# WPA 2(Wi-Fi Protected Access 2) 구성 예

## 목차



## 소개

이 문서에서는 WLAN(무선 LAN)에서 WPA 2(Wi-Fi Protected Access 2)를 사용할 때의 장점을 설명합니다. 이 문서에서는 WLAN에서 WPA 2를 구현하는 방법에 대한 두 가지 구성 예를 제공합니다.첫 번째 예에서는 엔터프라이즈 모드에서 WPA 2를 구성하는 방법을 보여 주고, 두 번째 예에서는 개인 모드에서 WPA 2를 구성합니다.

**참고:** WPA는 EAP(Extensible Authentication Protocol)와 작동합니다.

## 사전 요구 사항

### 요구 사항

이 컨피그레이션을 시도하기 전에 이러한 주제에 대한 기본적인 지식을 가지고 있는지 확인합니다.

- WPA

- WLAN 보안 솔루션**참고:** Cisco WLAN 보안 솔루션에 대한 자세한 내용은 Cisco Aironet Wireless LAN 보안 개요를 참조하십시오.

## 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS® 소프트웨어 릴리스 12.3(2)JA를 실행하는 Cisco Aironet 1310G AP(Access Point)/Bridge
- 펌웨어 2.5를 실행하는 Aironet 802.11a/b/g CB21AG Client Adapter
- 펌웨어 2.5를 실행하는 ADU(Aironet Desktop Utility)

**참고:** Aironet CB21AG 및 PI21AG 클라이언트 어댑터 소프트웨어는 다른 Aironet 클라이언트 어댑터 소프트웨어와 호환되지 않습니다.CB21AG 및 PI21AG 카드와 함께 ADU를 사용해야 하며 다른 모든 Aironet 클라이언트 어댑터를 사용해야 합니다.CB21AG 카드 및 ADU를 설치하는 방법에 대한 자세한 내용은 클라이언트 어댑터 설치를 참조하십시오.

**참고:** 이 문서는 통합 안테나가 있는 AP/브리지를 사용합니다.외부 안테나가 필요한 AP/브리지를 사용하는 경우 안테나가 AP/브리지에 연결되어 있는지 확인합니다.그렇지 않으면 AP/브리지가 무선 네트워크에 연결할 수 없습니다.일부 AP/브리지 모델은 내장형 안테나를 사용하는 반면, 다른 모델에서는 일반적인 작동을 위해 외부 안테나가 필요합니다.내부 또는 외부 안테나와 함께 제공되는 AP/브리지 모델에 대한 자세한 내용은 해당 디바이스의 주문 가이드/제품 가이드를 참조하십시오.

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.

# 배경 정보

WPA는 기본 WLAN의 취약성을 해결하는 Wi-Fi Alliance의 표준 기반 보안 솔루션입니다.WPA는 WLAN 시스템에 대해 향상된 데이터 보호 및 액세스 제어를 제공합니다.WPA는 원래 IEEE 802.11 보안 구현에서 알려진 모든 WEP(Wired Equivalent Privacy) 취약성을 해결하며 기업 및 소규모 사무실, 홈 오피스(SOHO) 환경 모두에서 WLAN에 즉각적인 보안 솔루션을 제공합니다.

WPA 2는 차세대 Wi-Fi 보안입니다.WPA 2는 승인된 IEEE 802.11i 표준의 Wi-Fi Alliance 상호 운용 가능한 구현입니다.WPA 2는 CCMP(Cipher Block Chaining Message Authentication Code Protocol)를 사용하여 카운터 모드를 사용하는 NIST(National Institute of Standards and Technology) 권장 AES(Advanced Encryption Standard) 암호화 알고리즘을 구현합니다.AES 카운터 모드는 128비트 암호화 키를 사용하여 한 번에 128비트 데이터 블록을 암호화하는 블록 암호입니다.CCMP 알고리즘은 무선 프레임에 대한 데이터 원본 인증 및 데이터 무결성을 제공하는 MIC(Message Integrity Code)를 생성합니다.

**참고:** CCMP는 CBC-MAC이라고도 합니다.

AES는 TKIP(Temporal Key Integrity Protocol)보다 강력한 암호화를 제공하므로 WPA 2는 WPA보다 높은 수준의 보안을 제공합니다.TKIP는 WPA에서 사용하는 암호화 알고리즘입니다.WPA 2는 모든 연결에 새 세션 키를 만듭니다.네트워크의 각 클라이언트에 사용되는 암호화 키는 고유하며

해당 클라이언트에 한정됩니다.결국, 공기를 통해 전송되는 모든 패킷은 고유한 키로 암호화됩니다.키 재사용이 없으므로 새롭고 고유한 암호화 키를 사용하여 보안이 강화됩니다.WPA는 여전히 안전한 것으로 간주되며 TKIP가 손상되지 않았습니다.그러나 Cisco에서는 가능한 한 빨리 고객이 WPA 2로 전환할 것을 권장합니다.

WPA와 WPA 2는 모두 두 가지 작동 모드를 지원합니다.

- 엔터프라이즈 모드
- 개인 모드

이 문서에서는 WPA 2와 함께 이러한 두 모드를 구현하는 방법에 대해 설명합니다.

## Cisco Aironet 장비를 사용한 WPA 2 지원

WPA 2는 이 장비에서 지원됩니다.

- Aironet 1130AG AP 시리즈 및 1230AG AP 시리즈
- Aironet 1100 AP 시리즈
- Aironet 1200 AP 시리즈
- Aironet 1300 AP 시리즈

**참고:** 이러한 AP에 802.11g 무선 장치를 연결하고 Cisco IOS Software 릴리스 12.3(2)JA 이상을 사용하십시오.

WPA 2 및 AES는 다음 항목에서도 지원됩니다.

- 부품 번호가 AIR-RM21A 및 AIR-RM22A인 Aironet 1200 시리즈 라디오 모듈**참고:** 부품 번호가 AIR-RM20A인 Aironet 1200 무선 모듈은 WPA 2를 지원하지 않습니다.
- 펌웨어 버전 2.5가 포함된 Aironet 802.11a/b/g Client Adapter

**참고:** Cisco Aironet 350 시리즈 제품은 AES 지원이 부족하여 WPA 2를 지원하지 않습니다.

**참고:** Cisco Aironet 1400 Series Wireless Bridge는 WPA 2 또는 AES를 지원하지 않습니다.

# 엔터프라이즈 모드에서 구성

**엔터프라이즈 모드**는 인증을 위한 PSK(Pre-Shared Key) 및 IEEE 802.1x 작업 모드에서 모두 상호 운용되도록 테스트된 제품을 의미합니다.802.1x는 다양한 인증 메커니즘 및 더 강력한 암호화 알고리즘을 지원하는 유연성으로 인해 레거시 인증 프레임워크보다 더 안전한 것으로 간주됩니다.엔터프라이즈 모드의 WPA 2는 두 단계로 인증을 수행합니다.개방 인증 컨피그레이션은 첫 번째 단계에서 이루어집니다.두 번째 단계는 EAP 방법 중 하나를 사용하는 802.1x 인증입니다.AES는 암호화 메커니즘을 제공합니다.

엔터프라이즈 모드에서 클라이언트와 인증 서버는 EAP 인증 방법을 사용하여 서로를 인증하고 클라이언트와 서버는 PMK(Pairwise Master Key)를 생성합니다. WPA 2에서는 서버가 동적으로 PMK를 생성하고 PMK를 AP에 전달합니다.

이 섹션에서는 엔터프라이즈 모드 작동 모드에서 WPA 2를 구현하는 데 필요한 컨피그레이션에 대해 설명합니다.

## 네트워크 설정

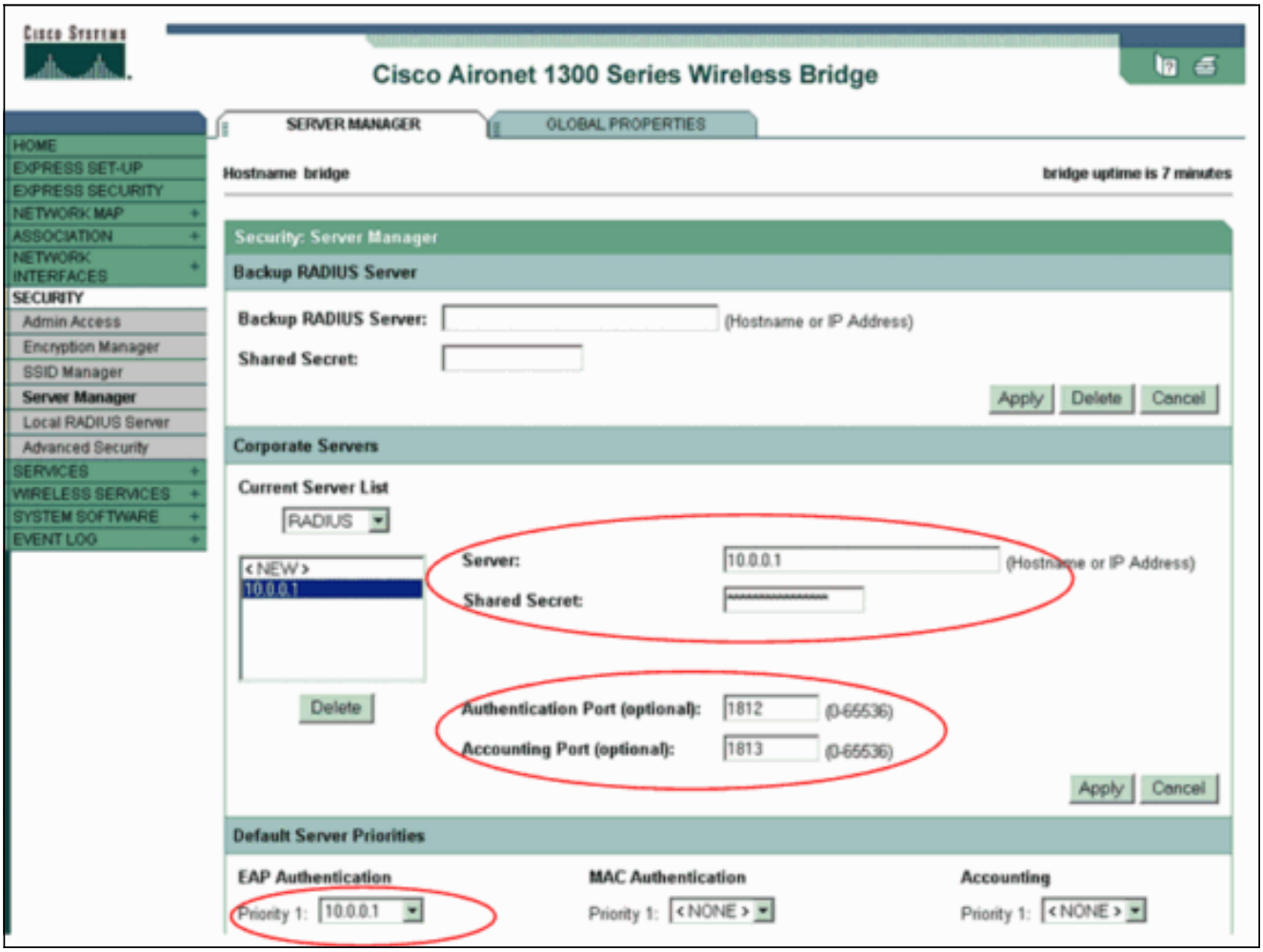
이 설정에서 Cisco LEAP(Lightweight Extensible Authentication Protocol)를 실행하는 Aironet 1310G AP/Bridge는 WPA 2 호환 클라이언트 어댑터를 사용하는 사용자를 인증합니다.키 관리는 AES-CCMP 암호화가 구성된 WPA 2를 사용하여 발생합니다.AP는 LEAP 인증을 실행하는 로컬 RADIUS 서버로 구성됩니다.이 설정을 구현하려면 클라이언트 어댑터 및 AP를 구성해야 합니다 .Configure the AP and Configure the Client Adapter(AP 구성 및 클라이언트 어댑터 구성) 섹션에는 AP 및 클라이언트 어댑터의 컨피그레이션이 표시됩니다.

