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

Table des matières

- Introduction
  - Guide de conception CX
- Pourquoi 6 GHz et Wi-Fi 7
- Configuration de base requise pour les opérations 6 GHz et le Wi-Fi 7
  - Bande 6 GHz requise
  - Wi-Fi 7 requis
    - Cisco IOS® XE 17.15.3 et versions ultérieures 17.15.x
    - Cisco IOS XE 17.18.1/17.18.2
    - Cisco IOS XE 17.18.3 et versions ultérieures
- Considérations de conception radio pour une couverture 6 GHz
  - Comportements d'itinérance entre les points d'accès pré-Wi-Fi 6E/7 et Wi-Fi 6E/7
- Activation globale du Wi-Fi 7
  - Activation globale de Wi-Fi 7 sur Cisco IOS XE
  - Activation globale du Wi-Fi 7 sur le tableau de bord Cisco Meraki
- Scénarios :
  - Réseaux d'entreprise 802.1X / WPA3
    - Configuration WPA3-Enterprise sur Cisco IOS XE
    - Configuration WPA3-Enterprise sur le tableau de bord Cisco Meraki
  - Phrase de passe / WPA3 personnel / Réseaux IoT
    - Configuration WPA3-SAE sur Cisco IOS XE
    - Configuration WPA3-SAE sur le tableau de bord Cisco Meraki
  - Réseaux ouverts/améliorés ouverts/OWE/Invités
    - Configuration OWE sur Cisco IOS XE
    - Configuration OWE sur le tableau de bord Cisco Meraki
- WPA3 supplémentaire et options associées
  - Protection de balise
  - GCMP256
- Dépannage et vérification
  - Liste de vérification du dépannage
- Références

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 spécifiées par 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 une phrase de passe. SAE-FT (SAE avec transition rapide) est un autre AKM possible et est recommandé car la connexion SAE n'est pas triviale, et FT permet d'ignorer cet échange plus long.
- Enhanced Open avec cryptage sans fil opportuniste (OWE)

Bien que la spécification WPA3 v3.4 (Section 11.2) indique que le mode de transition Enhanced Open n'est pas pris en charge sur 6 GHz, de nombreux fournisseurs (y compris Cisco jusqu'à Cisco IOS XE 17.18) n'appliquent pas encore cette restriction. Par conséquent, il est techniquement possible de configurer, par exemple, un SSID ouvert sur 5 GHz et un SSID ouvert amélioré correspondant sur 5 et 6 GHz, les deux avec le mode de transition activé, sans respecter les spécifications standard. Cependant, dans un tel scénario, configurez plutôt un SSID ouvert amélioré sans mode de transition disponible uniquement sur 6 GHz (les clients prenant en charge 6 GHz prennent généralement en charge également l'ouverture améliorée), tout en conservant notre SSID ouvert normal sur 5 GHz, également sans mode de transition.

Il n'existe aucune nouvelle exigence spécifique 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, dont Cisco, considèrent que seuls les protocoles 802.1X-SHA256 ou « FT + 802.1X » (qui correspond à 802.1X avec SHA256 et Fast Transition) sont conformes à la norme WPA3. La norme 802.1X standard (qui utilise SHA1) est considérée comme faisant partie de WPA2 et n'est donc pas adaptée ou 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. Certaines de ces exigences permettent l'utilisation de débits de données 802.11be et d'améliorations de protocole, tandis que d'autres prennent en charge les opérations MLO (Multi-

Link Operations), 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). La nouvelle spécification WPA3 (v3.4) modifie la condition en « Le point d'accès doit offrir l'algorithme GCMP256 », même si le client est toujours autorisé à utiliser AES128. Cela crée des différences dans le comportement du client : certains clients tentent d'utiliser le Wi-Fi 7 Entreprise avec AES128, tandis que d'autres attendent déjà le GCMP256.
- 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, 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 :

Cisco IOS® XE 17.15.3 et versions ultérieures 17.15.x

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

Un client peut s'associer en tant que périphérique compatible Wi-Fi 7 et obtenir des débits de données Wi-Fi 7 quelle que soit la méthode de sécurité qu'il utilise, à condition que cette méthode soit prise en charge par le WLAN. Cependant, le client ne peut s'associer en tant que MLO (sur une ou plusieurs bandes) que s'il répond aux exigences strictes de sécurité Wi-Fi 7 ; dans le cas contraire, elle est rejetée.

Cela peut entraîner des problèmes lorsque des clients Wi-Fi 7 qui ne prennent pas en charge des chiffrements plus sécurisés, tels que GCMP256, tentent une association MLO avec un WLAN dont les paramètres de sécurité ne répondent pas aux exigences Wi-Fi 7. Dans une telle situation, le client est rejeté en raison de paramètres de sécurité non valides, même si ces paramètres peuvent toujours être configurés sur le WLAN.

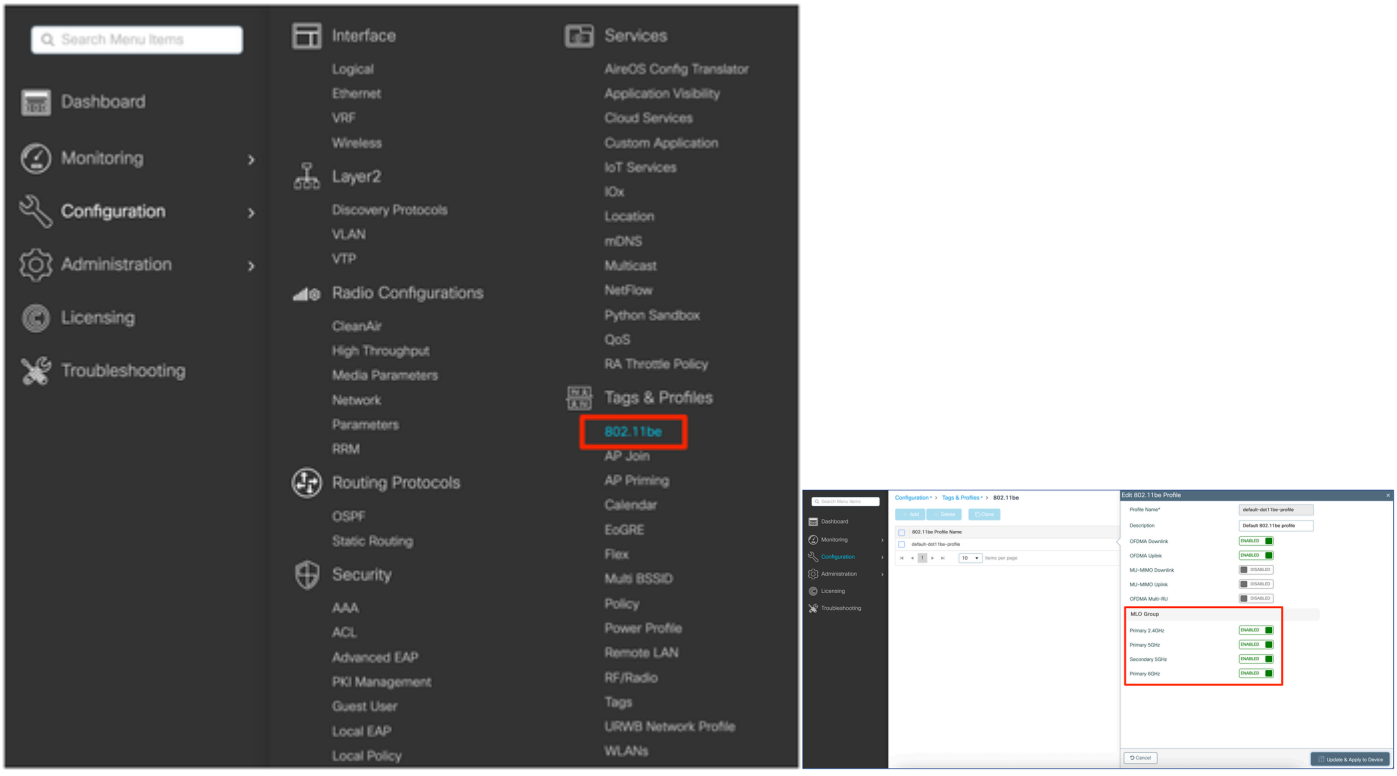
Cisco IOS XE 17.18.1/17.18.2

Beacon Protection est automatiquement activé si votre WLAN est compatible Wi-Fi 7, que vous cochiez ou non la case.

Cisco IOS XE 17.18.1 et les versions ultérieures annoncent un WLAN comme compatible Wi-Fi 7 et MLO uniquement si les exigences de sécurité appropriées sont activées dans les paramètres WLAN. Par exemple, un WLAN annonçant uniquement SAE, et non SAE-EXT, est diffusé comme MLO incapable.

La branche 17.18 introduit un profil 802.11be qui peut être associé à un profil WLAN pour contrôler l'activation du Wi-Fi 7 par SSID ou même par radio.

Un profil 802.11be préconfiguré nommé « default-dot11be-profile » est disponible par défaut dans le nouveau menu Configuration > Tags & Profiles > 802.11be.

