Migre a 6 GHz y a Wi-Fi 7 con Cisco Wireless

Contenido

Introducción

Este documento describe las pautas de diseño y configuración para optimizar el rendimiento de Wi-Fi 7 y aprovechar completamente el espectro de 6 GHz.

Guía de diseño de CX

Las guías de diseño de CX están escritas por especialistas de Cisco CX en colaboración con ingenieros de otros departamentos y son revisadas por expertos de Cisco; las guías se basan en las prácticas líderes de Cisco, así como en el conocimiento y la experiencia adquiridos a través de innumerables implementaciones en clientes durante muchos años. Las redes diseñadas y configuradas de acuerdo con las recomendaciones de este documento ayudan a evitar los obstáculos más comunes y a mejorar el funcionamiento de la red.

Por qué 6 GHz y Wi-Fi 7

La banda de 6 GHz comenzó a estar disponible para las operaciones de WLAN en 2020 y se necesitaba para la certificación Wi-Fi 6E. Mientras que Wi-Fi 6 funciona en las bandas de 2,4 GHz y 5 GHz, Wi-Fi 6E utiliza el mismo estándar IEEE 802.11ax, pero amplía su funcionalidad a la banda de 6 GHz, siempre que se cumplan los requisitos específicos.
La nueva certificación Wi-Fi 7 se basa en el estándar IEEE 802.11be y admite operaciones en las bandas de 2,4 GHz, 5 GHz y 6 GHz. Wi-Fi 7 también introduce nuevas funciones y mejoras en comparación con las certificaciones anteriores.

La compatibilidad con la banda de 6 GHz y/o Wi-Fi 7 conlleva requisitos específicos y, a menudo, requiere nuevas configuraciones y diseños de radiofrecuencia, especialmente en comparación con las prácticas establecidas para las bandas de 2,4 GHz y 5 GHz con Wi-Fi 6.

Por ejemplo, del mismo modo que el uso de una seguridad WEP obsoleta impide la adopción de estándares 802.11 más allá de 802.11a/b/g, los estándares más recientes imponen requisitos de seguridad aún más estrictos para fomentar la implementación de redes más seguras.

Por el contrario, la introducción de la banda de 6 GHz ofrece acceso a frecuencias más limpias, rendimiento mejorado y compatibilidad con nuevos casos prácticos. También permite una implementación más fluida de las aplicaciones existentes, como las conferencias de voz y vídeo.

Requisitos básicos para operaciones de 6 GHz y Wi-Fi 7

Estos son los requisitos de seguridad que figuran en las certificaciones para las operaciones de 6 GHz y Wi-Fi 7.

Requisitos de la banda de 6 GHz

La banda de 6 GHz sólo permite WLANs abiertas mejoradas o WPA3, lo que significa que una de

estas opciones de seguridad es:

- WPA3-Enterprise con autenticación 802.1X
- WPA3: autenticación simultánea de iguales (SAE) (también denominada WPA3-Personal) con frase de paso. SAE-FT (SAE with Fast Transition) es otro AKM posible y en realidad se recomienda para su uso ya que el intercambio de señales SAE no es trivial, y FT permite saltarse ese intercambio más largo.
- Open mejorado con cifrado inalámbrico oportunista (OWE)

Aunque, según las especificaciones de WPA3 v3.4 (sección 11.2), el modo de transición abierto mejorado no es compatible con 6 GHz, muchos proveedores (incluido Cisco hasta IOS® XE 17.18) todavía no aplican esta norma. Por lo tanto, es técnicamente posible configurar, por ejemplo, un SSID abierto a 5 GHz, un SSID abierto mejorado correspondiente a 5 y 6 GHz, ambos con el modo de transición habilitado, y todo esto sin cumplir con las especificaciones de los estándares. Sin embargo, en tal escenario, se debe esperar que configuremos un SSID abierto mejorado sin modo de transición y disponible solo en 6 GHz (los clientes que soportan 6 GHz generalmente soportan el modo abierto mejorado también), mientras mantenemos nuestro SSID abierto regular en 5 GHz, también sin modo de transición.

No existen nuevos requisitos de cifrado o algoritmo específicos para WPA3-Enterprise, aparte de la aplicación de 802.11w/Protected Management Frame (PMF). Muchos proveedores, incluido Cisco, consideran que 802.1X-SHA256 o "FT + 802.1X" (que en realidad es 802.1X con SHA256 y Fast Transition en la parte superior) solo es compatible con WPA3 y que el estándar 802.1X (que utiliza SHA1) se considera parte de WPA2, por lo que no es apto ni compatible con 6 GHz.

