Windows 및 ISE에서 단일 SSID 무선 BYOD 구성

목차

소개

이 문서에서는 Single-SSID와 Dual-SSID를 모두 사용하여 Windows 시스템용 Cisco ISE(Identity Services Engine)에서 BYOD(Bring Your Own Device)를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco ISE 버전 3.0 구성
- Cisco WLC 구성
- BYOD 작동

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ISE 버전 3.0
- Windows 10
- WLC 및 AP

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

잠재적인 영향을 이해해야 합니다.

이론

단일 SSID BYOD에서는 디바이스 온보딩 및 나중에 등록 디바이스에 대한 전체 액세스를 제공하는 데 하나의 SSID만 사용됩니다.먼저 사용자 이름과 비밀번호(MSCHAPv2)를 사용하여 SSID에 연결합니다. ISE에서 성공적으로 인증되면 사용자는 BYOD 포털로 리디렉션됩니다.디바이스 등록이 완료되면 최종 클라이언트는 ISE에서 NSA(Native Supplicant Assistant)를 다운로드합니다.NSA는 최종 클라이언트에 설치되고 ISE에서 프로파일 및 인증서를 다운로드합니다.NSA는 무선 신청자를 구성하고 클라이언트는 인증서를 설치합니다.엔드포인트는 EAP-TLS를 사용하여 다운로드한 인증서를 사용하여 동일한 SSID에 대해 다른 인증을 수행합니다.ISE는 클라이언트의 새 요청을 확인하고 EAP 방법 및 장치 등록을 확인하고 장치에 대한 전체 액세스 권한을 부여합니다.

Windows BYOD 단일 SSID 단계-

- 초기 EAP-MSCHAPv2 인증
- BYOD 포털로 리디렉션
- 장치 등록
- NSA 다운로드
- 프로필 다운로드
- 인증서 다운로드
- EAP-TLS 인증

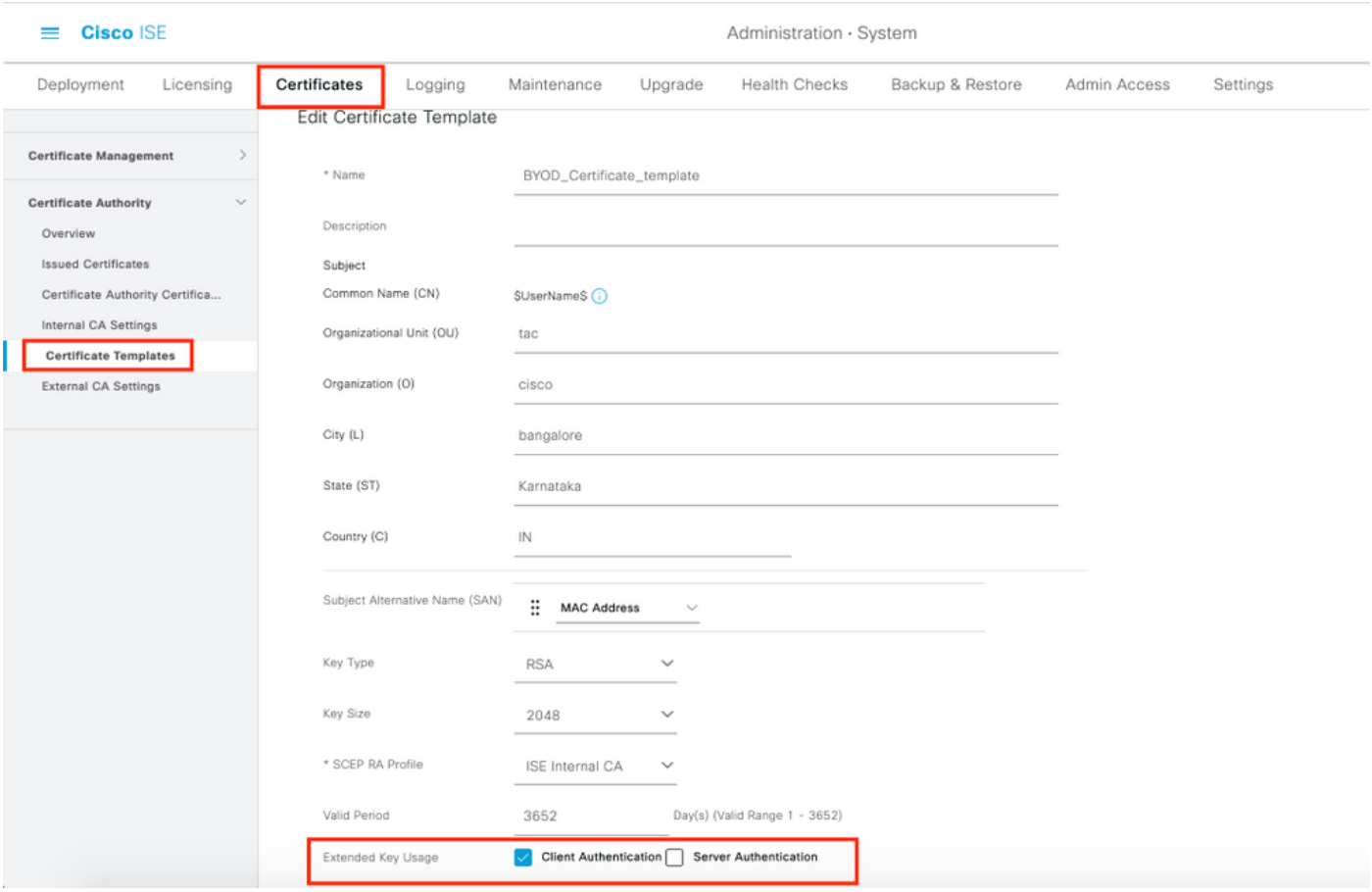
구성

ISE 컨피그레이션

1단계. ISE에 네트워크 디바이스를 추가하고 RADIUS 및 공유 키를 구성합니다.

ISE > **Administration > Network Devices > Add Network Device로 이동합니다**.

2단계. BYOD 사용자를 위한 인증서 템플릿을 만듭니다.템플릿에 클라이언트 인증 고급 키 사용이 있어야 합니다.기본 EAP_Certificate_Template을 사용할 수 있습니다.

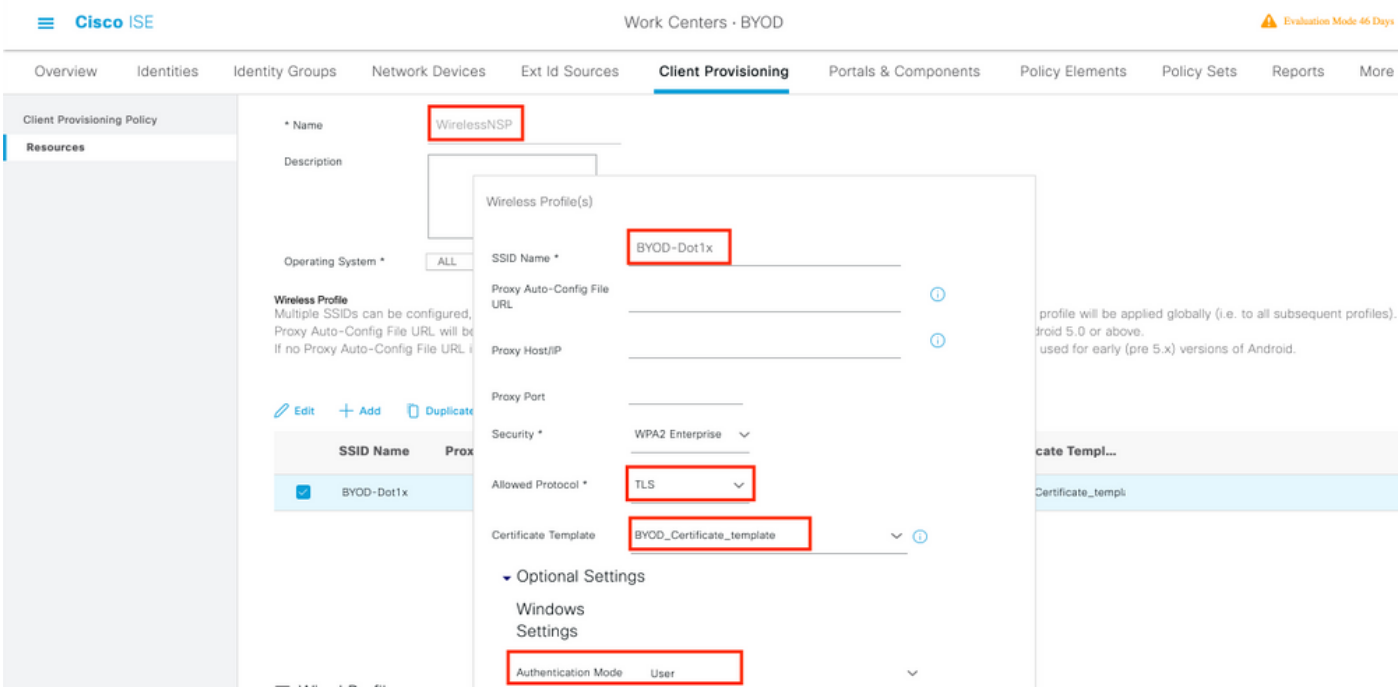


3단계. 무선 프로파일에 대한 기본 신청자 프로파일을 생성합니다.

ISE **> Work Centers(작업 센터) > BYOD > Client Provisioning(클라이언트 프로비저닝)으로 이동합니다**.Add(**추가**)를 클릭하고 드롭다운**에서 Native Supplicant Profile (NSP)**(기본 신청자 프로필 (NSP)을 선택합니다.

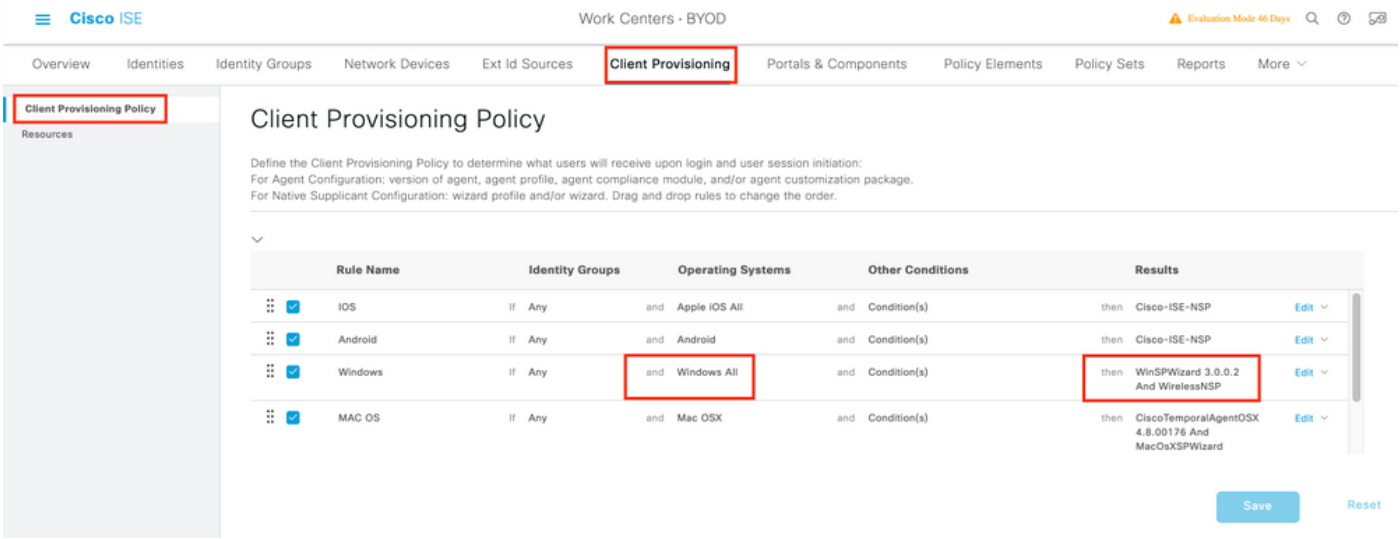
여기서 SSID 이름은 단일 SSID BYOD를 수행하기 전에 연결된 이름과 동일해야 합니다.Protocol as TLS를 선택합니다.이전 단계에서 생성한 인증서 템플릿을 선택하거나 기본 EAP_Certificate_Template을 사용할 수 있습니다.

선택 사항인 설정에서 사용자 또는 사용자 및 머신 인증을 요구 사항에 따라 선택합니다.이 예에서는 사용자 인증으로 구성됩니다.다른 설정은 기본값으로 둡니다.



4단계. Windows 장치에 대한 클라이언트 프로비저닝 정책을 만듭니다.

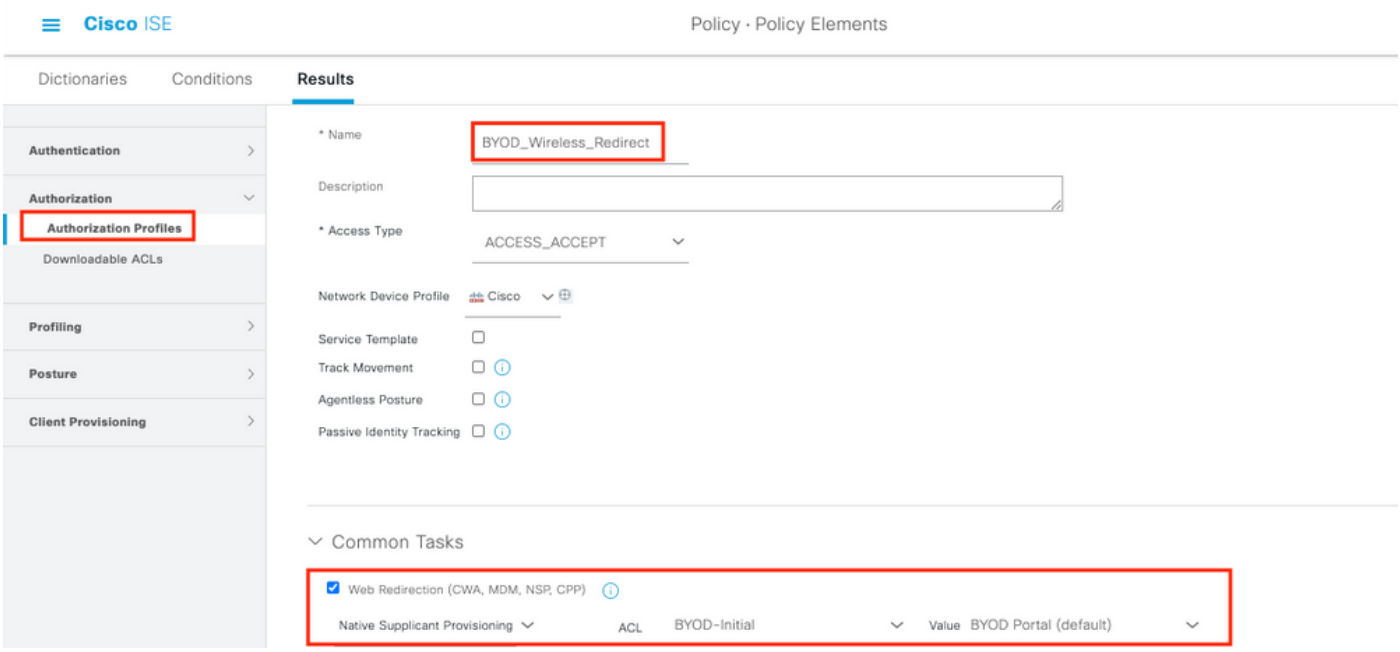
ISE **> Work Centers > BYOD > Client Provisioning > Client Provisioning Policy로 이동합니다**.운영 체제를 **Windows ALL로 선택합니다**.이전 단계**에서** 생성된 **WinSPWizard 3.0.0.2 및 NSP**를 선택합니다.



