Catalyst 9800 WLC 및 ISE에서 CWA(Central Web Authentication) 구성

목차

소개

이 문서에서는 Catalyst 9800 WLC 및 ISE에서 CWA 무선 LAN을 구성하는 방법에 대해 설명합니다
.

사전 요구 사항

요구 사항

9800 WLC(Wireless LAN Controller) 컨피그레이션에 대해 알고 있는 것이 좋습니다.

사용되는 구성 요소

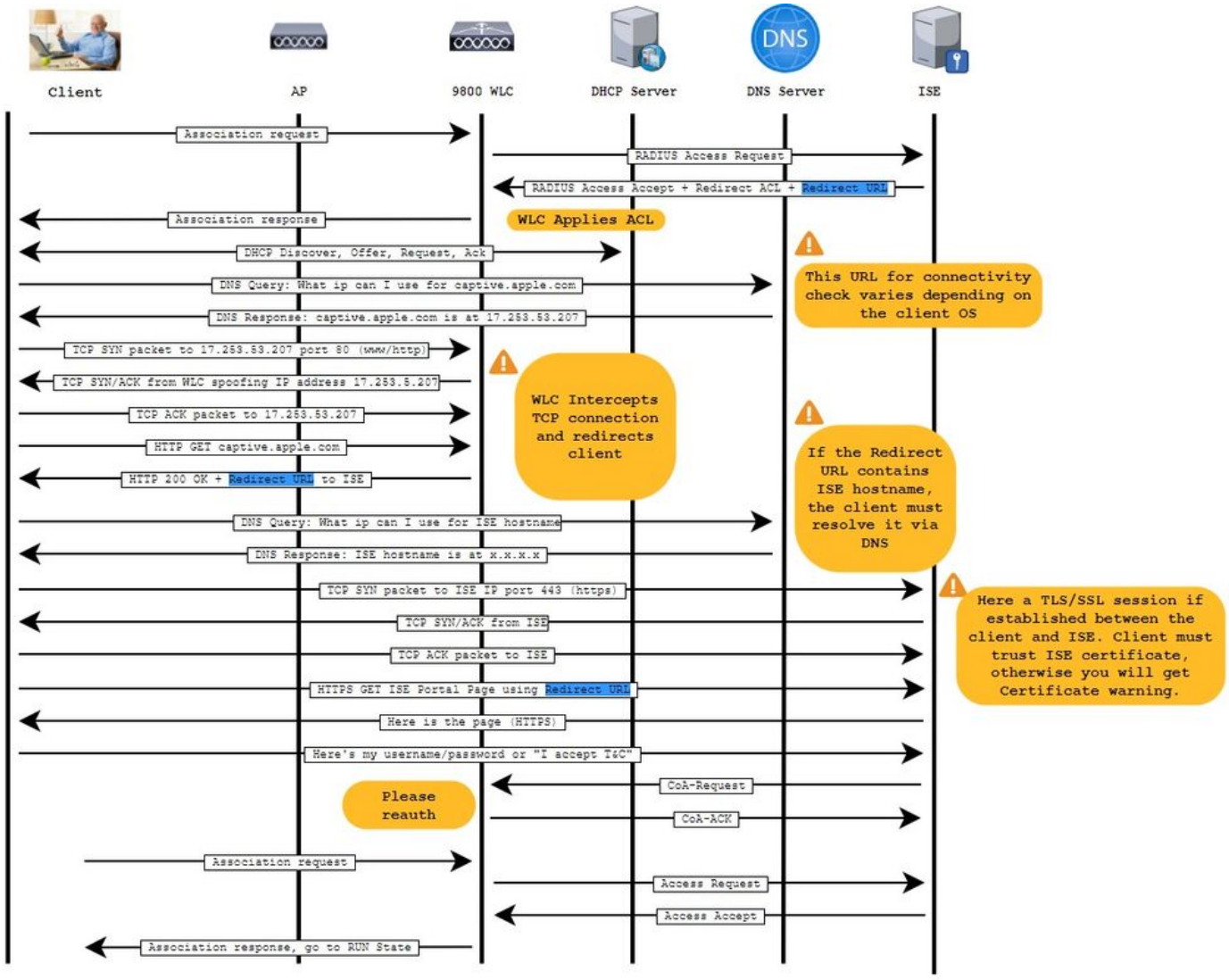
이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 9800 WLC Cisco IOS® XE Gibraltar v17.6.x
- ISE(Identity Service Engine) v3.0

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.

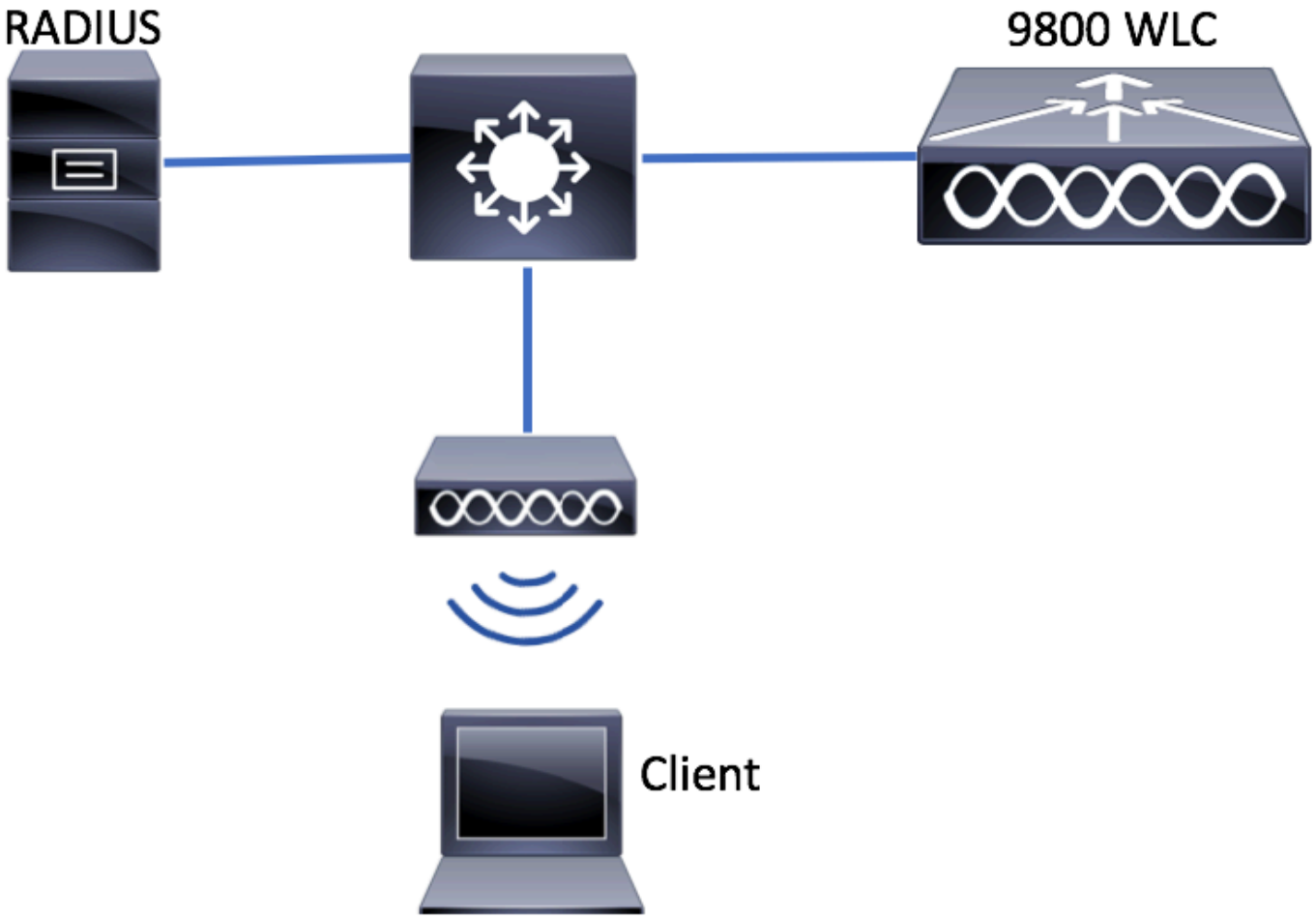
배경 정보

CWA 프로세스는 Apple 디바이스의 CWA 프로세스를 예로 볼 수 있는 여기에 나와 있습니다.



구성

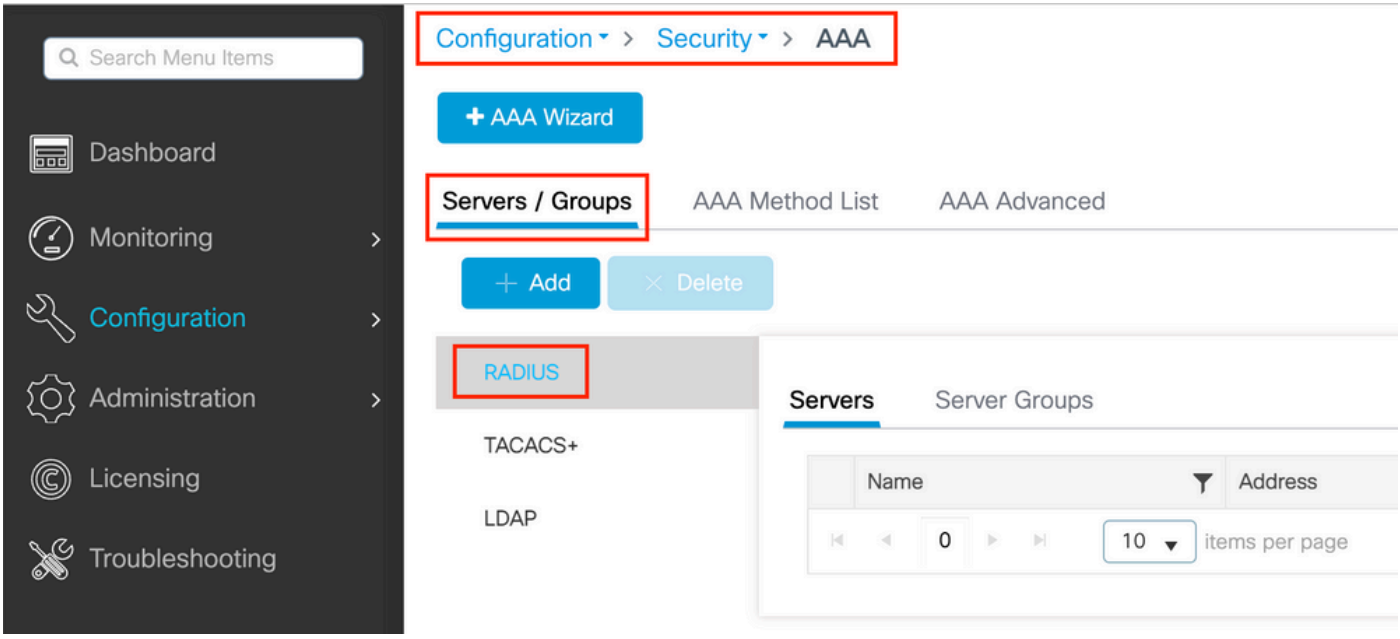
네트워크 다이어그램



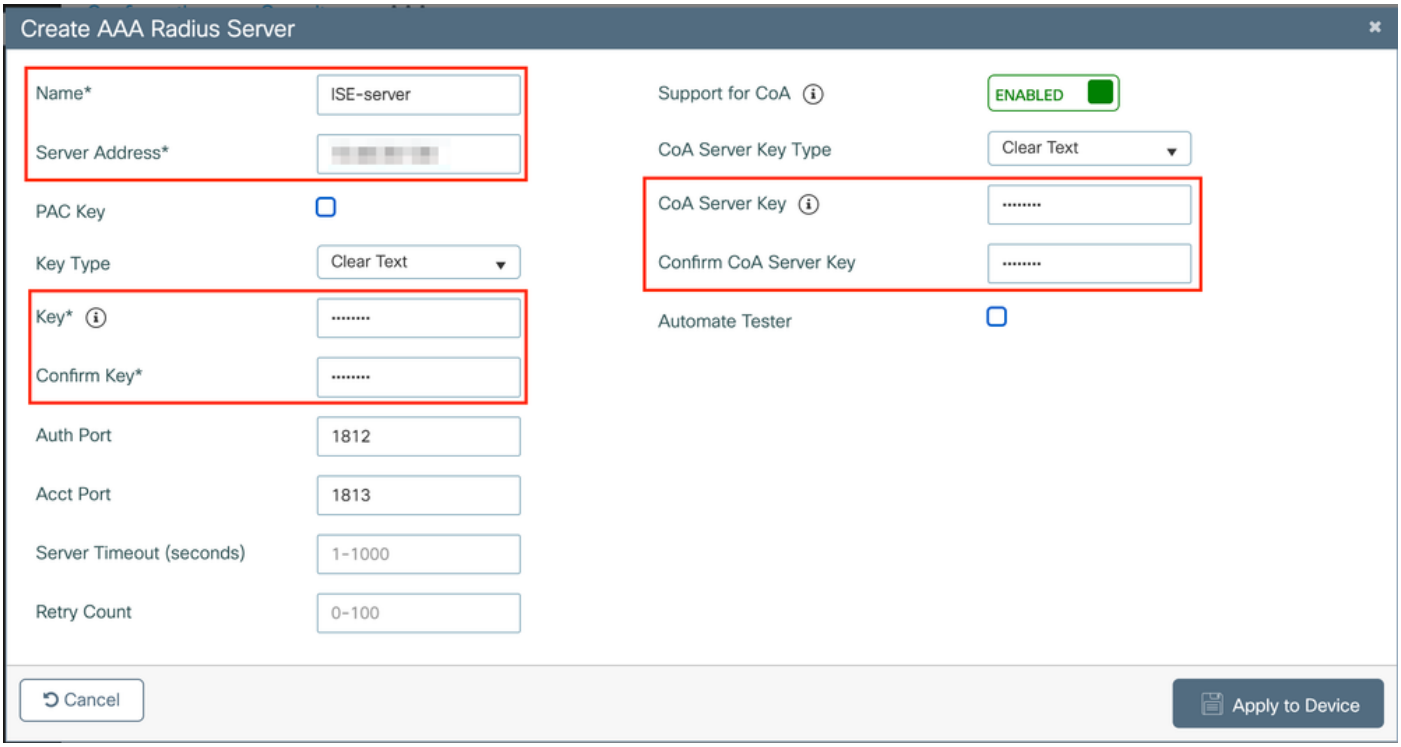
9800 WLC의 AAA 구성

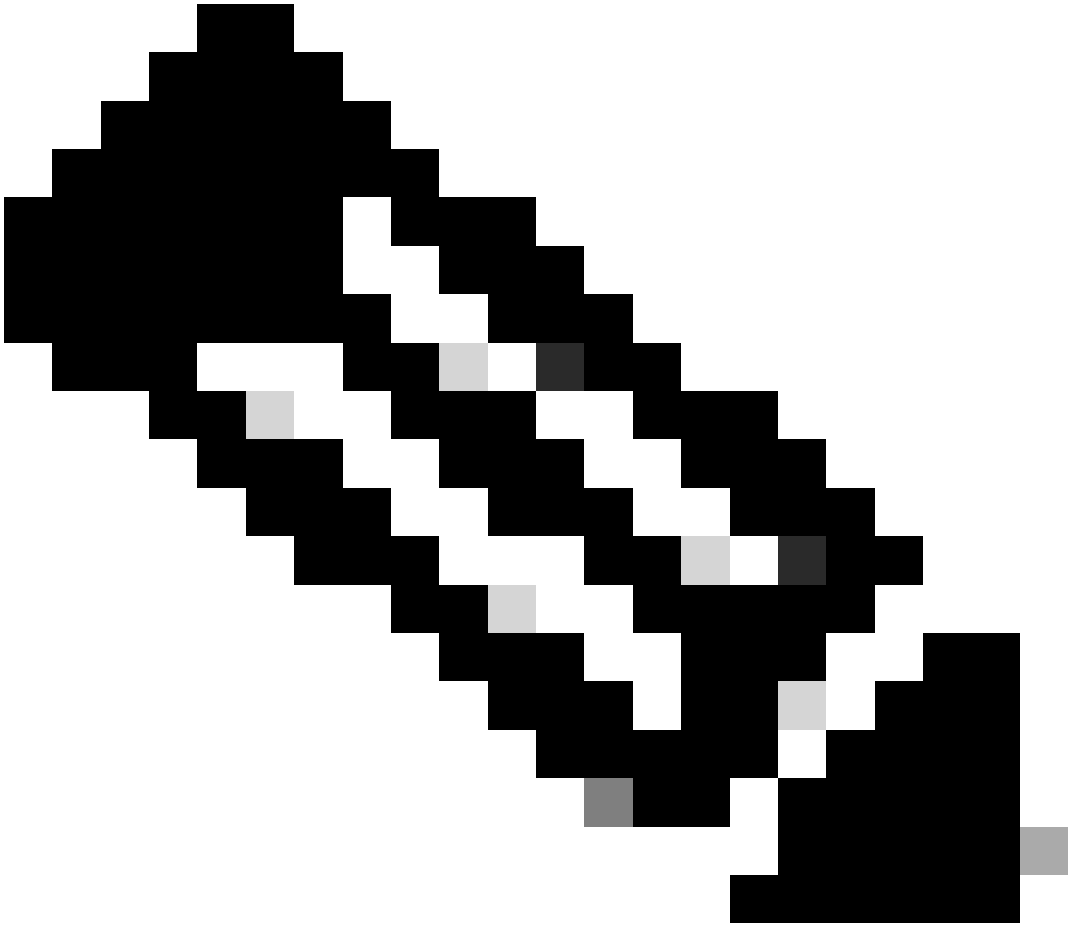
1단계. 9800 WLC 컨피그레이션에 ISE 서버를 추가합니다.

그림과 같이 Configuration > Security > AAA > Servers/Groups > RADIUS > Servers > + Add RADIUS 서버 정보를 찾아 입력합니다.



나중에 중앙 웹 인증(또는 CoA를 필요로 하는 모든 종류의 보안)을 사용하려는 경우 CoA 지원이 활성화되어 있는지 확인하십시오.

