



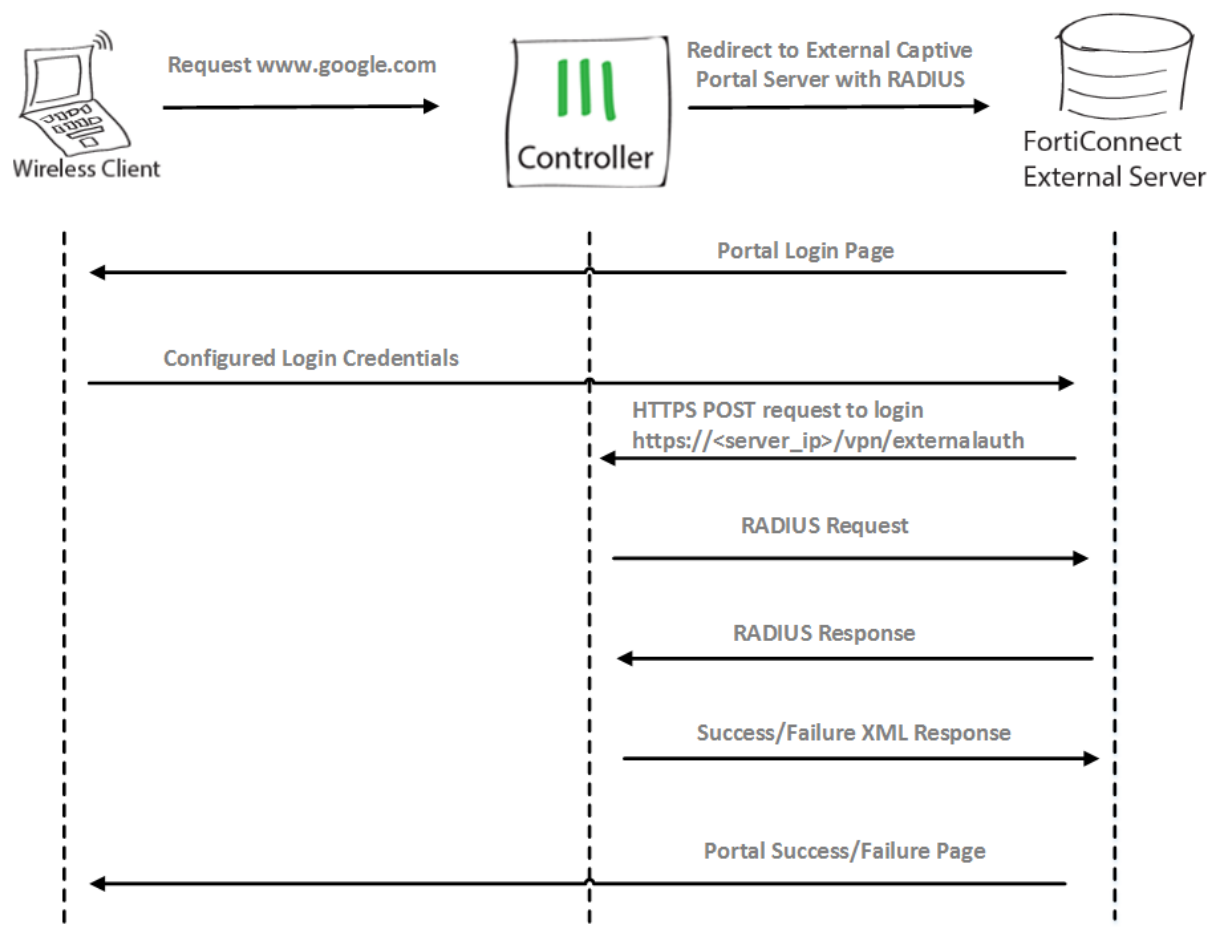
# THE FORTINET COOKBOOK

FortiWLC External Captive Portal

## Contents

Configuring a RADIUS Profile .....	5
Configuring QoS Settings .....	5
Configuring Captive Portal Profile .....	7
Enabling Captive Portal in the Security Profile.....	8
Configuring ESS Profile .....	8

