AireOS 컨트롤러를 사용하는 DNA Spaces 종속 포털 컨피그레이션 예

목차

소개

이 문서에서는 AireOS 컨트롤러와 함께 Cisco DNA Spaces를 사용하여 종속 포털을 구성하는 방법에 대해 설명합니다.

기고자: Andres Silva Cisco TAC 엔지니어

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 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.

- 5520 Wireless LAN Controller 버전 8.10.112.0

구성

네트워크 다이어그램

설정

WLC를 Cisco DNA Spaces에 연결

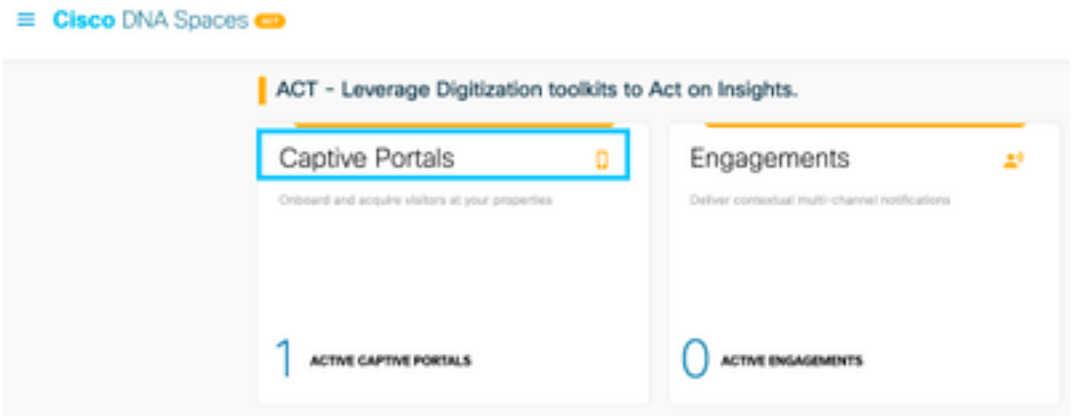
사용 가능한 설정 중 하나를 사용하여 DNA Spaces에 컨트롤러를 연결해야 합니다. Direct Connect, DNA Spaces Connector 또는 CMX Tethering을 통해 연결할 수 있습니다.

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

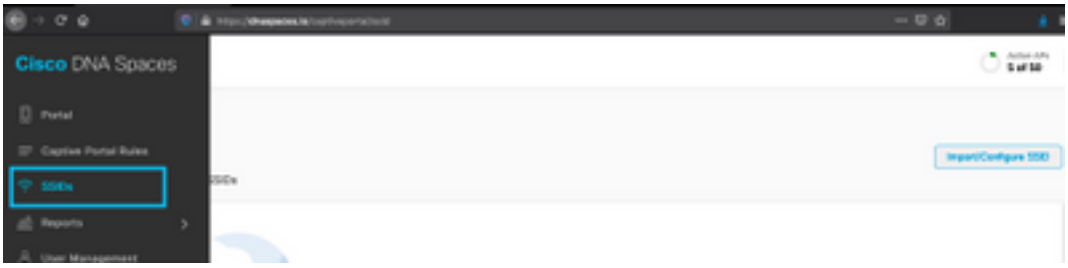
컨트롤러를 Cisco DNA Spaces에 연결하려면 HTTPS를 통해 Cisco DNA Spaces 클라우드에 연결할 수 있어야 합니다. 컨트롤러를 DNA Spaces에 연결하는 방법에 대한 자세한 내용은 다음 링크를 참조하십시오. DNA Spaces Direct Connect 컨피그레이션 예

DNA Spaces에 SSID 생성

1단계. DNA Spaces의 **대시보드**에서 Captive Portals(종속 포털)를 클릭합니다.



2단계. 페이지의 왼쪽 상단 모서리에 있는 3개의 회선 아이콘을 클릭하여 종속 포털 메뉴를 열고 SSIDs를 **클릭합니다.**

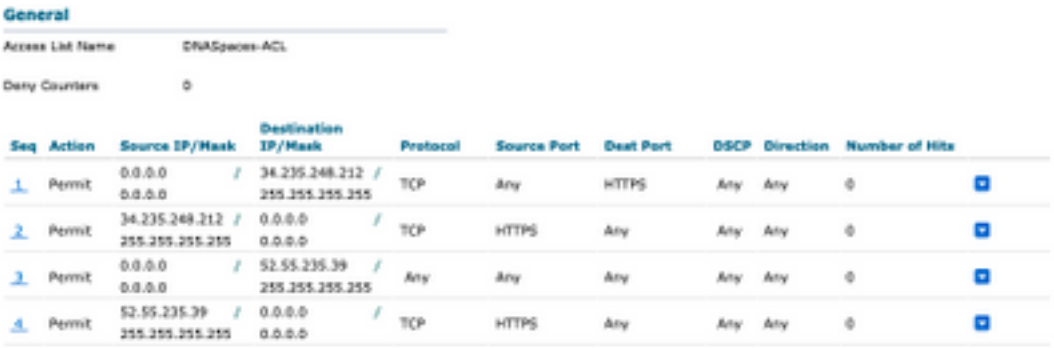


3단계. Import/**Configure SSID(SSID 가져오기/**구성)를 클릭하고 "Wireless Network(무선 네트워크)" 유형으로 CUWN**(CMX/**WLC)을 선택하고 SSID 이름을 입력합니다.

컨트롤러의 ACL 컨피그레이션

사전 인증 ACL은 웹 인증 SSID이므로 필요합니다. 무선 디바이스가 SSID에 연결하고 IP 주소를 수신하는 즉시 디바이스의 정책 관리자 상태가 Webauth_**Reqd 상태**로 이동하고 ACL이 클라이언트 세션에 적용되어 디바이스가 연결할 수 있는 리소스를 제한합니다.

1단계. Security(**보안) > Access Control Lists(액세스 제어 목록) > Access Control Lists(액세스 제어 목록)로 이동하고 New(새로 만들기)**를 클릭한 다음 무선 클라이언트와 DNA Spaces 간의 통신을 허용하는 규칙을 다음과 같이 구성합니다. IP 주소를 사용 중인 계정의 DNA Spaces에서 제공한 주소로 바꿉니다.