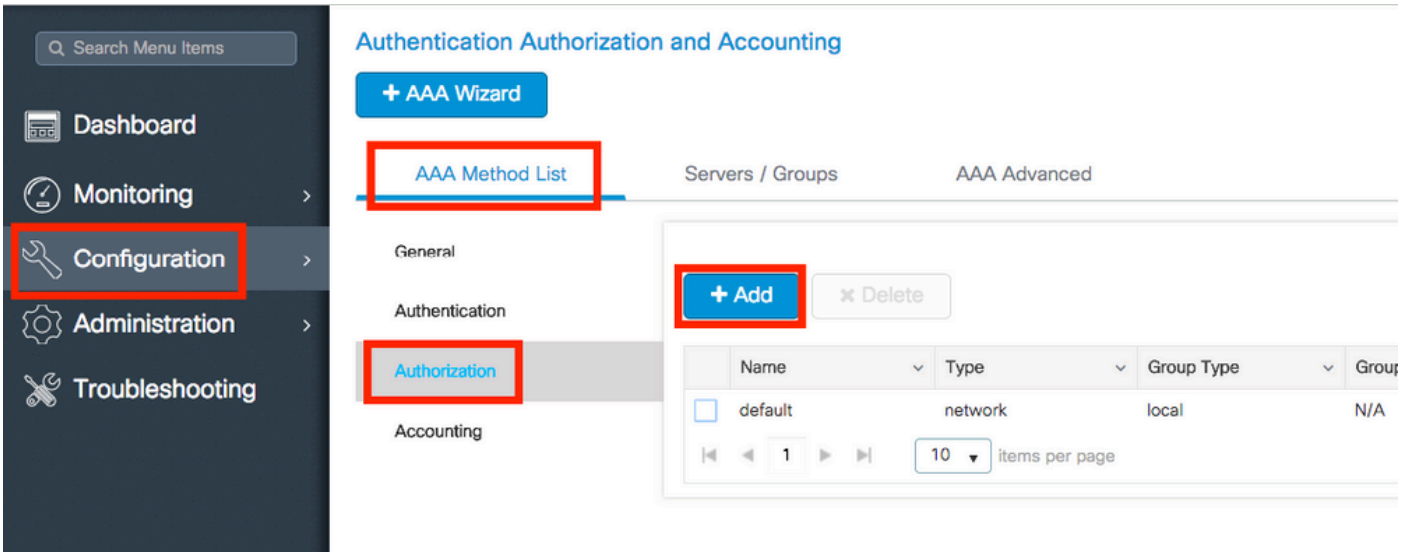


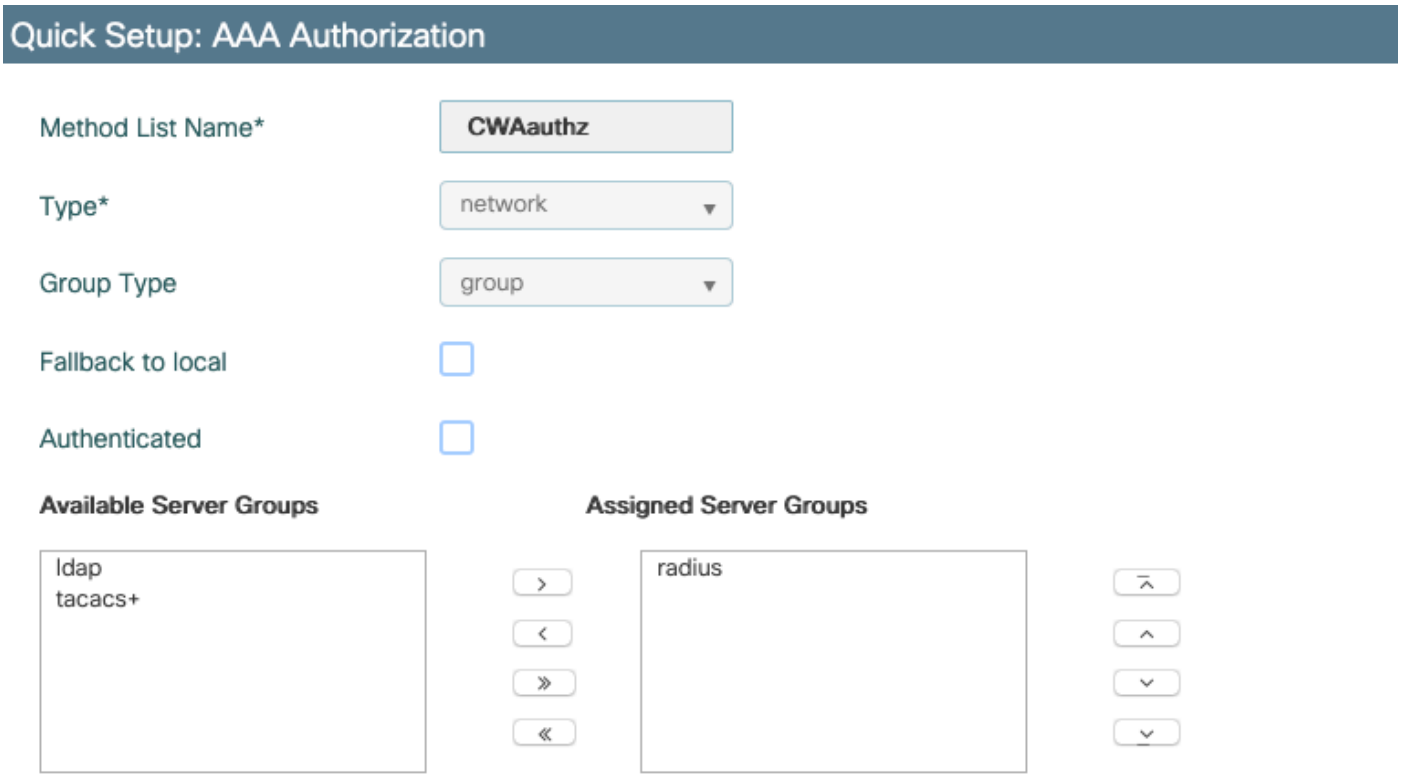


참고: 버전 17.4.X 이상에서는 RADIUS 서버를 구성할 때 CoA 서버 키도 구성해야 합니다. 공유 암호와 동일한 키를 사용합니다(ISE에서는 기본적으로 동일함). RADIUS 서버가 구성한 공유 암호가 아닌 CoA에 대해 다른 키를 선택적으로 구성하는 것이 목적입니다. Cisco IOS XE 17.3에서는 웹 UI에서 CoA 키와 동일한 공유 암호를 사용했습니다.

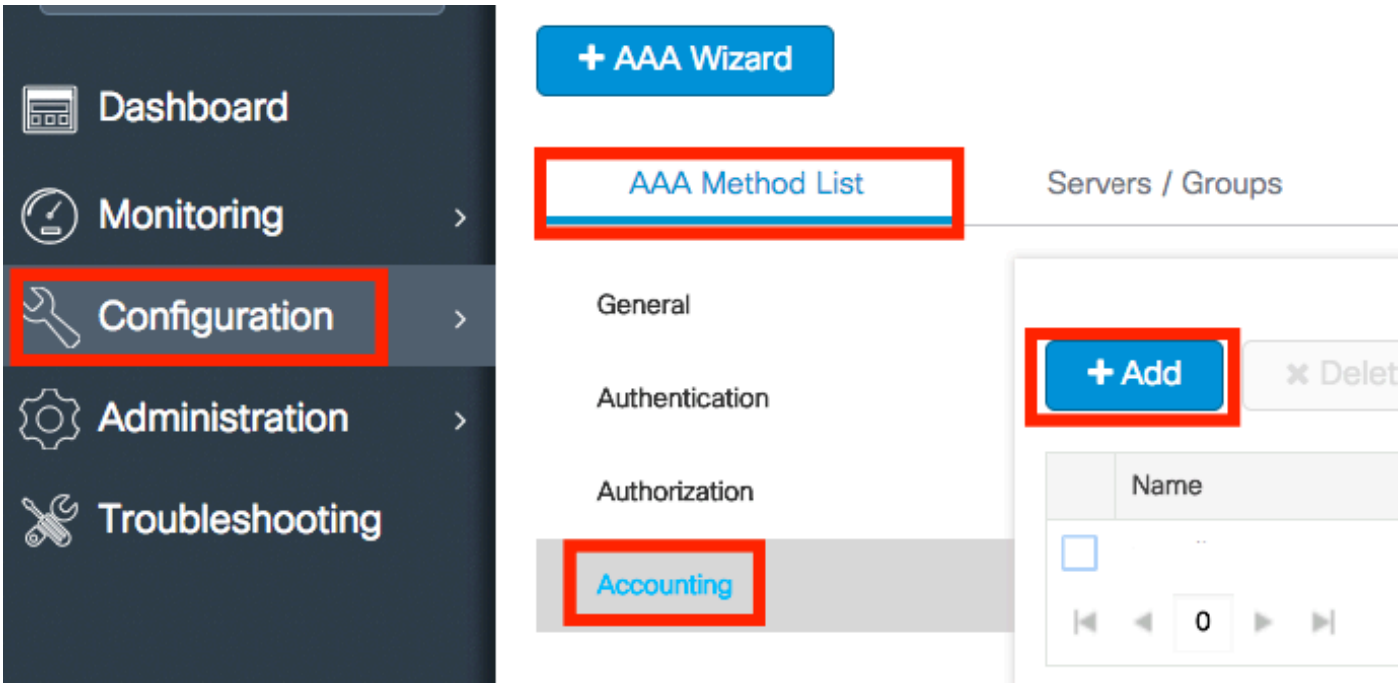
2단계. 권한 부여 방법 목록을 만듭니다.

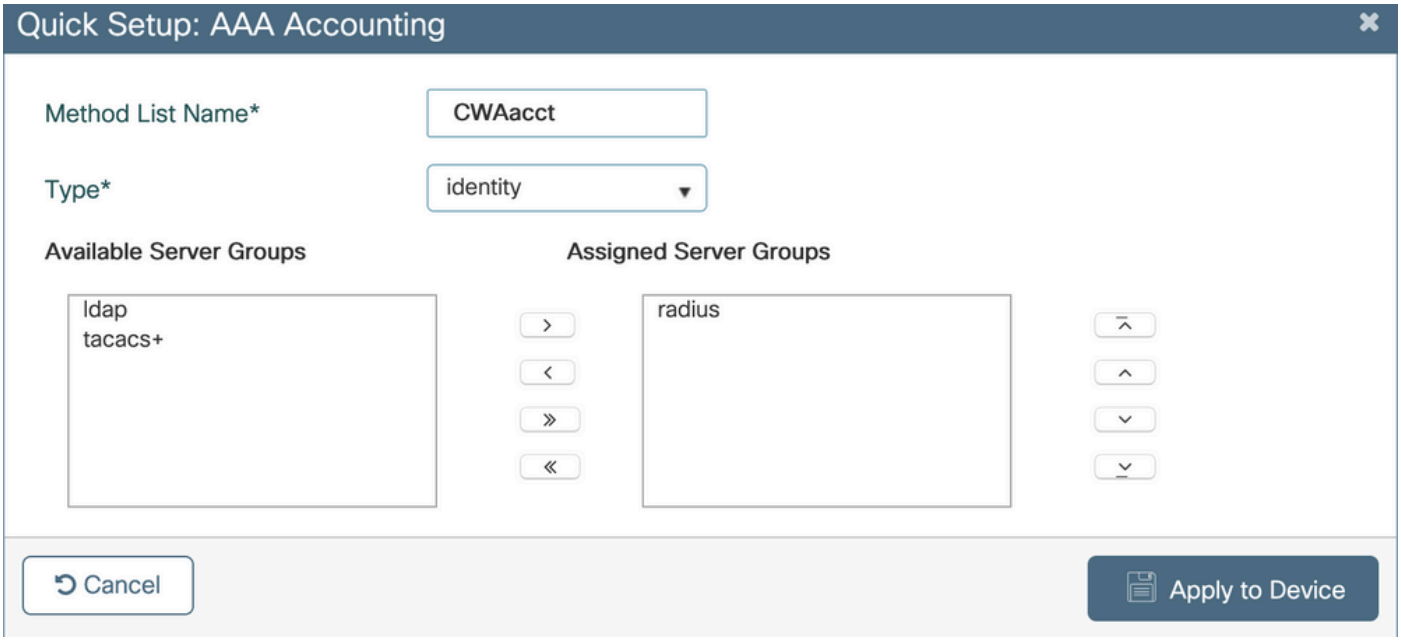
이미지에 Configuration > Security > AAA > AAA Method List > Authorization > + Add 표시된 대로 이동합니다.





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

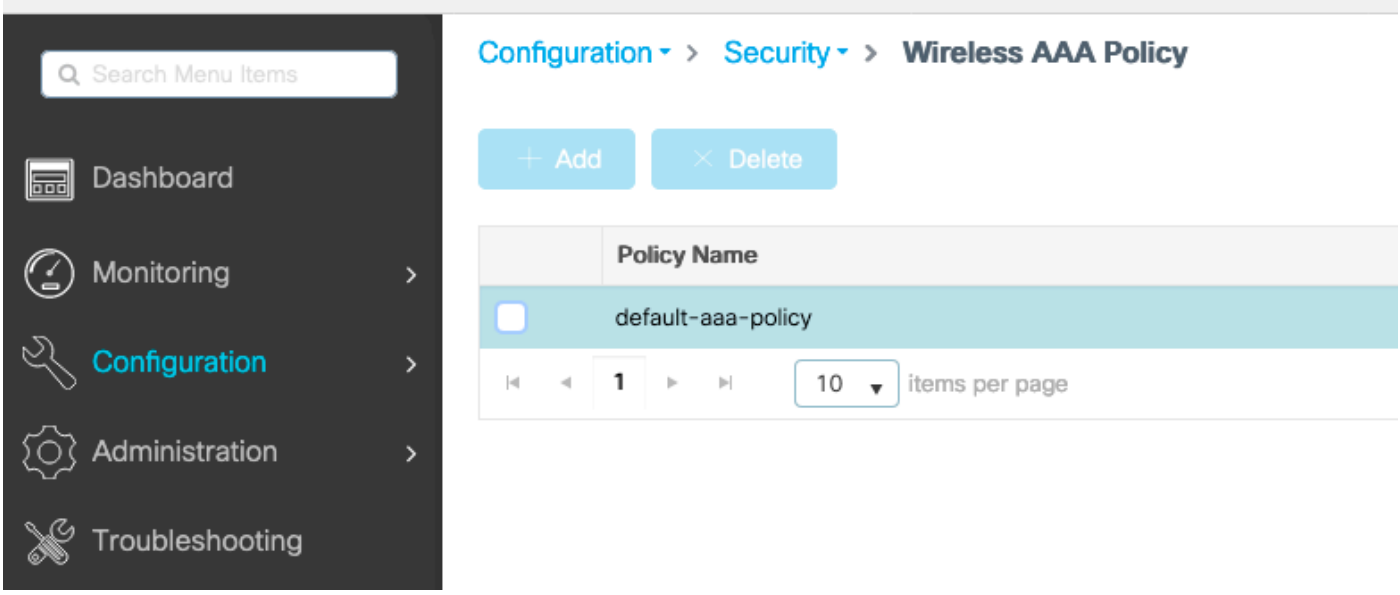




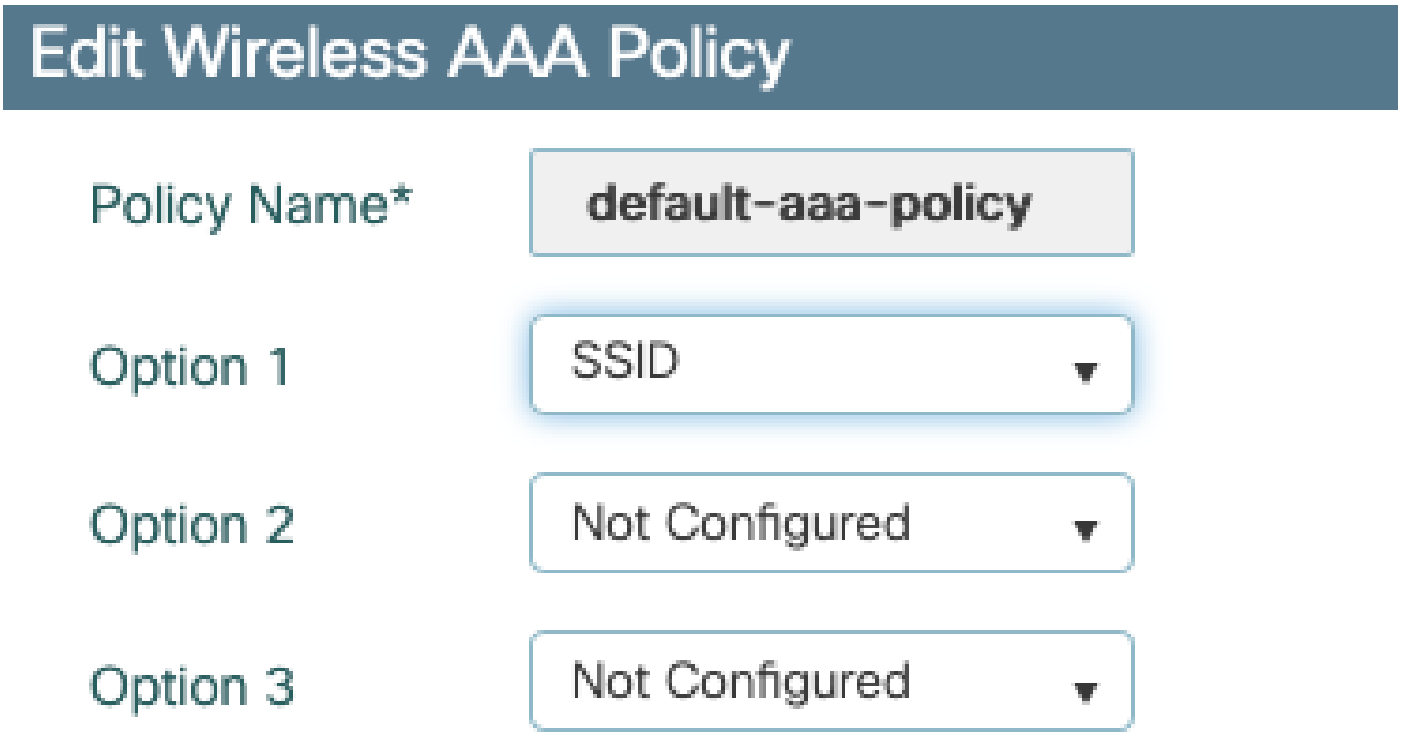
참고: Cisco 버그 ID CSCvh03827로 인해 Cisco IOS XE CLI 컨피그레이션에서 RADIUS 서버를 로드 밸런싱하기로 결정하면 CWA가 작동하지 않습니다. 외부 부하 분산 장치의 사용도 좋습니다. 그러나 calling-station-id RADIUS 특성을 사용하여 로드 밸런서가 클라이언트 단위로 작동하는지 확인합니다. UDP 소스 포트에 의존하는 것은 9800의 RADIUS 요청 밸런싱에 대해 지원되는 메커니즘이 아닙니다.

