# NXC5500/2500

Version 4.21
Edition 1, 11/2015

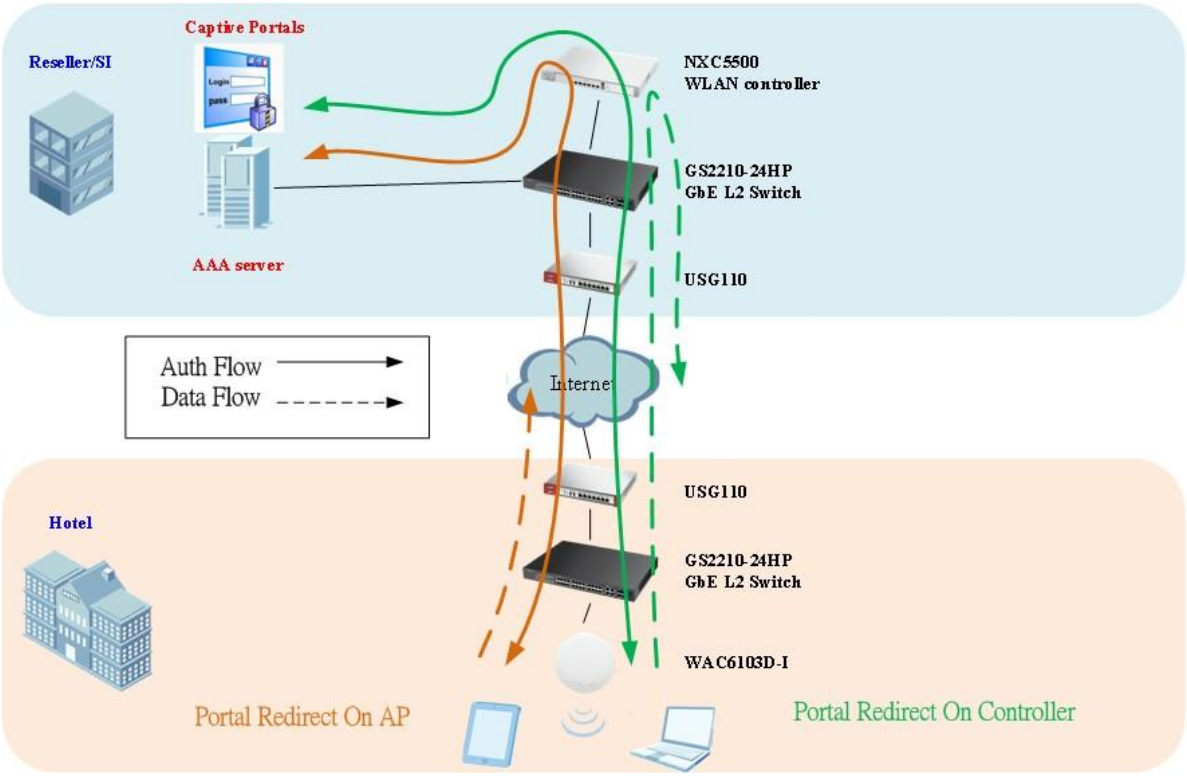
# Application Note

## Portal Redirection on Managed AP

# 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.



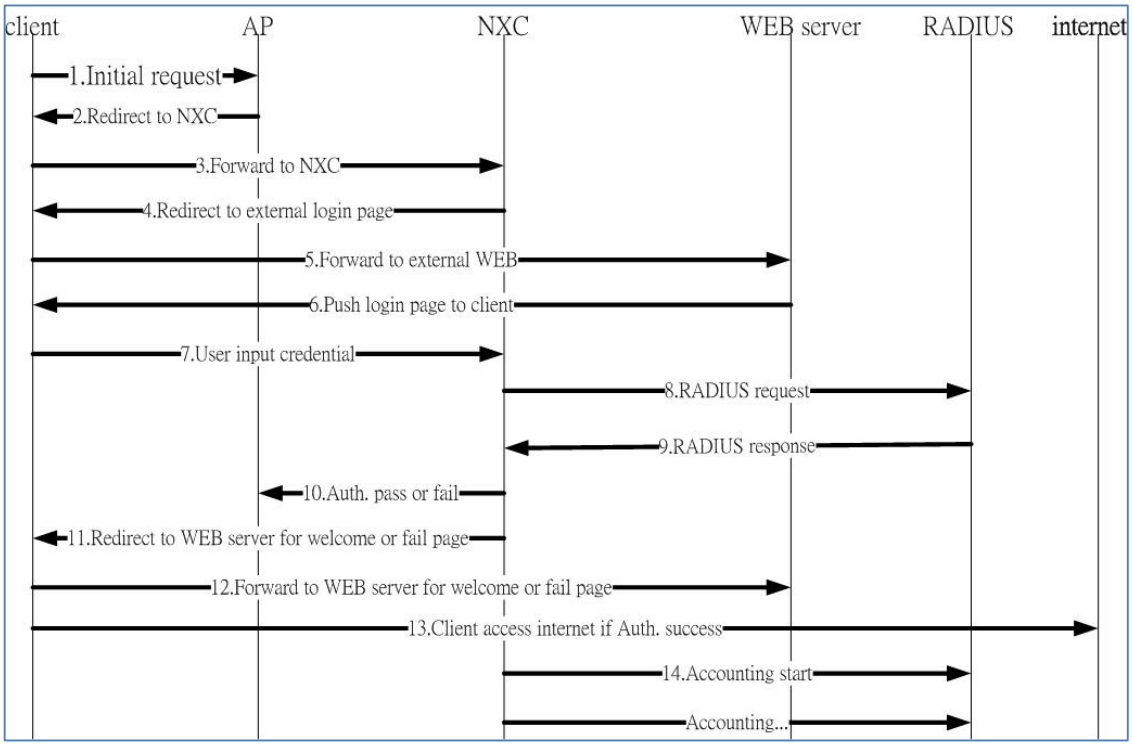

In FW release v4.20, captive portal redirect feature applies on the NXC controller only. From FW v4.21, captive portal redirect on Managed AP is introduced, which enhances network traffic efficiency