ACS 5.2 및 WLC로 PEAP 및 EAP-FAST 구성

목차

소개

이 문서에서는 ACS(Access Control Server) 5.2와 같은 외부 RADIUS 서버를 사용하여 EAP(Extensible Authentication Protocol) 인증을 위해 WLC(Wireless LAN Controller)를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 컨피그레이션을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- WLC 및 LAP(Lightweight Access Point)에 대한 기본 지식 보유
- AAA 서버에 대한 기능적 지식이 있어야 합니다
- 무선 네트워크 및 무선 보안 문제에 대한 철저한 지식 보유

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 펌웨어 릴리스 7.0.220.0을 실행하는 Cisco 5508 WLC
- Cisco 3502 Series LAP
- Intel 6300-N 드라이버 버전 14.3의 Microsoft Windows 7 기본 신청자
- 버전 5.2를 실행하는 Cisco Secure ACS
- Cisco 3560 Series 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 참조하십시오.

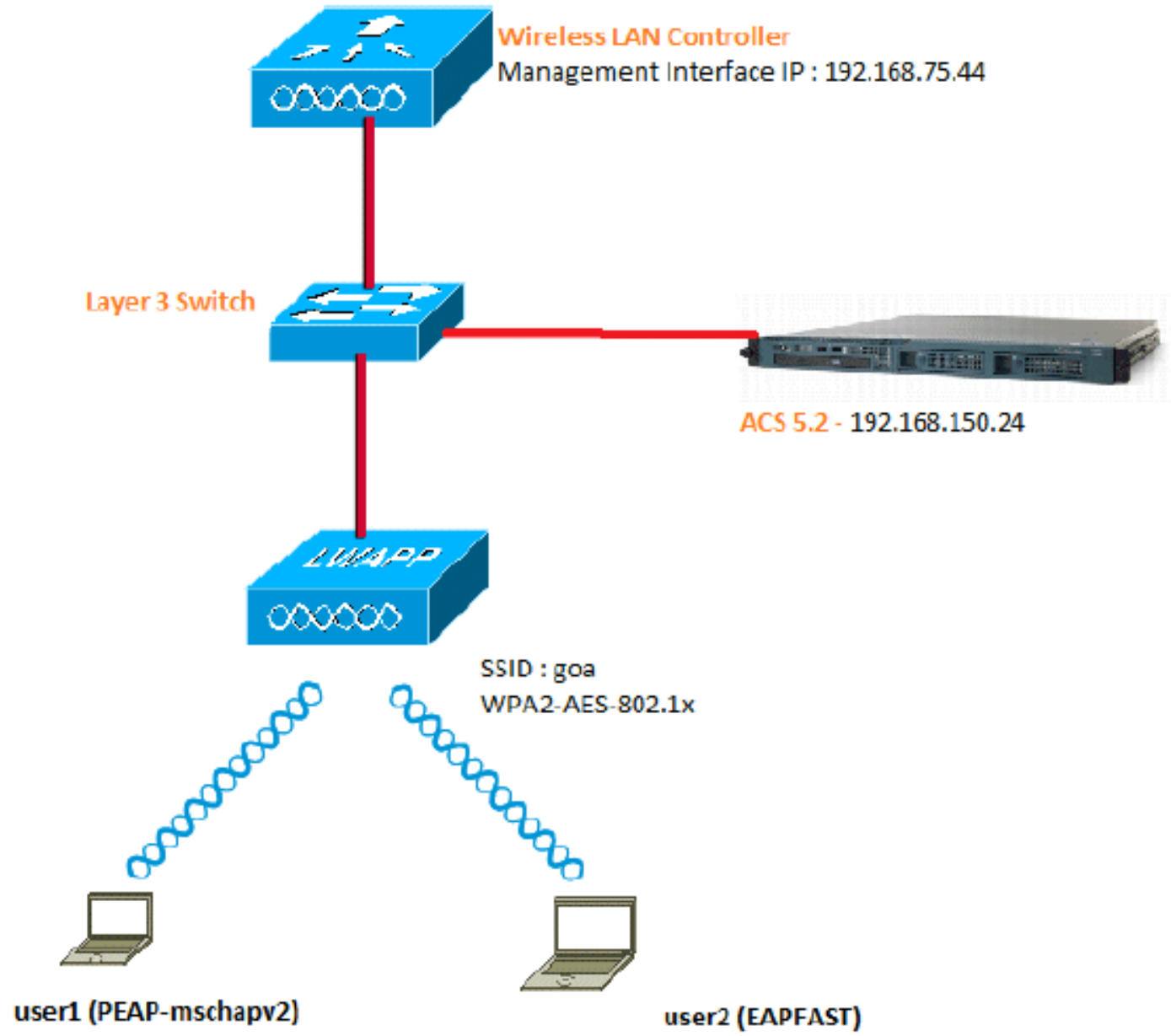
구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

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

네트워크 다이어그램

이 문서에서는 이 네트워크 설정을 사용합니다.



다음은 이 다이어그램에서 사용되는 구성 요소의 컨피그레이션 세부 정보입니다.

- ACS(RADIUS) 서버의 IP 주소는 192.168.150.24입니다.
- WLC의 관리 및 AP 관리자 인터페이스 주소는 192.168.75.44입니다.
- DHCP 서버 주소는 192.168.150.25입니다.
- VLAN 253은 이 컨피그레이션 전체에서 사용됩니다. 두 사용자 모두 동일한 SSID "goa"에 연결됩니다. 그러나 user1은 PEAP-MSCHAPv2를 사용하여 인증하고 user2는 EAP-FAST를 사용하여 인증하도록 구성됩니다.
- 사용자는 VLAN 253에서 할당됩니다.
  - VLAN 253: 192.168.153.x/24. 게이트웨이: 192.168.153.1
  - VLAN 75: 192.168.75.x/24. 게이트웨이: 192.168.75.1

가정

- 스위치는 모든 레이어 3 VLAN에 대해 구성됩니다.
- DHCP 서버에는 DHCP 범위가 할당됩니다.
- 레이어 3 연결은 네트워크의 모든 디바이스 간에 존재합니다.
- LAP가 이미 WLC에 연결되어 있습니다.
- 각 VLAN에는 /24 마스크가 있습니다.
- ACS 5.2에는 자체 서명 인증서가 설치되어 있습니다.

컨피그레이션 단계

이 컨피그레이션은 세 개의 상위 레벨 단계로 구분됩니다.

1. RADIUS 서버를 구성합니다.
2. WLC를 구성합니다.
3. 무선 클라이언트 유틸리티를 구성합니다.

RADIUS 서버 구성

RADIUS 서버 컨피그레이션은 4단계로 나뉩니다.

1. 네트워크 리소스를 구성합니다.
2. 사용자를 구성합니다.
3. 정책 요소를 정의합니다.
4. 액세스 정책을 적용합니다.

ACS 5.x는 정책 기반 액세스 제어 시스템입니다. 즉, ACS 5.x는 4.x 버전에서 사용된 그룹 기반 모델 대신 규칙 기반 정책 모델을 사용합니다.

ACS 5.x 규칙 기반 정책 모델은 이전의 그룹 기반 접근 방식에 비해 더 강력하고 유연한 액세스 제어를 제공합니다.

이전 그룹 기반 모델에서 그룹은 세 가지 유형의 정보를 포함하고 연결하므로 정책을 정의합니다.

- ID 정보 - 이 정보는 AD 또는 LDAP 그룹의 멤버십 또는 내부 ACS 사용자에 대한 정적 할당을 기반으로 할 수 있습니다.
- 기타 제한 또는 조건 - 시간 제한, 장치 제한 등
- 권한 - VLAN 또는 Cisco IOS® 권한 레벨

ACS 5.x 정책 모델은 다음 형식의 규칙을 기반으로 합니다.

- 조건이 충족되면

예를 들어, 그룹 기반 모델에 대해 설명된 정보를 사용합니다.

- ID-condition, restriction-condition, authorization-profile이 있는 경우

따라서 사용자가 네트워크에 액세스할 수 있는 조건은 물론 특정 조건이 충족될 때 허용되는 권한 부여 수준도 제한할 수 있는 유연성을 제공합니다.

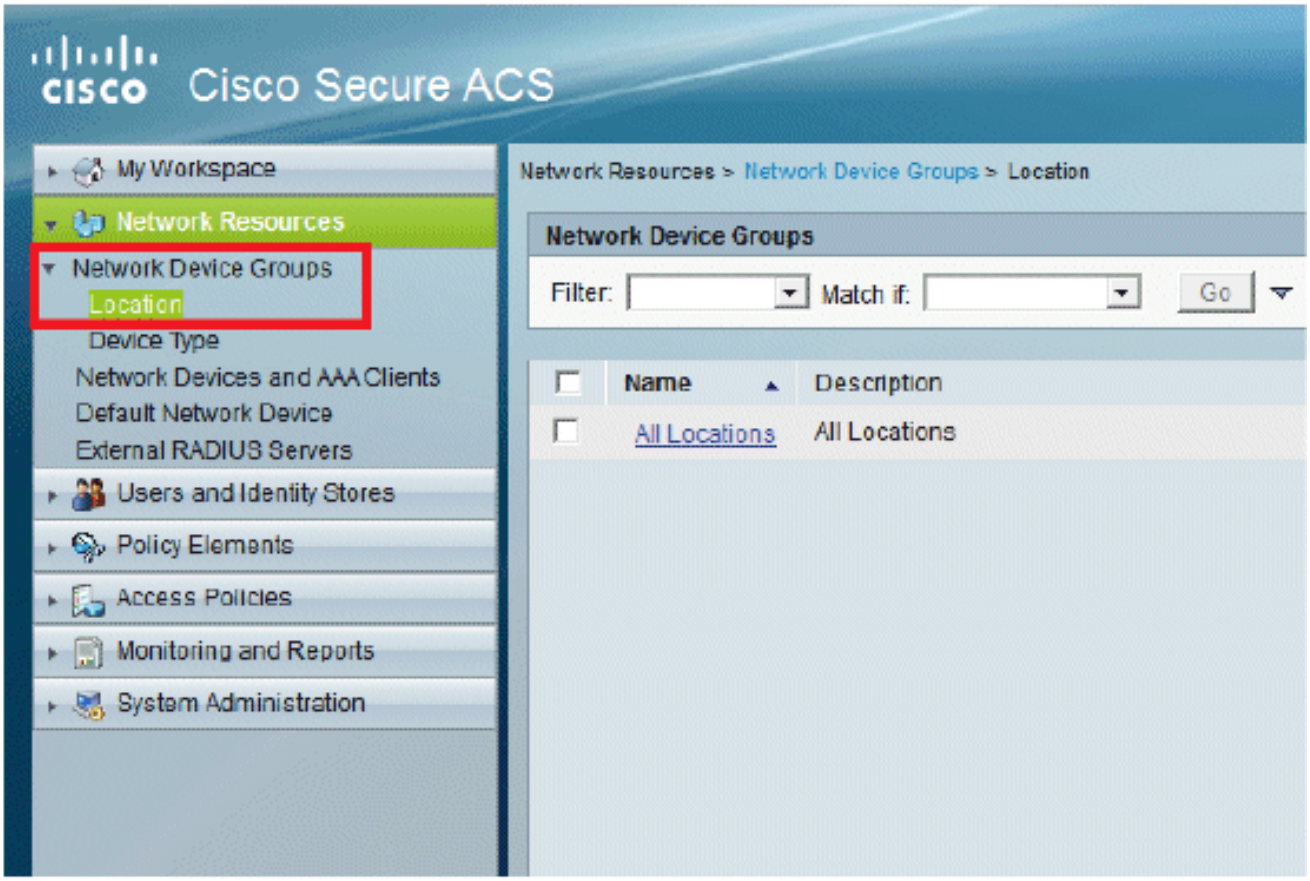
네트워크 리소스 구성

이 섹션에서는 RADIUS 서버의 WLC에 대해 AAA 클라이언트를 구성합니다.

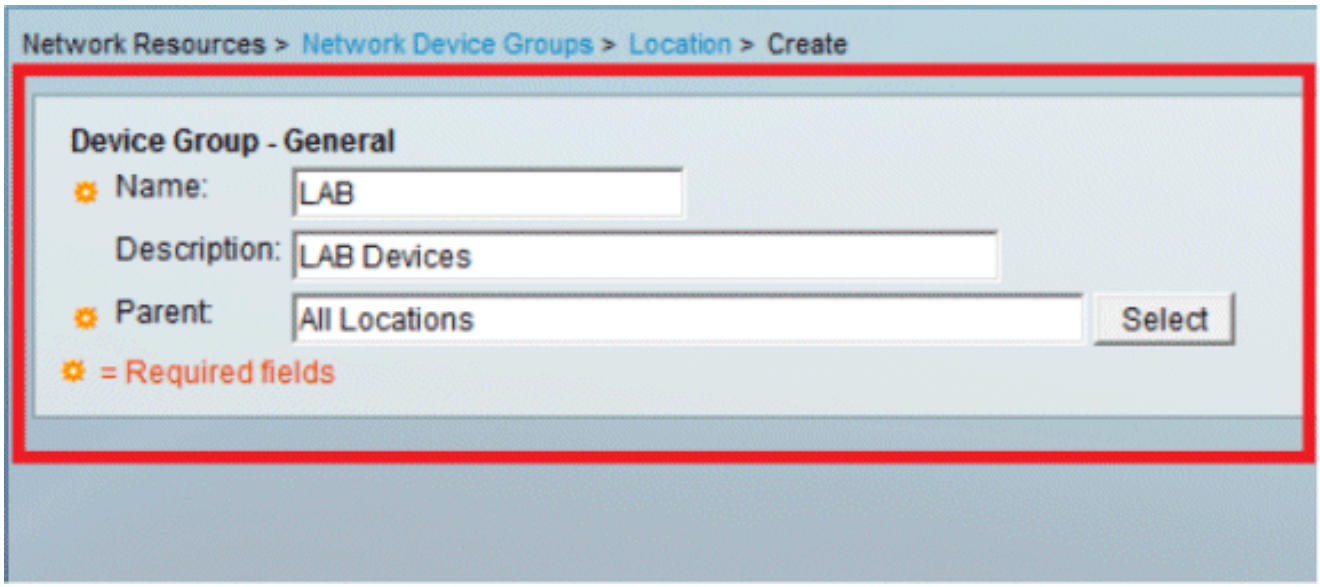
이 절차에서는 WLC가 사용자 자격 증명을 RADIUS 서버에 전달할 수 있도록 WLC를 RADIUS 서버에 AAA 클라이언트로 추가하는 방법에 대해 설명합니다.

다음 단계를 완료하십시오.

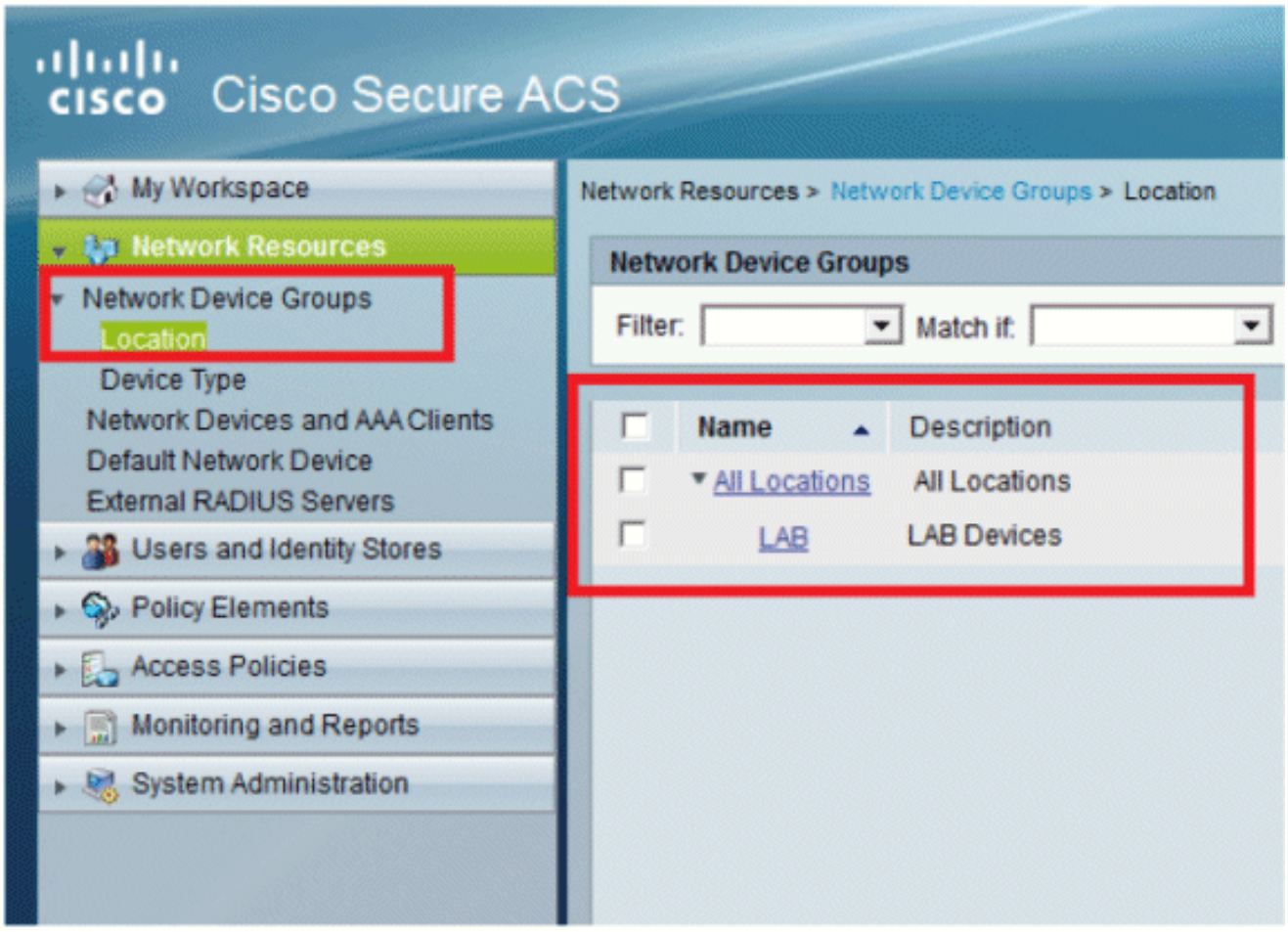
1. ACS GUI에서 Network Resources(네트워크 리소스) > Network Device Groups(네트워크 디바이스 그룹) > Location(위치)으로 이동하여 Create(생성)를 클릭합니다(맨 아래).



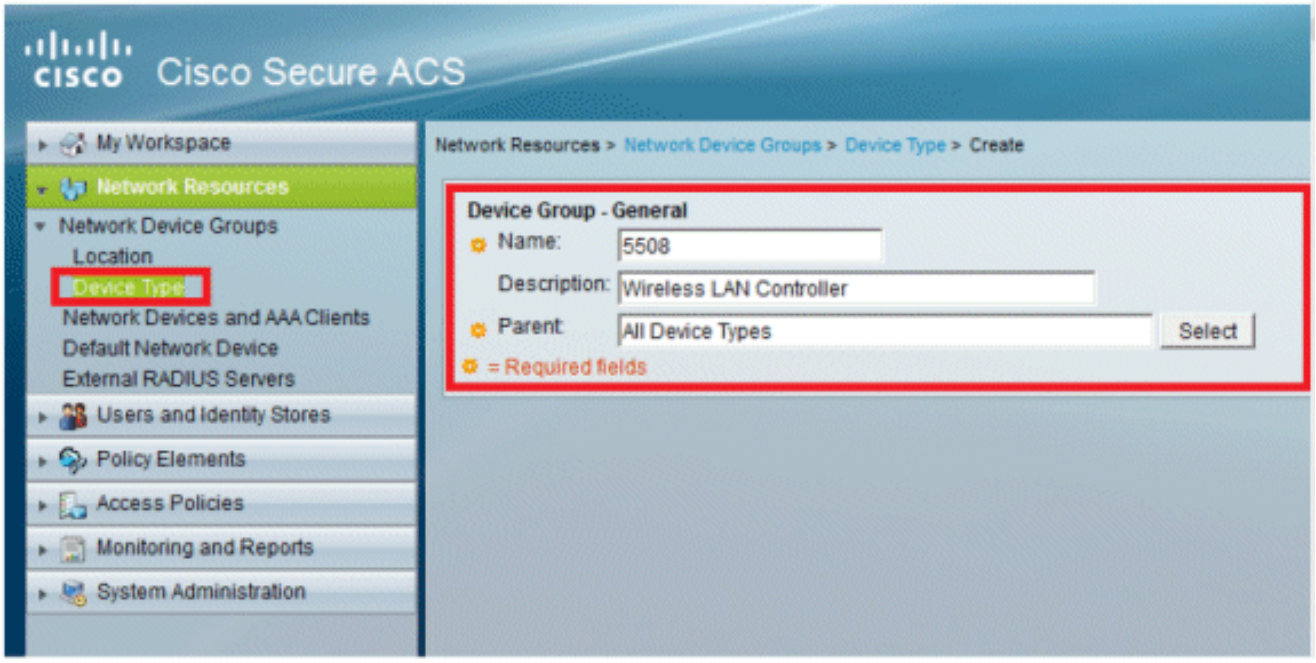
2. 필수 필드를 추가하고 Submit(제출)을 클릭합니다.



이제 다음 화면을 볼 수 있습니다.



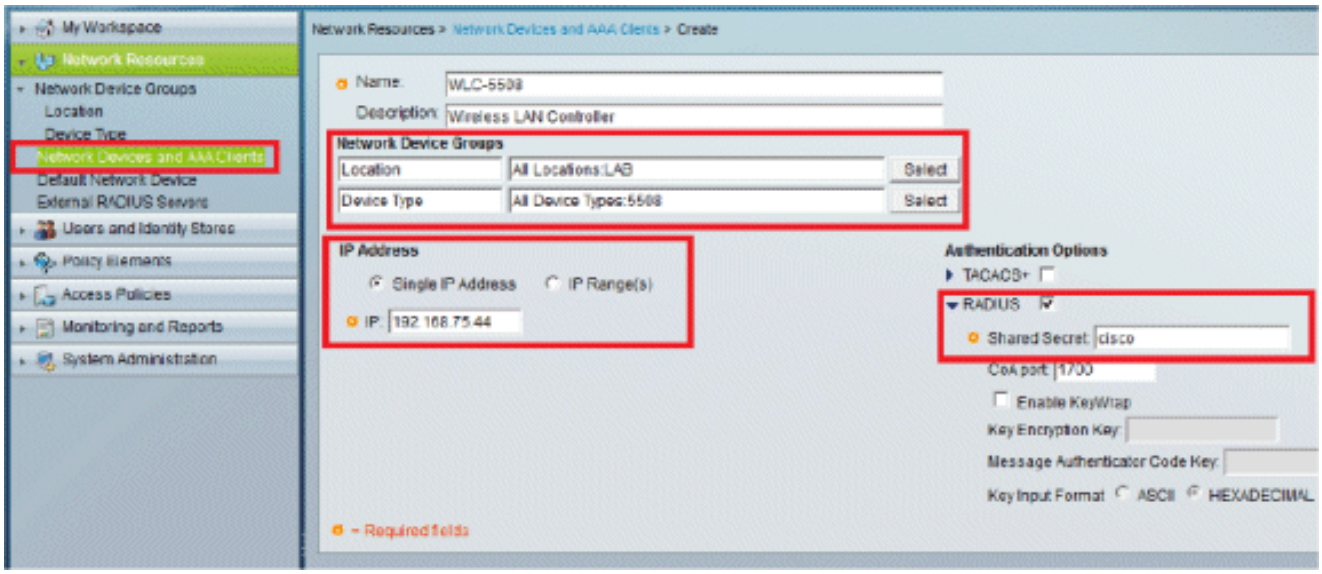
3. Device Type(디바이스 유형) > Create(생성)를 클릭합니다.



