WLAN 컨트롤러(WLC)를 사용하여 EAP 인증 구성

목차

소개

이 문서에서는 외부 RADIUS 서버를 사용하여 EAP(Extensible Authentication Protocol) 인증을 위한 WLC(Wireless LAN Controller)를 구성하는 방법에 대해 설명합니다. 이 컨피그레이션 예에서는 사용자 자격 증명을 검증하기 위해 Cisco ACS(Secure Access Control Server)를 외부 RADIUS 서버로 사용합니다.

사전 요구 사항

요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- AP(Lightweight Access Point) 및 Cisco WLC의 구성에 대한 기본 지식
- LWAPP(Lightweight AP Protocol)에 대한 기본 지식
- Cisco Secure ACS와 같은 외부 RADIUS 서버를 구성하는 방법에 대한 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Aironet 1232AG Series Lightweight AP
- 펌웨어 5.1을 실행하는 Cisco 4400 Series WLC
- 버전 4.1을 실행하는 Cisco Secure ACS
- Cisco Aironet 802.11 a/b/g Client Adapter
- 펌웨어 4.2를 실행하는 Cisco Aironet Desktop Utility(ADU)

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.

구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

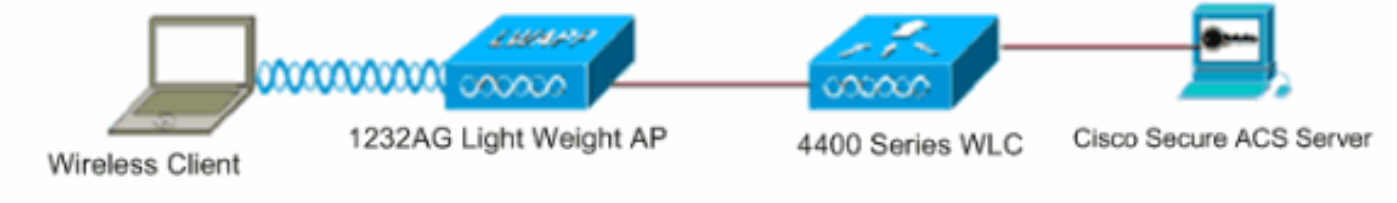
참고: 이 문서에 사용된 명령에 대한 자세한 내용을 보려면 명령 조회 도구(등록된 고객만 해당)를 사용하십시오.

EAP 인증을 위해 디바이스를 구성하려면 다음 단계를 완료합니다.

1. 기본 작동을 위해 WLC를 구성하고 경량 AP를 컨트롤러에 등록합니다.
2. 외부 RADIUS 서버를 통해 RADIUS 인증을 위한 WLC를 구성합니다.
3. WLAN 매개변수를 구성합니다.
4. Cisco Secure ACS를 외부 RADIUS 서버로 구성하고 클라이언트 인증을 위한 사용자 데이터베이스를 만듭니다.

네트워크 다이어그램

이 설정에서는 허브를 통해 Cisco 4400 WLC와 경량 AP가 연결됩니다. 외부 RADIUS 서버(Cisco Secure ACS)도 동일한 허브에 연결됩니다. 모든 디바이스가 동일한 서브넷에 있습니다. AP는 초기에 컨트롤러에 등록됩니다. LEAP(Lightweight Extensible Authentication Protocol) 인증을 위해 WLC 및 AP를 구성해야 합니다. AP에 연결하는 클라이언트는 LEAP 인증을 사용하여 AP와 연결합니다. Cisco Secure ACS는 RADIUS 인증을 수행하는 데 사용됩니다.



기본 작동을 위해 WLC를 구성하고 경량 AP를 컨트롤러에 등록

기본 작업을 위해 WLC를 구성하려면 CLI(Command Line Interface)에서 시작 컨피그레이션 마법사를 사용합니다. 또는 GUI를 사용하여 WLC를 구성할 수도 있습니다. 이 문서에서는 CLI에서 시작 컨피그레이션 마법사를 사용하여 WLC의 컨피그레이션에 대해 설명합니다.

WLC가 처음 부팅되면 시작 컨피그레이션 마법사로 직접 들어갑니다. 기본 설정을 구성하려면 컨피그레이션 마법사를 사용합니다. CLI 또는 GUI에서 마법사를 실행할 수 있습니다. 이 출력은 CLI에서 시작 컨피그레이션 마법사의 예를 보여줍니다.

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
System Name [Cisco_33:84:a0]: WLC-1
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (24 characters max): *****
Management Interface IP Address: 10.77.244.204
Management Interface Netmask: 255.255.255.224
Management Interface Default Router: 10.77.244.220
Management Interface VLAN Identifier (0 = untagged):
Management Interface Port Num [1 to 4]: 1
Management Interface DHCP Server IP Address: 10.77.244.220
AP Manager Interface IP Address: 10.77.244.205
AP-Manager is on Management subnet, using same values
AP Manager Interface DHCP Server (10.77.244.220):
Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: Test
Network Name (SSID): Cisco123
Allow Static IP Addresses [YES][no]: yes
Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.
Enter Country Code (enter 'help' for a list of countries) [US]:
Enable 802.11b Network [YES][no]: yes
Enable 802.11a Network [YES][no]: yes
Enable 802.11g Network [YES][no]: yes
Enable Auto-RF [YES][no]: yes

