Per User ACL with Wireless LAN Controllers and Cisco Secure ACS Configuration Example

Document ID: 98590

Introduction

This document explains through an example how to create access control lists (ACLs) on the WLCs and apply them to users dependent upon RADIUS authorization.

Prerequisites

Requirements

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

- Basic knowledge of how to configure a Cisco Secure ACS server to authenticate Wireless Clients
- Knowledge of the configuration of Cisco Aironet Lightweight Access Points (LAPs) and Cisco Wireless LAN Controllers (WLCs)
- Knowledge of Cisco Unified Wireless Security Solutions

Components Used

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

- Cisco 4400 Series Wireless LAN Controller that runs Version 5.0.148.0
- Cisco Aironet 1231 series Lightweight Access Points (LAPs)
- Cisco Aironet 802.11 a/b/g Cisco Wireless LAN client adapter that runs Version 3.6
- Cisco Aironet Desktop Utility Version 3.6

- Cisco Secure ACS Server Version 4.1
- Cisco 2800 Series Integrated Services Router that runs IOS® Version 12.4(11)T
- Cisco Catalyst 2900XL Series Switch that runs Version 12.0(5)WC3b

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 the Cisco Technical Tips Conventions for more information on document conventions.

Background Information

The per user Access Control List (ACL) is part of Cisco Identity networking. Cisco Wireless LAN Solution supports identity networking, which, while it allows the network to advertise a single SSID, it also allows specific users to inherit different policies based on their user profiles.

The per user ACL feature provides the ability to apply an ACL configured on the Wireless LAN Controller to a user based on the RADIUS authorization. This is accomplished with the Airespace−ACL−Name Vendor Specific Attribute (VSA).

This attribute indicates the ACL name to be applied to the client. When the ACL attribute is present in the RADIUS Access Accept, the system applies the ACL−Name to the client station after it authenticates. This overrides any ACLs that are assigned to the interface. It ignores the assigned interface−ACL and applies the new one.

A summary of the ACL−Name Attribute format is shown below. The fields are transmitted from left to right

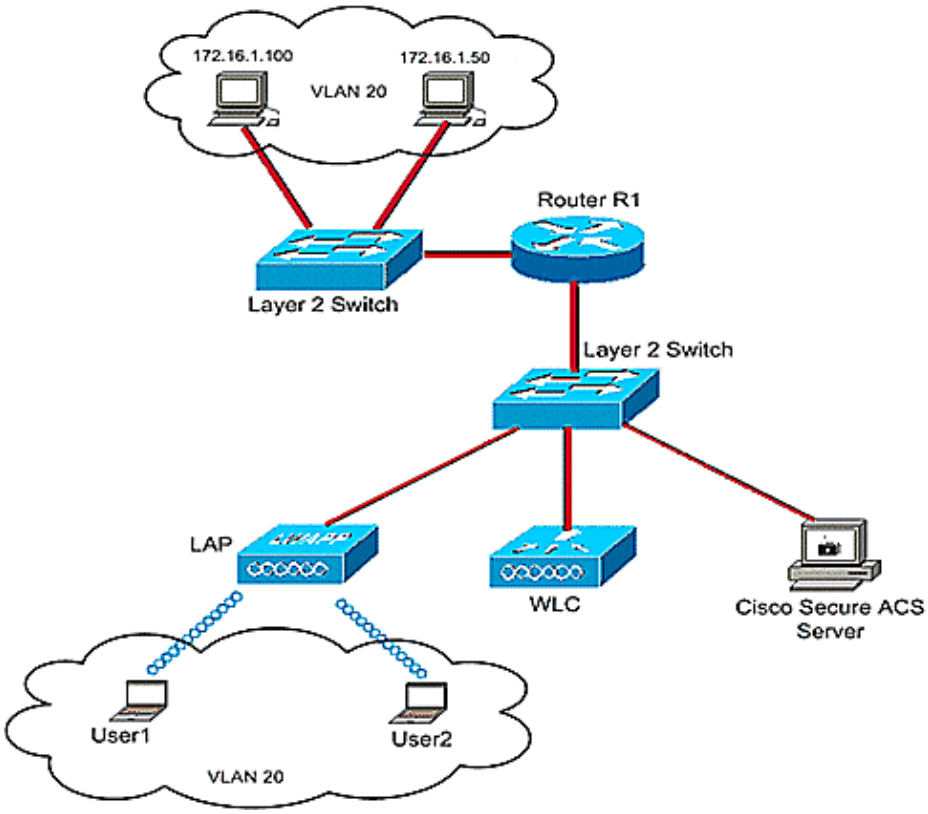
```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |  Length       |            Vendor-Id
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     Vendor-Id (cont.)          | Vendor type   | Vendor length |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        ACL Name...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
" Type − 26 for Vendor-Specific
" Length − >7
" Vendor-Id − 14179
" Vendor type − 6
" Vendor length − >0
" Value − A string that includes the name of the ACL to use for the client.
   The string is case sensitive.
```

For more information on the Cisco Unified Wireless Network Identity Networking, refer to the Configuring Identity Networking section of the document Configuring Security Solutions.

Network Diagram

This document uses this network setup:

In this setup, the Wireless LAN Controller WLC and LAP are used to provide wireless services to the users in Department A and Department B. All the wireless users use a common WLAN (SSID) Office to access the network and are in the VLAN Office−VLAN.



The Cisco Secure ACS server is used to authenticate wireless users. EAP authentication is used to authenticate users. The WLC, LAP, and Cisco Secure ACS server are connected with a Layer 2 Switch as shown.

Router R1 connects the servers on the wired side through the Layer 2 Switch as shown. Router R1 also acts as a DHCP server, which provides IP addresses to wireless clients from subnet 172.16.0.0/16.

You need to configure the devices so that this occurs:

User1 from Department A has access only to server 172.16.1.100

User2 from Department B has access only to server 172.16.1.50

In order to accomplish this, you need to create 2 ACLs on the WLC: one for User1, and the other for User2. Once the ACLs are created, you need to configure the Cisco Secure ACS server to return the ACL name attribute to the WLC upon successful authentication of the Wireless user. The WLC then applies the ACL to the user, and thus to the network is restricted dependent upon the user profile.

Note: This document uses LEAP authentication for authenticating users. Cisco LEAP is vulnerable to dictionary attacks. In real time networks, more secure authentication methods such as EAP FAST should be used. Since the focus of the document is to explain how to configure Per User ACL feature, LEAP is used for simplicity.

The next section provides the step−by−step instruction to configure the devices for this setup.

Configure

Before you configure the per user ACLs feature, you must configure the WLC for basic operation and register the LAPs to the WLC. This document assumes that the WLC is configured for basic operation and that the LAPs are registered to the WLC. If you are a new user, who tries to set up the WLC for basic operation with

LAPs, refer to Lightweight AP (LAP) Registration to a Wireless LAN Controller (WLC).

Once the LAPs are registered, complete these steps to configure the devices for this setup:

1. Configure the Wireless LAN Controller.
2. Configure the Cisco Secure ACS server.
3. Verify the configuration.

Note: This document discusses the configuration required on the Wireless side. The document assumes that the wired configuration is in place.

Configure the Wireless LAN Controller

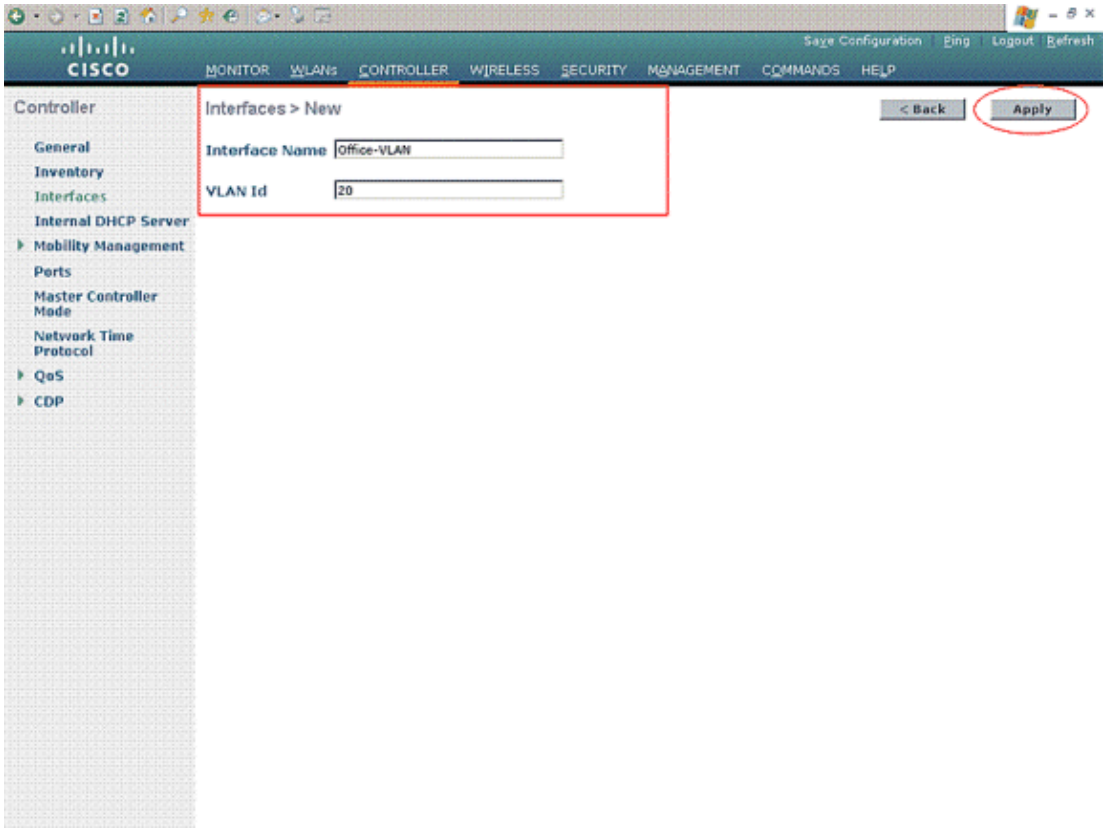
On the Wireless LAN Controller, you need to do this:

- Create a VLAN for the wireless users.
- Configure the WLC to authenticate wireless users with Cisco Secure ACS.
- Create a new WLAN for the wireless users.
- Define the ACLs for the wireless users.

