

# WLC에서 802.11w 관리 프레임 보호 구성

## 목차

---

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[MMIE\(관리 MIC 정보 요소\)](#)

[RSN IE에 대한 변경 사항](#)

[802.11w 관리 프레임 보호의 이점](#)

[802.11w를 사용하기 위한 요구 사항](#)

[구성](#)

[GUI](#)

[CLI](#)

[다음을 확인합니다.](#)

[문제 해결](#)

---

## 소개

이 문서에서는 IEEE 802.11w 관리 프레임 보호 및 Cisco WLC(Wireless LAN Controller)의 컨피그레이션에 대한 자세한 내용을 설명합니다.

## 사전 요구 사항

### 요구 사항

코드 7.6 이상을 실행하는 Cisco WLC에 대해 알고 있는 것이 좋습니다.

### 사용되는 구성 요소

이 문서의 정보는 코드 7.6을 실행하는 WLC 5508을 기반으로 합니다.

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

802.11w 표준은 위조 및 재생 공격으로부터 제어 및 관리 프레임과 강력한 관리 프레임을 보호하는데 목적이 있습니다. 보호되는 프레임 유형에는 Disassociation(연결 해제), Deauthentication(인증 해제), Robust Action(강력한 작업) 프레임(예:

- 스펙트럼 관리
- QoS(Quality of Service)
- 블록 Ack
- 무선 측정
- BSS(Fast Basic Service Set) 전환

802.11w는 프레임을 암호화하지 않지만 관리 프레임을 보호합니다. 메시지가 합법적인 소스에서 오도록 보장합니다. 그러기 위해서는 MIC(Message Integrity Check) 요소를 추가해야 합니다. 802.11w는 브로드캐스트/멀티캐스트 강력한 관리 프레임을 보호하는 데 사용되는 IGTK(Integrity Group Temporal Key)라는 새로운 키를 도입했습니다. 이는 WPA(Wireless Protected Access)와 함께 사용되는 4방향 키 핸드셰이크 프로세스의 일부로 파생됩니다. 따라서 802.11w를 사용해야 하는 경우 dot1x/PSK(Pre-Shared Key)가 필수 조건이 됩니다. 개방형/webauth SSID(Service Set Identifier)와 함께 사용할 수 없습니다.


관리 프레임 보호가 협상되면 AP(액세스 포인트)는 4방향 핸드셰이크의 메시지 3에서 전달되는 EAPOL 키 프레임의 GTK 및 IGTK 값을 암호화합니다. AP가 나중에 GTK를 변경하면 그룹 키 핸드셰이크를 사용하여 클라이언트에 새 GTK 및 IGTK를 전송합니다. IGTK 키를 사용하여 계산된 MIC를 추가합니다.

### MMIE(관리 MIC 정보 요소)

802.11w에는 관리 MIC 정보 요소라는 새로운 정보 요소가 도입되었습니다. 그림과 같은 헤더 형식을 가지고 있습니다.

1	1	2	6	8
Element ID	Length	KeyID	IPN	MIC

여기서 중요한 필드는 요소 ID와 MIC입니다. MMIE의 요소 ID는 0x4c 또한 무선 캡처를 분석할 때 유용한 식별자로 사용됩니다.

 참고: MIC - 관리 프레임에 대해 계산된 메시지 무결성 코드가 포함되어 있습니다. AP에서 이 기능이 추가된다는 점에 유의하십시오. 그런 다음 대상 클라이언트는 프레임에 대한 MIC를 다시 계산하고 이를 AP에서 전송한 값과 비교합니다. 값이 다르면 유효하지 않은 프레임으로 거부됩니다.

### RSN IE에 대한 변경 사항

강력한 RSN IE(Security Network Information Element)는 AP에서 지원하는 보안 매개변수를 지정합니다. 802.11w는 AP가 브로드캐스트/멀티캐스트 강력한 관리 프레임을 보호하기 위해 사용하는 암호 그룹 선택기를 포함하는 RSN IE에 Group Management Cipher Suite 선택기를 도입합니다. 이는 AP가 802.11w를 실행하는지 여부를 확인하는 가장 좋은 방법입니다. 이는 그림과 같이 검증할 수도 있다.

