WiNG5 DESIGN GUIDE

By Sriram Venkiteswaran

WiNG5 CAPTIVE PORTAL DESIGN GUIDE

June, 2011

TABLE OF CONTENTS HEADING STYLE

WiNG5 Captive Portal

INTRODUCTION TO CAPTIVE PORTAL

OVERVIEW

The Motorola Hotspot authentication feature offers a simple way to provide secure authenticated access on a WLAN for users and devices using a standard web browser. Hotspot authentication allows enterprises to offer authenticated access to the network by capturing and re-directing a web browsers session to a captive portal login page where the user must enter valid credentials to be granted access to the network.

The Motorola RF Switch supports the following advanced feature set that can be deployed to support Hotspot authentication for guest user or private user access:

COMMON APPLICATIONS

Hotspot authentication can be utilized for multiple applications including guest and visitor access or private user access and can be found in telecom, private enterprises, hospitality, healthcare, transportation and education environments. Hotspot authentication is fast becoming a popular means for authenticating users and devices as it provides administrators with the means for performing authentication without deploying 802.1X or distributing shared keys.

Authenticated Visitor Access:

A common application for the Hotspot feature is to provide secure authenticated access for guest users and visitors at a site. Prior to Hotspot authentication organizations wishing to provide guest access would establish an open ESSID that was separated from the internal network which any authorized or unauthorized device could access. While this approach provided the necessary access it also provided no means of authentication and provided free open access to the Internet for any device in range of the network.

Hotspot authentication solved this problem by providing an authentication component using a standard web browser. Visitors and guest users at a site would be provided with a temporary username and password from front desk personnel during the sign-in process which would permit access to the network for the duration of their visit. Once the time for the guest account expired, the user would be denied access to the network.

Employing Hotspot authentication for visitor access provides enterprises with the following benefits:

1) Authentication ensures that only authorized users are permitted access to the guest network. Casual users looking for a free Internet access are not permitted.

2) Provides the ability to associate different network access permissions to classes of users. For example visitors can be provided with one class of access vs. contractors who be provided with a different class of access.

3) Time limits can be applied and enforced for accounts ensuring that Internet access is only permitted to a visitor for the duration of the visit.

4) Time of day and day of week policies can be enforced for long term visitors ensuring Internet access is only permitted during operating business hours.

5) Bandwidth policies can be applied ensuring guest users cannot monopolize or abuse the network.

6) Firewall policies can be applied to restrict access to only specific protocols and applications.

Authenticated Private Access:

Another common application for the Hotspot feature is to provide authenticated access to private networks for un-managed devices. In certain vertical markets such as education administrators need to provide access to un-managed devices that are owned and maintained by end users such as students and faculty.

In typical enterprise environments 802.1X authentication is commonly employed to provide secured authenticated access into the private network. This approach is typically very easy to deploy and maintain as the end user devices are all owned, managed and maintained by the enterprise IT organization. However in environments such as education the make, model and OS of the end-user devices varies making 802.1X very challenging to deploy, manage and maintain.

Prior to Hotspot authentication it was very common for education environments to deploy an SSID that utilized shared keys and/or MAC authentication. This approach eliminated the need for 802.1X authentication but placed increased burden on IT staff which each semester had manage and rotate keys as well as maintain MAC lists of all the permitted devices.

Hotspot authentication provides an elegant way to solve these administrative challenges. First Hotspot authentication provides the means for tying the user authentication into an existing RADIUS or LDAP user database allowing students to authenticate using their assigned student ID and password. Secondly as Hotspot authentication only requires a standard web browser for authentication any end-user device can be supported.

Employing Hotspot authentication for private network access provides enterprises with the following benefits:

1) Eliminates the administrative burden for managing and maintaining MAC address lists.

2) Ties authentication into an existing RADIUS or LDAP back end allowing users to utilize their network credentials for access.

3) Provides secure authentication without having to deploy, manage or maintain 802.1X on the end user devices.

4) Provides the ability to associate different network access permissions to classes of users. For example students can be provided with one class of access vs. faculty who be provided with a different class of access.

5) Bandwidth policies can be applied ensuring users cannot monopolize or abuse the network.

6) Allows network access to be restricted based on location. For example firewall policies can be dynamically applied to sessions to restrict outbound Internet access at specific locations.

7) Allows administrators to eliminate account sharing by limiting the number of simultaneous times a user-id can be used to access the Hotspot.

Paid Internet Access:

The final common application for Hotspot authentication is to provide paid access to the Internet. Hotspot authentication allows organizations to offer paid Internet access to subscribers be offering a block of time that users can use over multiple days or a block of time that can be utilized for one day only. Additionally Hotspot authentication allows providers to offer tired services to users by providing bandwidth allocations or different classes of service based on the purchased access package.

Paid Internet access typically employs a specialized back-end that the Hotspot users are re-directed to during the capture process which provides the account creation and billing integration. Existing users with account balances can enter their credentials in the portal and authenticate to the network which provides access for the time remaining on their account. New user's sign up for new access and can select a package or amount of time which is charged to a credit card. Once billing has been performed the user is provided access for the purchased block of time.

Hotspot authentication is attractive for paid access applications as it requires no client or specialized software to be installed on the end user device. Hotspot authentication leverages the end users web browser to perform the secure payment transaction and authentication and leverages the features implemented on the RF Switch which can controls time restrictions and bandwidth allocation

HOTSPOT AUTHENTICATION PROCESS:

Hotspot authentication requires no client software on the end user device and leverages the end users web browser to perform authentication. When a user initially associates to a Hotspot enabled WLAN, the user has limited network access until they open their web browser and authenticate.

Prior to authentication the user is only provided limited access to the network allowing devices to obtain an IP address from DHCP, resolve hostnames using DNS and communicate with the Hotspot service. Once authentication has been performed, network access is determined based on any firewall rules statically applied to the Hotspot enabled WLAN, physical port or the Hotspot virtual IP interface. Dynamic firewall policies can also be applied to users if an advanced security license is installed on the RF Switch.

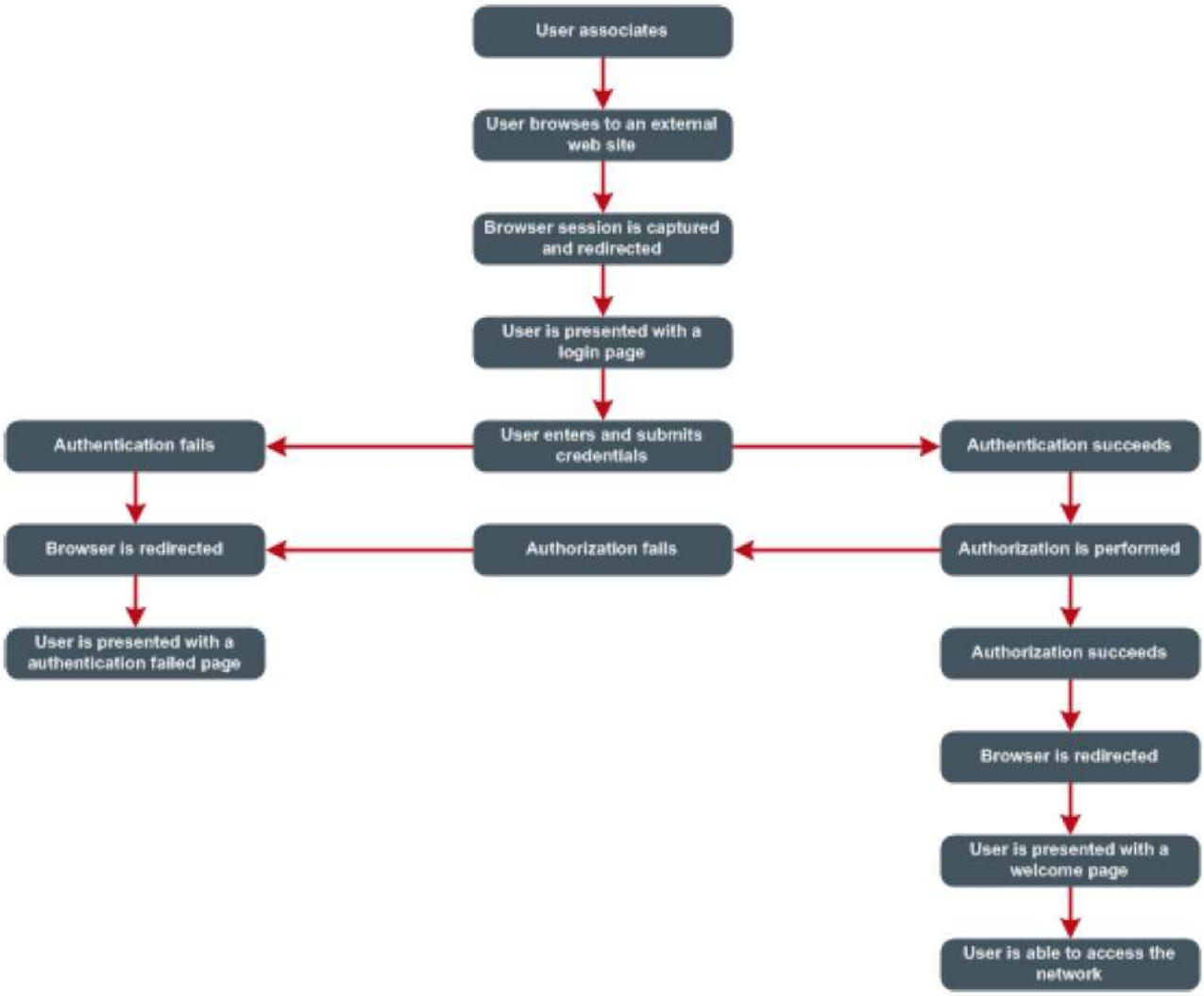


Fig 1 – Hotspot Authentication Process

1) The user associates to the Hotspot WLAN. The WiNG5 AP / RF Controller only permits access to DHCP, DNS and Hotspot Login Page

2) The user opens their web browser and attempts to connect to an external website

3) The WiNG5 AP intercepts the browser session and redirects the web browser to a login page hosted on the WiNG5 AP / RF Controller or external web server.

4) The user enters and submits their credentials

5) The WiNG5 AP / RF Switch performs the authentication using the internal RADIUS Server, external RADIUS Server or external LDAP server

   a. If authentication fails the web browser is redirected to a failed page hosted on the WiNG5 AP / RF Controller or external web server

   b. If authentication succeeds authorization is performed. RADIUS Accounting information is also forwarded if enabled.

6) The WiNG5 AP / RF Switch verifies that the user is permitted to access the network based on user account expiry settings and time-of-day or day-of-week policies applied to the user group

   a. If authorization fails the web browser is redirected to a failed page hosted on the WiNG5 AP / RF Controller or external web server

   b. If authorization succeeds the web browser is redirected to a welcome page hosted on the WiNG5 AP / RF Controller or external web server

7) The WiNG5 AP / RF Switch evaluates and assigns a role based policy to the session

   a. If no advanced security license is present on the RF Switch, a default-role is assigned to the hotspot user

   b. If an advanced security license is present but no roles match the session, a default-role is assigned to the hotspot user

   c. If an advanced security license is present and a role is matched, the role is assigned to the Hotspot user

HOTSPOT COMPONENTS

1. Hotspot Enforcement Point

The Hotspot enforcement point is the one which intercepts the traffic from the client and provides a redirect URL to the client for authentication. In WiNG5 architecture it is always the AP that intercepts the wireless client traffic and provides redirect URL to the wireless client.

2. Web page Hosting Server

   This is the one that hosts the web page for the login, failure and welcome pages. In WiNG5 the web pages can be either hosted on an AP or a Controller or hosted on any external server.

3. Captive Portal Server

   The Captive Portal Server is the one to which the web page sends the user credentials for authentication. The Captive Portal performs the user authentication by sending the credentials to the RADIUS Server. The Captive Portal then sends authentication status message to the AP to allow or disallow the user.

4. RADIUS Server

   The RADIUS server performs the user authentication.

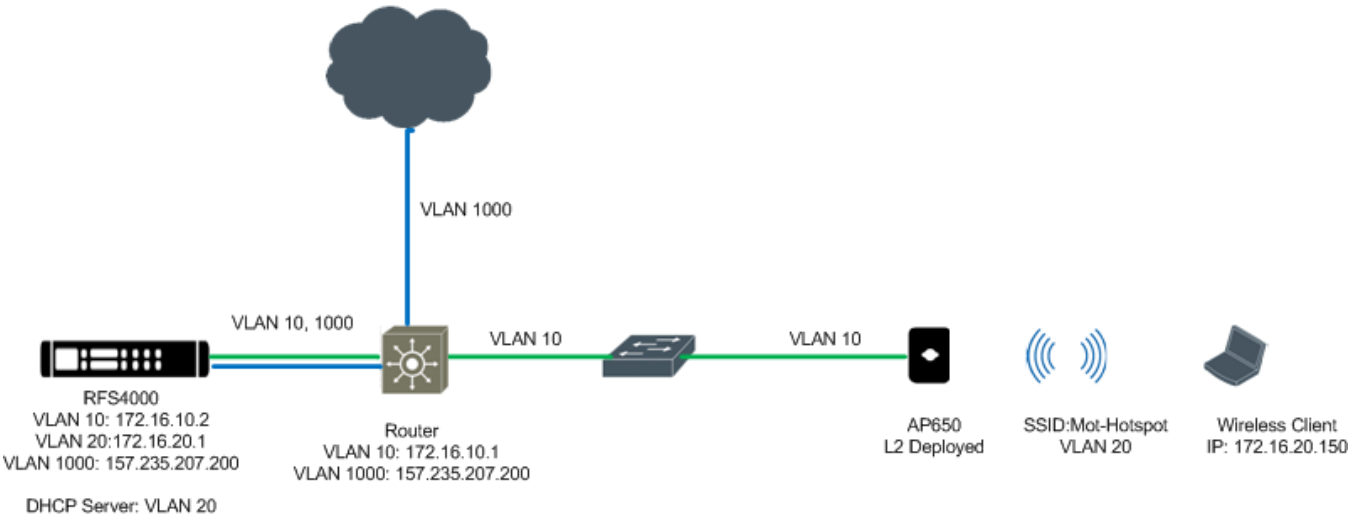
5. User Data Base

   This is the one that stores the user database – it could either be the internal database on the AP or the RFS Controller or could be an external data source like Microsoft LDAP Active Directory server.

DEPLOYMENT SCENARIOS

DEPLOYMENT MODEL – 1: CENTRALIZED CAPTIVE PORTAL SERVER WITH INTERNAL PAGES

This is typically deployed by small and medium business offices - which want a quick way to setup hotspot access to visitors. This solution do not require any external devices to setup the hotspot for guest access. A guest user admin account can log into the system and create user accounts to visitors as and when required.



Captive Portal Server

The Controller acts as the Captive Portal Server.

Captive Portal Pages

The redirection web pages are stored in the controller.

RADIUS Server

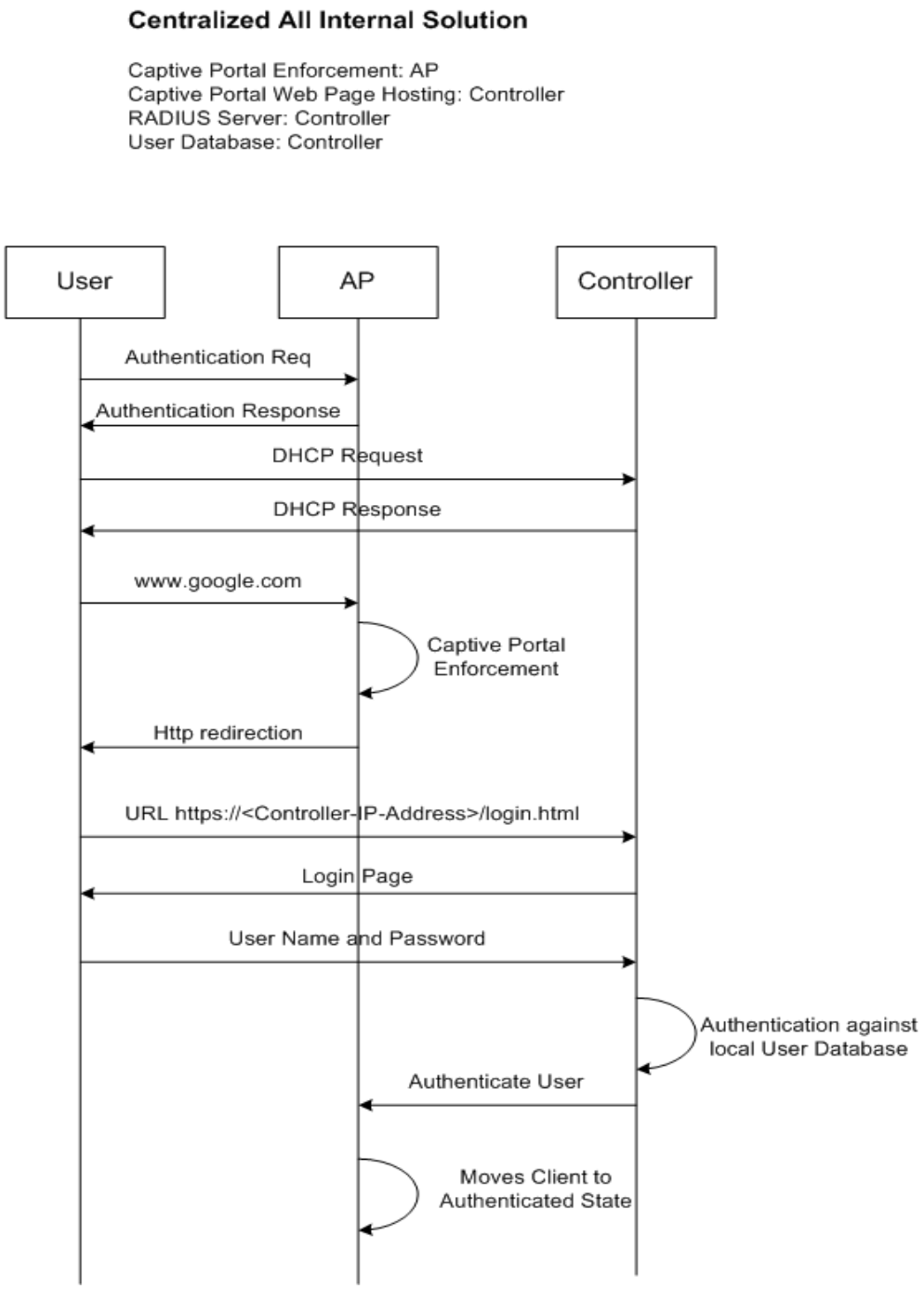
The controller acts as the AAA server.

User Database

The user database is also stored in the controller.

The figure below depicts the message flow of this deployment model.

Message Flow

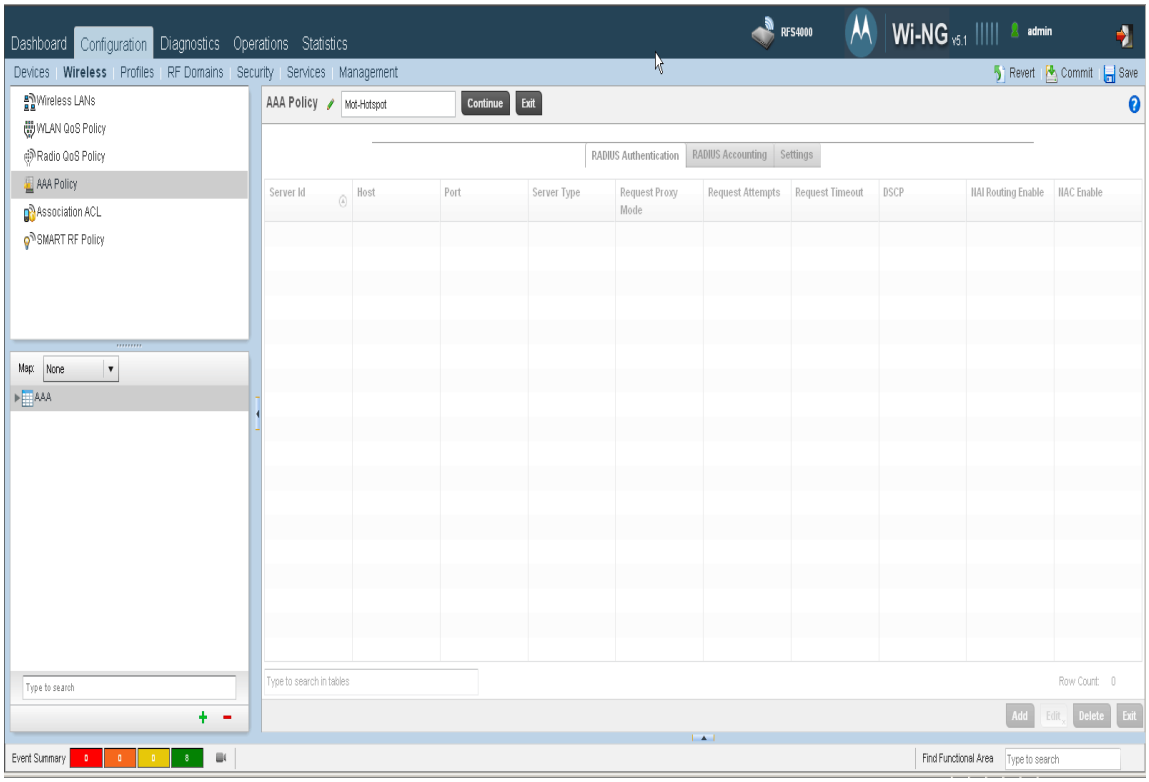


Configuration Steps

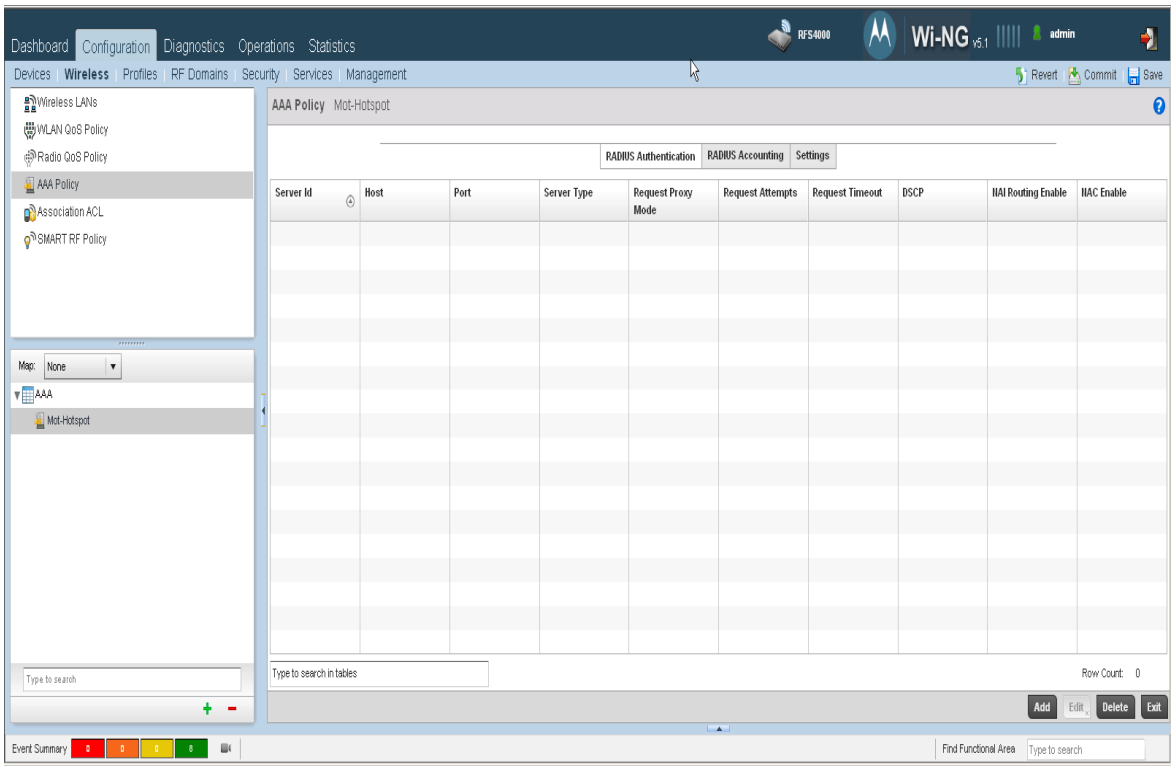
1) Create AAA Policy

a. Under the context: Configuration->Wireless->AAA Policy, click ‘Add’