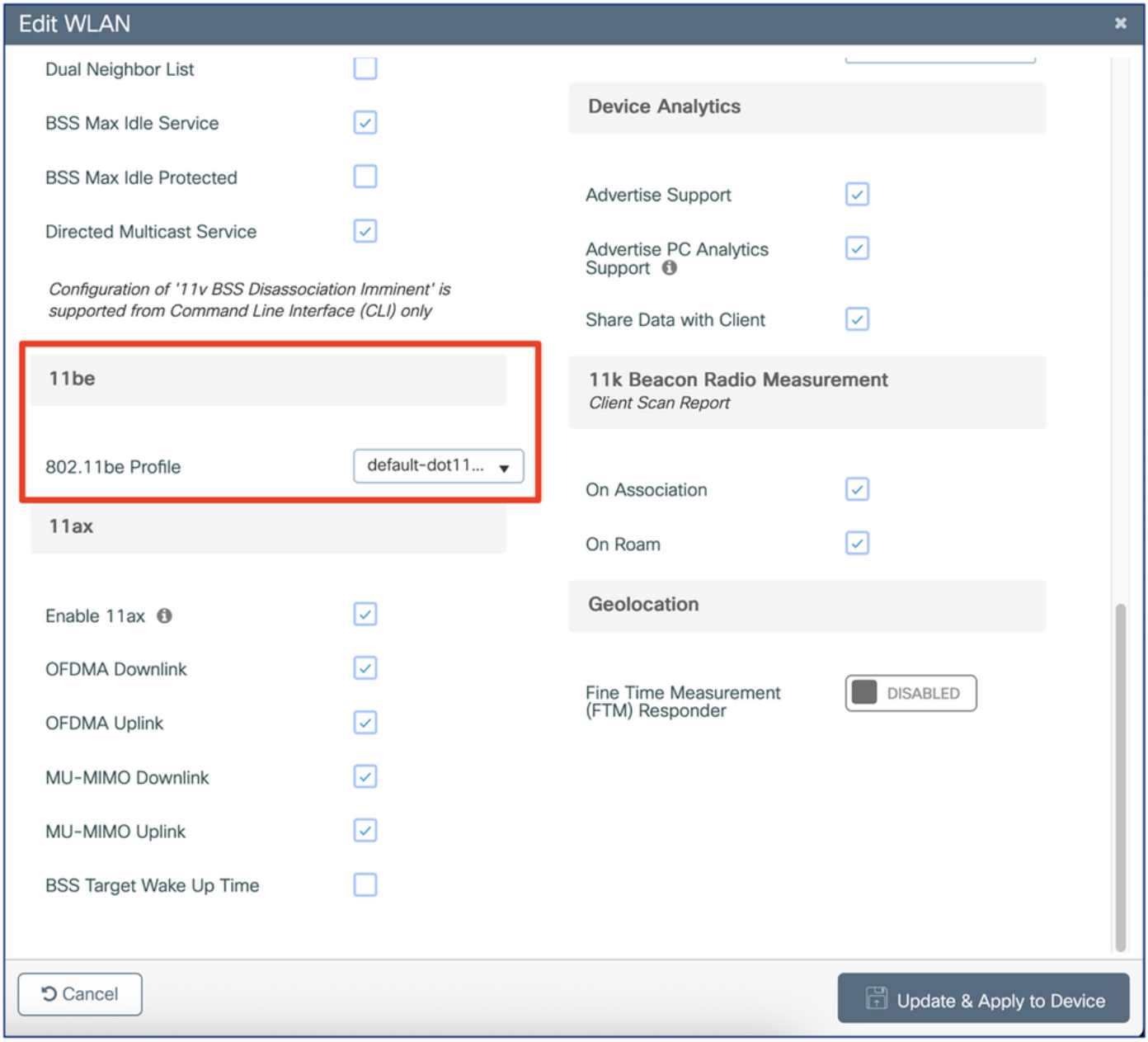


Les quatre principaux paramètres d'activation ou de désactivation du Wi-Fi 7 se trouvent dans la

section « MLO Group ». La désactivation des quatre paramètres désactive le Wi-Fi 7 sur toutes les bandes d'un profil WLAN auquel le profil 802.11be est connecté. L'activation de tout ou partie d'entre eux active le Wi-Fi 7 sur les bandes/radios correspondantes du profil WLAN connecté.

Le « default-dot11be-profile » active MLO et Wi-Fi 7 sur toutes les radios, et il est attaché par défaut à chaque profil WLAN.
En créant un nouveau profil 802.11be avec tous les paramètres « MLO Group » désactivés et en l'attachant à des profils WLAN spécifiques, nous pouvons, par exemple, désactiver sélectivement le Wi-Fi 7 pour certains de nos SSID.

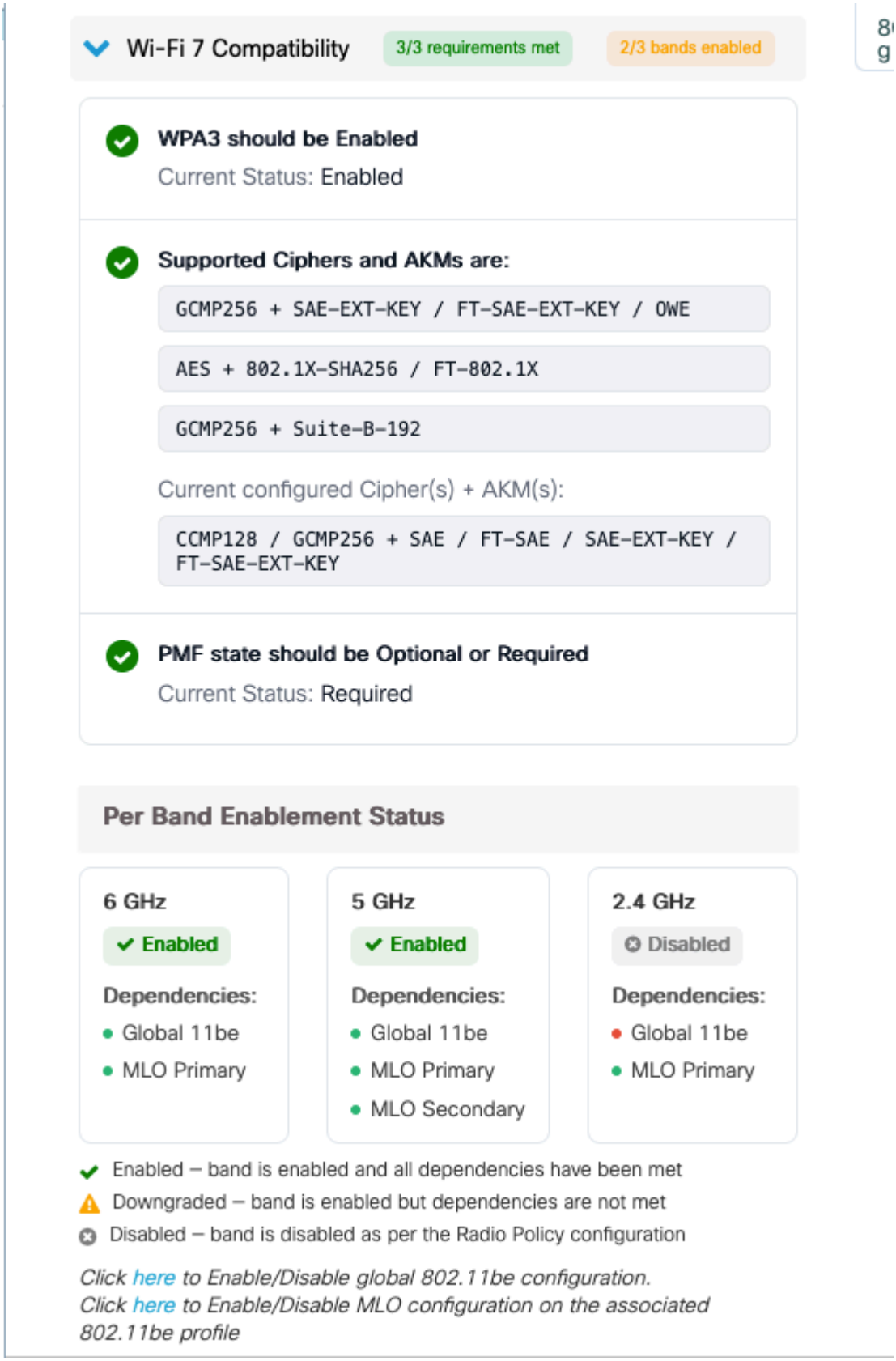
Dans l'onglet « Advanced » settings de chaque profil WLAN, un profil 802.11be correspondant est associé :



Comme nous pouvons le voir dans l'exemple, le « default-dot11be-profile » est attaché par défaut à n'importe quel profil WLAN.

Remarque : Si le Wi-Fi 7 n'est pas globalement activé sur le contrôleur, comme expliqué plus loin, le Wi-Fi 7 est désactivé pour tous les profils WLAN et les profils 802.11be ne sont pas appliqués.

17.18.2 présente un petit assistant dans la page WLAN edit qui vous aide à visualiser si votre WLAN est conforme à la norme Wi-Fi 7 et vous montre ce qui manque :



17.18.2 assistant de sécurité

Cisco IOS XE 17.18.3 et versions ultérieures

Cisco IOS 17.18.3 vous permet de configurer le chiffrement GCMP256 pour un SSID d'entreprise

802.1X, ce qui n'était pas possible dans les versions précédentes. Cela répond aux exigences de certains clients pour que les SSID d'entreprise Wi-Fi 7 proposent GCMP256 en plus des chiffrements AES128 et est conforme à la spécification WPA3 v3.4.

GCMP256 est automatiquement ajouté à votre configuration lors de la mise à niveau si votre SSID était compatible Wi-Fi 7 avant la mise à niveau, afin d'éviter qu'il ne se dégrade en un SSID Wi-Fi 6E si GCMP256 n'était pas activé après la mise à niveau vers 17.18.3.

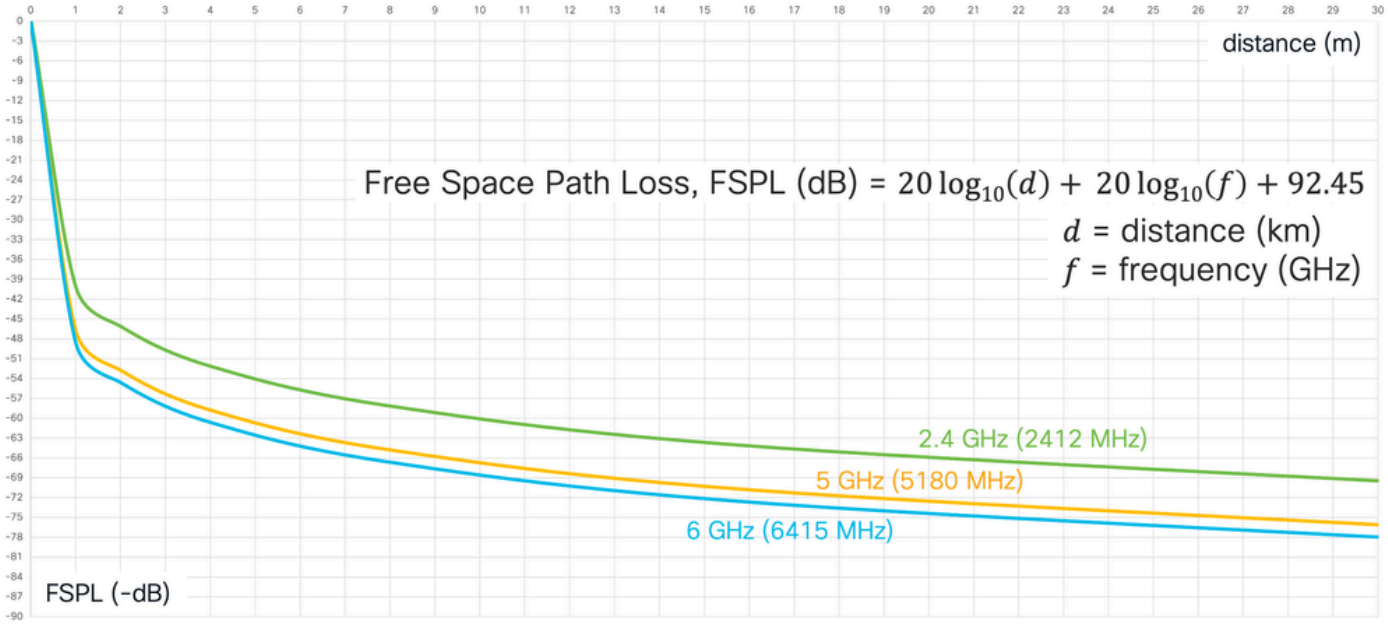
Considérations de conception radio pour une couverture 6 GHz

Sans tenter d'être un guide normatif complet pour les études de site, cette section décrit brièvement quelques considérations de base lors de la conception d'une couverture 6 GHz, en particulier lors de la migration d'une installation 2,4/5 GHz existante vers le Wi-Fi 6E ou 7.

