

# 동적 VLAN 할당을 위한 RADIUS 서버 및 WLC 구성

## 목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[RADIUS 서버를 사용한 동적 VLAN 할당](#)

[구성](#)

[네트워크 다이어그램](#)

[구성](#)

[구성 단계](#)

[RADIUS 서버 구성](#)

[동적 VLAN 할당을 위해 Cisco Aireospace VSA 특성을 사용하여 ACS 구성](#)

[여러 VLAN에 대한 스위치 구성](#)

[WLC 컨피그레이션](#)

[무선 클라이언트 유틸리티 구성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[관련 정보](#)

## 소개

이 문서에서는 동적 VLAN 할당 개념을 소개합니다. 이 문서에서는 특정 VLAN에 무선 LAN(WLAN) 클라이언트를 동적으로 할당하도록 WLC(무선 LAN 컨트롤러) 및 RADIUS 서버를 구성하는 방법에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- WLC 및 LAP(Lightweight Access Point)에 대한 기본적인 지식 보유
- AAA 서버에 대한 기능 지식 보유
- 무선 네트워크 및 무선 보안 문제에 대한 철저한 지식 보유
- LWAPP(Lightweight AP Protocol)에 대한 기본적인 지식 보유

## 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 펌웨어 릴리스 5.2를 실행하는 Cisco 4400 WLC
- Cisco 1130 Series LAP
- 펌웨어 릴리스 4.4를 실행하는 Cisco 802.11a/b/g Wireless Client Adapter
- 버전 4.4를 실행하는 Cisco Aironet Desktop Utility(ADU)
- 버전 4.1을 실행하는 CiscoSecure ACS(Access Control Server)
- Cisco 2950 시리즈 스위치

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## 표기 규칙

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 표기 규칙을 참고하십시오.](#)

## RADIUS 서버를 사용한 동적 VLAN 할당

대부분의 WLAN 시스템에서 각 WLAN에는 컨트롤러 용어에서 SSID(Service Set Identifier) 또는 WLAN과 연결된 모든 클라이언트에 적용되는 정적 정책이 있습니다. 강력하지만 이 방법은 여러 QoS 및 보안 정책을 상속하기 위해 클라이언트가 다른 SSID와 연결해야 하기 때문에 제한이 있습니다.

그러나 Cisco WLAN 솔루션은 ID 네트워킹을 지원합니다. 이를 통해 네트워크에서 단일 SSID를 광고할 수 있지만, 특정 사용자가 사용자 자격 증명을 기반으로 다른 QoS 또는 보안 정책을 상속할 수 있습니다.

동적 VLAN 할당은 사용자가 제공한 자격 증명을 기반으로 무선 사용자를 특정 VLAN에 넣는 기능입니다. 특정 VLAN에 사용자를 할당하는 이 작업은 CiscoSecure ACS와 같은 RADIUS 인증 서버에서 처리됩니다. 예를 들어, 이를 사용하여 무선 호스트가 캠퍼스 네트워크 내에서 이동하는 동일한 VLAN에 유지되도록 할 수 있습니다.

따라서 클라이언트가 컨트롤러에 등록된 LAP에 연결하려고 하면 LAP는 검증을 위해 사용자의 자격 증명을 RADIUS 서버에 전달합니다. 인증에 성공하면 RADIUS 서버는 특정 IETF(Internet Engineering Task Force) 특성을 사용자에게 전달합니다. 이러한 RADIUS 특성은 무선 클라이언트에 할당해야 하는 VLAN ID를 결정합니다. 사용자가 항상 이 미리 결정된 VLAN ID에 할당되므로 클라이언트의 SSID(WLAN, WLC)는 중요하지 않습니다.

VLAN ID 할당에 사용되는 RADIUS 사용자 특성은 다음과 같습니다.

- IETF 64 (Tunnel Type) - VLAN으로 설정합니다.
- IETF 65 (Tunnel Medium Type) - 802로 설정합니다.
- IETF 81(Tunnel Private Group ID) - VLAN ID로 설정합니다.

VLAN ID는 12비트이며 1과 4094 사이의 값을 포함합니다(포함). Tunnel-Private-Group-ID는 RFC2868 에서 IEEE 802.1X와 함께 사용하기 위해 정의된 문자열 유형이므로 VLAN ID 정수 값은 문자열로 인코딩됩니다. 이러한 터널 특성이 전송되면 Tag 필드를 입력해야 합니다.

RFC2868 , 섹션 3.1: Tag 필드는 길이가 18진이며 동일한 터널을 참조하는 동일한 패킷에서 특성

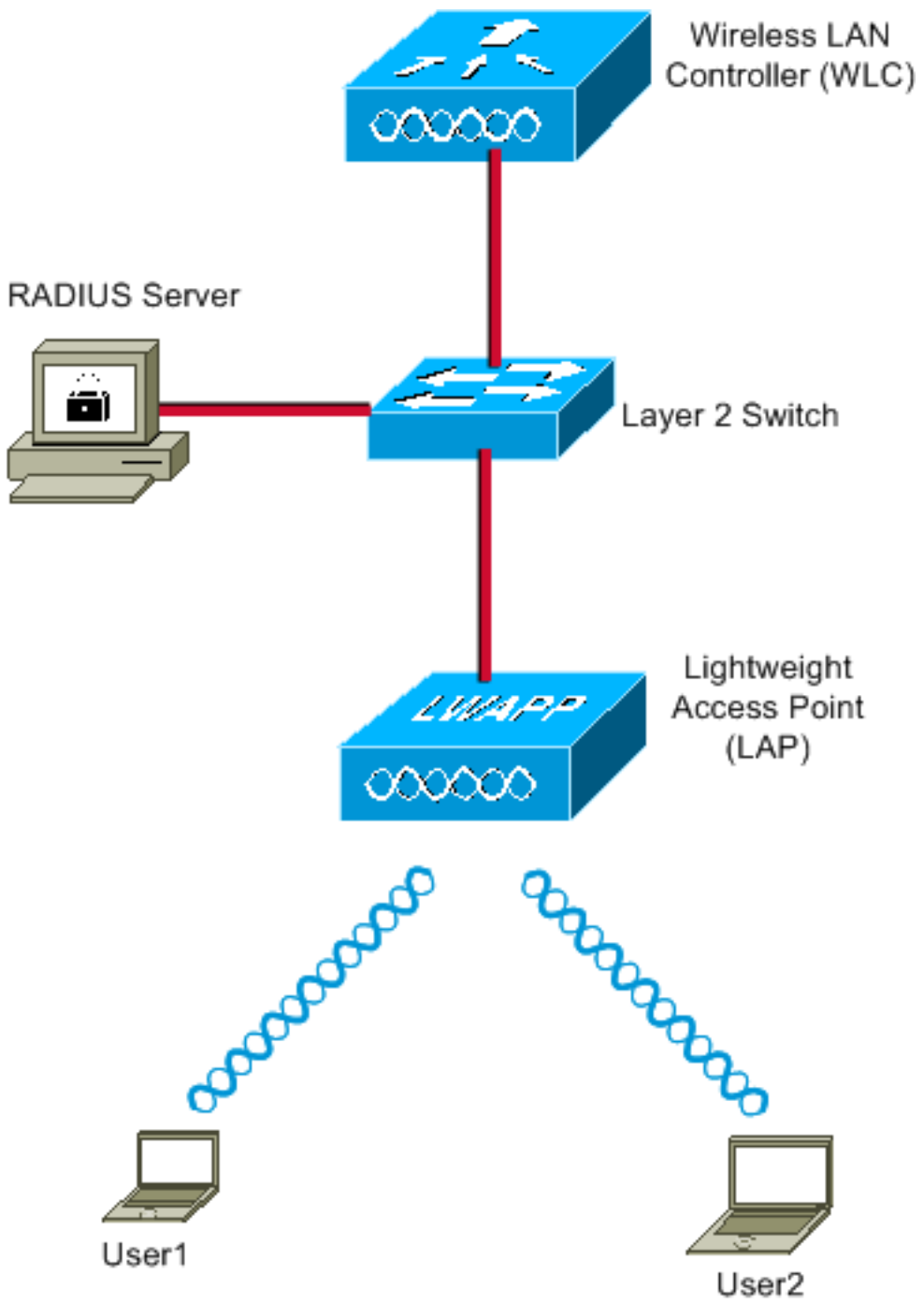
을 그룹화하는 방법을 제공합니다. 이 필드에 유효한 값은 0x01~0x1F(포함)입니다. 태그 필드가 사용되지 않으면 0이어야 합니다(0x00). 모든 RADIUS [특성에](#) 대한 자세한 내용은 RFC 2868 을 참조하십시오.

## 구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

### 네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



다음은 이 다이어그램에서 사용되는 구성 요소의 구성 세부 정보입니다.

