

IOS AP 이미지 다운로드가 2022년 12월 4일에 게시된 만료된 이미지 서명 인증서로 인해 실패함 (CSCwd80290)

목차

[소개](#)

[영향을 받는 제품](#)

[문제](#)

[근본 원인](#)

[증상](#)

[AireOS WLC에서](#)

[IOS-XE C9800 WLC에서](#)

[SHA-1 AP\(2014년 중반 이전에 제조\):](#)

[SHA-2 AP\(2014년 중반 이후 제조\):](#)

[해결 방법](#)

[고정 소프트웨어로 업그레이드](#)

[AireOS WLC에서](#)

[IOS-XE 9800 WLC에서](#)

[FAQ\(자주 묻는 질문\)](#)

소개

이 문서에서는 2022년 12월 4일 이후 AireOS 및 C9800 WLC(Wireless LAN Controller)에서 발생한 IOS AP(액세스 포인트) 조인 실패에 대한 세부 정보를 제공합니다. 이 문제는 Cisco 버그 [CSCwd80290](#) 및 Field Notice [FN725240](#)에 의해 추적되며 AP 이미지 서명 인증서 검증 실패로 인해 발생합니다.

영향을 받는 제품

이 문제는 IOS를 실행하는 모든 경량형 액세스 포인트에 영향을 미칩니다. 여기에는 802.11ac Wave 1 AP(IW3702/3700/2700/1700/1570 시리즈) 및 700/1530/1550/3600/2600/1600/3500/AP802/AP803 시리즈를 포함하는 이전 AP가 포함됩니다. 영향을 받는 경량 IOS 이미지는 2012년 12월부터 2022년 11월까지 제작되었습니다. AireOS, Catalyst 9800 Series 및 Converged Access Controller가 영향을 받습니다. AP-COS(802.11ac Wave 2, Wi-Fi 6, Wi-Fi 6E AP)를 실행하는 AP는 영향을 받지 않으며 자동 모드의 IOS AP도 영향을 받지 않습니다.

문제

IOS AP가 CAPWAP를 통해 업그레이드되거나 다운그레이드되는 경우, 2022년 12월 4일 이후에는 이미지 다운로드 루프에 걸려서 다운로드된 이미지에서 서명 인증서의 유효성 검사에 실패하여 WLC에 조인하지 못할 수 있습니다.

근본 원인

AP IOS 이미지에 번들로 제공된 이미지 서명 인증서는 2012년 12월 4일에 발급되었으며 2022년 12월 4일에 만료되었습니다. IOS AP는 AP에 소프트웨어를 설치하기 전에 이 인증서를 사용하여 WLC에서 다운로드한 이미지를 검증합니다. 따라서 2022년 12월 4일 이후 AP가 소프트웨어 업그레이드/다운그레이드로 인해 또는 서로 다른 버전을 실행하는 WLC 간 이동으로 인해 코드를 다운로드할 때 AP는 이미지의 유효성을 검사하지 못하고 이미지 다운로드 루프에 무기한 남아 있게 됩니다. 모든 AireOS 및 IOS-XE 버전에서 문제가 나타납니다.

증상

이 문제가 발생하고 있는지 확인하려면 먼저 WLC에서 AP가 Downloading(다운로드 중) 상태에 머물러 있는지 확인합니다. 그런 다음 문제를 긍정적으로 식별하려면 영향을 받는 AP에 대한 ssh, 텔넷 또는 콘솔을 사용하여 로그를 확인하거나 syslog 서버에서 AP 로그를 확인합니다.

AireOS WLC에서

WLC에서 show ap image status (AireOS 8.10)는 영향받는 AP가 "Downloading" 상태로 표시됩니다.

8.5에서는 "Downloading"에서 0이 아닌 개수의 AP를 표시하는 show ap image all을 사용합니다.

```
(AireOS WLC-8.5) >show ap image all
```

```
Total number of APs..... 1
Number of APs
  Initiated..... 0
  Downloading..... 1
  Predownloading..... 0
  Completed predownloading..... 0
  Not Supported..... 0
  Failed to Predownload..... 0
```

AP Name	Primary Image	Backup Image	Predownload Status	Predownload Version	Next Retry Time	Retry
AP1700	8.5.182.0	0.0.0.0	None	None	NA	NA

```
(AireOS WLC-8.10) >show ap image status
```

```
Total number of APs..... X
Total AP's Downloading..... 1
AP Name      Primary Image  Download Status
-----
CAP3702E.4CD4  17.3.6.76     Downloading
```

IOS-XE C9800 WLC에서

C9800#ap 요약 표시

9800-L#show ap summary

AP Name	Slots	AP Model	Ethernet MAC	Radio MAC	Location
AP2702E	2	2702E	0081.c4fb.2e74	843d.c673.10d0	default location

이 문제가 발생할 때 AP 로그에 다음과 유사한 오류가 표시됩니다.

