WiNG5 DESIGN GUIDE By Sriram Venkiteswaran

WING5 CAPTIVE PORTAL DESIGN GUIDE

June, 2011

TABLE OF CONTENTS HEADING STYLE

Introduction To Captive Portal	1
Overview	1
Common Applications	1
Authenticated Visitor Access:	1
Authenticated Private Access:	2
Paid Internet Access:	3
Hotspot Authentication Process:	4
Hotspot Components	5
Deployment Scenarios	7
Deployment Model – 1: Centralized Captive Portal Server With Internal Pages	7
Message Flow	8
Configuration Steps	9
Deployment Model – 2: Centralized Captive Portal Server with External Pages	30
Message Flow	31
Configuring External Web Page	32
Configuration Steps for External Web pages	35
Configuration Steps Summary	36
Deployment Model – 3: Distributed Captive Portal Server with External Pages And RADIUS	37
Message Flow	38
Configuration Steps4	10

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.
- 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.
- 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.



DHCP Server: VLAN 20

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

Centralized All Internal Solution

Captive Portal Enforcement: AP Captive Portal Web Page Hosting: Controller RADIUS Server: Controller User Database: Controller



Configuration Steps

- 1) Create AAA Policy
 - a. Under the context: Configuration->Wireless->AAA Policy, click 'Add'

Enter the AAA Policy Name and click 'Continue'

Dashboard Configuration Diagnostics Ope	rations Statisti					🔷 R ⁱ	=54000 M	Wi-NG v6.	. 2 admin	-1
Devices Wireless Profiles RF Domains Sec	urity Services	Management			4				灯 Revert 🛃	🖢 Commit 🛛 🔚 Save
Mireless LANs	AAA Policy 🥖	Mot-Hotspot	Continue	ixit						0
WLAN QoS Policy										
Radio GoS Policy				RADI	US Authentication R/	ADIUS Accounting Se	ettings			
🚆 AAA Policy	Server Id	Host	Port	Server Type	Request Proxy	Request Attempts	Request Timeout	DSCP	NAI Routing Enable	NAC Enable
Resociation ACL		(Å)			Mode					
PSMART RF Policy										
Map: None V										
▶AAA	•									
	-									
Type to search	Type to search in ta	bles								Row Count: 0
+ -									Add	lit _x Delete Exit
Event Summery 0 0 0 0					-	▲		Find Function	nel Area Turo in anno	-la

b. Add RADIUS server by clicking 'Add'

Dashboard Configuration Diagnostics Ope	erations Statist	tics			X	🔷 R	=S4000	Wi-NG 😽	.1 2 admir	e 🚽
Devices Wireless Profiles RF Domains Sec	curity Services	Management			42				5) Revert	👆 Commit । 📊 Save
B Wireless LANs	AAA Policy M	/lot-Hotspot								0
WLAN QoS Policy										
Radio QoS Policy				RAD	IUS Authentication R	ADIUS Accounting Se	ttings			
aAA Policy	Server Id	Host	Port	Server Type	Request Proxy	Request Attempts	Request Timeout	DSCP	NAI Routing Enable	NAC Enable
Association ACL		•			Mode					
on SMART RF Policy										
Map: None v										
V AAA										
🚆 Mot-Hötspot	-									
Type to search	Type to search in ta	ables								Row Count: 0
+ -									Add	dit _x Delete Exit
Event Summery					l.	▲ T		Find Function	onal Area Type to sear	ch

Enter the 'Server Id'

Select 'Server Type' as 'onboard-controller'

Authentication Serv	/er	×
Server Id 🥒 1	(1 to 6)	0
Settings		Ê
Host	Hostname	
Port	1812 (1 to 65,535)	
Server Type	✓ onboard-controller	
Secret		
Request Proxy Mode	None 🗸	
Request Attempts	3 (1 to 10)	
Request Timeout	3 Seconds V (1 to 60)	=
Retry Timeout Factor	100 (50 to 200)	
DSCP	46 🔹 (0 to 63)	
Network Access Identifi	er Routing	
NAI Routing Enable		
Realm		
Realm Type	Prefix Suffix	
Strip Realm		Ţ
	» OK Reset	Exit

2) Create DNS Whitelist

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

Enter a name for the DNS Whitelist

Dashboard Configuration Diagnostics Ope	rations Statistics		🔷 RF54000	Wi-NG _{v5.1} & admin 🚽
Devices Wireless Profiles RF Domains Secu	rity Services Management	Ŕ		튓 Revert 🛛 📩 Commit : 🔚 Save
🗖 @Captive Portals	DNS Whitelist			0
Portals	Name			6
DNS Whitelist				0
EDHCP Server Policy				
🖬 📴 RADIUS				
Marr None v				
DNS Whitelist				
	•			
	-			
	Type to search in tables			Row Count 0
Type to search	The examplification			NOW COOL
+ -				Add Edit _x Delete
Event Summary 0 0 0 1		1		Find Functional Area Type to search

b. Click 'Add Row'

