Migre para 6 GHz e Wi-Fi 7 com o Cisco Wireless

Contents

- Introdução
  - Guia de design do CX
- Por que 6 GHz e Wi-Fi 7
- Requisitos básicos para operações de 6 GHz e Wi-Fi 7
  - Requisitos de banda de 6 GHz
  - Requisitos de Wi-Fi 7
    - IOS XE 17.18.1 e posterior
    - IOS XE 17.15.3 e versões posteriores 17.15.x
- Considerações de projeto de rádio para cobertura de 6 GHz
  - Comportamentos de roaming entre APs pré-Wi-Fi 6E/7 e Wi-Fi 6E/7
- Habilitando o Wi-Fi 7 globalmente
  - Ativação global do Wi-Fi 7 no IOS XE
  - Ativação global do Wi-Fi 7 no painel do Cisco Meraki
- Casos de uso
  - Redes 802.1X / WPA3-Enterprise
    - Configuração WPA3-Enterprise no IOS XE
    - Configuração WPA3-Enterprise no painel do Cisco Meraki
  - Senha / WPA3-Personal / Redes da IoT
    - Configuração WPA3-SAE e WPA2-Personal no IOS XE
    - Configuração WPA3-SAE no painel do Cisco Meraki
  - Redes abertas / aprimoradas abertas / OWE / Convidado
    - Configuração OWE no IOS XE
    - Configuração OWE no painel do Cisco Meraki
- WPA3 adicional e opções relacionadas
  - Proteção de beacon
  - GCMP256
- Solucionar problemas e verificar
- Referências

Introdução

Este documento descreve as diretrizes de design e configuração para otimizar o desempenho do Wi-Fi 7 e aproveitar totalmente o espectro de 6 GHz.

Guia de design do CX

Os guias de design do CX são escritos por especialistas do Cisco CX em colaboração com engenheiros de outros departamentos e revisados por especialistas da Cisco; os guias se baseiam nas práticas recomendadas da Cisco, bem como no conhecimento e na experiência adquiridos com inúmeras implementações de clientes ao longo de muitos anos. As redes projetadas e configuradas de acordo com as recomendações neste documento ajudam a evitar armadilhas comuns e a melhorar a operação da rede.

Por que 6 GHz e Wi-Fi 7

A banda de 6 GHz tornou-se disponível para operações de WLAN em 2020 e era necessária para a certificação Wi-Fi 6E. Enquanto o Wi-Fi 6 opera nas bandas de 2,4 GHz e 5 GHz, o Wi-Fi 6E utiliza o mesmo padrão IEEE 802.11ax, mas estende sua funcionalidade para a banda de 6 GHz, desde que requisitos específicos sejam atendidos.
A nova certificação Wi-Fi 7 é baseada no padrão IEEE 802.11be e suporta operações nas faixas de 2,4 GHz, 5 GHz e 6 GHz. O Wi-Fi 7 também apresenta novos recursos e aprimoramentos em comparação com certificações anteriores.

O suporte à banda de 6 GHz e/ou Wi-Fi 7 vem com requisitos específicos, muitas vezes necessitando de novas configurações e designs de RF, especialmente quando comparado às práticas estabelecidas para as bandas de 2,4 GHz e 5 GHz com Wi-Fi 6.

Por exemplo, assim como o uso de segurança WEP desatualizada impede a adoção de padrões 802.11 além de 802.11a/b/g, padrões mais recentes impõem pré-requisitos de segurança ainda mais rigorosos para incentivar a implantação de redes mais seguras.

Por outro lado, a introdução da banda de 6 GHz oferece acesso a frequências mais claras, melhor desempenho e suporte para novos casos de uso. Ele também permite uma implementação mais uniforme dos aplicativos existentes, como conferência de voz e vídeo.

Requisitos básicos para operações de 6 GHz e Wi-Fi 7

Estes são os requisitos de segurança escritos nas certificações para operações de 6 GHz e Wi-Fi 7.

Requisitos de banda de 6 GHz

A banda de 6 GHz permite apenas WPA3 ou Enhanced Open WLANs, o que significa uma destas

opções de segurança:

- WPA3-Enterprise com autenticação 802.1X
- WPA3 - Autenticação Simultânea de Iguais (SAE - Simultaneous Authentication of Equals) (também conhecida como WPA3-Personal) com senha. SAE-FT (SAE com Transição Rápida) é outro AKM possível e é realmente recomendado para uso desde que o handshake SAE não é trivial, e FT permite pular essa troca mais longa.
- Aberto aprimorado com criptografia sem fio oportunista (OWE)

Embora, de acordo com as especificações do WPA3 v3.4 (Seção 11.2), o modo de transição Aberto Aprimorado não seja suportado com 6 GHz, muitos fornecedores (incluindo a Cisco até o IOS® XE 17.18) ainda não aplicam isso. Portanto, é tecnicamente possível configurar, por exemplo, um SSID aberto em 5 GHz, um SSID aberto aprimorado correspondente em 5 e 6 GHz, ambos com o Modo de transição ativado, e tudo isso sem estar em conformidade com as especificações padrão. No entanto, em tal cenário, deve-se esperar que, em vez disso, configuremos um SSID Aberto Aprimorado sem o modo de transição e disponível somente em 6 GHz (os clientes que suportam 6 GHz normalmente suportam também o Aberto Aprimorado), enquanto mantemos nosso SSID Aberto regular em 5 GHz, também sem o modo de transição.

Não há novos requisitos específicos de cifras ou algoritmos para WPA3-Enterprise, exceto a aplicação do 802.11w/Protected Management Frame (PMF). Muitos fornecedores, incluindo a Cisco, consideram o 802.1X-SHA256 ou "FT + 802.1X" (que na verdade é 802.1X com SHA256 e Fast Transition no topo) apenas compatível com WPA3 e o 802.1X simples (que usa SHA1) é considerado parte do WPA2, portanto, não se encaixa/é suportado para 6 GHz.

Requisitos de Wi-Fi 7

Com a certificação Wi-Fi 7 do padrão 802.11be, a Wi-Fi Alliance aumentou os requisitos de segurança. Alguns deles permitem o uso de taxas de dados 802.11be e melhorias de protocolo, enquanto outros são específicos para suportar Multi-Link Operations (MLO), permitindo que dispositivos compatíveis (clientes e/ou APs) usem várias bandas de frequência enquanto mantêm a mesma associação.

Em geral, o Wi-Fi 7 exige um destes tipos de segurança:

- WPA3-Empresa com AES(CCMP128) e 802.1X-SHA256 ou FT + 802.1X (que ainda usa SHA256, mesmo que não seja explícito em sua nomeação). Isso não representa uma mudança em relação aos pré-requisitos de segurança WPA3 existentes anteriormente para a banda de 6 GHz.
- WPA3-Personal com GCMP256 e SAE-EXT-KEY e/ou FT + SAE-EXT-KEY (AKM 24 ou 25). O Wi-Fi 6E exige WPA3 SAE e/ou FT + SAE com AES regular (CCMP128) e nenhuma utilização estendida adicional de chaves; isso significa que uma nova cifra foi introduzida especificamente para o Wi-Fi 7.
- Enhanced Open / OWE com GCMP256. Embora o AES(CCMP128) ainda possa ser configurado no mesmo SSID, os clientes que usam o AES 128 não suportam Wi-Fi 7. Antes do Wi-Fi 7, a maioria dos clientes que suportam o Enhanced Open usavam apenas o AES 128, portanto, esse é um requisito novo e mais forte. Quanto ao suporte para 6 GHz, não é

permitido o modo de transição.

Independentemente do tipo de segurança selecionado, são necessários Protected Management Frames (PMF) e Beacon Protection para suportar o Wi-Fi 7 na WLAN.

Como o Wi-Fi 7 ainda é uma certificação recente no momento da elaboração deste documento, com uma versão o mais cedo possível, muitos fornecedores não aplicaram todos esses requisitos de segurança desde o início.

Mais recentemente, a Cisco vem aplicando progressivamente as opções de configuração para estar em conformidade com a certificação Wi-Fi 7. Estes são os comportamentos específicos da versão:

IOS XE 17.18.1 e posterior

O IOS XE 17.18 e versões posteriores somente anunciam uma determinada WLAN como Wi-Fi 7 habilitada se a WLAN tiver parâmetros de segurança que correspondam aos requisitos do Wi-Fi 7 (proteção de beacon, PMF e o AKM correto conforme descrito anteriormente, dependendo do tipo de WLAN, bem como da presença de GCMP256 para atingir o MLO do Wi-Fi 7, no caso de OWE ou SAE-EXT). A presença do AES128 é tolerada no SSID, mas quando usado, ele apenas fornece Wi-Fi 6E e não Wi-Fi 7 MLO.

Um cliente pode se associar como Wi-Fi 7 e atingir taxas de dados Wi-Fi 7 independentemente do método de segurança que usar (desde que ainda seja suportado pela WLAN). No entanto, o cliente só pode se associar como capaz de MLO (em uma ou mais bandas) se respeitar os requisitos rigorosos de segurança Wi-Fi 7, ou se for rejeitado.

IOS XE 17.15.3 e versões posteriores 17.15.x

Nesta filial, todas as WLANs são transmitidas como SSIDs Wi-Fi 7, desde que o Wi-Fi 7 seja ativado globalmente e independentemente das configurações de segurança.

Um cliente pode se associar como compatível com Wi-Fi 7 e atingir taxas de dados Wi-Fi 7, independentemente do método de segurança usado, desde que ainda seja suportado pela WLAN. No entanto, o cliente só pode se associar como capaz de MLO (em uma ou mais bandas) se respeitar os requisitos rigorosos de segurança Wi-Fi 7, ou se for rejeitado.

Isso poderia causar problemas quando alguns dos primeiros clientes do Wi-Fi 7 não puderem suportar cifras mais seguras, como o GCMP256, tentarem se associar como Wi-Fi 7 MLO capaz a uma WLAN, cujas configurações de segurança não correspondem aos requisitos do Wi-Fi 7. Nesse caso, o cliente é rejeitado devido às configurações de segurança inválidas (ainda podem ser configuradas na WLAN).