Enter the AAA Policy Name and click ‘Continue’



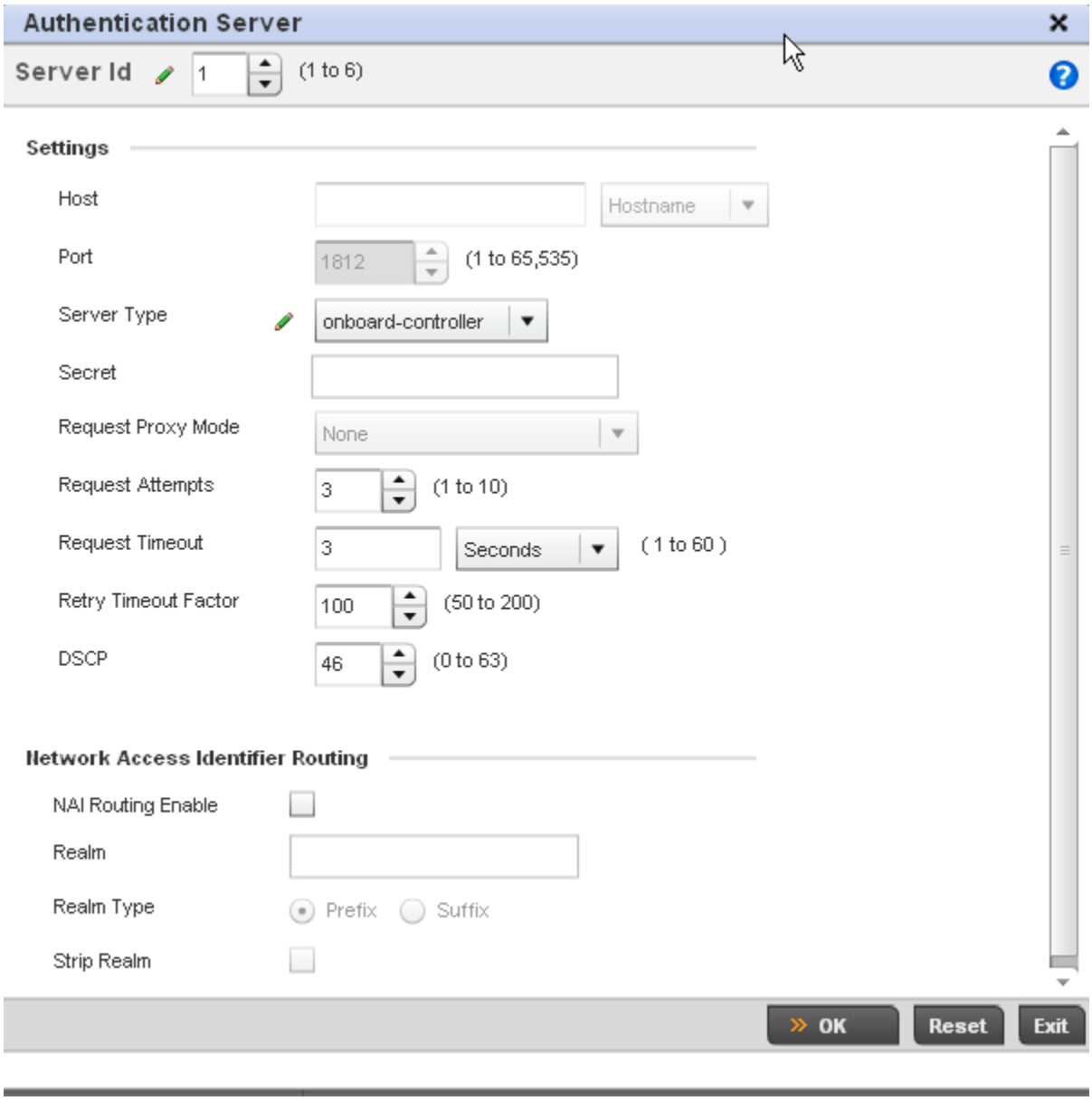
b. Add RADIUS server by clicking ‘Add’



Enter the ‘Server Id’

Select ‘Server Type’ as ‘onboard-controller’

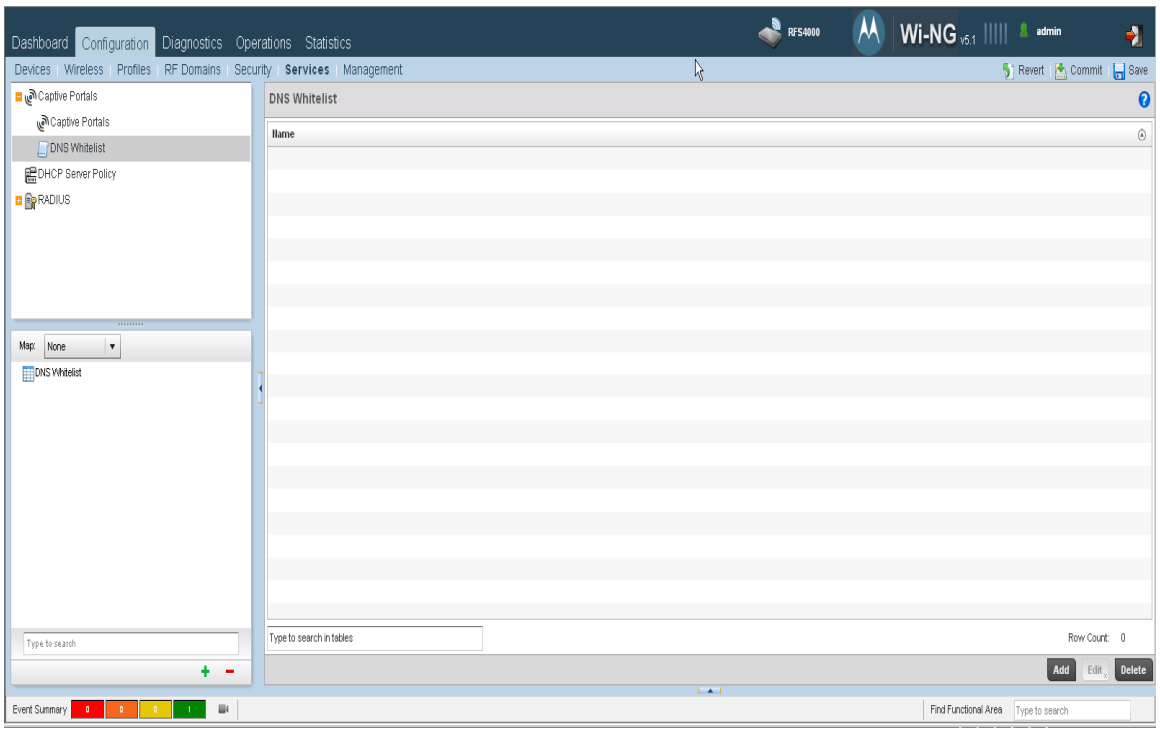
Click ‘OK’



2) Create DNS Whitelist

a. Under the context: Configuration->Services->Captive Portals->DNS Whitelist, click ‘Add’

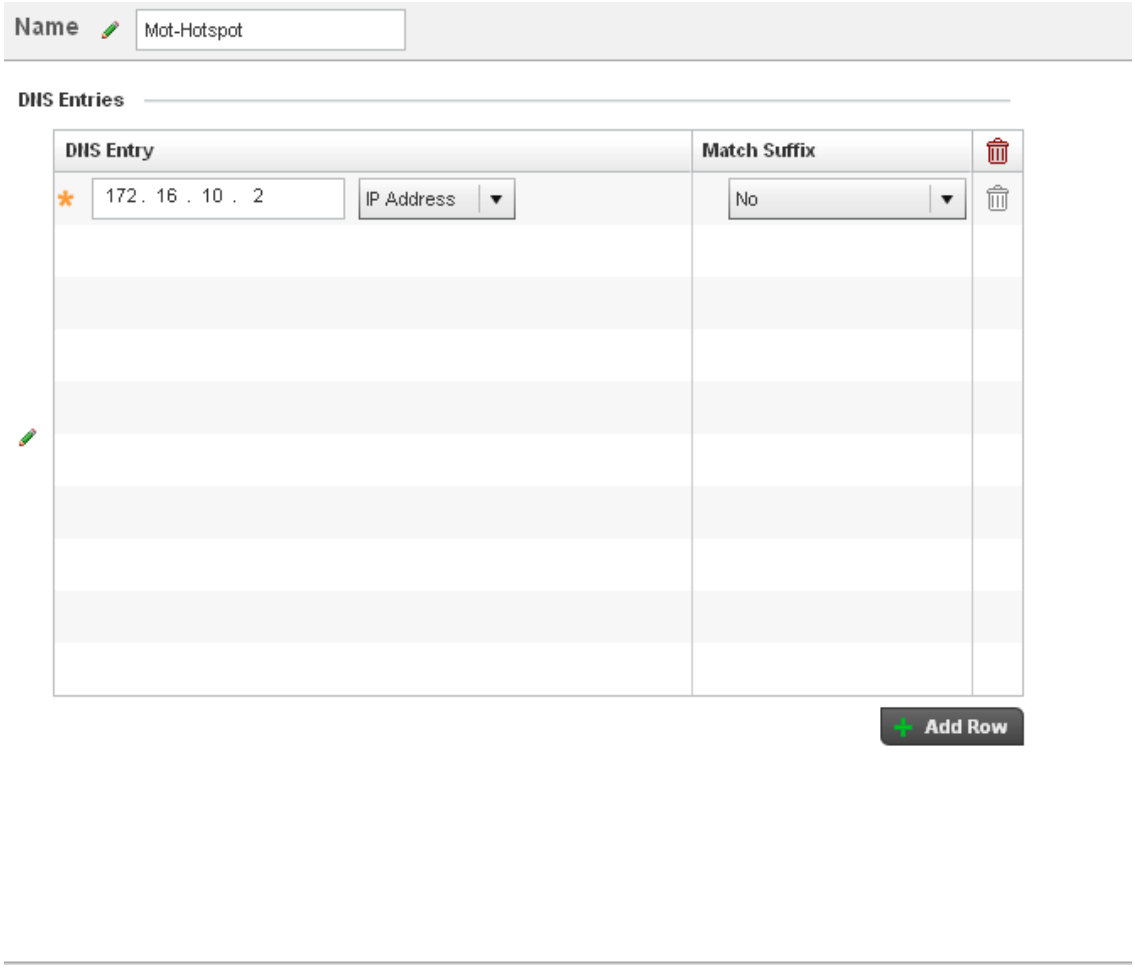
Enter a name for the DNS Whitelist



b. Click ‘Add Row’

Enter the list of IP address that you want to grant access even if the client is not authenticated.

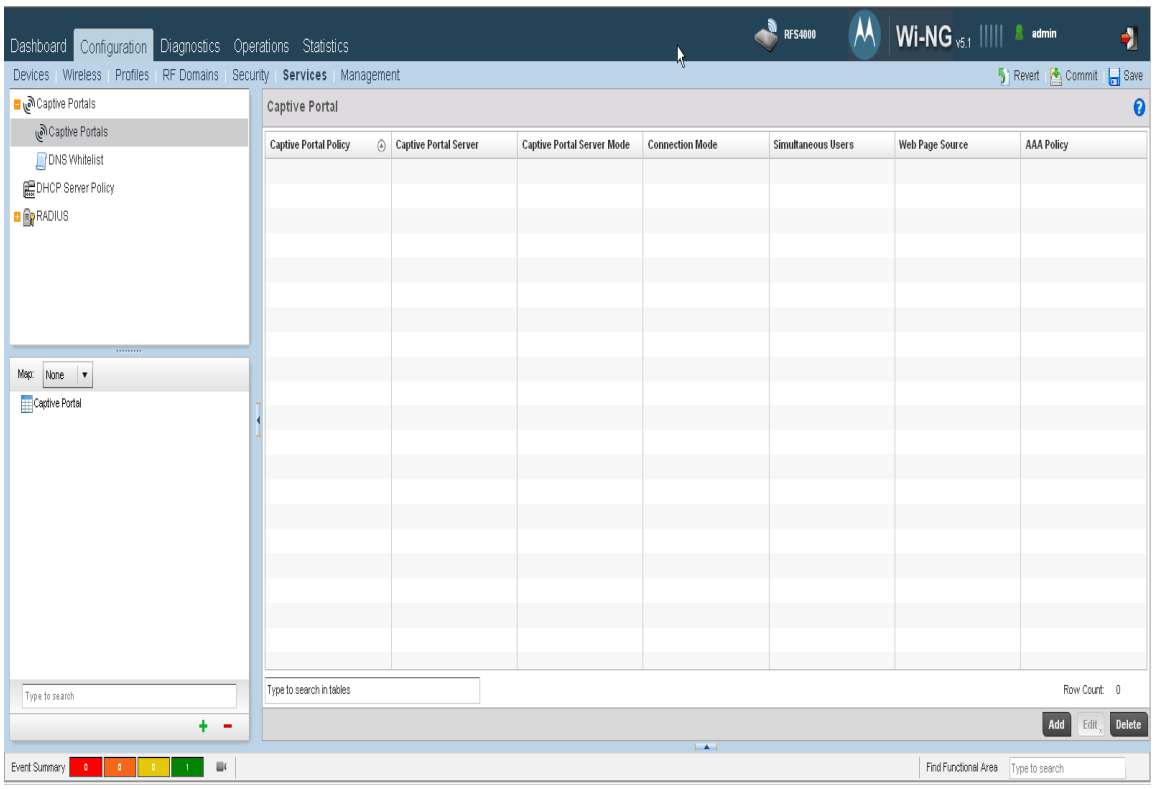
Click ‘OK’



Note: Since we are using the controller to host the pages, we should allow the client to access the controller's IP Address used to host the pages. In this example we are using the controller's VLAN 20 interface to host the captive portal pages, so we are allowing access to 172.16.10.2.

3) Create Captive Portal Policy

a. Under the context: Configuration->Services->Captive Portals->Captive Portals, click 'Add'



Enter the Captive Portal Policy Name

Set ‘Captive Portal Server Mode’ to ‘Centralized’

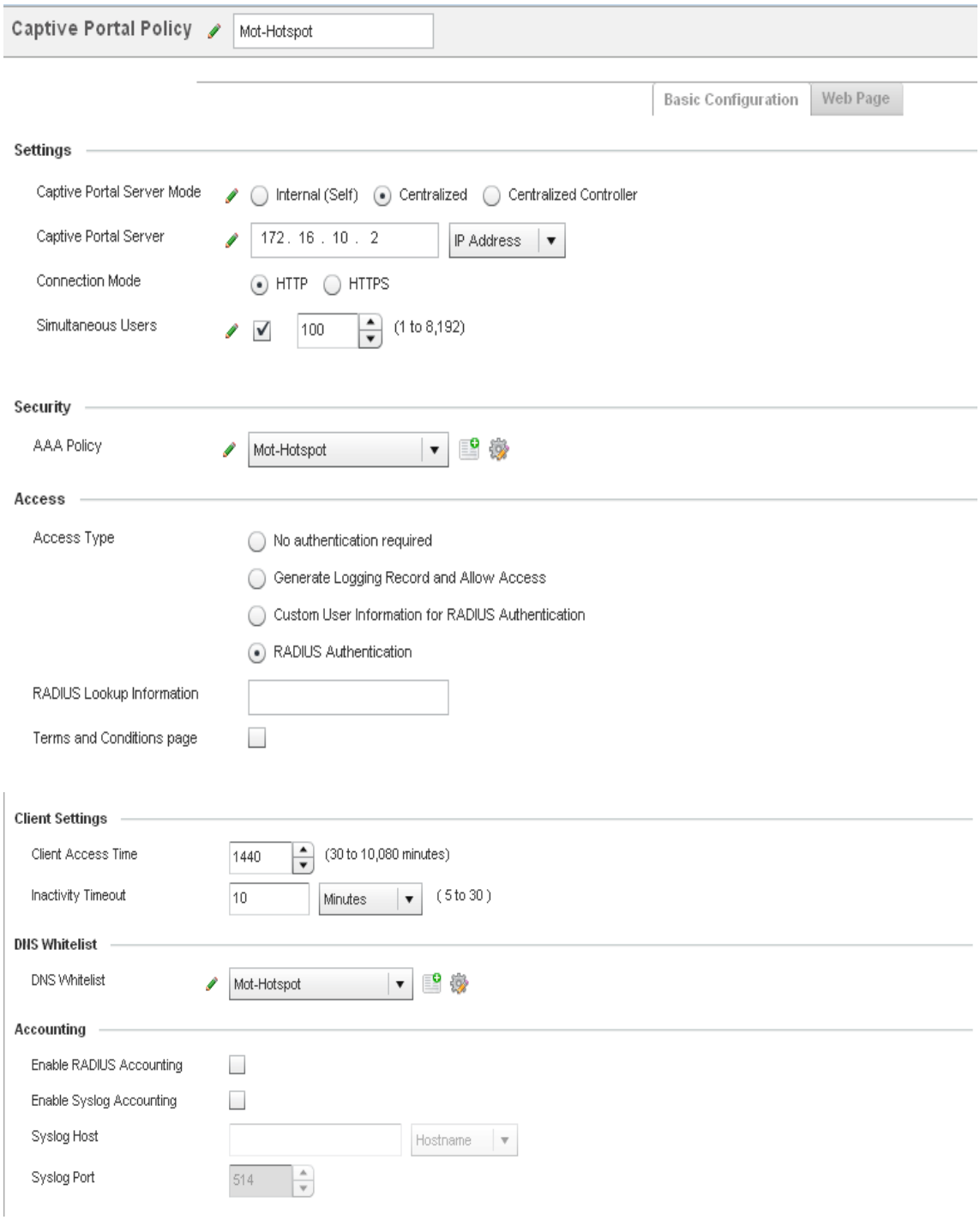
Set ‘Simultaneous Users’ to 100

Set AAA Policy to ‘Mot-Hotspot’ (created in Step 1)

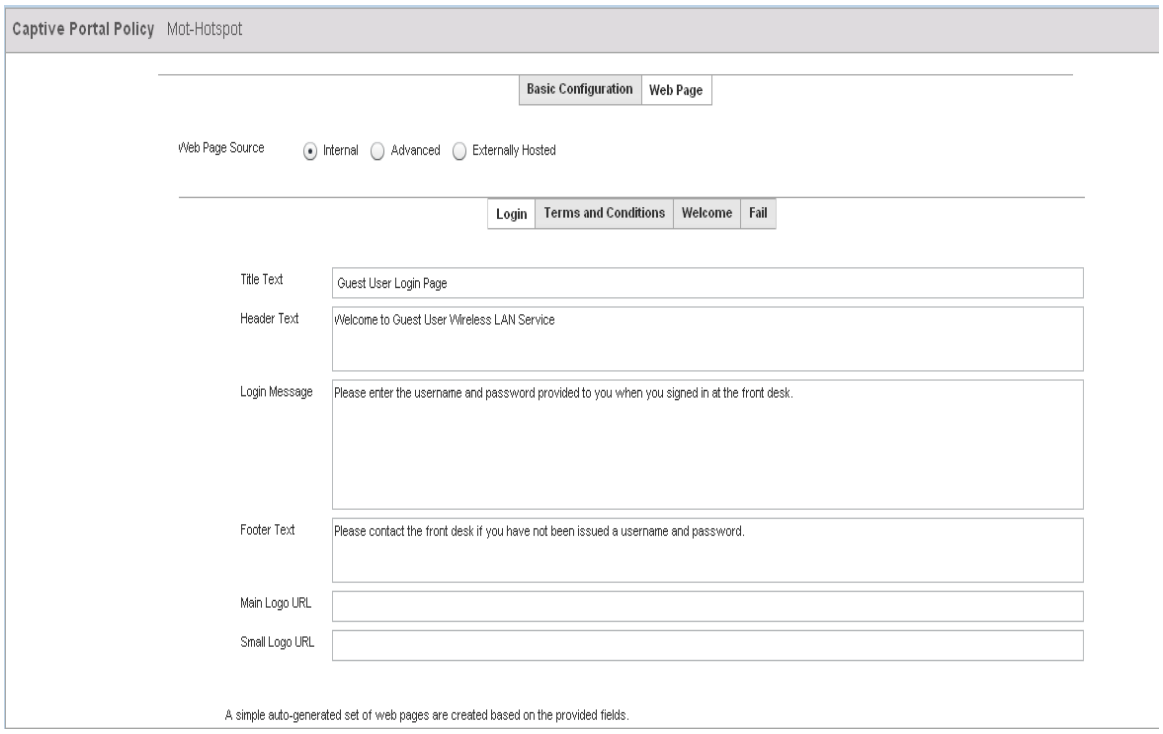
Set Access Type to ‘Radius Authentication’