Filter: wlan\_mgt.ssid == "PMF" Expression... Clear Apply Save

802.11 Channel: Channel Offset: FCS Filter: All Frames None Wireless Settings... Decryption Keys...

No.	Time	Source	Destination	DSCP	Protocol	VLAN	Length	Info
43	0.97510900	Cisco_21:c9:74	IntelCor_20:52:b8	802.11	285	Probe Response, SN=127, FN=0, Flags=...R..., BI=102, SSID=PMF [Malformed Packet]		
68	1.20985500	Cisco_21:c9:74	IntelCor_20:52:b8	802.11	285	Probe Response, SN=132, FN=0, Flags=...R..., BI=102, SSID=PMF [Malformed Packet]		
108	2.07189800	Cisco_21:c9:74	Broadcast	802.11	291	Beacon frame, SN=3969, FN=0, Flags=..., BI=102, SSID=PMF [Malformed Packet]		
117	2.14027800	Cisco_21:c9:7b	IntelCor_20:52:b8	802.11	285	Probe Response, SN=74, FN=0, Flags=...R..., BI=102, SSID=PMF [Malformed Packet]		
122	2.15696900	Cisco_21:c9:7b	Broadcast	802.11	291	Beacon frame, SN=3185, FN=0, Flags=..., BI=102, SSID=PMF [Malformed Packet]		
217	5.98307800	Cisco_21:c9:74	IntelCor_20:52:b8	802.11	285	Probe Response, SN=137, FN=0, Flags=...R..., BI=102, SSID=PMF [Malformed Packet]		
241	6.19374400	Cisco_21:c9:74	IntelCor_20:52:b8	802.11	285	Probe Response, SN=142, FN=0, Flags=...R..., BI=102, SSID=PMF [Malformed Packet]		
271	8.00264200	Cisco_21:c9:74	IntelCor_20:52:b8	802.11	285	Probe Response, SN=166, FN=0, Flags=...R..., BI=102, SSID=PMF [Malformed Packet]		
272	8.00588300	Cisco_21:c9:74	IntelCor_20:52:b8	802.11	285	Probe Response, SN=167, FN=0, Flags=...R..., BI=102, SSID=PMF [Malformed Packet]		

```

Tag: HT Capabilities (802.11n D1.10)
Tag: RSN Information
Tag Number: RSN Information (48)
Tag length: 26
RSN Version: 1
Group Cipher Suite: 00-0F-ac (Ieee8021) AES (CCM)
Pairwise Cipher Suite Count: 1
Pairwise Cipher Suite List 00-0F-ac (Ieee8021) AES (CCM)
Auth Key Management (AKM) Suite Count: 1
Auth Key Management (AKM) List 00-0F-ac (Ieee8021) WPA (SHA256)
RSN Capabilities: 0x00e8
... ..0 = RSN Pre-Auth capabilities: Transmitter does not support pre-authentication
... ..0 = RSN No Pairwise capabilities: Transmitter can support WEP default key 0 simultaneously with Pairwise key
... ..10 = RSN PTKSA Replay Counter capabilities: 4 replay counters per PTKSA/GTKSA/STakeysA (0x0002)
... ..10 = RSN GTKSA Replay Counter capabilities: 4 replay counters per PTKSA/GTKSA/STakeysA (0x0002)
... ..1 = Management Frame Protection Required: True
... ..1 = Management Frame Protection Capable: True
... ..0 = PeerKey Enabled: False
PMKID Count: 0
PMKID List
Group Management Cipher Suite: 00-0F-ac (Ieee8021) BIP
Group Management Cipher Suite OUI: 00-0F-ac (Ieee8021)
Group Management Cipher Suite type: BIP (6)
Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
  
```

여기서는 802.11w가 사용되고 있음을 보여 주는 group management cipher suite 필드를 찾을 수 있습니다.

