LAP를 사용한 포트 기반 인증을 위한 ACS 5.2 구성

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[표기 규칙](#)
[배경 정보](#)
[구성](#)
[네트워크 다이어그램](#)
[가정](#)
[컨피그레이션 단계](#)
[LAP 구성](#)
[스위치 구성](#)
[RADIUS 서버 구성](#)
[네트워크 리소스 구성](#)
[사용자 구성](#)
[정책 요소 정의](#)
[액세스 정책 적용](#)
[다음을 확인합니다.](#)
[문제 해결](#)
[관련 정보](#)

소개

이 문서에서는 ACS(Access Control Server) 5.2와 같은 RADIUS 서버에 대해 인증하기 위해 LAP를 802.1x 신청자로 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 컨피그레이션을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- WLC(Wireless LAN Controller) 및 LAP에 대한 기본 지식을 갖추고 있습니다.
- AAA 서버에 대한 기능적 지식이 있어야 합니다.
- 무선 네트워크 및 무선 보안 문제에 대해 철저하게 알고 있어야 합니다.

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
- 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.

배경 정보

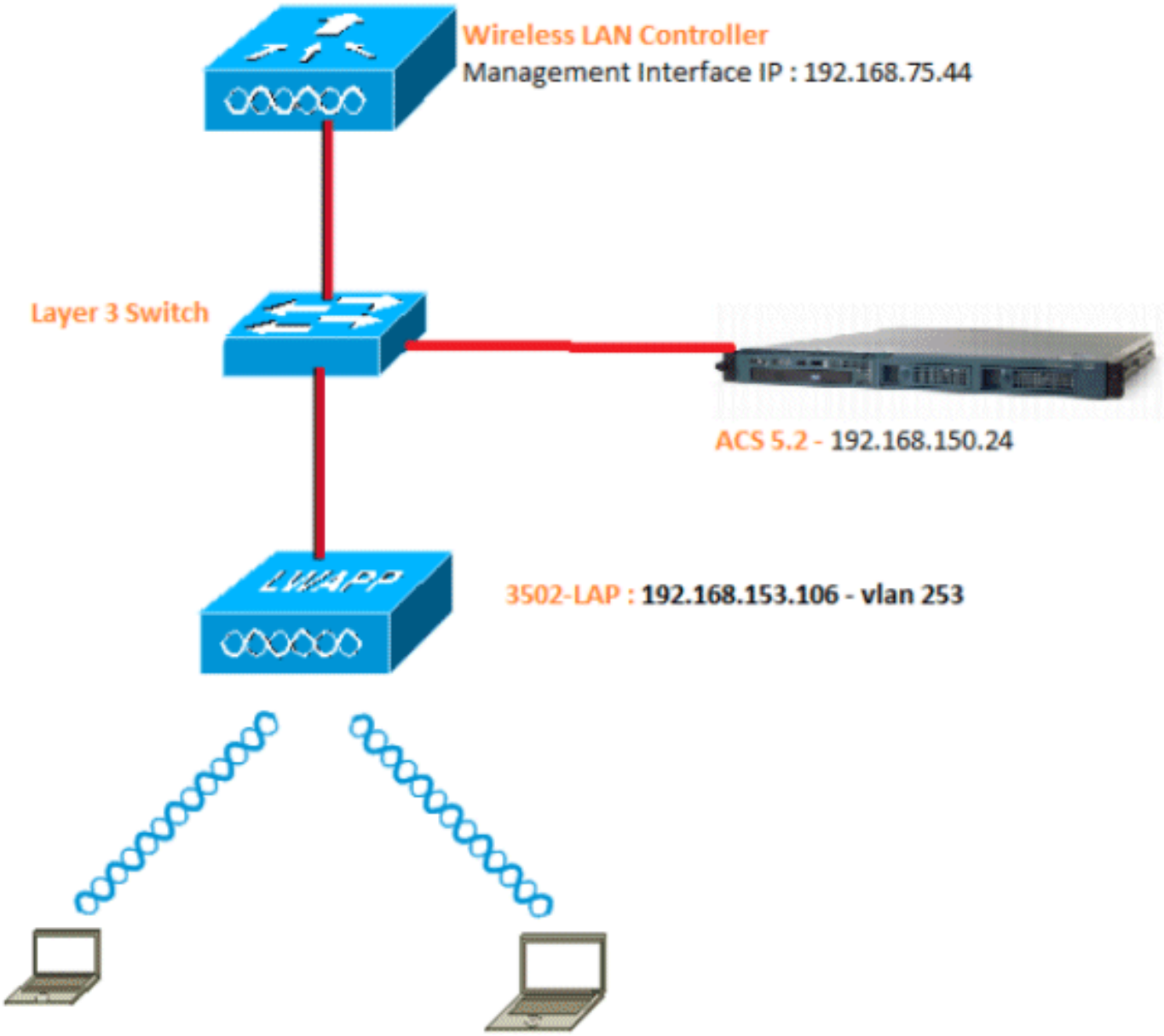
LAP는 제조 시 디바이스에 구워지는 X.509 인증서(개인 키로 서명됨)를 공장에서 출하하여 설치했습니다. LAP는 가입 프로세스에서 WLC를 인증하기 위해 이 인증서를 사용합니다. 이 방법은 LAP를 인증하는 또 다른 방법을 설명합니다. WLC 소프트웨어를 사용하면 Cisco Aironet AP(액세스 포인트)와 Cisco 스위치 간에 802.1x 인증을 구성할 수 있습니다. 이 경우 AP는 802.1x 신청자 역할을 하며 익명 PAC 프로비저닝과 함께 EAP-FAST를 사용하는 RADIUS 서버(ACS)에 대해 스위치에 의해 인증됩니다. 802.1x 인증을 위해 구성된 경우, 스위치에 포트에 연결된 디바이스가 성공적으로 인증될 때까지 802.1x 트래픽 이외의 트래픽은 포트를 통과할 수 없습니다. AP가 WLC에 연결되기 전 또는 WLC에 연결된 후 AP를 인증할 수 있습니다. 이 경우 LAP가 WLC에 연결된 후 스위치에 802.1x를 구성합니다.

구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

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.
- LAP는 VLAN 253에 배치됩니다.
- VLAN 253: 192.168.153.x/24. 게이트웨이: 192.168.153.10
- 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 3가지 카테고리로 구분됩니다.

1. LAP를 구성합니다.
2. 스위치를 구성합니다.
3. RADIUS 서버를 구성합니다.

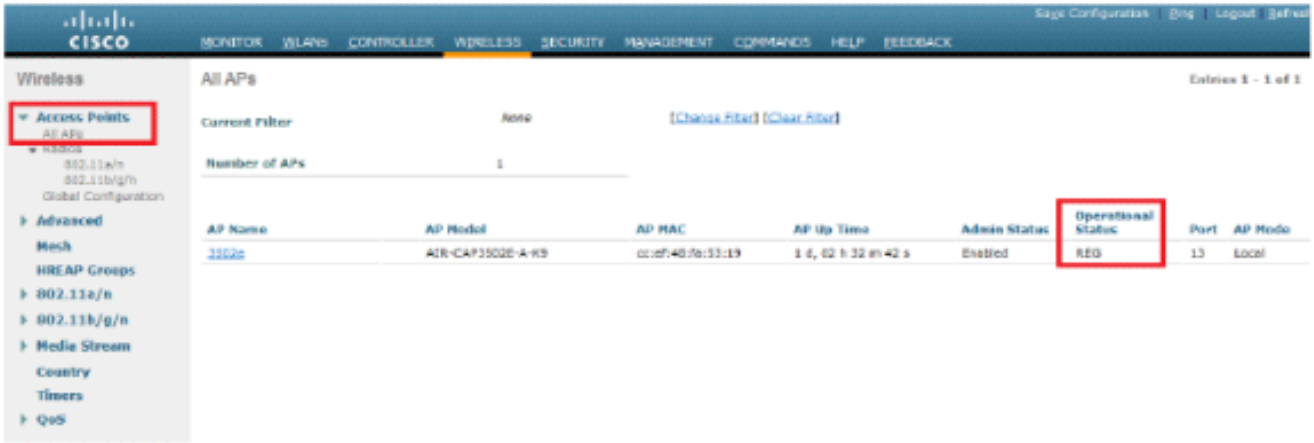
LAP 구성

가정:

LAP는 옵션 43, DNS 또는 정적으로 구성된 WLC 관리 인터페이스 IP를 사용하여 WLC에 이미 등록되었습니다.

다음 단계를 완료하십시오.

1. WLC에서 LAP 등록을 확인하려면 Wireless(무선) > Access Points(액세스 포인트) > All APs(모든 AP)로 이동합니다.

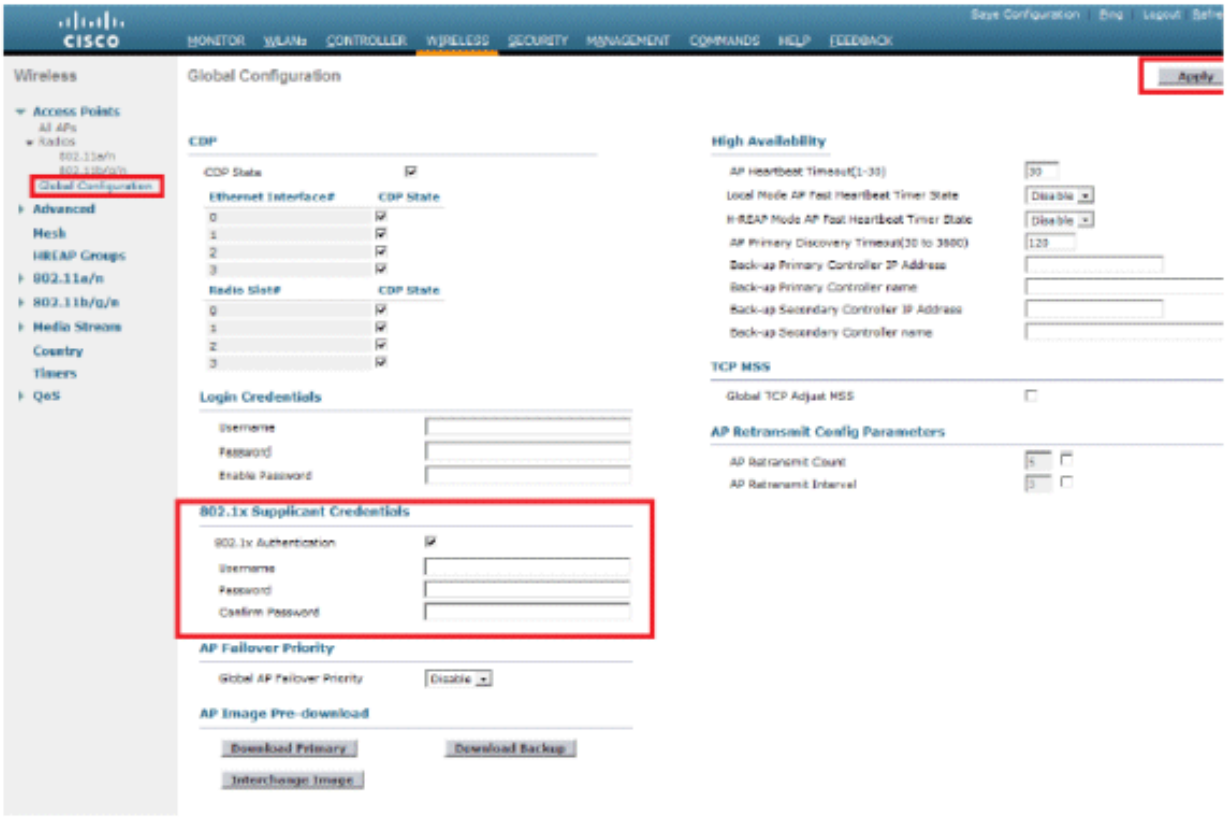


2. 모든 LAP의 802.1x 자격 증명(사용자 이름/비밀번호)을 두 가지 방법으로 구성할 수 있습니다.