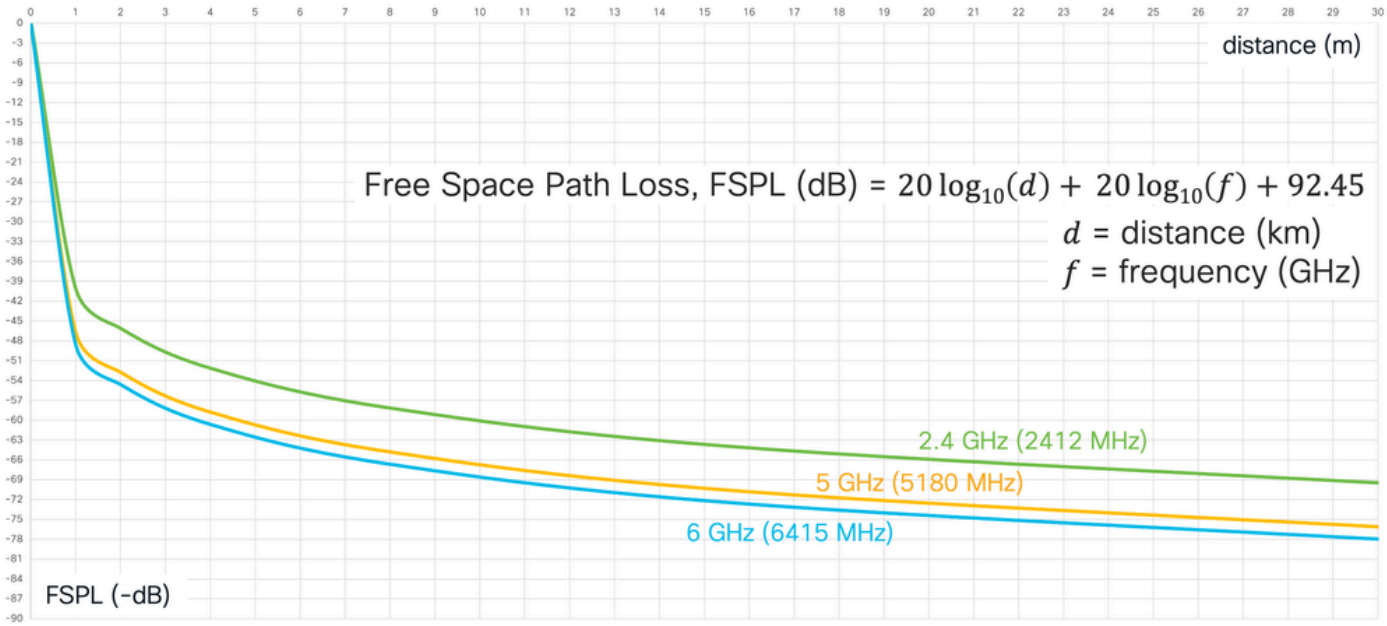
Considerações de projeto de rádio para cobertura de 6 GHz

Sem querer tornar-se um guia prescritivo completo sobre as pesquisas do local, esta seção descreve brevemente algumas considerações básicas ao projetar a cobertura de 6 GHz,

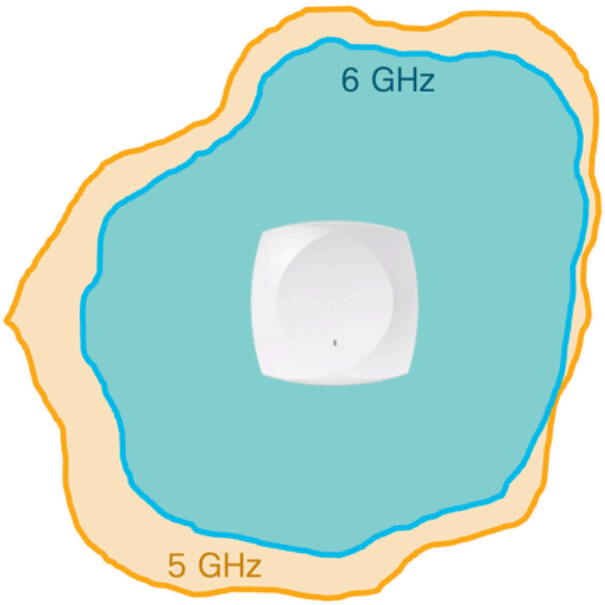
especialmente se já houver uma instalação existente para 2,4/5 GHz que gostaríamos de migrar para Wi-Fi 6E ou 7.
Como em qualquer nova implantação de Wi-Fi a que estivemos acostumados em 2,4 e/ou 5 GHz, um novo projeto sem fio em 6 GHz deve incluir também uma pesquisa de site dedicada correspondente em 6 GHz.

Quando os APs pré-Wi-Fi 6E/7 já estão posicionados para cobertura e necessidades específicas de 5 GHz, em alguns casos, podemos esperar substituí-los por APs com capacidade para Wi-Fi 6E/7 e ainda obter boa cobertura em 6 GHz. Para que essa teoria funcione, nossos APs existentes já devem fornecer cobertura correta de 5 GHz para as necessidades pretendidas (somente dados, voz, aplicativos específicos e assim por diante) e, ao mesmo tempo, já devem ter pelo menos 3 a 4 níveis de potência de transmissão abaixo do limite máximo. Os APs normalmente têm de 7 a 8 níveis de potência, e cada nível de potência divide a potência de transmissão pela metade. Isso significa que um ponto confortável é quando os APs estão usando o meio de sua faixa de potência de transmissão permitida.

De acordo com cálculos de perda de espaço livre, os sinais de 6 GHz são atenuados em 2 dB por mais de 5 GHz. Além disso, os sinais de 6 GHz também podem ser mais afetados por obstáculos do que seus equivalentes de 5 GHz.



Quando um AP Cisco aumenta/diminui sua potência de transmissão em um nível, ele faz isso por um "salto" de 3 dB. Um AP que passa de um nível de potência de 4, com uma potência de transmissão de 11 dBm, por exemplo, para um nível de potência de 3, aumenta sua potência de transmissão para 14 dBm (11 dBm para o nível de potência 4 e 14 dBm para o nível de potência 3 são apenas um exemplo genérico, pois modelos/gerações diferentes de APs podem ter valores de potência de transmissão ligeiramente diferentes em dBm para o mesmo número de nível de potência).



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.

Se um AP pré-Wi-Fi 6E/7 já fornece uma boa cobertura a 5 GHz no nível de potência 4, por exemplo, um AP Wi-Fi 6E/7 mais recente com padrões de rádio de 5 GHz semelhantes poderia substituir esse AP anterior sem qualquer impacto significativo na rede de 5 GHz existente.

Além disso, o rádio de 6 GHz do novo AP Wi-Fi 6E/7 poderia fornecer uma cobertura de 6 GHz semelhante à de 5 GHz apenas por estar em um nível de potência de transmissão (portanto 3 dB) mais alto.

Se 5 GHz já estiver coberto corretamente com o rádio de 5 GHz do AP em níveis de potência de 3 a 4 abaixo do seu máximo, o rádio de 6 GHz correspondente poderia ser definido em níveis de potência de 2 a 3 abaixo do seu máximo para cobertura comparável.

Além disso, se o rádio de 6 GHz já fornecer cobertura correta a 2-3 níveis de potência inferiores ao máximo, ele ainda poderá excepcionalmente ir até alguns níveis superiores, por exemplo, para tentar contornar brechas temporárias de cobertura inesperadas (falha de um AP vizinho, obstáculos não anunciados, novas necessidades de RF e assim por diante).

Comportamentos de roaming entre APs pré-Wi-Fi 6E/7 e Wi-Fi 6E/7

A implantação de APs que suportam diferentes padrões e/ou faixas de frequência na mesma área de cobertura sempre não foi uma prática recomendada, especialmente se essas diferentes gerações de APs forem instaladas de forma "salina e pimenta" (ou seja, misturadas na mesma zona).

Embora um controlador sem fio possa lidar com operações (por exemplo, atribuição dinâmica de canal, controle de energia de transmissão, distribuição de cache PMK e assim por diante) de um grupo de vários modelos de AP, clientes que se movem entre diferentes padrões e até mesmo bandas de frequência diferentes nem sempre são capazes de lidar com isso corretamente e provavelmente podem enfrentar problemas de roaming, por exemplo.

Além disso, devido aos padrões mais recentes, os APs Wi-Fi 6E/7 suportam cifras GCMP256

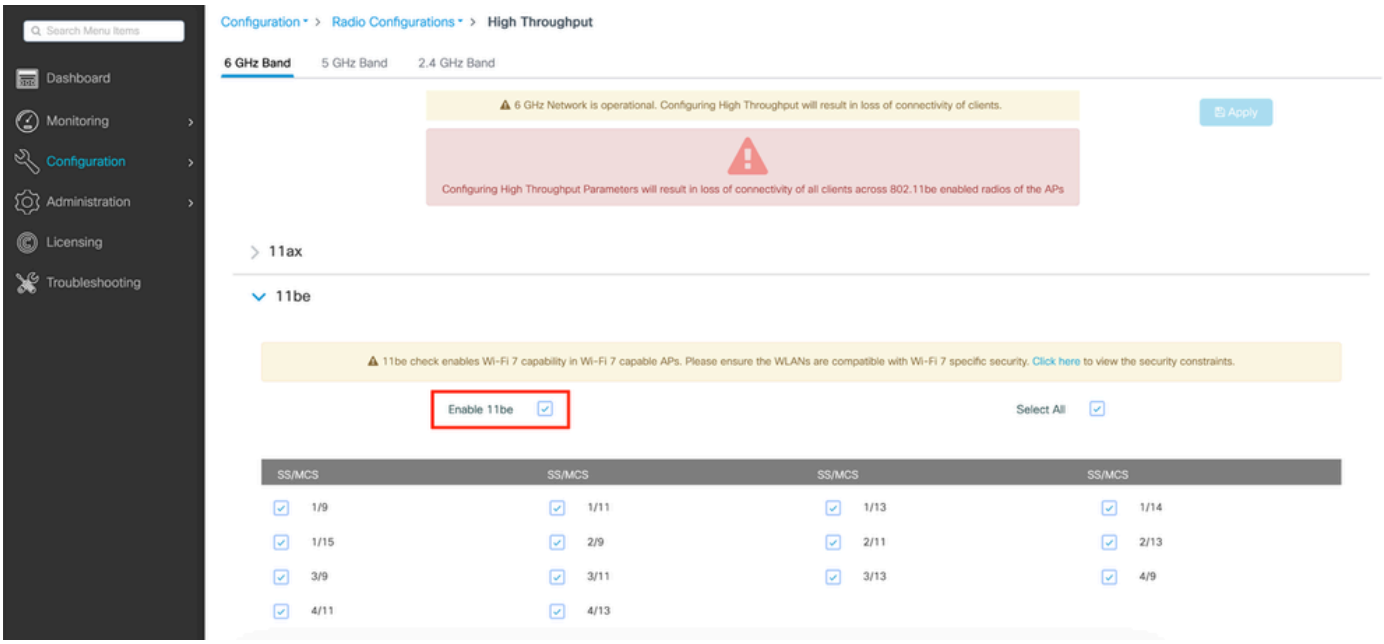
para WPA3. O mesmo nem sempre pode ser verdade para alguns APs Wi-Fi 6 e modelos anteriores. Para senhas/WPA3-Personal e SSIDs Open/OWE aprimorados, que exigem a configuração de cifras AES(CCMP128) e GCMP256, determinadas cifras Wi-Fi 6 (como as séries 9105, 9115 e 9120) não oferecem suporte a GCMP256 e podem oferecer cifras AES(CCMP128) somente para clientes associados, incluindo as habilitadas para Wi-Fi 6E/7. Se esses clientes Wi-Fi 6E/7 precisassem fazer roaming de/para APs Wi-Fi 6E/7 vizinhos que suportassem GCMP256, eles teriam que passar por uma associação totalmente nova, já que a renegociação de cifras entre AES(CCMP128) e GCMP256 não é suportada para roaming transparente. Além disso, em geral, não é ideal ter APs que ofereçam diferentes recursos na mesma área: essa implantação não permite que os clientes usem esses recursos de forma confiável durante a movimentação e pode levar à adesão ou desconexões.
Embora esse cenário deva representar um caso de vértice, queremos ainda ter em mente que, com as cifras GCMP256 configuradas na WLAN, o roaming de clientes Wi-Fi 6E/7 entre APs 9105/9115/9120 e APs 9130/9124/916x/917x não pode ser possível, já que essas últimas séries suportam GCMP256 e as primeiras não.

Larguras de canal de 40 MHz ou mais em 6 GHz também podem causar adesão para clientes com capacidade de 6 GHz, que podem se recusar a se reassociar a outras bandas. Isso deve ser mais um motivo para não misturar APs com capacidade de 6 GHz e APs sem capacidade de 6 GHz na mesma área de roaming.

Habilitando o Wi-Fi 7 globalmente

Ativação global do Wi-Fi 7 no IOS XE

Ao instalar ou atualizar para uma versão do IOS XE que suporta Wi-Fi 7, por padrão, o suporte para Wi-Fi 7 é desabilitado globalmente.
Para ativá-lo, precisamos navegar no menu de configuração Alta taxa de transferência de cada banda de 2,4/5/6 GHz e marcar a caixa para ativar o 11be.