without tunneling data traffic back to the NXC controller at the central site.

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

## How Does It Work?

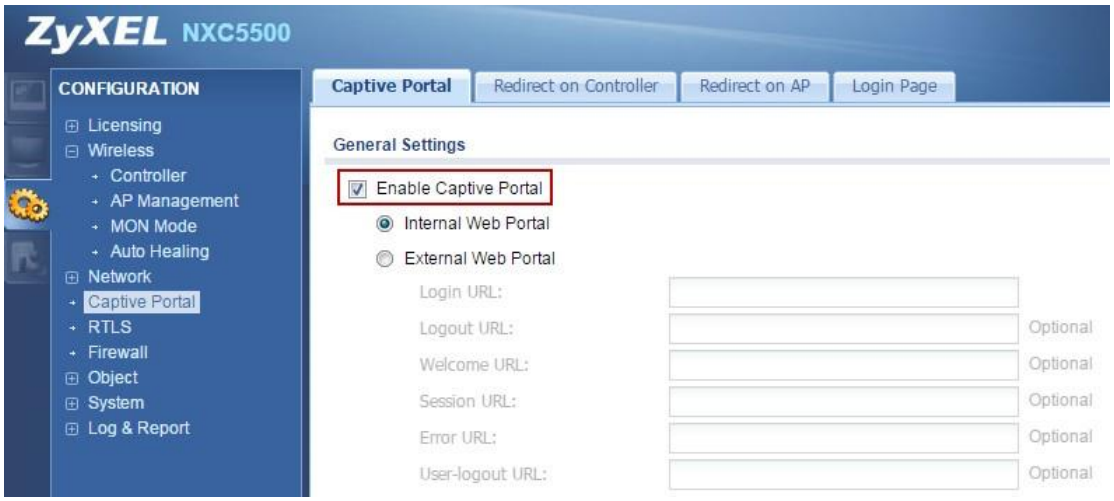
There are two portal redirect modes on the new firmware 4.21: redirect on controller and redirect on AP. Redirect on AP is a new feature to process web authentication over distributed APs to reduce centralized traffic loading on the controller.

