Flex 7500 Wireless Branch Controller 구축 설명서

목차

소개

이 문서에서는 Cisco Flex 7500 무선 브랜치 컨트롤러를 구축하는 방법에 대해 설명합니다.이 문서의 목적은 다음과 같습니다.

- Cisco FlexConnect 솔루션의 다양한 네트워크 요소와 커뮤니케이션 흐름에 대해 설명합니다.
- Cisco FlexConnect 무선 브랜치 솔루션을 설계하기 위한 일반적인 구축 지침을 제공합니다.
- 제품에 대한 정보 베이스를 보강하는 7.2.103.0 코드 릴리스의 소프트웨어 기능에 대해 설명합니다.

참고: 7.2 이전 버전에서는 FlexConnect를 HREAP(Hybrid REAP)이라고 했습니다. 이제 FlexConnect라고 합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

제품 개요

그림 1:Cisco Flex 7500

Cisco Flex 7500 Series Cloud Controller는 멀티 사이트 무선 구축을 위한 확장성이 뛰어난 지사 컨트롤러입니다.프라이빗 클라우드에 구축된 Cisco Flex 7500 Series Controller는 중앙 집중식 제어를 통해 무선 서비스를 분산된 지사로 확장하여 총 운영 비용을 절감합니다.

Cisco Flex 7500 Series(그림 1)는 최대 500개 지점에서 무선 액세스 포인트를 관리할 수 있으며 IT

관리자는 데이터 센터에서 최대 3,000개의 AP(액세스 포인트) 및 30,000개의 클라이언트를 구성, 관리 및 해결할 수 있습니다.Cisco Flex 7500 Series 컨트롤러는 안전한 게스트 액세스, PCI(Payment Card Industry) 규정 준수를 위한 비인가 감지, 지사 내(로컬 스위치) Wi-Fi 음성 및 비디오를 지원합니다.

이 표에서는 Flex 7500, WiSM2 및 WLC 5500 컨트롤러 간의 확장성 차이를 보여 줍니다.

확장성	Flex 7500	WiSM2	WLC 5500
총 액세스 포인트	6,000	1000	500
총 클라이언트 수	64,000	15,000	7,000
최대 FlexConnect 그룹	2000	100	100
FlexConnect 그룹당 최대 AP 수	100	25	25
최대 AP 그룹	6000	1000	500

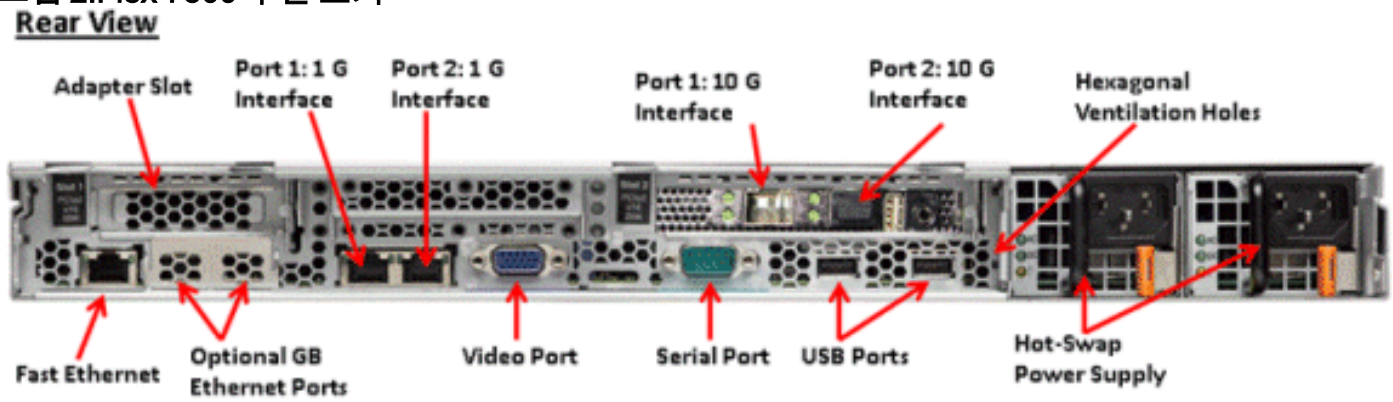
제품 사양

데이터 시트

http://www.cisco.com/en/US/prod/collateral/wireless/ps6302/ps8322/ps11635/data_sheet_c78-650053.html을 참조하십시오.

플랫폼 기능

그림 2:Flex 7500 후면 보기



네트워크 인터페이스 포트

인터페이스 포트	사용
고속 이더넷	IMM(Integrated Management Module)
포트 1:1G	WLC 서비스 포트
포트 2:1G	WLC RP(Redundant Port)
포트 1:10G	WLC 관리 인터페이스
포트 2:10G	WLC 백업 관리 인터페이스 포트(포트 오류)

옵션 Gb 이더넷 포트	해당 없음

참고:

- 2x10G 인터페이스에 대한 LAG를 지원하므로 신속한 장애 조치 링크 이중화를 통해 액티브-액티브 링크 작업이 가능합니다.LAG가 있는 추가 활성 10G 링크는 컨트롤러 무선 처리량을 변경하지 않습니다.
- 2x10G 인터페이스
- 2x10G 인터페이스는 SFP 제품 # SFP-10G-SR을 사용하는 옵틱 케이블만 지원합니다.
- 스위치 측 SFP 제품 # X2-10GB-SR

시스템 MAC 주소

포트 1:10G(관리 인터페이스)	시스템/기본 MAC 주소
포트 2:10G(백업 관리 인터페이스)	기본 MAC 주소 + 5
포트 1:1G(서비스 포트)	기본 MAC 주소 + 1
포트 2:1G(이중화 포트)	기본 MAC 주소 + 3

직렬 콘솔 리디렉션

WLC 7500은 기본적으로 전송 속도 9600에서 콘솔 리디렉션을 활성화하여 흐름 제어 없이 Vt100 터미널을 시뮬레이션합니다.

인벤토리 정보

그림 3:WLC 7500 콘솔

```
(Cisco Controller) >show inventory

Burned-in MAC Address.............................. E4:1F:13:65:DB:6C
Maximum number of APs supported.................... 2000
NAME: "Chassis"    , DESCR: "Cisco Wireless Controller"
PID: AIR-CT7510-K9,  VID: V01,  SN: KQZZXWL
```

DMI(Desktop Management Interface) 테이블에는 서버 하드웨어 및 BIOS 정보가 포함됩니다.

WLC 7500은 인벤토리의 일부로 BIOS 버전, PID/VID 및 일련 번호를 표시합니다.

Flex 7500 부팅

소프트웨어 유지 관리를 위한 Cisco 부트 로더 옵션은 Cisco의 기존 컨트롤러 플랫폼과 동일합니다
.

그림 4:부팅 순서

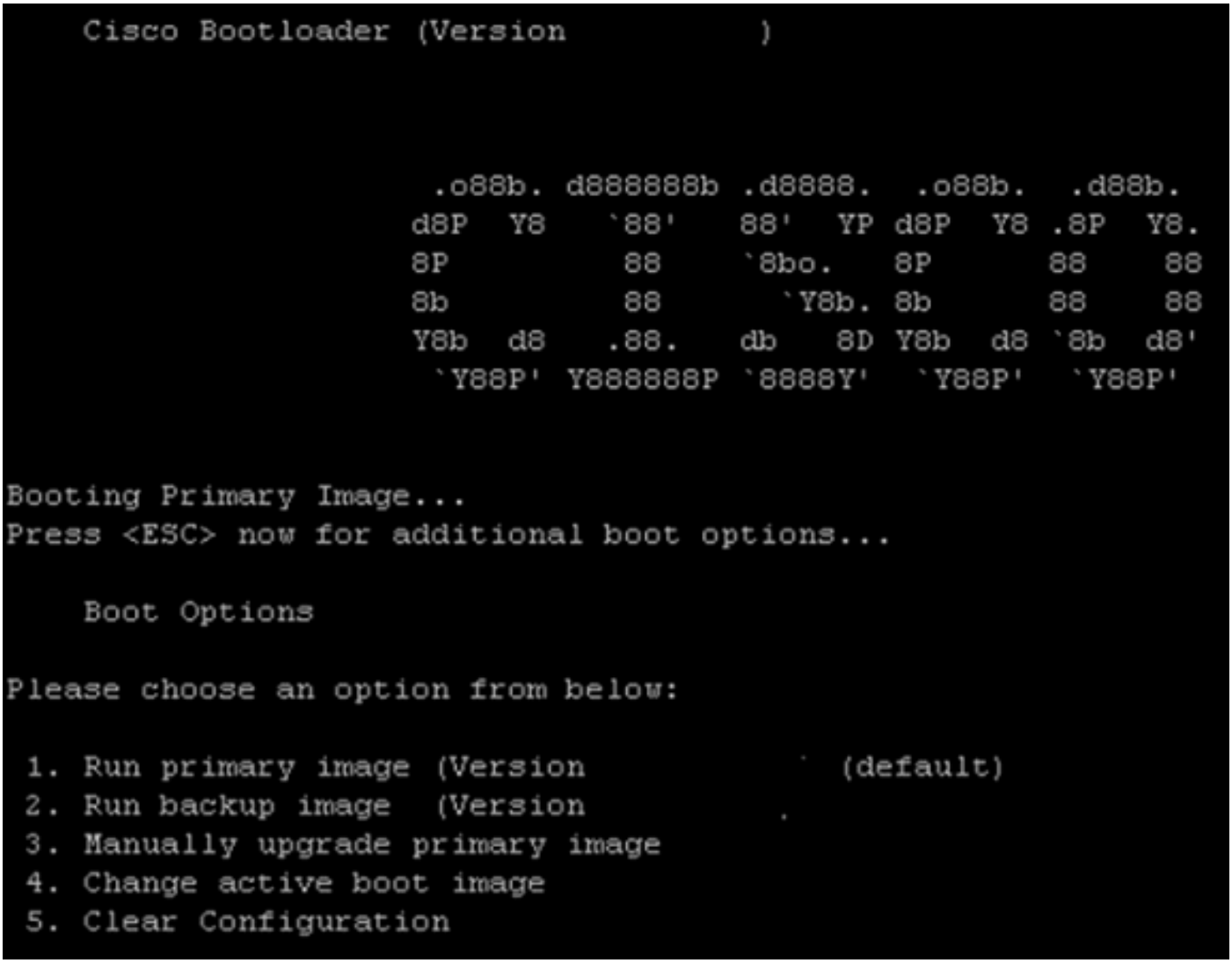


그림 5:WLC 구성 마법사

```
Would you like to terminate autoinstall? [yes]:

System Name [Cisco_65:db:6c] (31 characters max):
AUTO-INSTALL: process terminated -- no configuration loaded

Enter Administrative User Name (24 characters max): admin
Default values (admin or Cisco or its variants) in password is not allowed.
Enter Administrative Password (24 characters max): *******
Re-enter Administrative Password                  : *******

Management Interface IP Address: 172.20.227.174
Management Interface Netmask: 255.255.255.224
Management Interface Default Router: 172.20.227.161
Management Interface VLAN Identifier (0 = untagged):
Management Interface Port Num [1 to 2]: 1
Management Interface DHCP Server IP Address: 172.20.227.161

Virtual Gateway IP Address: 1.1.1.1

Mobility/RF Group Name: mobility

Network Name (SSID): DataCenter

Configure DHCP Bridging Mode [yes][NO]: NO

Allow Static IP Addresses [YES][no]: Yes

Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.

Enter Country Code list (enter 'help' for a list of countries) [US]:

Enable 802.11b Network [YES][no]: yes
Enable 802.11a Network [YES][no]: yes
Enable 802.11g Network [YES][no]: yes
Enable Auto-RF [YES][no]: yes

Configure a NTP server now? [YES][no]: no
Configure the system time now? [YES][no]: yes
Enter the date in MM/DD/YY format: 09/02/10
Enter the time in HH:MM:SS format: 11:50:00

Configuration correct? If yes, system will save it and reset. [yes][NO]: yes
```

Management Port 1: 10G

참고: Flex 7500 부팅 시퀀스는 동일하며 기존 컨트롤러 플랫폼과 일치합니다.초기 부팅에는 마법사를 사용하여 WLC 컨피그레이션이 필요합니다.

Flex 7500 라이센싱

AP 기본 개수 라이센싱

AP 기본 수 SKU
300

500
1000
2000
3000
6000

AP 업그레이드 라이센싱

AP 업그레이드 SKU
100
250
500
1000

기본 및 업그레이드 수를 제외하고 주문, 설치 및 보기를 다루는 전체 라이센스 절차는 Cisco의 기존 WLC 5508과 유사합니다.

전체 라이센싱 절차를 다루는 WLC 7.3 컨피그레이션 가이드를 참조하십시오.

소프트웨어 릴리스 지원

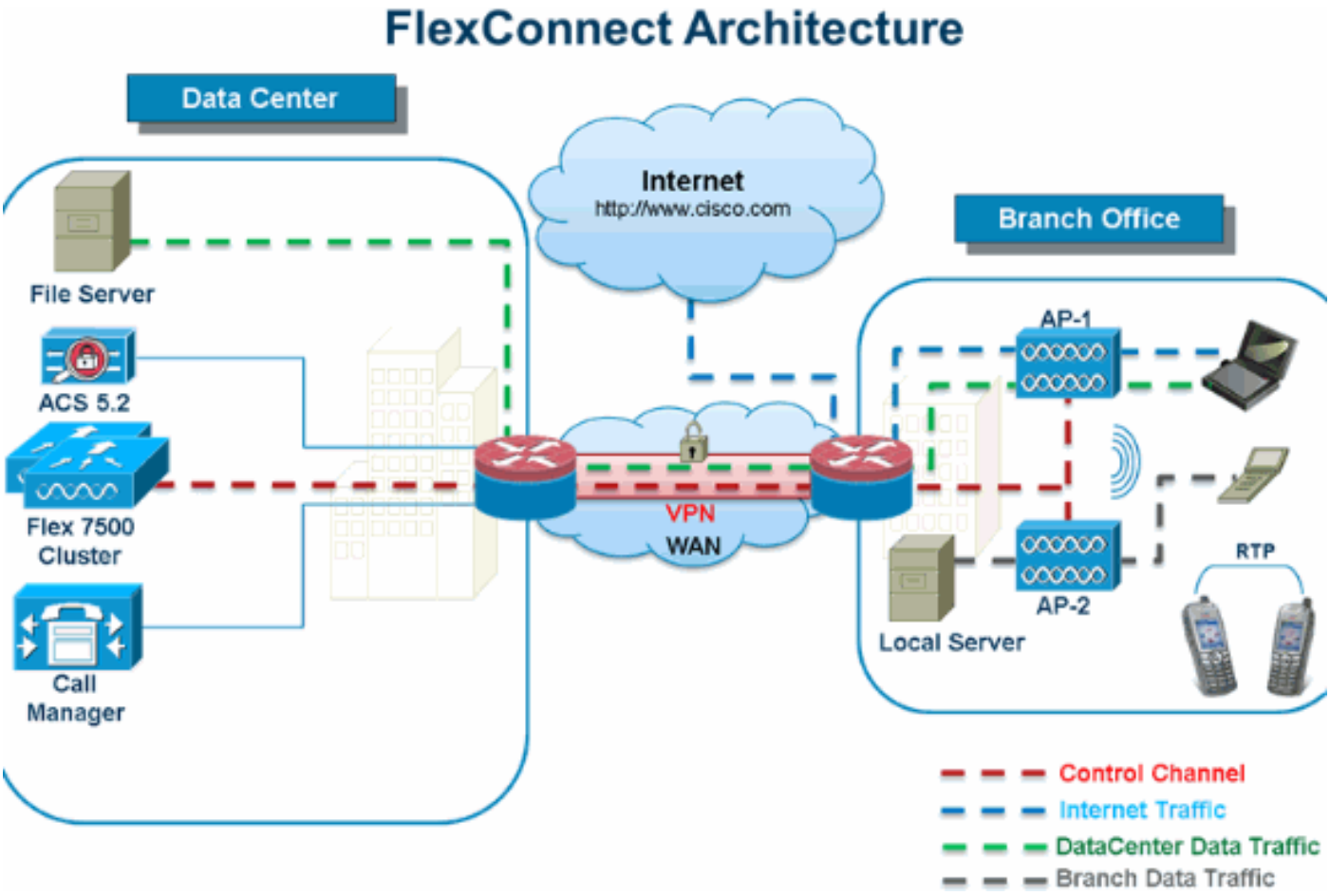
Flex 7500은 WLC 코드 버전 7.0.116.x 이상만 지원합니다.

지원되는 액세스 포인트

액세스 포인트 1040, 1130, 1140, 1550, 3500, 3600, 2600, 1250, 1260, 1240, OEAP 600, ISR 891 및 ISR 8881은 Flex500050에서 지원됩니다.

FlexConnect 아키텍처

그림 6:일반적인 무선 브랜치 토폴로지



FlexConnect는 지사 및 원격 사무실 구축을 위한 무선 솔루션입니다.이를 하이브리드 REAP 솔루션이라고도 하지만 이 문서에서는 이를 FlexConnect라고 합니다.

FlexConnect 솔루션을 통해 고객은 다음과 같은 이점을 누릴 수 있습니다.

- 데이터 센터에서 AP의 제어 및 관리 트래픽을 중앙 집중화합니다.제어 트래픽은 그림 6에서 빨간색 대시로 표시됩니다.
- 각 지사에서 클라이언트 데이터 트래픽을 배포합니다.데이터 트래픽은 그림 6에서 파란색, 녹색 및 자주색 대시로 표시됩니다.각 트래픽 흐름은 가장 효율적인 방식으로 최종 목적지로 이동합니다.

액세스 포인트 제어 트래픽 중앙 집중화의 장점

- 모니터링 및 문제 해결 단일 창
- 관리 용이성
- 데이터 센터 리소스에 대한 안전하고 원활한 모바일 액세스
- 브랜치 공간 감소
- 운영 비용 절감 증가

클라이언트 데이터 트래픽 배포의 장점

- 완전한 WAN 링크 장애 또는 컨트롤러 비가용성에 대한 운영 다운타임(존속성) 없음
- WAN 링크 장애 시 지사 내 모빌리티 복원력
- 브랜치 확장성 향상최대 100개의 AP와 250,000제곱피트(5000제곱피트까지 확장 가능한 브랜치 크기를 지원합니다.AP당 피트)

Cisco FlexConnect Solution은 또한 중앙 클라이언트 데이터 트래픽을 지원하지만 게스트 데이터 트래픽만 제한해야 합니다.다음 표에서는 데이터 트래픽이 데이터 센터에서 중앙 집중식으로 전환되는 비 게스트 클라이언트에 대해서만 WLAN L2 보안 유형의 제한에 대해 설명합니다.

중앙에서 스위칭된 비 게스트 사용자를 위한 L2 보안 지원

WLAN L2 보안	유형	결과
없음	해당 없음	허용
WPA + WPA2	802.1x	허용
	CCKM	허용
	802.1x + CCKM	허용
	PSK	허용
802.1x	WEP	허용
고정 WEP	WEP	허용
WEP + 802.1x	WEP	허용
CKIP		허용

참고: 이러한 인증 제한은 데이터 트래픽이 브랜치에 배포된 클라이언트에는 적용되지 않습니다.

중앙 및 로컬로 스위칭된 사용자를 위한 L3 보안 지원

WLAN L3 보안	유형	결과
웹 인증	내부	허용
	외부	허용
	맞춤형	허용
웹 통과	내부	허용
	외부	허용
	맞춤형	허용
조건부 웹 리디렉션	외부	허용
스플래시 페이지 웹 리디렉션	외부	허용

Flexconnect 외부 웹 인증 배포에 대한 자세한 내용은 Flexconnect 외부 웹 인증 구축 설명서를 참조하십시오.

HREAP/FlexConnect AP 상태 및 데이터 트래픽 스위칭 옵션에 대한 자세한 내용은 FlexConnect 구성을 참조하십시오.

FlexConnect 작동 모드

FlexConnect 모드	설명
연결됨	FlexConnect는 CAPWAP 컨트롤 플레인을 컨트롤러에 다시 연결하여 작동할 때 연결 모드에 있다고 하는데, 이는 WAN 링크가 다운되지 않았음을 의미합니다.
독립형	독립형 모드는 FlexConnect가 컨트롤러에 더 이상 연결할 수 없을 때 시작되는 작동 상태로 지정됩니

	다.독립형 모드의 FlexConnect AP는 전원 장애 및 WLC 또는 WAN 장애 시에도 마지막으로 알려진 컨피그레이션으로 계속 작동합니다.

FlexConnect 운영 이론에 대한 자세한 내용은 H-Reap / FlexConnect 설계 및 구축 가이드를 참조하십시오.

WAN 요구 사항

FlexConnect AP는 브랜치 사이트에 구축되며 WAN 링크를 통해 데이터 센터에서 관리됩니다.데이터 구축의 경우 왕복 지연 시간이 300ms보다 크지 않고 데이터 + 음성 구축의 경우 100ms로 AP당 최소 대역폭 제한이 12.8kbps로 유지되는 것이 좋습니다.MTU(최대 전송 단위)는 500바이트 이상이어야 합니다.

배포 유형	WAN 대역폭(최소)	WAN RTT 레이턴시(최대)	지사당 최대 AP 수	지사당 최대 클라이언트 수
데이터	64kbps	300밀리초	5	25
데이터 + 음성	128kbps	100밀리초	5	25
모니터	64kbps	2초	5	해당 없음
데이터	640kbps	300밀리초	50	1000
데이터 + 음성	1.44Mbps	100밀리초	50	1000
모니터	640kbps	2초	50	해당 없음

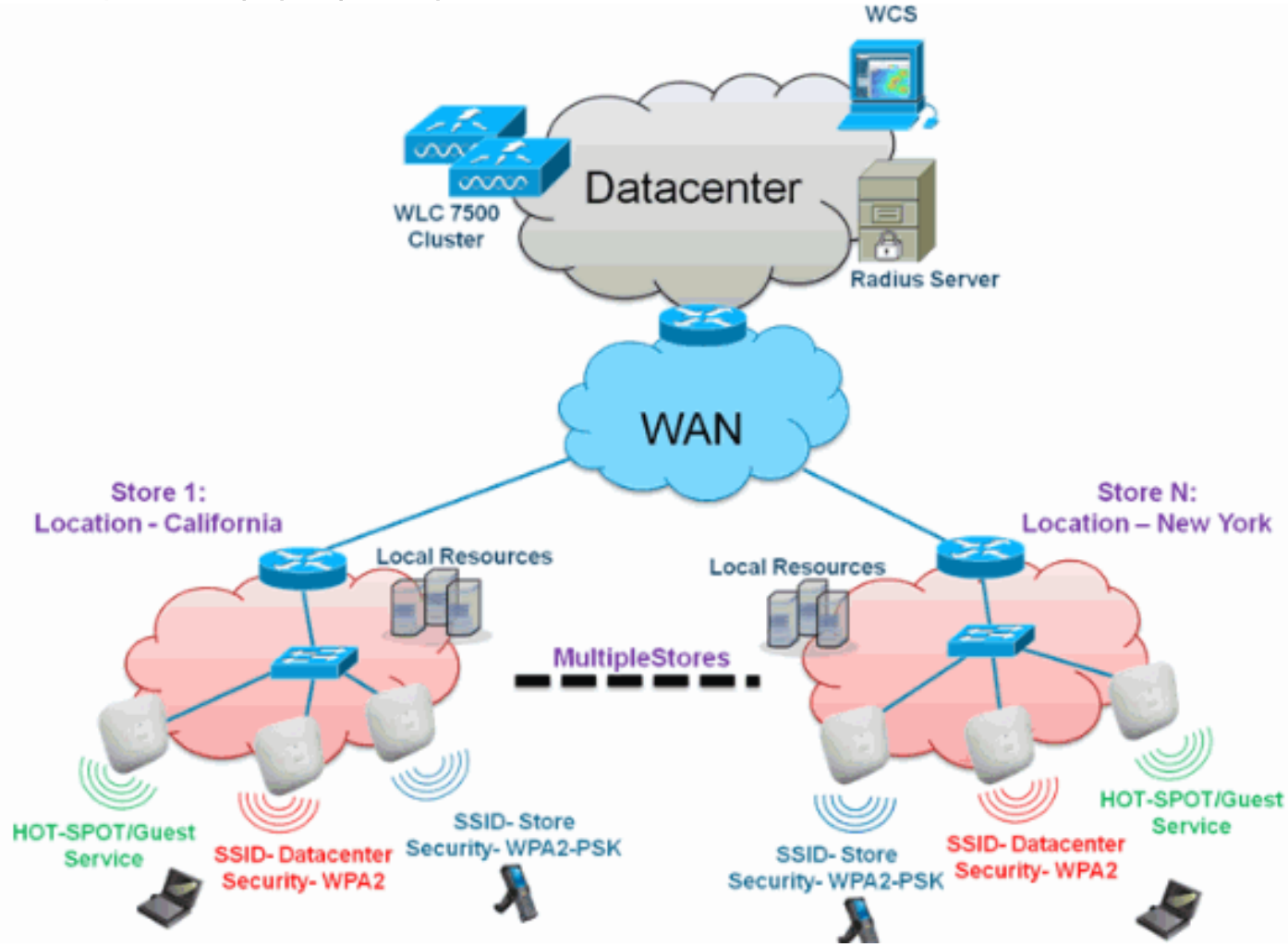
무선 브랜치 네트워크 설계

이 문서의 나머지 부분에서는 지침을 중점적으로 설명하고 보안 분산 브랜치 네트워크를 구현하는 모범 사례를 설명합니다.FlexConnect 아키텍처는 이러한 설계 요구 사항을 충족하는 무선 브랜치 네트워크에 권장됩니다.

기본 설계 요구 사항

- 최대 100개의 AP와 250,000제곱피트(5000제곱피트까지 확장 가능한 브랜치 크기.AP당 피트)
- 중앙 관리 및 문제 해결
- 운영 다운타임 없음
- 클라이언트 기반 트래픽 세그멘테이션
- 기업 리소스에 원활하고 안전한 무선 연결
- PCI 규정 준수
- 게스트 지원

그림 7:무선 브랜치 네트워크 설계



개요

지사 고객은 지리적 위치에 걸쳐 확장 가능하고 안전한 모든 기능을 갖춘 네트워크 서비스를 제공하는 것이 점점 더 어렵고 비용이 많이 든다는 것을 알게 됩니다.고객을 지원하기 위해 Cisco는 Flex 7500을 도입하여 이러한 과제를 해결하고 있습니다.

Flex 7500 솔루션은 데이터 센터 내에서 복잡한 보안, 관리, 구성 및 문제 해결 작업을 가상화한 다음 각 브랜치로 투명하게 확장합니다.Flex 7500을 사용하는 구축은 IT가 더욱 쉽게 설정, 관리 및 확장할 수 있습니다.

장점

- 6000 AP 지원으로 확장성 향상
- FlexConnect 내결함성을 사용하여 복원력 향상
- FlexConnect를 사용하여 트래픽 분할 증가(중앙 및 로컬 스위칭)
- AP 그룹 및 FlexConnect 그룹을 사용하여 매장 설계를 복제하여 관리 용이성

브랜치 네트워크 설계를 지원하는 기능

설명서의 나머지 섹션에서는 그림 7에 나와 있는 네트워크 설계를 실현하기 위한 기능 사용 및 권장 사항을 다룹니다.

기능:

주요 기능	주요 내용
AP 그룹	여러 브랜치 사이트를 처리할 때 운영/관리 용이성을 제공합니다.또한 유사한 지사 사이트에 대한 구성을 유연하게 복제할 수 있습니다.
FlexConnect 그룹	FlexConnect 그룹은 로컬 백업 Radius, CCKM/OKC 빠른 로밍 및 로컬 인증의 기능을 제공합니다.
내결함성	무선 브랜치 복원력을 개선하고 운영 다운타임을 제공하지 않습니다.
ELM(적응형 wIPS를 위한 향상된 로컬 모드)	클라이언트 성능에 영향을 주지 않고 클라이언트를 서비스할 때 적응형 wIPS 기능을 제공합니다.
WLAN당 클라이언트 제한	브랜치 네트워크의 총 게스트 클라이언트 제한
AP 사전 이미지 다운로드	브랜치 업그레이드 시 다운타임을 줄입니다.
FlexConnect에서 AP 자동 변환	FlexConnect의 AP를 브랜치에 자동으로 변환하는 기능입니다.
게스트 액세스	FlexConnect를 사용하여 기존 Cisco 게스트 액세스 아키텍처를 계속하십시오.

IPv6 지원 매트릭스

기능	중앙 스위치		로컬 스위치드	
	5500 / WiSM-2	Flex 7500	5500 / WiSM-2	Flex 7500
IPv6(클라이언트 모빌리티)	지원됨	지원되지 않음	지원되지 않음	지원되지 않음
IPv6 RA 가드	지원됨	지원됨	지원됨	지원됨
IPv6 DHCP 가드	지원됨	지원되지 않음	지원되지 않음	지원되지 않음
IPv6 소스 가드	지원됨	지원되지 않음	지원되지 않음	지원되지 않음
RA 제한/속도 제한	지원됨	지원되지 않음	지원되지 않음	지원되지 않음
IPv6 ACL	지원됨	지원되지 않음	지원되지 않음	지원되지 않음
IPv6 클라이언트 가시성	지원됨	지원되지 않음	지원되지 않음	지원되지 않음
IPv6 인접 디바이스 검색 캐싱	지원됨	지원되지 않음	지원되지 않음	지원되지 않음

IPv6 브리징	지원됨	지원되지 않음	지원됨	지원됨

기능 매트릭스

FlexConnect 기능에 대한 기능 매트릭스는 FlexConnect 기능 매트릭스를 참조하십시오.

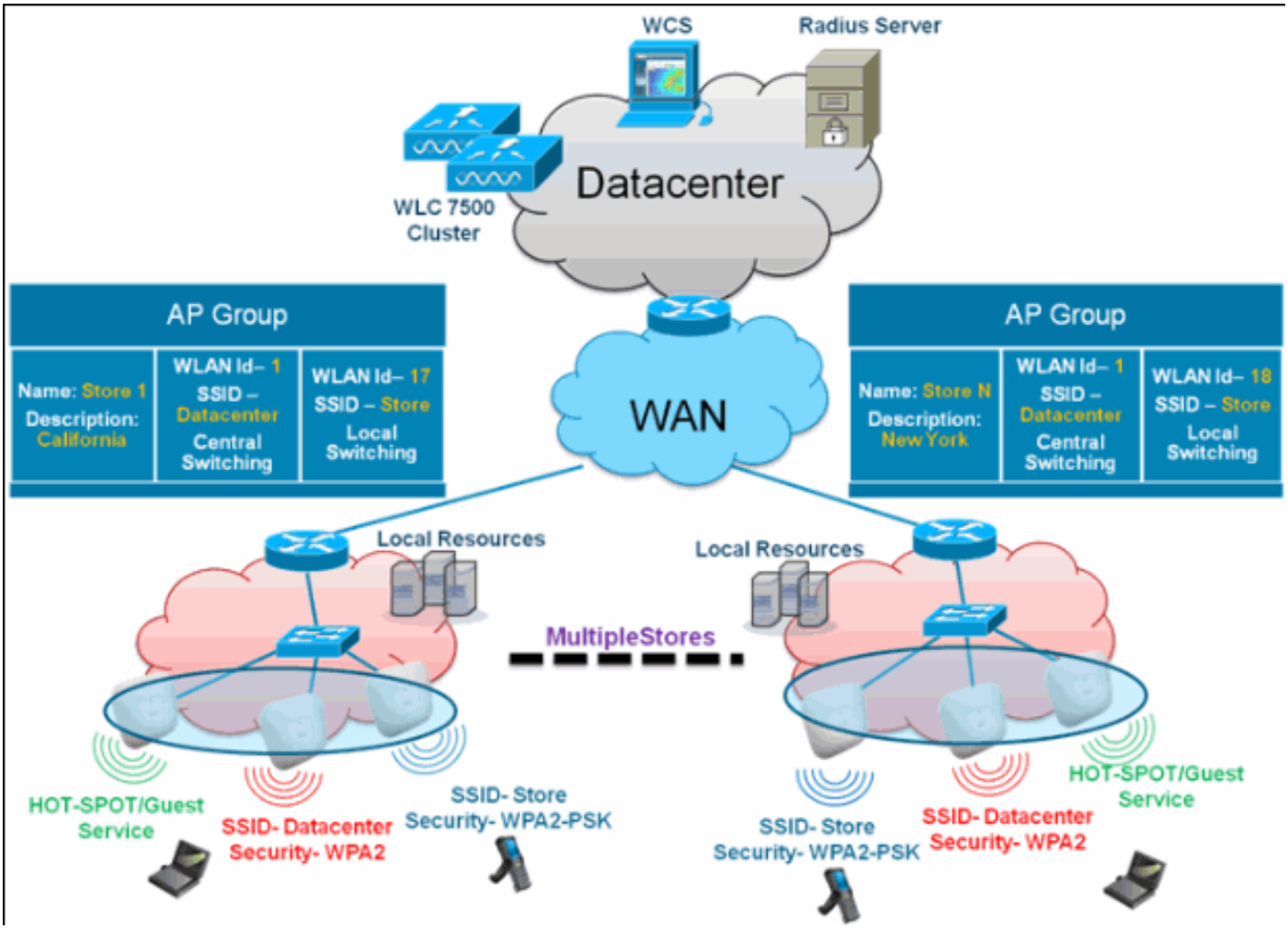
AP 그룹

컨트롤러에서 WLAN을 생성한 후 무선 네트워크를 보다 효율적으로 관리하기 위해 액세스 포인트 그룹을 사용하여 여러 액세스 포인트에 선택적으로 게시할 수 있습니다.일반적인 구축에서는 WLAN의 모든 사용자가 컨트롤러의 단일 인터페이스에 매핑됩니다.따라서 해당 WLAN에 연결된 모든 사용자는 동일한 서브넷 또는 VLAN에 있습니다.그러나 액세스 포인트 그룹을 생성하여 여러 인터페이스 간에 로드를 분산하거나 개별 부서(예: 마케팅, 엔지니어링 또는 운영)와 같은 특정 기준에 따라 사용자 그룹에 로드를 분산하도록 선택할 수 있습니다.또한 이러한 액세스 포인트 그룹은 별도의 VLAN에서 구성하여 네트워크 관리를 간소화할 수 있습니다.

이 문서에서는 AP 그룹을 사용하여 여러 지리적 위치를 관리할 때 네트워크 관리를 간소화합니다.이 문서는 운영 편의성을 위해 다음 요구 사항을 충족하기 위해 저장소당 하나의 AP 그룹을 만듭니다.

- 로컬 저장소 관리자 관리 **액세스를** 위해 모든 저장소에서 중앙 스위치드 SSID 데이터 센터
- 핸드헬드 **스캐너의** 모든 매장에서 다른 WPA2-PSK 키를 사용하는 로컬 스위치드 SSID 저장소.

그림 8:AP 그룹을 사용하는 무선 네트워크 설계 참조

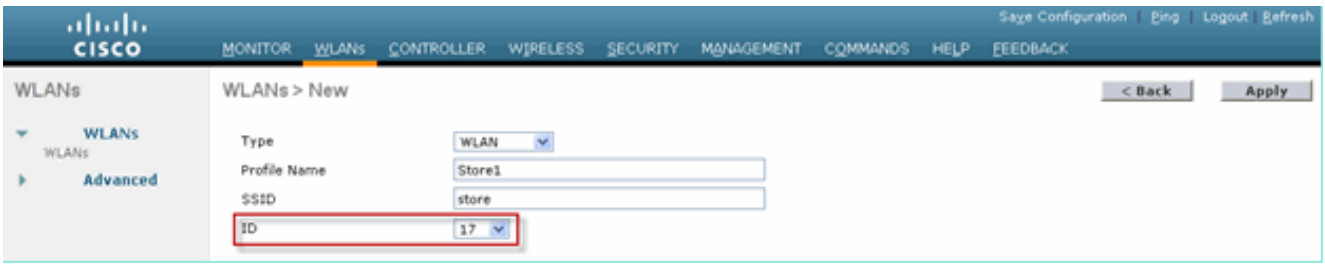


WLC의 구성

다음 단계를 완료하십시오.

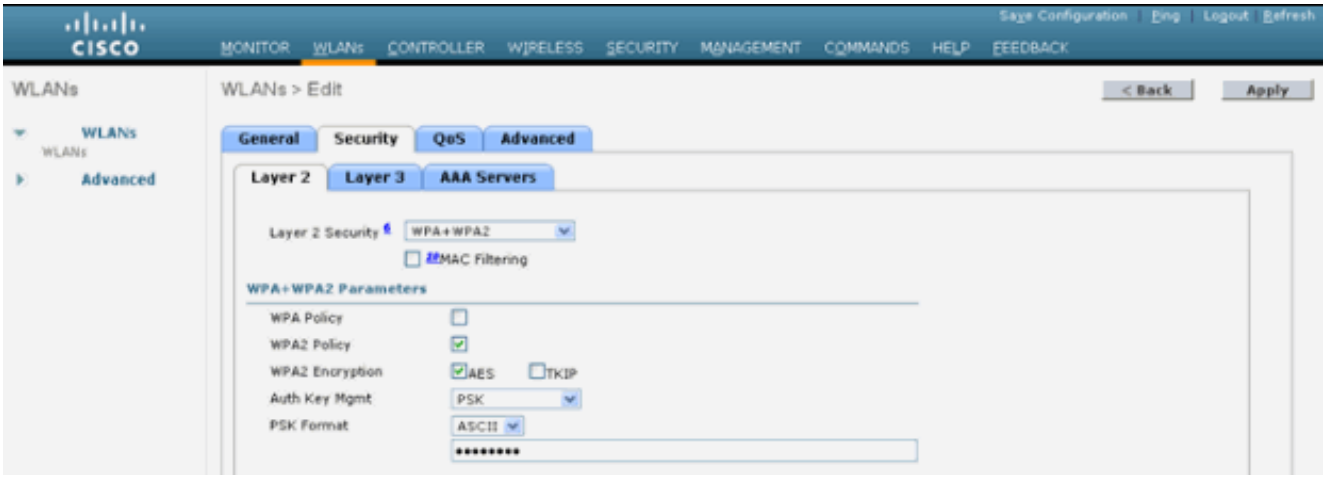
1. WLANs(WLANs) > New(새) 페이지의 Profile Name(프로파일 이름) 필드에 **Store1**을 입력하고 SSID 필드에 **store(저장)를** 입력하고 ID 드롭다운 목록에서 **17**을 선택합니다.**참고:** WLAN ID 1-16은 기본 그룹의 일부이므로 삭제할 수 없습니다.다른 WPA2-PSK를 사용하여 저장소당 동일한 SSID 저장소를 사용하는 요건을 충족하려면 WLAN ID 17 이상을 사용해야 합니다. WLAN ID는 기본 그룹의 일부가 아니며 각 스토어로 제한될 수 있기 때문입니다

.