Requisitos de Wi-Fi 7

Con la certificación Wi-Fi 7 del estándar 802.11be, Wi-Fi Alliance aumentó los requisitos de seguridad. Algunas de ellas permiten el uso de las velocidades de datos de 802.11be y mejoras de protocolo, mientras que otras son específicas para admitir operaciones de enlaces múltiples (MLO), lo que permite a los dispositivos compatibles (clientes o AP) utilizar varias bandas de frecuencia al tiempo que mantienen la misma asociación.

En general, Wi-Fi 7 exige uno de estos tipos de seguridad:

- WPA3-Enterprise con AES (CCMP128) y 802.1X-SHA256 o FT + 802.1X (que sigue utilizando SHA256, aunque no sea explícito en su denominación). Esto no supone ningún cambio en comparación con los requisitos previos de seguridad de WPA3 anteriores para la banda de 6 GHz.
- WPA3-Personal con GCMP256 y SAE-EXT-KEY o FT + SAE-EXT-KEY (AKM 24 o 25). Wi-Fi 6E exige WPA3 SAE y/o FT + SAE con AES (CCMP128) normal y sin usos adicionales de claves ampliadas; esto significa que se introdujo un nuevo cifrado específicamente para Wi-Fi 7.
- Apertura/OWE mejorada con GCMP256. Aunque AES (CCMP128) se puede seguir configurando en el mismo SSID, los clientes que utilizan AES 128 no admiten Wi-Fi 7. Antes de Wi-Fi 7, la mayoría de los clientes que admitían AES mejorado solo utilizaban AES 128, por lo que este es un requisito nuevo y más importante. En cuanto a la compatibilidad con 6

GHz, no se permite ningún modo de transición.

Independientemente del tipo de seguridad seleccionado, se requieren marcos de gestión protegidos (PMF) y protección de baliza para admitir Wi-Fi 7 en la WLAN.

Dado que Wi-Fi 7 sigue siendo una certificación reciente en el momento de redactar este documento, con una versión lo antes posible, muchos proveedores no han aplicado todos estos requisitos de seguridad desde el principio.

Más recientemente, Cisco ha ido aplicando progresivamente las opciones de configuración para cumplir con la certificación Wi-Fi 7. Estos son los comportamientos específicos de la versión:

IOS XE versión 17.15.3 y posterior versión 17.15.x

En esta sucursal, todas las WLAN se transmiten como SSID de Wi-Fi 7, siempre que Wi-Fi 7 esté habilitado de forma global e independientemente de la configuración de seguridad.

Un cliente puede asociarse como compatible con Wi-Fi 7 y lograr velocidades de datos de Wi-Fi 7 independientemente del método de seguridad que utilice, siempre que la WLAN siga admitiéndolo. Sin embargo, el cliente solo puede asociarse con capacidad MLO (en una o más bandas) si respeta los estrictos requisitos de seguridad Wi-Fi 7 o si se rechaza.

