

9800 WLC 및 Aruba ClearPass 구성 - 게스트 액세스 및 FlexConnect

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[CWA 게스트 엔터프라이즈 구축을 위한 트래픽 흐름](#)

[네트워크 다이어그램](#)

[구성](#)

[게스트 무선 액세스 C9800 매개변수 구성](#)

[C9800 - 게스트용 AAA 컨피그레이션](#)

[C9800 - 리디렉션 ACL 구성](#)

[C9800 - 게스트 WLAN 프로파일 컨피그레이션](#)

[C9800 - 게스트 정책 프로필 정의](#)

[C9800 - 정책 태그](#)

[C9800 - AP 가입 프로필](#)

[C9800 - Flex 프로필](#)

[C9800 - 사이트 태그](#)

[C9800 - RF 프로파일](#)

[C9800 - AP에 태그 할당](#)

[Aruba CPPM 인스턴스 구성](#)

[Aruba ClearPass 서버 초기 컨피그레이션](#)

[라이선스 신청](#)

[서버 호스트 이름](#)

[CPPM 웹 서버 인증서\(HTTPS\) 생성](#)

[C9800 WLC를 네트워크 디바이스로 정의](#)

[게스트 포털 페이지 및 CoA 타이머](#)

[ClearPass - 게스트 CWA 컨피그레이션](#)

[ClearPass 끝점 메타데이터 특성: 게스트 인터넷 허용](#)

[ClearPass 시행 정책 구성 재인증](#)

[ClearPass 게스트 포털 리디렉션 적용 프로파일 컨피그레이션](#)

[ClearPass 메타데이터 적용 프로필 컨피그레이션](#)

[ClearPass 게스트 인터넷 액세스 적용 정책 컨피그레이션](#)

[ClearPass 게스트 사후 AUP 시행 정책 컨피그레이션](#)

[ClearPass MAB 인증 서비스 컨피그레이션](#)

[ClearPass Webauth 서비스 컨피그레이션](#)

[ClearPass - 웹 로그인](#)

[확인 - 게스트 CWA 권한 부여](#)

[부록](#)

소개

이 문서에서는 Catalyst 9800 WLC(Wireless LAN Controller)와 Aruba ClearPass의 통합을 통해 AP(Access Point) 구축의 Flexconnect 모드에서 CWA(Central Web Authentication)를 활용하는 게스트 SSID(Wireless Service Set Identifier)를 무선 클라이언트에 제공하는 방법을 설명합니다.

게스트 무선 인증은 게스트 포털에서 AUP(Anonymous Acceptable User Policy) 페이지를 통해 지원되며, DMZ(secure demilitarized zone) 세그먼트의 Aruba Clearpass에서 호스팅됩니다.

사전 요구 사항

이 설명서에서는 다음 구성 요소가 구성되고 확인되었다고 가정합니다.

- 모든 관련 구성 요소가 NTP(Network Time Protocol)에 동기화되고 올바른 시간이 있는지 확인됨(인증서 검증에 필요)
- 운영 DNS 서버(게스트 트래픽 흐름, CRL(Certificate Revocation List) 검증에 필요)
- 운영 DHCP 서버
- 선택적 CA(Certificate Authority)(CPPM 호스팅 게스트 포털에 서명하는 데 필요)
- Catalyst 9800 WLC
- Aruba ClearPass Server(플랫폼 라이선스, 액세스 라이선스, 온보드 라이선스 필요)
- Vmware ESXi

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- C9800 구축 및 새로운 구성 모델
- C9800의 Flexconnect 스위칭
- 9800 CWA 인증(<https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213920-central-web-authentication-cwa-on-cata.html> [참조](#))

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 17.3.4c를 실행하는 Cisco Catalyst C9800-L-C
- Cisco Catalyst C9130AX
- Aruba ClearPass, 6-8-0-109592 및 6.8-3 패치
- MS Windows 서버 Active Directory(관리되는 엔드포인트에 대한 자동화된 머신 기반 인증서 발급을 위해 구성된 GP)DHCP 서버(옵션 43 및 옵션 60)DNS 서버모든 구성 요소를 시간 동기화하기 위한 NTP 서버CA

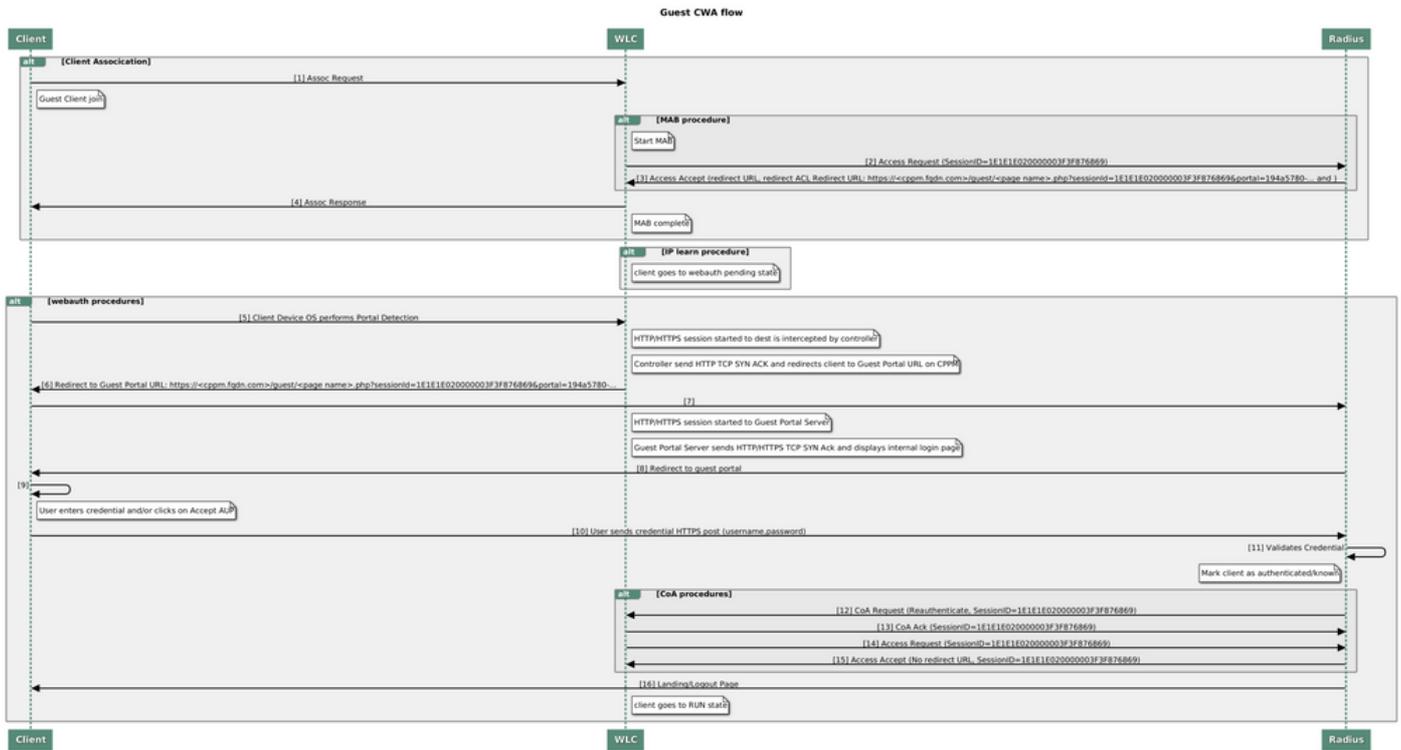
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

이 다이어그램은 게스트 사용자가 네트워크에서 허용되기 전에 게스트 Wifi 액세스 교환의 세부 정보를 전달합니다.

1. 게스트 사용자가 원격 사무실에서 게스트 Wifi와 연결합니다.
2. 초기 RADIUS Access-Request가 C9800에 의해 RADIUS 서버로 프록시됩니다.
3. 서버가 로컬 MAC 엔드포인트 데이터베이스에서 제공된 게스트 MAC 주소를 찾습니다. MAC 주소가 없는 경우 서버는 MAB(MAC Authentication Bypass) 프로파일로 응답합니다. 이 RADIUS 응답에는 다음이 포함됩니다.
 - URL 리디렉션 ACL(Access Control List)
 - URL 리디렉션
4. 클라이언트는 IP 주소가 할당된 IP Learn 프로세스를 거칩니다.
5. C9800은 게스트 클라이언트(MAC 주소로 식별됨)를 '웹 인증 보류 중' 상태로 전환합니다.
6. 게스트 WLAN과 연결된 대부분의 최신 디바이스 OS는 일종의 종속 포털 탐지를 수행합니다. 정확한 탐지 메커니즘은 특정 OS 구현에 따라 달라집니다. 클라이언트 OS는 RADIUS Access-Accept 응답의 일부로 제공된 RADIUS 서버가 호스팅하는 게스트 포털 URL로 C9800에 의해 리디렉션된 페이지가 포함된 팝업(의사 브라우저) 대화 상자를 엽니다.
7. 게스트 사용자는 제시된 팝업 ClearPass의 약관에 동의하고 클라이언트가 인증을 완료했음을 나타내기 위해 엔드포인트 데이터베이스(DB)의 클라이언트 MAC 주소에 대한 플래그를 설정하며 라우팅 테이블에 따라 인터페이스를 선택하여 RADIUS CoA(Change of Authorization)를 시작합니다 (ClearPass에 여러 인터페이스가 있는 경우).
8. WLC는 게스트 클라이언트를 '실행' 상태로 전환하며 사용자는 더 이상 리디렉션 없이 인터넷에 액세스할 수 있습니다.

참고: Cisco 9800 Foreign, Anchor Wireless Controller state flow diagram with RADIUS and externally hosted Guest Portal의 경우 이 문서의 부록 섹션을 참조하십시오.