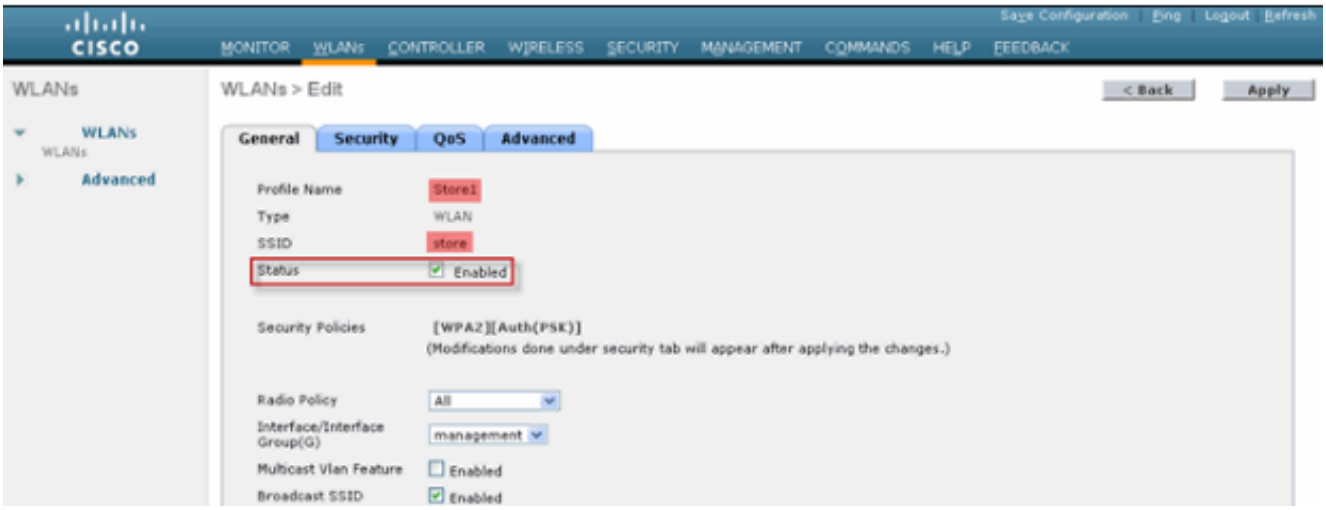
2. WLAN > Security의 Auth **Key Mgmt** 드롭다운 목록에서 PSK를 선택하고 PSK Format(PSK 형식) 드롭다운 목록에서 **ASCII**를 선택한 다음 Apply(적용)를 **클릭합니다**

.

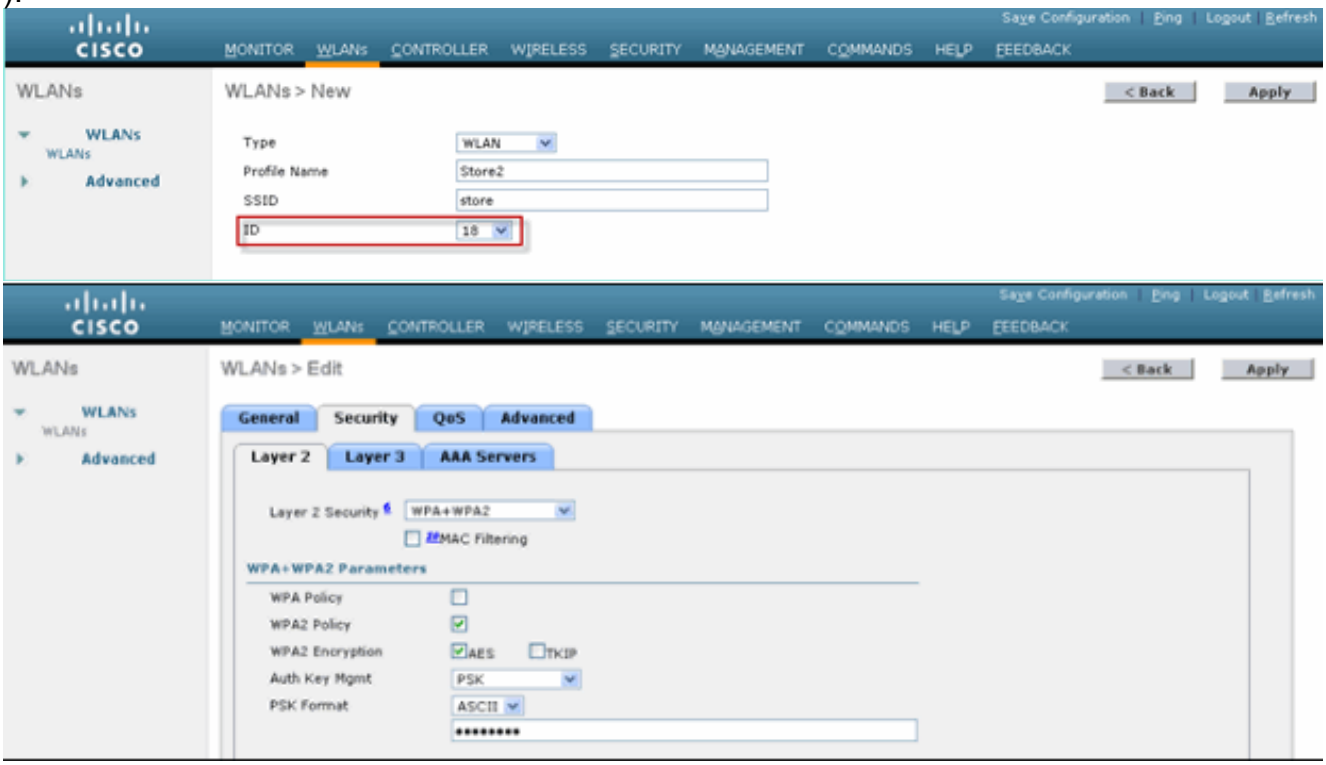


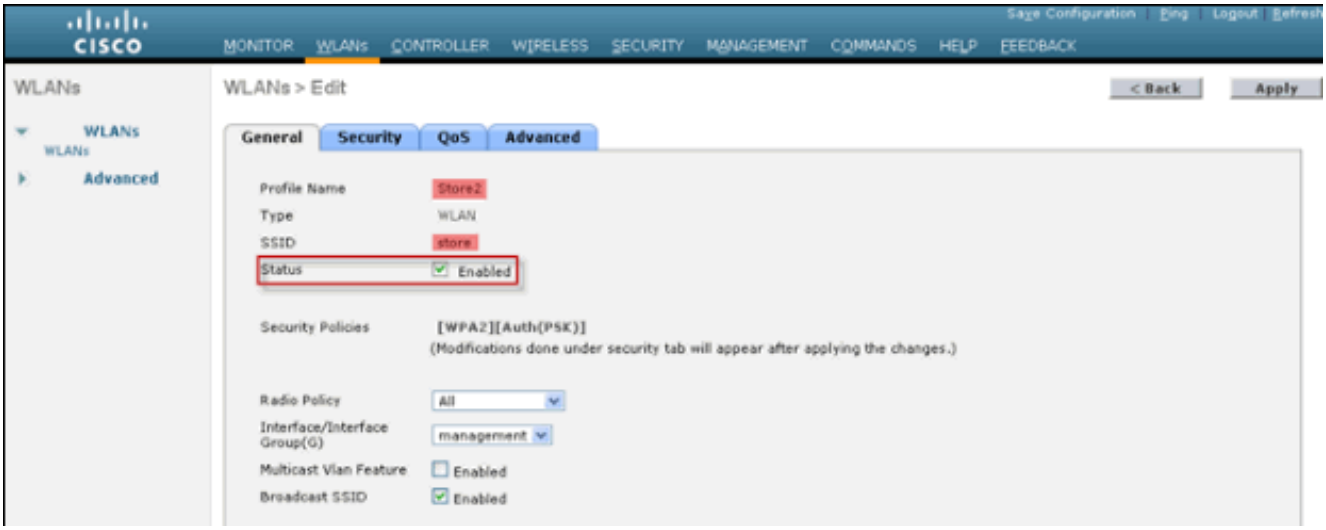
3. WLAN **> General(일반)**을 클릭하고 Security Policies(보안 정책) 변경을 확인한 다음 Status(**상태**) 확인란을 선택하여 WLAN을 활성화합니다

.



4. 새 WLAN 프로파일 **Store2**에 대해 1, 2, 3단계를 반복합니다(SSID **저장소** 및 ID 18 포함).



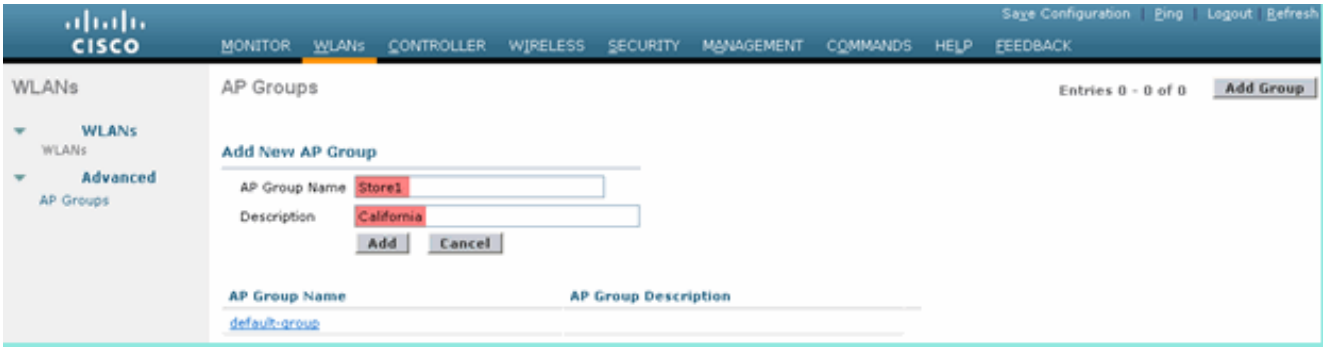


5. 프로파일 이름 DataCenter, SSID **DataCenter** 및 ID 1을 사용하여 WLAN 프로파일을 생성하고 활성화합니다.**참고:** 생성 시 1~16의 WLAN ID는 자동으로 기본-ap-group에 포함됩니다.
6. WLAN에서 WLAN ID 1, 17 및 18의 상태를 확인합니다

.

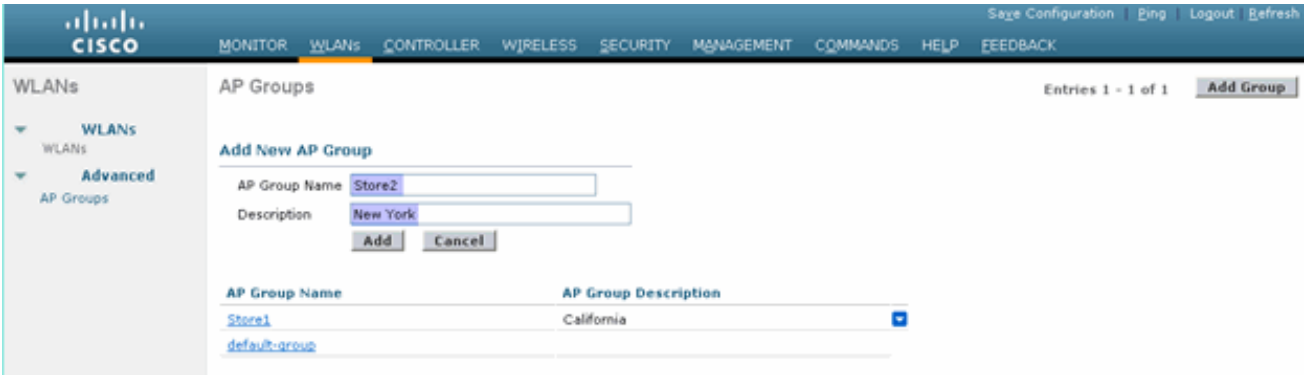
7. WLAN **> Advanced > AP group > Add Group을 클릭합니다**.
8. AP 그룹 이름 **Store1**(WLAN 프로필 **Store1**과 동일) 및 설명(Description)을 스토어 위치로 추가합니다.이 예에서는 California가 매장 위치로 사용됩니다.
9. 완료되면 **Add**(추가)를 클릭합니다

.



10. Add **Group(그룹 추가)**을 클릭하고 AP Group Name **Store2**(AP 그룹 이름 **스토어2)** 및 Description(설명) New York을 생성합니다.
11. Add(**추가)를 클릭합니다**

.

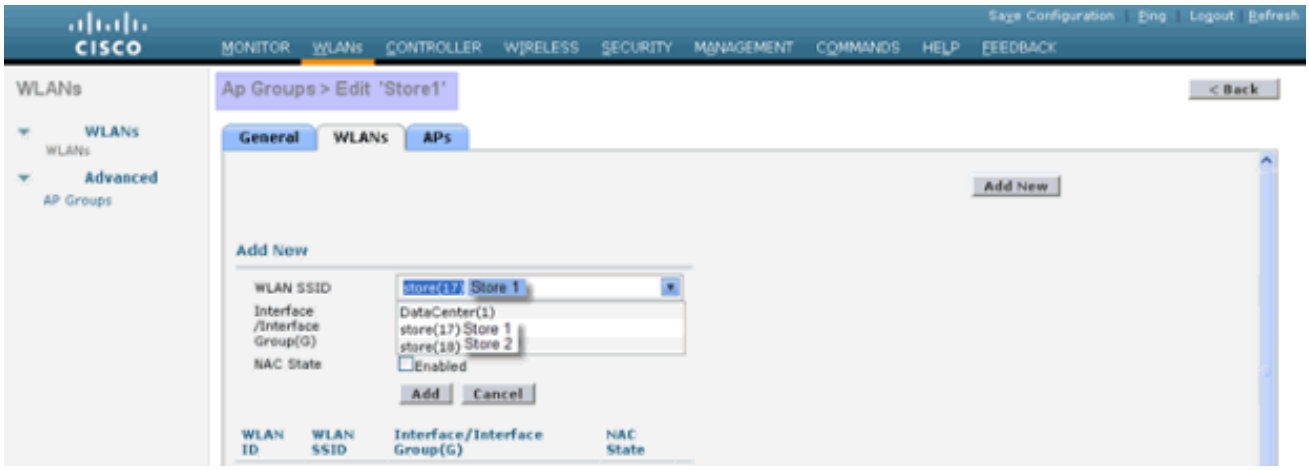


12. **WLAN > Advanced > AP Groups**를 클릭하여 그룹 생성**을 확인합니다**

.

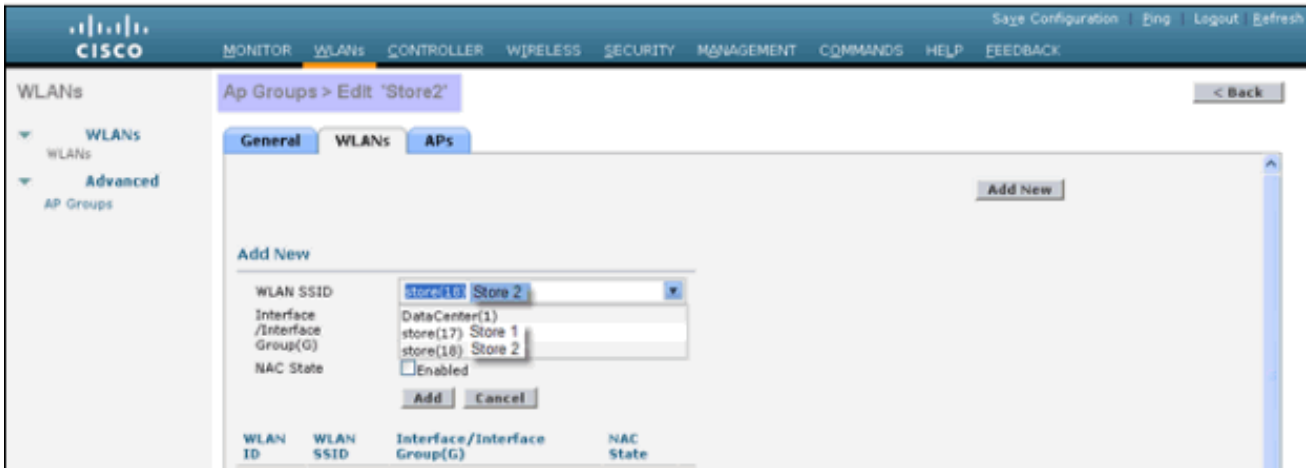
13. AP Group Name **Store1**을 클릭하여 WLAN을 추가하거나 편집합니다.
14. Add **New(새로 추가)**를 클릭하여 WLAN을 선택합니다.
15. WLAN 아래의 WLAN SSID 드롭다운에서 **WLAN ID 17 store(17)를** 선택합니다.
16. WLAN **ID** 17을 선택한 후 Add를 클릭합니다.
17. WLAN ID 1 DataCenter(1)에 대해 14-16단계를 반복합니다. 이 단계는 선택 사항이며 원격 리소스 액세스를 허용하려는 경우에만 필요합니다

.

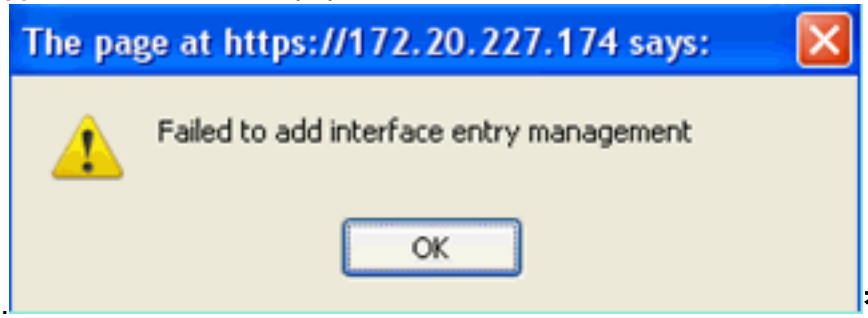


18. **WLAN > Advanced > AP Groups** 화면으로 돌아갑니다.
19. WLAN을 추가하거나 편집하려면 AP Group Name **Store2**를 클릭합니다.
20. Add **New(새로 추가)**를 클릭하여 WLAN을 선택합니다.
21. WLAN 아래의 WLAN SSID 드롭다운에서 **WLAN ID 18 store(18)를** 선택합니다.
22. WLAN **ID** 18을 선택한 후 Add를 클릭합니다.
23. WLAN ID 1 DataCenter(1)에 대해 14-16단계를 반복합니다

.



참고: 단일 AP 그룹에서 동일한 SSID를 가진 여러 WLAN 프로파일을 추가할 수 없습니다



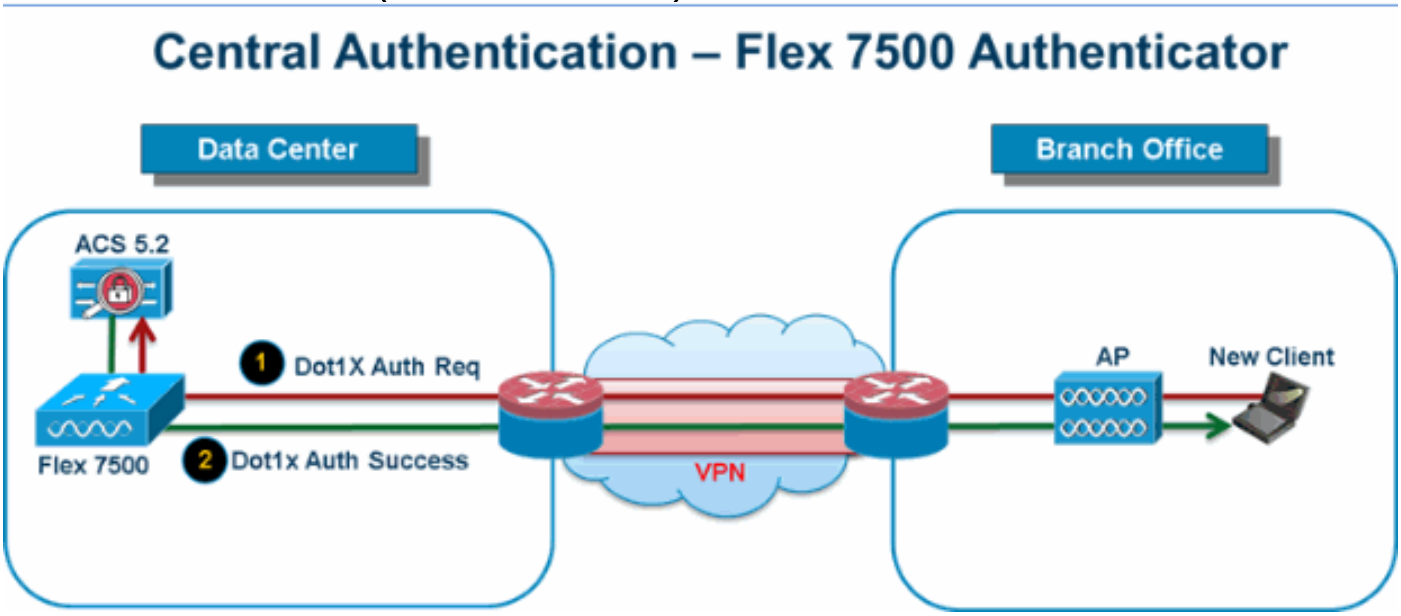
참고: AP 그룹에 AP를 추가하는 것은 이 문서에서 캡처되지 않지만 클라이언트가 네트워크 서비스에 액세스하는 데 필요합니다.

요약

- AP 그룹은 네트워크 관리를 간소화합니다.
- 지점 단위 세분화를 통한 문제 해결 용이성
- 유연성 향상

FlexConnect 그룹

그림 9:Central Dot1X 인증(Flex 7500 인증 역할)



대부분의 일반적인 브랜치 구축에서는 그림 9에 나와 있는 것처럼 클라이언트 802.1X 인증이 데이

터 센터에서 중앙 집중식으로 이루어진다고 쉽게 예측할 수 있습니다. 위의 시나리오는 완벽하게 유효하기 때문에 다음과 같은 문제가 발생합니다.

- Flex 7500이 실패할 경우 무선 클라이언트가 802.1X 인증을 수행하고 데이터 센터 서비스에 액세스하려면 어떻게 해야 합니까?
- 지사와 데이터 센터 간의 WAN 링크가 실패할 경우 무선 클라이언트가 802.1X 인증을 어떻게 수행할 수 있습니까?
- WAN 장애 시 브랜치 모빌리티에 어떤 영향이 있습니까?
- FlexConnect 솔루션은 운영 브랜치 다운타임을 제공하지 않습니까?

FlexConnect 그룹은 주로 설계되었으며 이러한 과제를 해결하기 위해 개발되어야 합니다.또한 각 브랜치 사이트의 모든 FlexConnect 액세스 포인트가 단일 FlexConnect 그룹에 포함되므로 각 브랜치 사이트를 쉽게 구성할 수 있습니다.

참고: FlexConnect 그룹은 AP 그룹과 유사하지 않습니다.

FlexConnect 그룹의 기본 목표

백업 RADIUS 서버 장애 조치

- 독립형 모드의 FlexConnect 액세스 포인트가 백업 RADIUS 서버에 대한 전체 802.1X 인증을 수행하도록 컨트롤러를 구성할 수 있습니다.브랜치 복원력을 높이기 위해 관리자는 기본 백업 RADIUS 서버 또는 기본 및 보조 백업 RADIUS 서버를 모두 구성할 수 있습니다.이러한 서버는 FlexConnect 액세스 포인트가 컨트롤러에 연결되지 않은 경우에만 사용됩니다.

참고: 백업 RADIUS 계정 관리는 지원되지 않습니다.

로컬 인증

- 7.0.98.0 코드 릴리스 이전에는 FlexConnect가 독립형 모드에 있을 때만 로컬 인증이 지원되어 WAN 링크 장애 시 클라이언트 연결이 영향을 받지 않도록 했습니다.7.0.116.0 릴리스에서는 FlexConnect 액세스 포인트가 연결 모드인 경우에도 이 기능이 지원됩니다.**그림 10:Central Dot1X 인증(FlexConnect AP가 인증자로 작동)**

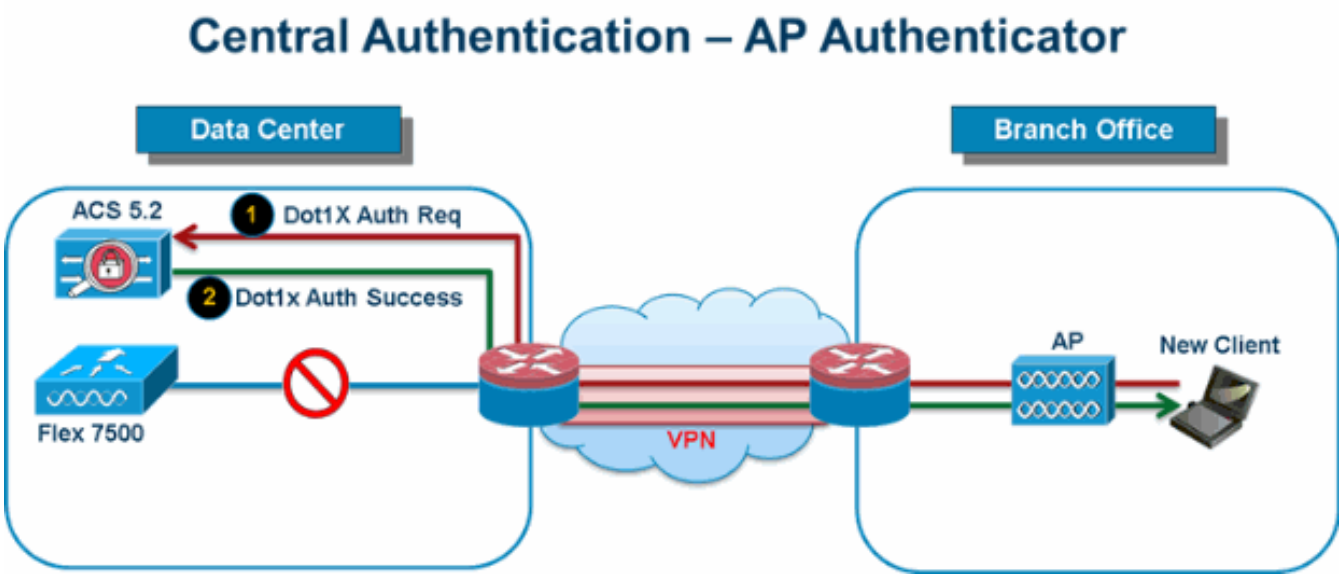
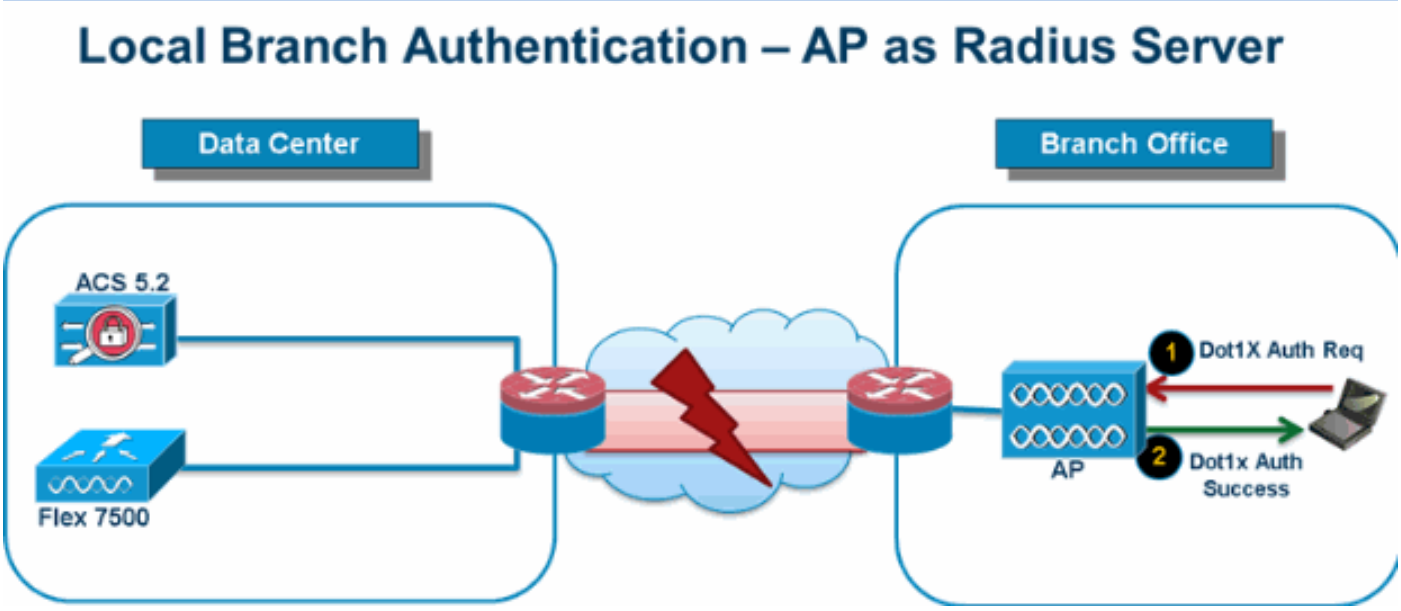


그림 10에 나와 있는 것처럼 FlexConnect 브랜치 AP가 Flex 7500과 연결되지 않을 경우 브랜치 클라이언트는 802.1X 인증을 계속 수행할 수 있습니다.브랜치 사이트에서 RADIUS/ACS 서버에 연결할 수 있는 한 무선 클라이언트는 계속 인증하고 무선 서비스에 액세스합니다.즉, RADIUS/ACS가 브랜치 내에 있으면 클라이언트는 WAN 중단 중에도 무선 서비스를 인증하고

액세스합니다.**참고:** 이 기능은 FlexConnect 백업 RADIUS 서버 기능과 함께 사용할 수 있습니다.FlexConnect 그룹이 백업 RADIUS 서버 및 로컬 인증으로 구성된 경우, FlexConnect 액세스 포인트는 항상 기본 백업 RADIUS 서버를 사용하여 클라이언트를 인증한 다음 보조 백업 RADIUS 서버(기본 서버에 연결할 수 없는 경우), 마지막으로 FlexConnect 액세스 포인트 자체의 로컬 EAP 서버(기본 및 보조 서버에 연결할 수 없는 경우)를 시도합니다.

로컬 EAP(로컬 인증 계속)

그림 11:Dot1X 인증(로컬 EAP 서버로 작동하는 FlexConnect AP)



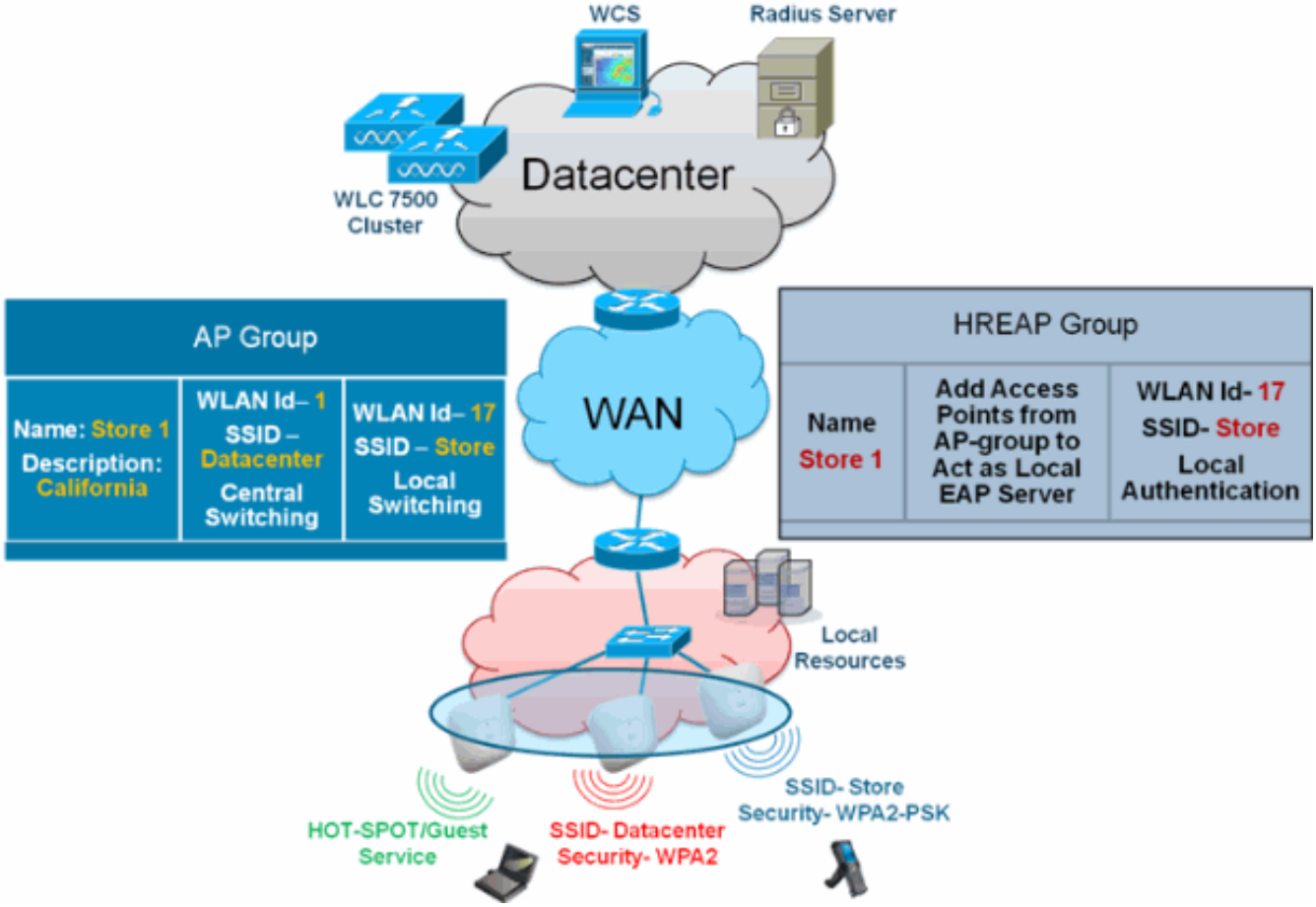
- 독립형 또는 연결 모드에서 FlexConnect AP가 정적으로 구성된 최대 100명의 사용자에 대해 LEAP 또는 EAP-FAST 인증을 수행하도록 컨트롤러를 구성할 수 있습니다.컨트롤러는 컨트롤러에 조인할 때 해당 특정 FlexConnect 그룹의 각 FlexConnect 액세스 포인트에 사용자 이름 및 비밀번호의 정적 목록을 보냅니다.그룹의 각 액세스 포인트는 고유한 연결된 클라이언트만 인증합니다.
- 이 기능은 자동 액세스 포인트 네트워크에서 경량 FlexConnect 액세스 포인트 네트워크로 마이그레이션하고 대규모 사용자 데이터베이스를 유지 관리하는 데 관심이 없거나 자동 액세스 포인트에서 사용 가능한 RADIUS 서버 기능을 대체할 다른 하드웨어 장치를 추가하는 고객에게 적합합니다.
- 그림 11에 표시된 것처럼 데이터 센터 내의 RADIUS/ACS 서버에 연결할 수 없는 경우 FlexConnect AP는 자동으로 로컬 EAP 서버 역할을 하여 무선 브랜치 클라이언트에 대해 Dot1X 인증을 수행합니다.

CCKM/OKC 빠른 로밍

- FlexConnect 액세스 포인트에서 작동하려면 CCKM/OKC 빠른 로밍이 필요합니다.빠른 로밍은 전체 EAP 인증에서 마스터 키의 파생물을 캐싱하여 무선 클라이언트가 다른 액세스 포인트로 로밍할 때 간단하고 안전한 키 교환을 수행할 수 있도록 합니다.이 기능은 클라이언트가 한 액세스 포인트에서 다른 액세스 포인트로 로밍할 때 전체 RADIUS EAP 인증을 수행할 필요성을 방지합니다.FlexConnect 액세스 포인트는 컨트롤러에 다시 보내는 대신 신속하게 처리할 수 있도록 연결할 수 있는 모든 클라이언트에 대한 CCKM/OKC 캐시 정보를 가져와야 합니다.예를 들어, 300개의 액세스 포인트와 100개의 클라이언트가 연결될 수 있는 컨트롤러가 있는 경우, 100개의 모든 클라이언트에 대해 CCKM/OKC 캐시를 전송하는 것이 실용적이지 않습니다.제한된 수의 액세스 포인트로 구성된 FlexConnect 그룹을 생성할 경우(예: 원격 사무실의 4개 액세스 포인트에 대한 그룹을 생성할 경우), 클라이언트는 이 4개의 액세스 포인트 중 하나에만 로밍하며, CCKM/OKC 캐시는 클라이언트가 그 중 하나에 연결될 때만 이 4개의 액세스 포인트

간에 분산됩니다.

- 이 기능은 백업 RADIUS 및 로컬 인증(로컬 EAP)과 함께 지사 사이트의 **운영** 다운타임을 방지합니다.**참고:** FlexConnect 및 비FlexConnect 액세스 포인트 간의 CCKM/OKC 빠른 로밍은 지원되지 않습니다.**그림 12:FlexConnect 그룹을 사용한 무선 네트워크 설계 참조**

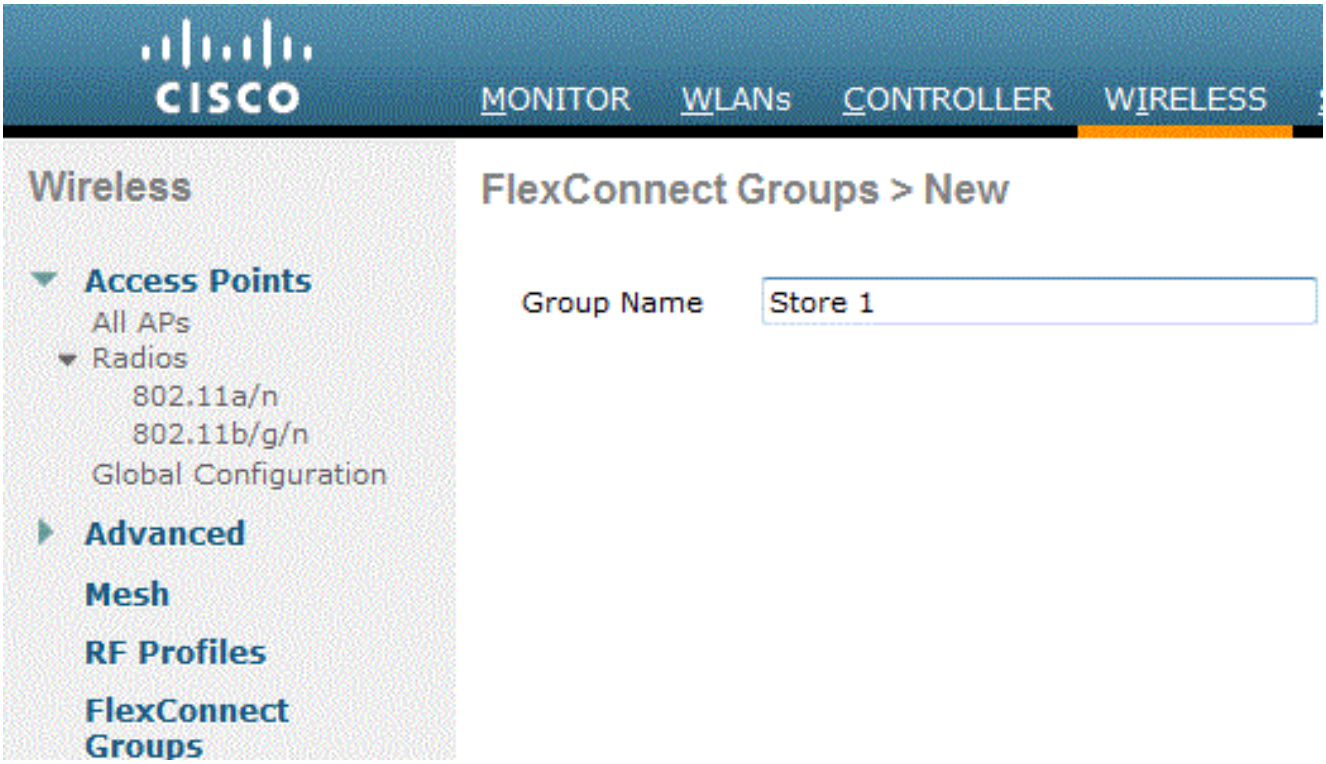


WLC의 FlexConnect 그룹 컨피그레이션

FlexConnect가 Connected(연결됨) 또는 Standalone(독립형) 모드에 있을 때 LEAP를 사용하여 로컬 인증을 지원하도록 FlexConnect 그룹을 구성하려면 이 섹션의 단계를 완료합니다.그림 12의 컨피그레이션 샘플에서는 AP 그룹과 FlexConnect 그룹 간의 목표 차이점과 1:1 매핑을 보여줍니다.

