# Konfigurieren des 802.11w Management Frame Protection auf dem WLC

## Inhalt

[Einleitung](#)
[Voraussetzungen](#)
[Anforderungen](#)
[Verwendete Komponenten](#)
[Hintergrundinformationen](#)
[Management MIC Information Element (MMIE)](#)
[Änderungen an RSN IE](#)
[Vorteile des 802.11w Management Frame Protection](#)
[Voraussetzungen für 802.11w](#)
[Konfigurieren](#)
[GUI](#)
[CLI](#)
[Überprüfung](#)
[Fehlerbehebung](#)

## Einleitung

In diesem Dokument werden Details zum IEEE 802.11w Management Frame Protection und seiner Konfiguration auf dem Cisco Wireless LAN Controller (WLC) beschrieben.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse des Cisco WLC mit Code 7.6 oder höher verfügen.

### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf WLC 5508, der Code 7.6 ausführt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

## Hintergrundinformationen

Der 802.11w-Standard soll Kontroll- und Management-Frames sowie eine Reihe robuster Management-Frames vor Fälschungs- und Replay-Angriffen schützen. Zu den geschützten Frametypen gehören Frames zur Aufhebung der Zuordnung, zur Deauthentifizierung und zur robusten Aktion, z. B.:

- Spektrum-Management
- Quality of Service (QoS)

- Bestätigung blockieren
- Funkmessung
- Fast Basic Service Set (BSS)-Umstellung

802.11w verschlüsselt die Frames nicht, schützt jedoch die Management-Frames. Es stellt sicher, dass die Nachrichten aus legitimen Quellen stammen. Dazu müssen Sie ein MIC-Element (Message Integrity Check) hinzufügen. 802.11w hat einen neuen Schlüssel eingeführt, den Integrity Group Temporal Key (IGTK), der für den Schutz robuster Broadcast-/Multicast-Management-Frames verwendet wird. Dies wird als Teil des Vier-Wege-Handshake-Prozesses abgeleitet, der mit Wireless Protected Access (WPA) verwendet wird. Daher ist der dot1x/Pre-Shared Key (PSK) eine Voraussetzung für die Verwendung von 802.11w. Es kann nicht mit einem offenen/webauthentischen Service Set Identifier (SSID) verwendet werden.

Wenn der Management Frame Protection ausgehandelt wird, verschlüsselt der Access Point (AP) die GTK- und IGTK-Werte im EAPOL-Key-Frame, der in Meldung 3 des 4-Wege-Handshakes übermittelt wird. Wenn der WAP später den GTK ändert, sendet er den neuen GTK und IGTK unter Verwendung des Group Key Handshake an den Client. Es fügt ein MIC hinzu, das mithilfe des IGTK-Schlüssels berechnet wird.

## Management MIC Information Element (MMIE)

In 802.11w wird ein neues Informationselement eingeführt, das Management MIC-Informationselement. Es hat das Header-Format, wie im Bild gezeigt.

| 1 | 1 | 2 | 6 | 8 |
|---|---|---|---|---|
| Element ID | Length | KeyID | IPN | MIC |

Die wichtigsten Problemfelder sind hierbei die **Element-ID** und das **MIC**. Die Element-ID für MMIE ist 0x4c und dient als nützliche Identifizierung, wenn Sie die Wireless-Aufnahmen analysieren.