CWA(Guest Central Web Authentication) 상태 다이어그램

CWA 게스트 엔터프라이즈 구축을 위한 트래픽 흐름

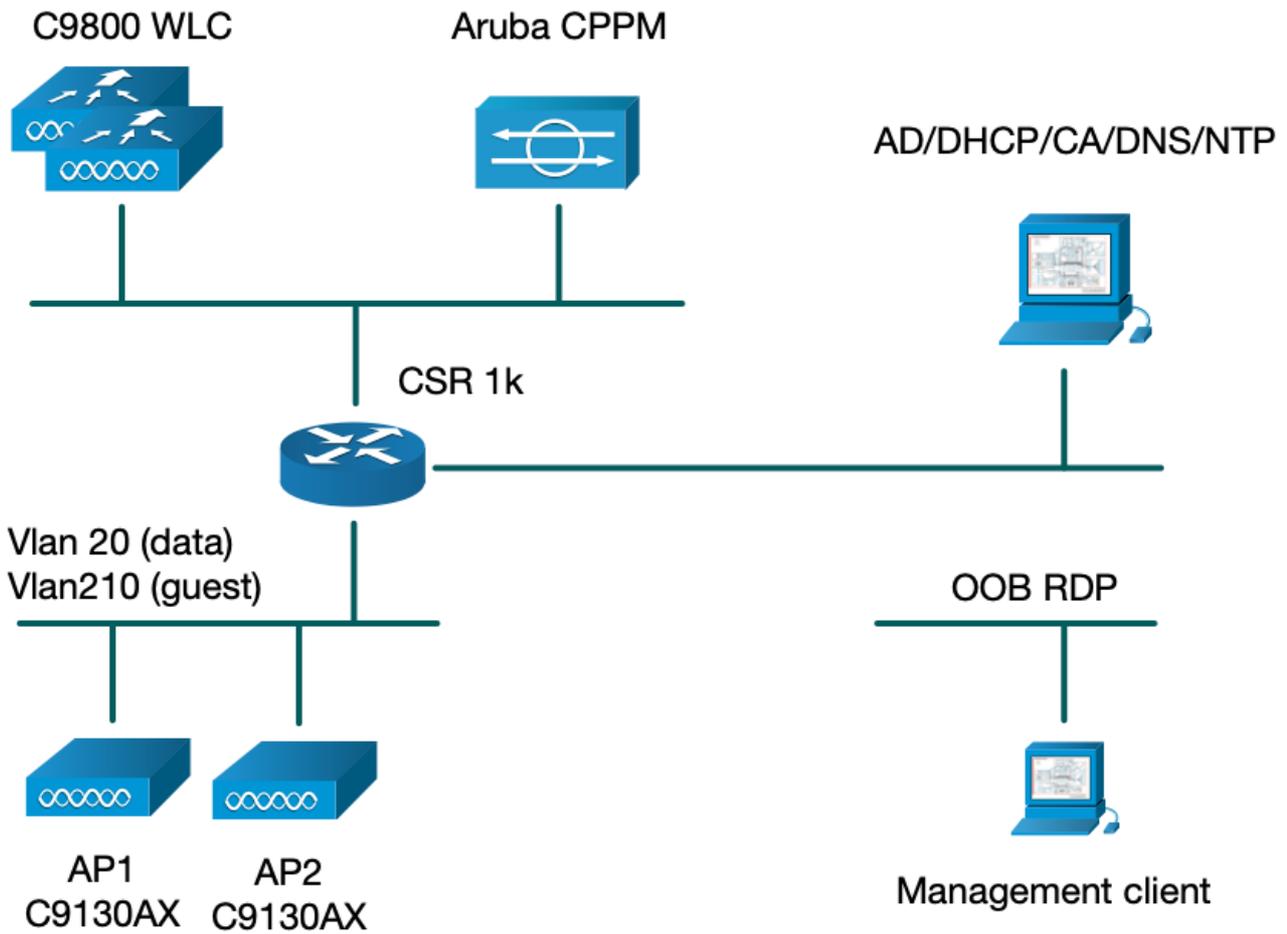
여러 지사를 사용하는 일반적인 엔터프라이즈 구축에서 각 지사는 게스트가 EULA에 동의하면 게스트 포털을 통해 안전하고 세분화된 액세스를 제공하도록 설정됩니다.

이 컨피그레이션 예에서는 9800 CWA가 네트워크의 보안 DMZ에서 게스트 사용자를 위해 배타적으로 구축된 별도의 ClearPass 인스턴스에 대한 통합을 통해 게스트 액세스에 사용됩니다.

게스트는 DMZ ClearPass 서버에서 제공하는 웹 동의 팝업 포털에 명시된 약관에 동의해야 합니다. 이 컨피그레이션 예에서는 익명 게스트 액세스 방법(즉, 게스트 포털을 인증하는 데 게스트 사용자 이름/비밀번호가 필요하지 않음)에 중점을 둡니다.

이 구축에 해당하는 트래픽 흐름이 이미지에 표시됩니다.

1. RADIUS - MAB 단계
2. 게스트 클라이언트 URL이 게스트 포털로 리디렉션
3. 게스트 포털에서 EULA의 게스트 승인 후 RADIUS CoA 재인증이 CPPM에서 9800 WLC로 발행됩니다.
4. 게스트는 인터넷에 액세스할 수 있습니다.



구성

이 컨피그레이션 예에서는 C9800의 새 컨피그레이션 모델을 활용하여 엔터프라이즈 브랜치에 dot1x Corporate Access 및 CWA 게스트 액세스를 제공하는 데 필요한 프로파일 및 태그를 생성합니다. 결과 컨피그레이션이 이 이미지에 요약되어 있습니다.

AP
MAC: XXXX.XXXX.XXXX

Policy Tag: PT_CAN01

WLAN Profile: WP_Guest
SSID: Guest
Layer 2: Security None
Layer 2: MAC Filtering Enabled
Authz List: AAA_Authz-CPPM

Policy Profile: PP_Guest
Central Switching: Disabled
Central Auth: Enabled
Central DHCP: Disabled
Vlan: guest (21)
AAA Policy: Allow AAA Override Enabled
AAA Policy: NAC State Enabled
AAA Policy: NAC Type RADIUS
AAA Policy Accounting List: Guest_Accounting

Site Tag: ST_CAN01
Enable Local Site: Off

AP Join Profile: MyApProfile
NTP Server: 10.0.10.4

Flex Profile: FP_CAN01
Native Vlan 2
Policy ACL: CAPTIVE_PORTAL_REDIRECT,
ACL CWA: Enabled
VLAN: 21 (Guest)

RF Tag: Branch_RF

5GHz Band RF: Typical_Client_Density_rf_5gh

2GHz Band RF: Typical_Client_Density_rf_2gh

게스트 무선 액세스 C9800 매개변수 구성

C9800 - 게스트용 AAA 컨피그레이션

참고: Cisco 버그 ID [CSCvh03827](#)에 대해, 메커니즘이 ClearPass RADIUS 교환을 위해 WLC의 SessionID 지속성을 사용하므로 정의된 AAA(Authentication, Authorization, and Accounting) 서버가 로드 밸런싱되지 않는지 확인합니다.

1단계. 9800 WLC 컨피그레이션에 Aruba ClearPass DMZ 서버를 추가하고 인증 방법 목록을 생성합니다. Configuration(컨피그레이션) > **Security(보안)** > **AAA** > **Servers/Groups(서버/그룹)** > **RADIUS** > **Servers(서버)** > **+Add(추가)**로 이동하고 RADIUS 서버 정보를 입력합니다.

Create AAA Radius Server



Name*	<input type="text" value="CPPM"/>
Server Address*	<input type="text" value="10.85.54.98"/>
PAC Key	<input type="checkbox"/>
Key Type	<input type="text" value="Clear Text"/>
Key*	<input type="text" value="....."/>
Confirm Key*	<input type="text" value="....."/>
Auth Port	<input type="text" value="1812"/>
Acct Port	<input type="text" value="1813"/>
Server Timeout (seconds)	<input type="text" value="5"/>
Retry Count	<input type="text" value="3"/>
Support for CoA	<input checked="" type="checkbox"/> ENABLED

Cancel

Apply to Device

2단계. 게스트에 대한 AAA 서버 그룹을 정의하고 1단계에서 구성한 서버를 이 서버 그룹에 할당합니다. Configuration(컨피그레이션) > Security(보안) > AAA > Servers/Groups(서버/그룹) > RADIUS > Groups(그룹) > +Add(추가)로 이동합니다.

Create AAA Radius Server Group



Name*	<input type="text" value="AAA_Radius_CPPM"/>
Group Type	<input type="text" value="RADIUS"/>
MAC-Delimiter	<input type="text" value="none"/>
MAC-Filtering	<input type="text" value="none"/>
Dead-Time (mins)	<input type="text" value="5"/>
Source Interface VLAN ID	<input type="text" value="1"/>

Available Servers

Assigned Servers



CPPM



Cancel

Apply to Device

3단계. 게스트 액세스를 위한 권한 부여 방법 목록을 정의하고 2단계에서 생성한 서버 그룹을 매핑합니다. **Configuration > Security > AAA > AAA Method List > Authorization > +Add**로 이동합니다. Type **Network(네트워크 유형)**를 선택한 다음 2단계에서 구성한 **AAA Server Group(AAA 서버 그룹)**을 선택합니다.

Quick Setup: AAA Authorization

Method List Name*

Type* ⓘ

Group Type ⓘ

Fallback to local

Authenticated

Available Server Groups: radius, ldap, tacacs+

Assigned Server Groups: AAA_Radius_CPPM

4단계. 게스트 액세스를 위한 계정 관리 방법 목록을 생성하고 2단계에서 생성한 서버 그룹을 매핑합니다. **Configuration > Security > AAA > AAA Method List > Accounting > +Add**로 이동합니다. 드롭다운 메뉴에서 Type **Identity(유형 ID)**를 선택한 다음 2단계에서 구성한 **AAA Server Group(AAA 서버 그룹)**을 선택합니다.

Quick Setup: AAA Accounting

Method List Name*

Type* ⓘ

Available Server Groups: radius, ldap, tacacs+

Assigned Server Groups: AAA_Radius_CPPM

리디렉션 ACL은 게스트 포털로 리디렉션해야 하는 트래픽과 리디렉션 없이 통과해야 하는 트래픽을 정의합니다. 여기서 ACL 거부(우회 리디렉션 또는 통과(pass through))를 의미하며 permit은 포털로의 리디렉션을 의미합니다. 각 트래픽 클래스에 대해 ACE(Access Control Entries)를 생성하고 인그레스 및 이그레스 트래픽에 모두 일치하는 ACE를 생성할 때 트래픽 방향을 고려해야 합니다.

Configuration(컨피그레이션) > Security(보안) > ACL로 이동하고 CAPTIVE_PORTAL_REDIRECT라는 새 ACL을 정의합니다. 다음 ACE로 ACL을 구성합니다.

- ACE1: 양방향 ICMP(Internet Control Message Protocol) 트래픽이 리디렉션을 우회하도록 허용하며 주로 연결 가능성을 확인하는 데 사용됩니다.
- ACE10, ACE30: DNS 서버 10.0.10.4로 양방향 DNS 트래픽 흐름을 허용하고 포털로 리디렉션하지 않습니다. 게스트 플로우를 트리거하려면 DNS 조회 및 응답에 대한 가로채기가 필요합니다.
- ACE70, ACE80, ACE110, ACE120: 사용자가 포털과 함께 표시되도록 게스트 종속 포털에 대한 HTTP 및 HTTPS 액세스를 허용합니다.
- ACE150: 모든 HTTP 트래픽(UDP 포트 80)이 리디렉션됩니다.