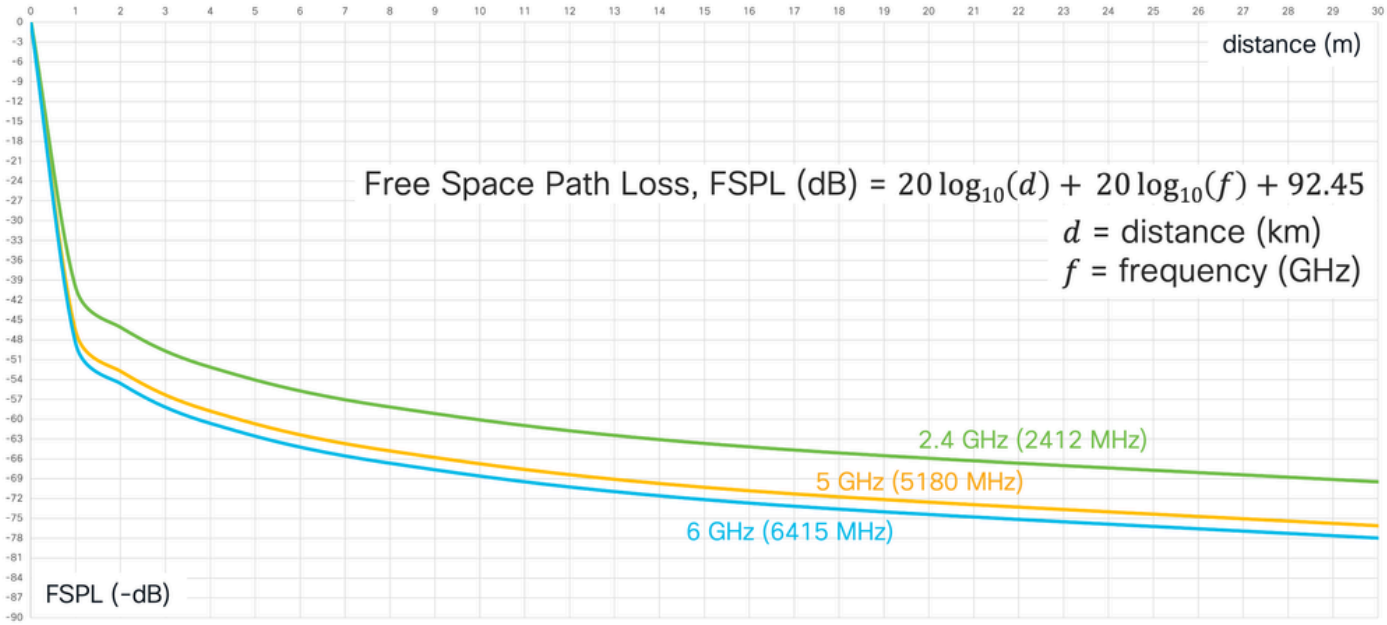
Esto podría causar problemas cuando algunos clientes de Wi-Fi 7 anteriores no pueden soportar cifrados más seguros, como GCMP256, intentan asociarse como Wi-Fi 7 MLO capaz de una WLAN, cuya configuración de seguridad no coincide con los requisitos de Wi-Fi 7. En tal situación, el cliente es rechazado debido a las configuraciones de seguridad inválidas (todavía se permite ser configurado bajo el WLAN).

Consideraciones de diseño de radio para la cobertura de 6 GHz

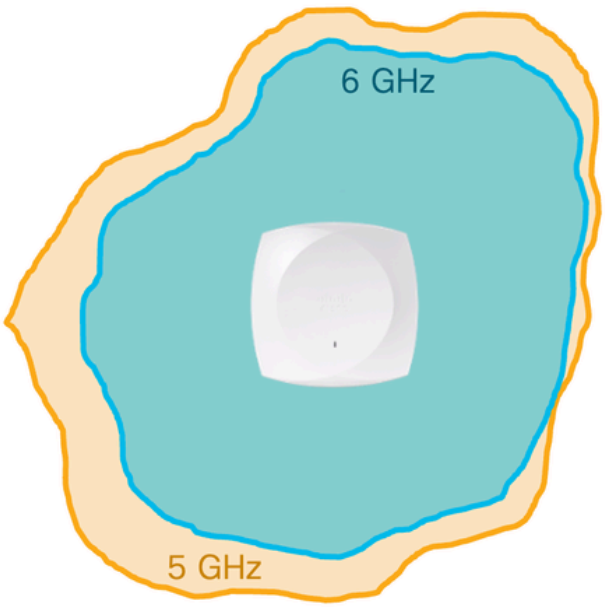
Sin ánimo de convertirse en una guía prescriptiva completa sobre los estudios in situ, en esta sección se describen brevemente algunas consideraciones básicas a la hora de diseñar una cobertura de 6 GHz, especialmente si ya existe una instalación de 2,4/5 GHz que nos gustaría migrar a Wi-Fi 6E o 7.
En cuanto a las nuevas implementaciones de Wi-Fi a las que estábamos acostumbrados en 2,4 y 5 GHz, un nuevo proyecto inalámbrico en 6 GHz debe incluir también un sondeo del sitio dedicado de 6 GHz correspondiente.

Cuando los AP pre-Wi-Fi 6E/7 ya están posicionados para una cobertura y necesidades específicas de 5 GHz, en algunos casos, podemos esperar poder sustituirlos por AP compatibles con Wi-Fi 6E/7 y aún así obtener una buena cobertura en 6 GHz. Para que esta teoría funcione, nuestros AP existentes ya deben proporcionar una cobertura correcta de 5 GHz para las necesidades previstas (solo datos, voz, aplicaciones específicas, etc.) mientras que ya están al menos 3-4 niveles de potencia de transmisión por debajo de su límite máximo. Los AP típicamente tienen de 7 a 8 niveles de energía, y cada nivel de energía divide la potencia de transmisión por la mitad. Esto significa que un lugar cómodo a ser es cuando los AP están utilizando el medio de su rango de potencia de transmisión permitido.

