

Configure 802.11w Management Frame Protection on WLC

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Management MIC Information Element \(MMIE\)](#)

[Changes to RSN IE](#)

[Benefits of 802.11w Management Frame Protection](#)

[Requirements to Enable 802.11w](#)

[Configure](#)

[GUI](#)

[CLI](#)

[Verify](#)

[Troubleshoot](#)

Introduction

This document describes details about IEEE 802.11w management frame protection and its configuration on the Cisco Wireless LAN Controller (WLC).

Prerequisites

Requirements

Cisco recommends that you have knowledge of Cisco WLC that runs code 7.6 or later.

Components Used

The information in this document is based on WLC 5508 which runs code 7.6.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

The 802.11w standard aims to protect control and management frames and a set of robust management frames against forgery and replay attacks. The frame types protected include Disassociation, Deauthentication, and Robust Action frames such as:

- Spectrum management
- Quality of Service (QoS)
- Block Ack
- Radio measurement
- Fast Basic Service Set (BSS) Transition

802.11w does not encrypt the frames, however, it protects the management frames. It ensures that the messages come from legitimate sources. In order to do that, you have to add a Message Integrity Check (MIC) element. 802.11w has introduced a new key called Integrity Group Temporal Key (IGTK), which is used to protect broadcast/multicast robust management frames. This is derived as part of the four-way key handshake process used with Wireless Protected Access (WPA). This makes dot1x/Pre-Shared Key (PSK) a requirement when you need to use 802.11w. It cannot be used with open/webauth Service Set Identifier (SSID).


When Management Frame Protection is negotiated, the Access Point (AP) encrypts the GTK and IGTK values in the EAPOL-Key frame which is delivered in Message 3 of the 4-way handshake. If the AP later changes the GTK, it sends the new GTK and IGTK to the client with the use of the Group Key Handshake. It adds a MIC that is calculated with the use of the IGTK key.

Management MIC Information Element (MMIE)

802.11w introduces a new information element called the Management MIC information element. It has the header format as shown in the image.

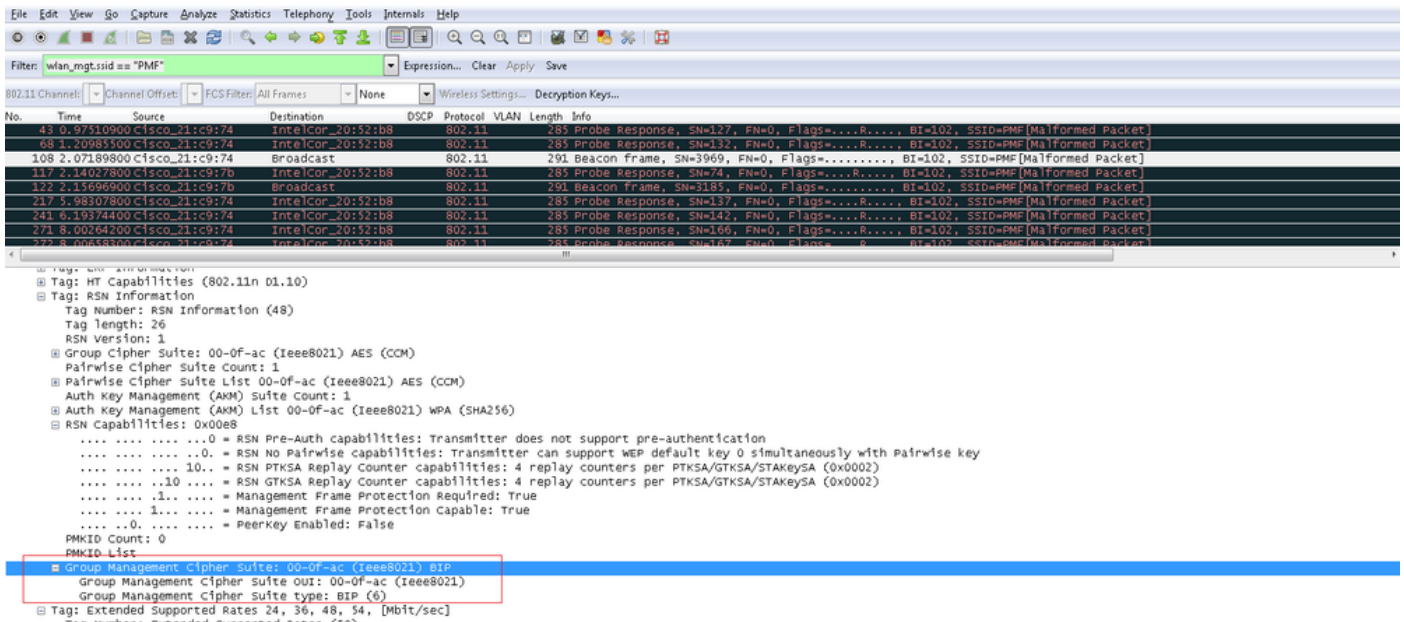
1	1	2	6	8
Element ID	Length	KeyID	IPN	MIC

