Catalyst 9800 WLC 및 ISE에서 포스처 구성

목차

소개

이 문서에서는 GUI(Graphic User Interface)를 통해 Catalyst 9800 WLC 및 ISE에서 포스처 WLAN을 구성하는 방법을 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 9800 WLC 일반 컨피그레이션
- ISE 정책 및 프로필 컨피그레이션

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 9800 WLC Cisco IOS® XE Cupertino v17.9.5
- ISE(Identity Service Engine) v3.2
- 랩톱 Windows 10 Enterprise

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

무선 LAN 컨트롤러 RADIUS NAC 및 CoA 기능 흐름

1. 클라이언트가 dot1x 인증을 사용하여 인증합니다.

2. RADIUS Access Accept(RADIUS 액세스 수락)는 포트 80에 대한 리디렉션된 URL 및 IP 주소 및 포트 허용 또는 VLAN 격리를 포함하는 사전 인증 ACL을 전달합니다.

3. 클라이언트가 액세스 승인에 제공된 URL로 리디렉션되고 보안 상태 검증이 완료될 때까지 새 상태가 됩니다. 이 상태의 클라이언트는 ISE 서버와 통신하며 ISE NAC 서버에 구성된 정책과 비교하여 자신을 검증합니다.

4. 클라이언트의 NAC 에이전트가 상태 검증(포트 80으로의 트래픽)을 시작합니다. 에이전트는 액세스 수락에서 제공된 URL로 컨트롤러가 리디렉션하는 포트 80에 HTTP 검색 요청을 보냅니다. ISE는 클라이언트가 연결을 시도하고 클라이언트에 직접 응답한다는 것을 알고 있습니다. 이렇게 하면 클라이언트가 ISE 서버 IP에 대해 알게 되고 이제부터 클라이언트가 ISE 서버와 직접 통신합니다.

5. ACL이 이 트래픽을 허용하도록 구성되어 있으므로 WLC에서 이 트래픽을 허용합니다. VLAN 재정의의 경우 트래픽이 ISE 서버에 도달하도록 브리지됩니다.

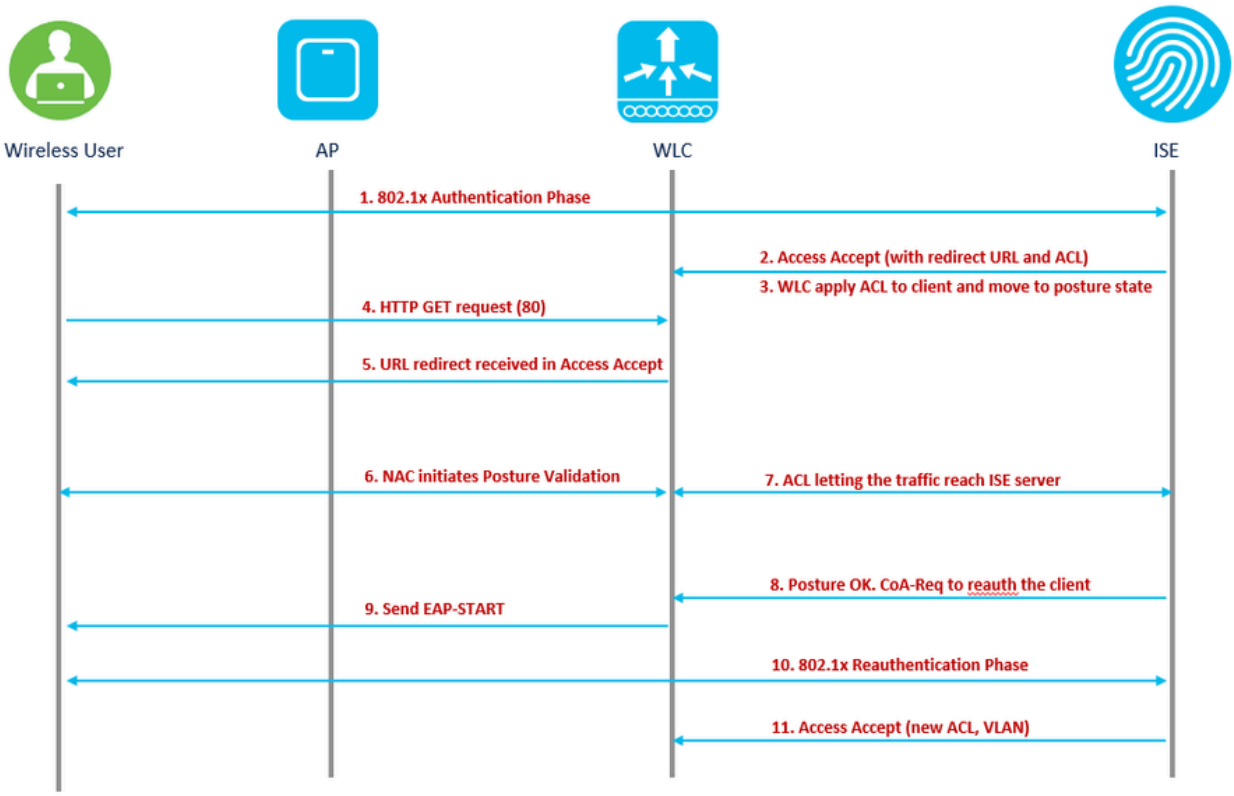
6. ISE 클라이언트가 평가를 완료하면 RADIUS CoA-Req(재인증 서비스 포함)가 WLC로 전송됩니다. 이렇게 하면 EAP-START를 전송하여 클라이언트의 재인증이 시작됩니다. 재인증이 성공하면 ISE는 새 ACL(있는 경우)과 URL 리디렉션 없음 또는 액세스 VLAN을 사용하여 액세스 승인을 보냅니다.

7. WLC는 RFC 3576에 따라 CoA-Req 및 Disconnect-Req를 지원합니다. RFC 5176에 따라 WLC는 재인증 서비스를 위해 CoA-Req를 지원해야 합니다.

8. 다운로드 가능한 ACL 대신 사전 구성된 ACL이 WLC에서 사용됩니다. ISE 서버는 컨트롤러에 이미 구성된 ACL 이름만 전송합니다.

9. 이 설계는 VLAN 및 ACL 케이스 모두에 적용됩니다. VLAN 재정의의 경우 포트 80이 리디렉션되고 격리 VLAN의 나머지 트래픽을 허용합니다(브리지). ACL의 경우 액세스 수락에서 수신한 사전 인증 ACL이 적용됩니다.

이 그림에서는 이 기능 흐름을 시각적으로 보여줍니다.



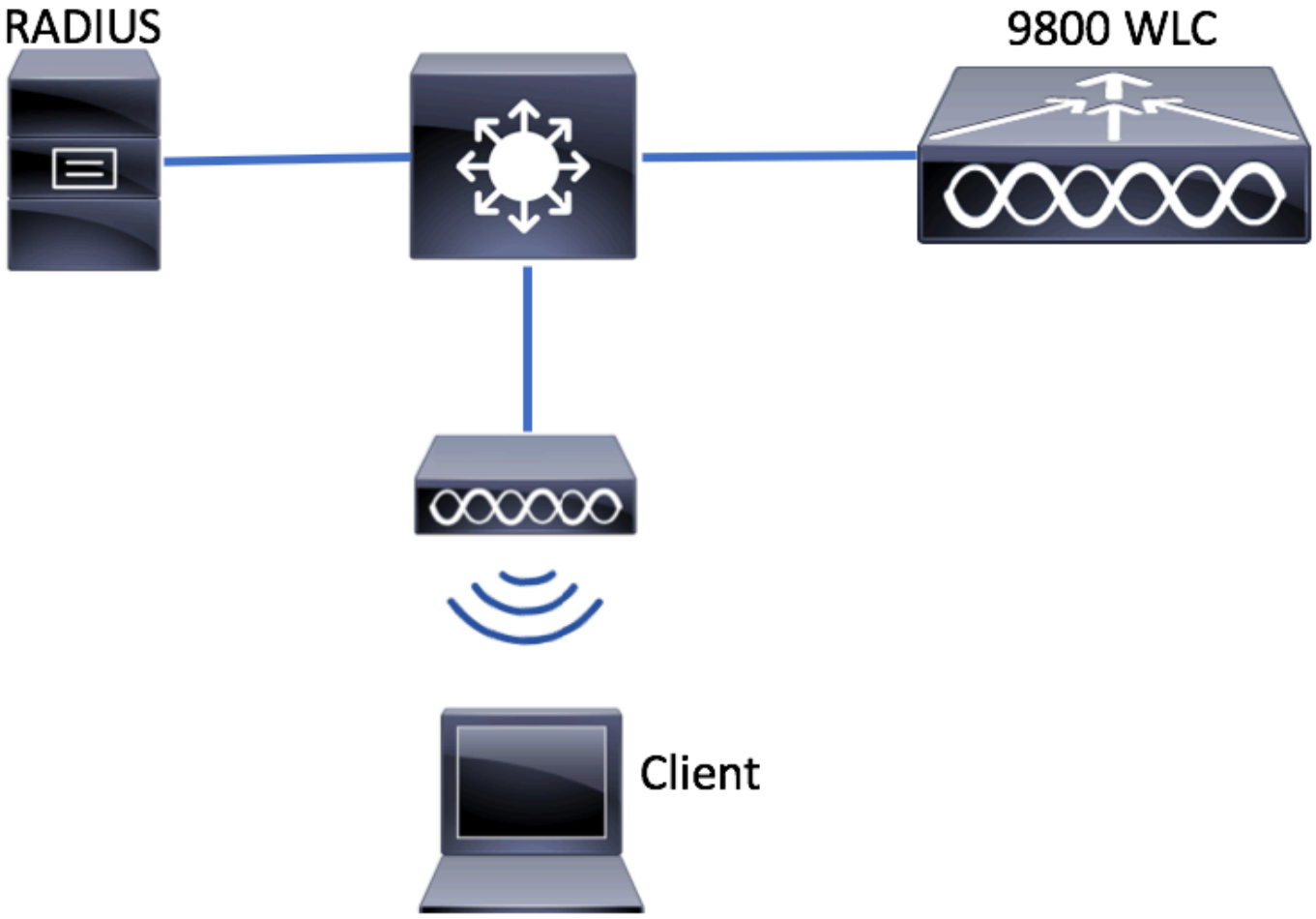
기능 워크플로

이 활용 사례에서는 기업 사용자에게만 사용되는 SSID가 포스처에 대해 활성화됩니다. BYOD, 게스트 등 다른 사용 사례는 이 SSID에 없습니다.

무선 클라이언트가 처음으로 Posture SSID에 연결하는 경우 ISE의 리디렉션된 포털에 Posture Module을 다운로드하여 설치해야 하며, 마지막으로 포스처 확인 결과(Compliant/Non-Compliant)에 따라 관련 ACL을 적용해야 합니다.

구성

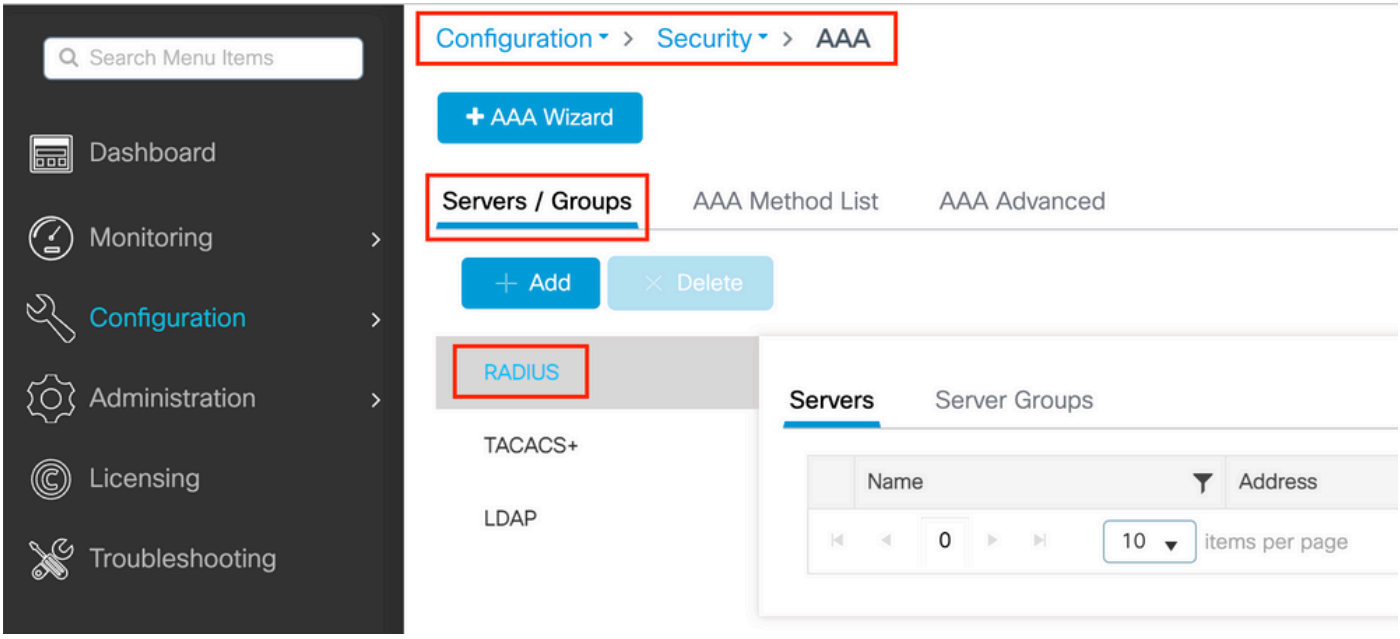
네트워크 다이어그램



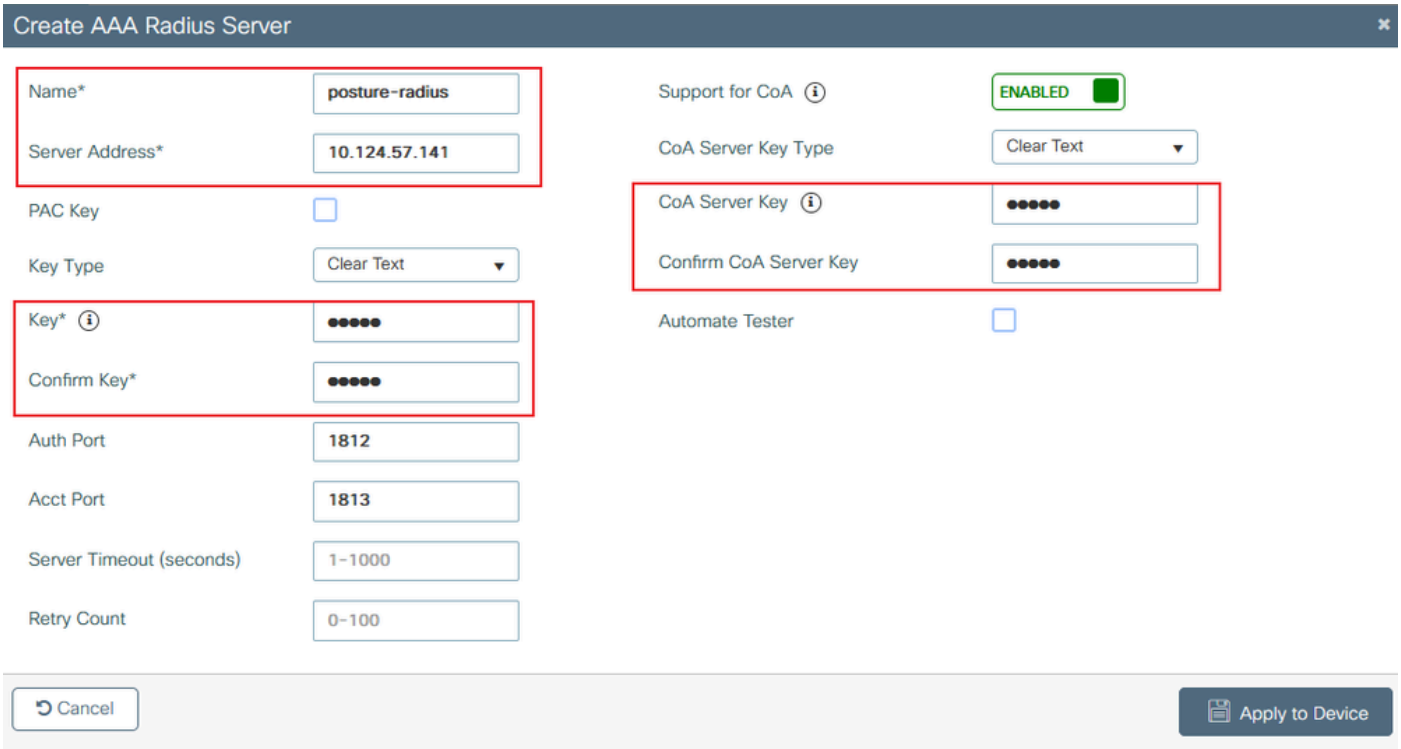
네트워크 다이어그램

9800 WLC의 AAA 구성

1단계. 9800 WLC 컨피그레이션에 ISE 서버를 추가합니다. Configuration(컨피그레이션) > Security(보안) > AAA > Servers/Groups(서버/그룹) > RADIUS > Servers(서버) > + Add(추가)로 이동하고 이미지에 표시된 대로 RADIUS 서버 정보를 입력합니다. CoA에 대한 지원은 상태 NAC에 대해 활성화 되어 있는지 확인 하십시오.

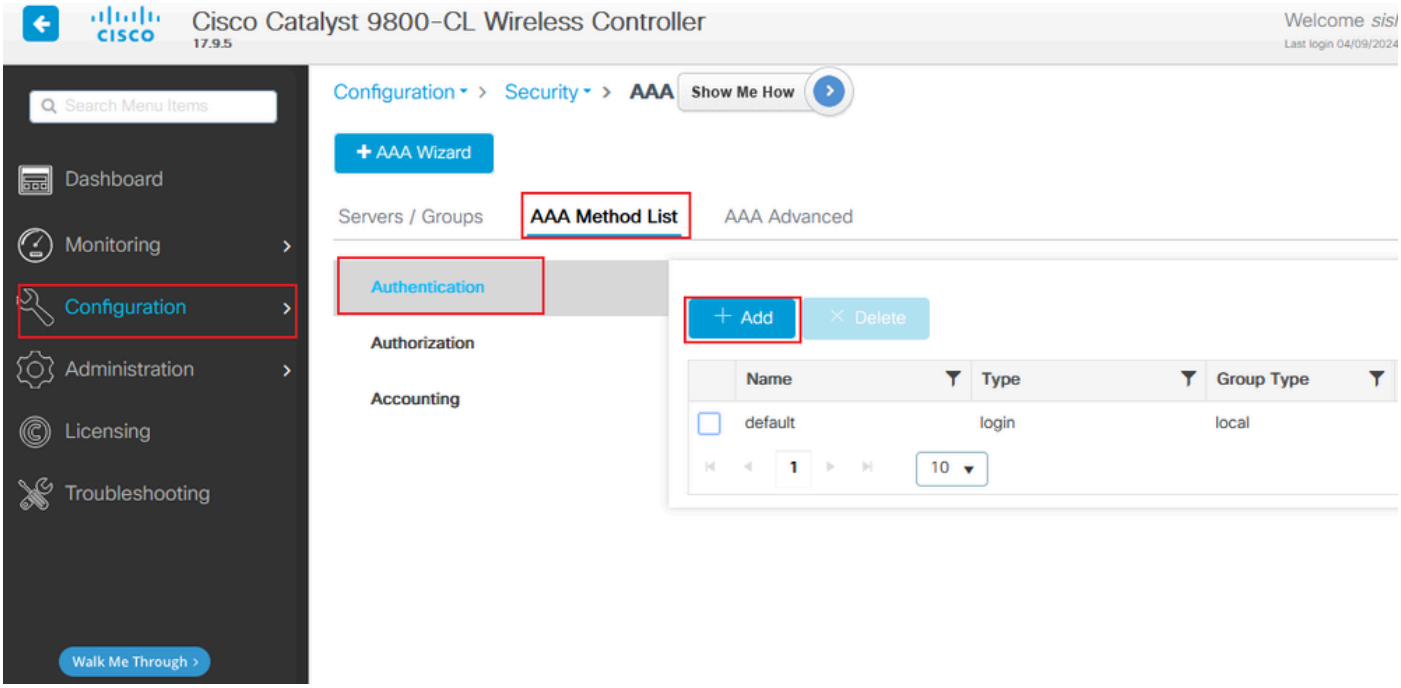


9800 radius 서버 생성

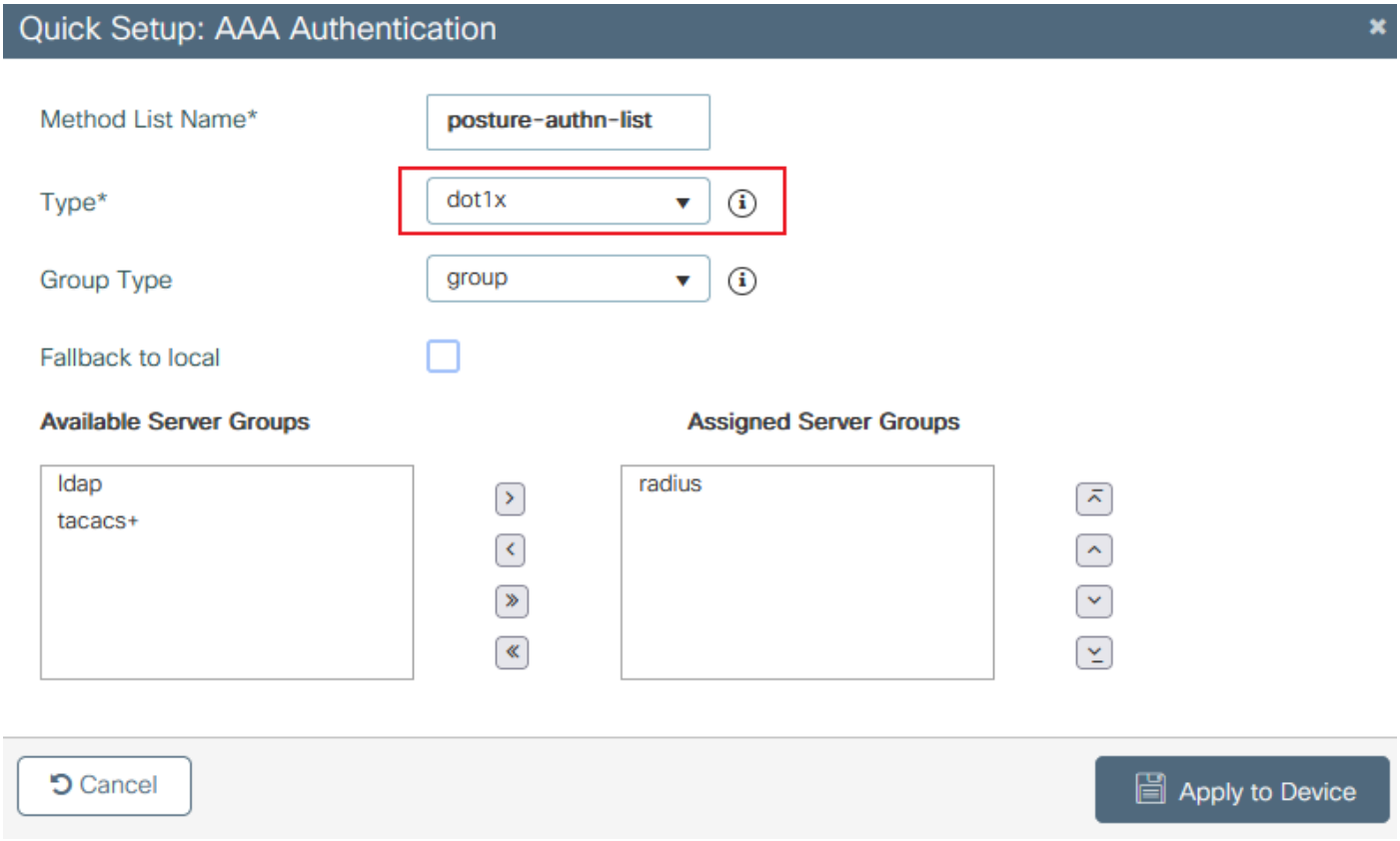


9800 radius 세부 정보 생성

2단계. 인증 방법 목록을 생성합니다. 이미지에 표시된 대로 Configuration > Security > AAA > AAA Method List > Authentication > + Add로 이동합니다.