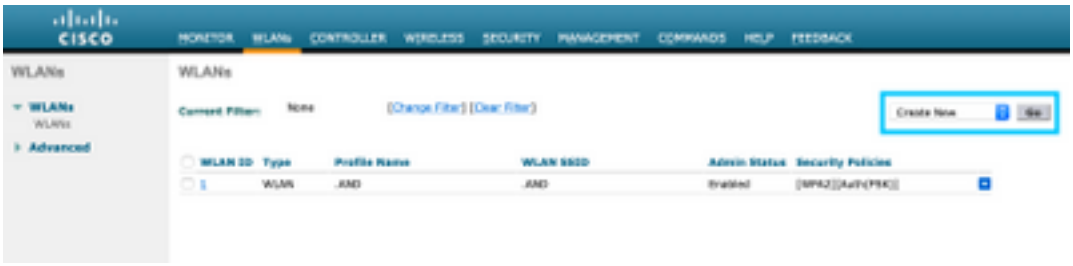
참고: ACL에서 허용할 DNA Spaces의 IP 주소를 가져오려면 ACL 컨피그레이션 섹션의 3단계에서 생성한 SSID에서 Configure Manually(수동으로 **구성) 옵션을** 클릭합니다.

RADIUS 서버를 사용하거나 사용하지 않도록 SSID를 구성할 수 있습니다. 종속 포털 규칙 컨피그레이션의 **Actions 섹션**에서 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.

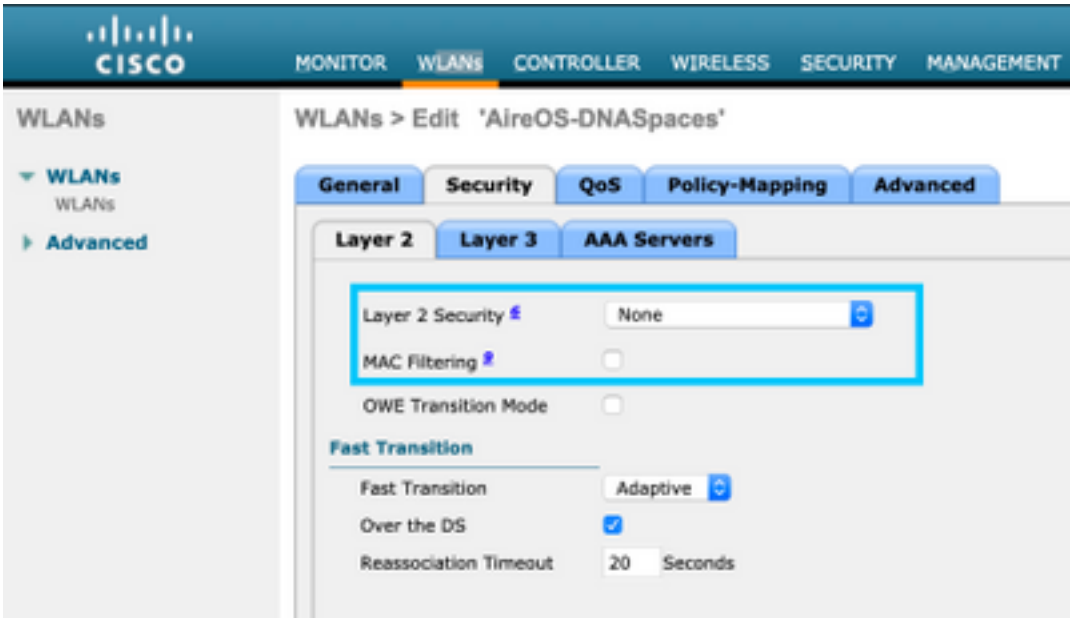
DNA 공간에 RADIUS 서버가 없는 종속 포털

컨트롤러의 SSID 컨피그레이션

1단계. WLAN(WLAN) **> WLANs(WLAN)로 이동합니다.** 새 WLAN을 생성합니다. 프로파일 이름 및 SSID를 구성합니다. SSID 이름이 **DNA** Spaces에 SSID 생성 섹션의 3단계**에 구성된 과 동일한지 확인합니다.**



2단계. 레이어 2 보안을 구성합니다. WLAN Configuration(WLAN 컨피그레이션) 탭에서 **Security(보안) > Layer 2**(레이어 2) 탭으로 이동하고 Layer 2 Security(레이어 2 보안) 드롭다운 메뉴에서 **None(없음**)으로 선택합니다**.** MAC 필터링이 비활성화되어 있는지 확인합니다.



3단계. 레이어 3 보안을 구성합니다. WLAN 컨피그레이션 탭에서 Security(보안) > Layer 3(레이어 3) 탭으로 이동하고, Layer **3 보안 방법으로 Web Policy(웹 정책)를 구성하고, Passthrough(통과)를 활성화하고, 사전 인증 ACL을 구성하고, Override Global Config(전역 컨피그레이션 재정의)를 활성화하고**, Web Auth Type(**웹 인증 유형)을 External(외부)**로 설정하고**, Redirect URL(리디렉션 URL)을 구성합니다.**

참고: 리디렉션 URL을 가져오려면 Configure Manually(수동으로 **구성) 옵션**을 클릭합니다. 이 옵션은 SSID 컨피그레이션 섹션에서 **DNA Spaces에 SSID**를 생성합니다.

