Cisco Unified Wireless Network 컨피그레이션의 Wi-Fi Protected Access(WPA) 예

목차

소개

이 문서에서는 Cisco Unified Wireless Network에서 WPA(Wi-Fi Protected Access)를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 컨피그레이션을 시도하기 전에 다음 항목에 대한 기본 지식을 갖추고 있는지 확인합니다.

- WPA
- 무선 LAN(WLAN) 보안 솔루션**참고:** Cisco WLAN 보안 솔루션에 대한 자세한 내용은 Cisco Wireless LAN Security Overview(Cisco Wireless LAN 보안 개요)를 참조하십시오.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco 1000 Series LAP(Lightweight Access Point)

- 펌웨어 4.2.61.0을 실행하는 Cisco 4404 WLC(Wireless LAN Controller)
- 펌웨어 4.1을 실행하는 Cisco 802.11a/b/g 클라이언트 어댑터
- 펌웨어 4.1을 실행하는 ADU(Aironet Desktop Utility)
- Cisco Secure ACS 서버 버전 4.1

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 참조하십시오.

WPA 및 WPA2 지원

Cisco Unified Wireless Network에는 Wi-Fi Alliance 인증 WPA 및 WPA2에 대한 지원이 포함되어 있습니다. WPA는 2003년 Wi-Fi Alliance에 의해 도입되었습니다. WPA2는 2004년 Wi-Fi Alliance에 의해 도입되었습니다. WPA2에 대해 Wi-Fi 인증을 받은 모든 제품은 WPA에 대해 Wi-Fi 인증을 받은 제품과 상호 운용되어야 합니다.

WPA 및 WPA2는 최종 사용자 및 네트워크 관리자에게 데이터가 비공개로 유지되며 네트워크에 대한 액세스가 인증된 사용자로 제한됨을 높은 수준으로 보장합니다. 두 가지 모두 두 시장 부문의 고유한 요구 사항을 충족하는 개인 및 기업 운영 모드를 보유하고 있습니다. 각각의 엔터프라이즈 모드는 인증에 IEEE 802.1X 및 EAP를 사용합니다. 각각의 개인 모드에서는 인증에 PSK(Pre-Shared Key)를 사용합니다. Cisco는 사용자 인증에 PSK를 사용하므로 비즈니스 또는 정부 구축에 개인 모드를 권장하지 않습니다. PSK는 엔터프라이즈 환경에서 안전하지 않습니다.

WPA는 원래 IEEE 802.11 보안 구현의 알려진 모든 WEP 취약점을 해결하여 엔터프라이즈 및 SOHO(소규모 사무실/홈 오피스) 환경 모두에서 WLAN에 즉각적인 보안 솔루션을 제공합니다. WPA는 암호화에 TKIP를 사용합니다.

WPA2는 차세대 Wi-Fi 보안입니다. Wi-Fi Alliance는 승인된 IEEE 802.11i 표준을 상호 운용 가능하게 구현한 것입니다. CCMP(Counter Mode with Cipher Block Chaining Message Authentication Code Protocol)를 사용하여 NIST(National Institute of Standards and Technology) 권장 AES 암호화 알고리즘을 구현합니다. WPA2는 정부 FIPS 140-2 규정 준수를 용이하게 합니다.

WPA 및 WPA2 모드 유형 비교

	WPA	WPA2
엔터프라이즈 모드(비즈니스, 정부, 교육)	• 인증: IEEE 802.1X/EAP • 암호화: TKIP/MIC	• 인증: IEEE 802.1X/EAP • 암호화: AES-CCMP
개인 모드(SOHO, 홈/개인)	• 인증: PSK • 암호화: TKIP/MIC	• 인증: PSK • 암호화: AES-CCMP

엔터프라이즈 운영 모드에서 WPA 및 WPA2는 모두 802.1X/EAP를 사용하여 인증합니다. 802.1X는 클라이언트와 인증 서버 간의 강력한 상호 인증을 WLAN에 제공합니다. 또한 802.1X는 사용자별, 세션별 동적 암호화 키를 제공하므로, 정적 암호화 키를 둘러싼 관리 부담과 보안 문제가 해소됩니다.

802.1X에서는 로그온 비밀번호와 같은 인증에 사용되는 자격 증명이 암호화되지 않은 상태로 또는 암호화되지 않은 상태로 무선 매체를 통해 전송되지 않습니다. 802.1X 인증 유형은 무선 LAN에 대한 강력한 인증을 제공하지만, 표준 802.11 WEP 암호화는 네트워크 공격에 취약하기 때문에 802.1X 외에도 암호화에 TKIP 또는 AES가 필요합니다.

여러 802.1X 인증 유형이 있으며, 각각 클라이언트와 액세스 포인트 간 통신에 동일한 프레임워크 및 EAP에 의존하면서 서로 다른 인증 방식을 제공합니다. Cisco Aironet 제품은 다른 어떤 WLAN 제품보다 더 많은 802.1X EAP 인증 유형을 지원합니다. 지원되는 유형은 다음과 같습니다.

- Cisco LEAP
- EAP-FAST(Flexible Authentication via Secure Tunneling)
- EAP-TLS(EAP-Transport Layer Security)
- PEAP(Protected Extensible Authentication Protocol)
- EAP-TTLS(EAP-Tunneled TLS)
- EAP-SIM(EAP-Subscriber Identity Module)

802.1X 인증의 또 다른 이점은 정책 기반 키 순환, 동적 키 할당, 동적 VLAN 할당, SSID 제한 등 WLAN 사용자 그룹을 중앙 집중식으로 관리할 수 있다는 것입니다. 이러한 기능은 암호화 키를 회전합니다.

개인 운영 모드에서는 사전 공유 키(비밀번호)가 인증에 사용됩니다. 개인 모드에는 액세스 포인트 및 클라이언트 장치만 필요하지만 엔터프라이즈 모드에는 일반적으로 네트워크에 RADIUS 또는 기타 인증 서버가 필요합니다.

이 문서에서는 Cisco Unified Wireless 네트워크에서 WPA2(엔터프라이즈 모드) 및 WPA2-PSK(개인 모드)를 구성하는 예를 제공합니다.

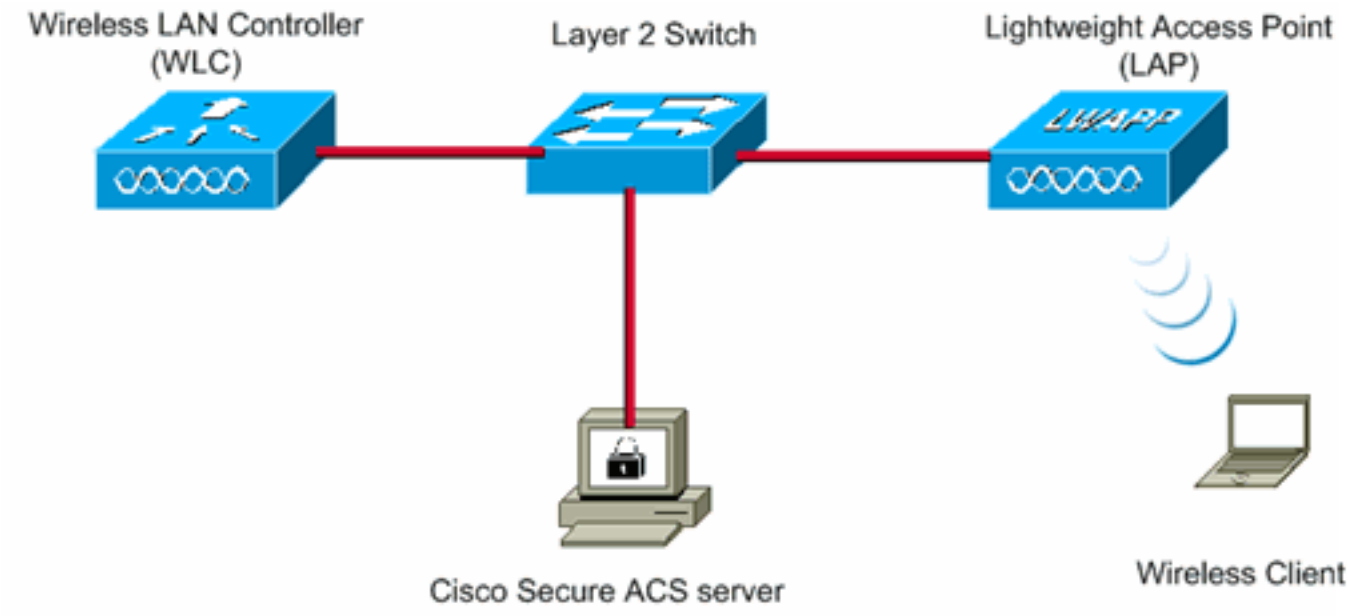
네트워크 설정

이 설정에서는 Cisco 4404 WLC와 Cisco 1000 Series LAP가 레이어 2 스위치를 통해 연결됩니다. 외부 RADIUS 서버(Cisco Secure ACS)도 동일한 스위치에 연결됩니다. 모든 디바이스가 동일한 서브넷에 있습니다. LAP(Access Point)는 컨트롤러에 처음 등록됩니다. WPA2 엔터프라이즈 모드용 무선 LAN과 WPA2 개인 모드용 무선 LAN 두 개를 만들어야 합니다.

WPA2-엔터프라이즈 모드 WLAN(SSID: WPA2-엔터프라이즈)은 무선 클라이언트 인증에 EAP-FAST를 사용하고 암호화에 AES를 사용합니다. Cisco Secure ACS 서버는 무선 클라이언트 인증을 위한 외부 RADIUS 서버로 사용됩니다.

WPA2-개인 모드 WLAN(SSID: WPA2-PSK)은 미리 공유된 키 "abcdefghijk"를 사용하는 인증에 WPA2-PSK를 사용합니다.

이 설정에 대한 장치를 구성해야 합니다.



WLC Management IP address:	10.77.244.204
WLC AP Manager IP address:	10.77.244.205
Wireless Client IP address:	10.77.244.221
Cisco Secure ACS server IP address	10.77.244.196
Subnet Mask used in this example	255.255.255.224

WPA2 엔터프라이즈 모드에 대한 장치 구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

WPA2 엔터프라이즈 작동 모드에 대한 장치를 구성하려면 다음 단계를 수행하십시오.

1. 외부 RADIUS 서버를 통한 RADIUS 인증을 위한 WLC 구성
2. WPA2 엔터프라이즈 모드 인증(EAP-FAST)을 위한 WLAN 구성
3. WPA2 엔터프라이즈 모드에 대한 무선 클라이언트 구성

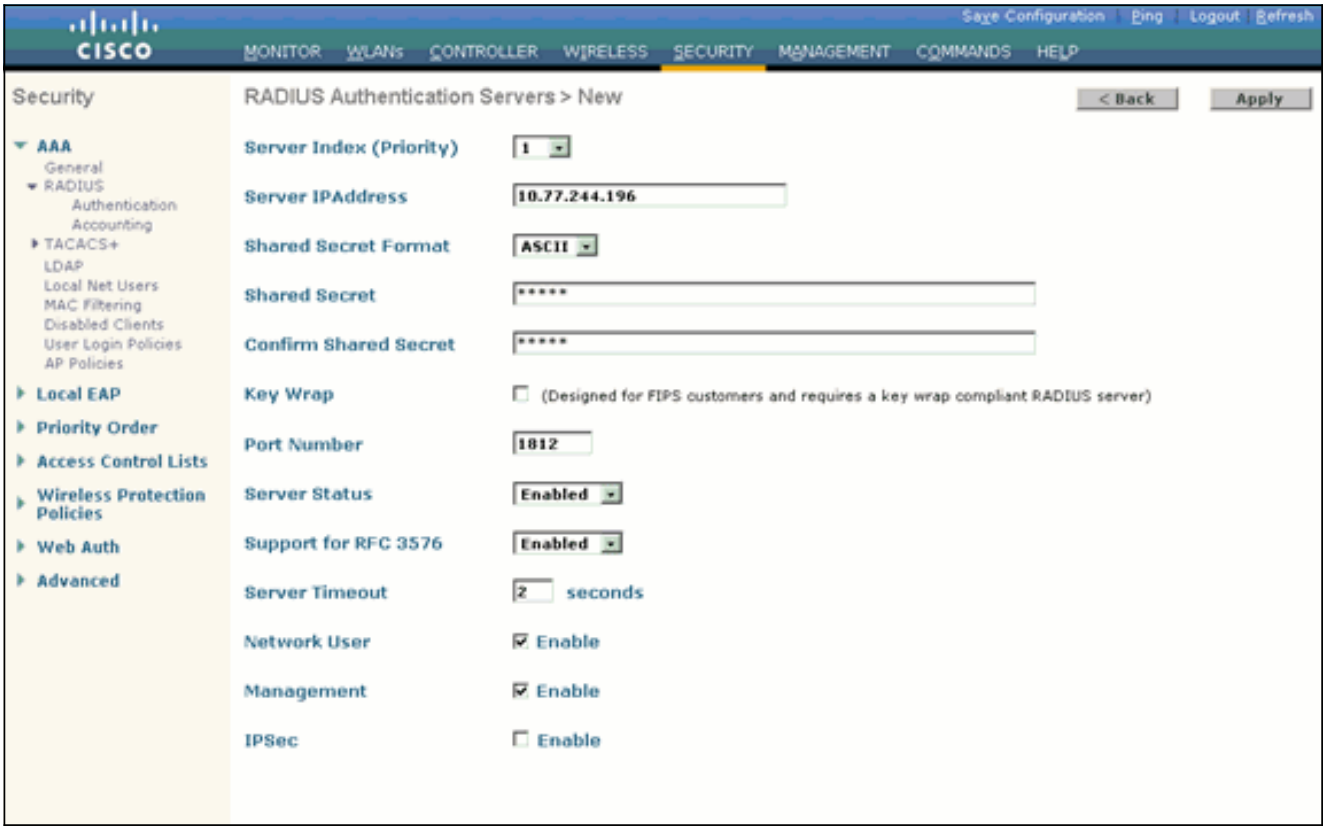
외부 RADIUS 서버를 통한 RADIUS 인증을 위한 WLC 구성

외부 RADIUS 서버에 사용자 자격 증명을 전달하려면 WLC를 구성해야 합니다. 그런 다음 외부 RADIUS 서버는 EAP-FAST를 사용하여 사용자 자격 증명을 검증하고 무선 클라이언트에 대한 액세스를 제공합니다.

외부 RADIUS 서버에 대한 WLC를 구성하려면 다음 단계를 완료합니다.

1. 컨트롤러 GUI에서 **Security** and **RADIUS Authentication(보안** 및 RADIUS 인증)을 선택하여 RADIUS Authentication Servers(RADIUS 인증 서버) 페이지를 표시합니다. 그런 다음 RADIUS **서버**를 정의하려면 New(새로 만들기)를 클릭합니다.
2. RADIUS Authentication Servers(RADIUS 인증 서버) **> New(새) 페이지에서 RADIUS 서버 매개변수를** 정의합니다. 이러한 매개변수에는 다음이 포함됩니다.RADIUS 서버 IP 주소공유 암호포트 번호서버 상태이 문서에서는 IP 주소가 10.77.244.196인 ACS 서버를 사용합니다

.



