

Configuration de la protection de trame de gestion 802.11w sur WLC

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

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

[Modifications apportées à RSN IE](#)

[Avantages de la protection de trame de gestion 802.11w](#)

[Configuration requise pour activer la norme 802.11w](#)

[Configurer](#)

[IUG](#)

[CLI](#)

[Vérifier](#)

[Dépannage](#)

Introduction

Ce document décrit en détail la protection de la trame de gestion IEEE 802.11w et sa configuration sur le contrôleur LAN sans fil Cisco (WLC).

Conditions préalables

Exigences

Cisco recommande que vous ayez connaissance de Cisco WLC qui exécute le code 7.6 ou ultérieur.

Composants utilisés

Les informations dans ce document sont basées sur le WLC 5508 qui exécute le 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

La norme 802.11w vise à protéger les trames de contrôle et de gestion ainsi qu'un ensemble de trames de gestion robustes contre la falsification et les attaques par relecture. Les types de trames protégés sont les trames Disassociation, Deauthentication et Robust Action, telles que :

- Gestion du spectre
- Qualité de service (QoS)
- Block Ack
- Mesure radio
- Transition vers Fast Basic Service Set (BSS)

La norme 802.11w ne chiffre pas les trames, mais protège les trames de gestion. Il garantit que les messages proviennent de sources légitimes. Pour ce faire, vous devez ajouter un élément de contrôle d'intégrité des messages (MIC). La norme 802.11w a introduit une nouvelle clé appelée IGTK (Integrity Group Temporal Key), qui est utilisée pour protéger les trames de gestion robustes de diffusion/multidiffusion. Ceci est dérivé dans le cadre du processus d'échange de clés en quatre étapes utilisé avec Wireless Protected Access (WPA). Cela rend dot1x/Pre-Shared Key (PSK) obligatoire lorsque vous devez utiliser la norme 802.11w. Il ne peut pas être utilisé avec un SSID (Service Set Identifier) ouvert/webauth.


Lors de la négociation de la protection de trame de gestion, le point d'accès (AP) chiffre les valeurs GTK et IGTK dans la trame EAPOL-Key qui est livrée dans le message 3 de la connexion en 4 étapes. Si le point d'accès modifie ultérieurement le GTK, il envoie le nouveau GTK et le nouveau IGTK au client à l'aide de la connexion de clé de groupe. Il ajoute un MIC qui est calculé avec l'utilisation de la clé IGTK.

Management MIC Information Element (MMIE)

La norme 802.11w introduit un nouvel élément d'information appelé élément d'information MIC de gestion. Il a le format d'en-tête tel qu'illustré dans l'image.