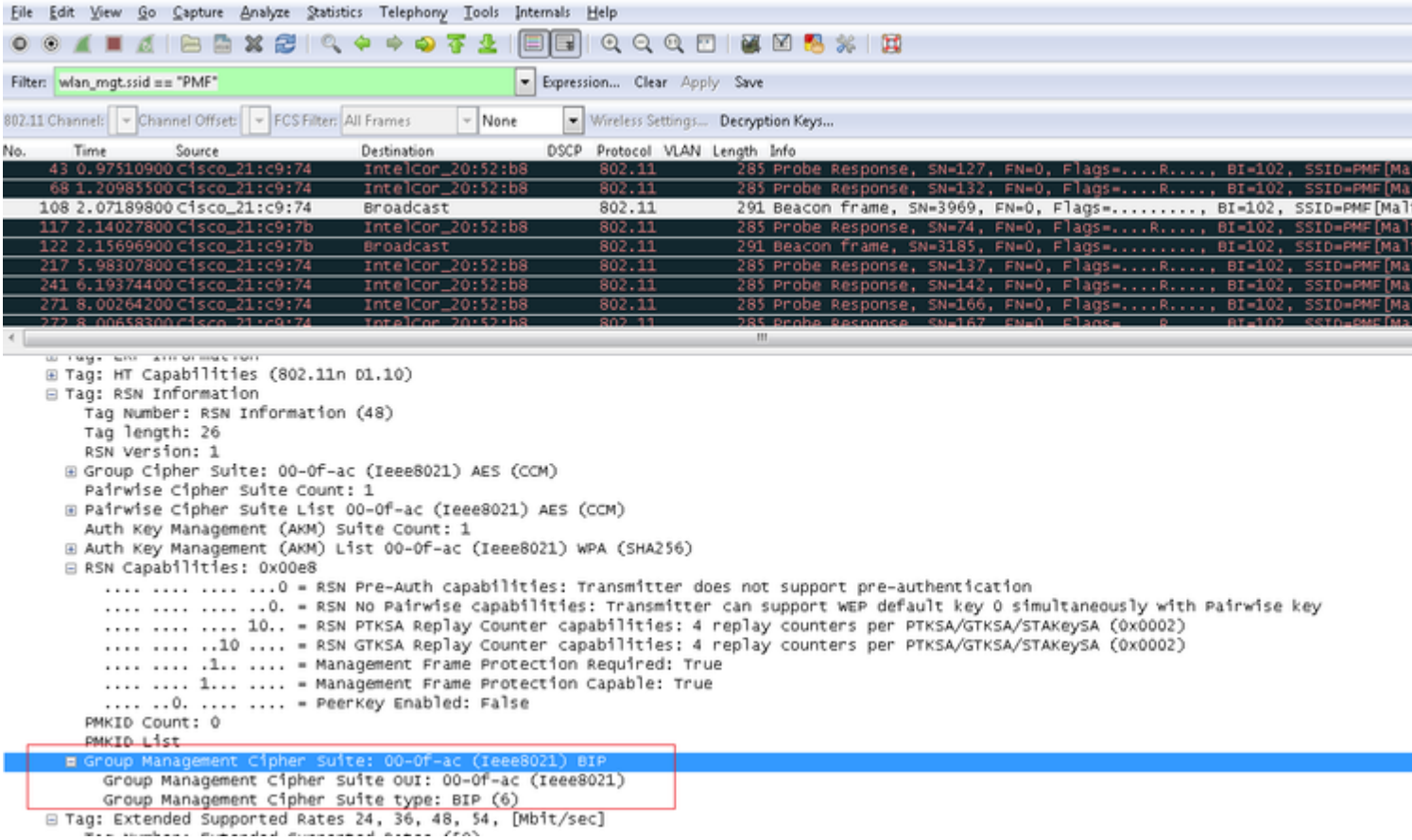
---

> **Hinweis**: MIC: Dieser enthält den Integritätscode der Nachricht, der über den Management-Frame berechnet wird. Beachten Sie, dass dies am Access Point hinzugefügt wird. Der Ziel-Client berechnet dann das MIC für den Frame neu und vergleicht es mit den Daten, die vom Access Point gesendet wurden. Wenn sich die Werte unterscheiden, wird dies als ungültiger Frame zurückgewiesen.

---

## Änderungen an RSN IE

Robust Security Network Information Element (RSN IE) legt die vom WAP unterstützten Sicherheitsparameter fest. Mit 802.11w wird RSN IE ein Group Management Cipher Suite-Selektor hinzugefügt, der den vom Access Point verwendeten Cipher Suite-Selektor zum Schutz robuster Broadcast-/Multicast-Management-Frames enthält. Dies ist die beste Methode, um zu erfahren, ob ein AP 802.11w unterstützt. Dies kann auch überprüft werden, wie im Bild gezeigt.