5단계. BYOD 디바이스로 등록되지 않은 디바이스에 대한 권한 부여 프로파일을 생성합니다.

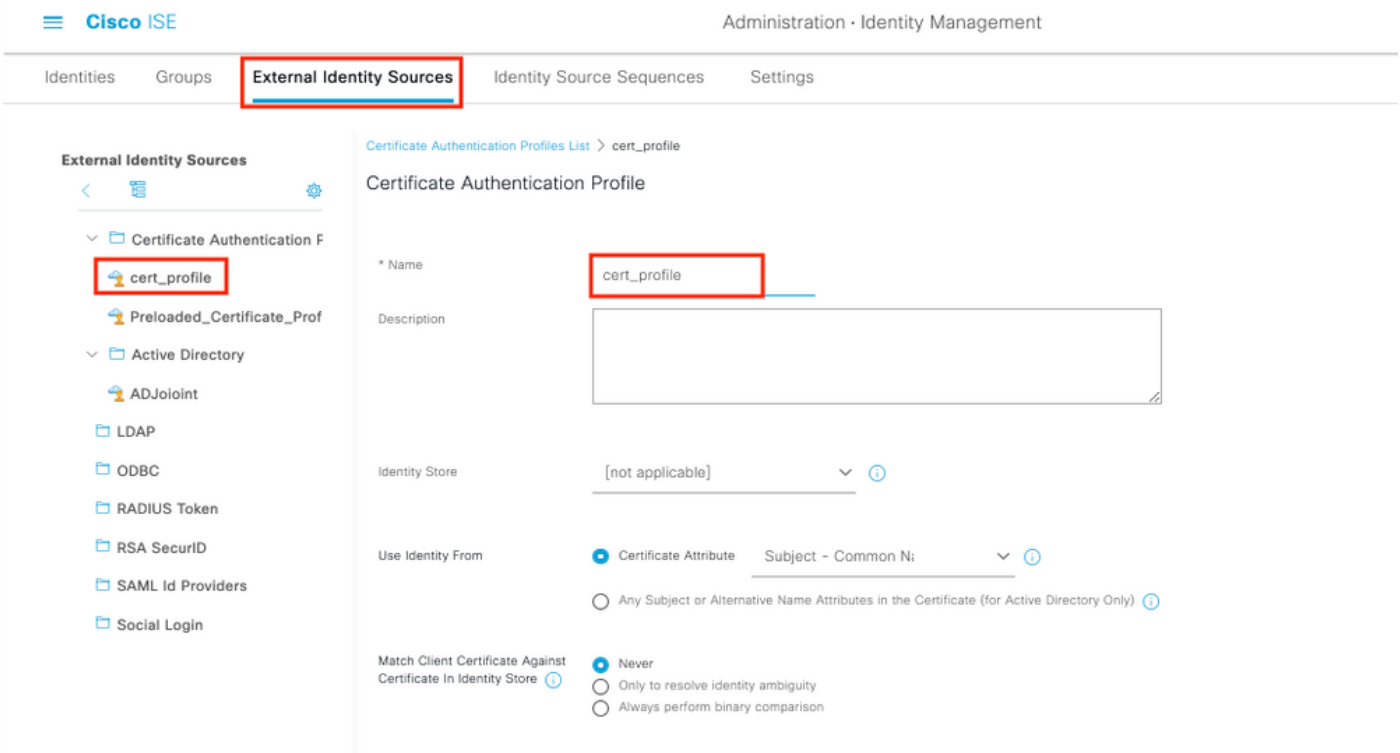
ISE **> Policy > Policy Elements > Results > Authorization > Authorization Profiles > Add로 이동합니다**.

Common **Task(공통 작업)**에서 Native **Supplicant Provisioning(기본 신청자 프로비저닝)을 선택합니다**.WLC에 생성된 리디렉션 ACL 이름을 정의하고 BYOD 포털을 선택합니다.기본 포털이 사용됩니다.맞춤형 BYOD 포털을 생성할 수 있습니다.ISE **> Work Centers(작업 센터) > BYOD > Portals** and components(포털 및 구성 요소)로 이동하고 **Add(추가)**를 클릭합니다.

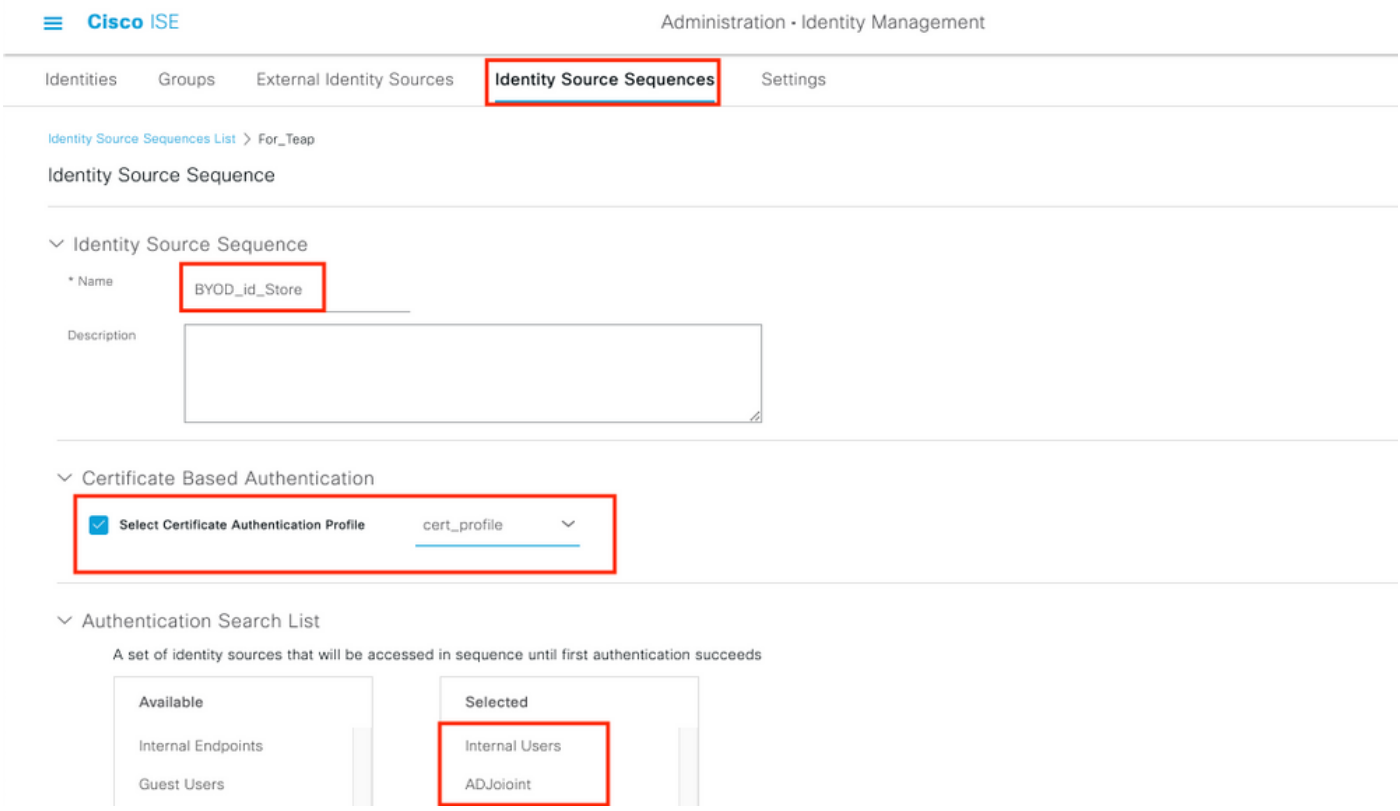


6단계. 인증서 프로파일을 생성합니다.

ISE **> 관리 > 외부 ID 소스 > 인증서 프로필로 이동합니다**.여기에서 새 인증서 프로파일을 생성하거나 기본 인증서 프로파일을 사용합니다.



7단계. ID 소스 시퀀스를 생성하고 이전 단계에서 생성한 인증서 프로파일을 선택하거나 기본 인증서 프로파일을 사용합니다.사용자가 BYOD 등록 후 EAP-TLS를 수행하여 전체 액세스 권한을 얻는 경우 이 작업이 필요합니다.



8단계. 정책 세트, 인증 정책 및 권한 부여 정책을 생성합니다.

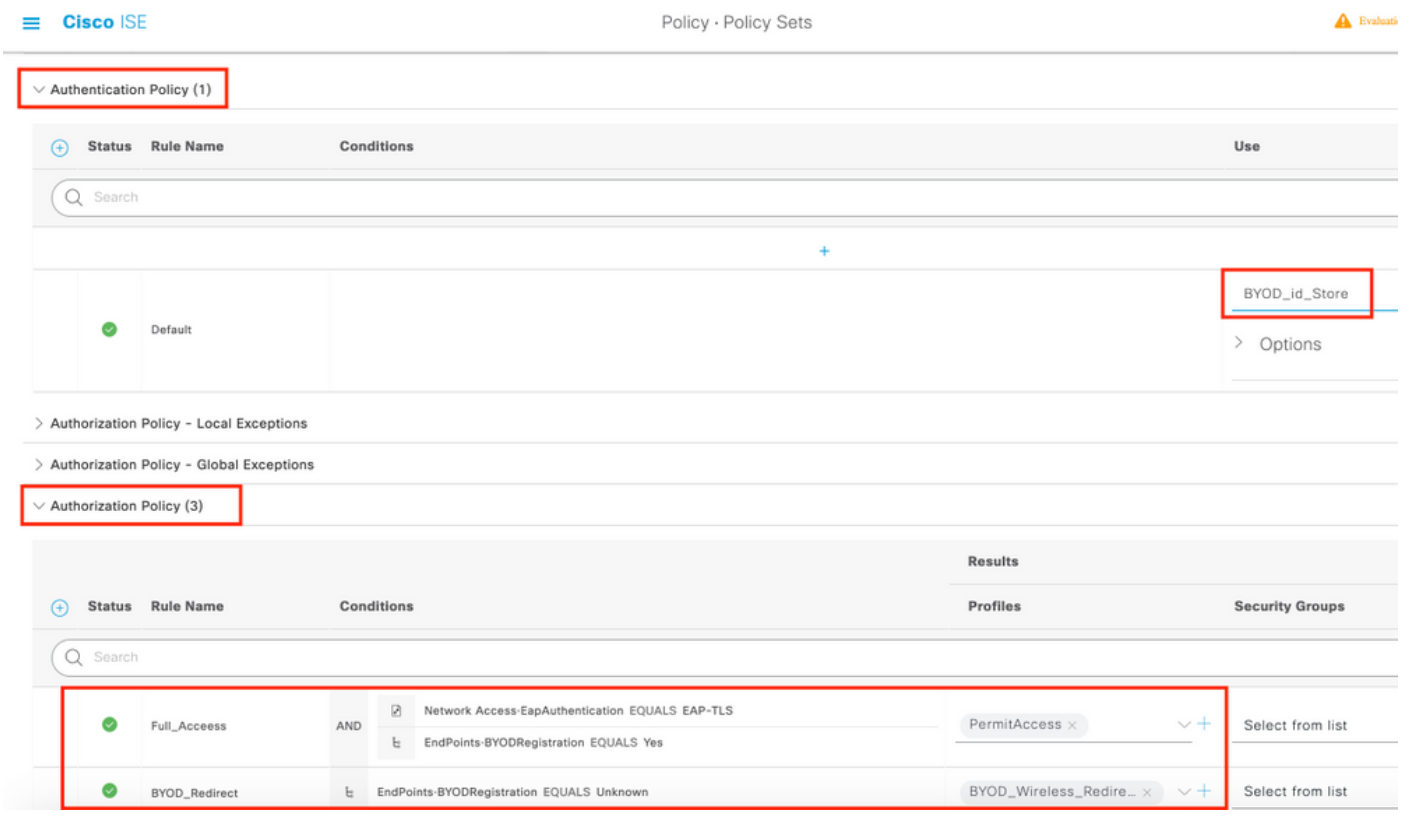
ISE **> Policy > Policy Sets로 이동합니다**.정책 세트를 생성하고 **저장합니다**.

인증 정책을 생성하고 이전 단계에서 생성한 ID 소스 시퀀스를 선택합니다.

권한 부여 정책을 생성합니다.두 개의 정책을 생성해야 합니다.