4단계. (선택 사항) SSID 이름을 Called-station-id 특성으로 전송하도록 AAA 정책을 정의할 수 있습니다. 이 특성은 이 프로세스의 나중에 ISE에서 이 조건을 활용하려는 경우 유용할 수 있습니다.

기본 AAA 정책으로 이동하여Configuration > Security > Wireless AAA Policy 편집하거나 새 정책을 만듭니다.



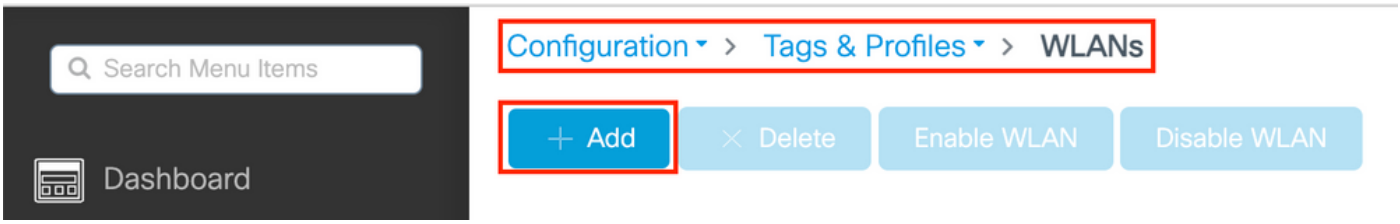
옵션 1로 선택할 수SSID 있습니다. SSID만 선택하는 경우에도 수신 스테이션 ID는 SSID 이름에 AP MAC 주소를 계속 추가합니다.



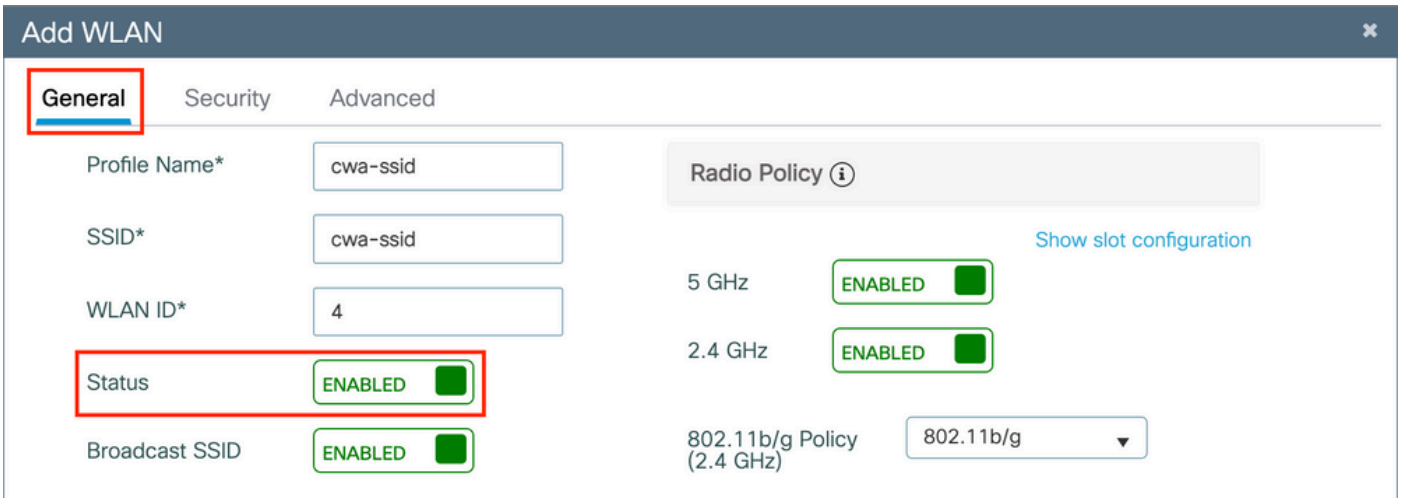
WLAN 구성

1단계. WLAN을 생성합니다.

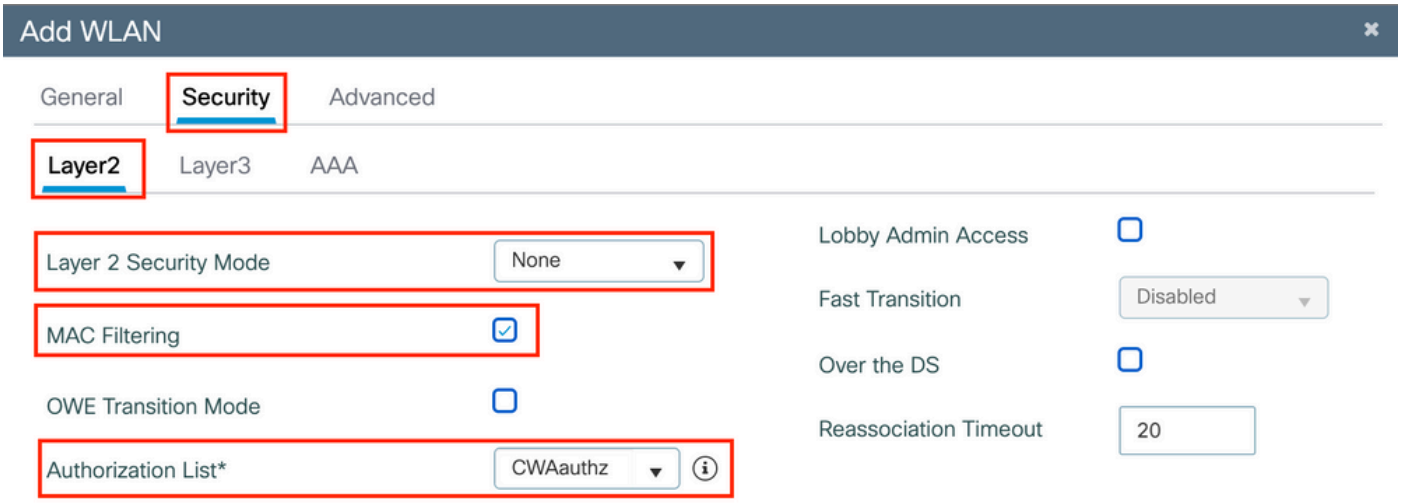
필요에 따라 Configuration > Tags & Profiles > WLANs > + Add 네트워크를 탐색하고 구성합니다.



2단계. WLAN 일반 정보를 입력합니다.



3단계. 탭으로 Security 이동하여 필요한 보안 방법을 선택합니다. 이 경우 'MAC 필터링' 및 AAA 권한 부여 목록(AAA Configuration 섹션 2단계에서 생성한)만 필요합니다.



CLI:

```
#config t
(config)#wlan cwa-ssid 4 cwa-ssid
(config-wlan)#mac-filtering CWAauthz
(config-wlan)#no security ft adaptive
(config-wlan)#no security wpa
(config-wlan)#no security wpa wpa2
```

(config-wlan)#no security wpa wpa2 ciphers aes
(config-wlan)#no security wpa akm dot1x
(config-wlan)#no shutdown

정책 프로파일 구성

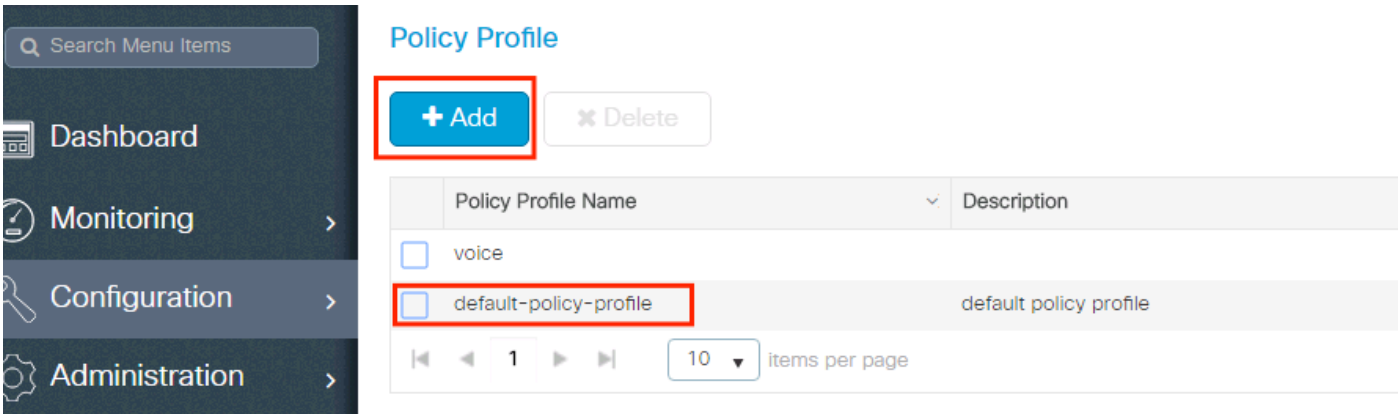
정책 프로필 내에서 다른 설정(예: ACL(Access Controls List), QoS(Quality of Service), Mobility Anchor, Timers 등) 중에서 VLAN을 할당할 클라이언트를 결정할 수 있습니다.

기본 정책 프로파일을 사용하거나 새 프로파일을 생성할 수 있습니다.

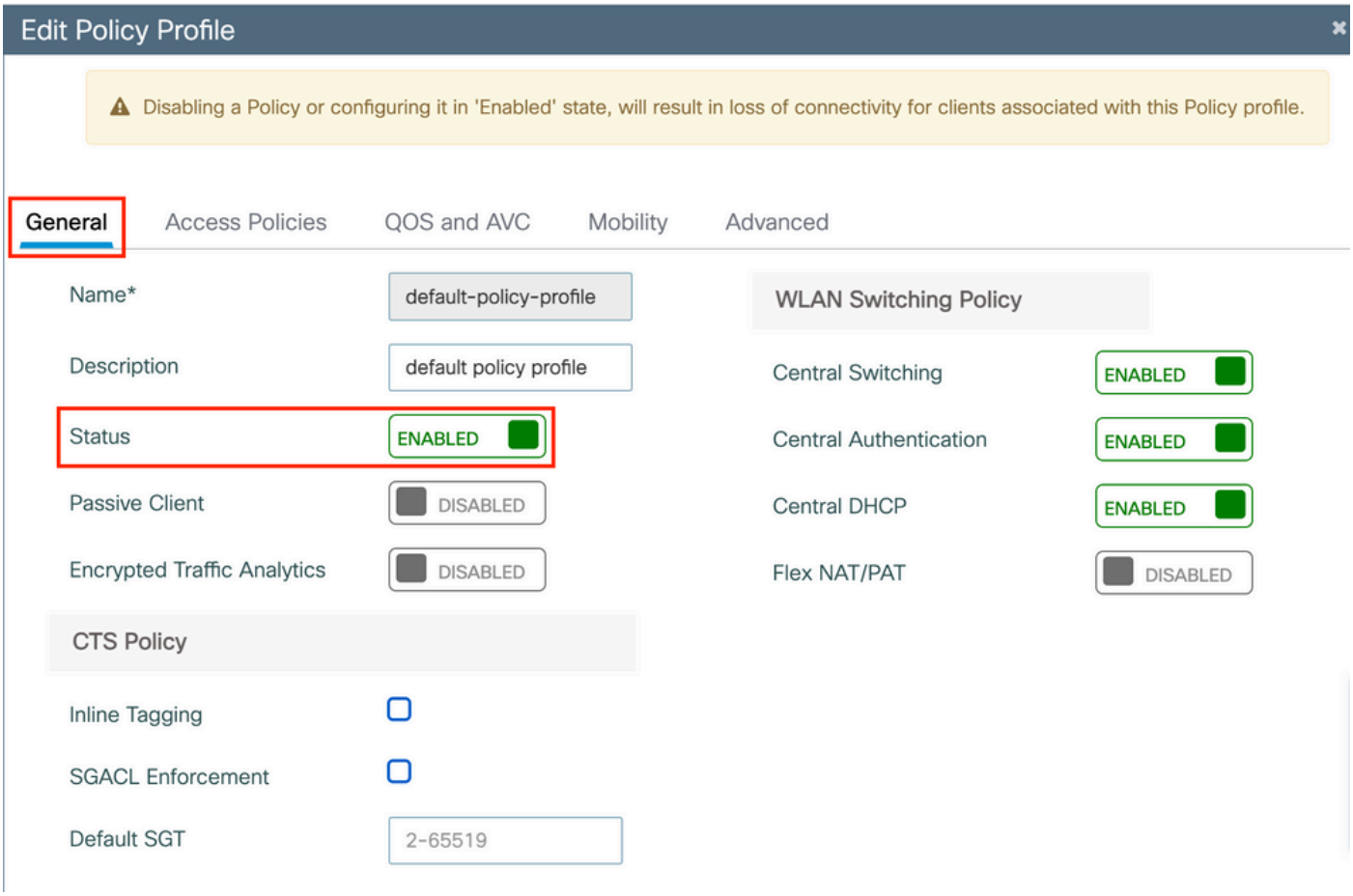
GUI:

1단계. 새 를 Policy Profile 만듭니다.

로 Configuration > Tags & Profiles > Policy 이동하여 를 구성하거나 새 default-policy-profile 를 만듭니다.

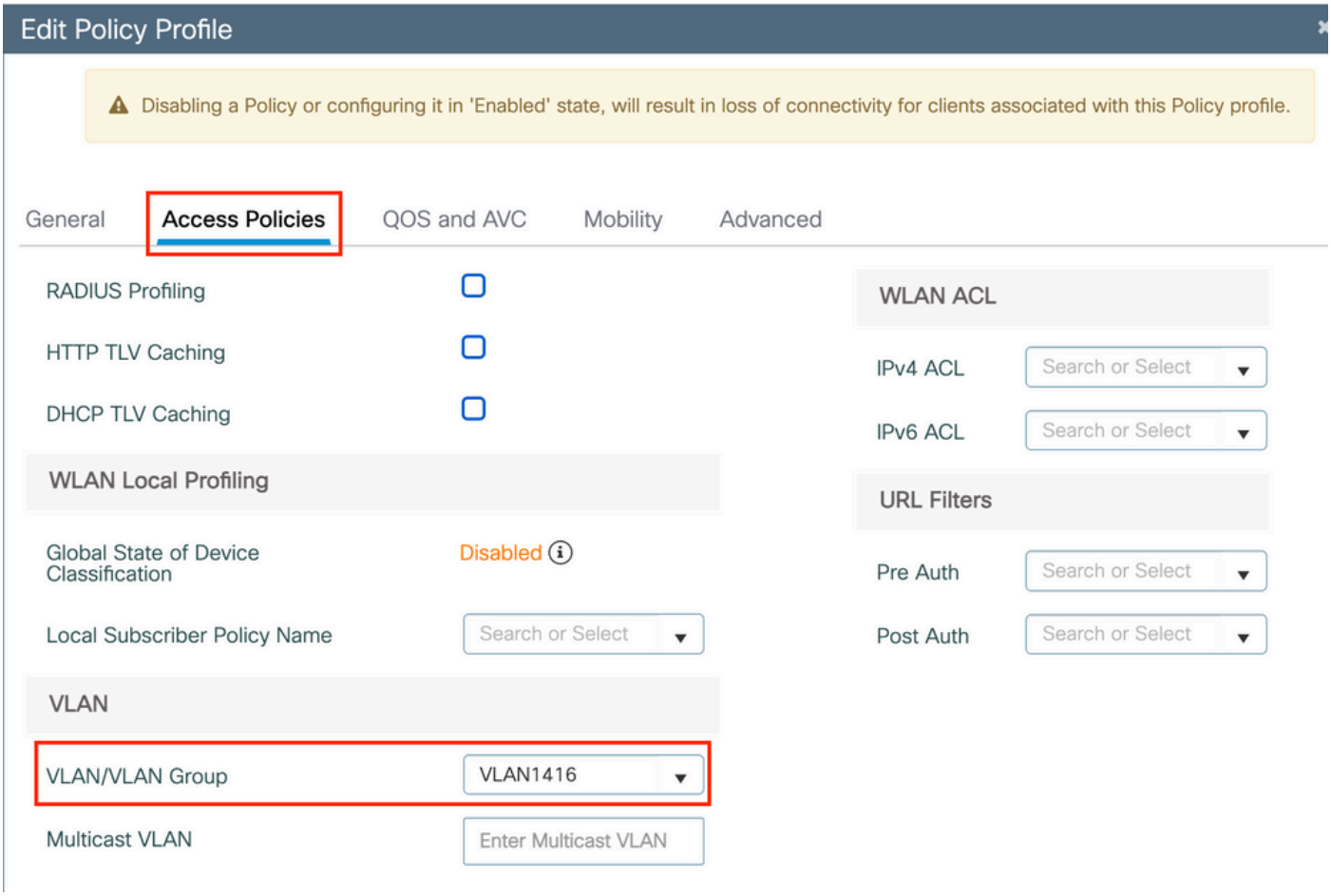


프로파일이 활성화되어야 합니다.