1	1	2	6	8
Element ID	Length	KeyID	IPN	MIC

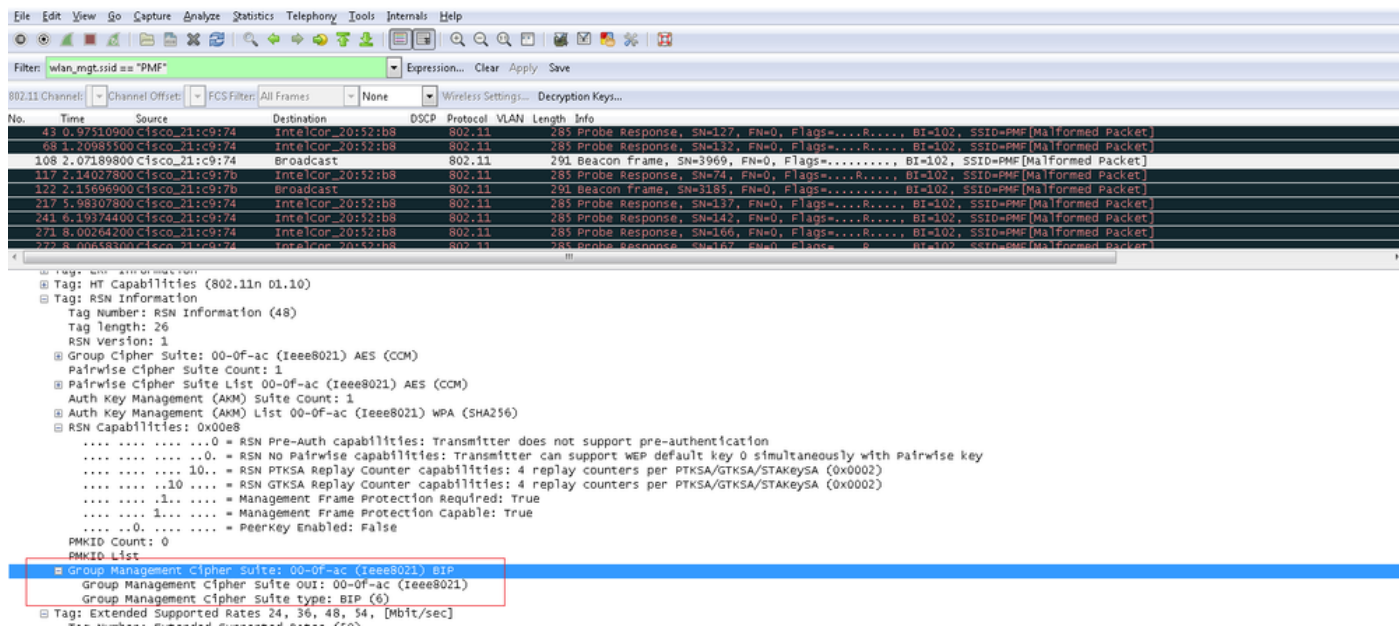
Les principaux domaines de préoccupation sont l'ID d'élément et la MIC. L'ID d'élément pour MMIE est `0x4c` et il sert d'identification utile lorsque vous analysez les captures sans fil.

 Remarque : MIC - contient le code d'intégrité du message calculé sur la trame de gestion. Il est important de noter que ceci est ajouté au point d'accès. Le client de destination recalcule ensuite le MIC de la trame et le compare à ce qui a été envoyé par le point d'accès. Si les valeurs sont différentes, cette trame est rejetée comme étant non valide.

Modifications apportées à RSN IE

Robuste Security Network Information Element (RSN IE) spécifie les paramètres de sécurité pris en charge par le point d'accès. La norme 802.11w introduit un sélecteur de suite de chiffrement de

gestion de groupe dans RSN IE qui contient le sélecteur de suite de chiffrement utilisé par le point d'accès pour protéger les trames de gestion robustes de diffusion/multidiffusion. C'est la meilleure façon de savoir si un AP fait 802.11w ou non. Cela peut également être vérifié comme illustré dans l'image.



Ici, vous trouvez le champ group management cipher suite qui montre que 802.11w est utilisé.

Des modifications ont également été apportées aux capacités RSN. Les bits 6 et 7 sont maintenant utilisés pour indiquer différents paramètres pour 802.11w.

- Bit 6 : Management Frame Protection Required (MFPR) - Un STA définit ce bit sur 1 pour annoncer que la protection des trames de gestion robustes est obligatoire.
- Bit 7 : Management Frame Protection Capable (MFPC) - Un STA définit ce bit sur 1 pour annoncer que la protection des trames de gestion robustes est activée. Lorsque le point d'accès définit cela, il informe qu'il prend en charge la protection de trame de gestion.

Si vous définissez la protection de la trame de gestion comme requis dans les options de configuration, les bits 6 et 7 sont définis. Ceci est illustré dans l'image de capture de paquets ici.