3. Apply를 **클릭합니다**.

WPA2 엔터프라이즈 작동 모드에 대한 WLAN 구성

다음으로, 클라이언트가 무선 네트워크에 연결하는 데 사용할 WLAN을 구성합니다. WPA2 엔터프라이즈 모드의 WLAN SSID는 WPA2-Enterprise입니다. 이 예에서는 이 WLAN을 관리 인터페이스에 할당합니다.

WLAN 및 관련 매개변수를 구성하려면 다음 단계를 완료합니다.

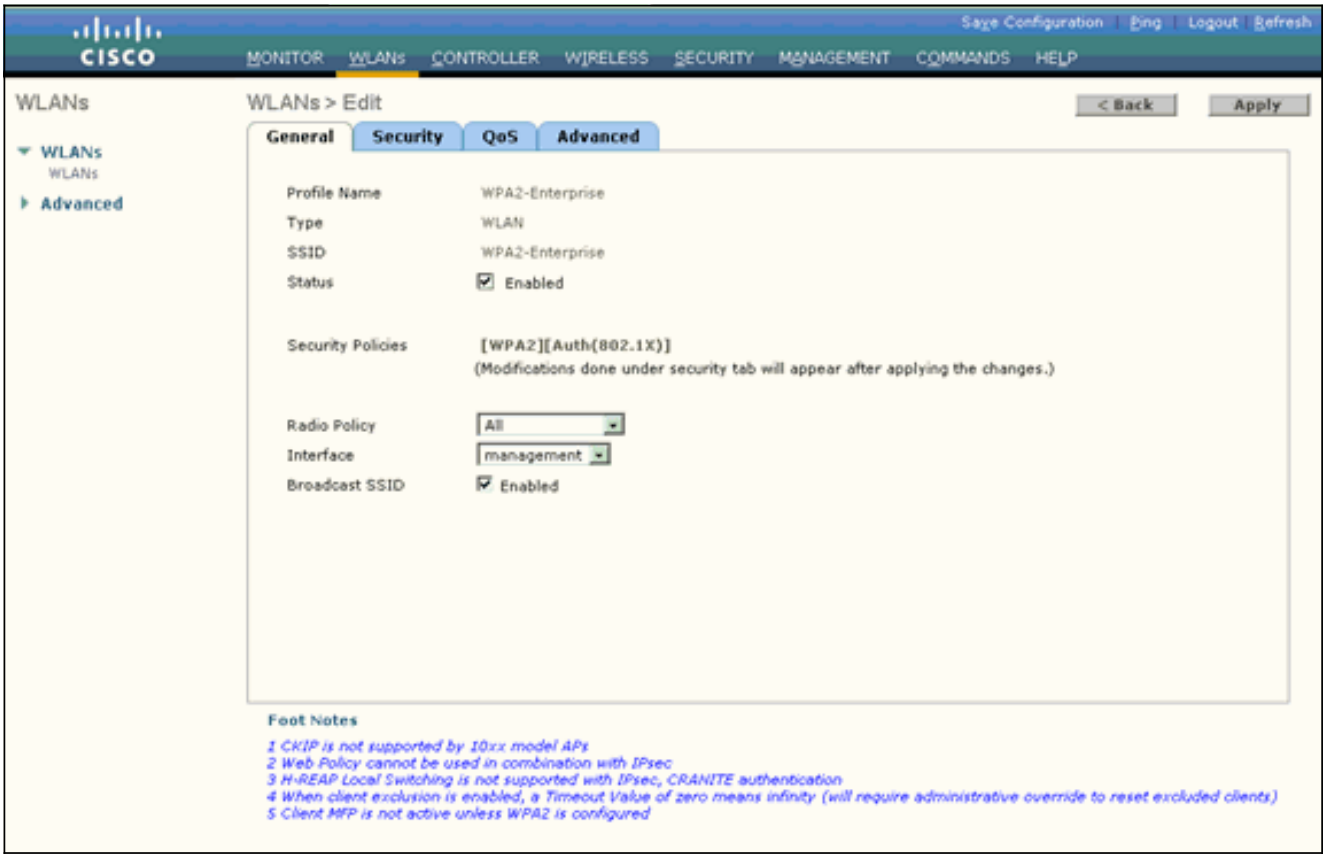
1. WLANs **페이지**를 표시하려면 컨트롤러의 GUI에서 WLANs를 클릭합니다.이 페이지에는 컨트롤러에 있는 WLAN이 나열됩니다.
2. 새 **WLAN**을 생성하려면 New(새로 만들기)를 클릭합니다.
3. WLANs(WLAN) > New(새로 만들기) 페이지에서 WLAN SSID **이름**과 프로파일 **이름을** 입력합니다. 그런 다음 Apply를 **클릭합니다**.이 예에서는 **WPA2-Enterprise**를 SSID로 사용합니다

.

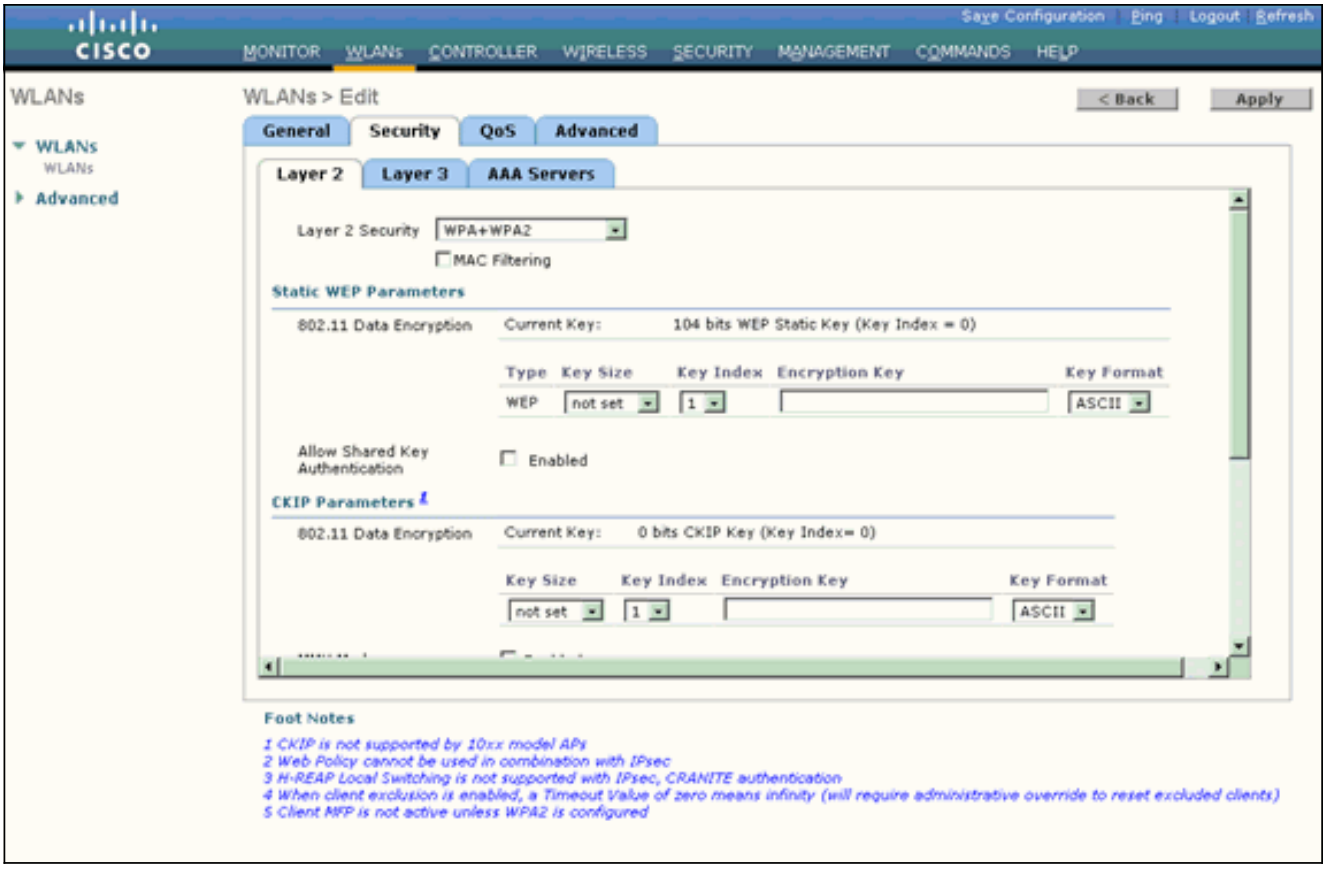
4. 새 WLAN을 생성하면 새 WLAN에 대한 **WLAN > Edit** 페이지가 나타납니다. 이 페이지에서 이 WLAN에 대한 다양한 매개변수를 정의할 수 있습니다. 여기에는 일반 정책, 보안 정책, QOS

정책 및 고급 매개변수가 포함됩니다.

5. General Policies(일반 정책)에서 **Status(상태)** 확인란을 선택하여 WLAN을 활성화합니다
.

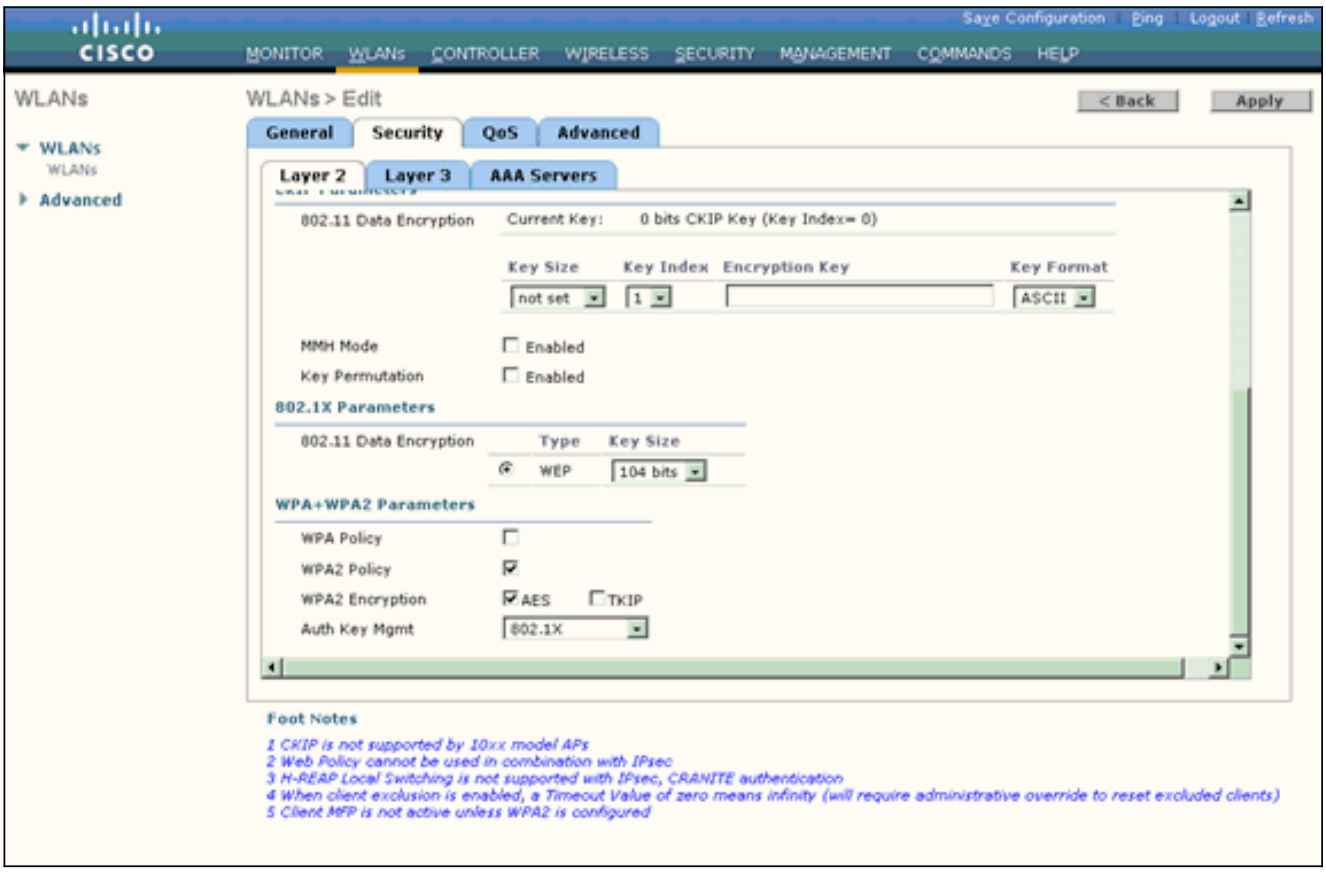


6. AP가 비콘 프레임에서 SSID를 브로드캐스트하도록 하려면 Broadcast SSID(브로드캐스트 SSID) **확인란**을 선택합니다.
7. **보안** 탭을 클릭합니다. Layer 2 Security(레이어 2 보안) 아래에서 **WPA+WPA2를** 선택합니다 .이렇게 하면 WLAN에 대한 WPA 인증이 활성화됩니다
.



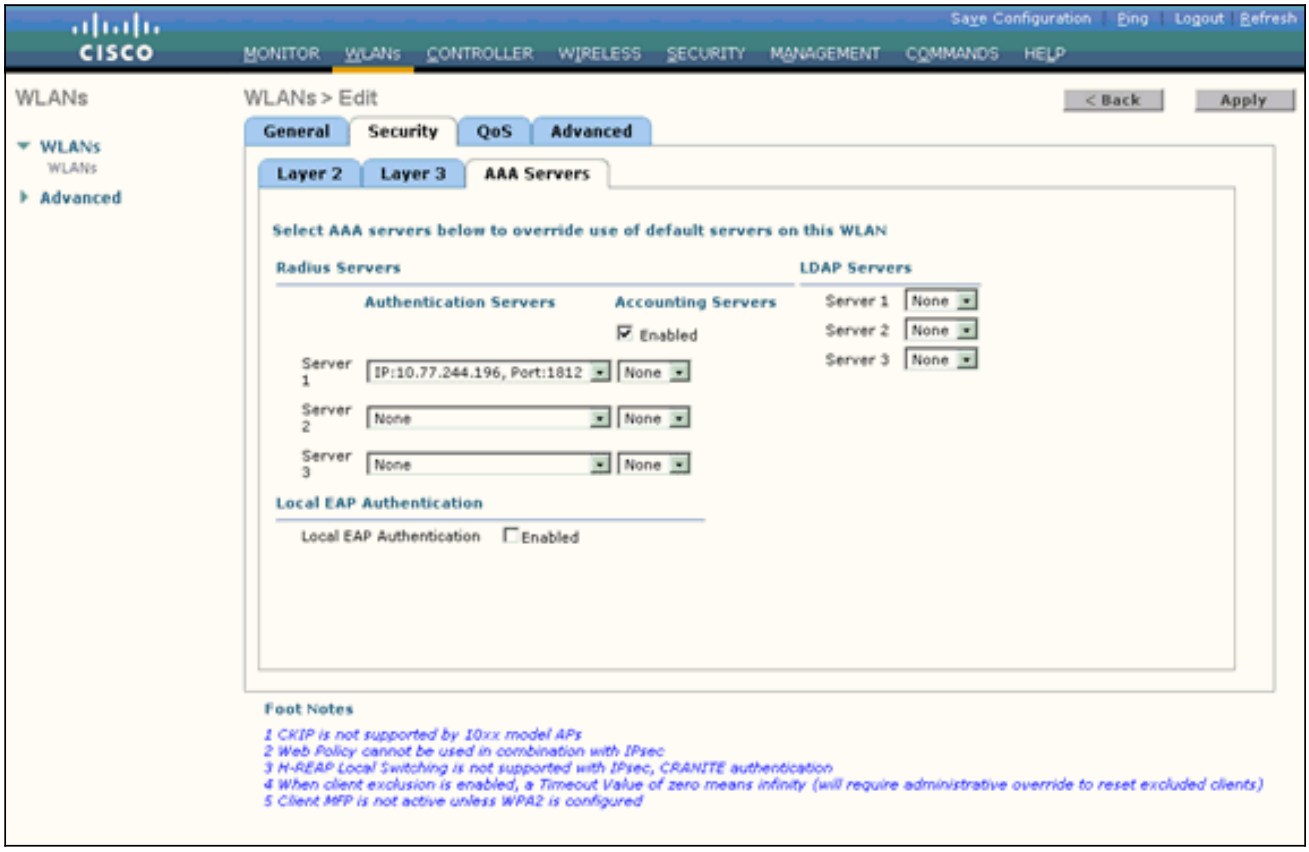
8. 페이지를 아래로 스크롤하여 **WPA+WPA2 매개변수를 수정합니다**.이 예에서는 WPA2 정책 및 AES 암호화를 선택합니다

.