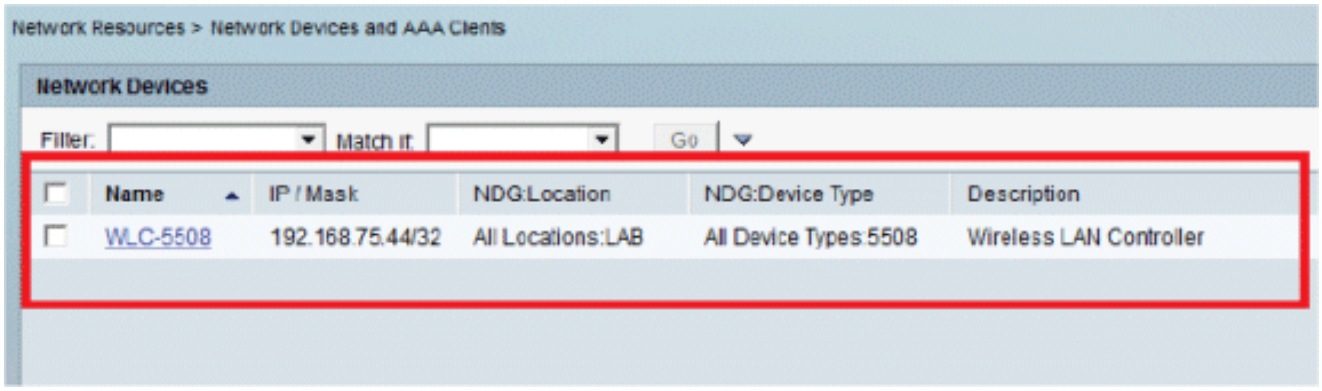
4. Submit(제출)을 클릭합니다. 이제 다음 화면을 볼 수 있습니다.

5. Network Resources(네트워크 리소스) > Network Devices and AAA Clients(네트워크 디바이스 및 AAA 클라이언트)로 이동합니다.

6. Create(생성)를 클릭하고 여기에 표시된 대로 세부 정보를 입력합니다.



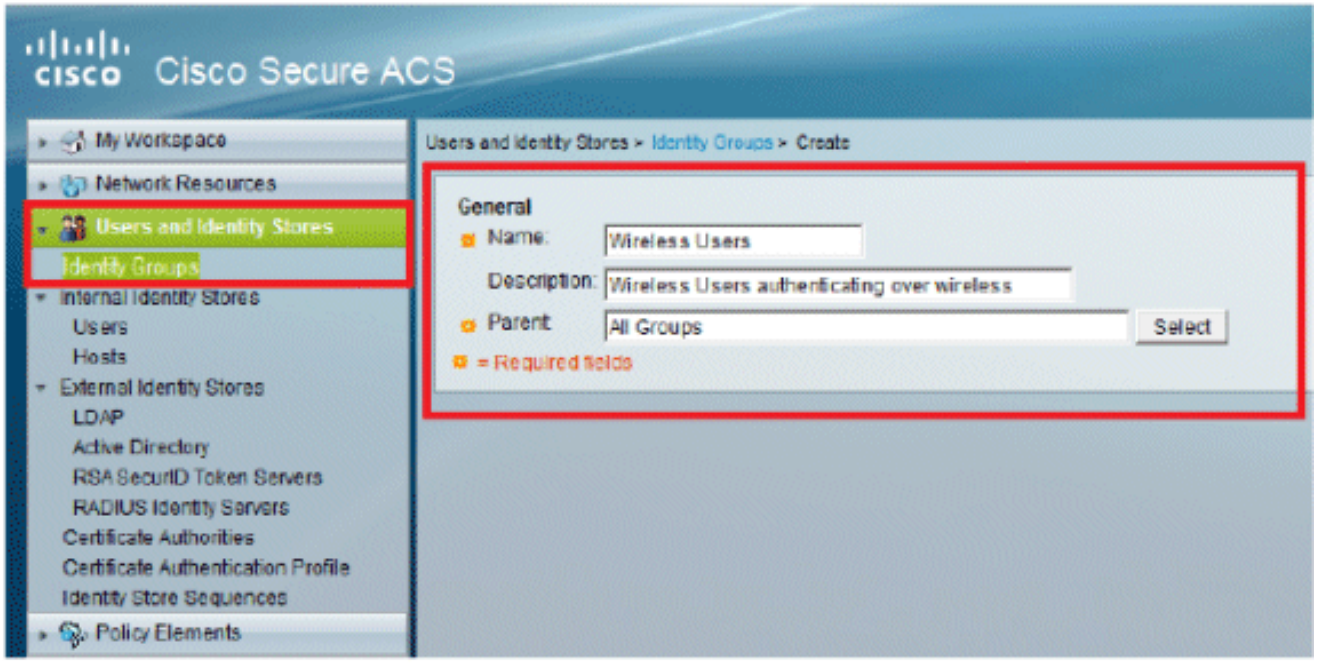
7. Submit(제출)을 클릭합니다. 이제 다음 화면을 볼 수 있습니다.



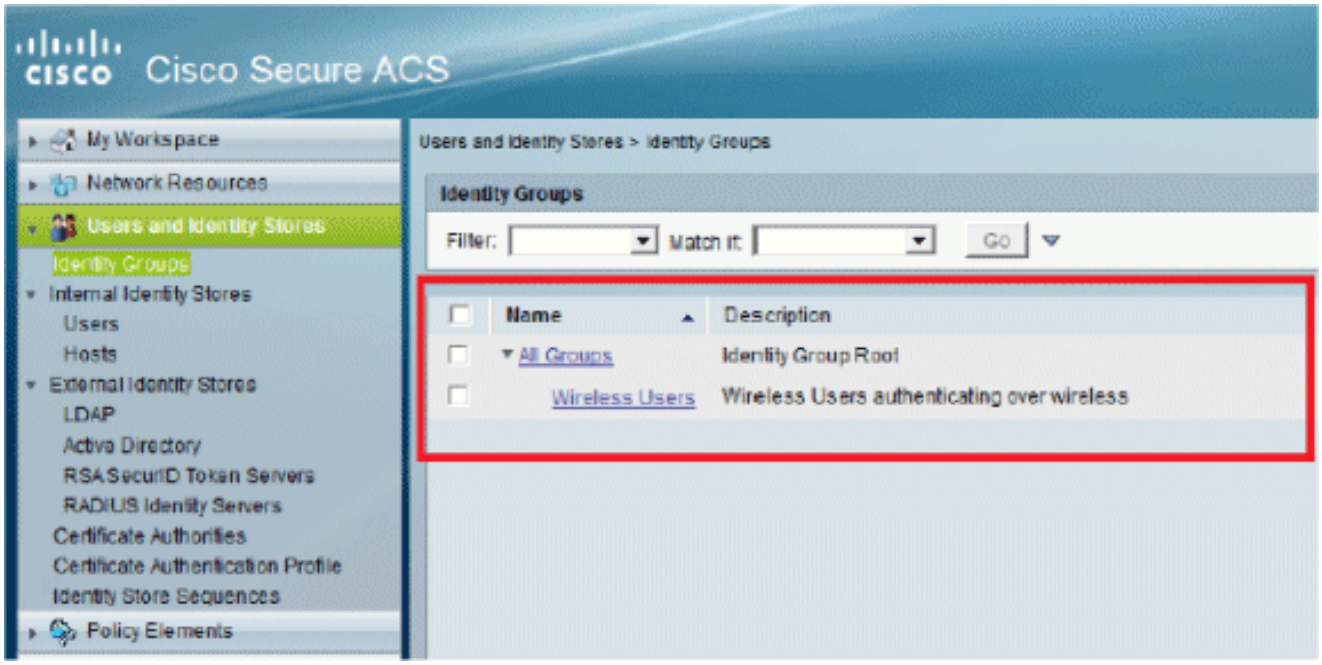
사용자 구성

이 섹션에서는 ACS에서 로컬 사용자를 생성합니다. 두 사용자(user1 및 user2)는 모두 "무선 사용자"라는 그룹에 할당됩니다.

1. Users and Identity Stores(사용자 및 ID 저장소) > Identity Groups(ID 그룹) > Create(생성)로 이동합니다.

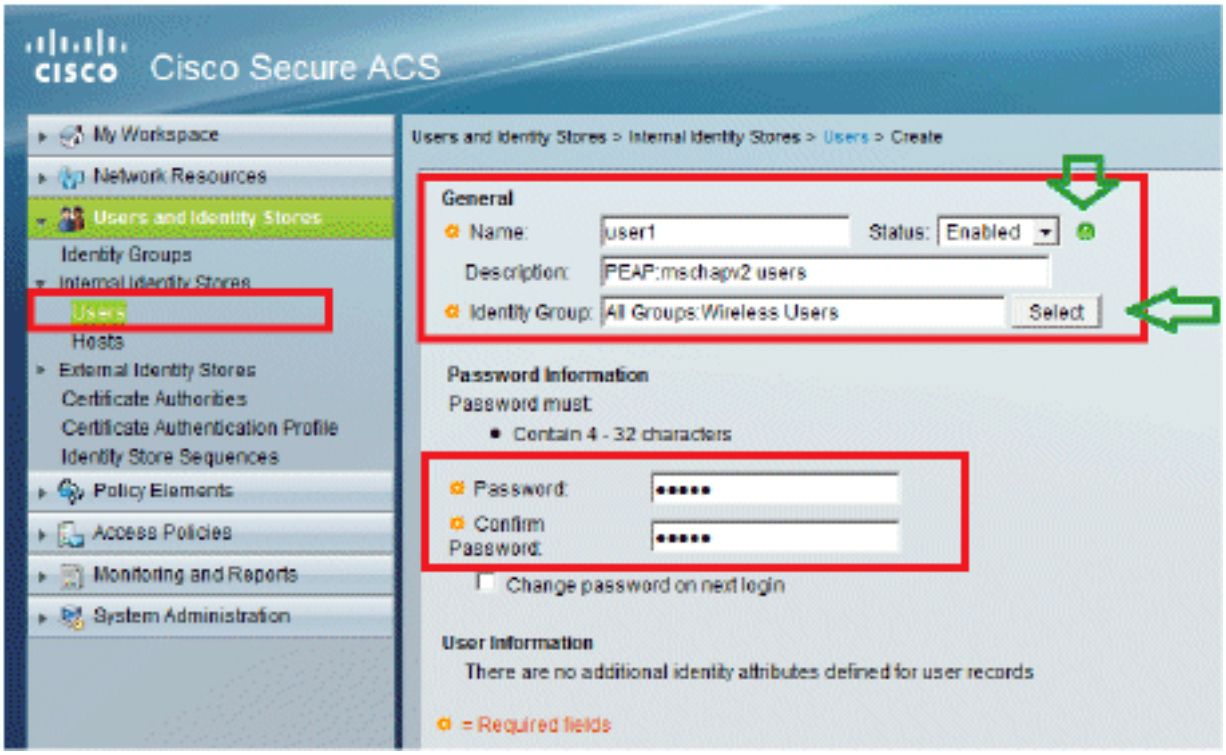


2. Submit(제출)을 클릭하면 페이지가 다음과 같이 표시됩니다.

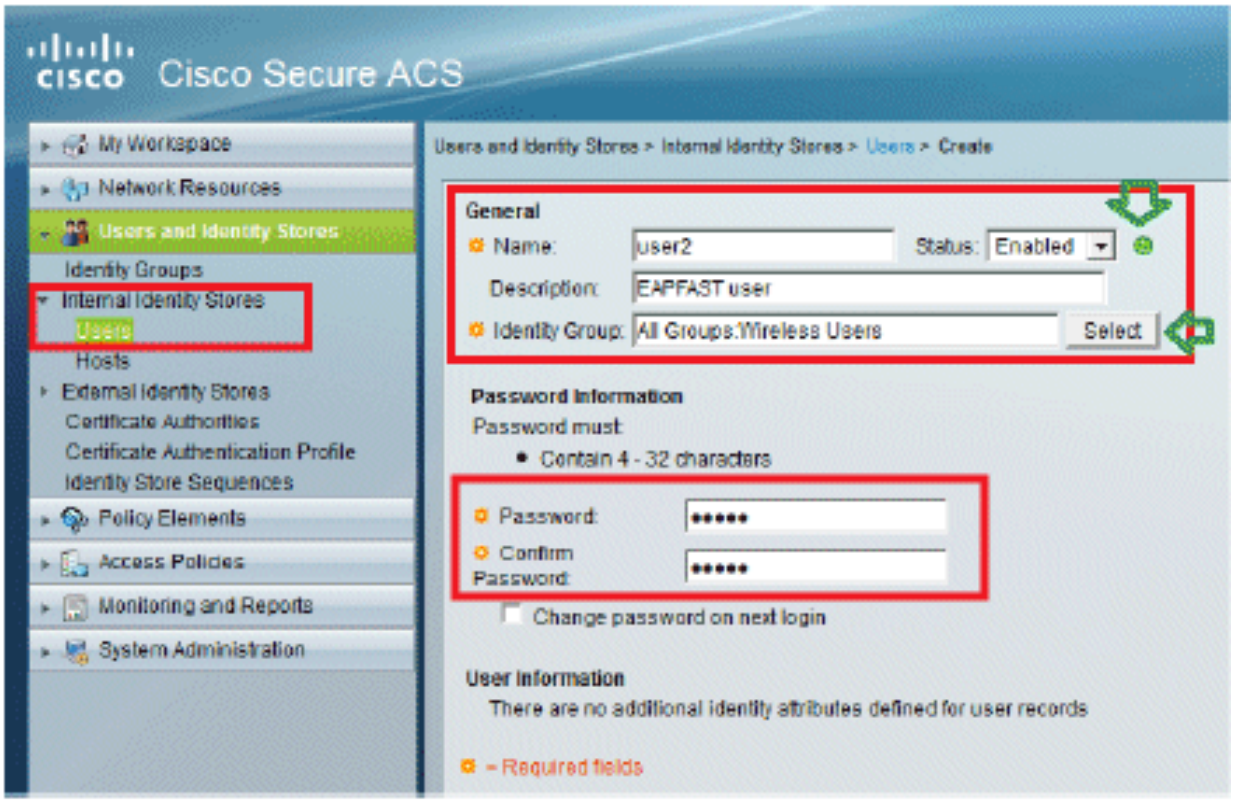


3. 사용자 user1 및 user2를 생성하고 "Wireless Users" 그룹에 할당합니다.

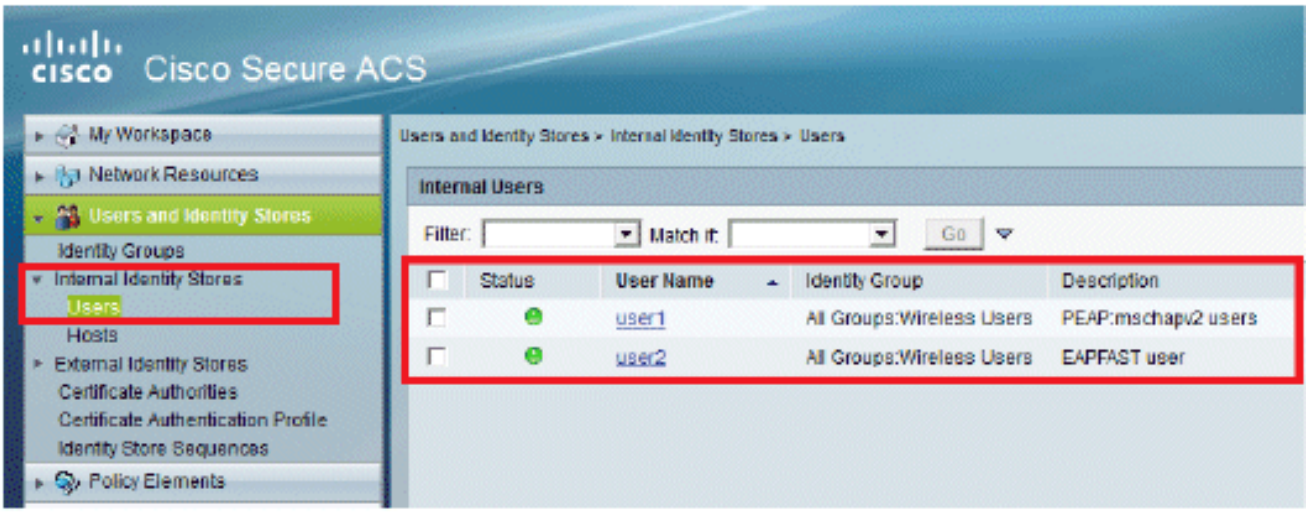
   a. Users and Identity Stores(사용자 및 ID 저장소) > Identity Groups(ID 그룹) > Users(사용자) > Create(생성)를 클릭합니다.



b. 마찬가지로 user2를 생성합니다.

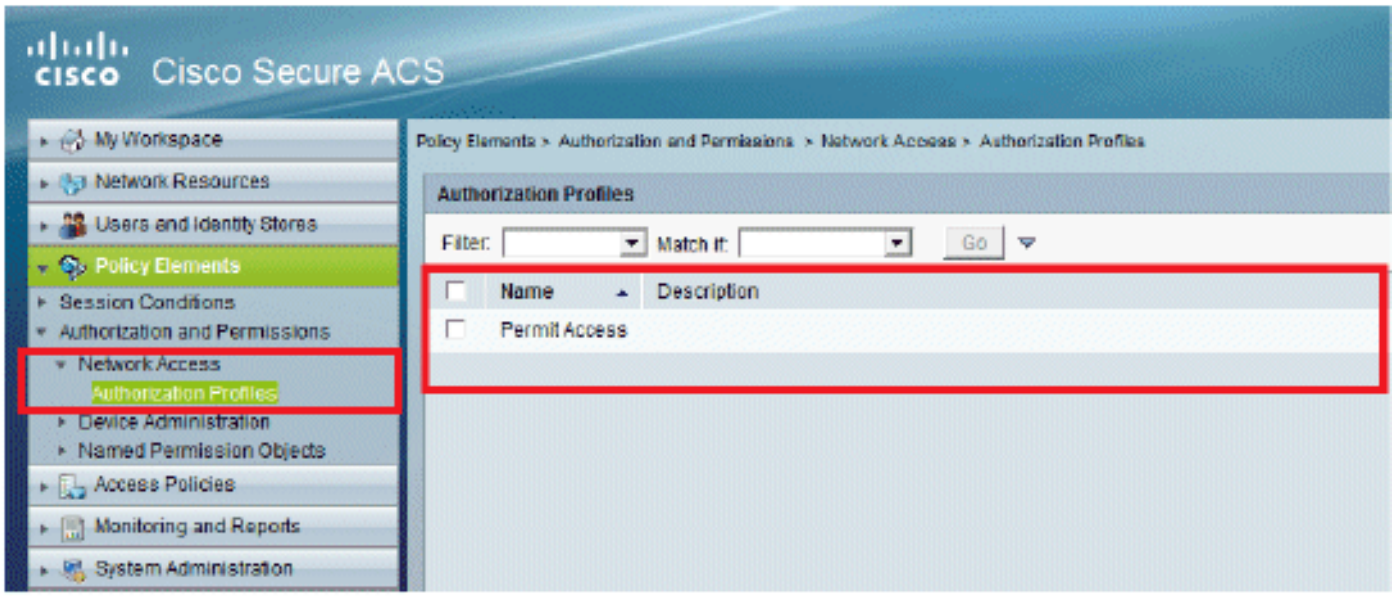


화면은 다음과 같습니다.



정책 요소 정의

Permit Access(액세스 허용)가 설정되어 있는지 확인합니다.

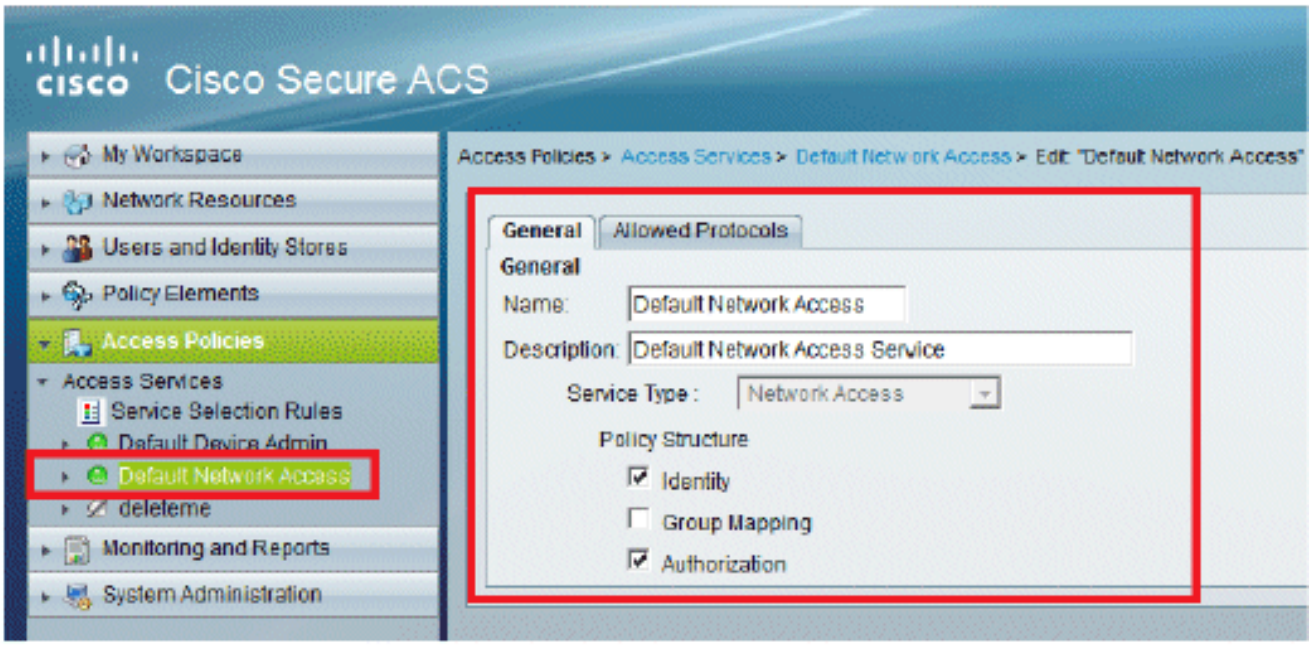


액세스 정책 적용

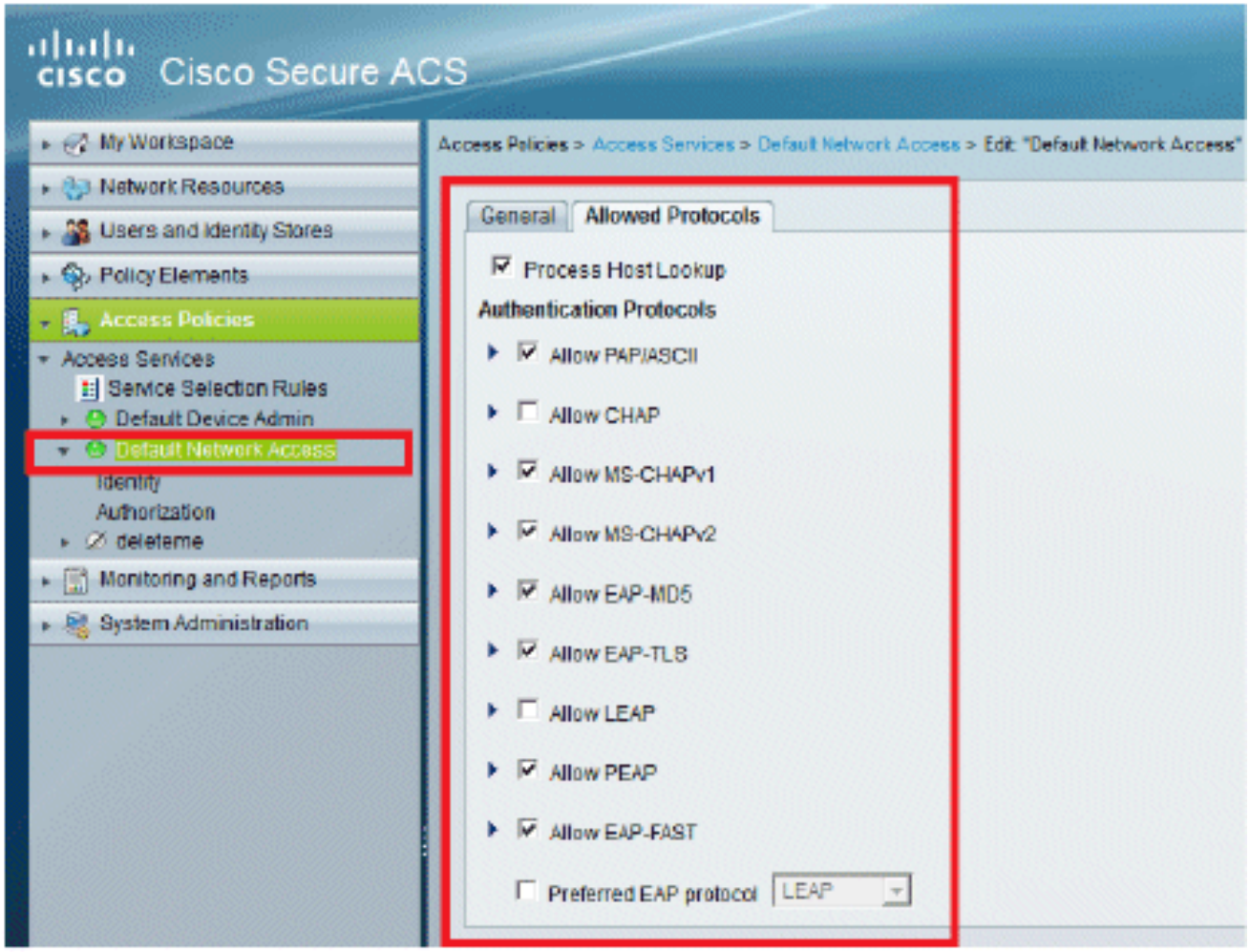
이 섹션에서는 사용할 인증 방법과 규칙을 구성하는 방법을 선택하겠습니다. 이전 단계를 기반으로 규칙을 생성합니다.