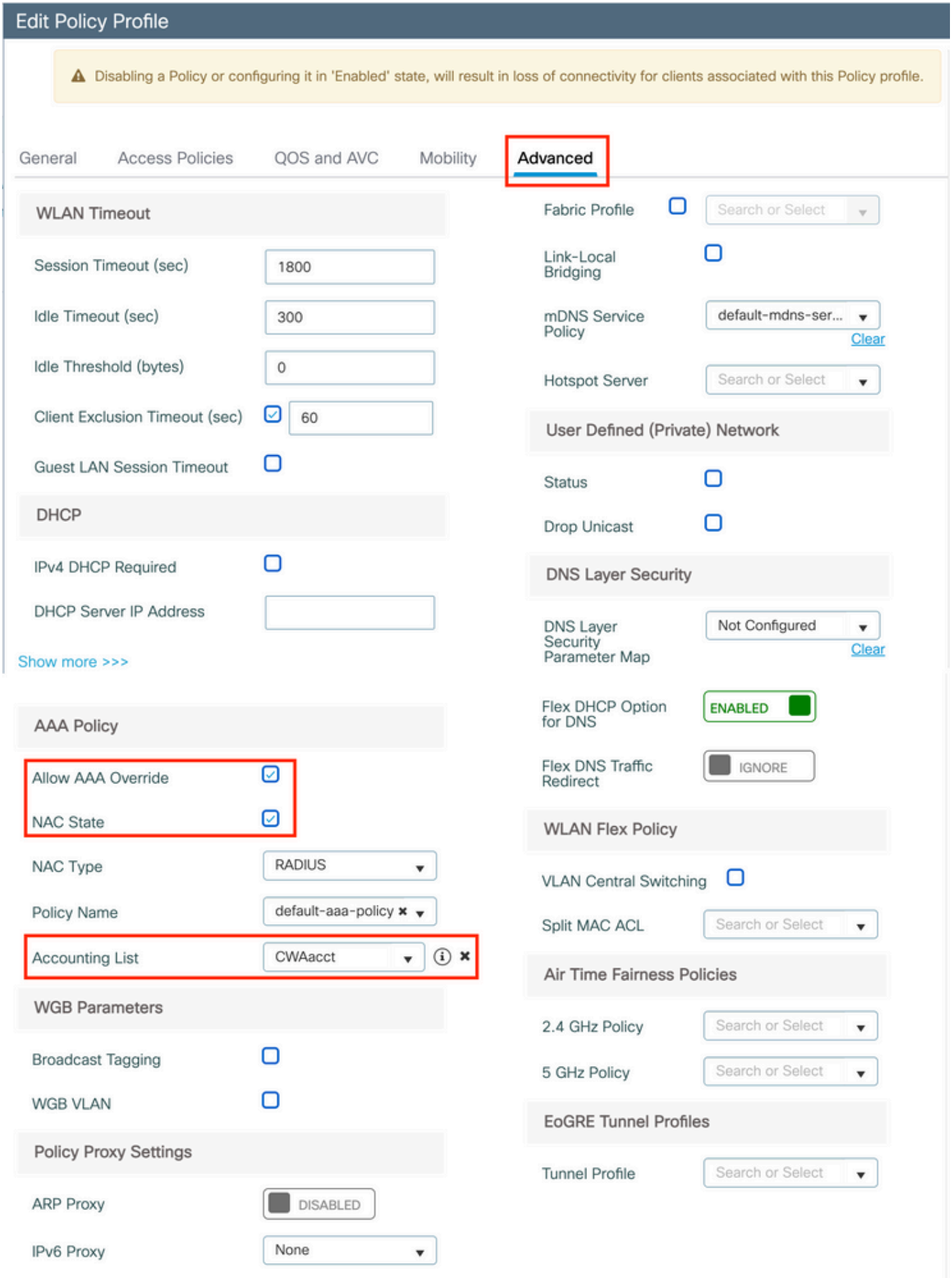


2단계. VLAN을 선택합니다.

탭으로 Access Policies 이동하여 드롭다운에서 VLAN 이름을 선택하거나 VLAN-ID를 수동으로 입력합니다. 정책 프로파일에서 ACL을 구성하지 마십시오.



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


Edit Policy Profile
Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.
General
Access Policies
QOS and AVC
Mobility
Advanced
WLAN Timeout
Session Timeout (sec)
1800
Idle Timeout (sec)
300
Idle Threshold (bytes)
0
Client Exclusion Timeout (sec)
60
Guest LAN Session Timeout
DHCP
IPv4 DHCP Required
DHCP Server IP Address
Show more >>>
AAA Policy
Allow AAA Override
NAC State
NAC Type
RADIUS
Policy Name
default-aaa-policy
Accounting List
CWAacct
WGB Parameters
Broadcast Tagging
WGB VLAN
Policy Proxy Settings
ARP Proxy
DISABLED
IPv6 Proxy
None
Fabric Profile
Search or Select
Link-Local Bridging
mDNS Service Policy
default-mdns-ser...
Clear
Hotspot Server
Search or Select
User Defined (Private) Network
Status
Drop Unicast
DNS Layer Security
DNS Layer Security Parameter Map
Not Configured
Clear
Flex DHCP Option for DNS
ENABLED
Flex DNS Traffic Redirect
IGNORE
WLAN Flex Policy
VLAN Central Switching
Split MAC ACL
Search or Select
Air Time Fairness Policies
2.4 GHz Policy
Search or Select
5 GHz Policy
Search or Select
EoGRE Tunnel Profiles
Tunnel Profile
Search or Select

CLI:

config # wireless profile policy <policy-profile-name> # aaa-override
nac
vlan <vlan-id_or_vlan-name>
accounting-list <acct-list>
no shutdown

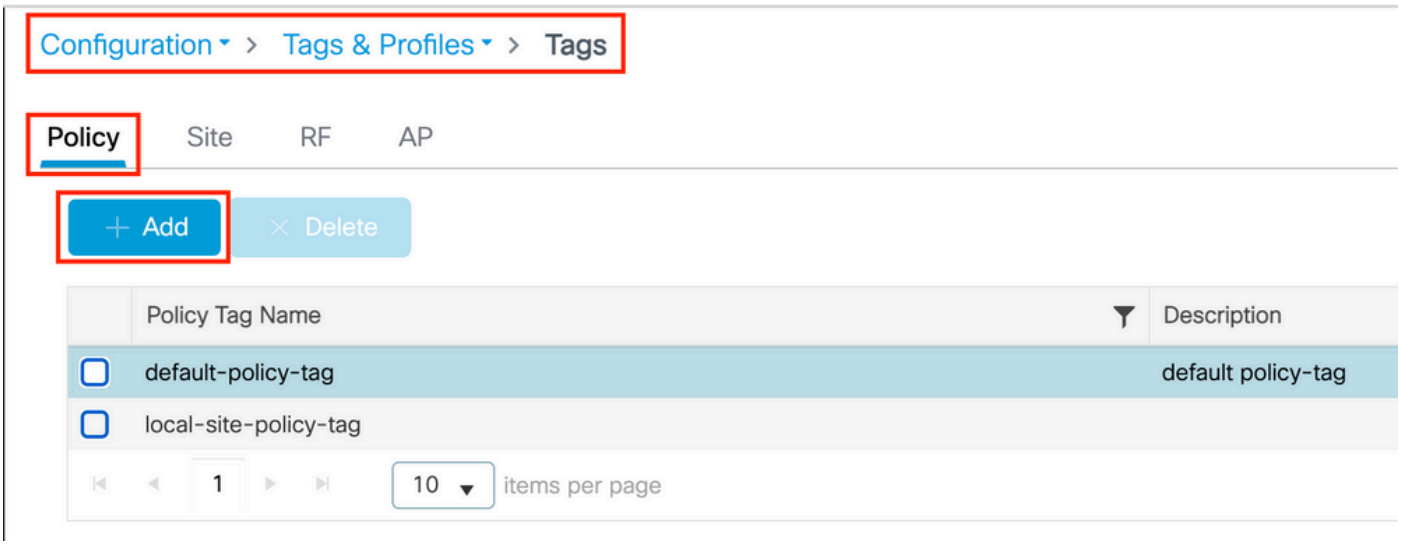
정책 태그 구성

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

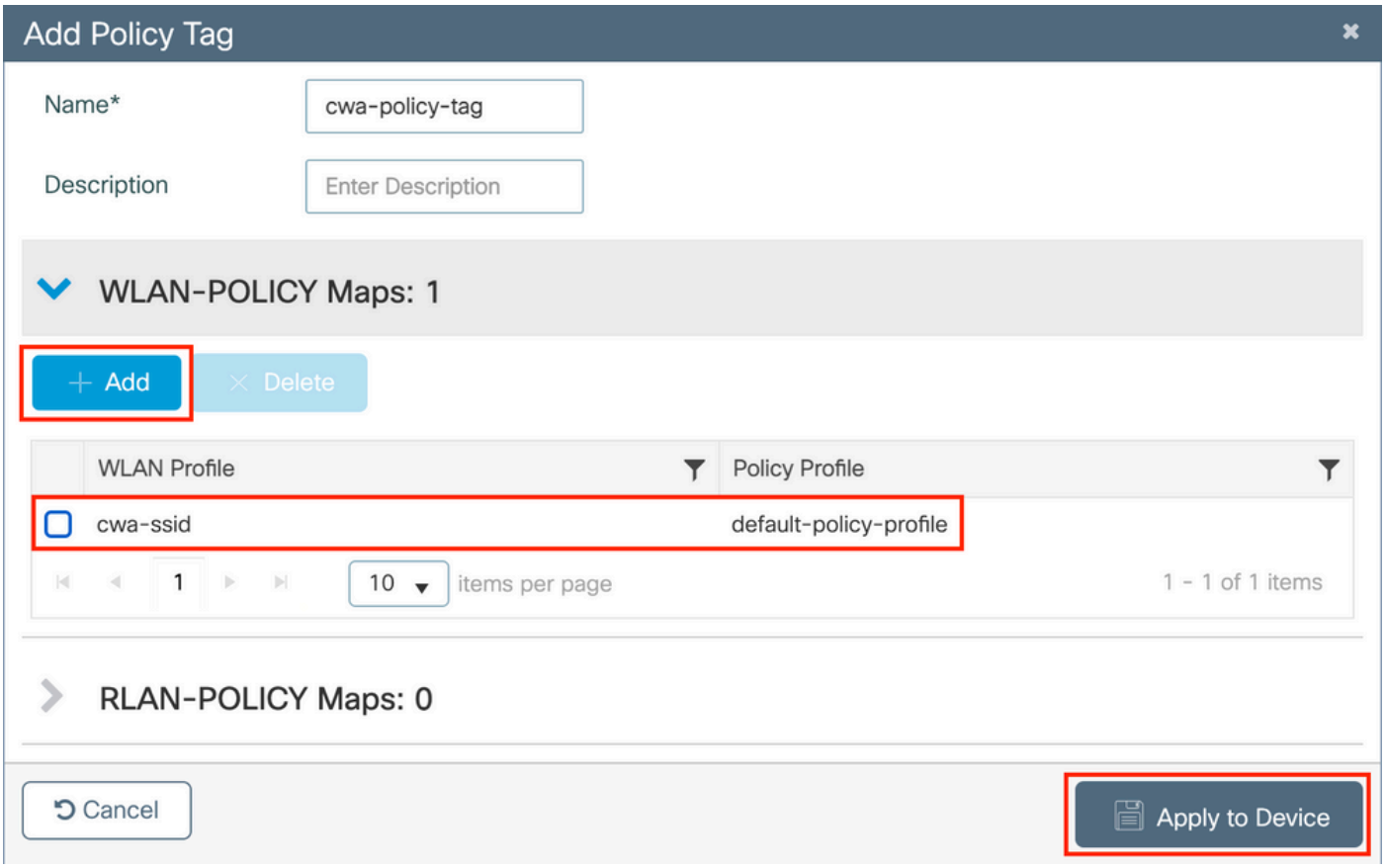
참고: default-policy 태그는 WLAN ID가 1~16인 SSID를 자동으로 default-policy 프로필에 매핑합니다. 수정하거나 삭제할 수 없습니다. ID가 17 이상인 WLAN이 있는 경우 default-policy 태그를 사용할 수 없습니다.

GUI:

그림에 표시된 대로 필요한 경우 Configuration > Tags & Profiles > Tags > Policy 새 디렉토리로 이동하여 추가합니다.



WLAN 프로파일을 원하는 정책 프로파일에 연결합니다.



CLI:

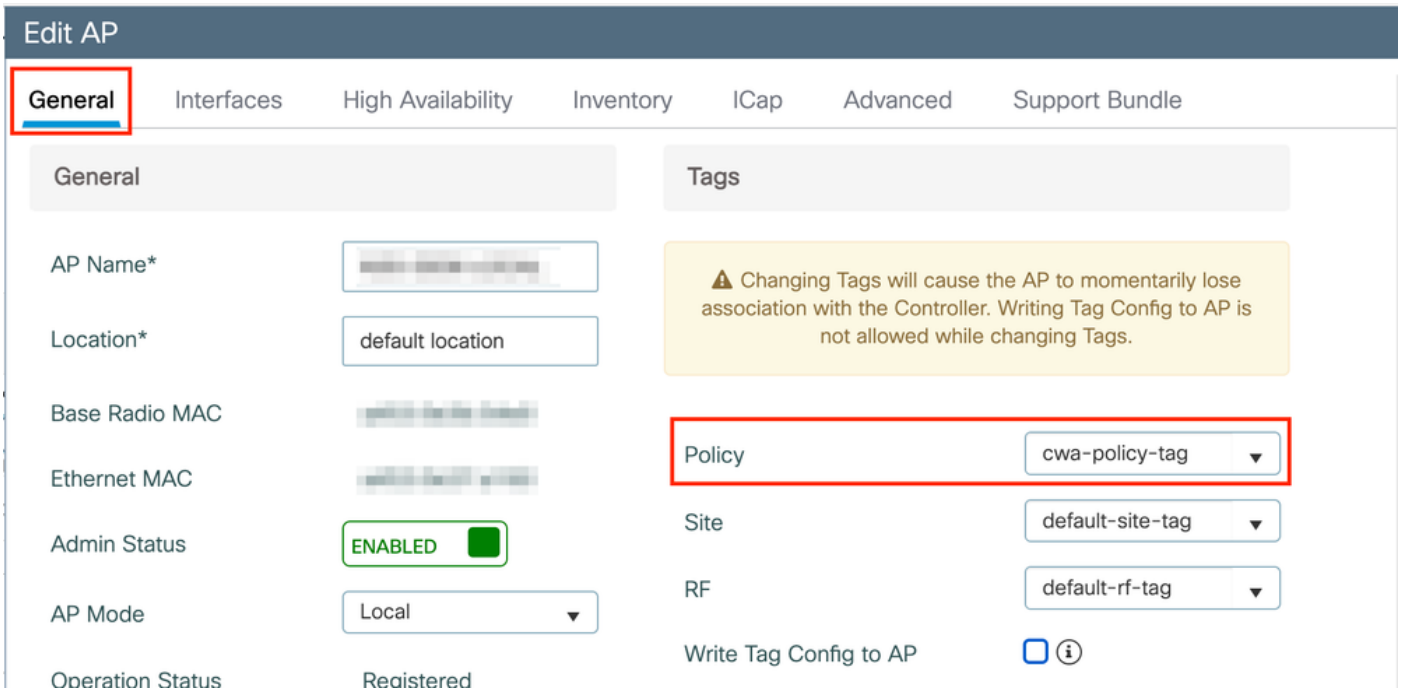
config t # wireless tag policy <policy-tag-name> # wlan <profile-name> policy <policy-profile-name>

정책 태그 할당

필요한 AP에 정책 태그를 할당합니다.

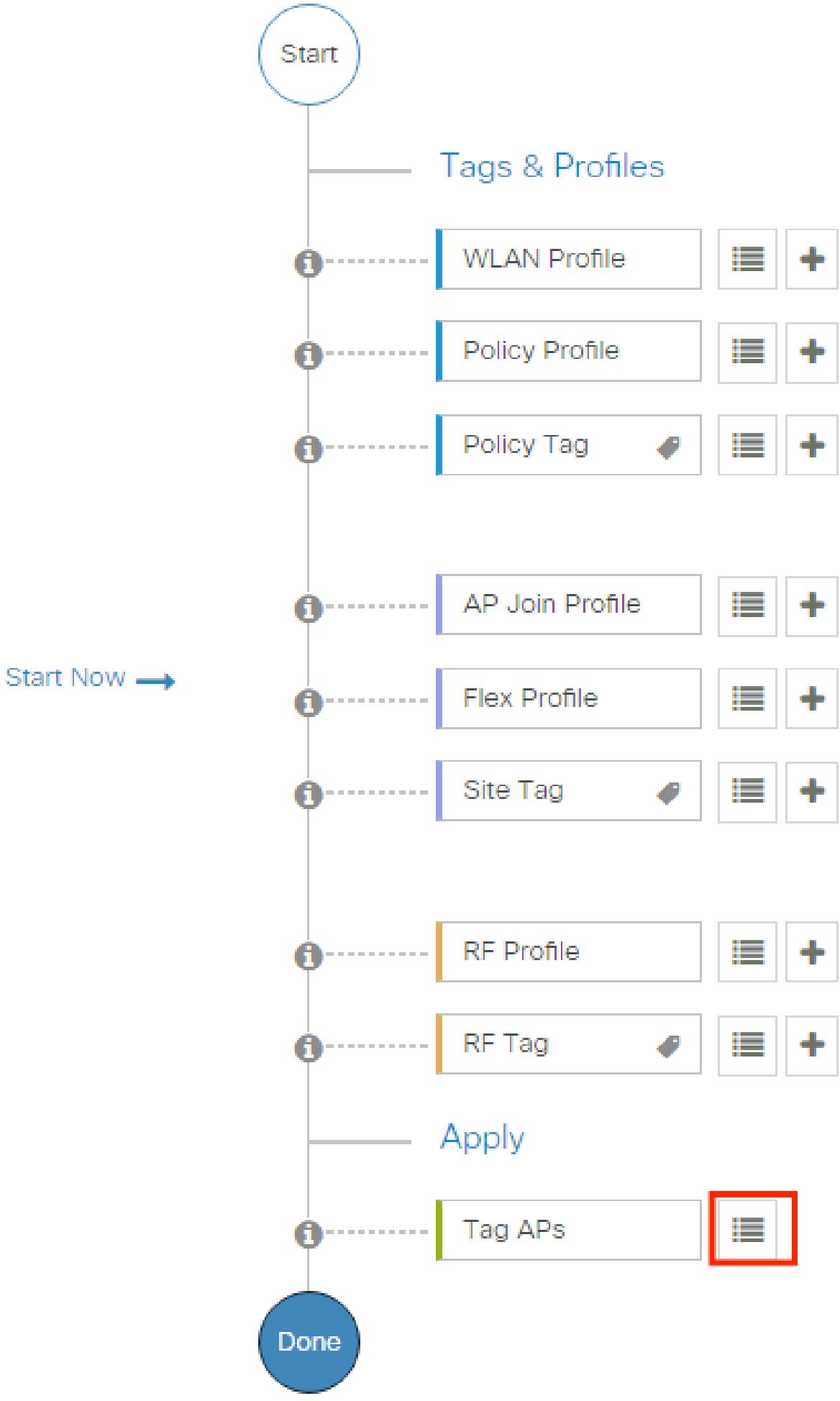
GUI:

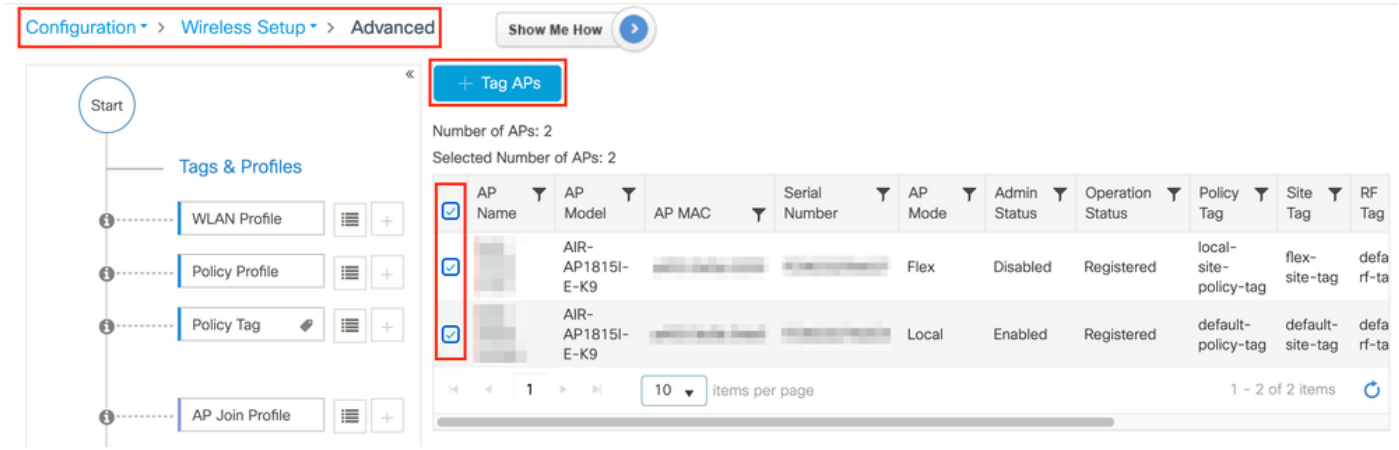
하나의 AP에 태그를 할당하려면 로 이동하여 Configuration > Wireless > Access Points > AP Name > General Tags 필요한 할당을 수행한 다음 을 클릭합니다Update & Apply to Device.



