ISE 3.3에서 단일 및 이중 SSID를 사용하여 ISE BYOD 구성

목차

소개

이 문서에서는 ISE에서 BYOD 문제를 구성하고 트러블슈팅하는 방법에 대해 설명합니다.

배경

BYOD는 사용자가 ISE에서 개인 디바이스를 온보딩하여 환경에서 네트워크 리소스를 사용할 수 있도록 하는 기능입니다. 또한 네트워크 관리자가 사용자가 개인 디바이스에서 중요한 리소스에 액세스하는 것을 제한할 수 있습니다.

ISE의 내부 저장소 또는 Active Directory를 사용하여 게스트 페이지에서 디바이스를 인증하는 게스트 흐름과 다릅니다. BYOD를 통해 네트워크 관리자는 엔드포인트에 엔드포인트 프로파일을 설치하여 EAP 방법 유형을 선택할 수 있습니다. EAP-TLS와 같은 시나리오에서 클라이언트 인증서는 엔드포인트와 ISE 간에 신뢰를 생성하기 위해 ISE 자체에서 서명됩니다.

사전 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- WLC 컨트롤러
- ISE에 대한 기본 지식

사용된 구성 요소

사용되는 이러한 디바이스는 BYOD 플로우의 특정 버전 하나로 제한되지 않습니다.

- Catalyst 9800-CL Wireless Controller(17.12.3)
- ISE 가상 머신(3.3)

ISE의 단일 SSID 및 이중 SSID BYOD란 무엇입니까?

단일 SSID BYOD

단일 SSID BYOD 설정에서 사용자는 개인 장치를 기업 무선 네트워크에 직접 연결합니다. 온보딩 프로세스는 동일한 SSID에서 발생하며, 여기서 ISE는 디바이스 등록, 프로비저닝 및 정책 시행을 용이하게 합니다. 이 접근 방식은 사용자 환경을 간소화하지만 네트워크 보안을 보장하기 위해 보안 온보딩과 적절한 인증 방법이 필요합니다.

듀얼 SSID BYOD

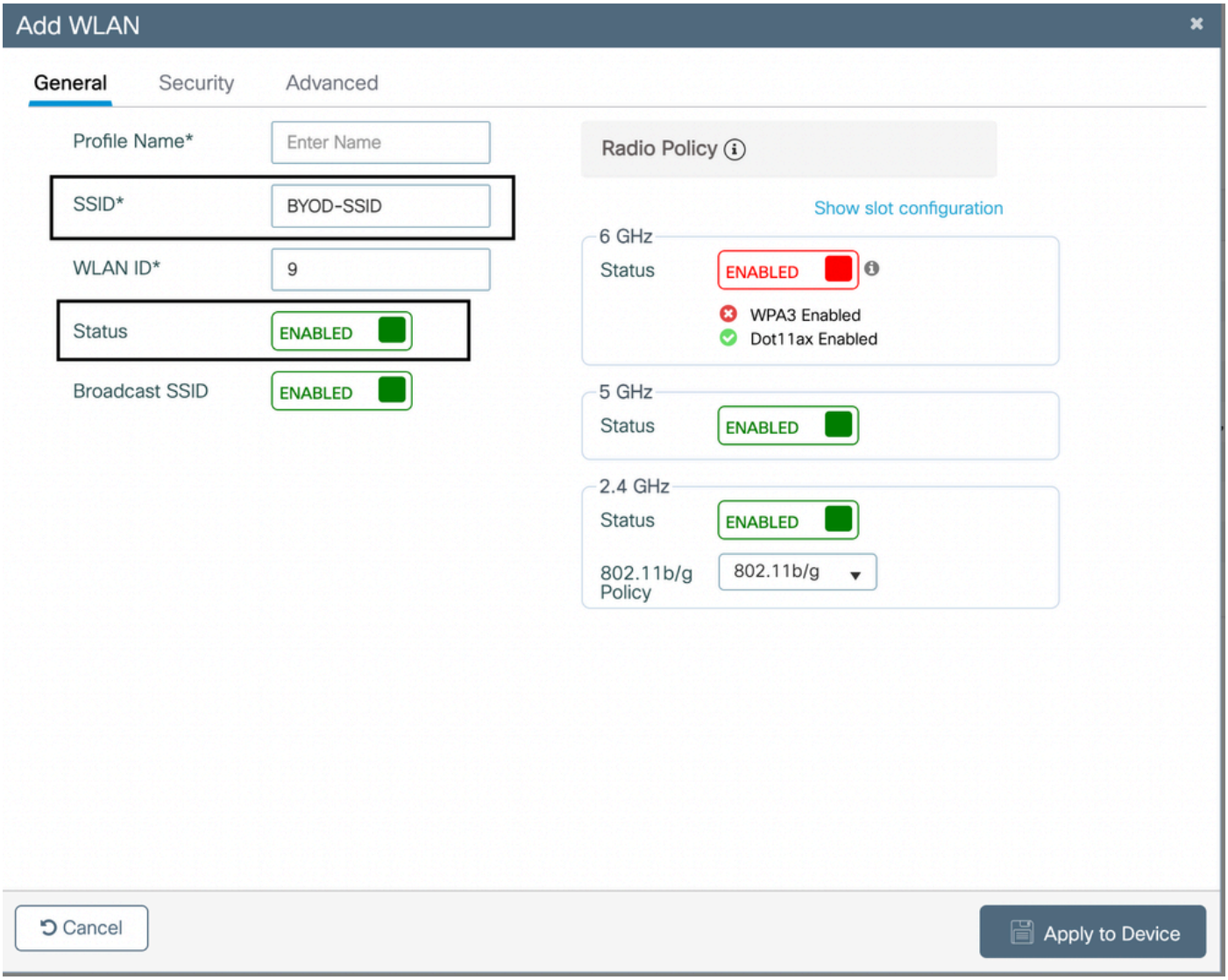
듀얼 SSID BYOD 설정에서는 두 개의 개별 SSID가 사용됩니다. 하나는 온보딩(안전하지 않은 액세스 또는 제한된 액세스)용이고 다른 하나는 기업 네트워크 액세스용입니다. 사용자는 처음에 온보딩 SSID에 연결하고 ISE를 통해 디바이스 등록 및 프로비저닝을 완료한 다음 네트워크 액세스를 위해 보안 기업 SSID로 전환합니다. 따라서 온보딩 트래픽을 프로덕션 트래픽에서 분리하여 보안을 한층 강화할 수 있습니다.

WLC 컨피그레이션

CWA용 WLAN 생성

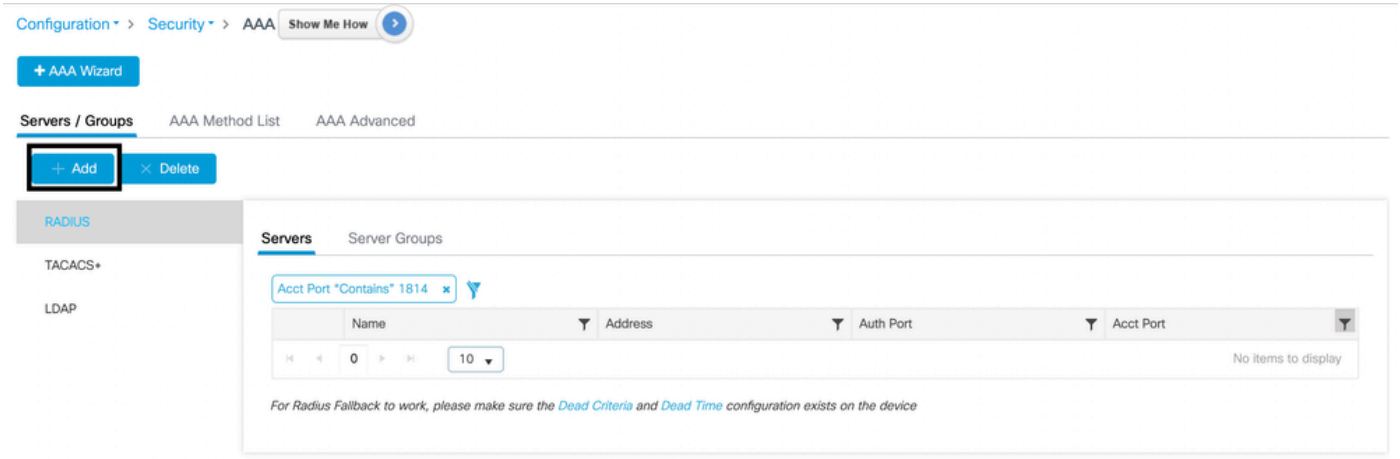
1. Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로필) > WLANs로 이동합니다.
2. Add(추가)를 클릭하여 새 WLAN을 생성합니다.

   - WLAN 이름 및 SSID(예: BYOD-WiFi)를 설정합니다.
   - WLAN을 활성화합니다.

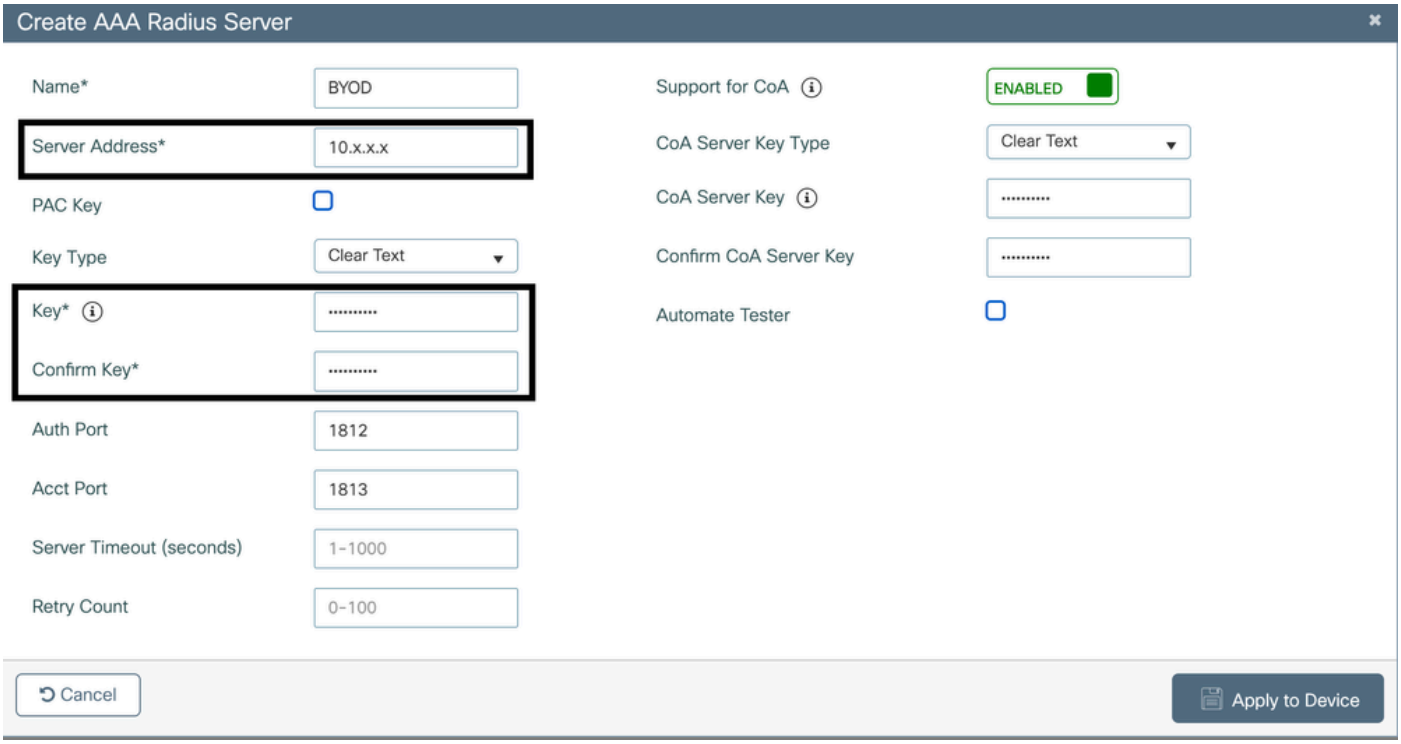


RADIUS 서버 구성

1. Configuration(컨피그레이션) > Security(보안) > AAA > RADIUS > Servers(서버)로 이동합니다.

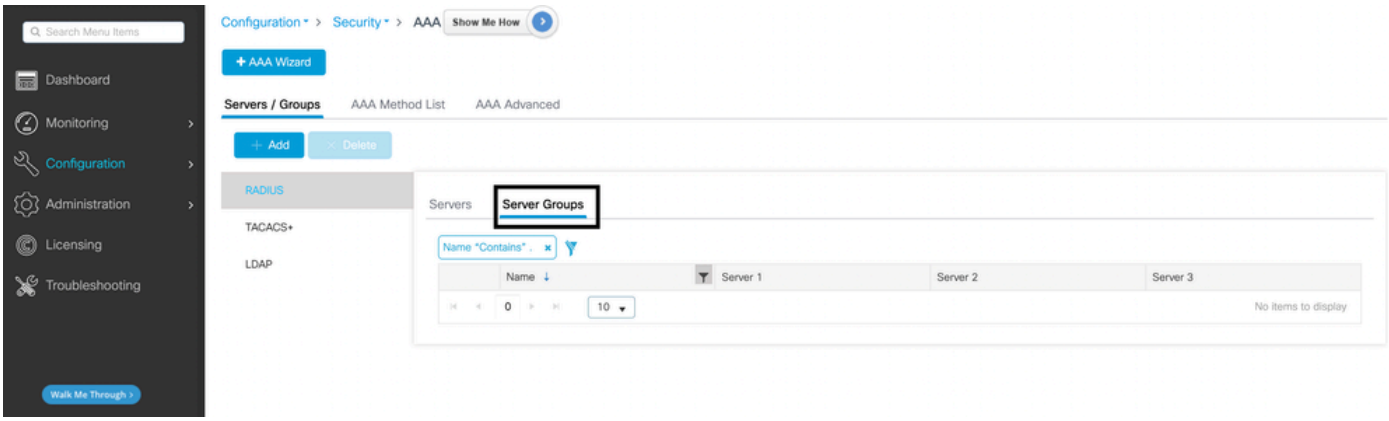


2. ISE를 RADIUS 서버로 구성하려면 Add(추가)를 클릭합니다.
    - 서버 IP: ISE의 IP 주소입니다.
    - 공유 암호: ISE에 구성된 공유 암호를 확인합니다.

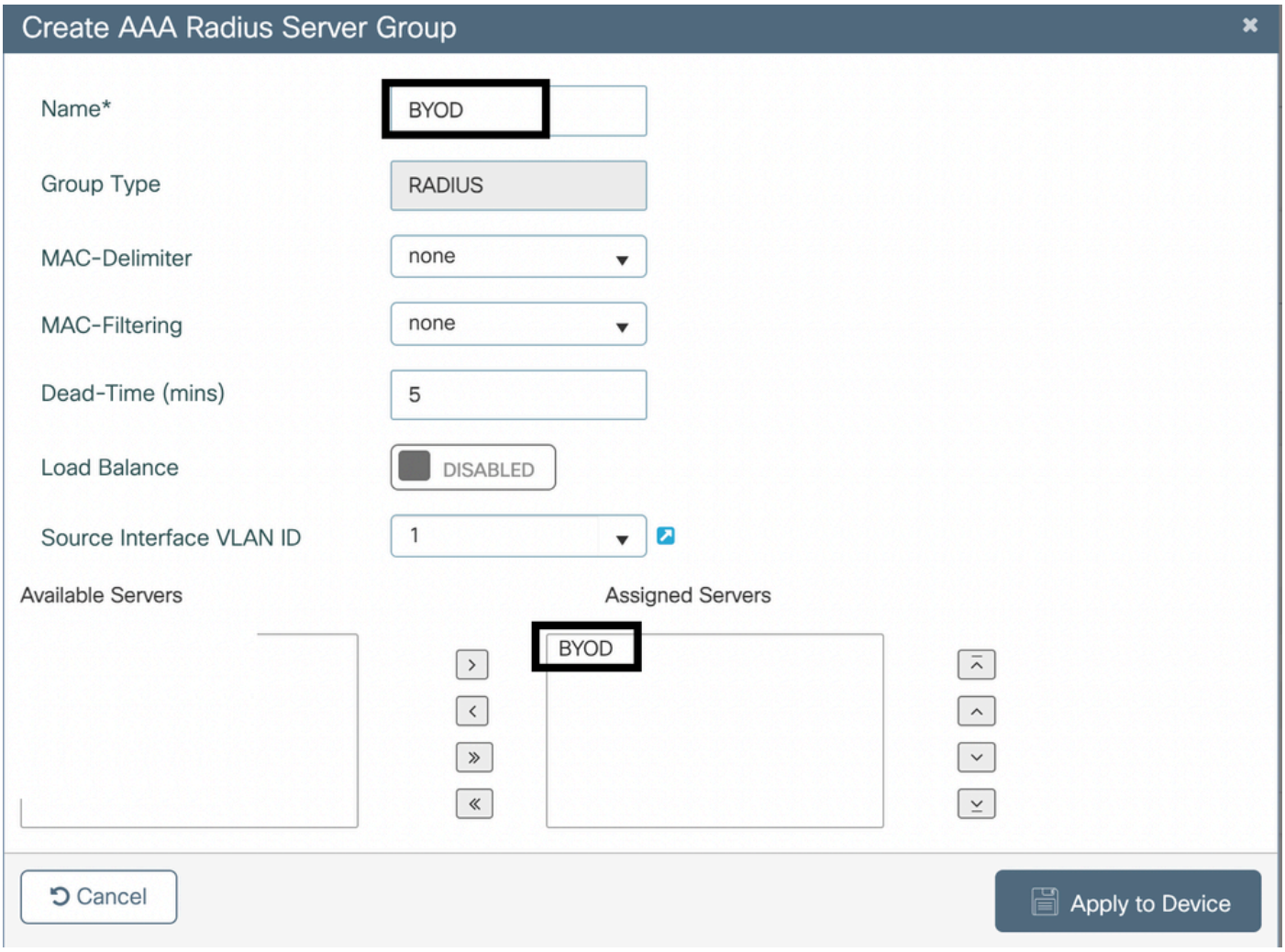


AAA 서버 구성

1. Configuration(컨피그레이션) > Security(보안) > AAA > Servers/Groups(서버/그룹)로 이동합니다.



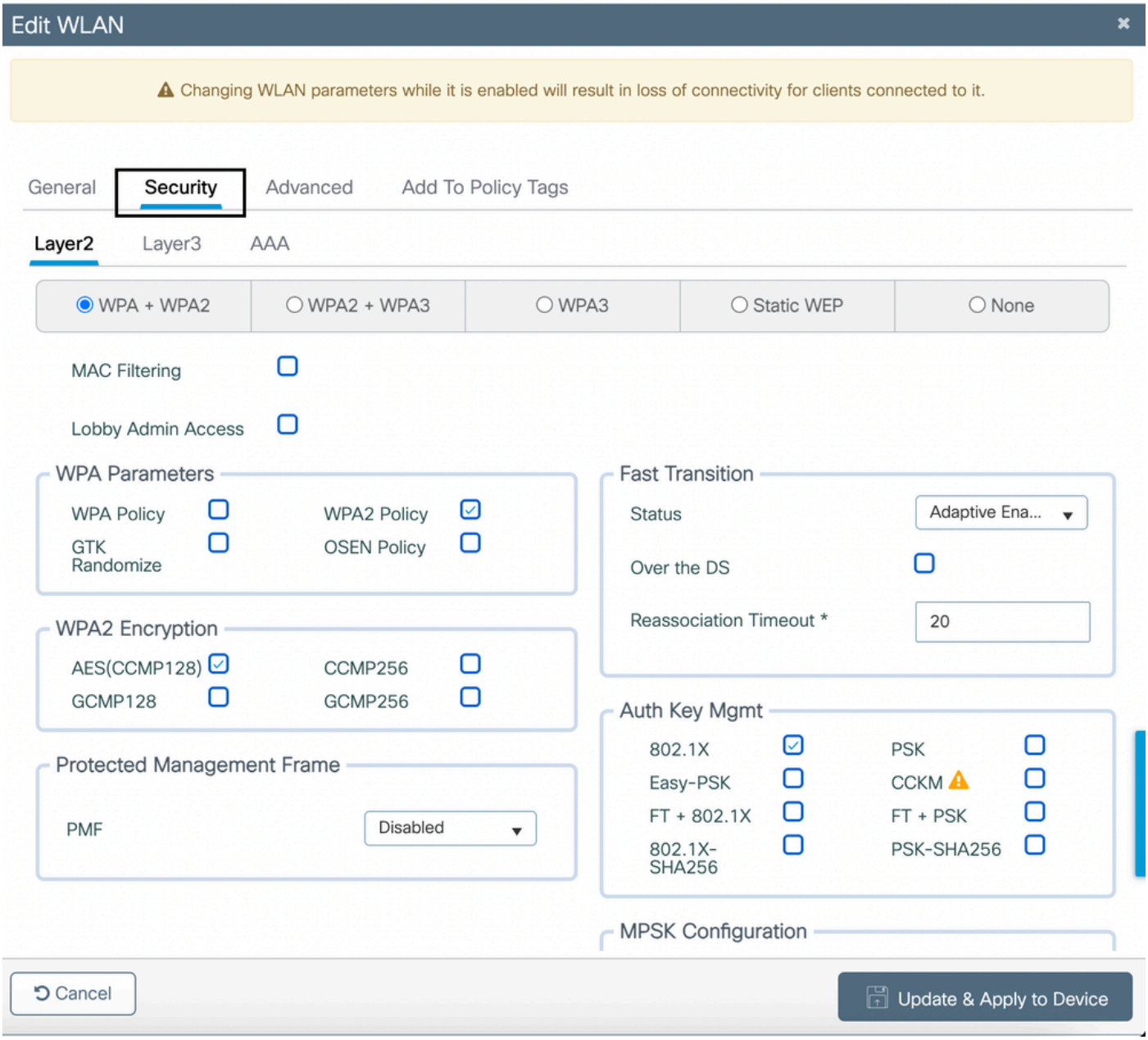
2. RADIUS 서버를 신규 또는 기존 서버 그룹에 할당합니다.