- ACS(RADIUS) 서버의 IP 주소는 172.16.1.1입니다.
- WLC의 관리 인터페이스 주소는 172.16.1.30입니다.
- WLC의 AP-Manager 인터페이스 주소는 172.16.1.31입니다.
- DHCP 서버 주소 172.16.1.1은 LWAPP에 IP 주소를 할당하는 데 사용됩니다. **컨트롤러의 내부 DHCP 서버는 무선 클라이언트에 IP 주소를 할당하는 데 사용됩니다.**
- VLAN10 및 VLAN11은 이 컨피그레이션 전체에서 사용됩니다. user1은 VLAN10에 배치되도록 구성되고 user2는 RADIUS 서버에 의해 VLAN11에 배치되도록 구성됩니다. **참고:** 이 문서는 user1과 관련된 모든 구성 정보만 표시합니다. 이 문서에서는 user2에 대해 설명한 것과 동일한 절차를 완료합니다.
- 이 문서에서는 LEAP가 포함된 802.1x를 보안 메커니즘으로 사용합니다. **참고:** WLAN을 보호하기 위해 EAP-FAST 및 EAP-TLS 인증과 같은 고급 인증 방법을 사용하는 것이 좋습니다. 이 문서에서는 LEAP만 사용하여 단순화합니다.

## 구성

구성 전에 이 문서에서는 LAP가 WLC에 이미 등록된 것으로 가정합니다. 자세한 내용은 [Wireless LAN Controller 및 Lightweight Access Point 기본 구성 예](#)를 참조하십시오. 관련된 등록 절차에 대한 자세한 내용은 [WLC\(Wireless LAN Controller\)에 대한 LAP\(Lightweight AP\) 등록](#)을 참조하십시오.

## 구성 단계

이 컨피그레이션은 다음 세 가지 범주로 구분됩니다.

1. [RADIUS 서버 구성](#)
2. [여러 VLAN에 대한 스위치 구성](#)
3. [WLC 컨피그레이션](#)
4. [무선 클라이언트 유틸리티 구성](#)

## RADIUS 서버 구성

이 구성에는 다음 단계가 필요합니다.

- [RADIUS 서버에서 WLC를 AAA 클라이언트로 구성](#)
- [RADIUS 서버에서 동적 VLAN 할당에 사용되는 사용자 및 RADIUS\(IETF\) 특성 구성](#)

## RADIUS 서버의 WLC에 대한 AAA 클라이언트 구성

이 절차에서는 WLC가 사용자 자격 증명을 RADIUS 서버에 전달할 수 있도록 RADIUS 서버에 AAA 클라이언트로 WLC를 추가하는 방법에 대해 설명합니다.

다음 단계를 완료하십시오.

1. ACS GUI에서 **Network Configuration(네트워크 컨피그레이션)**을 클릭합니다.
2. **AAA Clients** 필드 아래에서 Add Entry(항목 추가) 섹션을 클릭합니다.
3. AAA Client IP Address and Key(AAA 클라이언트 IP 주소 및 키)를 입력합니다. IP 주소는 WLC의 관리 인터페이스 IP 주소여야 합니다. 입력한 키가 Security(보안) 창의 WLC에 구성된 키와 동일한지 확인합니다. AAA 클라이언트(WLC)와 RADIUS 서버 간의 통신에 사용되는 비

밀 키입니다.

- 인증 유형에 대한 Authenticate Using 필드에서 RADIUS(Cisco Airespace)를 선택합니다

**Network Configuration**

**Add AAA Client**

AAA Client Hostname: WLC4400

AAA Client IP Address: 172.16.1.30

Shared Secret: cisco

**RADIUS Key Wrap**

Key Encryption Key: [ ]

Message Authenticator Code Key: [ ]

Key Input Format:  ASCII  Hexadecimal

Authenticate Using: RADIUS (Cisco Airespace)

Single Connect TACACS+ AAA Client (Record stop in accounting on failure)

Log Update/Watchdog Packets from this AAA Client

Log RADIUS Tunneling Packets from this AAA Client

Replace RADIUS Port info with Username from this AAA Client

Match Framed-IP-Address with user IP address for accounting packets from this AAA Client

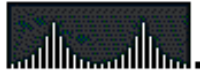
Submit Submit + Apply Cancel

## [RADIUS 서버에서 동적 VLAN 할당에 사용되는 사용자 및 RADIUS\(IETF\) 특성 구성](#)

이 절차에서는 RADIUS 서버의 사용자 및 이러한 사용자에게 VLAN ID를 할당하는 데 사용되는 RADIUS(IETF) 특성을 구성하는 방법에 대해 설명합니다.

다음 단계를 완료하십시오.

- ACS GUI에서 **User Setup(사용자 설정)**을 클릭합니다.
- User Setup(사용자 설정) 창의 User(사용자) 필드에 사용자 이름을 입력하고 **Add/Edit(추가/수정)**를 클릭합니다



# User Setup

## Select

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Posture Validation
- Network Access Profiles
- Reports and Activity
- Online Documentation













User:

List users beginning with letter/number:

[A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#)  
[N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#) [X](#) [Y](#) [Z](#)  
[0](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#)

Back to Help

3. Edit(편집) 페이지에서 다음과 같이 필요한 사용자 정보를 입력합니다

-  User Setup
-  Group Setup
-  Shared Profile Components
-  Network Configuration
-  System Configuration
-  Interface Configuration
-  Administration Control
-  External User Databases
-  Posture Validation
-  Network Access Profiles
-  Reports and Activity
-  Online Documentation

## User: User1

Account Disabled


### Supplementary User Info

Real Name

Description

### User Setup

Password Authentication:



CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password

Confirm Password

Separate (CHAP/MS-CHAP/ARAP)

Password

Confirm Password

When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

이 다이어그램에서 User Setup(사용자 설정) 섹션에서 제공하는 비밀번호는 사용자 인증 중에 클라이언트측에서 제공한 비밀번호와 동일해야 합니다.

4. Edit(편집) 페이지를 아래로 스크롤하여 IETF RADIUS Attributes(IETF RADIUS 특성) 필드를 찾습니다.
5. IETF RADIUS Attributes(IETF RADIUS 특성) 필드에서 3개의 Tunnel attributes(터널 특성) 옆의 확인란을 선택하고 다음과 같이 특성 값을 구성합니다



# User Setup

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Posture Validation
- Network Access Profiles
- Reports and Activity
- Online Documentation

Failed attempts since last successful login: 0

Reset current failed attempts count on submit

## Downloadable ACLs

Assign IP ACL: VPN\_Access

## IETF RADIUS Attributes

[064] Tunnel-Type

Tag 1 Value VLAN

Tag 2 Value

[065] Tunnel-Medium-Type

Tag 1 Value 802

Tag 2 Value

[081] Tunnel-Private-Group-ID

Tag 1 Value 10

Tag 2 Value

**참고:** ACS 서버의 초기 구성에서 IETF RADIUS 특성이 표시되지 않을 수 있습니다. Interface Configuration(인터페이스 컨피그레이션) > RADIUS(IETF)를 선택하여 사용자 컨피그레이션 창에서 IETF 특성을 활성화합니다.그런 다음 User and Group(사용자 및 그룹) 열에서 특성 64, 65 및 81의 확인란을 선택합니다





## Interface Configuration

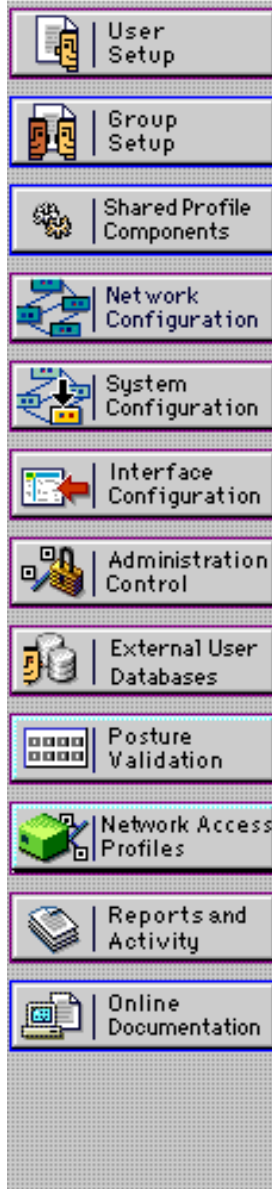
- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Posture Validation
- Network Access Profiles
- Reports and Activity
- Online Documentation

- [029] Termination-Action
- [033] Proxy-State
- [034] Login-LAT-Service
- [035] Login-LAT-Node
- [036] Login-LAT-Group
- [037] Framed-AppleTalk-Link
- [038] Framed-AppleTalk-Network
- [039] Framed-AppleTalk-Zone
- [062] Port-Limit
- [063] Login-LAT-Port
- [064] Tunnel-Type
- [065] Tunnel-Medium-Type
- [066] Tunnel-Client-Endpoint
- [067] Tunnel-Server-Endpoint
- [069] Tunnel-Password
- [071] ARAP-Features
- [072] ARAP-Zone-Access
- [078] Configuration-Token
- [081] Tunnel-Private-Group-ID
- [082] Tunnel-Assignment-ID
- [083] Tunnel-Preference
- [085] Acct-Interim-Interval
- [090] Tunnel-Client-Auth-ID
- [091] Tunnel-Server-Auth-ID

**참고:** RADIUS 서버가 특정 VLAN에 클라이언트를 동적으로 할당하려면 RADIUS 서버의 IETF 81(Tunnel-Private-Group-ID) 필드 아래에 구성된 VLAN-ID가 WLC에 있어야 합니다. 사용자별 컨피그레이션에 대해 RADIUS 서버를 활성화하려면 Interface Configuration(인터페이스 컨피그레이션) > Advanced Options(고급 옵션) 아래의 Per User TACACS+/RADIUS 특성 확인란을 선택합니다. 또한 LEAP는 인증 프로토콜로 사용되므로 RADIUS 서버의 시스템 구성 창에서 LEAP가 활성화되었는지 확인합니다



## System Configuration



Cisco client initial message:

PEAP session timeout (minutes):

Enable Fast Reconnect:

### EAP-FAST

[EAP-FAST Configuration](#)

### EAP-TLS

Allow EAP-TLS

Select one or more of the following options:

Certificate SAN comparison

Certificate CN comparison

Certificate Binary comparison

EAP-TLS session timeout (minutes):

### LEAP

Allow LEAP (For Aironet only)

### EAP-MD5

Allow EAP-MD5

AP EAP request timeout (seconds):

## [동적 VLAN 할당을 위해 Cisco Airespace VSA 특성을 사용하여 ACS 구성](#)

최신 ACS 버전에서는 ACS의 사용자 컨피그레이션에 따라 VLAN 인터페이스 이름(VLAN ID 아님)을 사용하여 성공적으로 인증된 사용자를 할당하도록 Cisco Airespace [VSA(Vendor-Specific)] 특성을 구성할 수도 있습니다. 이를 위해 이 섹션의 단계를 수행합니다.

