NXC5500/2500

Version 4.21

Edition 1, 11/2015

Application Note

Contents

Contents 0

Smart Client Steering 1

- Smart Client Steering Introduction 1
- Terminologies of Smart Client Steering 1
- How Does It Work? 2
- Configuration 3

Dual-optimized Antenna Switch 6

- Dual-optimized Antenna Switch Introduction 6
- Terminologies of Dual-optimized Antenna Switch 7
- How Does It Work? 7
- Configuration 8

ZyXEL One Network Utility Supports Managed AP 12

- ZyXEL One Network Introduction 12
- How Does It Work? 13

Portal Redirection on Managed AP Application 15

- Portal Redirection on Managed AP Application Introduction 15
- How Does It Work? 15
- Application Scenario 18
- Conclusion: 23

Smart Client Steering

Smart Client Steering Introduction

- ### What is Smart Client Steering?

Due to the Bring Your Own Device (BYOD) trend, more and more access points (APs) are being deployed to meet the connectivity requirements of handheld devices. However, the 2.4 GHz frequency band which is commonly used by handheld devices is often congested. Gadgets running on the 2.4 GHz frequency typically experience interference from Bluetooth devices, electronics such as microwave ovens, and cordless phones, as well as co-channel interference from other APs, considering there are only three non-overlapping channels available for the IEEE 802.11 b/g/n wireless standards. The Band Select function enables devices with dual-band capability (2.4 GHz and 5 GHz) to move to a less congested AP that is operating on 5 GHz. Thus, the 5 GHz channel becomes an alternative choice for providing Wi-Fi service. The Band Select function provides a better wireless experience for users.

While more and more clients support the 5 GHz frequency, wireless resource optimization becomes more and more important. To avoid the legacy clients from occupying the wireless resource, ZyXEL provides some features to improve the wireless network.

- ### This technology helps:
  - Optimize wireless spectrum usage
  - Improve user experience

Terminologies of Smart Client Steering

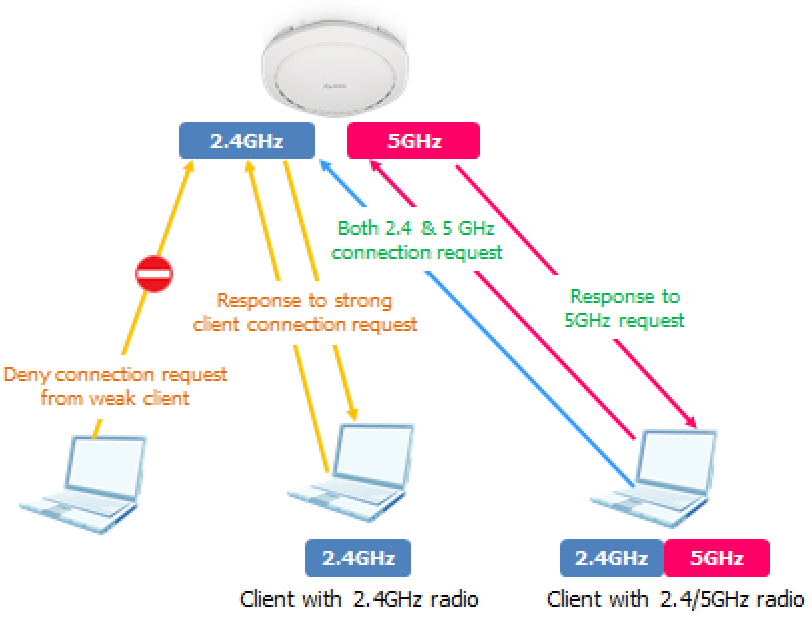
- ### Client Band Select
  - ✧ Band Select allows devices with dual-band capability (2.4 GHz and 5 GHz) to move to a less congested AP operating on 5 GHz. Thus, the 5 GHz channel utilization is further enhanced when providing Wi-Fi service.

- **Client Band Balancing**
  - ✧ Today there are more and more 5 GHz capable clients. This function helps to prevent situations such as 5 GHz radio overload and 2.4 GHz radio underload, thus provides a well-balanced spectrum utilization.

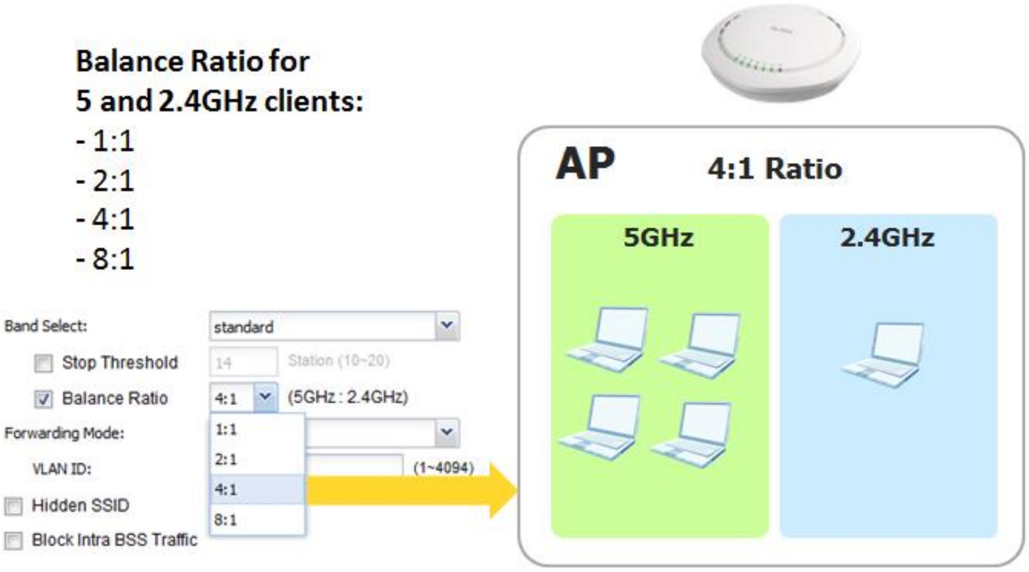
- **RSSI Threshold**
  - ✧ RSSI is an indication of the power level being received by the access point. Thus, the higher the RSSI number, the stronger the signal. With the RSSI threshold settings, users can specify a signal strength level to prevent poor signal clients from affecting the wireless network.

How Does It Work?

- Features with band select and client signal thresholds
- Monitor the capabilities of each wireless client and direct the clients to the best radio on the best AP by using the band select and signal thresholds.


2.4GHz
5GHz
Both 2.4 & 5 GHz connection request
Response to strong client connection request
Response to 5GHz request
Deny connection request from weak client
2.4GHz
Client with 2.4GHz radio
2.4GHz
5GHz
Client with 2.4/5GHz radio

- Smart Client Steering supports the Client Band Balancing feature which detects dual-radio clients and distributes clients across the 2.4 and 5 GHz band APs based on two independent configurable parameters - Stop Threshold & Balance Ratio.



Balance Ratio for 5 and 2.4GHz clients:

- 1:1
- 2:1
- 4:1
- 8:1

Band Select: standard

□ Stop Threshold 14 Station (10~20)

☑ Balance Ratio 4:1 (5GHz : 2.4GHz)

Forwarding Mode:

VLAN ID: (1~4094)

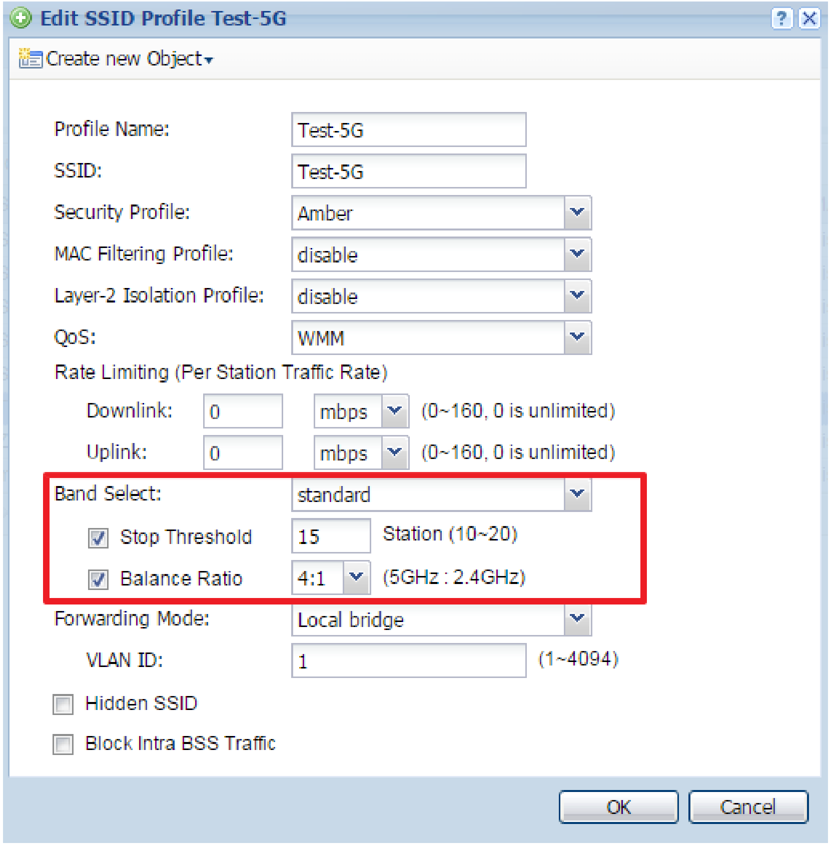
□ Hidden SSID

□ Block Intra BSS Traffic

Configuration

- **Band Select / Band Balance**

  Web GUI Setting Path: **Configuration** > **Object** > **AP Profile** > **SSID**



Profile Name:	Test-5G
SSID:	Test-5G
Security Profile:	Amber
MAC Filtering Profile:	disable
Layer-2 Isolation Profile:	disable
QoS:	WMM

Rate Limiting (Per Station Traffic Rate)

Downlink:	0	mbps	(0~160, 0 is unlimited)
Uplink:	0	mbps	(0~160, 0 is unlimited)

Band Select: standard

☑ Stop Threshold 15 Station (10~20)

☑ Balance Ratio 4:1 (5GHz : 2.4GHz)

Forwarding Mode: Local bridge

VLAN ID: 1 (1~4094)

□ Hidden SSID

□ Block Intra BSS Traffic

- **Stop Threshold:**

  Select this option and set the threshold number of the connected wireless clients with the Band Select feature disabled.