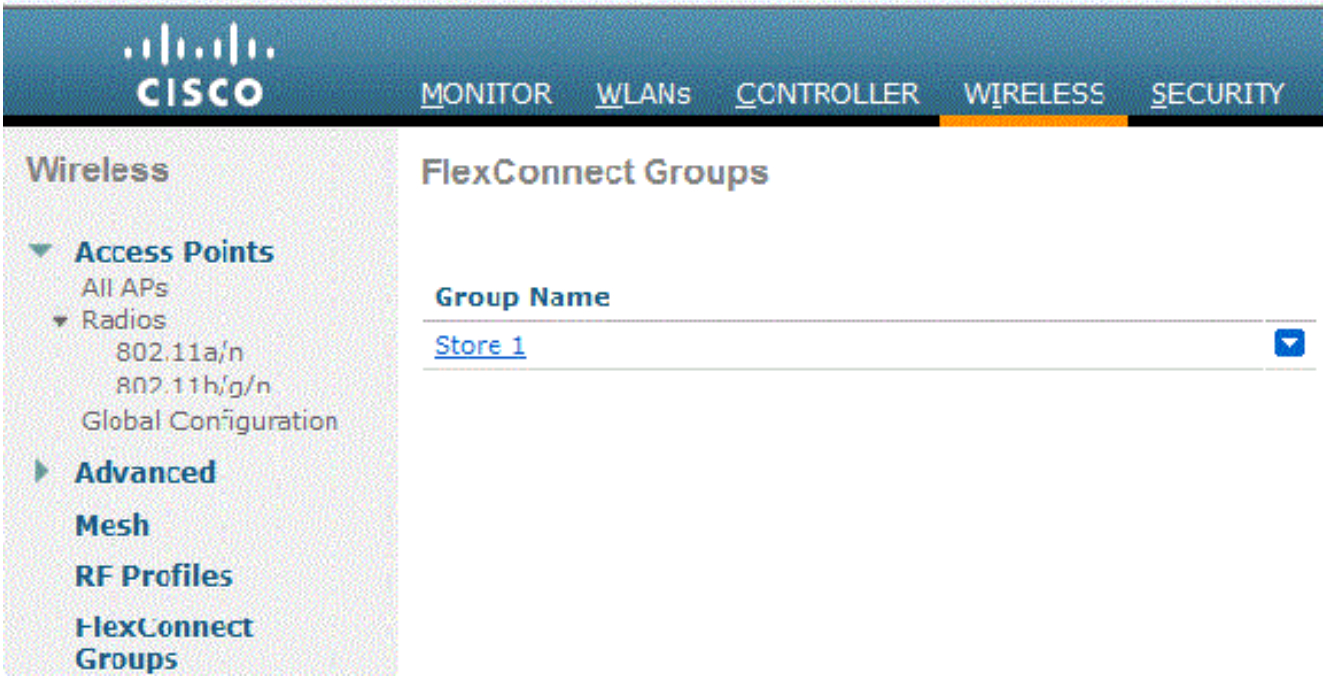
1. Wireless(무선) > FlexConnect Groups(FlexConnect 그룹)에서 New(**새로 만들기**)를 클릭합니다.
2. 그림 12에 나와 있는 샘플 컨피그레이션과 유사한 그룹 이름 매장 1을 할당합니다.
3. 그룹 **이름**이 설정되면 적용을 누릅니다

.



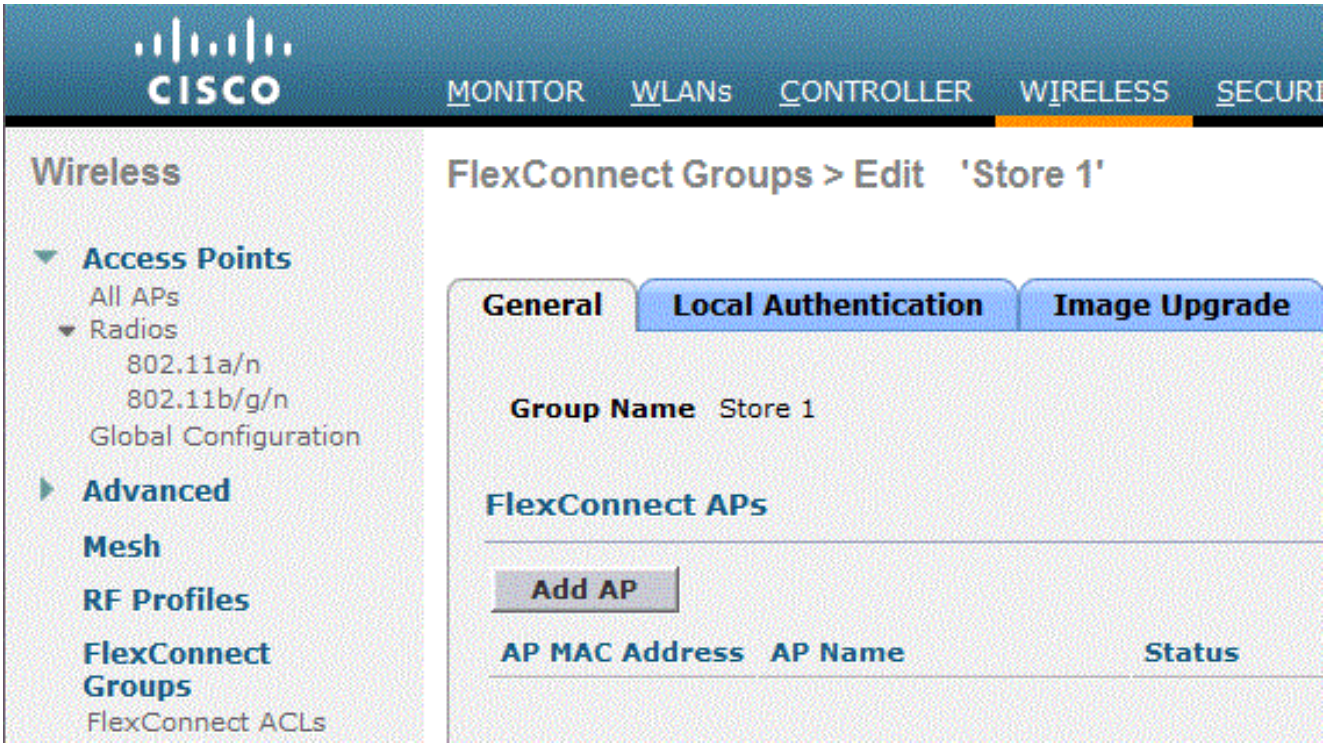
4. 추가 컨피그레이션을 위해 방금 생성한 Group Name **Store 1**을 클릭합니다

.



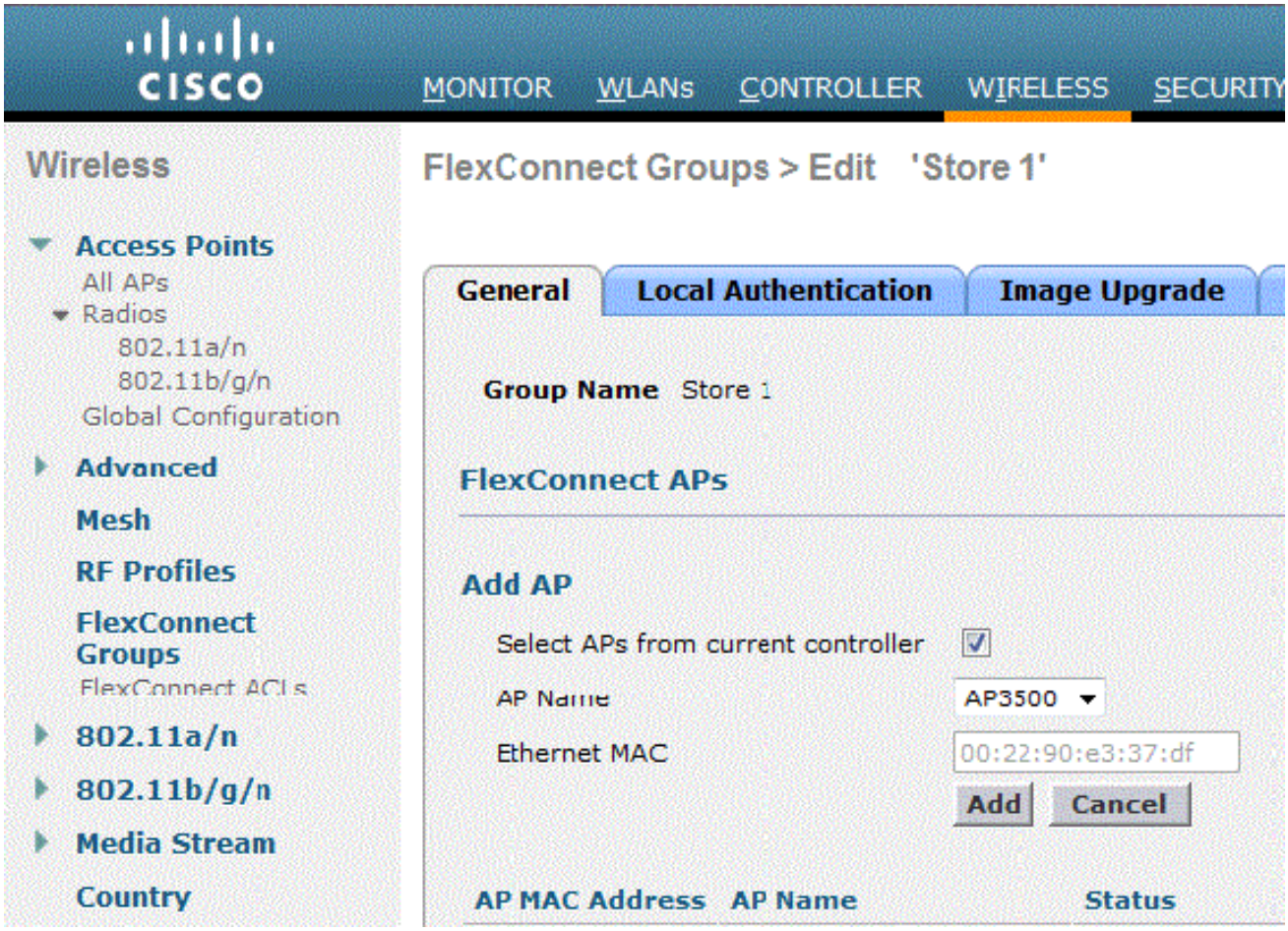
5. Add **AP(AP 추가)를 클릭합니다**

.

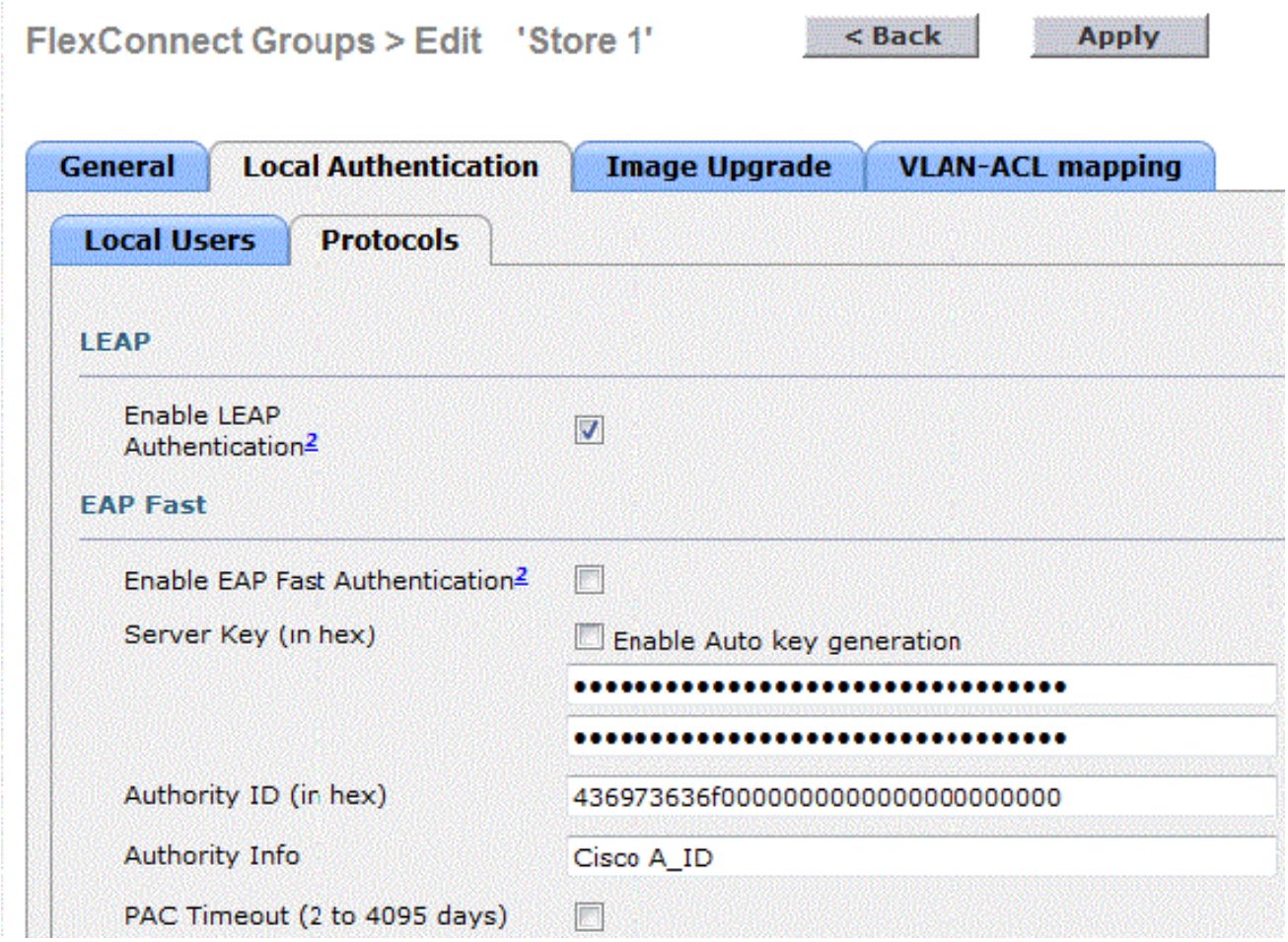


6. AP가 **독립형** 모드일 때 로컬 인증을 활성화하려면 Enable AP Local Authentication(AP 로컬 인증 활성화) 상자를 선택합니다.**참고:** 20단계에서는 연결 모드 AP에 대해 로컬 인증을 활성화하는 방법을 보여줍니다.
7. AP **Name** 드롭다운 메뉴**를 활성화하려면 Select APs from current controller(현재 컨트롤러**에서 AP 선택) 상자를 선택합니다.
8. 드롭다운에서 이 FlexConnect 그룹에 포함되어야 하는 AP를 선택합니다.
9. 드롭다운에서 AP를 선택한 후 **Add**를 클릭합니다.
10. AP-Group Store 1에도 포함된 이 FlexConnect 그룹에 모든 AP를 추가하려면 7단계와 8단계를 반복합니다. 그림 12를 참조하여 AP-Group과 FlexConnect 그룹 간의 1:1 매핑을 파악하십시오.스토어당 AP-그룹을 생성한 경우(그림 8) 해당 AP 그룹의 모든 AP가 이 FlexConnect 그룹에 포함되어야 합니다(그림 12). AP-Group과 FlexConnect 그룹 간의 1:1 비율을 유지하면 네트워크 관리가 간소화됩니다

.

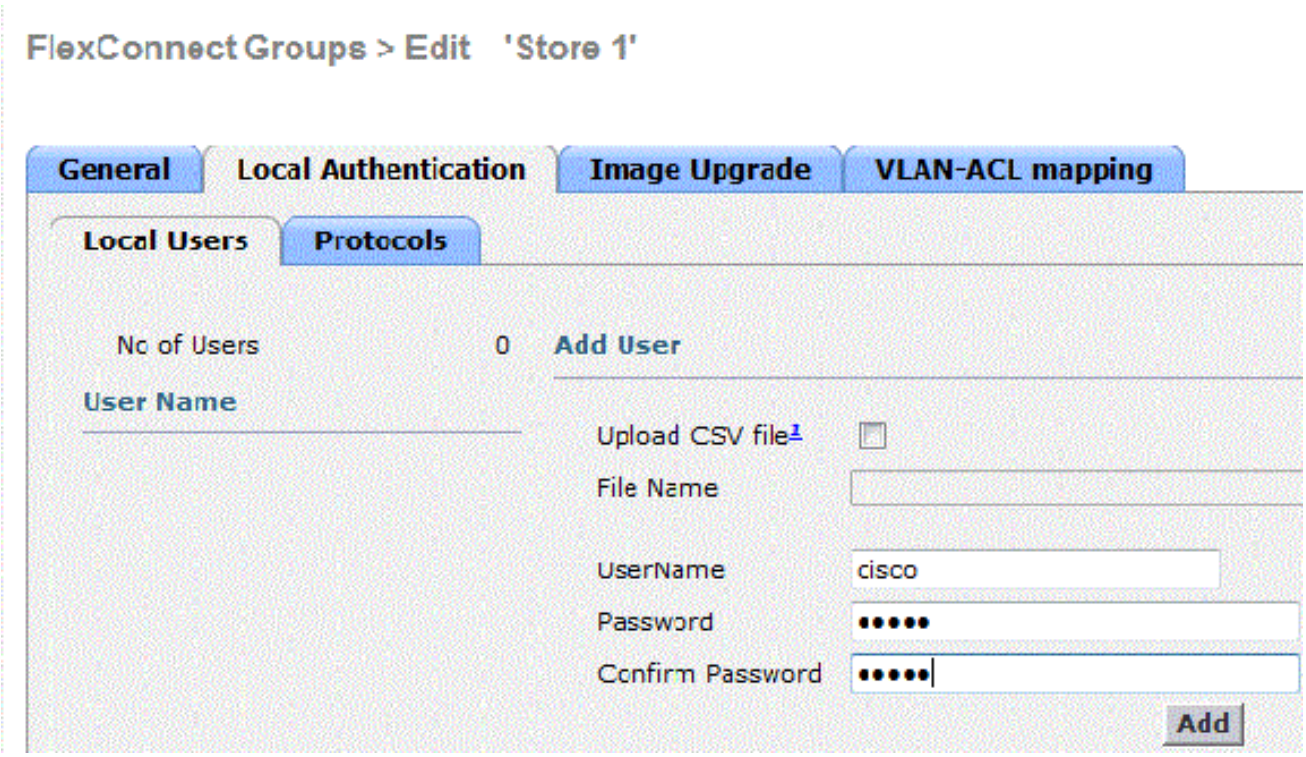


11. Local **Authentication(로컬 인증) > Protocols(프로토콜)**를 클릭하고 Enable LEAP **Authentication(LEAP 인증 활성화)** 상자를 선택합니다.
12. 확인란이 설정된 후 Apply를 클릭합니다.**참고:** 백업 컨트롤러가 있는 경우 FlexConnect 그룹이 동일하고 AP MAC 주소 항목이 FlexConnect 그룹별로 포함되어 있는지 확인하십시오
.



13. Local Authentication(로컬 인증)에서 Local Users(**로컬 사용자)를 클릭합니다**.
14. Username(사용자 이름), Password(비밀번호) 및 Confirm Password(비밀번호 확인) 필드를 설정한 다음 **Add(추가)**를 클릭하여 AP에 있는 로컬 EAP 서버에서 사용자 항목을 생성합니다.
15. 로컬 사용자 이름 목록이 모두 사용될 때까지 13단계를 반복합니다.100명 이상의 사용자를 구성하거나 추가할 수 없습니다.
16. 14단계가 완료되고 No of Users(사용자 수)가 확인된 후 Apply(적용)를 클릭합니다

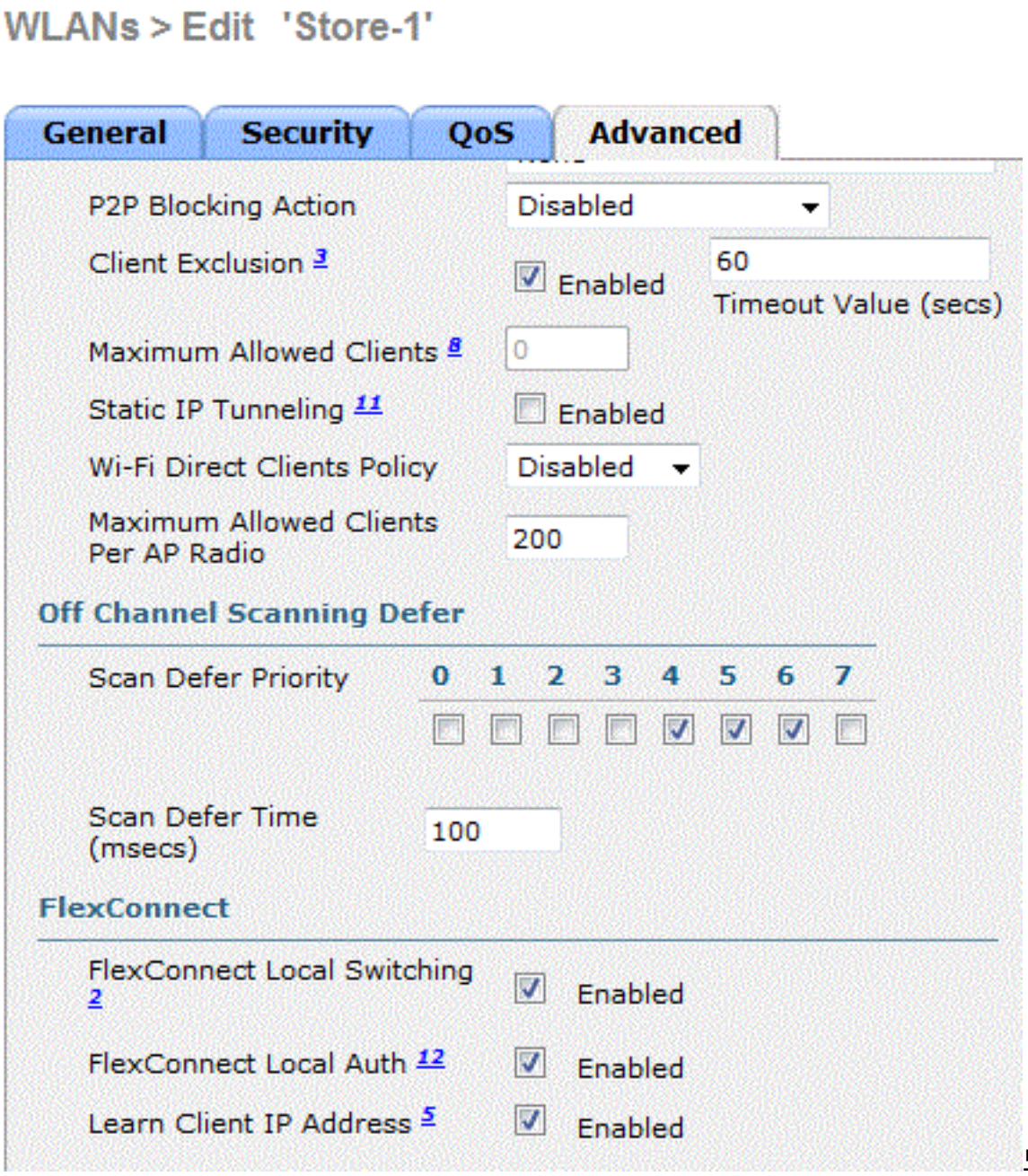
.



17. 상단 창에서 **WLANs**를 클릭합니다.
18. WLAN **ID 17**을 클릭합니다. AP 그룹을 생성하는 동안 생성되었습니다.그림 8을 참조하십시오

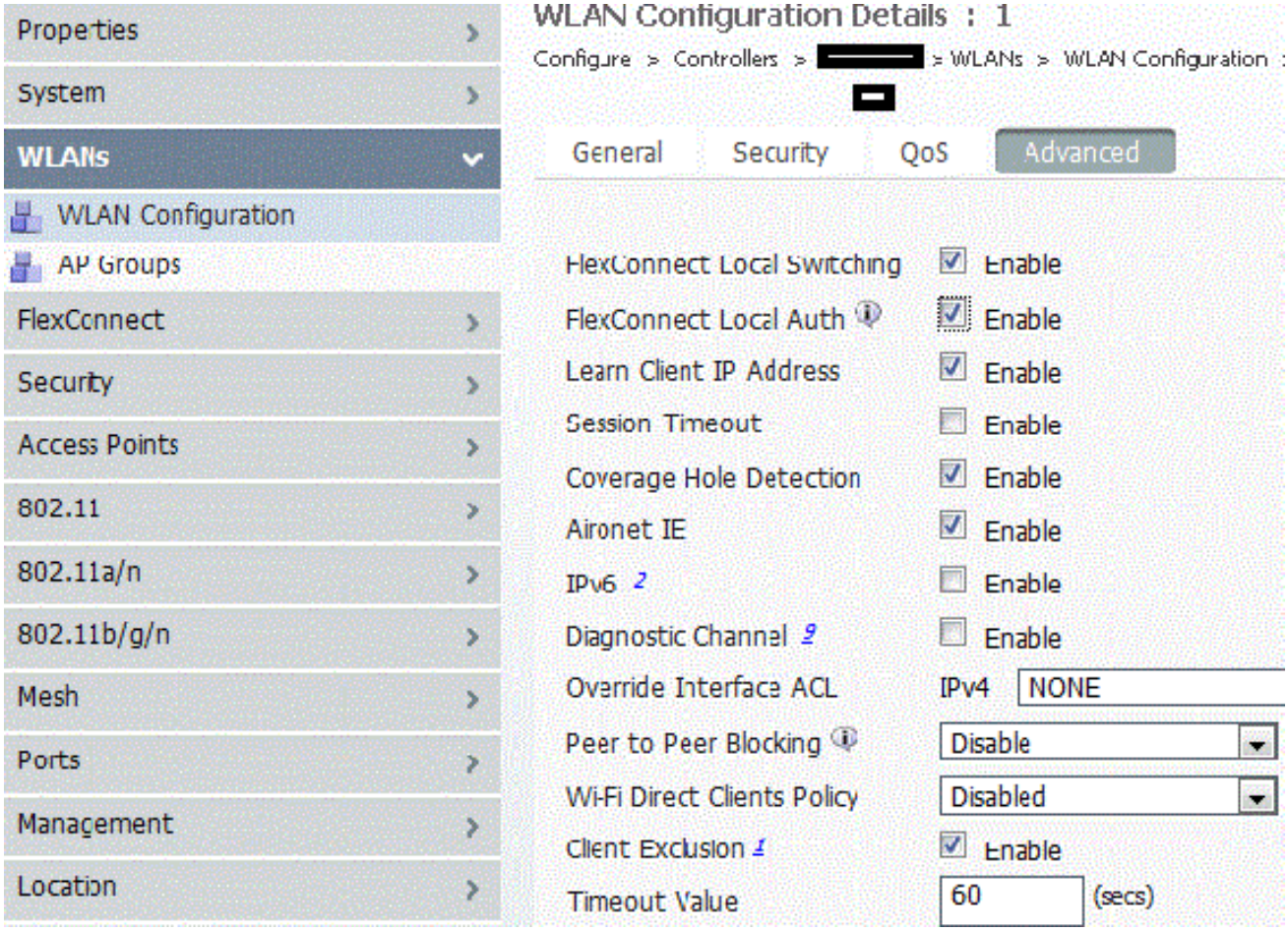
.

19. WLAN(WLAN) > Edit for WLAN ID 17(WLAN ID 17에 대한 편집)에서 Advanced(고급)를 **클릭합니다**.
20. Connected Mode(연결 모드)에서 Local Authentication(로컬 인증)을 활성화하려면 FlexConnect Local Auth(FlexConnect 로컬 인증) 상자를 선택합니다.**참고:** 로컬 인증은 FlexConnect with Local Switching에만 지원됩니다.**참고:** WLAN에서 로컬 인증을 활성화하기 전에 항상 FlexConnect 그룹을 만들어야 합니다



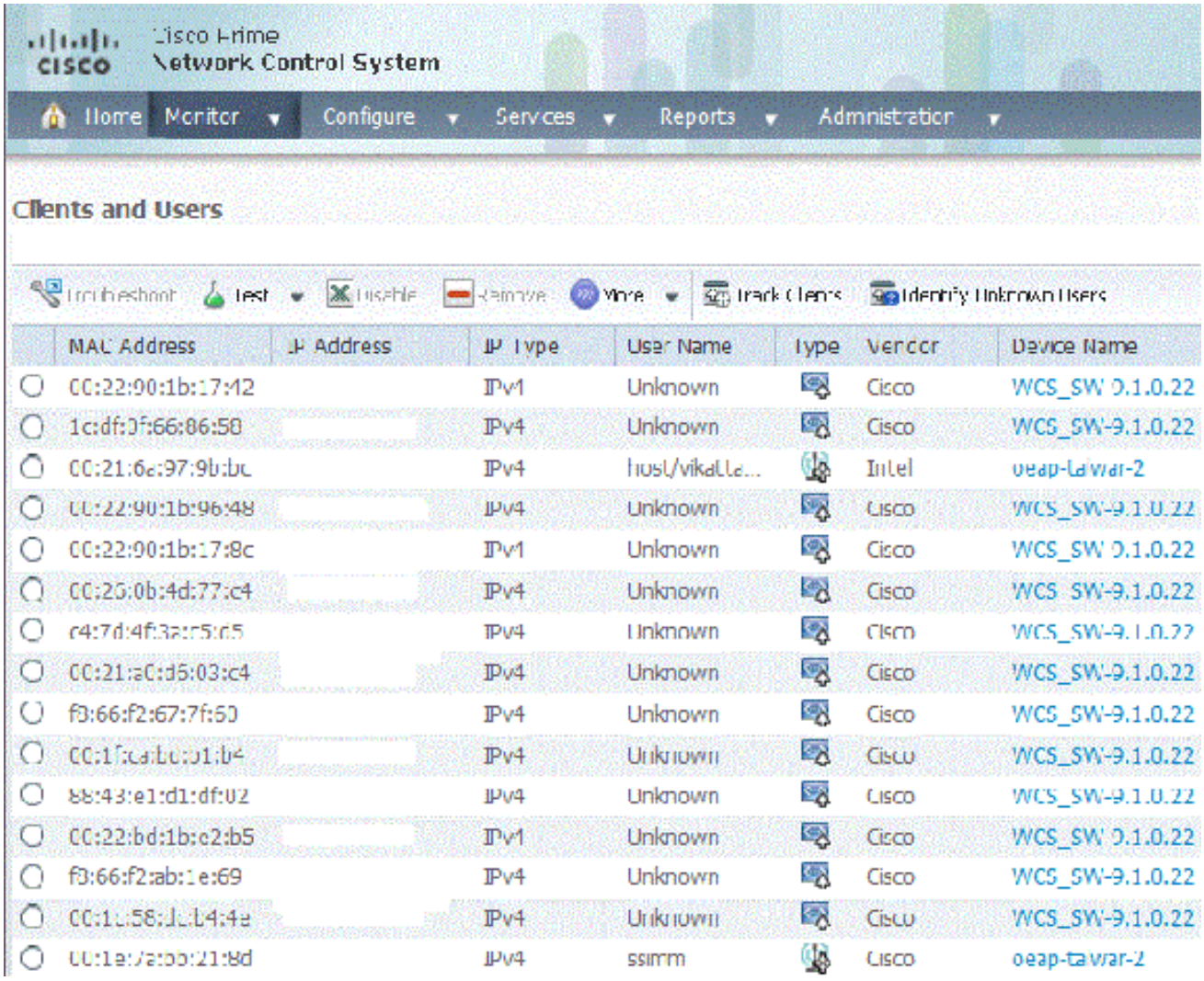
. 또한 NCS는 Connected Mode에서 Local Authentication(로컬 인증)을 활성화하기 위해 FlexConnect Local Auth(FlexConnect 로컬 인증) 확인란도 제공합니다

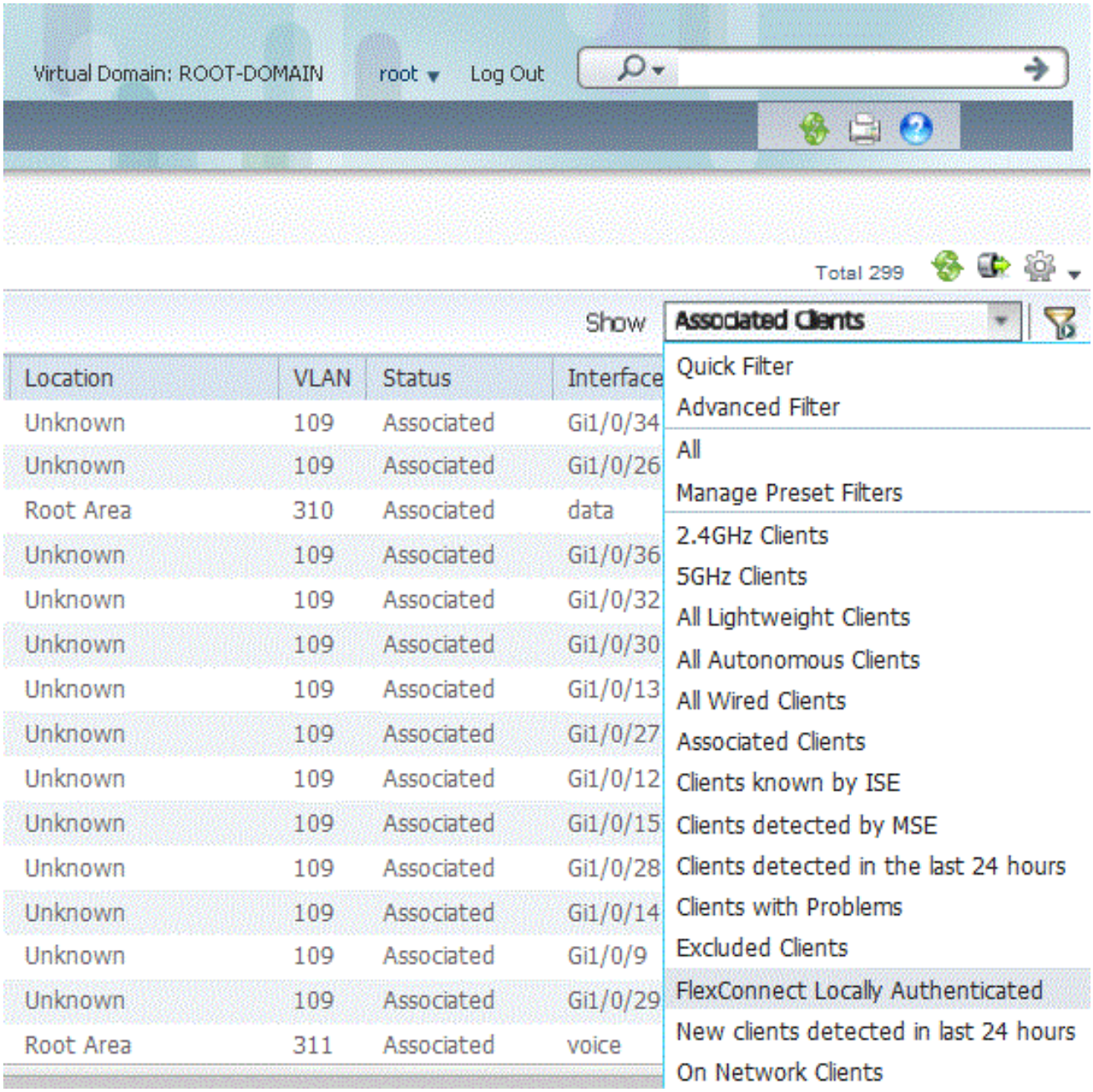
.



또한 NCS는 다음과 같이 FlexConnect 로컬 인증 클라이언트를 필터링하고 모니터링하는 기능을 제공합니다

.


Cisco Prime
Network Control System
Home
Monitor
Configure
Services
Reports
Administration
Clients and Users
Troubleshoot
Test
Disable
Remove
More
Track Clients
Identify Unknown Users
MAC Address
IP Address
IP Type
User Name
Type
Vendor
Device Name
00:22:90:1b:17:12 IPv4 Unknown Cisco WCS_SW 9.1.0.22
1c:df:0f:66:86:58 IPv4 Unknown Cisco WCS_SW-9.1.0.22
00:21:6a:97:9b:bc IPv4 host/vikalla... Intel deap-tavar-2
00:22:90:1b:96:48 IPv4 Unknown Cisco WCS_SW-9.1.0.22
00:22:90:1b:17:8c IPv4 Unknown Cisco WCS_SW 9.1.0.22
00:25:0b:4d:77:c4 IPv4 Unknown Cisco WCS_SW-9.1.0.22
c4:7d:4f:3a:c5:c5 IPv4 Unknown Cisco WCS_SW-9.1.0.22
00:21:a0:d5:03:c4 IPv4 Unknown Cisco WCS_SW-9.1.0.22
f0:66:f2:67:7f:50 IPv4 Unknown Cisco WCS_SW-9.1.0.22
00:1f:ca:bc:b1:b4 IPv4 Unknown Cisco WCS_SW-9.1.0.22
88:43:e1:d1:df:02 IPv4 Unknown Cisco WCS_SW-9.1.0.22
00:22:bd:1b:e2:b5 IPv4 Unknown Cisco WCS_SW 9.1.0.22
f0:66:f2:ab:1e:69 IPv4 Unknown Cisco WCS_SW-9.1.0.22
00:1c:58:bc:b4:4a IPv4 Unknown Cisco WCS_SW-9.1.0.22
00:1e:7a:bb:21:8d IPv4 ssimm Cisco deap-tavar-2



CLI를 사용한 확인

WLC에서 이 CLI를 사용하여 클라이언트 인증 상태 및 스위칭 모드를 신속하게 확인할 수 있습니다 .