Configuration saved!
Resetting system with new configuration..
```

이러한 매개변수는 기본 작업을 위해 WLC를 설정합니다. 이 컨피그레이션 예에서 WLC는 **10.77.244.204**를 관리 인터페이스 IP 주소로, **10.77.244.205**를 AP-관리자 인터페이스 IP 주소로 사용합니다.

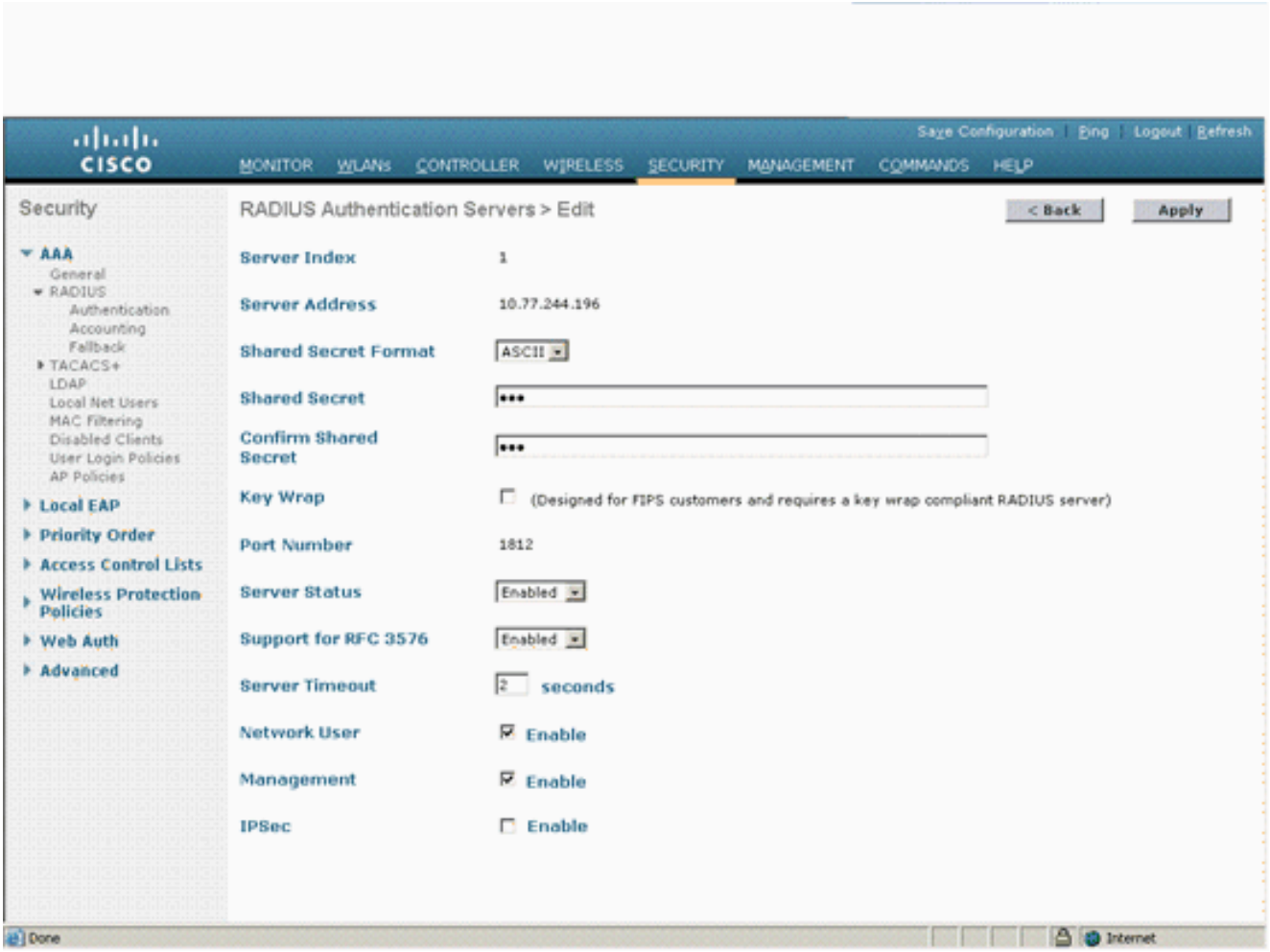
WLC에서 다른 기능을 구성하기 전에 경량 AP를 WLC에 등록해야 합니다. 이 문서에서는 경량 AP가 WLC에 등록된 것으로 가정합니다. 경량 AP가 WLC에 등록되는 방법에 대한 자세한 내용은 WLC(Wireless LAN Controller)에 대한 LAP(Lightweight AP) 등록을 참조하십시오.

외부 RADIUS 서버를 통해 RADIUS 인증을 위한 WLC 구성

사용자 자격 증명을 외부 RADIUS 서버로 전달하려면 WLC를 구성해야 합니다. 그런 다음 외부 RADIUS 서버가 사용자 자격 증명을 확인하고 무선 클라이언트에 대한 액세스를 제공합니다.

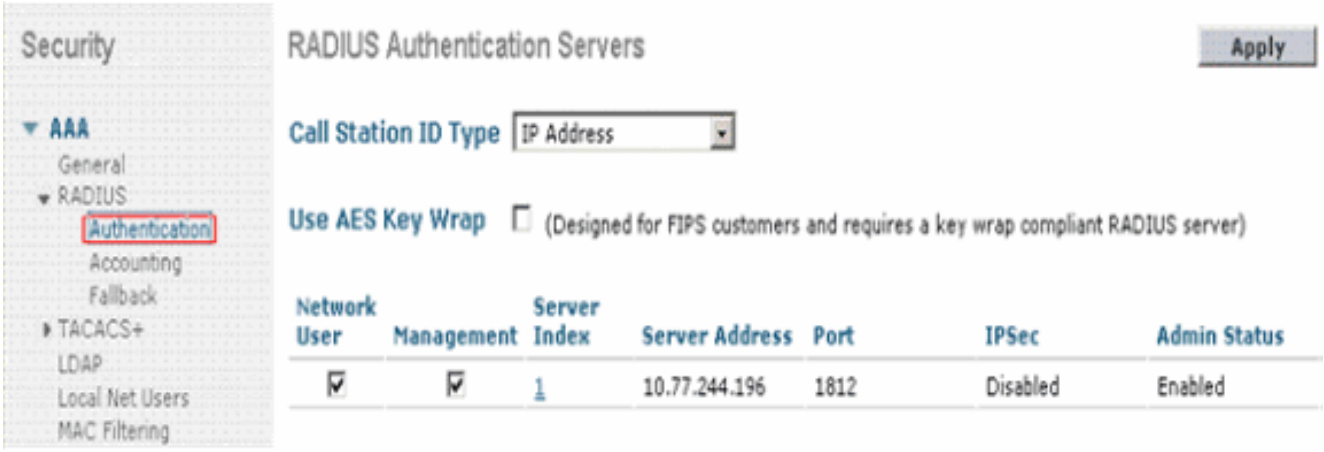
외부 RADIUS 서버에 대해 WLC를 구성하려면 다음 단계를 완료합니다.

1. RADIUS Authentication Servers(RADIUS **인증 서버**) 페이지를 표시하려면 컨트롤러 GUI에서 Security(보안) 및 RADIUS Authentication(RADIUS 인증)을 선택합니다. 그런 다음 **New**(새로 만들기)를 클릭하여 RADIUS 서버를 정의합니다
   .



2. RADIUS 인증 서버 > 새 페이지에서 RADIUS 서버 매개변수를 정의합니다. 이러한 매개변수에는 RADIUS 서버 IP 주소, 공유 암호, 포트 번호 및 서버 상태가 포함됩니다.Network User and Management(네트워크 사용자 및 관리) 확인란은 RADIUS 기반 인증이 WLC 관리 및 네트워크 사용자에 적용되는지 여부를 결정합니다. 이 예에서는 Cisco Secure ACS를 IP 주소가 10.77.244.196인 RADIUS 서버로 사용합니다.
3. 이제 WLC에서 인증을 위해 RADIUS 서버를 사용할 수 있습니다. Security(보안) > Radius(**RADIUS**) **> Authentication(인증)을** 선택하면 Radius Server(RADIUS 서버)가 **나열됩니다**

.



RFC 3576은 Cisco CNS CAR(Access Registrar) RADIUS 서버에서 지원되지만 Cisco Secure ACS Server 버전 4.0 이하에서는 지원되지 않습니다.로컬 RADIUS 서버 기능을 사용하여 사용자를 인증할 수도 있습니다. 로컬 RADIUS 서버가 버전 4.1.171.0 코드와 함께 도입되었습니다. 이전 버전을 실행하는 WLC에는 로컬 radius 기능이 없습니다. 로컬 EAP는 사용자 및 무선 클라이언트가 로컬로 인증될 수 있도록 하는 인증 방법입니다. 백엔드 시스템이 중단되거