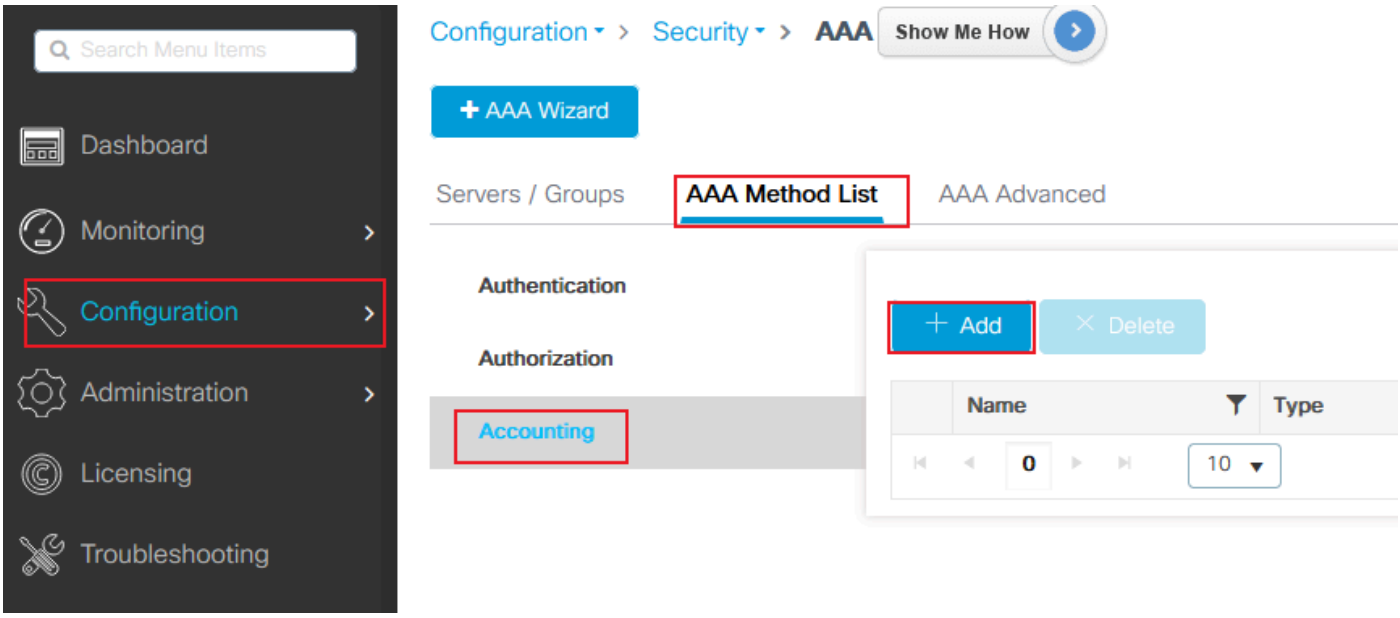


9800 인증 목록 추가

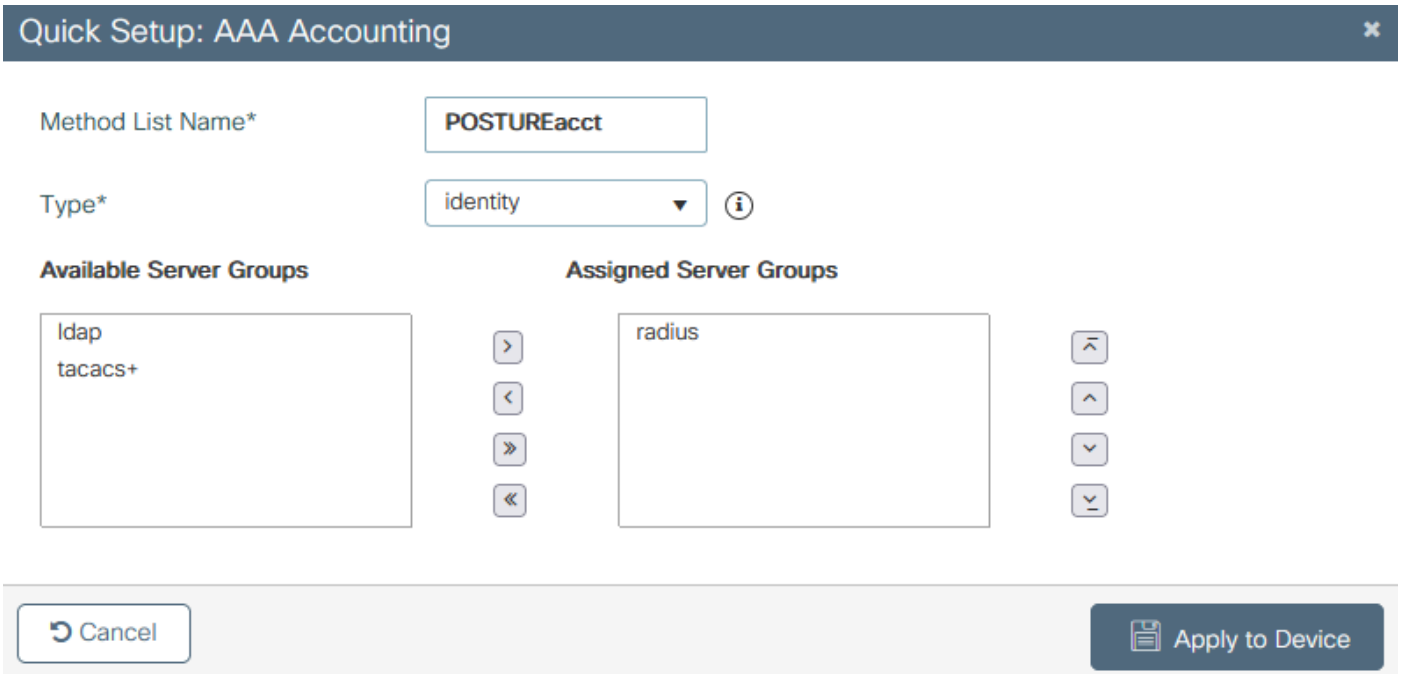


9800 인증 목록 세부 정보 생성

단계 3. (선택 사항) 이미지에 표시된 대로 회계 방법 목록을 생성합니다.



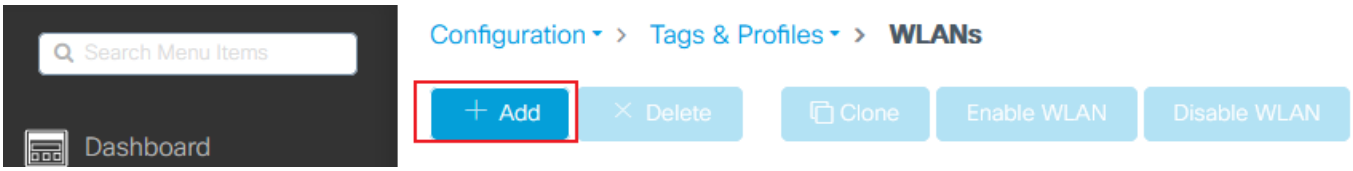
9800 계정 목록 추가



9800 계정 목록 생성 세부 정보

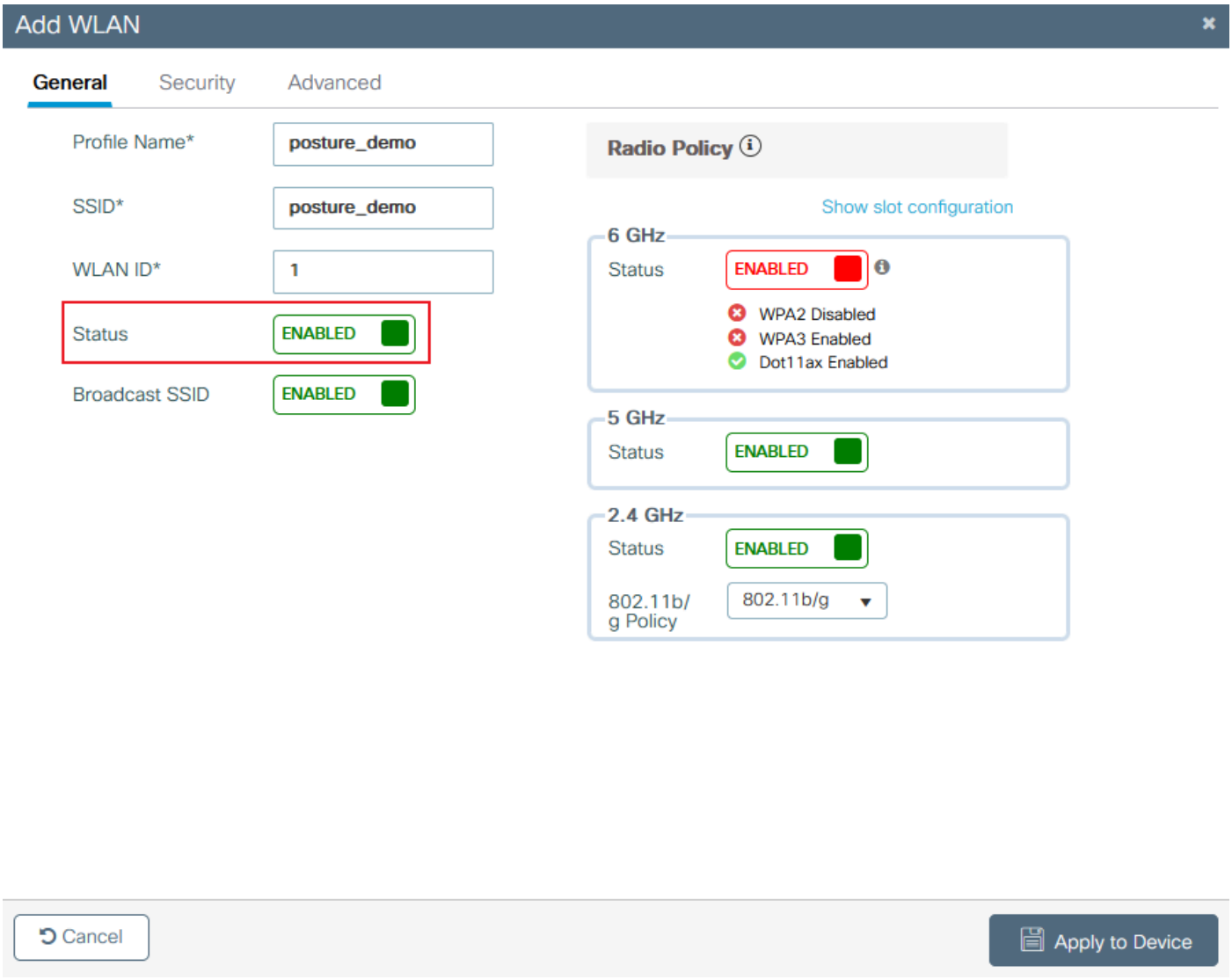
WLAN 구성

1단계. WLAN 생성. Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로필) > WLANs(WLAN) > + Add(추가)로 이동하여 필요에 따라 네트워크를 구성합니다.



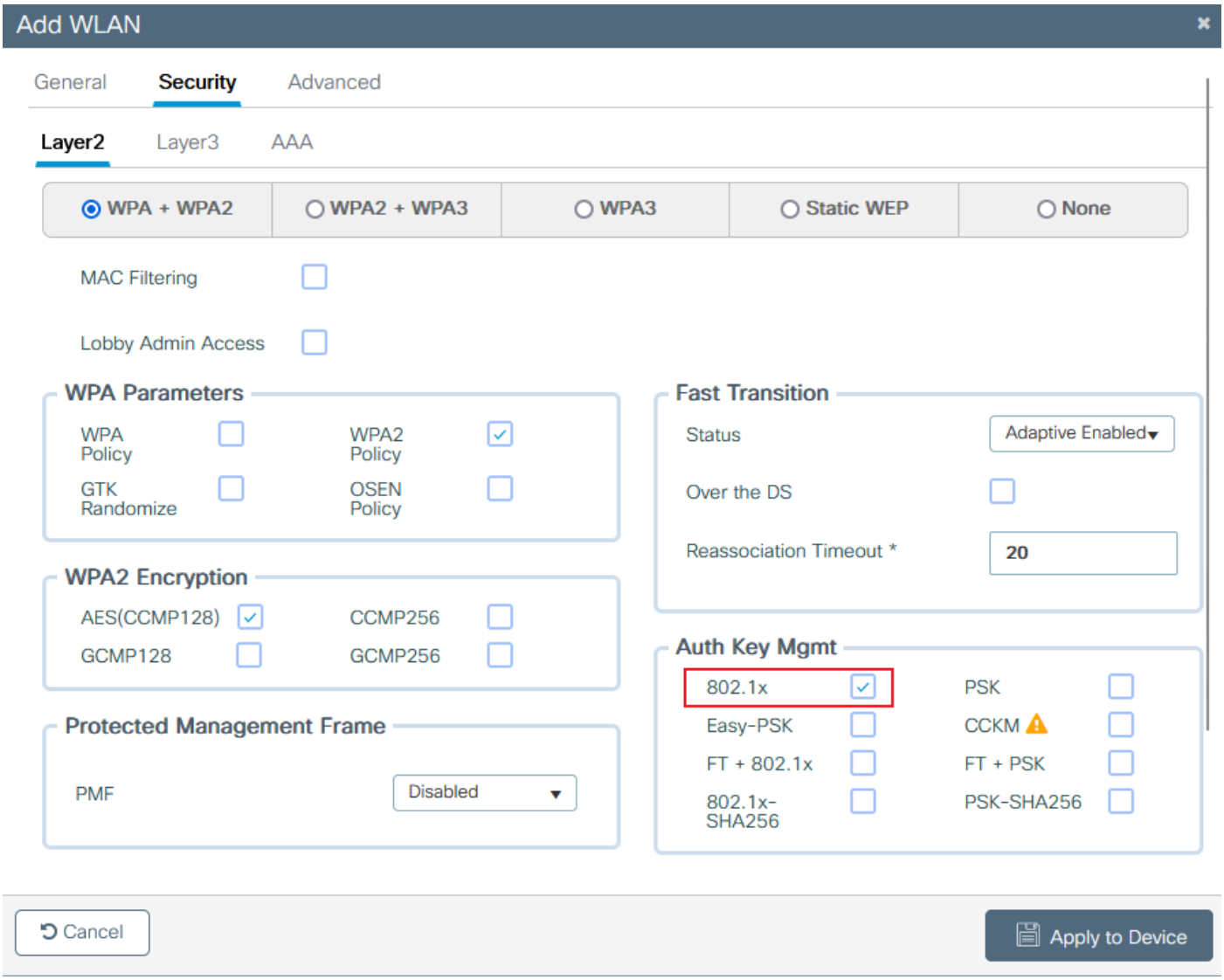
9800 WLAN 추가

2단계. WLAN 일반 정보를 입력합니다.

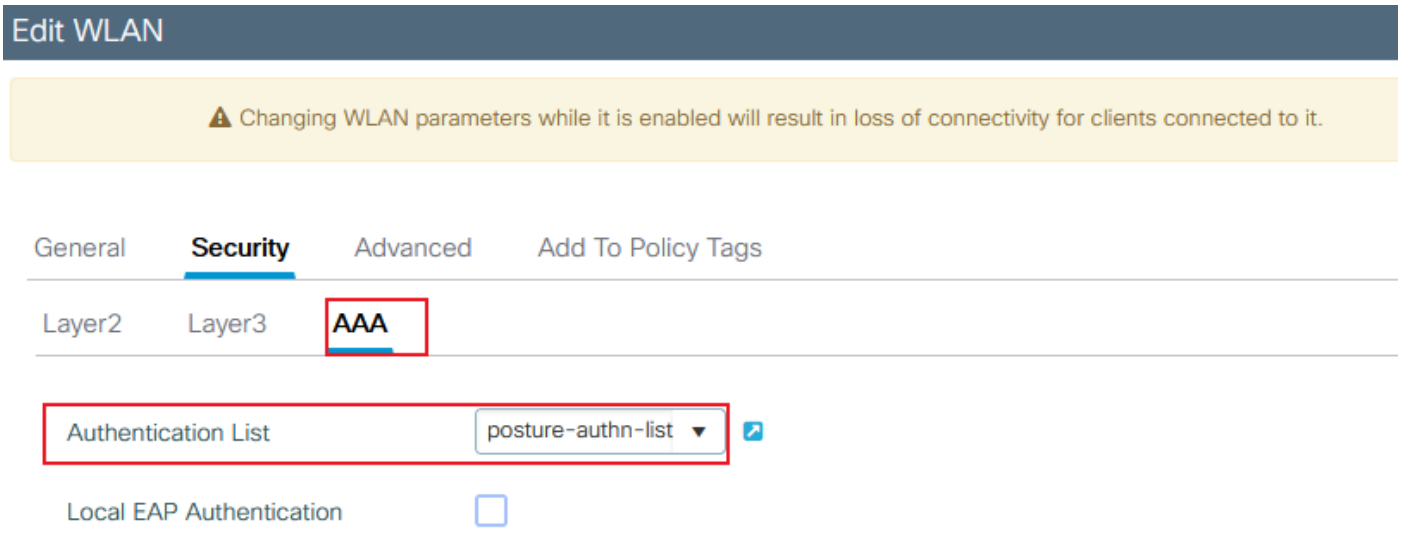


9800 create WLAN general(WLAN 일반 생성)

3단계. 보안 탭으로 이동하여 필요한 보안 방법을 선택합니다. 이 경우 '802.1x'를 선택하고 AAA 인증 목록(AAA Configuration(AAA 컨피그레이션) 섹션의 2단계에서 생성한)이 필요합니다.



9800 WLAN 보안 L2 생성

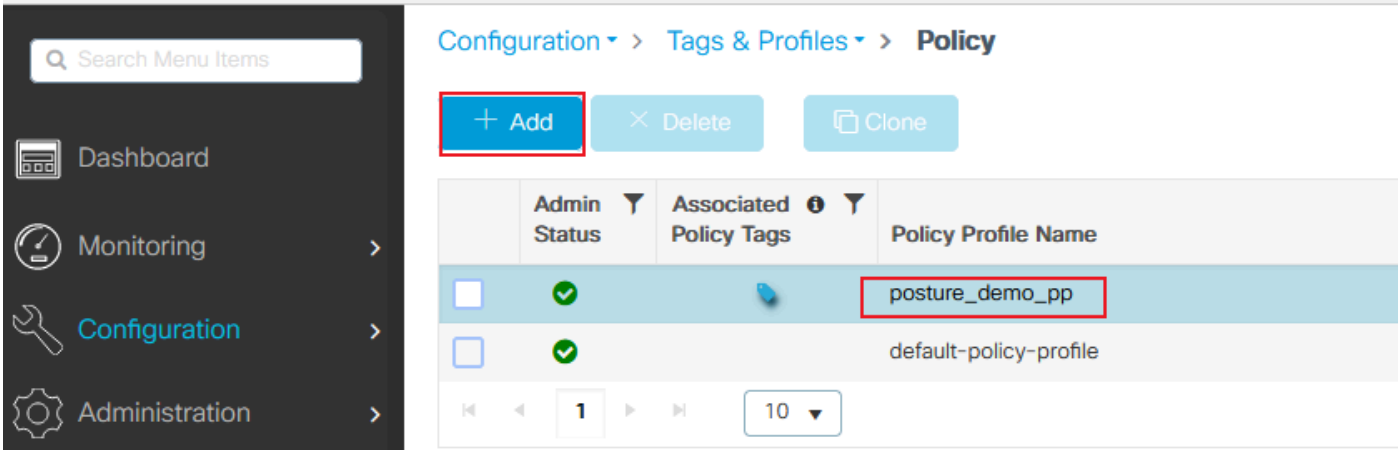


9800 WLAN 보안 AAA 생성

정책 프로파일 구성

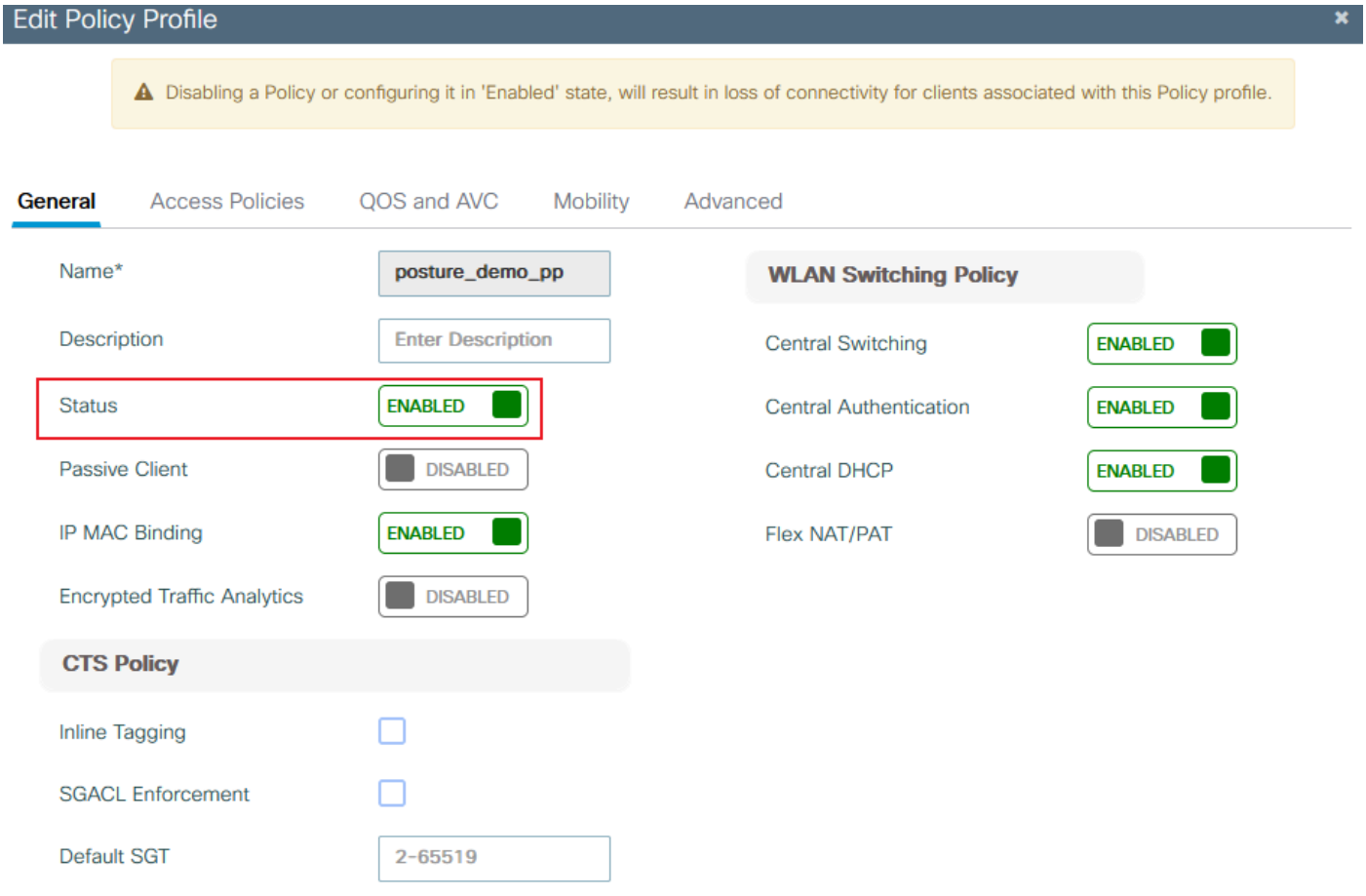
정책 프로필 내에서 다른 설정(예: ACL(Access Controls List), QoS(Quality of Service), Mobility Anchor, Timers 등) 중에서 VLAN을 할당할 클라이언트를 결정할 수 있습니다. 기본 정책 프로파일을 사용하거나 새 프로파일을 생성할 수 있습니다.