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

me 🖋 Mot-Hotspot		
S Entries		
DNS Entry	Match Suffix	Û
★ 172.16.10.2	No	· 💼

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'

Dashboard Configuration Diagnostics Ope	erations Statistics			•	RF54000	Wi-NG _{v5.1}	admin 🚽	
Devices Wireless Profiles RF Domains Secu	urity Services Manageme	nt		.0		51	Revert 📩 Commit 🔚 S	Save
🗖 🖓 Captive Portals	Captive Portal							0
്രി Captive Portals	Captive Portal Policy	Captive Portal Server	Captive Portal Server Mode	Connection Mode	Simultaneous Users	Web Page Source	AAA Policy	
DNS Whitelist								
EDHCP Server Policy								
🖬 😭 RADIUS								
Map: None V								
Captive Portal	4							
	1							
Type to search	Type to search in tables						Row Count: 0	
+ -							Add Edit _x Del	elete
Event Summary 0 0 0 1 🖬						Find Functional Area T	ype to search	

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)

Captive Portal Policy 🥖	Mot-Hotspot
	Basic Configuration Web Page
Settings	
Captive Portal Server Mode	🖋 🔵 Internal (Self) 💿 Centralized 🔘 Centralized Controller
Captive Portal Server	✓ 172.16.10.2 IP Address
Connection Mode	• HTTP O HTTPS
Simultaneous Users	 100 (1 to 8,192)
Security	
AAA Policy	🖌 Mot-Hotspot
Access	
Access Type	No authentication required
	Generate Logging Record and Allow Access
	Custom User Information for RADIUS Authentication
	RADIUS Authentication
RADIUS Lookup Information	
Terms and Conditions page	
I	
Client Settings	
Client Access Time	1440 (30 to 10,080 minutes)
Inactivity Timeout	10 Minutes 🗸 (5 to 30)
DNS Whitelist	
DNS Whitelist 🥒	Mot-Hotspot
Accounting	
Enable RADIUS Accounting	
Enable Syslog Accounting	
Syslog Host	Hostname
Syslog Port	514

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

		В	Basic Configuration	Web Pag	e			
Web Page Source 💽	nternal 🔘 Advanced 🔵 Ext	ernally Ho	osted					
		Login	Terms and Condi	tions We	lcome	Fail		
Title Text	Guest User Login Page							
Header Text	Welcome to Guest User Wireless	s LAN Ser	rvice					
Login Message	Please enter the username and p	bassword	d provided to you wher	n you signed	in at the 1	ront desk.		
Footer Text	Please contact the front desk if	/ou have i	not been issued a use	rname and p	assword.			
Main Logo URL								
Small Logo URL								

4) Create RADIUS Group Policy

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

Dashboard Configuration Diagnostics Ope	erat	ions Statistics				🔷 RFS4000	M Wi	i-NG _{v5.1}	🤱 admin 🚽
Devices Wireless Profiles RF Domains Secu	urity	/ Services Manageme	nt		4			5	Revert 📥 Commit 🔚 Save
■ @Captive Portals		RADIUS Group							6
ര്യ Captive Portais		RADIUS Group Policy	Guest User Group	Management Group	Role	VLAII	Time	e Start	Time Stop
DNS Whitelist									
BDHCP Server Policy									
C RADIUS									
RADI IS Group									
	4								
	-								
Type to search		Type to search in tables							Row Count: 0
+ -									Add Edit _x Delete
Event Summery					1.4.1			Find Functional Area	Type to search

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'

RADIUS Group Poli	V / Mot-Hotspot		0
Settings		Schedule	_
Guest User Group		Time Start 12 + 0 + 0 AM O PM	
VLAN ,		Time Stop 11 🐳 : 59 🐳 🔾 AM 💿 PM	
WLAN SSID	Mot-Hotspot	Days Monday Tuesday Vlednesday	
Rate Limit from Air	100 (100 to 1,000,000 kbps)	Thursday	
Rate Limit to Air	100 (100 to 1,000,000 kbps)	Friday	
Management Group		Saturday	
Access		Sunday	
Role	v		
		» OK Reset	Exit

5) Create RADIUS User Pools

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

Dashboard Configuration Diagnostics Ope	erations Statistics	k	🔷 RFS4000	ᄊ 🛛 🗰 🔥 🕺 🕺 Wi-NG v5.1
Devices Wireless Profiles RF Domains Secu	urity Services Management			5 Revert 📐 Commit 🕁 Save
Captive Portals هي 🖻	RADIUS User Pool			0
്ര Captive Portals	User Pool			0
DNS Whitelist				0
EDHCP Server Policy				
RADIUS				
🕵 Groups				
🙆 User Pools				
Server Policy				
RADUS User Pool				
1111 1				
	4			
	-			
		1		2
Type to search	Type to search in tables			Row Count: U
+ -				Add Edit, Delete
Event Summery 0 0 0 1 🔤				Find Functional Area Type to search

Enter 'User Pool' name

Click 'Continue'