DNA 공간에 RADIUS 서버가 있는 종속 포털

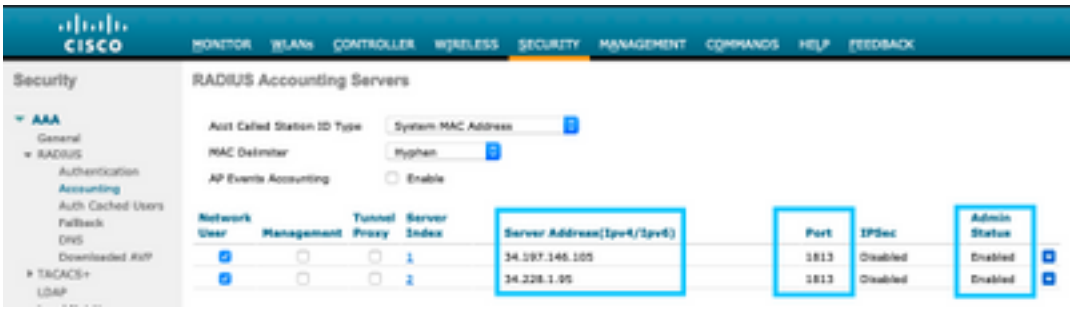
참고: DNA Spaces RADIUS 서버는 컨트롤러에서 오는 PAP 인증만 지원합니다.

컨트롤러의 RADIUS 서버 컨피그레이션

1단계. **Security(보안) > AAA > RADIUS > Authentication(인증)**으로 이동하고 New(새로 만들기)를 클릭하고 RADIUS 서버 정보를 입력합니다. Cisco DNA Spaces는 사용자 인증을 위해 RADIUS 서버 역할을 하며 2개의 IP 주소에서 응답할 수 있습니다. 두 RADIUS 서버를 모두 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(수동**으로 구성) 옵션**을** 클릭하고 **RADIUS Server Configuration(RADIUS 서버 컨피그레이션) 섹션**으로 이동합니다.

2단계. 어카운팅 RADIUS 서버를 구성합니다. **Security(보안) > AAA > RADIUS > Accounting(어카운팅)**으로 이동하고 **New(새로 만들기)**를 클릭합니다. 두 RADIUS 서버를 동일하게 구성합니다.

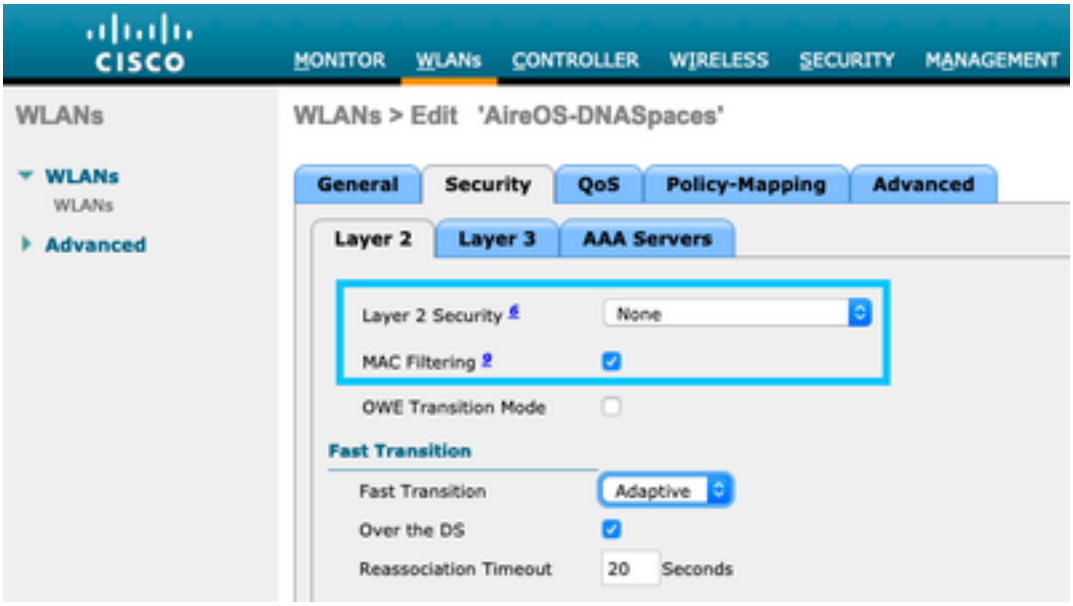


컨트롤러의 SSID 컨피그레이션

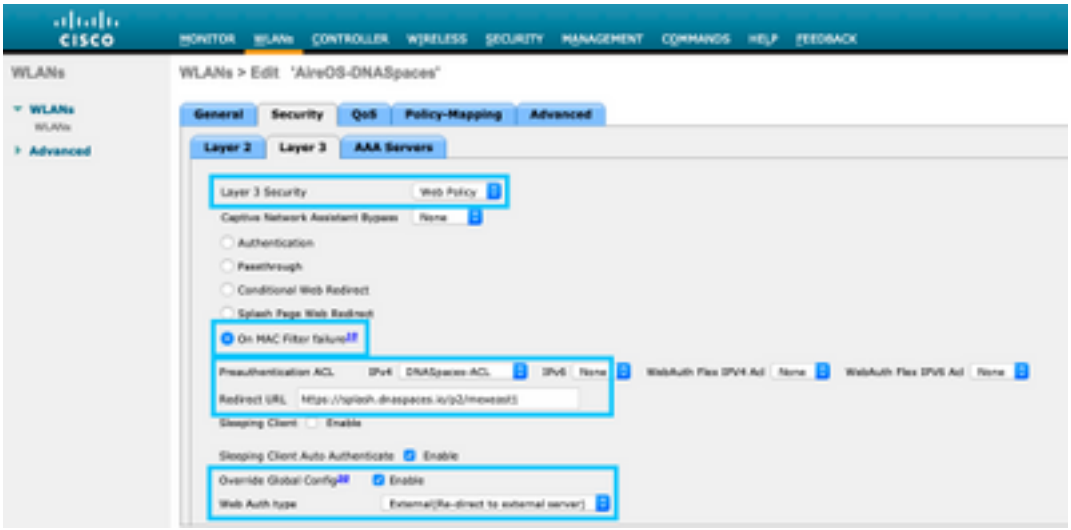
중요: SSID 컨피그레이션으로 시작하기 전에 Controller(컨트롤러) > General(일반)에서 **Web Radius Authentication(웹** RADIUS 인증)이 "PAP"로 설정되어 있는지 확인합니다.