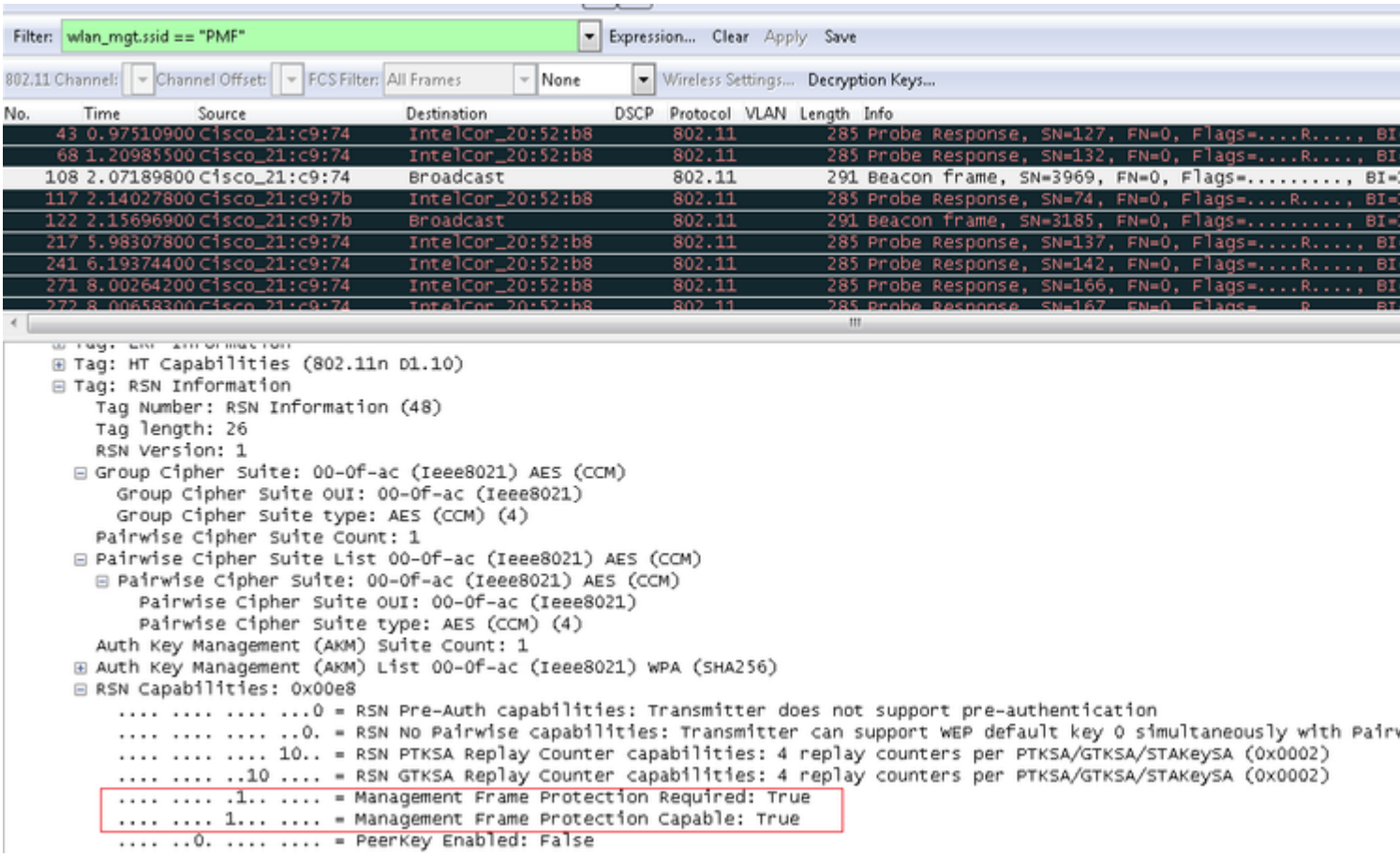



Hier finden Sie das Feld **Group Management Cipher Suite**, das anzeigt, dass 802.11w verwendet wird.