   - 전 세계

     이미 조인된 LAP의 경우 WLC에 조인하는 모든 LAP가 이러한 자격 증명을 상속하도록

자격 증명을 전역으로 설정할 수 있습니다.

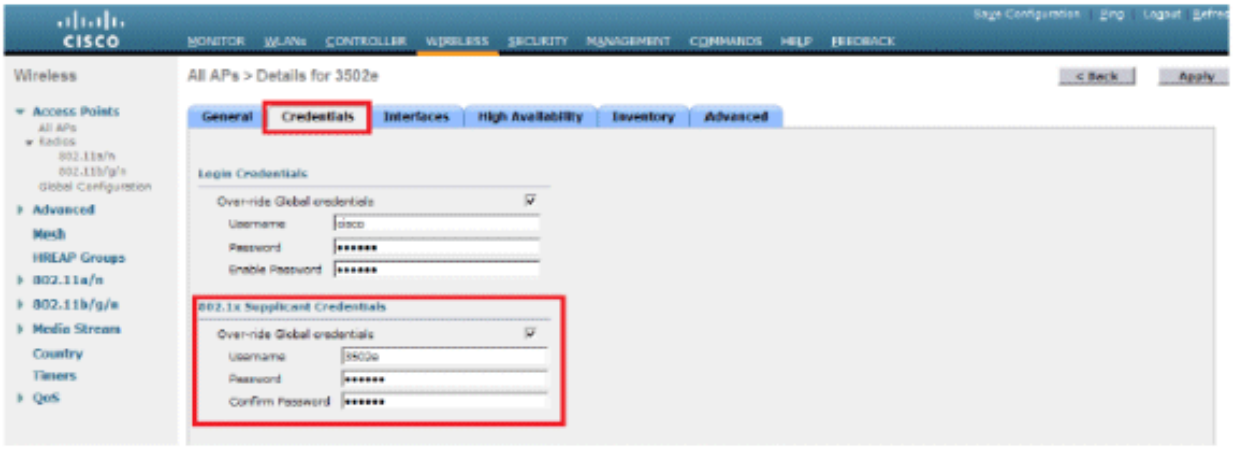


- 개별적으로

AP당 802.1 x 프로필을 구성합니다. 이 예에서는 AP당 자격 증명을 구성합니다.

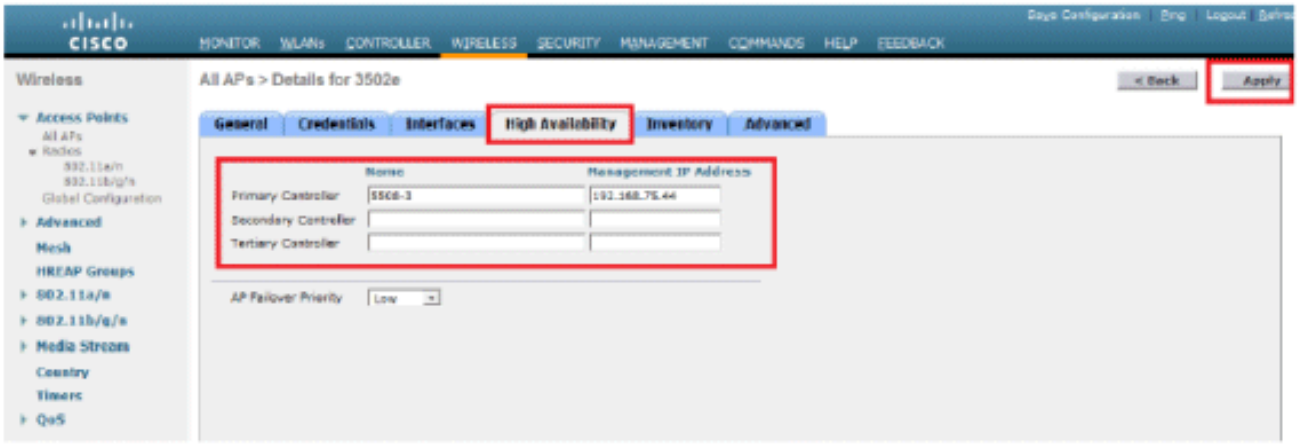
a. Wireless(무선) > All APs(모든 AP)로 이동하여 관련 AP를 선택합니다.

b. 802.1x Supplicant Credentials(신청자 자격 증명) 필드에 사용자 이름 및 비밀번호를 추가합니다.



참고: 로그인 자격 증명은 텔넷, SSH 또는 콘솔에서 AP에 로그인하는 데 사용됩니다.

3. High Availability 섹션을 구성하고 Apply를 클릭합니다.



참고: 저장되면 이러한 자격 증명은 WLC에서 유지되고 AP가 재부팅됩니다. 자격 증명은 LAP가 새 WLC에 조인할 때만 변경됩니다. LAP는 새 WLC에 구성된 사용자 이름 및 비밀번호를 사용합니다.

AP가 아직 WLC에 조인하지 않은 경우 자격 증명을 설정하려면 LAP에 콘솔로 로그인해야 합니다. 활성화 모드에서 다음 CLI 명령을 실행합니다.

LAP#lwapp ap dot1x 사용자 이름 <username> 암호 <password>

또는

LAP#capwap ap dot1x 사용자 이름 <username> 암호 <password>

참고: 이 명령은 복구 이미지를 실행하는 AP에만 사용할 수 있습니다.

LAP의 기본 사용자 이름 및 비밀번호는 각각 `cisco` 및 `Cisco`입니다.

스위치 구성

스위치는 LAP의 인증자 역할을 하며 RADIUS 서버에 대해 LAP를 인증합니다. 스위치에 호환 소프트웨어가 없는 경우 스위치를 업그레이드합니다. 스위치 포트에서 802.1x 인증을 활성화하려면 스위치 CLI에서 다음 명령을 실행합니다.

<#root>

```
switch#
configure terminal
switch(config)#
dot1x system-auth-control
switch(config)#
aaa new-model

!--- Enables 802.1x on the Switch.

switch(config)#
```

```
aaa authentication dot1x default group radius

switch(config)#

radius server host 192.168.150.24 key cisco


!--- Configures the RADIUS server with shared secret and enables switch to send !--- 802.1x information

switch(config)#

ip radius source-interface vlan 253


!--- We are sourcing RADIUS packets from VLAN 253 with NAS IP: 192.168.153.10.

switch(config)interface gigabitEthernet 0/11
switch(config-if)switchport mode access
switch(config-if)switchport access vlan 253
switch(config-if)mls qos trust dscp
switch(config-if)spanning-tree portfast

!--- gig0/11 is the port number on which the AP is connected.

switch(config-if)dot1x pae authenticator

!--- Configures dot1x authentication.

switch(config-if)dot1x port-control auto

!--- With this command, the switch initiates the 802.1x authentication.
```

참고: 동일한 스위치에 다른 AP가 있고 802.1x를 사용하지 않으려는 경우 802.1x에 대해 포트를 구성하지 않은 상태로 두거나 다음 명령을 실행할 수 있습니다.

<#root>

```
switch(config-if)authentication port-control force-authorized
```

RADIUS 서버 구성

LAP는 EAP-FAST로 인증됩니다. Cisco ACS 5.2를 사용하지 않는 경우 사용하는 RADIUS 서버가 이 EAP 방법을 지원하는지 확인합니다.

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 ACS입니다. 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

그 결과 사용자가 네트워크에 액세스할 수 있는 조건 및 특정 조건이 충족될 때 허용되는 권한 수준을 제한할 수 있는 유연성을 제공합니다.

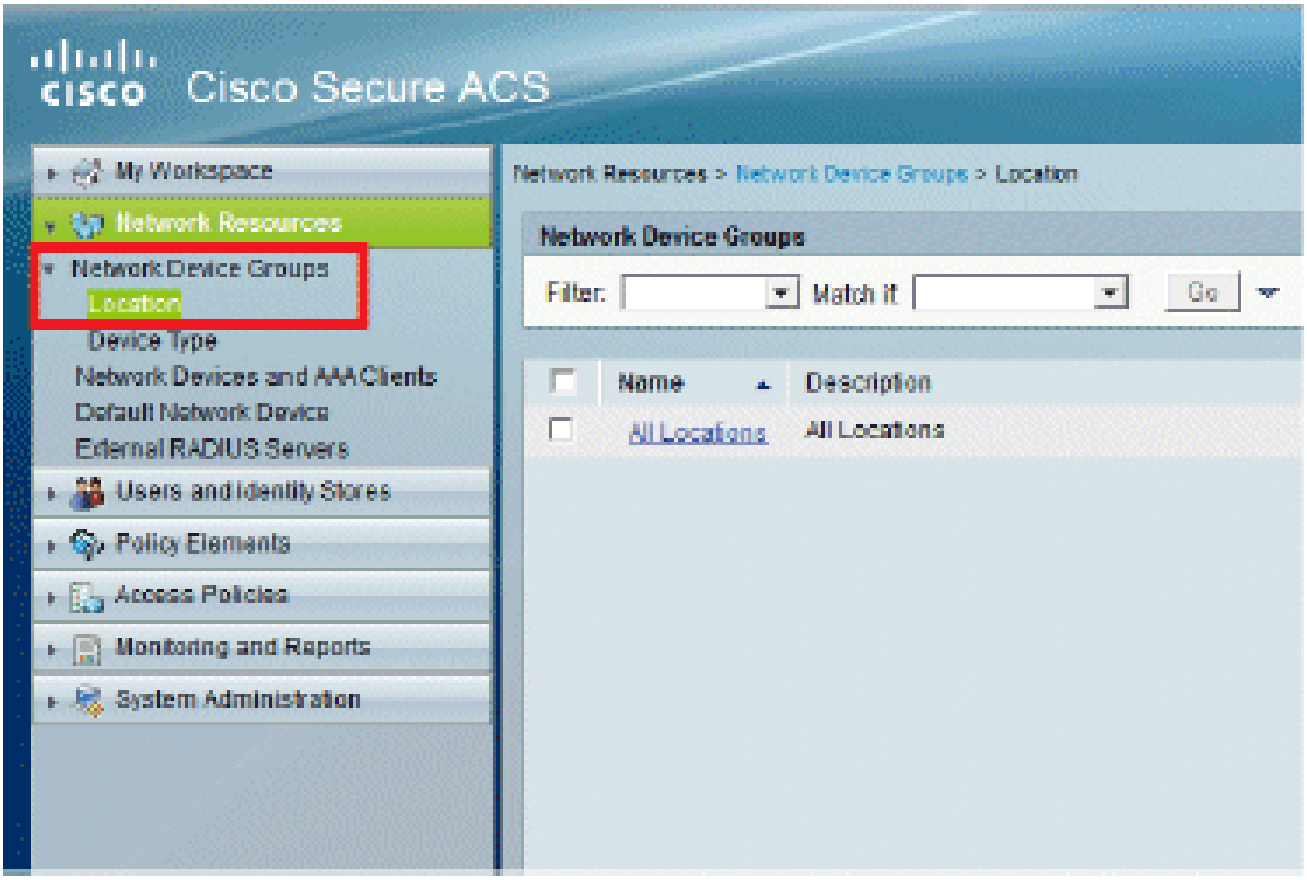
네트워크 리소스 구성

이 섹션에서는 RADIUS 서버의 스위치에 대해 AAA 클라이언트를 구성합니다.