SHA-1 AP(2014년 중반 이전에 제조):

```
*Dec 6 21:35:24.259: Using SHA-1 signed certificate for image signing validation.  
*Dec 6 21:35:24.327: %PKI-3-CERTIFICATE_INVALID_EXPIRED: Certificate chain validation has failed. The c  
*Dec 6 21:35:24.327: Image signing certificate validation failed (1A).  
*Dec 6 21:35:24.327: Failed to validate signature  
*Dec 6 21:35:24.327: Digital Signature Failed Validation (flash:/update/ap3g2-k9w8-mx.153-3.JPJ9/final  
*Dec 6 21:35:24.327: AP image integrity check FAILED
```

SHA-2 AP(2014년 중반 이후 제조):

```
*Dec 6 08:47:20.159: Using SHA-2 signed certificate for image signing validation.  
*Dec 6 08:47:20.223: DTLS_CLIENT_ERROR: ../capwap/base_capwap/dtls/base_capwap_dtls_record.c:169 Pkt to  
*Dec 6 08:47:20.227: %PKI-3-CERTIFICATE_INVALID_EXPIRED: Certificate chain validation has failed. The c  
*Dec 6 08:47:20.227: Image signing certificate validation failed (1A).  
*Dec 6 08:47:20.231: Failed to validate signature  
*Dec 6 08:47:20.231: Digital Signature Failed Validation (flash:/update/ap3g2-k9w8-mx.153-3.JPJ7c/final  
*Dec 6 08:47:20.231: AP image integrity check FAILED
```

해결 방법

고정 소프트웨어를 실행하고 있지 않은 경우 다음 단계에 따라 IOS AP가 참여할 수 있도록 허용합니다.

1. 컨트롤러가 자동으로 시간 앞으로 설정하지 못하게 하려면 NTP를 비활성화합니다.

```
AireOS:  
(AireOS WLC)>show time
```

make a note of all configured NTP servers, and delete each one:

```
(AireOS WLC)>config time ntp delete
```

```
IOS-XE: C9800#show run | i ntp ntp server ip
```

```
C9800#config terminal (config)#no ntp server ip
```

```
! for each configured NTP server
```

2. 컨트롤러 또는 최신 AP의 인증서가 무효화될 수 있으므로 WLC의 날짜를 2022년 12월 4일 이전이지만 2022년 11월 1일 이전으로 변경합니다.

```
(AireOS WLC)> config time manual 12/02/22 00:00:00
```

```
C9800#clock set 00:00:00 2 Dec 2022
```

3. WLC의 시간이 변경되었는지 확인합니다.

```
(AireOS WLC)> show time
```


```
Time..... Fri Dec 2 00:00:02 2022
```

```
C9800#show clock
```

```
00:00:02.573
```

```
Fri Dec 2 2022
```

4. 모든 AP가 새 이미지를 사용하여 Registered(등록됨) 상태로 나타날 때까지 기다립니다.

 참고: 경우에 따라 날짜 변경 후 AP를 재부팅해야 AP가 조인되는 경우가 있습니다. 그러나 AP를 재부팅하기 전에 AP가 다시 참여할 수 있도록 30분 이상 기다려 주십시오

5. NTP를 다시 활성화합니다

```
(AireOS WLC)>config time ntp server 1
```

```
C9800#configure terminal (config)#ntp server ip
```

6. 구성을 저장합니다.

```
(AireOS WLC)>save config  
Are you sure you want to save? (y/n) y
```

```
C9800#write memory
```