Según los cálculos de pérdida de espacio libre, las señales de 6 GHz se atenúan con 2 dB más que las de 5 GHz. Además, los obstáculos también pueden afectar más a las señales de 6 GHz que a sus equivalentes de 5 GHz.



Cuando un AP de Cisco aumenta/disminuye su potencia de transmisión en un nivel, lo hace mediante un "salto" de 3 dB. Un AP que pasa de un nivel de potencia de 4, con una potencia de transmisión de 11 dBm por ejemplo, a un nivel de potencia de 3, aumenta su potencia de transmisión a 14 dBm (11 dBm para el nivel de potencia 4 y 14 dBm para el nivel de potencia 3 son solo un ejemplo genérico, ya que diferentes modelos/generaciones de AP podrían tener valores de potencia de transmisión ligeramente diferentes en dBm para el mismo número de nivel de potencia).



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 AP 6E/7 pre-Wi-Fi ya proporciona una buena cobertura a 5 GHz en el nivel de potencia 4, por ejemplo, un AP 6E/7 Wi-Fi más nuevo con patrones de radio similares de 5 GHz podría reemplazar a ese AP anterior sin ningún impacto significativo en la red de 5 GHz existente.

Además, la radio de 6 GHz del nuevo punto de acceso Wi-Fi 6E/7 podría proporcionar una cobertura de 6 GHz similar a la de 5 GHz con solo estar en un nivel de potencia de transmisión (3 dB) superior.

Si 5 GHz ya está cubierto correctamente con la radio de 5 GHz del AP en 3-4 niveles de potencia por debajo de su máximo, la radio de 6 GHz correspondiente podría, por lo tanto, configurarse en 2-3 niveles de potencia por debajo de su máximo para una cobertura comparable.

Además, si la radio de 6 GHz ya proporciona una cobertura correcta con 2-3 niveles de potencia inferiores a su máximo, podría incluso aumentar excepcionalmente un par de niveles, por ejemplo, para intentar solucionar agujeros temporales de cobertura inesperados (fallo de un punto de acceso vecino, obstáculos no anunciados, nuevas necesidades de radiofrecuencia, etc.).

Comportamientos de roaming entre puntos de acceso 6E/7 anteriores a la conexión Wi-Fi y 6E/7 de Wi-Fi

La implementación de APs que admitan diferentes estándares y/o bandas de frecuencia en la misma área de cobertura no siempre ha sido una práctica recomendada, especialmente si esas diferentes generaciones de APs se instalan de manera "salada y pimienta" (es decir, se mezclan en la misma zona).

Mientras que un controlador inalámbrico podría manejar las operaciones (por ejemplo, asignación de canal dinámico, control de potencia de transmisión, distribución de caché PMK, etc.) desde un grupo de varios modelos de AP, los clientes que se mueven entre diferentes estándares e incluso diferentes bandas de frecuencia no siempre son capaces de manejar eso correctamente y es probable que se encuentren con problemas de roaming, por ejemplo.

Además, debido a los estándares más nuevos, los AP Wi-Fi 6E/7 soportan los cifrados GCMP256 para WPA3. Sin embargo, lo mismo no siempre podría ser cierto para algunos AP Wi-Fi 6 y modelos anteriores. Para los SSID de frase de paso/WPA3-Personal y de apertura/OWE mejorada, que requieren la configuración de los cifrados AES (CCMP128) y GCMP256, ciertos Wi-Fi 6 (como las series 9105, 9115 y 9120) no admiten GCMP256 y solo pueden ofrecer cifrados AES (CCMP128) a clientes asociados, incluidos los habilitados para Wi-Fi 6E/7. Si estos clientes Wi-Fi 6E/7 necesitaran itinerar desde/hacia los puntos de acceso Wi-Fi 6E/7 vecinos que admiten GCMP256, tendrían que pasar por una asociación completamente nueva, ya que la renegociación de los cifrados entre AES(CCMP128) y GCMP256 no es compatible con el roaming transparente. Además, en general, no es óptimo tener AP que ofrezcan diferentes capacidades en la misma área: esta implementación no permite a los clientes utilizar estas funciones de forma fiable mientras se mueven y puede dar lugar a adhesividad o desconexiones.
Aunque este escenario debe representar un caso de esquina, queremos tener en cuenta que, con los cifrados GCMP256 configurados bajo la WLAN, el roaming de los clientes Wi-Fi 6E/7 entre los AP 9105/9115/9120 y los AP 9130/9124/916x/917x no puede ser posible, ya que estas últimas series soportan GCMP256 y las primeras no.

