

Catalyst 9800 WLC로 DNA Spaces Captive Portal 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[네트워크 다이어그램](#)

[9800 컨트롤러를 Cisco DNA Spaces에 연결](#)

[DNA Spaces에 SSID 생성](#)

[9800 컨트롤러의 ACL 및 URL 필터 컨피그레이션](#)

[DNA 공간에 RADIUS 서버가 없는 종속 포털](#)

[9800 컨트롤러의 웹 인증 매개변수 맵 컨피그레이션](#)

[9800 컨트롤러에서 SSID를 생성합니다](#)

[9800 컨트롤러에서 정책 프로파일 구성](#)

[9800 컨트롤러에서 정책 태그 구성](#)

[DNA 공간에 RADIUS 서버가 있는 종속 포털](#)

[9800 컨트롤러의 웹 인증 매개변수 맵 컨피그레이션](#)

[9800 컨트롤러의 RADIUS 서버 컨피그레이션](#)

[9800 컨트롤러에서 SSID를 생성합니다](#)

[9800 컨트롤러에서 정책 프로파일 구성](#)

[9800 컨트롤러에서 정책 태그 구성](#)

[전역 매개변수 맵을 구성합니다](#)

[DNA Spaces에서 포털 생성](#)

[DNA 공간에 종속 포털 규칙 구성](#)

[DNA Spaces에서 특정 정보 가져오기](#)

[DNA Spaces에서 사용하는 IP 주소는 무엇입니까?](#)

[DNA Spaces 로그인 포털에서 사용하는 URL은 무엇입니까?](#)

[DNA Spaces에 대한 RADIUS 서버 세부사항은 무엇입니까?](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[일반적인 문제](#)

[항상 추적](#)

[조건부 디버깅 및 무선 활성 추적](#)

[성공한 시도의 예](#)

소개

이 문서에서는 Cisco DNA Spaces에서 종속 포털을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

이 문서에서는 Catalyst 9800 Wireless LAN Controller(C9800 WLC)의 클라이언트가 DNA Spaces를 외부 웹 인증 로그인 페이지로 사용할 수 있습니다.

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 9800 무선 컨트롤러에 대한 CLI(Command Line Interface) 또는 GUI(Graphic User Interface) 액세스
- Cisco DNA 공간

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 9800-L 컨트롤러 버전 16.12.2s

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

웹 인증은 신청자 또는 클라이언트 유틸리티가 필요 없는 간단한 레이어 3 인증 방법입니다. 이 작업을 수행할 수 있습니다

- a) C9800 WLC의 내부 페이지(있는 그대로 또는 수정 후)
- b) 맞춤형 로그인 번들을 C9800 WLC에 업로드한 경우
- c) 외부 서버에서 호스팅되는 사용자 지정 로그인 페이지

DNA Spaces에서 제공하는 종속 포털을 활용하는 것은 기본적으로 C9800 WLC에서 클라이언트에 대한 외부 웹 인증을 구현하는 방법입니다.

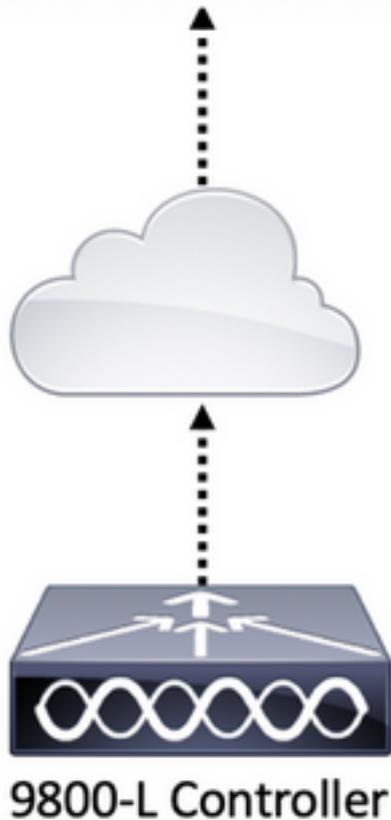
외부 webauth 프로세스에 대한 자세한 내용은 다음을 참조하십시오.

<https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/web-authentication/b-configuring-web-based-authentication-on-cisco-catalyst-9800-series-controllers/m-external-web-authentication-configuration.html>

C9800 WLC에서 가상 IP 주소는 전역 매개변수 맵으로 정의되며 일반적으로 192.0.2.1입니다

구성

네트워크 다이어그램



9800 컨트롤러를 Cisco DNA Spaces에 연결

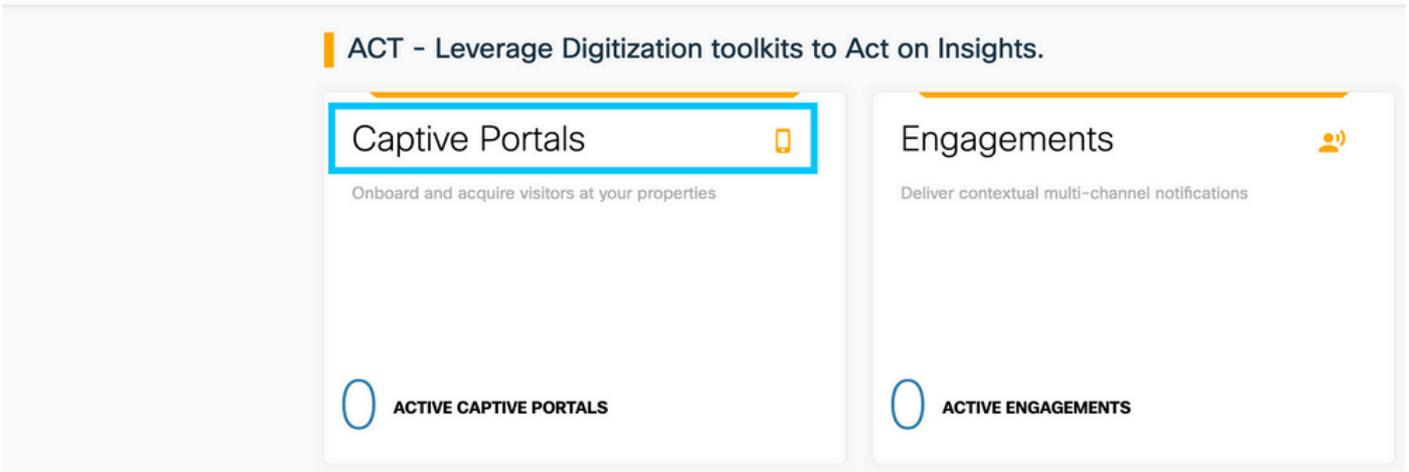
컨트롤러는 Direct Connect, DNA Spaces Connector 또는 CMX Tethering 옵션을 사용하여 DNA Spaces에 연결해야 합니다.

이 예에서는 종속 포털이 모든 설정에 대해 동일한 방식으로 구성되었지만 직접 연결 옵션이 사용 중입니다.

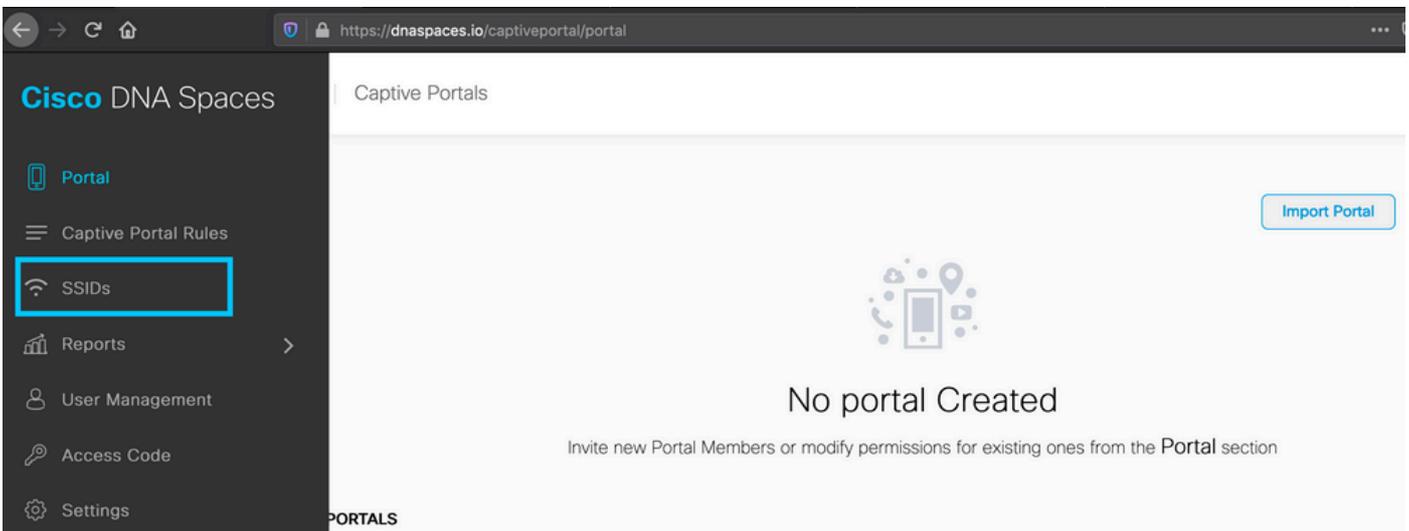
컨트롤러를 Cisco DNA Spaces에 연결하려면 HTTPS를 통해 Cisco DNA Spaces Cloud에 연결할 수 있어야 합니다. 9800 컨트롤러를 DNA Spaces에 연결하는 방법에 대한 자세한 내용은 DNA Spaces - [9800 Controller Direct Connect 링크를 참조하십시오.](#)

DNA Spaces에 SSID 생성

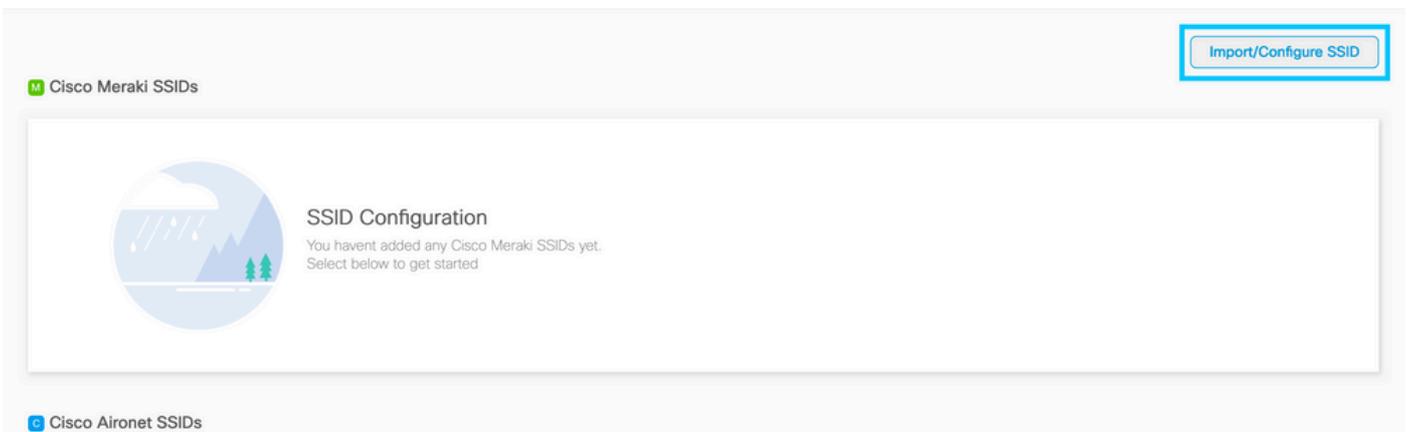
1단계. DNA Spaces의 대시보드에서 Captive Portals(종속 포털)를 클릭합니다.



2단계. 종속 포털 관련 메뉴를 열고 페이지의 왼쪽 상단 모서리에 있는 세 개의 회선 아이콘을 클릭한 다음 SSIDs를 클릭합니다.



3단계. Import/Configure SSID(SSID 가져오기/구성)를 클릭하고 "Wireless Network(무선 네트워크)" 유형으로 CUWN(CMX/WLC)을 선택하고 SSID 이름을 입력합니다.