1단계. WLAN(WLAN) **> WLANs(WLAN)로 이동합니다.** 새 WLAN을 생성합니다. 프로파일 이름 및 SSID를 구성합니다. SSID 이름이 **DNA** Spaces에 SSID 생성 섹션의 3단계**에 구성된 과 동일한지 확인합니다.**

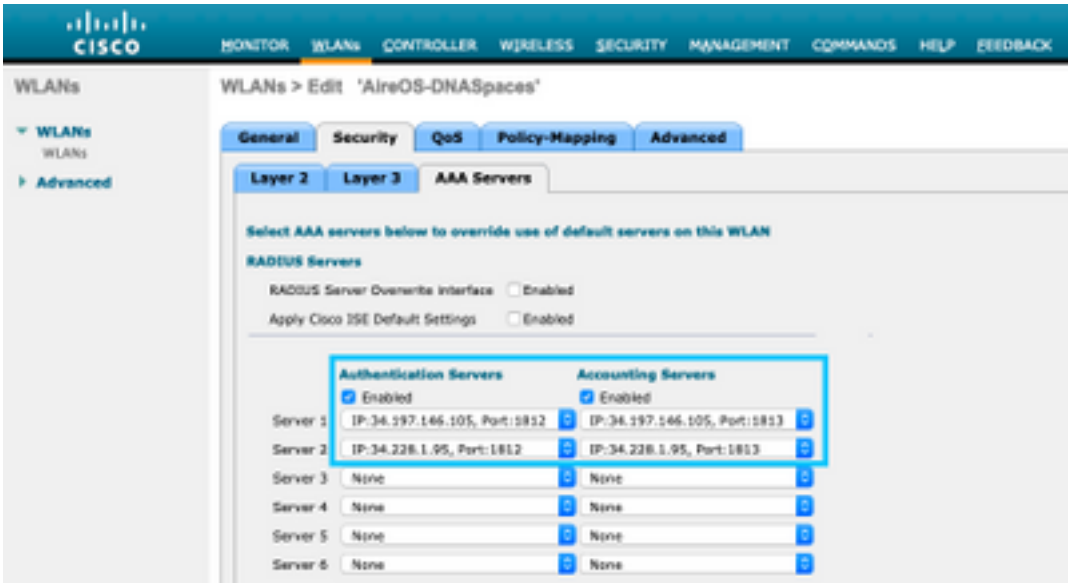
2단계. 레이어 2 보안을 구성합니다. WLAN 컨피그레이션 탭에서 **Security(보안) > Layer 2**(레이어 **2**) 탭으로 이동합니다. 레이어 2 보안을 None으로 **구성합니다**. Mac 필터링을 활성화합니다.



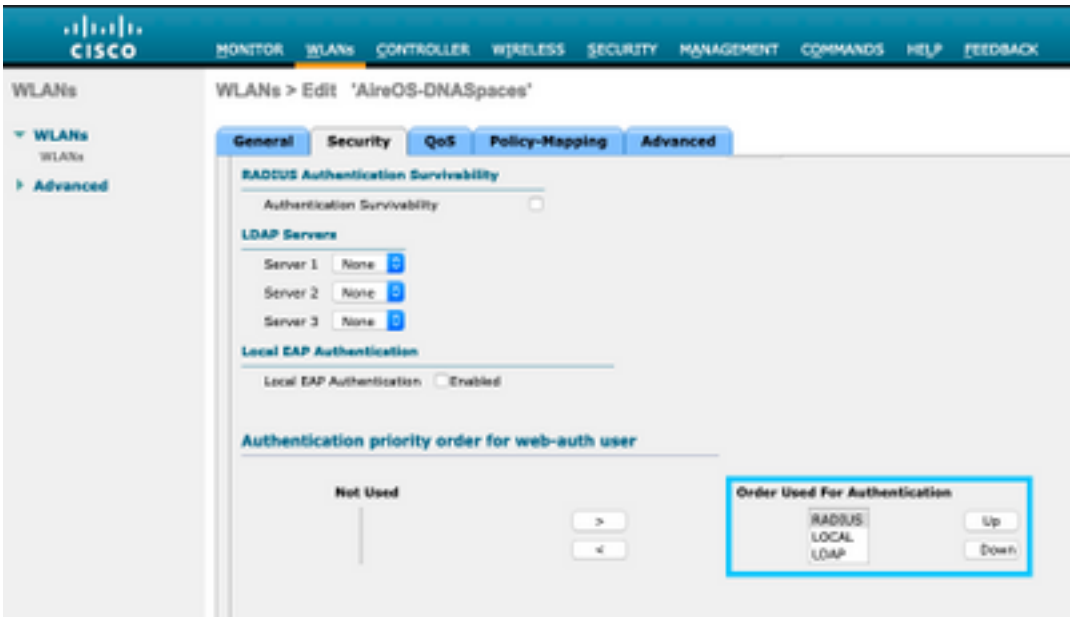
3단계. 레이어 3 보안을 구성합니다. WLAN 컨피그레이션 탭에서 Security(보안) > Layer 3(레이어 3) 탭으로 이동하고, Layer **3 보안 방법으로 Web Policy(웹 정책)를 구성하고, Enable On Mac Filter(Mac 필터 실패 시 활성화), preauthentication ACL(사전 인증 ACL)을 구성하고, Override Global Config(전역 컨피그레이션 재정의)를 활성화하고**, **Web Auth Type(웹 인증 유형)을 External(외부)**로 설정하고, **Redirect URL(리디렉션 URL)을 구성합니다.**