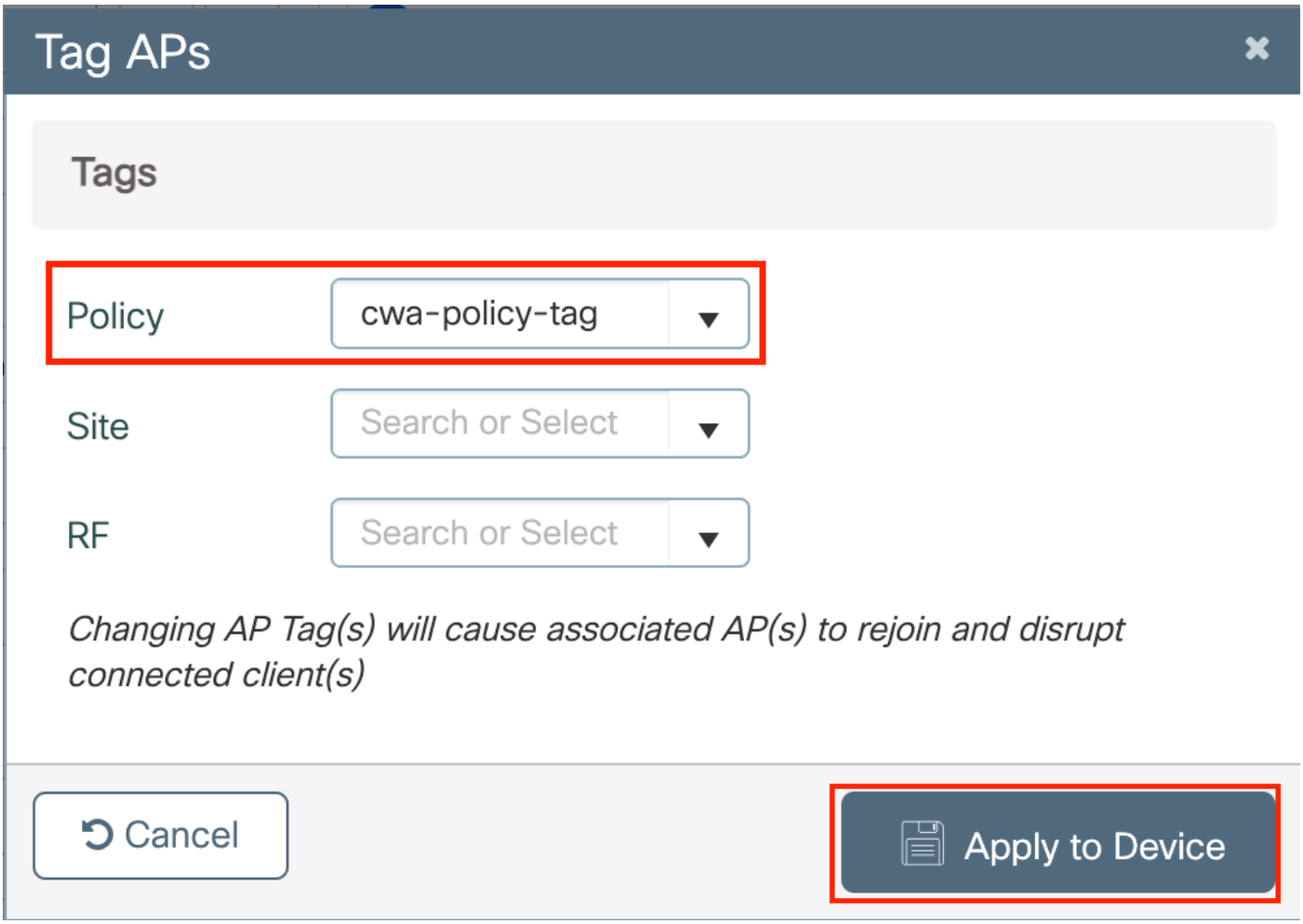
참고: AP에서 정책 태그를 변경하면 9800 WLC와의 연결이 끊기고 약 1분 내에 다시 결합됩니다.

동일한 정책 태그를 여러 AP에 할당하려면 로 Configuration > Wireless > Wireless Setup > Advanced > Start Now 이동합니다.


Start
Tags & Profiles
WLAN Profile
Policy Profile
Policy Tag
AP Join Profile
Start Now
Flex Profile
Site Tag
RF Profile
RF Tag
Apply
Tag APs
Done



그림과 같이 흰색의 태그를 선택하고 클릭합니다Save & Apply to Device.



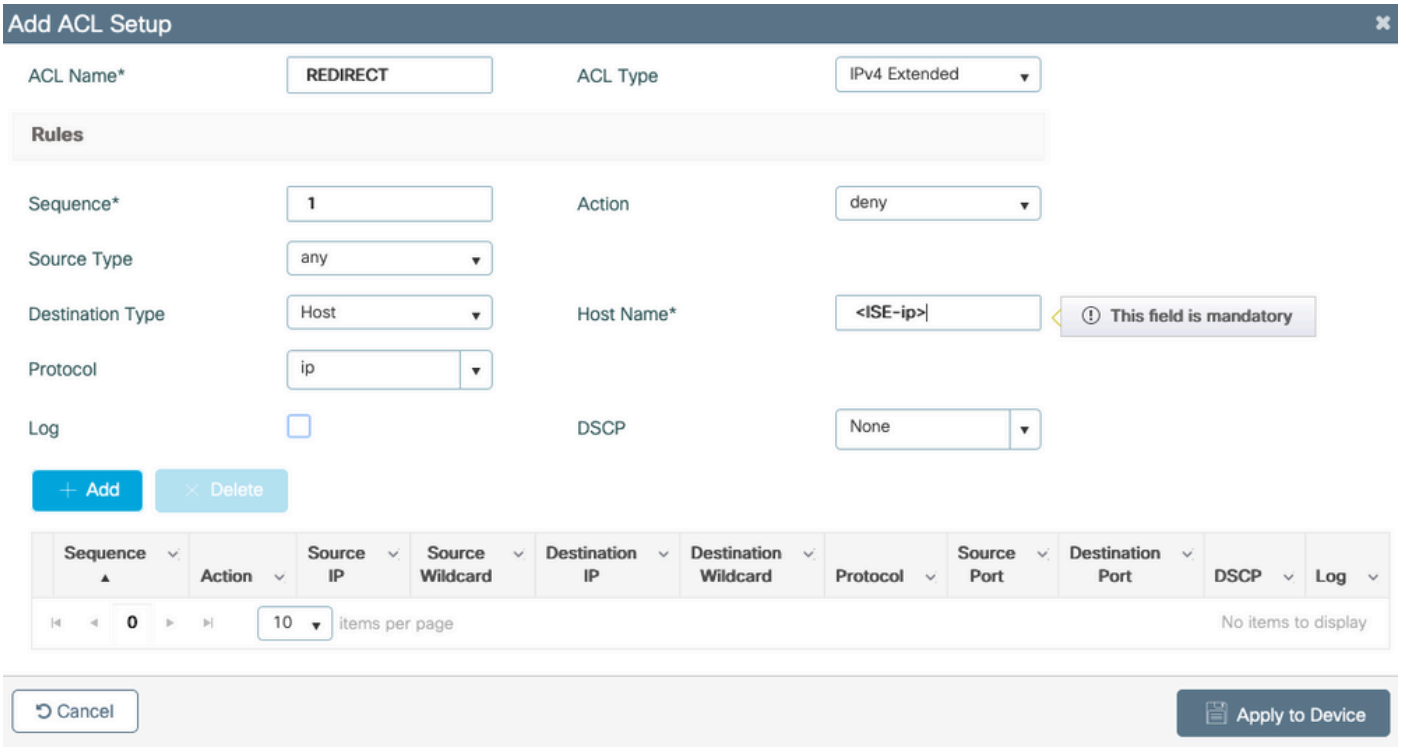
CLI:

config t # ap <ethernet-mac-addr> # policy-tag <policy-tag-name> # end

ACL 구성 리디렉션

1단계. 새 ACLConfiguration > Security > ACL > + Add 을 생성하려면 로 이동합니다.

이미지에 표시된 대로 ACL의 이름을 선택하고 IPv4 Extended 모든 규칙을 입력하고 시퀀스로 추가합니다.



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 10.48.39.28을 ISE IP 주소로 대체).

Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
10	deny	any		10.48.39.28		ip			None	Disabled
20	deny	10.48.39.28		any		ip			None	Disabled
30	deny	any		any		udp		eq domain	None	Disabled
40	deny	any		any		udp	eq domain		None	Disabled
50	permit	any		any		tcp		eq www	None	Disabled

1 10 items per page 1 - 5 of 5 items

참고: 리디렉션 ACL의 경우 작업을 deny 거부 리디렉션(트래픽을 거부하지 않음)으로 간주하고 작업을 permit 허용 리디렉션으로 간주합니다. WLC는 리디렉션할 수 있는 트래픽(기본적으로 포트 80 및 443)만 조사합니다.

CLI:

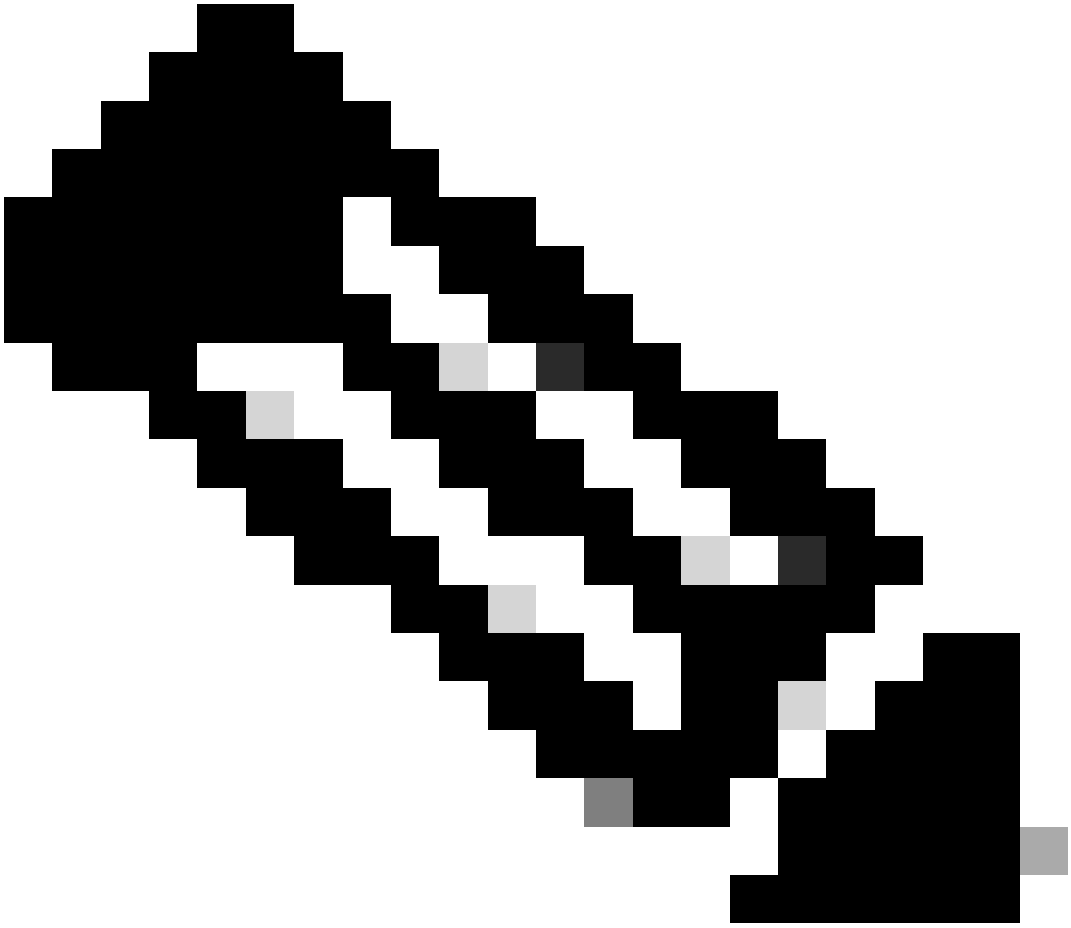
```
ip access-list extended REDIRECT
 deny ip any host <ISE-IP>
 deny ip host<ISE-IP> any
 deny udp any any eq domain
 deny udp any eq domain any
 permit tcp any any eq 80
```

참고: 포트 80에permit ip any any 집중된 허용 대신에 ACL을 종료하면 WLC도 HTTPS를 리디렉션합니다. 이는 자체 인증서를 제공해야 하고 항상 인증서 위반을 생성해야 하기 때문에 바람직하지 않은 경우가 많습니다. 이는 CWA의 경우 WLC에 인증서가 필요하지 않다고 말하는 이전 문의 예외입니다. HTTPS 가로채기를 활성화했지만 어쨌든 유효한 것으로 간주되지 않는 경우 인증서가 필요합니다.

ISE 서버에 대한 게스트 포트 8443만 거부하도록 조치하여 ACL을 개선할 수 있습니다.

HTTP 또는 HTTPS에 대한 리디렉션 사용

웹 관리 포털 컨피그레이션은 웹 인증 포털 컨피그레이션과 연결되어 있으며 리디렉션하려면 포트 80에서 수신해야 합니다. 따라서 리디렉션이 제대로 작동하려면 HTTP를 활성화해야 합니다. 전역ip http server으로 활성화하도록 선택하거나(명령을 사용하여) 웹 인증 모듈에만 HTTP를 활성화할 수 있습니다(매개변수 맵 아래의 명령을 사용하여webauth-http-enable).



참고: HTTP 트래픽의 리디렉션은 FlexConnect 로컬 스위칭의 경우에도 CAPWAP 내에서 발생합니다. 인터셉션 작업을 수행하는 WLC이므로 AP는 CAPWAP 터널 내에서 HTTP(S) 패킷을 전송하고 WLC에서 리디렉션을 다시 CAPWAP로 수신합니다

HTTPS URL에 액세스하려고 할 때 리디렉션하려면 매개 변수 맵에 명령intercept-https-enable을 추가하되, 이는 최적의 컨피그레이션이 아니므로 WLC CPU에 영향을 미치고 인증서 오류를 생성한다는 점에 유의하십시오.