- **Balance Ratio:**

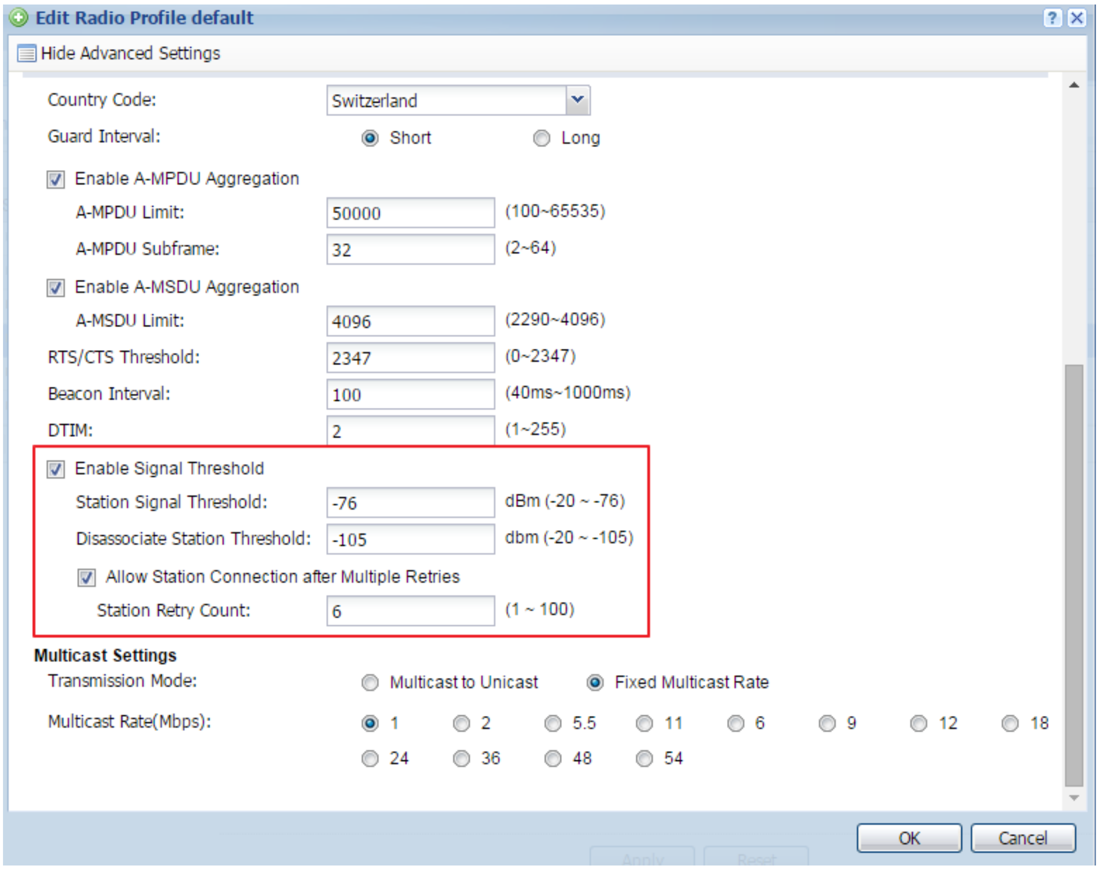
  Select this option and set a ratio of the wireless clients using the 5 GHz band to the wireless clients using the 2.4 GHz band.

- **Notice:**

  The ideal ratio is to make full use of the two radios. The current status depends on the client's wireless card behavior. For example, more and more dual-band capable clients has 5 GHz set as the default preference. This feature will impact the actual ratio that you set in the ***Band Select-Balance Ratio*** *option.*

RSSI Threshold

Web GUI Setting Path: **Configuration** > **Object** > **AP Profile** > **Radio**



Edit Radio Profile default

Hide Advanced Settings

Country Code: Switzerland

Guard Interval: ● Short ○ Long

☑ Enable A-MPDU Aggregation

A-MPDU Limit: 50000 (100~65535)

A-MPDU Subframe: 32 (2~64)

☑ Enable A-MSDU Aggregation

A-MSDU Limit: 4096 (2290~4096)

RTS/CTS Threshold: 2347 (0~2347)

Beacon Interval: 100 (40ms~1000ms)

DTIM: 2 (1~255)

☑ Enable Signal Threshold

Station Signal Threshold: -76 dBm (-20 ~ -76)

Disassociate Station Threshold: -105 dbm (-20 ~ -105)

☑ Allow Station Connection after Multiple Retries

Station Retry Count: 6 (1 ~ 100)

Multicast Settings

Transmission Mode: ○ Multicast to Unicast ● Fixed Multicast Rate

Multicast Rate(Mbps): ● 1 ○ 2 ○ 5.5 ○ 11 ○ 6 ○ 9 ○ 12 ○ 18 ○ 24 ○ 36 ○ 48 ○ 54

- **Station Signal Threshold**

  Set the minimum client signal strength. A wireless client is allowed to connect to the AP only when its signal strength is stronger than the specified threshold.

  The parameter -20 dBm is the strongest signal you can require and -76 dBm is the weakest.

- **Disassociate Station Threshold**

  Set the minimum kick-off signal strength. When a wireless client's signal strength is lower than the specified threshold, the NXC disconnects the wireless client from the AP.

  The parameter -20 dBm is the strongest signal you can require and -90 dBm is the weakest.

- **Allow Station Connection after Multiple Retries**

  Select this option to allow a wireless client to try to associate with the AP again after it is disconnected due to weak signal strength.

- **Notice**

  This feature detects the wireless signal from the AP. It means the strength calculation is based on the signal sent from the client and received by the AP. Since the AP is more sensitive than the wireless client, it can usually hear from a further distance than the client.

Dual-optimized Antenna Switch

Dual-optimized Antenna Switch Introduction

- **What is Dual-optimized Antenna Switch?**

Today, most access points in the market are designed with single static radiation pattern, typically for ceiling-mount. When an AP with ceiling-mount pattern is installed in a wall-mount scenario, its signal coverage does not fit the wall-mount deployment. Adapting an AP with external antenna may be an alternative option. However, external antenna installation requires know-hows for antenna selection, and it would seem awkward for interior decoration.

The WAC6103D-I is an 802.11ac AP designed for dual-way installation of wall and ceiling-mount. Its dual-optimized antenna allows pattern optimization to adapt to both the wall and ceiling-mount installations. The installation technician can instantly change the antenna pattern via the physical antenna switch without rebooting the device. If needed, administrators can perform granular signal optimization per floor plan via software configuration remotely. With this flexibility, the WAC6103D-I easily fits wall-mount or ceiling-mount deployment without the hassles of antenna selection and signal coverage adjustment.

- **This Technology helps:**

The dual-optimized antenna allows radiation pattern to be changed manually by adapting to versatile installations, thus delivering benefits such as:

- Coverage Optimization
- Dead Spots Elimination
- User Experience Improvement

Terminologies of Dual-optimized Antenna Switch

- **Physical Switch**

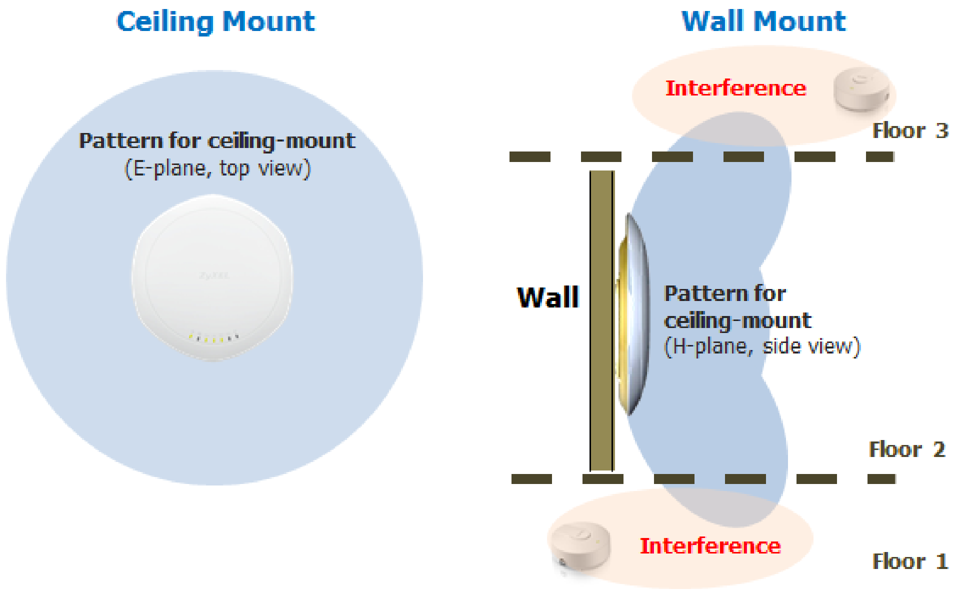
  Provide a dip switch at the rear side of the WAC6103D-I AP for pattern selection between wall-mount or ceiling-mount installation. By default, the setting is ceiling-mount.

- **Software Configuration**

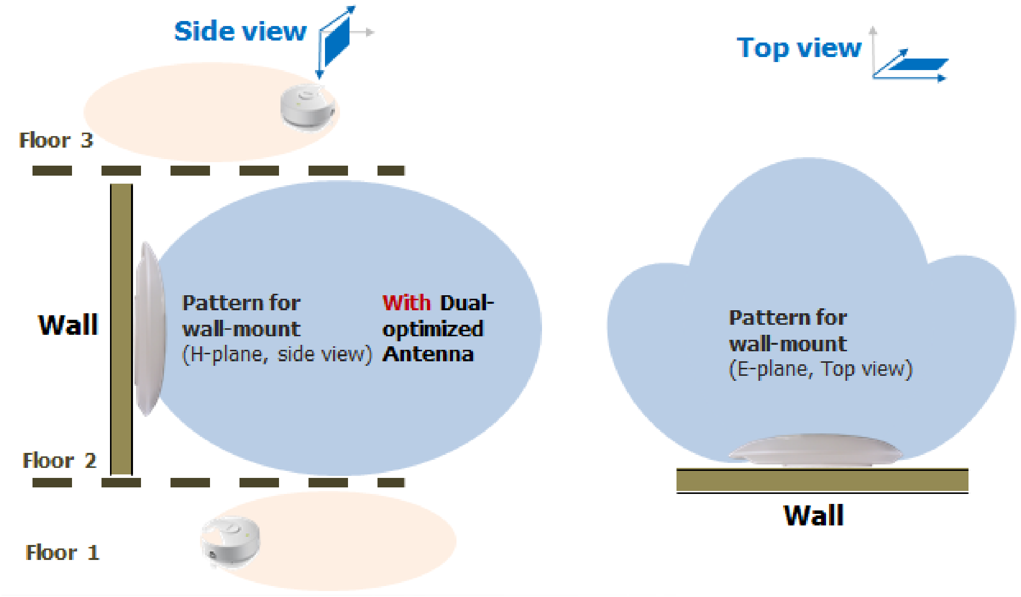
  Software configuration replaces a physical switch to allow remote antenna pattern adjustment.