7. WLC에서 시계 재확인

```
(AireOS WLC)>show time  
C9800# show clock
```

고정 소프트웨어로 업그레이드

AireOS WLC에서

1. AP 다운로드가 중단된 경우, 소프트웨어로 업그레이드하기 전에 AP가 다운로드를 완료하고 등록 상태로 올라올 수 있도록 컨트롤러 시간을 다시 설정합니다.
 1. 뒤로 시간을 설정하는 방법에 대한 자세한 내용은 위의 해결 방법을 참조하십시오
 2. 작동 상의 이유로 시간을 다시 설정할 수 없는 경우, 이를테면 스위치포트를 종료하거나 CAPWAP를 차단하기 위해 ACL을 설치하여 해당 IOS AP가 컨트롤러 가입을 시도하는 것을 차단합니다.
2. 어떤 AP도 다운로드 상태가 아니므로 WLC의 시간이 현재 시간으로 설정되어 있는지 확인합니다(NTP 다시 활성화).
3. AireOS WLC에 고정 소프트웨어(8.10.183.0 이상 또는 8.5에서 업그레이드할 수 없는 경우 8.5.182.7, 8.5 메인라인 또는 8.5.182.105(8.5 IRCM용)를 설치합니다. 아래 링크를 참조하여 고정 소프트웨어를 다운로드하십시오.
 - 8.10
 - 8540:
<https://software.cisco.com/download/home/286284728/type/280926587/release/8.10.183.0>
 - 5520:
<https://software.cisco.com/download/home/286284738/type/280926587/release/8.10.183.0>
 - 3504:
<https://software.cisco.com/download/home/286312601/type/280926587/release/8.10.183.0>
 - vWLC:
<https://software.cisco.com/download/home/284464214/type/280926587/release/8.10.183.0>
 - 8.5 (숨겨진 게시물)
 - 8.5.182.7(8.5 메인라인):
<https://software.cisco.com/download/specialrelease/8f166c6d88b9f77aabb63f78affa9749>.
 - 8.5.182.105(8.5 IRCM):
<https://software.cisco.com/download/specialrelease/bc334964055fbd9440834f008e5aca34>.
4. (선택 사항) 재부팅하기 전에 조인된 AP에 고정 소프트웨어를 미리 다운로드합니다.
5. WLC를 재부팅합니다.
6. AP 스위치포트를 종료하거나 CAPWAP를 차단한 경우, IOS AP가 다시 가입하고 업그레이드할 수 있도록 블록을 제거합니다.

IOS-XE 9800 WLC에서

1. 17.3.6, 17.6.4, 17.9.2 IOS-XE 소프트웨어를 9800 플래시에 다운로드합니다. 사용 중인 환경의 AP 모델 및 [사용 중인 기능](#)에 따라 해당 환경에 가장 적합한 버전을 선택하려면 [C9800 WLC](#)용 권장 IOS-XE 릴리스를 참조하십시오.
2. 9800 플래시에 17.3.6 APSP7 또는 17.6.4 APSP1 또는 17.9.2 APSP1 파일(IOS AP 수정 포함)을 다운로드합니다.

- 17.3.6: CSCwd83653/CSCwe10047을 통한 17.3.6 APSP7(APSP2 및 APSP5에도 수정 사항 포함)

9800-40: <https://software.cisco.com/download/home/286316412/type/286325254/release/17.3.6>

9800-80: <https://software.cisco.com/download/home/286321396/type/286325254/release/17.3.6>

9800-CL:

<https://software.cisco.com/download/home/286322605/type/286325254/release/17.3.6>

9800-L: <https://software.cisco.com/download/home/286323430/type/286325254/release/17.3.6>

- 17.6.4: CSCwd를 통한 17.6.4 APSP1(IW3702의 [경우87305](#))

9800-40: <https://software.cisco.com/download/home/286316412/type/286325254/release/17.6.4>

9800-80: <https://software.cisco.com/download/home/286321396/type/286325254/release/17.6.4>

9800-CL:

<https://software.cisco.com/download/home/286322605/type/286325254/release/17.6.4>

9800-L: <https://software.cisco.com/download/home/286323430/type/286325254/release/17.6.4>

- CSCwd를 통해 17.9.2:17.9.2 APSP1(IW3702의 [경우87612](#))

9800-40: <https://software.cisco.com/download/home/286322605/type/286325254/release/17.9.2>

9800-80: <https://software.cisco.com/download/home/286321396/type/286325254/release/17.9.2>

9800-CL:

<https://software.cisco.com/download/home/286322605/type/286325254/release/17.9.2>

9800-L: <https://software.cisco.com/download/home/286323430/type/286325254/release/17.9.2>



참고:

- 1) 17.3.6 APSP7에는 CSCwd를 비롯하여 여러 버그(CSCvx32806, CSCwc32182, CSCvz99036, CSCwd37092, CSCwc78435, [CSCwc88148](#))에 대한 수정 사항이 포함되어 있습니다80290
- 2) 17.6.4 APSP1에는 CSCwd80290(IW3700의 경우) 외에도 여러 버그(CSCwc73090, CSCwc71198, CSCwc78435, [CSCwd40731](#), [CSCvx32806](#))에 대한 수정 사항이 포함되어 있습니다.

3. 17.3.6이 이미 설치되어 있지 않으면 지금 17.3.6 IOS-XE를 설치하고 다시 로드합니다.

```
C9800#install add file bootflash:/C9800-L-universalk9_wlc.17.03.06.SPA.bin activate commit
```

4. 9800이 재부팅된 후 - 컨트롤러 시간이 다시 설정된 경우 시간을 현재(NTP 다시 활성화)로 설정

합니다.