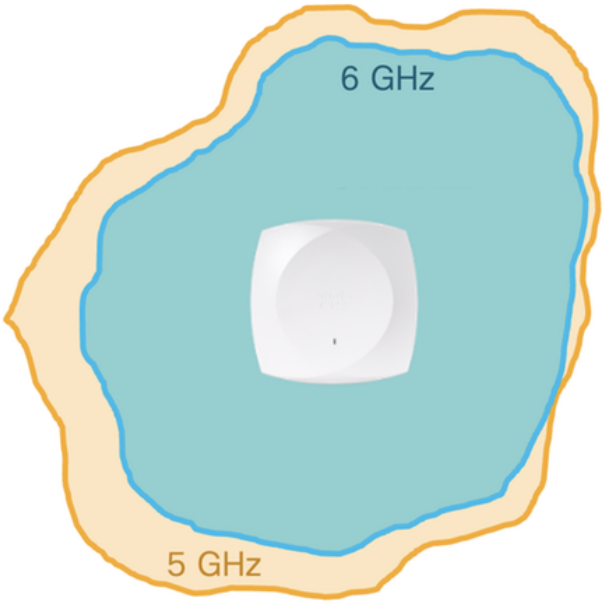
Comme pour tout nouveau déploiement Wi-Fi dans les bandes 2,4 GHz et/ou 5 GHz, un nouveau projet sans fil 6 GHz doit également inclure une étude de site 6 GHz dédiée.

Lorsque les points d'accès pré-Wi-Fi 6E/7 sont déjà positionnés pour répondre à des besoins de couverture 5 GHz spécifiques, dans certains cas, nous pouvons nous attendre à les remplacer par des points d'accès compatibles Wi-Fi 6E/7 et à obtenir une bonne couverture sur 6 GHz. Pour que cette approche fonctionne, nos points d'accès existants doivent déjà fournir une couverture 5 GHz adéquate pour les besoins prévus (données uniquement, voix, applications spécifiques, etc.) tout en fonctionnant avec au moins 3 à 4 niveaux de puissance de transmission inférieurs à leur maximum. Les points d’accès ont généralement de 7 à 8 niveaux de puissance, et chaque niveau de puissance successif divise par deux la puissance de transmission. Un point de fonctionnement confortable se trouve donc près du milieu de la plage de puissance de transmission autorisée.

Selon les calculs de perte en espace libre, les signaux de 6 GHz subissent une atténuation de 2 dB de plus que les signaux de 5 GHz. En outre, les signaux 6 GHz peuvent être plus affectés par les obstacles que leurs équivalents 5 GHz.



Lorsqu'un point d'accès Cisco augmente ou diminue sa puissance de transmission d'un niveau, il le fait dans un « saut » de 3 dB. Par exemple, un point d'accès passant du niveau de puissance 4, avec une puissance d'émission de 11 dBm, au niveau de puissance 3 augmente sa puissance d'émission à 14 dBm. Les valeurs de 11 dBm pour le niveau de puissance 4 et de 14 dBm pour le niveau de puissance 3 ne sont que des exemples génériques, car différents modèles et générations de points d'accès peuvent avoir des valeurs de puissance de transmission 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 similaire à celle de la radio 5 GHz en utilisant un niveau de puissance d'émission (3 dB) plus élevé.

Si une couverture 5 GHz adéquate est déjà fournie par la radio AP 5 GHz à des niveaux de puissance 3-4 inférieurs à son maximum, la radio 6 GHz correspondante pourrait donc être réglée à des niveaux de puissance 2-3 inférieurs à son maximum pour une couverture comparable. Cette hypothèse fonctionne à condition que les réglementations du pays de déploiement permettent aux radios 6 GHz et aux niveaux PIRE d'utiliser une puissance supérieure à 5 GHz. L'agrégation de canaux et le modèle de point d'accès spécifique peuvent également être pris en compte ; reportez-vous au tableau des paramètres d'alimentation de chaque modèle de point d'accès pour obtenir des informations spécifiques au pays.

En outre, si la radio 6 GHz fournit déjà une couverture adéquate à des niveaux de puissance 2-3 inférieurs à son maximum, elle pourrait encore augmenter de quelques niveaux dans des situations exceptionnelles, par exemple, pour contourner les trous de couverture temporaires et inattendus causés par une défaillance d'un point d'accès voisin, des obstacles inopinés, de nouvelles exigences 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 différentes générations de points d'accès sont installées de manière « salée et poivrée » (c'est-à-dire mélangées dans la même zone).

Alors qu'un contrôleur sans fil peut gérer les opérations (par exemple, l'attribution dynamique de canal, le contrôle de puissance de transmission, la distribution de cache PMK, etc.) pour un groupe de plusieurs modèles de point d'accès, les clients se déplaçant entre différentes normes et bandes de fréquences ne gèrent parfois pas ces transitions correctement et peuvent rencontrer des problèmes d'itinérance.

En outre, les points d'accès Wi-Fi 6E/7 prennent en charge les chiffrements GCMP256 pour WPA3, mais il n'en va pas toujours de même pour certains modèles de points d'accès Wi-Fi 6 et antérieurs. Pour les SSID de phrase de passe/WPA3-Personal et Enhanced Open/OWE qui nécessitent à la fois les algorithmes de chiffrement AES(CCMP128) et GCMP256, certains points d'accès Wi-Fi 6 (tels que les gammes 9105, 9115 et 9120, ainsi que les points d'accès 802.11ac Wave 2 x800) ne prennent pas en charge GCMP256 et ne peuvent offrir que le chiffrement AES(CCMP128) aux clients associés, notamment Clients compatibles Wi-Fi 6E/7. Si ces clients Wi-Fi 6E/7 doivent se déplacer entre des points d'accès Wi-Fi 6E/7 voisins qui prennent en charge GCMP256, ils doivent effectuer une nouvelle association, car la renégociation des chiffres entre AES(CCMP128) et GCMP256 n'est pas prise en charge pour l'itinérance transparente. En outre, il n'est généralement pas optimal d'avoir des points d'accès offrant des fonctionnalités différentes

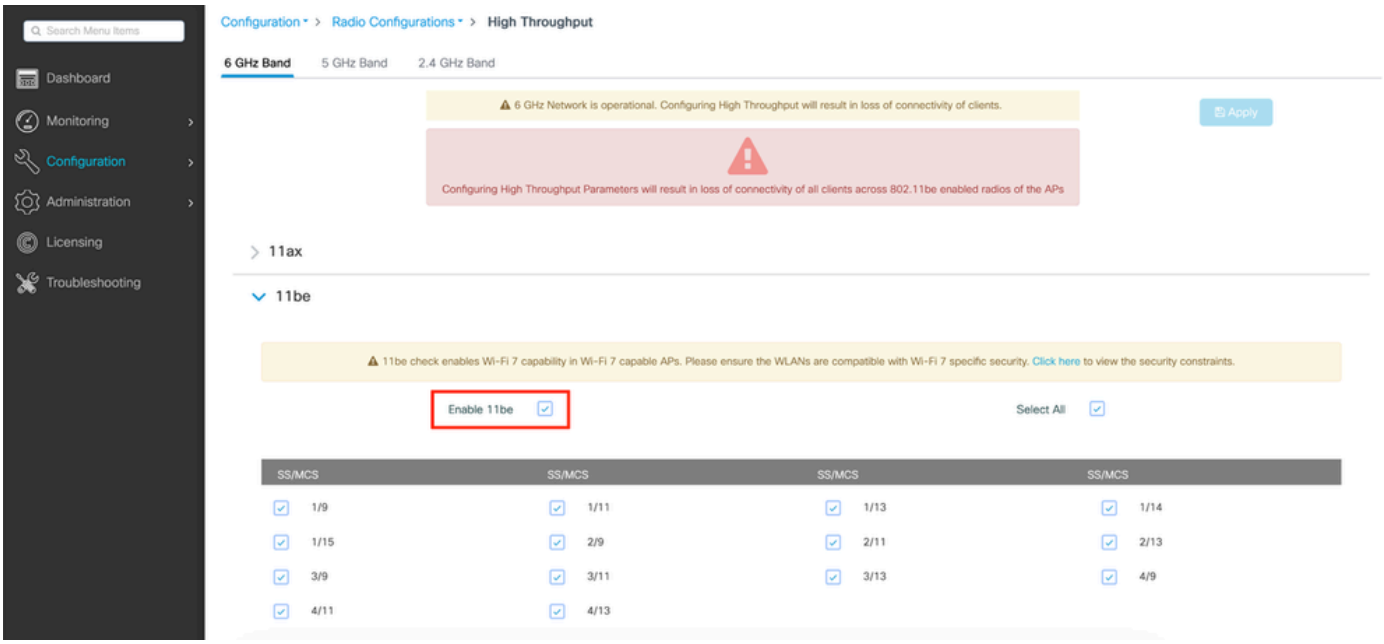
dans la même zone : un tel déploiement ne permet pas aux clients d'utiliser ces fonctionnalités de manière fiable lors de leur déplacement et peut entraîner une rémanence ou des déconnexions. Bien que ce scénario soit un cas d'angle, gardez à l'esprit que, avec les chiffrements GCMP256 configurés sur le WLAN, l'itinérance des clients Wi-Fi 6E/7 entre les points d'accès 9105/9115/9120 et 9130/9124/916x/917x peut être impossible, car la dernière série prend en charge GCMP256 et les premiers 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 sur d'autres bandes. C'est une autre raison de ne pas mélanger des points d'accès 6 GHz et des points d'accès non 6 GHz dans la même zone d'itinérance.

Activation globale du Wi-Fi 7

Activation globale de Wi-Fi 7 sur Cisco IOS XE

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



Vous pouvez également exécuter ces trois commandes via SSH ou 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

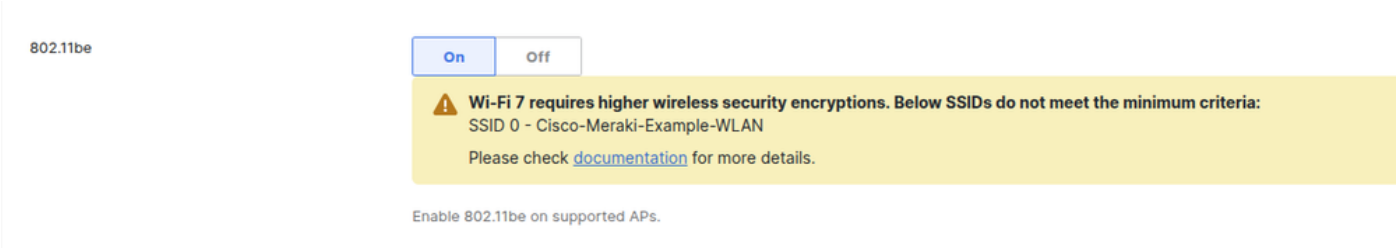
Lorsque vous ajoutez des points d'accès compatibles Wi-Fi 7 (par exemple, CW9178I ou CW9176I/D1) à un réseau de tableau de bord Cisco Meraki pour la première fois, la prise en charge du fonctionnement 802.11be est activée dans leur profil RF par défaut.
Pour l'activer, accédez à Wireless > Radio Settings, cliquez sur l'onglet RF Profile, et sélectionnez le profil assigné au point d'accès (le profil par défaut est 'Basic Indoor Profile' 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 d'alerte, comme illustré dans l'image suivante.