9800 컨트롤러의 ACL 및 URL 필터 컨피그레이션

무선 클라이언트의 트래픽은 인증을 완료할 때까지 네트워크에서 허용되지 않습니다. 웹 인증의 경우, 이를 완료하기 위해 무선 클라이언트가 이 SSID에 연결되고 IP 주소를 수신한 다음 클라이언트

정책 관리자 상태가 Webauth_reqd 상태로 이동합니다. 클라이언트가 아직 인증되지 않았으므로 클라이언트 IP 주소에서 오는 모든 트래픽 소싱은 DHCP, DNS 및 HTTP(가로채기 및 리디렉션)를 제외하고 삭제됩니다.

기본적으로 9800은 웹 인증 WLAN을 설정할 때 하드 코딩된 사전 인증 ACL을 생성합니다. 이러한 하드코딩된 ACL은 DHCP, DNS 및 외부 웹 인증 서버로의 트래픽을 허용합니다. 나머지 모든 트래픽은 http 트래픽처럼 리디렉션됩니다.

그러나 특정 비 HTTP 트래픽 유형을 통과하도록 허용해야 하는 경우 사전 인증 ACL을 구성할 수 있습니다. 그런 다음 이 섹션의 1단계에서 기존 하드코딩된 사전 인증 ACL의 내용을 모방하고 필요에 맞게 확장해야 합니다.

1단계. 현재 하드코딩된 ACL 확인

CLI 구성:

```
Andressi-9800L#show ip access list
```

```
Extended IP access list WA-sec-34.235.248.212
```

```
10 permit tcp any host 34.235.248.212 eq www
20 permit tcp any host 34.235.248.212 eq 443
30 permit tcp host 34.235.248.212 eq www any
40 permit tcp host 34.235.248.212 eq 443 any
50 permit tcp any any eq domain
60 permit udp any any eq domain
70 permit udp any any eq bootpc
80 permit udp any any eq bootps
90 deny ip any any
```

```
Extended IP access list WA-v4-int-34.235.248.212
```

```
10 deny tcp any host 34.235.248.212 eq www
20 deny tcp any host 34.235.248.212 eq 443
30 permit tcp any any eq www
40 permit tcp any host 192.0.2.1 eq 443
```

WA-sec-34.235.248.212는 WA(Automatic Web Auth) 보안(sec) ACL 또는 포털 IP "34.235.248.212"이기 때문에 호출됩니다. 허용(허용 시) 또는 삭제(거부 시)할 항목을 보안 ACL에서 정의했습니다.

Wa-v4-int는 가로채기 ACL, 즉 punt ACL 또는 redirect ACL이며 리디렉션을 위해 CPU로 전송되는 것(허용 시) 또는 데이터 플레인으로 전송되는 것(거부 시)을 정의합니다.

WA-v4-int34.235.248.212는 클라이언트에서 들어오는 트래픽에 먼저 적용되며 DNA Spaces 포털 IP 34.235.248.212로 향하는 HTTP 트래픽을 데이터 플레인에 유지합니다(아직 삭제 또는 전달 작업이 아니라 데이터 플레인으로 전달합니다). 모든 HTTP(s) 트래픽을 CPU로 전송합니다(웹 서버에서 서비스하는 가상 IP 트래픽을 제외한 리디렉션의 경우). 다른 유형의 트래픽은 데이터 플레인에 제공됩니다.

WA-sec-34.235.248.212는 웹 인증 매개변수 맵에서 구성한 DNA 공간 IP 34.235.248.212에 대한 HTTP 및 HTTPS 트래픽을 허용하며, DNS 및 DHCP 트래픽도 허용하고 나머지는 삭제합니다. 가로챈 HTTP 트래픽은 이 ACL에 도달하기 전에 이미 가로채기되었으므로 이 ACL에서 다를 필요가 없습니다.

참고: ACL에서 허용할 DNA Spaces의 IP 주소를 가져오려면 ACL 컨피그레이션 섹션의 3단계에서 생성한 SSID에서 Configure Manually(수동으로 구성) 옵션을 클릭합니다. 예는 문서 끝부분의 "DNA Spaces에서 사용하는 IP 주소는 무엇입니까" 섹션에 있습니다.

DNA Spaces는 2개의 IP 주소를 사용하며 1단계의 메커니즘은 하나의 포털 IP만 허용합니다. 더 많은 HTTP 리소스에 대한 사전 인증 액세스를 허용하려면 URL 필터에 URL을 입력하는 웹 사이트와 관련된 IP에 대해 가로채기(리디렉션) 및 보안(사전 인증) ACL에 동적으로 허점을 만드는 URL 필터를 사용해야 합니다. DNS 요청은 9800에서 해당 URL의 IP 주소를 학습하고 이를 동적으로 ACL에 추가하기 위해 동적으로 스누핑됩니다.

2단계. DNA Spaces 도메인을 허용하도록 URL 필터를 구성합니다. Configuration(컨피그레이션) > Security(보안) > URL Filters(URL 필터)로 이동하고 +Add(추가)를 클릭하고 목록 이름을 구성하고, 유형으로 PRE-AUTH(사전 인증)를 선택하고, PERMIT(허용)로 작업을 선택하고 URL splash.dnaspaces.io(또는 EMEA 포털을 사용하는 경우 .eu)를 선택합니다.

CLI 구성:

```
Andressi-9800L(config)#urlfilter list
```

```
Andressi-9800L(config-urlfilter-params)#action permit
```

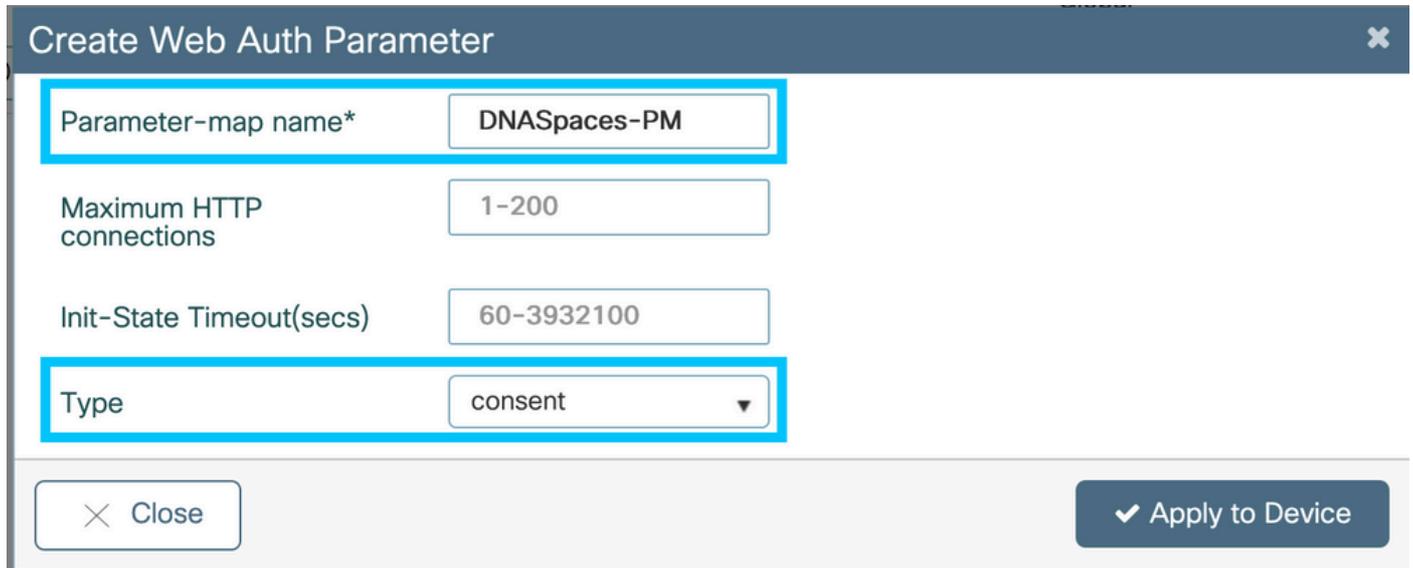
```
Andressi-9800L(config-urlfilter-params)#url splash.dnaspaces.io
```

RADIUS 서버를 사용하거나 사용하지 않도록 SSID를 구성할 수 있습니다. 종속 포털 규칙 컨피그레이션의 Actions(작업) 섹션에서 세션 기간, 대역폭 제한 또는 인터넷의 원활한 프로비저닝이 구성된 경우 SSID를 RADIUS 서버로 구성해야 합니다. 그렇지 않으면 RADIUS 서버를 사용할 필요가 없습니다. DNA Spaces의 모든 종류의 포털은 두 컨피그레이션에서 모두 지원됩니다.

DNA 공간에 RADIUS 서버가 없는 종속 포털

9800 컨트롤러의 웹 인증 매개변수 맵 컨피그레이션

1단계. Configuration(컨피그레이션) > Security(보안) > Web Auth(웹 인증)로 이동하고 +Add(추가)를 클릭하여 새 매개변수 맵을 만듭니다. 팝업 창에서 매개변수 맵 이름을 구성하고 유형으로 Consent를 선택합니다.



Create Web Auth Parameter

Parameter-map name*	DNASpaces-PM
Maximum HTTP connections	1-200
Init-State Timeout(secs)	60-3932100
Type	consent

Close Apply to Device

2단계. 이전 단계에서 구성한 매개변수 맵을 클릭하고 **Advanced(고급)** 탭으로 이동한 다음 Redirect for log-in URL(로그인 URL에 대한 리디렉션), Append for AP MAC Address(AP MAC 주소에 대한 추가), Append for Client MAC Address(클라이언트 MAC 주소에 대한 추가), Append for WLAN SSID and portal IPv4 Address(WLAN SSID 및 포털 IPv4 주소에 대한 추가)를 입력합니다. 그림과 같이 Update & Apply(업데이트 및 적용)를 클릭합니다.

General

Advanced

Redirect to external server

Redirect for log-in

Redirect On-Success

Redirect On-Failure

Redirect Append for AP MAC Address

Redirect Append for Client MAC Address

Redirect Append for WLAN SSID

Portal IPV4 Address

Portal IPV6 Address

Customized page

Login Failed Page 

Login Page 

Logout Page 

Login Successful Page 

✕ Cancel

 Update & Apply

참고: 스플래시 페이지 URL 및 IPv4 리디렉션 주소를 가져오려면 DNA Spaces의 SSID 페이지에서 Configure Manually(수동 구성) 옵션을 클릭합니다. 이 내용은 문서 끝부분의 "DNA Spaces 포털에서 사용하는 URL은 무엇입니까?"에 나와 있습니다

참고: Cisco DNA Spaces 포털은 2개의 IP 주소로 확인할 수 있지만, 9800 컨트롤러에서는 1개의 IP 주소만 구성할 수 있습니다. 이러한 IP 주소 중 하나를 선택하고 매개변수 맵에서 이를 포털 IPv4 주소로 구성합니다.

참고: 가상 IPv4 및 IPv6 주소는 모두 전역 웹 인증 매개변수 맵에서 구성됩니다. Virtual IPv6가 구성되지 않은 경우 클라이언트는 구성된 DNA Spaces 포털이 아닌 내부 포털로 리디렉션되는 경우가 있습니다. 따라서 가상 IP를 항상 구성해야 합니다. "192.0.2.1"은 Virtual IPv4로, FE80:0:0:903A::11E4는 Virtual IPV6로 구성할 수 있습니다. 다른 IP를 사용해야 할 이유는 거의 없거나 전혀 없습니다.

CLI 구성:

```
Andressi-9800L(config)#parameter-map type webauth
Andressi-9800L(config-params-parameter-map)#type consent
Andressi-9800L(config-params-parameter-map)#timeout init-state sec 600
Andressi-9800L(config-params-parameter-map)#redirect for-login
```

```
Andressi-9800L(config-params-parameter-map)#redirect append ap-mac tag ap_mac
Andressi-9800L(config-params-parameter-map)#redirect append wlan-ssid tag wlan
Andressi-9800L(config-params-parameter-map)#redirect append client-mac tag client_mac
Andressi-9800L(config-params-parameter-map)#redirect portal ipv4
```

```
Andressi-9800L(config-params-parameter-map)#logout-window-disabled
Andressi-9800L(config-params-parameter-map)#success-window-disabled
```

9800 컨트롤러에서 SSID를 생성합니다

1단계. Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로필) > WLANs(WLAN)로 이동하고 +Add(추가)를 클릭합니다. 프로파일 이름, SSID를 구성하고 WLAN을 활성화합니다. SSID 이름이 DNA Spaces에 SSID 생성 섹션의 3단계에서 구성된 이름과 동일한지 확인합니다.