## AP 구성

GUI를 사용하여 AP를 구성하려면 다음 단계를 완료합니다.

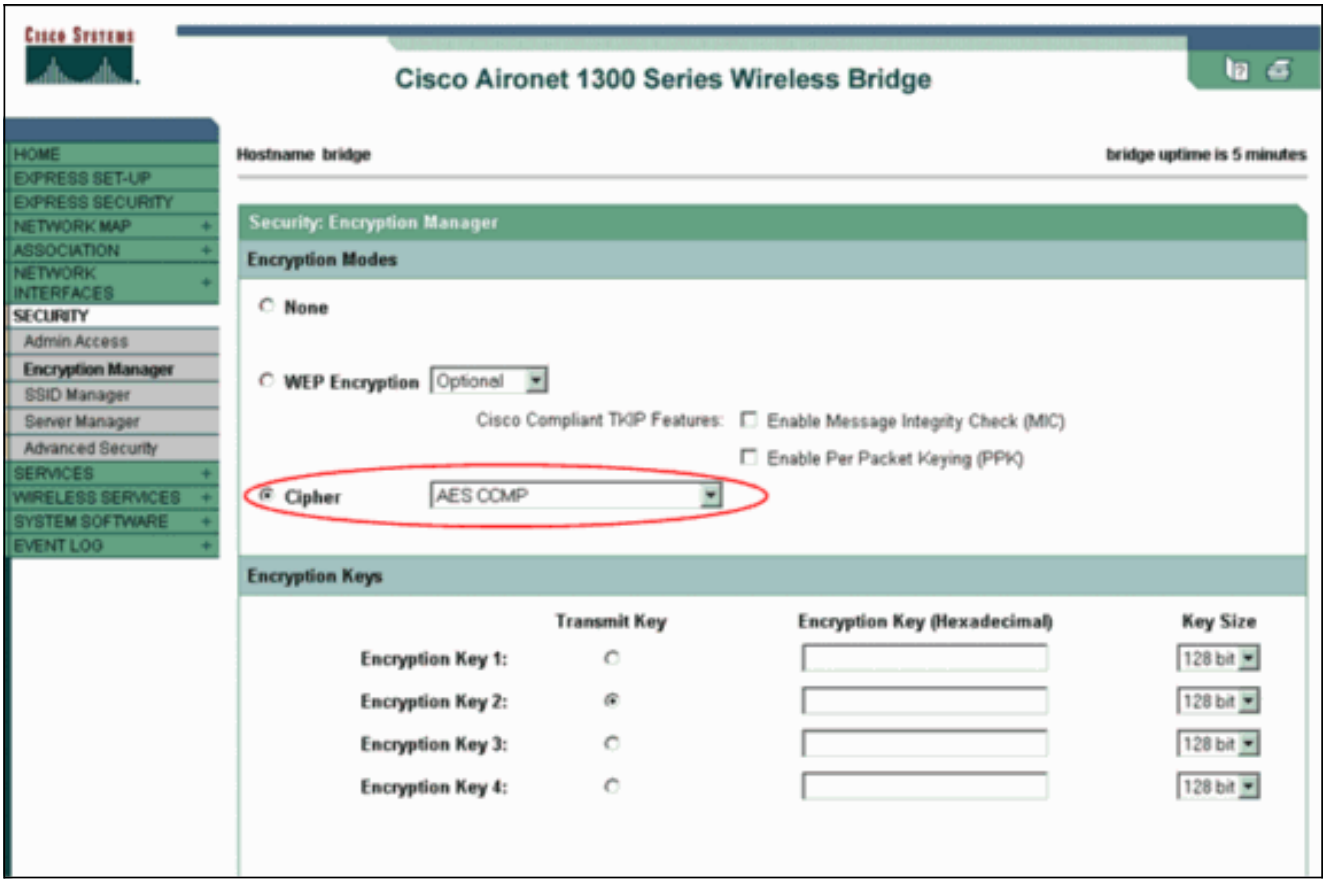
1. AP를 LEAP 인증을 실행하는 로컬 RADIUS 서버로 구성합니다.왼쪽 메뉴에서 **Security > Server Manager**를 선택하고 RADIUS 서버의 IP 주소, 포트 및 공유 암호를 정의합니다.이 컨피그레이션은 AP를 로컬 RADIUS 서버로 구성하므로 AP의 IP 주소를 사용합니다.로컬 RADIUS 서버 작동을 위해 포트 1812 및 1813을 사용합니다.Default Server Priorities(기본 서버 우선순위) 영역에서 기본 EAP 인증 우선순위를 10.0.0.1으로 정의합니다.**참고:** 10.0.0.1 는 로컬 RADIUS 서버입니다

.




2. 왼쪽 메뉴에서 **Security(보안) > Encryption Manager(암호화 관리자)**를 선택하고 다음 단계를 완료합니다.Cipher 메뉴에서 AES CCMP**를** 선택합니다.이 옵션은 CBC-MAC에서 카운터 모드를 사용하는 AES 암호화를 활성화합니다

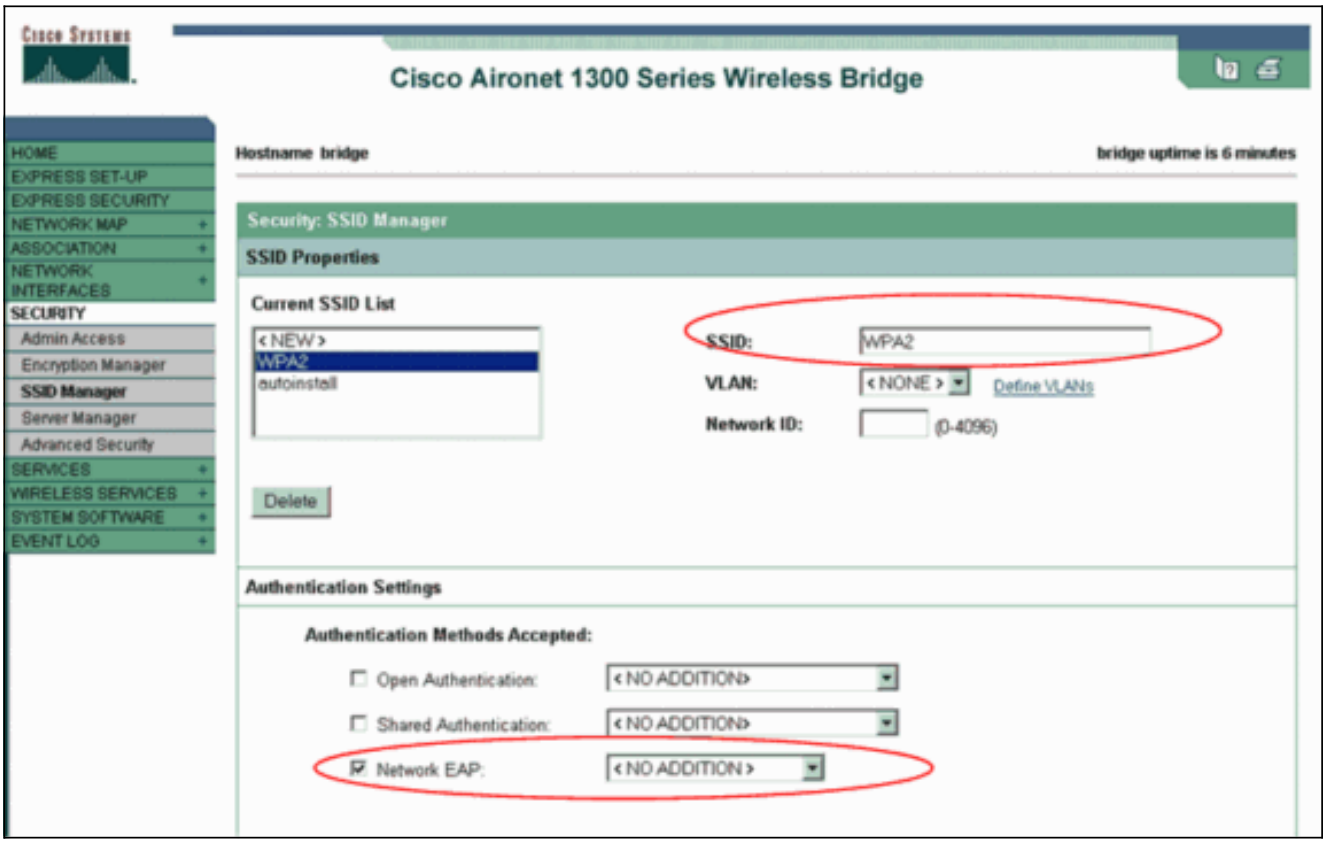
.




Apply를 **클릭합니다**.

3. Security(**보안) > SSID Manager(SSID 관리자**)를 선택하고 WPA 2와 함께 사용할 새 SSID(Service Set Identifier)를 생성합니다.Authentication Methods **Accepted(**인증 방법 수락) 영역에서 Network EAP(네트워크 EAP) 확인란을 선택합니다

.