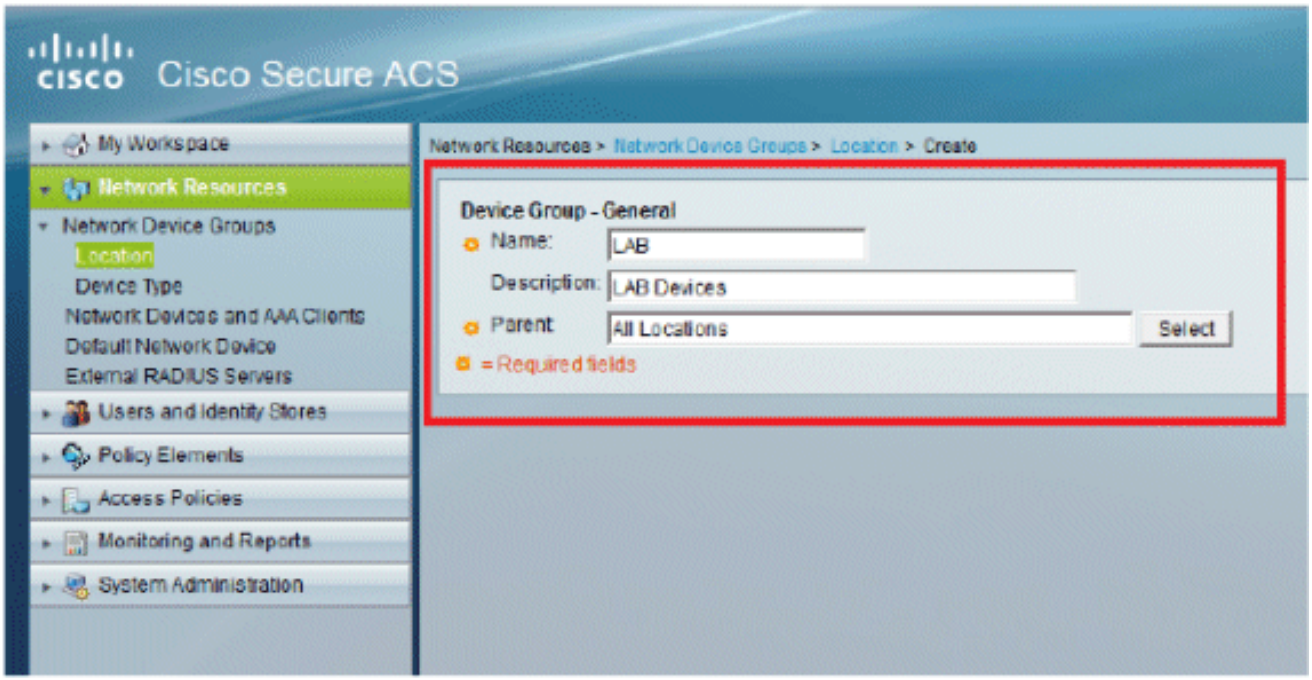
이 절차에서는 스위치가 RADIUS 서버에 LAP의 사용자 자격 증명을 전달할 수 있도록 RADIUS 서버에서 스위치를 AAA 클라이언트로 추가하는 방법에 대해 설명합니다.

다음 단계를 완료하십시오.

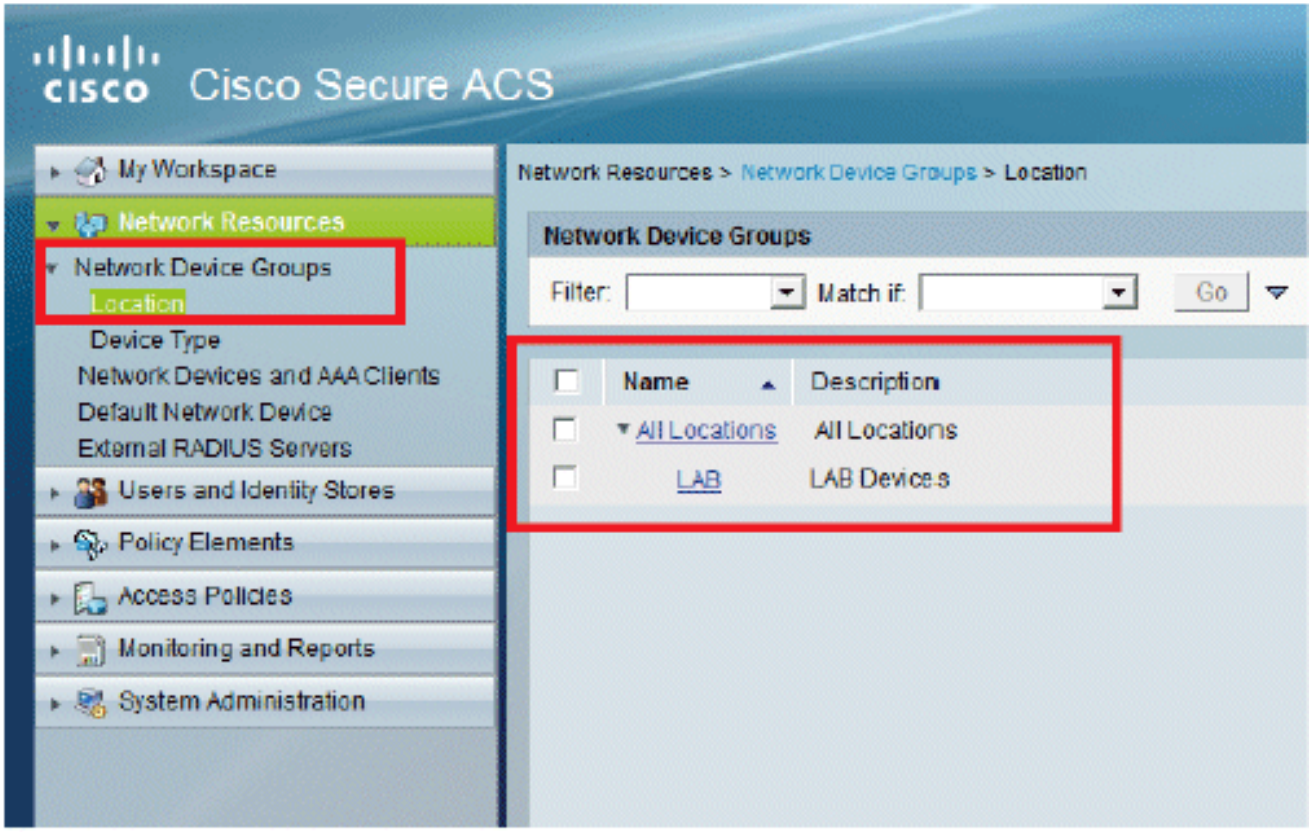
1. ACS GUI에서 Network Resources(네트워크 리소스)를 클릭합니다.
2. Network Device Groups(네트워크 디바이스 그룹)를 클릭합니다.
3. 위치 > 생성(하단)으로 이동합니다.



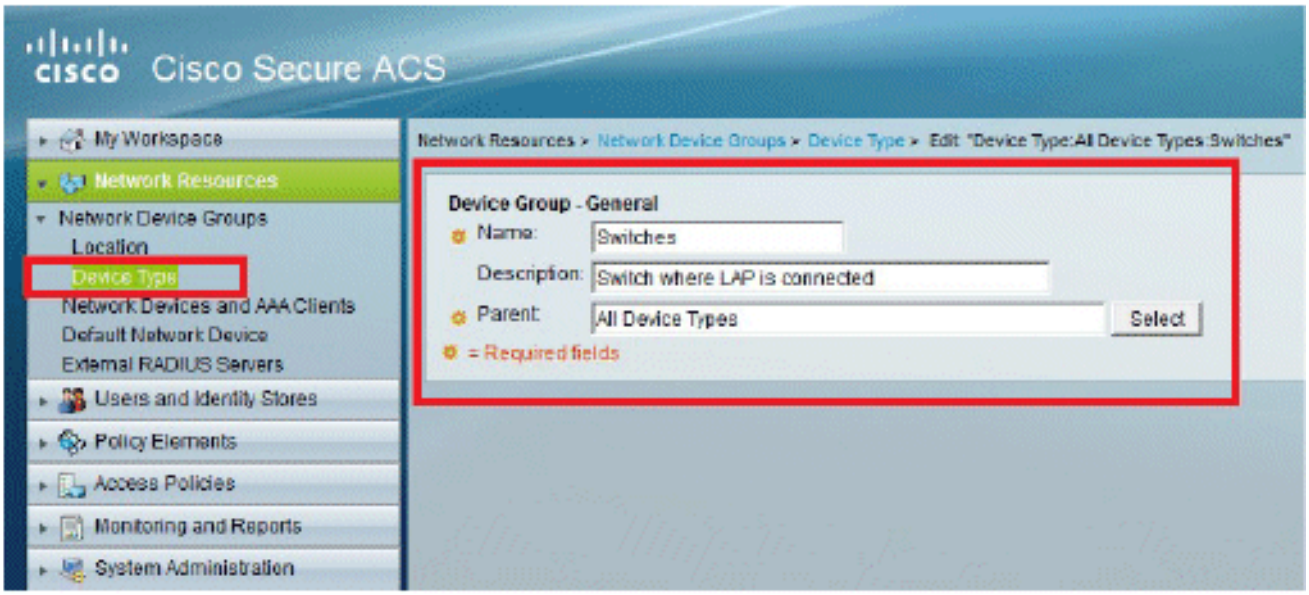
4. 필수 필드를 추가하고 Submit(제출)을 클릭합니다.



5. 창이 업데이트됩니다.



