

# Catalyst 9800 WLC와의 AP 연결 프로세스 이해

## 목차

---

### [소개](#)

#### [사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

#### [배경 정보](#)

[CAPWAP 세션 설정](#)

[DTLS 세션 설정](#)

[Wireless LAN Controller 검색 방법](#)

[무선 LAN 컨트롤러 선택](#)

[CAPWAP 상태 시스템](#)

[CAPWAP 상태: 검색](#)

[CAPWAP 상태: DTLS 설정](#)

[CAPWAP 상태: 가입](#)

[CAPWAP 상태: 이미지 데이터](#)

[CAPWAP 상태: 구성](#)

[CAPWAP 상태: 실행](#)

#### [구성](#)

[정적 WLC 선택](#)

[AP에 대한 텔넷/SSH 액세스 활성화](#)

[데이터 링크 암호화](#)

[다음을 확인합니다.](#)

#### [문제 해결](#)

[알려진 문제](#)

[WLC GUI 확인](#)

#### [명령](#)

[WLC에서](#)

[Wave 2 및 Catalyst 11ax AP](#)

[Wave 1 AP에서](#)

[방사선 흔적](#)

---

## 소개

이 문서에서는 Cisco Catalyst 9800 WLC와의 AP 조인 프로세스에 대해 자세히 설명합니다.

## 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- CAPWAP(Control and Provisioning Wireless Access Point)에 대한 기본적인 이해
- WLC(Wireless Lan Controller) 사용에 대한 기본 이해

## 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Catalyst 9800-L WLC, Cisco IOS® XE Cupertino 17.9.3
- Catalyst 9120AXE Access Point

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

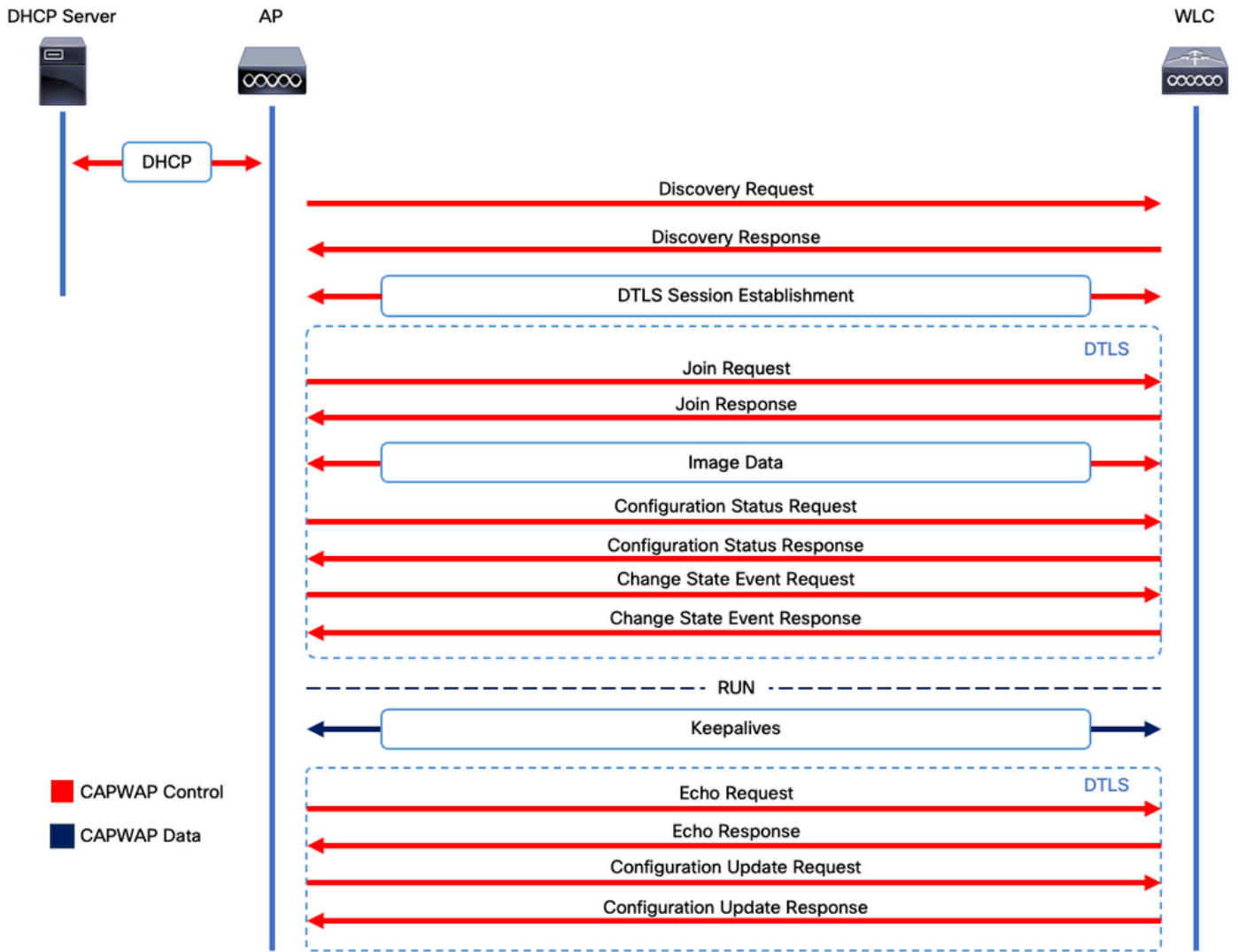
### CAPWAP 세션 설정

CAPWAP(Control And Provisioning Wireless Access Point)는 AP(Access Point) 및 WLC(Wireless LAN Controller)가 보안 통신 터널(CAPWAP 제어용)을 통해 제어 및 데이터 평면 정보를 교환하는데 사용하는 전송 메커니즘을 제공하는 프로토콜입니다.

AP 가입 프로세스에 대해 자세히 설명하려면 CAPWAP(Control And Provisioning Wireless Access Point) 세션 설정 프로세스를 이해하는 것이 중요합니다.

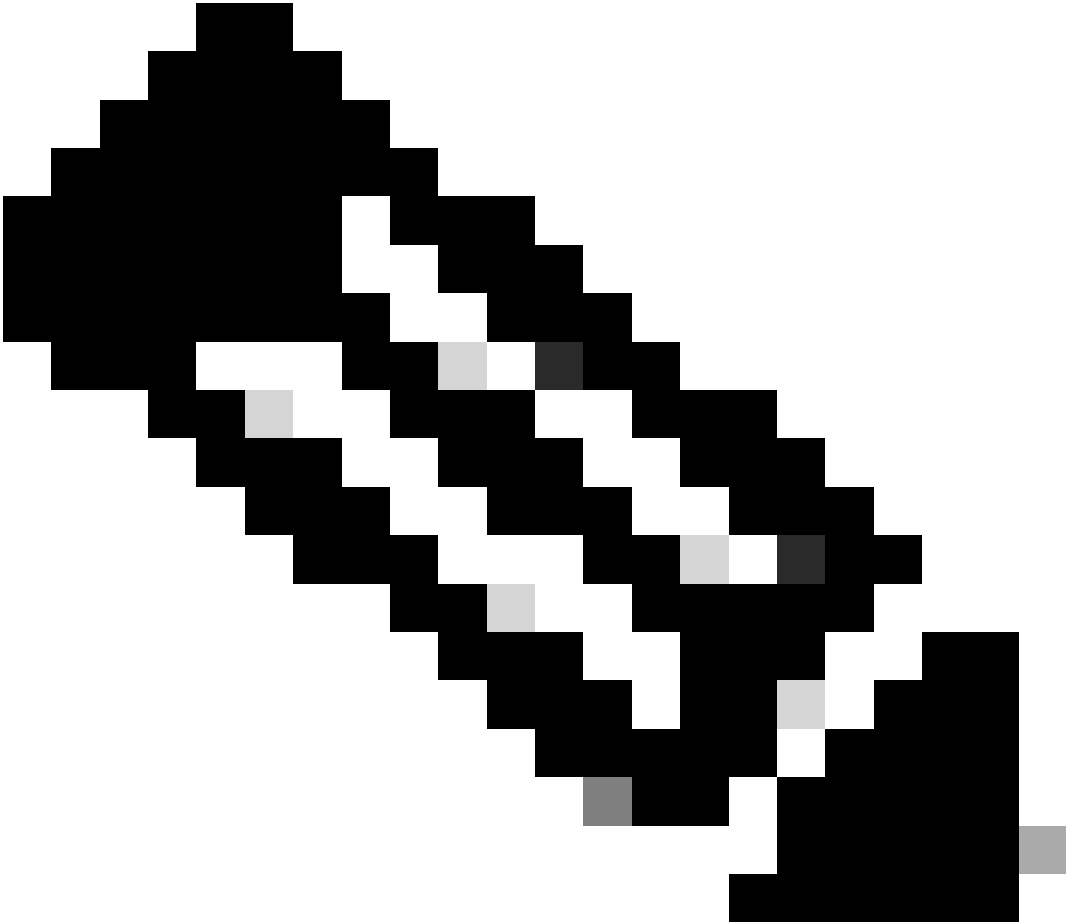
AP에 IP 주소가 있어야 CAPWAP 프로세스를 시작할 수 있습니다. AP에 IP 주소가 없으면 CAPWAP 세션 설정 프로세스를 시작하지 않습니다.