1단계. 새 정책 프로파일을 생성합니다. Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로필) > Policy(정책)로 이동하여 새 정책을 생성합니다.



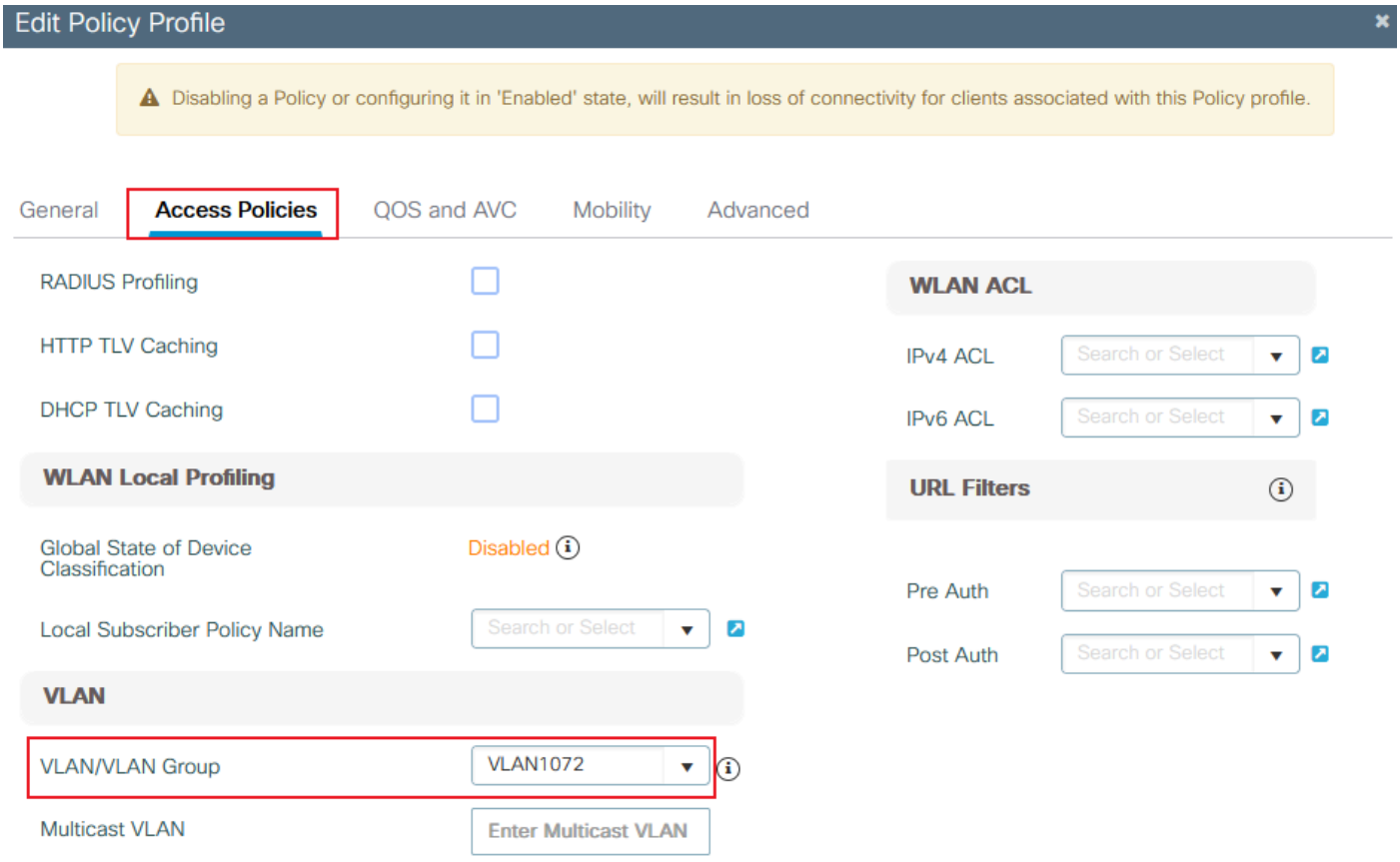
9800 정책 프로필 추가

프로파일이 활성화되어야 합니다.



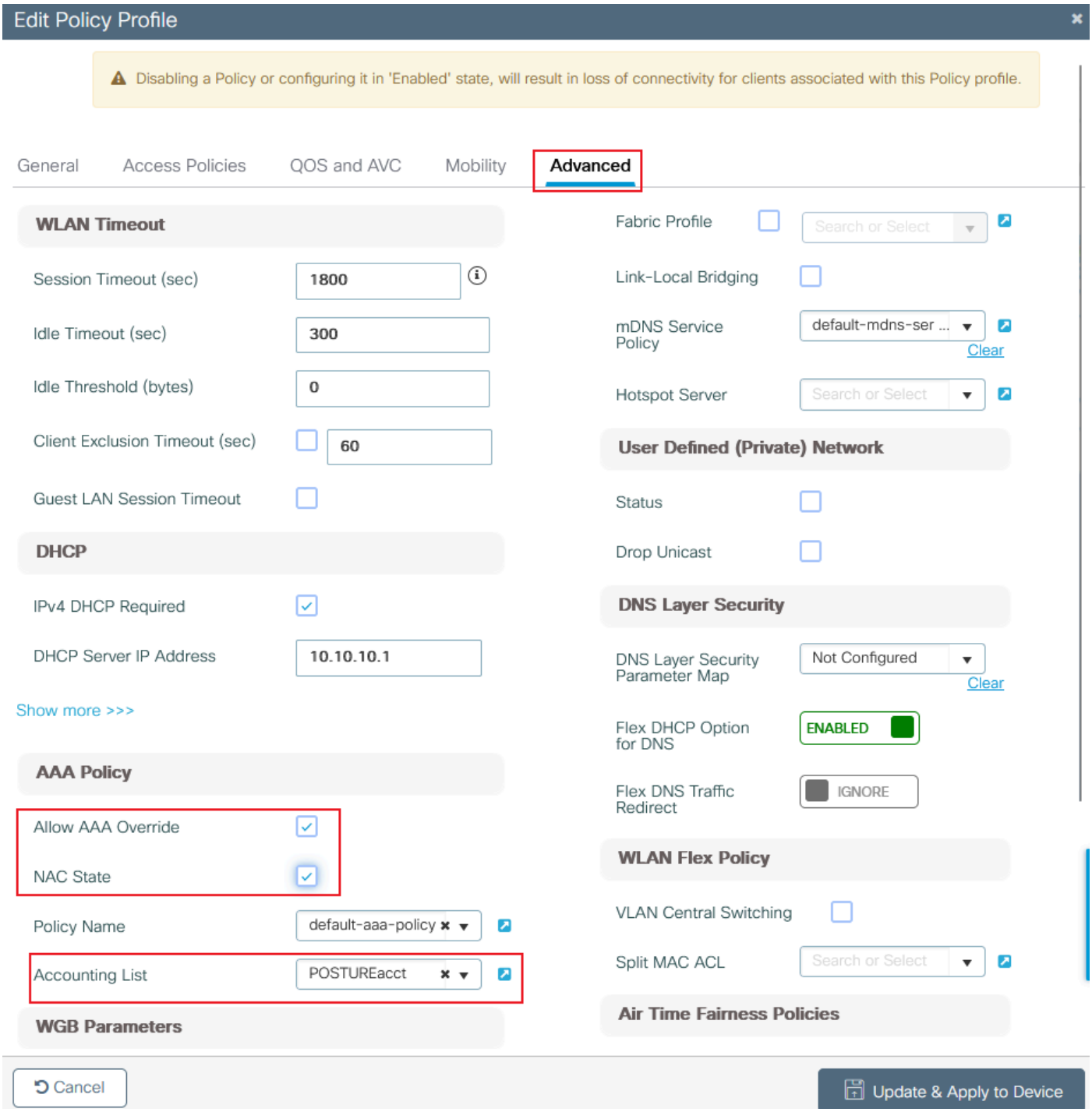
9800 정책 프로파일 생성 일반

2단계. VLAN을 선택합니다. Access Policies(액세스 정책) 탭으로 이동하고 드롭다운에서 VLAN 이름을 선택하거나 VLAN-ID를 수동으로 입력합니다. 정책 프로파일에서 ACL을 구성하지 마십시오:



9800 정책 프로필 VLAN 생성

3단계.ISE 재정의(AAA 재정의 허용) 및 CoA(Change of Authorization) (NAC 상태)를 수락하도록 정책 프로파일을 구성합니다. 선택적으로 어카운팅 방법도 지정할 수 있습니다:

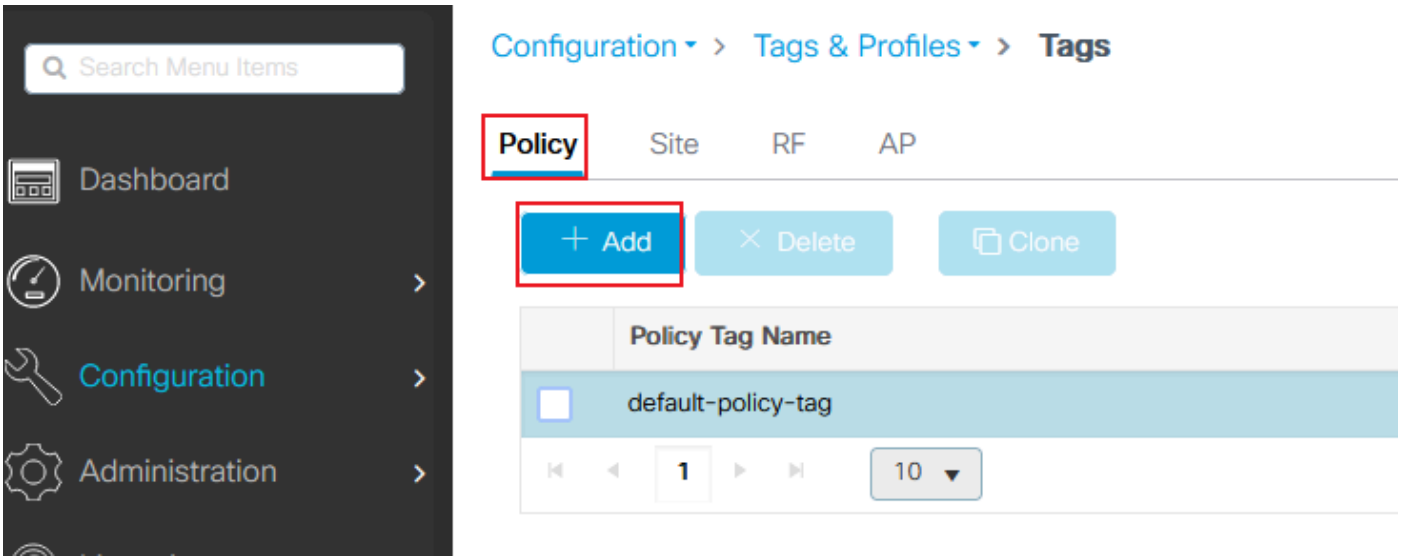


9800 정책 프로파일 생성 고급

정책 태그 구성

정책 태그 내부에서는 SSID를 정책 프로파일과 연결합니다. 새 정책 태그를 생성하거나 default-policy 태그를 사용할 수 있습니다.

Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로필) > Tags(태그) > Policy(정책)로 이동하고 이미지에 표시된 대로 필요한 경우 새 정책을 추가합니다.



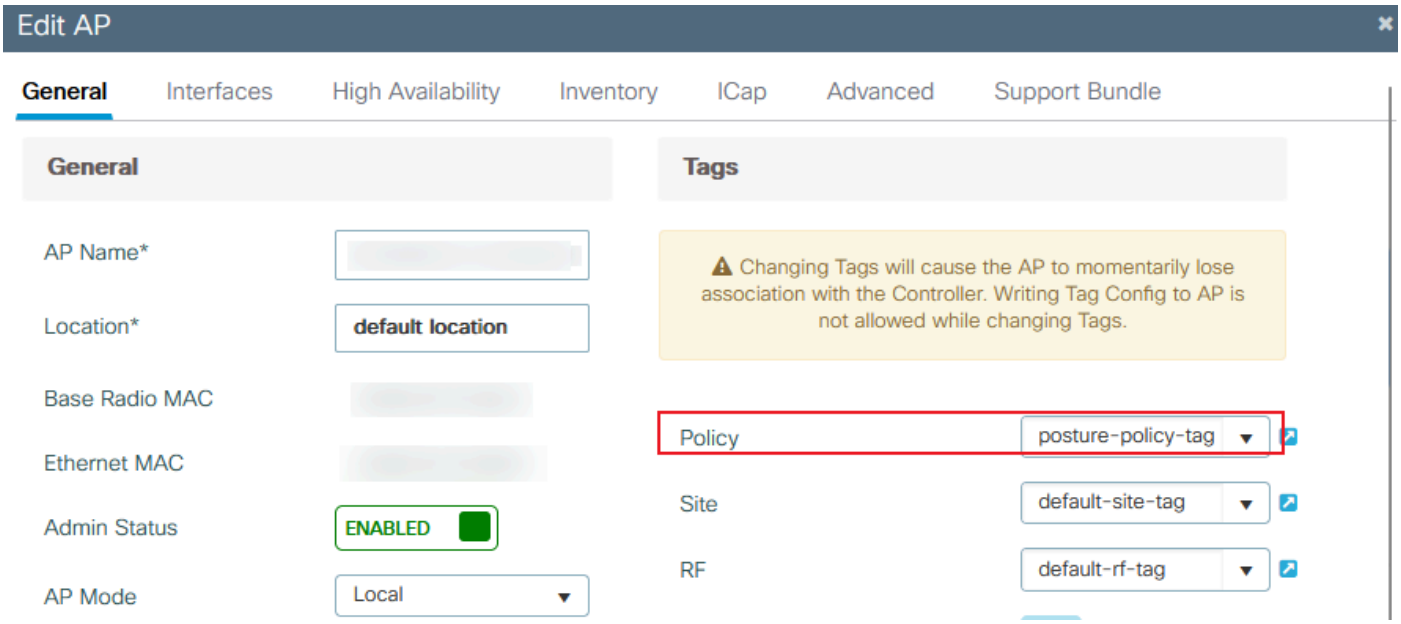
9800 정책 태그 추가

WLAN 프로파일을 원하는 정책 프로파일에 연결합니다:

9800 정책 태그 세부사항

정책 태그 할당

필요한 AP에 정책 태그를 할당합니다. Configuration(컨피그레이션) > Wireless(무선) > Access Points(액세스 포인트) > AP Name(AP 이름) > General Tags(일반 태그)로 이동하여 필요한 할당을 만든 다음 Update & Apply to Device(디바이스에 업데이트 및 적용)를 클릭합니다.



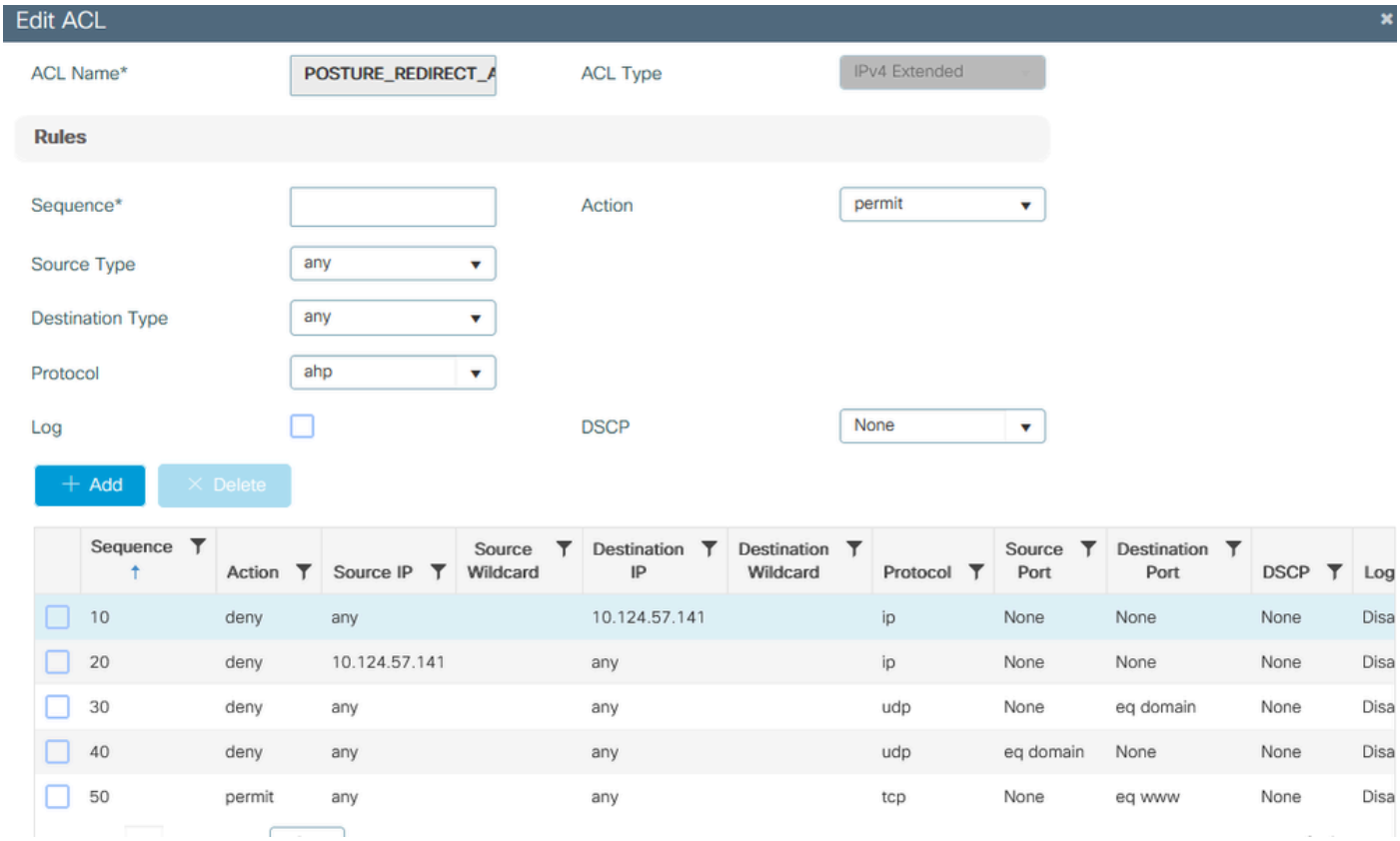
9800 정책 태그 할당

ACL 구성 리디렉션

새 ACL을 생성하려면 Configuration(컨피그레이션) > Security(보안) > ACL > + Add(추가)로 이동합니다.

포스처 포털 리디렉션에 사용되는 ACL에는 CWA(Central Web Authentication)와 동일한 요구 사항이 있습니다.

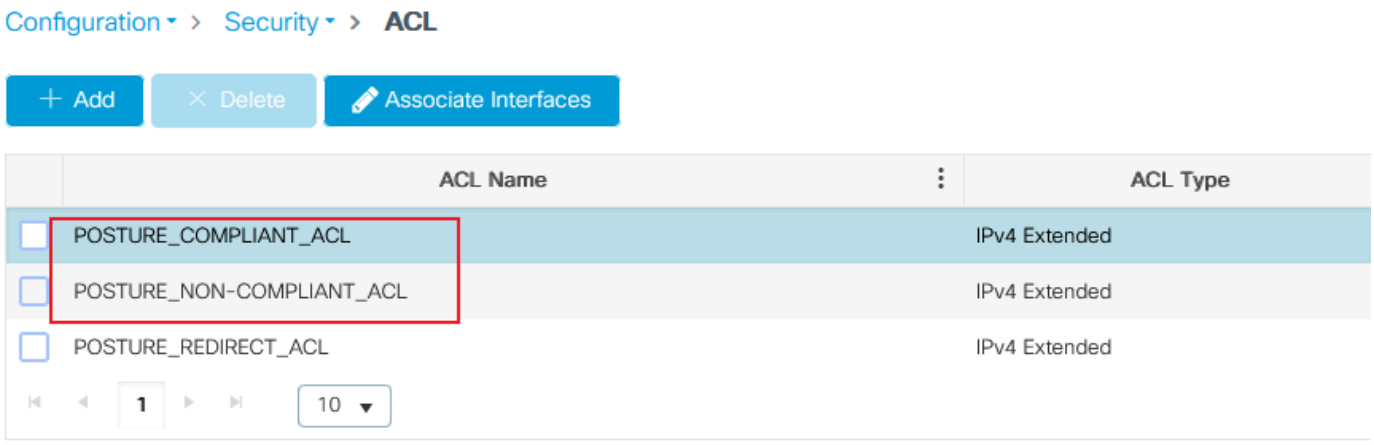
ISE PSN 노드에 대한 트래픽과 DNS를 거부하고 나머지는 모두 허용해야 합니다. 이 리디렉션 ACL은 보안 ACL이 아니라 추가 처리(리디렉션 등)를 위해 CPU에 어떤 트래픽(허용 시)을 전송할지, 데이터 평면에 어떤 트래픽(거부 시)을 유지할지 정의하고 리디렉션을 방지하는 punt ACL입니다. ACL은 다음과 같아야 합니다(이 예에서는 10.124.57.141을 ISE IP 주소로 대체).