나 외부 인증 서버가 다운될 때 무선 클라이언트와의 연결을 유지하려는 원격 사무실에서 사용하도록 설계되었습니다. 로컬 EAP는 사용자를 인증하기 위해 로컬 사용자 데이터베이스 또는 LDAP 백 엔드 데이터베이스에서 사용자 자격 증명을 검색합니다. 로컬 EAP는 LEAP, PAC를 사용하는 EAP-FAST, 인증서를 사용하는 EAP-FAST, 컨트롤러와 무선 클라이언트 간의 EAP-TLS 인증을 지원합니다.로컬 EAP는 백업 인증 시스템으로 설계되었습니다. 컨트롤러에 RADIUS 서버가 구성된 경우 컨트롤러는 먼저 RADIUS 서버로 무선 클라이언트를 인증하려고 시도합니다. RADIUS 서버가 시간 초과되었거나 RADIUS 서버가 구성되지 않았기 때문에 RADIUS 서버를 찾을 수 없는 경우에만 로컬 EAP를 시도합니다.무선 LAN 컨트롤러에서 로컬 EAP를 구성하는 방법에 대한 자세한 내용은 EAP-FAST 및 LDAP 서버 컨피그레이션을 사용하는 무선 LAN 컨트롤러의 로컬 EAP 인증 예를 참조하십시오.

WLAN 매개변수 구성

다음으로, 클라이언트가 무선 네트워크에 연결하는 데 사용하는 WLAN을 구성합니다. WLC에 대한 기본 매개변수를 구성한 경우 WLAN에 대한 SSID도 구성했습니다. WLAN에 이 SSID를 사용하거나 새 SSID를 생성할 수 있습니다. 이 예에서는 새 SSID를 생성합니다.

참고: 컨트롤러에서 최대 16개의 WLAN을 구성할 수 있습니다. Cisco WLAN 솔루션은 경량 AP에 대해 최대 16개의 WLAN을 제어할 수 있습니다. 각 WLAN에 고유한 보안 정책을 할당할 수 있습니다. 경량 AP는 모든 활성 Cisco WLAN 솔루션 WLAN SSID를 브로드캐스트하고 각 WLAN에 대해 정의하는 정책을 적용합니다.

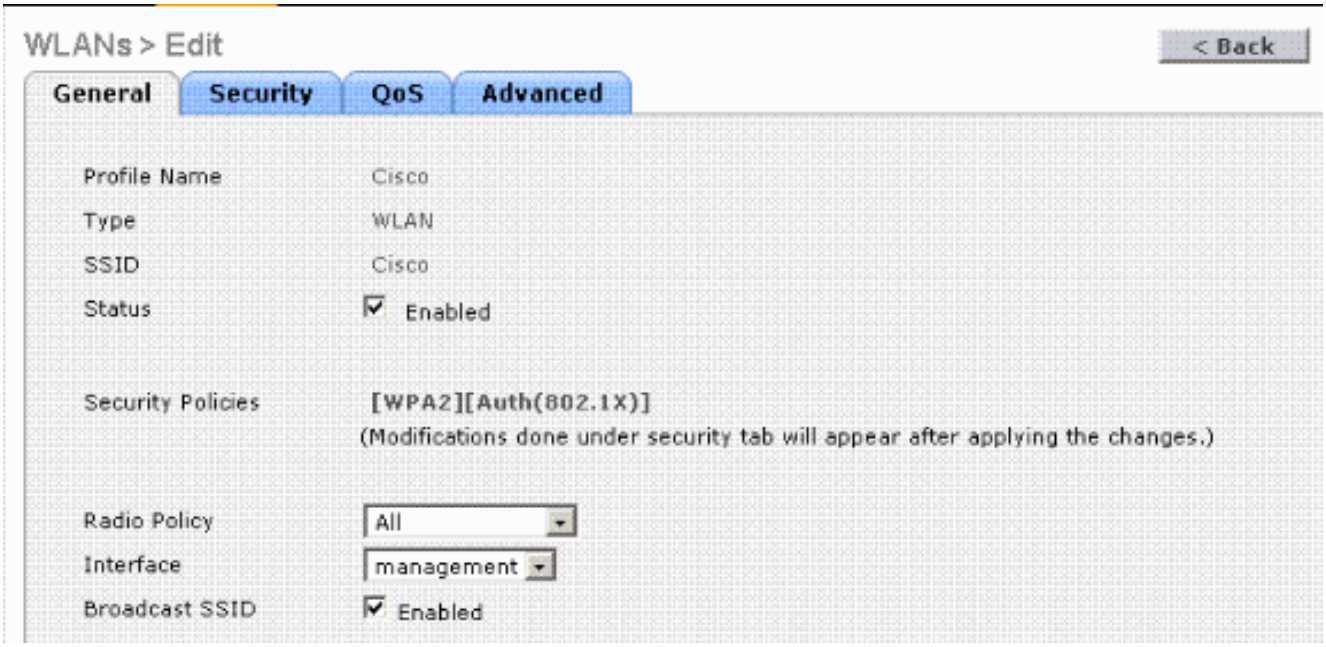
새 WLAN 및 관련 매개변수를 구성하려면 다음 단계를 완료합니다.

1. WLANs 페이지를 표시하려면 컨트롤러의 GUI에서 WLANs를 클릭합니다.이 페이지에는 컨트롤러에 있는 WLAN이 나열됩니다.
2. 새 WLAN을 생성하려면 New를 선택합니다. WLAN에 대한 프로파일 이름 및 WLAN SSID를 입력하고 Apply(적용)를 **클릭합니다**. 이 예에서는 Cisco를 SSID로 사용합니다

.

3. 새 WLAN을 생성하면 새 WLAN에 대한 WLAN > Edit 페이지가 나타납니다. 이 페이지에서는 일반 정책, 보안 정책, QOS 정책 및 기타 고급 매개변수를 포함하는 이 WLAN에 특정한 다양한 매개변수를 정의할 수 있습니다

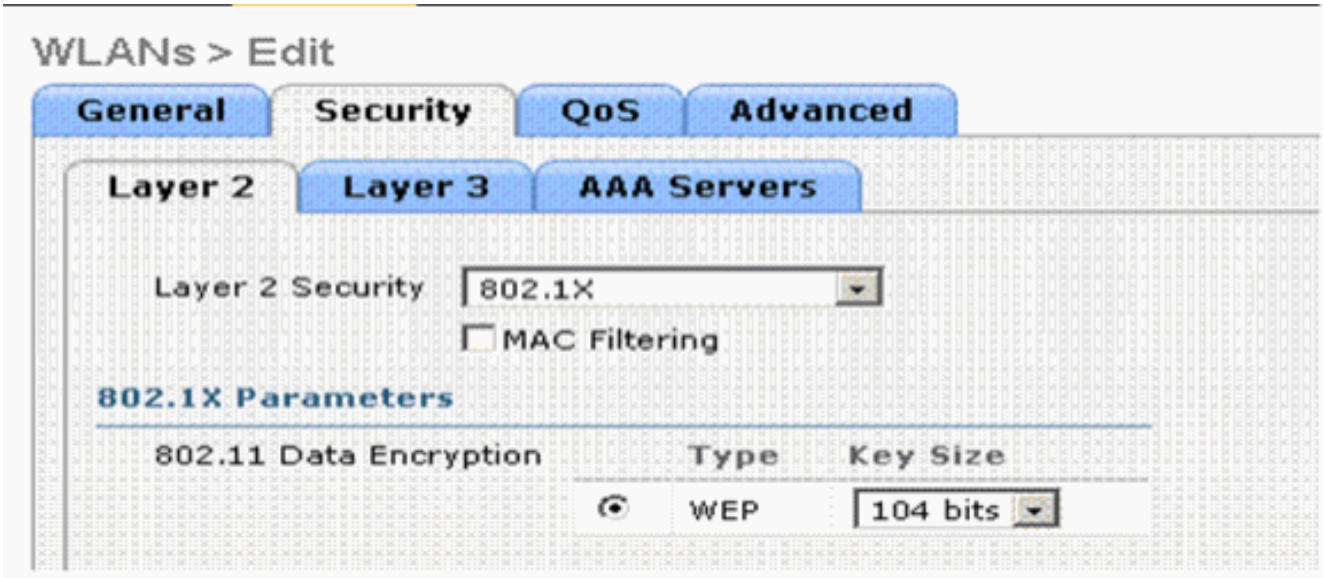
.



드롭다운 메뉴에서 적절한 인터페이스를 선택합니다. 다른 매개변수는 WLAN 네트워크의 요구 사항에 따라 수정할 수 있습니다.General Policies(일반 **정책**) 아래의 Status(상태) 상자를 선택하여 WLAN을 활성화합니다.

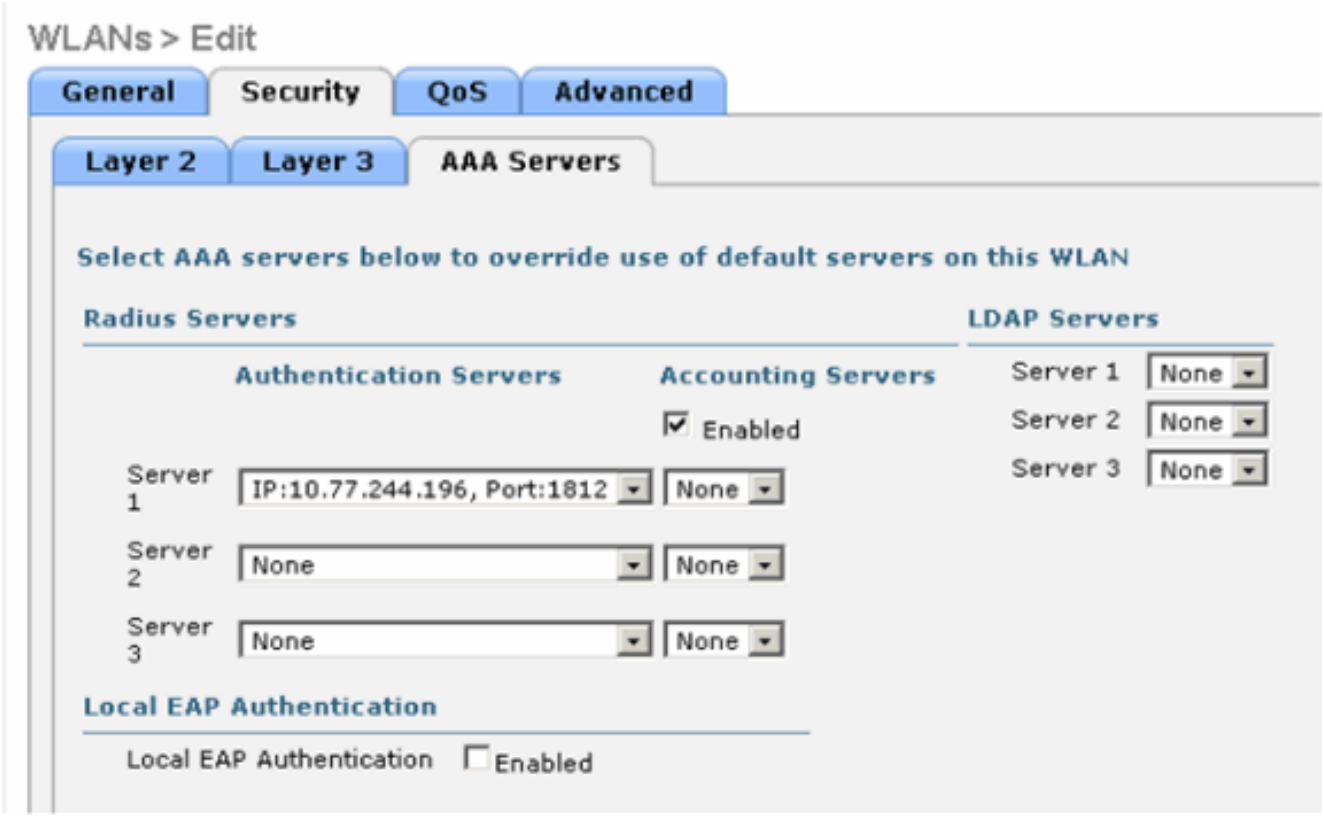
