Migration vers 6 GHz et Wi-Fi 7 avec Cisco Wireless

Table des matières

Introduction

Ce document décrit les directives de conception et de configuration pour optimiser les performances du Wi-Fi 7 et exploiter pleinement le spectre 6 GHz.

Guide de conception CX

Les guides de conception CX sont rédigés par des spécialistes de Cisco CX, en collaboration avec des ingénieurs d'autres départements, et examinés par des experts au sein de Cisco ; ces guides s'appuient sur les meilleures pratiques de Cisco ainsi que sur les connaissances et l'expérience acquises lors de nombreuses mises en oeuvre par les clients au fil des ans. Les réseaux conçus et configurés conformément aux recommandations de ce document permettent d'éviter les pièges courants et d'améliorer le fonctionnement du réseau.

Pourquoi 6 GHz et Wi-Fi 7

La bande 6 GHz est devenue disponible pour les opérations WLAN en 2020 et était requise pour la certification Wi-Fi 6E. Alors que le Wi-Fi 6 fonctionne dans les bandes 2,4 GHz et 5 GHz, le Wi-Fi 6E utilise la même norme IEEE 802.11ax mais étend sa fonctionnalité à la bande 6 GHz, à condition que des exigences spécifiques soient satisfaites.
La nouvelle certification Wi-Fi 7 est basée sur la norme IEEE 802.11be et prend en charge les opérations dans les bandes 2,4 GHz, 5 GHz et 6 GHz. Wi-Fi 7 introduit également de nouvelles fonctionnalités et améliorations par rapport aux certifications précédentes.

La prise en charge de la bande 6 GHz et/ou du Wi-Fi 7 s'accompagne d'exigences spécifiques, nécessitant souvent de nouvelles configurations et de nouvelles conceptions RF, notamment par rapport aux pratiques établies pour les bandes 2,4 GHz et 5 GHz avec le Wi-Fi 6.

Par exemple, tout comme l'utilisation d'une sécurité WEP obsolète empêche l'adoption de normes 802.11 au-delà de 802.11a/b/g, les nouvelles normes imposent des conditions de sécurité encore plus strictes pour encourager le déploiement de réseaux plus sécurisés.

À l'inverse, l'introduction de la bande 6 GHz offre un accès à des fréquences plus propres, de meilleures performances et la prise en charge de nouveaux cas d'utilisation. Elle permet également une mise en oeuvre plus transparente des applications existantes, telles que la conférence vocale et vidéo.

Configuration de base requise pour les opérations 6 GHz et le Wi-Fi 7

Il s'agit des exigences de sécurité inscrites dans les certifications pour les opérations 6 GHz et Wi-Fi 7.

Bande 6 GHz requise

La bande 6 GHz autorise uniquement les WPA3 ou WLAN ouverts améliorés, ce qui signifie l'une des options de sécurité suivantes :

- WPA3-Enterprise avec authentification 802.1X
- WPA3 Simultaneous Authentication of Equals (SAE) (également appelé WPA3-Personal) avec phrase de passe. SAE-FT (SAE avec transition rapide) est un autre AKM possible et est en fait recommandé pour une utilisation puisque la prise de contact SAE n'est pas triviale, et FT permet de sauter cet échange plus long.
- Enhanced Open avec cryptage sans fil opportuniste (OWE)

Bien que, conformément aux spécifications WPA3 v3.4 (Section 11.2), le mode de transition Enhanced Open n'est pas pris en charge avec 6 GHz, de nombreux fournisseurs (y compris Cisco jusqu'à IOS® XE 17.18) ne l'appliquent pas encore. Par conséquent, il est techniquement possible de configurer, par exemple, un SSID ouvert sur 5 GHz, un SSID ouvert amélioré correspondant sur 5 et 6 GHz, les deux avec le mode de transition activé, et tout cela sans respecter les spécifications des normes. Cependant, dans un tel scénario, il faut s'attendre à ce que nous configurions plutôt un SSID ouvert amélioré sans mode de transition et disponible sur 6 GHz seulement (les clients prenant en charge 6 GHz prennent généralement en charge également l'ouvert amélioré), tout en conservant notre SSID ouvert régulier sur 5 GHz, également sans mode de transition.

Il n'y a pas de nouvelles exigences spécifiques en matière de chiffrement ou d'algorithme pour WPA3-Enterprise, à l'exception de l'application 802.11w/PMF (Protected Management Frame). De nombreux fournisseurs, y compris Cisco, considèrent que la norme 802.1X-SHA256 ou « FT + 802.1X » (qui correspond en fait à la norme 802.1X avec SHA256 et Fast Transition au-dessus) est uniquement conforme à la norme WPA3 et que la norme 802.1X standard (qui utilise SHA1) est considérée comme faisant partie de la norme WPA2. Elle n'est donc pas adaptée/prise en charge pour la bande 6 GHz.

Wi-Fi 7 requis

Avec la certification Wi-Fi 7 de la norme 802.11be, la Wi-Fi Alliance a augmenté les exigences de sécurité. Certains d'entre eux permettent d'utiliser les débits de données 802.11be et d'améliorer les protocoles, tandis que d'autres sont spécifiques à la prise en charge des opérations multiliaison (MLO), permettant aux périphériques compatibles (clients et/ou points d'accès) d'utiliser plusieurs bandes de fréquences tout en conservant la même association.

En général, le Wi-Fi 7 impose l'un de ces types de sécurité :

- WPA3-Enterprise avec AES (CCMP128) et 802.1X-SHA256 ou FT + 802.1X (qui utilise toujours SHA256, même si son nom n'est pas explicite). Cela ne représente pas un changement par rapport aux conditions de sécurité WPA3 existantes pour la bande 6 GHz.
- WPA3 personnel avec GCMP256 et SAE-EXT-KEY et/ou FT + SAE-EXT-KEY (AKM 24 ou 25). Wi-Fi 6E exige WPA3 SAE et/ou FT + SAE avec AES standard (CCMP128) et aucune utilisation de clé étendue supplémentaire ; cela signifie qu'un nouveau chiffrement a été

spécifiquement introduit pour le Wi-Fi 7.
- Enhanced Open / OWE avec GCMP256. Bien qu'AES(CCMP128) puisse toujours être configuré sur le même SSID, les clients utilisant AES 128 ne prennent pas en charge Wi-Fi 7. Avant Wi-Fi 7, la plupart des clients prenant en charge Enhanced Open utilisaient uniquement AES 128, il s'agit donc d'une exigence nouvelle et plus forte. En ce qui concerne la prise en charge de la bande 6 GHz, aucun mode de transition n'est autorisé.

Quel que soit le type de sécurité sélectionné, les fonctions PMF (Protected Management Frames) et Beacon Protection sont requises pour prendre en charge le Wi-Fi 7 sur le WLAN.

Comme Wi-Fi 7 est encore une certification récente au moment de la rédaction de ce document, avec une version aussi précoce que possible, de nombreux fournisseurs n'ont pas appliqué toutes ces exigences de sécurité depuis le début.

Plus récemment, Cisco a progressivement mis en oeuvre les options de configuration pour être conforme à la certification Wi-Fi 7. Voici les comportements spécifiques à la version :

IOS XE 17.15.3 et versions ultérieures 17.15.x

Dans cette branche, tous les WLAN sont diffusés sous forme de SSID Wi-Fi 7, à condition que le Wi-Fi 7 soit activé globalement et quels que soient les paramètres de sécurité.

Un client peut s'associer en tant que Wi-Fi 7 et obtenir des débits de données Wi-Fi 7 quelle que soit la méthode de sécurité qu'il utilise, à condition qu'il soit toujours pris en charge par le WLAN. Cependant, le client ne peut s'associer en tant que MLO (sur une ou plusieurs bandes) que s'il respecte les exigences strictes de la sécurité Wi-Fi 7, ou s'il est rejeté.

Cela peut potentiellement poser des problèmes lorsque certains clients Wi-Fi 7 n'étant pas en mesure de prendre en charge des chiffrements plus sécurisés, comme GCMP256, tentent de s'associer en tant que Wi-Fi 7 MLO à un WLAN, dont les paramètres de sécurité ne correspondent pas aux exigences de Wi-Fi 7. Dans une telle situation, le client est rejeté en raison de paramètres de sécurité non valides (toujours autorisés à être configurés sous le WLAN).

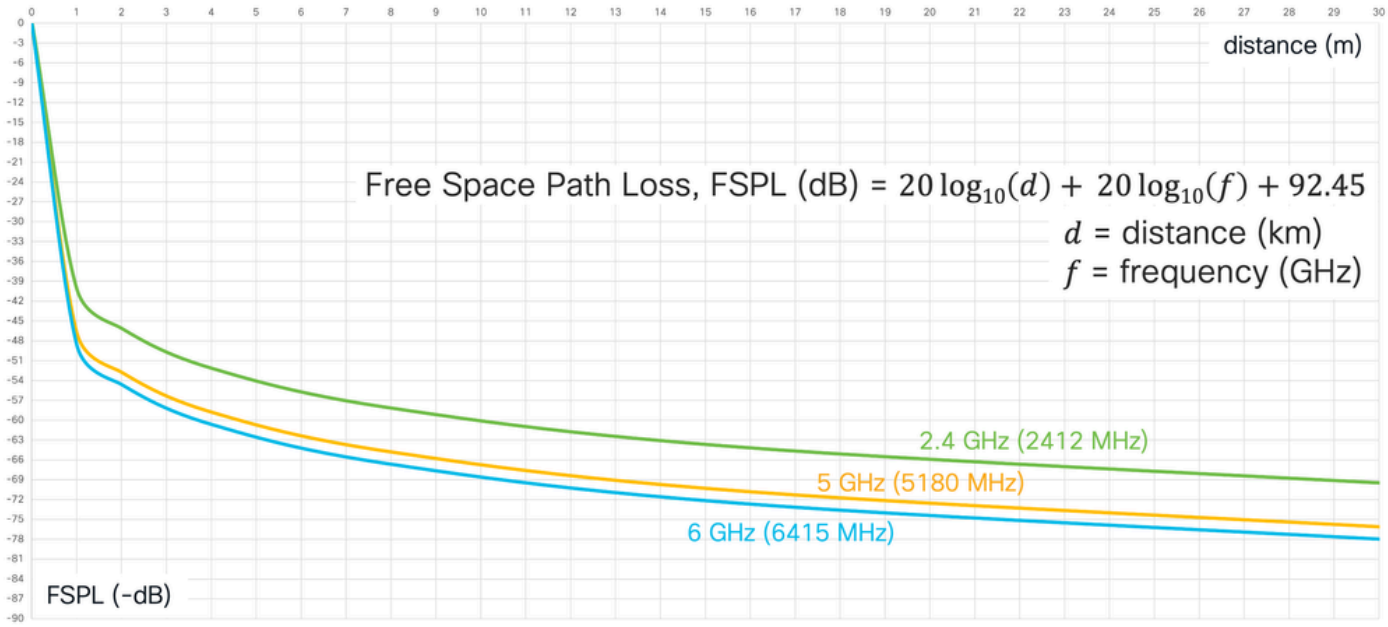
Considérations de conception radio pour une couverture 6 GHz

Sans vouloir devenir un guide normatif complet sur les études sur site, cette section décrit brièvement quelques considérations de base lors de la conception pour la couverture 6 GHz, en particulier s'il existe déjà une installation pour 2,4/5 GHz que nous souhaiterions migrer vers le Wi-Fi 6E ou 7.
Comme pour tout nouveau déploiement Wi-Fi auquel nous étions habitués sur 2,4 et/ou 5 GHz, un nouveau projet sans fil sur 6 GHz doit également inclure une étude de site dédiée correspondante sur 6 GHz.