**참고:** 라디오 인터페이스에서 인증 유형을 구성할 때 다음 지침을 사용합니다.Cisco 클라이언트 - 네트워크 EAP를 사용합니다.타사 클라이언트(CCX[Cisco Compatible Extensions] 호환

제품 포함) - EAP를 사용하여 개방형 인증을 사용합니다.Cisco 및 타사 클라이언트의 조합 - 네트워크 EAP와 EAP를 통한 개방 인증을 모두 선택합니다.Security SSID Manager(보안 SSID 관리자) 창을 아래로 스크롤하여 Authenticated Key Management(인증된 키 관리) 영역으로 이동한 후 다음 단계를 완료합니다.Key Management(키 관리) 메뉴에서 Mandatory(필수)를 **선택합니다**.오른쪽에서 **WPA** 확인란을 선택합니다.Apply를 **클릭합니다**.**참고:** VLAN의 정의는 선택 사항입니다.VLAN을 정의할 경우 이 SSID의 사용과 연결된 클라이언트 디바이스는 VLAN으로 그룹화됩니다.VLAN을 구현하는 방법에 대한 자세한 내용은 VLAN 구성을 참조하십시오

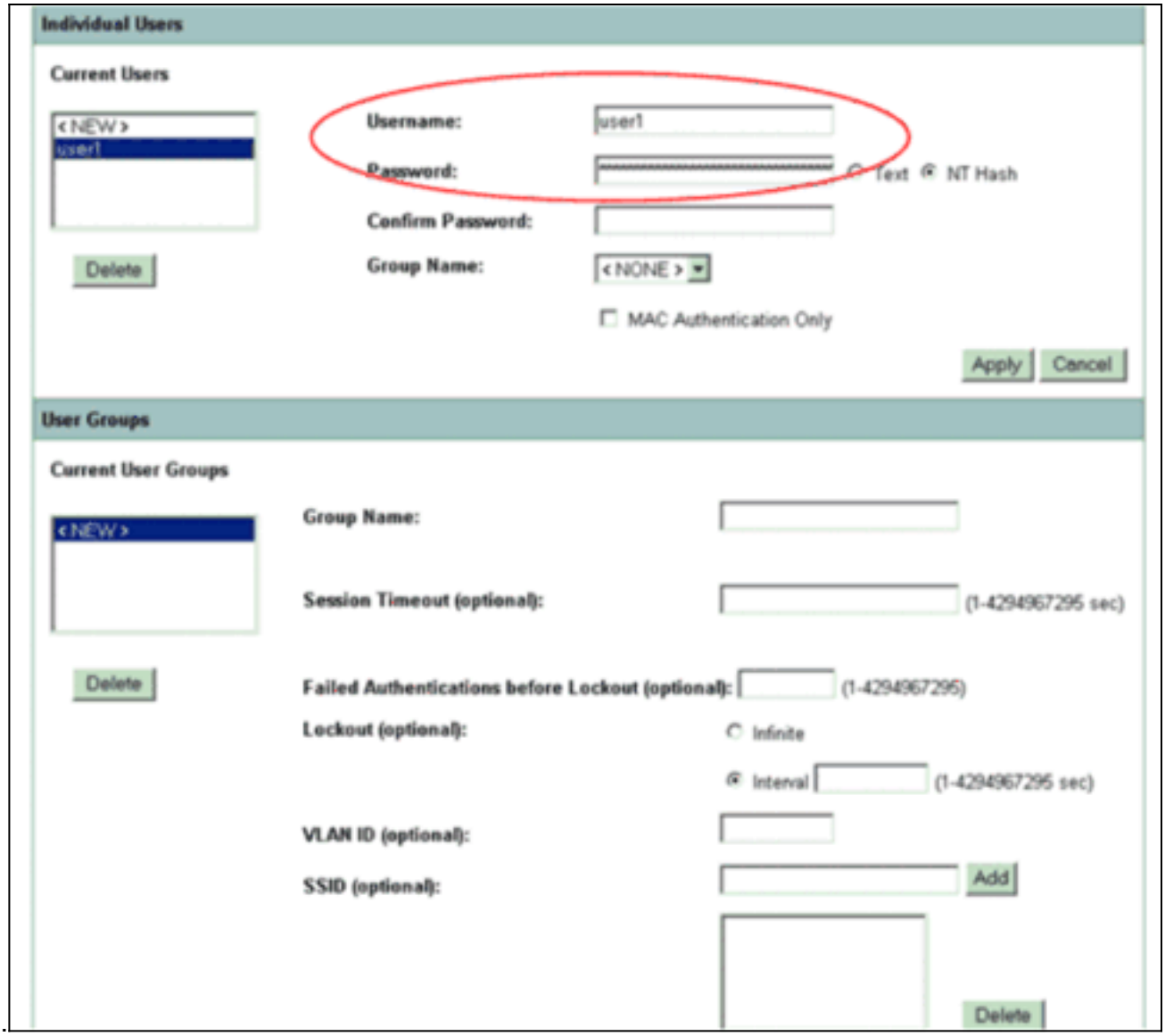

.

4. Security(**보안) > Local Radius Server(로컬 RADIUS 서버)를** 선택하고 다음 단계를 완료합니다.창 상단에 **있는 일반 설정** 탭을 클릭합니다.LEAP 확인란을 선택하고 Apply를 **클릭합니다**.Network Access Servers(네트워크 액세스 서버) 영역에서 RADIUS 서버의 IP 주소 및 공유 암호를 정의합니다.로컬 RADIUS 서버의 경우 AP의 IP 주소를 사용합니다

.


Apply를 **클릭합니다**.

5. 일반 설정 창을 아래로 스크롤하여 개별 사용자 영역으로 이동한 다음 개별 사용자를 정의합니다.사용자 그룹의 정의는 선택 사항입니다




이 컨피그레이션은 "user1"이라는 이름과 비밀번호를 가진 사용자를 정의합니다.또한 컨피그레이션에서는 비밀번호에 대해 NT 해시를 선택합니다.이 섹션의 절차를 완료한 후 AP는 클라이언트의 인증 요청을 수락할 준비가 되었습니다.다음 단계는 클라이언트 어댑터를 구성하는 것입니다.

## CLI 컨피그레이션

**액세스 포인트**

```
ap#show running-config
Building configuration...
.
.
.
aaa new-model !--- This command reinitializes the
authentication, !--- authorization and accounting
functions. ! ! aaa group server radius rad_eap
 server 10.0.0.1 auth-port 1812 acct-port 1813
!--- A server group for RADIUS is created called
"rad_eap" !--- that uses the server at 10.0.0.1 on ports
1812 and 1813. . . . aaa authentication login
eap_methods group rad_eap
!--- Authentication [user validation] is to be done for
!--- users in a group called "eap_methods" who use
server group "rad_eap". . . . ! bridge irb ! interface
Dot11Radio0 no ip address no ip route-cache !
```

```
encryption vlan 1 key 1 size 128bit
   12345678901234567890123456 transmit-key
!---This step is optional !--- This value seeds the
initial key for use with !--- broadcast
[255.255.255.255] traffic. If more than one VLAN is !---
used, then keys must be set for each VLAN. encryption
vlan 1 mode wep mandatory
!--- This defines the policy for the use of Wired
Equivalent Privacy (WEP). !--- If more than one VLAN is
used, !--- the policy must be set to mandatory for each
VLAN. broadcast-key vlan 1 change 300
  !--- You can also enable Broadcast Key Rotation for
each vlan and Specify the time after which Brodacst key
is changed. If it is disabled Broadcast Key is still
used but not changed. ssid cisco vlan 1
!--- Create a SSID Assign a vlan to this SSID
authentication open eap eap_methods
 authentication network-eap eap_methods
 !--- Expect that users who attach to SSID "cisco" !---
request authentication with the type 128 Open EAP and
Network EAP authentication !--- bit set in the headers
of those requests, and group those users into !--- a
group called "eap_methods." ! speed basic-1.0 basic-2.0
basic-5.5 basic-11.0 rts threshold 2312 channel 2437
station-role root bridge-group 1 bridge-group 1
subscriber-loop-control bridge-group 1 block-unknown-
source no bridge-group 1 source-learning no bridge-group
1 unicast-flooding bridge-group 1 spanning-disabled . .
. interface FastEthernet0 no ip address no ip route-
cache duplex auto speed auto bridge-group 1 no bridge-
group 1 source-learning bridge-group 1 spanning-disabled
! interface BVI1 ip address 10.0.0.1 255.255.255.0 !---
The address of this unit. no ip route-cache ! ip
default-gateway 10.77.244.194 ip http server ip http
help-path
http://www.cisco.com/warp/public/779/smbiz/prodconfig/he
lp/eag/ivory/1100 ip radius source-interface BVI1 snmp-
server community cable RO snmp-server enable traps tty
radius-server local
!--- Engages the Local RADIUS Server feature. nas
10.0.0.1 key shared_secret
!--- Identifies itself as a RADIUS server, reiterates !-
-- "localness" and defines the key between the server
(itself) and the access point(itself). ! group testuser
!--- Groups are optional. ! user user1 nthash password1
group testuser
!--- Individual user user user2 nthash password2 group
testuser
!--- Individual user !--- These individual users
comprise the Local Database ! radius-server host
10.0.0.1 auth-port 1812 acct-port
   1813 key shared_secret
!--- Defines where the RADIUS server is and the key
between !--- the access point (itself) and the server.
radius-server retransmit 3 radius-server attribute 32
include-in-access-req format %h radius-server
authorization permit missing Service-Type radius-server
vsa send accounting bridge 1 route ip ! ! line con 0
line vty 5 15 ! end
```

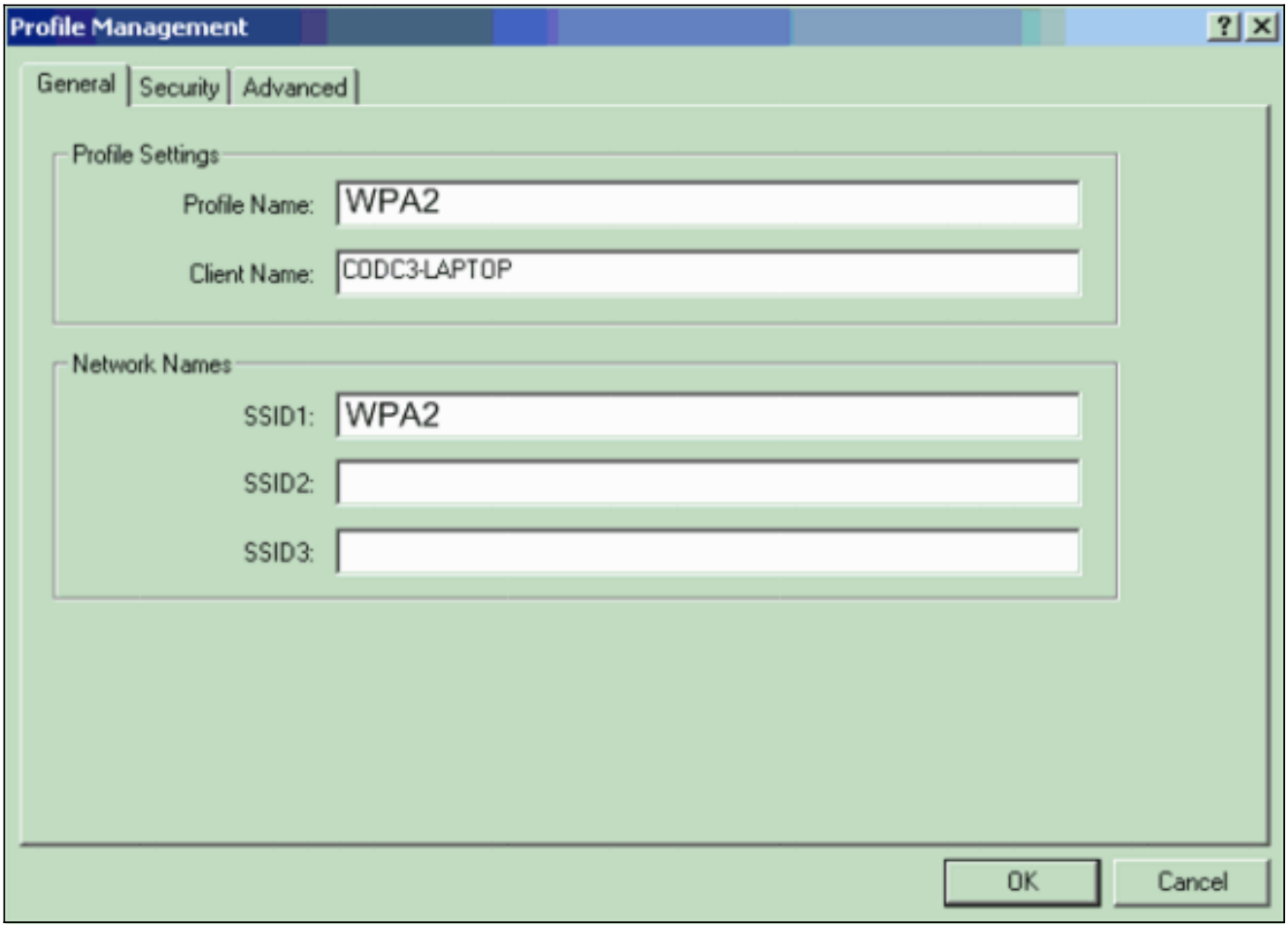
## 클라이언트 어댑터 구성

다음 단계를 완료하십시오.