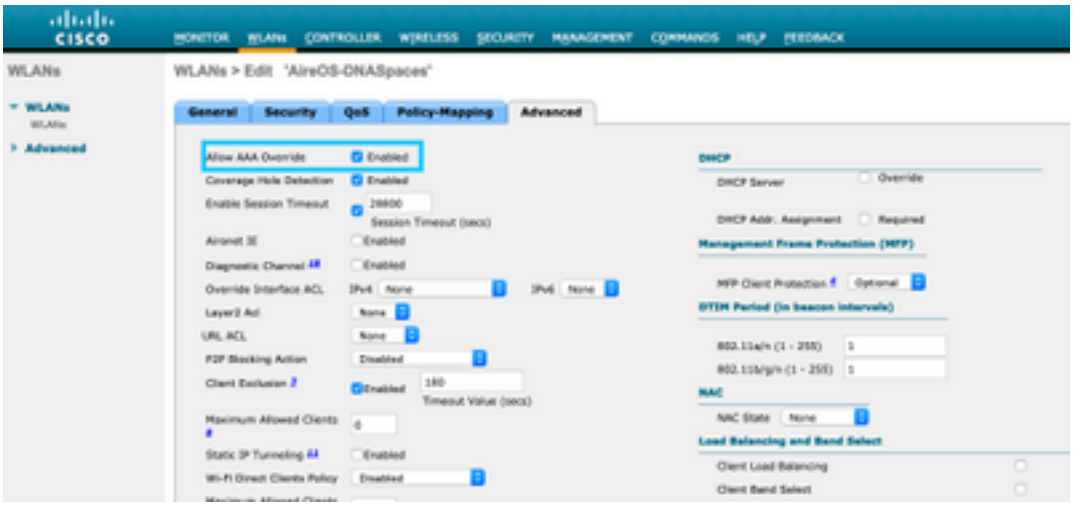
4단계. AAA 서버를 구성합니다. WLAN Configuration(WLAN 컨피그레이션) 탭에서 **Security(보안) > AAA Servers(AAA 서버)** 탭으로 이동하여 **Authentication Servers** and **Accounting Servers(인증 서버** 및 **어카운팅 서버)를 활성화하고** 드롭다운 메뉴에서 두 개의 RADIUS 서버를 선택합니다.



6단계. **웹 인증** 사용자에 **대한 인증 우선 순위 순서를 구성합니다**. WLAN Configuration(WLAN 컨피그레이션) **탭**에서 **Security(보안) > AAA Servers(AAA 서버)** 탭으로 이동하고 RADIUS를 순서대로 첫 번째로 설정합니다.

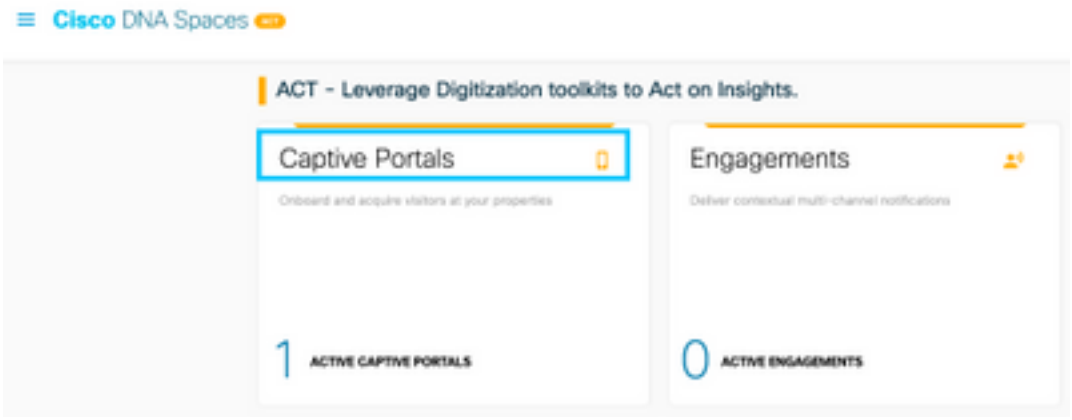


7단계. WLAN Configuration(WLAN 컨피그레이션) **탭**에서 Advanced(고급) 탭으로 이동하고 Allow **AAA Override(AAA 재정의 허용)를 활성화합니다.**