9800 리디렉션 ACL 세부사항

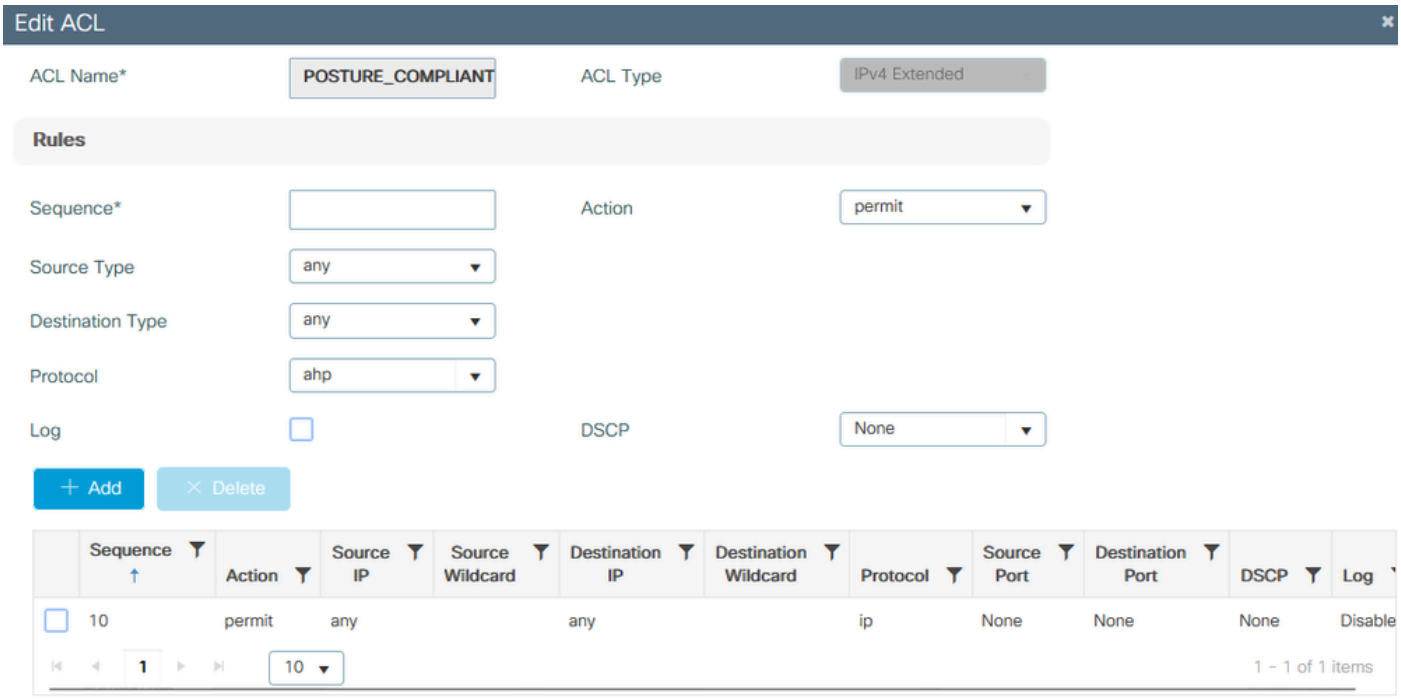
정책 ACL 컨피그레이션

이 경우 ISE에 대해 9800 WLC에 별도의 ACL을 정의하여 상태 확인 결과에 따라 규정 준수 및 비준수 시나리오를 인증해야 합니다.



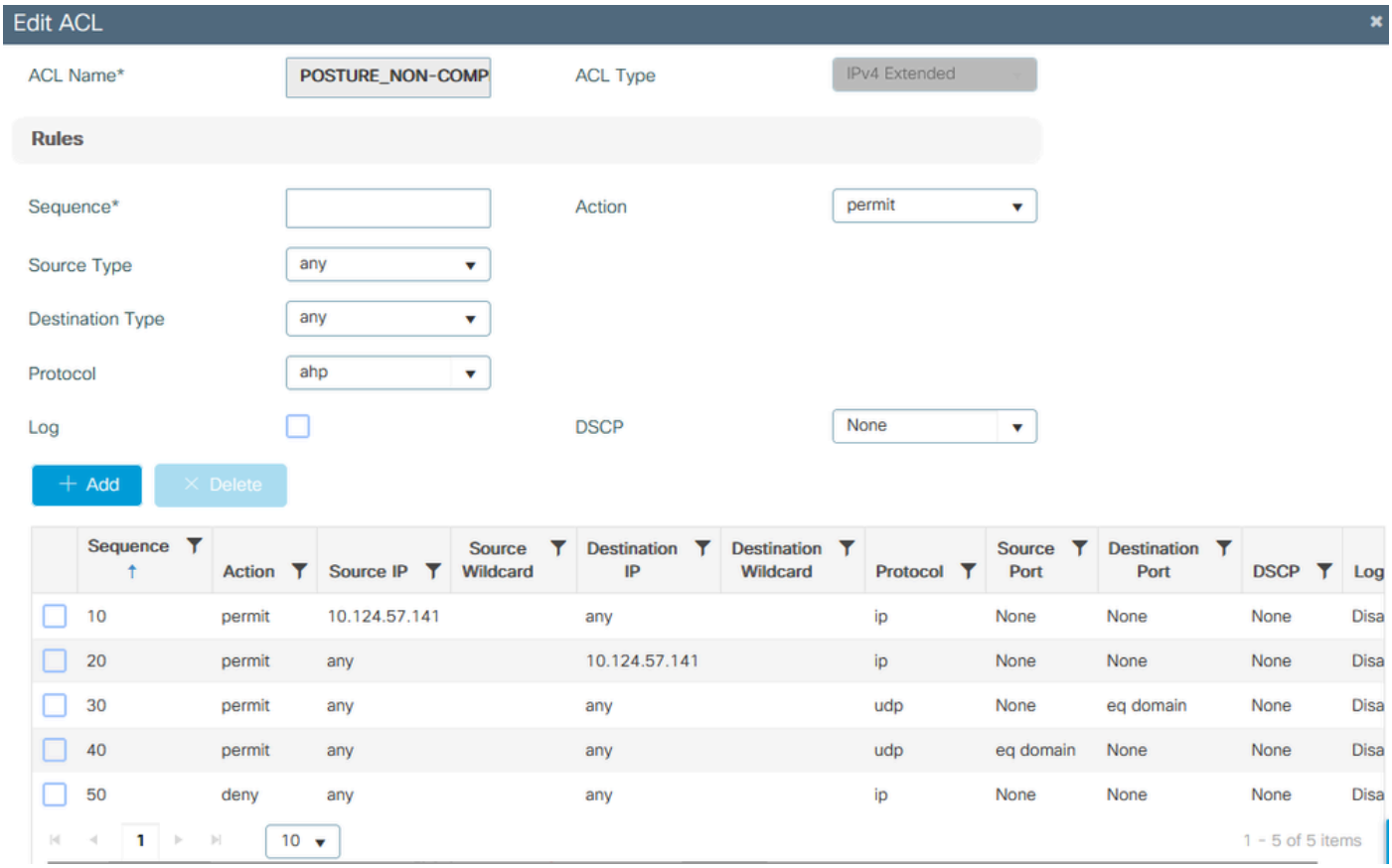
9800 ACL 일반

규정 준수 시나리오의 경우 이 경우 모두 허용을 사용합니다. 또 다른 일반적인 컨피그레이션으로서, ISE가 규정 준수 결과에서 어떤 ACL도 인증하지 않도록 할 수도 있습니다. 이는 9800 측에서 모두 허용하는 것과 같습니다.



9800 ACL - 규정 준수

비준수 시나리오의 경우, 클라이언트는 특정 네트워크, 일반적으로 리미디에이션 서버(이 경우 ISE 자체)에 대한 액세스만 허용합니다.

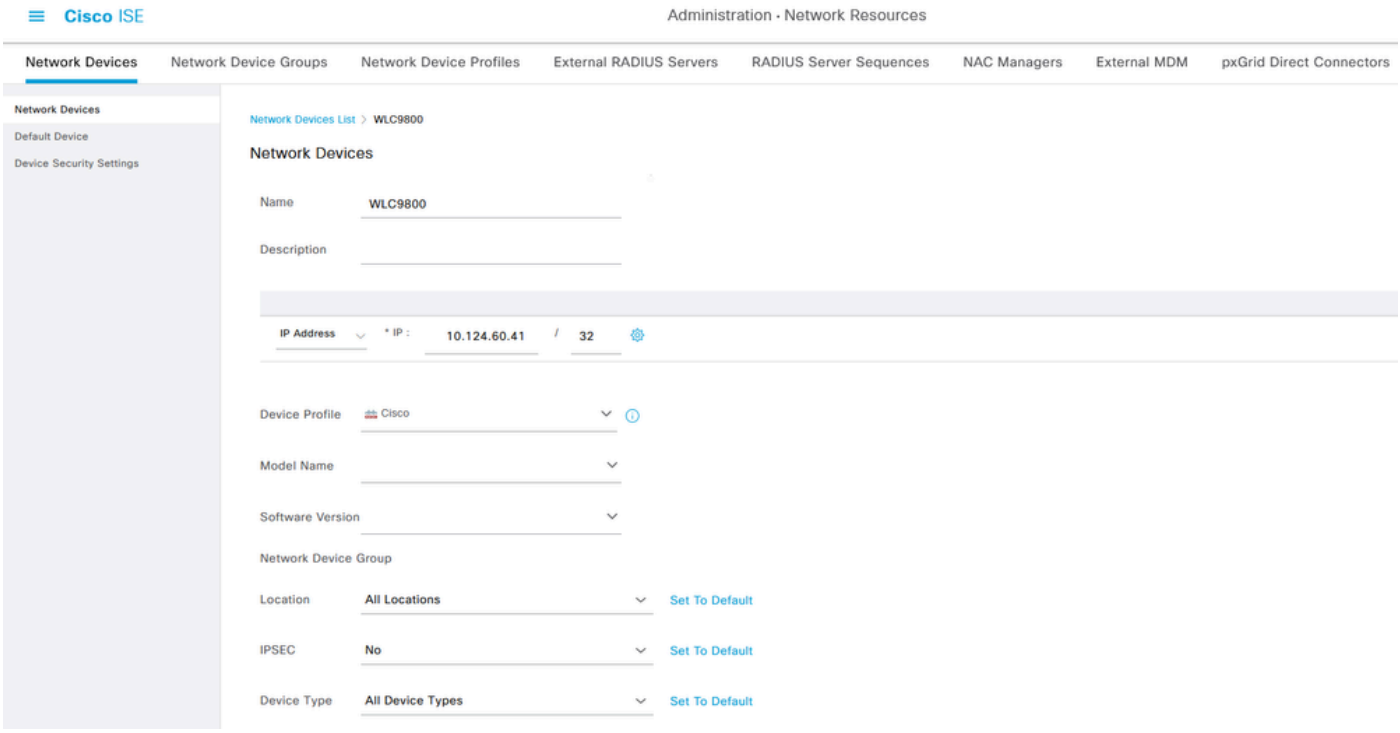


9800 ACL - 비준수

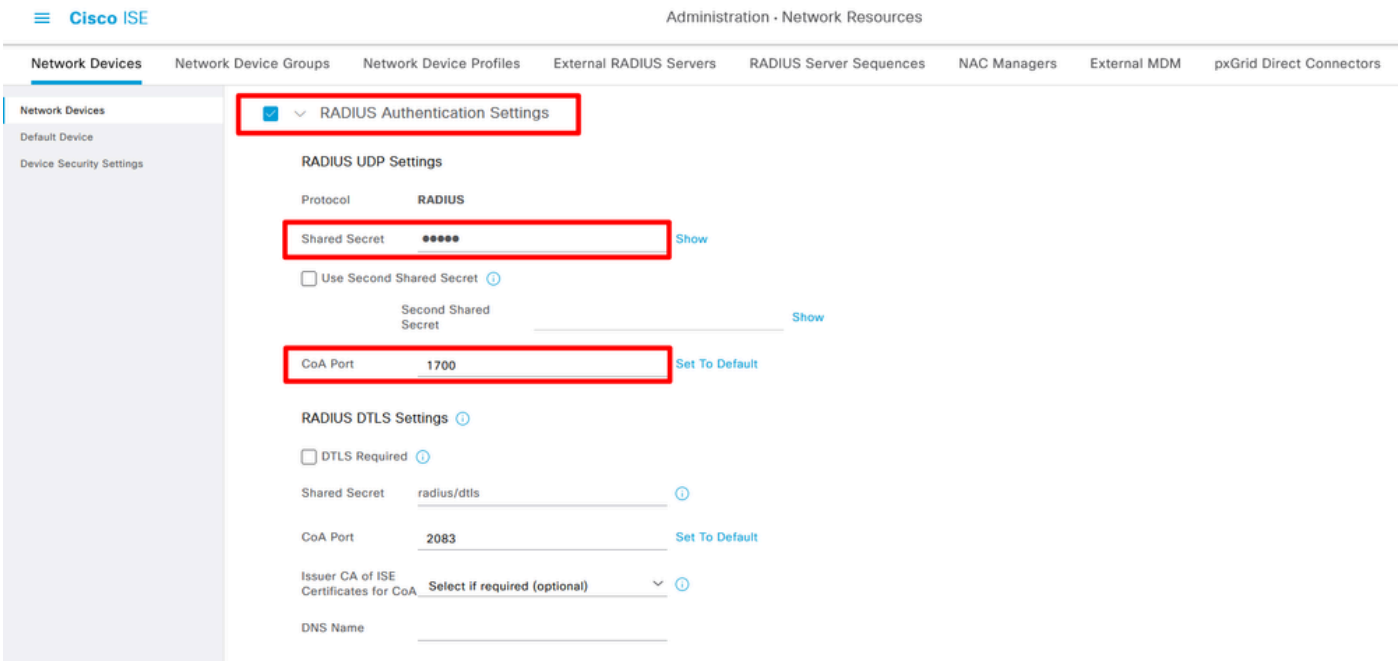
ISE의 AAA 컨피그레이션 및 상태 설정

상태 요구 사항: 이 예에서 규정 준수를 확인하기 위한 요구 사항은 Windows PC를 테스트하는 데 사용되는 데스크톱에 특정 테스트 파일이 있는지 여부를 감지하는 것입니다.

1단계. ISE에서 WLC 9800을 NAD로 추가합니다. Administration(관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스) > Add(추가)로 이동합니다.



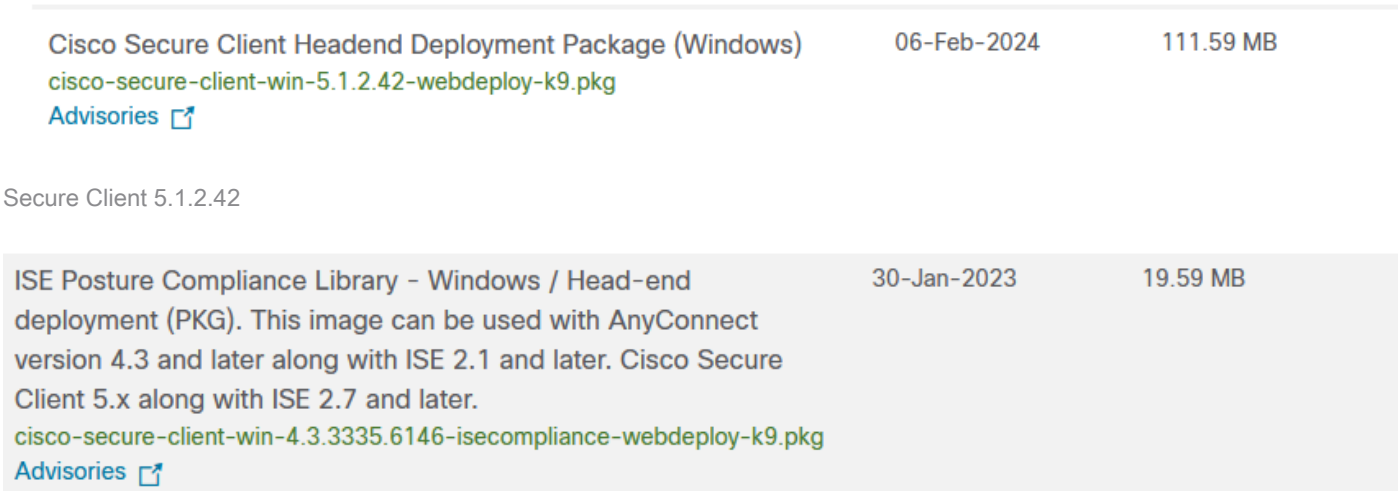
네트워크 디바이스 추가 01



네트워크 디바이스 추가 02

2단계. Cisco Software CCO 웹 사이트에서 Cisco Secure Client Headend Deployment Package and Compliance Module을 다운로드합니다.

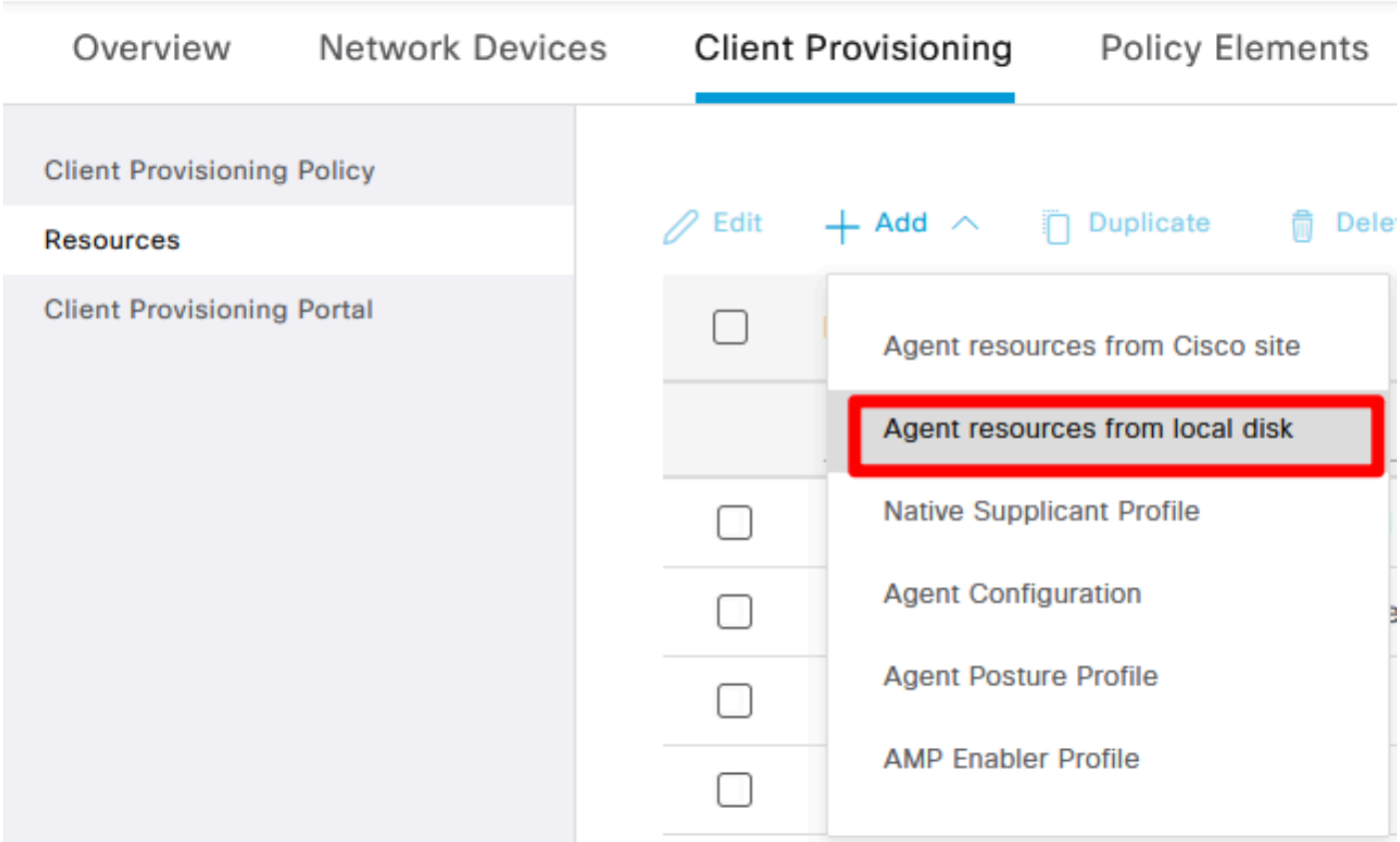
Cisco Secure Client 액세스 및 검색:



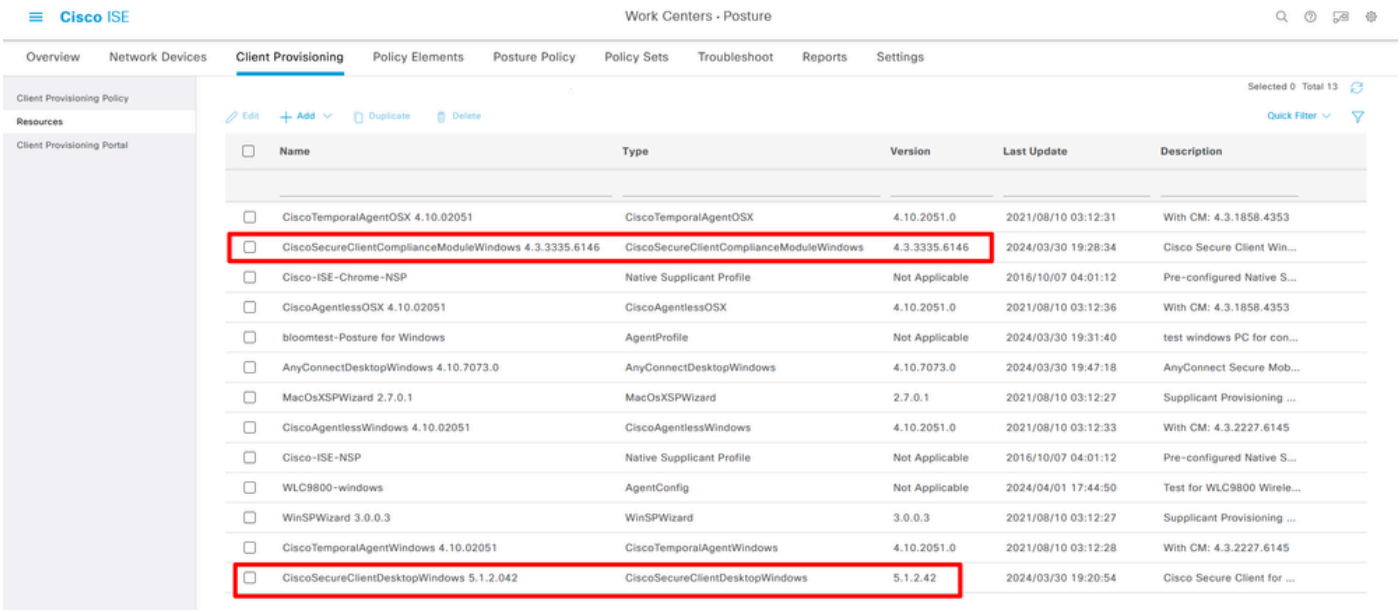
Secure Client 5.1.2.42

ISE Compliance module 4.3

3단계. ISE 클라이언트 프로비저닝에 Cisco Secure Client Headend Deployment Package 및 Compliance Module 패키지를 업로드합니다. Work Centers(작업 센터) > Posture(포스처) > Client Provisioning(클라이언트 프로비저닝) > Resources(리소스)로 이동합니다. Add(추가)를 클릭하고 드롭다운 상자에서 로컬 디스크의 Agent resources(에이전트 리소스)를 선택합니다.