**참고:** 이 문서에서는 펌웨어 2.5를 실행하는 Aironet 802.11a/b/g 클라이언트 어댑터를 사용하며 ADU 버전 2.5를 사용하는 클라이언트 어댑터의 컨피그레이션에 대해 설명합니다.

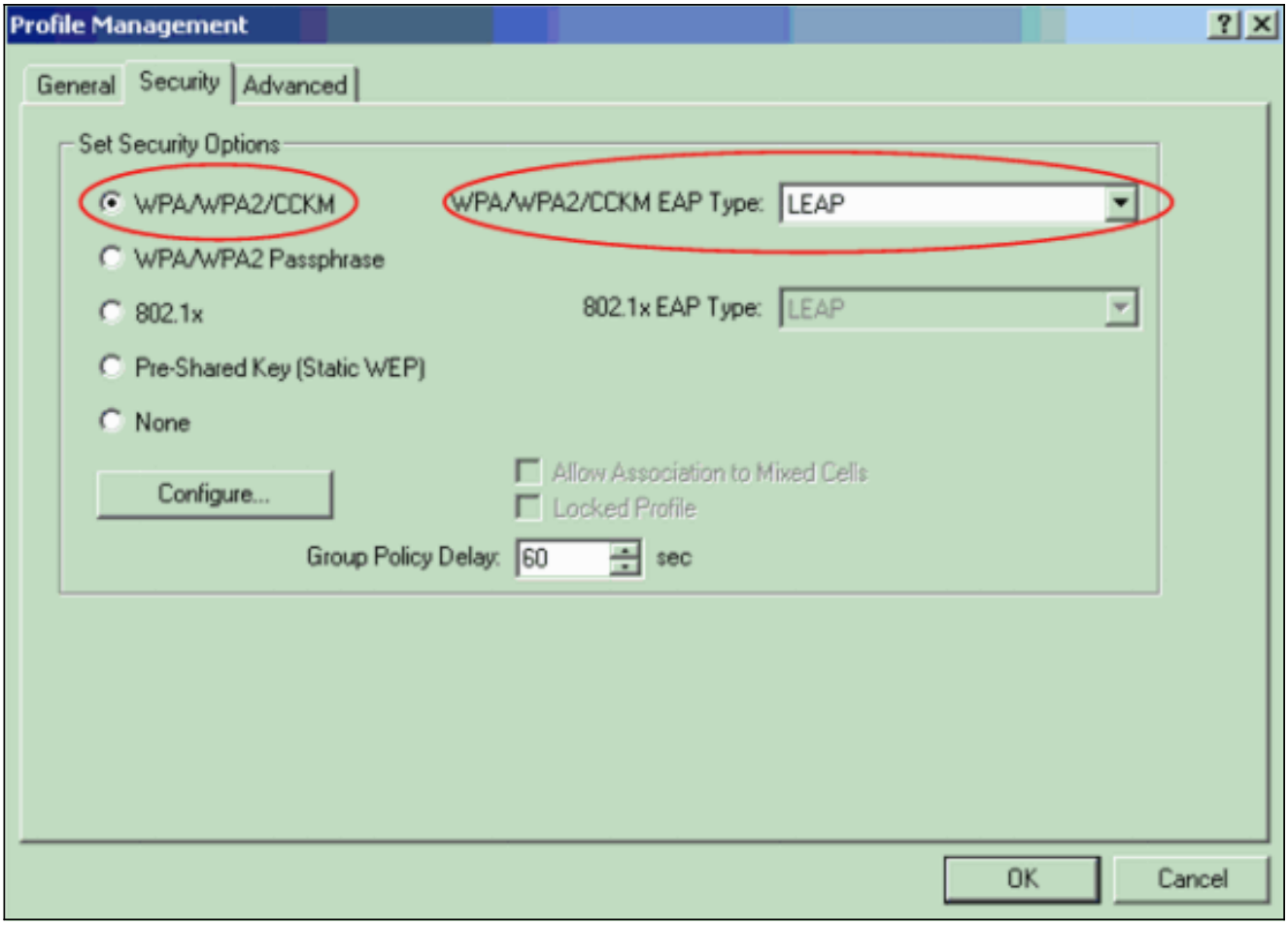
1. ADU의 Profile Management(프로필 관리) 창에서 **New(새로 만들기)를** 클릭하여 새 프로필을 생성합니다.WPA 2 엔터프라이즈 모드 작업에 대한 구성을 설정할 수 있는 새 창이 표시됩니다.General(일반) 탭에서 클라이언트 어댑터가 사용할 프로파일 이름 및 SSID를 입력합니다.이 예에서는 프로파일 이름과 SSID가 WPA2입니다.**참고:** SSID는 WPA 2에 대해 AP에 구성한 SSID와 일치해야 합니다

   .

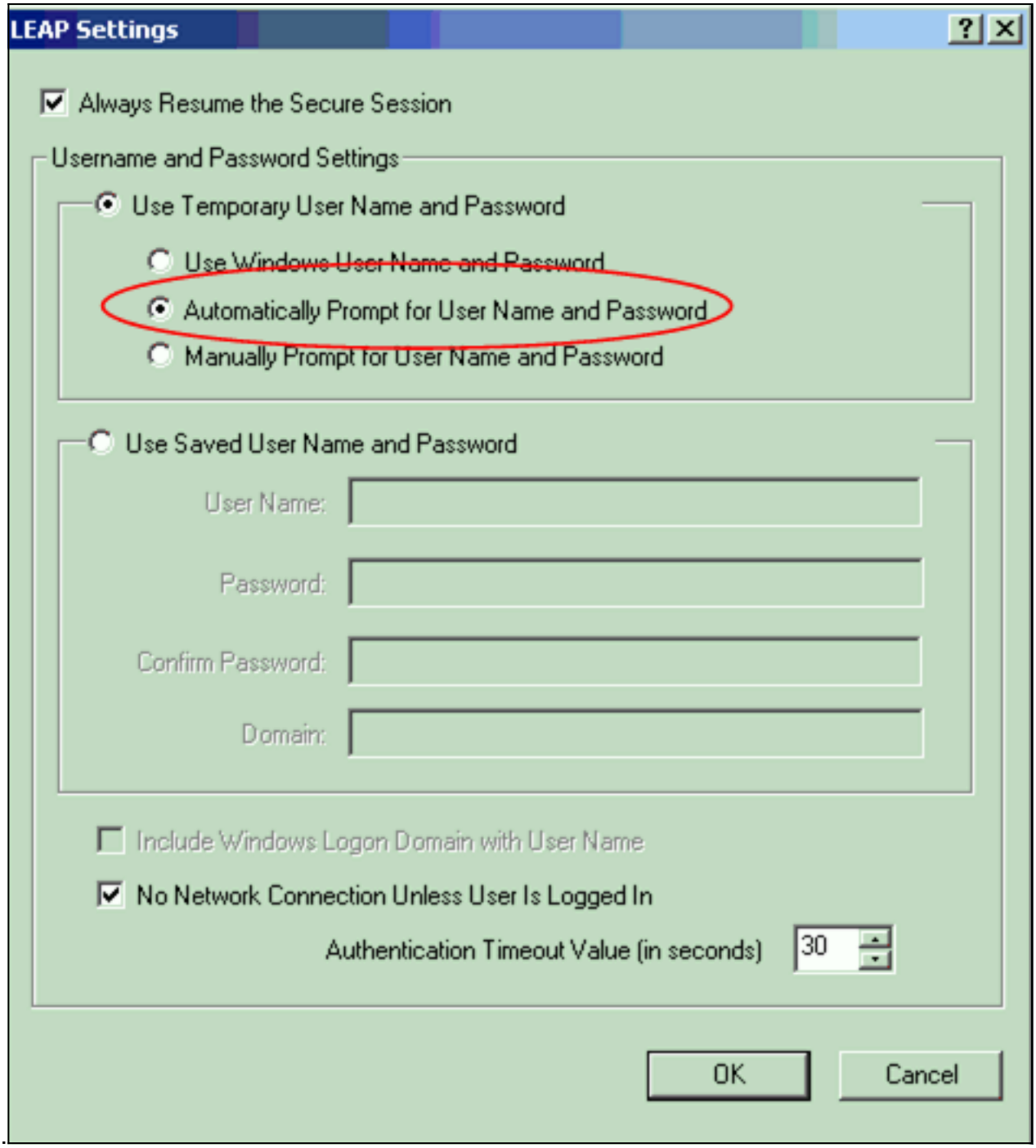



2. **보안** 탭을 클릭하고 **WPA/WPA2/CCKM**을 클릭한 다음 WPA/WPA2/CCKM EAP 유형 메뉴에서 LEAP를 선택합니다.이 작업은 AP에서 구성하는 WPA 또는 WPA 2를 활성화합니다