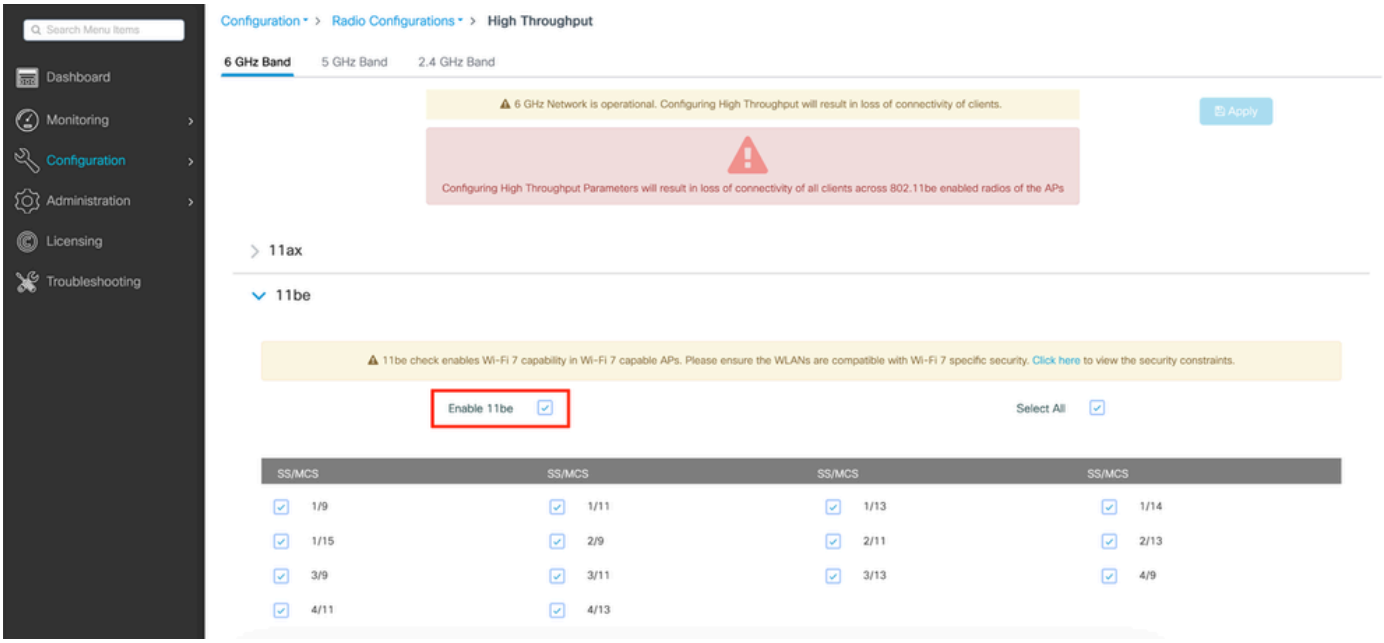
Los anchos de canal de 40 MHz o más en 6 GHz también pueden causar adhesividad para los clientes compatibles con 6 GHz, que pueden negarse a volver a asociarse a otras bandas. Esta debe ser una razón más para no mezclar APs con capacidad para 6 GHz y APs sin capacidad

para 6 GHz en la misma área de roaming.

Habilitación global de Wi-Fi 7

Habilitación global de Wi-Fi 7 en IOS XE

Al instalar o actualizar a una versión de IOS XE compatible con Wi-Fi 7, de forma predeterminada, la compatibilidad con Wi-Fi 7 está deshabilitada globalmente.
Para activarlo, debemos navegar por el menú de configuración de alto rendimiento de cada banda de 2,4/5/6 GHz y marcar la casilla para habilitar 11be.