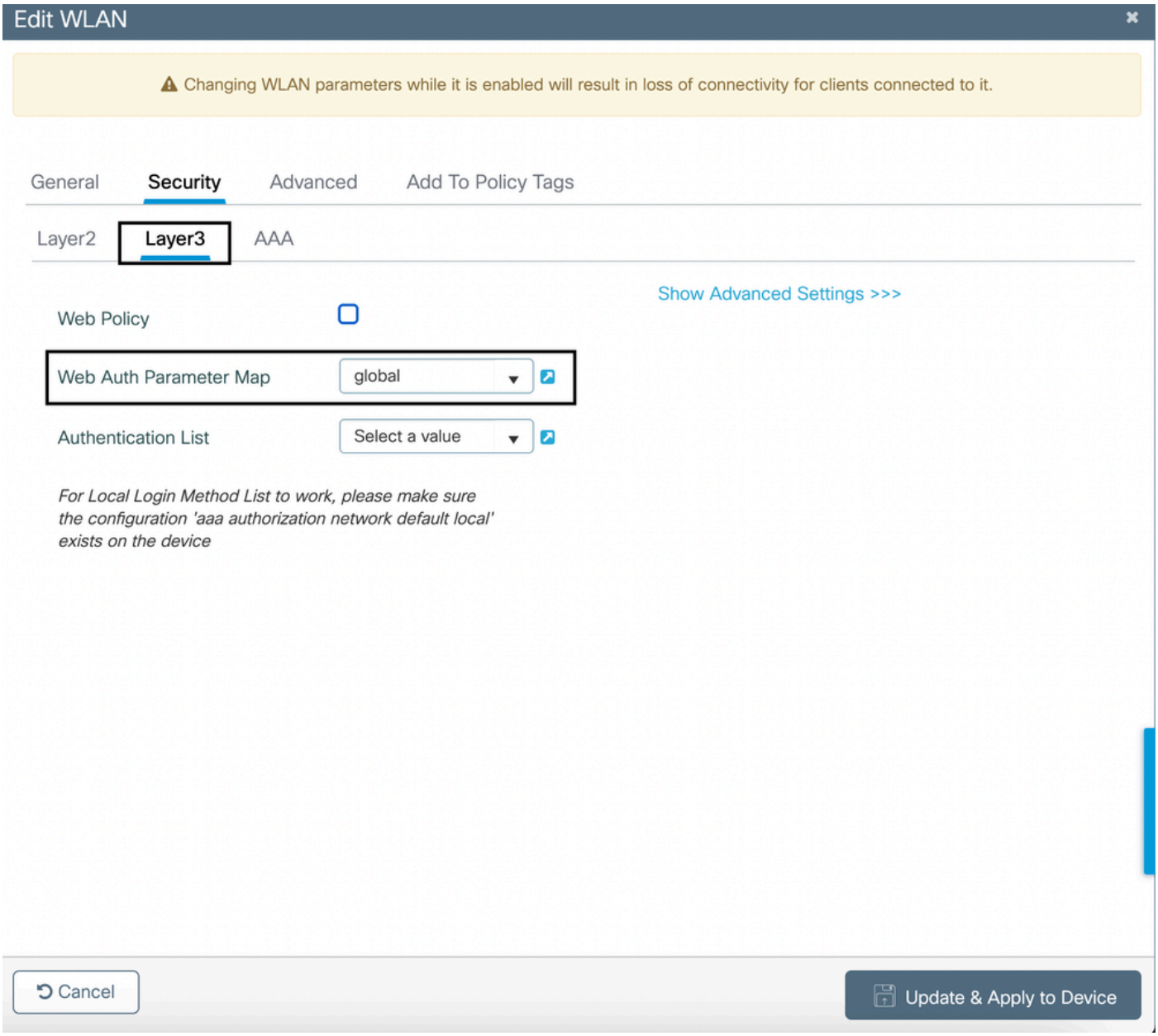
WLAN에 대한 보안 정책 구성

1. Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로필) > WLANs(WLAN)로 이동합니다. 이전에 생성한 WLAN을 편집합니다.

2. Security(보안) > Layer 2(레이어 2) 탭 아래에서 다음을 수행합니다.
   - WPA+WPA2 사용
   - WPA2 암호화에서 AES(CCMP128) 설정
   - 802.1X로 인증 키 관리



3. Security(보안) > Layer 3(레이어 3) 탭 아래의 Web Auth Parameter Map(웹 인증 매개변수 맵) 드롭다운에서 global(전역)을 선택합니다.



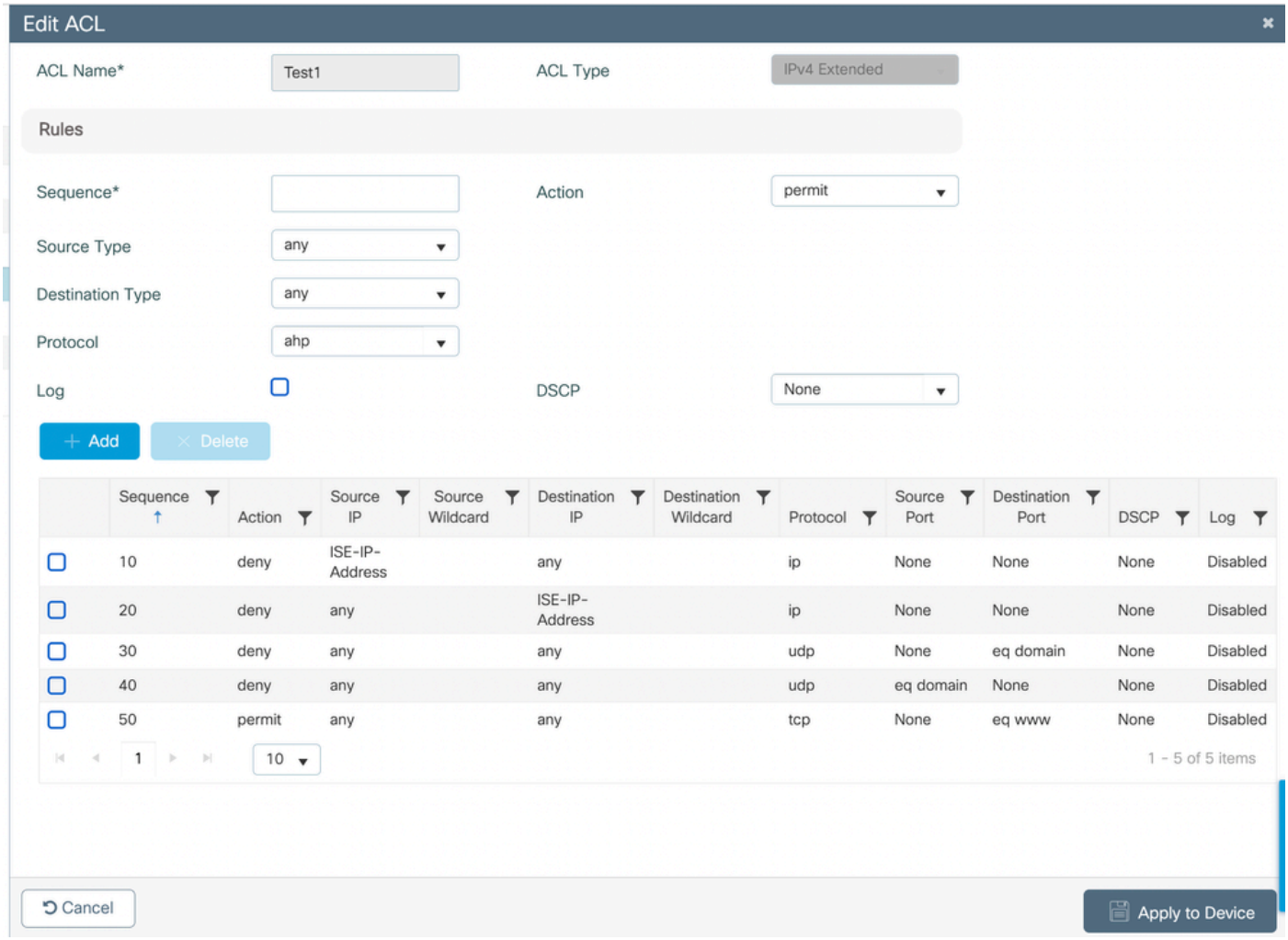
사전 인증 ACL 구성

ACL을 생성하여리디렉션에 대한 작업 사용:

- DNS 트래픽
- ISE 포털에 대한 HTTP/HTTPS
- 필요한 모든 백엔드 서비스.

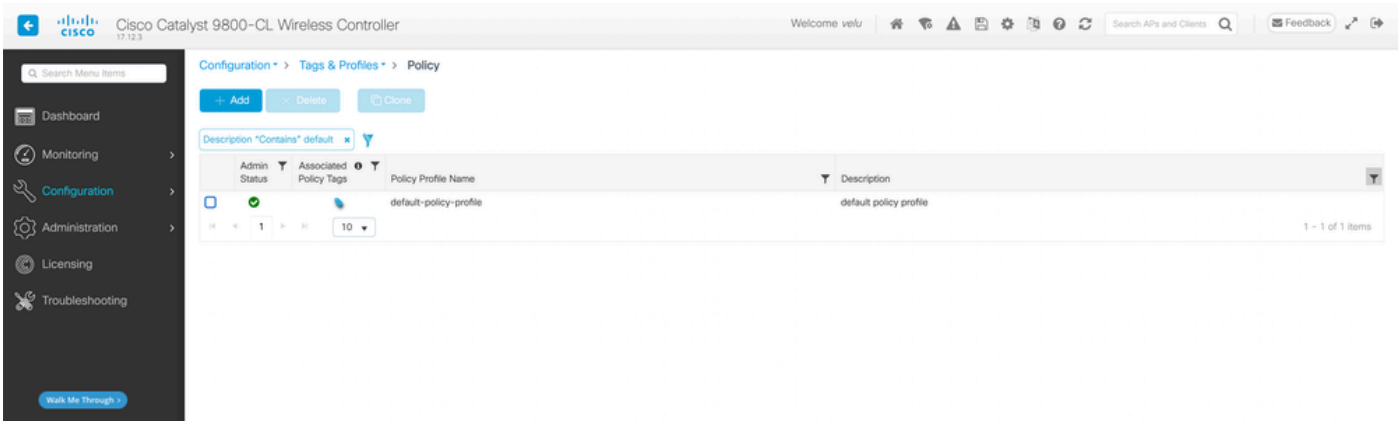
이렇게 하려면

1. Configuration > Security > ACLs > Access Control Lists로 이동합니다.
2. 필요한 트래픽을 허용하는 규칙으로 새 ACL을 생성합니다.

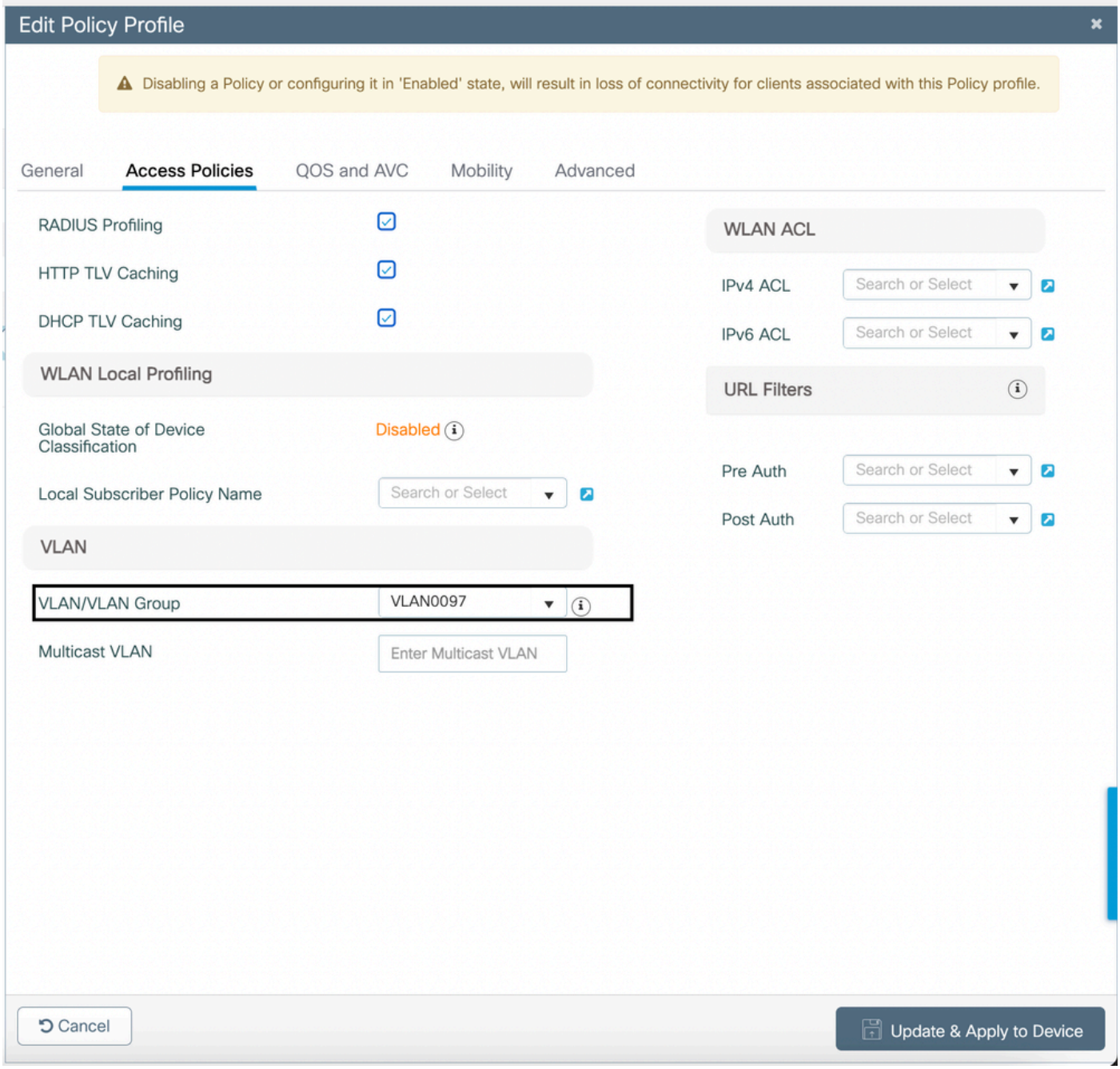


정책 프로필 구성

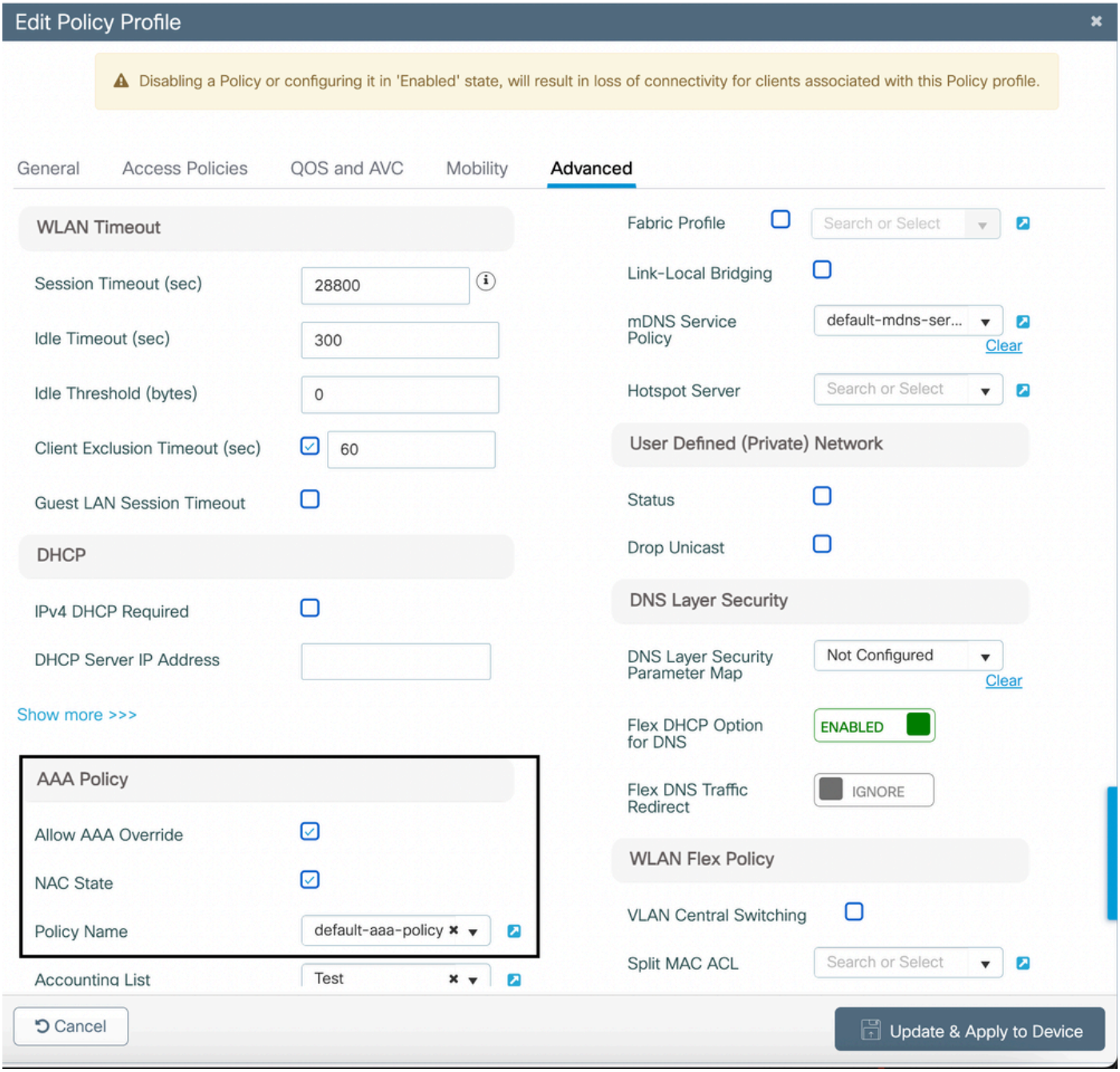
1. Configuration > Tags & Profiles > Policy로 이동합니다. 기본 정책을 생성하거나 사용할 수 있습니다



2. Access Policies(액세스 정책)에서 적절한 VLAN 할당

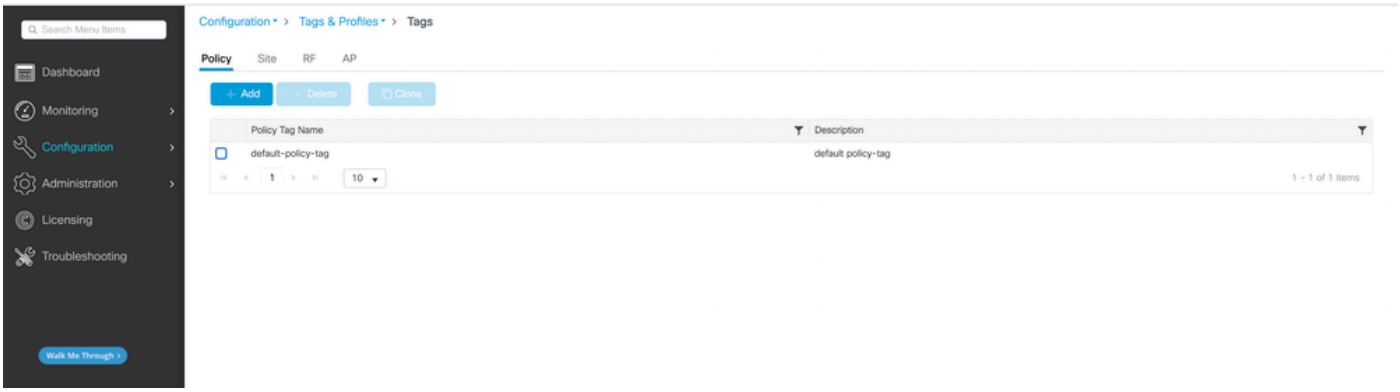


3. 또한 Advanced(고급) 정책에서 Allow AAA Override and NAC state(AAA 재정의 및 NAC 상태 허용)를 활성화합니다.