RSN 기능 하에서도 변경이 있었습니다. 이제 비트 6과 7은 802.11w에 대한 서로 다른 파라미터를 나타내기 위해 사용된다.

- 비트 6: MFPR(Management Frame Protection Required) - STA는 강력한 관리 프레임 보호가 필수임을 알리기 위해 이 비트를 1로 설정합니다.
- 비트 7: MFPC(Management Frame Protection Capable) - STA는 강력한 관리 프레임 보호가 활성화되었음을 알리기 위해 이 비트를 1로 설정합니다. AP는 이를 설정할 때 관리 프레임 보호를 지원함을 알립니다.

컨피그레이션 옵션에서 필요에 따라 관리 프레임 보호를 설정하면 비트 6과 7이 모두 설정됩니다. 이 내용은 패킷 캡처 이미지에 나와 있습니다.

Filter: wlan\_mgt.ssid == "PMF" Expression... Clear Apply Save

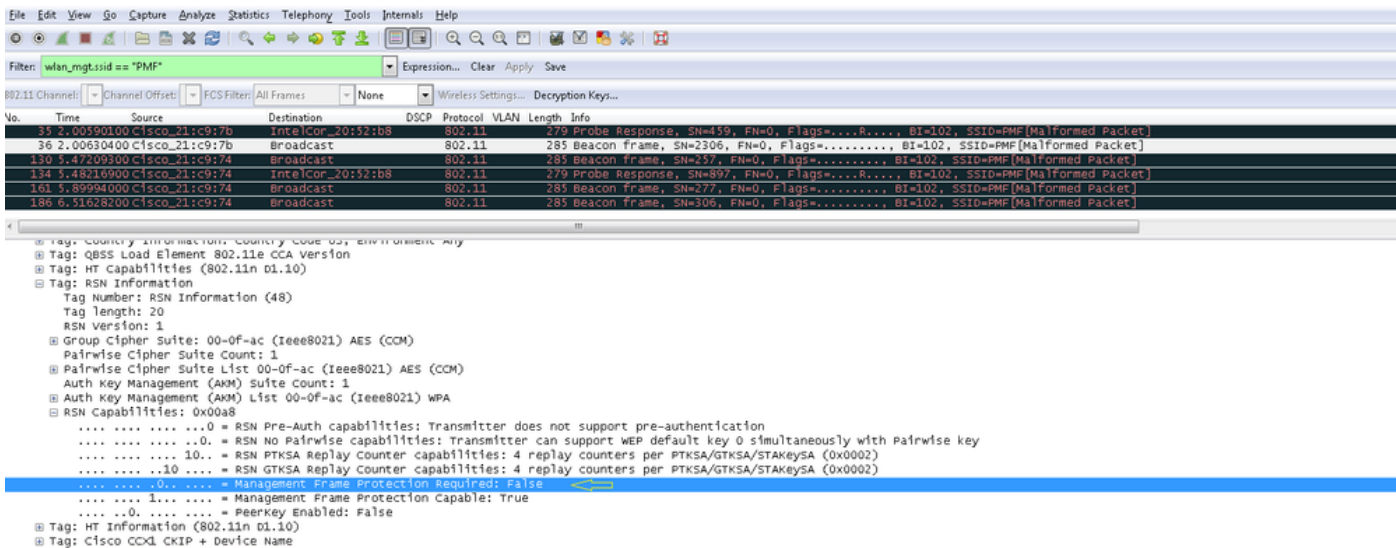
802.11 Channel: Channel Offset: FCS Filter: All Frames None Wireless Settings... Decryption Keys...