1. BYOD가 등록되지 아니한 장치의 경우5단계에서 생성한 리디렉션 프로파일을 제공합니다.

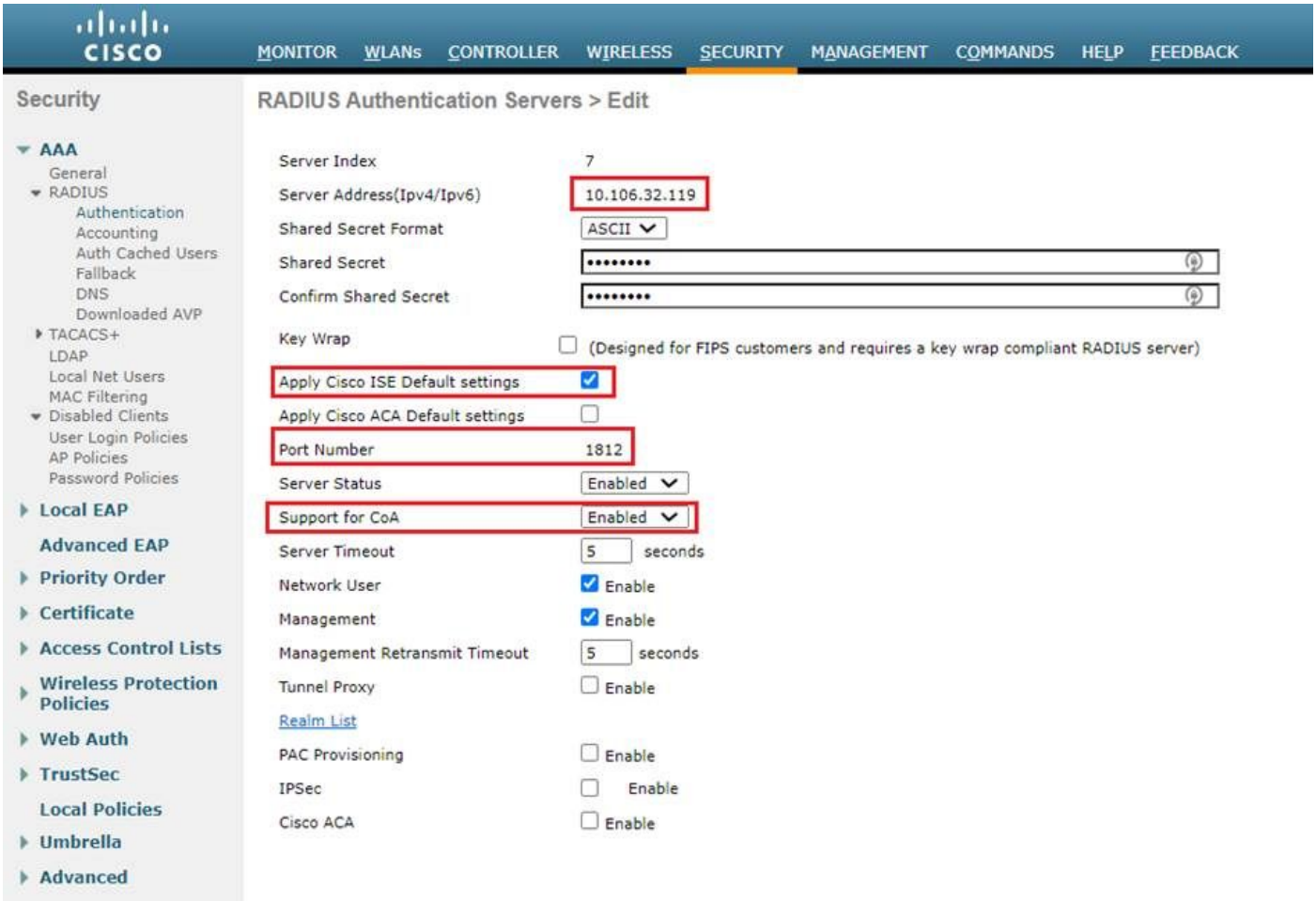
2. BYOD가 등록되고 EAP-TLS를 수행하는 장치이러한 장치에 대한 모든 액세스 권한을 부여합니다.



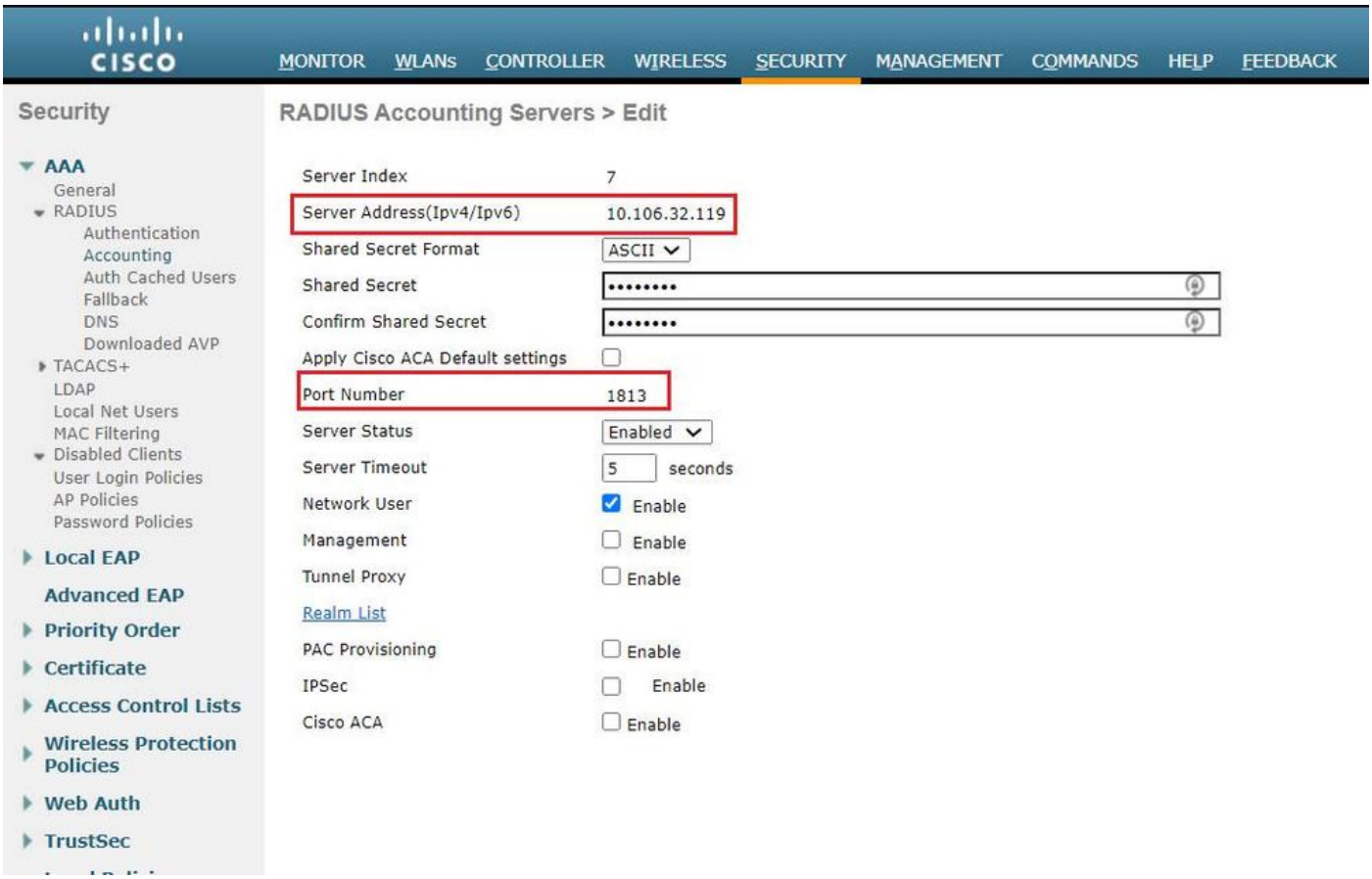
WLC 컨피그레이션

1단계. WLC에서 Radius 서버를 구성합니다.

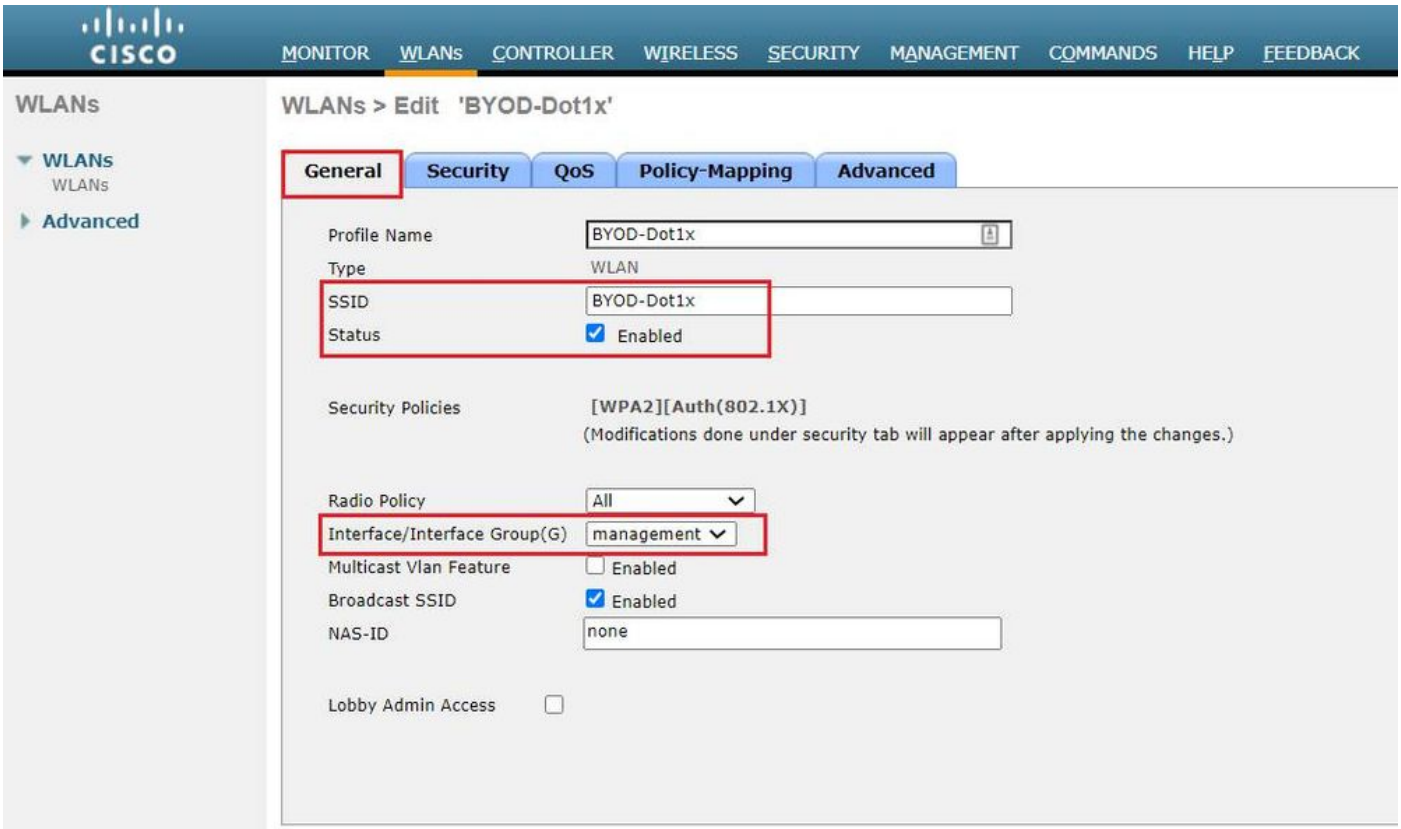
Security(**보안) > AAA > Radius > Authentication(인증)으로 이동합니다.**

