

# Aruba ClearPass와 9800 WLC 통합 구성 - Dot1x & 브랜치 구축을 위한 FlexConnect

## 목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[트래픽 흐름](#)

[네트워크 다이어그램](#)

[Catalyst 9800 Wireless Controller 구성](#)

[C9800 - dot1x에 대한 AAA 매개변수 구성](#)

[C9800 - 'Corp' WLAN 프로파일 구성](#)

[C9800 - 정책 프로필 구성](#)

[C9800 - 정책 태그 구성](#)

[C9800 - AP 가입 프로필](#)

[C9800 - Flex 프로필](#)

[C9800 - 사이트 태그](#)

[C9800 - RF 태그](#)

[C9800 - AP에 태그 할당](#)

[Aruba CPPM 구성](#)

[Aruba ClearPass Policy Manager 서버 초기 컨피그레이션](#)

[라이선스 적용](#)

[C9800 무선 컨트롤러를 네트워크 디바이스로 추가합니다](#)

[Windows AD를 인증 소스로 사용하도록 CPPM 구성](#)

[CPPM Dot1X 인증 서비스 구성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[관련 정보](#)

## 소개

이 문서에서는 Catalyst 9800 Wireless Controller를 Aruba CPPM(ClearPass Policy Manager) 및 Microsoft AD(Active Directory)와 통합하여 Flexconnect 구축에서 무선 클라이언트에 dot1x 인증을 제공하는 방법을 설명합니다.

## 사전 요구 사항

### 요구 사항

Cisco에서는 이러한 항목에 대해 알고 있으며 이러한 항목이 구성 및 확인되었음을 권장합니다.

- Catalyst 9800 Wireless Controller
- Aruba ClearPass Server(플랫폼 라이선스, 액세스 라이선스, 온보드 라이선스 필요)
- 운영 Windows AD
- 선택적 CA(Certificate Authority)
- 운영 DHCP 서버
- 운영 DNS 서버(인증서 CRL 검증에 필요)
- ESXi
- 모든 관련 구성 요소가 NTP에 동기화되고 올바른 시간을 가지는 것으로 확인됨(인증서 검증에 필요)
- 주제의 지식: C9800 구축 및 새로운 구성 모델 C9800의 FlexConnect 작업 Dot1x 인증

## 사용되는 구성 요소

이 문서의 정보는 다음 하드웨어 및 소프트웨어 버전을 기반으로 합니다.

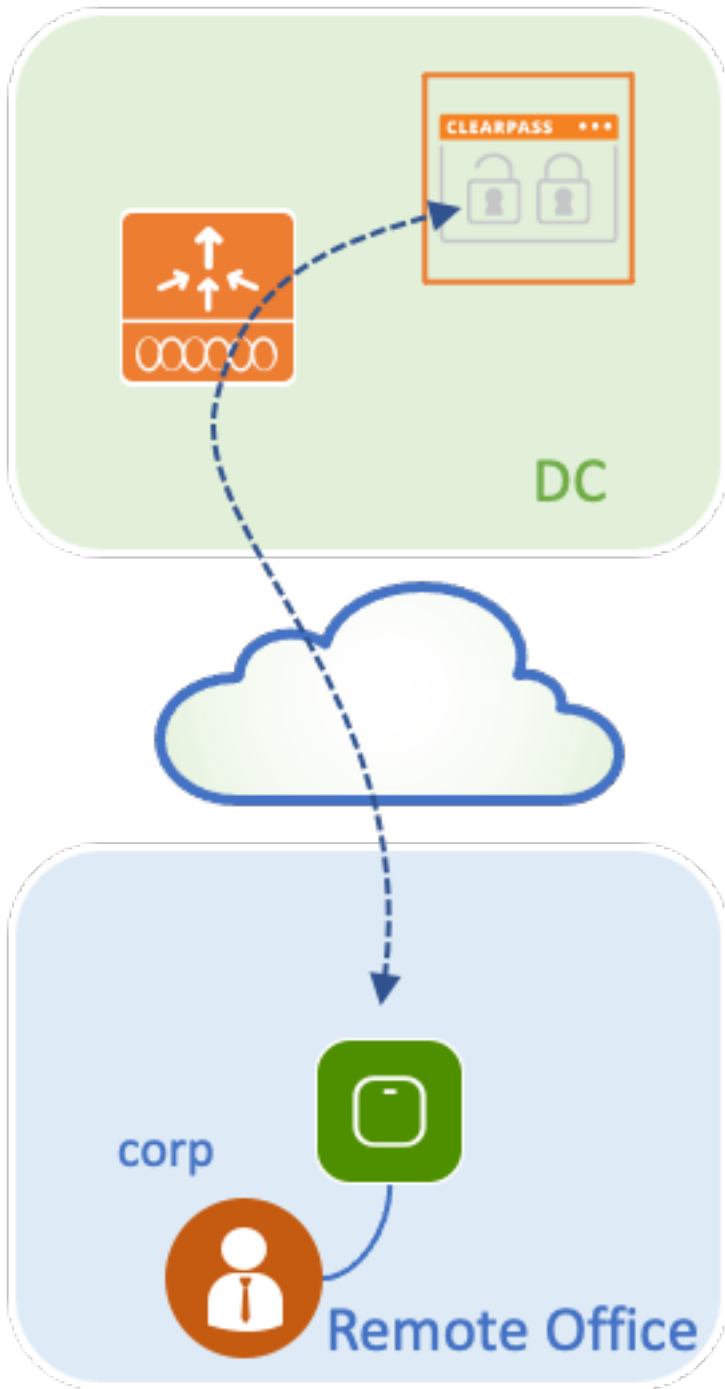
- C9800-L-C Cisco IOS-XE 17.3.3
- C9130AX, 4800 AP
- Aruba ClearPass, 6-8-0-109592 및 6.8-3 패치
- MS Windows 서버 Active Directory(관리되는 엔드포인트에 대한 자동화된 머신 기반 인증서 발급을 위해 구성된 GP)DHCP 서버(옵션 43 및 옵션 60)DNS 서버모든 구성 요소를 시간 동기화 하기 위한 NTP 서버캐나다

