WiNG 5.X Feature Guide

802.11i Wireless LANs

October 2010

Revision 1

Table of Contents:

1. Overview:

Wireless LANs are defined individually within a WiNG 5.0 system and can be assigned to groups of Access Point radios using profiles or to individual Access Point radios as device overrides. Wireless LAN specific parameters such as SSID names and VLAN IDs may also be overridden using Wireless LAN overrides assigned to a RF Domain or defined on an Access Point as a device overrides.

Each Wireless LAN consists of policies and configuration parameters which define the basic operating parameters as well as authentication, encryption, QoS and firewall options. Changes made to a Wireless LANs configuration or assigned policy are automatically inherited by all Access Points serving the Wireless LAN.

Policies	Configuration Parameters	
▪ AAA Policy	Basic Configuration:	Firewall:
▪ Association ACL Policy	▪ SSID	▪ IP Firewall Rules
▪ Captive Portal Policy	▪ Description	▪ MAC Firewall Rules
▪ IP Access List	▪ Status	▪ Association ACL
▪ MAC Access List	▪ Broadcast Settings	▪ Trust Parameters
▪ QoS Policy	▪ VLAN Assignment	▪ Wireless Client Deny
	Security:	▪ Advanced
	▪ Authentication	Client Settings:
	▪ Captive Portal	▪ Client Settings
	▪ Encryption	▪ Motorola Client Extensions
	▪ Key Settings	
	▪ Key Rotation	
	▪ Fast Roaming	
	▪ Advanced	

Table 1.0 – Wireless LAN Configuration Elements

2. Managing Wireless LANs:

802.11i Wireless LANs can be added, edited or removed from the master configuration using the CLI or WiNG 5.0 UI. Configuration changes using the CLI are made in the Wireless LAN configuration context while changes in the WiNG 5.0 UI are made by selecting the Configuration tab. All changes made to Wireless LAN or assigned policy are automatically inherited by the Access Points serving the Wireless LAN.

2.1 Adding Wireless LANs:

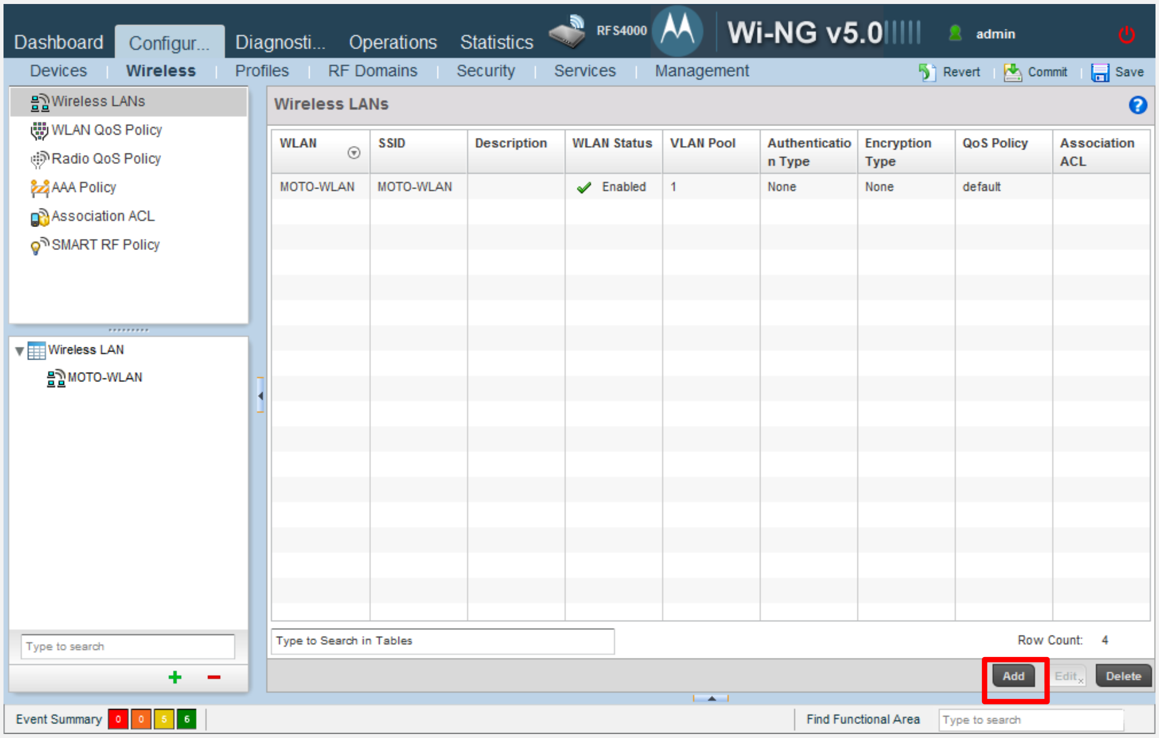
Wireless LANs can be added using the CLI by issuing the ***wlan*** command followed by the Wireless LAN ***name***. The command will create the new Wireless LAN and will access configuration context for the Wireless LAN allowing parameters to be defined and policies to be assigned. The new Wireless LAN is only added to the running-configuration when the ***commit*** command is invoked.

Adding Wireless LANs:

```
rfsX000(config)# wlan <wlan-name>
rfsX000(config-wlan-<wlan-name>)#
```

Wireless LANs can be added using the WiNG 5.0 UI by clicking ***Configuration > Wireless > Wireless LANs > Add***. Enter the ***WLAN*** name then click ***OK***. The new Wireless LAN is only added to the running-configuration when a ***Commit*** is invoked.

Configuration > Wireless > Wireless LANs > Add:



Wireless LANs

WLAN	SSID	Description	WLAN Status	VLAN Pool	Authentication Type	Encryption Type	QoS Policy	Association ACL
MOTO-WLAN	MOTO-WLAN		✓ Enabled	1	None	None	default	

Row Count: 4

2.2 Editing Wireless LANs:

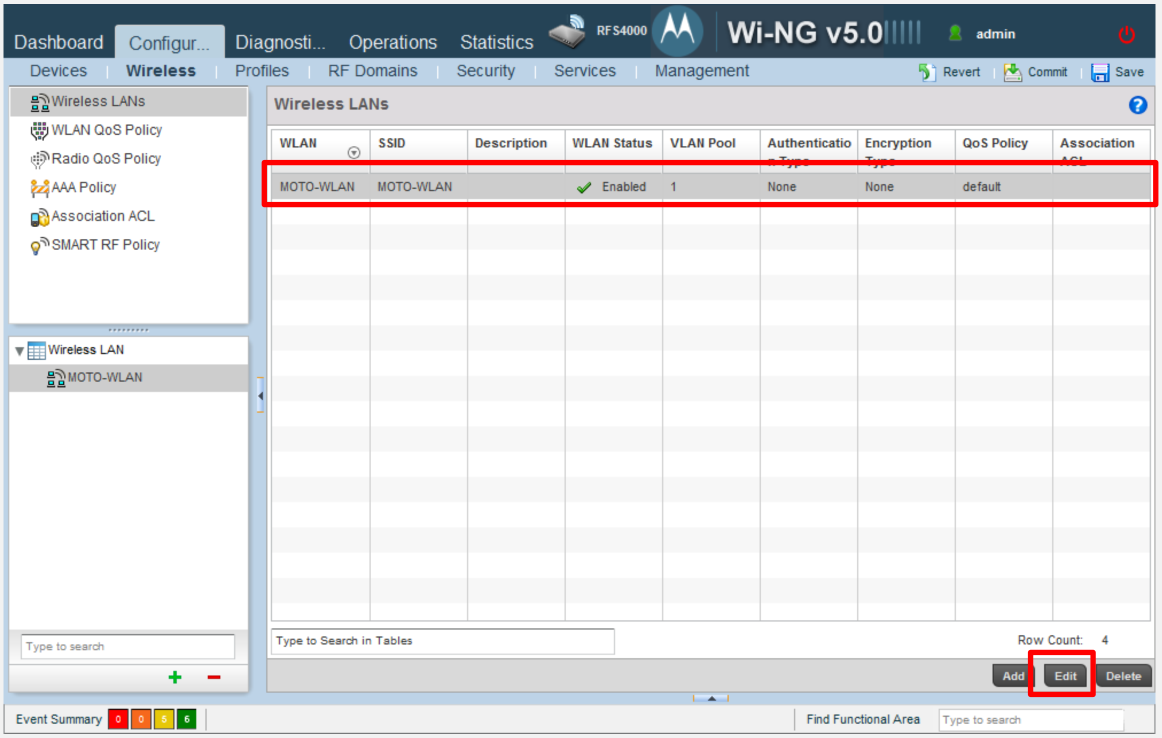
Wireless LANs can be edited using the CLI by issuing the ***wlan*** command followed by the Wireless LAN ***name***. The command will access configuration context for the Wireless LAN allowing configuration parameters and policy assignments to be modified. Configuration changes are only applied to the running-configuration when the ***commit*** command is invoked.

Editing Wireless LANs:

```
rfsX000(config)# wlan <wlan-name>
rfsX000(config-wlan-<wlan-name>)#
```

Wireless LANs can be edited in the WiNG 5.0 UI by clicking ***Configuration > Wireless > Wireless LANs*** selecting the Wireless LAN name to modify then clicking ***Edit***. Configuration changes are only applied to the running-configuration when a ***Commit*** is invoked.

Configuration > Devices > Adoption Policy > Add:



Wireless LANs

WLAN	SSID	Description	WLAN Status	VLAN Pool	Authentication Type	Encryption Type	QoS Policy	Association ACL
MOTO-WLAN	MOTO-WLAN		✓ Enabled	1	None	None	default	

Row Count: 4

2.3 Deleting Wireless LANs:

Wireless LANs can be deleted using the CLI by issuing the ***no wlan*** command followed by the Wireless LAN ***name***. The Wireless LAN will be removed from the running-configuration when the ***commit*** command is invoked.

If the Wireless LAN is assigned to a profile or device a warning will be displayed when the initial ***commit*** command is invoked. A second ***commit*** is required to remove the Wireless LAN and any profile or device associations.