Filter: wlan_mgmt.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	283	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	283	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	2.14102700	Cisco_21:c9:7b	IntelCor_20:52:b8	802.11	283	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=3183, FN=0, Flags=....., BI=102, SSID=PMF [Malformed Packet]		
217	5.98307800	Cisco_21:c9:74	IntelCor_20:52:b8	802.11	283	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	283	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	283	Probe Response, SN=166, FN=0, Flags=...R..., BI=102, SSID=PMF [Malformed Packet]		
322	8.00659300	Cisco_21:c9:74	IntelCor_20:52:b8	802.11	283	Probe Response, SN=137, 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
    ....0.0 = 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
  
```

Cependant, si vous définissez cette option sur facultatif, seul le bit 7 est défini, comme illustré dans l'image.

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help


Filter: wlan_mgmt.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	3.00590100	Cisco_21:c9:7b	IntelCor_20:52:b8	802.11	285	Probe Response, SN=159, 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	3.47209300	Cisco_21:c9:74	Broadcast	802.11	285	Beacon frame, SN=217, 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 Int)
Tag: QoS 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 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
  RSN Capabilities: 0x00a8
    ....0 = RSN Pre-Auth capabilities: Transmitter does not support pre-authentication
    ....0.0 = 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
  
```

 Remarque : le WLC ajoute cet élément d'information RSN modifié dans les réponses d'association/de réassociation et l'AP ajoute cet élément d'information RSN modifié dans les balises et les réponses de sonde.

Avantages de la protection de trame de gestion 802.11w


- Protection du client

Pour ce faire, une protection cryptographique est ajoutée aux trames de désauthentification et de dissociation. Cela empêche un utilisateur non autorisé de lancer une attaque Denial of Service (DOS) en usurpant l'adresse MAC d'utilisateurs légitimes et en envoyant les trames d'authentification/désassociation.

- Protection AP

La protection côté infrastructure est ajoutée par l'ajout d'un mécanisme de protection de démontage de l'association de sécurité (SA) qui consiste en un temps de retour d'association et une procédure de requête SA. Avant la norme 802.11w, si un point d'accès recevait une demande d'association ou d'authentification d'un client déjà associé, le point d'accès met fin à la connexion actuelle, puis démarre une nouvelle connexion. Lorsque vous utilisez le MFP 802.11w, si le STA est associé et a négocié la protection de trame de gestion, le point d'accès rejette la demande d'association avec le code d'état de retour 30 Association request rejected temporarily; Try again later au client.

La réponse d'association inclut un élément d'information de temps de retour d'association qui spécifie un temps de retour quand le point d'accès est prêt à accepter une association avec ce STA. Vous pouvez ainsi vous assurer que les clients légitimes ne sont pas dissociés en raison d'une demande d'association usurpée.

 Remarque : le WLC (AireOS ou 9800) ignore les trames de désassociation ou de désauthentification envoyées par les clients s'ils n'utilisent pas le protocole 802.11w PMF. L'entrée client n'est supprimée immédiatement à la réception d'une telle trame que si le client utilise PMF. Cela permet d'éviter le déni de service par des périphériques malveillants, car il n'y a pas de sécurité sur ces trames sans PMF.

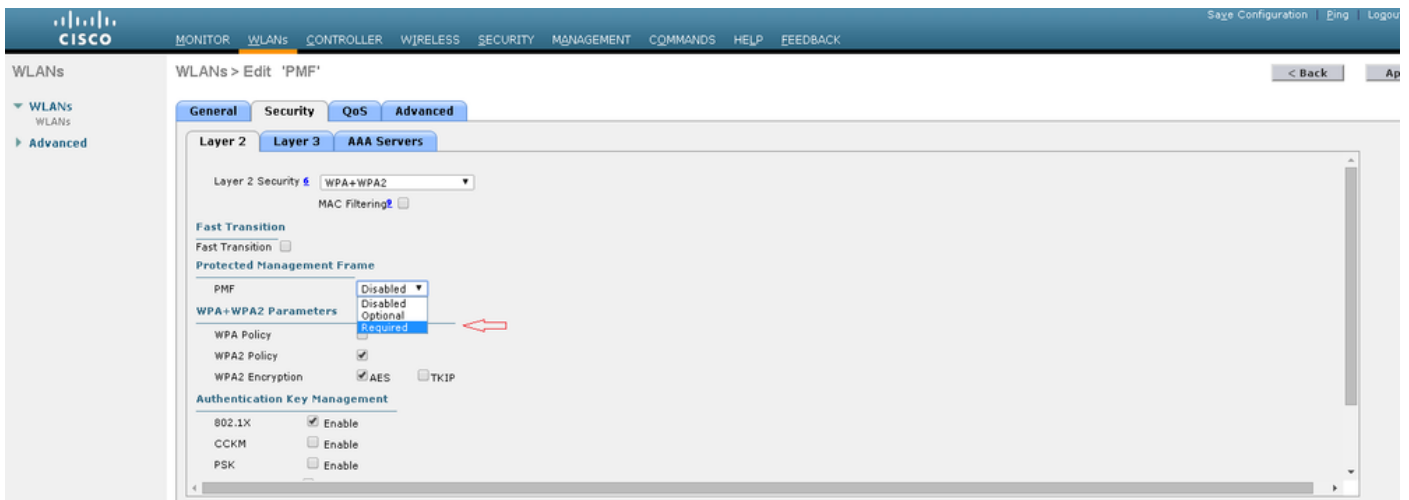
Configuration requise pour activer la norme 802.11w

