

# Dynamic VLAN Assignment with WLCs based on ACS to Active Directory Group Mapping Configuration Example

Document ID: 99121

## Contents

### Introduction

#### Prerequisites

- Requirements
- Components Used
- Conventions

#### Background Information

- ACS Restrictions on Group Mapping with Windows User Database

#### Configure

- Network Diagram
- Configuration Setup

#### Configure Active Directory and Windows User Database

- Configure the Server in Your Network as the Domain Controller
- Create Active Directory Users and Groups in the Domain
- Add ACS Server as the Member of the Domain

#### Configure the Cisco Secure ACS

- Configure the ACS for Windows User Database Authentication and Group Mapping
- Configure ACS for Dynamic VLAN Assignment

#### Configure the Wireless LAN Controller

- Configure the WLC with Details of the Authentication Server
- Configure the Dynamic Interfaces (VLANs) on the WLC
- Configure the WLANs (SSID)

#### Configure the Wireless Client

#### Verify

#### Troubleshoot

- Troubleshooting Commands

#### Related Information

## Introduction

This document explains how to authenticate the wireless client using Microsoft® Windows Active Directory (AD) database, how to configure group mapping between the AD group and Cisco Secure Access Control Server (ACS) group, and how to assign the authenticated client dynamically to a VLAN configured on the mapped ACS group. This document focuses on AD group mapping only with the ACS software product and not with the ACS Solution Engine.

## Prerequisites

### Requirements

Ensure that you meet these requirements before you attempt this configuration:

- Have basic knowledge of Wireless LAN Controllers (WLCs) and Lightweight Access Points (LAPs)

- Have functional knowledge of Cisco Secure ACS
- Have thorough knowledge of wireless networks and wireless security issues
- Have functional and configurable knowledge on dynamic VLAN assignment

Refer to Dynamic VLAN Assignment for more information.

- Have basic understanding of Microsoft Windows AD services, as well as domain controller and DNS concepts
- Have basic knowledge of Lightweight AP Protocol (LWAPP)

## Components Used

The information in this document is based on these software and hardware versions:

- Cisco 2000 Series WLC that runs firmware release 4.0.217.0
- Cisco 1000 Series LAP Cisco 802.11a/b/g
- Wireless Client Adapter that runs firmware release 3.6
- Cisco Aironet Desktop Utility (ADU) that runs version 3.6
- Cisco Secure ACS that runs version 4.1
- Microsoft Windows 2003 Server configured as a domain controller
- Cisco 2950 Series Switch that runs version 12.1

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

## Background Information

Cisco Secure ACS Release 4.1 for Windows authenticates wireless users against one of several possible databases, which includes its internal database. You can configure ACS to authenticate users with more than one type of database. You can configure the ACS to forward authentication of users to one or more external user databases. Support for external user databases means that the ACS does not require you to create duplicate user entries in the user database.

Wireless users can be authenticated by using several external databases such as:

- Windows Database
- Novell NetWare Directory Services (NDS)
- Generic Lightweight Directory Access Protocol (LDAP)
- Open Database Connectivity (ODBC)–compliant relational databases
- LEAP Proxy Remote Access Dial–In User Service (RADIUS) servers
- Rivest, Shamir, and Adelman (RSA) SecurID token servers
- RADIUS–compliant token servers

The ACS Authentication and User Database Compatibility tables list the various authentication protocols supported by the ACS internal and external databases.

This document focuses on authenticating wireless users that use Windows external database.

You can configure the ACS to authenticate users with the external user database in one of two ways:

- **By Specific User Assignment** You can configure the ACS to authenticate specific users with an external user database. In order to do this, the user must exist in the ACS internal database and you must set the Password Authentication list in User Setup to the external user database that the ACS should use to authenticate the user.
- **By Unknown User Policy** You can configure the ACS to attempt authentication of users who are not in the ACS internal database by using an external user database. You do not need to define new users in the ACS internal database for this method.

This document focuses on authenticating wireless users using the Unknown User Policy method.

When the ACS attempts to authenticate the user against Windows database, the ACS forwards user credentials to the Windows database. The Windows database validates the user credentials, and upon successful authentication, informs the ACS.

After successful authentication, the ACS gathers the group information of this user from the Windows database. After receiving this group information, the ACS associates the users of the gathered Windows database group information with the corresponding mapped ACS group for the purpose of assigning dynamic VLANs to the wireless client. In short, the ACS can be configured to map the Windows database to an ACS group and assign the authenticated user dynamically to a VLAN configured in the mapped ACS group.

Also, after the first successful authentication, the user is dynamically created on the ACS. Once the user is successfully authenticated for the first time, the user is cached in the ACS with a pointer to its database. This avoids the ACS from searching the entire database list during subsequent authentication attempts.

## **ACS Restrictions on Group Mapping with Windows User Database**

ACS has these limits on group mapping for users who are authenticated by a Windows user database:

- ACS can only support group mapping for users who belong to 500 or fewer Windows groups.
- ACS can only perform group mapping by using the local and global groups to which a user belongs in the domain that authenticated the user.

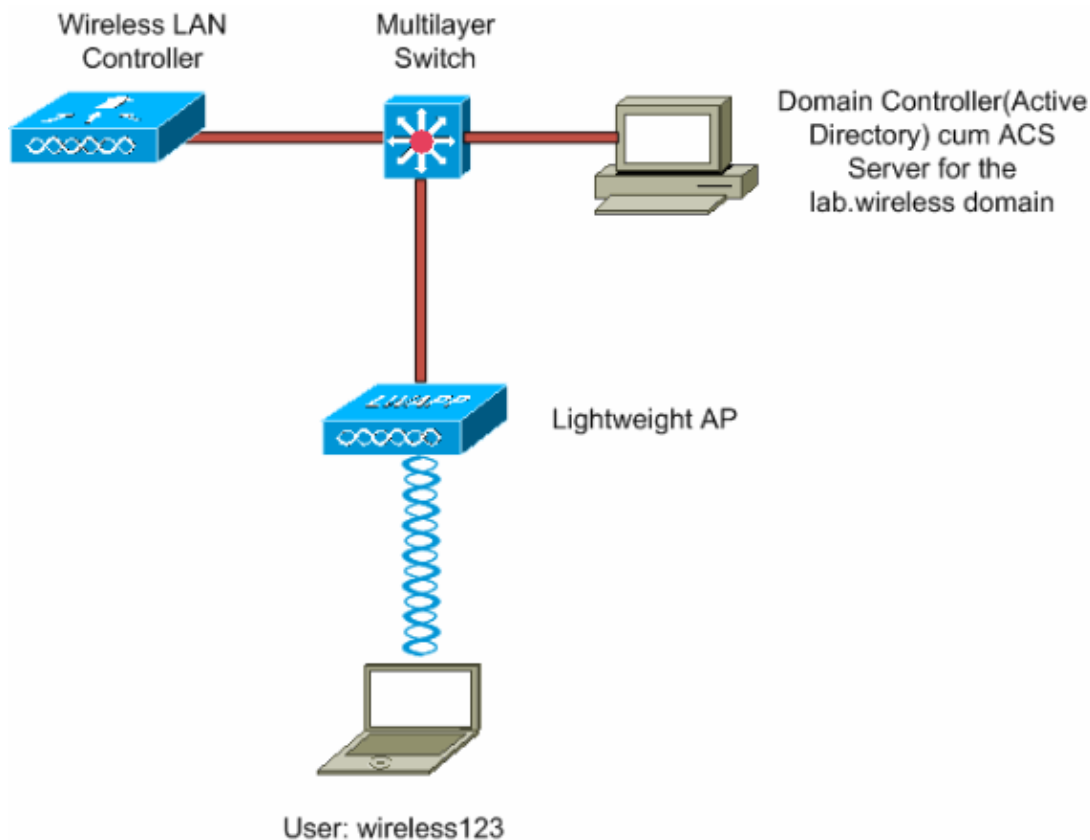
## **Configure**

In this example, you are configured on the Windows AD and mapped to a particular AD group. Cisco Secure ACS is configured to use the external database on Windows AD for authenticating wireless clients. Then, the AD is then mapped to the ACS group for authenticated users thereby assigning the user of that particular AD group to a VLAN specified in the corresponding mapped ACS group.

The next section explains how to configure the devices for this.

## **Network Diagram**

This document uses this network setup:



## Configuration Setup

This document uses these configurations:

- Microsoft Windows Domain Name: **lab.wireless**
- AD users: **wireless123**
- AD user: **wireless123** assigned to AD group: **vlan 20**
- AD group: **vlan 20** mapped to ACS group: **Group 20** where Group 20 is configured to assign the authenticated users of this group into the Interface **vlan20** on the WLC.
- Here the *Domain Controller* and the *ACS Server* are configured in the same machine.

These assumptions are made before you perform this configuration:

- The LAP is already registered with the WLC.
- You are aware of how to configure an internal DHCP server or an external DHCP server on the controller in order to assign the IP address to the wireless client. Refer to Configuring DHCP in order to configure an internal DHCP server on the controller.
- The document discusses the configuration required on the wireless side and assumes that the wired network is in place.

In order to accomplish dynamic VLAN assignment with WLCs based on ACS to AD group mapping, these steps must be performed:

1. Configure Active Directory and Windows User Database
2. Configure the Cisco Secure ACS
3. Configure the Wireless LAN Controller

# Configure Active Directory and Windows User Database

In order to configure AD and Windows user database to be used to authenticate wireless clients, these steps must be performed:

1. Configure the Server in Your Network as the Domain Controller
2. Create Active Directory Users and Groups in the Domain
3. Add ACS Server as the Member of the Domain

## Configure the Server in Your Network as the Domain Controller

The configuration of a domain controller involves the creation of a new AD structure, and the installation and configuration of DNS service on the server.

This document creates a domain **lab.wireless** on the Windows 2003 server configured as domain controller.

As part of this AD creation process, you install the DNS server on the Windows 2003 server in order to resolve lab.wireless to its own IP address and other name resolution processes in the domain. You can also configure an external DNS server in order to connect to the Internet.

**Note:** Make sure you have the Windows 2003 CD in order to install the DNS server on the server machine.

Refer to Installing and Configuring Windows 2003 as a Domain Controller for a detailed configuration procedure.

## Create Active Directory Users and Groups in the Domain

The next step is to create users and groups in the lab.wireless domain. Refer to steps 1 and 2 of the Adding Users and Computers to the Active Directory Domain section of this Microsoft Support document in order to create AD users and groups.

As already mentioned in the Configuration Setup section of this document, a user **wireless123** is created and mapped to the AD group **vlan20**.

## Add ACS Server as the Member of the Domain

Refer to steps 1 and 2 of the Adding Users and Computers to the Active Directory Domain section of this Microsoft Support document in order to add the ACS server to the lab.wireless domain.

**Note:** This section only mentions how to add the Windows machine that runs ACS software to the domain. This procedure is not applicable for adding the ACS Solution Engine as member of the domain.

## Configure the Cisco Secure ACS

In order to configure ACS for this setup, these steps must be performed:

1. Configure the ACS for Windows User Database Authentication and Group Mapping
2. Configure ACS for Dynamic VLAN Assignment

# Configure the ACS for Windows User Database Authentication and Group Mapping

Now that the ACS server is joined to the lab.wireless domain, the next step is to configure the ACS for Windows user database authentication and map the external Windows AD database to the ACS group. Unknown users who authenticate by using the specified database automatically belong to, and inherit the authorizations of the group.

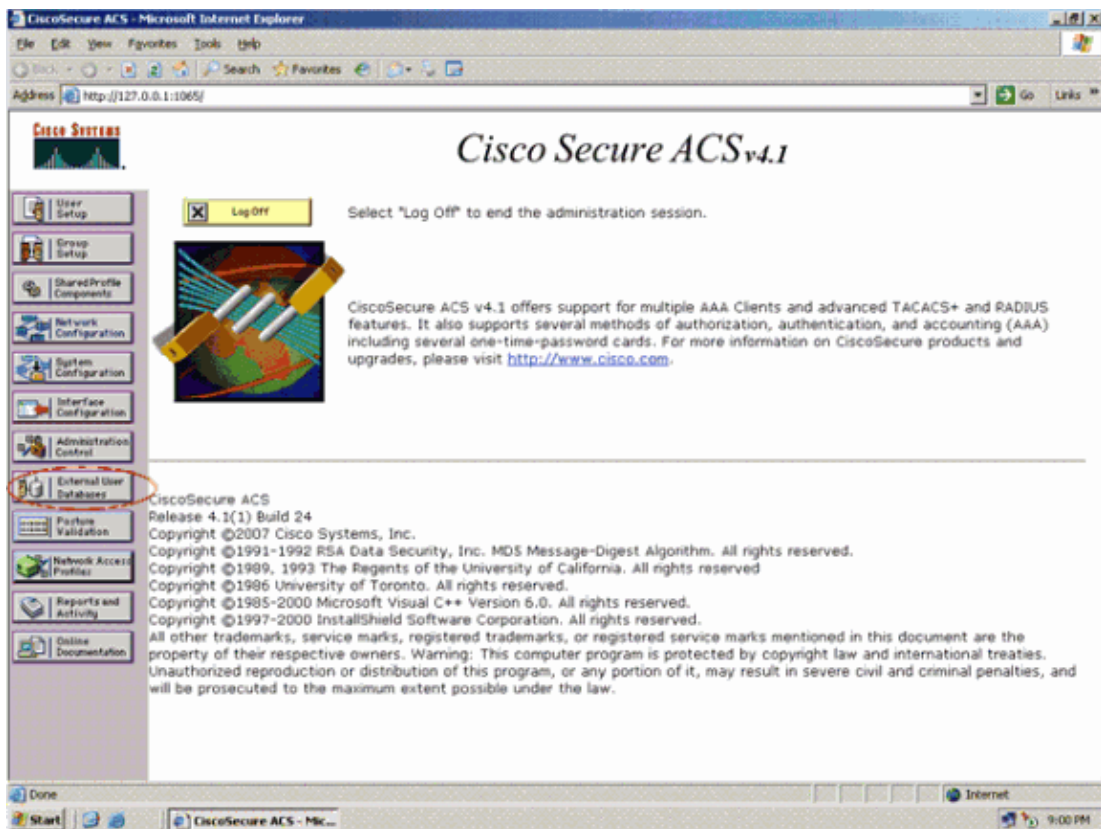
As mentioned earlier, this example maps the AD group vlan 20, with the ACS group Group 20.

**Note:** Before you configure the ACS server, perform the tasks as explained in the Windows Authentication Configuration chapter for reliable user authentication and group mapping.