4. Security(**보안**) 탭을 클릭하고 Layer **2 Security(레이어 2 보안)를 선택합니다**. Layer 2 Security 드롭다운 메뉴에서 **802.1x**를 선택합니다. 802.1x 매개 변수에서 WEP 키 크기를 선택합니다. 이 예에서는 104비트 WEP 키와 24비트 초기화 벡터를 더한 128비트 WEP 키를 사용합니다

.



5. **AAA Servers(AAA 서버**) 탭**을** 선택합니다. Authentication Servers (RADIUS)(인증 서버 (RADIUS)) 드롭다운 메뉴에서 적절한 RADIUS 서버를 선택합니다. 이 서버는 무선 클라이언트를 인증하는 데 사용됩니다

.



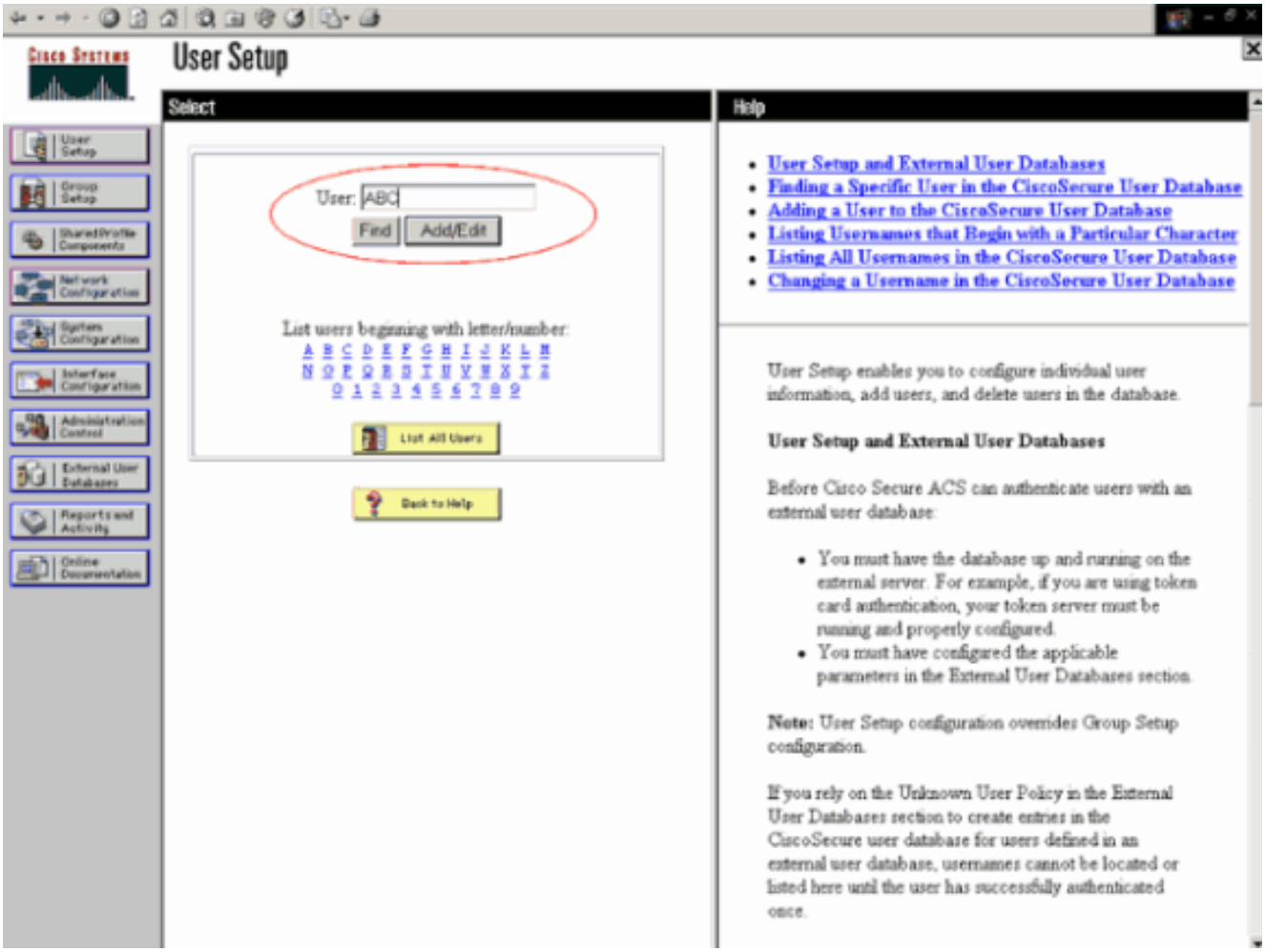
6. Apply(**적용**)를 클릭하여 컨피그레이션을 저장합니다.

Cisco Secure ACS를 외부 RADIUS 서버로 구성하고 인증 클라이언트에 대한 사용자 데이터베이스 생성

사용자 데이터베이스를 생성하고 Cisco Secure ACS에서 EAP 인증을 활성화하려면 다음 단계를 완료합니다.

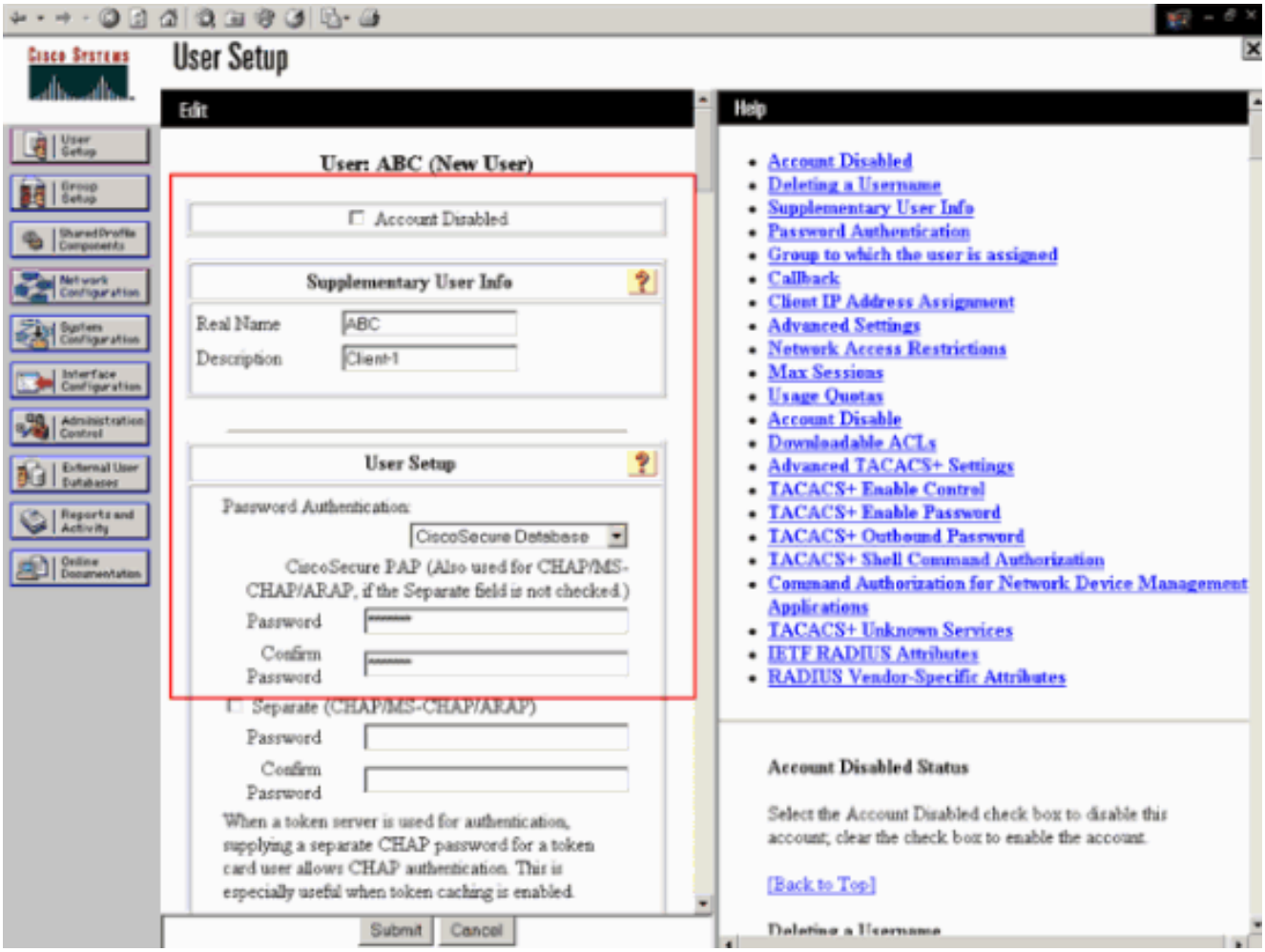
1. ACS GUI에서 **User Setup(사용자 설정)**을 선택하고 사용자 이름을 입력한 다음 Add/**Edit(추가/수정)를 클릭합니다**. 이 예에서는 사용자가 **ABC**입니다

.



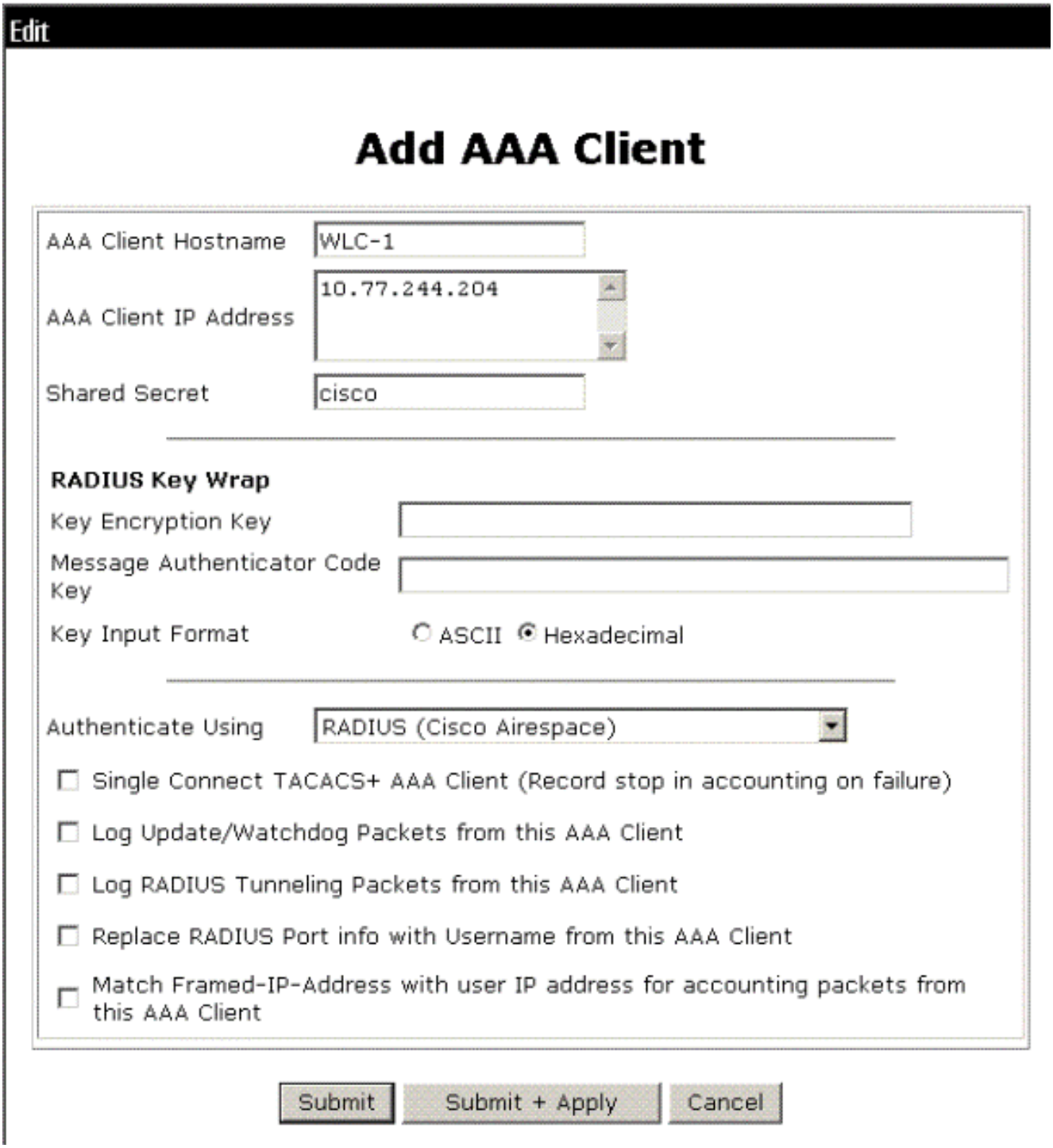
2. User Setup 페이지가 나타나면 해당 사용자에 대한 모든 매개변수를 정의합니다. 이 예에서는 EAP 인증을 위해 이 매개변수만 필요하므로 사용자 이름, 비밀번호 및 보조 사용자 정보가 구성됩니다.데이터베이스에 사용자를 더 추가하려면 Submit(제출)을 클릭하고 동일한 프로세스를 반복합니다. 기본적으로 모든 사용자는 기본 그룹 아래에 그룹화되고 그룹에 대해 정의된 것과 동일한 정책이 할당됩니다. 특정 사용자를 다른 그룹에 할당하려는 경우 자세한 내용은 User Guide for Cisco Secure ACS for Windows Server 3.2의 User Group Management 섹션을 참조하십시오

.



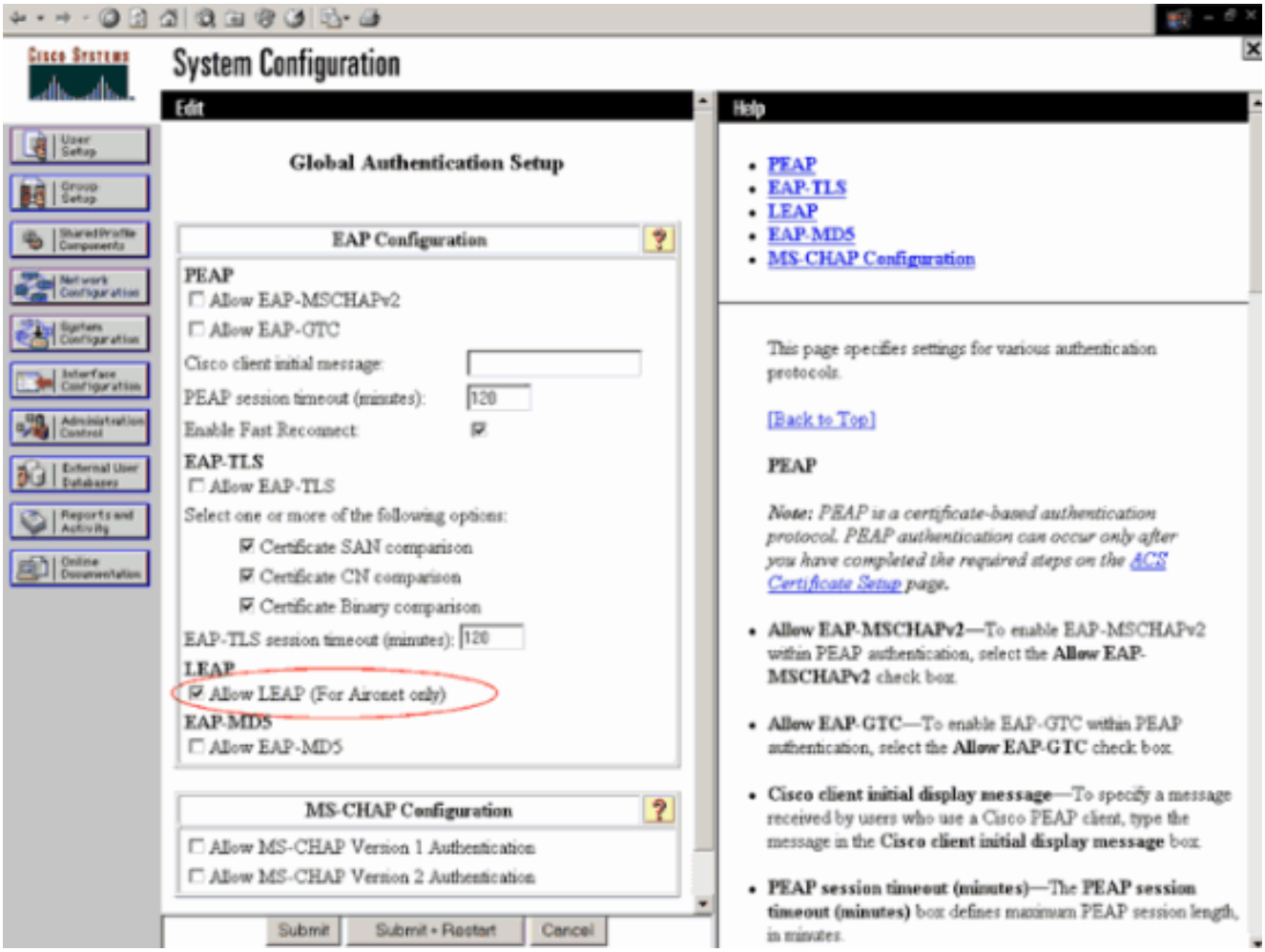
3. 컨트롤러를 ACS 서버에서 AAA 클라이언트로 정의합니다. ACS GUI에서 Network Configuration(네트워크 컨피그레이션)을 클릭합니다.Network Configuration(네트워크 컨피그레이션) 페이지가 나타나면 WLC의 이름, IP 주소, 공유 암호 및 인증 방법(RADIUS Cisco Airespace)을 정의합니다. 다른 비 ACS 인증 서버에 대해서는 제조업체의 설명서를 참조하십시오.**참고:** WLC 및 ACS 서버에서 구성하는 공유 비밀 키가 일치해야 합니다. 공유 암호는 대/소문자를 구분합니다

.



4. 원하는 EAP **인증** 방법**을** 수행하도록 인증 서버가 구성되어 있는지 확인하려면 System Configuration and **Global Authentication Setup**을 클릭합니다. EAP 컨피그레이션 설정에서 적절한 EAP 방법을 선택합니다. 이 예에서는 LEAP 인증을 사용합니다. 완료되면 **Submit(제출**)을 클릭합니다