**참고:** 이 섹션에서는 ACS 4.1 버전을 사용하여 Cisco Airespace VSA 특성을 구성합니다.

## [Cisco Airespace VSA 특성 옵션을 사용하여 ACS 그룹 구성](#)

다음 단계를 완료하십시오.

1. ACS 4.1 GUI의 탐색 모음에서 Interface Configuration을 클릭합니다. 그런 다음 Cisco Airespace 속성 옵션을 구성하려면 Interface Configuration 페이지에서 RADIUS(Cisco Airespace)를 선택합니다.

2. RADIUS(Cisco Airespace) 창에서 Aire-Interface-Name 옆에 있는 User 확인란(필요한 경우 그룹 확인란)을 선택하여 User Edit 페이지에 표시합니다. 그런 다음 Submit(제출)을 클릭합니다

**CISCO SYSTEMS**

## Interface Configuration

Edit

### RADIUS (Cisco Airespace)

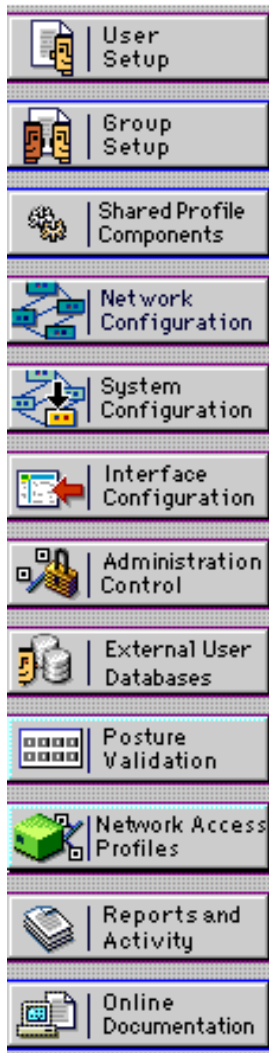
User	Group	
<input type="checkbox"/>	<input type="checkbox"/>	[026/14179/002] Aire-QoS-Level
<input type="checkbox"/>	<input type="checkbox"/>	[026/14179/003] Aire-DSCP
<input type="checkbox"/>	<input type="checkbox"/>	[026/14179/004] Aire-802.1P-Tag
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	[026/14179/005] Aire-Interface-Name
<input type="checkbox"/>	<input type="checkbox"/>	[026/14179/006] Aire-Acl-Name

[? Back to Help](#)

3. user1의 Edit 페이지로 이동합니다.
4. User Edit(사용자 수정) 페이지에서 아래로 스크롤하여 Cisco Airespace RADIUS Attributes(Cisco Airespace RADIUS 특성) 섹션으로 이동합니다. Aire-Interface-Name 특성 옆의 확인란을 선택하고 사용자 인증 성공 시 할당할 동적 인터페이스의 이름을 지정합니다.이 예에서는 사용자를 관리 VLAN에 할당합니다



## User Setup



Date exceeds: May 24 2009

Failed attempts exceed:

Failed attempts since last successful login: 0

Reset current failed attempts count on submit

**Downloadable ACLs** ?

Assign IP ACL: VPN\_Access

**Cisco Airespace RADIUS Attributes** ?

[14179\005] Aire-Interface-Name

5. Submit(제출)을 클릭합니다.

## 여러 VLAN에 대한 스위치 구성

스위치를 통해 여러 VLAN을 허용하려면 컨트롤러에 연결된 스위치 포트를 구성하려면 다음 명령을 실행해야 합니다.

1. Switch(config-if)#switchport mode trunk
2. Switch(config-if)#switchport trunk encapsulation dot1q

**참고:** 기본적으로 대부분의 스위치는 트렁크 포트를 통해 해당 스위치에 생성된 모든 VLAN을 허용합니다.

이러한 명령은 Catalyst 운영 체제(CatOS) 스위치에 따라 다릅니다.

유선 네트워크가 스위치에 연결된 경우 이 동일한 컨피그레이션을 무선 네트워크에 연결하는 스위치 포트에 적용할 수 있습니다. 이렇게 하면 유무선 네트워크의 동일한 VLAN 간에 통신이 가능합니다.

**참고:** 이 문서에서는 VLAN 간 통신에 대해 설명하지 않습니다. 이 문서는 범위를 벗어납니다. VLAN 간 라우팅의 경우 적절한 VLAN 및 트렁킹 컨피그레이션을 사용하는 레이어 3 스위치 또는

외부 라우터가 필요하다는 점을 이해해야 합니다. VLAN 간 라우팅 컨피그레이션을 설명하는 여러 문서가 있습니다.

## WLC 컨피그레이션

이 구성에는 다음 단계가 필요합니다.

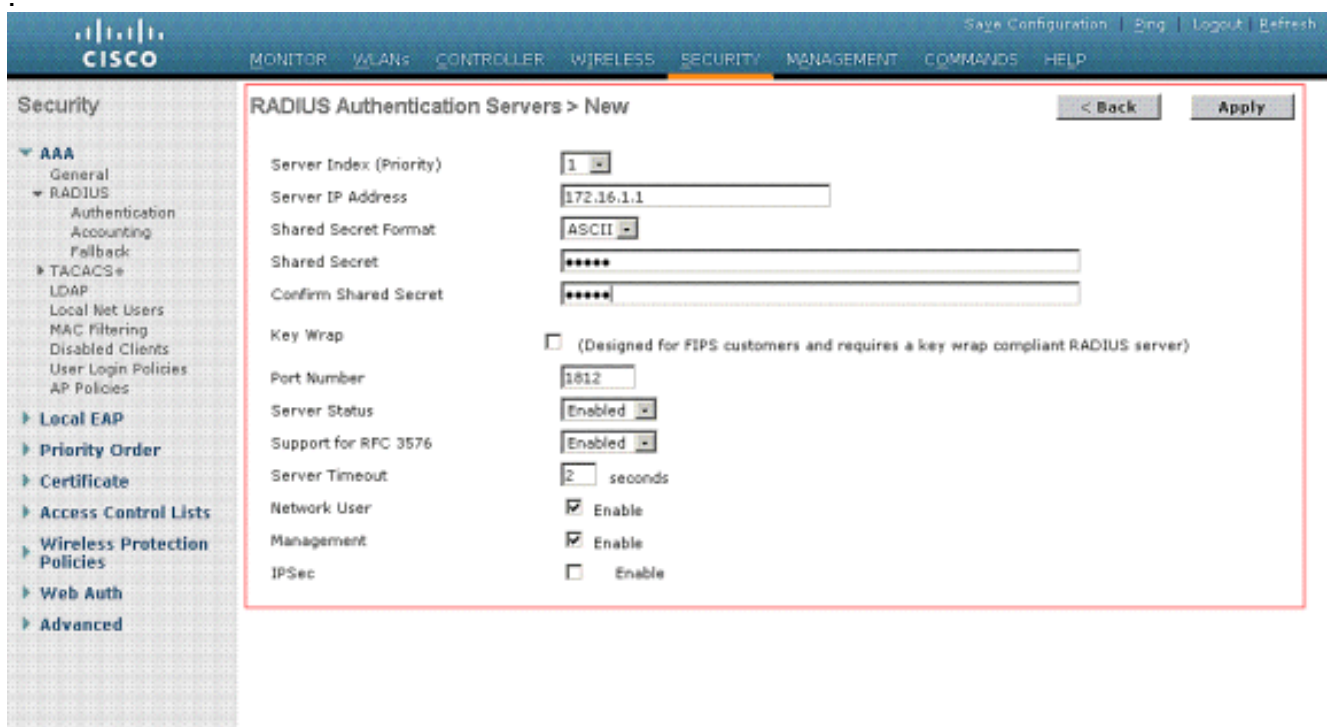
- [인증 서버의 세부 정보로 WLC 구성](#)
- [동적 인터페이스\(VLAN\) 구성](#)
- [WLAN\(SSID\) 구성](#)

### 인증 서버의 세부 정보로 WLC 구성

RADIUS 서버와 통신하여 클라이언트 및 다른 모든 트랜잭션에 대해 인증할 수 있도록 WLC를 구성해야 합니다.