Dashboard Configuration Diagnostics Ope	erations Statistics			k _	🗞 RFS4000 – 🔼	Wi-NG v5.1	admin 🊽
Devices Wireless Profiles RF Domains Secu	irity Services Manageme	nt		,		51	Revert 💾 Commit 🛛 🔒 Save
Captive Portals 🕼 🗖	User Pool 🥖 Mot-Hotspot	Continue	Exit				0
@Captive Portals						1	
DNS Whitelist	User Id 🛞	Guest User	Group	Start Date	Start Time	Expiry Date	Expiry Time
EDHCP Server Policy							
E 🔐 RADIUS							
🕵 Groups							
🖉 User Pools							
😭 Server Policy							
RADI S Liver Doni							
	4						
	-						
Type to search	Type to search in tables					-	Row Count: 0
+ -							Add <mark>Edit_x Delete Exit</mark>
Event Summary 0 0 0 1						Find Functional Area T	ype to search

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

Dashboard Configuration Diagnostics Ope	rations Statistics				RF54000	Wi-NG _{15.1}	admin 🌖
Devices Wireless Profiles RF Domains Secu	rity Services Manageme	ent		~~		5) F	Revert 🛃 Commit 🔚 Save
🗖 🖉 Captive Portals	User Pool Mot-Hotspot						0
്ര Captive Portals		a			0 T		
DNS Whitelist	User Id (A)	Guest User	Group	Start Date	start lime	Expiry Date	Expiry Time
EDHCP Server Policy							
RADIUS							
🔐 Groups							
🕵 User Pools							
Server Policy							
= PADLIC Hear Dool							
Mil-Brison							
	1						
	-						
Type to search	Type to search in tables						Row Count: 0
+ -							Add Edit, Delete Exit
Event Summary 0 0 0 1						Find Functional Area	ype to search

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

User		×
Userid 🥒 gu	uest1	0
Settings		
Password	Show	
Guest User		
Group	🖋 Mot-Hotspot 🔍 📑 🎆	
Time		
Expiry Date 🔸	04/30/2011 📰 Expiry Time 🜟 5 🚔 : 22 🚔 🔾 AM 💿 PM	
	» OK Reset	Exit

- 6) Create RADIUS Server Policy
 - a. Under the context: Configuration->Services->RADIUS->Server Policy, Click 'Add'

Dashboard Configuration Diagnostics Ope	erations Statistics			🔷 RF54000	Wi-NG van III	💄 admin 🛛 🚽
Devices Wireless Profiles RF Domains Secu	rity Services Management		Å			퇏 Revert : 📐 Commit : 🔚 Save
🗖 🖓 Captive Portals	RADIUS Server					0
്രീ Captive Portals	RADIUS Server Policy	RADIUS User Pools	Authentication Data Source	Local Authentication Type	LDAP Authentication Type	CRL Validation
DNS Whitelist						
E DHCP Server Policy						
RADIUS						
😤 Groups						
🕵 User Pools						
Rever Policy						
Map: Profile v						
RADIUS Server	-					
	1					
Type to search	Type to search in tables					Row Count: 0
+ -				• 1		Add Edit _x Delete
Event Summary					Find Functional Are	a Type to search

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'

RADIUS Server Policy 🥒	Mot-Hotspot
	Server Policy Client Proxy LDAP
Settings	
RADIUS User Pools	Mot-Hotspot
LDAP Server Dead Period	5 Minutes v (0 to 10)
LDAP Groups	Mot-Hotspot
LDAP Group Verification	\checkmark
Local Realm	
Autheritication Date Source	
Local Authentication Type	
LDAP Authentication Type	All v
Enable CRL Validation	
Session Resumption / Fast Read	ithentication
Enable Session Resumption	
Cached Entry Lifetime	1 (1 to 24 hours)
Maximum Cache Entries	128 (10 to 1,024)

- 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'

Dashboard Configuration Diagnostics Ope	erations Statistics	RF54000	ᄊ Wi-NG v5.1 🙎 admin 🚽
Devices Wireless Profiles RF Domains Seci	urity Services Management		🅤 Revert 📩 Commit 🔚 Save
aptive Portals 🖉 🖕	DHCP Server		0
رهاCaptive Portals	DHCP Server Policy	() Ignore BOOTP Requests	Ping Timeout
DNS Whitelist			
EDHCP Server Policy			
DHCP Server			
La	·		
Type to search	Type to search in tables		Row Count: 0
+ -			Add Edit, Delete
Event Summary			Find Functional Area Type to search

Set 'DHCP Server Policy Name'

Click 'Continue'

DHCP Server Policy	🖋 🛛 Motorola Lab I	OHCP Server	Continue	Exit			
					DHCP Pool	Global Settings	Class Policy
DHCP Pool	۲	Subnet			Domain Na	me	