Add WLAN ✕

General Security Advanced

Profile Name* Radio Policy

SSID* Broadcast SSID ENABLED

WLAN ID*

Status ENABLED

2단계. Security(보안) > Layer2로 이동합니다. Layer 2 Security Mode(레이어 2 보안 모드)를 None(없음)으로 설정하고 MAC Filtering(MAC 필터링)이 비활성화되어 있는지 확인합니다.

Add WLAN ✕

General **Security** Advanced

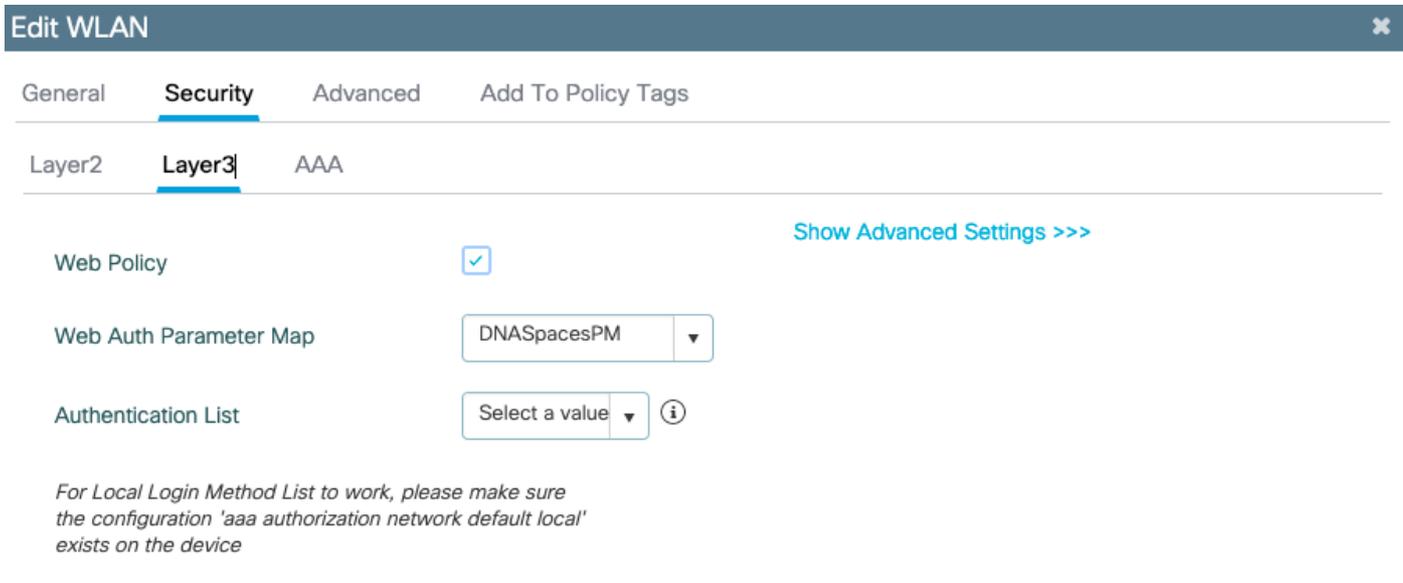
Layer2 Layer3 AAA

Layer 2 Security Mode Fast Transition

MAC Filtering Over the DS

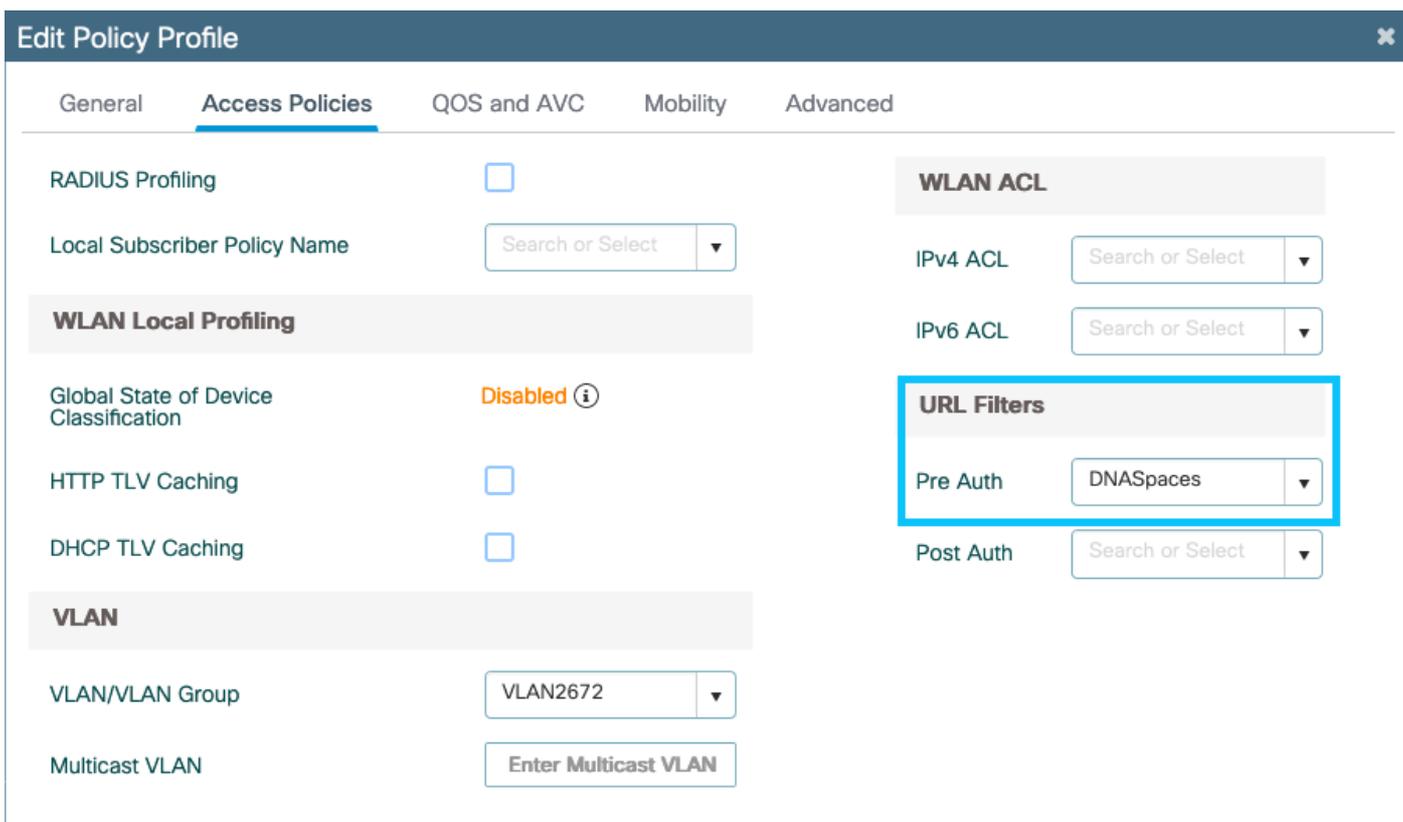
Transition Mode WLAN ID Reassociation Timeout

3단계. Security(보안) > Layer3로 이동합니다. 웹 정책을 활성화하고 웹 인증 매개변수 맵을 구성합니다. Apply to Device(디바이스에 적용)를 클릭합니다.



9800 컨트롤러에서 정책 프로파일 구성

1단계. Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로파일) > Policy(정책)로 이동하여 새 정책 프로파일을 생성하거나 기본 정책 프로파일을 사용합니다. Access Policies(액세스 정책) 탭에서 클라이언트 VLAN을 구성하고 URL 필터를 추가합니다.



9800 컨트롤러에서 정책 태그 구성

1단계. Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로파일) > Policy(정책)로 이동합니다. 새 정책 태그를 생성하거나 기본 정책 태그를 사용합니다. WLAN을 정책 태그의 정책 프로파일에 매핑합니다.

Add Policy Tag ✕

Name* DNASpaces-PT

Description Enter Description

▼ **WLAN-POLICY Maps: 1**

+ Add
✕ Delete

	WLAN Profile	Policy Profile
<input type="checkbox"/>	9800DNASpaces	DNASpaces-PP

⏪ < 1 > ⏩
10 items per page
1 - 1 of 1 items

➤ **RLAN-POLICY Maps: 0**

↶ Cancel
📄 Apply to Device

2단계. SSID를 브로드캐스트하려면 AP에 정책 태그를 적용합니다. Configuration(컨피그레이션) > Wireless(무선) > Access Points(액세스 포인트)로 이동하고 해당 AP를 선택한 다음 Policy Tag(정책 태그)를 추가합니다. 이렇게 하면 AP가 CAPWAP 터널을 다시 시작하고 9800 컨트롤러에 다시 조인합니다.

General

AP Name*

Location*

Base Radio MAC

Ethernet MAC

Admin Status ENABLED

AP Mode

Operation Status

Fabric Status

LED State ENABLED

LED Brightness Level

CleanAir [NSI Key](#)

Version

Primary Software Version	16.12.2.132
Predownloaded Status	N/A
Predownloaded Version	N/A
Next Retry Time	N/A
Boot Version	1.1.2.4
IOS Version	16.12.2.132
Mini IOS Version	0.0.0.0

IP Config

CAPWAP Preferred Mode	IPv6
SLAAC IPv6 Address	2001:172:16:30:ed0:f8ff:fe94:118c
Static IP (IPv4/IPv6)	<input type="checkbox"/>

Tags

⚠ Changing Tags will cause the AP to momentarily lose association with the Controller.

Policy

Site

RF

Time Statistics

Up Time	11 days 22 hrs 49 mins 12 secs
Controller Association Latency	3 mins 44 secs

CLI 구성:

```
Andressi-9800L(config)#wlan
```

```
Andressi-9800L(config-wlan)#no security wpa
Andressi-9800L(config-wlan)#no security wpa akm dot1x
Andressi-9800L(config-wlan)#no security wpa wpa2 ciphers aes
Andressi-9800L(config-wlan)#security web-auth
Andressi-9800L(config-wlan)#security web-auth parameter-map
Andressi-9800L(config-wlan)#no shutdown
```

```
Andressi-9800L(config)#wireless profile policy
```

```
Addresssi-9800L(config-wireless-policy) #vlan <id>
Addresssi-9800L(config-wireless-policy) #urlfilter list pre-auth-filter
```

```
Addresssi-9800L(config-wireless-policy) #no shutdown
```

```
Addresssi-9800L(config) #wireless tag policy
```

```
Addresssi-9800L(config-policy-tag) #wlan
```

DNA 공간에 RADIUS 서버가 있는 종속 포털

참고: DNA Spaces RADIUS 서버는 컨트롤러에서 오는 PAP 인증만 지원합니다.

9800 컨트롤러의 웹 인증 매개변수 맵 컨피그레이션

1단계. 웹 인증 매개변수 맵을 만듭니다. Configuration(컨피그레이션) > Security(보안) > Web Auth(웹 인증)로 이동하고 +Add(추가)를 클릭한 다음 매개변수 맵 이름을 구성하고 webauth를 유형으로 선택합니다.

Create Web Auth Parameter ✕

Parameter-map name*	DNASpaces-PM
Maximum HTTP connections	1-200
Init-State Timeout(secs)	60-3932100
Type	webauth ▼

✕ Close ✓ Apply to Device

2단계. 1단계에서 구성한 매개변수 맵을 클릭하고 Advanced(고급)를 클릭한 다음 Redirect for log-

in(로그인을 위해 리디렉션), Append for AP MAC Address(AP MAC 주소에 추가), Append for Client MAC Address(클라이언트 MAC 주소에 추가), Append for WLAN SSID and portal IPv4 Address(WLAN SSID 및 포털 IPv4 주소에 추가)를 입력합니다. **Update & Apply**를 클릭합니다.