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.

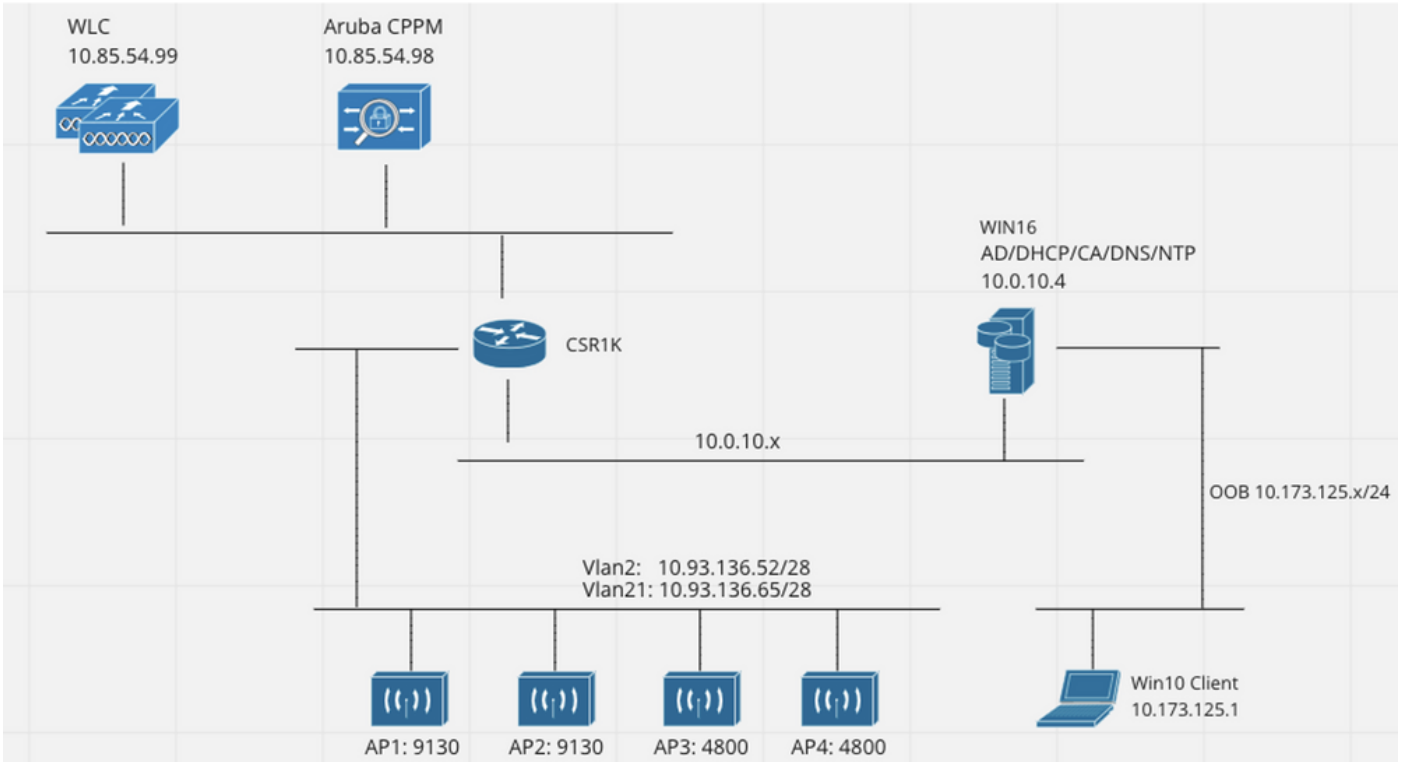
## 배경 정보

### 트래픽 흐름

여러 지사가 있는 일반적인 엔터프라이즈 구축에서는 각 지사가 회사 직원에게 dot1x 액세스를 제공하도록 설정됩니다. 이 컨피그레이션 예에서는 PEAP를 사용하여 중앙 DC(데이터 센터)에 구축된 ClearPass 인스턴스를 통해 기업 사용자에게 dot1x 액세스를 제공합니다. 머신 인증서는 Microsoft AD 서버에 대한 직원 자격 증명 확인과 함께 사용됩니다.




네트워크 다이어그램



## Catalyst 9800 Wireless Controller 구성

이 컨피그레이션 예에서는 C9800의 새로운 컨피그레이션 모델을 활용하여 엔터프라이즈 브랜치에 dot1x Corporate Access 기능을 제공하는 데 필요한 프로필 및 태그를 생성합니다. 결과 컨피그레이션이 다이어그램에 요약되어 있습니다.



AP  
MAC: xxxx.xxxx.xxxx

**Policy Tag: PT\_Branch**

**WLAN Profile: WP\_Corp**  
 SSID: Corp  
 Layer 2: WPA+WPA2  
 WPA: AES, 802.1x  
 AAA: Dot1X\_Authentication

**Policy Profile: PP\_Corp**  
 Central Switching: Disabled  
 Central Auth: Enabled  
 Central DHCP: Disabled  
 Vlan: data (2)

**Site Tag: ST\_Branch\_01**  
 Enable Local Site: Off (to enable FlexConnect)

