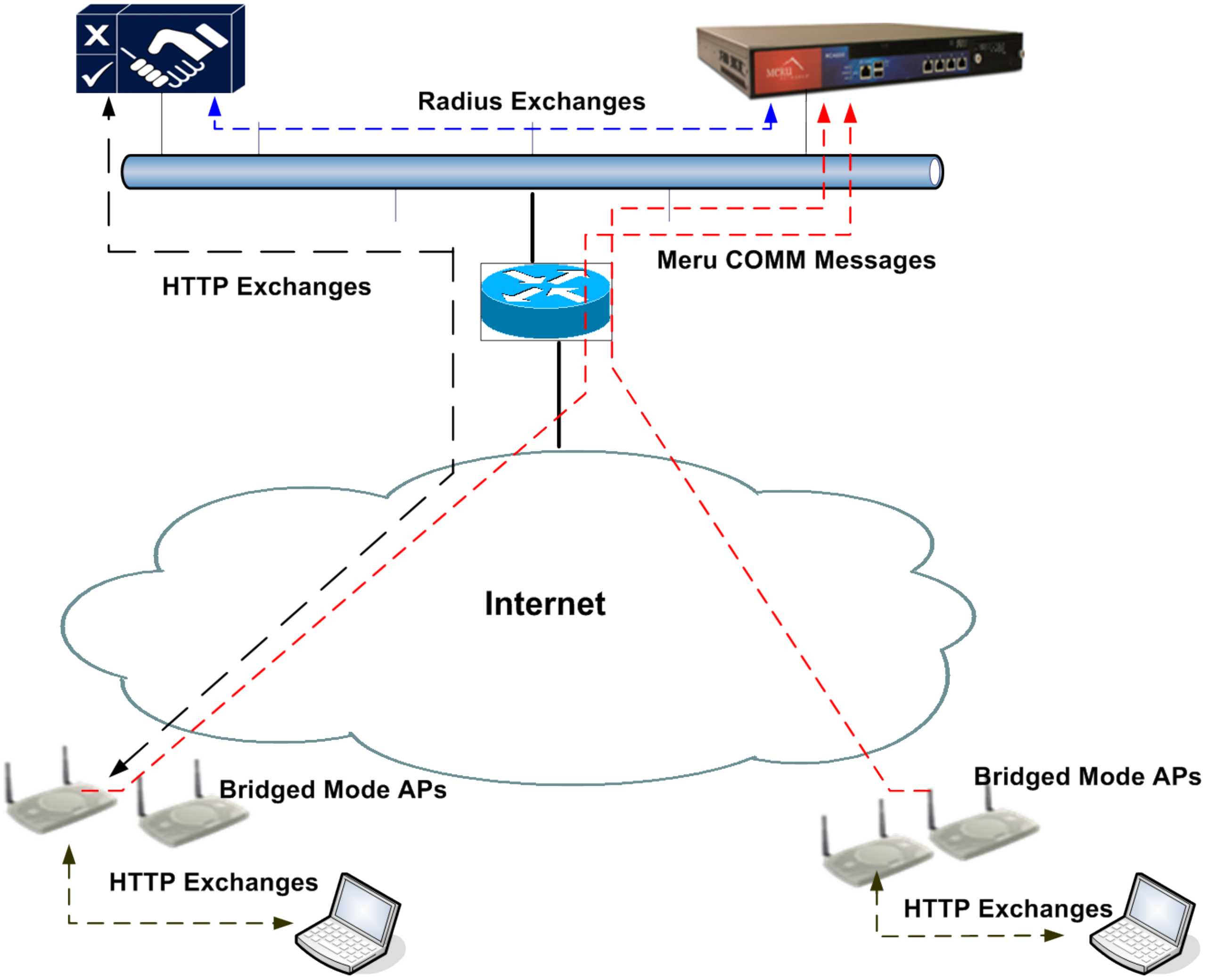
Bridge Mode Captive Portal

Introduction

With SD 6.0 the Meru APs will be able to provide Captive Portal authentication on bridged mode SSID's. The feature is similar to the tunneled mode operation, but the traffic is intercepted locally by the AP before user authentication. When a user connected to a Guest SSID, opens a web browser the request will be redirected to a Captive Portal page hosted by the controller or to an external device like Meru Identity Manager. After successful authentication, the Guest user will be given network / Internet access by the AP. The APs are compatible with external RADIUS guest access provisioning systems such as IDM to provide a paid hot-spot feature to meet enterprise business requirements. This feature helps to provide Guest access in geographically dispersed remote branch offices with controller placed in the centralized location. This guide discusses the various aspects of Bridged Captive portal deployment scenarios and explains the necessary configuration requirements.

Figure 1 illustrates Captive Portal in Bridged Mode.

.



System Requirements

For bridged mode Captive Portal, you will need:

- System Director Release 6.0-2-0 or later.
- AP Models : AP110, AP10xx, AP332, AP832, AP400

Internal Captive Portal

By using the internal captive portal feature, the AP redirects guest user to the controller hosted default captive portal Page. Customized Captive Portal Pages are also supported by the APs in bridged mode. The Guest user Database is maintained in the controller and the AP forwards the user credentials to controller for validation. After successful authentication by the controller, the guest users are redirected to the originally requested URL.

Figure 2: The Internal Captive Portal redirection with local user database maintained in controller.