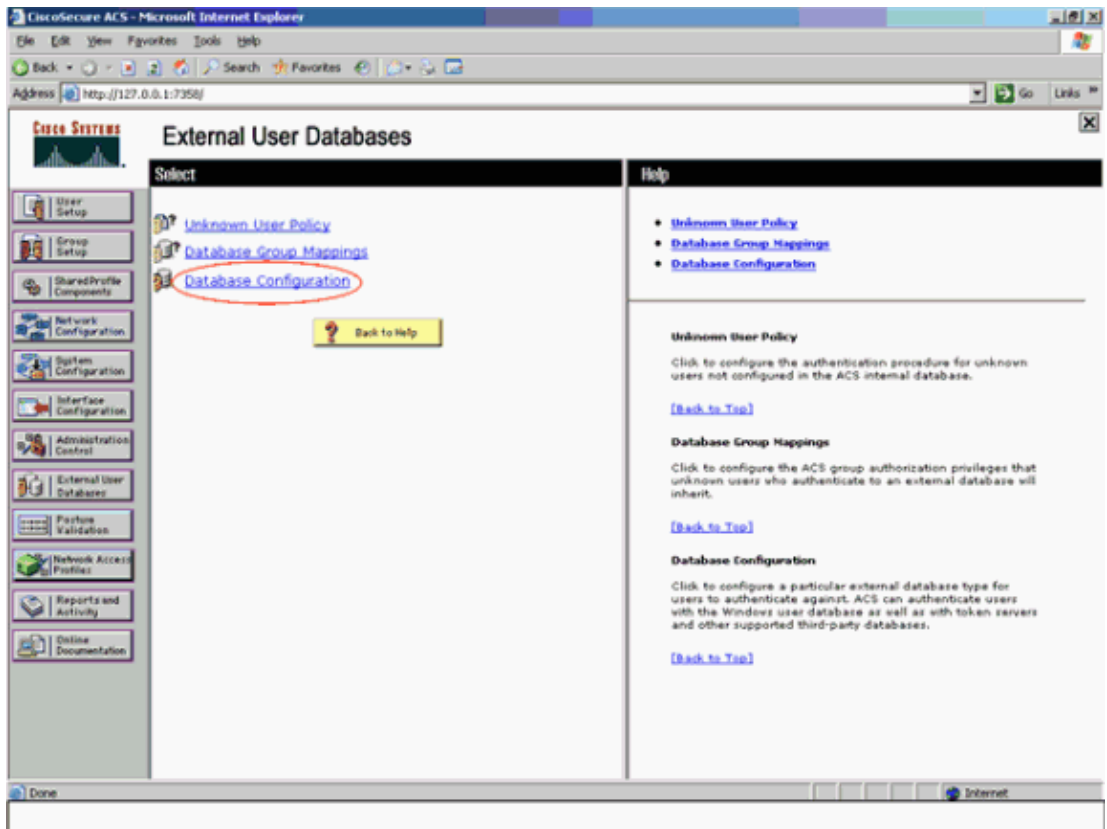
## Configure the Windows External User Database in the ACS Server

From the ACS GUI, complete these steps:

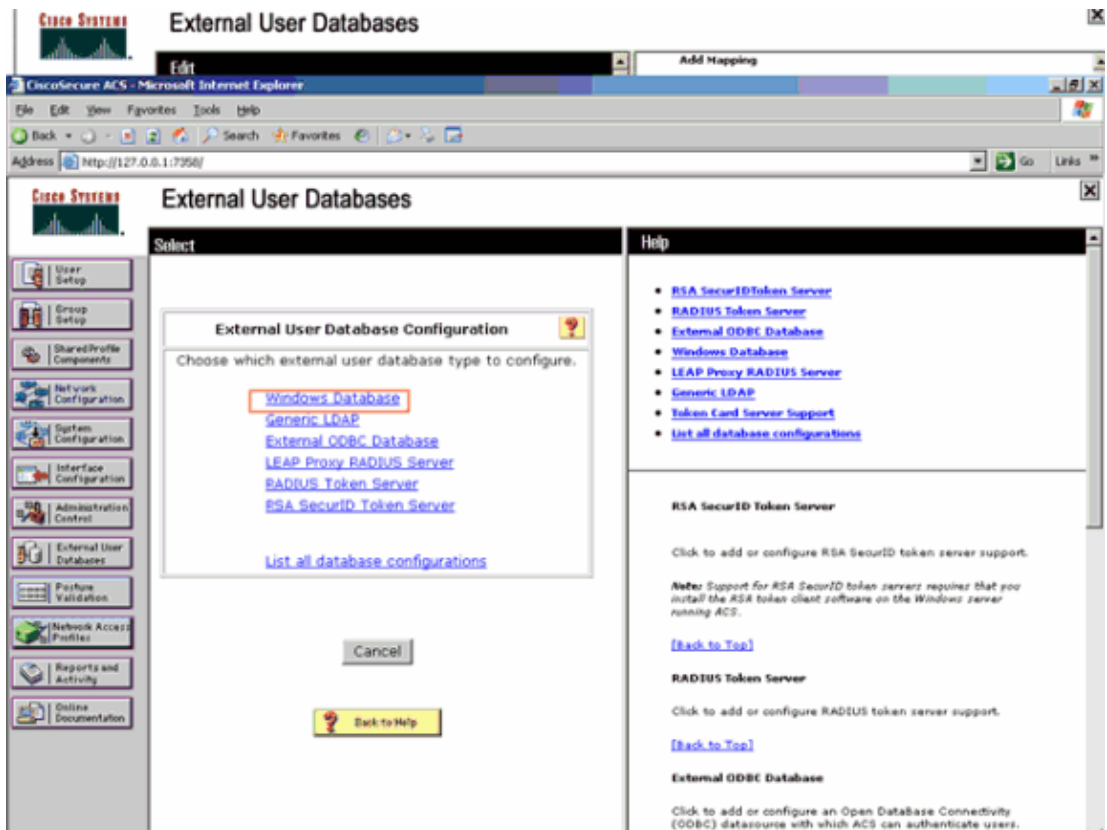
1. In the navigation bar, click **External User Databases**.



2. On the External User Databases page, click **Database Configuration**.

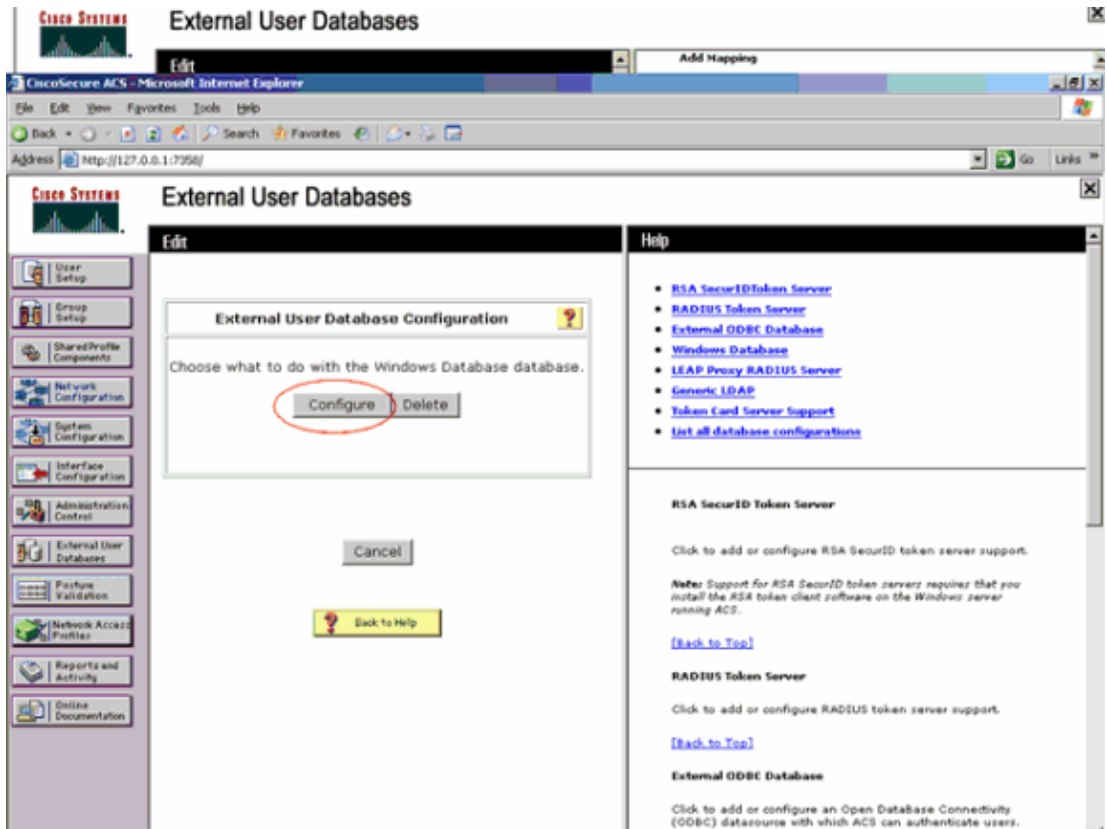


The ACS displays a list of all possible external user database types.  
 3. Click **Windows Database**.



If no Windows database configuration exists, the Database Configuration Creation table appears. Otherwise, the External User Database Configuration page appears.

4. Click **Configure**.



The Windows User Database Configuration page appears with several options.

5. Configure the required options. All the settings on the **Windows User Database Configuration** page are optional and do not need to be enabled unless you want to permit and configure the specific features that they support.

**Note:** This document does not configure any of these options manually as they are not needed for this configuration example.

Refer to Windows User Database Configuration Options for more information.

6. Click **Submit** in order to finish this configuration.

The ACS saves the Windows user database configuration that you created. You can now add it to your Unknown User Policy or assign specific user accounts to use this database for authentication. This document adds this configuration to the Unknown User Policy.

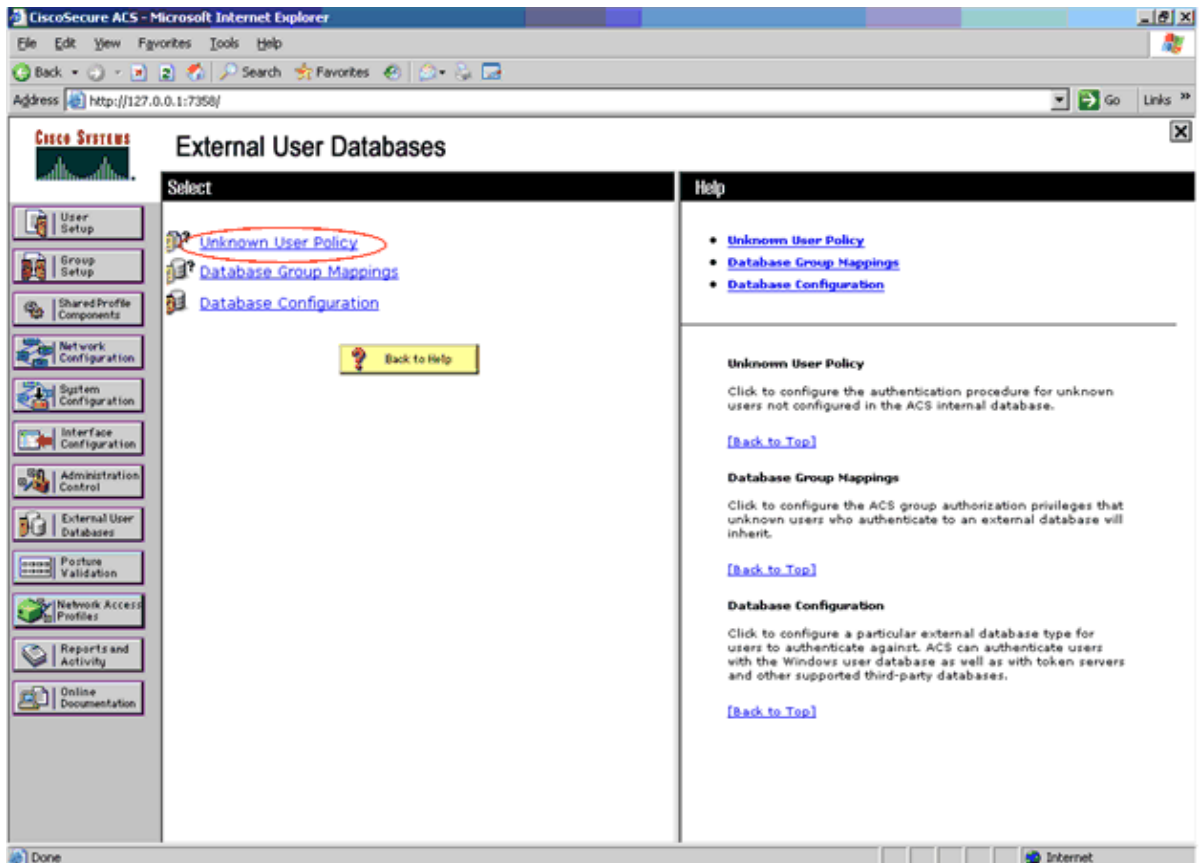
## Configure Unknown User Policy with the Windows Database

The Unknown User Policy is a form of authentication forwarding. In essence, this feature is an extra step in the authentication process. If a username does not exist in the ACS internal database, the ACS forwards the authentication request of an incoming username and password to external databases with which it is configured to communicate. The external database must support the authentication protocol used in the authentication request.

Refer to Unknown User Policy for more information.

In this example, the ACS should forward the authentication request coming through the WLC from a wireless client to the Windows database configured in the previous section. In order to achieve this, the Unknown User group should be mapped to the external Windows database (lab.wireless) using these steps:

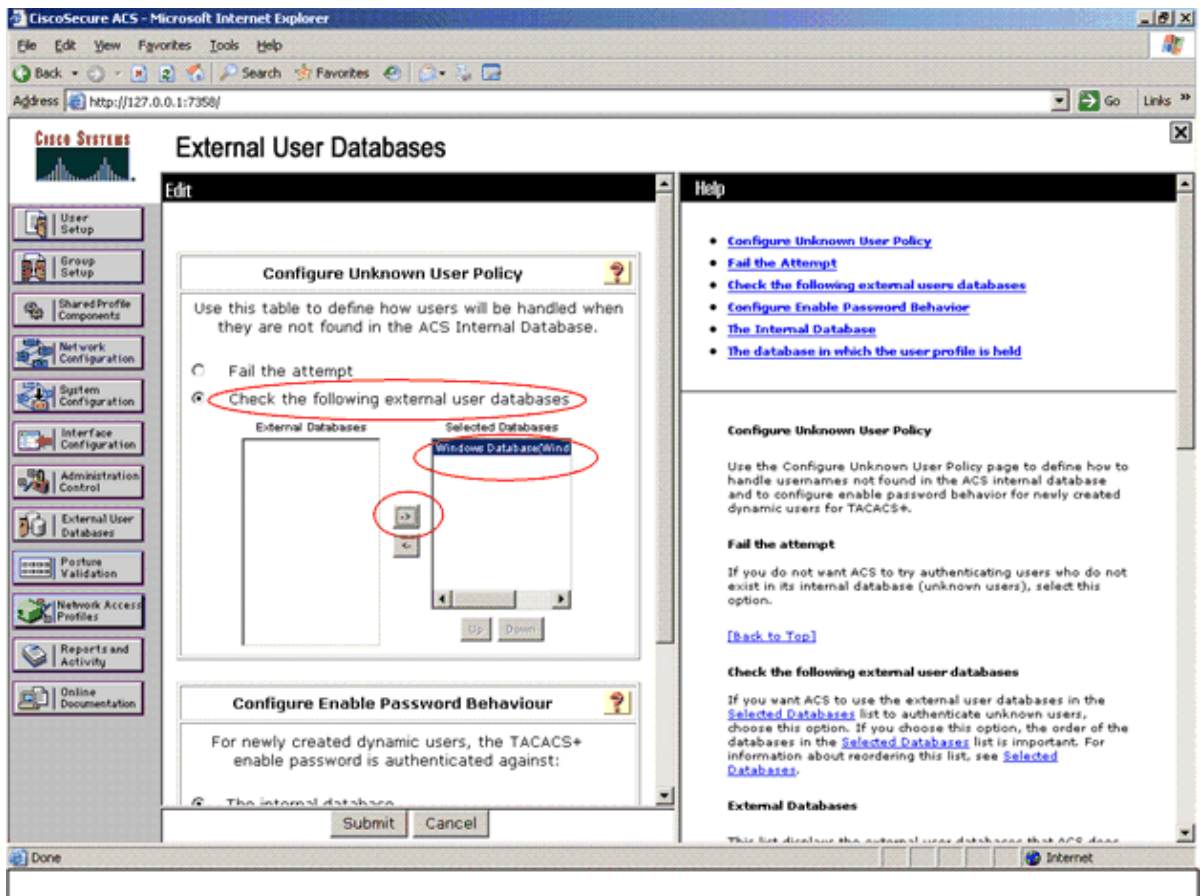
1. In the navigation bar, click **External User Databases**. Then, click **Unknown User Policy**.