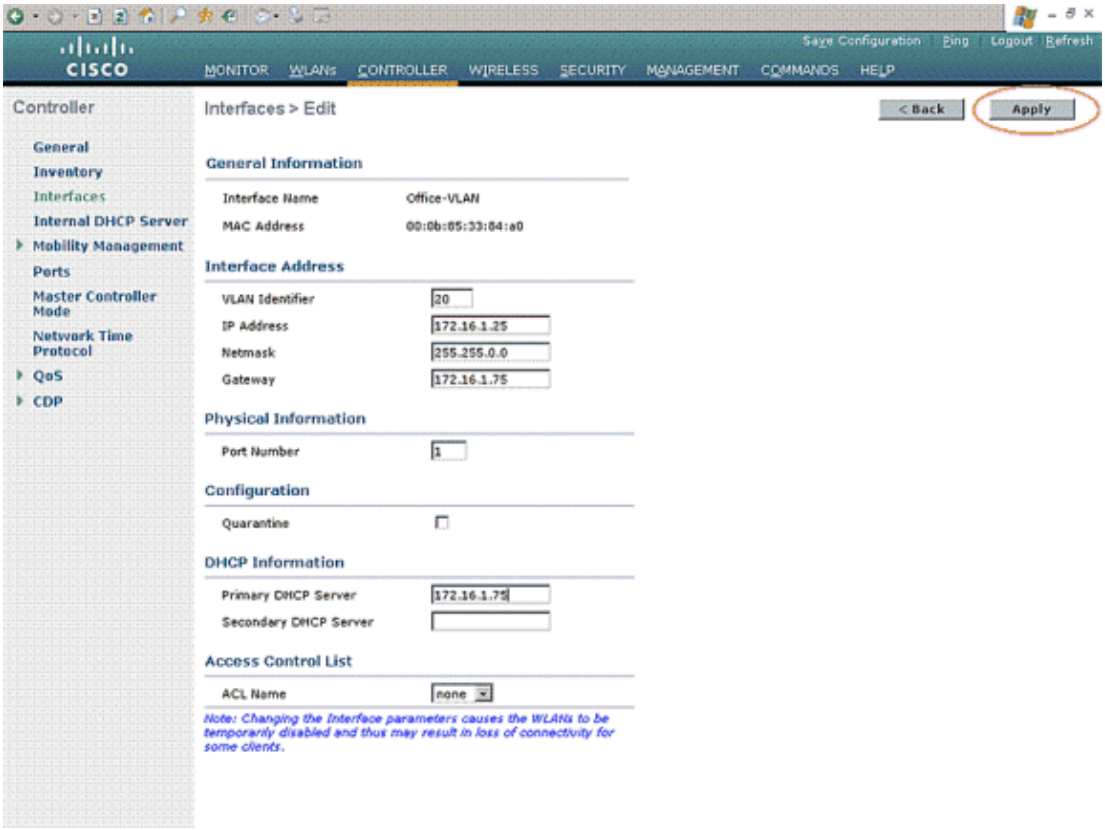
Create a VLAN for the Wireless Users

In order to create a VLAN for the wireless users, complete these steps.

1. Go to the WLC GUI and choose **Controller > Interfaces**. The Interfaces window appears. This window lists the interfaces that are configured on the controller.
2. Click **New** in order to create a new dynamic interface.
3. In the **Interfaces > New** window, enter the Interface Name and the VLAN ID. Then click Apply. In this example, the dynamic interface is named Office−VLAN, and the VLAN ID is assigned 20.



4. In the **Interfaces > Edit** window, enter the IP address, the subnet mask, and the default gateway for the dynamic interface. Assign it to a physical port on the WLC, and enter the IP address of the DHCP server. Then click **Apply**.



For this example, these parameters are used for the Office−VLAN interface:

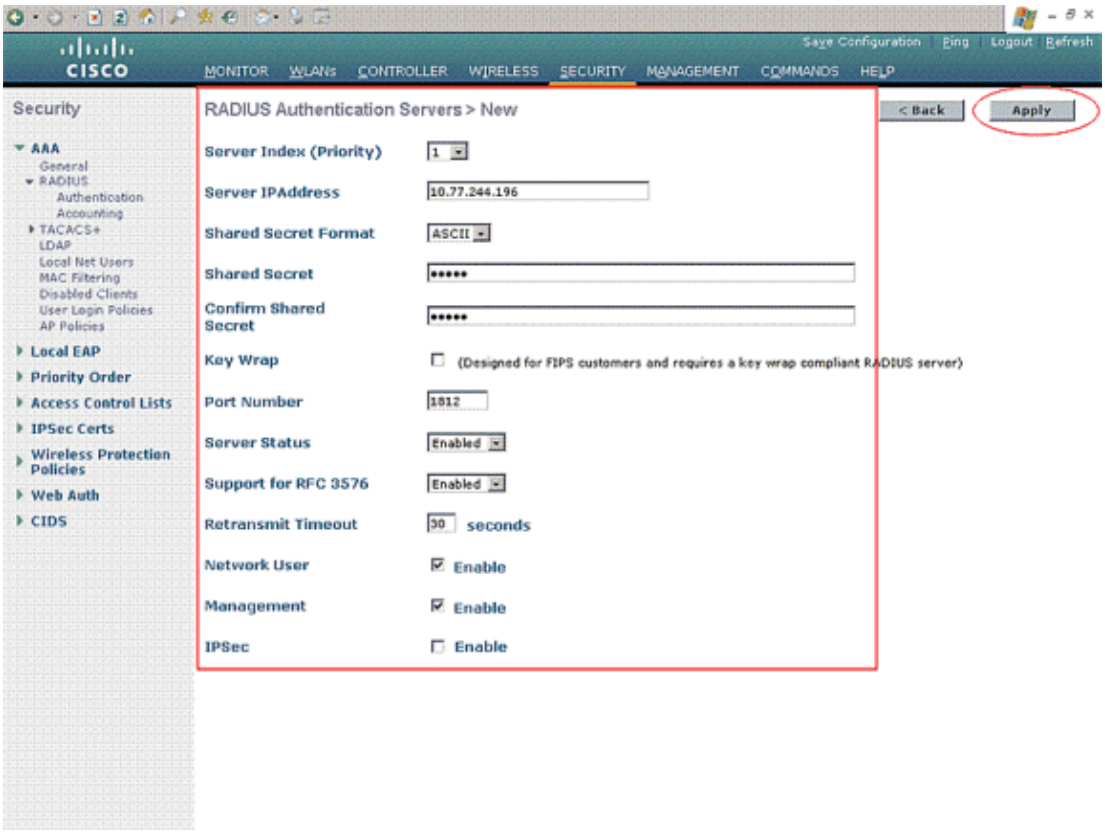
```
Office−VLAN
        IP address: 172.16.1.25
        Netmask: 255.255.0.0
        Default gateway: 172.16.1.75 (sub−interface on Router R1)
        Port on WLC: 1
        DHCP server: 172.16.1.75
```

Configure the WLC to Authenticate with Cisco Secure ACS

The WLC needs to be configured in order to forward the user credentials to an external RADIUS server (in this case, the Cisco Secure ACS). The RADIUS server then validates the user credentials and returns the ACL name attribute to the WLC upon successful authentication of the wireless user.

Complete these steps in order to configure the WLC for the RADIUS server:

1. Choose **Security** and **RADIUS Authentication** from the controller GUI to display the **RADIUS Authentication Servers** page. Then click **New** in order to define a RADIUS server.
2. Define the RADIUS server parameters in the **RADIUS Authentication Servers > New** page. These parameters include the RADIUS Server IP Address, Shared Secret, Port Number, and Server Status.

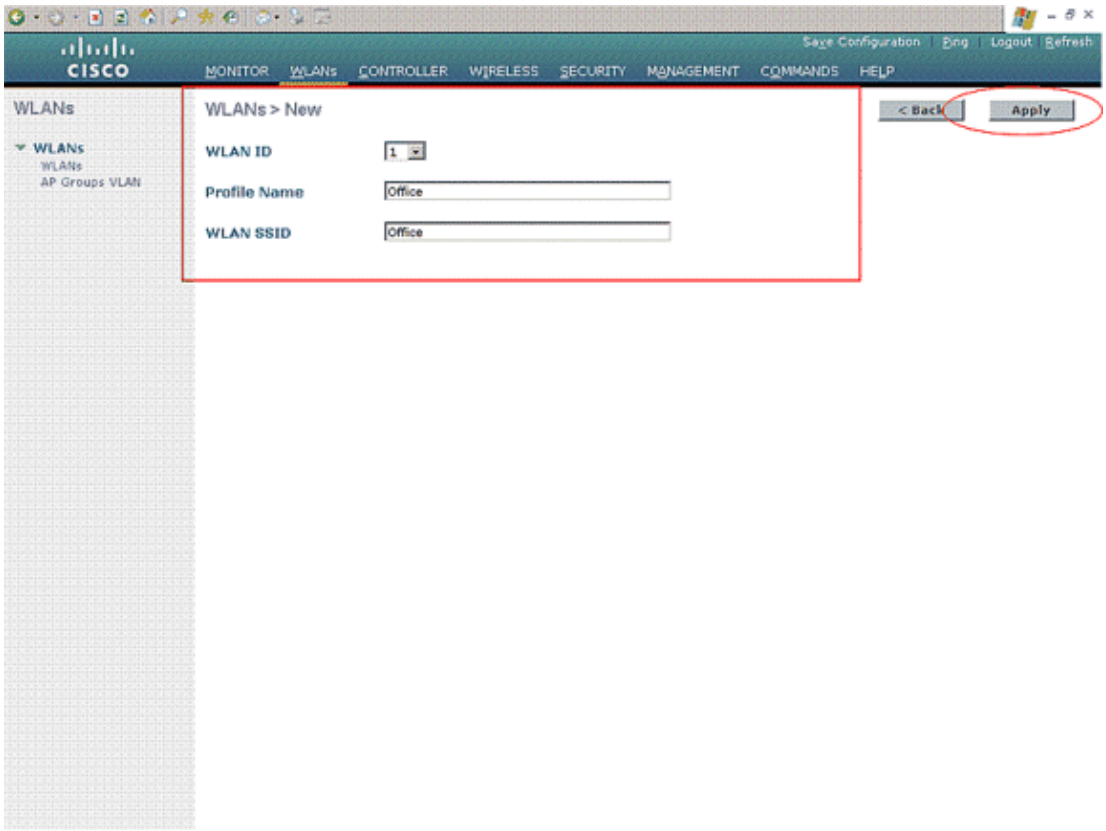


3. The **Network User** and **Management** check boxes determine if the RADIUS−based authentication applies for management and network users. This example uses the Cisco Secure ACS as the RADIUS server with IP address 10.77.244.196. Click **Apply**.

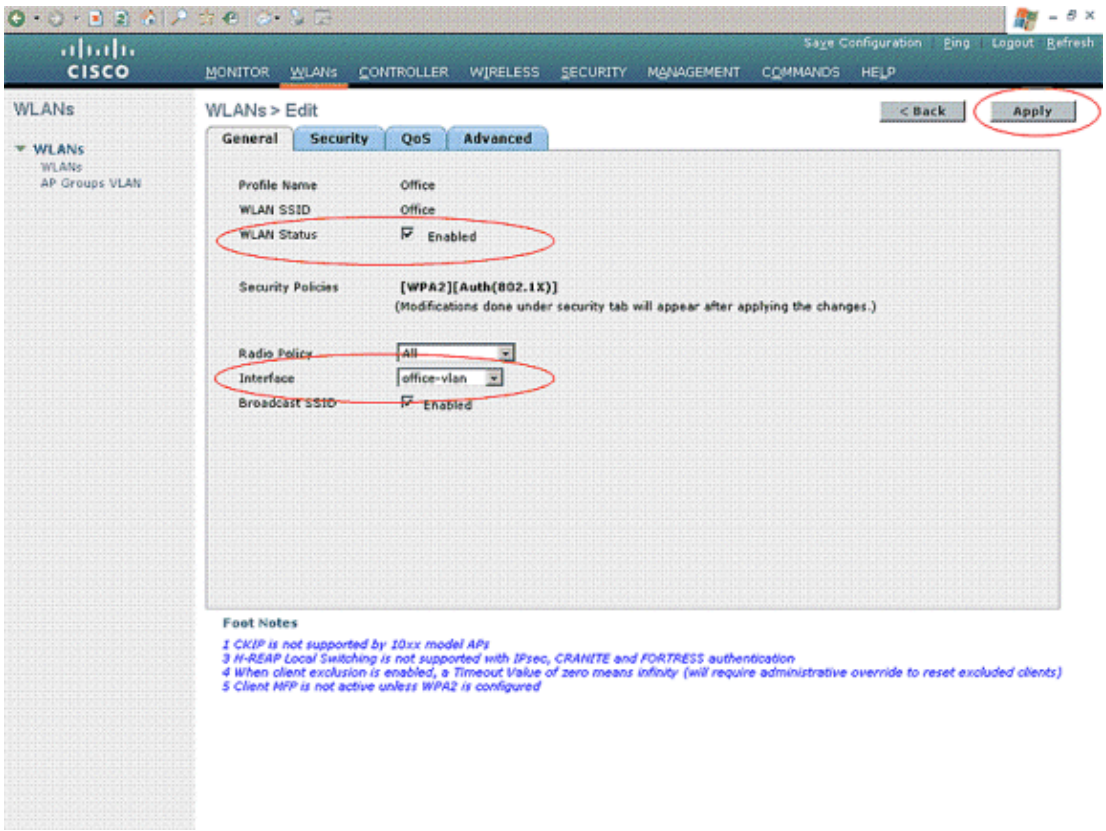
Create a New WLAN for the Wireless Users

Next, you need to create a WLAN to which the wireless users can connect. In order to create a new WLAN, complete these steps:

1. From the Wireless LAN Controller GUI, click **WLANs**. This page lists the WLANs that exist on the controller.
2. Choose **New** in order to create a new WLAN. Enter the WLAN ID, Profile Name, and the WLAN SSID for the WLAN, and click **Apply**. For this setup, create a WLAN **Office**.