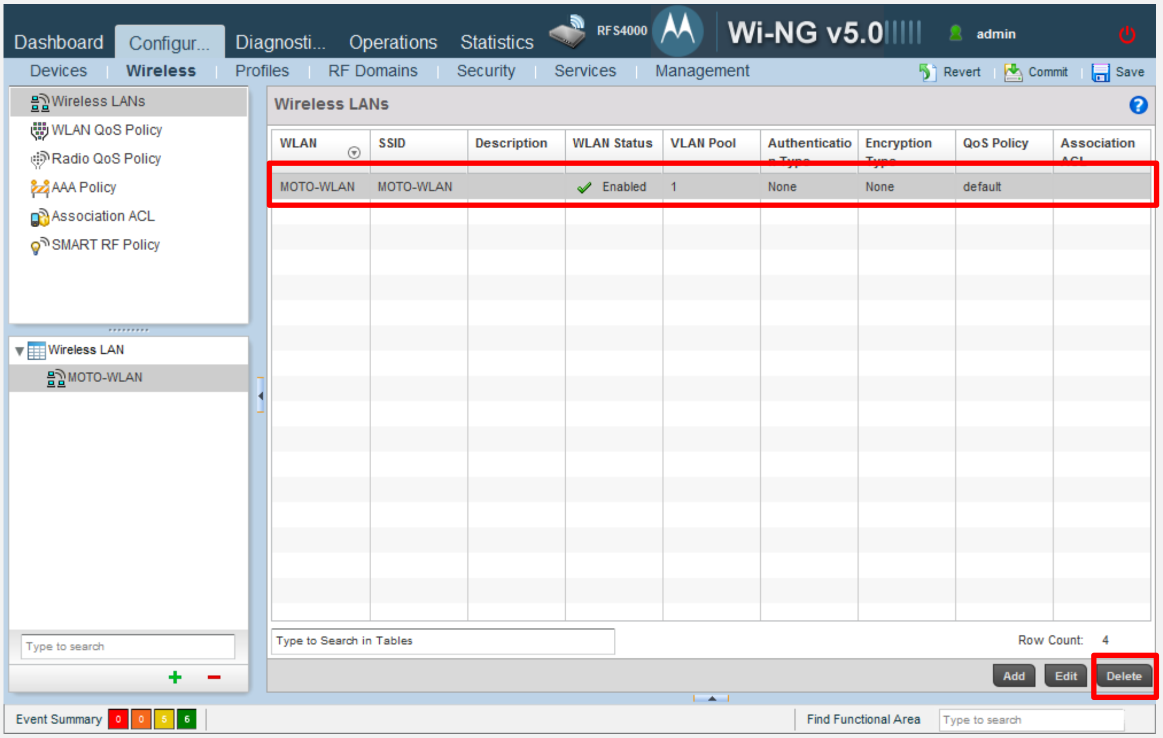
Removing Wireless LANs:

```
rfsX000(config)# no wlan <wlan-name>
```

Wireless LANs can be removed in the WiNG 5.0 UI by clicking ***Configuration > Wireless > Wireless LAN*** selecting the Wireless LAN name to remove then clicking ***Delete***. The Wireless LAN will be removed from the running-configuration when a ***Commit*** is invoked.

If the Wireless LAN is assigned to a profile or device a warning message will be displayed confirming if you want to ***commit*** or ***revert*** the changes. Selecting ***Commit*** will remove the Wireless LAN from the running-configuration along with any profile or device associations.

Configuration > Devices > Adoption Policy > Adoption-Policy-Name > Delete:



WLAN	SSID	Description	WLAN Status	VLAN Pool	Authentication Type	Encryption Type	QoS Policy	Association ACL
MOTO-WLAN	MOTO-WLAN		✓ Enabled	1	None	None	default	

Row Count: 4

3. Basic Configuration Parameters:

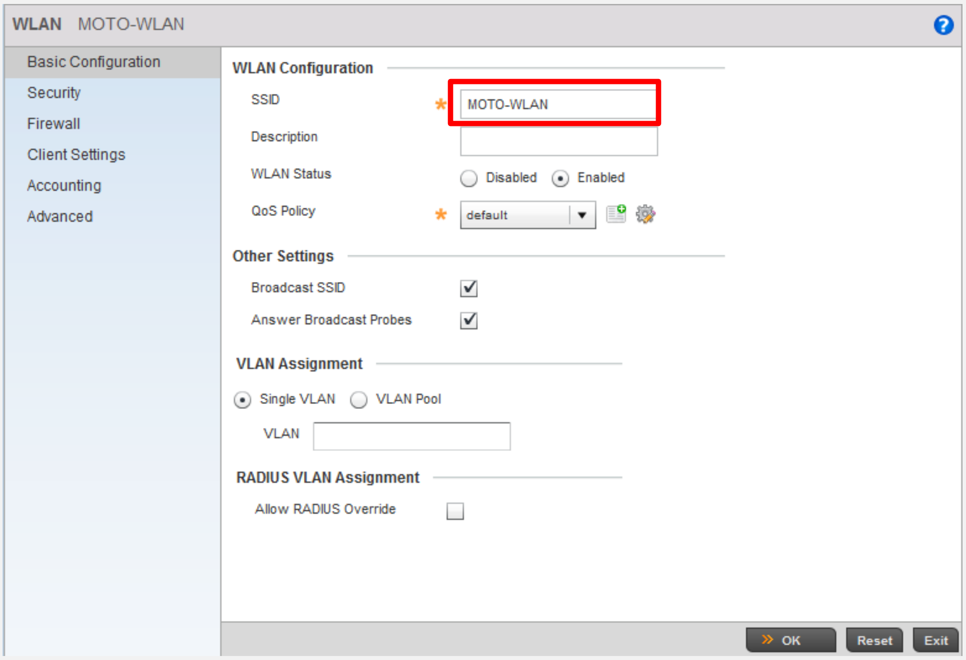
Each 802.11i Wireless LAN contains basic configuration parameters that define the SSID, encryption and authentication options. The following section outlines common configuration parameters required to configure and enable 802.11i Wireless LANs using various authentication types:

3.1 SSID Name:

The Service Set Identifier (SSID) name is mandatory configuration parameter for each Wireless LAN that defines the Wireless LAN name that is advertised to clients by 802.11 radios servicing the Wireless LAN. Each SSID name can contain up to 32 alphanumeric characters and is case sensitive.

Example:

```
ssid MOTO-WLAN
```



WLAN Configuration

SSID * MOTO-WLAN

Description

WLAN Status ○ Disabled ● Enabled

QoS Policy * default

Other Settings

Broadcast SSID ☑

Answer Broadcast Probes ☑

VLAN Assignment

● Single VLAN ○ VLAN Pool

VLAN

RADIUS VLAN Assignment

Allow RADIUS Override □

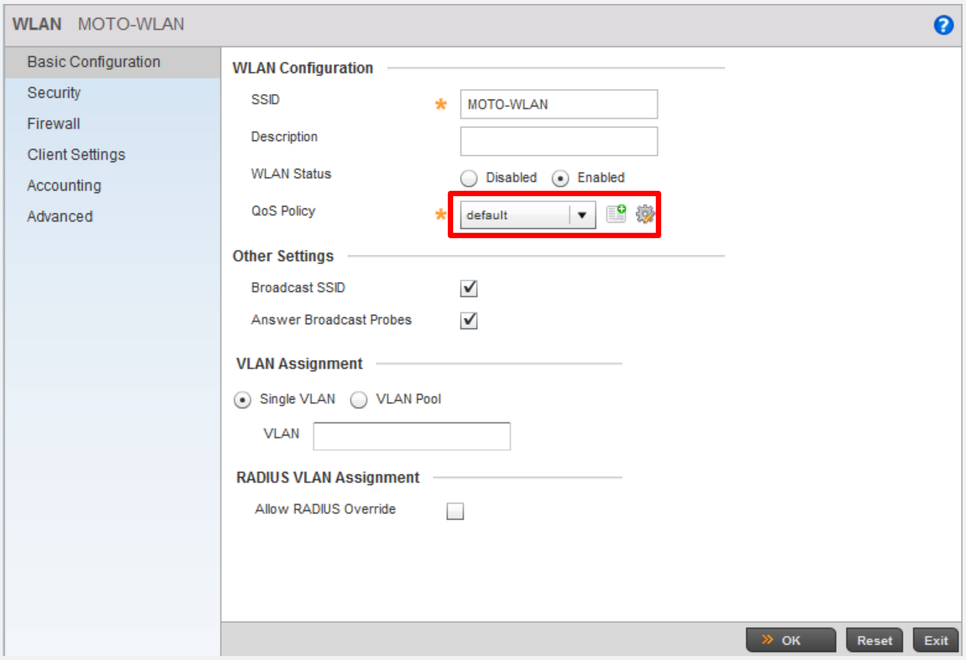
3.2 QoS Policy:

Each Wireless LAN must be assigned a QoS policy that determines the Wireless QoS parameters for the Wireless LAN. By default all Wireless LANs are assigned to a default QoS policy which prioritises traffic using WMM and supports U-APSD power management & TSPEC admission control.

The default QoS policy is adequate for most Wireless LAN deployments and in most cases will not need to be modified. However if the Wireless LAN is supporting non WMM devices or requires rate limiting, a user defined QoS policy can be created and assigned to the Wireless LAN as required.