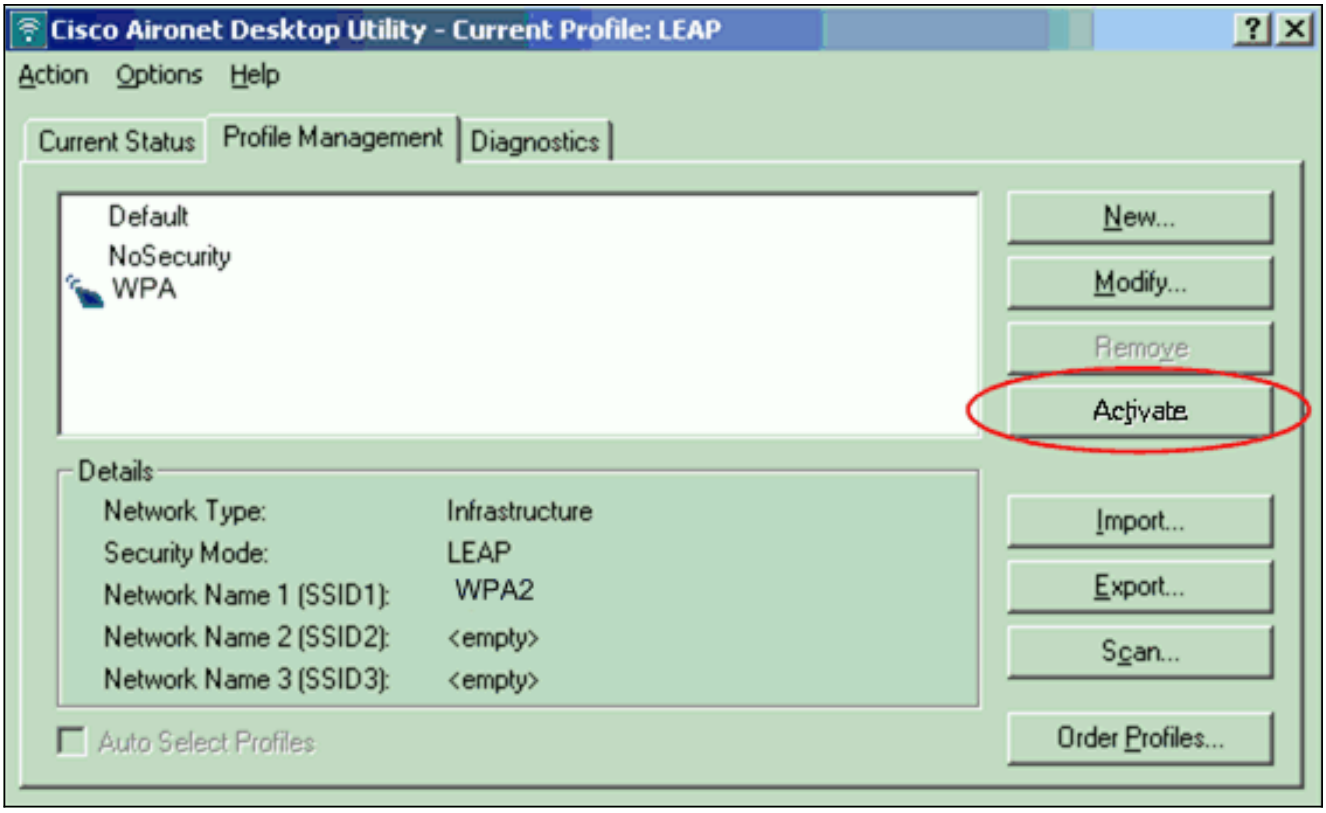
   .




3. LEAP 설정을 정의하려면 Configure를 클릭합니다.
4. 요구 사항에 따라 적절한 사용자 이름 및 비밀번호 설정을 선택하고 **확인**을 클릭합니다.이 컨피그레이션에서는 Automatically Prompt for User Name and Password 옵션을 선택합니다.이 옵션을 사용하면 LEAP 인증이 발생할 때 사용자 이름과 비밀번호를 수동으로 입력할 수 있습니다




5. OK(**확인**)를 클릭하여 Profile Management(프로필 관리) 창을 종료합니다.
6. 클라이언트 어댑터에서 이 프로파일을 활성화하려면 Activate를 클릭합니다
.

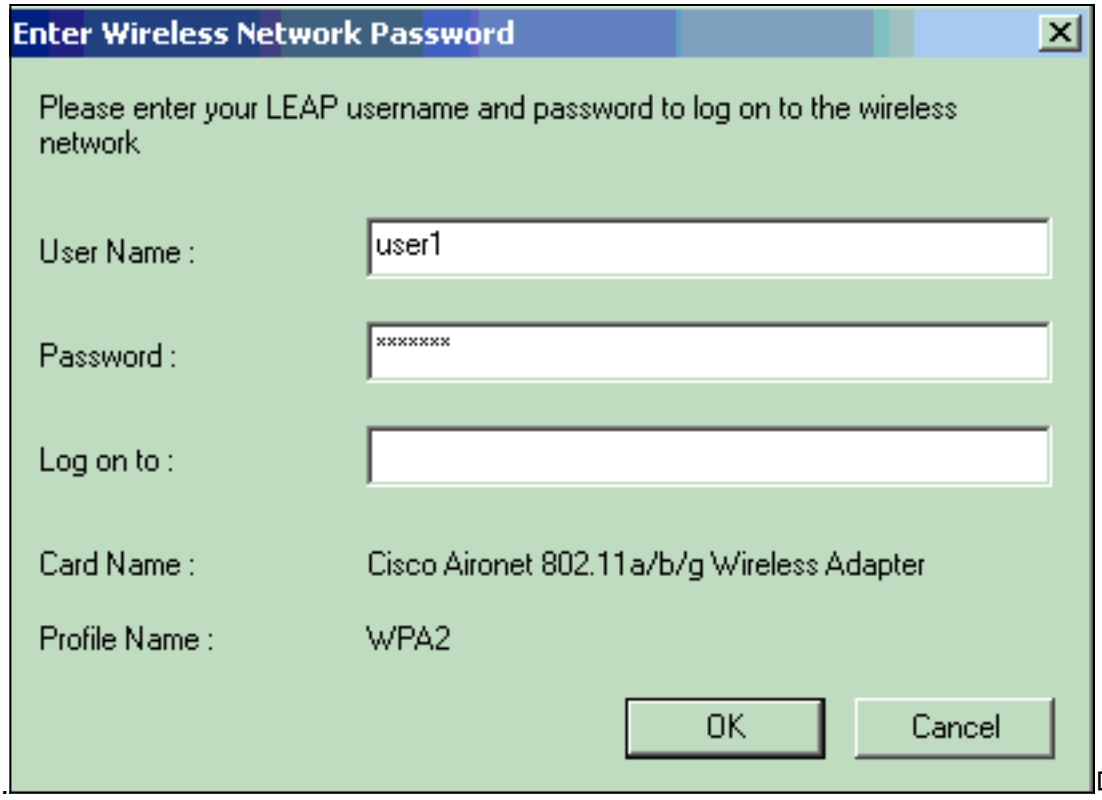



**참고:** Microsoft WZC(Wireless Zero Configuration)를 사용하여 클라이언트 어댑터를 구성하는 경우 기본적으로 WZC에서는 WPA 2를 사용할 수 없습니다.따라서 WZC 지원 클라이언트가 WPA 2를 실행하도록 허용하려면 Microsoft Windows XP용 핫픽스를 설치해야 합니다.설치는 Microsoft 다운로드 센터 - Update for Windows XP(KB893357) 를 참조하십시오.핫픽스를 설치한 후 WZC를 사용하여 WPA 2를 구성할 수 있습니다.

## 다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

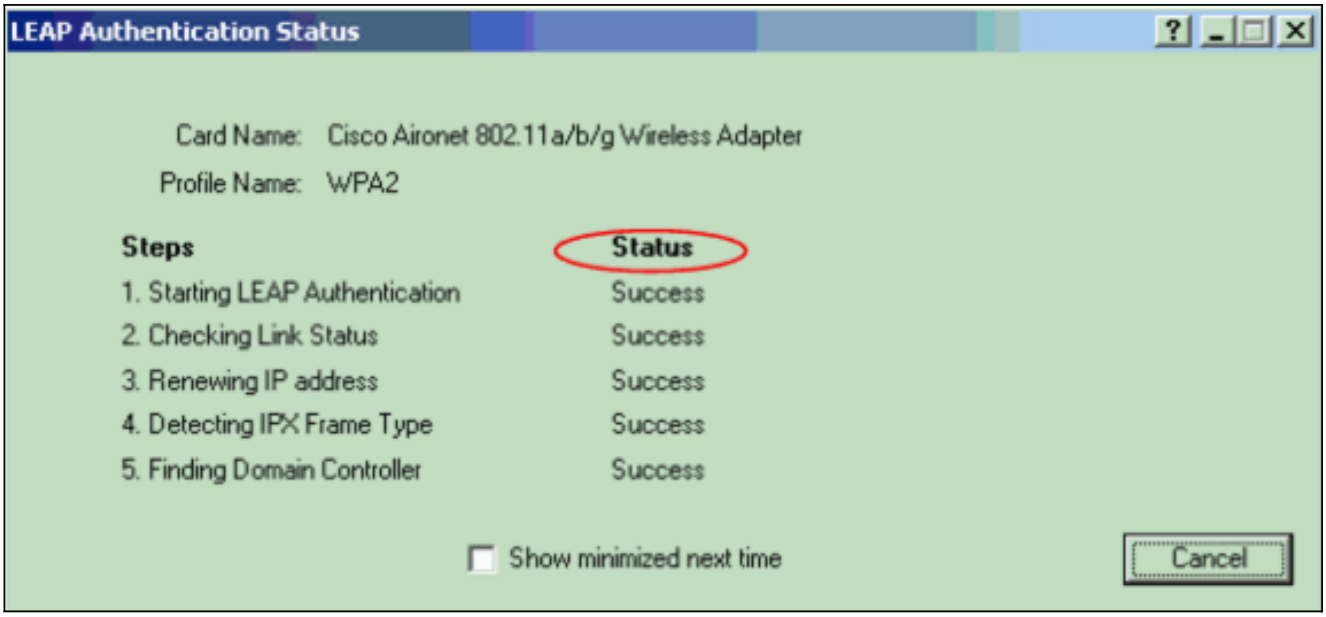
1. Enter Wireless Network Password(무선 네트워크 비밀번호 입력) 창이 표시되면 사용자 이름과 비밀번호를 입력합니다




다음 창은 LEAP 인증 상태입니다.이 단계에서는 로컬 RADIUS 서버에 대한 사용자 자격 증명을 확인합니다.

2. 인증 결과를 보려면 Status(상태) 영역을 확인합니다

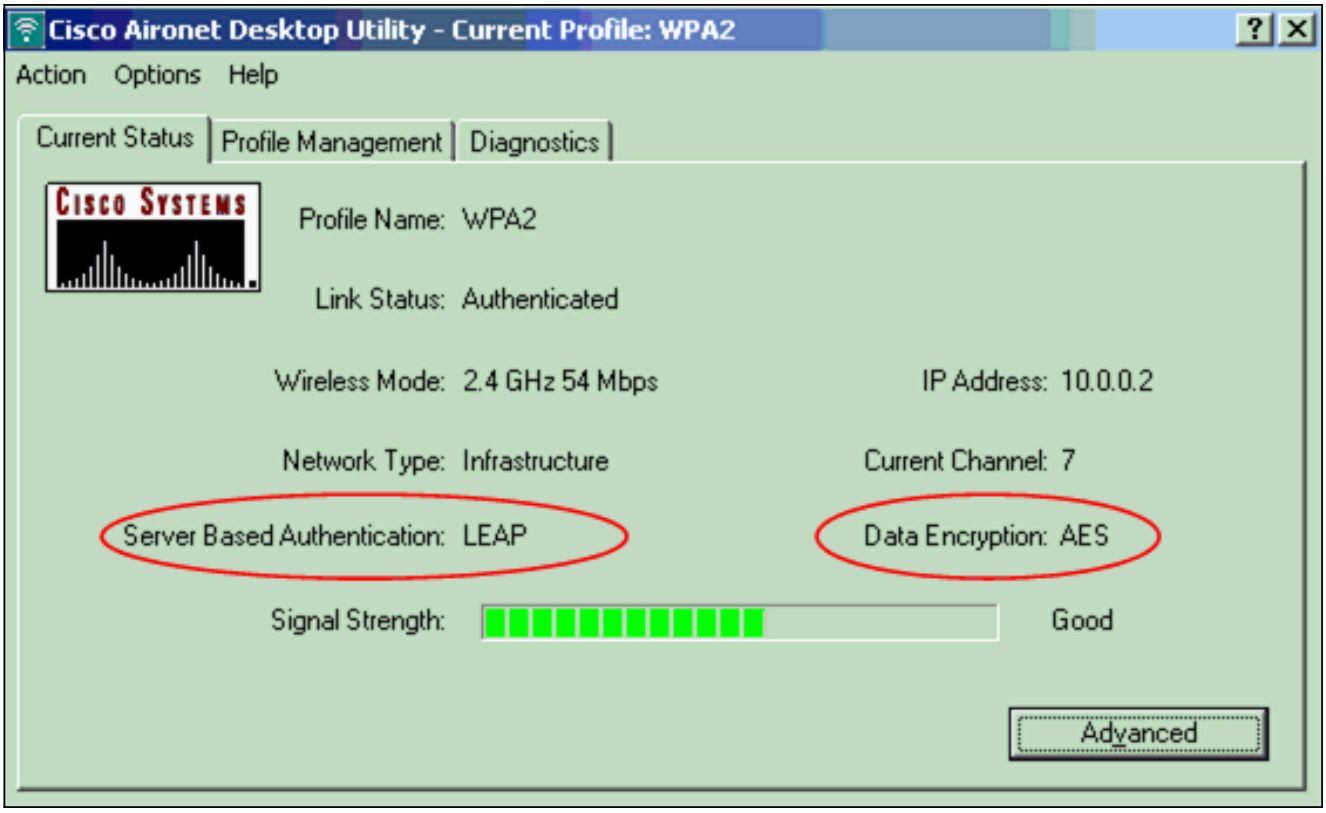
.