.

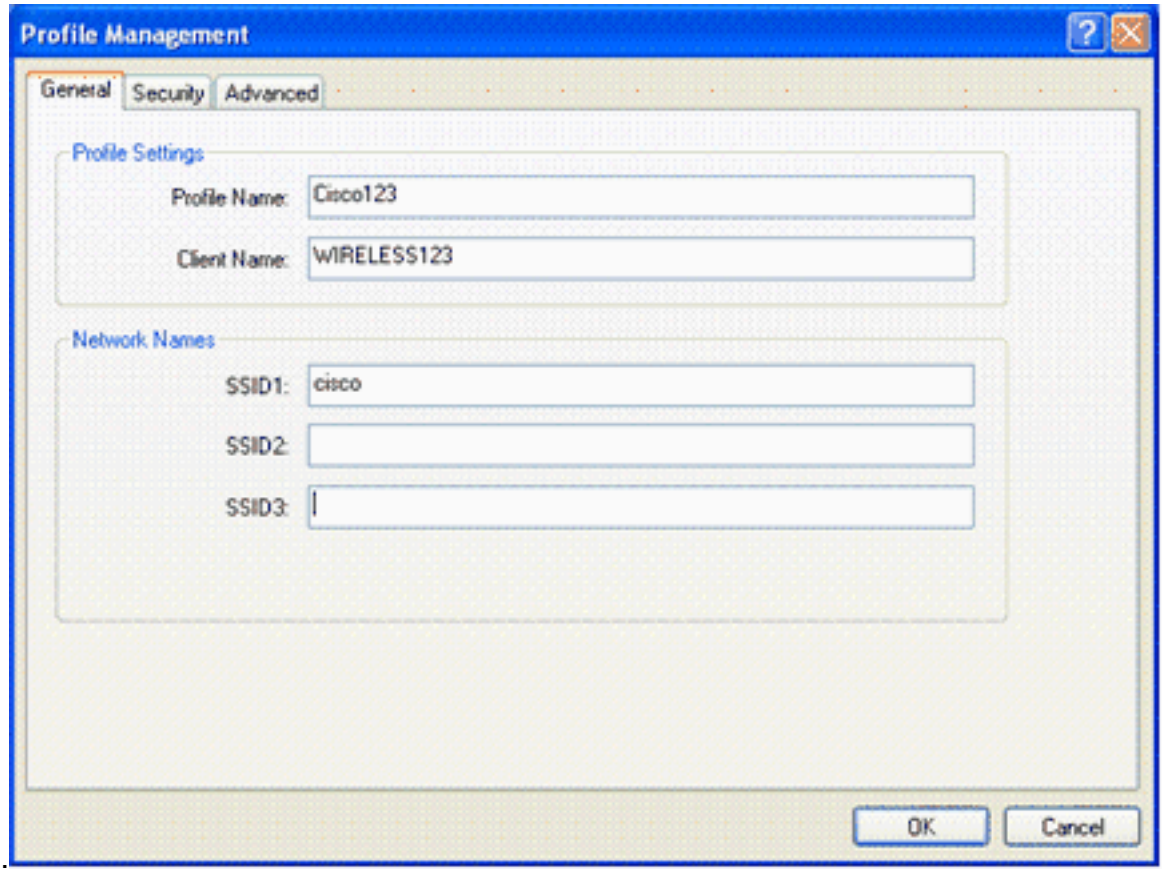


클라이언트 구성

또한 적절한 EAP 유형에 대해 클라이언트를 구성해야 합니다. 클라이언트는 EAP 협상 프로세스 중에 서버에 EAP 유형을 제안합니다. 서버가 해당 EAP 유형을 지원하는 경우 EAP 유형을 승인합니다. EAP 유형이 지원되지 않는 경우, Negative acknowledgement를 전송하고 클라이언트는 다른 EAP 방법으로 다시 협상합니다. 이 프로세스는 지원되는 EAP 유형이 협상될 때까지 계속됩니다. 이 예에서는 LEAP를 EAP 유형으로 사용합니다.

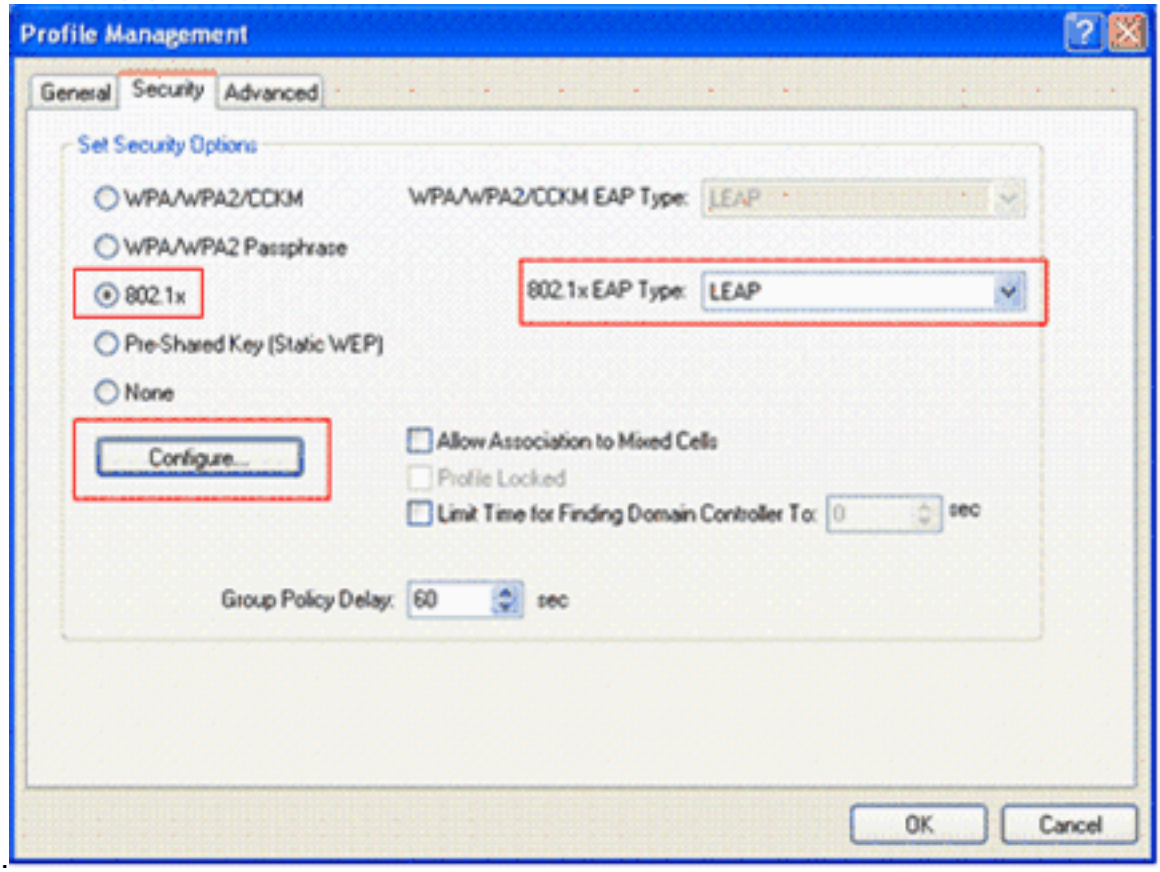
Aironet Desktop Utility를 사용하여 클라이언트에서 LEAP를 구성하려면 다음 단계를 완료하십시오 .

1. Aironet **Utility** 아이콘을 두 번 클릭하여 엽니다.
2. Profile **Management** 탭을 클릭합니다.
3. 프로파일을 클릭하고 Modify(수정)를 **선택합니다**.
4. General(일반) 탭에서 Profile Name(*프로파일 이름)을* 선택합니다. WLAN의 **SSID**를 입력합니

다. 

참고: SSID는 대/소문자를 구분하며 WLC에 구성된 SSID와 정확히 일치해야 합니다.

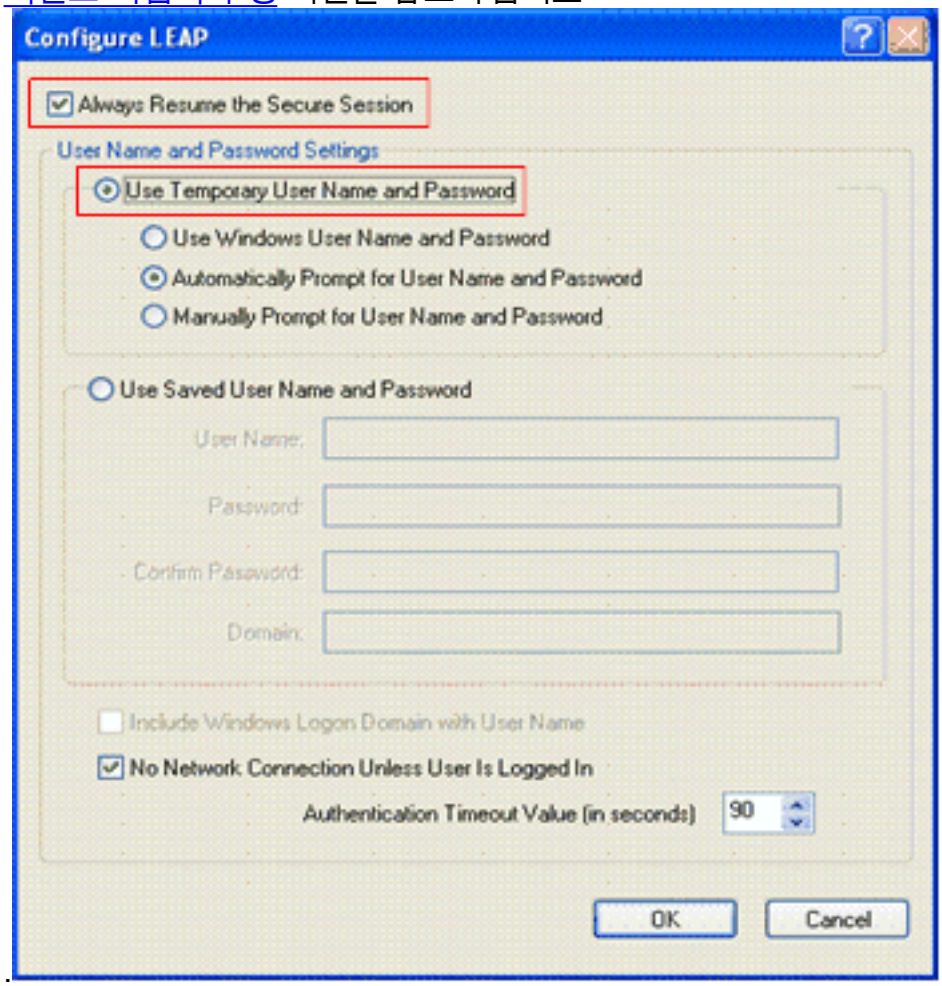
5. Security(**보안**) 탭 아래에서 *802.1x*를 선택합니다. LEAP로 EAP 유형**을** 선택하고 Configure**를 클릭합니다**



.

6. 컴퓨터**가 재부팅될** 때마다 사용자 자격 증명을 입력하라는 메시지를 표시하는 Use Temporary Username and Password를 선택합니다.여기에 제공된 세 가지 옵션 중 하나를 선택합니다. 이 예에서는 **Automatically Prompt for Username and Password(사용자 이름 및 비밀번호 자동 프롬프트**)를 사용합니다. 이 경우 *Windows 사용자 이름 및 비밀번호* 외에 LEAP

사용자 자격 증명을 입력해야 창에 로그인할 수 있습니다.LEAP 서 플리 컨 트가 클라이언트 어댑터가 로밍하고 네트워크에 다시 연결할 때마다 자격 증명을 다시 입력하라는 프롬프트를 표시하지 않고 항상 이전 세션을 다시 시작하도록 하려면 창 맨 위에 있는 Always Resume **the Secure Session** 확인란을 선택합니다.**참고:** 기타 옵션에 대한 자세한 내용은 Cisco Aironet 802.11a/b/g Wireless LAN Client Adapter(CB21AG 및 PI21AG) 설치 및 구성 설명서의 클라이언트 어댑터 구성 섹션을 참조하십시오



7. **고급** 탭 아래에서 프리앰블, Aironet 확장 및 기타 802.11 옵션(예: 전원, 주파수 등)을 구성할 수 있습니다.
8. **확인을 클릭합니다**. 이제 클라이언트가 구성된 매개변수와 연결하려고 시도합니다.

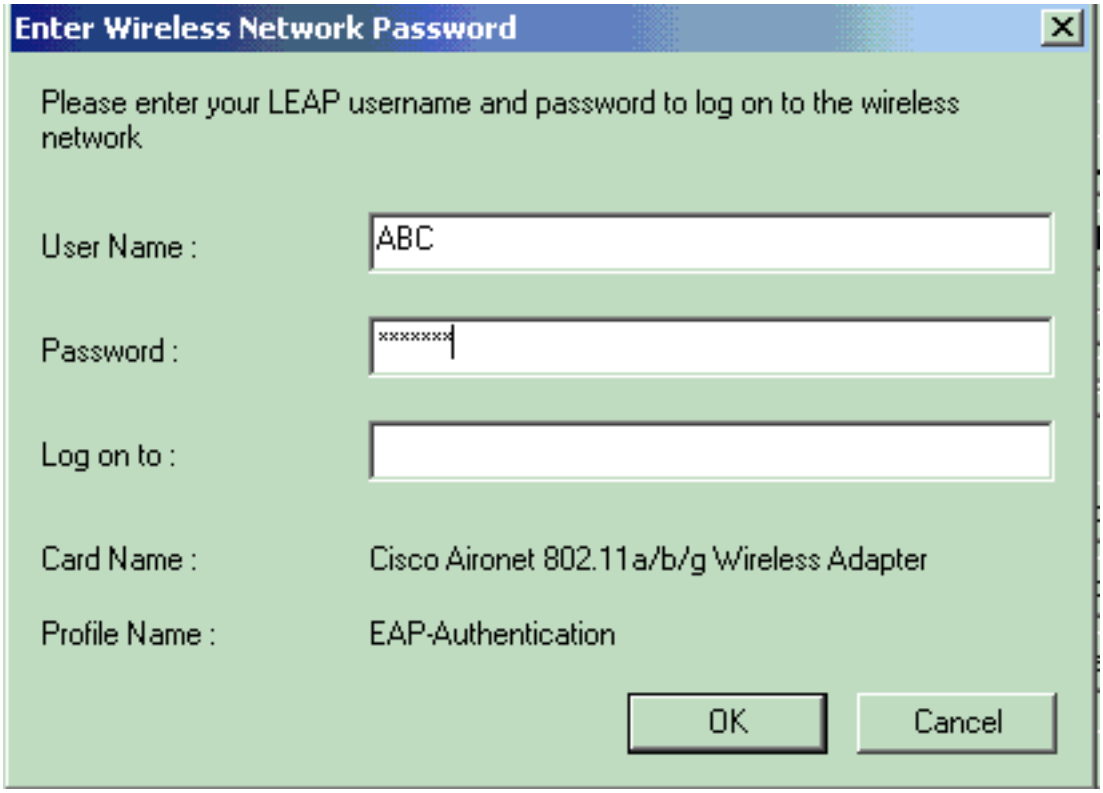