Example:

```
use wlan-qos-policy default
```



WLAN Configuration

SSID * MOTO-WLAN

Description

WLAN Status ○ Disabled ● Enabled

QoS Policy * default

Other Settings

Broadcast SSID ☑

Answer Broadcast Probes ☑

VLAN Assignment

● Single VLAN ○ VLAN Pool

VLAN

RADIUS VLAN Assignment

Allow RADIUS Override □

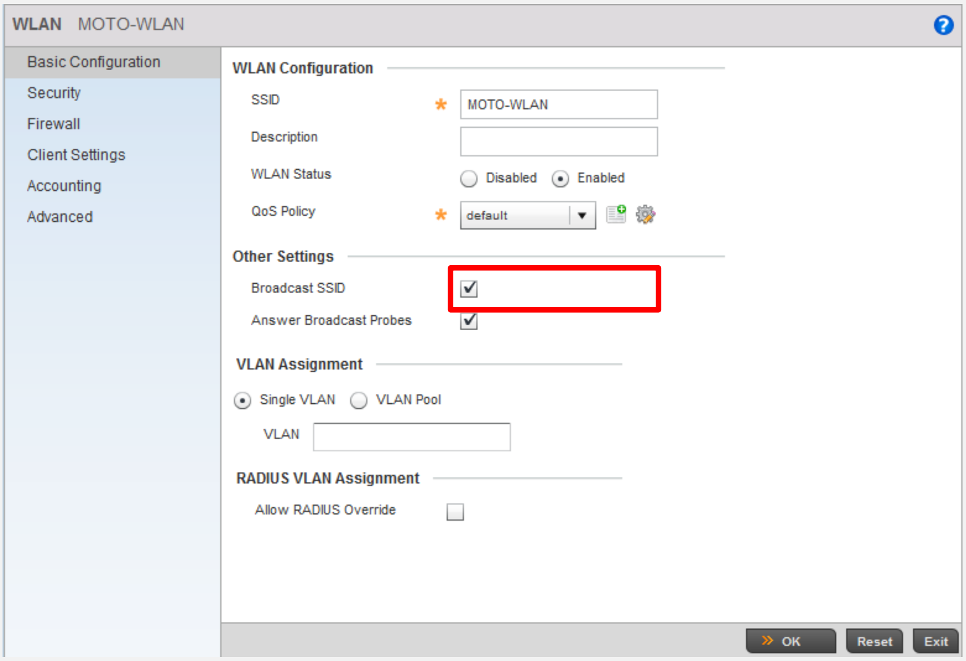
3.3 Broadcast SSID:

The Broadcast SSID configuration parameter determines if the SSID name is advertised by Access Point radios in beacons. By default all radios servicing the Wireless LAN will advertise the SSID in beacons allowing the SSID name to be visible over the air. When the Broadcast SSID parameter is disabled, Access Point radios serving the Wireless LAN will supress the SSID name in the beacons hiding the Wireless LAN.

The SSID is not designed nor intended as a security mechanism. Motorola does not recommend disabling Broadcast SSID as the only mode of security as then SSID name can be recovered by over the air by monitoring management frames.

Example:

```
no broadcast-ssid
```



WLAN MOTO-WLAN

WLAN Configuration

SSID * MOTO-WLAN

Description

WLAN Status ○ Disabled ● Enabled

QoS Policy * default

Other Settings

Broadcast SSID ☑

Answer Broadcast Probes ☑

VLAN Assignment

● Single VLAN ○ VLAN Pool

VLAN

RADIUS VLAN Assignment

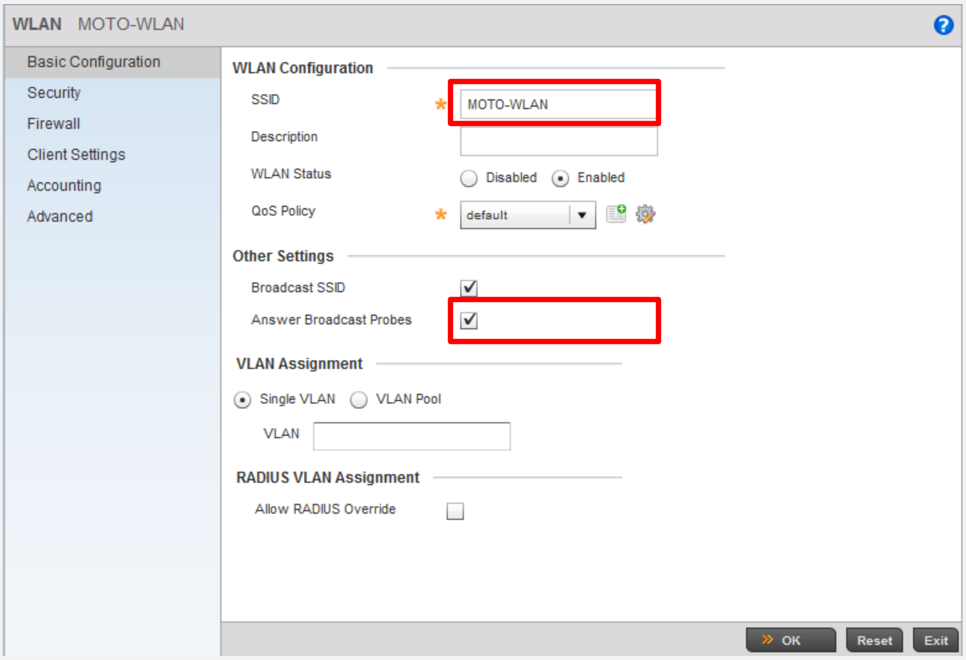
Allow RADIUS Override □

3.4 Answer Broadcast Probes:

The Answer Broadcast Probes configuration parameter determines if the Access Point will respond to probe requests that do not specify a SSID name. Broadcast Probe requests and will respond s is enabled by default but can be optionally disabled if required.

Example:

```
no answer-broadcast-probes
```



WLAN MOTO-WLAN

WLAN Configuration

SSID * MOTO-WLAN

Description

WLAN Status ○ Disabled ● Enabled

QoS Policy * default

Other Settings

Broadcast SSID ☑

Answer Broadcast Probes ☑

VLAN Assignment

● Single VLAN ○ VLAN Pool

VLAN

RADIUS VLAN Assignment

Allow RADIUS Override □

3.5 Single VLAN:

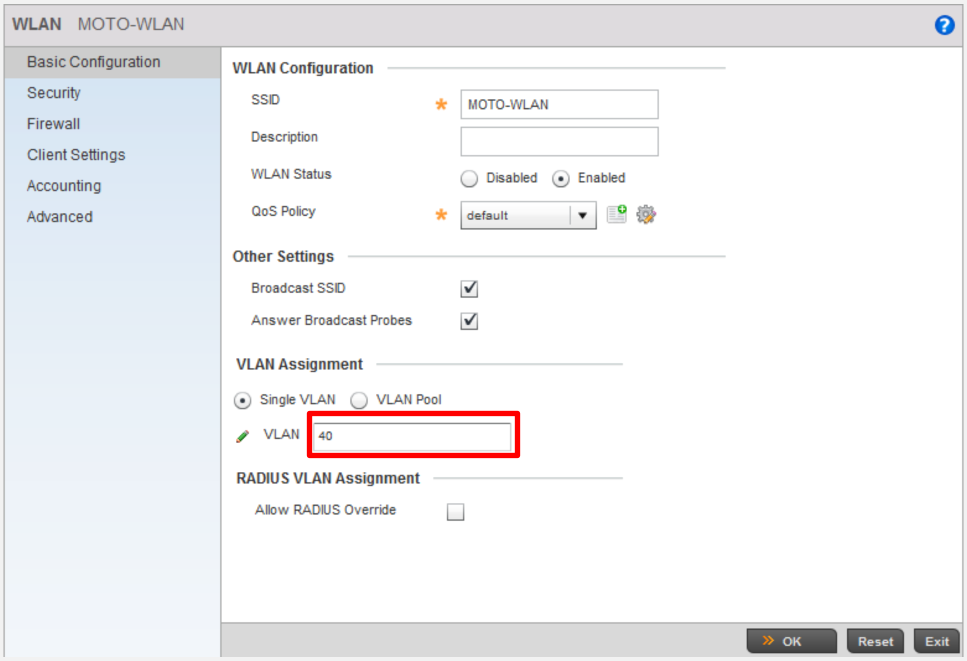
Wireless clients that are permitted access to a Wireless LAN can be assigned to single Virtual LAN ID that determines the network membership of the clients. The single VLAN ID can map users to a VLAN that is forwarded locally by Access Points or an extended VLAN which can tunnel the client's traffic to a Wireless Controller or other Access Point.

VLAN forwarding behaviour is controlled using bridging policies which are assigned to the Wireless Controllers and Access Points. By default all Access Points and Wireless Controllers are assigned a default bridging policy using profiles which automatically extends the VLANs for each Wireless LAN from the Access Points to a Wireless Controller.

A single VLAN ID must be set to a numerical value between 1 and 4094.

Single VLAN Example:

```
vlan 40
```



WLAN Configuration

SSID * MOTO-WLAN

Description

WLAN Status ○ Disabled ● Enabled

QoS Policy * default

Other Settings

Broadcast SSID ☑

Answer Broadcast Probes ☑

VLAN Assignment

● Single VLAN ○ VLAN Pool

VLAN 40

RADIUS VLAN Assignment

Allow RADIUS Override □

3.6 VLAN Pools:

Wireless clients that are permitted access to a Wireless LAN can be assigned to pool of Virtual LAN IDs that determines the network membership of the clients. VLAN pools are useful for larger deployments to distribute clients between multiple small broadcast domains rather that creating one large broadcast domain which can impact battery performance.