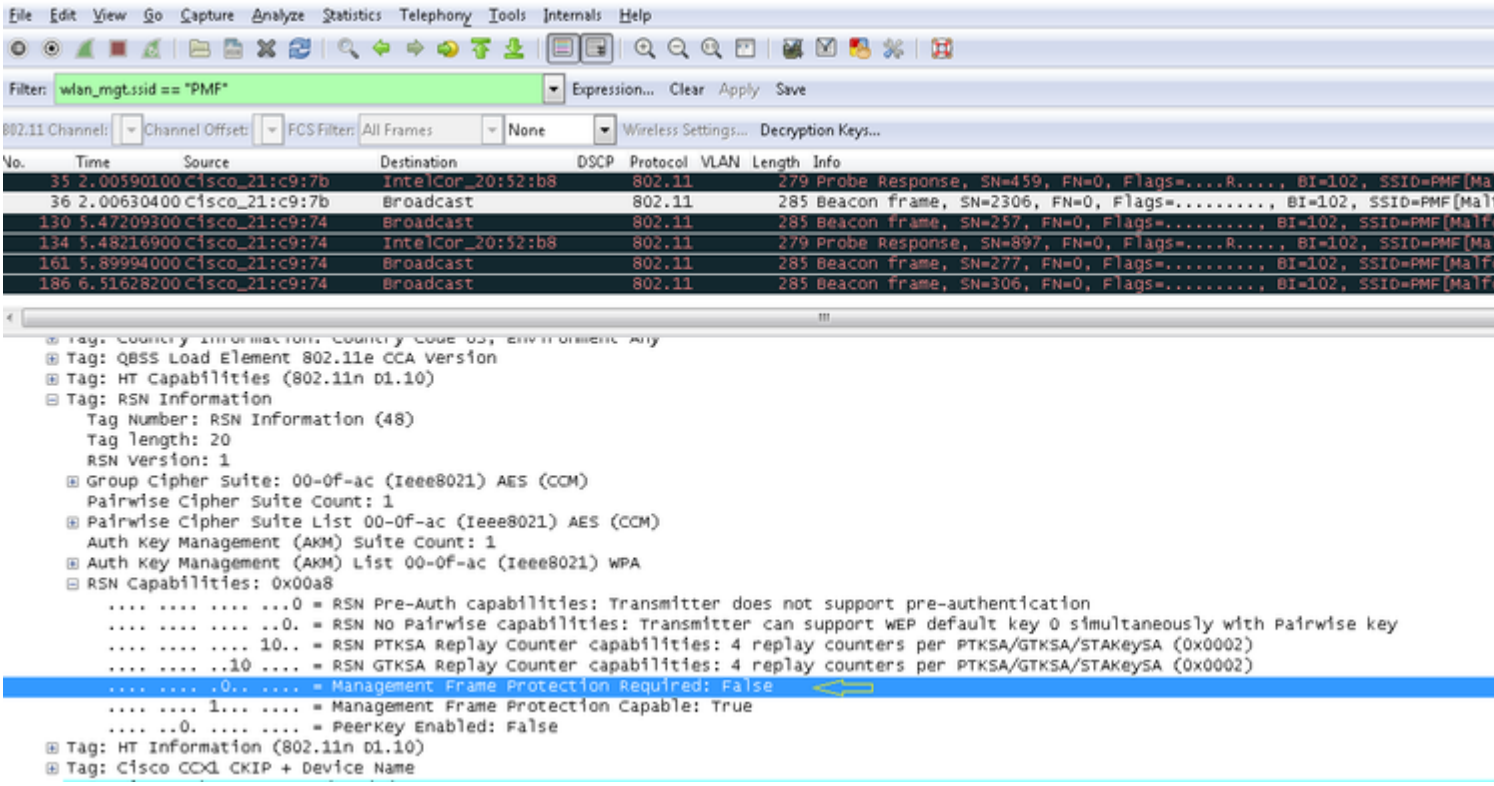
Auch bei den RSN-Funktionen wurden Änderungen vorgenommen. Die Bits 6 und 7 werden jetzt verwendet, um verschiedene Parameter für 802.11w anzugeben.

