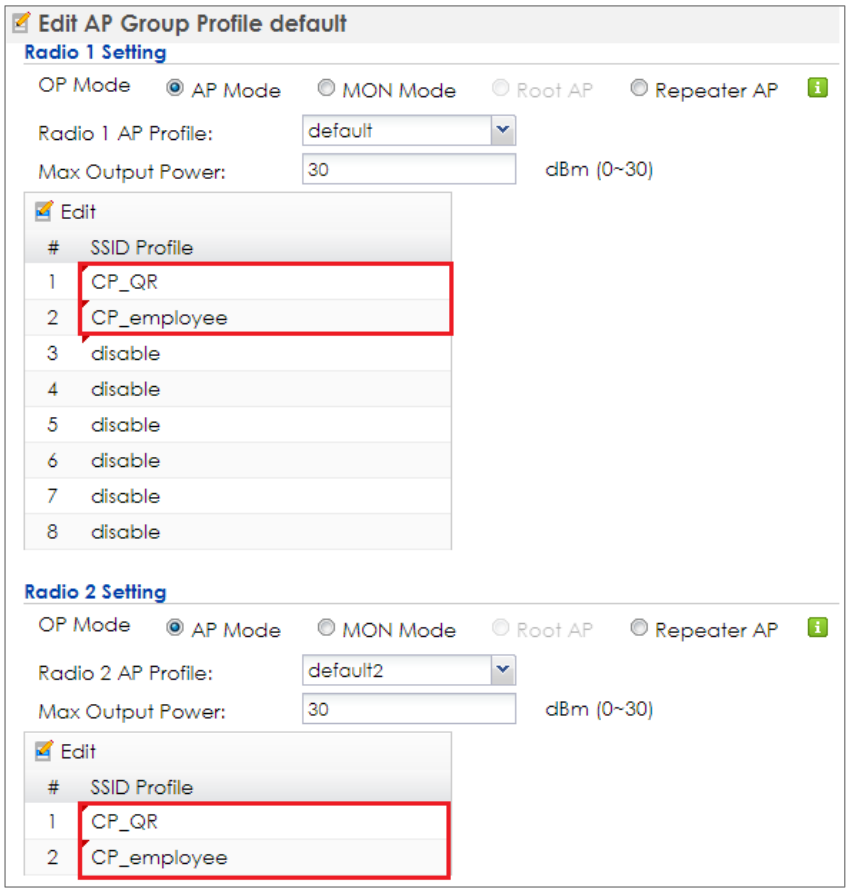


4 Go to **CONFIGURATION > Captive Portal > Redirect on Controller > QR Code Configuration**. Check **Print Out QR Code** and use the QR code for customer to do self-service.



5.3.6 Broadcast SSID

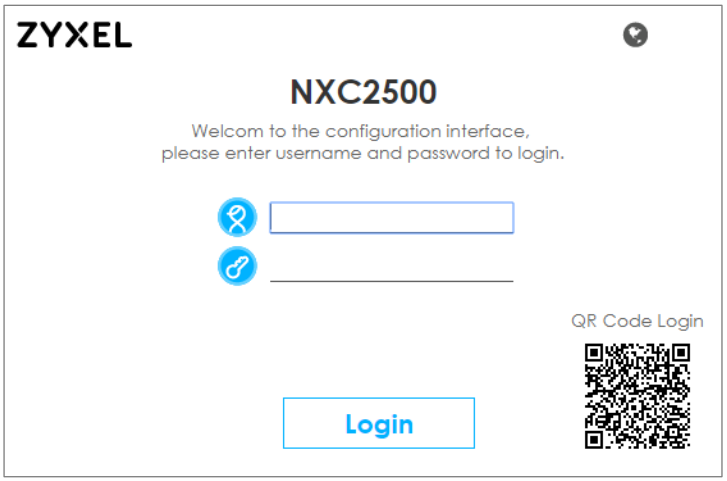
1 Go to **CONFIGURATION > Wireless > AP Management > AP Group**, click **default** to **Edit**. Change **#1** to **CP_QR** and **#2** to **CP_employee**.



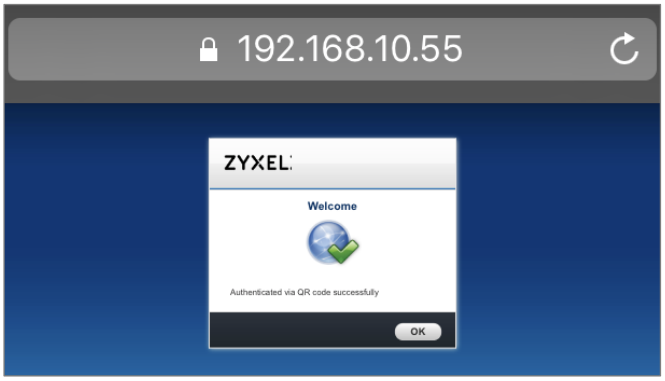
5.3.7 Test the Result

1 Authenticator-assisted

i. When the guests connect to the SSID 'CP_QR', they get IP addresses between 192.168.20.100 to 192.168.20.110, and are redirected to captive portal with QR code as shown below.

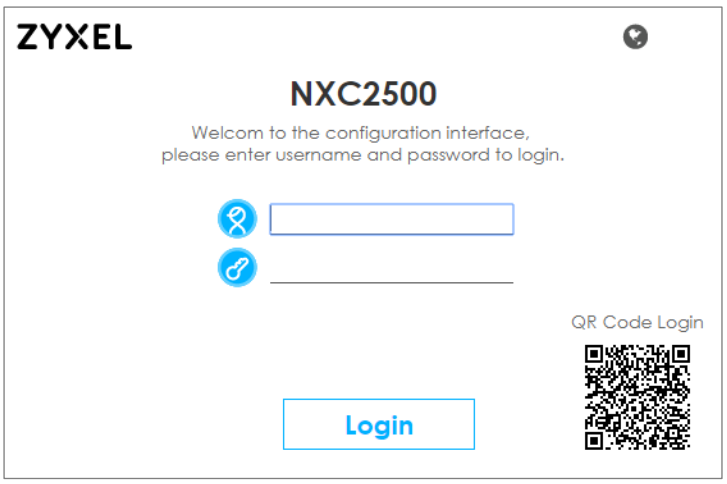


ii. When the captive portal page is shown, the customer asks for an employee who has connected with SSID "CP_employee" and gets the employee's help to scan the QR code. After the employee scans the QR code, there's a welcome page. The customer is able to access the Internet after the welcome page display.

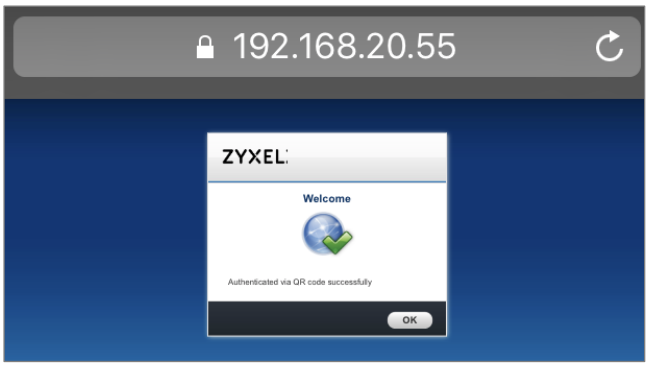


2 Self-serviced

i. When the guests connect to the SSID 'CP_RQ', they get an IP addresses between 192.168.20.100 to 192.168.20.110, and is redirected to captive portal with QR code as shown below.

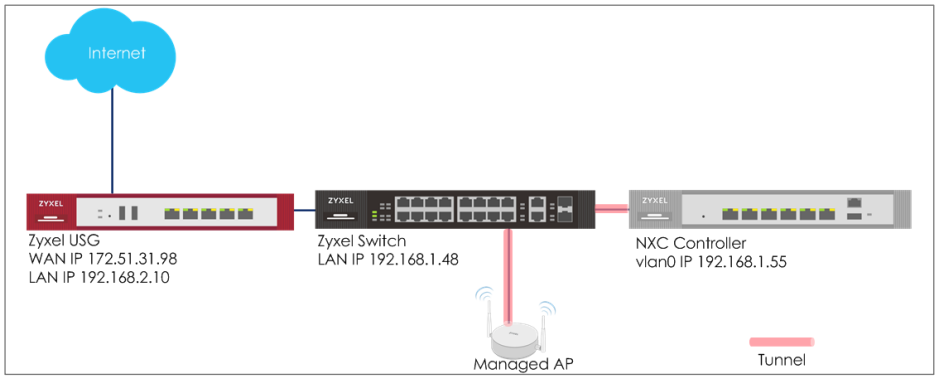


ii. When the captive portal page is shown, the guest scans the printed QR code in the last step. After scanning the QR code, a welcome page display and the guest is able to access the Internet.

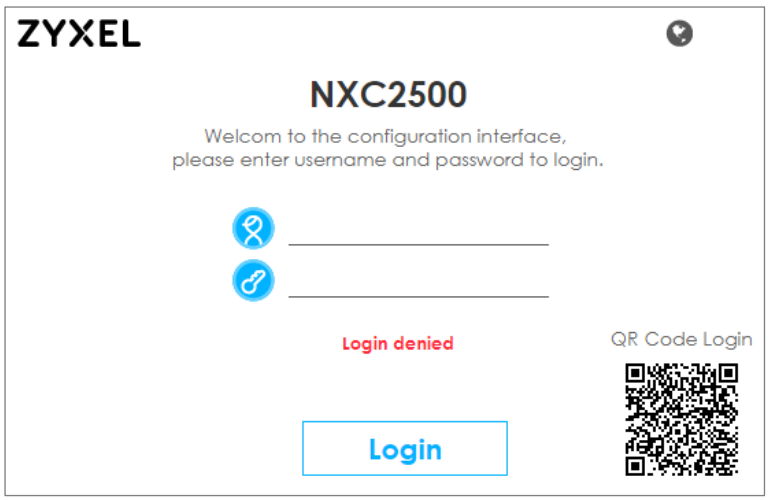


5.3.8 What Could Go Wrong

1. The DNS **MUST** be set in the DHCP server, or the captive portal might fail to redirect because NXC controller is not able to know the correct IP address of the website which stations want to access.
2. The captive portal fails to redirect the webpage if the station logs in to the NXC controller before and does not logout.
3. When USG is the gateway as shown in the topology below, the **Forwarding Mode** MUST be **Tunnel** mode to make sure the traffic from AP goes to NXC controller.



4. If the user enters an incorrect username or password, there is a login failure webpage. Please click **Retry** and use the correct username and password to log in.



5 When using the NXC2500 as the controller, the uplink port MUST be ge1.

5.4 How to Configure Captive Portal with External Webserver?

The example instructs how to set up captive portal redirect via the external web page. A captive portal can intercepts network traffic, according to the authentication policies, until the user authenticates his or her connection, usually through a specifically designated login web page. Typically, you often find captive portal pages in public hotspots. Here is an example when the customer wants to use an external captive portal for wireless client's authentication.

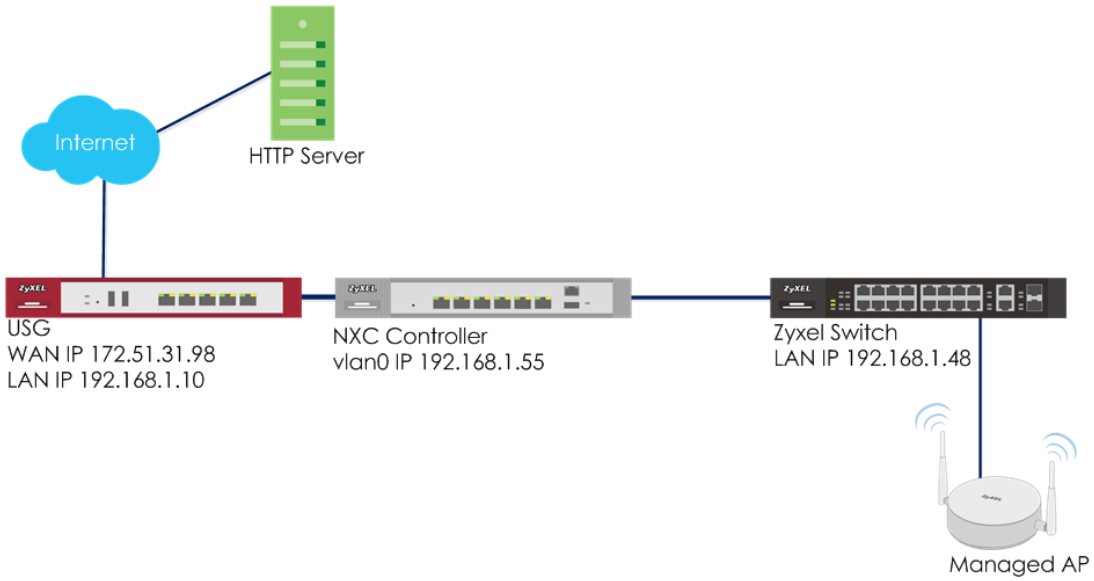
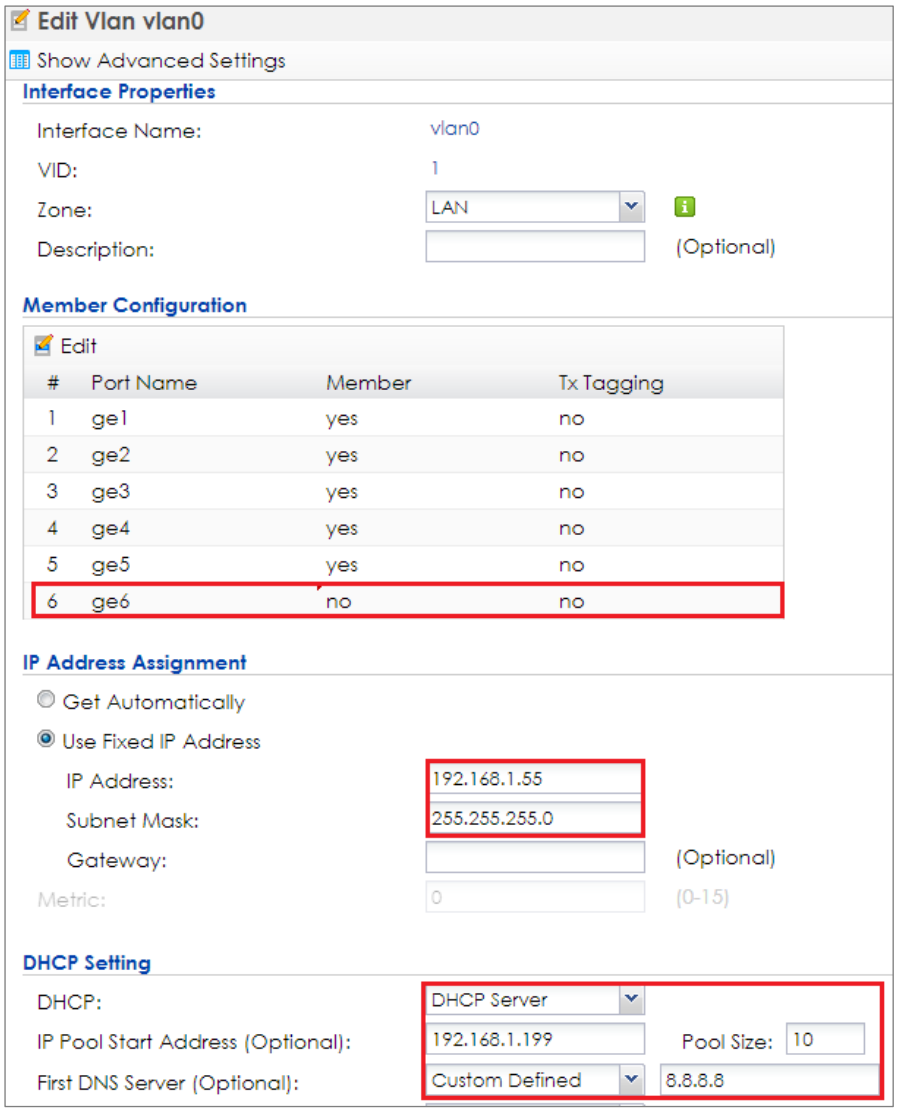


Figure 5.4 Captive Portal with External Webserver

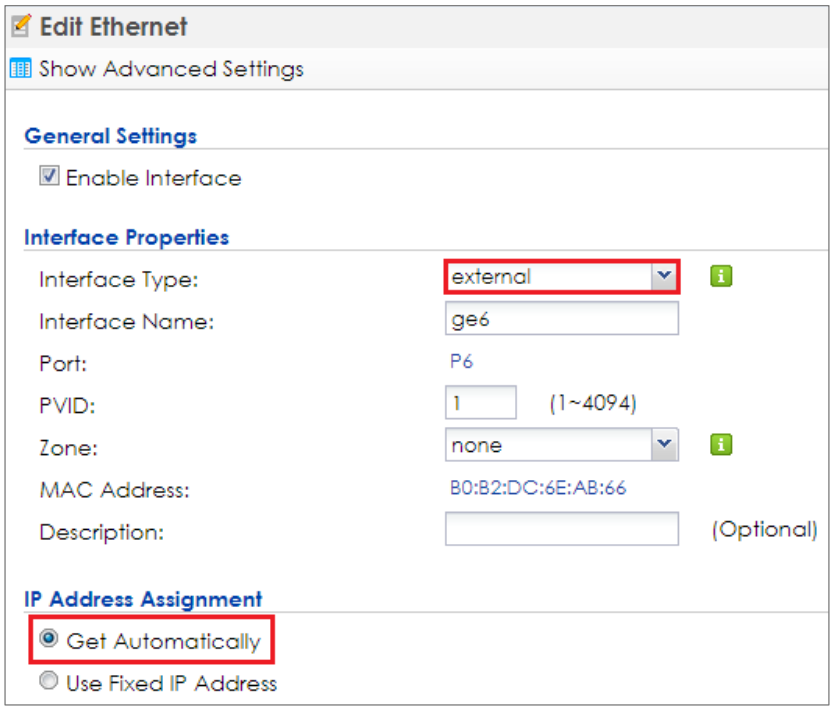
Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC2500 (Firmware Version: 5.30), GS2210-8HP (Firmware Version: V4.30).

5.4.1 Configure Interface

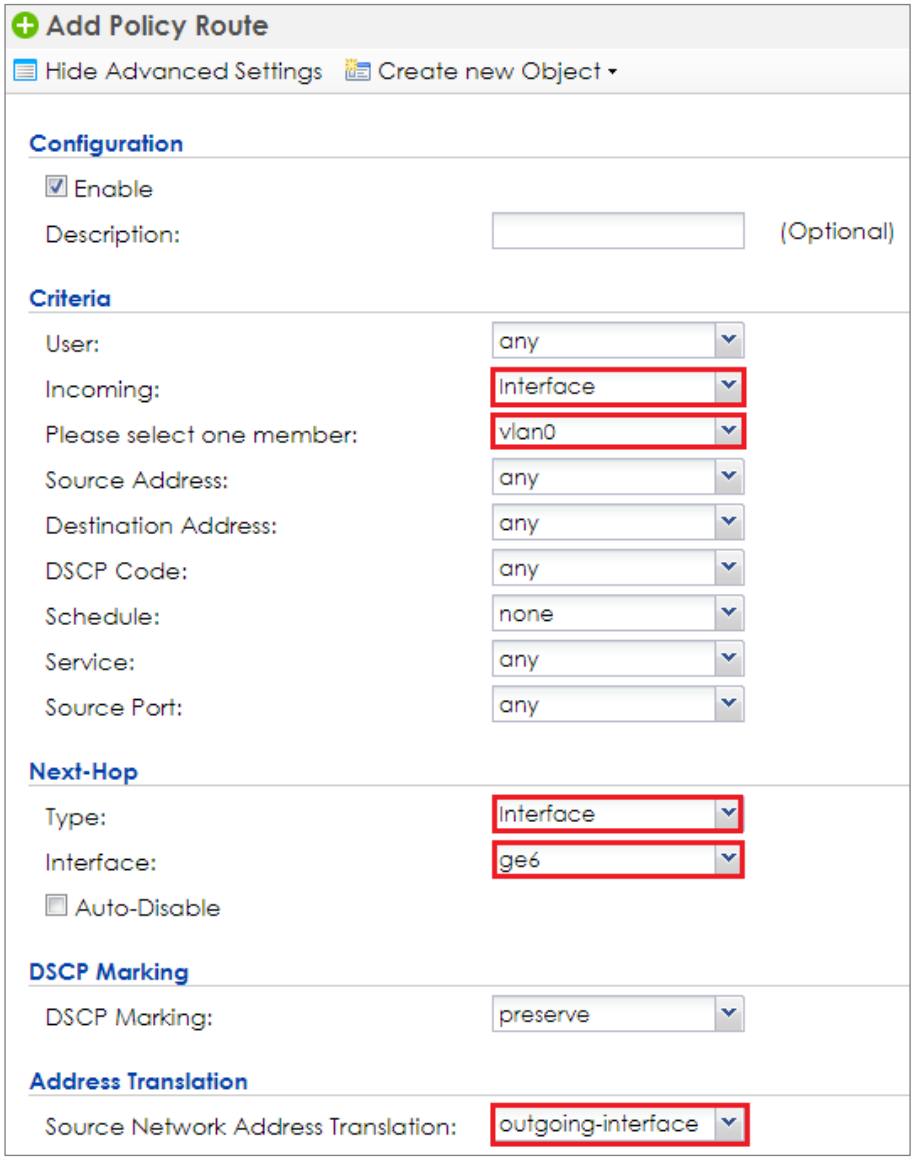
1 Go to **CONFIGURATION > Network > Interface > VLAN**, click **vlan0** and edit it. Remove ge6 by selecting "**no**" in the **Member Configuration**. Set a fixed IP for the interface, and use DHCP server with DNS. Click **OK** to save.