태그 적용 및 배포

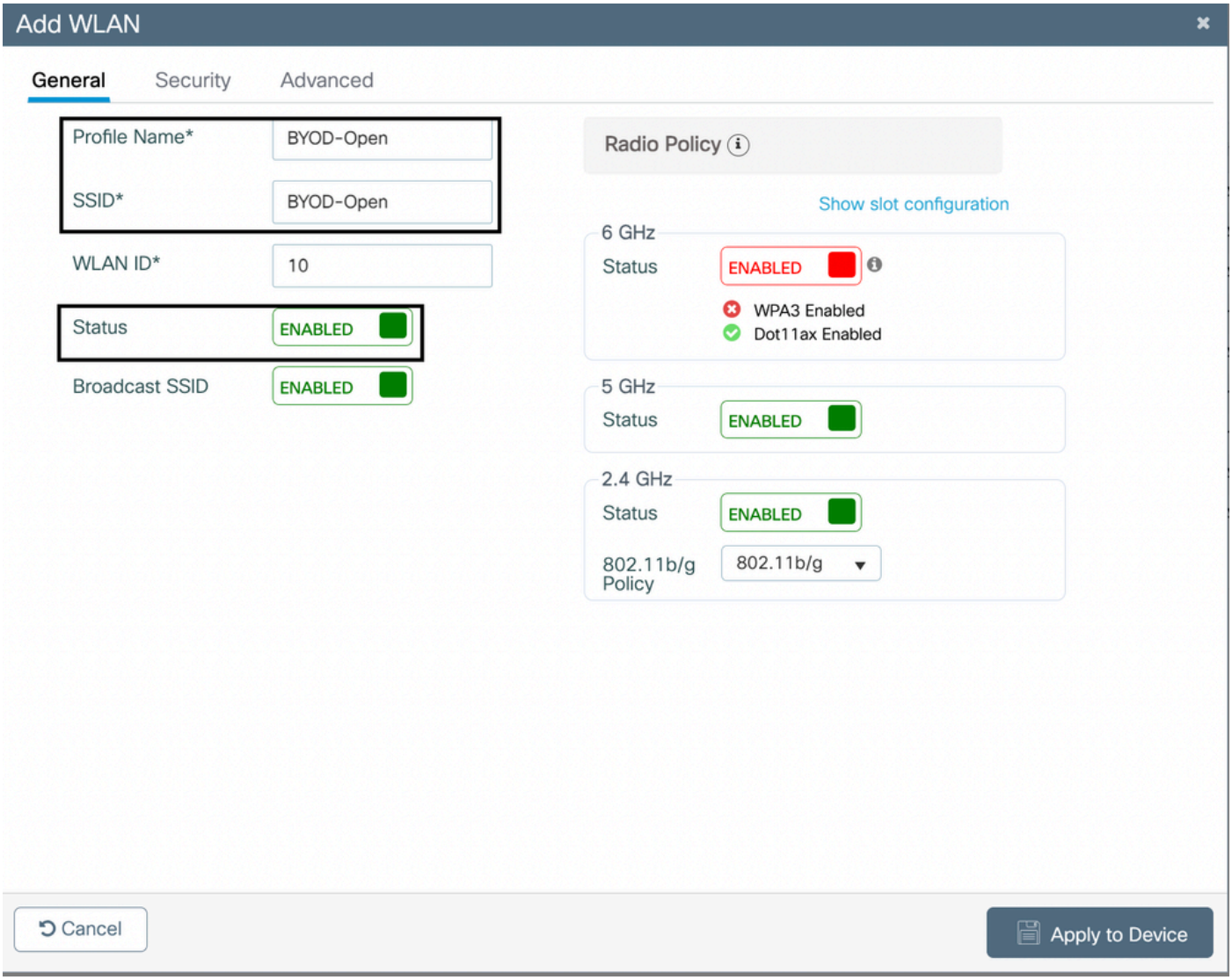
- Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로파일) > Tags(태그)로 이동합니다.
- WLAN 및 정책 프로필을 포함하도록 태그를 만들거나 수정합니다.
- 액세스 포인트에 태그를 할당합니다.



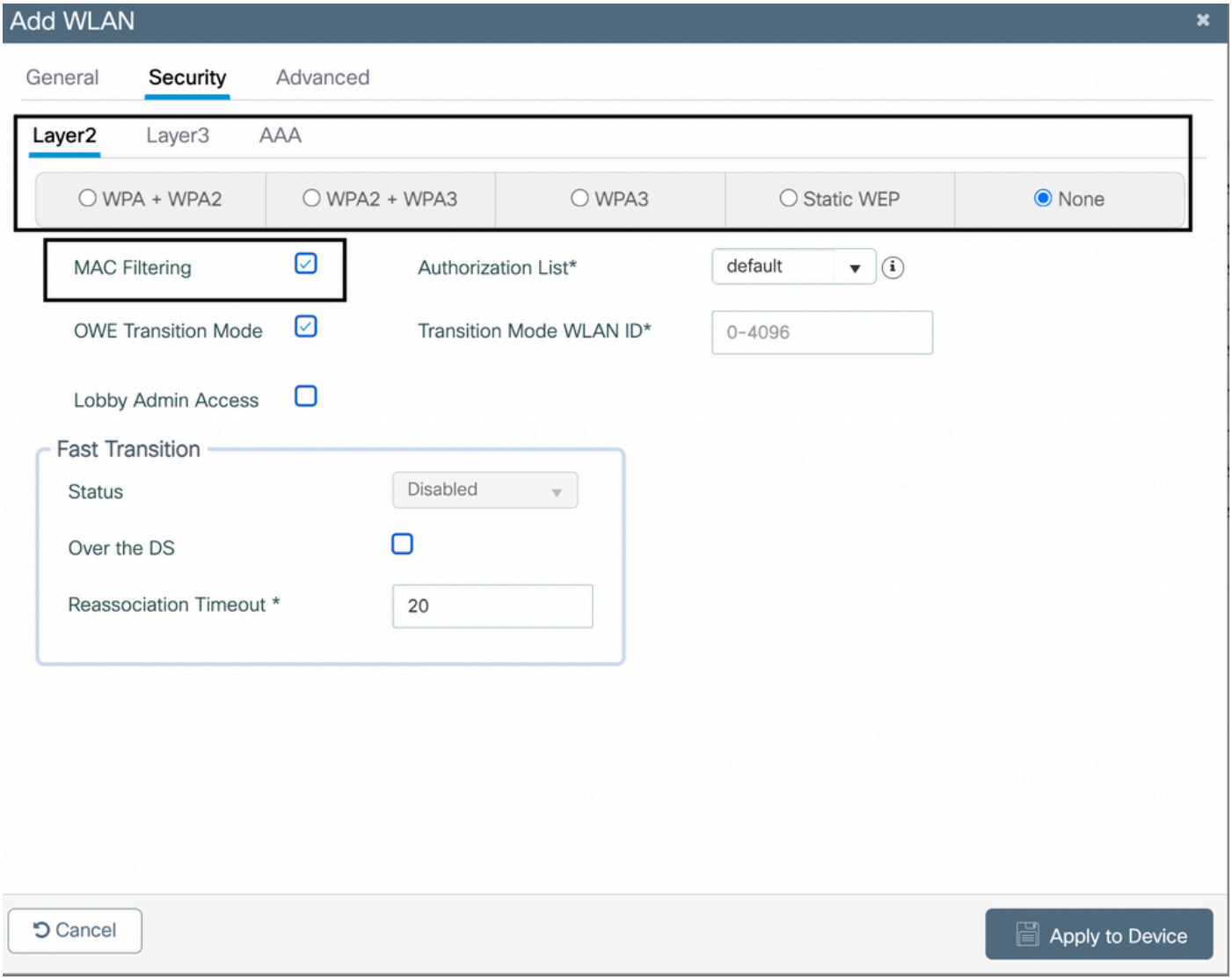
개방/비보안 SSID 구성

환경에 이중 SSID BYOD 컨피그레이션을 설정하기로 결정한 경우에만 Open SSID가 생성됩니다.

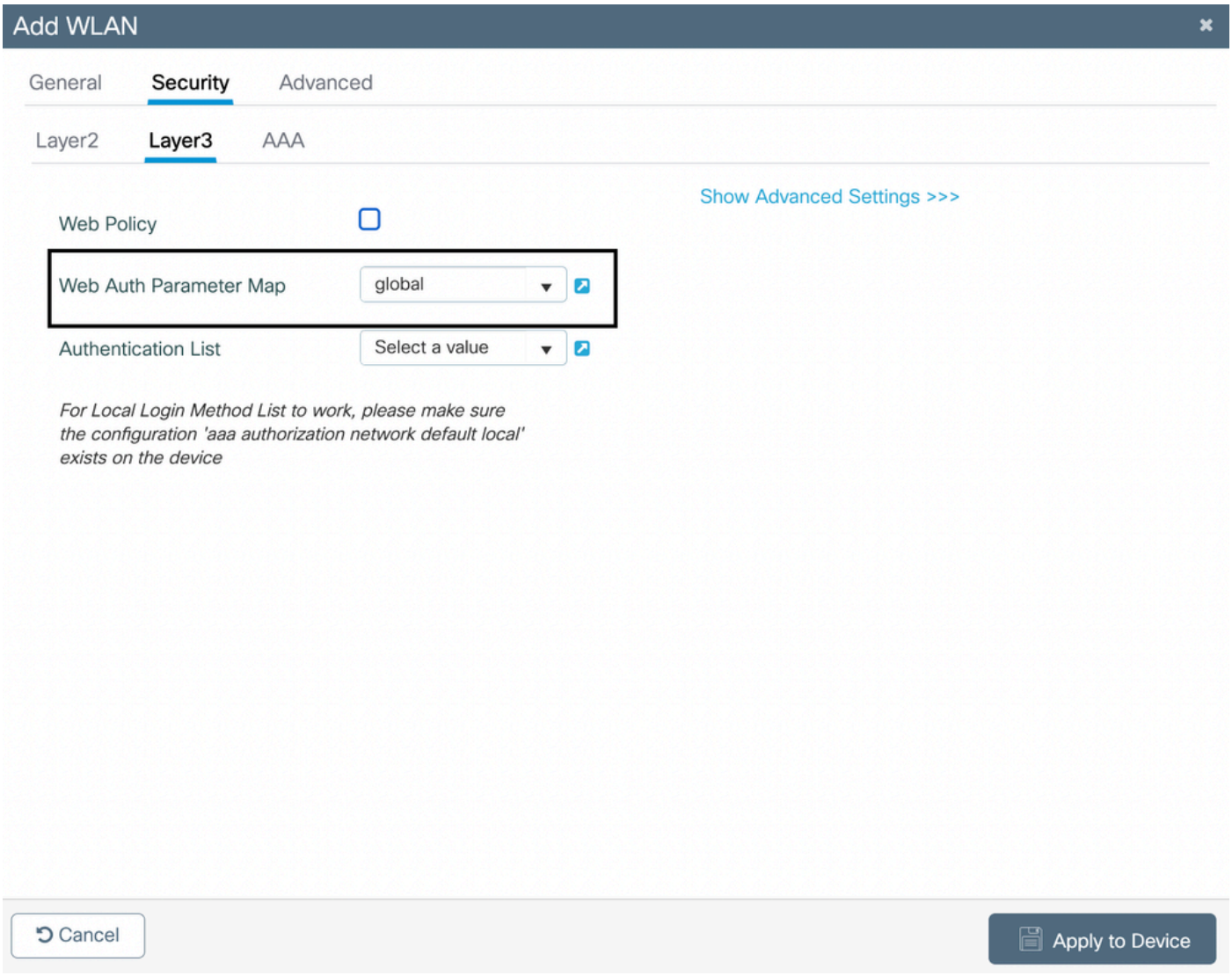
1. Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로필) > WLANs(WLAN)로 이동합니다. Add(추가) 버튼을 클릭합니다.
2. General(일반) 탭 아래에 SSID 이름을 입력하고 WLAN 버튼을 활성화합니다.



3. 같은 창에서 보안 탭을 클릭합니다. None 라디오 버튼을 선택하고 Mac Filtering을 활성화합니다.



4. Layer 3의 Security(보안)에서 웹 인증 매개변수 맵에 대한 전역 설정을 선택합니다. WLC에 구성된 다른 웹 인증 프로파일이 있는 경우 여기에 매핑할 수도 있습니다.



ISE 구성

전제 조건

- Cisco ISE가 설치되어 있고 BYOD 기능에 대한 라이센스가 있는지 확인합니다.
- RADIUS 공유 암호를 사용하여 ISE에 WLC를 네트워크 디바이스로 추가합니다.

인증서

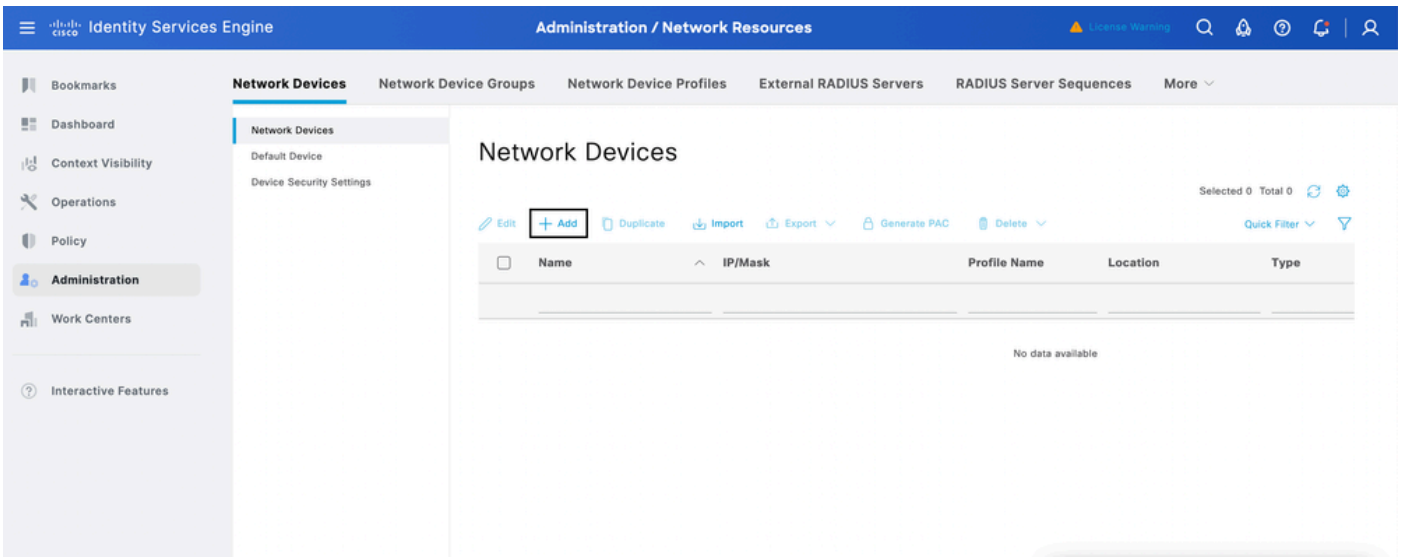
- 브라우저 보안 경고를 방지하려면 ISE에 유효한 서버 인증서를 설치하십시오.
- 인증서가 엔드포인트에서 신뢰되는지 확인합니다(잘 알려진 CA 또는 신뢰할 수 있는 루트가 있는 내부 CA에서 서명).

DNS 컨피그레이션

- DNS가 BYOD 포털에 대한 ISE 호스트 이름을 확인하는지 확인합니다.