인증이 성공하면 클라이언트는 무선 LAN에 연결됩니다.

3. 클라이언트가 AES 암호화 및 LEAP 인증을 사용하는지 확인하려면 ADU Current Status(ADU 현재 상태)를 확인합니다.이것은 WLAN에서 LEAP 인증 및 AES 암호화를 사용하여 WPA 2를 구현했음을 보여줍니다

.




4. 클라이언트가 WPA 2에서 성공적으로 인증되었는지 확인하려면 AP/bridge 이벤트 로그를 확인하십시오

.


## 문제 해결

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

# 개인 모드에서 구성

**개인 모드**라는 용어는 인증을 위한 PSK 전용 작동 모드에서 상호 운용되도록 테스트된 제품을 의미합니다.이 모드에서는 AP 및 클라이언트에서 PSK를 수동으로 구성해야 합니다.PSK는 클라이언

트 스테이션과 AP 모두에서 비밀번호 또는 식별 코드를 통해 사용자를 인증합니다.인증 서버가 필요하지 않습니다.클라이언트는 클라이언트 비밀번호가 AP 비밀번호와 일치하는 경우에만 네트워크에 액세스할 수 있습니다.이 비밀번호는 TKIP 또는 AES가 데이터 패킷 암호화를 위한 암호화 키를 생성하는 데 사용하는 키 자료를 제공합니다.개인 모드는 SOHO 환경을 대상으로 하며 엔터프라이즈 환경에서 안전한 것으로 간주되지 않습니다.이 섹션에서는 개인 작동 모드에서 WPA 2를 구현하는 데 필요한 컨피그레이션을 제공합니다.

## 네트워크 설정

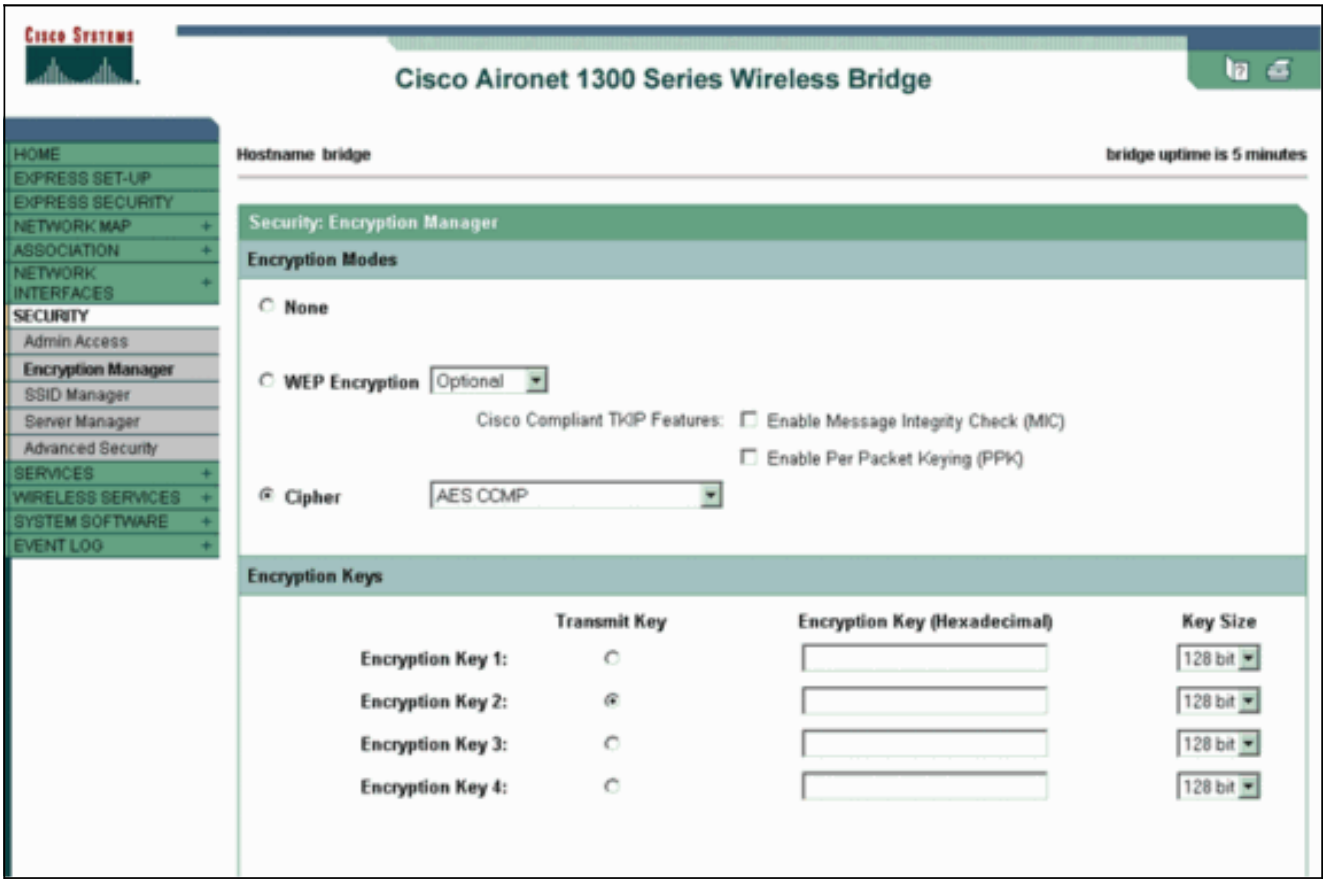
이 설정에서는 WPA 2 호환 클라이언트 어댑터가 있는 사용자가 Aironet 1310G AP/브리지를 인증합니다.키 관리는 AES-CCMP 암호화가 구성된 WPA 2 PSK를 사용하여 발생합니다.Configure the AP and Configure the Client Adapter(AP 구성 및 클라이언트 어댑터 구성) 섹션에는 AP 및 클라이언트 어댑터의 컨피그레이션이 표시됩니다.

## AP 구성

다음 단계를 완료하십시오.

1. 왼쪽 메뉴**에서 Security(보안) > Encryption Manager(암호화 관리자)**를 선택하고 다음 단계를 완료합니다.Cipher 메뉴에서 AES CCMP**를** 선택합니다.이 옵션은 CCMP와 함께 카운터 모드를 사용하여 AES 암호화를 활성화합니다

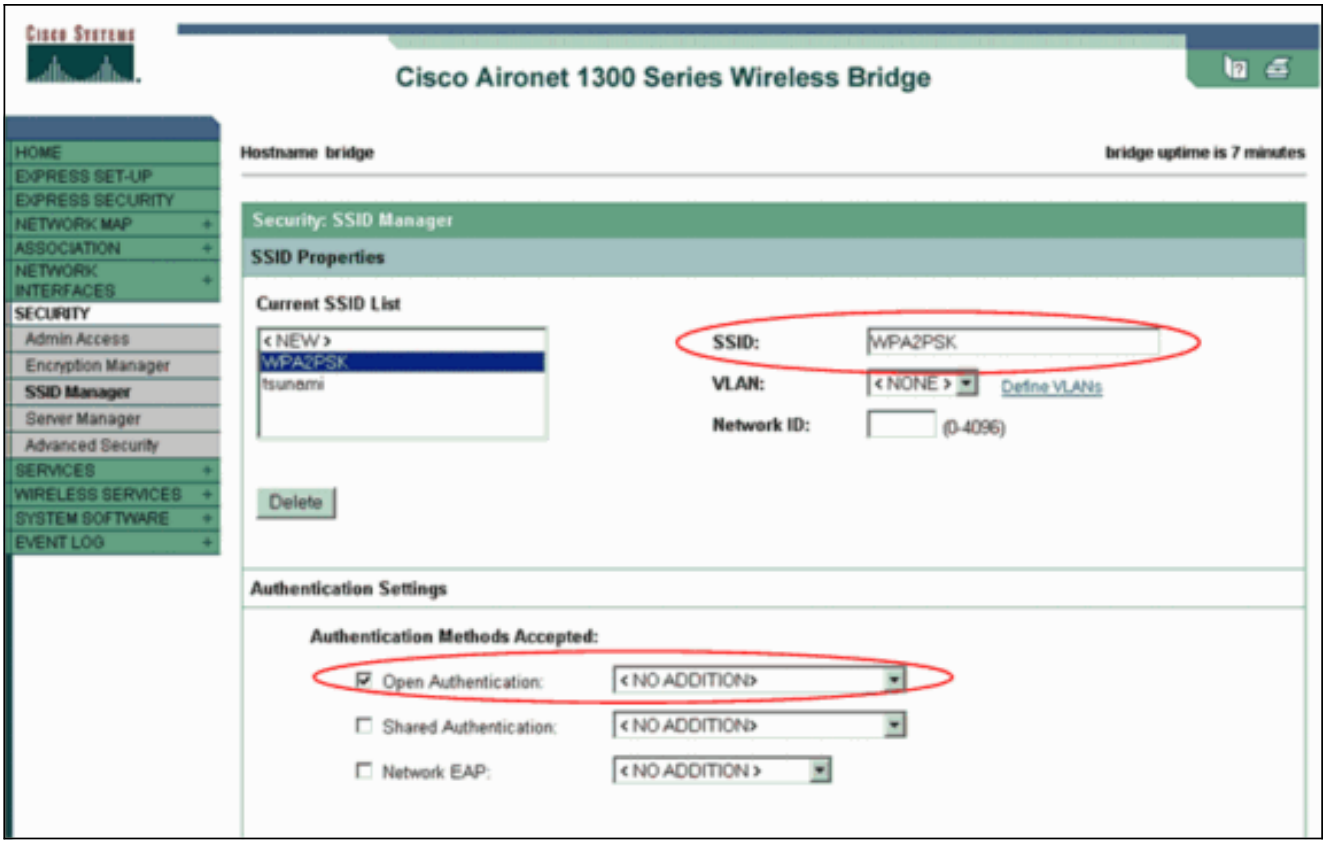
.




Apply를 **클릭합니다**.