Sequence ▲	Action ▼	Source IP ▼	Source Wildcard ▼	Destination IP ▼	Destination Wildcard ▼	Protocol ▼	Source Port ▼	Destination Port ▼
1	deny	any		any		icmp		
10	deny	any		10.0.10.4		udp		eq domain
30	deny	10.0.10.4		any		udp	eq domain	
70	deny	any		10.85.54.98		tcp		eq 443
80	deny	10.85.54.98		any		tcp	eq 443	
110	deny	any		10.85.54.98		tcp		eq www
120	deny	10.85.54.98		any		tcp	eq www	
150	permit	any		any		tcp		eq www

C9800 - 게스트 WLAN 프로파일 컨피그레이션

1단계. Configuration(구성) > Tags & Profiles(태그 및 프로파일) > Wireless(무선) > +Add(추가)로 이동합니다. 게스트 클라이언트가 연결하는 SSID 'Guest'의 브로드캐스트와 함께 새 SSID 프로파일 WP_Guest를 생성합니다.

Add WLAN ✕

General Security Advanced

Profile Name*	<input type="text" value="WP_Guest"/>	Radio Policy	<input type="text" value="All"/>
SSID*	<input type="text" value="Guest"/>	Broadcast SSID	<input checked="" type="checkbox"/> ENABLED
WLAN ID*	<input type="text" value="3"/>		
Status	<input checked="" type="checkbox"/> ENABLED		

Cancel

Apply to Device

동일한 Add WLAN(WLAN 추가) 대화 상자에서 Security(보안) > Layer 2(레이어 2) 탭으로 이동합니다.

- 레이어 2 보안 모드: 없음

- MAC 필터링: 사용

- 권한 부여 목록: 드롭다운 메뉴의 AAA_Authz_CPPM(3단계에서 AAA 컨피그레이션의 일부로 구성)

Add WLAN ✕

General Security Advanced

Layer2 Layer3 AAA

Layer 2 Security Mode	<input type="text" value="None"/>	Lobby Admin Access	<input type="checkbox"/>
MAC Filtering	<input checked="" type="checkbox"/>	Fast Transition	<input type="text" value="Adaptive Enab..."/>
OWE Transition Mode	<input checked="" type="checkbox"/>	Over the DS	<input type="checkbox"/>
Transition Mode WLAN ID*	<input type="text" value="1-4096"/>	Reassociation Timeout	<input type="text" value="20"/>
Authorization List*	<input type="text" value="AAA_Authz_C"/>		

Cancel

Apply to Device

C9800 - 게스트 정책 프로필 정의

C9800 WLC GUI에서 Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로필) > Policy(정책) > +Add(추가)로 이동합니다.

이름: PP_게스트

상태: 사용

중앙 스위칭: 비활성화됨

중앙 인증: 사용

중앙 DHCP: 비활성화됨

중앙 연결: 비활성화됨

Add Policy Profile ✕

General Access Policies QOS and AVC Mobility Advanced

⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

Name*	<input type="text" value="PP_Guest"/>	WLAN Switching Policy	
Description	<input type="text" value="Policy Profile for Guest"/>	Central Switching	<input type="checkbox"/> DISABLED
Status	<input checked="" type="checkbox"/> ENABLED	Central Authentication	<input checked="" type="checkbox"/> ENABLED
Passive Client	<input type="checkbox"/> DISABLED	Central DHCP	<input type="checkbox"/> DISABLED
Encrypted Traffic Analytics	<input type="checkbox"/> DISABLED	Central Association	<input type="checkbox"/> DISABLED
CTS Policy		Flex NAT/PAT	<input type="checkbox"/> DISABLED
Inline Tagging	<input type="checkbox"/>		
SGACL Enforcement	<input type="checkbox"/>		
Default SGT	<input type="text" value="2-65519"/>		

Add Policy Profile

⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

General

Access Policies

QOS and AVC

Mobility

Advanced

Name*

PP_Guest

Description

Profile for Branch Guest

Status

DISABLED

Passive Client

DISABLED

Encrypted Traffic Analytics

DISABLED

CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

2-65519

WLAN Switching Policy

Central Switching

DISABLED

Central Authentication

ENABLED

Central DHCP

DISABLED

Central Association

DISABLED

Flex NAT/PAT

DISABLED

Cancel

Apply to Device

동일한 Add Policy Profile(정책 프로필 추가) 대화 상자에서 Access Policies(액세스 정책) 탭으로 이동합니다.

- RADIUS 프로파일링: 사용

- VLAN/VLAN 그룹: 210(즉, VLAN 210은 각 브랜치 위치의 게스트 로컬 VLAN)

참고: Flex용 게스트 VLAN은 VLAN/VLAN 그룹 유형 VLAN 번호의 VLAN에 있는 9800 WLC에서 정의하지 않아도 됩니다.

알려진 결함: Cisco 버그 ID [CSCvn48234](#)는 동일한 Flex 게스트 VLAN이 WLC 및 Flex 프로필에 정의된 경우 SSID가 브로드캐스트되지 않습니다.

⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

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

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

WLAN Local Profiling

Global State of Device Classification ⓘ

Local Subscriber Policy Name

Search or Select ▼

VLAN

VLAN/VLAN Group

210 ▼

Multicast VLAN

Enter Multicast VLAN

WLAN ACL

IPv4 ACL

Search or Select ▼

IPv6 ACL

Search or Select ▼

URL Filters

Pre Auth

Search or Select ▼

Post Auth

Search or Select ▼

Cancel

Apply to Device

동일한 Add Policy Profile(정책 프로파일 추가) 대화 상자에서 **Advanced(고급)** 탭으로 이동합니다.

- AAA 재정의 허용: 사용

- NAC 상태: 사용

- NAC 유형: RADIUS

- 회계 목록: AAA_Accounting_CPPM(AAA 컨피그레이션의 일부로 4단계에서 정의됨)

⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

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

WLAN Timeout

Session Timeout (sec)

Idle Timeout (sec)

Idle Threshold (bytes)

Client Exclusion Timeout (sec)

Guest LAN Session Timeout

DHCP

IPv4 DHCP Required

DHCP Server IP Address

[Show more >>>](#)

AAA Policy

Allow AAA Override

NAC State

NAC Type

Policy Name

Accounting List

Fabric Profile

mDNS Service Policy

Hotspot Server

User Defined (Private) Network

Status

Drop Unicast

Umbrella

Umbrella Parameter Map [Clear](#)

Flex DHCP Option for DNS **ENABLED**

DNS Traffic Redirect **IGNORE**

WLAN Flex Policy

VLAN Central Switching

Split MAC ACL

Air Time Fairness Policies

2.4 GHz Policy

참고: C9800 WLC에서 RADIUS CoA 메시지를 수락하려면 'NAC(Network Admission Control) State - Enable'이 필요합니다.

C9800 - 정책 태그

C9800 GUI에서 Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로필) > Tags(태그) > Policy(정책) > +Add(추가)로 이동합니다.

-이름: PT_CAN01

-설명: CAN01 지사 사이트용 정책 태그

동일한 대화 상자에서 Add Policy Tag(정책 태그 추가)의 WLAN-POLICY MAPS(WLAN-POLICY 맵)에서 +Add(추가)를 클릭하고 이전에 생성한 WLAN 프로필을 Policy Profile(정책 프로필)에 매핑합

니다.

- WLAN 프로파일: WP_게스트

- 정책 프로파일: PP_게스트

Add Policy Tag ✕

Name*

Description

▼ WLAN-POLICY Maps: 0

WLAN Profile	Policy Profile
◀ 0 ▶ 10 items per page No items to display	

Map WLAN and Policy

WLAN Profile* Policy Profile*

➤ RLAN-POLICY Maps: 0

C9800 - AP 가입 프로파일

C9800 WLC GUI에서 Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로파일) > AP Join(AP 조인) > +Add(추가)로 이동합니다.

-이름: 브랜치_AP_프로파일

- NTP 서버: 10.0.10.4(실습 토폴로지 다이어그램 참조). 브랜치의 AP가 동기화를 위해 사용하는 NTP 서버입니다.

General

Client

CAPWAP

AP

Management

Security

ICap

QoS

Name* Description LED State LAG Mode NTP Server GAS AP Rate Limit Apphost

OfficeExtend AP Configuration

Local Access Link Encryption Rogue Detection

Cancel

Apply to Device

C9800 - Flex 프로파일

프로파일과 태그는 모듈식이며 여러 사이트에 재사용할 수 있습니다.

FlexConnect 구축의 경우 모든 브랜치 사이트에서 동일한 VLAN ID가 사용되는 경우 동일한 Flex 프로파일을 다시 사용할 수 있습니다.

1단계. C9800 WLC GUI에서 Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로파일) > Flex > +Add(추가)로 이동합니다.

-이름: FP_분기

- 네이티브 VLAN ID: 10(AP 관리 인터페이스를 사용하려는 기본이 아닌 네이티브 VLAN이 있는 경우에만 필요)

Add Flex Profile ✕

General Local Authentication Policy ACL VLAN Umbrella

Name*	FP_Branch	Fallback Radio Shut	<input type="checkbox"/>
Description	Branch Flex Profile	Flex Resilient	<input type="checkbox"/>
Native VLAN ID	10	ARP Caching	<input checked="" type="checkbox"/>
HTTP Proxy Port	0	Efficient Image Upgrade	<input checked="" type="checkbox"/>
HTTP-Proxy IP Address	0.0.0.0	OfficeExtend AP	<input type="checkbox"/>
CTS Policy		Join Minimum Latency	<input type="checkbox"/>
Inline Tagging	<input type="checkbox"/>	IP Overlap	<input type="checkbox"/>
SGACL Enforcement	<input type="checkbox"/>	mDNS Flex Profile	Search or Select ▾
CTS Profile Name	default-sxp-profile ✕ ▾		

Cancel

Apply to Device

동일한 Add Flex Profile(Flex 프로파일 추가) 대화 상자에서 Policy ACL(정책 ACL) 탭으로 이동하여 +Add(추가)를 클릭합니다.

- ACL 이름: CAPTIVE_PORTAL_REDIRECT

- 중앙 웹 인증: 사용

Flexconnect 구축에서는 리디렉션이 C9800이 아닌 AP에서 발생하므로 각 관리되는 AP가 리디렉션 ACL을 로컬로 다운로드해야 합니다.