Otra opción también podría ser ejecutar estas tres líneas de comandos a través de SSH/consola, en el modo de configuración de terminal:

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

Como se menciona en la nota de advertencia, al intentar modificar estos parámetros, el cambio del estado de la compatibilidad con 802.11be produce una breve pérdida de conectividad para todos los clientes de las radios de los puntos de acceso Wi-Fi 7. Si desea hacer MLO, lo que significa que los clientes se conectan a varias bandas al mismo tiempo, debe habilitar 11be en todas las bandas a las que desea que se conecte el cliente. No es necesario habilitar todas las bandas, pero se recomienda simplemente para el rendimiento.

Habilitación global de Wi-Fi 7 en el panel de Cisco Meraki

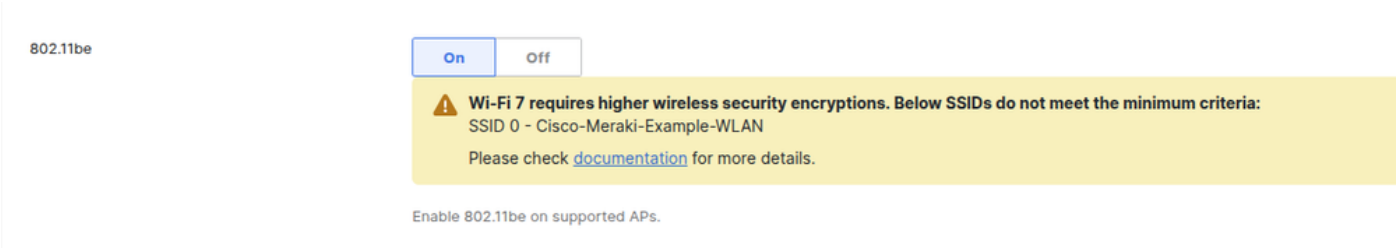
Al agregar puntos de acceso compatibles con Wi-Fi 7 (por ejemplo, CW9178I, CW9176I/D1) a

una red Cisco Meraki Dashboard por primera vez, la compatibilidad con el funcionamiento 802.11be se encuentra en su perfil de RF predeterminado.
Para activarlo, debemos navegar en Wireless > Radio Settings, hacer clic en la pestaña RF Profile y seleccionar el perfil asignado al AP (predeterminado: 'Perfil básico para interiores' para puntos de acceso interiores).

En la sección General, habilite 802.11be (encendido) como se muestra en esta captura de pantalla:

Si se configuran una o más WLAN con parámetros de seguridad más débiles que los requeridos por la especificación Wi-Fi 7, el panel muestra un banner que alerta a los usuarios, como se muestra a continuación.

Mientras que el panel permite guardar la configuración, Wi-Fi 7 no se activa en los SSID marcados hasta que se garantice el cumplimiento de los requisitos de Wi-Fi 7.
En el momento de escribir esto, todas las WLAN habilitadas en la red deben cumplir con los requisitos de la especificación Wi-Fi 7 para ser habilitadas en la versión de firmware MR 31.1.x y posteriores (este comportamiento cambia en una versión futura de firmware MR 32.1.x).