다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

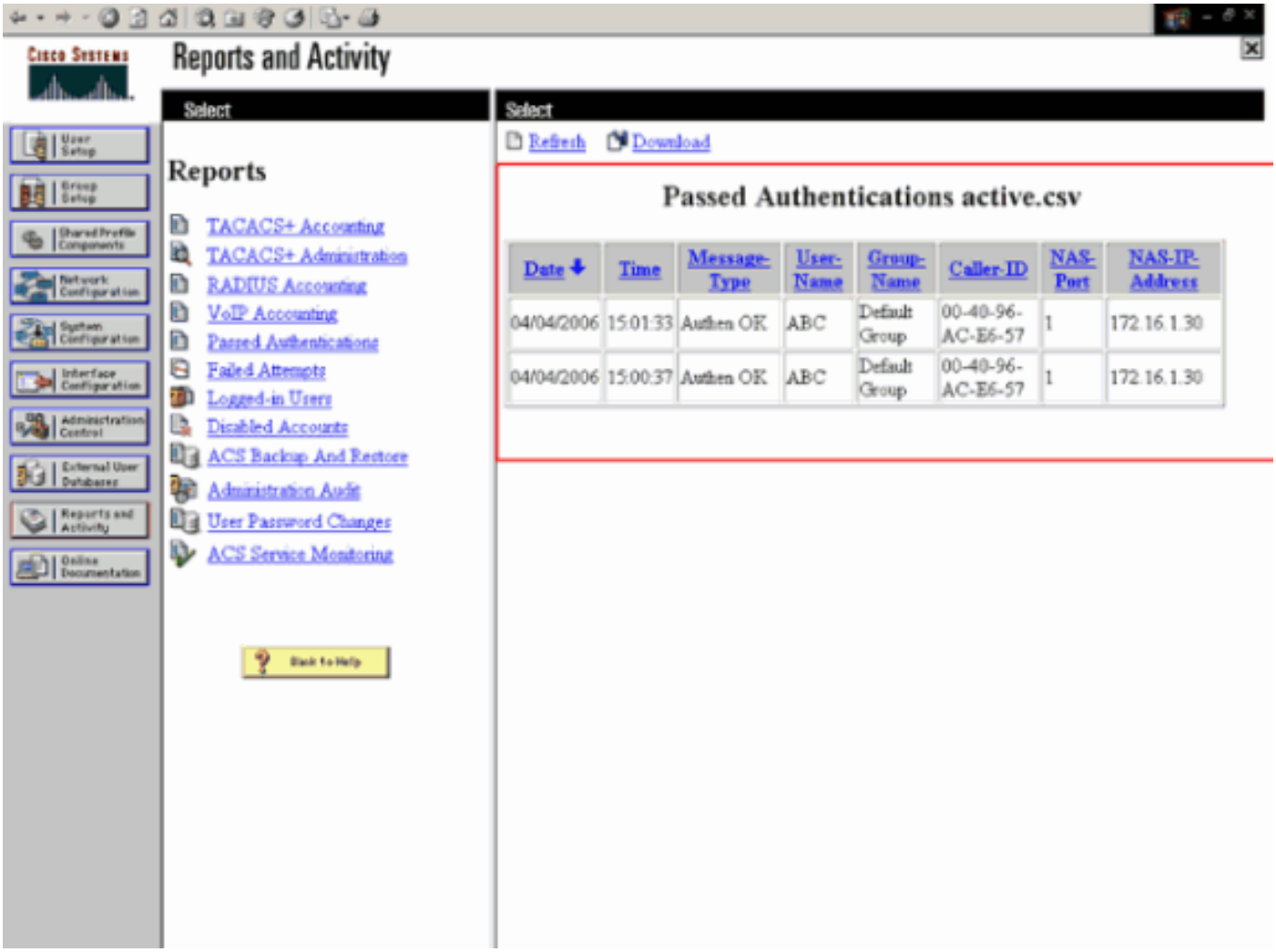
LEAP 인증을 사용하여 무선 클라이언트를 경량 AP와 연결하여 컨피그레이션이 예상대로 작동하는지 확인합니다.

참고: 이 문서에서는 클라이언트 프로파일이 LEAP 인증을 위해 구성된 것으로 가정합니다. LEAP 인증을 위해 802.11 a/b/g 무선 클라이언트 어댑터를 구성하는 방법에 대한 자세한 내용은 EAP 인증 사용을 참조하십시오.

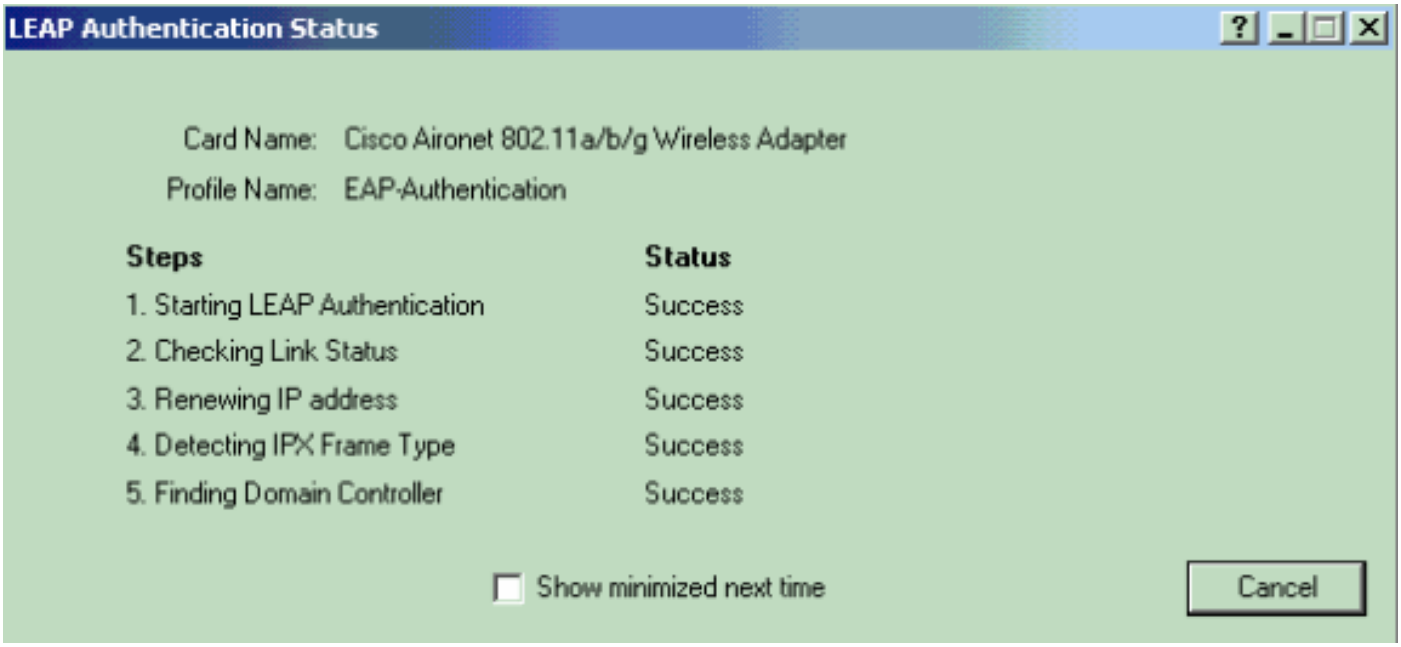
무선 클라이언트의 프로파일이 활성화되면 사용자에게 LEAP 인증을 위한 사용자 이름/비밀번호를 입력하라는 메시지가 표시됩니다. 예를 들면 다음과 같습니다.



경량 AP와 WLC는 자격 증명을 확인하기 위해 외부 RADIUS 서버(Cisco Secure ACS)에 사용자 자격 증명을 전달합니다. RADIUS 서버는 데이터를 사용자 데이터베이스와 비교하고 사용자 자격 증명을 확인하기 위해 사용자 자격 증명이 유효할 때마다 무선 클라이언트에 대한 액세스를 제공합니다. ACS 서버의 Passed Authentication 보고서는 클라이언트가 RADIUS 인증을 통과했음을 보여줍니다. 예를 들면 다음과 같습니다.



RADIUS 인증에 성공하면 무선 클라이언트가 경량형 AP와 연결됩니다.



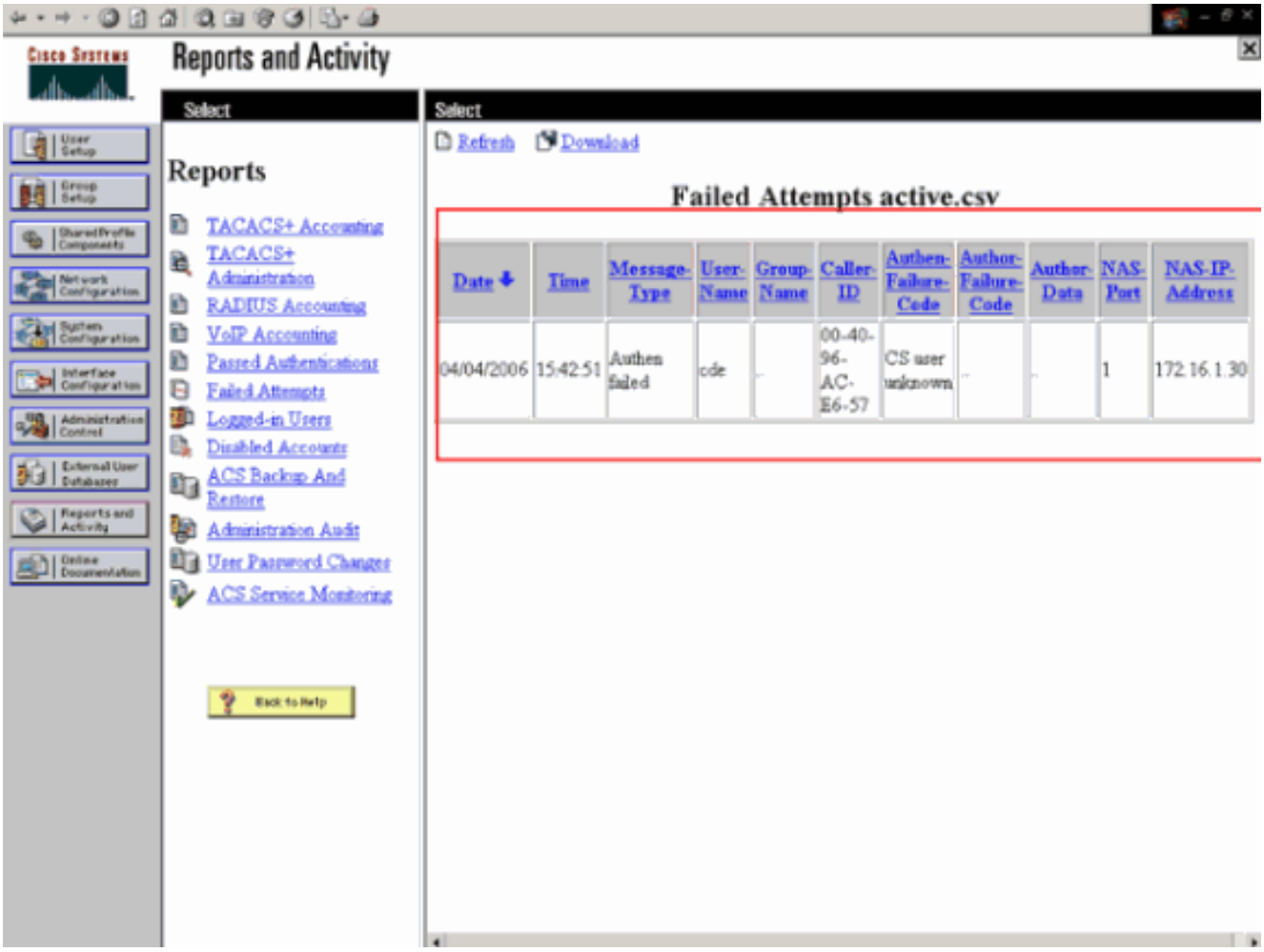
또한 WLC GUI의 **Monitor** 탭 아래에서 확인할 수 있습니다. Monitor(**모니터**) > **Clients(클라이언트**)를 선택하고 클라이언트의 MAC 주소를 확인합니다.

문제 해결

컨피그레이션 트러블슈팅을 위해 다음 단계를 완료합니다.

1. debug lwapp **events enable** 명령을 사용하여 AP가 WLC에 등록되는지 확인합니다.
2. RADIUS 서버가 무선 클라이언트에서 인증 요청을 수신하고 검증하는지 확인합니다. NAS-IP-주소, 날짜 및 시간을 확인하여 WLC가 RADIUS 서버에 연결할 수 있는지 확인합니다.이 작업을 수행하려면 ACS 서버에서 Passed Authentications and Failed Attempts 보고서를 확인합니다. 이러한 보고서는 ACS 서버의 Reports and Activities에서 사용할 수 있습니다. 다음은 RADIUS 서버 인증에 실패하는 경우의 예입니다

.



참고: Cisco Secure ACS의 문제 해결 및 디버그 정보를 가져오는 방법에 대한 자세한 내용은 Cisco Secure ACS for Windows의 버전 및 AAA 디버그 정보 가져오기를 참조하십시오.

3. AAA 인증을 트러블슈팅하기 위해 다음 **debug** 명령을 사용할 수도 있습니다.**debug aaa all enable** - 모든 AAA 메시지의 디버그를 구성합니다.**debug dot1x packet enable** - 모든 dot1x 패킷의 디버그를 활성화합니다.다음은 debug **802.1x aaa enable** 명령의 샘플 출력입니다.