2 Go to **CONFIGURATION > Network > Interface > Ethernet**, select **ge6** and **Edit** it. Change the **Interface Type** to **external** Click **OK** to save.

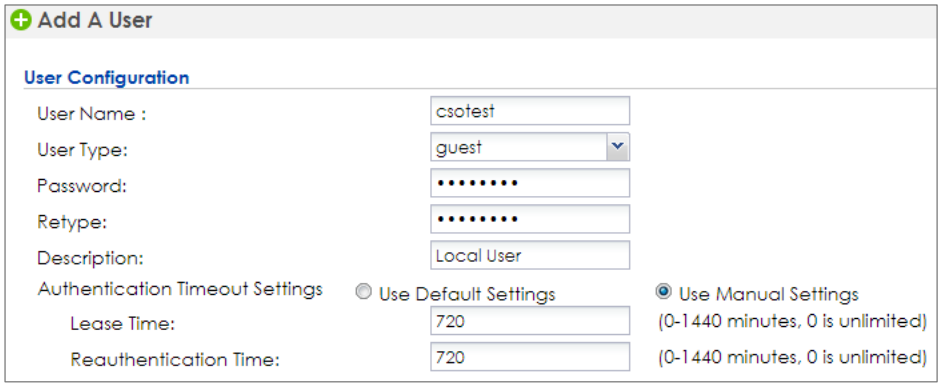


3 Go to **CONFIGURATION > Network > Policy Route**, click **Add** to add a routing rule for outgoing traffic. Click **Show Advanced Settings**. Check **Enable** in **Configuration**. Select **Interface** in **Incoming** and select to **vlan0** in **Please select one member**. Change **Type** to **Interface** and select **Interface ge6**. Change **Source Network Address Translation** to **outgoing-interface**. Click **OK**.

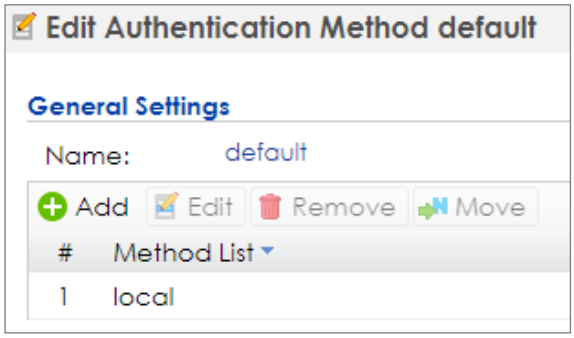


5.4.2 Configure Authentication Method Setting & Address

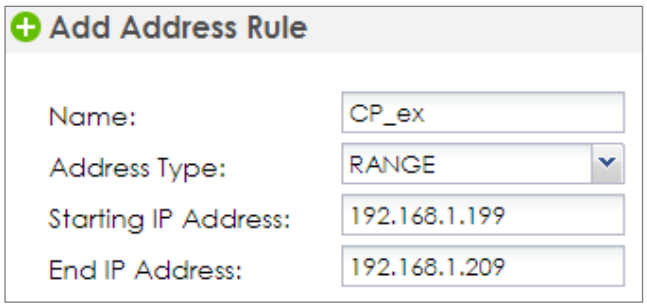
1 Go to **CONFIGURATION > Object > User/Group**, click **add** to create a new user ID and password. Stations can log in to the captive portal to access the Internet via this account. Enter the **User Name** as login ID for captive portal and **User Type** is **guest**. Enter the **Password** as the login password. The default of **Authentication Timeout Setting** is 1440 minutes, and usually it's shorter for guests. Select **Use Manual Settings** to set **Lease Time** and **Reauthentication Time**. Click **OK** to save.



2 Go to **CONFIGURATION > Object > Auth. Method**, click **add** to create an authentication method. Enter the **Name** of this authentication method and select local in the **Method List**.



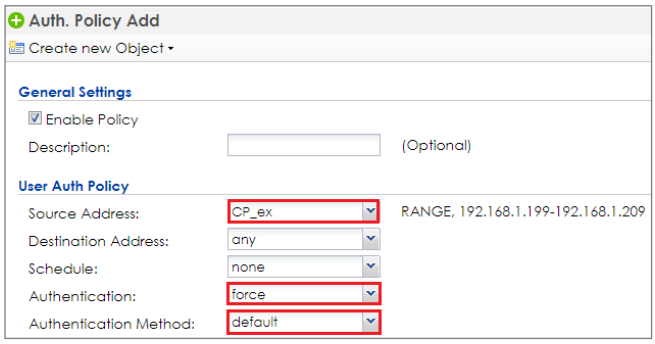
3 Go to CONFIGURATION > Object > Address > Address, click **add** to create an address range which needs to do captive portal authentication before accessing to the Internet. Enter profile **Name** and change **Address Type** to **RANGE**. In this example, the IP range for guest is **192.168.1.199** to **192.168.1.209**. Click **OK** to save.



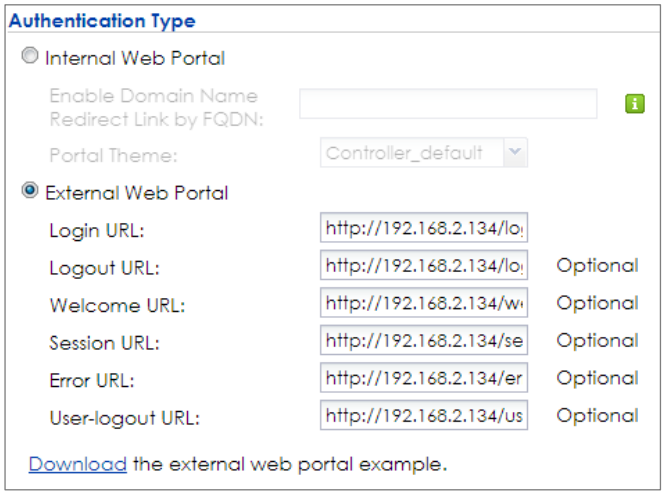
5.4.3 Configure Captive Portal

1 Go to **CONFIGURATION > Captive Portal > Redirect on Controller > Authentication Policy Rule**, click **add** to create a policy rule.

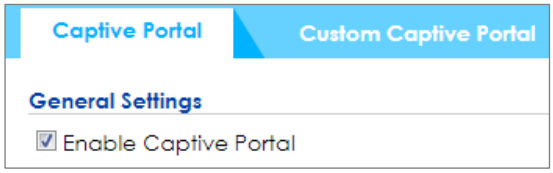
In **User Auth Policy**, change **Source Address** to **CP_ex** and **Authentication** is **required**. Check **Force User Authentication**, and change the **Authentication Method** to **default**. Click **OK** to save.



2 In the same setting page as previous step, click the "Download" hyperlink to download the external web portal example. You can use the downloaded example to add in the http server as the external webpage.



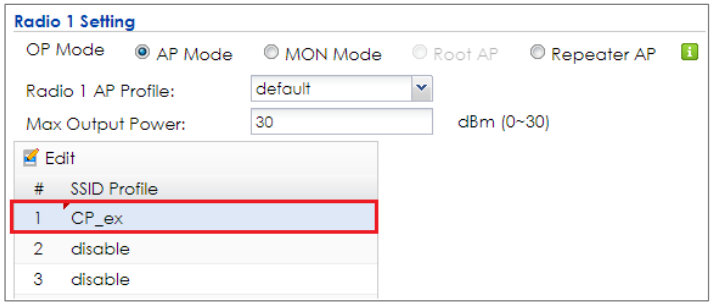
3 Go to **CONFIGURATION > Captive Portal > Captive Portal**, check **Enable Captive Portal**. Click **Apply** to apply the settings.



5.4.4 Configure AP Profile

1 Go to **CONFIGURATION > Object > AP Profile > SSID > SSID List**, double click **add** to add a SSID for wireless connection with external captive portal. Key in the **SSID** to **CP_ex**, and change **Security Profile** to **default** which sets none security. Click **OK** to save.

2 Go to **CONFIGURATION > Wireless > AP Management > AP Group**, click **default** to **Edit**. change **#1** to **CP_ex**. Click **Override Member AP Setting** to apply the SSID to AP and click **Yes** in the pop-up window. Click **OK.**

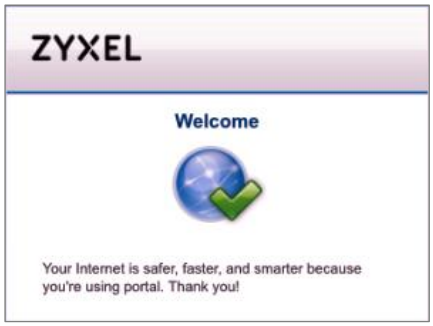


3 **Logout** from NXC controller.

5.4.5 Test the Result

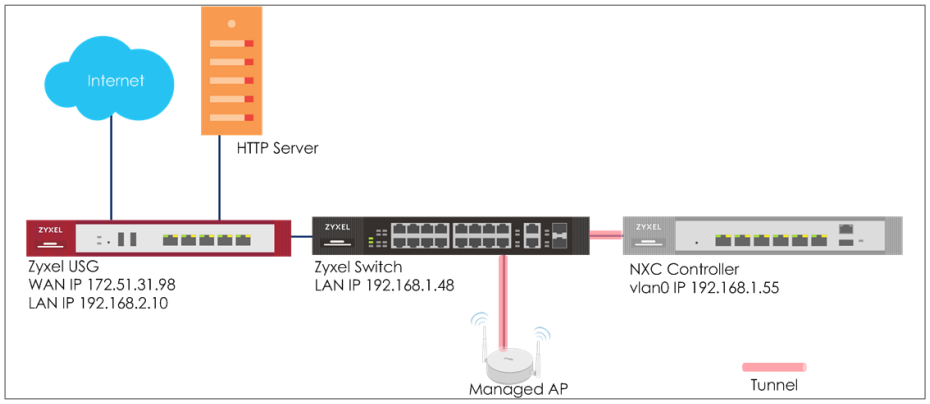
1 Connect the station to the SSID 'CP_ex'. Open a browser and visit a website after the computer and AP connect successfully. The browser redirects the webpage to external captive portal page and the user needs to enter the username and password for authentication before accessing the Internet.

2 After entering the username and password correctly, there's a successful webpage. The connected station is able to access the Internet now.

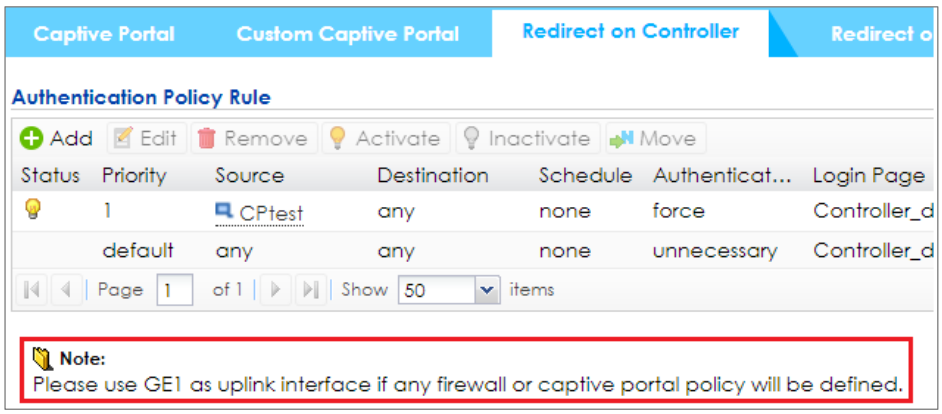


5.4.6 What Could Go Wrong

1. The DNS **MUST** be set in the DHCP server, or the captive portal might fail to redirect because NXC controller is not able to know the correct IP address of the website which stations want to access.
2. The captive portal fails to redirect the webpage if the station is log in to the NXC controller before and does not logout.
3. When USG is the gateway as shown in the topology below, the **Forwarding Mode** MUST be **Tunnel** mode to make sure the traffic from AP goes to NXC controller.



4. When using the NXC2500 as the controller, the uplink port MUST be ge1.



5.5 How to Configure Multiple Captive Portals for different users?

The example instructs how to set up different portal pages with different authentication policies and different authentication method. When there are different applications that all needs to use captive portal authentication, different portal pages and different authentication methods will be needed. Users are able to setup or upload multiple customized themes to the NXC controller. For each policy rule, users are able to select the login page and auth. method.

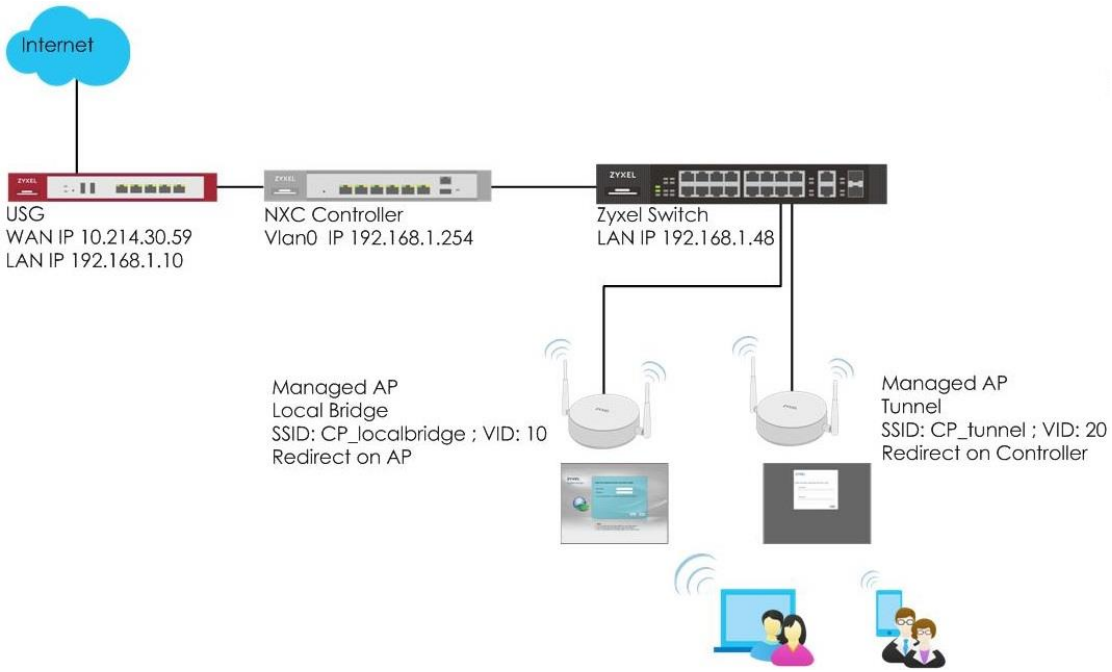


Figure 5.5 multiple captive portal for different users

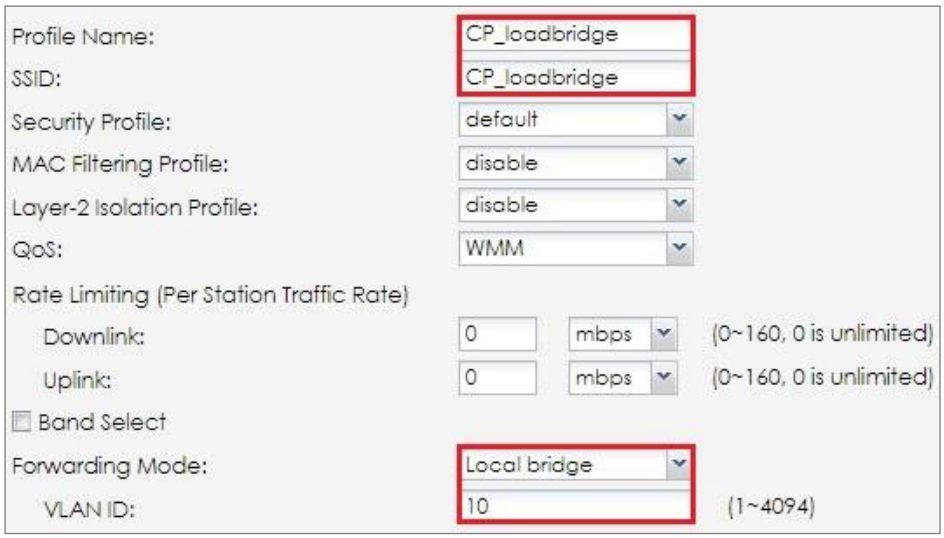
Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC2500 (Firmware Version: 5.30), GS2210-8HP (Firmware Version: V4.30).

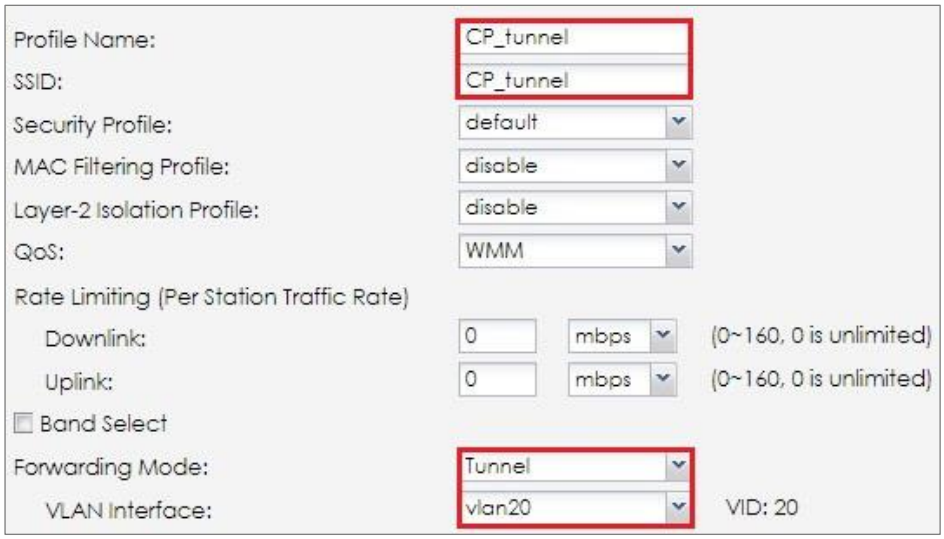
Note:
Some Zyxel APs are not supported tunnel mode, they only support localbridge mode.