1. 액세스 포인트에서 검색 요청을 보냅니다. 이에 대한 자세한 내용은 WLC 검색 방법 섹션을 참조하십시오
2. WLC에서 검색 응답 전송
3. DTLS 세션 설정 이 경우 이후의 모든 메시지가 암호화되며 패킷 분석 툴에서 DTLS 애플리케이션 데이터 패킷으로 표시됩니다.
4. 액세스 포인트에서 참가 요청 전송
5. WLC에서 참가 응답 전송
6. AP가 이미지 검사를 수행합니다. WLC와 동일한 이미지 버전을 가지고 있으면 다음 단계로 진행합니다. 그렇지 않으면 WLC에서 이미지를 다운로드하고 재부팅하여 새 이미지를 로드합니다. 이와 같은 경우에는 1단계의 과정을 반복하게 된다.
7. 액세스 포인트에서 구성 상태 요청을 보냅니다.
8. WLC에서 컨피그레이션 상태 응답 전송
9. 액세스 포인트가 실행 상태로 전환됨
10. RUN 상태에서 CAPWAP 터널 유지 관리는 두 가지 방법으로 수행됩니다.
  1. Keepalive는 CAPWAP 데이터 터널을 유지하기 위해 교환됩니다
  2. AP가 WLC에 에코 요청을 전송하며, 이 요청은 각 에코 응답으로 응답해야 합니다. 이는 CAPWAP 제어 터널을 유지하기 위한 것입니다.



CAPWAP 세션 설정 프로세스

---



참고: RFC 5415에 따라 CAPWAP는 UDP 포트 5246(CAPWAP 제어) 및 5247(CAPWAP 데이터)을 사용합니다.

---

## DTLS 세션 설정

액세스 포인트가 WLC에서 유효한 검색 응답을 수신하면 보안 터널을 통해 모든 후속 패킷을 전송하기 위해 DTLS 터널이 둘 사이에 설정됩니다. DTLS 세션을 설정하는 프로세스입니다.

1. AP가 클라이언트 Hello 메시지 전송
2. WLC는 검증에 사용되는 쿠키가 포함된 HelloVerifyRequest 메시지를 보냅니다.
3. AP는 유효성 검사에 사용되는 쿠키가 포함된 ClientHello 메시지를 보냅니다.
4. WLC는 다음 순서대로 패킷을 전송합니다.
  1. 서버헬로
  2. 인증서
  3. 서버 키 교환
  4. 인증서 요청
  5. 서버헬로완료

5. AP는 다음 순서대로 패킷을 전송합니다.

1. 인증서
2. 클라이언트 키 교환
3. 인증서 확인
4. 암호 사양 변경

6. WLC는 AP의 ChangeCipherSpec에 자체 ChangedCipherSpec으로 응답합니다.

1. 암호 사양 변경

WLC에서 보낸 마지막 ChangedCipherSpec 메시지 이후 보안 터널이 설정되고 양방향으로 전송된 모든 트래픽이 암호화됩니다.

## Wireless LAN Controller 검색 방법

네트워크에 있는 하나의 WLC의 존재를 액세스 포인트에 알리는 몇 가지 옵션이 있습니다.

- DHCP 옵션 43: 이 옵션은 가입할 WLC의 IPv4 주소를 AP에 제공합니다. 이 프로세스는 AP와 WLC가 서로 다른 사이트에 있는 대규모 구축에서 편리합니다.
- DHCP 옵션 52: 이 옵션은 가입할 WLC의 IPv6 주소를 AP에 제공합니다. DHCP 옵션 43과 동일한 시나리오에서 사용이 편리합니다.
- DNS 검색: AP는 도메인 이름 CISCO-CAPWAP-CONTROLLER.localdomain을 쿼리합니다. 가입할 WLC의 IPv4 또는 IPv6 주소를 확인하도록 DNS 서버를 구성해야 합니다. 이 옵션은 WLC가 AP와 동일한 사이트에 저장된 구축에서 편리합니다.
- 레이어 3 브로드캐스트: AP가 255.255.255.255에 브로드캐스트 메시지를 자동으로 전송합니다. AP와 동일한 서브넷 내의 모든 WLC는 이 검색 요청에 응답해야 합니다.
- 고정 컨피그레이션: `capwap ap primary-base <wlc-hostname> <wlc-IP-address>` 명령을 사용하여 AP의 WLC에 대한 고정 항목을 구성할 수 있습니다.
- **모빌리티 검색:** AP가 이전에 모빌리티 그룹의 일부인 WLC에 조인된 경우 AP는 해당 모빌리티 그룹에 있는 WLC의 레코드도 저장합니다.

---

참고: 나열된 WLC 검색 방법에는 우선 순위가 없습니다.

---

#### 무선 LAN 컨트롤러 선택

AP가 WLC 검색 방법을 사용하여 WLC에서 검색 응답을 받으면 다음 기준에 따라 참가할 컨트롤러 하나를 선택합니다.

- 기본 컨트롤러(capwap ap primary-base <wlc-hostname> <wlc-IP-address> 명령으로 구성됨)
- 보조 컨트롤러(capwap ap secondary-base <wlc-hostname> <wlc-IP-address> 명령으로 구성됨)
- 3차 컨트롤러(capwap ap tertiary-base <wlc-hostname> <wlc-IP-address> 명령으로 구성됨)

- 1차, 2차 또는 3차 WLC가 이전에 구성되지 않은 경우, AP는 사용 가능한 AP의 최대 용량을 가진 자체 검색 응답으로 검색 요청에 응답한 첫 번째 WLC(즉 주어진 시간에 가장 많은 AP를 지원할 수 있는 WLC)에 참여하려고 시도합니다.

## CAPWAP 상태 시스템

AP 콘솔에서 CAPWAP 상태 머신을 추적할 수 있으며, 이는 CAPWAP 세션 설정 섹션에 설명된 단계를 거칩니다.

### CAPWAP 상태: 검색

여기에서 검색 요청 및 응답을 볼 수 있습니다. AP가 DHCP를 통해 WLC IP를 수신하는 방법(옵션 43)을 확인하고 이전에 알려진 WLC에 검색 요청을 보냅니다.

<#root>

[\*09/14/2023 04:12:09.7740]

**CAPWAP State: Init**

[\*09/14/2023 04:12:09.7770]

[\*09/14/2023 04:12:09.7770]

**CAPWAP State: Discovery**

[\*09/14/2023 04:12:09.7790]

**Discovery Request sent to 172.16.0.20, discovery type STATIC\_CONFIG(1)**

[\*09/14/2023 04:12:09.7800]

**Discovery Request**

sent to 172.16.5.11, discovery type STATIC\_CONFIG(1)

[\*09/14/2023 04:12:09.7800]

**Got WLC address 172.16.5.11 from DHCP.**

[\*09/14/2023 04:12:09.7820]

**Discovery Request**

sent to 172.16.0.20, discovery type STATIC\_CONFIG(1)

[\*09/14/2023 04:12:09.7830]

**Discovery Request**

sent to 172.16.5.11, discovery type STATIC\_CONFIG(1)

[\*09/14/2023 04:12:09.7840]

**Discovery Request sent to 255.255.255.255, discovery type UNKNOWN(0)**

[\*09/14/2023 04:12:09.7850]

[\*09/14/2023 04:12:09.7850]

**CAPWAP State: Discovery**

[\*09/14/2023 04:12:09.7850]

Discovery Response

from 172.16.0.20

[\*09/14/2023 04:12:09.8030]

Discovery Response

from 172.16.5.11

[\*09/14/2023 04:12:09.8060]

Discovery Response

from 172.16.0.20

[\*09/14/2023 04:12:09.8060]

Discovery Response

from 172.16.5.11

[\*09/14/2023 04:12:09.8060]

Discovery Response

from 172.16.5.11

[\*09/14/2023 04:12:09.8060]

Discovery Response

from 172.16.0.20

[\*09/14/2023 04:12:09.8060]

Discovery Response

from 172.16.5.169

[\*09/14/2023 04:12:09.8060]

Discovery Response

from 172.16.5.169

이 AP는 고정으로 구성된 WLC(172.16.0.20) 및 DHCP 옵션 43(172.16.5.11)을 통해 표시된 WLC에서 검색 응답을 수신할 뿐만 아니라, 동일한 서브넷 내의 다른 WLC(172.16.5.169)에서 검색 응답을 수신했습니다. 브로드캐스트 검색 메시지가 수신되었기 때문입니다.