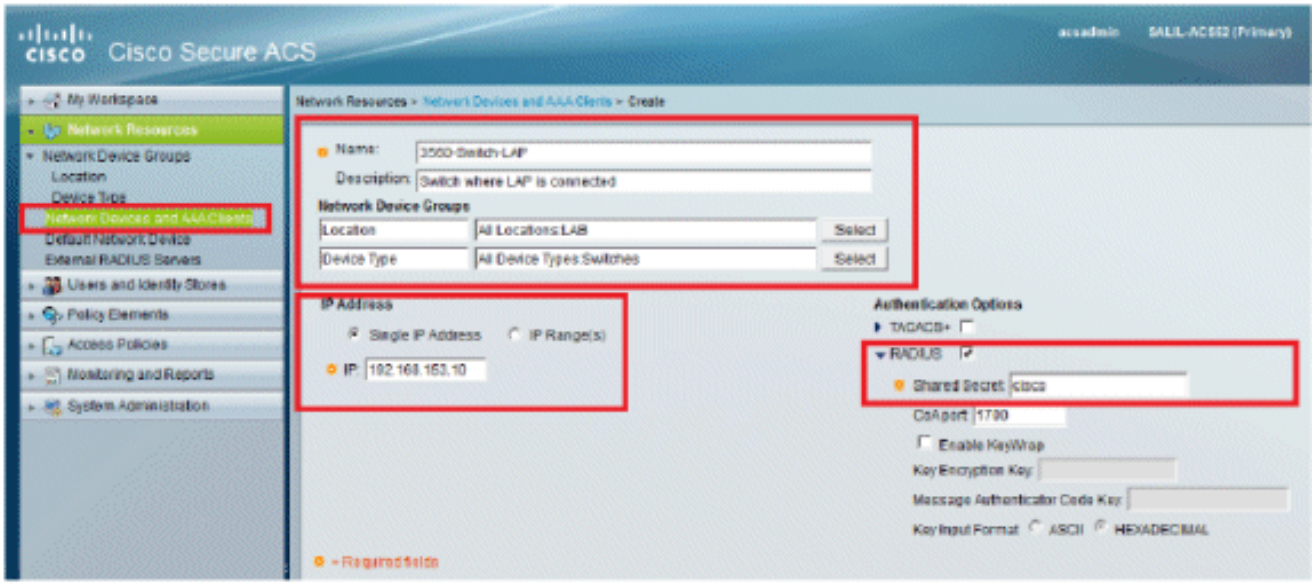
6. Device Type(디바이스 유형) > Create(생성)를 클릭합니다.



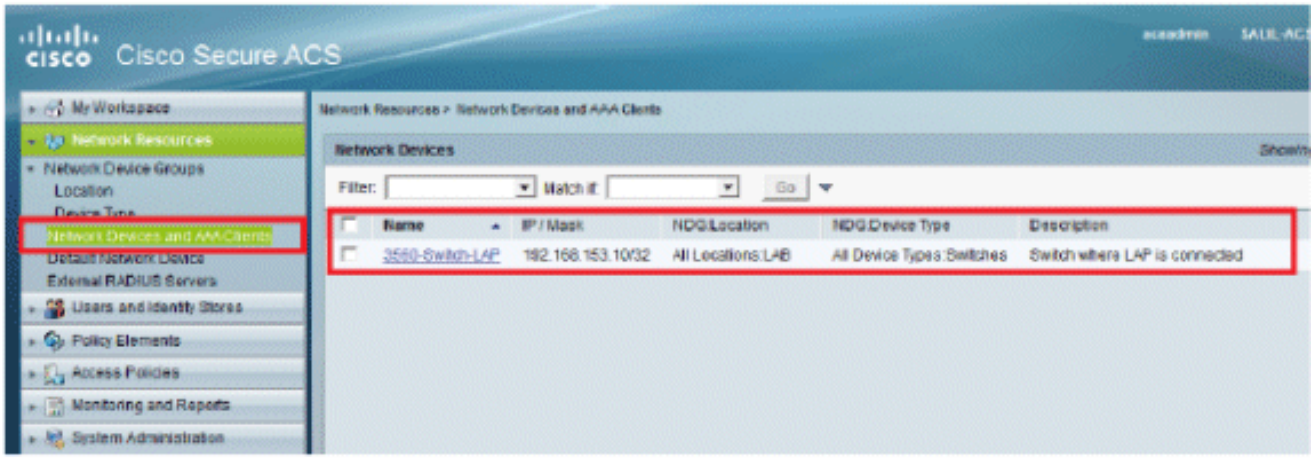
7. Submit(제출)을 클릭합니다. 완료되면 창이 새로 고쳐집니다.

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

9. Create(생성)를 클릭하고 여기에 표시된 대로 세부사항을 입력합니다.



10. Submit(제출)을 클릭합니다. 창이 업데이트됩니다.

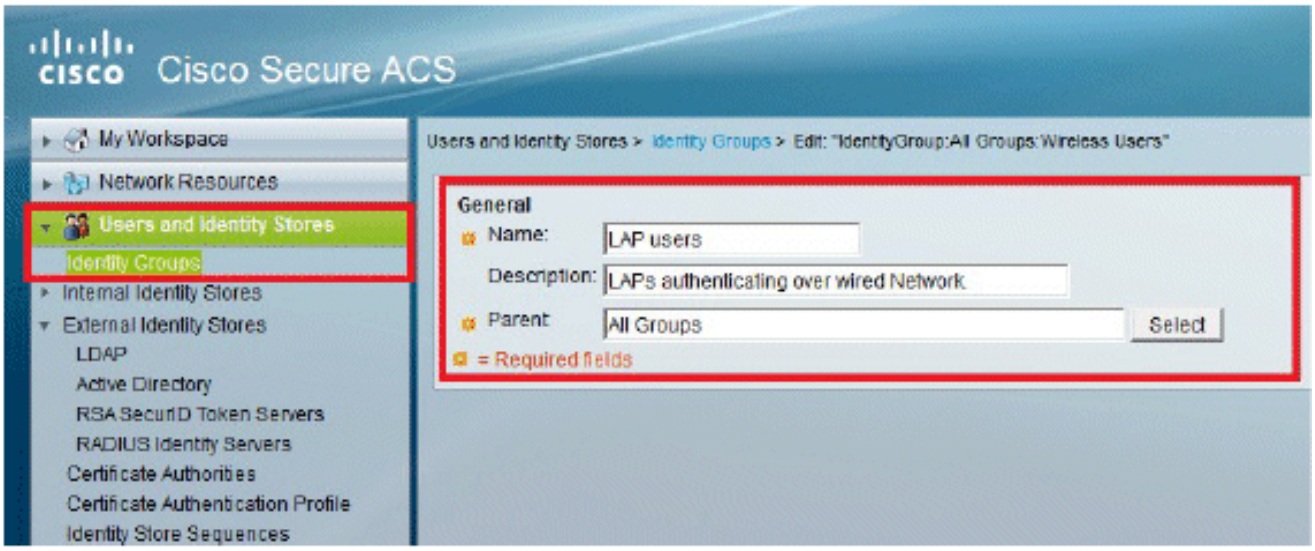


사용자 구성

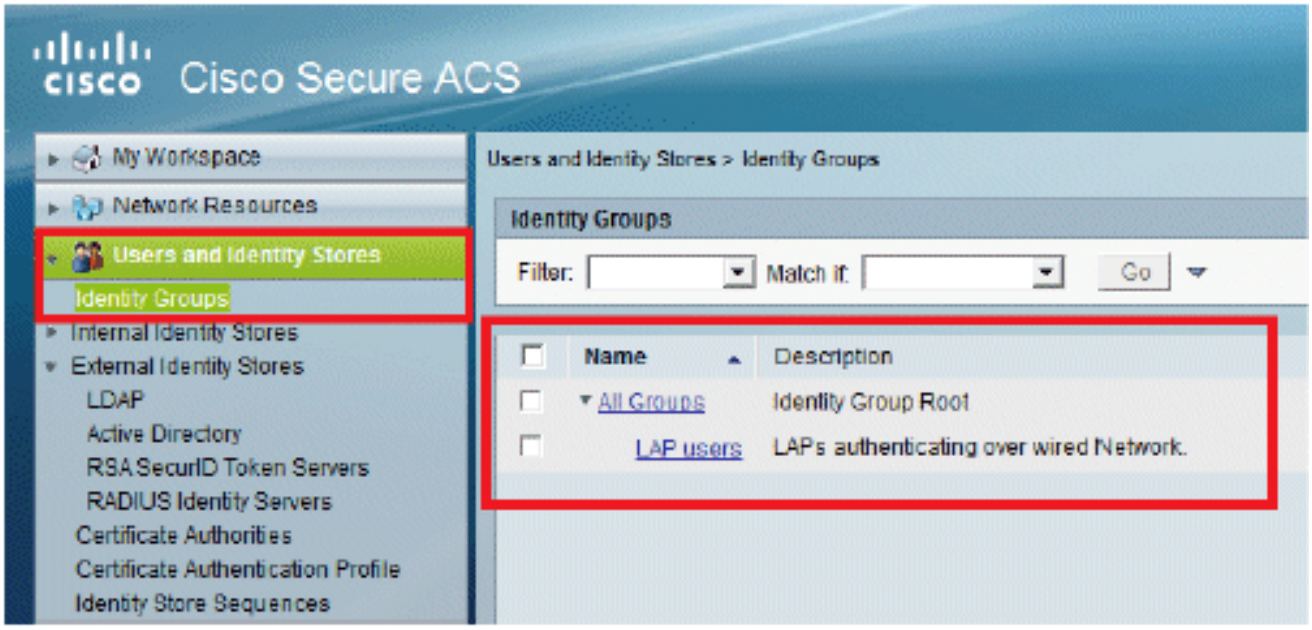
이 섹션에서는 이전에 구성된 ACS에서 사용자를 생성하는 방법을 살펴봅니다. "LAP 사용자"라는 그룹에 사용자를 할당합니다.

다음 단계를 완료하십시오.