No.	Time	Source	Destination	DSCP	Protocol	VLAN	Length	Info
43	0.97510900	Cisco_21:c9:74	IntelCor_20:52:b8	802.11	285	Probe Response, SN=127, FN=0, Flags=...R..., BI=102, SSID=PMF [Malformed Packet]		
68	1.20985500	Cisco_21:c9:74	IntelCor_20:52:b8	802.11	285	Probe Response, SN=132, FN=0, Flags=...R..., BI=102, SSID=PMF [Malformed Packet]		
108	2.07189800	Cisco_21:c9:74	Broadcast	802.11	291	Beacon frame, SN=3969, FN=0, Flags=..., BI=102, SSID=PMF [Malformed Packet]		
117	2.14027800	Cisco_21:c9:7b	IntelCor_20:52:b8	802.11	285	Probe Response, SN=74, FN=0, Flags=...R..., BI=102, SSID=PMF [Malformed Packet]		
122	2.15696900	Cisco_21:c9:7b	Broadcast	802.11	291	Beacon frame, SN=3185, FN=0, Flags=..., BI=102, SSID=PMF [Malformed Packet]		
217	5.98307800	Cisco_21:c9:74	IntelCor_20:52:b8	802.11	285	Probe Response, SN=137, FN=0, Flags=...R..., BI=102, SSID=PMF [Malformed Packet]		
241	6.19374400	Cisco_21:c9:74	IntelCor_20:52:b8	802.11	285	Probe Response, SN=142, FN=0, Flags=...R..., BI=102, SSID=PMF [Malformed Packet]		
271	8.00264200	Cisco_21:c9:74	IntelCor_20:52:b8	802.11	285	Probe Response, SN=166, FN=0, Flags=...R..., BI=102, SSID=PMF [Malformed Packet]		
272	8.00588300	Cisco_21:c9:74	IntelCor_20:52:b8	802.11	285	Probe Response, SN=167, FN=0, Flags=...R..., BI=102, SSID=PMF [Malformed Packet]		

```

Tag: HT Capabilities (802.11n D1.10)
Tag: RSN Information
Tag Number: RSN Information (48)
Tag length: 26
RSN Version: 1
Group Cipher Suite: 00-0F-ac (Ieee8021) AES (CCM)
Group Cipher Suite OUI: 00-0F-ac (Ieee8021)
Group Cipher Suite type: AES (CCM) (4)
Pairwise Cipher Suite Count: 1
Pairwise Cipher Suite List 00-0F-ac (Ieee8021) AES (CCM)
Pairwise Cipher Suite: 00-0F-ac (Ieee8021) AES (CCM)
Pairwise Cipher Suite OUI: 00-0F-ac (Ieee8021)
Pairwise Cipher Suite type: AES (CCM) (4)
Auth Key Management (AKM) Suite Count: 1
Auth Key Management (AKM) List 00-0F-ac (Ieee8021) WPA (SHA256)
RSN Capabilities: 0x00e8
... ..0 = RSN Pre-Auth capabilities: Transmitter does not support pre-authentication
... ..0 = RSN No Pairwise capabilities: Transmitter can support WEP default key 0 simultaneously with Pairwise key
... ..10 = RSN PTKSA Replay Counter capabilities: 4 replay counters per PTKSA/GTKSA/STakeysA (0x0002)
... ..10 = RSN GTKSA Replay Counter capabilities: 4 replay counters per PTKSA/GTKSA/STakeysA (0x0002)
... ..1 = Management Frame Protection Required: True
... ..1 = Management Frame Protection Capable: True
... ..0 = PeerKey Enabled: False
  
```

그러나 이 옵션을 선택 사항으로 설정하면 이미지에 표시된 대로 비트 7만 설정됩니다.



 참고: WLC는 연결/재연결 응답에 이 수정된 RSN IE를 추가하고 AP는 비콘 및 프로브 응답에 이 수정된 RSN IE를 추가합니다.

## 802.11w 관리 프레임 보호의 이점


- 클라이언트 보호

이는 Deauthentication 및 Disassociation 프레임에 암호화 보호가 추가됨으로써 가능합니다. 이렇게 하면 권한이 없는 사용자가 합법적인 사용자의 MAC 주소를 스푸핑하여 DOS(서비스 거부) 공격을 시작하고 deauth/disassociation 프레임을 전송하는 것을 방지할 수 있습니다.