- Bit 6: Management Frame Protection Required (MFPR) - Ein STA setzt dieses Bit auf 1, um anzukündigen, dass der Schutz von robusten Management-Frames obligatorisch ist.
- Bit 7: Management Frame Protection Capable (MFPC) - Ein STA setzt dieses Bit auf 1, um anzukündigen, dass der Schutz von robusten Management-Frames aktiviert ist. Wenn der Access Point diese Einstellung festlegt, informiert er, dass er den Management-Frame-Schutz unterstützt.

Wenn Sie den Management-Frame-Schutz gemäß den Konfigurationsoptionen festlegen, werden sowohl Bit 6 als auch Bit 7 festgelegt. Dies ist im folgenden Bild der Paketerfassung dargestellt.




Wenn Sie diese Einstellung jedoch auf "optional" setzen, wird nur das Bit 7 gesetzt, wie im Bild gezeigt.




**Hinweis**: Der WLC fügt diese modifizierte RSN IE den Zuordnungs-/Neuzuordnungs-Antworten hinzu, und der AP fügt diese modifizierte RSN IE den Beacons und den Test-Antworten hinzu.

### Vorteile des 802.11w Management Frame Protection

- Client-Schutz

Dies wird durch die Hinzufügung von kryptographischem Schutz zu Deauthentifizierungs- und Dissoziationsframes erreicht. Auf diese Weise wird verhindert, dass ein nicht autorisierter Benutzer einen Denial of Service (DOS)-Angriff starten kann, indem er die MAC-Adresse legitimer Benutzer manipuliert und die Frames zur Deaktivierung/Aufhebung der Zuordnung sendet.

- AP-Schutz

Der infrastrukturseitige Schutz wird durch einen Abbruchschutz der Security Association (SA) ergänzt, der aus einer Association Comeback Time und einer SA-Query-Prozedur besteht. Wenn ein WAP vor 802.11w entweder eine Assoziations- oder eine Authentifizierungsanforderung von einem bereits verknüpften Client empfangen hat, beendet er die aktuelle Verbindung und startet dann eine neue Verbindung. Wenn Sie 802.11w MFP verwenden und der STA zugeordnet ist und über einen Management Frame Protection verhandelt hat, lehnt der AP die Zuordnungsanfrage mit dem Rückgabestatuscode 30 ab. Association request rejected temporarily; Try again later an den Client gesendet.

In der Antwort auf die Zuordnung ist ein Informationselement für die Comeback-Zeit der Zuordnung enthalten, das eine Comeback-Zeit angibt, zu der der WAP bereit ist, eine Zuordnung zu diesem STA zu akzeptieren. Auf diese Weise können Sie sicherstellen, dass legitime Clients nicht aufgrund einer gefälschten Zuordnungsanforderung getrennt werden.

---

> **Hinweis**: Der WLC (AireOS oder 9800) ignoriert die Trennung bzw. Aufhebung der Authentifizierung von Frames, die von den Clients gesendet werden, wenn diese keine 802.11w-PMF verwenden. Der Client-Eintrag wird beim Empfang eines solchen Frames erst dann gelöscht, wenn der Client PMF verwendet. Auf diese Weise soll ein Denial of Service durch bösartige Geräte vermieden werden, da diese Frames ohne PMF keine Sicherheit bieten.