```
(Cisco Controller) >debug dot1x aaa enable

*Sep 23 15:15:43.792: 00:40:96:ac:dd:05 Adding AAA_ATT_USER_NAME(1) index=0
*Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLING_STATION_ID(31)
    index=1
*Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLED_STATION_ID(30)
    index=2
*Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT(5) index=3
*Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IP_ADDRESS(4) index=4
*Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IDENTIFIER(32)
    index=5
*Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_VAP_ID(1) index=6
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_SERVICE_TYPE(6) index=7
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_FRAMED_MTU(12) index=8
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT_TYPE(61) index=9
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_EAP_MESSAGE(79) index=10
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_MESS_AUTH(80) index=11
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 AAA EAP Packet created request =
    0x1533a288.. !!!!
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Sending EAP Attribute (code=2, length=8,
    id=2) for mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.794: 00000000: 02 02 00 08 01 41 42 43
    .....ABC
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 [BE-req] Sending auth request to
    'RADIUS' (proto 0x140001)
*Sep 23 15:15:43.799: 00:40:96:ac:dd:05 [BE-resp] AAA response 'Interim
    Response'
*Sep 23 15:15:43.799: 00:40:96:ac:dd:05 [BE-resp] Returning AAA response
*Sep 23 15:15:43.799: 00:40:96:ac:dd:05 AAA Message 'Interim Response' received
    for mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.799: 00:40:96:ac:dd:05 Received EAP Attribute (code=1,
    length=19,id=3, dot1xcb->id = 2) for mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.799: 00000000: 01 03 00 13 11 01 00 08  42 3a 8e d1 18 24 e8 9f
    ........B:...
*Sep 23 15:15:43.799: 00000010: 41 42 43
    ABC
*Sep 23 15:15:43.799: 00:40:96:ac:dd:05 Skipping AVP (0/80) for mobile
    00:40:96:ac:dd:05
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_USER_NAME(1) index=0
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLING_STATION_ID(31)
    index=1
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLED_STATION_ID(30)
    index=2
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT(5) index=3
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IP_ADDRESS(4) index=4
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IDENTIFIER(32)
    index=5
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_VAP_ID(1) index=6
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_SERVICE_TYPE(6) index=7
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_FRAMED_MTU(12) index=8
*Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT_TYPE(61) index=9
*Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Adding AAA_ATT_EAP_MESSAGE(79) index=10
*Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Adding AAA_ATT_RAD_STATE(24) index=11
*Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Adding AAA_ATT_MESS_AUTH(80) index=12
*Sep 23 15:15:43.902: 00:40:96:ac:dd:05 AAA EAP Packet created request =
    0x1533a288.. !!!!
*Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Sending EAP Attribute (code=2,
    length=35, id=3) for mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.902: 00000000: 02 03 00 23 11 01 00 18  83 f1 5b 32 cf 65 04 ed
    ...#......[2.e..
```

```
*Sep 23 15:15:43.902: 00000010: da c8 4f 95 b4 2e 35 ac  c0 6b bd fa 57 50 f3 13
    ..O...5..k..WP..
*Sep 23 15:15:43.904: 00000020: 41 42 43
    ABC
*Sep 23 15:15:43.904: 00:40:96:ac:dd:05 [BE-req] Sending auth request to
    'RADIUS' (proto 0x140001)
*Sep 23 15:15:43.907: 00:40:96:ac:dd:05 [BE-resp] AAA response 'Interim
    Response'
*Sep 23 15:15:43.907: 00:40:96:ac:dd:05 [BE-resp] Returning AAA response
*Sep 23 15:15:43.907: 00:40:96:ac:dd:05 AAA Message 'Interim Response' received
    for mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.907: 00:40:96:ac:dd:05 Received EAP Attribute (code=3,
    length=4,id=3, dot1xcb->id = 3) for mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.907: 00000000: 03 03 00 04
    ....
*Sep 23 15:15:43.907: 00:40:96:ac:dd:05 Skipping AVP (0/80) for mobile
    00:40:96:ac:dd:05
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_USER_NAME(1) index=0
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLING_STATION_ID(31)
    index=1
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLED_STATION_ID(30)
    index=2
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT(5) index=3
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IP_ADDRESS(4) index=4
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IDENTIFIER(32)
    index=5
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_VAP_ID(1) index=6
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_SERVICE_TYPE(6) index=7
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_FRAMED_MTU(12) index=8
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT_TYPE(61) index=9
*Sep 23 15:15:43.915: 00:40:96:ac:dd:05 Adding AAA_ATT_EAP_MESSAGE(79) index=10
*Sep 23 15:15:43.915: 00:40:96:ac:dd:05 Adding AAA_ATT_RAD_STATE(24) index=11
*Sep 23 15:15:43.915: 00:40:96:ac:dd:05 Adding AAA_ATT_MESS_AUTH(80) index=12
*Sep 23 15:15:43.915: 00:40:96:ac:dd:05 AAA EAP Packet created request =
    0x1533a288.. !!!!
*Sep 23 15:15:43.915: 00:40:96:ac:dd:05 Sending EAP Attribute (code=1,
    length=19, id=3) for mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.915: 00000000: 01 03 00 13 11 01 00 08  29 23 be 84 e1 6c d6 ae
    ........)#...l..
*Sep 23 15:15:43.915: 00000010: 41 42 43
    ABC
*Sep 23 15:15:43.915: 00:40:96:ac:dd:05 [BE-req] Sending auth request to
    'RADIUS' (proto 0x140001)
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 [BE-resp] AAA response 'Success'
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 [BE-resp] Returning AAA response
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 AAA Message 'Success' received for
    mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[0]: attribute 8,
    vendorId 0, valueLen 4
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[1]: attribute 79,
    vendorId 0, valueLen 35
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 Received EAP Attribute (code=2,
    length=35,id=3) for mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.918: 00000000: 02 03 00 23 11 01 00 18  03 66 2c 6a b3 a6 c3 4c
    ...#.....f,j...L
*Sep 23 15:15:43.918: 00000010: 98 ac 69 f0 1b e8 8f a2  29 eb 56 d6 92 ce 60 a6
    ..i.....).V...`.
*Sep 23 15:15:43.918: 00000020: 41 42 43
    ABC
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[2]: attribute 1,
    vendorId 9, valueLen 16
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[3]: attribute 25,
    vendorId 0, valueLen 21
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[4]: attribute 80,
```