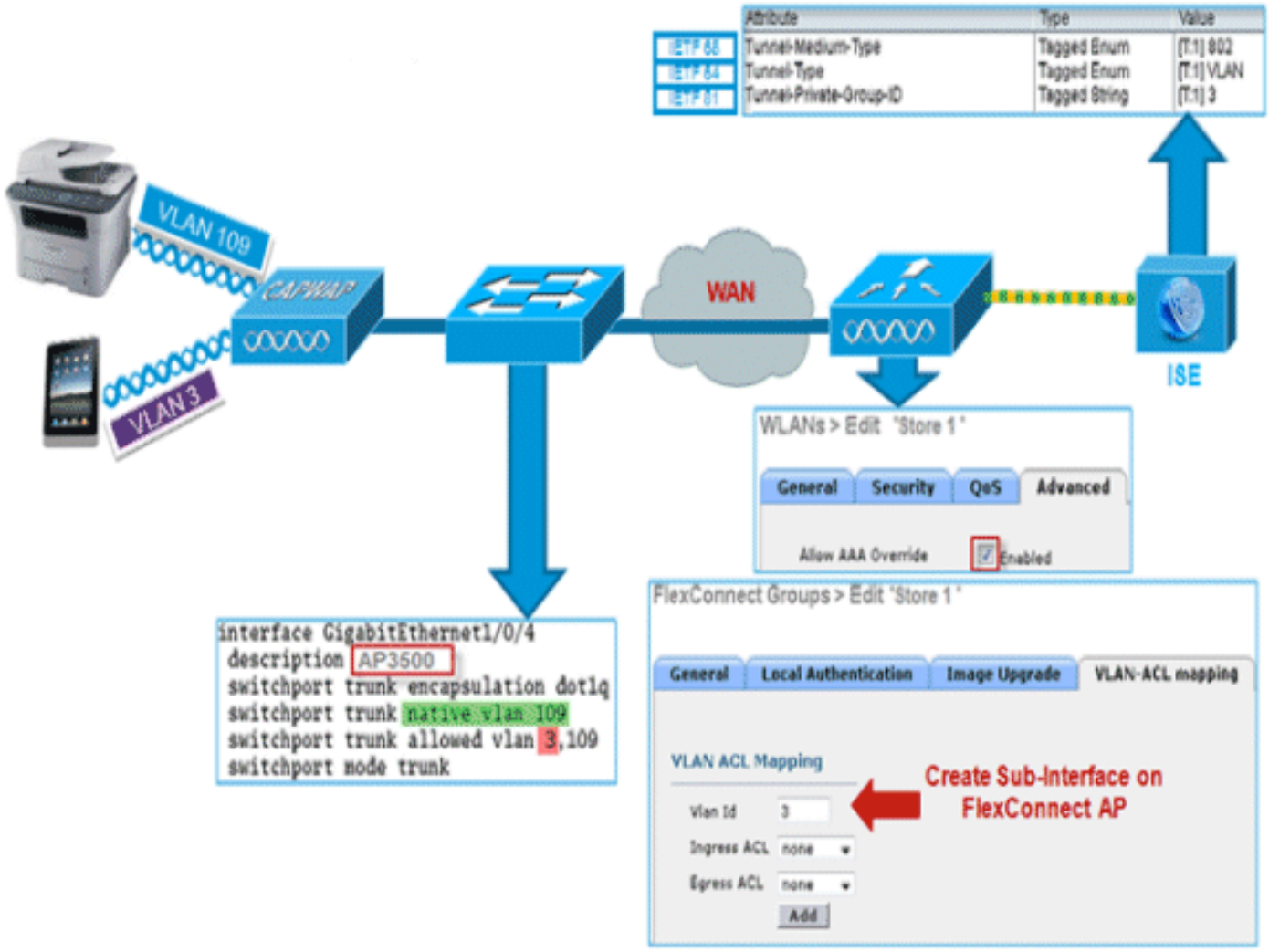
```
(Cisco Controller) >show client detail 00:24:d7:2b:7c:0c
Client MAC Address.............................. 00:24:d7:2b:7c:0c
Client Username ................................ N/A
AP MAC Address.................................. d0:57:4c:08:e6:70
Client State.................................... Associated
H-REAP Data Switching........................... Local
H-REAP Authentication........................... Local
```

FlexConnect VLAN 재정의

현재 FlexConnect 아키텍처에서는 WLAN을 VLAN에 엄격하게 매핑하므로 FlexConnect AP의 특정 WLAN에 연결된 클라이언트는 해당 VLAN에 매핑된 VLAN을 따라야 합니다.이 방법은 여러 VLAN

기반 정책을 상속하기 위해 클라이언트가 다른 SSID와 연결되어야 하므로 제한이 있습니다.

7.2 릴리스부터는 로컬 스위칭을 위해 구성된 개별 WLAN에서 VLAN의 AAA 재정의가 지원됩니다 .동적 VLAN을 할당하기 위해 AP는 개별 FlexConnect AP에 대해 기존 WLAN-VLAN 매핑을 사용하거나 FlexConnect 그룹에서 ACL-VLAN 매핑을 사용하여 컨피그레이션을 기반으로 VLAN에 대한 인터페이스를 미리 생성합니다.WLC는 AP에서 하위 인터페이스를 미리 생성하는 데 사용됩니다.



요약

- AAA VLAN 재정의는 중앙 및 로컬 인증 모드에서 로컬 스위칭을 위해 구성된 WLAN에 대해 릴리스 7.2에서 지원됩니다.
- 로컬 스위칭을 위해 구성된 WLAN에서 AAA 재지정을 활성화해야 합니다.
- FlexConnect AP에는 동적 VLAN 할당을 위해 WLC에서 미리 생성된 VLAN이 있어야 합니다.
- AAA 재정의에서 반환된 VLAN이 AP 클라이언트에 없으면 AP의 기본 VLAN 인터페이스에서 IP를 가져옵니다.

절차

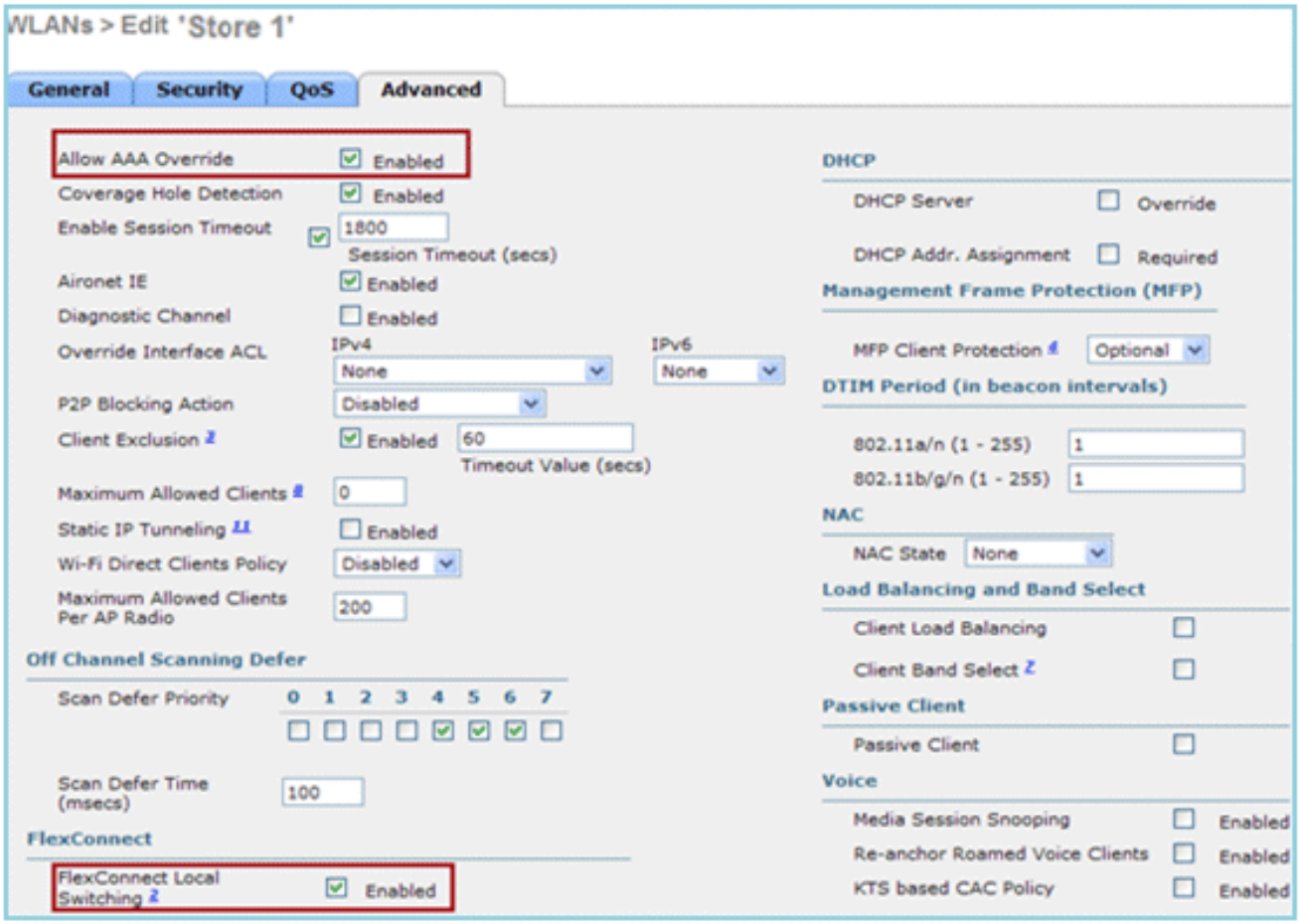
다음 단계를 완료하십시오.

1. 802.1x 인증을 위한 WLAN을 생성합니다

.

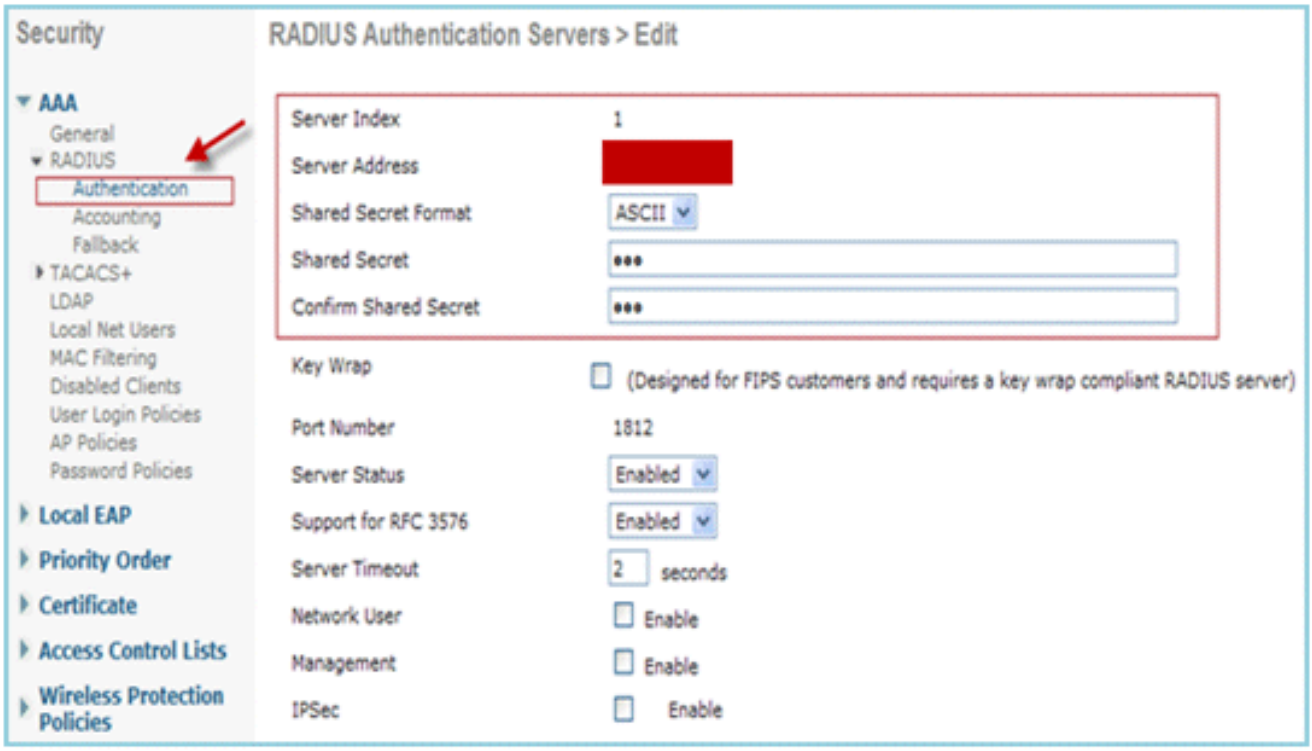
2. WLC에서 로컬 스위칭 WLAN에 대한 AAA 재정의 지원을 활성화합니다.**WLAN GUI > WLAN > WLAN ID > Advance 탭으로** 이동합니다

.



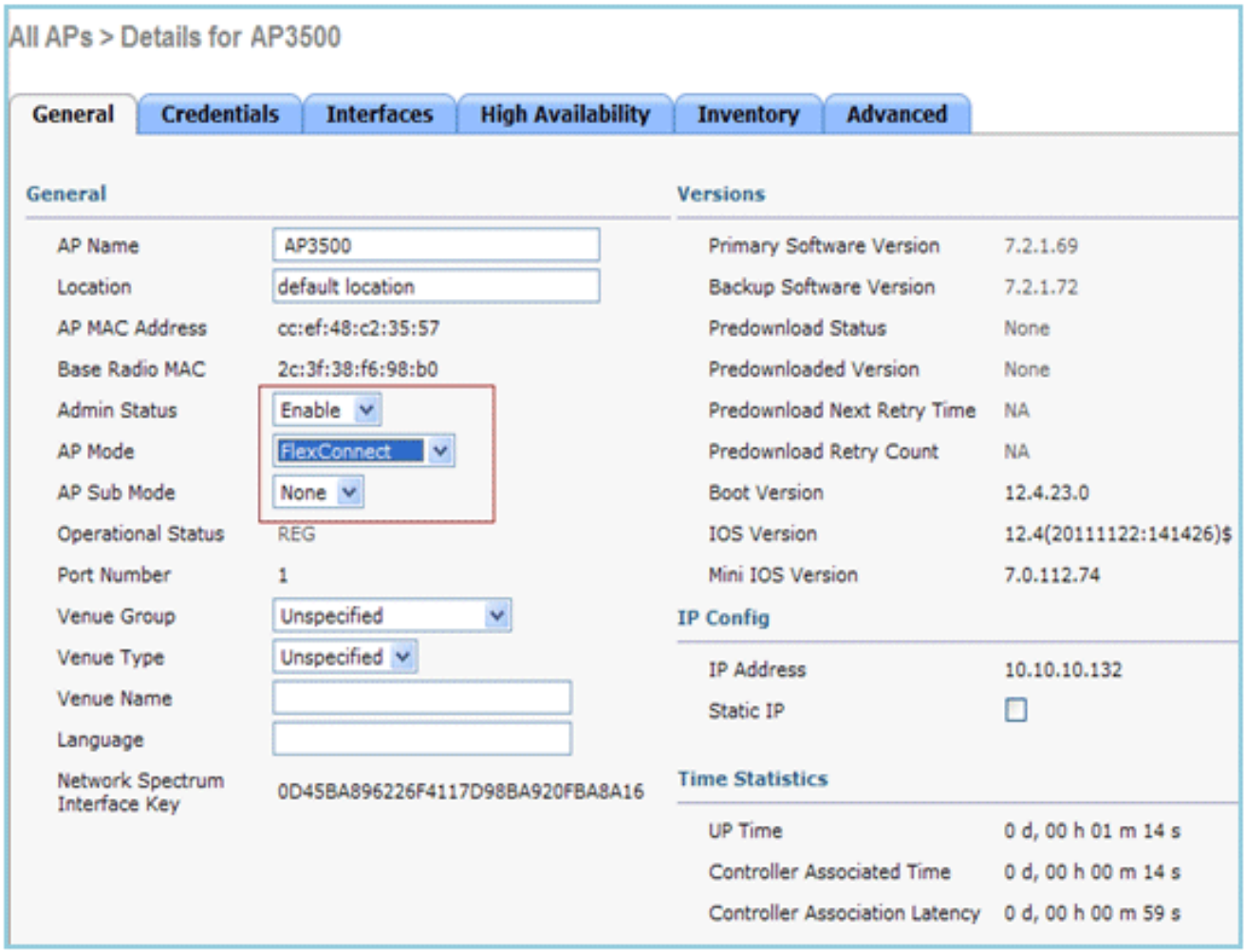
3. 802.1x 인증을 위해 컨트롤러에 AAA 서버 세부 정보를 추가합니다.AAA 서버를 추가하려면 **WLC GUI > Security > AAA > Radius > Authentication > New로** 이동합니다

.



4. AP는 기본적으로 로컬 모드이므로 모드를 FlexConnect 모드로 전환합니다.로컬 모드 AP는 Wireless(**무선) > All APs(모든 AP)로** 이동하여 Individual AP(개별 AP)를 클릭하여 FlexConnect 모드로 변환할 수 있습니다

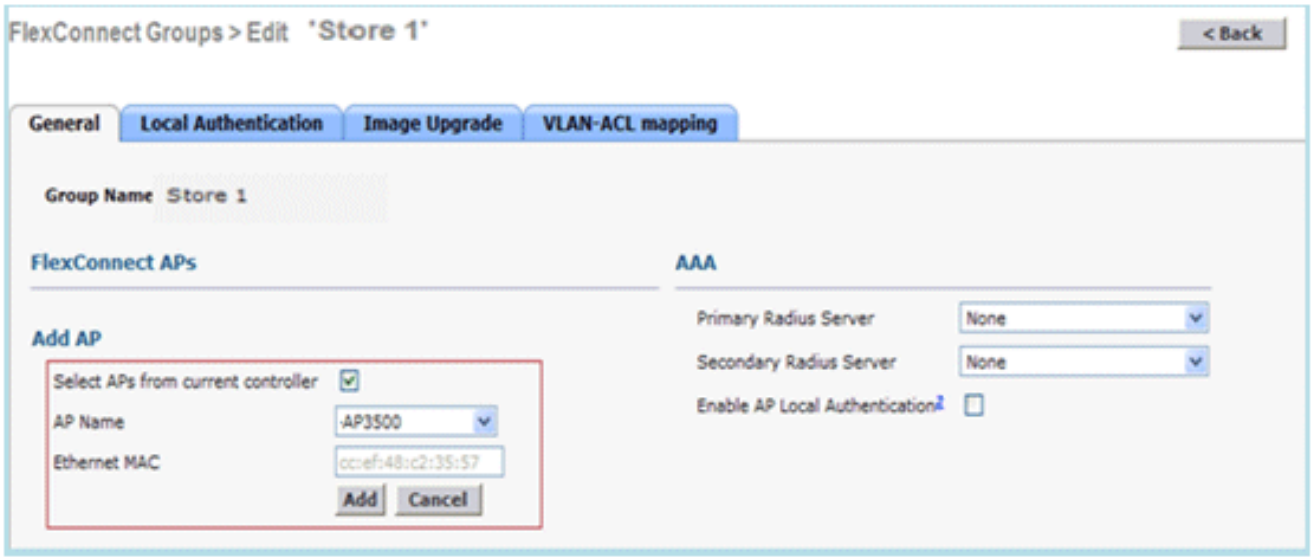
.



5. FlexConnect 그룹에 FlexConnect AP를 추가합니다.WLC **GUI > Wireless > FlexConnect**

Groups > Select FlexConnect Group > General 탭 > Add AP(AP 추가)로 이동합니다

.

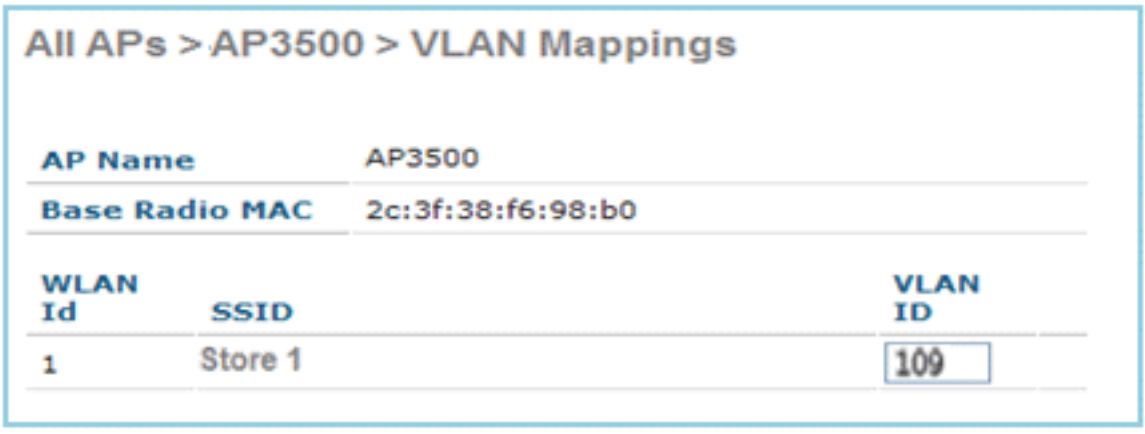


6. FlexConnect AP는 트렁크 포트에 연결되어야 하며 WLAN 매핑된 VLAN과 트렁크 포트에서 AAA 재정의 VLAN을 허용해야 합니다.

```
interface GigabitEthernet1/0/4
 description AP3500
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 109
 switchport trunk allowed vlan 3,109
 switchport mode trunk
```

참고: 이 컨피그레이션에서는 vlan 109가 WLAN VLAN 매핑에 사용되고 vlan 3은 AAA 재정의에 사용됩니다.

7. FlexConnect AP에 대해 WLAN과 VLAN 매핑을 구성합니다.이 컨피그레이션에 따라 AP에는 VLAN에 대한 인터페이스가 있습니다.AP가 VLAN 컨피그레이션을 수신하면 해당 dot11 및 이더넷 하위 인터페이스가 생성되고 브리지 그룹에 추가됩니다.이 WLAN에서 클라이언트를 연결하고 클라이언트가 연결할 때 VLAN(WLAN-VLAN 매핑을 기반으로 기본값)이 할당됩니다 .**WLAN GUI > Wireless > All APs** > 특정 AP > **FlexConnect** 탭을 클릭하고 VLAN Mapping을 **클릭합니다**



.

8. AAA 서버에서 사용자를 생성하고 IETF Radius 속성에서 VLAN ID를 반환하도록 사용자를 구성합니다

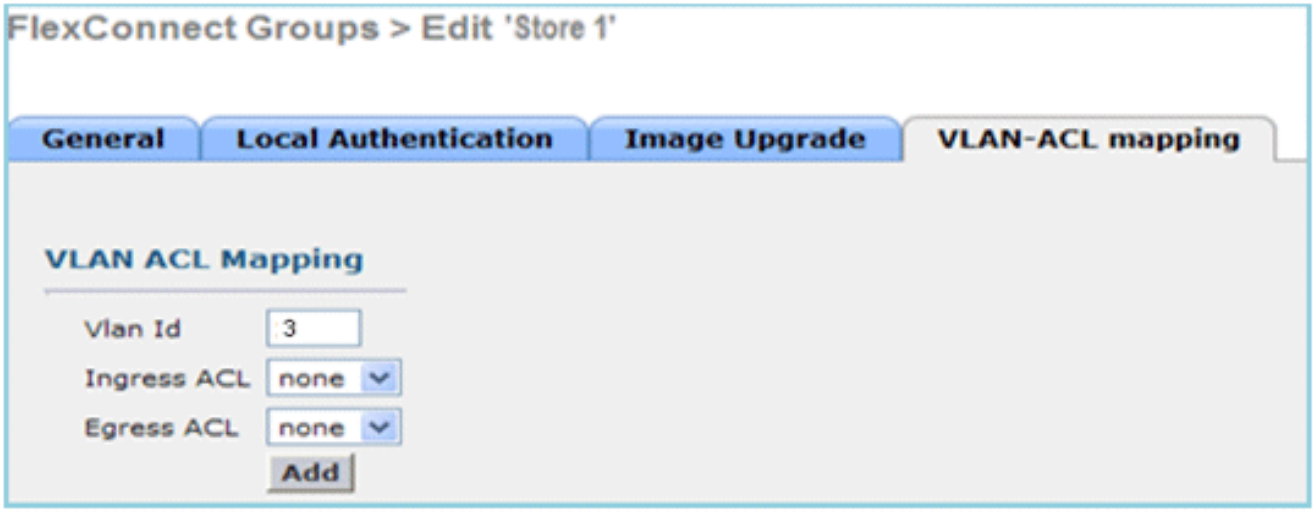
IETF 65
IETF 64
IETF 81

Attribute	Type	Value
Tunnel-Medium-Type	Tagged Enum	[T:1] 802
Tunnel-Type	Tagged Enum	[T:1] VLAN
Tunnel-Private-Group-ID	Tagged String	[T:1] 3

.

9. 동적 VLAN을 할당하기 위해 AP는 개별 FlexConnect AP에 대해 기존 WLAN-VLAN 매핑을 사용하거나 FlexConnect 그룹에서 ACL-VLAN 매핑을 사용하여 컨피그레이션을 기반으로 동적 VLAN에 대한 인터페이스를 미리 생성합니다.FlexConnect AP에서 AAA VLAN을 구성하려면 **WLC GUI > Wireless > FlexConnect Group** > 특정 FlexConnect 그룹 > **VLAN-ACL 매핑을** 클릭하고 **Vlan ID 필드**에 VLAN을 입력합니다

.



10. 이 WLAN에서 클라이언트를 연결하고 AAA VLAN을 반환하기 위해 AAA 서버에 구성된 사용자 이름을 사용하여 인증합니다.
11. 클라이언트는 AAA 서버를 통해 반환된 동적 VLAN에서 IP 주소를 수신해야 합니다.
12. 확인하려면 WLC **GUI > Monitor > Client** > 특정 클라이언트 MAC 주소를 클릭하여 클라이언트 세부사항을 확인합니다.

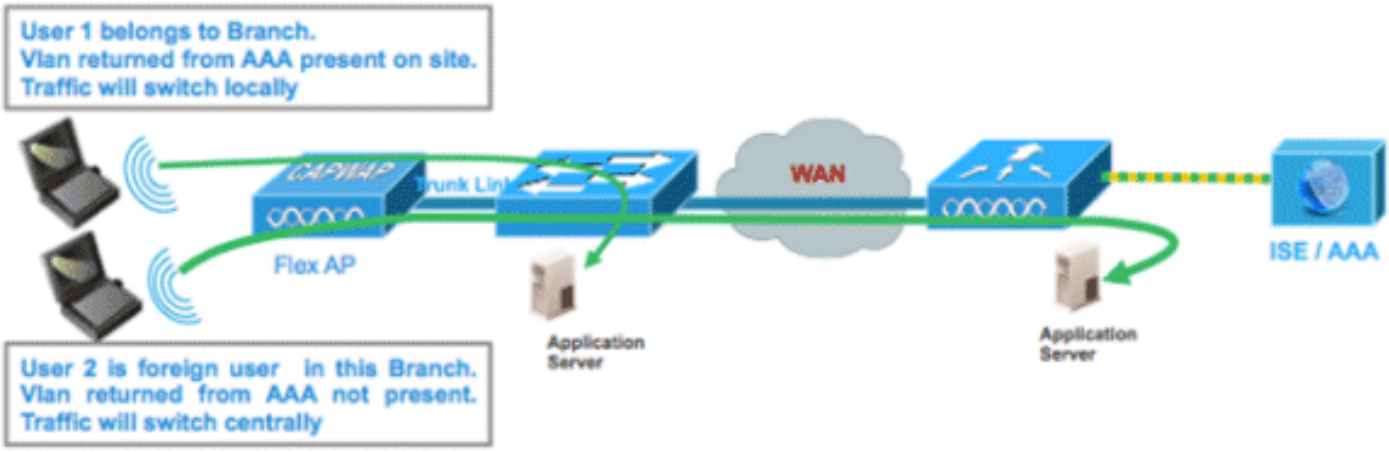
제한 사항

- **Cisco Airespace** 관련 특성은 지원되지 않으며 IETF 특성 VLAN ID만 지원됩니다.
- 개별 FlexConnect AP에 대해 WLAN-VLAN 매핑을 통해 또는 FlexConnect 그룹에서 ACL-VLAN 매핑을 사용하여 AP당 컨피그레이션에 최대 16개의 VLAN을 구성할 수 있습니다.

FlexConnect VLAN 기반 중앙 스위칭

컨트롤러 소프트웨어 릴리스 7.2에서는 로컬로 스위칭된 WLAN에 대한 VLAN(동적 VLAN 할당)의 AAA 재정의가 AAA 서버에서 제공하는 VLAN에 무선 클라이언트를 배치합니다.AAA 서버에서 제공한 VLAN이 AP에 없는 경우 클라이언트는 해당 AP의 WLAN 매핑된 VLAN에 배치되고 트래픽은 해당 VLAN에서 로컬로 전환됩니다.또한 릴리스 7.3 이전에는 WLAN 컨피그레이션에 따라 FlexConnect AP의 특정 WLAN에 대한 트래픽을 중앙 또는 로컬로 스위칭할 수 있습니다.

릴리스 7.3부터는 FlexConnect AP에 VLAN이 있는 경우 FlexConnect AP에 따라 FlexConnect AP의 트래픽을 중앙에서 또는 로컬로 스위칭할 수 있습니다.



요약

Flex AP가 연결 모드에 있을 때 로컬 스위칭을 위해 구성된 WLAN의 트래픽 흐름:

- VLAN이 AAA 특성 중 하나로 반환되고 VLAN이 Flex AP 데이터베이스에 없는 경우 트래픽은 중앙에서 전환되며 VLAN이 WLC에 있는 경우 AAA 서버에서 반환되는 이 VLAN/인터페이스가 클라이언트에 할당됩니다.
- VLAN이 AAA 특성 중 하나로 반환되고 해당 VLAN이 Flex AP 데이터베이스에 없는 경우 트래픽이 중앙에서 전환됩니다.해당 VLAN이 WLC에도 없는 경우 클라이언트는 WLC의 WLAN에 매핑된 VLAN/인터페이스를 할당합니다.
- VLAN이 AAA 특성 중 하나로 반환되고 해당 VLAN이 FlexConnect AP 데이터베이스에 있으면 트래픽은 로컬로 전환됩니다.
- AAA 서버에서 VLAN이 반환되지 않으면 해당 FlexConnect AP에 WLAN 매핑 VLAN이 클라이언트에 할당되고 트래픽은 로컬로 전환됩니다.

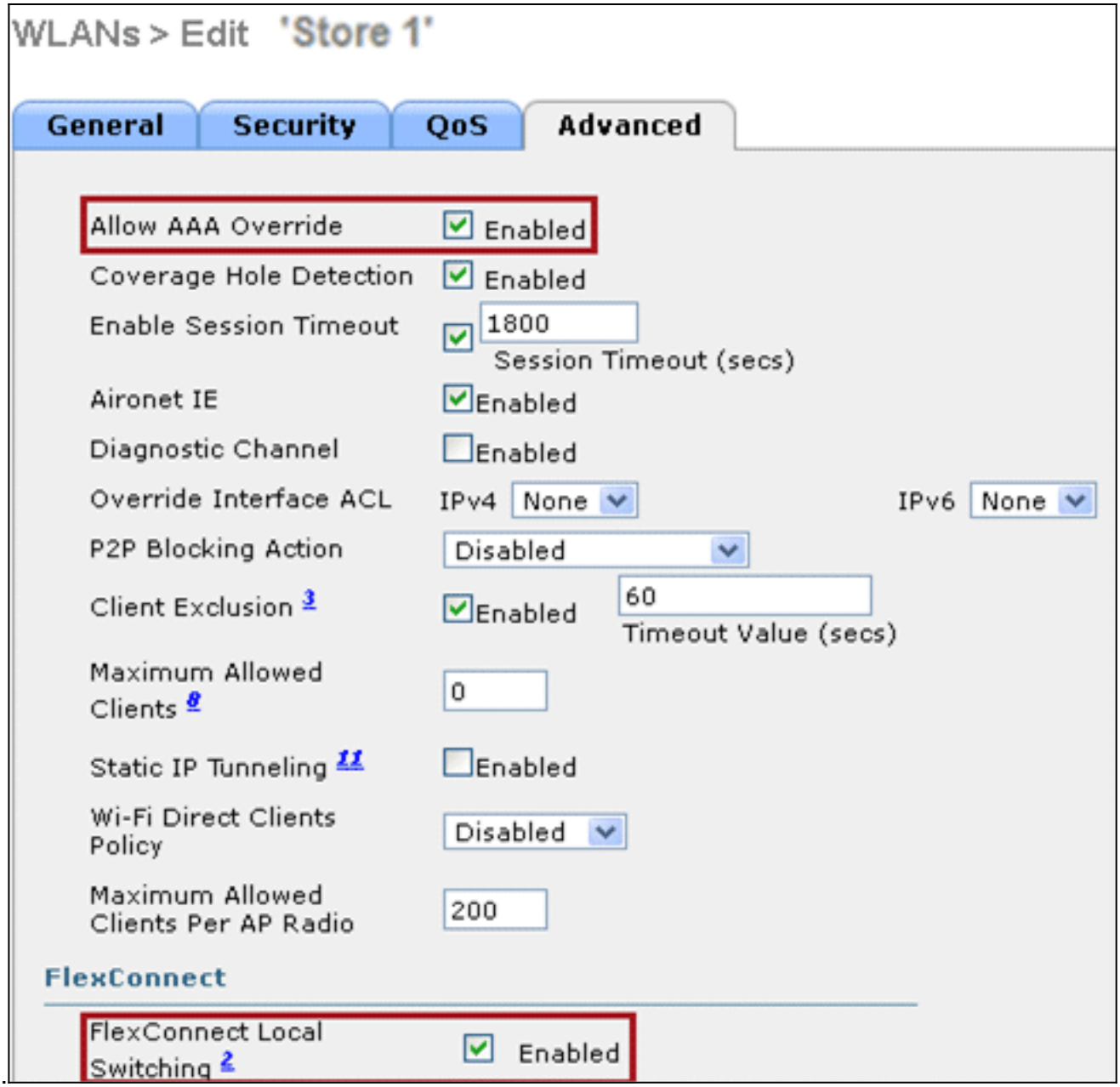
Flex AP가 독립형 모드에 있을 때 로컬 스위칭을 위해 구성된 WLAN의 트래픽 흐름:

- AAA 서버에서 반환한 VLAN이 Flex AP 데이터베이스에 없는 경우, 클라이언트는 기본 VLAN에 배치됩니다(즉, Flex AP의 WLAN 매핑 VLAN). AP가 다시 연결되면 이 클라이언트는 인증이 취소되고 중앙에서 트래픽을 전환합니다.
- AAA 서버에서 반환된 VLAN이 Flex AP 데이터베이스에 있는 경우 클라이언트는 반환된 VLAN에 배치되고 트래픽은 로컬로 전환됩니다.
- AAA 서버에서 VLAN이 반환되지 않으면 해당 FlexConnect AP에 WLAN 매핑 VLAN이 클라이언트에 할당되고 트래픽은 로컬로 전환됩니다.

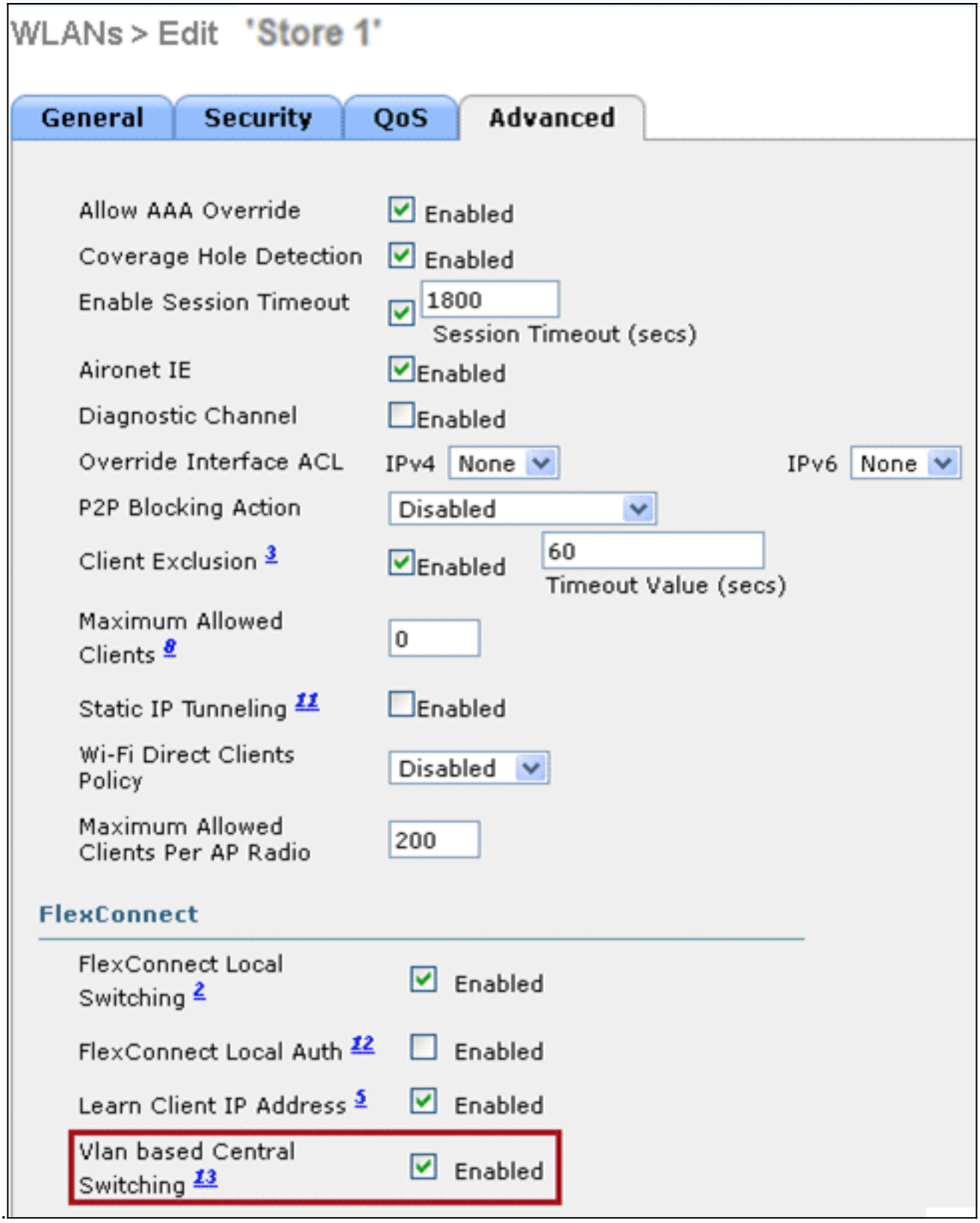
절차

다음 단계를 완료하십시오.