Add Flex Profile ✕

General Local Authentication Policy ACL VLAN Umbrella

+ Add × Delete

ACL Name	Central Web Auth	Pre Auth URL Filter
0		

10 items per page No items to display

ACL Name* CAPTIVE_PORTAL_F ▾

Central Web Auth

Pre Auth URL Filter Search or Select ▾

Save Cancel

Cancel

Apply to Device

동일한 Add Flex Profile(Flex 프로파일 추가) 대화 상자에서 VLAN 탭으로 이동하여 +Add(추가)를 클릭합니다(랩 토폴로지 다이어그램 참조).

- VLAN 이름: 게스트

- VLAN ID: 210

Add Flex Profile ✕

General Local Authentication Policy ACL **VLAN** Umbrella

+ Add ✕ Delete

VLAN Name	ID	ACL Name
<input type="checkbox"/> data	2	

◀ 1 ▶ 10 items per page 1 - 1 of 1 items

VLAN Name*

VLAN Id*

ACL Name

✓ Save ↶ Cancel

↶ Cancel Apply to Device

C9800 - 사이트 태그

9800 WLC GUI에서 Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로필) > Tags(태그) > Site(사이트) > Add(추가)로 이동합니다.

참고: 설명된 대로 2개의 무선 SSID를 지원해야 하는 각 원격 사이트에 대해 고유한 사이트 태그를 생성합니다.

지리적 위치, 사이트 태그 및 Flex Profile 컨피그레이션 간에는 1-1 매핑이 있습니다.

Flex Connect 사이트에는 연결된 Flex Connect 프로파일이 있어야 합니다. 각 Flex Connect 사이트에 대해 최대 100개의 액세스 포인트를 가질 수 있습니다.

- 이름: ST_CAN01
- AP 가입 프로필: 브랜치_AP_프로파일
- Flex 프로필: FP_분기
- 로컬 사이트 사용: 비활성화됨

Add Site Tag ✕

Name*

Description

AP Join Profile

Flex Profile

Fabric Control Plane Name

Enable Local Site

↶ Cancel Apply to Device

C9800 - RF 프로파일

9800 WLC GUI에서 Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로파일) > Tags(태그) > RF > Add(추가)로 이동합니다.

-이름: 지사 RF

- 5GHz 대역 RF(Radio Frequency) 프로파일: Typical_Client_Density_5gh(시스템 정의 옵션)

- 2.4GHz 대역 RF 프로파일: Typical_Client_Density_2gh(시스템 정의 옵션)

The screenshot shows the 'Add RF Tag' configuration window. The fields are as follows:

Name*	Branch_RF
Description	Typical Branch RF
5 GHz Band RF Profile	Client_Density_rf_5gh
2.4 GHz Band RF Profile	Typical_Client_Densi

Buttons: Cancel, Apply to Device

C9800 - AP에 태그 할당

정의된 태그를 구축의 개별 AP에 할당하는 데 사용할 수 있는 두 가지 옵션이 있습니다.

- AP Name(AP 이름) 필드의 패턴과 일치하는 regex 규칙을 활용하는 AP 이름 기반 할당 (Configure(구성) > Tags & Profiles(태그 및 프로파일) > Tags(태그) > AP > Filter(필터))

- AP 이더넷 MAC 주소 기반 할당 (Configure(구성) > Tags & Profiles(태그 및 프로파일) > Tags(태그) > AP > Static(고정))

DNA Center를 사용하는 프로덕션 구축에서는 DNAC 및 AP PNP 워크플로를 사용하거나 수동 AP당 할당을 방지하기 위해 9800에서 사용 가능한 정적 대량 CSV(Comma-Separated Values) 업로드 방법을 사용하는 것이 좋습니다. Configure(구성) > Tags & Profiles(태그 및 프로파일) > Tags(태그) > AP > Static(정적) > Add(추가)로 이동합니다(Upload File(파일 업로드) 옵션 참고).

- AP MAC 주소: <AP_ETHERNET_MAC>

- 정책 태그 이름: PT_CAN01

- 사이트 태그 이름: ST_CAN01

- RF 태그 이름: 지사 RF

참고: Cisco IOS®-XE 17.3.4c부터 컨트롤러당 최대 1,000개의 regex 규칙이 적용됩니다. 구축의 사이트 수가 이 수를 초과하면 MAC당 고정 할당을 활용해야 합니다.

Associate Tags to AP



AP MAC Address*	aaaa.bbbb.cccc
Policy Tag Name	PT_CAN01
Site Tag Name	ST_CAN01
RF Tag Name	Branch_RF

Cancel

Apply to Device

참고: 또는 AP 이름 regex 기반 태그 할당 방법을 활용하려면 Configure(구성) > Tags & Profiles(태그 및 프로필) > Tags(태그) > AP > Filter(필터) > Add(추가)로 이동합니다.

-이름: BR_CAN01

- AP 이름 regex: BR-CAN01-.{7}(이 규칙은 조직 내에서 채택된 AP 이름 규칙에 일치합니다. 이 예에서 태그는 'BR_CAN01-' 뒤에 7개의 문자가 포함된 AP 이름 필드가 있는 AP에 할당됩니다.)

-우선순위: 1

- 정책 태그 이름: PT_CAN01(정의된 대로)

- 사이트 태그 이름: ST_CAN01

- RF 태그 이름: 지사 RF

Associate Tags to AP



⚠ Rule "BR-CAN01" has this priority. Assigning it to the current rule will swap the priorities.

Rule Name*	BR_CAN01	Policy Tag Name	PT_CAN01
AP name regex*	BR-CAN01-.{7}	Site Tag Name	ST_CAN01
Active	YES <input checked="" type="checkbox"/>	RF Tag Name	Branch_RF
Priority*	1		

Cancel

Apply to Device

Aruba CPPM 인스턴스 구성

Aruba CPPM 컨피그레이션을 기반으로 한 프로덕션/모범 사례에 대해서는 현지 HPE Aruba SE 리소스에 문의하십시오.

Aruba ClearPass 서버 초기 컨피그레이션

Aruba ClearPass는 다음 리소스를 할당하는 ESXi <> 서버에서 OVF(Open Virtualization Format) 템플릿을 사용하여 구축됩니다.

- 예약된 가상 CPU 2개
- 6GB RAM
- 80GB 디스크(시스템 전원을 켜기 전에 초기 VM 구축 후 수동으로 추가해야 함)

라이선스 신청

다음은 통해 플랫폼 라이선스를 적용합니다. 관리 > 서버 관리자 > 라이선스. 플랫폼, 액세스 및 온보드 라이선스를 추가합니다.

서버 호스트 이름

Administration(관리) > Server Manager(서버 관리자) > Server Configuration(서버 컨피그레이션)으로 이동하고 새로 프로비저닝된 CPPM 서버를 선택합니다.

- 호스트 이름: cppm

- FQDN: cppm.example.com

- 관리 포트 IP 주소 지정 및 DNS 확인

Administration > Server Manager > Server Configuration - cppm

Server Configuration - cppm (10.85.54.98)

System	Services Control	Service Parameters	System Monitoring	Network	FIPS
Hostname:	cppm				
FQDN:	cppm.example.com				
Policy Manager Zone:	default				Manage F
Enable Performance Monitoring Display:	<input checked="" type="checkbox"/> Enable this server for performance monitoring display				
Insight Setting:	<input checked="" type="checkbox"/> Enable Insight <input checked="" type="checkbox"/> Enable as Insight Master Current Master:cppm(10.85.54.98)				
Enable Ingress Events Processing:	<input type="checkbox"/> Enable Ingress Events processing on this server				
Master Server in Zone:	Primary master				
Span Port:	-- None --				
		IPv4	IPv6	Action	
Management Port	IP Address	10.85.54.98		Configure	
	Subnet Mask	255.255.255.224			
	Default Gateway	10.85.54.97			
Data/External Port	IP Address			Configure	
	Subnet Mask				
	Default Gateway				
DNS Settings	Primary	10.85.54.122		Configure	
	Secondary				
	Tertiary				
	DNS Caching	Disabled			

CPPM 웹 서버 인증서(HTTPS) 생성

이 인증서는 ClearPass Guest Portal 페이지가 HTTPS를 통해 브랜치의 게스트 Wifi에 연결하는 게스트 클라이언트에 제공될 때 사용됩니다.

1단계. CA pub chain 인증서를 업로드합니다.

Administration > Certificates > Trust List > Add로 이동합니다.

- 사용법: 기타 사용

View Certificate Details	
Subject DN:	
Issuer DN:	
Issue Date/Time:	Dec 23, 2020 16:55:10 EST
Expiry Date/Time:	Dec 24, 2025 17:05:10 EST
Validity Status:	Valid
Signature Algorithm:	SHA256WithRSAEncryption
Public Key Format:	X.509
Serial Number:	86452691282006080280068723651711271611
Enabled:	true
Usage:	<input checked="" type="checkbox"/> EAP <input checked="" type="checkbox"/> RadSec <input checked="" type="checkbox"/> Database <input checked="" type="checkbox"/> Others
<input type="button" value="Update"/> <input type="button" value="Disable"/> <input type="button" value="Export"/> <input type="button" value="Close"/>	

2단계. 인증서 서명 요청을 생성합니다.

Administration > Certificates > Certificate Store > Server Certificates > Usage로 이동합니다.
HTTPS 서버 인증서.

- Create Certificate Signing Request(인증서 서명 요청 생성) 클릭

- 공용 이름: CPPM

- 조직: cppm.example.com

SAN 필드를 채워야 합니다(SAN에는 공통 이름이 있어야 하며 필요에 따라 IP 및 기타 FQDN도 있어야 함). 형식은 DNS입니다. <fqdn1>,DNS:<fqdn2>,IP<ip1>.

Create Certificate Signing Request

Common Name (CN):	cppm
Organization (O):	Cisco
Organizational Unit (OU):	Engineering
Location (L):	Toronto
State (ST):	ON
Country (C):	CA
Subject Alternate Name (SAN):	DNS:cppm.example.com
Private Key Password:
Verify Private Key Password:
Private Key Type:	2048-bit RSA
Digest Algorithm:	SHA-512

3단계. 선택한 CA에서 새로 생성된 CPPM HTTPS 서비스 CSR에 서명합니다.

4단계. Certificate Template(인증서 템플릿) > Web Server(웹 서버) > Import Certificate(인증서 가져오기)로 이동합니다.