- AP 보호

SA(Security Association) 해체 보호 메커니즘이 추가되어 인프라 측 보호가 추가됩니다. 이 메커니즘은 연결 재기 시간 및 SA-Query 절차로 구성됩니다. 802.11w 이전에 AP가 이미 연결된 클라이언트로부터 연결 또는 인증 요청을 받은 경우 AP는 현재 연결을 종료하고 새 연결을 시작합니다. 802.11w MFP를 사용할 때 STA가 연결되어 있고 관리 프레임 보호를 협상한 경우 AP는 반환 상태 코드 30으로 연결 요청을 거부합니다 Association request rejected temporarily; Try again later 고객에게 제공합니다.

Association Response에는 AP가 이 STA과의 연결을 허용할 준비가 되었을 때의 컴백 시간을 지정하는 Association Reback Time 정보 요소가 포함되어 있습니다. 이렇게 하면 스푸핑된 연결 요청으로 인해 합법적인 클라이언트가 연결 해제되지 않도록 할 수 있습니다.

 참고: 클라이언트가 802.11w PMF를 사용하지 않는 경우 WLC(AireOS 또는 9800)는 클라이언트에서 보낸 연결 해제 또는 인증 해제 프레임을 무시합니다. 클라이언트가 PMF를 사용하는 경우 클라이언트 항목은 그러한 프레임을 수신하는 즉시 삭제됩니다. 이는 PMF가 없는 프레임에는 보안이 없으므로 악의적인 장치의 서비스 거부를 피하기 위한 것입니다.

## 802.11w를 사용하기 위한 요구 사항

- 802.11w에서는 dot1x 또는 PSK로 SSID를 구성해야 합니다.
- 802.11w는 모든 802.11n 지원 AP에서 지원됩니다. 즉, AP 1130 및 1240은 802.11w를 지원

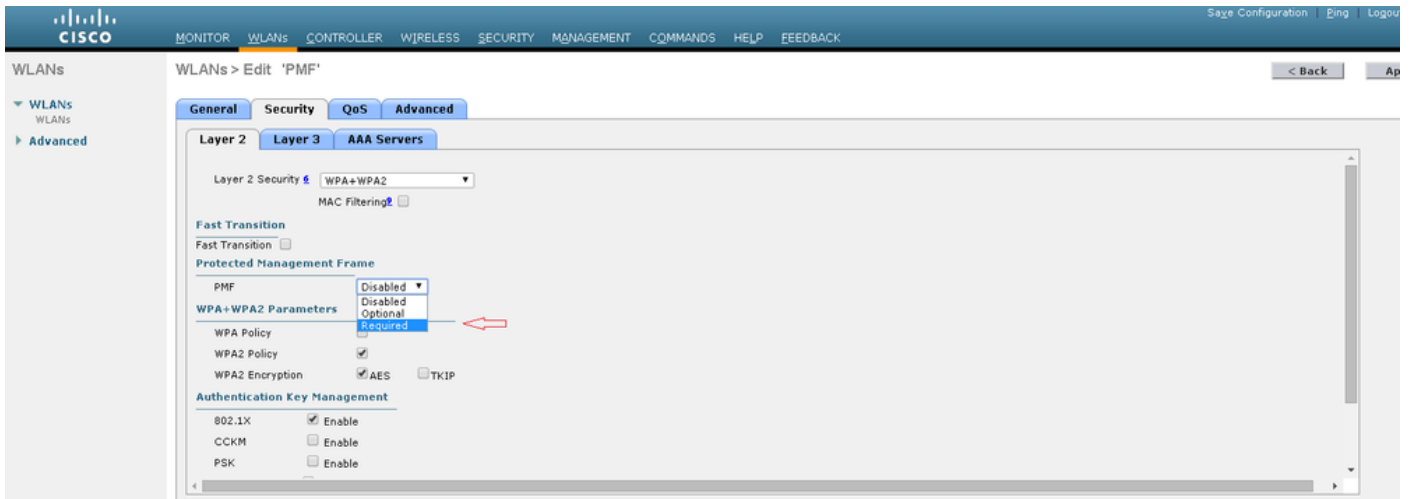
하지 않습니다.