Set DNS Whitelist to ‘Mot-Hotspot’ (created in Step 2)

Click ‘OK’

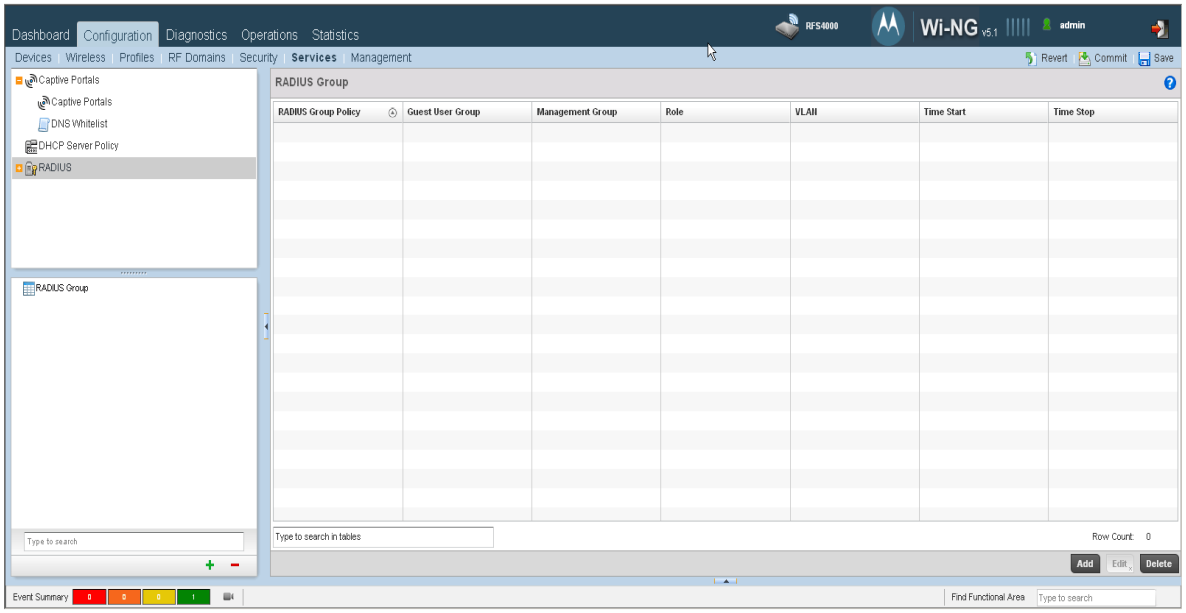


b. On the ‘Web Page’ tab ensure the ‘Web Page Source’ is set to ‘Internal’



4) Create RADIUS Group Policy

a. Under the context: Configuration->Services->RADIUS, click ‘Add’



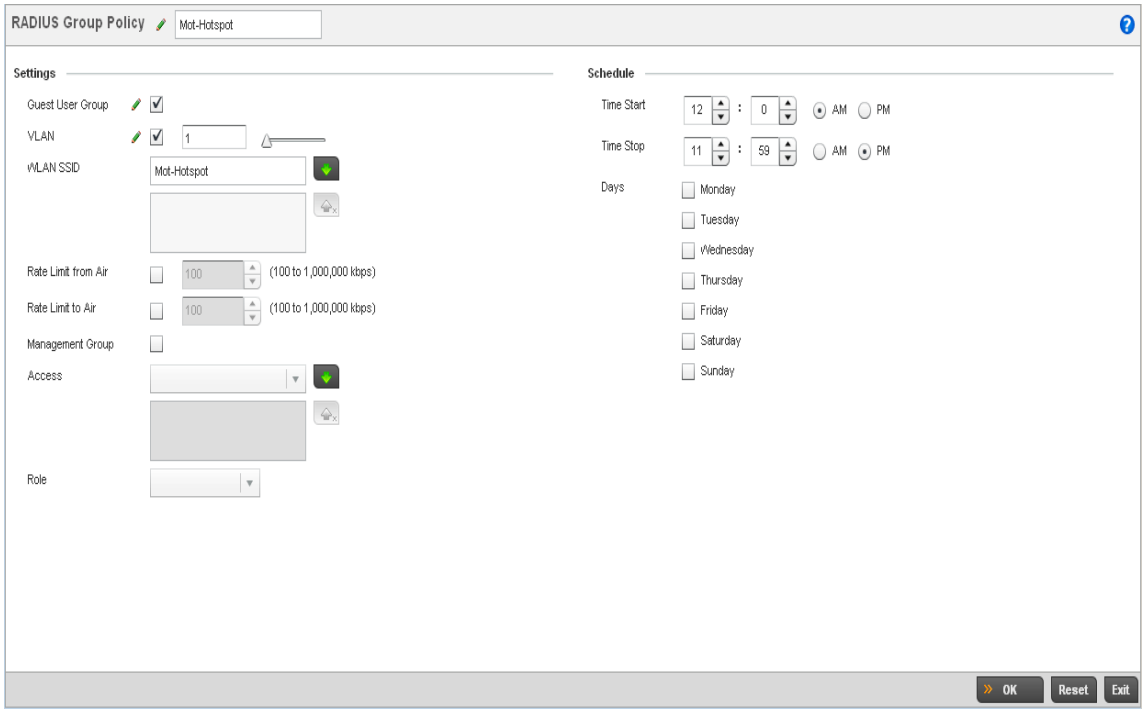
Enter the ‘Radius Group Policy’ Name

Enable ‘Guest User Group’

Set VLAN to ‘20’ – this will override any settings on the WLAN

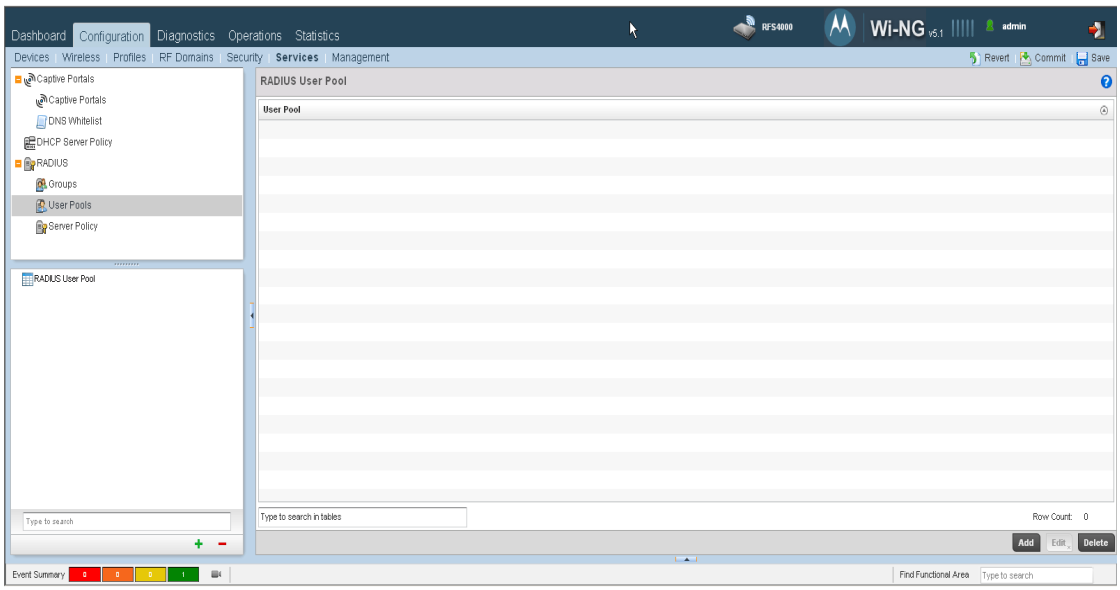
Set WLAN SSID to ‘Mot-Hotspot’

Click ‘OK’



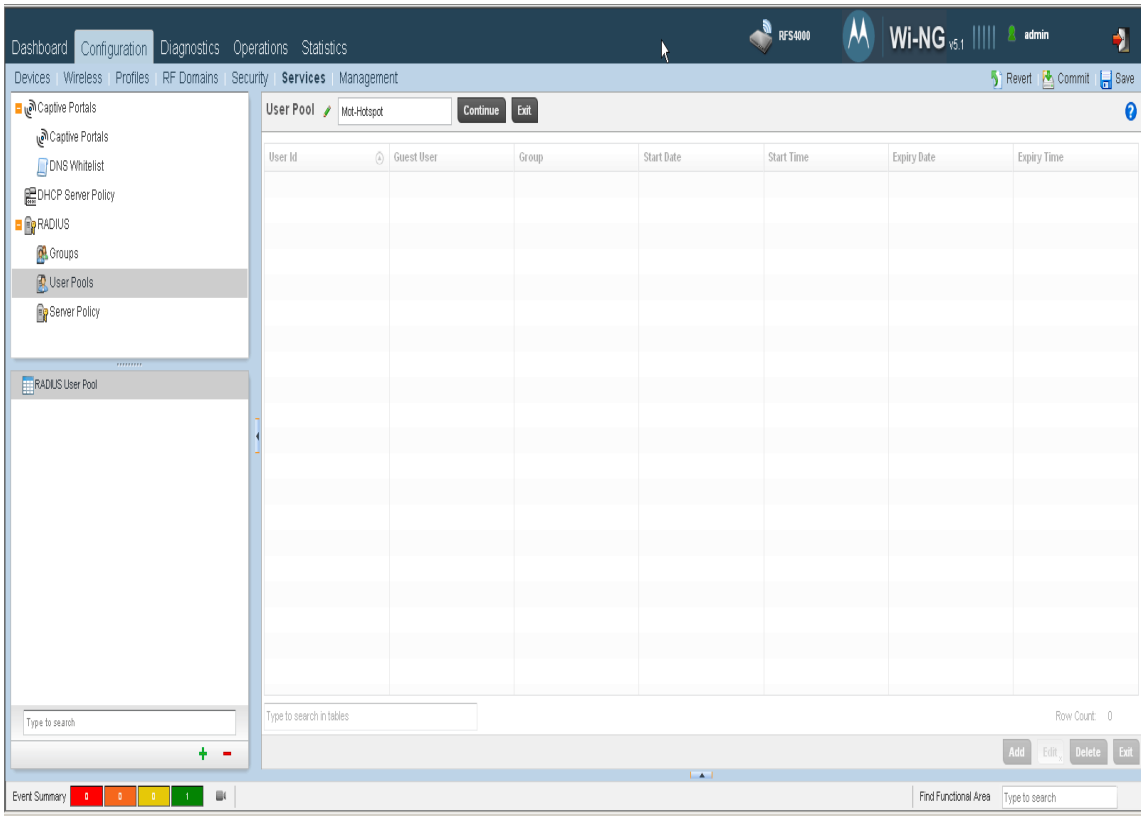
5) Create RADIUS User Pools

a. Under the context: Configuration->Services->RADIUS->User Pools, Click ‘Add’

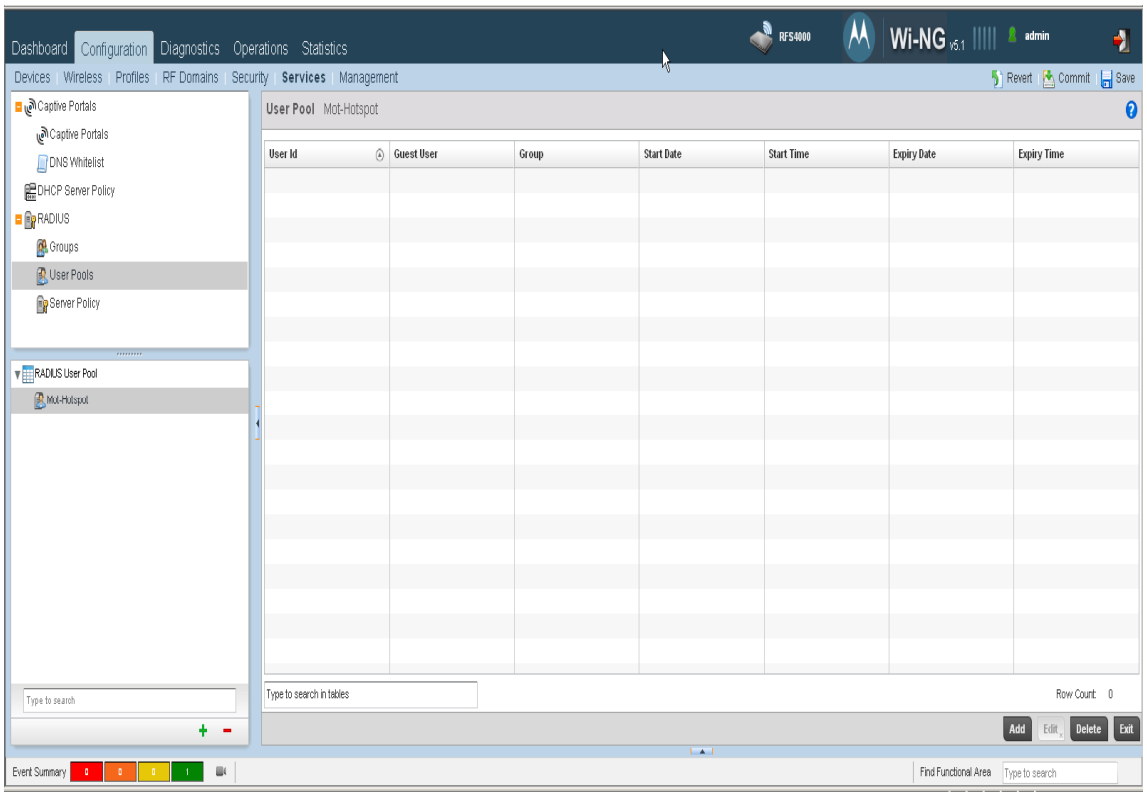


Enter ‘User Pool’ name

Click ‘Continue’



b. In the newly created Radius User Pool, Click ‘Add’ to add Users



Enter the ‘User Id’

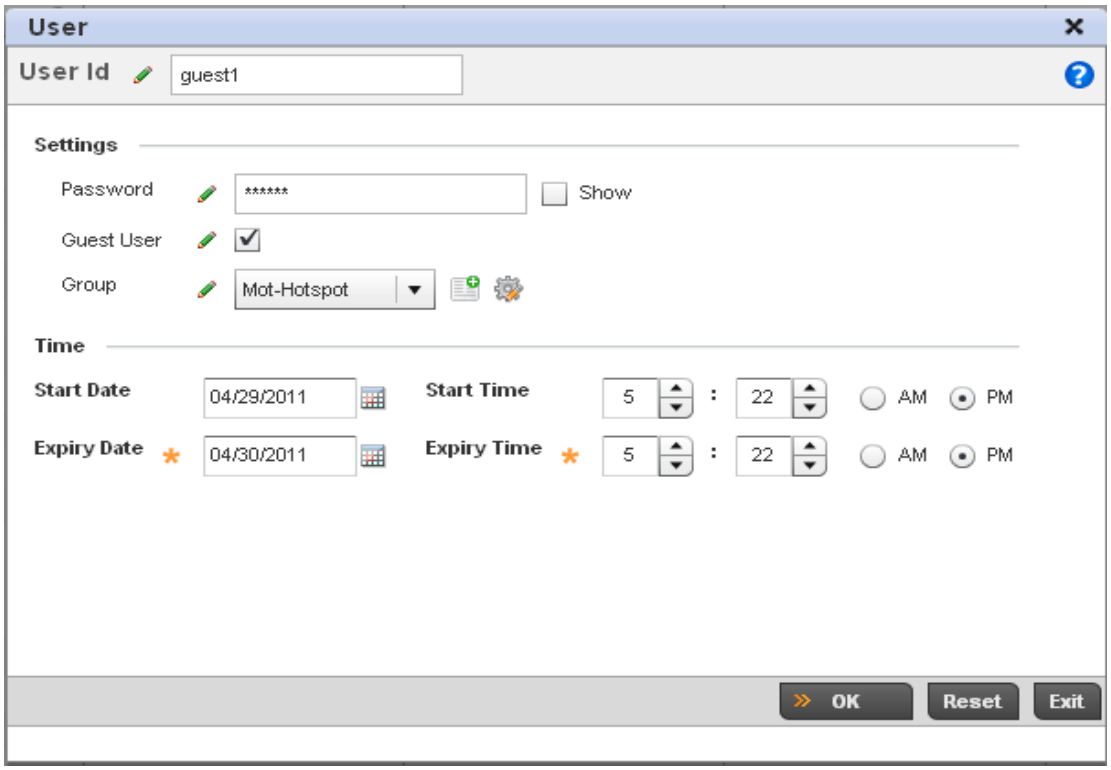
Enter ‘Password’

Select ‘Guest User’

Set Group to ‘Mot-Hotspot’ (create in step 4)

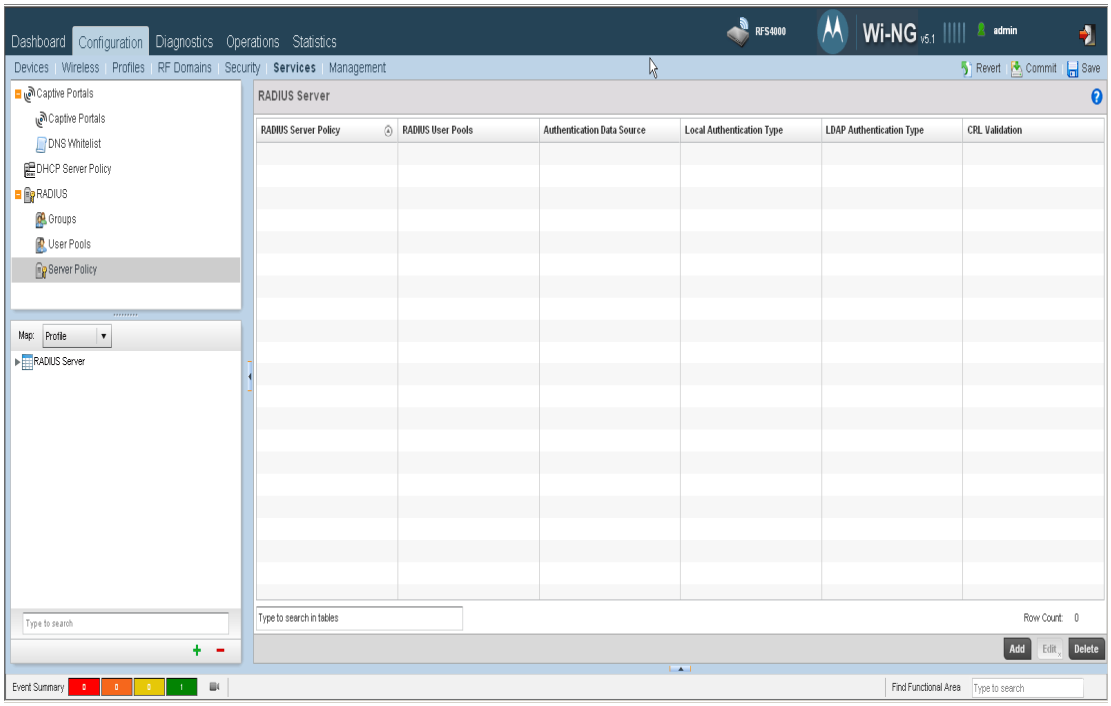
Set Start Date, Start Time, Expiry Date and Expiry Time accordingly

Click ‘OK’



6) Create RADIUS Server Policy

a. Under the context: Configuration->Services->RADIUS->Server Policy, Click ‘Add’