Alors que le tableau de bord permet d'enregistrer la configuration, le Wi-Fi 7 n'est pas activé sur les SSID marqués tant qu'ils ne sont pas conformes aux exigences du Wi-Fi 7. À l'heure actuelle, pour que le Wi-Fi 7 soit activé sur la version MR 31.1.x du micrologiciel et les versions ultérieures, tous les WLAN activés sur le réseau doivent répondre aux exigences de la spécification Wi-Fi 7 (ce comportement change dans une version ultérieure du micrologiciel MR 32.1.x).



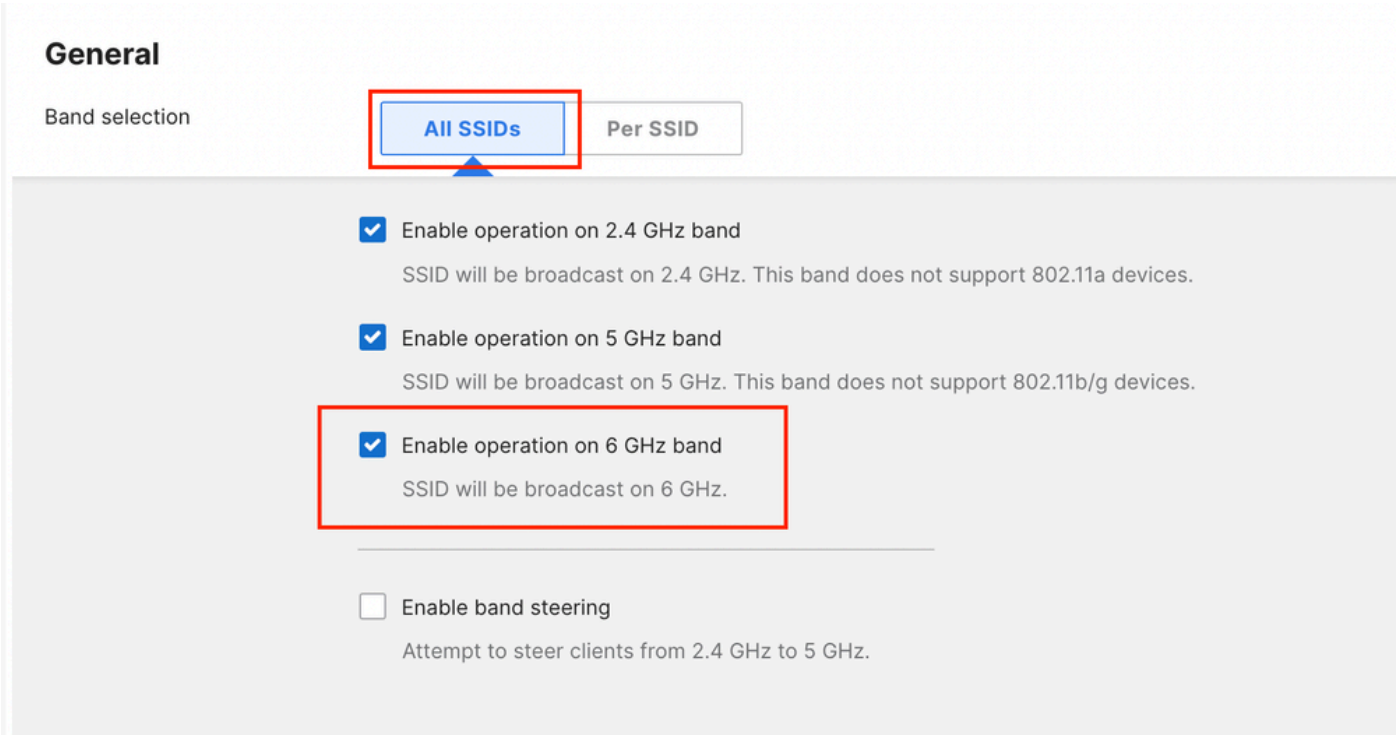
Une fois que la configuration du SSID répond aux critères minimum du Wi-Fi 7, la bannière disparaît.

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

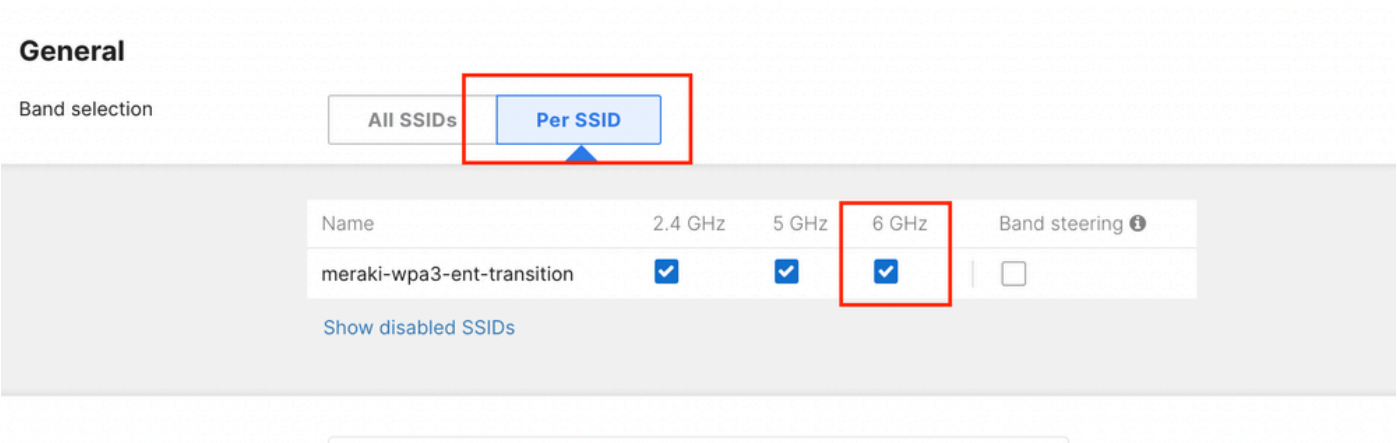
Cela peut être fait soit pour tous les SSID en masse ou par SSID individuel.

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 Cisco IOS XE

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

L'activation de votre SSID 802.1X pour 6 GHz nécessite l'activation de la prise en charge PMF, même si elle est facultative, 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, qui est annoncé sur la bande 5 GHz uniquement.

La prise en charge Wi-Fi 7 nécessite l'activation de Beacon Protection ; WPA2 802.1X (SHA1) peut rester sur le WLAN en tant qu'option de rétrocompatibilité.

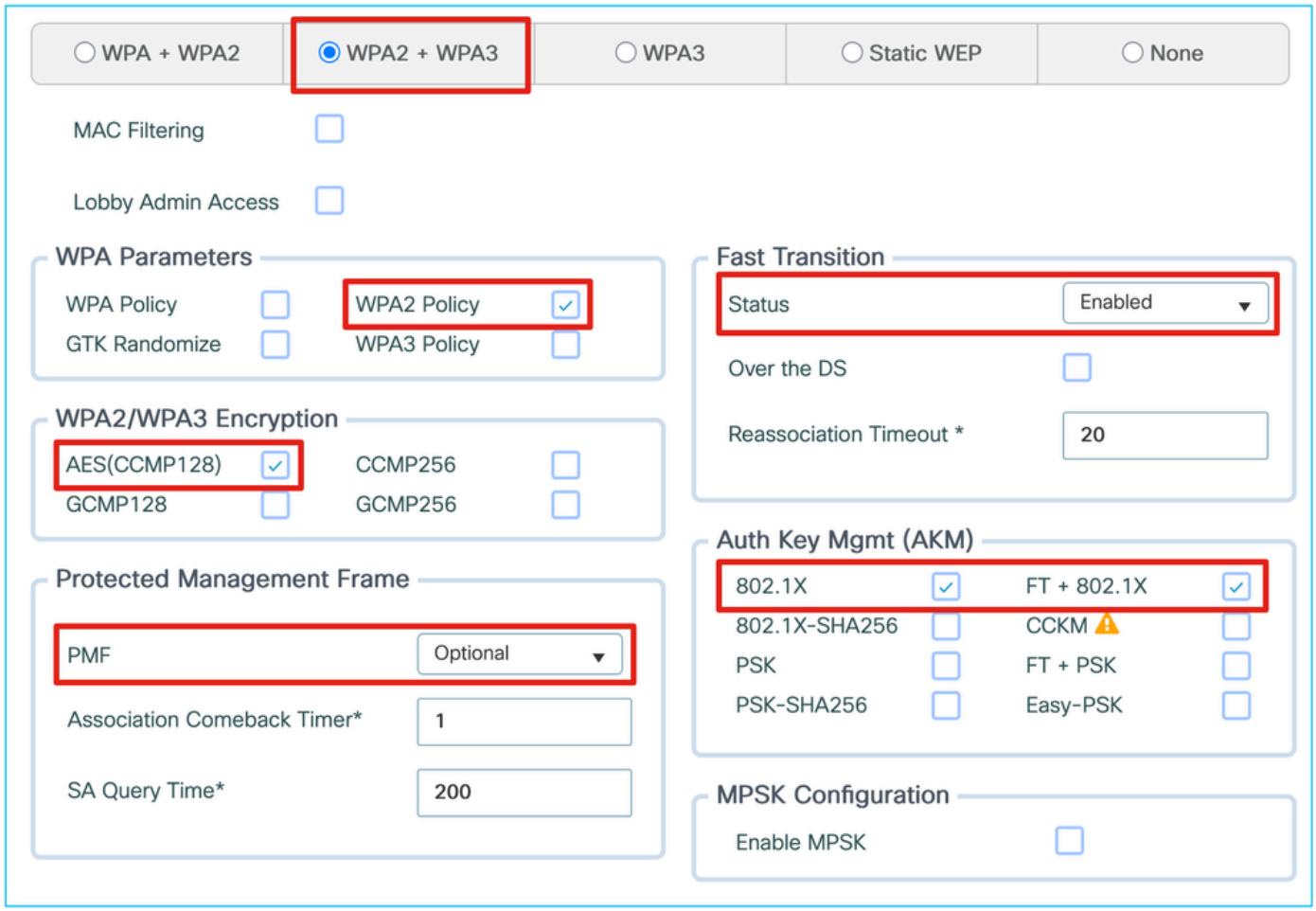
L'activation d'AES128 et de GCMP256, la définition de PMF comme facultatif et l'autorisation d'AKM WPA2 comme le standard 802.1X peuvent potentiellement prendre en charge de nombreux périphériques pour la compatibilité. Cependant, cela présente aux clients de nombreux choix. Si les clients annoncent la prise en charge de Wi-Fi 7 mais sélectionnent une configuration de sécurité qui n'est pas conforme à Wi-Fi 7, le point d'accès doit les rejeter, ce qui peut entraîner des problèmes de compatibilité.

Cependant, Cisco IOS XE 17.18.2 et les versions antérieures ne prennent pas en charge GCMP256 pour un SSID d'entreprise. La principale recommandation est de réserver ce cas d'utilisation aux environnements d'entreprise exécutant principalement des ordinateurs portables Windows 11.