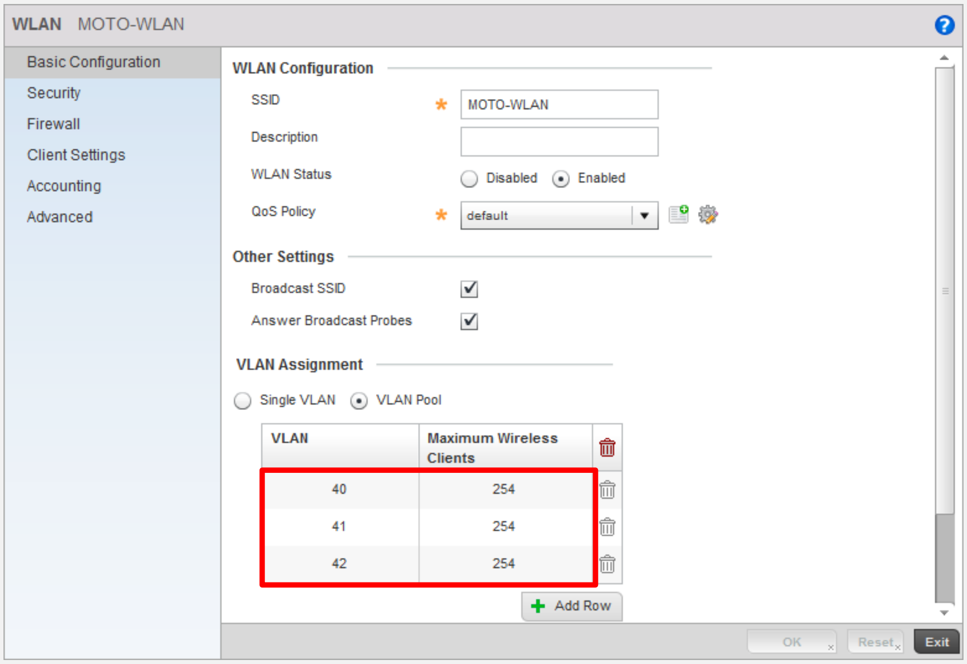
Each VLAN ID in the pool can map users to a local VLAN that is forwarded locally by Access Points or an extended VLAN which can tunnel the client's traffic to a Wireless Controller or other Access Points. As devices are permitted access to the Wireless LAN the Access Point will automatically distribute users between the available VLAN IDs in the pool.

Each VLAN in the pool must be set to a numerical value between 1 and 4094 and may optionally have a limit assigned which determines how many clients are supported by each pool.

The defined VLAN IDs in the pool must ether map users to local VLANs or extended VLANs but not both. Mixing local and extended VLAN IDs in a pool is not recommended or supported in WiNG 5.0.

VLAN Pool Example:

```
vlan-pool-member 40 limit 254
vlan-pool-member 41 limit 254
vlan-pool-member 42 limit 254
```



WLAN Configuration

SSID * MOTO-WLAN

Description

WLAN Status ○ Disabled ● Enabled

QoS Policy * default

Other Settings

Broadcast SSID ☑

Answer Broadcast Probes ☑

VLAN Assignment

○ Single VLAN ● VLAN Pool

VLAN	Maximum Wireless Clients
40	254
41	254
42	254

3.7 RADIUS VLAN Assignment:

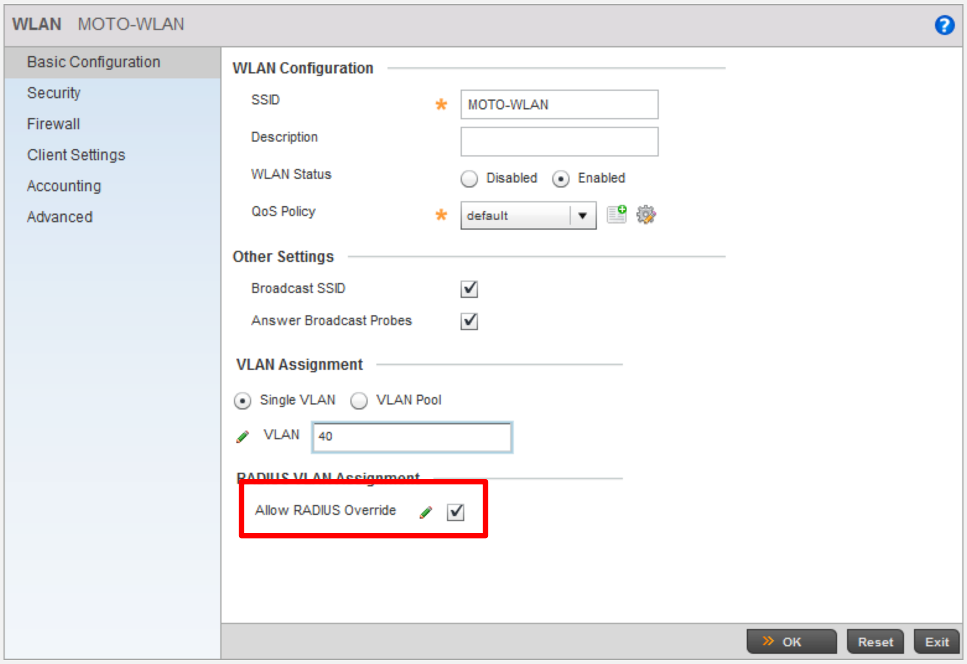
By default wireless clients are assigned a VLAN based on the VLAN IDs defined in the Single VLAN or VLAN Pool. When wireless clients are authenticated against a RADIUS server the RADIUS server can optionally assign the authenticating computer or user to a dynamic VLAN using the IETF standard ***tunnel-private-group-id*** return attribute.

When the RADIUS VLAN assignments option is enabled in a Wireless LAN, a wireless client will be dynamically assigned a VLAN ID based on the value supplied with the ***tunnel-private-group-id*** return attribute. The VLAN can either be bridged locally by the Access Point or be tunnelled to another Access Point or Wireless Controller on the network.

If the RADIUS VLAN assignment is enabled for a Wireless LAN and no VLAN membership is supplied by the RADIUS server, the wireless client will be mapped to a Single VLAN or a defined in the Single VLAN Pool.

RADIUS VLAN Assignment Example:

```
radius vlan-assignment
```



WLAN Configuration

SSID * MOTO-WLAN

Description

WLAN Status ○ Disabled ● Enabled

QoS Policy * default

Other Settings

Broadcast SSID ☑

Answer Broadcast Probes ☑

VLAN Assignment

● Single VLAN ○ VLAN Pool

VLAN 40

RADIUS VLAN Assignment

Allow RADIUS Override ☑

3.8 Authentication Types:

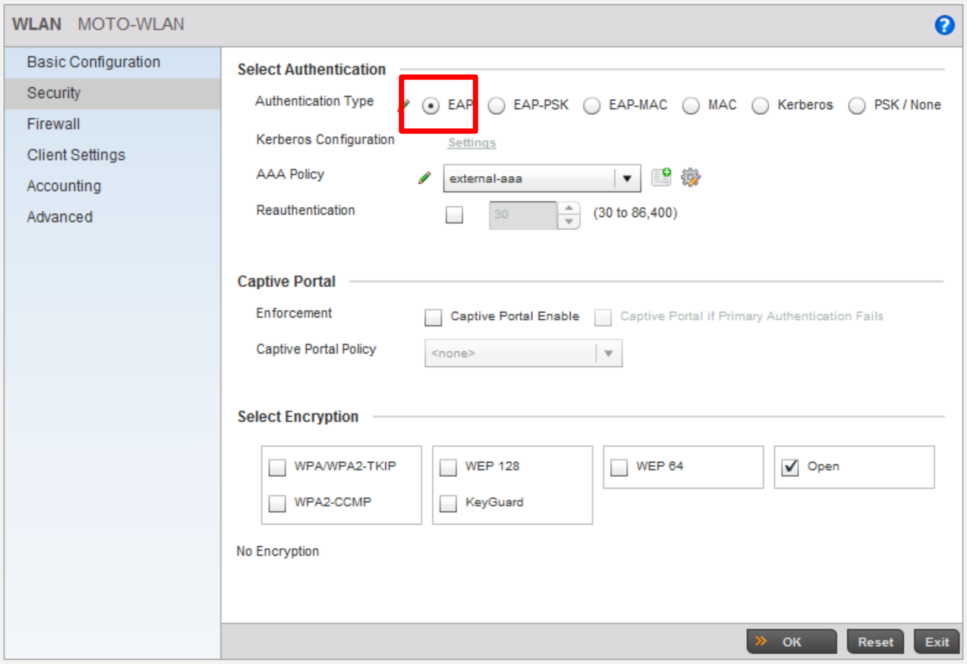
Each 802.11i Wireless LAN can support one authentication type that determines how the wireless session is authenticated. 802.11i wireless sessions can be authenticated using 802.1X and/or pre-shared-keys and support the EAP, EAP-PSK, MAC and PSK/None authentication types.

3.8.1 EAP:

The EAP authentication type can be enabled to authenticate wireless users and/or computers using 802.1X against one or more integrated or external RADIUS servers. To support EAP authentication the Wireless LAN must be assigned a AAA Policy and the RADIUS servers and wireless client must support EAP authentication and the same EAP authentication methods.

Example:

```
authentication-type eap
```



Select Authentication

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

Kerberos Configuration Settings

AAA Policy external-aaa

Reauthentication □ 30 (30 to 86,400)

Captive Portal

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

Captive Portal Policy <none>

Select Encryption

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

□ WPA2-CCMP □ KeyGuard

No Encryption

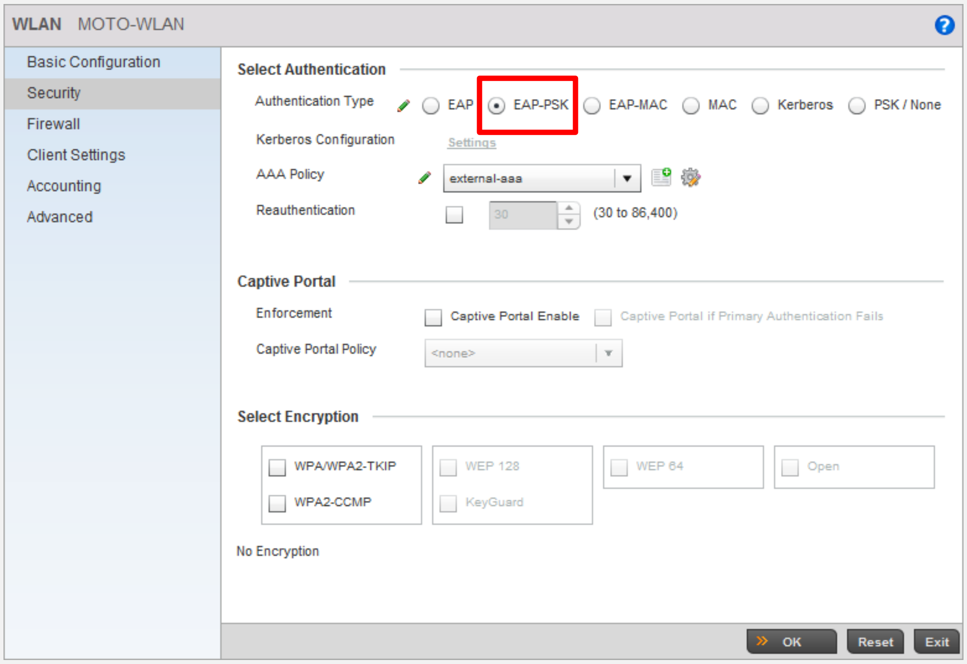
3.8.2 EAP-PSK:

The EAP-PSK authentication type can be enabled to authenticate wireless users and/or computers using 802.1X or wireless users using pre-shared-keys. This authentication type is useful for deployments that are migrating from pre-shared-keys to 802.1X and do not wish to deploy a second Wireless LAN.

