Catalyst 9800 컨트롤러 업그레이드 및 다운그레이드: 팁과 요령

목차

소개

이 문서에서는 Catalyst 9800 WLC(Wireless LAN Controller)를 업그레이드하거나 다운그레이드할 때 주의해야 할 사항에 대해 설명합니다.

계속 진행하기 전에

이 문서에서는 업그레이드할 때 항상 GO-TO 문서여야 하는 릴리스 노트를 교체하는 것을 목적으로 하지 않습니다. 릴리스 간에 가장 큰 영향을 미치는 변경 사항을 강조 표시하여 여러 릴리스를 통해 업그레이드를 용이하게 하는 데 목적이 있습니다.

이 문서는 대상 소프트웨어 릴리스의 릴리스 정보를 읽는 것을 대체하지 않습니다. 업그레이드를 진행하기 전에 컨피그레이션을 백업하고 필요한 모든 예방 조치를 취하십시오.

기본적으로 9800의 HTTP 서버는 업그레이드 후 변경이 가능한 특정 인증서/신뢰 지점에 정적으로 매핑되지 않습니다. 업그레이드하기 전에 컨피그레이션에서 HTTP 서버를 고정 신뢰 지점(목적에 따라 발급한 인증서 또는 기타 MIC 인증서)으로 설정합니다.

엔지니어링 특수 버전의 특수 사례

엔지니어링 특수 빌드에서는 ISSU 업그레이드를 지원하지 않습니다. 이 문서에서는 Cisco.com에 게시된 공개 릴리스에만 초점을 맞춥니다. 따라서 엔지니어링 특수 빌드 중이라면 업그레이드 관련 질문에 대한 지원을 받으려면 함께 받은 릴리스 노트를 참조하십시오.

업그레이드

목표로 하는 대상 소프트웨어 버전 아래의 메모를 직접 읽을 수 있습니다. 여러 릴리스를 통해 적용할 수 있는 팁은 사용자의 편의를 위해 매번 반복됩니다. 한 번에 3개 이상의 릴리스를 통해 업그레이드하지 마십시오. 예를 들어, 16.12.1에서 17.3.2로 업그레이드하는 경우를 이 문서에서 다루지만, 16.12에서 17.4로의 업그레이드는 다루지 않습니다. 이러한 시나리오에서는 17.3을 탐색하고 17.3 섹션의 메모를 확인한 다음 업그레이드를 수행한 다음 17.4 섹션을 살펴보고 두 번째 업그레이드를 준비합니다. 결론적으로, 주요 릴리스가 3개 릴리스된 후에는 더 이상 팁을 반복하지 않습니다. 주요 릴리스를 중간 릴리스로 진행하는 것으로 가정하기 때문에, 여전히 유효하더라도 마찬가지입니다.

지브롤터

16.12.2

- Cisco IOS® XE Gibraltar 16.12.2s에서 기본 정책 태그 아래의 기본 정책 프로필에 대한 자동

WLAN 매핑이 제거되었습니다. Cisco IOS XE Gibraltar 16.12.2s 이전 릴리스에서 업그레이드하는 경우, 그리고 무선 네트워크에서 기본 정책 태그를 사용하는 경우 기본 매핑 변경으로 인해 중단됩니다. 네트워크 작업을 복원하려면 기본 정책 태그 아래에 정책 매핑에 필요한 WLAN을 추가합니다.

- AP 이름에는 31자 이상을 사용하지 마십시오. AP 이름이 32자 이상이면 컨트롤러 충돌이 발생할 수 있습니다.

- OVA 파일을 VMware ESXi 6.5에 직접 구축하지 마십시오. OVF 툴을 사용하여 OVA 파일을 구축하는 것이 좋습니다.

16.12.3

- 16.12.3은 설명서에 지원 대상으로 나와 있는 SFP만 지원하는 첫 번째 릴리스입니다. 목록에 없는 SFP로 인해 포트 다운(port-down) 상황이 발생합니다. 업그레이드 후 데이터 포트가 다운되지 않도록 지원되는 SFP 목록을 확인하고 SFP가 호환되는지 확인합니다.
- 16.12.1 릴리스에 있는 경우 이 릴리스의 업그레이드 파일이 너무 커서 HTTP 업로드(웹 UI 업그레이드 수행 시)에 적합하지 않을 수 있습니다. 다른 전송 방법을 사용하거나 웹 UI를 통해 대용량 파일을 업로드할 수 있도록 지원하는 16.12.2를 계속 진행합니다.
- Cisco IOS XE Gibraltar 16.12.2s에서 기본 정책 태그 아래의 기본 정책 프로필에 대한 자동 WLAN 매핑이 제거되었습니다. Cisco IOS XE Gibraltar 16.12.2s 이전 릴리스에서 업그레이드하는 경우, 그리고 무선 네트워크에서 기본 정책 태그를 사용하는 경우 기본 매핑 변경으로 인해 중단됩니다. 네트워크 작업을 복원하려면 기본 정책 태그 아래에 정책 매핑에 필요한 WLAN을 추가합니다.

- AP 이름에는 31자 이상을 사용하지 마십시오. AP 이름이 32자 이상이면 컨트롤러 충돌이 발생할 수 있습니다.

- OVA 파일을 VMware ESXi 6.5에 직접 구축하지 마십시오. OVA 파일을 구축하려면 OVF 툴을 사용하는 것이 좋습니다.

16.12.4

- 16.12.3 및 17.2.1은 설명서에 지원 대상으로 나와 있는 SFP만 지원하는 첫 번째 릴리스입니다. 목록에 없는 SFP로 인해 포트 다운(port-down) 상황이 발생합니다. 업그레이드 후 데이터 포트가 다운되지 않도록 지원되는 SFP 목록을 확인하고 SFP가 호환되는지 확인합니다.
- 16.12.1 릴리스에 있는 경우 이 릴리스의 업그레이드 파일이 너무 커서 HTTP 업로드(웹 UI 업그레이드 수행 시)에 적합하지 않을 수 있습니다. 다른 전송 방법을 사용하거나 웹 UI를 통해 대용량 파일을 업로드할 수 있도록 지원하는 16.12.2를 계속 진행합니다.
- Cisco IOS XE Gibraltar 16.12.2s에서 기본 정책 태그 아래의 기본 정책 프로필에 대한 자동 WLAN 매핑이 제거되었습니다. Cisco IOS XE Gibraltar 16.12.2s 이전 릴리스에서 업그레이드하는 경우, 그리고 무선 네트워크에서 기본 정책 태그를 사용하는 경우 기본 매핑 변경으로 인해 중단됩니다. 네트워크 작업을 복원하려면 기본 정책 태그 아래에 정책 매핑에 필요한 WLAN을 추가합니다.

- AP 이름에는 31자 이상을 사용하지 마십시오. AP 이름이 32자 이상이면 컨트롤러 충돌이 발생할 수 있습니다.

- OVA 파일을 VMware ESXi 6.5에 직접 구축하지 마십시오. OVA 파일을 구축하려면 OVF 툴을 사용하는 것이 좋습니다.

16.12.5, 16.12.6a 및 16.12.7

16.12.4 릴리스와 동일합니다.

암스테르담

17.1.1

- 16.12.1 릴리스에 있는 경우 이 릴리스의 업그레이드 파일이 너무 커서 HTTP 업로드(웹 UI 업그레이드 수행 시)에 적합하지 않을 수 있습니다. 다른 전송 방법을 사용하거나 웹 UI를 통해 대용량 파일을 업로드할 수 있도록 지원하는 16.12.2를 계속 진행합니다.
- Cisco IOS XE Gibraltar 16.12.2s에서 기본 정책 태그 아래의 기본 정책 프로필에 대한 자동 WLAN 매핑이 제거되었습니다. Cisco IOS XE Gibraltar 16.12.2s 이전 릴리스에서 업그레이드할 경우, 무선 네트워크에서 기본 정책 태그를 사용하는 경우 기본 매핑 변경으로 인해 다운됩니다. 네트워크 작업을 복원하려면 기본 정책 태그 아래에 정책 매핑에 필요한 WLAN을 추가합니다.
- 이번 릴리스부터는 새로운 게이트웨이 연결 가능성 검사가 도입되었습니다. AP는 연결을 확인하기 위해 기본 게이트웨이에 주기적인 ICMP 에코 요청(ping)을 보냅니다. AP와 기본 게이트웨이 간의 ICMP ping을 허용하려면 AP와 기본 게이트웨이 간의 트래픽 필터링(예: ACL)을 확인해야 합니다. 이러한 ping이 차단되면 컨트롤러와 AP 간의 연결이 활성화되어 있더라도 AP가 4시간 간격으로 다시 로드됩니다.

17.2.1

- 16.12.3 및 17.2.1은 설명서에 지원 대상으로 나와 있는 SFP만 지원하는 첫 번째 릴리스입니다. 목록에 없는 SFP로 인해 포트 다운(port-down) 상황이 발생합니다. 업그레이드 후 데이터 포트가 다운되지 않도록 지원되는 SFP 목록을 확인하고 SFP가 호환되는지 확인합니다.
- 16.12.1 릴리스에 있는 경우 이 릴리스의 업그레이드 파일이 너무 커서 HTTP 업로드(웹 UI 업그레이드 수행 시)에 적합하지 않을 수 있습니다. 다른 전송 방법을 사용하거나 웹 UI를 통해 대용량 파일을 업로드할 수 있도록 지원하는 16.12.2를 계속 진행합니다.
- Cisco IOS XE Gibraltar 16.12.2s에서 기본 정책 태그 아래의 기본 정책 프로필에 대한 자동 WLAN 매핑이 제거되었습니다. Cisco IOS XE Gibraltar 16.12.2s 이전 릴리스에서 업그레이드하는 경우 및 무선 네트워크에서 기본 정책 태그를 사용하는 경우 기본 매핑 변경으로 인해 중지될 수 있습니다. 네트워크 작업을 복원하려면 기본 정책 태그 아래에 정책 매핑에 필요한 WLAN을 추가합니다.
- 17.1 이상에서는 새로운 게이트웨이 연결 가능성 검사가 도입되었습니다. AP는 연결을 확인하기 위해 기본 게이트웨이에 주기적인 ICMP 에코 요청(ping)을 보냅니다. AP와 기본 게이트웨이 간의 ICMP ping을 허용하려면 AP와 기본 게이트웨이 간의 트래픽 필터링(예: ACL)을 확인해야 합니다. 이러한 ping이 차단되면 컨트롤러와 AP 간의 연결이 활성화되어 있더라도 AP가 4시간 간격으로 다시 로드됩니다.