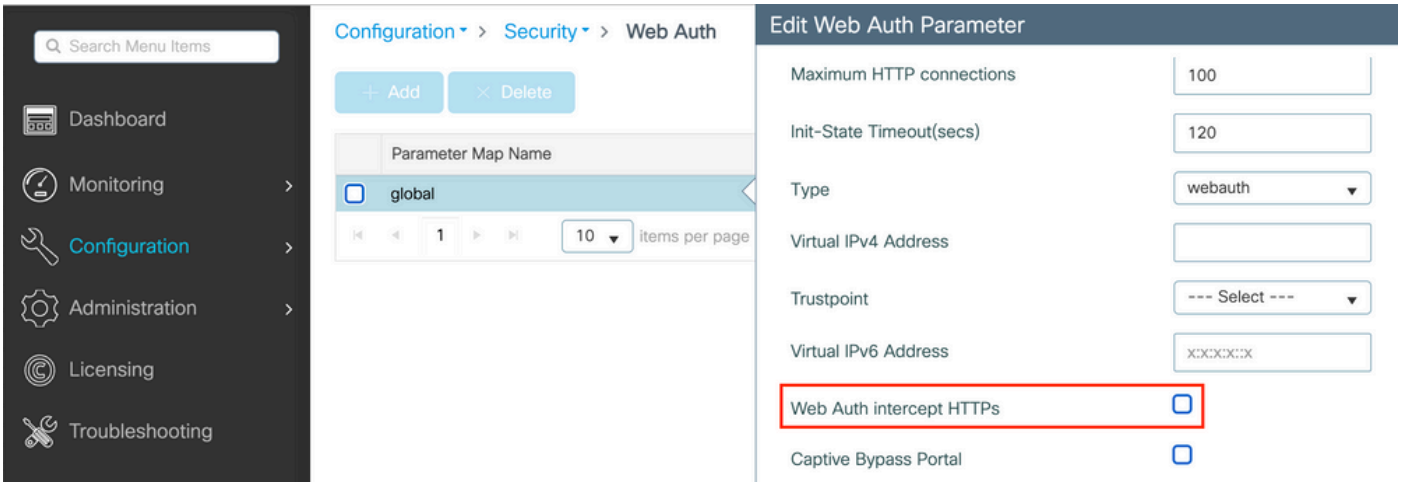
<#root>

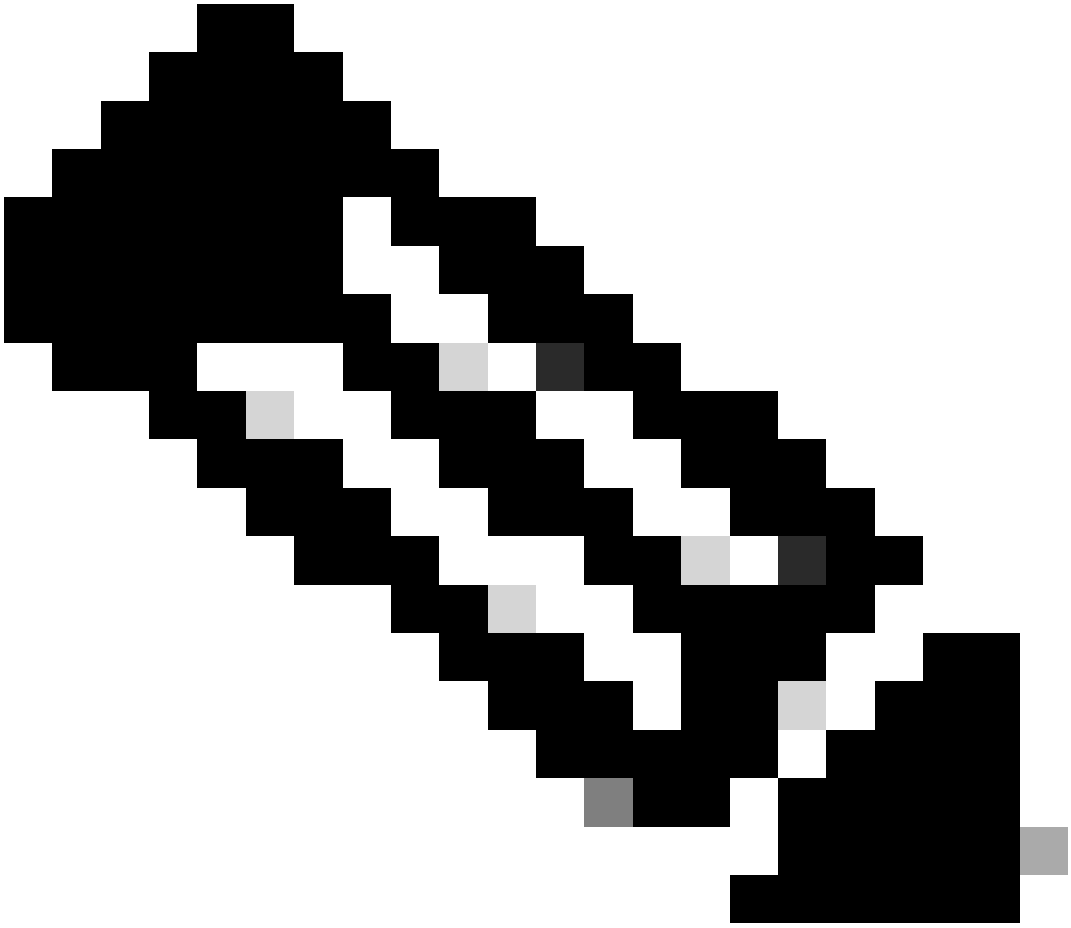
parameter-map type webauth global
 type webauth

```
intercept-https-enable

 trustpoint xxxxx
```

또한 매개 변수 맵(Configuration > Security > Web Auth)에서 선택한 '웹 인증 가로채기 HTTPS' 옵션을 사용하여 GUI를 통해 수행할 수 있습니다.



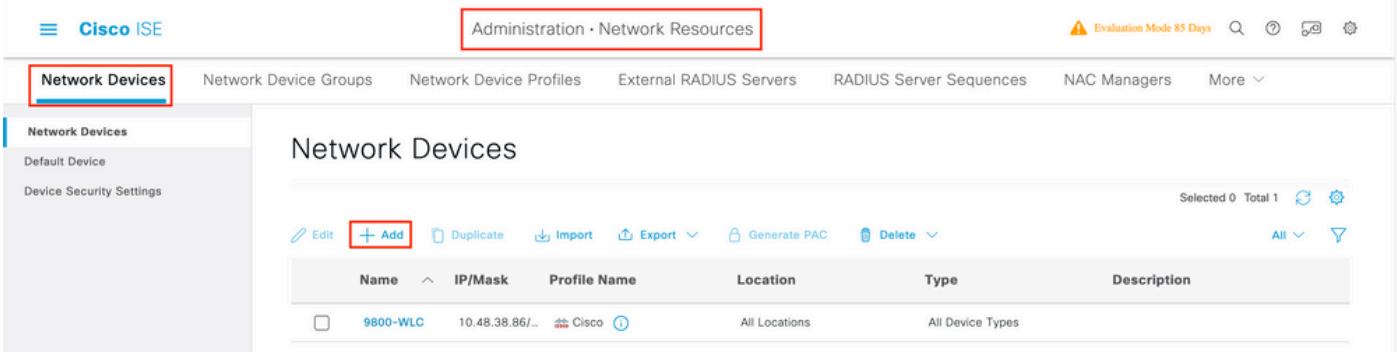


참고: 기본적으로 브라우저에서는 HTTP 웹 사이트를 사용하여 리디렉션 프로세스를 시작합니다. HTTPS 리디렉션이 필요한 경우 웹 인증 가로채기 HTTPS를 선택해야 합니다. 그러나 이 구성은 CPU 사용량을 늘리기 때문에 권장되지 않습니다.

ISE 구성

ISE에 9800 WLC 추가

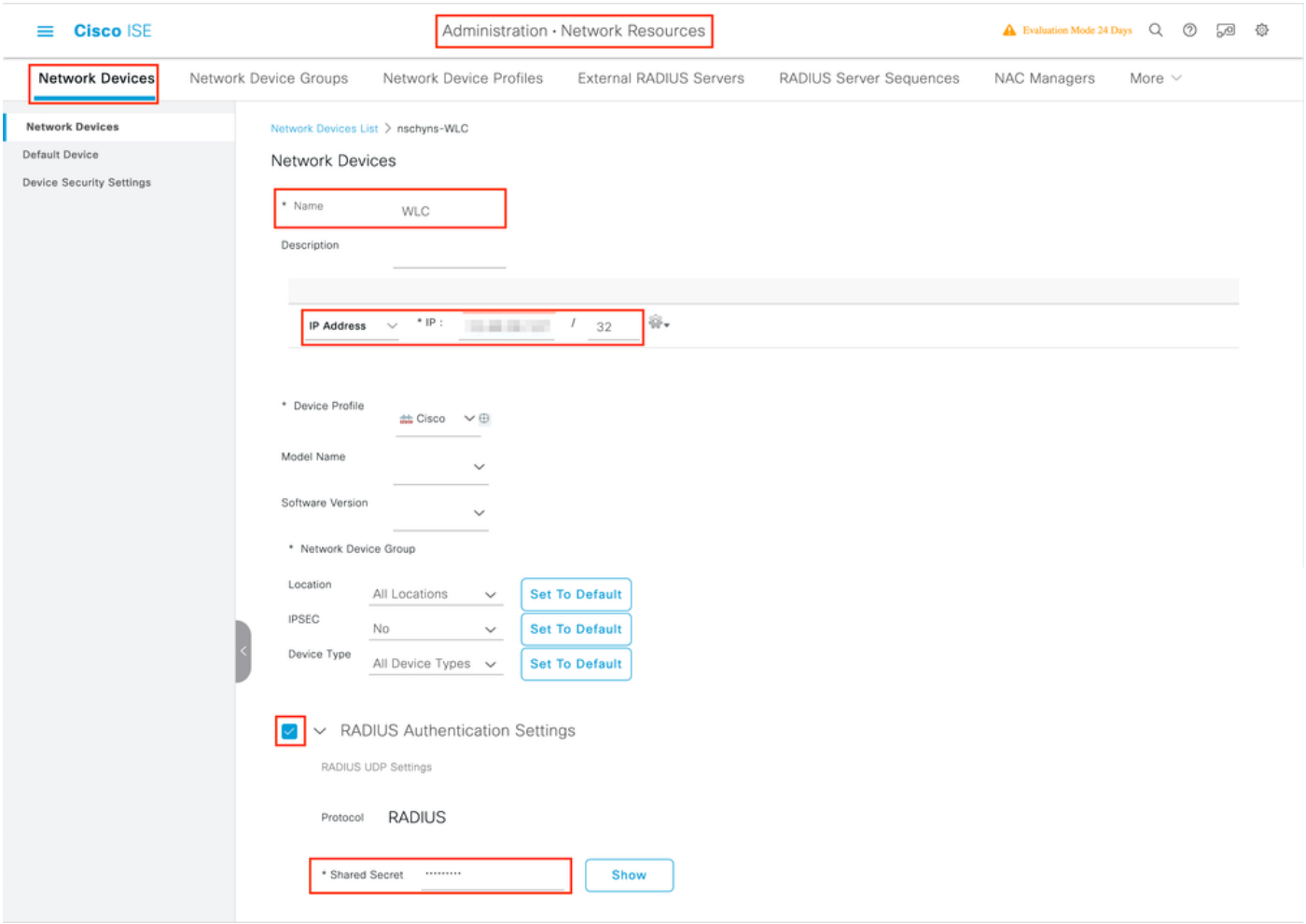
1단계. ISE 콘솔을 열고 이미지에 표시된Administration > Network Resources > Network Devices > Add 대로 로 이동합니다.



2단계. 네트워크 디바이스를 구성합니다.

선택적으로, 지정된 모델 이름, 소프트웨어 버전 및 설명이 될 수 있으며 디바이스 유형, 위치 또는 WLC에 따라 네트워크 디바이스 그룹을 할당할 수 있습니다.

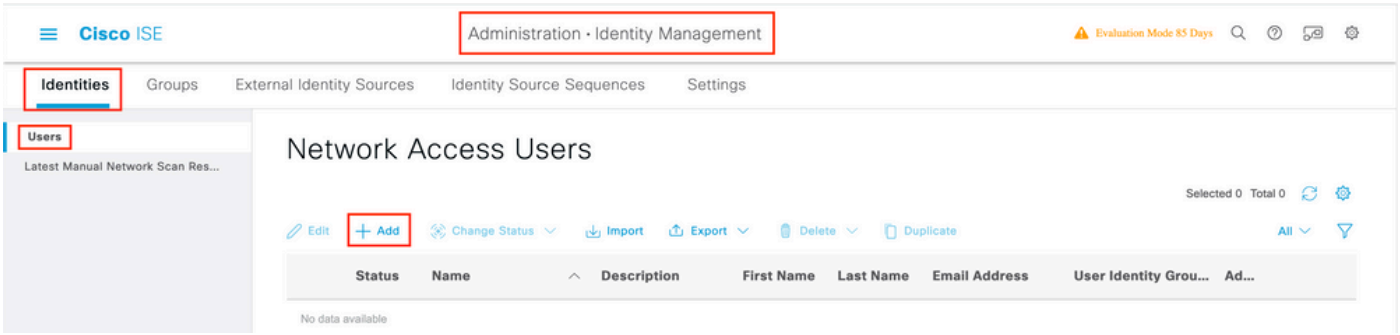
여기서 IP 주소는 인증 요청을 전송하는 WLC 인터페이스에 해당합니다. 기본적으로 이 인터페이스는 이미지에 표시된 관리 인터페이스입니다.



네트워크 디바이스 그룹에 대한 자세한 내용은 ISE 관리 가이드 장: 네트워크 디바이스 관리: ISE - 네트워크 디바이스 그룹을 참조하십시오.

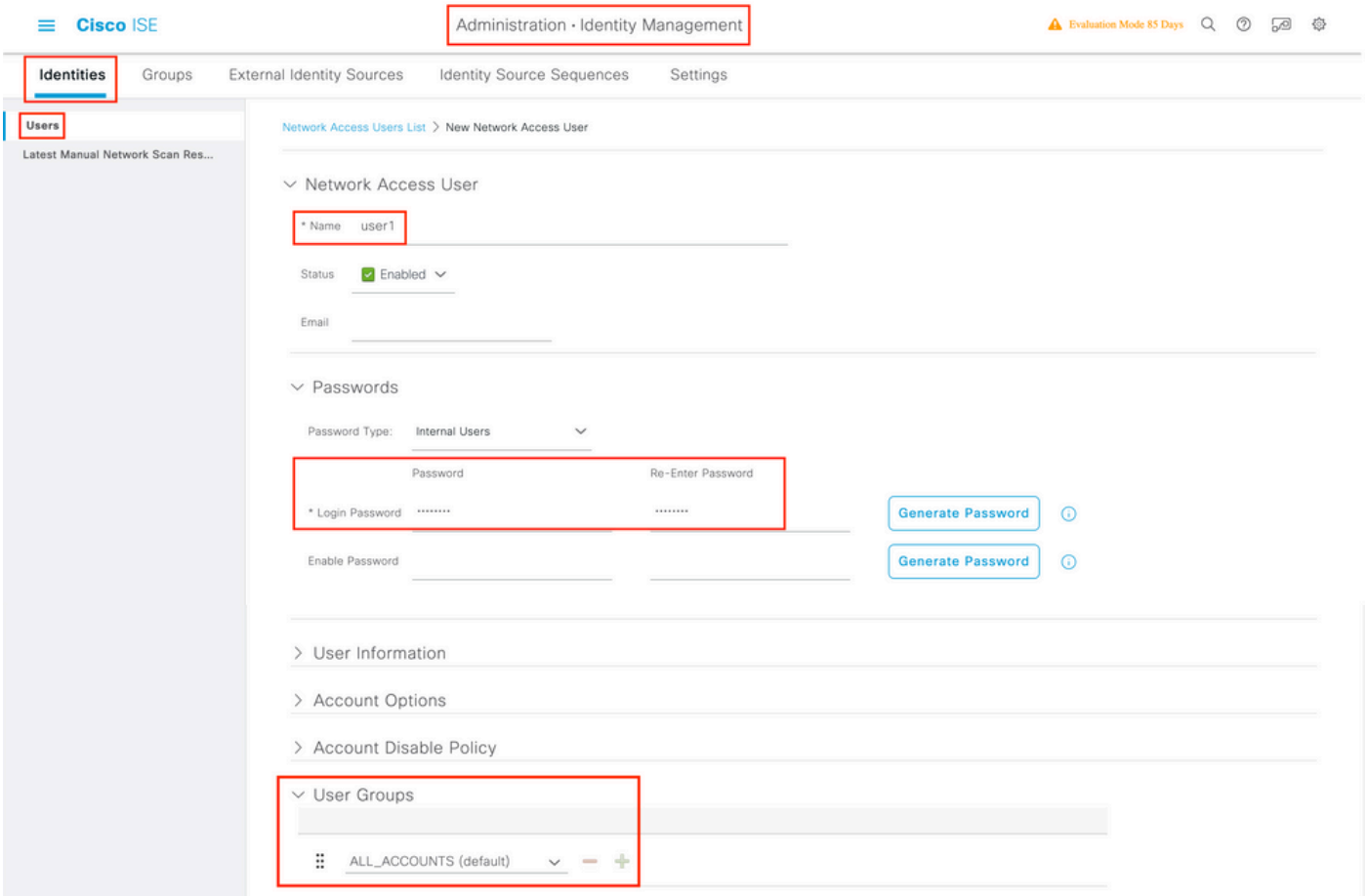
ISE에서 새 사용자 생성

1단계. 이미지에 Administration > Identity Management > Identities > Users > Add 표시된 대로 이동합니다.



2단계. 정보를 입력합니다.

이 예에서 이 사용자는 라는 그룹에 속하지만ALL_ACCOUNTS 이미지에 표시된 대로 필요에 따라 조정할 수 있습니다.

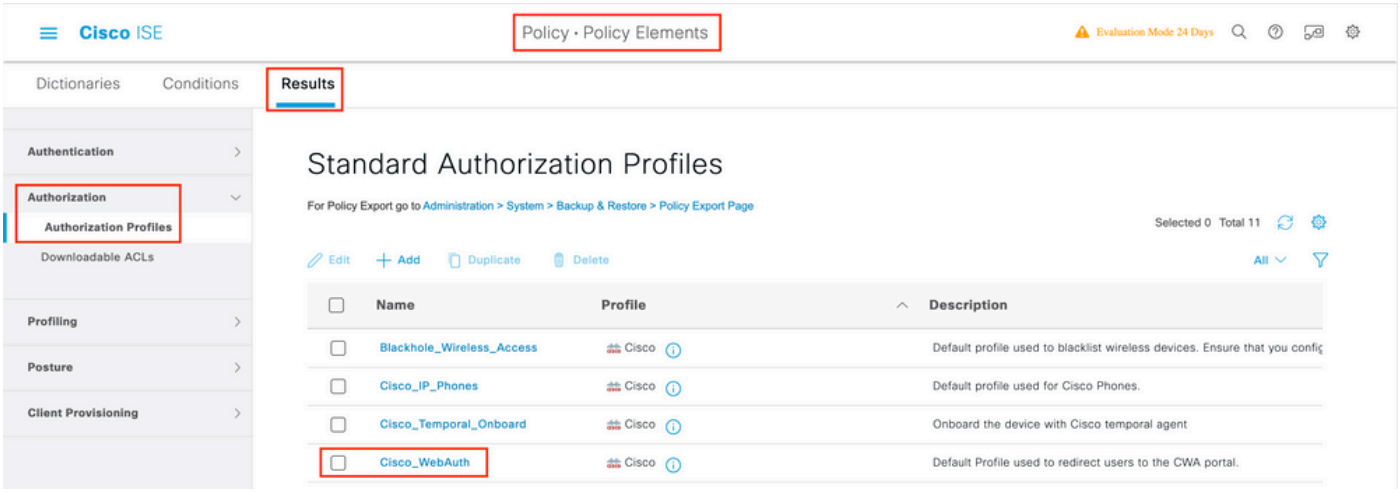


권한 부여 프로파일 생성

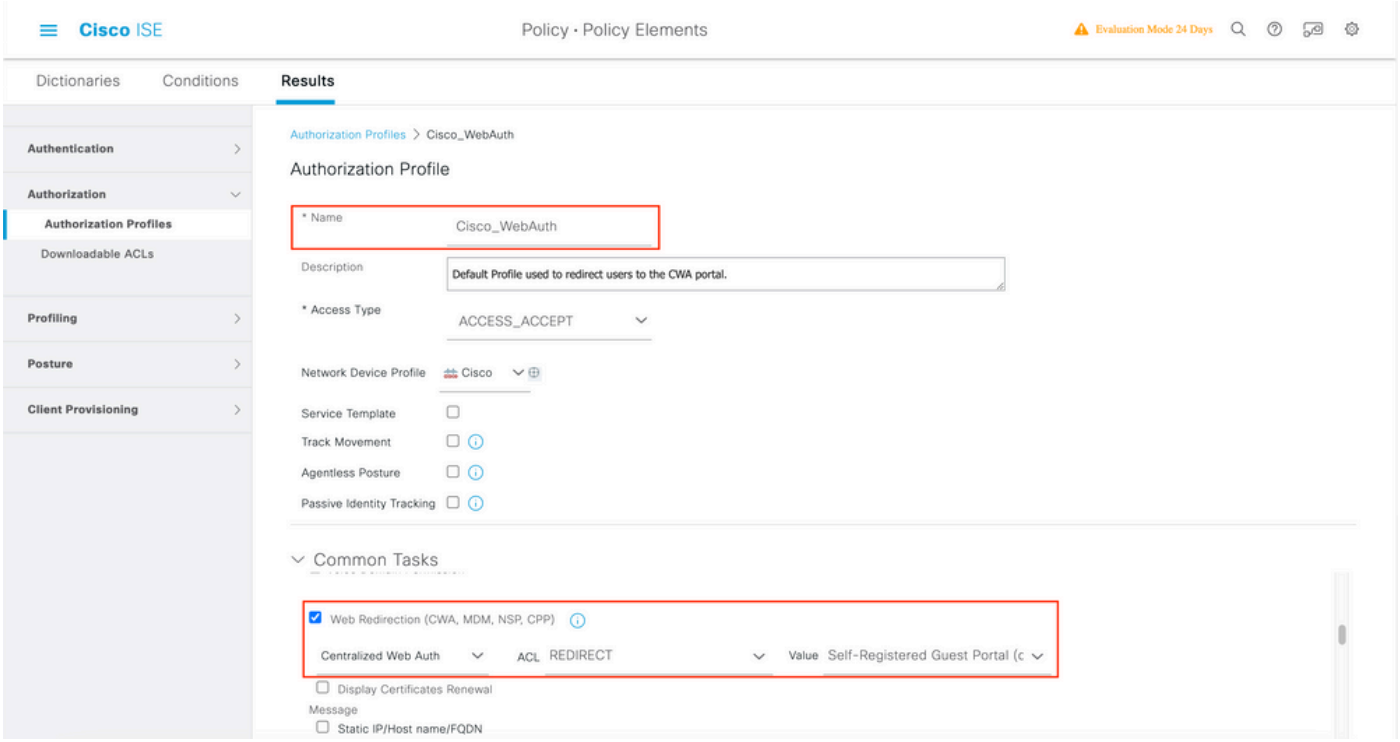
정책 프로필은 매개 변수(예: mac 주소, 자격 증명, 사용된 WLAN 등)를 기반으로 클라이언트에 할당된 결과입니다. VLAN(Virtual Local Area Network), ACL(Access Control List), URL(Uniform Resource Locator) 리디렉션 등 특정 설정을 할당할 수 있습니다.