- NWA5120 series (5121-NI / 5123-NI / 5121-N) / NWA5301-NJ / WAC5302D-S / NWA5123-AC-HD

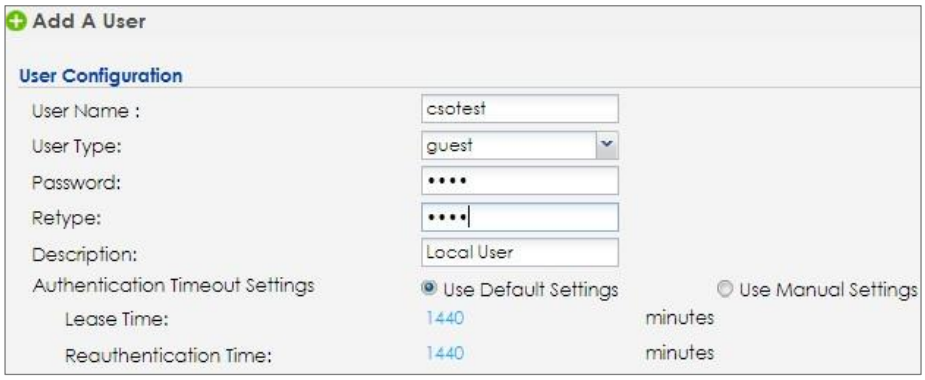
5.5.1 Configure AP Profile and User

1 Go to **CONFIGURATION > Object > AP Profile > SSID > SSID List**, click **Add** to add two SSIDs for captive portal. Key-in the **SSID names** are **CP_localbridge** and **CP_tunnel**, and select **Security Profile** to **default** which sets none security. Click **OK** to save.

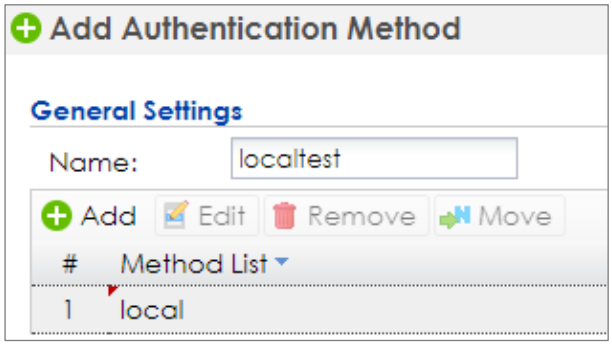




2 Go to **CONFIGURATION > Object > User/Group**, and click **add** to create a new user ID and password. Stations can log in captive portal to access Internet via this account. Enter the **User Name** as login ID for captive portal and **User Type** is **guest**. Enter the **Password** as the login password. The default of **Authentication Timeout Setting** is 1440 minutes, and usually it's shorter for guests. Select to **Use Manual Settings** to set **Lease Time** and **Reauthentication Time**. Click **OK** to save.

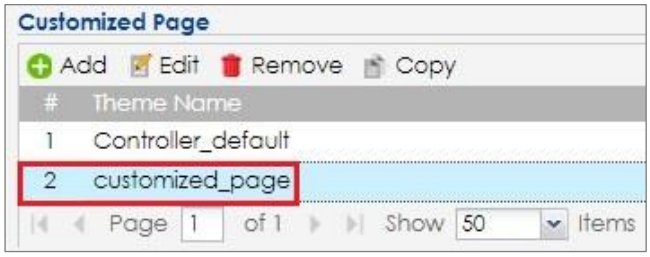


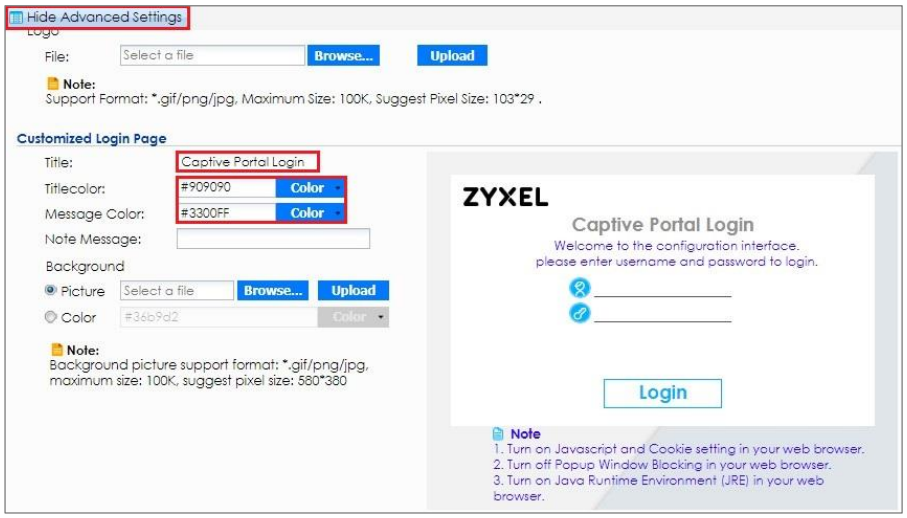
3 Go to **CONFIGURATION > Object > Auth. Method**,and click **add** to create an authentication method. Enter the **Name** of this authentication method and select to local in the **Method List**.



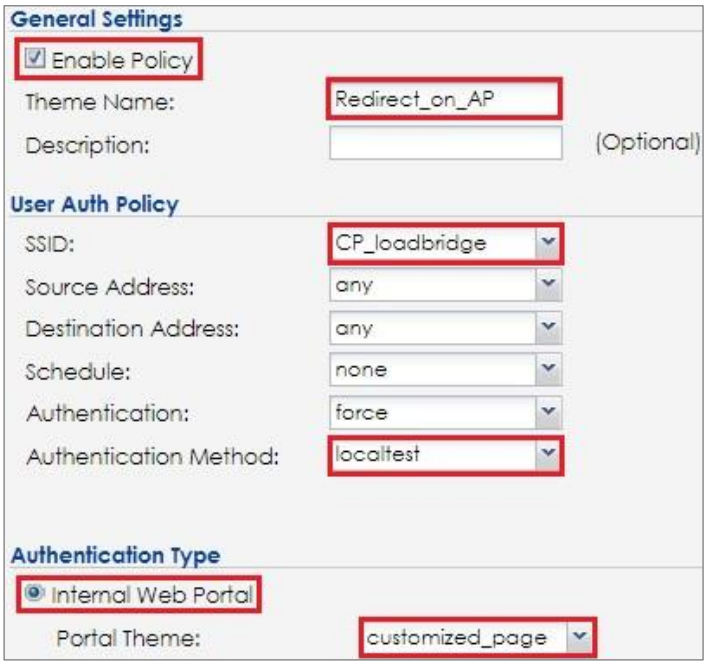
5.5.2 Configure Captive Portal

1 Go to **CONFIGURATION > Custom Captive Portal > customized page**.

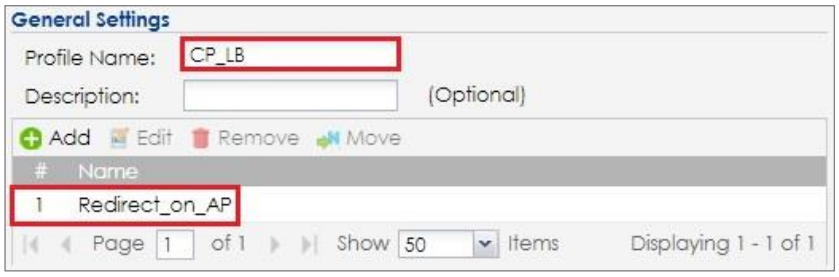




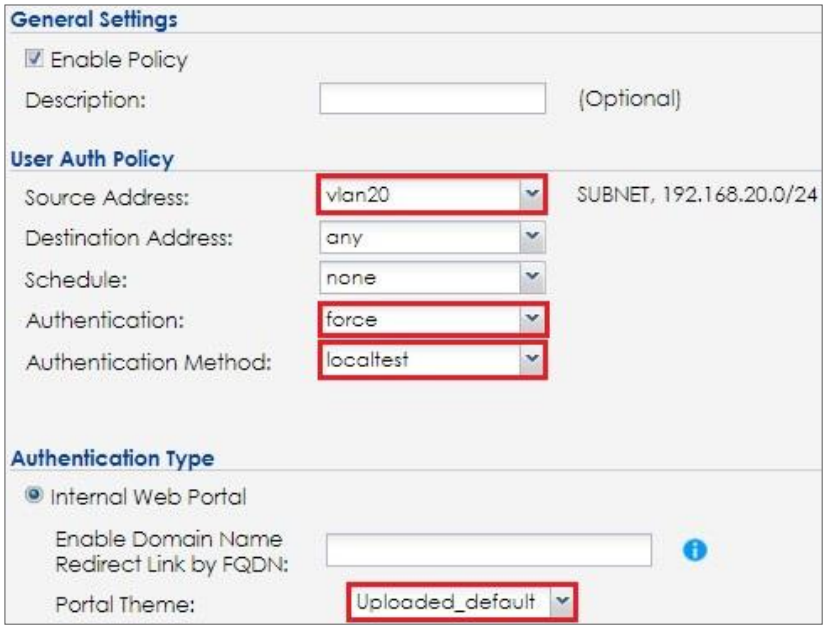
2 Go to **CONFIGURATION > Captive Portal > Redirect on AP > Authentication Policy Rule**, and click **add** to create a policy rule for stations which connect to SSID profile **CP_localbridge**.
In **General Settings**, check **Enable Policy** and enter the **Theme Name** of this policy.
In **User Auth Policy**, change **SSID** to **CP_localbridge** and **Authentication** is **Force**, and change the **Authentication Method** to **localtest**. Click **OK** to save.



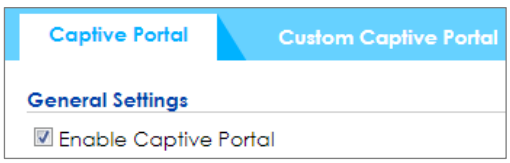
3 Go to **CONFIGURATION > Captive Portal > Redirect on AP > Authentication Policy Group**. In the setting, click **Add** to add the policy rule which is created in previous step.



4 Go to **CONFIGURATION > Captive Portal > Redirect on Controller > Authentication Policy Rule**, click **add** to create a policy rule for stations which get an SUBNET from 192.168.20.x.
In **General Settings**, check **Enable Policy** and enter the **Description** of this policy.
In **User Auth Policy**, change **Source Address** to **vlan20** and **Authentication** is **Force**. Check **Force User Authentication**, and change the **Authentication Method** to **localtest**. Click **OK** to save.

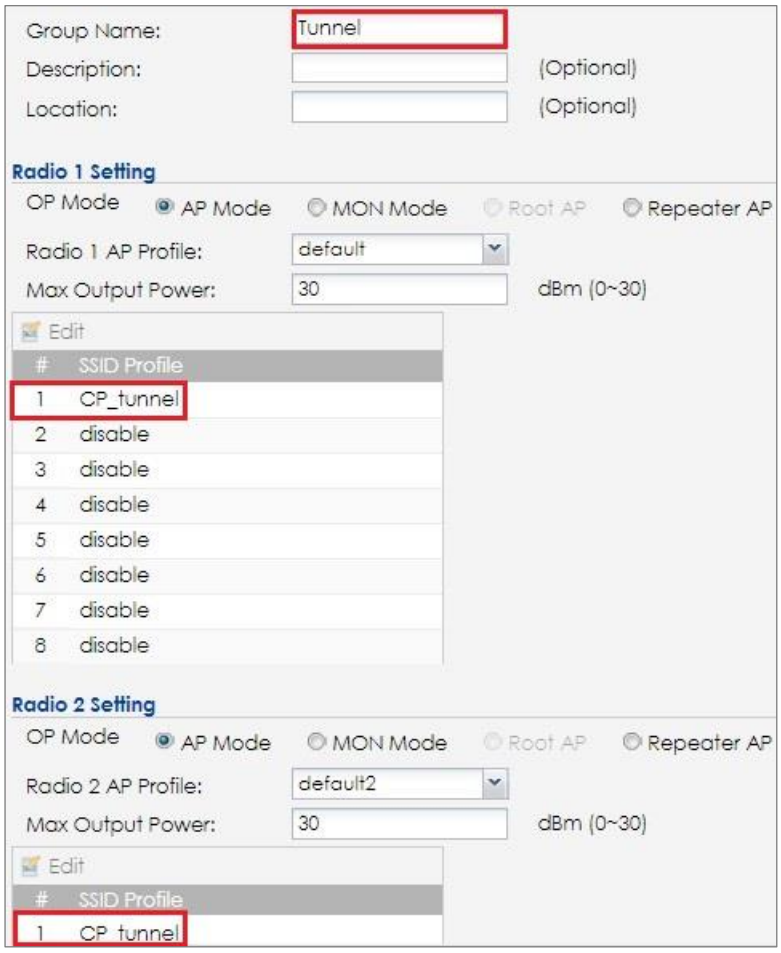


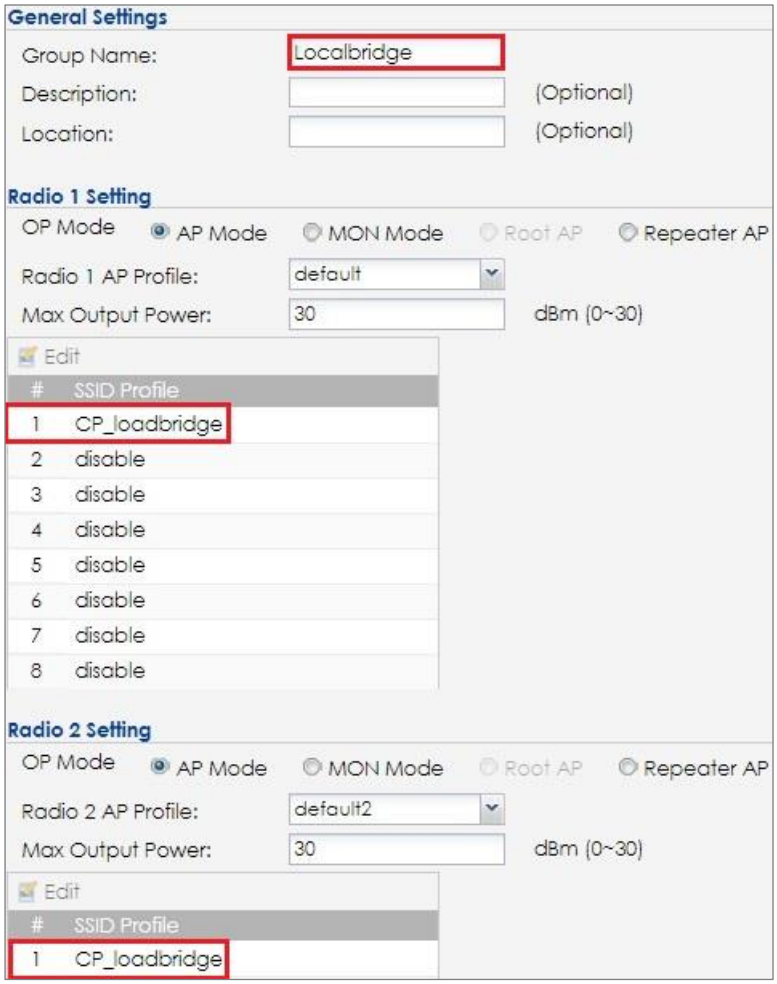
5 Go to **CONFIGURATION > Captive Portal > Captive Portal**, check **Enable Captive Portal**. Click **Apply** to apply the settings.



5.5.3 Broadcast SSID

1 Go to **CONFIGURATION > Wireless > AP Management > AP Group**, click Add two SSIDs: Localbridge and Tunnel.



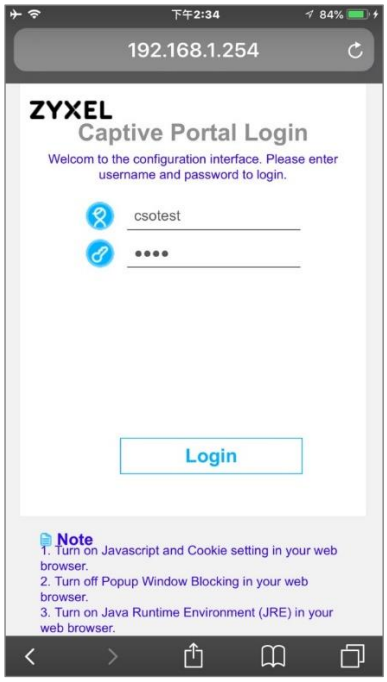


2 In the same setting page as previous step, select **CP_LB** for **Auth. Policy Group** in **Poral Redirect on AP**. Click **OK** to save.

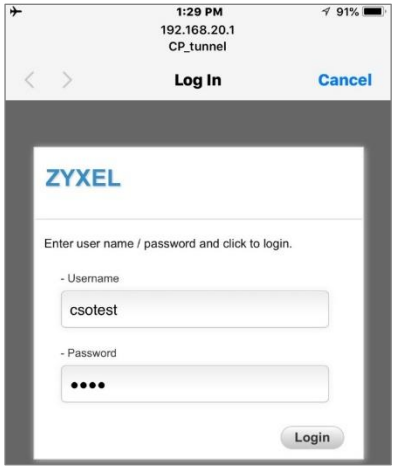
3 **Logout** from NXC controller.

5.5.4 Test the Result

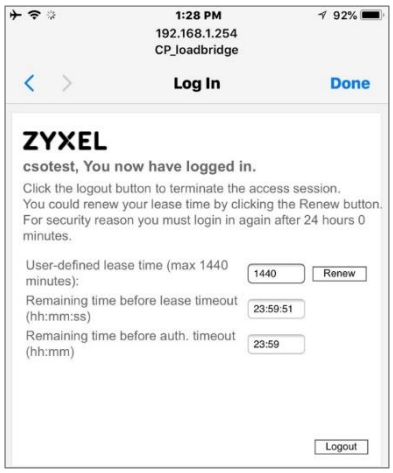
1 Connect the station to the SSID 'CP_localbridge'. The browser redirects the webpage to captive portal page and the user needs to enter the username and password for authentication before accessing the Internet.

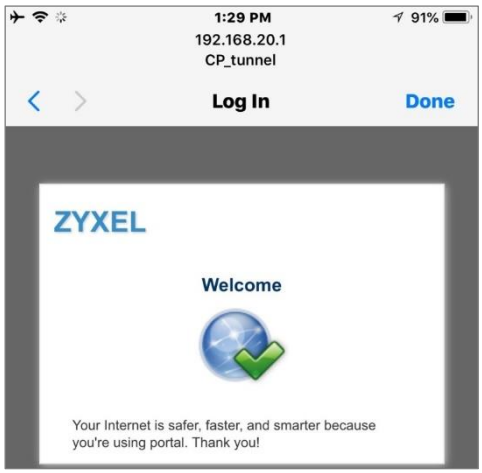


2 Connect the station to the SSID 'CP_tunnel'. The browser redirects the webpage to captive portal page and the user needs to enter the username and password for authentication before accessing the Internet.



3 After entering the username and password correctly, the connected station is able to access the Internet now. There is also a pop-window to show the detail information of the renew time and re-authentication time after authentication succeed or a successful welcome page.





5.5.5 What Could Go Wrong

1. The DNS **MUST** be set in the DHCP setting, or the captive portal might fail to redirect because NXC controller is not able to know the correct IP address of the website which stations access to.
2. The captive portal fails to redirect the webpage if the station logs in to the NXC controller before and does not logout.
3. When you use redirect on AP, the **Forwarding Mode** MUST be **Local bridge** mode.
4. If the user enters an incorrect username or password, there is a login failure webpage. Please use the correct username and password to log in again.

Secure the Wireless Environment – Others

6.1 How to Configure MAC Authentication?

The example instructs how to set up MAC authentication. Authenticate the wireless client by its MAC address instead of using username and password to authenticate the wireless.

In the classroom, the teachers' devices are trusted on the controller; they can pass MAC authentication directly and are regarded as MAC user roles on controller.

In this topology, we set the NXC as an authenticated server to save the devices' MAC addresses. The gateway USG is a DHCP server.