How Does It Work?

When you install a ceiling-mount designed AP on a wall, the strengthened signals become interference to the upper and lower floors.



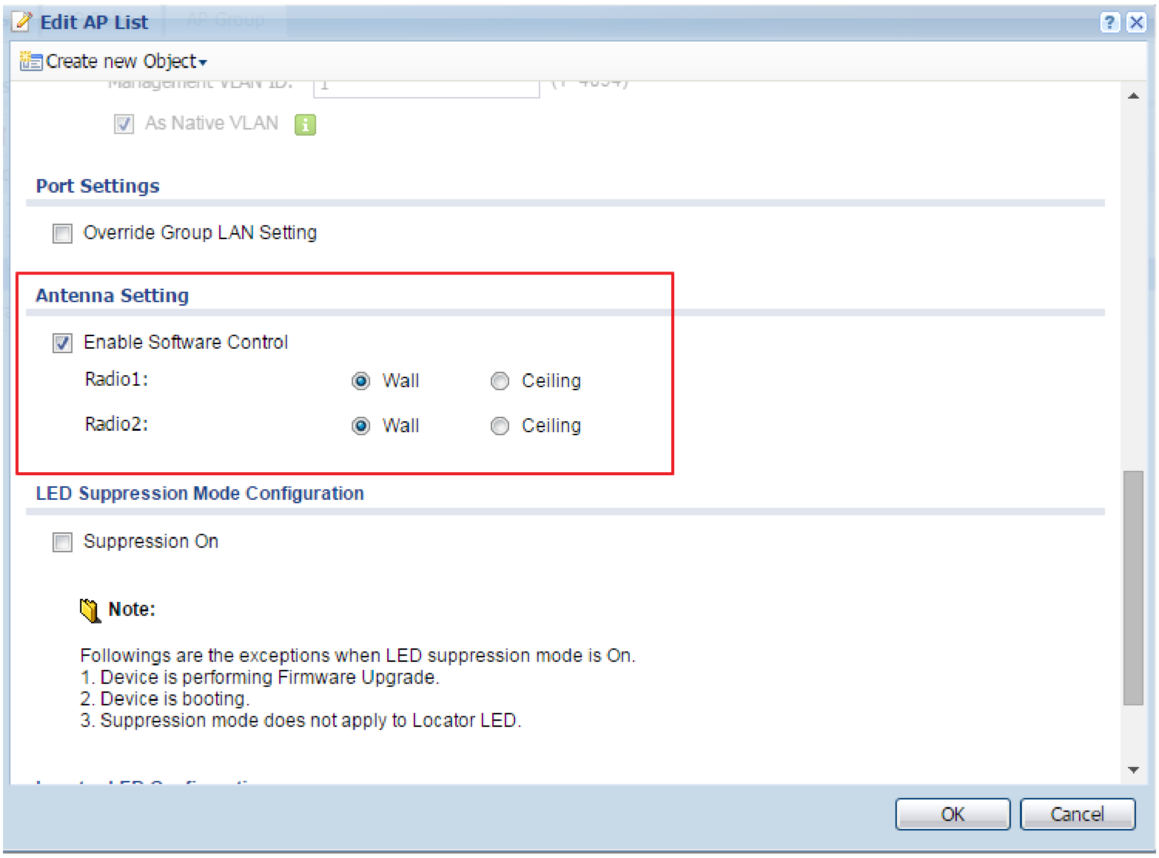
The WAC6103D-I wall-mount pattern focuses the signals to the front end to eliminate interference to other floors.


Side view
Floor 3
Wall
Pattern for wall-mount (H-plane, side view)
With Dual-optimized Antenna
Floor 2
Floor 1
Top view
Pattern for wall-mount (E-plane, Top view)
Wall

Configuration

▪ Controller/Managed AP

Web GUI Configuration Path: **CONFIGURATION > Wireless** > **AP Management**



Management VLAN ID: 1 (1~4094)

☑ As Native VLAN

Port Settings

□ Override Group LAN Setting

Antenna Setting

☑ Enable Software Control

Radio1: ● Wall ○ Ceiling

Radio2: ● Wall ○ Ceiling

LED Suppression Mode Configuration

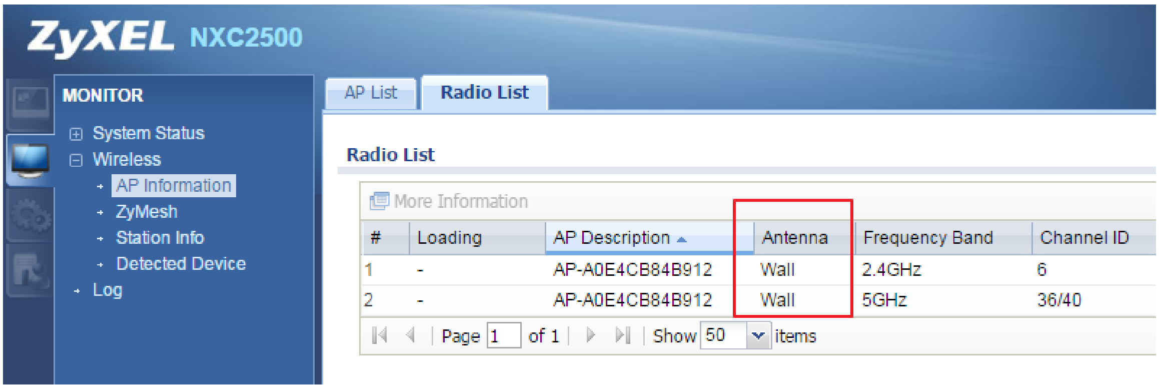
□ Suppression On

Note:

Followings are the exceptions when LED suppression mode is On.
1. Device is performing Firmware Upgrade.
2. Device is booting.
3. Suppression mode does not apply to Locator LED.

Check the Current Status

Path: **MONITOR** > **Wireless** > **AP information** > **Radio List**

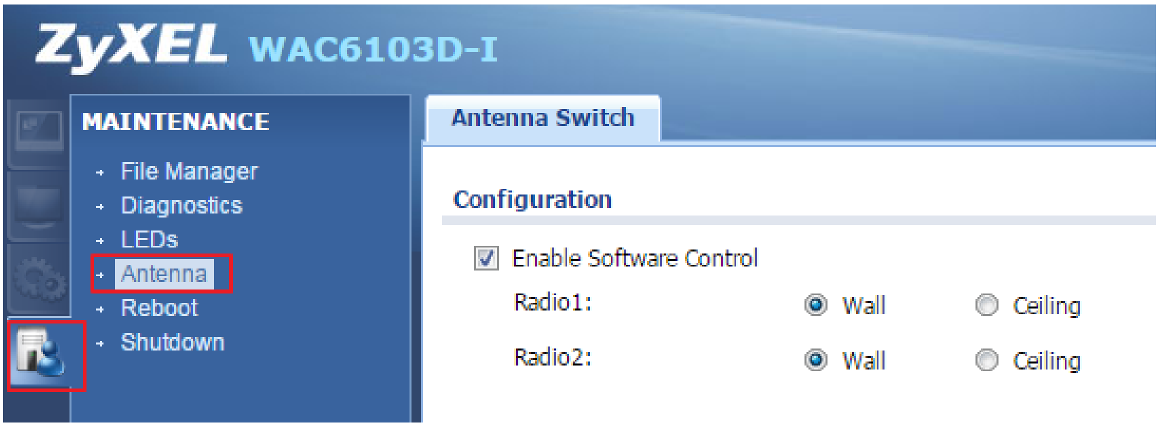


Radio List

#	Loading	AP Description	Antenna	Frequency Band	Channel ID
1	-	AP-A0E4CB84B912	Wall	2.4GHz	6
2	-	AP-A0E4CB84B912	Wall	5GHz	36/40

- **Standalone AP**

Web GUI Configuration Path: **MAINTENANCE** > **Antenna**



Configuration

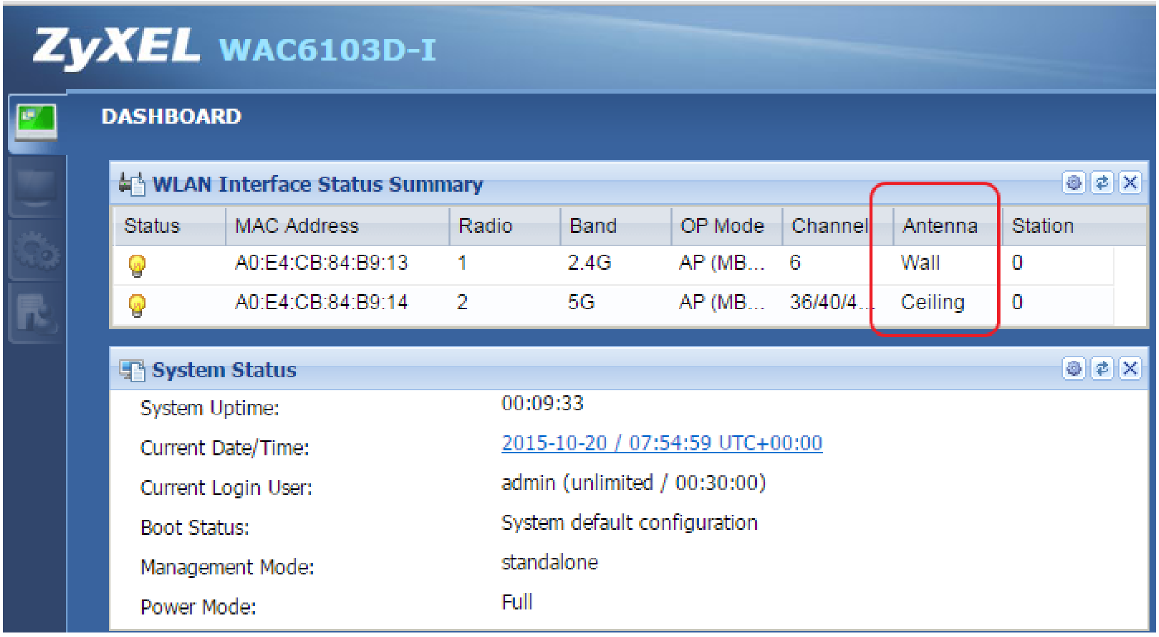
☑ Enable Software Control

Radio1: ● Wall ○ Ceiling

Radio2: ● Wall ○ Ceiling

Check the Current Status

Web GUI Path: **MONITOR** > **Wireless** > **AP information** > **Radio List**



WLAN Interface Status Summary

Status	MAC Address	Radio	Band	OP Mode	Channel	Antenna	Station
	A0:E4:CB:84:B9:13	1	2.4G	AP (MB...	6	Wall	0
	A0:E4:CB:84:B9:14	2	5G	AP (MB...	36/40/4...	Ceiling	0

