WEB ANALYTICS

HOW-TO GUIDE

Contents

1 Network Equipment Configuration 5

1.1 Network Equipment Configuration Page 5

1.1.1 Access the Network Equipment Configuration page 5

1.2 WiNG 5.4 Captive Portal Configuration 6

1.2.1 Create an AAA policy 6

1.2.2 Create a DNS whitelist 8

1.2.3 Create a Captive Portal policy 9

1.2.4 Create a Wireless LAN profile 11

1.2.5 Enable the Wireless LAN on an AP profile.............................. 12

1.3 WiNG 5.4 Web Analytics Data Collection 14

1.3.1 Configure DNS on the controller 14

1.3.2 Enable the analytics licenses on the controller 15

1.3.3 Enable analytics services on an AP profile 16

1.3.4 Enable analytics forwarding on the WLAN profile 17

1.4 ADSP 9.03 Presence Configuration 19

1.4.1 Enable presence detection 19

1.4.2 Configure the API to push data to the cloud service 21

2 Web Analytics Configuration 23

2.1 Locations Configuration 23

2.2 Captive Portal Bundle Configuration 24

2.2.1 Access the Captive Portal bundle 24

2.2.2 Edit the Captive Portal bundle 25

2.2.3 Create the Captive Portal bundle 25

2.3 Appearance Configuration 26

2.3.1 Brand logos 27

2.3.2 Brand websites 27

2.4 Debug 28

2.5 Notifications Configuration 28

3 Best Practices 30

3.1 Presence Configuration 30

3.1.1 Event triggers 30

3.1.2 Client location tracking 30

3.2 Update Intervals 30

3.2.1 Real time applications 30

3.2.2 Asychronous Applications 30

3.3 Privacy 31

3.3.1 Welcome Back page 31

3.3.2 Terms Have Changed page 31

3.4 Access Points 31

3.4.1 Reccomended APs 31

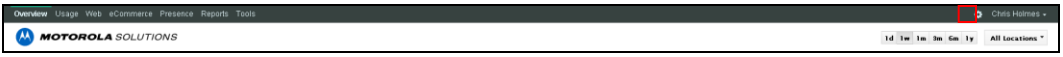
3.4.2 Compatible APs 31

1 Network Equipment Configuration

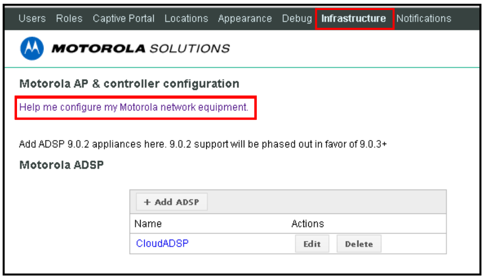
1.1 Network Equipment Configuration Page

1.1.1 Access the Network Equipment Configuration page

From the browser, navigate to Web Analytics Portal URL. Select the gear icon to change the dashboard to the configuration view.



Navigate to the *Infrastructure* tab. Select *Help me configure my Motorola network equipment.*



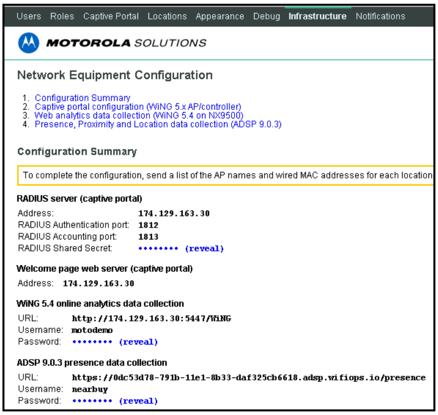
Motorola AP & controller configuration

Help me configure my Motorola network equipment.

Add ADSP 9.0.2 appliances here. 9.0.2 support will be phased out in favor of 9.0.3+

Motorola ADSP

Name	Actions
CloudADSP	Edit Delete



Network Equipment Configuration

1. Configuration Summary
2. Captive portal configuration (WiNG 5.x AP/controller)
3. Web analytics data collection (WiNG 5.4 on NX9500)
4. Presence, Proximity and Location data collection (ADSP 9.0.3)

Configuration Summary

To complete the configuration, send a list of the AP names and wired MAC addresses for each location

RADIUS server (captive portal)

Address: 174.129.163.30
RADIUS Authentication port: 1812
RADIUS Accounting port: 1813
RADIUS Shared Secret: •••••••• (reveal)

Welcome page web server (captive portal)

Address: 174.129.163.30

WiNG 5.4 online analytics data collection

URL: http://174.129.163.30:5447/WiNG
Username: motodemo
Password: •••••••• (reveal)

ADSP 9.0.3 presence data collection

URL: https://0dc53d78-791b-11e1-8b33-daf325cb6618.adsp.wifiops.io/presence
Username: nearbuy
Password: •••••••• (reveal)

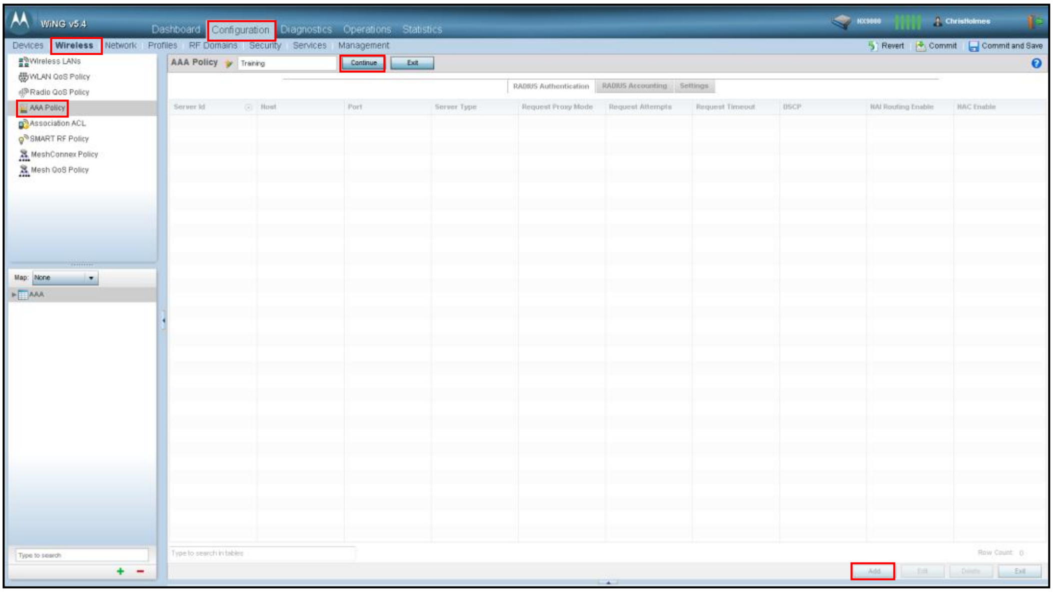
The Configuration Summary of the Network Configuration Page contains all of the information needed to configure:

1) RADIUS server (captive portal)
2) Welcome page server (captive portal)
3) WiNG 5.4 online analytics data collection
4) ADSP 9.0.3 presence data collection

1.2 WiNG 5.4 Captive Portal Configuration

1.2.1 Create an AAA policy

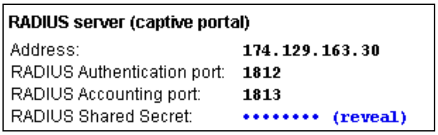
Navigate to *Configuration* → *Wireless* → *AAA Policy*. Select *Add*. Create the name of the *AAA Policy* in the text box. Select *Continue.*



AAA Policy: Training

The AAA policy is now created and the Radius Authentication, Radius Accounting and Settings must be configured.

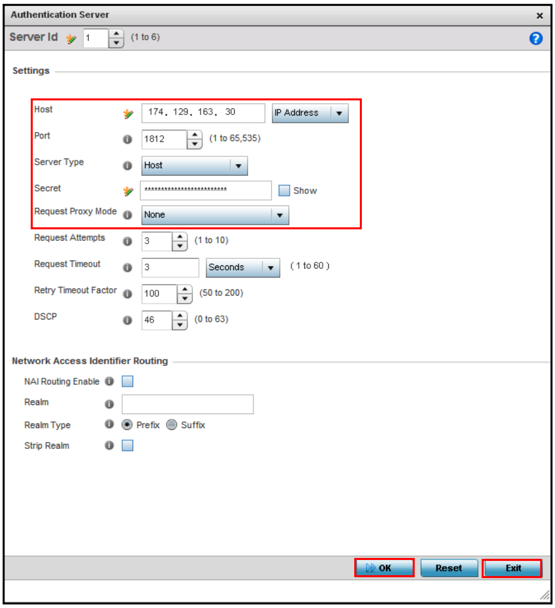
Navigate to the *Radius Authentication* tab*.* Select *Add.* Set the *Host* drop-down box to *IP Address.* Set the *Server Type* to *Host* and the *Request Proxy Mode* to *None.* Input the *Address, Port* and *Secret* from the Radius server (captive portal) section of the Network Equipment Configuration page.



RADIUS server (captive portal)

Address:	174.129.163.30
RADIUS Authentication port:	1812
RADIUS Accounting port:	1813
RADIUS Shared Secret:	•••••••• (reveal)

Select *OK* and *Exit.* Repeat the above steps for the *Radius Accounting* tab.



Authentication Server

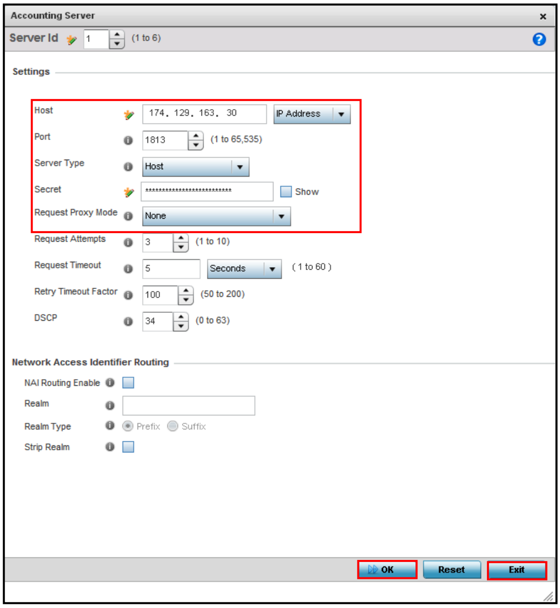
Server Id: 1 (1 to 6)

Settings

- Host: 174. 129. 163. 30 — IP Address
- Port: 1812 (1 to 65,535)
- Server Type: Host
- Secret: ************************ □ Show
- Request Proxy Mode: None
- Request Attempts: 3 (1 to 10)
- Request Timeout: 3 Seconds (1 to 60)
- Retry Timeout Factor: 100 (50 to 200)
- DSCP: 46 (0 to 63)

Network Access Identifier Routing

- NAI Routing Enable: □
- Realm:
- Realm Type: ● Prefix ○ Suffix
- Strip Realm: □



Accounting Server

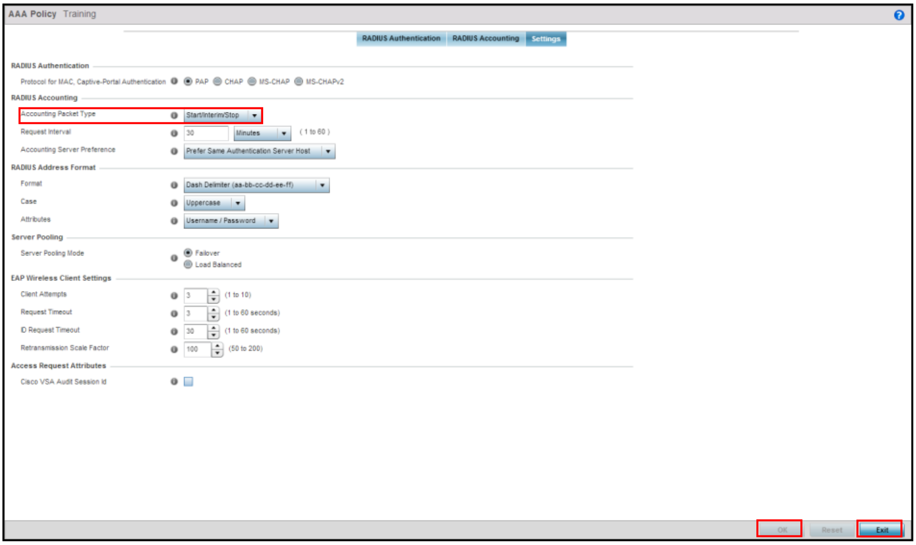
Server Id: 1 (1 to 6)