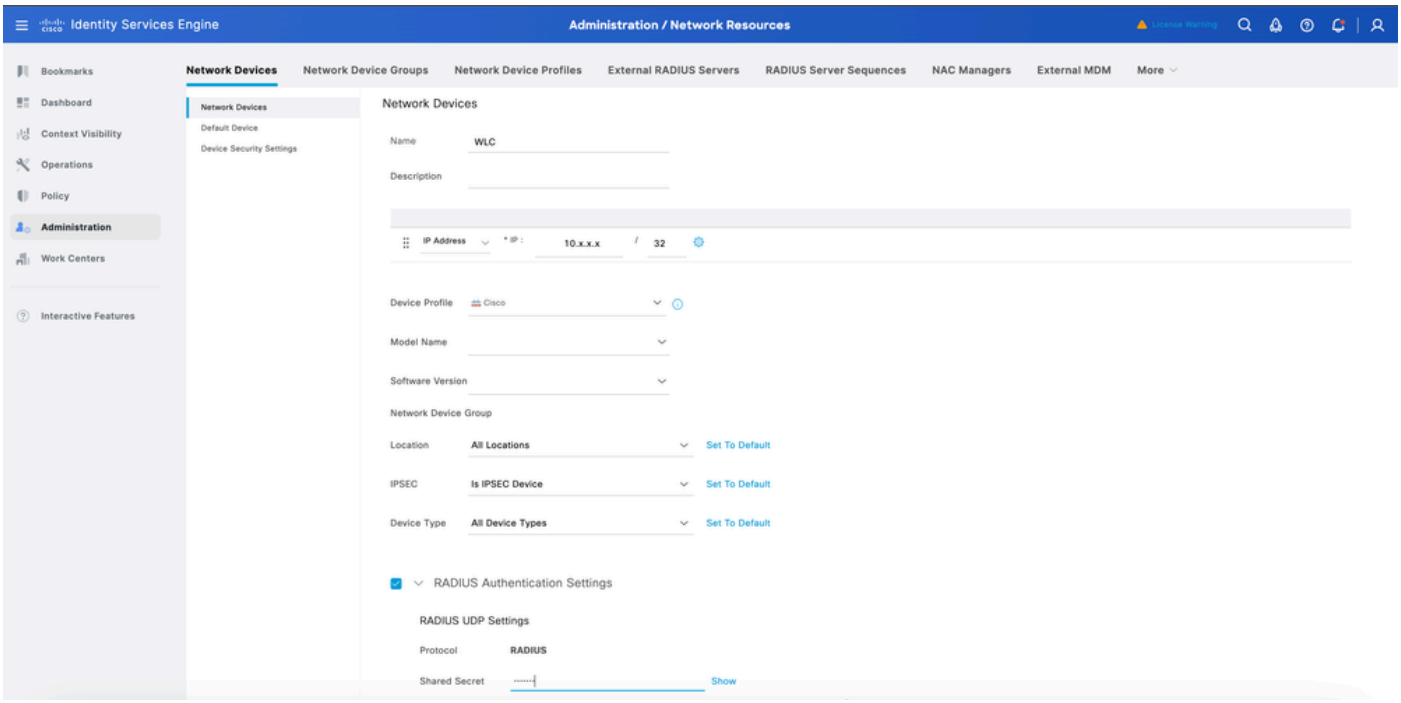
ISE 네트워크 디바이스 구성

1. ISE 웹 UI에 로그인합니다.
2. Administration(관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스)로 이동합니다.



3. WLC를 네트워크 디바이스로 추가합니다.

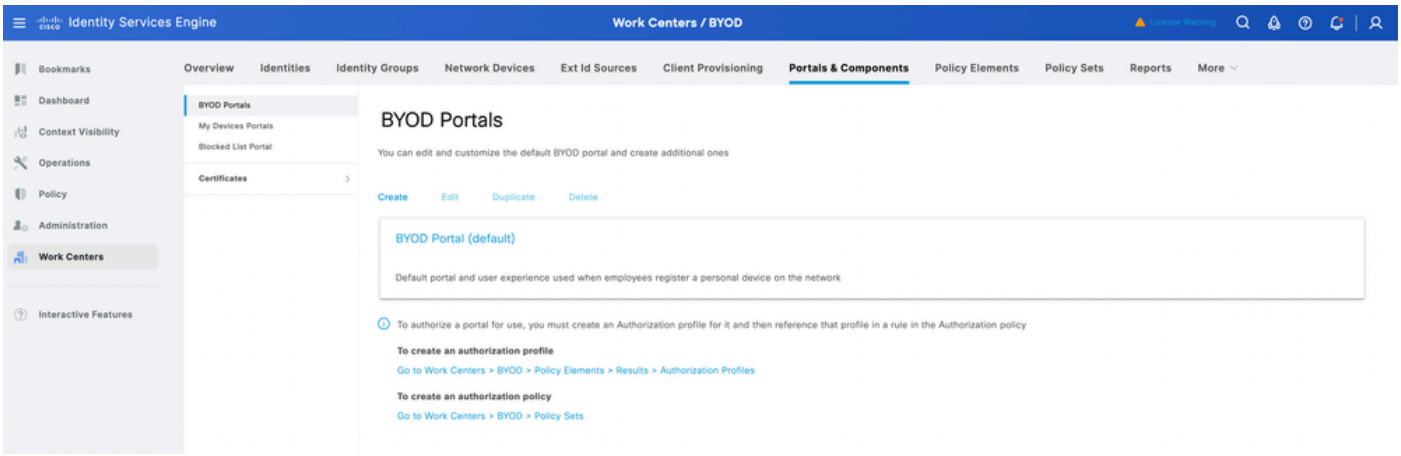
- 이름: WLC의 이름을 입력합니다.
- IP 주소: WLC 관리 IP를 입력 합니다.
- RADIUS 공유 암호: WLC에 구성된 것과 동일한 공유 암호를 입력합니다.
- Submit(제출)을 클릭합니다.



BYOD 포털 생성

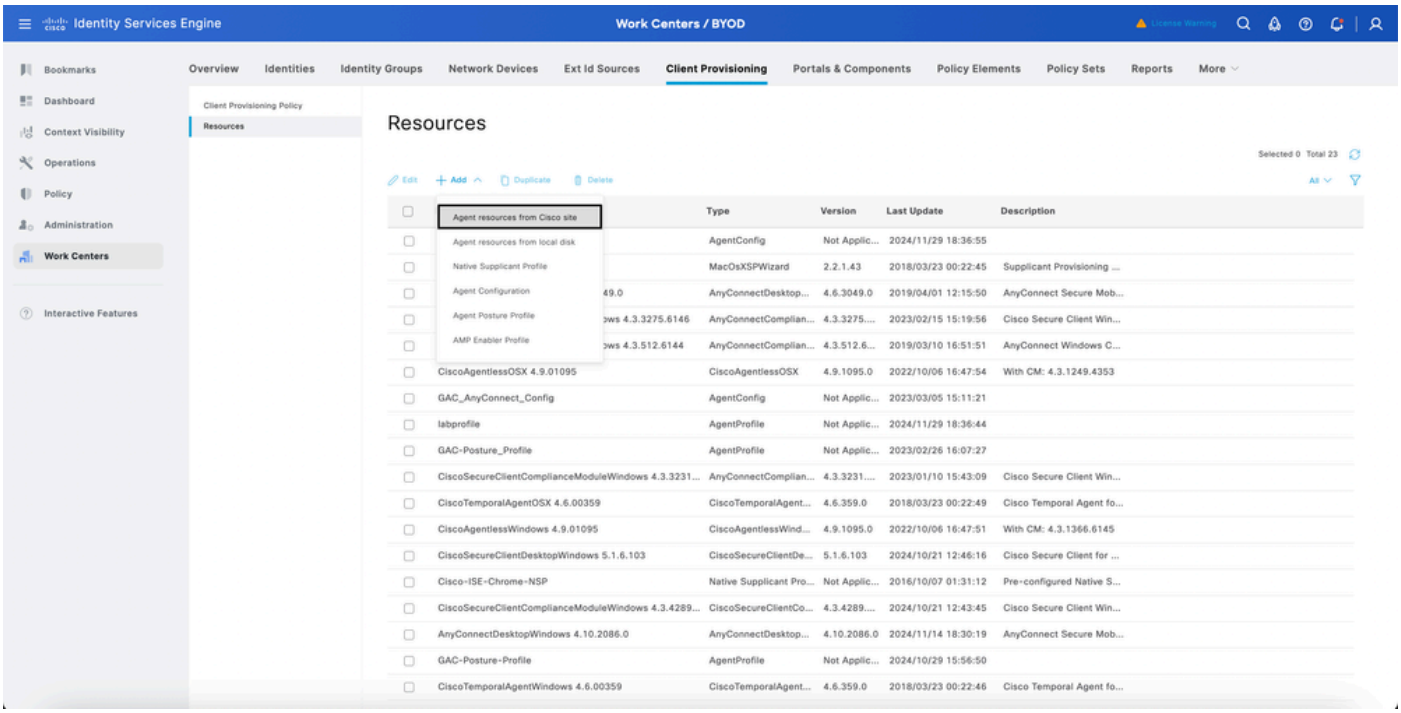
1. Work Centers(작업 센터) > BYOD > Settings(설정) > Portals & Components(포털 및 구성 요소) > BYOD Portals(BYOD 포털)로 이동합니다.

2. Add(추가)를 클릭하여 BYOD 포털을 생성하거나 ISE에서 기존 기본 포털을 사용할 수 있습니다.



Cisco IOS® 최신 버전 다운로드

1. Work Centers(작업 센터) > BYOD > Client provisioning(클라이언트 프로비저닝) > Resources(리소스)로 이동합니다.
2. 추가 버튼을 클릭하고 Cisco 사이트에서 에이전트 리소스를 선택합니다.



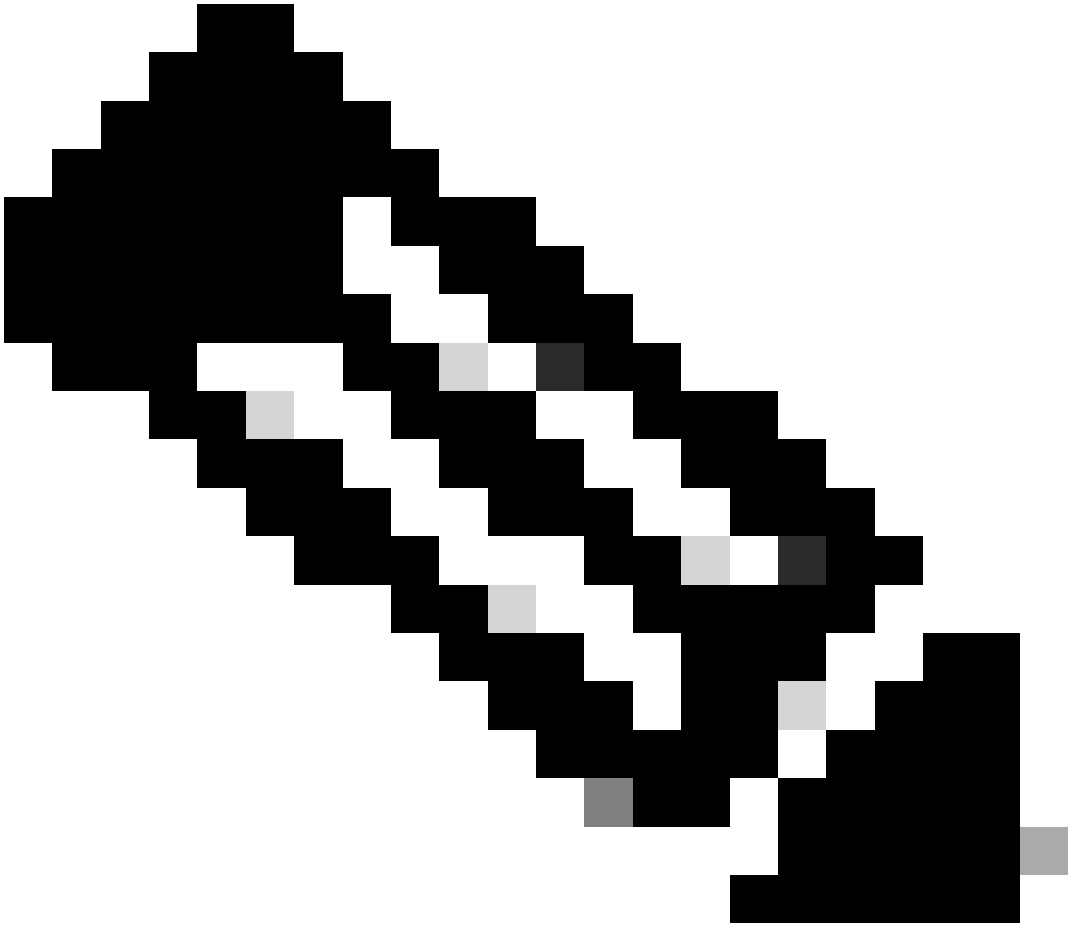
3. 소프트웨어 목록에서 다운로드할 최신 Cisco IOS 버전을 선택합니다.

Download Remote Resources

	Name	Description
☐	MacOsXSPWizard 2.7.0.1	Supplicant Provisioning Wizard for Mac OsX (ISE 2.2 and above releases)
☐	MacOsXSPWizard 3.1.0.1	Supplicant Provisioning Wizard for MAC OSX Version 3.1.0.1
☐	MacOsXSPWizard 3.1.0.2	Supplicant Provisioning Wizard for Mac OsX (ISE 2.2 and above releases)
☐	MacOsXSPWizard 3.2.0.1	Supplicant Provisioning Wizard for Mac OsX (ISE 2.2 and above releases)
☐	MacOsXSPWizard 3.4.0.0	Supplicant Provisioning Wizard for Mac OsX (ISE 2.2 and above releases)
☐	WinSPWizard 3.0.0.2	Supplicant Provisioning Wizard for Windows (ISE 2.x and Above)
☑	WinSPWizard 3.0.0.3	Supplicant Provisioning Wizard for Windows (ISE 2.x and Above)

For Agent software, please download from http://cisco.com/go/ciscosecureclient. Use the "Agent resource from local disk" add option, to import into ISE

Cancel Save

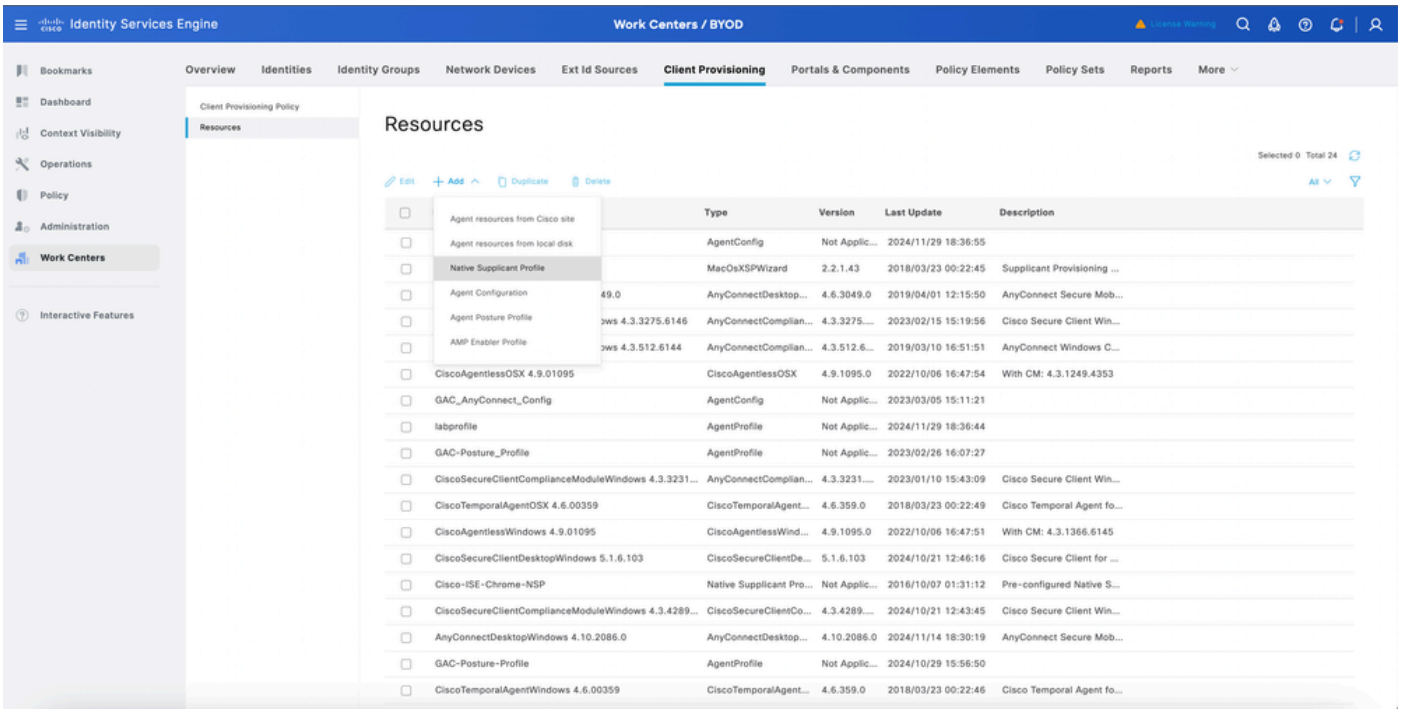


참고: Cisco IOS 소프트웨어는 Windows 및 MacOS 엔드포인트용 ISE에서 다운로드됩니다. Apple iPhone IOS의 경우 기본 신청자를 사용하여 디바이스를 프로비저닝하고 Android 디바이스의 경우 Play Store에서 다운로드해야 하는 Network Setup Assistant가 있습니다.

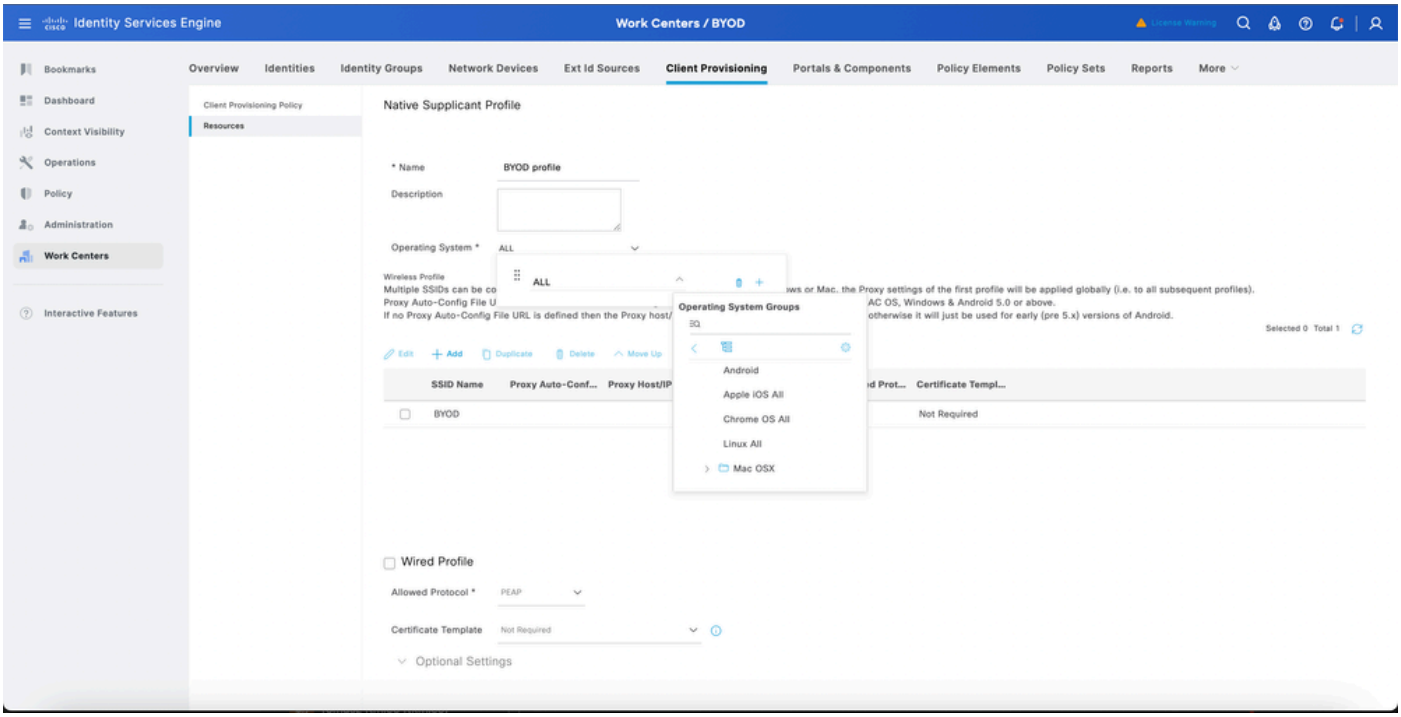
엔드포인트 프로파일 생성

1. Work Centers(작업 센터) > BYOD > Client provisioning(클라이언트 프로비저닝) > Resources(리소스)로 이동합니다.

2. 추가를 클릭하고, 드롭다운 메뉴에서 기본 신청자 프로파일을 선택합니다.