CAPWAP 상태: DTLS 설정

여기서, AP와 WLC 간의 DTLS 세션이 교환된다.

<#root>

[\*09/27/2023 21:50:41.0000]

CAPWAP State: DTLS Setup

[\*09/27/2023 21:50:41.7140] sudi99\_request\_check\_and\_load: Use HARSА SUDI certificat



CAPWAP 상태: 가입

DTLS 세션을 설정한 후 이제 WLC에 대한 가입 요청이 보안 세션을 통해 전송됩니다. WLC의 Join Response(참여 응답)를 사용하여 이 요청이 즉시 응답되는 방식을 확인합니다

<#root>

[\*09/27/2023 21:50:41.9880]

CAPWAP State: Join

[\*09/27/2023 21:50:41.9910]

Sending Join request to 172.16.5.11

through port 5270

[\*09/27/2023 21:50:41.9950]

Join Response from 172.16.5.11

[\*09/27/2023 21:50:41.9950]

AC accepted join request

with result code: 0

[\*09/27/2023 21:50:41.9990] Received wlcType 0, timer 30

[\*09/27/2023 21:50:41.9990] TLV ID 2216 not found

[\*09/27/2023 21:50:41.9990] TLV-DEC-ERR-1: No proc for 2216

CAPWAP 상태: 이미지 데이터

AP는 자신의 이미지를 WLC의 이미지와 비교합니다. 이 경우 AP의 활성 파티션과 백업 파티션 모두 WLC와 다른 이미지를 가지고 있으므로 AP가 WLC에 적절한 이미지를 요청하고 현재 비활성 파티션으로 다운로드하도록 지시하는 **upgrade.sh** 스크립트를 호출합니다.

<#root>

[\*09/27/2023 21:50:42.0430]

CAPWAP State: Image Data

[\*09/27/2023 21:50:42.0430]

AP image version 8.10.185.0 backup 8.10.105.0, Controller 17.9.3.50

[\*09/27/2023 21:50:42.0430]

Version does not match.

[\*09/27/2023 21:50:42.0680]

upgrade.sh

: Script called with args:[PRECHECK]  
[\*09/27/2023 21:50:42.1060] do PRECHECK,

part2 is active part

[\*09/27/2023 21:50:42.1240]

upgrade.sh

: /tmp space: OK available 101476, required 40000

[\*09/27/2023 21:50:42.1250] wtpImgFileReadRequest: request ap1g7, local /tmp/part.tar

[\*09/27/2023 21:50:42.1310]

Image Data Request sent to 172.16.5.11

, fileName [ap1g7], slaveStatus 0

[\*09/27/2023 21:50:42.1340]

Image Data Response from 172.16.5.11

[\*09/27/2023 21:50:42.1340] AC accepted join request with result code: 0

[\*09/27/2023 21:50:42.1450] <.....

[\*09/27/2023 21:50:55.4980] .....

[\*09/27/2023 21:51:11.6290] .....Discarding msg CAPWAP\_WTP\_EVENT\_REQUEST(type

[\*09/27/2023 21:51:19.7220] .....

[\*09/27/2023 21:51:24.6880] .....

[\*09/27/2023 21:51:37.7790] .....

[\*09/27/2023 21:51:50.9440] .....> 76738560 bytes, 57055 msgs, 930 last

[\*09/27/2023 21:51:59.9160] Last block stored, IsPre 0, WriteTaskId 0

[\*09/27/2023 21:51:59.9160]

Image transfer completed from WLC

, last 1

이미지 전송이 완료되면 AP는 이를 검증하기 위해 이미지 서명 확인 프로세스를 시작합니다. 그런 다음 **upgrade.sh** 스크립트는 이미지를 현재 비활성 파티션에 설치하고 부팅하는 파티션을 교체합니다. 마지막으로, AP가 다시 로드되고 처음부터 프로세스를 반복합니다(CAPWAP 상태: 검색).

<#root>

[\*09/27/2023 21:52:01.1280]

Image signing verify success.

[\*09/27/2023 21:52:01.1440]

[\*09/27/2023 21:52:01.1440] [9/27/2023 21:53:2] : Shadow is now in-synced with master

[\*09/27/2023 21:52:01.1440]

[\*09/27/2023 21:52:01.1440] [9/27/2023 21:53:2] : Verifying against bundle image b1ldr.img...

[\*09/27/2023 21:52:01.1570]

upgrade.sh

:

part to upgrade is part1

[\*09/27/2023 21:52:01.1780]

**upgrade.sh**

: AP version1: part1 8.10.105.0, img 17.9.3.50  
[\*09/27/2023 21:52:01.1960]

**upgrade.sh**

: Extracting and verifying image in part1...  
[\*09/27/2023 21:52:01.2080]

**upgrade.sh**

: BOARD generic case execute  
[\*09/27/2023 21:52:01.5280]

**upgrade.sh**

: Untar /tmp/part.tar to /bootpart/part1...  
[\*09/27/2023 21:52:01.7890]

**upgrade.sh**

: Sync image to disk...  
[\*09/27/2023 21:52:31.4970]

**upgrade.sh**

: status '

**Successfully verified image in part1.**

'  
[\*09/27/2023 21:52:32.5270]

**upgrade.sh**

: AP version2: part1 17.9.3.50, img 17.9.3.50  
[\*09/27/2023 21:52:32.5540]

**upgrade.sh**

: AP backup version: 17.9.3.50  
[\*09/27/2023 21:52:32.5700]

**upgrade.sh**

:  
**Finished upgrade task.**

[\*09/27/2023 21:52:32.5840]

**upgrade.sh**

: Cleanup for do\_upgrade...  
[\*09/27/2023 21:52:32.5970]

**upgrade.sh**

: /tmp/upgrade\_in\_progress cleaned  
[\*09/27/2023 21:52:32.6090]

**upgrade.sh**

: Cleanup tmp files ...  
[\*09/27/2023 21:52:32.6720]

**upgrade.sh**

: Script called with args:[ACTIVATE]  
[\*09/27/2023 21:52:32.7100] do ACTIVATE, part2 is active part  
[\*09/27/2023 21:52:32.7640]

**upgrade.sh**

: Verifying image signature in part1  
[\*09/27/2023 21:52:33.7730]

**upgrade.sh**

: status 'Successfully verified image in part1.'  
[\*09/27/2023 21:52:33.7850]

**upgrade.sh**

:  
**activate part1, set BOOT to part1**

[\*09/27/2023 21:52:34.2940]

**upgrade.sh**

:  
**AP primary version after reload: 17.9.3.50**

[\*09/27/2023 21:52:34.3070]

**upgrade.sh**

: AP backup version after reload: 8.10.185.0  
[\*09/27/2023 21:52:34.3190]

**upgrade.sh**

: Create after-upgrade.log  
[\*09/27/2023 21:52:37.3520]

**AP Rebooting: Reset Reason - Image Upgrade**



경고: Wave 1 액세스 포인트가 만료된 인증서로 인해 새 이미지를 다운로드하지 못할 수 있습니다. 자세한 내용은 [Field Notice 72524](#)를 참조하고 [2022년 12월 4일\(CSCwd80290\) Support Document\(IOS AP 이미지 다운로드 실패, Expired Image Signing Certificate Past\)](#)를 주의 깊게 읽어보십시오.

---

AP가 다시 로드되고 CAPWAP **Discover and Join**(CAPWAP 검색 및 조인) 상태를 다시 통과하면 **Image Data**(이미지 데이터) 상태에서 AP에 적절한 이미지가 있음을 감지합니다.