Settings

- Host: 174. 129. 163. 30 — IP Address
- Port: 1813 (1 to 65,535)
- Server Type: Host
- Secret: ************************** □ Show
- Request Proxy Mode: None
- Request Attempts: 3 (1 to 10)
- Request Timeout: 5 Seconds (1 to 60)
- Retry Timeout Factor: 100 (50 to 200)
- DSCP: 34 (0 to 63)

Network Access Identifier Routing

- NAI Routing Enable: □
- Realm:
- Realm Type: ● Prefix ○ Suffix
- Strip Realm: □



AAA Policy Training

RADIUS Authentication

- Protocol for MAC, Captive-Portal Authentication: ● PAP ○ CHAP ○ MS-CHAP ○ MS-CHAPv2

RADIUS Accounting

- Accounting Packet Type: Start/Interim/Stop
- Request Interval: 30 Minutes (1 to 60)
- Accounting Server Preference: Prefer Same Authentication Server Host

RADIUS Address Format

- Format: Dash Delimiter (aa-bb-cc-dd-ee-ff)
- Case: Uppercase
- Attributes: Username / Password

Server Pooling

- Server Pooling Mode: ● Failover ○ Load Balanced

EAP Wireless Client Settings

- Client Attempts: 3 (1 to 10)
- Request Timeout: 3 (1 to 60 seconds)
- ID Request Timeout: 30 (1 to 60 seconds)
- Retransmission Scale Factor: 100 (50 to 200)

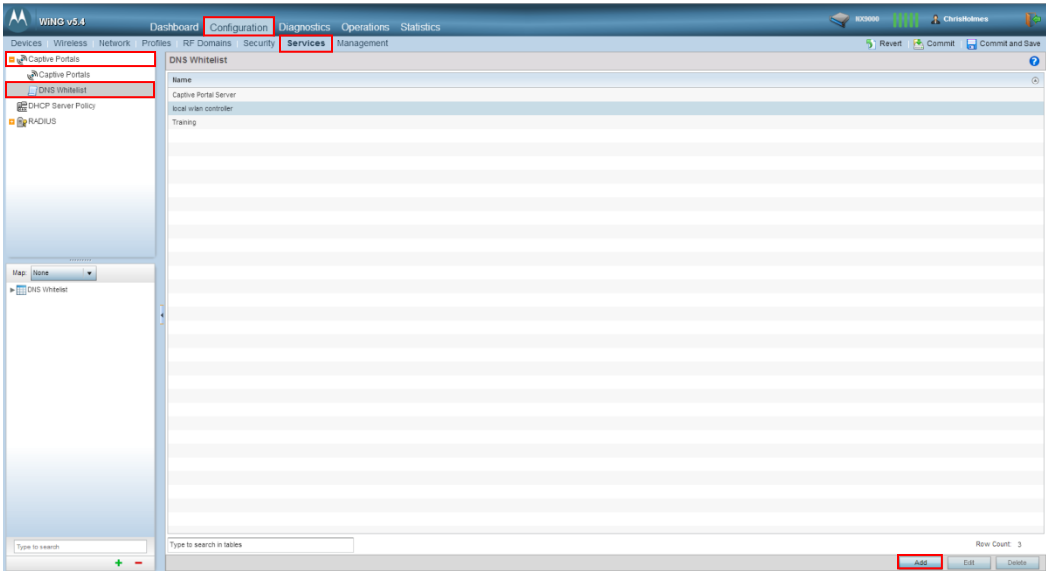
Access Request Attributes

- Cisco VSA Audit Session Id: □

Navigate to *Settings*. Set *Accounting Packet Type* to *Start/Interim/Stop.* Select *OK* and *Exit.*

1.2.2 Create a DNS whitelist

Navigate to *Configuration* → *Services* → *Captive Portals* → *DNS Whitelist.* Select *Add.*

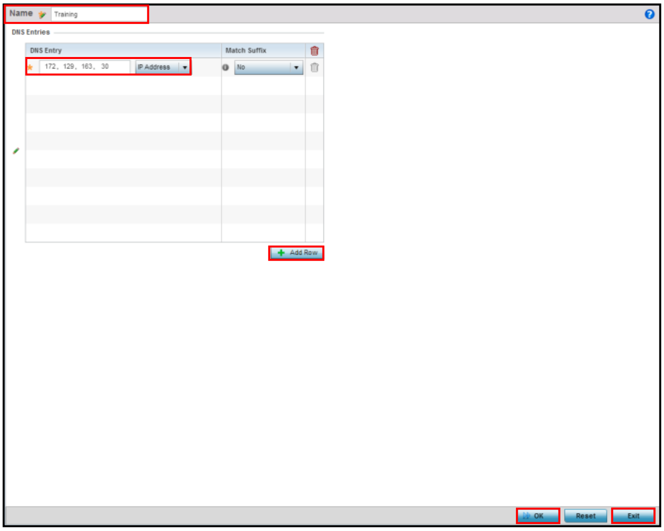


DNS Whitelist

Name
Captive Portal Server
local wlan controller
Training

Row Count: 3

Create the name of the *DNS Whitelist* in the text box. Select *Add* Row. Select *IP Address* from the *DNS Entry* drop-down box. Type the *IP Address* of the captive portal server from the Network Configuration Page. Select *OK* and *Exit.*



Name: Training

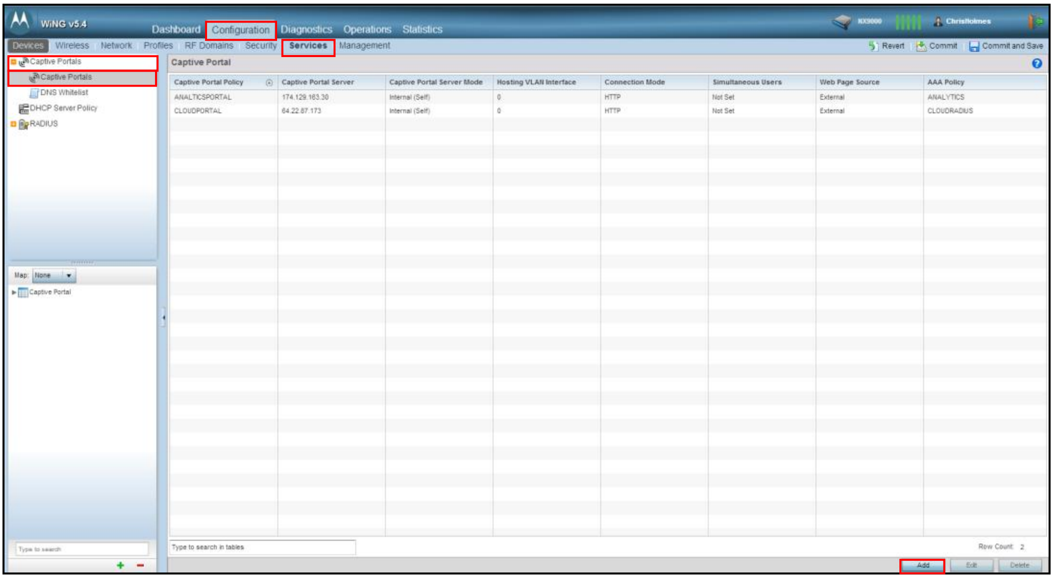
DNS Entries

DNS Entry		Match Suffix
172. 129. 163. 30	IP Address	No

Welcome page web server (captive portal)
Address: 174.129.163.30

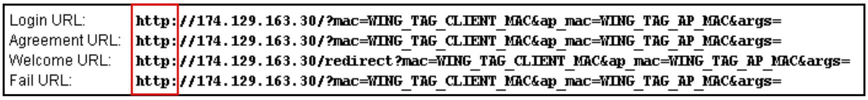
1.2.3 Create a Captive Portal policy

Navigate to *Configuration* → *Services* → *Captive Portals* → *Captive Portals.* Select *Add.*



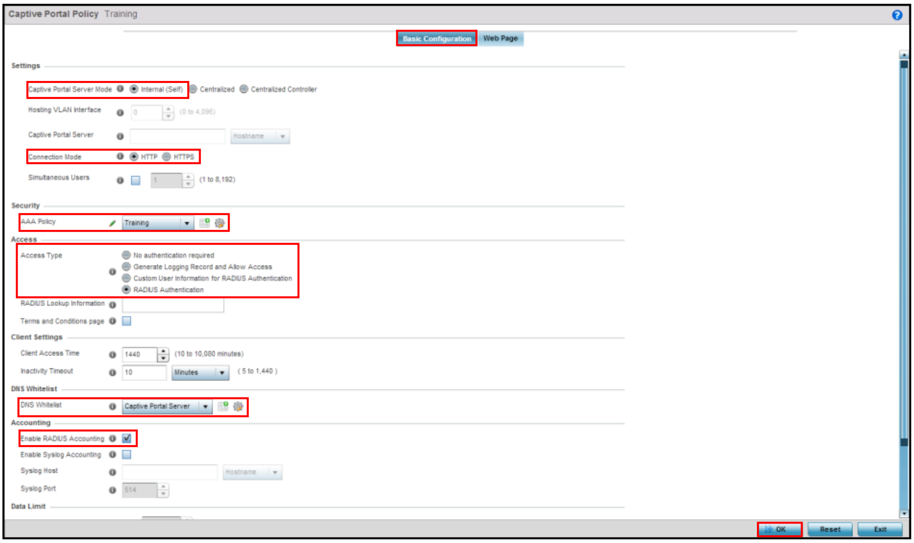
Captive Portal Policy	Captive Portal Server	Captive Portal Server Mode	Hosting VLAN Interface	Connection Mode	Simultaneous Users	Web Page Source	AAA Policy
ANALTICSPORTAL	174.129.163.30	Internal (Self)	0	HTTP	Not Set	External	ANALYTICS
CLOUDPORTAL	64.22.87.173	Internal (Self)	0	HTTP	Not Set	External	CLOUDRADIUS

Create the name of the *Captive Portal Policy* in the text box. Select *OK.* On the *Basic Configuration* tab. Select the *Connection Mode* based on application protocol (HTTP or HTTPS) of the externally hosted URLs found on the Network Equipment Configuration page.