System Status

System Uptime: 00:09:33

Current Date/Time: 2015-10-20 / 07:54:59 UTC+00:00

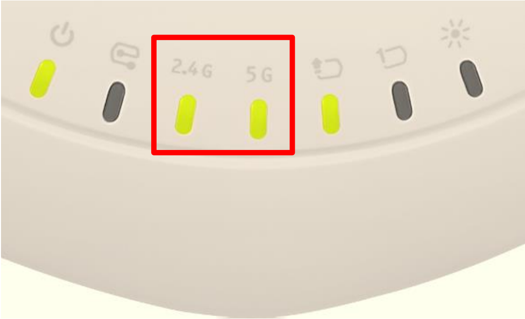
Current Login User: admin (unlimited / 00:30:00)

Boot Status: System default configuration

Management Mode: standalone

Power Mode: Full

- **The WLAN LEDs indicate the real-time antenna pattern status**



WLAN LED	Antenna Pattern	LED Color
2.4GHz LED	**Ceiling-mount**	**Green**
	Wall-mount	**Amber**
5GHz LED	**Ceiling-mount**	**Green**
	Wall-mount	**Amber**

ZyXEL One Network Utility Supports Managed AP

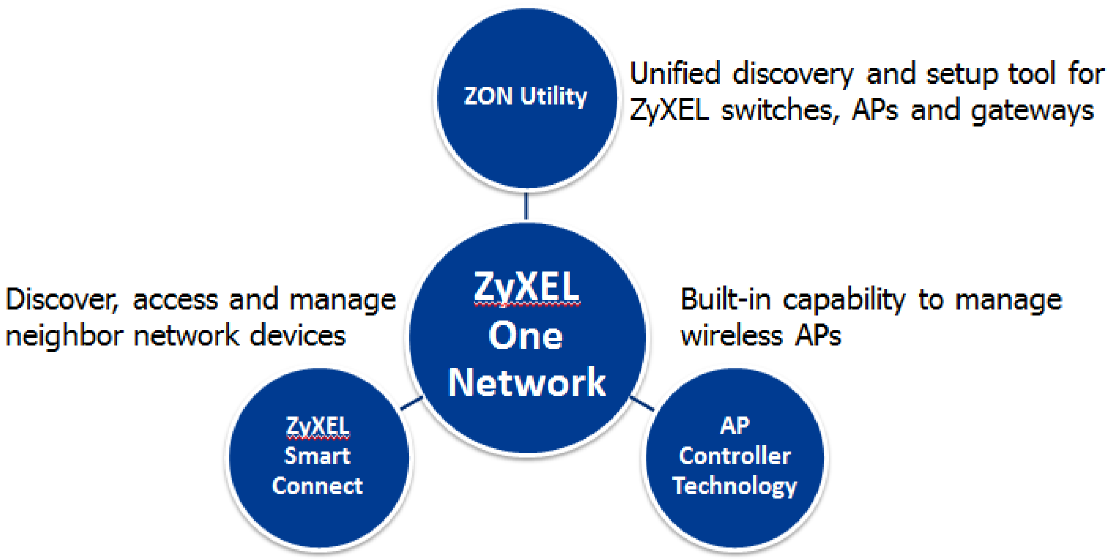
ZyXEL One Network Introduction

- ### What is ZyXEL One Network

The reality of today's networking business is that different product lines lack consistency and integration. In this industry, the equipment manufacturers often acquire new technologies for a shorter time-to-market. As a result, products under one brand might have totally different graphic or command line interfaces, or similar names for features that perform differently. As a networking brand that strives to deliver the best solutions to its customers, ZyXEL addresses this problem and aims to take the business of networking to a new height by introducing the ZyXEL One Network feature.

With the vision to make the world connect, ZyXEL presents comprehensive business networking solutions from switches to wireless, security appliances, and gateways. The robust, reliable networking equipments from ZyXEL, which is one of the few companies that possess the key technologies for all business networking product lines, enable us to fully integrate switches, wireless APs and gateways in an innovative way.

The easiest, most efficient network setup and management for businesses



ZON Utility

Unified discovery and setup tool for ZyXEL switches, APs and gateways

ZyXEL One Network

Discover, access and manage neighbor network devices

ZyXEL Smart Connect

Built-in capability to manage wireless APs

AP Controller Technology

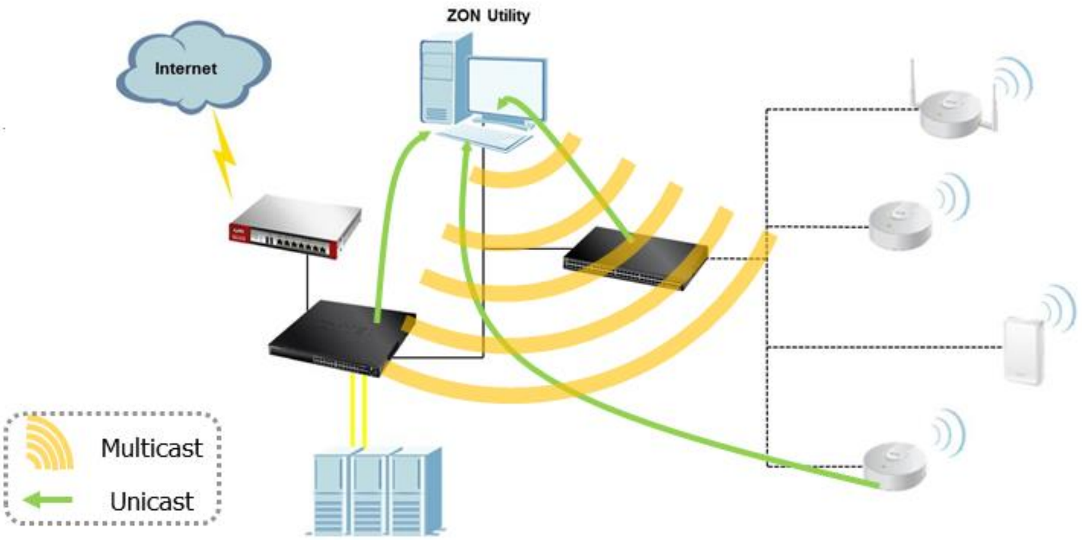
- **ZyXEL One Network Utility helps:**

- Discover deployed ZyXEL devices
- Change the default IPs and assign new ones
- Firmware upgrade
- Reboot devices
- Link to ZyXEL AP Configurator (ZAC) for advanced settings on a wireless AP

How Does It Work?

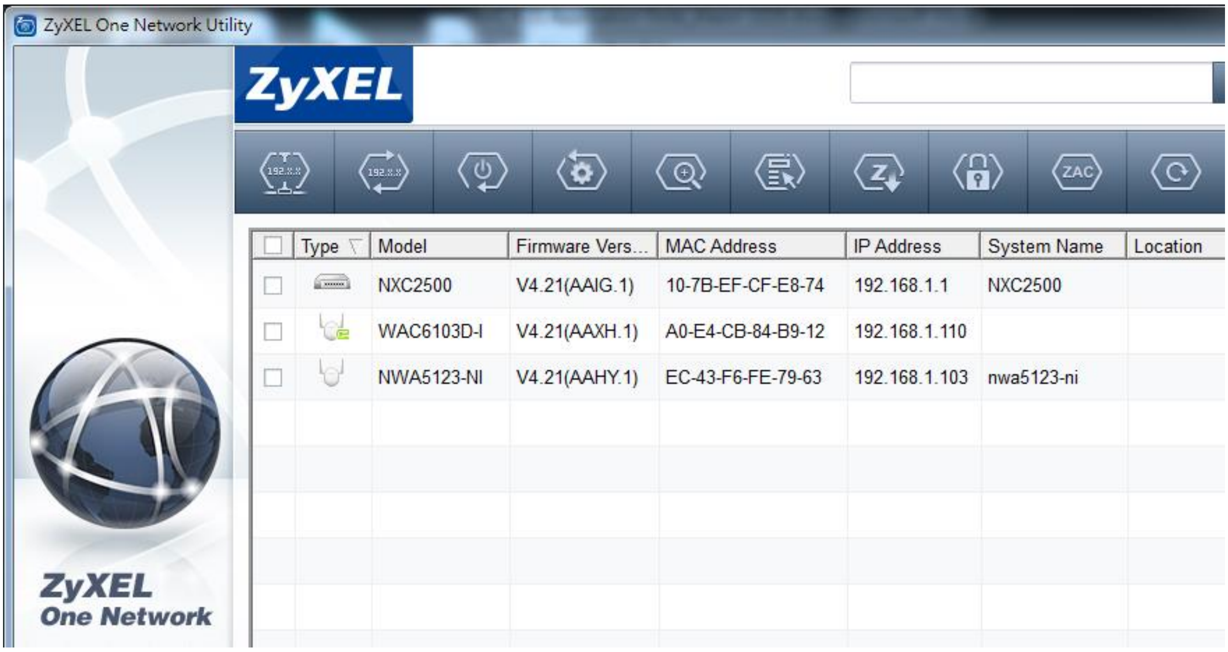
- **ZyXEL Discovery Protocol (ZDP) is used to realize the ZON Utility functions**

- ZyXEL proprietary protocol
- When the user clicks the **Scan** button, the utility sends out multicast discovery packets to the broadcast domain.
- ZyXEL devices will reply via unicast to the ZON utility.
- Click the **Scan** button again to refresh the discovery of newly added devices.