Outra opção também poderia ser executar essas três linhas de comando via SSH/console, no modo de configuração de terminal:

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

Como mencionado na nota de aviso, ao tentar modificar essas configurações, a alteração do status do suporte a 802.11be resulta em uma breve perda de conectividade para todos os clientes em rádios de APs Wi-Fi 7. Se você quiser executar o MLO, que significa que os clientes se conectam a várias bandas ao mesmo tempo, você precisará ativar o 11be em todas as bandas às quais deseja que o cliente se conecte. Não é necessário habilitar todas as faixas, mas é recomendado apenas para desempenho.

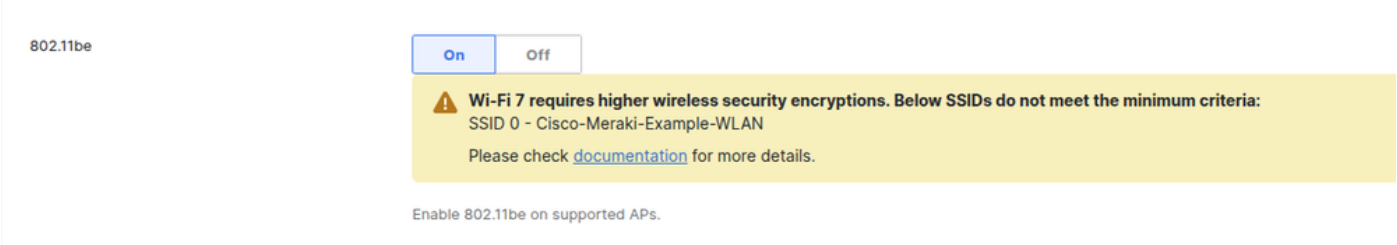
Ativação global do Wi-Fi 7 no painel do Cisco Meraki

Ao adicionar APs com capacidade para Wi-Fi 7 (por exemplo, CW9178I, CW9176I/D1) a uma rede do painel Cisco Meraki pela primeira vez, o suporte para a operação 802.11be está no perfil de RF padrão.
Para ativá-lo, precisamos navegar em Wireless > Radio Settings, clicar na guia RF Profile e selecionar o perfil atribuído ao AP (padrão: 'Basic Indoor Profile' para APs internos).

Na seção Geral, habilite 802.11be (on) como mostrado nesta captura de tela:

Se uma ou mais WLANs estiverem configuradas com configurações de segurança mais fracas do que as exigidas pela especificação Wi-Fi 7, o Painel exibirá um banner alertando os usuários, como mostrado a seguir.

Embora o Painel permita que a configuração seja salva, o Wi-Fi 7 não é habilitado nos SSIDs sinalizados até que a conformidade com os requisitos do Wi-Fi 7 seja garantida.
A partir deste momento, todas as WLANs habilitadas na rede devem atender aos requisitos da especificação Wi-Fi 7 para serem habilitadas na versão MR 31.1.x do firmware e posterior (esse comportamento muda em uma versão futura do MR 32.1.x do firmware).



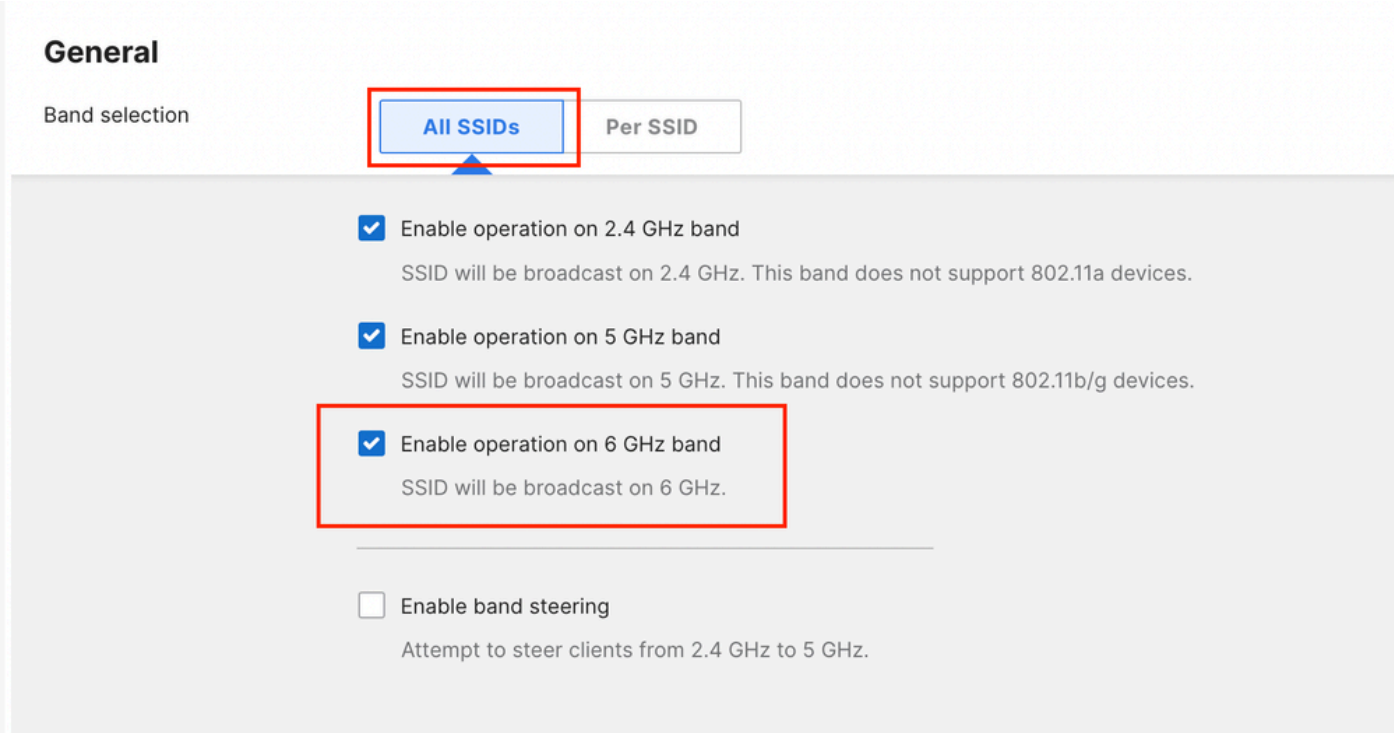
Quando a configuração do SSID atender aos critérios mínimos de Wi-Fi 7, o banner desaparece.

No mesmo perfil de RF, certifique-se de habilitar a operação de 6 GHz nos APs.

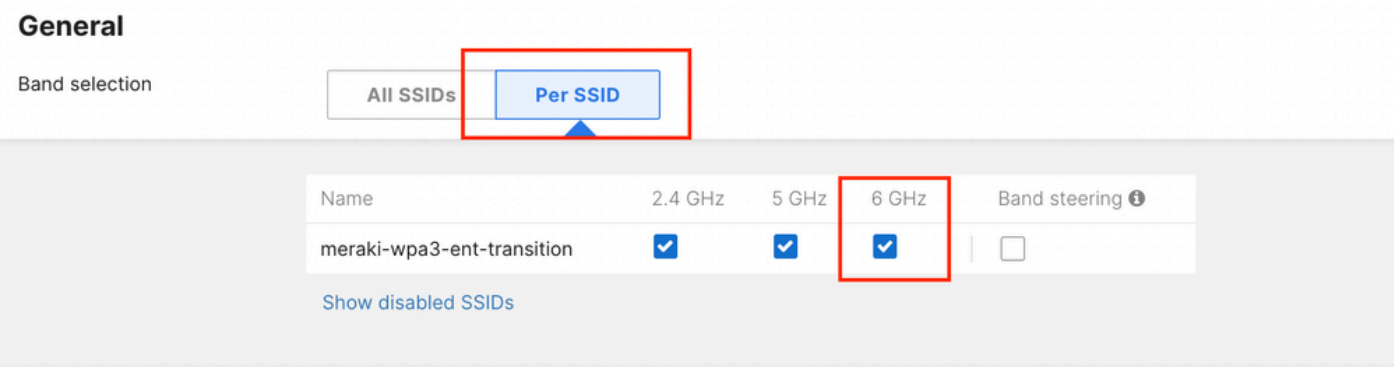
Isso pode ser feito para todos os SSIDs em massa ou por SSID individual.

Observe que a direção de banda está disponível apenas entre 2,4 e 5 GHz.

Exemplo de habilitação de 6 GHz para todos os SSIDs.



Exemplo de habilitação de 6 GHz para um único SSID.



Casos de uso

Redes 802.1X / WPA3-Enterprise

Configuração WPA3-Enterprise no IOS XE

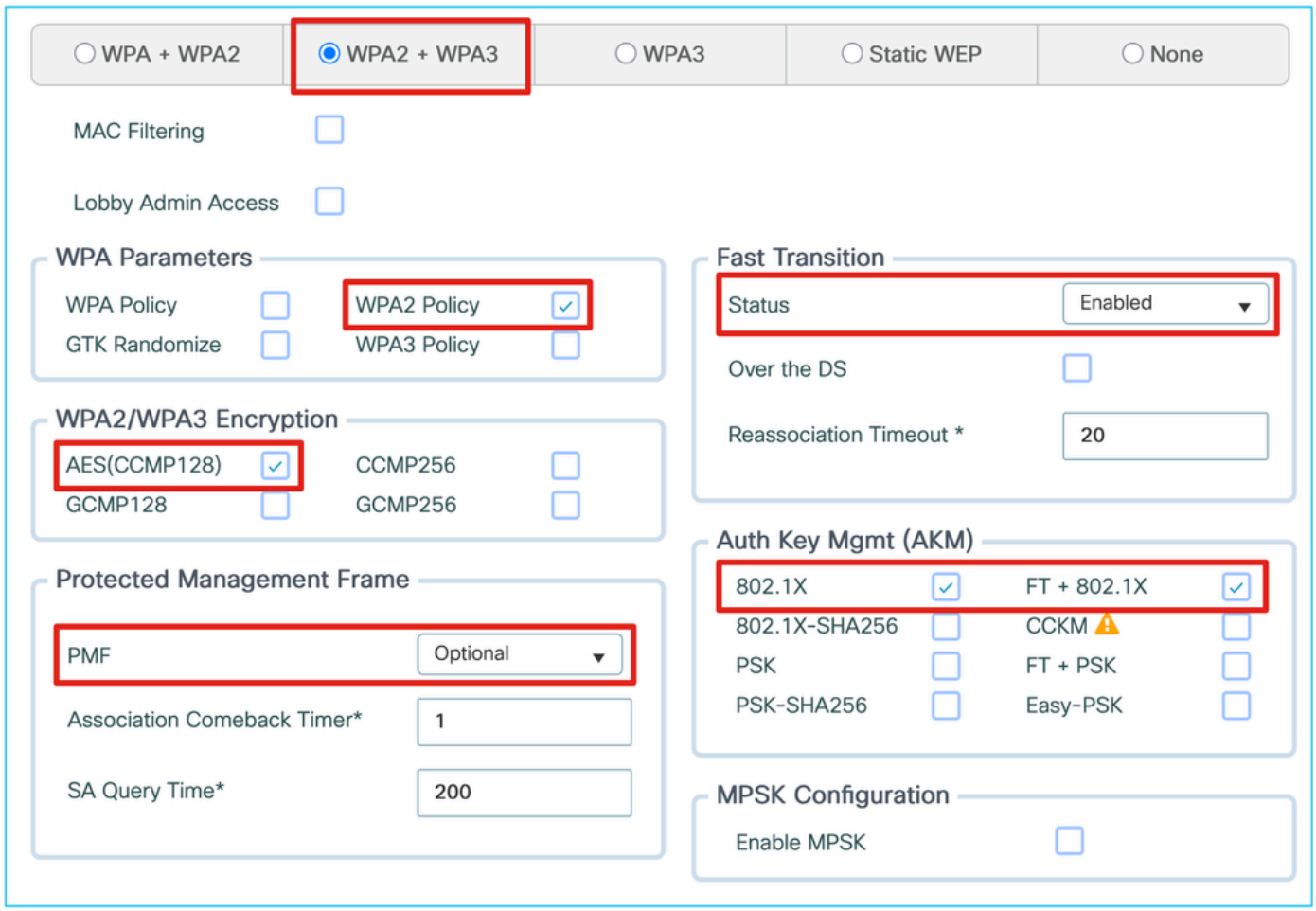
As WLANs corporativas baseadas em WPA2/3 com autenticação 802.1X são as mais fáceis de

migrar para 6 GHz e/ou Wi-Fi 7.