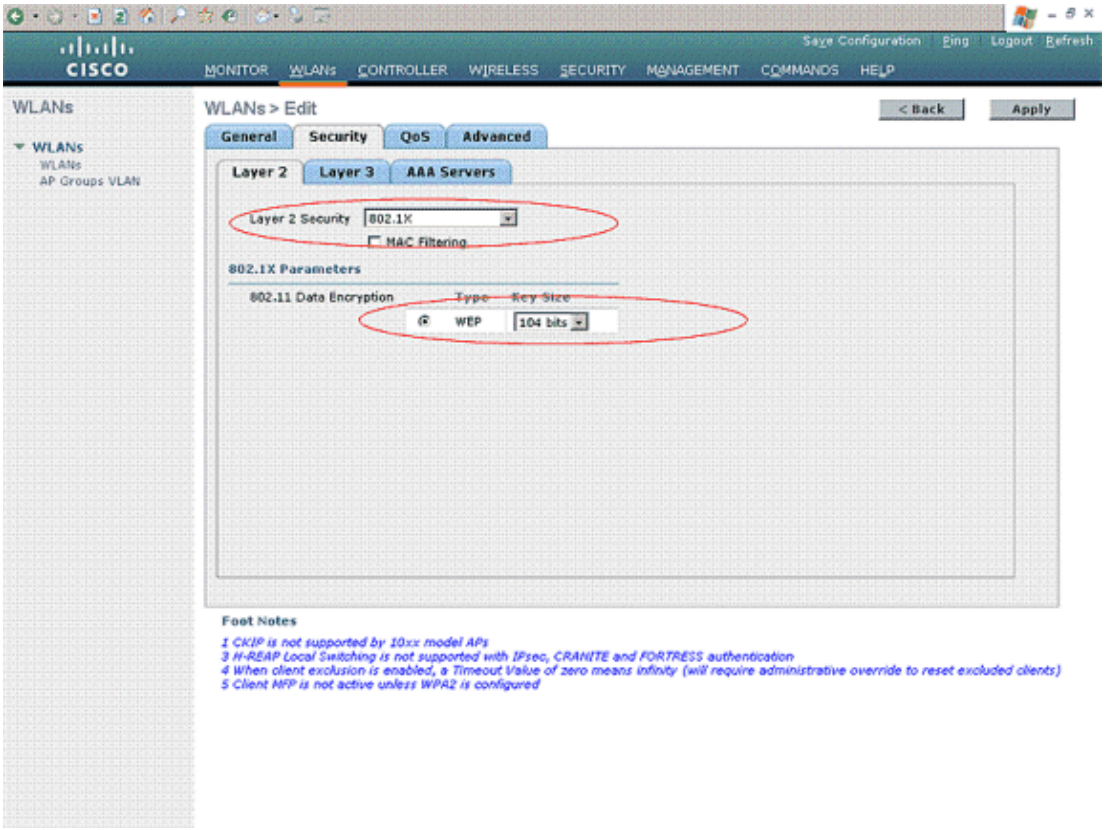
3. Once you create a new WLAN, the **WLAN > Edit** page for the new WLAN appears. In this page, you can define various parameters specific to this WLAN that includes General policies, Security, QoS, and Advanced parameters.



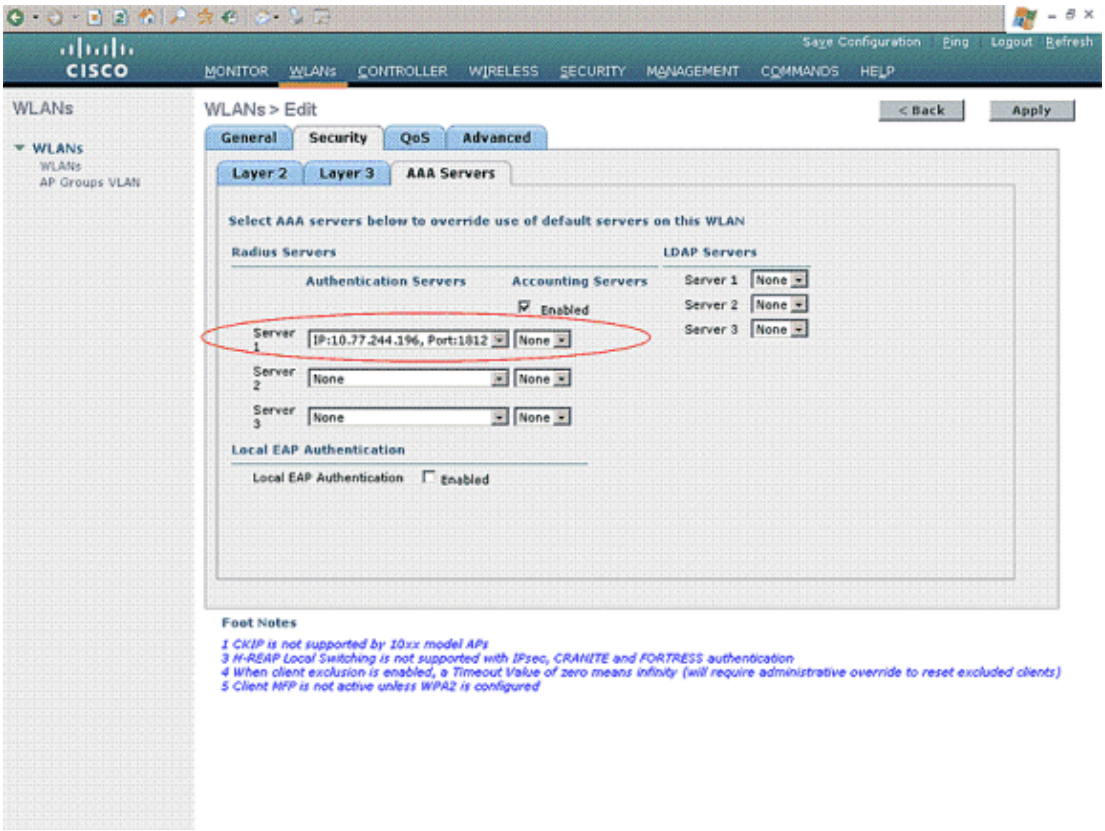
Check **WLAN Status** under General policies in order to enable the WLAN. Choose the appropriate interface from the pull−down menu. In this example, use the interface **Office−vlan**. The other

parameters on this page can be modified based on the requirement of the WLAN network.

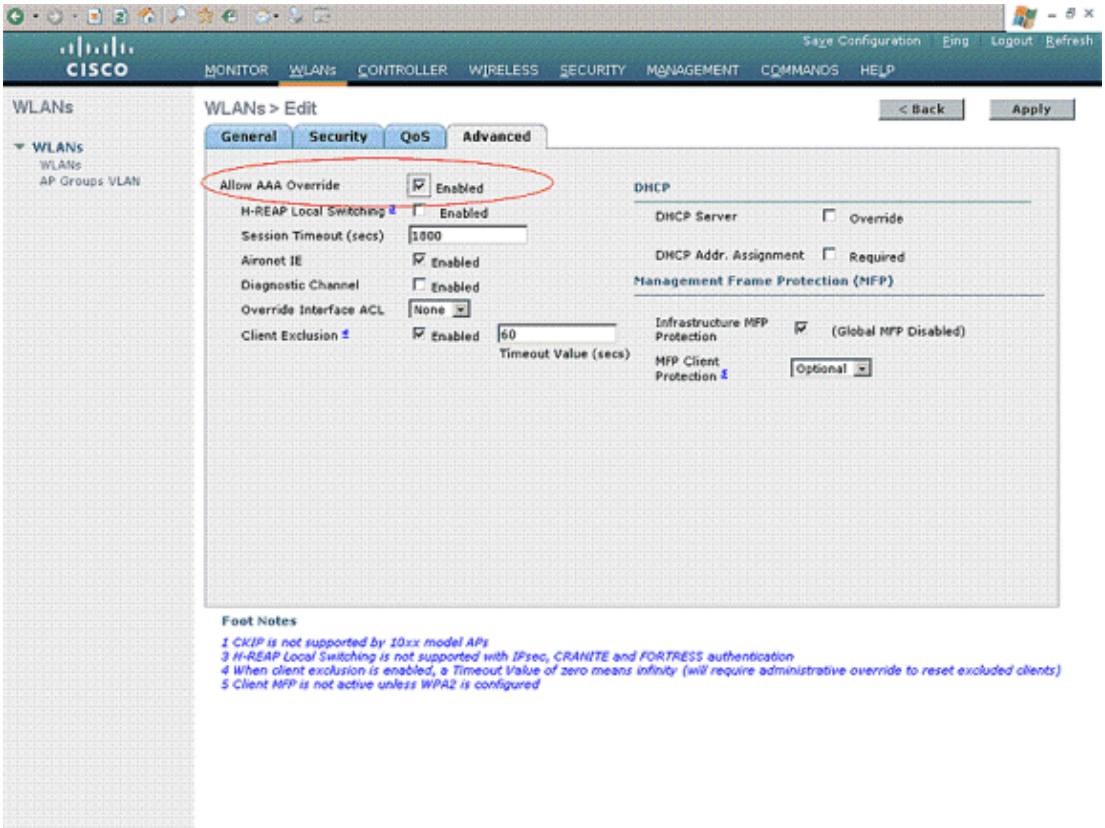
4. Choose the **Security tab**. Choose **802.1x** from the Layer 2 security pull−down menu (since this is a LEAP authentication). Choose the appropriate WEP key size under 802.1x parameters.



5. Under the Security tab, choose the **AAA server** sub−tab. Choose the AAA server that is used to authenticate wireless clients. In this example, use ACS server 10.77.244.196 to authenticate wireless clients.



6. Choose the **Advanced** tab. Check **Allow AAA Override** to configure user policy override through the AAA on a wireless LAN.



When AAA override is enabled, and a client has conflicting AAA and Cisco Wireless LAN controller wireless LAN authentication parameters, then client authentication is performed by the AAA server. As part of this authentication, the operating system moves clients from the default Cisco wireless

LAN solution wireless LAN VLAN to a VLAN returned by the AAA server and predefined in the Cisco Wireless LAN controller interface configuration, which only happenswhen configured for MAC filtering, 802.1X, and/or WPA operation. In all cases, the operating system also uses QoS, DSCP, 802.1p priority tag values and ACL provided by the AAA server, as long as they are predefined in the Cisco Wireless LAN controller interface configuration.