Login URL:	http://174.129.163.30/?mac=WING_TAG_CLIENT_MAC&ap_mac=WING_TAG_AP_MAC&args=
Agreement URL:	http://174.129.163.30/?mac=WING_TAG_CLIENT_MAC&ap_mac=WING_TAG_AP_MAC&args=
Welcome URL:	http://174.129.163.30/redirect?mac=WING_TAG_CLIENT_MAC&ap_mac=WING_TAG_AP_MAC&args=
Fail URL:	http://174.129.163.30/?mac=WING_TAG_CLIENT_MAC&ap_mac=WING_TAG_AP_MAC&args=

Select the *Captive Portal Server Mode* as *Internal.* Select the *AAA Policy* created in step 1.2.1. Select the *Access* Type as *Radius Authentication.* Select the *DNS* Whitelist created in the previous step. Check *Enable RADIUS Accounting*. Select *OK.*



Captive Portal Policy Training

Settings

Captive Portal Server Mode ● Internal (Self) ○ Centralized ○ Centralized Controller

Hosting VLAN Interface 0 (0 to 4,096)

Captive Portal Server Hostname

Connection Mode ● HTTP ○ HTTPS

Simultaneous Users □ 1 (1 to 8,192)

Security

AAA Policy Training

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 □

Client Settings

Client Access Time 1440 (10 to 10,080 minutes)

Inactivity Timeout 10 Minutes (5 to 1,440)

DNS Whitelist

DNS Whitelist Captive Portal Server

Accounting

Enable RADIUS Accounting ☑

Enable Syslog Accounting □

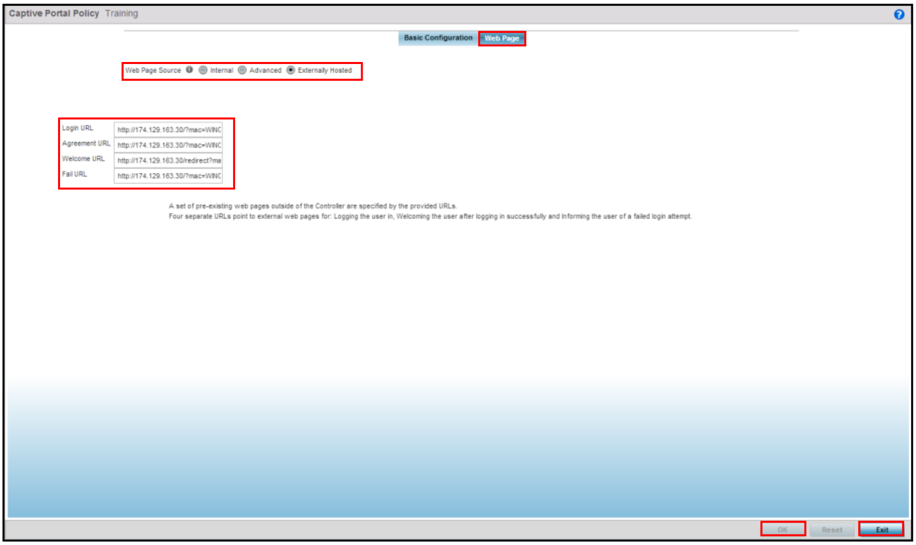
Syslog Host Hostname

Syslog Port 514

Data Limit

Navigate to the *Web Page* tab. Select the *Externally Hosted Web Page Source* radio button. Input the externally hosted URLs found the Network Equipment Configuration page. Select *OK* and *Exit.*

Login URL:	**http://174.129.163.30/?mac=WING_TAG_CLIENT_MAC&ap_mac=WING_TAG_AP_MAC&args=**
Agreement URL:	**http://174.129.163.30/?mac=WING_TAG_CLIENT_MAC&ap_mac=WING_TAG_AP_MAC&args=**
Welcome URL:	**http://174.129.163.30/redirect?mac=WING_TAG_CLIENT_MAC&ap_mac=WING_TAG_AP_MAC&args=**
Fail URL:	**http://174.129.163.30/?mac=WING_TAG_CLIENT_MAC&ap_mac=WING_TAG_AP_MAC&args=**



Captive Portal Policy Training

Web Page Source ○ Internal ○ Advanced ● Externally Hosted

Login URL http://174.129.163.30/?mac=WINC

Agreement URL http://174.129.163.30/?mac=WINC

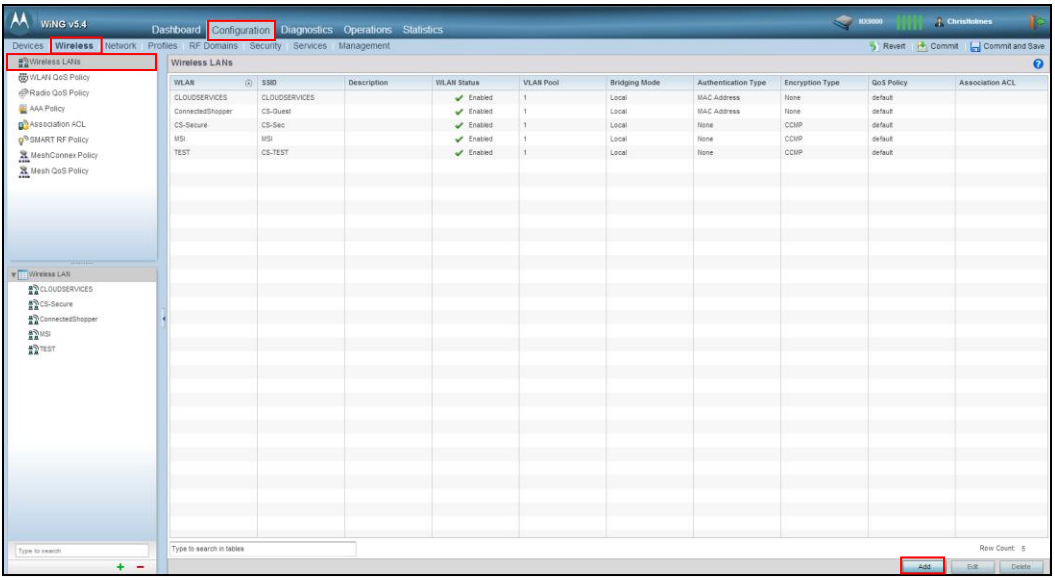
Welcome URL http://174.129.163.30/redirect?ma

Fail URL http://174.129.163.30/?mac=WINC

A set of pre-existing web pages outside of the Controller are specified by the provided URLs.
Four separate URLs point to external web pages for: Logging the user in, Welcoming the user after logging in successfully and Informing the user of a failed login attempt.

1.2.4 Create a Wireless LAN profile

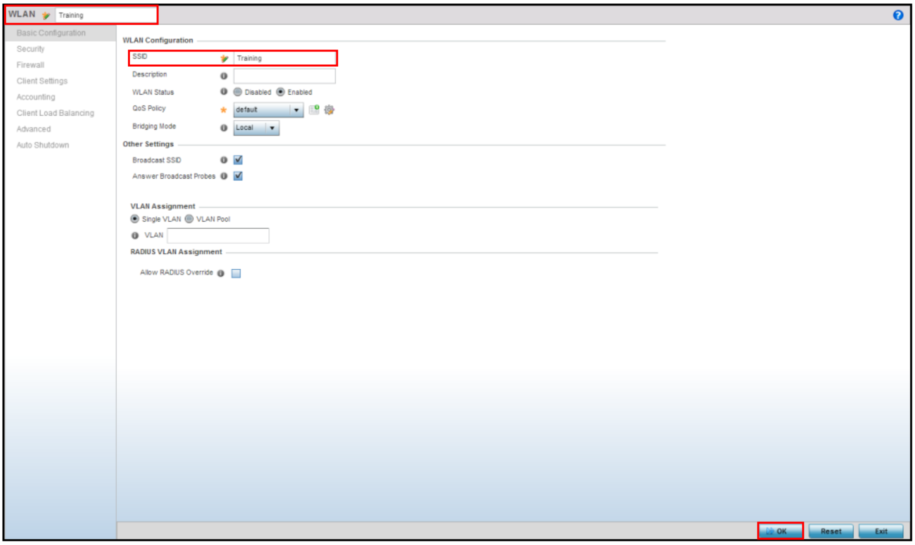
Navigate to *Configuration* → *Wireless* → *Wireless LANs*. Select *Add*.



Wireless LANs

WLAN	SSID	Description	WLAN Status	VLAN Pool	Bridging Mode	Authentication Type	Encryption Type	QoS Policy	Association ACL
CLOUDSERVICES	CLOUDSERVICES		✓ Enabled	1	Local	MAC Address	None	default	
ConnectedShopper	CS-Guest		✓ Enabled	1	Local	MAC Address	None	default	
CS-Secure	CS-Sec		✓ Enabled	1	Local	None	CCMP	default	
MSI	MSI		✓ Enabled	1	Local	None	CCMP	default	
TEST	CS-TEST		✓ Enabled	1	Local	None	CCMP	default	

Create the name of the *WLAN* profile in the text box. Input the SSID. Select *OK.*



WLAN Training

WLAN Configuration

SSID: Training
Description:
WLAN Status: ○ Disabled ● Enabled
QoS Policy: default
Bridging Mode: Local

Other Settings

Broadcast SSID ☑
Answer Broadcast Probes ☑

VLAN Assignment

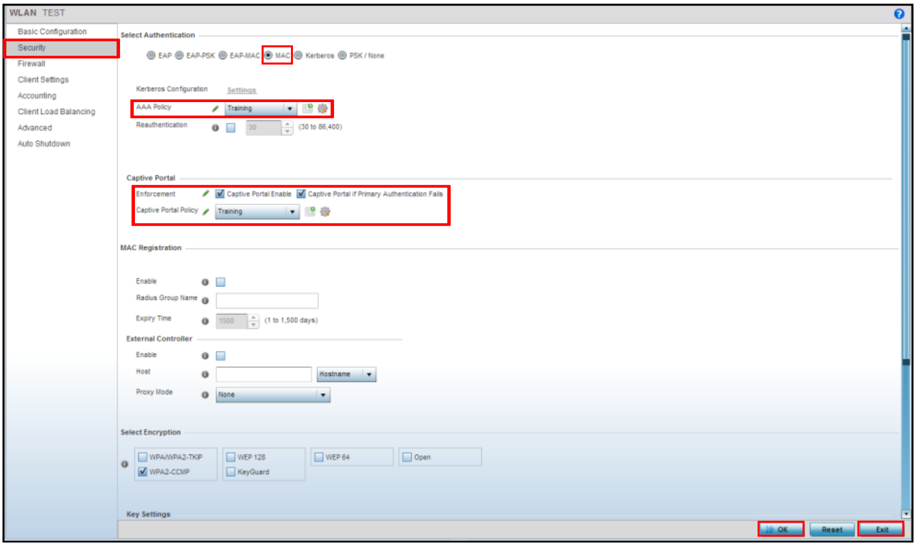
● Single VLAN ○ VLAN Pool
VLAN:

RADIUS VLAN Assignment

Allow RADIUS Override □

Navigate to the *Security* tab. Select the *MAC* authentication radio button. Select the *AAA Policy* created in step 1.2.1. Check *Captive Portal Enable* and *Captive Portal if Primary Authentication*

Fails. Select the *Captive Portal Policy* created in step 1.2.3. Select the desired *Encryption* security protocol. Select *OK* and *Exit.*



Select Authentication

○ EAP ○ EAP-PSK ○ EAP-MAC ● MAC ○ Kerberos ○ PSK / None

Kerberos Configuration Settings

AAA Policy: Training

Reauthentication □ 30 (30 to 86,400)

Captive Portal

Enforcement ☑ Captive Portal Enable ☑ Captive Portal if Primary Authentication Fails

Captive Portal Policy: Training

MAC Registration

Enable □

Radius Group Name

Expiry Time 1500 (1 to 1,500 days)

External Controller

Enable □

Host: Hostname

Proxy Mode: None

Select Encryption

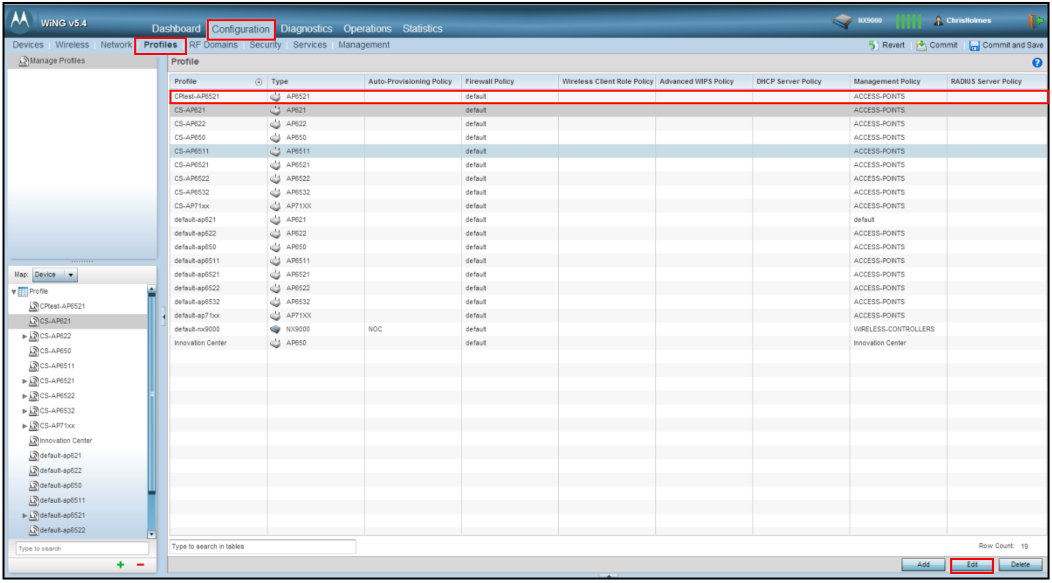
□ WPA/WPA2-TKIP □ WEP 128 □ WEP 64 □ Open