---

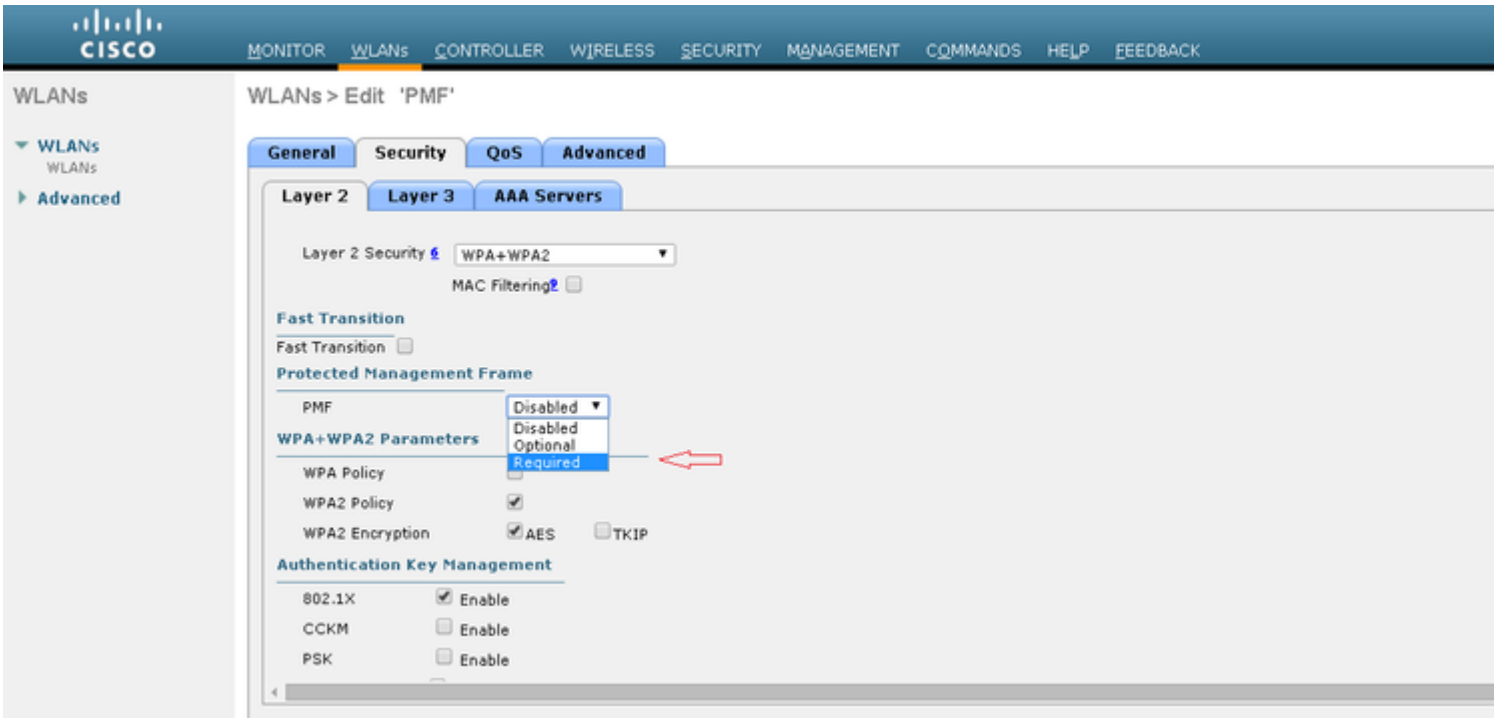
### Voraussetzungen für 802.11w

- Für 802.11w muss die SSID mit dot1x oder PSK konfiguriert werden.
- 802.11w wird von allen 802.11n-fähigen Zugangspunkten unterstützt. Das bedeutet, dass AP 1130 und 1240 802.11w nicht unterstützen.
- In Version 7.4 wird 802.11w auf Flexconnect AP und 7510 WLC nicht unterstützt. Unterstützung wurde seit Version 7.5 hinzugefügt.