다음 단계를 완료하십시오.

1. 컨트롤러 GUI에서 Security(보안)를 클릭합니다.
2. RADIUS 서버의 IP 주소와 RADIUS 서버와 WLC 간에 사용되는 Shared Secret 키를 입력합니다. 이 공유 암호 키는 Network Configuration(네트워크 컨피그레이션) > AAA Clients(AAA 클라이언트) > Add Entry(항목 추가)에서 RADIUS 서버에 구성된 키와 같아야 합니다. 다음은 WLC의 예제 창입니다



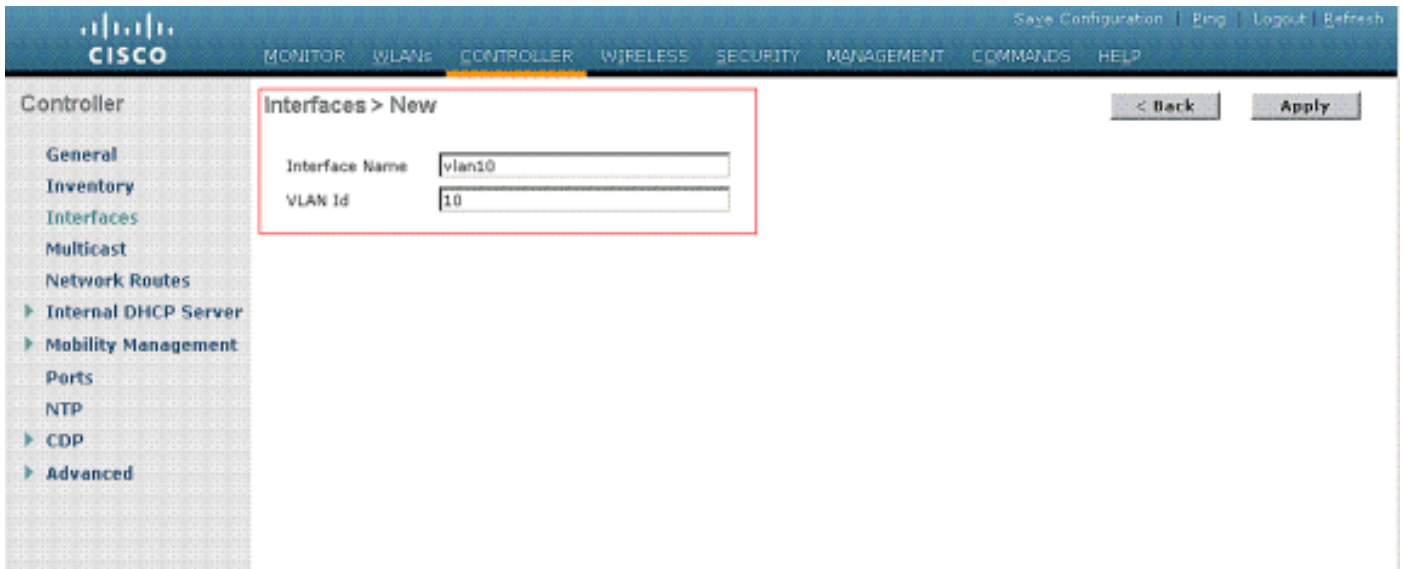
### 동적 인터페이스(VLAN) 구성

이 절차에서는 WLC에서 동적 인터페이스를 구성하는 방법에 대해 설명합니다. 이 문서의 앞부분에서 설명한 대로 RADIUS 서버의 Tunnel-Private-Group ID 특성에 지정된 VLAN ID도 WLC에 있어야 합니다.

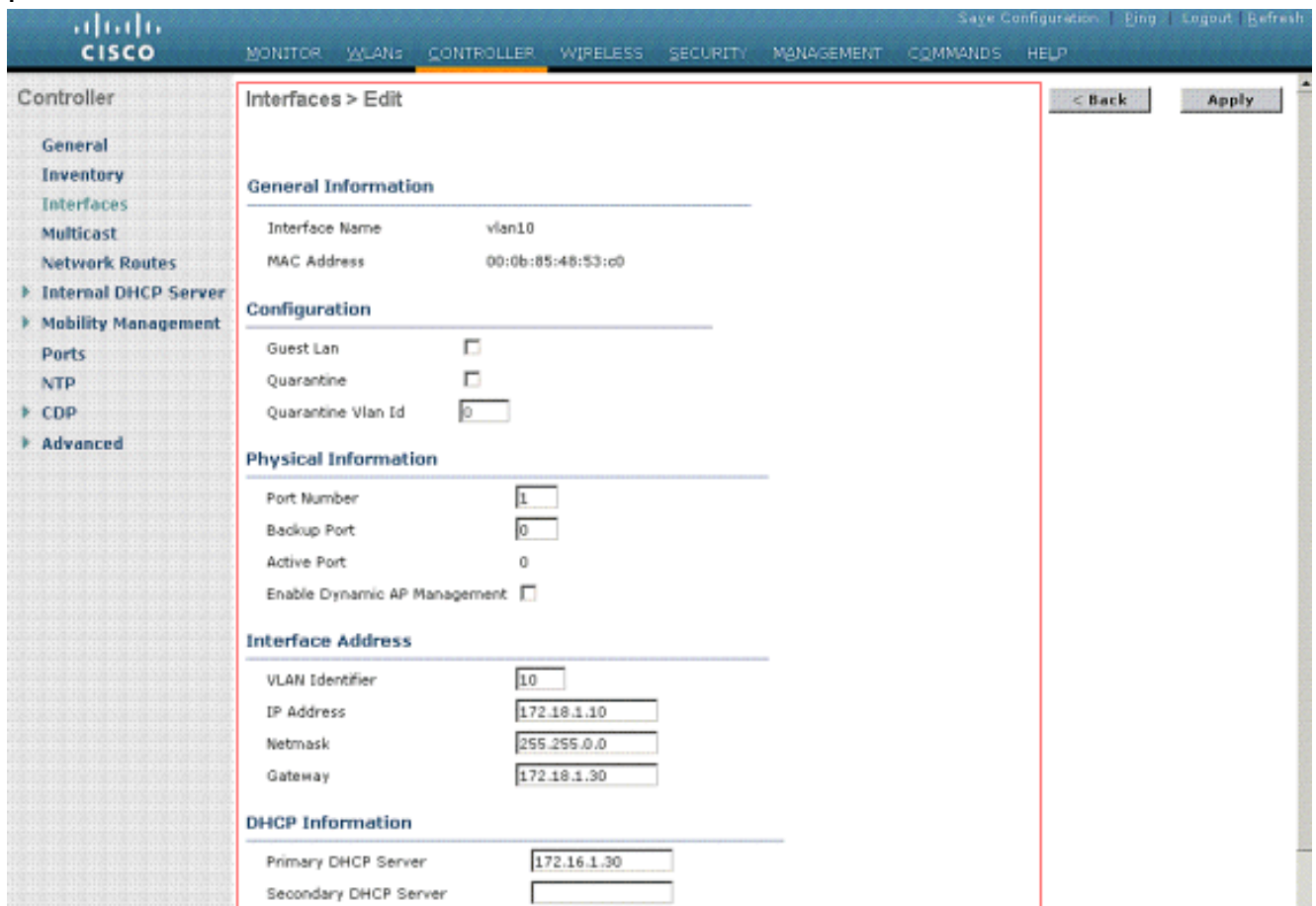
이 예에서 user1은 RADIUS 서버에서 Tunnel-Private-Group ID 10(VLAN = 10)으로 지정됩니다.

user1 User Setup 창의 [IETF RADIUS Attributes](#) 섹션을 참조하십시오.

이 예에서는 WLC에 구성된 동일한 동적 인터페이스(VLAN=10)를 볼 수 있습니다. 컨트롤러 GUI의 Controller(컨트롤러) > Interfaces(인터페이스) 창에서 동적 인터페이스가 구성됩니다.



1. 이 창에서 Apply를 클릭합니다. 그러면 이 동적 인터페이스의 Edit(수정) 창(VLAN 10 here)으로 이동합니다.
2. 이 동적 인터페이스의 IP 주소 및 기본 게이트웨이를 입력합니다



**참고:** 이 문서는 컨트롤러에서 내부 DHCP 서버를 사용하므로 이 창의 기본 DHCP 서버 필드는 WLC 자체의 관리 인터페이스를 가리킵니다. 외부 DHCP 서버, 라우터 또는 RADIUS 서버 자체를 무선 클라이언트에 대한 DHCP 서버로 사용할 수도 있습니다. 이러한 경우 기본 DHCP 서버 필드는 DHCP 서버로 사용되는 디바이스의 IP 주소를 가리킵니다. 자세한 내용은

DHCP 서버 설명서를 참조하십시오.

3. Apply를 클릭합니다.이제 WLC에서 동적 인터페이스로 구성됩니다. 마찬가지로 WLC에서 여러 동적 인터페이스를 구성할 수 있습니다. 그러나 특정 VLAN을 클라이언트에 할당하려면 동일한 VLAN ID가 RADIUS 서버에도 있어야 합니다.