☑ WPA2-CCMP □ KeyGuard

Key Settings

1.2.5 Enable the Wireless LAN on an AP profile

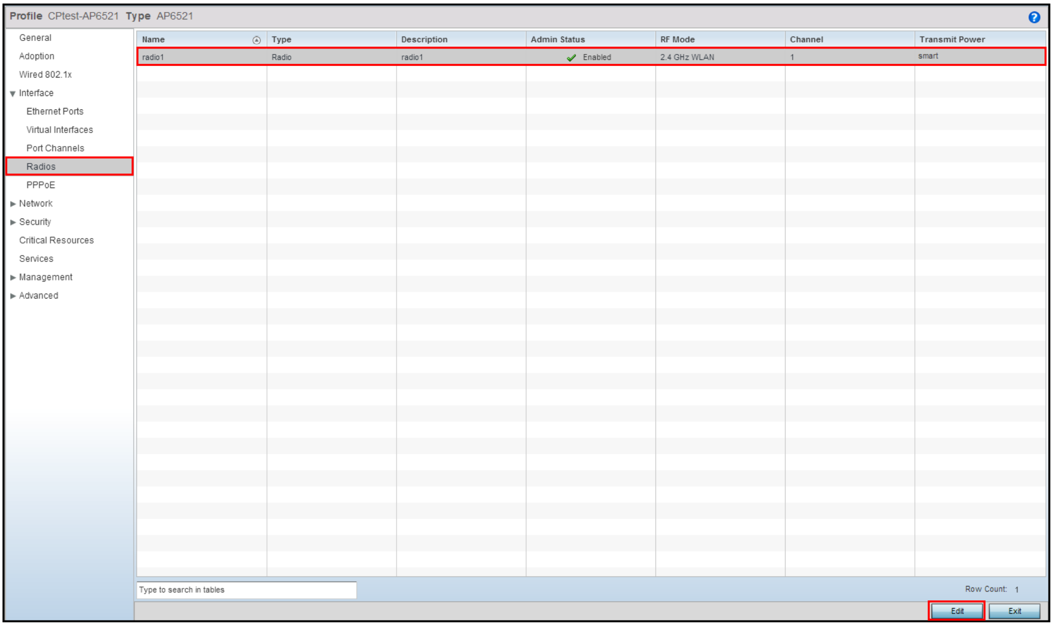
Navigate to *Configuration* → *Profiles.* Select the AP profile(s) that captive portal needs to be enabled on. Select *Edit.*



Profile

Profile	Type	Auto-Provisioning Policy	Firewall Policy	Wireless Client Role Policy	Advanced WIPS Policy	DHCP Server Policy	Management Policy	RADIUS Server Policy
CPtest-AP6521	AP6521		default				ACCESS-POINTS	
CS-AP621	AP621		default				ACCESS-POINTS	
CS-AP622	AP622		default				ACCESS-POINTS	
CS-AP650	AP650		default				ACCESS-POINTS	
CS-AP6511	AP6511		default				ACCESS-POINTS	
CS-AP6521	AP6521		default				ACCESS-POINTS	
CS-AP6522	AP6522		default				ACCESS-POINTS	
CS-AP6532	AP6532		default				ACCESS-POINTS	
CS-AP71xx	AP71XX		default				ACCESS-POINTS	
default-ap621	AP621		default				default	
default-ap622	AP622		default				ACCESS-POINTS	
default-ap650	AP650		default				ACCESS-POINTS	
default-ap6511	AP6511		default				ACCESS-POINTS	
default-ap6521	AP6521		default				ACCESS-POINTS	
default-ap6522	AP6522		default				ACCESS-POINTS	
default-ap6532	AP6532		default				ACCESS-POINTS	
default-ap71xx	AP71XX		default				ACCESS-POINTS	
default-nx9000	NX9000	NOC	default				WIRELESS-CONTROLLERS	
Innovation Center	AP650		default				Innovation Center	

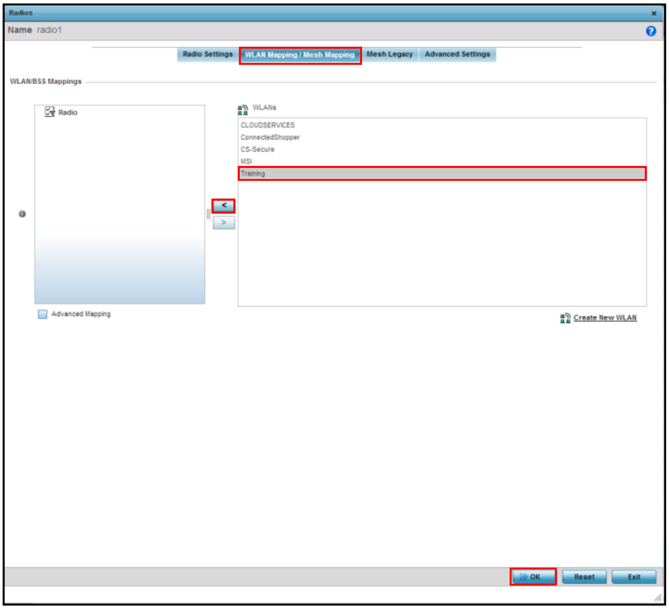
Navigate to *Interface → Radios.* Select the radio profile. Select *Edit.*



Profile CPtest-AP6521 **Type** AP6521

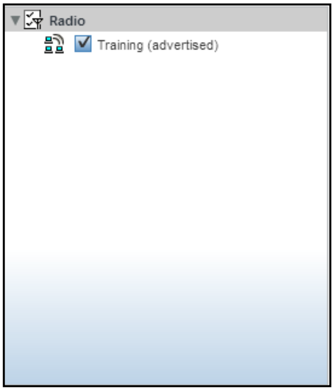
Name	Type	Description	Admin Status	RF Mode	Channel	Transmit Power
radio1	Radio	radio1	✓ Enabled	2.4 GHz WLAN	1	smart

Navigate to the *WLAN Mapping/ Mesh Mapping* tab. Select the WLAN profile created in step 1.2.4. Move the WLAN profile to the *Radio* section with the left arrow button. Select *OK* and *Exit.*



CLOUDSERVICES
ConnectedShopper
CS-Secure
MSI
Training

□ Advanced Mapping



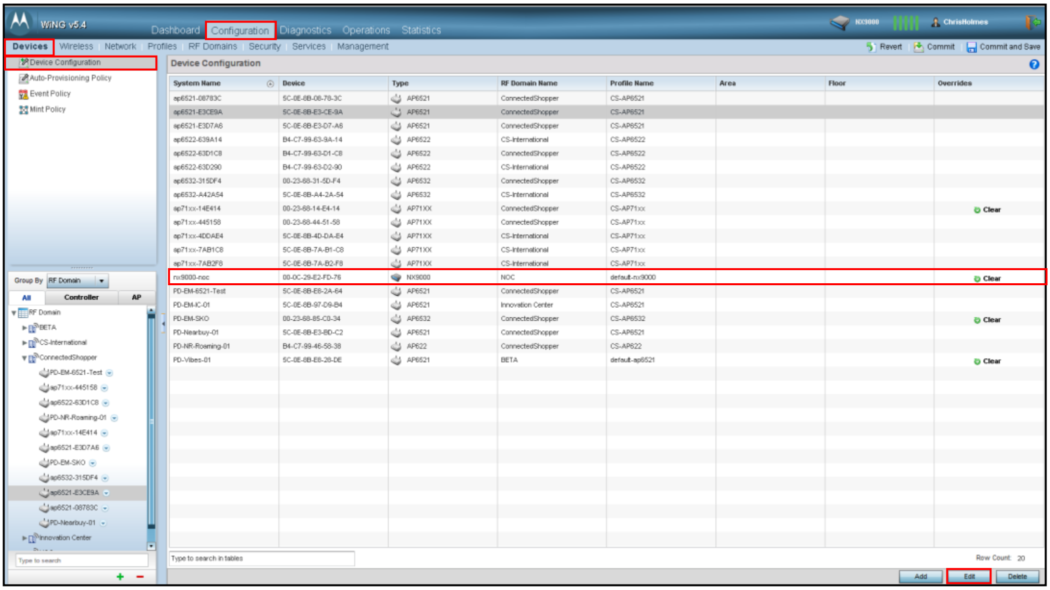
☑ Training (advertised)

Commit and Save the changes to complete the configuration.

1.3 WiNG 5.4 Web Analytics Data Collection

1.3.1 Configure DNS on the controller

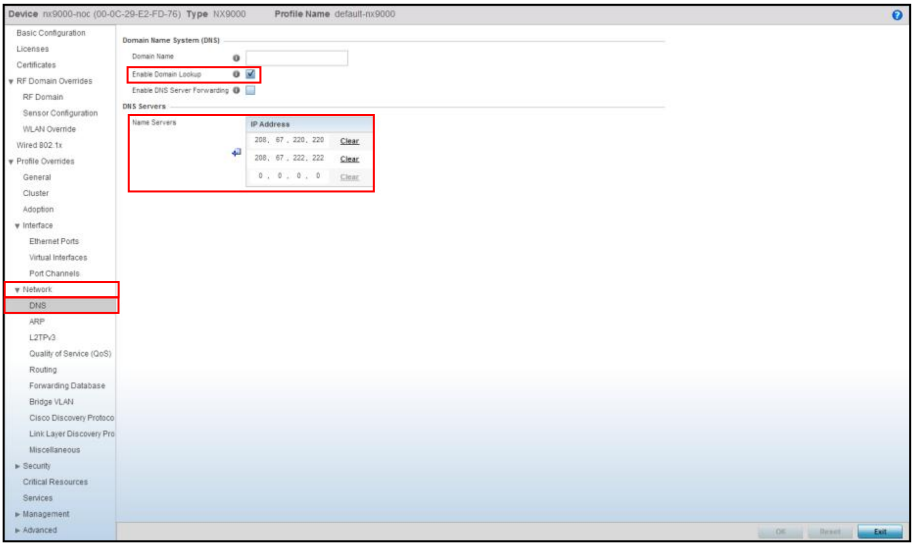
Navigate to *Configuration → Devices →Device Configuration.* Select the controller. Select *Edit.*



Device Configuration

System Name	Device	Type	RF Domain Name	Profile Name	Area	Floor	Overrides
ap6521-08783C	5C-0E-8B-08-78-3C	AP6521	ConnectedShopper	CS-AP6521			
ap6521-E3CE9A	5C-0E-8B-E3-CE-9A	AP6521	ConnectedShopper	CS-AP6521			
ap6521-E3D7A6	5C-0E-8B-E3-D7-A6	AP6521	ConnectedShopper	CS-AP6521			
ap6522-639A14	B4-C7-99-63-9A-14	AP6522	CS-International	CS-AP6522			
ap6522-63D1C8	B4-C7-99-63-D1-C8	AP6522	ConnectedShopper	CS-AP6522			
ap6522-63D290	B4-C7-99-63-D2-90	AP6522	CS-International	CS-AP6522			
ap6532-315DF4	00-23-68-31-5D-F4	AP6532	ConnectedShopper	CS-AP6532			
ap6532-A42A54	5C-0E-8B-A4-2A-54	AP6532	CS-International	CS-AP6532			
ap71xx-14E414	00-23-68-14-E4-14	AP71XX	ConnectedShopper	CS-AP71xx			Clear
ap71xx-445158	00-23-68-44-51-58	AP71XX	ConnectedShopper	CS-AP71xx			
ap71xx-4DDAE4	5C-0E-8B-4D-DA-E4	AP71XX	CS-International	CS-AP71xx			
ap71xx-7AB1C8	5C-0E-8B-7A-B1-C8	AP71XX	CS-International	CS-AP71xx			
ap71xx-7AB2F8	5C-0E-8B-7A-B2-F8	AP71XX	CS-International	CS-AP71xx			
nx9000-noc	00-0C-29-E2-FD-76	NX9000	NOC	default-nx9000			Clear
PD-EM-6521-Test	5C-0E-8B-E8-2A-64	AP6521	ConnectedShopper	CS-AP6521			
PD-EM-IC-01	5C-0E-8B-97-D9-B4	AP6521	Innovation Center	CS-AP6521			
PD-EM-SKO	00-23-68-85-C0-34	AP6532	ConnectedShopper	CS-AP6532			Clear
PD-Nearbuy-01	5C-0E-8B-E3-BD-C2	AP6521	ConnectedShopper	CS-AP6521			
PD-NR-Roaming-01	B4-C7-99-46-58-38	AP622	ConnectedShopper	CS-AP622			
PD-Vibes-01	5C-0E-8B-E8-28-DE	AP6521	BETA	default-ap6521			Clear

Navigate to *Network* → *DNS.* Check *Enable Domain Lookup.* Under *DNS Servers*, input one or more valid domain name servers.