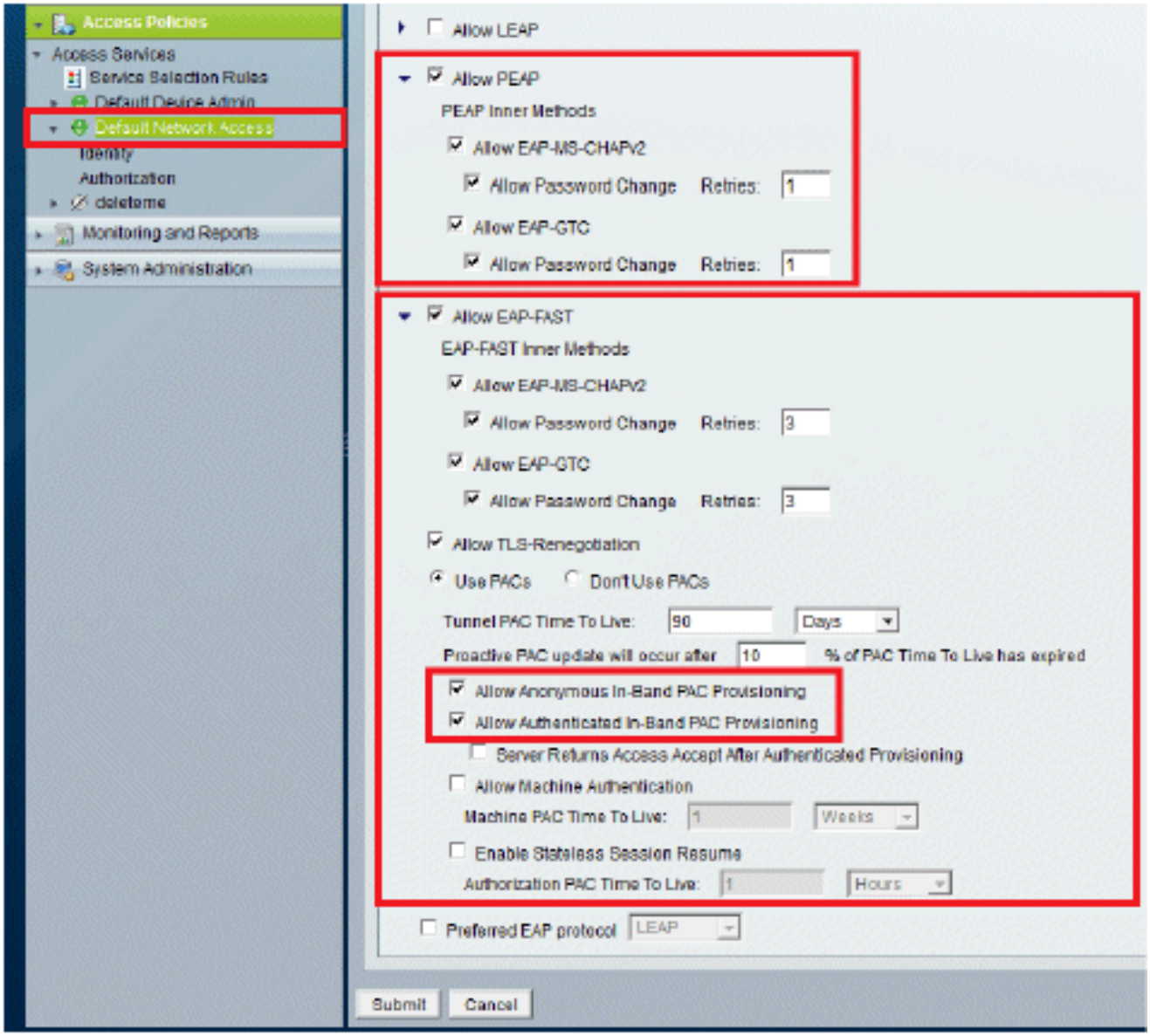
다음 단계를 완료하십시오.

1. Access Policies(액세스 정책) > Access Services(액세스 서비스) > Default Network Access(기본 네트워크 액세스) > Edit: "Default Network Access(기본 네트워크 액세스)"로 이동합니다.



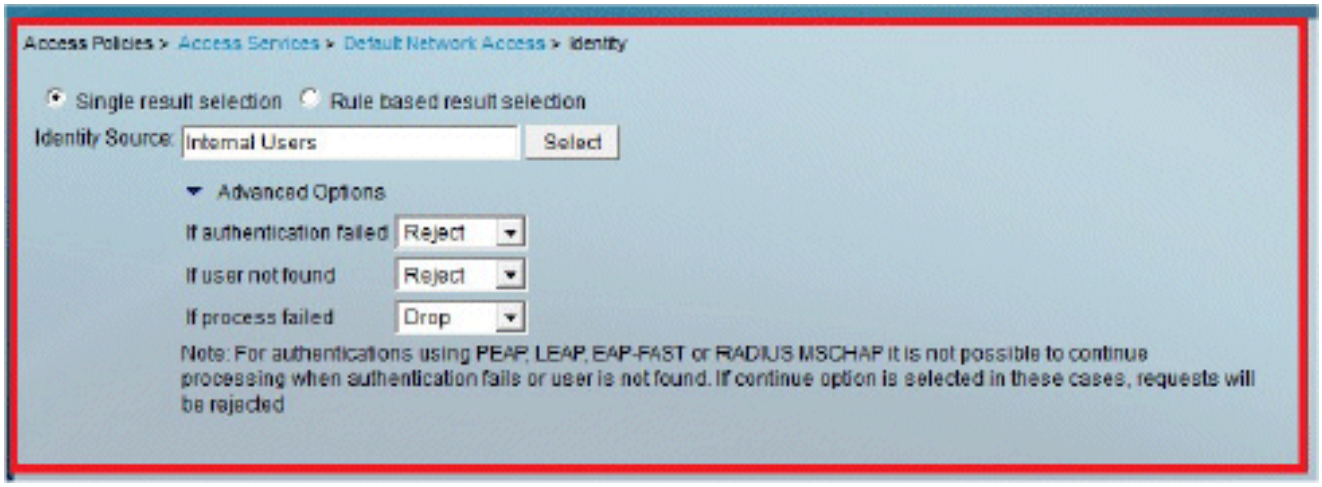
2. 무선 클라이언트에서 인증할 EAP 방법을 선택합니다. 이 예에서는 PEAP- MSCHAPv2 및 EAP-FAST를 사용합니다.





3. Submit(제출)을 클릭합니다.

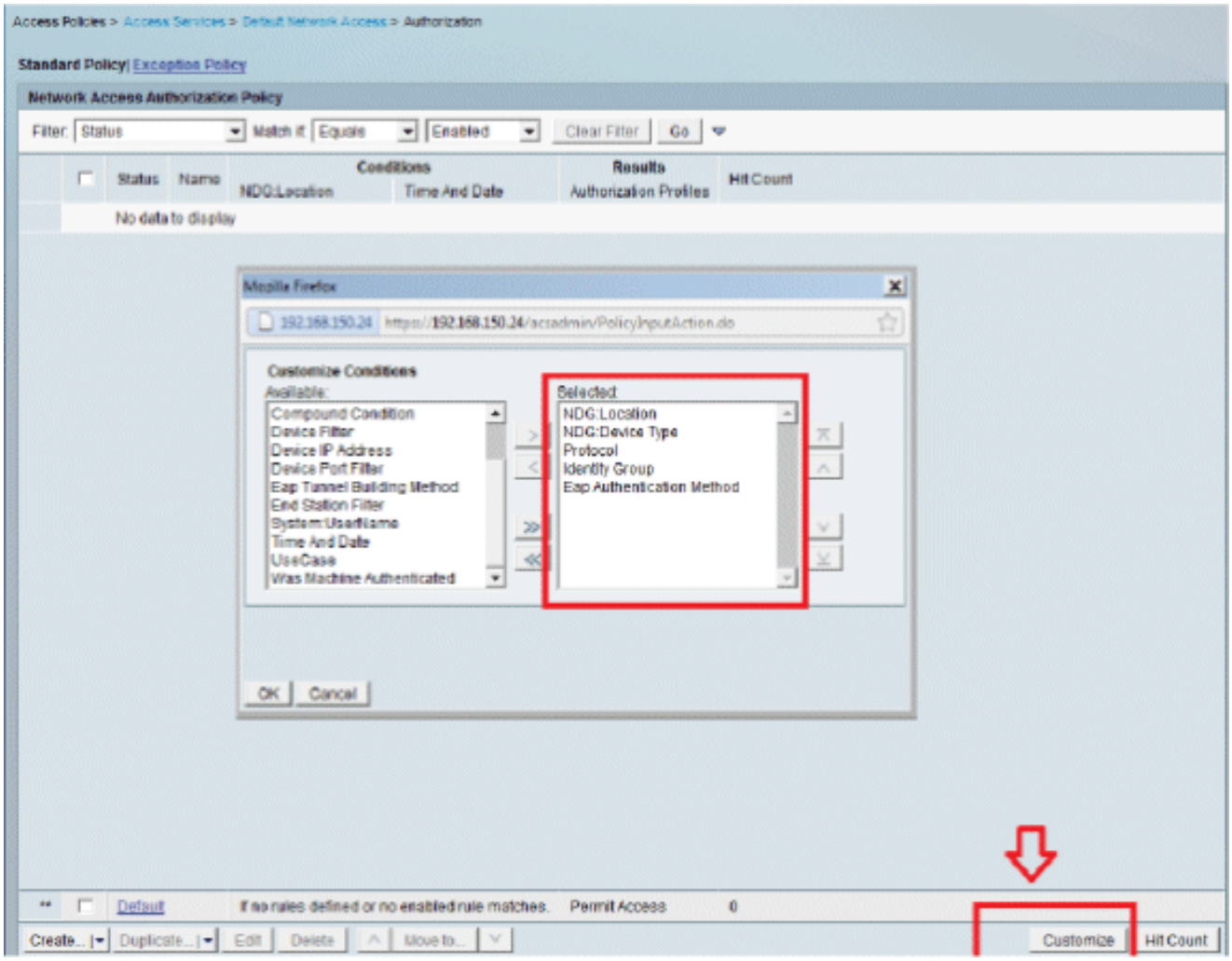
4. 선택한 ID 그룹을 확인합니다. 이 예에서는 ACS에서 생성한 Internal Users를 사용합니다. 변경 사항을 저장합니다.



5. 권한 부여 프로파일을 확인하려면 Access Policies(액세스 정책) > Access Services(액세스 서

비스) > Default Network Access(기본 네트워크 액세스) > Authorization(권한 부여)으로 이동합니다.

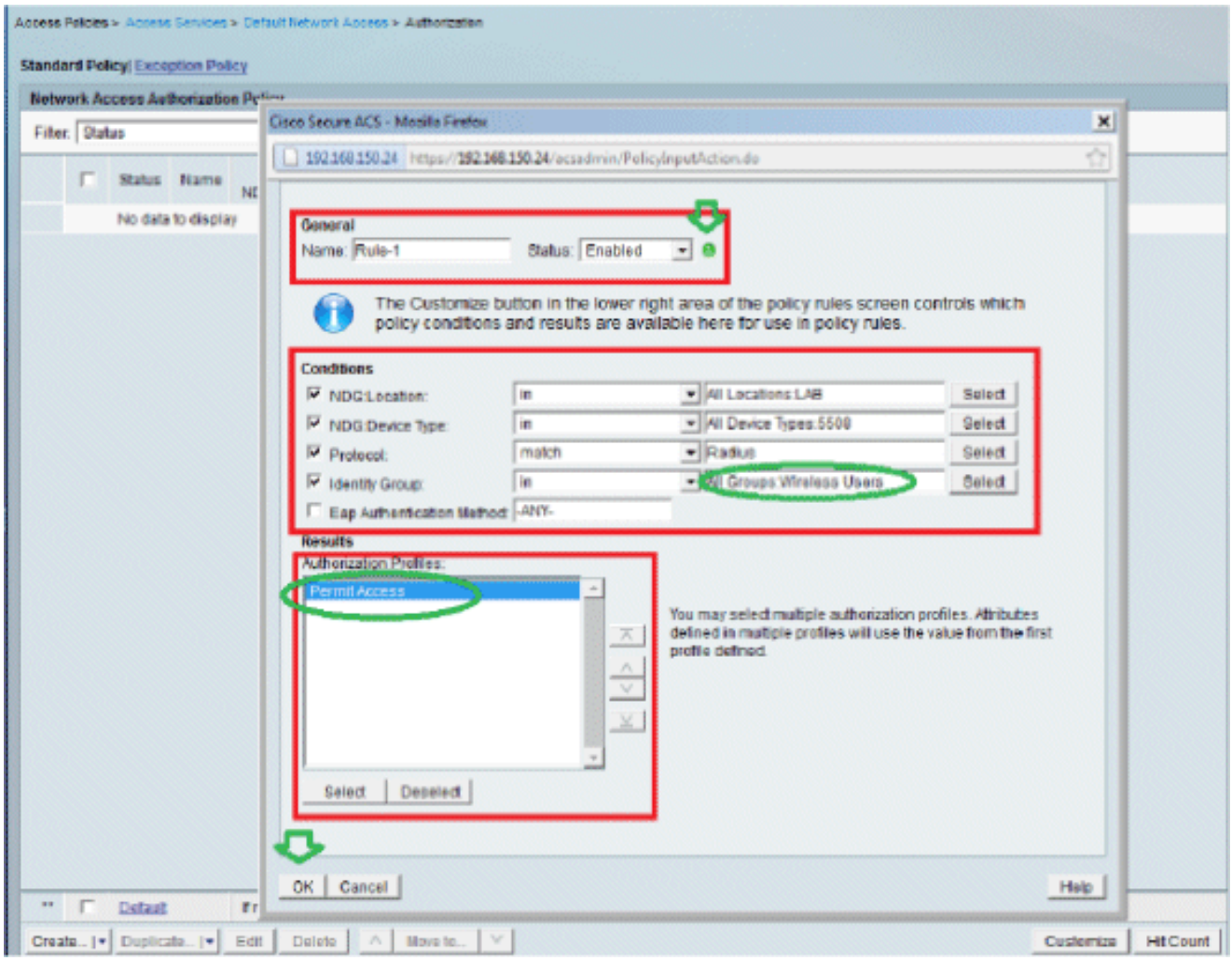
네트워크에 대한 사용자 액세스를 허용할 조건 및 인증 후 전달 할 인증 프로파일 (특성) 하에서 사용자 정의 할 수 있습니다. 이 세분화는 ACS 5.x에서만 사용할 수 있습니다. 이 예에서는 Location, Device Type, Protocol, Identity Group, EAP Authentication Method를 선택했습니다 (예:



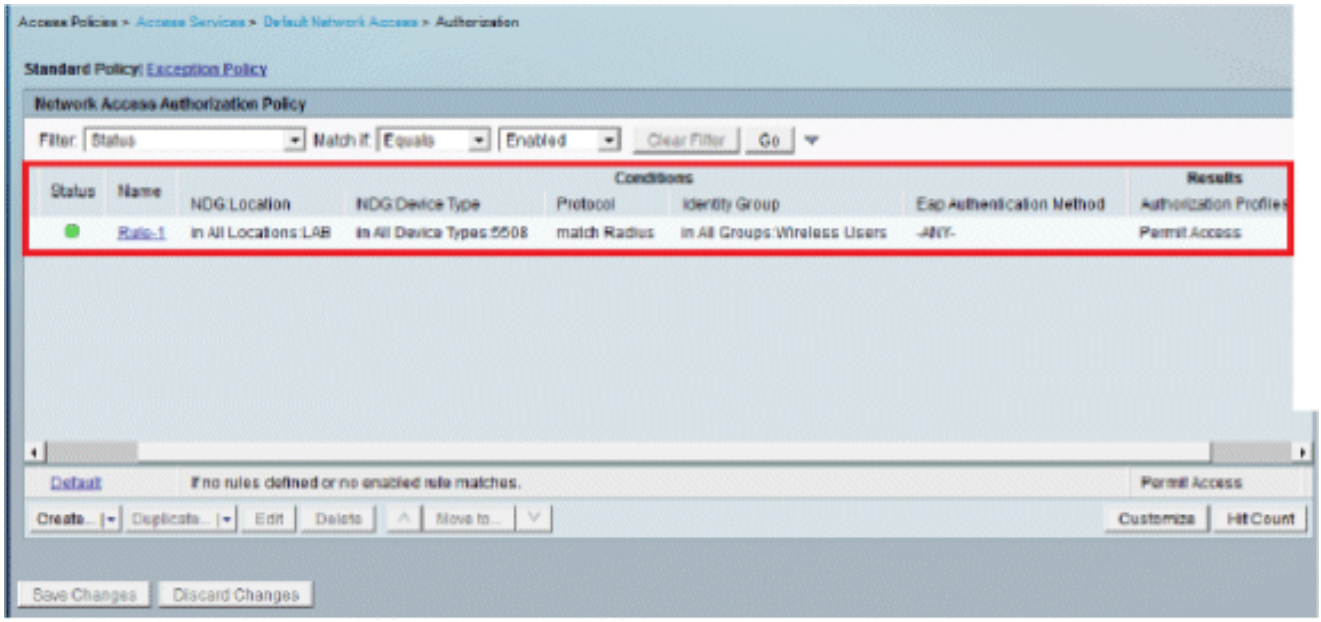
6. OK(확인)를 클릭하고 Save Changes(변경 사항 저장)를 클릭합니다.

7. 다음 단계는 규칙을 생성하는 것입니다. 정의된 규칙이 없는 경우 클라이언트는 조건 없이 액세스가 허용됩니다.

   Create(생성) > Rule-1을 클릭합니다. 이 규칙은 "무선 사용자" 그룹의 사용자를 위한 것입니다.



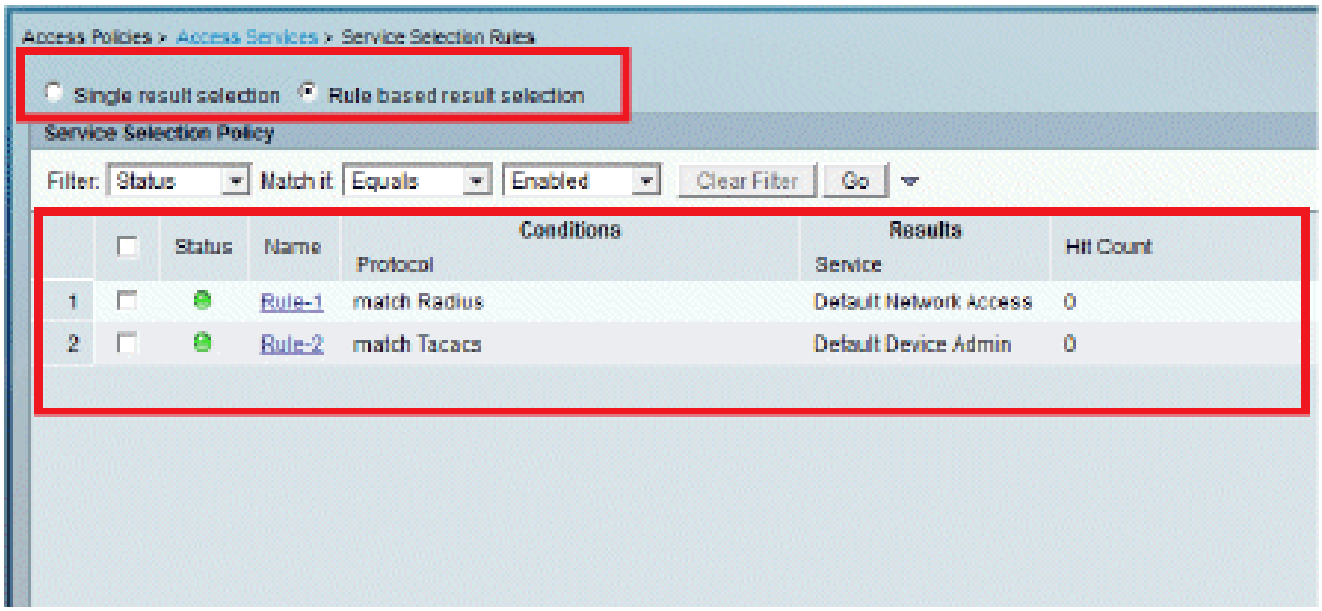
8. 변경 사항을 저장합니다. 화면은 다음과 같습니다.



조건과 일치하지 않는 사용자를 거부하도록 하려면 기본 규칙을 편집하여 "액세스 거부"라고 말합니다.

9. 이제 서비스 선택 규칙을 정의하겠습니다. 수신 요청에 적용할 서비스를 결정하는 단순 또는

규칙 기반 정책을 구성하려면 이 페이지를 사용합니다. 이 예에서는 규칙 기반 정책이 사용됩니다.



WLC 구성

이 컨피그레이션에는 다음 단계가 필요합니다.

1. 인증 서버의 세부 정보를 사용하여 WLC를 구성합니다.
2. VLAN(Dynamic Interface)을 구성합니다.
3. WLAN(SSID)을 구성합니다.

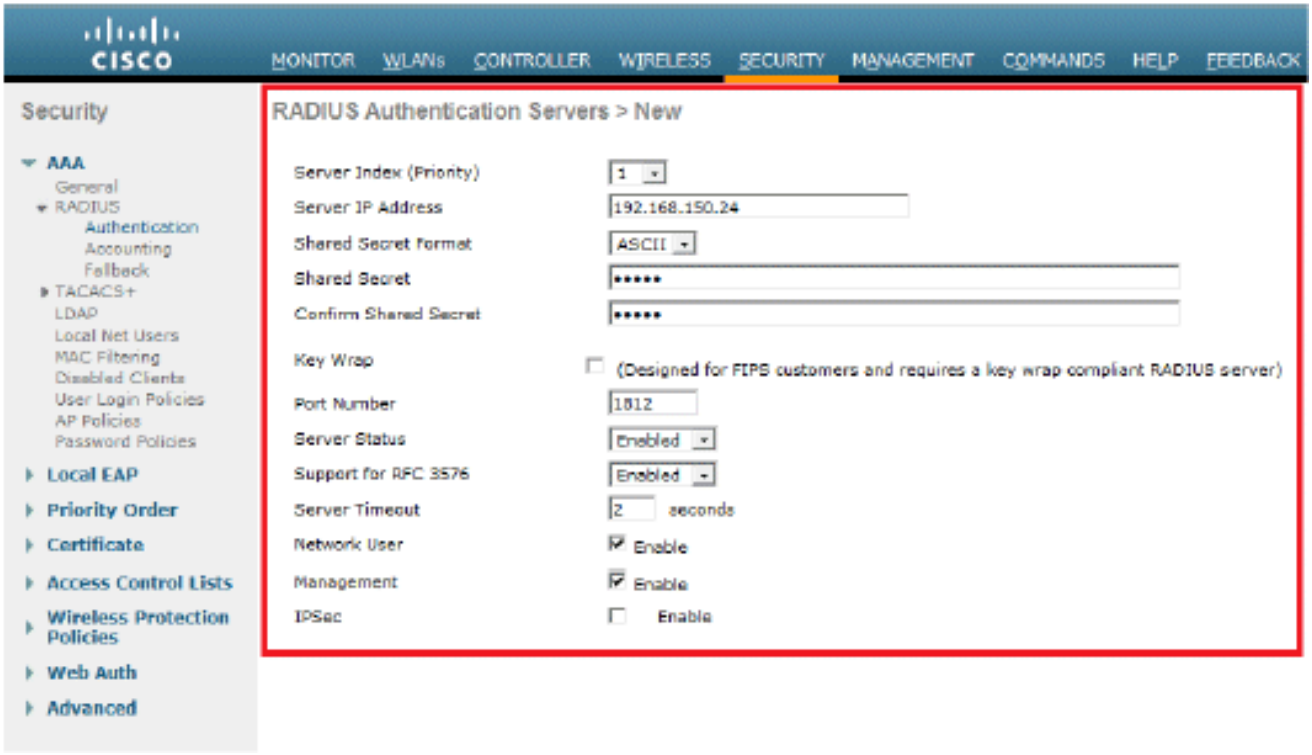
인증 서버의 세부 정보를 사용하여 WLC 구성

클라이언트를 인증하기 위해 RADIUS 서버와 통신할 수 있도록 WLC를 구성하고 다른 트랜잭션에도 구성해야 합니다.