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

Dashboard Configuration Diagnostics Ope	erations Statistics		RF	54000 🙌 Wi-I	NG v5.1 🙎 admin 🚽
Devices Wireless Profiles RF Domains Secu	urity Services Management		<i>,</i> //		🅤 Revert : 🛃 Commit : 🔚 Save
Captive Portals هي 🖻	DHCP Server Policy Motorola Lab D	DHCP Server			0
Pcaptive Portals					
DNS Whitelist		DF	ICP Pool Global Settings Class Policy		
EDHCP Server Policy	DHCP Pool ()	Subnet D	iomain Name	Boot File	Lease Time
Ren Mulurula Lab DHCP Server					
Type to search	Type to search in tables				Row Count: 0
+ -					Add Edit _x Delete Exit
Event Summary					Find Functional Area Type to search

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

General	Basic Settings	Static Bindings Advanced		•
General	Basic Settings	Static Bindings Advanced		
Subnet ////////////////////////////////////	20 . 0 / 24 🗸	General Lease Time Default Routers	 ✓ 86400 IP Address 172. 16. 20. 1 0. 0. 0. 0 0. 0. 0. 0 	Clear = Clear =
0.0. 0.0. IP Address Ranges	0.0 <u>Clear</u> 0.0 <u>Clear</u> ▼	Class Policy	0.0.0.0	<u>Clear</u> v
* 172.16.20.100	172.16.20.150	■ 1000 1 000 j		
		+	Add Row	Reset Exit

- 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)

Dashboard Configuration Diagnostics Ope	rations Statistics		🔷 RF54000 🛛 🕅 W	/i-NG _{v5.1} 🔱 admin 🛛 🌖
Devices Wireless Profiles RF Domains Sec	urity Services Managem	ent 🔓		5) Revert i 📐 Commit i 🔚 Save
🔊 Manage Profiles	Profile default-rfs4000	Type rfs4000		0
Manage Profiles	Profile default-rfs4000 General Cluster Cluster Interface Network Security Security Sentices Advanced Advanced	Captive Portal Hosting Create Captive Portal Hosting Image: Captive Portal Hosting Captive Portal Policies Image: Captive Portal Hosting DBICP Server Image: Captive Portal Hosting DBICP Server Image: Captive Portal Hosting RADUS Server Policy Image: Maderial Lab DHCP Server RADUS Server Policy Image: Maderial Lab DHCP Server		•
Type to search		L.A.I		OK Reset Ext Fod Functional Area Trave to search

10) Create WLAN for Hotspot

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

Dashboard Configuration Diagnostics Ope	rations Statistics				•	🔷 RFS4000	M Wi-N	G v5.1 🙎 adr	nin 🌖
Devices Wireless Profiles RF Domains Sec	urity Services Man	agement			~1			🅤 Revert	皆 Commit 🛛 🔚 Save
튌Wireless LANs	Wireless LANs								0
WLAN QoS Policy	WLAN A	SSID	Description	WLAN Status	VLAN Pool	Authentication Type	Encryption Type	0oS Policy	Association ACL
Radio QoS Policy	wian1	motorola		X Disabled	1	None	None	default	
🚆 AAA Policy									
Association ACL									
PSMART RF Policy									
▶WARRESS LAN									
	1								
Type to search	Type to search in tables								Row Count: 1
+ -									Add Edit, Delete
Event Summary 0 0 0 1							Fin	d Functional Area Type to s	earch

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'

WLAN 🖋 Mot-Hotspot	
Basic Configuration	WLAN Configuration
Security	SSID 🖉 Mot-Hotspot
Firewall	Description
Client Settings	WLAN Status
Accounting	
Client Load Balancing	default
Advanced	Bridging Mode 🖉 Tunnel 🔻
	Other Settings
	Broadcast SSID
	Answer Broadcast Probes
	VLAN Assignment
	Single VLAN VLAN Pool
	/ VLAN 20
	RADIUS VLAN Assignment
	Allow RADIUS Override

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)

Dashboard Configuration Diagnostics Oper	rations Statistics	😽 RE56000 🔛 WI-NG 15:1 🚨 admin 🍕
Devices Wireless Profiles RF Domains Secu	urity Services Managem	nt 👘 Reret 🔮 Commit 🔒 Save
Direless LANs	WLAN Mot-Hotspot	0
WILAN GOS Policy Padio GoS Policy Association ACL PSMART RF Policy	Basic Configuration Security Firewall Client Settings Accounting Client Load Balancing Advanced	Select Authentication Authentication Type EAP EAP EAPAKC MAC Ketheros Ketheros Configuration Settings AAA Policy Contre Resultertication Image: Type Image: Type Image: Type Captive Portal Enforcement Enforcement Captive Portal Enable Captive Portal Captive Portal Enable
Big Mut-Histopot		Cighre Portal Policy V MocHologot V V Sector Cighre Portal Policy V Mor 128 V Mor Pola V Open V Mor 128 V Mor Pola V Open V Mor 128 V Open V Mor Pola V Open V Mor Pola V Mor Pola V Open V Mor Pola V
Event Summary 0 0 0 1		Find Functional Area Type to search