General

Advanced

Redirect to external server

Redirect for log-in

Redirect On-Success

Redirect On-Failure

Redirect Append for AP MAC Address

Redirect Append for Client MAC Address

Redirect Append for WLAN SSID

Portal IPV4 Address

Portal IPV6 Address

Customized page

Login Failed Page 

Login Page 

Logout Page 

Login Successful Page 

✕ Cancel

 Update & Apply

참고: 스플래시 페이지 URL 및 IPv4 리디렉션 주소를 가져오려면, 섹션의 3단계에서 생성한 SSID에서 수동으로 구성 옵션을 클릭합니다. WLC Direct Connect에서 SSID 생성 섹션의 DNA Spaces에 SSID 생성 섹션에서 SSID 생성 액세스 제어 목록 컨피그레이션 생성 섹션을 각각 클릭합니다.

참고: Cisco DNA Spaces 포털은 2개의 IP 주소로 확인될 수 있지만 9800 컨트롤러에서는 1개의 IP 주소만 구성할 수 있습니다. 한 가지 경우 매개변수 맵에 포털 IPv4 주소로 구성할 IP 주소 중 하나를 선택합니다.

참고: 전역 웹 인증 매개변수 맵에 가상 IPv4 주소와 IPv6 주소가 모두 구성되어 있는지 확인하십시오. 가상 IPv6가 구성되어 있지 않으면 클라이언트가 구성된 DNA Spaces 포털 대신 내부 포털로 리디렉션되는 경우가 있습니다. 따라서 가상 IP를 항상 구성해야 합니다.

"192.0.2.1"은 Virtual IPv4로, FE80:0:0:0:903A::11E4는 Virtual IPV6로 구성할 수 있습니다. 다른 IP를 사용해야 할 이유는 거의 없거나 전혀 없습니다.

CLI 구성:

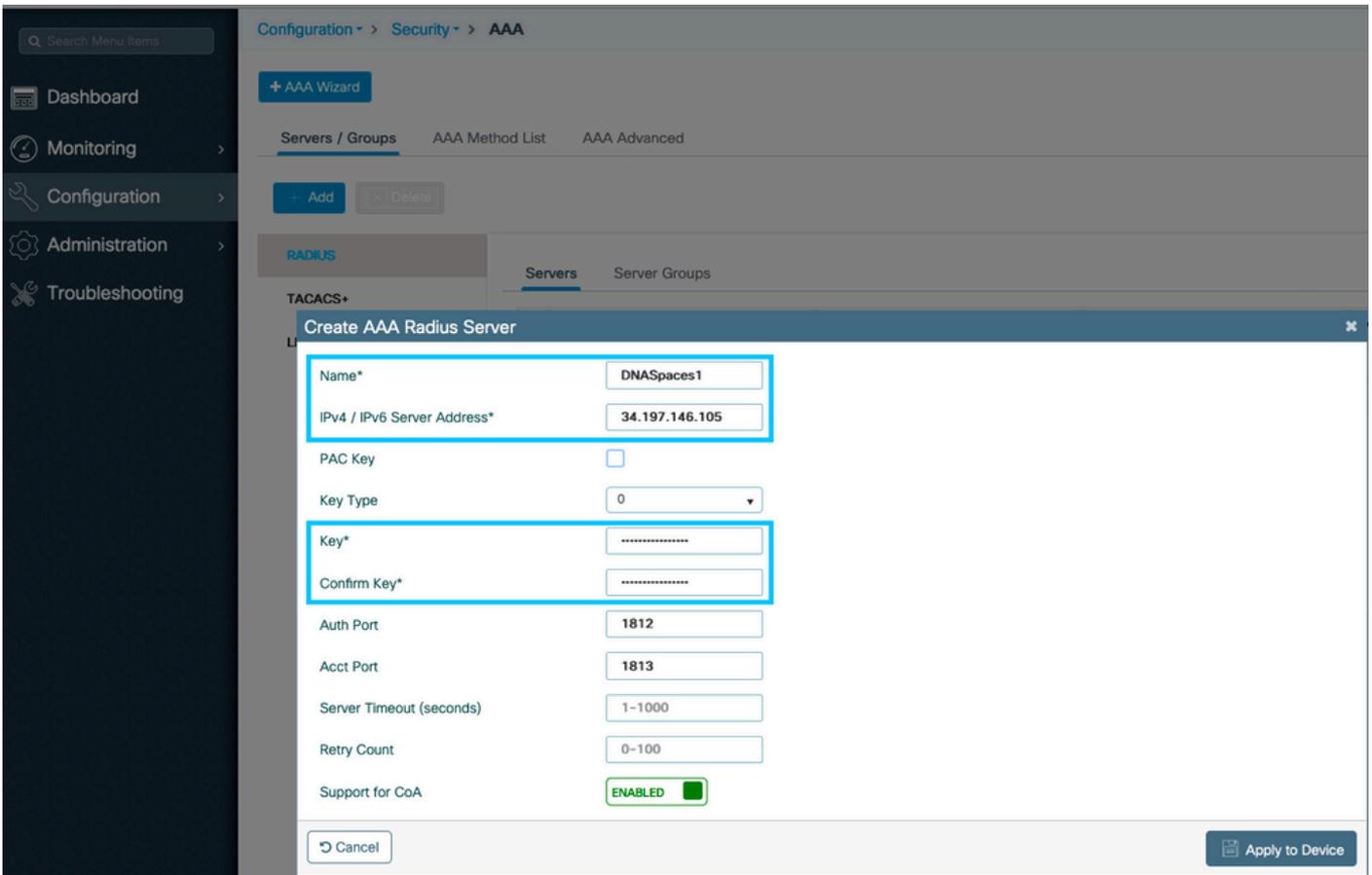
```
Andressi-9800L(config)#parameter-map type webauth
Andressi-9800L(config-params-parameter-map)#type webauth
Andressi-9800L(config-params-parameter-map)#timeout init-state sec 600
Andressi-9800L(config-params-parameter-map)#redirect for-login
```

```
Andressi-9800L(config-params-parameter-map)#redirect append ap-mac tag ap_mac
Andressi-9800L(config-params-parameter-map)#redirect append wlan-ssid tag wlan
Andressi-9800L(config-params-parameter-map)#redirect append client-mac tag client_mac
Andressi-9800L(config-params-parameter-map)#redirect portal ipv4
```

```
Andressi-9800L(config-params-parameter-map)#logout-window-disabled
Andressi-9800L(config-params-parameter-map)#success-window-disabled
```

9800 컨트롤러의 RADIUS 서버 컨피그레이션

1단계. RADIUS 서버를 구성합니다. Cisco DNA Spaces는 사용자 인증을 위해 RADIUS 서버 역할을 하며 2개의 IP 주소에서 응답할 수 있습니다. Configuration(컨피그레이션) > Security(보안) > AAA(AAA)로 이동하여 +Add(추가)를 클릭하고 두 RADIUS 서버를 구성합니다.



참고: 기본 및 보조 서버 모두에 대한 RADIUS IP 주소와 비밀 키를 가져오려면 **DNA Spaces**에서 SSID 생성 섹션의 3단계에서 생성한 SSID에서 **Configure Manually**(수동으로 구성) 옵션을 클릭하고 **RADIUS Server Configuration**(RADIUS 서버 컨피그레이션) 섹션으로 이동합니다.

2단계. RADIUS 서버 그룹을 구성하고 두 RADIUS 서버를 모두 추가합니다. Configuration(컨피그레이션) > Security(보안) > AAA > Servers/Groups(서버그룹) > RADIUS > Server Groups(서버 그룹)로 이동하고 +add(추가)를 클릭한 다음 서버 그룹 이름, MAC-Delimiter as Hyphen(MAC 구분 기호를 하이픈으로), MAC-Filtering as MAC(MAC 필터링)을 구성하고 두 개의 RADIUS 서버를 할당합니다.

+ AAA Wizard

Servers / Groups AAA Method List AAA Advanced

+ Add

- Delete

RADIUS

TACACS+

LDAP

Servers Server Groups

Name Server 1 Server 2

0 10 items per page

Create AAA Radius Server Group

Name* DNASpaces

Group Type RADIUS

MAC-Delimiter hyphen

MAC-Filtering mac

Dead-Time (mins) 1-1440

Available Servers

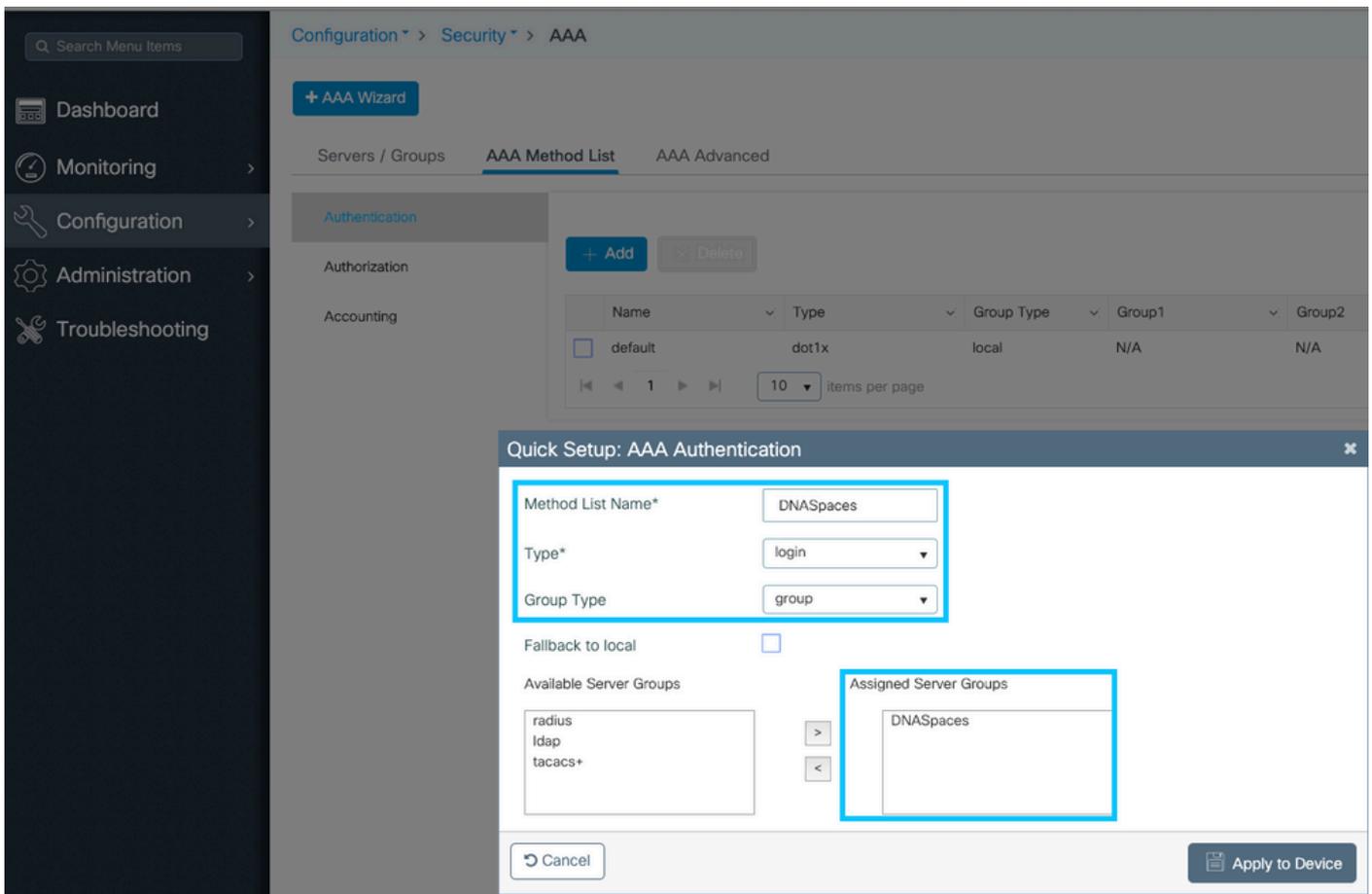
Assigned Servers

DNASpaces1
DNASpaces2

Cancel

Apply to Device

3단계. Authentication Method(인증 방법) 목록을 구성합니다. Configuration(컨피그레이션) > Security(보안) > AAA > AAA Method List(AAA 방법 목록) > Authentication(인증)으로 이동하고 +add(추가)를 클릭합니다. 메소드 목록 이름을 구성하고 유형으로 login을 선택하고 서버 그룹을 할당합니다.