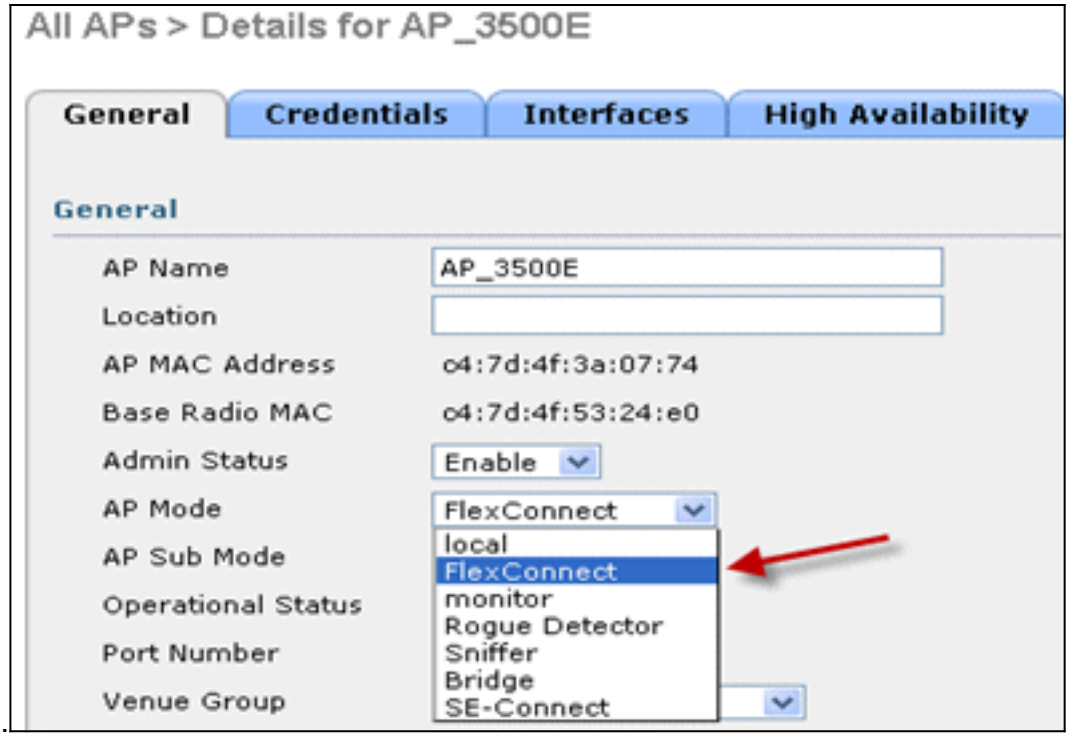
1. 로컬 스위칭을 위한 WLAN을 구성하고 AAA 재지정을 활성화합니다



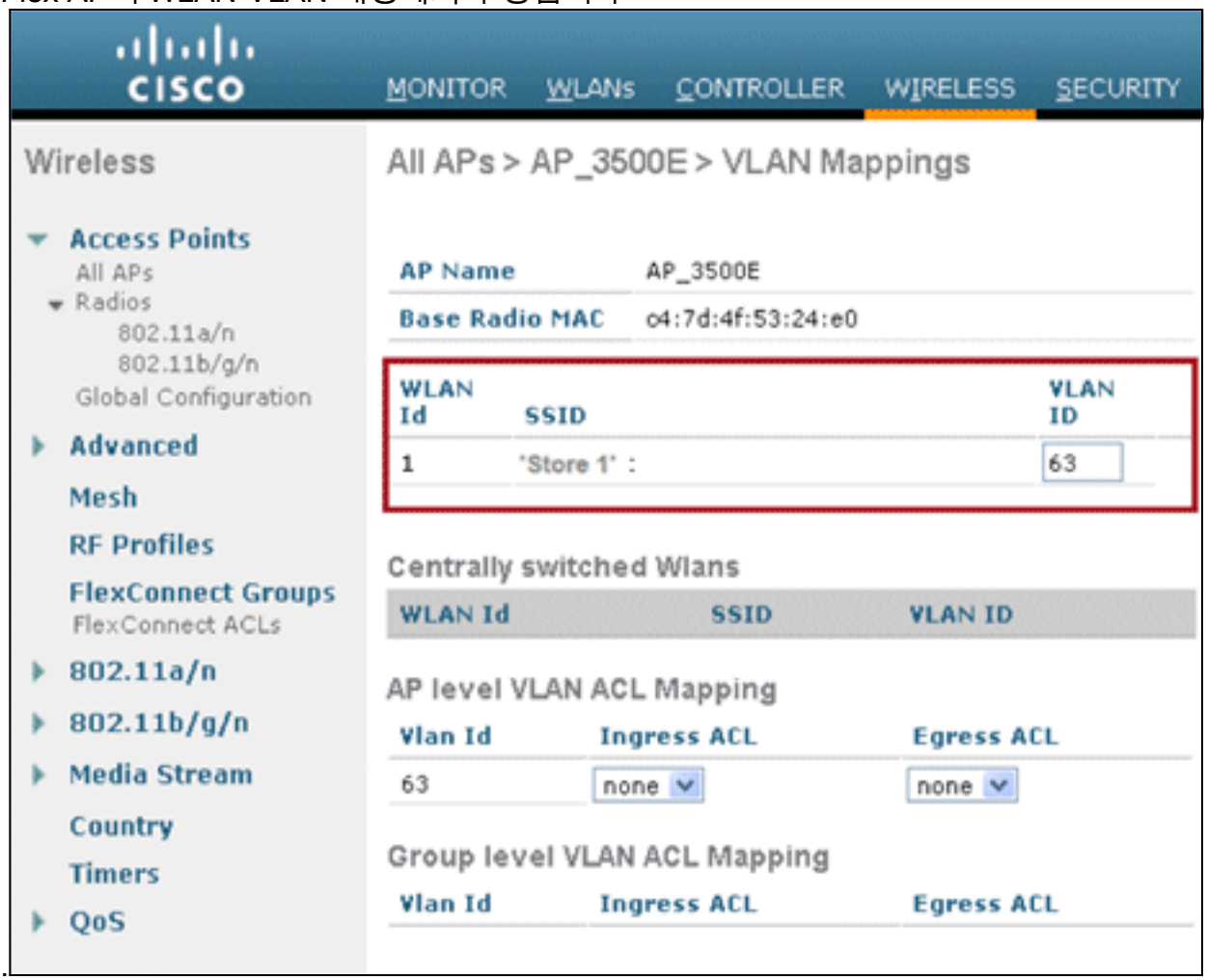
2. 새로 **생성된 WLAN**에서 VLAN **기반 중앙 스위칭**을 활성화합니다



3. AP 모드를 FlexConnect로 **설정합니다**

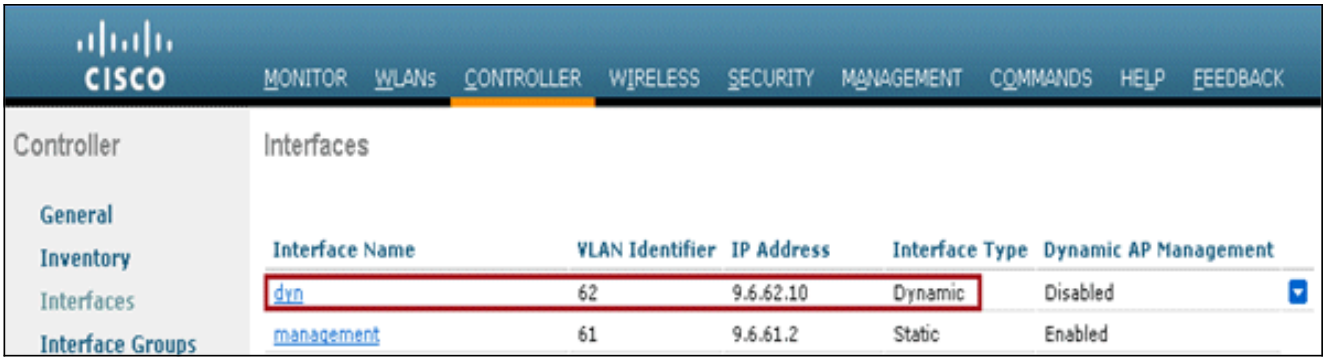


4. FlexConnect AP의 데이터베이스에 특정 Flex AP의 WLAN-VLAN 매핑을 통해 또는 Flex 그룹에서 VLAN을 구성하여 일부 하위 인터페이스가 있는지 확인합니다.이 예에서 VLAN 63은 Flex AP의 WLAN-VLAN 매핑에서 구성됩니다



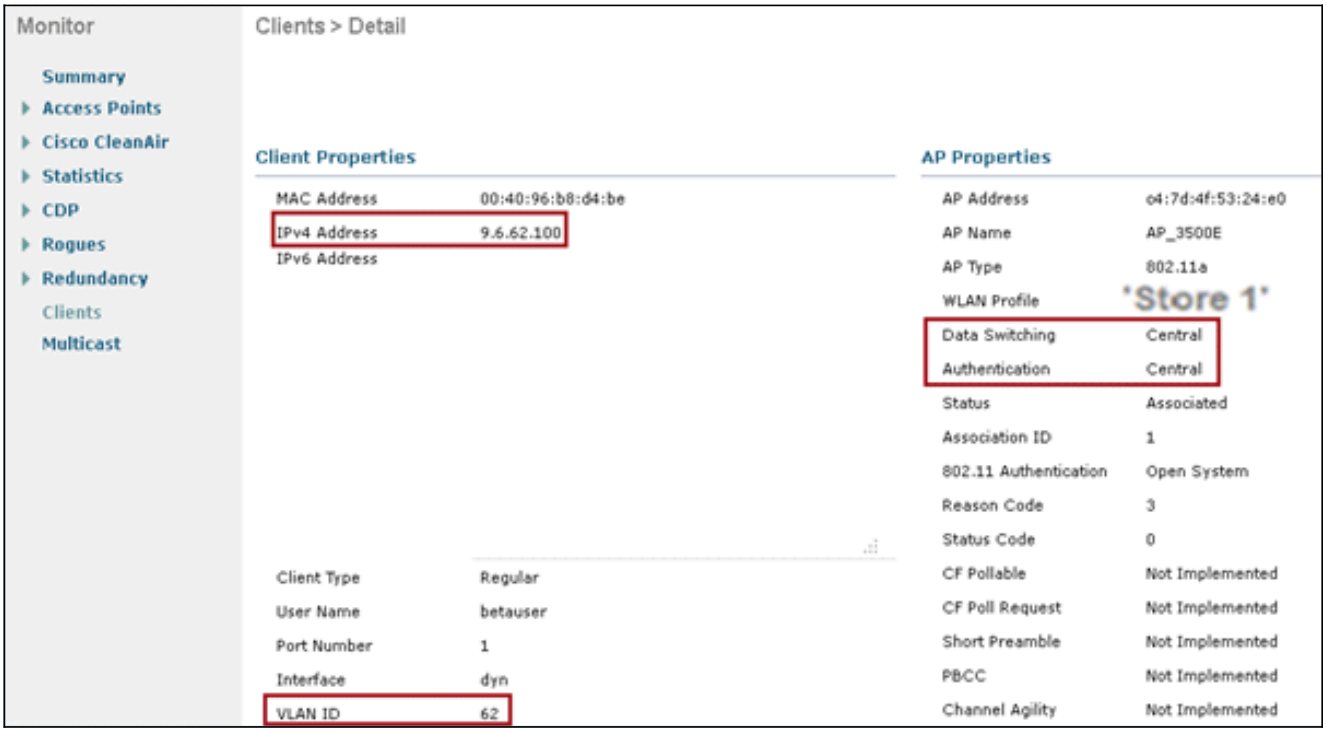
5. 이 예에서 VLAN 62는 WLC에 동적 인터페이스 중 하나로 구성되며 WLC의 WLAN에 매핑되지 않습니다.WLC의 WLAN은 관리 VLAN(즉, VLAN 61)에 매핑됩니다

.



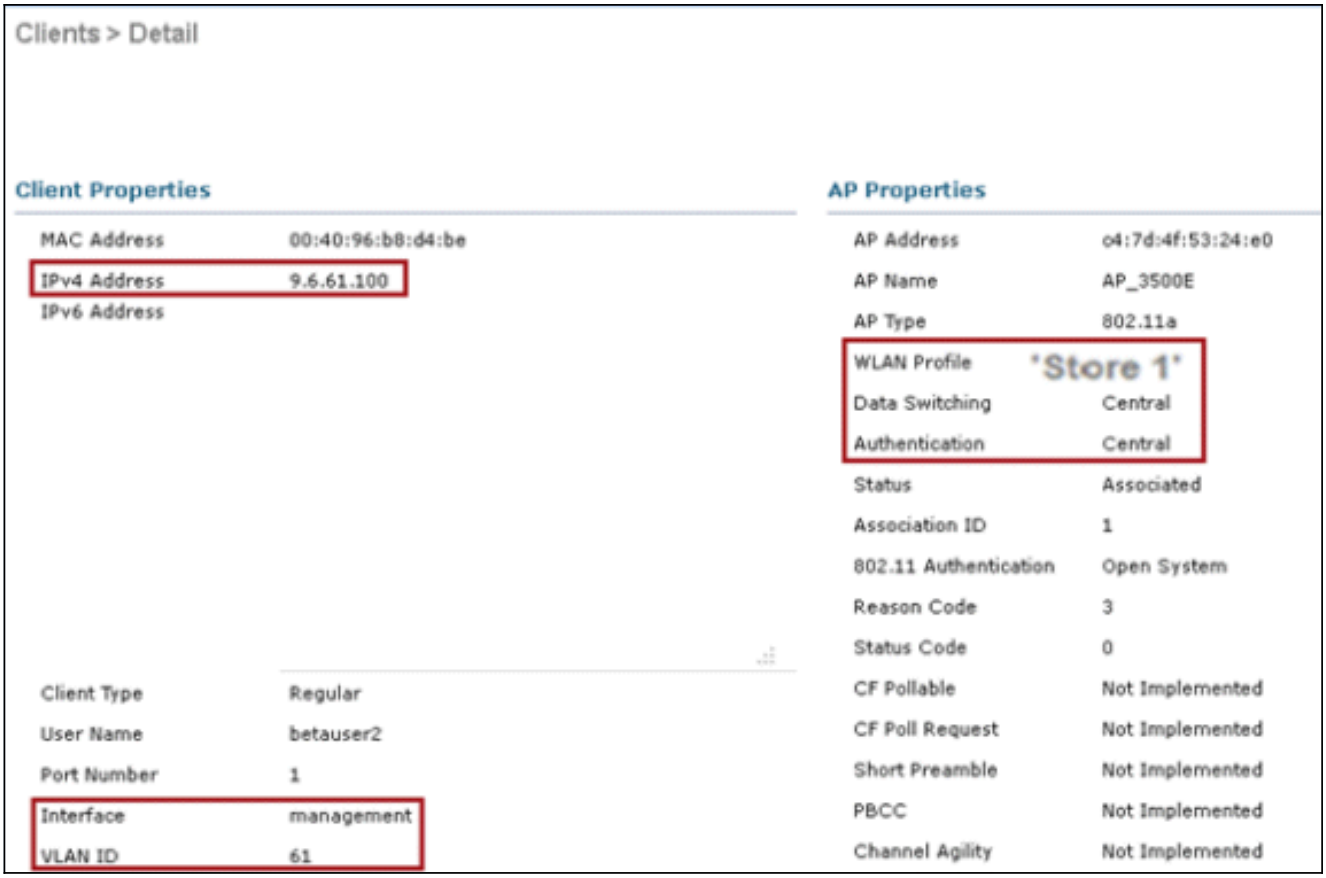
6. 클라이언트를 이 Flex AP의 1단계에서 구성된 WLAN에 연결하고 AAA 서버에서 VLAN 62를 반환합니다.VLAN 62는 이 Flex AP에 없지만 동적 인터페이스로 WLC에 있으므로 트래픽이 중앙에서 전환되고 클라이언트는 WLC에 VLAN 62를 할당합니다.여기서 캡처된 출력에서 클라이언트는 VLAN 62를 할당했으며 데이터 스위칭 및 인증은 **Central**으로 설정됩니다

.



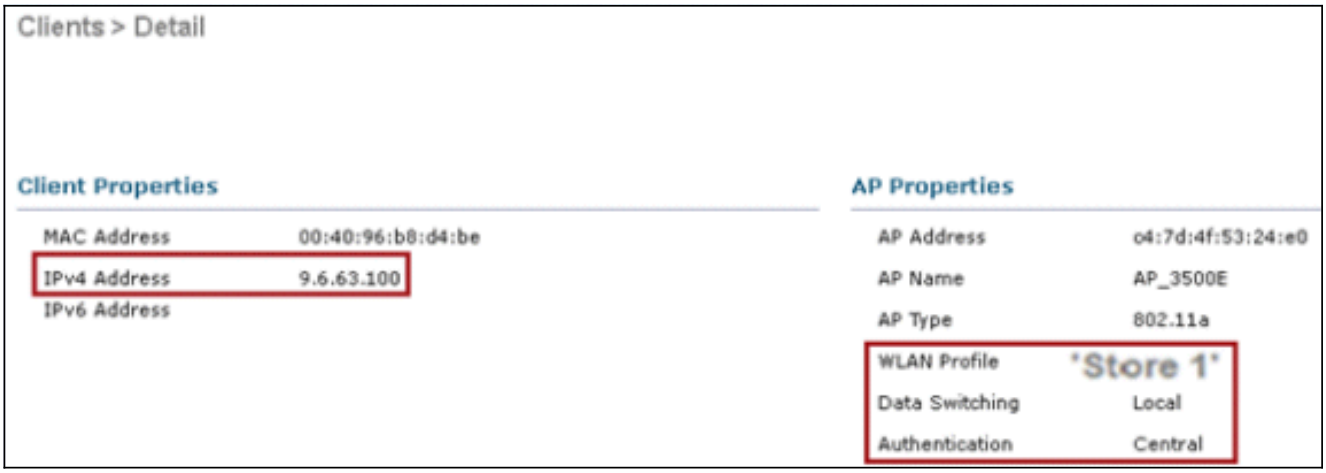
참고: WLAN이 로컬 스위칭에 대해 구성되었지만 VLAN이 있는 경우(즉, AAA 서버에서 반환되는 VLAN 62가 AP 데이터베이스에 없는 경우)에 따라 이 클라이언트의 데이터 스위칭 필드가 중앙 필드임을 확인합니다.

7. 다른 사용자가 이 생성된 WLAN의 동일한 AP에 연결되고 AP와 WLC에 없는 AAA 서버에서 일부 VLAN이 반환되면 트래픽이 중앙에서 전환되고 WLC의 WLAN 매핑 인터페이스(즉, 이 예시 설정의 VLAN 61)가 클라이언트에 할당됩니다. WLAN이 VLAN 61에 대해 구성된 관리 인터페이스에 매핑되기 때문입니다



참고: WLAN이 로컬 스위칭에 대해 구성되었지만 VLAN이 있는 경우 이 클라이언트의 Data Switching 필드가 Central임을 확인합니다.즉, AAA 서버에서 반환되는 VLAN 61은 AP 데이터베이스에 없지만 WLC 데이터베이스에는 없습니다.따라서 클라이언트에는 WLAN에 매핑된 기본 인터페이스 VLAN/인터페이스가 할당됩니다.이 예에서는 WLAN이 관리 인터페이스(즉, VLAN 61)에 매핑되므로 클라이언트가 VLAN 61에서 IP 주소를 수신했습니다.

8. 이 생성된 WLAN에서 다른 사용자가 이 WLAN에 연결하고 VLAN 63이 AAA 서버(이 Flex AP에 있음)에서 반환되면 클라이언트에 VLAN 63이 할당되고 트래픽은 로컬로 전환됩니다
.

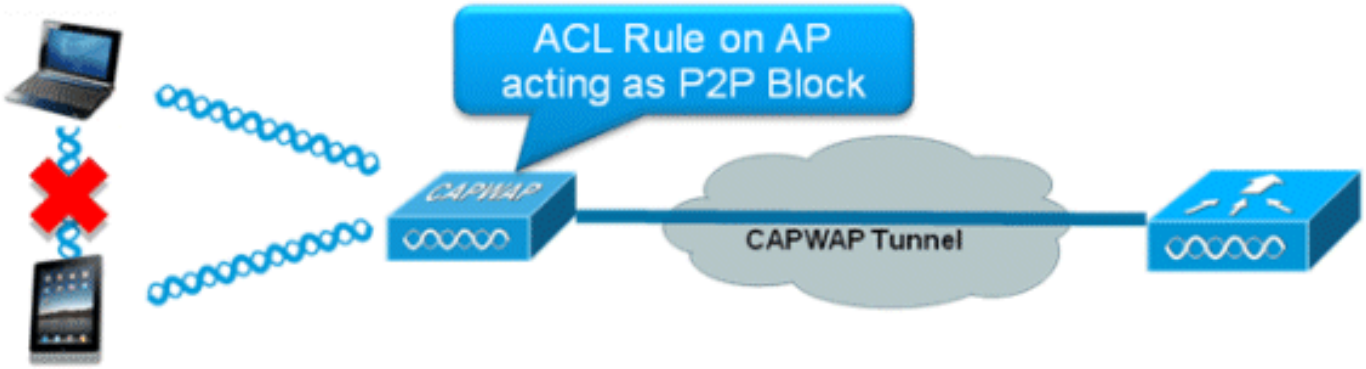


제한 사항

- VLAN 기반 중앙 스위칭은 중앙 인증 및 로컬 스위칭을 위해 구성된 WLAN에서만 지원됩니다.
- AP 하위 인터페이스(즉, VLAN 매핑)는 FlexConnect AP에서 구성해야 합니다.

FlexConnect ACL

FlexConnect에 ACL이 도입됨에 따라 FlexConnect AP에서 액세스 제어의 필요성을 충족시키는 메커니즘이 있어 AP에서 로컬로 스위칭된 데이터 트래픽을 보호하고 무결성을 보장합니다 .FlexConnect ACL은 WLC에서 생성되며, AAA 재정의 VLAN에 사용할 VLAN-ACL 매핑을 사용하여 FlexConnect AP 또는 FlexConnect 그룹에 있는 VLAN으로 구성해야 합니다.그런 다음 AP로 푸시됩니다.



요약

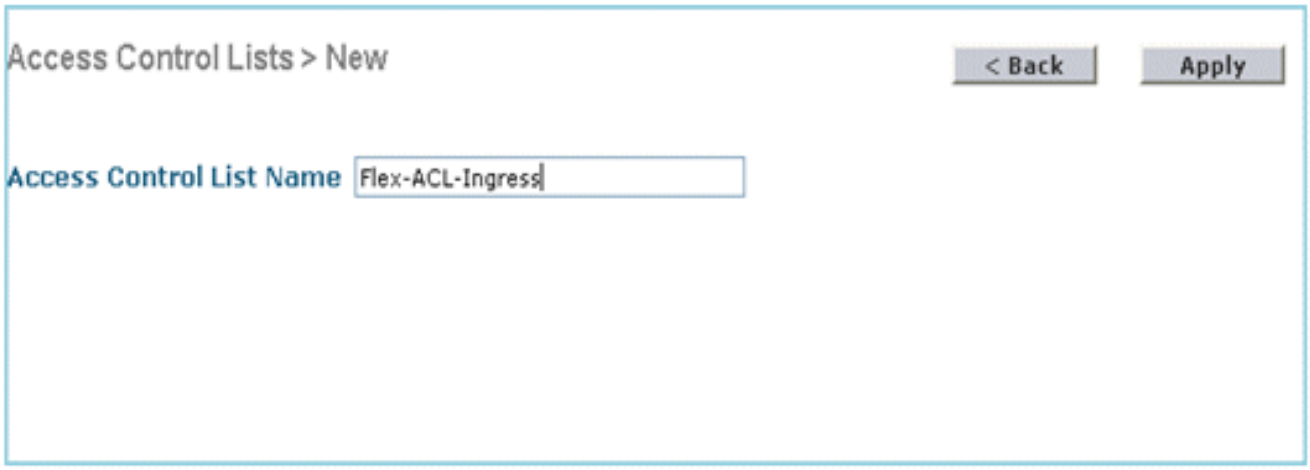
- 컨트롤러에서 FlexConnect ACL을 생성합니다.
- AP 레벨 VLAN ACL 매핑 아래의 FlexConnect AP에 있는 VLAN에도 동일하게 적용합니다.
- VLAN-ACL 매핑(일반적으로 AAA 재정의된 VLAN에 대해 수행)에서 FlexConnect 그룹에 있는 VLAN에 적용할 수 있습니다.
- VLAN에 ACL을 적용하는 동안 적용할 방향을 "인그레스", "이그레스" 또는 "인그레스 및 이그레스"로 선택합니다.

절차

다음 단계를 완료하십시오.

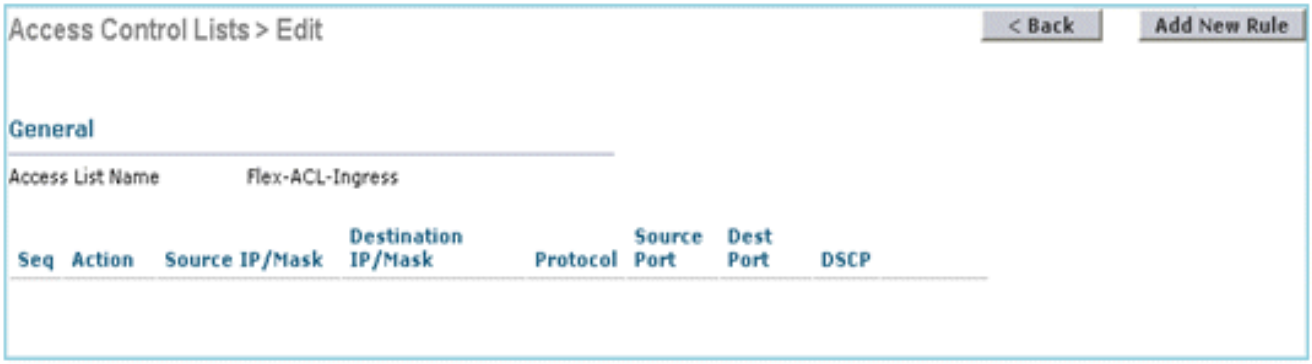
1. WLC에서 FlexConnect ACL을 생성합니다.WLC **GUI > Security > Access Control List > FlexConnect ACLs로 이동합니다**
   .

2. New(**새로 만들기)를 클릭합니다**.
3. ACL 이름을 구성합니다
   .



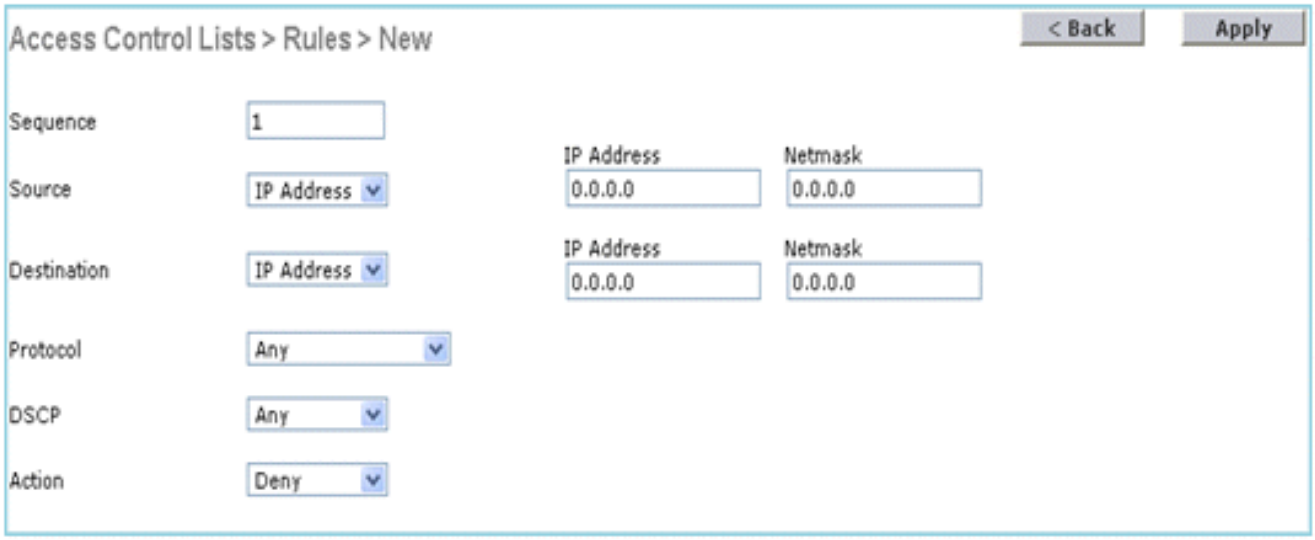
4. Apply를 **클릭합니다**.
5. 각 ACL에 대한 규칙을 생성합니다.규칙을 생성하려면 WLC **GUI > Security > Access Control List > FlexConnect ACLs로** 이동하고 위에서 생성한 ACL을 클릭합니다

.



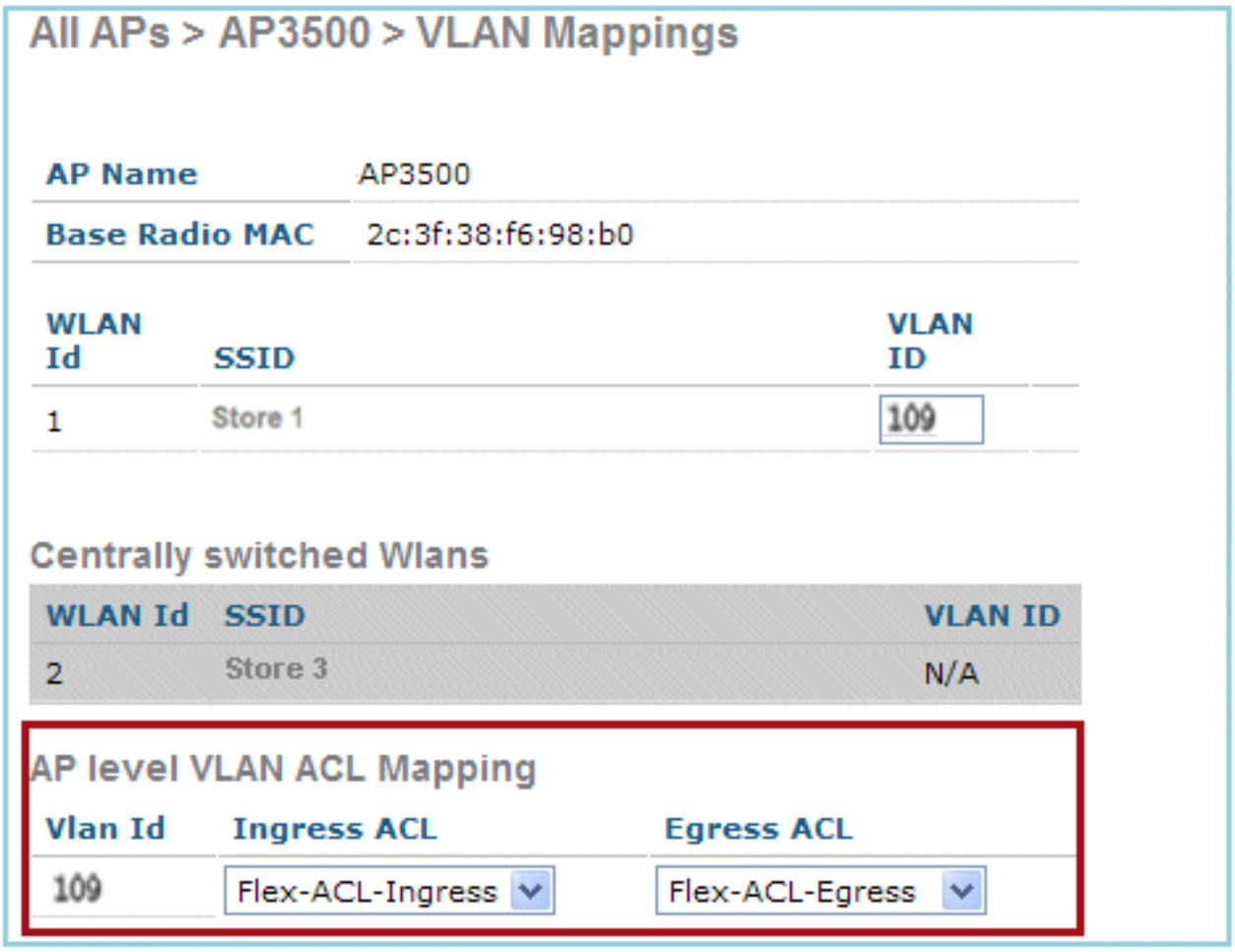
6. Add **New Rule을 클릭합니다**

.

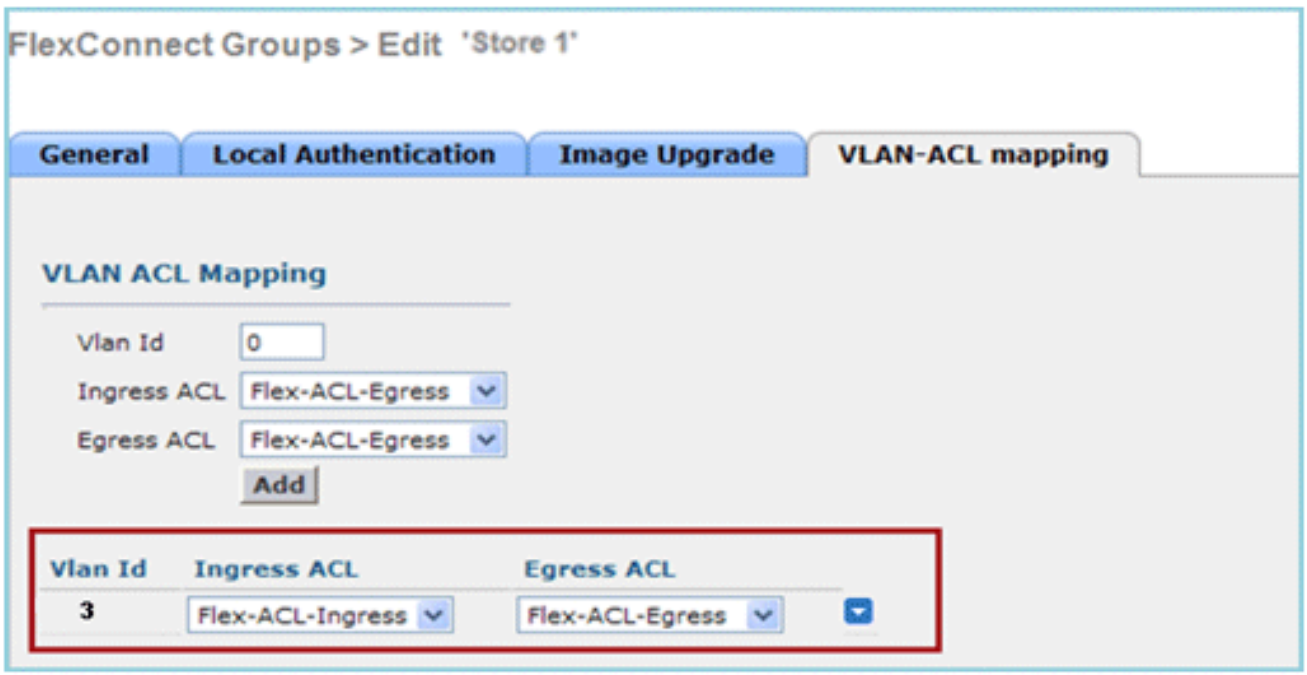


참고: 요구 사항에 따라 규칙을 구성합니다.permit any 규칙이 마지막에 구성되지 않은 경우 모든 트래픽을 차단하는 암시적 거부가 있습니다.

7. FlexConnect ACL이 생성되면 개별 FlexConnect AP에서 WLAN-VLAN 매핑에 대해 매핑하거나 FlexConnect 그룹의 VLAN-ACL 매핑에 적용할 수 있습니다.
8. 개별 FlexConnect AP에 대한 VLAN 매핑에서 개별 VLAN에 대해 AP 레벨에서 구성된 FlexConnect ACL을 매핑합니다.WLC **GUI > Wireless > All AP** > 특정 AP > **FlexConnect** 탭 > **VLAN Mapping**을 클릭합니다



9. FlexConnect ACL은 FlexConnect 그룹의 VLAN-ACL 매핑에도 적용할 수 있습니다 .FlexConnect 그룹의 VLAN-ACL 매핑에서 생성된 VLAN은 주로 동적 VLAN 재정의에 사용됩니다



제한 사항

- WLC에서 최대 512개의 FlexConnect ACL을 구성할 수 있습니다.
- 각 개별 ACL은 64개의 규칙으로 구성할 수 있습니다.

- FlexConnect 그룹당 또는 FlexConnect AP당 최대 32개의 ACL을 매핑할 수 있습니다.
- 지정된 시점에 FlexConnect AP에는 최대 16개의 VLAN과 32개의 ACL이 있습니다.

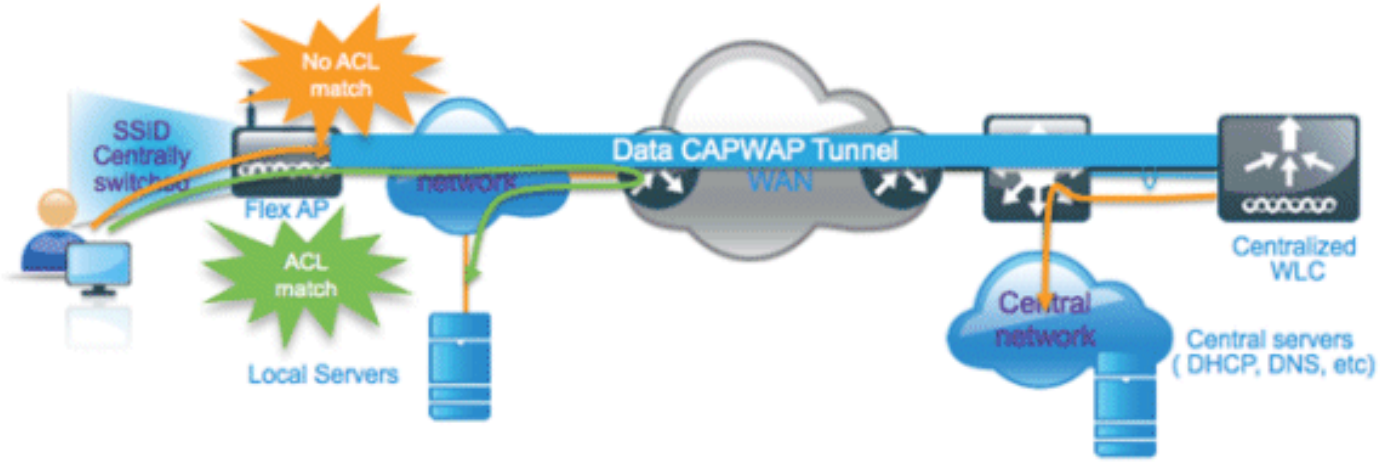
FlexConnect 스플릿 터널링

7.3 이전 WLC 릴리스에서 중앙 스위치드 WLAN과 연결된 FlexConnect AP에 연결하는 클라이언트가 로컬 사이트/네트워크에 있는 장치로 일부 트래픽을 전송해야 하는 경우, CAPWAP를 통해 트래픽을 WLC로 전송한 다음 동일한 트래픽을 CAPWAP를 통해 로컬 사이트로 다시 전송하거나 일부 오프 밴드 연결을 사용해야 합니다.

릴리스 7.3부터 **Split Tunneling은** 클라이언트에서 보낸 트래픽이 **Flex ACL을 사용하여** 패킷 내용에 따라 분류되는 메커니즘을 **도입합니다**.일치하는 패킷은 Flex AP에서 로컬로 스위칭되고 나머지 패킷은 CAPWAP를 통해 중앙에서 전환됩니다.

스플릿 터널링 기능은 CAPWAP를 통해 패킷을 전송함으로써 WAN 대역폭을 사용하지 않고 기업 SSID의 클라이언트가 로컬 네트워크의 디바이스(프린터, 원격 LAN 포트의 유선 머신 또는 개인 SSID의 무선 디바이스)와 직접 통신할 수 있는 OEAP AP 설정에 추가된 장점입니다.스플릿 터널링은 OEAP 600 AP에서 지원되지 않습니다.로컬 사이트/네트워크에 있는 모든 디바이스를 허용하기 위해 규칙을 사용하여 Flex ACL을 생성할 수 있습니다.회사 SSID의 무선 클라이언트의 패킷이 OEAP AP에 구성된 Flex ACL의 규칙과 일치하면 해당 트래픽은 로컬로 스위칭되고 나머지 트래픽(즉, 암시적 거부 트래픽)은 CAPWAP를 통해 중앙에서 전환됩니다.