## WLAN(SSID) 구성

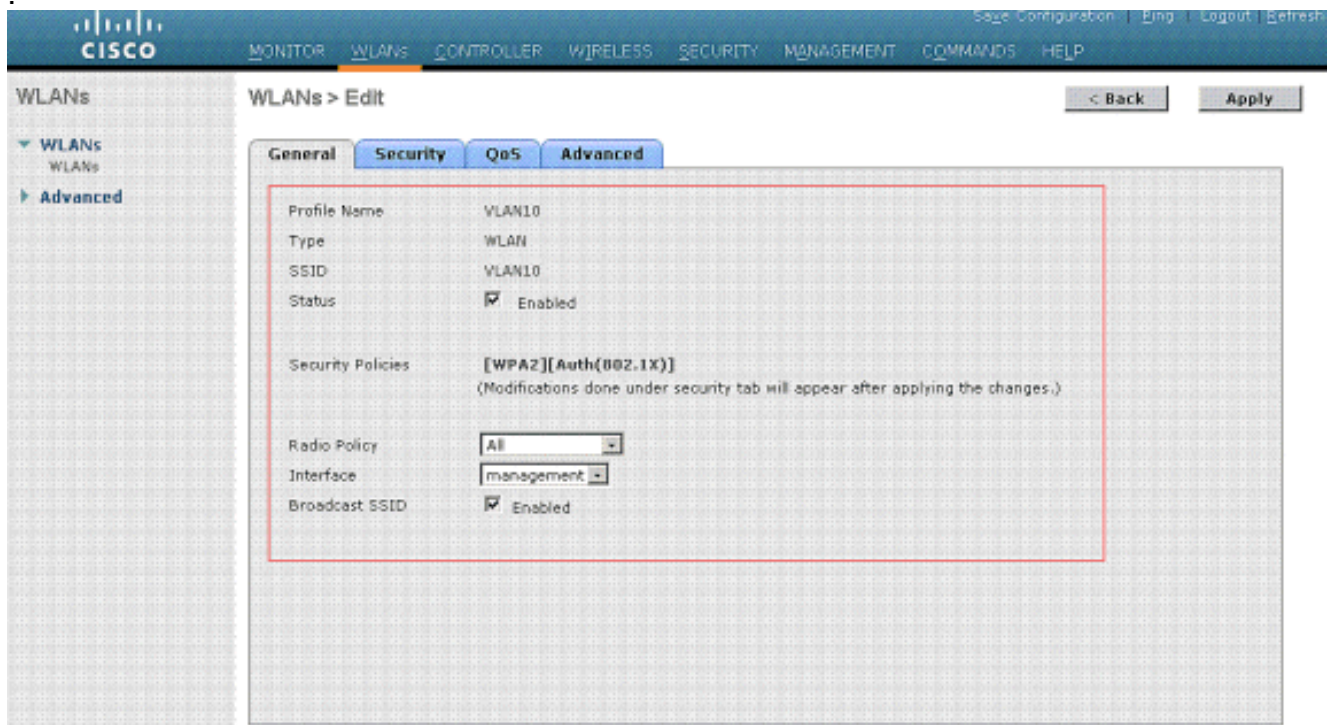
이 절차에서는 WLC에서 WLAN을 구성하는 방법에 대해 설명합니다.

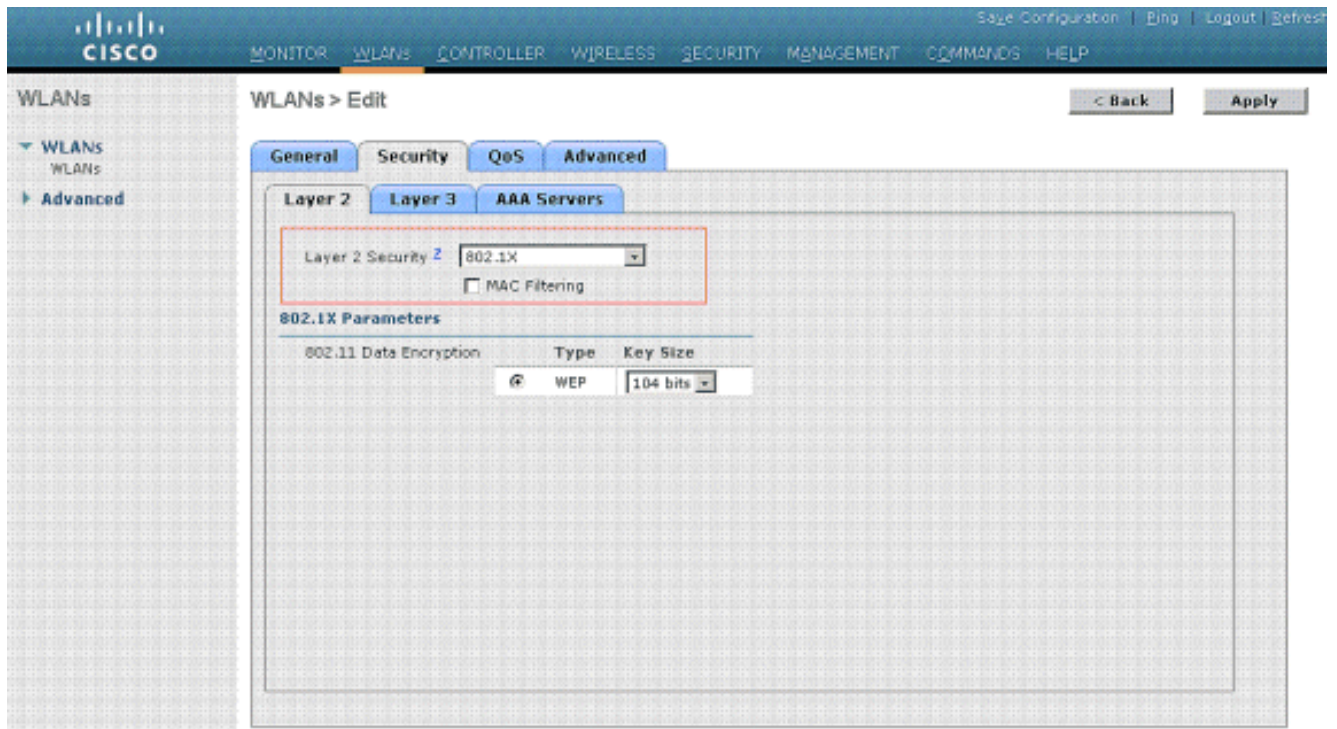
다음 단계를 완료하십시오.

1. 컨트롤러 GUI에서 새 WLAN을 생성하려면 **WLANs(WLAN) > New(새로 만들기)**를 선택합니다. New WLANs(새 WLANs) 창이 표시됩니다.
2. WLAN ID 및 WLAN SSID 정보를 입력합니다.WLAN SSID로 이름을 입력할 수 있습니다. 이 예에서는 VLAN10을 WLAN SSID로 사용합니다