```
vendorId 0, valueLen 16
```

참고: 디버그 출력의 일부 행은 공간 제약 조건으로 인해 래핑되었습니다.

4. RADIUS 서버가 사용자 자격 증명을 수신하는지 확인하기 위해 WLC의 로그를 모니터링합니다. WLC GUI에서 로그를 확인하려면 Monitor를 클릭합니다. 왼쪽 메뉴에서 **Statistics**(통계)를 클릭하고 옵션 목록에서 **Radius 서버**를 클릭합니다.WLC의 RADIUS 서버 컨피그레이션이 잘못된 경우 RADIUS 서버가 사용자 자격 증명을 받지 못하는 경우가 있으므로 이는 매우 중요합니다.RADIUS 매개변수가 잘못 구성된 경우 WLC에 로그가 표시되는 방법은 다음과 같습니다

.

show wlan summary 명령의 조합을 사용하여 어떤 WLAN에서 RADIUS 서버 인증을 사용하는지 인식할 수 있습니다. 그런 다음 **show client summary** 명령을 보고 어떤 MAC 주소(클라이언트)가 RADIUS WLAN에서 성공적으로 인증되었는지 확인할 수 있습니다. 또한 이를 Cisco Secure ACS에서 시도 또는 실패한 시도 로그와 연계할 수 있습니다.

문제 해결 정보

- 컨트롤러에서 RADIUS 서버가 상태이고 또는 않았는지 .
- WLC에서 **Radius** 서버에 연결할 수 있는지 확인하려면 ping 명령을 사용합니다.
- WLAN(SSID)의 드롭다운 메뉴에서 RADIUS 서버가 선택되었는지 확인합니다.
- WPA를 사용하는 경우 Windows XP SP2용 최신 Microsoft WPA 핫픽스를 설치해야 합니다. 또한 클라이언트 신청자용 드라이버를 최신 버전으로 업그레이드해야 합니다.
- PEAP를 수행하는 경우, 예를 들어 XP, SP2에서 Microsoft wireless-0 유틸리티로 카드를 관리하는 경우 Microsoft에서 KB885453 패치를 받아야 합니다.Windows Zero Config/클라이언트 서 플리 컨 트를 사용하는 경우 **빠른 재연결 활성화를 비활성화합니다**. Wireless Network Connection Properties(**무선 네트워크 연결 속성) > Wireless Networks(무선 네트워크) > Preferred networks(기본 설정 네트워크)를** 선택한 경우 이 작업을 수행할 수 있습니다. 그런 다음 SSID **> 속성 > 열기 > WEP > 인증 > EAP 유형 > PEAP > 속성 > 빠른 재연결 활성화 를** 선택합니다. 그런 다음 창 끝에서 활성화 또는 비활성화 옵션을 찾을 수 있습니다.
- 인텔 2200 또는 2915 카드가 있는 경우 인텔 웹 사이트에서 해당 카드의 알려진 문제에 대한 설명을 참조하십시오.인텔® PRO/무선 2200BG 네트워크 연결인텔® PRO/무선 2915ABG 네트워크 연결문제를 피하기 위해 최신 인텔 드라이버를 다운로드합니다. 인텔 드라이버는 http://downloadcenter.intel.com/에서 다운로드할 수 있습니다.
- WLC에서 적극적인 장애 조치 기능이 활성화된 경우 WLC가 너무 공격적이어서 AAA 서버가 것으로 . 그러나 AAA 서버가 해당 특정 클라이언트에만 응답하지 않을 수 있으므로 이 작업은 수행하지 않아야 합니다. 유효한 인증서가 있는 다른 유효한 클라이언트에 대한 응답일 수 있습니다. 그러나 WLC는 여전히 AAA 서버가 응답하지 않는 것으로 표시할 수 있습니다.이를 해결하려면 적극적인 장애 조치 기능을 비활성화합니다. 컨트롤러 GUI에서 **config radius**

aggressive-failover disable 명령을 실행하여 이를 수행합니다. 이 기능이 비활성화된 경우, RADIUS 서버로부터 응답을 받지 못한 연속된 세 개의 클라이언트가 있는 경우 컨트롤러는 다음 AAA 서버로 장애 조치됩니다.

EAP 타이머 조작

802.1x 인증 중에 사용자는 `DOT1X-1-MAX_EAPOL_KEY_RETRANS_FOR_MOBILE` 볼 수 있습니다. `xx:xx:xx:xx:xx:xx:xx` 오류 메시지 `EAPOL-Key M1` .

이 오류 메시지는 클라이언트가 WPA(802.1x) 키 협상 중에 컨트롤러에 제때 응답하지 않았음을 나타냅니다. 컨트롤러는 키 협상 중에 응답에 대한 타이머를 설정합니다. 일반적으로 이 메시지가 표시되면 신청자의 문제 때문입니다. 최신 버전의 클라이언트 드라이버 및 펌웨어를 실행해야 합니다. WLC에는 클라이언트 인증에 도움이 되도록 조작할 수 있는 몇 개의 EAP 타이머가 있습니다. 이러한 EAP 타이머에는 다음이 포함됩니다.

```
EAP-Identity-Request Timeout
EAP-Identity-Request Max Retries
EAP-Request Timeout (seconds)
EAP-Request Max Retries
EAPOL-Key Timeout
EAPOL-Key Max Retries
```

이러한 값을 조작하려면 먼저 해당 값이 무엇을 하고 어떻게 변경되었다가 네트워크에 어떤 영향을 주는지 파악해야 합니다.

- **EAP-ID-요청 시간 초과:**이 타이머는 EAP ID 요청 간의 대기 시간에 영향을 줍니다. 기본적으로 1초(4.1 이하) 및 30초(4.2 이상)입니다. 이러한 변화의 이유는 일부 클라이언트, 핸드헬드, 전화, 스캐너 등이 빠르게 대응하는 데 어려움을 겪었기 때문입니다. 랩톱과 같은 장치는 일반적으로 이러한 값을 조작할 필요가 없습니다. 사용 가능한 값은 1~120입니다.그러면 이 속성이 30 값으로 설정되면 어떻게 됩니까? 클라이언트가 처음 연결되면 EAPOL Start를 네트워크로 전송하고 WLC는 EAP 패킷을 전송하여 사용자 또는 시스템의 ID를 요청합니다. WLC가 ID 응답을 받지 못하면 첫 번째 ID 요청 후 30초 후에 또 다른 ID 요청을 보냅니다. 이는 클라이언트가 로밍할 때 초기 연결에서 발생합니다.타이머를 늘리면 어떻게 됩니까? 만약 모든 것이 좋다면, 아무런 영향도 없다. 그러나 네트워크에 문제가 있을 경우(클라이언트 문제, AP 문제 또는 RF 문제 포함) 네트워크 연결이 지연될 수 있습니다. 예를 들어 타이머를 최대값인 120초로 설정하면 WLC는 ID 요청 사이에 2분을 기다립니다. 클라이언트가 로밍되고 WLC에서 응답을 받지 못한 경우, 이 클라이언트에 대해 최소 2분 동안 중단이 생성되었습니다.이 타이머에 대한 권장 사항은 *5*입니다. 현재 이 타이머를 최대값에 배치할 이유는 없습니다.
- **EAP-ID-요청 최대 재시도 횟수:**Max Retries(최대 재시도 횟수) 값은 WLC가 MSCB에서 해당 항목을 제거하기 전에 클라이언트에 ID 요청을 보내는 횟수입니다. Max Retries(최대 재시도 횟수)에 도달하면 WLC는 클라이언트에 인증 해제 프레임을 전송하여 EAP 프로세스를 다시 시작해야 합니다. 사용 가능한 값은 1~20입니다. 다음으로, 이를 자세히 살펴보겠습니다.Max Retries(최대 재시도 횟수)는 ID 시간 초과와 함께 작동합니다. ID 시간 초과가 120으로 설정되어 있고 최대 재시도 횟수가 20으로 설정된 경우 2400(또는 120 * 20)이 얼마나 소요됩니까? 즉, 클라이언트를 제거하고 EAP 프로세스를 다시 시작하는 데 40분이 걸립니다. Identity Timeout(ID 시간 초과)을 5로 설정하고 Max Retries(최대 재시도 횟수) 값을 12로 설정하면 60(또는 5 * 12)이 소요됩니다. 이전 예와 달리, 클라이언트가 제거되고 EAP를 시작해야 할 때까지 1분이 걸립니다.최대 재시도 횟수의 권장 사항은 *12입니다*.
- **EAPOL-키 시간 초과:**EAPOL-Key Timeout 값의 경우 기본값은 1초 또는 1000밀리초입니다.

즉, AP와 클라이언트 간에 EAPOL 키가 교환될 때 AP는 키를 보내고 클라이언트가 응답할 때까지 기본적으로 최대 1초까지 기다립니다. 정의된 시간 값을 기다린 후 AP가 키를 다시 전송합니다. 이 설정을 변경하려면 **config advanced eap eapol-key-timeout *<time>* 명령을** 사용할 수 있습니다. 6.0의 사용 가능한 값은 200~5000밀리초이며, 6.0 이전의 코드는 1초에서 5초 사이의 값을 허용합니다. 키 시도에 응답하지 않는 클라이언트가 있는 경우 타이머를 확장하여 응답하는 데 시간이 조금 더 걸릴 수 있습니다. 그러나 이 경우 전체 802.1x 프로세스를 새로 시작하기 위해 WLC/AP가 클라이언트를 인증하는 데 걸리는 시간이 길어집니다.

- **EAPOL-키 최대 재시도 횟수:**EAPOL-Key Max Retries(EAPOL-키 최대 재시도 횟수) 값의 경우 기본값은 2입니다. 즉, 클라이언트에 대한 원래 키 시도를 두 번 재시도합니다. 이 설정은 config **advanced eap eapol-key-retries *<retries>* 명령**을 사용하여 변경할 수 있습니다. 사용 가능한 값은 0~4번 재시도입니다. EAPOL-Key Timeout(즉, 1초)에 대한 기본값 및 EAPOL-Key Retry(2)에 대한 기본값을 사용하면 클라이언트가 초기 키 시도에 응답하지 않을 경우 프로세스는 다음과 같이 진행됩니다.AP가 클라이언트에 키 시도를 보냅니다.1초간 기다렸다가 회신을 합니다.응답이 없으면 첫 번째 EAPOL-Key Retry(EAPOL-키 재시도)가 전송됩니다.1초간 기다렸다가 회신을 합니다.응답이 없으면 두 번째 EAPOL-Key Retry(EAPOL-키 재시도)가 전송됩니다.클라이언트로부터 아직 응답이 없고 재시도 값이 충족되면 클라이언트가 인증되지 않습니다. EAPOL-Key Timeout과 마찬가지로 EAPOL-Key 재시도 값을 확장하면 어떤 경우에는 유용할 수 있습니다. 그러나 이 값을 최대로 설정하면 인증 취소 메시지가 길어지기 때문에 다시 손상될 수 있습니다.

문제 해결을 위해 ACS RADIUS 서버에서 패키지 파일 추출

ACS를 외부 RADIUS 서버로 사용하는 경우 이 섹션을 사용하여 컨피그레이션 문제를 해결할 수 있습니다. package.cab는 ACS를 효율적으로 트러블슈팅하기 위해 필요한 모든 파일을 포함하는 Zip 파일입니다. CSSupport.exe 유틸리티를 사용하여 package.cab를 만들거나 파일을 수동으로 수집할 수 있습니다.

WCS에서 패키지 파일을 생성하고 추출하는 방법에 대한 자세한 내용은 *Getting Version and AAA Debug Information for Windows* for Cisco Secure ACS for Windows의 package.cab 파일 생성 섹션을 참조하십시오.

관련 정보

- 경량 액세스 포인트에 대한 WLAN 컨트롤러 장애 조치 컨피그레이션 예
- WLC(Wireless LAN Controller) 소프트웨어 업그레이드
- Cisco Wireless LAN Controller 명령 참조
- 기술 지원 및 문서 – Cisco Systems