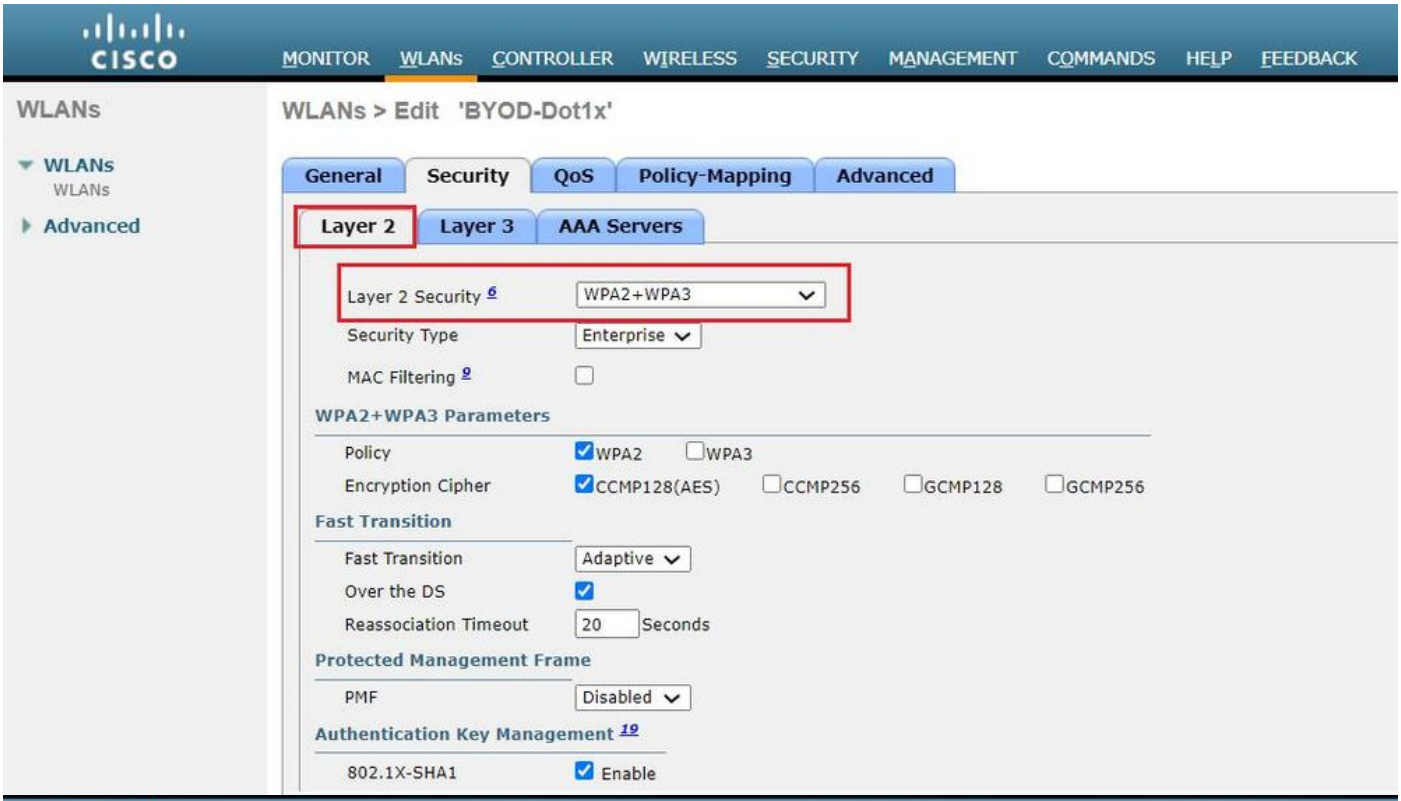


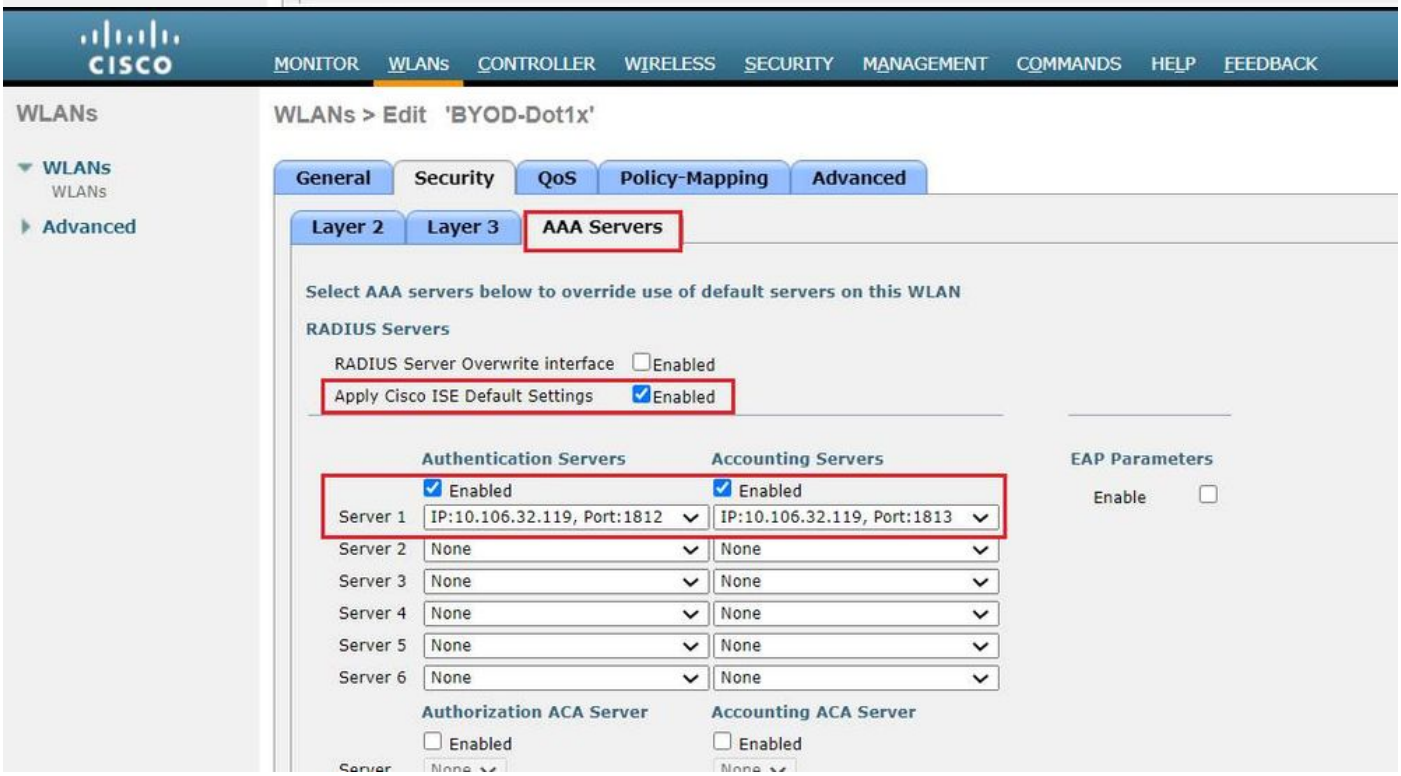
Security(보안) > AAA > Radius > Accounting(계정 관리)으로 이동합니다.

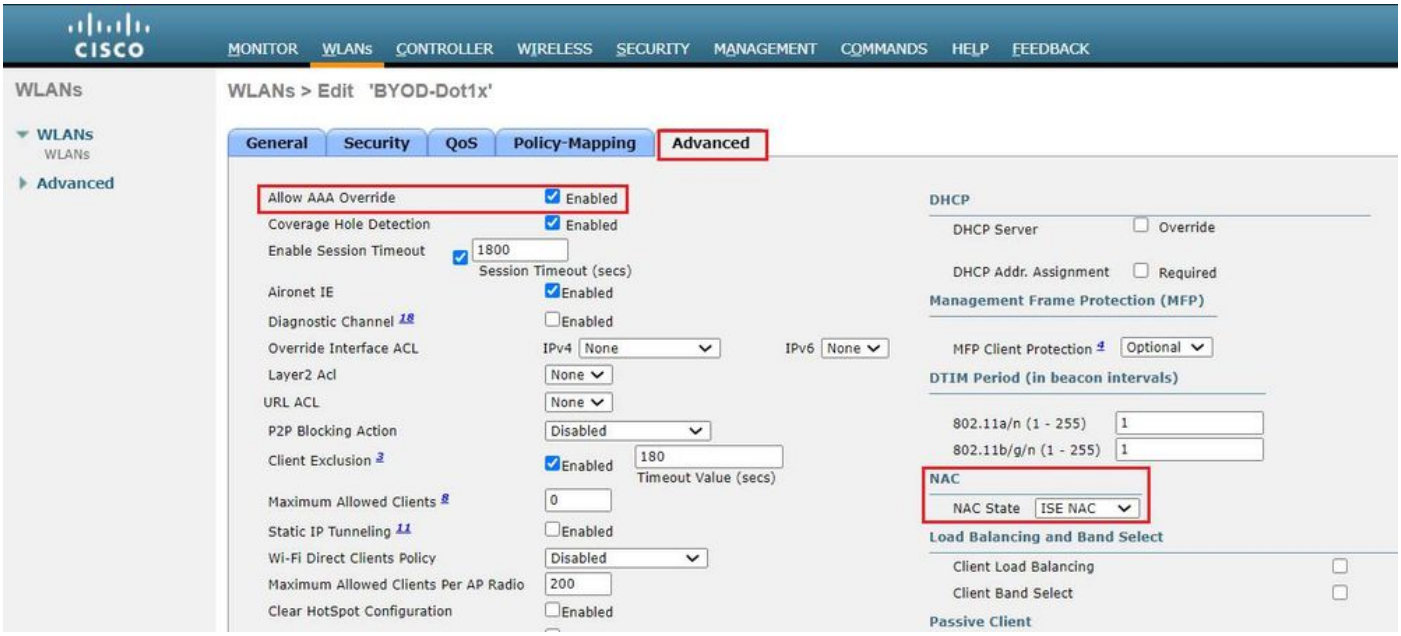


2단계. Dot1x SSID를 구성합니다.




MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
WLANs
WLANs
Advanced
WLANs > Edit 'BYOD-Dot1x'
General Security QoS Policy-Mapping Advanced
Layer 2 Layer 3 AAA Servers
Layer 2 Security 6 WPA2+WPA3
Security Type Enterprise
MAC Filtering 9
WPA2+WPA3 Parameters
Policy WPA2 WPA3
Encryption Cipher CCMP128(AES) CCMP256 GCMP128 GCMP256
Fast Transition
Fast Transition Adaptive
Over the DS
Reassociation Timeout 20 Seconds
Protected Management Frame
PMF Disabled
Authentication Key Management 19
802.1X-SHA1 Enable

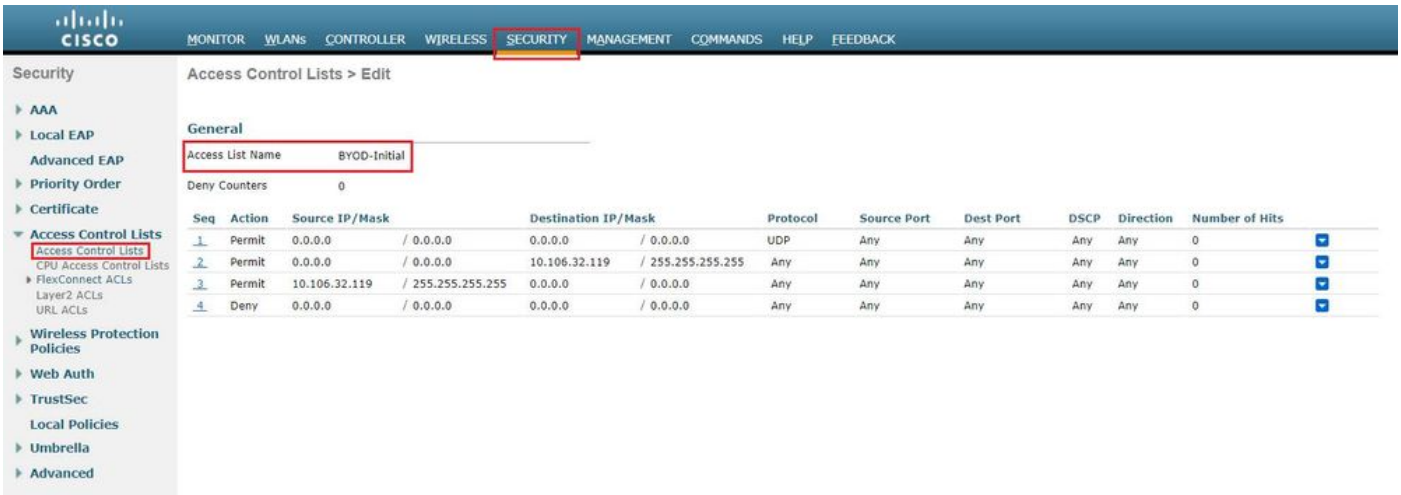

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
WLANs
WLANs
Advanced
WLANs > Edit 'BYOD-Dot1x'
General Security QoS Policy-Mapping Advanced
Layer 2 Layer 3 AAA Servers
Select AAA servers below to override use of default servers on this WLAN
RADIUS Servers
RADIUS Server Overwrite interface Enabled
Apply Cisco ISE Default Settings Enabled
Authentication Servers
Accounting Servers
EAP Parameters
Enabled
Enabled
Enable
Server 1 IP:10.106.32.119, Port:1812 IP:10.106.32.119, Port:1813
Server 2 None None
Server 3 None None
Server 4 None None
Server 5 None None
Server 6 None None
Authorization ACA Server
Accounting ACA Server
Enabled
Enabled



3단계. 디바이스 프로비저닝을 위한 제한된 액세스를 제공하도록 리디렉션 ACL을 구성합니다.

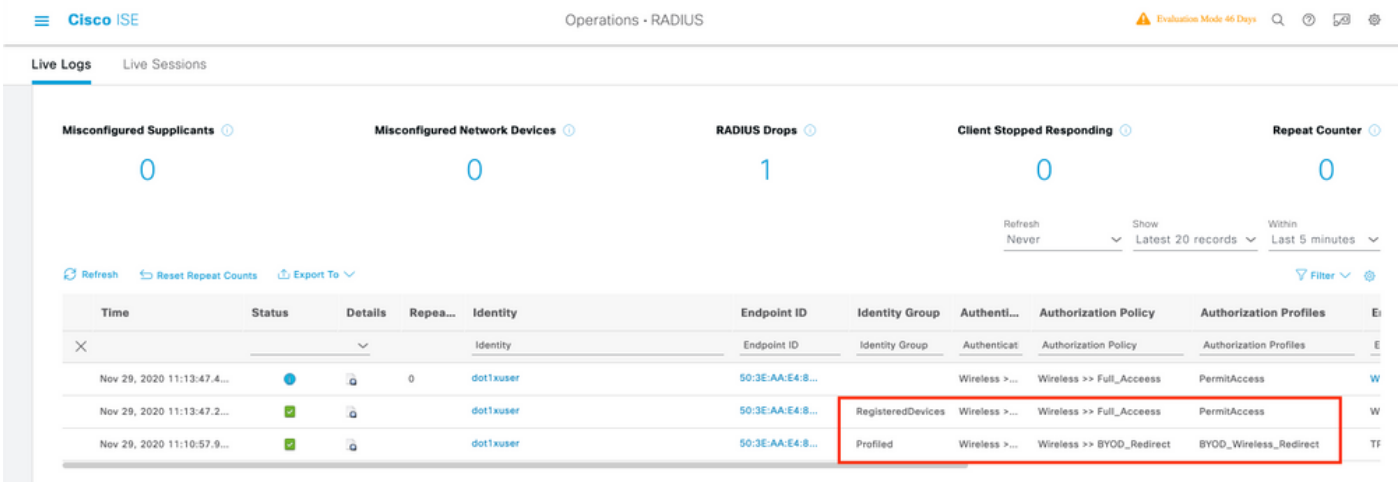
- DHCP 및 DNS에 대한 UDP 트래픽 허용(DHCP는 기본적으로 허용됨)
- ISE와의 통신.
- 다른 트래픽을 거부합니다.

이름:BYOD-Initial(또는 권한 부여 프로필에서 ACL을 수동으로 지정한 항목)