- 인증서 유형: 서버 인증서
- 사용법: HTTP 서버 인증서
- 인증서 파일: CA 서명 CPPM HTTPS 서비스 인증서 찾아보기 및 선택

Import Certificate

Certificate Type:	Server Certificate
Server:	cppm
Usage:	HTTPS Server Certificate
Upload Method:	Upload Certificate and Use Saved Private Key
Certificate File:	Browse... No file selected.

C9800 WLC를 네트워크 디바이스로 정의

Configuration(컨피그레이션) > Network(네트워크) > Devices(디바이스) > Add(추가)로 이동합니다.

- 이름: WLC_9800_지사
- IP 또는 서브넷 주소: 10.85.54.99(랩 토폴로지 다이어그램 참조)
- RADIUS 공유 Cisco: <WLC RADIUS 암호>
- 공급업체 이름: Cisco
- RADIUS 동적 권한 부여 활성화: 1700

게스트 포털 페이지 및 CoA 타이머

구성 전체에서 올바른 타이머 값을 설정하는 것은 매우 중요합니다. 타이머가 조정되지 않은 경우 클라이언트가 'Run State'에 있지 않은 상태에서 순환 웹 포털 리디렉션으로 실행될 수 있습니다. 다음에 유의할 타이머:

- 포털 웹 로그인 타이머: 이 타이머는 상태 전환을 CPPM 서비스에 알리고, 엔드포인트 사용자 지정 특성 'Allow-Guest-Internet' 값을 등록하고, CPPM에서 WLC로의 CoA 프로세스를 트리거하기 위해 게스트 포털 페이지에 대한 액세스를 허용하기 전에 리디렉션 페이지를 지연시킵니다. **Guest > Configuration > Pages > Web Logins**로 이동합니다.
 - 게스트 포털 이름 선택: Lab Anonymous Guest Registration(이 게스트 포털 페이지 컨피그레이션은 다음과 같이 자세히 표시됨)
 - Edit를 클릭합니다.
 - 로그인 지연: 6초

- ClearPass CoA 지연 타이머: 따라서 ClearPass에서 WLC로의 CoA 메시지 생성이 지연됩니다. 이는 CPPM이 WLC에서 CoA 승인(ACK)이 반환되기 전에 내부적으로 클라이언트 엔드포인트의 상태를 성공적으로 전환하기 위해 필요합니다. 랩 테스트에서는 WLC의 밀리초 미만의 응답 시간을 보여 주며, CPPM이 엔드포인트 특성 업데이트를 완료하지 않은 경우 WLC의 새 RADIUS 세션이 인증되지 않은 MAB 서비스 시행 정책과 일치하며 클라이언트에 다시 리디렉션 페이지가 제공됩니다. CPPM > Administration(관리) > Server Manager(서버 관리자) >

Server Configuration(서버 컨피그레이션)으로 이동하고 CPPM Server(CPPM 서버) > Service Parameters(서비스 매개변수)를 선택합니다.

- RADIUS 동적 권한 부여(DM/CoA) 지연 - 6초로 설정



ClearPass - 게스트 CWA 컨피그레이션

ClearPass측 CWA 컨피그레이션은 (3) 서비스 포인트/단계로 구성됩니다.

ClearPass 구성 요소	서비스 유형	목적
1. 정책 관리자	서비스: Mac 인증	사용자 지정 특성 Allow-Guest-Internet = TRUE 이면 네트워크 허용합니다. 그렇지 않으면 리디렉션 및 COA를 트리거합니다. 재인증 명령 로그인 AUP 페이지를 표시합니다.
2. 게스트	웹 로그인	Post-auth set custom attribute Allow-Guest-Internet = TRUE . 엔드포인트를 알려진 상태로 업데이트
3. 정책 관리자	서비스: 웹 기반 인증	사용자 지정 특성 Allow-Guest-Internet = TRUE 설정 COA: 재인증

ClearPass 끝점 메타데이터 특성: 게스트 인터넷 허용

클라이언트가 'Webauth Pending' 및 'Run' 상태 간에 전환될 때 게스트 엔드포인트 상태를 추적하려면 Boolean 형식의 메타데이터 특성을 만듭니다.

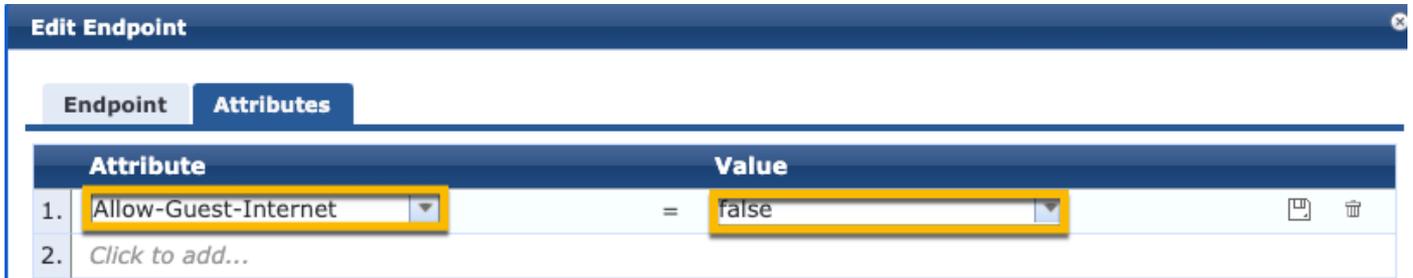
- wifi에 연결하는 새 게스트의 기본 메타데이터 특성이 Allow-Guest-Internet=false로 설정되어 있습니다. 이 특성에 따라 클라이언트 인증은 MAB 서비스를 통해 이동

- AUP Accept(AUP 수락) 버튼을 클릭하면 게스트 클라이언트의 메타데이터 특성이 Allow-Guest-Internet=true로 업데이트됩니다. True(참)로 설정된 이 특성에 기반한 후속 MAB는 인터넷에 리디렉션되지 않은 액세스를 허용합니다

ClearPass > Configuration(컨피그레이션) > Endpoints(엔드포인트)로 이동하고 목록에서 엔드포인트

트를 선택하고 **Attributes(특성)** 탭을 클릭한 다음 **Allow-Guest-Internet** with value **false** and **Save(잘못된 값과 Save)**를 추가합니다.

참고: 동일한 엔드포인트를 편집하고 바로 이 특성을 삭제할 수도 있습니다. 이 단계에서는 정책에서 사용할 수 있는 Endpoints 메타데이터 DB에 필드를 생성합니다.



ClearPass 시행 정책 구성 재인증

클라이언트가 게스트 포털 페이지에서 AUP를 수락 한 직후 게스트 클라이언트에 할당 된 적용 프로파일을 작성 합니다.

ClearPass > Configuration > Profiles > Add로 이동합니다.

- 템플릿: RADIUS 동적 권한 부여

-이름: Cisco_WLC_Guest_COA

Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Profile	Attributes	Summary
Template:	RADIUS Dynamic Authorization	
Name:	Cisco_WLC_Guest_COA	
Description:		
Type:	RADIUS_CoA	
Action:	<input checked="" type="radio"/> Accept <input type="radio"/> Reject <input type="radio"/> Drop	
Device Group List:	<div style="display: flex; align-items: center;"> <div style="flex-grow: 1;"> <input type="text"/> </div> <div style="margin-left: 10px;"> <input type="button" value="Remove"/> <input type="button" value="View Details"/> <input type="button" value="Modify"/> </div> </div>	
	<input type="text" value="--Select--"/>	

반경:IETF

호출 스테이션 Id

%{Radius:IETF:Calling-Station

Radius:Cisco

Cisco-AVPair

subscriber:command=reauth
e

Radius:Cisco

Cisco-AVPair

%{Radius:Cisco:Cisco-AVPair:subscriber:audit-session} 가입자:reauthenticate-type=last type=last

Radius:Cisco

Cisco-AVPair

ClearPass 게스트 포털 리디렉션 적용 프로파일 컨피그레이션

'Allow-Guest-Internet'이 'true'로 설정된 CPPM 엔드포인트 데이터베이스에서 MAC 주소를 찾을 수 없는 경우 초기 MAB 단계 중에 게스트에 적용되는 시행 프로필을 생성합니다.

그러면 9800 WLC에서 외부 인증을 위해 게스트 클라이언트를 CPPM 게스트 포털로 리디렉션합니다.

ClearPass > Enforcement > Profiles > Add로 이동합니다.

-이름: Cisco_Portal_Redirect

-유형: RADIUS

-작업: 수락

Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Profile	Attributes	Summary
Template:	Aruba RADIUS Enforcement	
Name:	Cisco_Portal_Redirect	
Description:		
Type:	RADIUS	
Action:	<input checked="" type="radio"/> Accept <input type="radio"/> Reject <input type="radio"/> Drop	
Device Group List:		<div style="text-align: right;"> <input type="button" value="Remove"/> <input type="button" value="View Details"/> <input type="button" value="Modify"/> </div>
		--Select--

ClearPass 리디렉션 적용 프로파일

동일한 대화 상자의 Attributes(특성) 탭에서 이 이미지에 따라 두 개의 특성을 구성합니다.

Enforcement Profiles - Cisco_Portal_Redirect

Summary	Profile	Attributes
Type	Name	Value
1. Radius:Cisco	Cisco-AVPair	= url-redirect-acl=CAPTIVE_PORTAL_REDIRECT
2. Radius:Cisco	Cisco-AVPair	= url-redirect=https://cpm.example.com/guest/accept.php?cmd-login&mac=%{Connection:Client-Mac-Address-Hyphen}&switchip=%{Radius:IETF:NAS-IP-Address}

ClearPass 리디렉션 프로파일 특성

url-redirect-acl 특성은 C9800에서 생성된 ACL의 이름인 CAPTIVE-PORTAL-REDIRECT로 설정됩니다.

참고: ACL에 대한 참조만 RADIUS 메시지에 전달되고 ACL 내용은 전달되지 않습니다. 그림과 같이 9800 WLC에 생성된 ACL의 이름이 이 RADIUS 특성의 값과 정확히 일치해야 합니다.