- 802.11w는 7.4 릴리스의 flexconnect AP 및 7510 WLC에서 지원되지 않습니다. 7.5 릴리스부터 지원이 추가되었습니다.

## 구성

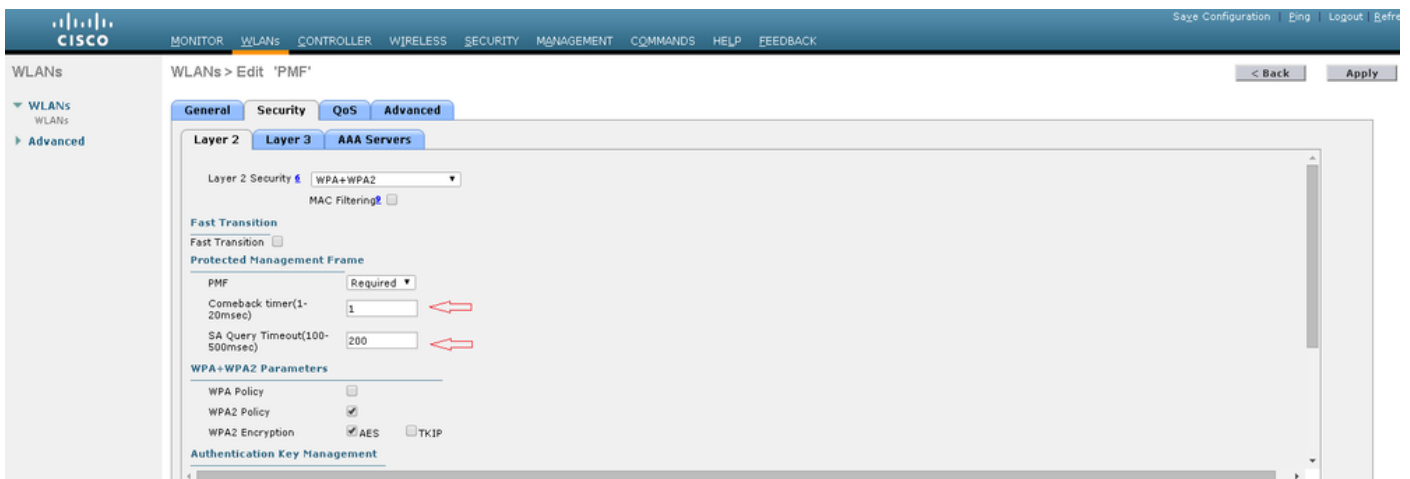
### GUI

1단계. 802.1x/PSK로 구성된 SSID에서 보호된 관리 프레임을 활성화해야 합니다. 그림과 같이 세 가지 옵션이 있습니다.