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

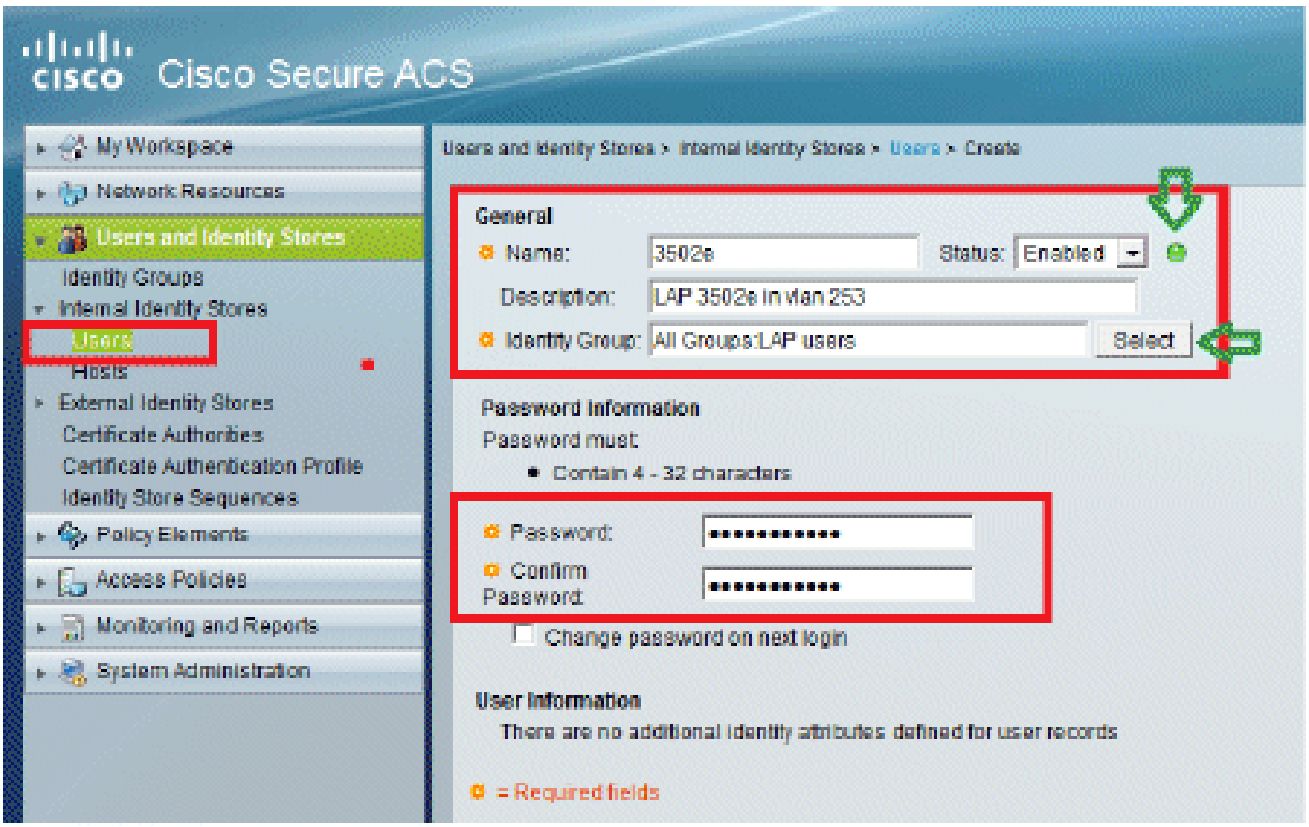


2. Submit(제출)을 클릭합니다.

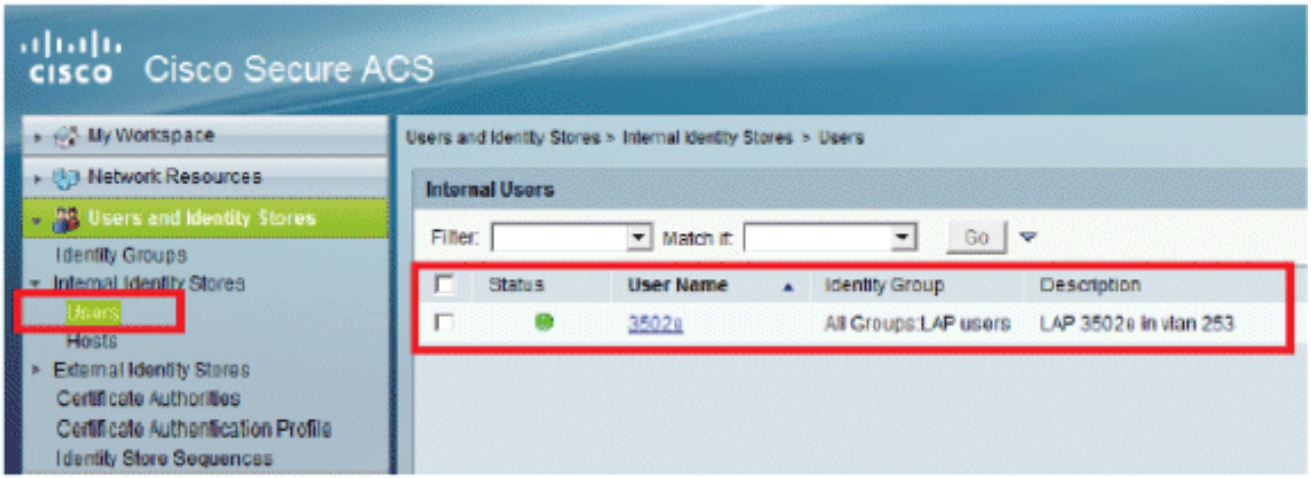


3. 3502e를 생성하고 그룹 "LAP 사용자"에 할당합니다.

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

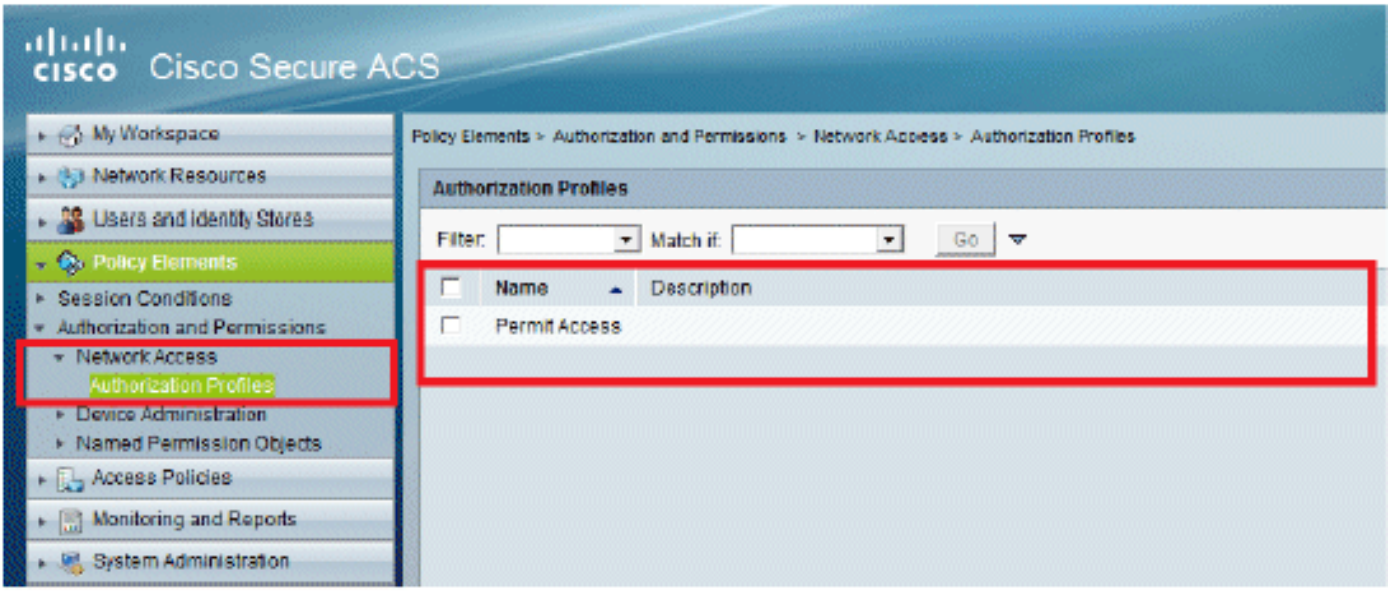


5. 업데이트된 정보가 표시됩니다.



정책 요소 정의

Permit Access(액세스 허용)가 설정되어 있는지 확인합니다.