<#root>

[\*09/27/2023 21:56:13.7640]

CAPWAP State: Image Data

[\*09/27/2023 21:56:13.7650]

AP image version 17.9.3.50 backup 8.10.185.0, Controller 17.9.3.50

[\*09/27/2023 21:56:13.7650]

Version is the same, do not need update.

[\*09/27/2023 21:56:13.7650] status '

upgrade.sh: Script called with args:[NO\_UPGRADE]

,

[\*09/27/2023 21:56:13.7850] do NO\_UPGRADE, part1 is active part

CAPWAP 상태: 구성

AP가 WLC와 버전이 동일한지 검증한 후 AP는 현재 컨피그레이션을 WLC에 알립니다. 일반적으로 이는 AP가 컨피그레이션을 유지할지(WLC에서 사용 가능한 경우) 묻는 것을 의미합니다.

<#root>

[\*09/27/2023 21:56:14.8680]

CAPWAP State: Configure

[\*09/27/2023 21:56:15.8890] Telnet is not supported by AP, should not encode this payload

[\*09/27/2023 21:56:15.8890] Radio [1] Administrative state DISABLED change to ENABLED

[\*09/27/2023 21:56:16.0650] Radio [0] Administrative state DISABLED change to ENABLED

[\*09/27/2023 21:56:16.0750] DOT11\_CFG[1]: Starting radio 1

[\*09/27/2023 21:56:16.1150] DOT11\_DRV[1]: Start Radio1

[\*09/27/2023 21:56:16.1160] DOT11\_DRV[1]: set\_channel Channel set to 36/20

[\*09/27/2023 21:56:16.4380] Started Radio 1

[\*09/27/2023 21:56:16.4880] DOT11\_CFG[0]: Starting radio 0

[\*09/27/2023 21:56:17.5220] DOT11\_DRV[0]: Start Radio0

[\*09/27/2023 21:56:16.5650] DOT11\_DRV[0]: set\_channel Channel set to 1/20

[\*09/27/2023 21:56:16.5650] Started Radio 0

[\*09/27/2023 21:56:16.5890] sensord psage\_base init: RHB Sage base ptr a1030000

CAPWAP 상태: 실행

이 시점에서 AP가 성공적으로 컨트롤러에 연결되었습니다. 이 상태에서 WLC는 AP에서 요청한 컨피그레이션을 재정의하는 메커니즘을 트리거합니다. AP가 무선 및 자격 증명 컨피그레이션을 푸시하고, WLC가 이 AP에 대한 이전 지식이 없으므로 기본 정책 태그에도 할당됨을 확인할 수 있습니다.

<#root>

[\*09/27/2023 21:56:17.4870]

CAPWAP State: Run

[\*09/27/2023 21:56:17.4870]

AP has joined controller

uwu-9800

[\*09/27/2023 21:56:17.4940] DOT11\_DRV[0]: set\_channel Channel set to 1/20  
[\*09/27/2023 21:56:17.5440] sensord split\_glue psage\_base: RHB Sage base ptr a1030000  
[\*09/27/2023 21:56:17.6010] sensord split\_glue sage\_addr: RHB Sage base ptr a1030000  
[\*09/27/2023 21:56:17.6230] ptr a1030000  
[\*09/27/2023 21:56:17.6420]

DOT11\_DRV[0]: set\_channel Channel set to 1/20

[\*09/27/2023 21:56:17.8120]

DOT11\_DRV[1]: set\_channel Channel set to 36/20

[\*09/27/2023 21:56:17.9350] Previous AP mode is 0, change to 0  
[\*09/27/2023 21:56:18.0160] Current session mode: ssh, Configured: Telnet-No, SSH-Yes, Console-Yes  
[\*09/27/2023 21:56:18.1220] Current session mode: telnet, Configured: Telnet-No, SSH-Yes, Console-Yes  
[\*09/27/2023 21:56:18.1310] Current session mode: console, Configured: Telnet-No, SSH-Yes, Console-Yes  
[\*09/27/2023 21:56:18.1340]

chpasswd: password for user changed

[\*09/27/2023 21:56:18.1350]

chpasswd: password for user changed

[\*09/27/2023 21:56:18.1520] systemd[1]: Starting Cisco rsyslog client watcher...  
[\*09/27/2023 21:56:18.1610] Same LSC mode, no action needed  
[\*09/27/2023 21:56:18.1640] CLSM[00:00:00:00:00:00]: U3 Client RSSI Stats feature is deprecated; can no  
[\*09/27/2023 21:56:18.1720] systemd[1]: Stopping rsyslog client...  
[\*09/27/2023 21:56:18.2120] systemd[1]: Starting Cisco syslog service...  
[\*09/27/2023 21:56:18.2230] systemd[1]: Started Cisco syslog service.  
[\*09/27/2023 21:56:18.2410] systemd[1]: Started rsyslog client.  
[\*09/27/2023 21:56:18.2440] AP is in good condition, BLE is off  
[\*09/27/2023 21:56:18.2510] SET\_SYS\_COND\_INTF: allow\_usb state: 1 (up) condition  
[\*09/27/2023 21:56:18.2530] systemd[1]: Starting dhcpv6 client watcher...  
[\*09/27/2023 21:56:18.2530] systemd[1]: Stopping DHCPv6 client...  
[\*09/27/2023 21:56:18.2530] systemd[1]: Starting DHCPv6 client...  
[\*09/27/2023 21:56:18.2530] systemd[1]: Started DHCPv6 client.  
[\*09/27/2023 21:56:18.2530] systemd[1]: Started dhcpv6 client watcher.  
[\*09/27/2023 21:56:18.2560]

Set radio 0 power 4 antenna mask 15

[\*09/27/2023 21:56:18.2530]

Set radio 1 power 4 antenna mask 15

[\*09/27/2023 21:56:18.2530] Got WSA Server config TLVs  
[\*09/27/2023 21:56:18.2720]

AP tag change to default-policy-tag

[\*09/27/2023 21:56:18.2780] Chip flash OK

## 구성

### 정적 WLC 선택

GUI에서 Configuration(컨피그레이션) > **Wireless(무선)** > **Access Points(액세스 포인트)**로 이동하여 AP를 선택하고 High Availability(고가용성) 탭으로 이동할 수 있습니다. 여기서는 이 문서의 Wireless LAN Controller Selection(무선 LAN 컨트롤러 선택) 섹션에 설명된 대로 1차, 2차 및 3차 WLC를 구성할 수 있습니다. 이 컨피그레이션은 액세스 포인트별로 수행됩니다.

The screenshot displays the Cisco Catalyst 9800-L Wireless Controller GUI. The main navigation pane on the left includes Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The central pane shows the 'All Access Points' table with columns for AP Name, AP Model, and Slots. The right pane shows the 'Edit AP' configuration for 'wlc-9800' under the 'High Availability' tab, with fields for Primary, Secondary, and Tertiary Controller, and AP failover priority.

AP Name	AP Model	Slots
AP70F0.967E.AFAC	C9120AXE-B	2
AP7c0e.ce14.8088	AIR-CAP3702I-N-K9	2
C9120AXI-EMORENOA	C9120AXI-A	2
AP9130AX-luisajim	C9130AXE-A	3
3802-emorenoa	AIR-AP3802I-B-K9	2

Name	Management IP Address (IPv4/IPv6)
Primary Controller	wlc-9800 172.16.5.11
Secondary Controller	
Tertiary Controller	

AP failover priority: Low

AP에 대한 1차, 2차 및 3차 WLC.