17.3.1

- 16.12.3 및 17.2.1은 설명서에 지원 대상으로 나와 있는 SFP만 지원하기 위한 첫 번째 릴리스입니다. 목록에 없는 SFP로 인해 포트 다운(port-down) 상황이 발생합니다. 업그레이드 후 데이터 포트가 다운되지 않도록 지원되는 SFP 목록을 확인하고 SFP가 호환되는지 확인합니다.
- 16.12.1 릴리스에 있는 경우 이 릴리스의 업그레이드 파일이 너무 커서 HTTP 업로드(웹 UI 업그레이드 수행 시)에 적합하지 않을 수 있습니다. 다른 전송 방법을 사용하거나 웹 UI를 통해 대용량 파일을 업로드할 수 있도록 지원하는 16.12.2를 계속 진행합니다.
- Cisco IOS XE Gibraltar 16.12.2s에서 기본 정책 태그 아래의 기본 정책 프로필에 대한 자동 WLAN 매핑이 제거되었습니다. Cisco IOS XE Gibraltar 16.12.2s 이전 릴리스에서 업그레이드할 경우, 무선 네트워크에서 기본 정책 태그를 사용하는 경우 기본 매핑 변경으로 인해 다운됩니다. 네트워크 작업을 복원하려면 기본 정책 태그 아래에 정책 매핑에 필요한 WLAN을 추가합니다.
- 17.1 이후부터는 새로운 게이트웨이 연결 가능성 검사가 도입됩니다. AP는 연결을 확인하기 위해 기본 게이트웨이에 주기적인 ICMP 에코 요청(ping)을 보냅니다. AP와 기본 게이트웨이 간의 ICMP ping을 허용하려면 AP와 기본 게이트웨이 간의 트래픽 필터링(예: ACL)을 확인해야 합니다. 이러한 ping이 차단되면 컨트롤러와 AP 간의 연결이 활성화되어 있더라도 AP가 4시간 간격으로 다시 로드됩니다.
- FIPS 모드를 구성한 경우, Cisco IOS XE Amsterdam 17.3.x를`security wpa wpa1 cipher tkip`이전 버전에서 업그레이드하기 전에 WLAN에서 컨피그레이션을 제거해야 합니다. 이렇게 하지 않으면 WLAN 보안이 TKIP로 설정되며, 이는 FIPS 모드에서 지원되지 않습니다. 업그레이드 후에는 WLAN을 AES로 재구성해야 합니다.
- Cisco IOS XE Amsterdam 17.3.1 이상에서는 Cisco Catalyst 9800-CL Wireless Controller를 새로 구축하기 위해 16GB의 디스크 공간이 필요합니다. 17.3 이미지의 재설치를 통해서만 디스크 공간 크기를 늘릴 수 있습니다.
- Cisco IOS XE Amsterdam 17.3.1 이상에서는 AP 이름을 최대 32자까지만 입력할 수 있습니다.
- 로컬 MAC 주소 인증(클라이언트 또는 AP)의 경우 17.3.1부터는`aaaabbbbcccc`구분 기호 없이 형식만 지원됩니다. 즉, 웹 UI 또는 CLI에서 구분 기호가 있는 MAC 주소를 추가하면 인증이 실패합니다.
- 이 릴리스부터는 AP가 WLC에 조인할 수 없고 게이트웨이를 ping할 수 없으며 게이트웨이의 ARP를 수행할 수 없는 경우 4시간 후에 다시 로드됩니다(AP가 재부팅되려면 세 가지가 모두 실패해야 함). 이전 릴리스의 이전 ICMP 전용 게이트웨이 확인에 대한 개선 사항(Cisco 버그 ID CSCvt89970)입니다.
- 17.3.1 이후부터는 액세스 포인트에 대한 국가 코드를 구성하는 새로운 방법이 다른 국가 코드로`Wireless country <1 country code>`여러 번 반복할 수 있는 명령입니다. 이렇게 하면 국가 코드의 최대 양을 20보다 크게 늘릴 수 있습니다. 명령`ap country`은 여전히 존재하고 작동하지만, 이후 버전에서`Wireless country`이 사용되지 않으므로명령으로`ap country`변경하는 것이 좋습니다.

17.3.2

- 16.12.3 및 17.2.1은 설명서에 지원 대상으로 나와 있는 SFP만 지원하는 첫 번째 릴리스입니다. 목록에 없는 SFP로 인해 포트 다운(port-down) 상황이 발생합니다. 업그레이드 후 데이터 포트가 다운되지 않도록 지원되는 SFP 목록을 확인하고 SFP가 호환되는지 확인합니다.
- 16.12.1 릴리스에 있는 경우 이 릴리스의 업그레이드 파일이 너무 커서 HTTP 업로드(웹 UI 업그레이드 수행 시)에 적합하지 않을 수 있습니다. 다른 전송 방법을 사용하거나 웹 UI를 통해 대용량 파일을 업로드할 수 있도록 지원하는 16.12.2를 계속 진행합니다.
- Cisco IOS XE Gibraltar 16.12.2s에서 기본 정책 태그 아래의 기본 정책 프로필에 대한 자동

WLAN 매핑이 제거되었습니다. Cisco IOS XE Gibraltar 16.12.2s 이전 릴리스에서 업그레이드할 경우, 무선 네트워크에서 기본 정책 태그를 사용하는 경우 기본 매핑 변경으로 인해 다운됩니다. 네트워크 작업을 복원하려면 기본 정책 태그 아래에 정책 매핑에 필요한 WLAN을 추가합니다.

- 17.1 이후부터는 새로운 게이트웨이 연결 가능성 검사가 도입됩니다. AP는 연결을 확인하기 위해 기본 게이트웨이에 주기적인 ICMP 에코 요청(ping)을 보냅니다. AP와 기본 게이트웨이 간의 ICMP ping을 허용하려면 AP와 기본 게이트웨이 간의 트래픽 필터링(예: ACL)을 확인해야 합니다. 이러한 ping이 차단되면 컨트롤러와 AP 간의 연결이 활성화되어 있더라도 AP가 4시간 간격으로 다시 로드됩니다.
- FIPS 모드를 구성한 경우, Cisco IOS XE Amsterdam 17.3.x를`security wpa wpa1 cipher tkip`이전 버전에서 업그레이드하기 전에 WLAN에서 컨피그레이션을 제거해야 합니다. 이렇게 하지 않으면 WLAN 보안이 TKIP로 설정되며, 이는 FIPS 모드에서 지원되지 않습니다. 업그레이드 후에는 WLAN을 AES로 재구성해야 합니다.
- Cisco IOS XE Amsterdam 17.3.1 이상에서는 Cisco Catalyst 9800-CL Wireless Controller를 새로 구축하기 위해 16GB의 디스크 공간이 필요합니다. 17.3 이미지의 재설치를 통해서만 디스크 공간 크기를 늘릴 수 있습니다.
- Cisco IOS XE Amsterdam 17.3.1 이상에서는 AP 이름을 최대 32자까지만 입력할 수 있습니다.
- 로컬 MAC 주소 인증(클라이언트 또는 AP)의 경우 17.3.1부터는`aaaabbbbcccc`구분 기호 없이 형식만 지원됩니다. 즉, 웹 UI 또는 CLI에서 구분 기호가 있는 MAC 주소를 추가하면 인증이 실패합니다.
- 17.3.1 이후부터는 AP가 WLC에 조인할 수 없고, 게이트웨이를 ping할 수 없으며, 게이트웨이의 ARP를 수행할 수 없는 경우 4시간 후에 다시 로드됩니다(AP가 재부팅되려면 세 가지가 모두 실패해야 함). 이는 이전 릴리스에서 ICMP 전용 게이트웨이 확인을 위한 개선 사항(Cisco 버그 ID CSCvt89970)입니다.
- 17.3.1 이후부터는 액세스 포인트에 대한 국가 코드를 구성하는 새로운 방법이 다른 국가 코드로`Wireless country <1 country code>`여러 번 반복할 수 있는 명령입니다. 이렇게 하면 국가 코드의 최대 수가 20을 훨씬 넘게 증가할 수 있습니다. 이 명령`ap country`은 여전히 존재하고 실행되지만, 이후 버전에서는 이 명령이 더 이상 사용되지 않으므로`Wireless country`이 명령을`ap country`명령으로 변경하는 것이 좋습니다.

17.3.3

- 16.12.3 및 17.2.1은 설명서에 지원 대상으로 나와 있는 SFP만 지원하는 첫 번째 릴리스입니다. 목록에 없는 SFP로 인해 포트 다운(port-down) 상황이 발생합니다. 업그레이드 후 데이터 포트가 다운되지 않도록 지원되는 SFP 목록을 확인하고 SFP가 호환되는지 확인합니다.
- 16.12.1 릴리스에 있는 경우 이 릴리스의 업그레이드 파일이 너무 커서 HTTP 업로드(웹 UI 업그레이드 수행 시)에 적합하지 않을 수 있습니다. 다른 전송 방법을 사용하거나 웹 UI를 통해 대용량 파일을 업로드할 수 있도록 지원하는 16.12.2를 계속 진행합니다.
- Cisco IOS XE Gibraltar 16.12.2s에서 기본 정책 태그 아래의 기본 정책 프로필에 대한 자동 WLAN 매핑이 제거되었습니다. Cisco IOS XE Gibraltar 16.12.2s 이전 릴리스에서 업그레이드할 경우, 무선 네트워크에서 기본 정책 태그를 사용하는 경우 기본 매핑 변경으로 인해 다운됩니다. 네트워크 작업을 복원하려면 기본 정책 태그 아래에 정책 매핑에 필요한 WLAN을 추가합니다.
- 17.1 이상에서는 새로운 게이트웨이 연결 가능성 검사가 도입되었습니다. AP는 연결을 확인하기 위해 기본 게이트웨이에 주기적인 ICMP 에코 요청(ping)을 보냅니다. AP와 기본 게이트

웨이 간의 ICMP ping을 허용하려면 AP와 기본 게이트웨이 간의 트래픽 필터링(예: ACL)을 확인해야 합니다. 이러한 ping이 차단되면 컨트롤러와 AP 간의 연결이 활성화되어 있더라도 AP가 4시간 간격으로 다시 로드됩니다.