The main fields of concern here are **element ID** and **MIC**. The element ID for MMIE is `0x4c` and it serves as a useful identification when you analyze the wireless captures.

 **Note:** MIC - It contains the message integrity code calculated over the Management frame. It is important to note that this is added at the AP. The destination client then re-computes the MIC for the frame and compares it with what was sent by the AP. If the values are different, this is rejected as an invalid frame.

Changes to RSN IE

Robust Security Network Information Element (RSN IE) specifies the security parameters supported by the AP. The 802.11w introduces a Group Management Cipher suite selector to RSN IE that contains the cipher suite selector used by the AP to protect broadcast/multicast robust management frames. This is the best way to know if an AP does 802.11w or not. This can also be verified as shown in the image.

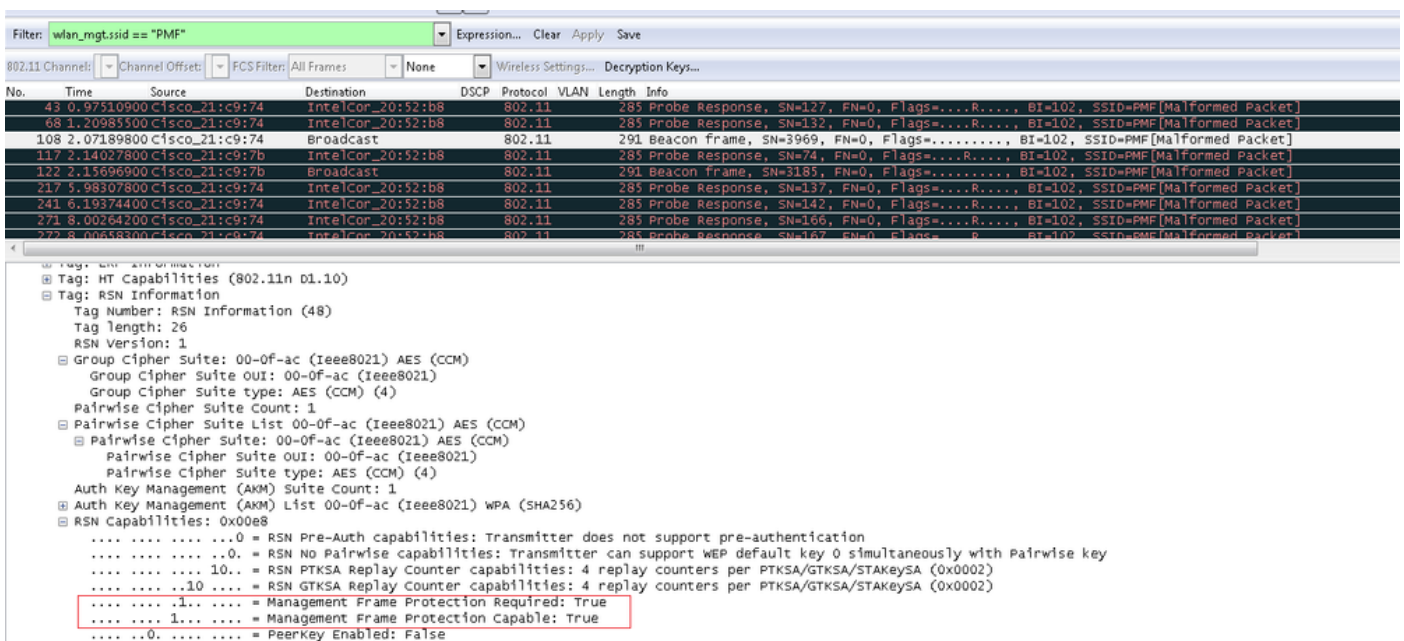


Here, you find the **group management cipher suite** field which shows that 802.11w is used.