To support EAP authentication the Wireless LAN must be assigned a AAA Policy and the RADIUS servers and wireless client must support EAP authentication and the same EAP authentication methods.

Example:

```
authentication-type eap-psk
```



WLAN MOTO-WLAN

Select Authentication

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

Kerberos Configuration Settings

AAA Policy external-aaa

Reauthentication □ 30 (30 to 86,400)

Captive Portal

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

Captive Portal Policy <none>

Select Encryption

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

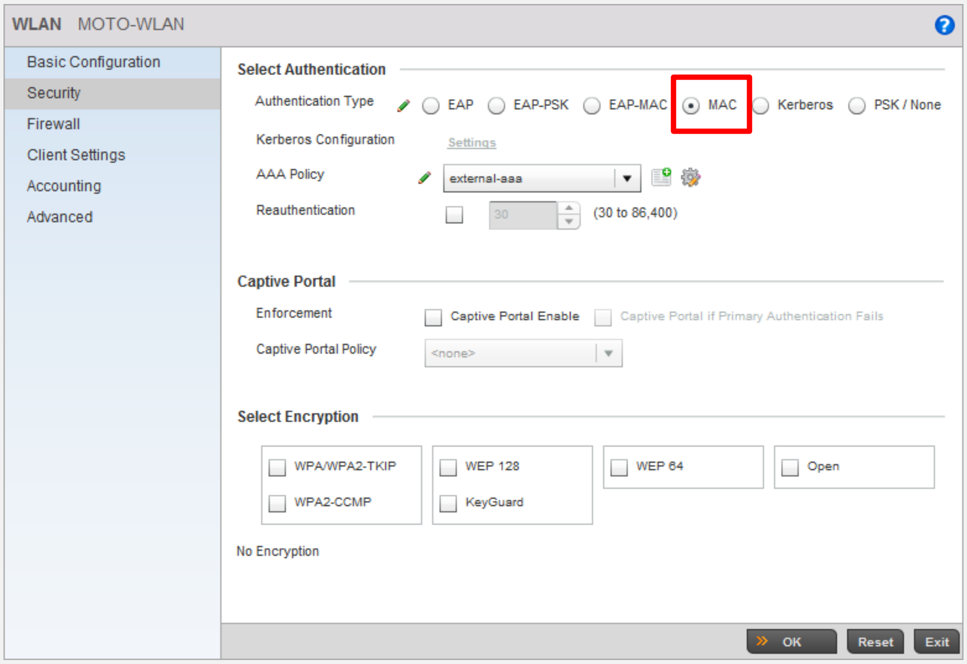
No Encryption

3.8.3 MAC:

The MAC authentication type can be enabled to authenticate wireless users using pre-shared-keys and computers using the host MAC address. The MAC authentication type is useful for assigning authorisation attributes from RADIUS AAA servers for pre-shared-key deployments which do not credentials. To support MAC authentication the Wireless LAN must be assigned a AAA Policy.

Example:

```
authentication-type mac
```



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

Kerberos Configuration Settings

AAA Policy external-aaa

Reauthentication □ 30 (30 to 86,400)

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

Captive Portal Policy <none>

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

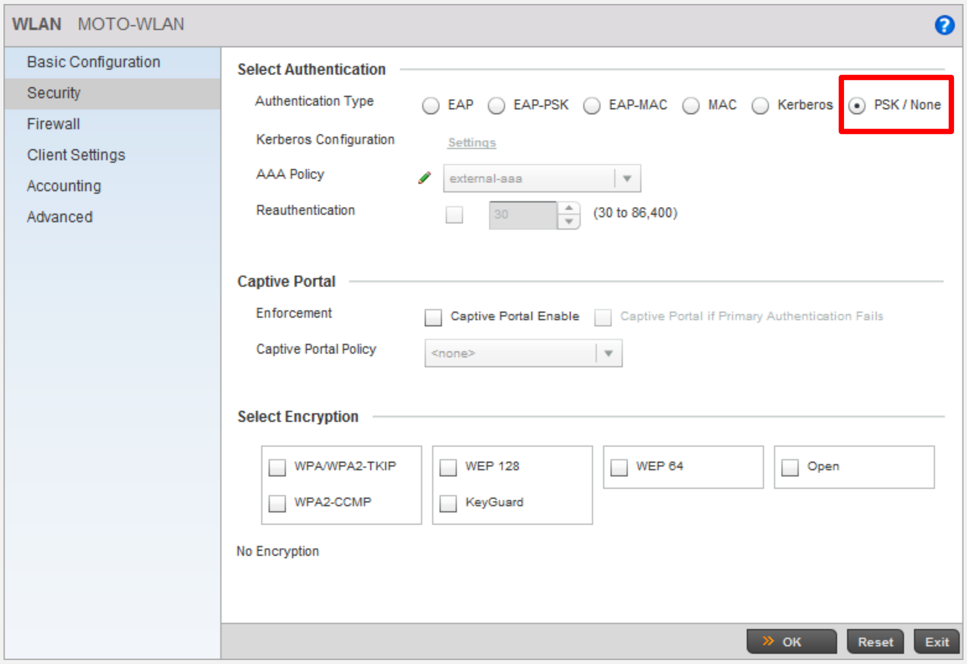
No Encryption

3.8.4 PSK/None:

The PSK/None authentication type can be enabled to authenticate wireless users using an ASCII or hex pre-shared-key. As a common pre-share-key is used to authenticate all wireless users on the Wireless LAN, no AAA policy is required.

Example:

```
authentication-type none
```



Select Authentication

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

Kerberos Configuration Settings

AAA Policy external-aaa

Reauthentication □ 30 (30 to 86,400)

Captive Portal

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

Captive Portal Policy <none>

Select Encryption

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

□ WPA2-CCMP □ KeyGuard

No Encryption

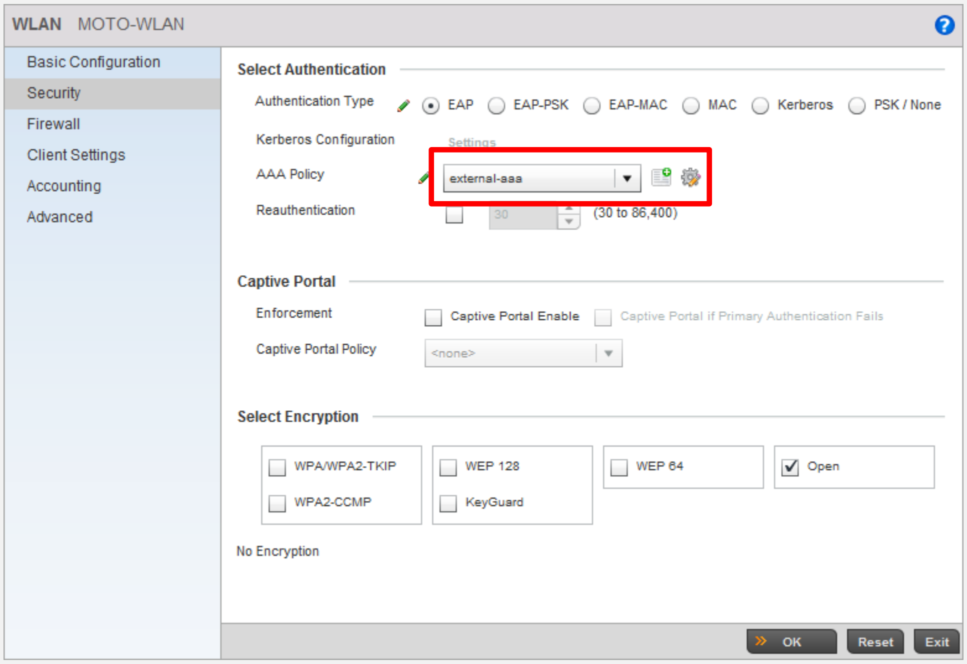
3.9 AAA Policy:

A AAA policy is required for any Wireless LAN using the EAP, EAP-PSK or MAC authentication type and defines where the Access Points forward AAA requests and how the AAA requests are proxied. Each AAA policy can contain up to 6 RADIUS authentication and accounting server entries which can be load-balanced or fail-over. Authentication requests can be forwarded to an integrated RADIUS server built into the Wireless Controller or Access Point as well as external RADIUS servers.

Each server entry can be configured to proxy authentication requests through a specific device on the network. Authentication requests can be forwarded directly from the Access Points to the RADIUS AAA servers or can be proxied through an Access Point at a site operating as a RF Domain manager. Authentication requests may also be proxied through a centralised Wireless Controller.