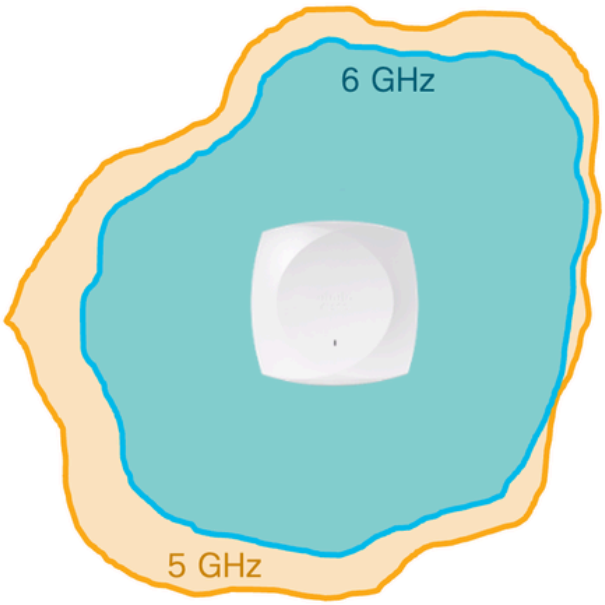
Lorsque les points d'accès pré-Wi-Fi 6E/7 sont déjà positionnés pour une couverture et des besoins spécifiques de 5 GHz, dans certains cas, nous pouvons nous attendre à pouvoir les remplacer par des points d'accès compatibles Wi-Fi 6E/7 et obtenir toujours une bonne couverture sur 6 GHz. Pour que cette théorie fonctionne, nos points d'accès existants doivent déjà fournir une

couverture 5 GHz correcte pour les besoins prévus (données uniquement, voix, applications spécifiques, etc.) tout en étant déjà au moins 3-4 niveaux de puissance de transmission sous leur limite maximale. Les points d'accès ont généralement de 7 à 8 niveaux de puissance, et chaque niveau de puissance divise la puissance de transmission par deux. Cela signifie qu'un endroit confortable à être est lorsque les AP utilisent le support de leur plage de puissance de transmission autorisée.

Selon les calculs de perte d'espace libre, les signaux de 6 GHz sont atténués de 2 dB de plus que les signaux de 5 GHz. En outre, les signaux 6 GHz peuvent également être plus affectés par les obstacles que leurs équivalents 5 GHz.



Lorsqu'un point d'accès Cisco augmente/diminue sa puissance de transmission d'un niveau, il le fait par un « saut » de 3 dB. Un point d'accès passant d'un niveau de puissance de 4, avec une puissance d'émission de 11 dBm par exemple, à un niveau de puissance de 3, augmente sa puissance d'émission à 14 dBm (11 dBm pour le niveau de puissance 4 et 14 dBm pour le niveau de puissance 3 ne sont qu'un exemple générique, car différents modèles/générations de points d'accès pourraient avoir des valeurs de puissance d'émission légèrement différentes en dBm pour le même numéro de niveau de puissance).



Assuming similar antenna gains/patterns and the same transmit power level, the 6 GHz radio is expected to cover slightly less than the 5 GHz radio.
The overall 6 GHz coverage throughout multiple APs could be more comparable, especially if those APs are already dense enough for good 5 GHz coverage.

Si un point d'accès Wi-Fi 6E/7 offre déjà une bonne couverture à 5 GHz sur le niveau de puissance 4, par exemple, un point d'accès Wi-Fi 6E/7 plus récent avec des modèles radio 5 GHz similaires pourrait remplacer cet ancien point d'accès sans impact significatif sur le réseau 5 GHz existant.

En outre, la radio 6 GHz du nouveau point d'accès Wi-Fi 6E/7 pourrait fournir une couverture 6 GHz similaire à celle de 5 GHz simplement en étant à un niveau de puissance de transmission (donc 3 dB) plus élevé.

Si la bande 5 GHz est déjà correctement couverte par la radio 5 GHz du point d'accès à des niveaux de puissance 3-4 sous son maximum, la radio 6 GHz correspondante pourrait donc être réglée à des niveaux de puissance 2-3 sous son maximum pour une couverture comparable.

En outre, si la radio 6 GHz fournit déjà une couverture correcte à des niveaux de puissance 2-3 inférieurs à son maximum, elle pourrait exceptionnellement aller même quelques niveaux plus élevés, par exemple pour essayer de contourner les trous de couverture temporaires inattendus (défaillance d'un point d'accès voisin, obstacles non annoncés, nouveaux besoins RF, etc.).

Comportements d'itinérance entre les points d'accès pré-Wi-Fi 6E/7 et Wi-Fi 6E/7

Le déploiement de points d'accès prenant en charge différentes normes et/ou bandes de fréquences dans la même zone de couverture n'a jamais été recommandé, en particulier si ces différentes générations de points d'accès sont installées de manière « salée et poivrée » (c'est-à-dire mélangées dans la même zone).

Bien qu'un contrôleur sans fil puisse gérer les opérations (par exemple, l'attribution dynamique de canaux, le contrôle de la puissance de transmission, la distribution de cache PMK, etc.) à partir d'un groupe de plusieurs modèles de points d'accès, les clients se déplaçant entre différentes normes et même entre différentes bandes de fréquences ne sont pas toujours en mesure de gérer cela correctement et ils pourraient rencontrer des problèmes d'itinérance, par exemple.

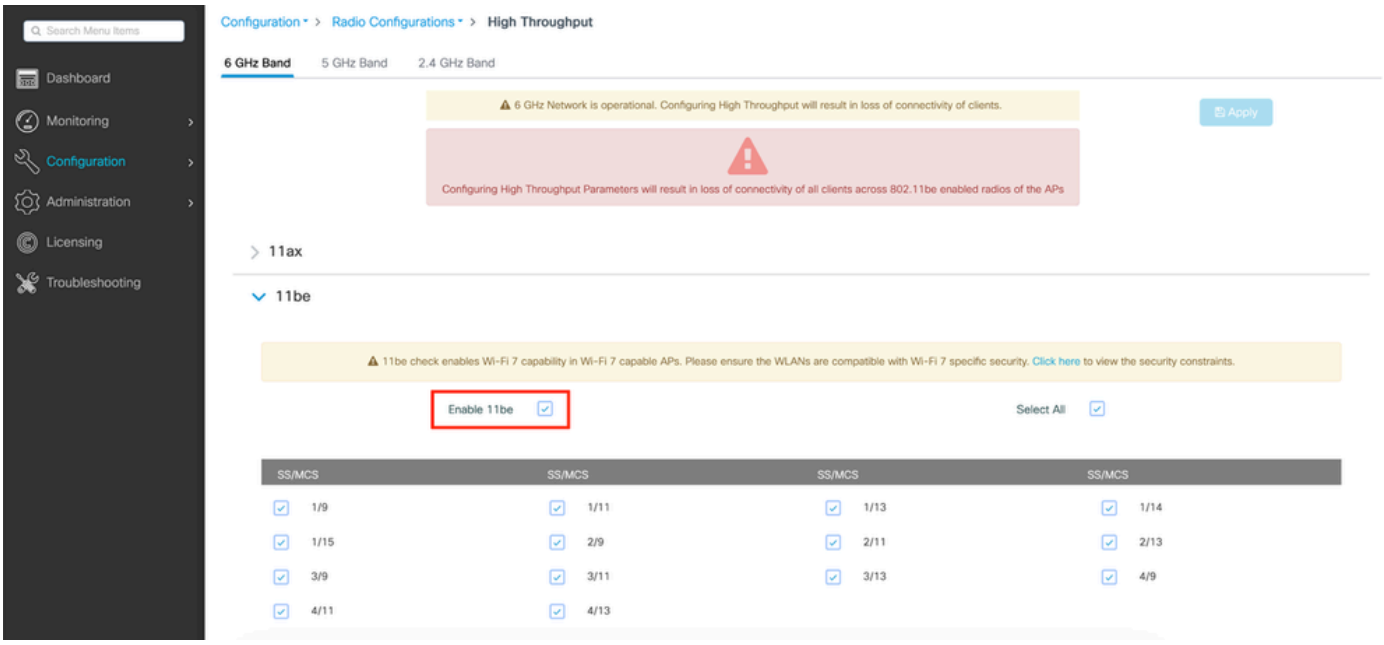
De plus, en raison des nouvelles normes, les points d'accès Wi-Fi 6E/7 prennent en charge les chiffrements GCMP256 pour WPA3. Il n'en va pas toujours de même pour certains points d'accès Wi-Fi 6 et les modèles antérieurs. Pour les SSID de phrase de passe/WPA3 personnel et Enhanced Open/OWE, nécessitant la configuration des algorithmes de chiffrement AES(CCMP128) et GCMP256, certains algorithmes de chiffrement Wi-Fi 6 (comme les gammes 9105, 9115 et 9120) ne prennent pas en charge GCMP256 et peuvent proposer des algorithmes de chiffrement AES(CCMP128) uniquement aux clients associés, y compris ceux compatibles Wi-Fi 6E/7. Si ces clients Wi-Fi 6E/7 devaient se déplacer depuis/vers les points d'accès Wi-Fi 6E/7 voisins prenant en charge GCMP256, ils devraient passer par une toute nouvelle association, car la renégociation des chiffres entre AES(CCMP128) et GCMP256 n'est pas prise en charge pour l'itinérance transparente. De plus, en général, il n'est pas optimal d'avoir des AP offrant des capacités différentes dans le même domaine : ce déploiement ne permet pas aux clients d'utiliser ces fonctionnalités de manière fiable lors de leur déplacement et peut entraîner une rémanence ou des déconnexions.
Bien que ce scénario doive représenter un cas d'angle, nous voulons toujours garder à l'esprit que, avec les chiffrements GCMP256 configurés sous le WLAN, l'itinérance des clients Wi-Fi 6E/7 entre les AP 9105/915/9120 et les AP 9130/9124/916x/917x ne peut pas être possible, car ces dernières séries prennent en charge GCMP256 et les premiers ne le font pas.

Les largeurs de canaux de 40 MHz ou plus sur 6 GHz peuvent également entraîner un collage pour les clients compatibles 6 GHz, qui peuvent refuser de se réassocier à d'autres bandes. Cela doit être une raison supplémentaire de ne pas mélanger des points d'accès compatibles 6 GHz et des points d'accès non compatibles 6 GHz dans la même zone d'itinérance.

Activation globale du Wi-Fi 7

Activation globale de Wi-Fi 7 sur IOS XE

Lors de l'installation ou de la mise à niveau vers une version IOS XE prenant en charge Wi-Fi 7, par défaut, la prise en charge de Wi-Fi 7 est globalement désactivée.
Pour l'activer, nous devons naviguer dans le menu de configuration Haut débit de chaque bande 2,4/5/6 GHz et cocher la case pour activer 11be.