스플릿 터널링 솔루션은 중앙 사이트의 클라이언트와 연결된 서브넷/VLAN이 로컬 사이트에 없다고 가정합니다(즉, 중앙 사이트에 있는 서브넷에서 IP 주소를 수신하는 클라이언트의 트래픽은 로컬로 전환할 수 없습니다). 스플릿 터널링 기능은 WAN 대역폭 소비를 방지하기 위해 로컬 사이트에 속하는 서브넷에 대해 로컬로 트래픽을 전환하도록 설계되었습니다.Flex ACL 규칙과 일치하는 트래픽은 로컬로 스위칭되며, NAT 작업은 클라이언트의 소스 IP 주소를 로컬 사이트/네트워크에서 라우팅 가능한 Flex AP의 BVI 인터페이스 IP 주소로 변경합니다.



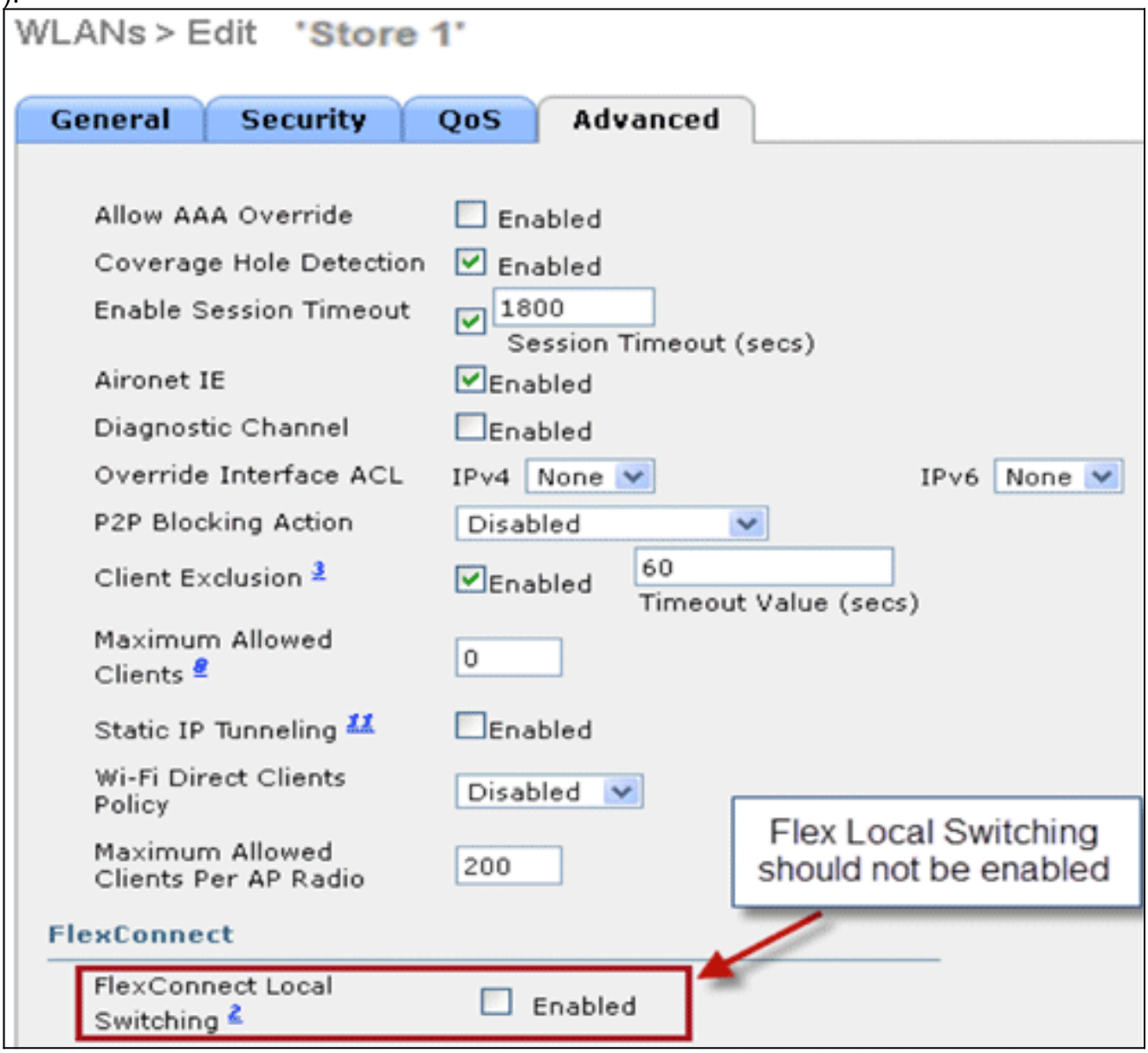
요약

- 스플릿 터널링 기능은 Flex AP에서만 광고되는 중앙 스위칭에 대해 구성된 WLAN에서 지원됩니다.
- 스플릿 터널링에 대해 구성된 WLAN에서 필요한 DHCP를 활성화해야 합니다.
- 스플릿 터널링 컨피그레이션은 Flex AP당 또는 FlexConnect 그룹의 모든 Flex AP에 대해 중앙 스위칭을 위해 구성된 WLAN당 적용됩니다.

절차

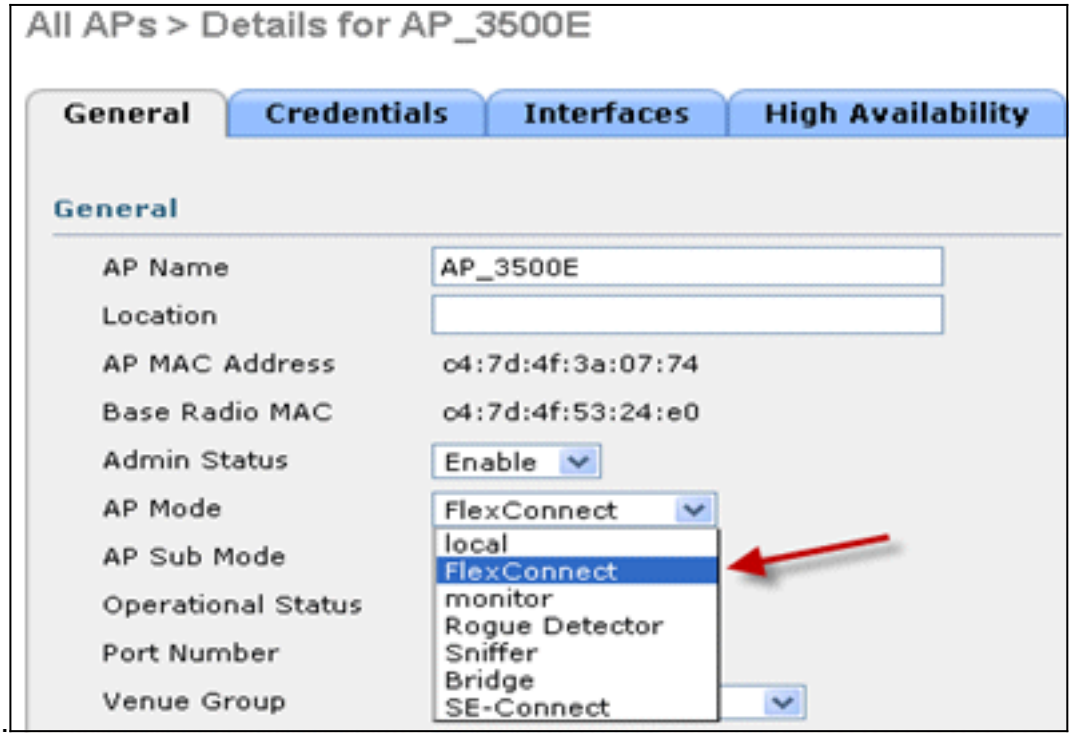
다음 단계를 완료하십시오.

1. 중앙 스위칭을 위한 WLAN을 구성합니다(즉, **Flex Local Switching**을 활성화하지 않아야 함).



2. DHCP Address Assignment(DHCP 주소 할당)를 **Required(필수)로 설정합니다**.

3. AP 모드를 FlexConnect로 **설정합니다**



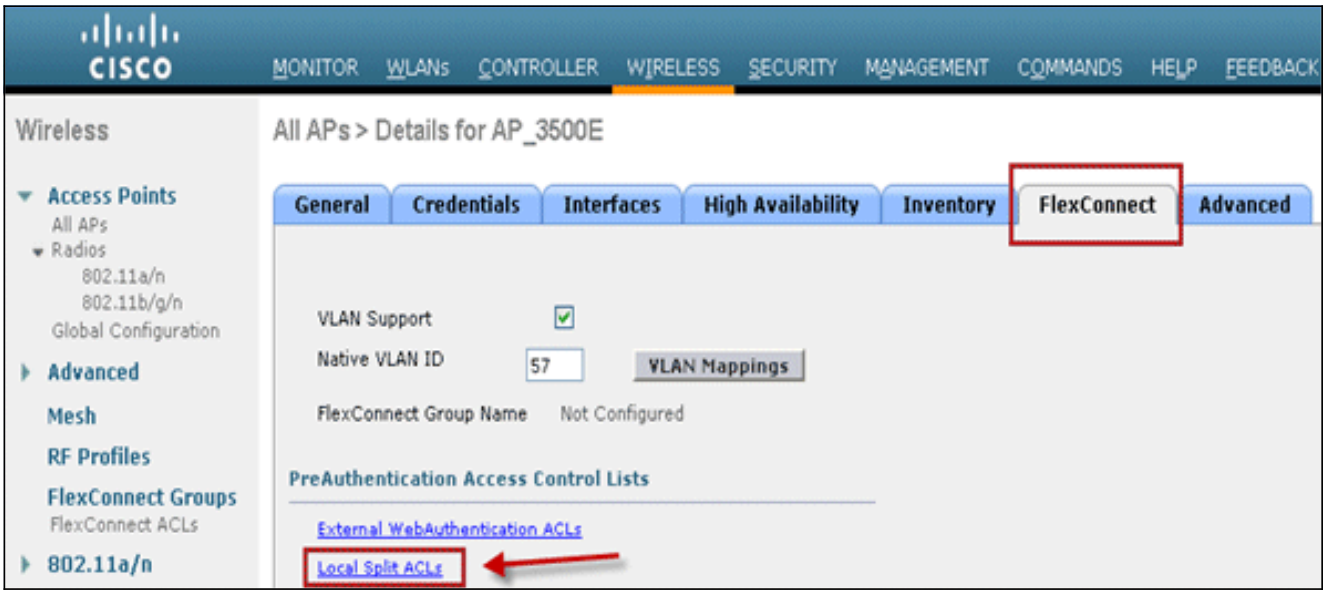
.

4. 중앙 스위치 WLAN에서 로컬로 전환해야 하는 트래픽에 대한 허용 규칙으로 FlexConnect ACL을 구성합니다.이 예에서 FlexConnect ACL 규칙은 Flex AP에 NAT 작업이 적용된 후 9.6.61.0 서브넷에 있는 모든 클라이언트(즉, 중앙 사이트에 있음)에서 로컬로 스위칭되도록 ICMP 트래픽을 9.1.0.150에 알리도록 구성됩니다.나머지 트래픽은 암시적 거부 규칙에 도달하고 CAPWAP를 통해 중앙에서 전환됩니다

.

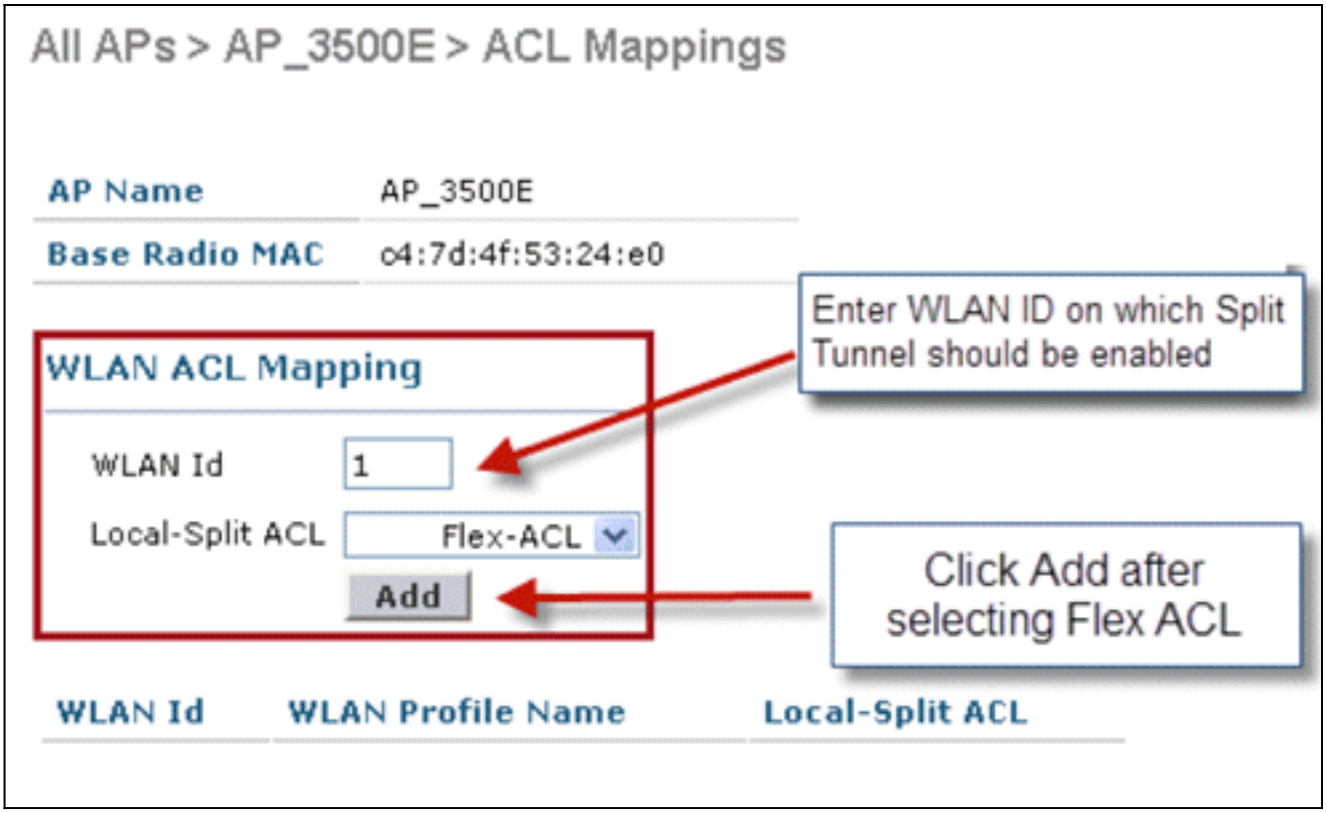
5. 이렇게 생성된 FlexConnect ACL은 개별 Flex AP에 스플릿 터널 ACL로 푸시하거나 Flex Connect 그룹의 모든 Flex AP에 푸시될 수도 있습니다.Flex ACL을 로컬 분할 ACL로 개별 Flex AP에 푸시하려면 다음 단계를 완료하십시오.Local **Split ACLs를 클릭합니다**

.

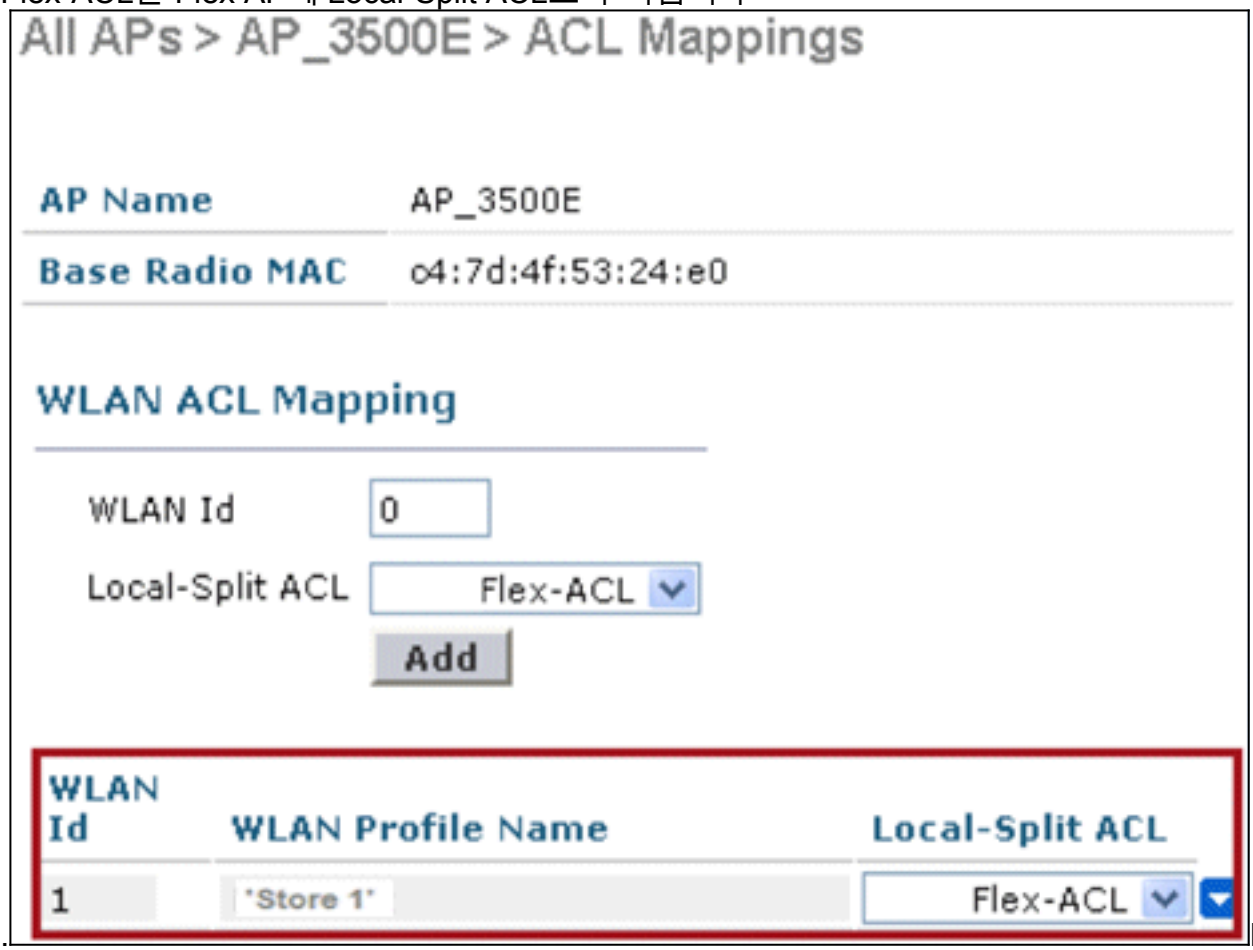


스플릿 터널 기능을 활성화해야 하는 **WLAN Id**를 선택하고 **Flex-ACL**을 선택한 다음 **Add**를 클릭합니다

.



Flex-ACL은 Flex AP에 Local-Split ACL로 푸시됩니다

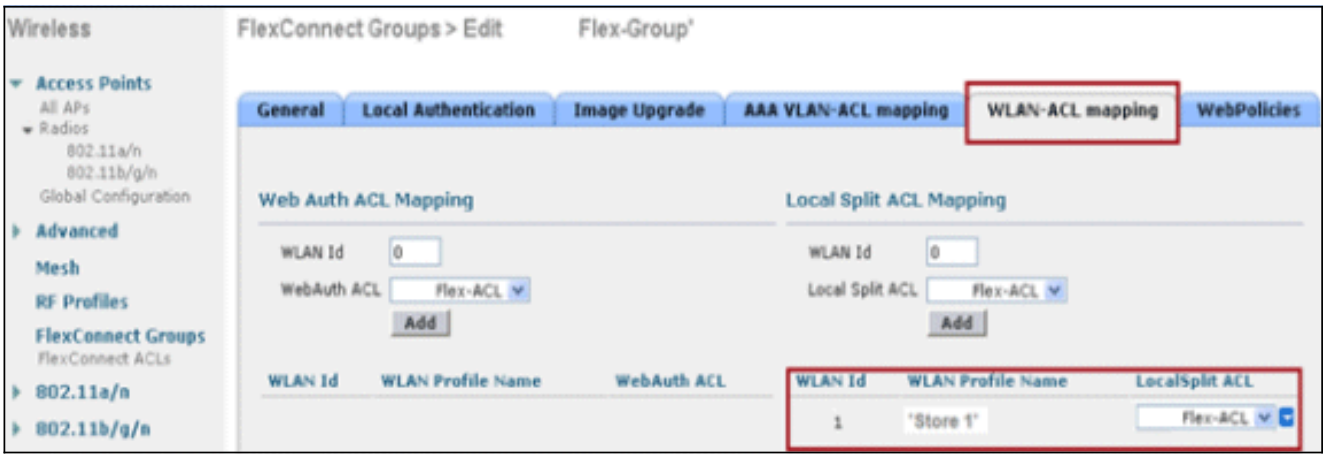


. Flex ACL을 FlexConnect 그룹에 로컬 스플릿 ACL로 푸시하려면 다음 단계를 완료하십시오.스플릿 터널링 기능을 활성화해야 하는 WLAN Id를 선택합니다.**WLAN-ACL 매핑** 탭의 FlexConnect 그룹에서 특정 Flex AP가 추가된 FlexConnect ACL을 선택하고 Add(**추가**)를 클릭합니다

.

Flex-ACL은 해당 Flex 그룹의 Flex AP에 LocalSplit ACL로 푸시됩니다

.



제한 사항

- Flex ACL 규칙은 소스 및 대상과 동일한 서브넷을 사용하여 permit/deny 문을 구성하지 않아야 합니다.
- 스플릿 터널링에 대해 구성된 중앙 스위치 WLAN의 트래픽은 무선 클라이언트가 로컬 사이트에 있는 호스트에 대한 트래픽을 시작할 경우에만 로컬로 스위칭할 수 있습니다.구성된 WLAN의 무선 클라이언트에 대해 로컬 사이트의 클라이언트/호스트에서 트래픽을 시작할 경우 대상에 도달할 수 없습니다.
- 멀티캐스트/브로드캐스트 트래픽에는 스플릿 터널링이 지원되지 않습니다.멀티캐스트/브로드캐스트 트래픽은 Flex ACL과 일치하더라도 중앙에서 전환됩니다.

내결함성

FlexConnect 내결함성은 다음과 같은 경우에 지사 클라이언트에 무선 액세스 및 서비스를 허용합니다.

- FlexConnect 브랜치 AP는 기본 Flex 7500 컨트롤러와의 연결이 끊깁니다.
- FlexConnect 브랜치 AP가 보조 Flex 7500 컨트롤러로 전환되고 있습니다.
- FlexConnect Branch AP가 기본 Flex 7500 컨트롤러에 대한 연결을 다시 설정하고 있습니다.

FlexConnect Fault Tolerance(내결함성)는 위에서 설명한 로컬 EAP와 함께 네트워크 중단 중에 지사 다운타임을 전혀 제공하지 않습니다.이 기능은 기본적으로 활성화되어 있으며 비활성화할 수 없습니다.컨트롤러 또는 AP에 컨피그레이션이 필요하지 않습니다.그러나 내결함성이 원활하고 적용되도록 하려면 다음 기준을 유지해야 합니다.

- WLAN 주문 및 구성은 기본 및 백업 Flex 7500 컨트롤러 전체에서 동일해야 합니다.

- VLAN 매핑은 기본 및 백업 Flex 7500 컨트롤러 전체에서 동일해야 합니다.
- 모빌리티 도메인 이름은 기본 및 백업 Flex 7500 컨트롤러 전체에서 동일해야 합니다.
- 기본 컨트롤러와 백업 컨트롤러 모두 Flex 7500을 사용하는 것이 좋습니다.

요약

- 컨트롤러에서 컨피그레이션이 변경되지 않는 경우 AP가 동일한 컨트롤러에 다시 연결되면 FlexConnect에서 클라이언트의 연결을 끊지 않습니다.
- 컨피그레이션이 변경되지 않고 백업 컨트롤러가 기본 컨트롤러와 동일한 경우 FlexConnect는 백업 컨트롤러에 연결할 때 클라이언트의 연결을 끊지 않습니다.
- 컨트롤러에서 컨피그레이션이 변경되지 않는 경우 FlexConnect는 기본 컨트롤러에 다시 연결할 때 무선 장치를 재설정하지 않습니다.

제한 사항

- 로컬 스위칭이 있는 중앙/로컬 인증을 사용하는 FlexConnect에만 지원됩니다.
- 중앙에서 인증된 클라이언트는 FlexConnect AP가 독립형 모드에서 연결 모드로 전환되기 전에 클라이언트 세션 타이머가 만료되면 전체 재인증이 필요합니다.
- Flex 7500 기본 컨트롤러와 백업 컨트롤러는 동일한 모빌리티 도메인에 있어야 합니다.

WLAN당 클라이언트 제한

트래픽 세그먼테이션과 함께 무선 서비스에 액세스하는 전체 클라이언트를 제한할 필요가 발생합니다.

예:브랜치 터널링에서 데이터 센터로 총 게스트 클라이언트 제한

이 문제를 해결하기 위해 Cisco는 WLAN당 허용되는 총 클라이언트를 제한할 수 있는 WLAN당 클라이언트 제한을 도입합니다.

기본 목표

- 최대 클라이언트에 대한 제한 설정
- 운영 용이성

참고: 이는 QoS의 형식이 아닙니다.

기본적으로 이 기능은 비활성화되어 있으며 제한을 강제하지 않습니다.

제한 사항

이 기능은 FlexConnect가 독립형 작업 상태일 때 클라이언트 제한을 적용하지 않습니다.

WLC 컨피그레이션

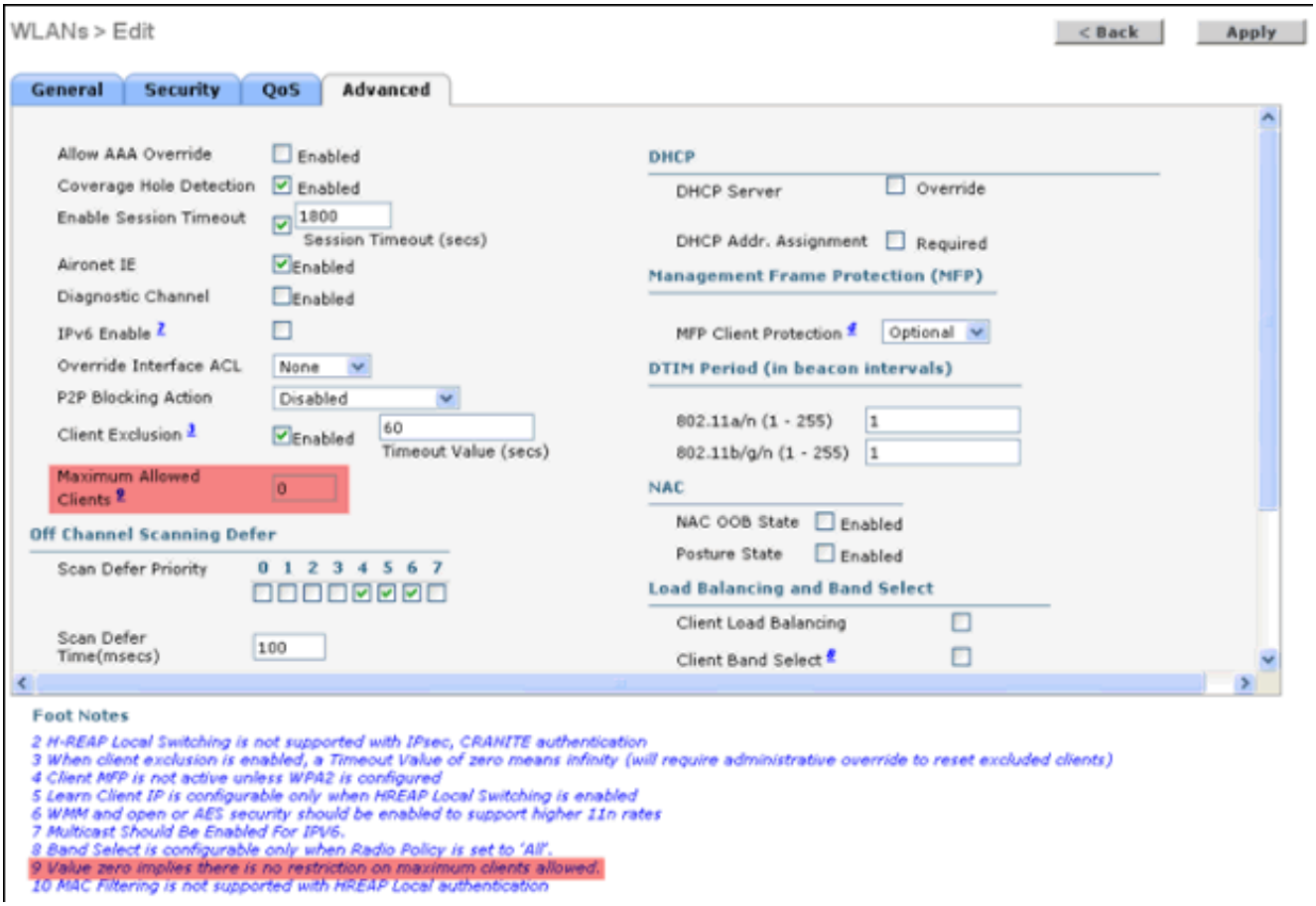
다음 단계를 완료하십시오.

1. Centralized Switched WLAN ID 1 with SSID **DataCenter를 선택합니다**.이 WLAN은 AP 그룹

생성 중에 생성되었습니다.그림 8을 참조하십시오.

2. WLAN ID 1의 **Advanced**(고급) 탭을 클릭합니다.
3. Maximum Allowed Clients 텍스트 필드에 대한 클라이언트 제한 값을 설정합니다.
4. Maximum Allowed Clients에 대한 텍스트 필드가 설정된 후 Apply를 클릭합니다

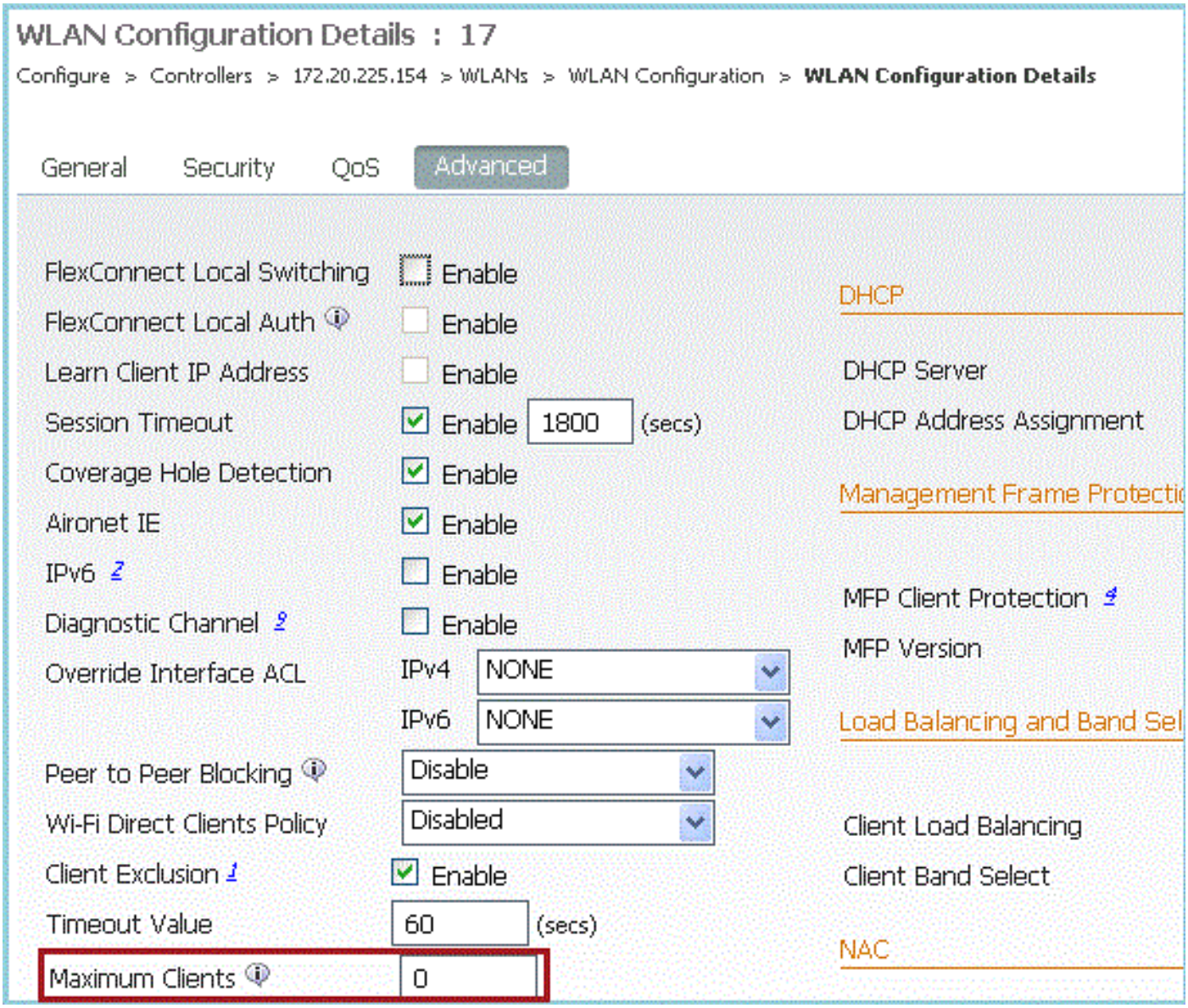
.



Maximum Allowed Clients(최대 허용 클라이언트)의 기본값은 0으로 설정되어 있으며, 이는 제한이 없고 기능이 비활성화되었음을 의미합니다.

NCS 컨피그레이션

NCS에서 이 기능을 활성화하려면 Configure(구성) > Controllers(컨트롤러) > **Controller IP(컨트롤러 IP) > WLANs(WLAN) > WLAN Configuration(WLAN 컨피그레이션) > WLAN Configuration Details(WLAN 컨피그레이션 세부사항)로** 이동합니다.

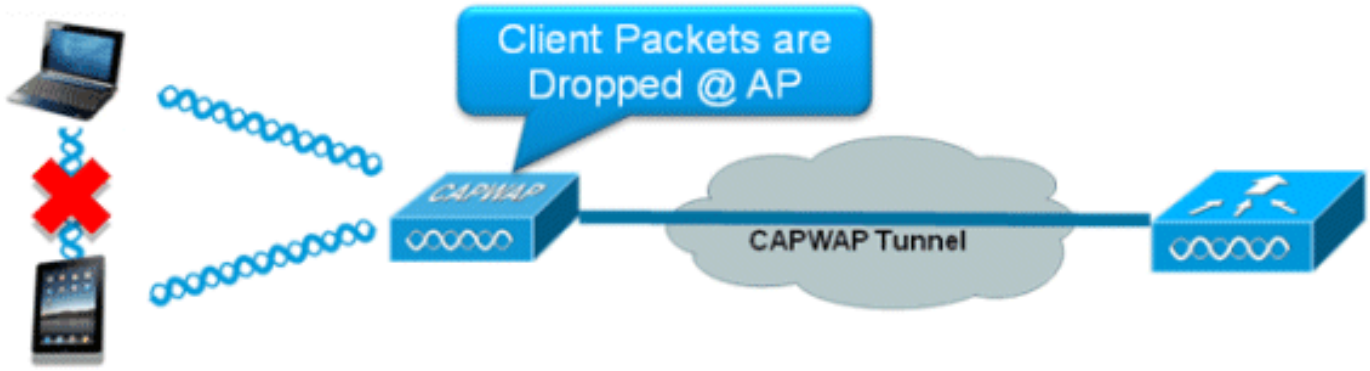


P2P 차단

7.2 이전 컨트롤러 소프트웨어 릴리스에서는 중앙 스위칭 WLAN에 대해서만 P2P(peer-to-peer) 차단이 지원되었습니다.다음 세 가지 작업 중 하나로 WLAN에서 P2P 차단을 구성할 수 있습니다.

- **Disabled**(비활성화됨) - 동일한 서브넷에 있는 클라이언트에 대해 컨트롤러 내에서 피어 투 피어 차단 및 로컬로 연결된 트래픽을 비활성화합니다.이것이 기본값입니다.
- **Drop**(삭제) - 컨트롤러가 동일한 서브넷에 있는 클라이언트에 대한 패킷을 삭제하도록 합니다.
- **Forward Up-Stream** - 패킷이 업스트림 VLAN에 전달되도록 합니다.컨트롤러 위의 디바이스는 패킷과 관련하여 수행할 작업을 결정합니다.

릴리스 7.2부터는 로컬 스위칭 WLAN에 연결된 클라이언트에 대해 P2P 차단이 지원됩니다.WLAN에 따라 컨트롤러에서 FlexConnect AP로 피어 투 피어 컨피그레이션이 푸시됩니다.



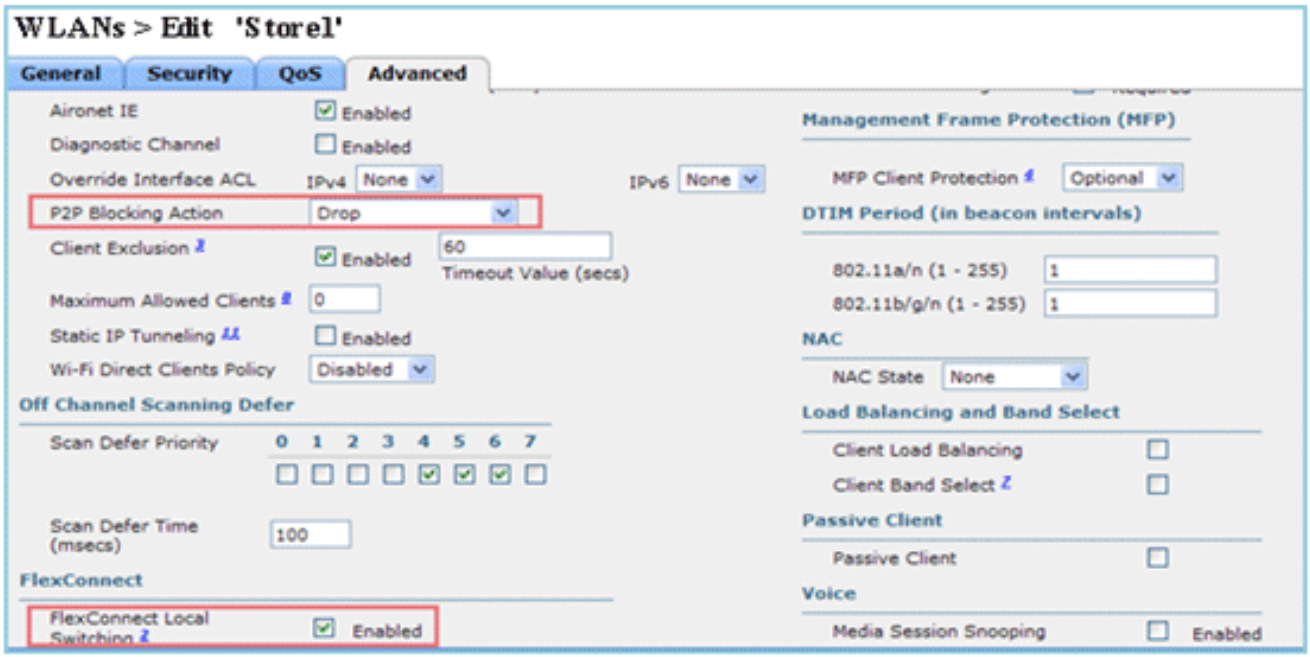
요약

- WLAN당 P2P 차단 구성
- WLAN에 따라 WLC에서 FlexConnect AP로 피어 투 피어 차단 컨피그레이션이 푸시됩니다.
- WLAN에서 drop 또는 upstream-forward로 구성된 P2P 차단 작업은 FlexConnect AP에서 활성화된 P2P 차단으로 처리됩니다.