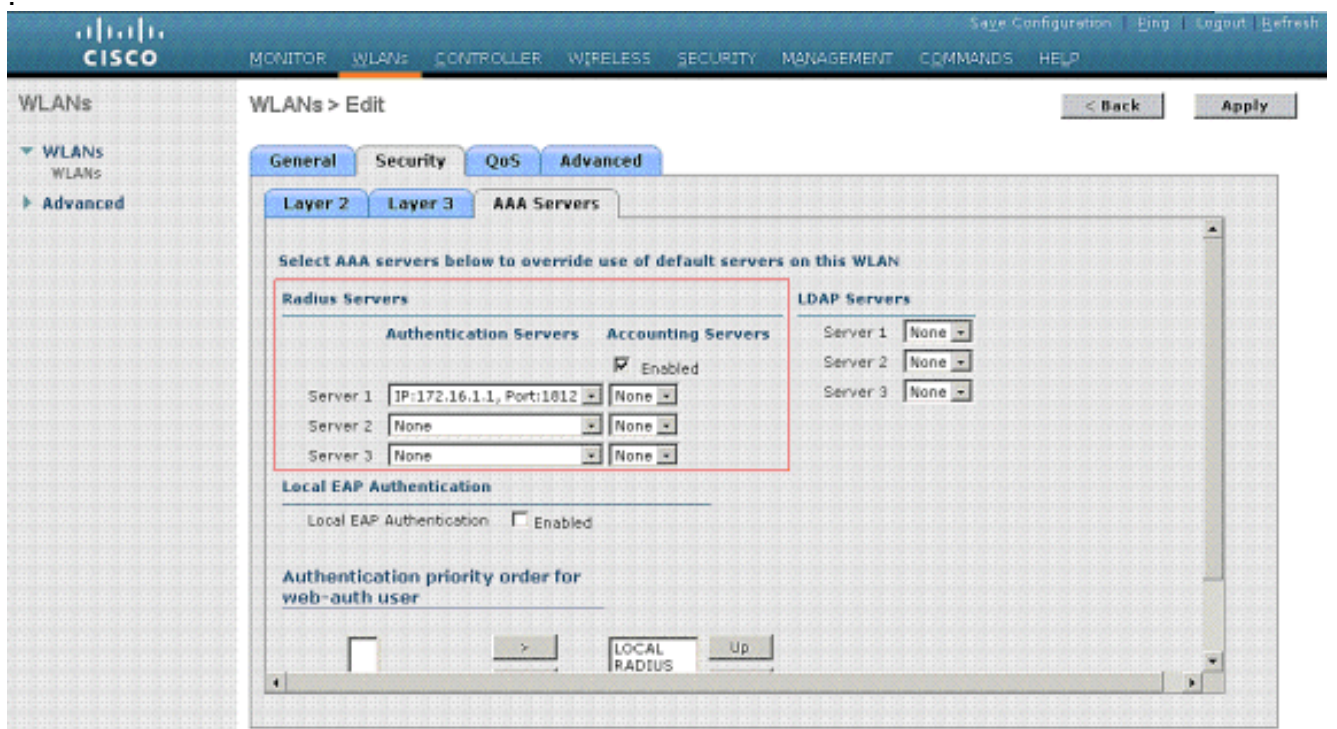


3. WLAN SSID10의 Edit(편집) 창으로 이동하려면 Apply(적용)를 클릭합니다





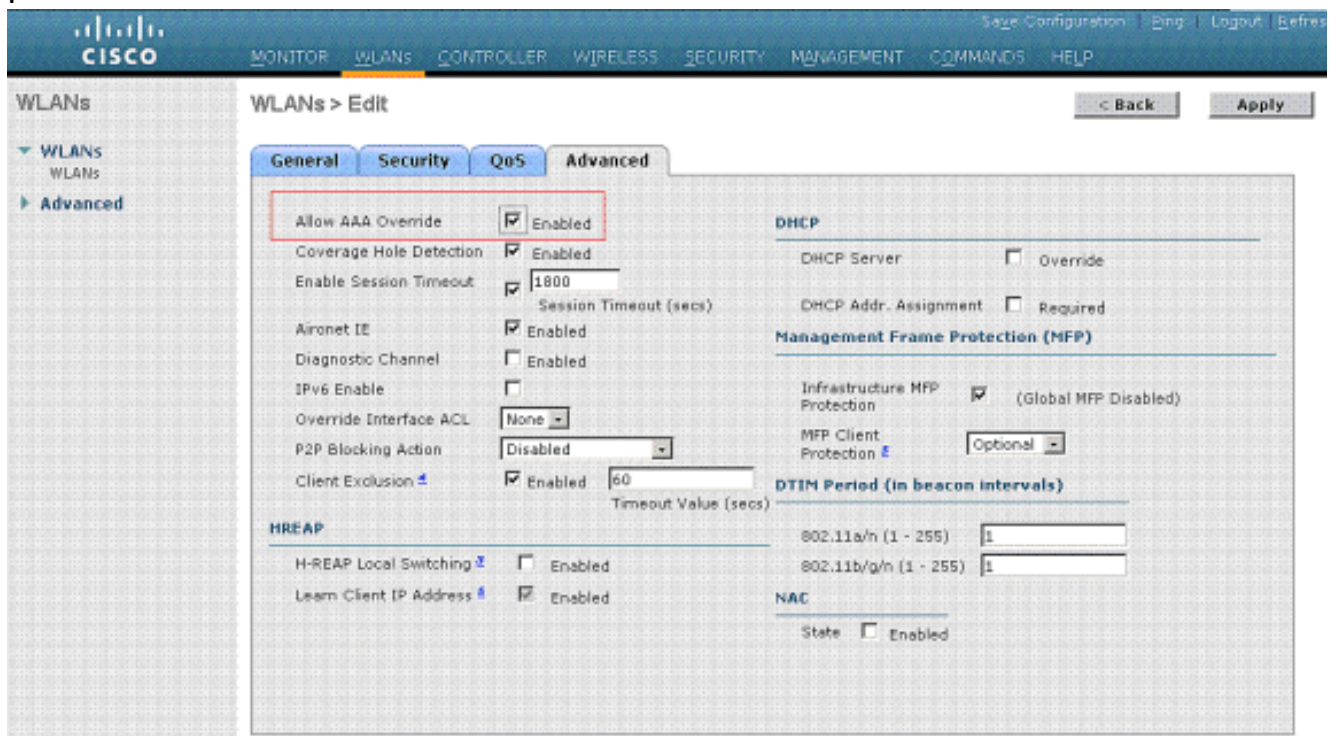
일반적으로 무선 LAN 컨트롤러에서 각 WLAN은 특정 VLAN(SSID)에 매핑되므로 해당 WLAN에 속한 특정 사용자가 특정 VLAN에 매핑됩니다. 이 매핑은 일반적으로 WLAN SSID 창의 Interface Name(인터페이스 이름) 필드에서 수행됩니다



제공된 예에서는 인증 성공 시 무선 클라이언트를 특정 VLAN에 할당하는 것이 RADIUS 서버의 작업입니다. WLAN은 WLC의 특정 동적 인터페이스에 매핑할 필요가 없습니다. 또는 WLC에서 WLAN에 동적 인터페이스 매핑이 수행되더라도 RADIUS 서버는 이 매핑을 재정의하고 해당 WLAN을 통해 들어오는 사용자를 RADIUS 서버의 사용자 터널 그룹 사설 ID 필드에 지정된 VLAN에 할당합니다.

4. RADIUS 서버에서 WLC 컨피그레이션을 재정의하려면 Allow AAA Override 확인란을 선택합니다.
5. 구성된 각 WLAN(SSID)에 대해 컨트롤러에서 Allow AAA Override(AAA 재정의 허용)를 활성화합니다