최신 버전의 ISE에는 Cisco_Webauth 권한 부여 결과가 이미 있습니다. 여기에서 WLC에 구성한 것과 일치하도록 리디렉션 ACL 이름을 수정하도록 편집할 수 있습니다.

1단계. 로 Policy > Policy Elements > Results > Authorization > Authorization Profiles 이동합니다. add 사용자를 만들거나 기본 결과를 편집하려면 클릭하십시오Cisco_Webauth.

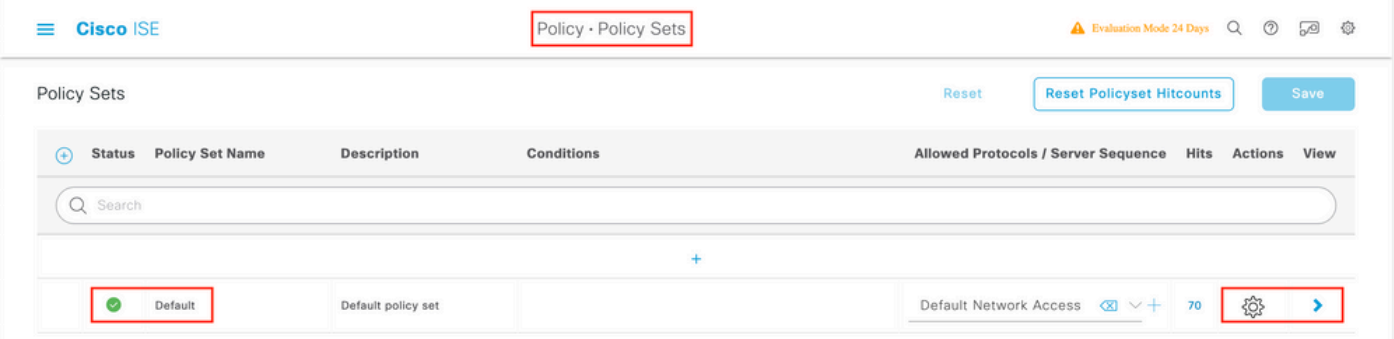


2단계. 리디렉션 정보를 입력합니다. ACL 이름이 9800 WLC에 구성된 이름과 동일한지 확인합니다.

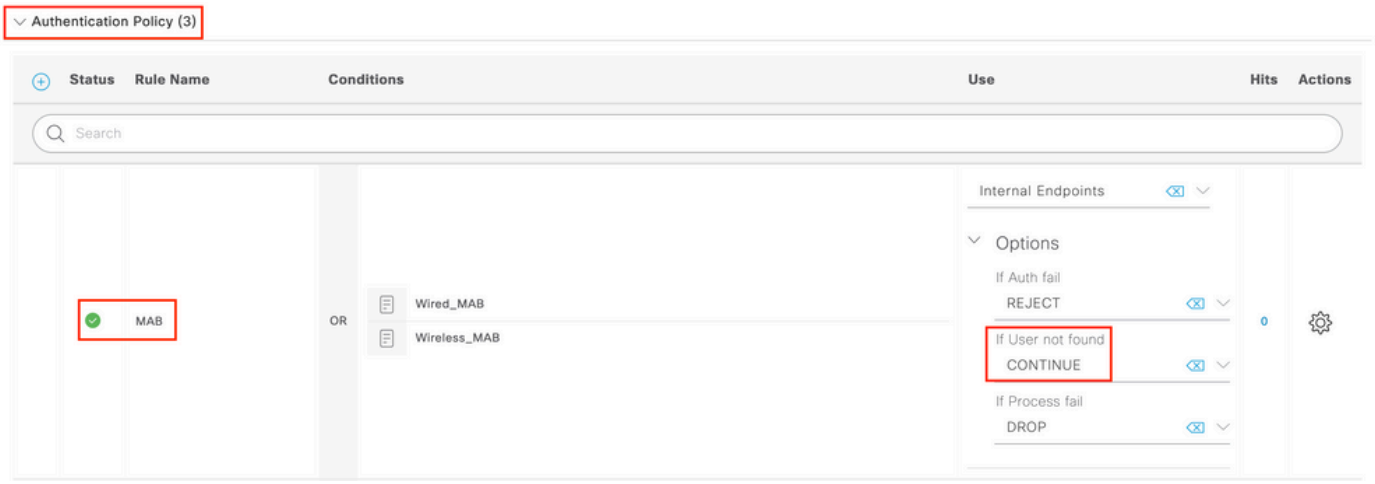


인증 규칙 구성

1단계. 정책 집합은 인증 및 권한 부여 규칙의 모음을 정의합니다. 하나를 생성하려면 로Policy > Policy Sets 이동하여 목록에서 첫 번째 정책 세트의 기어를 Insert new row 클릭하고 오른쪽의 파란색 화살표를 클릭하여 기본 정책 세트를 선택합니다.



2단계. 정책을 Authentication 펼칩니다. 규칙MAB Options(유선 또는 무선 MAB에서 일치)의 경우를 확장하고 '사용자를CONTINUE 찾을 수 없는 경우' 옵션을 선택합니다.



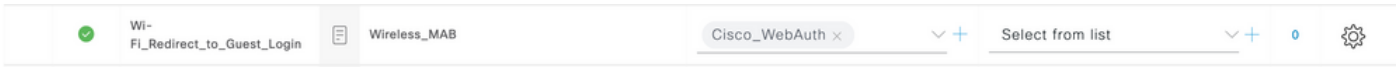
3단계. 변경 사항Save 을 저장하려면 를 클릭합니다.

권한 부여 규칙 구성

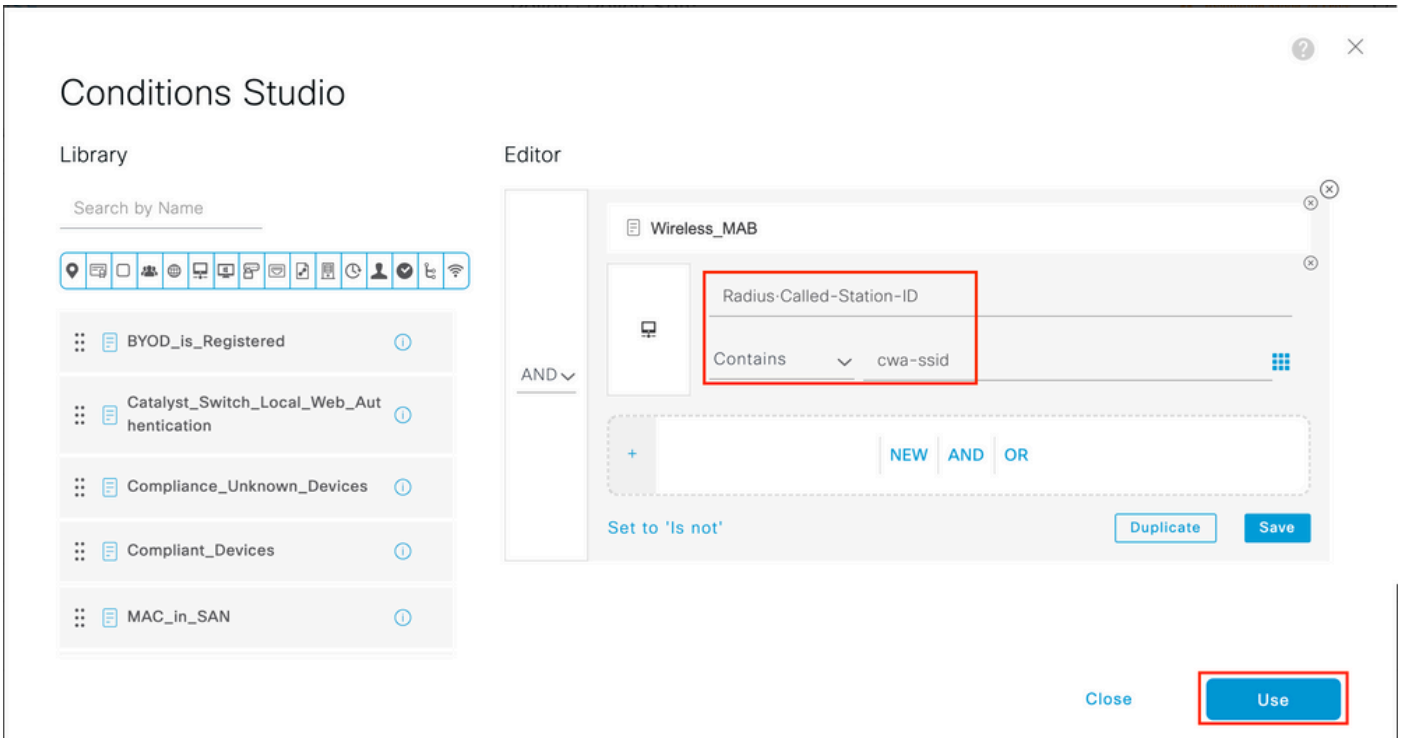
권한 부여 규칙은 클라이언트에 어떤 권한(권한 부여 프로파일) 결과를 적용할지 결정하는 역할을 합니다.

1단계. 동일한 정책 설정 페이지에서 를 Authentication Policy 닫고 이미지Authorziation Policy 에 표시된 대로 확장합니다.

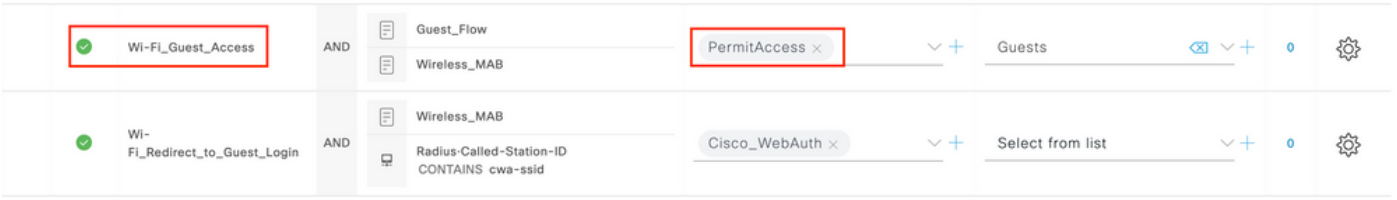
2단계. 최신 ISE 버전은 대부분 우리의 요구와 일치하는Wifi_Redirect_to_Guest_Login 미리 생성된 규칙에서 시작합니다. 왼쪽에 있는 회색 판을 enable 돌려.



3단계. 이 규칙은 Wireless_MAB에만 일치하며 CWA 리디렉션 특성을 반환합니다. 이제 선택적으로 약간의 비틀기를 추가하고 특정 SSID에만 일치하도록 할 수 있습니다. Conditions Studio(조건 스튜디오)를 표시하려면 조건(현재 Wireless_MAB)을 선택합니다. 오른쪽에 조건을 추가하고 특성이 있는Radius 사전을 Called-Station-ID 선택합니다. SSID 이름과 일치하도록 합니다. 그림과 같이Use 화면 하단의 를 사용하여 확인합니다.



4단계. 이제 사용자가 포털에서 인증되면 네트워크 액세스 세부사항을 반환하기 위해 조건과 매칭하는Guest Flow 더 높은 우선 순위로 정의된 두 번째 규칙이 필요합니다. 최근 ISEWifi Guest Access 버전에서도 기본적으로 미리 생성된 규칙을 사용할 수 있습니다. 그런 다음 왼쪽에 녹색 표시가 있는 규칙만 활성화해야 합니다. 기본 PermitAccess를 반환하거나 더 정확한 액세스 목록 제한을 구성할 수 있습니다.



5단계. 규칙을 저장합니다.

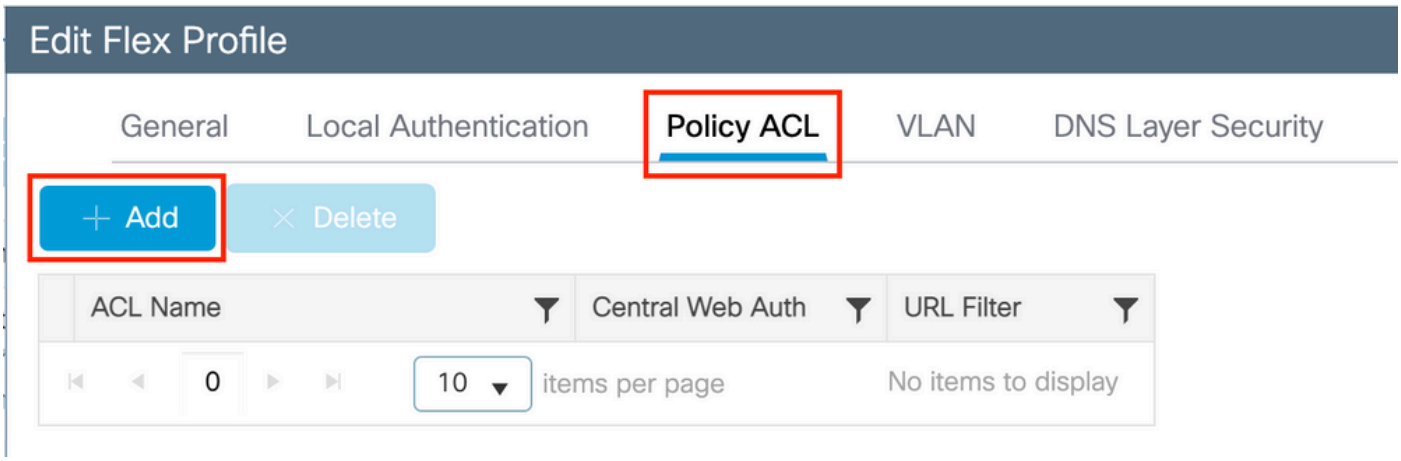
규칙Save 의 하단을 클릭합니다.

FlexConnect 로컬 스위칭 액세스 포인트 전용

FlexConnect 로컬 스위칭 액세스 포인트 및 WLAN이 있는 경우 어떻게 해야 합니까? 이전 섹션은 여전히 유효합니다. 그러나 리디렉션 ACL을 AP에 미리 푸시하려면 추가 단계가 필요합니다.

Flex 프로필로 Configuration > Tags & Profiles > Flex 이동하여 선택합니다. 그런 다음 탭으로 Policy ACL 이동합니다.

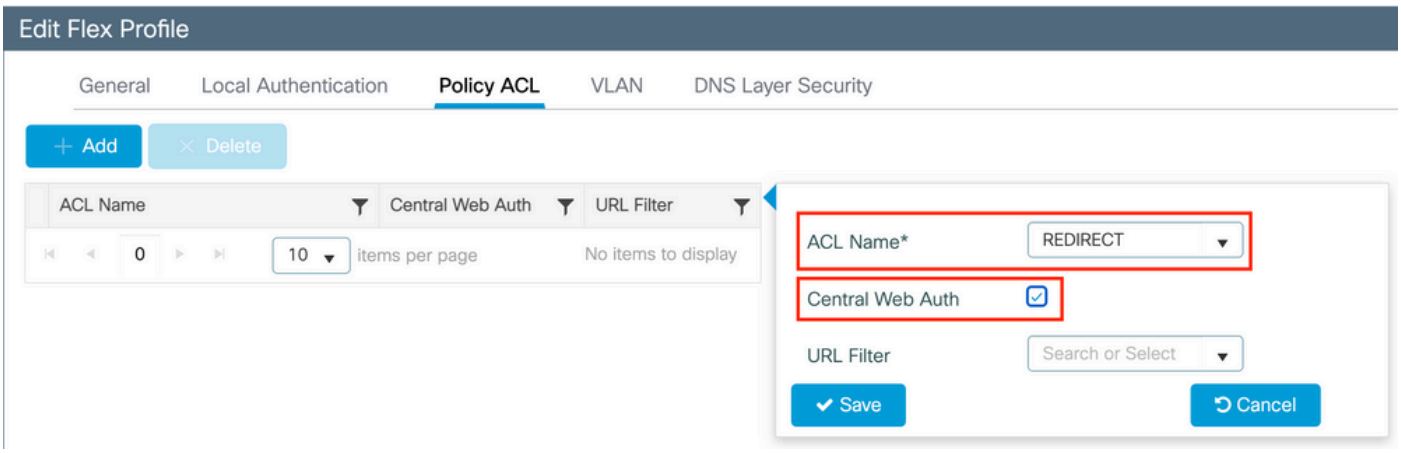
이미지Add 에 표시된 대로 클릭합니다.