9. Auth Key Mgmt(인증 키 관리)에서 **802.1x를** 선택합니다.그러면 WLAN에 802.1x/EAP 인증 및 AES 암호화를 사용하여 WPA2를 사용할 수 있습니다.
10. **AAA Servers(AAA 서버) 탭**을 클릭합니다. Authentication Servers(인증 서버)에서 적절한 서버 IP 주소를 선택합니다.이 예에서는 10.77.244.196이 RADIUS 서버로 사용됩니다

.



11. Apply를 **클릭합니다.참고:** 이 설정은 EAP 인증을 위해 컨트롤러에서 구성해야 하는 유일한 EAP 설정입니다. EAP-FAST에 특정한 다른 모든 컨피그레이션은 RADIUS 서버 및 인증해야 하는 클라이언트에서 수행해야 합니다.

WPA2 엔터프라이즈 모드 인증(EAP-FAST)을 위한 RADIUS 서버 구성

이 예에서는 Cisco Secure ACS가 외부 RADIUS 서버로 사용됩니다. EAP-FAST 인증을 위해 RADIUS 서버를 구성하려면 다음 단계를 수행합니다.

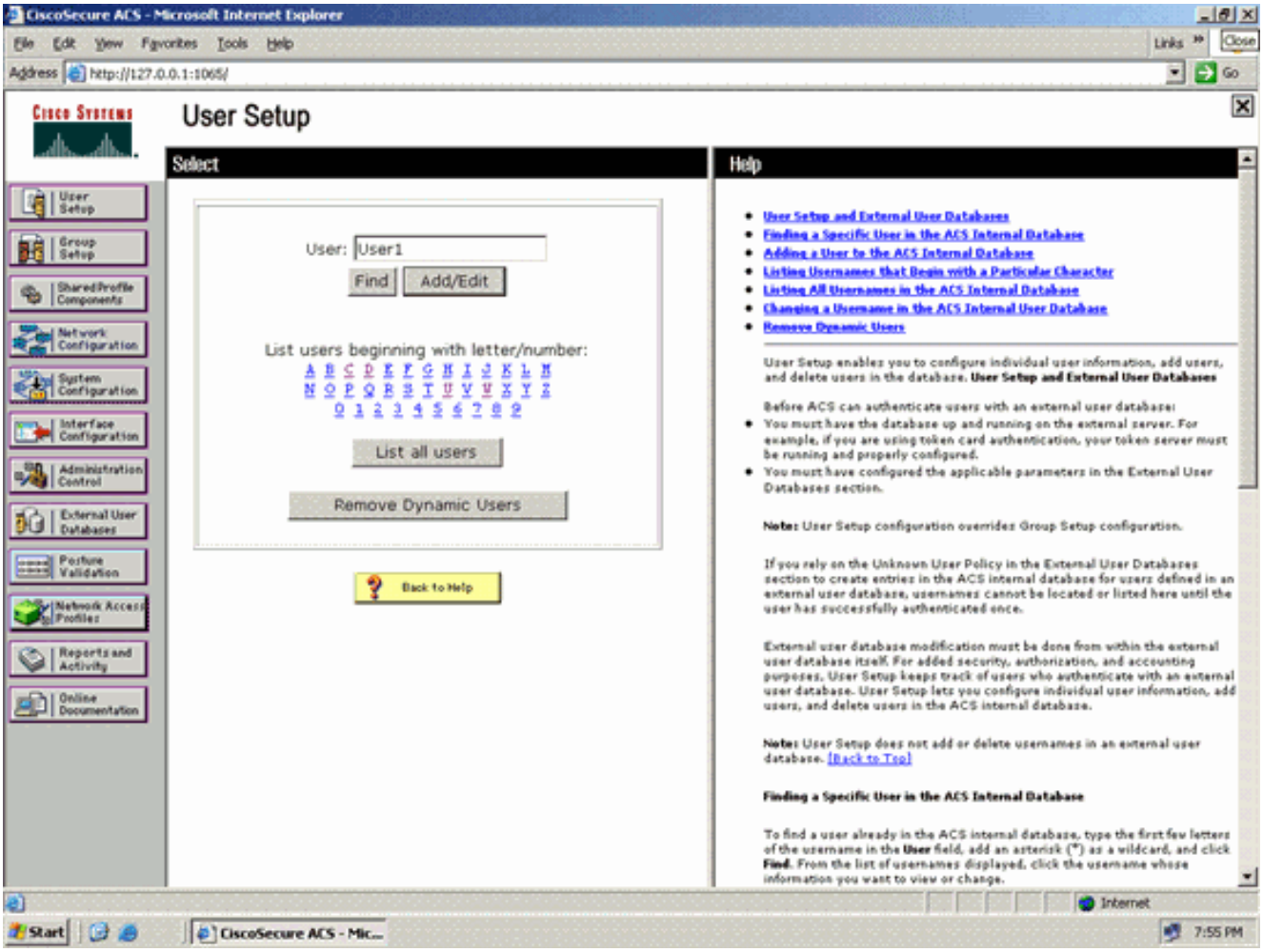
1. 클라이언트를 인증할 사용자 데이터베이스 생성
2. WLC를 RADIUS 서버에 AAA 클라이언트로 추가
3. 익명 대역 내 PAC 프로비저닝을 사용하여 RADIUS 서버에 EAP-FAST 인증 구성**참고:** EAP-FAST는 익명 대역 내 PAC 프로비저닝 또는 인증된 대역 내 PAC 프로비저닝으로 구성할 수 있습니다. 이 예에서는 익명 대역 내 PAC 프로비저닝을 사용합니다. 익명 대역 내 PAC 프로비저닝 및 인증된 대역 내 프로비저닝을 사용하여 EAP FAST를 구성하는 방법에 대한 자세한 내용 및 예는 무선 LAN 컨트롤러 및 외부 RADIUS 서버 컨피그레이션의 EAP-FAST 인증 예를 참조하십시오.

EAP-FAST 클라이언트를 인증하기 위한 사용자 데이터베이스 생성

ACS에서 EAP-FAST 클라이언트에 대한 사용자 데이터베이스를 생성하려면 다음 단계를 완료합니다. 이 예에서는 EAP-FAST 클라이언트의 사용자 이름 및 비밀번호를 각각 User1 및 User1로 구성합니다.

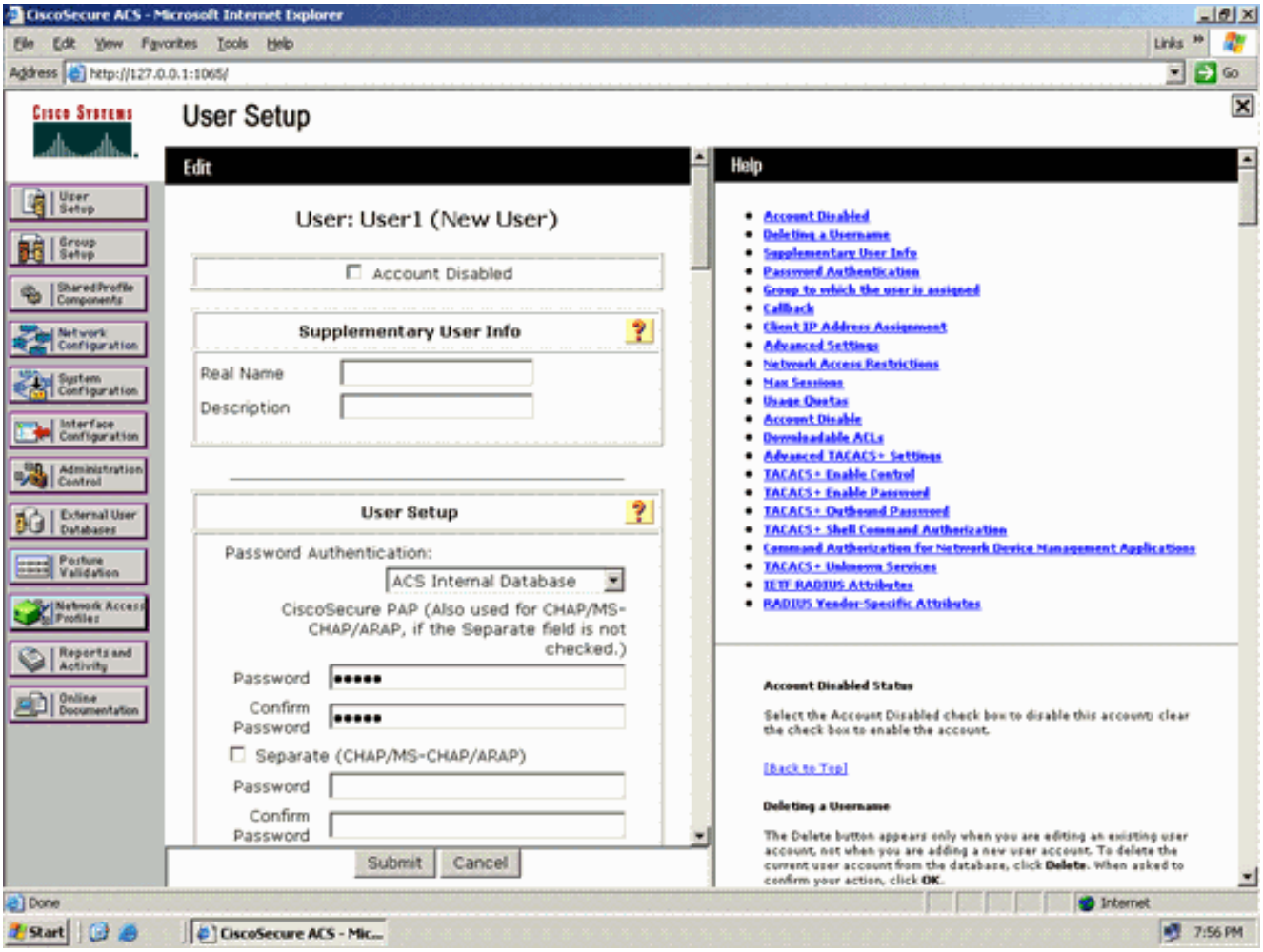
1. 탐색 모음의 ACS GUI에서 **User** Setup(**사용자 설정**)을 **선택합니다**. 새 사용자 무선을 만든 다음 **Add/Edit**를 클릭하여 이 사용자의 Edit 페이지로 이동합니다

.



2. 이 예에 표시된 대로 User Setup Edit(사용자 설정 수정) 페이지에서 Real Name(실제 이름) 및 Description(설명)과 Password(비밀번호) 설정을 구성합니다.이 문서에서는 비밀번호 **인증에 ACS 내부** 데이터베이스를 사용합니다

.



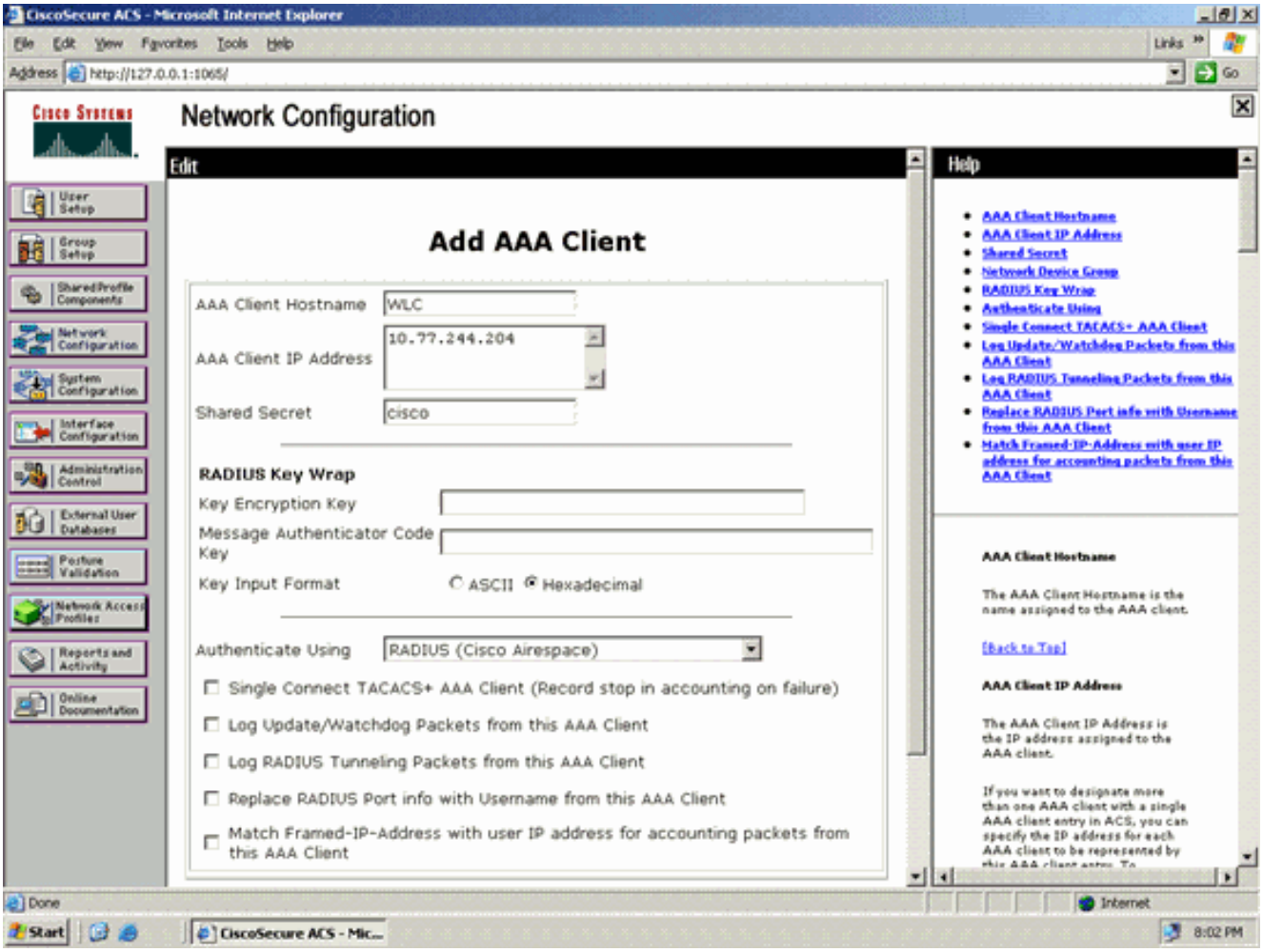
3. Password **Authentication(비밀번호** 인증) 드롭다운 상자에서 ACS Internal Database(ACS 내부 데이터베이스)를 선택합니다.
4. 다른 모든 필수 매개변수를 구성하고 Submit(제출)을 **클릭합니다**.