There were changes also made under RSN capabilities. Bits 6 and 7 are now used to indicate different parameters for 802.11w.

- Bit 6: Management Frame Protection Required (MFPR) - A STA sets this bit to 1 to advertise that the protection of Robust Management Frames is mandatory.
- Bit 7: Management Frame Protection Capable (MFPC) - A STA sets this bit to 1 to advertise that protection of Robust Management Frames is enabled. When the AP sets this, it informs that it supports management frame protection.

If you set management frame protection as required under the configuration options then both bits 6 and 7 are set. This is as shown in the packet capture image here.



However, if you set this to optional then only bit 7 is set, as shown in the image.

```

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
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
35 2.00590100 Cisco_21:c9:7b IntelCOR_20:52:b8 802.11 279 Probe Response, SN=459, FN=0, Flags=.....R..... BI=102, SSID=PMF [Malformed Packet]
36 2.00630400 Cisco_21:c9:7b broadcast 802.11 285 Beacon Frame, SN=2306, FN=0, Flags=..... BI=102, SSID=PMF [Malformed Packet]
130 5.47209300 Cisco_21:c9:74 broadcast 802.11 285 Beacon Frame, SN=257, FN=0, Flags=..... BI=102, SSID=PMF [Malformed Packet]
134 5.48216900 Cisco_21:c9:74 IntelCOR_20:52:b8 802.11 279 Probe Response, SN=897, FN=0, Flags=...R..... BI=102, SSID=PMF [Malformed Packet]
161 5.89994000 Cisco_21:c9:74 broadcast 802.11 285 Beacon Frame, SN=277, FN=0, Flags=..... BI=102, SSID=PMF [Malformed Packet]
186 6.51628200 Cisco_21:c9:74 broadcast 802.11 285 Beacon Frame, SN=306, FN=0, Flags=..... BI=102, SSID=PMF [Malformed Packet]
...
Tag: Country Information: Country Code: US, Environment: Any
Tag: QSSS Load Element 802.11e CCA Version
Tag: HT Capabilities (802.11n D1.10)
Tag: RSN Information
Tag Number: RSN Information (48)
Tag Length: 20
RSN Versions: 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
RSN Capabilities: 0x00a8
... ..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)
... ..0... = Management Frame Protection Required: False
... ..1... = Management Frame Protection Capable: True
... ..0... = Peerkey Enabled: False
Tag: HT Information (802.11n D1.10)
Tag: Cisco CCK1 CKIP + Device Name

```

Note: The WLC adds this modified RSN IE in association/re-association responses and the AP adds this modified RSN IE in beacons and probe responses.

Benefits of 802.11w Management Frame Protection

- Client Protection

This is achieved by the addition of cryptographic protection to Deauthentication and Disassociation frames. This prevents an unauthorized user to launch a Denial of Service (DOS) attack by spoofing the MAC address of legitimate users and send the death/disassociation frames.

- AP Protection

Infrastructure side protection is added by the addition of a Security Association (SA) teardown protection mechanism which consists of an Association Comeback Time and an SA-Query procedure. Prior to 802.11w, if an AP received either an Association or Authentication request from an already associated client, the AP terminates the current connection and then starts a new connection. When you use 802.11w MFP, if the STA is associated and has negotiated Management Frame Protection, the AP rejects the Association Request with return status code 30 Association request rejected temporarily; Try again later to the client.

Included in the Association Response is an Association Comeback Time information element which specifies a comeback time when the AP is ready to accept an association with this STA. This way you can ensure that legitimate clients are not disassociated due to a spoofed association request.

Note: The WLC (AireOS or 9800) ignores disassociation or de-authentication frames sent by the clients if they do not use 802.11w PMF. The client entry only gets deleted immediately upon reception of such a frame if the client uses PMF. This is to avoid denial of service by malicious devices since there is no security on those frames without PMF.