다음 단계를 완료하십시오.

1. 컨트롤러 GUI에서 Security(보안)를 클릭합니다.
2. RADIUS 서버의 IP 주소 및 RADIUS 서버와 WLC 간에 사용되는 공유 암호 키를 입력합니다.

   이 공유 암호 키는 RADIUS 서버에 구성된 것과 동일해야 합니다.

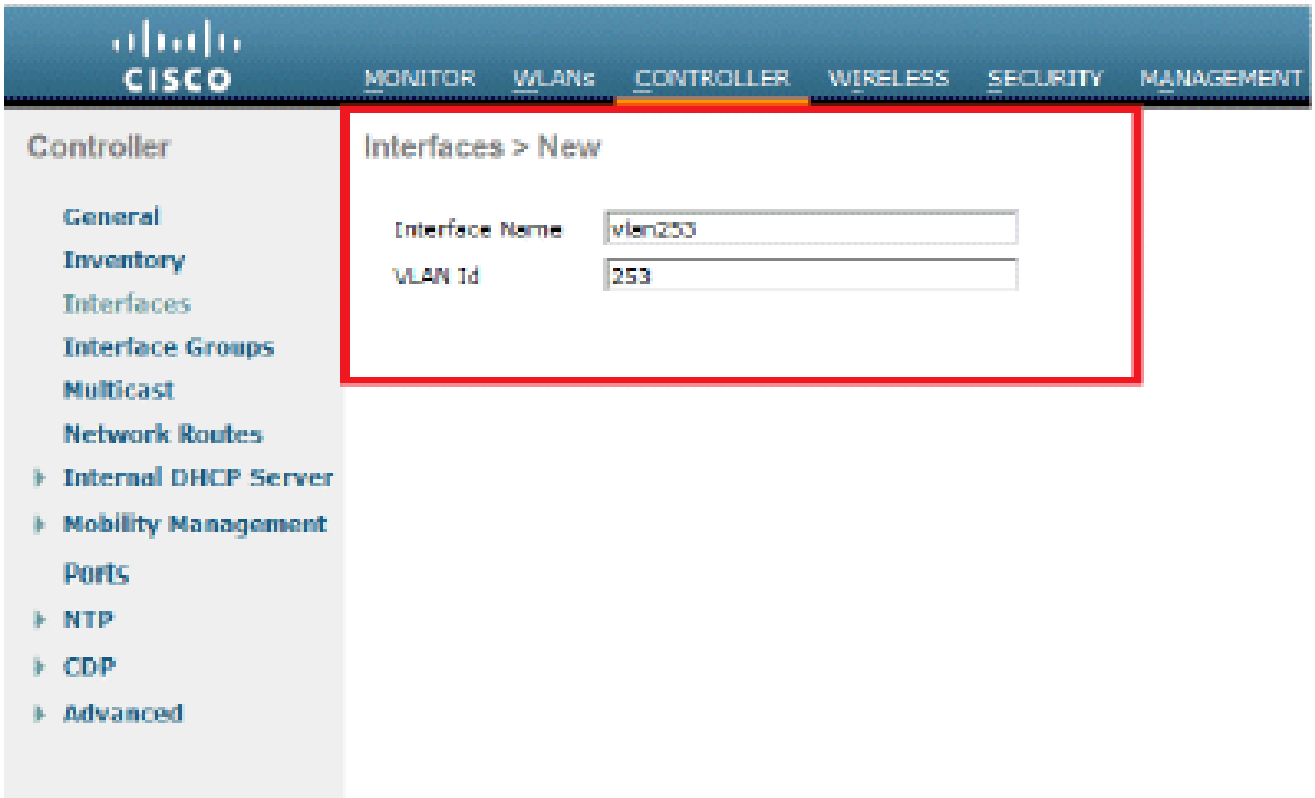


VLAN(Dynamic Interface) 구성

이 절차에서는 WLC에서 동적 인터페이스를 구성하는 방법에 대해 설명합니다.

다음 단계를 완료하십시오.

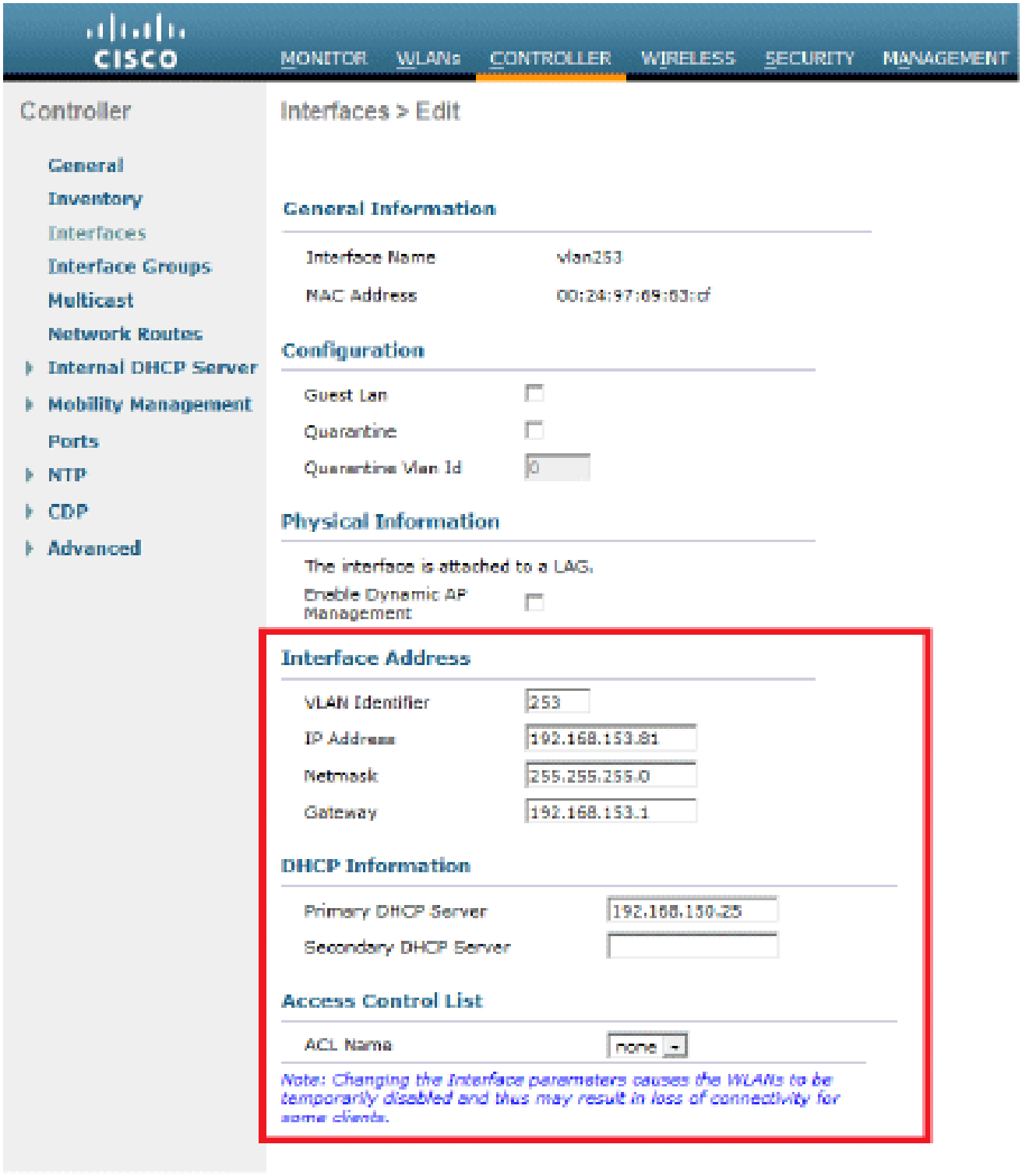
1. 동적 인터페이스는 컨트롤러 GUI의 Controller(컨트롤러) > Interfaces(인터페이스) 창에서 구성합니다.



2. 적용을 클릭합니다.

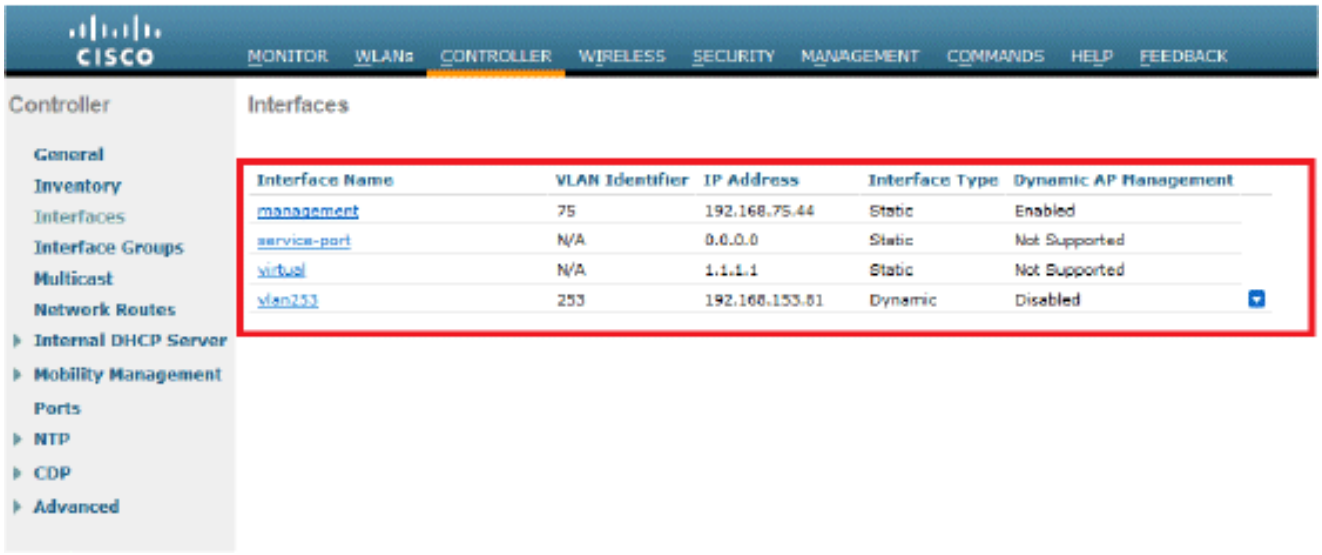
그러면 이 동적 인터페이스의 Edit(수정) 창(여기서는 VLAN 253)으로 이동합니다.

3. 이 동적 인터페이스의 IP 주소 및 기본 게이트웨이를 입력합니다.



4. 적용을 클릭합니다.

5. 구성된 인터페이스는 다음과 같습니다.



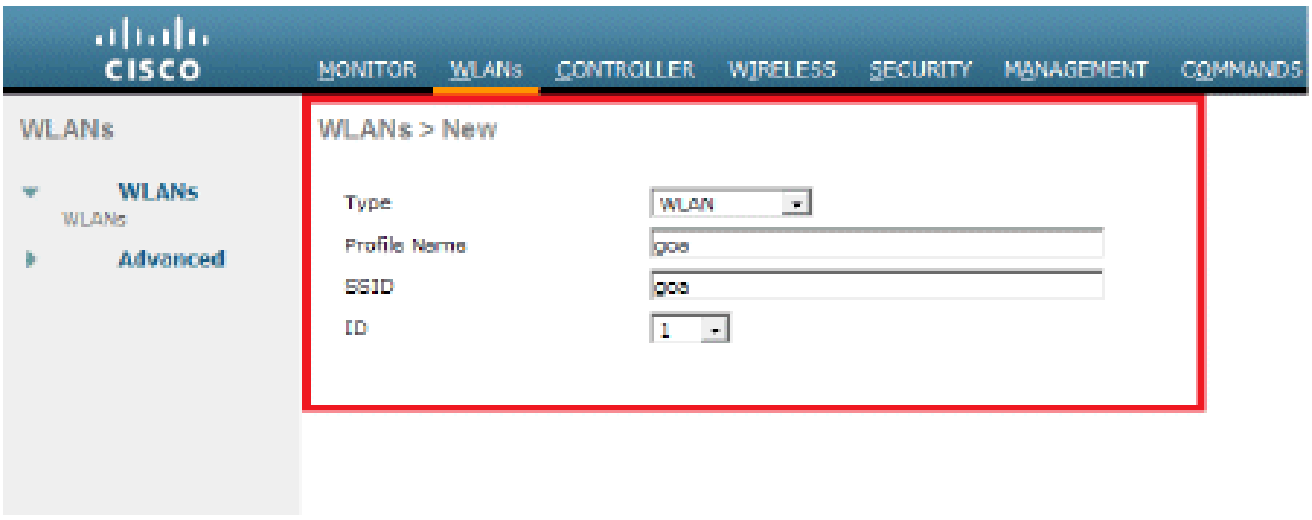
WLAN(SSID) 구성

이 절차에서는 WLC에서 WLAN을 구성하는 방법에 대해 설명합니다.

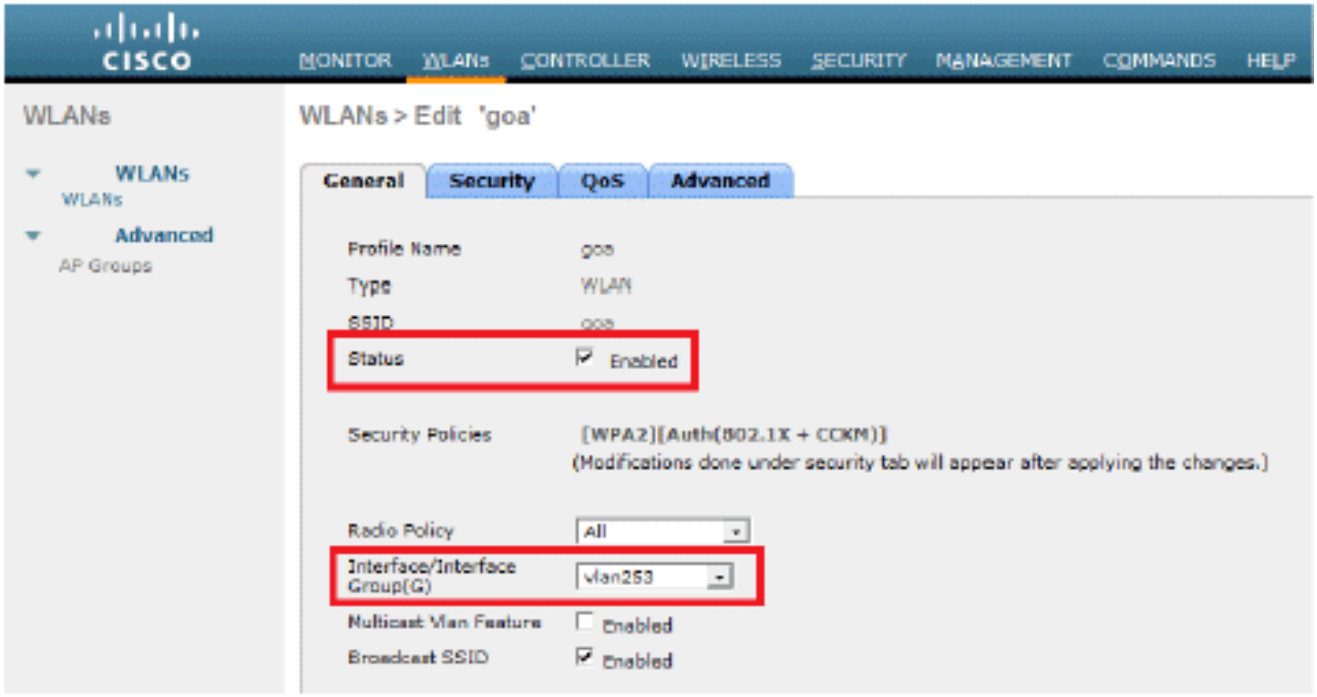
다음 단계를 완료하십시오.

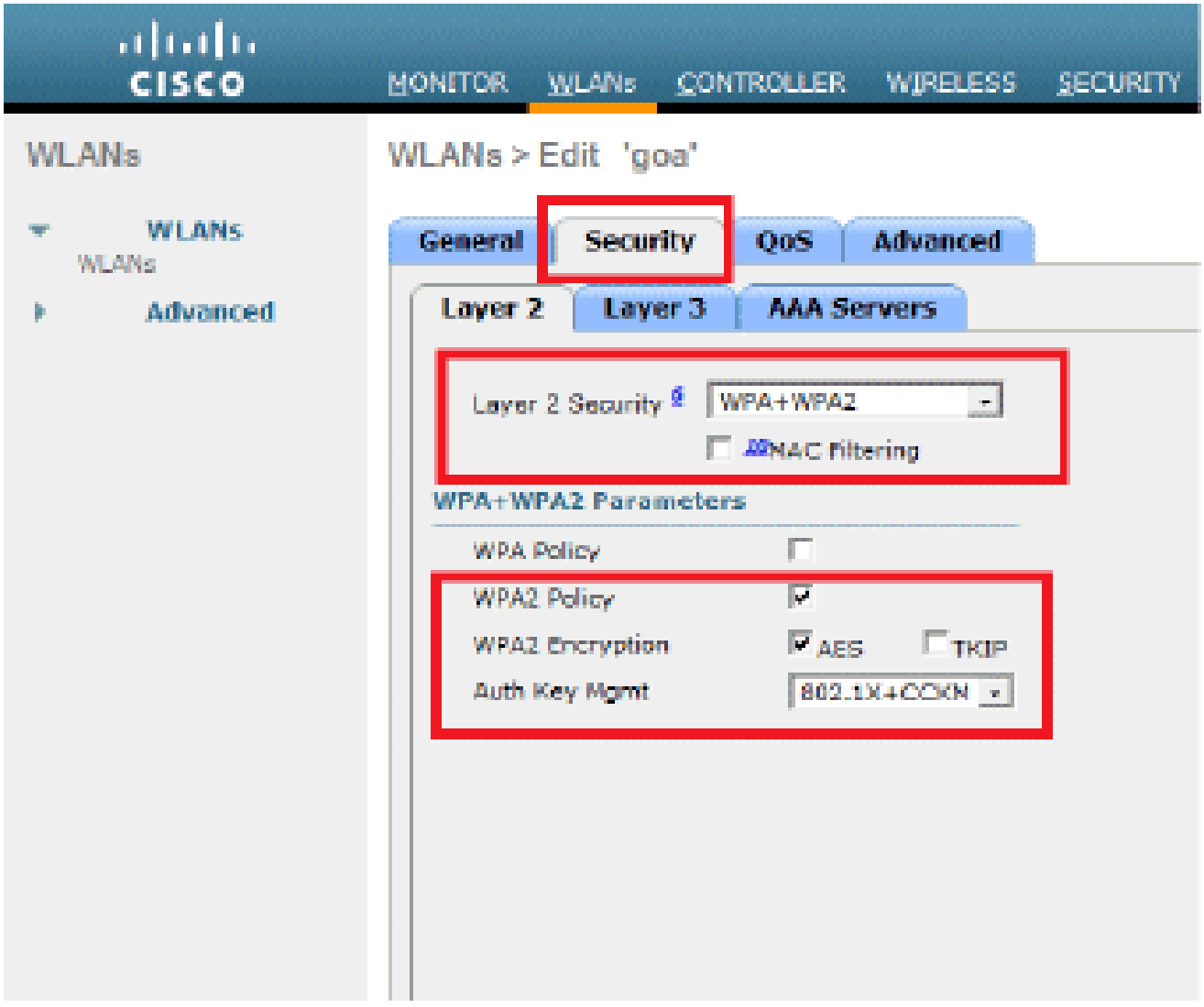
1. 컨트롤러 GUI에서 WLANs(WLAN) > Create New(새로 만들기)로 이동하여 새 WLAN을 생성합니다. New WLANs(새 WLAN) 창이 표시됩니다.
2. WLAN ID 및 WLAN SSID 정보를 입력합니다.

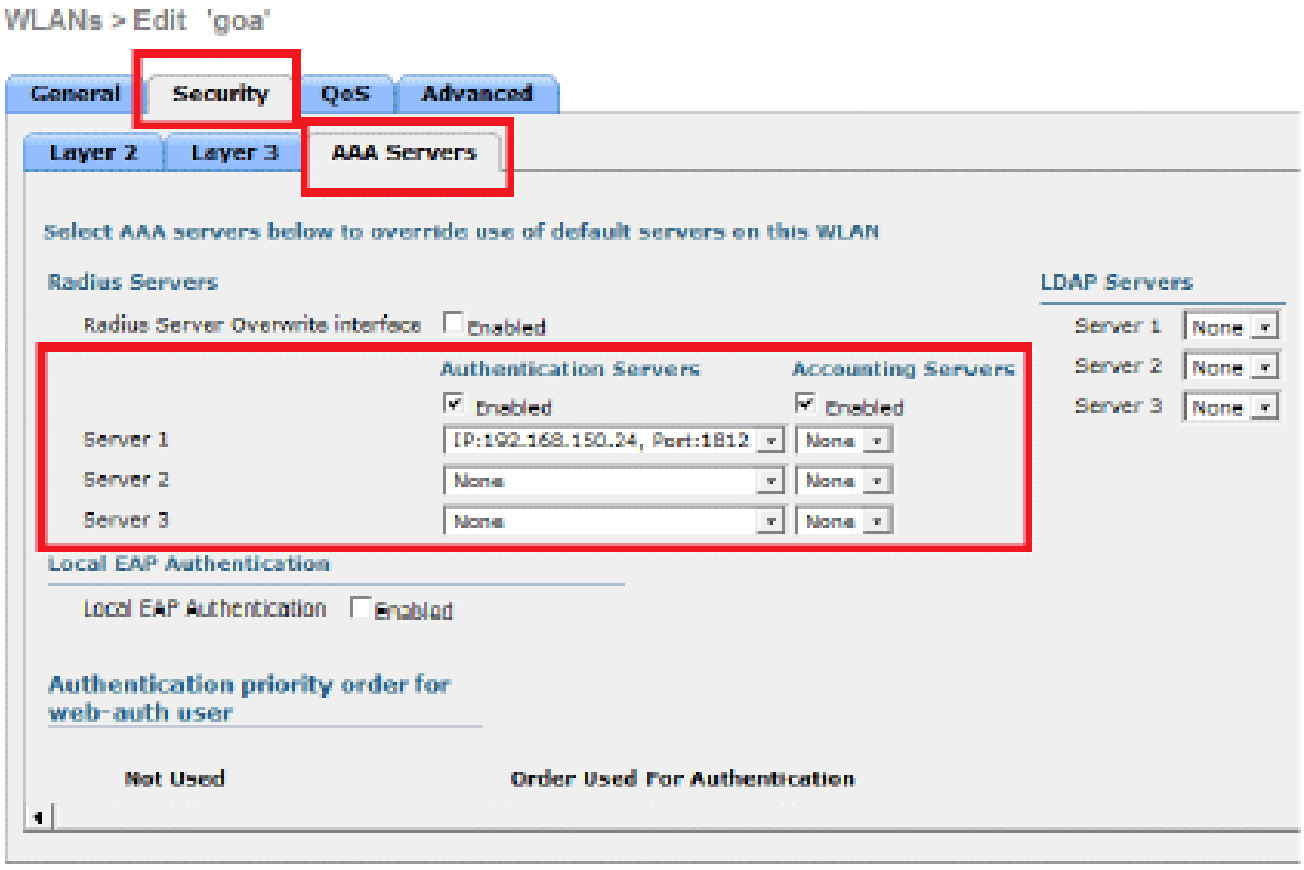
   어떤 이름이든 WLAN SSID로 입력할 수 있습니다. 이 예에서는 goa를 WLAN SSID로 사용합니다.