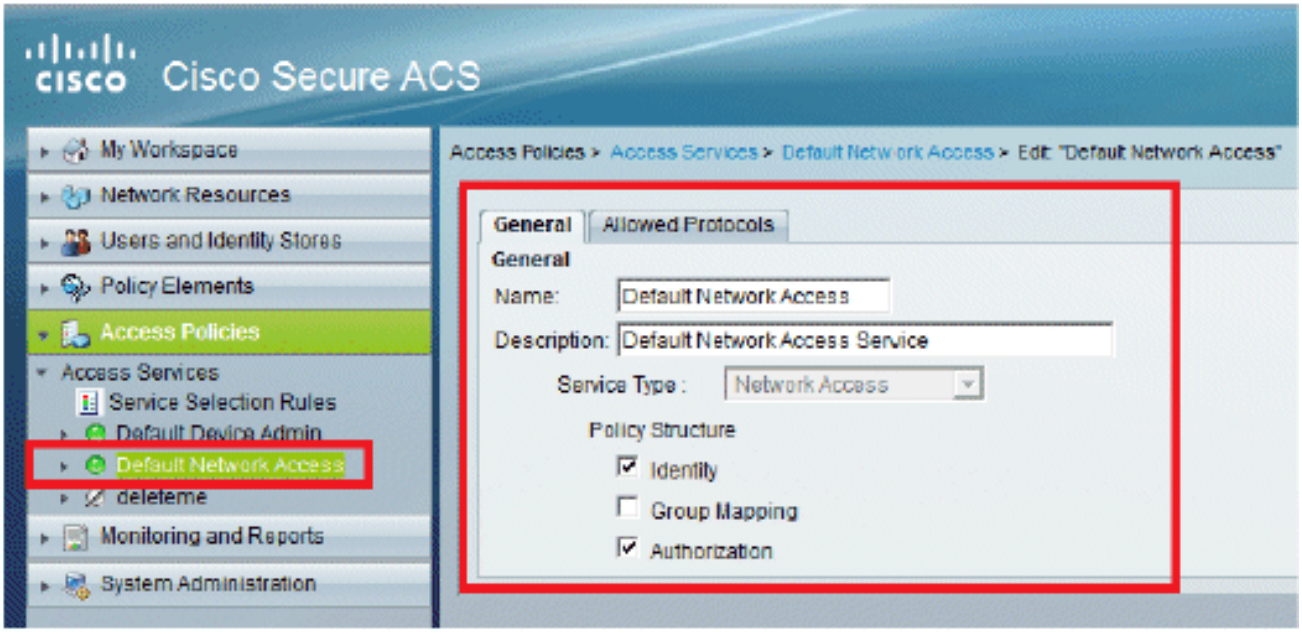


액세스 정책 적용

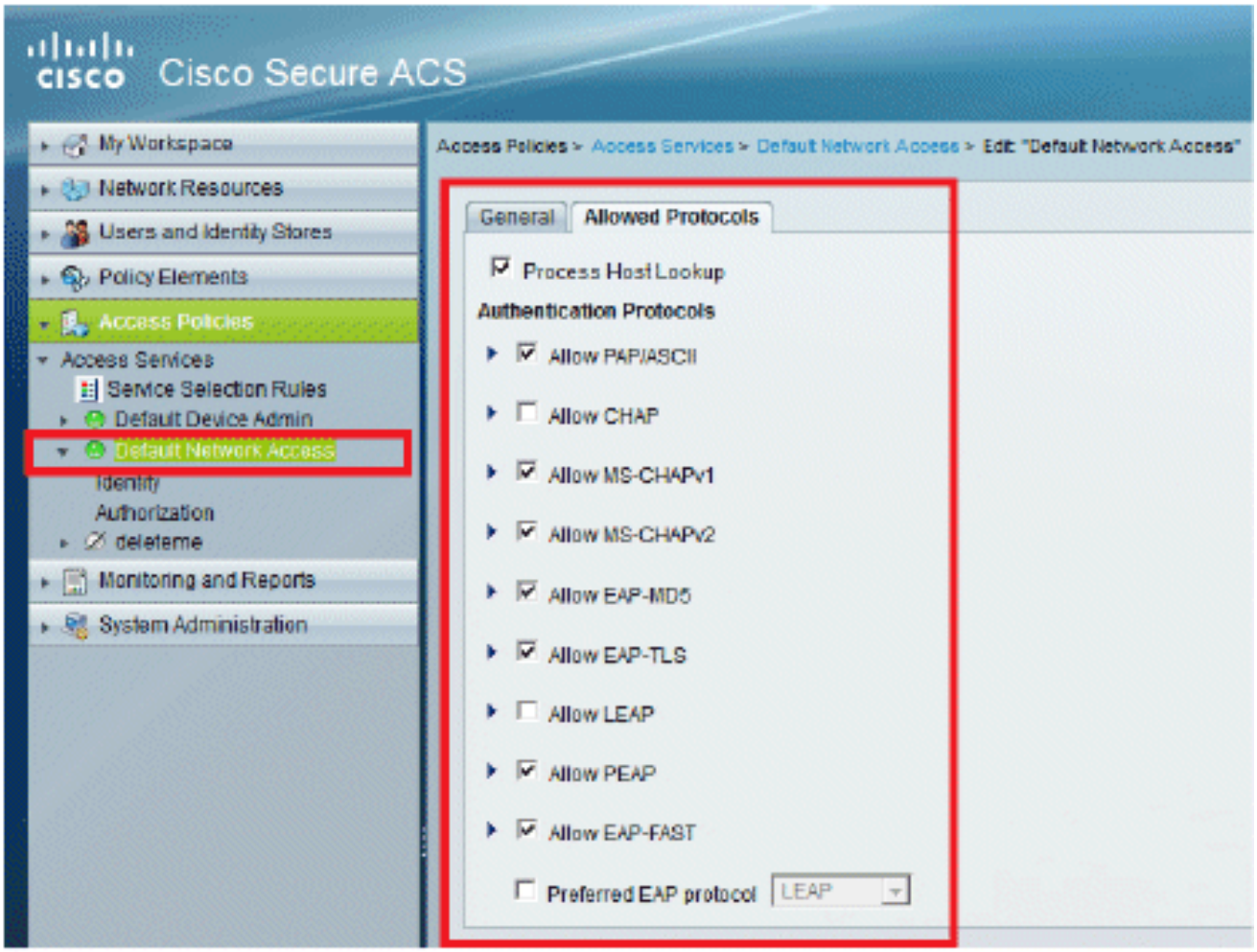
이 섹션에서는 인증을 위해 LAP에 사용되는 인증 방법으로 EAP-FAST를 선택합니다. 그런 다음 이전 단계를 기반으로 규칙을 생성합니다.

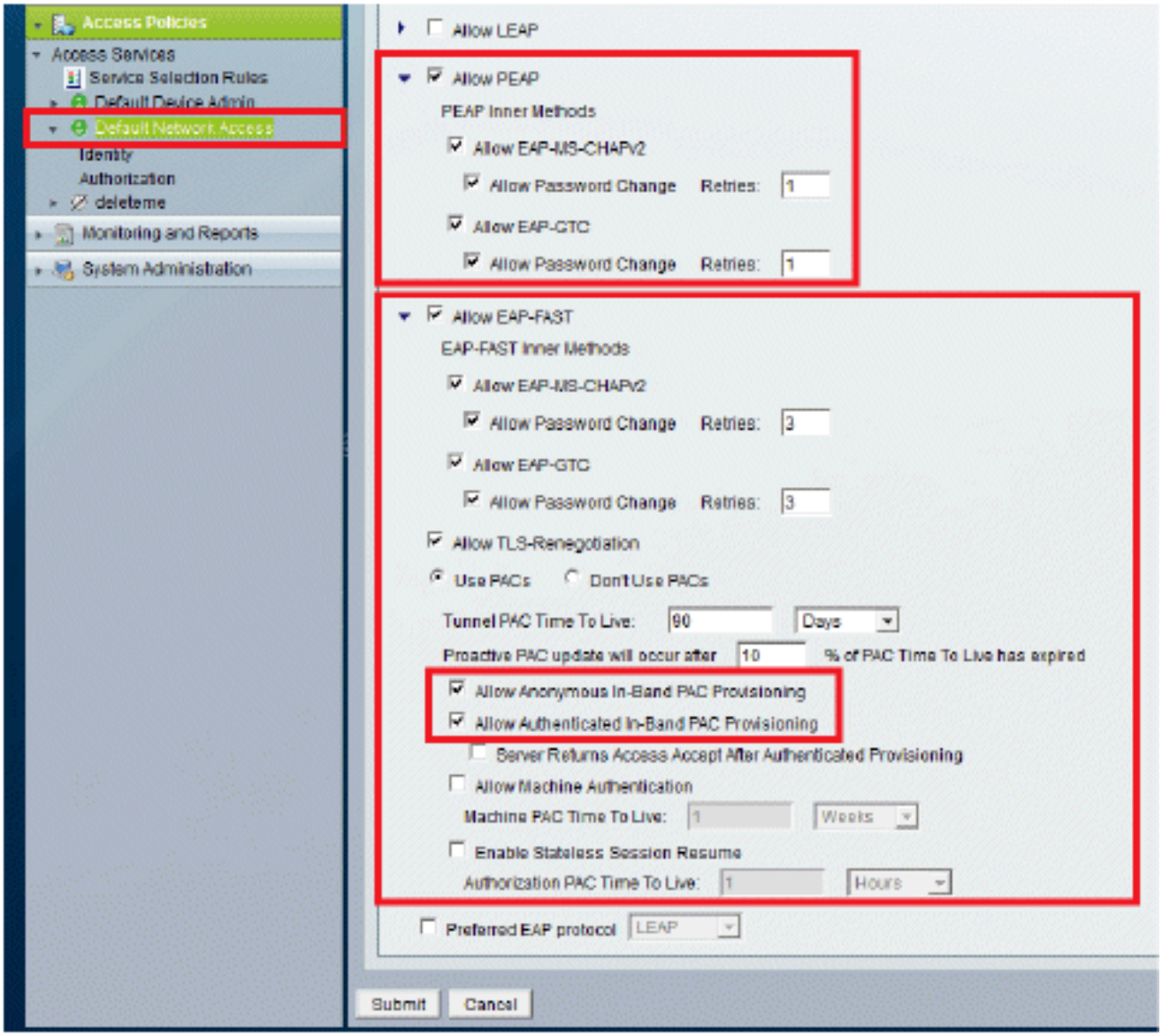
다음 단계를 완료하십시오.

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



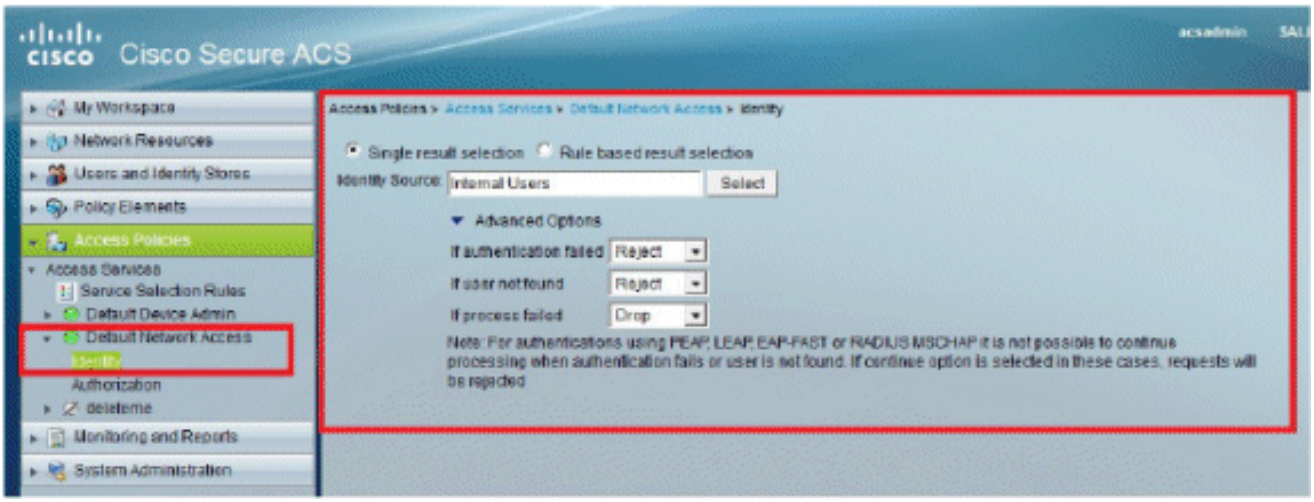
2. EAP-FAST 및 익명 대역 내 PAC 프로비저닝을 활성화했는지 확인합니다.





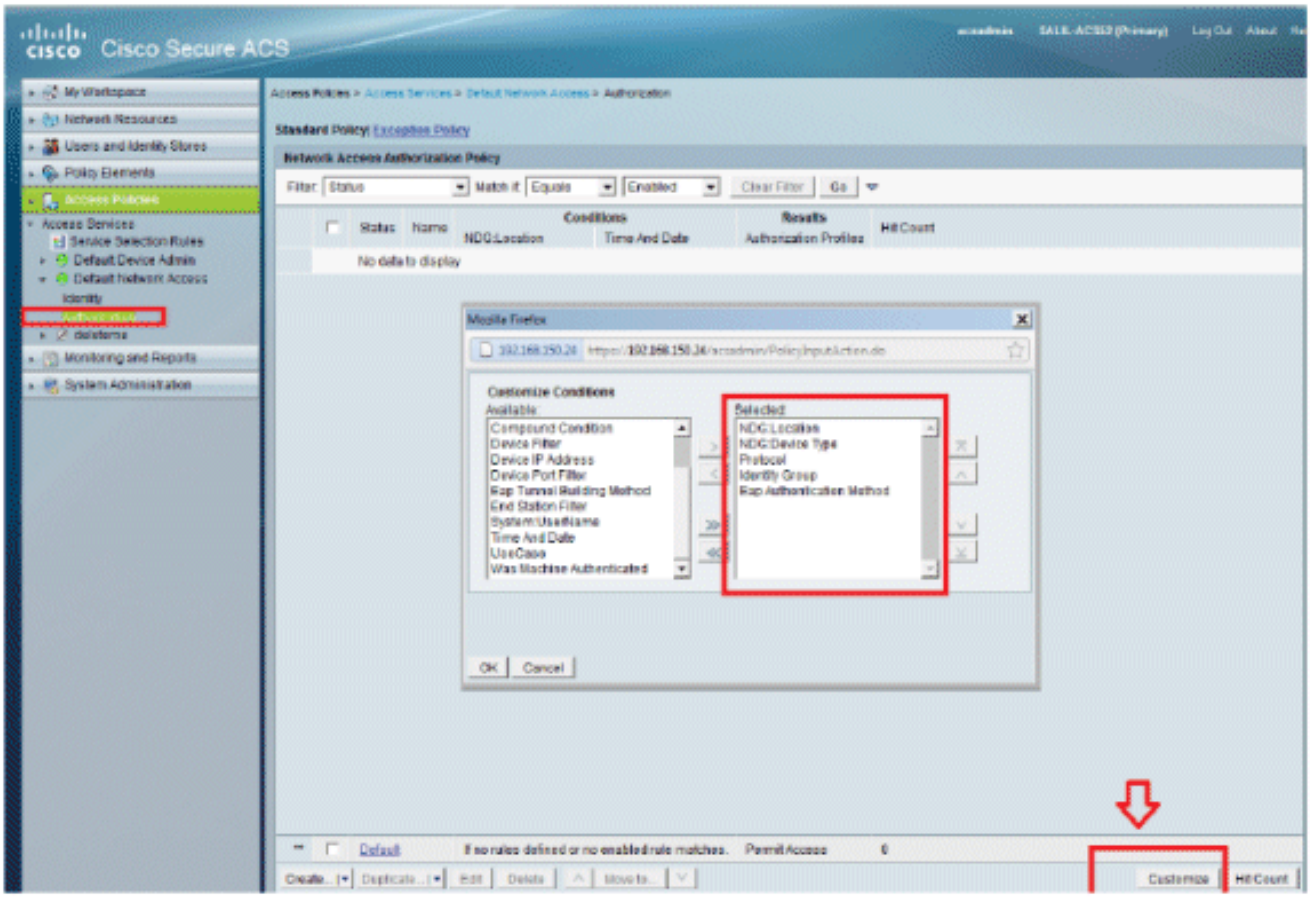
3. Submit(제출)을 클릭합니다.