▪ What's New in V4.21

Before firmware v4.21, the ZON Utility can only discover and configure standalone APs. Since the release of firmware v4.21, the ZON Utility can discover not only standalone APs but also NXC controllers and managed APs.



□	Type	Model	Firmware Vers...	MAC Address	IP Address	System Name	Location
□		NXC2500	V4.21(AAIG.1)	10-7B-EF-CF-E8-74	192.168.1.1	NXC2500	
□		WAC6103D-I	V4.21(AAXH.1)	A0-E4-CB-84-B9-12	192.168.1.110		
□		NWA5123-NI	V4.21(AAHY.1)	EC-43-F6-FE-79-63	192.168.1.103	nwa5123-ni	

The above screen shows an example of the ZON Utility discovery: one NXC2500, one WAC6103D-I, and one NWA5123-NI. The WAC6103D-I is configured as a managed AP and the NWA5123-NI is configured as a standalone AP. With the new firmware v4.21, you can see that both AP modes can be discovered via the ZON Utility.

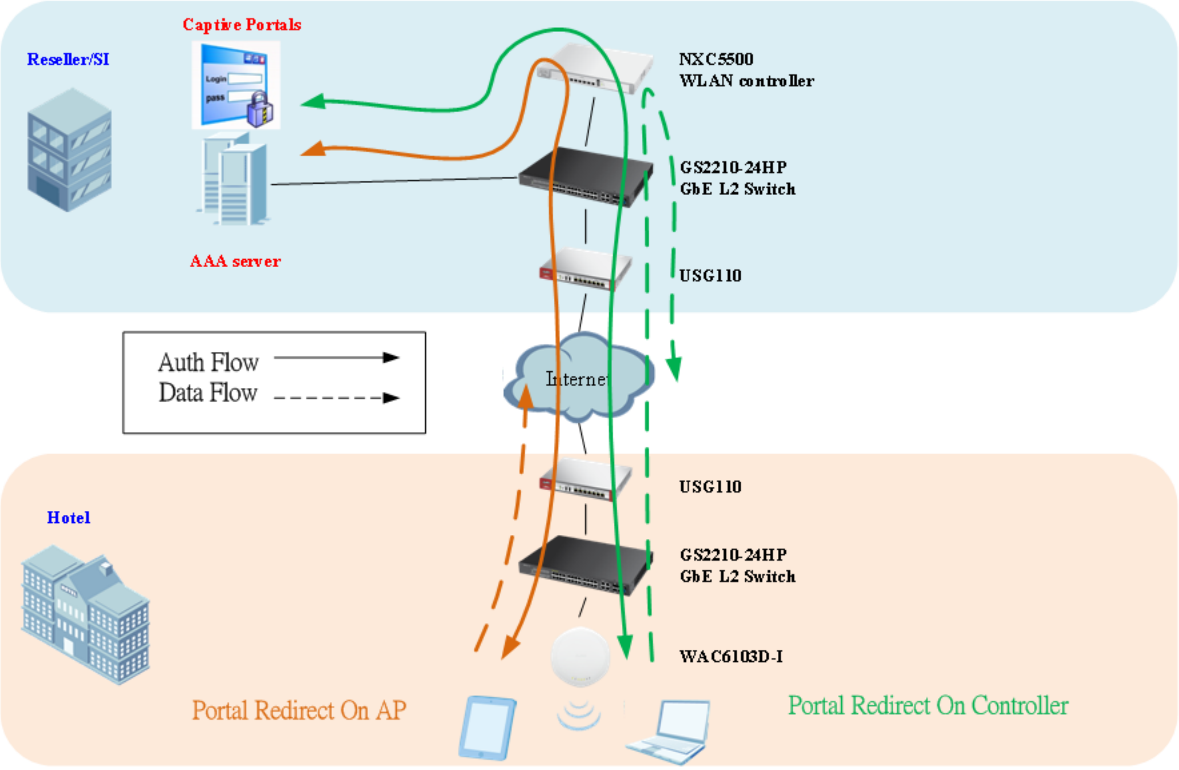
Notice:

1. *Fuctions such as configuration through the device's web GUI, upgrading firmware, and changing the password are not permitted for managed APs.*
2. *ZAC is only available for standalone APs.*

Portal Redirection on Managed AP Application

Portal Redirection on Managed AP Application Introduction

It is ideal to have captive portal application for controllers and APs located in different geographical locations or for hotspots without captive portal gateway deployment.



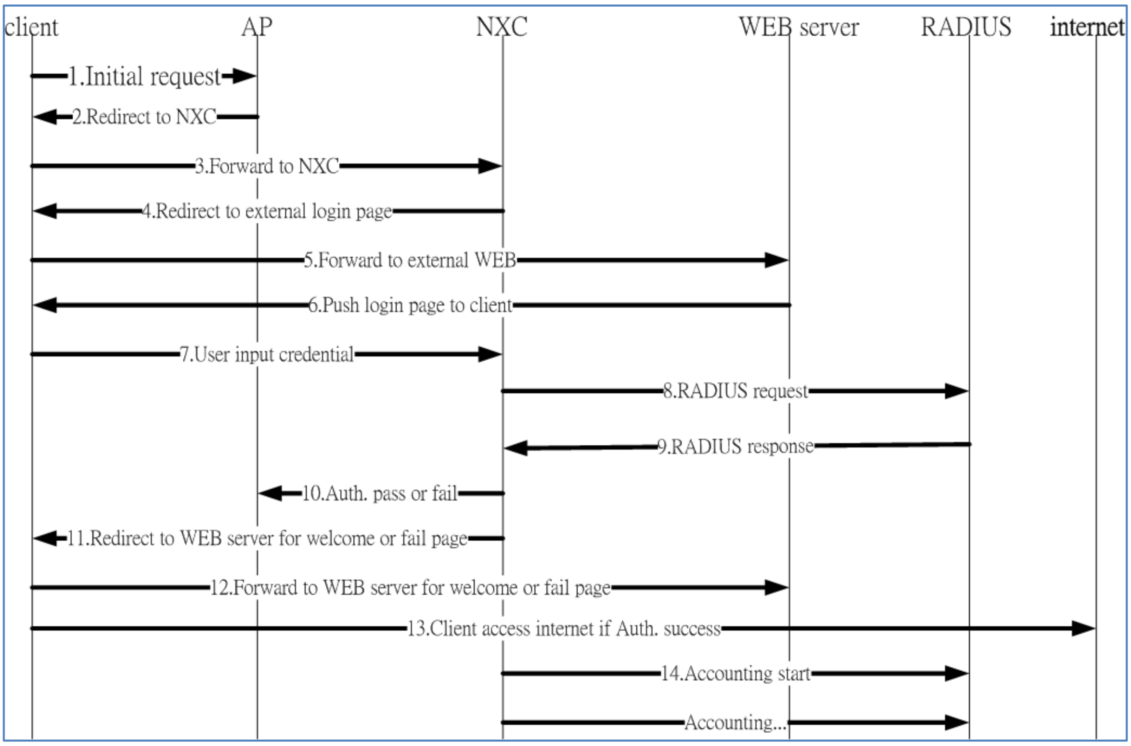
In FW release v4.20, captive portal redirect feature applies on the NXC controller only. From FW v4.21, captive portal redirect on Managed AP is introduced, which enhances network traffic efficiency without tunneling data traffic back to the NXC controller at the central site.

This provides more flexibility for web authentication configuration in both tunnel mode and local bridge mode.

How Does It Work?

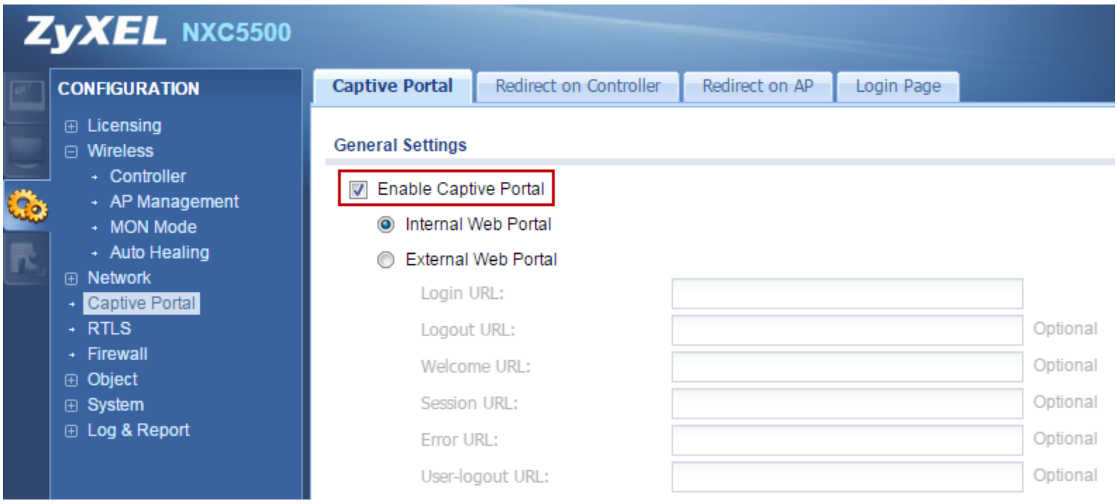
There are two portal redirect modes on the new firmware 4.21: redirect on controller and redirect on AP. Redirect on AP is a new feature to process web authentication over distributed APs to reduce centralized traffic loading on the controller.

The portal redirect on AP traffic flow chart is as shown below.


client
AP
NXC
WEB server
RADIUS
internet
1.Initial request
2.Redirect to NXC
3.Forward to NXC
4.Redirect to external login page
5.Forward to external WEB
6.Push login page to client
7.User input credential
8.RADIUS request
9.RADIUS response
10.Auth. pass or fail
11.Redirect to WEB server for welcome or fail page
12.Forward to WEB server for welcome or fail page
13.Client access internet if Auth. success
14.Accounting start
Accounting...