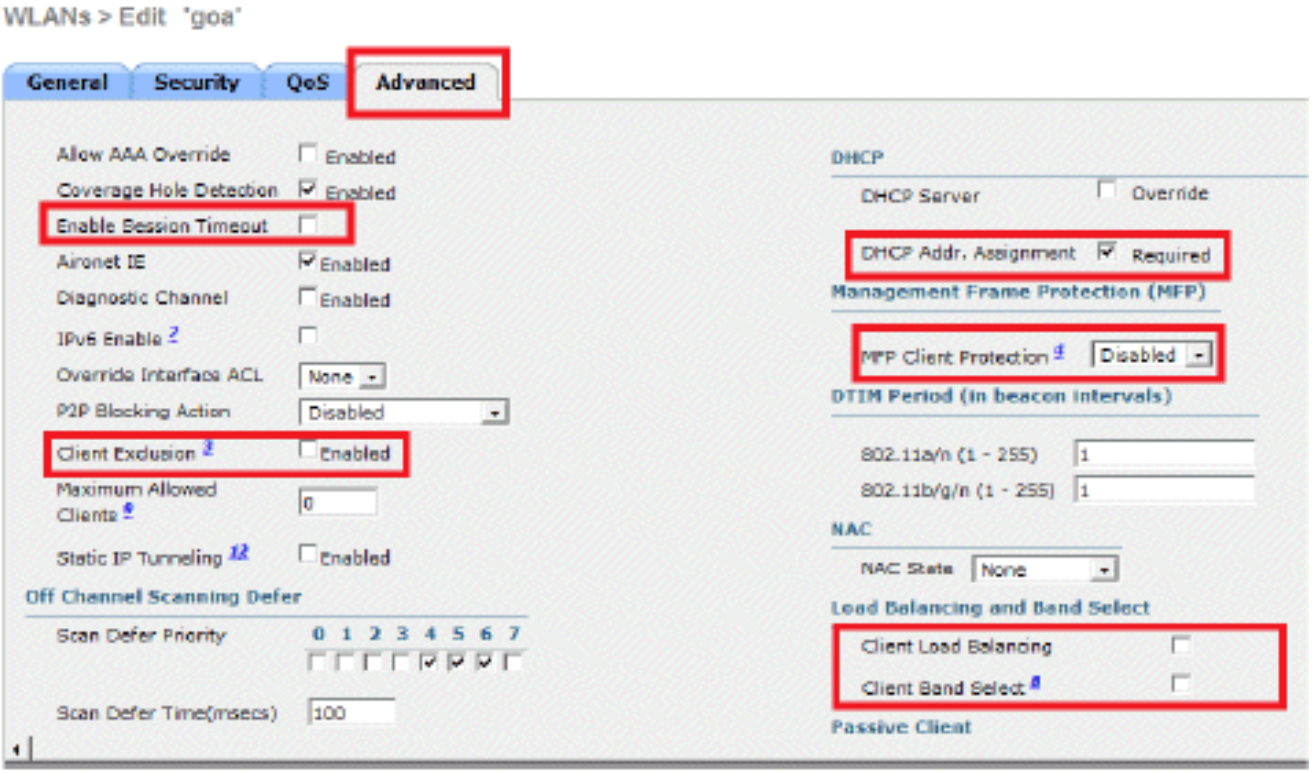


3. Apply(적용)를 클릭하여 WLAN 경로의 Edit(편집) 창으로 이동합니다.


CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
Advanced
AP Groups
WLANs > Edit 'goa'
General Security QoS Advanced
Profile Name goa
Type WLAN
SSID goa
Status Enabled
Security Policies [WPA2][Auth(802.1X + CCKM)]
(Modifications done under security tab will appear after applying the changes.)
Radio Policy All
Interface/Interface Group(G) vlan253
Multicast Vlan Feature Enabled
Broadcast SSID Enabled


CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY
WLANs
WLANs
WLANs
Advanced
WLANs > Edit 'goa'
General Security QoS Advanced
Layer 2 Layer 3 AAA Servers
Layer 2 Security WPA+WPA2
MAC Filtering
WPA+WPA2 Parameters
WPA Policy
WPA2 Policy
WPA2 Encryption AES TKIP
Auth Key Mgmt 802.1X+CCKM





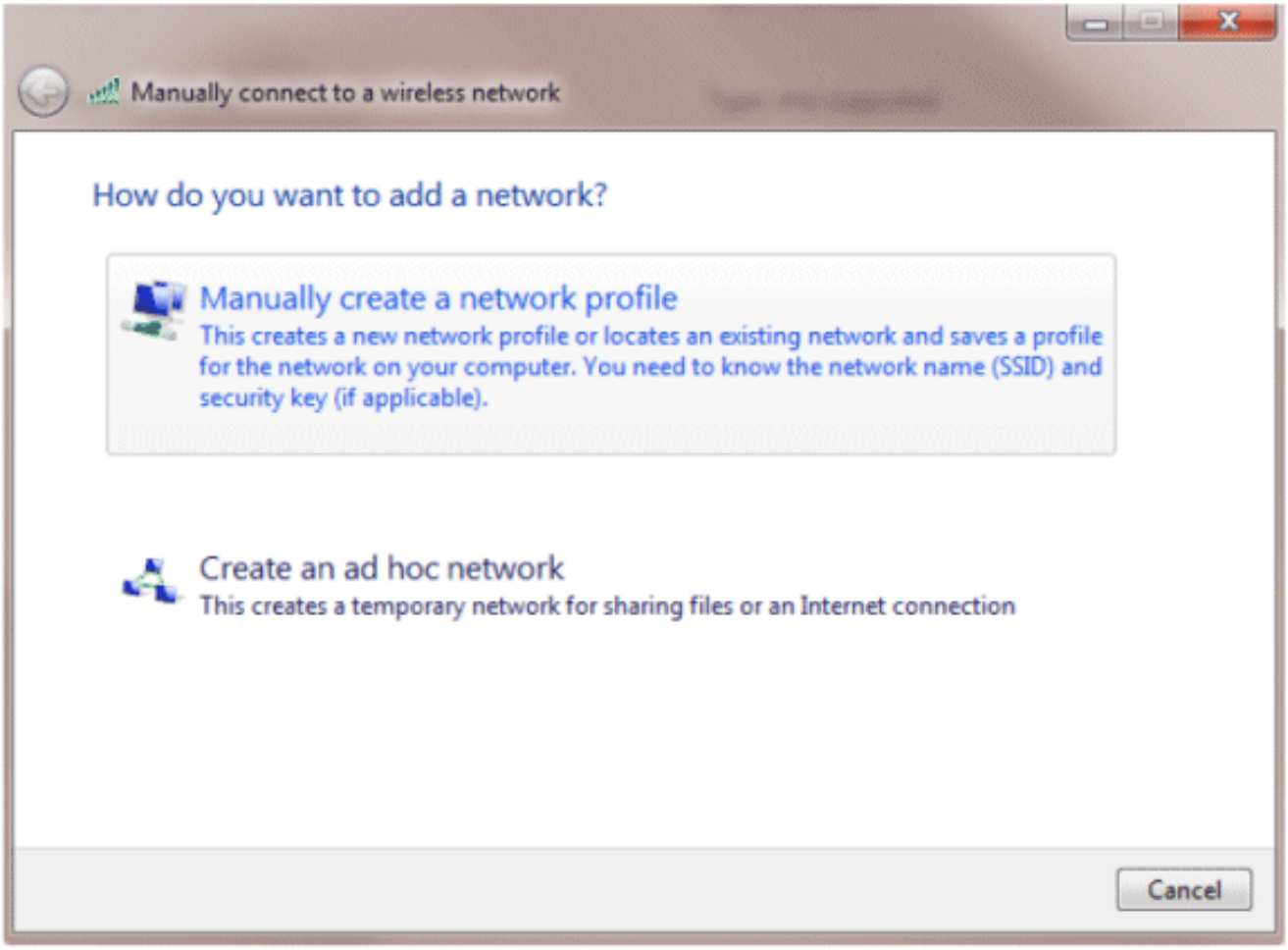
무선 클라이언트 유틸리티 구성

PEAP-MSCHAPv2(user1)

테스트 클라이언트에서는 14.3 드라이버 버전을 실행하는 Intel 6300-N 카드와 함께 Windows 7 기본 신청자를 사용하고 있습니다. 공급업체의 최신 드라이버를 사용하여 테스트하는 것이 좋습니다.

WZC(Windows Zero Config)에서 프로필을 생성하려면 다음 단계를 완료하십시오.

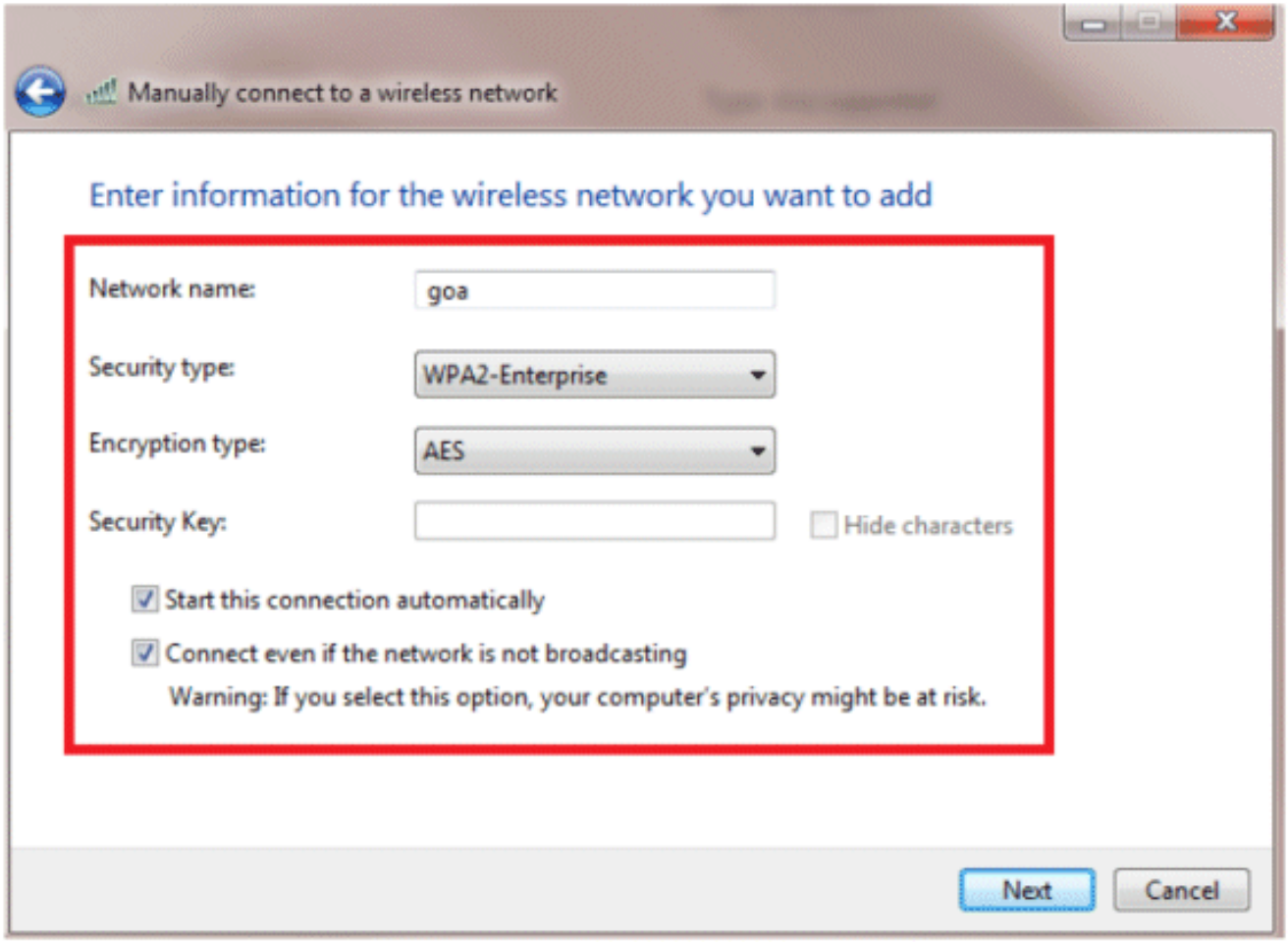
1. 제어판 > 네트워크 및 인터넷 > 무선 네트워크 관리로 이동합니다.
2. Add(추가) 탭을 클릭합니다.
3. Manually create a network profile을 클릭합니다.



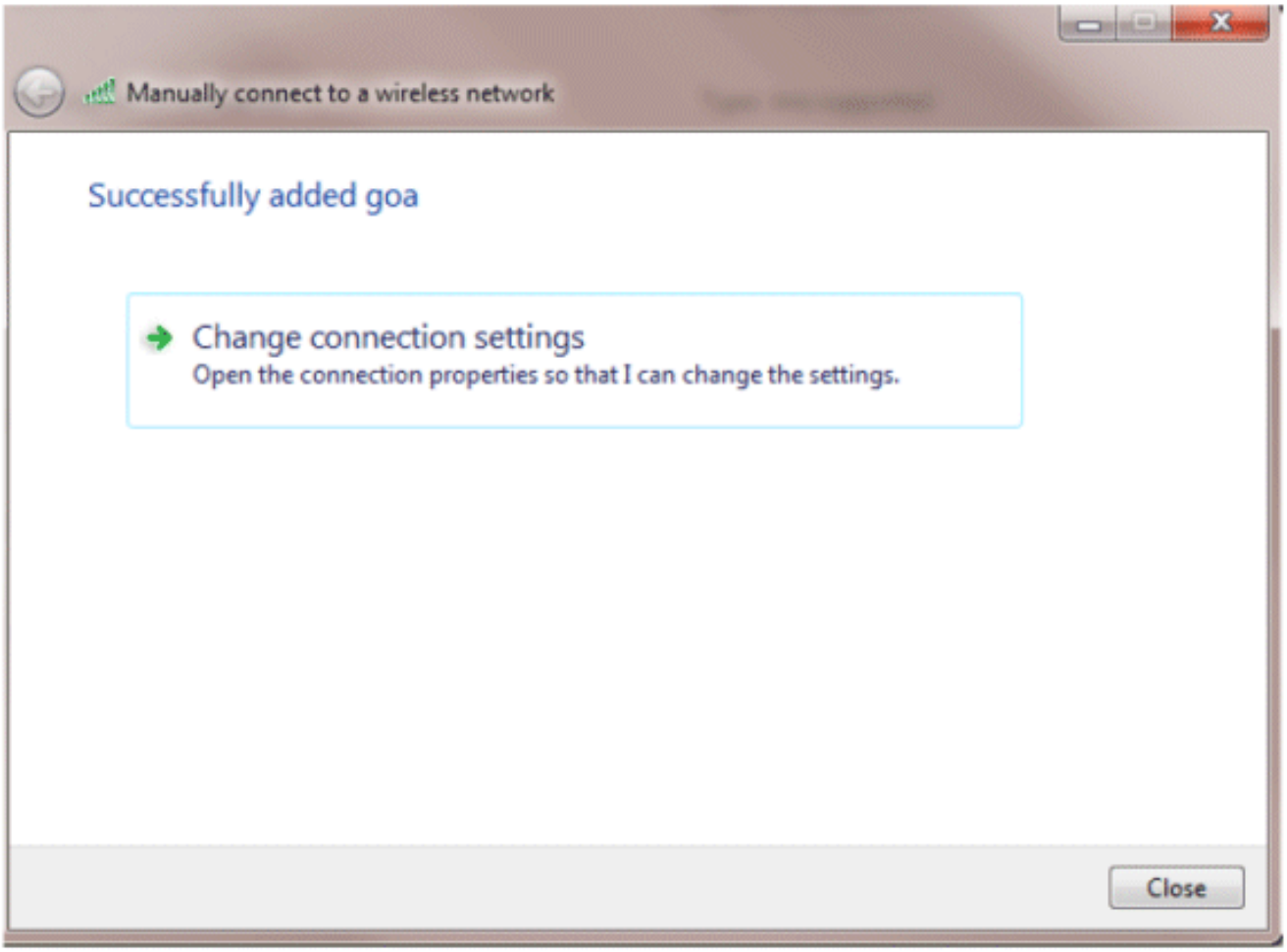
4. WLC에 구성된 대로 세부사항을 추가합니다.

   참고: SSID는 대/소문자를 구분합니다.

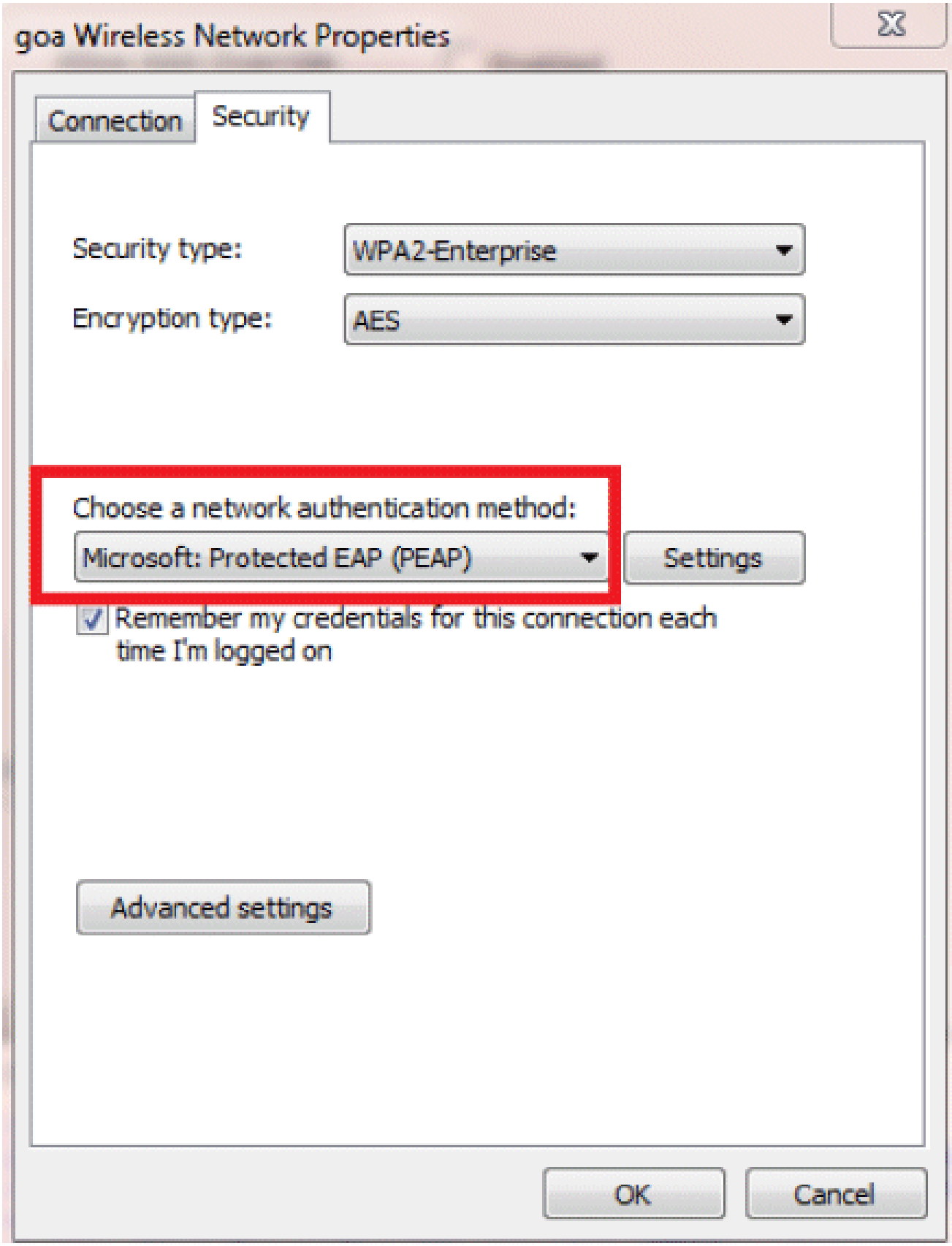
5. Next(다음)를 클릭합니다.

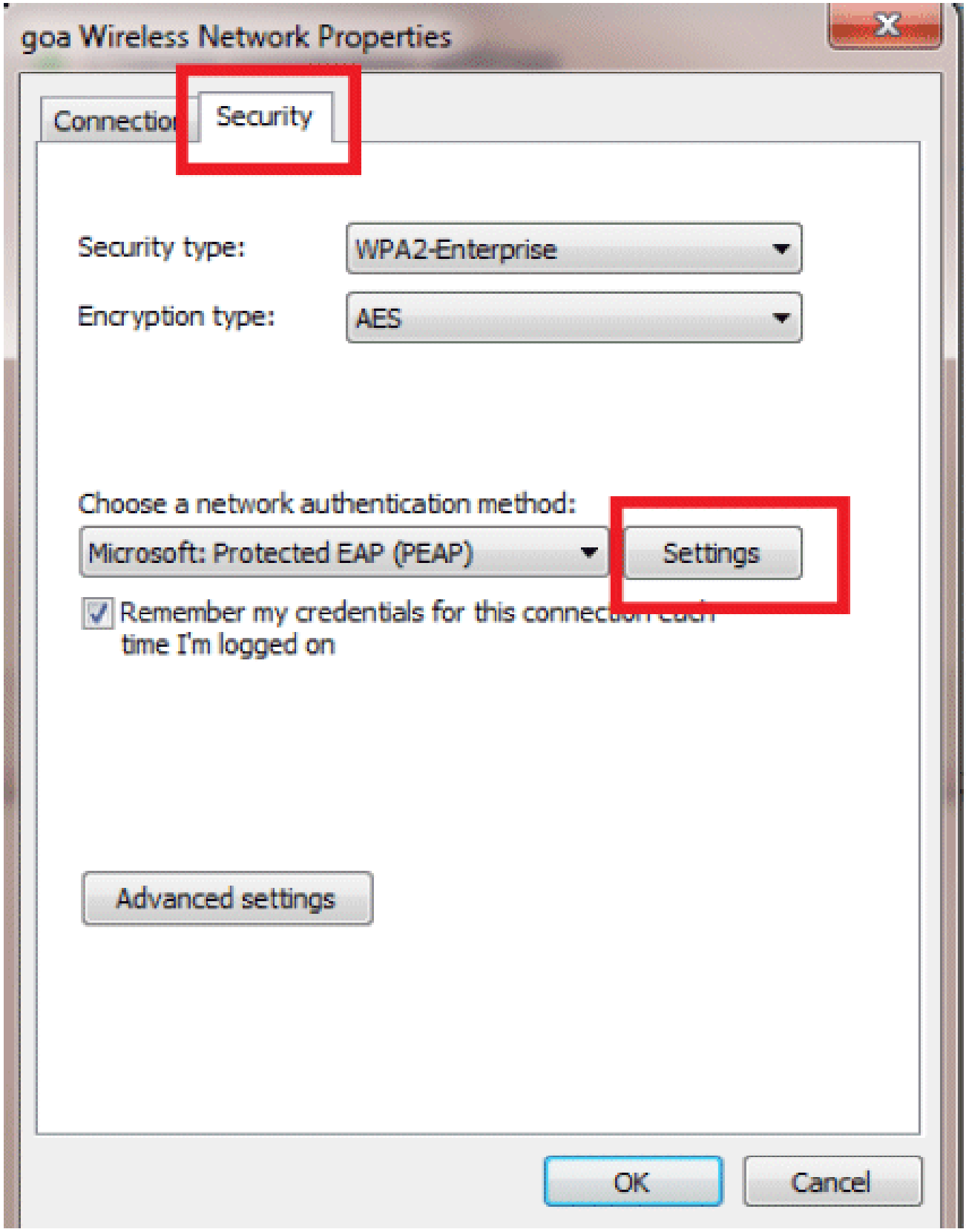


6. 설정을 다시 확인하려면 연결 설정 변경을 클릭합니다.