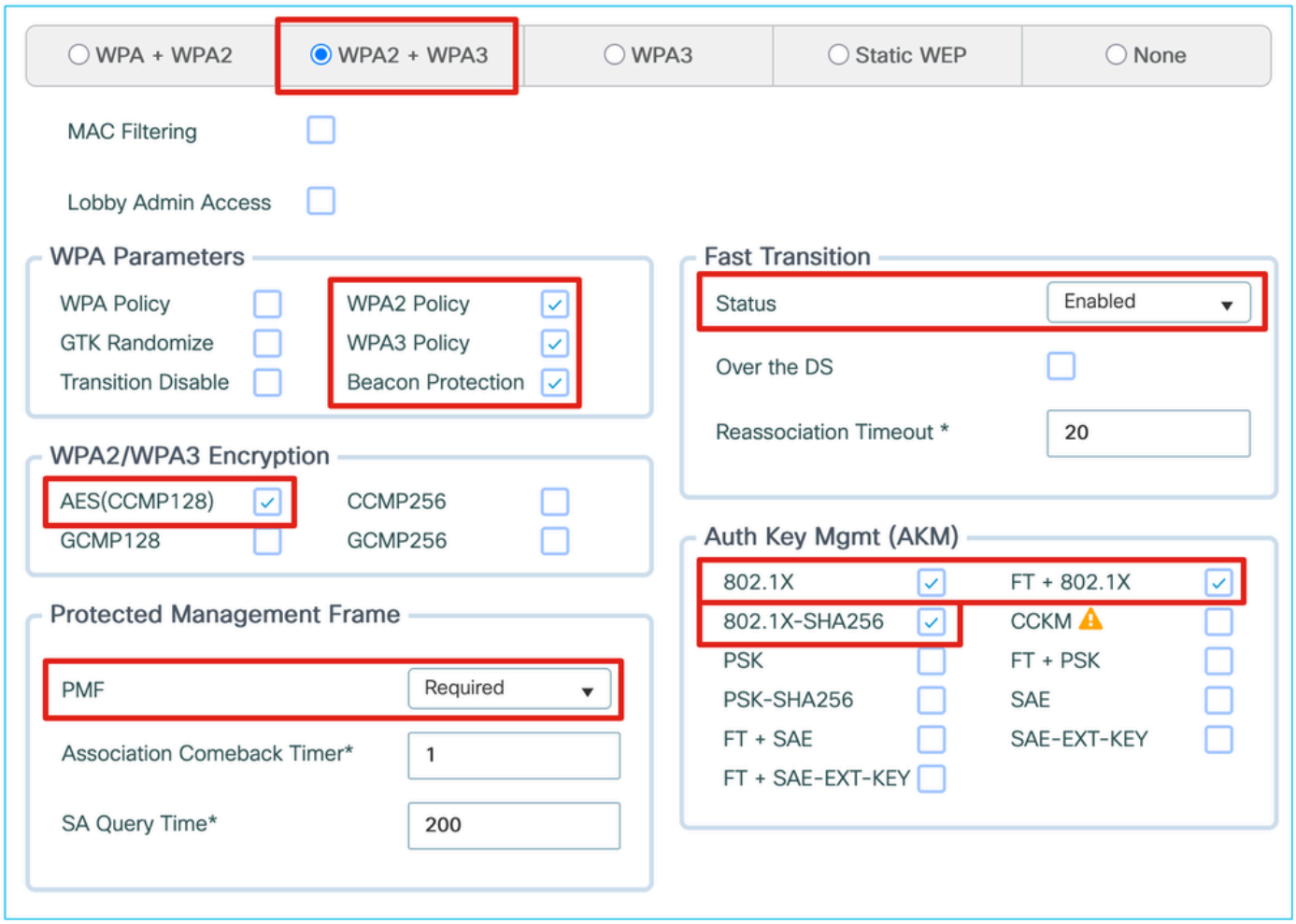
A habilitação do SSID 802.1X para 6 GHz exige apenas a habilitação do suporte a PMF, mesmo como opcional, bem como 802.1X-SHA256 e/ou FT + 802.1X AKMs, ambos compatíveis com WPA3.

Podemos continuar oferecendo WPA2 com 802.1X (SHA1) padrão na mesma WLAN. O suporte a Wi-Fi 7 requer a ativação da Proteção de Beacon e a definição de PMF conforme necessário, em vez de opcional; A WPA2 802.1X (SHA1) pode permanecer presente na WLAN como uma opção de compatibilidade com versões anteriores. Isso significa que você pode ter todos os seus dispositivos corporativos em um único SSID, desde que eles suportem 802.11w/PMF, que é bastante comum em placas de rede sem fio atuais para laptops e outros terminais móveis.

De um SSID WPA2 típico com estas configurações de segurança L2:



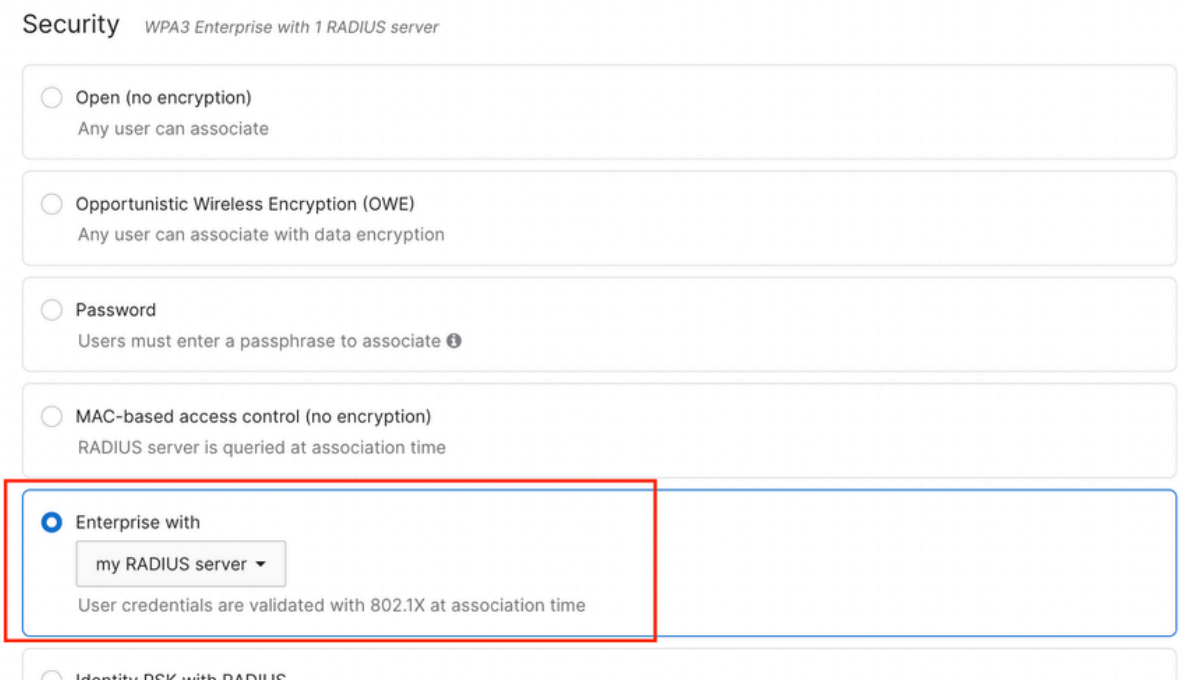
Podemos migrar a configuração para suporte a WPA3, 6 GHz e Wi-Fi 7 como mostrado aqui:



Configuração WPA3-Enterprise no painel do Cisco Meraki

No momento em que este documento foi escrito, a operação WPA3-Enterprise estava disponível apenas com um servidor RADIUS externo (também conhecido como "meu servidor RADIUS").

A WPA3-Enterprise não está disponível com a autenticação de nuvem da Meraki.



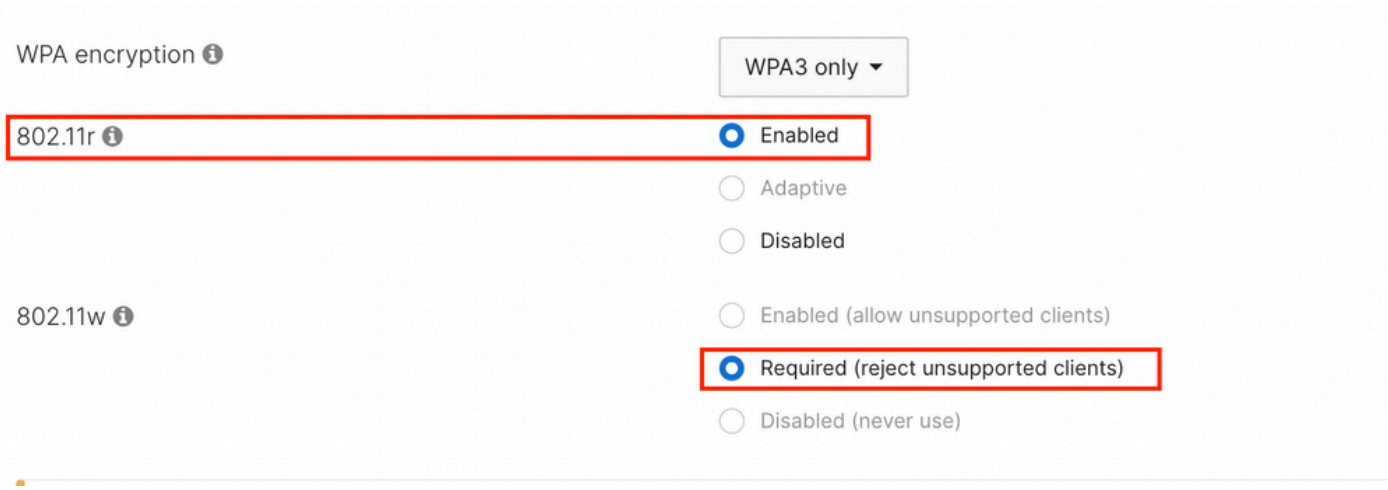
A partir do MR 31.x, os tipos de WPA são:

- 'WPA3 only', que usa as mesmas cifras que a WPA2, mas requer 802.11w (PMF).
- 'WPA3 192-bit', que permite somente o método EAP-TLS com 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. Este modo requer a configuração dos mesmos chipers no servidor RADIUS ative esse modo.
- 'Modo de transição WPA3' (também conhecido como modo misto), que permite a coexistência de clientes WPA2 na mesma WLAN usada para WPA3.

Ao usar 'WPA3 only' ou 'WPA3 192-bit Security', o PMF é obrigatório para todos os clientes.