▪ Fundamental Configuration on GUI

1. In the **CONFIGURATION** > **Network** > **Captive Portal** screen, select **Enable Captive Portal**.



General Settings

☑ Enable Captive Portal

● Internal Web Portal

○ External Web Portal

Login URL:

Logout URL: Optional

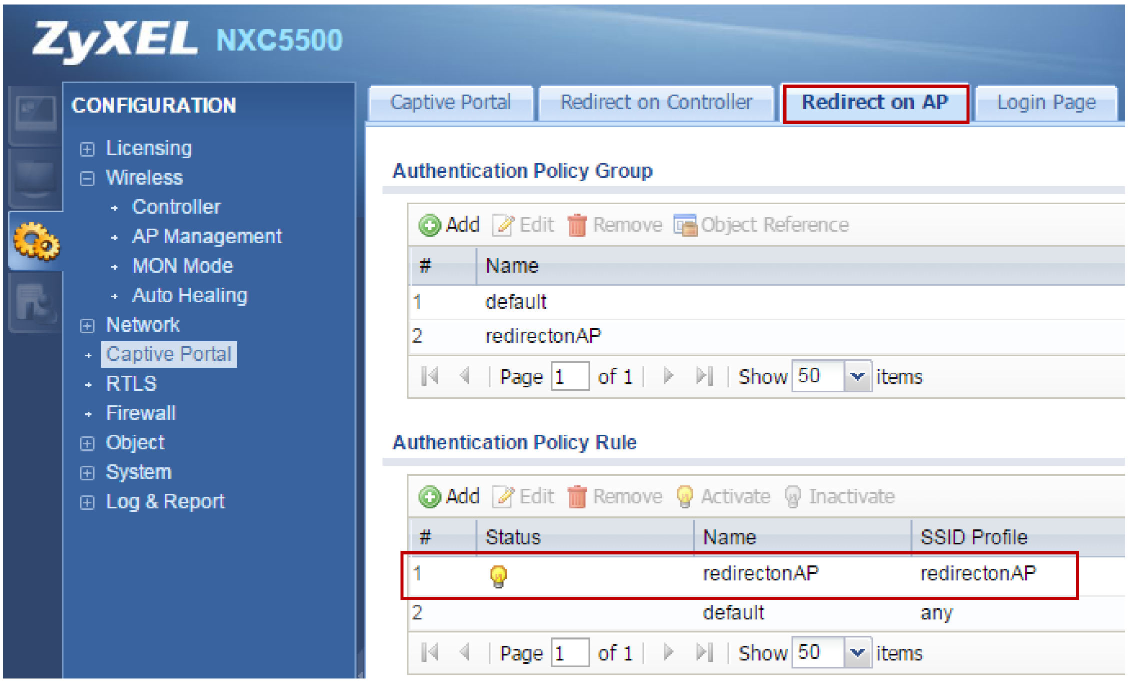
Welcome URL: Optional

Session URL: Optional

Error URL: Optional

User-logout URL: Optional

2. Click the Redirect on AP tab and create an Authentication Policy Rule which is an SSID-based policy to filter the traffic from the AP.



Authentication Policy Group

Add Edit Remove Object Reference

#	Name
1	default
2	redirectonAP

Page 1 of 1 Show 50 items

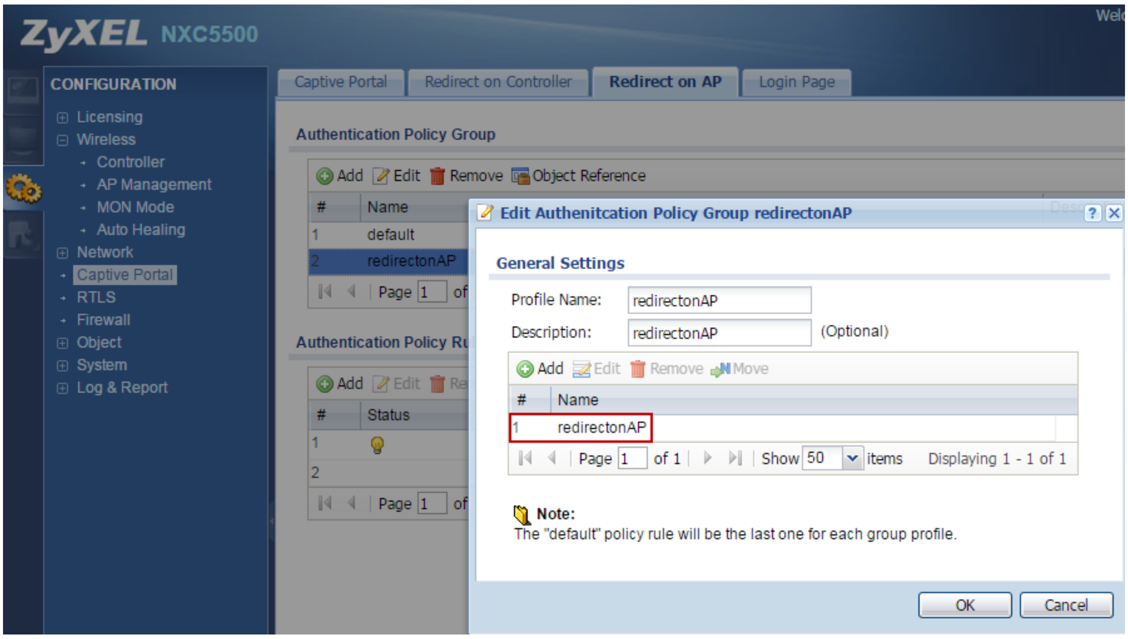
Authentication Policy Rule

Add Edit Remove Activate Inactivate

#	Status	Name	SSID Profile
1	💡	redirectonAP	redirectonAP
2		default	any

Page 1 of 1 Show 50 items

3. Create an authentication policy group profile and include the rule entry created in Step 2.



Edit Authenitcation Policy Group redirectonAP

General Settings

Profile Name: redirectonAP

Description: redirectonAP (Optional)

Add Edit Remove Move

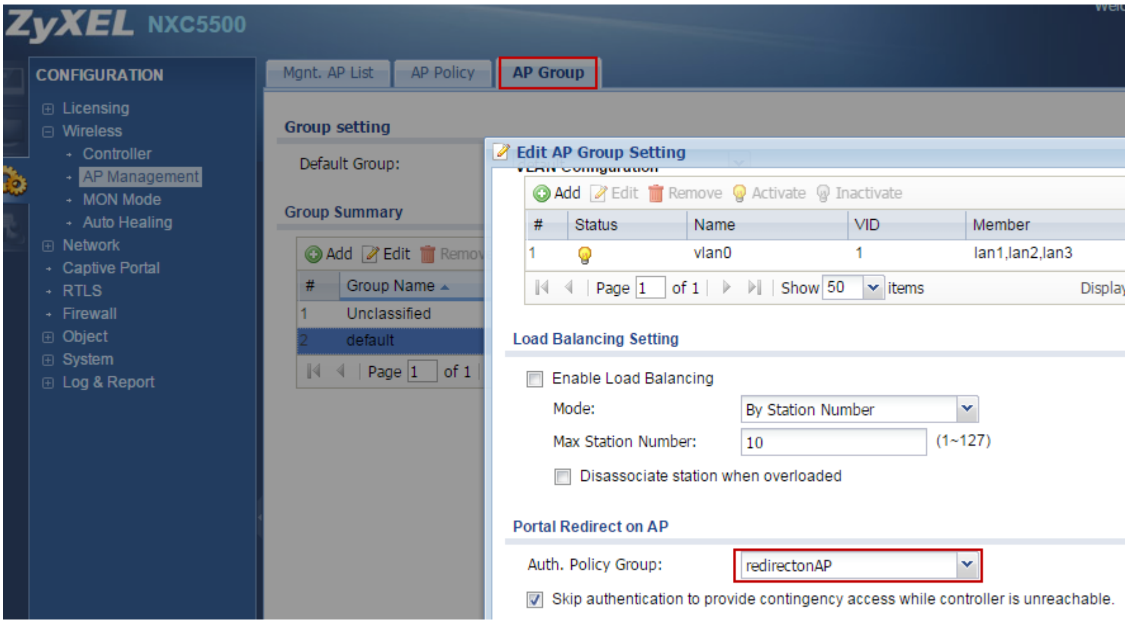
#	Name
1	redirectonAP

Page 1 of 1 Show 50 items Displaying 1 - 1 of 1

Note:
The "default" policy rule will be the last one for each group profile.

OK Cancel

4. Select the policy for the AP group.
   Noted: Portal redirect on the AP still needs the controller to be involved in the authentication flow. If the connection to the controller is lost, there is an option to skip authentication.



Group setting

Default Group:

Group Summary

#	Group Name
1	Unclassified
2	default

Edit AP Group Setting

VLAN Configuration

#	Status	Name	VID	Member
1	💡	vlan0	1	lan1,lan2,lan3

Load Balancing Setting

□ Enable Load Balancing

Mode: By Station Number

Max Station Number: 10 (1~127)

□ Disassociate station when overloaded

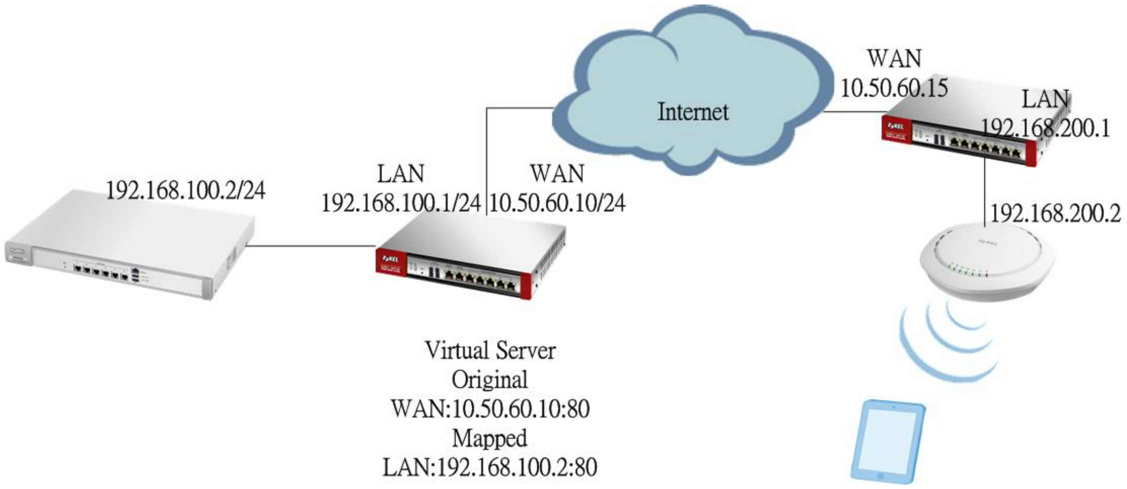
Portal Redirect on AP

Auth. Policy Group: redirectonAP

☑ Skip authentication to provide contingency access while controller is unreachable.