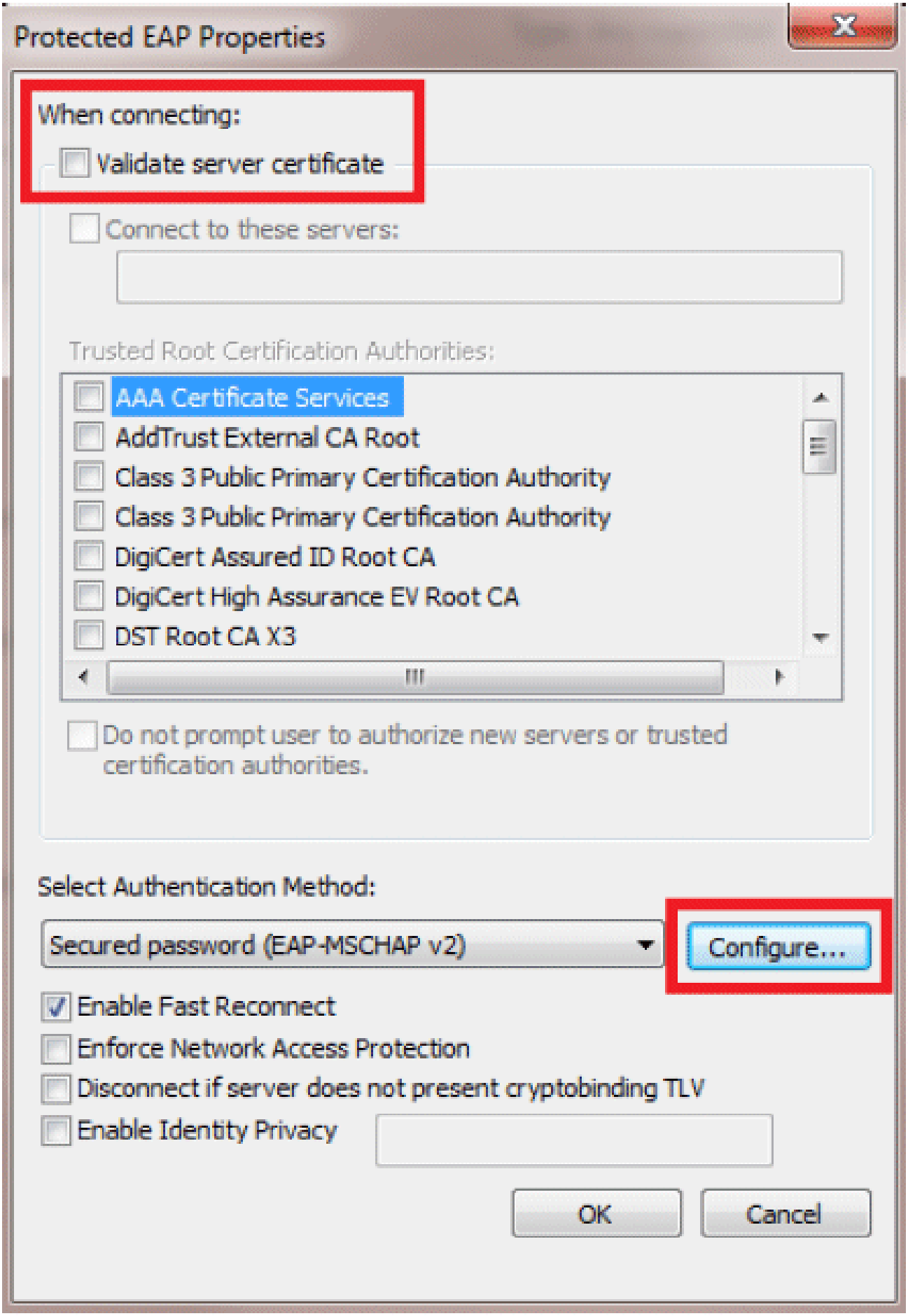


7. PEAP가 활성화되어 있는지 확인합니다.


goa Wireless Network Properties
Connection
Security
Security type:
WPA2-Enterprise
Encryption type:
AES
Choose a network authentication method:
Microsoft: Protected EAP (PEAP)
Settings
Remember my credentials for this connection each time I'm logged on
Advanced settings
OK
Cancel

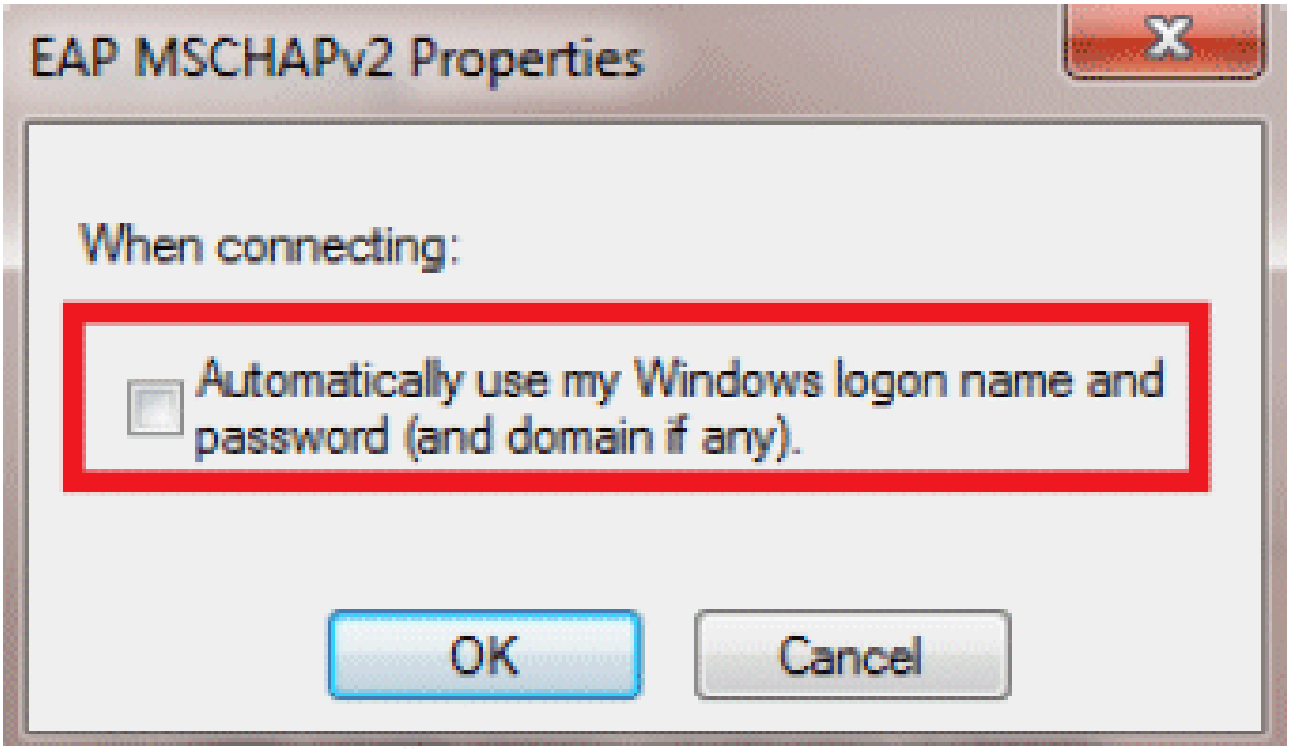


8. 이 예에서는 서버 인증서의 유효성을 검사하지 않습니다. 이 확인란을 선택했지만 연결할 수 없는 경우 기능을 비활성화하고 다시 테스트해 보십시오.

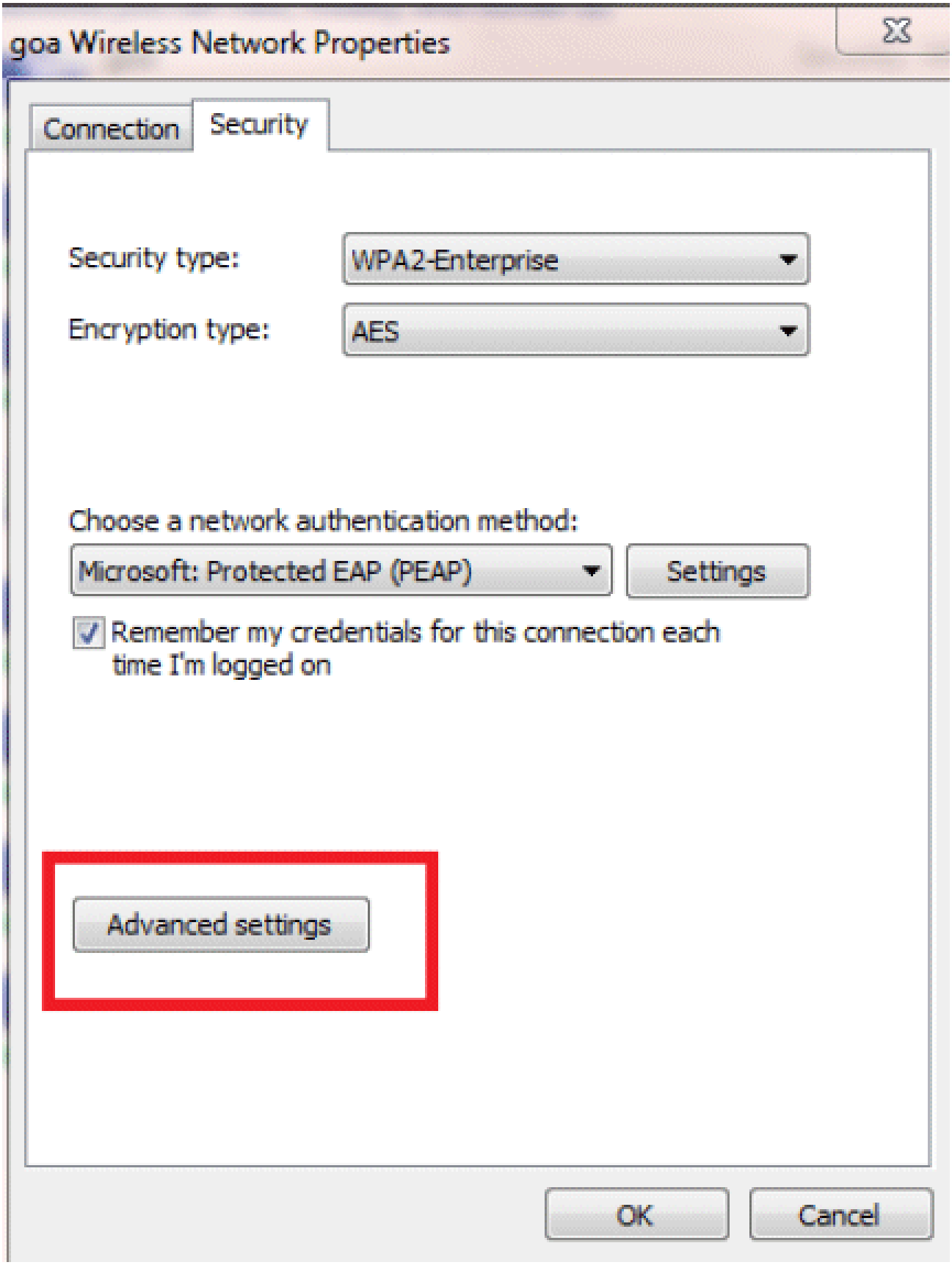


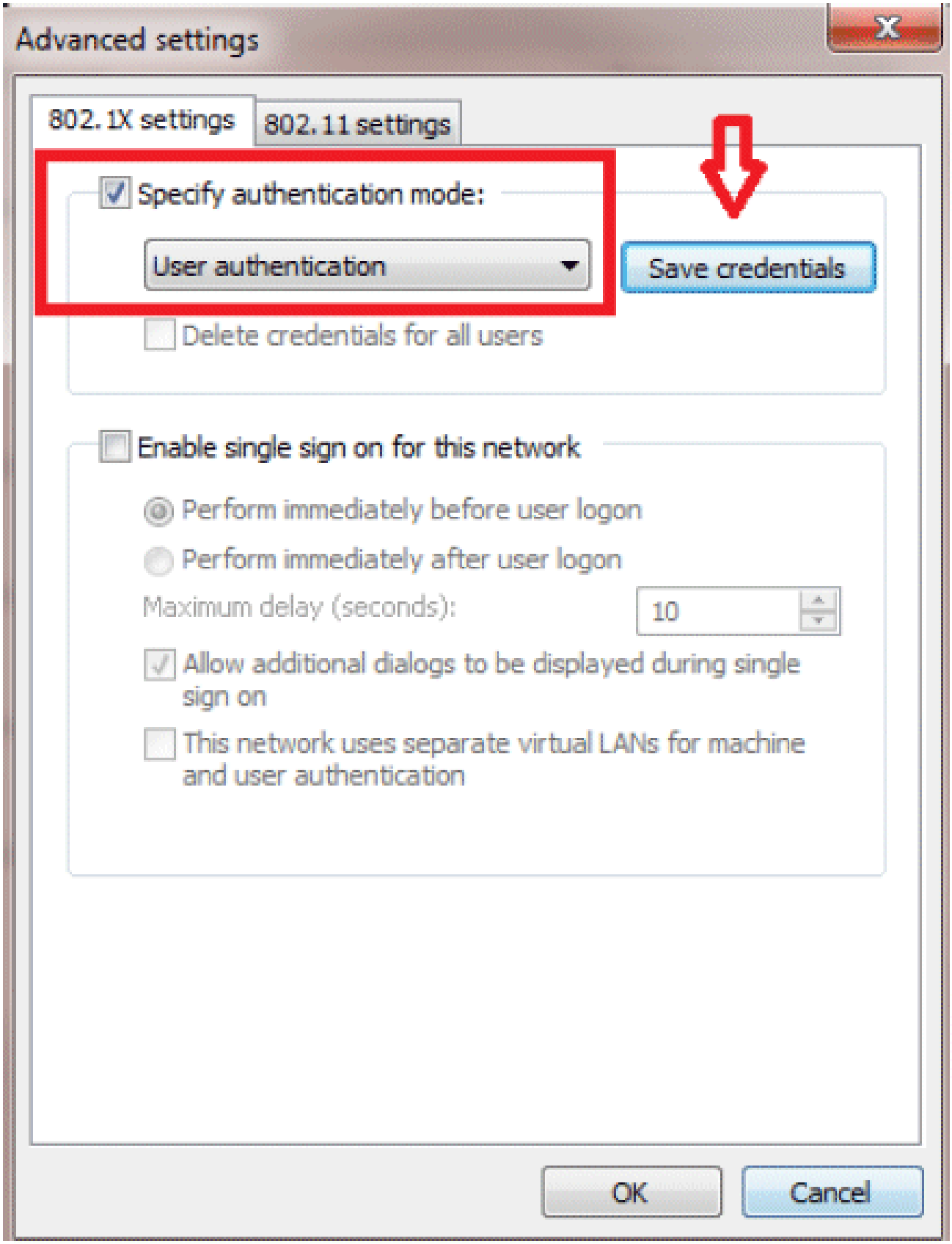
9. 또는 Windows 자격 증명을 사용하여 로그인할 수 있습니다. 그러나 이 예에서는 이를 사용하

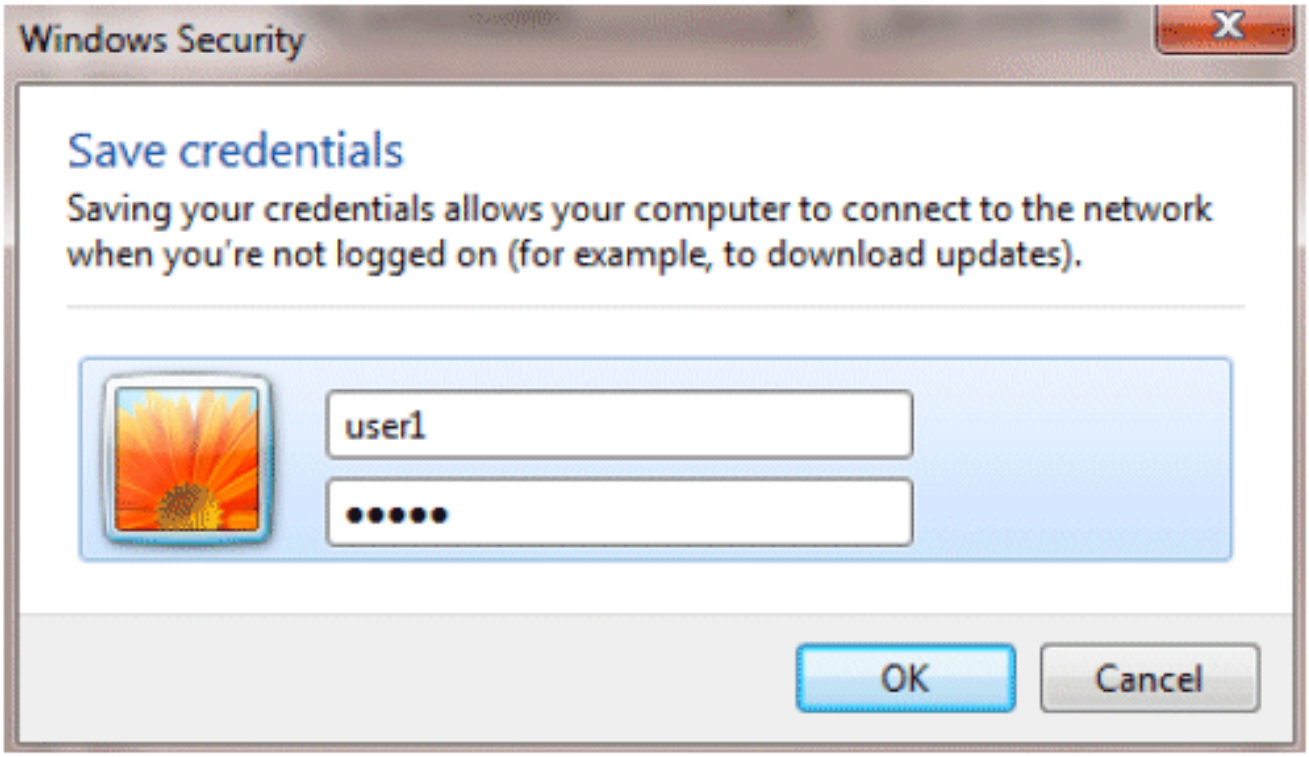
지 않습니다. OK(확인)를 클릭합니다.



10. 사용자 이름과 비밀번호를 구성하려면 Advanced settings를 클릭합니다.


goa Wireless Network Properties
Connection
Security
Security type:
WPA2-Enterprise
Encryption type:
AES
Choose a network authentication method:
Microsoft: Protected EAP (PEAP)
Settings
Remember my credentials for this connection each time I'm logged on
Advanced settings
OK
Cancel


Advanced settings
802.1X settings
802.11 settings
Specify authentication mode:
User authentication
Save credentials
Delete credentials for all users
Enable single sign on for this network
Perform immediately before user logon
Perform immediately after user logon
Maximum delay (seconds):
10
Allow additional dialogs to be displayed during single sign on
This network uses separate virtual LANs for machine and user authentication
OK
Cancel



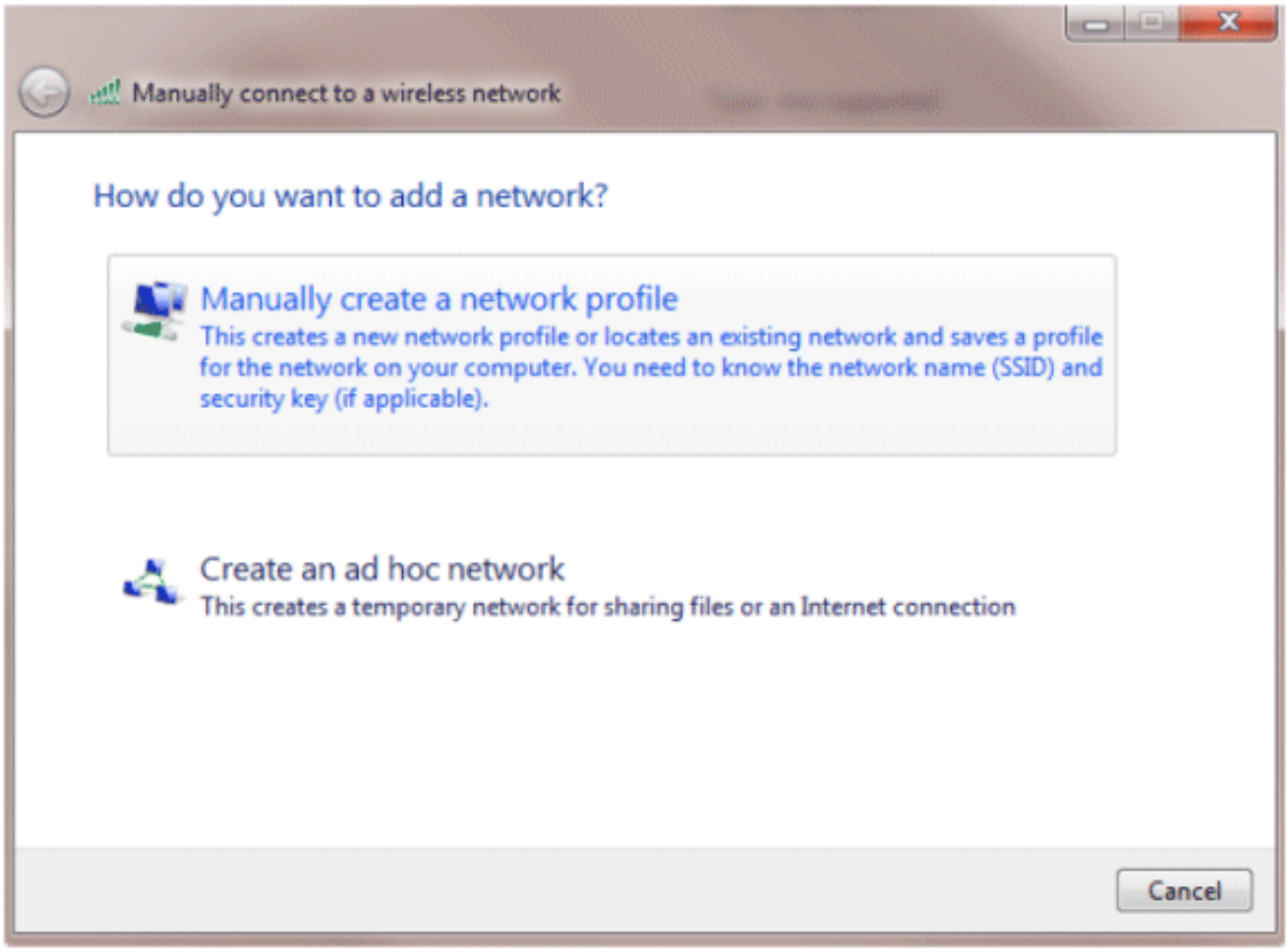
클라이언트 유틸리티에 연결할 준비가 되었습니다.

EAP-FAST(사용자2)

테스트 클라이언트에서는 14.3 드라이버 버전을 실행하는 Intel 6300-N 카드와 함께 Windows 7 기본 신청자를 사용하고 있습니다. 공급업체의 최신 드라이버를 사용하여 테스트하는 것이 좋습니다.

WZC에서 프로파일을 생성하려면 다음 단계를 완료하십시오.