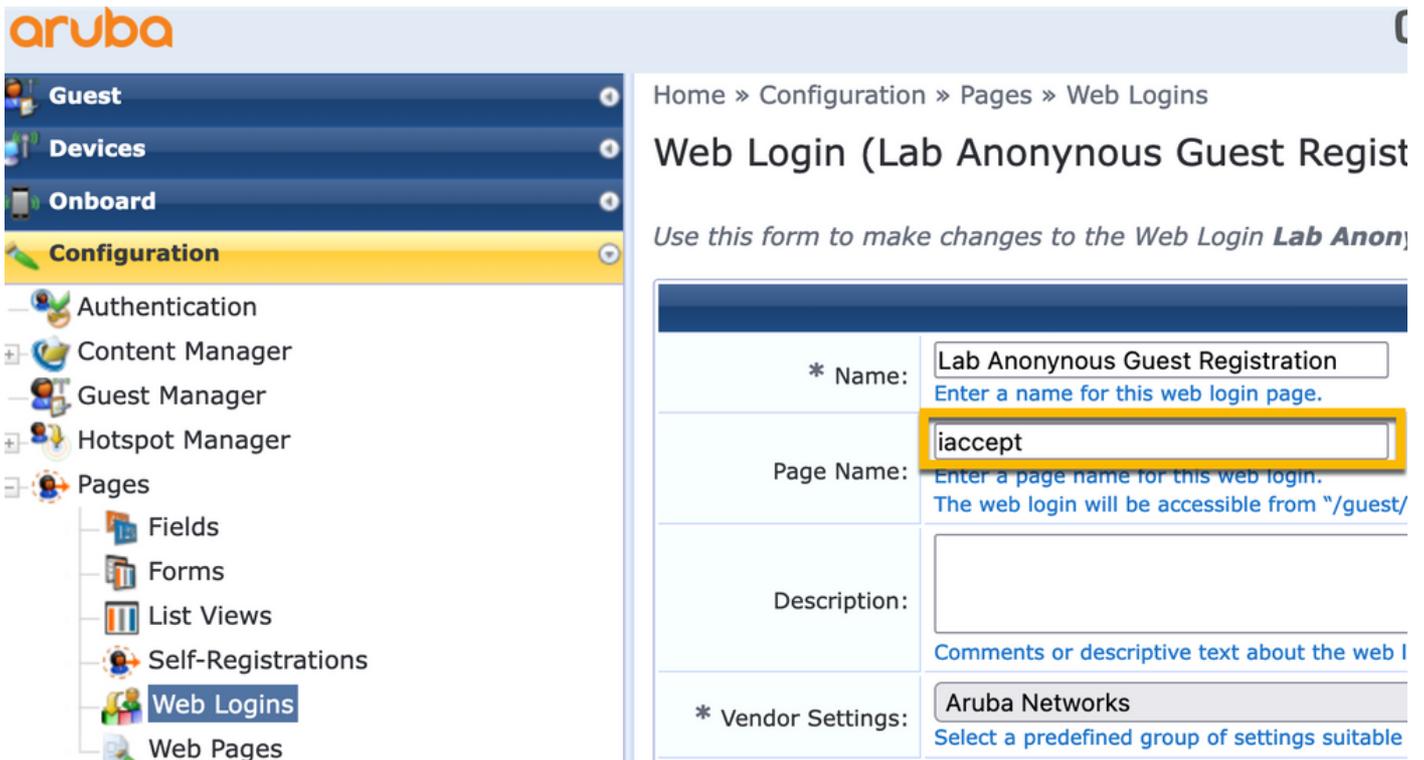
url-redirect 특성은 여러 매개변수로 구성됩니다.

- 게스트 포털이 호스팅되는 대상 URL, <https://cppm.example.com/guest/iaccept.php>
- 게스트 클라이언트 MAC, 매크로 %{Connection:Client-Mac-Address-Hyphen}
- 인증 기관 IP(9800 WLC에서 리디렉션 트리거), 매크로 %{Radius:IETF:NAS-IP-Address}
- cmd-login 작업

ClearPass 게스트 웹 로그인 페이지의 URL은 CPPM(CPPM) > Guest(게스트) > Configuration(컨피그레이션) > Pages(페이지) > Web Logins(웹 로그인) > Edit(편집)로 이동할 때 표시됩니다.

이 예에서는 CPPM의 게스트 포털 페이지 이름이 iaccept로 정의됩니다.

참고: 게스트 포털 페이지의 컨피그레이션 단계는 다음과 같습니다.



참고: Cisco 디바이스의 경우 audit_session_id가 일반적으로 사용되지만 다른 벤더에서는 지원되지 않습니다.

ClearPass 메타데이터 적용 프로필 컨피그레이션

CPPM에서 상태 전환 추적에 사용되는 엔드포인트 메타데이터 특성을 업데이트하도록 시행 프로필을 구성합니다.

이 프로파일은 엔드포인트 데이터베이스의 게스트 클라이언트 MAC 주소 항목에 적용되며 'Allow-

'Guest-Internet' 인수를 'true'로 설정합니다.

ClearPass > Enforcement > Profiles > Add로 이동합니다.

- 템플릿: ClearPass 엔터티 업데이트 적용

-유형: Post_Authentication

Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Profile | Attributes | Summary

Template:	ClearPass Entity Update Enforcement
Name:	Make-Cisco-Guest-Valid
Description:	
Type:	Post_Authentication
Action:	<input checked="" type="radio"/> Accept <input type="radio"/> Reject <input type="radio"/> Drop
Device Group List:	<div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div> <div style="text-align: right;"><button>Remove</button> <button>View Details</button> <button>Modify</button></div>

동일한 대화 상자에서 Attributes 탭을 선택합니다.

-유형: 엔드포인트

-이름: 게스트 인터넷 허용

참고: 이 이름이 드롭다운 메뉴에 나타나도록 하려면 단계에 설명된 대로 하나 이상의 엔드포인트에 대해 이 필드를 수동으로 정의해야 합니다.

-가치: 참

Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Profile | **Attributes** | Summary

Type	Name	Value
1. Endpoint	Allow-Guest-Internet	= true
2. Click to add...		

ClearPass 게스트 인터넷 액세스 적용 정책 컨피그레이션

ClearPass > Enforcement > Policies > Add로 이동합니다.

-이름: WLC Cisco 게스트 허용

- 적용 유형: RADIUS

- 기본 프로필: Cisco_Portal_Redirect

Configuration » Enforcement » Policies » Add

Enforcement Policies

The screenshot shows the 'Enforcement Policies' configuration page. It has three tabs: 'Enforcement', 'Rules', and 'Summary'. The 'Enforcement' tab is active. The 'Name' field contains 'WLC Cisco Guest Allow'. The 'Description' field is empty. The 'Enforcement Type' is set to 'RADIUS' with radio buttons for 'TACACS+', 'WEBAUTH (SNMP/Agent/CLI/CoA)', 'Application', and 'Event'. The 'Default Profile' is set to 'Cisco_Portal_Redirect' with a dropdown menu. There are 'View Details' and 'Modify' buttons.

동일한 대화 상자에서 Rules(규칙) 탭으로 이동하고 Add Rule(규칙 추가)을 클릭합니다.

-유형: 엔드포인트

-이름: 게스트 인터넷 허용

- 연산자: 같음

- 값 True

- 프로필 이름/추가할 항목 선택: [RADIUS] [액세스 프로필 허용]

The screenshot shows the 'Rules Editor' configuration page. It has two main sections: 'Conditions' and 'Enforcement Profiles'. The 'Conditions' section has a header 'Match ALL of the following conditions:' and a table with columns 'Type', 'Name', 'Operator', and 'Value'. The first row is highlighted with a yellow box and contains: Type: Endpoint, Name: Allow-Guest-Internet, Operator: EQUALS, Value: true. The second row is 'Click to add...'. The 'Enforcement Profiles' section has a 'Profile Names:' label and a dropdown menu with '[RADIUS] [Allow Access Profile]' selected. There are 'Move Up ↑', 'Move Down ↓', and 'Remove' buttons. At the bottom right, there are 'Save' and 'Cancel' buttons.

ClearPass 게스트 사후 AUP 시행 정책 컨피그레이션

ClearPass > Enforcement > Policies > Add로 이동합니다.

-이름: Cisco WLC 웹 인증 시행 정책

- 적용 유형: WEBAUTH(SNMP/에이전트/CLI/CoA)
- 기본 프로필: [RADIUS_CoA] Cisco_Reauthenticate_Session

Configuration » Enforcement » Policies » Add

Enforcement Policies

Enforcement	Rules	Summary
Name:	Cisco WLC Webauth Enforcement Policy	
Description:		
Enforcement Type:	<input type="radio"/> RADIUS <input type="radio"/> TACACS+ <input checked="" type="radio"/> WEBAUTH (SNMP/Agent/CLI/CoA) <input type="radio"/> Application <input type="radio"/> Event	
Default Profile:	[RADIUS_CoA] Cisco_Reautht	<input type="button" value="View Details"/> <input type="button" value="Modify"/>

동일한 대화 상자에서 **Rules > Add**로 이동합니다.

- 조건: 인증
- 이름: 상태
- 연산자: 같음
- 가치: 사용자
- 프로필 이름: <각각 추가>
- [인증 후] [엔드포인트 알 수 있는 업데이트]
- [인증 후] [Make-Cisco-Guest-Valid]
- [RADIUS_CoA] [Cisco_WLC_Guest_COA]

Rules Editor

Conditions

Match ALL of the following conditions:

Type	Name	Operator	Value
1. Authentication	Status	EQUALS	User
2.	Click to add...		

Enforcement Profiles

Profile Names:	[Post Authentication] [Update Endpoint Known] [Post Authentication] Make-Cisco-Guest-Valid [RADIUS_CoA] Cisco_WLC_Guest_COA	<input type="button" value="Move Up ↑"/> <input type="button" value="Move Down ↓"/> <input type="button" value="Remove"/>
	<input type="text" value="--Select to Add--"/>	

참고: 연속 게스트 포털 리디렉션 의사 브라우저 팝업으로 시나리오를 실행하는 경우 CPPM 타이머를 조정해야 하거나 RADIUS CoA 메시지가 CPPM과 9800 WLC 간에 제대로 교환되지 않음을 나타냅니다. 이러한 사이트를 확인합니다.

- CPPM > Monitoring > Live Monitoring > Access Tracker로 이동하고 RADIUS 로그 항목에 RADIUS CoA 세부 정보가 포함되어 있는지 확인합니다.

- 9800 WLC에서 Troubleshooting(문제 해결) > Packet Capture(패킷 캡처)로 이동하고 RADIUS CoA 패킷이 도착할 것으로 예상되는 인터페이스에서 pcap를 활성화하고 CPPM에서 RADIUS CoA 메시지가 수신되는지 확인합니다.

ClearPass MAB 인증 서비스 컨피그레이션

서비스는 AV(특성 값) 쌍 Radius에서 일치합니다. Cisco | CiscoAVPair | cisco-wlan-ssid

ClearPass > Configuration > Services > Add로 이동합니다.