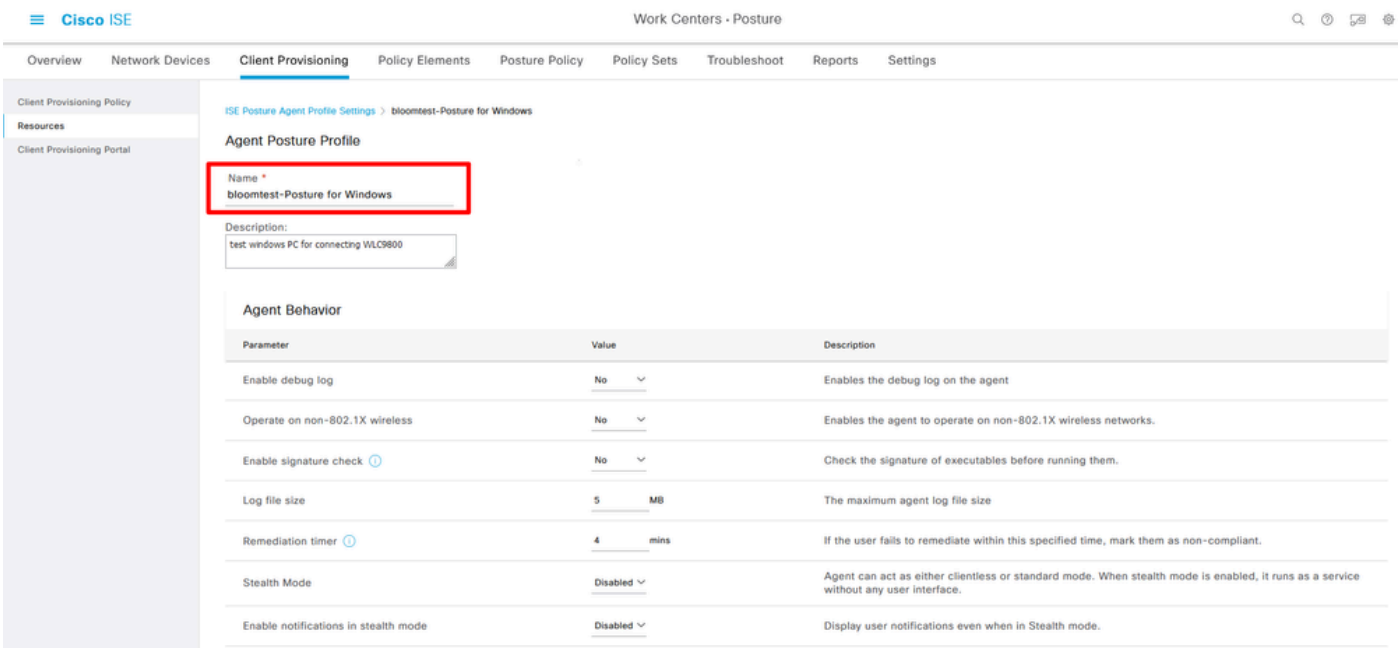


보안 클라이언트 업로드



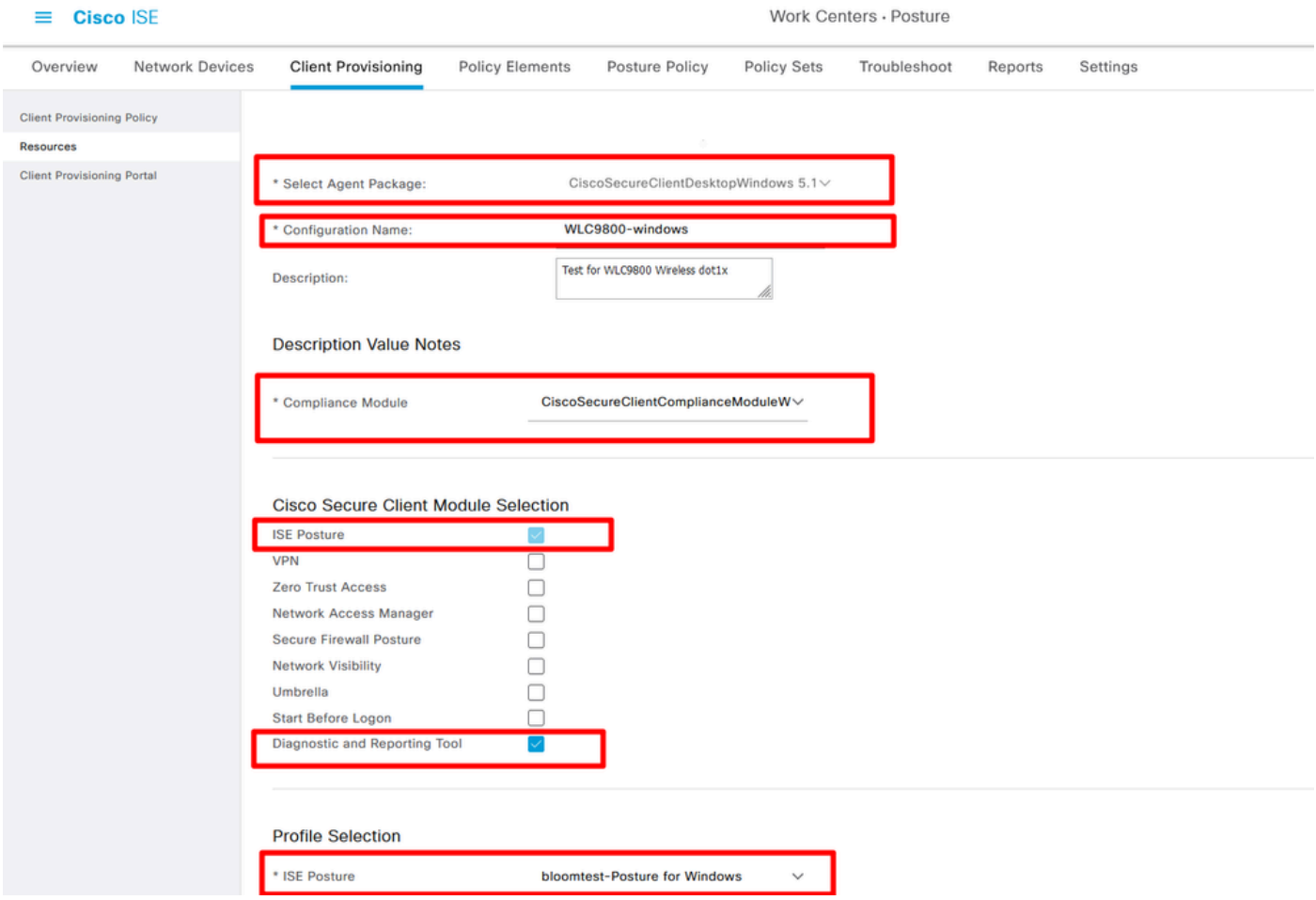
Secure Client 및 Compliance Module 업로드 성공

4단계. Agent Posture 프로파일 생성 Work Centers(작업 센터) > Posture(포스처) > Client Provisioning(클라이언트 프로비저닝) > Resources(리소스) > Add(추가) > Agent Posture Profile(에이전트 포스처 프로파일)로 이동합니다.



상담원 상태 프로파일

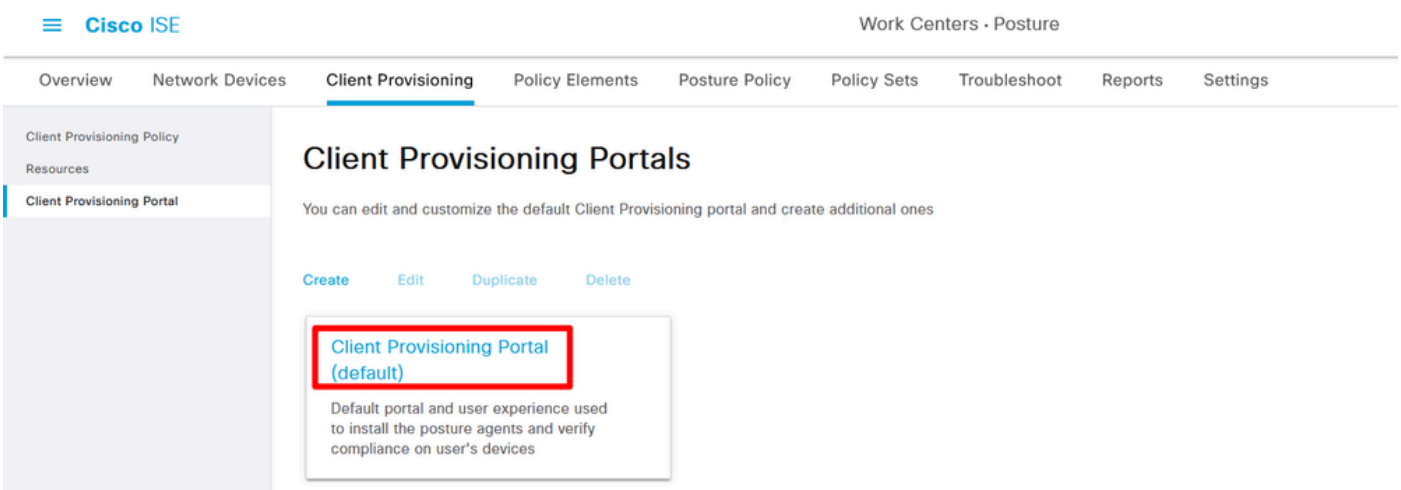
5단계. 에이전트 컨피그레이션 생성 Work Centers(작업 센터) > Posture(포스처) > Client Provisioning(클라이언트 프로비저닝) > Resources(리소스) > Add(추가) > Agent Configuration(에이전트 컨피그레이션)으로 이동합니다.



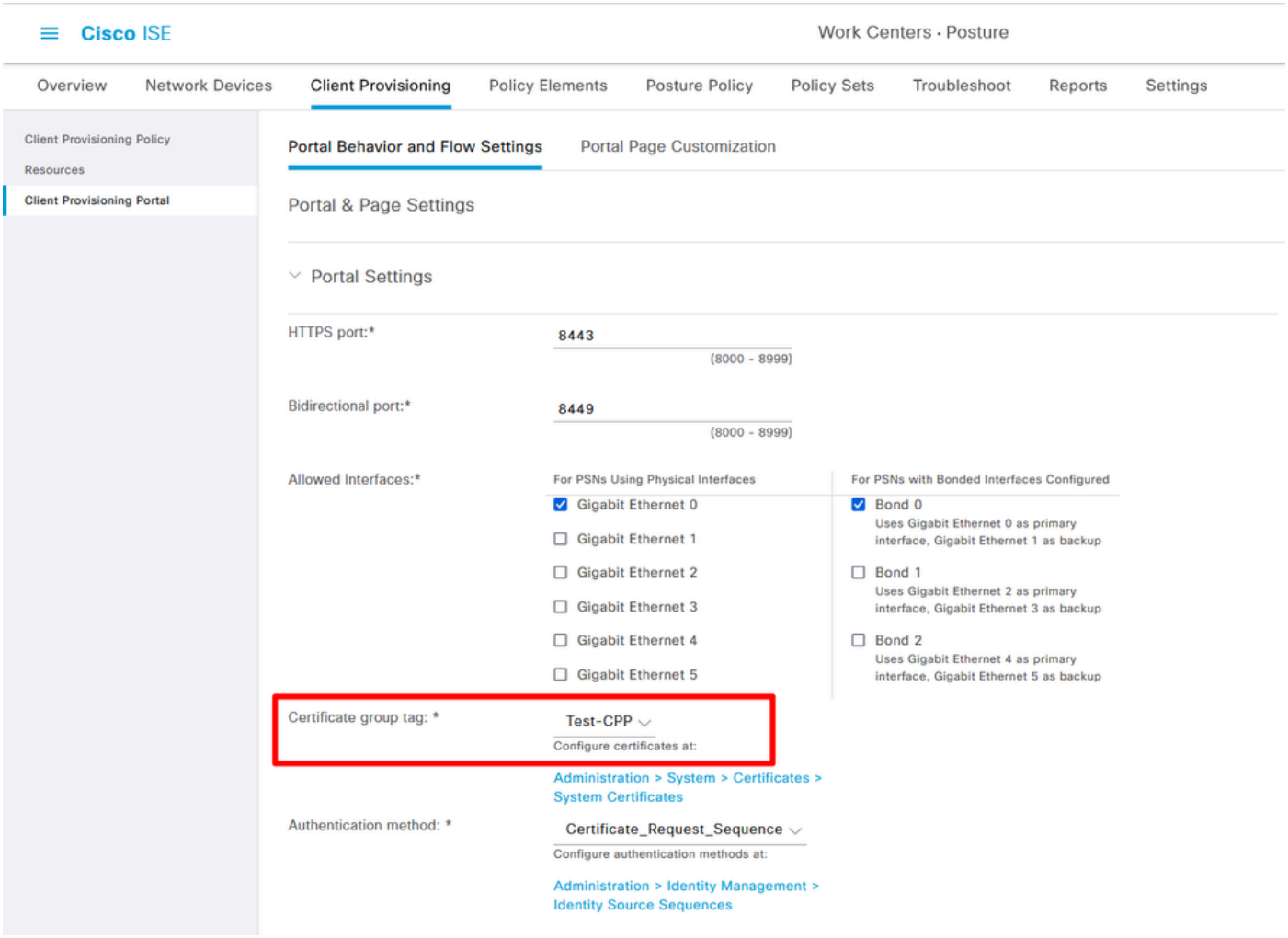
에이전트 구성 추가

6단계. 클라이언트 프로비저닝 포털을 확인하고 테스트에 기본 포털을 사용하십시오. CSR을 생성하고 CA 서버에서 SSL 인증서를 신청하고 이 포털 설정에서 인증서 그룹 태그를 바꾸십시오. 그렇지 않으면 테스트 프로세스 중에 인증서의 신뢰할 수 없는 경고가 발생합니다.

Work Centers(작업 센터) > Posture(포스처) > Client Provisioning(클라이언트 프로비저닝) > Client Provisioning Portals(클라이언트 프로비저닝 포털)로 이동합니다.

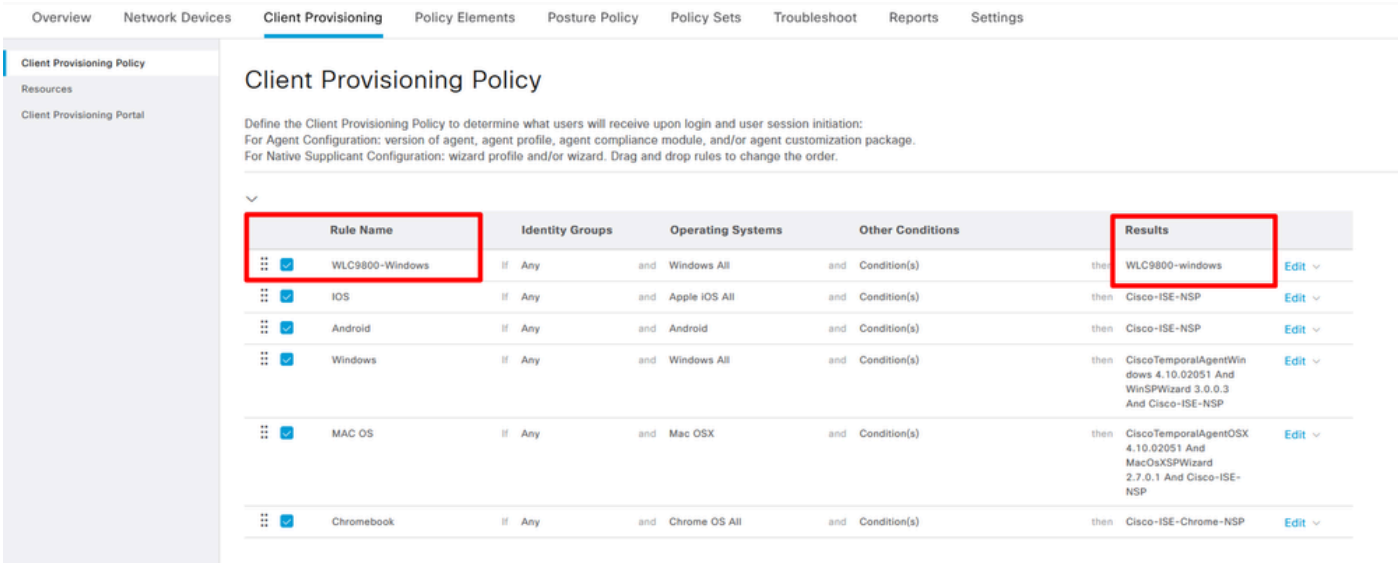


Client Provisioning Portal(클라이언트 프로비저닝 포털) 01 선택



Client Provisioning Portal(클라이언트 프로비저닝 포털) 02 선택

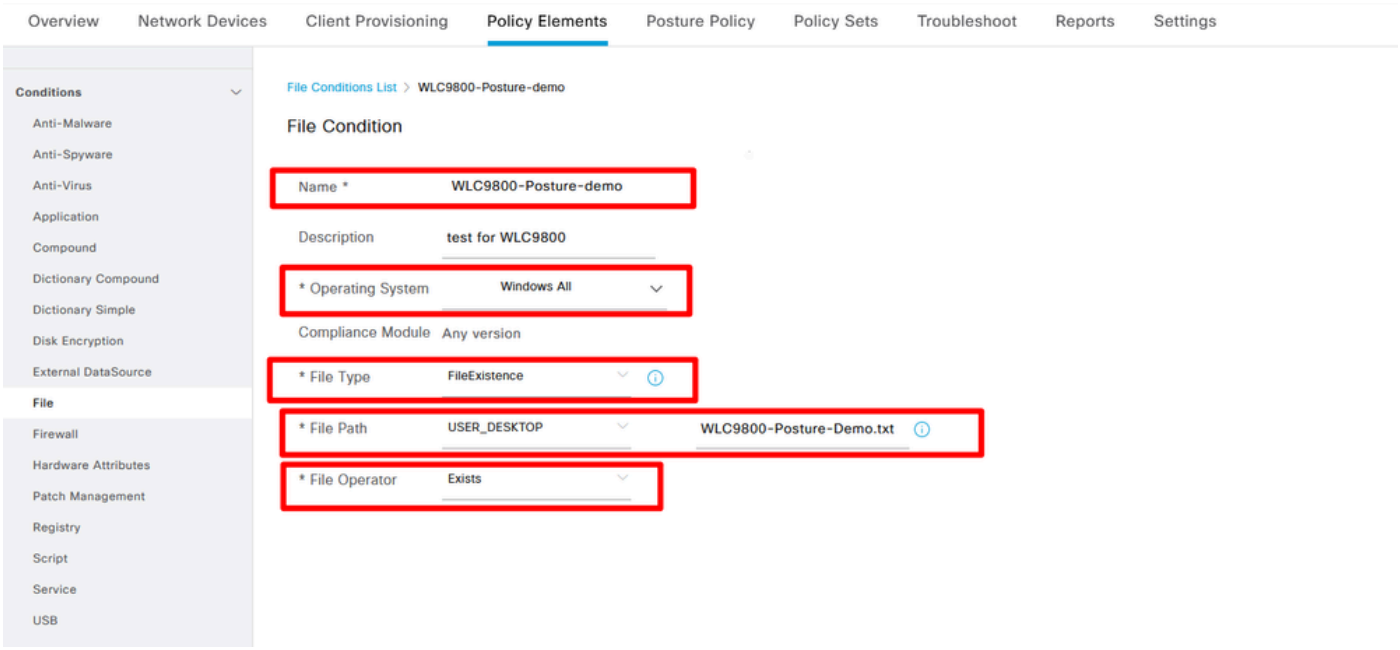
7단계. 클라이언트 프로비저닝 정책을 생성합니다. Work Centers(작업 센터) > Posture(포스처) > Client Provisioning(클라이언트 프로비저닝) > Client Provisioning Policy(클라이언트 프로비저닝 정책) > Edit(편집) > insert new policy above(위에 새 정책 삽입)로 이동합니다.



클라이언트 프로비저닝 정책 생성

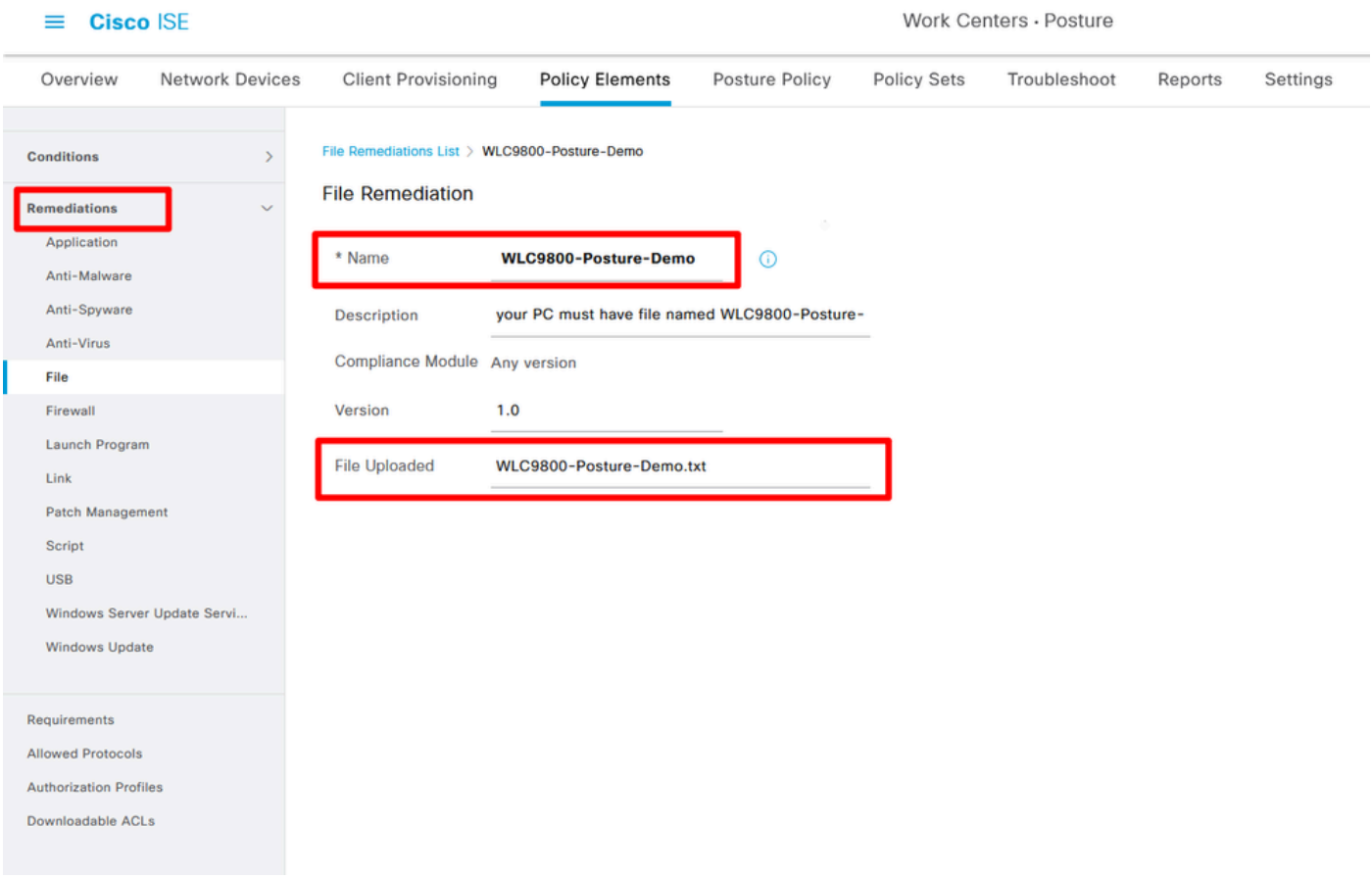
8단계. 파일 조건을 생성합니다. Work Centers(작업 센터) > Posture(포스처) > Policy Elements(정

책 요소) > Conditions(조건) > File(파일) > File Conditions(파일 조건) > Add(추가)로 이동합니다.