Device nx9000-noc (00-0C-29-E2-FD-76) Type NX9000 Profile Name default-nx9000

Domain Name System (DNS)

Domain Name

Enable Domain Lookup ☑

Enable DNS Server Forwarding □

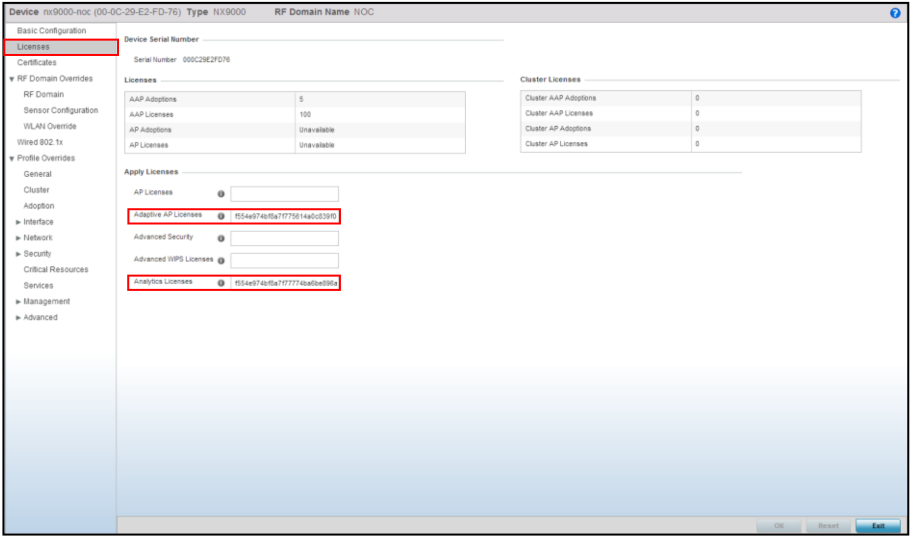
DNS Servers

Name Servers

IP Address	
208 . 67 . 220 . 220	Clear
208 . 67 . 222 . 222	Clear
0 . 0 . 0 . 0	Clear

1.3.2 Enable the analytics licenses on the controller

Navigate to *Licenses.* Input the *Adaptive AP Licenses* and the *Analytics License*.



Device nx9000-noc (00-0C-29-E2-FD-76) **Type** NX9000 **RF Domain Name** NOC

Device Serial Number

Serial Number 000C29E2FD76

Licenses

AAP Adoptions	5
AAP Licenses	100
AP Adoptions	Unavailable
AP Licenses	Unavailable

Cluster Licenses

Cluster AAP Adoptions	0
Cluster AAP Licenses	0
Cluster AP Adoptions	0
Cluster AP Licenses	0

Apply Licenses

AP Licenses

Adaptive AP Licenses f554e974bf8a7f775614a0c839f0

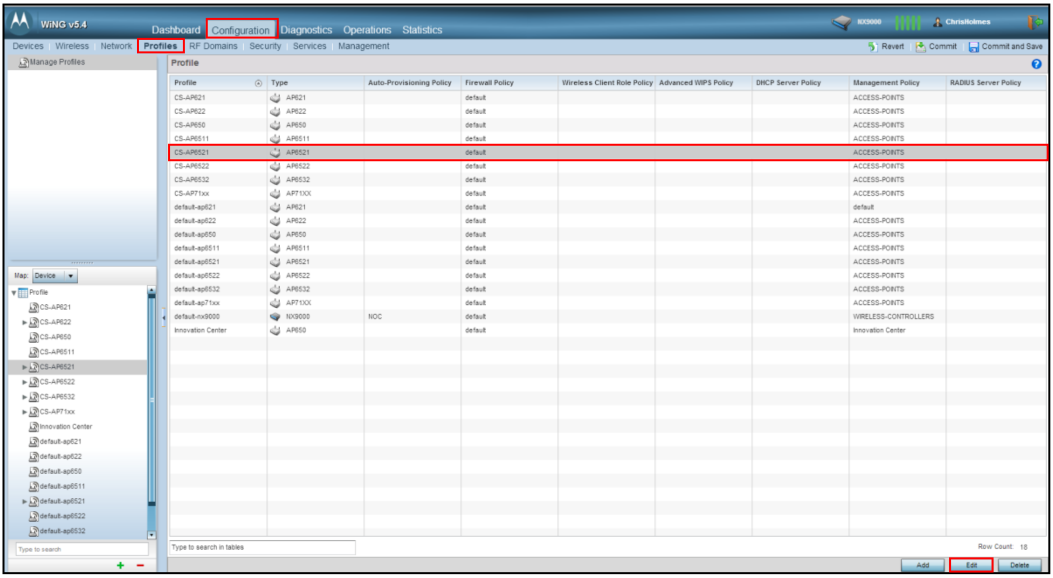
Advanced Security

Advanced WIPS Licenses

Analytics Licenses f554e974bf8a7f77774ba6be896a

1.3.3 Enable analytics services on an AP profile

Navigate to *Configuration → Profiles.* Select the AP Profile for each of the AP models that web analytics will be enabled on. Select the profile. Select *Edit.*

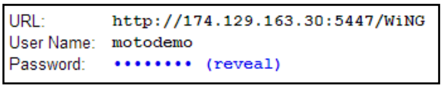


Profile

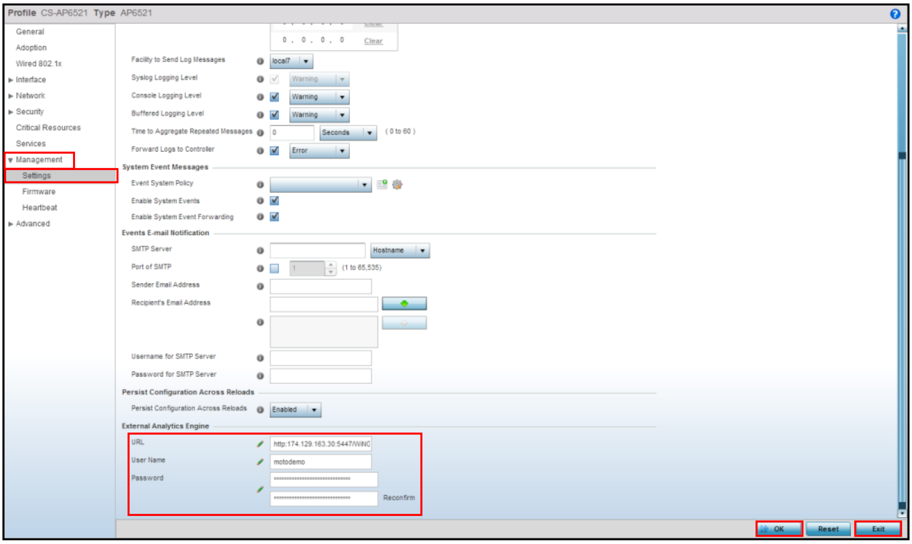
Profile	Type	Auto-Provisioning Policy	Firewall Policy	Wireless Client Role Policy	Advanced WIPS Policy	DHCP Server Policy	Management Policy	RADIUS Server Policy
CS-AP621	AP621		default				ACCESS-POINTS	
CS-AP622	AP622		default				ACCESS-POINTS	
CS-AP650	AP650		default				ACCESS-POINTS	
CS-AP6511	AP6511		default				ACCESS-POINTS	
CS-AP6521	AP6521		default				ACCESS-POINTS	
CS-AP6522	AP6522		default				ACCESS-POINTS	
CS-AP6532	AP6532		default				ACCESS-POINTS	
CS-AP71xx	AP71XX		default				ACCESS-POINTS	
default-ap621	AP621		default				default	
default-ap622	AP622		default				ACCESS-POINTS	
default-ap650	AP650		default				ACCESS-POINTS	
default-ap6511	AP6511		default				ACCESS-POINTS	
default-ap6521	AP6521		default				ACCESS-POINTS	
default-ap6522	AP6522		default				ACCESS-POINTS	
default-ap6532	AP6532		default				ACCESS-POINTS	
default-ap71xx	AP71XX		default				ACCESS-POINTS	
default-nx9000	NX9000	NOC	default				WIRELESS-CONTROLLERS	
Innovation Center	AP650		default				Innovation Center	

Row Count: 18

Navigate to *Management* → *Settings*. Input the *URL, User Name* and *Password* from the Network Equipment Configuration page. Select *OK* and *Exit.*



URL: http://174.129.163.30:5447/WiNG
User Name: motodemo
Password: •••••••• (reveal)



Profile CS-AP6521 Type AP6521

0 . 0 . 0 . 0 Clear

Facility to Send Log Messages: local7
Syslog Logging Level: ✓ Warning
Console Logging Level: ☑ Warning
Buffered Logging Level: ☑ Warning
Time to Aggregate Repeated Messages: 0 Seconds (0 to 60)
Forward Logs to Controller: ☑ Error

System Event Messages

Event System Policy:
Enable System Events: ☑
Enable System Event Forwarding: ☑

Events E-mail Notification

SMTP Server: Hostname
Port of SMTP: □ 1 (1 to 65,535)
Sender Email Address:
Recipient's Email Address:
Username for SMTP Server:
Password for SMTP Server:

Persist Configuration Across Reloads

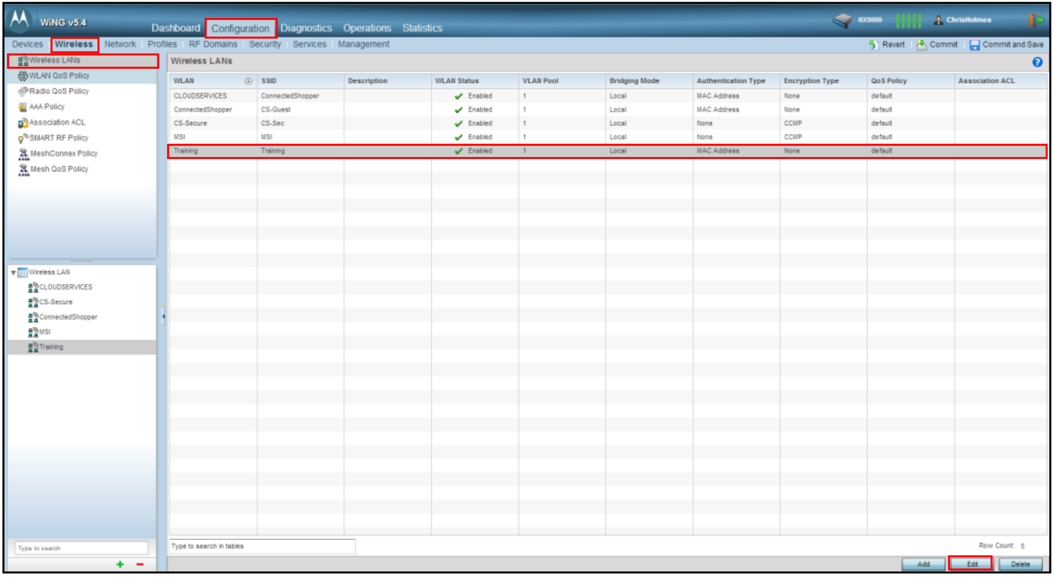
Persist Configuration Across Reloads: Enabled

External Analytics Engine

URL: http:174.129.163.30:5447/WiNG
User Name: motodemo
Password: ****************************
**************************** Reconfirm