2. In order to allow unknown user authentication, enable the Unknown User Policy:

- a. Select the **Check the following external user databases** option.
- b. Select the **Windows Database in the External Databases** list and click --> (right arrow button) to move it from External Databases to the Selected Databases list. In order to remove a database from the Selected Databases list, select the database, and then click <-- (left arrow button) to move it back to the External Databases list.

3. Click **Submit**.

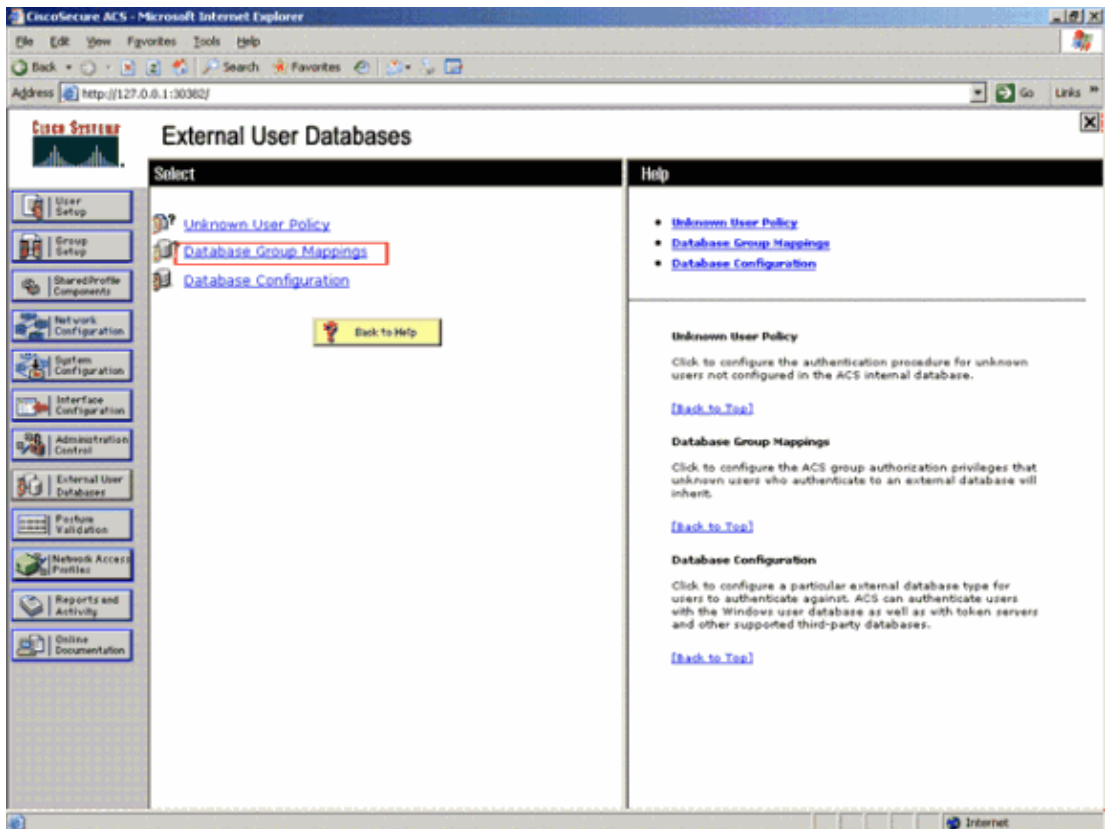


The ACS saves and implements the Unknown User Policy configuration that you created.

## Create ACS Group Mapping with Windows Group

Complete these steps from the ACS GUI:

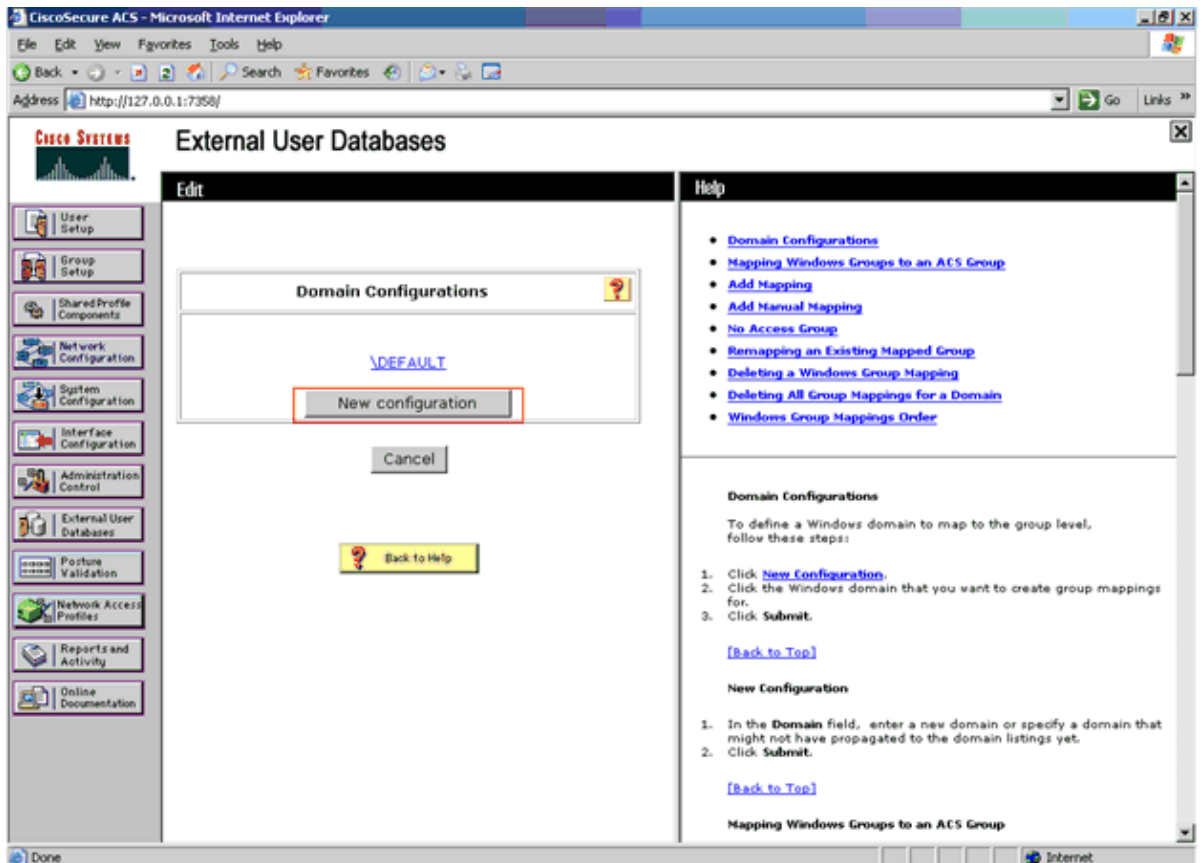
1. In the navigation bar, click **External User Databases**. Then, click **Database Group Mappings**.



2. Click the external user database name for which you want to configure a group mapping.

In this example, it is Windows database.

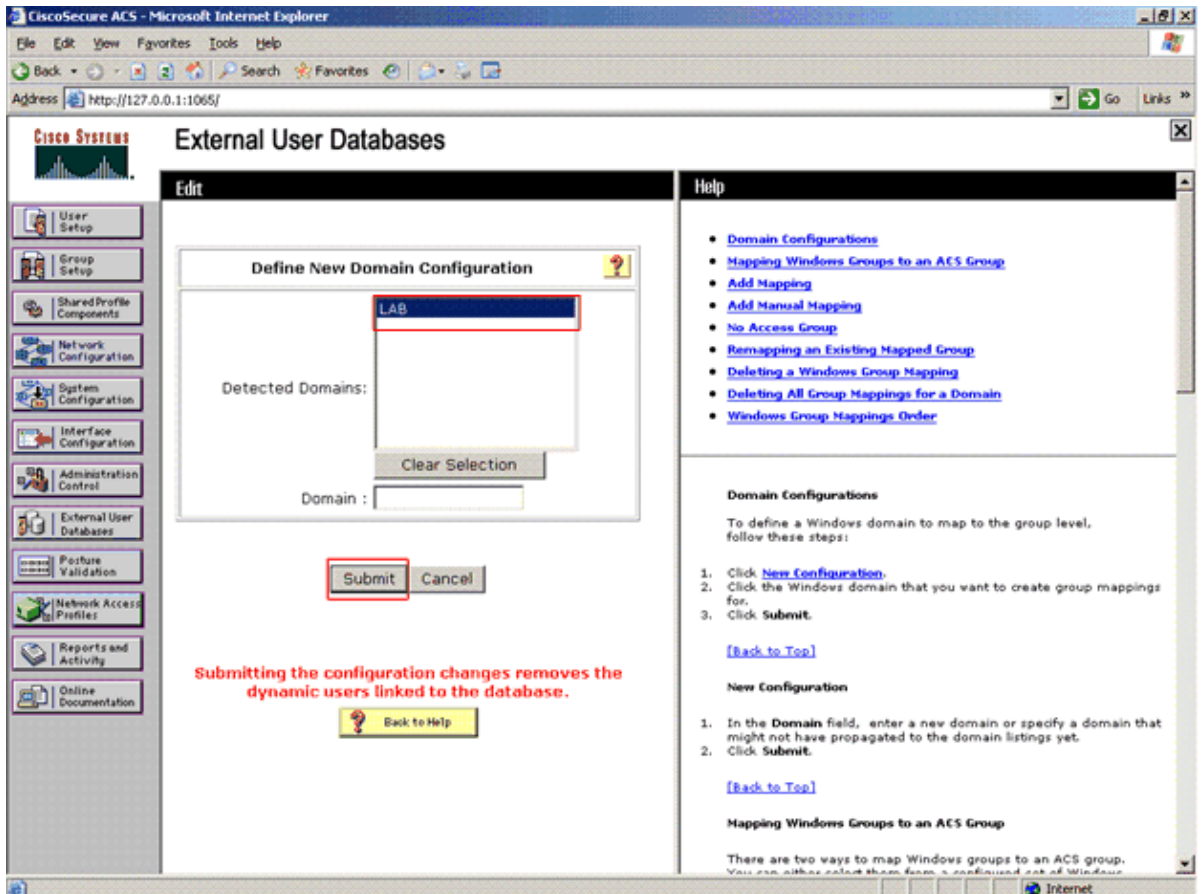
3. In the resultant Domain Configurations page, click **New configuration**.



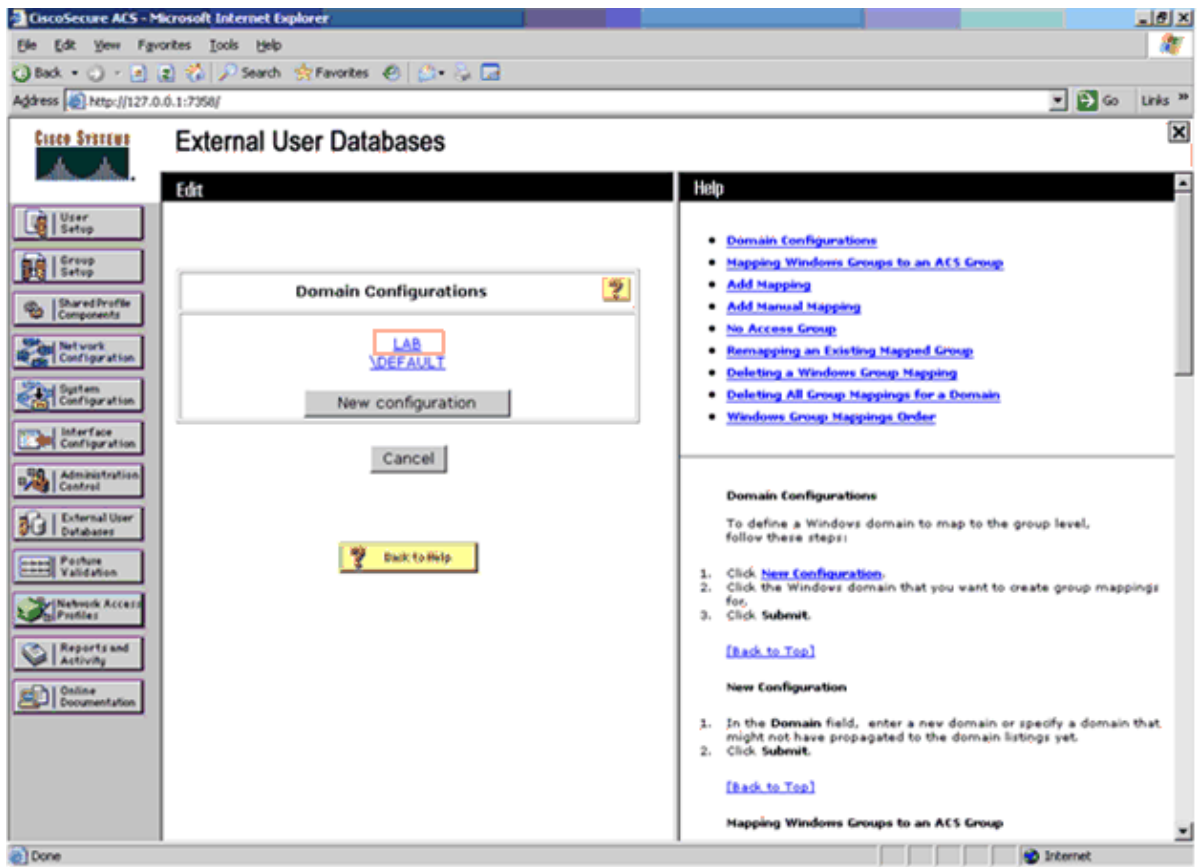
**Note:** By default you see only the domain \DEFAULT on this page.

The Define New Domain Configuration page appears..