3. Operating system(운영 체제) 드롭다운 목록에서 디바이스를 온보딩하려는 필수 운영 체제를 선택하거나, 해당 환경의 모든 엔드포인트를 온보딩하기 위해 ALL(모두)로 설정할 수 있습니다.



4. 페이지에서 Add(추가)를 클릭하여 엔드포인트에 대한 802.1X를 구성하기 위한 엔드포인트 프로필을 생성합니다.

Wireless Profile(s)

SSID Name * BYOD

Proxy Auto-Config File URL

Proxy Host/IP

Proxy Port

Security * WPA2 Enterprise

Allowed Protocol * PEAP

Certificate Template Not Required

Optional Settings

Windows Settings

Authentication Mode User or Computer

- [ ] Automatically use logon name and password (and domain if any)
- [x] Enable fast reconnect
- [ ] Enable quarantine checks
- [ ] Disconnect if server does not present cryptobinding TLV
- [ ] Do not prompt user to authorize new servers or trusted certification authorities
- [x] Connect even if the network is not broadcasting its name (SSID)

iOS Settings

- [ ] Enable if target network is hidden

Android Settings

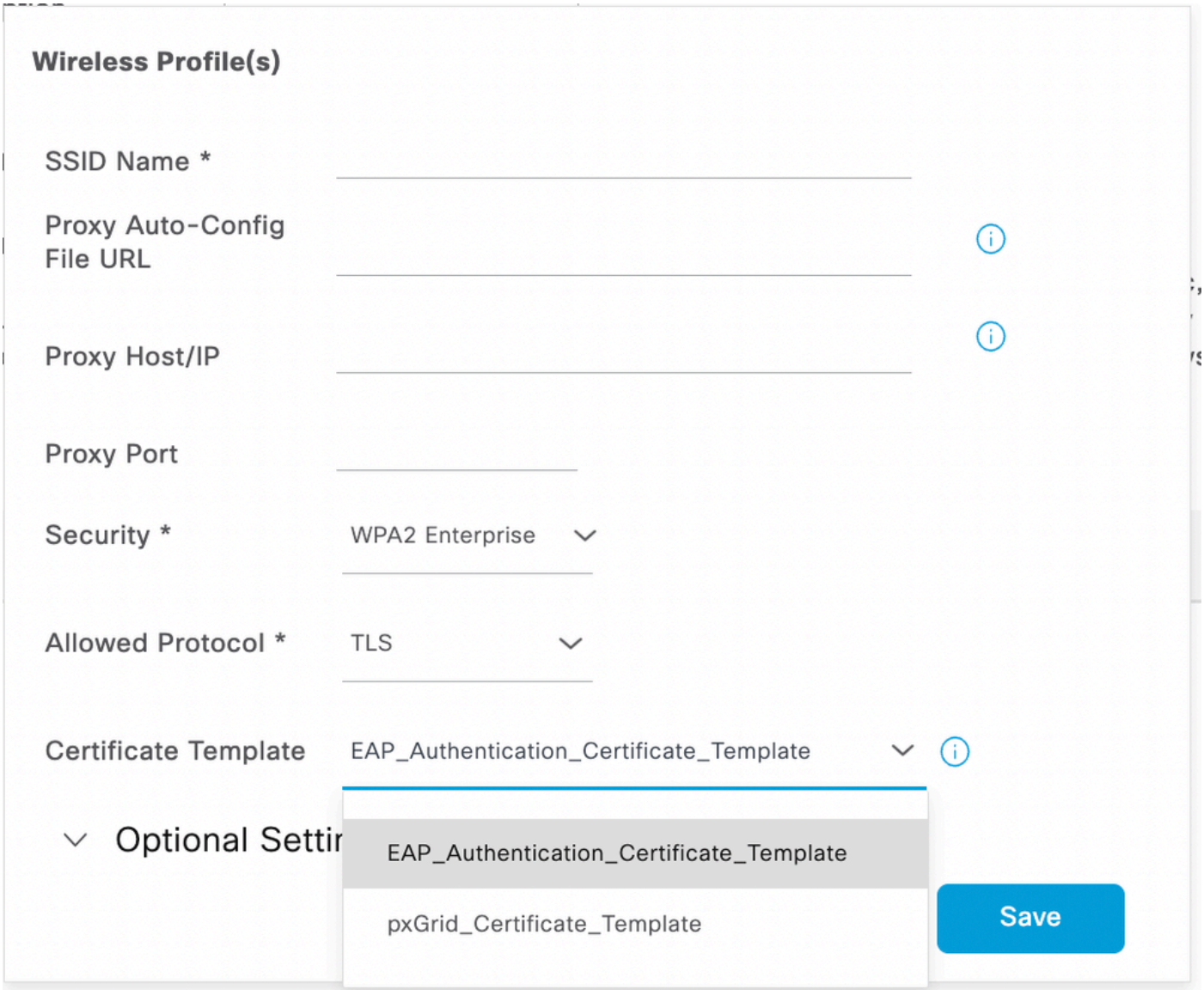
Certificate Enrollment Protocol:

요구 사항에 따라 사용자 환경의 엔드포인트에 대한 엔드포인트 프로필을 구성하십시오. 엔드포인트 프로필을 사용하여 EAP-PEAP, EAP-TLS를 구성할 수 있습니다.

5. 저장, 엔드포인트 프로파일에서 제출을 클릭합니다.

인증서 템플릿

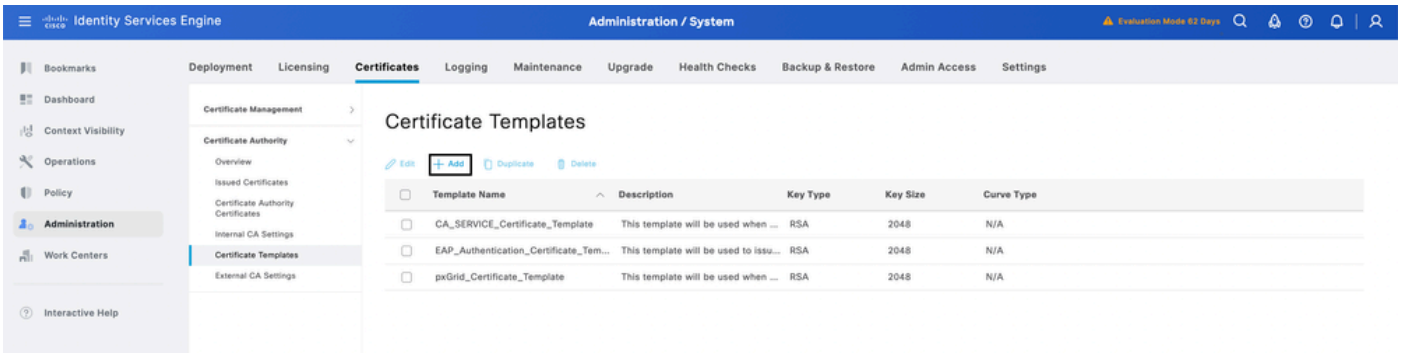
엔드포인트 프로파일은 EAP-TLS를 수행하도록 미리 구성됩니다. 인증서 템플릿을 프로파일에 추가해야 합니다. 기본적으로 ISE에는 드롭다운 메뉴에서 선택할 수 있는 미리 정의된 두 개의 템플릿이 있습니다.



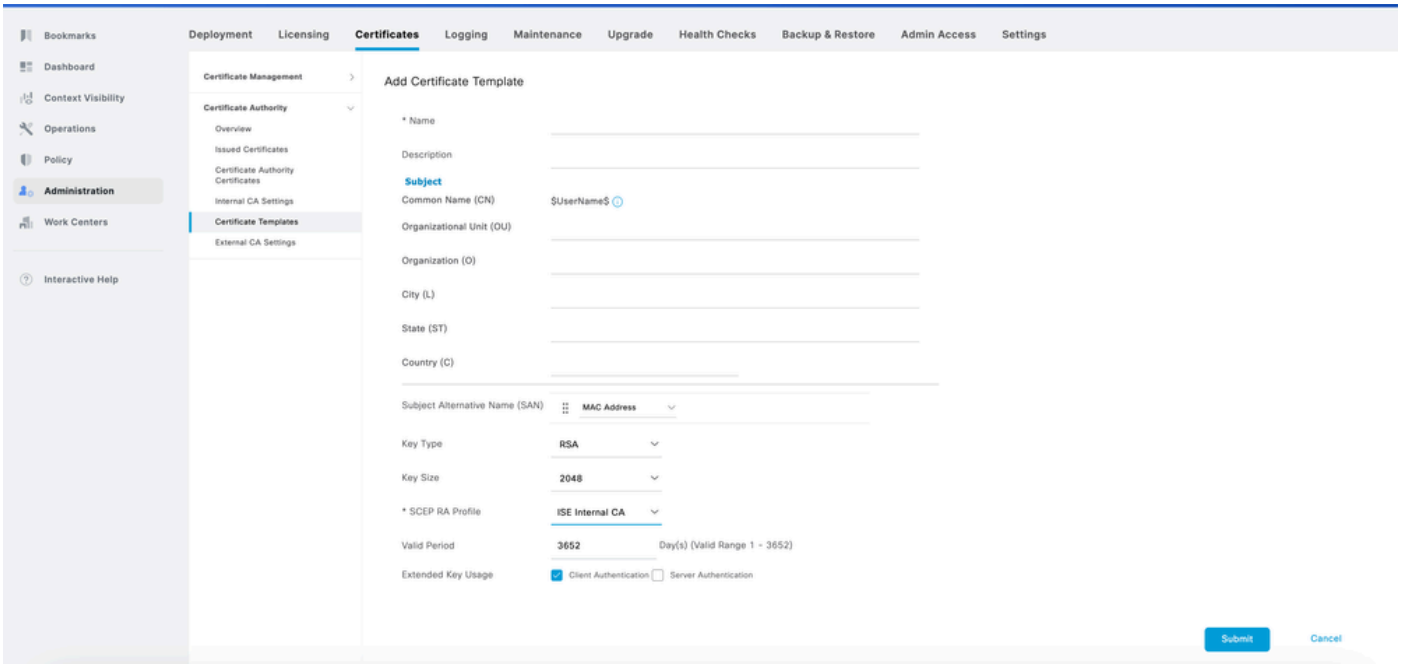
새 인증서 템플릿을 생성하려면 다음 단계를 수행합니다.

1. Administration > System > Certificates > Certificate Authority > Certificate Templates로 이동합니다.

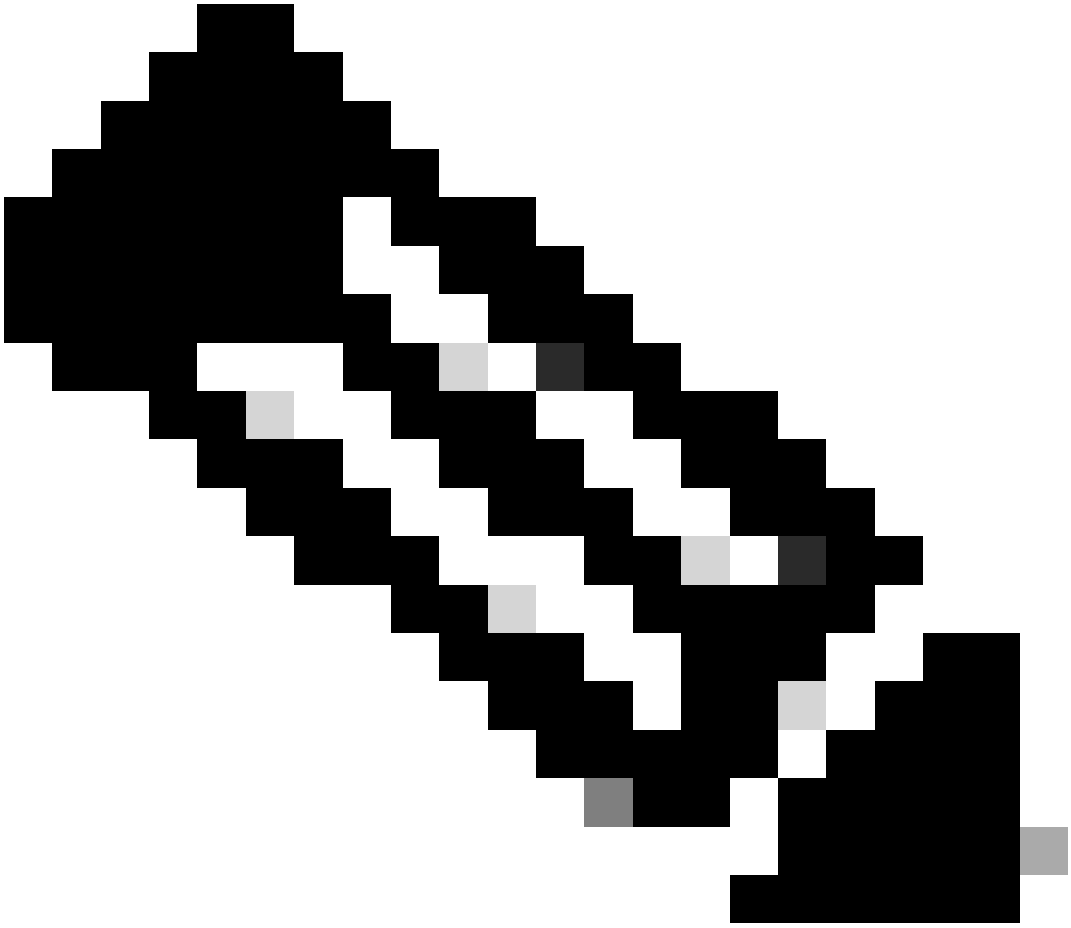
2. 페이지에서 Add(추가) 버튼을 클릭합니다.



3. 조직의 특정 요구 사항에 맞게 조정된 세부 정보를 입력합니다.



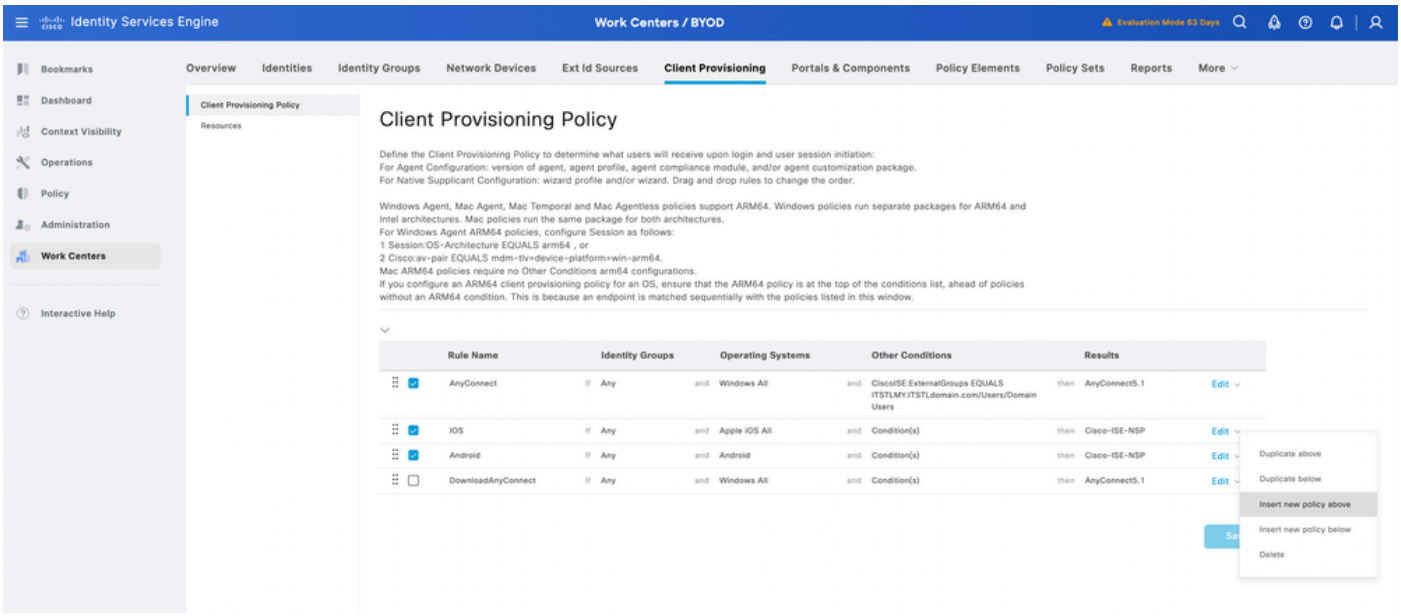
4. 변경 사항을 저장하려면 실행을 누릅니다.



참고: 인증서 템플릿은 다른 도메인이 있고 인증서의 OU에 다른 값을 추가하여 사용자를 분할하는 시나리오에서 유용할 수 있습니다.

엔드포인트 프로필을 클라이언트 프로비저닝 포털에 매핑

1. Work Centers(작업 센터) > BYOD > Client provisioning(클라이언트 프로비저닝) > Client provisioning Policy(클라이언트 프로비저닝 정책)로 이동합니다.
2. 규칙의 v on을 클릭하여 새 클라이언트 프로비저닝 규칙을 생성합니다.