5 IOS AP를 복구하려면 APSP7을 설치합니다.

```
C9800#install add file bootflash:/C9800-universalk9_wlc.17.03.06.CSCwe10047 .SPA.apsp.bin
C9800#install activate file bootflash:/C9800-universalk9_wlc.17.03.06.CSCwe10047 .SPA.apsp.bin
C9800#install commit
```

FAQ(자주 묻는 질문)

- 이 문제로 인해 현재 등록된 AP의 연결이 끊기거나 가입에 실패합니까?
WLC와 동일한 버전을 실행 중인 AP는 문제 없이 계속 작동하며 정상적으로 부팅하고 조인합니다. 이 문제는 이미지 업그레이드의 일부로 수행되는 이미지 검증 프로세스에만 영향을 줍니다.
- AP 사전 다운로드가 영향을 받습니까?

예. AP 사전 다운로드에는 AP로 이미지를 다운로드하고 AP에서 이미지를 검증하는 작업이 포함되므로 만료된 동일한 인증서와 이미지 검증 실패가 발생합니다.

- 시간 변화에 따른 서비스 영향은 무엇입니까? 고객이 정오에 이 작업을 수행할 수 있습니까? 아니면 다운타임이 발생하고 서비스에 영향을 미치는 유지 보수 기간을 예약해야 합니까?
컨트롤러 시간을 변경해도 AP 조인 및 무선 클라이언트 연결에는 영향을 미치지 않습니다. 그러나 DNA Center Assurance, CMX 및 Cisco (DNA) Spaces가 영향을 받을 수 있습니다. AP가 연결되고 시간이 현재 시간으로 설정되면 이러한 서비스가 복구될 것으로 예상됩니다.
- 프로덕션 컨트롤러에 시간을 다시 설정할 수 없는 경우 어떻게 해야 합니까?
프로덕션 WLC와 동일한 코드 버전으로 스테이징 WLC(vWLC 또는 9800-CL도 작동)를 설정합니다. 스테이징 WLC에서 시간을 되돌리고 AP를 스테이징 WLC에 조인합니다. AP가 코드를 다운로드하고 스테이징 WLC에서 Registered 상태로 이동하면 AP를 프로덕션 WLC로 이동합니다.
- 고정 버전을 설치하려면 시간을 변경해야 합니까?

AireOS에서만 AP가 다운로드 상태에서 멈춘 경우 자세한 내용은 고정 소프트웨어로 업그레이드 섹션을 참조하십시오.

- 새 AP를 추가하면 어떻게 됩니까?
새 AP가 컨트롤러와 동일한 버전으로 설치된 경우 AP는 문제 없이 연결해야 합니다. 반면, 버전이 일치하지 않으면 AP는 해당 이미지를 다운로드하려고 시도합니다. 컨트롤러의 코드에 고정 AP 번들 이미지가 없는 경우, AP는 설명된 대로 업그레이드에 실패하며 해결 방법이 필요합니다.
컨트롤러가 고정 버전 중 하나로 업그레이드된 경우 새 AP를 정상적으로 추가하고 업그레이드 프로세스를 완료할 수 있습니다.
- RMA에서 받은 유닛에 대해서는 어떻게 됩니까?

이는 새 AP를 추가하는 것과 같습니다. AP 이미지 픽스와 함께 컨트롤러 버전을 실행 중인 경우, 해당 AP는 정상적으로 가입하고 업그레이드됩니다. 그렇지 않은 경우 시간 해결 방법을 적용합니다.

- 운영을 위해 수정된 시간을 그대로 유지해야 하나요?
아니요. AP가 업그레이드 프로세스를 완료하면 컨트롤러를 현재 시간으로 다시 설정하고 NTP를 다시 활성화할 수 있습니다.
- AP 로그 %PKI-3-CERTIFICATE_INVALID_NOT_YET_VALID에 이 오류가 있습니다. 인증서 체인 검증에 실패했습니다. 인증서(SN: xx)가 아직 유효하지 않습니다. 유효 기간은 HH:MM:SS UTC Mar 1 2022"에 시작합니다. 같은 증상인가요, 새로운 증상인가요?

이 오류는 WLC의 시계가 인증서의 시작 날짜인 2022년 3월 1일 이후로 설정되어 있음을 나타냅니다(이 경우). 이 날짜는 WLC를 제조한 시기 또는 가상 WLC의 자체 서명 인증서가 생성된 시기에 따라 달라집니다.

WLC의 시계를 수정하여 인증서를 유효하게 만듭니다.

- 이 문제가 재발하지 않도록 Cisco는 어떤 조치를 취하고 있습니까?
감지되지 않았을 수 있는 유사한 문제를 파악하고 시정 조치를 이행하기 위해 모든 엔터프라이즈 제품에 대한 전체 감사를 완료합니다
또한 이 문제를 해결하기 위해 IOS AP 이미지 번들 프로세스에 변경 사항이 적용되었습니다.

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.