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

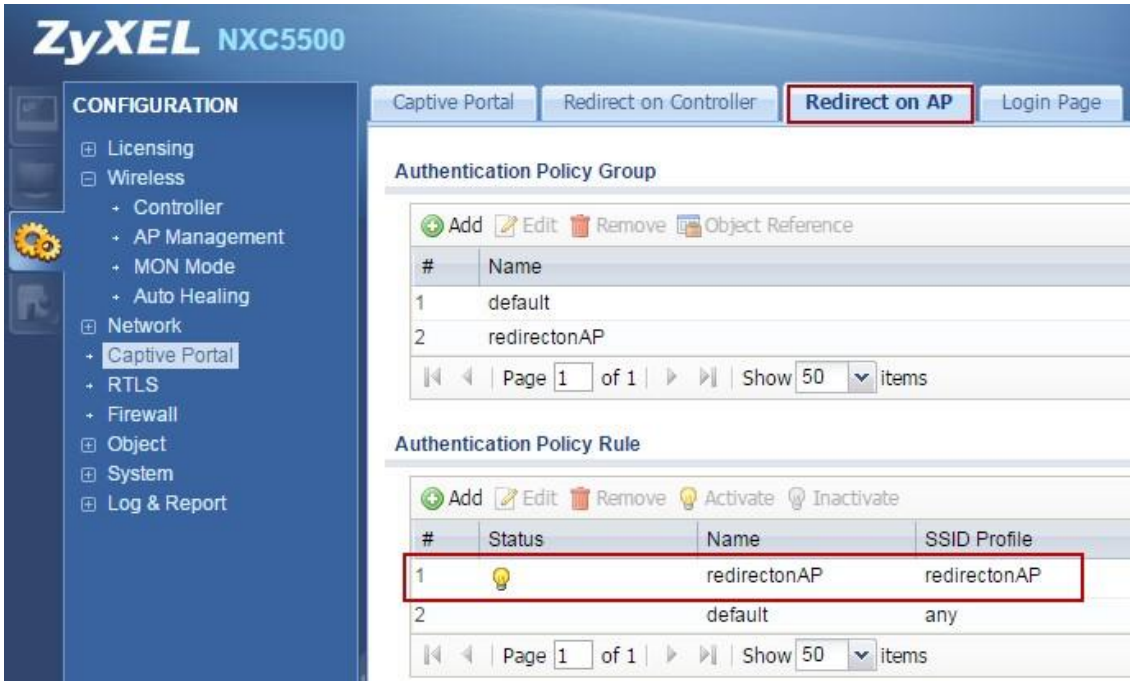



- Fundamental Configuration on GUI

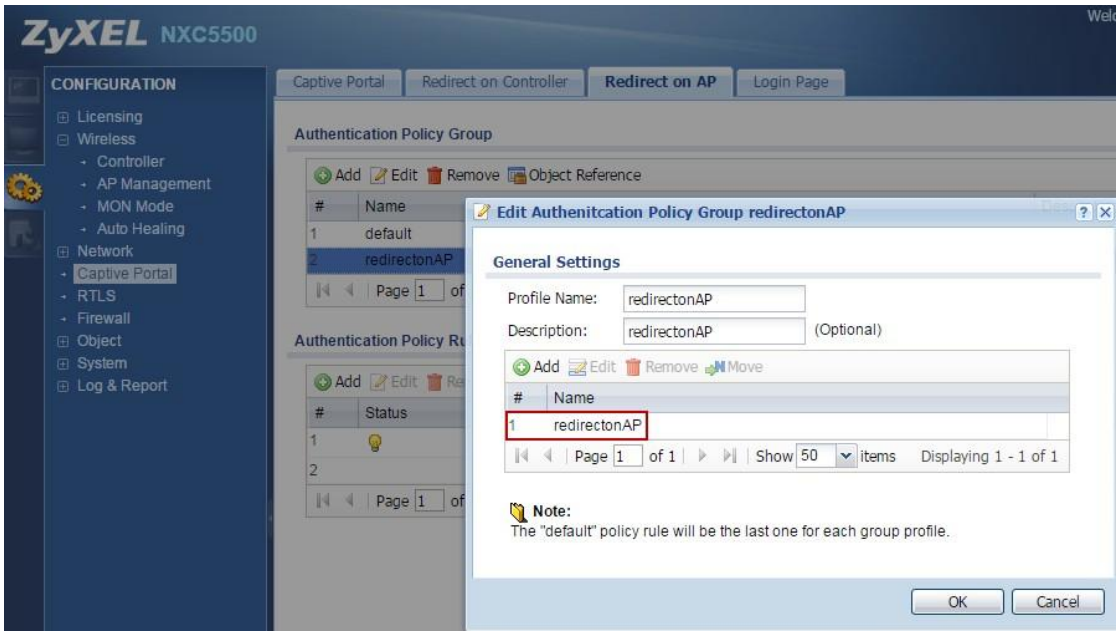
1. In the CONFIGURATION > Network > Captive Portal screen, select Enable Captive Portal.