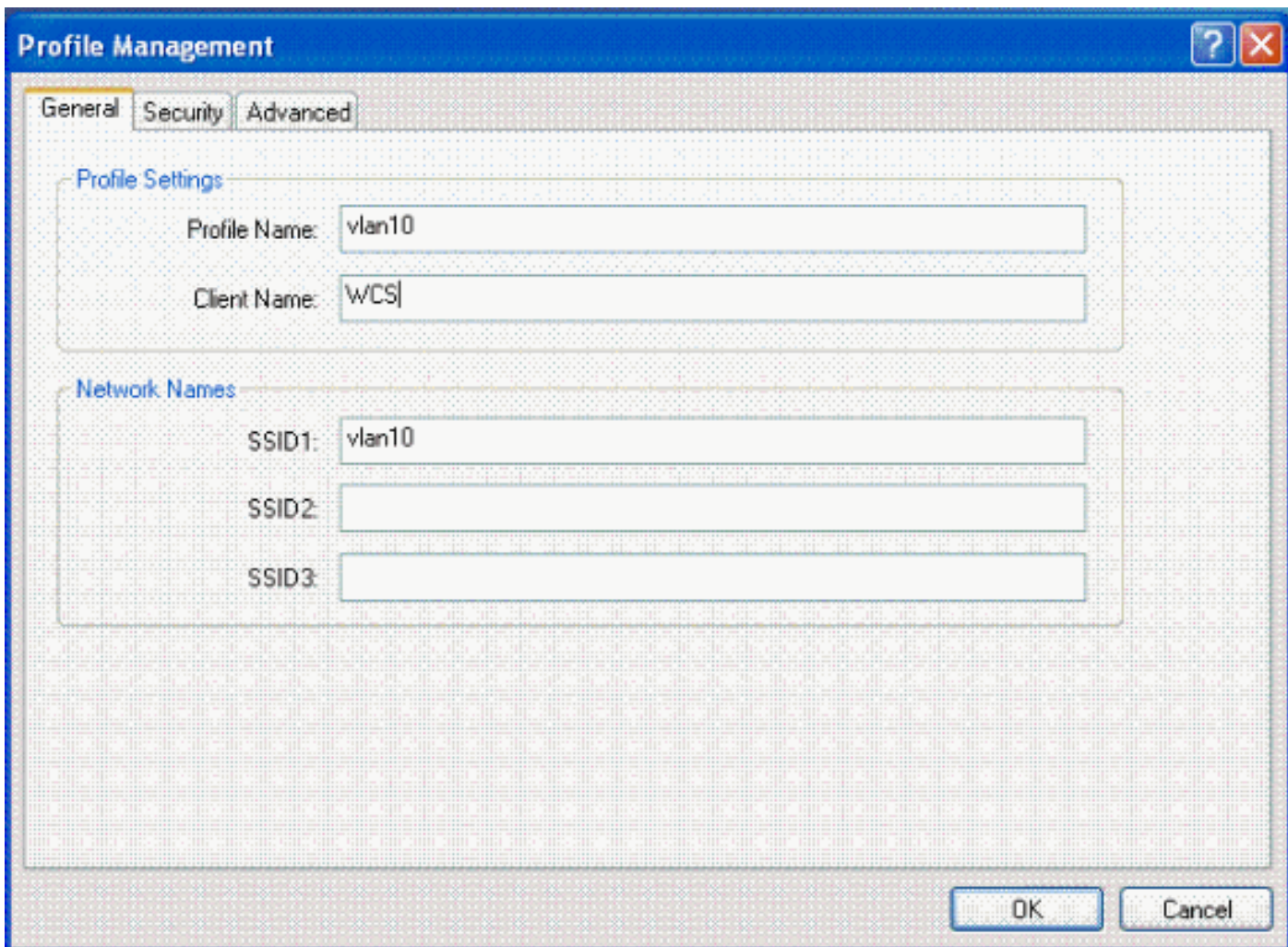
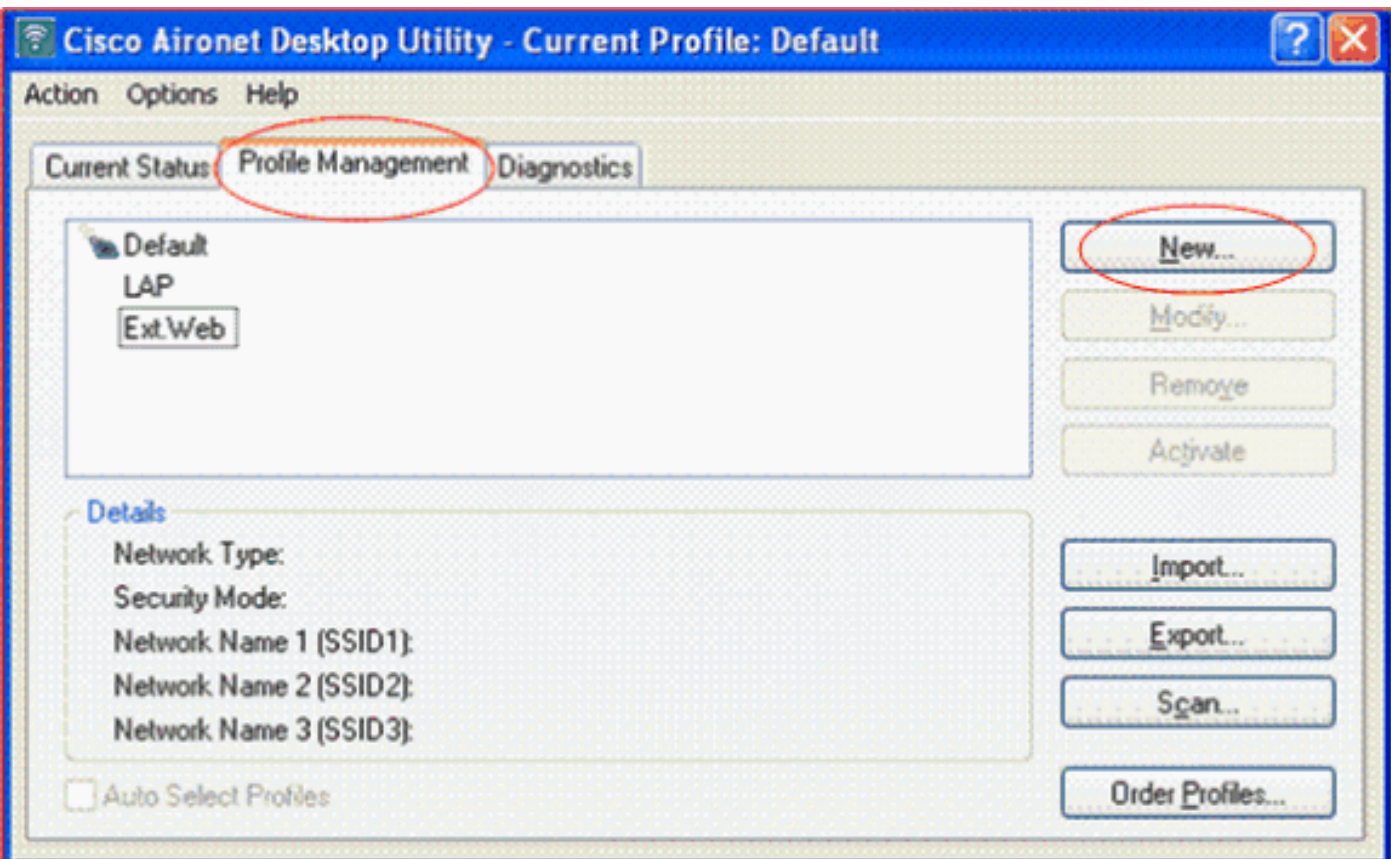
AAA Override(AAA 재정의)가 활성화되고 클라이언트에 충돌하는 AAA 및 컨트롤러 WLAN 인증 매개변수가 있는 경우 클라이언트 인증은 AAA(RADIUS) 서버에 의해 수행됩니다. 이 인증의 일부로 운영 체제는 클라이언트를 AAA 서버에서 반환한 VLAN으로 이동합니다. 컨트롤러 인터페이스 컨피그레이션에서 미리 정의됩니다. 예를 들어, 회사 WLAN이 주로 VLAN 2에 할당된 관리 인터페이스를 사용하고 AAA Override가 VLAN 100으로 리디렉션을 반환하는 경우 VLAN 100이 할당된 물리적 포트라도 운영 체제는 모든 클라이언트 전송을 VLAN 100으로 리디렉션합니다. AAA Override(AAA 재정의)를 비활성화하면 모든 클라이언트 인증은 기본적으로 컨트롤러 인증 매개변수 설정으로 설정되며, 컨트롤러 WLAN에 클라이언트별 인증 매개변수가 없는 경우 AAA 서버에서만 인증이 수행됩니다.

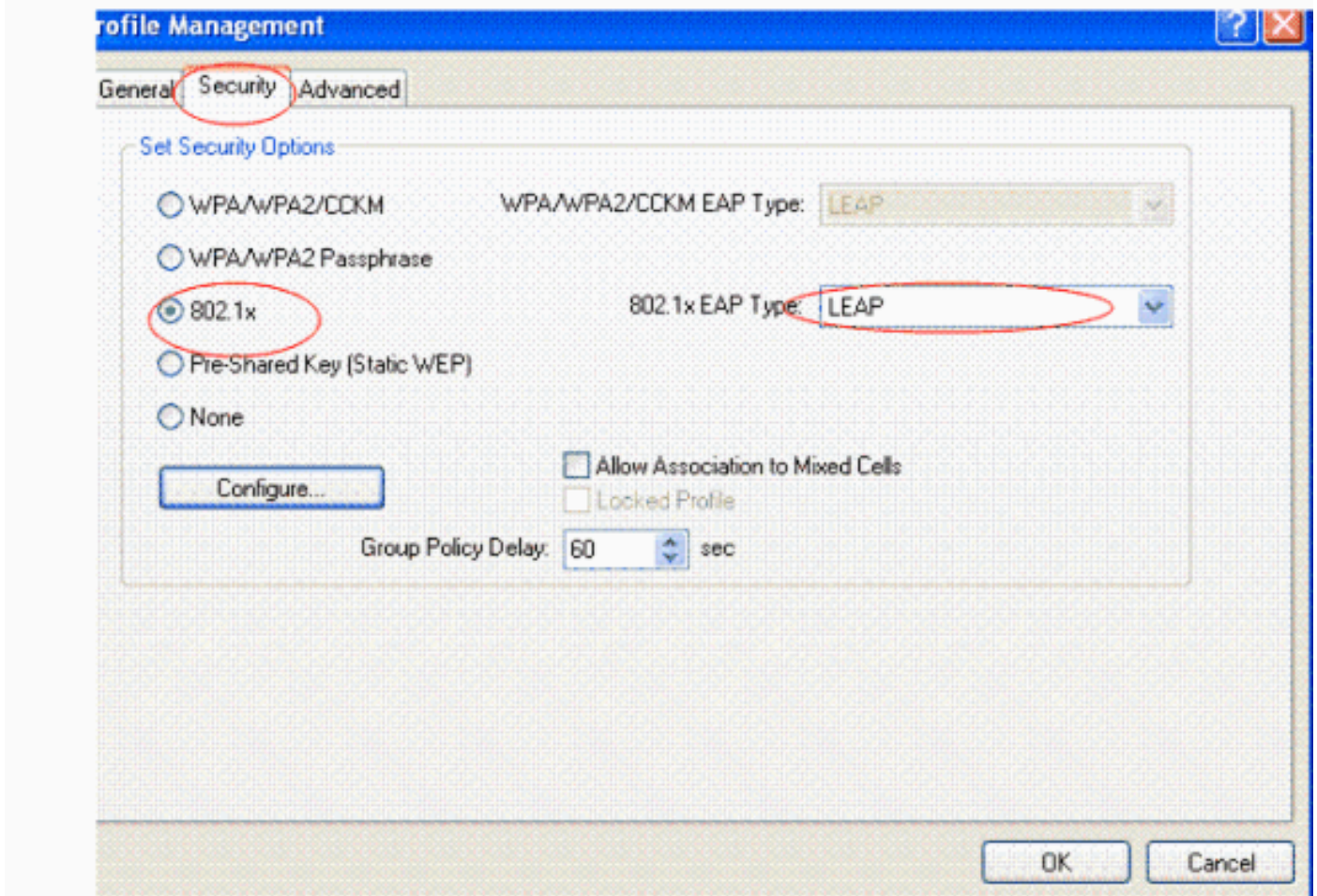
## 무선 클라이언트 유틸리티 구성

이 문서에서는 ADU를 사용자 프로필 컨피그레이션을 위한 클라이언트 유틸리티로 사용합니다. 이 구성에서는 LEAP를 인증 프로토콜로 사용합니다. 이 섹션의 예와 같이 ADU를 구성합니다.

ADU 메뉴 모음에서 **프로파일 관리 > 새로 만들기**를 선택하여 새 프로파일을 생성합니다.

예제 클라이언트는 SSID VLAN10의 일부로 구성됩니다. 이러한 다이어그램은 클라이언트에서 사용자 프로필을 구성하는 방법을 보여줍니다.