Une autre option pourrait également être d'exécuter ces trois lignes de commande via SSH/console, en mode de configuration de terminal :

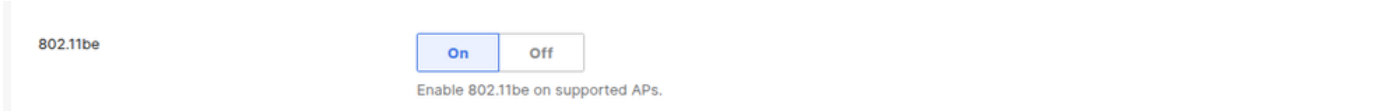
```
ap dot11 24ghz dot11be
ap dot11 5ghz dot11be
ap dot11 6ghz dot11be
```

Comme indiqué dans la note d'avertissement, lorsque vous essayez de modifier ces paramètres, la modification de l'état de la prise en charge de la norme 802.11be entraîne une brève perte de connectivité pour tous les clients sur les radios des points d'accès Wi-Fi 7. Si vous voulez effectuer une MLO, ce qui signifie que les clients se connectent à plusieurs bandes en même temps, vous devez activer 11be sur toutes les bandes auxquelles vous voulez que le client se connecte. Il n'est pas nécessaire d'activer toutes les bandes, mais recommandé simplement pour les performances.

Activation globale du Wi-Fi 7 sur le tableau de bord Cisco Meraki

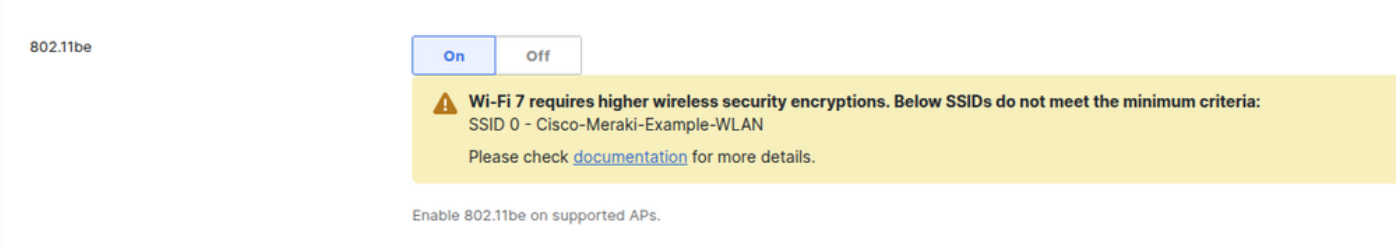
Lors de l'ajout de points d'accès compatibles Wi-Fi 7 (par exemple CW9178I, CW9176I/D1) à un réseau de tableau de bord Cisco Meraki pour la première fois, la prise en charge du fonctionnement de la norme 802.11be se fait sur leur profil RF par défaut.
Pour l'activer, nous devons naviguer sous Wireless > Radio Settings, cliquez sur l'onglet RF Profile et sélectionnez le profil assigné au point d'accès (par défaut : « Profil intérieur de base » pour les points d'accès intérieurs).

Dans la section General, activez 802.11be (on) comme indiqué dans cette capture d'écran :



Si un ou plusieurs WLAN sont configurés avec des paramètres de sécurité inférieurs à ceux requis par la spécification Wi-Fi 7, le tableau de bord affiche une bannière pour alerter les utilisateurs, comme indiqué ci-après.

Alors que le tableau de bord permet d'enregistrer la configuration, le Wi-Fi 7 n'est pas activé sur les SSID marqués tant que la conformité aux exigences du Wi-Fi 7 n'est pas assurée.
À l'heure de la rédaction de ce document, tous les réseaux locaux sans fil activés sur le réseau doivent répondre aux exigences de la spécification Wi-Fi 7 pour être activés sur la version du microprogramme MR 31.1.x et ultérieure (ce comportement change dans une future version du microprogramme MR 32.1.x).



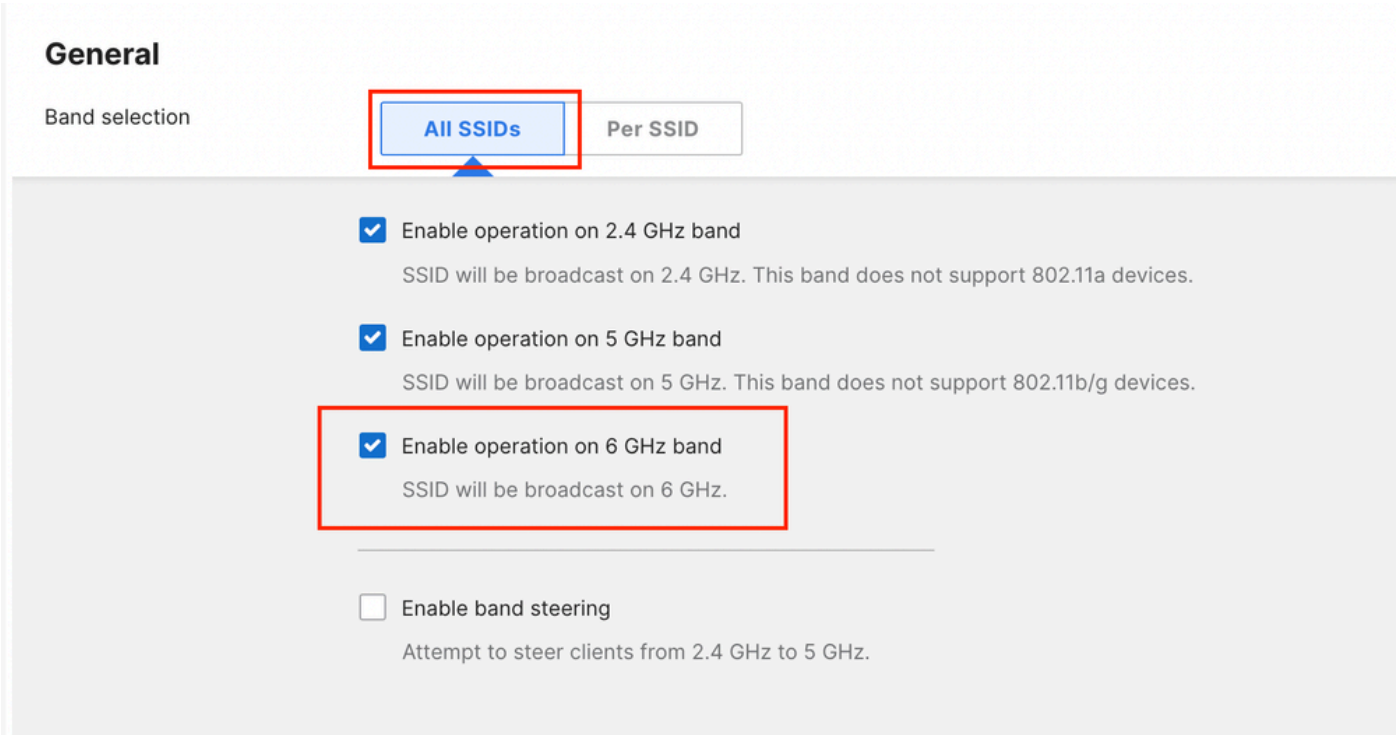
Une fois que la configuration du SSID répond aux critères minimum du Wi-Fi 7, la bannière disparaît.

Dans le même profil RF, assurez-vous d'activer le fonctionnement à 6 GHz sur les points d'accès.

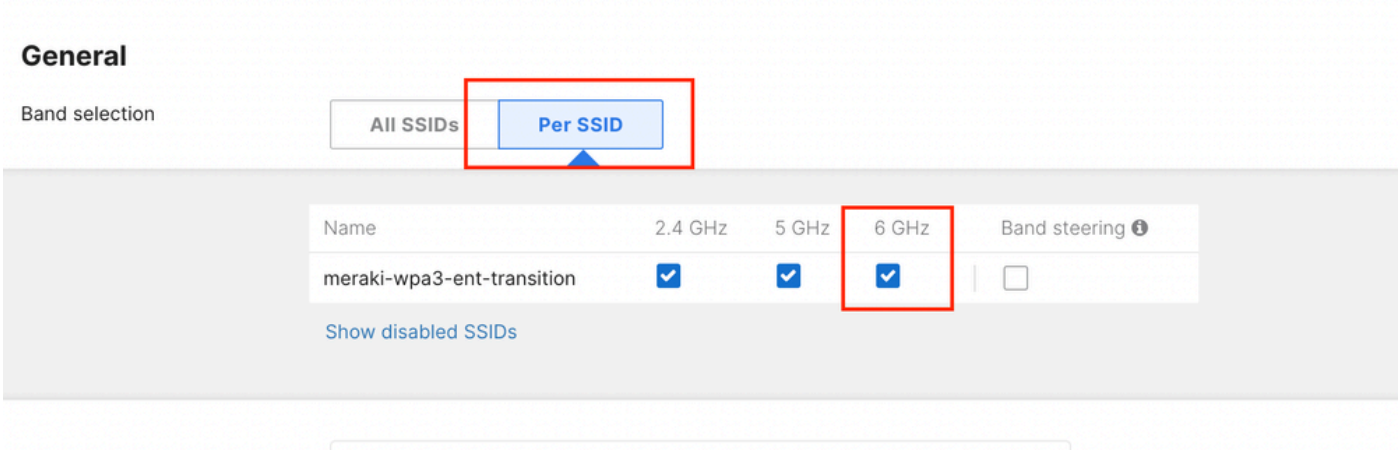
Cela peut être fait soit pour tous les SSID en masse ou par SSID individuel.

Notez que le réglage de bande est disponible uniquement entre 2,4 et 5 GHz.

Exemple d'activation de 6 GHz pour tous les SSID.



Exemple d'activation 6 GHz pour un seul SSID.