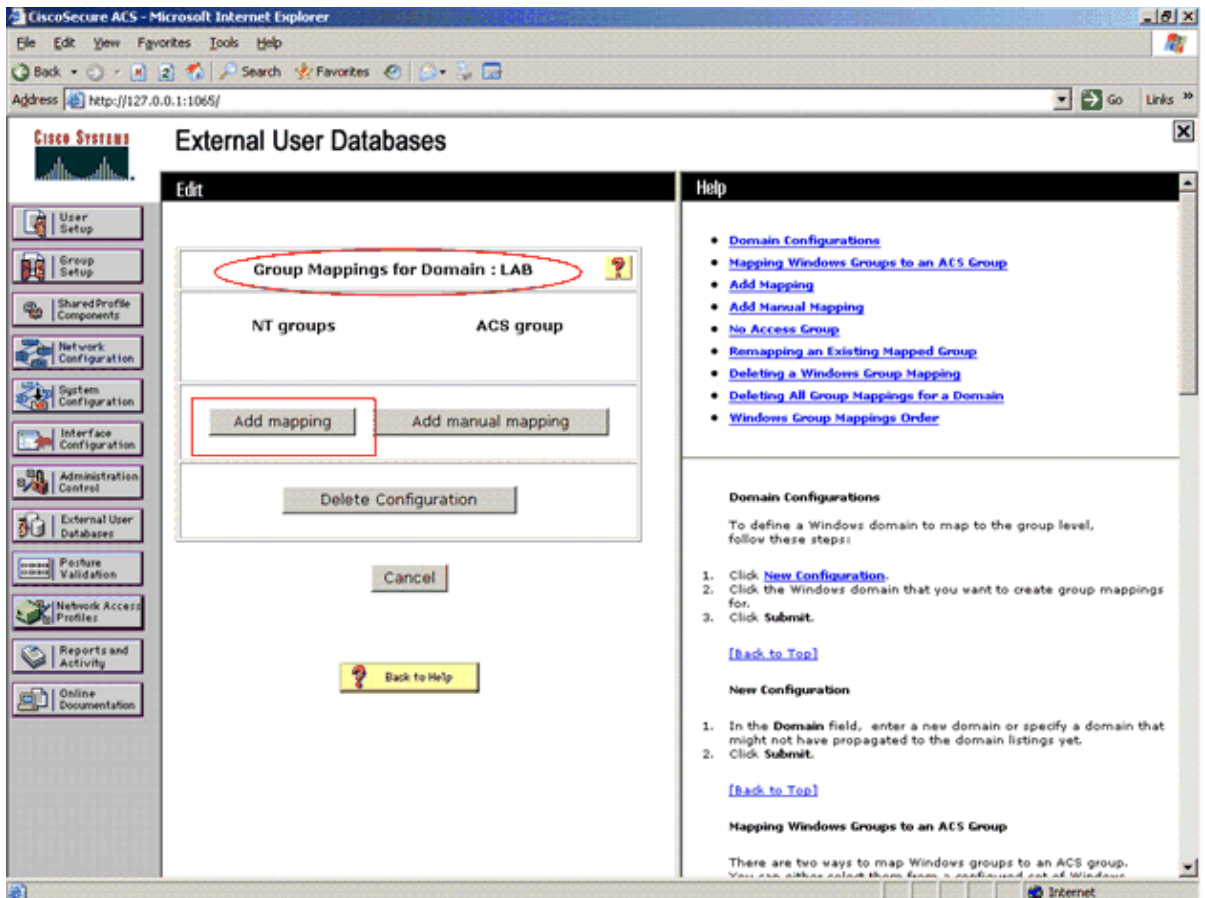
4. In the Detected Domains box of this page, you should be able to see the Windows user database **LAB**. Click **Submit**.



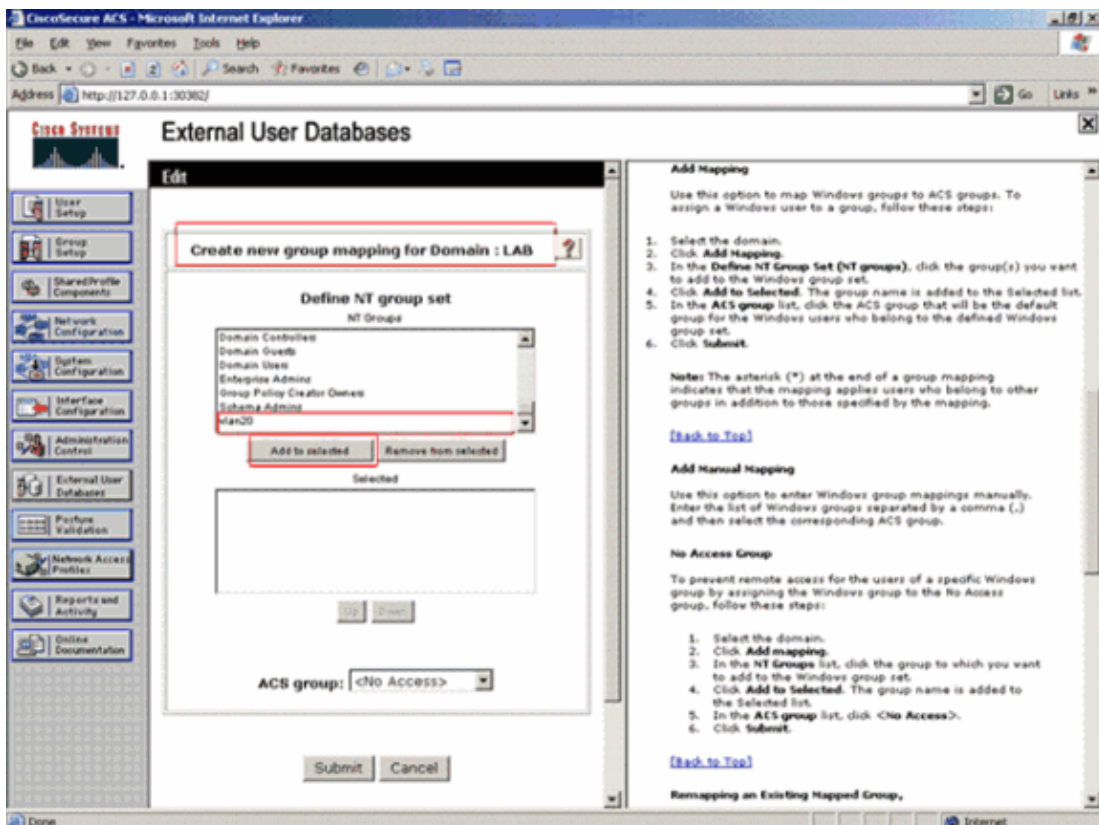
5. Click the **LAB** domain.



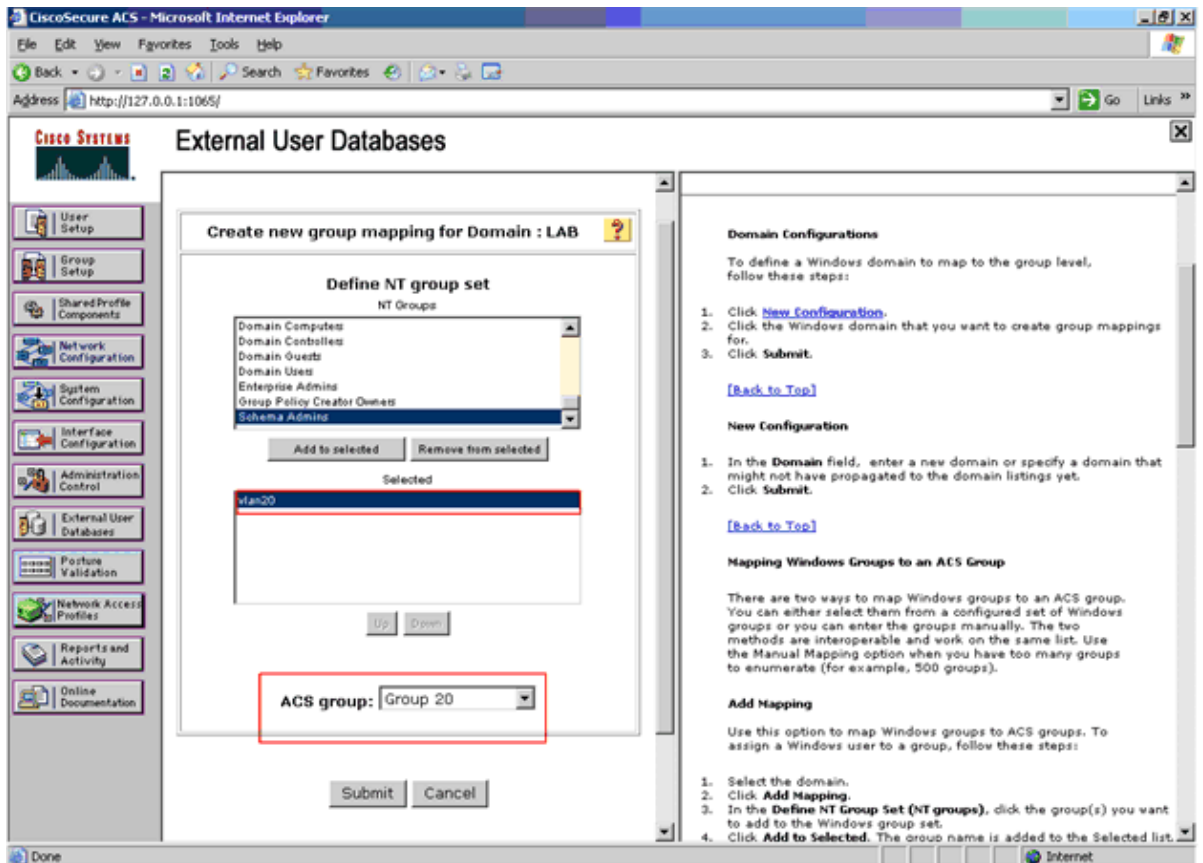
The Group Mappings for the Domain: LAB table appears.  
6. Click **Add mapping**.



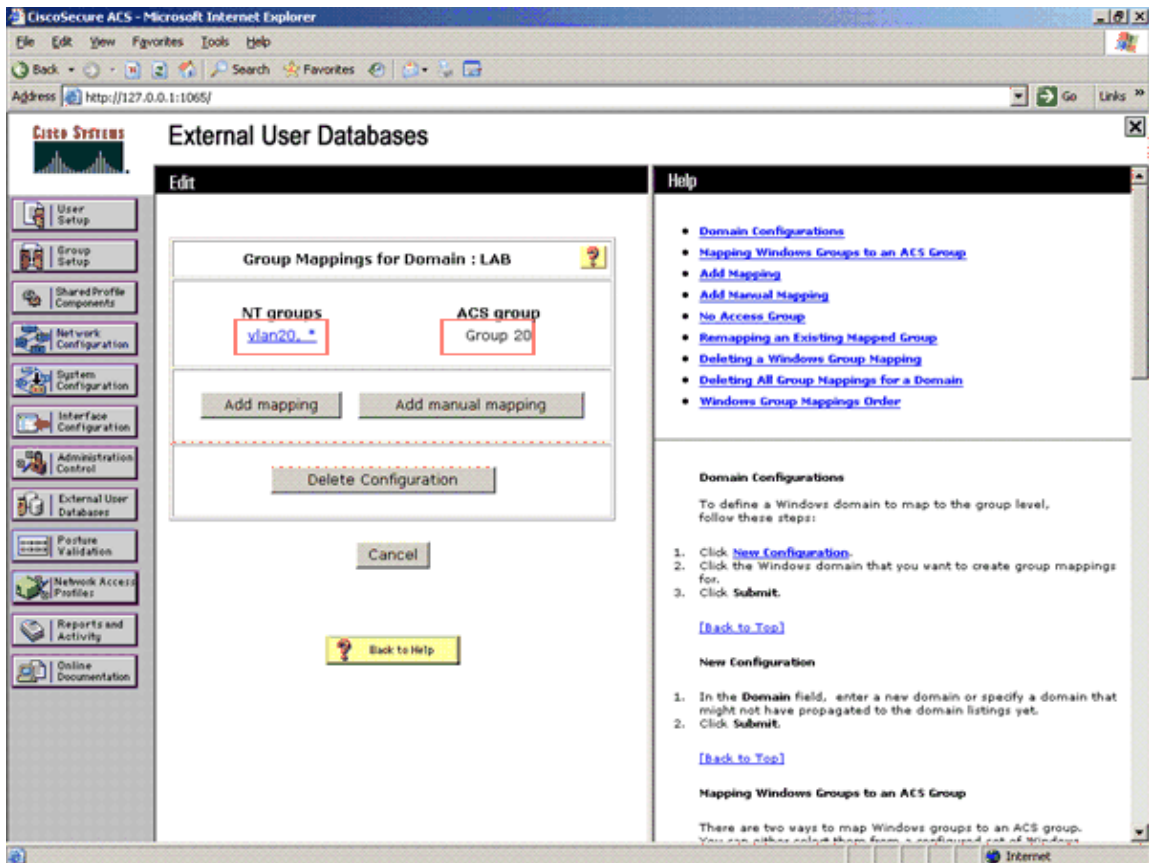
The Create new group mapping for Domain: LAB page opens. The group list displays group names that are derived from the LAB database. In this Group set, you should be able to see the group vlan20 created in the AD of this lab domain.



7. Choose **vlan20** from the group list, then click **Add to selected**.
8. In the ACS group drop-down box, choose **Group20** to which you want to map users who belong to AD group: vlan 20.
9. Click **Submit**.



The group mapped to the ACS list appears at the bottom of the database groups column as shown in the example. The asterisk (\*) at the end of each set of groups indicates that users who are authenticated with the external user database can belong to other groups besides those in the set.



## Configure ACS for Dynamic VLAN Assignment

Dynamic VLAN assignment is one feature that places a wireless user into a specific VLAN based on the credentials supplied by the user. This task of assigning users to a specific VLAN is handled by a RADIUS authentication server, such as Cisco Secure ACS. This can be used, for example, to allow the wireless host to remain on the same VLAN as it moves within a campus network.

**Note:** This document uses Cisco Airespace [VSA (Vendor-Specific)] Attribute to assign a successfully authenticated user with a VLAN interface name (not the VLAN ID) as per the group configuration on the ACS.

In order to configure the ACS for dynamic VLAN assignment, these steps must be performed:

1. Add the WLC as AAA Client to the ACS
2. Configure the ACS Group with Cisco Airespace VSA Attribute Option

### Add the WLC as AAA Client to the ACS

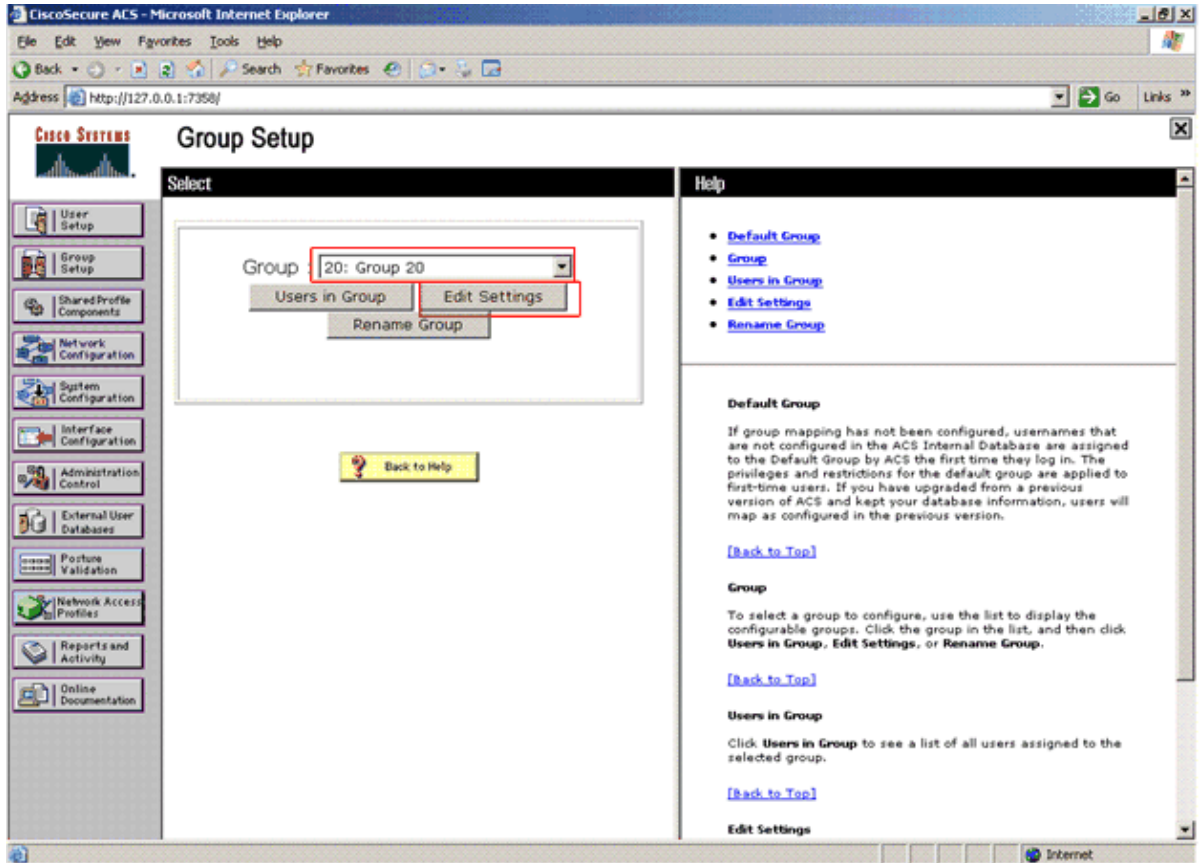
In order to configure ACS for dynamic VLAN assignment, you need to configure the AAA client for the WLC on the RADIUS server. This document assumes that the WLC is already added to the ACS as an AAA client. Refer to Adding AAA Clients to an ACS for information on how to add the AAA client to the ACS.