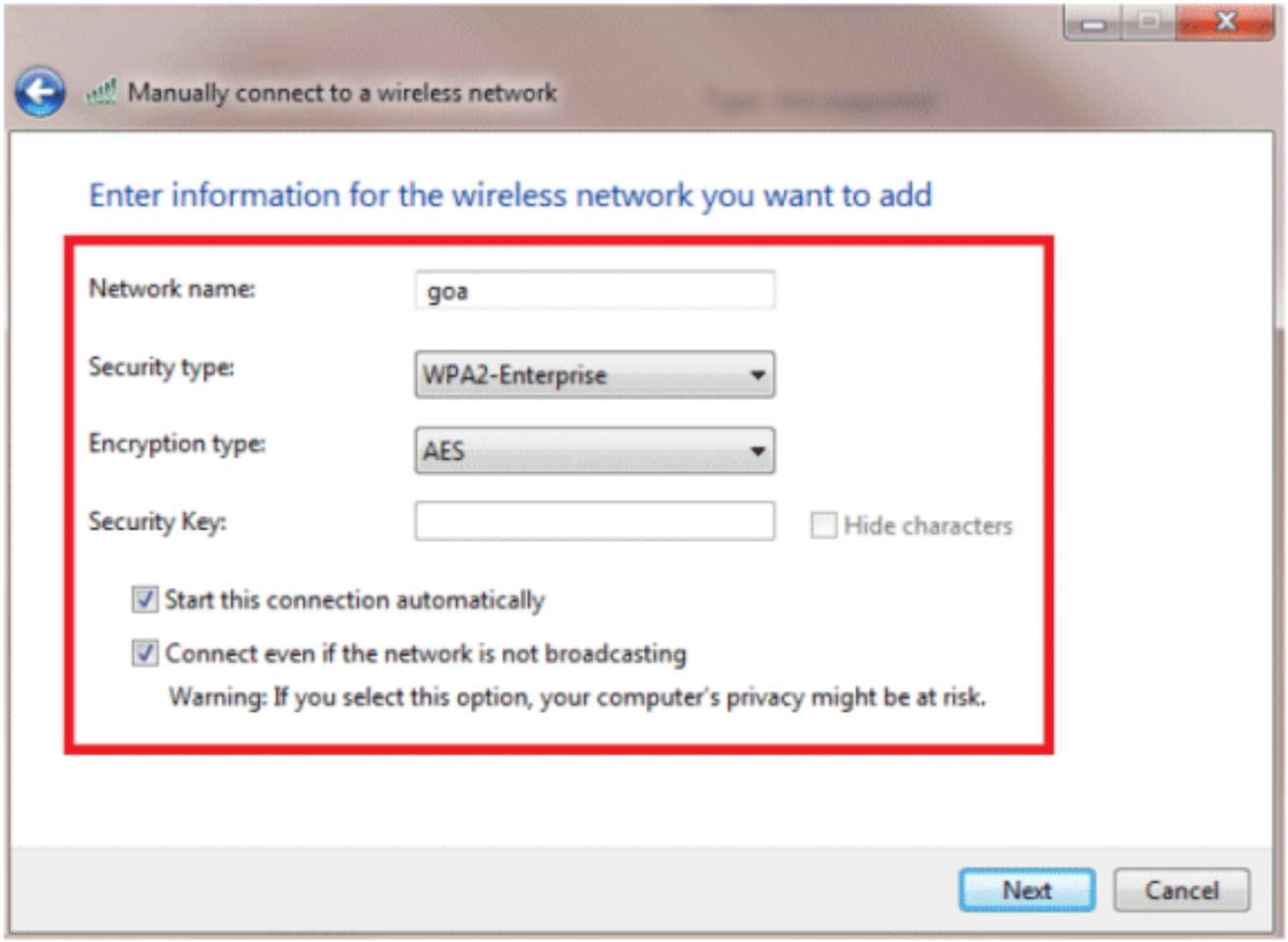
1. 제어판 > 네트워크 및 인터넷 > 무선 네트워크 관리로 이동합니다.
2. Add(추가) 탭을 클릭합니다.
3. Manually create a network profile을 클릭합니다.



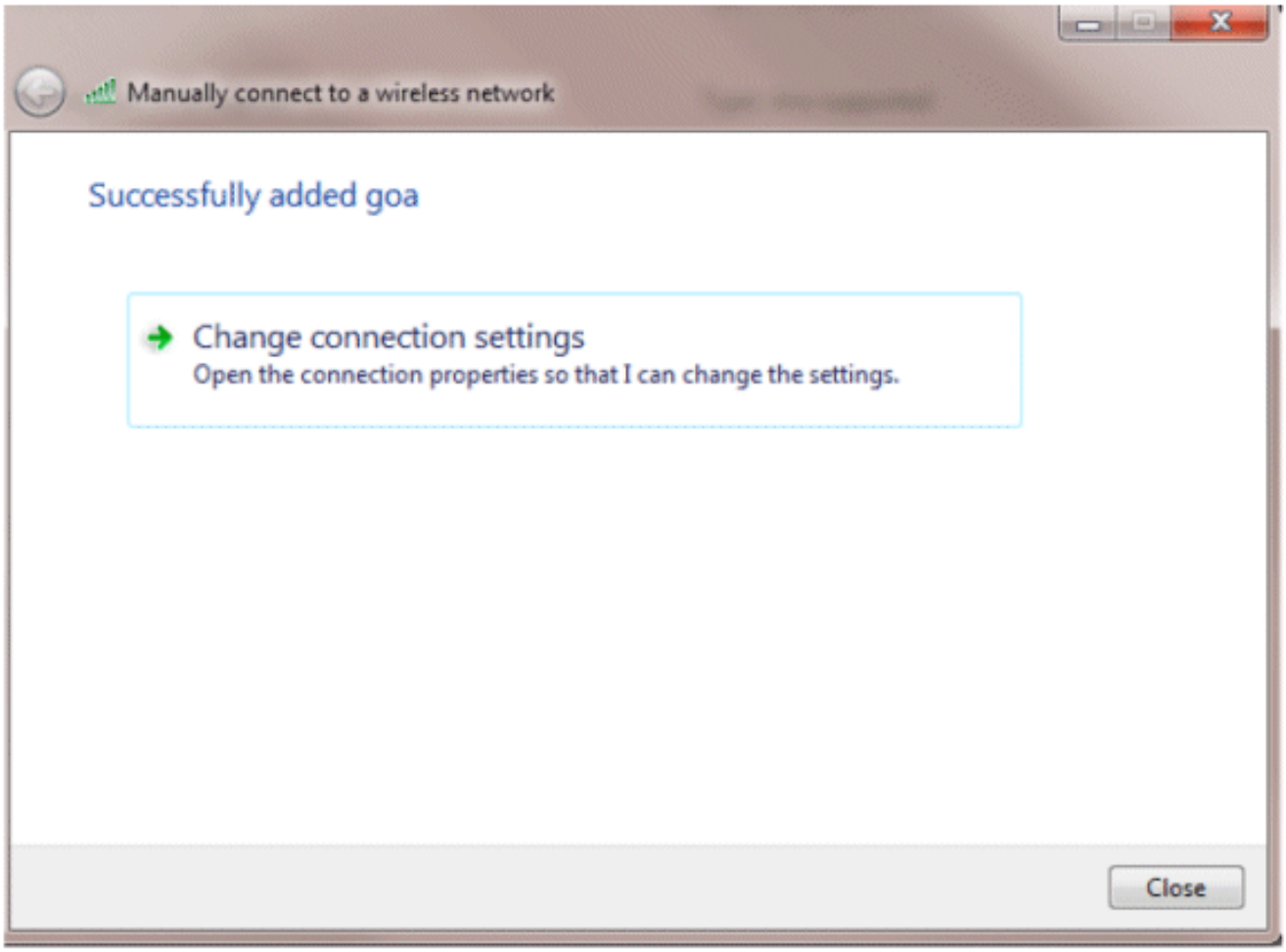
4. WLC에 구성된 대로 세부사항을 추가합니다.

   참고: SSID는 대/소문자를 구분합니다.

5. Next(다음)를 클릭합니다.

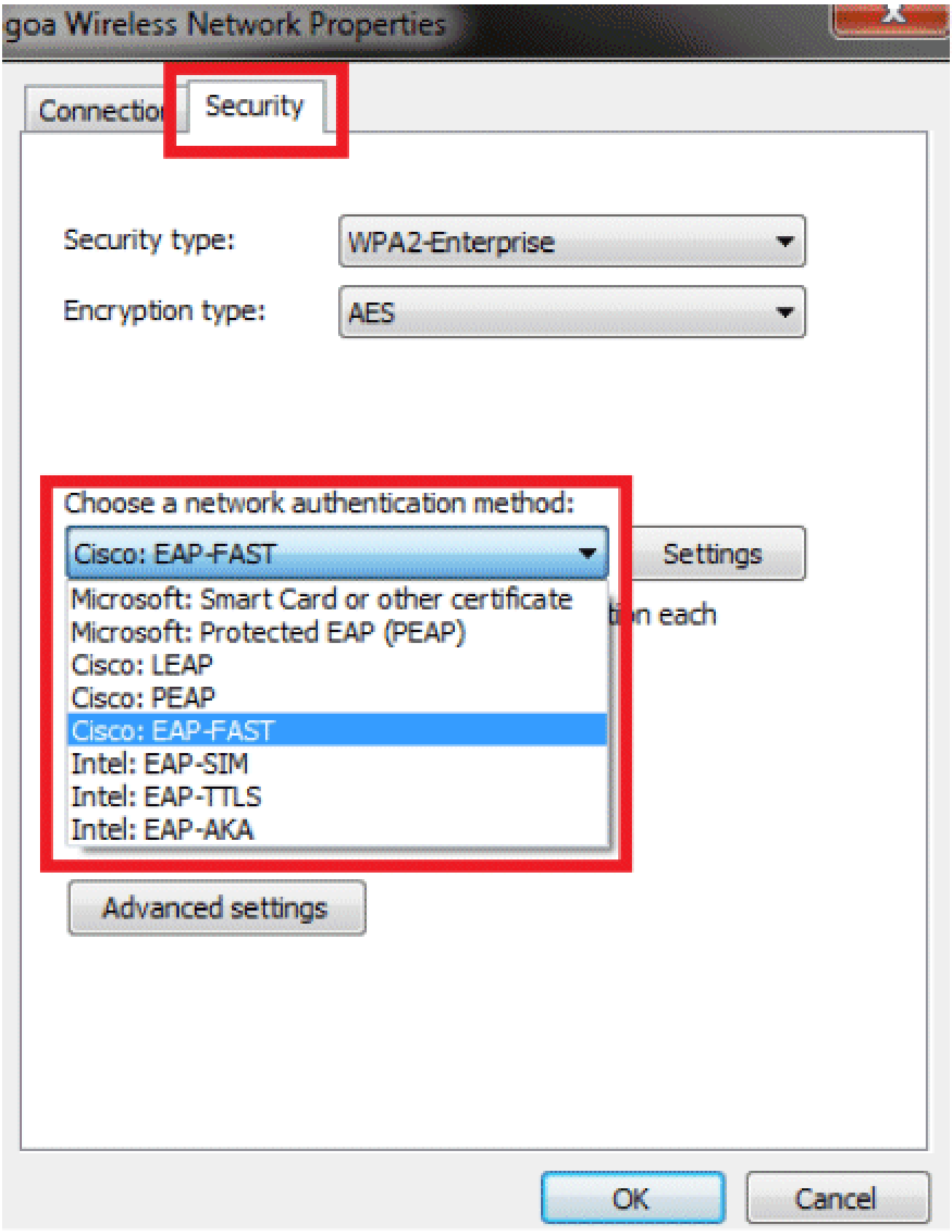


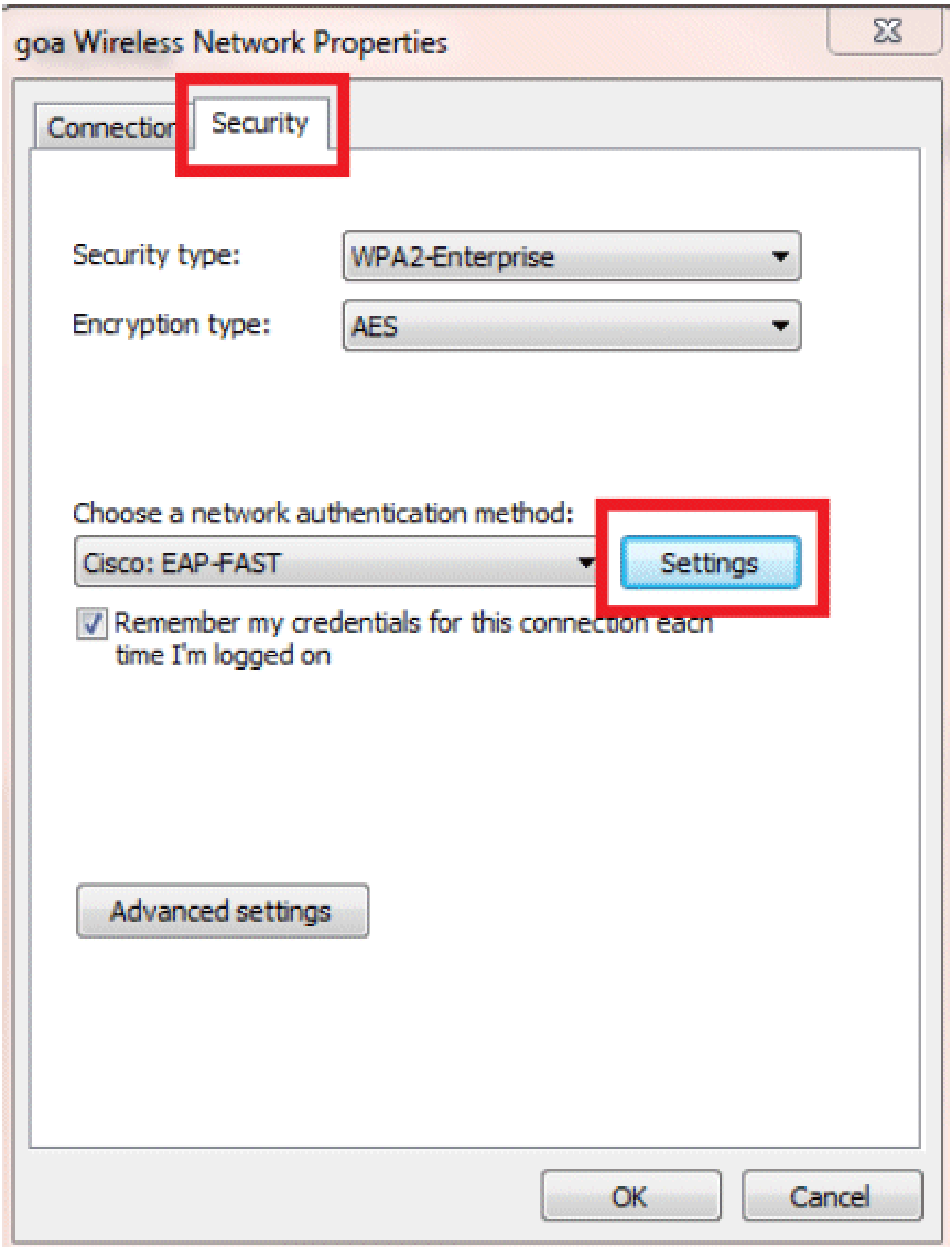
6. 설정을 다시 확인하려면 연결 설정 변경을 클릭합니다.



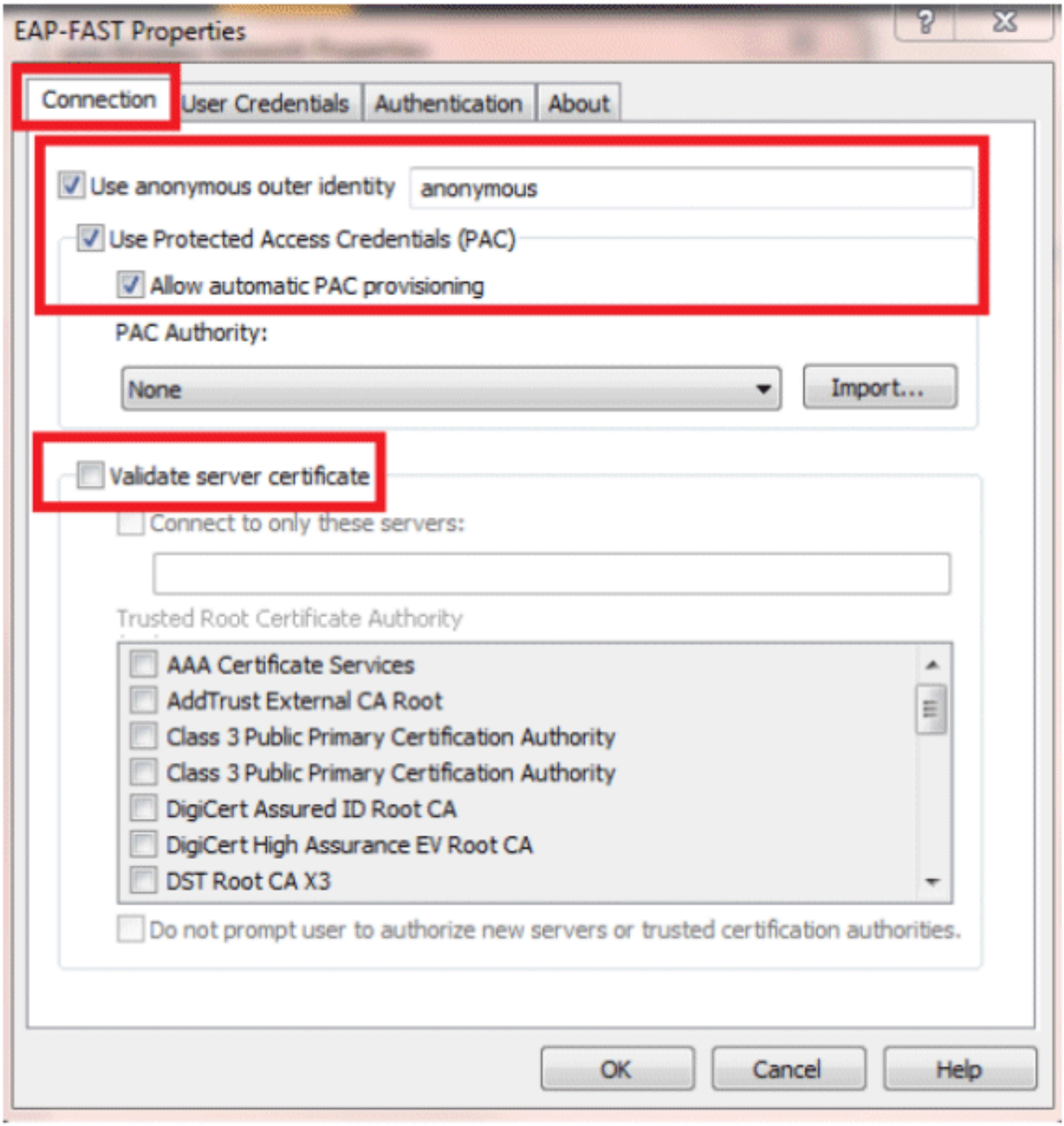
7. EAP-FAST를 활성화했는지 확인합니다.

   참고: 기본적으로 WZC에는 인증 방법으로 EAP-FAST가 없습니다. 타사 공급업체에서 유틸리티를 다운로드해야 합니다. 이 예에서는 Intel 카드이므로 시스템에 Intel PROSet이 설치되어 있습니다.

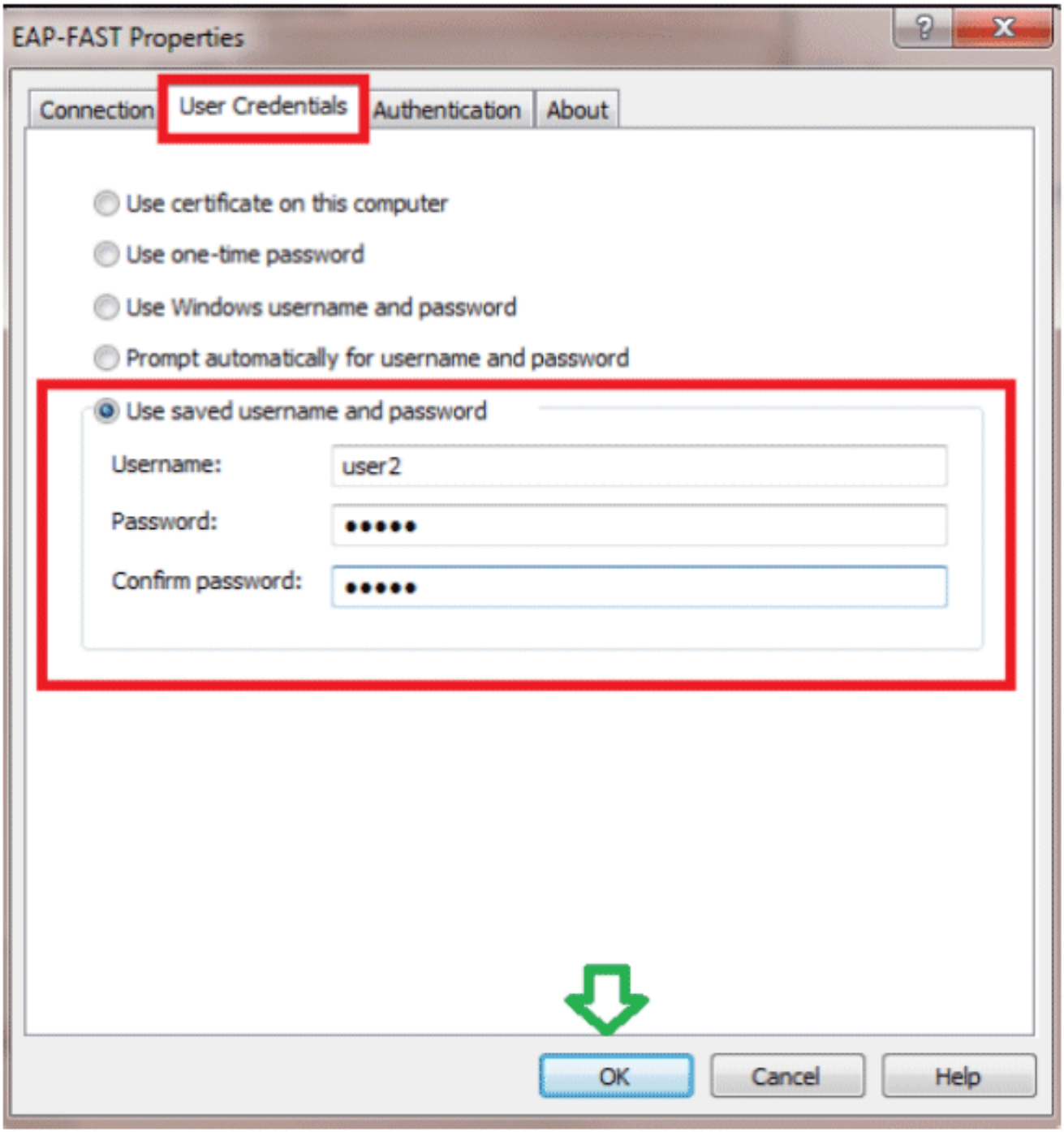

goa Wireless Network Properties
Connectio
Security
Security type:
WPA2-Enterprise
Encryption type:
AES
Choose a network authentication method:
Cisco: EAP-FAST
Settings
Microsoft: Smart Card or other certificate
Microsoft: Protected EAP (PEAP)
Cisco: LEAP
Cisco: PEAP
Cisco: EAP-FAST
Intel: EAP-SIM
Intel: EAP-TTLS
Intel: EAP-AKA
Advanced settings
OK
Cancel



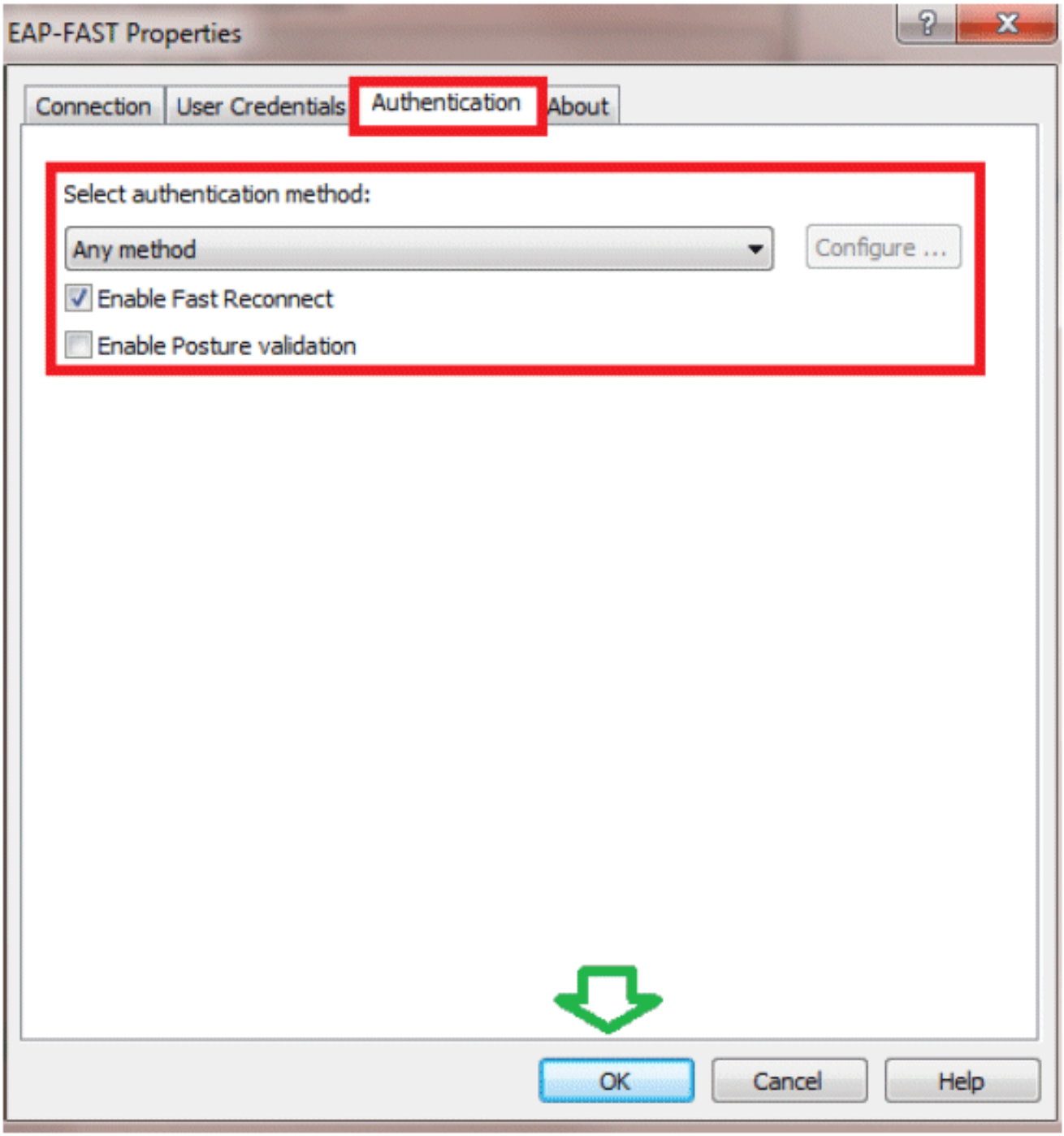
8. Allow automatic PAC provisioning(자동 PAC 프로비저닝 허용)을 활성화하고 Validate server certificate(서버 인증서 검증)가 선택되지 않았는지 확인합니다.