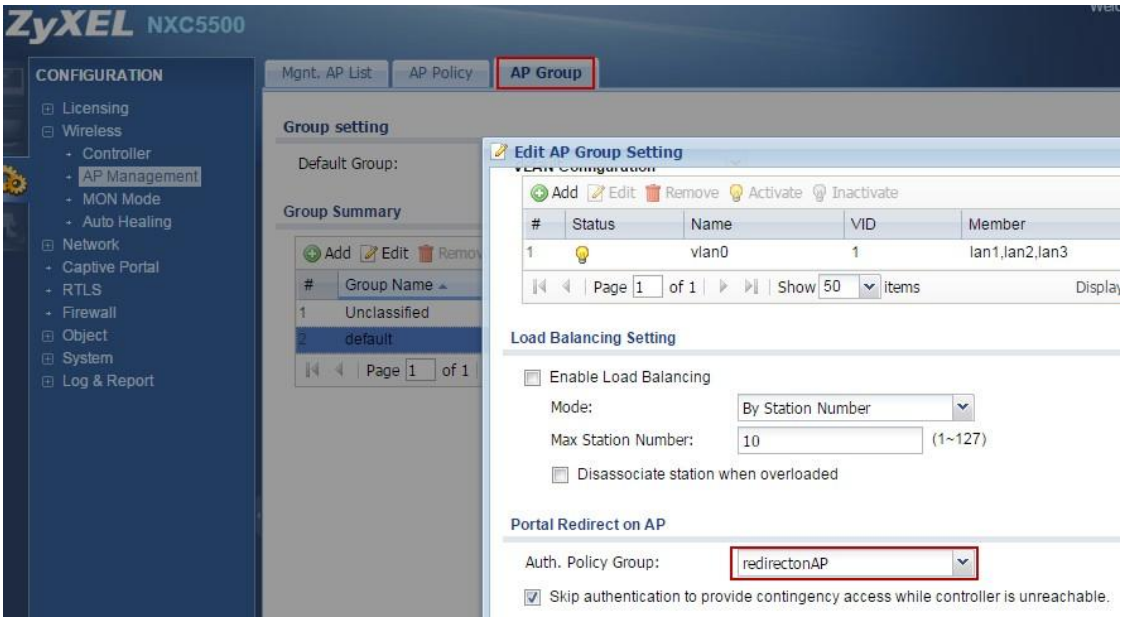
2. Click the Redirect on AP tab and create an Authentication Policy Rule which is an SSID-based policy to filter the traffic from the AP.