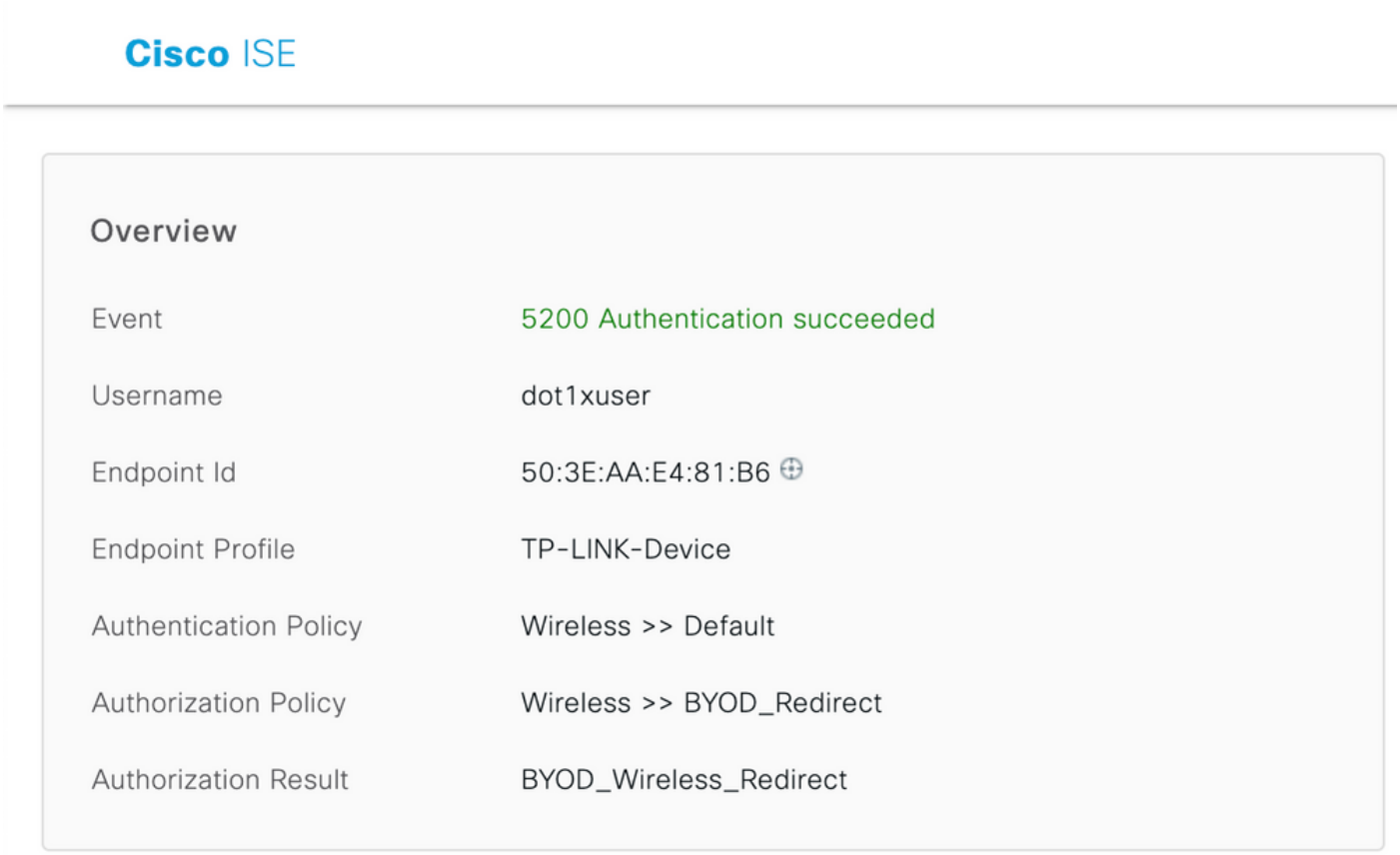


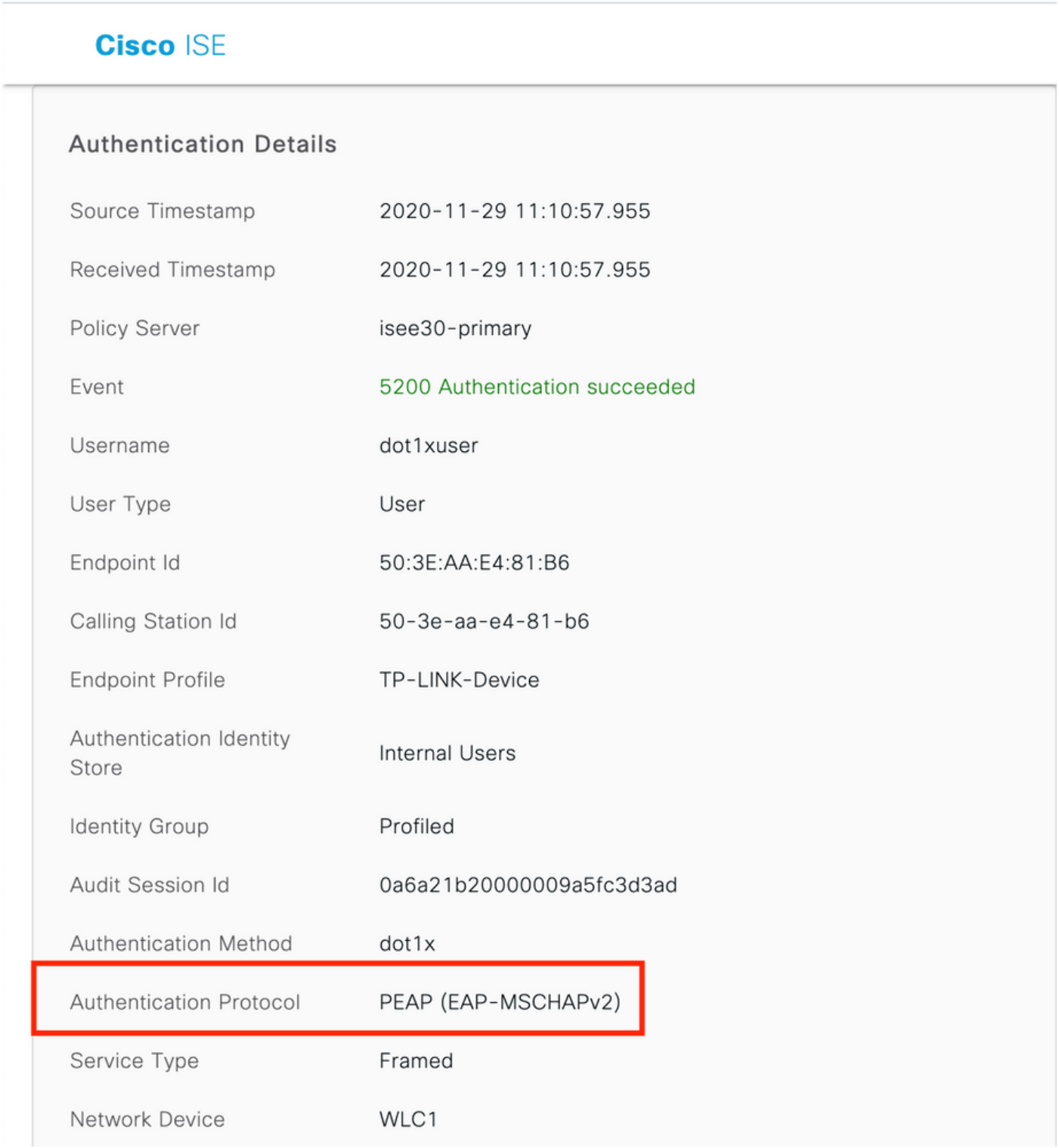
다음을 확인합니다.

인증 플로우 확인



1. 처음 로그인할 때 사용자는 사용자 이름과 비밀번호를 사용하여 PEAP 인증을 수행합니다.ISE에서 사용자는 Redirect Rule BYOD-Redirect를 시작합니다.



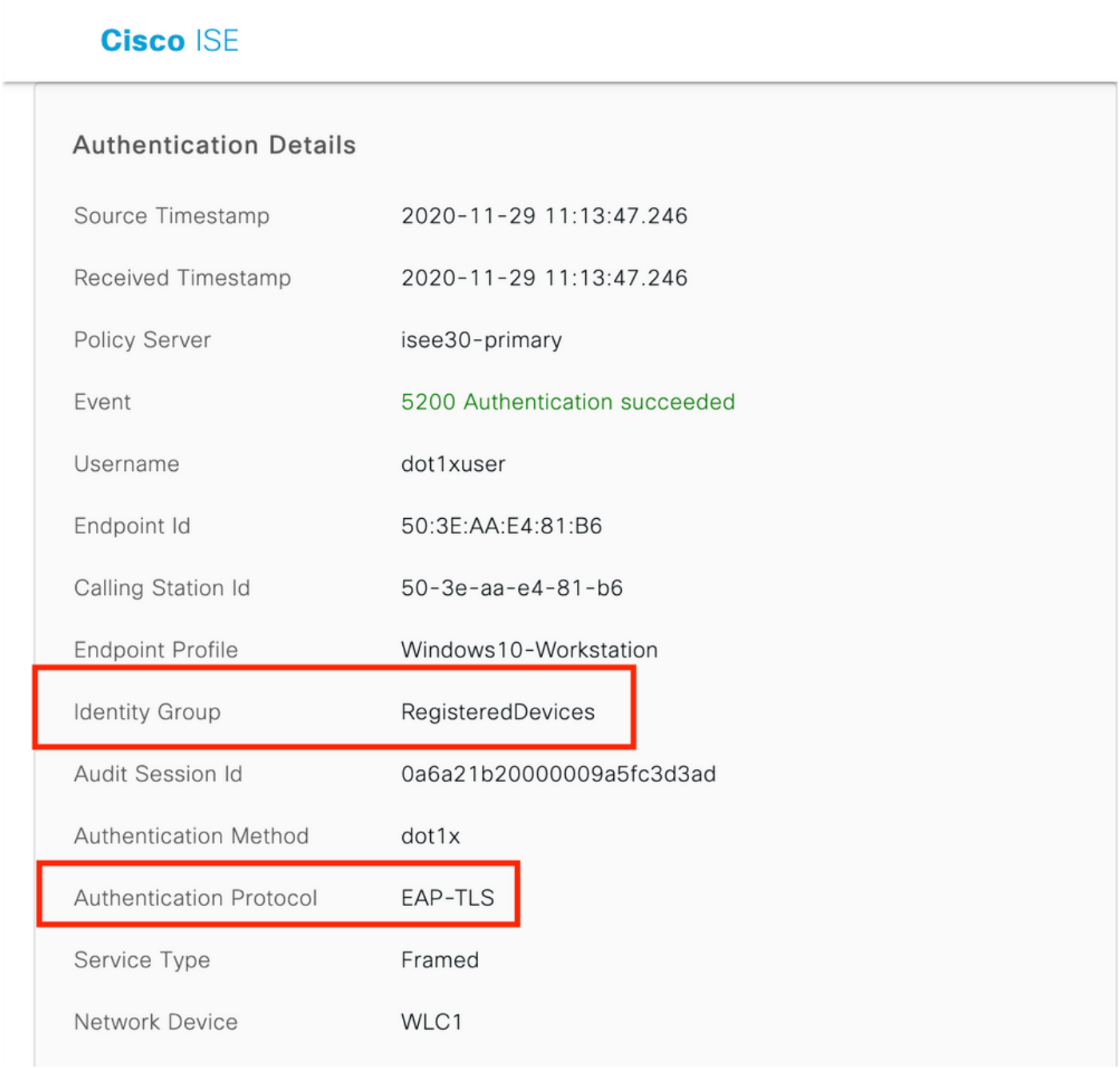


2. BYOD 등록 후 사용자는 등록된 장치에 추가되고 이제 EAP-TLS를 수행하고 전체 액세스 권한을 얻습니다.

Cisco ISE

Overview

Event	5200 Authentication succeeded
Username	dot1xuser
Endpoint Id	50:3E:AA:E4:81:B6
Endpoint Profile	Windows10-Workstation
Authentication Policy	Wireless >> Default
Authorization Policy	Wireless >> Full_Acceess
Authorization Result	PermitAccess

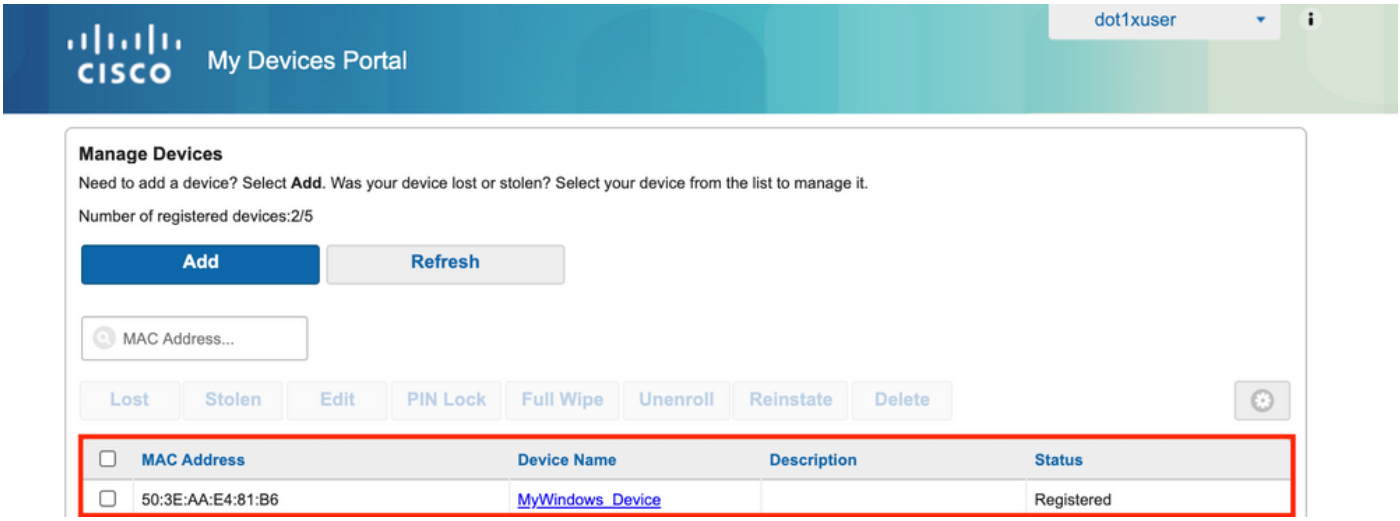


내 장치 포털 확인

MyDevices Portal(내 디바이스 포털)로 이동하고 자격 증명을 사용하여 로그인합니다. 디바이스 이름과 등록 상태를 볼 수 있습니다.

MyDevices 포털에 대한 URL을 생성할 수 있습니다.

ISE **> Work Centers(작업 센터) > BYOD > Portal and Components(포털 및 구성 요소) > My Devices Portal(내 디바이스 포털) > Login Settings(로그인 설정)로 이동한** 다음 Fully Qualified URL을 입력합니다.



문제 해결

일반 정보

BYOD 프로세스의 경우 PSN 노드의 디버그에서 이 ISE 구성 요소를 활성화해야 합니다.

scep - scep 로그 메시지.대상 로그 **filesguest.log 및 ise-psc.log**.

client-webapp - 인프라 메시지를 담당하는 구성 요소입니다.대상 로그 파일 - **ise-psc.log**

portal-web-action - 클라이언트 프로비저닝 정책 처리를 담당하는 구성 요소입니다.대상 로그 파일 - **guest.log**.

portal - 모든 포털 관련 이벤트대상 로그 파일 - **guest.log**

portal-session-manager -대상 로그 파일 - **포털 세션 관련 디버그 메시지 - gues.log**

ca-service- ca-service 메시지 -대상 로그 파일 -**caservice.log 및 caservice-misc.log**

ca-service-cert- ca-service 인증서 메시지 - 대상 로그 파일 - caservice.**log 및 caservice-misc.log**

admin-ca- ca-service admin messages -대상 로그 파일 **ise-psc.log**, **caservice.log 및 casrvice-misc.log**

certprovisioningportal- 인증서 프로비저닝 포털 메시지 -대상 로그 **파일 ise-psc.log**

nsf - NSF 관련 메시지 -대상 로그 파일 **ise-psc.log**

nsf-session- 세션 캐시 관련 메시지 -대상 로그 파일 **ise-psc.log**

runtime-AAA- 모든 런타임 이벤트입니다.대상 로그 파일 - **prrt-server.log**.