**Note:** In this document's example, the **RADIUS (Airespace)** option under the Authenticate Using pull down menu of the Add AAA Client page should be configured, while the WLC as the AAA client to the ACS is configured.

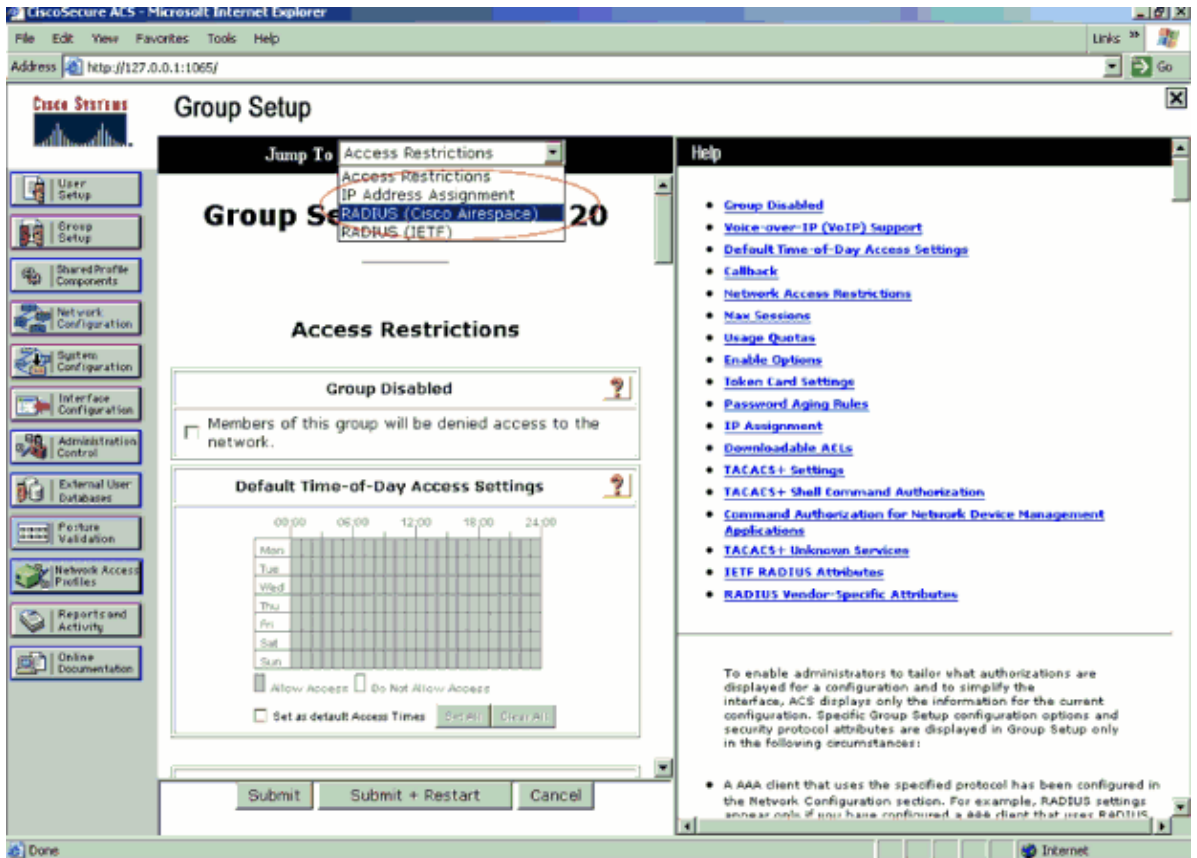
## Configure the ACS Group with Cisco Airespace VSA Attribute Option

Complete these steps:

1. From the ACS GUI in the navigation bar, click **Group Setup** from the left-hand side in order to configure a new group.
2. In the Group drop-down box, choose **Group 20** (as per this example) and click **Edit Settings**.

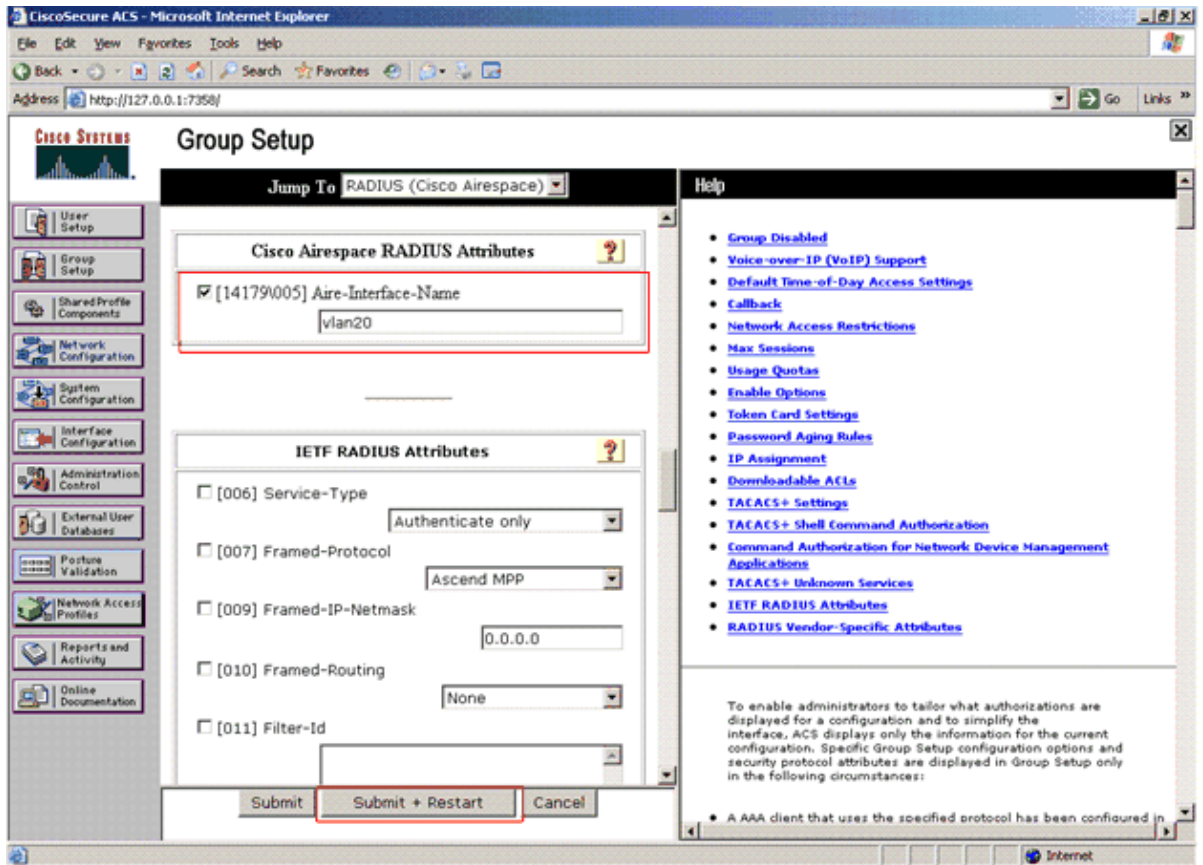


3. On the Group 20 edit settings page, click the **Jump To** drop-down box and choose **RADIUS (Cisco Airespace)** in order to configure the Airespace VSA attribute setting.



**Note:** If this attribute is not displayed under Group setting, edit the **RADIUS (Airespace)** settings to include the interface name under the Interface configuration screen of the ACS.

4. In the Cisco Airespace RADIUS Attributes section, enable the **Air-Interface-Name** and enter **vlan20** as the interface name to be returned by this ACS group upon successful authentication.



5. Click **Submit + Restart**.

## Configure the Wireless LAN Controller

In order to configure WLC for this setup, these steps must be performed:

1. Configure the WLC with Details of the Authentication Server
2. Configure the Dynamic Interfaces (VLANs) on the WLC
3. Configure the WLANs (SSID)

## Configure the WLC with Details of the Authentication Server

Complete these steps in order to configure the WLC for this setup:

1. From the controller GUI, click **Security**.
2. Click **New**.
3. On the RADIUS (ACS) Authentication Server configuration page, enter the IP address of the RADIUS server and the Shared Secret key used between the RADIUS server and the WLC.

This Shared Secret key should be the same as the one configured in the ACS under **Network Configuration > AAA Clients > Add Entry**. This document uses the ACS server with the IP address of 10.77.244.196/27.

4. Make sure that the Server Status is Enabled. Check the **Network User** box. This ensures that the Network users are authenticated against this server.

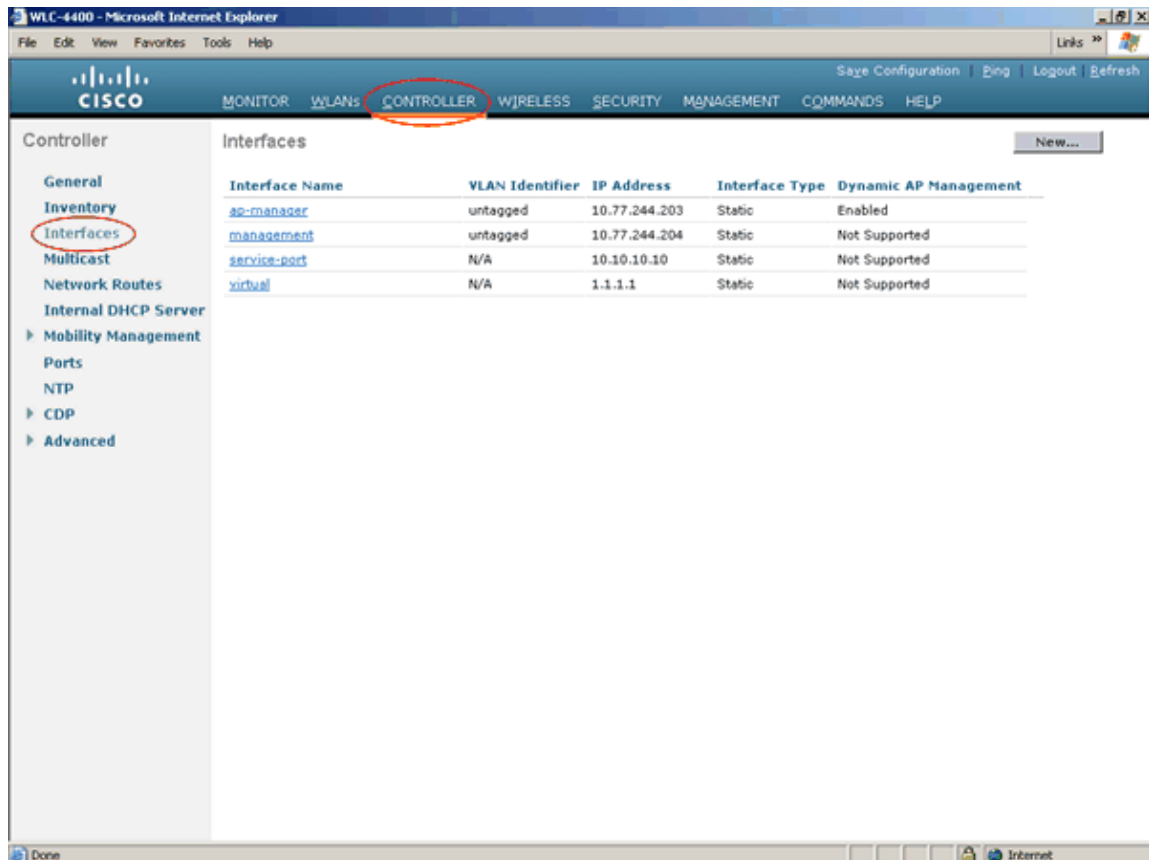
## Configure the Dynamic Interfaces (VLANs) on the WLC

This procedure explains how to configure dynamic interfaces on the WLC. For a successful dynamic VLAN assignment, the VLAN interface name specified under the VSA attribute configuration of ACS server should also be configured in the WLC.

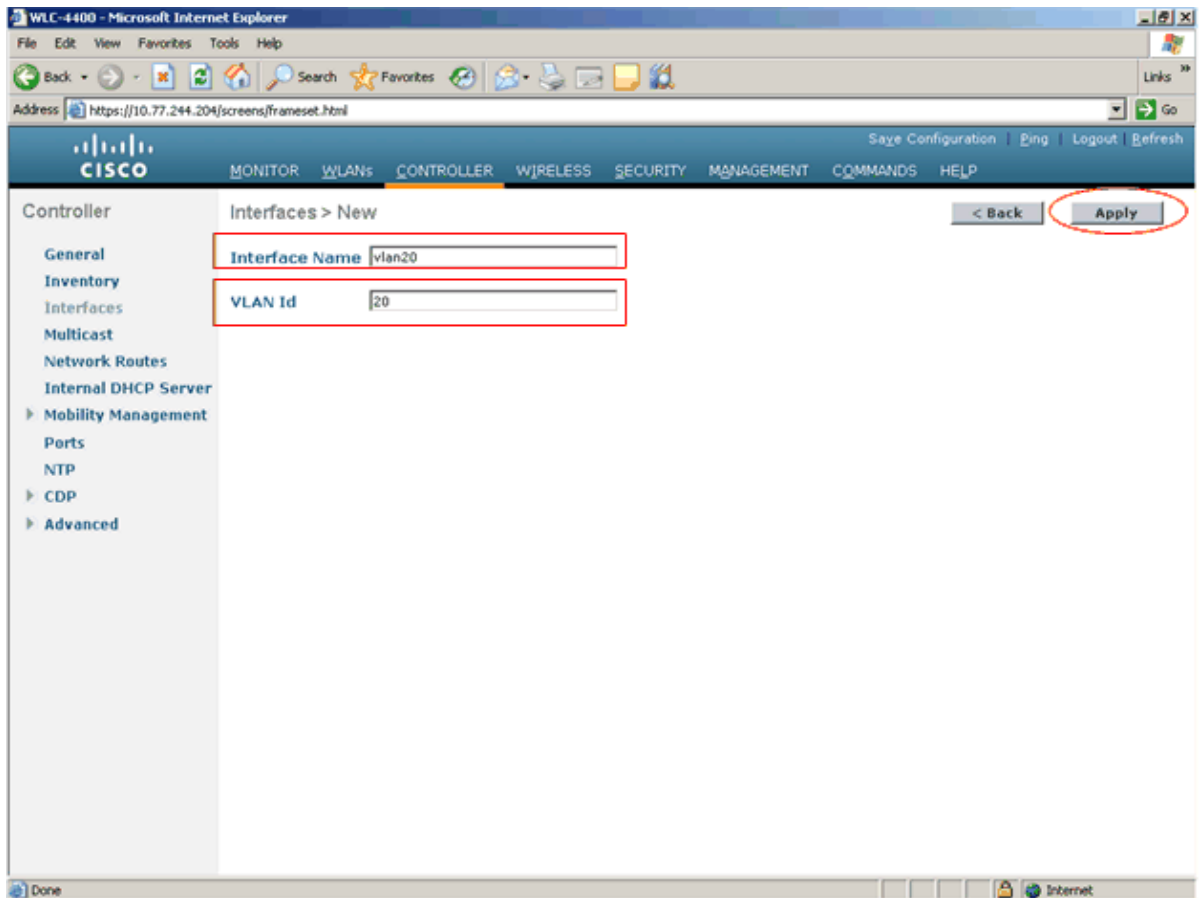
This document configures the VLAN interface with name "vlan20" and VLAN ID = 20, and VLAN interface with name in the WLC.