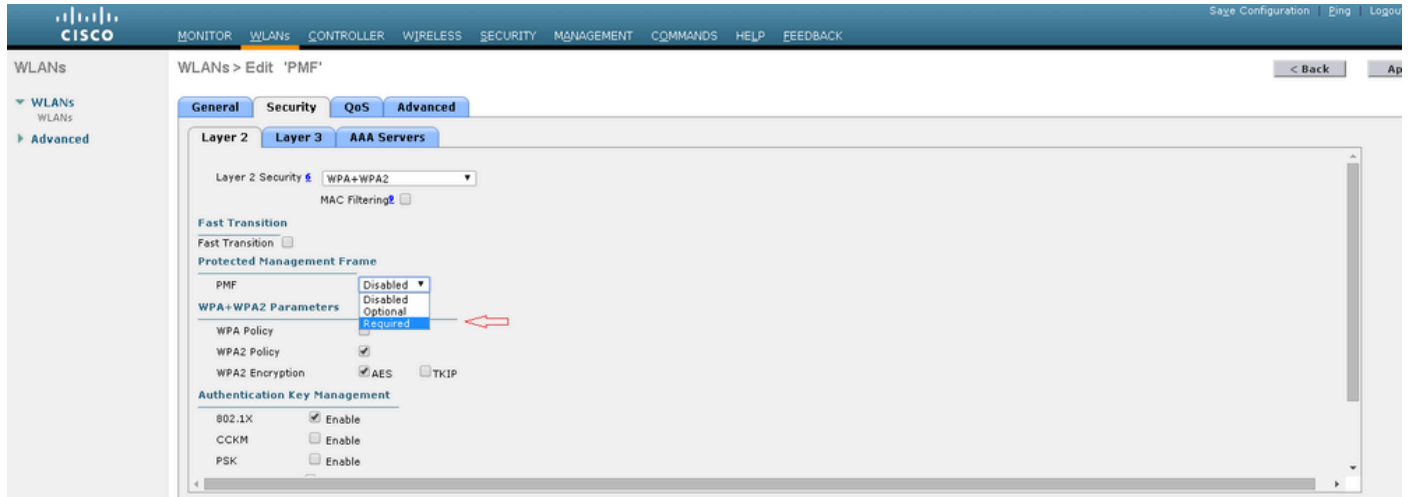
Requirements to Enable 802.11w

- 802.11w requires the SSID to be configured with either dot1x or PSK.
- 802.11w is supported on all 802.11n capable AP. This means that AP 1130 and 1240 do not support 802.11w.
- 802.11w is not supported on Flexconnect AP and 7510 WLC in the 7.4 release. Support has been added since the 7.5 release.

Configure

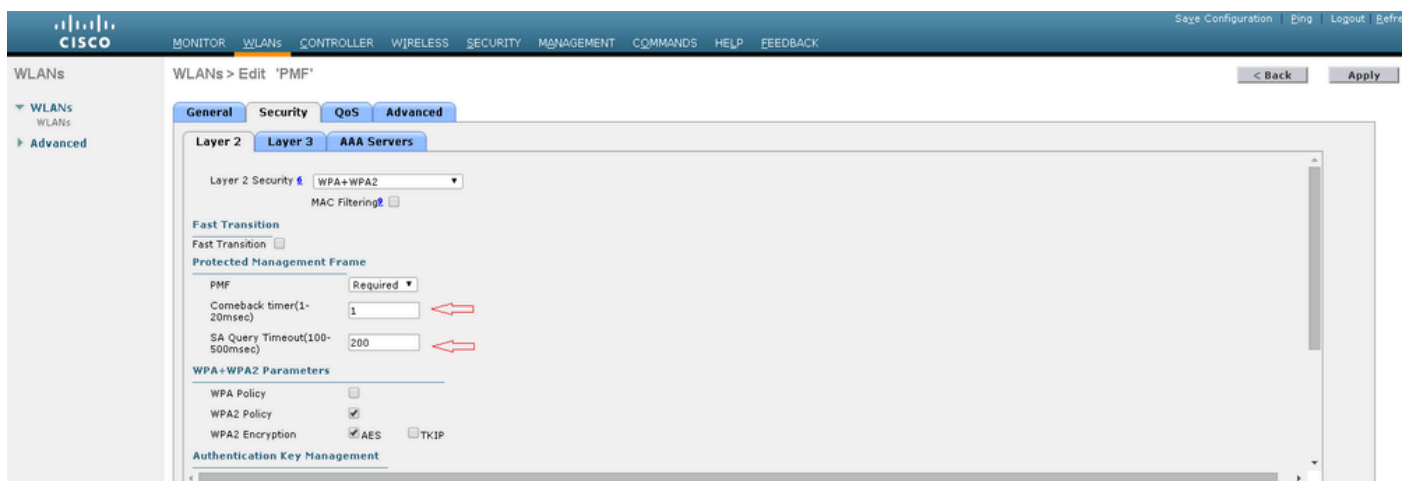
GUI

Step 1. You need to enable the protected management frame under the SSID configured with 802.1x/PSK. You have three options as shown in the image.