The FortiWLC integrates with several external captive portal solutions like FortiConnect , FortiAuthenticator, and Aruba Clear Pass. The underlying HTTP/HTTPS client redirection mechanism to send unauthenticated traffic to receive the captive portal login page differs with each solution. This document describes an example to configure the FortiWLC external captive portal solution using FortiConnect as the external server. Any third party captive portal solution can be integrated with FortiWLC following this example. For more information on integrating Aruba Clear Pass with FortiWLC, see the *FortiWLC-ClearPass Integration* cookbook.



The controller redirects with GET/POST requests to the configured URL along with following parameters.

POST Variable	Description
<i>Server_IP</i>	The controller's IP address.
<i>Login_url</i>	The login URL format is <b>https://&lt;server_ip&gt;/vpn/externalauth</b> OR <b>https://&lt;server_ip&gt;/vpn/externalapauth</b> in the bridge mode.
<i>Original_url</i>	The original URL requested by the controller.
<i>ssid</i>	The SSID to which the wireless station is connected.
<i>station_mac</i>	The MAC address of the wireless client.
<i>station_ip</i>	The IP address of the wireless client.

The external captive portal server provides the login page to the client after receiving the redirect. After the client enters the login credentials, the external captive portal server sends an HTTPS POST to the controller and passes the following credentials.

POST Variable	Description
<i>POST url</i>	The login URL format is <b>https://&lt;server_ip&gt;/vpn/externalauth</b> OR <b>https://&lt;server_ip&gt;/vpn/externalapauth</b> in the bridge mode.
<i>userid</i>	The user name provided by the client.
<i>password</i>	The password provided by the client.
<i>station_mac</i>	The MAC address of the wireless client.
<i>station_ip</i>	The IP address of the wireless client.

The controller then sends a RADIUS authentication request to the external captive portal server (if it handles RADIUS) or any other configured RADIUS server. The RADIUS authentication result is sent to the external captive portal server as an XML response. The following is an example.

```
#<HTTParty::Response:0x7fb96ee07660
@parsed_response={"external_web_auth"=>{"status"=>"success"}}, @response=#<Net::HTTPOK 200
OK readbody=true>, @headers={"content-type"=>["application/xml; charset=UTF-8"],
"connection"=>["close"], "server"=>["Apache"], "date"=>["Thu, 19 Jun 2014 19:32:41 GMT"],
"content-length"=>["101"]}>
```

Based on the response, the external captive portal server provides the login success/failure page to the client. If the client authentication is successful, the external captive portal server optionally redirects the client to the original URL or a pre-defined URL, and the controller allows all traffic from that client.

## Configuring a RADIUS Profile

Navigate to **Configuration > Security > RADIUS** and create a RADIUS profile each for authentication and accounting.

**RADIUS Profiles - Add**

RADIUS Profile Name\*  
RADIUS-Test1

RADIUS Secret\*  
.....

RADIUS Relay AP-ID  
No Relay AP

Use Client IP as calling station id  
No

COA  
☒

NAS IP

IPSec Phase1 LifeTime in hours  
24

Description

RADIUS Port  
1812

MAC Address Delimiter Calling Station  
Hyphen (-)

Password Type  
Shared Key

RADIUS Server Timeout  
2

RADIUS Server with IPSec  
☐

IPSec Phase2 LifeTime in hours  
8

RADIUS IP\*  
10.33.1.23

Remote RADIUS Server  
☐

MAC Address Delimiter Called Station  
Hyphen (-)

Called-Station-ID Type  
Default

RADIUS Server Retries  
3

IPSec Server X.509 Name Identifier  
\*

NAS Identifier

**RADIUS Profiles - Add**

RADIUS Profile Name\*  
RADIUS-Test2

RADIUS Secret\*  
.....