Example:

```
use aaa-policy external-aaa
```



WLAN MOTO-WLAN

Select Authentication

Authentication Type: ● EAP ○ EAP-PSK ○ EAP-MAC ○ MAC ○ Kerberos ○ PSK / None

Kerberos Configuration: Settings

AAA Policy: external-aaa

Reauthentication: □ 30 (30 to 86,400)

Captive Portal

Enforcement: □ Captive Portal Enable □ Captive Portal if Primary Authentication Fails

Captive Portal Policy: <none>

Select Encryption

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

□ WPA2-CCMP □ KeyGuard

No Encryption

3.10 Encryption Types:

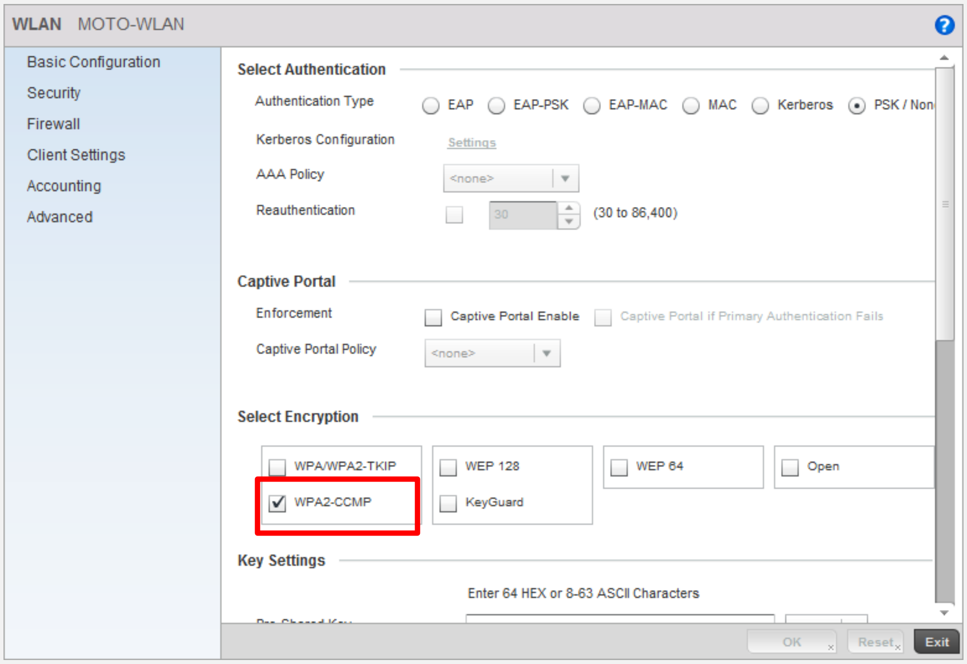
Each Wireless LAN can support encryption that determines how the wireless user's data is protected when forwarded over the air. The 802.11i standard mandates support for CCMP encryption but may optionally support TKIP encryption for legacy clients.

3.10.1 CCMP:

The CCMP encryption type uses the Advanced Encryption Standard (AES) algorithm that currently provides the most secure data forwarding option available for Wireless LANs. The CCMP encryption type is recommended for all new Wireless LAN deployments and support is available on all new wireless client devices.

Example:

```
encryption-type ccmp
```



WLAN MOTO-WLAN

Select Authentication

Authentication Type ○ EAP ○ EAP-PSK ○ EAP-MAC ○ MAC ○ Kerberos ● PSK / Non

Kerberos Configuration Settings

AAA Policy <none>

Reauthentication □ 30 (30 to 86,400)

Captive Portal

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

Captive Portal Policy <none>

Select Encryption

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

☑ WPA2-CCMP □ KeyGuard

Key Settings

Enter 64 HEX or 8-63 ASCII Characters

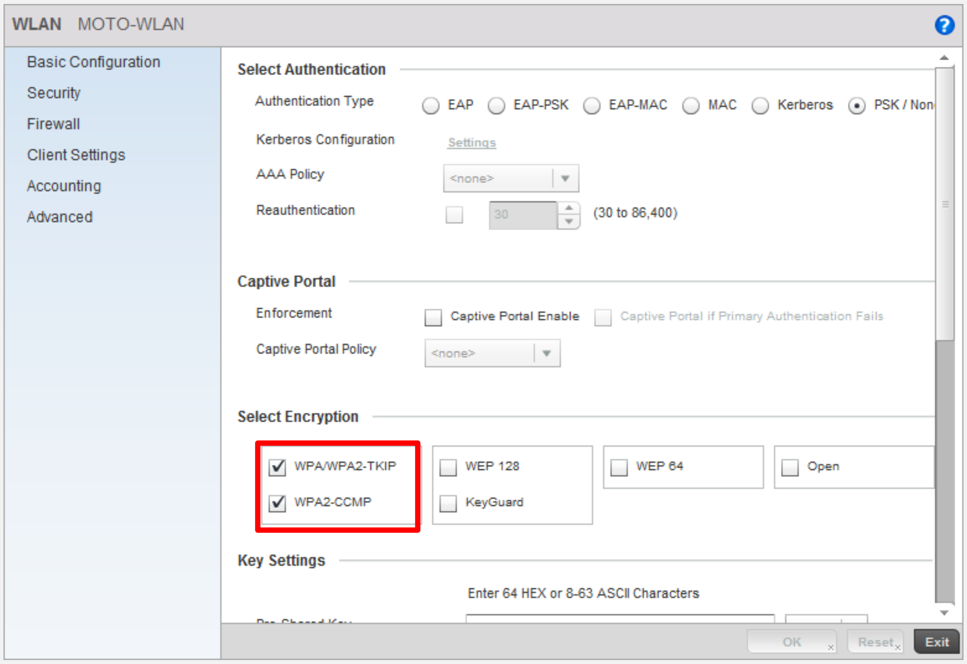
3.10.2 TKIP-CCMP:

The TKIP-CCMP encryption type provides simultaneous support for wireless clients using AES as well as legacy clients supporting Temporal Key Integrity Protocol (TKIP). The TKIP-CCMP encryption type is useful for Wireless LAN deployments that are migrating from TKIP to AES without having to deploy a second Wireless LAN.

Whenever possible it is recommended that the CCMP encryption type be deployed. While TKIP offers better security than WEP, TKIP it is known to have several vulnerabilities.

Example:

```
encryption-type tkip-ccmp
```



Select Authentication

Authentication Type ○ EAP ○ EAP-PSK ○ EAP-MAC ○ MAC ○ Kerberos ● PSK / Non

Kerberos Configuration Settings

AAA Policy <none>

Reauthentication □ 30 (30 to 86,400)

Captive Portal

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

Captive Portal Policy <none>

Select Encryption

☑ WPA/WPA2-TKIP
☑ WPA2-CCMP
□ WEP 128
□ KeyGuard
□ WEP 64
□ Open

Key Settings

Enter 64 HEX or 8-63 ASCII Characters

3.11 Key Settings:

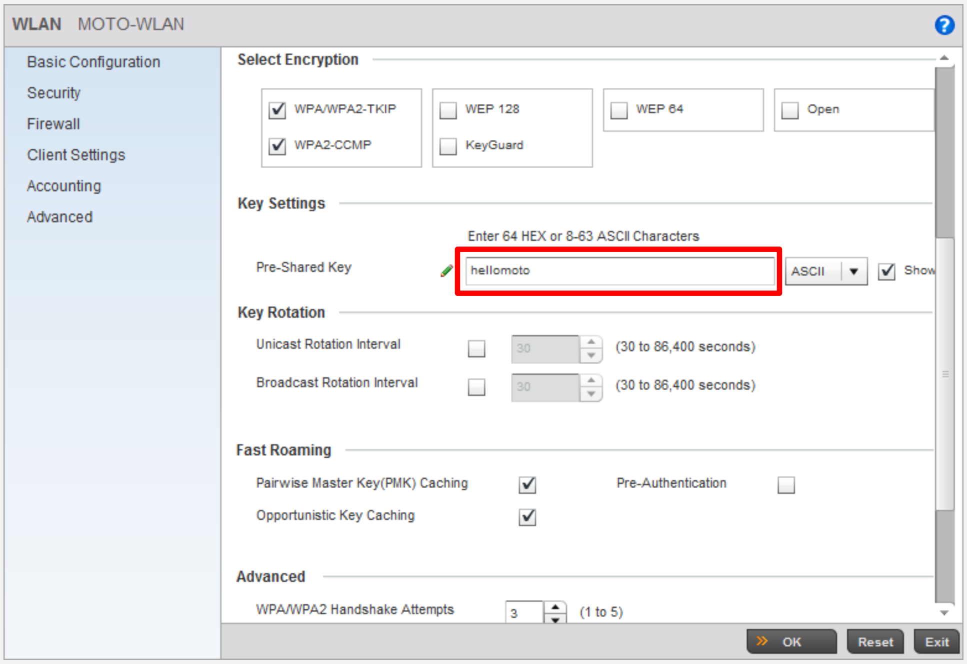
When EAP-PSK, MAC or PSK/None authentication types are enabled in a Wireless LAN a pre-shared-key also needs to be defined. The pre-shared-key can be entered as an 8 – 63 character ASCII passphrase or a 64 character HEX string. If an ASCII passphrase is used, the 256-bit key is calculated by applying a password-based key derivation function to the passphrase using the SSID.

Wireless clients wishing to associate to the Wireless LAN have to enter the correct passphrase or HEX key before being permitted access to the Wireless LAN.

Pre-shared-keys are vulnerable to dictionary password cracking attacks if a weak passphrases are used. To protect against brute force attacks a random passphrase of 13 or more characters should be used.

Example:

encryption-type tkip-ccmp



Select Encryption

☑ WPA/WPA2-TKIP
☑ WPA2-CCMP
□ WEP 128
□ KeyGuard
□ WEP 64
□ Open

Key Settings

Enter 64 HEX or 8-63 ASCII Characters

Pre-Shared Key: hellomoto ASCII ☑ Show

Key Rotation

Unicast Rotation Interval □ 30 (30 to 86,400 seconds)

Broadcast Rotation Interval □ 30 (30 to 86,400 seconds)

Fast Roaming

Pairwise Master Key(PMK) Caching ☑ Pre-Authentication □

Opportunistic Key Caching ☑

Advanced

WPA/WPA2 Handshake Attempts 3 (1 to 5)

4. Assignments:

Wireless LANs can be assigned to groups of Access Point radios using profiles or to individual Access Point radios using overrides. Wireless LANs can be assigned to AP650 and AP7131 Access Points as well as the RFS4000 Wireless Controller with an integrated Access Point.