Complete these steps:

1. From the controller GUI, under the **Controller > Interfaces** window, the dynamic interfaces are configured.

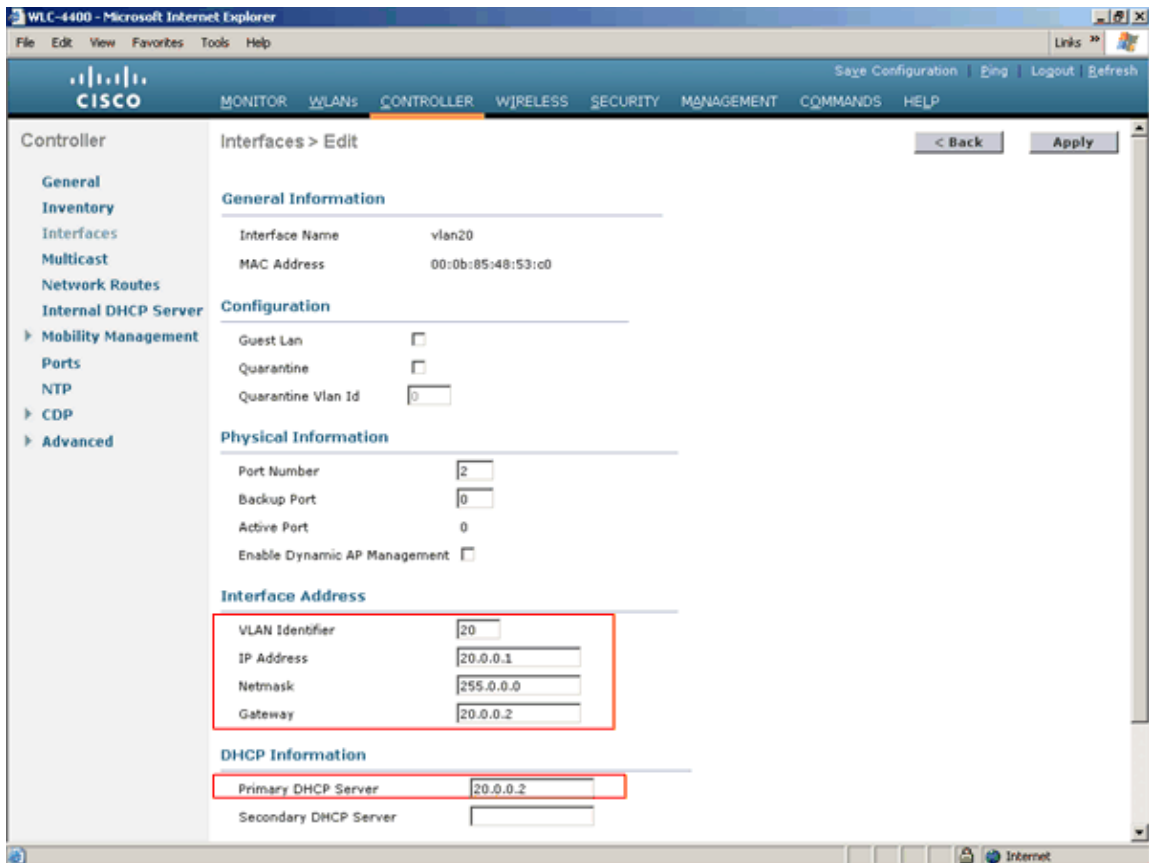


2. Click **New**.
3. On the **Interfaces > New** window, type the Interface Name as *vlan20*, which is same as the Airespace-Interface parameter configured on the ACS and VLAN ID as 20 to assign it to VLAN 20.
4. Click **Apply**.



5. On the **Interfaces > Edit** page, configure the VLAN ID, IP address, Netmask and Gateway address information from VLAN 20 subnet as shown in this window.

**Note:** It is always recommended to use a DHCP server to assign IP address to clients. In that case, the primary DHCP server address field should be filled with the IP address of the DHCP server.

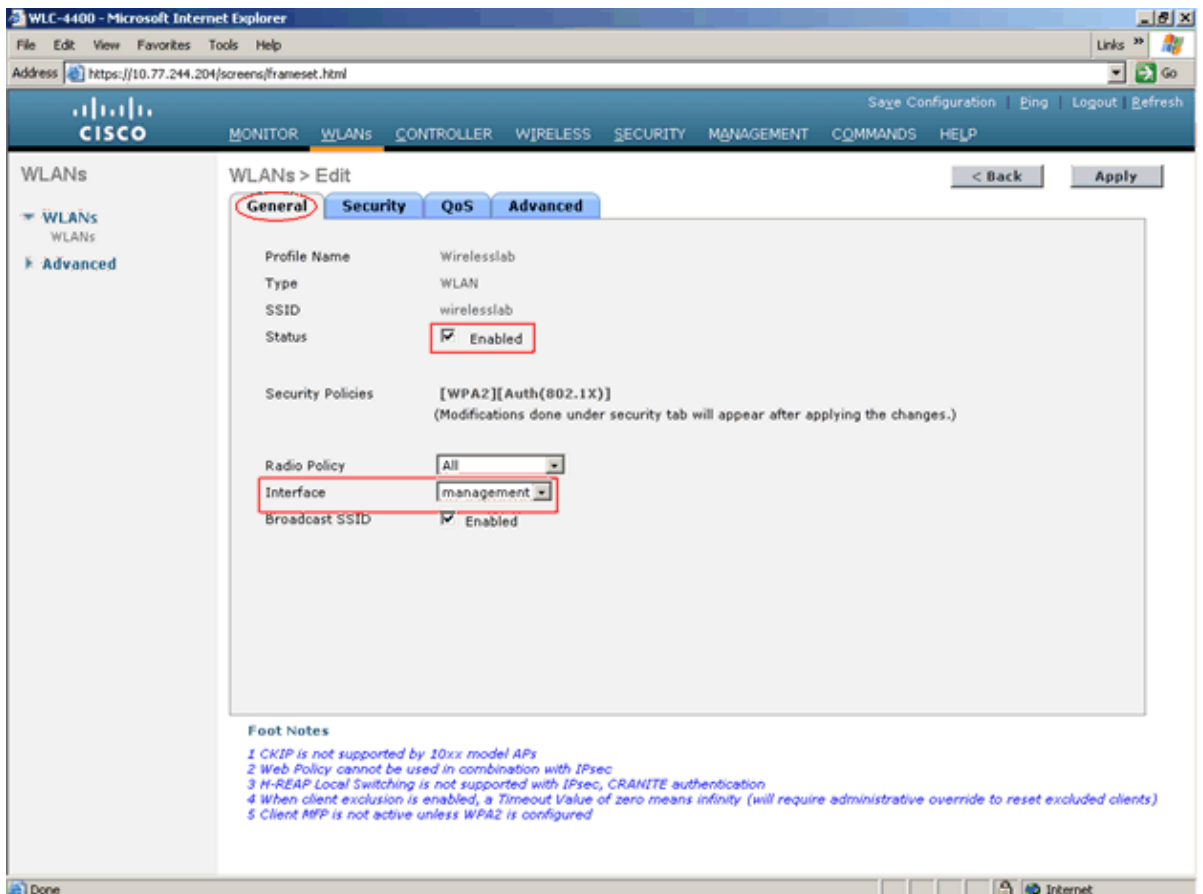


6. Click **Apply**.

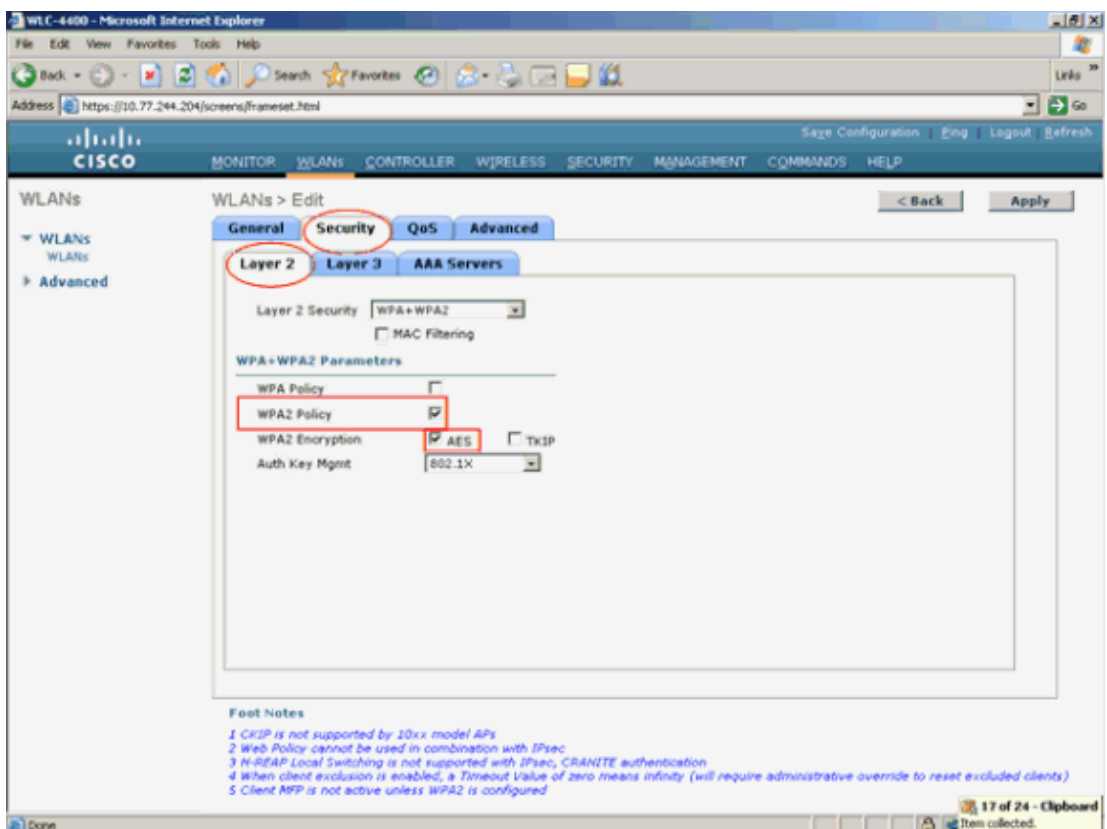
## Configure the WLANs (SSID)

On the WLC, you configure the SSID *wirelesslab* and choose an authentication method, which prompts for username and password from the client. In this example, you use **LEAP** as the authentication method to authenticate the user. Complete these steps:

1. On the WLC GUI, click **WLANs**. Click **New**.
2. Choose a Profile Name and enter the WLAN SSID *wirelesslab*.
3. Click **Apply**.
4. Choose **WLANs > Edit**, and under the General tab, enable the WLAN and choose the Interface as *management* in order to assign the IP addresses from the management subnet .



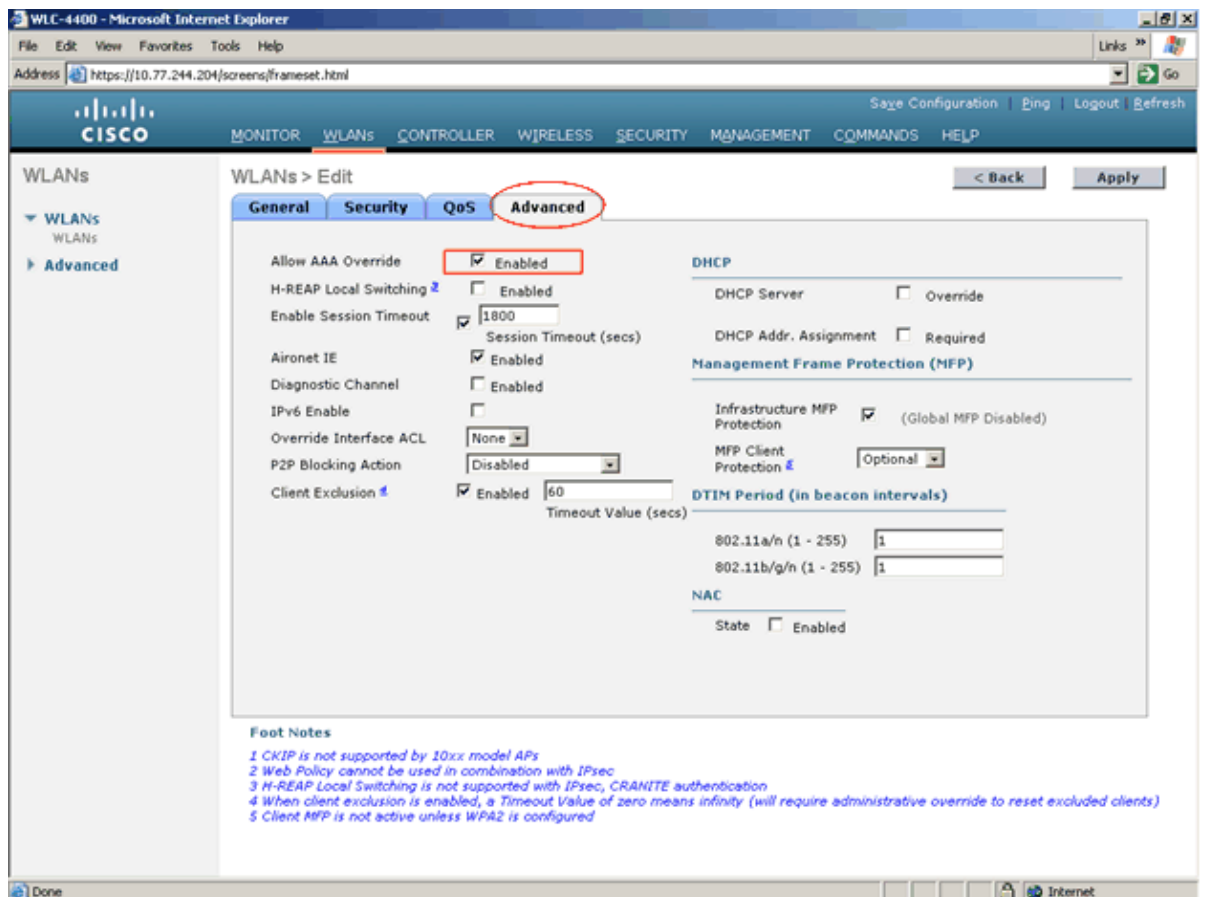
5. Click **Security**. Under the Layer 2 tab, choose **WPA+WPA2** as **Layer 2 Security**. You can choose either WPA or WPA2 policy. In this example you choose **WPA2** with **TKIP** encryption and **802.1x** as the authentication method .



6. Click **AAA Servers** and choose **10.77.244.196** as the Authentication Server in order to authenticate

users of this WLAN against this server.

7. Wireless users are assigned to the Management interface. In order to assign the user to an interface supplied by the Radius server, choose **Advanced > Allow AAA Override**.