**AP Join Profile: APJP\_Branch**  
 NTP Server: 10.0.10.4

**Flex Profile: FP\_Branch**  
 Native Vlan 2  
 VLAN: 2 (Corp)

**RF Tag: RFT\_Branch**

**5GHz Band RF: Typical\_Client\_Density\_rf\_5gh**

**2GHz Band RF: Typical\_Client\_Density\_rf\_2gh**

## C9800 - dot1x에 대한 AAA 매개변수 구성

1단계. 9800 WLC 컨피그레이션에 Aruba ClearPass Policy Manager 'Corp' 서버를 추가합니다. Configuration(구성) > Security(보안) > AAA > Servers/Groups(서버/그룹) > RADIUS > Servers(서버)로 이동합니다.+Add(추가)를 클릭하고 RADIUS 서버 정보를 입력합니다. 이 이미지에 표시된 대로 Apply to Device(디바이스에 적용) 버튼을 클릭합니다.

Name*	<input type="text" value="CPPM_Corp"/>
Server Address*	<input type="text" value="10.85.54.97"/>
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

2단계. 회사 사용자를 위한 AAA 서버 그룹을 정의합니다. **Configuration > Security > AAA > Servers/Groups > RADIUS > Groups**로 이동하고 **+Add**를 클릭하고 RADIUS 서버 그룹 이름을 입력하고 RADIUS 서버 정보를 할당합니다. 이 이미지에 표시된 대로 **Apply to Device**(디바이스에 적용) 버튼을 클릭합니다.