## Konfigurieren

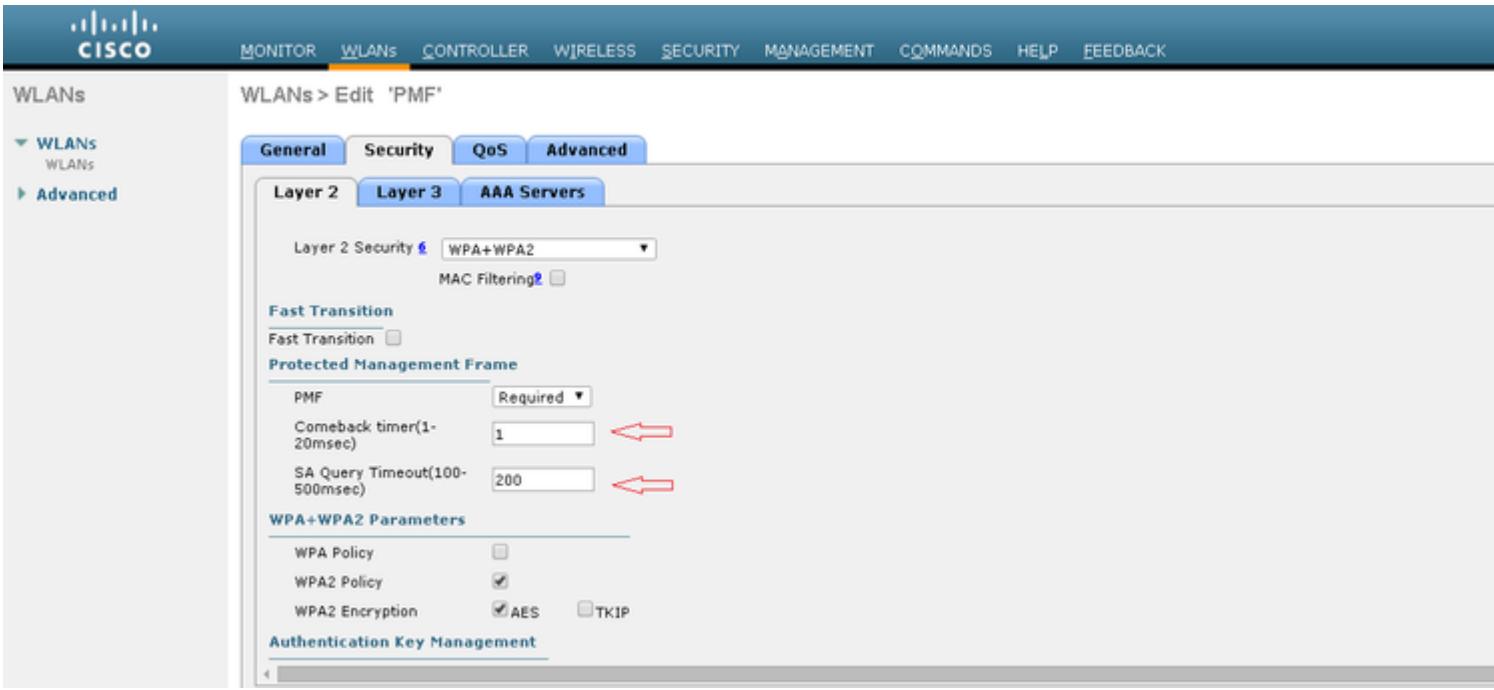
### GUI

Schritt 1: Sie müssen den geschützten Management-Frame unter der mit 802.1x/PSK konfigurierten SSID aktivieren. Sie haben drei Optionen, wie im Bild dargestellt.