4. 선택한 ID 그룹을 확인합니다. 이 예에서는 ACS에서 생성된 Internal Users(내부 사용자)를 사용하고 변경 사항을 저장합니다.



5. Access Policies(액세스 정책) > Access Services(액세스 서비스) > Default Network Access(기본 네트워크 액세스) > Authorization(권한 부여)으로 이동하여 권한 부여 프로파일을 확인합니다.

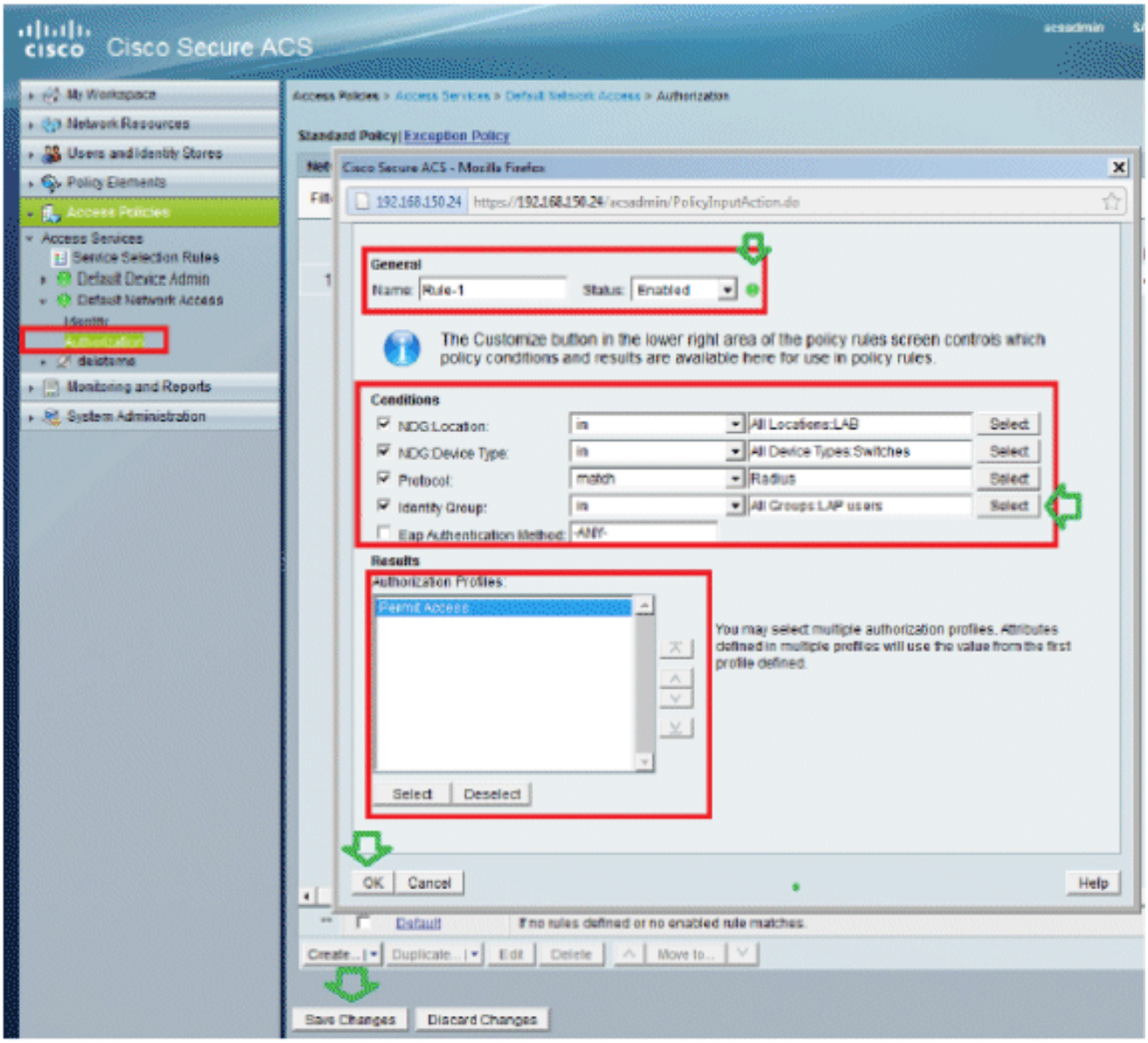
   네트워크에 대한 사용자 액세스를 허용할 조건 및 인증 후 전달 할 인증 프로파일 (특성) 하에서 사용자 정의 할 수 있습니다. 이 세분화는 ACS 5.x에서만 사용할 수 있습니다. 이 예에서는 Location, Device Type, Protocol, Identity Group 및 EAP Authentication Method를 선택합니다.



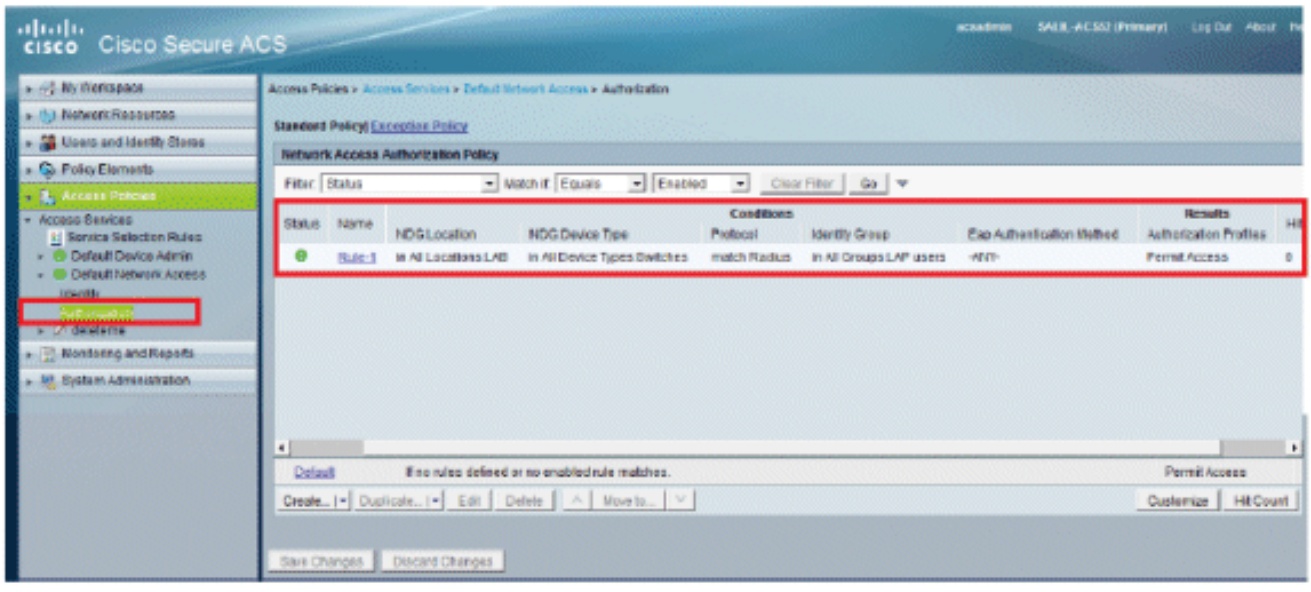
6. OK(확인)를 클릭하고 Save Changes(변경 사항 저장)를 클릭합니다.

7. 다음 단계는 규칙을 생성하는 것입니다. 정의된 규칙이 없으면 조건 없이 LAP에 액세스할 수 있습니다.

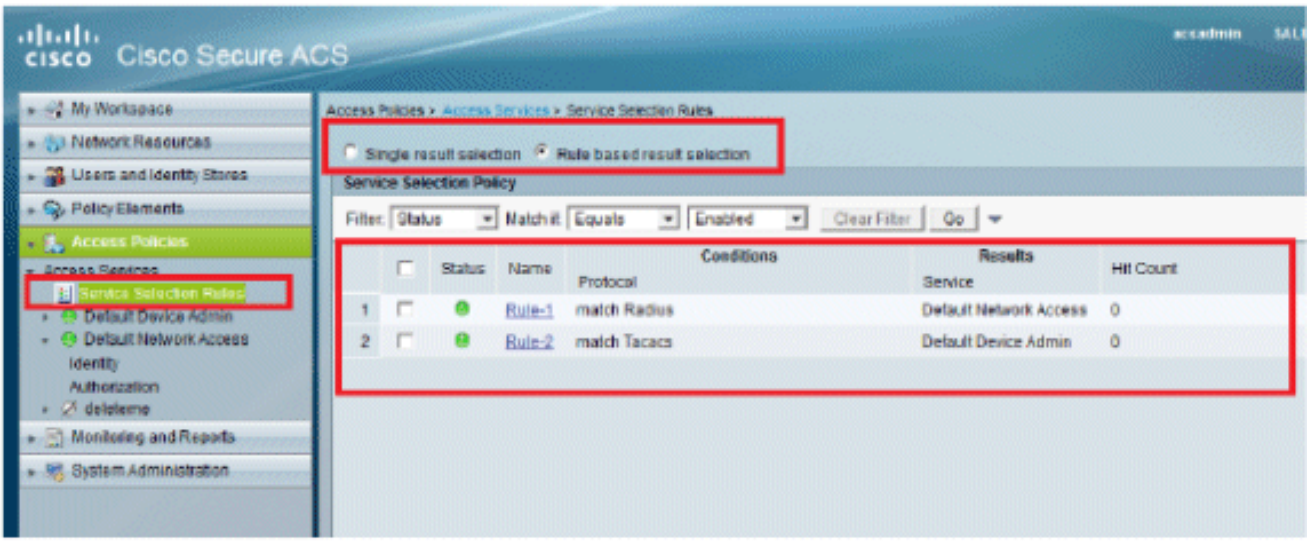
8. Create(생성) > Rule-1을 클릭합니다. 이 규칙은 "LAP 사용자" 그룹의 사용자를 위한 것입니다.



9. Save Changes(변경 사항 저장)를 클릭합니다. 조건과 일치하지 않는 사용자를 거부하도록 하려면 기본 규칙을 편집하여 "Deny Access(액세스 거부)"라고 말합니다.



10. 마지막 단계는 서비스 선택 규칙을 정의하는 것입니다. 이 페이지에서는 수신 요청에 적용할 서비스를 결정하기 위해 단순 또는 규칙 기반 정책을 구성할 수 있습니다. 예를 들면 다음과 같습니다.