Create AAA Radius Server Group
✕

Name*	AAA_Group_Corp
Group Type	RADIUS
MAC-Delimiter	none ▼
MAC-Filtering	none ▼
Dead-Time (mins)	5
Source Interface VLAN ID	none ▼

**Available Servers**

CPPM\_Guest

>  
<  
>>  
<<

**Assigned Servers**

CPPM\_Corp

^  
^  
v  
v

↶ Cancel

📄 Apply to Device

3단계. 기업 사용자를 위한 dot1x 인증 방법 목록을 정의합니다. Configuration(컨피그레이션) > Security(보안) > AAA > AAA Method List(AAA 방법 목록) > Authentication(인증)으로 이동하고 +Add(추가)를 클릭합니다. 드롭다운 메뉴에서 Type dot1x를 선택합니다. 이 이미지에 표시된 대로 [장치에 적용] 단추를 누릅니다.

## Quick Setup: AAA Authentication

Method List Name\*

Dot1X\_Authentication

Type\*

dot1x

Group Type

group

Fallback to local

Available Server Groups

radius  
ldap  
tacacs+  
WLC\_Tacacs\_Servers  
AAA\_Group\_Guest



Assigned Server Groups

AAA\_Group\_Corp



Cancel

Apply to Device

## C9800 - 'Corp' WLAN 프로파일 구성

1단계. Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로필) > Wireless(무선)로 이동하고 +Add(추가)를 클릭합니다. 프로파일 이름, SSID 'Corp' 및 아직 사용 중이 아닌 WLAN ID를 입력합니다.

## Add WLAN

General

Security

Advanced

Profile Name\*

WP\_Corp

Radio Policy

All

SSID\*

Corp

Broadcast SSID

ENABLED

WLAN ID\*

3

Status

ENABLED

Cancel

Apply to Device

2단계. 보안 탭과 Layer2 하위 탭으로 이동합니다. 이 컨피그레이션 예의 기본 매개변수를 변경할 필요가 없습니다.

## Add WLAN

General **Security** Advanced

**Layer2** Layer3 AAA

Layer 2 Security Mode

MAC Filtering

Protected Management Frame

PMF

WPA Parameters

WPA Policy

WPA2 Policy

GTK Randomize

OSEN Policy

WPA2 Encryption  AES(CCMP128)  
 CCMP256  
 GCMP128  
 GCMP256

Auth Key Mgmt  802.1x  
 PSK  
 CCKM  
 FT + 802.1x  
 FT + PSK  
 802.1x-SHA256  
 PSK-SHA256

Lobby Admin Access

Fast Transition

Over the DS

Reassociation Timeout

MPSK Configuration

MPSK

3단계. **AAA** 하위 탭으로 이동하여 이전에 구성한 인증 방법 목록을 선택합니다. 이 이미지에 표시된 대로 **Apply to Device**(디바이스에 적용) 버튼을 클릭합니다.



Add WLAN ✕

General **Security** Advanced

Layer2 Layer3 **AAA**

Authentication List Dot1X\_Authenticatio ▼ i

Local EAP Authentication

↶ Cancel Apply to Device

## C9800 - 정책 프로파일 구성

1단계. Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로파일) > Policy(정책)로 이동하고 +Add(추가)를 클릭한 후 정책 프로파일 이름 및 설명을 입력합니다. 그림과 같이 기업 사용자 트래픽이 AP에서 로컬로 스위칭되므로 정책을 활성화하고 중앙 스위칭, DHCP 및 연결을 비활성화합니다.

⚠ 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_Corp		WLAN Switching Policy	
Description	Policy Profile for Corp		Central Switching	<input type="checkbox"/> DISABLED
Status	ENABLED <input checked="" type="checkbox"/>		Central Authentication	ENABLED <input checked="" type="checkbox"/>
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	2-65519			

2단계. **Access Policies(액세스 정책)** 탭으로 이동하고 지사에서 회사 사용자 트래픽에 사용할 VLAN의 ID를 수동으로 입력합니다. 이 VLAN은 C9800 자체에서 구성할 필요가 없습니다. 자세한 내용은 Flex Profile에서 구성해야 합니다. 드롭다운 목록에서 VLAN 이름을 선택하지 마십시오 (Cisco 버그 ID CSCvn [참조48234](#) 을(를) 참조하십시오. 이 이미지에 표시된 대로 **Apply to Device(디바이스에 적용)** 버튼을 클릭합니다.