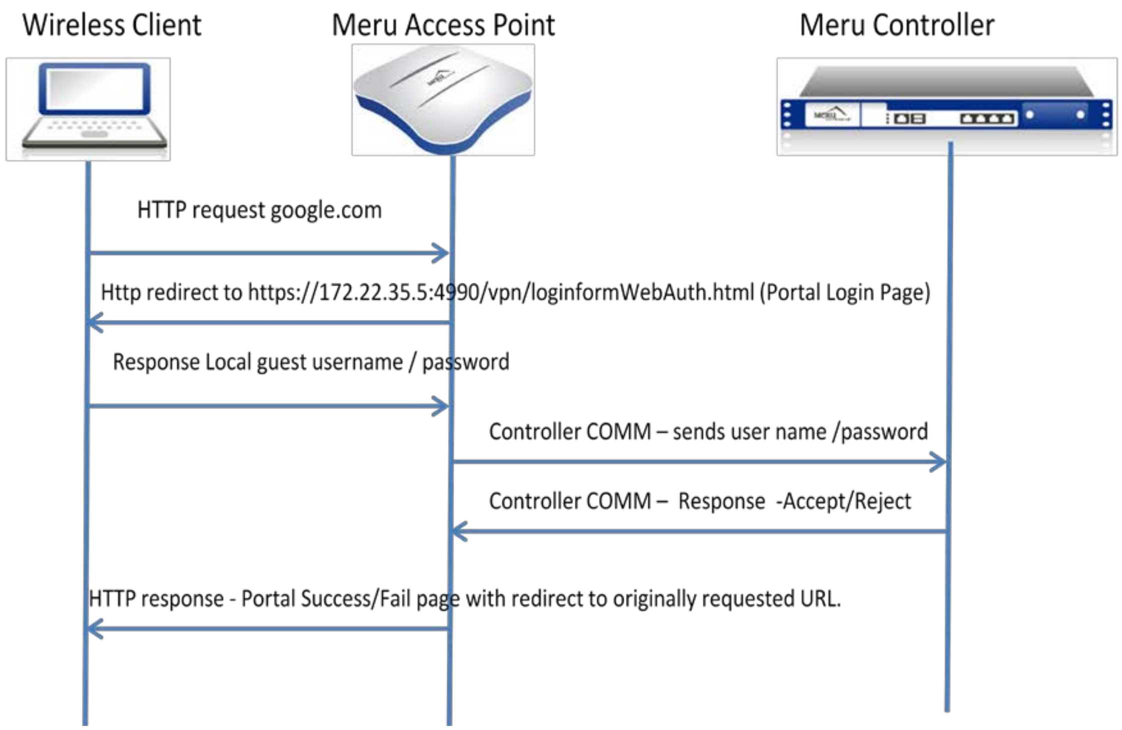
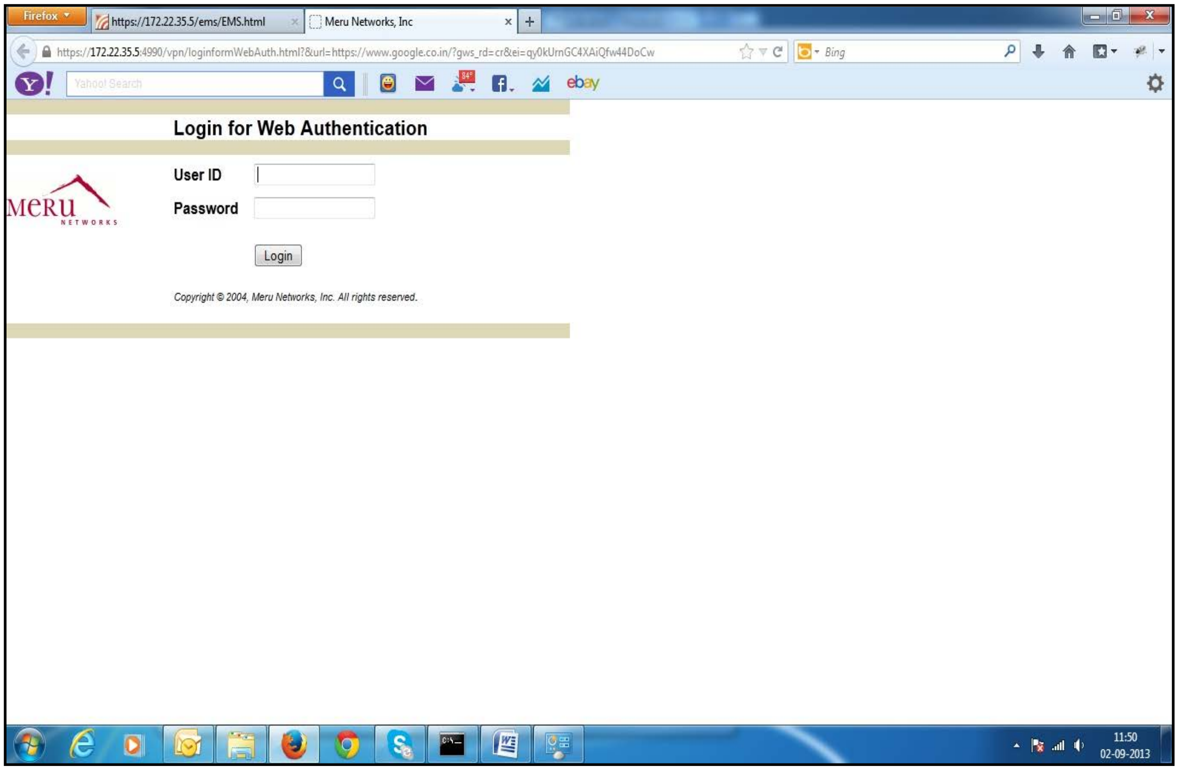

Wireless Client
Meru Access Point
Meru Controller
HTTP request google.com
Http redirect to https://172.22.35.5:4990/vpn/loginformWebAuth.html (Portal Login Page)
Response Local guest username / password
Controller COMM – sends user name /password
Controller COMM – Response -Accept/Reject
HTTP response - Portal Success/Fail page with redirect to originally requested URL.

Figure 3: The controller hosted default Captive portal Page.