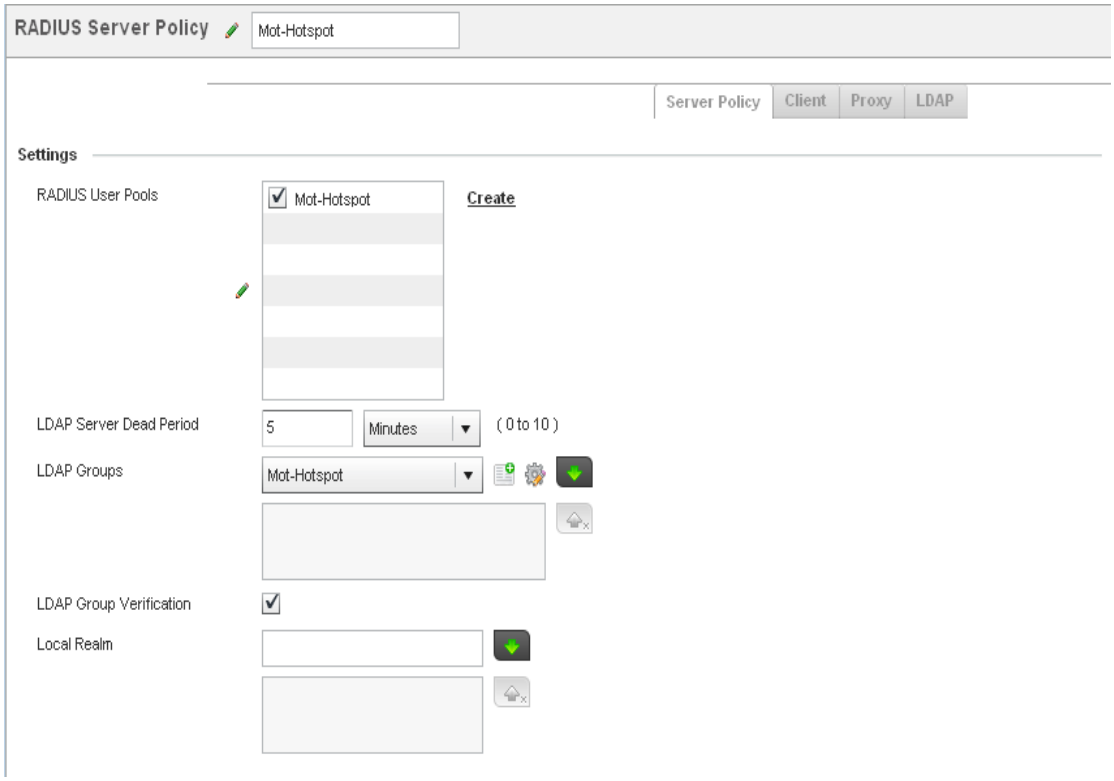
Set ‘RADIUS Server Policy’ name

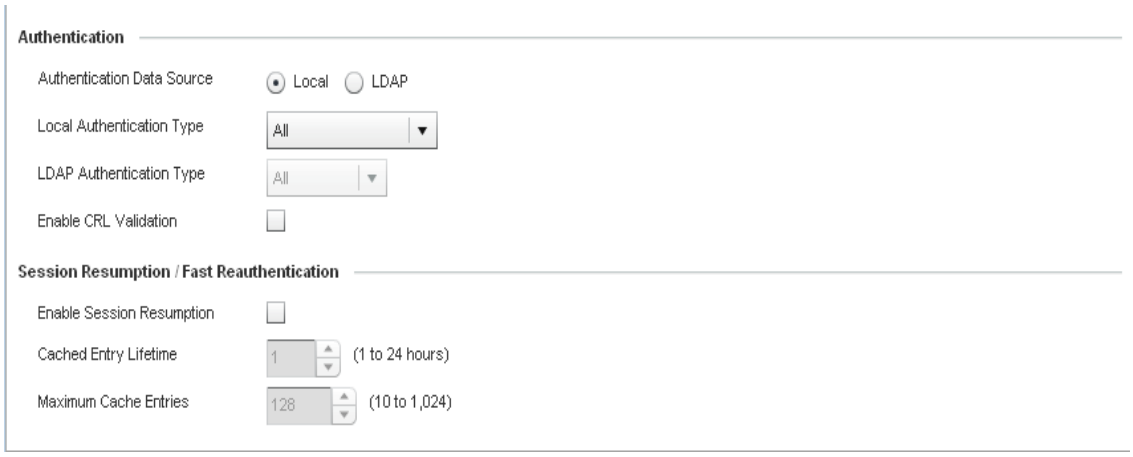
Set ‘RADIUS User Pools’ to ‘Mot-Hotspot’ (created in Step 5)

Set ‘LDAP Groups’ to ‘Mot-Hotspot’ (created in Step 4)

Set ‘Authentication Data Source’ to ‘Local’

Click ‘OK’

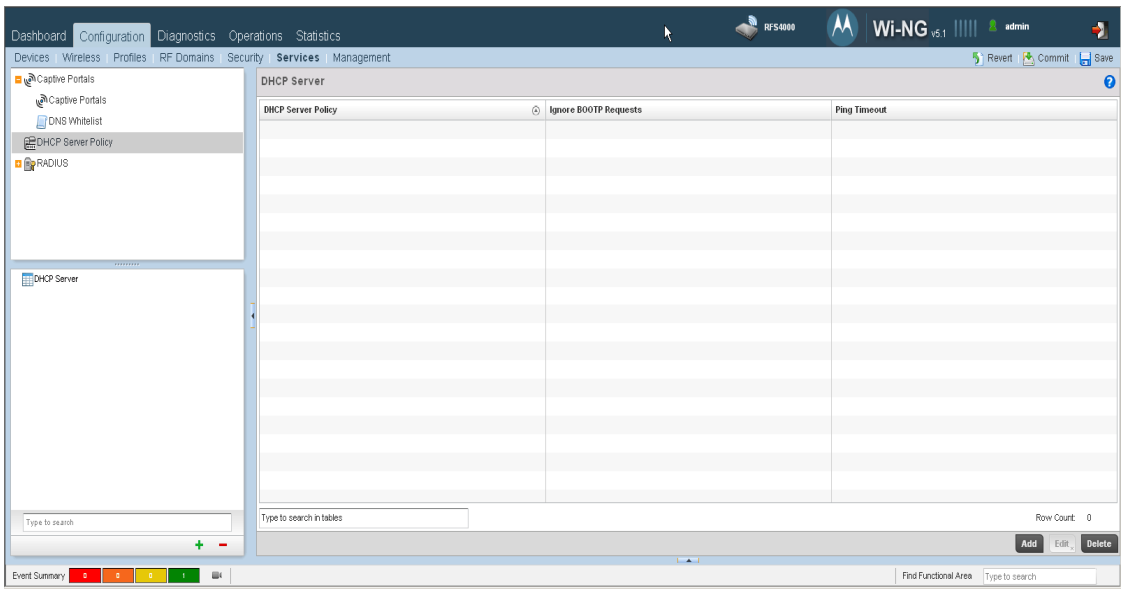




7) Create VLAN 20 for Wireless Hotspot Users and set the IP Address of the VLAN 20 interface as 172.16.20.1

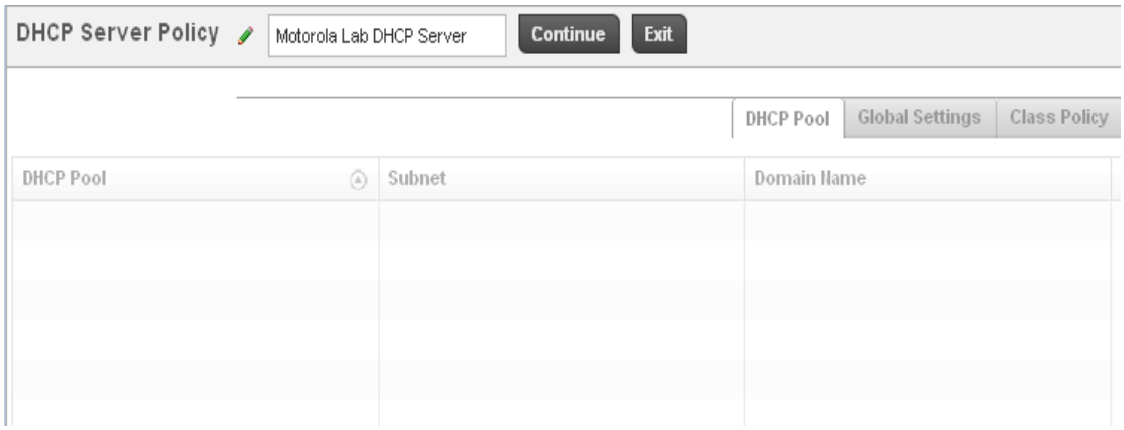
8) Create DHCP Server Policy to give IP address on VLAN20 for Wireless Hotspot Users

a. Under the context: Configuration->Services->DHCP Server Policy, Click ‘Add’

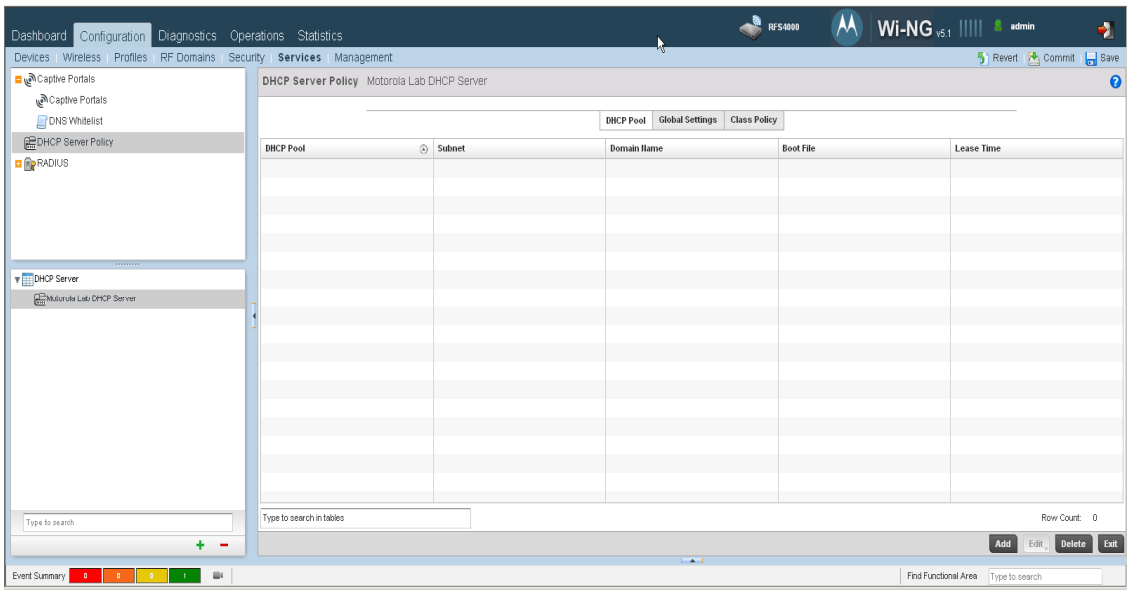


Set ‘DHCP Server Policy Name’

Click ‘Continue’



b. Under the context of newly created DHCP Server Policy, Click ‘Add’ to create a DHCP pool



Set ‘DHCP Pool’ name

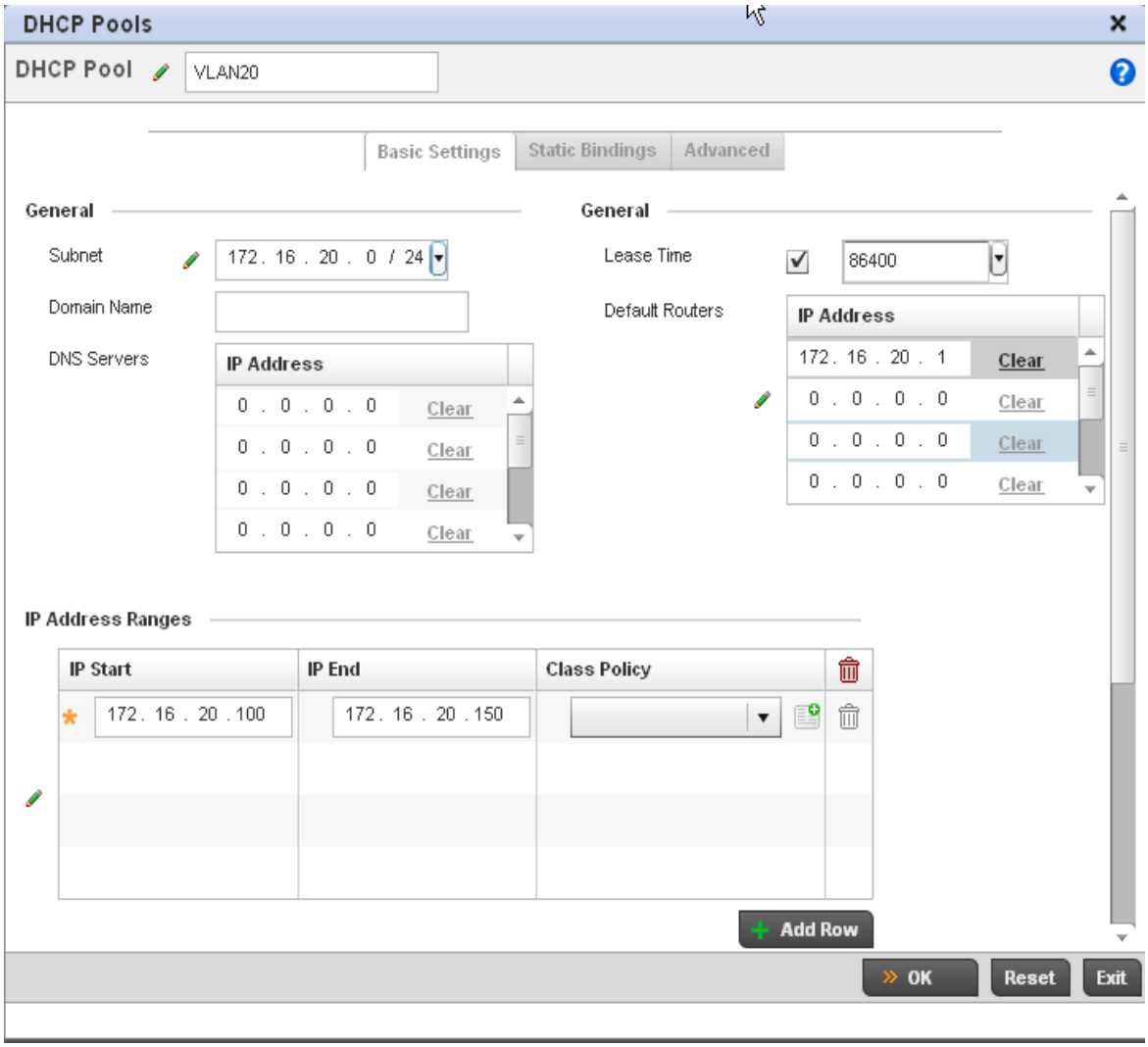
Set ‘Subnet’ to VLAN 20 subnet – 172.16.20.0/24

Set ‘Default Routers’ to VLAN 20 interface IP address – 172.16.20.1

Under ‘IP Address Range’ Click ‘Add Row’

Enter the range of IP Addresses – 172.16.20.100 to 172.16.20.150

Click ‘OK’



9) Map RADIUS Server, DHCP Server and Captive Portal policy in rfs4000 profile

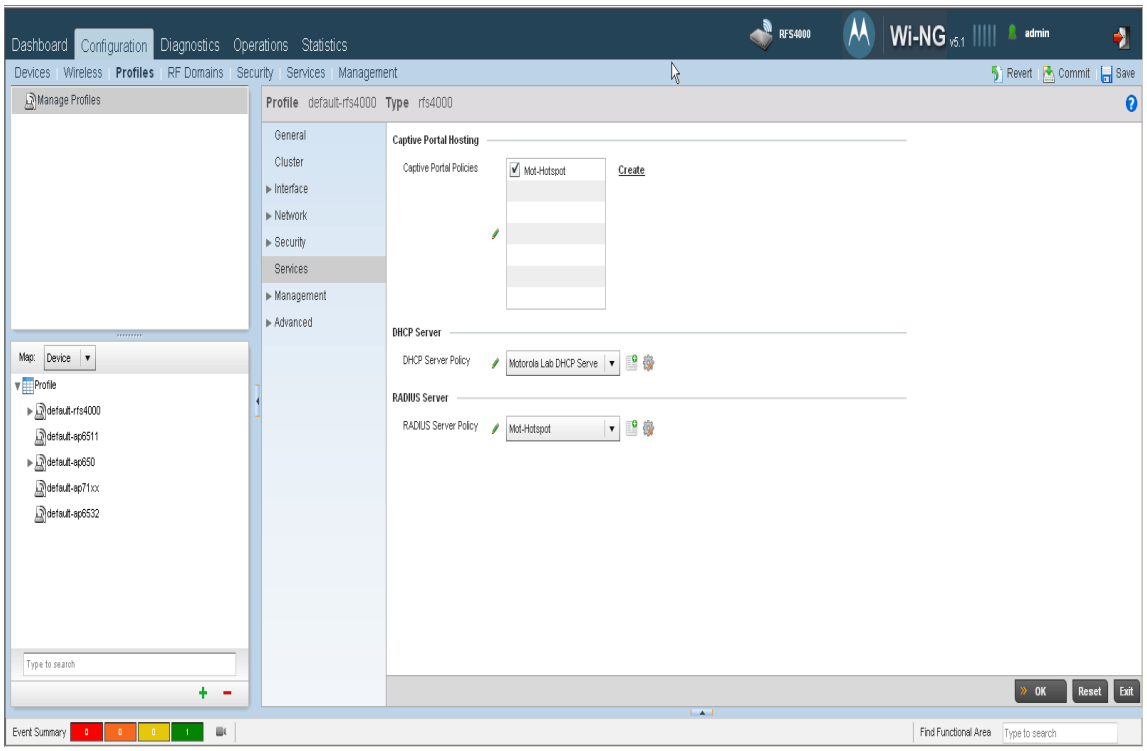
a. Under the context: Configuration->Profiles->Profile->default-rfs4000->services

Set ‘Captive Portal Policies’ to ‘Mot-Hotpot’ (created in Step 3)

Set ‘DHCP Server Policy’ to ‘Motorola Lab DHCP Server’ (created in Step 8)

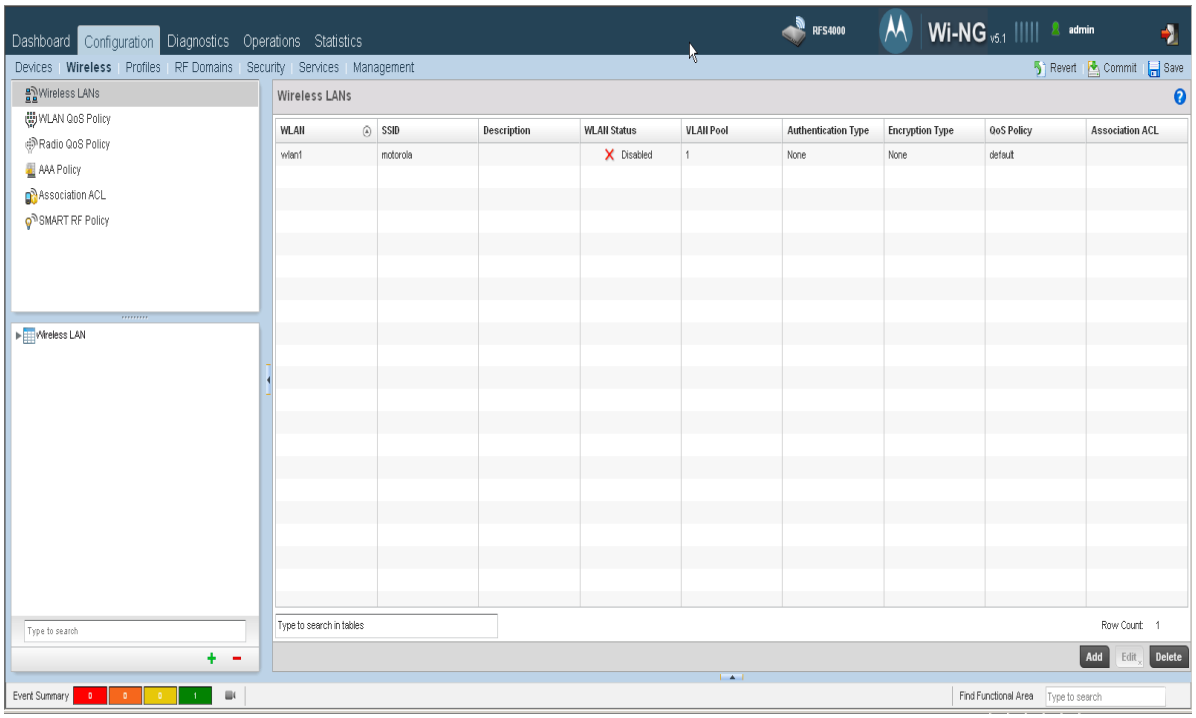
Set ‘RADIUS Server Policy’ to ‘Mot-Hotspot’ (created in Step 6)

Click ‘OK’



10) Create WLAN for Hotspot

a. Under the context: Configuration->Wireless->Wireless LANs, click ‘Add’



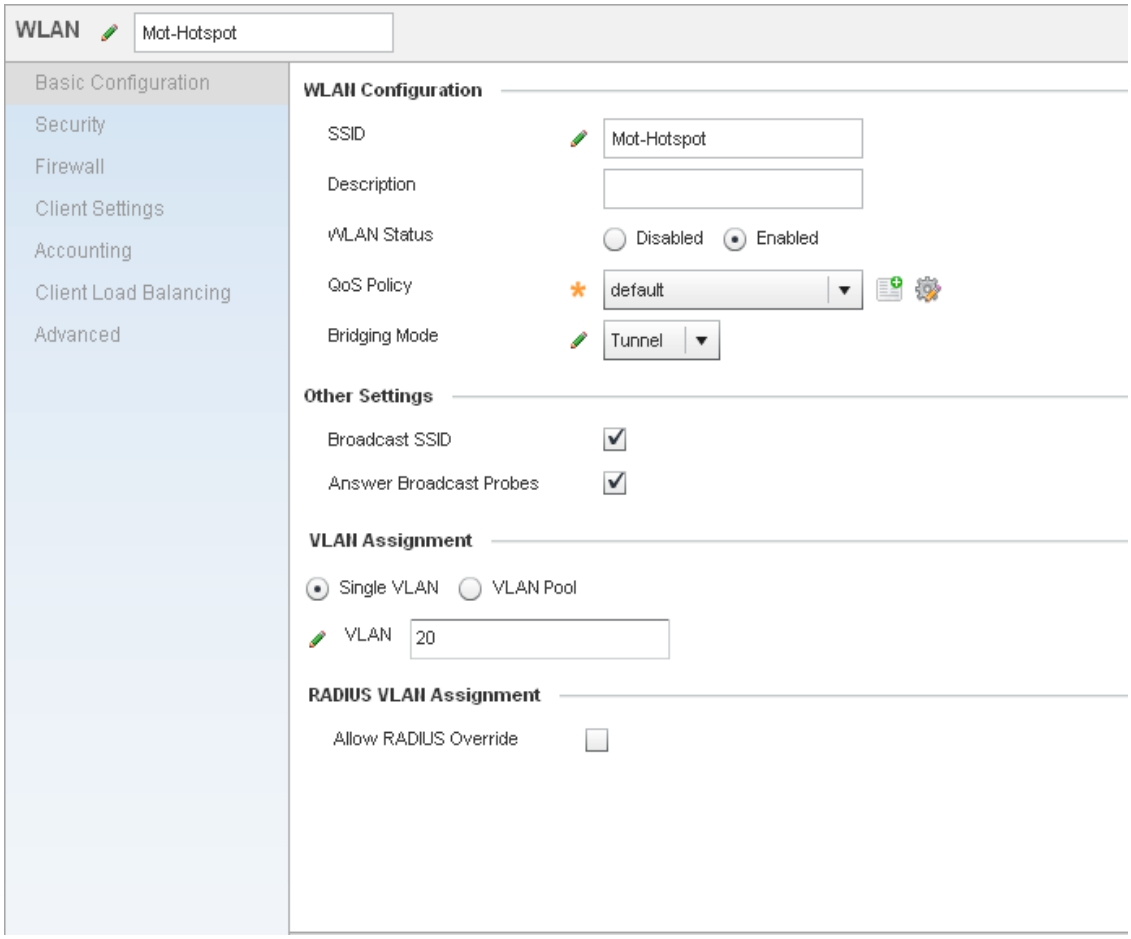
Set ‘WLAN’ name

Set ‘SSID’ – this should match the one you entered in Step 4b

Set ‘Bridging Mode’ to ‘Tunnel’