11) Map WLAN to radios of the AP650 profile

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

Dashboard Configuration Diagnostics Ope	erations Statistics			h	🔷 RFS4000	M Wi	-NG v5.1 🙎 v	idmin 🌖	
Devices Wireless Profiles RF Domains Sec	curity Services Manageme	ent					5 Reve	rt 🛃 Commit 📊 Save	
Manage Profiles	Profile default-ap650 T	ype ap650					0		
	General	Name 🛞	Туре	Description	Admin Status	RF Mode	Channel	Transmit Power	
	Adoption	radio1	Radio	radio1	🖌 Enabled	2.4 GHz WLAN	smart	smart	
	v Interface	radio2	Radio	radio2	🖌 Enabled	5 GHz WILAN	smart	smart	
	Ethernet Ports								
	Virtual Interfaces								
	Radios								
	▶ Network								
	▶ Security								
Mar Davias a	Services								
	▶ Management								
V Profile	Advanced								
▶ Dietaut-rts4000	-								
Dietaut-ap6511									
▶ Dicetaut-apcou									
Dietaut-ap/1xx									
Egloetaut-aptc32									
Type to search		Type to search in tables						Row Count: 2	
+ -								Edit Exit	
Event Summary 0 0 0 2							Find Functional Area Type to	o search	

Select 'Radio 1' and Click 'Edit'

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

Radios					×
Name radio1					0
	Radio Settings	WLAN Mapping	Mesh	Advanced Settings	
WLAN/BSS Mapping	IS				
▼ Radio B P P T P T P T T T T T T T T T T T T T	Mot-Hotspot (advert wlan1 (advertised)	ised			
Advanced	Mapping			9	Create New WLAN
				» ок	Reset Exit

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 <u>www.google.com</u>

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

Centralized Captive Portal with External Web Page Server

Captive Portal Enforcement: AP Captive Portal Web Page Hosting: External RADIUS Server: Controller User Database: Controller



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

Dashboard Configuration Diagnostics Ope	erations Statistics		🔷 RFS4000	ᄊ Wi-NG _{v5.1} 💄 admin	->
Devices Certificates SMART RF		k			
	Device MAC rfs4000-2	2A5DC (00-23-68-22-A5-DC)			0
⊒ 🌍 default	Device Details	File Transfers			
@rfs4000-22A5DC	File Transfers				
	File Browser	Source			
	🛃 AP Upgrade	Server			
		Fie Browse			
	T				
	-				
		Target			
		Server 💿 Wireless Controller			
		Fie Browse			
Search				Cop	y _× Reset
Fund O annual and a state of the state		L.*.	l.	First Desidered Asso	
Event Summary				Find Functional Area Type to search	

c. Select 'Server' as the target

To download using FTP / TFP click Advanced

Download the file

flash	system	nvram	cf	usb1	usb2
Path: flas	h:/hotspot/Mot-Hotspo	ot/			
	File Name		Size	Last N	lodified
	agreement	.html	3496	2011-0	2-04 01:32:01
	fail.html		5202	2011-0	2-04 01:32:01
	welcome.h	tml	7712	2011-0	2-04 01:32:01
	login.html		4961	2011-0	2-04 01:32:01
dd New Fol	der				
Create F	older				

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

Dashboard Configuration Diagnostics C	perat	tions Statistics			🔷 RFS4000 – 🔼	Wi-NG v6.1	edmin 2	-)
Devices Wireless Profiles RF Domains S	ecurity	/ Services Management	ر م				5 Revert i 🖄 Co	ommit 🔚 Save
🗖 🖓 Captive Portals		Name Mot-Hotspot						0
Captive Portals								
DNS Whitelist		DIIS Entries						
EDHCP Server Policy		DNS Entry	Match Suffix	Û				
RADIUS		172.16.10.2	×	Û				
		172.16.10.3	×	Û				
Map: None 🔻								
V DNS Whitelist	1.							
Mot-Hotspot	1							
			🔶 Add	Row				
Type to search								
+ -							ок "	Reset _x Exit
Event Summery				1.4		Find Functional Area	Tune to energh	
						Tino Tunctional Area	17pe to search	

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

Dashboard Configuration	Diagnostics	Opera	ations S [.]	itatistics			🔷 RFS4000	M	Wi-NG v5.1		🧕 admin	N
Devices Wireless Profiles	RF Domains	Securi	ity Servi	ces Managa	ement	k				5	Revert 🛃 (Commit 🔚 Save
🗖 @Captive Portals			Captive F	Portal Policy	Mot-Hotspot							0
്ര Captive Portals												
DNS Whitelist						Basic Configuration Web	b Page					
E DHCP Server Policy												
🖪 🔐 RADIUS					Web Page Source 🥖	Internal 🔘 Advanced 💿 Externally Hosted						
					Login URL	http://172.16.10.3/login.html						
					Agreement URL	http://172.16.10.3/agree.html						
Mao: None v					Welcome URL	http://172.16.10.3/welcome.html						
Captive Portal		-			Fail URL	http://172.16.10.3/fail.html						
Mot-Hotspot		4										
Mot-Hotspot-Distributed					A set of pre-exis	ting web pages outside of the switch are specified by the provided URLs.						
					Three separate U	RLs point to external web pages for: Logging the user in, Welcoming the user a	after logging in successfully	and Informing	the user of a failed login	attempt.		
		-										
Type to search											N 0/	
	+ -										» ок	Reset
Event Summary 0 0 2	2 5 🔤	1							Find Function	il Area 🛛	Type to search	