Each radio supports 8 BSSIDs allowing up to 8 Wireless LANs to be serviced per radio with a unique BSSID MAC address. Each radio can support a maximum or 16 Wireless LANs, however when the maximum number of BSSIDs are reached Wireless LAN will share BSSIDs.

4.1 Profiles:

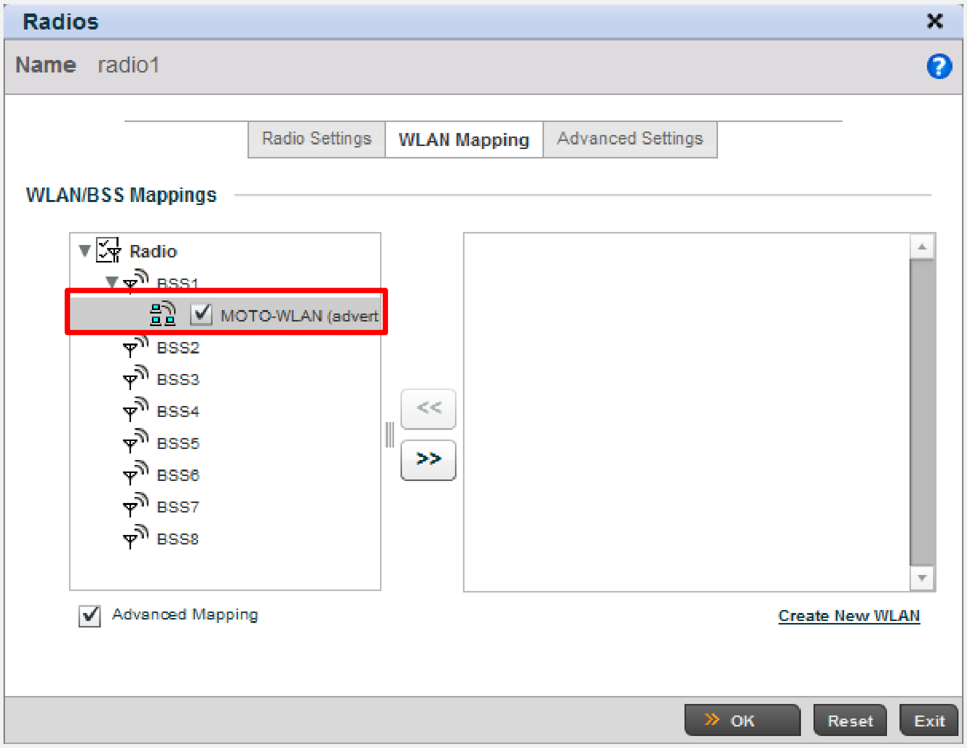
Wireless LANs can be assigned to profiles using the CLI by issuing the ***interface radio*** command followed by the radio number. This will access the radio configuration context allowing Wireless LANs to be added or removed from the radio. Wireless LAN configuration is applied to the profile when the ***commit*** command is invoked.

Assigning Wireless LANs to Profiles:

```
rfsX000(config)# profile (rfs4000 | ap650 | ap7131) <profile-name>
rfsX000(config-profile-<profile-name>)# interface radio <1 | 2>
rfsX000(config-profile-<profile-name-if-radio>)# wlan <wlan-name> bss <1-8>
```

Wireless LANs can be assigned to profiles in the WiNG 5.0 UI by clicking ***Configuration > Profiles***, highlighting the Profile then selecting ***Edit***. The Wireless LAN can be assigned to radios in the profile in the ***Interface > Radios > WLAN Mapping*** configuration window. Wireless LANs are assigned to the profile when a ***Commit*** is invoked.

Configuration > Profiles > Profile-Name > Interface > Radios > Radio-ID > WLAN Mapping


Radios

Name radio1

WLAN/BSS Mappings

☑ Advanced Mapping

4.2 Device Overrides:

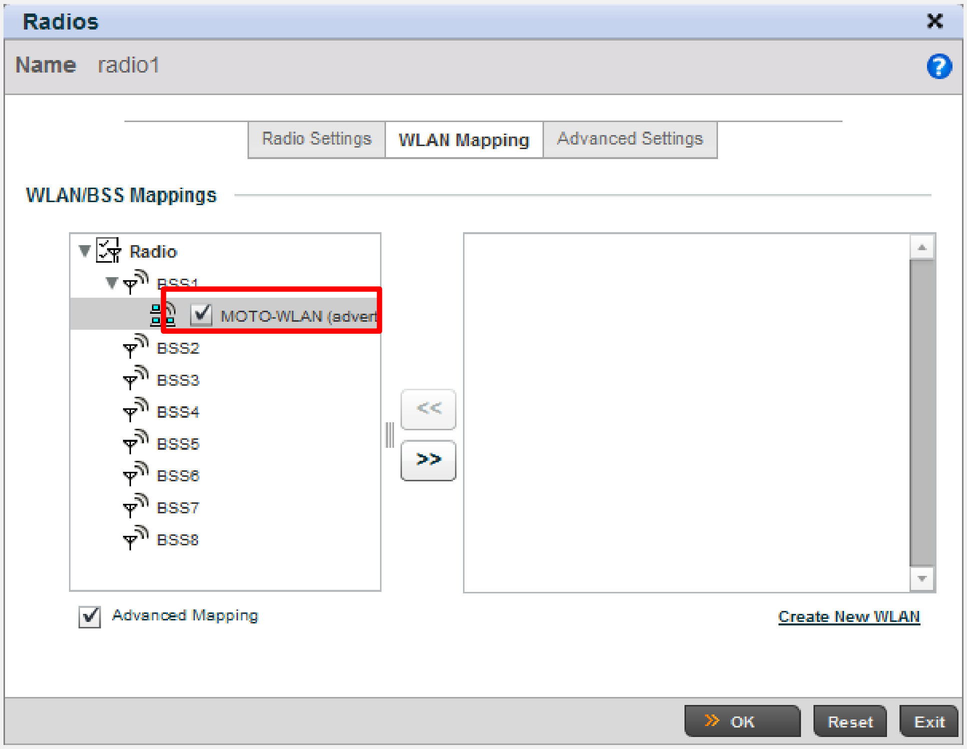
Wireless LANs can be assigned to devices as overrides using the CLI by issuing the ***interface radio*** command followed by the radio number. This will access the radio configuration context for the device allowing Wireless LANs to be added or removed from the radio. Wireless LAN configuration is applied to the device when the ***commit*** command is invoked.

Assigning Wireless LANs to Devices:

```
rfsX000(config)# (rfs4000 | ap650 | ap7131) <mac-address>
rfsX000(config-device-<mac-address>)# interface radio <1 | 2>
rfsX000(config-device-<mac-address-if-radio>)# wlan <wlan-name> bss <1-8>
```

Wireless LANs can be assigned to devices in the WiNG 5.0 UI by clicking ***Configuration > Devices***, highlighting the device then selecting ***Edit***. The Wireless LAN can be assigned to radios in the device in the ***Profile Overrides > Interface > Radios > WLAN Mapping*** configuration window. Wireless LANs are assigned to the device when a ***Commit*** is invoked.

Configuration > Profiles > Device-MAC > Profile Overrides > Interface > Radios > Radio-ID > WLAN Mapping


Radios

Name radio1

5. Example Use Cases:

5.1 802.11i PSK Wireless LAN:

In the following scenario a customer needs to deploy a Wireless LAN at their corporate facility that supports Polycom Voice handheld devices. As these devices do not support 802.1X authentication the customer has elected to implement CCMP encryption with pre-shared-key authentication.

The customer wants to assign the Polycom voice handsets to a voice VLAN 80 which is tunneled to the Wireless Controllers in the data-center where the SVP servers reside. The Polycom handsets use SVP for QoS requiring a user defined QoS policy to be assigned.

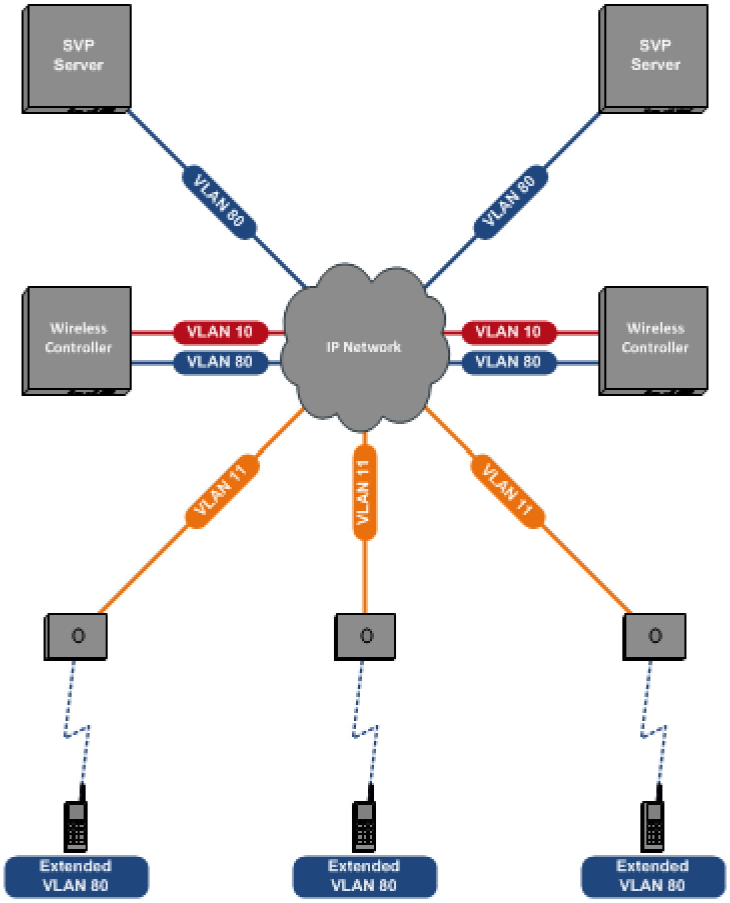


Figure 5.1 – Example Topology:

Bridging Policy:

```
!
bridging-policy default
 no access-point local-bridging
!
```

QoS Policy:

```
!
wlan-qos-policy SVP
 no wmm power-save
 svp-prioritization
 qos trust dscp
 qos trust wmm
!
```

Wireless LAN:

```
!
wlan WLAN-PSK
 wlan WLAN-PSK
 vlan 80
 encryption-type ccmp
 authentication-type none
 wpa-wpa2 psk motorolaisbest
 use wlan-qos-policy SVP
!
```

Device Profiles:

```
!
profile ap650 default-ap650
 interface radio1
  wlan WLAN-PSK bss 1 primary
 interface radio2
  wlan WLAN-PSK bss 1 primary
 interface ge1
  switchport mode access
  switchport access vlan 11
  qos trust dscp
  qos trust 802.1p
 interface vlan1
  shutdown
 interface vlan11
  description ap-vlan
  ip address dhcp
  ip dhcp client request options all
 ..
 use bridging-policy default
!
```

```
!
profile rfs4000 default-rfs4000
 ..
 ..
 interface up1
  switchport mode trunk
  switchport trunk native vlan 10
  switchport trunk native tagged
  switchport trunk allowed vlan 10,80
  qos trust dscp
  qos trust 802.1p
 ..
 use bridging-policy default
!
```

5.2 802.11i EAP-PSK Wireless LAN:

In the following scenario a customer needs to deploy a Wireless LAN that supports new devices that authenticate using EAP as well as legacy devices that support pre-shared-keys. The customer would like to deploy a single Wireless LAN that can support both devices until the migration to EAP is completed.