클라이언트측 로그의 경우:

%temp%\spwProfileLog.txt를 찾습니다(예:C:\Users\<사용자 이름 >\AppData\Local\Temp\spwProfileLog.txt

작업 로그 분석

ISE 로그

초기 액세스 - 리디렉션 ACL과 함께 BYOD 포털용 리디렉션 URL을 사용합니다.

prrt-server.log-

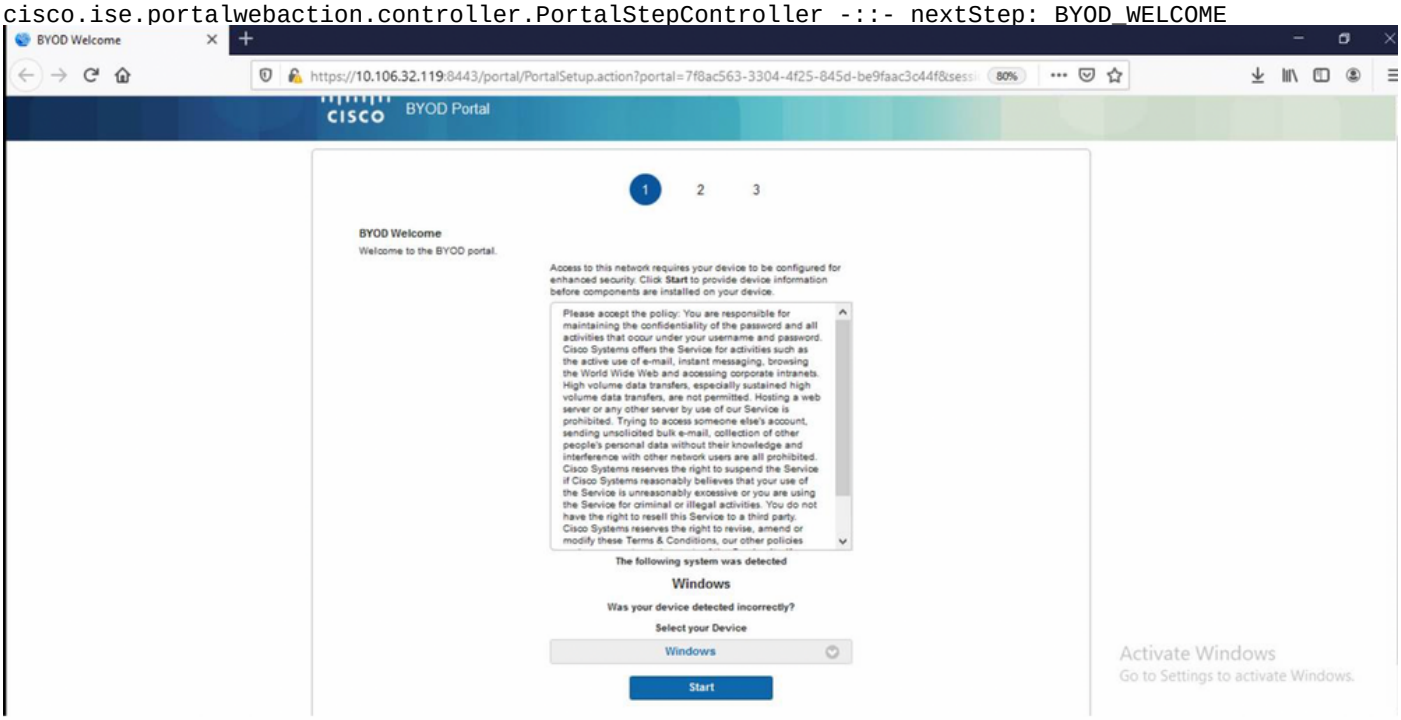
```
Radius,2020-12-02 05:43:52,395,DEBUG,0x7f433e6b8700,cntx=0008590803,sesn=isee30-
primary/392215758/699,CPMSessionID=0a6a21b20000009f5fc770c7,user=dot1xuser,CallingStationID=50-
3e-aa-e4-81-b6,RADIUS PACKET:: Code=2(AccessAccept) Identifier=254 Length=459 [1] User-Name -
value: [dot1xuser] [25] Class - value: [****] [79] EAP-Message - value: [ñ [80] Message-
Authenticator - value: [.2{wëbÙ¨ÅþO5‹Z] [26] cisco-av-pair - value: [url-redirect-acl=BYOD-
Initial] [26] cisco-av-pair - value: [url-
redirect=https://10.106.32.119:8443/portal/gateway?sessionId=0a6a21b20000009f5fc770c7&portal=7f8
ac563-3304-4f25-845d-be9faac3c44f&action=nsp&token=53a2119de6893df6c6fca25c8d6bd061] [26] MS-
MPPE-Send-Key - value: [****] [26] MS-MPPE-Recv-Key - value: [****] ,RADIUSHandler.cpp:2216
```

최종 사용자가 웹 사이트로 이동하려고 시도하여 WLC에 의해 ISE 리디렉션 URL로 리디렉션된 경우.

Guest.log -

```
2020-12-02 05:43:58,339 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-5][]
com.cisco.ise.portal.Gateway -::- Gateway Params (after update):
redirect=www.msftconnecttest.com/redirect client_mac=null daysToExpiry=null ap_mac=null
switch_url=null wlan=null action=nsp sessionId=0a6a21b20000009f5fc770c7 portal=7f8ac563-3304-
4f25-845d-be9faac3c44f isExpired=null token=53a2119de6893df6c6fca25c8d6bd061 2020-12-02
05:43:58,339 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-5][]
cisco.ise.portalwebaction.utils.RadiusSessionUtil -::- sessionId=0a6a21b20000009f5fc770c7 :
token=53a2119de6893df6c6fca25c8d6bd061 2020-12-02 05:43:58,339 DEBUG [https-jsse-nio-
10.106.32.119-8443-exec-5][] cisco.ise.portalwebaction.utils.RadiusSessionUtil -::- Session
token successfully validated. 2020-12-02 05:43:58,344 DEBUG [https-jsse-nio-10.106.32.119-8443-
exec-5][] cisco.ise.portal.util.PortalUtils -::- UserAgent : Mozilla/5.0 (Windows NT 10.0;
Win64; x64; rv:83.0) Gecko/20100101 Firefox/83.0 2020-12-02 05:43:58,344 DEBUG [https-jsse-nio-
10.106.32.119-8443-exec-5][] cisco.ise.portal.util.PortalUtils -::- isMozilla: true 2020-12-02
05:43:58,344 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-5][] com.cisco.ise.portal.Gateway -
::- url: /portal/PortalSetup.action?portal=7f8ac563-3304-4f25-845d-
be9faac3c44f&sessionId=0a6a21b20000009f5fc770c7&action=nsp&redirect=www.msftconnecttest.com%2Fre
direct 2020-12-02 05:43:58,355 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7][]
cisco.ise.portalwebaction.controller.PortalFlowInterceptor -::- start guest flow interceptor...
2020-12-02 05:43:58,356 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7][]
cisco.ise.portalwebaction.actions.BasePortalAction -::- Executing action PortalSetup via request
/portal/PortalSetup.action 2020-12-02 05:43:58,356 DEBUG [https-jsse-nio-10.106.32.119-8443-
exec-7][] cisco.ise.portalwebaction.actions.PortalSetupAction -::- executeAction... 2020-12-02
05:43:58,360 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7][]
cisco.ise.portalwebaction.actions.BasePortalAction -::- Result from action, PortalSetup: success
2020-12-02 05:43:58,360 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7][]
cisco.ise.portalwebaction.actions.BasePortalAction -::- Action PortalSetup Complete for request
/portal/PortalSetup.action 2020-12-02 05:43:58,360 DEBUG [https-jsse-nio-10.106.32.119-8443-
exec-7][] cpm.guestaccess.flowmanager.processor.PortalFlowProcessor -::- Current flow step:
INIT, otherInfo=id: 226ea25b-5e45-43f5-b79d-fb59cab96def 2020-12-02 05:43:58,361 DEBUG [https-
jsse-nio-10.106.32.119-8443-exec-7][] cpm.guestaccess.flowmanager.step.StepExecutor -::- Getting
next flow step for INIT with TranEnum=PROCEED 2020-12-02 05:43:58,361 DEBUG [https-jsse-nio-
10.106.32.119-8443-exec-7][] cpm.guestaccess.flowmanager.step.StepExecutor -::- StepTran for
Step=INIT=> tranEnum=PROCEED, toStep=BYOD_WELCOME 2020-12-02 05:43:58,361 DEBUG [https-jsse-nio-
10.106.32.119-8443-exec-7][] cpm.guestaccess.flowmanager.step.StepExecutor -::- Find Next
Step=BYOD_WELCOME 2020-12-02 05:43:58,361 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7][]
cpm.guestaccess.flowmanager.step.StepExecutor -::- Step : BYOD_WELCOME will be visible! 2020-12-
```

```
02 05:43:58,361 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7][]
cpm.guestaccess.flowmanager.step.StepExecutor -::- Returning next step =BYOD_WELCOME 2020-12-02
05:43:58,362 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7][]
cpm.guestaccess.flowmanager.adaptor.PortalUserAdaptorFactory -::- Looking up Guest user with
uniqueSubjectId=5f5592a4f67552b855ecc56160112db42cf7074e 2020-12-02 05:43:58,365 DEBUG [https-
jsse-nio-10.106.32.119-8443-exec-7][]
cpm.guestaccess.flowmanager.adaptor.PortalUserAdaptorFactory -::- Found Guest user 'dot1xuserin
DB using uniqueSubjectID '5f5592a4f67552b855ecc56160112db42cf7074e'. authStoreName in
DB=Internal Users, authStoreGUID in DB=9273fe30-8c01-11e6-996c-525400b48521. DB ID=bab8f27d-
c44a-48f5-9fe4-5187047bffc0 2020-12-02 05:43:58,366 DEBUG [https-jsse-nio-10.106.32.119-8443-
exec-7][] cisco.ise.portalwebaction.controller.PortalStepController -::- ++++ updatePortalState:
PortalSession (e0d457d9-a346-4b6e-bcca-5cf29e12dacc) current state is INITIATED and current step
is BYOD_WELCOME 2020-12-02 05:40:35,611 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-6][]
com.cisco.ise.portalSessionManager.PortalSession -::- Setting the portal session state to ACTIVE
2020-12-02 05:40:35,611 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-6][]
cisco.ise.portalwebaction.controller.PortalStepController -::- nextStep: BYOD_WELCOME
```



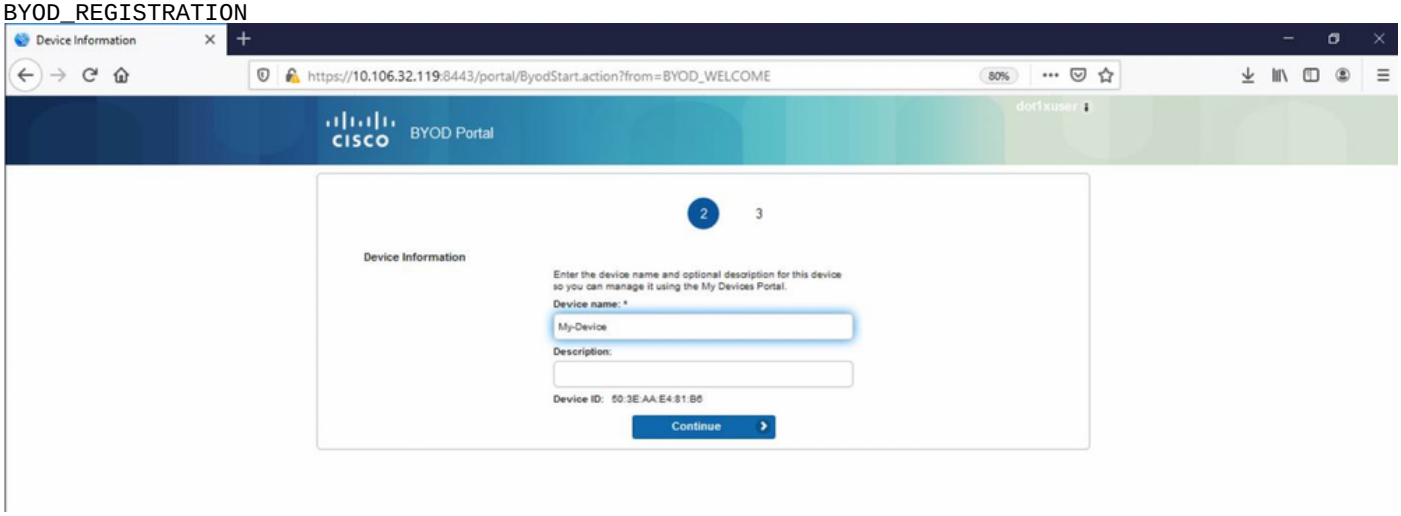
BYOD Welcome 페이지에서 Start(시작)를 클릭합니다.

```
020-12-02 05:44:01,926 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-3][]
cisco.ise.portalwebaction.actions.BasePortalAction -:dot1xuser:- Executing action ByodStart via
request /portal/ByodStart.action 2020-12-02 05:44:01,926 DEBUG [https-jsse-nio-10.106.32.119-
8443-exec-3][] cisco.ise.portalwebaction.controller.PortalPreResultListener -:dot1xuser:-
currentStep: BYOD_WELCOME
```

이 시점에서 ISE는 BYOD에 필요한 파일/리소스가 있는지 여부를 평가하고 자신을 BYOD INIT 상태로 설정합니다.

