WiNG 5.X How-To Guide

Active Directory Authentication

Part No. TME-12-2011-01 Rev. B

Table of Contents

1. Introduction

The Lightweight Directory Access Protocol, or LDAP, is an application protocol for querying and modifying directory services running over TCP/IP. A directory is a set of objects with attributes organized in a logical and hierarchical manner. A simple example is the telephone directory, which consists of a list of names organized alphabetically, with each name having an address and phone number associated with it.

An LDAP directory tree often reflects various geographic and organizational boundaries depending on the deployment model chosen. LDAP deployments today tend to use Domain name system (DNS) names for structuring the topmost levels of the hierarchy. Deeper inside the directory might appear entries representing people, organizational units, printers, documents, groups of people or anything else that represents a given tree entry.

LDAP authentication allows the Motorola Wireless Controllers and Independent Access Points to authenticate and authorize users against a number of LDAP compliant user directories including Microsoft's Active Directory, Novell's eDirectory, OpenLDAP and Sun's Directory Server.

This guide provides a step-by-step example of how to configure Motorola Wireless Controllers or Independent Access Points running WiNG 5.X to authenticate EAP Wireless LAN users against a Microsoft Active Directory user directory.

1.1 Microsoft Active Directory

Microsoft Active Directory is the distributed directory service that is included with Microsoft Windows Server 2000, Microsoft Windows Server 2003 and Microsoft Windows 2008 operating systems. Active Directory enables centralized secure management of an entire network which might span a building, a city, or multiple locations throughout the world.

- Active Directory is an LDAP like technology created by Microsoft that provides a variety of network services including:
- LDAP-like directory services and scaling
- Kerberos-based authentication
- DNS-based naming and other network information
- Central location for network administration and delegation of authority
- Information security and single sign-on for user access to networked based resources
- Central storage location for application data
- Synchronization of directory updates amongst several servers

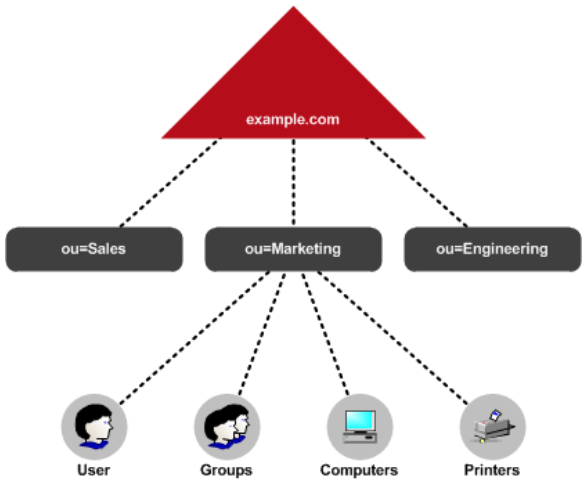


Figure 1.1 – Microsoft Active Directory Tree

In Windows environments Active Directory also allows administrators to assign policies, deploy software, and apply critical updates to an organization. Active Directory networks can vary from a small installation with a few computers, users and printers to tens of thousands of users, many different domains and large server farms spanning many geographical locations.

1.2 LDAP Authentication

LDAP authentication is supported by all Motorola Wireless Controllers and Independent Access Points running WiNG 5.X software and maybe used to authenticate and authorize Wireless Clients associated to EAP and Captive Portal Wireless LANs. LDAP by itself does not provide support 802.1X and must have a RADIUS server to terminate the EAP requests. This functionality is provided by an integrated RADIUS service built into Motorola Wireless Controllers and Independent Access Points.

LDAP authentication is a global option on the integrated RADIUS service and once enabled the Wireless Controller or Independent Access Point will authenticate user credentials against a defined primary or secondary LDAP server and optionally authorize users using local groups. Once LDAP authentication is enabled, the integrated RADIUS service is no-longer able to authenticate users against its local user database.

In addition to user authentication, the integrated RADIUS service can optionally perform authorization. After an LDAP user has been successfully authenticated the integrated RADIUS service may optionally query the LDAP user directory for authenticating user's group membership. The LDAP directory will return all the LDAP groups the user is a member of and will compare the returned LDAP groups to a defined local group to determine if the user is authorized to access the Wireless LAN and assign authorization attributes such as Time of Day, Day of Week, roles or bandwidth.

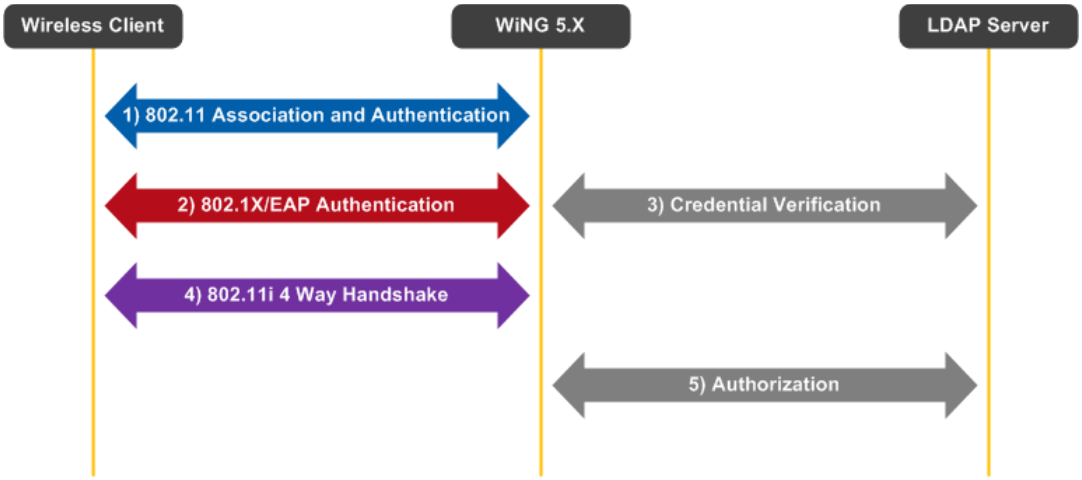


Figure 1.2 – LDAP Authentication

One main advantage of LDAP authentication with EAP authentication is that the integrated RADIUS service processes the 4-way handshake. In a large scale Wireless LAN deployment a centralized RADIUS server can potentially become overloaded as it is processing all the EAP requests for the organization. Each EAP authentication request requires a secure TLS session between the RADIUS server and client which can cause performance issues resulting in slow authentication times.

Processing the EAP requests locally on the Motorola Wireless Controllers or Independent Access Points provides a scalable distributed RADIUS environment that can support more authentication requests than a centralized RADIUS model. In addition this model allows RADIUS services to be provided at remote sites without requiring separate RADIUS servers reducing management and operational expenses and providing availability.

1.3 EAP Method Support

Each EAP method supports one or more inner authentication protocols. The LDAP protocol natively supports PAP, CHAP and MS-CHAP authentication protocols which limit the EAP methods that can be supported when using LDAP to only EAP methods that support these inner authentication protocols. As a result, when LDAP authentication is enabled on a Motorola Wireless Controller or Independent Access Point EAP method support is restricted to EAP-TTLS with PAP and EAP-GTC.

The following table outlines the supported EAP methods on a Motorola Wireless Controller or Independent Access Point running WiNG 5.X software when using external LDAP user authentication:

EAP Method	Local RADIUS	External RADIUS	External LDAP
Cisco LEAP	No	Yes	No
EAP-FAST	No	Yes	No
EAP-TLS	Yes	Yes	Yes
EAP-TTLS (MD5)	Yes	Yes	No
EAP-TTLS (PAP)	Yes	Yes	Yes
EAP-TTLS (MSCHAPv2)	Yes	Yes	No
PEAPv0 (MSCHAPv2)	Yes	Yes	No
PEAPv1 (GTC)	Yes	Yes	Yes
EAP-FAST	No	Yes	No
EAP-TLS	Yes	Yes	Yes
EAP-TTLS (MD5)	Yes	Yes	No
EAP-TTLS (PAP)	Yes	Yes	Yes

Table 1.3 – EAP Method Support

Note: EAP-TTLS authentication uses PAP as an inner authentication protocol. As such this requires the Active Directory users passwords to be stored using reversible encryption format.

1.4 Known Limitations

The following is a list of known LDAP limitations with the current 5.2.0.0-069R release:

1. The current release does not support spaces in Common Names or Organizational Units. Support for spaces in Common Names and Organizational Units is planned for the WiNG 5.3 release.
2. The current release does not provide support for spaces in Group Names. Support for spaces in Group Names is planned for the WiNG 5.4 release.
3. The current release does not provide support for NTLM which is required for MSCHAPv2 authentication. NTLM support is planned for the WiNG 5.5 release.

2. Pre-Requisites

2.1 Requirements

The following requirements must be met prior to attempting this configuration:

- One or two RFS4000, RFS6000 or RFS6000 Wireless Controllers are installed and operational on the network with one or more adopted Access Points.
- One Windows Server 2003 or Windows Server 2008 is installed and operational on the network functioning as an Active Directory Domain Controller.
- One or more Active Directory Groups and Users are defined in Active Directory.
- One workstation is available with Microsoft Internet Explorer or Mozilla Firefox to perform Web UI or CLI configuration.
- The reader has read the Motorola Solutions WiNG 5 System Reference Guide.

2.2 Components Used

The configuration example in this document is based on the following hardware and software versions:

- 1 x Windows 2008 Server Enterprise Edition
- 1 x RFS4000 Version 5.2.0.0-069R
- 1 x AP-6532 Independent Access Points

Note: Registered users may download the latest WiNG firmware from the Motorola Solutions Technical Support Site by visiting http://support.symbol.com.

3. Configuration

The following section outlines the configuration steps required to configure a Motorola Wireless LAN Controller to authenticate users against a Microsoft Active Directory:

1. Active Directory Bind User [Section 3.1]
2. AAA Policy [Section 3.2]
3. Wireless LAN [Section 3.3]
4. RADIUS Groups [Section 3.4]
5. RADIUS Server Policy [Section 3.5]
6. Trustpoints [Section 3.6]
7. RADIUS Server Policy Assignment [Section 3.7]
8. Wireless LAN Assignment [Section 3.8]

Figure 3.0 provides a detailed topology of the hardware and software components highlighted in section 2.2 used to create this guide:

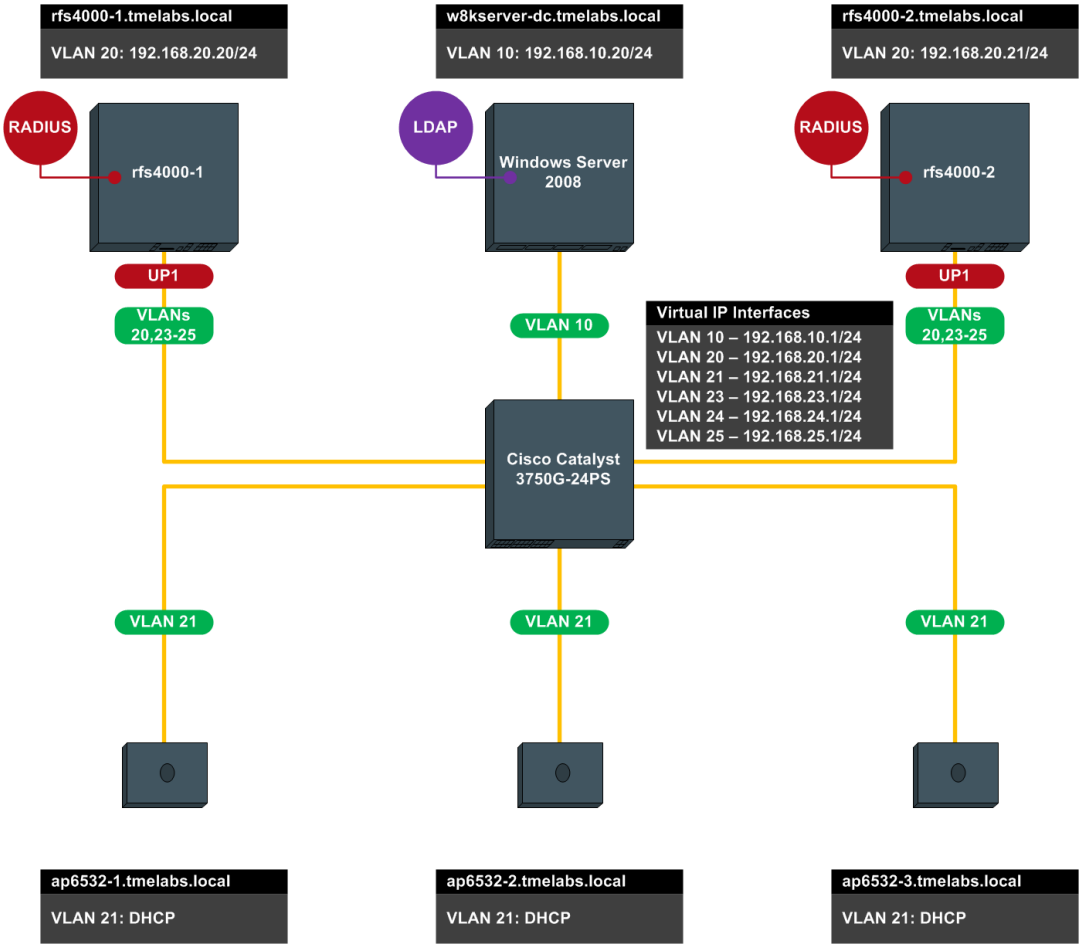


Figure 3.0 – Topology

3.1 Active Directory

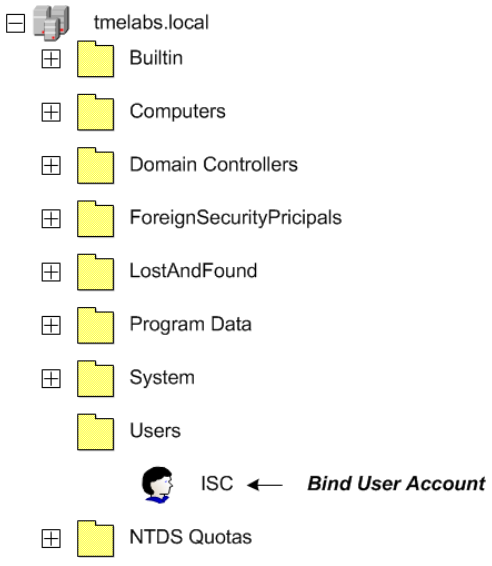
Before the RADIUS service on a Wireless Controller or Independent Access Point can authenticate users against Active Directory, an Active Directory bind user account must be created. The bind user account is used by the integrated RADIUS service to establish communications with an Active Directory user store to authenticate users and optionally determine Active Directory group membership.

The Active Directory bind user account can be created in the default ***Users*** container or a user defined ***Organizational Unit*** (limitations provided in section 1.4). Only one bind user account is required as it can be shared by multiple Motorola Wireless Controllers or Access Points. No special Active Directory permissions are required but it is strongly recommended that the defined password be fixed to eliminate potential downtime during password resets.

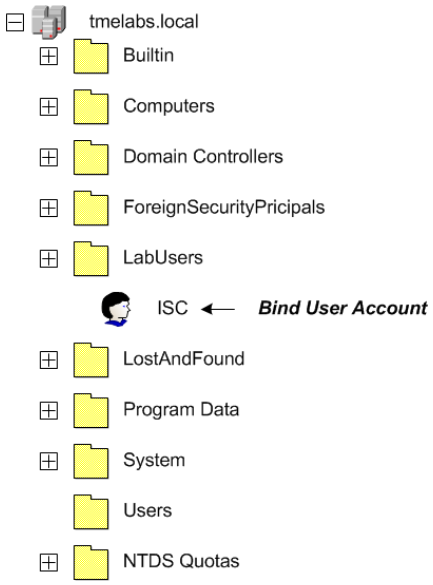
It is recommended that the bind user account be created using the following parameters:

1) The account name must ***NOT*** include any spaces.
2) The password ***MUST*** be stored using ***Reversible Encryption***.
3) The password should be fixed and exempt from password policies that require frequent password changes.
4) Must be a member of the ***Domain Users*** group.

For this configuration step a bind user account named ***ISC*** will be defined in the default ***Users*** container. The bind user account will be required for the LDAP configuration on the integrated RADIUS serviced in a later step:



cn=ISC,cn=users,ou=tmelabs,ou=local



cn=ISC,ou=LabUsers,ou=tmelabs,ou=local

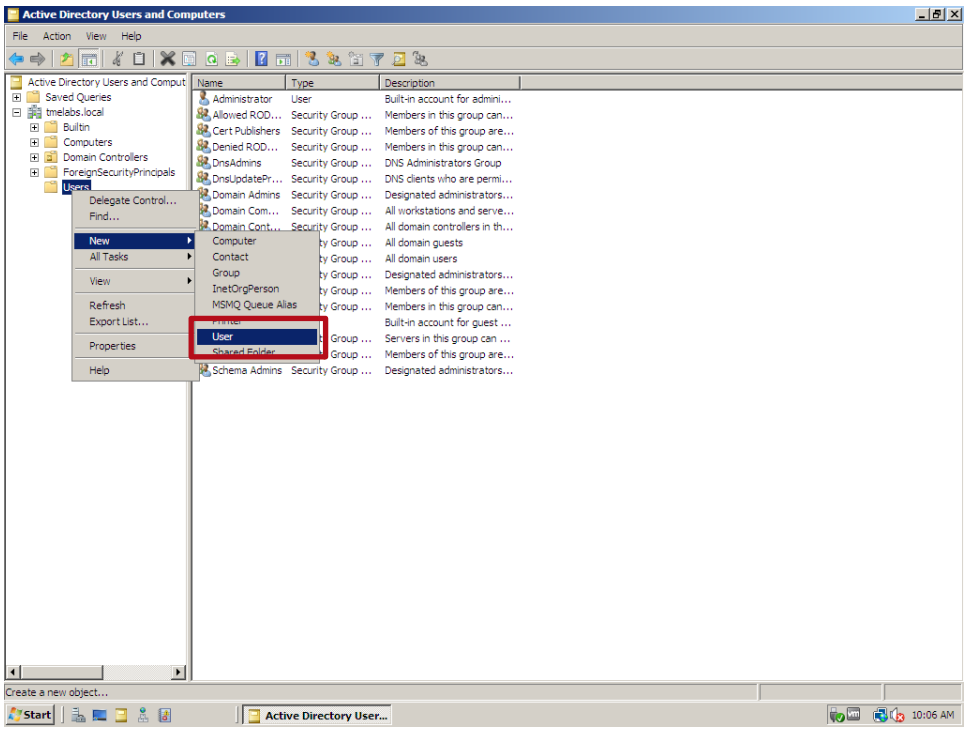
Figure 2.1 – Bind User Account Examples

Note: In Active Directory the default Users container is a Common Name (CN) while a user defined container is considered an Organizational Unit (OU).

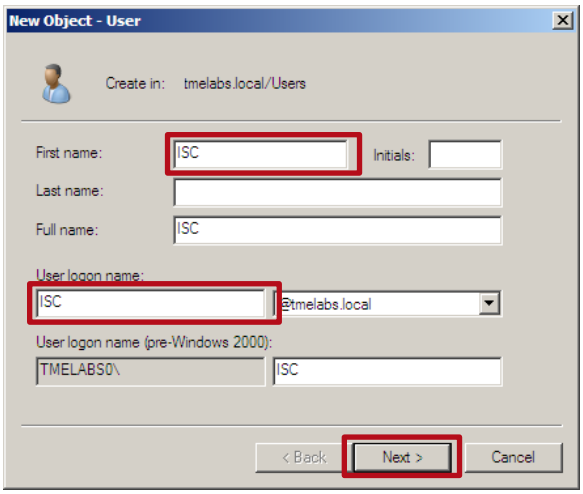
3.1.1 Active Directory Users and Computers

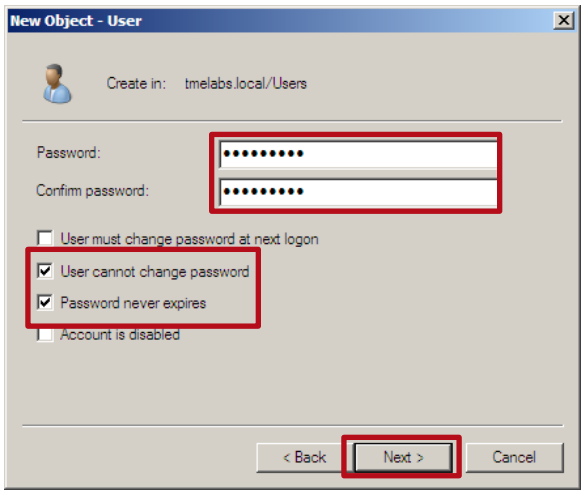
The following procedure highlights how to create a bind user account using the Active Directory Users and Computers snap-in on a Windows Server 2003 or Windows Server 2008 domain controller:

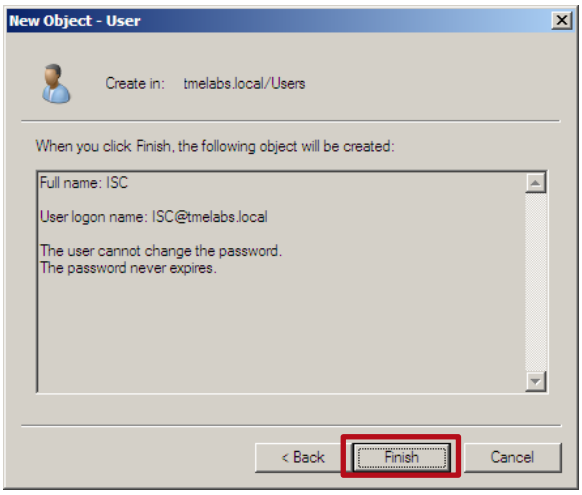
1 Open the *Active Directory Users and Computers* snap-in. Select the default *Users* container then right-click and select *New* → *User*:



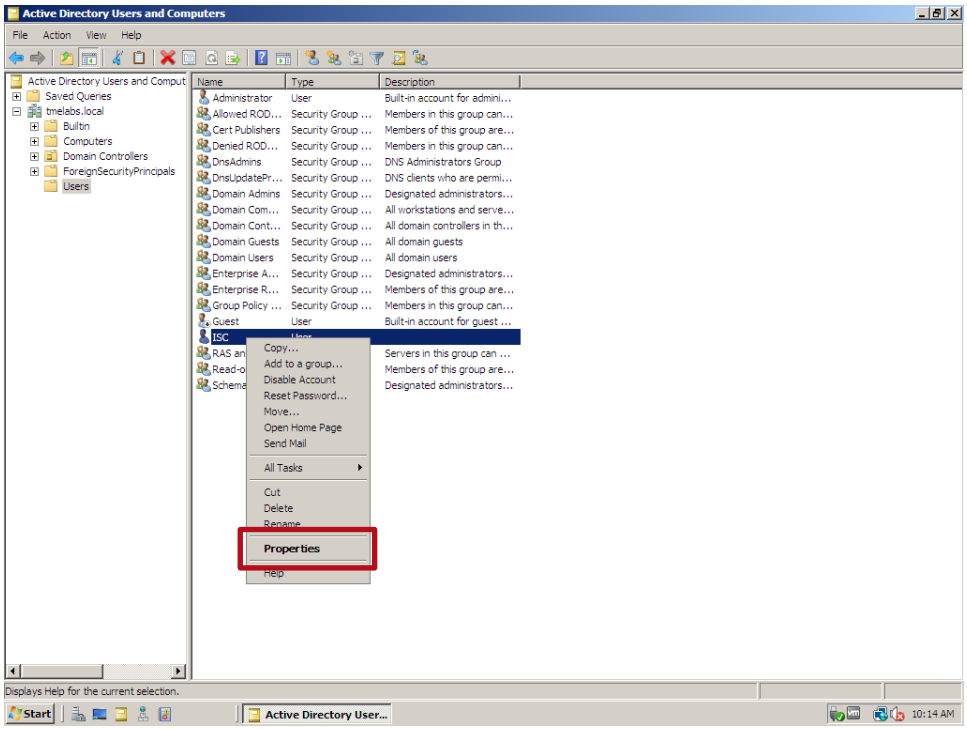
2 In the *First Name* and *User Logon Name* fields enter *ISC* then click *Next*. Enter and confirm the *Password* then uncheck the option *User must change password at next logon*. Check the options *User cannot change password* and *Password never expires* then click *Next*. Verify the account information then click *Finish*:



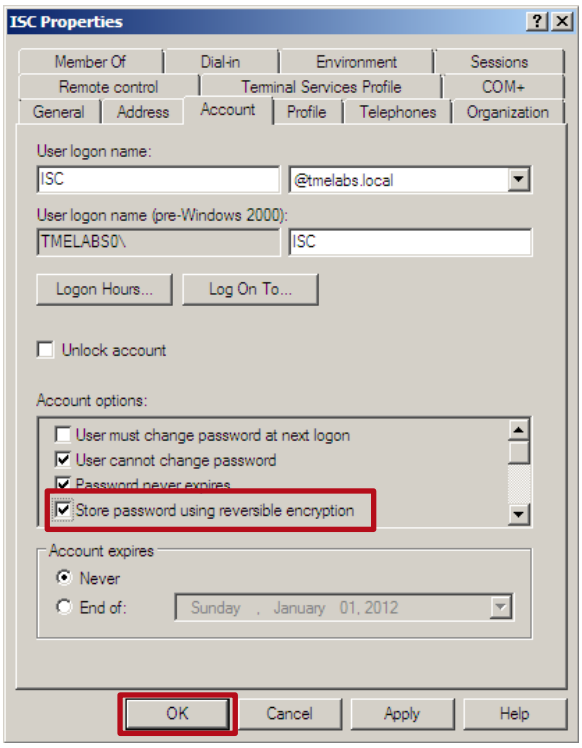




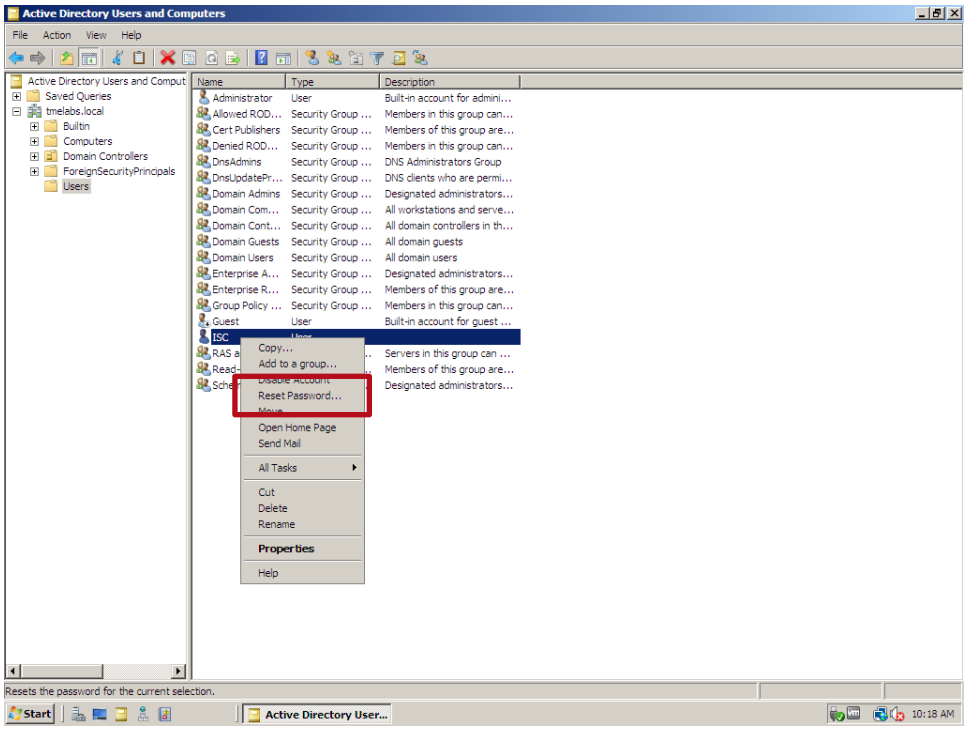
3 Select on the bind user account then right-click and select *Properties*:



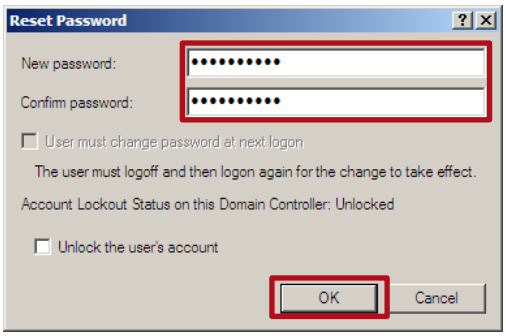
4 Select the *Account* tab then check the option *Store password using reversible encryption*. Click *OK*:



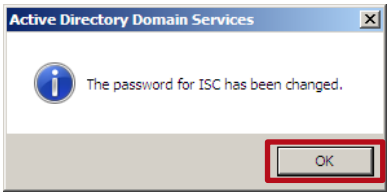
5 Click on the bind user account then right-click and select *Reset Password*:



7 Enter and confirm the password then click *OK*:



6 Click *OK*:



3.2 AAA Policy

802.11i EAP enabled Wireless LANs require a AAA Policy to determine where the RADIUS authentication server resides. For Active Directory Authentication the RADIUS Server can reside locally on each individual Independent Access Point (***onboard-self***) or centrally on the Wireless Controller (***onboard-controller***). EAP Authentication requests are forwarded to the RADIUS service on the Access Points or Wireless Controllers which terminates the TLS session and provides authentication and authorization.

For this configuration step a AAA Policy named ***internal-aaa*** will be defined using the ***onboard-controller*** server type which will point to the integrated RADIUS services on the Wireless Controllers managing the Access Points.

3.2.1 Command Line Interface

The following procedure highlights how to create an AAA Policy and RADIUS Server entry using the Command Line Interface (CLI):

1 Using the CLI create a new AAA Policy named *internal-aaa* and add an authentication server entry with the type *onboard controller*:

```
rfs4000-1(config)# aaa-policy internal-aaa
rfs4000-1(config-aaa-policy-internal-aaa)# authentication server 1 onboard controller
rfs4000-1(config-aaa-policy-internal-aaa)#exit
```

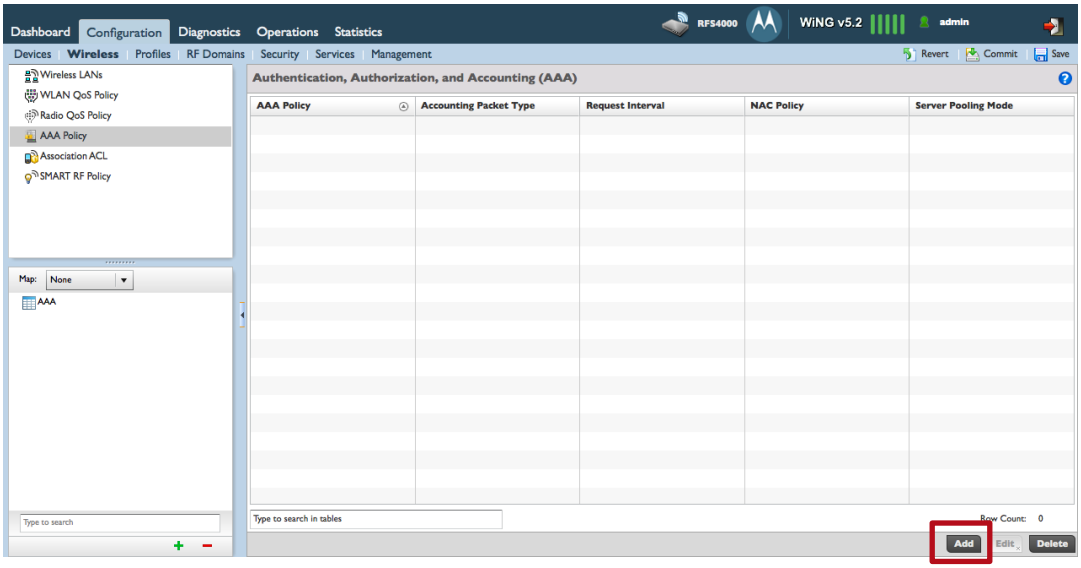
2 *Commit* and *Save* the changes:

```
rfs4000-1(config)# commit write
```

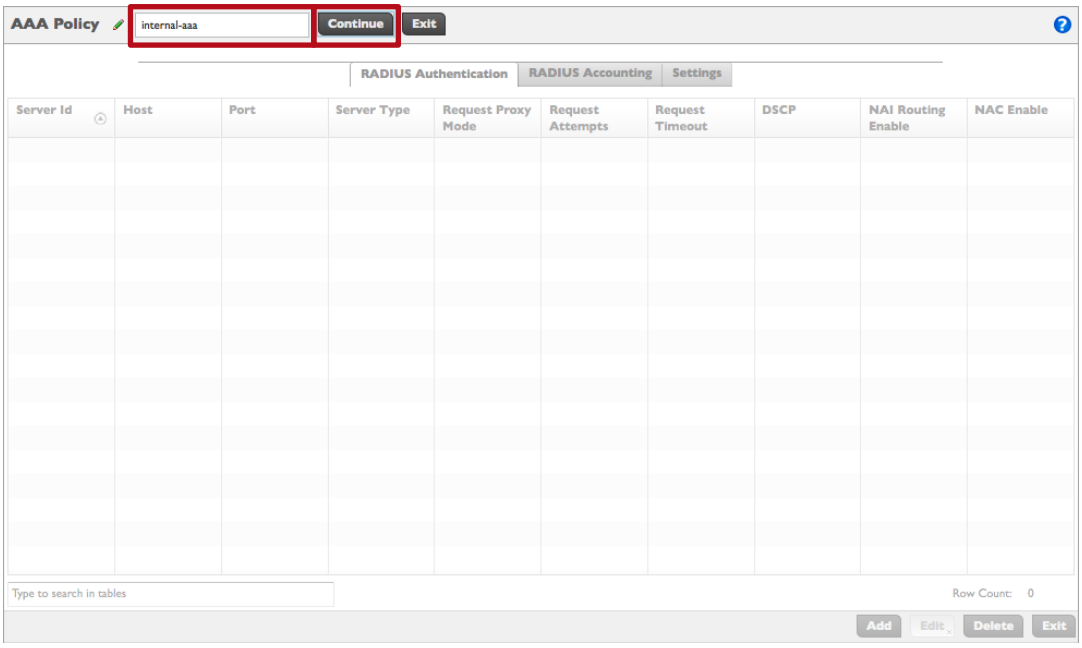
3.2.2 Web User Interface

The following procedure highlights how to create an AAA Policy and RADIUS Server entry using the Web User Interface (Web UI):

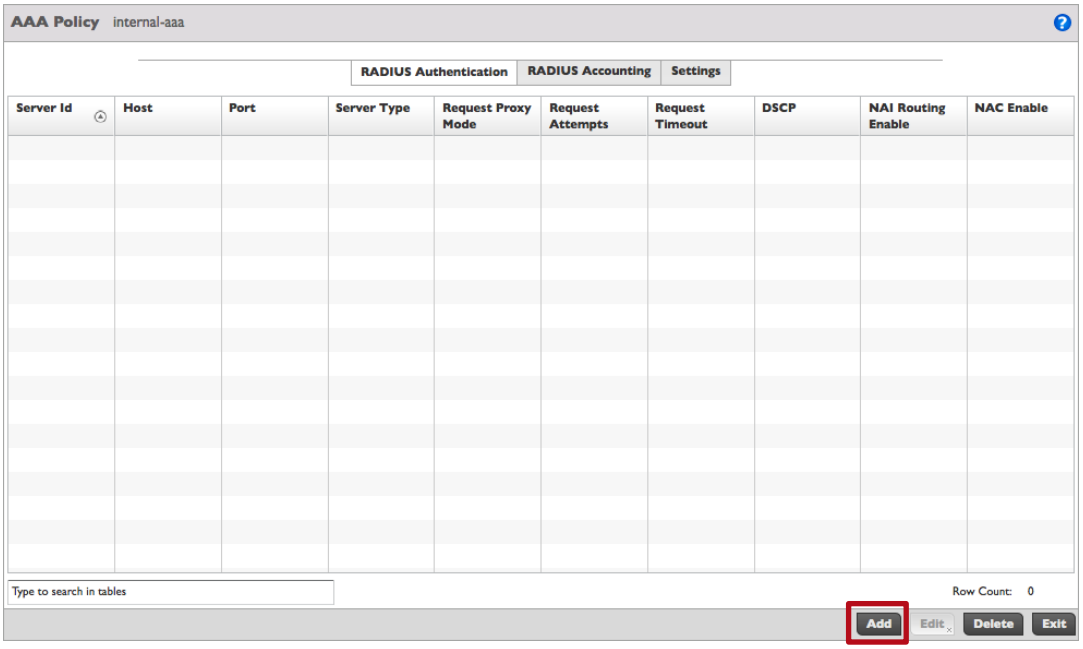
1 Select *Configuration* → *Wireless* → *AAA Policy* → *Add*:



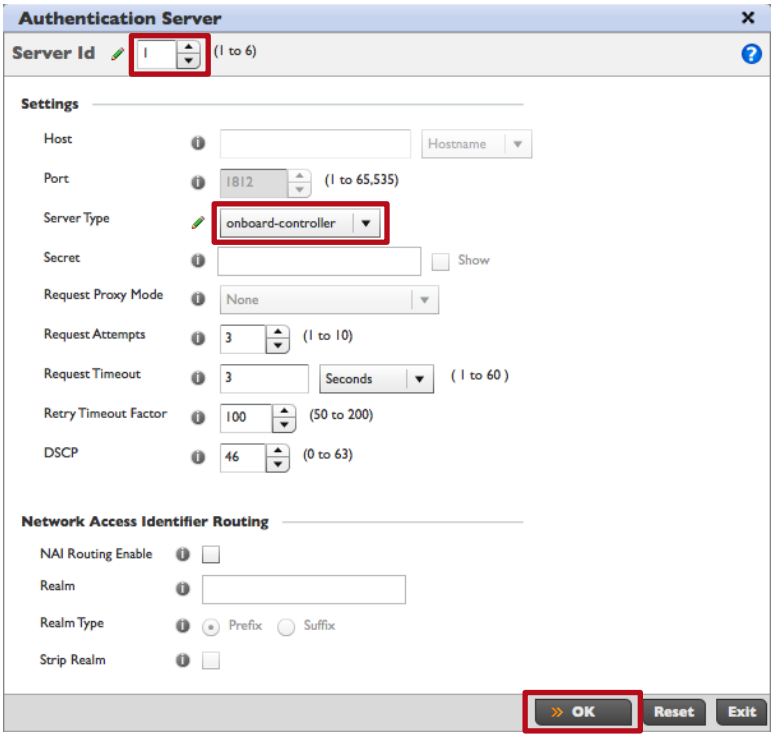
2 In the *AAA Policy* name field enter *internal-aaa* then click *Continue*:



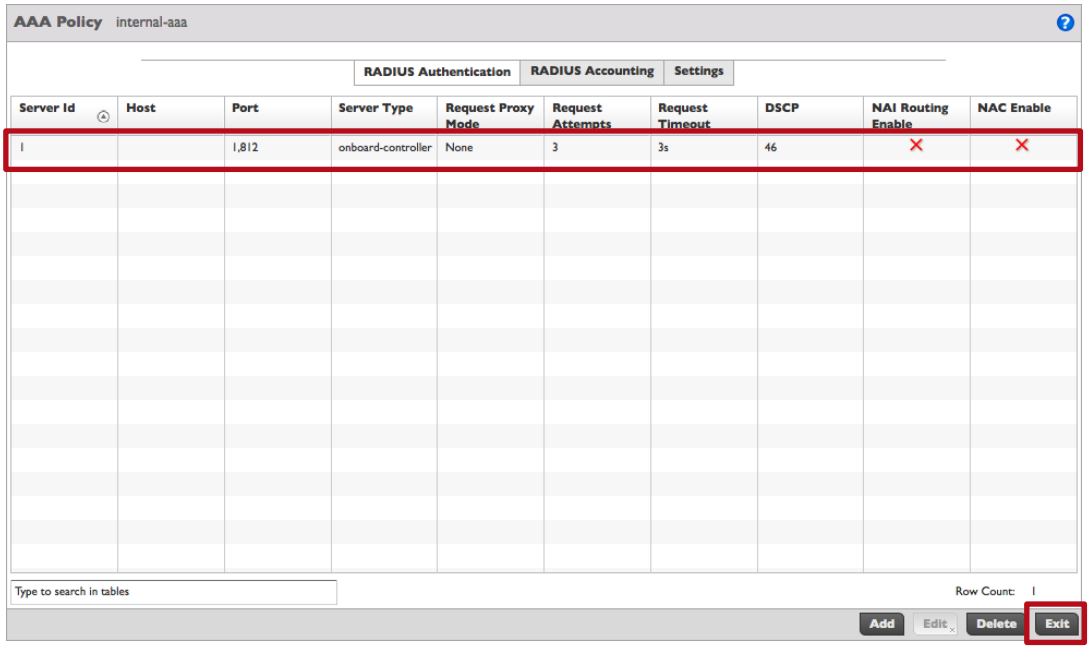
3 Select the *RADIUS Authentication* tab then click *Add*:



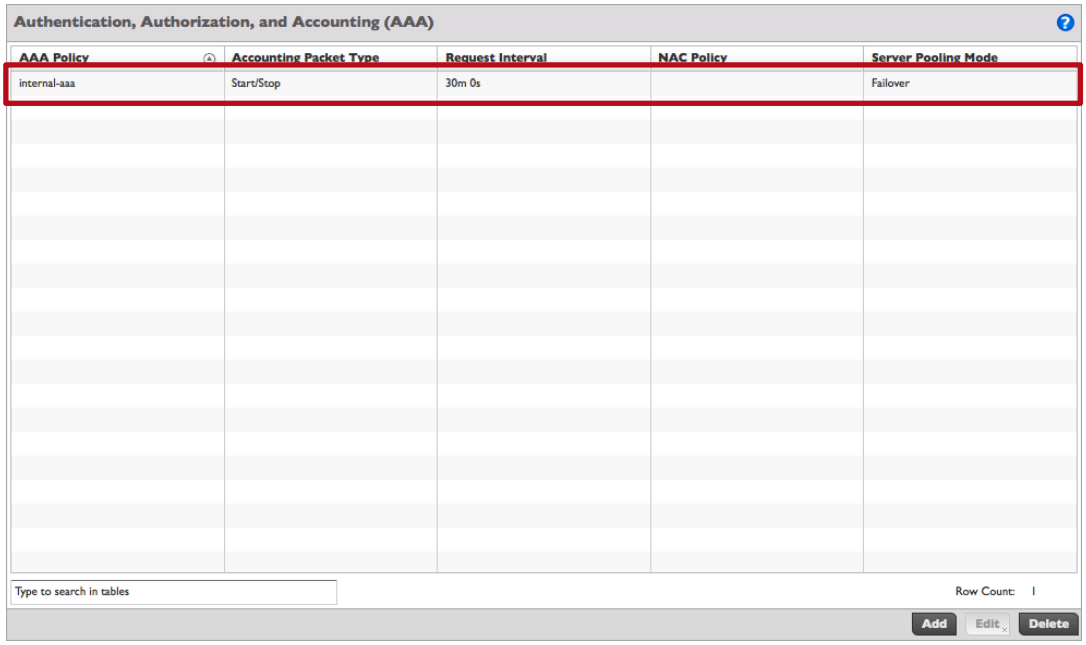
4 Set the *Server Id* to *1* then select the *Server Type* option *onboard-controller*. Click *OK*:



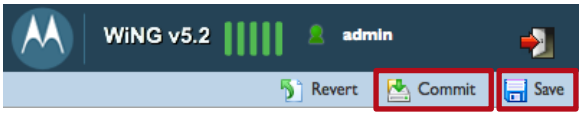
5 A *RADIUS Authentication* server entry has now been defined. Click *Exit*:



6 A AAA Policy named *internal-aaa* has now been defined:



7 *Commit* and Save the changes:



3.2.3 Resulting Configuration

```
!
aaa-policy internal-aaa
 authentication server 1 onboard controller
!
```

3.3 Wireless LAN

Wireless LANs are defined individually within a WiNG 5.X system and can be assigned to groups of Access Point radios using Profiles or to individual Access Point radios as Overrides. Each Wireless LAN consists of policies and configuration parameters which define the basic operating parameters for the Wireless LAN as well as authentication, encryption, VLAN, QoS and firewall parameters. Changes made to a Wireless LANs configuration or assigned policies are automatically inherited by all Access Points serving the Wireless LAN.

For this configuration step a Wireless LAN named ***TMELABS-DOT1X*** will be defined requiring ***EAP*** authentication and ***CCMP*** encryption. The AAA Policy named ***internal-aaa*** will be assigned which will forward EAP authentication requests to the integrated RADIUS service residing on the Wireless Controllers managing the Access Points. In addition the Wireless Clients not receiving dynamic VLAN assignments will be mapped to ***tunneled*** VLAN ***23*** and ***re-authentication*** will be enabled. Dynamic VLAN assignments will also be enabled to permit dynamic VLAN membership based on Active Directory group membership.