Set ‘VLAN’ to ‘20’

Click ‘OK’

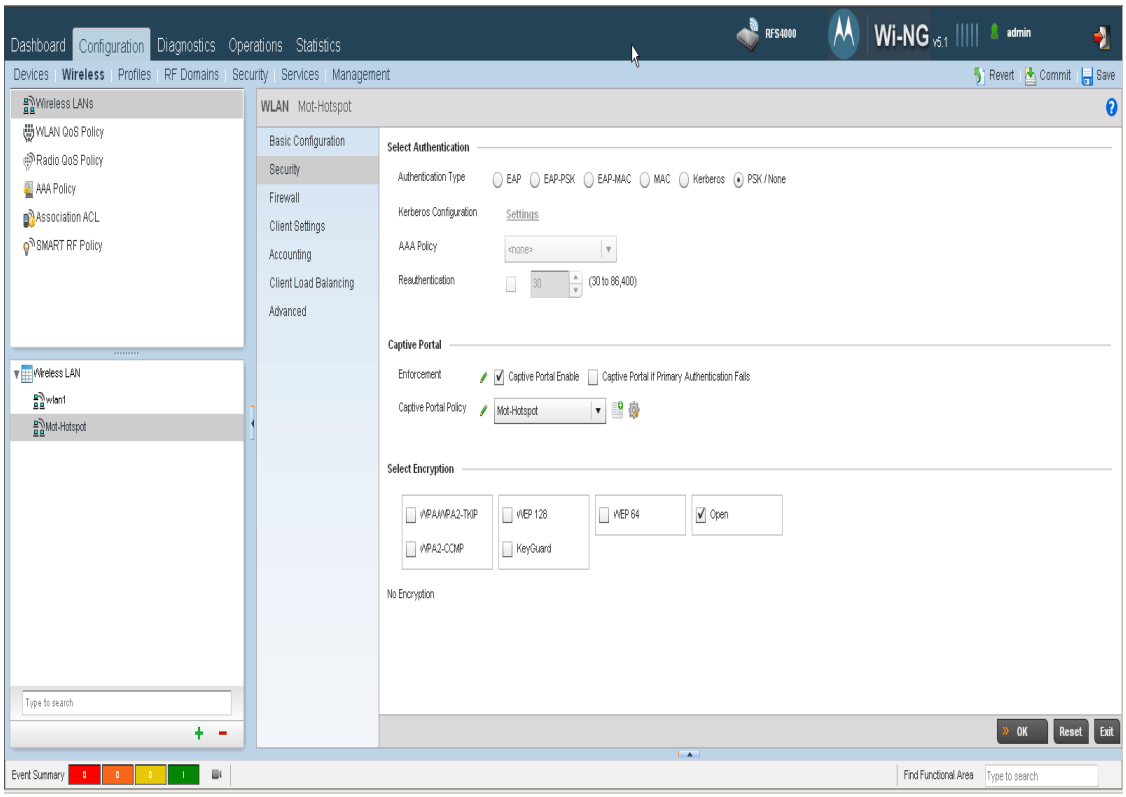


b. Under the Security Menu of the newly created WLAN

Set ‘Enforcement’ to ‘Captive Portal Enable’

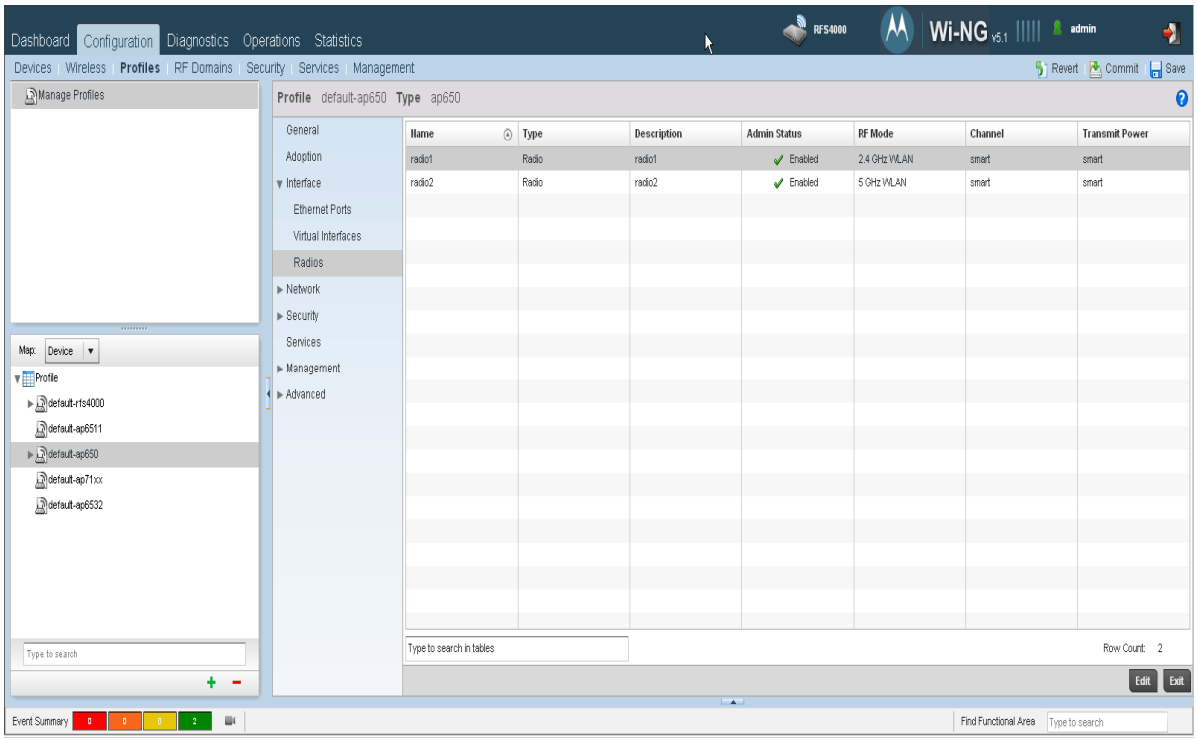
Set ‘Captive Portal Policy’ to ‘Mot-Hotspot’ (created in Step 3)

Click ‘OK’



11) Map WLAN to radios of the AP650 profile

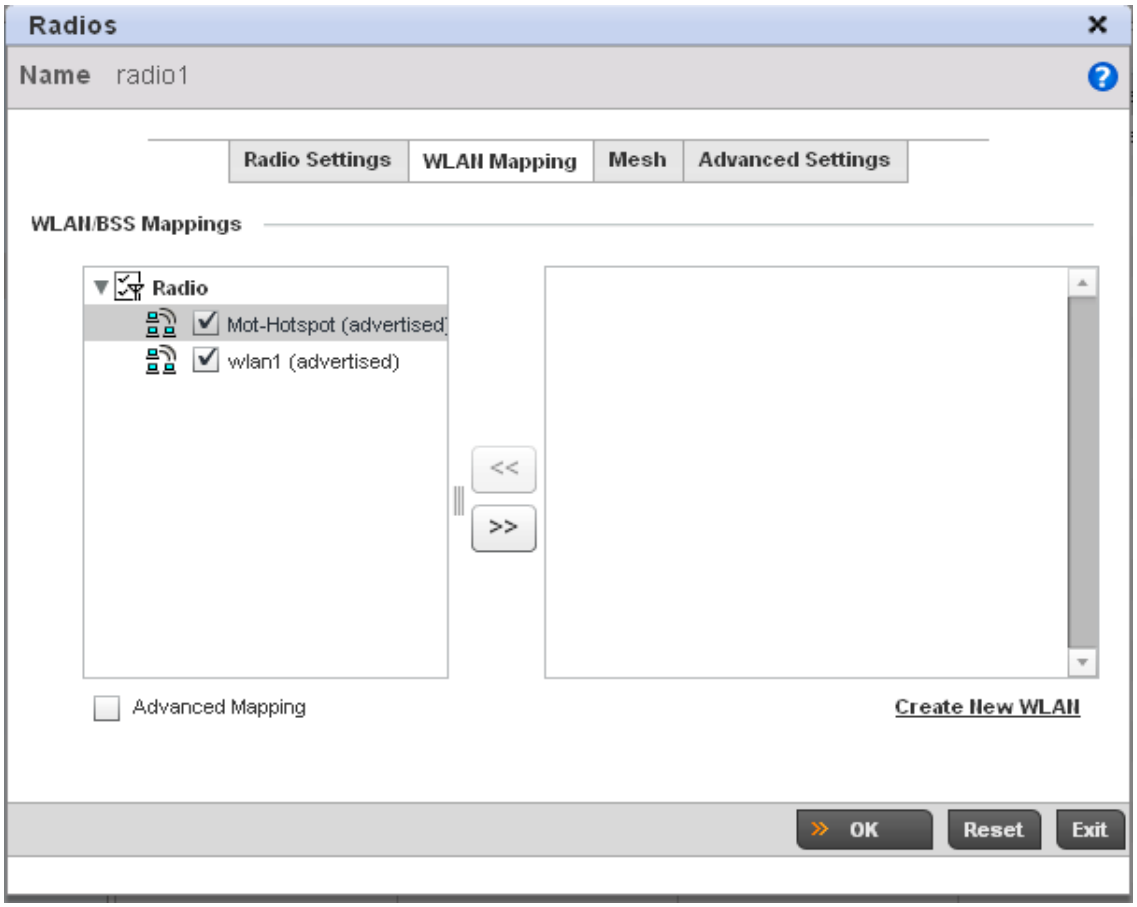
a. Under the context: Configuration->Profiles->Profile->default-ap650->Interface->Radios



Select ‘Radio 1’ and Click ‘Edit’

Under ‘WLAN Mapping’ tab, add ‘Mot-Hotspot’ WLAN (created in Step 10)

Click ‘OK’



Repeat the above 3 steps for Radio 2

To Test the setup

1) Connect the Wireless Client to 'Mot-Hotspot' SSID

   Observe that the Wireless client is assigned IP address in the VLAN 20 range.

2) Open the browser, type www.google.com

   Note: Ensure that DNS resolution happens for the website – the Controller should be connected to the internet which can resolve the entry. Else type any IP Address on the browser.

3) The web page should be redirected to the internal login.html page

4) Enter the user credentials (create in Step 5b)

5) You should now see the authentication success page and should be able to browse the internet.

DEPLOYMENT MODEL – 2: CENTRALIZED CAPTIVE PORTAL SERVER WITH EXTERNAL PAGES

This model describes how to use external web page server which hosts the captive portal server.

Captive Portal Server

The Controller acts as the Captive Portal Server.

Captive Portal Pages

The redirection web pages are stored in an external server.

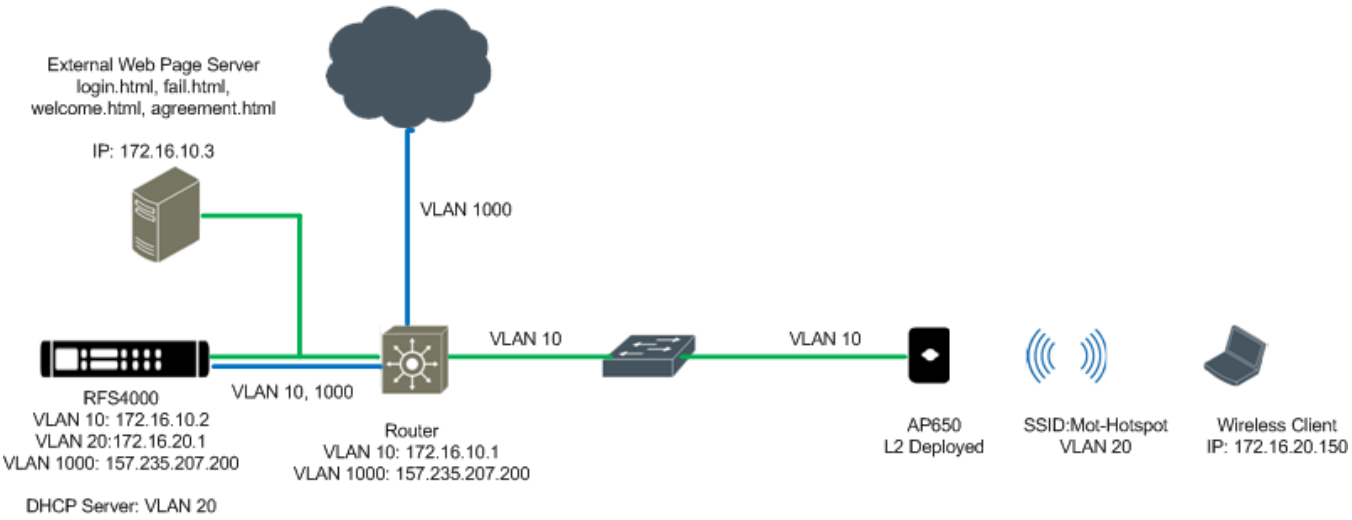
RADIUS Server

The controller acts as the AAA server.

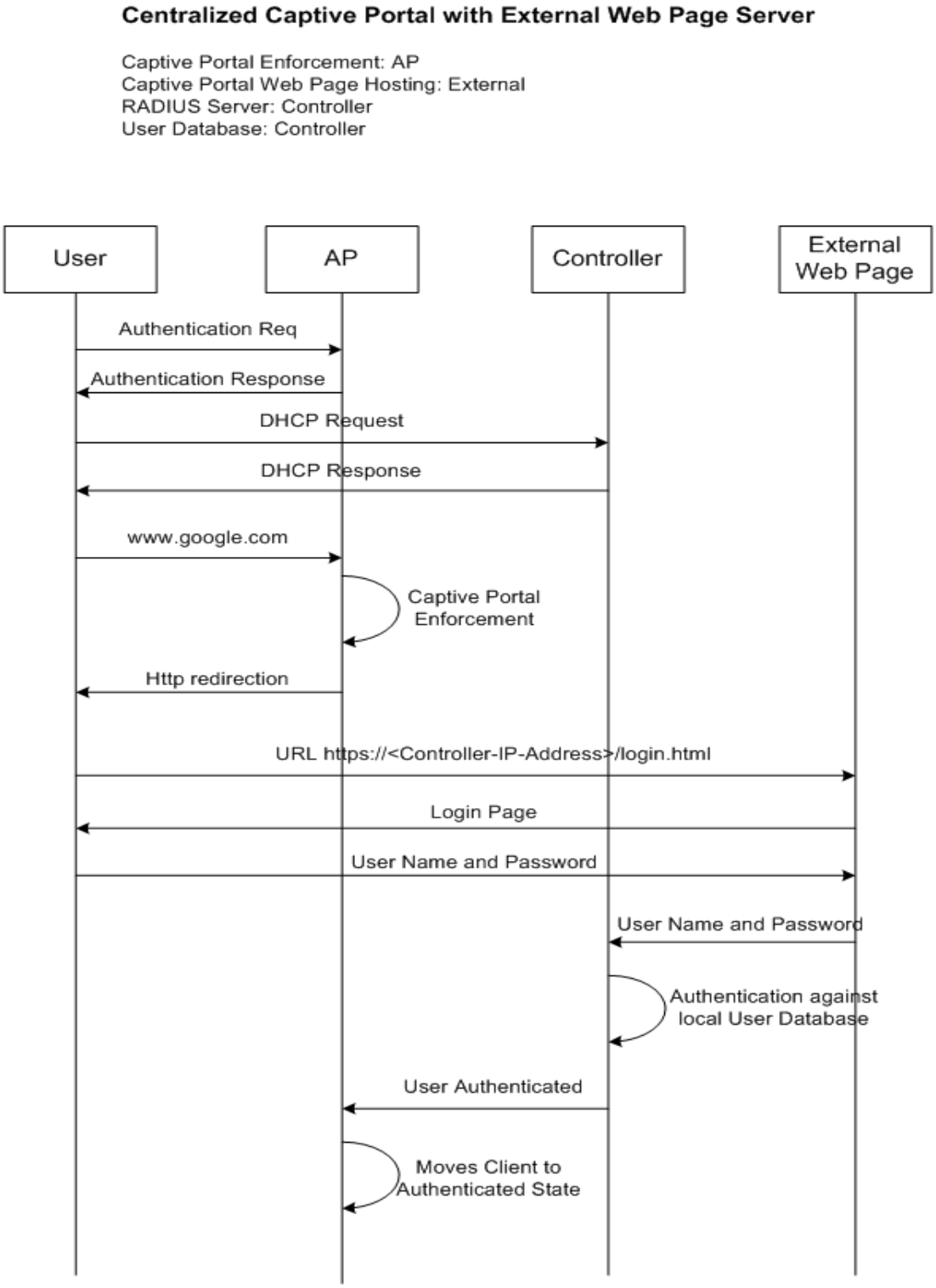
User Database

The user database is also stored in the controller.

The figure below depicts the message of this deployment model.



Message Flow



Configuring External Web Page

An external web server will provide capture and redetection to fully customized Login, Failed and Welcome pages hosted on an external web server.

Advanced pages are hosted on an external HTTP server and support full customization. Using standard HTML authoring tools, administrators or web designers can create fully customized Login, Failed and Welcome pages and host the content on external servers locally at the site in a NOC. External pages can support any HTML compliant content supported by the external web server including client and server extensions.

Including the HTML scripts for passing user name and password back to the Controller

One of the important aspects to keep in mind while deploying external web pages is to include the HTML scripts required to pass the user name and password to the controller. One can see from the message flow figure above that the external web page server sends the user name and password to the controller through the HTML Post method.

Including the POST method script to pass user name and password to controller

To look at the source code of the HTML post method, the internal login.html should be downloaded. Please follow the following steps to download the internal login.html file.

a. Create a Captive Portal Policy with web page option as internal

b. Under the context: operations->File Transfers

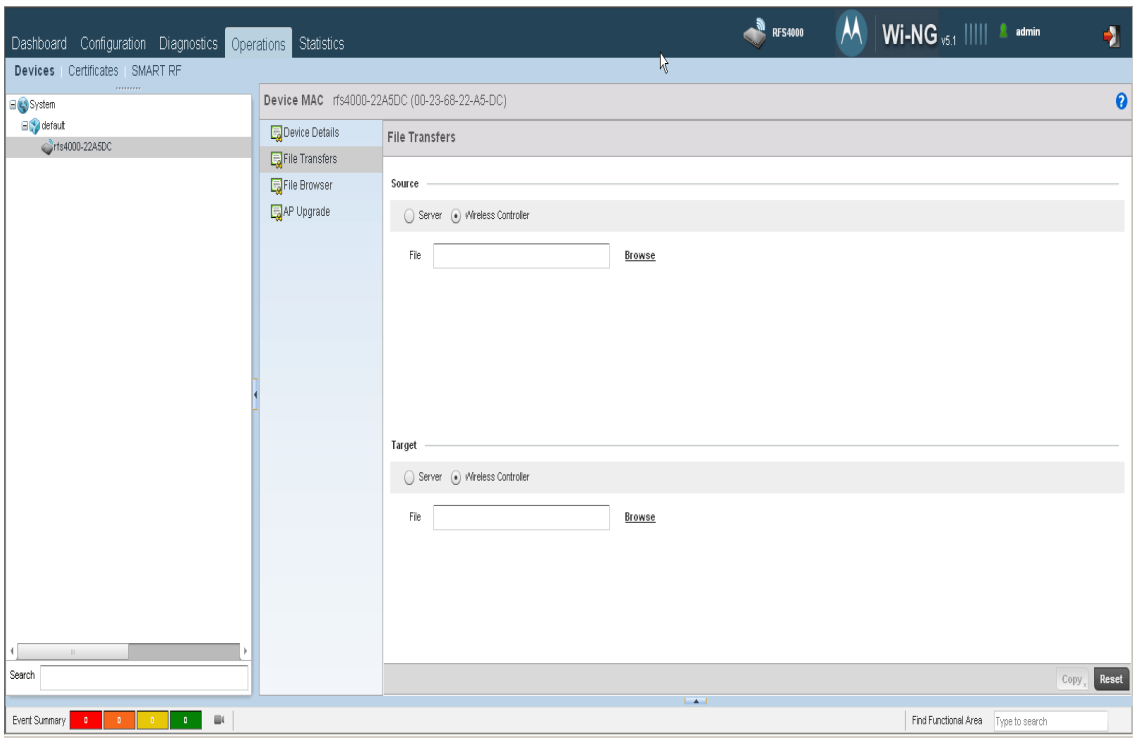
Select ‘Wireless Controller’ as Source

Click Browse

Under flash, select hotspot

Select the captive portal policy that you created (Mot-Hotspot)

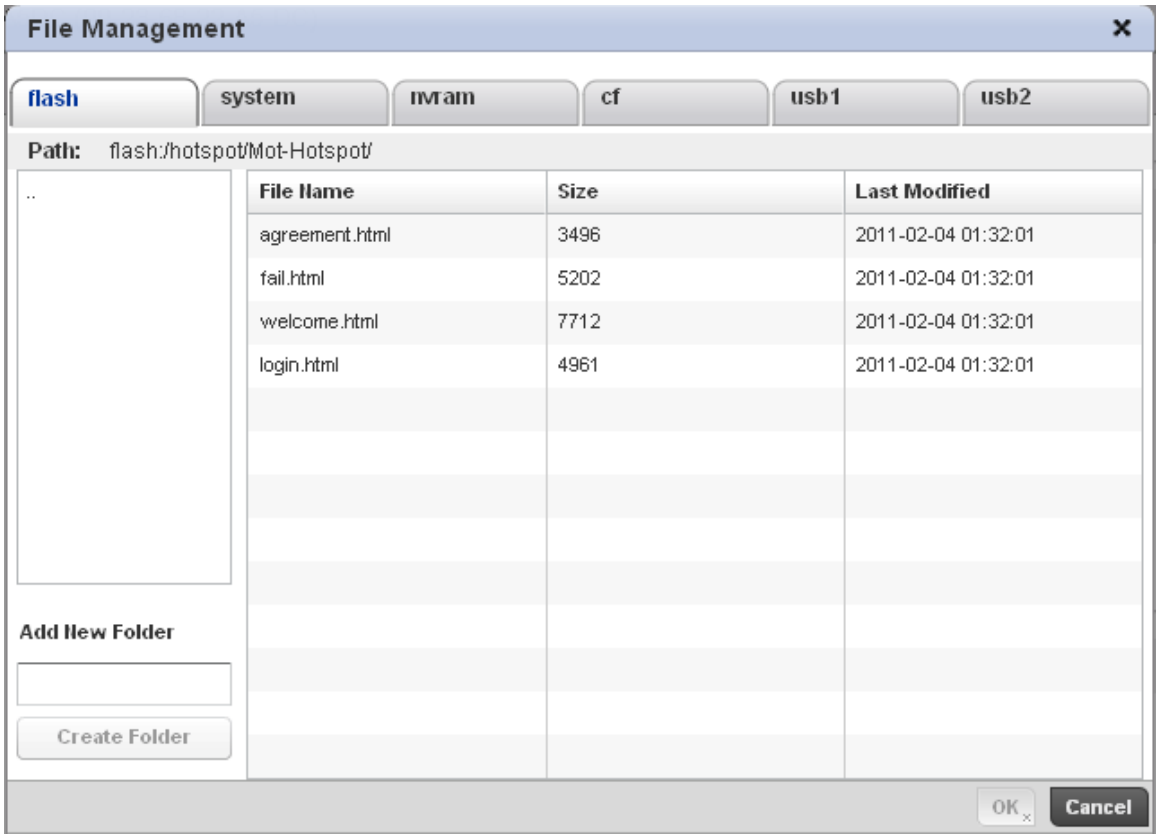
Click the login.html and select ok



c. Select ‘Server’ as the target

To download using FTP / TFP click Advanced

Download the file



Once the login.html is downloaded, open it in a browser and view the source. To view the source in Internet Explorer go to view->source.