WLC를 RADIUS 서버에 AAA 클라이언트로 추가

컨트롤러를 ACS 서버에서 AAA 클라이언트로 정의하려면 다음 단계를 완료하십시오.

1. ACS GUI에서 **Network** Configuration(네트워크 컨피그레이션)을 클릭합니다. Network Configuration(네트워크 컨피그레이션) 페이지의 Add AAA client(AAA 클라이언트 추가) 섹션에서 Add **Entry(항목 추가)**를 클릭하여 RADIUS 서버에 AAA 클라이언트로 WLC를 추가합니다.
2. AAA Client(AAA 클라이언트) 페이지에서 WLC 이름, IP 주소, 공유 암호 및 인증 방법(RADIUS/Cisco Airespace)을 정의합니다. 다른 비 ACS 인증 서버에 대해서는 제조업체의 설명서를 참조하십시오

.



참고: WLC와 ACS 서버에서 구성하는 공유 비밀 키가 일치해야 합니다. 공유 암호는 대/소문자를 구분합니다.

3. Submit**+Apply를 클릭합니다**.

익명 대역 내 PAC 프로비저닝을 사용하여 RADIUS 서버에 EAP-FAST 인증 구성

익명 대역 내 프로비저닝

이는 ACS가 클라이언트에 새 PAC를 제공하기 위해 최종 사용자 클라이언트와의 보안 연결을 설정하는 두 가지 인밴드 프로비저닝 방법 중 하나입니다. 이 옵션은 최종 사용자 클라이언트와 ACS 간의 익명 TLS 핸드셰이크를 허용합니다.

이 방법은 피어가 ACS 서버를 인증하기 전에 ADHP(Authenticated Diffie-HellmanKey Agreement Protocol) 터널 내에서 작동합니다.

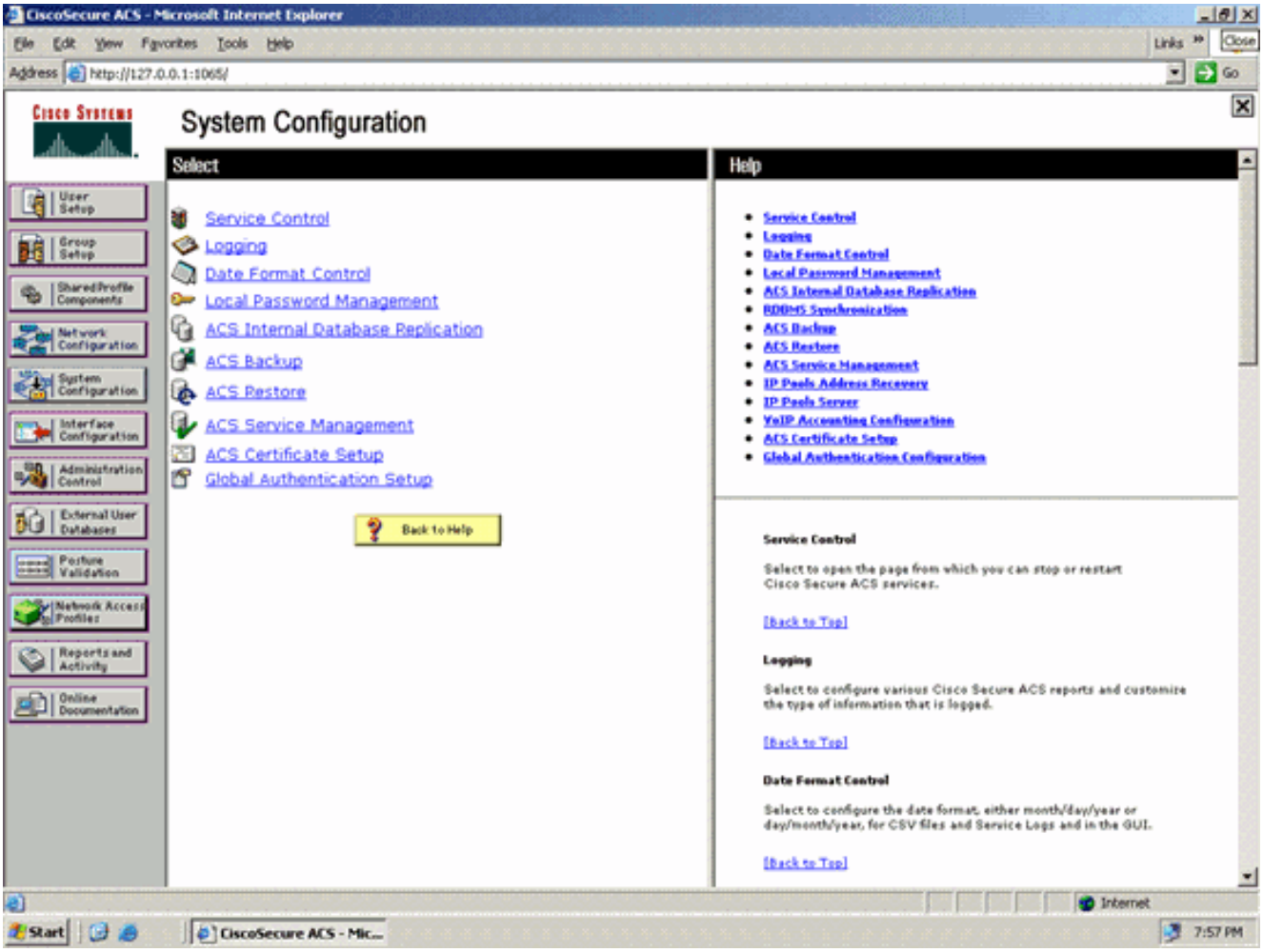
그런 다음 ACS는 사용자의 EAP-MS-CHAPv2 인증을 요구합니다. 사용자 인증에 성공하면 ACS는 최종 사용자 클라이언트와 Diffie-Hellman 터널을 설정합니다. ACS는 사용자에 대한 PAC를 생성하고 이 ACS에 대한 정보와 함께 이 터널의 최종 사용자 클라이언트로 전송합니다. 이 프로비저닝 방법은 0단계에서 인증 방법으로 EAP-MSCHAPv2를 사용하고 2단계에서 EAP-GTC를 사용합니다.

인증되지 않은 서버가 프로비저닝되므로 일반 텍스트 비밀번호를 사용할 수 없습니다. 따라서 MS-CHAP 자격 증명만 터널 내에서 사용할 수 있습니다. MS-CHAPv2는 피어의 ID를 증명하고 추가 인증 세션에 대한 PAC를 수신하는 데 사용됩니다(EAP-MS-CHAP는 내부 방법으로만 사용됨).

익명 대역 내 프로비저닝을 위해 RADIUS 서버에서 EAP-FAST 인증을 구성하려면 다음 단계를 완료하십시오.

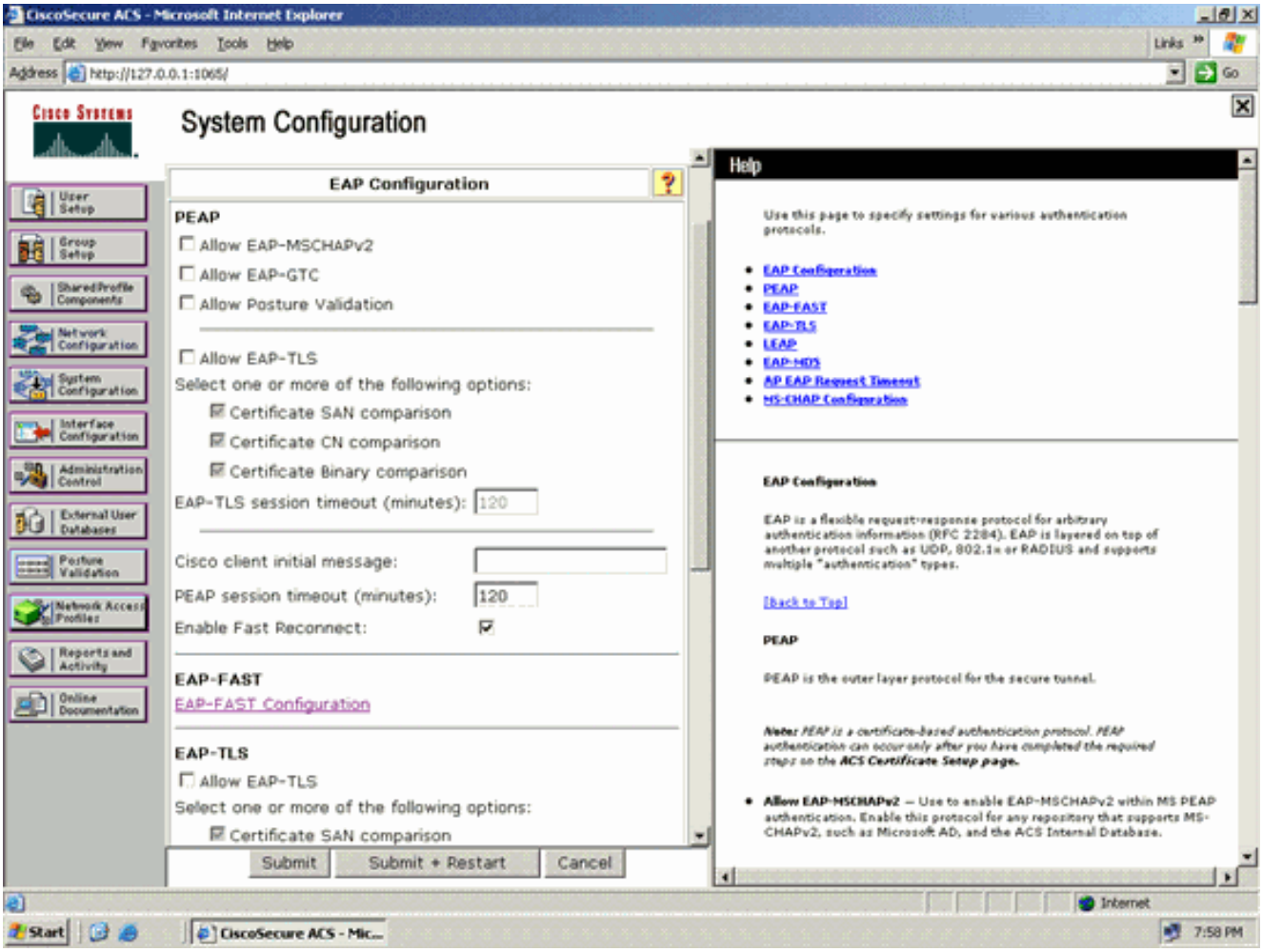
1. RADIUS 서버 GUI에서 **System** Configuration(**시스템 컨피그레이션**)을 클릭합니다. System Configuration(시스템 컨피그레이션) 페이지에서 **Global Authentication Setup(전역 인증 설정)**을 **선택합니다**

.



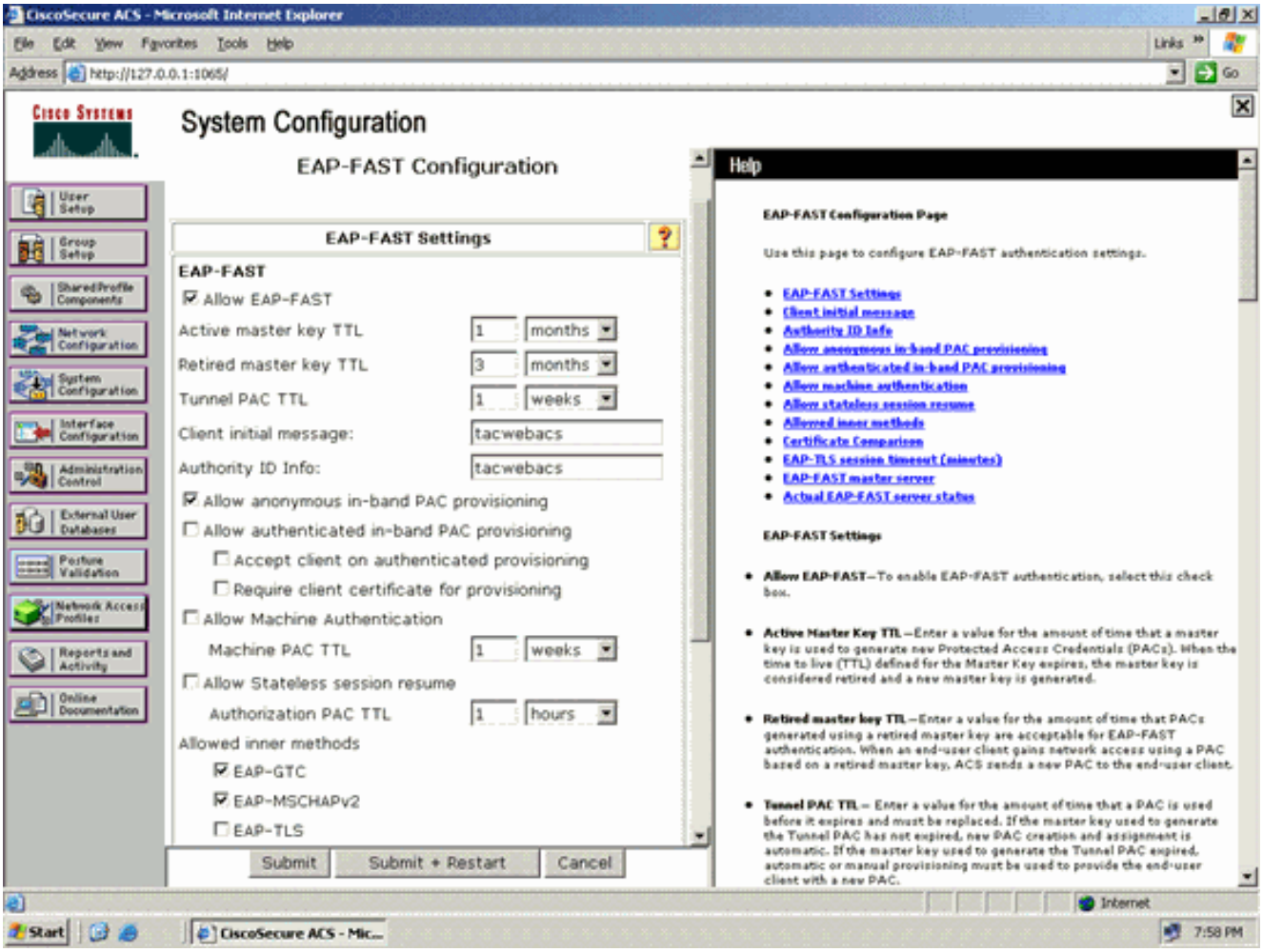
2. EAP-FAST 설정 페이지로 이동하려면 **Global** Authentication(전역 인증) 설정 페이지에서 EAP-FAST Configuration(EAP-FAST 구성)을 클릭합니다

.