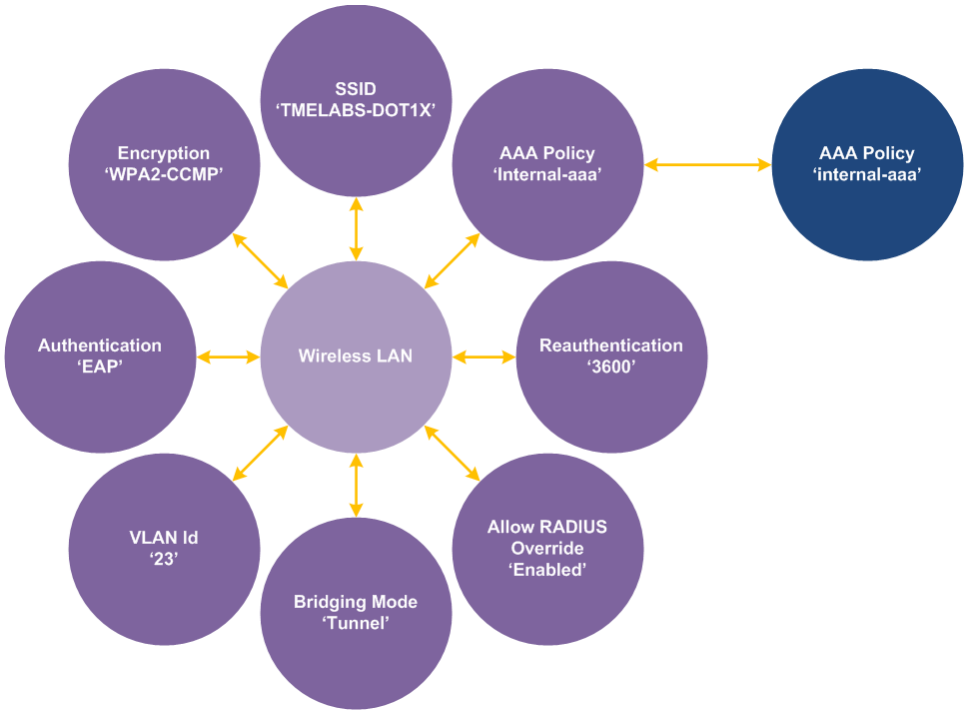


Figure 2.3 – 802.11i EAP Enabled Wireless LAN

3.3.1 Command Line Interface

The following procedure highlights how to create an 802.11i EAP Wireless LAN and assign a AAA Policy using the Command Line Interface (CLI):

1 Using the CLI create a new Wireless LAN named *TMELABS-DOT1X*:

- **I. Set the *encryption-type* to *CCMP***
- **II. Set the *authentication-type* to EAP**
- **III. Assign the *AAA Policy* named *internal-aaa***
- **IV. Assign the tunneled VLAN id *23***
- **V. Enable re-authentication (example *3600* seconds)**
- **VI. Enable dynamic RADIUS VLAN assignments**

```
rfs4000-1(config)# wlan TMELABS-DOT1X
rfs4000-1(config-wlan-TMELABS-DOT1X)# encryption-type ccmp
rfs4000-1(config-wlan-TMELABS-DOT1X)# authentication-type eap
rfs4000-1(config-wlan-TMELABS-DOT1X)# use aaa-policy internal-aaa
rfs4000-1(config-wlan-TMELABS-DOT1X)# vlan 23
rfs4000-1(config-wlan-TMELABS-DOT1X)# bridging-mode tunnel
rfs4000-1(config-wlan-TMELABS-DOT1X)# wireless-client reauthentication 3600
rfs4000-1(config-wlan-TMELABS-DOT1X)# radius vlan-assignment
rfs4000-1(config-wlan-TMELABS-DOT1X)# exit
```

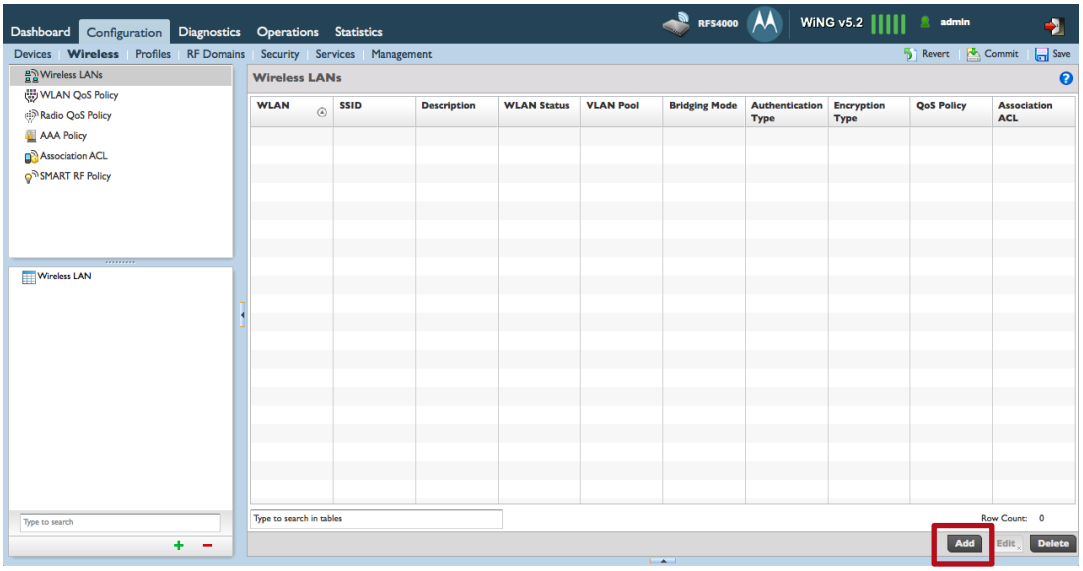
2 *Commit* and *Save* the changes:

```
rfs4000-1(config)# commit write
```

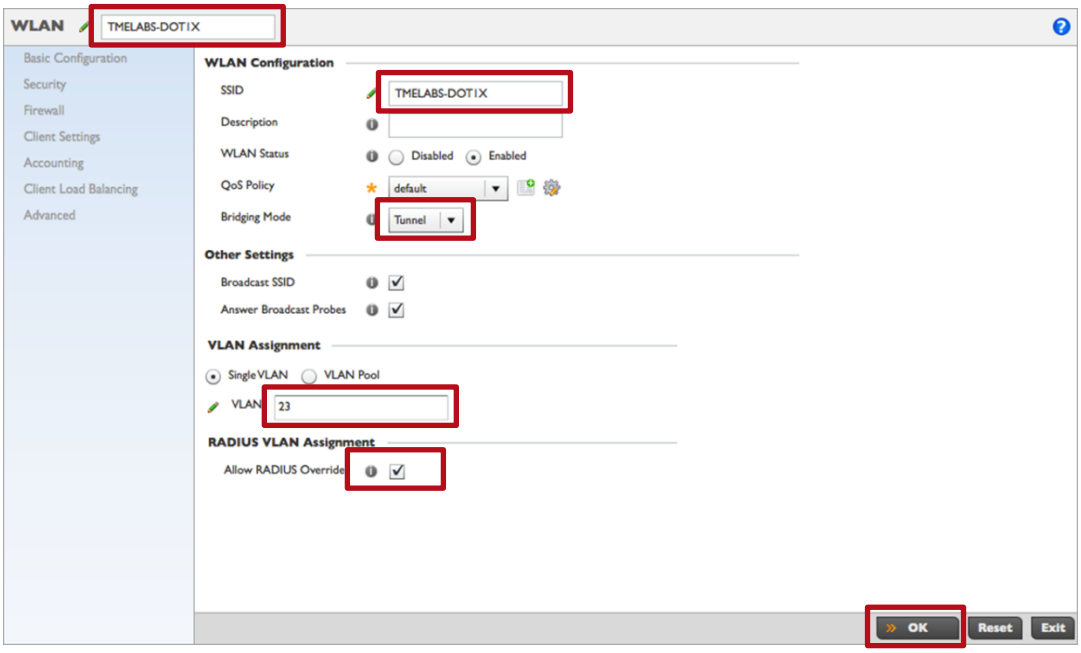
3.3.2 Web User Interface

The following procedure highlights how to create an 802.11i EAP Wireless LAN and assign a AAA Policy using the Web User Interface (Web UI):

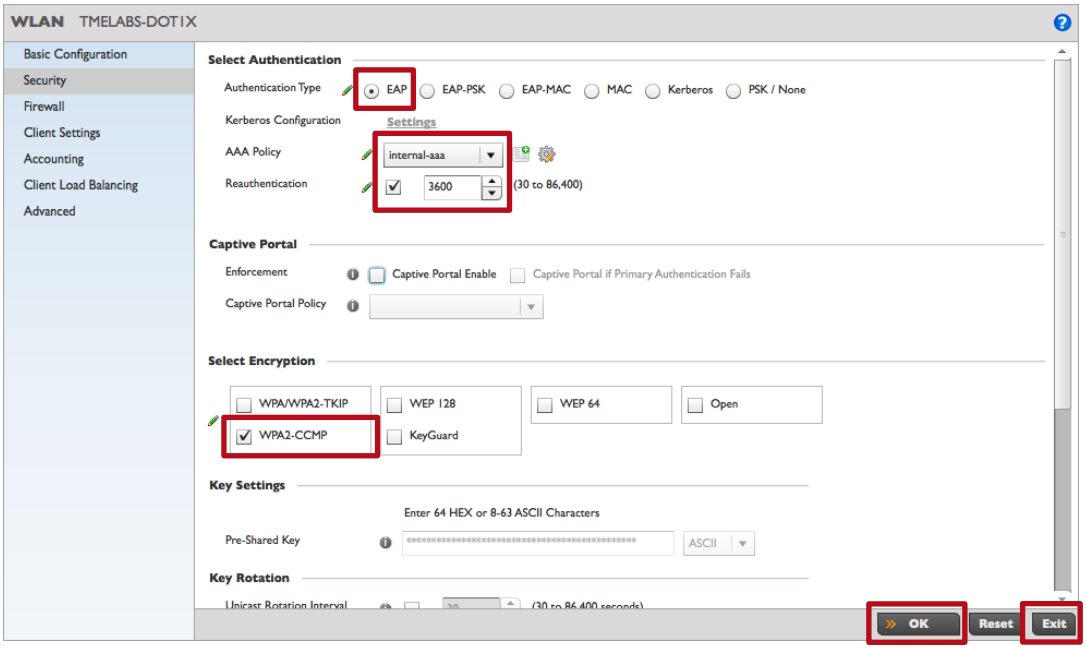
1 Select *Configuration* → *Wireless* → *Wireless LANs* → *Add*:



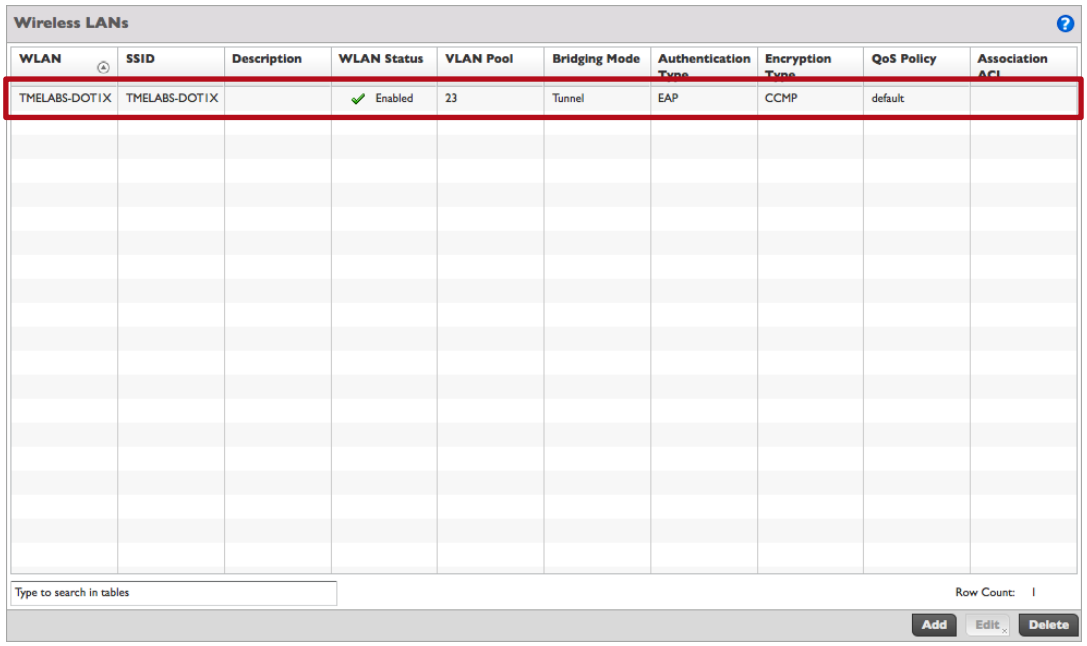
2 In the *WLAN* and *SSID* fields enter *TMELABS-DOT1X*. Set the *Bridging Mode* to *Tunnel* then enter a *VLAN*. Check the option *Allow RADIUS Override* then click *OK*:



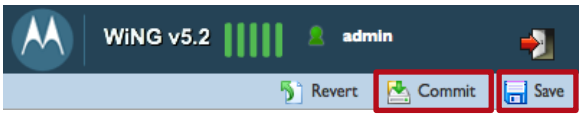
3 Select *Security*. Set the *Authentication Type* to *EAP* then assign the *AAA Policy* named *internal-aaa*. Enable *Reauthentication* then enter the re-authentication value *3600* (1 hour). Set the *Encryption Type* to *WPA2-CCMP* then click *OK* and *Exit*:



4 A 802.11i EAP Wireless LAN named *TMELABS-DOT1X* has now been defined:



5 *Commit* and Save the changes:



3.3.3 Resulting Configuration

```
!
wlan TMELABS-DOT1X
 ssid TMELABS-DOT1X
 vlan 23
 bridging-mode tunnel
 encryption-type ccmp
 authentication-type eap
 wireless-client reauthentication 3600
 radius vlan-assignment
 use aaa-policy internal-aaa
!
```

3.4 RADIUS Groups

Once an EAP Wireless Client has been authenticated the Wireless Client can be optionally authorized using local groups. When LDAP Group Verification is enabled on a RADIUS Server Policy, the integrated RADIUS service will query Active Directory for the groups the authenticated user is a member of and will attempt to match a returned Active Directory group name to a locally defined group which has authorization attributes assigned:

1. If no local group can be matched or authorization fails, the user will be denied access to the Wireless LAN.
2. If a group is matched and all the authorization attribute checks pass, the user is permitted access to the Wireless LAN and dynamic VLAN membership assigned.

The local group name must match the corresponding Active Directory group name. In addition each local group must include the SSID name that the users are authorized to access. All other authorization attributes such as Time of Day, Day or Week, VLAN, Roles, Rate Limits are optional.

For this configuration step three local groups named Engineering, Marketing and Sales will be defined which match the group names Wireless Clients are members of in Active Directory:

1. A local group called ***Engineering*** will be defined with the following attributes:
   a. Users will be permitted access to the ***TMELABS-DOT1X*** Wireless LAN
   b. Users will be mapped to the tunneled VLAN ***25***
   c. Users will be permitted access ***Monday → Sunday*** from ***6:00AM → 11:59PM***
2. A local group called ***Marketing*** will be defined with the following attributes:
   a. Users will be permitted access to the ***TMELABS-DOT1X*** Wireless LAN
   b. Users will be mapped to the tunneled VLAN ***24***
   c. Users will be permitted access ***Monday → Friday*** from ***7:00AM → 9:00PM***
3. A local group called ***Sales*** will be defined with the following attributes:
   a. Users will be permitted access to the ***TMELABS-DOT1X*** Wireless LAN
   b. Users will be mapped to the tunneled VLAN ***23***
   c. Users will be permitted access ***Monday → Sunday*** from ***8:00AM → 7:00PM***

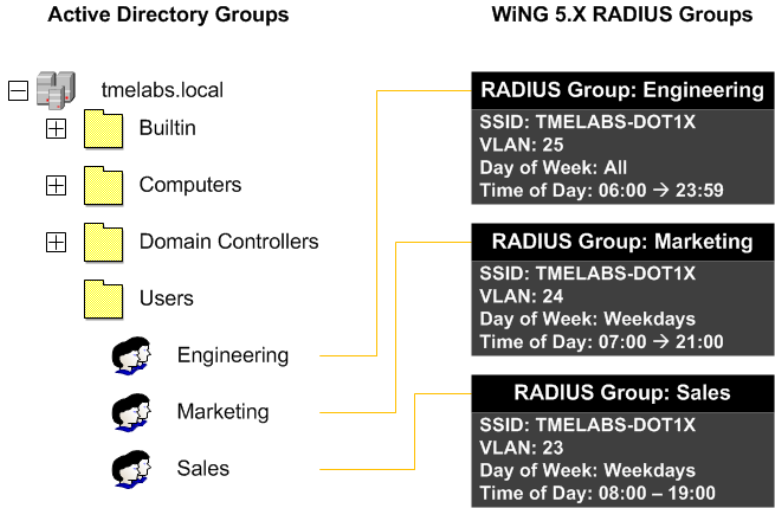


Figure 2.4 – RADIUS Groups

3.4.1 Command Line Interface

The following procedure highlights how to create RADIUS Groups and Authorization Attributes using the Command Line Interface (CLI):

1 Using the CLI create a RADIUS Group named *Engineering* and assign *SSID*, *Time of Day* and *Day of Week* authorization attributes and *VLAN* membership:

```
rfs4000-1(config)# radius-group Engineering
rfs4000-1(config-radius-group-Engineering)# policy vlan 25
rfs4000-1(config-radius-group-Engineering)# policy ssid TMELABS-DOT1X
rfs4000-1(config-radius-group-Engineering)# policy day all
rfs4000-1(config-radius-group-Engineering)# policy time start 06:00 end 23:59
rfs4000-1(config-radius-group-Engineering)# exit
```

2 Using the CLI create a RADIUS Group named *Marketing* and assign *SSID*, *Time of Day* and *Day of Week* authorization attributes and *VLAN* membership:

```
rfs4000-1(config)# radius-group Marketing
rfs4000-1(config-radius-group-Marketing)# policy vlan 24
rfs4000-1(config-radius-group-Marketing)# policy ssid TMELABS-DOT1X
rfs4000-1(config-radius-group-Marketing)# policy day weekdays
rfs4000-1(config-radius-group-Marketing)# policy time start 07:00 end 21:00
rfs4000-1(config-radius-group-Marketing)# exit
```

3 Using the CLI create a RADIUS Group named *Sales* and assign *SSID*, *Time of Day* and *Day of Week* authorization attributes and *VLAN* membership:

```
rfs4000-1(config)# radius-group Sales
rfs4000-1(config-radius-group-Sales)# policy vlan 23
rfs4000-1(config-radius-group-Sales)# policy ssid TMELABS-DOT1X
rfs4000-1(config-radius-group-Sales)# policy day weekdays
rfs4000-1(config-radius-group-Sales)# policy time start 08:00 end 19:00
rfs4000-1(config-radius-group-Sales)# exit
```

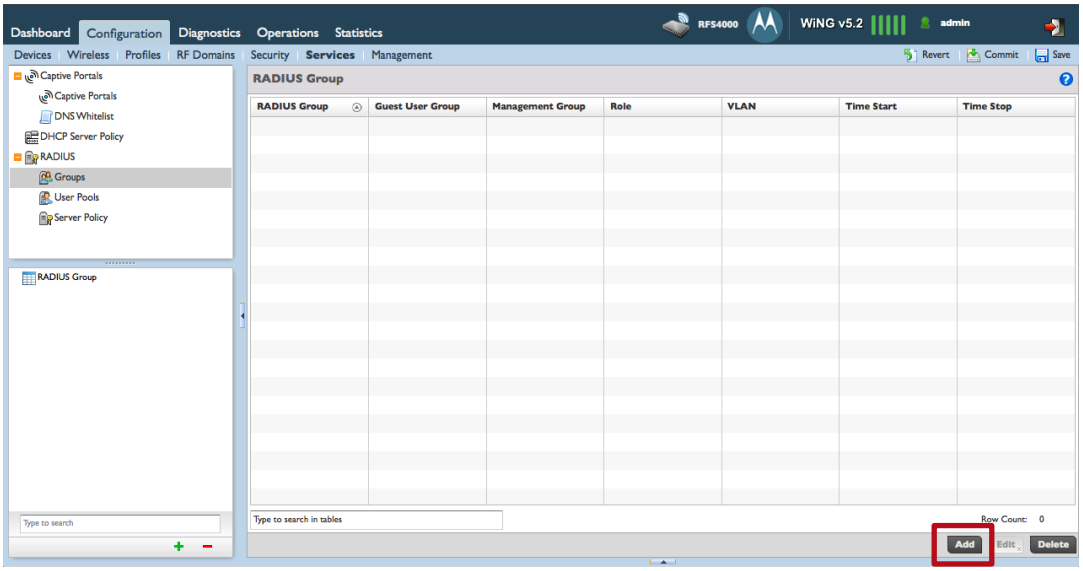
7 *Commit* and *Save* the changes:

```
rfs4000-1(config)# commit write
```

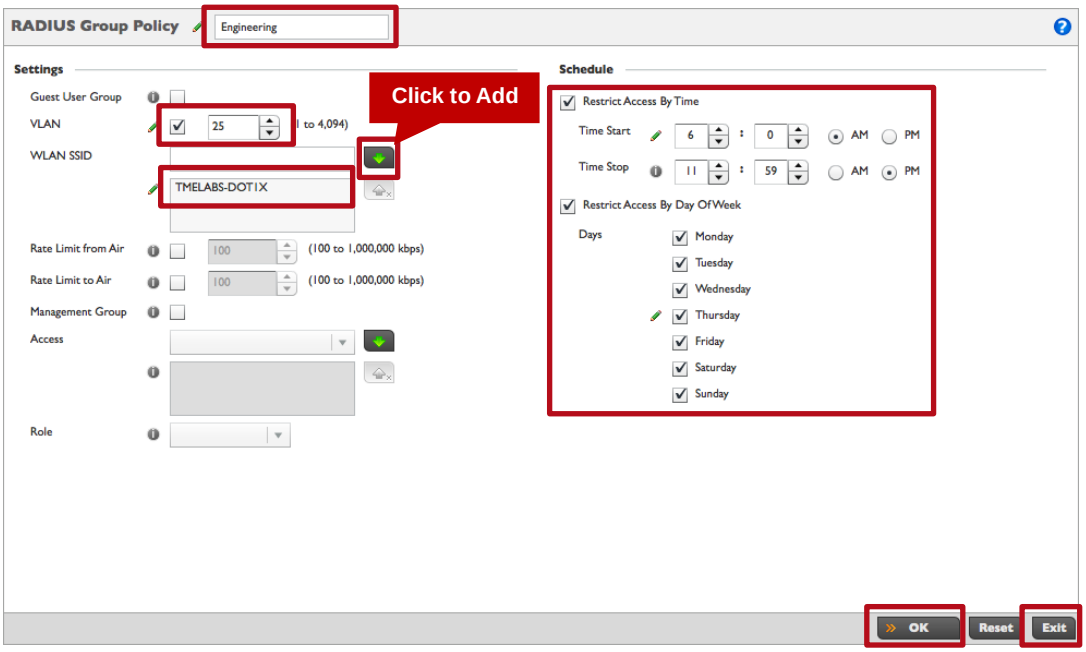
3.4.2 Web User Interface

The following procedure highlights how to create RADIUS Groups Authorization Attributes using the Web User Interface (Web UI):