Scénarios :

Réseaux d'entreprise 802.1X / WPA3

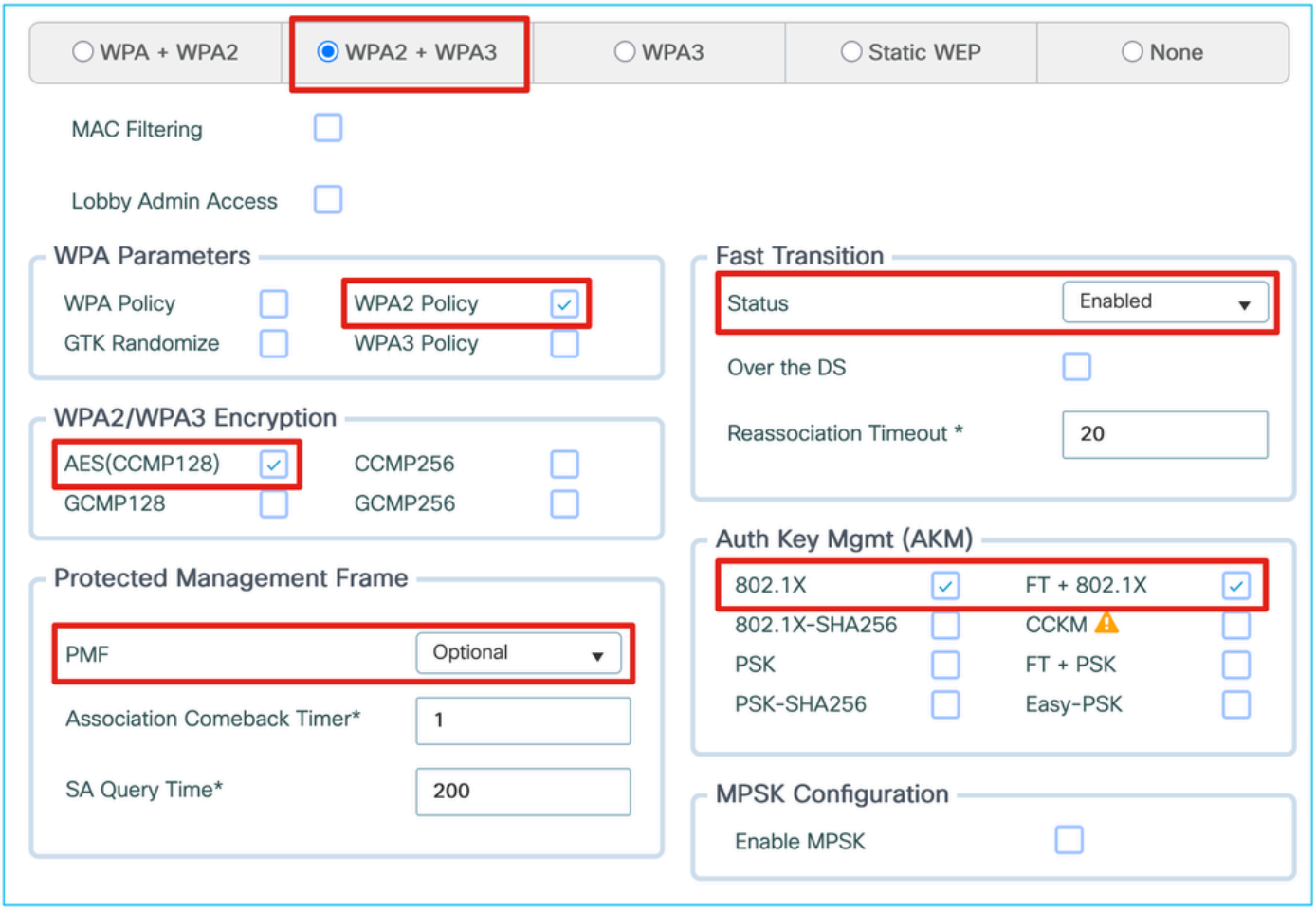
Configuration WPA3-Enterprise sur IOS XE

Les WLAN d'entreprise basés sur WPA2/3 avec authentification 802.1X sont les plus faciles à migrer vers 6 GHz et/ou Wi-Fi 7.

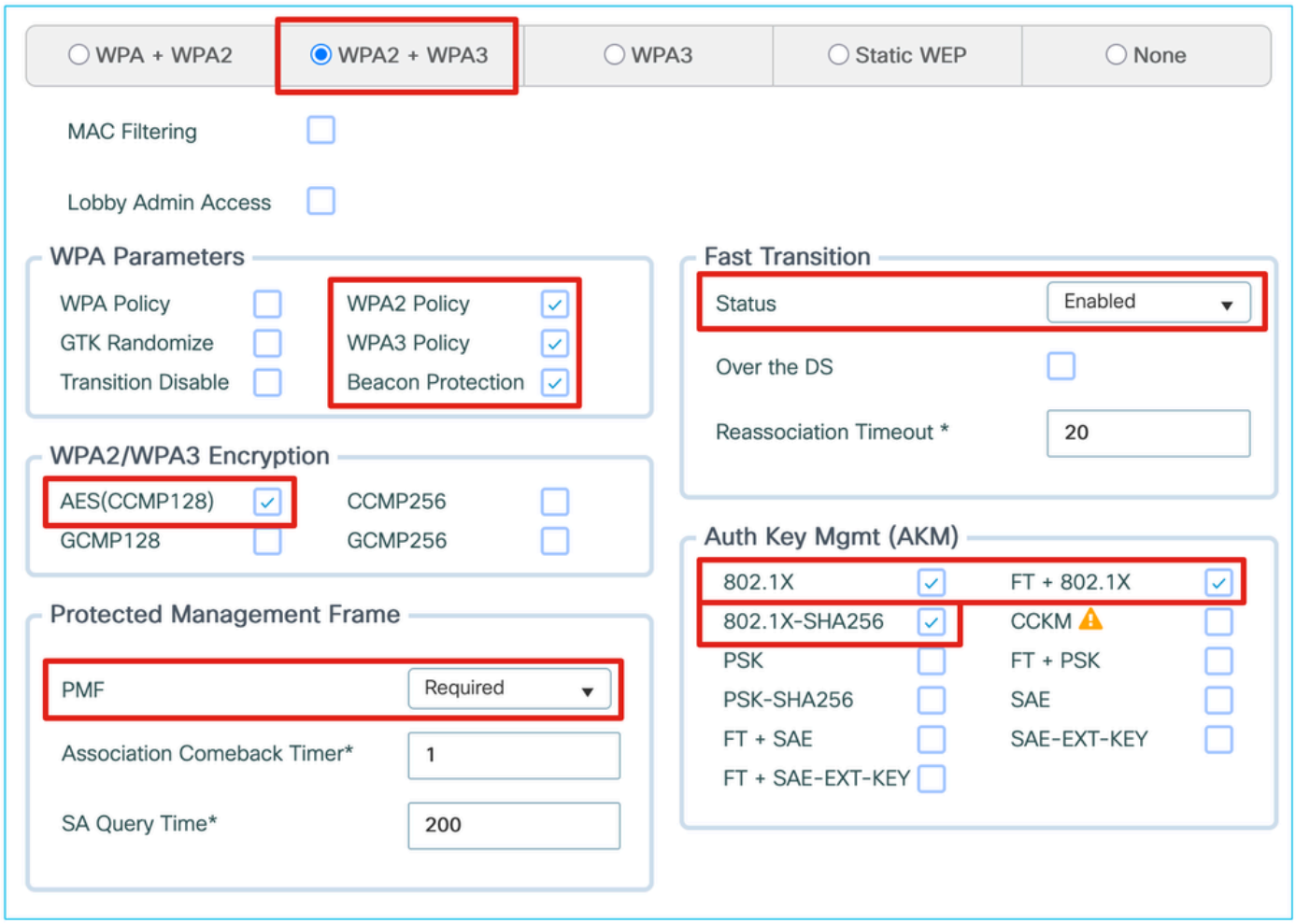
L'activation de votre SSID 802.1X pour 6 GHz ne nécessite que l'activation de la prise en charge PMF, même en option, ainsi que des AKM 802.1X-SHA256 et/ou FT + 802.1X, tous deux conformes à la norme WPA3.

Nous pouvons continuer à proposer le WPA2 avec la norme 802.1X (SHA1) sur le même WLAN. La prise en charge du Wi-Fi 7 nécessite l'activation de Beacon Protection et le paramétrage de PMF plutôt qu'en option ; WPA2 802.1X (SHA1) peut rester présent sur le WLAN en tant qu'option de rétrocompatibilité. Cela signifie que vous pouvez placer tous vos périphériques d'entreprise sous un seul SSID, à condition qu'ils prennent en charge la norme 802.11w/PMF, ce qui est assez courant sur les cartes réseau sans fil actuelles pour les ordinateurs portables et autres terminaux mobiles.

À partir d'un SSID WPA2 typique avec ces paramètres de sécurité L2 :



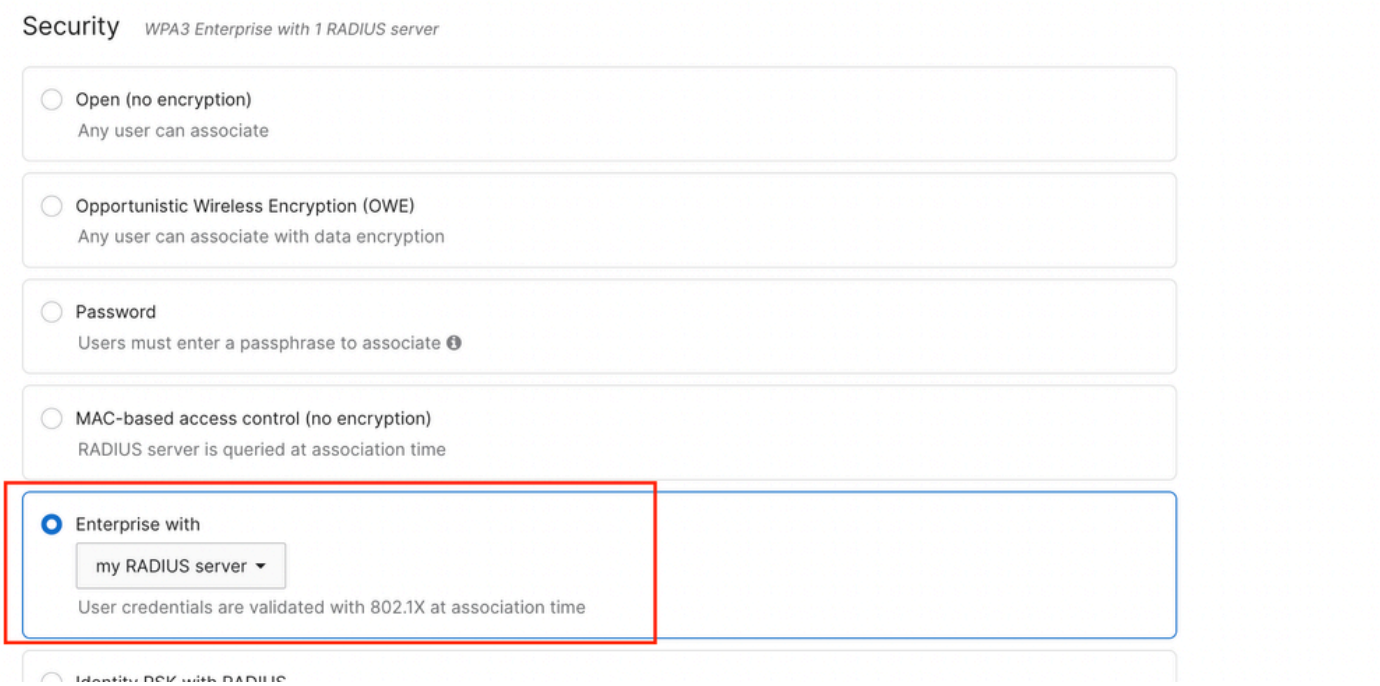
Nous pouvons migrer la configuration pour la prise en charge de WPA3, 6 GHz et Wi-Fi 7, comme illustré ci-dessous :



Configuration WPA3-Enterprise sur le tableau de bord Cisco Meraki

Au moment de la rédaction de ce document, le mode WPA3-Enterprise n'est disponible qu'avec un serveur RADIUS externe (également appelé « mon serveur RADIUS »).

WPA3-Enterprise n'est pas disponible avec l'authentification cloud Meraki.