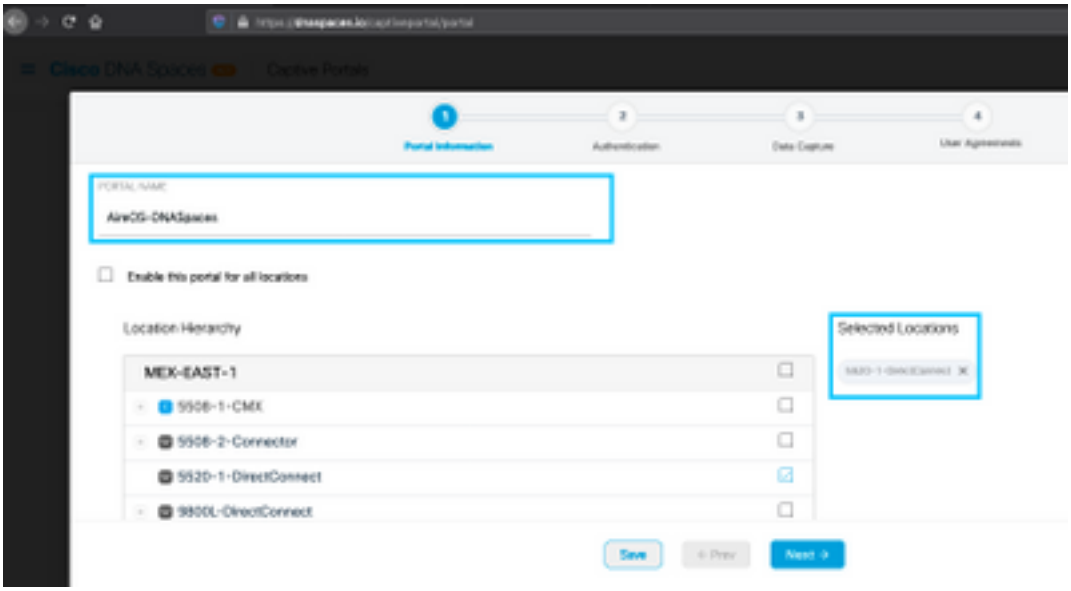


DNA Spaces에서 포털 생성

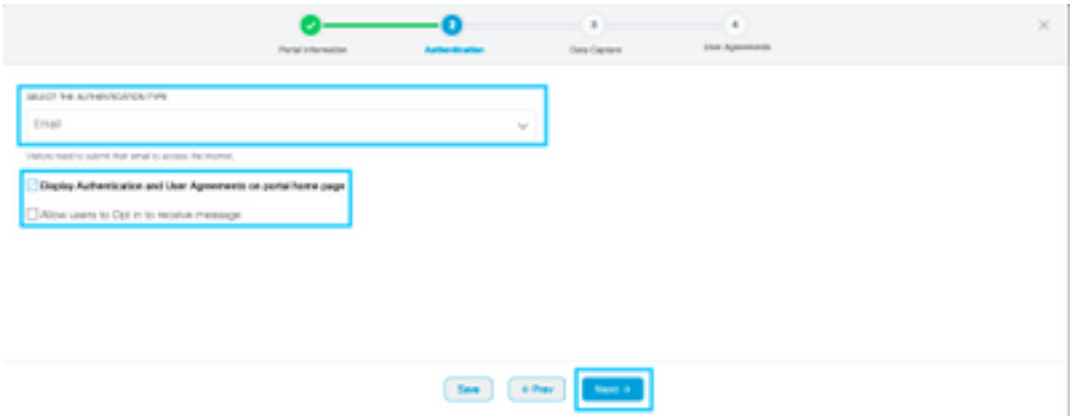
1단계. DNA Spaces의 **대시보드**에서 Captive Portals(종속 포털)를 클릭합니다.



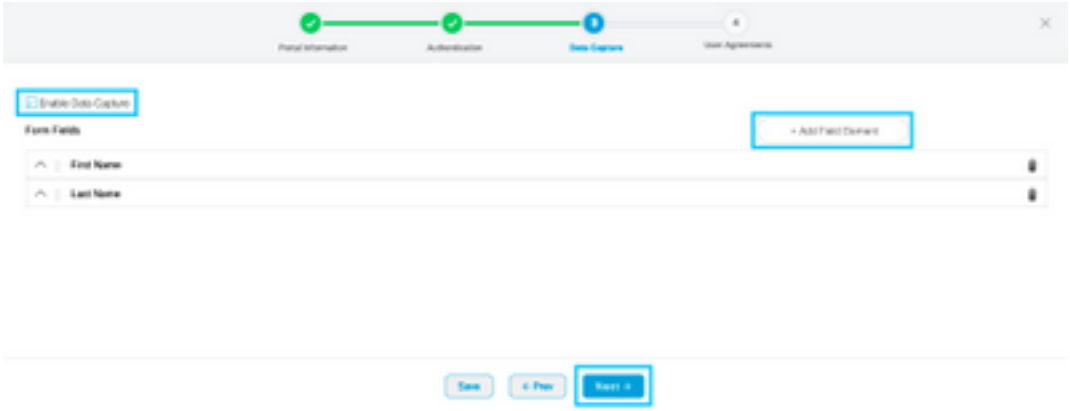
2단계. Create **New(새로 만들기)**를 클릭하고 포털 이름을 입력한 다음 포털을 사용할 수 있는 위치를 선택합니다.



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**.

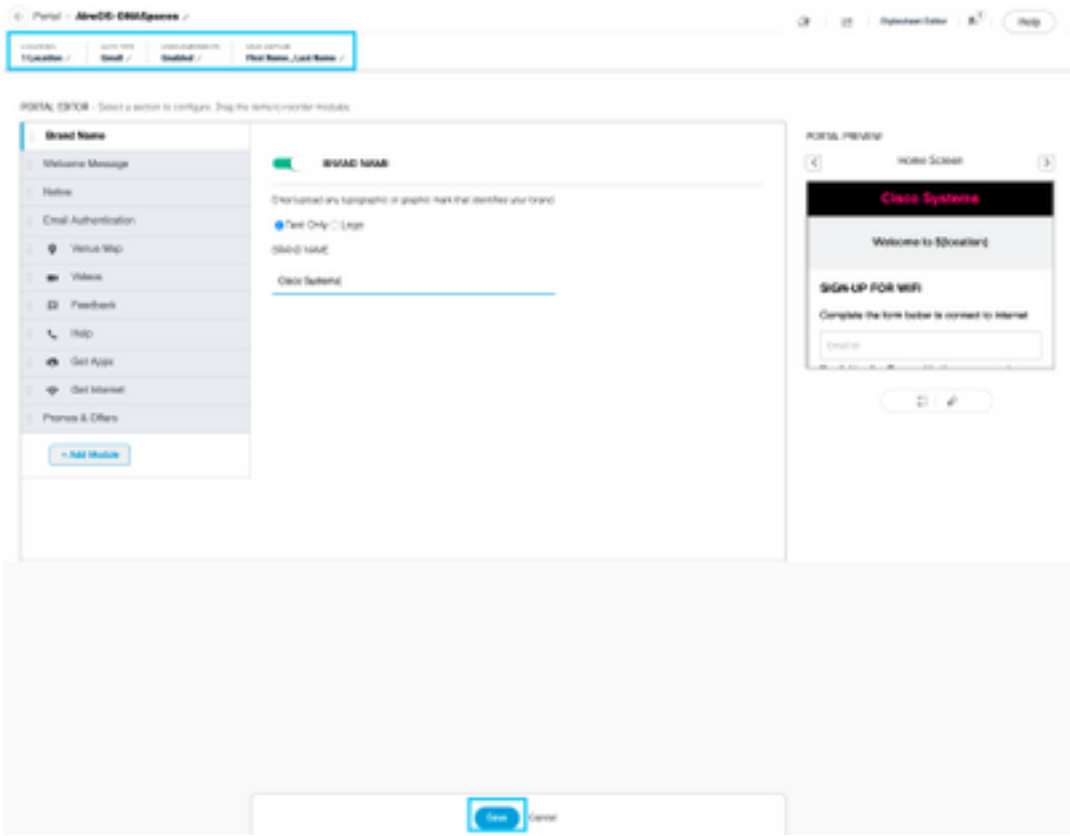


4단계. 데이터 캡처 요소를 구성합니다. 사용자로부터 데이터를 캡처하려면 Enable Data Capture(**데이터 캡처 활성화) 상자**를 선택하고 **+Add Field Element(필드 요소 추가)**를 클릭하여 원하는 필드를 추가합니다. 다음을 **클릭합니다**.