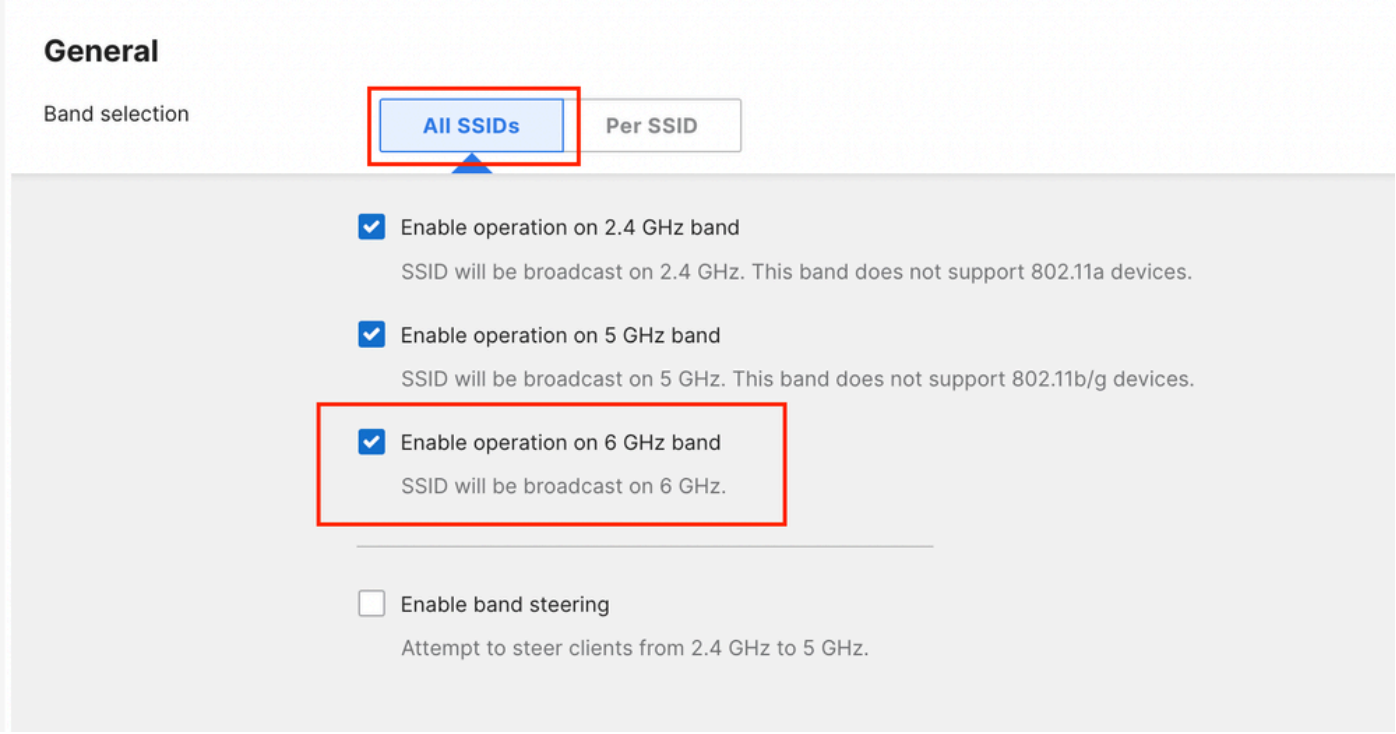
Una vez que la configuración del SSID cumple los criterios mínimos de Wi-Fi 7, el banner desaparece.

En el mismo perfil de RF, asegúrese de habilitar el funcionamiento de 6 GHz en los AP.

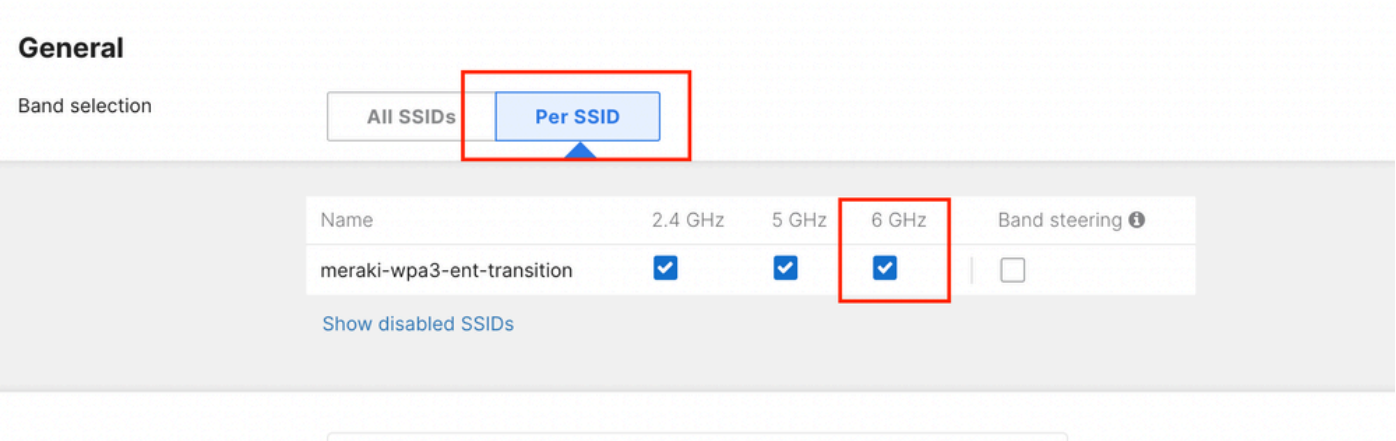
Esto se puede realizar para todos los SSID de forma masiva o por SSID individual.

Tenga en cuenta que la dirección en banda sólo está disponible entre 2,4 y 5 GHz.

Ejemplo de habilitación de 6 GHz para todos los SSID.



Ejemplo de habilitación de 6 GHz para un único SSID.