1.3.4 *Enable analytics forwarding on the WLAN profile*

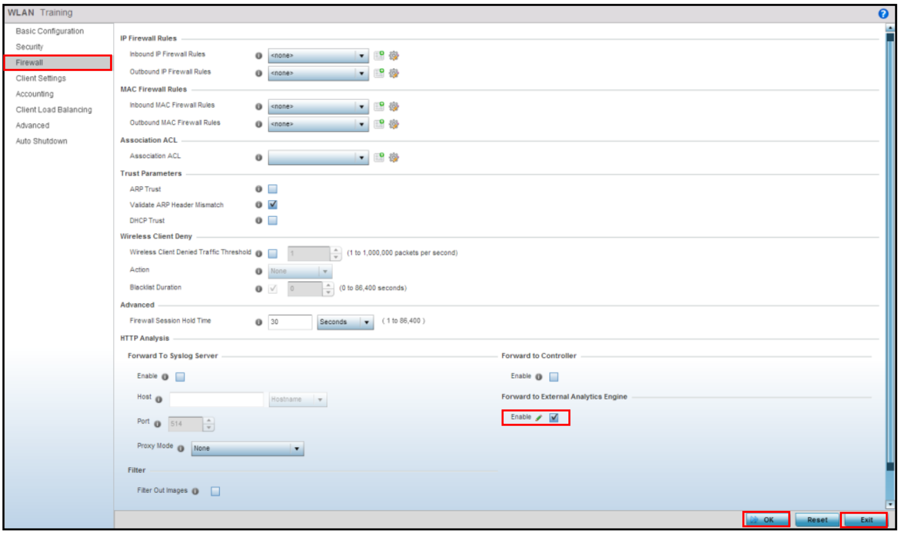
Navigate to *Configuration* → *Wireless* → *Wireless LANs*. Select the WLAN profile created in step 1.2.4. Select *Edit.*



Wireless LANs

WLAN	SSID	Description	WLAN Status	VLAN Pool	Bridging Mode	Authentication Type	Encryption Type	QoS Policy	Association ACL
CLOUDSERVICES	ConnectedShopper		✓ Enabled	1	Local	MAC Address	None	default	
ConnectedShopper	CS-Guest		✓ Enabled	1	Local	MAC Address	None	default	
CS-Secure	CS-Sec		✓ Enabled	1	Local	None	CCMP	default	
MSI	MSI		✓ Enabled	1	Local	None	CCMP	default	
Training	Training		✓ Enabled	1	Local	MAC Address	None	default	

Navigate to *Firewall.* Check *Enable* under *Forward to External Analytics Engine*. Select *OK* and *Exit.*



IP Firewall Rules

Inbound IP Firewall Rules <none>

Outbound IP Firewall Rules <none>

MAC Firewall Rules

Inbound MAC Firewall Rules <none>

Outbound MAC Firewall Rules <none>

Association ACL

Association ACL:

Trust Parameters

ARP Trust □

Validate ARP Header Mismatch ☑

DHCP Trust □

Wireless Client Deny

Wireless Client Denied Traffic Threshold □ 1 (1 to 1,000,000 packets per second)

Action: None

Blacklist Duration ✓ 0 (0 to 86,400 seconds)

Advanced

Firewall Session Hold Time: 30 Seconds (1 to 86,400)

HTTP Analysis

Forward To Syslog Server

Enable □

Host: Hostname

Port: 514

Proxy Mode: None

Filter

Filter Out Images □

Forward to Controller

Enable □

Forward to External Analytics Engine

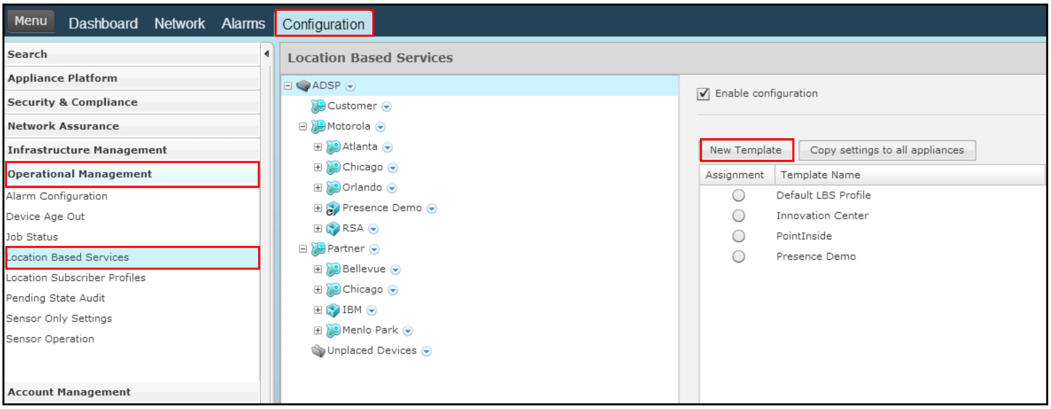
Enable ☑

Commit and Save the changes to complete the configuration.

1.4 ADSP 9.03 Presence Configuration

1.4.1 Enable presence detection

Navigate to *Configuration → Operational Management → Location Based Services.* Select *New Template*.

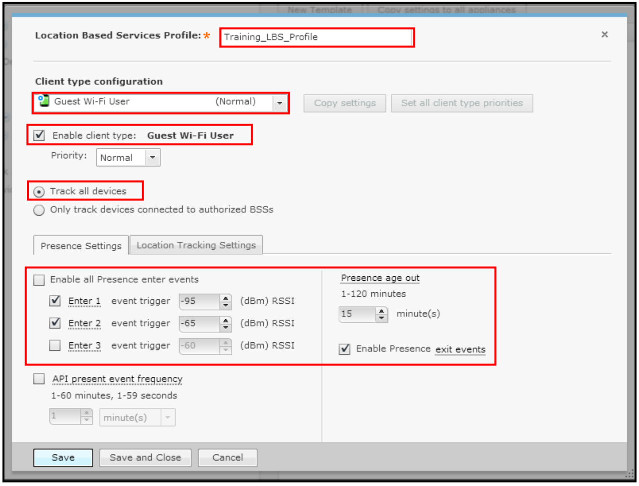


☑ Enable configuration

Assignment	Template Name
○	Default LBS Profile
○	Innovation Center
○	PointInside
○	Presence Demo

Create the name of the *Location Based Services* profile in the text box. Select *Guest Wi-Fi User* from the *Client type configuration* drop-down box. Check *Enable client type.* Check *Track all devices*. Uncheck *Enter 3.* Set the *Presence age out* to *15 minutes.* Check *Enable Presence exit events.*

The *Enter 1* and *Enter 2* event triggers will need to be configured based on the RF environment. The default triggers are *-95 (dBm) RSSI* for *Enter 1* and *-75 (dBm) RSSI* for *Enter 2.* For best practice recommendations, see section 3.1.1.


New Template
Copy settings to all appliances
×
Copy settings
Set all client type priorities
Presence Settings
Location Tracking Settings
Save
Save and Close
Cancel

Location Based Services Profile: * Training_LBS_Profile

Client type configuration

Guest Wi-Fi User (Normal)

☑ Enable client type: **Guest Wi-Fi User**

Priority: Normal

● Track all devices

○ Only track devices connected to authorized BSSs

□ Enable all Presence enter events

☑ Enter 1 event trigger -95 (dBm) RSSI

☑ Enter 2 event trigger -65 (dBm) RSSI

□ Enter 3 event trigger -60 (dBm) RSSI

Presence age out

1-120 minutes

15 minute(s)

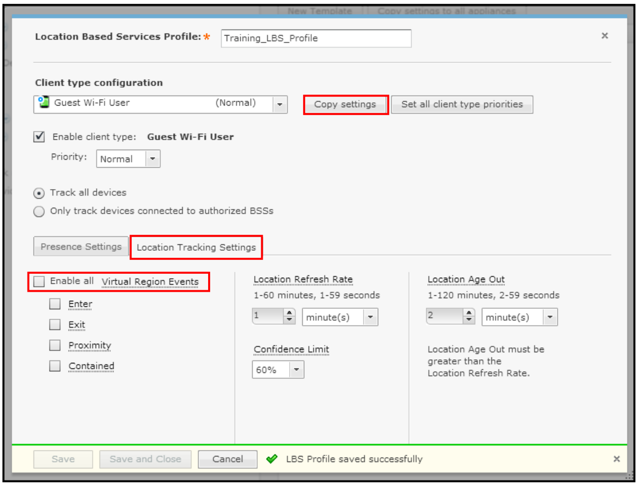
☑ Enable Presence exit events

□ API present event frequency

1-60 minutes, 1-59 seconds

1 minute(s)

Navigate to the *Location Tracking Settings* tab. Uncheck *Enable all Virtual Region Events.* Select *Save.* Select *Copy Settings.*


New Template
Copy settings to all appliances
×
Copy settings
Set all client type priorities
Presence Settings
Location Tracking Settings
Save
Save and Close
Cancel
×

Location Based Services Profile: * Training_LBS_Profile

Client type configuration

Guest Wi-Fi User (Normal)

☑ Enable client type: **Guest Wi-Fi User**

Priority: Normal

● Track all devices

○ Only track devices connected to authorized BSSs

□ Enable all Virtual Region Events

□ Enter

□ Exit

□ Proximity

□ Contained

Location Refresh Rate

1-60 minutes, 1-59 seconds

1 minute(s)

Confidence Limit

60%

Location Age Out

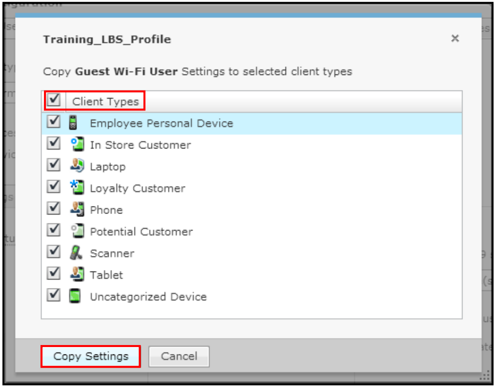
1-120 minutes, 2-59 seconds

2 minute(s)

Location Age Out must be greater than the Location Refresh Rate.

✓ LBS Profile saved successfully

Select the client types that require location based services enabled. Select *Copy Settings*. For best practice recommendations, see section 3.1.2



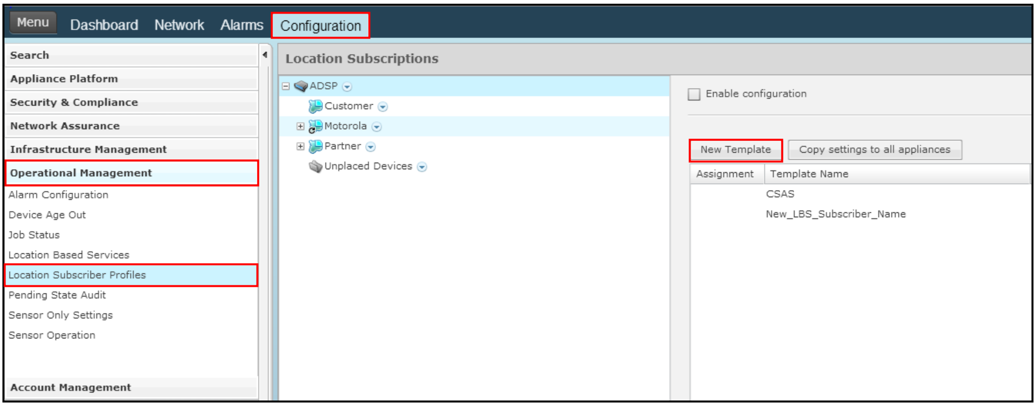
Training_LBS_Profile

Copy **Guest Wi-Fi User** Settings to selected client types

- ☑ Client Types
- ☑ Employee Personal Device
- ☑ In Store Customer
- ☑ Laptop
- ☑ Loyalty Customer
- ☑ Phone
- ☑ Potential Customer
- ☑ Scanner
- ☑ Tablet
- ☑ Uncategorized Device