Firefox
https://172.22.35.5/ems/EMS.html
Meru Networks, Inc
https://172.22.35.5:4990/vpn/loginformWebAuth.html?&url=https://www.google.co.in/?gws_rd=cr&ei=qy0kUrnGC4XAiQfw44DoCw
Bing
Yahoo! Search
ebay
MERU NETWORKS
11:50
02-09-2013

Login for Web Authentication

User ID

Password

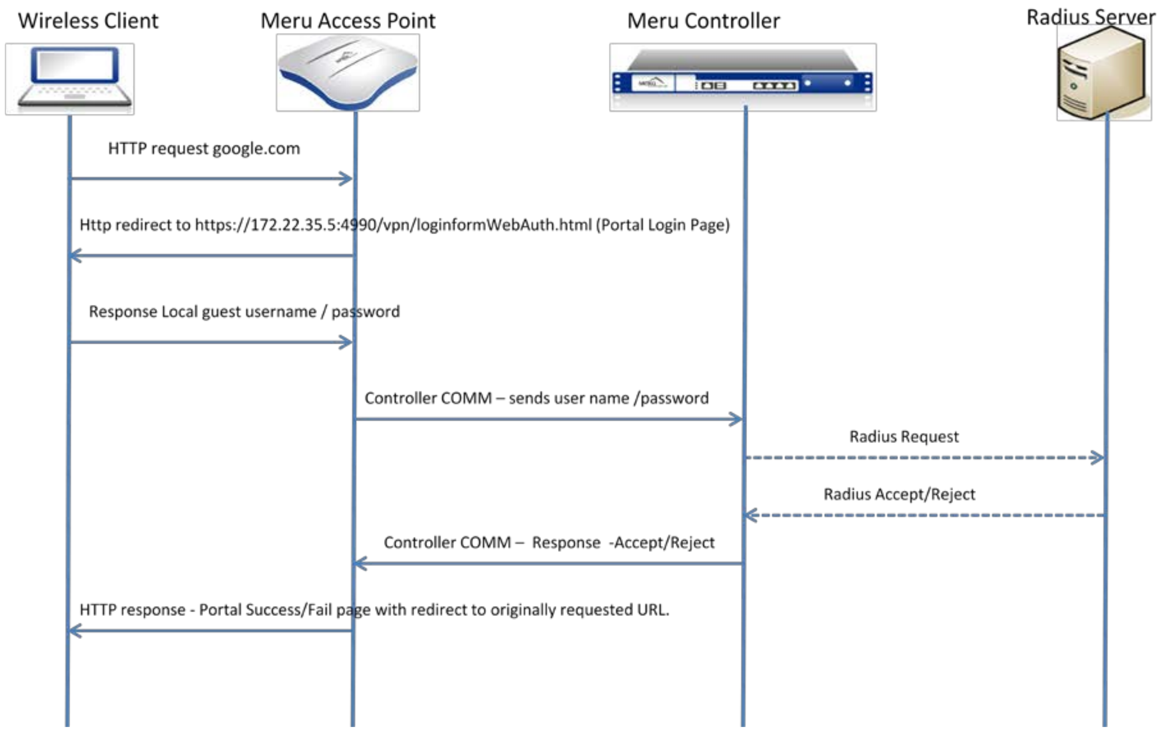
Login

Copyright © 2004, Meru Networks, Inc. All rights reserved.

Internal Captive Portal with Radius

User authentication can also be achieved using RADIUS for Internal Captive Portal. All Captive Portal configuration requirements remain same as compared to the above section, except having Radius profiles configured for authentication and accounting.