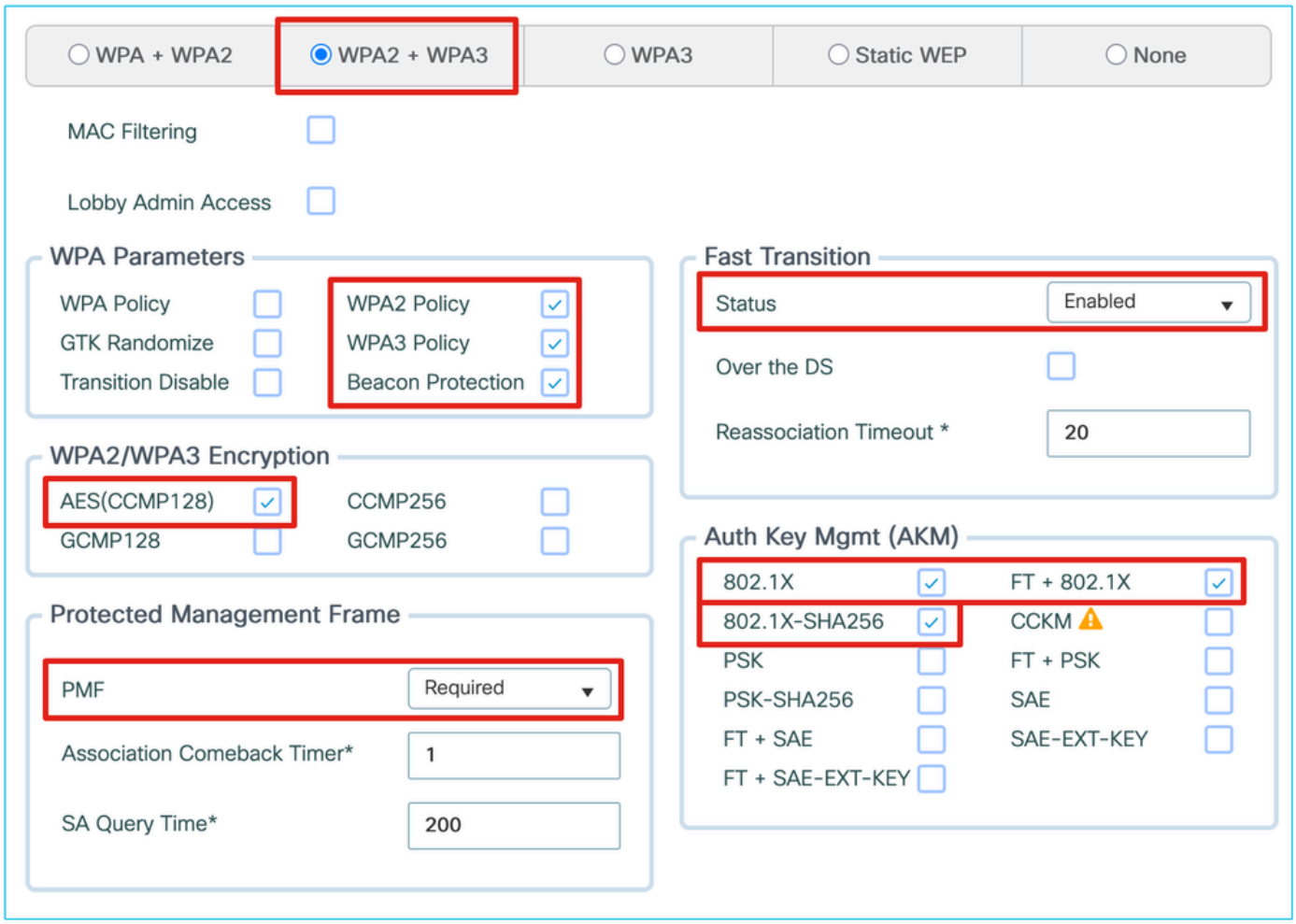
Lorsque vous exécutez 17.18.3 ou une version ultérieure, vous pouvez activer GCMP256 et prendre en charge correctement des catégories de périphériques mobiles plus larges (certains clients refusent de se connecter si le SSID prétend être Wi-Fi 7 mais prend uniquement en charge AES128).

Le tableau de bord Meraki Cloud prend en charge GCMP256 et l'exige pour activer le Wi-Fi 7 sur le SSID. Bien qu'un client Wi-Fi 7 ne puisse prendre en charge qu'AES128, un point d'accès Wi-Fi 7 certifié doit fournir AES128 et GCMP256.

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 partiel, comme illustré ci-dessous :

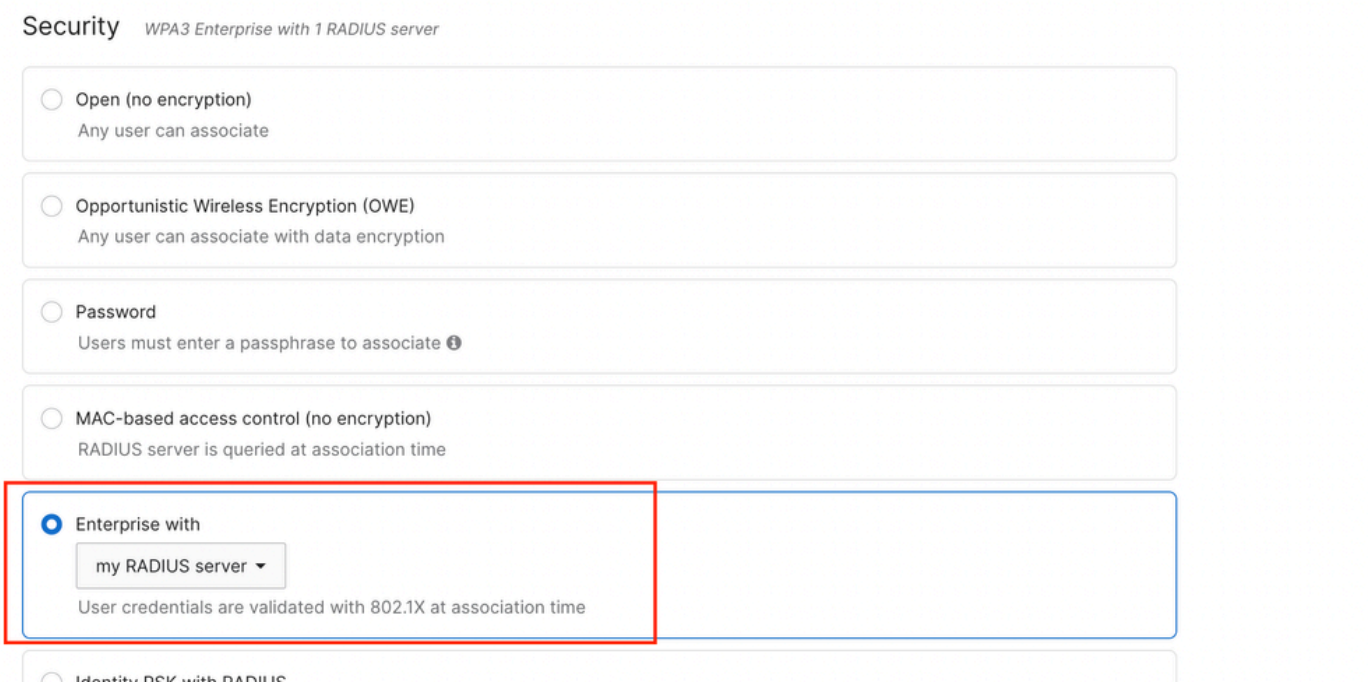


GCMP256 est manquant dans cette dernière capture d'écran pour une prise en charge Wi-Fi 7 correcte. Proposer ce nombre de chiffrements différents peut également entraîner des problèmes de compatibilité client. Par conséquent, envisagez de passer dès que possible à un WLAN WPA3 complet avec AES128+GCMP256.

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 :

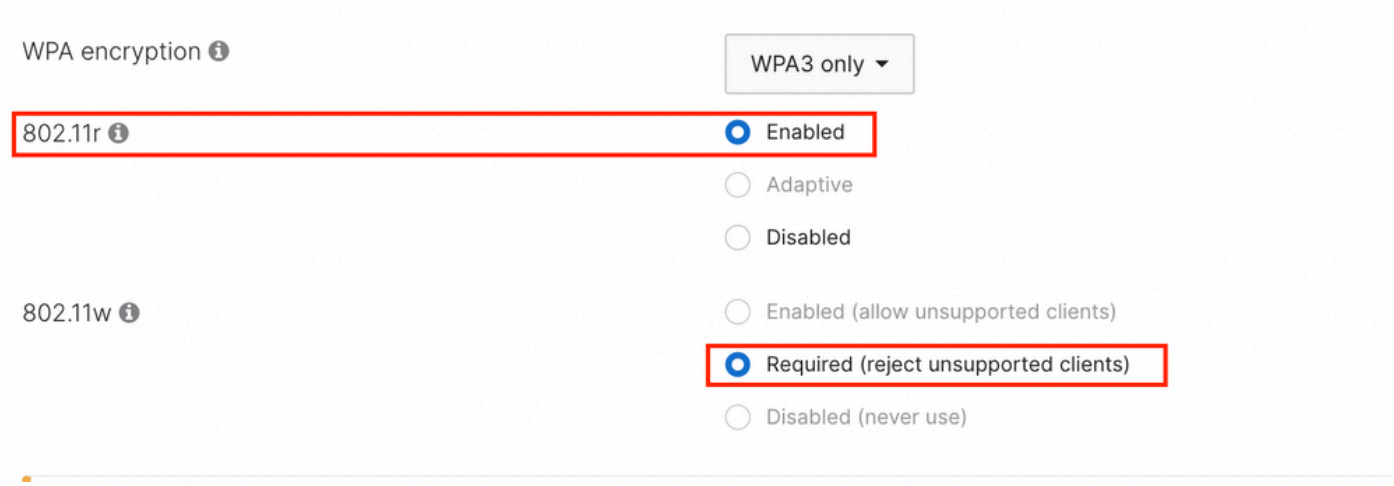
- « WPA3 only », qui utilise les mêmes chiffres que WPA2, mais nécessite la norme 802.11w (PMF).
- 'WPA3 192 bits', qui autorise uniquement la méthode EAP-TLS avec des chiffrements TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ou TLS_DHE_RSA_WITH_AES_256_GCM_SHA384. Les mêmes chiffrements doivent être configurés 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.