Application Scenario

Topology:



Scenario Description:

The application scenario illustrated a common scenario in chain stores or café where provides hotspot service. In these venues, typically the NXC controller locates at the central site and APs locate in remote sites, and captive portal redirect is configured on the remote AP.

Misconfiguration Case Description:

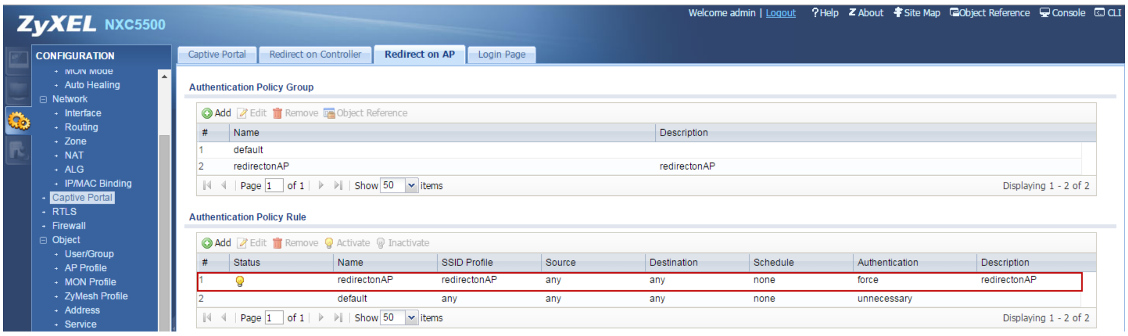
If the controller is behind NAT and its authentication policy rule of redirect on the controller is configured without certain directions (for example, **any** to **any** force authentication), the authentication flow from the AP might require authentication again by the controller's authentication policy while authenticated traffic from the USG enters the controller. This kind of double authentication will cause portal redirect malfunction.

Suggested Solution:

1. Do not enable captive portal redirect on the NXC controller and on the Managed AP simultaneously.
2. Specify a secure source/destination traffic direction for the authentication policy over the controller, and avoid to specify a loose authentication policy such as "**any** to **any** force authentication" to prevent double authentication.

Configuration Example for Suggested Solution 2 :

1. In the **CONFIGURATION** > **Network** > **Captive Portal** > **Redirect on AP** screen, click **Add** in the **Authentication Policy Rule** section to add a new rule. The SSID **redirectonAP** is used as an example. Any client that connects to this SSID will be required to perform authentication.



Authentication Policy Group

#	Name	Description
1	default	
2	redirectonAP	redirectonAP

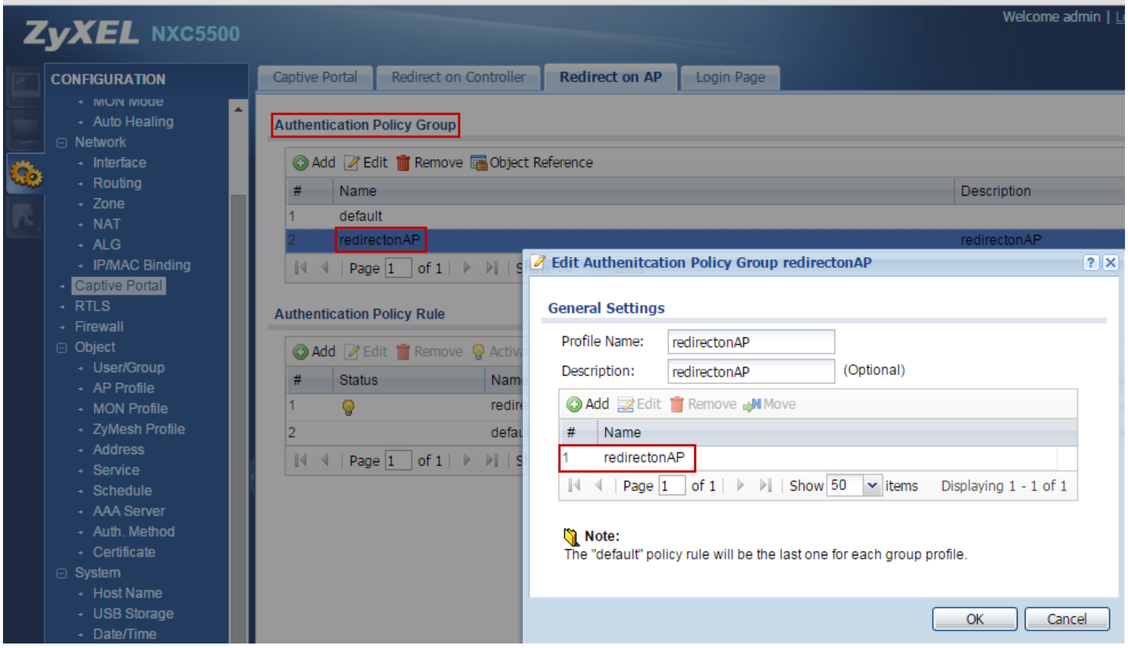
Page 1 of 1 | Show 50 items — Displaying 1 - 2 of 2

Authentication Policy Rule

#	Status	Name	SSID Profile	Source	Destination	Schedule	Authentication	Description
1	●	redirectonAP	redirectonAP	any	any	none	force	redirectonAP
2		default	any	any	any	none	unnecessary	

Page 1 of 1 | Show 50 items — Displaying 1 - 2 of 2

2. Add this authentication policy rule to the **Authentication Policy Group**.



#	Name	Description
1	default	
2	redirectonAP	redirectonAP

Edit Authenitcation Policy Group redirectonAP

General Settings

Profile Name: redirectonAP

Description: redirectonAP (Optional)

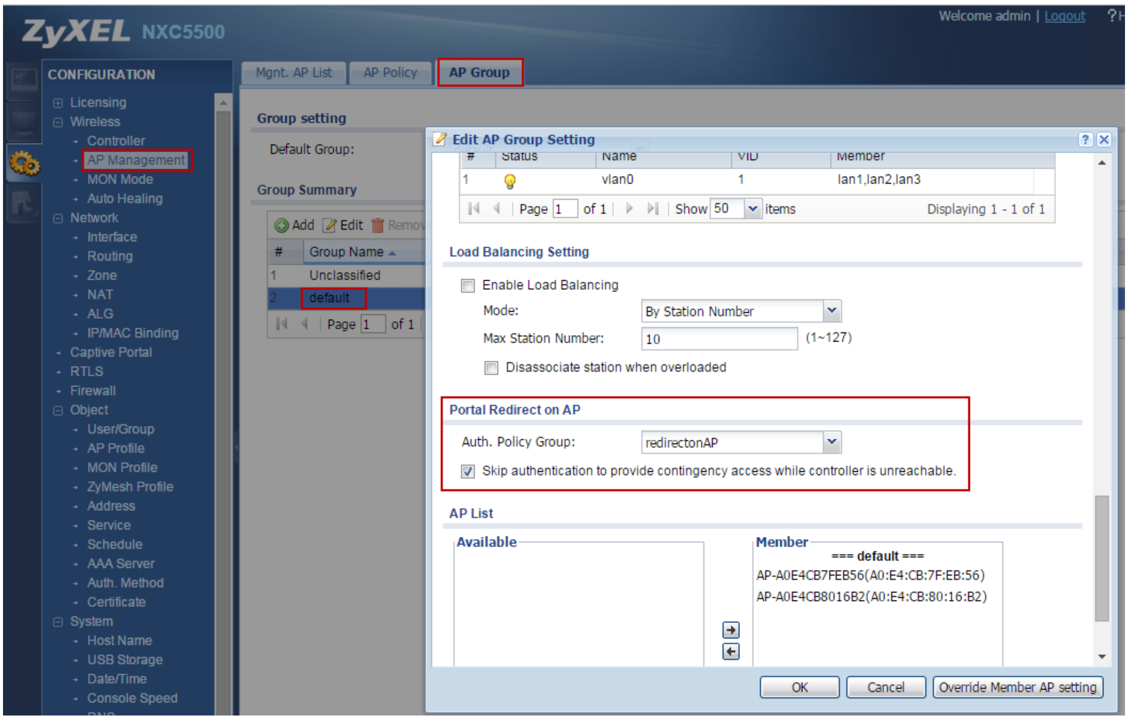
#	Name
1	redirectonAP

Page 1 of 1 Show 50 items Displaying 1 - 1 of 1

Note:
The "default" policy rule will be the last one for each group profile.

3. In the **AP Group** screen, select this authentication policy group in the **Portal Redirect on AP** field.

Note: Select the checkbox below this field to skip authentication when the controller is unreachable.



#	Group Name
1	Unclassified
2	default

Edit AP Group Setting

#	Status	Name	VID	Member
1	●	vlan0	1	lan1,lan2,lan3

Page 1 of 1 Show 50 items Displaying 1 - 1 of 1

Load Balancing Setting

☐ Enable Load Balancing

Mode: By Station Number

Max Station Number: 10 (1~127)

☐ Disassociate station when overloaded

Portal Redirect on AP

Auth. Policy Group: redirectonAP

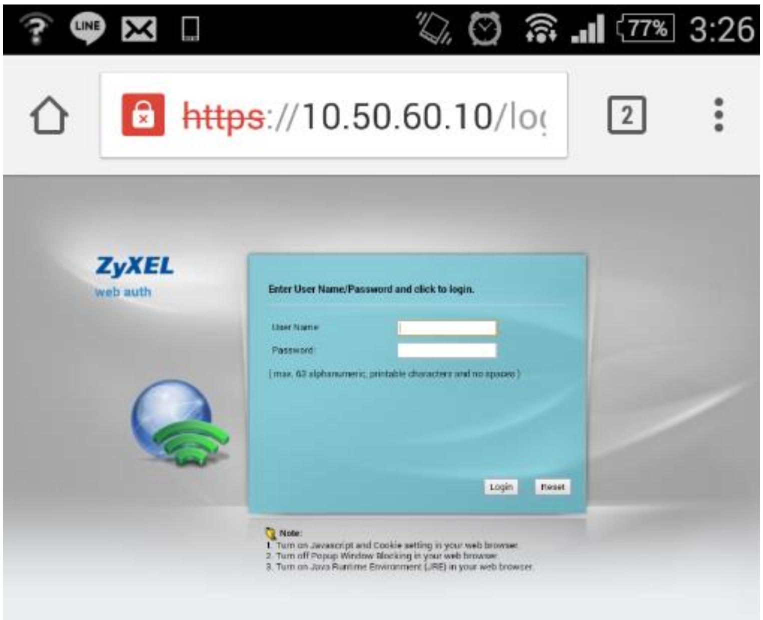
☑ Skip authentication to provide contingency access while controller is unreachable.