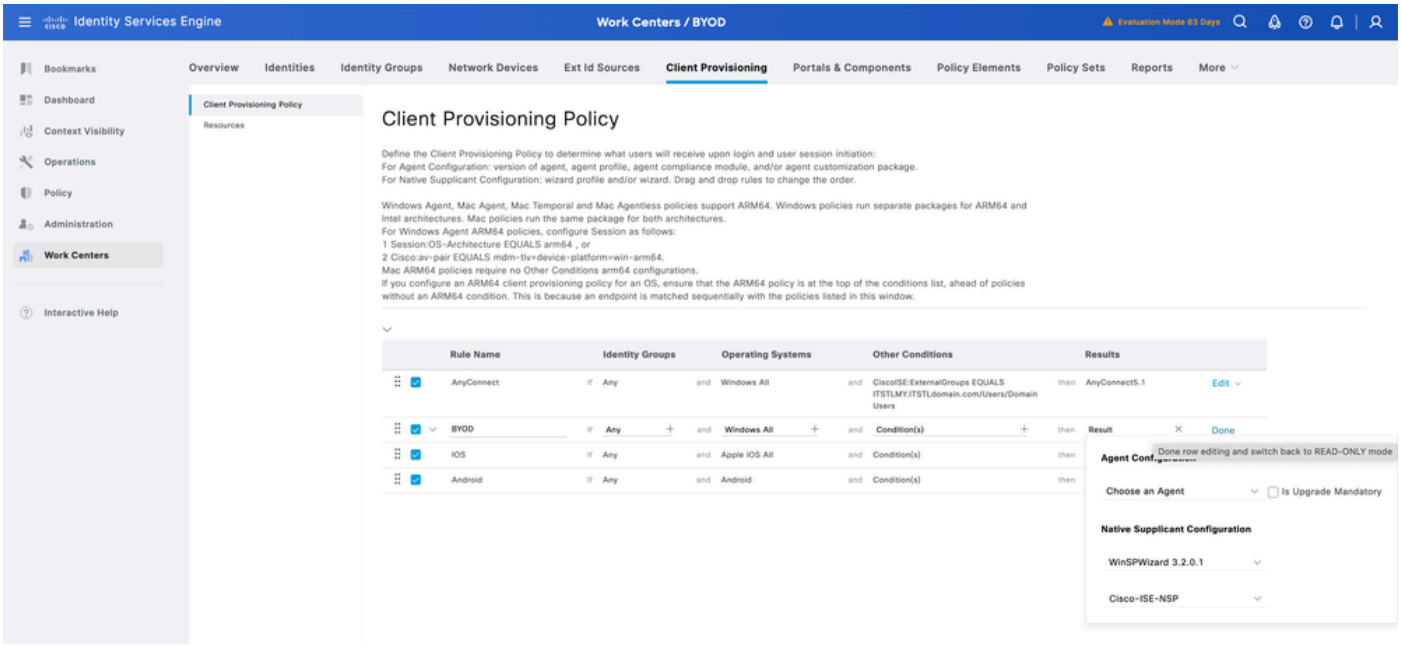


3. 페이지에 새 규칙 생성 게시

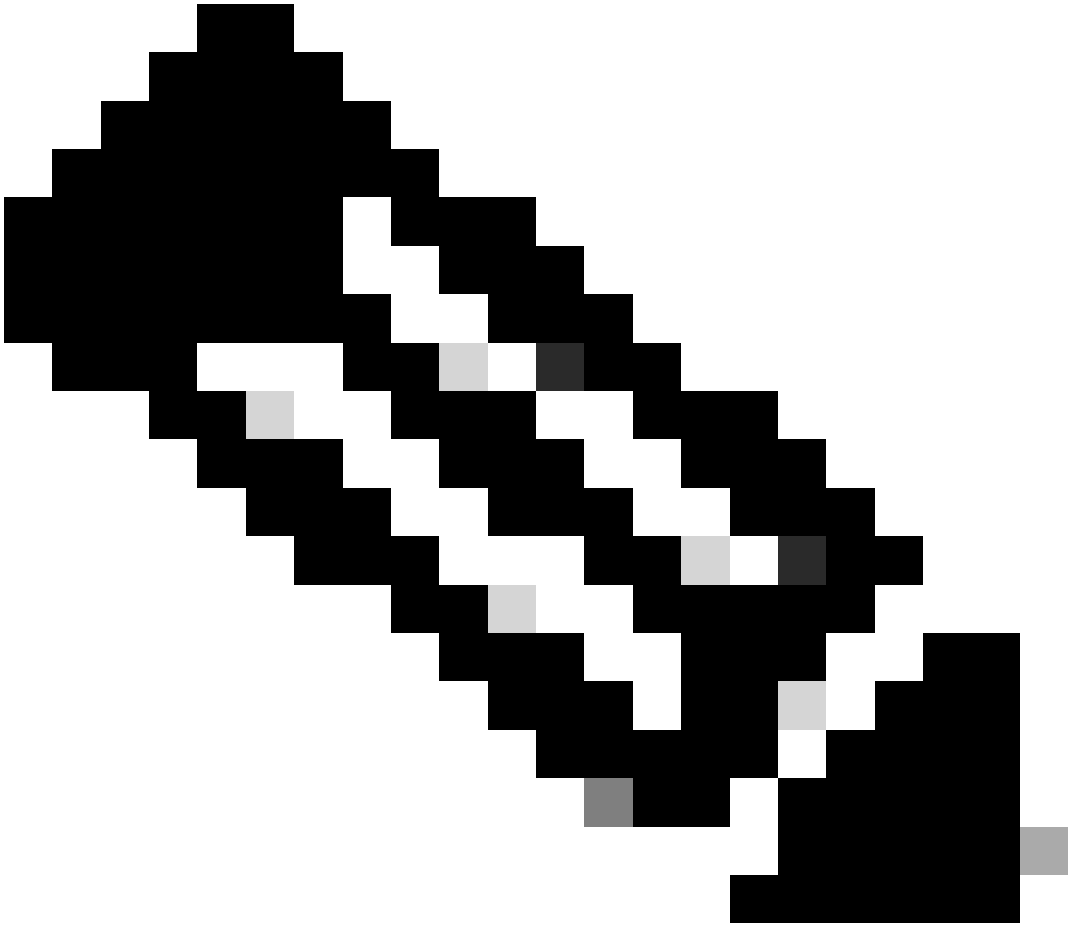
4. 특정 사용자가 BYOD 포털을 사용하도록 제한하려면 ID 그룹을 추가합니다

5. BYOD 포털에 액세스하려는 운영 체제를 추가합니다

6. 드롭다운에서 Cisco IOS 버전을 매핑하고 결과에서 생성한 엔드포인트 프로파일도 선택합니다



7. 완료를 누른 다음 저장 버튼을 누릅니다.

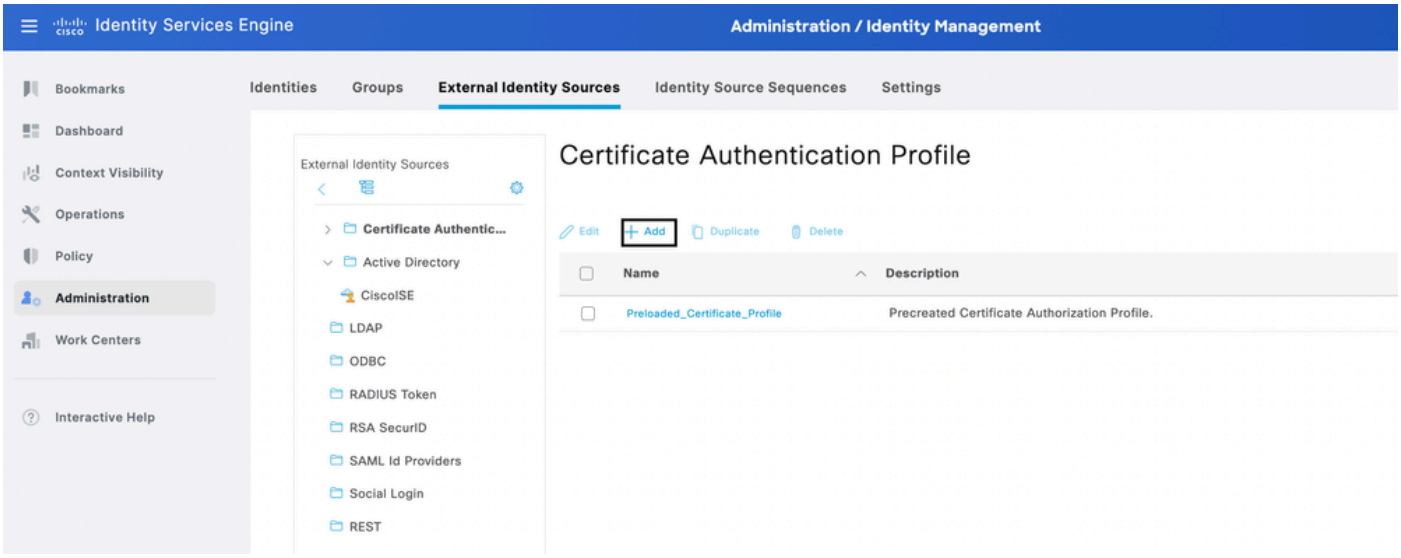


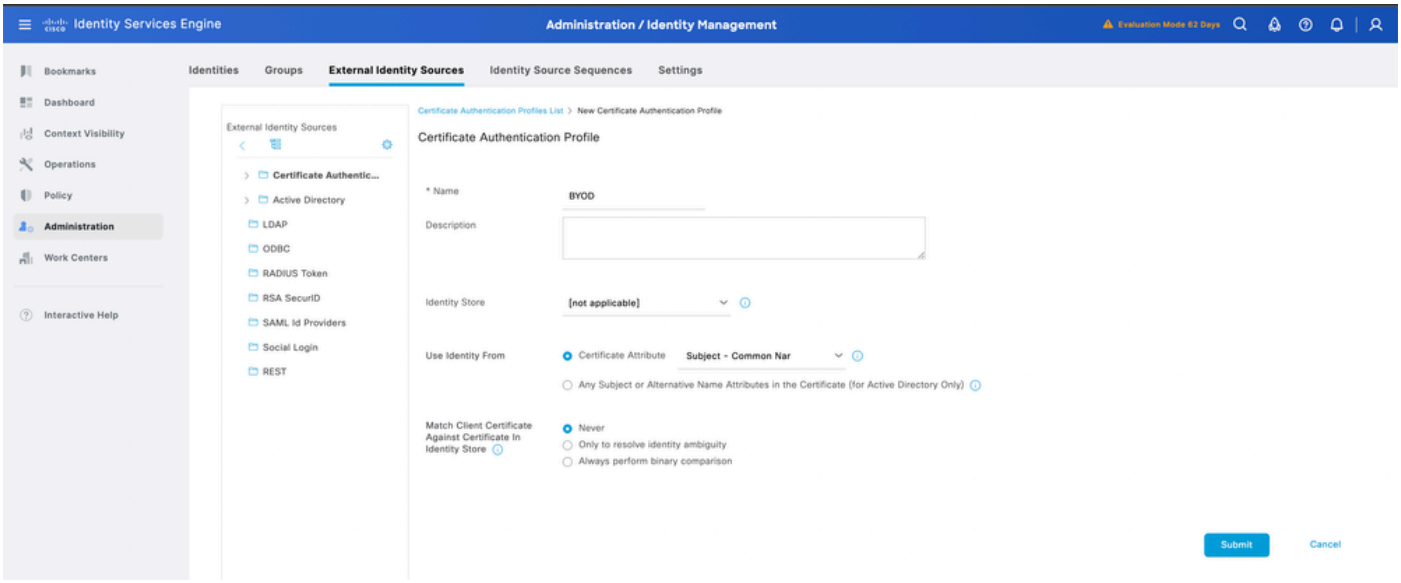
참고: 이 정책은 포스처 클라이언트 프로비저닝 및 BYOD 프로비저닝에 모두 영향을 줍니다. 에이전트 구성 섹션에서는 포스처 확인을 위해 시행되는 포스처 에이전트 및 규정준수 모듈을 확인하고, 기본 신청자 구성 섹션에서는 BYOD 프로비저닝 흐름에 대한 설정을 관리합니다

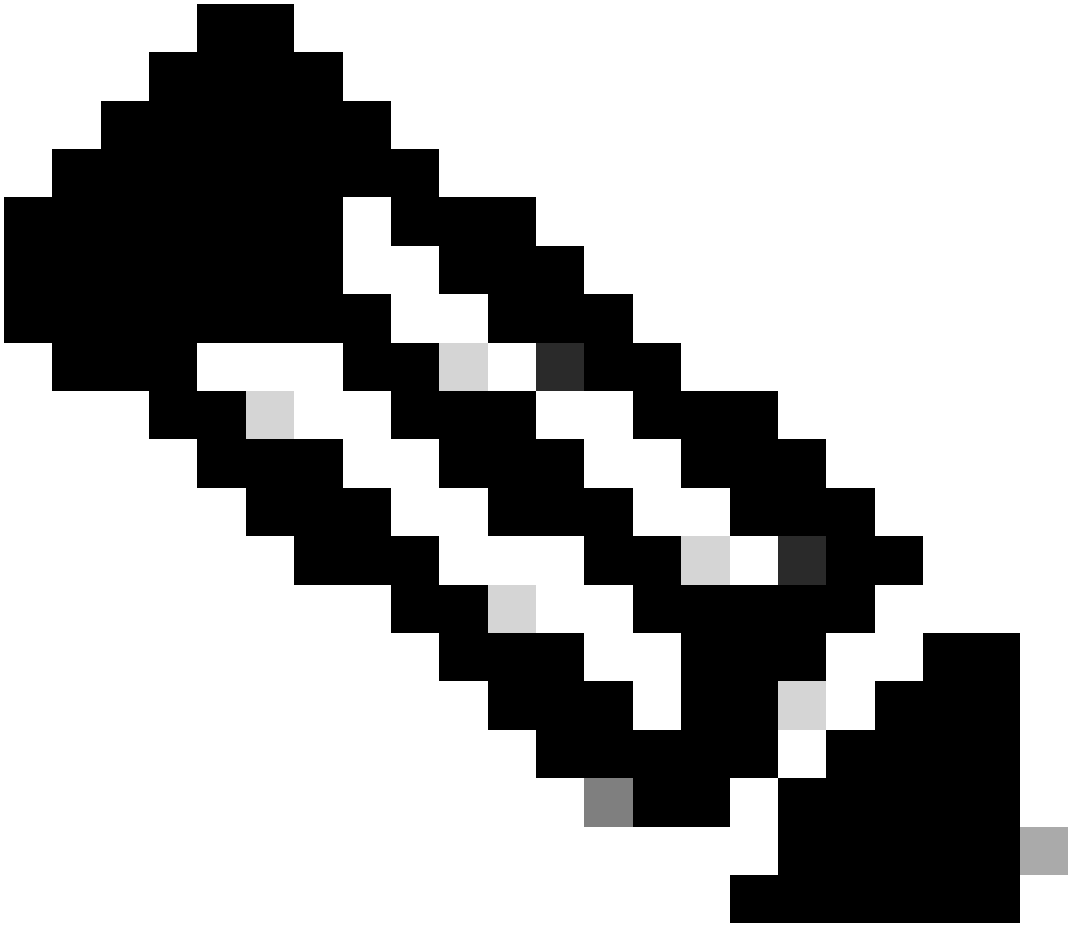
단일 SSID BYOD에 대한 ISE 정책 집합 구성

1. Policy(정책) > Policy Set(정책 설정)로 이동하여 ISE의 BYOD 플로우에 대한 정책을 생성합니다.

2. 그런 다음 Administration(관리) > Identity Management(ID 관리) > External Identity Sources(외부 ID 소스) > Certificate Authentication Profile(인증서 인증 프로파일)로 이동합니다. 추가 버튼을 클릭하여 인증서 프로필을 생성합니다.

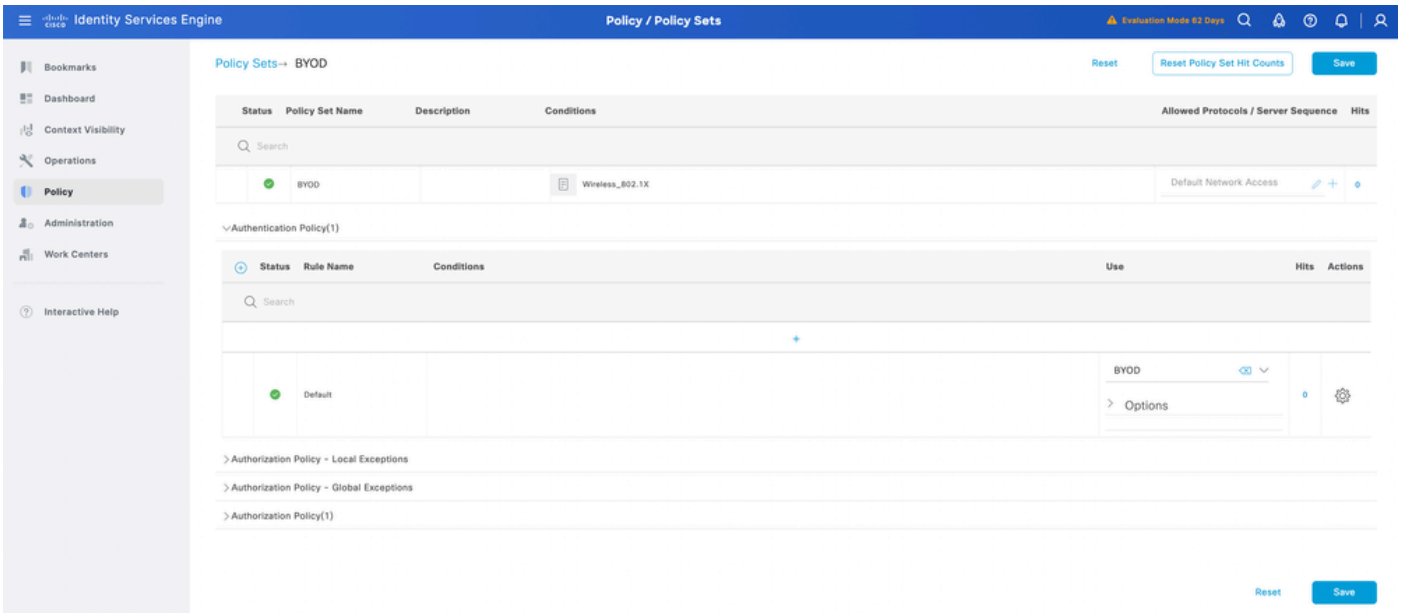






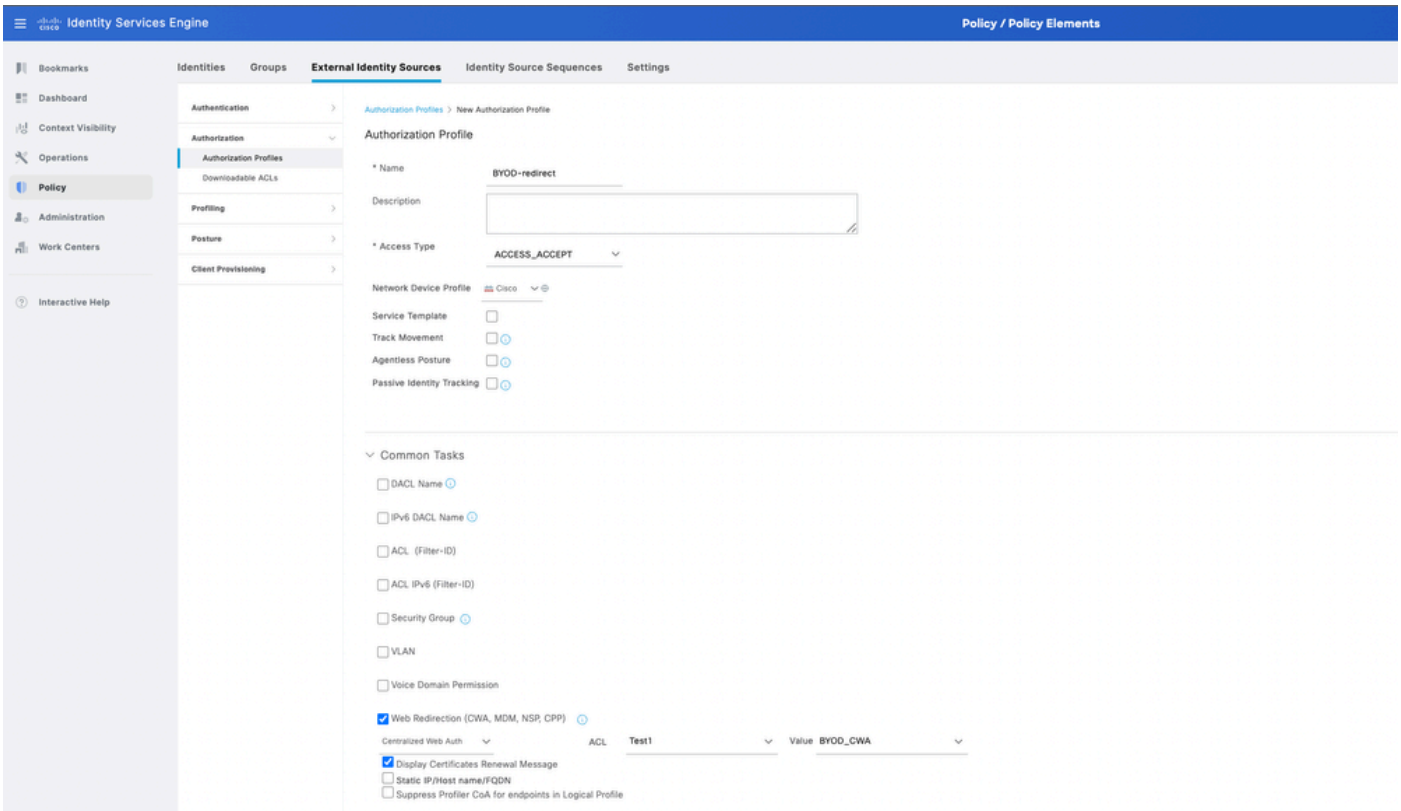
참고: ID 저장소에서 추가 보안을 위해 인증서에서 사용자 조회를 수행하기 위해 ISE에 통합된 Active Directory를 항상 선택할 수 있습니다.