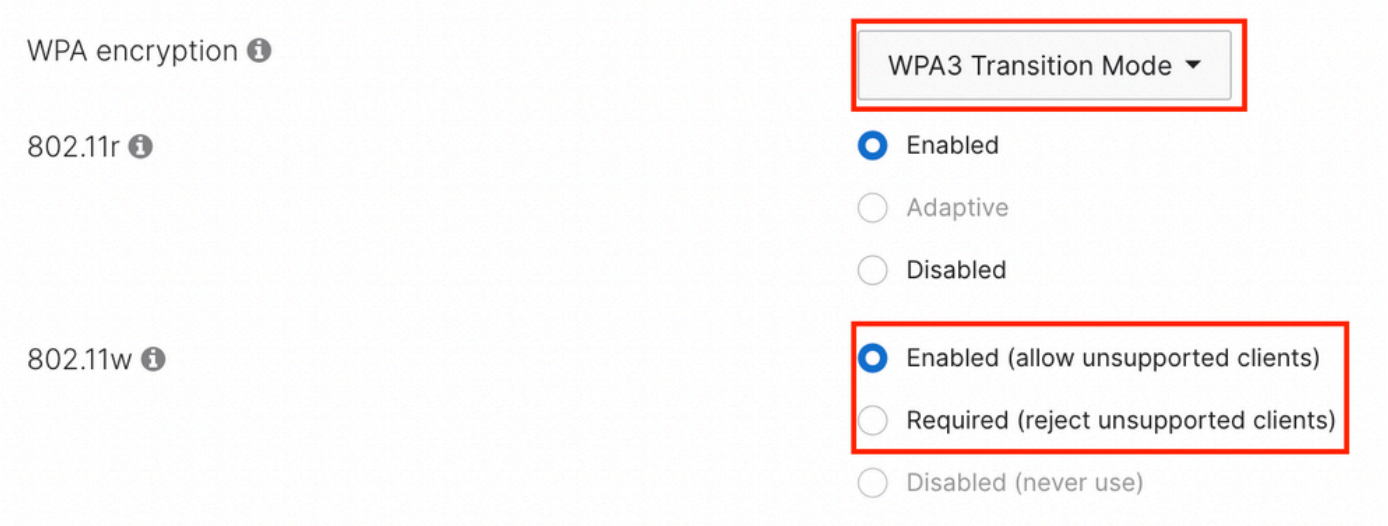
Na maioria dos aplicativos, o FT (802.11r), embora não seja obrigatório, deve ser habilitado para reduzir o impacto da latência de roaming e reautenticação ao usar um servidor RADIUS externo.

A operação em 6 GHz exige a ativação do PMF (802.11w).



Ao selecionar o Modo de transição WPA3, todos os clientes capazes de usar a WPA3 assumem como padrão o uso do PMF. Todos os clientes que operam em 6 GHz usam WPA3.

Neste modo, você pode selecionar se o cliente herdado que usa WPA2 deve usar PMF (802.11w obrigatório) ou se esse recurso é opcional (802.11w habilitado).



Independentemente da seleção WPA3, os APs Cisco Meraki exigem que o conjunto de cifras GCMP 256 esteja habilitado para operar no modo Wi-Fi 7.

Além disso, a Proteção de Beacon é habilitada por padrão em 2,4, 5 e 6 GHz quando os APs estão operando no modo Wi-Fi 7.

Senha / WPA3-Personal / Redes da IoT

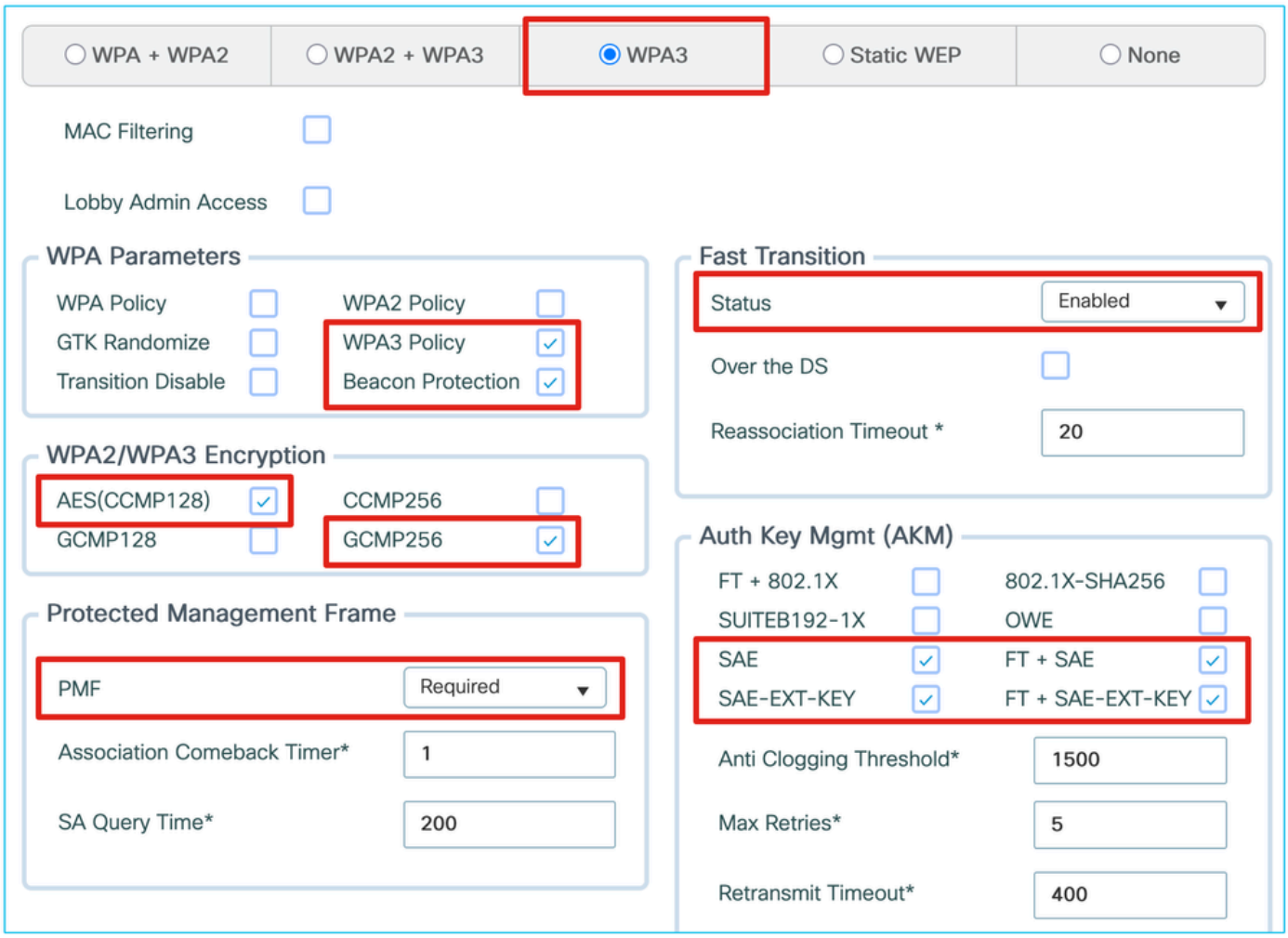
A habilitação de uma senha SSID para 6 GHz, suporte até Wi-Fi 6E, é simples e requer SAE e/ou FT + SAE, juntamente com outros AKMs WPA2 PSK, se necessário. No entanto, para o suporte do Wi-Fi 7, a certificação exige a remoção de qualquer opção WPA2 PSK e a adição de SAE-EXT-KEY e/ou FT + SAE-EXT-KEY AKMs, juntamente com a cifra GCMP256. Portanto, não é possível ter uma WLAN baseada em senha com compatibilidade máxima para clientes mais antigos e desempenho Wi-Fi 7.

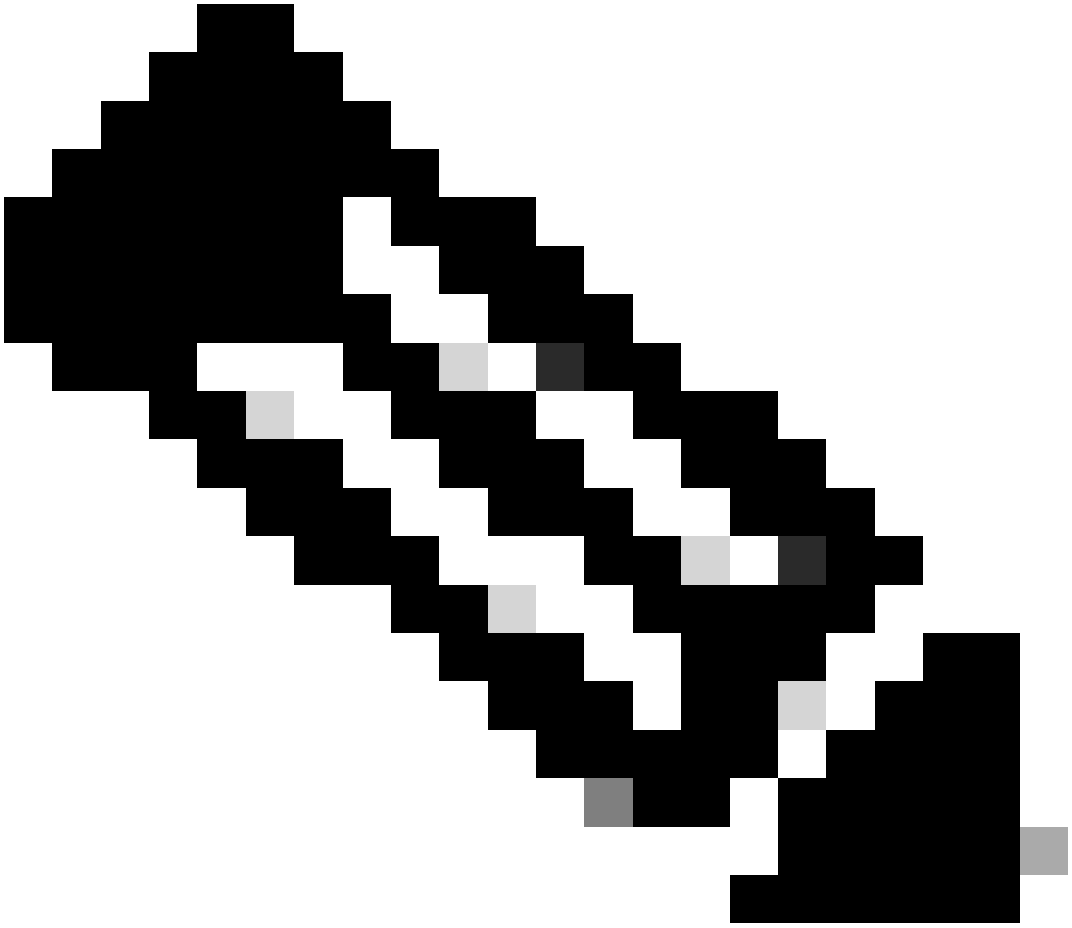
Nesses casos, precisamos configurar um SSID dedicado somente WPA3 com SAE, FT + SAE, SAE-EXT-KEY e FT + SAE-EXT-KEY, oferecendo cifras AES(CCMP128) e GCMP256, para clientes Wi-Fi 6E e Wi-Fi 7 mais recentes.

Em todos esses cenários, é altamente recomendável habilitar a FT ao usar o SAE. A troca de quadros SAE é cara em termos de recursos e mais longa do que o handshake de quatro vias WPA2 PSK.

Alguns fabricantes de dispositivos, como a Apple, esperam usar o SAE apenas quando o FT estiver habilitado e podem recusar a conexão se não estiverem disponíveis.