3. RADIUS 서버에서 EAP-FAST를 활성화 하려면 EAP-**FAST** 설정 페이지에서 EAP-FAST를 허용 확인 란을 선택 합니다

.



4. 활성/폐기된 마스터 키 TTL(Time-to-Live) 값을 원하는 대로 구성하거나 이 예에 표시된 대로 기본값으로 설정합니다.활성 및 폐기된 마스터 키에 대한 자세한 내용은 마스터 키를 참조하십시오. 또한 자세한 내용은 마스터 키 및 PAC TTL을 참조하십시오.Authority ID Info(권한 ID 정보) 필드는 이 ACS 서버의 텍스트 ID를 나타냅니다. 최종 사용자는 이 ACS 서버를 사용하여 인증할 ACS 서버를 결정할 수 있습니다. 이 필드는 반드시 입력해야 합니다.Client initial display message(클라이언트 초기 표시 메시지) 필드는 EAP-FAST 클라이언트로 인증하는 사용자에게 보낼 메시지를 지정합니다. 최대 길이는 40자입니다. 최종 사용자 클라이언트가 디스플레이를 지원하는 경우에만 사용자에게 초기 메시지가 표시됩니다.
5. ACS가 익명 대역 내 PAC 프로비저닝을 수행하도록 하려면 Allow anonymous **대역 내 PAC provisioning(익명 대역 내 PAC 프로비저닝 허용) 확인란**을 선택합니다.
6. **Allowed inner methods(허용된 내부** 방법) - 이 옵션은 EAP-FAST TLS 터널 내에서 어떤 내부 EAP 방법을 실행할 수 있는지를 결정합니다. 익명 대역 내 프로비저닝의 경우 이전 버전과의 호환성을 위해 EAP-GTC 및 EAP-MS-CHAP를 활성화해야 합니다. Allow anonymous in-band PAC provisioning(익명 대역 내 PAC 프로비저닝 허용)을 선택하는 경우 EAP-MS-CHAP(0단계) 및 EAP-GTC(2단계)를 선택해야 합니다.

WPA2 엔터프라이즈 작동 모드에 대한 무선 클라이언트 구성

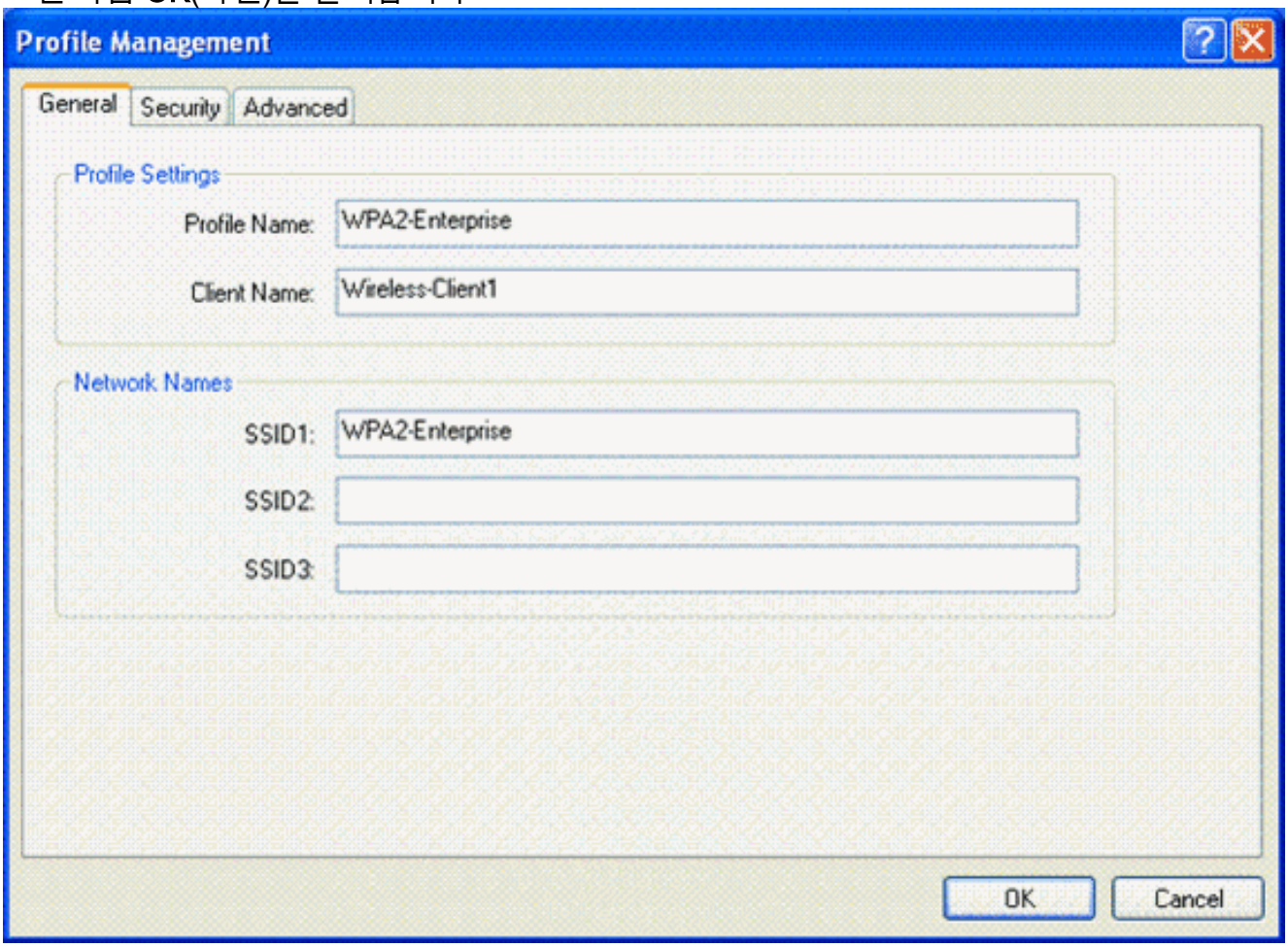
다음 단계는 WPA2 엔터프라이즈 작동 모드에 대한 무선 클라이언트를 구성하는 것입니다.

WPA2 엔터프라이즈 모드에 대한 무선 클라이언트를 구성하려면 다음 단계를 완료하십시오.

1. Aironet Desktop Utility 창에서 WPA2-Enterprise WLAN 사용자에 대한 프로파일을 생성하려면 **Profile Management(프로파일 관리) > New(새로 만들기)**를 클릭합니다.앞에서 언급한 대로 이 문서에서는 WLAN/SSID 이름을 무선 **클라이언트에** 대한 **WPA2-**Enterprise로 사용합니

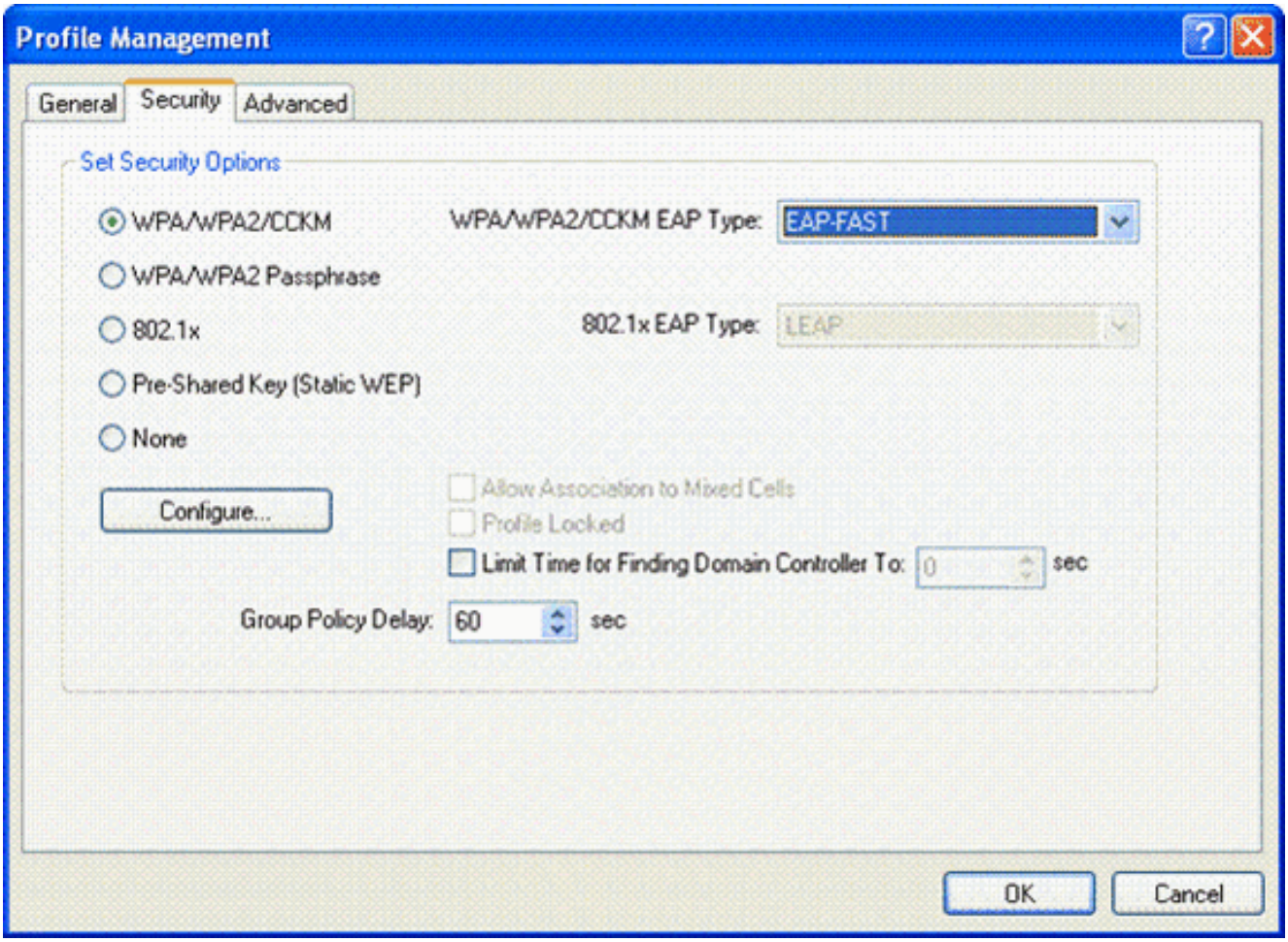
다.

2. Profile Management(프로파일 관리) 창에서 **General(일반)** 탭을 클릭하고 이 예에 표시된 대로 Profile Name(프로파일 이름), Client Name(클라이언트 이름) 및 SSID 이름을 구성합니다. 그런 다음 **OK**(확인)를 클릭합니다



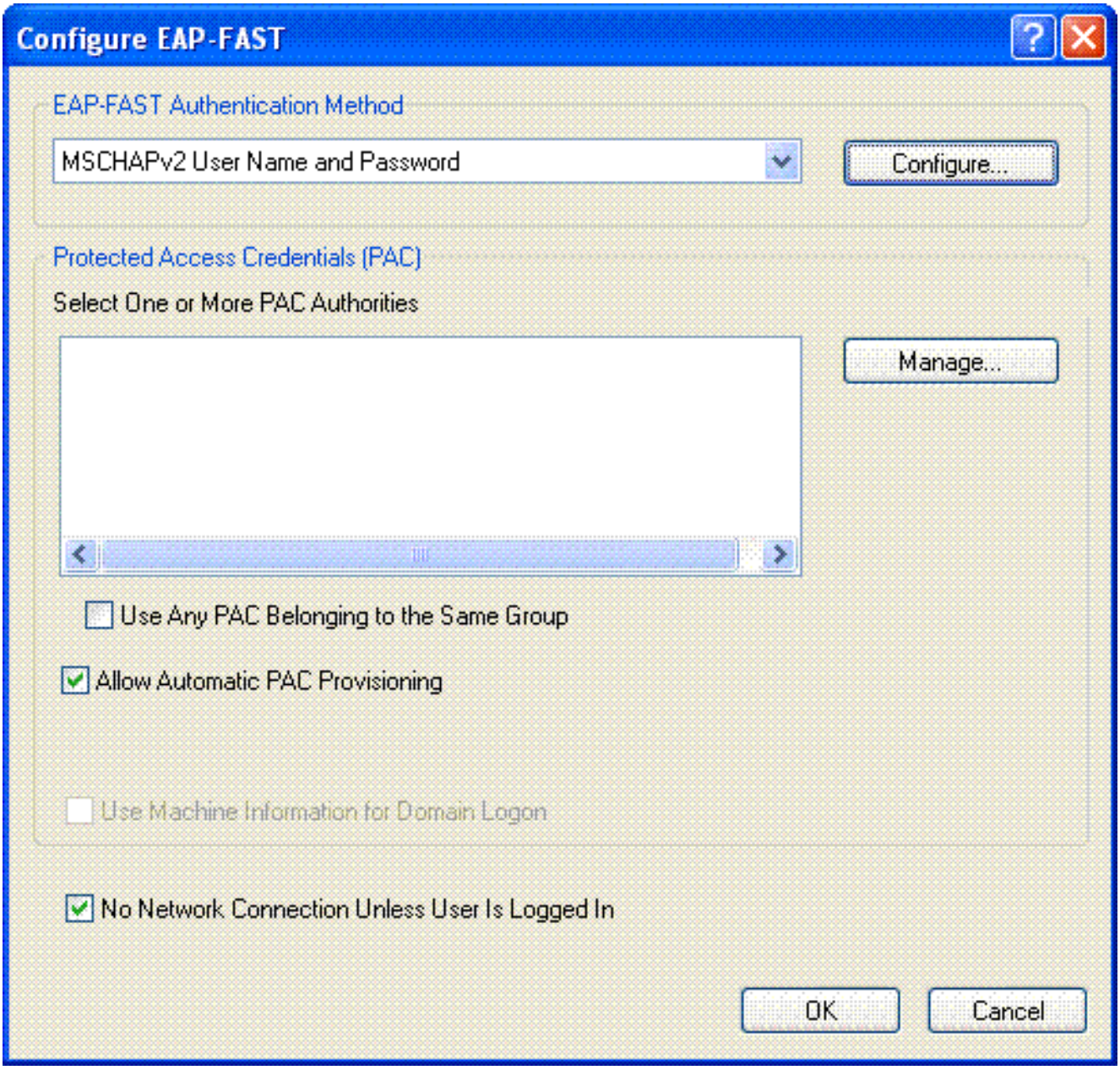
3. **Security(보안) 탭**을 클릭하고 **WPA/WPA2/CCKM**을 선택하여 WPA2 작동 모드를 활성화합니다. WPA/WPA2/CCKM EAP Type(WPA/WPA2/CCKM EAP 유형)에서 EAP-**FAST**를 선택합니다. EAP-**FAST** 설정을 구성하려면 Configure(구성)를 클릭합니다

.