- FIPS 모드를 구성한 경우, Cisco IOS XE Amsterdam 17.3.x를`security wpa wpa1 cipher tkip`이전 버전에서 업그레이드하기 전에 WLAN에서 컨피그레이션을 제거해야 합니다. 이렇게 하지 않으면 WLAN 보안이 TKIP로 설정되며, 이는 FIPS 모드에서 지원되지 않습니다. 업그레이드 후에는 WLAN을 AES로 재구성해야 합니다.
- Cisco IOS XE Amsterdam 17.3.1 이상에서는 Cisco Catalyst 9800-CL Wireless Controller를 새로 구축하기 위해 16GB의 디스크 공간이 필요합니다. 17.3 이미지의 재설치를 통해서만 디스크 공간 크기를 늘릴 수 있습니다.
- Cisco IOS XE Amsterdam 17.3.1 이상에서는 AP 이름을 최대 32자까지만 입력할 수 있습니다.
- 로컬 MAC 주소 인증(클라이언트 또는 AP)의 경우 17.3.1부터는`aaaabbbbcccc`구분 기호 없이 형식만 지원됩니다. 즉, 웹 UI 또는 CLI에서 구분 기호가 있는 MAC 주소를 추가하면 인증이 실패합니다.
- 17.3.1 이후부터는 AP가 WLC에 조인할 수 없고, 게이트웨이를 ping할 수 없으며, 게이트웨이의 ARP를 수행할 수 없는 경우 4시간 후에 다시 로드됩니다(AP가 재부팅되려면 세 가지가 모두 실패해야 함). 이는 이전 릴리스의 이전 ICMP 전용 게이트웨이 확인에 대한 개선 사항(Cisco 버그 ID CSCvt89970)입니다.
- 17.3.1 이후부터는 액세스 포인트에 대한 국가 코드를 구성하는 새로운 방법이 다른 국가 코드로`Wireless country <1 country code>`여러 번 반복할 수 있는 명령입니다. 이렇게 하면 국가 코드의 최대 양을 20보다 크게 늘릴 수 있습니다. 명령`ap country`은 여전히 존재하고 작동하지만, 이후 버전에서`Wireless country`이 사용되지 않으므로명령으로`ap country`변경하는 것이 좋습니다.
- AP의 호스트 이름이 32자를 초과할 경우 WLC가 충돌할 수 있습니다(Cisco 버그 ID CSCvy11981).

17.3.4

- 16.12.3 및 17.2.1은 설명서에 지원 대상으로 나와 있는 SFP만 지원하기 위한 첫 번째 릴리스입니다. 목록에 없는 SFP로 인해 포트 다운(port-down) 상황이 발생합니다. 업그레이드 후 데이터 포트가 다운되지 않도록 지원되는 SFP 목록을 확인하고 SFP가 호환되는지 확인합니다.
- 16.12.1 릴리스에 있는 경우 이 릴리스의 업그레이드 파일이 너무 커서 HTTP 업로드(웹 UI 업그레이드 수행 시)에 적합하지 않을 수 있습니다. 다른 전송 방법을 사용하거나 웹 UI를 통해 대용량 파일을 업로드할 수 있도록 지원하는 16.12.2를 계속 진행합니다.
- Cisco IOS XE Gibraltar 16.12.2s에서 기본 정책 태그 아래의 기본 정책 프로필에 대한 자동 WLAN 매핑이 제거되었습니다. Cisco IOS XE Gibraltar 16.12.2s 이전 릴리스에서 업그레이드할 경우, 무선 네트워크에서 기본 정책 태그를 사용하는 경우 기본 매핑 변경으로 인해 다운됩니다. 네트워크 작업을 복원하려면 기본 정책 태그 아래에 정책 매핑에 필요한 WLAN을 추가합니다.
- 17.1 이후부터는 새로운 게이트웨이 연결 가능성 검사가 도입됩니다. AP는 기본 게이트웨이에 주기적인 ICMP 에코 요청(ping)을 전송하여 연결을 확인합니다. AP와 기본 게이트웨이 간의 ICMP ping을 허용하려면 AP와 기본 게이트웨이 간의 트래픽 필터링(예: ACL)을 확인해야 합니다. 이러한 ping이 차단되면 컨트롤러와 AP 간의 연결이 활성화되어 있더라도 AP가 4시간 간격으로 다시 로드됩니다.
- FIPS 모드를 구성한 경우, Cisco IOS XE Amsterdam 17.3.x를`security wpa wpa1 cipher tkip`이전 버전에서 업그레이드하기 전에 WLAN에서 컨피그레이션을 제거해야 합니다. 이렇게 하지 않으면

WLAN 보안이 TKIP로 설정되며, 이는 FIPS 모드에서 지원되지 않습니다. 업그레이드 후에는 WLAN을 AES로 재구성해야 합니다.

- Cisco IOS XE Amsterdam 17.3.1 이상에서는 Cisco Catalyst 9800-CL Wireless Controller를 새로 구축하기 위해 16GB의 디스크 공간이 필요합니다. 17.3 이미지의 재설치를 통해서만 디스크 공간 크기를 늘릴 수 있습니다.
- Cisco IOS XE Amsterdam 17.3.1 이상에서는 AP 이름을 최대 32자까지만 입력할 수 있습니다.
- 로컬 MAC 주소 인증(클라이언트 또는 AP)의 경우 17.3.1부터는aaaabbbbcccc구분 기호 없이 형식만 지원됩니다. 즉, 웹 UI 또는 CLI에서 구분 기호가 있는 MAC 주소를 추가하면 인증이 실패합니다.
- 17.3.1 이후부터 APsI은 WLC에 조인할 수 없고 게이트웨이를 ping할 수 없으며 게이트웨이의 ARP를 수행할 수 없는 경우 4시간 후에 다시 로드됩니다(AP가 재부팅되려면 세 가지가 모두 실패해야 함). 이는 이전 릴리스의 이전 ICMP 전용 게이트웨이 확인에 대한 개선 사항(Cisco 버그 ID CSCvt89970)입니다.
- 17.3.1 이상, 액세스 포인트에 대한 국가 코드를 구성하는 새로운 방법은 다른 국가 코드를 Wireless country <1 country code>사용하여 여러 번 반복할 수 있는 명령입니다. 이렇게 하면 국가 코드의 최대 양을 20보다 크게 늘릴 수 있습니다. 명령ap country은 여전히 존재하고 작동하지만, 향후 버전에서Wireless country더 이상 사용되지 않을 계획이므로명령으로 변경할ap country것을 고려하십시오.
- 17.3.4 이상으로 업그레이드할 경우, 16.12.5r 부트로더/롬몬이 해당하는 컨트롤러(9800-80)에 설치하는 것이 좋습니다. (현재 9800-40에는 rommon 16.12.5r이 없으며 rommon 업그레이드가 필요하지 않습니다.)
- Cisco IOS XE Bengaluru 17.3.x에서 ISSU를 사용하는 모든 릴리스로의 컨트롤러 업그레이드는 snmp-server enable traps hsrp명령이 구성되었습니다. Cisco IOS XE Bengaluru 17.4.xsnmp-server enable traps hsrp에서 명령이 제거되었으므로 ISSU 업그레이드를 시작하기 전에snmp-server enable traps hsrp컨피그레이션에서 명령을 제거했는지 확인합니다.

- Cisco IOS XE 17.3.x 이상 릴리스로 업그레이드하는 동안 이 명령이ip http active-session-modules none활성화된 경우 HTTPS를 사용하여 컨트롤러 GUI에 액세스할 수 없습니다. HTTPS를 사용하여 GUI에 액세스하려면 다음 명령을 실행합니다.

    - ip http session-module-list pkilist OPENRESTY_PKI

    - ip http active-session-modules pkilist

17.3.5

- Cisco 버그 ID CSCwb13784로 인해, 경로 MTU가 1500바이트보다 작으면 AP가 조인할 수 없습니다. 이 문제를 해결하려면 17.3.5에 사용 가능한 SMU 패치를 다운로드합니다.
- 16.12.3 및 17.2.1은 설명서에 지원 대상으로 나와 있는 SFP만 지원하기 위한 첫 번째 릴리스입니다. 목록에 없는 SFP로 인해 포트 다운(port-down) 상황이 발생합니다. 업그레이드 후 데이터 포트가 다운되지 않도록 지원되는 SFP 목록을 확인하고 SFP가 호환되는지 확인합니다.
- 16.12.1 릴리스에 있는 경우 이 릴리스의 업그레이드 파일이 너무 커서 HTTP 업로드(웹 UI 업그레이드 수행 시)에 적합하지 않을 수 있습니다. 다른 전송 방법을 사용하거나 웹 UI를 통해 대용량 파일을 업로드할 수 있도록 지원하는 16.12.2를 계속 진행합니다.
- Cisco IOS XE Gibraltar 16.12.2s에서 기본 정책 태그 아래의 기본 정책 프로필에 대한 자동 WLAN 매핑이 제거되었습니다. Cisco IOS XE Gibraltar 16.12.2s 이전 릴리스에서 업그레이

드할 경우, 무선 네트워크에서 기본 정책 태그를 사용하는 경우 기본 매핑 변경으로 인해 다운됩니다. 네트워크 작업을 복원하려면 기본 정책 태그 아래에 정책 매핑에 필요한 WLAN을 추가합니다.