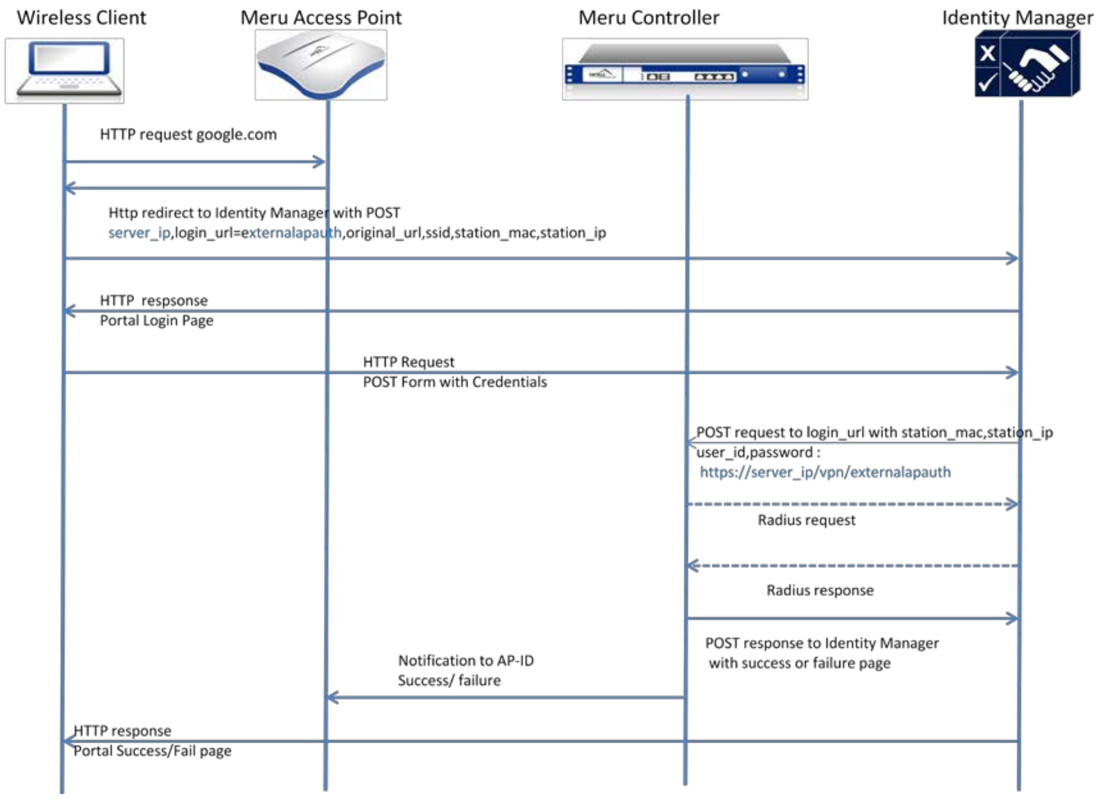
Figure4: The Internal Captive Portal redirection with RADIUS authentication.


Wireless Client
Meru Access Point
Meru Controller
Radius Server
HTTP request google.com
Http redirect to https://172.22.35.5:4990/vpn/loginformWebAuth.html (Portal Login Page)
Response Local guest username / password
Controller COMM – sends user name /password
Radius Request
Radius Accept/Reject
Controller COMM – Response -Accept/Reject
HTTP response - Portal Success/Fail page with redirect to originally requested URL.

External Captive Portal (IDM)

The provisioning of Captive portal pages and user authentication is handled by an external Guest management solution like Identity Manager. An external Captive Portal URL configured in the Controller redirects guest user to the portals defined in the external system. Additional configuration requirements for this feature are explained later in this document.

Figure5: The External Captive redirection with Identity Manager.


Wireless Client
Meru Access Point
Meru Controller
Identity Manager
HTTP request google.com
Http redirect to Identity Manager with POST
server_ip,login_url=externalapauth,original_url,ssid,station_mac,station_ip
HTTP respsonse
Portal Login Page
HTTP Request
POST Form with Credentials
POST request to login_url with station_mac,station_ip
user_id,password :
https://server_ip/vpn/externalapauth
Radius request
Radius response
POST response to Identity Manager
with success or failure page
Notification to AP-ID
Success/ failure
HTTP response
Portal Success/Fail page