- 802.11w nécessite que le SSID soit configuré avec dot1x ou PSK.
- 802.11w est pris en charge sur tous les points d'accès compatibles 802.11n. Cela signifie que les points d'accès 1130 et 1240 ne prennent pas en charge la norme 802.11w.
- 802.11w n'est pas pris en charge sur le point d'accès flexconnect et le WLC 7510 dans la version 7.4. La prise en charge a été ajoutée depuis la version 7.5.

Configurer

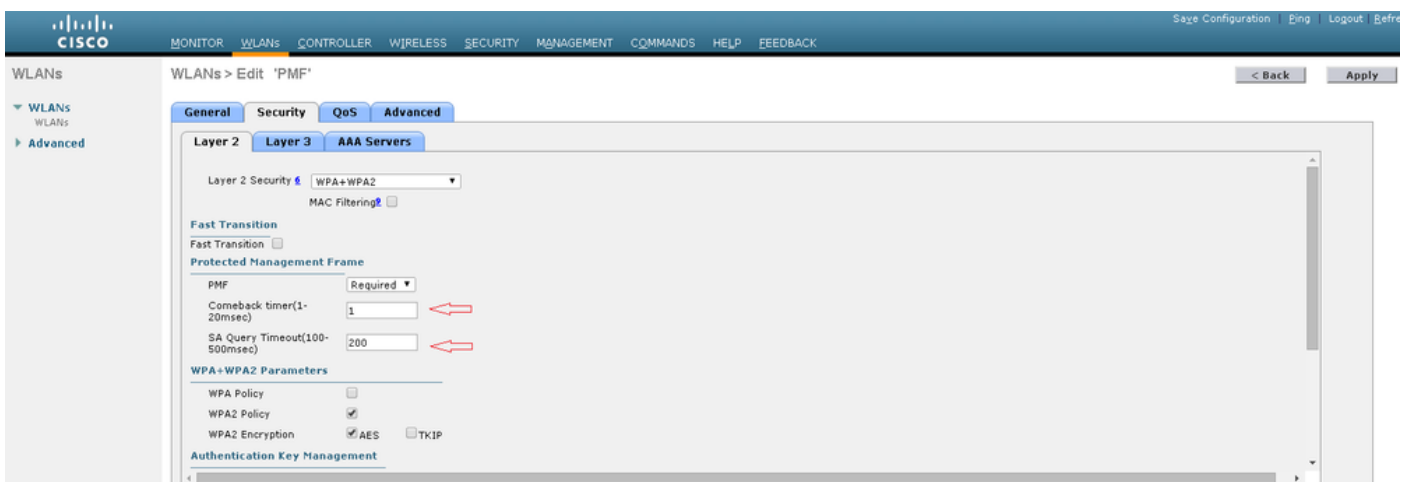
IUG

Étape 1. Vous devez activer la trame de gestion protégée sous le SSID configuré avec 802.1x/PSK. Vous disposez de trois options, comme illustré dans l'image.