The customer wants to assign computers and users to VLAN 40 which is tunneled to the Wireless Controllers in the data-center. As all the Windows client devices support WMM the default QoS policy can be assigned.

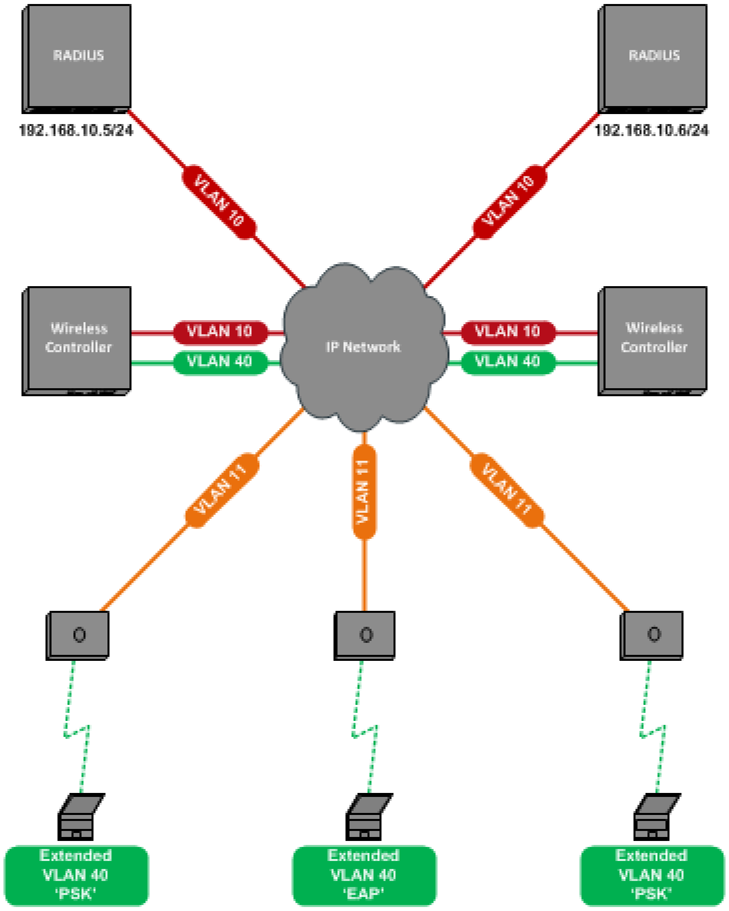


Figure 5.2 – Example Topology:

AAA Policy:

```
!
aaa-policy external-aaa
 authentication server 1 host 192.168.10.5 secret 0 hellomoto
 authentication server 1 proxy-mode through-controller
 authentication server 1 host 192.168.10.6 secret 0 hellomoto
 authentication server 1 proxy-mode through-controller
!
```

Bridging Policy:

```
!
bridging-policy default
 no access-point local-bridging
!
```

QoS Policy:

```
!
wlan-qos-policy default
 qos trust dscp
 qos trust wmm
!
```

Wireless LAN:

```
!
wlan WLAN-EAPPSK
 wlan WLAN-EAPPSK
 vlan 40
 encryption-type ccmp
 authentication-type eap-psk
 wpa-wpa2 psk motorolaisbest
 use aaa-policy external-aaa
 use wlan-qos-policy default
!
```

Device Profiles:

```
!
profile ap650 default-ap650
 interface radio1
  wlan WLAN-EAPPSK bss 1 primary
 interface radio2
  wlan WLAN-EAPPSK bss 1 primary
 interface ge1
  switchport mode access
  switchport access vlan 11
  qos trust dscp
  qos trust 802.1p
 interface vlan1
  shutdown
 interface vlan11
  description ap-vlan
  ip address dhcp
  ip dhcp client request options all
 ..
 use bridging-policy default
!
```

```
!
profile rfs4000 default-rfs4000
 ..
 ..
 interface up1
  switchport mode trunk
  switchport trunk native vlan 10
  switchport trunk native tagged
  switchport trunk allowed vlan 10,40
  qos trust dscp
  qos trust 802.1p
 ..
 use bridging-policy default
!
```

5.3 802.11i EAP Wireless LAN:

In the following scenario a customer needs to deploy a Wireless LAN that can authenticate users and computers using EAP authentication with end-point inspection. The computers and users will authenticate using PEAP-MSCHAPv2 against Microsoft Network Access Protection (NAP) servers and will be dynamically assigned a VLAN based on compliance state.

Compliant users will be assigned to VLAN 40 which is bridged locally by the Access Point while non-compliant users will be assigned to VLAN 50 which is tunneled to the Wireless Controller in the data-center where remediation servers reside.

As all the Windows client devices support WMM the default QoS policy can be assigned.

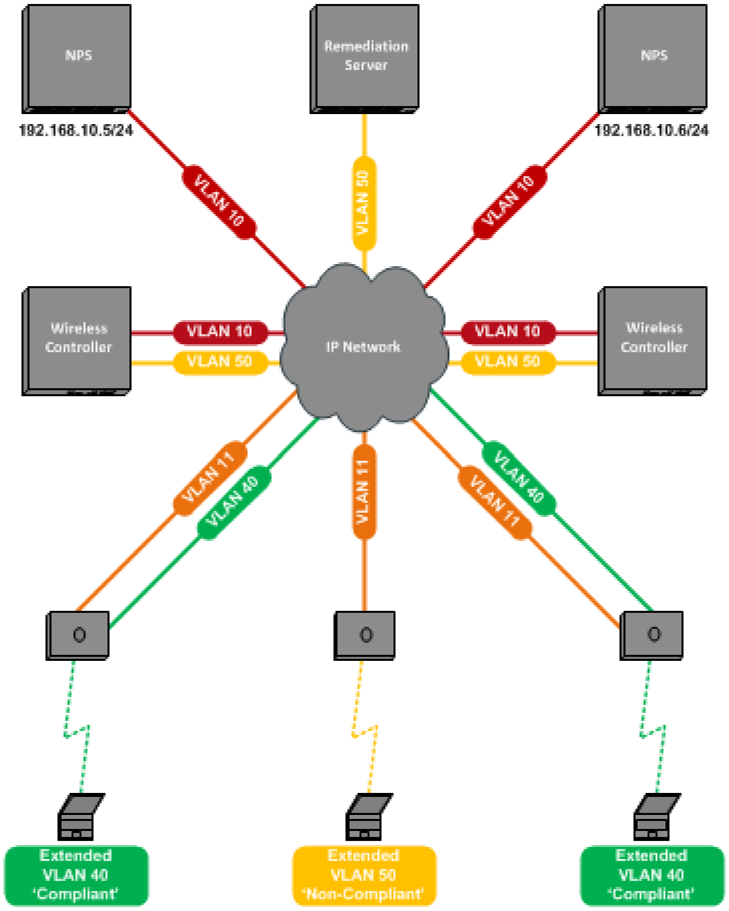


Figure 5.3 – Example Topology:

AAA Policy:

```
!
aaa-policy microsoft-nps
 authentication server 1 host 192.168.10.5 secret 0 hellomoto
 authentication server 1 proxy-mode through-controller
 authentication server 1 host 192.168.10.6 secret 0 hellomoto
 authentication server 1 proxy-mode through-controller
!
```

Bridging Policy:

```
!
bridging-policy default
 extended-vlan 40
 access-point local-bridging
!
```

QoS Policy:

```
!
wlan-qos-policy default
 qos trust dscp
 qos trust wmm
!
```

Wireless LAN:

```
!
wlan WLAN-NAP
 wlan WLAN-NAP
 vlan 50
 encryption-type ccmp
 authentication-type eap
 radius vlan-assignment
 use aaa-policy microsoft-nps
 use wlan-qos-policy default
!
```

Device Profiles:

```
!
profile ap650 default-ap650
 interface radio1
  wlan WLAN-NAP bss 1 primary
 interface radio2
  wlan WLAN-NAP bss 1 primary
 interface ge1
  switchport mode trunk
  switchport trunk native vlan 11
  no switchport trunk native tagged
  switchport trunk allowed vlan 11,40,50
  qos trust dscp
  qos trust 802.1p
 interface vlan1
  shutdown
 interface vlan11
  description ap-vlan
  ip address dhcp
  ip dhcp client request options all
 ..
 use bridging-policy default
!
```

```
!
profile rfs4000 default-rfs4000
 ..
 ..
 interface up1
  switchport mode trunk
  switchport trunk native vlan 10
  switchport trunk native tagged
  switchport trunk allowed vlan 10,50
  qos trust dscp
  qos trust 802.1p
 ..
 use bridging-policy default
!
```