⚠ 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	<input type="checkbox"/>			
HTTP TLV Caching	<input type="checkbox"/>			
DHCP TLV Caching	<input type="checkbox"/>			
<b>WLAN Local Profiling</b>				
Global State of Device Classification	<input type="checkbox"/>			
Local Subscriber Policy Name	<input type="text" value="Search or Select"/>			
<b>VLAN</b>				
VLAN/VLAN Group	<input type="text" value="2"/>			
Multicast VLAN	<input type="text" value="Enter Multicast VLAN"/>			
<b>WLAN ACL</b>				
IPv4 ACL	<input type="text" value="Search or Select"/>			
IPv6 ACL	<input type="text" value="Search or Select"/>			
<b>URL Filters</b>				
Pre Auth	<input type="text" value="Search or Select"/>			
Post Auth	<input type="text" value="Search or Select"/>			

## C9800 - 정책 태그 구성

WLAN 프로파일(WP\_Corp) 및 정책 프로파일(PP\_Corp)이 생성되면 이러한 WLAN 및 정책 프로파일을 함께 바인딩하기 위한 정책 태그를 생성해야 합니다. 이 정책 태그는 액세스 포인트에 적용됩니다. 이 정책 태그를 액세스 포인트에 할당하여 이 정책 태그의 컨피그레이션을 트리거하여 선택한 SSID를 활성화합니다.

1단계. Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로파일) > Tags(태그)로 이동하고 Policy(정책) 탭을 선택한 후 +Add(추가)를 클릭합니다. 정책 태그 이름 및 설명을 입력합니다. WLAN-POLICY Maps(WLAN-정책 맵) 아래에서 +Add(추가)를 클릭합니다. 이전에 생성한 WLAN 프로파일 및 정책 프로파일을 선택한 다음 이 이미지에 표시된 것처럼 확인 표시 버튼을 클릭합니다.

### Add Policy Tag ✕

Name\*

Description

▼ WLAN-POLICY Maps: 0

WLAN Profile	Policy Profile
No items to display	

Map WLAN and Policy

WLAN Profile\*

Policy Profile\*

➤ RLAN-POLICY Maps: 0

2단계. 이 이미지에 표시된 대로 **Apply to Device**(디바이스에 적용) 버튼을 확인하고 클릭합니다.

Add Policy Tag
✕

Name\*

Description

▼ WLAN-POLICY Maps: 1

+ Add
✕ Delete

WLAN Profile	Policy Profile
<input checked="" type="checkbox"/> WP_Corp	PP_Corp

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

➤ RLAN-POLICY Maps: 0

↶ Cancel

📄 Apply to Device

## C9800 - AP 가입 프로파일

AP 조인 프로파일 및 Flex 프로파일을 구성하고 사이트 태그가 있는 액세스 포인트에 할당해야 합니다. 브랜치 내에서 802.11r 빠른 전환(FT)을 지원하되 해당 브랜치의 AP 사이에서만 클라이언트 PMK의 배포를 제한하려면 각 브랜치에 대해 다른 사이트 태그를 사용해야 합니다. 여러 브랜치에서 동일한 사이트 태그를 다시 사용하지 않는 것이 중요합니다. AP 가입 프로파일을 구성합니다. 모든 분기가 유사한 경우 단일 AP 조인 프로파일을 사용할 수 있으며, 구성된 매개변수 중 일부가 달라야 하는 경우 여러 프로파일을 생성할 수 있습니다.

1단계. Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로파일) > AP Join(AP 조인)으로 이동하고 +Add(추가)를 클릭합니다. AP Join 프로파일 이름 및 설명을 입력합니다. 이 이미지에 표시된 대로 Apply to Device(디바이스에 적용) 버튼을 클릭합니다.

**Add AP Join Profile** [X]

**General** Client CAPWAP AP Management Security ICap QoS

Name\* APJP\_Branch

Description Profiles for branches

LED State

LAG Mode

NTP Server 0.0.0.0

GAS AP Rate Limit

Apphost

OfficeExtend AP Configuration

Local Access

Link Encryption

Rogue Detection

Cancel Apply to Device

## C9800 - Flex 프로필

이제 Flex 프로필을 구성합니다. 또한 모든 브랜치가 유사하고 동일한 VLAN/SSID 매핑을 갖는 경우 모든 브랜치에 대해 단일 프로파일을 사용할 수 있습니다. 또는, VLAN 할당과 같이 구성된 매개 변수 중 일부가 다른 경우 여러 프로파일을 생성할 수 있습니다.

1단계. Configuration(구성) > Tags & Profiles(태그 및 프로파일) > Flex로 이동하고 +Add(추가)를 클릭합니다. Flex Profile 이름과 설명을 입력합니다.