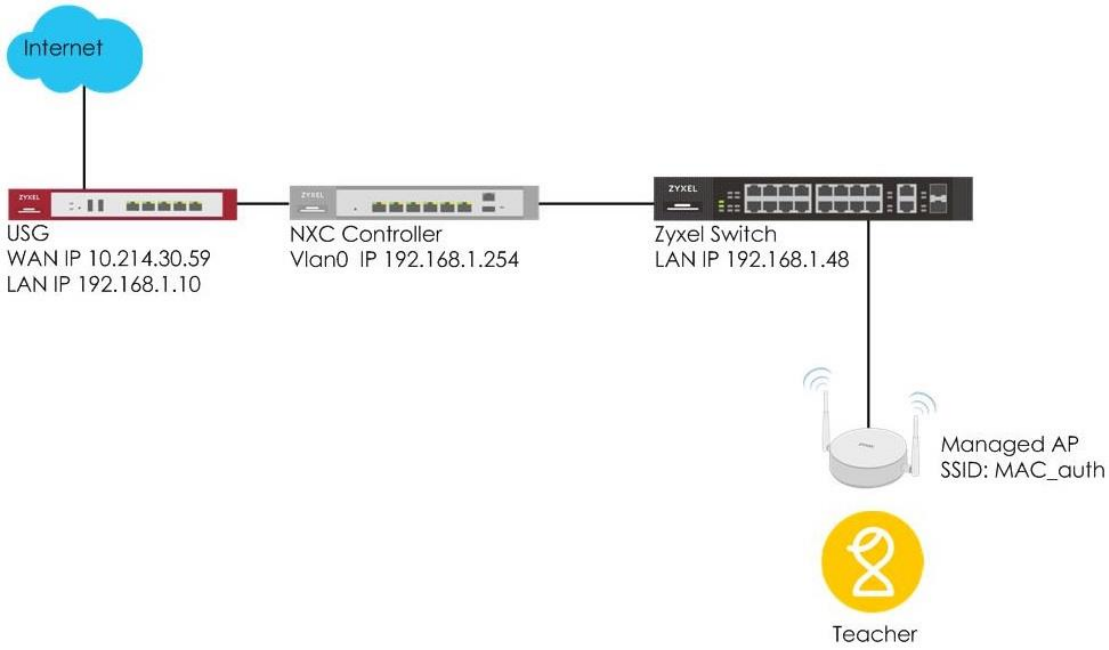
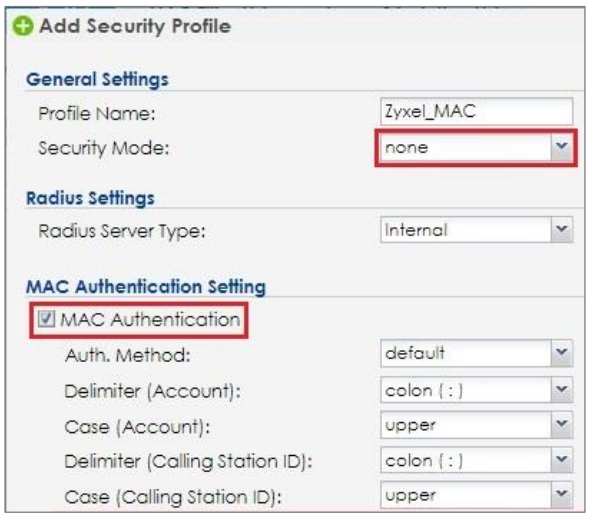


Figure 6.1 MAC Authentication

Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC2500 (Firmware Version: 5.30), GS2210-8HP (Firmware Version: V4.30).

6.1.1 Configure AP Profile

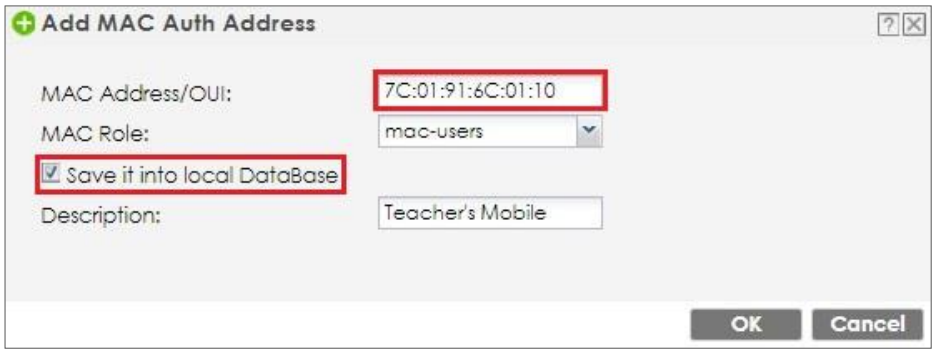
1 Go to **CONFIGURATION > Object > AP Profile > SSID > Security > Add**. Create a new security profile which sets none security and enables **MAC Authentication**.

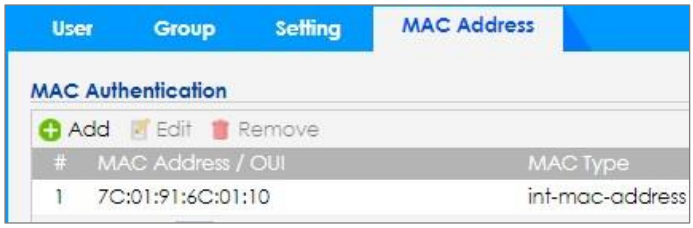


2 Go to **CONFIGURATION > Object > AP Profile > SSID > SSID List**, Create the SSID profile with the security profile.

6.1.2 Configure User/Group Profile

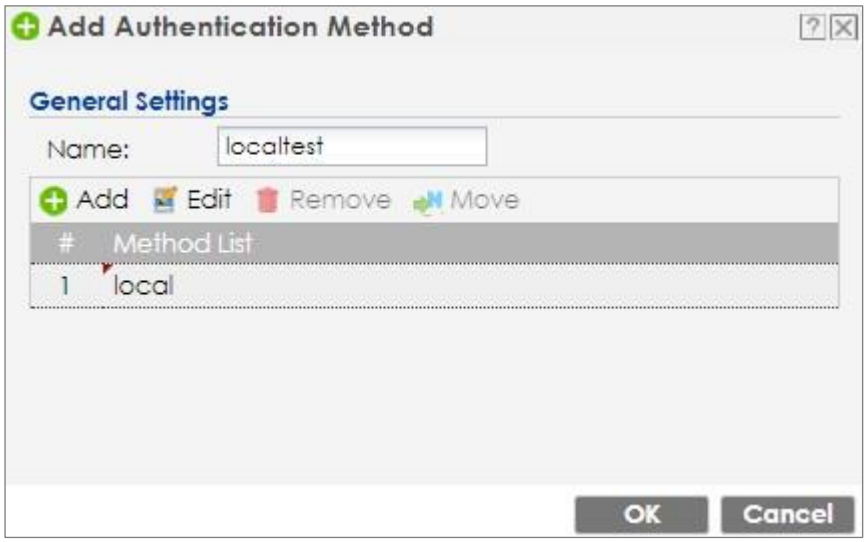
1 Go to **CONFIGURATION > Object > User/Group > MAC Address > MAC Authentication**. Add the teacher's MAC address for MAC authentication in the NXC local server.

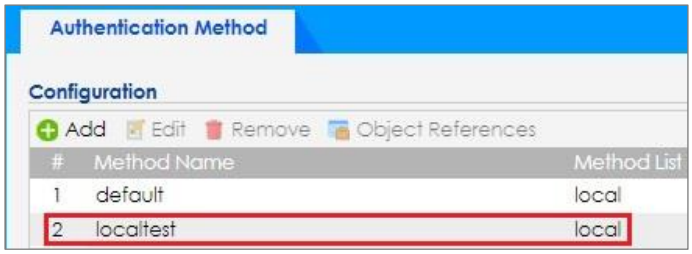




6.1.3 Configure Authentication Method Setting

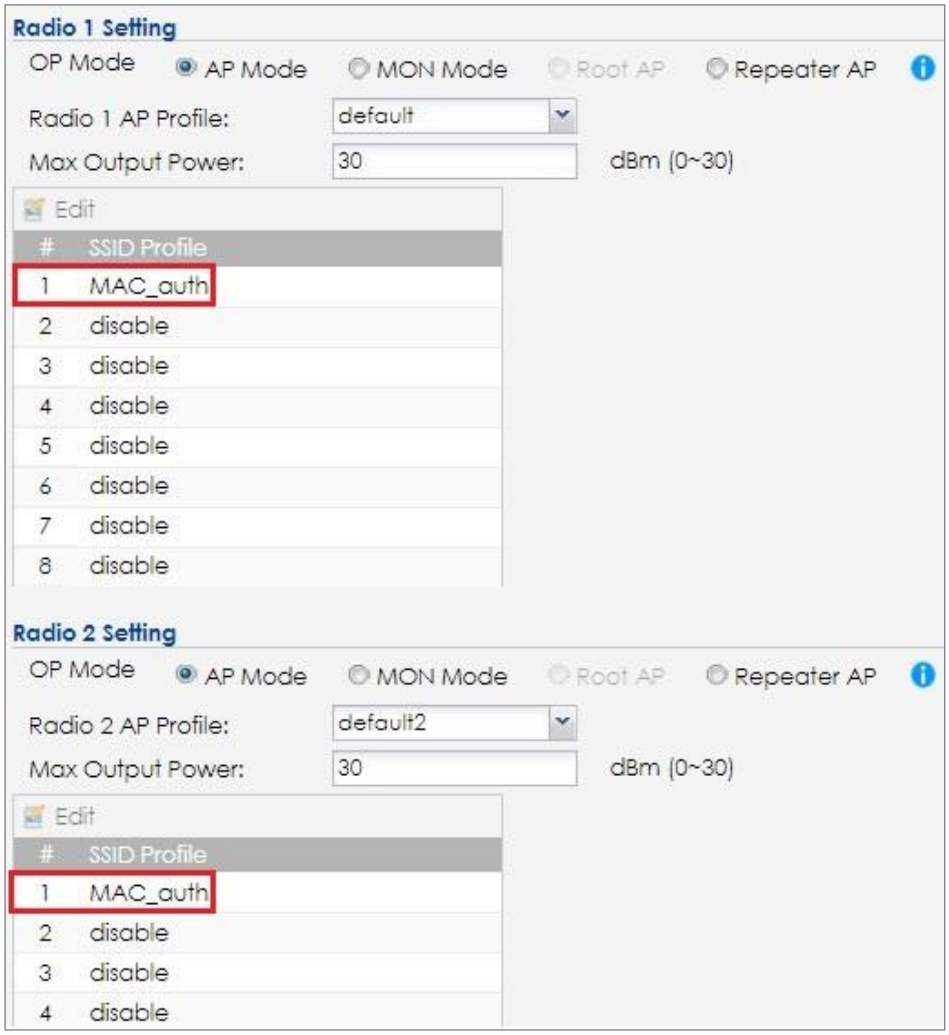
1 Go to **CONFIGURATION > Object > Auth. Method**, click **Add** to create an authentication method. Enter the **Name** of this authentication method and select to local in the **Method List**.





6.1.4 Configure AP Group Profile

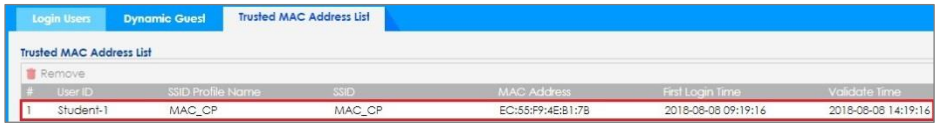
1 Go to **CONFIGURATION > Wireless > AP Management > AP Group > Group Summary > Radio setting**. Set the SSID profile to the AP radio.



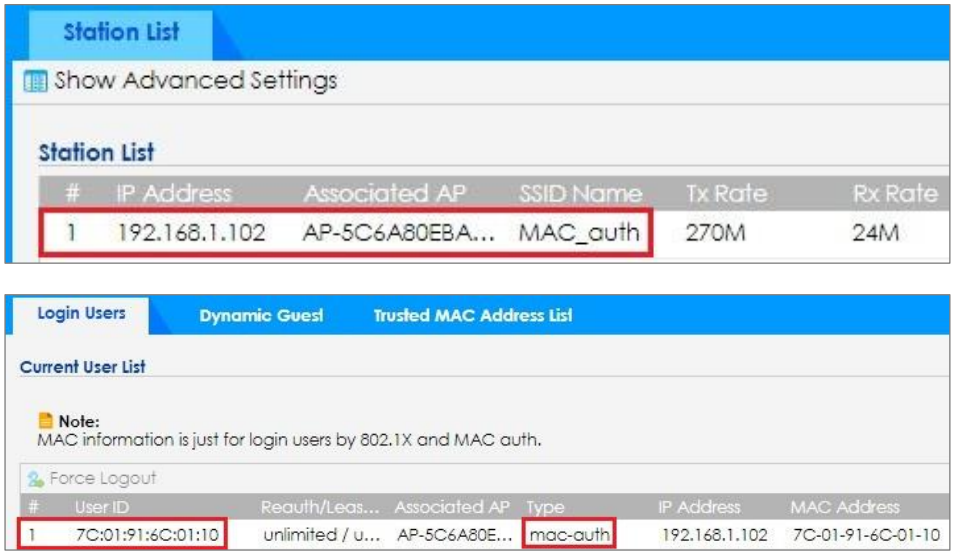
6.1.5 Test the Result

1 Use the teacher's trusted device and connect to the SSID: **MAC_auth**. The device successfully passes the MAC authentication and is allowed to access the Internet directly.

2 Go to **MONITOR > Wireless > Station Info**. Check the station information on the NXC.



3 Go to **MONITOR > System Status > Login Users > Login Users**. Check the logged in users on the NXC and find the teacher's device information.



6.2 MAC Authentication fallback to Captive Portal?

The example instructs how to set up MAC authentication fallback to captive portal. User can decide NXC whether cache the trusted client's mac address or not. If user decides NXC not to cache the trusted client's MAC address, it will work as captive portal. If user enters the trusted client's mac address on the authenticated server before, it will work as MAC authentication.

In the classroom, the teachers and students all use Wi-Fi service but have different privileges and restrictions. The teachers' devices are trusted on the controller; they can pass MAC authentication directly and are regarded as MAC user roles on controller. The students' devices need to pass captive portal authentication with their own IDs/passwords. They are regarded as portal user roles on controller.

In this topology, we set the NXC as an authenticated server to save the devices' MAC addresses and clients' names and passwords. The gateway USG is a DHCP server.

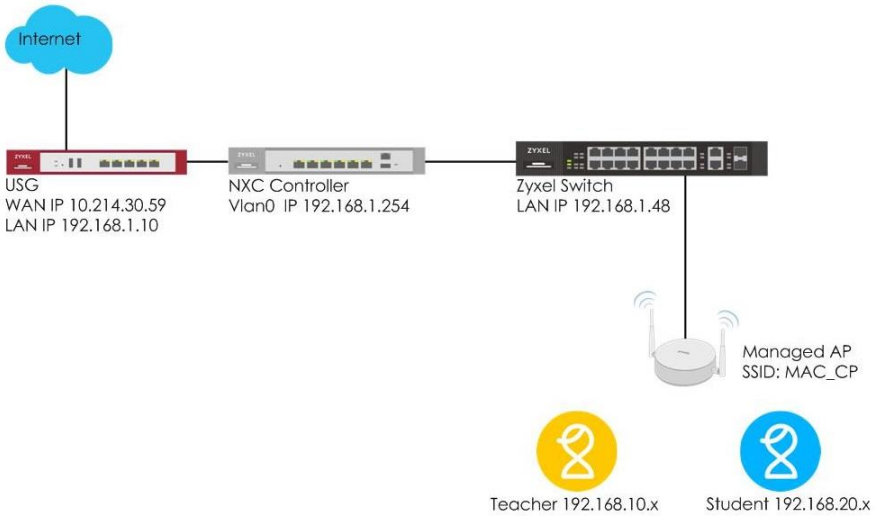
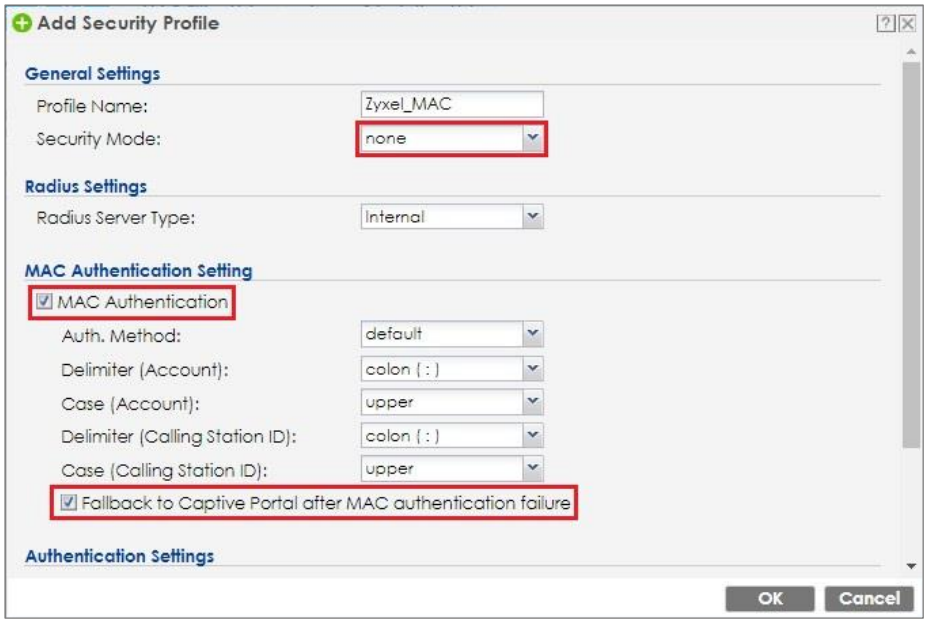


Figure 6.2 MAC Authentication fallback to captive portal

Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC2500 (Firmware Version: 5.30), GS2210-8HP (Firmware Version: V4.30).

6.2.1 Configure AP Profile

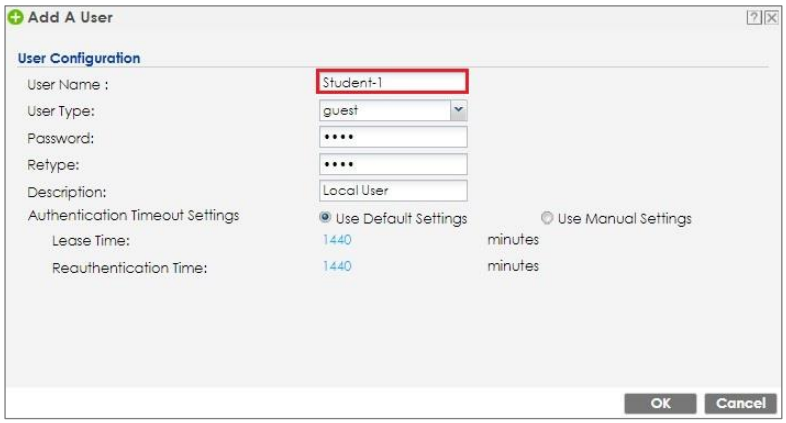
1 Go to **CONFIGURATION > Object > AP Profile > SSID > Security > Add**. Create a new security profile which sets none security and enables **MAC Authentication** and **Fallback to captive Portal after MAC authentication failure**.



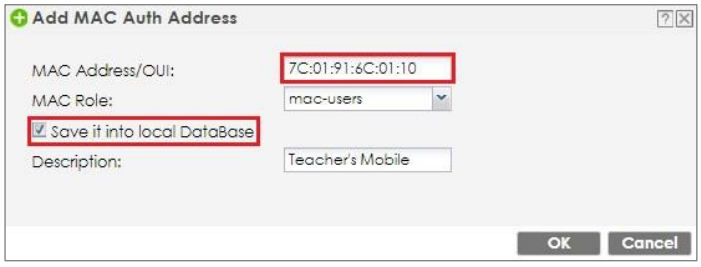
2 Go to **CONFIGURATION > Object > AP Profile > SSID > SSID List**, Create the SSID profile with the security profile.

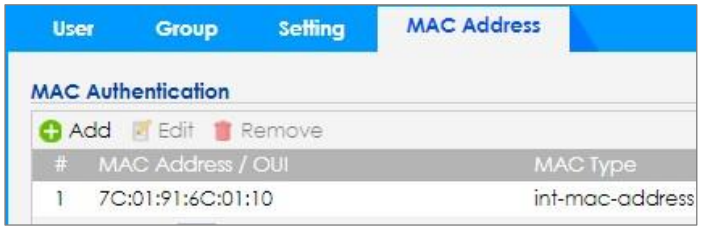
6.2.2 Configure User/Group Profile

1 Go to **CONFIGURATION > Object > User/Group > User > Add**. Click **Add** to create a new user ID and password. Stations can log in captive portal to access the Internet via this account. Add the student's name and password for captive portal authentication in the NXC local server. **User Type** is **guest**. Enter the **Password** as the login password. The default of **Authentication Timeout Setting** is 1440 minutes, and usually it's shorter for guests. Select to **Use Manual Settings** to set **Lease Time** and **Reauthentication Time**. Click **OK** to save.