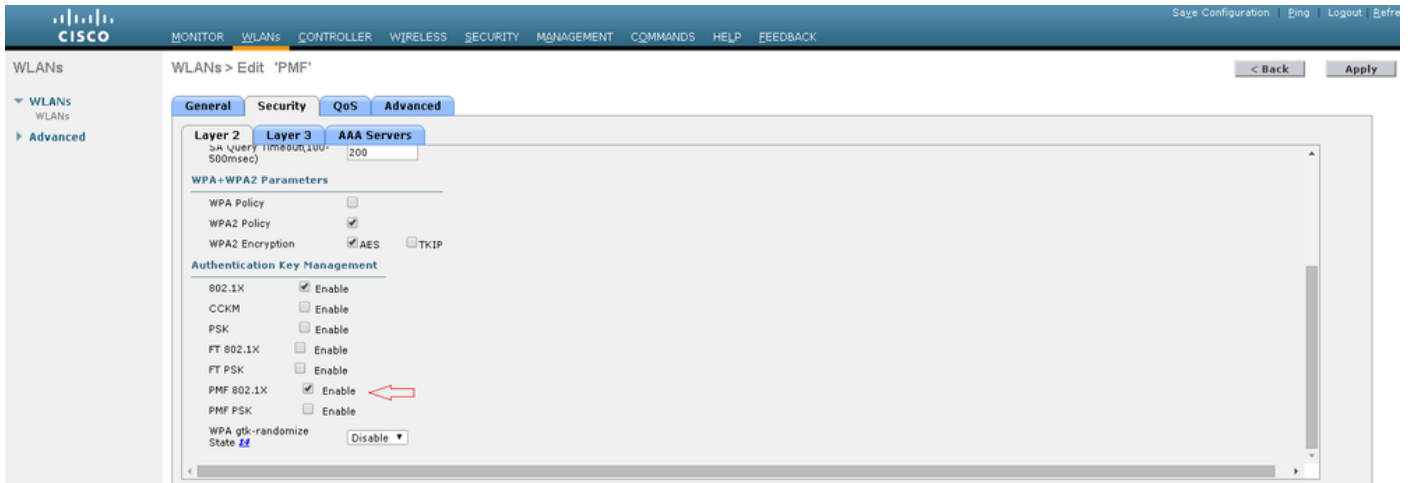


'Obligatoire' spécifie qu'un client qui ne prend pas en charge 802.11w n'est pas autorisé à se connecter. 'Optional' spécifie que même les clients qui ne prennent pas en charge 802.11w sont autorisés à se connecter.

Étape 2. Vous devez ensuite spécifier le délai de retour et le délai de requête SA. Le compteur de retour spécifie le temps qu'un client associé doit attendre avant que l'association puisse être tentée à nouveau lorsqu'elle est refusée pour la première fois avec un code d'état 30. SA query timeout spécifie la durée pendant laquelle le WLC attend une réponse du client pour le processus de requête. En l'absence de réponse du client, son association est supprimée du contrôleur. Cette opération est effectuée comme indiqué dans l'image.



Étape 3. Vous devez activer « PMF 802.1x » si vous utilisez 802.1x comme méthode de gestion des clés d'authentification. Si vous utilisez PSK, vous devez sélectionner la case à cocher PMF PSK comme indiqué dans l'image.



CLI

- Afin d'activer ou de désactiver la fonctionnalité 11w, exécutez la commande :

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

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

- Afin d'activer ou de désactiver les cadres de gestion protégés, exécutez la commande :

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

- Paramètres d'heure de retour d'association :

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

- Paramètres du délai d'attente des tentatives de requête SA :

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

Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

La configuration 802.11w peut être vérifiée. Vérifiez la configuration WLAN :

```
(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
```

Dépannage

Cette section fournit les informations que vous pouvez utiliser afin de dépanner votre configuration.

Ces commandes debug sont disponibles pour dépanner les problèmes 802.11w sur le WLC :

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

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.