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

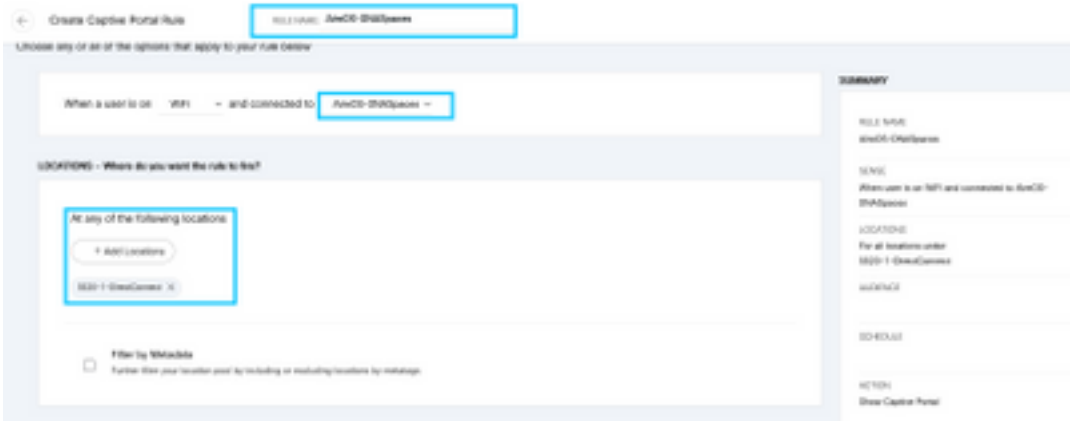
6단계. 필요에 따라 포털을 수정하고 Save(저장)를 **클릭합니다.**



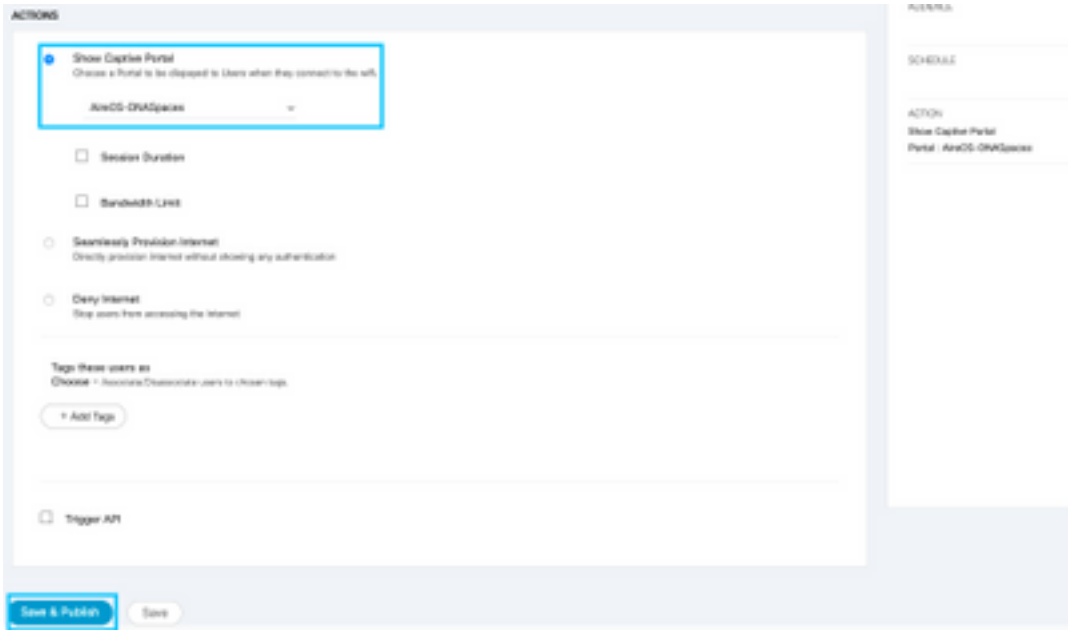
DNA 공간에 종속 포털 규칙 구성

1단계. 종속 포털 메뉴를 열고 종속 **포털** 규칙을 **클릭합니다.**

2단계. + Create **New Rule을 클릭합니다**. 규칙 이름을 입력하고 이전에 구성한 SSID를 선택한 다음 이 포털 규칙이 사용 가능한 위치를 선택합니다.

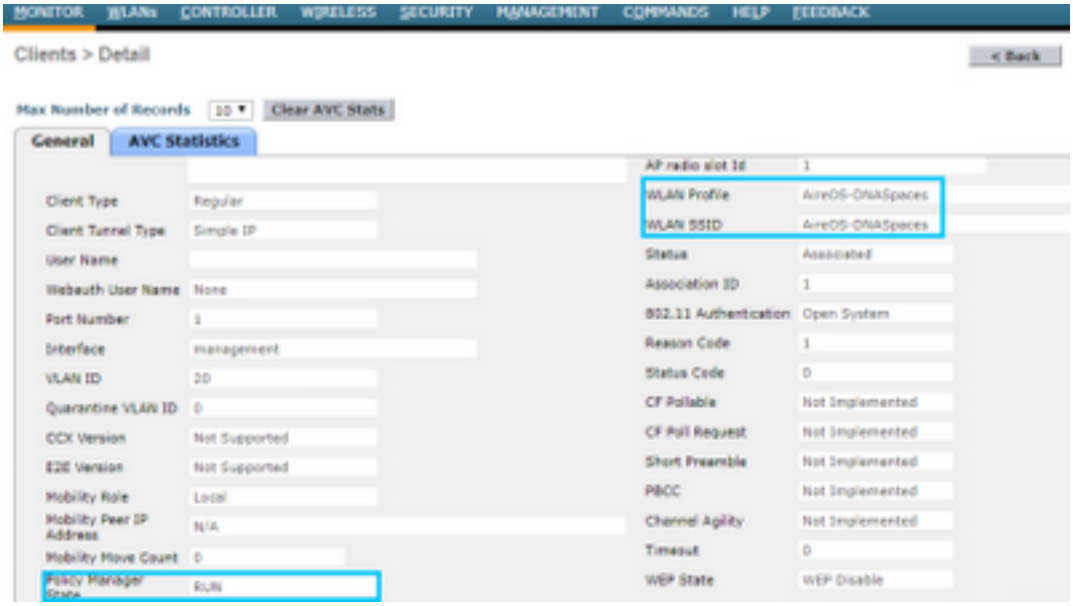


3단계. 종속 포털의 작업을 선택합니다. 이 경우, 규칙이 적중되면 포털이 표시됩니다. 저장 **및 게시를 클릭합니다.**



다음을 확인합니다.