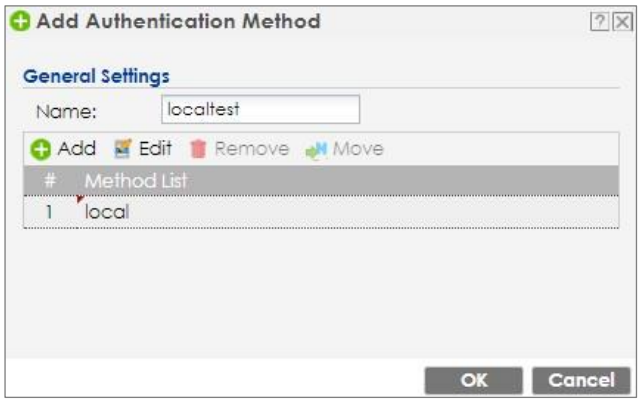
2 Go to **CONFIGURATION > Object > User/Group > MAC Address > MAC Authentication**. Add the teacher's MAC address for MAC authentication in the NXC local server.

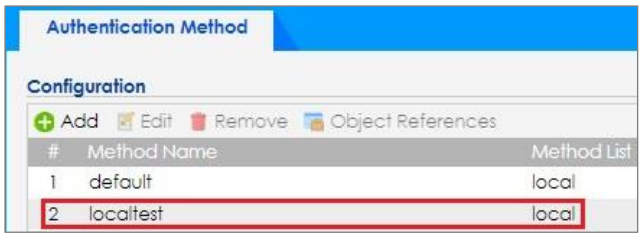




6.2.3 Configure Authentication Method Setting

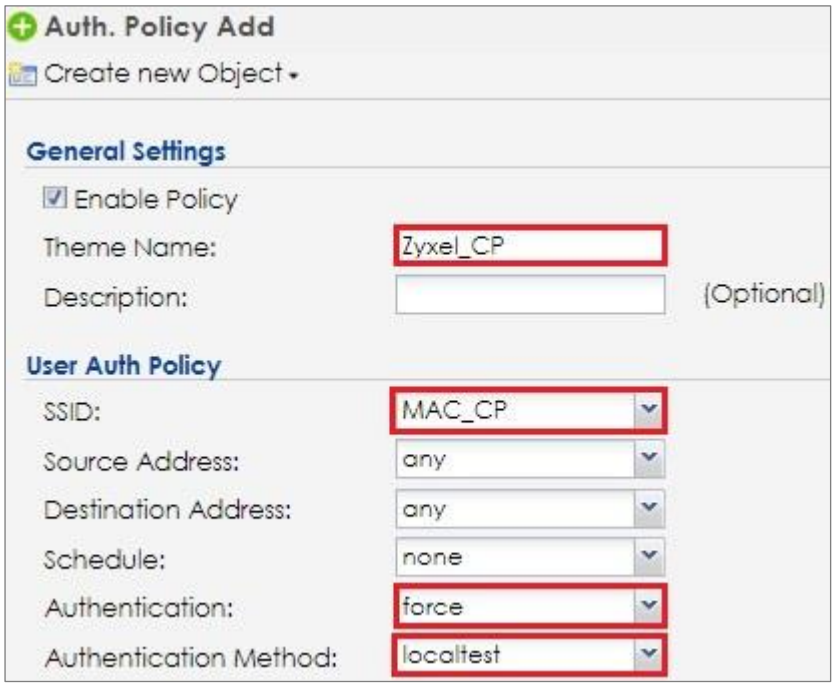
1 Go to **CONFIGURATION > Object > Auth. Method**, click **Add** to create an authentication method. Enter the **Name** of this authentication method and select to local in the **Method List**.



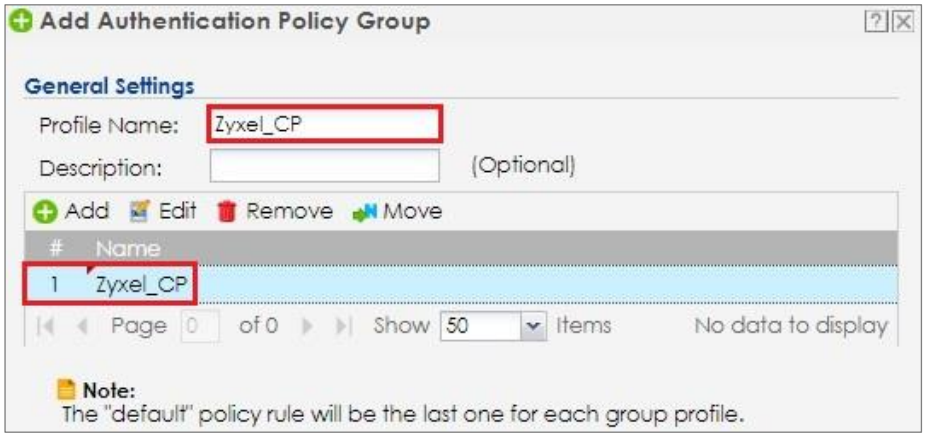


6.2.4 Configure Captive Portal Setting

1 Go to **CONFIGURATION > Network > Captive Portal > Redirect on AP > Authentication Policy Rule > Add**. Set the SSID for user authentication policy to redirect captive portal on the AP.



2 Go to **CONFIGURATION > Network > Captive Portal > Redirect on AP > Authentication Policy Group > Add**. Set the authentication policy rule in the policy group.

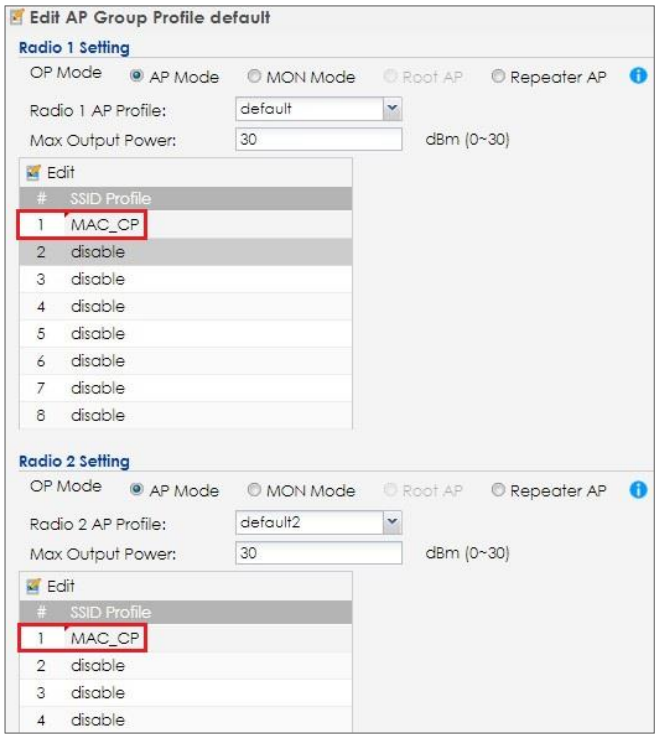


3 Go to **CONFIGURATION > Network > Captive Portal > Captive Portal > General Settings**. Enable the captive portal function.

4 Go to **CONFIGURATION > Network > Captive Portal > Captive Portal > SSID Profile with MAC Cache > Add**. Set the SSID profile with the MAC cache. The MAC address cache time can be set from 1-168 hours.

6.2.5 Configure AP Group Profile

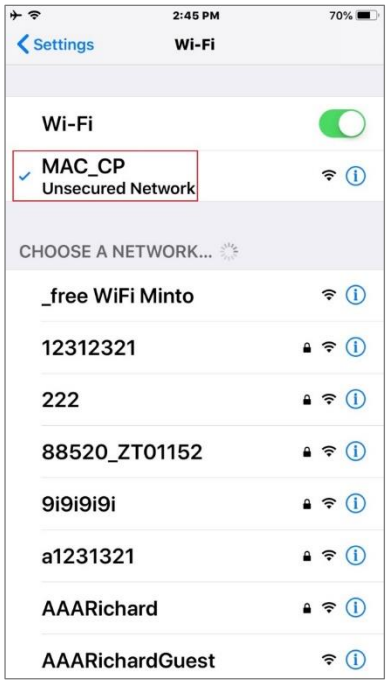
1 Go to **CONFIGURATION > Wireless > AP Management > AP Group > Group Summary > Radio setting**. Set the SSID profile to the AP radio.

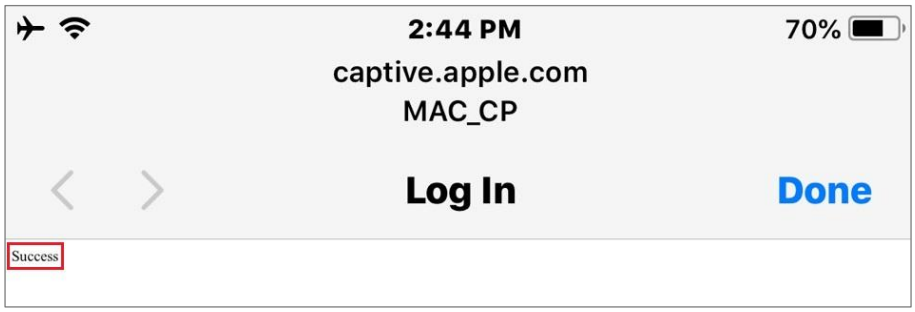


2 Go to **CONFIGURATION > Wireless > AP Management > AP Group > Group Summary > Portal redirect on AP**. Set the authentication policy group.

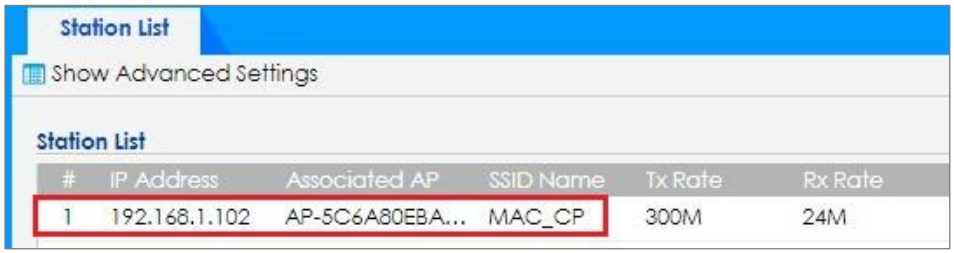
6.2.6 Test the Result

1 Use the teacher's trusted device and connect to the SSID: **MAC_CP**. The captive portal doesn't pop up because the devices' MAC address is trusted by the NXC's local server. The device successfully passes the MAC authentication and is allowed to access the Internet directly.

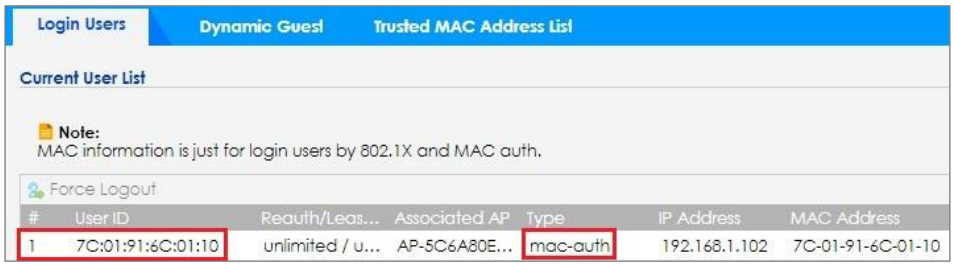




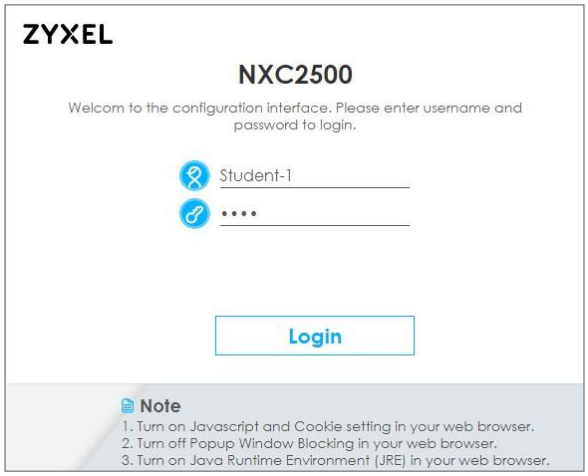
2 Go to **MONITOR > Wireless > Station Info**. Check the station information on the NXC.

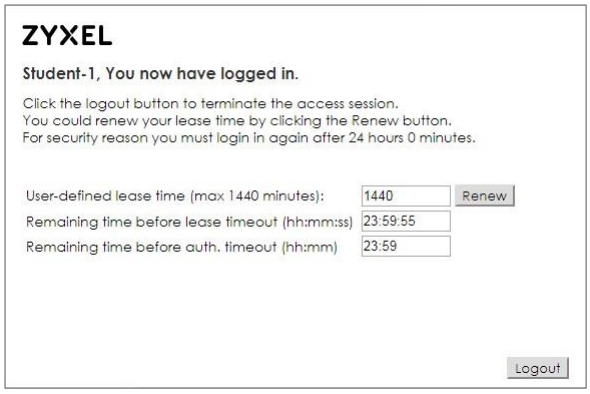


3 Go to **MONITOR > System Status > Login Users > Login Users**. Check the logged in users on the NXC and find the teacher's device information.

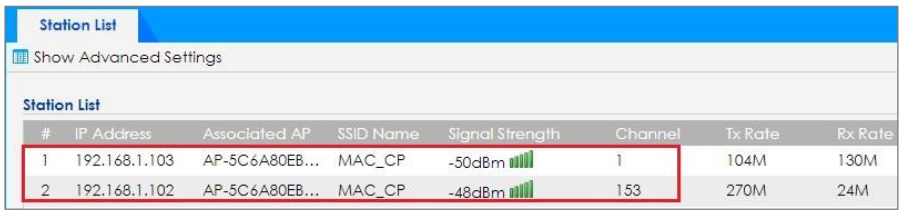


4 Use the student's mobile device or PC to connect to the SSID: **MAC_CP**. Open the browser and it will redirect to the captive portal screen. Enter the student's username and password to pass the captive portal.

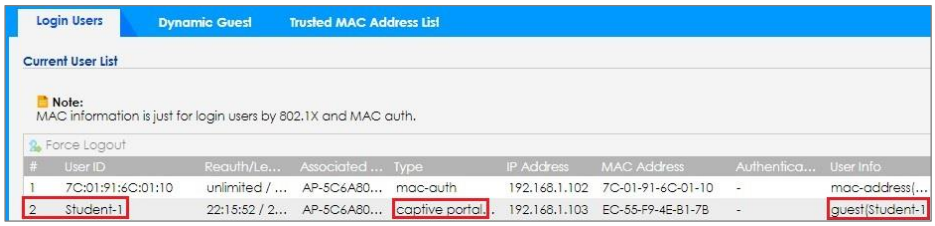




5 Go to **MONITOR > Wireless > Station Info**. Check the station information on the NXC.



6 Go to **MONITOR > System Status > Login Users > Login Users**. Check the logged in users on the NXC and find the student's device information.



7 The student's device was cached in the NXC's trusted MAC address list with a 5 hour limitation

6.2.7 What Could Go Wrong

1. If captive portal page is not redirected for student role, please check whether the MAC address cache time is still cached during that time.
2. If captive portal is not enabled but the fallback option is selected, the users can always connect to the Wi-Fi regardless of whether the MAC authentication is successful or not.
3. This Feature does not support with legacy NWA3KN and NWA5KN series products.

6.3 How to Defect the Rogue AP?

A rogue AP works without being controlled by the administrator of the Network. It may cause the security issue for the network and we can use the AP in monitor mode to contain the rogue AP.

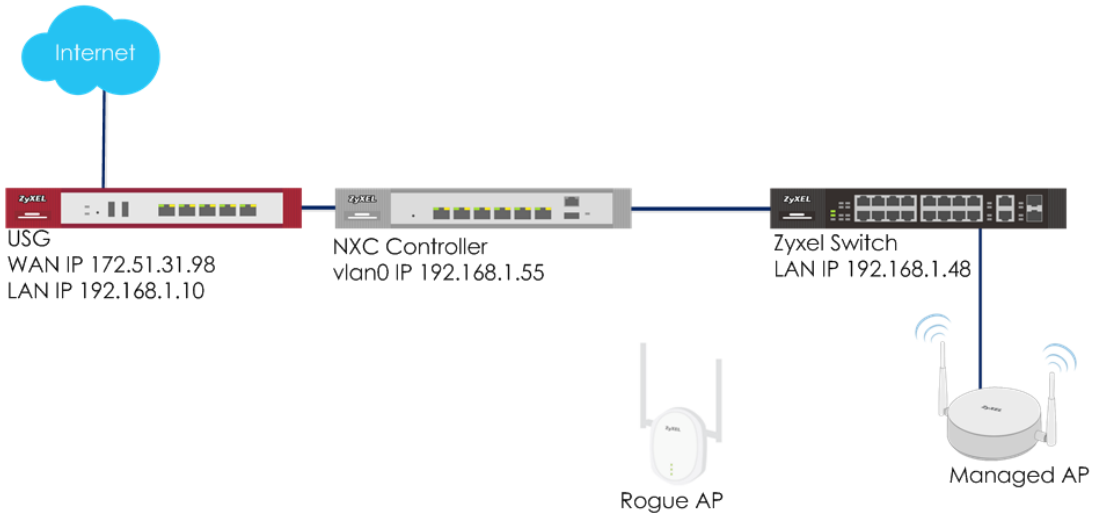
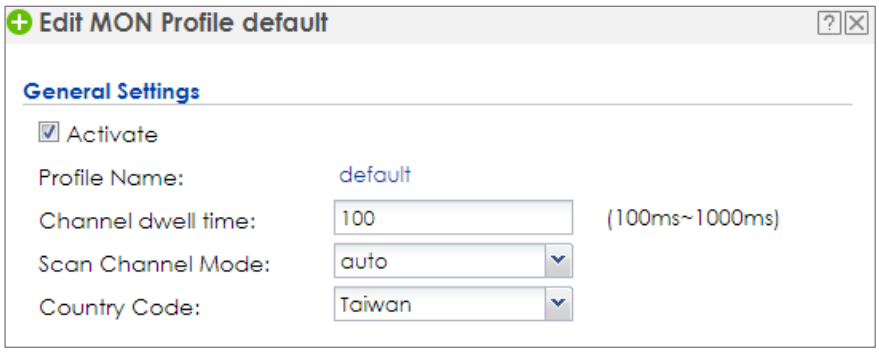


Figure 6.3 Monitor Rogue AP and Containment

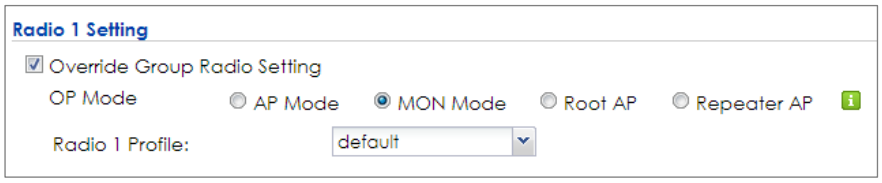
Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC2500 (Firmware Version: 5.30), GS2210-8HP (Firmware Version: V4.30).

6.3.1 Configure AP to Monitor Mode

1 Configure a monitor profile in **CONFIGURATION > Object > MON Profile**. Select the **default** profile and click **Edit** to change. Check the **Scan Channel Mode** is **auto** and **Country Code** is correct and is the location where you use the AP. Click **OK** to save.