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

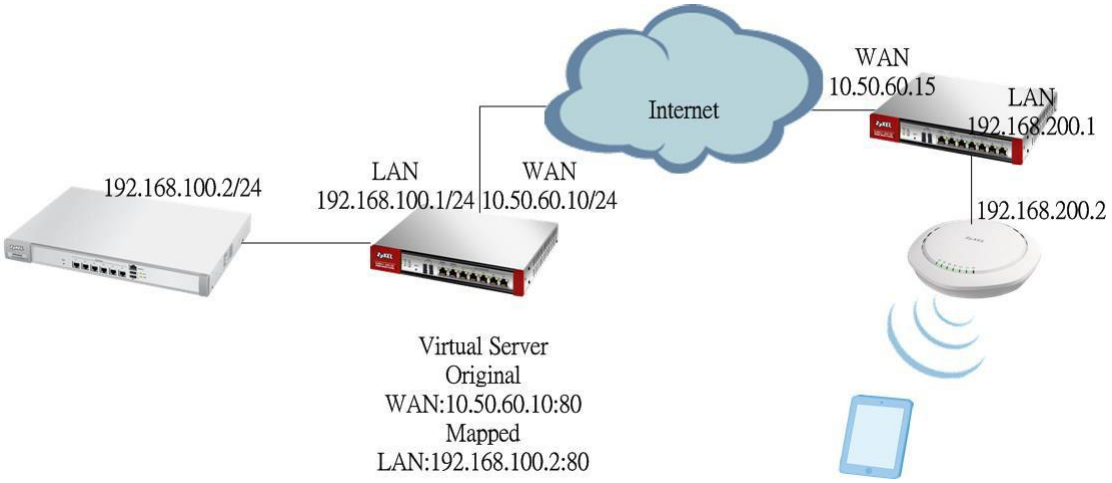


4. Select the policy for the AP group.
   Noted: Portal redirect on the AP still needs the controller to be involved in the authentication flow. If the connection to the controller is lost, there is an option to skip authentication.




## 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:

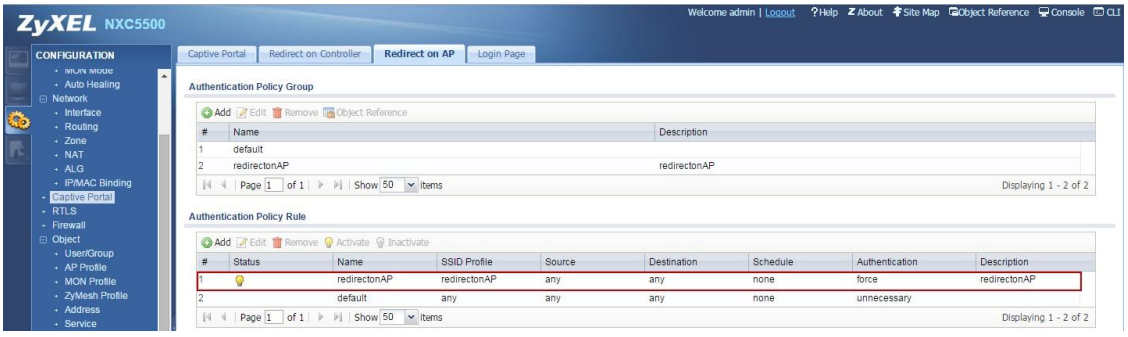
If the controller is behind NAT and its authentication policy rule of redirect on the controller is configured without certain directions (for example, any to any force authentication), the authentication flow from the AP might require authentication again by the controller's authentication policy while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

Suggested Solution:

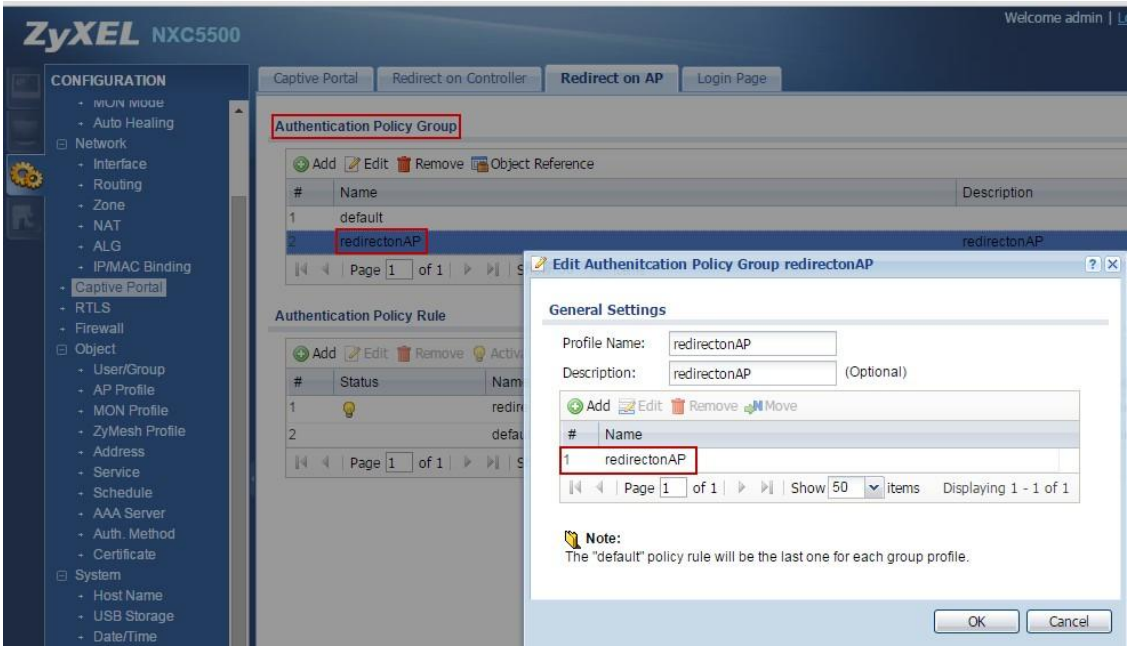
1. Do not enable captive portal redirect on the NXC controller and on the Managed AP simultaneously.
2. Specify a secure source/destination traffic direction for the authentication policy over the controller, and avoid to specify a loose authentication policy such as "any to any force authentication"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