**Add Flex Profile** [X]

**General** Local Authentication Policy ACL VLAN Umbrella

Name\* FP\_Branch

Description Flex Profile for branches

Native VLAN ID 1

HTTP Proxy Port 0

HTTP-Proxy IP Address 0.0.0.0

CTS Policy

Inline Tagging

SGACL Enforcement

CTS Profile Name default-sxp-profile x

Fallback Radio Shut

Flex Resilient

ARP Caching

Efficient Image Upgrade

OfficeExtend AP

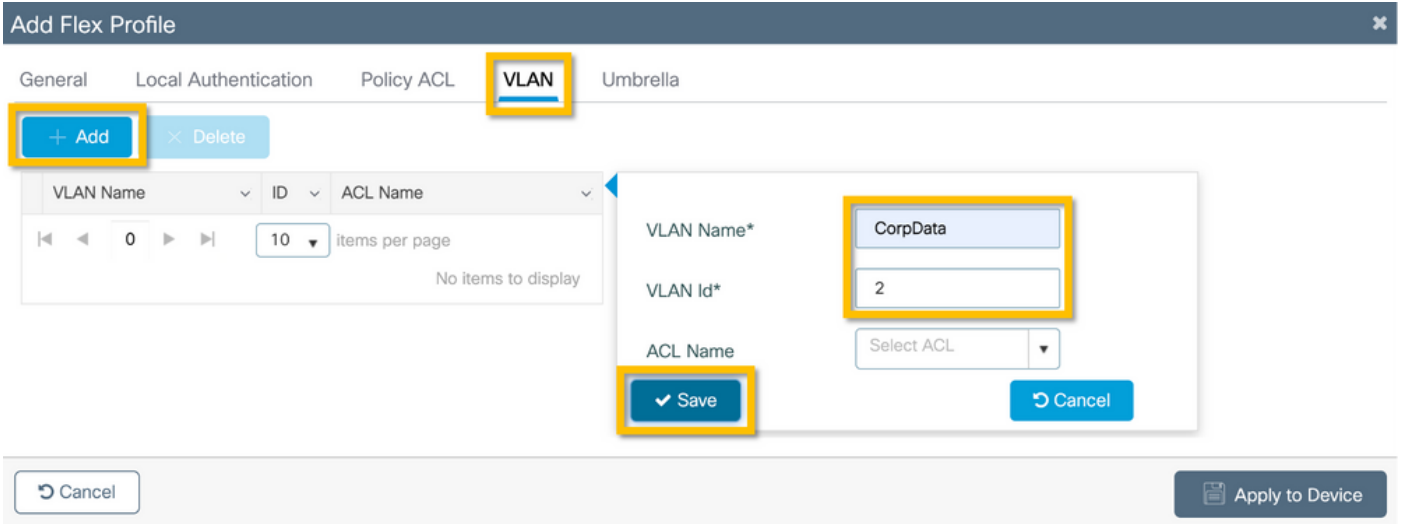
Join Minimum Latency

IP Overlap

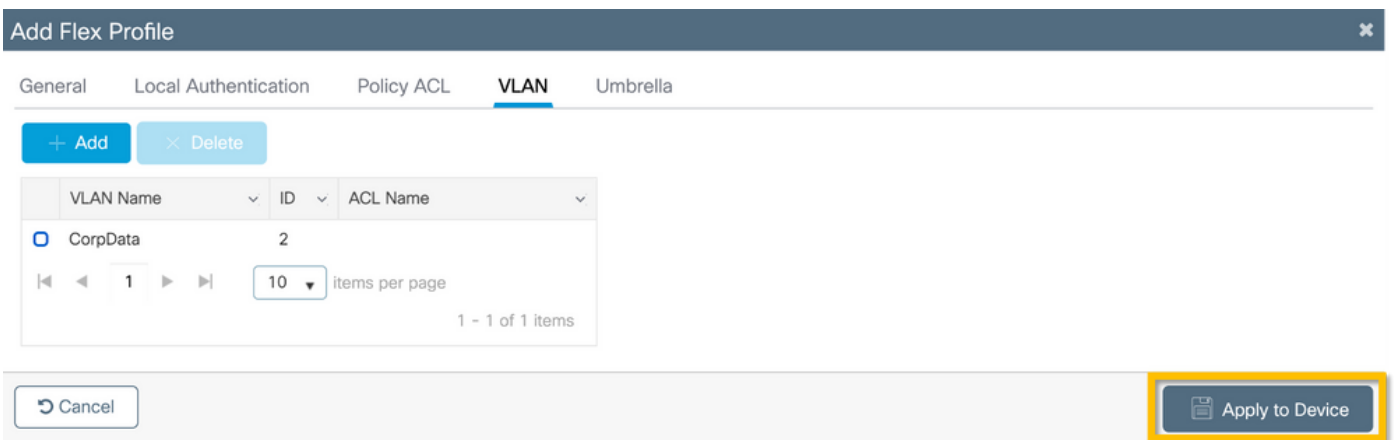
mDNS Flex Profile Search or Select

Cancel Apply to Device

2단계. VLAN 탭으로 이동하고 +Add를 클릭합니다. AP가 기업 사용자 트래픽을 로컬로 전환하는 데 사용해야 하는 브랜치에 로컬 VLAN의 VLAN 이름과 ID를 입력합니다. 이 이미지에 표시된 대로 Save(저장) 버튼을 클릭합니다.



3단계. 이 이미지에 표시된 대로 **Apply to Device**(디바이스에 적용) 버튼을 확인하고 클릭합니다.



## C9800 - 사이트 태그

사이트 태그는 액세스 포인트에 조인 프로파일과 가변 프로파일을 지정하는 데 사용됩니다. 앞에서 설명한 것처럼 브랜치 내에서 802.11r 빠른 전환(FT)을 지원하면서도 해당 브랜치의 AP 사이에서만 클라이언트 PMK의 배포를 제한하려면 각 브랜치에 대해 다른 사이트 태그를 사용해야 합니다. 여러 브랜치 간에 동일한 사이트 태그를 다시 사용하지 않는 것이 중요합니다.