3. 제출을 클릭하여 구성을 저장합니다. 그런 다음 인증서 프로필을 BYOD에 대한 정책 집합에 매핑합니다.

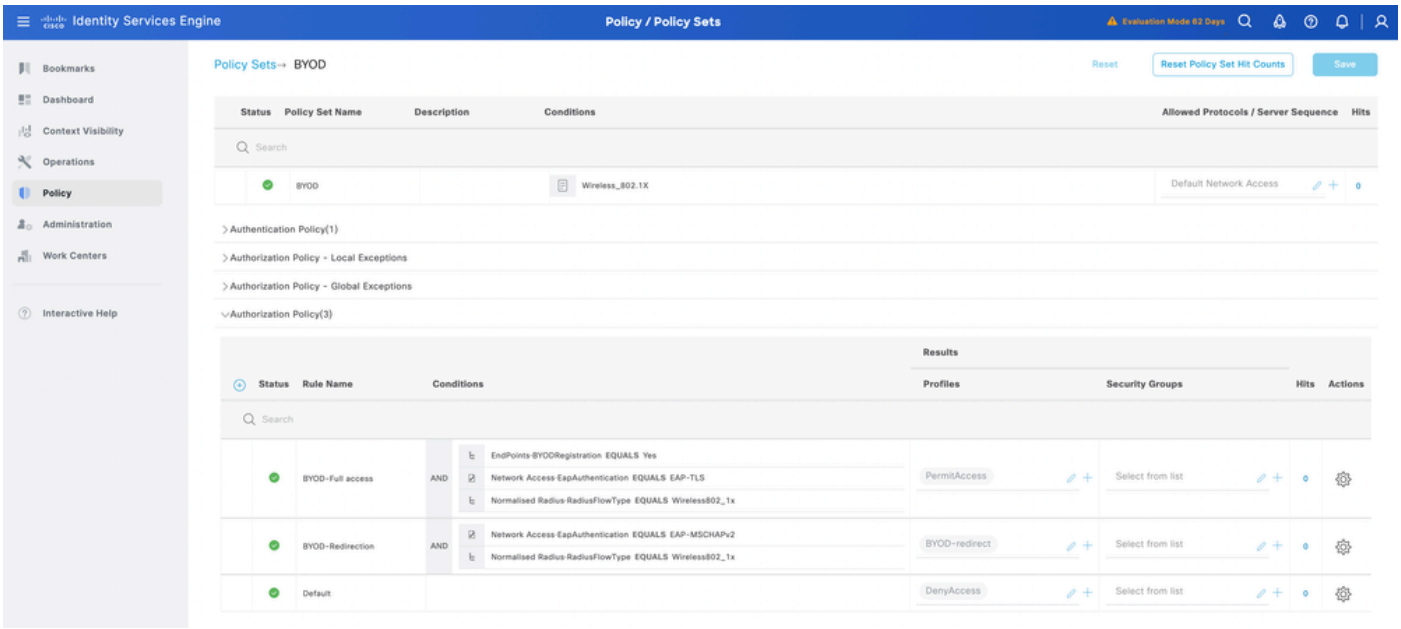


4. BYOD 리디렉션 및 BYOD 플로우 후 전체 액세스를 위한 권한 부여 프로파일을 구성합니다. Policy(정책) > Policy Elements(정책 요소) > Results(결과) > Authorization(권한 부여) > Authorization Profiles(권한 부여 프로파일)로 이동합니다.

5. Add(추가)를 클릭하고 권한 부여 프로파일을 생성합니다. 웹 리디렉션(CWA,MDM,NSP,CPP)을 확인하고 BYOD 포털 페이지를 매핑합니다. 또한 WLC의 리디렉션 ACL 이름을 프로필에 추가합니다. Full access(전체 액세스) 프로파일의 경우, 프로파일의 각 기업 VLAN으로 permit access(액세스 허용)를 구성합니다.



6. 권한 부여 프로파일을 권한 부여 규칙에 매핑합니다. 사용자가 BYOD 플로우를 게시한 네트워크에 대한 전체 액세스 권한을 얻으려면 BYOD 전체 액세스 권한에 EndPoints·BYODRegistration이 yes가 되어야 합니다.

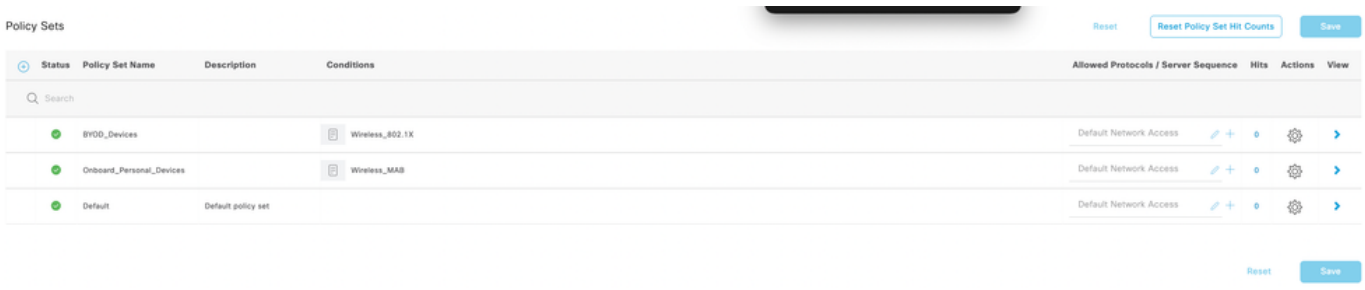


이중 SSID BYOD에 대한 ISE 정책 집합 구성

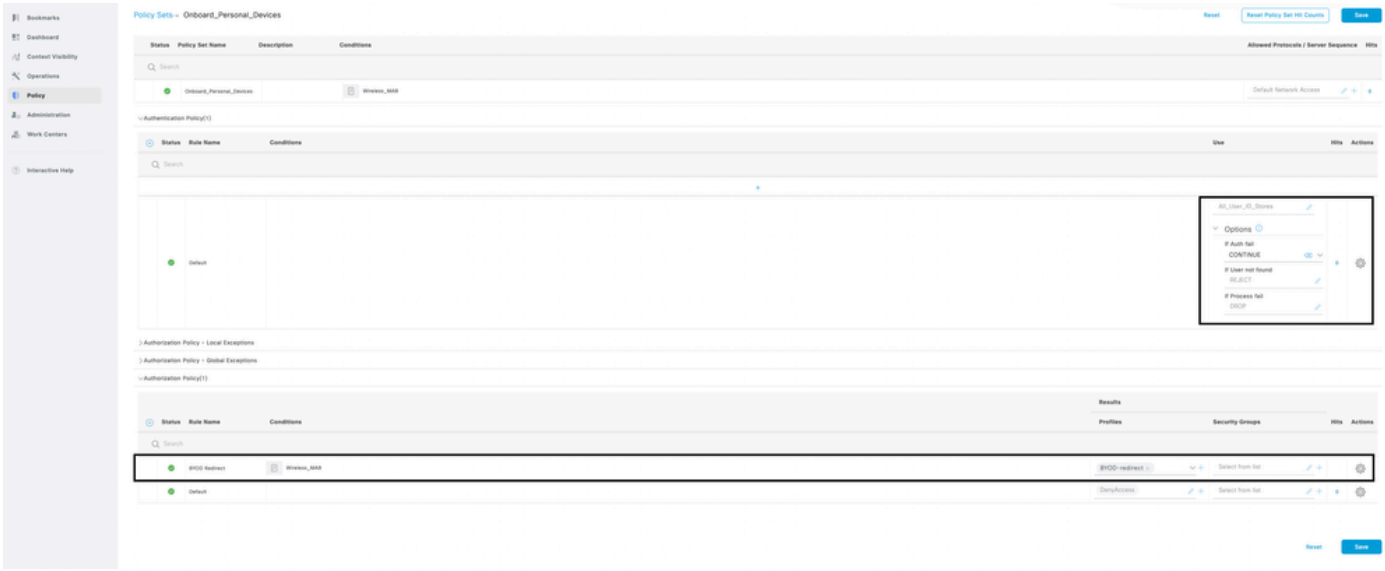
이중 SSID BYOD 컨피그레이션에서는 2개의 정책 집합이 ISE에 구성됩니다. 첫 번째 정책 세트는 개방/비보안 SSID에 대한 것입니다. 여기서 정책 세트 컨피그레이션은 개방/비보안 SSID에 연결할 때 사용자를 BYOD 페이지로 리디렉션합니다

1. Policy(정책) > Policy Set(정책 설정)로 이동하고 ISE에서 BYOD 플로우에 대한 정책을 생성합니다.

2. ISE에서 등록된 BYOD 사용자를 인증하는 Open/Unsecured SSID 및 Corporate SSID에 대한 정책 집합을 생성합니다.

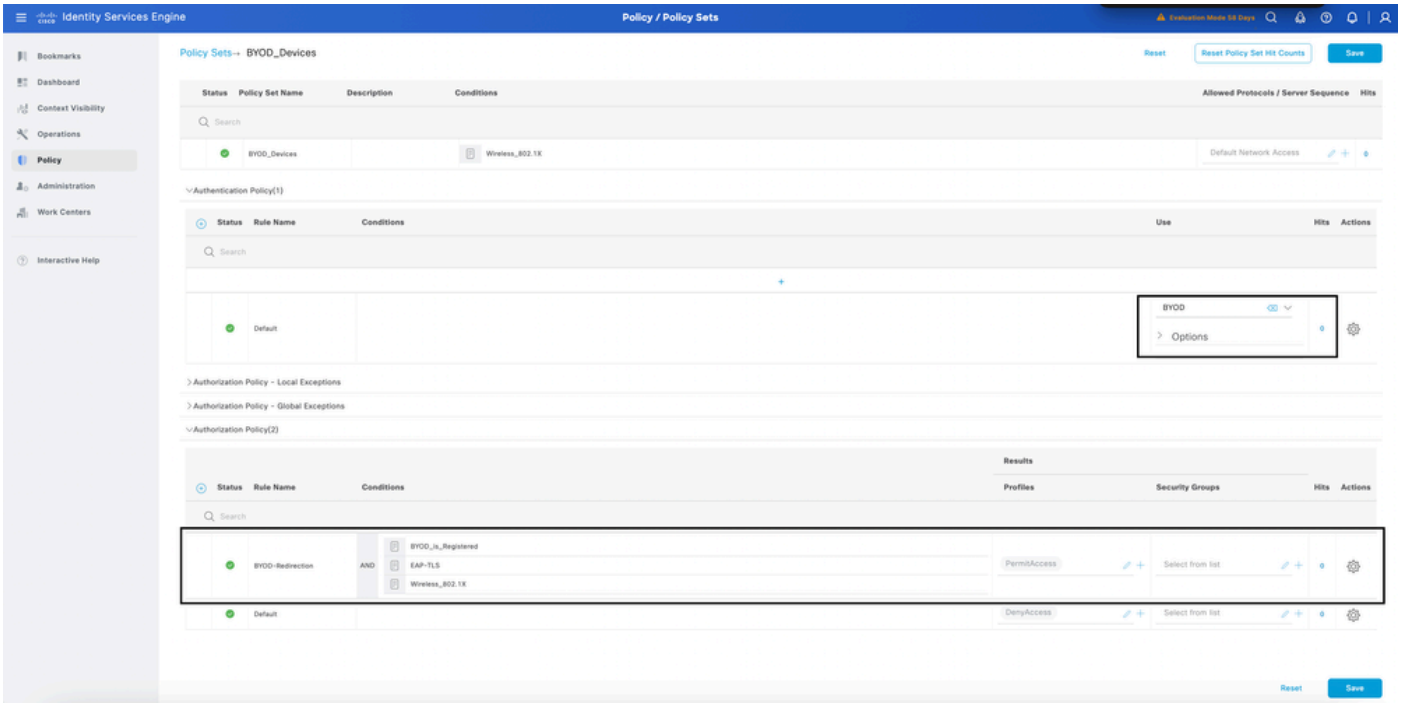


3. 온보딩 정책 세트의 옵션에서 계속 선택을 찾습니다. 권한 부여 정책의 경우 조건을 생성하고 리디렉션 권한 부여 프로파일을 매핑합니다. 동일한 단계는 포인트 4에서 찾을 수 있는 권한 부여 프로파일을 생성하는 데 사용됩니다.



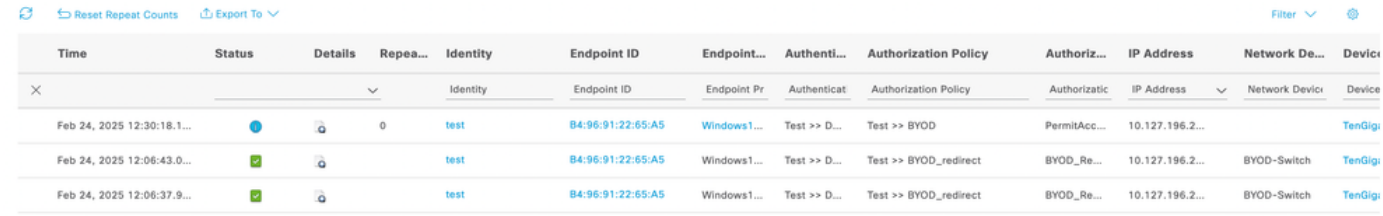
4. BYOD Registered Policy Set(BYOD 등록 정책 집합)에서 찾은 것과 동일한 인증서 프로필로 인증 정책을 구성합니다.

포인트 2의 단일 SSID BYOD에 대한 ISE 정책 집합 구성에서 권한 부여 정책에 대한 조건을 생성하고 정책에 전체 액세스 프로필을 매핑합니다.

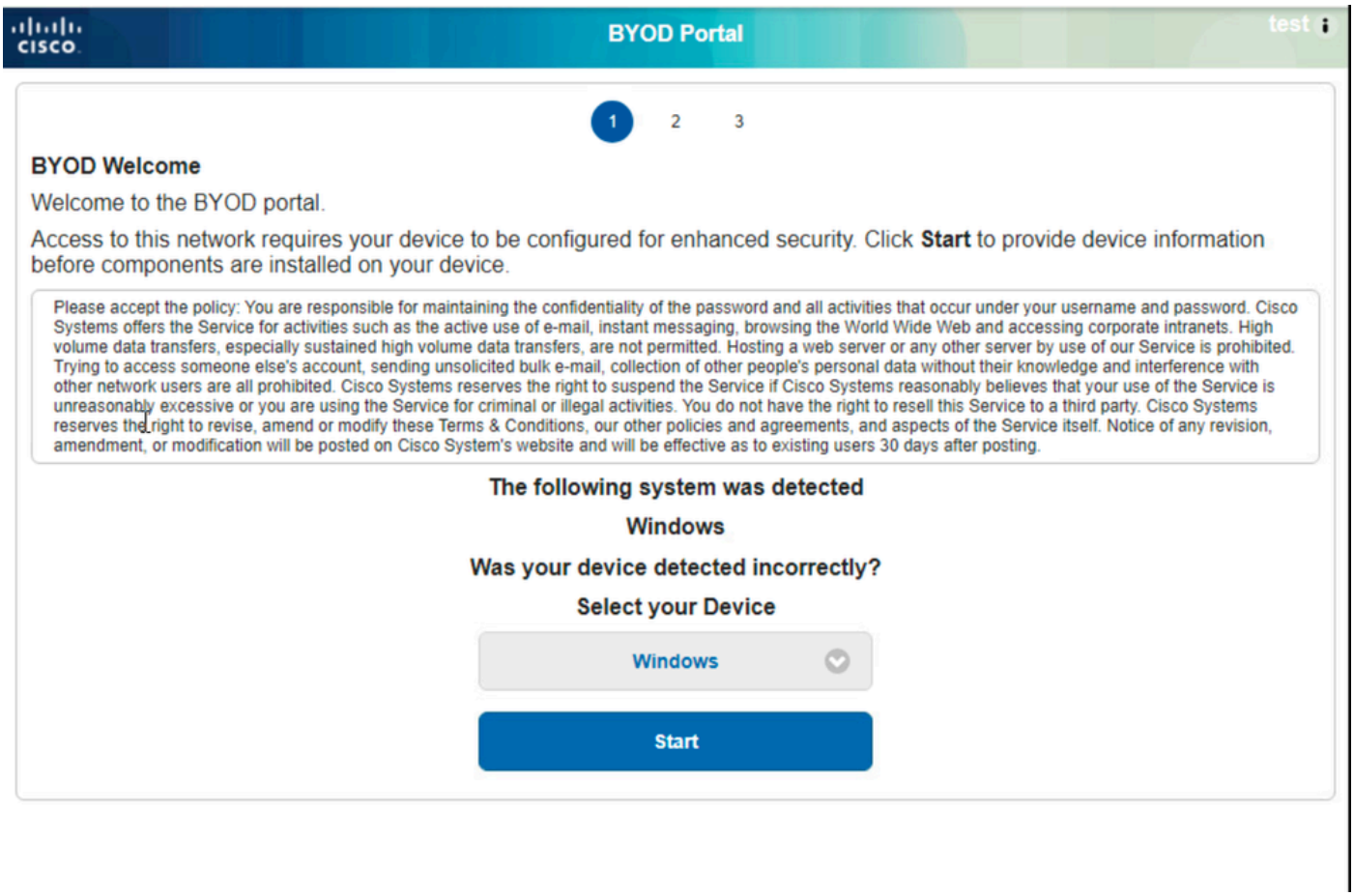


로깅

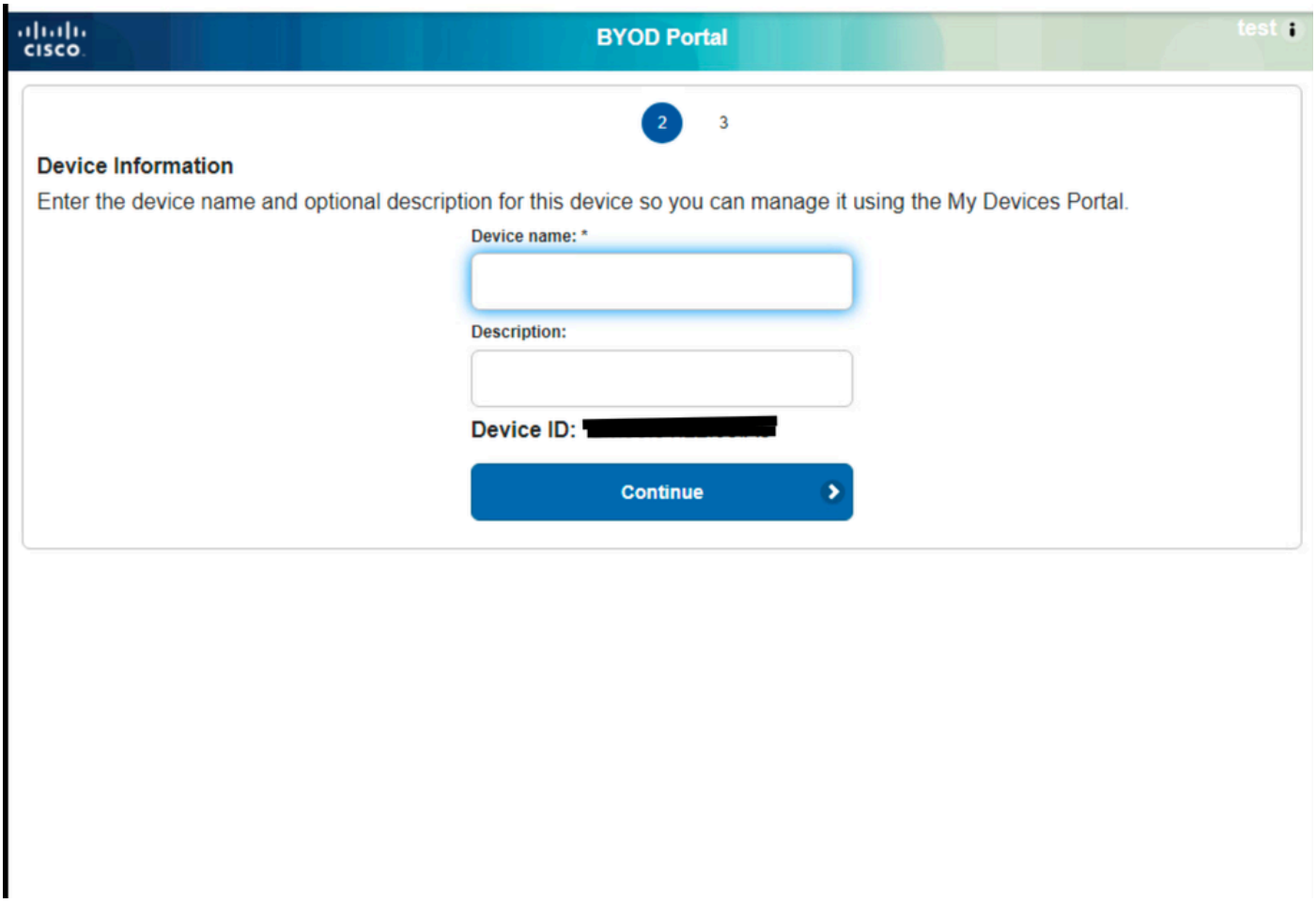
ISE의 라이브 로그에서 사용자 인증이 성공하고 BYOD 포털 페이지로 리디렉션됩니다. BYOD 흐름을 완료한 후 사용자는 네트워크에 대한 액세스 권한을 부여 받게 됩니다