9. User Credentials(사용자 자격 증명) 탭을 클릭하고 user2의 자격 증명을 입력합니다. 또는 Windows 자격 증명을 사용하여 로그인할 수 있습니다. 그러나 이 예에서는 이를 사용하지 않습니다.

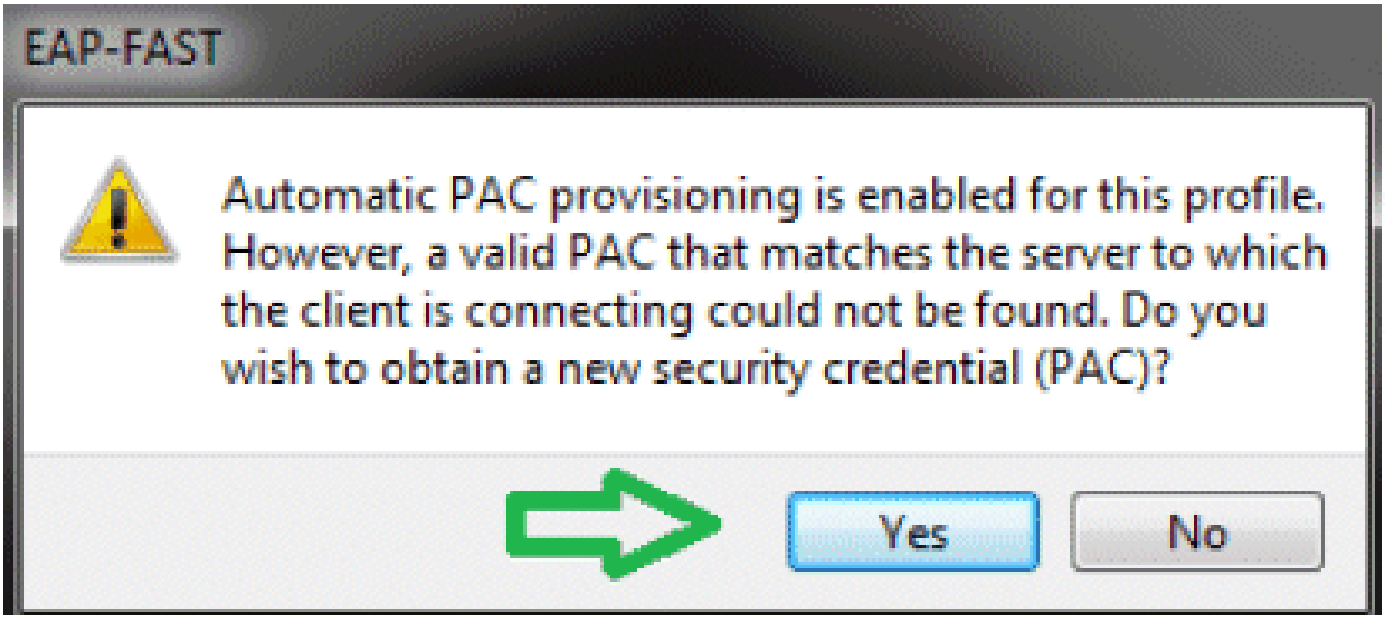


10. OK(확인)를 클릭합니다.



이제 클라이언트 유틸리티가 user2를 위해 연결할 준비가 되었습니다.

참고: user2가 인증을 시도할 때 RADIUS 서버는 PAC를 전송합니다. 인증을 완료하려면 PAC를 수락합니다.



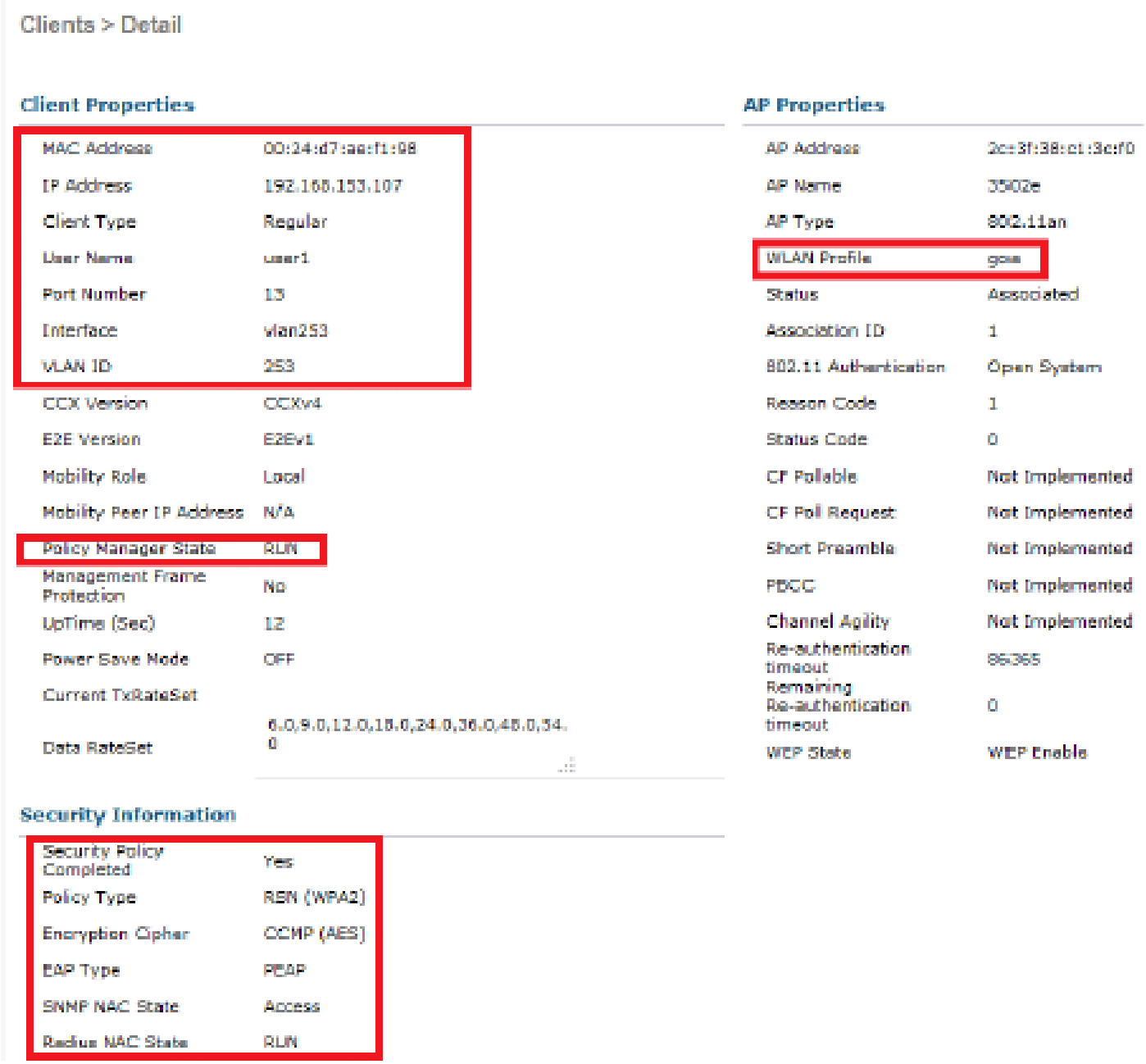
다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

OIT(Output Interpreter Tool)(등록된 고객만 해당)는 특정 show 명령을 지원합니다. OIT를 사용하여 show 명령 출력 분석을 볼 수 있습니다.

사용자1(PEAP-MSCHAPv2) 확인

WLC GUI에서 Monitor(모니터) > Clients(클라이언트)로 이동하여 MAC 주소를 선택합니다.



WLC RADIUS 통계:

<#root>

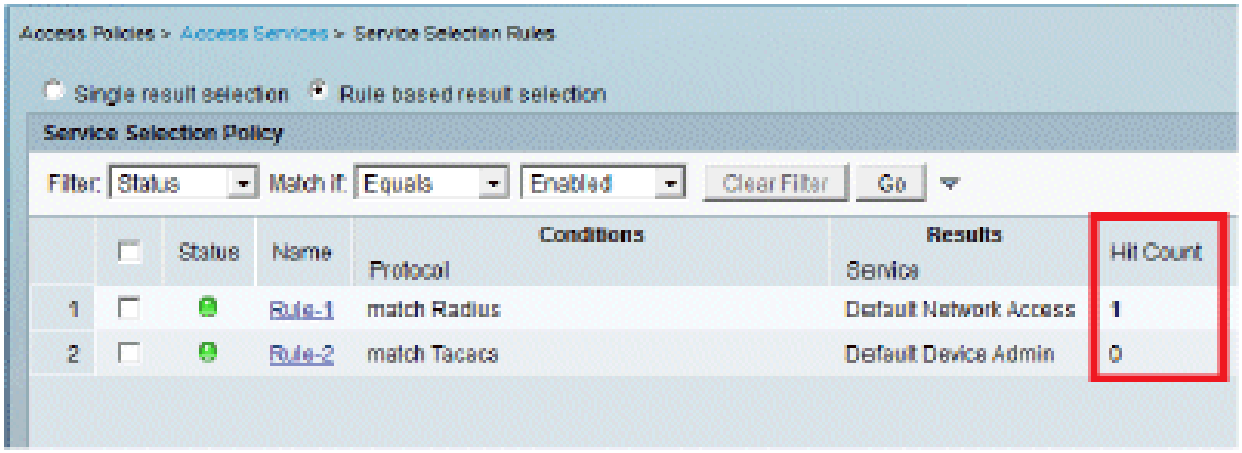
```
(Cisco Controller) >

show radius auth statistics

Authentication Servers:
Server Index..................................... 1
Server Address................................... 192.168.150.24
Msg Round Trip Time.............................. 1 (msec)
First Requests................................... 8
Retry Requests................................... 0
Accept Responses................................. 1
Reject Responses................................. 0
Challenge Responses.............................. 7
Malformed Msgs................................... 0
Bad Authenticator Msgs........................... 0
```

```
Pending Requests.............................. 0
Timeout Requests.............................. 0
Unknowntype Msgs.............................. 0
Other Drops................................... 0
```

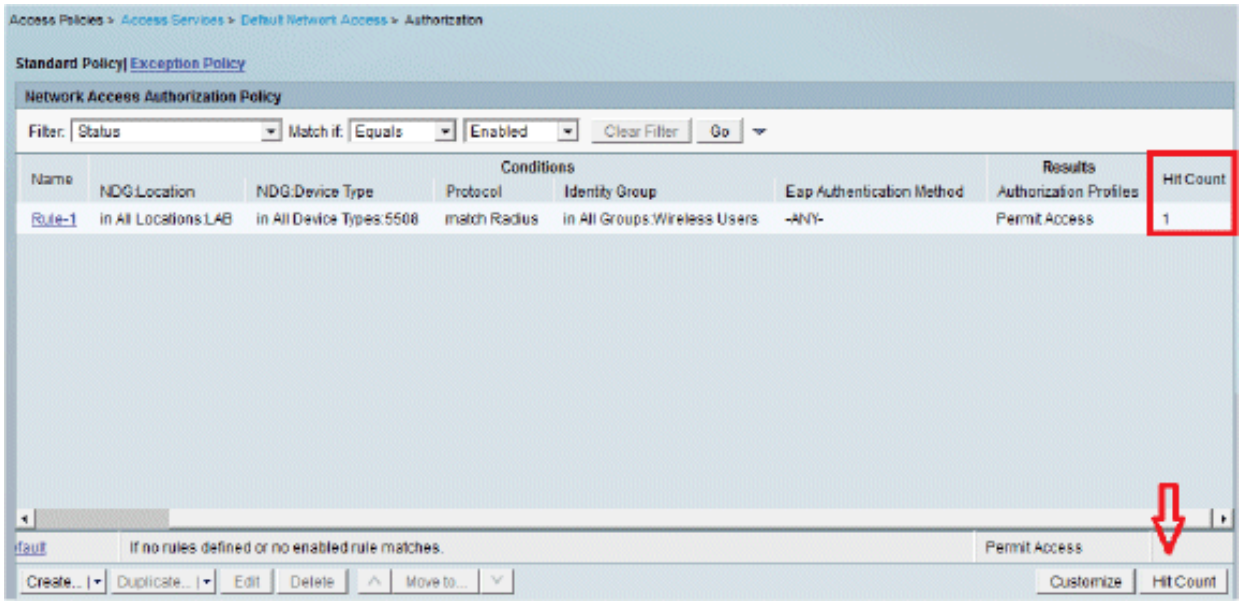
ACS 로그:

1. 적중 횟수를 보려면 다음 단계를 완료하십시오.

   a. 인증 후 15분 내에 로그를 확인하는 경우 적중 횟수를 새로 고쳐야 합니다.



   b. 같은 페이지 하단에 Hit Count(적중 횟수) 탭이 있습니다.



2. Monitoring and Reports(모니터링 및 보고서)를 클릭하면 New(새) 팝업 창이 나타납니다. Authentications(인증) -Radius -Today(오늘)로 이동합니다. 어떤 서비스 선택 규칙이 적용되었는지 확인하기 위해 Details를 클릭할 수도 있습니다.

사용자2(EAP-FAST) 확인

WLC GUI에서 Monitor(모니터) > Clients(클라이언트)로 이동하여 MAC 주소를 선택합니다.

Clients > Detail

Client Properties

MAC Address	00:24:d7:ae:f1:98
IP Address	192.168.153.111
Client Type	Regular
User Name	user2
Port Number	13
Interface	vlan253
VLAN ID	253
CCX Version	CCXv4
E2E Version	E2Ev1
Mobility Role	Local
Mobility Peer IP Address	N/A
Policy Manager State	RUN
Management Frame Protection	No
UpTime (Sec)	29
Power Save Mode	OFF
Current TxRateSet	m15
Data RateSet	6.0,9.0,12.0,18.0,24.0,36.0,48.0,54.0

AP Properties

AP Address	2c:3f:38:c1:3c:f0
AP Name	3502e
AP Type	802.11an
WLAN Profile	goa
Status	Associated
Association ID	1
802.11 Authentication	Open System
Reason Code	1
Status Code	0
CF Pollable	Not Implemented
CF Poll Request	Not Implemented
Short Preamble	Not Implemented
PBCC	Not Implemented
Channel Agility	Not Implemented
Re-authentication timeout	86392
Remaining Re-authentication timeout	0
WEP State	WEP Enable

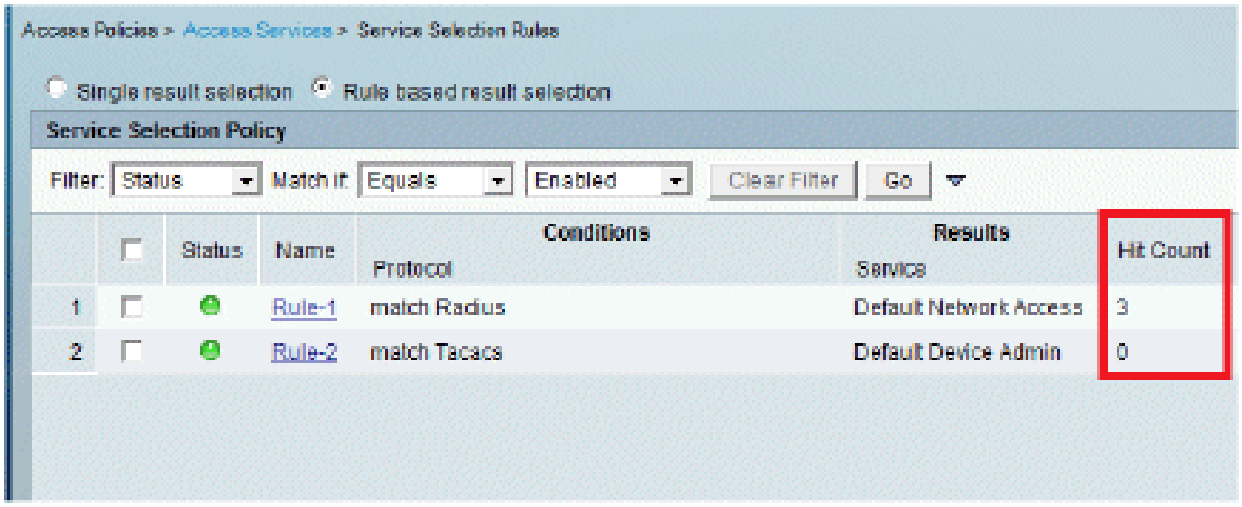
Security Information

Security Policy Completed	Yes
Policy Type	RSN (WPA2)
Encryption Cipher	CCMP (AES)
EAP Type	EAP-FAST
SNMP NAC State	Access
Radius NAC State	RUN

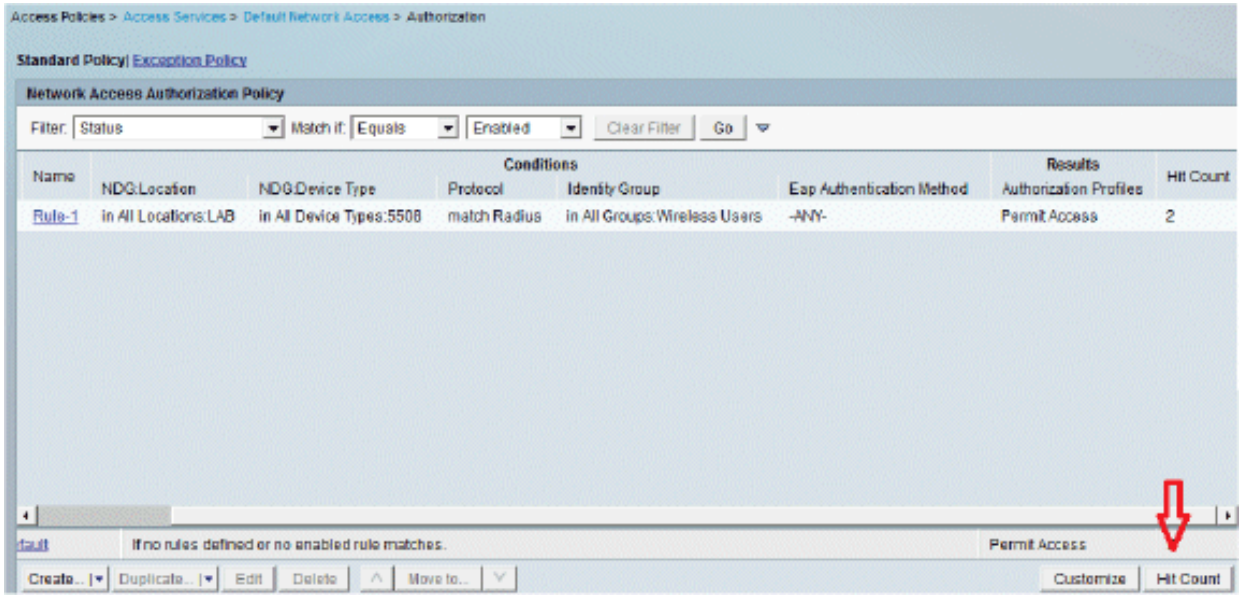
ACS 로그:

1. 적중 횟수를 보려면 다음 단계를 완료하십시오.

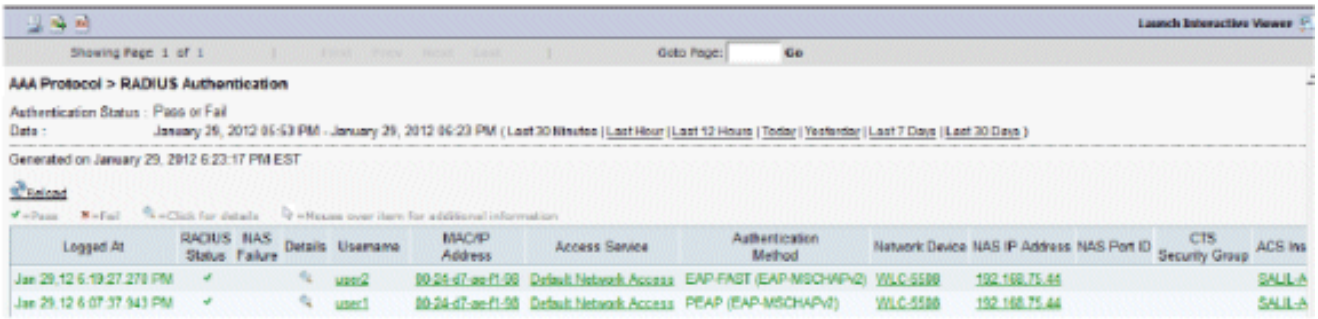
a. 인증 후 15분 내에 로그를 확인하는 경우 HIT 수를 새로 고쳐야 합니다.



b. 같은 페이지 하단에 Hit Count(적중 횟수) 탭이 있습니다.



2. Monitoring and Reports(모니터링 및 보고서)를 클릭하면 New(새) 팝업 창이 나타납니다. Authentications(인증) -Radius -Today(오늘)로 이동합니다. 어떤 서비스 선택 규칙이 적용되었는지 확인하기 위해 Details를 클릭할 수도 있습니다.



문제 해결

이 섹션에서는 설정 문제 해결에 사용할 수 있는 정보를 제공합니다.

트러블슈팅 명령

OIT(Output Interpreter Tool)(등록된 고객만 해당)는 특정 show 명령을 지원합니다. OIT를 사용하여 show 명령 출력 분석을 볼 수 있습니다.

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

1. 문제가 발생하면 WLC에서 다음 명령을 실행합니다.
    - debug client <클라이언트의 mac 추가>
    - debug aaa all enable
    - show client detail <mac addr> - 정책 관리자 상태를 확인합니다.
    - show radius auth statistics - 실패 사유를 확인합니다.
    - debug disable-all - 디버그를 끕니다.
    - clear stats radius auth all - WLC에서 radius 통계를 지웁니다.
2. ACS의 로그를 확인하고 실패 이유를 기록합니다.

관련 정보

- 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.