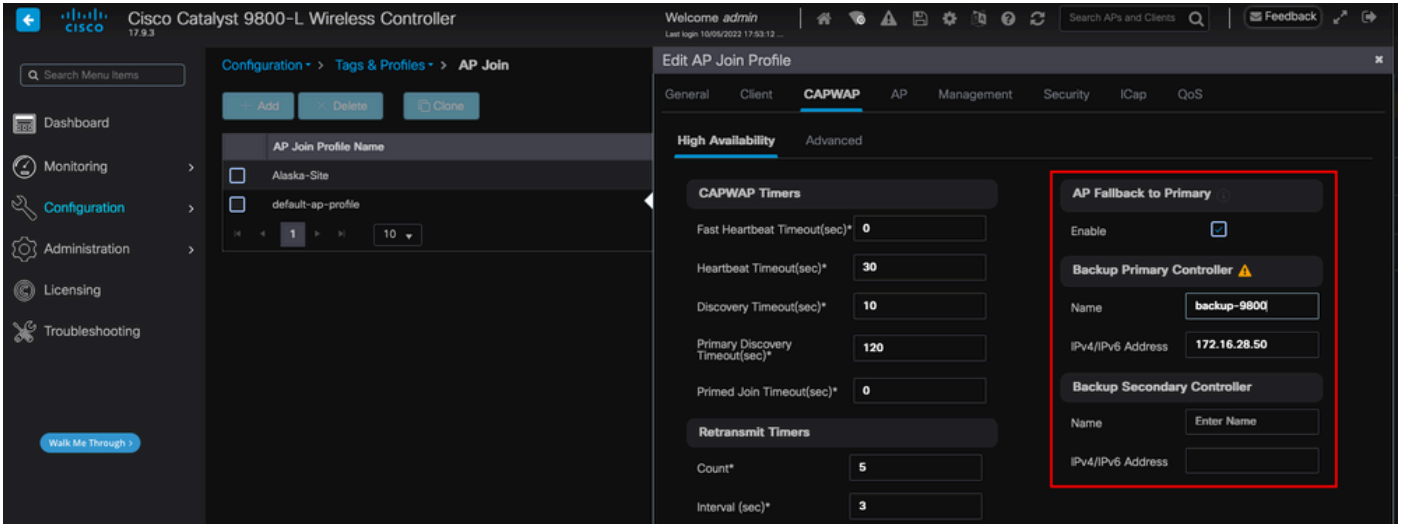
---

**참고:** Cisco IOS XE 17.9.2를 시작하면 Priming Profiles를 사용하여 정규식(regex)과 일치하는 AP 그룹 또는 개별 AP에 대해 1차, 2차 및 3차 컨트롤러를 구성할 수 있습니다. 자세한 내용은 컨피그레이션 [가이드의 AP 프라이밍 프로필 섹션에 구성된 컨트롤러](#)에 대한 [AP](#) 폴백을 참조하십시오.

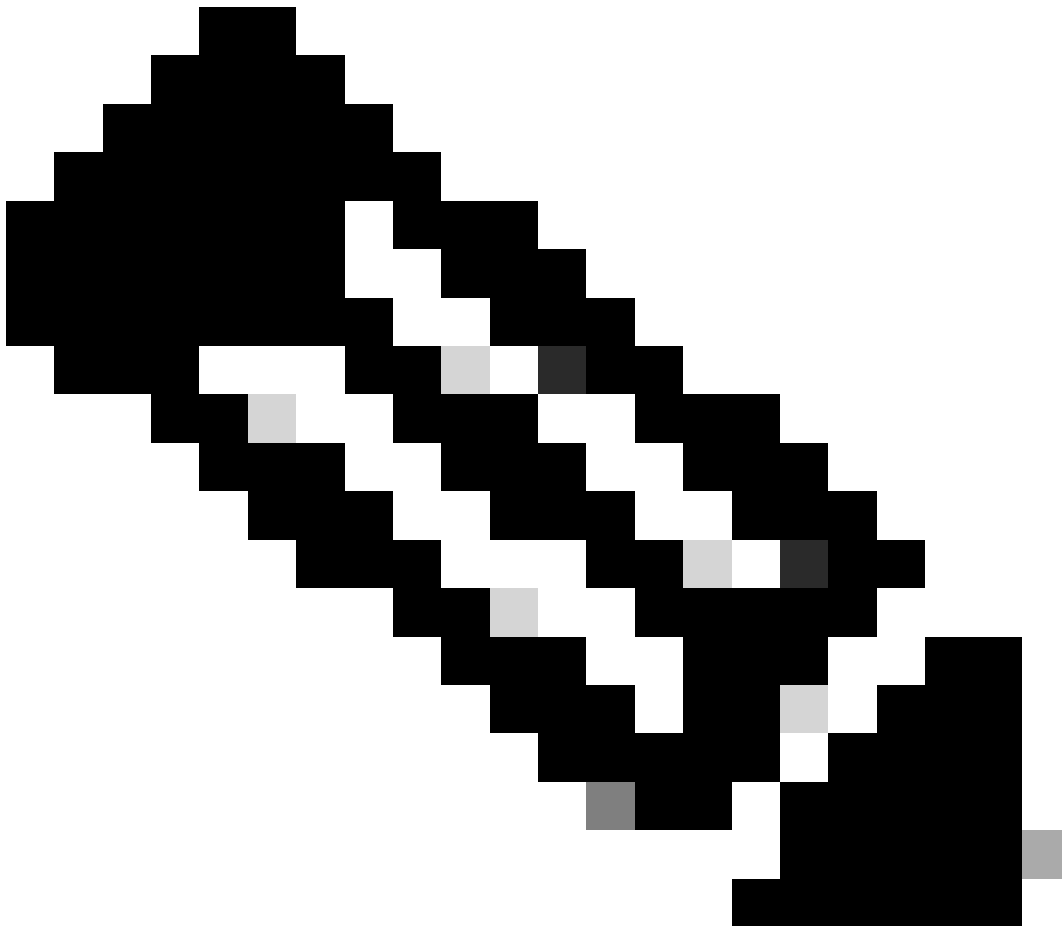
---

AP High Availability(AP 고가용성) 탭에 구성된 기본, 보조 및 3차 컨트롤러는 CAPWAP > **High Availability(고가용성)** 탭 아래의 **AP Join Profile(AP 조인 프로파일)**에 따라 구성할 수 있는 Backup Primary(백업 기본) 및 Secondary(보조) WLC와 다릅니다. 기본, 보조 및 3차 컨트롤러는 우선순위 1, 2 및 3을 가진 WLC로 간주되는 반면, 백업 기본 및 2차 컨트롤러는 우선순위 4 및 5를 가진 WLC로 간주됩니다.

AP 대체가 활성화된 경우 AP는 다른 WLC에 조인할 때 기본 컨트롤러를 능동적으로 검색합니다. CAPWAP 다운 이벤트가 발생하고 백업 기본 및 보조 컨트롤러를 사용할 수 없으면 AP는 우선 순위 4 및 5의 WLC만 검색합니다.



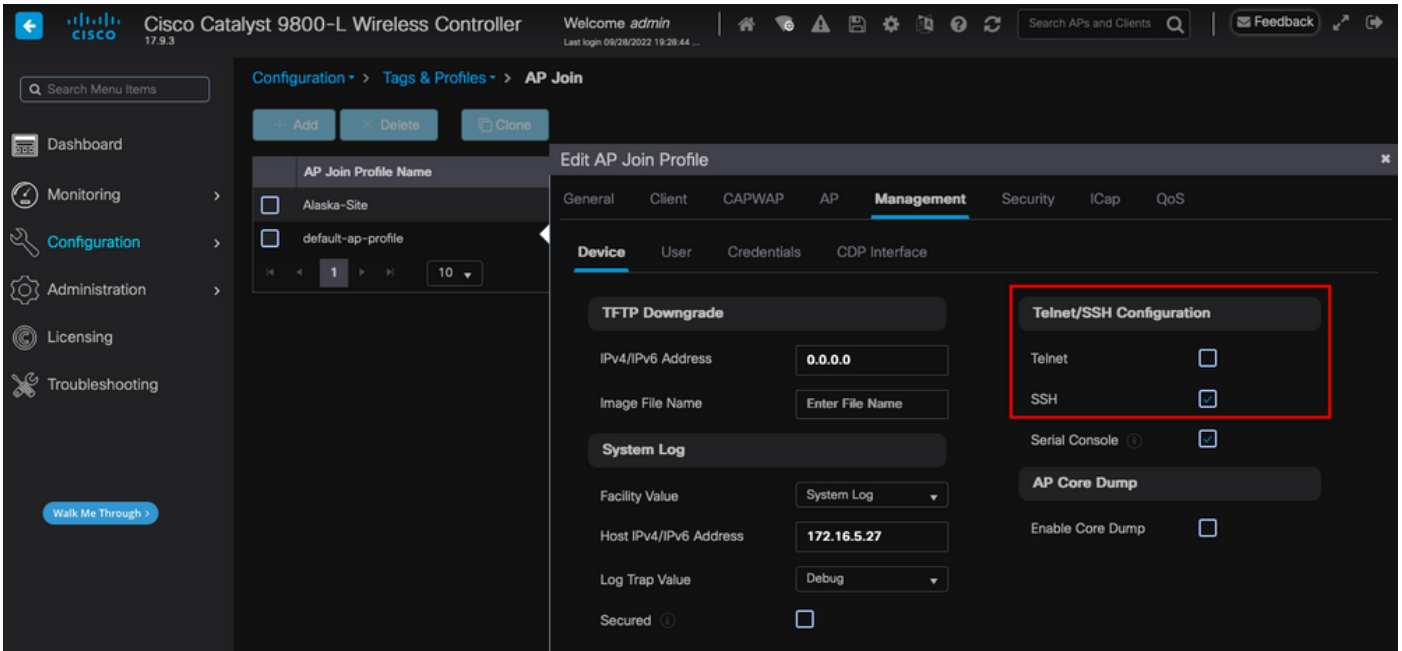
AP 조인 프로파일의 고가용성 옵션



참고: AP 조인 프로파일의 백업 기본 및 백업 보조 WLC의 컨피그레이션은 액세스 포인트의 High Availability(고가용성) 탭의 고정 기본 및 보조 항목을 채우지 않습니다.