- 17.1 이상에서는 새로운 게이트웨이 연결 가능성 검사가 도입되었습니다. AP는 연결을 확인하기 위해 기본 게이트웨이에 주기적인 ICMP 에코 요청(ping)을 보냅니다. AP와 기본 게이트웨이 간의 ICMP ping을 허용하려면 AP와 기본 게이트웨이 간의 트래픽 필터링(예: ACL)을 확인해야 합니다. 이러한 ping이 차단되면 컨트롤러와 AP 간의 연결이 활성화되어 있더라도 AP가 4시간 간격으로 다시 로드됩니다.
- FIPS 모드를 구성한 경우, Cisco IOS XE Amsterdam 17.3.x를`security wpa wpa1 cipher tkip`이전 버전에서 업그레이드하기 전에 WLAN에서 컨피그레이션을 제거해야 합니다. 이렇게 하지 않으면 WLAN 보안이 TKIP로 설정되며, 이는 FIPS 모드에서 지원되지 않습니다. 업그레이드 후에는 WLAN을 AES로 재구성해야 합니다.
- Cisco IOS XE Amsterdam 17.3.1 이상, Cisco Catalyst 9800-CL Wireless Controller를 새로 구축하려면 16GB의 디스크 공간이 필요합니다. 17.3 이미지의 재설치를 통해서만 디스크 공간 크기를 늘릴 수 있습니다.
- Cisco IOS XE Amsterdam 17.3.1 이상에서는 AP 이름을 최대 32자까지만 입력할 수 있습니다.
- 로컬 MAC 주소 인증(클라이언트 또는 AP)의 경우 17.3.1부터는`aaaabbbbcccc`구분 기호 없이 형식만 지원됩니다. 즉, 웹 UI 또는 CLI에서 구분 기호가 있는 MAC 주소를 추가하면 인증이 실패합니다.
- 17.3.1 이상, APsI은 WLC에 조인할 수 없고 게이트웨이를 ping할 수 없으며 게이트웨이의 ARP를 수행할 수 없는 경우 4시간 후에 다시 로드됩니다(AP가 재부팅되려면 세 가지가 모두 실패해야 함). 이는 이전 릴리스에서 ICMP 전용 게이트웨이 확인을 위한 개선 사항(Cisco 버그 ID CSCvt89970)입니다.
- 17.3.1 이상, 액세스 포인트에 대한 국가 코드를 구성하는 새로운 방법은 다른 국가 코드를`Wireless country <1 country code>`사용하여 여러 번 반복할 수 있는 명령입니다. 이렇게 하면 국가 코드의 최대 양을 20보다 크게 늘릴 수 있습니다. 명령`ap country`은 여전히 존재하고 작동하지만, 향후 버전에서`Wireless country`더 이상 사용되지 않을 계획이므로명령으로 변경할`ap country`것을 고려하십시오.
- 17.3.4 이상으로 업그레이드할 경우, 16.12.5r 부트로더/롬몬이 해당하는 컨트롤러(9800-80)에 설치하는 것이 좋습니다. (현재 9800-40에는 rommon 16.12.5r이 없으며 rommon 업그레이드가 필요하지 않습니다.)
- Cisco IOS XE Bengaluru 17.3.x에서 ISSU를 사용하는 모든 릴리스로의 컨트롤러 업그레이드는 `snmp-server enable traps hsrp`명령이 구성되었습니다. Cisco IOS XE Bengaluru 17.4.x`snmp-server enable traps hsrp`에서 명령이 제거되었으므로 ISSU 업그레이드를 시작하기 전에`snmp-server enable traps hsrp`컨피그레이션에서 명령을 제거했는지 확인합니다.

- Cisco IOS XE 17.3.x 이상 릴리스로 업그레이드하는 동안 이 명령이`ip http active-session-modules none`활성화된 경우 HTTPS를 사용하여 컨트롤러 GUI에 액세스할 수 없습니다. HTTPS를 사용하여 GUI에 액세스하려면 다음 명령을 실행합니다.
    - ip http session-module-list pkilist OPENRESTY_PKI
    - ip http active-session-modules pkilist

벵갈루루

17.4.1

- 17.4.1 이상, Wave 1 Cisco IOS 기반 AP는 IW3700을 제외하고 더 이상 지원되지 않습니다(1700,2700,3700,1570).
- WLAN이 비 WPA(게스트, 개방형 또는 CWA SSID)이고 적응형 FT가 구성된 경우 업그레이드 후 WLAN을 종료할 수 있습니다. 해결 방법은 업그레이드 전에 적응형 FT 컨피그레이션을 제거하는 것입니다(Cisco 버그 ID CSCvx34349). 적응형 FT 컨피그레이션은 비 WPA SSID에서 의미가 없으므로 이를 제거하여 손실되는 것이 없습니다.
- AP의 호스트 이름이 32자를 초과하는 경우 WLC가 충돌할 수 있습니다(Cisco 버그 ID CSCvy11981).

17.5.1

- 17.4.1 이상, Wave 1 Cisco IOS 기반 AP는 IW3700을 제외하고 더 이상 지원되지 않습니다(1700,2700,3700,1570).
- Cisco IOS XE Bengaluru Release 17.4.1 이상에서는 텔레메트리 솔루션에서 텔레메트리 데이터의 IP 주소 대신 수신기 주소의 이름을 제공합니다. 이는 추가 옵션입니다. 컨트롤러 다운그레이드 및 후속 업그레이드 과정에서 새로 명명된 수신기를 사용하는 업그레이드 버전에 문제가 있을 수 있으며, 이러한 버전은 다운그레이드에서 인식되지 않습니다. 새 컨피그레이션이 거부되고 후속 업그레이드에서 실패합니다. Cisco DNA Center에서 업그레이드 또는 다운그레이드를 수행할 때 컨피그레이션 손실을 방지할 수 있습니다.
- WLAN이 비 WPA(게스트, 개방형 또는 CWA SSID)이고 적응형 FT가 구성된 경우 업그레이드 후 WLAN을 종료할 수 있습니다. 해결 방법은 업그레이드 전에 적응형 FT 컨피그레이션을 제거하는 것입니다(Cisco 버그 ID CSCvx34349). 적응형 FT 컨피그레이션은 비 WPA SSID에서 의미가 없으므로 이를 제거하여 손실되는 것이 없습니다.
- AP의 호스트 이름이 32자를 초과하는 경우 WLC가 충돌할 수 있습니다(Cisco 버그 ID CSCvy11981).
- 한 릴리스에서 다른 릴리스로 GUI를 업그레이드할 때 모든 GUI 페이지를 올바르게 다시 로드하려면 브라우저 캐시를 지우는 것이 좋습니다.

- Cisco IOS XE 17.3.x 이상 릴리스로 업그레이드하는 동안 이 명령을`ip http active-session-modules none`활성화하면 HTTPS를 사용하여 GUI에 액세스할 수 없습니다. HTTPS를 사용하여 GUI에 액세스하려면 다음 명령을 실행합니다.
    - ip http session-module-list pkilist OPENRESTY_PKI
    - ip http active-session-modules pkilist

- 재부팅 또는 시스템 충돌 후 GUI에서 "ERR_SSL_VERSION_OR_CIPHER_MISMATCH" 오류가 발생하면 신뢰 지점 인증서를 다시 생성하는 것이 좋습니다.
- 새 자체 서명 신뢰 지점을 생성하는 절차는 다음과 같습니다.

```
configure terminal
no crypto pki trustpoint
```

```
no ip http server no ip http secure-server ip http server ip http secure-server ip http authentica
```

```
! use local or aaa as applicable.
```

17.6.1

- 17.4.1 이상, Wave 1 Cisco IOS 기반 AP는 IW3700을 제외하고 더 이상 지원되지 않습니다 (1700,2700,3700,1570).
- Cisco IOS XE Bengaluru Release 17.4.1 이상에서는 텔레메트리 솔루션에서 텔레메트리 데이터의 IP 주소 대신 수신기 주소의 이름을 제공합니다. 이는 추가 옵션입니다. 컨트롤러 다운그레이드 및 후속 업그레이드 과정에서 새로 명명된 수신기를 사용하는 업그레이드 버전에 문제가 있을 수 있으며, 이러한 버전은 다운그레이드에서 인식되지 않습니다. 새 컨피그레이션이 거부되고 후속 업그레이드에서 실패합니다. Cisco DNA Center에서 업그레이드 또는 다운그레이드를 수행할 때 컨피그레이션 손실을 방지할 수 있습니다.
- WLAN이 비 WPA(게스트, 개방형 또는 CWA SSID)이고 적응형 FT가 구성된 경우 업그레이드 후 WLAN을 종료할 수 있습니다. 해결 방법은 업그레이드 전에 적응형 FT 컨피그레이션을 제거하는 것입니다(Cisco 버그 ID CSCvx34349). 적응형 FT 컨피그레이션은 비 WPA SSID에서 의미가 없으므로 이를 제거하여 손실되는 것이 없습니다.
- 한 릴리스에서 다른 릴리스로 GUI를 업그레이드할 때 모든 GUI 페이지를 올바르게 다시 로드하려면 브라우저 캐시를 지우는 것이 좋습니다.
- 17.6.1 이상 WLC에 가입한 AP는 8.10.162 이상 또는 8.5.176.2 이상 8.5 코드를 실행하지 않는 한 더 이상 AireOS WLC에 가입할 수 없습니다.
- 17.6,1 이상으로 업그레이드하려면 16.12.5r 부트로더/롬몬이 해당하는 컨트롤러(9800-80)에 설치하는 것이 좋습니다. (현재 9800-40에는 rommon 16.12.5r이 없으며 rommon 업그레이드가 필요하지 않습니다.)
- Cisco IOS XE Bengaluru 17.3.x에서 ISSU를 사용하는 모든 릴리스로의 컨트롤러 업그레이드는 `snmp-server enable traps hsrp`명령이 구성되었습니다. Cisco IOS XE Bengaluru 17.4.x`snmp-server enable traps hsrp`에서 명령이 제거되었으므로 ISSU 업그레이드를 시작하기 전에`snmp-server enable traps hsrp`컨피그레이션에서 명령을 제거했는지 확인합니다.