4단계. Authorization Method(권한 부여 방법) 목록을 구성합니다. Configuration(컨피그레이션) > Security(보안) > AAA > AAA Method List(AAA 메서드 목록) > Authorization(권한 부여)으로 이동하고 +add(추가)를 클릭합니다. 메서드 목록 이름을 구성하고 유형으로 network를 선택하고 서버 그룹을 할당합니다.

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups **AAA Method List** AAA Advanced

Authentication

Authorization

Accounting

+ Add × Delete

Name	Type	Group Type	Group1	Group2
<input type="checkbox"/> MeshAP	credential-download	local	N/A	N/A

10 items per page

Quick Setup: AAA Authorization

Method List Name* DNASpaces

Type* network

Group Type group

Fallback to local

Authenticated

Available Server Groups

radius
ldap
tacacs+

> <

Assigned Server Groups

DNASpaces

Cancel Apply to Device

9800 컨트롤러에서 SSID를 생성합니다

1단계. Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로필) > WLANs(WLAN)로 이동하고 +Add(추가)를 클릭합니다. 프로파일 이름, SSID를 구성하고 WLAN을 활성화합니다. SSID 이름이 DNA Spaces에 SSID 생성 섹션의 3단계에서 구성된 이름과 동일한지 확인합니다.

Add WLAN ✕

General Security Advanced

Profile Name* Radio Policy ▼

SSID* Broadcast SSID

WLAN ID*

Status

2단계. Security(보안) > Layer2로 이동합니다. Layer 2 Security Mode(레이어 2 보안 모드)를 None(없음)으로 설정하고 MAC Filtering(MAC 필터링)을 활성화하고 Authorization List(권한 부여 목록)를 추가합니다.

Add WLAN ✕

General **Security** Advanced

Layer2 Layer3 AAA

Layer 2 Security Mode ▼

MAC Filtering

Transition Mode WLAN ID

Authorization List* ▼

Fast Transition ▼

Over the DS

Reassociation Timeout

3단계. Security(보안) > Layer3로 이동합니다. 웹 정책을 활성화하고 웹 인증 매개변수 맵 및 인증 목록을 구성합니다. Mac 필터 실패 시 활성화하고 사전 인증 ACL을 추가합니다. Apply to Device(디바이스에 적용)를 클릭합니다.

Add WLAN

General **Security** Advanced

Layer2 **Layer3** AAA

Web Policy
 Web Auth Parameter Map
 Authentication List

For Local Login Method List to work, please make sure the configuration 'aaa authorization network default local' exists on the device

<< Hide

On Mac Filter Failure

Splash Web Redirect DISABLED

Preauthentication ACL

IPv4

IPv6

9800 컨트롤러에서 정책 프로파일 구성

1단계. Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로파일) > Policy(정책)로 이동하여 새 정책 프로파일을 생성하거나 기본 정책 프로파일을 사용합니다. Access Policies(액세스 정책) 탭에서 클라이언트 VLAN을 구성하고 URL 필터를 추가합니다.

Edit Policy Profile

General **Access Policies** QOS and AVC Mobility Advanced

RADIUS Profiling

Local Subscriber Policy Name

WLAN Local Profiling

Global State of Device Classification Disabled ⓘ

HTTP TLV Caching

DHCP TLV Caching

VLAN

VLAN/VLAN Group

Multicast VLAN

WLAN ACL

IPv4 ACL

IPv6 ACL

URL Filters

Pre Auth

Post Auth

2단계. Advanced(고급) 탭에서 AAA Override(AAA 재정의)를 활성화하고 선택적으로 어카운팅 방법 목록을 구성합니다.

WLAN Timeout

Session Timeout (sec)

Idle Timeout (sec)

Idle Threshold (bytes)

Client Exclusion Timeout (sec)

DHCP

IPv4 DHCP Required

DHCP Server IP Address

Show more >>>

AAA Policy

Allow AAA Override

NAC State

Policy Name

Accounting List

Fabric Profile

Umbrella Parameter Map

mDNS Service Policy [Clear](#)

WLAN Flex Policy

VLAN Central Switching

Split MAC ACL

Air Time Fairness Policies

2.4 GHz Policy

5 GHz Policy

9800 컨트롤러에서 정책 태그 구성

1단계. Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로필) > Policy(정책)로 이동합니다. 새 정책 태그를 생성하거나 기본 정책 태그를 사용합니다. WLAN을 정책 태그의 정책 프로파일에 매핑합니다.

Add Policy Tag ✕

Name* DNASpaces-PT

Description Enter Description

▼ **WLAN-POLICY Maps: 1**

+ Add
✕ Delete

	WLAN Profile	Policy Profile
<input type="checkbox"/>	9800DNASpaces	DNASpaces-PP

⏪ ⏩ 1 ⏪ ⏩
10 items per page
 1 - 1 of 1 items

➤ **RLAN-POLICY Maps: 0**

↶ Cancel

📄 Apply to Device

2단계. SSID를 브로드캐스트하려면 AP에 정책 태그를 적용합니다. Configuration(컨피그레이션) > Wireless(무선) > Access Points(액세스 포인트)로 이동하고 해당 AP를 선택한 다음 Policy Tag(정책 태그)를 추가합니다. 이렇게 하면 AP가 CAPWAP 터널을 다시 시작하고 9800 컨트롤러에 다시 조인합니다.

General

AP Name*

Location*

Base Radio MAC

Ethernet MAC

Admin Status ENABLED

AP Mode

Operation Status

Fabric Status

LED State ENABLED

LED Brightness Level

CleanAir [NSI Key](#)

Version

Primary Software Version	16.12.2.132
Predownloaded Status	N/A
Predownloaded Version	N/A
Next Retry Time	N/A
Boot Version	1.1.2.4
IOS Version	16.12.2.132
Mini IOS Version	0.0.0.0

IP Config

CAPWAP Preferred Mode	IPv6
SLAAC IPv6 Address	2001:172:16:30:ed0:f8ff:fe94:118c
Static IP (IPv4/IPv6)	<input type="checkbox"/>

Tags

⚠ Changing Tags will cause the AP to momentarily lose association with the Controller.

Policy

Site

RF

Time Statistics

Up Time	11 days 22 hrs 49 mins 12 secs
Controller Association Latency	3 mins 44 secs

CLI 구성:

```
Andressi-9800L(config)#wlan
```

```
Andressi-9800L(config-wlan)#ip access-group web
```

```
Andressi-9800L(config-wlan)#no security wpa
Andressi-9800L(config-wlan)#no security wpa akm dot1x
```

```
Andressi-9800L(config-wlan)#no security wpa wpa2 ciphers aes
Andressi-9800L(config-wlan)#mac-filtering
```

```
Andressi-9800L(config-wlan)#security web-auth
Andressi-9800L(config-wlan)#security web-auth authentication-list
```

```
Andressi-9800L(config-wlan)#security web-auth on-macfilter-failure
Andressi-9800L(config-wlan)#security web-auth parameter-map
Andressi-9800L(config-wlan)#no shutdown
```

```
Andressi-9800L(config)#wireless profile policy
```

```
Andressi-9800L(config-wireless-policy)#aaa-override
Andressi-9800L(config-wireless-policy)#accounting-list
```

```
Andressi-9800L(config-wireless-policy)#vlan <id>
Andressi-9800L(config-wireless-policy)#urlfilter list pre-auth-filter
```

```
Andressi-9800L(config-wireless-policy)#no shutdown
```

```
Andressi-9800L(config)#wireless tag policy
```

```
Andressi-9800L(config-policy-tag)#wlan
```

전역 매개변수 맵을 구성합니다

권장되지 않는 단계: HTTPS 리디렉션을 허용하려면 이 명령을 실행하되, 클라이언트 운영 체제에서 종속 포털 탐지를 수행하고 CPU 사용률이 더 높아지며 항상 인증서 경고를 보내는 경우 클라이언트 HTTPS 트래픽에서 리디렉션할 필요가 없다는 점에 유의하십시오. 따라서 매우 구체적인 활용 사례에 필요하지 않은 경우에는 구성하지 않는 것이 좋습니다.

```
Andressi-9800L(config)#parameter-map type webauth global
Andressi-9800L(config-params-parameter-map)#intercept-https-enable
```

참고: Cisco Catalyst 9800 Series Wireless Controller에 설치된 가상 IP에 유효한 SSL 인증서가 있어야 합니다.

1단계. 확장명이 .p12인 서명된 인증서 파일을 TFTP 서버에 복사하고 이 명령을 실행하여 인증서를 9800 컨트롤러로 전송하고 설치합니다.

```
Andressi-9800L(config)#crypto pki import
```

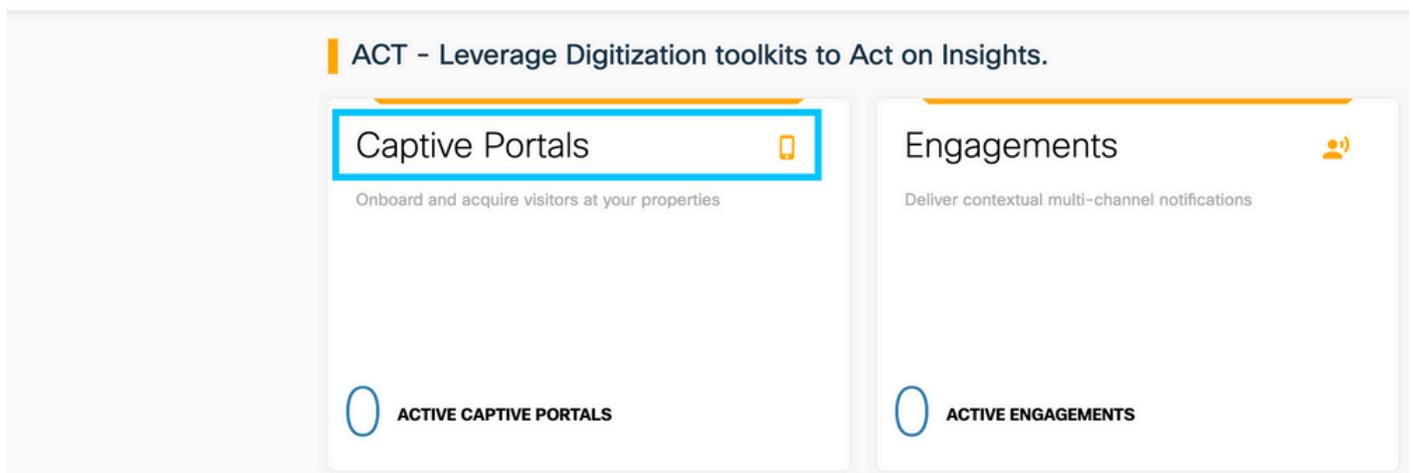
2단계. 설치된 인증서를 웹 인증 매개변수 맵에 매핑하려면 다음 명령을 실행합니다.

```
Andressi-9800L(config)#parameter-map type webauth global
Andressi-9800L(config-params-parameter-map)#trustpoint
```

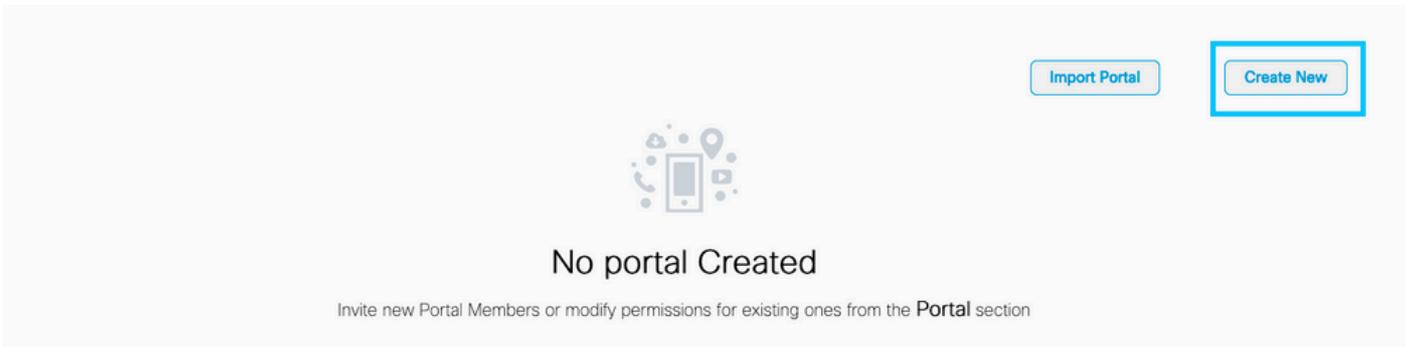
DNA Spaces에서 포털 생성

1단계. DNA Spaces의 대시보드에서 Captive Portals(중속 포털)를 클릭합니다.