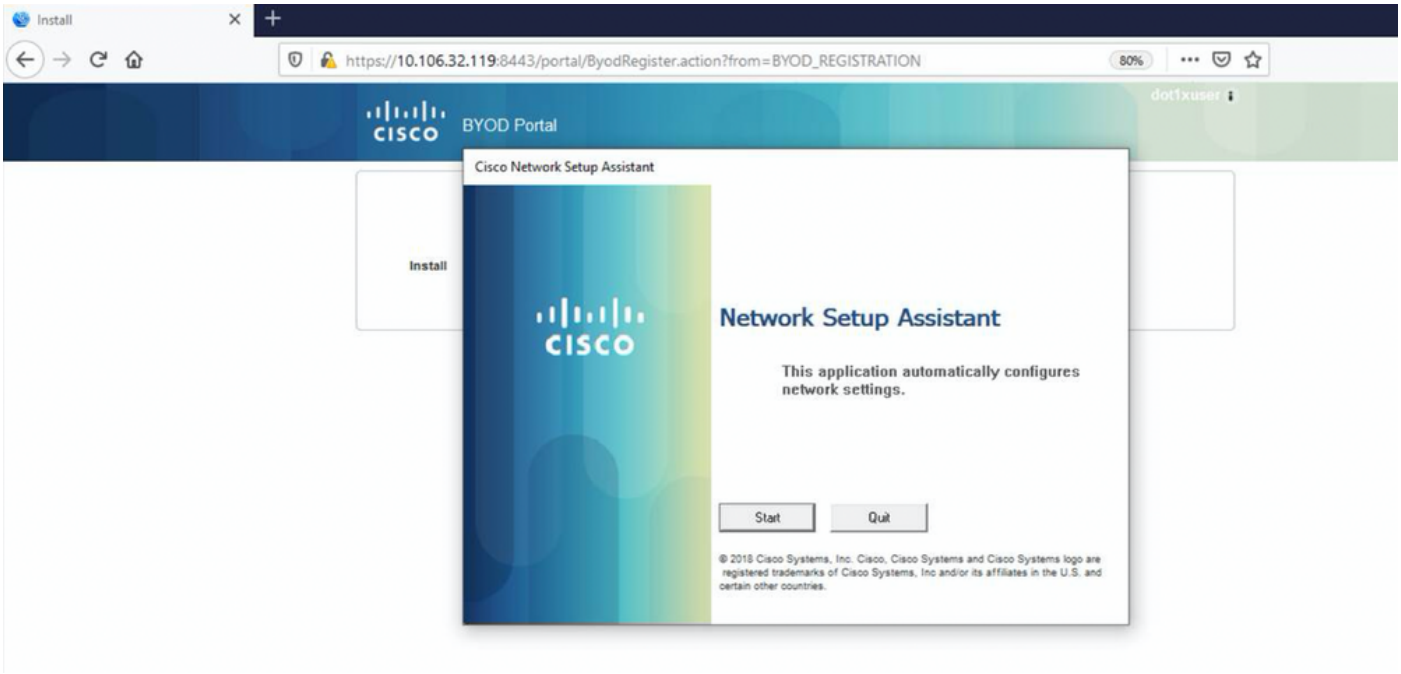
```
2020-12-02 05:44:01,936 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-3][]
guestaccess.flowmanager.step.guest.ByodWelcomeStepExecutor -:dot1xuser:- userAgent=Mozilla/5.0
(Windows NT 10.0; Win64; x64; rv:83.0) Gecko/20100101 Firefox/83.0, os=Windows 10 (All),
nspStatus=SUCCESS 2020-12-02 05:44:01,936 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-3][]
guestaccess.flowmanager.step.guest.ByodWelcomeStepExecutor -:dot1xuser:- NSP Downloadalble
Resource data=>, resource=DownloadableResourceInfo :WINDOWS_10_ALL
https://10.106.32.119:8443/auth/provisioning/download/a2b317ee-df5a-4bda-abc3-
e4ec38ee188c/WirelessNSP.xml?sessionId=0a6a21b20000009f5fc770c7&os=WINDOWS_10_ALL null null
https://10.106.32.119:8443/auth/provisioning/download/90a6dc9c-4aae-4431-a453-81141ec42d2d/ null
null https://10.106.32.119:8443/auth/provisioning/download/90a6dc9c-4aae-4431-a453-
81141ec42d2d/NetworkSetupAssistant.exe, coaType=NoCoa 2020-12-02 05:44:01,936 DEBUG [https-jsse-
```

nio-10.106.32.119-8443-exec-3][] cpm.guestaccess.flowmanager.utils.NSPProvAccess -:dot1xuser:- It is a WIN/MAC! 2020-12-02 05:44:01,936 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-3][] cpm.guestaccess.flowmanager.step.StepExecutor -:dot1xuser:- Returning next step =BYOD_REGISTRATION 2020-12-02 05:44:01,950 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-3][] cisco.ise.portalwebaction.controller.PortalStepController -:dot1xuser:- ++++ updatePortalState: PortalSession (e0d457d9-a346-4b6e-bcca-5cf29e12dacc) current state is ACTIVE and current step is BYOD_REGISTRATION 2020-12-02 05:44:01,950 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-3][] cisco.ise.portalwebaction.controller.PortalStepController -:dot1xuser:- nextStep: BYOD_REGISTRATION



디바이스 이름을 입력하고 등록을 클릭합니다.

2020-12-02 05:44:14,682 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][] cisco.ise.portalwebaction.actions.BasePortalAction -:dot1xuser:- Executing action ByodRegister via request /portal/ByodRegister.action Request Parameters: from=BYOD_REGISTRATION token=PZBMFBHX3FBPXT8QF98U717ILNOTD68D device.name=My-Device device.description= 2020-12-02 05:44:14,682 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][] cisco.ise.portal.actions.ByodRegisterAction -:dot1xuser:- executeAction... 2020-12-02 05:44:14,682 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][] cisco.ise.portalwebaction.actions.BasePortalAction -:dot1xuser:- Result from action, ByodRegister: success 2020-12-02 05:44:14,682 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][] cisco.ise.portalwebaction.actions.BasePortalAction -:dot1xuser:- Action ByodRegister Complete for request /portal/ByodRegister.action 2020-12-02 05:44:14,683 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][] cpm.guestaccess.apiservices.mydevices.MyDevicesServiceImpl -:dot1xuser:- Register Device : 50:3E:AA:E4:81:B6 username= dot1xuser idGroupID= aa13bb40-8bff-11e6-996c-525400b48521 authStoreGUID= 9273fe30-8c01-11e6-996c-525400b48521 nadAddress= 10.106.33.178 isSameDeviceRegistered = false 2020-12-02 05:44:14,900 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][] cpm.guestaccess.flowmanager.step.StepExecutor -:dot1xuser:- Returning next step =BYOD_INSTALL 2020-12-02 05:44:14,902 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][] cisco.ise.portalwebaction.controller.PortalStepController -:dot1xuser:- ++++ updatePortalState: PortalSession (e0d457d9-a346-4b6e-bcca-5cf29e12dacc) current state is ACTIVE and current step is BYOD_INSTALL 2020-12-02 05:44:01,954 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-3][] cisco.ise.portalwebaction.controller.PortalFlowInterceptor -:dot1xuser:- result: success 2020-12-02 05:44:14,969 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-10][] cisco.cpm.client.provisioning.StreamingServlet -::- StreamingServlet URI:/auth/provisioning/download/90a6dc9c-4aae-4431-a453-81141ec42d2d/NetworkSetupAssistant.exe

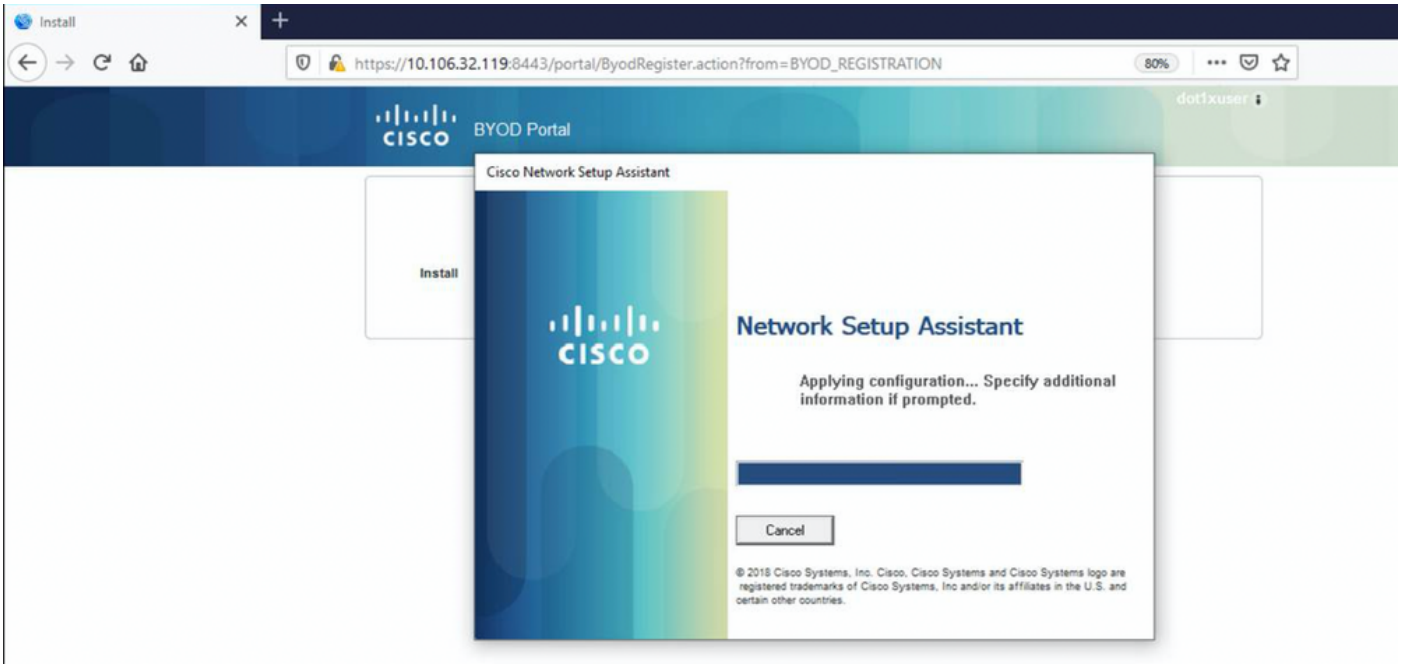


이제 사용자가 NSA에서 시작을 클릭하면 TCP 포트 8905에서 다운로드된 Cisco-ISE-NSP.xml에서 콘텐츠를 복사하는 클라이언트에 **spwProfile.xml**이라는 파일이 임시로 생성됩니다.

Guest.log -

```
2020-12-02 05:45:03,275 DEBUG [portal-http-service15][]
cisco.cpm.client.provisioning.StreamingServlet -::- StreamingServlet
URI:/auth/provisioning/download/a2b317ee-df5a-4bda-abc3-e4ec38ee188c/WirelessNSP.xml 2020-12-02
05:45:03,275 DEBUG [portal-http-service15][] cisco.cpm.client.provisioning.StreamingServlet -::-
Streaming to ip:10.106.33.167 file type: NativeSPProfile file name:WirelessNSP.xml 2020-12-02
05:45:03,308 DEBUG [portal-http-service15][] cisco.cpm.client.provisioning.StreamingServlet -::-
SPW profile :: 2020-12-02 05:45:03,308 DEBUG [portal-http-service15][]
cisco.cpm.client.provisioning.StreamingServlet -::-
```

spwProfile.**xml**에서 내용을 읽은 후, NSA는 네트워크 프로필을 구성하고 CSR을 생성한 다음 ISE에 전송하여 URL https://10.106.32.119:8443/auth/pkiclient.exe을 사용하여 인증서를 가져옵니다.



ise-psc.log-

```
2020-12-02 05:45:11,298 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][]
cisco.cpm.provisioning.cert.CertProvisioningFactory -::::- Found incoming certifcate request for
internal CA. Increasing Cert Request counter. 2020-12-02 05:45:11,331 DEBUG [https-jsse-nio-
10.106.32.119-8443-exec-1][] cisco.cpm.provisioning.cert.CertProvisioningFactory -::::- Key type
is RSA, retrieving ScepCertRequestProcessor for caProfileName=ISE Internal CA 2020-12-02
05:45:11,331 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][]
cisco.cpm.provisioning.cert.CertRequestValidator -::::- Session user has been set to = dot1xuser
2020-12-02 05:45:11,331 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][]
cisco.cpm.scep.util.ScepUtil -::::- Algorithm OID in CSR: 1.2.840.113549.1.1.1 2020-12-02
05:45:11,331 INFO [https-jsse-nio-10.106.32.119-8443-exec-1][]
com.cisco.cpm.scep.ScepCertRequestProcessor -::::- About to forward certificate request
C=IN,ST=Karnataka,L=bangalore,O=cisco,OU=tac,CN=dot1xuser with transaction id n@P~N6E to server
http://127.0.0.1:9444/caservice/scep 2020-12-02 05:45:11,332 DEBUG [https-jsse-nio-
10.106.32.119-8443-exec-1][] org.jscep.message.PkiMessageEncoder -::::- Encoding message:
org.jscep.message.PkcsReq@5c1649c2[transId=4d22d2e256a247a302e900ffa71c35d75610de67,messageType=
PKCS_REQ,senderNonce=Nonce
[7d9092a9fab204bd7600357e38309ee8],messageData=org.bouncycastle.pkcs.PKCS10CertificationRequest@
4662a5b0] 2020-12-02 05:45:11,332 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][]
org.jscep.message.PkcsPkiEnvelopeEncoder -::::- Encrypting session key using key belonging to
[issuer=CN=Certificate Services Endpoint Sub CA - isee30-primary;
serial=162233386180991315074159441535479499152] 2020-12-02 05:45:11,333 DEBUG [https-jsse-nio-
10.106.32.119-8443-exec-1][] org.jscep.message.PkiMessageEncoder -::::- Signing message using
key belonging to [issuer=CN=isee30-primary.anshsinh.local;
serial=126990069826611188711089996345828696375] 2020-12-02 05:45:11,333 DEBUG [https-jsse-nio-
10.106.32.119-8443-exec-1][] org.jscep.message.PkiMessageEncoder -::::- SignatureAlgorithm
SHA1withRSA 2020-12-02 05:45:11,334 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][]
org.jscep.message.PkiMessageEncoder -::::- Signing
org.bouncycastle.cms.CMSProcessableByteArray@5aa9dfcc content
```

ca-service.log -

```
2020-12-02 05:45:11,379 DEBUG [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67
0x67ee11d5 request] com.cisco.cpm.caservice.CrValidator -::::::- performing certificate request
validation: version [0] subject [C=IN,ST=Karnataka,L=bangalore,O=cisco,OU=tac,CN=dot1xuser] ---
output omitted--- 2020-12-02 05:45:11,379 DEBUG [CAService-Scep][scep job
4d22d2e256a247a302e900ffa71c35d75610de67 0x67ee11d5 request validation]
com.cisco.cpm.caservice.CrValidator -::::::- RDN value = dot1xuser 2020-12-02 05:45:11,379 DEBUG
[CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67ee11d5 request]
com.cisco.cpm.caservice.CrValidator -::::::- request validation result CA_OK
```

caservice-misc.log -

```
2020-12-02 05:45:11,380 DEBUG [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67
0x67ee11d5 request issuance] cisco.cpm.scep.util.ScepUtil -::::::- Algorithm OID in CSR:
1.2.840.113549.1.1.1 2020-12-02 05:45:11,380 DEBUG [CAService-Scep][scep job
4d22d2e256a247a302e900ffa71c35d75610de67 0x67ee11d5 request issuance]
com.cisco.cpm.scep.CertRequestInfo -::::::- Found challenge password with cert template ID.
```

caservice.log -

```
2020-12-02 05:45:11,380 DEBUG [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67
0x67ee11d5 request issuance] cisco.cpm.caservice.util.CaServiceUtil -::::::- Checking cache for
certificate template with ID: e2c32ce0-313d-11eb-b19e-e60300a810d5 2020-12-02 05:45:11,380 DEBUG
[CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67ee11d5 request issuance]
com.cisco.cpm.caservice.CertificateAuthority -::::::- CA SAN Extensions = GeneralNames: 1: 50-3E-
AA-E4-81-B6 2020-12-02 05:45:11,380 DEBUG [CAService-Scep][scep job
4d22d2e256a247a302e900ffa71c35d75610de67 0x67ee11d5 request issuance]
com.cisco.cpm.caservice.CertificateAuthority -::::::- CA : add SAN extension... 2020-12-02
05:45:11,380 DEBUG [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67ee11d5
request issuance] com.cisco.cpm.caservice.CertificateAuthority -::::::- CA Cert Template name =
```

```
BYOD_Certificate_template 2020-12-02 05:45:11,395 DEBUG [CAService-Scep][scep job
4d22d2e256a247a302e900ffa71c35d75610de67 0x67ee11d5 request issuance]
cisco.cpm.caservice.util.CaServiceUtil -::::::- Storing certificate via REST for serial number:
518fa73a4c654df282ffdb026080de8d 2020-12-02 05:45:11,395 INFO [CAService-Scep][scep job
4d22d2e256a247a302e900ffa71c35d75610de67 0x67ee11d5 request issuance]
com.cisco.cpm.caservice.CertificateAuthority -::::::- issuing Certificate Services Endpoint
Certificate: class [com.cisco.cpm.caservice.CaResultHolder] [1472377777]: result: [CA_OK]
subject [CN=dot1xuser, OU=tac, O=cisco, L=bangalore, ST=Karnataka, C=IN] version [3] serial
[0x518fa73a-4c654df2-82ffdb02-6080de8d] validity [after [2020-12-01T05:45:11+0000] before [2030-
11-27T07:35:10+0000]] keyUsages [ digitalSignature nonRepudiation keyEncipherment ]
```