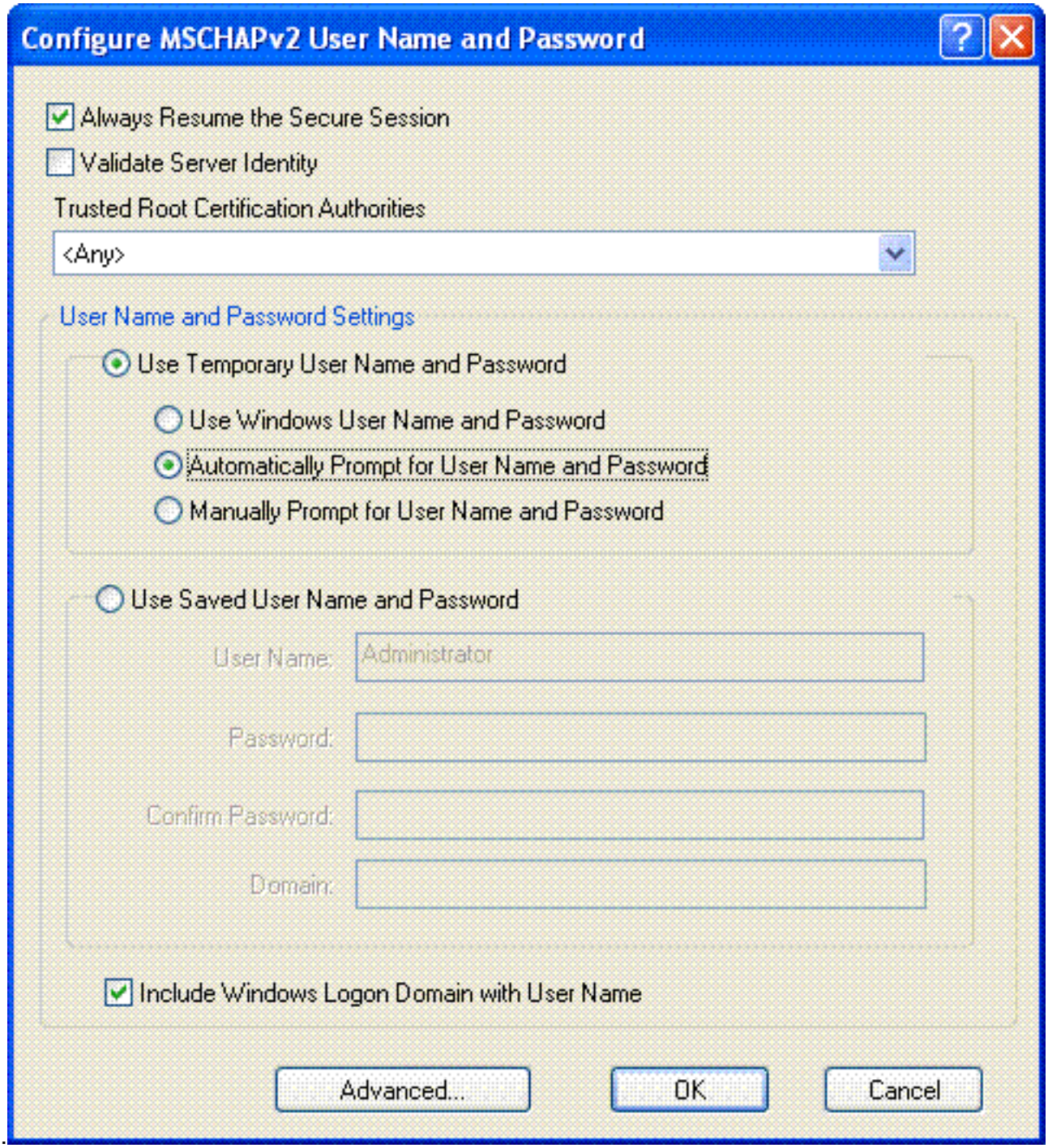


4. Configure EAP-FAST(EAP-FAST 구성) 창에서 Allow **Automatic PAC Provisioning(자동 PAC 프로비저닝 허용)** 확인란을 선택합니다. 익명 PAC 프로비저닝을 구성하려는 경우 EAP-MS-CHAP는 0단계에서 유일한 내부 방법으로 사용됩니다

.



5. EAP-FAST Authentication Method(EAP-FAST 인증 방법) 드롭다운 상자에서 인증 방법으로 MSCHAPv2 User Name and Password(MSCHAPv2 사용자 이름 및 비밀번호)를 선택합니다. Configure를 **클릭합니다**.
6. Configure MSCHAPv2 User Name and Password(MSCHAPv2 사용자 이름 및 비밀번호 구성) 창에서 적절한 사용자 이름과 비밀번호 설정을 선택합니다.이 예에서는 Automatically **Prompt for User Name and Password를 선택합니다**



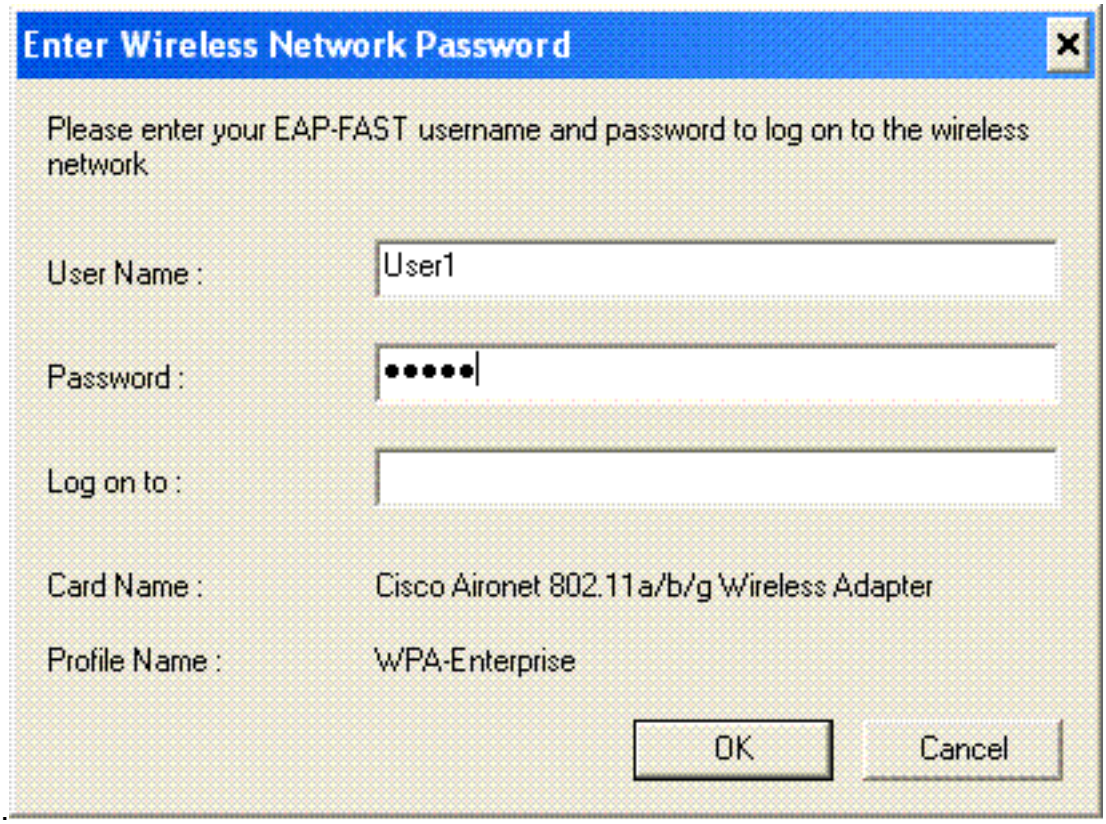
동일한 사용자 이름과 비밀번호를 ACS에 등록해야 합니다. 앞에서 설명한 것처럼 이 예에서는 사용자 이름과 비밀번호로 각각 User1 및 User1을 사용합니다. 또한 이는 익명의 대역 내 프로비저닝입니다. 따라서 클라이언트는 서버 인증서를 검증할 수 없습니다. Validate Server Identity(서버 ID 검증) 확인란이 선택되지 않았는지 확인해야 합니다.

7. **OK(확인)**를 클릭합니다.

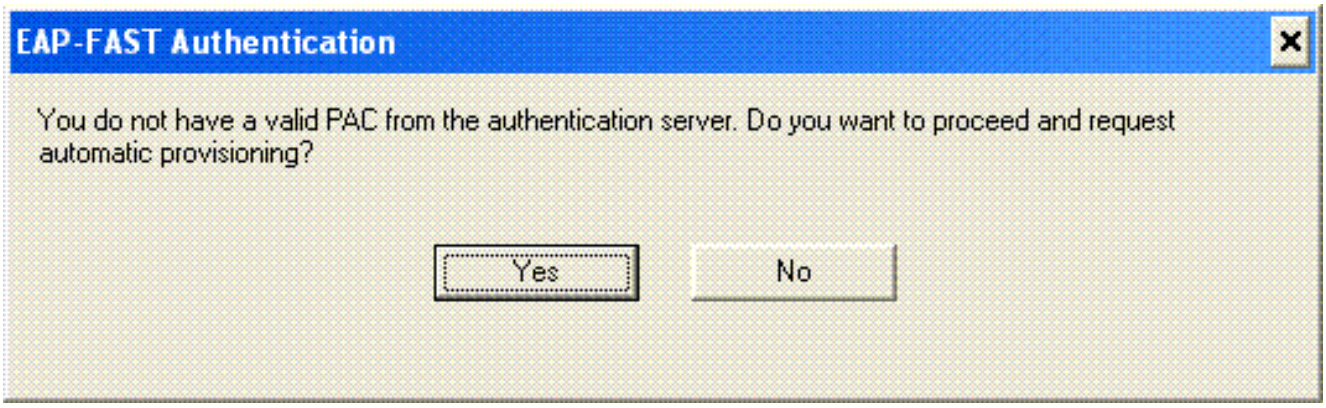
WPA2 엔터프라이즈 운영 모드 확인

WPA2 엔터프라이즈 모드 컨피그레이션이 제대로 작동하는지 확인하려면 다음 단계를 완료하십시오.

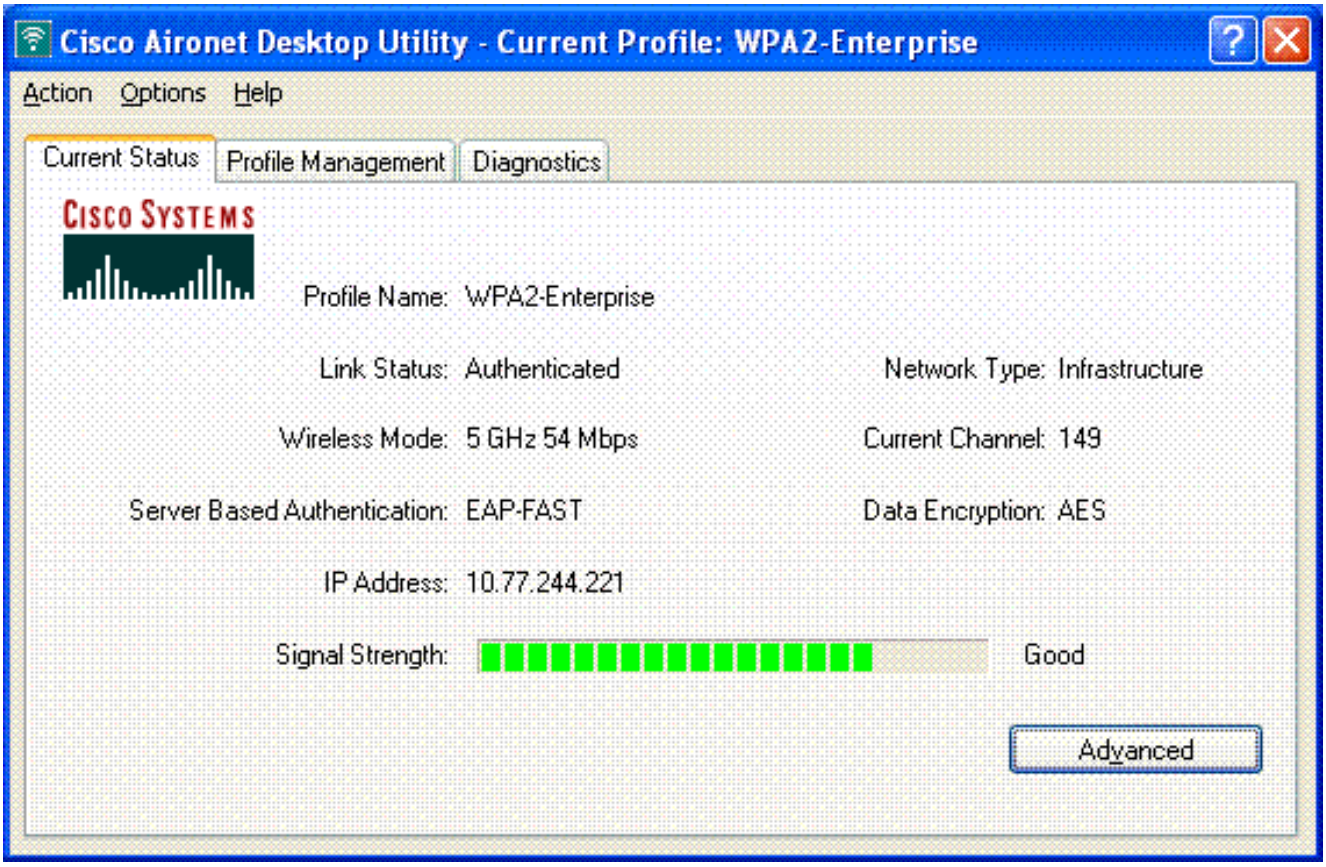
1. 무선 클라이언트 프로파일을 활성화하려면 Aironet Desktop Utility 창에서 프로파일 **WPA2-Enterprise**를 선택하고 **Activate**(활성화)를 클릭합니다.
2. 인증으로 MS-CHAP ver2를 활성화한 경우 클라이언트는 사용자 이름과 비밀번호를 묻는 메시지를 표시합니다



3. 사용자의 EAP-FAST 처리 중에 클라이언트에서 RADIUS 서버에서 PAC를 요청하라는 프롬프트가 표시됩니다. **Yes(예)**를 클릭하면 PAC 프로비저닝이 시작됩니다



4. 단계 0에서 PAC 프로비저닝이 성공하면 단계 1 및 2가 뒤따르고 성공적인 인증 절차가 이루어집니다.인증에 성공하면 무선 클라이언트가 WLAN WPA2-Enterprise에 연결됩니다. 스크린샷은 다음과 같습니다



RADIUS 서버가 무선 클라이언트로부터 인증 요청을 수신하고 검증하는지 여부도 확인할 수 있습니다. 이를 위해 ACS 서버에서 Passed Authentications and Failed Attempts(통과한 인증 및 실패 시도) 보고서를 확인합니다. 이러한 보고서는 ACS 서버의 Reports and Activities(보고서 및 활동)에서 사용할 수 있습니다.

WPA2 개인 모드에 대한 장치 구성

WPA2-개인 작동 모드에 대한 장치를 구성하려면 다음 단계를 수행하십시오.