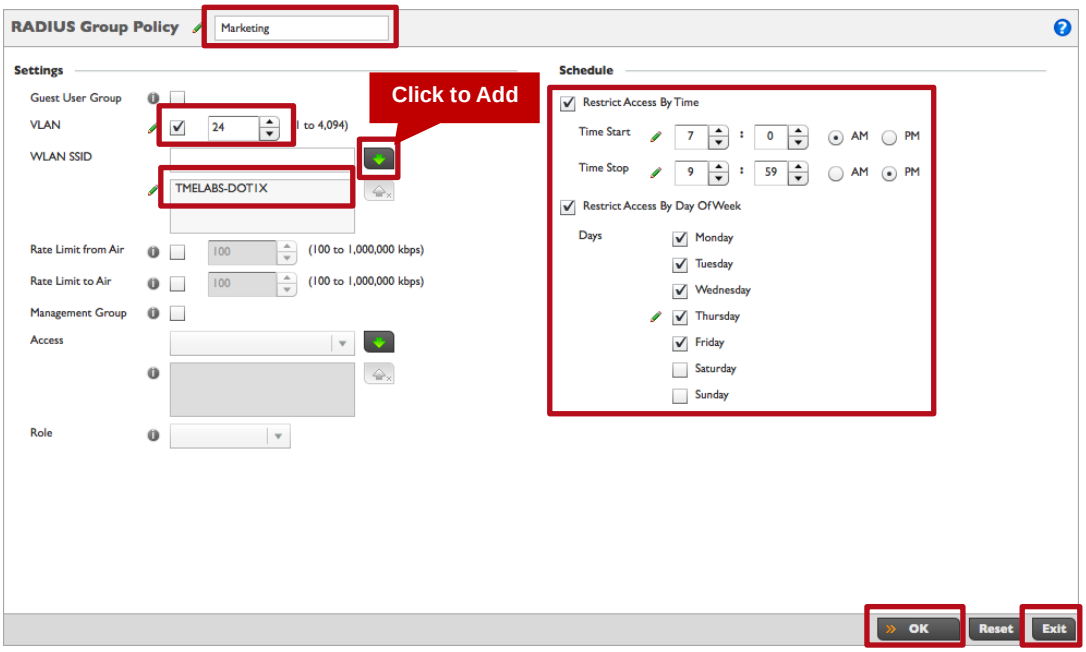
1 Select *Configuration* → *Services* → *RADIUS* → *Groups* → *Add*:



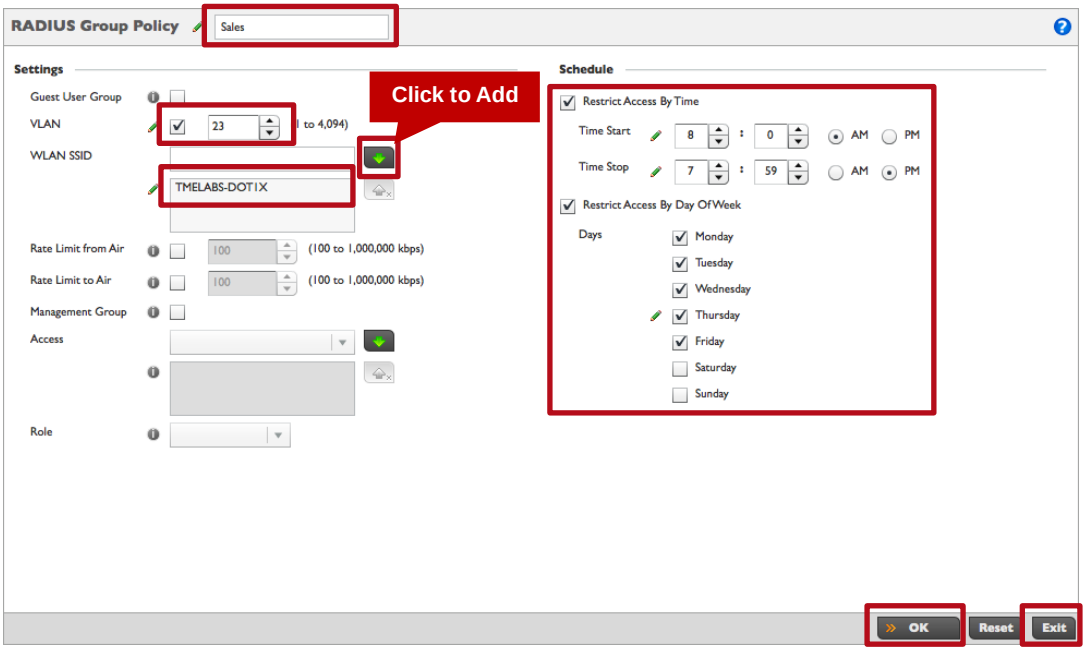
2 In the *RADIUS Group Policy* field enter *Engineering*. Set the VLAN to *25* then in the *WLAN SSID* name field type *TMELABS-DOT1X* then click the down arrow to *Add*. Assign *Time* and *Day* permissions then click *OK*:



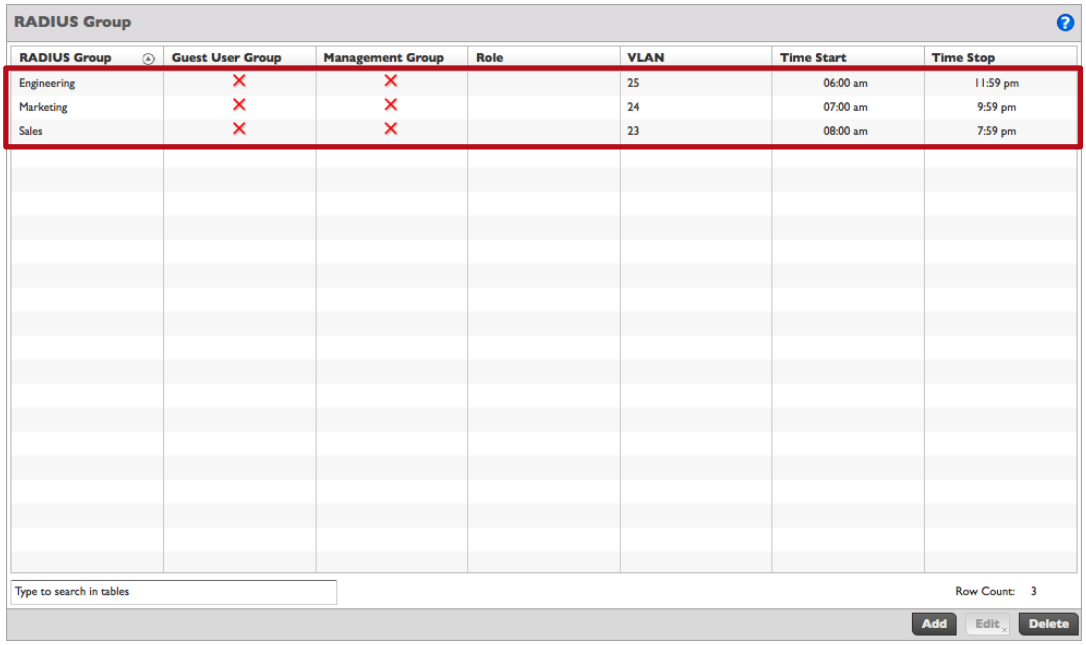
3 In the *RADIUS Group Policy* field enter *Marketing*. Set the VLAN to *24* then in the *WLAN SSID* name field type *TMELABS-DOT1X* then click the down arrow to *Add*. Assign *Time* and *Day* permissions then click *OK*:



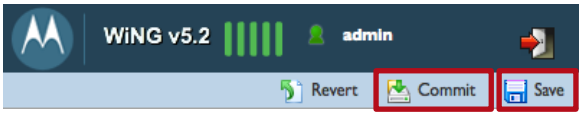
4 In the *RADIUS Group Policy* field enter *Sales*. Set the VLAN to *23* then in the *WLAN SSID* name field type *TMELABS-DOT1X* then click the down arrow to *Add*. Assign *Time* and *Day* permissions then click *OK*:



5 RADIUS groups named *Engineering*, *Marketing* and *Sales* have now been defined:



5 *Commit* and Save the changes:



3.4.3 Resulting Configuration

```
!
radius-group Engineering
 policy vlan 25
 policy ssid TMELABS-DOT1X
 policy day mo
 policy day tu
 policy day we
 policy day th
 policy day fr
 policy day sa
 policy day su
 policy time start 06:00 end 23:59
!
radius-group Marketing
 policy vlan 24
 policy ssid TMELABS-DOT1X
```

```
 policy day mo
 policy day tu
 policy day we
 policy day th
 policy day fr
 policy time start 07:00 end 21:00
!
radius-group Sales
 policy vlan 23
 policy ssid TMELABS-DOT1X
 policy day mo
 policy day tu
 policy day we
 policy day th
 policy day fr
 policy time start 08:00 end 19:00
!
```

3.5 RADIUS Server Policy

The RADIUS Server Policy configures the RADIUS service that can be enabled on Wireless Controllers or Independent Access Points. Each RADIUS Server Policy determines which devices can authenticate, which authentication protocols are enabled and where the user directory resides. RADIUS Server Policies can be assigned to individual Wireless Controllers or Independent Access Points using Device Overrides or to groups of devices using Profiles.

For this configuration example a RADIUS Server Policy named ***internal-aaa*** will be defined with a single ***LDAP*** authentication server entry using the following parameters:

	Parameter	Value
Server Policy	Authentication Data Source	*LDAP*
	LDAP Groups	*Engineering* *Marketing* *Sales*
	LDAP Group Verification	*Enabled*
	Authentication Types	*All*
LDAP Network	IP Address	*192.168.10.20*
	Login	*(sAMAccountName=%{Stripped-User-Name:-%{User-Name}})*
	Port	*389*
	Timeout	*10*
LDAP Access	Bind DN	*cn=ISC,cn=Users,dc=tmelabs,dc=local*
	Base DN	*dc=tmelabs,dc=local*
	Bind Password	*hellomoto*
	Password Attribute	*UserPassword*
LDAP Attributes	Group Attribute	*cn*
	Group Filter	*(|(&(objectClass=group)(member=%{Ldap-UserDn}))(&(objectClass=GroupOfUniqueNames)(uniquemember=%{Ldap-userDn})))*
	Group Membership Attribute	*radiusGroupName*

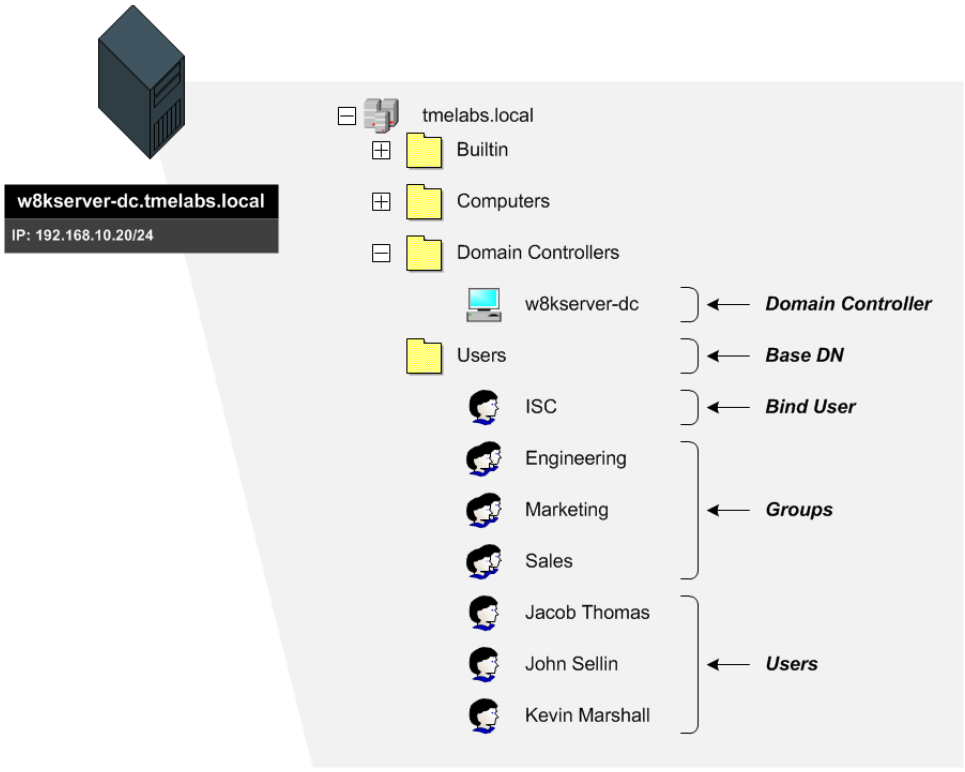


Figure 3.5 – Active Directory Server Configuration

3.5.1 Command Line Interface

The following procedure highlights how to create an RADIUS Server Policy and define LDAP parameters using the Command Line Interface (CLI):

1 Using the CLI create a new *RADIUS Server Policy* named *internal-aaa* and enable the *LDAP* data-source:

```
rfs4000-1(config)# radius-server-policy internal-aaa
rfs4000-1(config-radius-server-policy-internal-aaa)# authentication data-source ldap
```

2 Add the RADIUS Groups named *Engineering*, *Marketing* and *Sales* which will be used for authorization:

```
rfs4000-1(config-radius-server-policy-internal-aaa)# use radius-group Engineering
rfs4000-1(config-radius-server-policy-internal-aaa)# use radius-group Marketing
rfs4000-1(config-radius-server-policy-internal-aaa)# use radius-group Sales
```

3 Create a primary LDAP server and enter the *IP Address*, *Bind DN*, *Base DN* and required attribute parameters:

```
rfs4000-1(config-radius-server-policy-internal-aaa)# ldap-server primary host
192.168.10.20 port 389 login (sAMAccountName=%{Stripped-User-Name:-%{User-Name}})
bind-dn cn=ISC,cn=Users,dc=tmelabs,dc=local base-dn cn=Users,dc=tmelabs,dc=local
passwd 0 hellomot passwd-attr UserPassword group-attr cn group-filter
(|(&(objectClass=group)(member=%{Ldap-
UserDn}))(&(objectClass=GroupOfUniqueNames)(uniquemember=%{Ldap-userDn}))) group-
membership radiusGroupName net-timeout 10
```

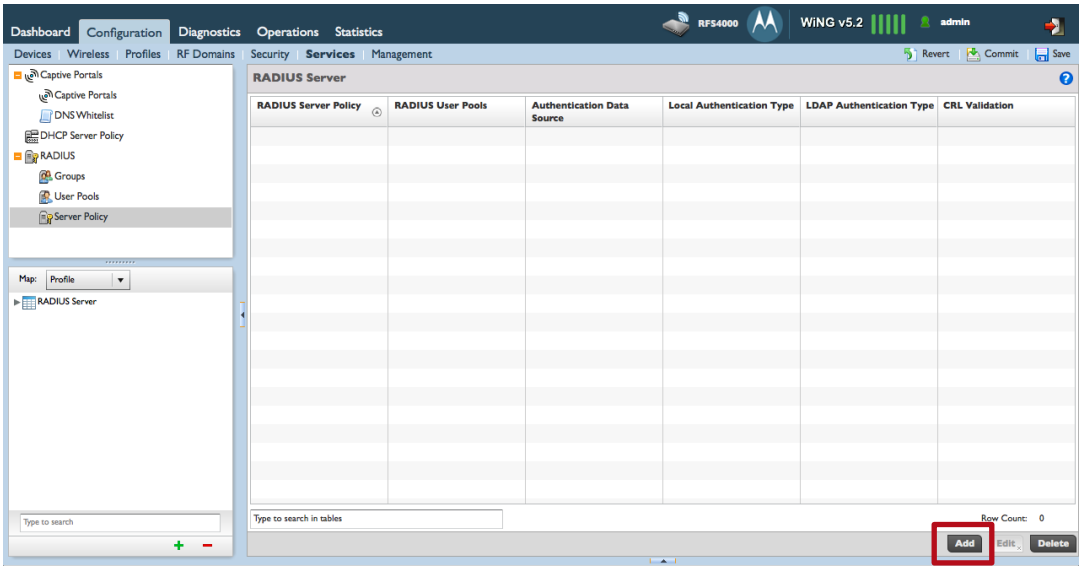
4 *Exit* then *Commit* and *Save* the changes:

```
rfs4000-1(config-radius-server-policy-internal-aaa)# exit
rfs4000-1(config)# commit write
```

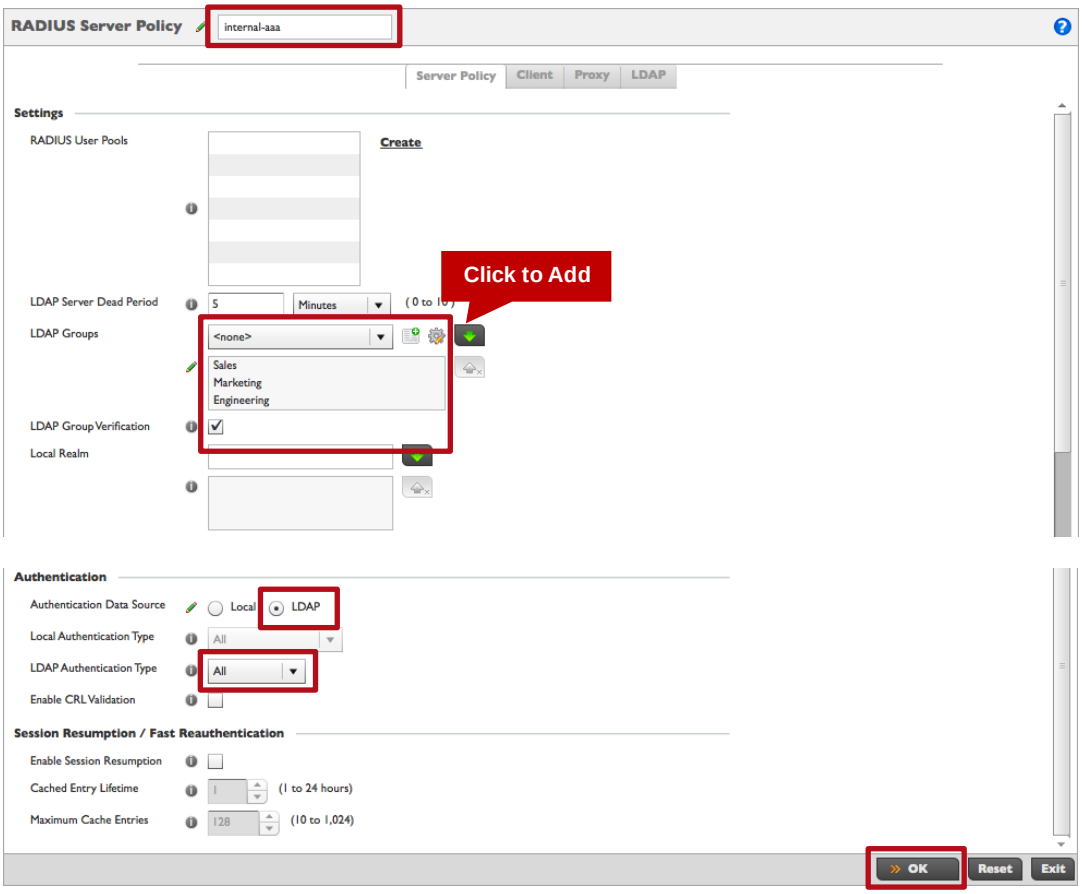
3.5.2 Web User Interface

The following procedure highlights how to create an RADIUS Server Policy and define LDAP parameters using the Web User Interface (Web UI):

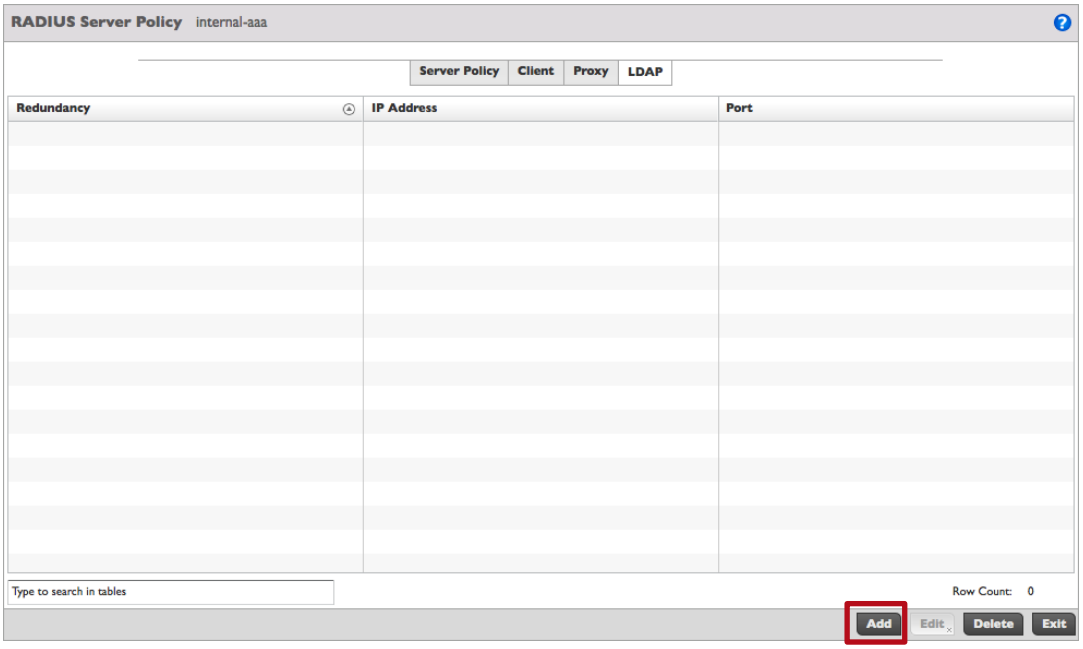
1 Select *Configuration* → *Services* → *RADIUS* → *Server Policy* → *Add*:



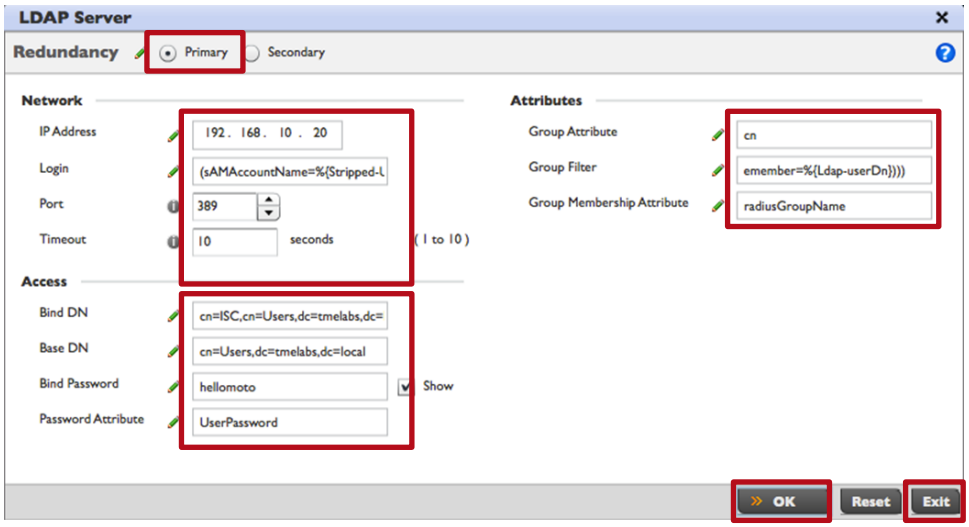
2 In the *RADIUS Server Policy Name* field enter *internal-aaa*. Under the *LDAP Groups* pull-down menu select and add the *Engineering*, *Marketing* and *Sales* groups. Check the option *LDAP Group Verification* then select the *Authentication Data Source* type *LDAP*. Select the *LDAP Authentication Type* option *All* then click *OK*:



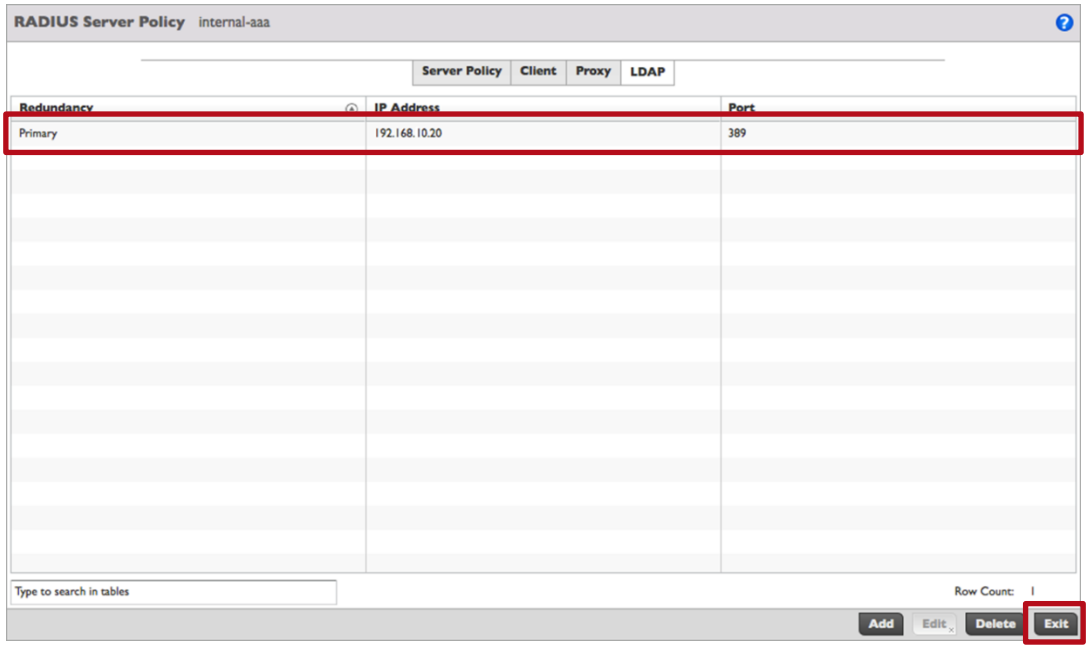
3 Select the *LDAP* tab then click *Add*:



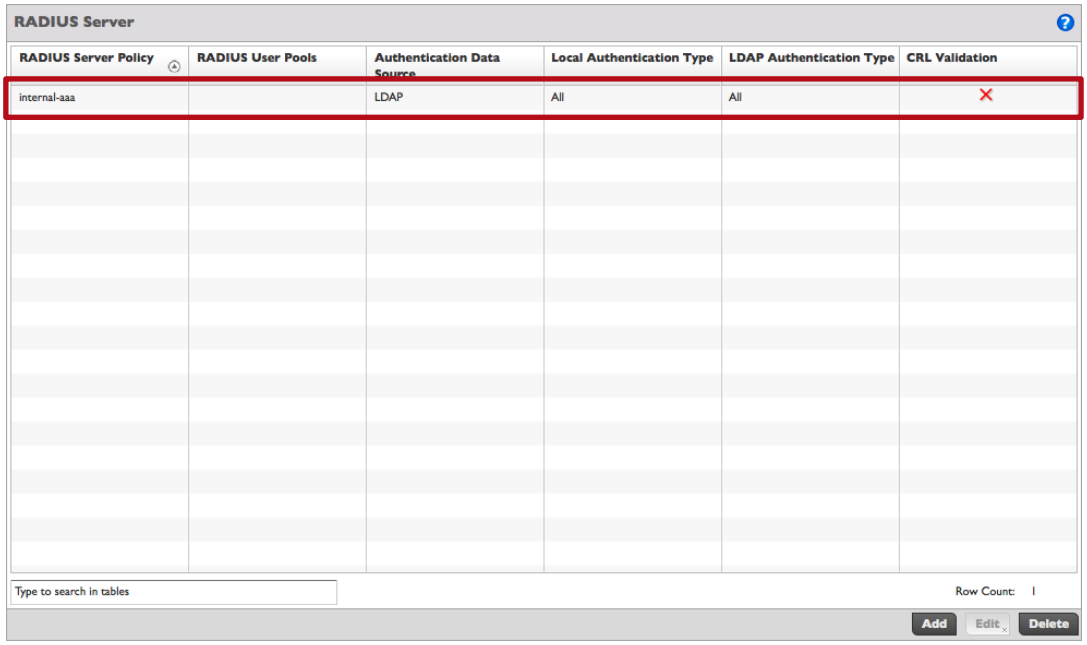
4 Select the *Redundancy* option *Primary* then enter the *IP Address*, *Bind DN*, *Base DN* and required attribute parameters. Click *OK* then *Exit*:



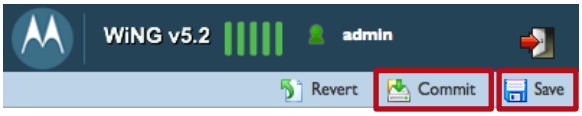
5 A *Primary* LDAP Server has now been defined. Click *Exit*:



6 A *RADIUS Server Policy* named *internal-aaa* has now been defined:



7 *Commit* and *Save* the changes:



3.5.3 Resulting Configuration

```
!
radius-server-policy internal-aaa
 authentication data-source ldap
 ldap-server primary host 192.168.10.20 port 389 login (sAMAccountName=%{Stripped-User-Name:-%{User-Name}}) bind-dn cn=ISC,cn=Users,dc=tmelabs,dc=local base-dn cn=Users,dc=tmelabs,dc=local passwd 0 hellomoto passwd-attr UserPassword group-attr cn group-filter (|(&(objectClass=group)(member=%{Ldap-UserDn}))(&(objectClass=GroupOfUniqueNames)(uniquemember=%{Ldap-userDn}))) group-membership radiusGroupName net-timeout 10
 use radius-group Sales
 use radius-group Marketing
 use radius-group Engineering
!
```

3.6 Trustpoints

EAP authentication requires Public Key Infrastructure (PKI) to provide privacy and mutual authentication. In WiNG 5.X server and CA certificates are installed into Trustpoints which can be used by the RADIUS service for EAP authentication as well as the HTTPS Captive Portal and management interfaces.

By default each Motorola Wireless Controller and Access Point includes a self-signed certificate which is that installed into a Trustpoint named ***default-trustpoint***. As the certificate is self-signed there is no ability for the Wireless Client to verify the server certificate. While the default Trustpoint can be used for demonstrations or lab trials it is recommended that a signed certificate be installed into a new Trustpoint that is assigned to the RADIUS service so the Wireless Clients to verify the identity of the RADIUS server prior to forwarding any credentials.

For this configuration step a new ***RSA Keypair*** will be generated and used to create a ***Certificate Signing Request*** (CSR) that can be signed by a public or private ***Certificate Authority*** (CA). The signed certificate and corresponding Root CA Certificate will be installed into a new Trustpoint named ***lab-ca*** which will be to the RADIUS service.

Note: Certificates are device specific and a unique certificate will be required for each Wireless Controller or Access Point providing RADIUS services.

3.6.1 Command Line Interface

The following procedure highlights how to create a RSA Keypair, generate a Certificate Signing Request (CSR) install a CA and Signed Certificate into a new Trustpoint, then assign the Trustpoint to the RADIUS service using the Command Line Interface (CLI):

1 Generate a *2048-bit RSA keypair* and name it the same as the *Hostname* of the *Wireless Controller*:

```
rfs4000-1# crypto key generate rsa rfs4000-1 2048


RSA Keypair successfully generated
```

2 View the installed *RSA keypairs*:

```
rfs4000-1# show crypto key rsa
-------------------------------------------------------------------------------
        #                       KEY NAME                        KEY LENGTH
-------------------------------------------------------------------------------
  1                 rfs4000-1                       2048
  2                 default_rsa_key                 1024
-------------------------------------------------------------------------------
```

3 Generate a *Certificate Signing Request* (CSR) using the *RSA keypair* created above. Optionally include an email address, domain name and IP address. The CSR in this example uses automatically generated information and saves the *CSR* to a file named *rfs4000-1-csr.txt* on an external TFTP server *192.168.10.5*. The CSR can then be signed by a public or private *Certificate Authority* (CA):

```
rfs4000-1# crypto pki export request use-rsa-key rfs4000-1 autogen-subject-name email
admin@tmelabs.local fqdn tmelabs.local ip-address 192.168.20.20
tftp://192.168.10.5/rfs4000-1-csr.txt

Successfully generated and exported certificate request
```

4 Import the *Root CA Certificate* issued from the public or private *CA* that signed the *CSR* generated above. In the below example the *Root CA Certificate* with the filename *lab-ca.cer* is imported from the TFTP server *192.168.10.5* and is installed into a new Trustpoint named *lab-ca*:

```
rfs4000-1# crypto pki authenticate lab-ca tftp://192.168.10.5/lab-ca.cer

Successfully imported CA certificate
```

5 Import the signed *Server Certificate* issued from the public or private *CA*. In the below example the signed Server Certificate with the filename *rfs4000-1-cert.cer* is imported from the TFTP server *192.168.10.5* and is installed into a new Trustpoint named *lab-ca*:

```
rfs4000-1# crypto pki import certificate lab-ca tftp://192.168.10.5/rfs4000-1-cert.cer

Signed certificate for Trustpoint lab-ca sucessfully imported
```

6 View the new Trustpoint:

```
rfs4000-1# show crypto pki trustpoints lab-ca
```

```
Trustpoint Name: lab-ca
-------------------------------------------------------------------------------
  CRL present: no
  Server Certificate details:
    Key used: rfs4000-1
    Serial Number: 6150e21d000000000003
    Subject Name:
      C=us, L=JohnsonCityTN, CN=rfs4000-1/emailAddress=admin@tmelabs.local
    Subject Alternative Name:
      email:admin@tmelabs.local, DNS:tmelabs.local, IP Address:192.168.20.20
    Issuer Name:
      DC=local, DC=tmelabs, CN=LAB-CA
    Valid From : Thu Dec  1 21:09:55 2011 UTC
    Valid Until: Sat Nov 30 21:09:55 2013 UTC

  CA Certificate details:
    Serial Number: 72eb31106dcce78144b552ecd43f8f3c
    Subject Name:
      DC=local, DC=tmelabs, CN=LAB-CA
    Issuer Name:
      DC=local, DC=tmelabs, CN=LAB-CA
    Valid From : Thu Dec  1 20:54:14 2011 UTC
    Valid Until: Thu Dec  1 21:04:12 2016 UTC
```

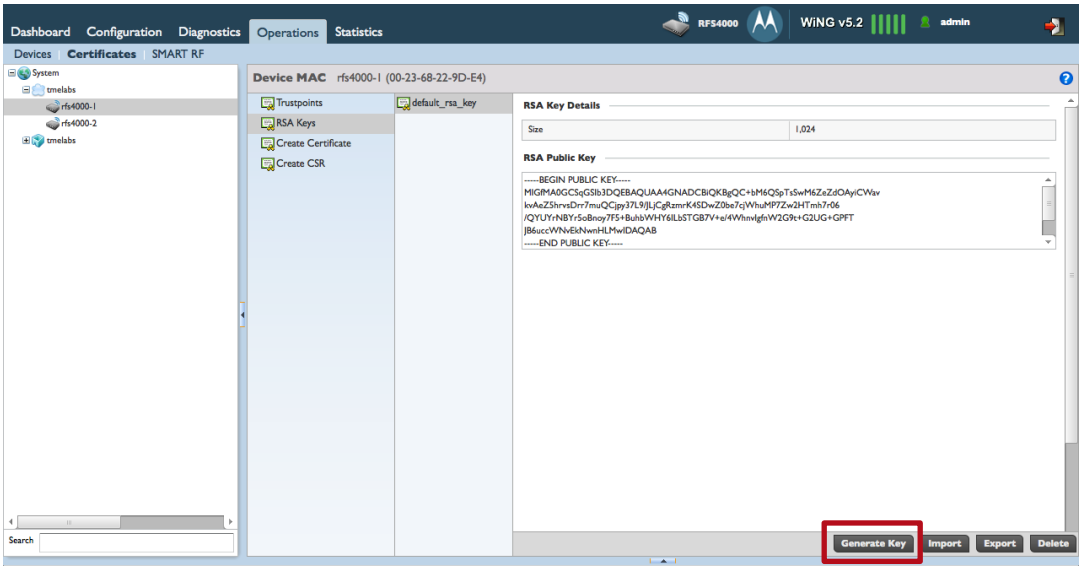
7 Access the Wireless Controllers *Device* configuration and assign the new *Trustpoint* to the RADIUS service:

```
rfs4000-1(config)# self
rfs4000-1(config-device-00-23-68-22-9D-E4)# trustpoint radius-ca tme-lab
rfs4000-1(config-device-00-23-68-22-9D-E4)# trustpoint radius-server tme-lab
rfs4000-1(config-device-00-23-68-22-9D-E4)# exit
rfs4000-1(config)# commit write
```

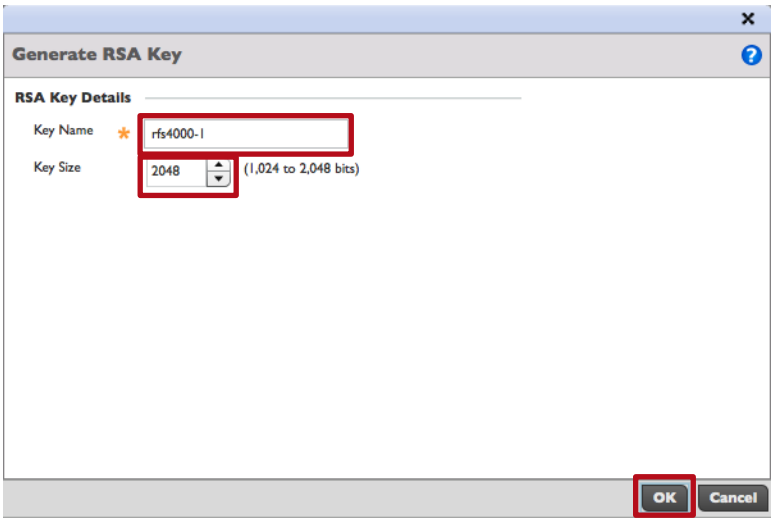
3.6.2 Web User Interface

The following procedure highlights how to create a RSA Keypair, generate a Certificate Signing Request (CSR) install a CA and Signed Certificate into a new Trustpoint, then assign the Trustpoint to the RADIUS service using the Web User Interface (Web UI):

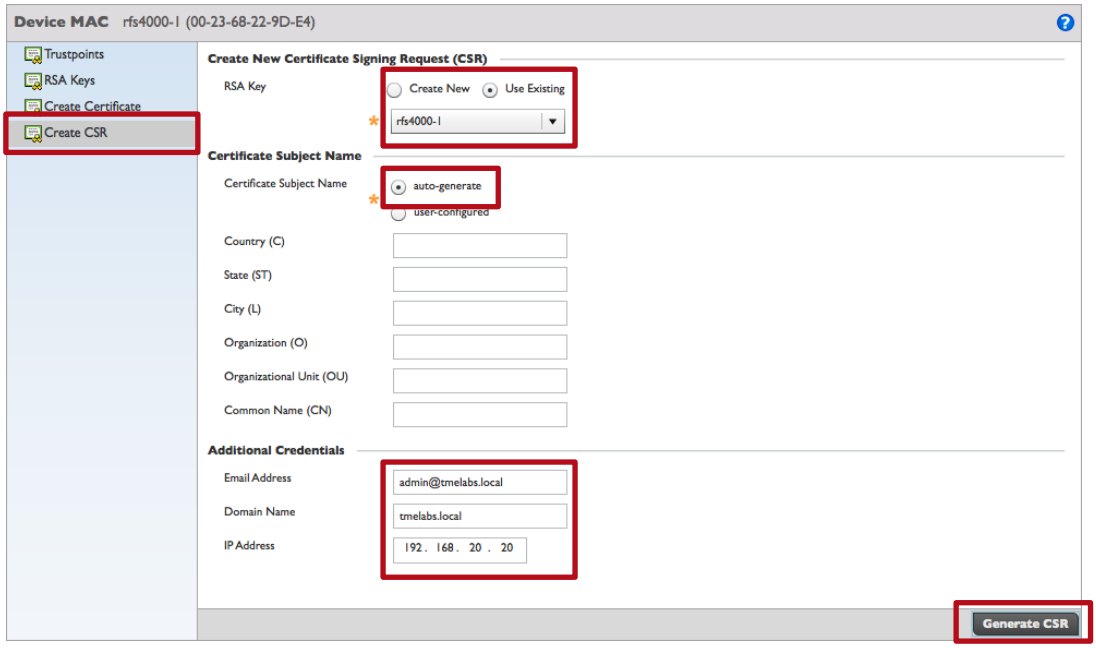
1 Select *Operations* → *Certificates* → *RF-Domain-Name* → *Controller-Name* → *Generate Key*:



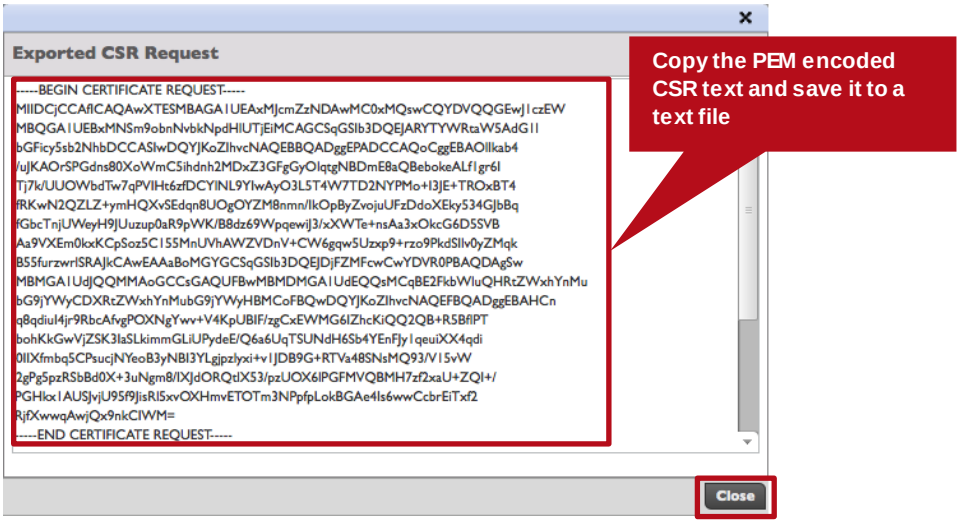
2 In the *Key Name* field enter the *Hostname* of the *Wireless Controller* then set the *Key Size* to *2048*. Click *OK*:



3 In the *Left* panel select *Create CSR*. Select the *RSA Key* option *Use Existing* then select the *RSA Keypair* name created in the previous step. Select the *Certificate Subject Name* option *auto-generate* then optionally enter the *Additional Credentials*. Click *Generate CSR*:

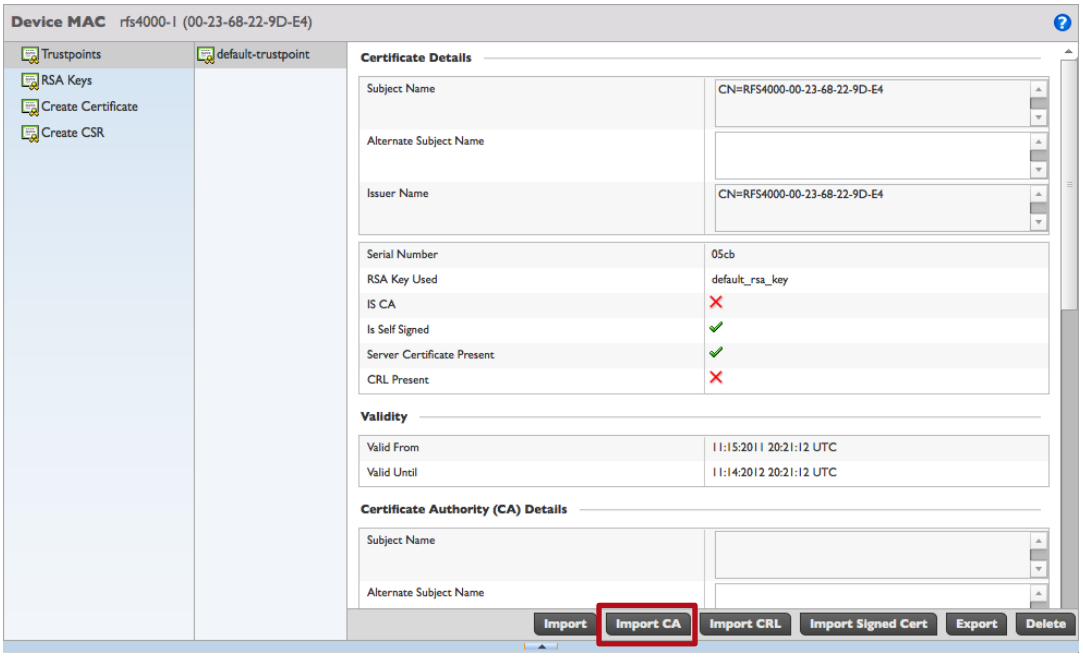


4 *Copy* the PEM encoded text provided in the *Exported CSR Request* window and save it to a text file. This PEM encoded text will need to be required by the public or private *Certificate Authority (CA)* to sign the Certificate. Click *Close*:

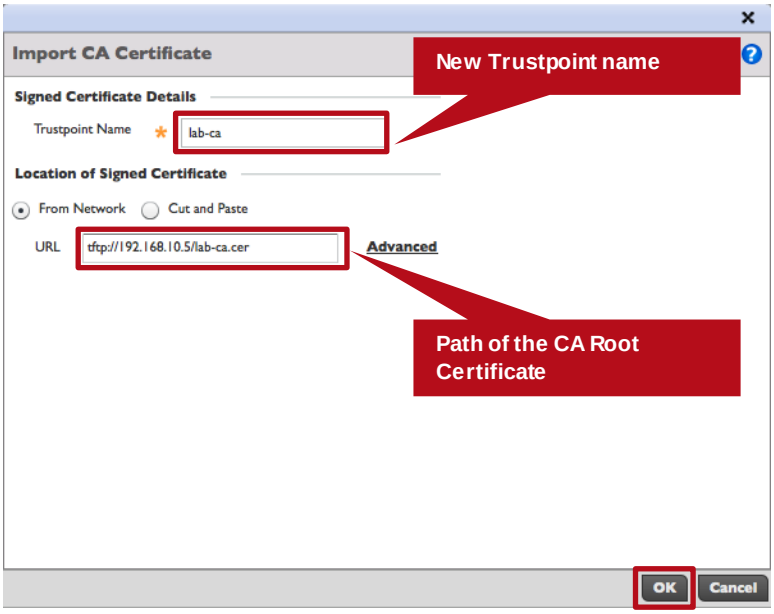


Note: Before proceeding the Certificate Signing Request (CSR) ***MUST*** be signed by a public or private Certificate Authority (CA). Additionally the CAs Root Certificate and Signed Certificate MUST be downloaded from the CA using a Base 64 / PEM encoded format before they can be imported into a trustpoint on the Wireless Controller / Independent Access Point.