다음을 확인합니다.

스위치 포트에서 802.1x가 활성화되면 802.1x 트래픽을 제외한 모든 트래픽이 포트를 통해 차단됩니다. WLC에 이미 등록된 LAP의 연결이 끊어집니다. 802.1x 인증이 성공한 후에만 다른 트래픽이 통과할 수 있습니다. 스위치에서 802.1x가 활성화된 후 WLC에 LAP를 성공적으로 등록하면 LAP 인증이 성공했음을 나타냅니다.

AP 콘솔:

<#root>

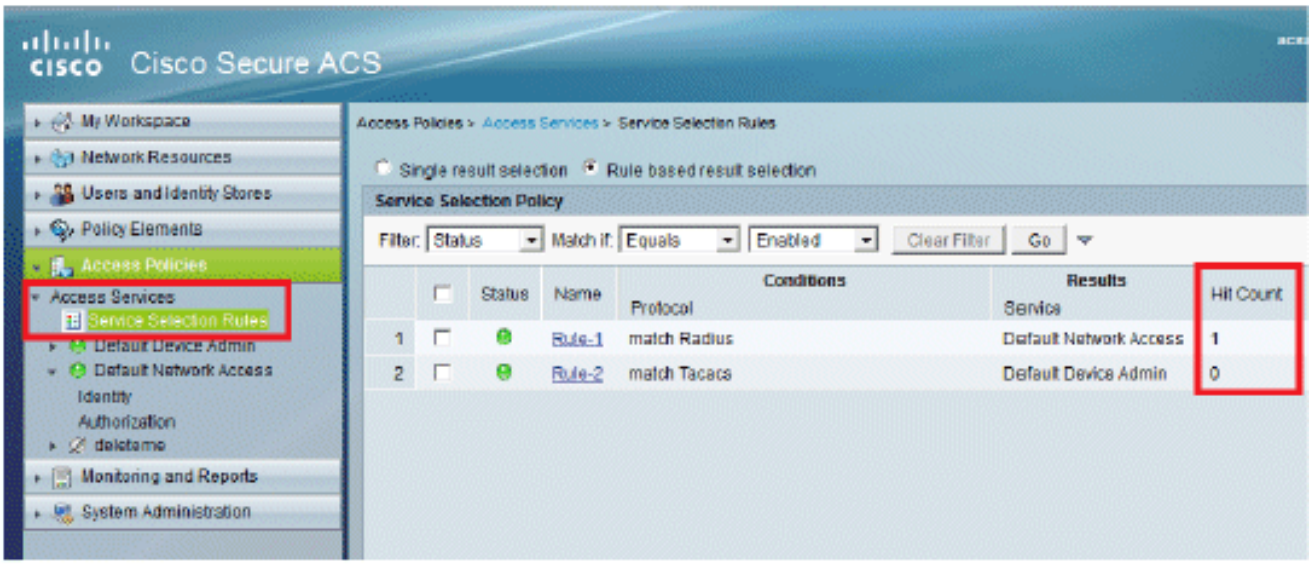
```
*Jan 29 09:10:24.048: %DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to
   192.168.75.44:5246
*Jan 29 09:10:27.049: %DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to
   192.168.75.44:5247

!--- AP disconnects upon adding dot1x information in the gig0/11.

*Jan 29 09:10:30.104: %WIDS-5-DISABLED: IDS Signature is removed and disabled.
*Jan 29 09:10:30.107: %CAPWAP-5-CHANGED: CAPWAP changed state to DISCOVERY
*Jan 29 09:10:30.107: %CAPWAP-5-CHANGED: CAPWAP changed state to DISCOVERY
*Jan 29 09:10:30.176: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
   administratively down
*Jan 29 09:10:30.176: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to
   administratively down
*Jan 29 09:10:30.186: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
   reset
*Jan 29 09:10:30.201: %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to up
*Jan 29 09:10:30.211: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Jan 29 09:10:30.220: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to
   reset
Translating "CISCO-CAPWAP-CONTROLLER"...domain server (192.168.150.25)
*Jan 29 09:10:36.203: status of voice_diag_test from WLC is false

*Jan 29 09:11:05.927: %DOT1X_SHIM-6-AUTH_OK: Interface GigabitEthernet0 authenticated [EAP-FAST] *Jan 29
```

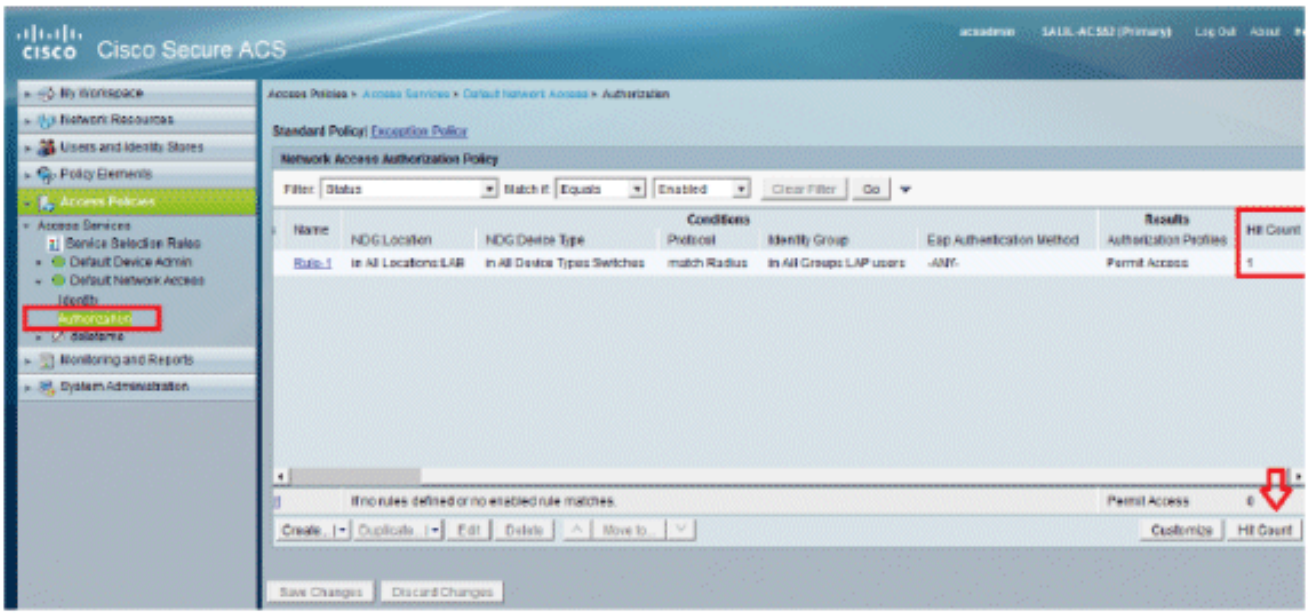
```
!--- Authentication is successful and the AP gets an IP.

Translating "CISCO-CAPWAP-CONTROLLER.Wlab"...domain server (192.168.150.25)
*Jan 29 09:11:37.000: %CAPWAP-5-DTLSREQSEND: DTLS connection request sent
   peer_ip: 192.168.75.44 peer_port: 5246
*Jan 29 09:11:37.000: %CAPWAP-5-CHANGED: CAPWAP changed state to
*Jan 29 09:11:37.575: %CAPWAP-5-DTLSREQSUCC: DTLS connection created
   successfully peer_ip: 192.168.75.44 peer_port: 5246
*Jan 29 09:11:37.578: %CAPWAP-5-SENDJOIN: sending Join Request to 192.168.75.44


*Jan 29 09:11:37.578: %CAPWAP-5-CHANGED: CAPWAP changed state to JOIN


*Jan 29 09:11:37.748: %CAPWAP-5-CHANGED: CAPWAP chan
wmmAC status is FALSEged state to CFG
*Jan 29 09:11:38.890: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to
   down
*Jan 29 09:11:38.900: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
   reset
*Jan 29 09:11:38.900: %CAPWAP-5-CHANGED: CAPWAP changed state to UP
*Jan 29 09:11:38.956: %CAPWAP-5-JOINEDCONTROLLER: AP has joined controller
   5508-3
*Jan 29 09:11:39.013: %CAPWAP-5-DATA_DTLS_START: Starting Data DTLS handshake.
   Wireless client traffic will be blocked until DTLS tunnel is established.
*Jan 29 09:11:39.013: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Jan 29 09:11:39.016: %LWAPP-3-CLIENTEVENTLOG: SSID goa added to the slot[0]
*Jan 29 09:11:39.028: %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to
   down
*Jan 29 09:11:39.038: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to
   reset
*Jan 29 09:11:39.054: %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to up
*Jan 29 09:11:39.060: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to
   down
*Jan 29 09:11:39.069: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
   reset
*Jan 29 09:11:39.085: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Jan 29 09:11:39.135: %LWAPP-3-CLIENTEVENTLOG: SSID goa added to the slot[1]DTLS
   keys are plumbed successfully.
*Jan 29 09:11:39.151: %CAPWAP-5-DATA_DTLS_ESTABLISHED: Data DTLS tunnel
   established.
*Jan 29 09:11:39.161: %WIDS-5-ENABLED: IDS Signature is loaded and enabled

!--- AP joins the 5508-3 WLC.
```

ACS 로그:

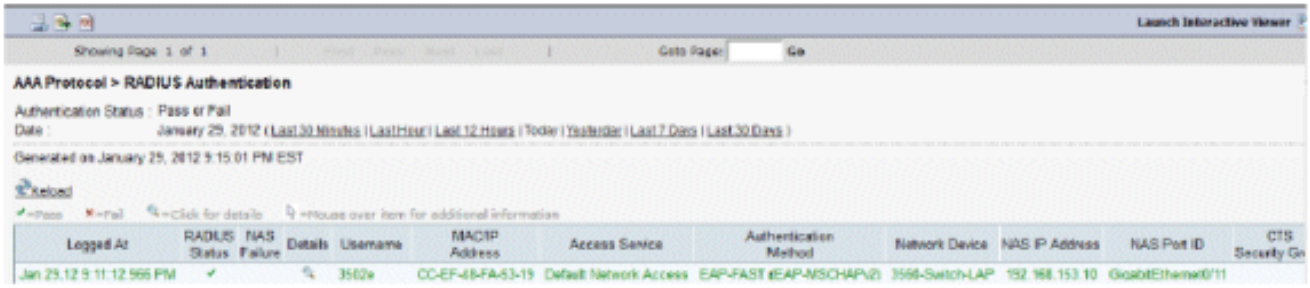
1. 적중 횟수 보기:

   인증 후 15분 내에 로그를 확인하는 경우 Hit Count를 새로 고쳐야 합니다. 같은 페이지의 하단에 Hit Count(적중 횟수) 탭이 있습니다.





2. Monitoring and Reports(모니터링 및 보고서)를 클릭하면 새 팝업 창이 나타납니다. Authentications -RADIUS -Today를 클릭합니다. 어떤 서비스 선택 규칙이 적용되었는지 확인하기 위해 Details를 클릭할 수도 있습니다.



문제 해결

현재 이 설정에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- Cisco Secure Access Control System
- 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.