7. Choose the other parameters based on the requirements of the network. Click **Apply**.

Define the ACLs for the Users

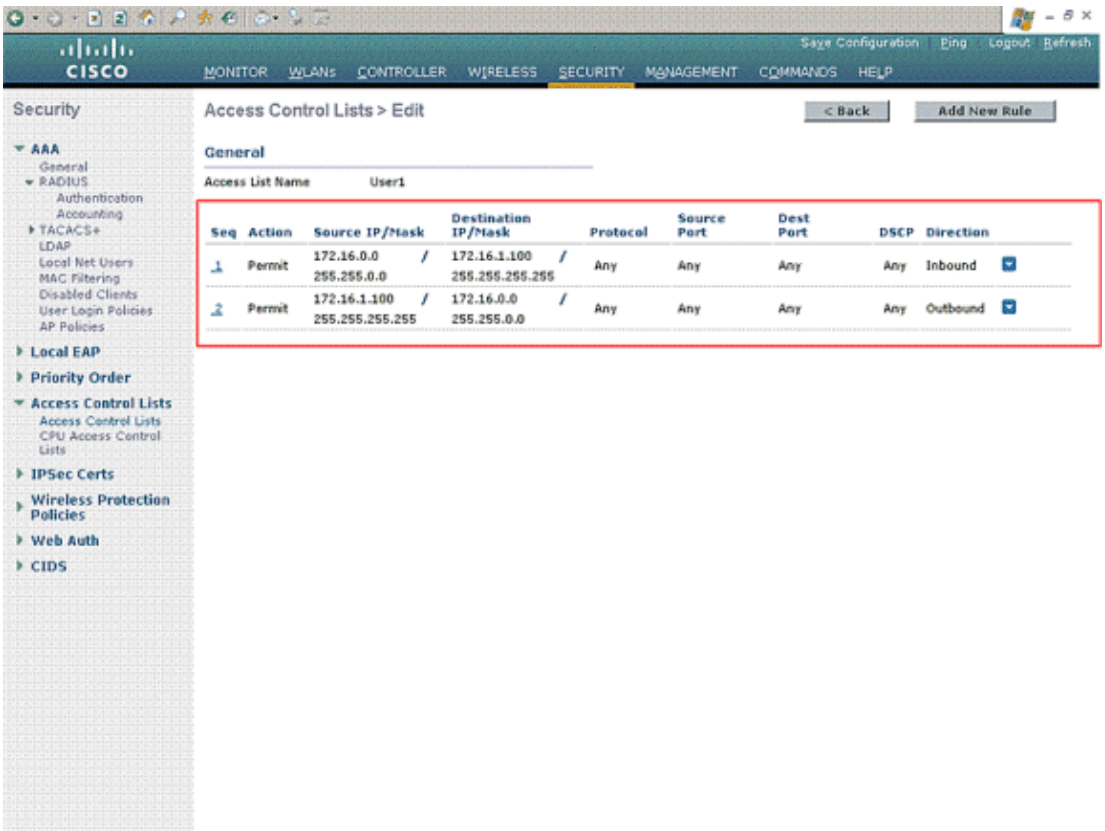
You need to create two ACLs for this setup:

- ACL1: In order to provide access to User1 to the server 172.16.1.100 only
- ACL2: In order to provide access to User2 to the server 172.16.1.50 only

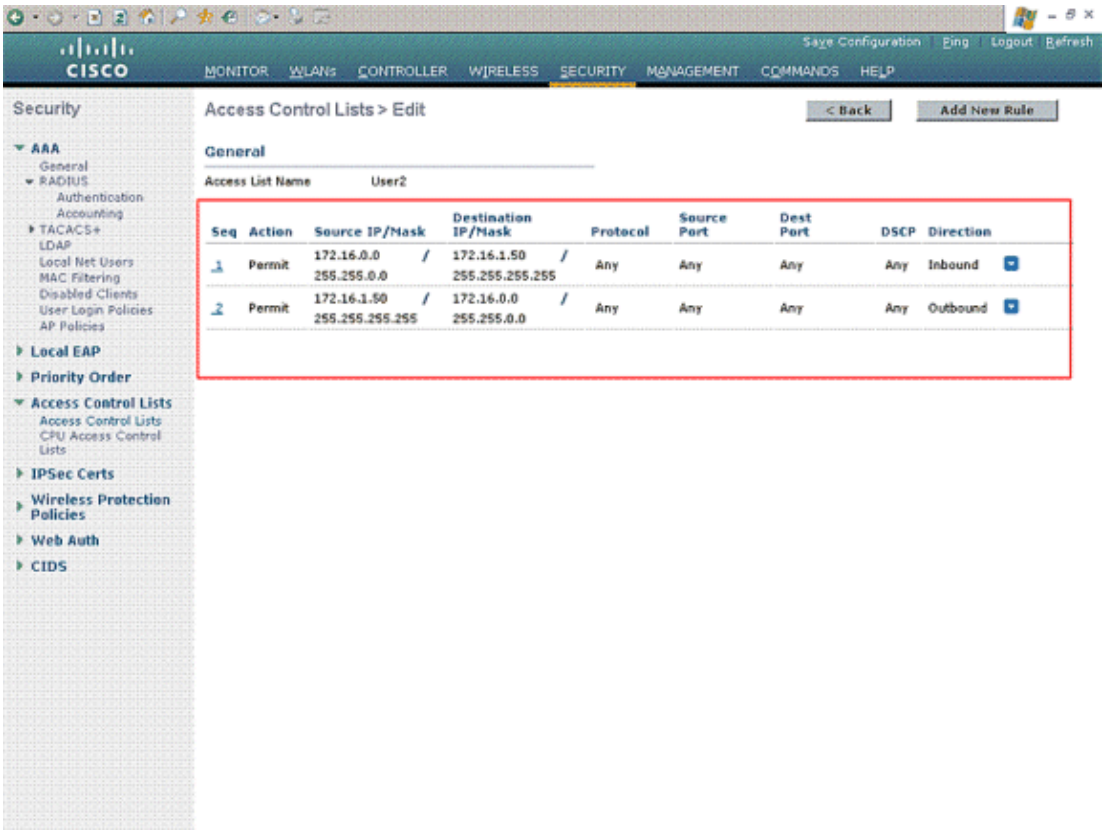
Complete these steps to configure the ACLs on the WLC:

1. From the WLC GUI, choose **Security > Access Control Lists**. The Access Control Lists page appears. This page lists the ACLs that are configured on the WLC. It also enables you to edit or remove any of the ACLs. In order to create a new ACL, click **New**.
2. This page allows you to create new ACLs. Enter the name of the ACL and click **Apply**. Once the ACL is created, click **Edit** in order to create rules for the ACL.
3. User1 needs to be able to access server 172.16.1.100 only and must be denied access to all other devices. For this, you need to define these rules.

   Refer to the ACLs on Wireless LAN Controller Configuration Example for more information on how to configure ACLs on Wireless LAN Controllers.



4. Similarly, you need to create an ACL for User2, which allows User2 access to server 172.16.1.50 only. This is the ACL required for User2.



You have now configured the Wireless LAN Controller for this setup. The next step is to configure the Cisco Secure Access Control server to authenticate the wireless clients and to return the ACL Name attribute to the WLC upon successful authentication.

Configure the Cisco Secure ACS Server

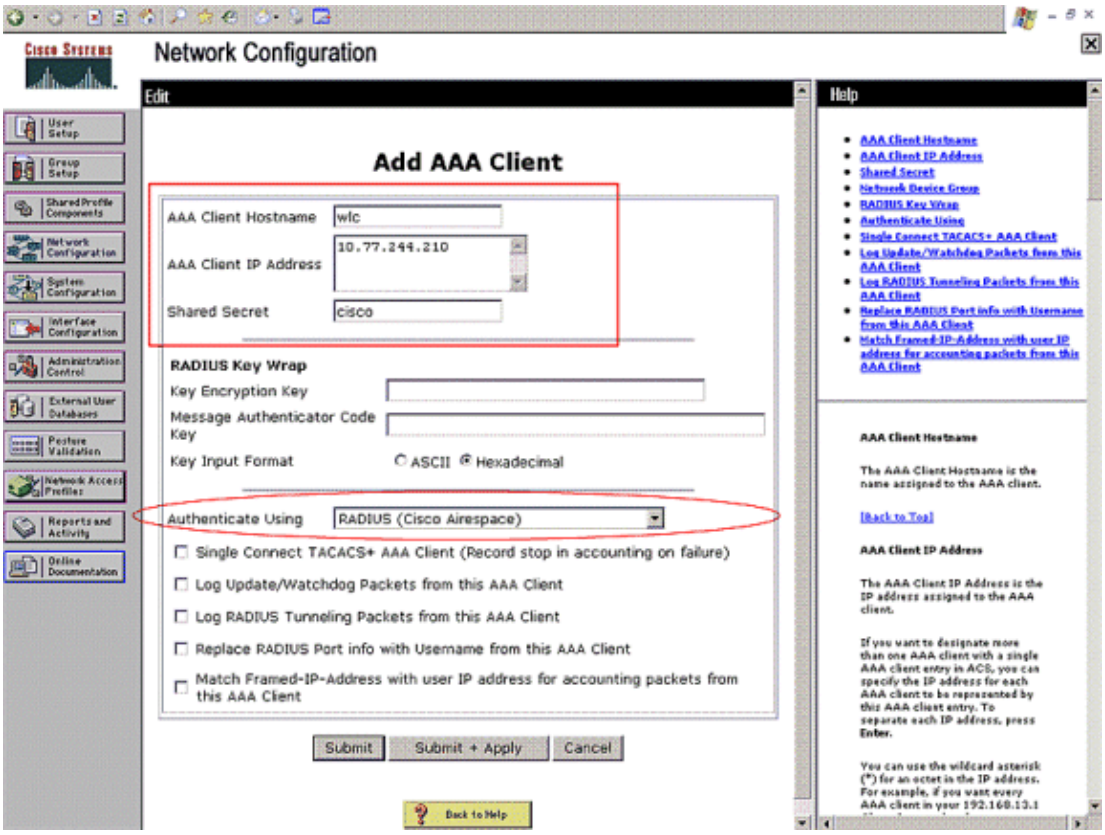
For the Cisco Secure ACS to be able to authenticate Wireless clients, you need to complete these steps:

- Configure the Wireless LAN Controller as a AAA client on the Cisco Secure ACS.
- Configure the users and user profiles on the Cisco Secure ACS.