AP List

Available

Member
=== default ===
AP-A0E4CB7FEB56(A0:E4:CB:7F:EB:56)
AP-A0E4CB8016B2(A0:E4:CB:80:16:B2)

4. Remote wireless clients can be redirected to the portal login page with the local gateway IP (https://10.50.60.10) while connected to the remote AP.



Enter User Name/Password and click to login.

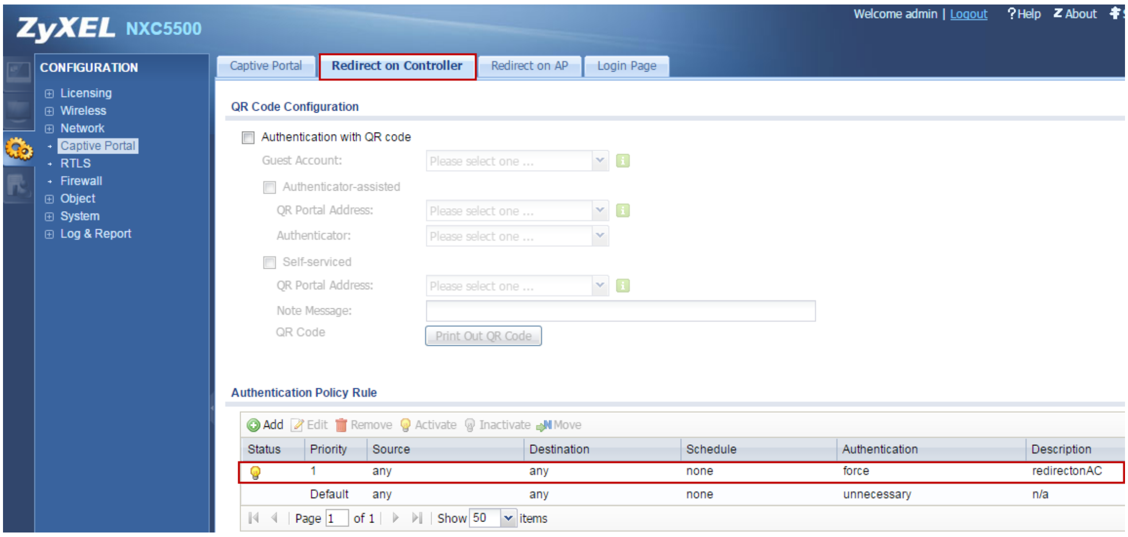
User Name:

Password:

(max. 63 alphanumeric, printable characters and no spaces)

Note:
1. Turn on Javascript and Cookie setting in your web browser.
2. Turn off Popup Window Blocking in your web browser.
3. Turn on Java Runtime Environment (JRE) in your web browser.

5. What if the authentication policy rule is configured without certain directions, such as **any** to **any** force authentication?



QR Code Configuration

□ Authentication with QR code

Guest Account: Please select one ...

□ Authenticator-assisted

QR Portal Address: Please select one ...

Authenticator: Please select one ...

□ Self-serviced

QR Portal Address: Please select one ...

Note Message:

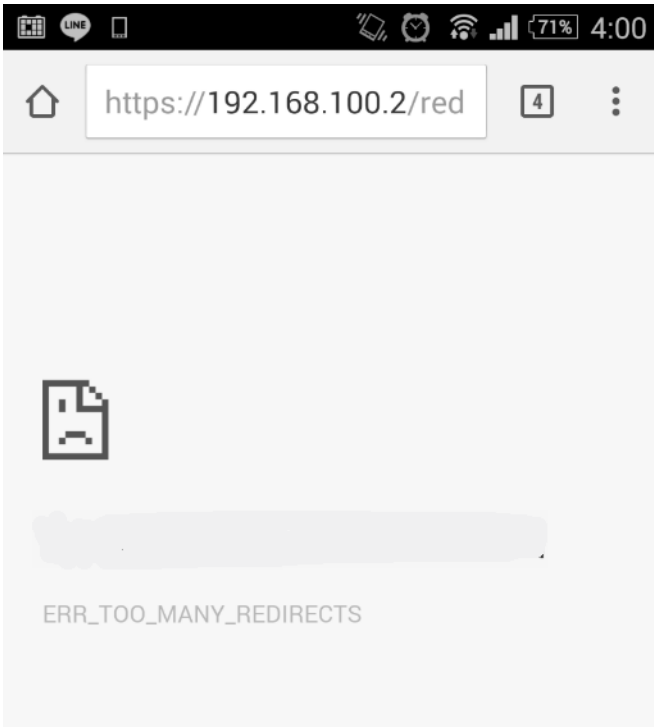
QR Code

Authentication Policy Rule

Status	Priority	Source	Destination	Schedule	Authentication	Description
●	1	any	any	none	force	redirectonAC
	Default	any	any	none	unnecessary	n/a

Page 1 of 1 | Show 50 items

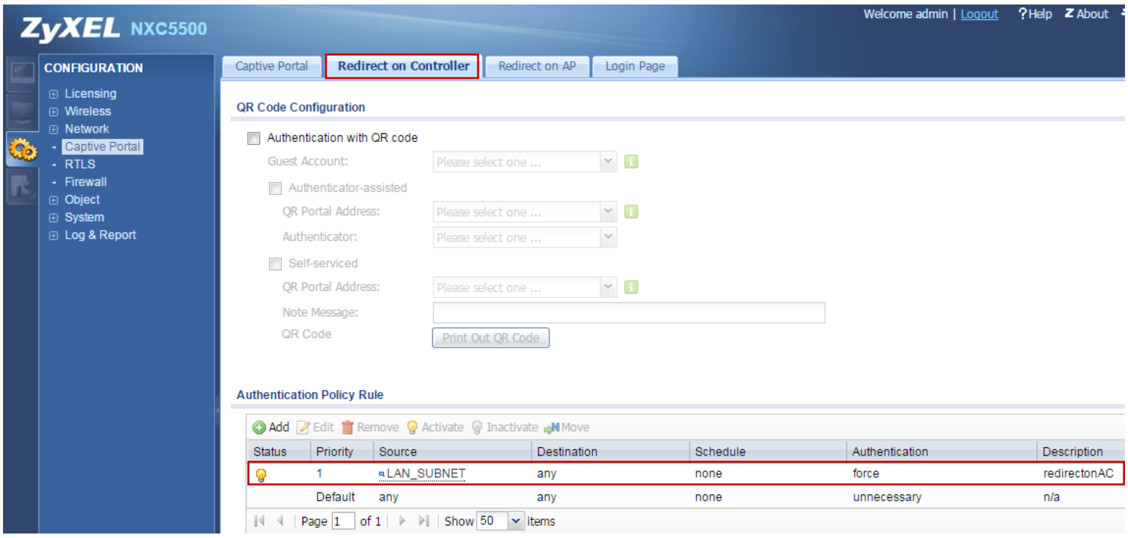
6. The remote wireless clients can't be redirected to the portal login page successfully while connected to the remote AP. The root cause is double web authentication, which causes portal redirection to occur recursively.



https://192.168.100.2/red

ERR_TOO_MANY_REDIRECTS

7. Continuing with step 5, if the authentication policy rule is configured with a certain direction, for example, **LAN_SUBNET** to **any** force authentication, the remote wireless clients can be redirected to the portal login page successfully.



QR Code Configuration

□ Authentication with QR code

Guest Account: Please select one ...

□ Authenticator-assisted

QR Portal Address: Please select one ...

Authenticator: Please select one ...

□ Self-serviced

QR Portal Address: Please select one ...

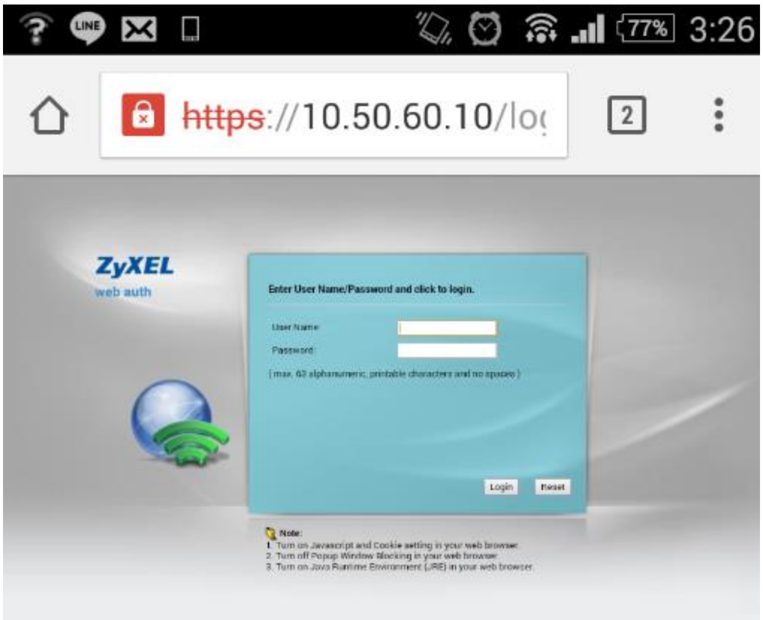
Note Message:

QR Code

Authentication Policy Rule

Status	Priority	Source	Destination	Schedule	Authentication	Description
●	1	LAN_SUBNET	any	none	force	redirectonAC
	Default	any	any	none	unnecessary	n/a

Page 1 of 1 | Show 50 items



Enter User Name/Password and click to login.

User Name:

Password:

(max. 63 alphanumeric, printable characters and no spaces)

Note:

1. Turn on Javascript and Cookie setting in your web browser.
2. Turn off Popup Window Blocking in your web browser.
3. Turn on Java Runtime Environment (JRE) in your web browser.

Conclusion:

Portal redirection on the AP is a new feature for the 11ac generation. The legacy captive portal will be handling all tasks of the controller, which has to process either authentication or data traffic from distributed traffic. 11ac is a new WiFi technology with more throughput than the 11n. To transfer to the 11ac will be a big challenge for the structure of the controller. How to offload the traffic stress on the controller is currently an important issue. ZyXEL's new technology, the Portal Redirect feature on the AP is considered an innovation to separate the authentication traffic and data flow on local site APs. As long as clients pass the captive portal authentication, all the traffic can be unloaded locally to save the remote bandwidth. Thus, the controller's traffic loading is reduced.