파일 조건 생성

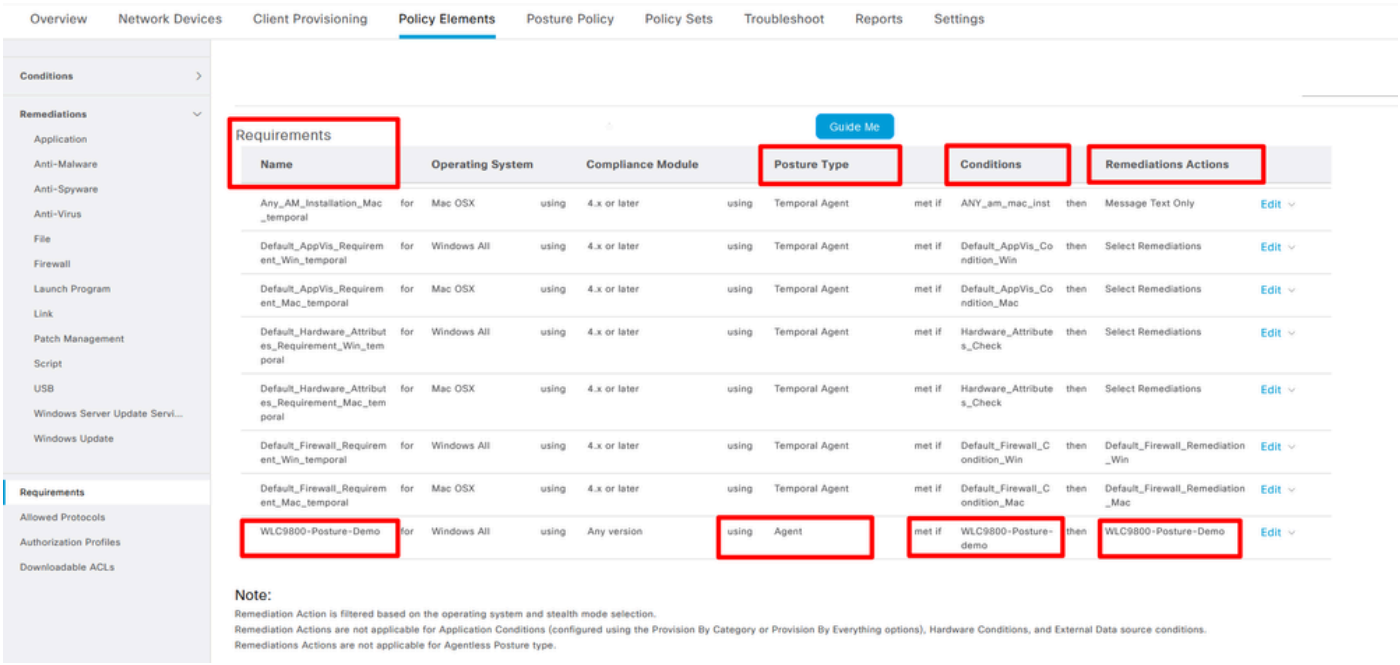
9단계. 교정 생성 Work Centers(작업 센터) > Posture(포스처) > Policy Elements(정책 요소) > Remediations(교정) > File(파일) > Add(추가)로 이동합니다.



파일 교정 생성

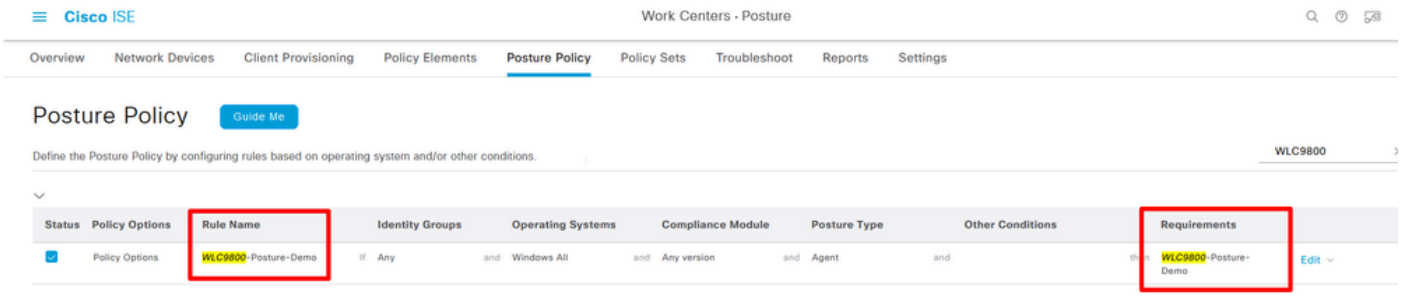
10단계. 요구 사항을 생성합니다. Work Centers(작업 센터) > Posture(포스처) > Policy

Elements(정책 요소) > Requirements(요구 사항) > Insert new Requirement(새 요구 사항 삽입)로 이동합니다.



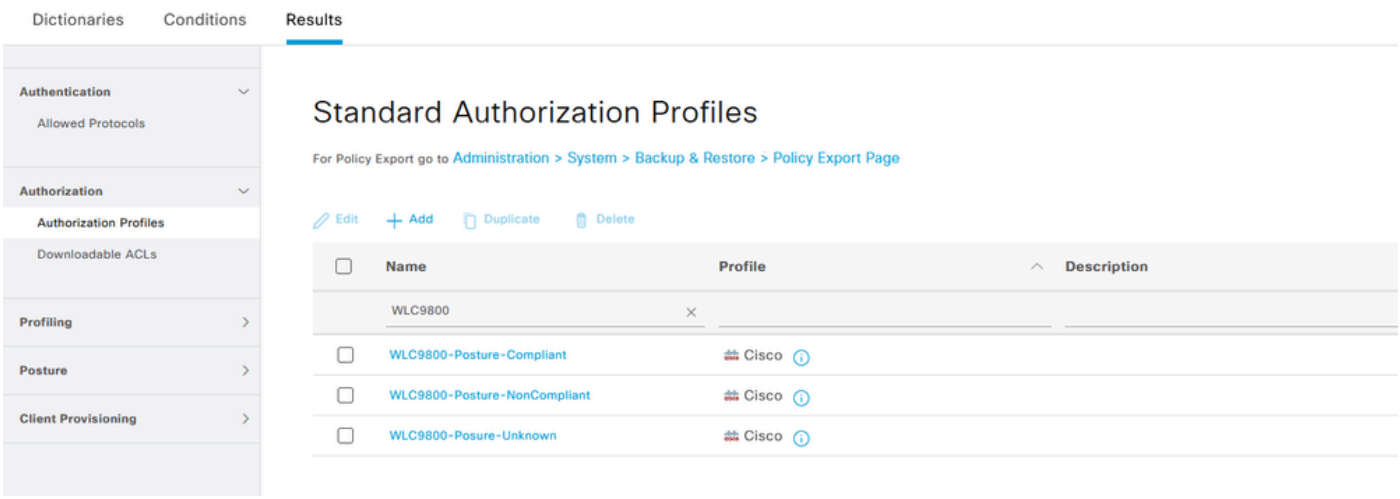
상태 요구 사항 생성

11단계. Posture Policy를 생성합니다. Work Centers(작업 센터) > Posture(포스처) > Insert new policy(새 정책 삽입)로 이동합니다.

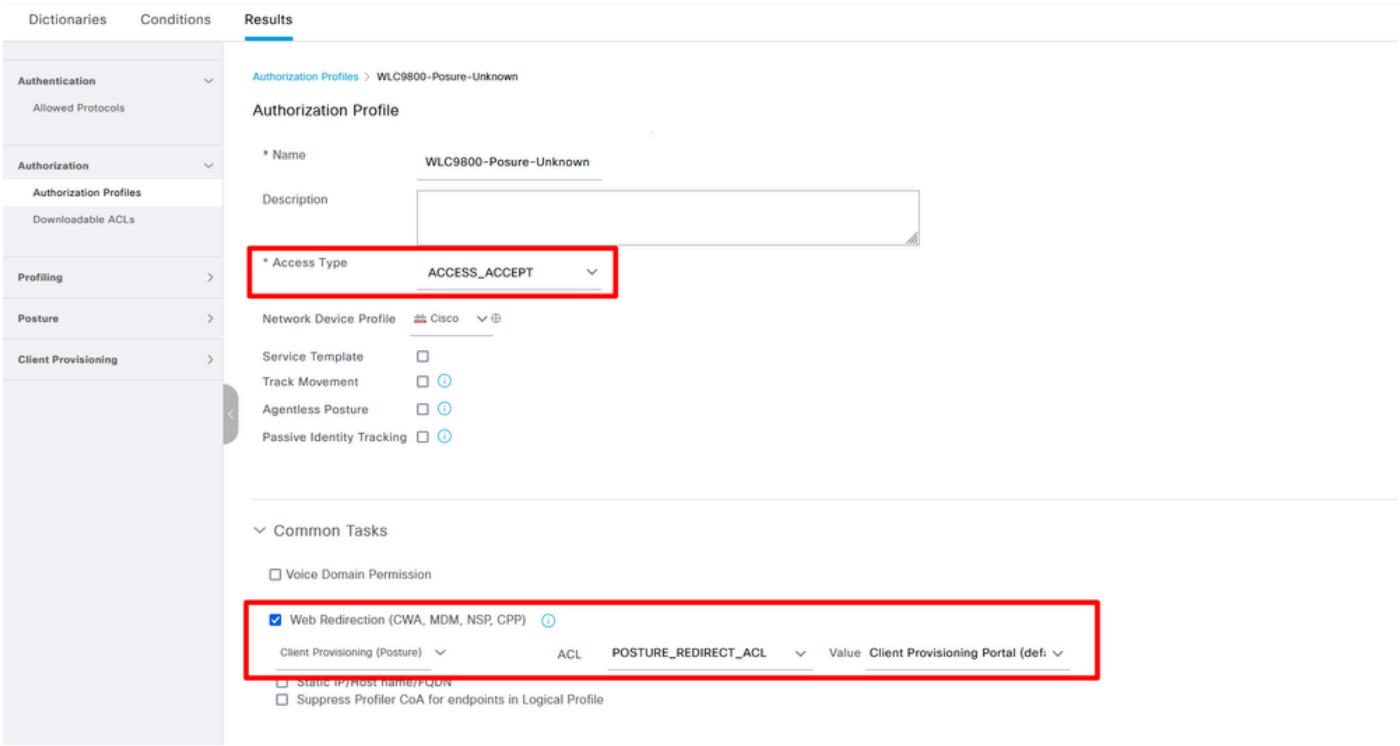


상태 정책 생성

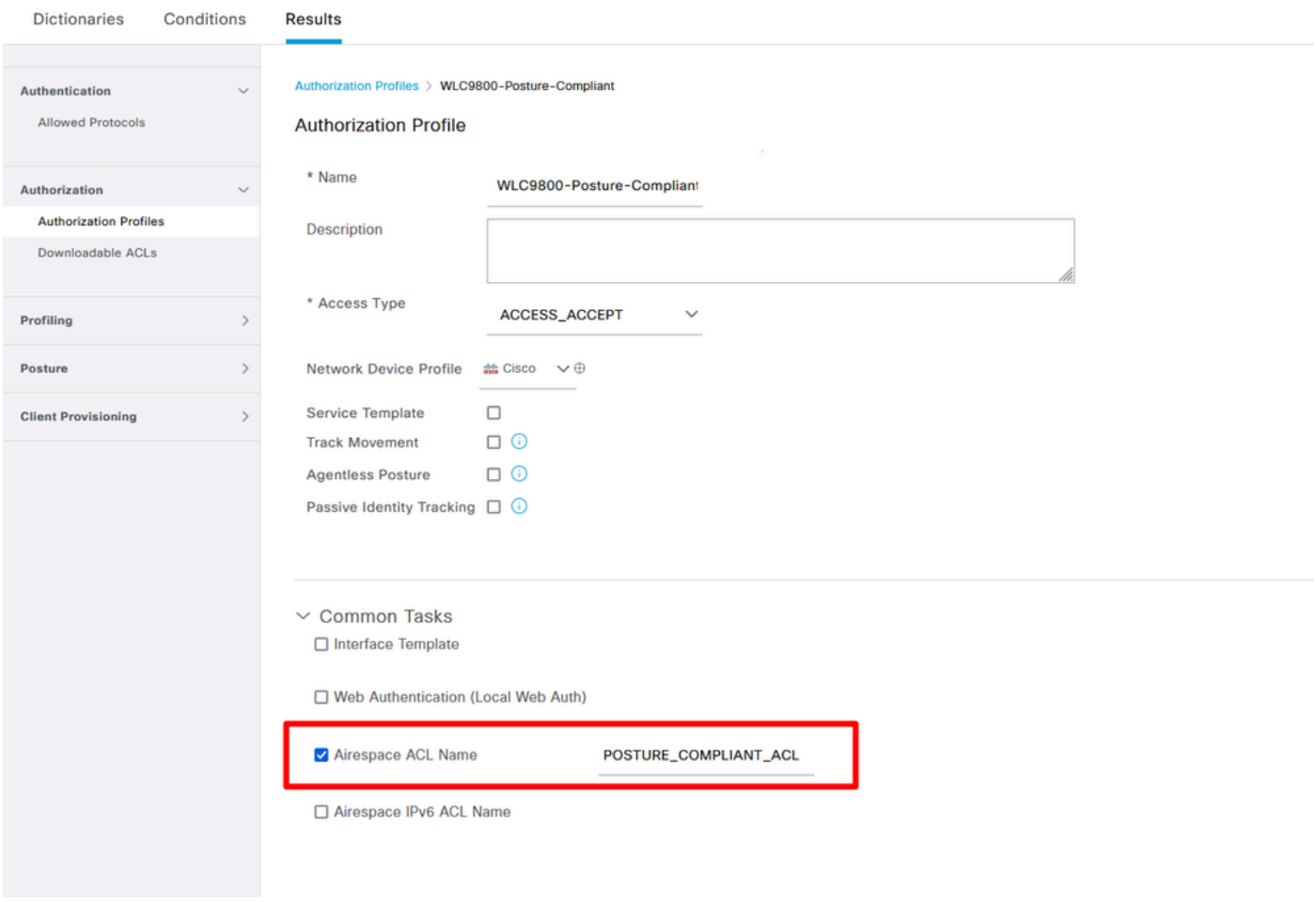
12단계. 다음 세 가지 권한 부여 프로파일을 생성합니다. 상태 상태가 알 수 없음; 포스처 상태가 Non-Compliant입니다. 포스처 상태는 Compliant입니다. Policy(정책) > Policy Elements(정책 요소) > Results(결과) > Authorization(권한 부여) > Authorization Profiles(권한 부여 프로파일) > Add(추가)로 이동합니다.



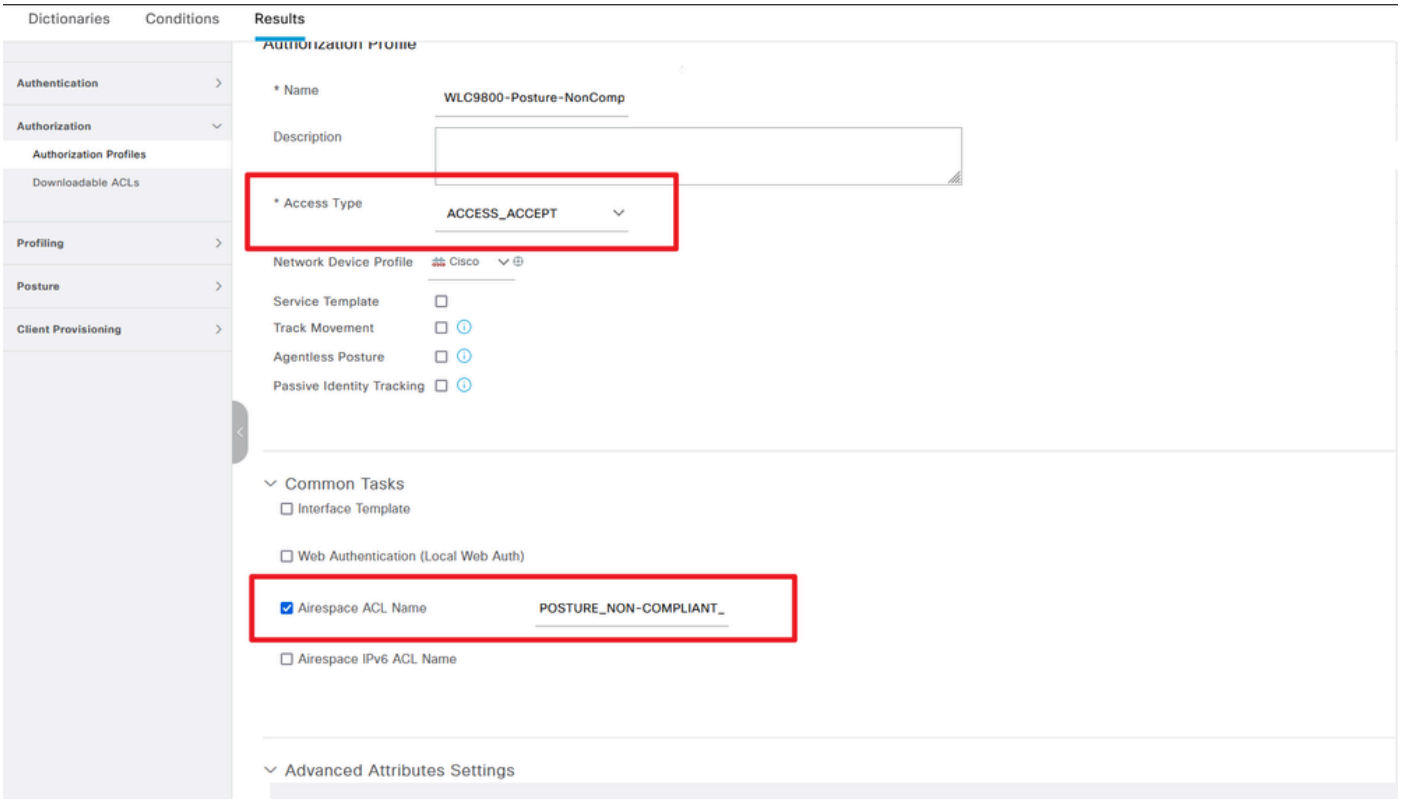
권한 부여 프로파일 생성 01



권한 부여 프로파일 생성 02



권한 부여 프로파일 생성 03

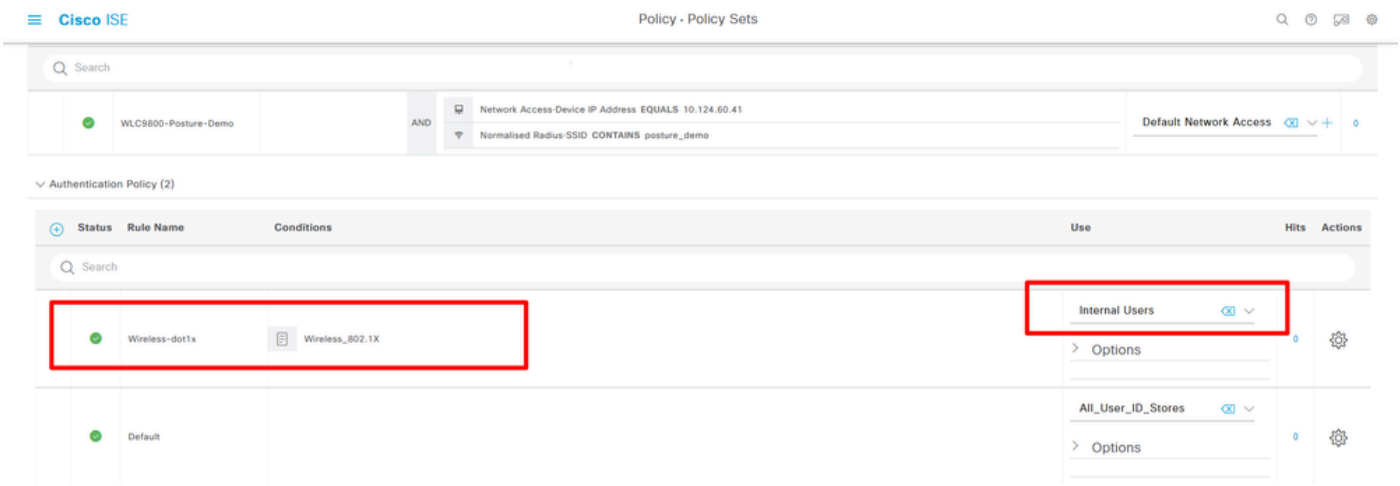


13단계. 정책 집합을 생성합니다. Policy(정책) > Policy(정책)로 이동합니다.

정책 집합 생성

설정> 추가 아이콘:

14단계. Create Authentication Policy(인증 정책 생성) Policy(정책) > Policy Sets(정책 집합) > Expand "WLC9800-Posture-Demo"(WLC9800-포스처-데모" 확장) > Authentication Policy(인증 정책) > Add(추가)로 이동합니다.



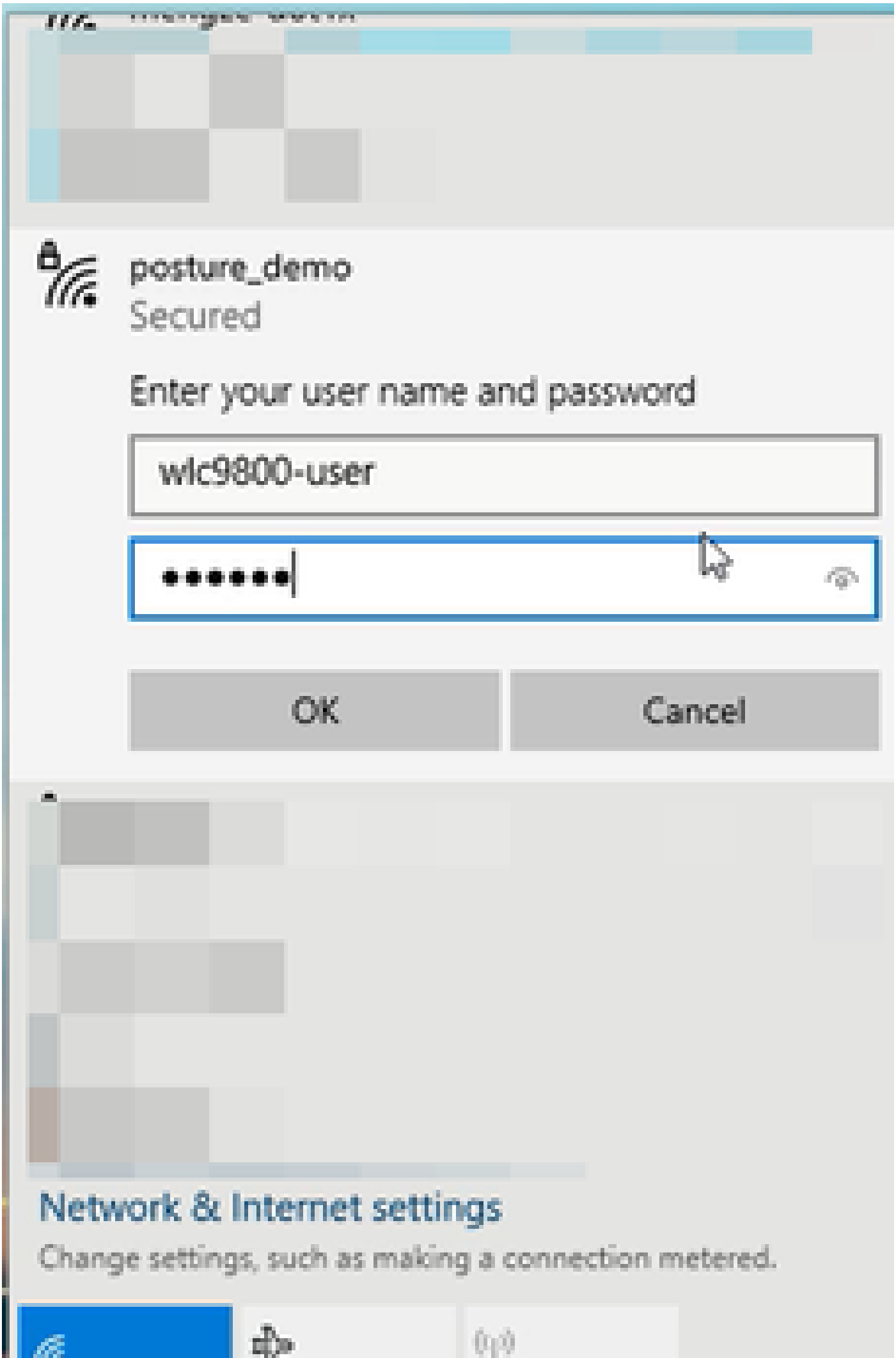
인증 정책 생성

15단계. Create Authorization Policy(권한 부여 정책 생성) Policy(정책) > Policy Sets(정책 집합) > Expand "WLC9800-Posture-Demo"(WLC9800-Posture-Demo"(WLC9800-Posture-Demo" 확장) > Authorization Policy(권한 부여 정책) > Add(추가)로 이동합니다.