À partir de MR 31.x, les types WPA sont les suivants :

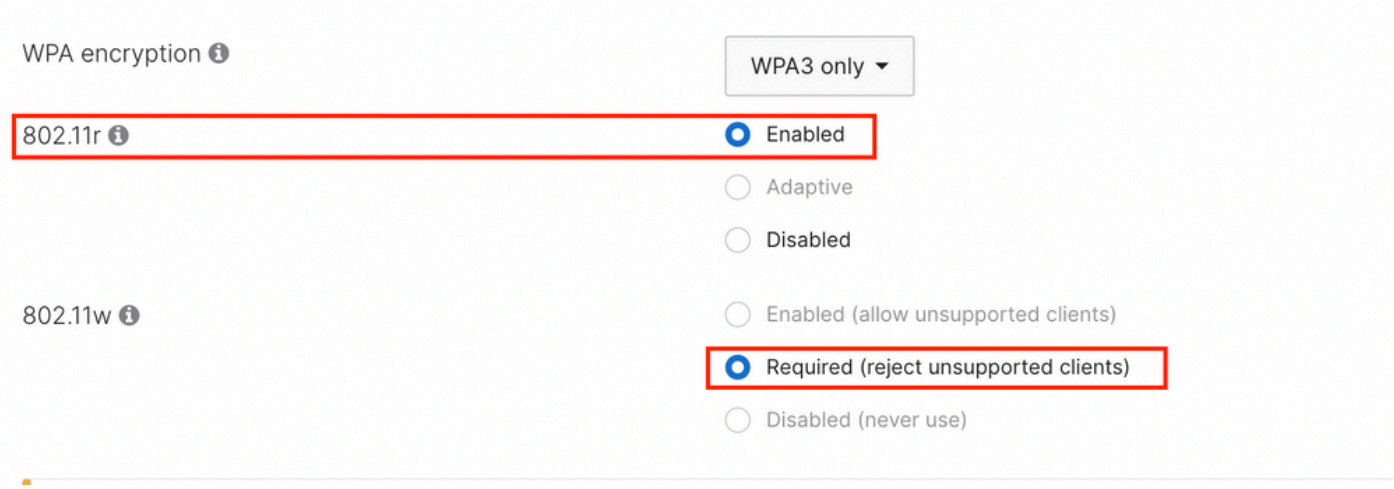
- « WPA3 only », qui utilise les mêmes chiffres que WPA2, mais nécessite la norme 802.11w (PMF).
- 'WPA3 192 bits', qui autorise uniquement la méthode EAP-TLS avec les chipers TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ou TLS_DHE_RSA_WITH_AES_256_GCM_SHA384. Ce mode nécessite la configuration des mêmes chipers sur le serveur RADIUS pour activer ce mode.
- « Mode de transition WPA3 » (ou mode mixte), qui permet la coexistence de clients WPA2 sur le même WLAN utilisé pour WPA3.

Lorsque vous utilisez « WPA3 only » ou « WPA3 192-bit Security », le protocole PMF est obligatoire pour tous les clients.

Dans la plupart des applications, la norme FT (802.11r), bien que non obligatoire, doit être mieux

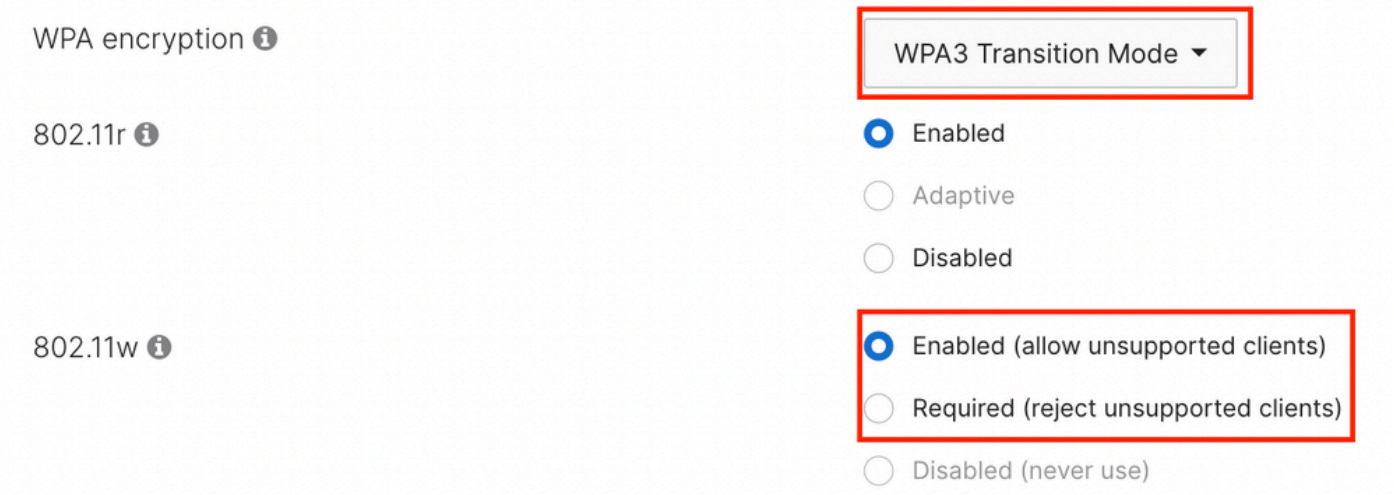
activée pour atténuer l'impact de l'itinérance et de la latence de réauthentification lors de l'utilisation d'un serveur RADIUS externe.

Le fonctionnement à 6 GHz nécessite l'activation du protocole PMF (802.11w).



Lorsque vous sélectionnez le mode de transition WPA3, tous les clients capables d'utiliser le mode WPA3 utilisent par défaut le mode PMF. Tous les clients fonctionnant sur 6 GHz utilisent le WPA3.

Dans ce mode, vous pouvez sélectionner si le client hérité utilisant WPA2 doit utiliser PMF (802.11w requis) ou si cette fonctionnalité est facultative (802.11w activé).



Quelle que soit la sélection WPA3, les points d'accès Cisco Meraki nécessitent que la suite de chiffrement GCMP 256 soit activée pour fonctionner en mode Wi-Fi 7.

En outre, Beacon Protection est activé par défaut sur 2,4, 5 et 6 GHz lorsque les points d'accès fonctionnent en mode Wi-Fi 7.

Phrase de passe / WPA3 personnel / Réseaux IoT

L'activation d'un SSID de phrase de passe pour 6 GHz, jusqu'à la prise en charge du Wi-Fi 6E, est simple et nécessite SAE et/ou FT + SAE, ainsi que d'autres AKM WPA2 PSK si nécessaire. Cependant, pour la prise en charge du Wi-Fi 7, la certification exige l'ajout des AKM SAE-EXT-KEY et/ou FT + SAE-EXT-KEY, ainsi que du chiffrement GCMP256. Il n'est donc pas possible d'avoir un WLAN basé sur des phrases de passe avec à la fois une compatibilité maximale pour les clients plus anciens et des performances Wi-Fi 7.

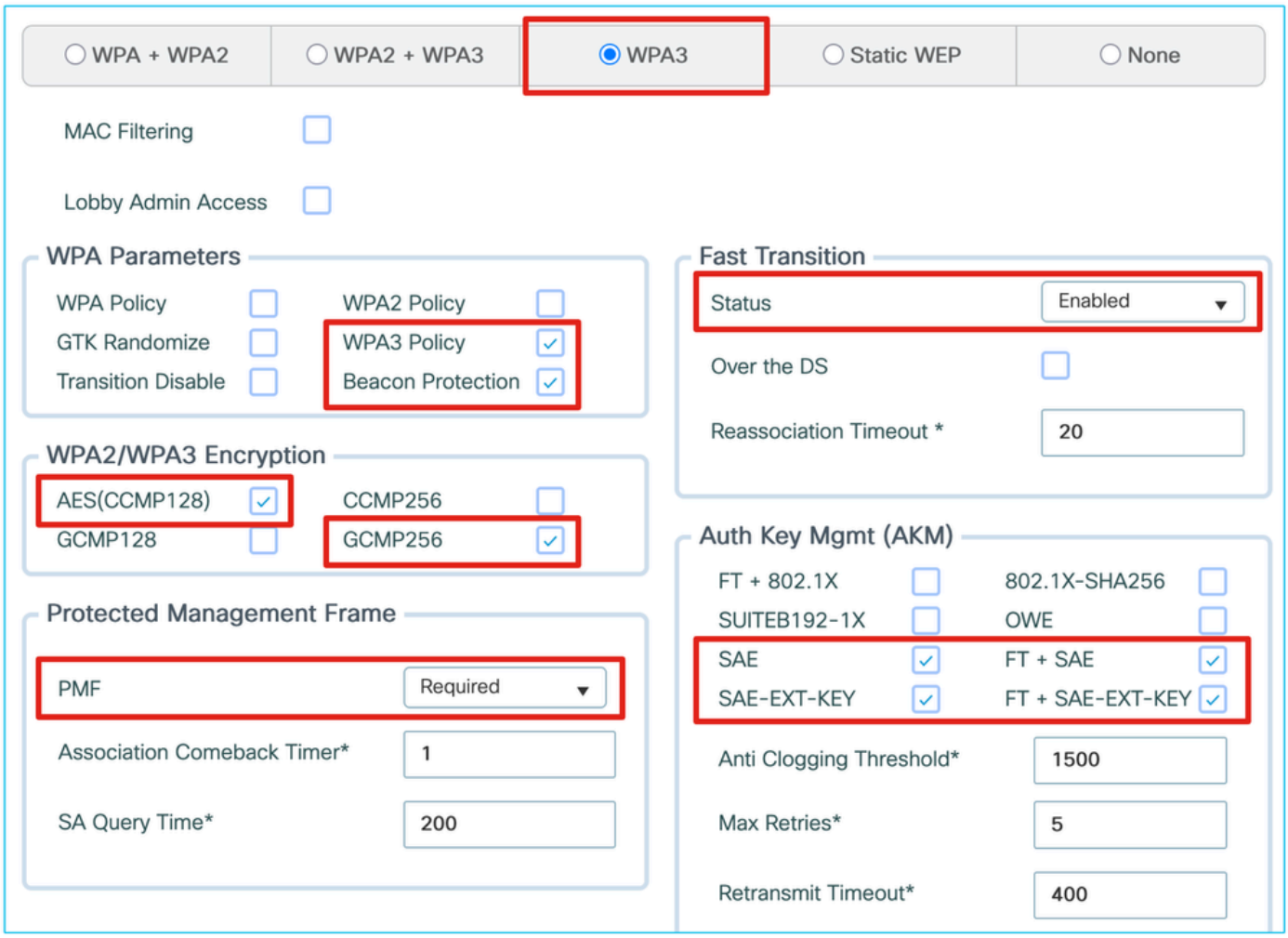
Dans de tels cas, nous pouvons configurer un SSID WPA3-only dédié avec SAE, FT + SAE, SAE-EXT-KEY et FT + SAE-EXT-KEY, offrant à la fois les chiffrements AES(CCMP128) et GCMP256, pour les clients Wi-Fi 6E et Wi-Fi 7 plus récents.