SSID에 연결된 클라이언트의 상태를 확인하려면 **Monitor(모니터) > Clients(클라이언트)**로 이동하고 MAC 주소를 클릭하고 Policy Manager State(정책 관리자 상태)를 찾습니다.



문제 해결

클라이언트의 연결 및 인증 프로세스를 확인하기 위해 테스트하기 전에 컨트롤러에서 다음 명령을 활성화할 수 있습니다.

```
(5520-Andressi) >debug client
```

```
(5520-Andressi) >debug web-auth redirect enable mac
```

이는 RADIUS 서버가 없는 SSID에 연결하는 동안 연결/인증 프로세스 중에 각 단계를 식별하려고 시도한 성공적인 시도의 출력입니다.

802.11 연결/인증:

```
*apfOpenDtlSocket: Apr 09 21:49:06.227: 34:e1:2d:23:a6:68 Received management frame ASSOCIATION
REQUEST on BSSID 70:d3:79:dd:d2:0f destination addr 70:d3:79:dd:d2:0f slotid 1
*apfMsConnTask_5: Apr 09 21:49:06.227: 34:e1:2d:23:a6:68 Updating the client capabiility as 4
*apfMsConnTask_5: Apr 09 21:49:06.227: 34:e1:2d:23:a6:68 Processing assoc-req
station:34:e1:2d:23:a6:68 AP:70:d3:79:dd:d2:00-01 ssid : AireOS-DNASpaces thread:bd271d6280
*apfMsConnTask_5: Apr 09 21:49:06.227: 34:e1:2d:23:a6:68 CL_EVENT_ASSOC_START (1), reasonCode
(1), Result (0), Ssid (AireOS-DNASpaces), ApMac (70:d3:79:dd:d2:00), RSSI (-72), SNR (22)
*apfMsConnTask_5: Apr 09 21:49:06.228: 34:e1:2d:23:a6:68 Sending assoc-resp with status 0
station:34:e1:2d:23:a6:68 AP:70:d3:79:dd:d2:00-01 on apVapId 1
```

DHCP 및 레이어 3 인증:

```
*apfMsConnTask_5: Apr 09 21:49:06.228: 34:e1:2d:23:a6:68 Mobility query, PEM State: DHCP_REQD
*webauthRedirect: Apr 09 21:49:51.949: captive-bypass detection enabled, checking for wispr in
HTTP GET, client mac=34:e1:2d:23:a6:68
*webauthRedirect: Apr 09 21:49:51.949: captiveNetworkMode enabled, mac=34:e1:2d:23:a6:68
```

```
user_agent = AnyConnect Agent 4.7.04056
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Preparing redirect URL according to
configured Web-Auth type
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- unable to get the hostName for virtual
IP, using virtual IP =192.0.2.1
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Checking custom-web config for WLAN
ID:1
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Global status is 0 on WLAN
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- checking on WLAN web-auth type
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Web-auth type External, using
URL:https://splash.dnaspaces.io/p2/mexeast1
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Added switch_url, redirect URL is now
https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Added ap_mac (Radio ), redirect URL is
now
https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79:
dd:d2:00
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Added client_mac , redirect URL is now
https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79:
dd:d2:00&client_mac=34:e1:2d:23:a6
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- Added wlan, redirect URL is now
https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79:
dd:d2:00&client_mac=34:e1:2d:23:a6:68&wla
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- http_response_msg_body1 is
<HTML><HEAD><TITLE> Web Authentication Redirect</TITLE><META http-equiv="Cache-control"
content="no-cache"><META http-equiv="Pragma" content="
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- added redirect=, URL is now
https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79:
dd:d2:00&client_mac=34:e1:2d:23:a6:68&wlan=Ai
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- str1 is now
https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79:
dd:d2:00&client_mac=34:e1:2d:23:a6:68&wlan=AireOS-DNASpaces&r

*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- Message to be sent is
HTTP/1.1 200 OK
Location:
https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79:
dd:d2:00&client_mac=34:
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- 200 send_data =HTTP/1.1 200 OK
Location:
https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79:
dd:d2:00&client_mac=34:e1:2d:23
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- send data length=688
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68-
Url:https://splash.dnaspaces.io/p2/mexeast1
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- cleaning up after send
```

레이어 3 인증에 성공하면 클라이언트를 RUN 상태로 이동합니다.

```
*emWeb: Apr 09 21:49:57.633: Connection created for MAC:34:e1:2d:23:a6:68
*emWeb: Apr 09 21:49:57.634:
ewaURLHook: Entering:url=/login.html, virtIp = 192.0.2.1, ssl_connection=0, secureweb=1

*ewmwebWebauth1: Apr 09 21:49:57.634: 34:e1:2d:23:a6:68 10.10.30.42 WEBAUTH_NOL3SEC (14) Change
state to RUN (20) last state WEBAUTH_NOL3SEC (14)
*ewmwebWebauth1: Apr 09 21:49:57.634: 34:e1:2d:23:a6:68 CL_EVENT_WEB_AUTH_DONE (8), reasonCode
(0), Result (0), ServerIp (), UserName ()
*ewmwebWebauth1: Apr 09 21:49:57.634: 34:e1:2d:23:a6:68 CL_EVENT_RUN (9), reasonCode (0), Result
(0), Role (1), VLAN/VNID (20), Ipv4Addr (10.10.30.42), Ipv6Present (No)
*ewmwebWebauth1: Apr 09 21:49:57.634: 34:e1:2d:23:a6:68 10.10.30.42 RUN (20) Successfully
plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255,URL ACL ID 255,URL ACL
Action 0)
```

```
*emWeb: Apr 09 21:49:57.634: User login successful, presenting login success page to user
```

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.