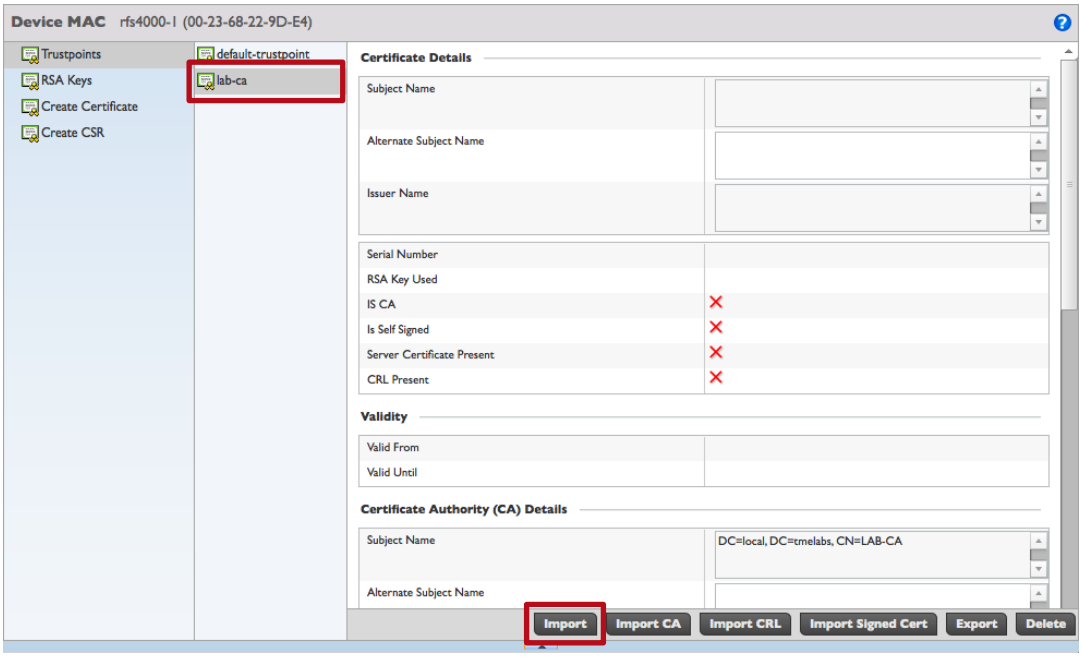
5 Select *Import Trustpoint*:



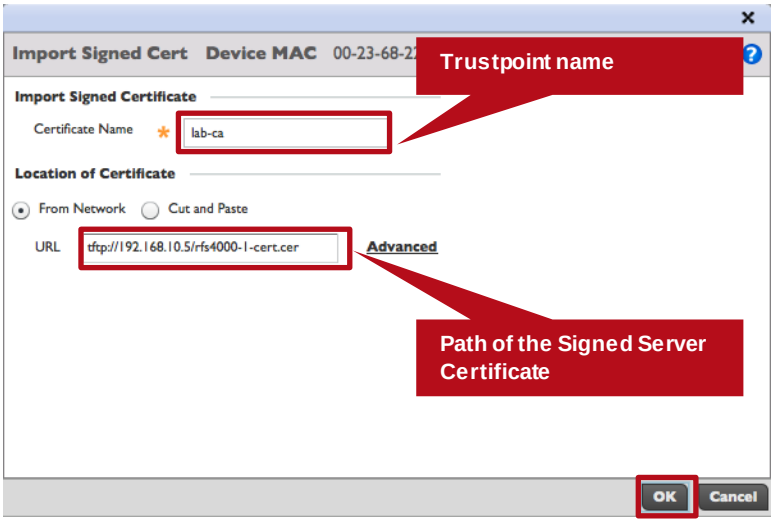
6 In the *Trustpoint Name* field enter the name of the Certificate Authority that signed the CSR. In the *URL* field enter the *Path* where the CAs root certificate can be imported from. In the below example a CA root certificate with the filename *lab-ca.cer* is imported into a new Trustpoint named *lab-ca* from the TFTP server with the IP address *192.168.10.5*. Click *OK*:



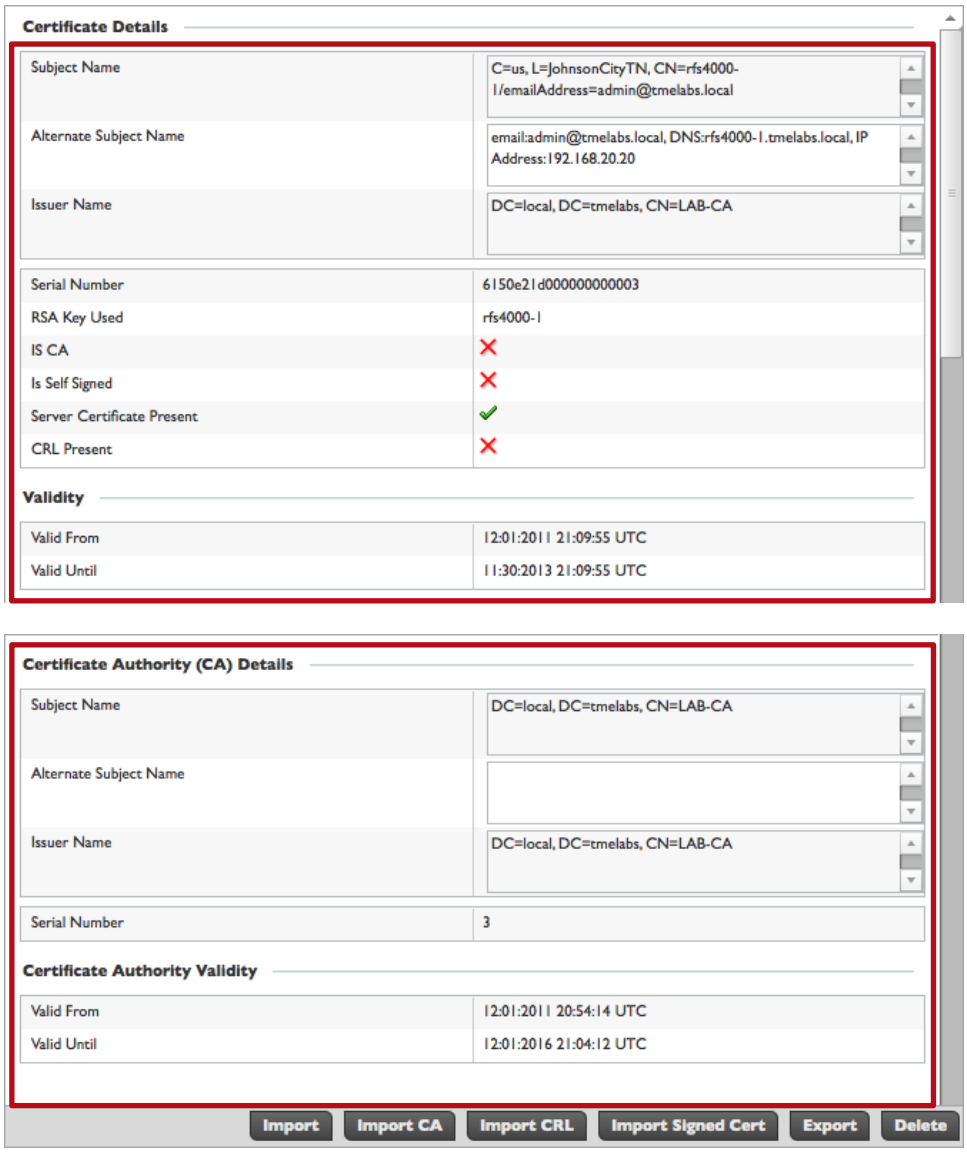
7 In the *Left* tree select the new *Trustpoint* name then click *Import*:



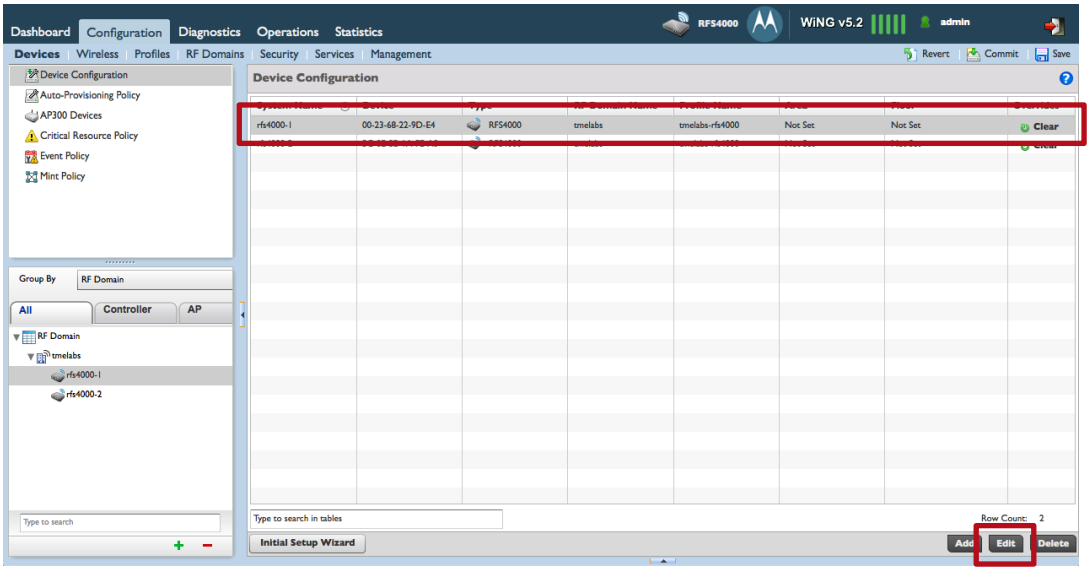
8 In the *Certificate Name* field enter the name of the Trustpoint created in the previous step. In the *URL* field enter the *Path* where the signed certificate can be imported from. In the below example the signed certificate with the filename *rfs4000-1-cert.cer* is imported into the Trustpoint named *lab-ca* from the TFTP server with the IP address *192.168.10.5*. Click *OK*:



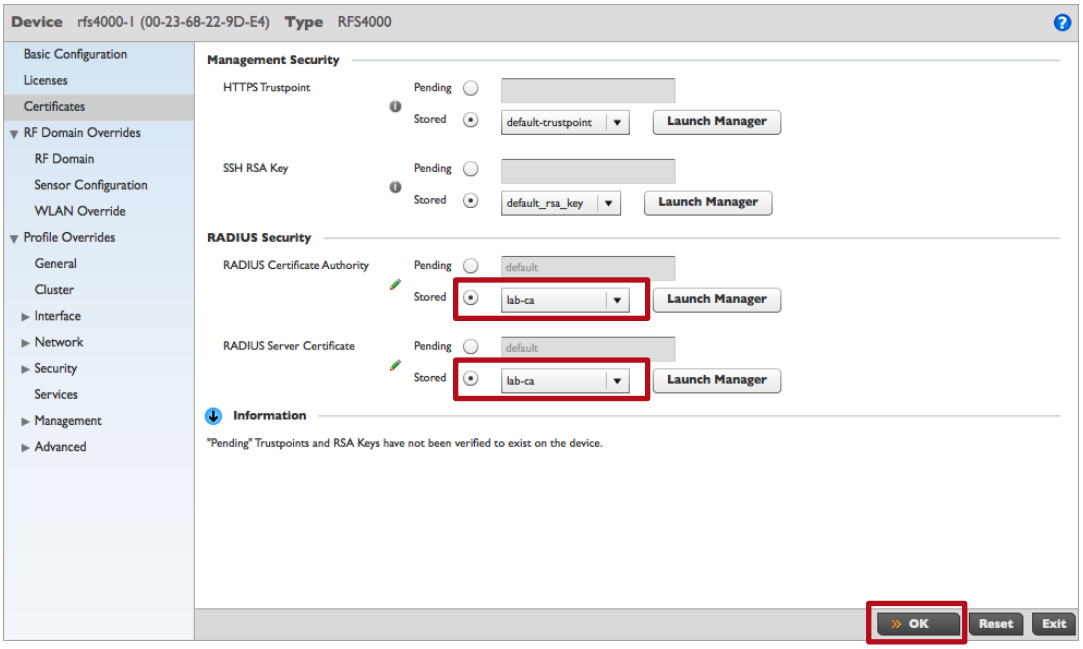
9 A *Root CA* certificate and signed *Server Certificate* have now been imported into a new Trustpoint:



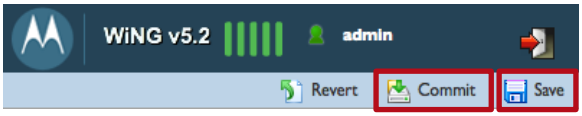
10 Select *Configuration* → *Devices* → *Controller-Name* → *Edit*:



11 Select *Certificates* then under *RADIUS Certificate Authority* and *RADIUS Server Certificate* select *Stored* then select the *Trustpoint* name created in the previous steps. Click *OK*:



12 *Commit* and Save the changes:



3.6.3 Resulting Configuration

```
!
rfs4000 00-23-68-22-9D-E4
use profile tmelabs-rfs4000
 use rf-domain tmelabs
 hostname rfs4000-1
 license AP DEFAULT-6AP-LICENSE
 trustpoint radius-ca lab-ca
 trustpoint radius-server lab-ca
 !
 ! Configuration Removed for Brevity
 !
!
```

3.7 RADIUS Server Policy Assignment

The RADIUS Server Policy can be assigned to individual Wireless Controllers or Independent Access Points as Overrides or to groups of devices using Profiles. For this configuration step the RADIUS Server Policy named ***internal-aaa*** created earlier will be assigned to a RFS4000 Profile named ***tmelabs-rfs4000*** which is assigned to both the RFS4000 Wireless Controllers providing RADIUS services.

3.7.1 Command Line Interface

The following procedure highlights how to assign a RADIUS Server Policy to a group of Wireless Controllers using the Command Line Interface (CLI):

1 Modifythe *Device Profile* of the *Wireless Controllers* and add the *RADIUS Server Policy* named *internal-aaa*. In this example a user defined *RFS4000 Profile* named *tmelabs-rfs4000* has been modified:

```
rfs4000-1(config)# profile rfs4000 tmelabs-rfs4000
rfs4000-1(config-profile-tmelabs-rfs4000)# use radius-server-policy internal-aaa
rfs4000-1(config-profile-tmelabs-rfs4000)# exit
```

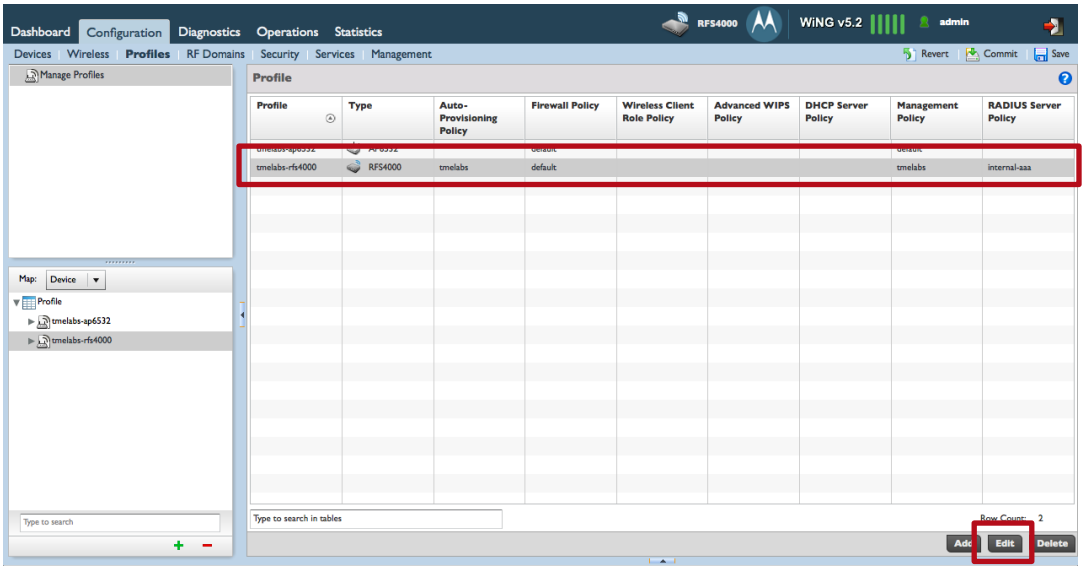
2 *Commit* and *Save* the changes:

```
rfs4000-1(config)# commit write
```

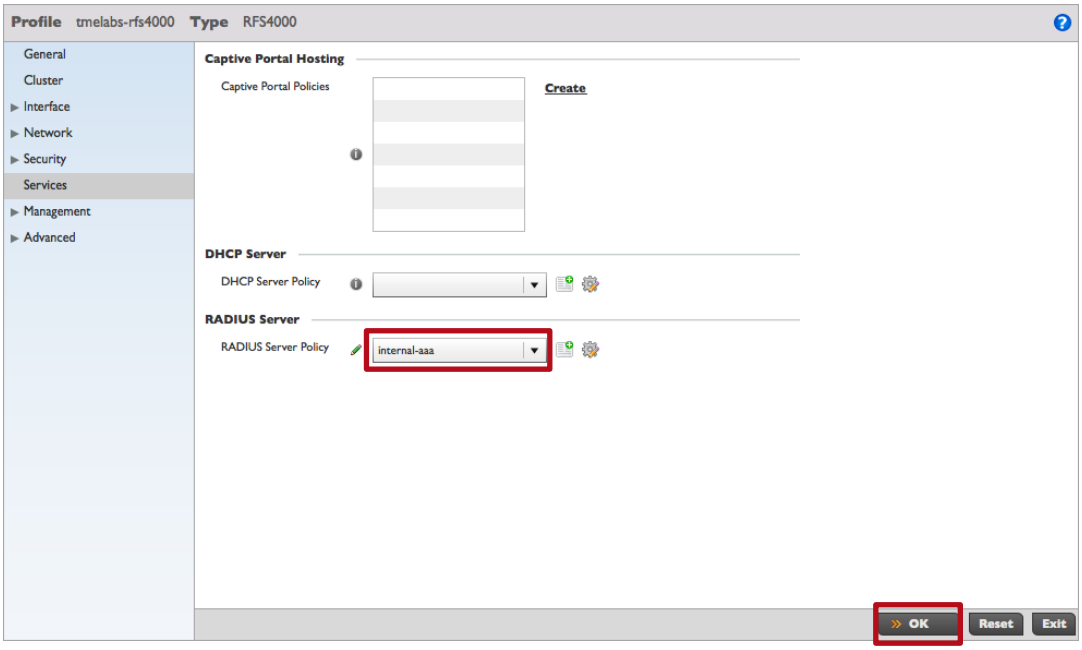
3.7.2 Web User Interface

The following procedure highlights how to assign a RADIUS Server Policy to a group of Wireless Controllers using the Web User Interface (Web UI):

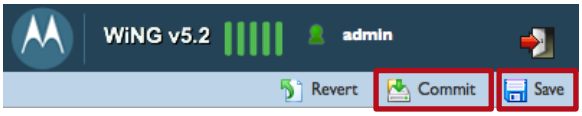
1 Select *Configuration* → *Profiles* → *Profile-Name* → *Edit*:



2 Select *Services* then assign the *RADIUS Server Policy* named *internal-aaa*. Click *OK*:



3 *Commit* and Save the changes:



3.7.3 Resulting Configuration

```
!
profile rfs4000 tmelabs-rfs4000
 ip name-server 192.168.10.5
 ip domain-name tmelabs.local
 no autoinstall configuration
 no autoinstall firmware
 use radius-server-policy internal-aaa
 !
 ! Configuration Removed for Brevity
 !
!
```

3.8 Wireless LAN Assignment

The 802.11i EAP Wireless LAN can be assigned to individual Access Point radios as Overrides or to groups of Access Point radios using Profiles. For this configuration step the ***TMELABS-DOT1X*** Wireless LAN will be assigned to both 2.4GHz and 5GHz radios using a user defined profile ***named tmelabs-ap6532*** which will be inherited by all the adopted Access Points.