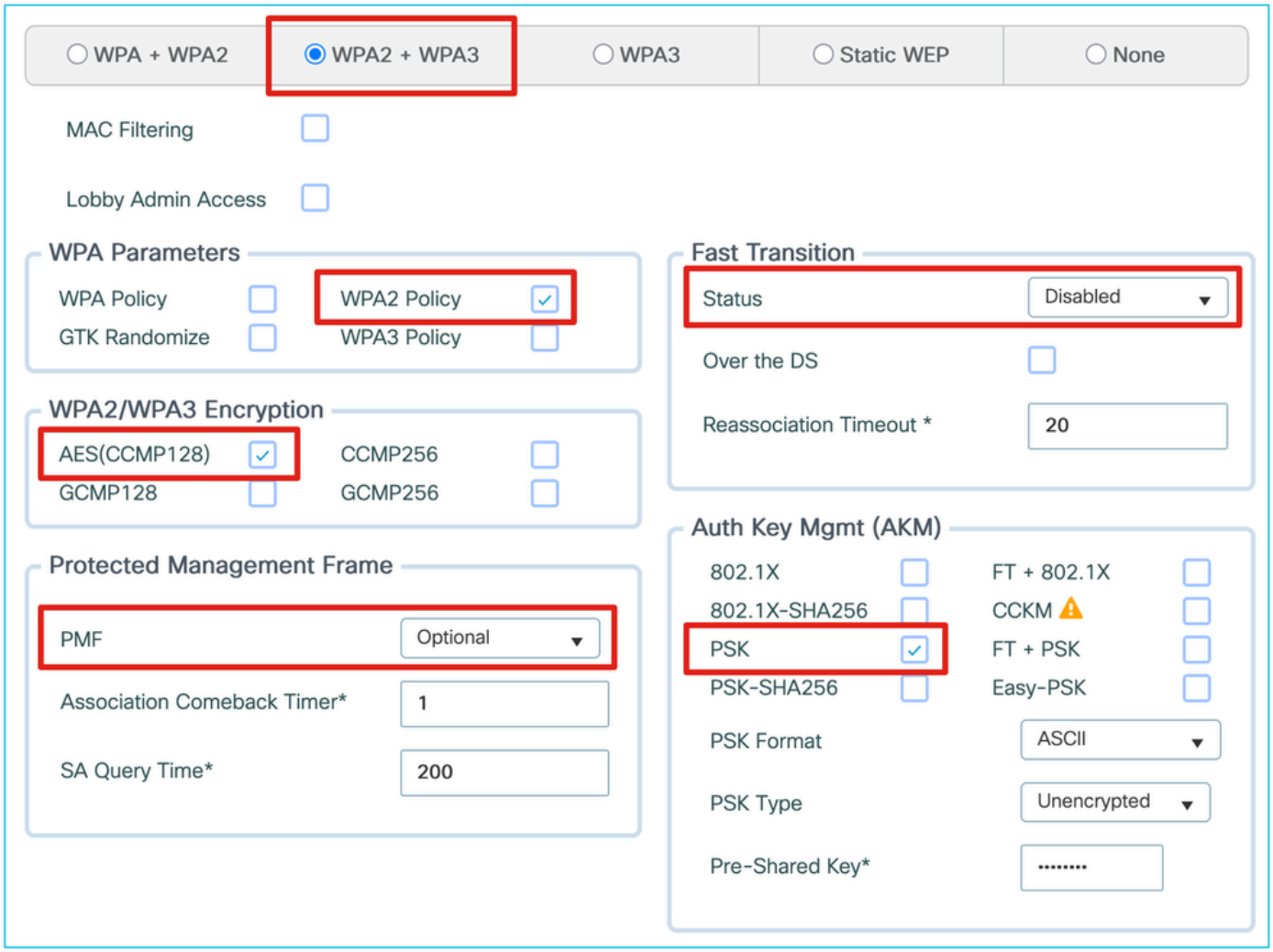
Configuração WPA3-SAE e WPA2-Personal no IOS XE


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



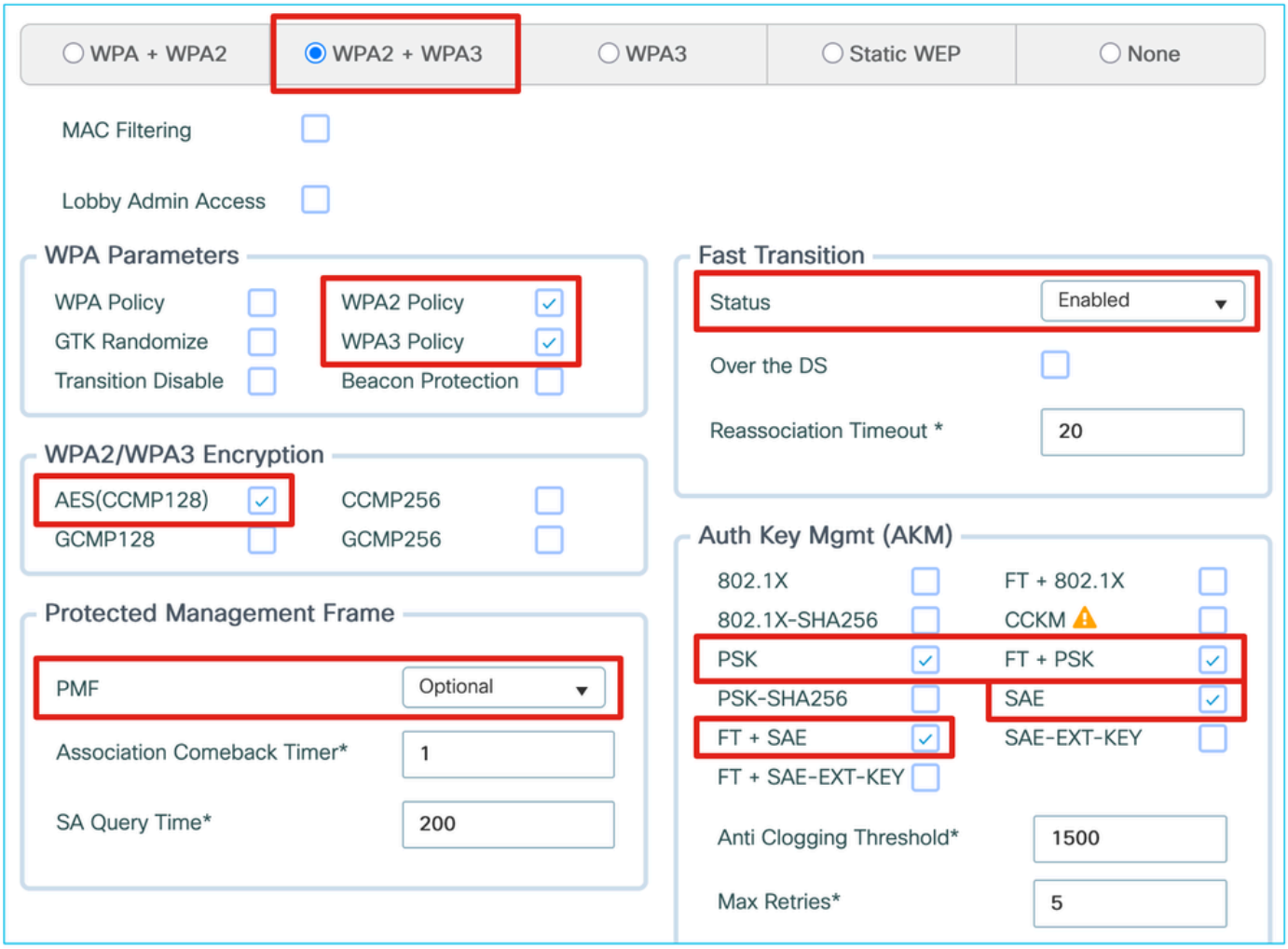
Note: Se o (FT +) SAE estiver habilitado na WLAN e um cliente Wi-Fi 7 tentar se associar a ele em vez de (FT +) SAE-EXT-KEY, ele será rejeitado. Desde que (FT +) SAE-EXT-KEY também esteja habilitado, os clientes Wi-Fi 7 devem de qualquer forma usar este último AKM, e este problema não deve acontecer.

Outro SSID WPA2 normal, por outro lado, ainda pode acomodar clientes herdados restantes.

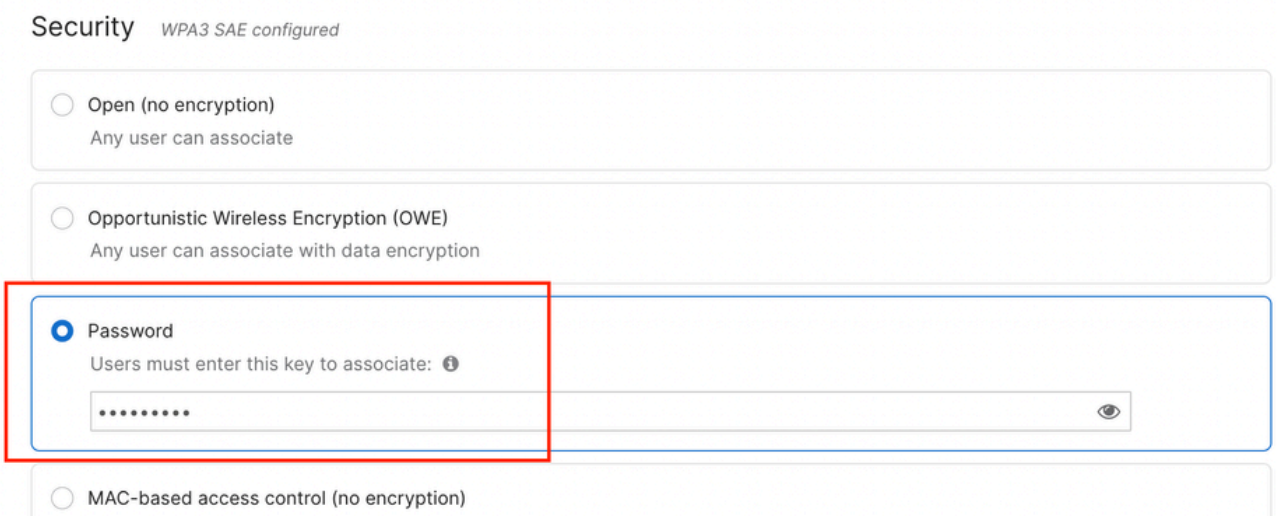


Embora essa combinação aumente a quantidade total de SSIDs, ela permite manter a compatibilidade máxima em um SSID, onde também podemos potencialmente desativar outros recursos avançados que poderiam afetar a compatibilidade e que poderiam ser úteis para muitos cenários de IoT, oferecendo recursos e desempenho máximos para dispositivos mais recentes por meio de outro SSID.
Outra opção também poderia ser, obviamente, não oferecer o Wi-Fi 7 SSID e manter apenas um único configurado para WPA2 PSK e WPA3 SAE. A ideia por trás disso pode ser que os dispositivos da IoT não precisam de desempenho do Wi-Fi 7.

Essa abordagem ainda suportaria 6 GHz para clientes com capacidade Wi-Fi 6E e Wi-Fi 7, que seriam capazes de se conectar com desempenho Wi-Fi 6E na melhor das hipóteses.