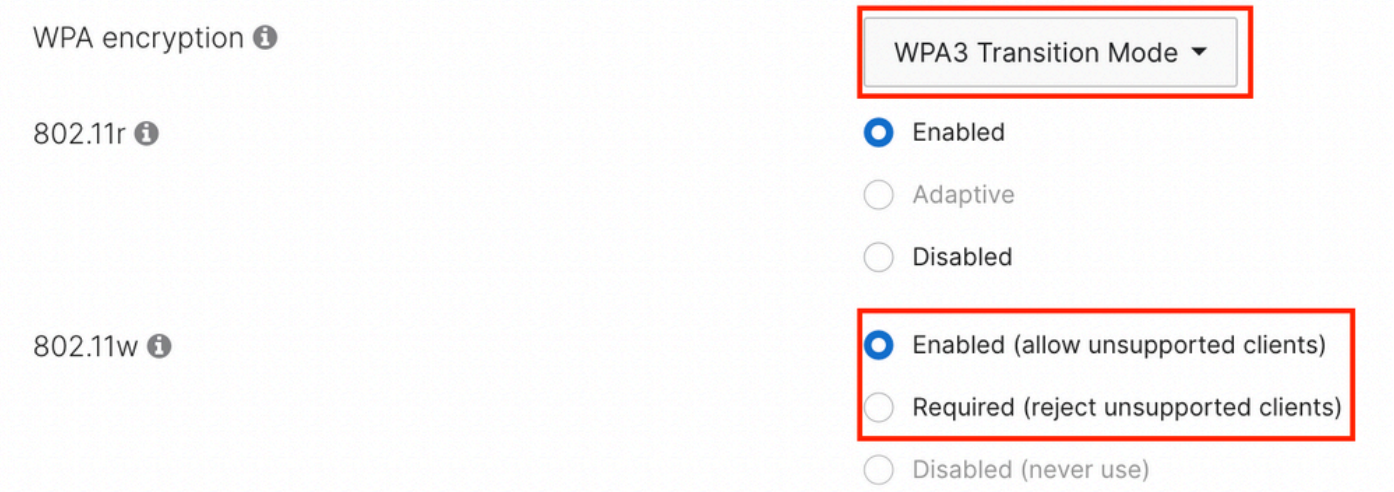
Dans la plupart des applications, il est recommandé d'activer la norme FT (802.11r), même si elle n'est pas obligatoire, pour limiter l'impact de la latence d'itinérance et de réauthentification lors de l'utilisation d'un serveur RADIUS externe.

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



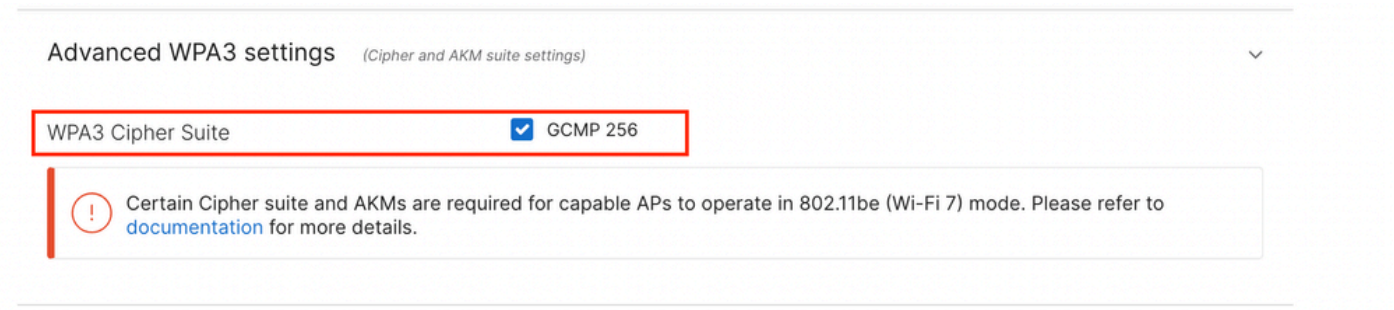
Lorsque vous sélectionnez le mode de transition WPA3, tous les clients capables d'utiliser le mode WPA3 utilisent par défaut le mode PMF. Tous les clients fonctionnant sur 6 GHz utilisent le WPA3.

Dans ce mode, vous pouvez choisir si les clients existants utilisant WPA2 doivent 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.

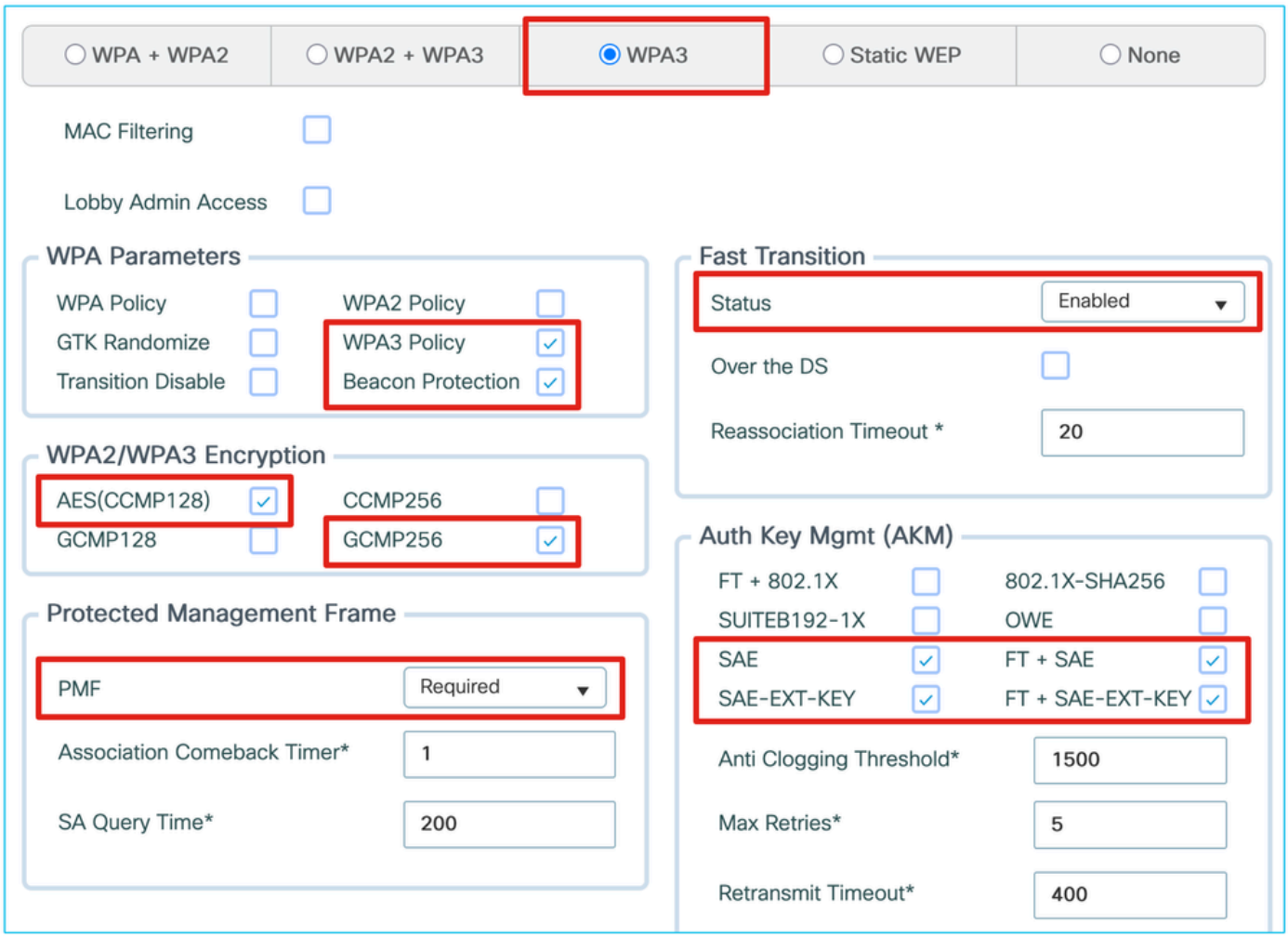
Cisco IOS XE 17.18.1 et versions ultérieures vous permettent de configurer WPA2-PSK en plus des quatre modules AKM SAE mentionnés ci-dessus. Cependant, cela peut présenter trop d'AKM pour des pilotes clients mal implémentés, même si la configuration est prise en charge par la norme. Nous vous recommandons de vérifier dans la pratique si vos clients WPA2 peuvent gérer tous les AKM activés sur le WLAN. Dans cette situation, les clients qui se connectent à l'aide de WPA2 ne peuvent pas utiliser MLO ou Wi-Fi 7, mais les clients qui se connectent avec SAE-EXT le peuvent. Le WLAN lui-même continue à annoncer les fonctionnalités Wi-Fi 7 et MLO.

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

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 plus gourmand en ressources et prend plus de temps que la connexion en quatre étapes WPA2 PSK.

Certains fabricants d'appareils, comme Apple, s'attendent à ce que FT soit activé lorsque SAE est utilisé, et leurs appareils peuvent refuser de se connecter si FT n'est pas disponible.

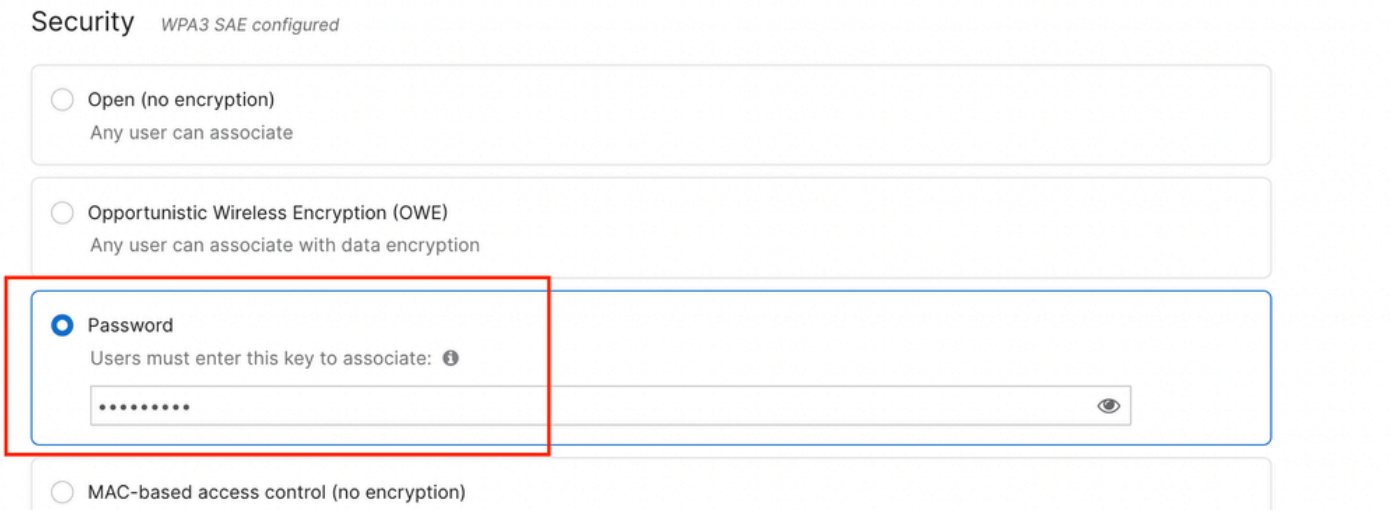
Configuration WPA3-SAE sur Cisco IOS XE



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 utiliser ce dernier AKM, de sorte que ce problème ne se produit pas.