절차

다음 단계를 완료하십시오.

1. FlexConnect 로컬 스위칭을 위해 구성된 WLAN에서 **Drop**으로 peer-to-peer blocking 작업을 활성화합니다
   .



2. 로컬 스위칭용으로 구성된 WLAN에서 P2P 차단 작업이 **Drop** 또는 **Forward-Upstream**으로 구성되면 WLC에서 FlexConnect AP로 푸시됩니다.FlexConnect AP는 이 정보를 플래시에 Reap 구성 파일에 저장합니다.이를 통해 FlexConnect AP가 독립형 모드인 경우에도 해당 하위 인터페이스에 P2P 컨피그레이션을 적용할 수 있습니다.

제한 사항

- FlexConnect에서 솔루션 P2P 차단 컨피그레이션은 특정 FlexConnect AP 또는 하위 AP 집합에만 적용할 수 없습니다.SSID를 브로드캐스트하는 모든 FlexConnect AP에 적용됩니다.
- 중앙 스위칭 클라이언트를 위한 통합 솔루션은 P2P 업스트림 포워드를 지원합니다.그러나 FlexConnect 솔루션에서는 지원되지 않습니다.이는 P2P 삭제로 처리되며 클라이언트 패킷은 다음 네트워크 노드로 전달되는 대신 삭제됩니다.
- 중앙 스위칭 클라이언트를 위한 통합 솔루션은 서로 다른 AP에 연결된 클라이언트에 대해 P2P 차단을 지원합니다.그러나 이 솔루션은 동일한 AP에 연결된 클라이언트만 대상으로 합니다 .FlexConnect ACL을 이 제한 사항의 해결 방법으로 사용할 수 있습니다.

AP 사전 이미지 다운로드

이 기능을 사용하면 AP에서 코드를 다운로드하는 동안 코드를 다운로드할 수 있습니다.AP 사전 이미지 다운로드는 소프트웨어 유지 보수 또는 업그레이드 과정에서 네트워크 다운타임을 줄이는 데 매우 유용합니다.

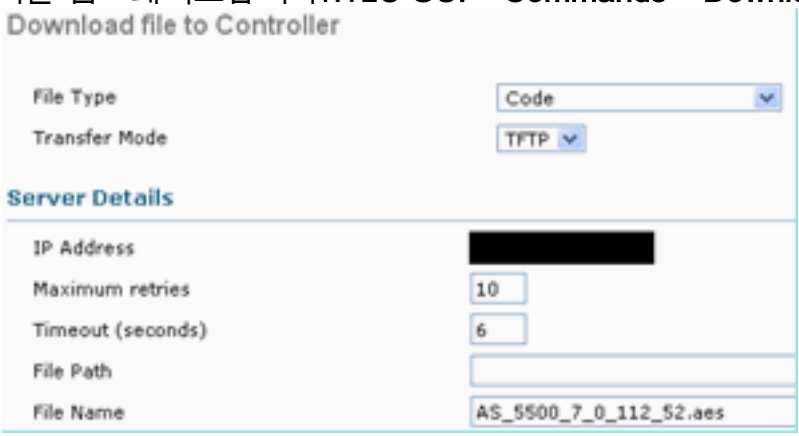
요약

- 소프트웨어 관리의 용이성
- 저장소별 업그레이드 예약:이를 위해서는 NCS가 필요합니다.
- 다운타임 감소

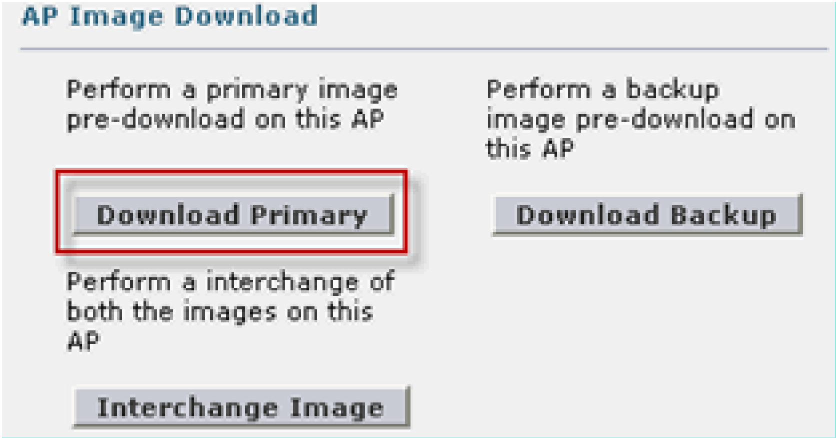
절차

다음 단계를 완료하십시오.

1. 기본 및 백업 컨트롤러에서 이미지를 업그레이드합니다.WLC **GUI > Commands > Download File**에서 다운로드를 시작합니다.



2. 컨트롤러에서 컨피그레이션을 저장하되 컨트롤러를 재부팅하지 마십시오.
3. 기본 컨트롤러에서 AP 사전 이미지 다운로드 명령을 실행합니다.WLC **GUI > Wireless > Access Points > All APs로 이동하고** 사전 이미지 다운로드를 시작할 액세스 포인트를 선택합니다.액세스 포인트를 선택한 후 **고급** 탭을 클릭합니다.Download **Primary(기본 다운로드)**를 클릭하여 이미지 이전 다운로드를 시작합니다




```
*Sep [redacted] 903: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
Image [redacted] not found in flash, predownloading.
examining image...!
extracting info (326 bytes)
Image info:
    Version Suffix: k9w8-.wnbu_j_mr.201009101910
    Image Name: c1250-k9w8-mx.wnbu_j_mr.201009101910
    Version Directory: c1250-k9w8-mx.wnbu_j_mr.201009101910
    Ios Image Size: 5530112
    Total Image Size: 5550592
    Image Feature: WIRELESS LAN|LWAPP
    Image Family: C1250
    Wireless Switch Management Version: [redacted]
Extracting files...
c1250-k9w8-mx.wnbu_j_mr.201009101910/ (directory) 0 (bytes)
extracting c1250-k9w8-mx.wnbu_j_mr.201009101910/c1250_avr_1.img (13696 bytes)!
extracting c1250-k9w8-mx.wnbu_j_mr.201009101910/W5.bin (17372 bytes)!
extracting c1250-k9w8-mx.wnbu_j_mr.201009101910/c1250-k9w8-mx.wnbu_j_mr.20100910
1910 (5322509 bytes)!!!!!!
*Sep 13 21:25:43.747: Loading file /c1250-pre[redacted]..
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
extracting c1250-k9w8-mx.wnbu_j_mr.201009101910/8001.img (172792 bytes)!!!!!!!!!
!!!!
extracting c1250-k9w8-mx.wnbu_j_mr.201009101910/W2.bin (4848 bytes)!
extracting c1250-k9w8-mx.wnbu_j_mr.201009101910/info (326 bytes)
extracting c1250-k9w8-mx.wnbu_j_mr.201009101910/c1250_avr_2.img (10880 bytes)!
extracting info.ver (326 bytes)
New software image installed in flash:/c1250-k9w8-mx.wnbu_j_mr.201009101910
archive download: takes 138 seconds

New backup software image installed in flash:/c1250-k9w8-mx.wnbu_j_mr.2010091019
10/c1250-k9w8-mx.wnbu_j_mr.201009101910
Reading backup version from flash:/c1250-k9w8-mx.wnbu_j_mr.201009101910/c1250-k9
w8-mx.wnbu_j_mr.201009101910done.
```

4. 모든 AP 이미지를 다운로드한 후 컨트롤러를 재부팅합니다.이제 컨트롤러가 재부팅될 때까지 AP가 독립형 모드로 돌아갑니다.**참고:** 독립형 모드에서는 내결함성이 클라이언트를 연결합니다.컨트롤러가 돌아오면 AP는 사전 다운로드된 이미지를 사용하여 자동으로 재부팅됩니다.재부팅 후 AP가 기본 컨트롤러에 다시 참가하고 클라이언트 서비스를 재개합니다.

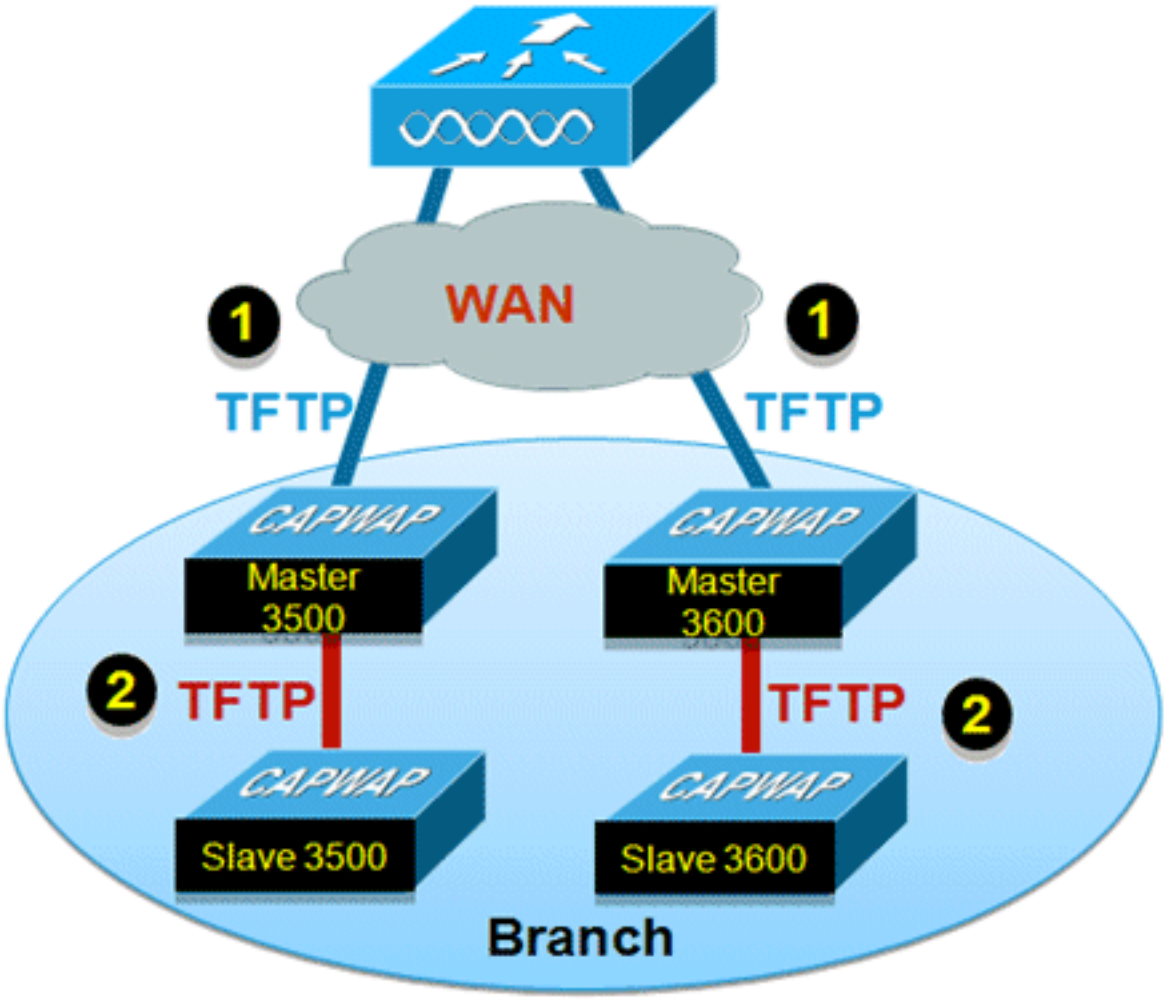
제한 사항

- CAPWAP AP에서만 작동합니다.

FlexConnect Smart AP 이미지 업그레이드

사전 이미지 다운로드 기능은 다운타임 기간을 일정 수준으로 단축하지만, 모든 FlexConnect AP는 레이턴시가 더 높은 WAN 링크를 통해 해당 AP 이미지를 미리 다운로드해야 합니다.

효율적인 AP 이미지 업그레이드로 각 FlexConnect AP의 다운타임을 줄일 수 있습니다.기본 개념은 각 AP 모델의 AP가 컨트롤러에서 이미지를 다운로드하고 마스터/서버 역할을 수행하며, 동일한 모델의 나머지 AP는 슬레이브/클라이언트로 작동하며 마스터에서 AP 이미지를 미리 다운로드합니다.서버에서 클라이언트로의 AP 이미지 분배는 로컬 네트워크에 있으며 WAN 링크의 지연 시간이 발생하지 않습니다.그 결과 프로세스가 더 빨라집니다.



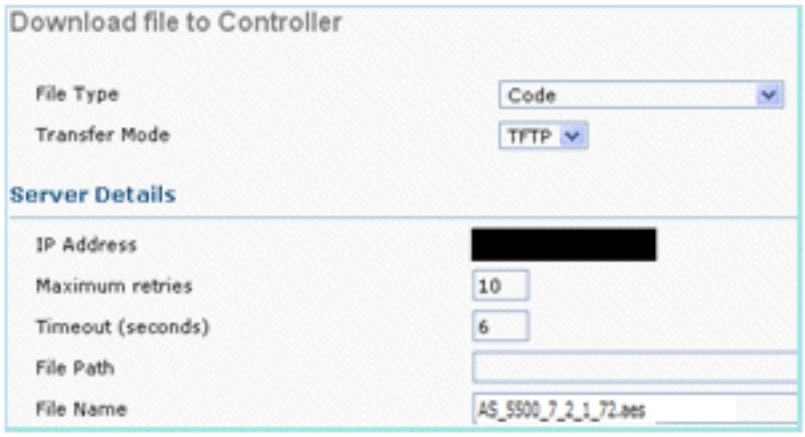
요약

- FlexConnect 그룹당 각 AP 모델에 대해 마스터 및 슬레이브 AP가 선택됩니다.
- 마스터가 WLC에서 이미지 다운로드
- 슬레이브가 마스터 AP에서 이미지 다운로드
- 다운타임 감소 및 WAN 대역폭 절약

절차

다음 단계를 완료하십시오.

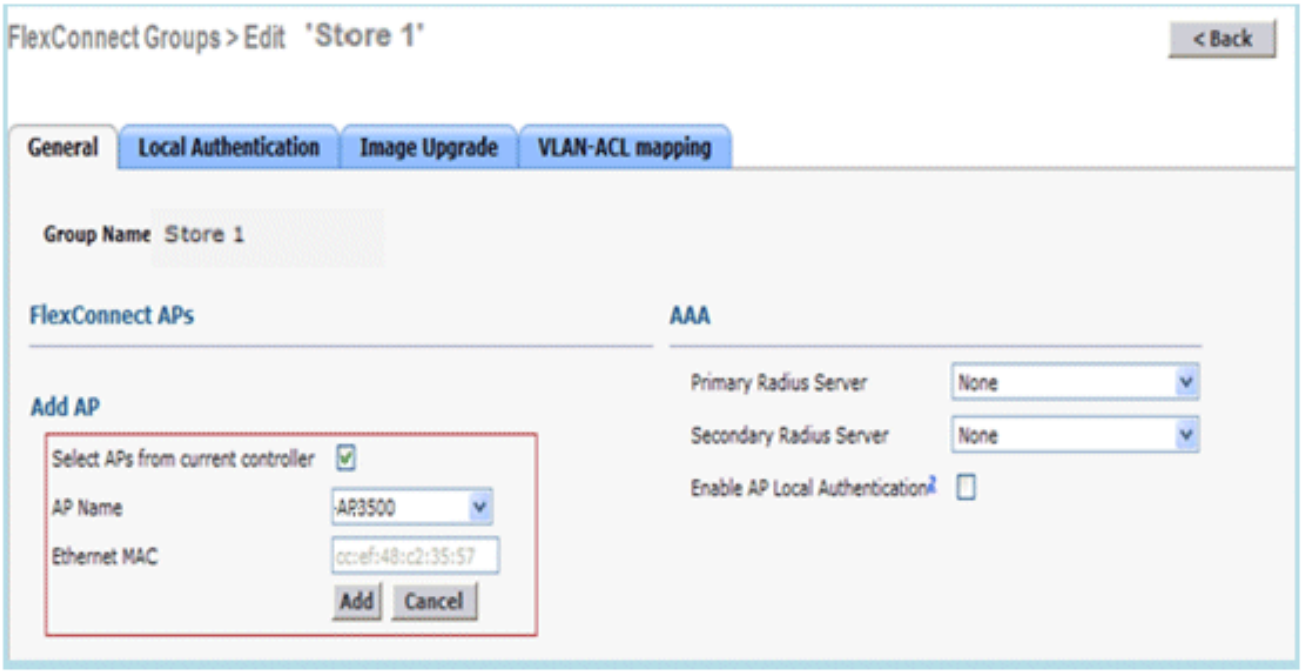
1. 컨트롤러의 이미지를 업그레이드합니다.WLC **GUI > Commands > Download File**로 이동하여



다운로드를 시작합니다.

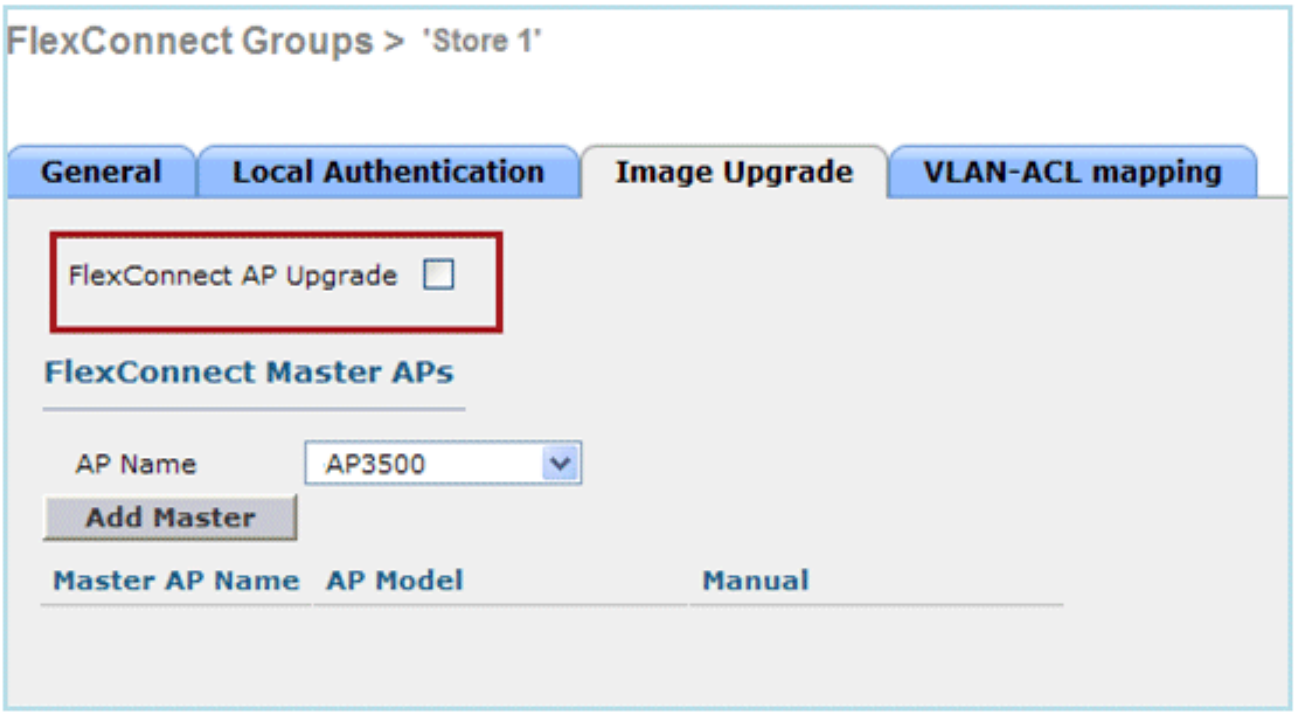
2. 컨트롤러에서 컨피그레이션을 저장하되 컨트롤러를 재부팅하지 마십시오.
3. FlexConnect 그룹에 FlexConnect AP를 추가합니다.WLC **GUI > Wireless > FlexConnect Groups > FlexConnect Group > General 탭 > Add AP를 선택합니다**

.



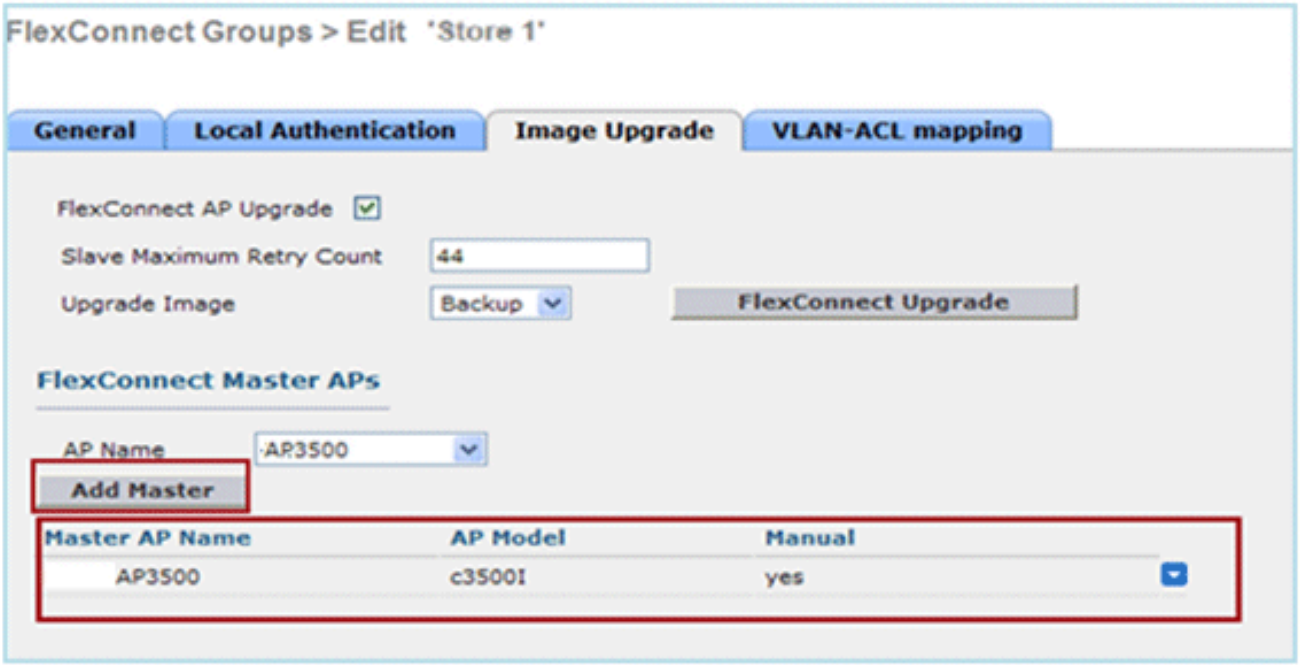
4. 효율적인 AP 이미지 업그레이드를 위해 **FlexConnect AP Upgrade** 확인란을 클릭합니다.WLC **GUI > Wireless > FlexConnect Groups >** FlexConnect **Group > Image Upgrade 탭을 선택합니다**

.



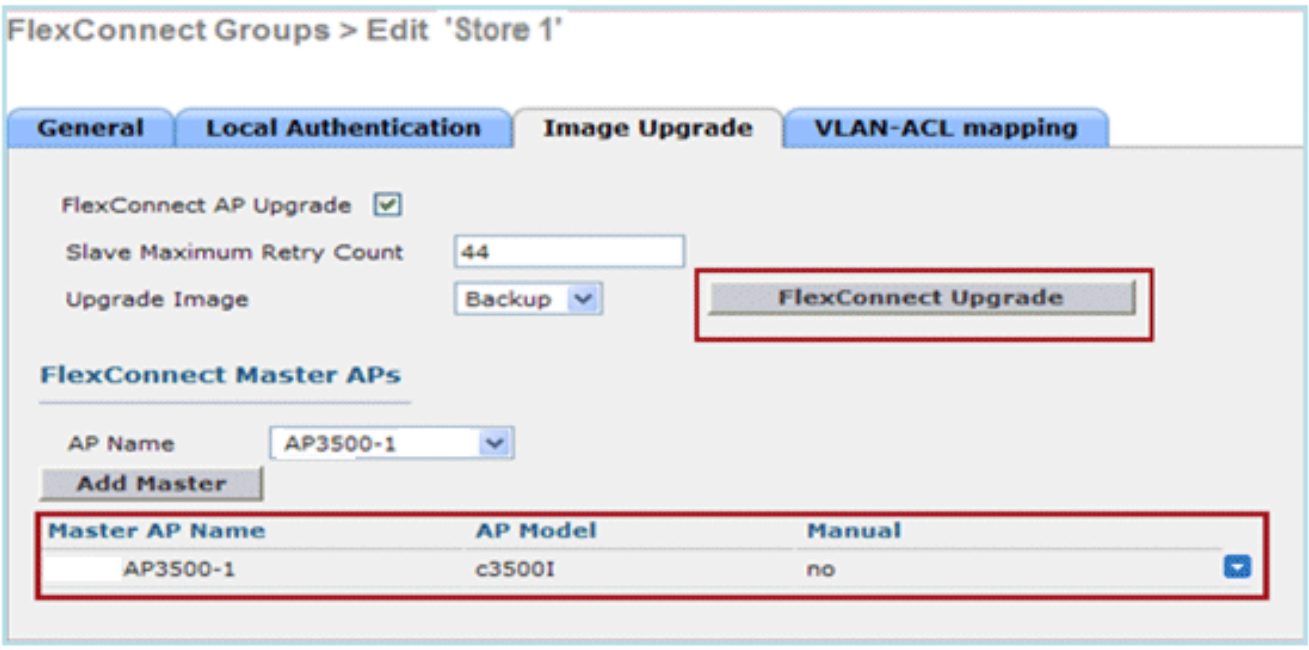
5. 마스터 AP는 수동 또는 자동으로 선택할 수 있습니다.마스터 AP를 수동으로 선택하려면 WLC GUI > Wireless > FlexConnect Groups > FlexConnect Group > Image Upgrade tab > FlexConnect Master APs를 선택하고 드롭다운 목록에서 **AP**를 선택한 다음 **Add Master**를 **클릭합니다**

.



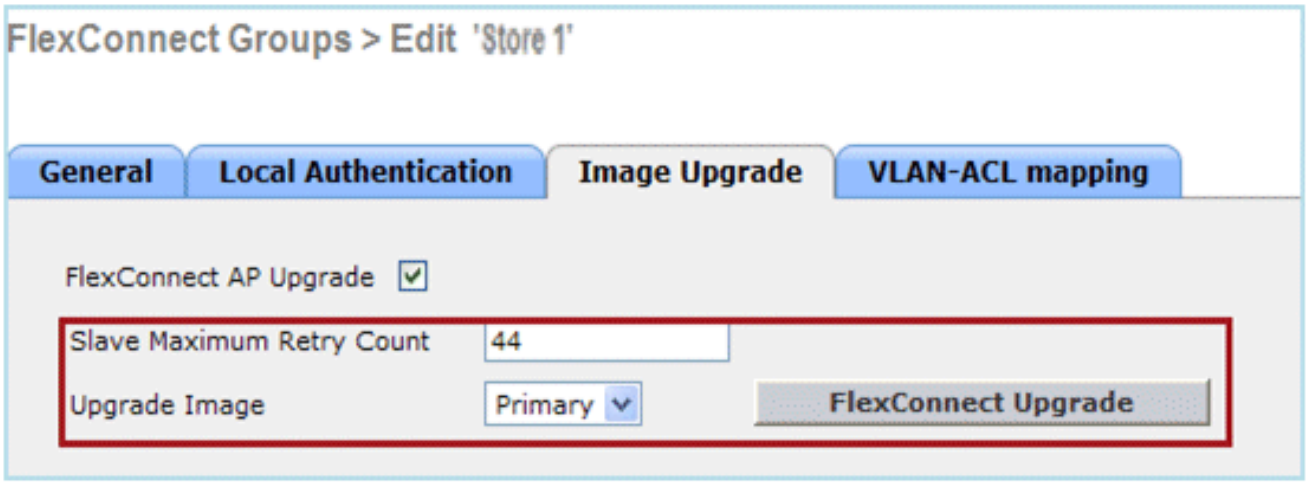
참고: 모델당 하나의 AP만 마스터 AP로 구성할 수 있습니다.마스터 AP가 수동으로 구성된 경우 수동 필드가 **예**로 업데이트됩니다.마스터 AP를 자동으로 선택하려면 **WLC GUI > Wireless > FlexConnect Groups > FlexConnect Group > Image Upgrade 탭을 선택하고 FlexConnect Upgrade를 클릭합니다**

.



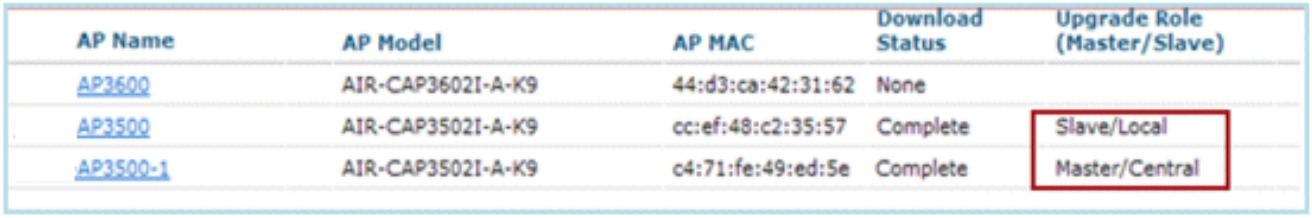
참고: 마스터 AP를 자동으로 선택하면 수동 필드가 **no**로 **업데이트됩니다**.

6. 특정 FlexConnect 그룹의 모든 AP에 대해 효율적인 AP 이미지 업그레이드를 시작하려면 FlexConnect **Upgrade**를 클릭합니다.WLC **GUI > Wireless > FlexConnect Groups > FlexConnect** group **> Image Upgrade 탭을 선택하고 FlexConnect Upgrade를 클릭합니다**
.



참고: Slave Maximum Retry Count는 슬레이브 AP가 마스터 AP에서 이미지를 다운로드하기 위해 시도할 횟수(기본적으로 44회)로, 그 이후에는 WLC에서 이미지를 다운로드하기 위해 다시 가져옵니다.WLC에 대해 20번 시도하여 관리자가 다운로드 프로세스를 다시 시작해야 새 이미지를 다운로드합니다.

7. FlexConnect 업그레이드가 시작되면 마스터 AP만 WLC에서 이미지를 다운로드합니다.All AP(모든 AP) 페이지 아래에서 "**Upgrade Role(역할 업그레이드)**"이 **Master/Central**으로 업데이트됩니다. 즉 마스터 AP가 중앙 위치에 있는 WLC에서 이미지를 다운로드했음을 의미합니다.슬레이브 AP는 로컬 사이트에 있는 마스터 AP에서 이미지를 다운로드하며, 이 이유는 All AP page "**Upgrade Role**"에서 **슬레이브/로컬**로 업데이트되기 때문입니다.이를 확인하려면 WLC **GUI > Wireless**로 **이동합니다**
.



AP Name	AP Model	AP MAC	Download Status	Upgrade Role (Master/Slave)
AP3600	AIR-CAP3602I-A-K9	44:d3:ca:42:31:62	None	
AP3500	AIR-CAP3502I-A-K9	cc:ef:48:c2:35:57	Complete	Slave/Local
AP3500-1	AIR-CAP3502I-A-K9	c4:71:fe:49:ed:5e	Complete	Master/Central

8. 모든 AP 이미지를 다운로드한 후 컨트롤러를 재부팅합니다.이제 컨트롤러가 재부팅될 때까지 AP가 독립형 모드로 돌아갑니다.**참고:** 독립형 모드에서는 내결함성이 클라이언트를 연결합니다.컨트롤러가 돌아오면 AP는 사전 다운로드된 이미지를 사용하여 자동으로 재부팅됩니다.재부팅한 후 AP가 기본 컨트롤러에 다시 참가하고 클라이언트 서비스를 재개합니다.

제한 사항

- 마스터 AP 선택은 FlexConnect 그룹 및 각 그룹의 AP 모델에 따라 결정됩니다.
- 동일한 모델의 슬레이브 AP는 3개만 마스터 AP에서 동시에 업그레이드할 수 있으며 나머지 슬레이브 AP는 임의 백 오프 타이머를 사용하여 AP 이미지를 다운로드하기 위해 마스터 AP에 대해 재시도합니다.
- 슬레이브 AP가 어떤 이유로 마스터 AP에서 이미지를 다운로드하지 못한 경우, 새 이미지를 가져오기 위해 WLC로 이동합니다.
- 이는 CAPWAP AP에서만 작동합니다.

FlexConnect 모드에서 AP 자동 변환

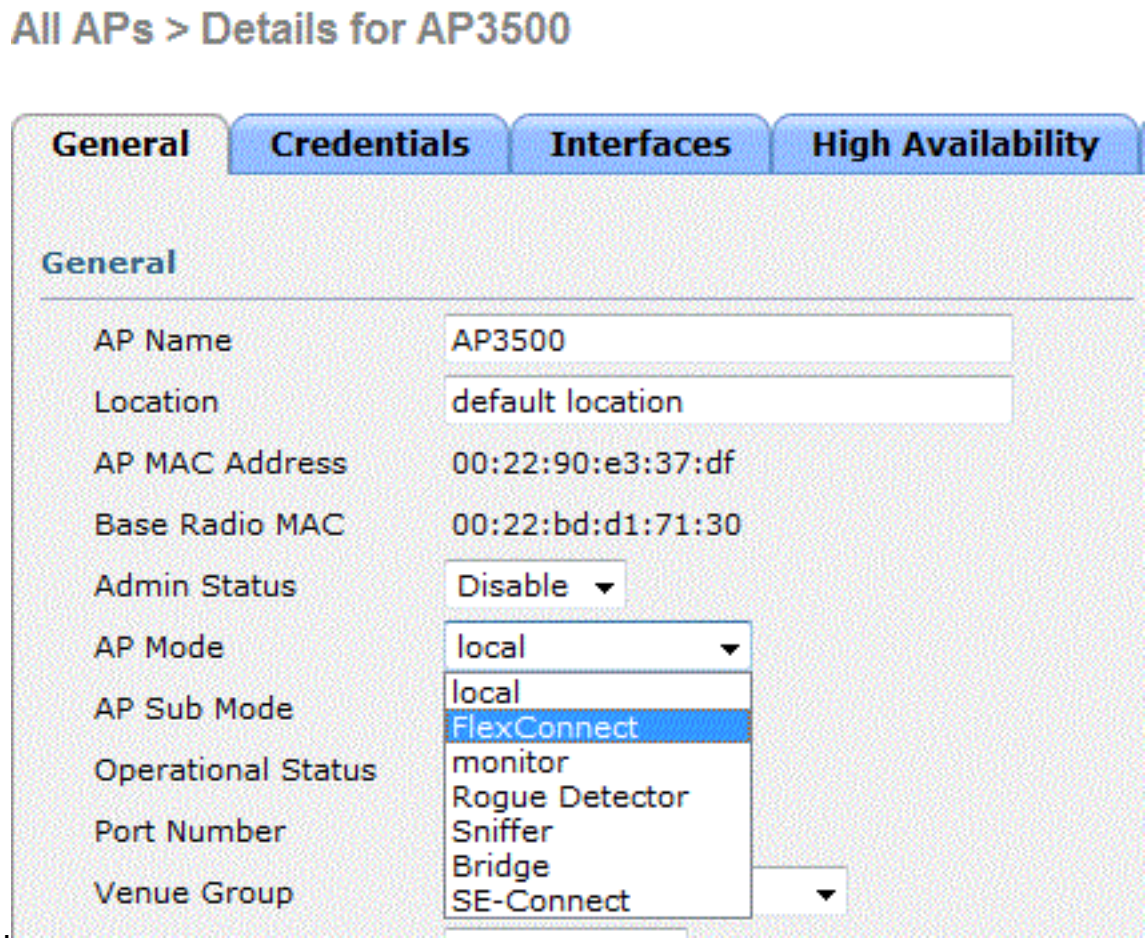
Flex 7500은 AP 모드를 FlexConnect로 변환하는 다음 두 가지 옵션을 제공합니다.

- 수동 모드
- 자동 변환 모드

수동 모드

이 모드는 모든 플랫폼에서 사용할 수 있으며 AP별로 변경할 수 있습니다.

1. WLC **GUI > Wireless > All APs로 이동하고** AP를 선택합니다.
2. FlexConnect**를** AP Mode로 선택한 다음 Apply를 **클릭합니다**.
3. AP 모드를 변경하면 AP가 재부팅됩니다



이 옵션은 현재 모든 WLC 플랫폼에서도 사용할 수 있습니다.

자동 변환 모드

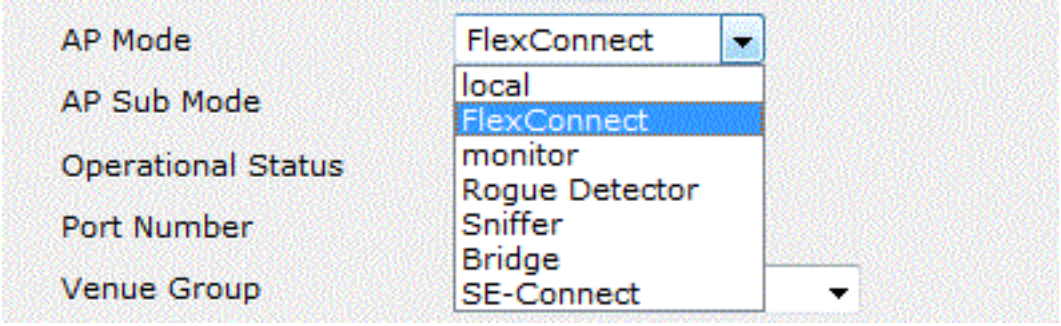
이 모드는 Flex 7500 Controller에만 사용할 수 있으며 CLI를 통해서만 지원됩니다.이 모드는 연결된 모든 AP에서 변경을 트리거합니다.이 CLI를 활성화하기 전에 Flex 7500을 기존 WLC 캠퍼스 컨트롤러와 다른 모빌리티 도메인에 구축하는 것이 좋습니다.

```
(Cisco Controller) >config ap autoconvert ?

disable         Disables auto conversion of unsupported mode APs to supported
                  modes when AP joins
flexconnect     Converts unsupported mode APs to flexconnect mode when AP joins
monitor         Converts unsupported mode APs to monitor mode when AP joins

(Cisco Controller) >
```

1. 자동 변환 기능은 기본적으로 비활성화되어 있습니다. 이 기능은 **show** 명령을 사용하여 확인할 수 있습니다.

   ```
   (Cisco Controller) >show ap autoconvert

   AP Autoconvert ..................................... Disabled
   ```

   지원되지 않는 AP 모드 = 로컬 모드, 스니퍼, 비인가 탐지기 및 브리지



이 옵션은 현재 CLI를 통해서만 사용할 수 있습니다.이러한 CLI는 WLC 7500에서만 사용할 수 있습니다.