3.8.1 Command Line Interface

The following procedure highlights how to assign the TMELABS-DOT1X Wireless LAN to groups of Access Point radios with Profiles using the Command Line Interface (CLI):

1 Modify the *Device Profile* of the *Access Points* and assign the Wireless LAN named TMELABS-DOT1X to the 2.4GHz and 5GHz radios. In this example a user defined AP6532 *Profile* named *tmelabs-ap6532* has been modified:

```
rfs4000-1(config)# profile ap6532 tmelabs-ap6532
rfs4000-1(config-profile-tmelabs-ap6532)# interface radio 1
rfs4000-1(config-profile-tmelabs-ap6532-if-radio1)# wlan TMELABS-DOT1X
rfs4000-1(config-profile-tmelabs-ap6532-if-radio1)# interface radio 2
rfs4000-1(config-profile-tmelabs-ap6532-if-radio2)# wlan TMELABS-DOT1X
rfs4000-1(config-profile-tmelabs-ap6532-if-radio2)# exit
rfs4000-1(config-profile-tmelabs-ap6532)# exit
```

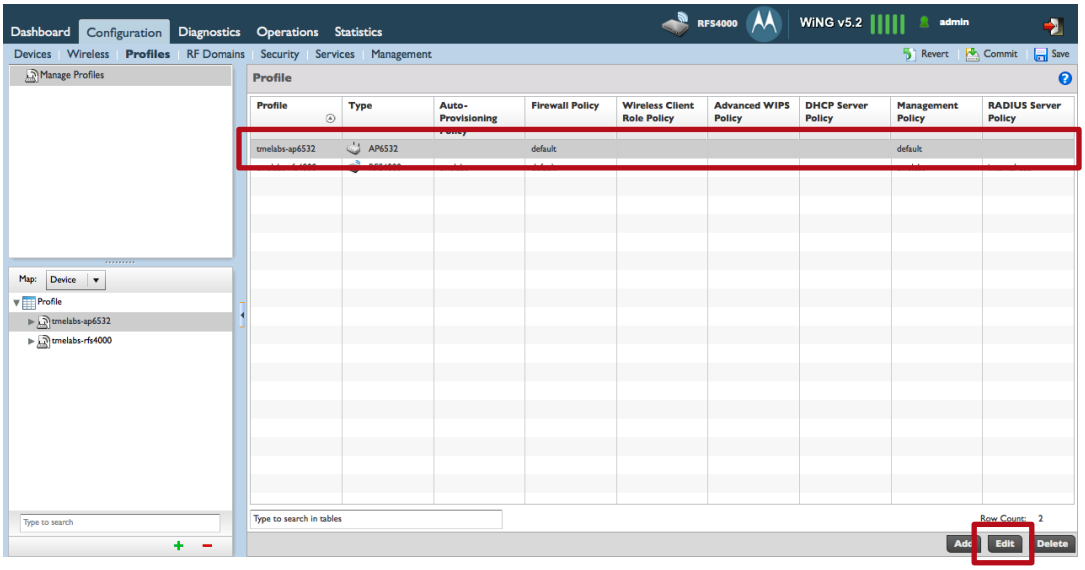
2 *Commit* and *Save* the changes:

```
rfs4000-1(config)# commit write
```

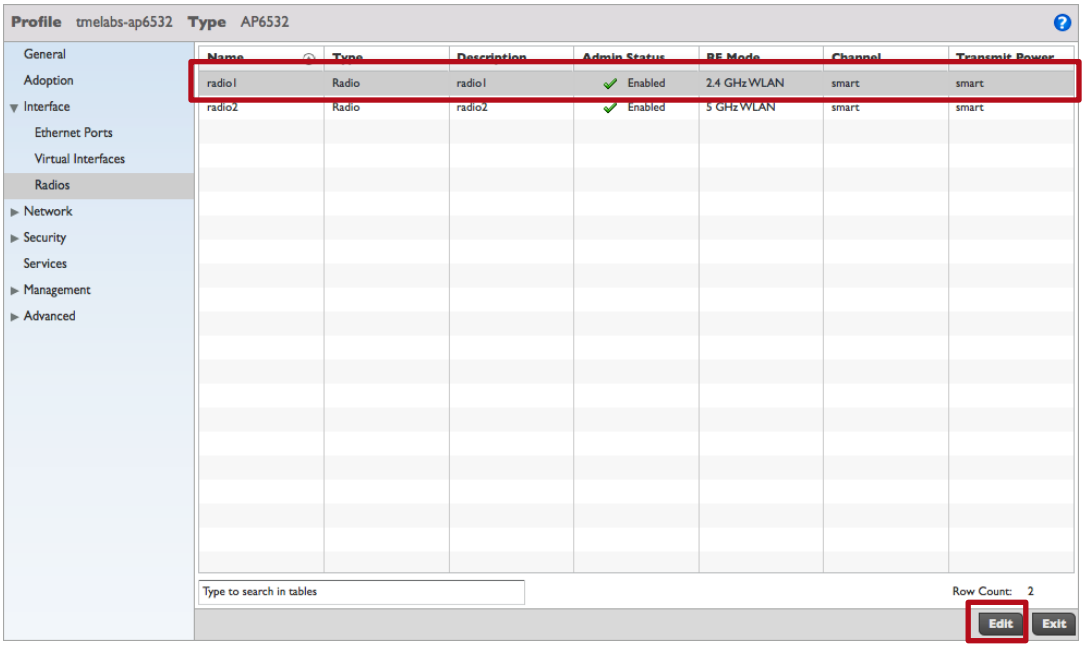
3.8.2 Web User Interface

The following procedure highlights how to assign the TMELABS-DOT1X Wireless LAN to groups of Access Point radios with Profiles using the Web User Interface (Web UI):

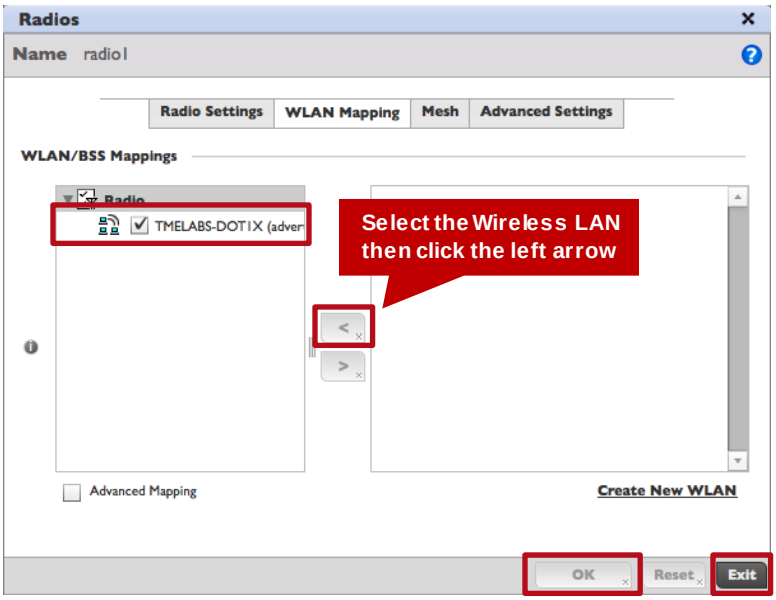
1 Select *Configuration* → *Profiles* → *Profile-Name* → *Edit*:



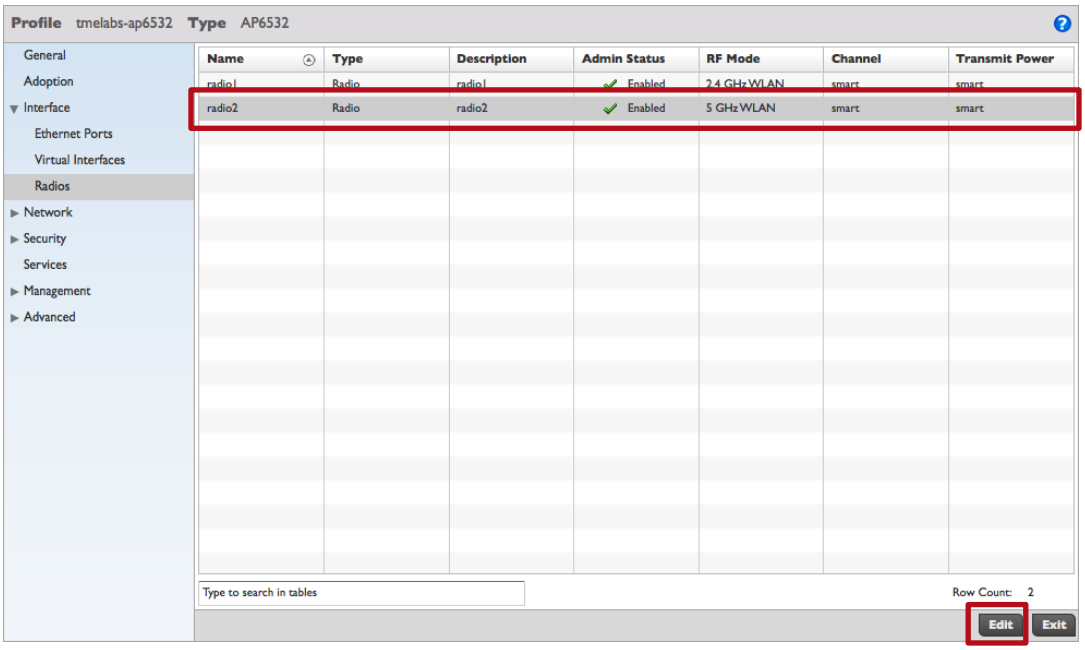
2 Select *Interface* → *Radios* → *radio1* → *Edit*:



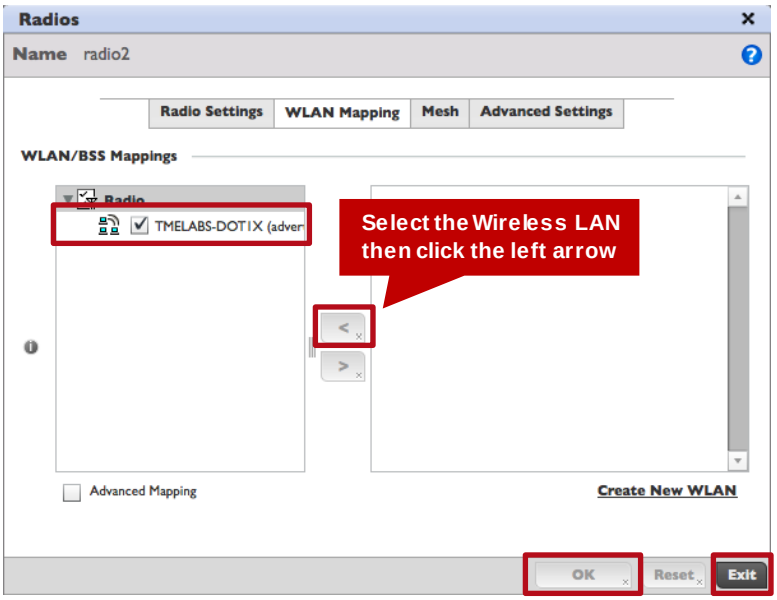
3 Select the 802.11i EAP Wireless LAN then click the *Left Arrow* to add the Wireless LAN to the Radio. Click *OK* then *Exit*:



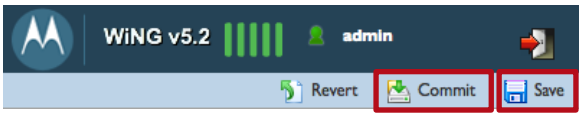
4 Select *Interface* → *Radios* → *radio2* → *Edit*:



5 Select the 802.11i EAP Wireless LAN then click the *Left Arrow* to add the Wireless LAN to the Radio. Click *OK* then *Exit*:



6 *Commit* and Save the changes:



3.8.3 Resulting Configuration

```
!
profile ap6532 tmelabs-ap6532
 ip name-server 192.168.10.5
 ip domain-name tmelabs.local
 no autoinstall configuration
 no autoinstall firmware
 interface radio1
  wlan TMELABS-DOT1X bss 1 primary
 interface radio2
  wlan TMELABS-DOT1X bss 1 primary
 !
 ! Configuration Removed for Brevity
 !
!
```

4. Verification / Troubleshooting

4.1 Verification Steps

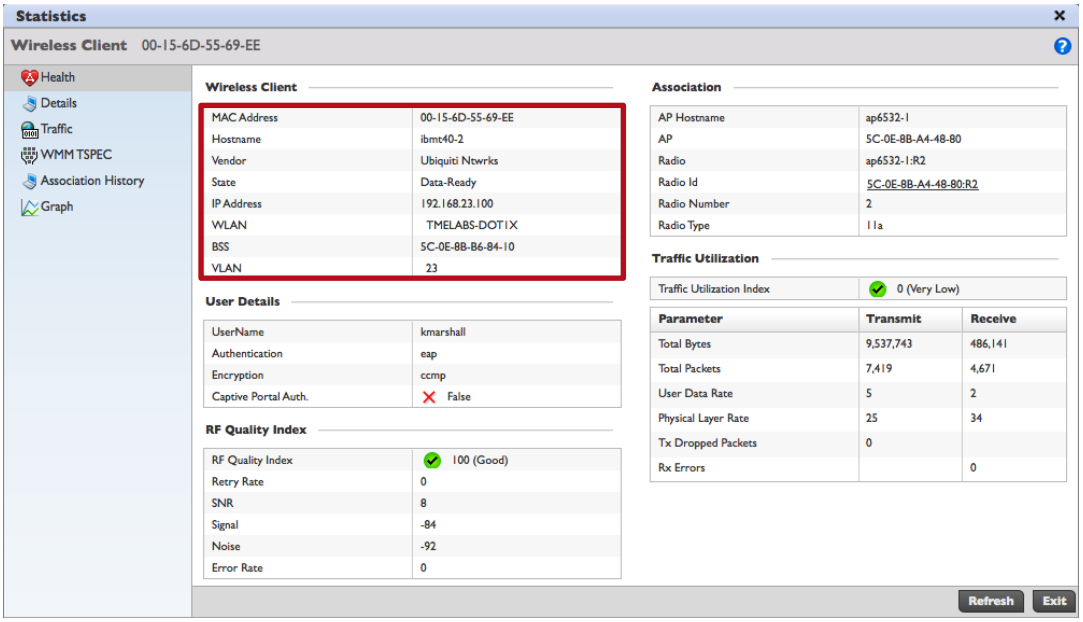
In this configuration example EAP users are authenticated against a back-end Active Directory user store and are authorized by matching an Active Directory group the user is a member of to a local group which has authorization attributes and dynamic VLAN membership defined. Upon successful EAP authentication and authorization an Active Directory user will be permitted access to the Wireless LAN and dynamically assigned to their designated VLAN.

1 Authenticate a Wireless Client using EAP-TTLS or EAP-GTC that's a member of the *Sales* group. The Wireless Client will be dynamically assigned to *VLAN 23* and will obtain an IP Address on its assigned VLAN:

```
rfs4000-1# show wireless client detail 00-15-6D-55-69-EE

  ADDRESS         : 00-15-6D-55-69-EE - 00-15-6D-55-69-EE  192.168.23.100 (vlan:23)
  USERNAME        : kmarshall
  WLAN            : TMELABS-DOT1X (ssid:TMELABS-DOT1X)
  ACCESS-POINT    : Name:ap6532-1 Location:JohnsonCityTN
  RADIO-ID        : 5C-0E-8B-A4-48-80:R2, alias ap6532-1:R2
  RADIO-NAME      : radio2 Bss:5C-0E-8B-B6-84-10
  STATE           : Data-Ready
  CLIENT-INFO     : 802.11a, vendor: Ubiquiti Ntwrks
  SECURITY        : Authentication: eap Encryption: ccmp
  DATA-RATES      : 6 9 12 18 24 36 48 54
  MAX-PHY_RATE    : 54.0 M
  MAX-USER_RATE   : 40.5 M
  QoS             : WMM: Y Type: Non Voice
  POWER-MGMT      : PS-Mode: N  Spatial-Multiplexing-PS: off WMM-PS/U-APSD: Disabled
  ACTIVITY        : Last Active: 00:00.00 ago
  SESSION INFO    : Session Timeout:   0 days 01:00.00  Idle Timeout: 00.:30.00
  RF-DOMAIN       : tmelabs
  MCAST STREAMS   :
```

Statistics → System → RF-Domain → Wireless Clients → Client-MAC-Address

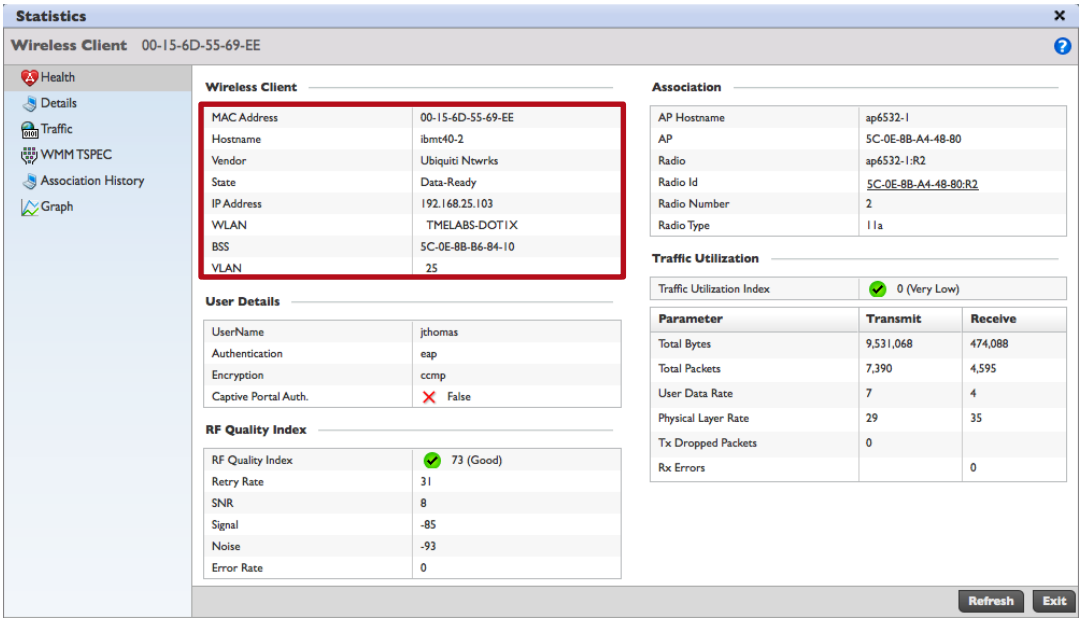


2 Authenticate a Wireless Client using EAP-TTLS or EAP-GTC that's a member of the *Marketing* group. The Wireless Client will be dynamically assigned to *VLAN 24* and will obtain an IP Address on its assigned VLAN:

```
rfs4000-1# show wireless client detail 00-15-6D-55-69-EE

  ADDRESS          : 00-15-6D-55-69-EE - 00-15-6D-55-69-EE  192.168.24.100 (vlan:24)
  USERNAME         : jsellin
  WLAN             : TMELABS-DOT1X (ssid:TMELABS-DOT1X)
  ACCESS-POINT     : Name:ap6532-1 Location:JohnsonCityTN
  RADIO-ID         : 5C-0E-8B-A4-48-80:R2, alias ap6532-1:R2
  RADIO-NAME       : radio2 Bss:5C-0E-8B-B6-84-10
  STATE            : Data-Ready
  CLIENT-INFO      : 802.11a, vendor: Ubiquiti Ntwrks
  SECURITY         : Authentication: eap Encryption: ccmp
  DATA-RATES       : 6 9 12 18 24 36 48 54
  MAX-PHY_RATE     : 54.0 M
  MAX-USER_RATE    : 40.5 M
  QoS              : WMM: Y Type: Non Voice
  POWER-MGMT       : PS-Mode: N  Spatial-Multiplexing-PS: off WMM-PS/U-APSD: Disabled
  ACTIVITY         : Last Active: 00:00.00 ago
  SESSION INFO     : Session Timeout:   0 days 01:00.00  Idle Timeout: 00.:30.00
  RF-DOMAIN        : tmelabs
  MCAST STREAMS    :
```

Statistics → System → RF-Domain → Wireless Clients → Client-MAC-Address

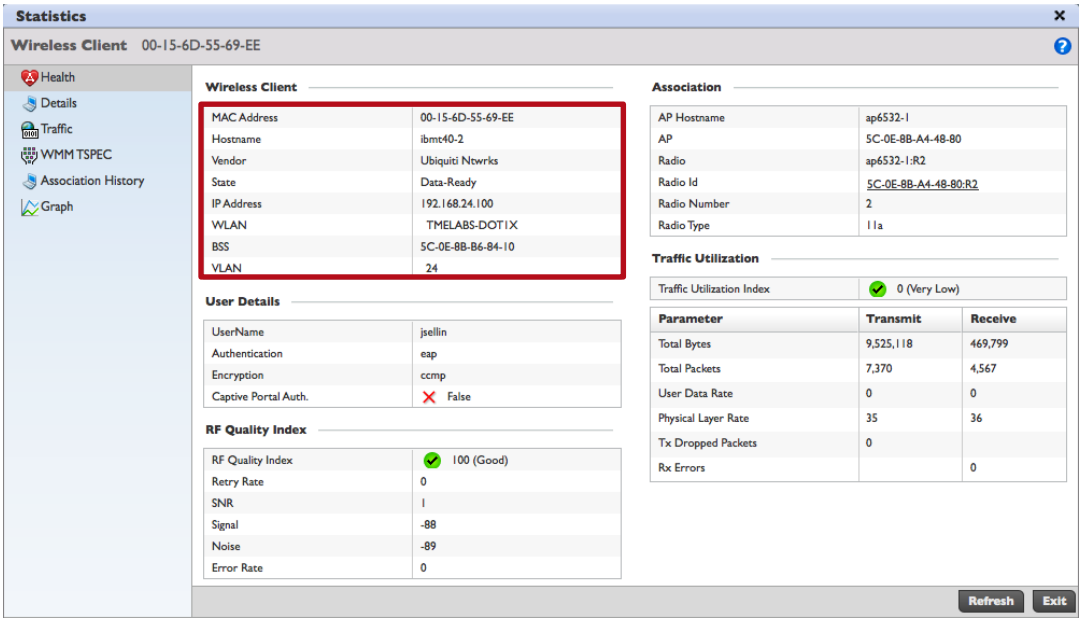


3 Authenticate a Wireless Client using EAP-TTLS or EAP-GTC that's a member of the *Engineering* group. The Wireless Client will be dynamically assigned to *VLAN 25* and will obtain an IP Address on its assigned VLAN:

```
rfs4000-1# show wireless client detail 00-15-6D-55-69-EE

  ADDRESS          : 00-15-6D-55-69-EE - 00-15-6D-55-69-EE  192.168.25.103 (vlan:25)
  USERNAME         : jthomas
  WLAN             : TMELABS-DOT1X (ssid:TMELABS-DOT1X)
  ACCESS-POINT     : Name:ap6532-1 Location:JohnsonCityTN
  RADIO-ID         : 5C-0E-8B-A4-48-80:R2, alias ap6532-1:R2
  RADIO-NAME       : radio2 Bss:5C-0E-8B-B6-84-10
  STATE            : Data-Ready
  CLIENT-INFO      : 802.11a, vendor: Ubiquiti Ntwrks
  SECURITY         : Authentication: eap Encryption: ccmp
  DATA-RATES       : 6 9 12 18 24 36 48 54
  MAX-PHY_RATE     : 54.0 M
  MAX-USER_RATE    : 40.5 M
  QoS              : WMM: Y Type: Non Voice
  POWER-MGMT       : PS-Mode: N  Spatial-Multiplexing-PS: off WMM-PS/U-APSD: Disabled
  ACTIVITY         : Last Active: 00:00.00 ago
  SESSION INFO     : Session Timeout:   0 days 01:00.00  Idle Timeout: 00.:30.00
  RF-DOMAIN        : tmelabs
  MCAST STREAMS    :
```

Statistics → System → RF-Domain → Wireless Clients → Client-MAC-Address



4.2 Troubleshooting

The following section provides a list of common issues and resolutions when authenticating Wireless Clients against Microsoft Active Directory.