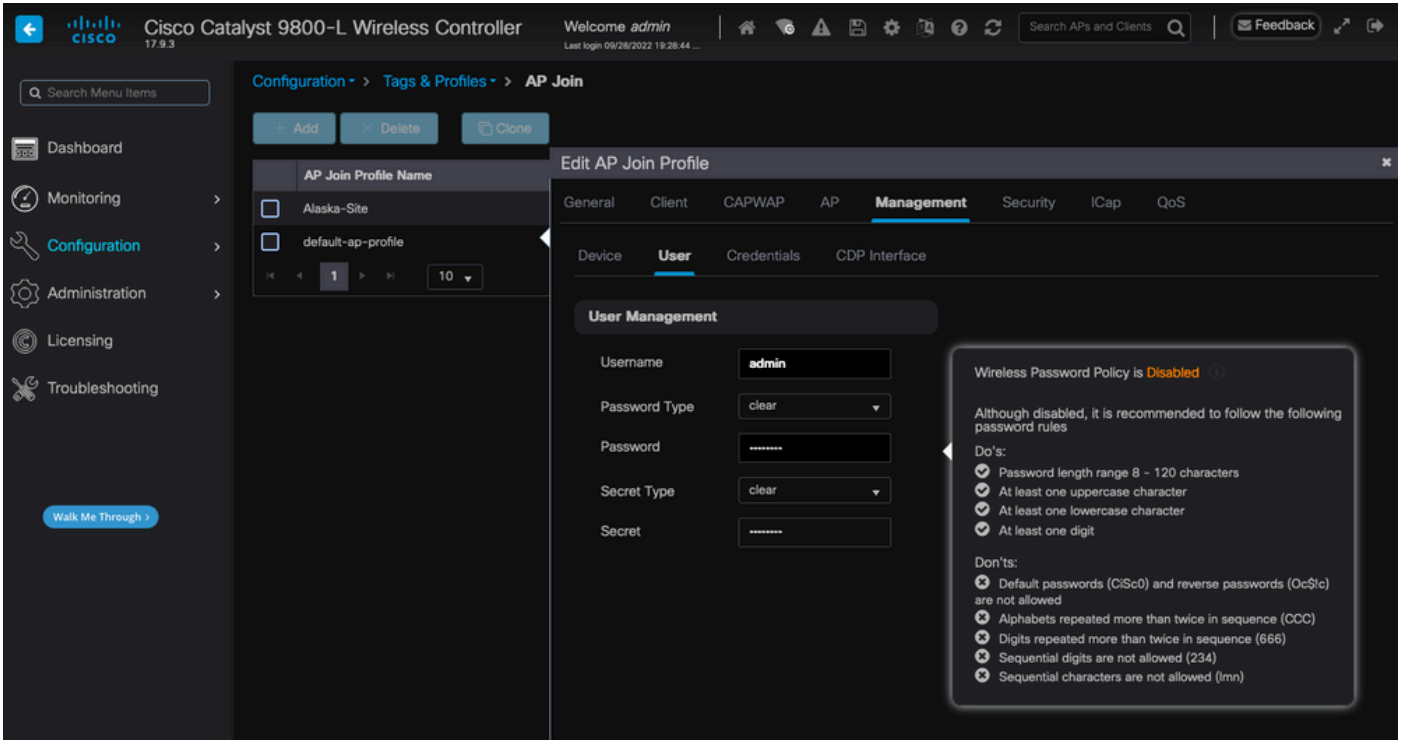
AP에 대한 텔넷/SSH 액세스 활성화

Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로파일) > AP Join(AP 조인) > Management(관리) > Device(디바이스)로 이동하여 SSH 및/또는 Telnet을 선택합니다.



AP 가입 프로파일에서 텔넷/SSH 액세스 활성화

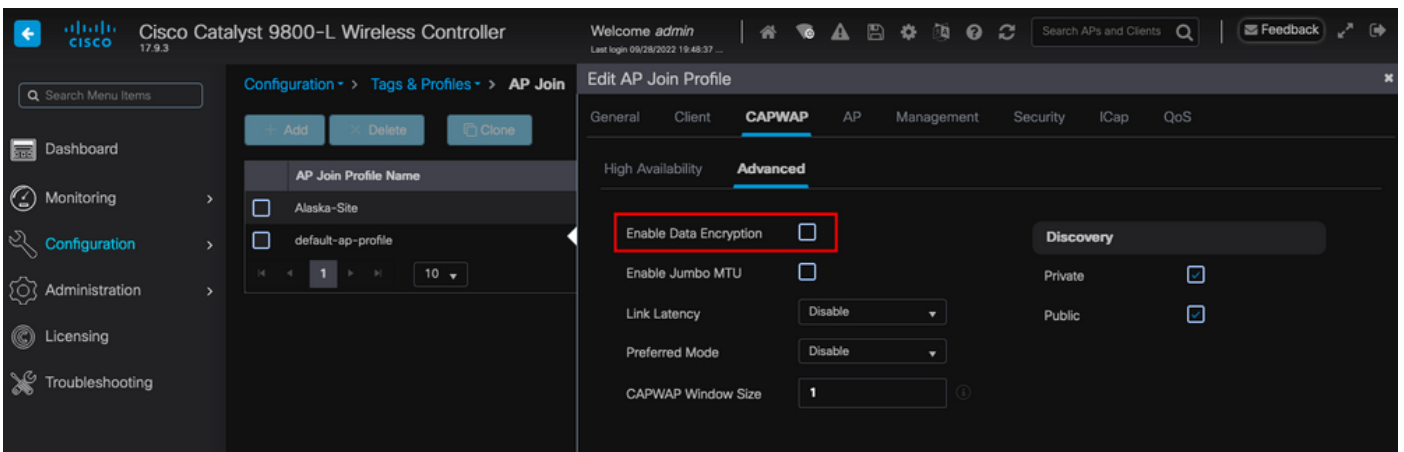
SSH/텔넷 자격 증명을 구성하려면 같은 창에서 User(사용자) 탭으로 이동하여 AP에 액세스할 사용자 이름, 비밀번호 및 비밀을 설정합니다.