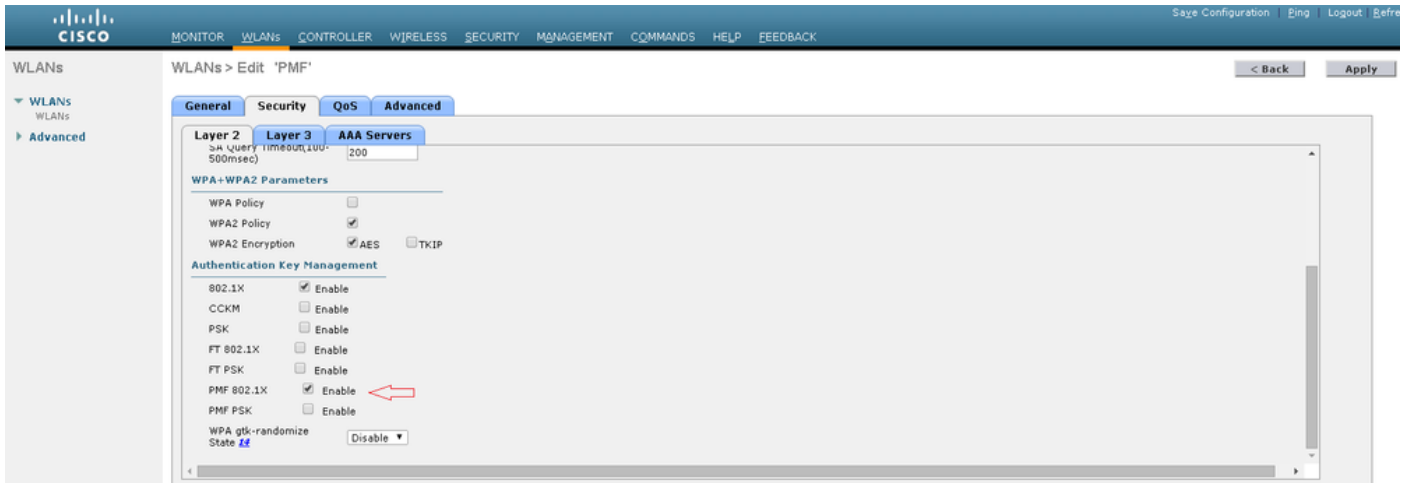


'필수'는 802.11w를 지원하지 않는 클라이언트는 연결할 수 없도록 지정합니다. '선택 사항'은 802.11w를 지원하지 않는 클라이언트도 연결할 수 있도록 지정합니다.

2단계. 그런 다음 재기 타이머 및 SA 쿼리 시간 제한을 지정해야 합니다. 컴백 타이머는 상태 코드 30으로 처음 거부된 경우 연결을 다시 시도하기 전에 연결된 클라이언트가 기다려야 하는 시간을 지정합니다. SA 쿼리 시간 초과는 WLC가 쿼리 프로세스에 대한 클라이언트의 응답을 기다리는 시간을 지정합니다. 클라이언트에서 응답이 없는 경우 컨트롤러에서 연결이 삭제됩니다. 이 작업은 이미지에 표시된 대로 수행됩니다.



3단계. 인증 키 관리 방법으로 802.1x를 사용하는 경우 'PMF 802.1x'를 활성화해야 합니다. PSK를 사용하는 경우 이미지에 표시된 대로 PMF PSK 확인란을 선택해야 합니다.



## CLI

- 11w 기능을 활성화하거나 비활성화하려면 다음 명령을 실행합니다.

```
config wlan security wpa akm pmf 802.1x enable/disable
```

```
config wlan security wpa akm pmf psk enable/disable
```

- 보호된 관리 프레임을 활성화하거나 비활성화하려면 다음 명령을 실행합니다.

```
config wlan security pmf optional/required/disable
```

- 연결 복귀 시간 설정:

```
config wlan security pmf 11w-association-comeback
```

- SA 쿼리 다시 시도 시간 초과 설정:

```
config wlan security pmf saquery-retry-time
```

## 다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

802.11w 구성을 확인할 수 있습니다. WLAN 컨피그레이션을 확인합니다.

```
(wlc)>show wlan 1
Wi-Fi Protected Access (WPA/WPA2)..... Enabled
<snip>
802.1x..... Enabled
PSK..... Disabled
CCKM..... Disabled
FT-1X(802.11r)..... Disabled
FT-PSK(802.11r)..... Disabled
PMF-1X(802.11w)..... Enabled
PMF-PSK(802.11w)..... Disabled
FT Reassociation Timeout..... 20
FT Over-The-DS mode..... Enabled
GTK Randomization..... Disabled
<snip>
PMF..... Required
PMF Association Comeback Time..... 1
PMF SA Query RetryTimeout..... 200
```

## 문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

이러한 debug 명령은 WLC에서 802.11w 문제를 해결하는 데 사용할 수 있습니다.

- **debug 11w-pmf events enable/disable**
- debug 11w-pmf keys enable/disable
- debug 11w-pmf all enable

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.