4.2.1 Bind User Issues

The most common issue when authenticating against Active Directory is an invalid Bind User account name and password. When a ***bindRequest*** is received by the Domain Controller with an invalid Name or Password, the Domain Controller will respond with a ***bindResponse*** message with ***invalidCredentials*** (figure 4.2.1.1 packet 23). This message indicates that the Wireless Controller or Independent Access Point is unable to bind with the Active Directory Domain Controller:

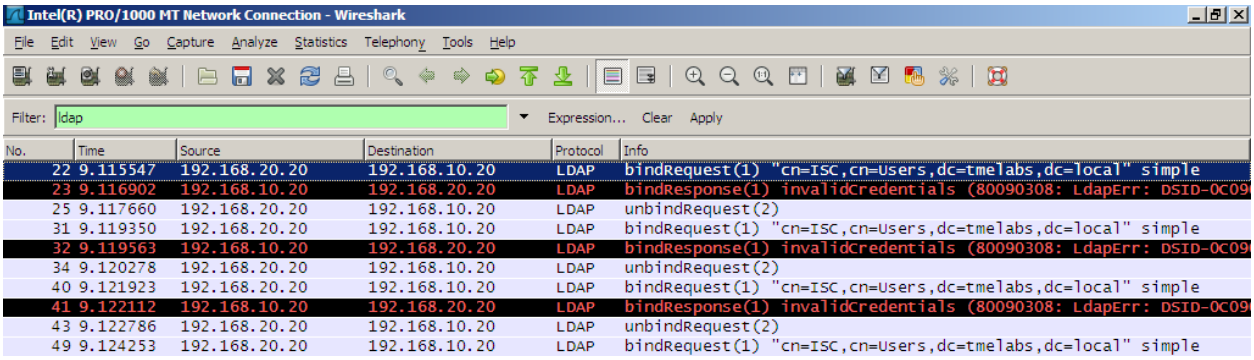


Figure 4.2.1.1 – Invalid Bind User or Credentials

Some common causes of a failed bind request include:

Potential Issue	Resolution
IP routing issues between the Wireless Controller and the Active Directory Domain Controller.	Verify that the Wireless Controller can ping the Active Directory Domain Controller and vice versa. If the ping is unsuccessful verify the Wireless Controller has the appropriate default route or static routes defined.
A Firewall is deployed between the Wireless Controller and Active Directory Domain Controller.	If a firewall is deployed between the Wireless Controller and Domain Controller verify that a firewall rule is present that permits TCP destination port 389.
Incorrect Active Directory Domain Controller server IP address configuration on Wireless Controller.	Verify that the IP address of the Active Directory Domain Controller is correct. This is a very common configuration error when implementing LDAP authentication especially in large Active Directory environments.
Incorrect Bind DN configuration on the Wireless Controller.	The Bind DN configuration will vary depending on where the Bind User account is created in the Active Directory tree. For smaller environments the Bind DN will typically be located in the default Users container such as *cn=username,cn=Users,dc=example,dc=com* where the Users container is designated as a Common Name (CN). However in larger Active Directory environments the Bind User account will typically be located in an Organization Unit (OU). One common configuration error is to designate the OU as a CN. For example the Wireless

	Controller administrator may incorrectly enter *cn=username,cn=US,dc=example,dc=com* where the correct Bind DN would be *cn=username,ou=US,dc=example,dc=com*. When entering the Bind DN is very important to know exactly where in the Active Directory tree and what type of container (i.e. CN or OU) the Bind User account is located.
Incorrect Bind Username in the Active Directory Domain Controller.	Verify the Active Directory name is correct for the Bind User account. A common configuration error is to populate the *First name*, *Last name* and *Initials* for the Bind User account in Active Directory. For a successful bind it is recommended that you only populate the *First name* field. If the Bind User account includes a *Last name* or *Initials*, rename the Bind User account so that only the First name is displayed in the Name field.
Incorrect Bind Password on the Wireless Controller or Active Directory Domain Controller.	The Bind User account requires special configuration within Active Directory as the Bind Request uses PAP authentication. If the Bind User is unable to authenticate with Active Directory there are several things that can be checked: 1. Verify that the Bind User account is not locked. Based on policy Active Directory may lock an account for inactivity or invalid password attempts. 2. Verify that the Bind User account has the Account options *Password Never Expires* and *Store password using reversible encryption* options enabled. 3. Re-synchronize the Bind Users passwords in both the Active Directory and the WLAN Switch Controller.
Insufficient Permissions	Verify that the Bind User account is a member of the *Domain Users* group. The Bind User must have adequate permissions to Bind to the Active Directory tree, authenticate users and search the tree.

A successful ***bindRequest*** will result in a ***bindResponse*** message with ***success*** (figure 4.2.1.2 packet 27). This message indicates that the Wireless Controller or Independent Access Point is able to bind with the Active Directory Domain Controller:

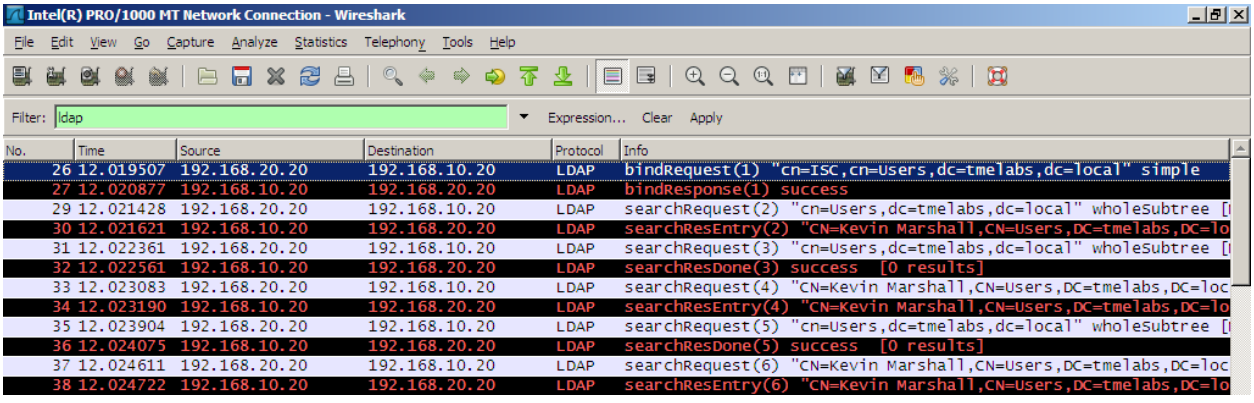


Figure 4.2.1.2 – Valid Bind User & Credentials

4.2.2 Base DN

The Base DN designates where in the Active Directory Tree the Wireless Controller or Independent Access Point searches for users and groups. Once a Base DN has been defined, the Wireless Controller or Independent Access Point will search the Active Directory tree for users and group from the Base DN and down. This includes all containers and sub-containers.

Using Figure 4.2.2.1 as an example, if the Base DN is set to ***ou=MotorolaSolutions,dc=example,dc=com*** the Wireless Controller or Independent Access Point will search for users and groups in the ***MotorolaSolutions***, ***APAC***, ***CALA***, ***EMEA*** and ***NA*** containers. The Wireless Controller or Independent Access Point will not however search the ***Motorola*** container as this container is at the same level as the ***MotorolaSolutions*** container.

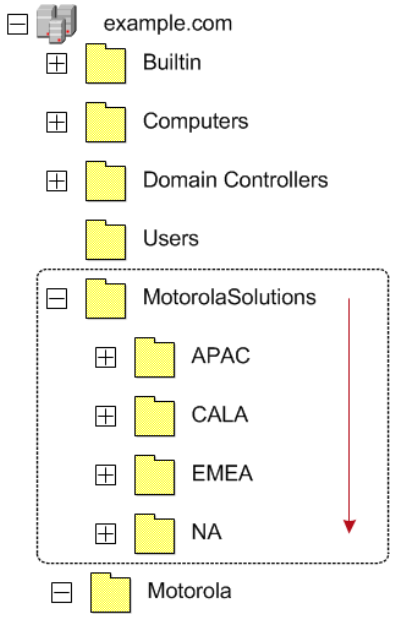


Figure 4.2.2.1 – Active Directory Tree Example

The most common issue when defining a Base DN with Active Directory is substituting a ***Common Name*** (CN) for an ***Organizational Unit*** (OU). In Microsoft Active Directory the default ***Users*** container is a ***CN*** while additional containers are ***OUs***. Designating a CN as an OU (or vice versa) will result in a LDAP ***searchDone*** response ***noSuchObject*** message (figure 4.2.2.2 packet 12):

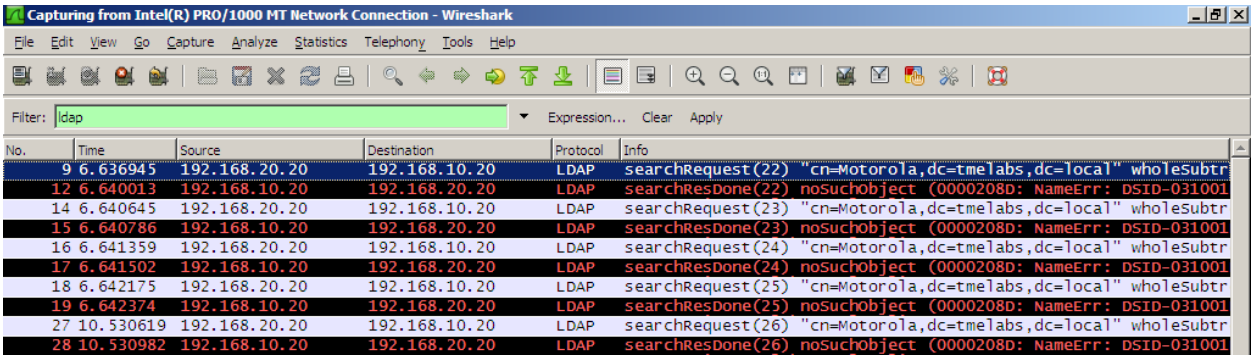


Figure 4.2.2.2 – Invalid Base DN

If the Base DN is valid but the User cannot be located in the current or lower containers, the Active Directory Domain Controller will response with a LDAP ***searchResDone*** message with ***[0 results]*** (figure 4.2.2.3 packet 49):

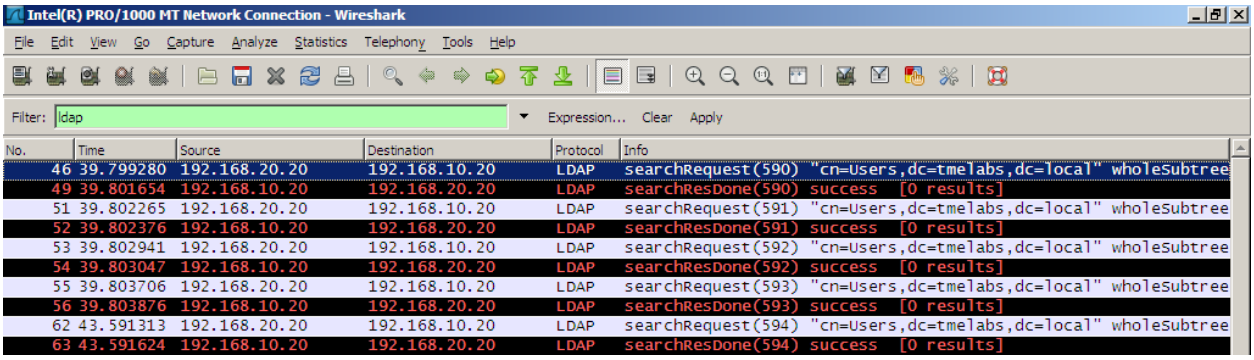


Figure 4.2.2.3 – Valid Base DN no User Match

A successful search will result in a ***searchResEntry*** response with the fully distinguished name of the authenticating user (figure 4.2.2.4 packet 16):

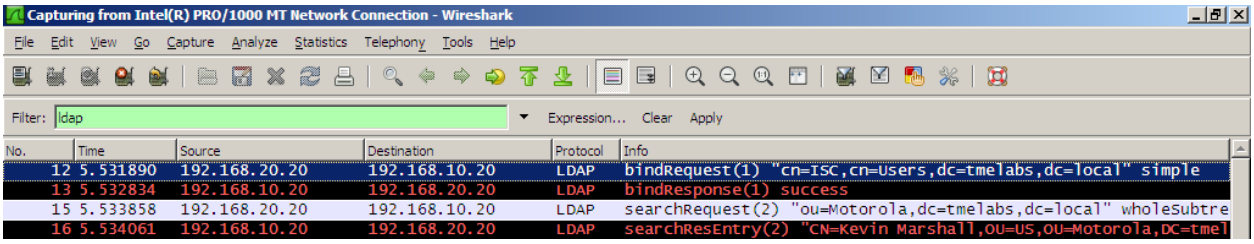


Figure 4.2.2.4 – Valid Base DN and User Match

4.2.3 LDAP Group Verification

Once an Active Directory user has been successfully authenticated, the Wireless Controller or Independent Access Point will perform authorization to verify that the authenticated user has permissions to access the Wireless LAN. The Wireless Controller or Independent Access Point will search the group membership of the Active Directory user and match one of the returned groups to a local group defined on the Wireless Controller or Independent Access Point. If a group cannot be matched, the user will fail authorization and will be denied access to the Wireless LAN.

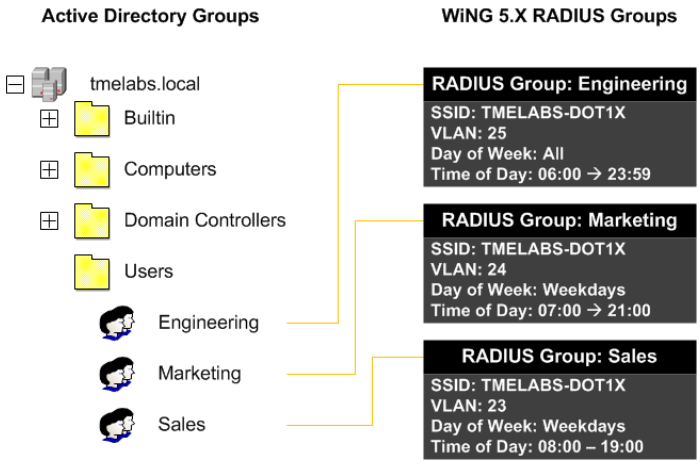


Figure 4.2.3.1 – LDAP Group Verification

Some common causes of a failed authorization include:

Potential Issue	Resolution
No group association.	Verify that the Active Directory groups have been defined on the Wireless Controller or Independent Access Point that matches the group names defined in Active Directory. For example if an Active Directory user is a member of the Active Directory group *Sales*, a local group called *Sales* will need to be created on the Wireless Controller or Independent Access Point.
No WLANs assigned to the local group on the WLAN Switch Controller.	Verify that the local group permits access to the appropriate Wireless LANs. For example if *Sales* users are permitted access to a Wireless LAN using the SSID *Corp*, the SSID *Corp* needs to be specifically added to the *Sales* group.
Authorization failure due to policies.	Each local group can be assigned policies that include Time of Day and Day of Week access. During authorization the Wireless Controller or Independent Access Point will compare the groups Time of Day and Day of Week permissions against the current time and date on the WLAN Switch Controller. If the group policy configuration is correct and authorization fails: 1. Verify the time-zone configuration is correctly defined in the RF Domain. 2. Verify that NTP has been enabled in the Wireless Controller and Access Point Profiles and the time is synchronized. When implementing Time and Day based policies it is recommended that the date and time be synchronized using NTP.

5. Appendix

5.1 Running Configuration

The following is the running configuration from the RFS4000 Wireless Controllers used in this guide:

```
!### show running-config
!
! Configuration of RFS4000 version 5.2.0.0-069R
!
!
version 2.1
!
!
firewall-policy default
 no ip dos tcp-sequence-past-window
!
igmp-snoop-policy default
 no igmp-snooping
 no querier
 unknown-multicast-fwd
!
!
mint-policy global-default
!
wlan-qos-policy default
 qos trust dscp
 qos trust wmm
!
radio-qos-policy default
!
aaa-policy internal-aaa
 authentication server 1 onboard controller
!
wlan TMELABS-DOT1X
 ssid TMELABS-DOT1X
 vlan 23
 bridging-mode tunnel
 encryption-type ccmp
 authentication-type eap
 wireless-client reauthentication 3600
 radius vlan-assignment
 use aaa-policy internal-aaa
```

```
!
auto-provisioning-policy tmelabs
 adopt ap6532 precedence 1 profile tmelabs-ap6532 rf-domain tmelabs ip 192.168.21.0/24
!
radius-group Engineering
 policy vlan 25
 policy ssid TMELABS-DOT1X
 policy day mo
 policy day tu
 policy day we
 policy day th
 policy day fr
 policy day sa
 policy day su
 policy time start 06:00 end 23:59
!
radius-group Marketing
 policy vlan 24
 policy ssid TMELABS-DOT1X
 policy day mo
 policy day tu
 policy day we
 policy day th
 policy day fr
 policy time start 07:00 end 21:59
!
radius-group Sales
 policy vlan 23
 policy ssid TMELABS-DOT1X
 policy day mo
 policy day tu
 policy day we
 policy day th
 policy day fr
 policy time start 08:00 end 19:59
!
radius-server-policy internal-aaa
 authentication data-source ldap
 ldap-server primary host 192.168.10.20 port 389 login (sAMAccountName=%{Stripped-User-Name:-
%{User-Name}}) bind-dn cn=ISC,cn=Users,dc=tmelabs,dc=local base-dn cn=Users,dc=tmelabs,dc=local
passwd 0 L0gic.L1ve passwd-attr UserPassword group-attr cn group-filter
(|(&(objectClass=group)(member=%{Ldap-
UserDn}))(&(objectClass=GroupOfUniqueNames)(uniquemember=%{Ldap-userDn}))) group-membership
radiusGroupName net-timeout 10
```

```
 use radius-group Sales
 use radius-group Marketing
 use radius-group Engineering
!
!
management-policy default
 no http server
 https server
 ssh
 user admin password 1 d22e848f0a3906708fca58246ce4ed0613bc4bf76d7c576b99bf865ca875976f role
superuser access all
 user operator password 1 41c68faf0d70180c97ff3ccd42362a3e1a42dc4b7019669c0bf12c1a18ca607c role
monitor access all
 no snmp-server manager v2
 snmp-server community public ro
 snmp-server user snmpoperator v3 encrypted des auth md5 0 operator
 snmp-server user snmptrap v3 encrypted des auth md5 0 motorola
 snmp-server user snmpmanager v3 encrypted des auth md5 0 motorola
!
management-policy tmelabs
 no http server
 https server
 ssh
 user admin password 1 9c5d73dc29b7e68306ef5e17e341250c992083440d181d1c34e8c006a2daa6ea role
superuser access all
!
profile rfs4000 tmelabs-rfs4000
 bridge vlan 23
  bridging-mode tunnel
  ip igmp snooping
  ip igmp snooping querier
 bridge vlan 24
  bridging-mode tunnel
  ip igmp snooping
  ip igmp snooping querier
 bridge vlan 25
  bridging-mode tunnel
  ip igmp snooping
  ip igmp snooping querier
 ip name-server 192.168.10.5
 ip domain-name tmelabs.local
 no autoinstall configuration
 no autoinstall firmware
 use radius-server-policy internal-aaa
```

```
 crypto isakmp policy default
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 interface radio1
 interface radio2
 interface up1
  description Uplink
  switchport mode trunk
  switchport trunk native vlan 20
  switchport trunk native tagged
  switchport trunk allowed vlan 20,23-25
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge1
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge2
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge3
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge4
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge5
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface wwan1
 use management-policy tmelabs
 use firewall-policy default
 use auto-provisioning-policy tmelabs
 ntp server 192.168.10.5
 no auto-learn-staging-config
 service pm sys-restart
!
profile ap6532 tmelabs-ap6532
```

```
 bridge vlan 23
  bridging-mode tunnel
  ip igmp snooping
  ip igmp snooping querier
 bridge vlan 24
  bridging-mode tunnel
  ip igmp snooping
  ip igmp snooping querier
 bridge vlan 25
  bridging-mode tunnel
  ip igmp snooping
  ip igmp snooping querier
 ip name-server 192.168.10.5
 ip domain-name tmelabs.local
 no autoinstall configuration
 no autoinstall firmware
 interface radio1
  wlan TMELABS-DOT1X bss 1 primary
 interface radio2
  wlan TMELABS-DOT1X bss 1 primary
 interface ge1
  switchport mode trunk
  switchport trunk native vlan 21
  no switchport trunk native tagged
  switchport trunk allowed vlan 21-22
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface vlan21
  ip address dhcp
  ip dhcp client request options all
 use firewall-policy default
 ntp server 192.168.10.5
 service pm sys-restart
!
rf-domain default
 no country-code
!
rf-domain tmelabs
 location JohnsonCityTN
 contact kmarshall@motorolasolutions.com
 timezone EST5EDT
```

```
 country-code us
!
rfs4000 00-23-68-22-9D-E4
 use profile tmelabs-rfs4000
 use rf-domain tmelabs
 hostname rfs4000-1
 license AP DEFAULT-6AP-LICENSE
 trustpoint radius-ca lab-ca
 trustpoint radius-server lab-ca
 ip default-gateway 192.168.20.1
 interface vlan20
  ip address 192.168.20.20/24
 cluster name tmelabs
 cluster member ip 192.168.20.21
 cluster master-priority 255
 logging on
 logging console warnings
 logging buffered warnings
!
rfs4000 5C-0E-8B-1A-FE-A0
 use profile tmelabs-rfs4000
 use rf-domain tmelabs
 hostname rfs4000-2
 license AP DEFAULT-6AP-LICENSE
 trustpoint radius-ca tme-lab
 trustpoint radius-server tme-lab
 ip default-gateway 192.168.20.1
 interface vlan20
  ip address 192.168.20.21/24
 cluster name tmelabs
 cluster member ip 192.168.20.20
 logging on
 logging console warnings
 logging buffered warnings
!
ap6532 5C-0E-8B-A4-48-80
 use profile tmelabs-ap6532
 use rf-domain tmelabs
 hostname ap6532-1
!
ap6532 5C-0E-8B-A4-4B-48
 use profile tmelabs-ap6532
```

```
 use rf-domain tmelabs
 hostname ap6532-2
!
ap6532 5C-0E-8B-A4-4C-3C
 use profile tmelabs-ap6532
 use rf-domain tmelabs
 hostname ap6532-3
!
!
end
```


MOTOROLA SOLUTIONS