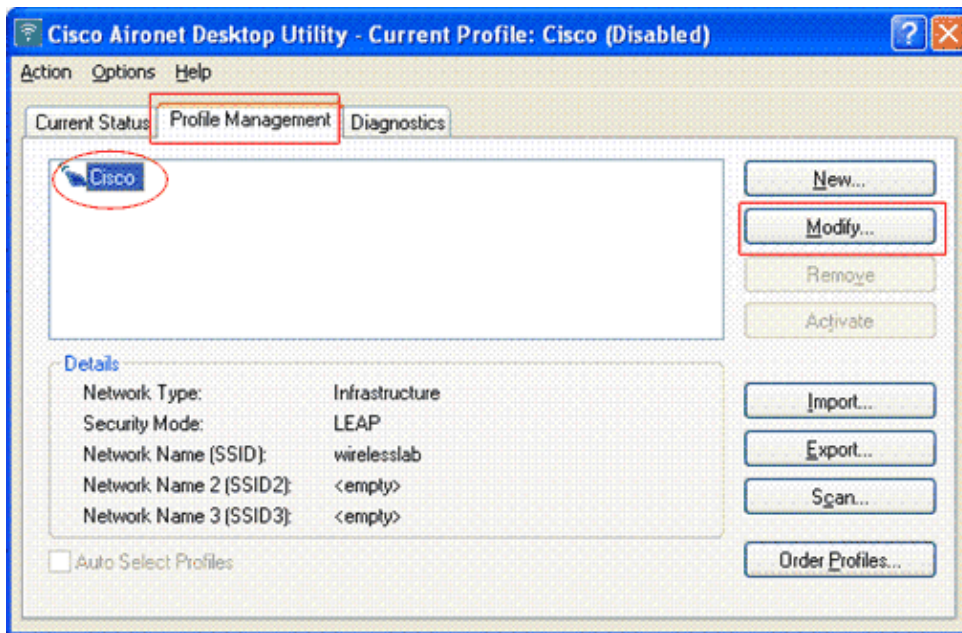


## Configure the Wireless Client

This section explains how to configure the wireless client . Complete these steps:

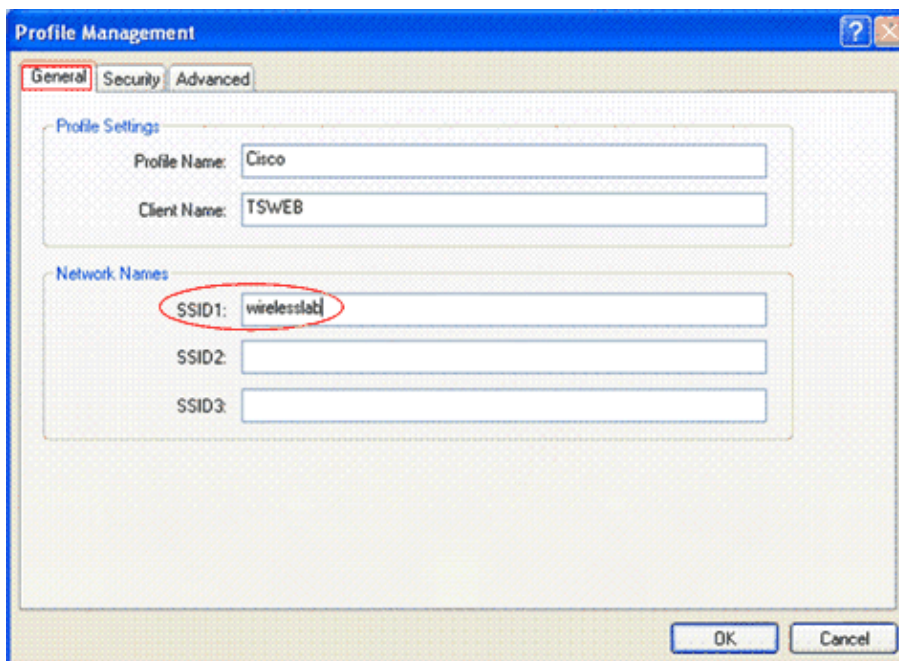
1. Click the **Cisco Aironet Desktop Utility**.
2. Choose **Profile Management**.
3. Highlight the existing Profile and choose **Modify** as shown in the Figure 1.

**Figure 1**



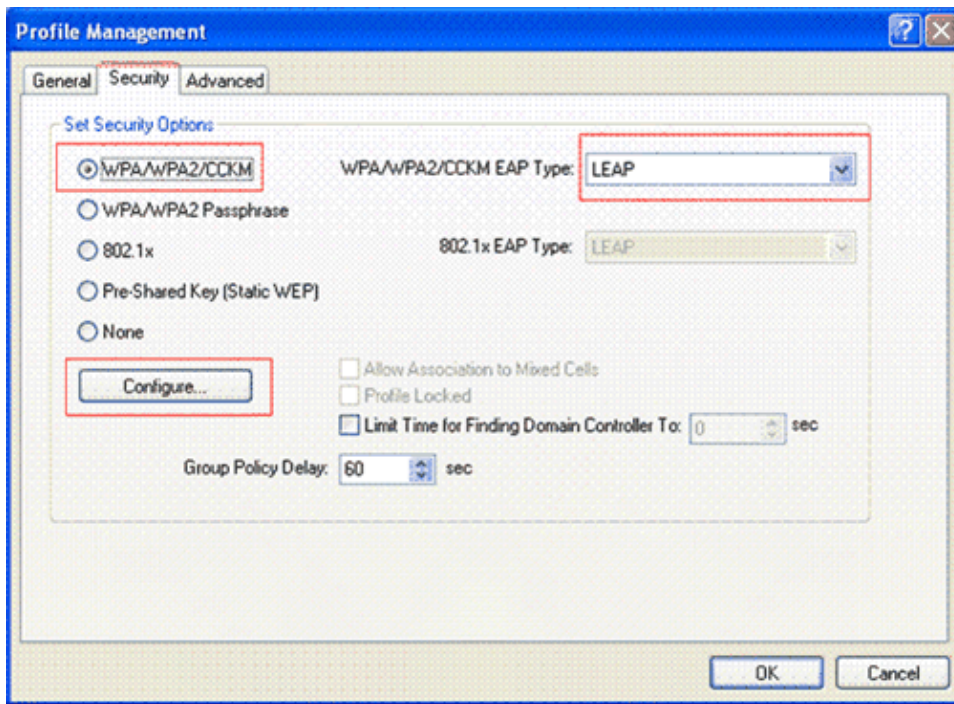
4. In the **General** tab, choose a **profile name**. This example uses the name *LAB*. Enter the SSID *wirelesslab* used in the WLC. Figure 2 shows how to do this.

**Figure 2**



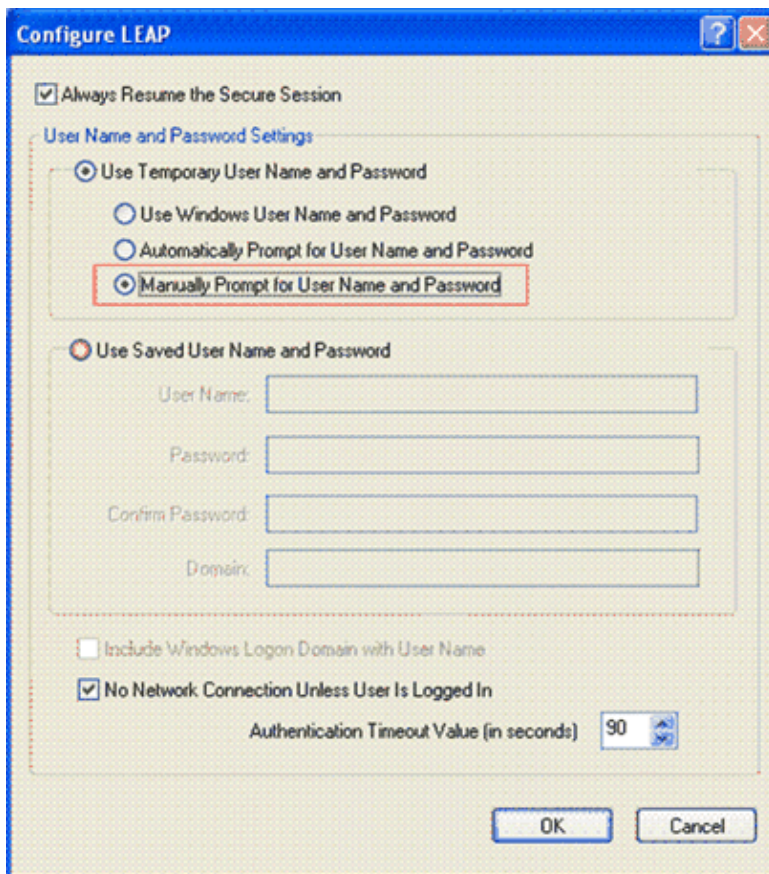
5. Click **Security**. The method of authentication configured on the client should be identical to that of WLC. Choose **WPA/WPA2/CCKM** and choose **EAP type** as *LEAP* as shown in the Figure 3.

**Figure 3**

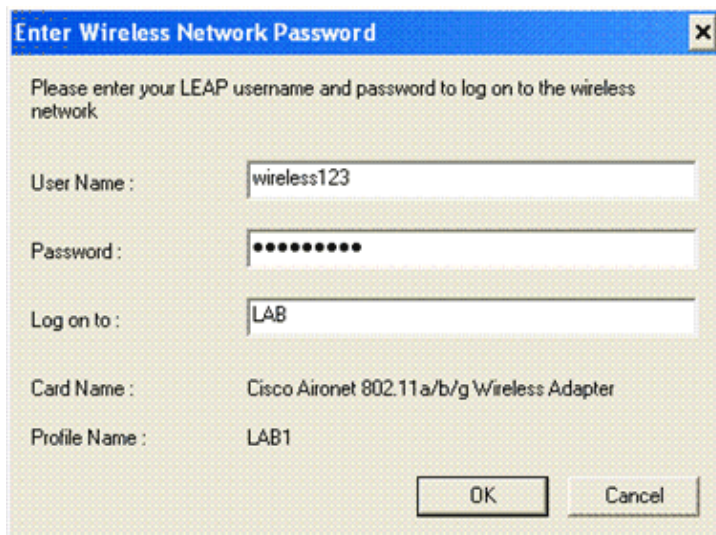


6. Click **Configure** and choose the **Manually Prompt for User Name and Password**. Figure 4 shows this.

**Figure 4**



7. Click **OK**. A window that prompts you for the username and password as shown appears. Enter the user Name and password you configured in the Windows Database. In this example, the user name is *wireless123*, the password is *Cisco123*. In the Log on to field, type in the Domain you configured in the Active Directory and click **OK**. In this example, it is *LAB*. demonstrates these steps.



## Verify

Activate the **LAB** user profile you have configured in the ADU. As per your configuration, the client is prompted for username and password.

This example uses this username and password from the client side to receive authentication and to be assigned to a VLAN by the RADIUS server:

- User Name = **wireless123**
- Password = **cisco123**

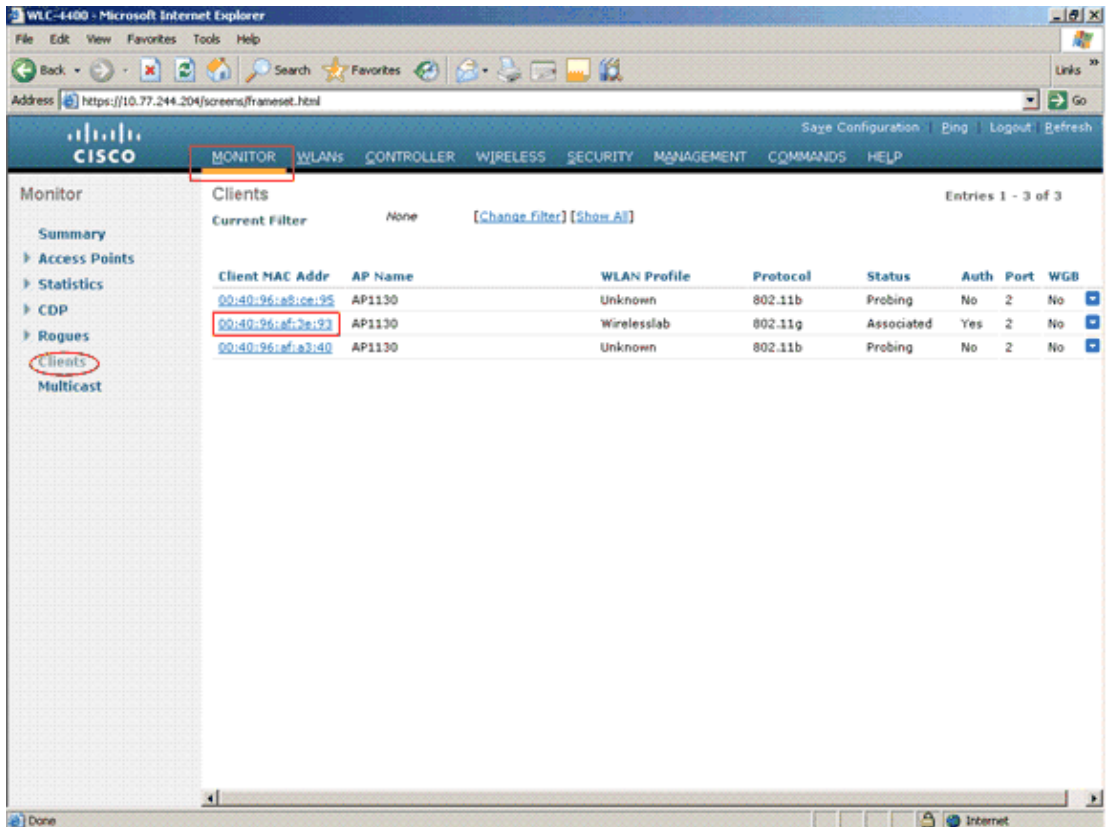
In addition, specify **lab.wireless** in the logon to field of the Enter Wireless Network Password dialogue box.

Once the wireless client successfully authenticates, finds the domain controller, joins the domain and associates to the WLAN network through the wirelesslab SSID, you need to verify that your client is assigned to the proper VLAN as per the VSA attributes sent by the RADIUS server group settings.

Complete these steps in order to accomplish this:

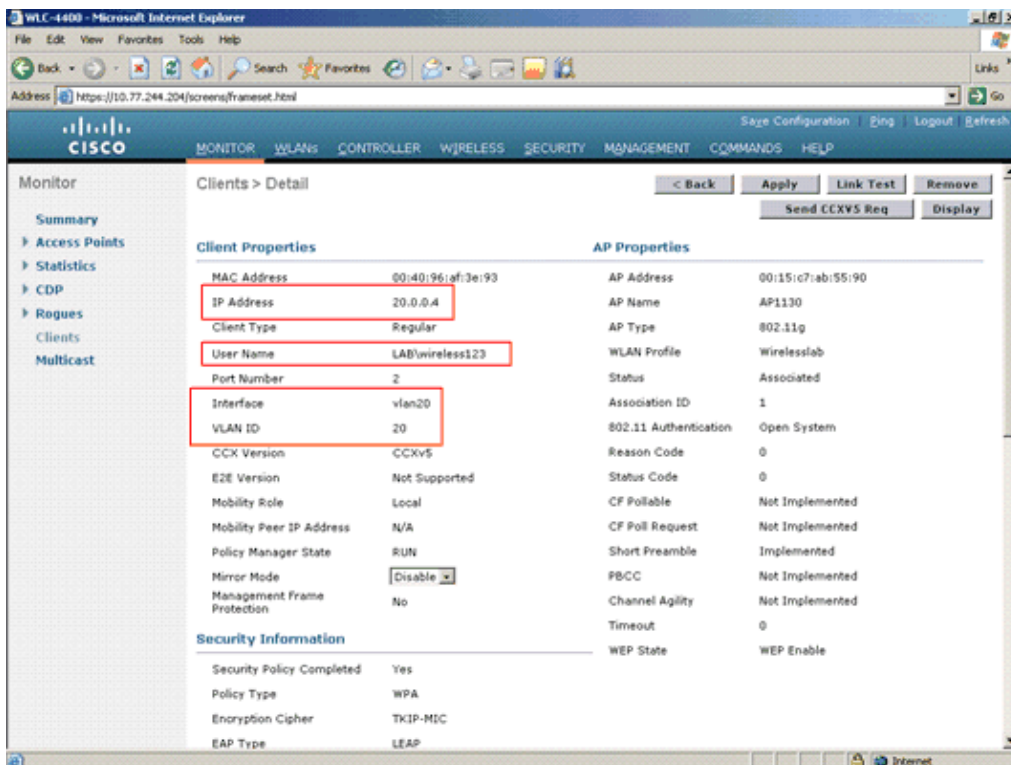
1. From the controller GUI, choose **Monitor**. Click **Clients** that appears on the left of the Access Points (APs) window.