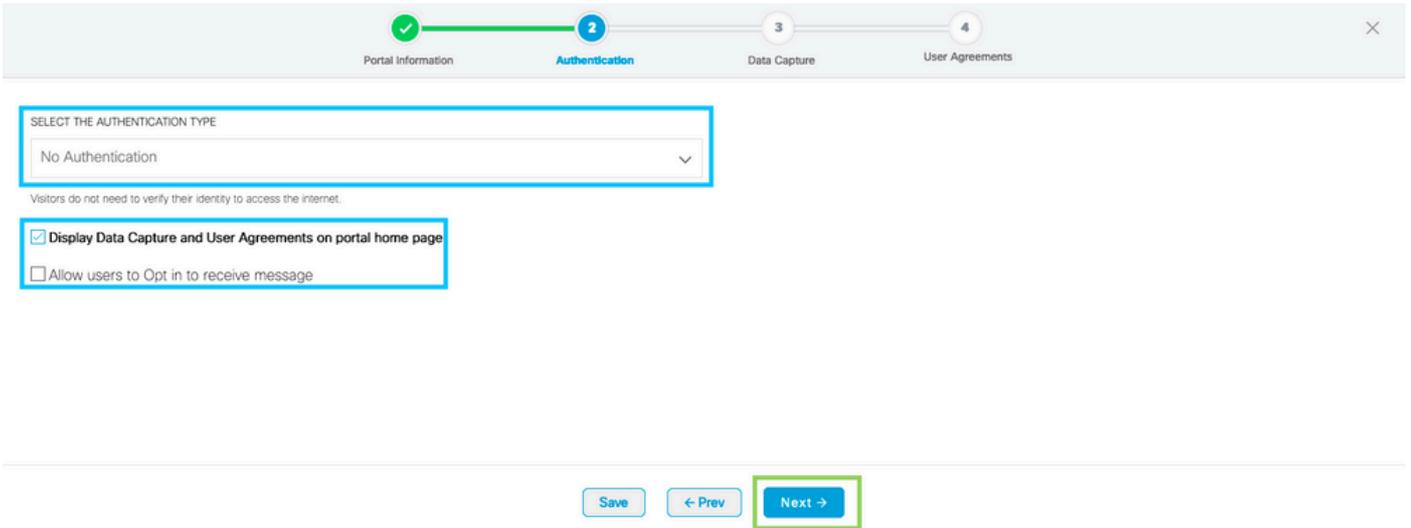
☰ Cisco DNA Spaces ACT



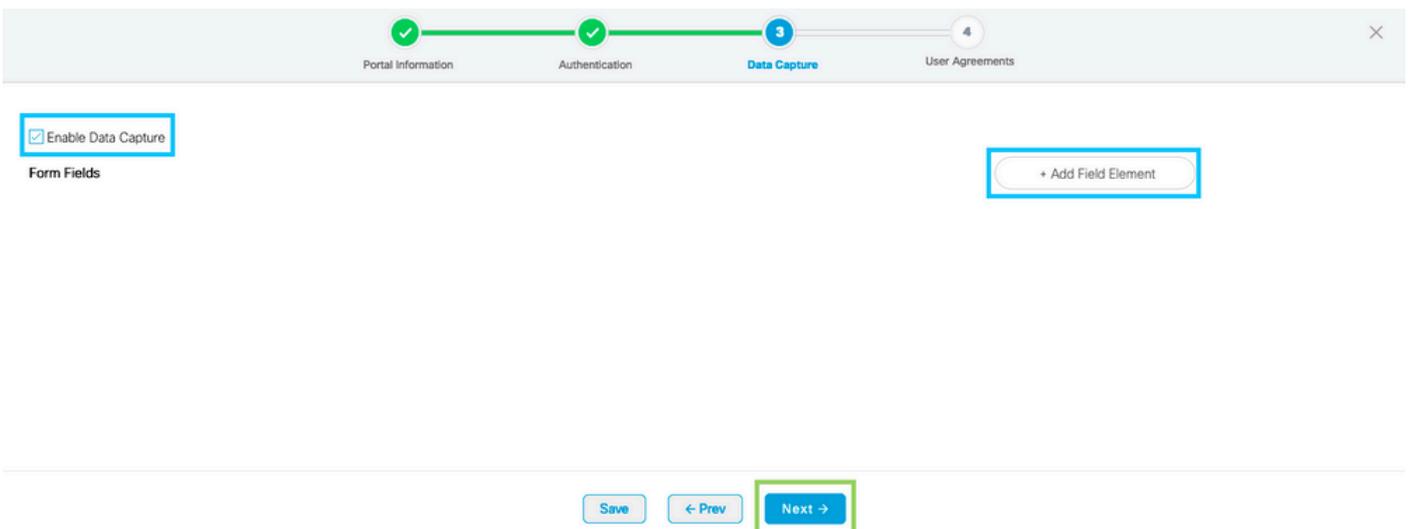
2단계. Create New(새로 만들기)를 클릭하고 포털 이름을 입력하고 포털을 사용할 수 있는 위치를 선택합니다.



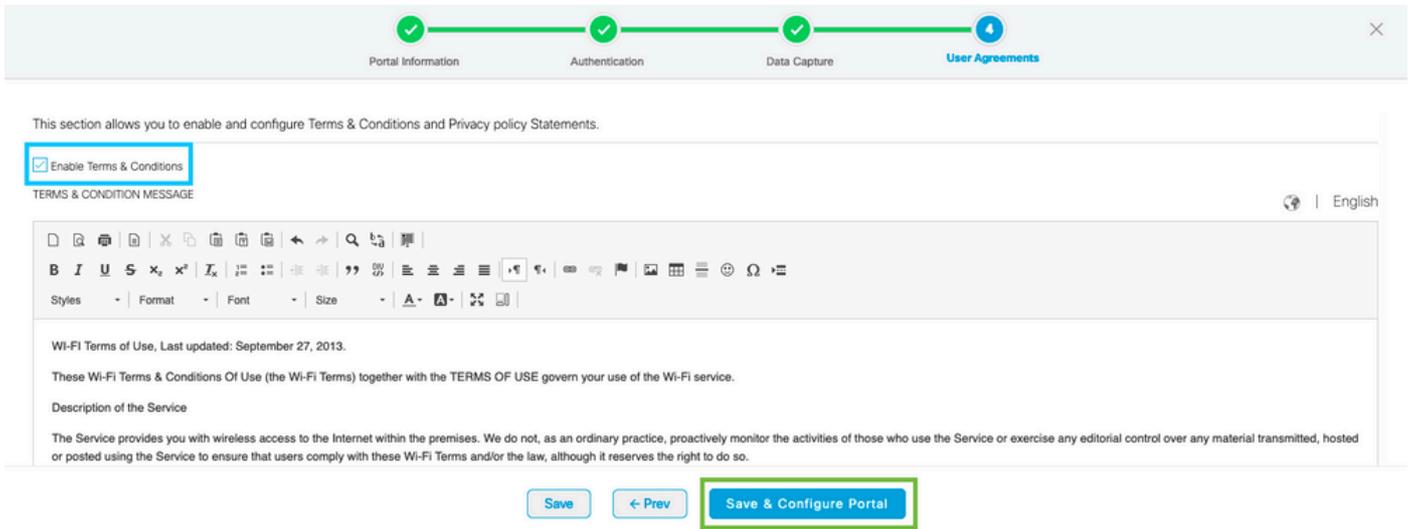
3단계. 인증 유형을 선택하고, 포털 홈 페이지에 데이터 캡처 및 사용자 계약을 표시할지 여부 및 사용자가 메시지 수신을 옵트인할 수 있는지 여부를 선택합니다. 다음을 클릭합니다.



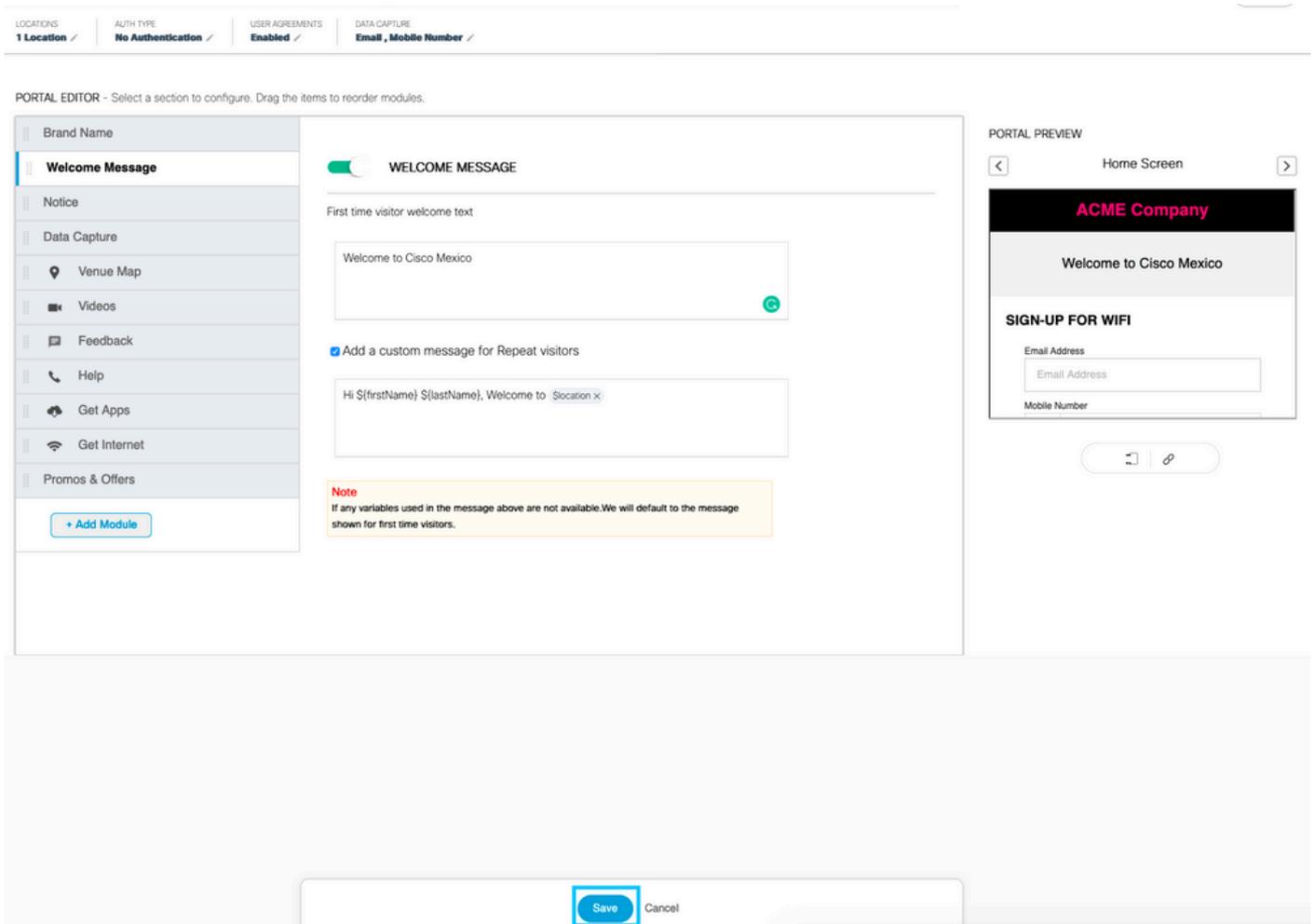
4단계. 데이터 캡처 요소를 구성합니다. 사용자로부터 데이터를 캡처하려면 Enable Data Capture(데이터 캡처 활성화) 상자를 선택하고 +Add Field Element(필드 요소 추가)를 클릭하여 원하는 필드를 추가합니다. 다음을 클릭합니다.