1.4.2 Configure the API to push data to the cloud service

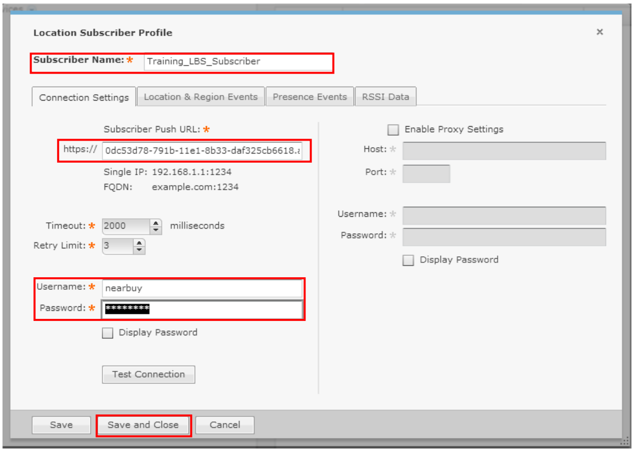
Navigate to *Configuration* → *Operation Management* → *Location Subscriber Profiles*. Select *New Template.*



□ Enable configuration

Assignment	Template Name
	CSAS
	New_LBS_Subscriber_Name

Input a *Subscriber Name* in the text box. Under the *Connection* Settings tab. Input the *URL, Username,* and *Password* from the Network Equipment Configuration page. Select *Save and Close.*



Location Subscriber Profile

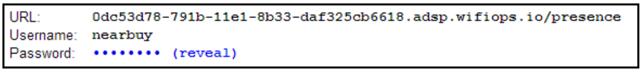
Subscriber Name: * Training_LBS_Subscriber

Subscriber Push URL: *
https:// 0dc53d78-791b-11e1-8b33-daf325cb6618.a
Single IP: 192.168.1.1:1234
FQDN: example.com:1234

Timeout: * 2000 milliseconds
Retry Limit: * 3

Username: * nearbuy
Password: * ********
□ Display Password

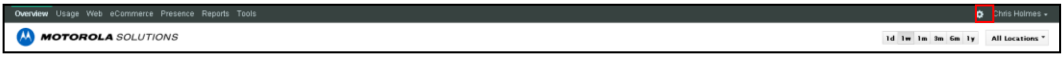
□ Enable Proxy Settings
Host: *
Port: *
Username: *
Password: *
□ Display Password



URL:	0dc53d78-791b-11e1-8b33-daf325cb6618.adsp.wifiops.io/presence
Username:	nearbuy
Password:	•••••••• (reveal)

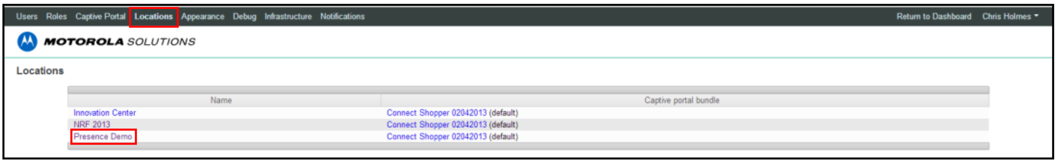
2 Web Analytics Configuration

From the browser, navigate to Web Analytics Portal URL. Select the gear icon to change the dashboard to the configuration view.



2.1 Locations Configuration

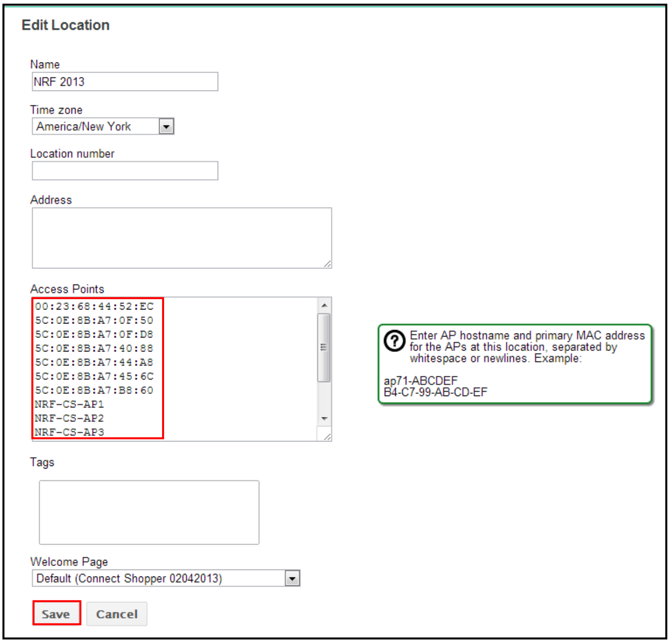
To enable the configured network, the devices must be added to the Web Analytics Portal. Select the *Locations* tab. Select a location to edit.



Locations

Name	Captive portal bundle
Innovation Center	Connect Shopper 02042013 (default)
NRF 2013	Connect Shopper 02042013 (default)
Presence Demo	Connect Shopper 02042013 (default)

Input the AP hostnames and primary MAC addresses for the APs at the location. Select *Save.*



Edit Location

Name
NRF 2013

Time zone
America/New York

Location number

Address

Access Points

```
00:23:68:44:52:EC
5C:0E:8B:A7:0F:50
5C:0E:8B:A7:0F:D8
5C:0E:8B:A7:40:88
5C:0E:8B:A7:44:A8
5C:0E:8B:A7:45:6C
5C:0E:8B:A7:B8:60
NRF-CS-AP1
NRF-CS-AP2
NRF-CS-AP3
```

Enter AP hostname and primary MAC address for the APs at this location, separated by whitespace or newlines. Example:

ap71-ABCDEF
B4-C7-99-AB-CD-EF

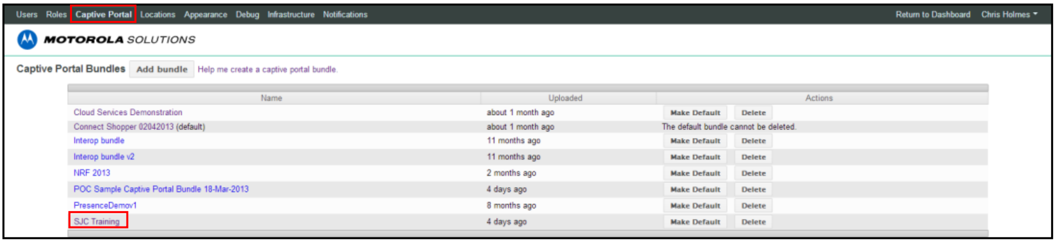
Tags

Welcome Page
Default (Connect Shopper 02042013)

2.2 Captive Portal Bundle Configuration

2.2.1 Access the Captive Portal bundle

Select the *Captive Portal* tab. Select an existing captive portal bundle as the base configuration.

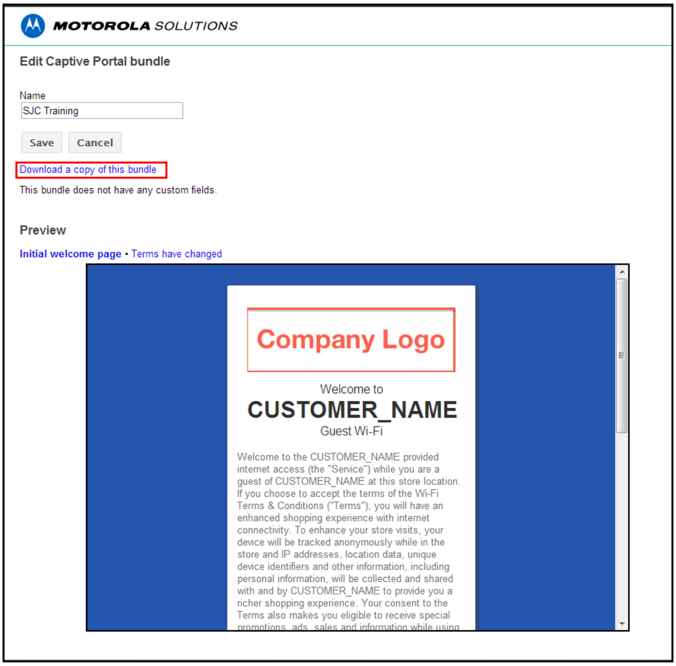


Captive Portal Bundles

Help me create a captive portal bundle.

Name	Uploaded	Actions
Cloud Services Demonstration	about 1 month ago	Make Default Delete
Connect Shopper 02042013 (default)	about 1 month ago	The default bundle cannot be deleted.
Interop bundle	11 months ago	Make Default Delete
Interop bundle v2	11 months ago	Make Default Delete
NRF 2013	2 months ago	Make Default Delete
POC Sample Captive Portal Bundle 18-Mar-2013	4 days ago	Make Default Delete
PresenceDemov1	8 months ago	Make Default Delete
SJC Training	4 days ago	Make Default Delete

Download and unzip the bundle.



Edit Captive Portal bundle

Name: SJC Training

Download a copy of this bundle

This bundle does not have any custom fields.

Preview

Initial welcome page • Terms have changed

Welcome to
CUSTOMER_NAME
Guest Wi-Fi

Welcome to the CUSTOMER_NAME provided internet access (the "Service") while you are a guest of CUSTOMER_NAME at this store location. If you choose to accept the terms of the Wi-Fi Terms & Conditions ("Terms"), you will have an enhanced shopping experience with internet connectivity. To enhance your store visits, your device will be tracked anonymously while in the store and IP addresses, location data, unique device identifiers and other information, including personal information, will be collected and shared with and by CUSTOMER_NAME to provide you a richer shopping experience. Your consent to the Terms also makes you eligible to receive special promotions, ads, sales and information while using

2.2.2 Edit the Captive Portal bundle

Create a preview of the welcome page by filling in the customer's information in the *index.html* file found in the *preview* folder. Use a text editor to find the following fields and replace the placeholder with the customer’s information.

CUSTOMER_NAME

CUSTOMER_LEGAL_NAME

CUSTOMER_INTELLECTUAL_PROPERTY_LAW_ADDRESS

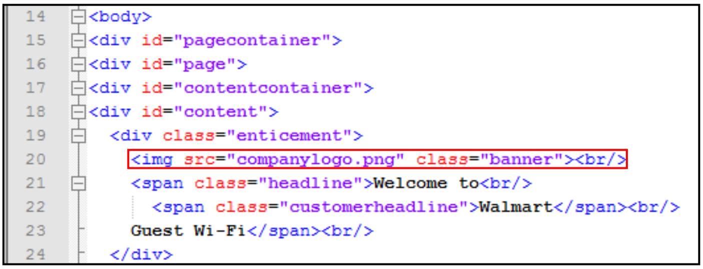
CUSTOMER_NOTICES_ADDRESS

CUSTOMER_NOTICES_ATTENTION

CUSTOMER_ADDRESS

CUSTOMER_EMAIL

Replace the company logo image in the preview folder. The size of the logo is irrelevant because the image will automatically be scaled to fit the captive portal page. The HTML "img" tag on line 20 of *index.html* can be edited to reflect the name of an image that is not the default, *companylogo.png.* The image type can be any of the standard image types for HTML, including JPG, PNG, and GIF.



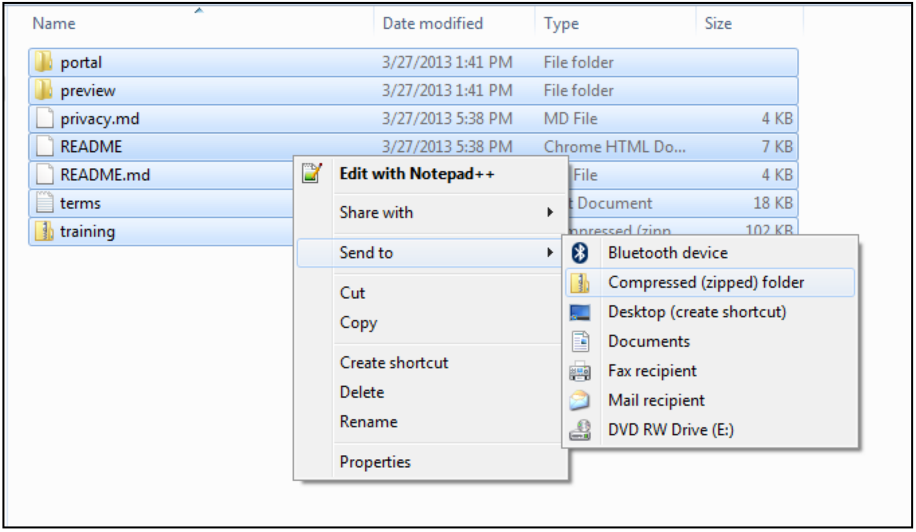
```
14  <body>
15  <div id="pagecontainer">
16  <div id="page">
17  <div id="contentcontainer">
18  <div id="content">
19    <div class="enticement">
20      <img src="companylogo.png" class="banner"><br/>
21      <span class="headline">Welcome to<br/>
22        <span class="customerheadline">Walmart</span><br/>
23      Guest Wi-Fi</span><br/>
24    </div>
```

Submit the preview to Guy Halpern at Motorola for final review.