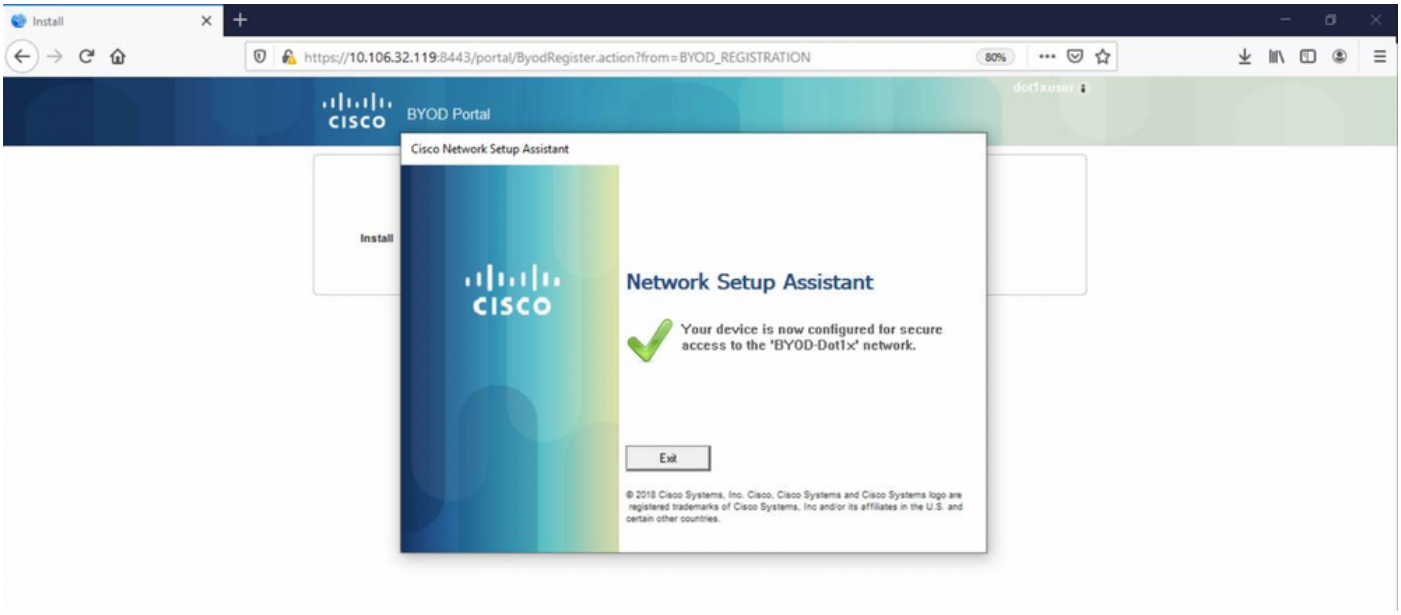
ise-psc.log -

```
2020-12-02 05:45:11,407 DEBUG [AsyncHttpClient-15-9][] org.jscep.message.PkiMessageDecoder -
::::- Verifying message using key belonging to 'CN=Certificate Services Endpoint RA - isee30-
primary'
```

caservice.log -

```
2020-12-02 05:45:11,570 DEBUG [Infra-CAServiceUtil-Thread][]
cisco.cpm.caservice.util.CaServiceUtil -::::::- Successfully stored endpoint certificate.
```

ise-psc.log -




```
2020-12-02 05:45:13,381 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-10][]
cisco.cpm.provisioning.cert.CertProvisioningFactory -::::- Performing doGetCertInitial found
Scep certificate processor for txn id n@P~N6E 2020-12-02 05:45:13,381 DEBUG [https-jsse-nio-
10.106.32.119-8443-exec-10][] com.cisco.cpm.scep.ScepCertRequestProcessor -::::- Polling
C=IN,ST=Karnataka,L=bangalore,O=cisco,OU=tac,CN=dot1xuser for certificate request n@P~N6E with
id {} 2020-12-02 05:45:13,385 INFO [https-jsse-nio-10.106.32.119-8443-exec-10][]
com.cisco.cpm.scep.ScepCertRequestProcessor -::::- Certificate request Complete for
C=IN,ST=Karnataka,L=bangalore,O=cisco,OU=tac,CN=dot1xuser Trx Idn@P~N6E 2020-12-02 05:45:13,596
DEBUG [https-jsse-nio-10.106.32.119-8443-exec-10][]
cisco.cpm.provisioning.cert.CertProvisioningFactory -::::- BYODStatus:COMPLETE_OTA_NSP
```

인증서 설치 후 클라이언트는 EAP-TLS를 사용하여 다른 인증을 시작하고 전체 액세스를 가져옵니다.

prrt-server.log -

```
Eap,2020-12-02 05:46:57,175,INFO ,0x7f433e6b8700,cntx=0008591342,sesn=isee30-
primary/392215758/701,CPMSessionID=0a6a21b20000009f5fc770c7,CallingStationID=50-3e-aa-e4-81-
b6,EAP: Recv EAP packet, code=Response, identifier=64, type=EAP-TLS, length=166
,EapParser.cpp:150 Radius,2020-12-02
05:46:57,435,DEBUG,0x7f433e3b5700,cntx=0008591362,sesn=isee30-
primary/392215758/701,CPMSessionID=0a6a21b20000009f5fc770c7,user=dot1xuser,CallingStationID=50-
3e-aa-e4-81-b6,RADIUS PACKET:: Code=2(AccessAccept) Identifier=5 Length=231 [1] User-Name -
value: [dot1xuser] [25] Class - value: [****] [79] EAP-Message - value: [E [80] Message-
Authenticator - value: [Ù(ØyËöžö|kÔ,¸}] [26] MS-MPPE-Send-Key - value: [****] [26] MS-MPPE-Recv-
Key - value: [****] ,RADIUSHandler.cpp:2216
```

클라이언트 로그(spw 로그)

클라이언트가 프로파일을 다운로드하기 시작합니다.

```
[Mon Nov 30 03:34:27 2020] Downloading profile configuration... [Mon Nov 30 03:34:27 2020]
Discovering ISE using default gateway [Mon Nov 30 03:34:27 2020] Identifying wired and wireless
network interfaces, total active interfaces: 1 [Mon Nov 30 03:34:27 2020] Network interface -
mac:50-3E-AA-E4-81-B6, name: Wi-Fi 2, type: unknown [Mon Nov 30 03:34:27 2020] Identified
default gateway: 10.106.33.1 [Mon Nov 30 03:34:27 2020] Identified default gateway: 10.106.33.1,
mac address: 50-3E-AA-E4-81-B6 [Mon Nov 30 03:34:27 2020] DiscoverISE - start [Mon Nov 30
03:34:27 2020] DiscoverISE input parameter : strUrl [http://10.106.33.1/auth/discovery] [Mon Nov
30 03:34:27 2020] [HTTPConnection] CrackUrl: host = 10.106.33.1, path = /auth/discovery, user =
, port = 80, scheme = 3, flags = 0 [Mon Nov 30 03:34:27 2020] [HTTPConnection] HttpSendRequest:
header = Accept: */* headerLength = 12 data = dataLength = 0 [Mon Nov 30 03:34:27 2020] HTTP
Response header: [HTTP/1.1 200 OK Location:
https://10.106.32.119:8443/portal/gateway?sessionId=0a6a21b20000009c5fc4fb5e&portal=7f8ac563-
3304-4f25-845d-
be9faac3c44f&action=nsp&token=29354d43962243bcb72193cbf9dc3260&redirect=10.106.33.1/auth/discove
ry [Mon Nov 30 03:34:36 2020] [HTTPConnection] CrackUrl: host = 10.106.32.119, path =
/auth/provisioning/download/a2b317ee-df5a-4bda-abc3-
e4ec38ee188c/WirelessNSP.xml?sessionId=0a6a21b20000009c5fc4fb5e&os=WINDOWS_10_ALL, user = , port
= 8443, scheme = 4, flags = 8388608 Mon Nov 30 03:34:36 2020] parsing wireless connection
setting [Mon Nov 30 03:34:36 2020] Certificate template: [keytype:RSA, keysize:2048,
subject:OU=tac;O=cisco;L=bangalore;ST=Karnataka;C=IN, SAN:MAC] [Mon Nov 30 03:34:36 2020] set
ChallengePwd
```

클라이언트 WLAN 서비스가 실행 중인지 확인합니다.

```
[Mon Nov 30 03:34:36 2020] WirelessProfile::StartWLanSvc - Start [Mon Nov 30 03:34:36 2020]
Wlansvc service is in Auto mode ... [Mon Nov 30 03:34:36 2020] Wlansvc is running in auto
mode... [Mon Nov 30 03:34:36 2020] WirelessProfile::StartWLanSvc - End [Mon Nov 30 03:34:36
2020] Wireless interface 1 - Desc: [TP-Link Wireless USB Adapter], Guid: [{65E78DDE-E3F1-4640-
906B-15215F986CAA}]... [Mon Nov 30 03:34:36 2020] Wireless interface - Mac address: 50-3E-AA-E4-
81-B6 [Mon Nov 30 03:34:36 2020] Identifying wired and wireless interfaces... [Mon Nov 30
03:34:36 2020] Found wireless interface - [ name:Wi-Fi 2, mac address:50-3E-AA-E4-81-B6] [Mon
Nov 30 03:34:36 2020] Wireless interface [Wi-Fi 2] will be configured... [Mon Nov 30 03:34:37
2020] Host - [ name:DESKTOP-965F94U, mac addresses:50-3E-AA-E4-81-B6]
```

클라이언트가 프로파일 적용을 시작합니다.

```
[Mon Nov 30 03:34:37 2020] ApplyProfile - Start... [Mon Nov 30 03:34:37 2020] User Id:
dot1xuser, sessionid: 0a6a21b20000009c5fc4fb5e, Mac: 50-3E-AA-E4-81-B6, profile: WirelessNSP
[Mon Nov 30 03:34:37 2020] number of wireless connections to configure: 1 [Mon Nov 30 03:34:37
2020] starting configuration for SSID : [BYOD-Dot1x] [Mon Nov 30 03:34:37 2020] applying
certificate for ssid [BYOD-Dot1x]
```

클라이언트 설치 인증서

```
[Mon Nov 30 03:34:37 2020] ApplyCert - Start... [Mon Nov 30 03:34:37 2020] using ChallengePwd
```

[Mon Nov 30 03:34:37 2020] creating certificate with subject = dot1xuser and subjectSuffix = OU=tac;O=cisco;L=bangalore;ST=Karnataka;C=IN [Mon Nov 30 03:34:38 2020] Self signed certificate [Mon Nov 30 03:34:44 2020] Installed [isee30-primary.anshsinh.local, hash: 5b a2 08 1e 17 cb 73 5f ba 5b 9f a2 2d 3b fc d2 86 0d a5 9b] as rootCA [Mon Nov 30 03:34:44 2020] Installed CA cert for authMode machineOrUser - Success Certificate is downloaded . Omitted for brevity - [Mon Nov 30 03:34:50 2020] creating response file name C:\Users\admin\AppData\Local\Temp\response.cer [Mon Nov 30 03:34:50 2020] Certificate issued - successfully [Mon Nov 30 03:34:50 2020] ScepWrapper::InstallCert start [Mon Nov 30 03:34:50 2020] ScepWrapper::InstallCert: Reading scep response file [C:\Users\admin\AppData\Local\Temp\response.cer]. [Mon Nov 30 03:34:51 2020] ScepWrapper::InstallCert GetCertHash -- return val 1 [Mon Nov 30 03:34:51 2020] ScepWrapper::InstallCert end [Mon Nov 30 03:34:51 2020] ApplyCert - End... [Mon Nov 30 03:34:51 2020] applied user certificate using template id e2c32ce0-313d-11eb-b19e-e60300a810d5

ISE에서 무선 프로파일 구성

[Mon Nov 30 03:34:51 2020] Configuring wireless profiles... [Mon Nov 30 03:34:51 2020] Configuring ssid [BYOD-Dot1x] [Mon Nov 30 03:34:51 2020] WirelessProfile::SetWirelessProfile - Start [Mon Nov 30 03:34:51 2020] TLS - TrustedRootCA Hash: [5b a2 08 1e 17 cb 73 5f ba 5b 9f a2 2d 3b fc d2 86 0d a5 9b]

프로필

Wireless interface succesfully initiated, continuing to configure SSID [Mon Nov 30 03:34:51 2020] Currently connected to SSID: [BYOD-Dot1x] [Mon Nov 30 03:34:51 2020] Wireless profile: [BYOD-Dot1x] configured successfully [Mon Nov 30 03:34:51 2020] Connect to SSID [Mon Nov 30 03:34:51 2020] Successfully connected profile: [BYOD-Dot1x] [Mon Nov 30 03:34:51 2020] WirelessProfile::SetWirelessProfile. - End [Mon Nov 30 03:35:21 2020] WirelessProfile::IsSingleSSID - Start [Mon Nov 30 03:35:21 2020] Currently connected to SSID: [BYOD-Dot1x], profile ssid: [BYOD-Dot1x], Single SSID [Mon Nov 30 03:35:21 2020] WirelessProfile::IsSingleSSID - End [Mon Nov 30 03:36:07 2020] Device configured successfully.