Configure the Wireless LAN Controller as a AAA Client on the Cisco Secure ACS

In order to configure the Wireless LAN Controller as an AAA client on the Cisco Secure ACS, complete these steps:

1. Click **Network Configuration > Add AAA client**. The **Add AAA client** page appears. In this page, define the WLC system name, Management Interface IP address, Shared Secret, and Authenticate Using **Radius Airespace**. Here is an example:



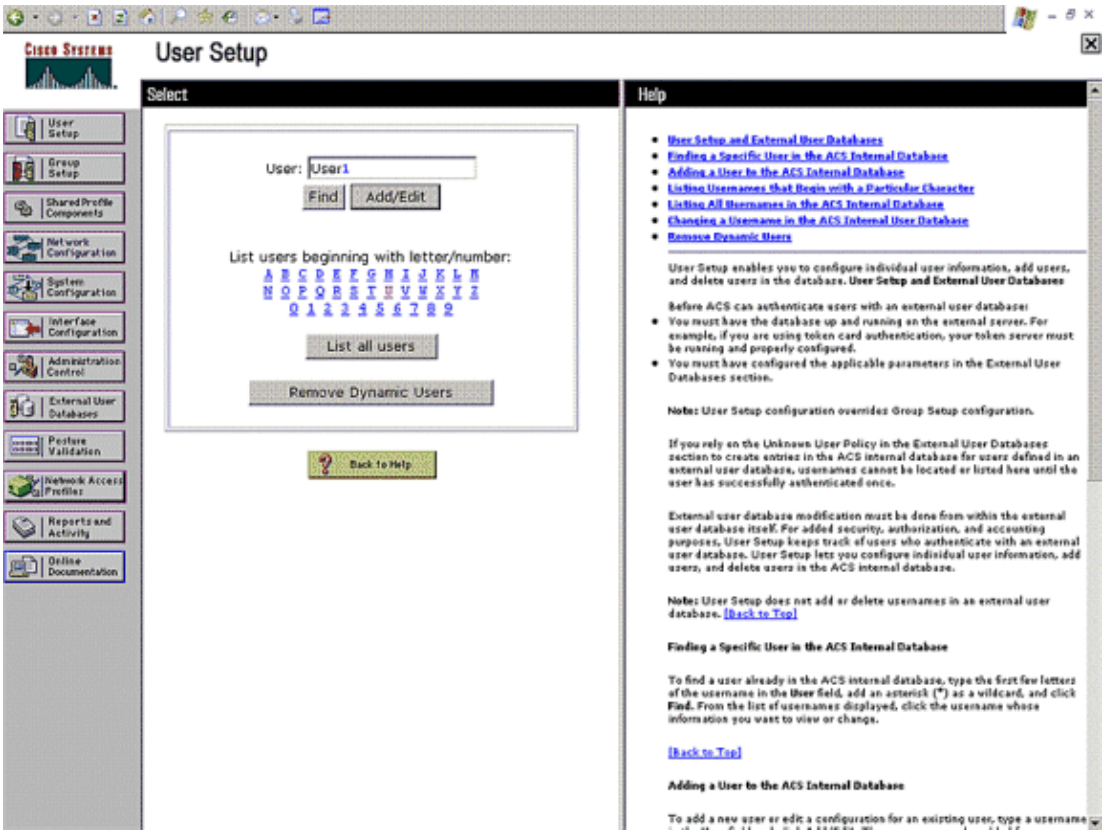
Note: The shared secret configured on the Cisco Secure ACS must match the shared secret configured on the WLC under **RADIUS Authentication Servers > New**.

2. Click **Submit+Apply**.

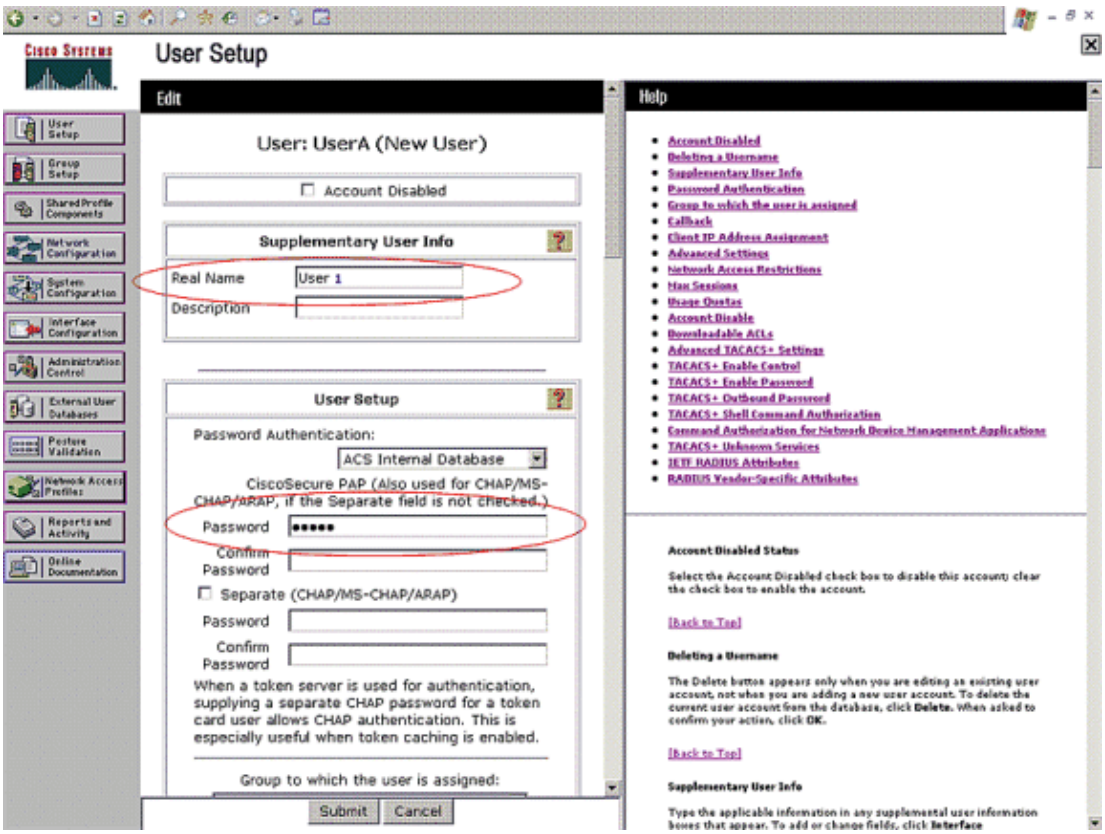
Configure Users and User Profile on the Cisco Secure ACS

In order to configure users on the Cisco Secure ACS, complete these steps:

1. Choose **User Setup** from the ACS GUI, enter the username, and click **Add/Edit**. In this example, the user is **User1**.

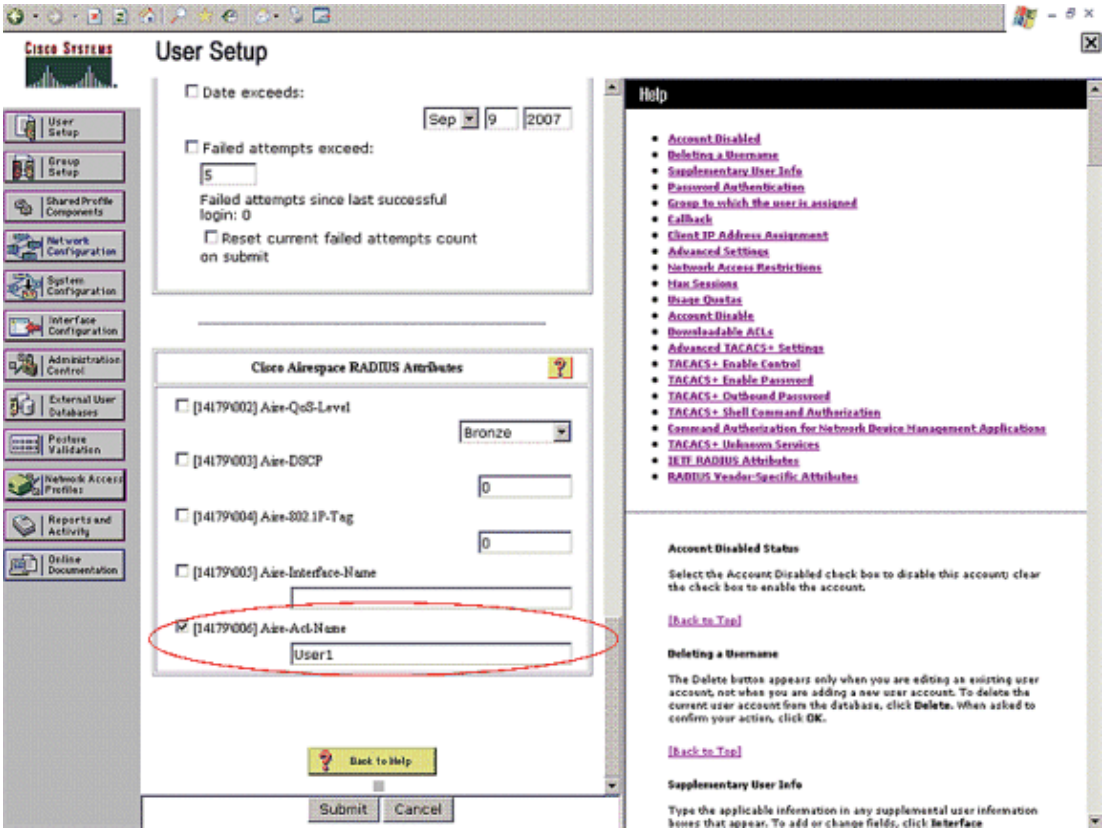


2. When the **User Setup** page appears, define all parameters specific to the user. In this example, the username, password, Supplementary User Information, and the RADIUS attributes are configured because you only need these parameters for EAP authentication.