- Cisco IOS XE 17.3.x 이상 릴리스로 업그레이드하는 동안 이 명령이`ip http active-session-modules none`활성화된 경우 컨트롤러 GUI에 대한 HTTPS 액세스가 작동하지 않습니다. HTTPS를 사용하여 GUI에 액세스하려면 다음 명령을 실행합니다.
    - ip http session-module-list pkilist OPENRESTY_PKI
    - ip http active-session-modules pkilist

- 재부팅 또는 시스템 충돌 후 GUI에서 "ERR_SSL_VERSION_OR_CIPHER_MISMATCH" 오류가 발생하면 신뢰 지점 인증서를 다시 생성하는 것이 좋습니다.
- 새 자체 서명 신뢰 지점을 생성하는 절차는 다음과 같습니다.

```
configure terminal
no crypto pki trustpoint
```

```
no ip http server no ip http securffwe-server ip http server ip http secure-server ip http authen
```

```
! use local or aaa as applicable.
```

17.6.2

- 17.4.1 이상, Wave 1 Cisco IOS 기반 AP는 IW3700을 제외하고 더 이상 지원되지 않습니다(1700,2700,3700,1570).
- Cisco IOS XE Bengaluru Release 17.4.1 이상에서는 텔레메트리 솔루션에서 텔레메트리 데이터의 IP 주소 대신 수신기 주소의 이름을 제공합니다. 이는 추가 옵션입니다. 컨트롤러 다운그레이드 및 후속 업그레이드 과정에서 새로 명명된 수신기를 사용하는 업그레이드 버전에 문제가 있을 수 있으며, 이러한 버전은 다운그레이드에서 인식되지 않습니다. 새 컨피그레이션이 거부되고 후속 업그레이드에서 실패합니다. Cisco DNA Center에서 업그레이드 또는 다운그레이드를 수행할 때 컨피그레이션 손실을 방지할 수 있습니다.
- WLAN이 비 WPA(게스트, 개방형 또는 CWA SSID)이고 적응형 FT가 구성된 경우 업그레이드 후 WLAN을 종료할 수 있습니다. 해결 방법은 업그레이드 전에 적응형 FT 컨피그레이션을 제거하는 것입니다(Cisco 버그 ID CSCvx34349). 적응형 FT 컨피그레이션은 비 WPA SSID에서 의미가 없으므로 이를 제거하여 손실되는 것이 없습니다.
- 한 릴리스에서 다른 릴리스로 GUI를 업그레이드할 때 모든 GUI 페이지를 올바르게 다시 로드하려면 브라우저 캐시를 지우는 것이 좋습니다.
- 17.6.1 이상 WLC에 가입한 AP는 8.10.162 이상 또는 8.5.176.2 이상 8.5 코드를 실행하지 않는 한 더 이상 AireOS WLC에 가입할 수 없습니다.
- 17.6,1 이상으로 업그레이드하려면 16.12.5r 부트로더/롬몬이 해당하는 컨트롤러(9800-80)에 설치하는 것이 좋습니다. (현재 9800-40에는 rommong 16.12.5r이 없으며 rommon 업그레이드가 필요하지 않습니다.)
- Cisco IOS XE Bengaluru 17.3.x에서 ISSU를 사용하는 모든 릴리스로의 컨트롤러 업그레이드

는 snmp-server enable traps hsrp명령이 구성되었습니다. Cisco IOS XE Bengaluru 17.4.xsnmp-server enable traps hsrp에서 명령이 제거되었으므로 ISSU 업그레이드를 시작하기 전에snmp-server enable traps hsrp컨피그레이션에서 명령을 제거했는지 확인합니다.

- Cisco IOS XE 17.3.x 이상 릴리스로 업그레이드하는 동안 이 명령이ip http active-session-modules none활성화되면 HTTPS 컨트롤러 GUI 액세스가 작동하지 않습니다. HTTPS를 사용하여 GUI에 액세스하려면 다음 명령을 실행합니다.
  - ip http session-module-list pkilist OPENRESTY_PKI
  - ip http active-session-modules pkilist
- AP 이름에는 31자 이상을 사용하지 마십시오. AP 이름이 32자 이상인 경우 컨트롤러 충돌이 발생할 수 있습니다.
- 재부팅 또는 시스템 충돌 후 GUI에서 "ERR_SSL_VERSION_OR_CIPHER_MISMATCH" 오류가 발생하면 신뢰 지점 인증서를 다시 생성하는 것이 좋습니다.
- 새 자체 서명 신뢰 지점을 생성하는 절차는 다음과 같습니다.

```
configure terminal
no crypto pki trustpoint
```

```
no ip http server no ip http secure-server ip http server ip http secure-server ip http authentic
```

```
! use local or aaa as applicable.
```

쿠페르티노

이 섹션에서는 17.6.1 이상에서 시작하여 Cupertino 릴리스로 업그레이드하는 것으로 가정합니다. 이전 릴리스(지원 가능)에서 직접 업그레이드하는 경우 릴리스 정보를 확인하여 확인하십시오. 17.3 및 17.6 섹션 주의 사항을 읽어 보십시오.

17.7.1

- AP 이름에는 31자 이상을 사용하지 마십시오. AP 이름이 32자 이상인 경우 컨트롤러 충돌이 발생할 수 있습니다.
- 17.7.1에서는 AP 조인 프로필에 AP 국가 코드를 구성해야 합니다.
- Cisco 버그 ID CSCvu22886으로 인해, 9130 또는 9124 AP가 있는 경우 17.3.4 이전 릴리스에서 17.7.1 이상으로 업그레이드할 때 17.3.5a를 통과해야 합니다.
- Cisco IOS XE Cupertino 17.7.1 이후부터 Cisco Catalyst 9800-CL Wireless Controller의 경우 RUM(Resource Utilization Measurement) 보고를 완료하고 제품 인스턴스에서 ACK를 한 번 이상 사용할 수 있는지 확인합니다. 이는 정확한 최신 사용 정보가 CSSM(Cisco Smart Software Manager)에 반영되도록 하기 위한 것입니다. 이렇게 하지 않으면 라이센스 보고서가 승인될 때까지 최대 50개의 AP가 9800-CL에 참가할 수 있습니다.
- 한 릴리스에서 다른 릴리스로 GUI를 업그레이드할 때 모든 GUI 페이지를 올바르게 다시 로드하려면 브라우저 캐시를 지우는 것이 좋습니다.

17.8.1

- AP 이름에는 31자 이상을 사용하지 마십시오. AP 이름이 32자 이상인 경우 컨트롤러 충돌이 발생할 수 있습니다.
- 17.7.1에서는 AP 조인 프로필에 AP 국가 코드를 구성해야 합니다.
- Cisco 버그 ID CSCvu22886으로 인해, 9130 또는 9124 AP가 있는 경우 17.3.4 이전 릴리스에서 17.7.1 이상으로 업그레이드할 때 17.3.5a를 통과해야 합니다.
- Cisco IOS XE Cupertino 17.7.1 이상(Cisco Catalyst 9800-CL Wireless Controller의 경우), RUM 보고를 완료하고 제품 인스턴스에서 ACK를 한 번 이상 사용할 수 있는지 확인합니다. 이는 정확하고 최신 사용 정보가 CSSM에 반영되도록 하기 위한 것입니다. 이렇게 하지 않으면 라이센스 보고서가 승인될 때까지 최대 50개의 AP가 9800-CL에 참가할 수 있습니다.
- 한 릴리스에서 다른 릴리스로 GUI를 업그레이드할 때 모든 GUI 페이지를 올바르게 다시 로드하려면 브라우저 캐시를 지우는 것이 좋습니다.

17.9.x

- Cisco IOS-XE 17.9.3을 실행하는 AP는 디렉토리 공간이 부족하여 소프트웨어를 업그레이드하려고 할 때 문제가 발생할 수/tmp있습니다. AP의/tmp공간이 가득 차면 새 AP 이미지의 다운로드가 방지됩니다. 이러한 경우에는 AP를 재부팅하는 것이 좋습니다.

- 11AC Wave 2 AP는 WAN 링크를 통해 소프트웨어를 업그레이드할 때 부팅 루프에 빠질 수 있습니다. 자세한 내용은 https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/220443-how-to-avoid-boot-loop-due-to-corrupted.html을 참조하십시오.

- 17.9.3 이상 릴리스는 Cisco IOS 기반 액세스 포인트(x700 Series 및 1570)에 대한 지원을 다시 제공합니다. 17.4와 17.9.2 사이에는 지원되지 않았습니다. 이러한 AP에 대한 지원은 일반적인 제품 라이프사이클 지원 이상으로 확장되지 않습니다. Cisco.com의 개별 End-of-Support 게시판을 참조하십시오.
- domain 명령이 구성된 경우 ISSU를 사용하여 Cisco IOS XE Bengaluru 17.3.x에서 Cisco IOS XE Bengaluru 17.6.x 또는 Cisco IOS XE Cupertino 17.9.x 이상으로 컨트롤러를 업그레이드할 수 없습니다. Cisco IOS XE Bengaluru 17.6.x에서 domain 명령이 제거되었으므로 ISSU 업그레이드를 시작하기 전에 no domain 명령을 실행해야 합니다.

- Cisco IOS XE Cupertino 17.7.1 이상(Cisco Catalyst 9800-CL Wireless Controller의 경우), RUM 보고를 완료하고 제품 인스턴스에서 ACK를 한 번 이상 사용할 수 있는지 확인합니다. 이는 정확하고 최신 사용 정보가 CSSM에 반영되도록 하기 위한 것입니다. 이렇게 하지 않으면 라이센스 보고서가 승인될 때까지 최대 50개의 AP가 9800-CL에 참가할 수 있습니다.
- 1500 미만의 프래그먼트화는 OOB(Gi0) 인터페이스에서 무선 클라이언트에 의해 생성된 RADIUS 패킷에 대해 지원되지 않습니다.
- 17.3 이상, 9800-CL이 제대로 작동하려면 16GB의 디스크 공간이 필요합니다. WLC 인스턴스가 8GB OVA로 시작된 경우(17.3 이전 버전) 크기를 동적으로 늘릴 수 없습니다. 유일한 방법은 17.3 이후의 OVA에서 새 WLC를 생성하는 것입니다.
- 한 릴리스에서 다른 릴리스로 GUI를 업그레이드할 때 모든 GUI 페이지를 올바르게 다시 로드하려면 브라우저 캐시를 지우는 것이 좋습니다.
- Cisco Catalyst 9800-L Wireless Controller는 부팅 시간 동안 콘솔 포트에서 수신한 중단 신호에 응답하지 않아 사용자가 탐색에 이르지 못할 수 있습니다. 이 문제는 2019년 11월까지 제조된 컨트롤러에서 관찰되며, 기본 config-register 설정은 0x2102입니다. config-register를 0x2002로 설정하면 이 문제를 방지할 수 있습니다. 이 문제는 Cisco Catalyst 9800-L Wireless Controller의 16.12(3r) 규칙에서 해결되었습니다. rommon 업그레이드 방법에 대한 자세한 내용은 Cisco Catalyst 9800 Series Wireless ControllerUpgrading rommon for Cisco Catalyst 9800-L Wireless Controllers용 Field Programmable Hardware Devices 업그레이드 문서 섹션을 참조하십시오.