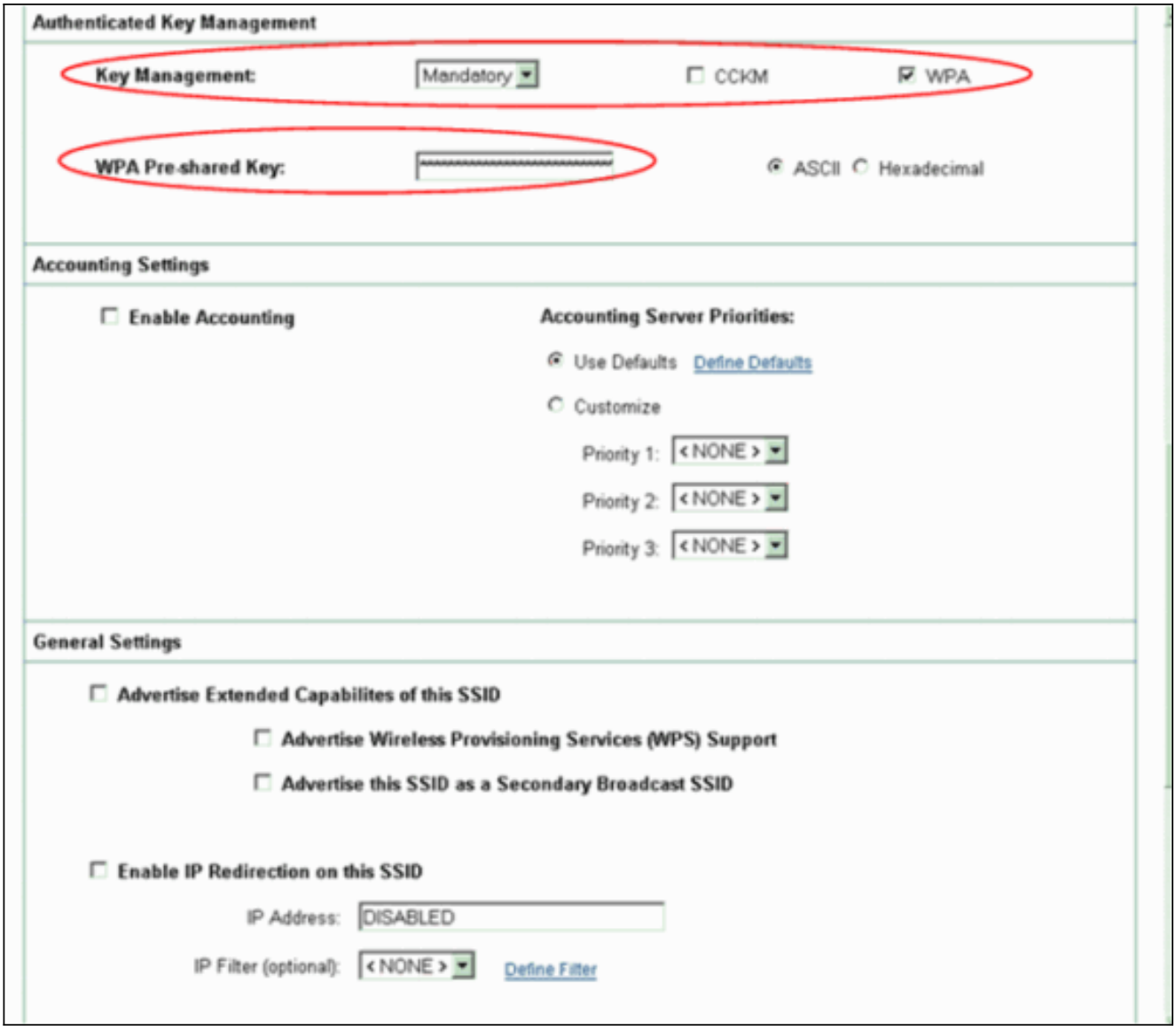
2. Security(**보안) > SSID Manager(SSID 관리자)**를 선택하고 WPA 2와 함께 사용할 새 SSID를 생성합니다.Open Authentication(**인증 열기)** 확인란을 선택합니다

.




아래로 스크롤하여 보안:SSID Manager 창에서 Authenticated Key Management(인증된 키 관리) 영역으로 이동하여 다음 단계를 완료합니다.Key Management(키 관리) 메뉴에서 Mandatory(필수)를 **선택합니다**.오른쪽에서 **WPA** 확인란을 선택합니다

.



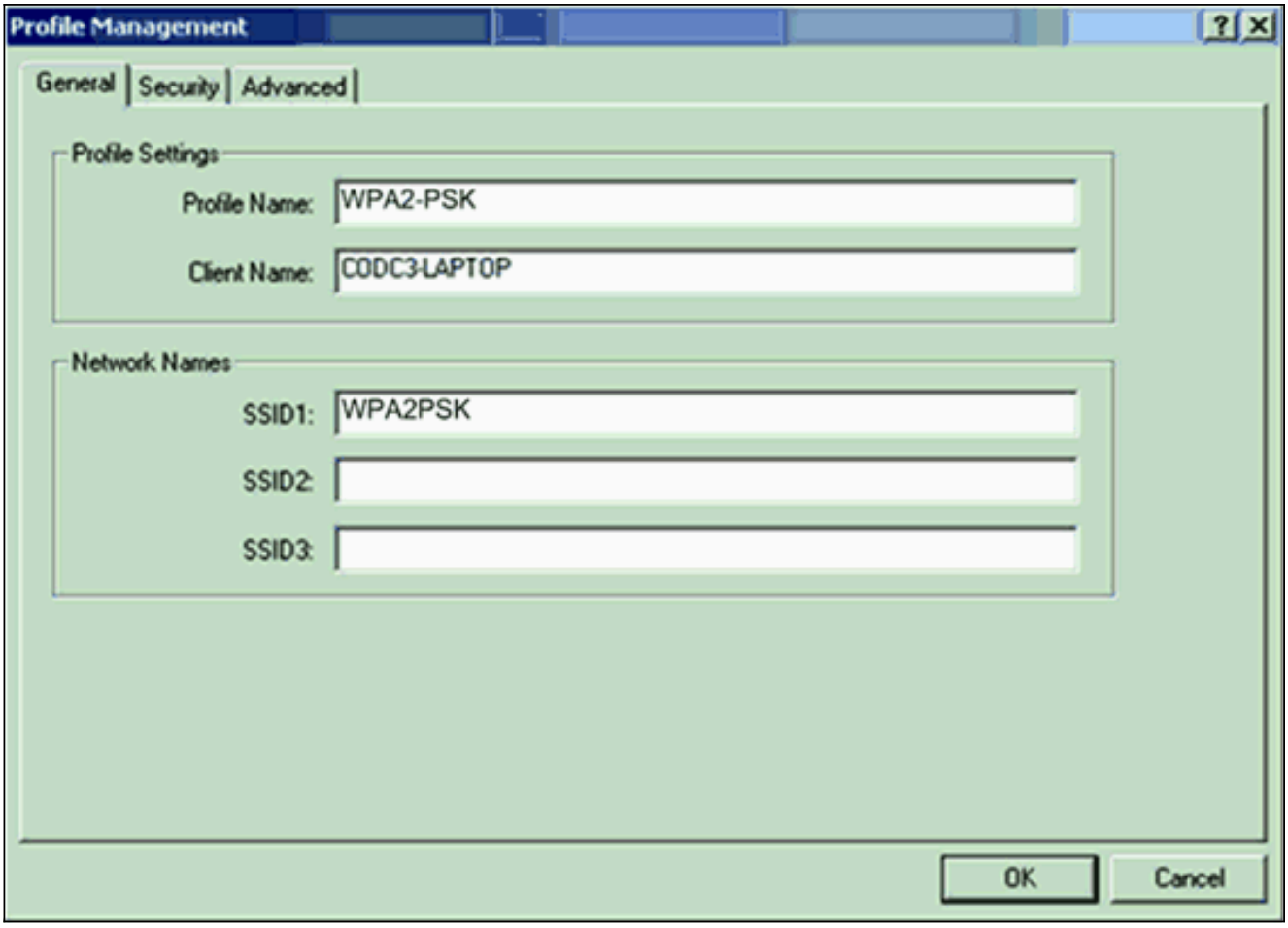

WPA PSK 공유 암호 키 또는 WPA PSK 암호 키를 입력합니다.이 키는 클라이언트 어댑터에서 구성한 WPA PSK 키와 일치해야 합니다.Apply를 **클릭합니다**.

이제 AP가 무선 클라이언트로부터 인증 요청을 받을 수 있습니다.

## 클라이언트 어댑터 구성

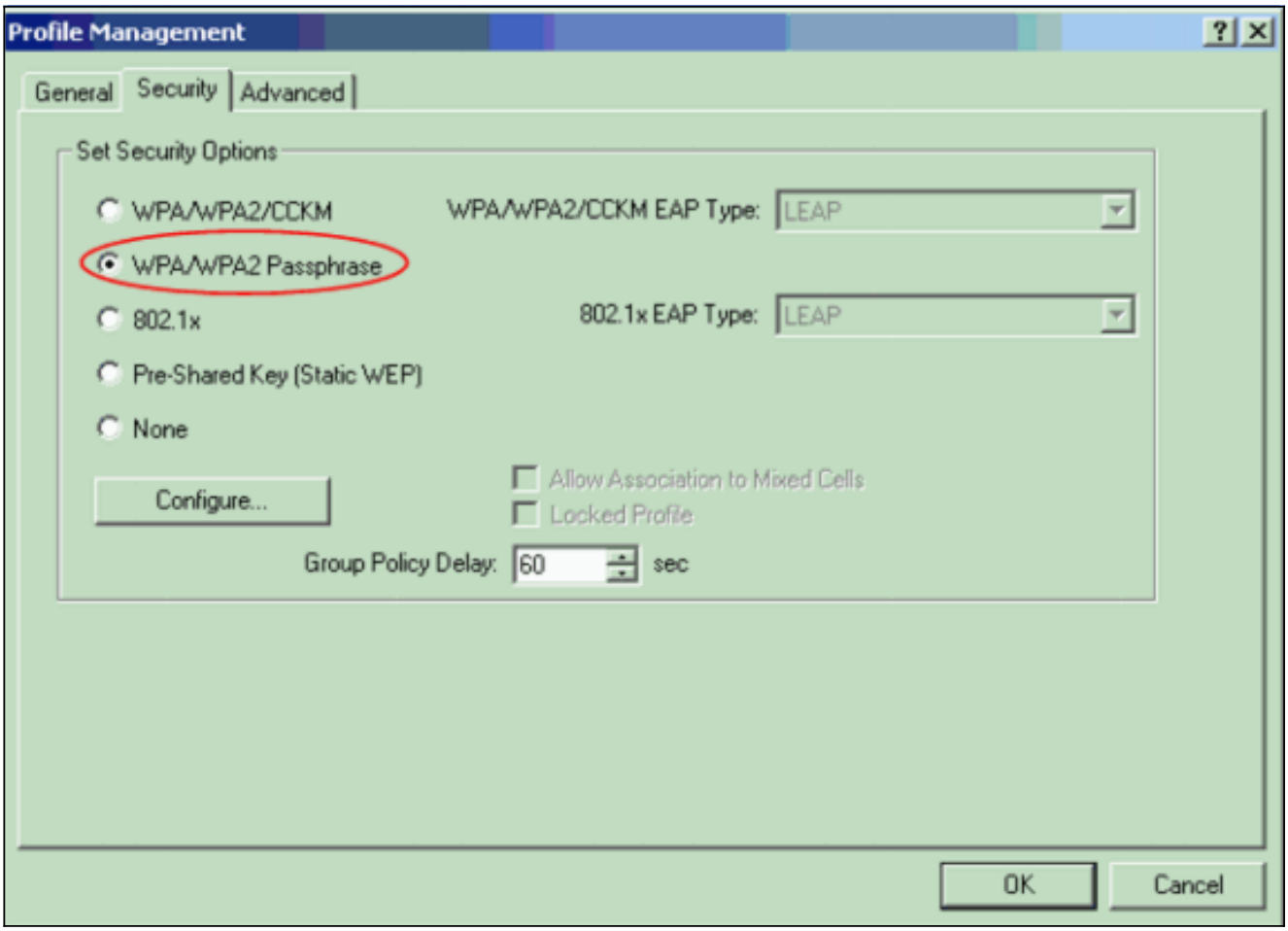
다음 단계를 완료하십시오.