## 다음을 확인합니다.

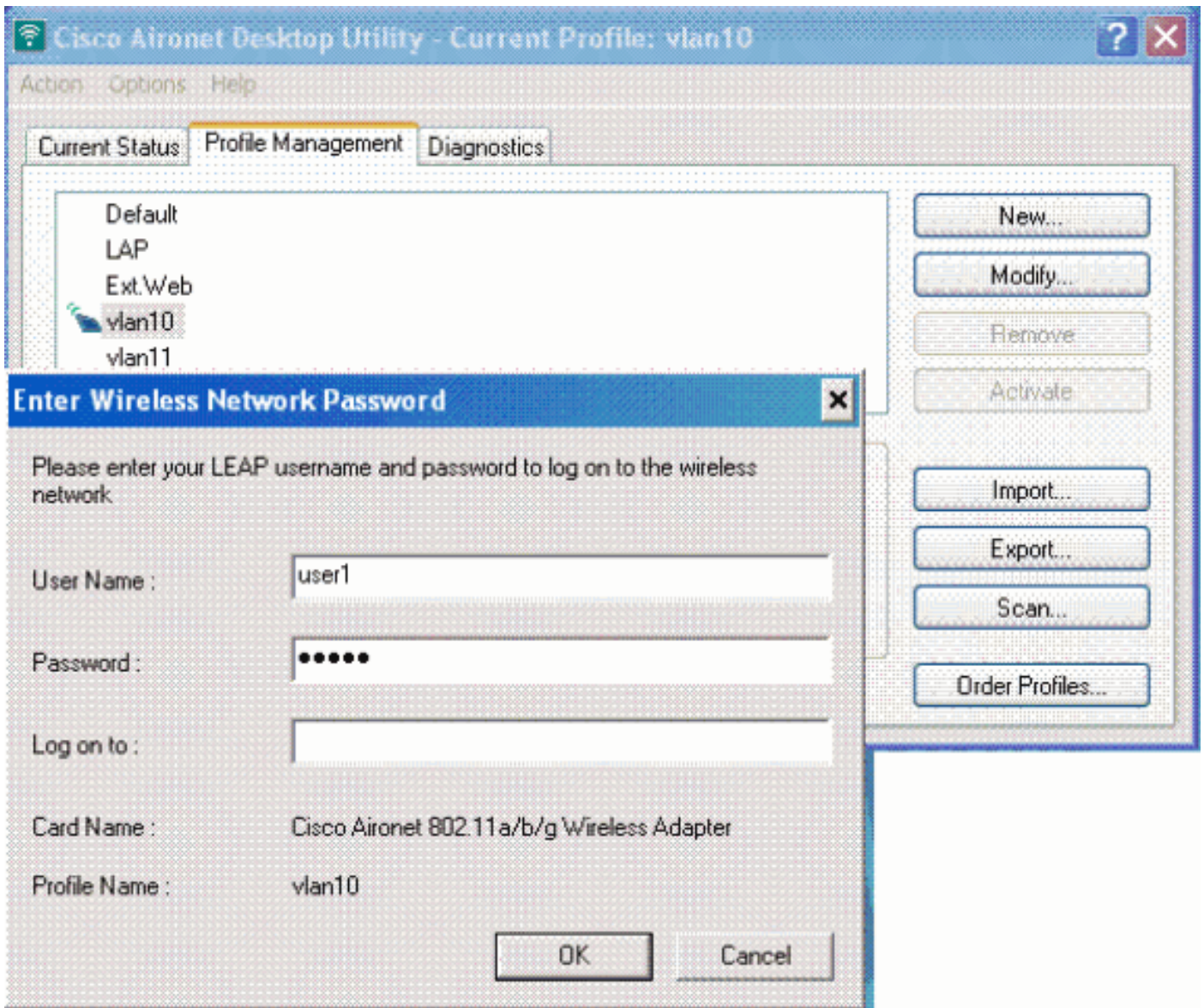
ADU에서 구성한 사용자 프로필을 활성화합니다. 컨피그레이션에 따라 사용자 이름과 비밀번호를 입력하라는 프롬프트가 표시됩니다. ADU에 인증을 위해 Windows 사용자 이름 및 비밀번호를 사용하도록 지시할 수도 있습니다. 클라이언트가 인증을 수신할 수 있는 여러 옵션이 있습니다. 생성한 사용자 프로필의 Security(보안) > Configure(구성) 탭에서 이러한 옵션을 구성할 수 있습니다.

이전 예에서 user1은 RADIUS 서버에 지정된 대로 VLAN10에 할당됩니다.

다음 예에서는 클라이언트 측에서 이 사용자 이름과 비밀번호를 사용하여 인증을 수신하고 RADIUS 서버에서 VLAN에 할당합니다.

- 사용자 이름 = user1
- 비밀번호 = user1

이 예에서는 SSID VLAN10에 사용자 이름과 비밀번호를 묻는 프롬프트가 표시되는 방법을 보여줍니다. 사용자 이름과 비밀번호는 다음 예에 입력됩니다.



인증 및 해당 검증이 성공하면 상태 메시지로 성공 메시지를 수신합니다.

그런 다음 전송된 RADIUS 특성에 따라 클라이언트가 적절한 VLAN에 할당되었는지 확인해야 합니다. 이 작업을 수행하려면 다음 단계를 완료하십시오.

1. 컨트롤러 GUI에서 Wireless(무선) > AP(AP)를 선택합니다.
2. AP(Access Points) 창의 왼쪽 모서리에 나타나는 Clients(클라이언트)를 클릭합니다. 클라이언트 통계가 표시됩니다

Client MAC Addr	AP Name	WLAN Profile	Protocol	Status	Auth	Port	WGB
00:21:5c:09:08:dd	AP1130	Unknown	802.11a	Probing	No	2	No
00:21:5c:50:3a:1f	AP1130	VLAN10	802.11g	Associated	Yes	2	No

3. IP 주소, 클라이언트가 할당된 VLAN 등 클라이언트의 전체 세부 정보를 식별하려면 Details를 클릭합니다. 이 예에서는 클라이언트 user1에 대한 다음 세부 정보를 표시합니다

The screenshot shows the Cisco AireSpace VSA configuration interface. The left sidebar contains navigation options: Monitor, Summary, Access Points, Statistics, CDP, Rogues, Clients, and Multicast. The main content area is titled 'Clients > Detail' and includes buttons for '< Back', 'Apply', 'Link Test', and 'Remove'. The 'Client Properties' section lists various attributes such as MAC Address (00:21:50:50:3a:1f), IP Address (17.18.1.35), Client Type (Regular), User Name (User1), Port Number (2), and Interface (vlan10, highlighted with a red box). The 'AP Properties' section lists attributes like AP Address (00:15:c7:ab:55:90), AP Name (AP1130), AP Type (802.11g), WLAN Profile (VLAN10), Status (Associated), Association ID (1), and 802.11 Authentication (Open System). The 'Security Information' section shows Security Policy Completed (Yes), Policy Type (802.1X), Encryption Cipher (WEP (104 bits)), EAP Type (LEAP), and NAC State (Access).

이 창에서 RADIUS 서버에 구성된 RADIUS 특성에 따라 이 클라이언트가 VLAN10에 할당되었는지 확인할 수 있습니다. **참고:** 동적 VLAN 할당이 Cisco AireSpace VSA 특성 설정을 기반으로 하는 경우, 인터페이스 이름은 클라이언트 세부사항 페이지에 이 예와 같이 관리자로 표시됩니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

- **debug aaa events enable** - 이 명령을 사용하여 컨트롤러를 통해 RADIUS 특성을 클라이언트로 성공적으로 전송할 수 있습니다. 디버그 출력의 이 부분은 RADIUS 특성의 성공적인 전송을 보장합니다.

```

Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[0]:
attribute 64, vendorId 0, valueLen 4
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[1]:
attribute 65, vendorId 0, valueLen 4
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[2]:
attribute 81, vendorId 0, valueLen 3
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[3]:
attribute 79, vendorId 0, valueLen 32
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 Received EAP Attribute
(code=2, length=32,id=0) for mobile 00:40:96:ac:e6:57
Fri Jan 20 02:25:08 2006: 00000000: 02 00 00 20 11 01 00 18
4a 27 65 69 6d e4 05 f5
.....J'eim...00000010: d0 98 0c cb 1a 0c 8a 3c
.....44 a9 da 6c 36 94 0a f3 <D..16...
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[4]:
attribute 1, vendorId 9, valueLen 16
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[5]:
attribute 25, vendorId 0, valueLen 28
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[6]:
attribute 80, vendorId 0, valueLen 16
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 Tunnel-Type 16777229
should be 13 for STA 00:40:96:ac:e6:57

```

```
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 Tunnel-Medium-Type 16777222  
should be 6 for STA 00:40:96:ac:e6:57
```

```
Fri Jan 20 02:30:00 2006: 00:40:96:ac:e6:57 Station 00:40:96:ac:e6:57  
setting dot1x reauth timeout = 1800
```

- 다음 명령도 유용할 수 있습니다. 디버그 dot1x aaa 활성화 디버그 aaa 패킷 활성화

## 문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

참고: 동적 VLAN 할당은 WLC의 웹 인증에 사용할 수 없습니다.

## 관련 정보

- [RADIUS 서버를 사용한 EAP 인증](#)
- [Cisco LEAP](#)
- [Cisco Wireless LAN Controller 컨피그레이션 가이드, 릴리스 4.0](#)
- [기술 지원 및 문서 - Cisco Systems](#)