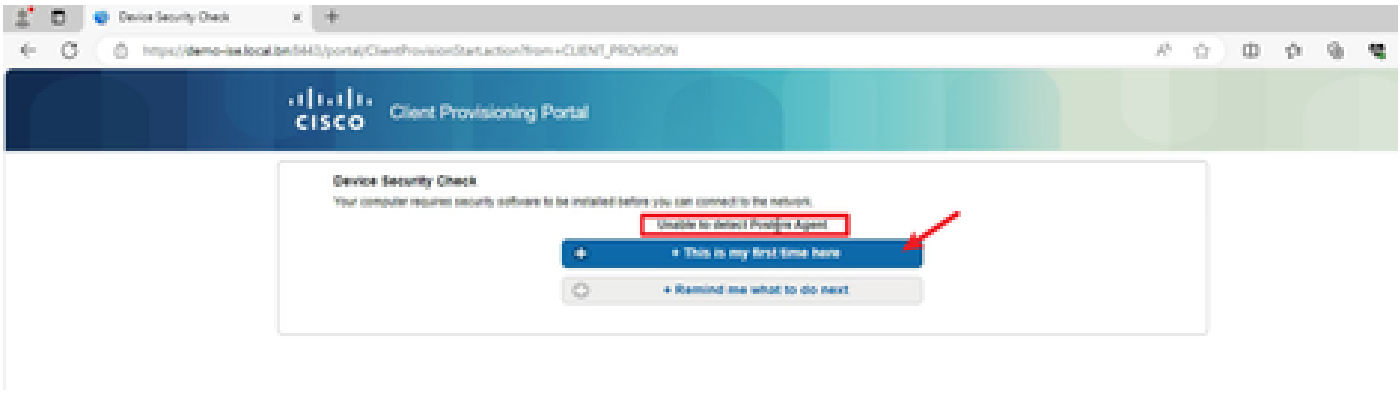
권한 부여 정책 생성

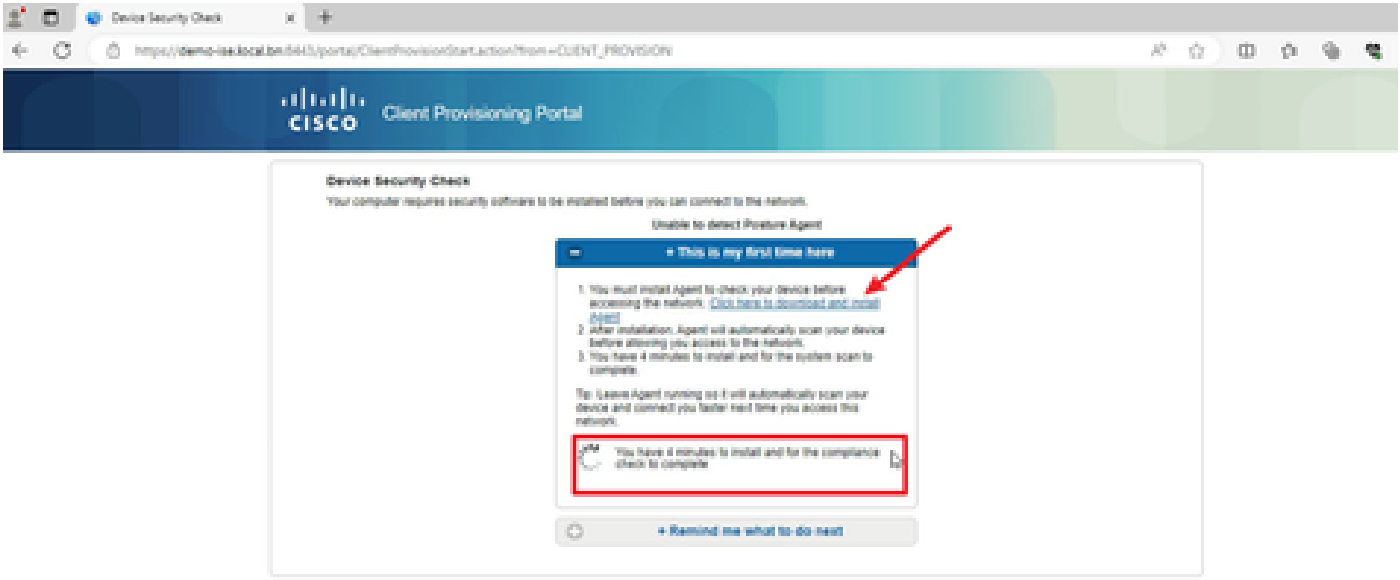
예

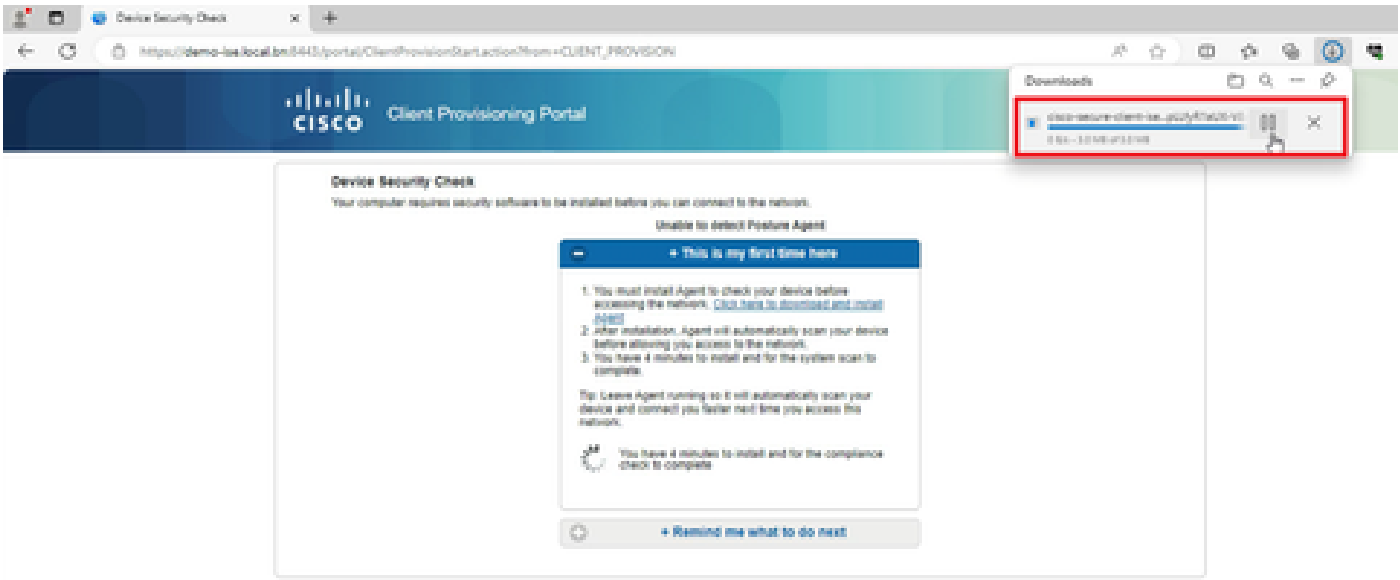
1. 올바른 802.1X 자격 증명을 사용하여 연결된 테스트 SSID posture_demo

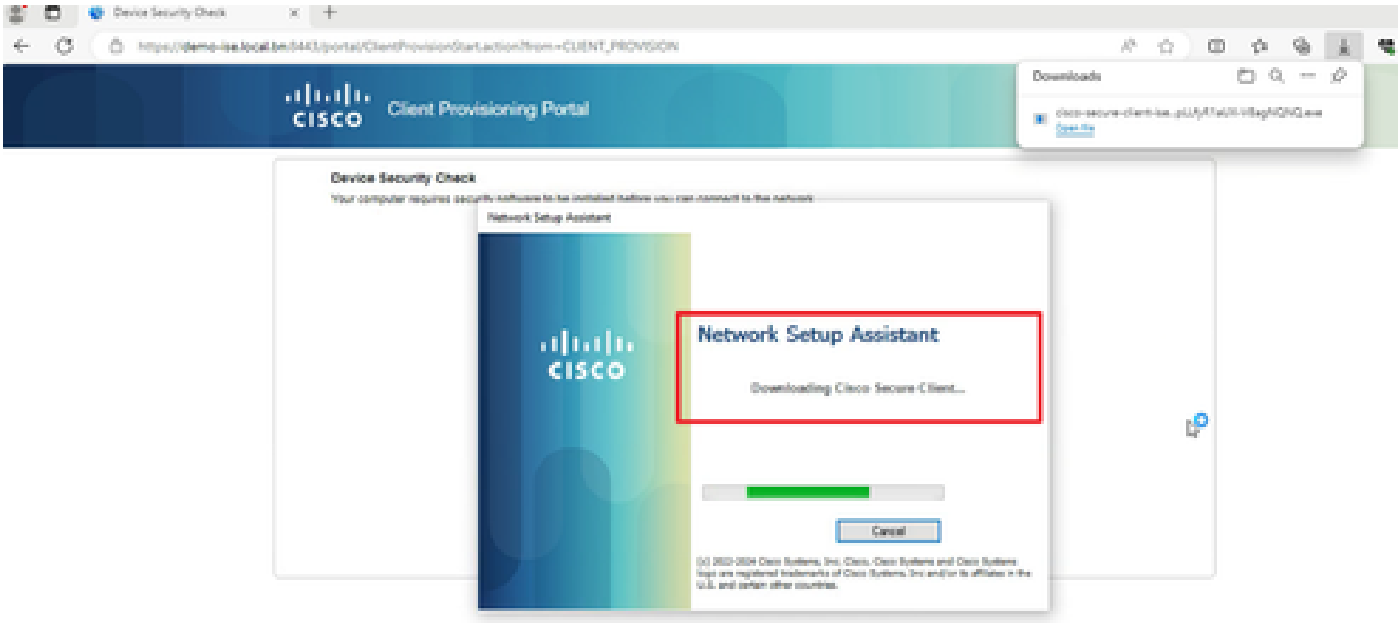

posture_demo
Secured
Enter your user name and password
wlc9800-user
OK
Cancel
Network & Internet settings
Change settings, such as making a connection metered.

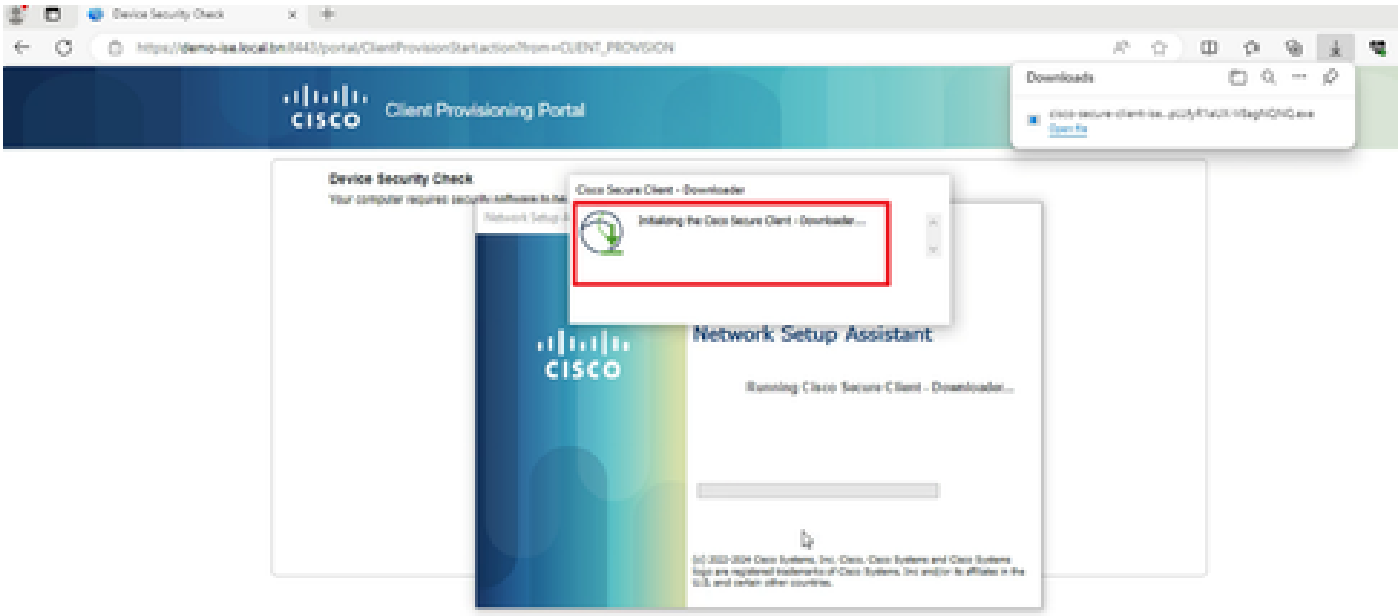
에 포스처 에이전트 버전이 설치되어 있지 않으면 "포스처 에이전트를 검색할 수 없습니다."라는 결과가 표시될 수 있습니다. 여기를 클릭하십시오. Agent를 다운로드하여 설치해야 합니다.

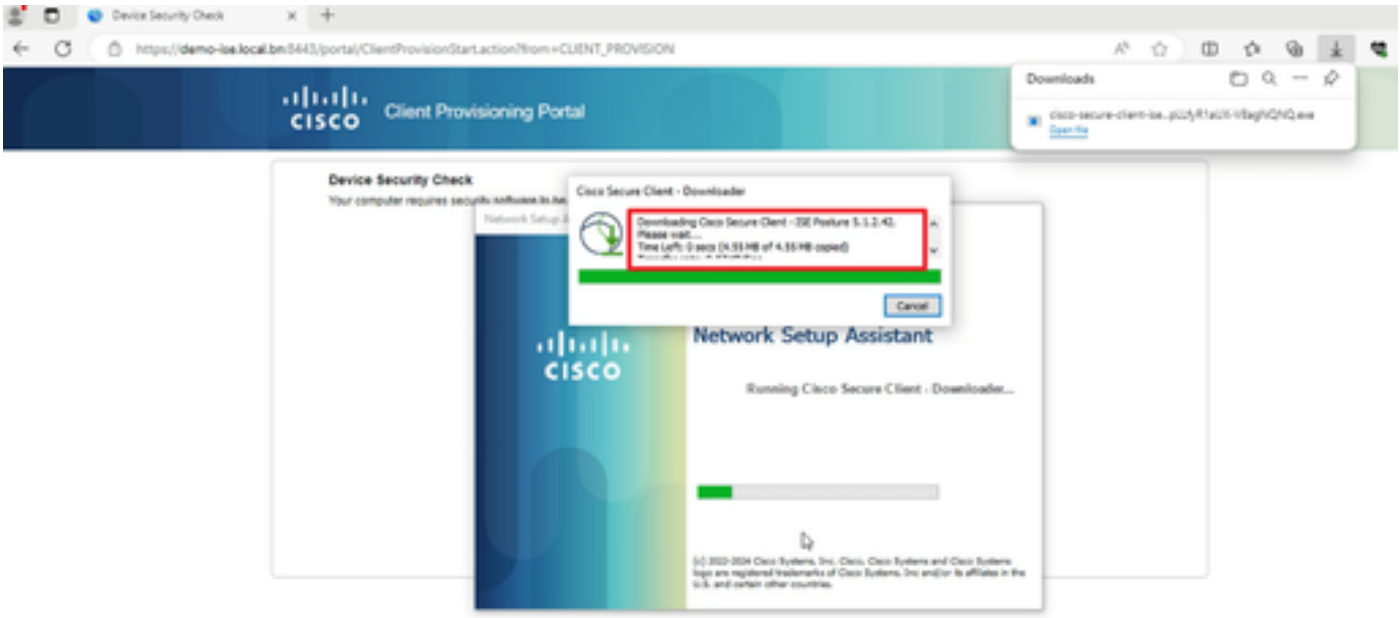


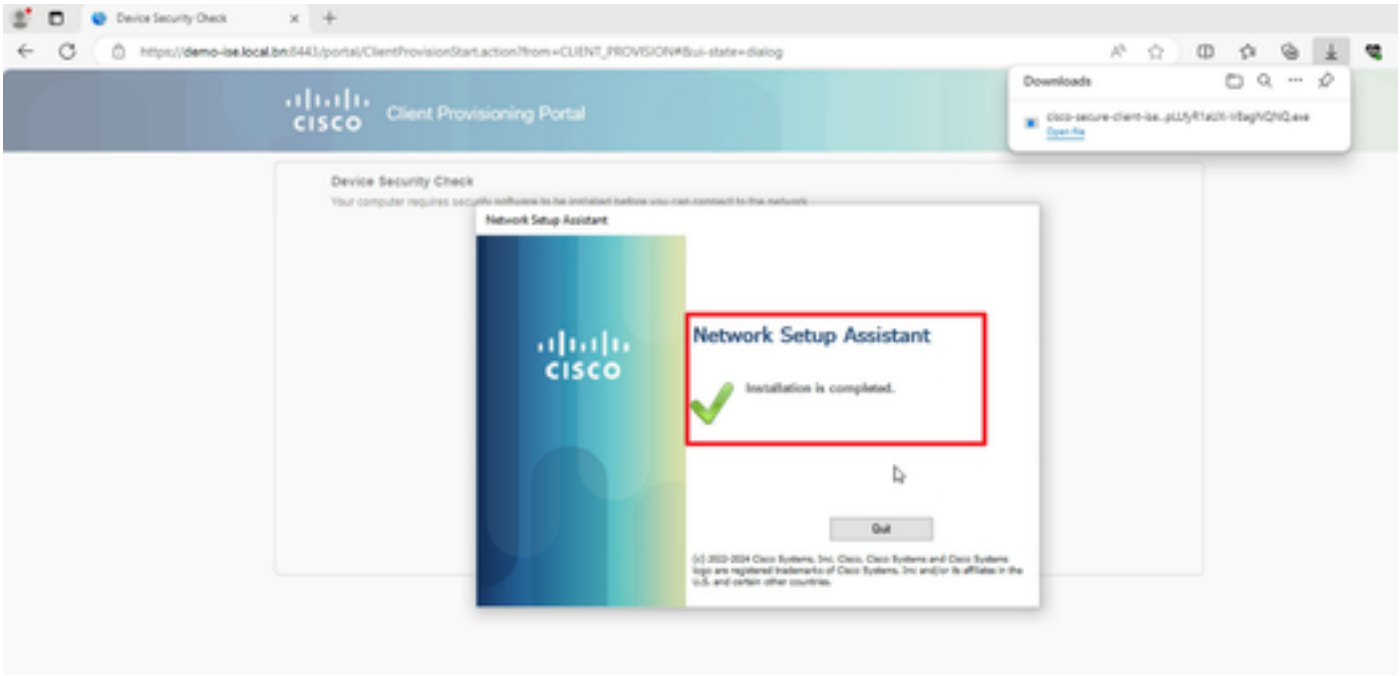




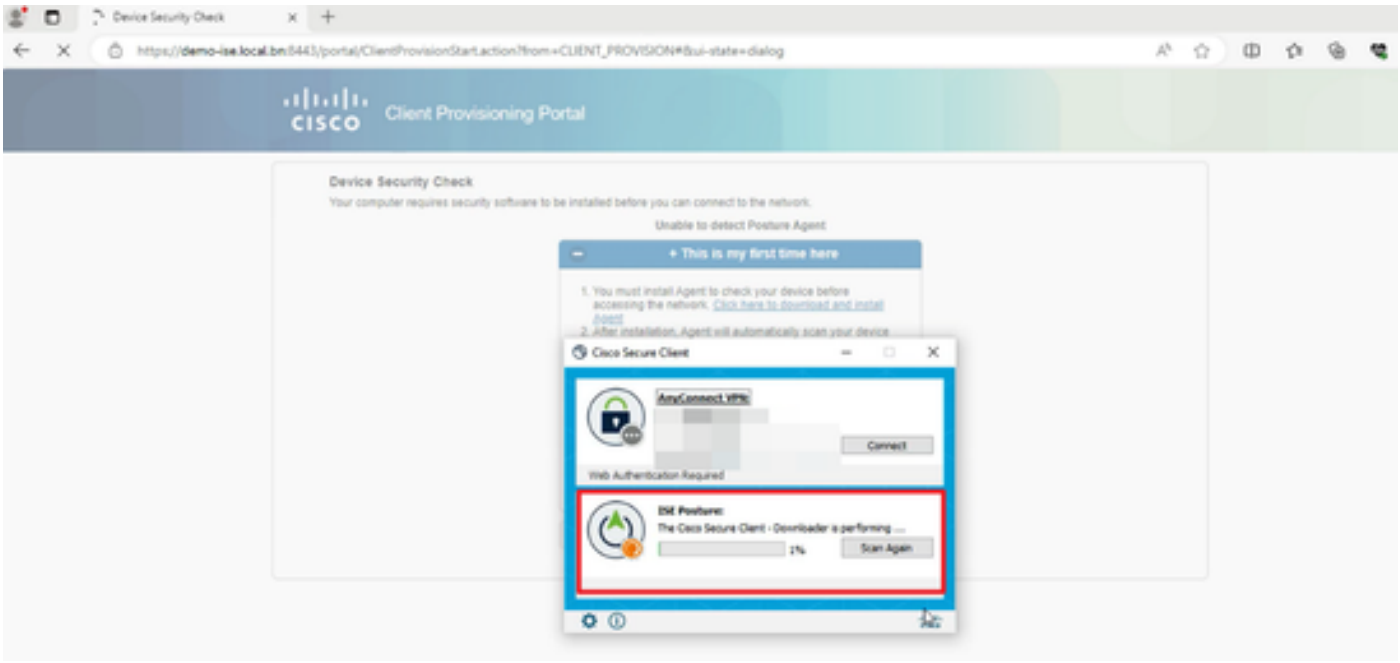

Client Provisioning Portal
Downloads
Device Security Check
Network Setup Assistant
Network Setup Assistant
Downloading Cisco Secure Client...
Cancel