5단계. Enable Terms & Conditions(약관 활성화)를 선택하고 Save & Configure Portal(포털 저장 및 구성)을 클릭합니다.

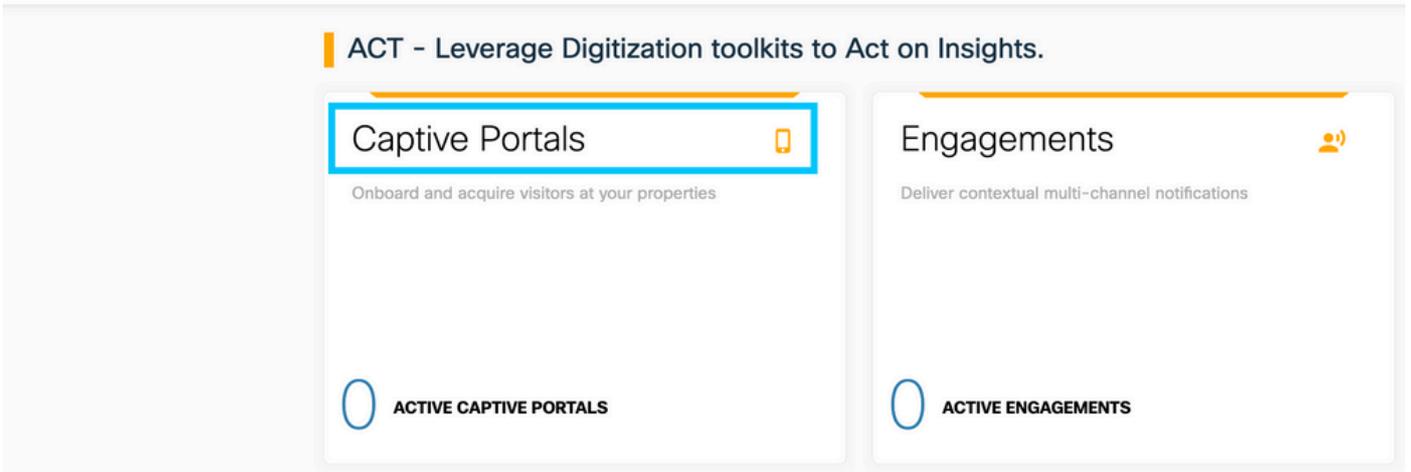


6단계. 필요에 따라 포털을 수정하고 Save(저장)를 클릭합니다.

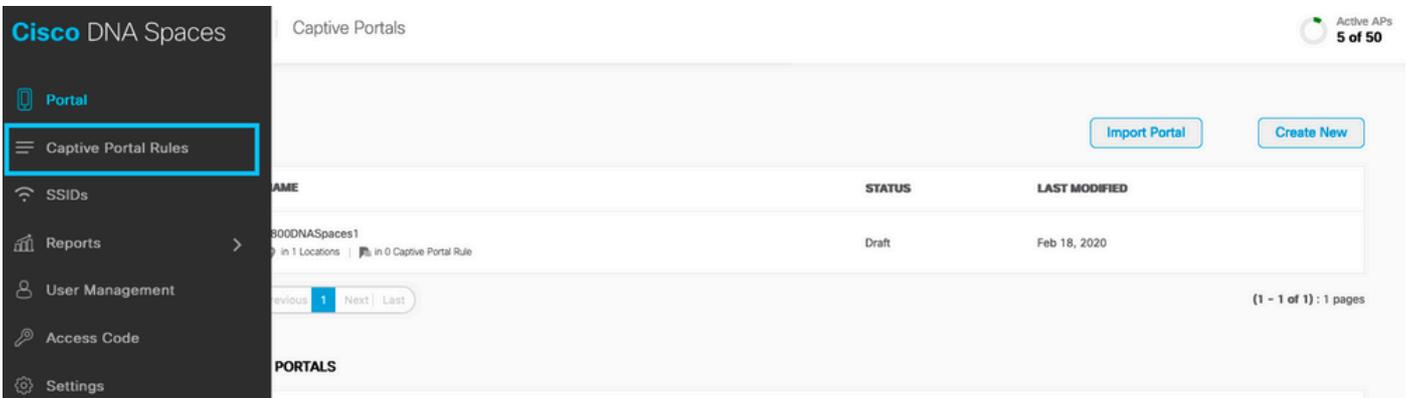


DNA 공간에 종속 포털 규칙 구성

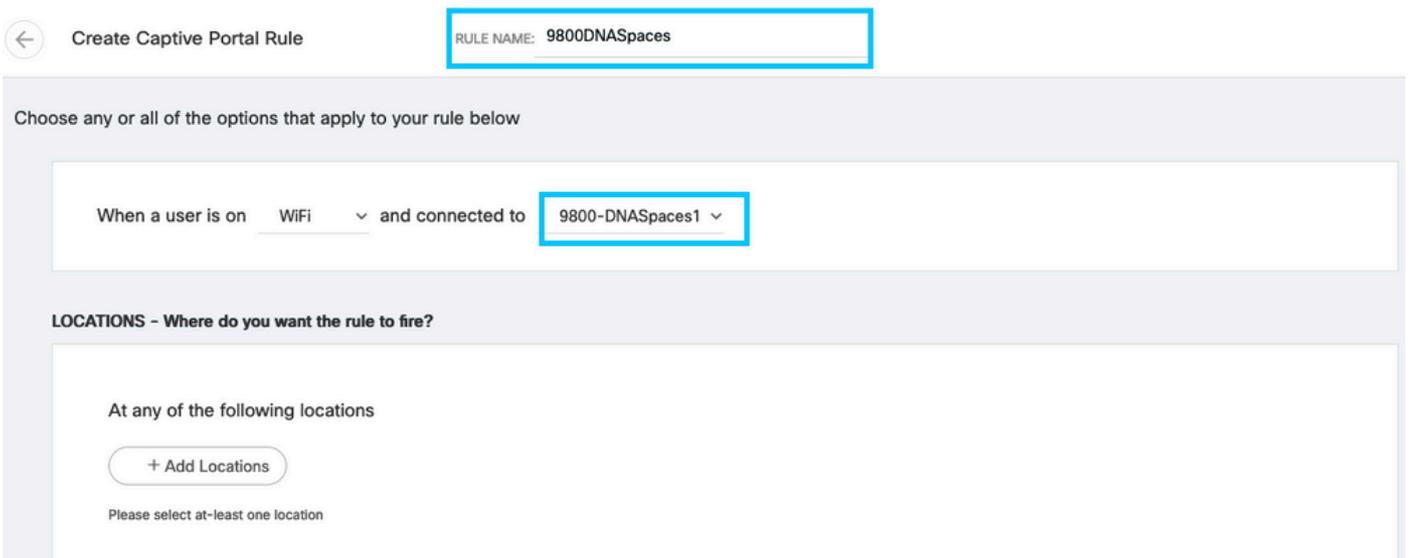
1단계. DNA Spaces의 대시보드에서 Captive Portals(종속 포털)를 클릭합니다.



2단계. 종속 포털 메뉴를 열고 종속 포털 규칙을 클릭합니다.



3단계. + Create New Rule을 클릭합니다. 규칙 이름을 입력하고 이전에 구성한 SSID를 선택합니다



4단계. 포털을 사용할 수 있는 위치를 선택합니다. LOCATIONS 섹션에서 + Add Locations를 클릭합니다. 위치 계층 구조에서 원하는 위치를 선택합니다.

Choose Locations

Location Hierarchy

MEX-EAST-1	<input type="checkbox"/>
+ 5508-1-CMX	<input type="checkbox"/>
+ 5508-2-Connector	<input type="checkbox"/>
+ 5520-1-DirectConnect	<input type="checkbox"/>
9800L-DirectConnect	<input checked="" type="checkbox"/>

Selected Locations

9800L-DirectConnect X

5단계. 종속 포털의 작업을 선택합니다. 이 경우, 규칙이 적용되면 포털이 표시됩니다. 저장 및 게시를 클릭합니다.

ACTIONS

- Show Captive Portal**
Choose a Portal to be displayed to Users when they connect to the wifi.
9800DNASpaces1
- Session Duration
- Bandwidth Limit
- Seamlessly Provision Internet
Directly provision internet without showing any authentication
- Deny Internet
Stop users from accessing the internet

Tags these users as
Choose - Associate/Disassociate users to chosen tags.
+ Add Tags

Trigger API

Save & Publish Save

SCHEDULE

ACTION
Show Captive Portal
Portal : 9800DNASpaces1

DNA Spaces에서 특정 정보 가져오기

DNA Spaces에서 사용하는 IP 주소는 무엇입니까?

DNA Spaces가 해당 지역의 포털에 사용하는 IP 주소를 확인하려면 DNA Space 홈의 Captival Portal 페이지로 이동합니다. 왼쪽 메뉴에서 **SSID**를 클릭한 다음 SSID 아래에서 **Configure manually(수동으로 구성)**를 클릭합니다. IP 주소는 ACL 예에서 언급됩니다. 이는 ACL 및 webauth 매개변수 맵에 사용할 포털의 IP 주소입니다. DNA Spaces는 제어 평면의 전체 NMSP/클라우드 연결에 다른 IP 주소를 사용합니다.



표시되는 팝업의 첫 번째 섹션에서 7단계는 ACL 정의에 언급된 IP 주소를 보여줍니다. 이러한 지침을 적용하고 ACL을 생성할 필요는 없으며 IP 주소만 기록해 두십시오. 해당 지역의 포털에서 사용하는 IP입니다

Configure



Creating the Access Control List

To create the access control list, perform the following steps:

- 1 Log in to the WLC Direct Connect with your WLC Direct Connect credentials.
- 2 Choose **Security > Access Control Lists > Access Control Lists**.
For FlexConnect local mode, choose **Security > Access Control Lists > FlexConnect ACLs**.
- 3 To add an ACL, click **New**.
- 4 In the **New** page that appears, enter the following:
 - a. In the **Access Control List Name** field, enter a name for the new ACL.

Note:
You can enter up to 32 alphanumeric characters.
 - b. Choose the ACL type as **IPv4**.

Note:
This option is not available for FlexConnect ACLs.
 - c. Click **Apply**.
- 5 When the **Access Control Lists** page reappears, click the name of the new ACL.
- 6 In the **Edit** page that appears, click **Add New Rule**. The **Rules > New** page appears.
- 7 Configure a rule for this ACL with the following wall garden ranges.

No	Dir	Source IP Address/Netmask	Destination IP Address/Netmask	Protocol	Source Port Range	Dest Port Range	DSCP	Action
1.	Any	0.0.0.0/0.0.0.0	54.77.207.183/255.255.255.255	TCP	Any	HTTPS	Any	Permit
2.	Any	54.77.207.183/255.255.255.255	0.0.0.0/0.0.0.0	TCP	HTTPS	Any	Any	Permit
3.	Any	0.0.0.0/0.0.0.0	34.252.175.120/255.255.255.255	TCP	Any	HTTPS	Any	Permit
4.	Any	34.252.175.120/255.255.255.255	0.0.0.0/0.0.0.0	TCP	HTTPS	Any	Any	Permit

DNA Spaces 로그인 포털에서 사용하는 URL은 무엇입니까?

해당 지역의 포털에 대해 어떤 로그인 포털 URL DNA Spaces를 사용하는지 확인하려면 DNA Space 홈의 Captival Portal 페이지로 이동합니다. 왼쪽 메뉴에서 **SSID**를 클릭한 다음 SSID 아래에서 **Configure manually(수동으로 구성)**를 클릭합니다.