1. WPA2 개인 모드 인증을 위한 WLAN 구성
2. WPA2 개인 모드에 대한 무선 클라이언트 구성

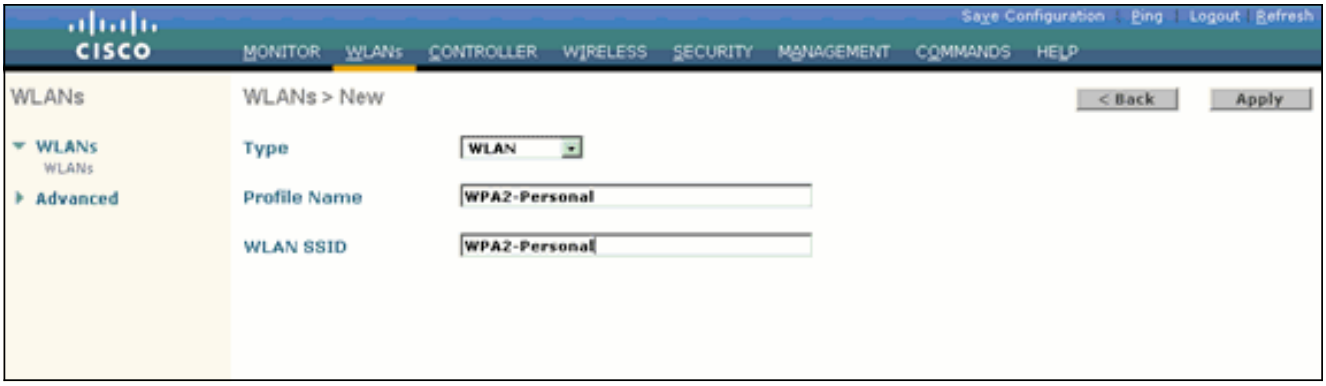
WPA2 개인 작동 모드에 맞게 WLAN 구성

클라이언트가 무선 네트워크에 연결하는 데 사용할 WLAN을 구성해야 합니다. WPA2 개인 모드의 WLAN SSID는 WPA2-Personal입니다. 이 예에서는 이 WLAN을 관리 인터페이스에 할당합니다.

WLAN 및 관련 매개변수를 구성하려면 다음 단계를 완료합니다.

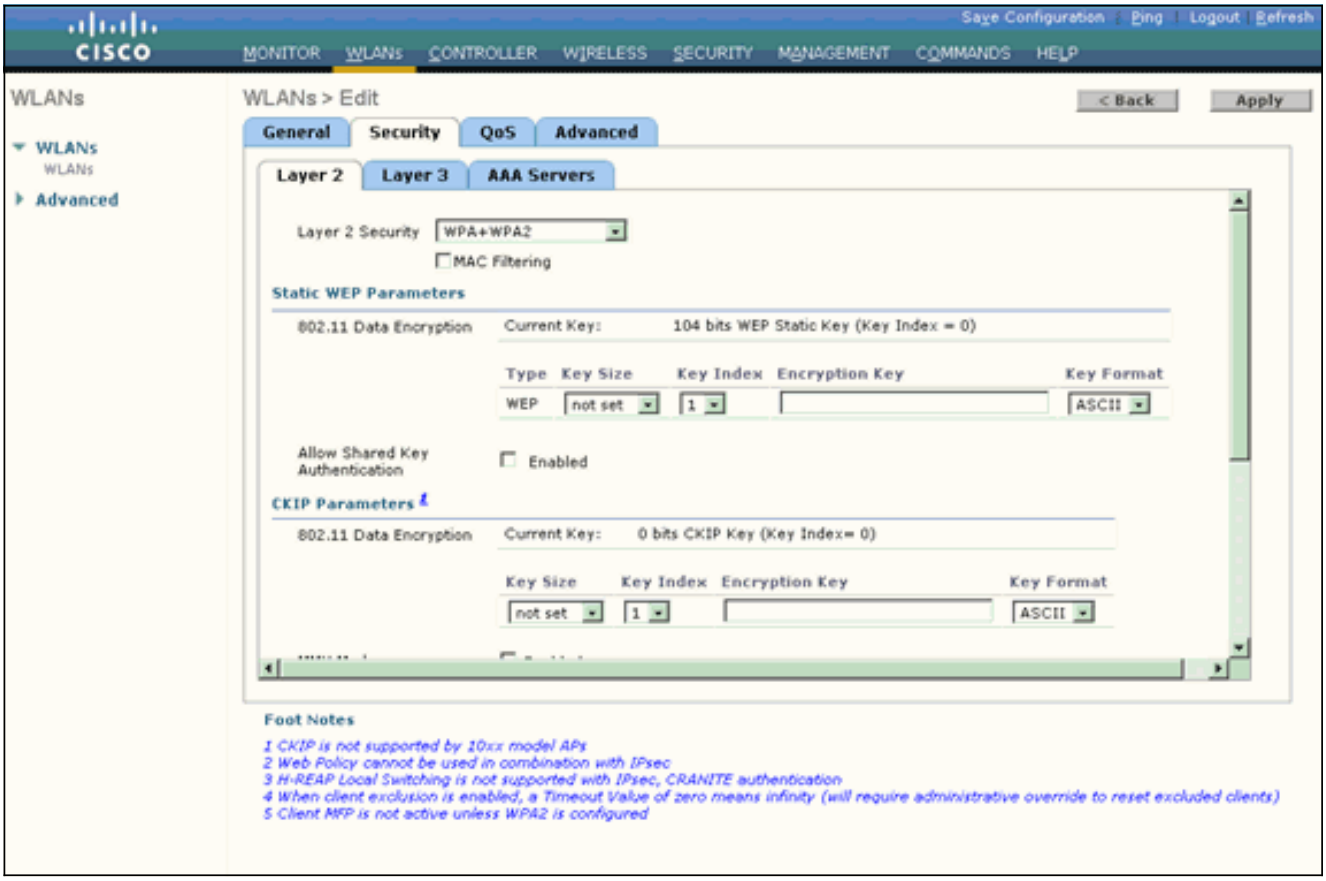
1. WLANs **페이지**를 표시하려면 컨트롤러의 GUI에서 WLANs를 클릭합니다.이 페이지에는 컨트롤러에 있는 WLAN이 나열됩니다.
2. 새 **WLAN**을 생성하려면 New(새로 만들기)를 클릭합니다.
3. WLANs(WLAN) > New(새로 만들기) 페이지에서 WLAN SSID 이름, 프로파일 이름 및 WLAN ID를 입력합니다. 그런 다음 Apply를 **클릭합니다**.이 예에서는 **WPA2-Personal**을 SSID로 사용합니다

.



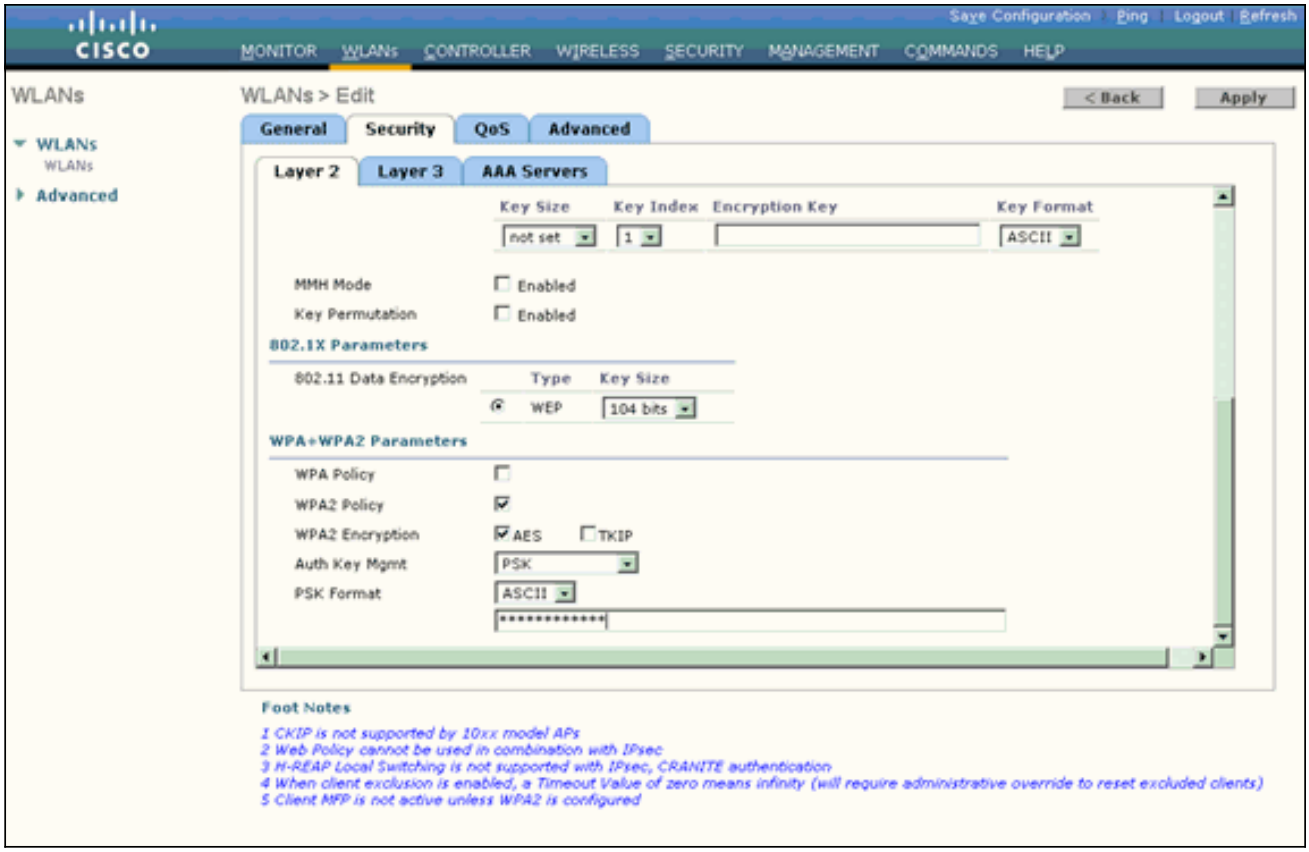
4. 새 WLAN을 생성하면 새 WLAN에 대한 **WLAN > Edit** 페이지가 나타납니다. 이 페이지에서 이 WLAN에 대한 다양한 매개변수를 정의할 수 있습니다. 여기에는 일반 정책, 보안 정책, QOS 정책 및 고급 매개변수가 포함됩니다.
5. General Policies(일반 정책)에서 **Status(상태)** 확인란을 선택하여 WLAN을 활성화합니다.
6. AP가 비콘 프레임에서 SSID를 브로드캐스트하도록 하려면 Broadcast SSID(브로드캐스트 SSID) **확인란**을 선택합니다.
7. **보안** 탭을 클릭합니다. Layer Security(레이어 보안) 아래에서 **WPA+WPA2를** 선택합니다.이렇게 하면 WLAN에 대한 WPA 인증이 활성화됩니다

.



8. 페이지를 아래로 스크롤하여 **WPA+WPA2 매개변수를 수정합니다**.이 예에서는 WPA2 정책 및 AES 암호화를 선택합니다.
9. Auth Key Mgmt(인증 키 관리)에서 WPA2-PSK를 활성화하려면 PSK를 선택합니다.
10. 표시된 대로 해당 필드에 사전 공유 키를 입력합니다

.



참고: WLC에 사용된 사전 공유 키는 무선 클라이언트에 구성된 키와 일치해야 합니다.

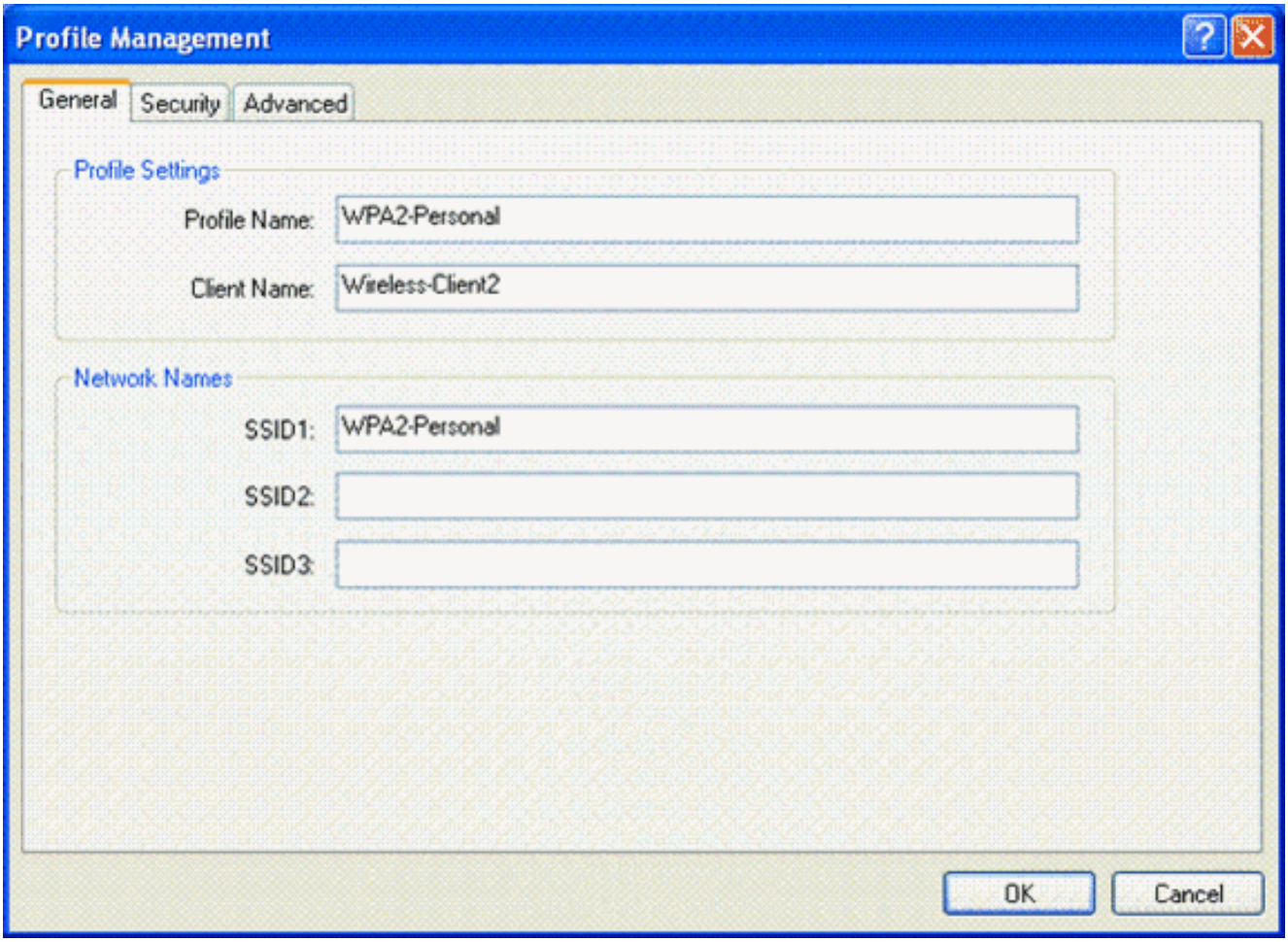
11. Apply를 **클릭합니다**.

WPA2 개인 모드에 대한 무선 클라이언트 구성

다음 단계는 WPA2-개인 작동 모드에 대한 무선 클라이언트를 구성하는 것입니다.