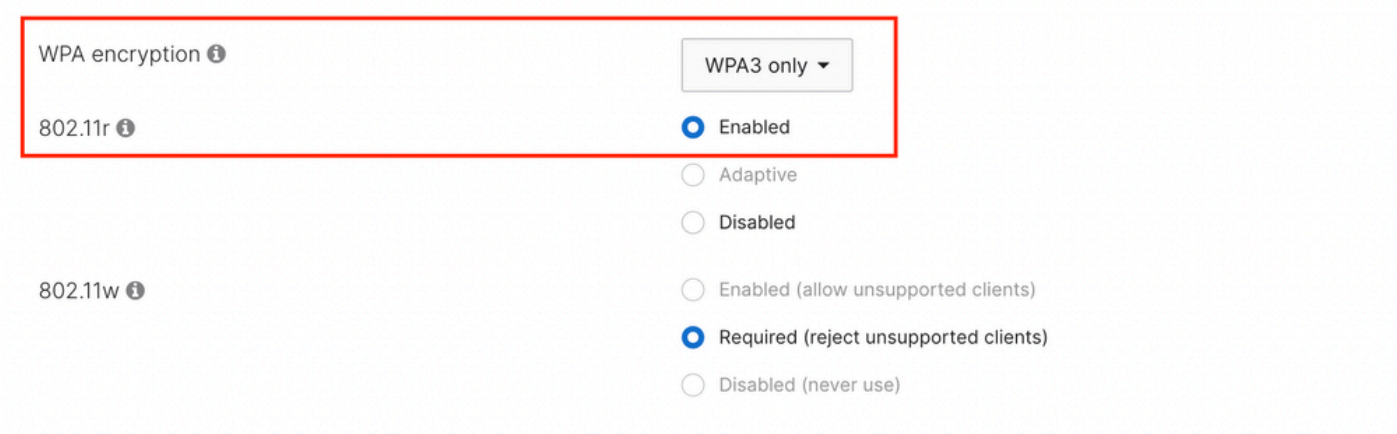


Configuração WPA3-SAE no painel do Cisco Meraki



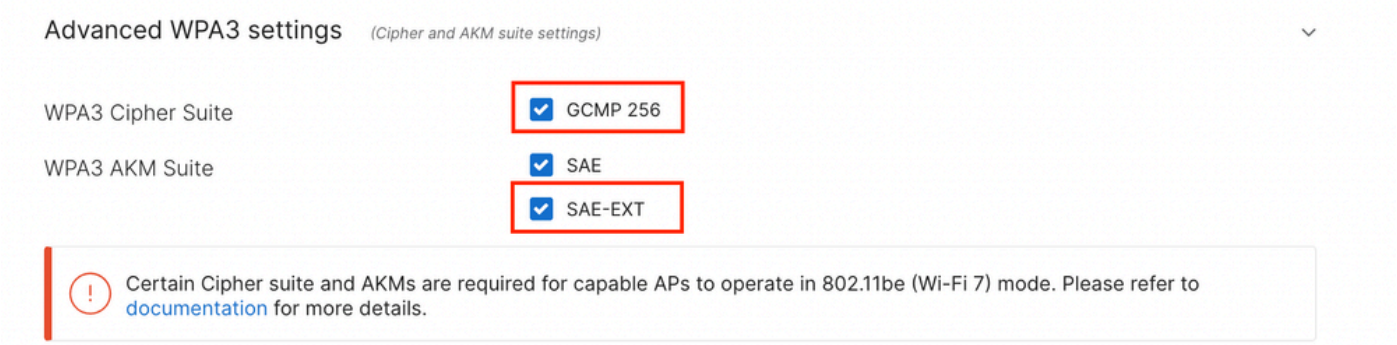
Até o firmware MR 30.x, o único tipo de WPA suportado é 'WPA3 only' e o painel não permite selecionar um método diferente.

O PMF é obrigatório nesta configuração, enquanto o FT (802.11r) é recomendado para ser habilitado ao usar o SAE.



Para permitir a operação do Wi-Fi 7, o conjunto de chips GCMP 256 e o conjunto SAE-EXT AKM devem ser ativados na configuração do SSID.

Elas são desativadas por padrão e podem ser ativadas em "Configurações WPA3 avançadas".



A partir deste momento, todas as WLANs ativadas na rede devem atender aos requisitos da especificação Wi-Fi 7 para serem ativadas na versão MR 31.1.x do firmware e mais recente.

Isso significa que um SSID Wi-Fi 7 configurado conforme descrito anteriormente não pode coexistir com outro SSID usando o Modo de transição WPA2-Personal ou WPA3-SAE.

Se um SSID WPA2-Personal for configurado na rede do painel, todos os APs Wi-Fi 7 serão revertidos para a operação Wi-Fi 6E.

Esse comportamento muda em uma versão futura do firmware MR 32.1.x.

Redes abertas / aprimoradas abertas / OWE / Convidado

As redes de convidados vêm com muitas opções. Geralmente, eles não exigem credenciais 802.1X ou senha para se conectar e possivelmente implicam em uma página inicial ou portal, que pode exigir credenciais ou um código. Tradicionalmente, isso é tratado com um SSID aberto e soluções de portal para convidados locais ou externos. No entanto, SSIDs com segurança aberta (sem criptografia) não são permitidos em 6 GHz ou para suporte a Wi-Fi 7.

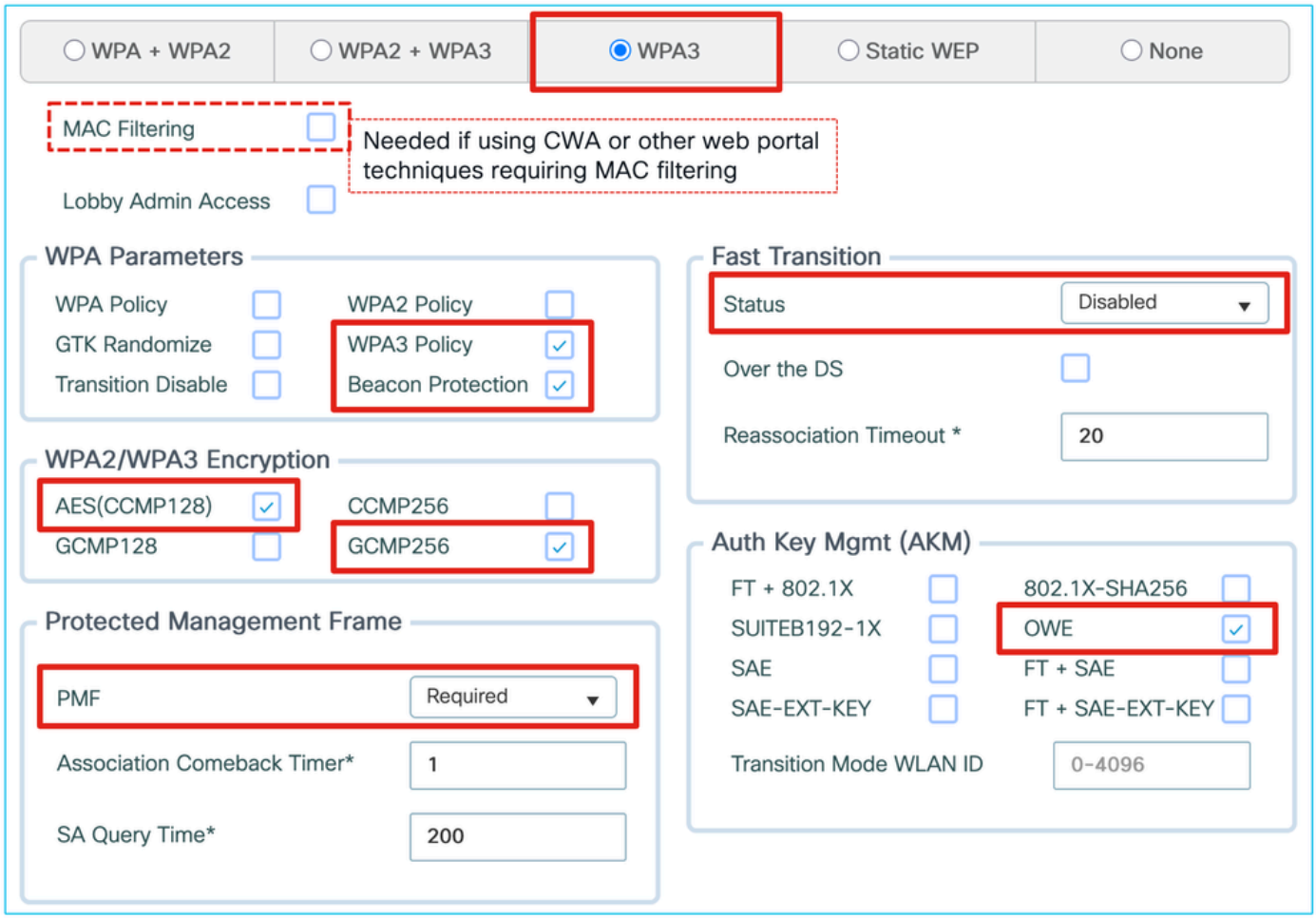
Uma primeira abordagem muito conservadora seria dedicar redes de convidados à banda de 5 GHz e Wi-Fi 6, na melhor das hipóteses. Isso deixa a banda de 6 GHz reservada para dispositivos corporativos, resolve o problema de complexidade e traz compatibilidade máxima,

embora não até desempenho Wi-Fi 6E/7.

Se, de um lado, o Enhanced Open é um excelente método de segurança que oferece privacidade e mantém a experiência "aberta" (os usuários finais não precisam inserir nenhuma credencial 802.1X ou senha), até hoje ele ainda tem suporte limitado entre os endpoints. Alguns clientes ainda não suportam isso e, mesmo quando o fazem, essa técnica nem sempre é tratada sem problemas (o dispositivo pode mostrar a conexão como não segura, enquanto ela é realmente segura, ou pode exibi-la como protegida por senha, mesmo que nenhuma senha seja necessária com OWE). Como se espera que uma rede de convidados funcione em todos os dispositivos não controlados de convidados, pode ser muito cedo para fornecer apenas um SSID Aberto Aprimorado e é recomendável fornecer ambas as opções por meio de SSIDs separados: um aberto em 5 GHz e um OWE habilitado em 5 e 6 GHz, ambos com o mesmo portal cativo atrás, se isso também for um requisito. O Modo de Transição não é suportado em Wi-Fi 6E, 6 GHz (embora ainda possa ser permitido no software) ou Wi-Fi 7, portanto essa não é uma solução recomendada. Todas as técnicas de redirecionamento do portal (autenticação da Web interna ou externa, autenticação da Web central, ...) ainda são suportadas com OWE.

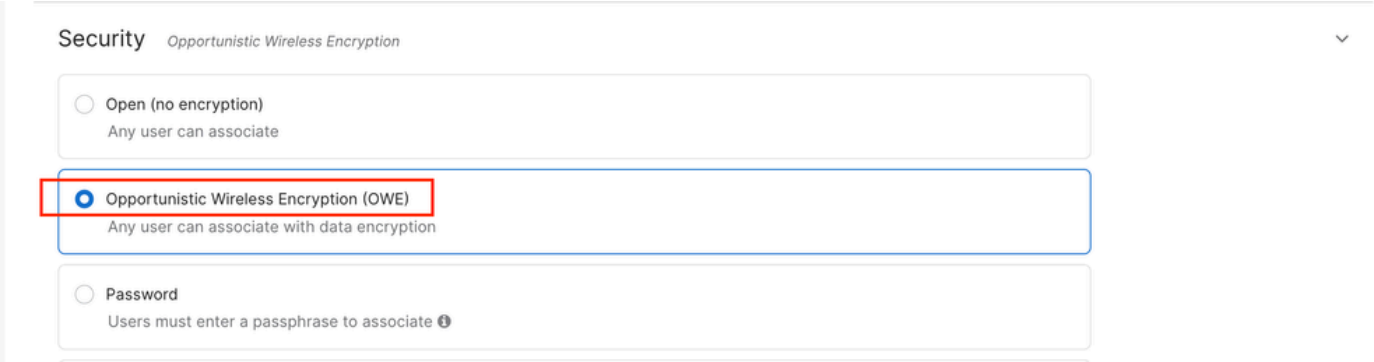
Configuração OWE no IOS XE

Se quiséssemos fornecer serviço de 6 GHz aos convidados, a recomendação seria criar um SSID separado com Enhanced Open / OWE (Opportunistic Wireless Encryption). Ele poderia oferecer tanto a cifra AES(CCMP128), para máxima compatibilidade até clientes Wi-Fi 6E, bem como GCMP256 bits para clientes com capacidade Wi-Fi 7.