Roaming with Captive Portal

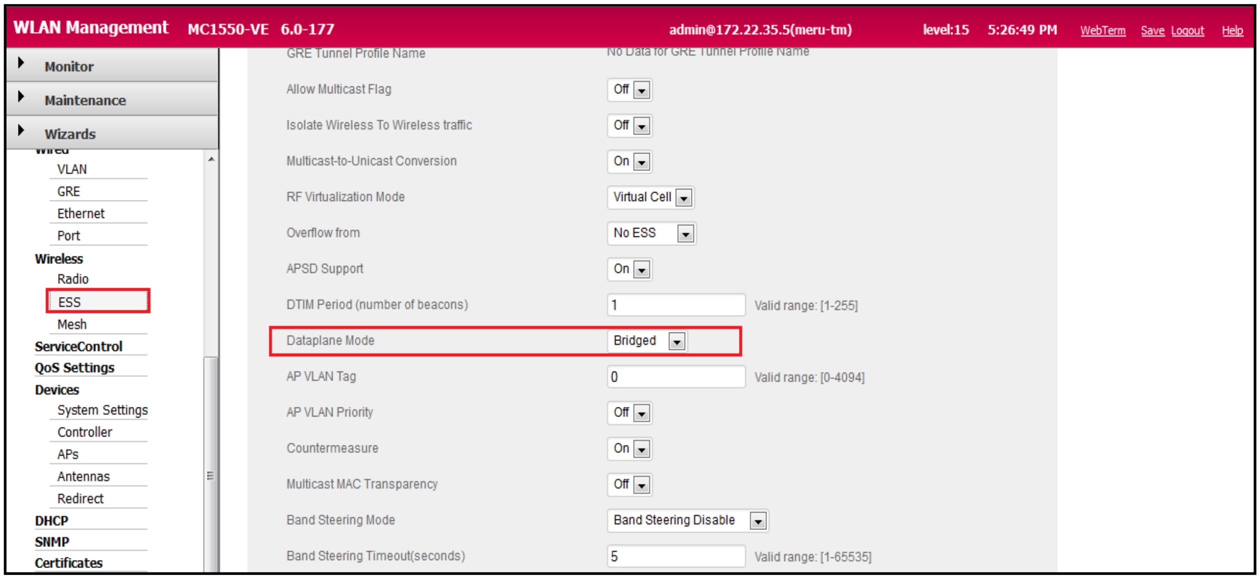
Captive Portal in Bridge mode is supported in all RF virtualization modes. In V-Cell/V-port deployments, client authentication status is included in the hand-off messages so that a station does not go through captive portal authentication once roamed to a new AP.

L3 User Session time-out is a configurable parameter which is maintained in the controller to preserve the Captive Portal Session of clients. A client which has to go through a hard hand-off in a Native Cell deployment scenario or if there is am L2 re-association, it will be prompted with the Captive Portal page only if the L3 User session time-out is expired.

Configuration Tasks

Enable Bridged mode in an ESS by choosing the Dataplane mode as Bridged.