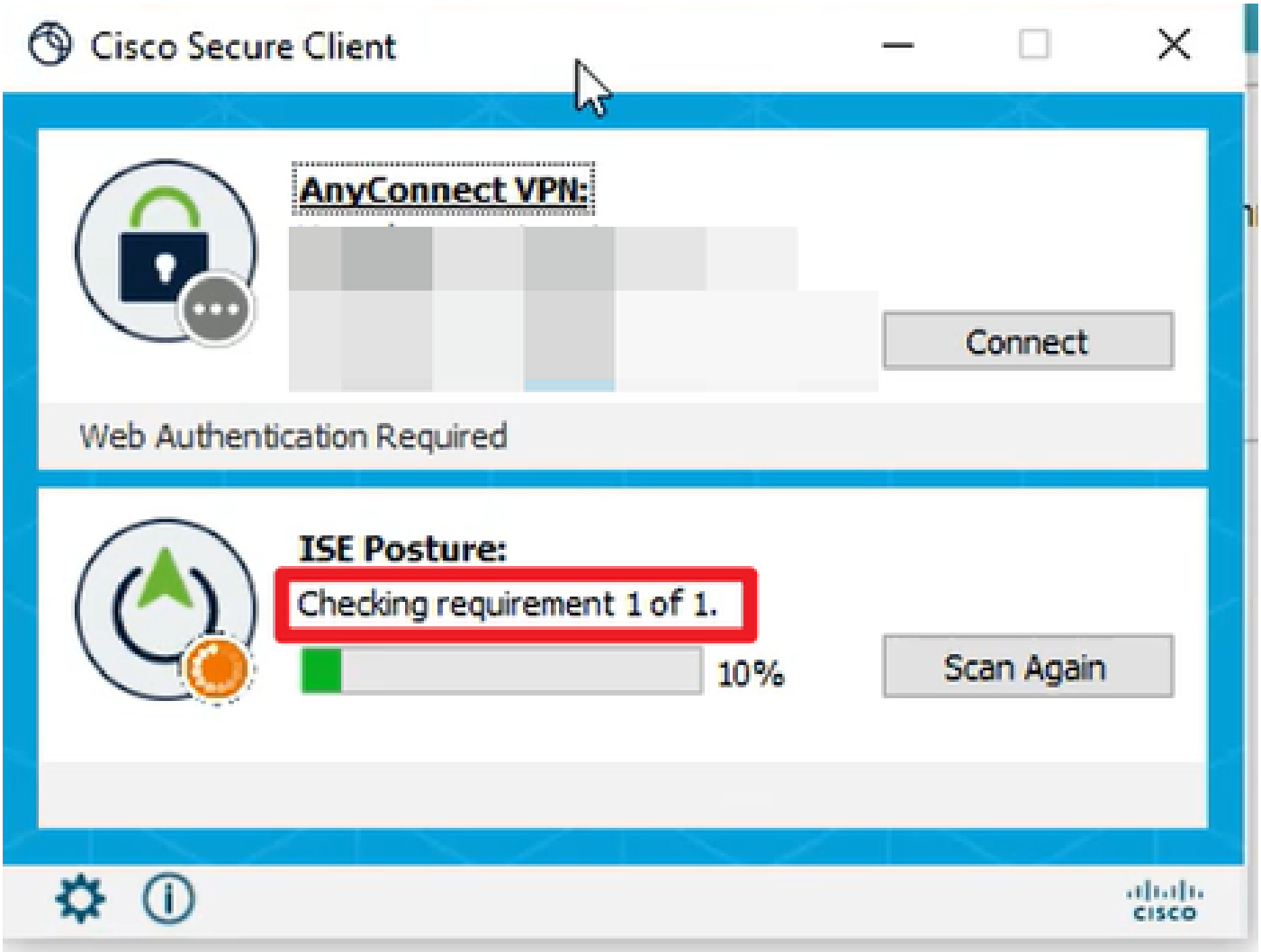

Client Provisioning Portal
Downloads
Device Security Check
Cisco Secure Client - Downloader
Initializing the Cisco Secure Client - Downloader...
Network Setup Assistant
Running Cisco Secure Client - Downloader...



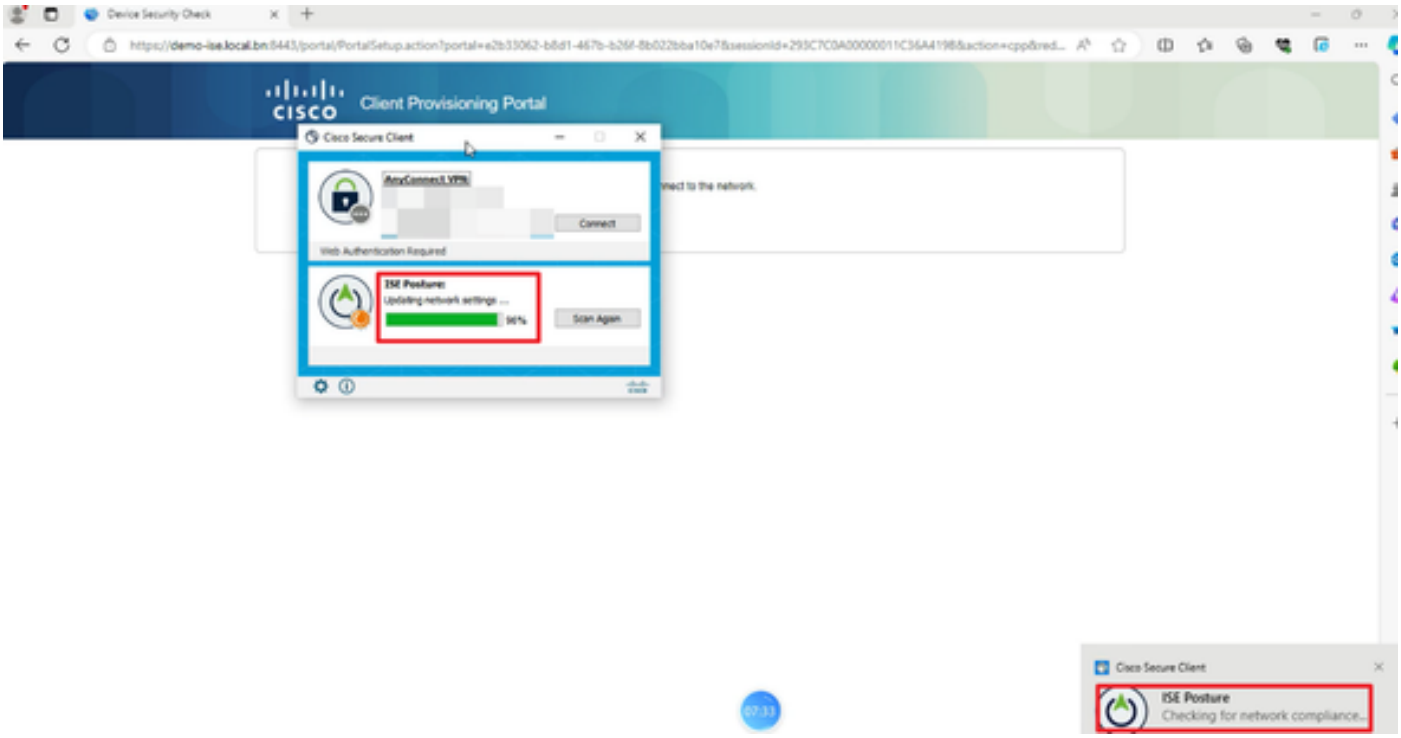


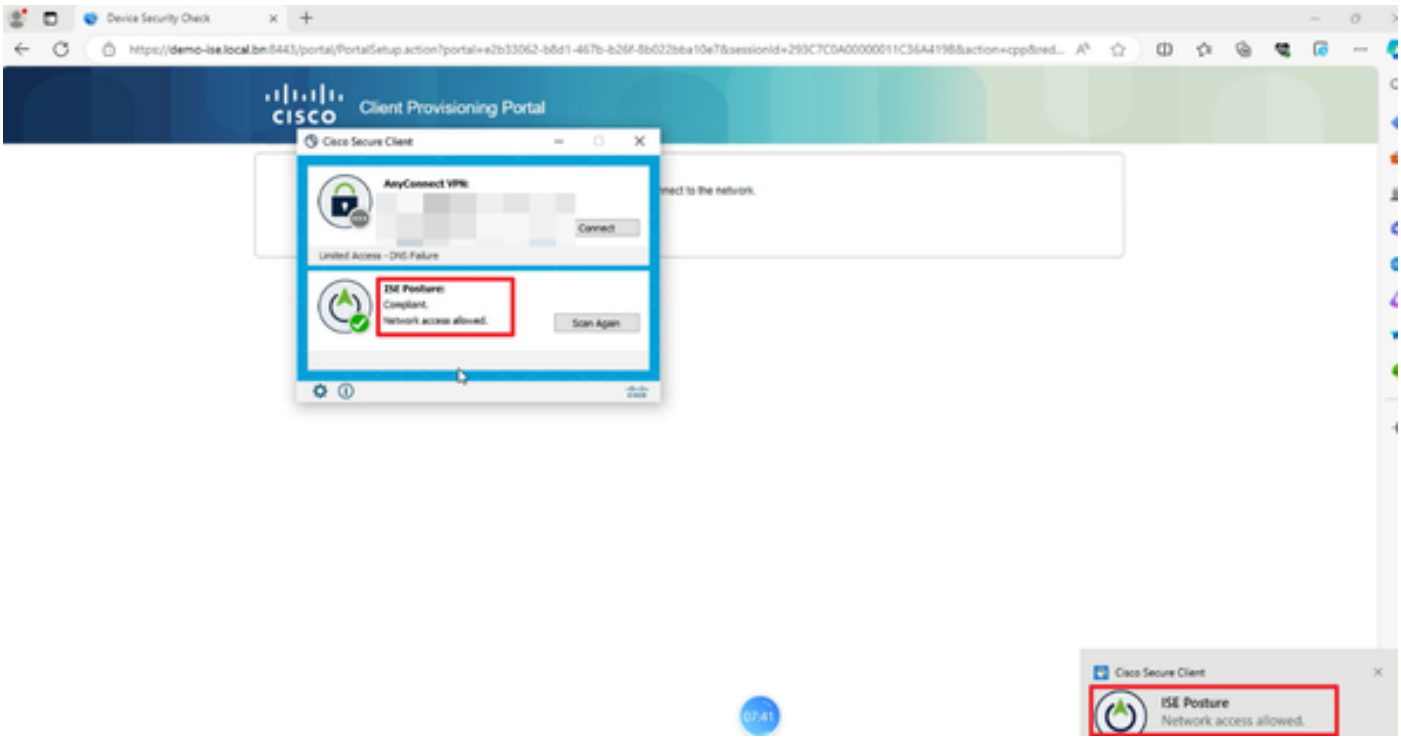
4. 상태 에이전트가 실행되고 ISE에서 상태 요구 사항을 가져옵니다.





5. 확인 결과가 포스처 요구 사항을 충족하면 PC가 포스처 규정 준수 보고서를 ISE에 보냅니다. 이 엔드포인트에 대해 Posture Status(상태)가 변경되었으므로 ISE가 CoA를 트리거합니다.

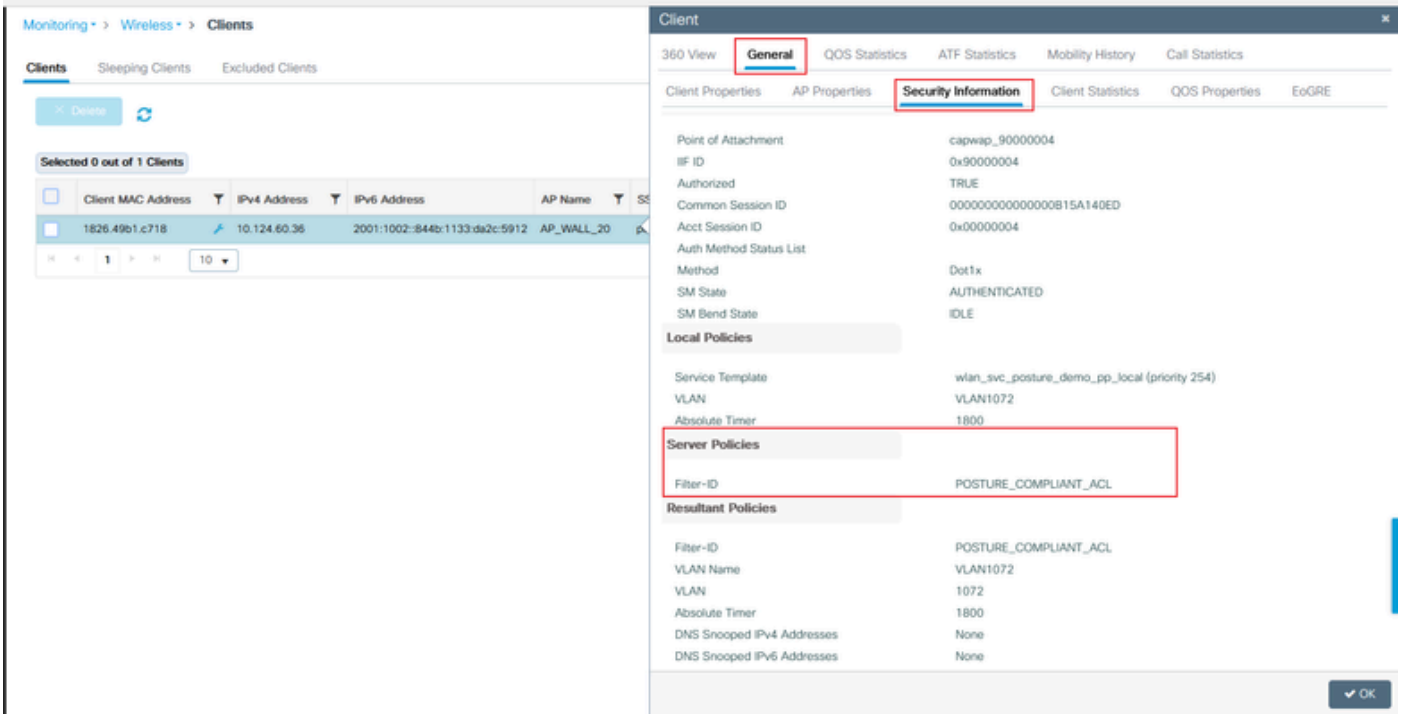




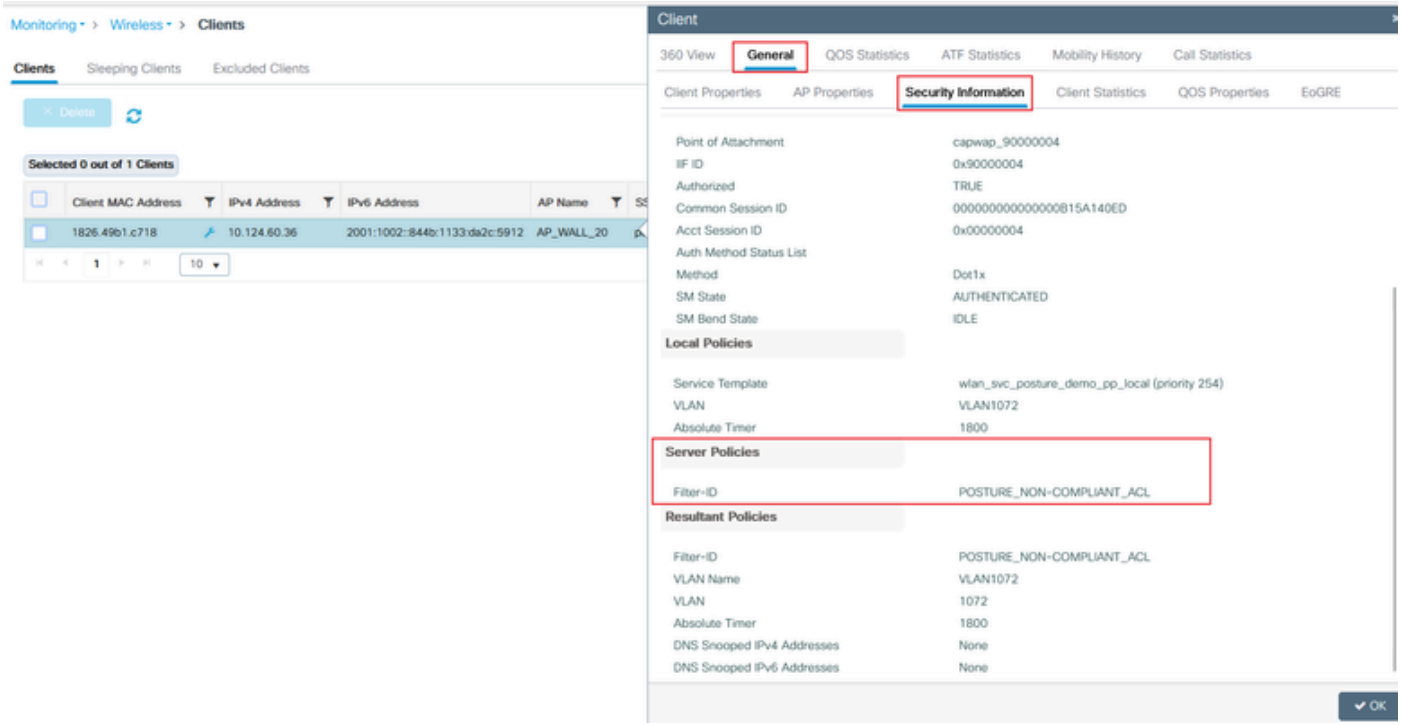
다음을 확인합니다.

C9800 GUI에서 클라이언트가 Complaint/Non-Complaint 포스처 결과에 따라 적절한 ACL을 얻는지 확인합니다.

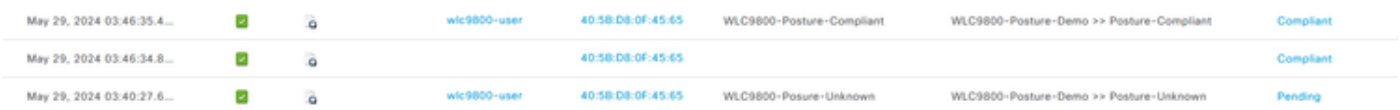
규정 준수:



규정 미준수:



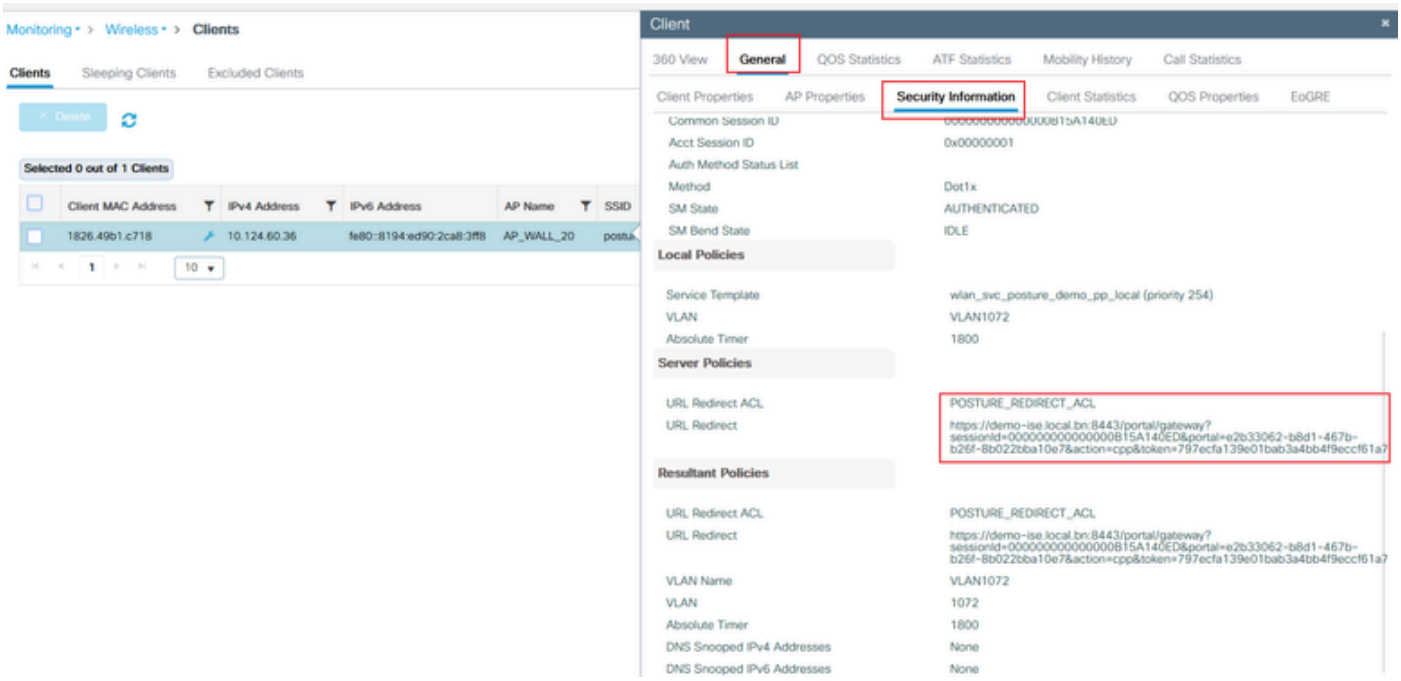
ISE에서 Radius 라이브 로그를 확인하여 올바른 정책이 일치하는지 확인합니다.



문제 해결

체크리스트

- 클라이언트가 연결되어 있고 유효한 IP 주소를 가져와야 합니다.
- WLC가 ISE에서 올바른 리디렉션 URL 및 ACL을 가져오는지 확인합니다. GUI를 통해 확인할 수 있습니다.



- 리디렉션이 자동이 아니면 브라우저를 열고 임의의 IP 주소를 시도합니다. 예를 들어 10.0.0.1입니다. 리디렉션이 작동하는 경우 DNS 확인 문제가 있을 수 있습니다. DHCP를 통해 제공된 유효한 DNS 서버가 있으며 호스트 이름을 확인할 수 있는지 확인합니다.
- 브라우저가 ISE 포털 URL로 리디렉션되었지만 페이지를 로드할 수 없는 경우, ISE 도메인 이름이 DNS 서버에 추가되지 않았는지 확인하십시오. 그러면 클라이언트가 포털 URL을 확인할 수 없습니다. 이 문제를 신속하게 해결하려면 Authorization Profile(권한 부여 프로파일)에서 Static IP/Host name/FQDN(고정 IP/호스트 이름/FQDN)을 확인하여 리디렉션 URL에 IP 주소를 제공합니다. 그러나 이는 ISE의 IP 주소를 노출하기 때문에 보안 문제가 될 수 있습니다.

디버그 수집

[C9800에서 디버그 사용]

[ISE에서 디버깅 활성화]

참조

- Catalyst 9800 WLC 및 ISE에서 CWA 구성 - Cisco
- Identity Services Engine을 사용하는 무선 BYOD
- ISE Posture 구축
- ISE 세션 관리 및 상태 문제 해결
- ISE Posture 리디렉션 플로우를 ISE Posture 리디렉션 플로우와 비교Redirectionless Flow

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.