The last section of the source code has a Javascript to post the user name and password to the controller. This script should be included in the external web page to post the user name and password back to the controller.

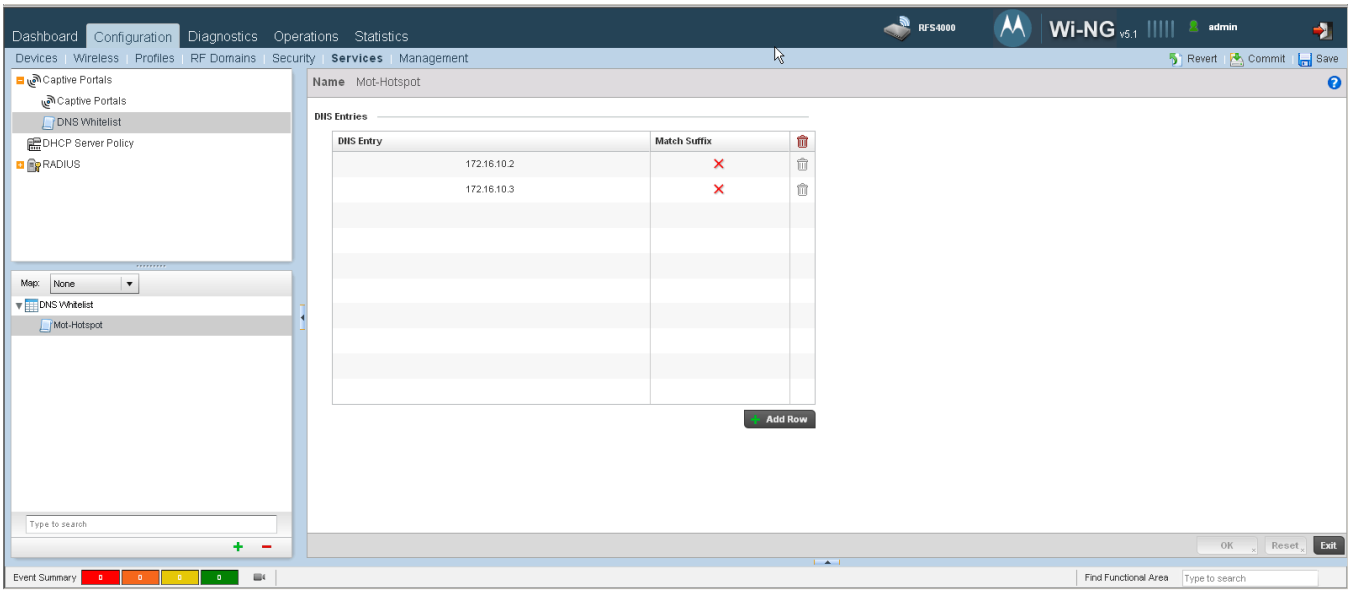
```
-------------------------------------------------------------------------------
<script language=javascript>
var hs_server = "NONE";
var port = 880;
var postToUrl = "/cgi-bin/hslogin.cgi";
hs_server = getQueryVariable("hs_server");
Qv = getQueryVariable("Qv");
postToUrl = ":" + port + postToUrl;

document.getElementById("f_hs_server").value = hs_server
document.getElementById("f_Qv").value = Qv
document.getElementById("frmLogin").action = "http://" + hs_server + postToUrl;
</script></body>
</html>
-------------------------------------------------------------------------------
```

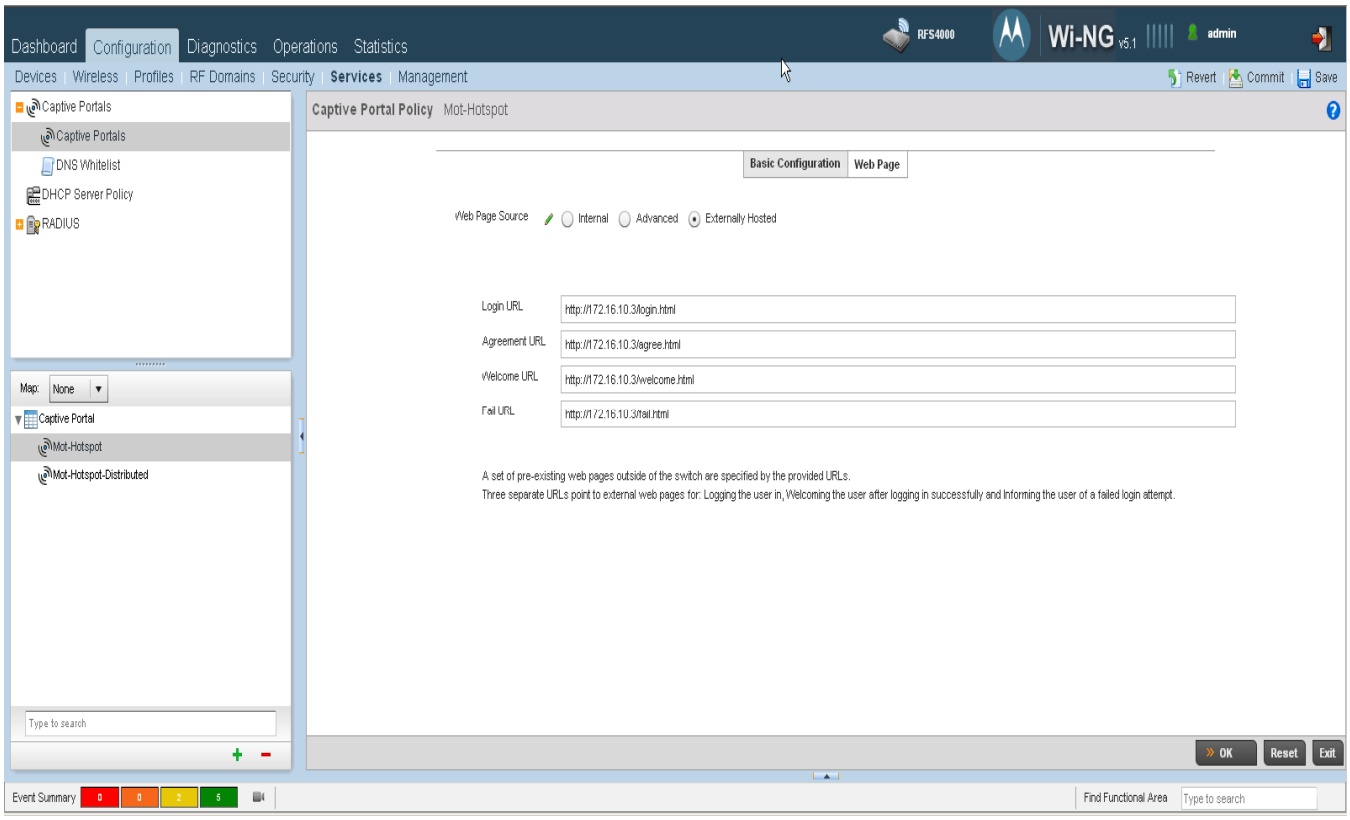
Configuration Steps for External Web pages

The configuration steps is the same as above except

1) In step 2b while creating DNS Whitelist also add the external web server in the allow list



2) In step 3b, select the web page source as ‘external’ instead of internal and input the URL of the externally stored html pages



CONFIGURATION STEPS SUMMARY

1) Create AAA Policy

   RADIUS Server configuration

2) Create DNS Whitelist

   List of IP Addresses to allow when the client gets connected to the Wireless network. If using internal web page, the IP address of the controller should be added in the allow list. If using external web page, the external server's IP address should be added

3) Create Captive Portal Policy

   Configure the captive portal server

   Attach AAA Policy

Attach DNS-Whitelist policy

Configure web page source

4) Create RADIUS Group Policy

Map the required SSID

5) Create RADIUS User Pool

Map the required groups and user settings

6) Create RADIUS Server Policy

Map the Radius Group and the User pools

7) Configure DHCP Server for the Wireless hotspot users

8) Map RADIUS Server, DHCP Server and Captive Portal policy in rfs4000 profile

9) Create WLAN and configure captive portal policy

10) Map WLAN to radios

DEPLOYMENT MODEL – 3: DISTRIBUTED CAPTIVE PORTAL SERVER WITH EXTERNAL PAGES AND RADIUS

This model describes how APs act as the captive portal server with external web pages.

Captive Portal Server

The AP acts as the Captive Portal Server.

Captive Portal Pages

The redirection web pages are stored in an external server.

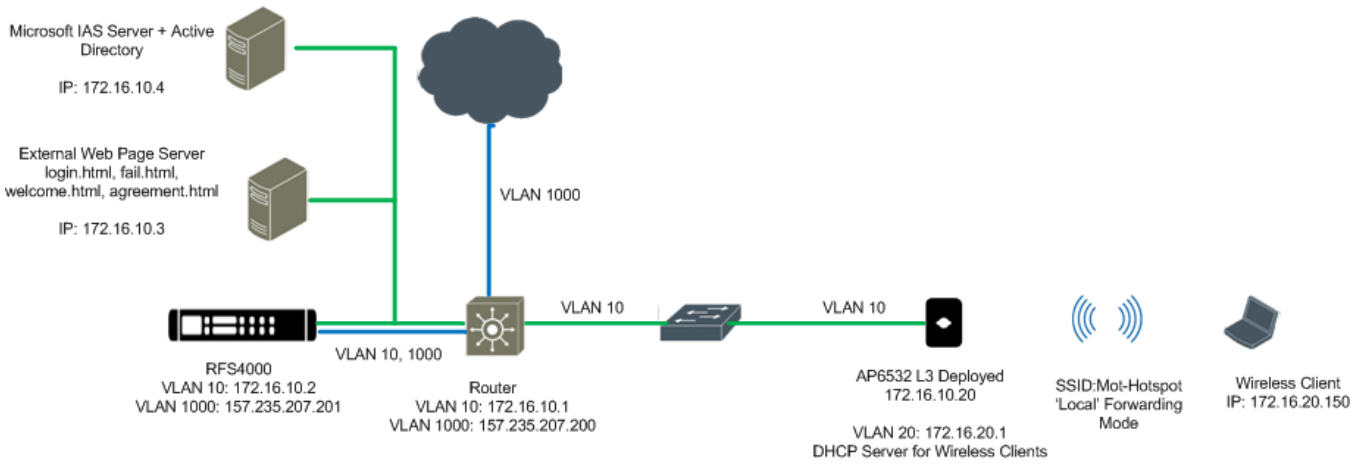
RADIUS Server

An external RADIUS server is used (MS IAS).

User Database

An external LDAP Server is used (MS AD).

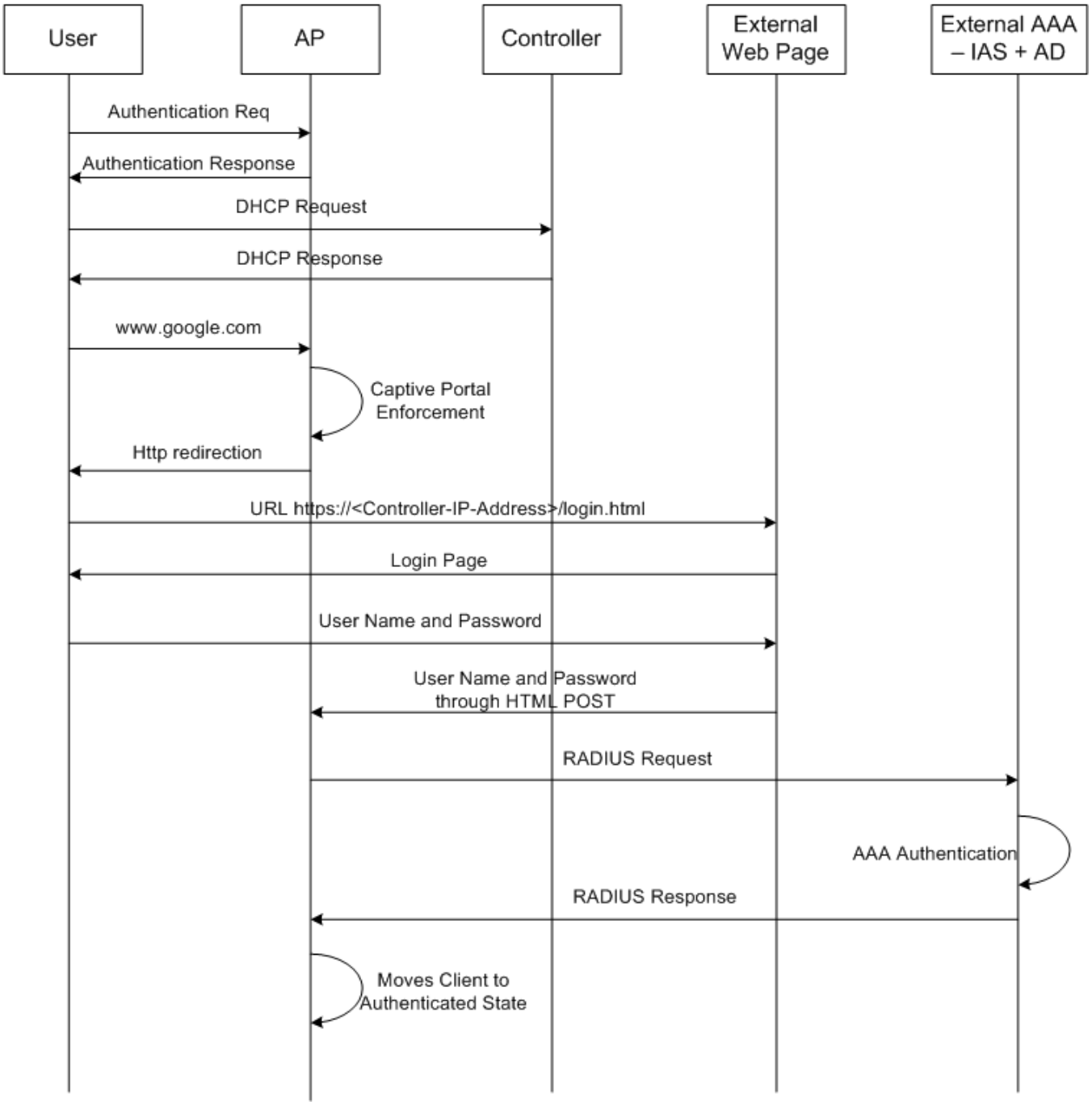
The figure below depicts the message of this deployment model.



Message Flow

Distributed Captive Portal with External Web Page Server

Captive Portal Enforcement: AP
Captive Portal Web Page Hosting: External
RADIUS Server: External AAA - IAS
User Database: External LDAP - AD



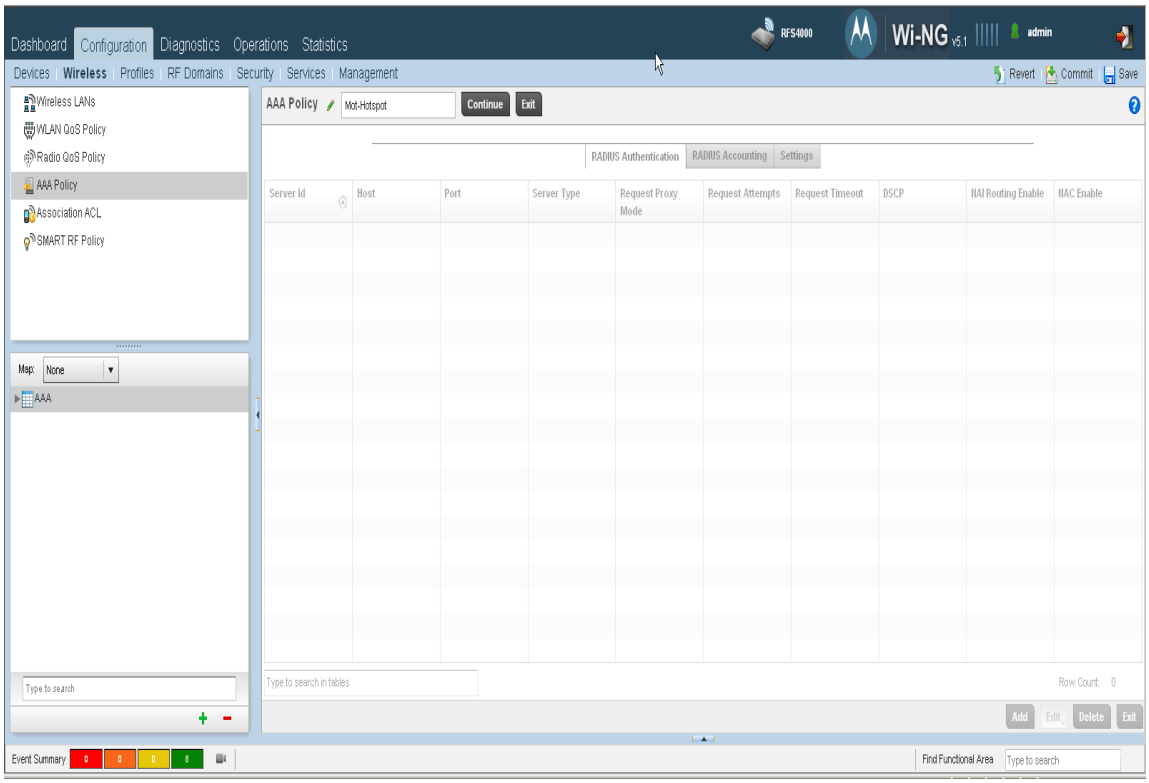
Configuration Steps

The configuration steps are very similar to the deployment scenario-1 except for a few changes.