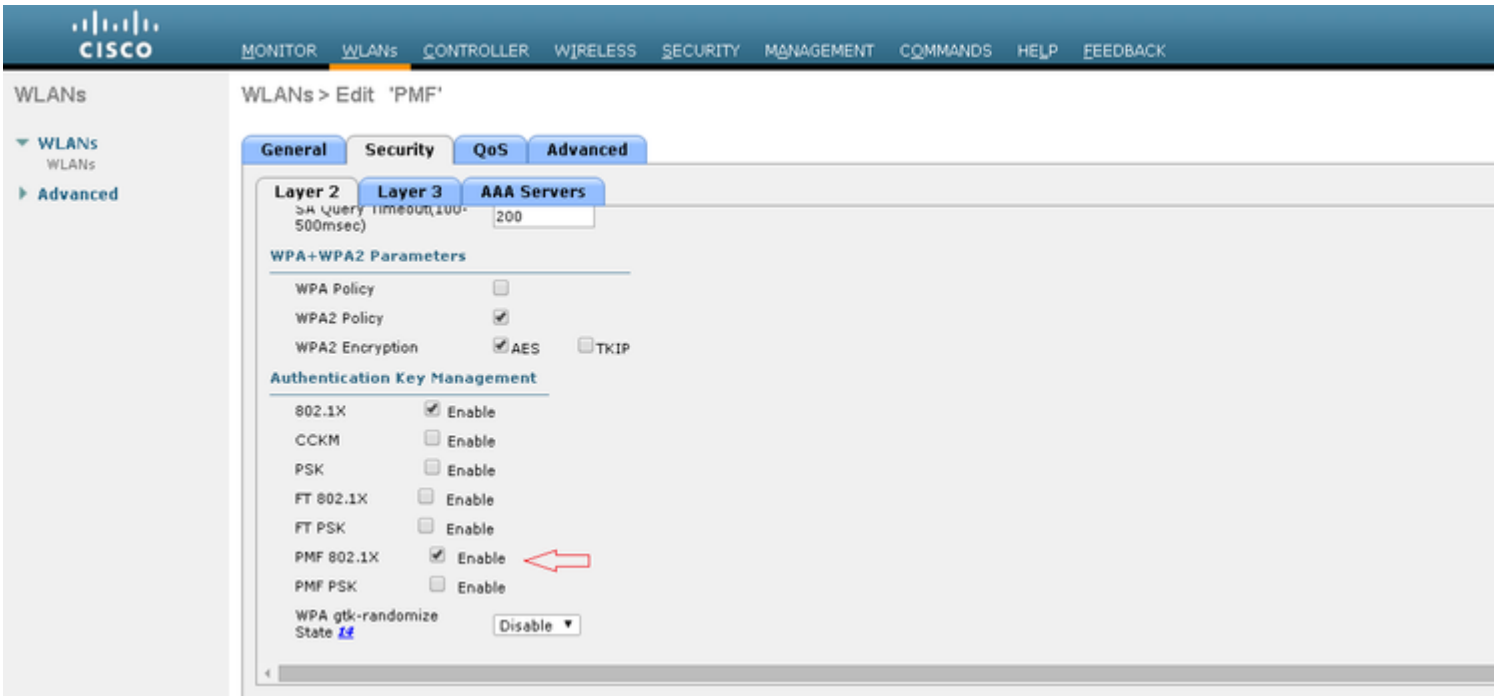



'Erforderlich' gibt an, dass ein Client, der 802.11w nicht unterstützt, keine Verbindung herstellen darf. 'Optional' gibt an, dass selbst Clients, die 802.11w nicht unterstützen, eine Verbindung herstellen dürfen.

Schritt 2: Anschließend müssen Sie den Comeback-Timer und den SA-Abfragetimeout angeben. Der Comeback-Timer gibt die Zeit an, die ein verbundener Client warten muss, bevor die Zuordnung erneut versucht werden kann, wenn er zum ersten Mal mit einem Statuscode 30 abgelehnt wird. Der SA-Abfragetimeout gibt an, wie lange der WLC auf eine Antwort des Clients für den Abfrageprozess wartet. Wenn der Client nicht antwortet, wird seine Zuordnung vom Controller gelöscht. Dies geschieht wie im Bild gezeigt.




Schritt 3: Sie müssen 'PMF 802.1x' aktivieren, wenn Sie 802.1x als Methode zur Verwaltung von Authentifizierungsschlüsseln verwenden. Wenn Sie PSK verwenden, müssen Sie das Kontrollkästchen **PMF PSK** aktivieren, wie im Bild gezeigt.




### CLI

- Führen Sie den folgenden Befehl aus, um die 11w-Funktion zu aktivieren oder zu deaktivieren:

config wlan security wpa akm pmf 802.1x enable/disable

config wlan security wpa akm pmf psk enable/disable

- Führen Sie den folgenden Befehl aus, um geschützte Management-Frames zu aktivieren oder zu deaktivieren:

config wlan security pmf optional/required/disable

- Zeiteinstellungen für das Comeback der Zuordnung:

config wlan security pmf 11w-association-comeback

- Timeout-Einstellungen für SA-Abfragewiederholung:

config wlan security pmf saquery-retry-time

## Überprüfung

Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Die 802.11w-Konfiguration kann überprüft werden. Überprüfen Sie die WLAN-Konfiguration:

```
(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
```

# Fehlerbehebung

In diesem Abschnitt erhalten Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

Die folgenden Debug-Befehle sind zur Behebung von 802.11w-Problemen auf dem WLC verfügbar:

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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.