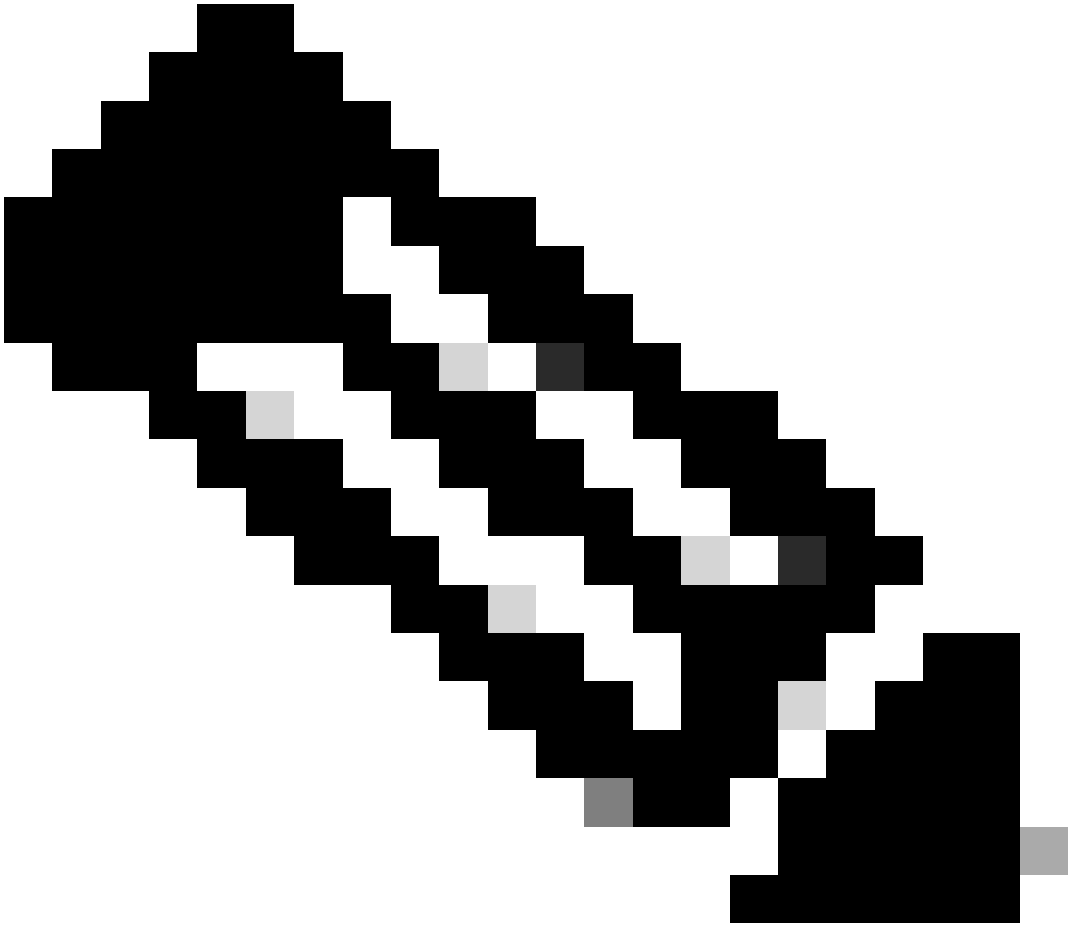
Il est possible d'avoir un WLAN en mode de transition qui autorise WPA2 PSK, en plus de WPA3 SAE et SAE-EXT, mais cela représente 6 AKM (si FT est utilisé) et certains clients légitimes pourraient avoir un problème avec cela. Nous vous recommandons de tester cette possibilité avec vos clients si vous décidez de passer en mode de transition WPA2-PSK+WPA3-SAE+SAE-EXT + FT.

Dans tous ces scénarios, nous vous recommandons vivement d'activer la fonction FT lors de l'utilisation de SAE. L'échange de trames SAE est coûteux en termes de ressources et plus long que la connexion en 4 étapes WPA2 PSK.

Certains fabricants d'appareils comme Apple s'attendent à utiliser SAE uniquement lorsque FT est activé et peuvent refuser de se connecter s'ils ne sont pas disponibles.

Configuration WPA3-SAE et WPA2-Personal sur IOS XE

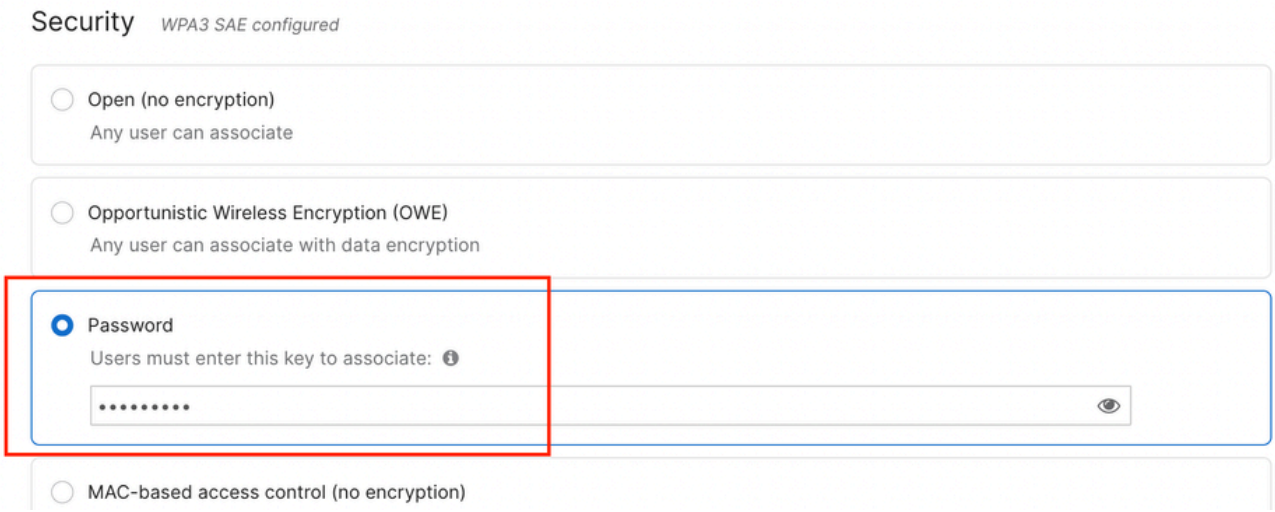

WPA + WPA2
WPA2 + WPA3
WPA3
Static WEP
None
MAC Filtering
Lobby Admin Access
WPA Parameters
WPA Policy
WPA2 Policy
GTK Randomize
WPA3 Policy
Transition Disable
Beacon Protection
WPA2/WPA3 Encryption
AES(CCMP128)
CCMP256
GCMP128
GCMP256
Protected Management Frame
PMF
Required
Association Comeback Timer*
1
SA Query Time*
200
Fast Transition
Status
Enabled
Over the DS
Reassociation Timeout *
20
Auth Key Mgmt (AKM)
FT + 802.1X
802.1X-SHA256
SUITEB192-1X
OWE
SAE
FT + SAE
SAE-EXT-KEY
FT + SAE-EXT-KEY
Anti Clogging Threshold*
1500
Max Retries*
5
Retransmit Timeout*
400



Remarque : Si (FT +) SAE est activé sur le WLAN et qu'un client Wi-Fi 7 tente de s'y associer au lieu de (FT +) SAE-EXT-KEY, il est rejeté. Tant que (FT +) SAE-EXT-KEY est également activé, les clients Wi-Fi 7 doivent de toute façon utiliser ce dernier AKM, et ce problème ne doit pas se produire.

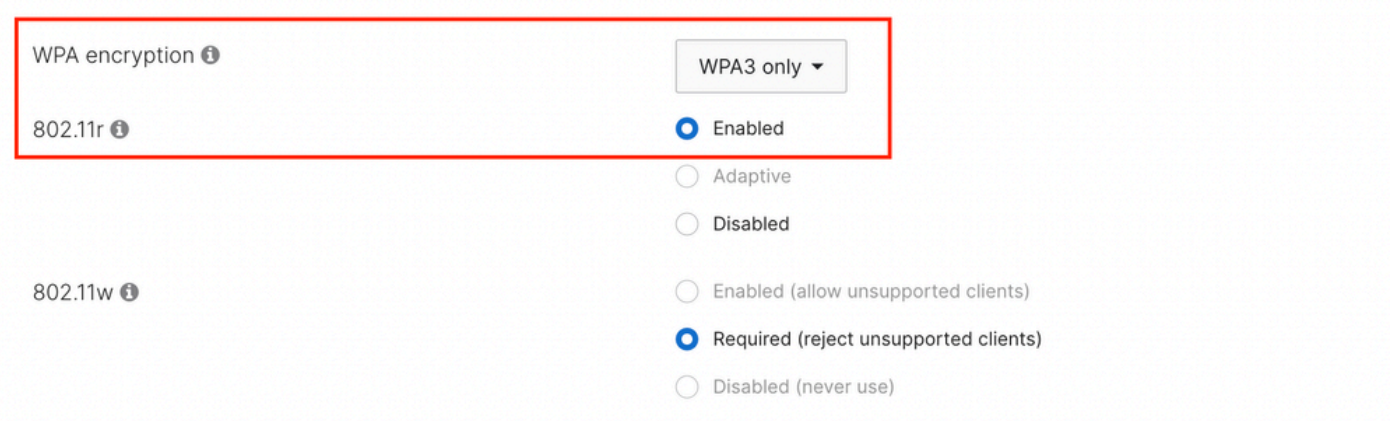
Bien que l'utilisation d'un WLAN hérité avec seulement un PSK au-dessus d'un WLAN WPA-3 seulement augmente la quantité de SSID totaux, elle permet de conserver une compatibilité maximale sur un SSID, où nous pouvons également potentiellement désactiver d'autres fonctionnalités avancées qui pourraient avoir un impact sur la compatibilité et qui pourraient être utiles pour de nombreux scénarios IoT, tout en offrant des fonctionnalités et des performances maximales aux périphériques plus récents par l'intermédiaire de l'autre SSID. Il peut s'agir d'un scénario préféré si vous avez des périphériques IoT plus anciens ou plus sensibles dans l'image. Si vous n'avez pas de périphériques IoT, opter pour un WLAN en mode de transition unique peut être plus efficace, car vous n'annoncez qu'un seul SSID.

Configuration WPA3-SAE sur le tableau de bord Cisco Meraki



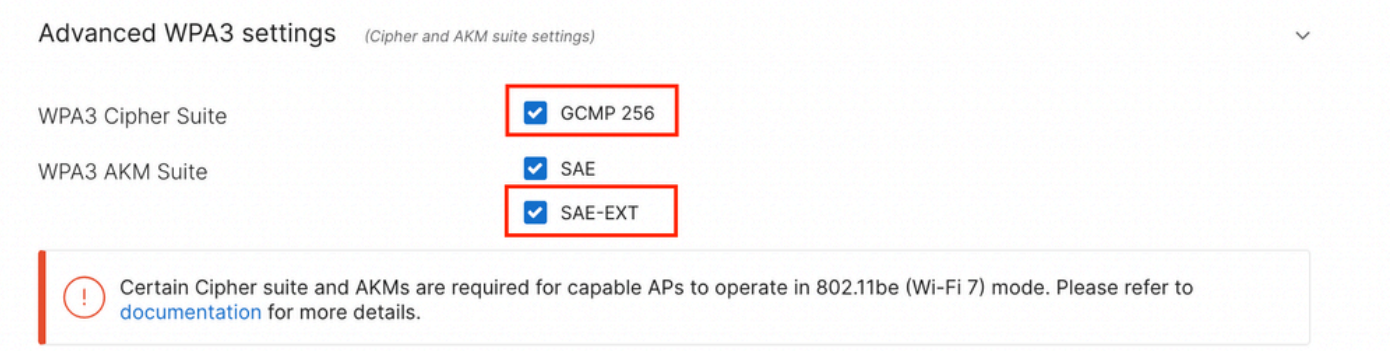
Jusqu'au micrologiciel MR 30.x, le seul type WPA pris en charge est « WPA3 uniquement » et le tableau de bord ne vous permet pas de sélectionner une autre méthode.