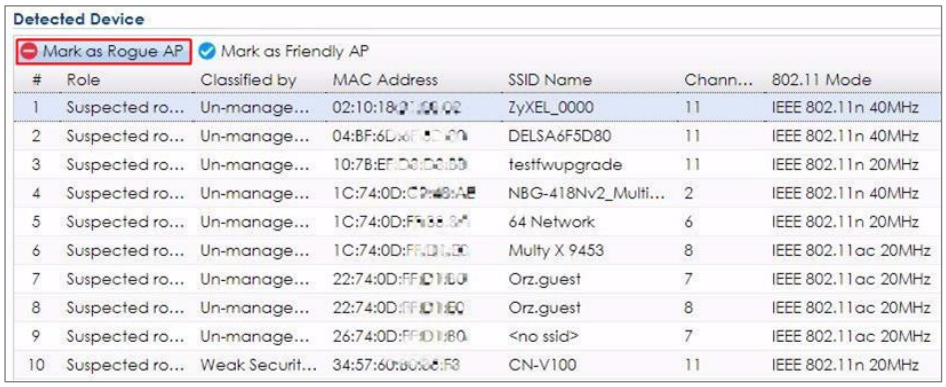


2 Configure AP to monitor mode in **CONFIGURATION > Wireless > AP Management**. Select the AP which is going to work in monitor mode and click **Edit** to change. Check **Override Group Radio Setting** and select **MON Mode** with **default radio 1 profile** which is set in step 1. Click **OK** to save.



6.3.2 Detected Devices and Containment

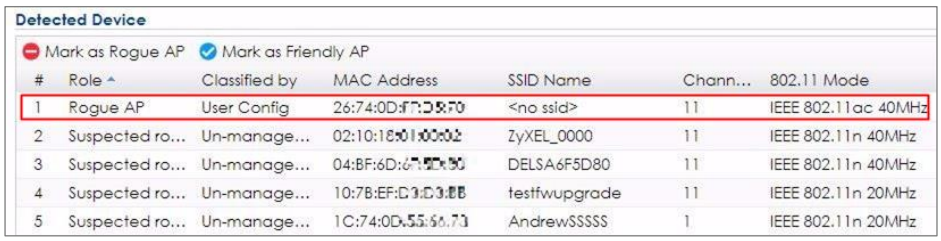
1 In **MONITOR > Wireless > Detected Device**, Click **Refresh** if there's no rogue AP in the list. Select the rogue AP and click **Mark as Rogue AP**.



2 When the AP is marked as a rogue AP, it can be set in the containment list in **CONFIGURATION > Wireless > Rogue AP > Rogue/Friendly AP List** and the stations are difficult to connect with the containment AP.

6.3.3 Test the Result

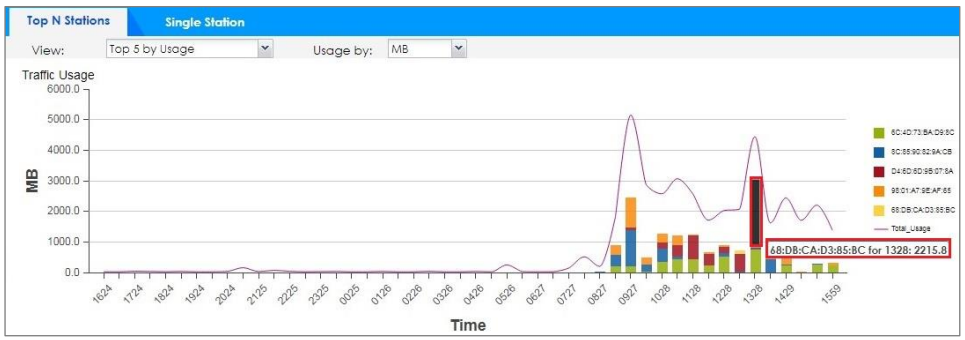
1 When the AP is marked as a rogue AP, it is shown in **MONITOR > Wireless > Detected Device**.



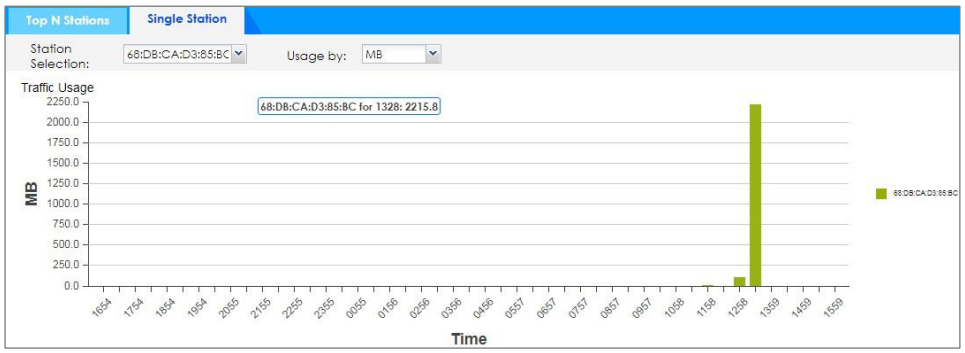
2 When the AP is set in the containment list, the stations are disconnected right away after they connect to the rogue AP.

6.4 How to monitor the traffic and stations on web GUI?

1 In **Dashboard > Station > Traffic**, Click the **Top N Stations** tab to view usage information for multiple stations at a time.



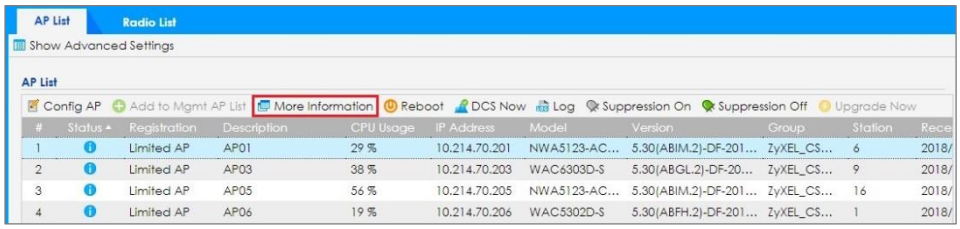
2 Or click the **Single Station** tab to view a specific wireless station's usage details.



The y-axis shows the amount of data (in MB or GB) consumed by the selected station(s).
The x-axis shows the time period over which the traffic flow occurred.

Move the cursor over a bar to see usage details over a specific time period.
The chart will record 24 hours of traffic usage.
For example, we can observe message of the station MAC: 68:DB:CA:D3:85:BC for 1328:2215.8 which means this MAC's traffic is 2215.8MB at 13:28.

3 As well as we can check the broadcast number on the AP. In **MONITOR > Wireless > AP Information > AP List**, click **More Information** on the AP.

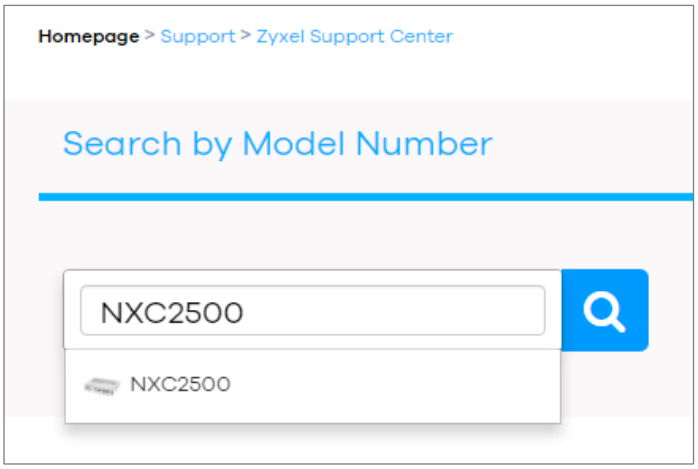


It displays the number of broadcast packets transmitted / received on the port.

Maintain NXC Controller

7.1 How to Do Firmware upgrade

1. There are two ways to do firmware upgrade, GUI and FTP. The firmware can be downloaded from Zyxel support center. Please find below the website address of the support center. http://www.zyxel.com/support/support_landing.shtml
2. Use "Search by Model Number" in the webpage.



3. Click the download icon in NXC2500 latest release as shown below.

7.1.1 Firmware from GUI?

The example instructs how to do FW upgrade from GUI. The Firmware version will be changed from v5.00 to v5.10.

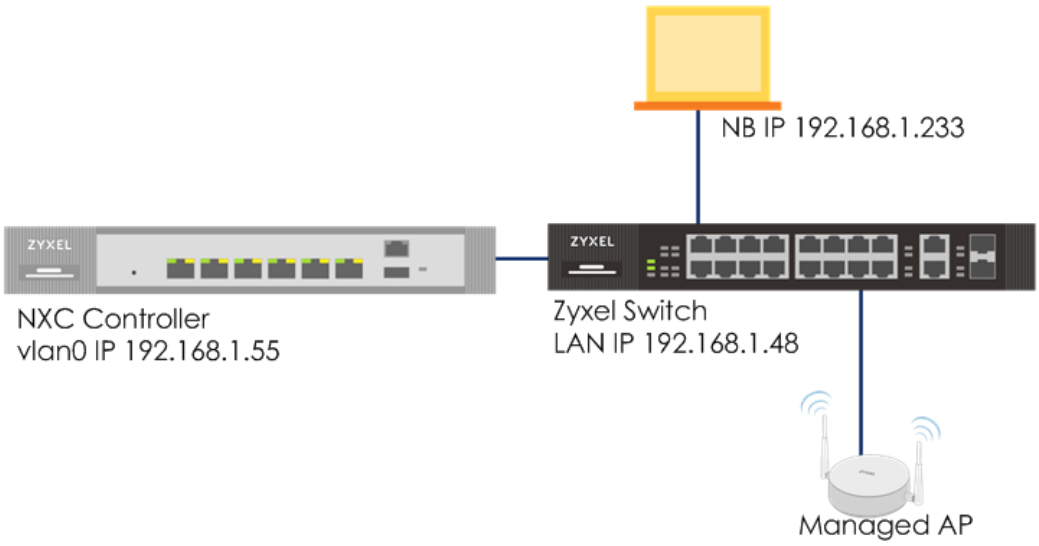


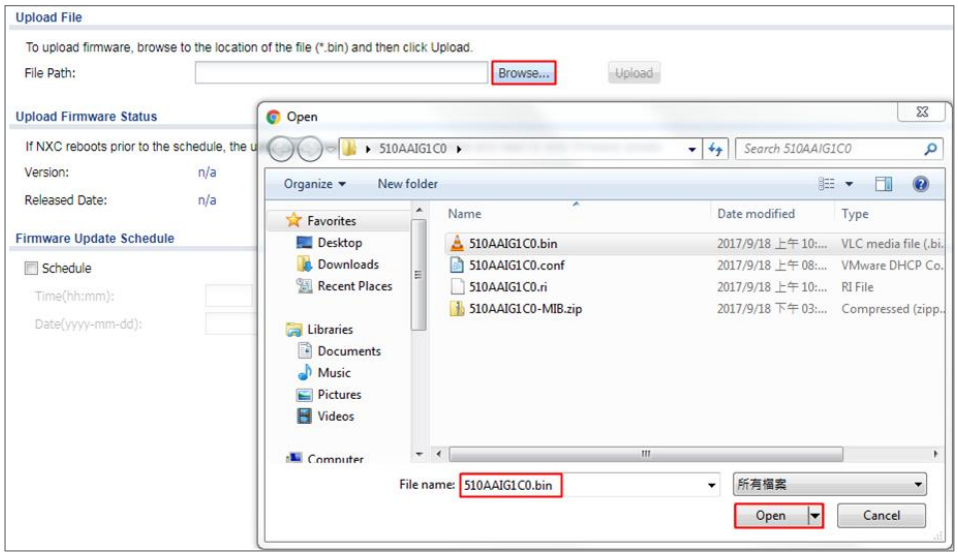
Figure 7.1.1 Firmware Upgrade from GUI

Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC2500 (Firmware Version: 5.00), GS2210-8HP (Firmware Version: V4.30).

7.1.1.1 Firmware Upgrade on GUI

1 In **MAINTENANCE > File Manager > Firmware Package**, check if the NXC's current firmware version is the same as the one you are going to install.

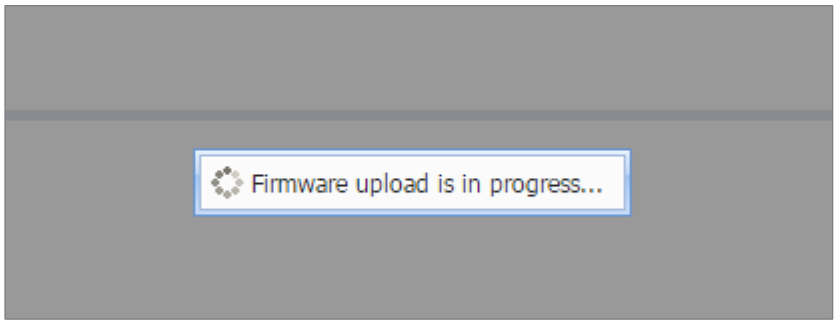
2 In **MAINTENANCE > File Manager > Firmware Package**, click **Browse…**in Upload File and select the firmware you want to install.



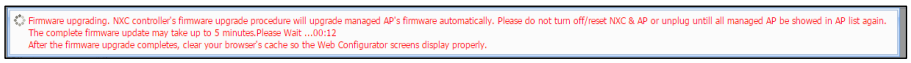
3 In **MAINTENANCE > File Manager > Firmware Package**, click Upload…to start to upload the firmware.

7.1.1.2 Test the Result

1 After starting firmware upgrade, there's a notification about firmware upload.



2 After finishing firmware upload, the system will start to firmware upgrade.



3 After the firmware upgrade is complete and successful, you can check it on GUI Dashboard.

7.1.1.3 What Could Go Wrong

1. When the firmware is uploading and the traffic for transferring the firmware is disconnected, the firmware upgrade will not be successful.
2. When the firmware is upgrading, please do not reset or reboot the controller. Otherwise, it might cause system crashes or firmware upgrade failure.

7.1.2 Firmware from FTP?

The example instructs how to do FW upgrade from FTP. This is usually used when you failed to access the web GUI.

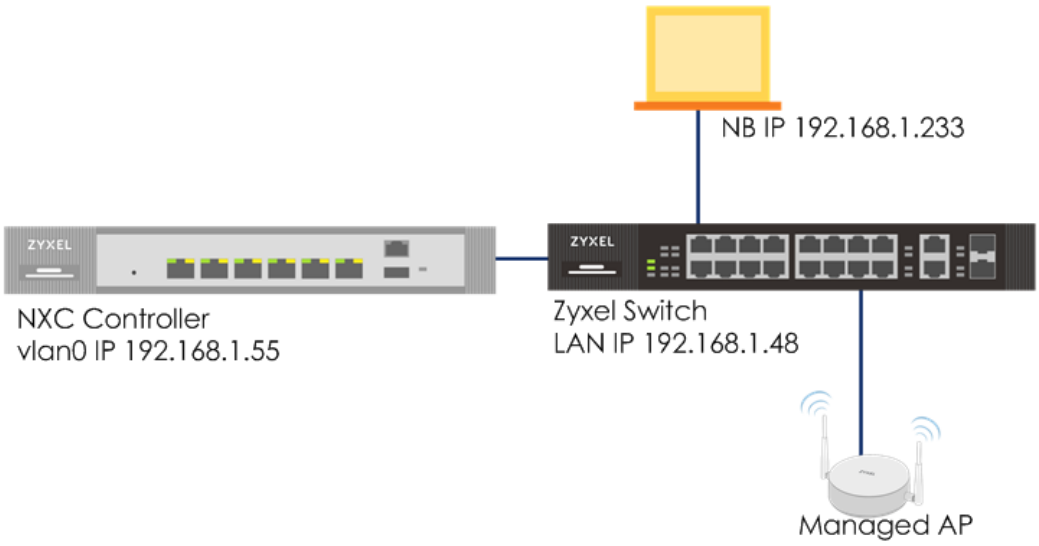
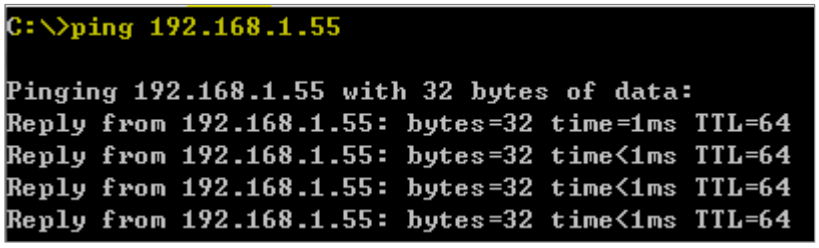


Figure 7.1.2 Firmware Upgrade from GUI

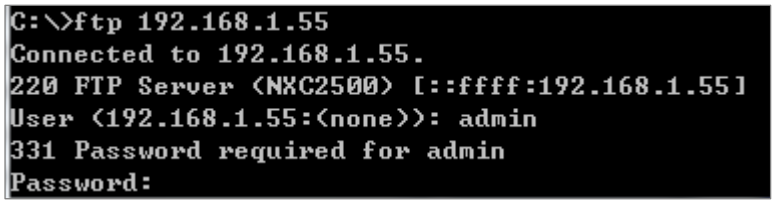
Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC2500 (Firmware Version: 5.30), GS2210-8HP (Firmware Version: V4.30).

7.1.2.1 Firmware Upgrade on GUI

1. Copy the firmware to the root directory of the C drive on your computer c:\ and do not change the file name of the firmware.
2. Use the following command to ping the controller for checking the connection.
   ping 192.168.1.55



3. In the Windows command prompt, type ftp 192.168.1.55 to log in to the controller via username **admin** and password **1234** (by default).



4. Enter bin for transfer mode to binary.

5 Enter **put c:\ 510AAIG1C0\510AAIG1C0.bin** and wait for the file transfer to complete. After the transmission is finished, the controller will start to upgrade.

```
ftp> put C:\510AAIG1C0\510AAIG1C0.bin
200 PORT command successful
150 Opening BINARY mode data connection for 510AAIG1C0.bin
226-firmware verifying...
226-firmware updating...
226-Please Wait about 5 minutes!!
226-Do not poweroff or reset,
226-system will reboot automatically after finished updating.
226 Transfer complete.
ftp: 254883548 bytes sent in 12.68Seconds 20102.81Kbytes/sec.
```

7.1.2.2 Test the Result

1. After starting firmware upgrade, the LED flashes and it takes about 5 minutes to finish.
2. After the firmware is upgraded successfully, you can check it on GUI Dashboard.

7.1.2.3 What Could Go Wrong

1. When the firmware is uploading and the traffic for transferring the firmware is disconnected, the firmware upgrade will not be successful.
2. When the firmware is upgrading, please do not reset or reboot the controller. Otherwise, it might cause system crashes or firmware upgrade failure.

7.2 How to Reset the Controller/AP?

The example instructs how to reset the controller/AP. This is usually used when there's a new deployment or misconfiguration.

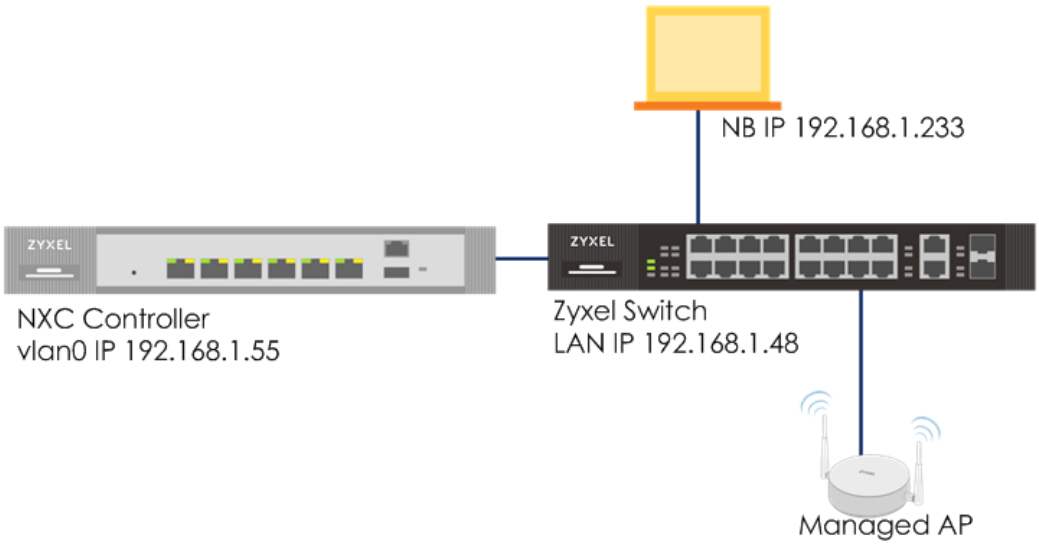
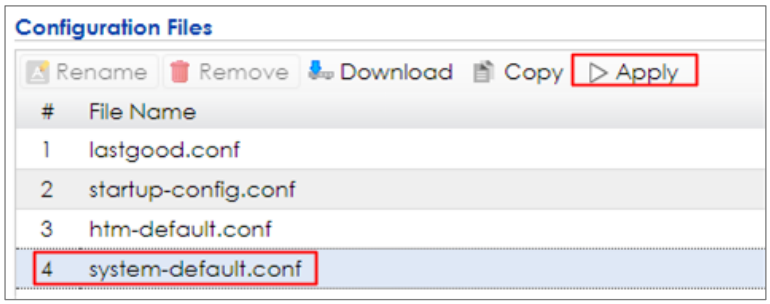


Figure 7.2 Firmware Upgrade from GUI

Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC2500 (Firmware Version: 5.30), GS2210-8HP (Firmware Version: V4.30).