1. ADU의 Profile Management(프로필 관리) 창에서 **New(새로 만들기)를** 클릭하여 새 프로필을 생성합니다.WPA 2 PSK 작동 모드에 대한 컨피그레이션을 설정할 수 있는 새 창이 표시됩니다.General(일반) 탭에서 클라이언트 어댑터가 사용할 프로파일 이름 및 SSID를 입력합니다.이 예에서 프로파일 이름은 WPA2-PSK이고 SSID는 WPA2PSK입니다.**참고:** SSID는 WPA 2 PSK용 AP에 구성한 SSID와 일치해야 합니다
.



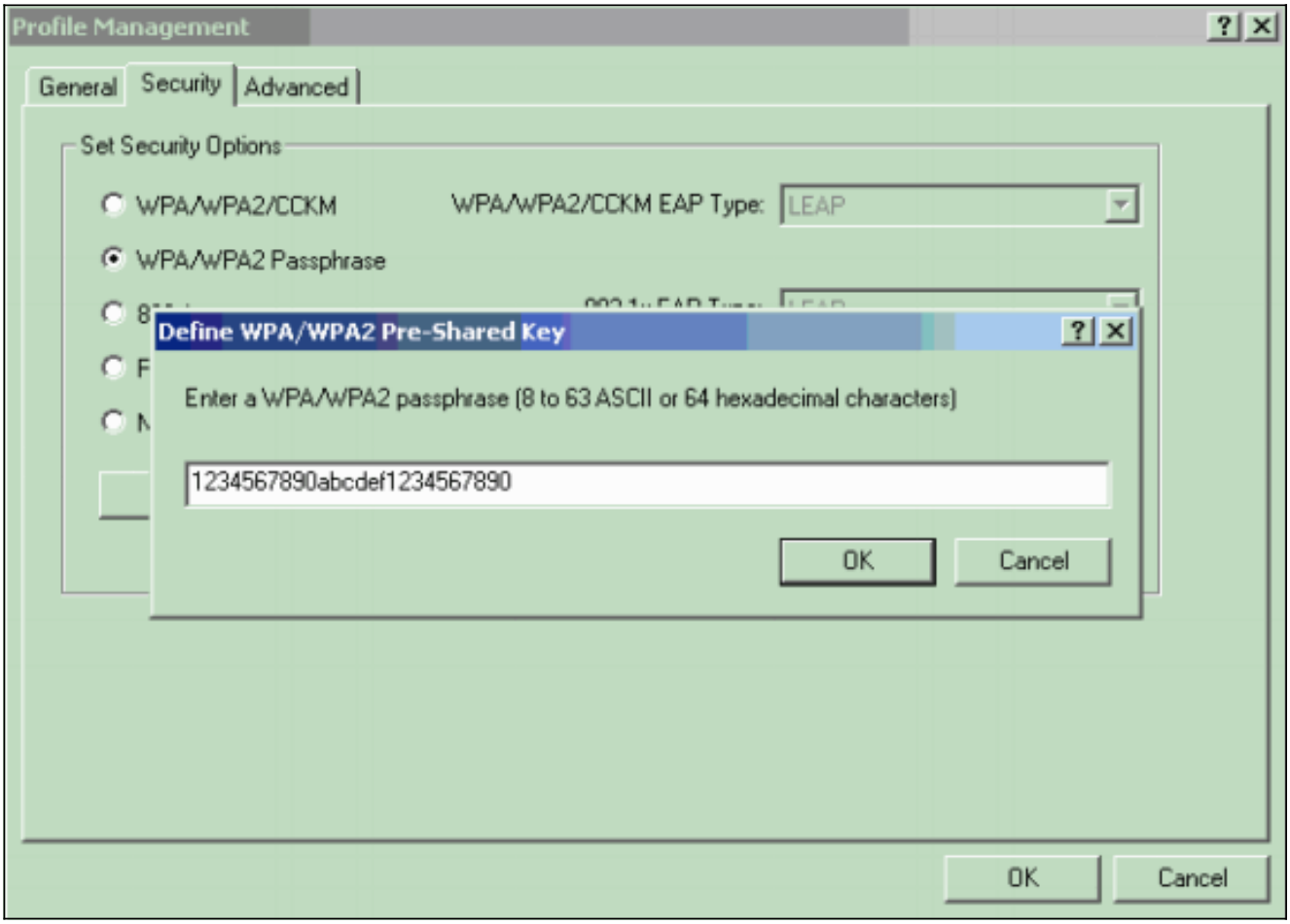

2. **보안** 탭을 클릭하고 **WPA/WPA2 암호**를 클릭합니다.이 작업은 AP에서 구성하는 WPA PSK 또는 WPA 2 PSK를 활성화합니다

.



3. 구성을 **클릭합니다**.WPA/WPA2 사전 공유 키 정의 창이 표시됩니다.
4. 시스템 관리자로부터 WPA/WPA2 암호를 얻은 후 WPA/WPA2 암호 필드에 암호를 입력합니다.인프라 네트워크의 AP에 대한 패스프레이즈 또는 Ad Hoc 네트워크의 다른 클라이언트에 대한 패스프레이즈를 가져옵니다.암호를 입력하려면 다음 지침을 사용하십시오.WPA/WPA2 암호는 8~63자의 ASCII 텍스트 문자 또는 64자의 16진수 문자를 포함해야 합니다.클라이언트 어댑터 WPA/WPA2 패스프레이즈는 통신할 AP의 패스프레이즈와 일치해야 합니다

.




5. **확인**을 클릭하여 암호를 저장하고 프로파일 관리 창으로 돌아갑니다.

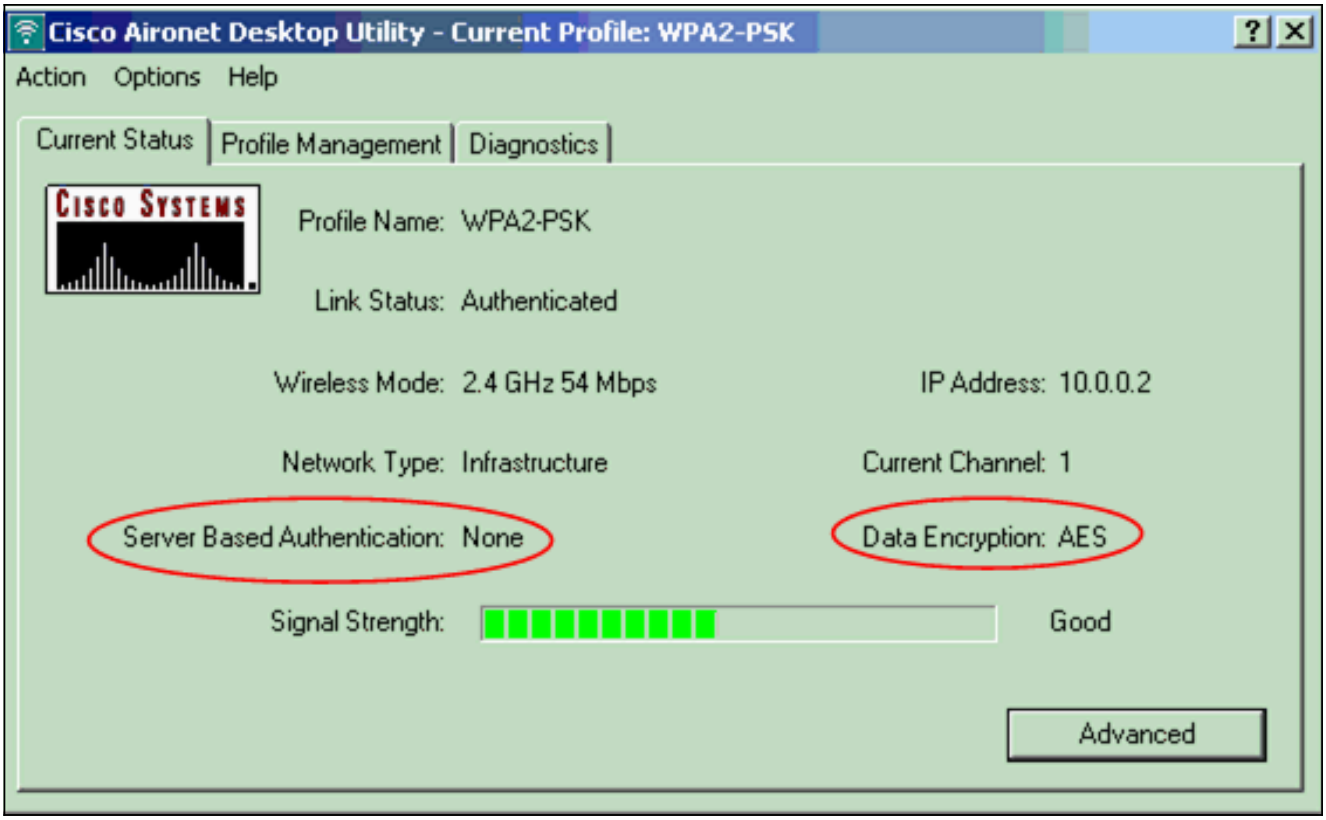
## 다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

WPA 2 PSK 프로파일이 활성화되면 AP는 WPA 2 암호(PSK)를 기반으로 클라이언트를 인증하고 WLAN에 대한 액세스를 제공합니다.

1. 성공적인 인증을 확인하려면 ADU Current Status(ADU 현재 상태)를 확인합니다.이 창은 예를 제공합니다.이 창에는 사용되는 암호화가 AES이고 서버 기반 인증이 수행되지 않음을 보여줍니다

.




2. 클라이언트가 WPA 2 PSK 인증 모드로 성공적으로 인증되었는지 확인하려면 AP/bridge 이벤트 로그를 확인합니다

.


## 문제 해결

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

# 관련 정보

- 암호 그룹 및 WEP 구성

- 인증 유형 구성
- WPA 구성 개요
- WPA2 - Wi-Fi 보호 액세스 2
- WPA 혼합 모드 작동이란 무엇이며 AP에서 어떻게 구성합니까?
- 무선 지원 페이지
- 기술 지원 및 문서 – Cisco Systems