The client statistics are displayed with the status as associated.



2. You see a list of wireless clients that are associated to this WLC. Click on the Client that authenticated with ACS.

On the details page, observe that the **user :wireless123** is authenticated and associated through *wirelesslab* SSID. Note that the IP address is *20.0.0.4* and the interface is *vlan20*.



# Troubleshoot

This section provides information you can use to troubleshoot your configuration. Refer to AAA Debug Information for Cisco Secure ACS for Windows for more information on how how to log and obtain AAA debug information in the ACS.

## Troubleshooting Commands

**Note:** Refer to Important Information on Debug Commands before you use **debug** commands.

- **debug aaa events enable** This command can be used to ensure successful transfer of the RADIUS attributes to the client via the controller. This portion of the debug output ensures a successful transmission of RADIUS attributes.

Here is the output of this command based on this document's example configuration:

```
Fri Oct 5 15:47:38 2007: 00:40:96:af:3e:93 Successful transmission of Authentication Packet (id 131) to 10.77.244.196:1812, proxy state 00:40:96:af:3e:93-96:af
Fri Oct 5 15:47:38 2007: ****Enter processIncomingMessages: response code=11
Fri Oct 5 15:47:38 2007: ****Enter processRadiusResponse: response code=11
Fri Oct 5 15:47:38 2007: 00:40:96:af:3e:93 Access-Challenge received from RADIUS server 10.77.244.196 for mobile 00:40:96:af:3e:93 receiveId = 3
Fri Oct 5 15:47:38 2007: 00:40:96:af:3e:93 Successful transmission of Authentication Packet (id 132) to 10.77.244.196:1812, proxy state 00:40:96:af:3e:93-96:af

Fri Oct 5 15:47:38 2007: ****Enter processIncomingMessages: response code=11
Fri Oct 5 15:47:38 2007: ****Enter processRadiusResponse: response code=11
Fri Oct 5 15:47:38 2007: 00:40:96:af:3e:93 Access-Challenge received from RADIUS server 10.77.244.196 for mobile 00:40:96:af:3e:93 receiveId = 3
Fri Oct 5 15:47:38 2007: 00:40:96:af:3e:93 Successful transmission of Authentication Packet (id 133) to 10.77.244.196:1812, proxy state 00:40:96:af:3e:93-96:af

Fri Oct 5 15:47:38 2007: ****Enter processIncomingMessages: response code=2
Fri Oct 5 15:47:38 2007: ****Enter processRadiusResponse: response code=2
Fri Oct 5 15:47:38 2007: 00:40:96:af:3e:93 Access-Accept received from RADIUS server 10.77.244.196 for mobile 00:40:96:af:3e:93 receiveId = 3
Fri Oct 5 15:47:38 2007: 00:40:96:af:3e:93 Applying new AAA override for station 00:40:96:af:3e:93
Fri Oct 5 15:47:38 2007: 00:40:96:af:3e:93 Override values for station 00:40:96:af:3e:93
    source: 4, valid bits: 0x200
    qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1
    dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
    vlanIfName: vlanIfNa
me: vlan20, acl
Fri Oct 5 15:47:38 2007: 00:40:96:af:3e:93 Inserting new RADIUS override into chain for station 00:40:96:af:3e:93
Fri Oct 5 15:47:38 2007: 00:40:96:af:3e:93 Override values for station 00:40:96:af:3e:93
    source: 4, valid bits: 0x200
    qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1
    dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
    vlanIfName: vlanIfNa
me: 'sales', acl
Fri Oct 5 15:47:38 2007: 00:40:96:af:3e:93 Applying override policy from source
Override Summation:
Fri Oct 5 15:47:38 2007: 00:40:96:af:3e:93 Override values for station 00:40:96:af:3e:93
```

```

        source: 256, valid bits: 0x200
        qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1

        dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
                                                    vlanIfNa
me: 'sales', a
Fri Oct 5 15:47:39 2007: 00:40:96:af:3e:93 Sending Accounting request (0) for
station 00:40:96:af:3e:93

```

As seen from this debug output, the WLC passed on the authentication requests and responses between the wireless client and RADIUS server 10.77.244.196. The server has successfully authenticated the wireless client (this can be verified using the **Access-Accept** message). Upon successful authentication, you can also see the RADIUS server transmitting the **VLAN interface name:vlan20**, therefore dynamically assigning the wireless client into VLAN20.

- **debug dot1x aaa enable** This command is used to debug entire dot1x authentication that takes place between the wireless client and the authentication server (ACS).
- **debug aaa all enable** Configures debug of all AAA messages.

Here is the output of this command based on this document's example configuration:

```

(Cisco Controller) >Fri Oct 5 16:17:18 2007: AuthenticationRequest: 0xac4be5c
Fri Oct 5 16:17:18 2007: Callback.....0x829a960
Fri Oct 5 16:17:18 2007: protocolType.....0x0040001
Fri Oct 5 16:17:18 2007: proxyState.....00:40:96:AF:3E:93-07:00
Fri Oct 5 16:17:18 2007: Packet contains 12 AVPs (not shown)
Fri Oct 5 16:17:18 2007: 00:40:96:af:3e:93 Successful transmission of
Authentication Packet (id 137) to 10.77.244.196:1812,
proxy state 00:40:96:af:3e:93-96:af
.....
.....
.....
Fri Oct 5 16:17:18 2007: ****Enter processIncomingMessages: response code=11
Fri Oct 5 16:17:18 2007: ****Enter processRadiusResponse: response code=11
Fri Oct 5 16:17:18 2007: 00:40:96:af:3e:93 Access-Challenge received from RADIUS
server 10.77.244.196 for mobile 00:40:96:af:3e:93 receiveId = 7
Fri Oct 5 16:17:18 2007: AuthorizationResponse: 0x9845500
Fri Oct 5 16:17:18 2007: structureSize.....130
Fri Oct 5 16:17:18 2007: resultCode.....255
Fri Oct 5 16:17:18 2007: protocolUsed.....0x0000001
Fri Oct 5 16:17:18 2007: proxyState.....00:40:96:AF:3E:93-07:00
Fri Oct 5 16:17:18 2007: Packet contains 3 AVPs (not shown)
.....
.....
.....
Fri Oct 5 16:17:18 2007: ****Enter processIncomingMessages: response code=11
Fri Oct 5 16:17:18 2007: ****Enter processRadiusResponse: response code=11
Fri Oct 5 16:17:18 2007: 00:40:96:af:3e:93 Access-Challenge received from
RADIUS server 10.77.244.196 for mobi)
Fri Oct 5 16:17:18 2007: 00:40:96:af:3e:93 Successful transmission of
Authentication Packet (id 139) to 10.77.244.196:1812,
proxy state 00:40:96:af:3e:93-96:af
Fri Oct 5 16:17:18 2007: 00000000: 01 8b 00 bb 54 4c 75 3a e5 b9 d2 c0 28 f2 9
3 b3 ....TLu:....(...)

```

```

Fri Oct 5 16:17:18 2007: 00000010: f2 81 50 65 01 10 77 69 72 65 6c 65 73 73 5
c 75 ..Pe..lab\wireless123
Fri Oct 5 16:17:18 2007: 00000020: 73 65 72 31 1f 13 30 30 2d 34 30 2d 39 36 2
d 41 ser1..00-40-96-A
Fri Oct 5 16:17:18 2007: 00000030: 46 2d 33 45 2d 39 33 1e 18 30 30 2d 30 42 2
d 38 F-3E-93..00-0B-8
Fri Oct 5 16:17:18 2007: 00000040: 35 2d 35 42 2d 46 42 2d 44 30 3a 41 44 53 3
1 05 5-5B-FB-D0:wireless123.
Fri Oct 5 16:17:18 2007: 00000050: 06 00 00 00 01 04 06 0a 4d f4 d4 20 06 57 4
c 43 .....M...WLC
Fri Oct 5 16:17:18 2007: 00000060: 31 1a 0c 00 00 37 63 01 06 00 00 00 02 06 0
6 00 1....7c.....
Fri Oct 5 16:17:18 2007: 00000070: 00 00 02 0c 06 00 00 05 14 3d 06 00 00 00 1
3 4f .....=.....O
Fri Oct 5 16:17:18 2007: 00000080: 20 01 05 00 1e 11 01 00 08 85 8e 81 b0 7d b
f ee .....}..
Fri Oct 5 16:17:18 2007: 00000090: b1 77 69 72 65 6c 65 73 73 5c 75 73 65 72 3
1 18 .lab\wireless123
.....
.....
Fri Oct 5 16:17:18 2007: 00000050: 31 1a 3b 00 00 00 09 01 35 6c 65 61 70 3a 7
3 65 l.;....5leap:se
Fri Oct 5 16:17:18 2007: 00000060: 73 73 69 6f 6e 2d 6b 65 79 3d 84 e7 c5 3c 3
3 bd ssion-key=...<3.
Fri Oct 5 16:17:18 2007: 00000070: a8 bf 7a 43 9d 6e bb c8 a8 2c 5d c6 91 d6 f
3 21 ..zC.n...,]....!
Fri Oct 5 16:17:18 2007: 00000080: df 1e 0e 28 c1 ef a5 31 a7 cd 62 da 1a 1f 0
0 00 ...(...1..b....
Fri Oct 5 16:17:18 2007: 00000090: 00 09 01 19 61 75 74 68 2d 61 6c 67 6f 2d 7
4 79 ....auth-algo-ty
Fri Oct 5 16:17:18 2007: 000000a0: 70 65 3d 65 61 70 2d 6c 65 61 70 19 17 43 4
1 43 pe=eap-leap..CAC
.....
.....
Fri Oct 5 16:17:18 2007: ****Enter processIncomingMessages: response code=2
Fri Oct 5 16:17:18 2007: ****Enter processRadiusResponse: response code=2
Fri Oct 5 16:17:18 2007: 00:40:96:af:3e:93 Access-Accept received from RADIUS
server 10.77.244.196 for mobile 00:40:96:af:3e:93 receiveId = 7
Fri Oct 5 16:17:18 2007: AuthorizationResponse: 0x9845500
Fri Oct 5 16:17:18 2007: structureSize.....228

Fri Oct 5 16:17:18 2007: resultCode.....0
Fri Oct 5 16:17:18 2007: protocolUsed.....0x0
0000001
Fri Oct 5 16:17:18 2007: proxyState.....00:
40:96:AF:3E:93-07:02
Fri Oct 5 16:17:18 2007: Packet contains 5 AVPs:
Fri Oct 5 16:17:18 2007: AVP[01] Airespace / Interface-Name.....
.....vlan20 (5 bytes)
Fri Oct 5 16:17:18 2007: AVP[02] EAP-Message.....
.....DATA (46 bytes)
Fri Oct 5 16:17:18 2007: AVP[03] Cisco / LEAP-Session-Key.....
.....DATA (16 bytes)
Fri Oct 5 16:17:18 2007: AVP[04] Class.....
.....CACS:0/5943/a4df4d4/1 (21 bytes)
Fri Oct 5 16:17:18 2007: AVP[05] Message-Authenticator.....
.....DATA (16 bytes)
Fri Oct 5 16:17:18 2007: 00:40:96:af:3e:93 Applying new AAA override for
station 00:40:96:af:3e:93
Fri Oct 5 16:17:18 2007: 00:40:96:af:3e:93 Override values for station 00:40:96
:af:3e:93
source: 4, valid bits: 0x200
qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1
dataAvgC: -1, rTavgC: -1, dataBurstC: -1, rTimeBurstC: -1

```

```

vlanIfNa
me: 'sales', acl
Fri Oct 5 16:17:18 2007: 00:40:96:af:3e:93 Inserting new RADIUS override into
chain for station 00:40:96:af:3e:93
Fri Oct 5 16:17:18 2007: 00:40:96:af:3e:93 Override values for station 00:40:96
:af:3e:93
        source: 4, valid bits: 0x200
        qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1
        dataAvgC: -1, rTAvGc: -1, dataBurstC: -1, rTimeBurstC: -1
vlanIfNa
me: 'sales', acl
Fri Oct 5 16:17:18 2007: 00:40:96:af:3e:93 Applying override policy from source
Override Summation:
Fri Oct 5 16:17:18 2007: 00:40:96:af:3e:93 Override values for station 00:40:96
:af:3e:93
        source: 256, valid bits: 0x200
        qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1
        dataAvgC: -1, rTAvGc: -1, dataBurstC: -1, rTimeBurstC: -1
vlanIfNa
me: 'sales', a
Fri Oct 5 16:17:18 2007: 00:40:96:af:3e:93 Sending Accounting request (0) for
station 00:40:96:af:3e:93
Fri Oct 5 16:17:18 2007: AccountingMessage Accounting Interim: 0xac4b1f0
Fri Oct 5 16:17:18 2007: Packet contains 20 AVPs:
Fri Oct 5 16:17:18 2007: AVP[01] User-Name.....
.....lab\wireless123 (14 bytes)
Fri Oct 5 16:17:18 2007: AVP[02] Nas-Port.....
.....0x00000001 (1) (4 bytes)
Fri Oct 5 16:17:18 2007: AVP[03] Nas-Ip-Address.....
.....0x0a4df4d4 (172881108) (4 bytes)
Fri Oct 5 16:17:18 2007: AVP[04] Class.....
.....CACs:0/5943/a4df4d4/1 (21 bytes)
Fri Oct 5 16:17:18 2007: AVP[05] NAS-Identifier.....
.....0x574c4331 (1464615729) (4 bytes)
Fri Oct 5 16:17:18 2007: AVP[06] Airespace / WLAN-Identifier.....
.....0x00000002 (2) (4 bytes)
.....
.....
.....

```

---

## Related Information

- [EAP Authentication with RADIUS Server](#)
  - [Windows Server 2003 Active Directory Diagnostics, Troubleshooting, and Recovery](#)
  - [Troubleshooting Active Directory Operations](#)
  - [Cisco LEAP](#)
  - [Cisco Wireless LAN Controller Configuration Guide, Release 4.0](#)
  - [Cisco Airespace VSAs on Cisco Secure ACS Server Configuration Example](#)
  - [Lightweight AP \(LAP\) Registration to a Wireless LAN Controller \(WLC\)](#)
  - [User Guide for Cisco Secure Access Control Server 4.1](#)
  - [Technical Support & Documentation – Cisco Systems](#)
-