1단계. Configuration(컨피그레이션) > **Tags & Profiles(태그 및 프로파일)** > **Tags(태그)**로 이동하여 **Site(사이트)** 탭을 선택하고 **+Add(추가)**를 클릭합니다. Site Tag(사이트 태그) 이름 및 설명을 입력하고 생성된 AP Join Profile(AP 조인 프로파일)을 선택한 다음 Enable Local **Site(로컬 사이트 활성화)** 상자의 선택을 취소하고 마지막으로 이전에 생성된 Flex Profile(플렉스 프로파일)을 선택합니다. 액세스 포인트를 로컬 모드에서 FlexConnect로 변경하려면 [로컬 사이트 사용] 상자를 선택 취소합니다. 마지막으로, 이 이미지에 표시된 대로 [장치에 적용] 단추를 누릅니다.

**Add Site Tag** ✕

Name\*

Description

AP Join Profile

Flex Profile

Fabric Control Plane Name

Enable Local Site

↶ Cancel 📄 Apply to Device

## C9800 - RF 태그

1단계. Configuration(구성) > Tags & Profiles(태그 및 프로파일) > Tags(태그)로 이동하여 RF 탭을 선택하고 +Add(추가)를 클릭합니다. RF 태그의 이름과 설명을 입력합니다. 드롭다운 메뉴에서 시스템 정의 RF 프로파일을 선택합니다<sup>1</sup>. 이 이미지에 표시된 대로 Apply to Device(디바이스에 적용) 버튼을 클릭합니다.

**Add RF Tag** ✕

Name\*

Description

5 GHz Band RF Profile

2.4 GHz Band RF Profile

↶ Cancel 📄 Apply to Device

## C9800 - AP에 태그 할당

이제 액세스 포인트를 구성하는 데 필요한 다양한 정책 및 프로필을 포함하는 태그가 생성되었으므로 이를 액세스 포인트에 할당해야 합니다. 이 섹션에서는 이더넷 MAC 주소를 기반으로 액세스 포인트에 수동으로 할당된 고정 태그를 수행하는 방법을 보여줍니다. 제품 생산 환경에서는 Cisco DNA Center AP PNP Workflow를 사용하거나 9800에서 사용 가능한 정적 대량 CSV 업로드 방법을 사용하는 것이 좋습니다.

1단계. Configure(구성) > Tags & Profiles(태그 및 프로파일) > Tags(태그)로 이동하고 AP 탭을 선택한 다음 Static(정적) 탭을 선택합니다. +추가를 클릭하고 AP MAC 주소를 입력한 다음 이전에 정의한 정책 태그, 사이트 태그 및 RF 태그를 선택합니다. 이 이미지에 표시된 대로 [장치에 적용] 단추를 누릅니다.