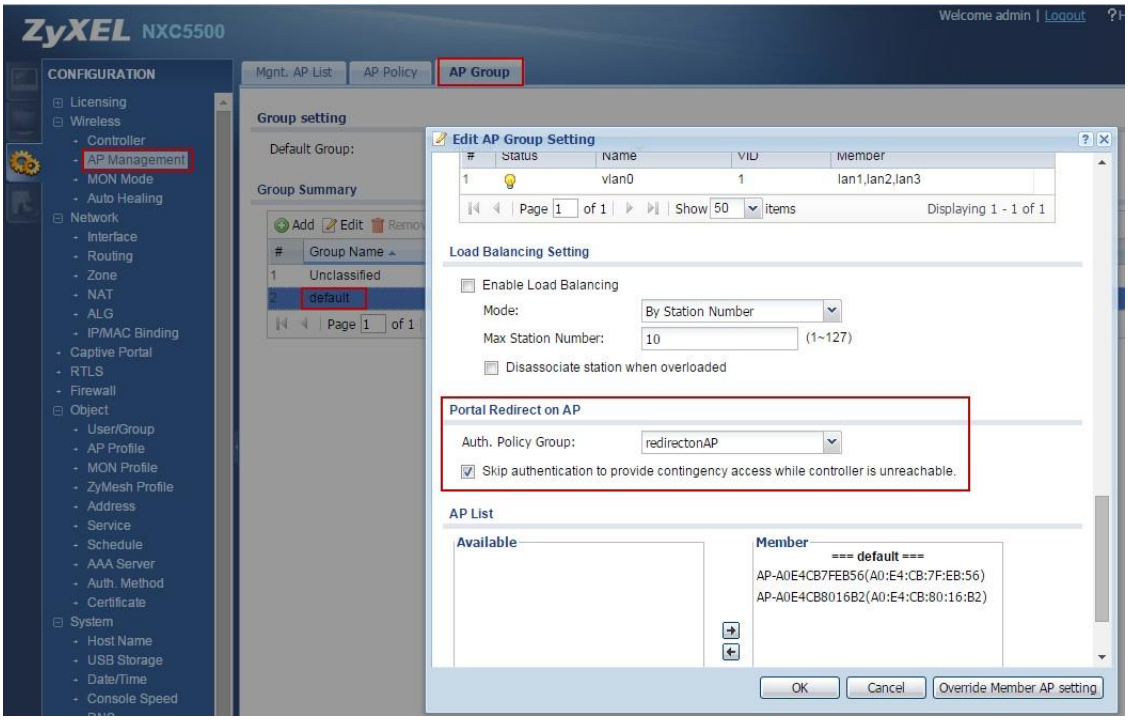


2. Add this authentication policy rule to the Authentication Policy Group.

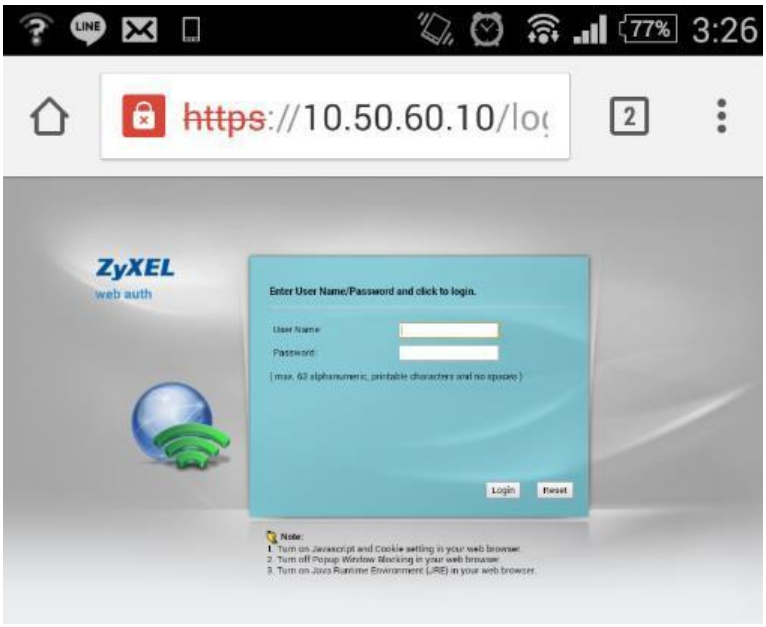



3. In the AP Group screen, select this authentication policy group in the Portal Redirect on AP field.

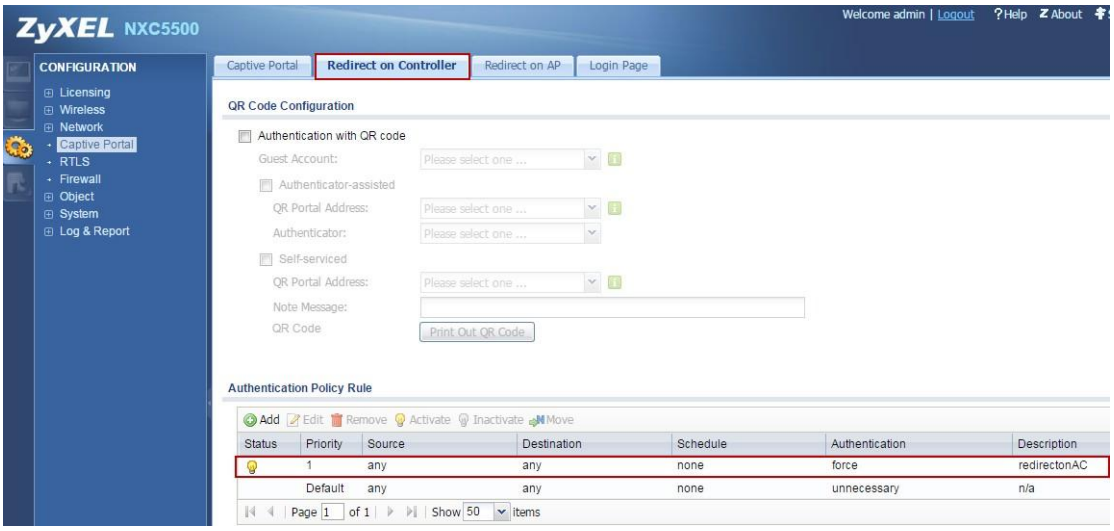