7.2.1 Reset to Default from GUI

1 Log in to controller and go to **MANTENANCE > File Manager > Configuration File**. Click "**system-default conf**" in the list and **Apply**.



7.2.2 Reset to Default from Hardware

1 Push the RESET button over 15 seconds for resetting to defaults.

7.2.3 Test the Result

1. After resetting to default settings, the controller's IP is 192.168.1.1 and AP's IP is 192.168.1.2.
2. All the settings are changed back to default settings.

7.3 How to upgrade the firmware for AP via NXC?

The example instructs how to upgrade the firmware for partial APs. We can decide if the AP will be upgraded firmware automatically by NXC or upgraded firmware manually by ourselves. And choose the updating method as CAPWAP or FTP. In this chapter, there is also an example instructs how to upgrade firmware for partial AP. Not upgrade AP firmware at the same time.

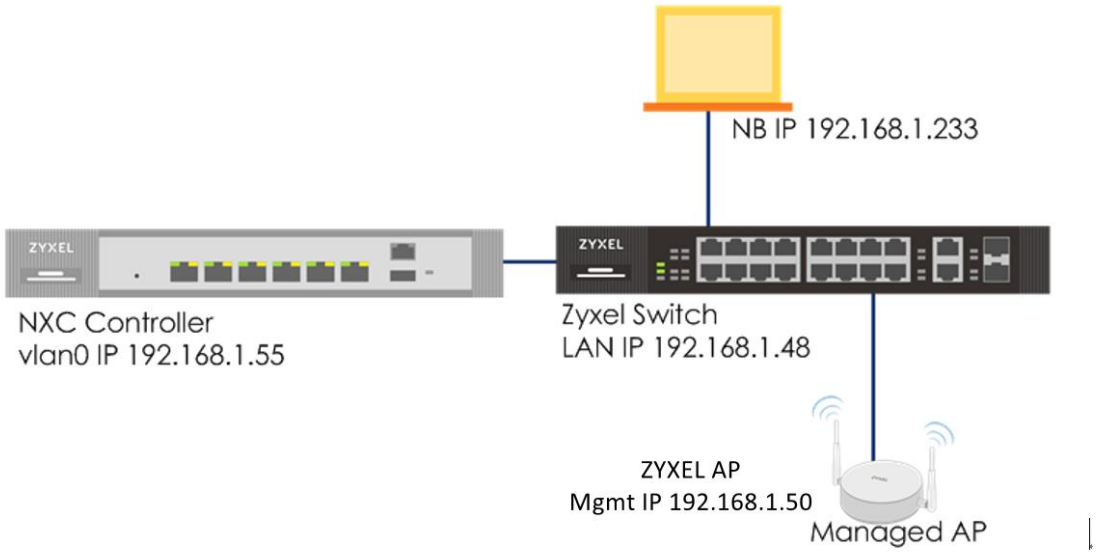


Figure 7.3 Upgrade AP firmware via GUI

Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using NXC2500 (Firmware Version: 5.30) and GS2210-8HP (Firmware Version: V4.30).

7.3.1 How to Change the Updating Method for the AP as Manual?

The example instructs how to change the updating mode for AP as Manual. The AP will not upgrade the firmware unless we click the "Upgrade Now". It can help to manage the upgrade time. We can choose when to upgrade the firmware to the AP.

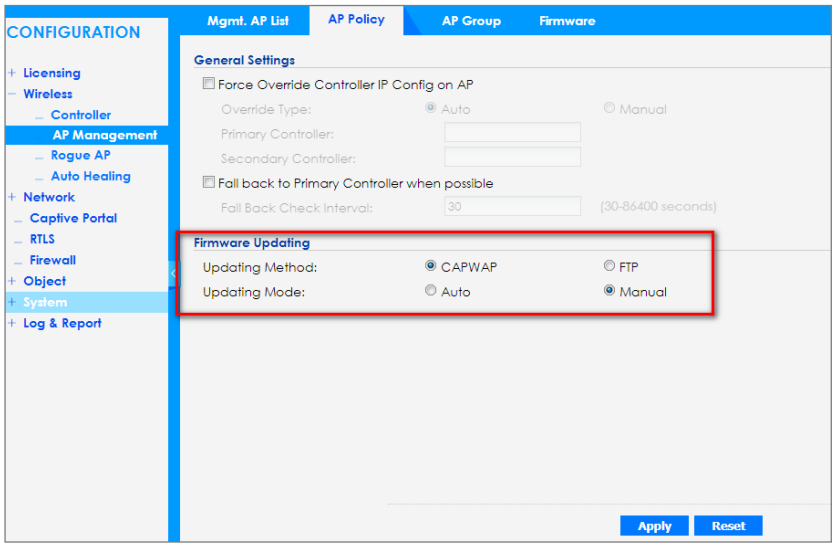
7.3.1.1 Change the Updating Method via GUI

1 Log in to controller and go to **CONFIGURATION > Wireless > AP Management > AP Policy > Firmware Updating.**

Updating Method: **CAPWAP**

Updating Mode: **Manual**

Click **Apply.**

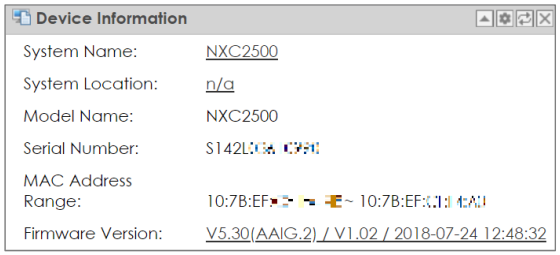


7.3.1.2 Test the Result

Connect the AP with firmware version 5.20 p3, and the AP will not be upgraded to 5.30 P2.

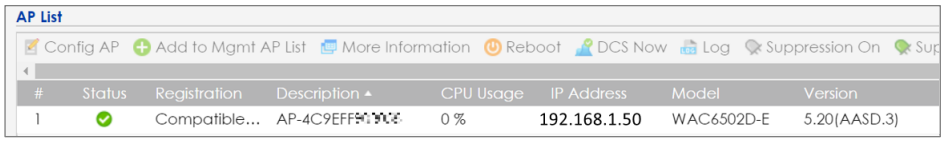
1 NXC: Go to **DASHBOARD > Device Information.**

Firmware version: V5.30(AAIG.2)



2 AP: Go to MONITOR > Wireless > AP Information > AP List.

Firmware version: V5.20(AAXH.3)



7.3.2 How to upgrade the specific AP firmware manually?

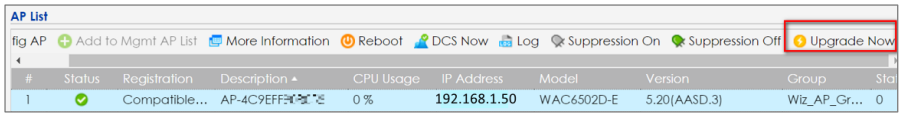
The example instructs how to upgrade the firmware for specific AP. We do not have to upgrade all the AP firmware at the same time.

7.3.2.1 Upgrade the AP firmware via GUI

1 Log in to controller and go to **Monitor > Wireless > AP Information > AP List.**

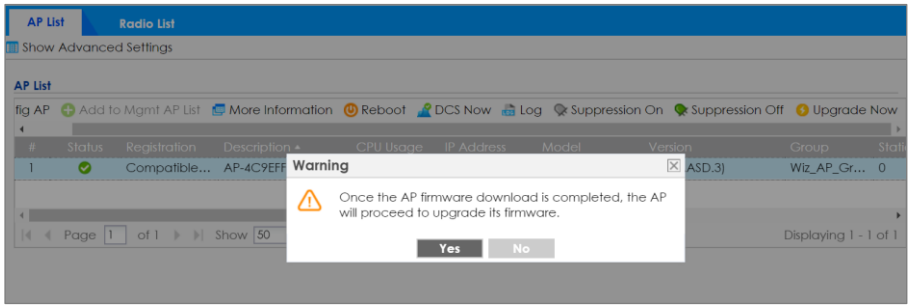
Choose the AP which is needed to be upgraded firmware.

Click **Upgrade Now**.

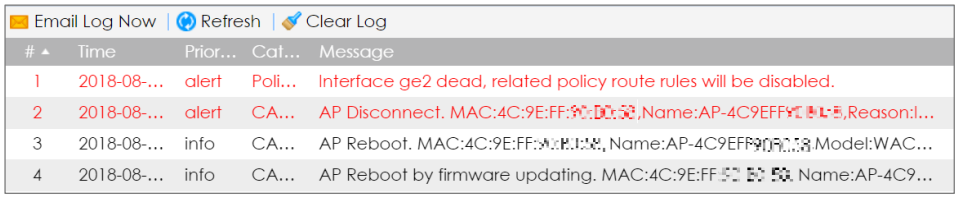


2 It will pop out a warning page.

Click **Yes**.

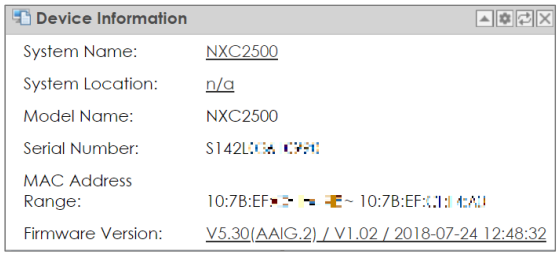


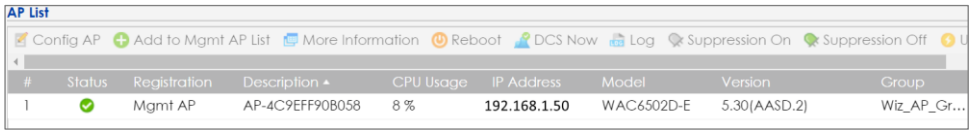
3 There is information about AP upgrading firmware in the Monitor log.



7.3.2.2 Test the Result

The AP firmware version should be the same with the NXC





7.3.2.3 What Could Go Wrong

1 If the AP firmware is the latest, the "Upgrade Now" button will be gray.

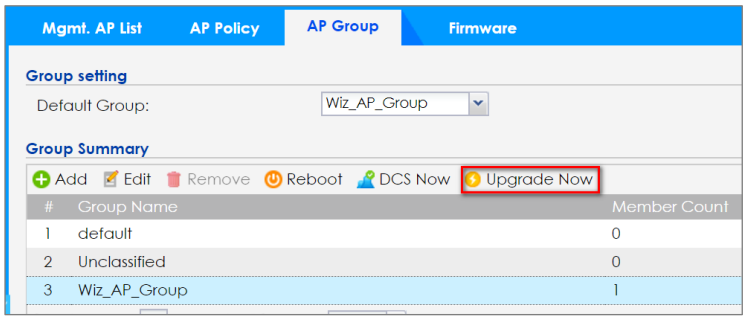
7.3.3 How to upgrade the firmware for AP group?

The example instructs how to upgrade the firmware for specific AP group.

7.3.3.1 Upgrade the firmware for AP group via GUI

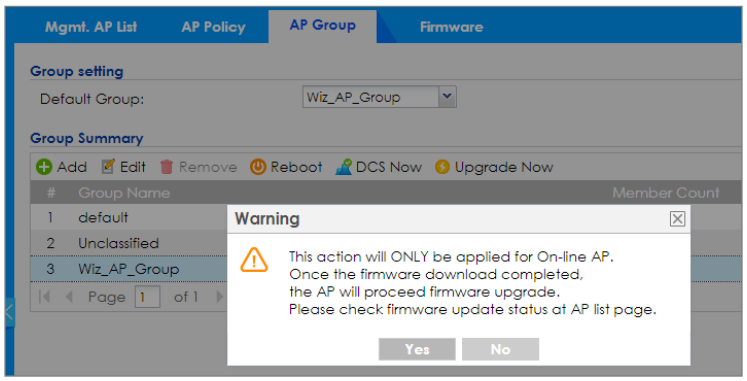
1 Log in to controller and go to **CONFIGURATION > Wireless > AP Management > AP Group.**

Choose the AP Group and click "**Upgrade Now**".



2 It will pop out a warning message.

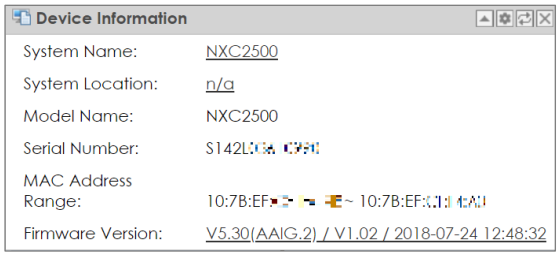
Click **Yes**.

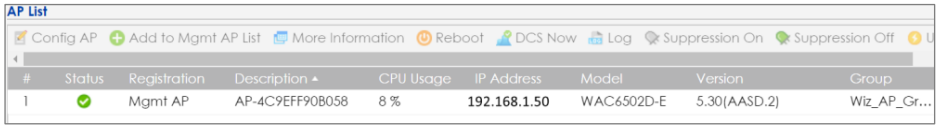


3 Check the log in Monitor. It will show the AP group Reboot by firmware updating.

7.3.3.2 Test the Result

The AP firmware version should be the same with the NXC.





7.3.3.3 What Could Go Wrong

1. If the AP firmware is the latest, there will no action for the firmware upgrade.
2. The firmware upgrade for the AP group will only be applied for O-line AP. If the AP is offline, it will not be upgraded.

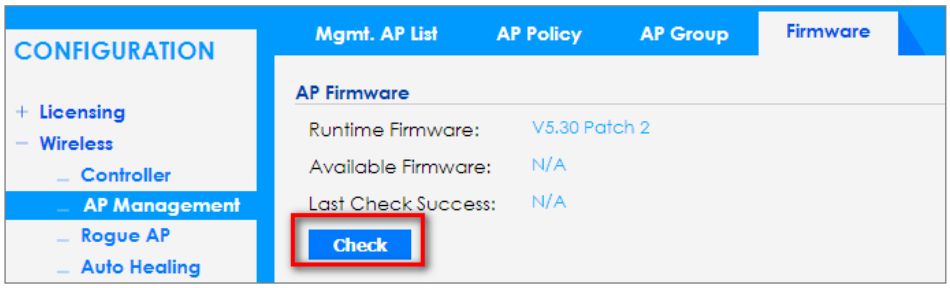
7.4 How to Upgrade the AP firmware via cloud?

The example instructs how to upgrade the AP firmware via cloud. We do not have to download the DF to out PC and upload it to the AP. Just check the firmware version via internet. If there is newer firmware version, we can download it to NXC then apply to AP.

7.4.1 Upgrade the firmware for AP group via GUI

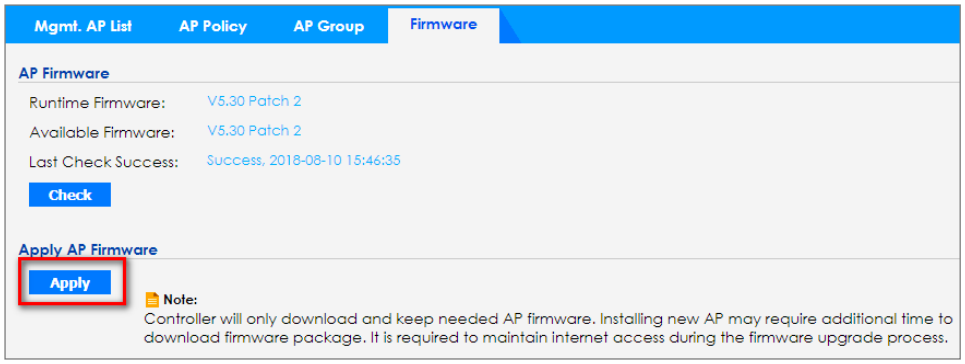
1 Log in to controller and go to **CONFIGURATION > Wireless > AP Management > Firmware.**

Click **Check.**



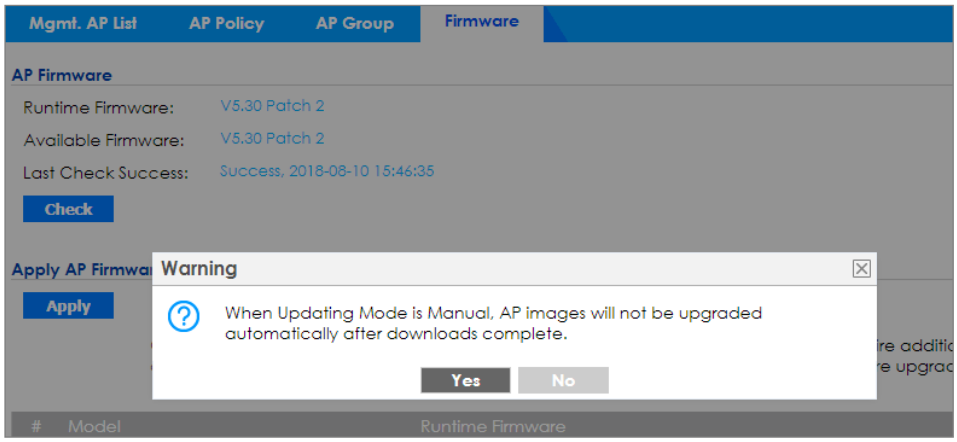
2 After getting the latest firmware version from the cloud, it will show the available firmware version and last check success time.

Click **Apply** to have the NXC download the latest AP firmware from the firmware server.



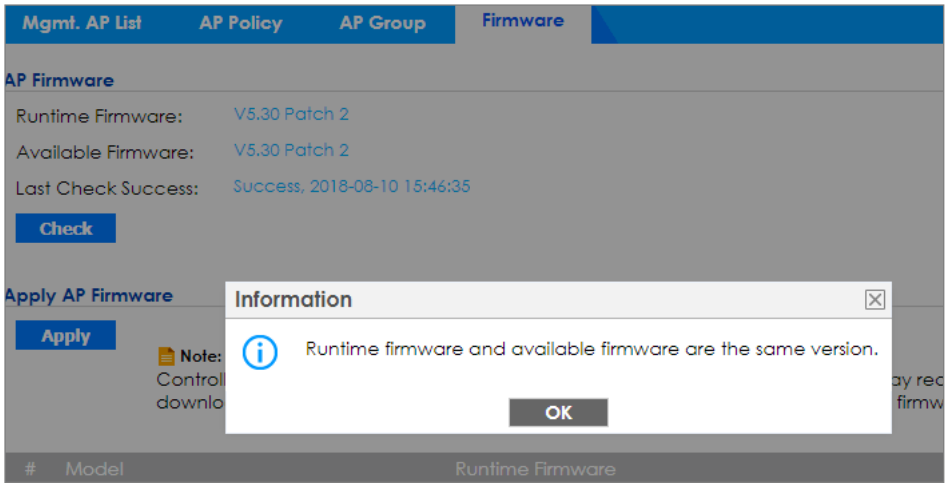
3 It will pop out a warning message.

Click **Yes**.



4 It will pop out information.

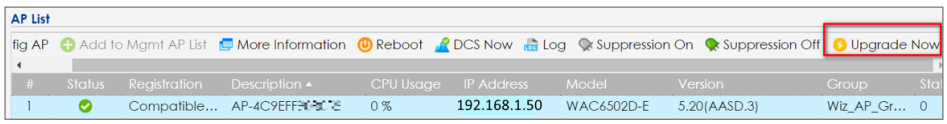
Click **OK**.