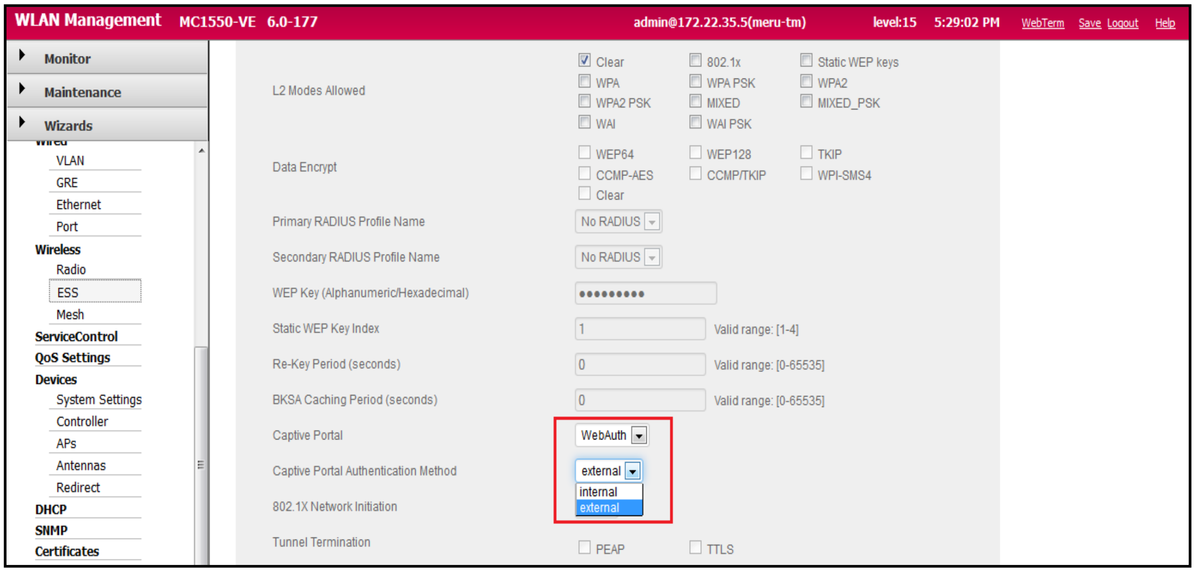
Figure 6 : ESS profile Configuration



GRE Tunnel Profile Name	No Data for GRE Tunnel Profile Name	
Allow Multicast Flag	Off	
Isolate Wireless To Wireless traffic	Off	
Multicast-to-Unicast Conversion	On	
RF Virtualization Mode	Virtual Cell	
Overflow from	No ESS	
APSD Support	On	
DTIM Period (number of beacons)	1	Valid range: [1-255]
Dataplane Mode	Bridged	
AP VLAN Tag	0	Valid range: [0-4094]
AP VLAN Priority	Off	
Countermeasure	On	
Multicast MAC Transparency	Off	
Band Steering Mode	Band Steering Disable	
Band Steering Timeout(seconds)	5	Valid range: [1-65535]

Figure 7: Security Profile configuration

In the security Profile which is mapped to the above ESS, enable WebAuth and choose the Captive Portal Authentication Method to be internal or external



L2 Modes Allowed	☑ Clear ☐ WPA ☐ WPA2 PSK ☐ WAI	☐ 802.1x ☐ WPA PSK ☐ MIXED ☐ WAI PSK ☐ Static WEP keys ☐ WPA2 ☐ MIXED_PSK
Data Encrypt	☐ WEP64 ☐ CCMP-AES ☐ Clear	☐ WEP128 ☐ CCMP/TKIP ☐ TKIP ☐ WPI-SMS4
Primary RADIUS Profile Name	No RADIUS	
Secondary RADIUS Profile Name	No RADIUS	
WEP Key (Alphanumeric/Hexadecimal)	●●●●●●●●●	
Static WEP Key Index	1	Valid range: [1-4]
Re-Key Period (seconds)	0	Valid range: [0-65535]
BKSA Caching Period (seconds)	0	Valid range: [0-65535]
Captive Portal	WebAuth	
Captive Portal Authentication Method	external internal external	
802.1X Network Initiation		
Tunnel Termination	☐ PEAP	☐ TTLS