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'

Dashboard Configuration Diagnostics Oper	ations Statistics					🗳 R ⁱ	54000 M	Wi-NG v6.	1 <mark>2</mark> admin	-
Devices Wireless Profiles RF Domains Secu	urity Services M	anagement			h§				퇏 Revert 🛃	🖢 Commit 🛛 🔚 Save
Mireless LANs	AAA Policy 🥖	fot-Hotspot	Continue	xit						0
WLAN QoS Policy										
Radio GoS Policy				RADI	IS Authentication R/	ADIUS Accounting Se	ttings			
🚆 AAA Policy	Server Id	Host	Port	Server Type	Request Proxy	Request Attempts	Request Timeout	DSCP	NAI Routing Enable	NAC Enable
Association ACL					Mode					
© [®] SMART RF Policy										
Max. Max.										
Map: None V										
▶AAA										
Type to search	Type to search in table:									Row Count: 0
+ -									Add E	dit _× Delete Exit
Event Support						▲]		Find Function	nal årea Turne to sear	ch

b. Add RADIUS server by clicking 'Add'

Dashboard Configuration Diagnostics Ope	erations Statistics	:			N	🤹 N	54000 M	Wi-NG vi	1 2 admin	1
Devices Wireless Profiles RF Domains Sec	urity Services M	anagement			4				灯 Revert	o Commit 🛛 🗖 Save
B Wireless LANs	AAA Policy Mot-	Hotspot								0
WLAN QOS Policy										
Radio QoS Policy				RAD	US Authentication R	ADIUS Accounting Se	ttings			
aAA Policy	Server Id	Host	Port	Server Type	Request Proxy	Request Attempts	Request Timeout	DSCP	NAI Routing Enable	NAC Enable
Association ACL					Mode					
SMART RF Policy										
Map: None v										
V AAA	I									
and Hotspot	1									
Type to search	Type to search in table:	3								Row Count: 0
+ -									Add	lit _x Delete Exit
Event Summary						A		Find Function	nal Area Type to sear	ch

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

uthentication Serv	ver	×
rverld 🥖 1	(1 to 6)	6
ettings		
Host	✓ 172.16.10.4 IP Address	
Port	1812 (1 to 65,535)	
Server Type	Host 🗸 🗸	
Secret	****	
	Reconfirm	
Request Proxy Mode	None	
Request Attempts	3 (1 to 10)	=
Request Timeout	3 Seconds v (1 to 60)	
Retry Timeout Factor	100 (50 to 200)	
DSCP	46 (0 to 63)	
etwork Access Identifi	ier Routing	
NAI Routing Enable		
Realm		
Realm Type	Prefix O Suffix	

2) Create DNS Whitelist

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

Enter a name for the DNS Whitelist

Dashboard Configuration Diagnostics Ope	rations Statistics		🔷 RF54000	Wi-NG _{v5.1} & admin 🚽
Devices Wireless Profiles RF Domains Secu	rity Services Management	Ŕ		튓 Revert 🛛 📩 Commit : 🔚 Save
🗖 @Captive Portals	DNS Whitelist			0
Portals	Name			6
DNS Whitelist				0
EDHCP Server Policy				
🖬 📴 RADIUS				
Marr None v				
DNS Whitelist				
	•			
	-			
	Type to search in tables			Row Count 0
Type to search	The examplificance			NOW COOL
+ -				Add Edit _x Delete
Event Summary 0 0 0 1		1		Find Functional Area Type to search

b. Click 'Add Row'

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

Dashboard Configuration Diagnostics Ope	ration	is Statistics				📣 RF54000 🛛 🕅 W	/ i-NG v5.1	🙎 admin	N
Devices Wireless Profiles RF Domains Secu	rity	Services Management		Ş			5	🕥 Revert i 🛃 Commit	🔒 Save
🗖 🔊 Captive Portals	Nar	me Mot-Hotspot							0
്ര Captive Portals									-
DNS Whitelist	DHS	S Entries							
E DHCP Server Policy		DHS Entry	Match Suffix		Û				
🖬 😭 RADIUS		172.16.10.2	>	<	Û				
		172.16.10.3	>	<	Ô				
Marr None V									
The second secon									
Mot-Hotsot	4								
				🕂 Add R	low				
Tests week									
Lible moregion	-							OK Doo	a Est
+ -						▲ I		UN X Kes	
Event Summary 0 0 0 0							Find Functional Area	Type to search	

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'