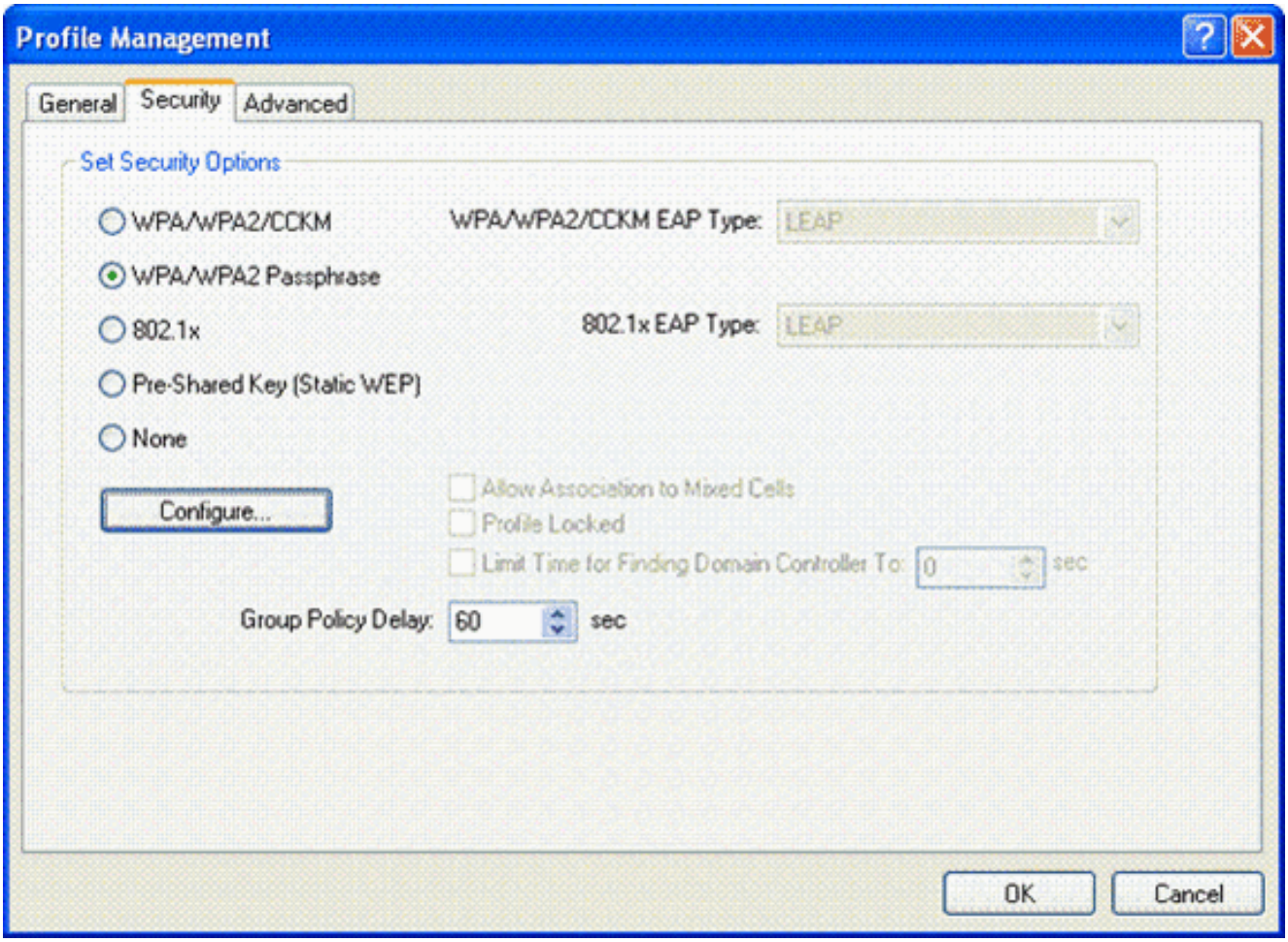
WPA2-개인 모드에 대한 무선 클라이언트를 구성하려면 다음 단계를 완료하십시오.

1. WPA2-PSK WLAN 사용자에 대한 프로필을 생성하려면 Aironet Desktop Utility 창에서 **Profile Management(프로필 관리) > New(새로 만들기)**를 클릭합니다.
2. Profile Management(프로파일 관리) 창에서 **General(일반)** 탭을 클릭하고 이 예에 표시된 대로 Profile Name(프로파일 이름), Client Name(클라이언트 이름) 및 SSID 이름을 구성합니다. 그런 다음 확인을 **클릭합니다**
.

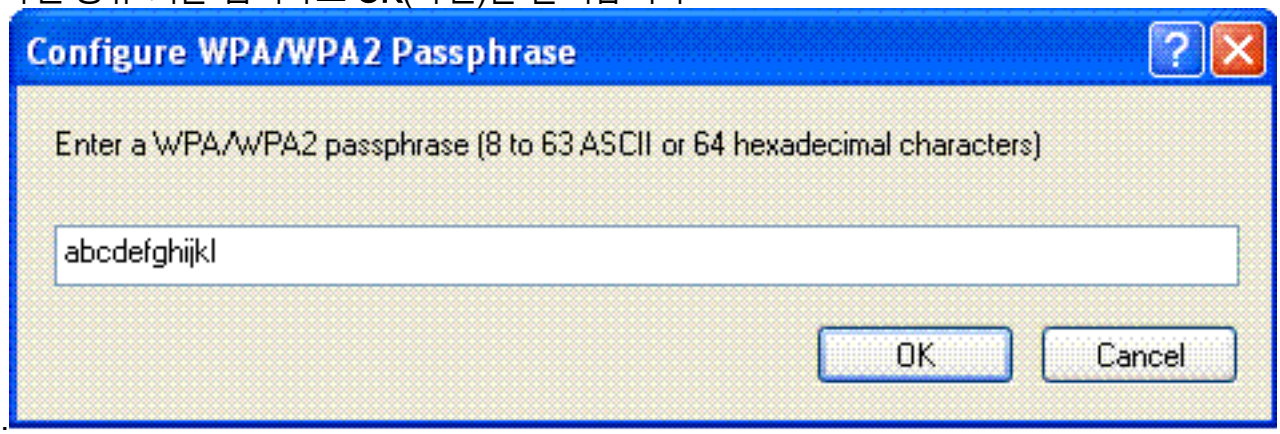


3. **보안** 탭을 클릭하고 **WPA/WPA2 암호**를 선택하여 WPA2-PSK 작동 모드를 활성화합니다. WPA-**PSK** 사전 공유 키를 구성하려면 Configure(구성)를 클릭합니다

.



4. 사전 공유 키를 입력하고 **OK**(확인)를 클릭합니다



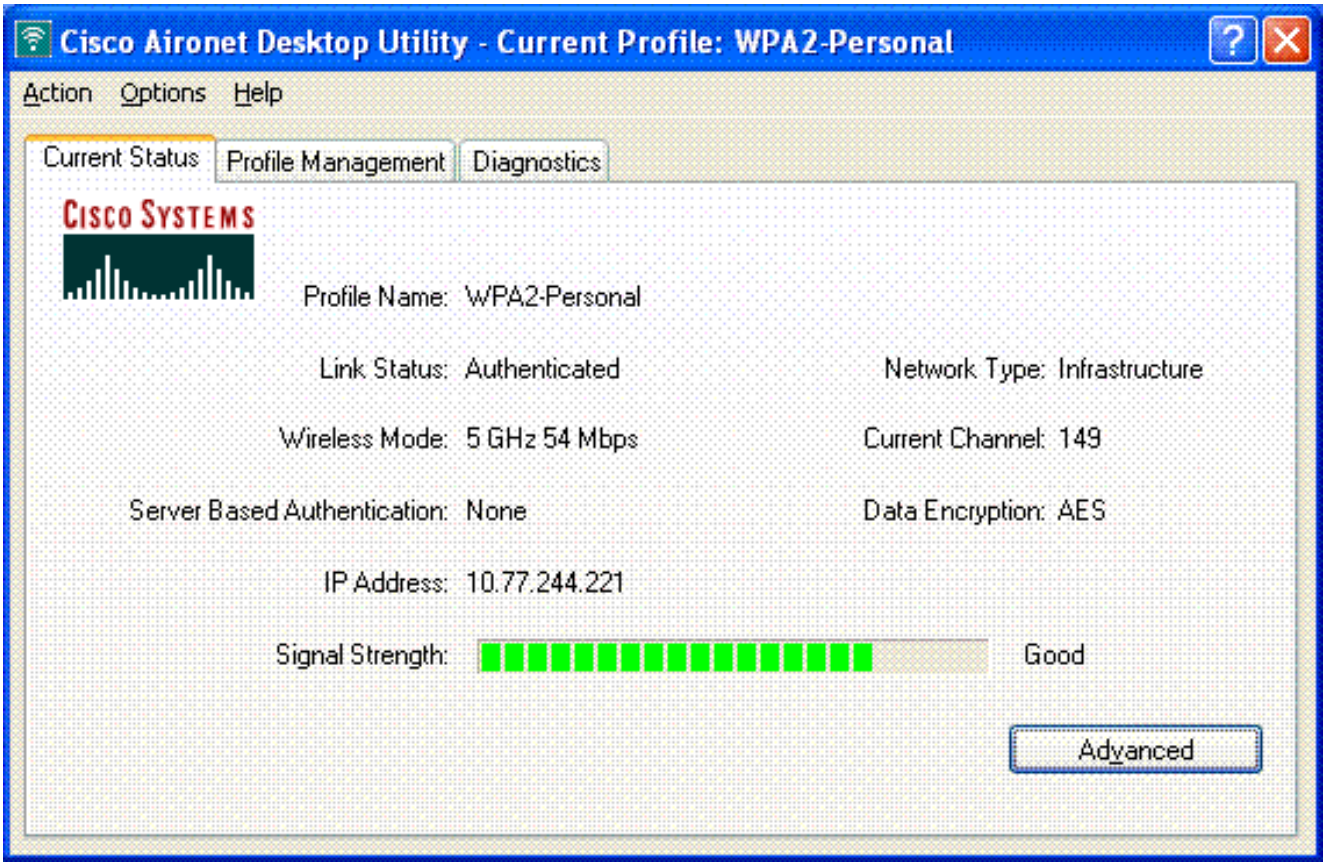
.

WPA2-개인 작동 모드 확인

WPA2-엔터프라이즈 모드 컨피그레이션이 제대로 작동하는지 확인하려면 다음 단계를 완료하십시오.

1. 무선 클라이언트 프로파일을 활성화하려면 Aironet Desktop Utility 창에서 프로파일 **WPA2-Personal**을 선택하고 **Activate**(활성화)를 클릭합니다.
2. 프로파일이 활성화되면 무선 클라이언트는 인증에 성공하면 WLAN에 연결됩니다.스크린샷은 다음과 같습니다

.



문제 해결

이 섹션에서는 설정 문제 해결에 사용할 수 있는 정보를 제공합니다.

이러한 **debug** 명령은 컨피그레이션 트러블슈팅에 유용합니다.

참고: debug 명령을 사용하기 전에 Debug 명령에 대한 중요 정보를 참조하십시오.

- **debug dot1x events enable** - 모든 dot1x 이벤트의 디버그를 활성화합니다. 다음은 성공적인 인증을 기반으로 한 디버그 출력의 예입니다.**참고:** 공간 제한으로 인해 이 출력의 일부 행이 두 번째 행으로 이동되었습니다.

```
(Cisco Controller)>debug dot1x events enable
Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Sending EAP -Request/Identity
to mobile 00:40:96:af:3e:93 (EAP Id 1)
Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Received EAPOL START from
mobile 00:40:96:af:3e:93
Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity
to mobile 00:40:96:af:3e:93 (EAP Id 2)
Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Received EAP Response packet with
mismatching id (currentid=2, eapid=1) from mobile 00:40:96:af:3e:93
Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Received Identity Response
(count=2) from mobile 00:40:96:af:3e:93
Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Processing Access-Challenge
for mobile 00:40:96:af:3e:93
.....
.....
.....
.....

Wed Feb 20 14:20:00 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 19, EAP Type 43)
Wed Feb 20 14:20:00 2007: 00:40:96:af:3e:93 Processing Access-Challenge
```

for mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:00 2007: 00:40:96:af:3e:93 **Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 20)**
Wed Feb 20 14:20:01 2007: 00:40:96:af:3e:93 **Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 20, EAP Type 43)**
Wed Feb 20 14:20:29 2007: Creating dot1x interface with key 00:0b:85:91:c3:c0 -0
Wed Feb 20 14:20:29 2007: Resetting the group key timer for 3689 seconds on AP 00:0b:85:91:c3:c0
Wed Feb 20 14:20:29 2007: Creating dot1x interface with key 00:0b:85:91:c3:c0 -1
Wed Feb 20 14:20:29 2007: Resetting the group key timer for 3696 seconds on AP 00:0b:85:91:c3:c0
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received EAPOL START from mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 22)
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received Identity Response (count=3) from mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 WARNING: updated EAP-Identifer 22 ===> 19 for STA 00:40:96:af:3e:93
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 19)
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 19, EAP Type 3)
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 20)
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 20, EAP Type 43)
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 21)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 21, EAP Type 43)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 22)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 22, EAP Type 43)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 23)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 23, EAP Type 43)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 24)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 24, EAP Type 43)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 25)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 25, EAP Type 43)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to

mobile 00:40:96:af:3e:93 (EAP Id 26)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 26, EAP Type 43)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to
mobile 00:40:96:af:3e:93 (EAP Id 27)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 27, EAP Type 43)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Reject for
mobile00:40:96:af:3e:93
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Failure to
mobile 00:4096:af:3e:93 (EAP Id 27)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Setting quiet timer for 5 seconds
for mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to
mobile 00:40:96:af:3e:93 (EAP Id 1)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to
mobile 00:40:96:af:3e:93 (EAP Id 1)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAPOL START from
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to
mobile 00:40:96:af:3e:93 (EAP Id 2)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received Identity Response (count=2)
from mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 WARNING: updated EAP-Identifer 2 ===>
20 for STA 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to
mobile 00:40:96:af:3e:93 (EAP Id 20)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 20, EAP Type 3)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to
mobile 00:40:96:af:3e:93 (EAP Id 21)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 21, EAP Type 43)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to
mobile 00:40:96:af:3e:93 (EAP Id 22)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 22, EAP Type 43)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 WARNING: updated EAP-Identifer 22 ===>
24 for STA 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to
mobile 00:40:96:af:3e:93 (EAP Id 24)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 24, EAP Type 43)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 **Processing Access-Challenge
for mobile 00:40:96:af:3e:93**
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 **Sending EAP Request from AAA
to mobile 00:40:96:af:3e:93 (EAP Id 25)**
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 **Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 25, EAP Type 43)**
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 **Processing Access-Accept for
mobile 00:40:96:af:3e:93**
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 **Creating a new PMK Cache Entry for
tation 00:40:96:af:3e:93 (RSN 0)**
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 **Sending EAP-Success to**

```
mobile 00:40:96:af:3e:93 (EAP Id 25)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending default RC4 key to
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending Key-Mapping RC4 key to
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received Auth Success while in
Authenticating state for mobile 00:40:96:af:3e:93
```

- **debug dot1x packet enable** - 802.1x 패킷 메시지의 디버그를 활성화합니다.
- **debug aaa events enable** - 모든 aaa 이벤트의 디버그 출력을 활성화합니다.

관련 정보

- WPA2 - Wi-Fi 보호 액세스 2
- 무선 LAN 컨트롤러 및 외부 RADIUS 서버 컨피그레이션을 통한 EAP-FAST 인증 예
- WLAN 컨트롤러(WLC)를 사용한 EAP 인증 컨피그레이션 예
- WPA 컨피그레이션 개요
- 무선 제품 지원
- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.