Associate Tags to AP ✕

AP MAC Address*	<input type="text" value="380e.4dbf.589a"/>
Policy Tag Name	<input type="text" value="PT_Branch"/> ▼
Site Tag Name	<input type="text" value="ST_Branch_01"/> ▼
RF Tag Name	<input type="text" value="RFT_Branch"/> ▼

↶ Cancel

📄 Apply to Device

## Aruba CPPM 구성

### Aruba ClearPass Policy Manager 서버 초기 컨피그레이션

Aruba clearpass는 ESXi 서버에서 OVF 템플릿을 통해 다음 리소스와 함께 구축됩니다.

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

### 라이선스 적용

다음을 통해 플랫폼 라이선스를 적용합니다. **관리 > 서버 관리자 > 라이선스**. 액세스 및 온보드 추가

### C9800 무선 컨트롤러를 네트워크 디바이스로 추가합니다

이 이미지에 표시된 대로 **Configuration(컨피그레이션) > Network(네트워크) > Devices(디바이스) > Add(추가)**로 이동합니다.

**Edit Device Details**

Device | SNMP Read Settings | SNMP Write Settings | CLI Settings | OnConnect Enforcement | Attributes

Name: >WLC-10.85.54.99

IP or Subnet Address: 10.85.54.99 (e.g., 192.168.1.10 or 192.168.1.1/24 or 192.168.1.1-20)

Description: LAB WLC 9800

RADIUS Shared Secret: ..... Verify: .....

TACACS+ Shared Secret: ..... Verify: .....

Vendor Name: Cisco

Enable RADIUS Dynamic Authorization:  Port: 1700

Enable RadSec:

Copy Save Cancel

## Windows AD를 인증 소스로 사용하도록 CPPM 구성

Configuration(컨피그레이션) > Authentication(인증) > Sources(소스) > Add(추가)로 이동합니다.  
 유형 선택: 이 이미지에 표시된 것처럼 드롭다운 메뉴의 Active Directory입니다.

**aruba** ClearPass Policy Manager

Configuration » Authentication » Sources » Add

Authentication Sources

General | Primary | Attributes | Summary

Name: LAB\_AD

Description:

Type: Active Directory

Use for Authorization:  Enable to use this Authentication Source to also fetch role mapping attributes

Authorization Sources: -- Select --

Server Timeout: 10 seconds

Cache Timeout: 36000 seconds

Backup Servers Priority: Add Backup Remove

## CPPM 구성 Dot1X 인증 서비스

1단계. 여러 RADIUS 특성에서 일치하는 '서비스'를 생성합니다.

- 반경:IETF | 이름: NAS IP 주소 | 같음 | <IP 주소>
- 반경:IETF | 이름: 서비스 유형 | 같음 | 1,2,8

2단계. 프로덕션의 경우 다중 WLC 구축에서 하나의 조건으로 충분하도록 'NAS-IP-Address' 대신

SSID 이름을 확인하는 것이 좋습니다. Radius:Cisco:Cisco-AVPair | cisco-wlan-ssid | Dot1XSSID

ClearPass Policy Manager

Configuration » Services » Edit - G \_DOT1X

Services - DOT1X

Summary Service Authentication Roles Enforcement

Name: DOT1X

Description: 802.1X Wireless Access Service

Type: 802.1X Wireless

Status: Enabled

Monitor Mode:  Enable to monitor network access without enforcement

More Options:  Authorization  Posture Compliance  Audit End-hosts  Profile Endpoints  Accounting Proxy

Service Rule

Matches  ANY or  ALL of the following conditions:

Type	Name	Operator	Value
1.	Radius:IETF	NAS-IP-Address	EQUALS 10.85.54.99
2.	Radius:IETF	Service-Type	BELONGS_TO Login-User (1), Framed-User (2), Authenticate-Only (8)
3.	Click to add...		

ClearPass Policy Manager

Configuration » Services » Edit - G \_DOT1X

Services - DOT1X

Summary Service Authentication Roles Enforcement

Authentication Methods:

- EAP PEAP]
- EAP FAST]
- EAP TLS]
- EAP TTLS]

--Select to Add--

Authentication Sources:

- LAB AD (Active Directory)

--Select to Add--

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

Service Certificate: --Select to Add--

다음을 확인합니다.

현재 이 설정에 사용 가능한 확인 절차는 없습니다.

## 문제 해결

현재 이 설정에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

## 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.