Dashboard Configuration Diagnostics Opt	erations Statistics			, <	🗞 RF54000	Wi-NG vs.t	admin 🌖	
Devices Wireless Profiles RF Domains Sec	urity Services Manageme	ent		U.		5	Revert Commit 🔚 Save	
🗖 🖓 Captive Portals	Captive Portal	Captive Portal 0						
്രീ Captive Portals	Captive Portal Policy	Captive Portal Server	Captive Portal Server Mode	Connection Mode	Simultaneous Users	Web Page Source	AAA Policy	
DNS Whitelist								
EDHCP Server Policy								
🖬 🔐 RADIUS								
Marri Name w								
mop. Nulle *								
Capitive Portai	•							
	-							
Type to search	Type to search in tables						Row Count: 0	
+ -							Add Edit _x Delete	
Event Summary 0 0 0 1						Find Functional Area	ype to search	

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'

,

Dashboard Configuration Diagnostics Ope	erations Statistics		k	🔷 RFS4000	M	Wi-NG _{v6.1}	<mark>8</mark> admin	-
Devices Wireless Profiles RF Domains Secu	irity Services Manageme	nt					5 Revert	🛓 Commit 🔒 Save
🗖 🔊 Captive Portals	Captive Portal Policy Mo	t-Hotspot						0
്രCaptive Portals								
DNS Whitelist			Basic Configuration We	eb Page				
EDHCP Server Policy	Settings							Â
C RADIUS	Captive Portal Server Mode	Internal (Self) Centralized Centralized Controller						
	Captive Portal Server	Hostosine 💌						
	Connection Mode							
	Connocadir mode							
	Simultaneous Users	V 100 (1 to 8,192)						
Map: None 🔻								
Taptive Portal	Security							
ر@Midt-Hotspot	AAA Policy	Mot-Hotspot 💌 🕒 🎲						
	Access							
	Access Type	O No authentication required						
		Generate Logging Record and Allow Access						
		O Custom User Information for RADIUS Authentication						
		RADIUS Authentication						
	RADIUS Lookup Information							
	Terms and Conditions page							
	Client Settings							
Type to search	Client Access Time	4440 A (30 to 10 090 minutes)						v
+ -							OK	_× Reset _× Exit
Event Summary	Saving data					Find Functional Are	a Type to sear	ch

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

Dashboard Configuration Diagnostics Oper	rations Statistics	📣 RF5400	🙌 Wi-NG v5.1 💄 admin 🚽
Devices Wireless Profiles RF Domains Secu	rity Services Management	k	5 Revert 📩 Commit 识 Save
🗖 🚱 Captive Portals	Captive Portal Policy Mot-Hotspot		0
്രി Captive Portals			
DNS Whitelist		Basic Configuration Web Page	
EDHCP Server Policy			
E RADIUS	Web Page Source 🧳	internal 🔾 Advanced 🕢 Externally Hosted	
	Login URL	http://172.16.10.3/cgin.html	
	Agreement URL	http://172.16.10.3/agree.html	
Map: None v	Welcome URL	http://172.16.10.3/welcome.html	
V Captive Portal	Fail URL	http://172.16.10.3/fail.html	
MotHolspot	1		
Ana Haspat Districted	A set of pre-exist Three separate UR	ng web pages outside of the switch are specified by the provided URLs. I'Ls point to external web pages for: Logging the user in, Welcoming the user after logging in successfully o	ind Informing the user of a failed login attempt.
179% W 404000			» OK Reset Exit
· · · · · · · · · · · · · · · · · · ·		L 🔺 J	
Event Summary 0 0 2 5			Find Functional Area Type to search

- 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'

Dashboard Configuration Diagnostics Ope	erations Statistics	۲	🗬 RF54000 🙌 Wi	-NG v5.1			
Captive Portais	DHCP Server						
কে Captive Portals DNS Whitelist	DHCP Server Policy	Ignore BOOTP Requests	Ping Timeout				
EDHCP Server Policy							
D RADUS							
				Benfant 0			
Type to search	Type to search in tables			Row Count: 0			
+ - Add Edit, Delete							
Event Summary				Find Functional Area Type to search			

Set 'DHCP Server Policy Name'

Click 'Continue'

DHCP Server Policy	🖉 Motorola Lab I	OHCP Server	Continue	Exit			
					DHCP Pool	Global Settings	Class Policy
DHCP Pool	۲	Subnet			Domain Na	me	

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

Dashboard Configuration Diagnostics Ope	erations Statistics		RF	54000 🙌 Wi-I	NG v5.1 🙎 admin 🚽
Devices Wireless Profiles RF Domains Secu	urity Services Management		<i>,</i> //		🅤 Revert : 🛃 Commit : 🔚 Save
Captive Portals هي 🖻	DHCP Server Policy Motorola Lab D	DHCP Server			0
Pcaptive Portals					
DNS Whitelist		DF	ICP Pool Global Settings Class Policy		
EDHCP Server Policy	DHCP Pool ()	Subnet D	iomain Name	Boot File	Lease Time
Ren Mulurula Lab DHCP Server					
Type to search	Type to search in tables				Row Count: 0
+ -					Add Edit _x Delete Exit
Event Summary					Find Functional Area Type to search