2. 컨피그레이션 **ap autoconvert flexconnect** CLI를 **수행하면** 네트워크의 모든 AP가 지원되지 않는 AP 모드를 FlexConnect 모드로 변환됩니다.이미 FlexConnect 또는 모니터 모드에 있는 AP는 영향을 받지 않습니다.

```
(Cisco Controller) >config ap autoconvert flexconnect


(Cisco Controller) >show ap autoconvert

AP Autoconvert ................................ FlexConnect

(Cisco Controller) >
```

3. 컨피그레이션 **ap 자동 변환 모니터** CLI를 수행하면 지원되지 않는 AP 모드를 사용하는 네트워크의 모든 AP가 모니터 모드로 변환됩니다.이미 FlexConnect 또는 모니터 모드에 있는 AP는 영향을 받지 않습니다.

```
(Cisco Controller >config ap autoconvert monitor


(Cisco Controller) >show ap autoconvert

AP Autoconvert ................................ Monitor
```

컨피그레이션 ap autoconvertflexconnect와 **config ap autoconvert 모니터**를 동시에 수행하는 옵션은 없습니다.

로컬 스위칭 WLAN을 위한 FlexConnect WGB/uWGB 지원

릴리스 7.3부터는 WGB를 지원하는 WGB/uWGB 및 유선/무선 클라이언트가 지원되며 로컬 스위칭을 위해 구성된 WLAN에서 일반 클라이언트로 작동합니다.

연결 후 WGB는 각 유선/무선 클라이언트에 대해 IAPP 메시지를 전송하며 Flex AP는 다음과 같이 작동합니다.

- Flex AP가 연결 모드에 있을 때 모든 IAPP 메시지를 컨트롤러에 전달하며 컨트롤러는 로컬 모드 AP와 동일한 방식으로 IAPP 메시지를 처리합니다.유선/무선 클라이언트의 트래픽은 Flex AP에서 로컬로 전환됩니다.
- AP가 독립형 모드에 있을 때 IAPP 메시지를 처리하며, WGB의 유선/무선 클라이언트는 등록 및 등록 취소를 수행할 수 있어야 합니다.연결된 모드로 전환하면 Flex AP는 유선 클라이언트의 정보를 컨트롤러에 다시 전송합니다.Flex AP가 Standalone(독립형)에서 Connected(연결됨) 모드로 전환되면 WGB는 등록 메시지를 3번 전송합니다.

유선/무선 클라이언트는 WGB의 컨피그레이션을 상속합니다. 즉, WGB를 지원하는 클라이언트에는 AAA 인증, AAA 재정의 및 FlexConnect ACL과 같은 별도의 컨피그레이션이 필요하지 않습니다.

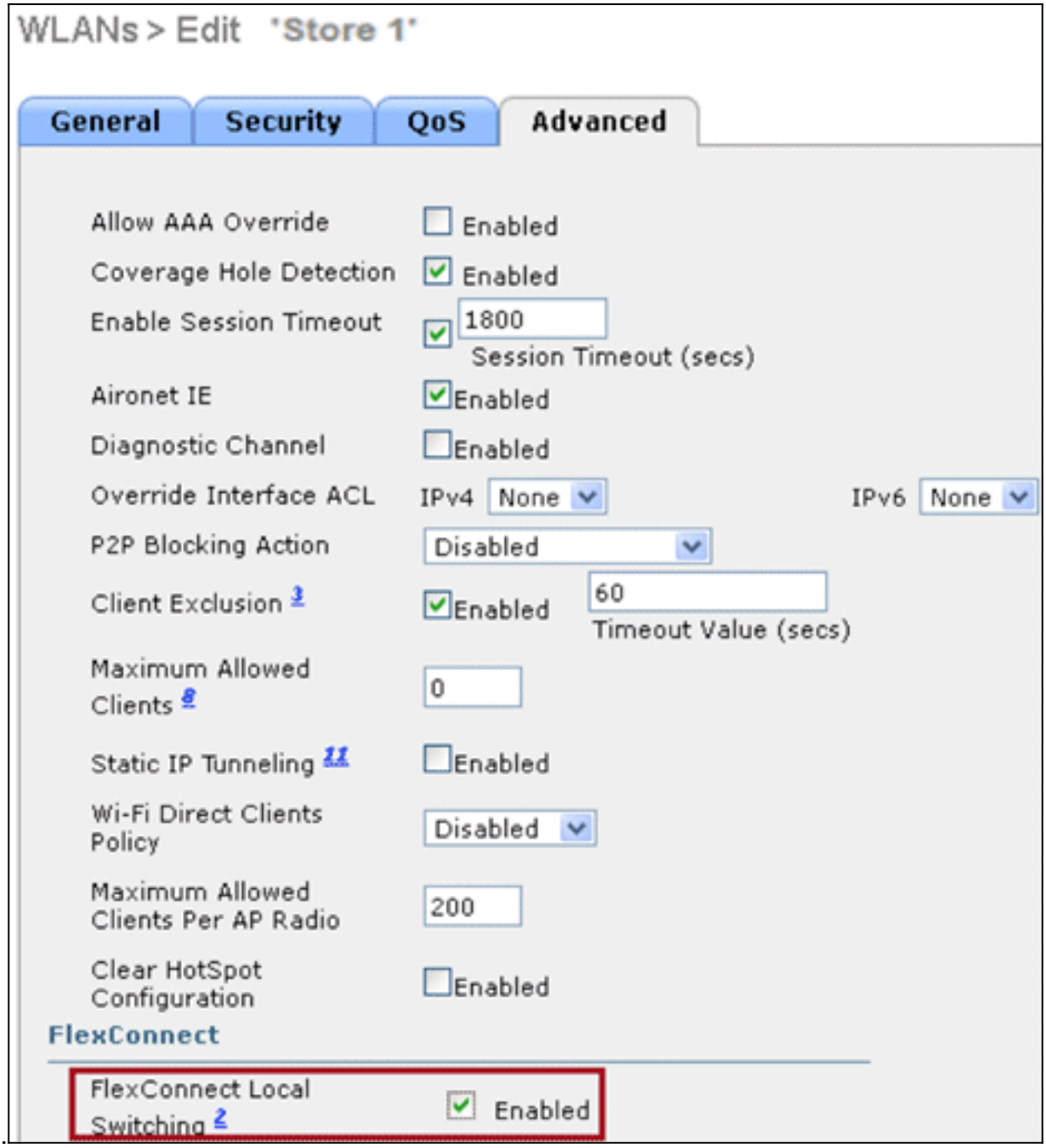
요약

- Flex AP에서 WGB를 지원하기 위해 WLC에 특별한 컨피그레이션이 필요하지 않습니다.
- 내결함성은 WGB 및 WGB 뒤의 클라이언트에 대해 지원됩니다.
- WGB는 IOS AP에서 지원됩니다.1240, 1130, 1140, 1260 및 1250.

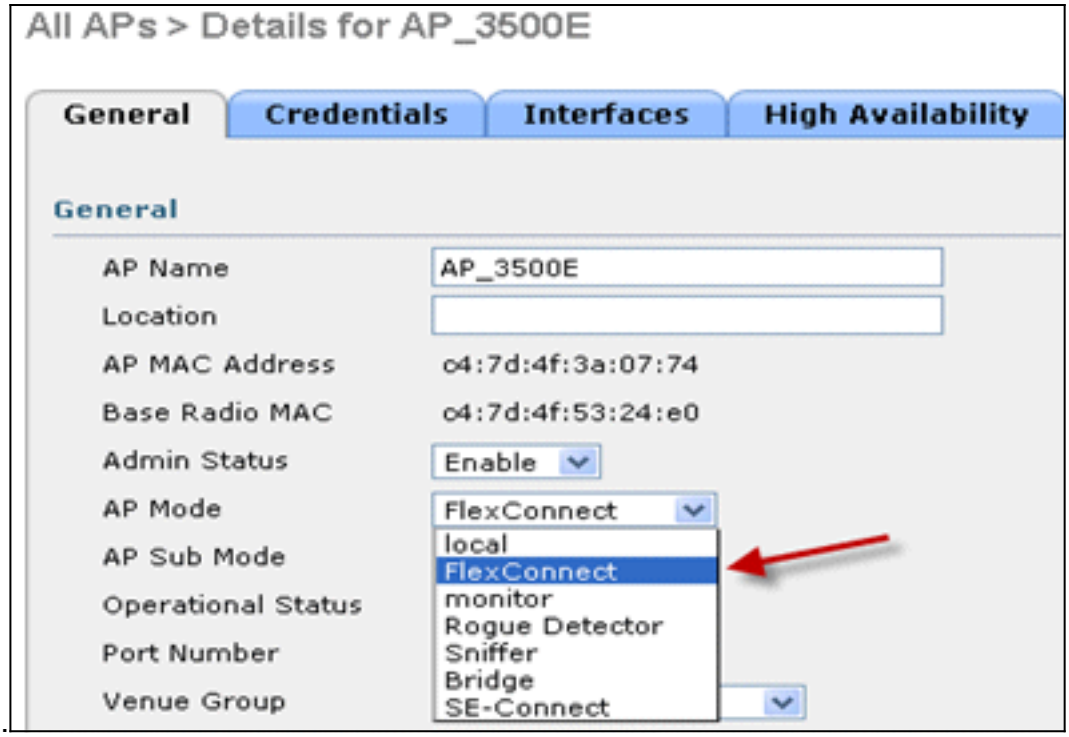
절차

다음 단계를 완료하십시오.

1. 로컬 스위칭에 WGB로 구성된 WLAN에 대해 FlexConnect AP에서 WGB/uWGB 지원을 활성화하려면 특별한 컨피그레이션이 필요하지 않습니다.또한 WGB 뒤의 클라이언트는 Flex AP에 의해 구성된 로컬 스위칭 WLAN에서 일반 클라이언트로 처리됩니다.WLAN**에서 FlexConnect 로컬 스위칭**을 활성화합니다



2. AP 모드를 FlexConnect로 **설정합니다**



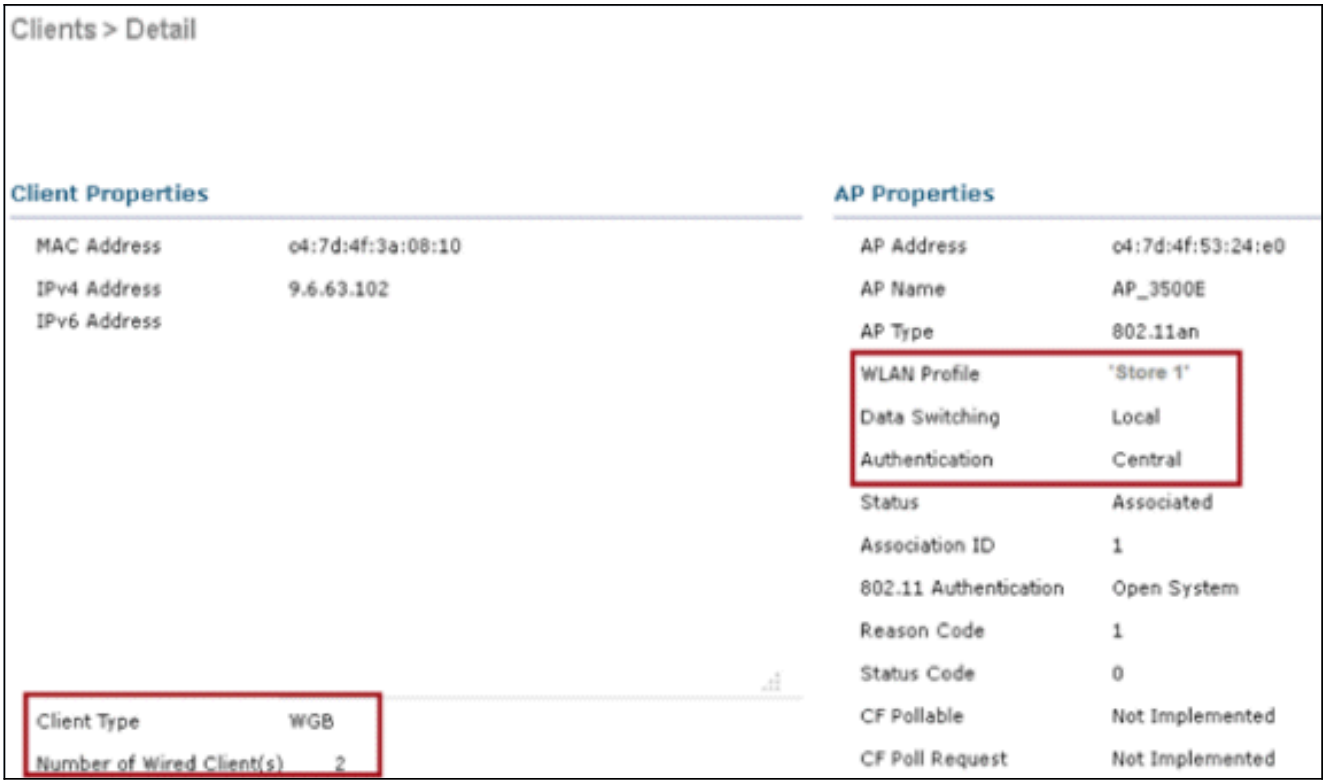
.

3. WGB를 이 구성된 WLAN 뒤에 있는 유선 클라이언트와 연결합니다

.

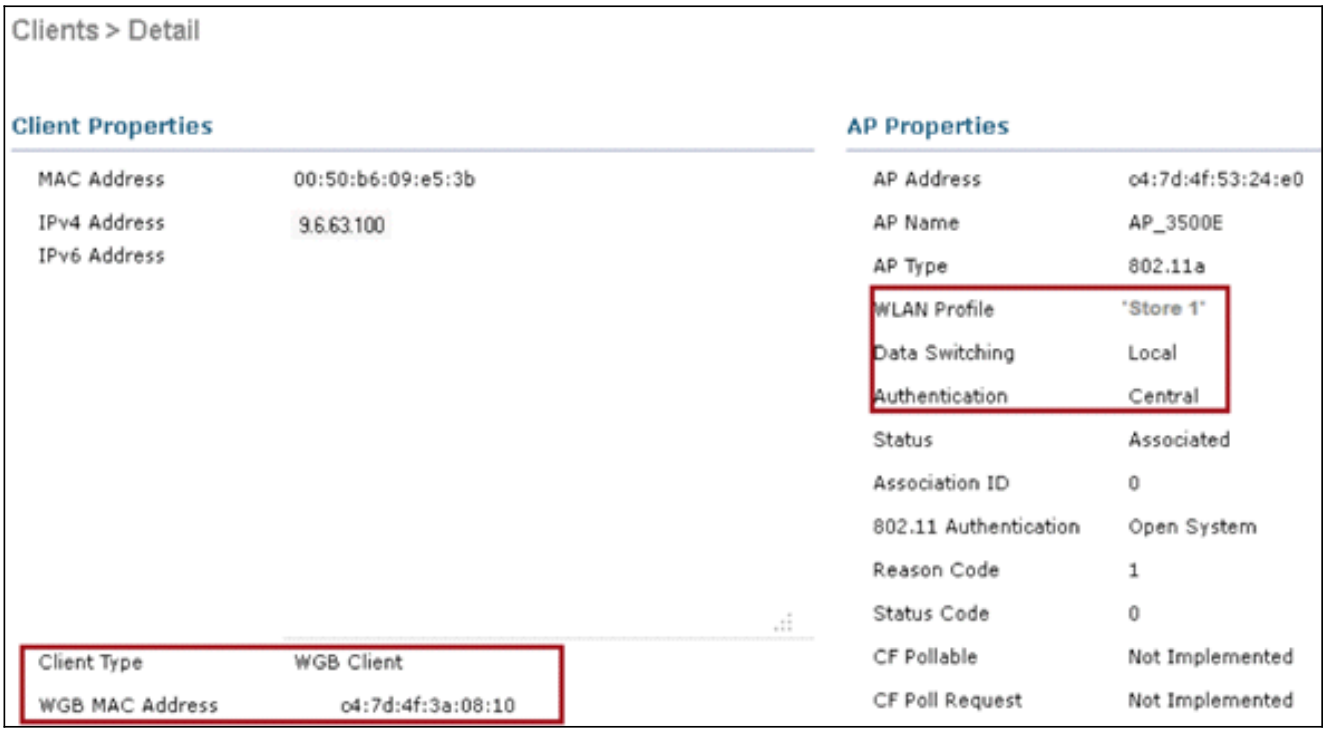
4. WGB에 대한 세부 정보를 확인하려면 **Monitor > Clients**로 이동하여 클라이언트 목록에서 WGB를 선택합니다

.



5. WGB 뒤에 있는 유/무선 클라이언트의 세부 정보를 확인하려면 **Monitor > Clients**로 이동하여 클라이언트를 선택합니다

.



제한 사항

- WGB 뒤에 있는 유선 클라이언트는 항상 WGN 자체와 동일한 VLAN에 있습니다.WGB를 지원하는 클라이언트에 대한 다중 VLAN 지원은 로컬 스위칭에 대해 구성된 WLAN용 Flex AP에서 지원되지 않습니다.
- 로컬 스위칭을 위해 구성된 WLAN의 Flex AP에 연결할 경우 WGB 뒤에서 최대 20개의 클라이언트(유선/무선)가 지원됩니다.이 번호는 로컬 모드 AP에서 WGB 지원을 위해 현재 보유하고 있는 것과 동일합니다.

- 로컬 스위칭을 위해 구성된 WLAN에 연결된 WGB를 지원하는 클라이언트에는 웹 인증이 지원되지 않습니다.

RADIUS 서버 수 증가 지원

릴리스 7.4 이전에는 컨트롤러의 RADIUS 서버 전역 목록에서 FlexConnect 그룹의 RADIUS 서버 컨피그레이션이 수행되었습니다.이 전역 목록에서 구성할 수 있는 최대 RADIUS 서버 수는 17개입니다. 브랜치 수가 증가하면 브랜치 사이트당 RADIUS 서버를 구성해야 합니다.릴리스 7.4부터는 FlexConnect 그룹별로 기본 및 백업 RADIUS 서버를 구성할 수 있습니다. 이 서버는 컨트롤러에 구성된 17개의 RADIUS 인증 서버의 전역 목록에 포함되거나 포함되지 않을 수도 있습니다.

RADIUS 서버에 대한 AP 특정 구성도 지원됩니다.AP별 컨피그레이션은 FlexConnect 그룹 컨피그레이션보다 우선순위가 높습니다.

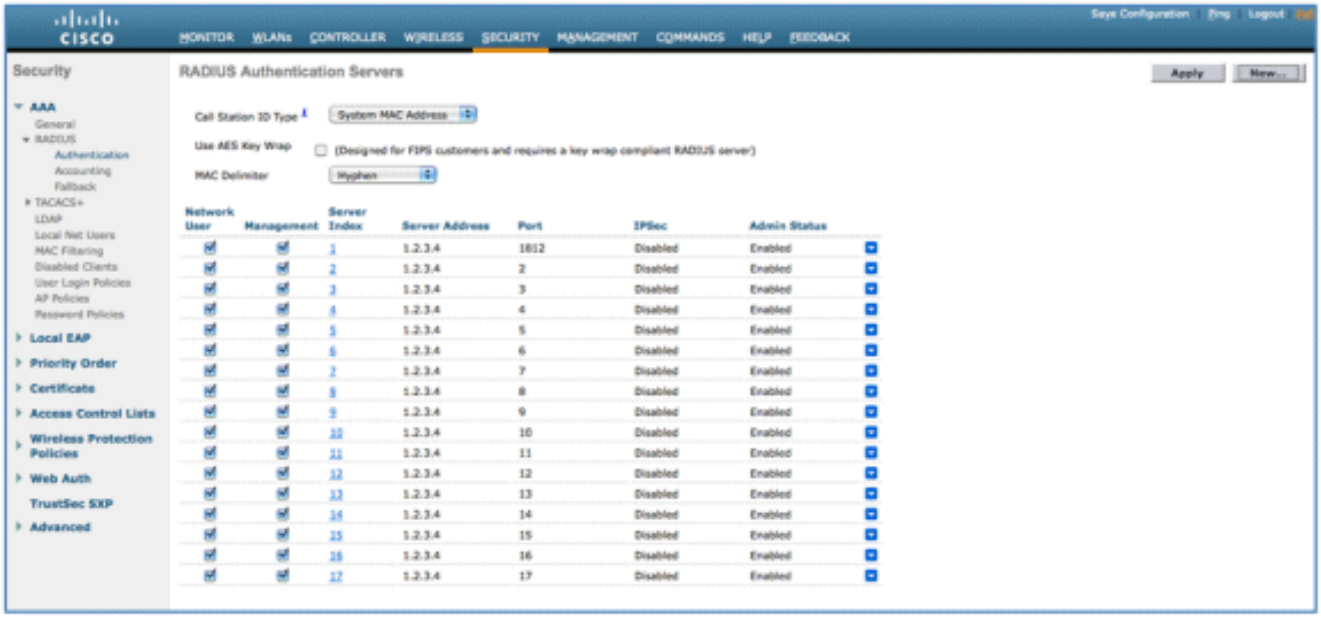
컨트롤러의 전역 RADIUS 서버 목록에 RADIUS 서버의 인덱스가 필요한 FlexConnect 그룹의 기존 컨피그레이션 명령은 더 이상 사용되지 않으며 컨피그레이션 명령으로 대체되며, 이는 서버의 IP 주소와 공유 암호를 사용하여 Flexconnect 그룹의 RADIUS 서버를 구성합니다.

요약

- FlexConnect 그룹당 기본 및 백업 RADIUS 서버의 컨피그레이션 지원. 이 서버는 RADIUS 인증 서버의 전역 목록에 있을 수도 있고 없을 수도 있습니다.
- WLC에 추가할 수 있는 고유한 RADIUS 서버의 최대 수는 지정된 플랫폼에서 구성할 수 있는 FlexConnect 그룹의 2배입니다.예를 들면 FlexConnect 그룹당 1개의 기본 및 1개의 보조 RADIUS 서버가 있습니다.
- 이전 릴리스에서 릴리스 7.4로 소프트웨어를 업그레이드해도 RADIUS 컨피그레이션이 손실되지 않습니다.
- 보조 RADIUS 서버를 삭제하지 않고도 기본 RADIUS 서버를 삭제할 수 있습니다.이는 RADIUS 서버에 대한 현재 FlexConnect 그룹 컨피그레이션과 일치합니다.

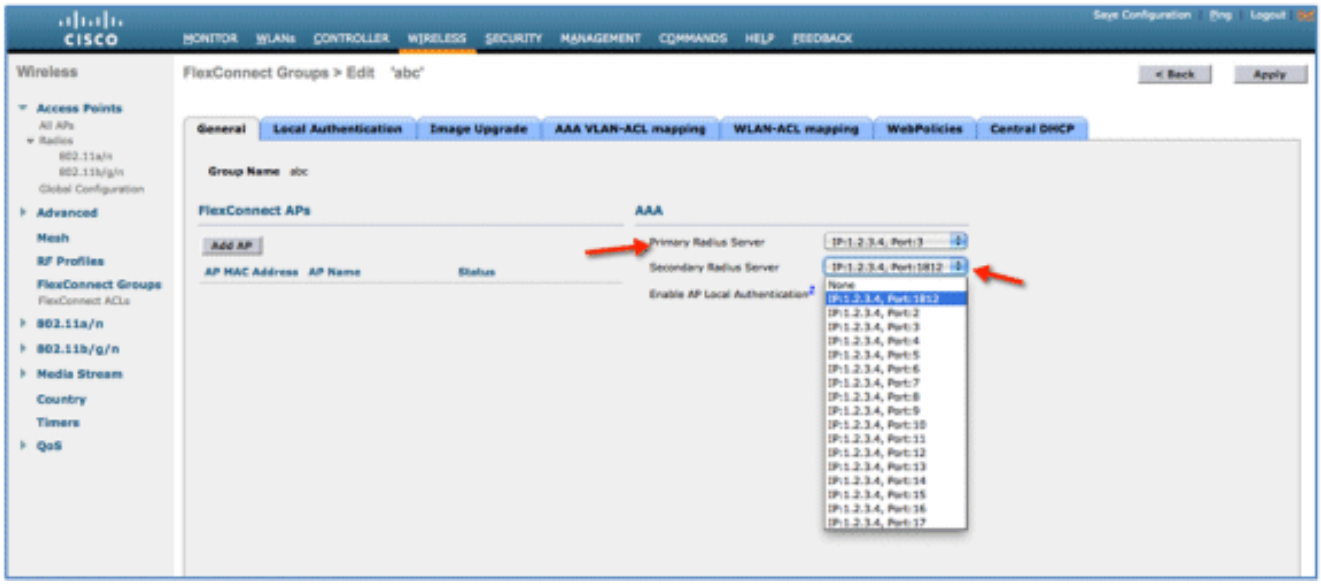
절차

1. 릴리스 7.4 이전의 구성 모드.AAA 인증 컨피그레이션에서 최대 17개의 RADIUS 서버를 구성할 수 있습니다
   .



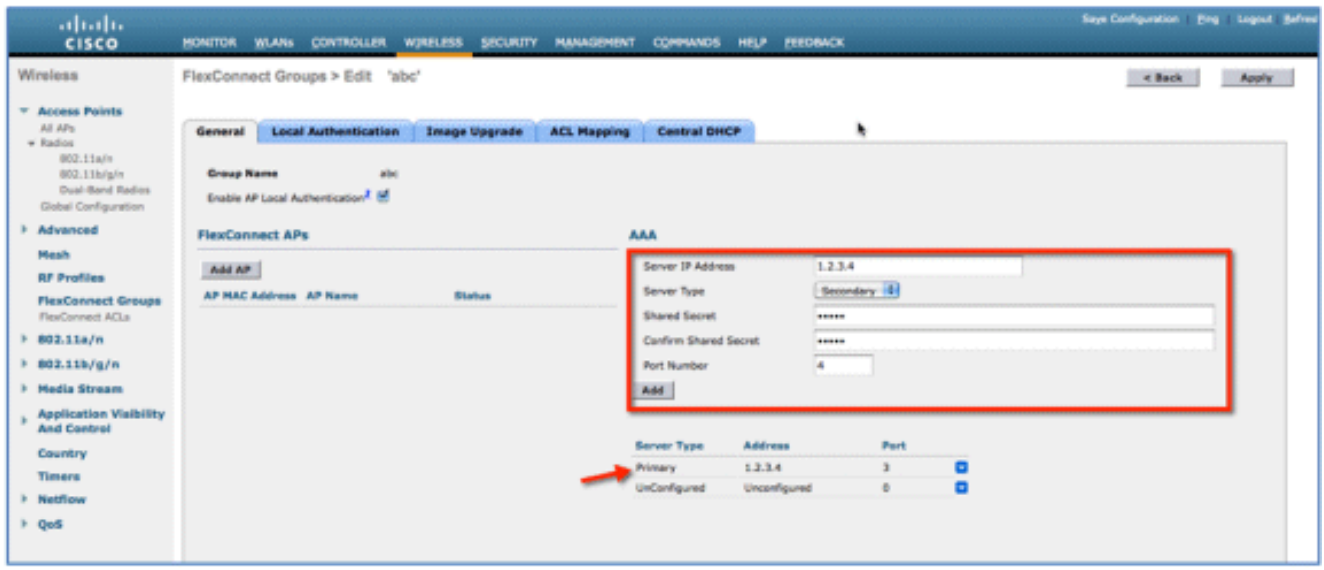
2. 기본 및 보조 RADIUS 서버는 AAA 인증 페이지에 구성된 RADIUS 서버로 구성된 드롭다운 목록을 사용하여 FlexConnect 그룹과 연결할 수 있습니다

.



3. 릴리스 7.4의 FlexConnect 그룹에서 구성 모드기본 및 보조 RADIUS 서버는 IP 주소, 포트 번호 및 공유 암호를 사용하여 FlexConnect 그룹에서 구성할 수 있습니다

.



제한 사항

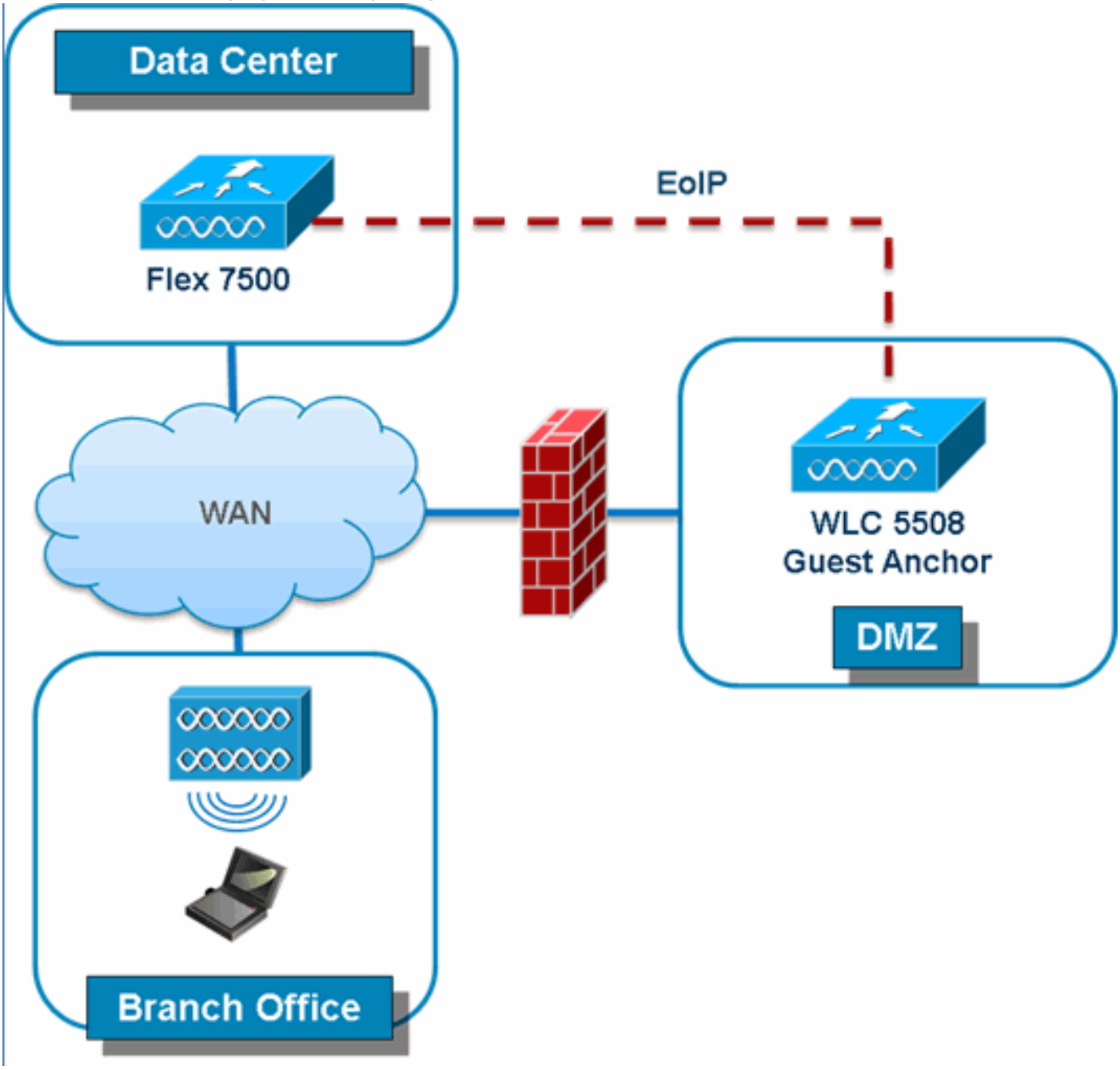
- 소프트웨어가 릴리스 7.4에서 이전 릴리스로 다운그레이드하면 컨피그레이션이 유지되지만 몇 가지 제한 사항이 있습니다.
- 이전 서버가 구성된 경우 기본/보조 RADIUS 서버를 구성하면 이전 항목이 새 항목으로 교체됩니다.

향상된 로컬 모드(ELM)

ELM은 FlexConnect 솔루션에서 지원됩니다.자세한 내용은 ELM의 모범 사례 가이드를 참조하십시오.

Flex 7500의 게스트 액세스 지원

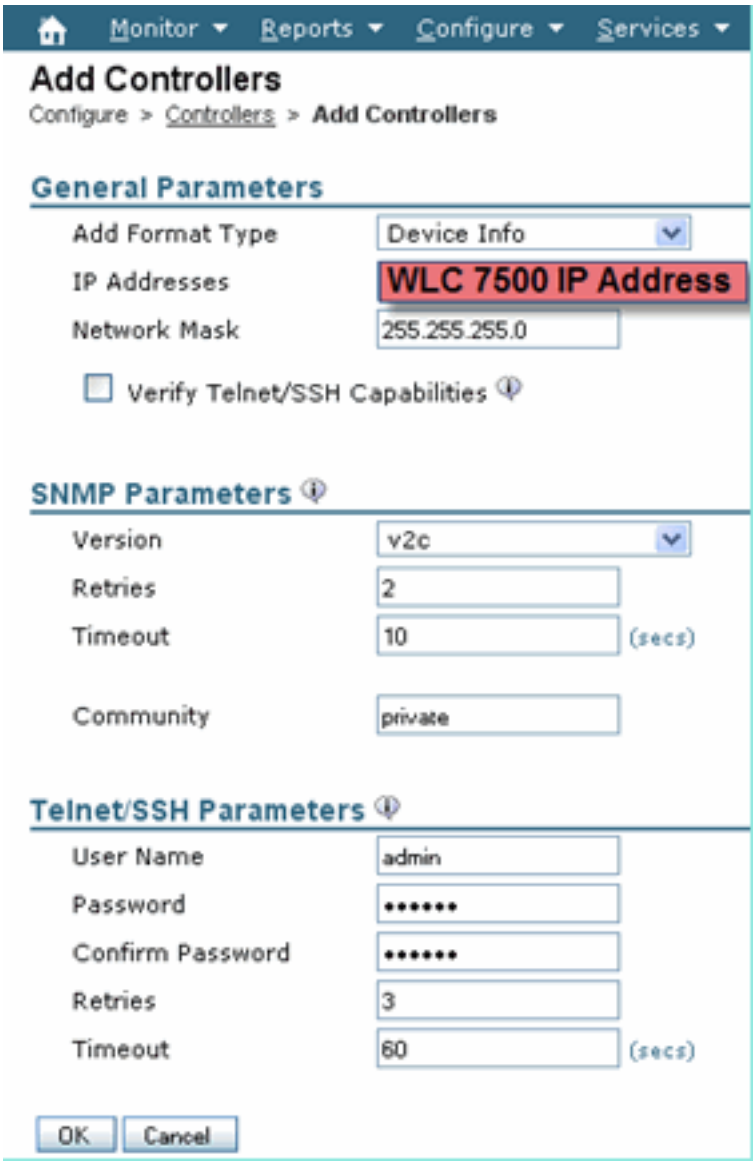
그림 13:Flex 7500의 게스트 액세스 지원

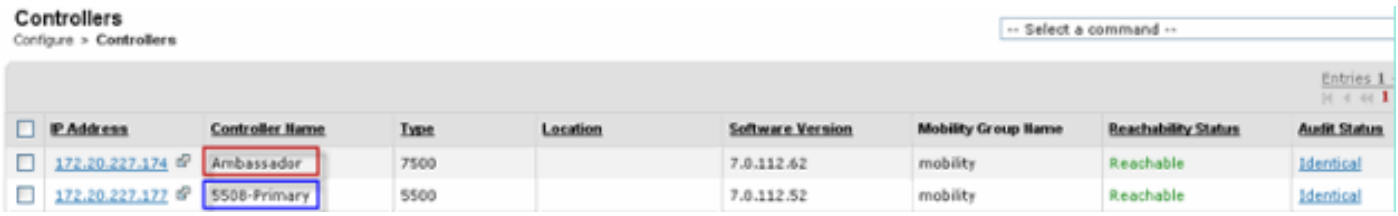


Flex 7500은 DMZ의 게스트 앵커 컨트롤러에 대한 EoIP 터널 생성을 허용 및 계속 지원합니다.무선 게스트 액세스 솔루션에 대한 모범 사례는 게스트 구축 가이드를 참조하십시오.

NCS에서 WLC 7500 관리

NCS에서 WLC 7500을 관리하는 것은 Cisco의 기존 WLC와 동일합니다.





WLC 관리 및 템플릿 검색에 대한 자세한 내용은 Cisco Wireless Control System Configuration Guide, Release 7.0.172.0을 참조하십시오.

FAQ

Q. 원격 위치에서 LAP를 FlexConnect로 구성하는 경우 해당 LAP를 기본 및 보조 컨트롤러로 지정할 수 있습니까?

예:사이트 A에 기본 컨트롤러가 있고 사이트 B에 보조 컨트롤러가 있습니다. 사이트 A의 컨트롤러가 실패하면 LAP는 사이트 B의 컨트롤러에 장애 조치를 수행합니다. 두 컨트롤러를 모두 사용할 수 없는 경우 LAP는 FlexConnect 독립형 모드로 전환됩니까?

A. 네.먼저 LAP는 보조 로 장애 조치됩니다.로컬로 스위칭되는 모든 WLAN은 변경 사항이 없으며, 중앙에서 스위칭되는 모든 WLAN은 트래픽을 새 컨트롤러로 보냅니다.그리고 보조 스위치가 실패하면 로컬 스위칭으로 표시된 모든 WLAN(및 AP 인증자를 수행 중인 공개/사전 공유 키 인증)이 작동 상태로 유지됩니다.

Q. 로컬 모드에서 구성된 액세스 포인트는 FlexConnect 로컬 스위칭으로 구성된 WLAN과 어떻게 거래합니까?

A. 로컬 모드 액세스 포인트는 이러한 WLAN을 일반 WLAN으로 처리합니다.인증 및 데이터 트래픽은 WLC로 다시 터널링됩니다.WAN 링크 실패 중에 이 WLAN은 완전히 다운되었으며 WLC에 대한 연결이 복원될 때까지 이 WLAN에서 활성화된 클라이언트가 없습니다.

Q. 로컬 스위칭으로 웹 인증을 수행할 수 있습니까?

A. 예, 웹 인증이 활성화된 SSID를 가질 수 있으며 웹 인증 후 트래픽을 로컬로 삭제할 수 있습니다.로컬 스위칭을 사용한 웹 인증은 정상적으로 작동합니다.

Q. H REAP에서 로컬로 처리되는 SSID에 대해 컨트롤러의 게스트 포털을 사용할 수 있습니까?대답이 "예"인 경우, 컨트롤러와의 연결이 끊기면 어떻게 됩니까?현재 클라이언트가 즉시 삭제됩니까?

A. 네.이 WLAN은 로컬로 스위칭되므로 WLAN을 사용할 수 있지만 웹 페이지를 사용할 수 없으므로 새 클라이언트가 인증할 수 없습니다.그러나 기존 클라이언트는 삭제되지 않습니다.

Q. FlexConnect에서 PCI 규정 준수를 인증할 수 있습니까?

A. 네.FlexConnect 솔루션은 비인가 탐지를 지원하여 PCI 규정 준수를 충족합니다.

관련 정보

- HREAP 설계 및 구축 설명서
- Cisco 4400 Series Wireless LAN Controller
- Cisco 2000 Series Wireless LAN Controller
- Cisco Wireless Control System
- Cisco 3300 Series 모빌리티 서비스 엔진
- Cisco Aironet 3500 시리즈
- Cisco Secure Access Control System
- 기술 지원 및 문서 – Cisco Systems