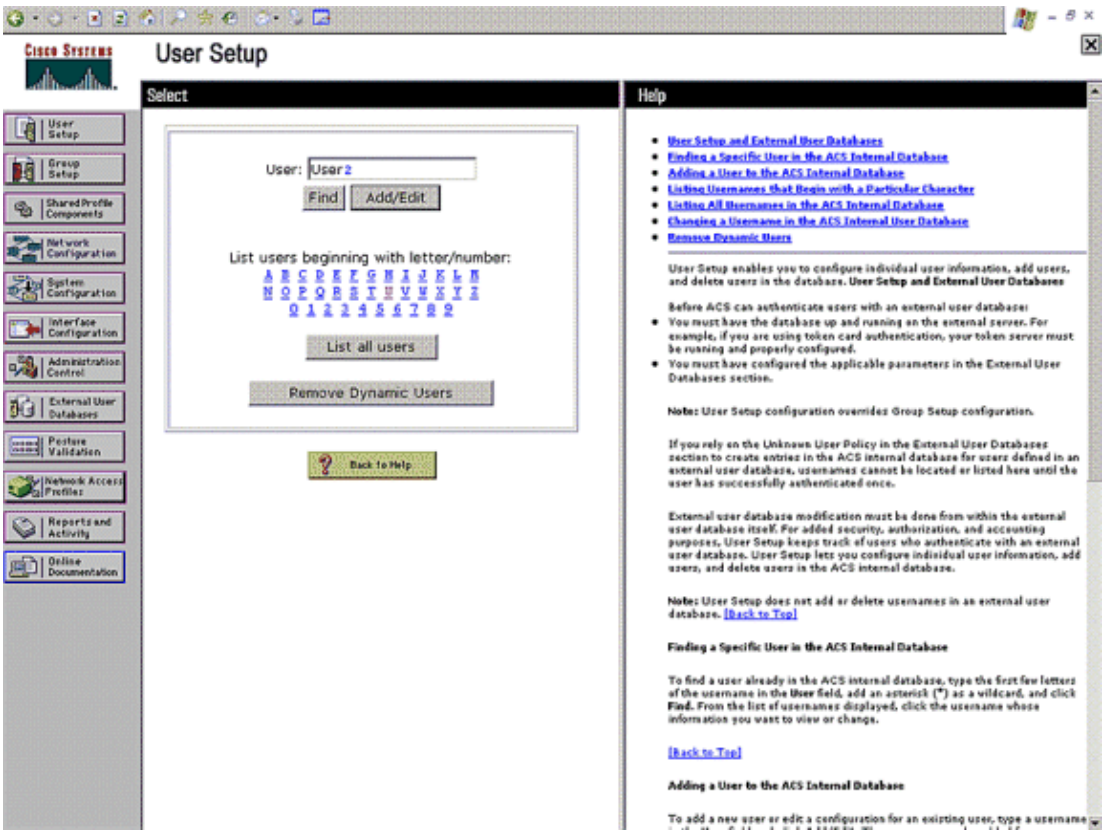


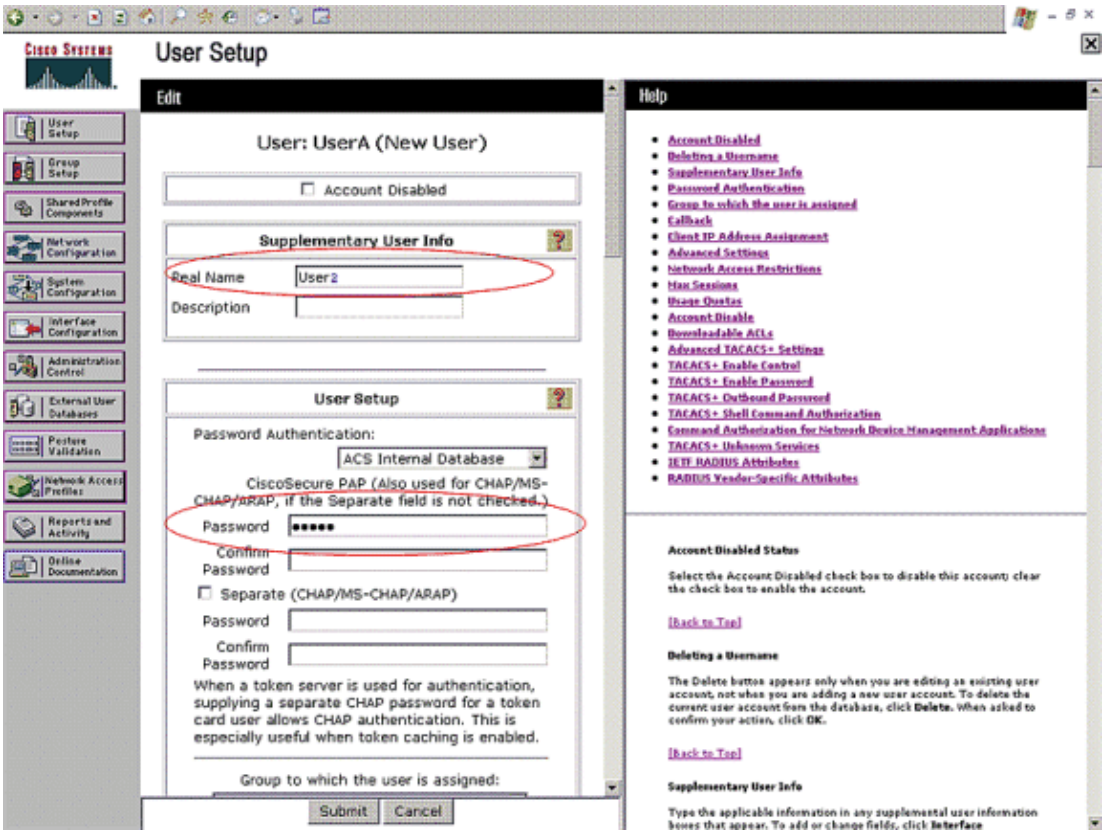
Scroll down until you see the Cisco Airespace RADIUS Attributes specific to the user. Check the **Aire−ACL−Name** to enable the ACS to return the ACL name to the WLC along with the successful

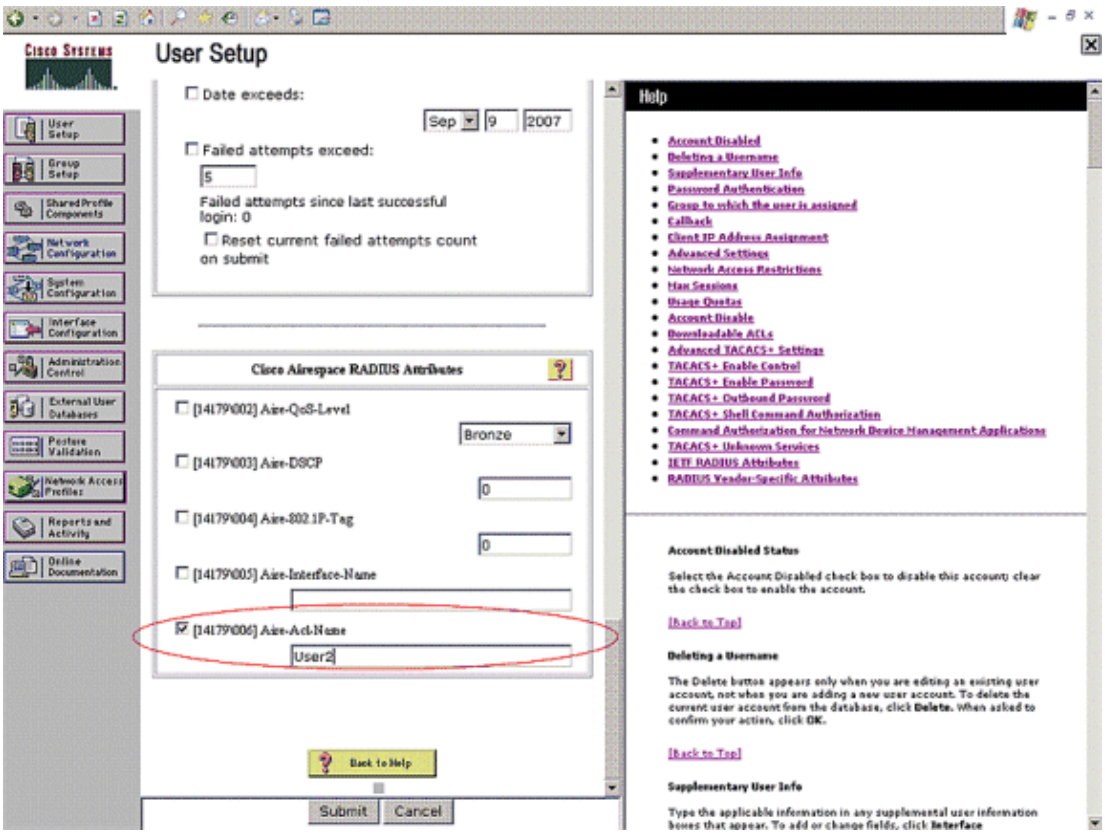
authentication response. For User1, create an ACL User1 on the WLC. Input the ACL name as User1.



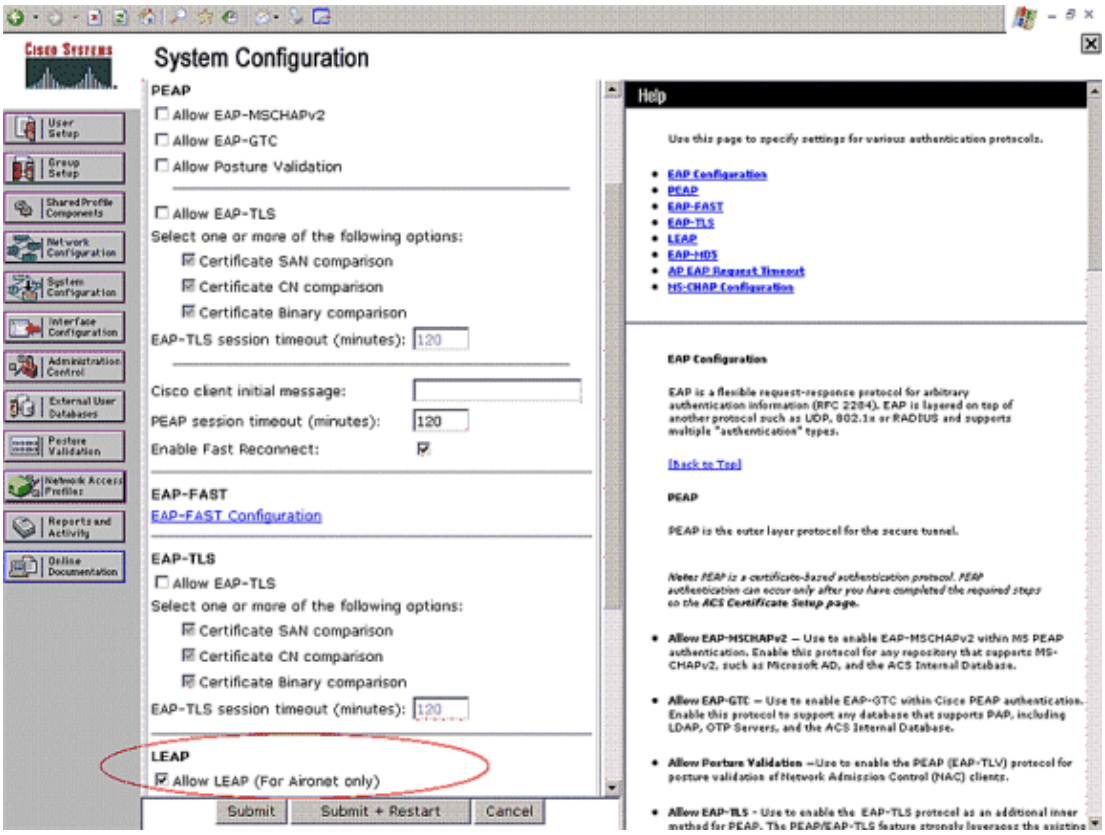
3. Repeat the same procedure to create User2 as shown here.







4. Click **System Configuration** and **Global Authentication Setup** in order to ensure that the authentication server is configured to perform the desired EAP authentication method. Under the EAP configuration settings, choose the appropriate EAP method. This example uses LEAP authentication. Click **Submit** when you are done.



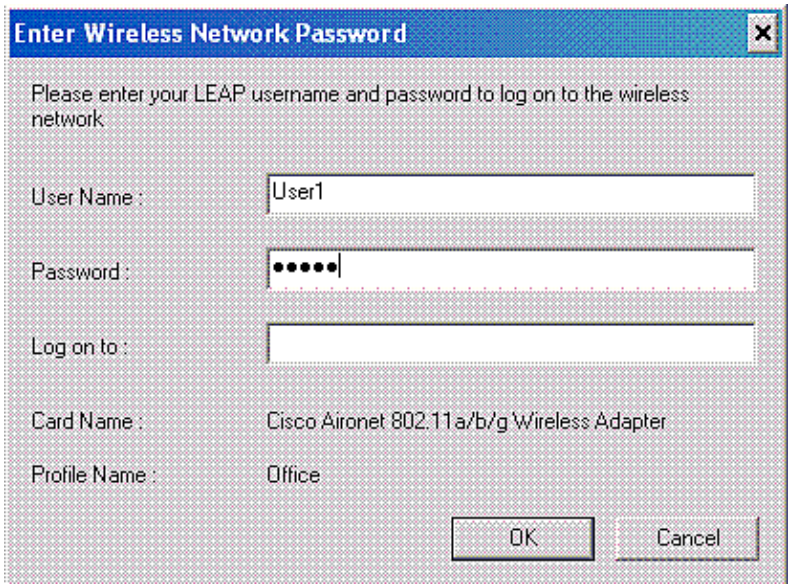
Verify

Use this section to confirm that your configuration works properly.