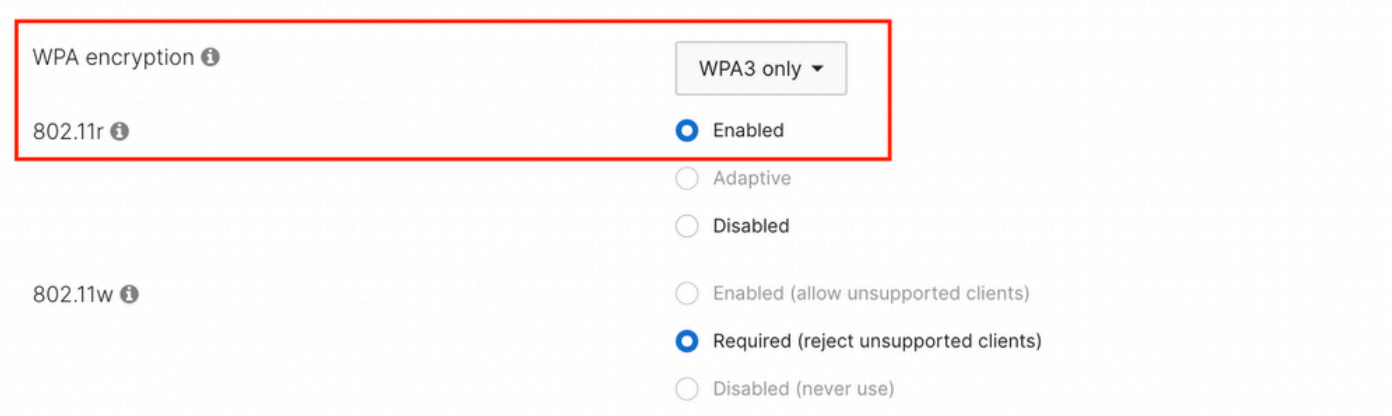
Bien que l'utilisation d'un WLAN PSK-only hérité en plus d'un WLAN WPA3-only augmente le nombre total de SSID, cela nous permet de maintenir une compatibilité maximale sur un SSID. Nous pouvons également désactiver les fonctionnalités avancées qui pourraient affecter la compatibilité, ce qui peut aider dans de nombreux scénarios IoT, tout en offrant des fonctionnalités et des performances maximales aux périphériques plus récents via l'autre SSID. Il peut s'agir d'une approche privilégiée si vous avez déployé des périphériques IoT plus anciens ou plus sensibles. Si vous ne disposez pas de périphériques IoT, l'utilisation d'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



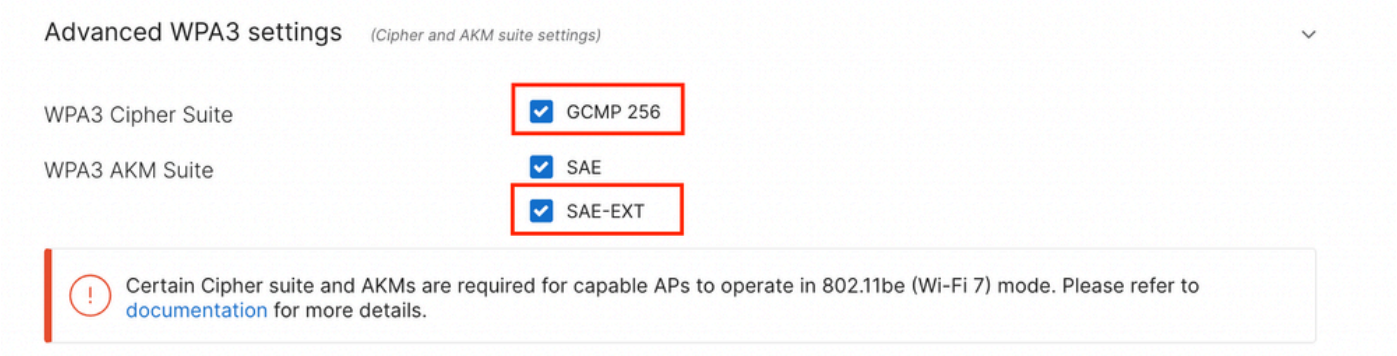
Jusqu'au micrologiciel MR 30.x, le seul type WPA pris en charge est « WPA3 uniquement » et le tableau de bord ne vous permet pas de sélectionner une autre méthode.

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



Pour permettre le fonctionnement du Wi-Fi 7, les suites de chiffrement GCMP 256 et 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 de différentes sortes. En général, ils ne nécessitent aucune identification 802.1X ou phrase de passe pour se connecter et peuvent inclure une page d'accueil ou un portail qui nécessite des informations d'identification ou un code. Ce problème est généralement traité avec un SSID ouvert et une solution de portail invité locale 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 approche prudente consiste à dédier les réseaux invités à la bande 5 GHz et au Wi-Fi 6 au mieux. La bande 6 GHz reste ainsi réservée aux périphériques d'entreprise, réduit la complexité et offre une compatibilité maximale, mais n'offre pas de performances Wi-Fi 6E/7.

Bien que l'option Enhanced Open soit une méthode de sécurité puissante qui assure la confidentialité tout en conservant l'expérience « ouverte » (les utilisateurs finaux n'ont pas besoin de saisir des informations d'identification 802.1X ou une phrase de passe), la prise en charge des terminaux reste limitée. Certains clients ne le prennent toujours pas en charge et, même lorsqu'ils le font, l'expérience n'est pas toujours fluide : un périphérique peut indiquer que la connexion n'est pas sécurisée lorsqu'elle l'est, ou qu'elle est protégée par une phrase de passe, même si OWE ne requiert aucune phrase de passe. Étant donné qu'un réseau invité est censé fonctionner avec tous

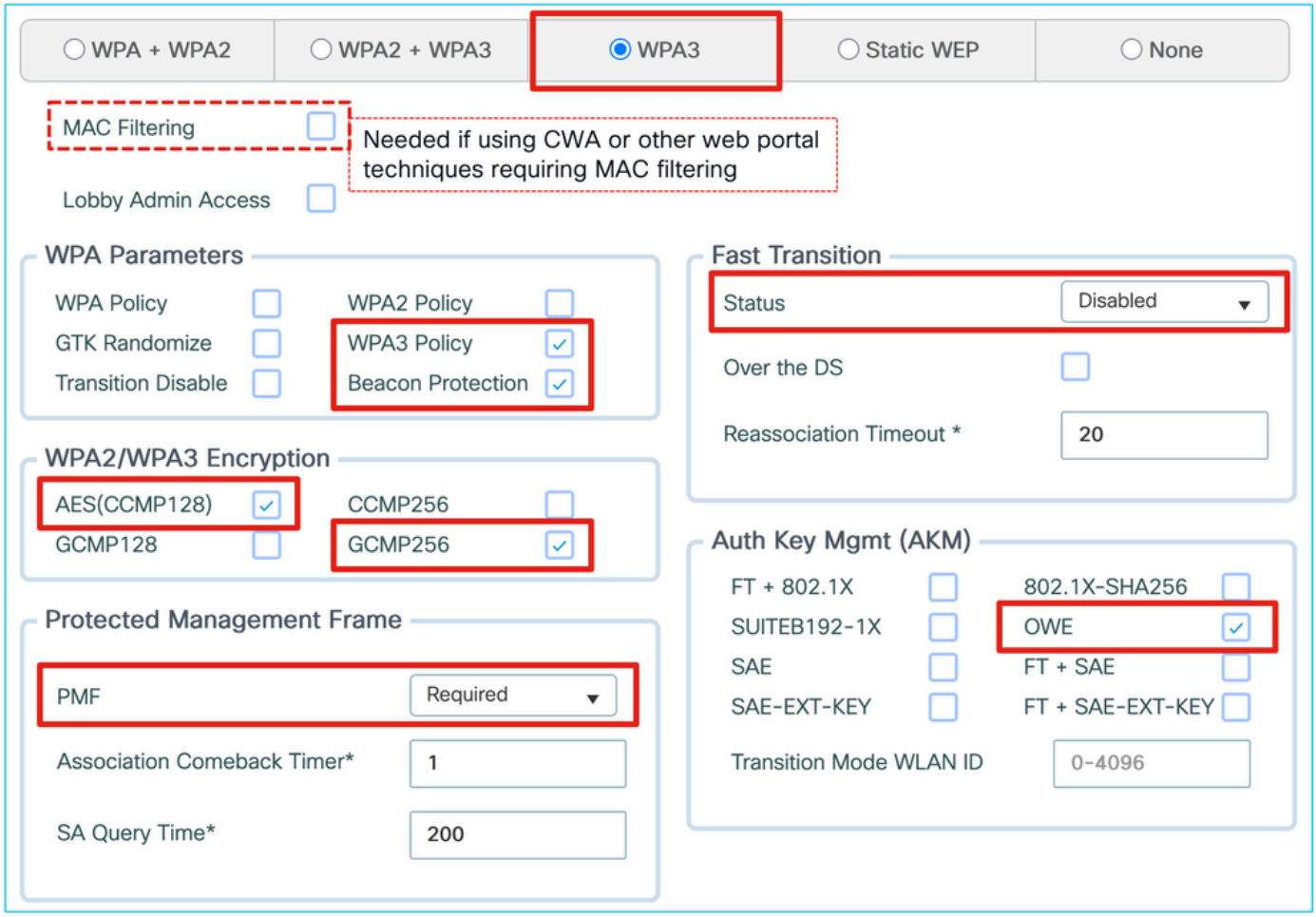
les périphériques invités non gérés, il peut être trop tôt pour fournir uniquement un SSID ouvert amélioré. Nous vous recommandons de fournir les deux options via des SSID distincts : un SSID ouvert sur 5 GHz et un SSID compatible OWE sur 5 et 6 GHz, les deux utilisant le même portail captif si nécessaire. Les deux réseaux doivent utiliser des noms SSID différents car, conformément à la norme 802.11, le nom SSID identifie tous les BSS sur lesquels un client peut se déplacer en toute transparence. L'utilisation du même nom SSID avec des paramètres de sécurité différents est donc non valide et dangereux. Le mode de transition n'est pas pris en charge sur les réseaux Wi-Fi 6E, 6 GHz (même si le logiciel peut toujours l'autoriser) ou Wi-Fi 7. Il n'est donc pas recommandé. Toutes les techniques de redirection de portail (authentification Web interne ou externe, authentification Web centrale, etc.) sont toujours prises en charge avec OWE.

Configuration OWE sur Cisco IOS XE

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

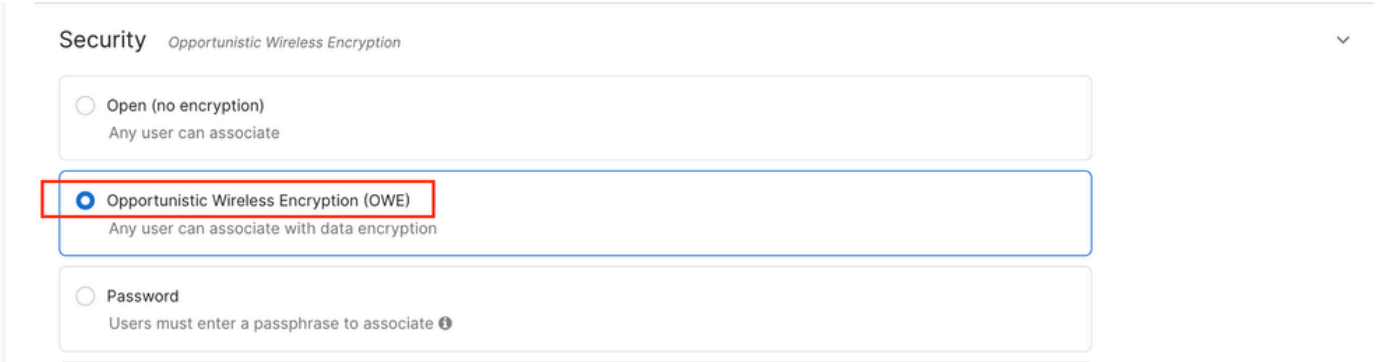
À l'heure actuelle, de nombreux clients mobiles offrent une prise en charge partielle ou peu conviviale d'OWE/Enhanced Open. Testez avec vos clients pour mesurer l'assistance.