Configuração OWE no painel do Cisco Meraki

Semelhante ao que foi feito no IOS XE, a recomendação é criar um SSID de convidado separado com Enhanced Open / OWE operando em 6 GHz no painel do Cisco Meraki.
Isso pode ser configurado novamente em Wireless > Access Control e selecionando "Opportunistic Wireless Encryption (OWE)" como o método de segurança.

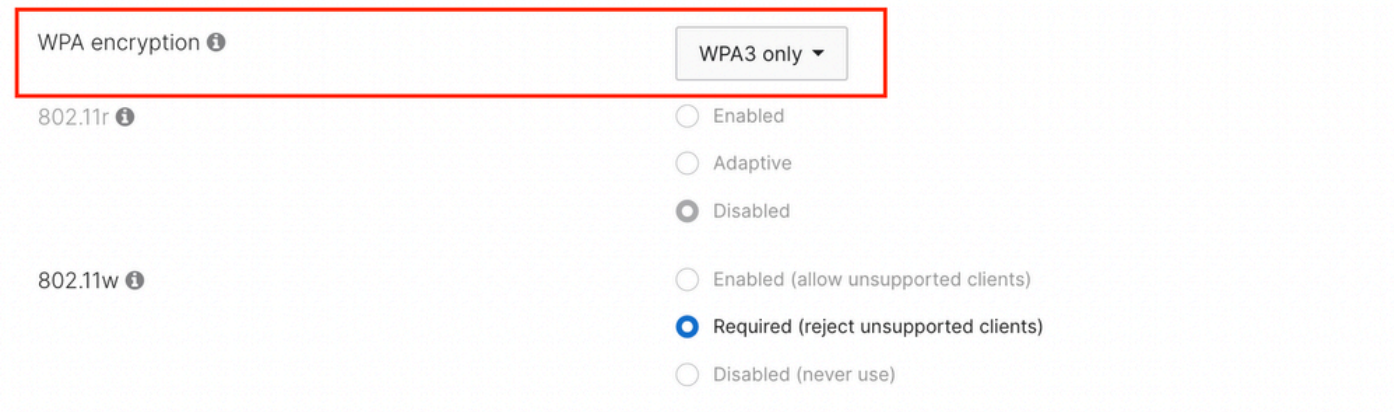


Ao executar o firmware até MR 31, o único tipo de WPA suportado é 'WPA3 only' e o painel não permite que você selecione um método diferente.

O PMF é obrigatório nesta configuração, enquanto o FT (802.11r) não pode ser habilitado.

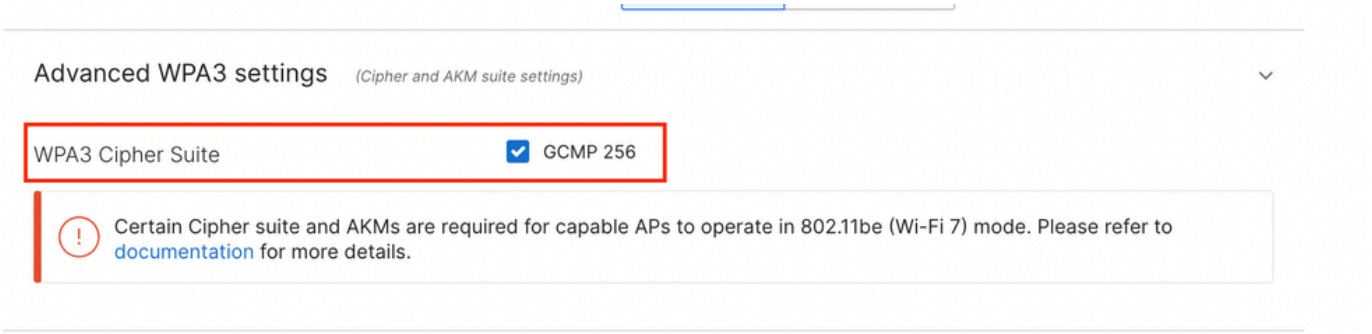
Observe que o rótulo 'WPA3 only' está sobrecarregado, pois OWE não faz parte do padrão WPA3; no entanto, essa configuração se refere ao OWE sem o Transition Mode.

O OWE Transition Mode está disponível como parte de uma versão futura do MR 32.1.x.



A codificação AES(CCMP128) é habilitada por padrão para máxima compatibilidade até clientes Wi-Fi 6E.

Os bits GCMP256 podem ser ativados junto com o CCMP128 para conformidade com os requisitos do Wi-Fi 7.



WPA3 adicional e opções relacionadas

Embora as opções de WPA3 sejam melhor descritas e abordadas no guia de implantação de WPA3, esta seção aborda algumas recomendações adicionais para WPA3 especificamente relacionadas ao suporte de 6 GHz e Wi-Fi 7.

Proteção de beacon

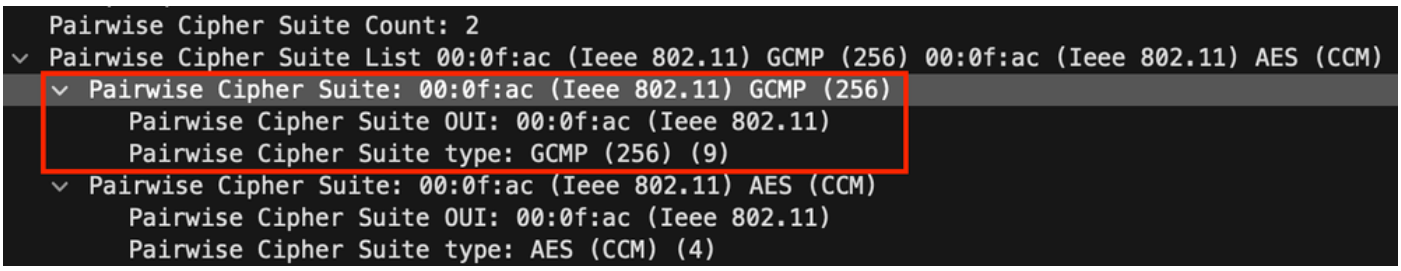
Esse é um recurso que resolve a vulnerabilidade, em que um invasor mal-intencionado pode transmitir beacons em vez do ponto de acesso legítimo, ao mesmo tempo em que modifica alguns campos para alterar a segurança ou outras configurações de clientes já associados. A proteção de beacon é um elemento de informação adicional (MIC de Gerenciamento) no beacon que atua como uma assinatura para o próprio beacon, para provar que ele foi enviado pelo ponto de acesso legítimo e que não foi violado. Somente clientes associados a uma chave de criptografia WPA3 podem verificar a legitimidade do beacon; os clientes de sondagem não têm meios para verificá-lo. O elemento de informação adicional no beacon deve simplesmente ser ignorado pelos clientes que não o suportam (isto refere-se a clientes não Wi-Fi 7), e normalmente não causa problemas de compatibilidade (a menos que com um driver de cliente mal programado).

Esta captura de tela mostra um exemplo do conteúdo do Elemento de Informações de MIC de Gerenciamento:

GCMP256

Até a certificação Wi-Fi 7, a maioria dos clientes implementava a criptografia por cifra AES(CCMP128). CCMP256 e GCMP256 são variantes muito específicas relacionadas ao SUITE-B 802.1X AKM. Embora algumas primeiras gerações de clientes Wi-Fi 7 no mercado aleguem o suporte Wi-Fi 7, às vezes ainda não implementam a criptografia GCMP256, que pode se tornar um problema se os APs Wi-Fi 7 que aplicam o padrão como esperado impedem que esses clientes se conectem sem o suporte GCMP256 adequado.

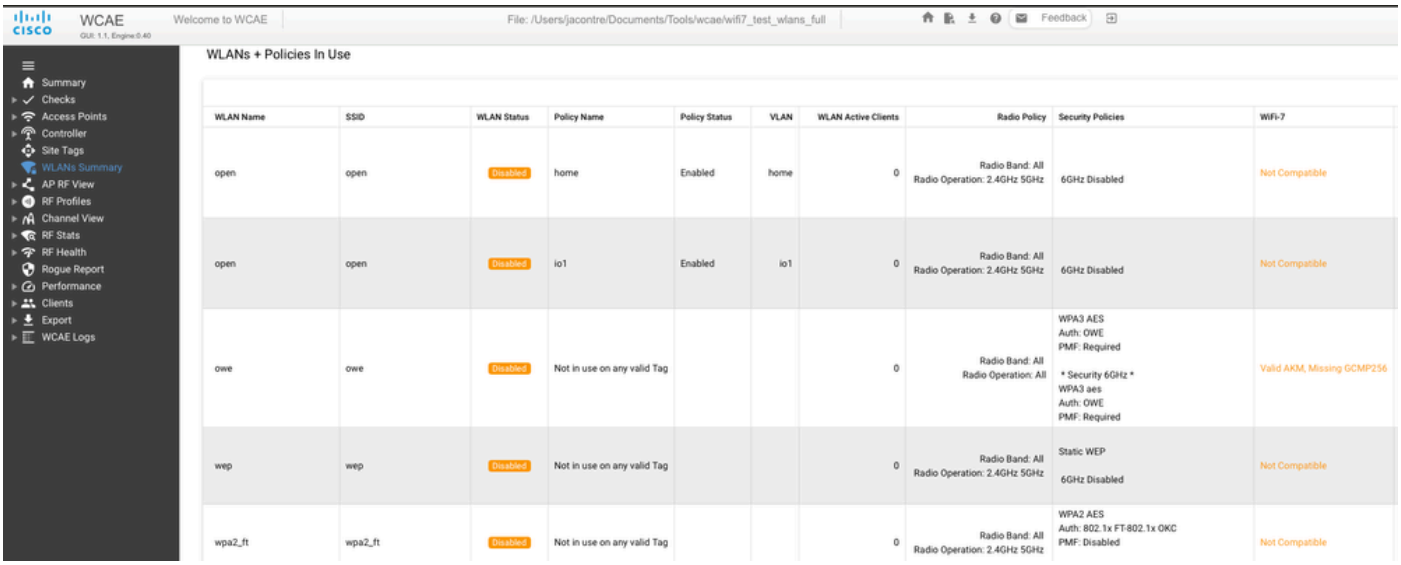
Quando o GCMP256 está habilitado, o RSNE (Elemento de Rede de Segurança Robusto) nos Quadros de Beacon para a WLAN anuncia a capacidade na Lista de Suítes de Chipers Pairwise como mostrado aqui.



Solucionar problemas e verificar

A versão mais recente do Wireless Configuration Analyzer Express (https://developer.cisco.com/docs/wireless-troubleshooting-tools/wireless-config-analyzer-express-gui/) tem uma verificação de prontidão Wi-Fi 7 que avalia sua configuração 9800 para todos os requisitos Wi-Fi 7 mencionados anteriormente.

Se você ainda tiver dúvidas se sua configuração está preparada para Wi-Fi 7, o WCAE permite que você saiba o que está errado.



Referências

1. Cisco Systems. "Guia de criptografia e configuração WPA3".
2. Guia Meraki WPA3

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.