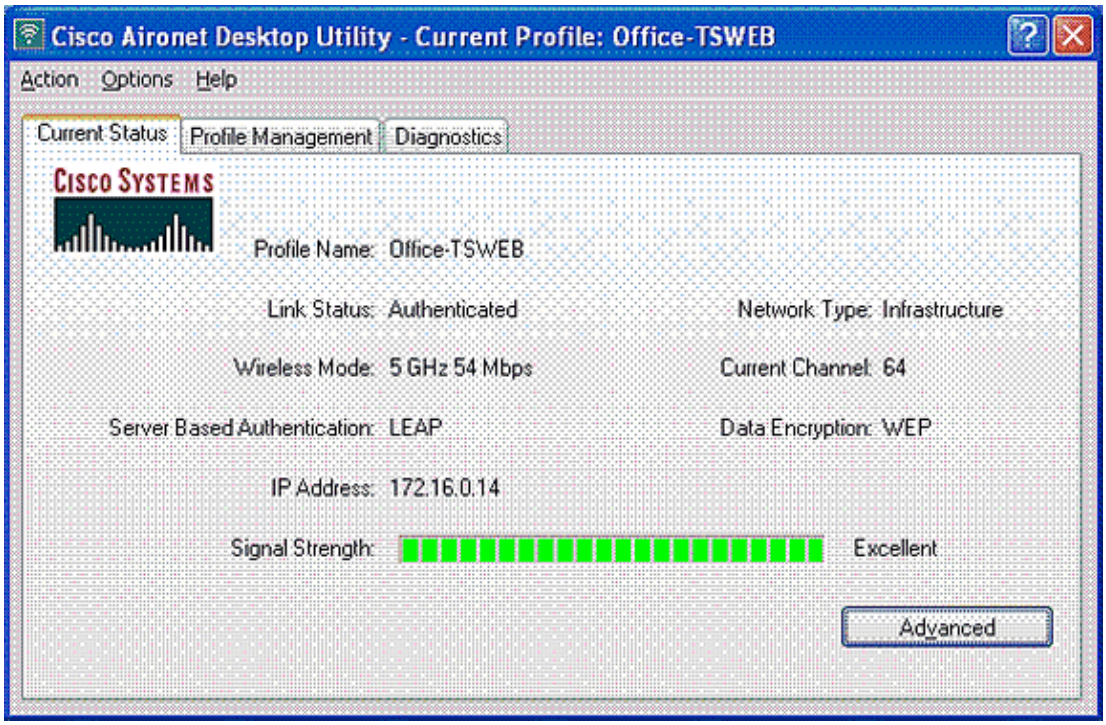
Try to associate a wireless client with the Lightweight AP with LEAP authentication in order to verify whether the configuration works as expected.

Note: This document assumes that the client profile is configured for LEAP authentication. Refer to Using EAP Authentication for more information on how to configure the 802.11 a/b/g Wireless Client Adapter for LEAP authentication.

Once the profile for the wireless client is activated, the user is asked to provide the username/password for LEAP authentication. This is what happens when User1 tries to authenticate to the LAP.



The Lightweight AP and then the WLC pass on the user credentials to the external RADIUS server (Cisco Secure ACS) in order to validate the credentials. The RADIUS server compares the data with the user database and, upon successful authentication, returns the ACL name configured for the user to the WLC. In this case, the ACL User1 is returned to the WLC.

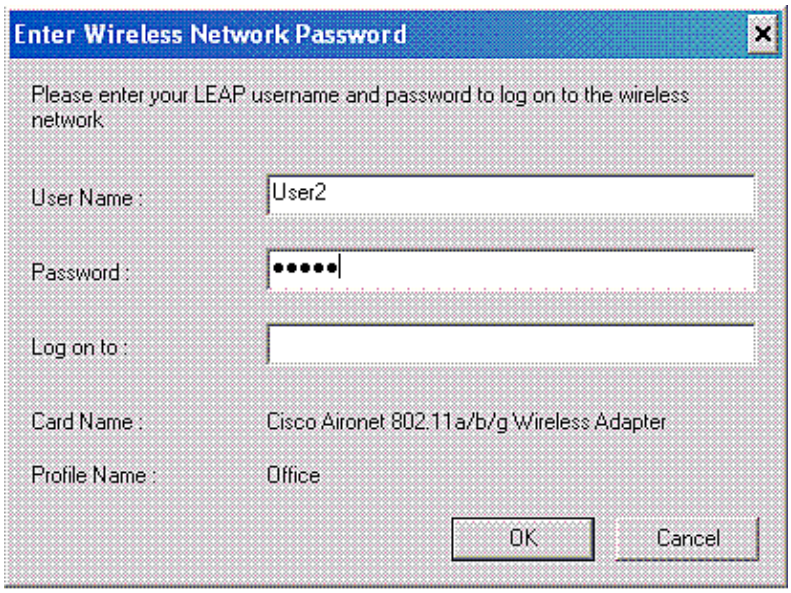


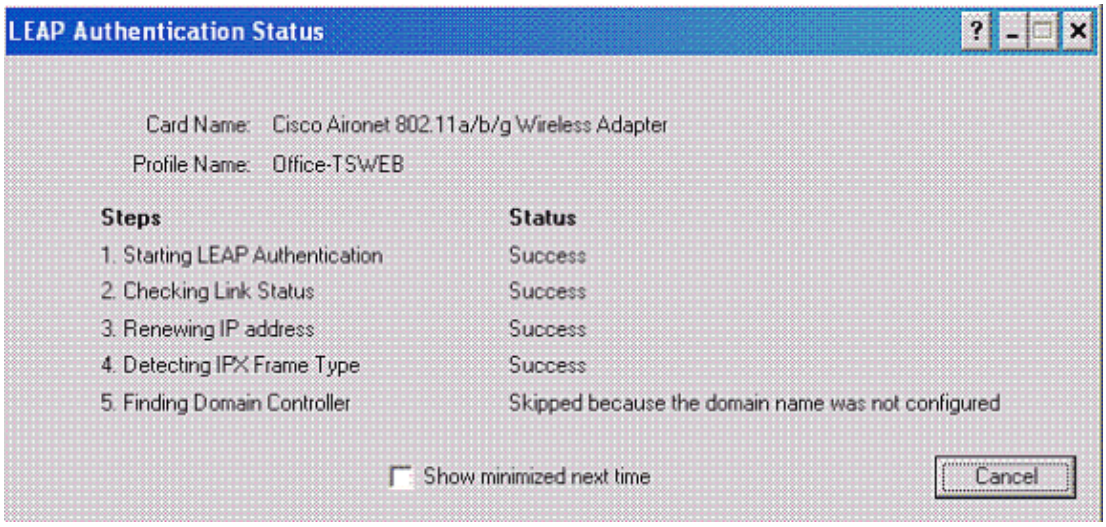
The Wireless LAN Controller applies this ACL to User1. This ping output shows that User1 is able to access only server 172.16.1.100, but not any other device.

```
D:\Documents and Settings\Administrator>ping 172.16.1.100

Pinging 172.16.1.100 with 32 bytes of data:

Reply from 172.16.1.100: bytes=32 time=3ms TTL=255
Reply from 172.16.1.100: bytes=32 time=1ms TTL=255
Reply from 172.16.1.100: bytes=32 time=1ms TTL=255
Reply from 172.16.1.100: bytes=32 time=1ms TTL=255
```

```
Ping statistics for 172.16.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 3ms, Average = 1ms

D:\Documents and Settings\Administrator>ping 172.16.1.50

Pinging 172.16.1.50 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.16.1.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (100% loss),
```

Similarly, when User2 tries to access the WLAN, the RADIUS server, upon successful authentication, returns the ACL User2 to the WLC.





The Wireless LAN Controller applies this ACL to User2. This ping output shows that User2 is able to access only server 172.16.1.50, but not any other device.

```
D:\Documents and Settings\Administrator>ping 172.16.1.50
```

```
Pinging 172.16.1.50 with 32 bytes of data:

Reply from 172.16.1.50: bytes=32 time=3ms TTL=255
Reply from 172.16.1.50: bytes=32 time=18ms TTL=255
Reply from 172.16.1.50: bytes=32 time=1ms TTL=255
Reply from 172.16.1.50: bytes=32 time=1ms TTL=255

Ping statistics for 172.16.1.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 18ms, Average = 5ms

D:\Documents and Settings\Administrator>ping 172.16.1.100

Pinging 172.16.1.100 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.16.1.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

On the Wireless LAN Controller, you can also use these debug commands in order to troubleshoot AAA authentication

- **debug aaa all enable** Configures the debug of all AAA messages
- **debug dot1x packet enable** Enables the debug of all dot1x packets
- **debug client <MAC Address>** Enables wireless client debugging

Here is an example of the **debug aaa all enable** command

Note: Some of the lines in the output have been moved to the second line due to space constraints.

```
Thu Aug 16 14:42:54 2007: AuthenticationRequest: 0xb1ab104
Thu Aug 16 14:42:54 2007:       Callback.................0x85ed228
Thu Aug 16 14:42:54 2007:       protocolType.............0x00140001
Thu Aug 16 14:42:54 2007:       proxyState...............00:40:96:AF:3E:93-03:01
Thu Aug 16 14:42:54 2007:       Packet contains 16 AVPs (not shown)
Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93
Successful transmission of Authentication Packet
   (id 1) to 10.77.244.196:1812, proxy state 00:40:96:af:3e:93-00:00
Thu Aug 16 14:42:54 2007: 00000000: 01 01 00 d0 2d 34 f5 99  b4 19 27 28 eb 5f 35 9c
   ....-4....'(._5.
Thu Aug 16 14:42:54 2007: 00000010: 8f a9 00 dd 01 07 75 73  65 72 31 1f 13 30 30 2d
   ......user1..00-
Thu Aug 16 14:42:54 2007: 00000020: 34 30 2d 39 36 2d 41 46  2d 33 45 2d 39 33 1e 20
   40-96-AF-3E-93..
Thu Aug 16 14:42:54 2007: 00000030: 30 30 2d 30 42 2d 38 35  2d 35 42 2d 46 42 2d 44
   00-0B-85-5B-FB-D
Thu Aug 16 14:42:54 2007: 00000040: 30 3a 4f 66 66 69 63 65  2d 54 53 57 45 42 05 06
   0:Office-TSWEB..
Thu Aug 16 14:42:54 2007: 00000050: 00 00 00 01 04 06 0a 4d  f4 d2 20 05 77 6c 63 1a
   .......M....wlc.
Thu Aug 16 14:42:54 2007: 00000060: 0c 00 00 37 63 01 06 00  00 00 01 06 06 00 00 00
```