   Note: Select the checkbox below this field to skip authentication when the controller is unreachable.



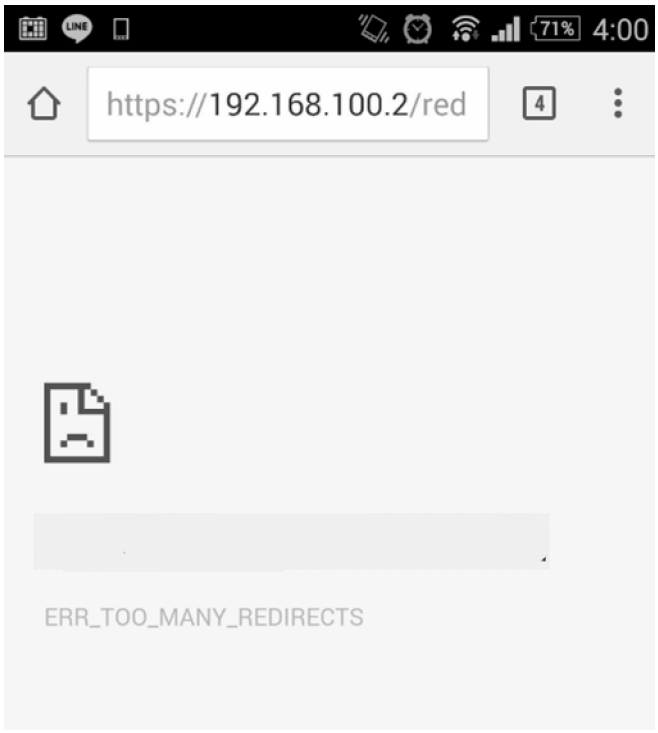
4. Remote wireless clients can be redirected to the portal login page with the local gateway IP (https://10.50.60.10) while connected to the remote AP.