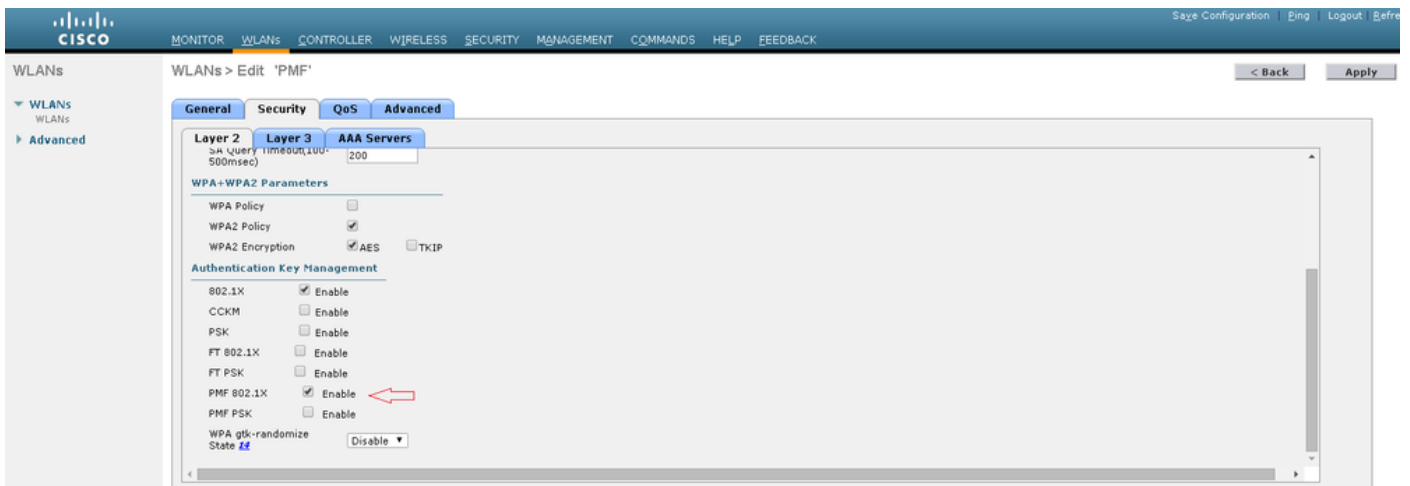


'Required' specifies that a client who does not support 802.11w is not allowed to connect. 'Optional' specifies that even clients that do not support 802.11w are allowed to connect.

Step 2. You then need to specify the comeback timer and SA query timeout. The comeback timer specifies the time that an associated client must wait before the association can be tried again when first denied with a status code 30. SA query timeout specifies the amount of time the WLC waits for a response from the client for the query process. If there is no response from the client, its association is deleted from the controller. This is done as shown in the image.



Step 3. You must enable 'PMF 802.1x' if you use 802.1x as the authentication key management method. In case you use PSK, you must choose the **PMF PSK** checkbox as shown in the image.



CLI

- In order to enable or disable the 11w feature, run the command:

```
config wlan security wpa akm pmf 802.1x enable/disable <wlan-id> config wlan security wpa akm pmf psk enable/disable <wlan-id>
```

- In order to enable or disable Protected Management Frames, run the command:

```
config wlan security pmf optional/required/disable <wlan-id>
```

- Association Comeback Time Settings:

```
config wlan security pmf 11w-association-comeback <time> <wlan-id>
```

- SA Query Retry TimeOut Settings:

```
config wlan security pmf saquery-retry-time <time> <wlan-id>
```

Verify

Use this section in order to confirm that your configuration works properly.

The 802.11w configuration can be verified. Check the WLAN configuration:

```
(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

Troubleshoot

This section provides the information you can use in order to troubleshoot your configuration.

These debug commands are available to troubleshoot 802.11w issues on the WLC:

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