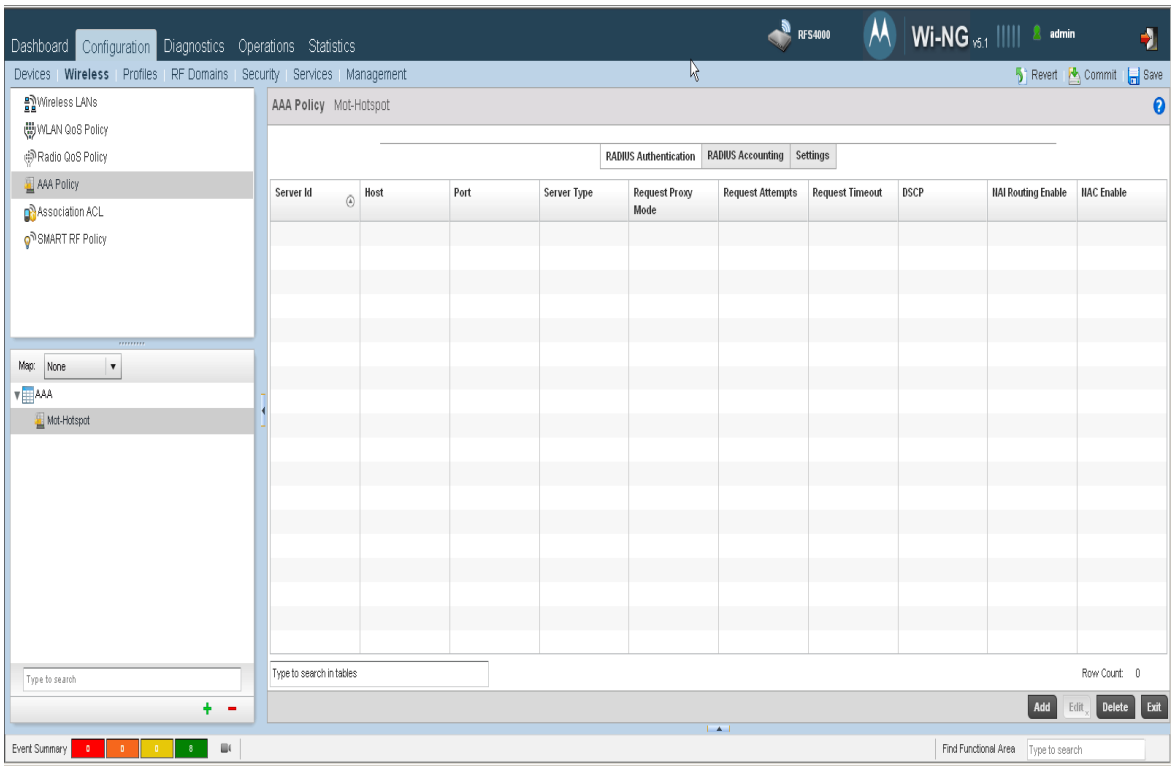
1) Create AAA Policy

a. Under the context: Configuration->Wireless->AAA Policy, click ‘Add’

Enter the AAA Policy Name and click ‘Continue’



b. Add RADIUS server by clicking ‘Add’



a. Add RADIUS server by clicking ‘Add’

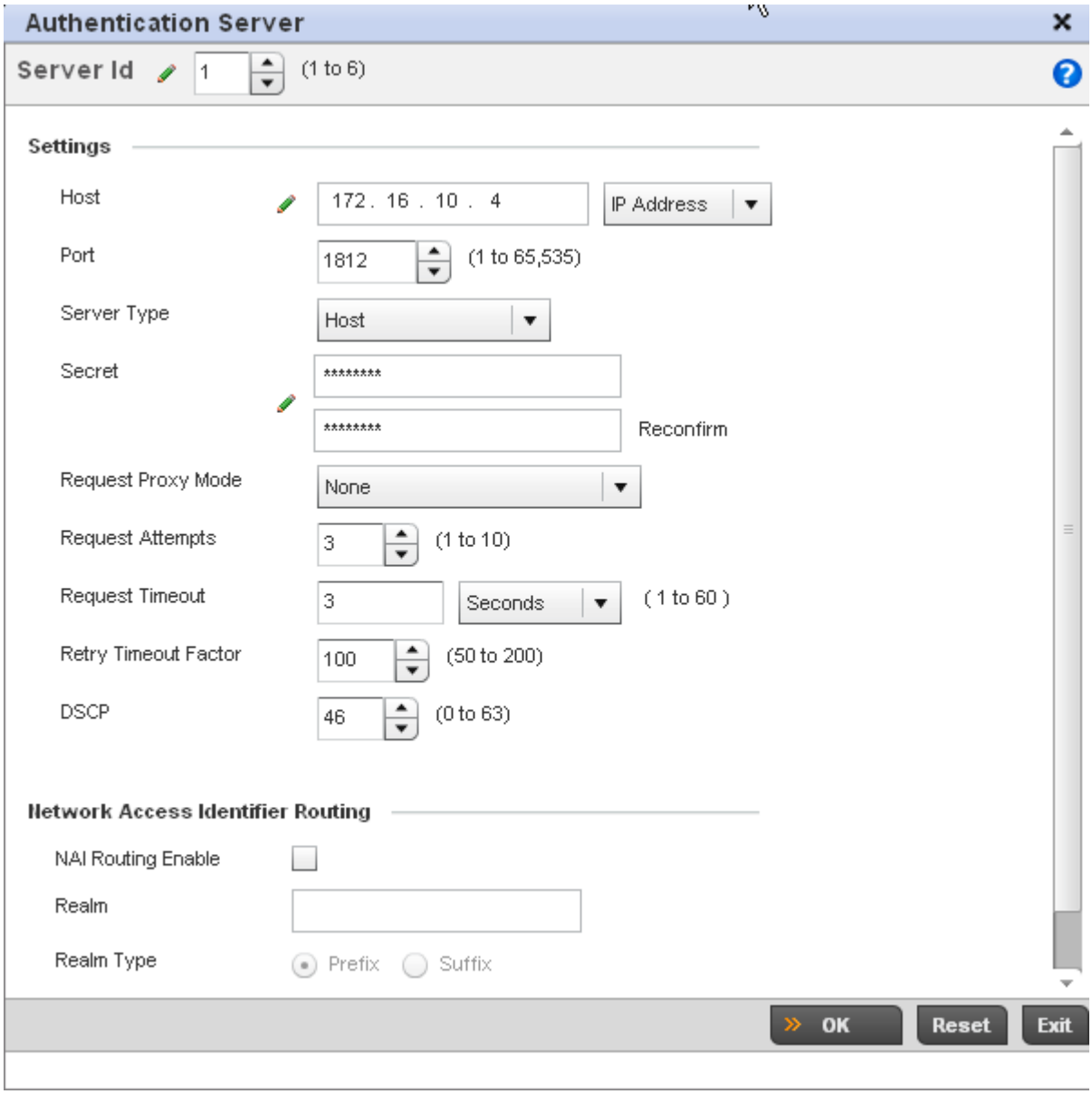
Enter the ‘Server Id’

Enter the IP Address of the external AAA Server (172.16.10.4)

Select ‘Server Type’ as ‘host’

Enter the secret

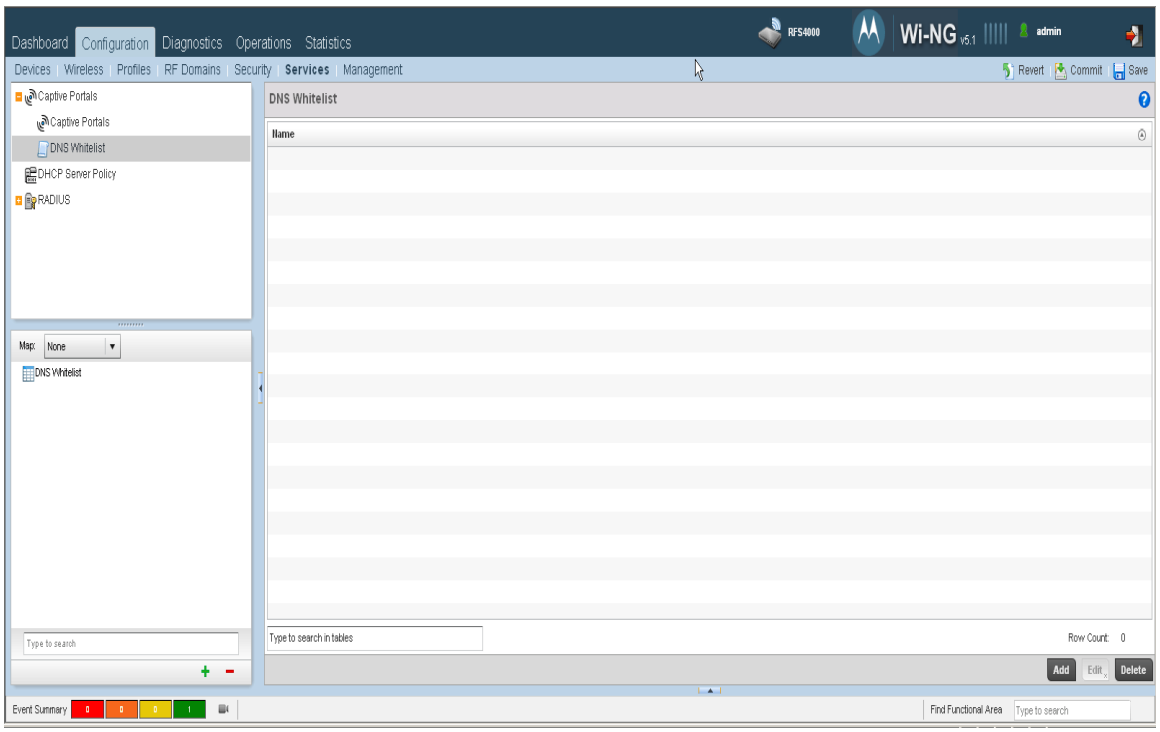
Click ‘OK’



2) Create DNS Whitelist

a. Under the context: Configuration->Services->Captive Portals->DNS Whitelist, click ‘Add’

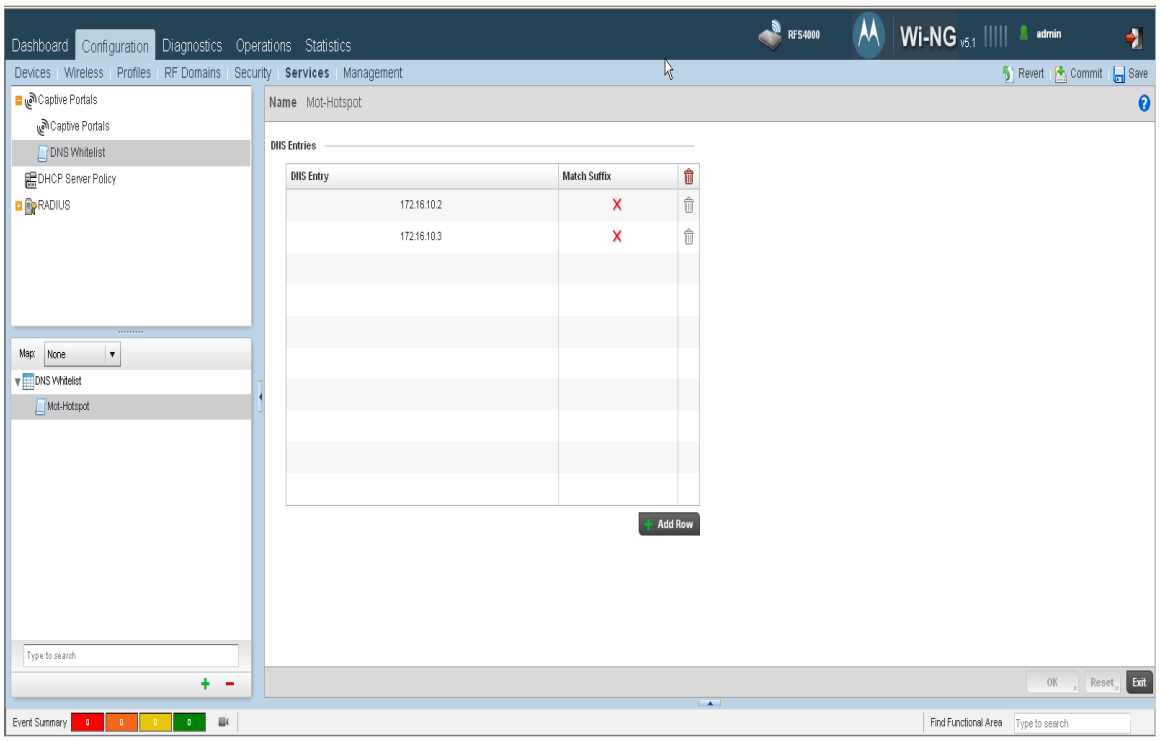
Enter a name for the DNS Whitelist



b. Click ‘Add Row’

Enter the list of IP address that you want to grant access even if the client is not authenticated.

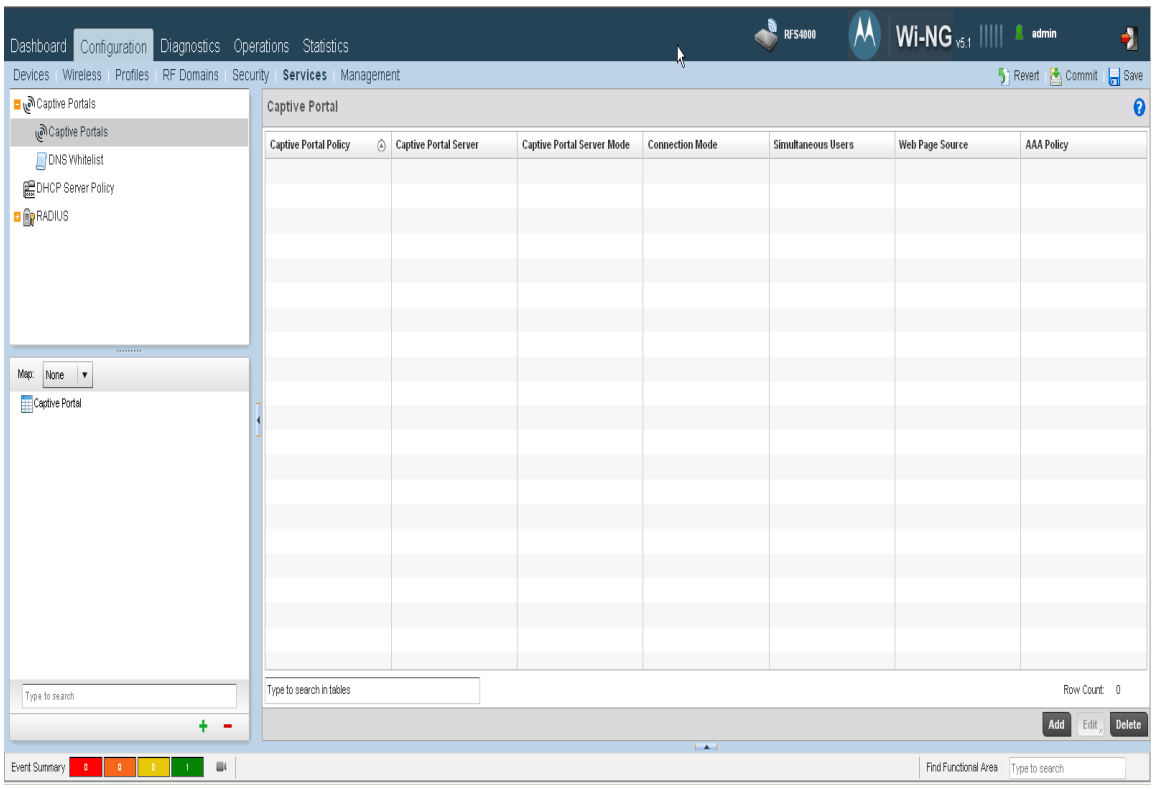
Click ‘OK’



Note: Since we are using the external server to host the pages, we should allow the client to access to the external server's IP Address used to host the pages. In this example the external server IP Address is 172.16.10.3, so we are allowing access to the external server.

3) Create Captive Portal Policy

a. Under the context: Configuration->Services->Captive Portals->Captive Portals, click 'Add'



Enter the Captive Portal Policy Name

Set ‘Captive Portal Server Mode’ to ‘Internal (self)’

Set ‘Simultaneous Users’ to 100

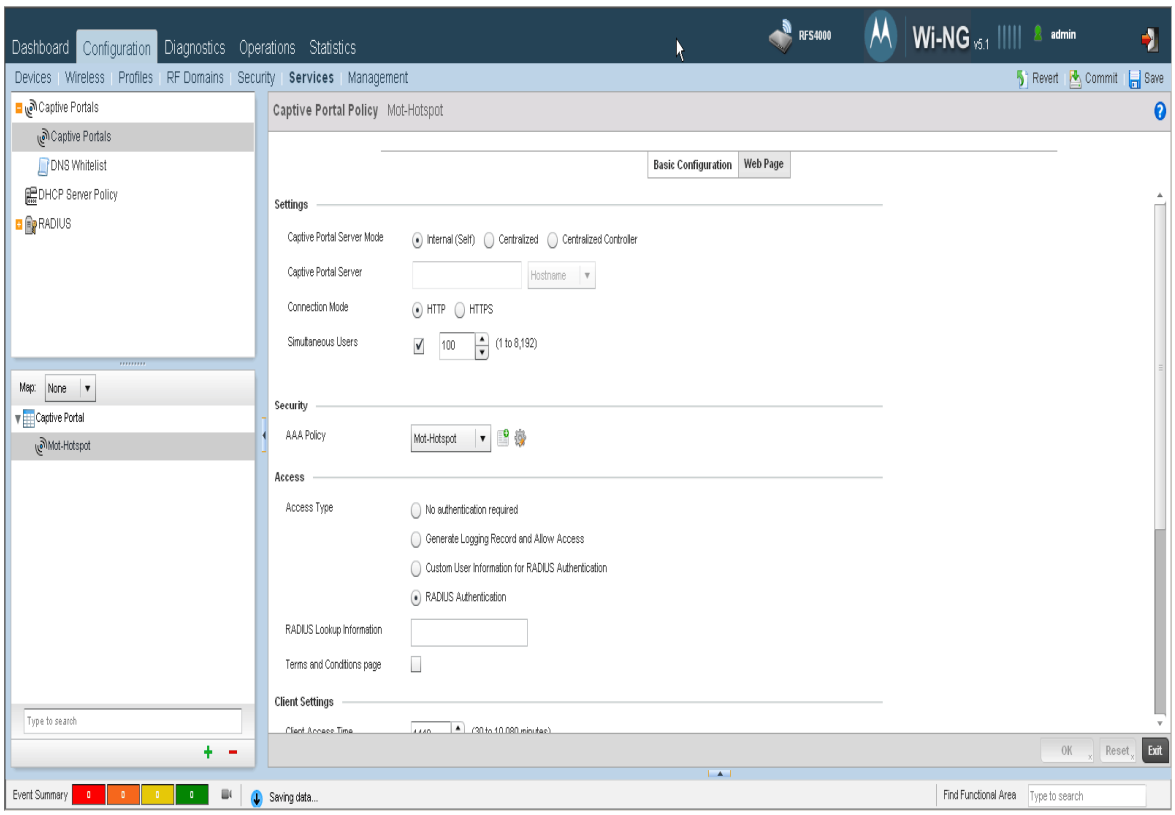
Set AAA Policy to ‘Mot-Hotspot’ (created in Step 1)

Set Access Type to ‘Radius Authentication’

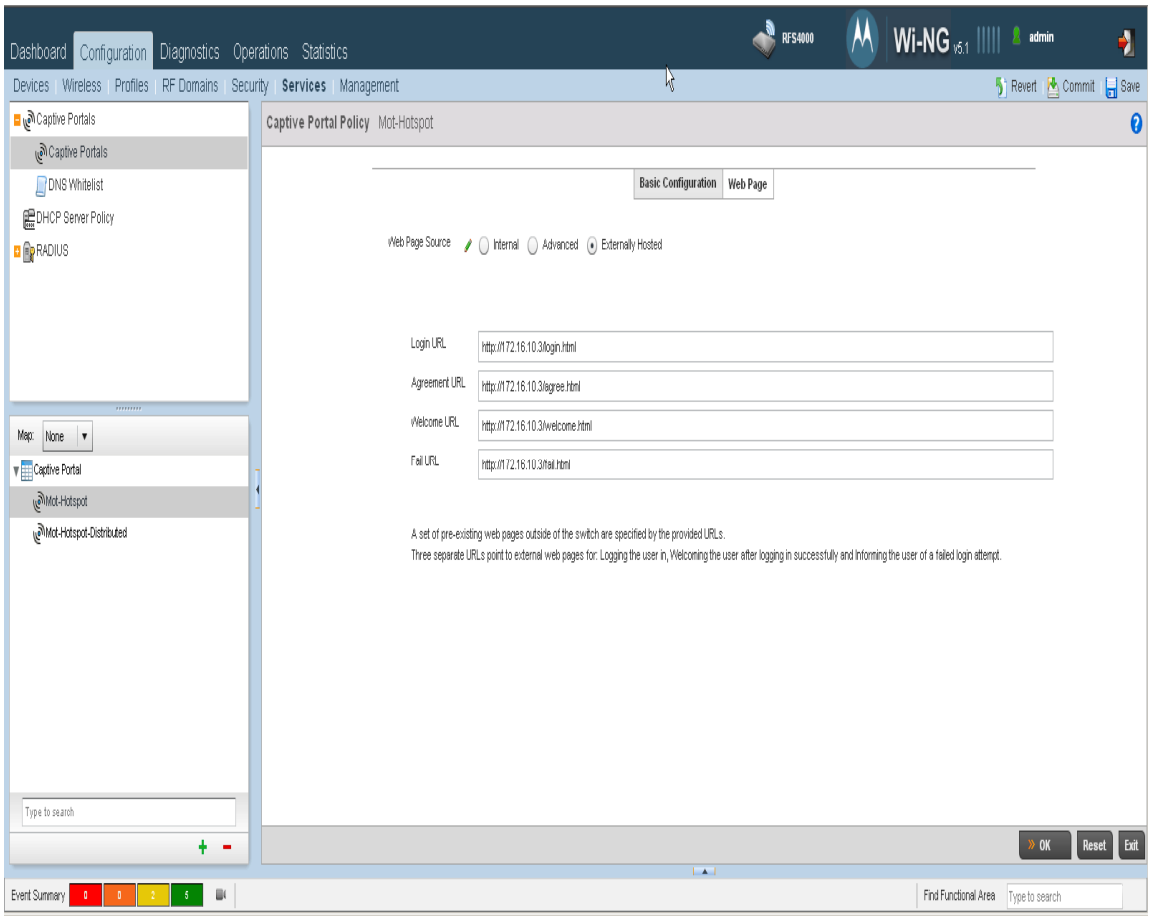
Set DNS Whitelist to ‘Mot-Hotspot’ (created in Step 2)

Click ‘OK’