리디렉션 ACL 이름을 선택하고 Central 웹 인증을 활성화합니다. 이 확인란은 AP 자체의 ACL을 자동으로 반전시킵니다. Cisco IOS XE의 WLC에서 'deny' 문은 '이 IP로 리디렉션하지 않음'을 의미하기 때문입니다. 그러나 AP에서 'deny' 문장은 그 반대를 의미합니다. 따라서 이 확인란은 AP에 대한 푸시를 수행할 때 모든 허가를 자동으로 스왑하고 거부합니다. AP CLI에서 이show ip access list를 확인할 수 있습니다.

참고: Flexconnect 로컬 스위칭 시나리오에서 ACL은 반환 명령문을 구체적으로 언급해야 합니다(로컬 모드에서 반드시 필요한 것은 아님). 따라서 모든 ACL 규칙이 (예를 들어 ISE로 들어오고 나가는) 트래픽의 두 가지 방법을 모두 다루도록 해야 합니다.

때리는 것Save 잊지 말고 Update and apply to the device하세요.



인증서

클라이언트가 웹 인증 인증서를 신뢰하도록 하려면 ISE 인증서(클라이언트가 신뢰해야 함)만 제공되므로 WLC에 인증서를 설치할

필요가 없습니다.

다음을 확인합니다.

이러한 명령을 사용하여 현재 구성을 확인할 수 있습니다.

<#root>

show run wlan # show run aaa # show aaa servers # show ap config general # show ap name <ap-name> config general
show ap tag summary
show ap name <AP-name> tag detail
show wlan { summary | id | nme | all }
show wireless tag policy detailed <policy-tag-name>
show wireless profile policy detailed <policy-profile-name>

다음은 이 예에 해당하는 WLC 컨피그레이션의 관련 부분입니다.

<#root>

aaa new-model !
aaa authorization network CWAauthz group radius aaa accounting identity CWAacct start-stop group radius ! aaa server radius dynamic-author client <ISE
 mac-filtering CWAauthz
 no security ft adaptive
 no security wpa
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 no security wpa akm dot1x
 no shutdown
ip http server (or "webauth-http-enable" under the parameter map)
ip http secure-server

문제 해결

체크리스트

- 클라이언트가 연결되어 있고 유효한 IP 주소를 가져와야 합니다.
- 리디렉션이 자동이 아니면 브라우저를 열고 임의의 IP 주소를 시도합니다. 예: 10.0.0.1. 리디렉션이 작동하는 경우 DNS 확인 문제가 있을 수 있습니다. DHCP를 통해 제공된 유효한 DNS 서버가 있으며 호스트 이름을 확인할 수 있는지 확인합니다.

- HTTP에서 리디렉션이ip http server 작동하도록 명령을 구성했는지 확인합니다. 웹 관리 포털 컨피그레이션은 웹 인증 포털 컨피그레이션과 연결되어 있으며 리디렉션하려면 포트 80에 나열되어야 합니다. 전역ip http server으로 활성화하도록 선택하거나(명령을 사용하여) 웹 인증 모듈에만 HTTP를 활성화할 수 있습니다(매개변수 맵 아래의 명령을 사용하여webauth-http-enable).

- HTTPS URL에 액세스하려고 할 때 리디렉션되지 않은 경우 매개 변수 맵에 다음 명령intercept-https-enable이 있는지 확인합니다.

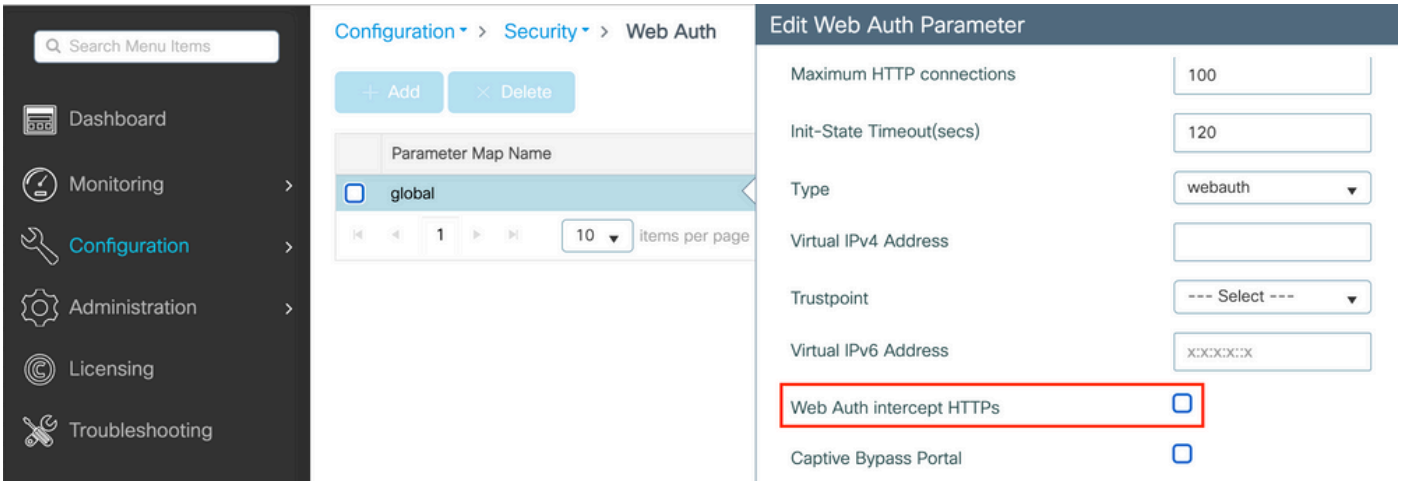
<#root>

parameter-map type webauth global
 type webauth

intercept-https-enable

trustpoint xxxxx

또한 GUI를 통해 매개변수 맵에서 'Web Auth intercept HTTPS' 옵션을 선택할 수도 있습니다.



RADIUS에 대한 서비스 포트 지원

Cisco Catalyst 9800 Series Wireless Controller에는 포트라고 하는 서비스 포트가 GigabitEthernet 0있습니다. 버전 17.6.1부터 RADIUS(CoA 포함)는 이 포트를 통해 지원됩니다.

RADIUS용 서비스 포트를 사용하려면 다음 컨피그레이션이 필요합니다.

<#root>

aaa server radius dynamic-author

client 10.48.39.28

```
vrf Mgmt-intf
 server-key cisco123
interface GigabitEthernet0

vrf forwarding Mgmt-intf

 ip address x.x.x.x x.x.x.x
!if using aaa group server:
aaa group server radius group-name
 server name nicoISE
 ip vrf forwarding Mgmt-intf


 ip radius source-interface GigabitEthernet0
```

디버그 수집

WLC 9800은 상시 추적 기능을 제공합니다. 이렇게 하면 모든 클라이언트 연결 관련 오류, 경고 및 알림 수준 메시지가 지속적으로 로깅되며, 사고 또는 장애 발생 후 상황에 대한 로그를 볼 수 있습니다.

참고: 로그에서 몇 시간에서 며칠로 돌아갈 수 있지만 생성된 로그의 볼륨에 따라 다릅니다.

기본적으로 9800 WLC가 수집한 추적을 보려면 SSH/텔넷을 통해 9800 WLC에 연결하고 다음 단계를 수행할 수 있습니다(세션을 텍스트 파일에 로깅해야 함).

1단계. WLC의 현재 시간을 확인하여 문제가 발생한 시간까지의 로그를 추적할 수 있습니다.

<#root>

show clock

2단계. 시스템 컨피그레이션에 따라 WLC 버퍼 또는 외부 syslog에서 syslog를 수집합니다. 이렇게 하면 시스템의 상태와 오류가 있는 경우 이를 빠르게 확인할 수 있습니다.

<#root>

show logging

3단계. 디버그 조건이 활성화되었는지 확인합니다.

<#root>

show debugging Cisco IOS XE Conditional Debug Configs: Conditional Debug Global State: Stop Cisco IOS XE Packet Tracing Configs: Packet Infra d

---

참고: 조건을 나열하면, 활성화된 조건(mac 주소, IP 주소 등)이 발생하는 모든 프로세스의 디버그 레벨에 추적이 로깅됨을 의미합니다. 이렇게 하면 로그의 볼륨이 증가합니다. 따라서 능동적으로 디버깅하지 않을 때는 모든 조건을 지우는 것이 좋습니다.

4단계. 테스트 중인 mac 주소가 3단계의 조건으로 나열되지 않았다는 가정하에 특정 mac 주소에 대한 always-on 알림 레벨 추적을 수집합니다.

<#root>

show logging profile wireless filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file always-on-<FILENAME.txt>

세션의 콘텐츠를 표시하거나 파일을 외부 TFTP 서버에 복사할 수 있습니다.

<#root>

more bootflash:always-on-<FILENAME.txt>
or
copy bootflash:always-on-<FILENAME.txt> tftp://a.b.c.d/path/always-on-<FILENAME.txt>

조건부 디버깅 및 무선 활성 추적

Always-on 추적을 통해 조사 중인 문제의 트리거를 확인할 수 있는 충분한 정보가 제공되지 않을 경우, 조건부 디버깅을 활성화하고 RA(Radio Active) 추적을 캡처할 수 있습니다. 그러면 지정된 조건(이 경우 클라이언트 mac 주소)과 상호 작용하는 모든 프로세스에 대해 디버그 레벨 추적을 제공합니다. 조건부 디버깅을 활성화하려면 다음 단계를 진행합니다.

5단계. 활성화된 디버그 조건이 없는지 확인합니다.

<#root>

clear platform condition all

6단계. 모니터링할 무선 클라이언트 mac 주소에 대한 디버그 조건을 활성화합니다.

이 명령은 30분(1,800초) 동안 제공된 MAC 주소를 모니터링하기 시작합니다. 선택적으로 이 시간을 최대 2,085,978,494초까지 늘릴 수 있습니다.

<#root>

debug wireless mac <aaaa.bbbb.cccc> {monitor-time <seconds>}

참고: 한 번에 둘 이상의 클라이언트를 모니터링하려면 mac 주소당 debug wireless mac <aaaa.bbbb.cccc> 명령을 실행합니다.

참고: 모든 것이 나중에 볼 수 있도록 내부적으로 버퍼링되므로 터미널 세션에서 클라이언트 활동의 출력이 표시되지 않습니다.

7단계` 모니터링할 문제나 동작을 재현합니다.

8단계. 기본 또는 구성된 모니터 시간이 끝나기 전에 문제가 재현되는 경우 디버그를 중지합니다.

<#root>

no debug wireless mac <aaaa.bbbb.cccc>

모니터 시간이 경과하거나 디버그 무선이 중지되면 9800 WLC는 다음과 같은 이름의 로컬 파일을 생성합니다.

ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

9단계. mac 주소 활동의 파일을 수집합니다. 를 외부 서버에 복사하거나ra trace .log 화면에 출력을 직접 표시할 수 있습니다.

RA 추적 파일의 이름을 확인합니다.

<#root>

dir bootflash: | inc ra_trace

파일을 외부 서버에 복사:

<#root>

copy bootflash: ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://a.b.c.d/ra-FILENAME.txt

콘텐츠 표시:

<#root>

more bootflash: ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

10단계. 근본 원인이 아직 명확하지 않은 경우 디버그 레벨 로그를 더 자세히 보여주는 내부 로그를 수집합니다. 이미 수집되어 내부적으로 저장된 디버그 로그를 더 자세히 살펴볼 뿐이므로 클라이언트를 다시 디버깅할 필요는 없습니다.

<#root>

show logging profile wireless internal filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file ra-internal-<FILENAME>.txt

---

참고: 이 명령 출력은 모든 프로세스에 대한 모든 로그 레벨의 추적을 반환하며 상당히 방대합니다. 이러한 추적을 분석하도록 Cisco TAC와 협력하십시오.

를 외부 서버에 복사하거나ra-internal-FILENAME.txt 화면에 출력을 직접 표시할 수 있습니다.

파일을 외부 서버에 복사:

<#root>

copy bootflash:ra-internal-<FILENAME>.txt tftp://a.b.c.d/ra-internal-<FILENAME>.txt

콘텐츠 표시:

<#root>

more bootflash:ra-internal-<FILENAME>.txt

11단계. 디버그 조건을 제거합니다.

<#root>

clear platform condition all

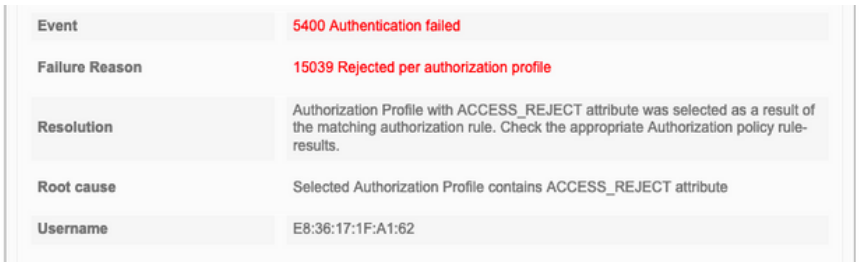
참고: 트러블슈팅 세션 후 항상 디버그 조건을 제거해야 합니다.

예

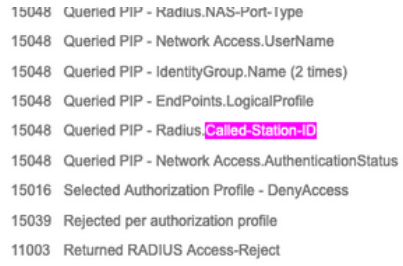
인증 결과가 예상과 다르면 ISE Operations > Live logs 페이지로 이동하여 인증 결과의 세부 정보를 가져오는 것이 중요합니다.

실패에 대한 이유(실패가 있는 경우) 및 ISE에서 수신하는 모든 Radius 특성이 표시됩니다.

다음 예시에서는 일치하는 권한 부여 규칙이 없으므로 ISE가 인증을 거부했습니다. 이는 권한 부여가 SSID 이름과 정확히 일치하는 반면 AP mac 주소에 추가된 SSID 이름으로 전송되는 Called-station-ID 특성이 표시되기 때문입니다. 해당 규칙이 'equal' 대신 'contains'로 변경되면서 수정됩니다.



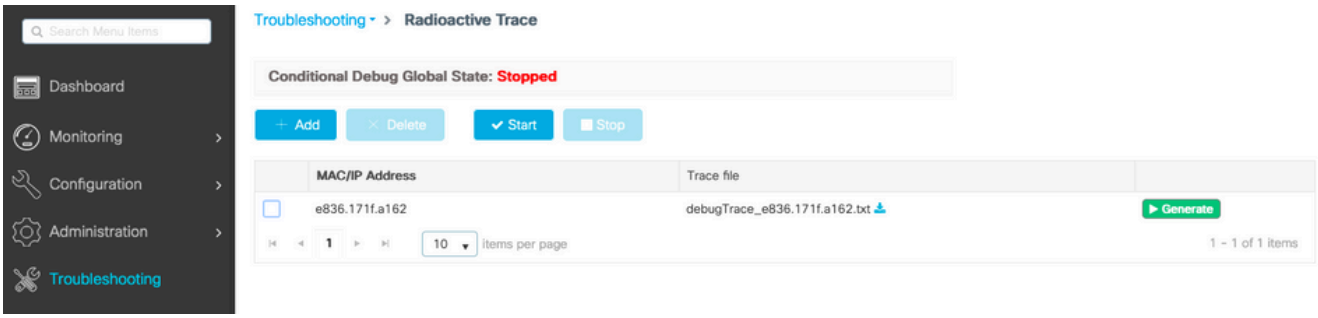
Event	5400 Authentication failed
Failure Reason	15039 Rejected per authorization profile
Resolution	Authorization Profile with ACCESS_REJECT attribute was selected as a result of the matching authorization rule. Check the appropriate Authorization policy rule-results.
Root cause	Selected Authorization Profile contains ACCESS_REJECT attribute
Username	E8:36:17:1F:A1:62



15048 Queried PIP - Radius.NAS-Port-Type
15048 Queried PIP - Network Access.UserName
15048 Queried PIP - IdentityGroup.Name (2 times)
15048 Queried PIP - EndPoints.LogicalProfile
15048 Queried PIP - Radius.Called-Station-ID
15048 Queried PIP - Network Access.AuthenticationStatus
15016 Selected Authorization Profile - DenyAccess
15039 Rejected per authorization profile
11003 Returned RADIUS Access-Reject

Other Attributes

ConfigVersionId	140
Device Port	58209
DestinationPort	1812
RadiusPacketType	AccessRequest
Protocol	Radius
NAS-Port	71111
Framed-MTU	1485
OriginalUserName	e836171fa162
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
IsThirdPartyDeviceFlow	false
AcsSessionID	nicoise26/356963261/1
UseCase	Host Lookup
SelectedAuthenticationIdentityStores	Internal Endpoints
IdentityPolicyMatchedRule	MAB
AuthorizationPolicyMatchedRule	Default
EndPointMACAddress	E8-36-17-1F-A1-62
ISEPolicySetName	Default
IdentitySelectionMatchedRule	MAB
DTLSSupport	Unknown
Network Device Profile	Cisco
Location	Location#All Locations
Device Type	Device Type#All Device Types
IPSEC	IPSEC#Is IPSEC Device#No
RADIUS Username	E8:36:17:1F:A1:62
NAS-Identifier	cwa-ssid
Device IP Address	10.48.71.120
CPMSessionID	7847300A0000012DFC227BF1
Called-Station-ID	00-27-e3-8f-33-a0:cwa-ssid
CiscoAVPair	service-type=Call Check, audit-session-id=7847300A0000012DFC227BF1, method=mab, client-iif-id=3003124185, vlan-id=1468, cisco-wlan-ssid=cwa-ssid,



이 경우 문제는 ACL 이름을 생성할 때 오타를 만들었고 ISE에서 반환한 ACL 이름과 일치하지 않거나 WLC에서 ISE에서 요청한 ACL과 같은 ACL이 없다고 불평하는 데 있습니다.

<#root>

2019/09/04 12:00:06.507 {wncd_x_R0-0}{1}: [client-auth] [24264]: (ERR): MAC: e836.171f.a162 client authz result: FAILURE 2019/09/04 12:00:06.51

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.