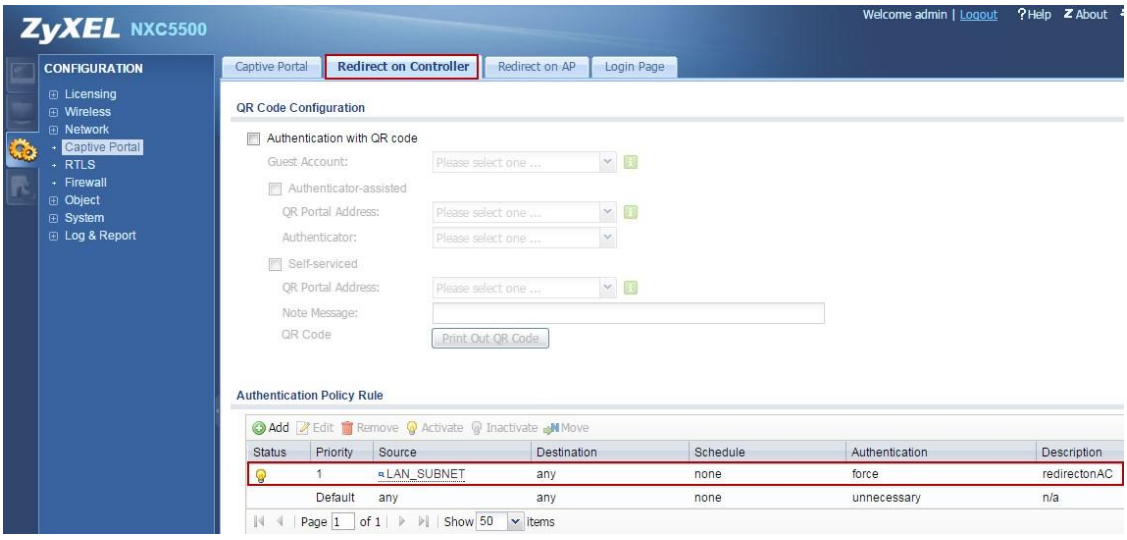

5. What if the authentication policy rule is configured without certain directions, such as any to any force authentication?

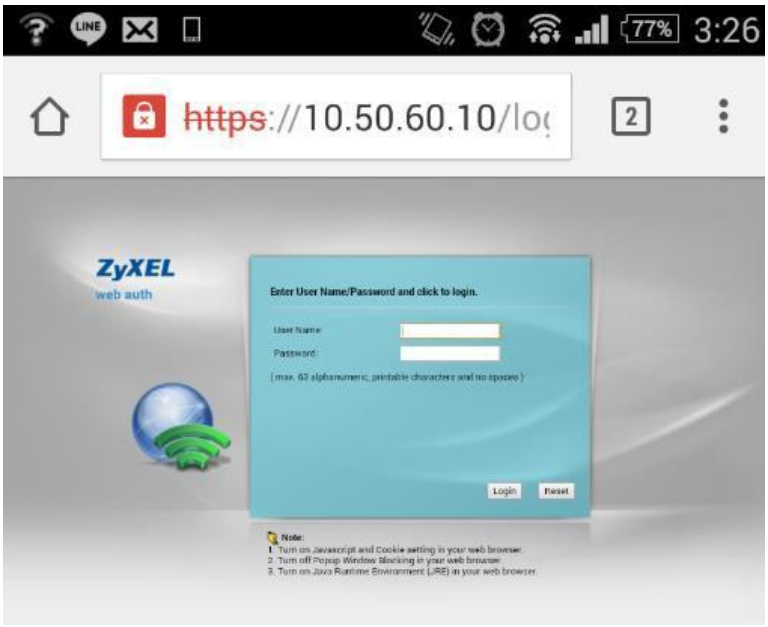


6. The remote wireless clients can't be redirected to the portal login page successfully while connected to the remote AP. The root cause is double web authentication, which causes portal redirection to occur recursively.




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.






## 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.