5 Log in to controller and go to **Monitor > Wireless > AP Information > AP List.**

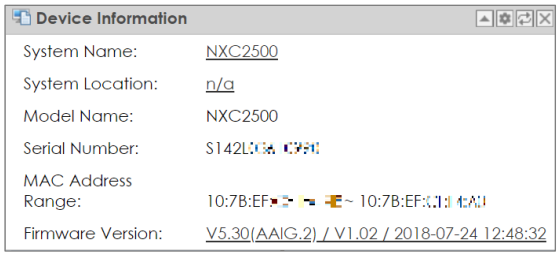
Choose the AP which is needed to be upgraded firmware.

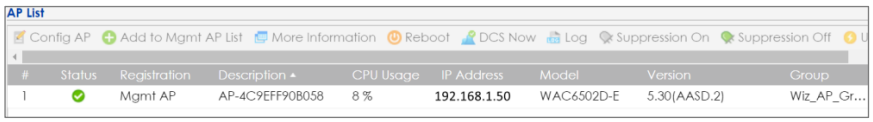
Click **Upgrade Now**.



7.4.2 Test the Result

The AP firmware version should be the same with the NXC.





7.4.3 What Could Go Wrong

1 If the AP firmware is the latest, there will no action for the firmware upgrade.

The firmware upgrade for the AP group will only be applied for O-line AP. If the AP is offline, it will not be upgraded.

Trouble Shooting

8.1 How to Collect the Diagnostic Info?

The diagnostic info needs to be collected when there's any problem happened on the controller or AP.

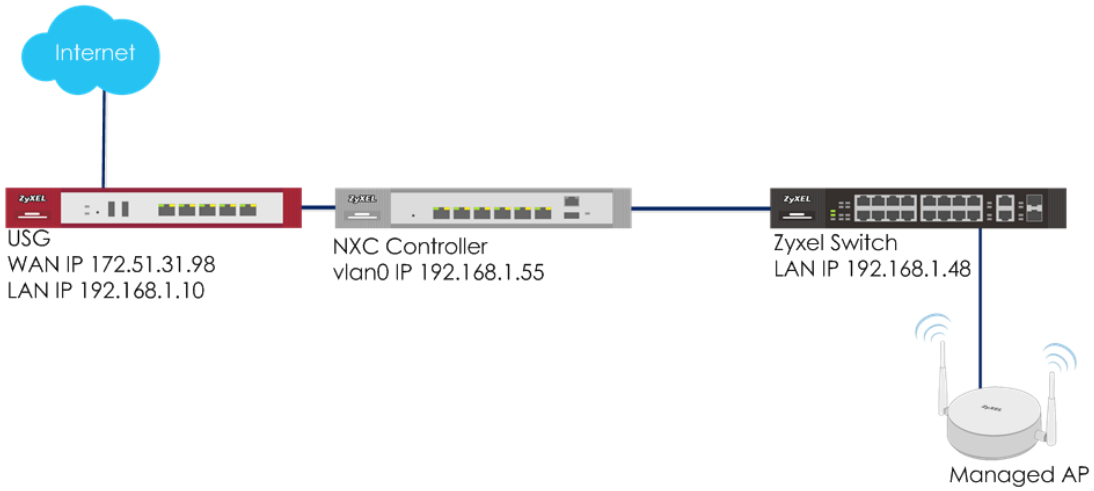
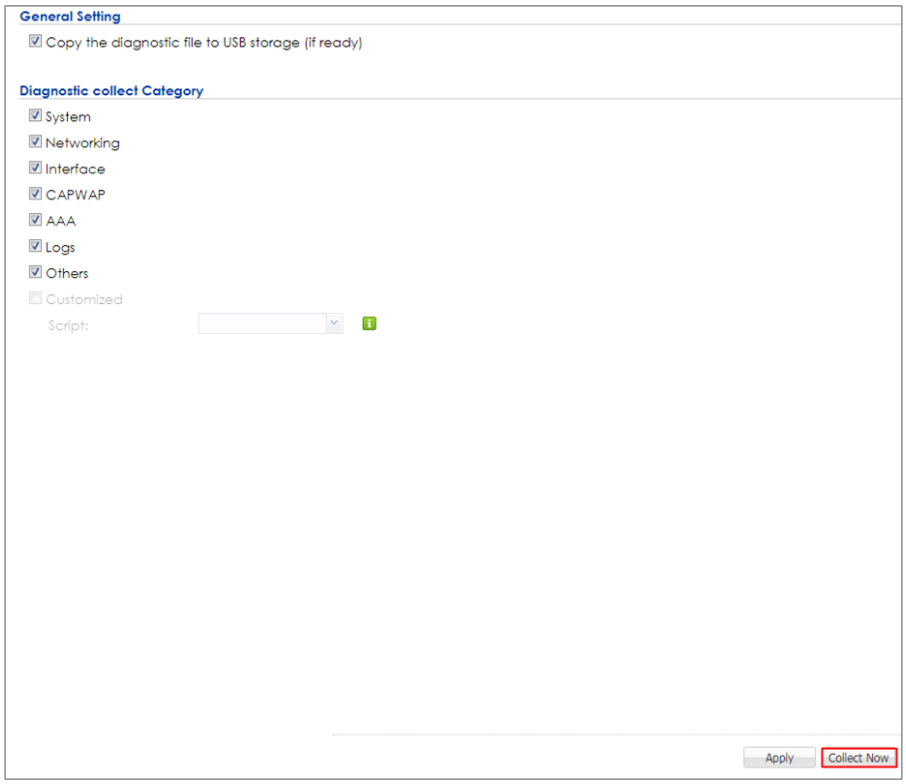


Figure 8.1 Collect the Diagnostic Info

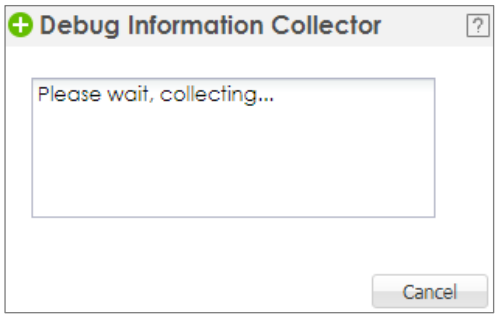
Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC2500 (Firmware Version: 5.40), GS2210-8HP (Firmware Version: V4.30).

8.1.1 Collect Diagnostic Info

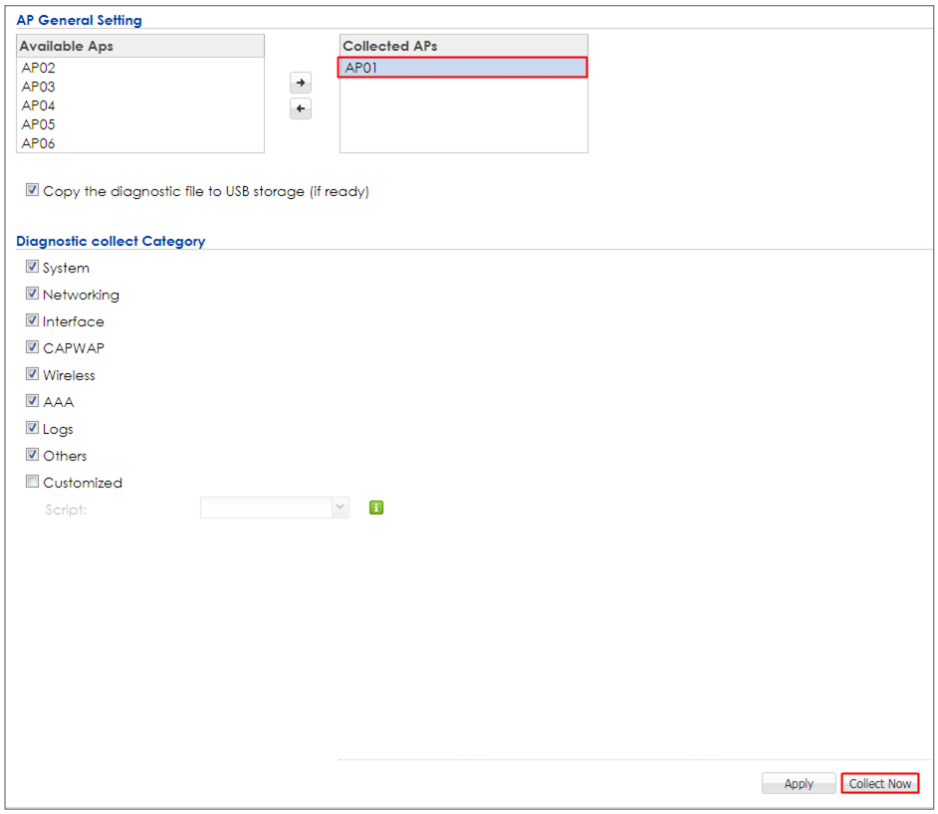
1 In **MAINTENANS > Diagnostic > Diagnostics**, select on **Collect on Controller** and click **Collect Now** when the controller has any problem.



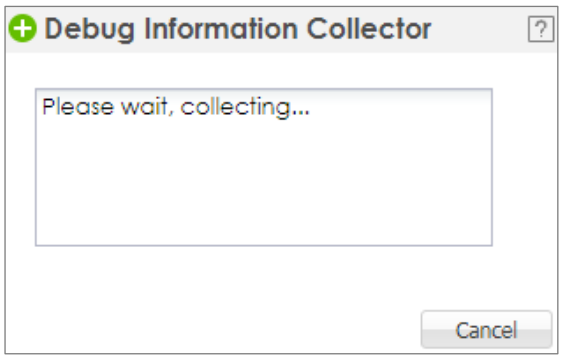
2 A window pops up when the controller is collecting the diagnostic.



3 In **MAINTENANS > Diagnostic > Diagnostics**, select on **Collect on AP** and move the AP's MAC to the **collected APs** list. Click **Collect Now** to start collection.

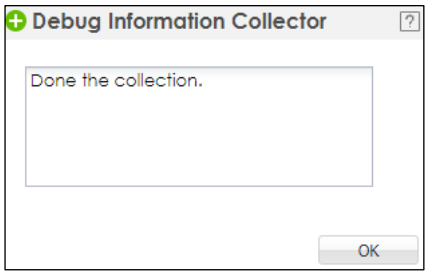


4 A window pops up when the controller is collecting the diagnostic.

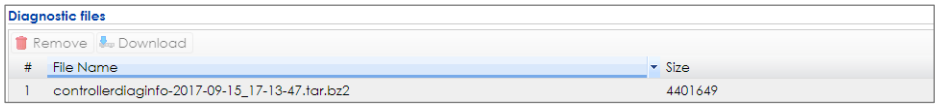


8.1.2 Test the Result

1 When the collection finished, a pop-up window shows "**Done the collection.**



2 After capturing the packet, there is a file in **MAINTENANCE > Diagnostics > Diagnostic > Files** for downloading.



8.2 How to Configure the E-mail Settings for Sending Logs?

This configuration set email for sending logs and let the controller manager gets the daily report and the system logs.

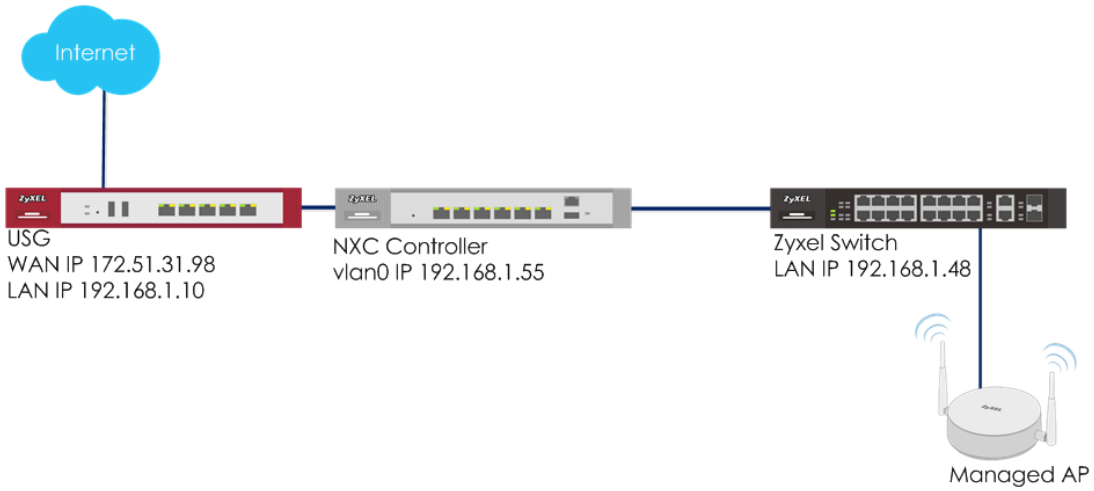


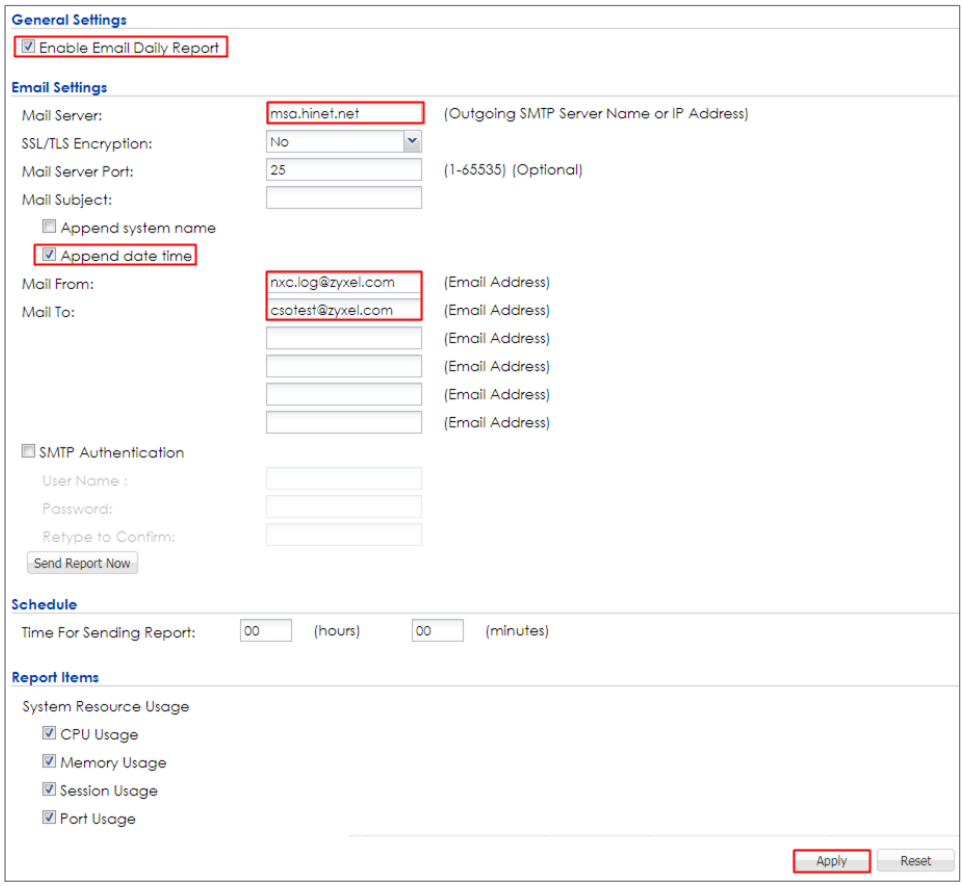
Figure 8.2 E-mail Settings for Sending Logs

Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC2500 (Firmware Version: 5.40), GS2210-8HP (Firmware Version: V4.30).

8.2.1 Configure Log & Report

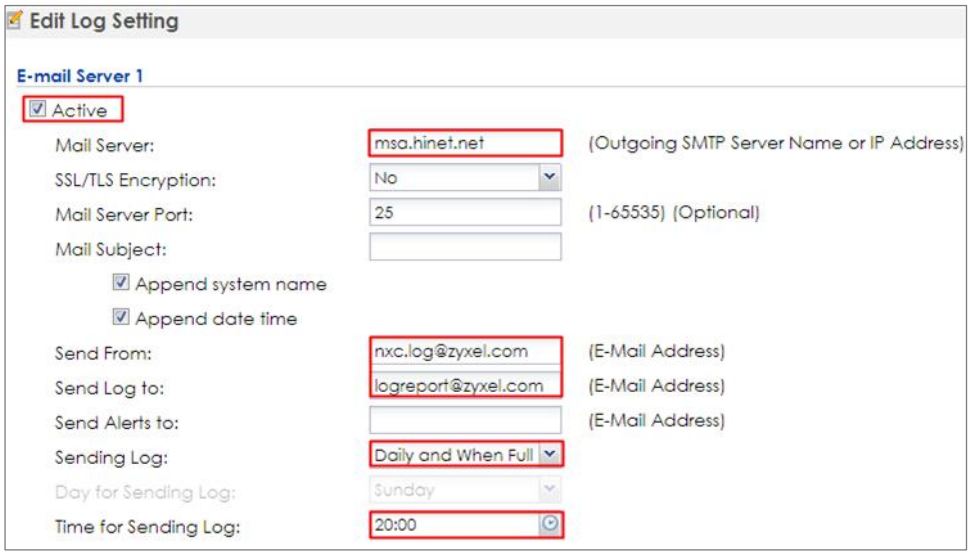
1 Configure daily report in **CONFIGURATION > Log & Report > Email Daily Report**.

In **Email Settings**, enter the **Mail Server** which can send out the email. Check the **Append data time** for daily report, and set the email address in **Mail From** and **Mail To**. Click **Apply** to save the setting.



2 Configure daily report in **CONFIGURATION > Log & Report > Log Settings**.

In **Log Settings**, click the first setting and **Edit** it. Check Active to activate this setting. Enter the **Mail Server**, and set the email address in **Mail From** and **Mail To**. Set the sending condition to **Daily and When Full**, and the **Time for Sending Log**. Click **OK** to save.



8.2.2 Test the Result

1 The manager who has the email receives the system Daily report.

Top Host IP Address/User

#	Direction	IP Address/User	Amount
1	Tx To	239.255.255.250	509.635 (MBytes)
2	Rx From	10.214.30.230	83.529 (MBytes)
3	Rx From	192.168.1.2	74.376 (MBytes)
4	Rx From	10.214.20.52	52.311 (MBytes)
5	Rx From	10.214.20.90	51.360 (MBytes)
6	Tx To	10.214.60.255	49.809 (MBytes)
7	Rx From	10.214.60.57	40.584 (MBytes)
8	Rx From	10.214.20.11	31.258 (MBytes)
9	Tx To	224.0.0.251	29.546 (MBytes)
10	Tx To	255.255.255.255	25.069 (MBytes)
11	Rx From	10.214.100.15	22.196 (MBytes)
12	Rx From	10.214.60.142	19.341 (MBytes)
13	Rx From	10.214.60.62	17.357 (MBytes)
14	Rx From	10.214.60.72	12.570 (MBytes)
15	Rx From	10.214.60.45	12.087 (MBytes)
16	Rx From	10.214.60.42	11.014 (MBytes)
17	Rx From	10.214.60.43	10.201 (MBytes)
18	Rx From	10.214.60.54	9.801 (MBytes)
19	Tx To	224.0.0.252	8.910 (MBytes)
20	Rx From	10.214.60.112	8.829 (MBytes)

2 The manager who has the email receives the log daily or when it's full.

No.	Date/Time	Source	Destination
	Priority	Category	Note
	Message		
1	2017-09-18 14:12:42		
	info	wlan-dcs	WLAN DCS
	Radio2 configure DCS as INTERVAL mode		
2	2017-09-18 14:12:45		
	info	capwap	
	Updated Configuration by a WLAN Controller Success. Partial Update [count=2]		
3	2017-09-18 14:12:50		
	info	wlan-dcs	WLAN DCS
	Radio1 configure DCS as INTERVAL mode		
4	2017-09-18 14:14:05		
	info	wlan-dcs	WLAN DCS
	Radio1 DCS start channel selection procedure		
5	2017-09-18 14:14:05		
	info	wlan-dcs	WLAN DCS
	Radio2 DCS start channel selection procedure		
6	2017-09-18 14:14:05		
	info	wlan-dcs	WLAN DCS
	Radio1 DCS change channel from 6 to 11. (At first time.)		
7	2017-09-18 14:14:05		
	info	wlan-dcs	WLAN DCS
	Radio2 DCS change channel from 36 to 40. (At first time.)		
8	2017-09-18 14:15:50		
	info	wlan-dcs	WLAN DCS
	Radio1 DCS start channel selection procedure		
9	2017-09-18 14:15:50		