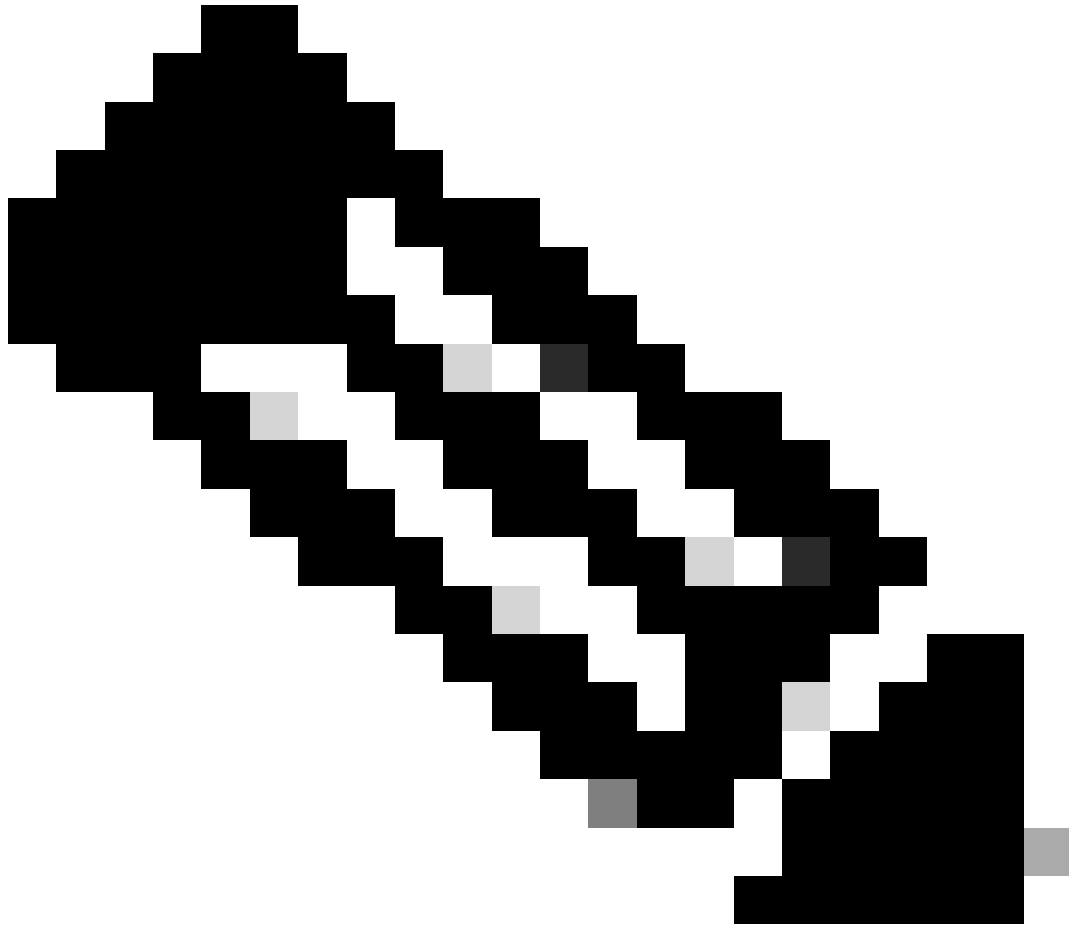
AP에 대한 SSH 및 텔넷 자격 증명

데이터 링크 암호화

AP 트래픽의 패킷 캡처를 수행해야 하는 클라이언트 문제를 해결해야 하는 경우, Configuration(구성) > Tags & Profiles(태그 및 프로필) > AP Join(AP 조인) > CAPWAP > Advanced(고급)에서 Data Link Encryption(데이터 링크 암호화)이 활성화되어 있는지 확인합니다. 그렇지 않으면 트래픽이 암호화됩니다.



데이터 링크 암호화



**참고:** 데이터 암호화는 CAPWAP 데이터 트래픽만 암호화합니다. CAPWAP 제어 트래픽은 DTLS를 통해 이미 암호화되었습니다.

---

다음을 확인합니다.

AP 콘솔에서 CAPWAP 상태 머신을 추적하는 것 외에도 WLC에서 [Embedded Packet Capture를 수행하여](#) AP 조인 프로세스를 분석할 수 있습니다.

No.	Time	Time delta from [Source]	Destination	Protocol	Length	Destination Port	Info
886	12:58:41.288976	0.022802000	172.16.5.65	CAPWAP-Control	294	5246	CAPWAP-Control - Discovery Request
887	12:58:41.288976	0.000000000	172.16.5.11	CAPWAP-Control	147	5267	CAPWAP-Control - Discovery Response
888	12:58:41.388974	0.027998000	172.16.5.65	CAPWAP-Control	294	5246	CAPWAP-Control - Discovery Request
889	12:58:41.388974	0.000000000	172.16.5.11	CAPWAP-Control	147	5267	CAPWAP-Control - Discovery Response
1156	12:58:50.794957	0.195989000	172.16.5.65	DTLSv1.2	276	5246	Client Hello
1157	12:58:50.795948	0.000991000	172.16.5.11	DTLSv1.2	98	5267	Hello Verify Request
1158	12:58:50.796955	0.001007000	172.16.5.65	DTLSv1.2	296	5246	Client Hello
1159	12:58:50.798954	0.001999000	172.16.5.11	DTLSv1.2	125	5267	Server Hello, Certificate (Fragment)
1160	12:58:50.798954	0.000000000	172.16.5.65	DTLSv1.2	562	5267	Certificate (Fragment)
1161	12:58:50.798954	0.000000000	172.16.5.11	DTLSv1.2	562	5267	Certificate (Reassembled), Server Key Exchange (Fragment)
1162	12:58:50.798954	0.000000000	172.16.5.11	DTLSv1.2	349	5267	Server Key Exchange (Reassembled), Certificate Request, Server Hello Done
1163	12:58:50.859948	0.060986000	172.16.5.65	DTLSv1.2	594	5246	Certificate (Fragment)
1164	12:58:50.859948	0.000000000	172.16.5.11	DTLSv1.2	594	5246	Certificate (Reassembled), Client Key Exchange (Fragment)
1181	12:58:51.204975	0.066997000	172.16.5.65	DTLSv1.2	463	5246	Client Key Exchange (Reassembled), Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
1182	12:58:51.205984	0.001000000	172.16.5.11	DTLSv1.2	125	5267	Change Cipher Spec, Encrypted Handshake Message
1328	12:58:55.914945	0.016997000	172.16.5.11	DTLSv1.2	1487	5246	Application Data
1321	12:58:55.916944	0.001999000	172.16.5.11	DTLSv1.2	1484	5267	Application Data
1330	12:58:56.246981	0.109003000	172.16.5.11	DTLSv1.2	1439	5246	Application Data
1331	12:58:56.246981	0.000000000	172.16.5.65	DTLSv1.2	1439	5246	Application Data
1332	12:58:56.246981	0.000000000	172.16.5.11	DTLSv1.2	379	5246	Application Data
1333	12:58:56.247973	0.000992000	172.16.5.11	DTLSv1.2	354	5267	Application Data
1364	12:58:57.292984	0.040999000	172.16.5.65	DTLSv1.2	1439	5246	Application Data
1365	12:58:57.292984	0.000000000	172.16.5.11	DTLSv1.2	690	5246	Application Data
1366	12:58:57.293975	0.000991000	172.16.5.11	DTLSv1.2	354	5267	Application Data
1368	12:58:57.387965	0.069989000	172.16.5.65	DTLSv1.2	902	5246	Application Data
1369	12:58:57.388972	0.001007000	172.16.5.11	DTLSv1.2	402	5267	Application Data
1376	12:58:57.469961	0.001999000	172.16.5.65	DTLSv1.2	148	5246	Application Data
1377	12:58:57.469961	0.000000000	172.16.5.11	DTLSv1.2	103	5267	Application Data
1378	12:58:57.470968	0.001007000	172.16.5.11	CAPWAP-Data	104	5247	CAPWAP-Data Keep-Alive(Malformed Packet)
1379	12:58:57.474966	0.003998000	172.16.5.11	DTLSv1.2	133	5267	Application Data
1380	12:58:57.477972	0.003006000	172.16.5.11	CAPWAP-Data	104	5267	CAPWAP-Data Keep-Alive(Malformed Packet)
1400	12:58:57.546968	0.003997000	172.16.5.65	DTLSv1.2	148	5246	Application Data
1401	12:58:57.546968	0.000000000	172.16.5.11	DTLSv1.2	119	5246	Application Data
1402	12:58:57.547968	0.000992000	172.16.5.11	DTLSv1.2	103	5267	Application Data
1403	12:58:57.547968	0.000000000	172.16.5.11	DTLSv1.2	121	5267	Application Data
1411	12:58:57.575958	0.002998000	172.16.5.65	DTLSv1.2	148	5246	Application Data
1412	12:58:57.575958	0.000000000	172.16.5.11	DTLSv1.2	103	5267	Application Data
1413	12:58:57.577957	0.001999000	172.16.5.65	DTLSv1.2	119	5246	Application Data
1414	12:58:57.577957	0.000000000	172.16.5.11	DTLSv1.2	143	5246	Application Data
1415	12:58:57.577957	0.000000000	172.16.5.65	DTLSv1.2	1190	5267	Application Data
1416	12:58:57.577957	0.000000000	172.16.5.11	DTLSv1.2	103	5267	Application Data
1425	12:58:57.688959	0.078995000	172.16.5.65	DTLSv1.2	119	5246	Application Data
1426	12:58:57.688959	0.000000000	172.16.5.11	DTLSv1.2	148	5246	Application Data
1427	12:58:57.688959	0.000000000	172.16.5.11	DTLSv1.2	119	5267	Application Data
1428	12:58:57.688959	0.000000000	172.16.5.11	DTLSv1.2	103	5267	Application Data
1429	12:58:57.688951	0.000992000	172.16.5.65	DTLSv1.2	119	5246	Application Data
1430	12:58:57.688951	0.000000000	172.16.5.11	DTLSv1.2	222	5246	Application Data
1431	12:58:57.690958	0.001007000	172.16.5.11	DTLSv1.2	175	5267	Application Data
1432	12:58:57.690958	0.000000000	172.16.5.65	DTLSv1.2	103	5267	Application Data
1433	12:58:57.692957	0.001999000	172.16.5.65	DTLSv1.2	119	5246	Application Data
1434	12:58:57.692957	0.000000000	172.16.5.65	DTLSv1.2	111	5246	Application Data

WLC의 임베디드 패킷 캡처에 표시된 AP 조인 프로세스

Chance Cipher Spec 패킷(패킷 번호 1182) 이후의 모든 트래픽은 DTLSv1.2를 통한 애플리케이션 데이터로만 표시되는 방법에 유의하십시오. 이는 모두 DTLS 세션 설정 이후의 암호화된 데이터입니다.