PMF est obligatoire dans cette configuration, tandis que FT (802.11r) est recommandé d'être activé lors de l'utilisation de SAE.



Pour permettre le fonctionnement du Wi-Fi 7, la suite de puces GCMP 256 et la suite SAE-EXT AKM doivent être activées lors de la configuration du SSID.

Ils sont désactivés par défaut et peuvent être activés sous « Paramètres WPA3 avancés ».



À l'heure de la rédaction de ce document, tous les WLAN activés sur le réseau doivent répondre aux exigences de la spécification Wi-Fi 7 pour être activés sur la version du microprogramme MR

31.1.x et ultérieure.

Cela signifie qu'un SSID Wi-Fi 7 configuré comme décrit précédemment ne peut pas coexister avec un autre SSID utilisant le mode de transition WPA2-Personal ou WPA3-SAE.

Si un SSID WPA2 personnel est configuré dans le réseau du tableau de bord, tous les points d'accès Wi-Fi 7 repasseraient en mode Wi-Fi 6E.

Ce comportement change dans une version future du microprogramme MR 32.1.x.

Réseaux ouverts/améliorés ouverts/OWE/Invités

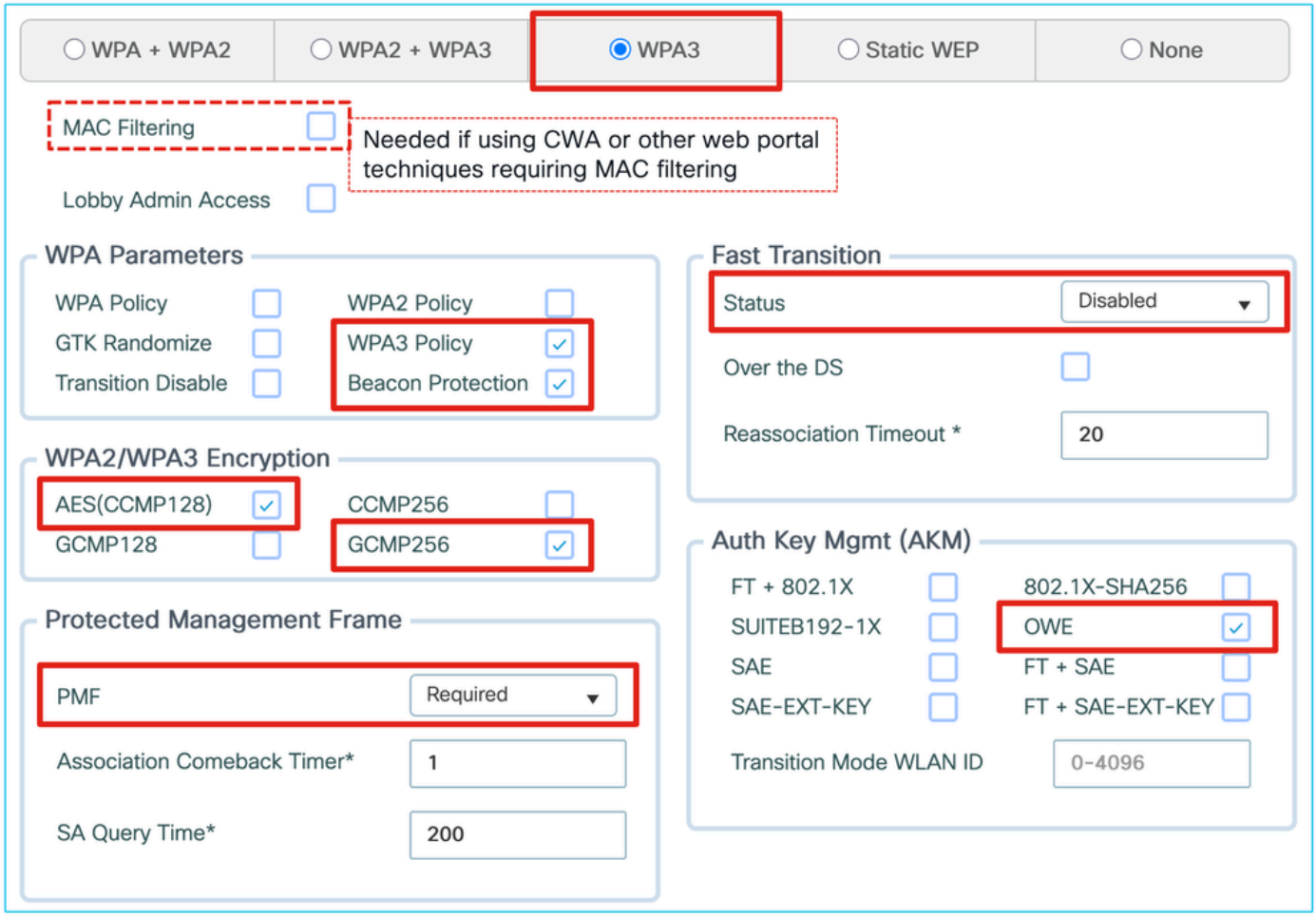
Les réseaux d'invités sont nombreux. En général, ils ne nécessitent aucune identification 802.1X ou phrase de passe pour se connecter, et peuvent impliquer une page d'accueil ou un portail, qui peut nécessiter des informations d'identification ou un code. Ce problème est généralement traité avec un SSID ouvert et des solutions de portail invité local ou externe. Cependant, les SSID avec sécurité ouverte (pas de cryptage) ne sont pas autorisés sur 6 GHz ou pour la prise en charge du Wi-Fi 7.

Une première approche très prudente consisterait à dédier les réseaux invités à la bande 5 GHz et au mieux au Wi-Fi 6. Cela laisse la bande 6 GHz réservée aux appareils d'entreprise, résout le problème de complexité et apporte une compatibilité maximale, mais pas jusqu'aux performances Wi-Fi 6E/7.

Si, d'un côté, l'option Enhanced Open est une excellente méthode de sécurité qui offre la confidentialité tout en conservant l'expérience « ouverte » (les utilisateurs finaux n'ont pas besoin de saisir d'informations d'identification ou de phrase de passe 802.1X), à ce jour, elle offre toujours une prise en charge limitée entre les terminaux. Certains clients ne le prennent toujours pas en charge et, même lorsqu'ils le font, cette technique n'est pas toujours bien gérée (le périphérique peut indiquer que la connexion n'est pas sécurisée, alors qu'elle l'est réellement, ou il peut l'afficher comme protégée par une phrase de passe, même si aucune phrase de passe n'est nécessaire avec OWE). Un réseau invité étant censé fonctionner sur tous les périphériques non contrôlés invités, il peut être trop tôt pour fournir uniquement un SSID ouvert amélioré et il est recommandé de fournir les deux options via des SSID distincts : un ouvert sur 5 GHz et un OWE activé sur 5 et 6 GHz, les deux avec le même portail captif derrière si cela est aussi une exigence. Le mode de transition n'est pas pris en charge sur les réseaux Wi-Fi 6E, 6 GHz (même s'il peut toujours être autorisé sur le logiciel) ou Wi-Fi 7, ce n'est donc pas une solution recommandée. Toutes les techniques de redirection du portail (authentification Web interne ou externe, authentification Web centrale, ...) sont toujours prises en charge avec OWE.

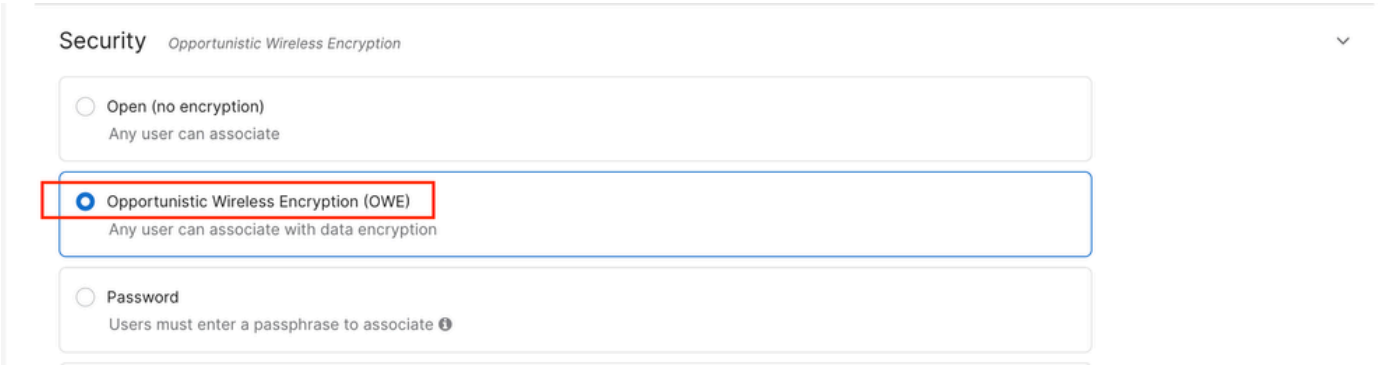
Configuration OWE sur IOS XE

Si nous souhaitions fournir un service 6 GHz aux invités, nous vous recommandons de créer un SSID distinct avec Enhanced Open / OWE (Opportunistic Wireless Encryption). Il peut offrir le chiffrement AES(CCMP128), pour une compatibilité maximale jusqu'aux clients Wi-Fi 6E, ainsi que les bits GCMP256 pour les clients compatibles Wi-Fi 7.



Configuration OWE sur le tableau de bord Cisco Meraki

À l'instar de ce qui a été fait sur IOS XE, la recommandation consiste à créer un SSID invité distinct avec Enhanced Open / OWE fonctionnant sur 6 GHz sur le tableau de bord Cisco Meraki. Vous pouvez le reconfigurer dans Wireless > Access Control, et sélectionner « Opportunistic Wireless Encryption (OWE) » comme méthode de sécurité.