- 재부팅 또는 시스템 충돌 후 이 오류 메시지가 표시되면 신뢰 지점 인증서를 다시 생성하는 것이 좋습니다.

```
ERR_SSL_VERSION_OR_CIPHER_MISMATCH
```

새 자체 서명 신뢰 지점 인증서를 생성하려면 지정된 순서대로 다음 명령을 사용합니다.

1. device# configure terminal
2. device(config)# no crypto pki trustpoint trustpoint_name
3. device(config)# no ip http server
4. device(config)# no ip http secure-server
5. device(config)# ip http server
6. device(config)# ip http secure-server
7. device(config)# ip http authentication local/aaa

- 명령으로 모빌리티 MAC 주소가 설정되어 있는지wireless mobility mac-address확인합니다.
- 이러한 프로토콜은 이제 17.9의 서비스 포트를 통해 지원됩니다.
  - Cisco DNA Center
  - Cisco 스마트 소프트웨어 관리자

    - Cisco Prime Infrastructure
    - Telnet
    - 컨트롤러 GUI
    - DNS
    - 파일 전송
    - GNMI
    - HTTP
    - HTTPS
    - LDAP
    - CSSM과 통신하기 위한 스마트 라이센싱 기능
    - Netconf
    - Netflow
    - NTP
    - RADIUS(CoA 포함)
    - Restconf
    - SNMP
    - SSH
    - SYSLOG
    - TACACS+
- 17.9의 AP 이미지가 원래 허용된 AP 플래시보다 큽니다. AP가 17.9 이미지를 다운로드할 때 공간이 충분하지 않다고 불평하는 경우, 릴리스 노트에서 설명한 대로 17.3.5를 통한 업그레이드 경로를 존중하지 않았거나 AP에서 이전 AireOS 이미지를 실행하고 있기 때문일 수 있습니다. 17.3.5 이상의 WLC를 통해 전송하거나 AireOS 이미지를 최신 버전으로 업그레이드하면 17.9 이미지를 다운로드할 수 있도록 AP 플래시 크기가 조정됩니다.

더블린

17.10.1

- CCKM(Cisco Centralized Key Management) 기능은 Cisco IOS XE Dublin 17.10.x에서 더 이상 사용되지 않습니다.
- Smart Call Home은 더 이상 사용되지 않으며, Smart Transport의 라이선스가 사용됩니다.

- Cisco IOS-XE 17.9.3 이상을 실행하는 AP는 디렉토리의 공간이 부족하여 소프트웨어를 업그레이드하려고 할 때 문제가 발생할 수/tmp있습니다. AP의/tmp공간이 가득 차면 새 AP 이미지의 다운로드가 방지됩니다. 이러한 경우에는 AP를 재부팅하는 것이 좋습니다.

  Wave 2 AP는 WAN 링크를 통해 소프트웨어를 업그레이드할 때 부팅 루프에 빠질 수 있습니다. 자세한 내용은 https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/220443-how-to-avoid-boot-loop-due-to-corrupted.html을 참조하십시오.

- Cisco IOS XE Cupertino 17.7.1 이후부터 Cisco Catalyst 9800-CL Wireless Controller의 경우 RUM 보고를 완료하고 제품 인스턴스에서 ACK를 한 번 이상 사용할 수 있는지 확인합니다. 이는 정확하고 최신 사용 정보가 CSSM에 반영되도록 하기 위한 것입니다. 이렇게 하지 않으면 라이센스 보고서가 승인될 때까지 최대 50개의 AP가 9800-CL에 참가할 수 있습니다.
- 한 릴리스에서 다른 릴리스로 GUI를 업그레이드할 때 모든 GUI 페이지를 올바르게 다시 로드하려면 브라우저 캐시를 지우는 것이 좋습니다.
- 1500 미만의 프래그먼트화는 OOB(Gi0) 인터페이스에서 무선 클라이언트에 의해 생성된 RADIUS 패킷에 대해 지원되지 않습니다.
- 17.3 이상, 9800-CL이 제대로 작동하려면 16GB의 디스크 공간이 필요합니다. WLC 인스턴스가 8GB OVA로 시작된 경우(17.3 이전 버전) 크기를 동적으로 늘릴 수 없습니다. 유일한 방법은 17.3 이후의 OVA에서 새 WLC를 생성하는 것입니다.
- Cisco Catalyst 9800-L Wireless Controller는 부팅 시간 동안 콘솔 포트에서 수신한 BREAK 신호에 응답하지 않아 사용자가 탐색에 도달하지 못할 수 있습니다. 이 문제는 2019년 11월까지 제조된 컨트롤러에서 관찰되며, 기본 config-register 설정은 0x2102입니다. config-register를 0x2002로 설정하면 이 문제를 방지할 수 있습니다. 이 문제는 Cisco Catalyst 9800-L Wireless Controller의 16.12(3r) 프롬프트에서 해결되었습니다. rommon 업그레이드 방법에 대한 자세한 내용은 Upgrading Field Programmable Hardware Devices for Cisco Catalyst 9800 Series Wireless Controllers 문서의 Upgrading rommon for Cisco Catalyst 9800-L Wireless Controllers 섹션을 참조하십시오.

- 재부팅 또는 시스템 충돌 후 이 오류 메시지가 표시되면 신뢰 지점 인증서를 다시 생성하는 것이 좋습니다.

```
ERR_SSL_VERSION_OR_CIPHER_MISMATCH
```

새 자체 서명 신뢰 지점 인증서를 생성하려면 지정된 순서대로 다음 명령을 사용합니다.

1. device# configure terminal
2. device(config)# no crypto pki trustpoint trustpoint_name
3. device(config)# no ip http server
4. device(config)# no ip http secure-server
5. device(config)# ip http server
6. device(config)# ip http secure-server

7. device(config)# ip http authentication local/aaa

- 명령으로 모빌리티 MAC 주소가 설정되어 있는지wireless mobility mac-address확인합니다.
- 이러한 프로토콜은 이제 17.9의 서비스 포트를 통해 지원됩니다.
    - Cisco DNA Center
    - Cisco 스마트 소프트웨어 관리자
    - Cisco Prime Infrastructure
    - Telnet
    - 컨트롤러 GUI
    - DNS
    - 파일 전송
    - GNMI
    - HTTP
    - HTTPS
    - LDAP
    - CSSM과 통신하기 위한 스마트 라이센싱 기능
    - Netconf
    - Netflow
    - NTP
    - RADIUS(CoA 포함)
    - Restconf
    - SNMP
    - SSH
    - SYSLOG
    - TACACS+
- 17.9의 AP 이미지가 원래 허용된 AP 플래시보다 큽니다. AP가 17.9 이미지를 다운로드할 때 공간이 충분하지 않다고 불평하는 경우, 릴리스 노트에서 설명한 대로 17.3.5를 통한 업그레이드 경로를 존중하지 않았거나 AP에서 이전 AireOS 이미지를 실행하고 있기 때문일 수 있습니다. 17.3.5 이상 WLC를 통해 전송하거나 AireOS 이미지를 최신 버전으로 업그레이드하면 17.9 이미지를 다운로드할 수 있도록 AP 플래시 크기가 조정됩니다.

17.11.1

- CCKM 기능은 Cisco IOS XE Dublin 17.10.x에서 더 이상 사용되지 않습니다.
- Smart Call Home은 더 이상 사용되지 않으며, Smart Transport의 라이센싱도 더 이상 사용되지 않습니다.
- 한 릴리스에서 다른 릴리스로 GUI를 업그레이드할 때 모든 GUI 페이지를 올바르게 다시 로드하려면 브라우저 캐시를 지우는 것이 좋습니다.

- Cisco IOS-XE 17.9.3 이상을 실행하는 AP는 디렉토리의 공간이 부족하여 소프트웨어를 업그레이드하려고 할 때 문제가 발생할 수/tmp있습니다. AP의/tmp공간이 가득 차면 새 AP 이미지의 다운로드가 방지됩니다. 이러한 경우에는 AP를 재부팅하는 것이 좋습니다.

  Wave 2 AP는 WAN 링크를 통해 소프트웨어를 업그레이드할 때 부팅 루프에 빠질 수 있습니다. 자세한 내용은 https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/220443-how-to-avoid-boot-loop-due-to-corrupted.html을 참조하십시오.