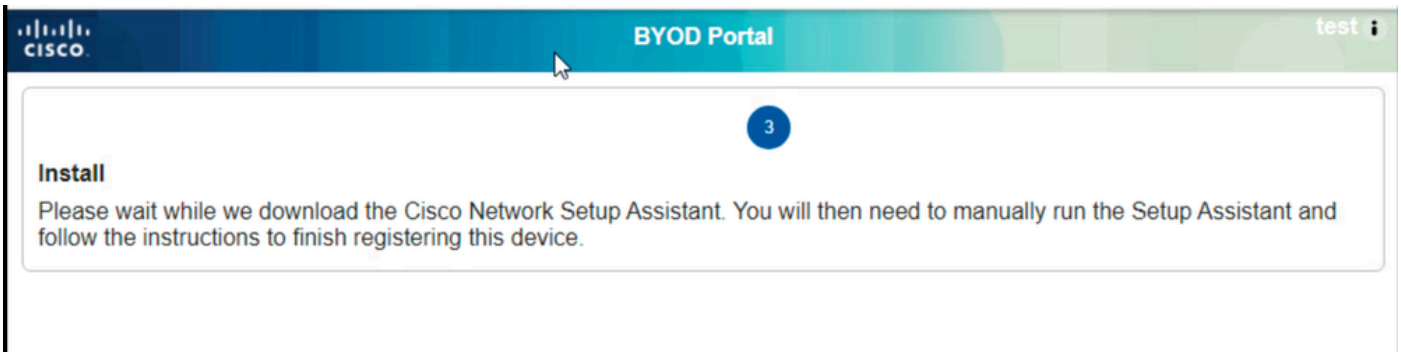
사용자의 관점에서 보면, 먼저 BYOD 페이지로 리디렉션되고 웹 페이지에서 적절한 장치를 선택해야 합니다. Windows 10 장치를 테스트하는 데 사용됨



Next(다음) 버튼을 클릭하면 디바이스 이름과 설명을 입력하라는 메시지가 표시되는 페이지로 이동합니다

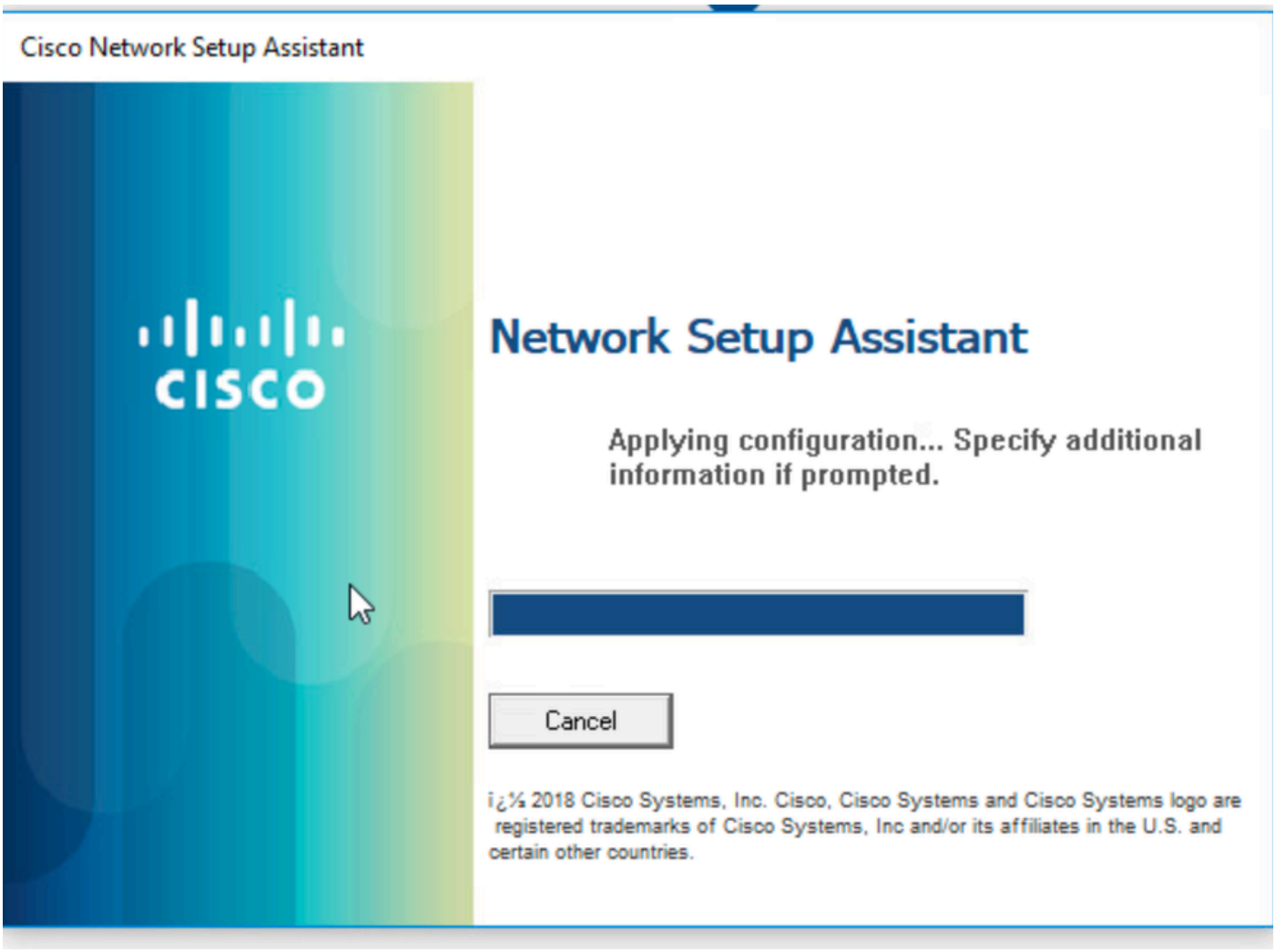


EAP-TLS 인증을 수행하도록 프로파일을 구성한 경우 엔드포인트 프로파일 및 인증을 위한 EAP TLS 인증서를 다운로드하기 위해 Network Assistant 툴을 다운로드하도록 사용자에게 요청할 수 있음을 게시합니다



관리자 권한으로 Network Assistant Application을 실행하고 시작 단추를 눌러 온보딩 플로우를 시작합니다.


Cisco Network Setup Assistant
Network Setup Assistant
This application automatically configures network settings.
Start
Quit
i¿¼ 2018 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc and/or its affiliates in the U.S. and certain other countries.



사용자가 리소스에 액세스하기 위해 개인 디바이스를 사용하여 네트워크에 성공적으로 온보딩되었습니다.

문제 해결

BYOD 문제를 해결하려면 ISE에서 이 디버그를 활성화하십시오

디버그 수준으로 설정할 특성:

- 클라이언트(guest.log)
- client-webapp(guest.log)
- scep(ise-psc.log)
- ca-service(ise-psc.log)
- admin-ca(ise-psc.log)
- 런타임 AAA(prrt-server.log)
- nsf(ise-psc.log)
- nsf-session(ise-psc.log)
- 프로파일러(profiler.log)

로그 스니펫

게스트 로그

이 로그는 사용자가 페이지로 성공적으로 리디렉션했고 Network Assistant 애플리케이션을 다운로드했음을 나타냅니다.

2025-02-24 12:06:08,053 INFO [https-jsse-nio-10.127.196.172-8443-exec-4][] portalwebaction.utils.portal.spring.ISPportalControllerUtils -:000000000000000B30D59CC5:::- action-forwards, forwarding에서 찾은 매핑 경로: pages/byodWelcome.jsp // BYOD 시작 페이지
2025-02-24 12:06:09,968 정보 [https-jsse-nio-10.127.196.172-8443-exec-8][] cpm.guestaccess.flowmanager.step.Executor -:000000000000000B30D59CC5::test:- pTranSteps:1
2025-02-24 12:06:09,968 정보 [https-jsse-nio-10.127.196.172-8443-exec-8][] cpm.guestaccess.flowmanager.step.StepExecutor -:000000000000000B30D59CC5::test:- getNextFlowStep, pTranSteps:[id: d2513b7b-7249-4bc3-a423-0e7d9a0b2500]
2025-02-24 12:06:09,968 정보 [https-jsse-nio-10.127.196.172-8443-exec-8][] cpm.guestaccess.flowmanager.step.StepExecutor -:000000000000000B30D59CC5::test:- getNextFlowStep, stepTran:d2513b7b-7249-4bc3-a423-0e7d9a0b2500
2025-02-24 12:06:09,979 정보 [https-jsse-nio-10.127.196.172-8443-exec-8][] portalwebaction.utils.portal.spring.ISPortalControllerUtils -:000000000000000B30D59CC5::::- 작업 전달에서 찾은 매핑 경로, 다음으로 전달: pages/byodRegistration.jsp을 참조하십시오.
2025-02-24 12:06:14,643 정보 [https-jsse-nio-10.127.196.172-8443-exec-2][] cpm.guestaccess.flowmanager.step.Executor -:000000000000000B30D59CC5::test:- pTranSteps:1
2025-02-24 12:06:14,643 정보 [https-jsse-nio-10.127.196.172-8443-exec-2][] cpm.guestaccess.flowmanager.step.StepExecutor -:000000000000000B30D59CC5::test:- getNextFlowStep, pTranSteps:[id: f203b757-9e8a-473e-abdc-879d0cd37491]
2025-02-24 12:06:14,643 정보 [https-jsse-nio-10.127.196.172-8443-exec-2][] cpm.guestaccess.flowmanager.step.StepExecutor -:000000000000000B30D59CC5::test:- getNextFlowStep, stepTran:f203b757-9e8a-473e-abdc-879d0cd37491
2025-02-24 12:06:14,647 정보 [https-jsse-nio-10.127.196.172-8443-exec-2][] portalwebaction.utils.portal.spring.ISPortalControllerUtils -:000000000000000B30D59CC5::::- 작업 전달에서 찾은 매핑 경로, 다음으로 전달: pages/byodInstall.jsp을 참조하십시오.
2025-02-24 12:06:14,713 디버그 [https-jsse-nio-10.127.196.172-8443-exec-10][] cisco.cpm.client.provisioning.StreamingServlet -:000000000000000B30D59CC5::::- 세션 = null
2025-02-24 12:06:14,713 디버그 [https-jsse-nio-10.127.196.172-8443-exec-10][] cisco.cpm.client.provisioning.StreamingServlet -:000000000000000B30D59CC5::::- portalSessionId = null
2025-02-24 12:06:14,713 디버그 [https-jsse-nio-10.127.196.172-8443-exec-10][[]] cisco.cpm.client.provisioning.StreamingServlet -:000000000000000B30D59CC5::::- StreamingServlet URI:/auth/provisioning/download/f6b73ef8-4502-4d50-81aa-bbb91e8828da/NetworkSetupAssistant.exe // 네트워크 지원 애플리케이션이 엔드포인트로 전송되었습니다.

Ise-Psc 로그

애플리케이션이 엔드포인트로 다운로드되면 애플리케이션은 ISE에서 클라이언트 인증서를 가져오기 위해 SCEP 플로우를 시작합니다.

2025-02-24 12:04:39,807 디버그 [DefaultQuartzScheduler_Worker-5][]
org.jscep.client.CertStoreInspector -:::- CertStore에 4개의 인증서 포함:
2025-02-24 12:04:39,807 디버그 [DefaultQuartzScheduler_Worker-5][]
org.jscep.client.CertStoreInspector -:::- 1. '[issuer=CN=Certificate Services Root CA - iseguest; serial=322815127387689606282525327846633020 89]'
2025-02-24 12:04:39,808 디버그 [DefaultQuartzScheduler_Worker-5][]
org.jscep.client.CertStoreInspector -:::- 2. '[issuer=CN=Certificate Services Endpoint Sub CA - iseguest; serial=131900858749761727853768227590303808637]'
2025-02-24 12:04:39,810 디버그 [DefaultQuartzScheduler_Worker-5][]
org.jscep.client.CertStoreInspector -:::- 3. '[issuer=CN=Certificate Services Root CA - iseguest; serial=686276201605863086858498187751006982 24]'
2025-02-24 12:04:39,810 디버그 [DefaultQuartzScheduler_Worker-5][]
org.jscep.client.CertStoreInspector -:::- 4. '[issuer=CN=Certificate Services Node CA - iseguest; serial=729347676986030971539324822275488749 53]'
2025-02-24 12:04:39,812 디버그 [DefaultQuartzScheduler_Worker-5][]
org.jscep.client.CertStoreInspector -:::- 암호화 인증서 선택
2025-02-24 12:04:39,812 디버그 [DefaultQuartzScheduler_Worker-5][]
org.jscep.client.CertStoreInspector -:::- keyEncipherment keyUsage가 있는 인증서 선택
2025-02-24 12:04:39,812 디버그 [DefaultQuartzScheduler_Worker-5][]
org.jscep.client.CertStoreInspector -:::- keyEncipherment keyUsage가 있는 인증서 1개를 찾았습니다.
2025-02-24 12:04:39,812 디버그 [DefaultQuartzScheduler_Worker-5][]
org.jscep.client.CertStoreInspector -:::- [issuer=CN=Certificate Services Endpoint Sub CA - iseguest; serial=131900858749761727853768227590303808637] - 메시지 암호화
2025-02-24 12:04:39,812 디버그 [DefaultQuartzScheduler_Worker-5][]
org.jscep.client.CertStoreInspector -:::- 확인 프로그램 인증서 선택
2025-02-24 12:04:39,812 디버그 [DefaultQuartzScheduler_Worker-5][]
org.jscep.client.CertStoreInspector -:::- digitalSignature keyUsage가 있는 인증서 선택
2025-02-24 12:04:39,812 디버그 [DefaultQuartzScheduler_Worker-5][]
org.jscep.client.CertStoreInspector -:::- digitalSignature keyUsage가 있는 인증서 1개를 찾았습니다.
2025-02-24 12:04:39,812 디버그 [DefaultQuartzScheduler_Worker-5][]
org.jscep.client.CertStoreInspector -:::- [issuer=CN=Certificate Services Endpoint Sub CA - iseguest; serial=131900858749761727853768227590303808637] - 메시지 확인
2025-02-24 12:04:39,812 디버그 [DefaultQuartzScheduler_Worker-5][]
org.jscep.client.CertStoreInspector -:::- 발급자 인증서 선택
2025-02-24 12:04:39,812 디버그 [DefaultQuartzScheduler_Worker-5][]
org.jscep.client.CertStoreInspector -:::- basicConstraints가 있는 인증서 선택
2025-02-24 12:04:39,812 디버그 [DefaultQuartzScheduler_Worker-5][]
org.jscep.client.CertStoreInspector -:::- basicConstraints가 있는 인증서 3개를 찾았습니다.

2025-02-24 12:04:39,812 디버그 [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -:::- [issuer=CN=Certificate Services Endpoint Sub CA - iseguest; serial=131900858749761727853768227590303808637](발급자)
2025-02-24 12:04:39,812 디버그 [DefaultQuartzScheduler_Worker-5][[]] com.cisco.cpm.scep.PKIServerLoadBalancer -:::- SCEP 서버 성능 측정 단위: name[live/dead, total reqs, total failures, inflight reqs, Average RTT] http://127.0.0.1:9444/caservice/scep[라이브,96444,1,0,120]

엔드포인트 프로파일 다운로드

SCEP 프로세스가 완료되고 엔드포인트가 인증서를 설치하면 애플리케이션은 디바이스에서 수행할 향후 인증을 위해 엔드포인트 프로파일을 다운로드합니다.

2025-02-24 12:06:26,539 디버그 [https-jsse-nio-8905-exec-1][[]] cisco.cpm.client.provisioning.EvaluationServlet -:::- Referer = Windows // 웹 페이지를 기반으로 Windows 장치가 검색되었습니다.
2025-02-24 12:06:26,539 디버그 [https-jsse-nio-8905-exec-1][[]] cisco.cpm.client.provisioning.EvaluationServlet -:::- 세션 = 000000000000000B30D59CC5
2025-02-24 12:06:26,539 디버그 [https-jsse-nio-8905-exec-1][[]] cisco.cpm.client.provisioning.EvaluationServlet -:::- 세션 = 000000000000000B30D59CC5
2025-02-24 12:06:26,539 디버그 [https-jsse-nio-8905-exec-1][[]] cisco.cpm.client.provisioning.EvaluationServlet -:::- nsp 프로필 프로비저닝
2025-02-24 12:06:26,546 디버그 [https-jsse-nio-8905-exec-2][[]] cisco.cpm.client.provisioning.StreamingServlet -:::- 세션 = 000000000000000B30D59CC5
2025-02-24 12:06:26,546 디버그 [https-jsse-nio-8905-exec-2][[]] cisco.cpm.client.provisioning.StreamingServlet -:::- portalSessionId = null
2025-02-24 12:06:26,546 디버그 [https-jsse-nio-8905-exec-2][[]] cisco.cpm.client.provisioning.StreamingServlet -:::- StreamingServlet URI:/auth/provisioning/download/b8ce01e6-b150-4d4e-9698-40e48d5e0197/Cisco-ISE-NSP.xml//NSP 프로파일이 엔드포인트에 다운로드됩니다.
2025-02-24 12:06:26,547 디버그 [https-jsse-nio-8905-exec-2][[]] cisco.cpm.client.provisioning.StreamingServlet -:::- ip로 스트리밍: 파일 형식: NativeSPProfile 파일 이름:Cisco-ISE-NSP.xml //The Network Assistant Application
2025-02-24 12:06:26,547 디버그 [https-jsse-nio-8905-exec-2][[]] cisco.cpm.client.provisioning.StreamingServlet -:::::- BYODStatus:INIT_PROFILE
2025-02-24 12:06:26,547 디버그 [https-jsse-nio-8905-exec-2][[]] cisco.cpm.client.provisioning.StreamingServlet -:::::- userId가 테스트로 설정되었습니다.
2025-02-24 12:06:26,558 디버그 [https-jsse-nio-8905-exec-2][[]] cisco.cpm.client.provisioning.StreamingServlet -:::::- 리디렉션 유형은 다음과 같습니다. SUCCESS_PAGE, 리디렉션 url: mac의 경우:

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.