RADIUS Relay AP-ID  
No Relay AP

Use Client IP as calling station id  
No

COA  
☒

NAS IP

IPSec Phase1 LifeTime in hours  
24

Description

RADIUS Port  
1813

MAC Address Delimiter Calling Station  
Hyphen (-)

Password Type  
Shared Key

RADIUS Server Timeout  
2

RADIUS Server with IPSec  
☐

IPSec Phase2 LifeTime in hours  
8

RADIUS IP\*  
10.33.1.23

Remote RADIUS Server  
☐

MAC Address Delimiter Called Station  
Hyphen (-)

Called-Station-ID Type  
Default

RADIUS Server Retries  
3

IPSec Server X.509 Name Identifier  
\*

NAS Identifier

## Configuring QoS Settings

Navigate to **Configuration > Policies > QoS > QoS and Firewall Rules** and configure the QoS and Firewall rules to allow pre-authentication traffic to the external captive portal server.

Ensure that the **Match** option is enabled for the configured fields.

QoS and Firewall Rules - Add ?

ID*	2020
Destination IP	10.33.1.23
Destination Netmask	255.255.255.255
Destination Port	443
Source IP	0
Source Netmask	0
Source Port	0
Network Protocol	6
Firewall Filter ID	ab10

Match
<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>
<input type="checkbox"/>
<input type="checkbox"/>
<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>

QoS and Firewall Rules - Add ?

ID*	2021
Destination IP	0
Destination Netmask	0
Destination Port	0
Source IP	10.33.1.23
Source Netmask	255.255.255.240
Source Port	443
Network Protocol	6
Firewall Filter ID	ab10

Match
<input type="checkbox"/>
<input type="checkbox"/>
<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>

## Configuring Captive Portal Profile

Navigate to **Configuration > Security > Captive Portal** to specify the captive portal profile settings.

The following screen-shots illustrate the process to create and assign a captive profile with FortiConnect as the external server.

Add Captive Portal Profile

CP Name\*

External-captive-portal

User Authentication

Authentication Type

radius

Radius Authentication

Primary Authentication

RADIUS-Test1

Secondary Authentication

dummy1

Radius Accounting

Primary Accounting

RADIUS-Test2

Secondary Accounting

dummy2

Accounting Interim Interval

600

External Portal Settings

External Server

Fortinet-Connect

External Portal URL

https://10.33.1.23/portal/172.24.0.2?meruInitialRe

Public IP of Controller

172.24.0.2

### Note:

The format of the external portal URL for FortiConnect is *https://<External-CP domain name>/portal/<controllerPublicIPAddress>?meruInitialRedirect*  
Configure the portal URL accordingly when using a third-party external server.

## Enabling Captive Portal in the Security Profile

The captive portal profile must be enabled in the security profile.

Security Profiles - Add ?

Security Profile Name\*  
security-test

Security Settings

Online Sign Up  
not-configured

Security Mode\*  
Open

Captive Portal Settings

Captive Portal  
WebAuth

Captive Portal profile  
External-captive-portal

Captive Portal AP Offload  
Disable

Captive Portal Authentication Method  
external

Passthrough Firewall Filter ID  
ab10

**Note:** In the **Passthrough Firewall Filter ID**, enter a firewall filter ID that was created using **Configuration > Qos > System Settings > QoS and Firewall Rules**.

## Configuring ESS Profile

Navigate to **Configure > Wireless > ESS** to create an ESS profile and add the captive portal enabled security profile.

ESS Profiles - Add ?

ESS Profile\*  
ESS-test

Enable/Disable  
☒

SSID  
SSIDAb

Security Profile  
security-test

Essid Type

Essid Type  
Regular

Backup ESS Profile  
No Backup ESS

Timer Profile  
No TIMER

Primary RADIUS Accounting Server  
Corp-Radius

Secondary RADIUS Accounting Server  
CorpGuestRadauth

Accounting Interim Interval (seconds)  
3600

Reconnect Primary Server (minutes)  
10

IPv6 Forwarding  
☐