- Cisco IOS XE Cupertino 17.7.1 이상(Cisco Catalyst 9800-CL Wireless Controller의 경우), RUM 보고를 완료하고 제품 인스턴스에서 ACK를 한 번 이상 사용할 수 있는지 확인합니다. 이는 정확하고 최신 사용 정보가 CSSM에 반영되도록 하기 위한 것입니다. 이렇게 하지 않으면 라이센스 보고서가 승인될 때까지 최대 50개의 AP가 9800-CL에 참가할 수 있습니다.
- 1500 미만의 프래그먼트화는 OOB(Gi0) 인터페이스에서 무선 클라이언트에 의해 생성된 RADIUS 패킷에 대해 지원되지 않습니다.
- 17.3 이상, 9800-CL이 제대로 작동하려면 16GB의 디스크 공간이 필요합니다. WLC 인스턴스가 8GB OVA로 시작된 경우(17.3 이전 버전) 크기를 동적으로 늘릴 수 없습니다. 유일한 방법은 17.3 이후의 OVA에서 새 WLC를 생성하는 것입니다.
- Cisco Catalyst 9800-L Wireless Controller는 부팅 시간 동안 콘솔 포트에서 수신한 중단 신호에 응답하지 않아 사용자가 탐색에 이르지 못할 수 있습니다. 이 문제는 2019년 11월까지 제조된 컨트롤러에서 관찰되며, 기본 config-register 설정은 0x2102입니다. config-register를 0x2002로 설정하면 방지할 수 있습니다. 이 문제는 Cisco Catalyst 9800-L Wireless Controller의 16.12(3r) 규칙에서 해결되었습니다. rommon 업그레이드 방법에 대한 자세한 내용은 Upgrading Field Programmable Hardware Devices for Cisco Catalyst 9800 Series Wireless Controllers 문서의 Upgrading rommon for Cisco Catalyst 9800-L Wireless Controllers 섹션을 참조하십시오.

- 재부팅 또는 시스템 충돌 후 이 오류 메시지가 표시되면 신뢰 지점 인증서를 다시 생성하는 것이 좋습니다.

```
ERR_SSL_VERSION_OR_CIPHER_MISMATCH
```

새 자체 서명 신뢰 지점 인증서를 생성하려면 지정된 순서대로 다음 명령을 사용합니다.

1. device# configure terminal

2. device(config)# no crypto pki trustpoint trustpoint_name
3. device(config)# no ip http server
4. device(config)# no ip http secure-server
5. device(config)# ip http server
6. device(config)# ip http secure-server
7. device(config)# ip http authentication local/aaa

- 명령으로 모빌리티 MAC 주소가 설정되어 있는지wireless mobility mac-address확인합니다.
- 이러한 프로토콜은 이제 17.9의 서비스 포트를 통해 지원됩니다.
    - Cisco DNA Center
    - Cisco 스마트 소프트웨어 관리자
    - Cisco Prime Infrastructure
    - Telnet
    - 컨트롤러 GUI
    - DNS
    - 파일 전송
    - GNMI
    - HTTP
    - HTTPS
    - LDAP
    - CSSM과 통신하기 위한 스마트 라이센싱 기능
    - Netconf
    - Netflow
    - NTP
    - RADIUS(CoA 포함)
    - Restconf
    - SNMP
    - SSH

    - SYSLOG
    - TACACS+

- 17.9의 AP 이미지가 원래 허용된 AP 플래시보다 큽니다. AP가 17.9 이미지를 다운로드할 때 공간이 충분하지 않다고 불평하는 경우, 릴리스 노트에서 설명한 대로 17.3.5를 통한 업그레이드 경로를 존중하지 않았거나 AP에서 이전 AireOS 이미지를 실행하고 있기 때문일 수 있습니다. 17.3.5 이상 WLC를 통해 전송하거나 AireOS 이미지를 최신 버전으로 업그레이드하면 17.9 이미지를 다운로드할 수 있도록 AP 플래시 크기가 조정됩니다.

17.12.1

- CCKM 기능은 Cisco IOS XE Dublin 17.10.x에서 더 이상 사용되지 않습니다.
- Smart Call Home은 더 이상 사용되지 않으며, Smart Transport의 라이선스가 사용됩니다.
- 한 릴리스에서 다른 릴리스로 GUI를 업그레이드할 때 모든 GUI 페이지를 올바르게 다시 로드하려면 브라우저 캐시를 지우는 것이 좋습니다.

- Cisco IOS-XE 17.9.3 이상을 실행하는 AP는 디렉토리의 공간이 부족하여 소프트웨어를 업그레이드하려고 할 때 문제가 발생할 수/tmp있습니다. AP의/tmp공간이 가득 차면 새 AP 이미지의 다운로드가 방지됩니다. 이러한 경우에는 AP를 재부팅하는 것이 좋습니다.

  Wave 2 AP는 WAN 링크를 통해 소프트웨어를 업그레이드할 때 부팅 루프에 빠질 수 있습니다. 자세한 내용은 https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/220443-how-to-avoid-boot-loop-due-to-corrupted.html을 참조하십시오.

- 17.12.1 이상 릴리스에서는 Cisco IOS 기반 액세스 포인트(x700 Series 및 1570)에 대한 지원을 다시 제공합니다. 17.4와 17.9.2 사이에는 지원되지 않았습니다. 이러한 AP에 대한 지원은 일반적인 제품 라이프사이클 지원 이상으로 확장되지 않습니다. Cisco.com의 개별 End-of-Support 게시판을 참조하십시오.
- Cisco IOS XE Cupertino 17.7.1 이상(Cisco Catalyst 9800-CL Wireless Controller의 경우), RUM 보고를 완료하고 제품 인스턴스에서 ACK를 한 번 이상 사용할 수 있는지 확인합니다. 이는 정확하고 최신 사용 정보가 CSSM에 반영되도록 하기 위한 것입니다. 이렇게 하지 않으면 라이센스 보고서가 승인될 때까지 최대 50개의 AP가 9800-CL에 참가할 수 있습니다.
- 1500 미만의 프래그먼트화는 OOB(Gi0) 인터페이스에서 무선 클라이언트에 의해 생성된 RADIUS 패킷에 대해 지원되지 않습니다.
- 17.3 이상, 9800-CL이 제대로 작동하려면 16GB의 디스크 공간이 필요합니다. WLC 인스턴스가 8GB OVA로 시작된 경우(17.3 이전 버전) 크기를 동적으로 늘릴 수 없습니다. 유일한 방법은 17.3 이후의 OVA에서 새 WLC를 생성하는 것입니다.
- Cisco Catalyst 9800-L Wireless Controller는 부팅 시간 동안 콘솔 포트에서 수신한 중단 신호에 응답하지 않아 사용자가 탐색에 이르지 못할 수 있습니다. 이 문제는 2019년 11월까지 제조된 컨트롤러에서 관찰되며, 기본 config-register 설정은 0x2102입니다. config-register를 0x2002로 설정하면 이 문제를 방지할 수 있습니다. 이 문제는 Cisco Catalyst 9800-L Wireless Controller의 16.12(3r) 규칙에서 해결되었습니다. rommon 업그레이드 방법에 대한 자세한 내용은 Upgrading Field Programmable Hardware Devices for Cisco Catalyst 9800 Series Wireless Controllers 문서의 Upgrading rommon for Cisco Catalyst 9800-L Wireless Controllers 섹션을 참조하십시오.

- 재부팅 또는 시스템 충돌 후 이 오류 메시지가 표시되면 신뢰 지점 인증서를 다시 생성하는 것이 좋습니다.

```
ERR_SSL_VERSION_OR_CIPHER_MISMATCH
```

새 자체 서명 신뢰 지점 인증서를 생성하려면 지정된 순서대로 다음 명령을 사용합니다.

1. device# configure terminal
2. device(config)# no crypto pki trustpoint trustpoint_name
3. device(config)# no ip http server
4. device(config)# no ip http secure-server
5. device(config)# ip http server
6. device(config)# ip http secure-server
7. device(config)# ip http authentication local/aaa

- 명령으로 모빌리티 MAC 주소가 설정되어 있는지wireless mobility mac-address확인합니다.
- 이러한 프로토콜은 이제 17.9의 서비스 포트를 통해 지원됩니다.
  - Cisco DNA Center
  - Cisco 스마트 소프트웨어 관리자
  - Cisco Prime Infrastructure
  - Telnet
  - 컨트롤러 GUI
  - DNS
  - 파일 전송
  - GNMI
  - HTTP
  - HTTPS
  - LDAP
  - CSSM과 통신하기 위한 스마트 라이센싱 기능

    - Netconf
    - Netflow
    - NTP
    - RADIUS(CoA 포함)
    - Restconf
    - SNMP
    - SSH
    - SYSLOG
    - TACACS+

- 17.9의 AP 이미지가 원래 허용된 AP 플래시보다 큽니다. AP가 17.9 이미지를 다운로드할 때 공간이 충분하지 않다고 불평하는 경우, 릴리스 노트에서 설명한 대로 17.3.5를 통한 업그레이드 경로를 존중하지 않았거나 AP에서 이전 AireOS 이미지를 실행하고 있기 때문일 수 있습니다. 17.3.5 이상 WLC를 통해 전송하거나 AireOS 이미지를 최신 버전으로 업그레이드하면 17.9 이미지를 다운로드할 수 있도록 AP 플래시 크기가 조정됩니다.
- AP가 17.12 이상 릴리스로 업그레이드되면 콘솔 전송 속도가 즉시 변경되지 않습니다. 그러나 공장 초기화(또는 기본 제공되는 새 AP가 17.12 이상의 WLC에 조인하는 경우)의 경우 기본적으로 115200 콘솔 전송 속도가 사용됩니다.

다운그레이드

다운그레이드는 공식적으로 지원되지 않으며 새로운 기능의 컨피그레이션 손실이 발생할 수 있습니다. 그러나 실제 환경에서는 다운그레이드가 발생할 수 있으므로 다운그레이드를 방지하기 위해 이 문서에서는 여전히 가장 일반적인 트랩을 나열합니다. 필요한 정보를 찾으려면 다운그레이드할 버전(다운그레이드하기 전의 버전)을 확인하십시오.

지브롤터

16.12.2

- 여기서 지적할 것은 없습니다.

16.12.3

- Cisco Catalyst 9800 Wireless Controller가 17.x에서 16.12.4a로 다운그레이드될 때 지속적인 다시 로드가 관찰됩니다. 16.12.4a 대신 Cisco IOS XE Gibraltar 16.12.5로 다운그레이드하는 것이 좋습니다.

16.12.4

- 이 릴리스에서 더 낮은 릴리스로 다운그레이드하는 경우 Cisco 버그 ID CSCvt6990/Cisco 버그 ID CSCvv87417로 인해 원격 분석이 구성된 경우 WLC가 부팅 루프에 빠질 수 있습니다.
- Cisco Catalyst 9800 Wireless Controller를 17.x에서 16.12.4a로 다운그레이드하면 다시 로드할 수 있습니다. 이를 방지하려면 16.12.4a 대신 Cisco IOS XE Gibraltar 16.12.5로 다운그레이드하는 것이 좋습니다.