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

DHCP Pools		4	×
DHCP Pool 🥒 🗸	LAN20		0
	Basic Settings	Static Bindings Advanced	
General		General	
Subnet 🥜	172.16.20.0/24 🗗	Lease Time	86400
Domain Name		Default Routers	IP Address
DNS Servers	IP Address		172.16.20.1 <u>Clear</u>
	0.0.0.0 <u>Clear</u>	· /	0.0.0.0 <u>Clear</u>
	0.0.0.0 <u>Clear</u>	=	0.0.0.0 <u>Clear</u>
	0.0.0.0 <u>Clear</u>		0.0.0.0 <u>Clear</u>
	0.0.0.0 <u>Clear</u>	Y	
IP Address Ranges	IP End	Class Policy	a
172 16 2	0 100 172 16 20 150	-	E9 m
· · · · · · · · · · · · · · · · · · ·			
/			
		+ /	Add Row
			» OK Reset Exit

- 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)

Dashboard Configuration Diagnostics Ope	erations Statistics		▶ 🔷 RF54000	M W	/i-NG v5.1 🔱 admin 🚽
Devices Wireless Profiles RF Domains Ser	curity Services Managem	ent			5) Revert 📐 Commit 🛛 🔚 Save
🔊 Manage Profiles	Profile default-ap6532	Type ap6532			0
Map: Device ▼ Prote ▶ @efeaut.rst000 @efeaut.rst010 @efeaut.rst011 ▶ > @fefaut.rst011 ▶ > @fefaut.rst011 ▶ > @fefaut.rst011 > > @fefaut.rst011 > > @fefaut.rst011 > > @fefaut.rst011 > > @fefaut.rst050 > > @fefaut.rst0522 >	General Adoption Interface Network Services Management Advanced	Captive Portal Hosting Captive Portal Hosting Captive Portal Hosting Unice Server DHCP Server DHCP Server RADIUS Server Policy RADIUS S			·
lype to search					» OK Reset Exit
Event Summary 0 0 0 0					Find Functional Area Type to search

7) Create WLAN for Hotspot

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

Dashboard Configuration Diagnostics Ope	rations Statistics				N	🗬 RFS4000	ᄊ 🛛 Wi-N	G v5.1 🙎 adr	nin 🊽		
Devices Wireless Profiles RF Domains Sec	urity Services Ma	anagement			N			5) Revert	🛃 Commit 🛛 🔚 Save		
BWireless LANs	Wireless LANs	Wireless LANs O									
WLAN GoS Policy	WLAN	A SSID	Description	WLAII Status	VLAN Pool	Authentication Type	Encryption Type	QoS Policy	Association ACL		
Radio QoS Policy	wlant	motorola		X Disabled	1	None	None	default			
AAA Policy											
RASSOCIATION ACL											
° SMART RF Policy											
Mireless LAN											
	-										
	4										
Type to search	Type to search in tables								Row Count: 1		
+ -									Add Edit, Delete		
Event Summary 0 0 0 1							Fin	Functional Area Type to s	earch		

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'

Dashboard Configuration Diagnostics Ope	erations Statistics 🔷 😽 RF54400 🚺 🚺	Vi-NG _{v5.1} 🙎 admin 🚽
Devices Wireless Profiles RF Domains Sec	curity Services Management	튓 Revert 📩 Commit 🛛 🔒 Save
BWireless LANs	WLAN Mot-Hotspot	0
WLAN QOS Policy Pradio QOS Policy AA Policy Association ACL PSMART RF Policy	Basic Configuration WLAII Configuration Security SSD Firewall Description Client Bettings WLAN Status Accounting QG Palcy Client Betlanding QG Palcy Advanced Bridging Mode Droxidant SSD Image: Client Law Balancing Other Settings Image: Client Law Balancing Droxidant SSD Image: Client Law Balancing Other Settings Image: Client Law Balancing ULAN Assignment Image: Client Law Balancing Allow RADUS Override Image: Client Law Balancing	
+ -		C OK Reset EXIT
Event Summery 0 0 0 0		Find Functional Area Type to search

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)

Dashboard Configuration Diagnostics Ope	erations Statistics	😽 R5400	Wi-NG v6.1 💄 admin 🚽
Devices Wireless Profiles RF Domains Sec	curity Services Managem	ent "V	灯 Revert 🛚 💾 Commit 🛛 🔒 Save
盟 Wireless LANs	WLAN Mot-Hotspot		0
WILLAN QOS Policy PRadio QOS Policy AA Policy AA Policy Association ACL Q ³ SMART RF Policy Y mythetess LAN Swhant	Basic Configuration Security Firewall Client Settings Accounting Client Load Balancing Advanced	Select Authentication Authentication Type EAP EAPPSK EAP EAPPSK MAC MAC Ketterss Configuration Settinuts AAA Policy conse Resulteritication 90 Image: Captive Portal 03 to 66,400 Captive Portal Captive Portal Enable Enforcement Captive Portal Enable Captive Portal Set Homesy Authentication Fails	
Type to search + -		Select Encryption WEP 128 WEP 84 WEP 2000P KeyOuard	♥ OK Reset Exit
Event Summary 0 0 0 1			Find Functional Area Type to search

8) Map WLAN to radios of the AP6532 profile