나타나는 팝업에서 아래로 스크롤하고 두 번째 섹션인 7단계에서는 9800의 매개변수 맵에서 구성해야 하는 URL을 보여줍니다.

Creating the SSIDs in WLC Direct Connect

To create the SSIDs in the WLC Direct Connect, perform the following steps:

- 1 In the WLC Direct Connect main window, click the **WLANS** tab.
- 2 To create a WLAN, choose **Create New** from the drop-down list at the right side of the page, and click **Go**.
- 3 In the New page that appears, enter the WLAN details like Type, Profile Name, SSID, and so on.
- 4 Click **Apply**.
The WLAN added appears in the WLANS page.
- 5 Click the WLAN you have newly created.
- 6 Choose **Security > Layer 2**, and configure the Layer 2 Security as **None**.
- 7 In the **Layer 3 tab**, do the following configurations:
 - a. From the Layer 3 security drop-down list, choose **Web Policy**.
 - b. Choose the **Passthrough** radio button.
 - c. In the Preauthentication ACL area, from the IPv4 drop-down list, choose the ACL created earlier.
 - d. Select the Enable check box for the Sleeping Client.
 - e. Select the Enable check box for the Override Global Config.
 - f. From the Web Auth Type drop-down list, choose **External**.
 - g. In the URL field that appears, enter the Cisco DNA Spaces splash URL.

<https://splash.dnaspaces.eu/p2/emeabru2>

DNA Spaces에 대한 RADIUS 서버 세부사항은 무엇입니까?

사용해야 하는 RADIUS 서버 IP 주소와 공유 암호를 알아보려면 DNA Space 홈의 Captival Portal(포털 포털) 페이지로 이동하십시오. 왼쪽 메뉴에서 **SSID**를 클릭한 다음 SSID 아래에서 **Configure manually(수동으로 구성)**를 클릭합니다.



표시되는 팝업에서 세 번째 섹션(RADIUS)에서 아래로 스크롤하고 7단계에서는 radius 인증을 위한 IP/포트 및 공유 암호를 제공합니다. 어카운팅은 선택 사항이며 12단계에서 다룹니다.

- 7 In the New page that appears, enter the details of the radius server for authentication, such as server IP address, port number, and secret key, select the Server Status as **Enabled**, and click **Apply**.

Host: 52.51.31.103,34.241.1.84
Port: 1812
Secret Key: emeab1299E2PqvJK

- 8 Choose **Radius > Accounting**.

The Radius Accounting Servers page appears.

- 9 From the Acct Called Station ID Type, choose **AP MAC Address:SSID**.

- 10 From the MAC Delimiter drop-down list, choose **Hyphen**.

- 11 Click **New**.

- 12 In the New page that appears, enter the details of the radius server for accounting, such as server IP address, port number, and secret key, select the Server Status as **Enabled**, and click **Apply**.

Host: 52.51.31.103,34.241.1.84
Port: 1813
Secret Key: emeab1299E2PqvJK

다음을 확인합니다.

SSID에 연결된 클라이언트의 상태를 확인하려면 **Monitoring(모니터링) > Clients(클라이언트)**로 이동하여 디바이스의 MAC 주소를 클릭하고 **Policy Manager State(정책 관리자 상태)**를 찾습니다.

Client	
360 View General QOS Statistics ATF Statistics Mobility History Call Statistics	
Client Properties AP Properties Security Information Client Statistics QOS Properties	
Wireless LAN Id	1
WLAN Profile Name	9800-DNASpaces1
Wireless LAN Network Name (SSID)	9800-DNASpaces1
BSSID	10b3.d694.00ef
Uptime(sec)	64 seconds
Session Timeout	1800 sec (Remaining time: 1762 sec)
Session Warning Time	Timer not running
Client Active State	Active
Power Save mode	OFF
Current TxRateSet	m2 ss1
Supported Rates	9.0,18.0,36.0,48.0,54.0
Join Time Of Client	03/11/2020 17:47:25 Central
Policy Manager State	Run

문제 해결

일반적인 문제

1. 컨트롤러의 가상 인터페이스에 구성된 IP 주소가 없는 경우, 클라이언트는 매개변수 맵에 구성된 리디렉션 포털 대신 내부 포털로 리디렉션됩니다.
2. 클라이언트가 DNA Spaces의 포털로 리디렉션되는 동안 503 오류가 발생하는 경우 컨트롤러가 DNA Spaces의 위치 계층 구조에 구성되었는지 확인합니다.

항상 추적

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: 생성되는 로그의 양에 따라 몇 시간에서 며칠로 돌아갈 수 있습니다.

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

1단계. 문제가 발생했을 때까지의 시간에 로그를 추적할 수 있도록 컨트롤러 현재 시간을 확인합니다.

```
# show clock
```

2단계. 시스템 컨피그레이션에 따라 컨트롤러 버퍼 또는 외부 syslog에서 syslog를 수집합니다. 이렇게 하면 시스템 상태 및 오류가 있는 경우 이를 빠르게 확인할 수 있습니다.

```
# show logging
```

3단계. 디버그 조건이 활성화되었는지 확인합니다.

```
# show debugging
Cisco IOS-XE Conditional Debug Configs:
```

```
Conditional Debug Global State: Stop
```

```
Cisco IOS-XE Packet Tracing Configs:
```

```
Packet Infra debugs:
```

```
Ip Address _____ Port _____
-----|-----
```

참고: 나열된 조건이 있는 경우, 이는 활성화된 조건(mac 주소, IP 주소 등)이 발생하는 모든 프로세스에 대한 추적이 디버그 레벨로 기록되고 있음을 의미합니다. 이로 인해 로그의 볼륨이 증가합니다. 따라서 적극적으로 디버깅하지 않을 때는 모든 조건을 지우는 것이 좋습니다.

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

```
# 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.

```
# 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 대한 디버그 레벨 추적이 제공됩니다. 조건부 디버깅을 활성화하려면 다음 단계를 수행합니다.

1단계. 활성화된 디버그 조건이 없는지 확인합니다.

```
# clear platform condition all
```

2단계. 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.

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

참고: 한 번에 둘 이상의 클라이언트를 모니터링하려면 mac 주소당 debug wireless mac

<aaaa.bbb.cccc> 명령을 실행합니다.

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

3단계. 모니터링할 문제나 동작을 재현합니다.

4단계. 기본 또는 구성된 모니터 시간이 끝나기 전에 문제가 재현되는 경우 디버그를 중지합니다.

```
# no debug wireless mac <aaaa.bbbb.cccc>
```

모니터링 시간이 경과하거나 무선 디버그가 중단되면 9800 WLC는 다음과 같은 이름의 로컬 파일을 생성합니다.

```
ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

5단계. MAC 주소 활동의 파일을 수집합니다. RA 추적 .log를 외부 서버에 복사하거나 출력을 화면에 직접 표시할 수 있습니다.

RA 추적 파일의 이름을 확인합니다

```
# dir bootflash: | inc ra_trace
```

파일을 외부 서버에 복사:

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

콘텐츠 표시:

```
# more bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

6단계. 근본 원인이 아직 명확하지 않은 경우 디버그 레벨 로그를 더 자세히 보여주는 내부 로그를 수집합니다. 이미 수집되어 내부적으로 저장된 디버그 로그만 더 자세히 살펴볼 것이므로 클라이언트를 다시 디버깅할 필요는 없습니다.

```
# 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 프로세스의 모든 로깅 레벨에 대한 추적을 반환하며 상당히 방대합니다. 이러한 추적을 구문 분석하는 데 도움이 되도록 Cisco TAC를 활성화하십시오.

ra-internal-FILENAME.txt를 외부 서버에 복사하거나 출력을 화면에 직접 표시할 수 있습니다.

파일을 외부 서버에 복사:

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

콘텐츠 표시:

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

7단계. 디버그 조건을 제거합니다.

```
# clear platform condition all
```

참고: 트러블슈팅 세션 후에는 항상 디버그 조건을 제거해야 합니다.

성공한 시도의 예

RADIUS 서버가 없는 SSID에 연결하는 동안 연결/인증 프로세스 중에 각 단계를 성공적으로 식별하기 위한 RA_traces의 출력입니다.

802.11 연결/인증:

```
Association received. BSSID 10b3.d694.00ee, WLAN 9800DNASpaces, Slot 1 AP 10b3.d694.00e0, 2802AP-9800L
Received Dot11 association request. Processing started,SSID: 9800DNASpaces1, Policy profile: DNASpaces-PP, AP Name: 2802AP-9800L, Ap Mac Address: 10b3.d694.00e0 BSSID MAC0000.0000.0000 wlan ID: 1RSSI: 0, SNR: 32
Client state transition: S_CO_INIT -> S_CO_ASSOCIATING
dot11 send association response. Sending association response with resp_status_code: 0
dot11 send association response. Sending assoc response of length: 144 with resp_status_code: 0, DOT11_STATUS: DOT11_STATUS_SUCCESS
Association success. AID 1, Roaming = False, WGB = False, 11r = False, 11w = False
DOT11 state transition: S_DOT11_INIT -> S_DOT11_ASSOCIATED
Station Dot11 association is successful
```

IP 학습 프로세스:

```
IP-learn state transition: S_IPLEARN_INIT -> S_IPLEARN_IN_PROGRESS
Client IP learn successful. Method: ARP IP: 10.10.30.42
IP-learn state transition: S_IPLEARN_IN_PROGRESS -> S_IPLEARN_COMPLETE
Received ip learn response. method: IPLEARN_METHOD_AR
```

레이어 3 인증:

```
Triggered L3 authentication. status = 0x0, Success
Client state transition: S_CO_IP_LEARN_IN_PROGRESS -> S_CO_L3_AUTH_IN_PROGRESS
L3 Authentication initiated. LWA
Client auth-interface state transition: S_AUTHIF_L2_WEBAUTH_DONE -> S_AUTHIF_WEBAUTH_PENDING

Client auth-interface state transition: S_AUTHIF_L2_WEBAUTH_DONE -> S_AUTHIF_WEBAUTH_PENDING
[webauth-httpd] [17798]: (info): capwap_90000005[34e1.2d23.a668][10.10.30.42]GET rcvd when in INIT state
[webauth-httpd] [17798]: (info): capwap_90000005[34e1.2d23.a668][10.10.30.42]HTTP GET request
[webauth-httpd] [17798]: (info): capwap_90000005[34e1.2d23.a668][10.10.30.42]Parse GET, src [10.10.30.42] dst [13.107.4.52] url [http://www.msftconnecttest.com/connecttest.txt]
[webauth-httpd] [17798]: (info): capwap_90000005[34e1.2d23.a668][10.10.30.42]Retrieved user-agent = Microsoft NCSI
[webauth-httpd] [17798]: (info): capwap_90000005[34e1.2d23.a668][10.10.30.42]GET rcvd when in LOGIN state
[webauth-httpd] [17798]: (info): capwap_90000005[34e1.2d23.a668][10.10.30.42]HTTP GET request
```

```
[webauth-httpd] [17798]: (info): capwap_90000005[34e1.2d23.a668][10.10.30.42]Parse GET, src  
[10.10.30.42] dst [151.101.24.81] url [http://www.bbc.com/]  
[webauth-httpd] [17798]: (info): capwap_90000005[34e1.2d23.a668][10.10.30.42]Retrieved user-  
agent = Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko  
[webauth-httpd] [17798]: (info): capwap_90000005[34e1.2d23.a668][10.10.30.42]POST rcvd when in  
LOGIN state
```

레이어 3 인증에 성공하면 클라이언트를 RUN 상태로 이동합니다.

```
[34e1.2d23.a668:capwap_90000005] Received User-Name 34E1.2D23.A668 for client 34e1.2d23.a668  
L3 Authentication Successful. ACL:[]  
Client auth-interface state transition: S_AUTHIF_WEBAUTH_PENDING -> S_AUTHIF_WEBAUTH_DONE  
%CLIENT_ORCH_LOG-6-CLIENT_ADDED_TO_RUN_STATE: Username entry (34E1.2D23.A668) joined with ssid  
(9800DNASpaces) for device with MAC: 34e1.2d23.a668  
Managed client RUN state notification: 34e1.2d23.a668  
Client state transition: S_CO_L3_AUTH_IN_PROGRESS -> S_CO_RU
```

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.