Le fait d'avoir deux WLAN invités distincts (un ouvert et un ouvert OWE/amélioré) peut constituer une solution, surtout si vous conservez le WLAN invité sécurisé OWE sur 6 GHz uniquement et le WLAN entièrement ouvert sur 5 GHz uniquement. Cependant, vous devez séparer les deux WLAN invités en sous-réseaux différents ; Dans le cas contraire, le WLAN ouvert annule l'avantage du WLAN sécurisé en fournissant un accès non chiffré au même sous-réseau.



Configuration OWE sur le tableau de bord Cisco Meraki

Comme avec Cisco IOS XE, nous vous recommandons de créer un SSID invité distinct avec Enhanced Open / OWE qui fonctionne sur 6 GHz.
Configurez-le sur le tableau de bord Cisco Meraki sous Wireless > Access Control en sélectionnant « Opportunistic Wireless Encryption (OWE) » comme méthode de sécurité.

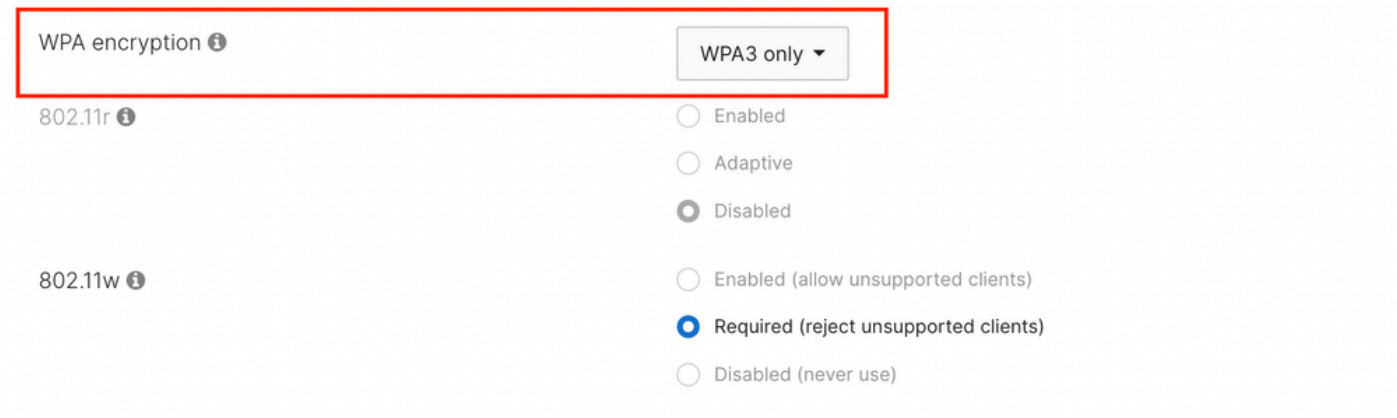


Lors de l'exécution du micrologiciel jusqu'à MR31, le seul type WPA pris en charge est « WPA3 uniquement » et le tableau de bord ne vous permet pas de sélectionner une autre méthode.

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

Notez que l'étiquette « WPA3 only » est trompeuse, 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 une future version MR 32.1.x.



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

Le GCMP256 peut être activé 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

Cette fonctionnalité corrige une vulnérabilité dans laquelle un pirate peut transmettre des balises qui empruntent l'identité du point d'accès légitime et modifier les champs pour modifier la sécurité ou d'autres paramètres pour des clients déjà associés. La protection de balise ajoute à la balise un élément d'information (Management MIC) qui agit comme une signature, prouvant que le point d'accès légitime a envoyé la balise et qu'elle n'a pas été falsifiée. 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. Les clients qui ne prennent pas en charge l'élément d'information supplémentaire (c'est-à-dire les clients non-Wi-Fi 7) doivent simplement l'ignorer, et il ne provoque normalement pas de problèmes de compatibilité, sauf si un client a un pilote mal programmé.

Après 17.18, les éléments de protection de balise sont activés automatiquement si votre WLAN est compatible Wi-Fi 7, que vous activiez ou non la case à cocher de protection de balise.

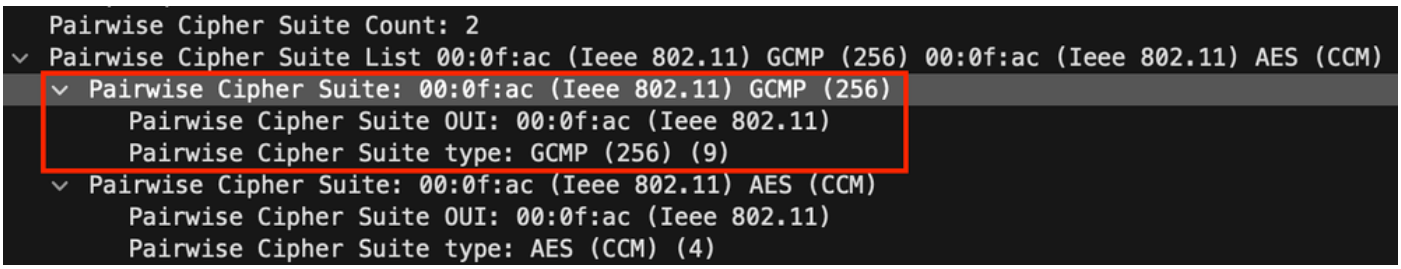
Cette capture d'écran présente un exemple du contenu de l'élément d'information MIC de gestion :



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 spécifiques liées à l'AKM SUITE-B 802.1X. Bien que certains des premiers clients Wi-Fi 7 sur le marché prétendent prendre en charge le Wi-Fi 7, ils ne mettent pas toujours en oeuvre le cryptage GCMP256. Cela peut devenir un problème lorsque les points d'accès Wi-Fi 7 appliquent la norme et empêchent les clients sans prise en charge GCMP256 appropriée de se connecter.

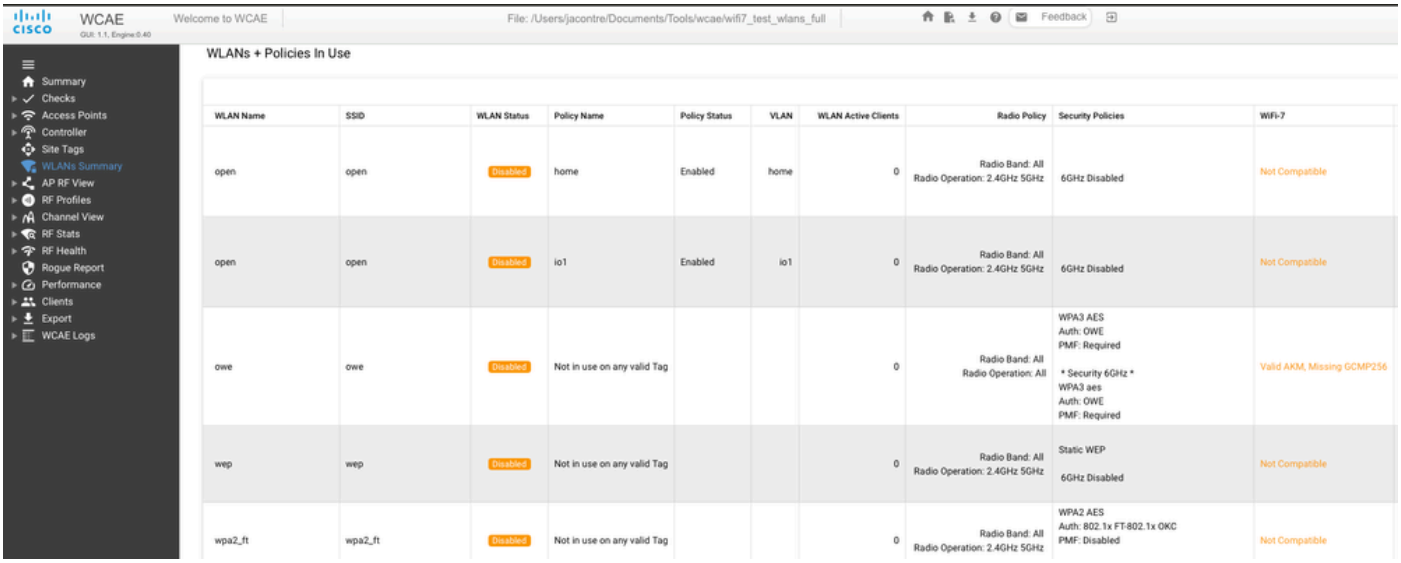
Lorsque le protocole GCMP256 est activé, le Robuste Security Network Element (RSNE) des trames de balise pour le WLAN annonce la capacité dans la liste Pairwise Chipher Suite List, comme indiqué ici.



Dépannage et vérification

La dernière version de Wireless Configuration Analyzer Express dispose d'un contrôle de préparation Wi-Fi 7 qui évalue votre configuration 9800 par rapport à toutes les exigences Wi-Fi 7 mentionnées précédemment.

Si vous ne savez toujours pas si votre configuration est compatible Wi-Fi 7, le WCAE identifie ce qui ne va pas.



Liste de vérification du dépannage

- L'interface utilisateur Web (dans R32 ou 17.18.2 et versions ultérieures) vous indique si votre WLAN est conforme à la norme Wi-Fi 7. Utilisez ce document pour vérifier que les paramètres de sécurité sont conformes.
- Assurez-vous que le client prend en charge le Wi-Fi 7. Un ordinateur portable Windows requiert au moins Windows 11 24H2. Assurez-vous que les pilotes de la carte sans fil sont à jour.
- La commande « netsh wlan show drivers » sous Windows est très utile pour répertorier les capacités de la carte sans fil et vérifier son état.
- Pour un ordinateur portable, accédez aux paramètres de la carte et vérifiez que le mode 11be est activé sur la carte. De nombreux adaptateurs livrés initialement avec le 11be sont désactivés et fonctionnent comme 11ax pour des raisons de compatibilité.
- En cas de doute, effectuez une capture de paquets en direct pour vérifier que :
    - Le point d'accès diffuse un élément d'information EHT dans la balise. Cela peut être capturé avec n'importe quel analyseur ; il n'a pas besoin de prendre en charge le Wi-Fi 7, car la balise est envoyée à des débits hérités.
    - Si l'AP diffuse correctement l'EHT, le client doit envoyer l'élément EHT dans sa demande d'association. Si ce n'est pas le cas, le client ne considère pas que les

paramètres de sécurité AP conformes à la norme Wi-Fi 7 ou 802.11be sont désactivés dans les propriétés de la carte.

Références

- Guide de configuration et de cryptage WPA3
- 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.