암스테르담

17.1.1

- 이 릴리스에서 더 낮은 릴리스로 다운그레이드하는 경우 Cisco 버그 ID CSCvt6990/CSCvv8741로 인해 원격 분석이 구성된 경우 WLC가 부팅 루프에 빠질 수 있습니다.
- Cisco Catalyst 9800 Wireless Controller가 17.x에서 16.12.4a로 다운그레이드될 때 지속적인 다시 로드가 관찰됩니다. 16.12.4a 대신 Cisco IOS XE Gibraltar 16.12.5로 다운그레이드하는 것이 좋습니다.

17.2.1

- 이 릴리스에서 더 낮은 릴리스로 다운그레이드하는 경우 Cisco 버그 ID CSCvt6990/Cisco 버그 ID CSCvv87417로 인해 원격 분석이 구성된 경우 WLC가 부팅 루프에 빠질 수 있습니다.
- Cisco IOS XE Amsterdam 17.3.1에서 이전 릴리스로 다운그레이드하면 4보다 높은 범위로 구성된 포트 채널이 사라집니다.
- Cisco Catalyst 9800 Wireless Controller가 17.x에서 16.12.4a로 다운그레이드될 때 지속적인 다시 로드가 관찰됩니다. 16.12.4a 대신 Cisco IOS XE Gibraltar 16.12.5로 다운그레이드하는 것이 좋습니다.

17.3.1

- 이 릴리스에서 더 낮은 릴리스로 다운그레이드하는 경우 Cisco 버그 ID CSCvt로 인해 텔레메트리를 구성한 경우 WLC가 부팅 루프에 들어갈 수 있습니다69990

  /CSCvv8741

- Cisco IOS XE Amsterdam 17.3.1에서 이전 릴리스로 다운그레이드하면 더 높은 범위로 구성된 포트 채널이 사라집니다.
- Cisco IOS XE Amsterdam 17.3.1에서 이전 릴리스로 다운그레이드하는 경우 17.3 이전에 존재하지 않는 '무선 국가' 명령을 구성한 경우 day-0 마법사를 다시 시작할 수 있습니다.
- Cisco Catalyst 9800 Wireless Controller가 17.x에서 16.12.4a로 다운그레이드될 때 지속적인 다시 로드가 관찰됩니다. 16.12.4a 대신 Cisco IOS XE Gibraltar 16.12.5로 다운그레이드하는 것이 좋습니다.
- Cisco IOS XE Amsterdam 17.3.x(로컬 스위칭 IPv6 AVC 지원)에서 Cisco IOS XE Gibraltar 16.12.x(로컬 스위칭 IPv6 AVC가 지원되지 않음)로 다운그레이드할 경우 WLAN 정책 프로필을 종료할 수 없습니다. 이러한 경우에는 기존 WLAN 정책 프로필을 삭제하고 새로 생성하는 것이 좋습니다.

17.3.2

- 이 릴리스에서 더 낮은 릴리스로 다운그레이드하면 Cisco 버그 ID CSCvt6990/Cisco 버그 ID CSCvv87417로 인해 텔레메트리를 구성한 경우 WLC가 부팅 루프로 종료됩니다.
- Cisco IOS XE Amsterdam 17.3.1에서 이전 릴리스로 다운그레이드하면 더 높은 범위로 구성된 포트 채널이 사라집니다.
- Cisco IOS XE Amsterdam 17.3.1에서 이전 릴리스로 다운그레이드하는 경우 17.3 이전에 존재하지 않는 '무선 국가' 명령을 구성한 경우 day-0 마법사를 다시 시작할 수 있습니다.
- Cisco Catalyst 9800 Wireless Controller가 17.x에서 16.12.4a로 다운그레이드될 때 지속적인 다시 로드가 관찰됩니다. 16.12.4a 대신 Cisco IOS XE Gibraltar 16.12.5로 다운그레이드하는 것이 좋습니다.
- Cisco IOS XE Amsterdam 17.3.x(로컬 스위칭 IPv6 AVC 지원)에서 Cisco IOS XE Gibraltar 16.12.x(로컬 스위칭 IPv6 AVC가 지원되지 않음)로 다운그레이드할 경우 WLAN 정책 프로필을 종료할 수 없습니다. 이러한 경우에는 기존 WLAN 정책 프로필을 삭제하고 새로 생성하는 것이 좋습니다.

17.3.3

- 이 릴리스에서 더 낮은 릴리스로 다운그레이드하는 경우 Cisco 버그 ID CSCvt6990/Cisco 버그 ID CSCvv87417로 인해 원격 분석이 구성된 경우 WLC가 부팅 루프에 빠질 수 있습니다.
- Cisco IOS XE Amsterdam 17.3.1에서 이전 릴리스로 다운그레이드하면 더 높은 범위로 구성된 포트 채널이 사라집니다.
- Cisco IOS XE Amsterdam 17.3.1에서 이전 릴리스로 다운그레이드하는 경우 17.3 이전에 존재하지 않는 '무선 국가' 명령을 구성한 경우 day-0 마법사를 다시 시작할 수 있습니다.
- Cisco Catalyst 9800 Wireless Controller가 17.x에서 16.12.4a로 다운그레이드될 때 지속적인 다시 로드가 관찰됩니다. 16.12.4a 대신 Cisco IOS XE Gibraltar 16.12.5로 다운그레이드하는 것이 좋습니다.
- Cisco IOS XE Amsterdam 17.3.x(로컬 스위칭 IPv6 AVC 지원)에서 Cisco IOS XE Gibraltar 16.12.x(로컬 스위칭 IPv6 AVC가 지원되지 않음)로 다운그레이드할 경우 WLAN 정책 프로필을 종료할 수 없습니다. 이러한 경우에는 기존 WLAN 정책 프로필을 삭제하고 새로 생성하는 것이 좋습니다.

17.4.1

- Cisco IOS XE Amsterdam 17.4.1에서 17.3 이전 릴리스로 다운그레이드하는 경우 17.3 이전에 존재하지 않는 '무선 국가' 명령을 구성한 경우 day-0 마법사를 다시 받을 수 있습니다.
- Cisco IOS XE Amsterdam 17.4.1에서 이전 릴리스로 다운그레이드하면 17.4에서 이전 버전에서 지원되지 않는 명령인 명명된 텔레메트리 대상을 사용하므로 텔레메트리 연결이 끊어집니다. 텔레메트리 연결을 다시 생성해야 합니다.
- Cisco Catalyst 9800 Wireless Controller가 17.x에서 16.12.4a로 다운그레이드될 때 지속적인 다시 로드가 관찰됩니다. 16.12.4a 대신 Cisco IOS XE Gibraltar 16.12.5로 다운그레이드하는 것이 좋습니다.

17.5.1

- Cisco IOS XE Amsterdam 17.4.1에서 17.3 이전 릴리스로 다운그레이드하는 경우 17.3 이전

에 존재하지 않는 '무선 국가' 명령을 구성한 경우 day-0 마법사를 다시 받을 수 있습니다.
- Cisco IOS XE Amsterdam 17.4.1에서 이전 릴리스로 다운그레이드하면 17.4에서 이전 버전에서 지원되지 않는 명령인 명명된 텔레메트리 대상을 사용하므로 텔레메트리 연결이 끊어집니다. 텔레메트리 연결을 다시 생성해야 합니다.
- Cisco Catalyst 9800 Wireless Controller가 17.x에서 16.12.4a로 다운그레이드될 때 지속적인 다시 로드가 관찰됩니다. 16.12.4a 대신 Cisco IOS XE Gibraltar 16.12.5로 다운그레이드하는 것이 좋습니다.

17.9.x

- 802.1x 비밀번호는 암호화되므로 이 릴리스에서 일반 텍스트로 볼 수 없습니다. 암호화된 비밀번호를 지원하지 않는 이전 이미지로 다운그레이드하면 AP가 중단되고 잘못된 자격 증명 때문에 dot1x 인증에 반복적으로 실패합니다. 일반 텍스트 비밀번호를 설정하기 전에 AP가 컨트롤러에 조인할 수 있도록 AP 스위치 포트에서 802.1x를 비활성화해야 합니다.

17.10.1

- 이 릴리스에서 802.1x 비밀번호는 암호화되므로 일반 텍스트로 표시되지 않습니다. 암호화된 비밀번호를 지원하지 않는 이전 이미지로 다운그레이드하면 AP가 중단되고 잘못된 자격 증명 때문에 dot1x 인증에 반복적으로 실패합니다. 일반 텍스트 비밀번호를 설정하기 전에 AP가 컨트롤러에 조인할 수 있도록 AP 스위치 포트에서 802.1x를 비활성화해야 합니다.

17.11.1

- 이 릴리스에서 802.1x 비밀번호는 암호화되므로 일반 텍스트로 표시되지 않습니다. 암호화된 비밀번호를 지원하지 않는 이전 이미지로 다운그레이드하면 AP가 중단되고 잘못된 자격 증명 때문에 dot1x 인증에 반복적으로 실패합니다. 일반 텍스트 비밀번호를 설정하기 전에 AP가 컨트롤러에 조인할 수 있도록 AP 스위치 포트에서 802.1x를 비활성화해야 합니다.

17.12.x

- 이 릴리스에서 802.1x 비밀번호는 암호화되므로 일반 텍스트로 표시되지 않습니다. 암호화된 비밀번호를 지원하지 않는 이전 이미지로 다운그레이드하면 AP가 중단되고 잘못된 자격 증명 때문에 dot1x 인증에 반복적으로 실패합니다. 일반 텍스트 비밀번호를 설정하기 전에 AP가 컨트롤러에 조인할 수 있도록 AP 스위치 포트에서 802.1x를 비활성화해야 합니다.

관련 정보

- 17.1 핫 패칭 및 롤링 AP 업그레이드 가이드
- 17.3 핫 패칭 및 ISSU 업그레이드 가이드.
- Cisco 기술 지원 및 다운로드

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.