문제 해결

알려진 문제

AP가 WLC에 조인하지 못할 수 있는 알려진 문제를 참조하십시오.

- [Wave 2 및 Catalyst 11ax Access Point\(CSCvx32806\)의 손상된 이미지로 인해 부팅 루프에 있는 AP](#)
- [현장 알림 72424: 2022년 9월부터 제조된 C9105/C9120/C9130 액세스 포인트를 사용하려면 Wireless LAN Controller에 소프트웨어를 업그레이드해야 할 수 있습니다.](#)
- [필드 알림 72524: 소프트웨어 업그레이드/다운그레이드 과정에서 Cisco IOS AP는 인증서 만료로 인해 2022년 12월 4일 이후에도 다운로드 상태를 유지할 수 있습니다. - 소프트웨어 업그레이드를 권장합니다.](#)
- [Cisco 버그 ID CSCwb13784: AP 조인 요청의 경로 MTU가 잘못되어 AP가 9800에 조인할 수 없습니다.](#)
- [Cisco 버그 ID CSCvu22886: C9130: 17.7로 업그레이드할 때 "unlzma: write: No space left on device" 메시지](#)

업그레이드하기 전에 항상 각 버전의 릴리스 노트의 업그레이드 경로 섹션을 참조하십시오.



**참고:** Cisco IOS XE Cupertino 17.7.1부터 Cisco Catalyst 9800-CL Wireless Controller는 스마트 라이선싱이 연결되어 있지 않은 경우 50개가 넘는 AP를 허용하지 않습니다.

---

#### WLC GUI 확인

WLC에서 **Monitoring(모니터링) > Wireless(무선) > AP Statistics(AP 통계) > Join Statistics(조인 통계)**로 이동하면 모든 AP에서 보고한 **마지막 재부팅 사유**와 WLC에서 등록된 **마지막 연결 끊기 사유**를 볼 수 있습니다.

AP Name	AP Model	Status	IP Address	Base Radio MAC	Ethernet MAC	Last Reboot Reason (Reported by AP)	Last Disconnect Reason
9120AP	C9120AXI-A	Red	172.16.5.23	3c41.0a31.7700	6c41.0e16.e79c	No reboot reason	DTLS close alert from peer
jochele9120	C9120AXI-B	Red	172.16.5.61	3c41.0a31.7780	6c41.0e16.e79c	No reboot reason	DTLS close alert from peer
AP19F9.2096.54F0	C9106AXI-B	Red	172.16.5.32	488b.0aa7.7940	1099.2096.54f0	No reboot reason	DTLS close alert from peer
AP72F9.9E76.AFAC	C9120AXI-B	Green	172.16.5.79	7090.9685.7980	7090.9676.afac	Controller reload command	Mode change to sniffer
AP710e.ea14.8088	AR-CA93702I-N-K9	Green	172.16.5.31	710e.ea76.8b00	710e.ea14.8088	Image upgrade successfully	NA
C9120AXI-EMORENCA	C9120AXI-A	Green	172.16.5.65	a49b.cdaa.1980	a49b.c050.a158	Image upgrade successfully	DTLS close alert from peer
BRCTAC0428	C9120AXI-B	Red	172.16.46.35	c884.a172.2600	c884.a165.8530	No reboot reason	DTLS close alert from peer
AP9130AXI-tulajam	C9130AXI-A	Green	172.16.5.67	011d.2a89.d840	7090.9606.4a44	Controller reload command	Mode change to sniffer
3802-emorenea	AR-AP9802I-B-K9	Green	172.16.5.25	802b.cba7.a5c0	286f.76f3.53ae	Controller reload command	Mode change to sniffer

WLC의 AP 조인 통계 페이지

임의의 AP를 클릭하고 AP 가입 통계 세부사항을 확인할 수 있습니다. 여기서는 AP가 마지막으로 가입하고 WLC 검색을 시도한 시간과 날짜 등의 자세한 정보를 볼 수 있습니다.

### Access Point Statistics Summary

Is the AP currently connected to controller	NOT JOINED
Time at which the AP joined this controller last time	09/27/2022 09:45:49
Type of error that occurred last	Join
Time at which the last join error occurred	09/27/2022 09:46:01

### Discovery Phase Statistics

Discovery requests received	106
Successful discovery responses sent	106
Unsuccessful discovery request processing	NA
Reason for last unsuccessful discovery attempt	None
Time at last successful discovery attempt	09/27/2022 09:52:27
Time at last unsuccessful discovery attempt	NA

### Last AP Disconnect Details

Reason for last AP connection failure	DTLS close alert from peer
Last Reboot Reason (Reported by AP)	No reboot reason

### Last AP message decryption failure details

Reason for last message decryption failure	NA
--	----

일반 AP 가입 통계

자세한 내용을 보려면 같은 창의 Statistics(통계) 탭으로 이동하십시오. 여기에서 전송된 조인 응답의 양과 수신된 조인 요청의 양을 비교할 수 있으며, 전송된 구성 응답과 수신된 구성 요청을 비교할 수 있습니다 있습니다 있습니다 있습니다입니다입니다



## Join Statistics

General

**Statistics**

### Control DTLS Statistics

DTLS Session request received	8
Established DTLS session	8
Unsuccessful DTLS session	0
Reason for last unsuccessful DTLS session	DTLS Handshake Success
Time at last successful DTLS session	09/27/2022 09:45:44
Time at last unsuccessful DTLS session	NA

### Join phase statistics

Join requests received	8
Successful join responses sent	8
Unsuccessful join request processing	0
Reason for last unsuccessful join attempt	DTLS close alert from peer
Time at last successful join attempt	09/27/2022 09:45:49
Time at last unsuccessful join attempt	NA

### Configuration phase statistics

Configuration requests received	15
Successful configuration responses sent	15
Unsuccessful configuration request processing	0
Reason for last unsuccessful configuration attempt	NA
Time at last successful configuration attempt	09/21/2022 01:39:07
Time at last unsuccessful configuration attempt	NA

### Data DTLS Statistics

DTLS Session request received	0
Established DTLS session	0
Unsuccessful DTLS session	0
Reason for last unsuccessful DTLS session	DTLS Handshake Success
Time at last successful DTLS session	NA
Time at last unsuccessful DTLS session	NA

자세한 AP 가입 통계

명령

다음 명령은 AP 조인 문제를 해결하는 데 유용합니다.

WLC에서

- ap 요약 표시
- 디버그 capwap 오류
- debug capwap 패킷

Wave 2 및 Catalyst 11ax AP

- debug capwap client events
- 디버그 capwap 클라이언트 오류
- dtls 클라이언트 오류 디버그
- dtls 클라이언트 이벤트 디버그
- debug capwap client keepalive
- capwap 재시작 테스트
- capwap ap erase all

#### Wave 1 AP에서

- debug capwap console cli
- debug capwap client no-reload
- dtls 통계 표시
- cawap ap all-config 지우기



**참고:** 문제 해결을 위해 텔넷/SSH를 통해 AP에 연결할 경우, AP에서 디버그를 활성화한 후 문제를 재현하면서 항상 명령 터미널 모니터를 실행하십시오. 그렇지 않으면 디버그의 출력을 볼 수 없습니다.

---

#### 방사선 흔적

AP 가입 문제를 해결할 때 좋은 시작 지점은 가입 문제가 있는 AP의 무선 및 이더넷 MAC 주소의 방사성 추적을 모두 사용하는 것입니다. 이러한 로그 생성에 [대한](#) 자세한 [내용은 Catalyst 9800 WLC의 디버그 및](#) 로그 수집을 참조하십시오.

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.