```
   ...7c...........
Thu Aug 16 14:42:54 2007: 00000070: 02 0c 06 00 00 05 14 3d  06 00 00 00 13 40 06 00
   .......=.....@..
Thu Aug 16 14:42:54 2007: 00000080: 00 00 0d 41 06 00 00 00  06 51 04 32 30 4f 27 02
   ...A.....Q.20O'.
Thu Aug 16 14:42:54 2007: 00000090: 01 00 25 11 01 00 18 1d  87 9d 0b f9 dd e5 39 0d
   ..%...........9.
Thu Aug 16 14:42:54 2007: 000000a0: 2e 82 eb 17 c6 23 b7 96  dc c3 55 ff 7c 51 4e 75
   .....#....U.|QNu
Thu Aug 16 14:42:54 2007: 000000b0: 73 65 72 31 18 0a 53 56  43 3d 30 2e 31 3b 50 12
   ser1..SVC=0.1;P.
Thu Aug 16 14:42:54 2007: 000000c0: 1a d5 3b 35 5e 93 11 c0  c6 2f 5e f5 65 e9 3e 2d
   ..;5^..../^.e.>-
Thu Aug 16 14:42:54 2007: 00000000: 0b 01 00 36 8c 31 6a b4  27 e6 d4 0e 1b 8e 5d 19
   ...6.1j.'.....].
Thu Aug 16 14:42:54 2007: 00000010: 60 1c c2 16 4f 06 03 01  00 04 18 0a 53 56 43 3d
   ...O.......SVC=
Thu Aug 16 14:42:54 2007: 00000020: 30 2e 31 3b 50 12 6c fb  90 ec 48 9b fb d7 ce ca
   0.1;P.l...H.....
Thu Aug 16 14:42:54 2007: 00000030: 3b 64 93 10 fe 09      ;d....
Thu Aug 16 14:42:54 2007: ****Enter processIncomingMessages: response code=11
Thu Aug 16 14:42:54 2007: ****Enter processRadiusResponse: response code=11
Thu Aug 16 14:42:54 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
Thu Aug 16 14:42:54 2007: AuthorizationResponse: 0x9c27800
Thu Aug 16 14:42:54 2007:       structureSize............104
Thu Aug 16 14:42:54 2007:       resultCode..............255
Thu Aug 16 14:42:54 2007:       protocolUsed............0x00000001
Thu Aug 16 14:42:54 2007:       proxyState..............
   00:40:96:AF:3E:93-03:01
Thu Aug 16 14:42:54 2007:       Packet contains 3 AVPs (not shown)
Thu Aug 16 14:42:54 2007: AuthenticationRequest: 0xb1ab104
Thu Aug 16 14:42:54 2007:       Callback................0x85ed228
Thu Aug 16 14:42:54 2007:       protocolType............0x00140001
Thu Aug 16 14:42:54 2007:       proxyState.........................
   00:40:96:AF:3E:93-03:02
Thu Aug 16 14:42:54 2007:       Packet contains 16 AVPs (not shown)
Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93
Successful transmission of Authentication Packet (id 2) to 10.77.244.196:1812,
proxy state 00:40:96:af:3e:93-00:00
Thu Aug 16 14:42:54 2007: 00000000: 01 02 00 c0 38 b6 b2 20  ff 5b f2 16 64 df 02 61
   ....8....[..d..a
Thu Aug 16 14:42:54 2007: 00000010: cf f5 93 4b 01 07 75 73  65 72 31 1f 13 30 30 2d
   ...K..User1..00-
Thu Aug 16 14:42:54 2007: 00000020: 34 30 2d 39 36 2d 41 46  2d 33 45 2d 39 33 1e 20
   40-96-AF-3E-93..
Thu Aug 16 14:42:54 2007: 00000030: 30 30 2d 30 42 2d 38 35  2d 35 42 2d 46 42 2d 44
   00-0B-85-5B-FB-D
Thu Aug 16 14:42:54 2007: 00000040: 30 3a 4f 66 66 69 63 65  2d 54 53 57 45 42 05 06
   0:Office..
Thu Aug 16 14:42:54 2007: 00000050: 00 00 00 01 04 06 0a 4d  f4 d2 20 05 77 6c 63 1a
   .......M....wlc.
Thu Aug 16 14:42:54 2007: 00000060: 0c 00 00 37 63 01 06 00  00 00 01 06 06 00 00 00
   ...7c...........
Thu Aug 16 14:42:54 2007: 00000070: 02 0c 06 00 00 05 14 3d  06 00 00 00 13 40 06 00
   .......=.....@..
Thu Aug 16 14:42:54 2007: 00000080: 00 00 0d 41 06 00 00 00  06 51 04 32 30 4f 17 01
   ...A.....Q.20O..
Thu Aug 16 14:42:54 2007: 00000090: 01 00 15 11 01 00 08 0f  14 05 65 1b 28 61 c9 75
   ..........e.(a.u
Thu Aug 16 14:42:54 2007: 000000a0: 73 65 72 31 18 0a 53 56  43 3d 30 2e 31 3b 50 12
   ser1..SVC=0.1;P.
Thu Aug 16 14:42:54 2007: 000000b0: 05 ba 6b af fe a4 b0 d1  a2 94 f8 39 80 ca 3c 96
   ..k........9..<.
Thu Aug 16 14:42:54 2007: 00000000: 02 02 00 ce c9 3d 5d c8  6c 07 8e fb 58 84 8d f6
```

```
   .....=].l...X...
Thu Aug 16 14:42:54 2007: 00000010: 33 6d 93 21 08 06 ff ff  ff ff 4f 27 02 01 00 25
   3m.!......O'...%
Thu Aug 16 14:42:54 2007: 00000020: 11 01 00 18 e5 e5 31 1e  33 b5 4e 69 90 e7 84 25
   ......1.3.Ni...%
Thu Aug 16 14:42:54 2007: 00000030: 42 a9 20 ac 84 33 9f 87  ca dc c9 b3 75 73 65 72
   B....3......user
Thu Aug 16 14:42:54 2007: 00000040: 31 1a 3b 00 00 00 09 01  35 6c 65 61 70 3a 73 65
   1.;.....5leap:se
Thu Aug 16 14:42:54 2007: 00000050: 73 73 69 6f 6e 2d 6b 65  79 3d 29 80 1d 2c 1c 85
   ssion-key=)..,..
Thu Aug 16 14:42:54 2007: 00000060: db 1c 29 7e 40 8a b8 93  69 2a 55 d2 e5 46 89 8b
   ..)~@...i*U..F..
Thu Aug 16 14:42:54 2007: 00000070: 2c 3b 65 49 3e 44 cf 7e  95 29 47 54 1a 1f 00 00
   ,;eI>D.~.)GT....
Thu Aug 16 14:42:54 2007: 00000080: 00 09 01 19 61 75 74 68  2d 61 6c 67 6f 2d 74 79
   ....auth-algo-ty
Thu Aug 16 14:42:54 2007: 00000090: 70 65 3d 65 61 70 2d 6c  65 61 70 1a 0d 00 00 37
   pe=eap-leap....7
Thu Aug 16 14:42:54 2007: 000000a0: 63 06 07 55 73 65 72 31  19 14 43 41 43 53 3a 30
   c..User1..CACS:0
Thu Aug 16 14:42:54 2007: 000000b0: 2f 39 2f 61 34 64 66 34  64 32 2f 31 50 12 9a 71
   /9/a4df4d2/1P..q
Thu Aug 16 14:42:54 2007: 000000c0: 09 99 7d 74 89 ad af e5  c8 b1 71 94 97 d1
   ..}t......q...
Thu Aug 16 14:42:54 2007: ****Enter processIncomingMessages: response code=2
Thu Aug 16 14:42:54 2007: ****Enter processRadiusResponse: response code=2
Thu Aug 16 14:42:54 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
Thu Aug 16 14:42:54 2007: AuthorizationResponse: 0x9c27800
Thu Aug 16 14:42:54 2007:       structureSize............236
Thu Aug 16 14:42:54 2007:       resultCode...............0
Thu Aug 16 14:42:54 2007:       protocolUsed.............0x0
0000001
Thu Aug 16 14:42:54 2007:       proxyState...............00:
40:96:AF:3E:93-03:02
Thu Aug 16 14:42:54 2007:  Packet contains 6 AVPs:
Thu Aug 16 14:42:54 2007:  AVP[01] Framed-IP-Address.........0xffffffff (-1)
   (4 bytes)
Thu Aug 16 14:42:54 2007:  AVP[02] EAP-Message...............DATA (37 bytes)
Thu Aug 16 14:42:54 2007:  AVP[03] Cisco / LEAP-Session-Key...DATA (16 bytes)
Thu Aug 16 14:42:54 2007:  AVP[04] Airespace / ACL-Name.......User1 (5 bytes)
Thu Aug 16 14:42:54 2007:  AVP[05] Class.....................CACS:0/9/a4df4d2/1
   (18 bytes)
Thu Aug 16 14:42:54 2007:  AVP[06] Message-Authenticator......DATA (16 bytes)
Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93 Applying new AAA override
   for station 00:40:96:af:3e:93
Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93 Override values
   for station 00:40:96:af:3e:93
               source: 4, valid bits: 0x400
         qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1

dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
                                                    vlanIfName: '',
aclName:User1
Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93
   Inserting new RADIUS override into chain for station 00:40:96:af:3e:93
```

You can use a combination of the **show wlan summary** command in order to recognize which of your WLANs employs RADIUS server authentication. Then you can view the **show client summary** command in order to see which MAC addresses (clients) are successfully authenticated on the RADIUS WLANs. You can also correlate this with your Cisco Secure ACS passed attempts or failed attempts logs.

Cisco recommends that you test your ACL configurations with a wireless client in order to ensure that you have configured them correctly. If they fail to operate correctly, verify the ACLs on the ACL web page and verify that your ACL changes were applied to the interface of the controller.

You can also use these show commands in order to verify your configuration:

- **show acl summary** In order to display the ACLs that are configured on the controller, use the **show acl summary** command.

Here is an example:

```
(Cisco Controller) >show acl summary

ACL Name                          Applied
--------------------------------- -------
User1                                   Yes
User2                                   Yes
```

- **show acl detailed** <ACL_Name> Displays detailed information on the configured ACLs.

  Here is an example:

  Note: Some of the lines in the output have been moved to the second line due to space constraints.

```
Cisco Controller) >show acl detailed User1

                    Source                        Destination
   Source Port   Dest Port
I  Dir       IP Address/Netmask              IP Address/Netmask
   Prot    Range       Range    DSCP   Action
-- --- ------------------------------- -------------------------------
   ---- ----------- ----------- ----    ------
 1  In      172.16.0.0/255.255.0.0        172.16.1.100/255.255.255.255
   Any  0-65535       0-65535   Any    Permit
 2 Out    172.16.1.100/255.255.255.255      172.16.0.0/255.255.0.0
   Any  0-65535       0-65535   Any    Permit


(Cisco Controller) >show acl detailed User2

                    Source                        Destination
   Source Port   Dest Port
I  Dir       IP Address/Netmask              IP Address/Netmask
   Prot    Range       Range    DSCP Action
-- --- ------------------------------- -------------------------------
   ---- ----------- ----------- ---- ------
1  In      172.16.0.0/255.255.0.0         172.16.1.50/255.255.255.255
   Any   0-65535       0-65535    Any  Permit
2 Out     172.16.1.50/255.255.255.255      172.16.0.0/255.255.0.0
   Any   0-65535       0-65535    Any  Permit
```

- **show client detail** <MAC Address of the client> − Displays detailed information about the Wireless client.

Troubleshooting Tips

Use these tips to troubleshoot:

- Verify on the controller that the RADIUS server is in active state, and not on standby or disabled.

- On the controller, check if the RADIUS server is chosen from the drop−down menu of the WLAN (SSID).
- Check if the RADIUS server receives and validates the authentication request from the wireless client.
- Check the Passed Authentications and Failed Attempts reports on the ACS server in order to accomplish this. These reports are available under Reports and Activities on the ACS server.

Related Information

- **ACLs on Wireless LAN Controllers: Rules, Limitations, and Examples**
- **ACLs on Wireless LAN Controller Configuration Example**
- **MAC Filters with Wireless LAN Controllers (WLCs) Configuration Example**
- **Cisco Wireless LAN Controller Configuration Guide, Release 5.2**
- **Technical Support & Documentation − Cisco Systems**

Updated: Mar 10, 2009 Document ID: 98590