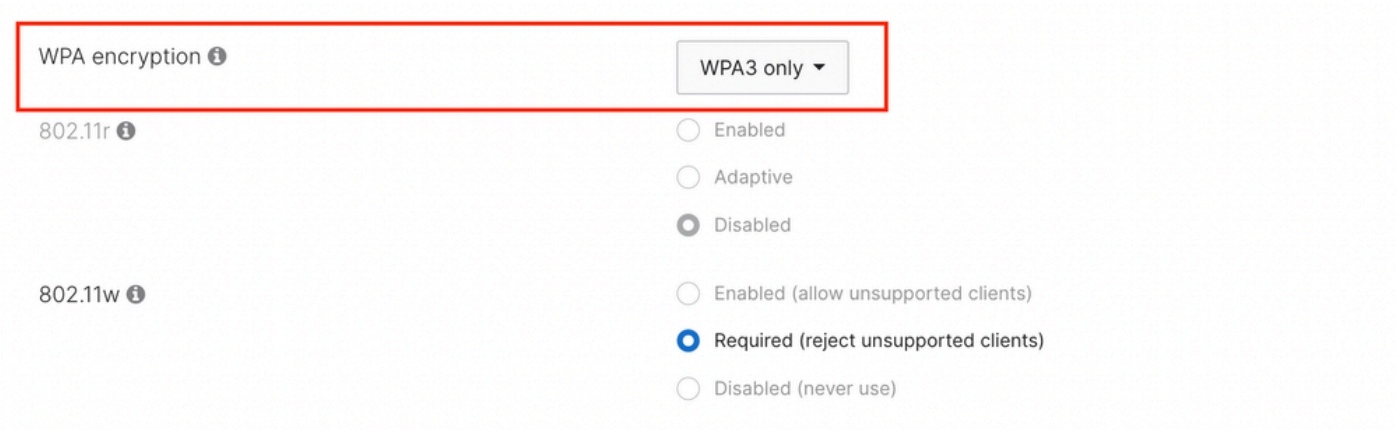
Lors de l'exécution du micrologiciel jusqu'à MR31, le seul type WPA pris en charge est « WPA3 uniquement » et le tableau de bord ne vous permet pas de sélectionner une autre méthode.

PMF est obligatoire dans cette configuration, tandis que FT (802.11r) ne peut pas être activé.

Notez que l'étiquetage « WPA3 only » est surchargé, car OWE ne fait pas partie de la norme

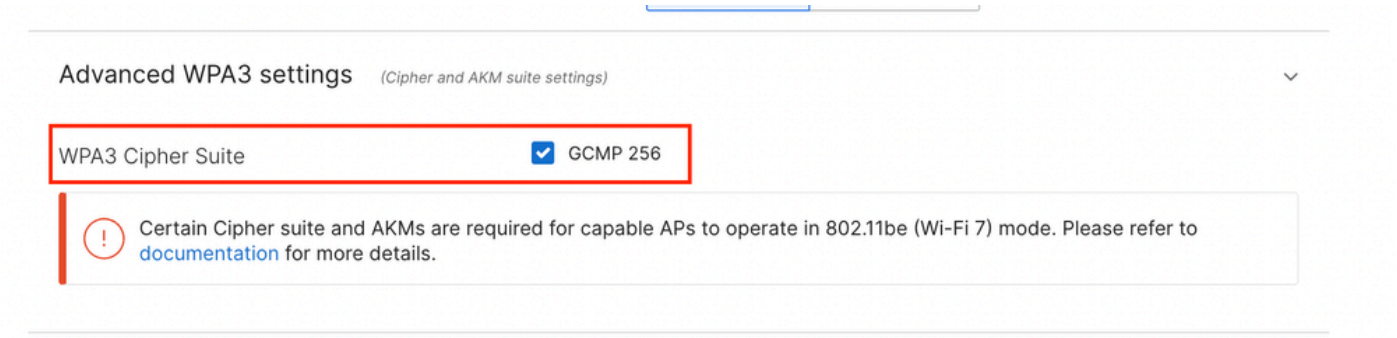
WPA3 ; cependant, cette configuration fait référence à OWE sans mode de transition.

Le mode de transition OWE est disponible dans le cadre d'une future version de MR 32.1.x.



Le chiffrement AES(CCMP128) est activé par défaut pour une compatibilité maximale jusqu'aux clients Wi-Fi 6E.

Les bits GCMP256 peuvent être activés en même temps que le CCMP128 pour la conformité aux exigences Wi-Fi 7.



WPA3 supplémentaire et options associées

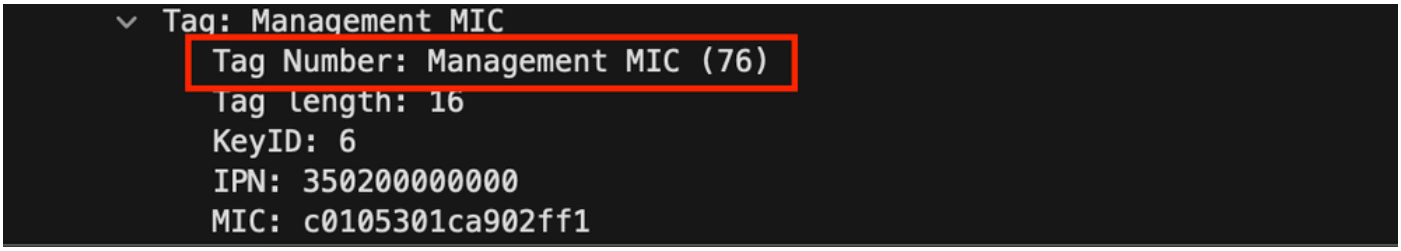
Bien que les options WPA3 soient mieux décrites et couvertes dans le guide de déploiement WPA3, cette section présente quelques recommandations supplémentaires pour WPA3 spécifiquement liées à la prise en charge de 6 GHz et du Wi-Fi 7.

Protection de balise

Il s'agit d'une fonctionnalité qui résout la vulnérabilité, où un attaquant malveillant peut transmettre des balises au lieu du point d'accès légitime, tout en modifiant certains champs pour modifier la sécurité ou d'autres paramètres des clients déjà associés. La protection de balise est un élément d'information supplémentaire (MIC de gestion) dans la balise agissant comme une signature pour la balise elle-même, afin de prouver qu'elle a été envoyée par le point d'accès légitime et qu'elle n'a pas été altérée. Seuls les clients associés à une clé de cryptage WPA3 peuvent vérifier la légitimité de la balise ; sonder les clients n'a aucun moyen de le vérifier. L'élément d'information supplémentaire de la balise doit simplement être ignoré par les clients qui ne la prennent pas en

charge (il s'agit de clients non Wi-Fi 7), et il ne provoque normalement pas de problèmes de compatibilité (sauf avec un pilote client mal programmé).

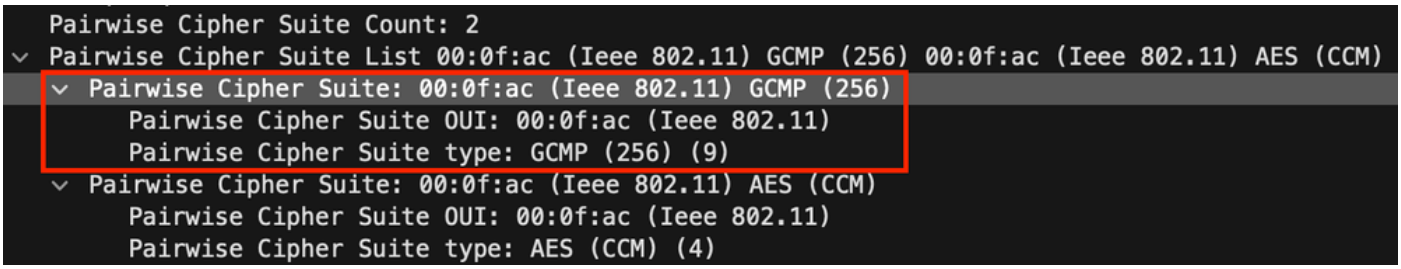
Cette capture d'écran présente un exemple du contenu de l'élément d'information MIC de gestion :



GCMP256

Jusqu'à la certification Wi-Fi 7, la plupart des clients mettaient en oeuvre le chiffrement AES(CCMP128). CCMP256 et GCMP256 sont des variantes très spécifiques de SUITE-B 802.1X AKM. Bien que certaines premières générations de clients Wi-Fi 7 sur le marché prétendent prendre en charge le Wi-Fi 7, ils ne mettent parfois toujours pas en oeuvre le chiffrement GCMP256, ce qui peut devenir un problème si les points d'accès Wi-Fi 7 appliquant la norme comme prévu empêchent ces clients de se connecter sans la prise en charge GCMP256 appropriée.

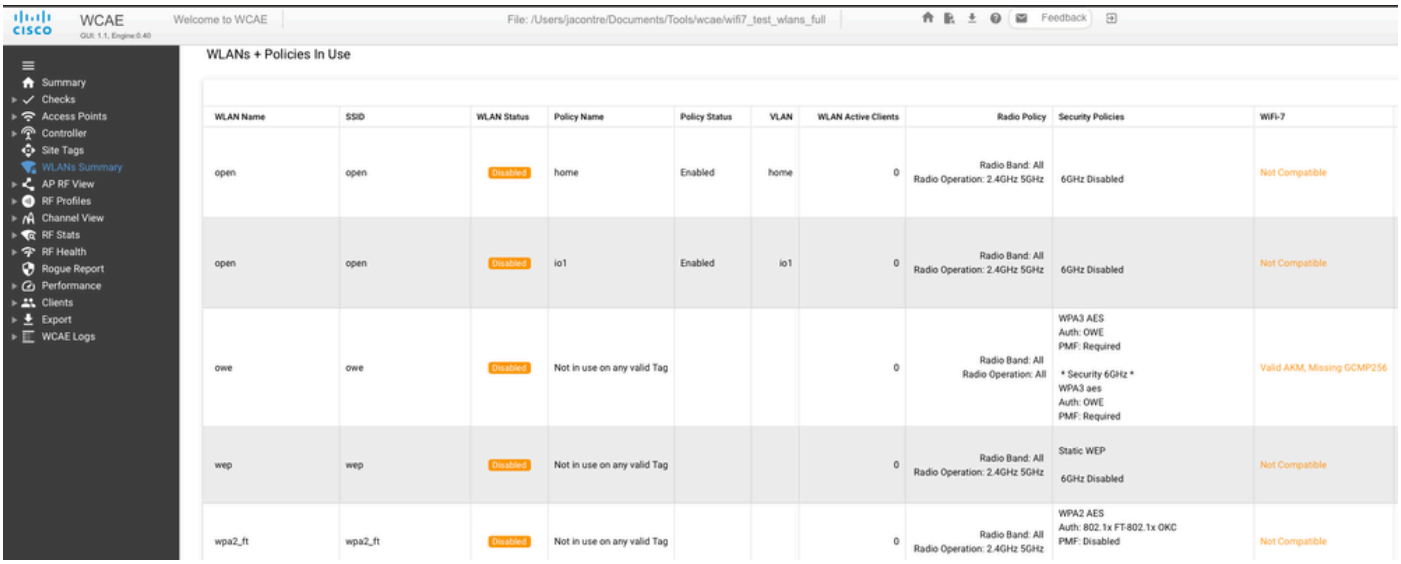
Lorsque GCMP256 est activé, le Robuste Security Network Element (RSNE) des trames de balise pour le WLAN annonce la capacité dans la liste Pairwise Chiper Suite comme indiqué ici.



Dépannage et vérification

La dernière version de Wireless Configuration Analyzer Express (https://developer.cisco.com/docs/wireless-troubleshooting-tools/wireless-config-analyzer-express-gui/) dispose d'un contrôle de préparation Wi-Fi 7 qui évalue votre configuration 9800 pour toutes les exigences Wi-Fi 7 mentionnées précédemment.

Si vous avez encore des doutes quant à la compatibilité de votre configuration avec le Wi-Fi 7, le WCAE vous indique ce qui ne va pas.



Références

1. Cisco Systems. « WPA3 Encryption and Configuration Guide ».
2. Guide WPA3 de Meraki

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.