서비스 탭:

-이름: 게스트 포털 - Mac 인증

-유형: MAC 인증

- 추가 옵션: Authorization(권한 부여), Profile Endpoints(엔드포인트 프로파일)를 선택합니다.

일치 규칙 추가:

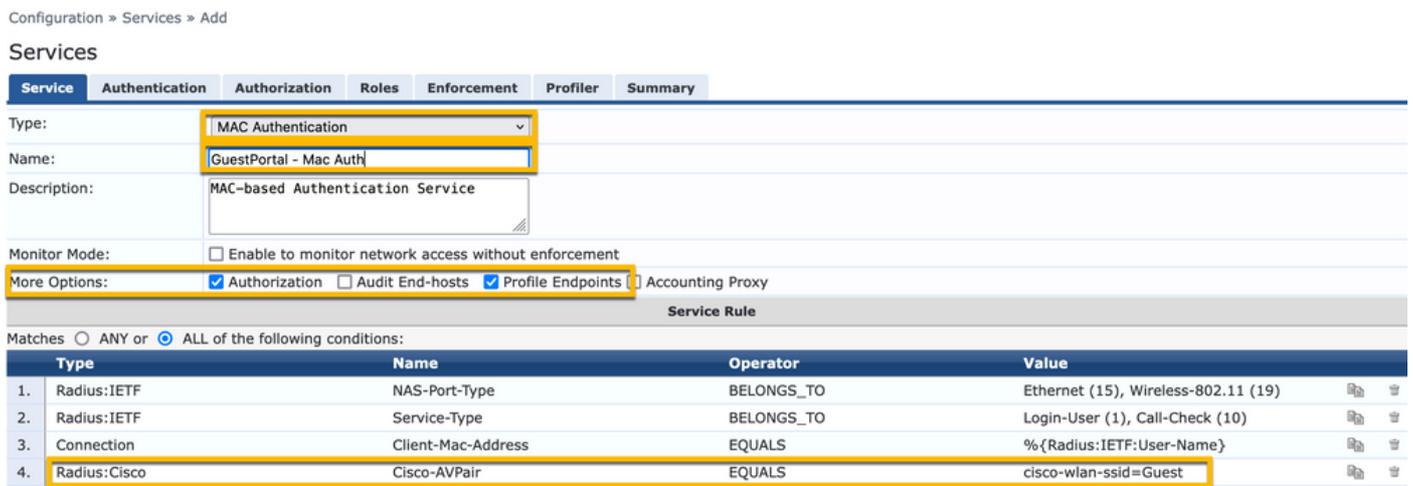
-유형: RADIUS: Cisco

-이름: Cisco-AVPair

- 연산자: 같음

-가치: cisco-wlan-ssid=게스트(구성된 게스트 SSID 이름 일치)

참고: 'Guest'는 9800 WLC에서 브로드캐스트한 게스트 SSID의 이름입니다.



동일한 대화 상자에서 Authentication(인증) 탭을 선택합니다.

- 인증 방법: [MAC AUTH] 제거, 추가 [모든 MAC AUTH 허용]

- 인증 소스: [엔드포인트 저장소][로컬 SQL DB], [게스트 사용자 저장소][로컬 SQL DB]

Configuration » Services » Edit - GuestPortal - Mac Auth

Services - GuestPortal - Mac Auth

Summary Service **Authentication** Authorization Roles Enforcement Profiler

Authentication Methods: [Allow All MAC AUTH]

Authentication Sources: [Endpoints Repository] [Local SQL DB] [Guest User Repository] [Local SQL DB]

Strip Username Rules: Enable to specify a comma-separated list of rules to strip username prefixes or suffixes

동일한 대화 상자에서 적용 탭을 선택합니다.

- 시행 정책: WLC Cisco 게스트 허용

Configuration » Services » Add

Services

Service Authentication Roles **Enforcement** Summary

Use Cached Results: Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: WLC Cisco Guest Allow **Modify**

Enforcement Policy Details

Description:	MAB Enforcement Redirect
Default Profile:	Cisco_Portal_Redirect
Rules Evaluation Algorithm:	first-applicable

Conditions	Enforcement Profiles
1. (Endpoint:Allow-Guest-Internet EQUALS true)	[Allow Access Profile]

동일한 대화 상자에서 적용 탭을 선택합니다.

Configuration » Services » Add

Services

Service Authentication Authorization Roles Enforcement **Profiler** Summary

Endpoint Classification: Select the classification(s) after which an action must be triggered -

RADIUS CoA Action: Cisco_Reauthenticate_Session **View Details** **Modify**

ClearPass Webauth 서비스 컨피그레이션

ClearPass > Enforcement > Policies > Add로 이동합니다.

-이름: Guest_Portal_Webauth

-유형: 웹 기반 인증

Configuration » Services » Add

Services

Service	Authentication	Roles	Enforcement	Summary
Type:	Web-based Authentication			
Name:	Guest			
Description:				
Monitor Mode:	<input type="checkbox"/> Enable to monitor network access without enforcement			
More Options:	<input type="checkbox"/> Authorization <input type="checkbox"/> Posture Compliance			
Matches <input type="radio"/> ANY or <input checked="" type="radio"/> ALL of the following conditions:				
Type	Name			
1.	Host	CheckType		
2.	Click to add...			

동일한 대화 상자의 **Enforcement** 탭에서 Enforcement Policy: Cisco WLC Webauth 시행 정책.

Configuration » Services » Add

Services

Service	Authentication	Roles	Enforcement	Summary
Use Cached Results:	<input type="checkbox"/> Use cached Roles and Posture attributes from previous sessions			
Enforcement Policy:	Cisco WLC Webauth Enforcement Policy Modify			Add New Enforcement Poli
Enforcement Policy Details				
Description:				
Default Profile:	Cisco_Reauthenticate_Session			
Rules Evaluation Algorithm:	first-applicable			
Conditions	Enforcement Profiles			
1. (Authentication:Status EQUALS User)	[Update Endpoint Known], Make-Cisco-Guest-Valid, Cisco_Reauthenticate_Session			

ClearPass - 웹 로그인

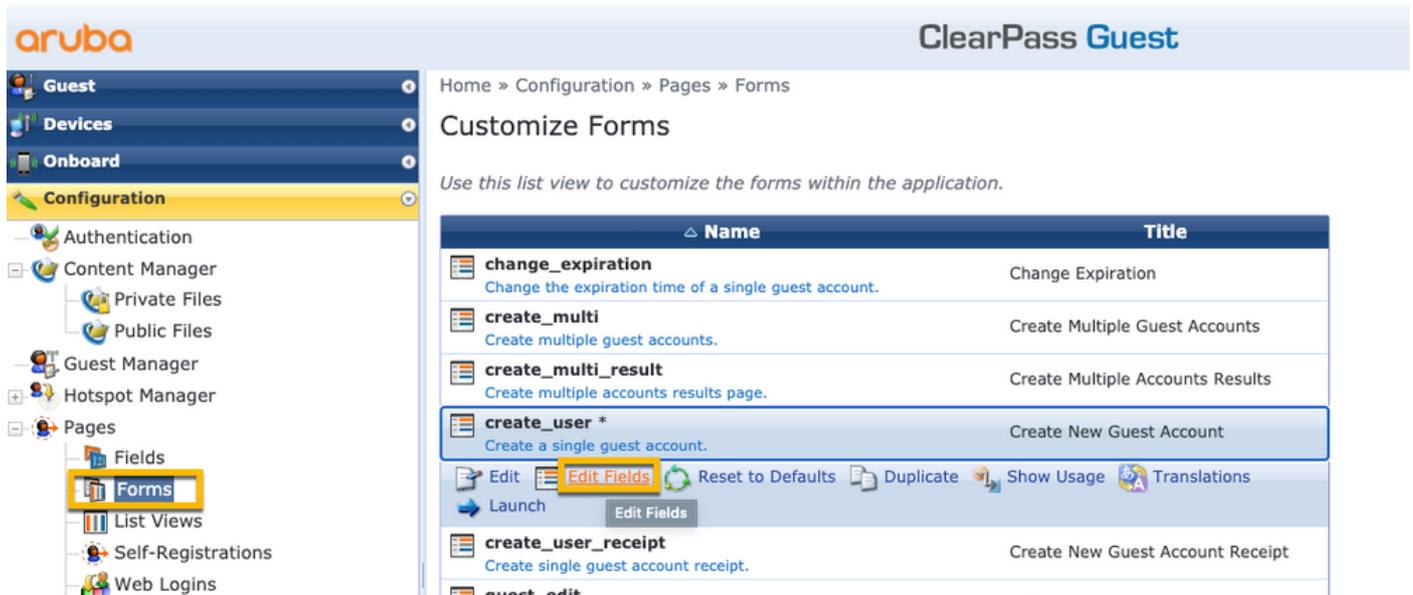
익명 AUP 게스트 포털 페이지의 경우 비밀번호 필드가 없는 단일 사용자 이름을 사용합니다.

사용되는 사용자 이름에는 다음 필드가 정의되어 있어야 합니다.

사용자 이름_인증 | 사용자 이름 인증: | 1

사용자에 대한 'username_auth' 필드를 설정하려면 먼저 'edit user'(사용자 수정) 양식에 해당 필드

를 표시해야 합니다. ClearPass > Guest > Configuration > Pages > Forms로 이동하고 create_user form을 선택합니다.



visitor_name(행 20)을 선택하고 Insert After(다음에 삽입)를 클릭합니다.

Home > Configuration > Pages > Forms

Customize Form Fields (create_user)

Use this list view to modify the fields of the form **create_user**.

Rank	Field	Type	Label	Description
1	enabled	dropdown	Account Status:	Select an option for changing the status of this account.
10	sponsor_name	text	Sponsor's Name:	Name of the person sponsoring this account.
13	sponsor_profile_name	text	Sponsor's Profile:	Profile of the person sponsoring this account.
15	sponsor_email	text	Sponsor's Email:	Email of the person sponsoring this account.
20	visitor_name	text	Guest's Name:	Name of the guest.

Edit Edit Base Field Remove Insert Before **Insert After** Disable Field

Customize Form Field (new)

Use this form to add a new field to the form **create_user**.