Figure 8 : Captive Portal Configuration

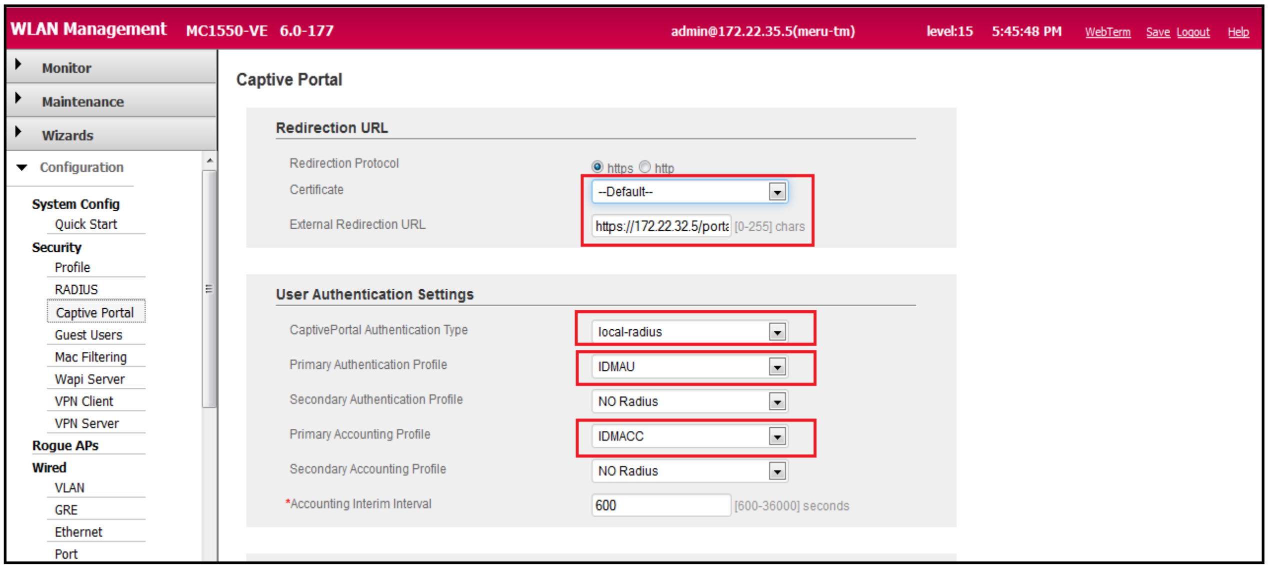
1) If external WebAuth is selected in the Security Profile, define the External redirection URL under Configuration →Captive Portal in the UI.

With IDM, the URL format would be https://<idm-ip or hostname>/portal/<controller-ip or hostname>?MeruInitialRedirect

If any certificates are used, ensure that the hostname defined for the controller matches the CN in the certificate.

2) Select the captive portal authentication type from the 3 available options, local, RADIUS, and local-radius. For External Captive Portal, the authentication type should be RADIUS and for Internal Captive Portal it can be either local or local-radius.

3) If using RADIUS, map the configured radius profiles for authentication and accounting respectively.



Captive Portal

Redirection URL

Redirection Protocol ● https ○ http

Certificate --Default--

External Redirection URL https://172.22.32.5/porta [0-255] chars

User Authentication Settings

CaptivePortal Authentication Type local-radius

Primary Authentication Profile IDMAU

Secondary Authentication Profile NO Radius

Primary Accounting Profile IDMACC

Secondary Accounting Profile NO Radius

*Accounting Interim Interval 600 [600-36000] seconds

Additional Notes

1) If the controller is not reachable no Captive Portal authentication takes place as the guest user database is maintained in the controller. The same rule applies for Internal Captive portal with Radius and External Captive Portal since the controller is still the Radius Client.

2) No logout is supported for Internal Captive Portal

3) The session time-out, activity time-out & L3 User session time-out values set in the controller is also applicable for bridged mode Captive Portal Clients. Copied below is the station-logs captured during a successful authentication of a Bridged mode Captive Portal Client.

Note: The session_time and idle_time values returned by the controller are same as the behavior you may observe for clients connecting in tunneled mode.

```
2013-Sep-10 09:24:22.260494 | b0:65:bd:4b:59:7d | CP User Authentication |
<User=CPuser> <ipaddr=172.18.144.11> Guest User Authenticated Successfully
<session_time=3600><idle_time=600>
```

4) The AP CLI command "`brcp show`" displays the Captive Portal authentication status of client in bridged mode.