2.2.3 Create the Captive Portal bundle

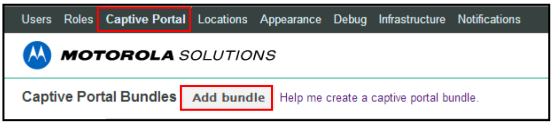
After obtaining Guy Halpern's approval, create the actual captive portal bundle. Zip the *preview* directory and send it to the customer for review. Make the requested customer changes. Create the captive portal bundle by zipping the files.

✓ ***NOTE*** Zip the captive portal bundle by selecting all of the files and zipping to a folder. The files must reside in the root location of the zip file.

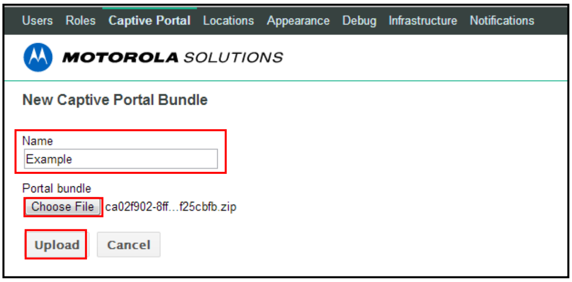


Name	Date modified	Type	Size
portal	3/27/2013 1:41 PM	File folder	
preview	3/27/2013 1:41 PM	File folder	
privacy.md	3/27/2013 5:38 PM	MD File	4 KB
README	3/27/2013 5:38 PM	Chrome HTML Do...	7 KB
README.md		File	4 KB
terms		t Document	18 KB
training		mpressed (zipp	102 KB

Navigate to the *Captive Portal* tab of the settings dashboard. Select *Add bundle.*



Create the name of the bundle in the text box. Select *Choose File* and select the zip file created in the previous step. Select *Upload.*

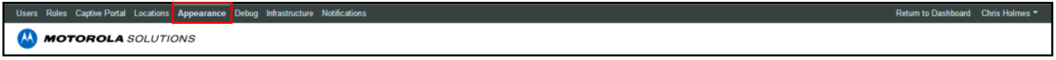


Name: Example

Portal bundle: Choose File ca02f902-8ff...f25cbfb.zip

2.3 Appearance Configuration

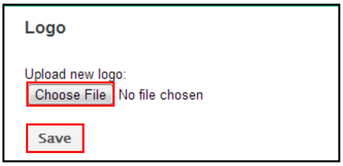
Select the *Appearance* tab.

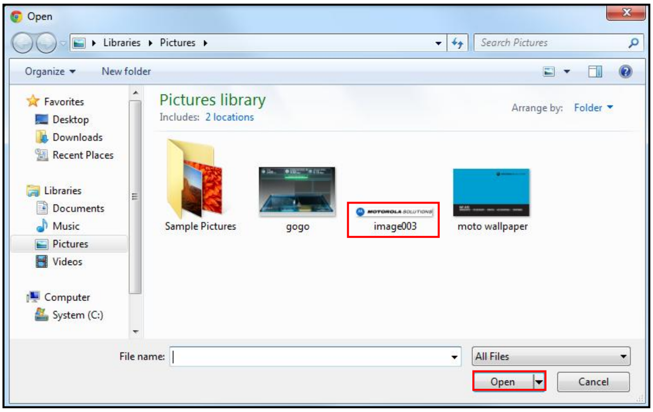


2.3.1 Brand logos

The logo that appears at the top of every landing page can be changed to brand the web analytics portal for a customer.

Select *Choose File*. Highlight the desired logo image. Select *Open*. Select *Save*

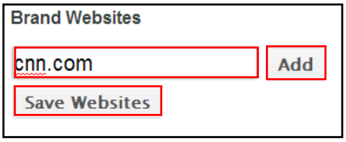




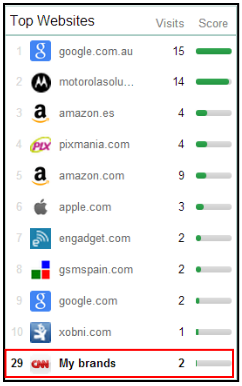
2.3.2 Brand websites

A list of the customer's branded websites can be specified. The rank of the customer's websites will be listed on the main overview page under *My brands.*

Input the name of the website in the text box. Select *Add.* Select *Save Websites.*


Brand Websites

cnn.com

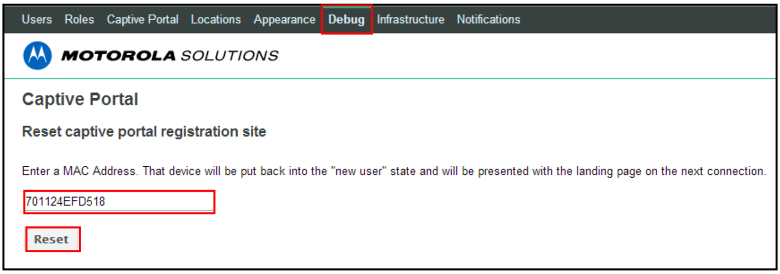


	Top Websites	Visits	Score
1	google.com.au	15	
2	motorolasolu...	14	
3	amazon.es	4	
4	pixmania.com	4	
5	amazon.com	9	
6	apple.com	3	
7	engadget.com	2	
8	gsmspain.com	2	
9	google.com	2	
10	xobni.com	1	
29	CNN **My brands**	2	

2.4 Debug

The Debug setting is used to reset a device back to the “new user” state. The device will be presented with the landing page on the next connection.

Select the *Debug tab*. Input the MAC address of the device into the text box. Select *Reset.*



Captive Portal

Reset captive portal registration site

Enter a MAC Address. That device will be put back into the "new user" state and will be presented with the landing page on the next connection.

701124EFD518

Reset

2.5 Notifications Configuration

The following *Events* can be posted to an external server from the API via an http request by creating a *Destination.*

Wi-Fi Enrollment

Wi-Fi Conneciton

Arrival Outside

Arrival Inside

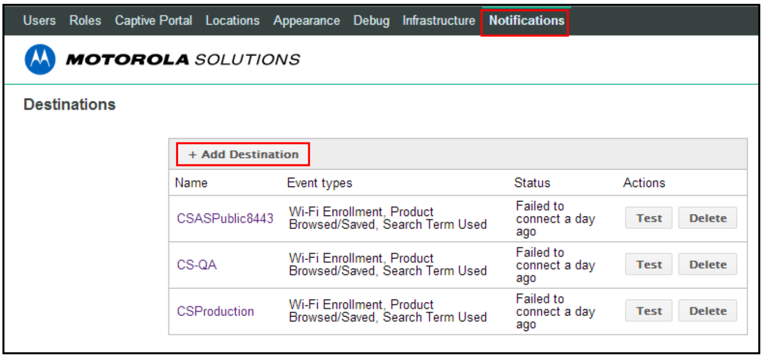
Inside Departure

Product Browed/Saved

Website Visited

Search Term Used

Select the *Notifications* tab. Select + *Add Destination.*

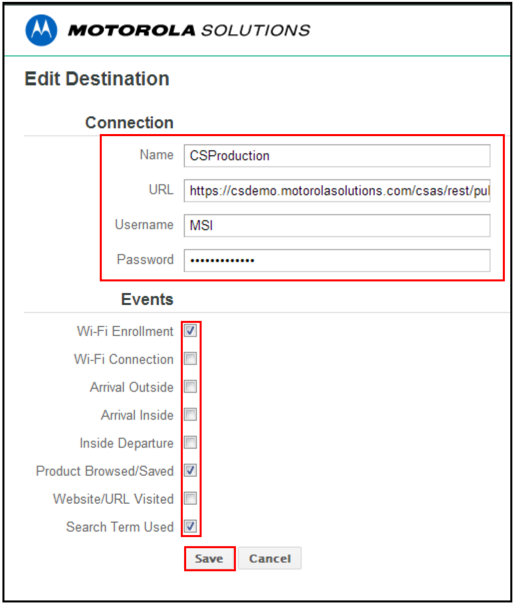


Destinations

+ Add Destination

Name	Event types	Status	Actions
CSASPublic8443	Wi-Fi Enrollment, Product Browsed/Saved, Search Term Used	Failed to connect a day ago	Test Delete
CS-QA	Wi-Fi Enrollment, Product Browsed/Saved, Search Term Used	Failed to connect a day ago	Test Delete
CSProduction	Wi-Fi Enrollment, Product Browsed/Saved, Search Term Used	Failed to connect a day ago	Test Delete

Create the name of the policy in the *Name* text box. Input the *URL, Username* and *Password.* Select the *Events* that will be exported. Select *Save.*



Edit Destination

Connection

Name CSProduction

URL https://csdemo.motorolasolutions.com/csas/rest/pul

Username MSI

Password ••••••••••••••

Events

☑ Wi-Fi Enrollment
☐ Wi-Fi Connection
☐ Arrival Outside
☐ Arrival Inside
☐ Inside Departure
☑ Product Browsed/Saved
☐ Website/URL Visited
☑ Search Term Used

3 Best Practices

3.1 Presence Configuration

3.1.1 Event triggers

The *Enter 1* trigger is the RSSI threshold where the end user is considered to be outside of the store. The *Enter 2* trigger event is the RSSI threshold where the end user is considered to be inside of the store. An RF analysis of the environment should be conducted to determine the appropriate trigger levels.

3.1.2 Client location tracking

The best practice recommendation is to enable location tracking for the following client types: *In Store Customer, Loyalty Customer, Potential Customer* and *Uncategorized Device.*

3.2 Update Intervals

3.2.1 Real time applications

For real time applications, such as client demos, it is recommended to lower the WiNG analytics update intervals to one second. These settings determine how long WiNG attempts to accumulate data before forwarding it upstream. In a live demo, it is best practice to update the analytics in real time. If the command line is not accessible, be aware that the default update interval is 60 seconds. The following commands must be executed through the command line interface:

From the AP to the NX controller:

```
#http-analyze update-interval 1 # seconds
```

From the NX controller to the Cloud Captive Portal & Analytics Service:

```
#http-analyze external-server update-interval 1 # seconds
```

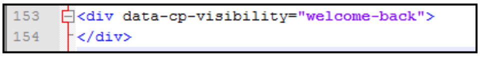
3.2.2 Asychronous Applications

For applications where web analytics not need to be updated in real time, it is recommended to keep the update interval to it’s default value of 60 seconds.

3.3 Privacy

3.3.1 Welcome Back page

The Welcome Back page can remind people about the service and require them to click through again to get back onto the network. The page is added to the captive portal bundle by adding a <div data-cp-visibility="welcome-back">…</div>. The time to control how often the page must be clicked through is set on the back end. Re-registration is currently supported only after some period of time, not after a number logins or idle time.



```
<div data-cp-visibility="welcome-back">
</div>
```

3.3.2 Terms Have Changed page

The Terms Have Changed requires the end user to re-agree to the Privacy Statement and the Terms and Conditions when the file is updated in the captive portal bundle.

3.4 Access Points

3.4.1 Reccomended APs

Recommended APs have been field tested and require no additional configuration to work with web analytics.

- AP622/6522
- AP650/6532
- AP7131
- AP8132

3.4.2 Compatible APs

These APs may require a software upgrade to adopt successfully and report data to the web analytics server.

- AP621/6521
- AP6511

MOTOROLA SOLUTIONS

Motorola Solutions, Inc.
1301 E. Algonquin Rd.
Schaumburg, IL 60196-1078, U.S.A.
http://www.motorolasolutions.com