Form Field Editor	
* Field Name:	<input type="text" value="username_auth"/> <small>Select the field definition to attach to the form.</small>
Form Display Properties <small>These properties control the user interface displayed for this field.</small>	
Field:	<input checked="" type="checkbox"/> Enable this field <small>When checked, the field will be included as part of the form.</small>
* Rank:	<input type="text" value="22"/> <small>Number indicating the relative ordering of user interface fields, which are displayed in order of increasing rank.</small>
* User Interface:	<input type="text" value="No user interface"/> <input type="button" value="Revert"/> <small>The kind of user interface element to use when entering or editing this field.</small>
Form Validation Properties <small>These properties control how the value of this field is checked.</small>	
Field Required:	<input type="checkbox"/> Field value must be supplied <small>Select this option if the field cannot be omitted or left blank.</small>
Initial Value:	<input type="text" value="1"/> <input type="button" value="Revert"/> <small>value to initialize this field with when the form is first displayed.</small>
* Validator:	<input type="text" value="IsValidBool"/> <small>The function used to validate the contents of a field.</small>
Validator Param:	<input type="text" value="(None)"/> <small>Optional name of field whose value will be supplied as the argument to a validator.</small>
Validator Argument:	<input type="text"/> <small>Optional value to supply as the argument to a validator.</small>
Validation Error:	<input type="text"/> <small>The error message to display if the field's value fails validation and the validator does not return an error message directly.</small>

이제 AUP 게스트 포털 페이지 뒤에서 사용할 사용자 이름을 생성합니다.

CPPM > Guest > Manage Accounts > Create로 이동합니다.

- 게스트 이름: 게스트와이파이
- 회사 이름: Cisco
- 이메일 주소: guest@example.com
- 사용자 이름 인증: 사용자 이름만 사용하여 게스트 액세스를 허용합니다. 사용
- 계정 활성화: 지금
- 계정 만료: 계정이 만료되지 않음
- 이용 약관: 후원자: 사용

Create Guest Account

New guest account being created by **admin**.

Create New Guest Account	
* Guest's Name:	<input type="text" value="GuestWiFi"/> Name of the guest.
* Company Name:	<input type="text" value="Cisco"/> Company name of the guest.
* Email Address:	<input type="text" value="guest@example.com"/> The guest's email address. This will become their username to log into the network.
Username Authentication:	<input checked="" type="checkbox"/> Allow guest access using their username only Guests will require the login screen setup for username-based authentication as well.
Account Activation:	<input type="text" value="Now"/> Select an option for changing the activation time of this account.
Account Expiration:	<input type="text" value="Account will not expire"/> Select an option for changing the expiration time of this account.
* Account Role:	<input type="text" value="[Guest]"/> Role to assign to this account.
Password:	281355
Notes:	<input type="text"/>
* Terms of Use:	<input checked="" type="checkbox"/> I am the sponsor of this account and accept the terms of use
<input type="button" value="Create"/>	

웹 로그인 양식을 만듭니다. CPPM > Guest > Configuration > Web Logins로 이동합니다.

인증 후 섹션의 엔드포인트 특성:

사용자 이름 | 사용자 이름
방문자 이름 | 방문자 이름
cn | 방문자 이름
방문자 전화 | 방문자 전화
email | 이메일
메일 | 이메일
스폰서_이름 | 스폰서 이름
스폰서_이메일 | 스폰서 이메일
게스트 인터넷 허용 | 참

CPPM에서 Live Monitoring(라이브 모니터링) > Access Tracker(액세스 추적기)로 이동합니다.

MAB 서비스를 연결 하고 시작 하는 새 게스트 사용자 입니다.

요약 탭:

Summary	Input	Output	RADIUS CoA
Login Status:	ACCEPT		
Session Identifier:	R0000471a-01-6282a110		
Date and Time:	May 16, 2022 15:08:00 EDT		
End-Host Identifier:	d4-3b-04-7a-64-7b (Computer / Windows / Windows)		
Username:	d43b047a647b		
Access Device IP/Port:	10.85.54.99:73120 (WLC_9800_Branch / Cisco)		
Access Device Name:	wlc01		
System Posture Status:	UNKNOWN (100)		
Policies Used -			
Service:	Guest SSID - GuestPortal - Mac Auth		
Authentication Method:	MAC-AUTH		
Authentication Source:	None		
Authorization Source:	[Guest User Repository], [Endpoints Repository]		
Roles:	[Employee], [User Authenticated]		
Enforcement Profiles:	Cisco Portal Redirect		

◀ ◀ Showing 8 of 1-8 records ▶ ▶ [Change Status](#) [Show Configuration](#) [Export](#) [Show Logs](#) [Close](#)

동일한 대화 상자에서 입력 탭으로 이동합니다.

Request Details

Summary Input Output **RADIUS CoA**

Username:	d43b047a647b
End-Host Identifier:	d4-3b-04-7a-64-7b (Computer / Windows / Windows)
Access Device IP/Port:	10.85.54.99:73120 (WLC_9800_Branch / Cisco)

RADIUS Request

Radius:Airespace:Airespace-Wlan-Id	4
Radius:Cisco:Cisco-AVPair	audit-session-id=6336550A00006227CE452457
Radius:Cisco:Cisco-AVPair	cisco-wlan-ssid=Guest
Radius:Cisco:Cisco-AVPair	client-iif-id=1728058392
Radius:Cisco:Cisco-AVPair	method=mab
Radius:Cisco:Cisco-AVPair	service-type=Call Check
Radius:Cisco:Cisco-AVPair	vlan-id=21
Radius:Cisco:Cisco-AVPair	wlan-profile-name=WP_Guest
Radius:IETF:Called-Station-Id	14-16-9d-df-16-20:Guest
Radius:IETF:Calling-Station-Id	d4-3b-04-7a-64-7b

◀ ◀ Showing 8 of 1-8 records ▶ ▶ [Change Status](#) [Show Configuration](#) [Export](#) [Show Logs](#) [Close](#)

동일한 대화 상자에서 출력 탭으로 이동합니다.

Request Details

Summary Input **Output** RADIUS CoA

Enforcement Profiles:	Cisco_Portal_Redirect
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

RADIUS Response

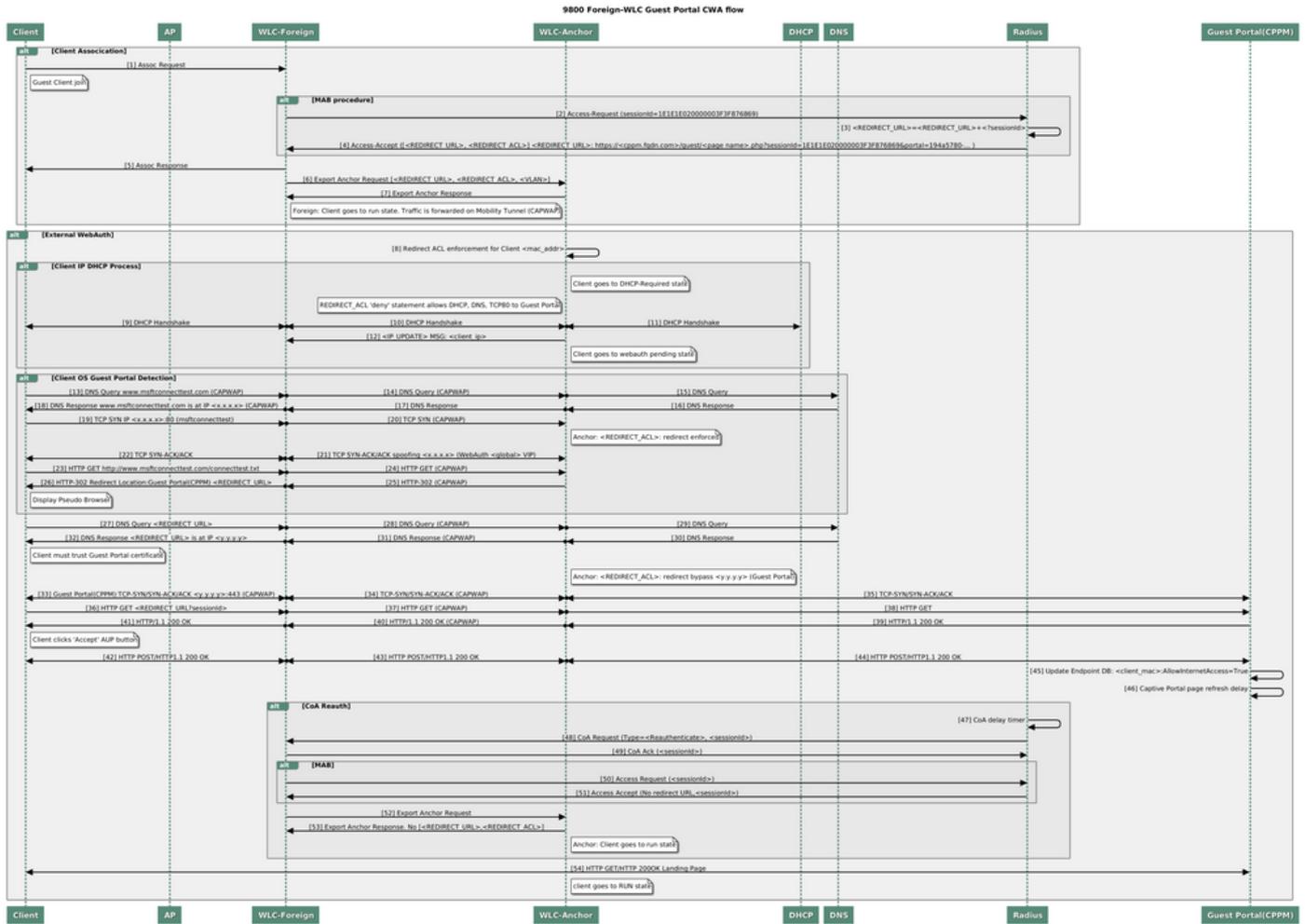
Radius:Cisco:Cisco-AVPair	url-redirect-acl=CAPTIVE_PORTAL_REDIRECT
Radius:Cisco:Cisco-AVPair	url-redirect=https://cppm.example.com/guest/iaccept.php?cmd-login&mac=d4-3b-04-7a-64-7b&switchip=10.85.54.99

◀ ◀ Showing 8 of 1-8 records ▶ ▶ [Change Status](#) [Show Configuration](#) [Export](#) [Show Logs](#) [Close](#)

부록

참고로, 여기서는 RADIUS 서버 및 외부에서 호스팅되는 게스트 포털과의 Cisco 9800 Foreign,

Anchor 컨트롤러 상호 작용에 대한 상태 흐름 다이어그램을 보여줍니다.



앵커 WLC를 사용하는 게스트 중앙 웹 인증 상태 다이어그램

관련 정보

- [Cisco 9800 구축 모범 사례 가이드](#)
- [Catalyst 9800 Wireless Controller 컨피그레이션 모델 이해](#)
- [Catalyst 9800 Wireless Controller의 FlexConnect 이해](#)
- [기술 지원 및 문서 - Cisco Systems](#)

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.