,



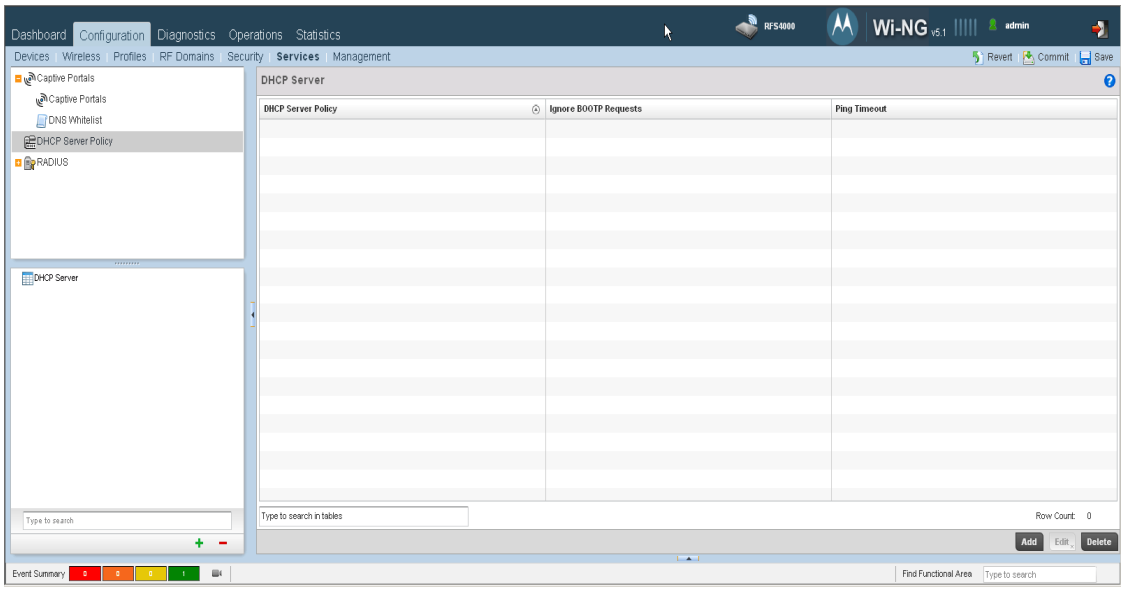
b. On the ‘Web Page’ tab ensure the ‘Web Page Source’ is set to ‘External’



4) Create VLAN 20 for Wireless Hotspot Users and set the IP Address of the VLAN 20 interface in the AP as 172.16.20.1

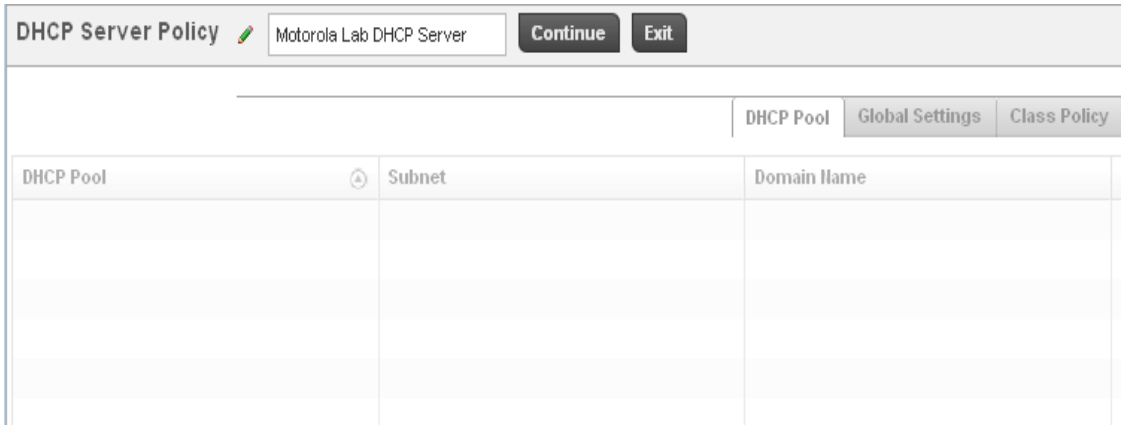
5) Create DHCP Server Policy to give IP address on VLAN20 for Wireless Hotspot Users

   a. Under the context: Configuration->Services->DHCP Server Policy, Click ‘Add’

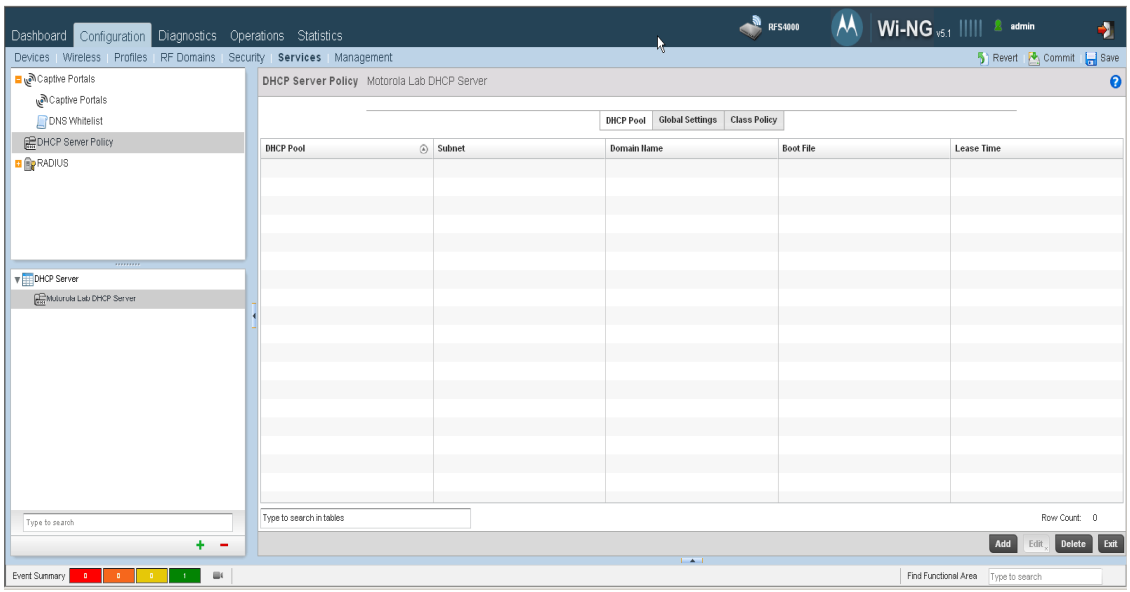


Set ‘DHCP Server Policy Name’

Click ‘Continue’



b. Under the context of newly created DHCP Server Policy, Click ‘Add’ to create a DHCP pool



Set ‘DHCP Pool’ name

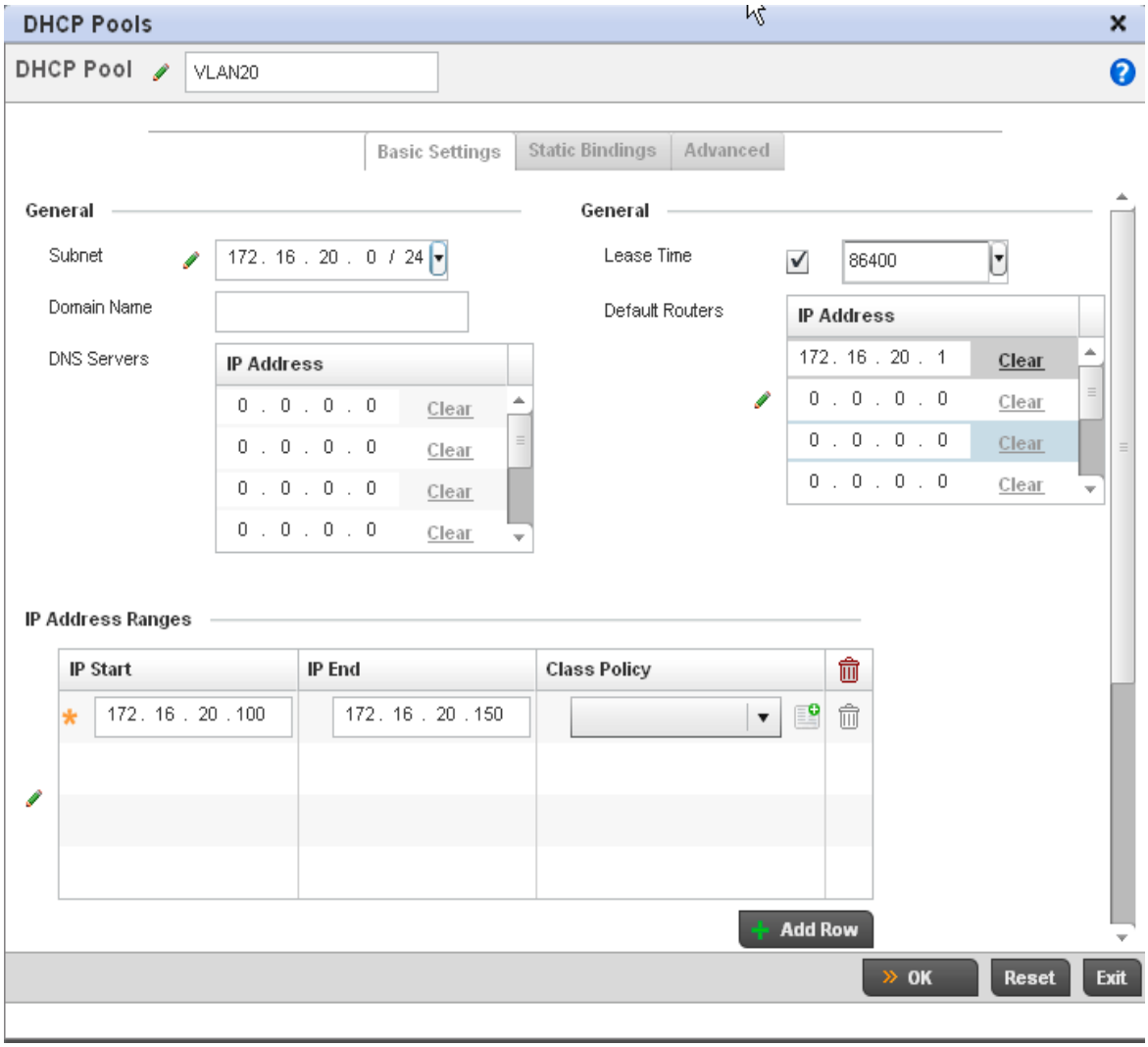
Set ‘Subnet’ to VLAN 20 subnet – 172.16.20.0/24

Set ‘Default Routers’ to VLAN 20 interface IP address – 172.16.20.1

Under ‘IP Address Range’ Click ‘Add Row’

Enter the range of IP Addresses – 172.16.20.100 to 172.16.20.150

Click ‘OK’



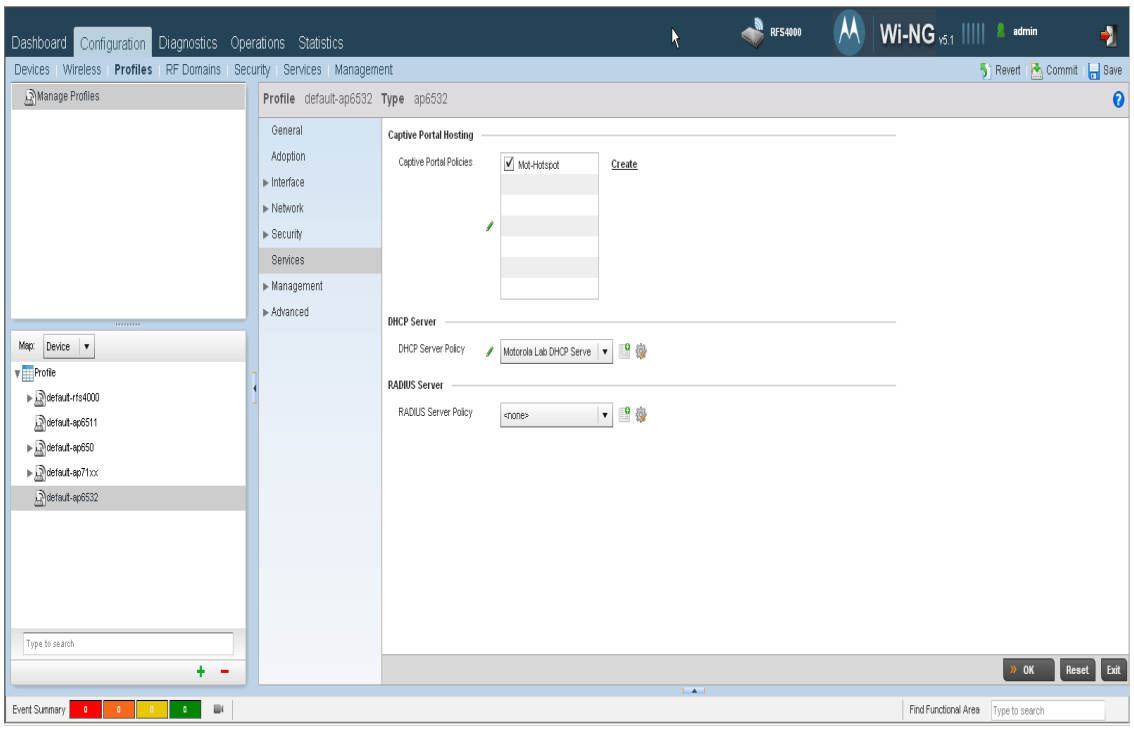
6) Map DHCP Server and Captive Portal policy in ap6532 profile

a. Under the context: Configuration->Profiles->Profile->default-ap6532->services

Set ‘Captive Portal Policies’ to ‘Mot-Hotpot’ (created in Step 3)

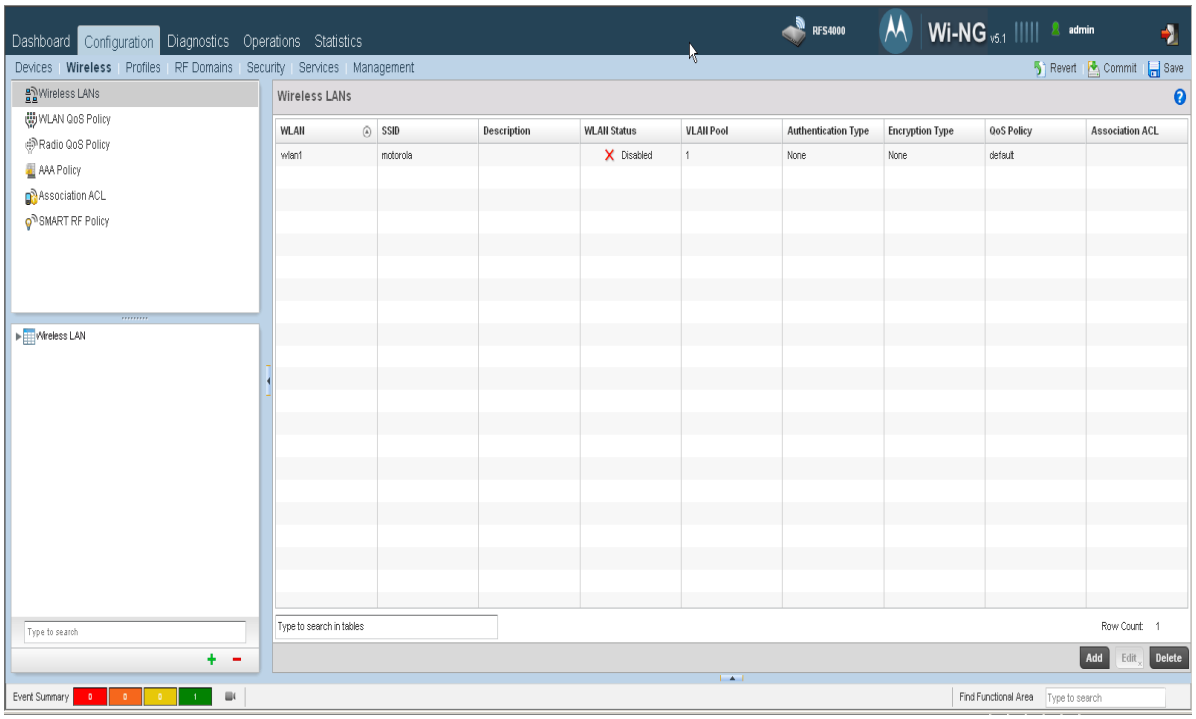
Set ‘DHCP Server Policy’ to ‘Motorola Lab DHCP Server’ (created in Step 5)

Click ‘OK’



7) Create WLAN for Hotspot

a. Under the context: Configuration->Wireless->Wireless LANs, click ‘Add’



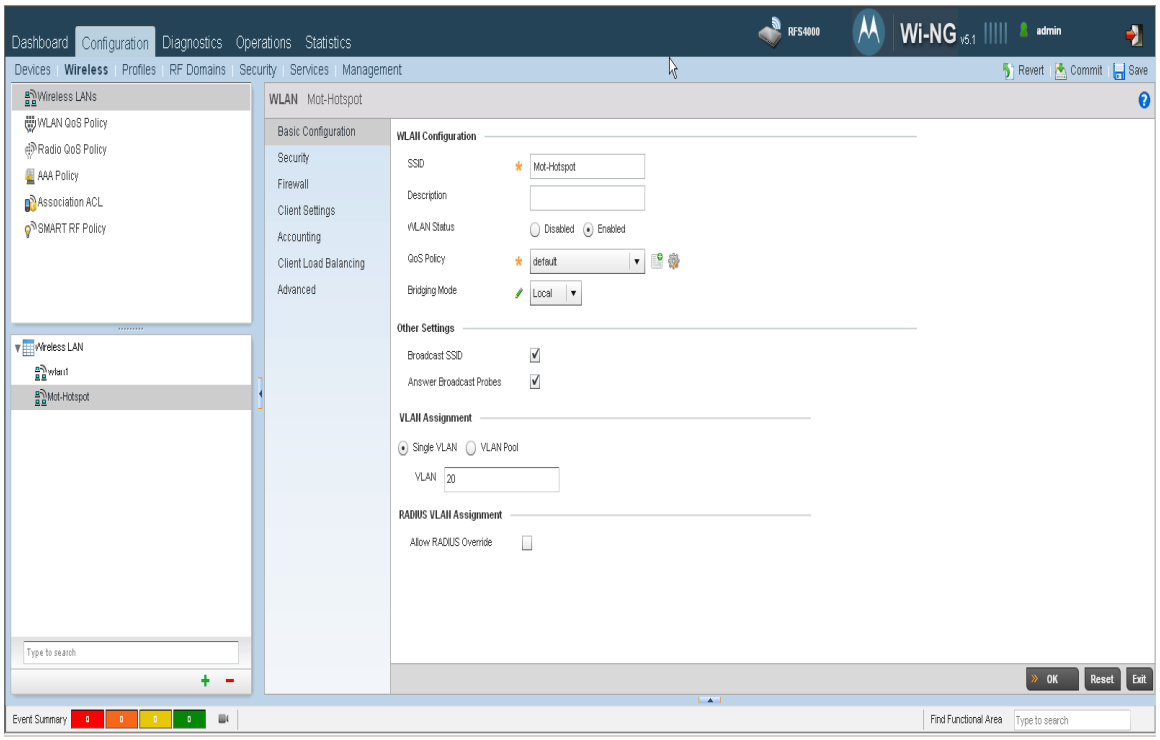
Set ‘WLAN’ name

Set ‘SSID’ – this should match the one you entered in Step 4b

Set ‘Bridging Mode’ to ‘Local’

Set ‘VLAN’ to ‘20’

Click ‘OK’

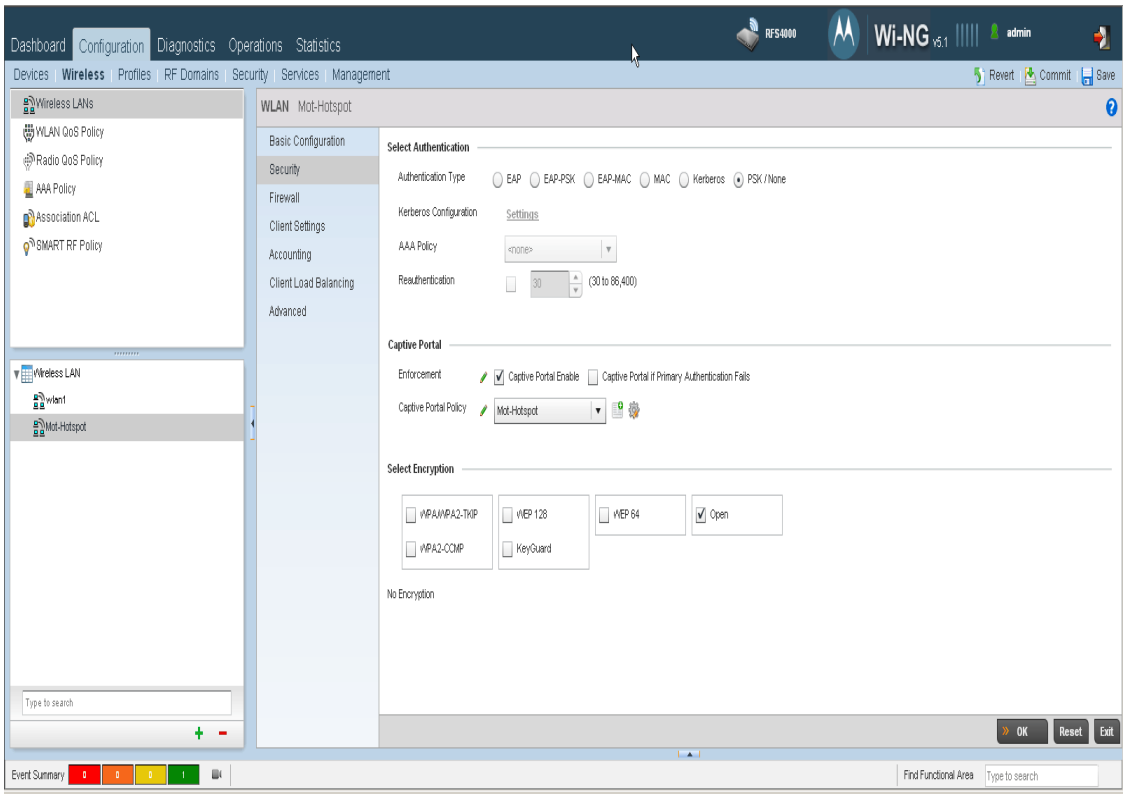


b. Under the Security Menu of the newly created WLAN

Set ‘Enforcement’ to ‘Captive Portal Enable’

Set ‘Captive Portal Policy’ to ‘Mot-Hotspot’ (created in Step 3)

Click ‘OK’



8) Map WLAN to radios of the AP6532 profile