Casos de uso

Redes 802.1X / WPA3-Enterprise

Configuración WPA3-Enterprise en IOS XE

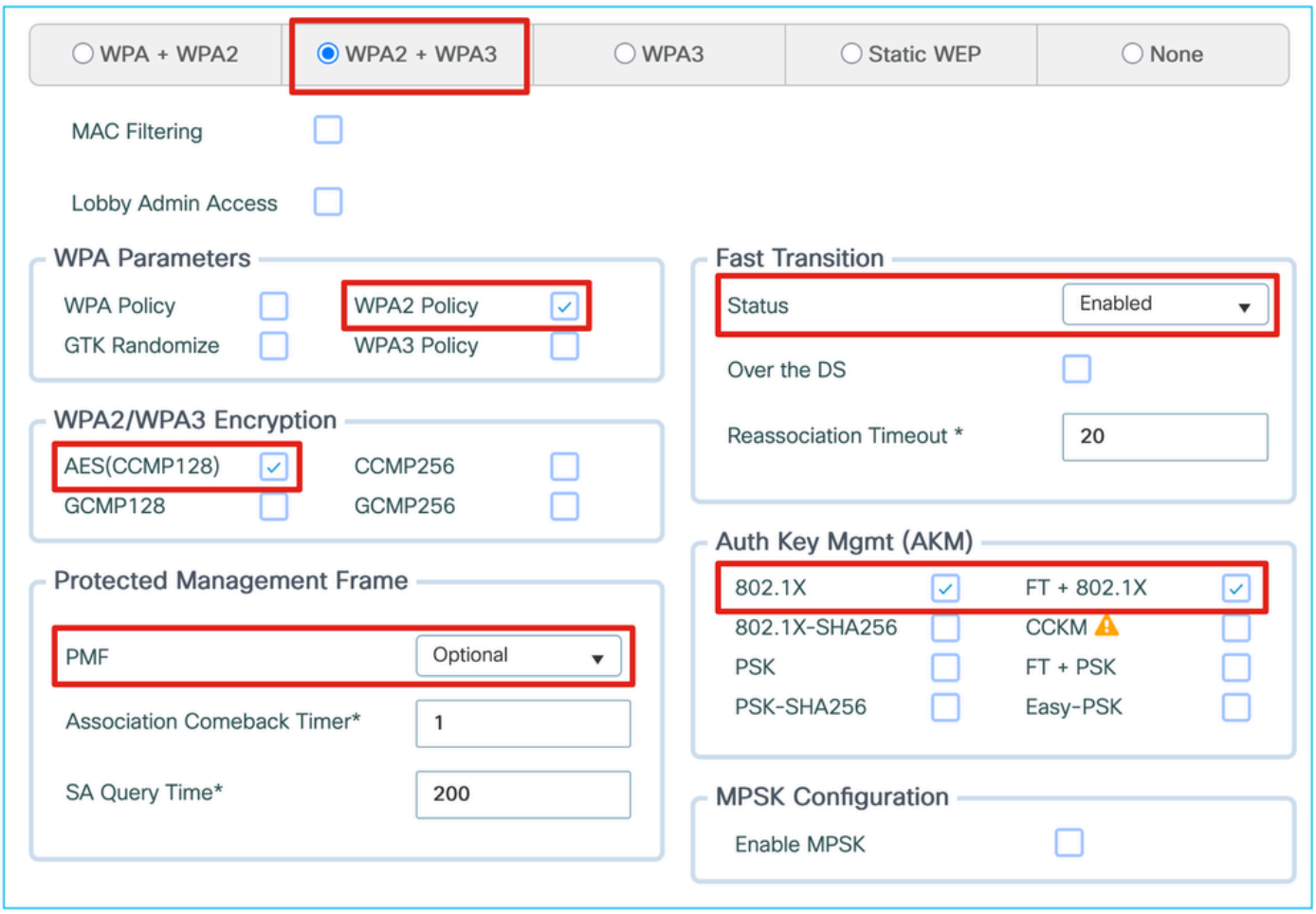
Las WLAN empresariales basadas en WPA2/3 con autenticación 802.1X son las más fáciles de migrar a 6 GHz o Wi-Fi 7.

Para activar el SSID 802.1X solo para 6 GHz es necesario activar la compatibilidad con PMF, incluso como opción, así como los AKM 802.1X-SHA256 y/o FT + 802.1X, ambos compatibles con WPA3.

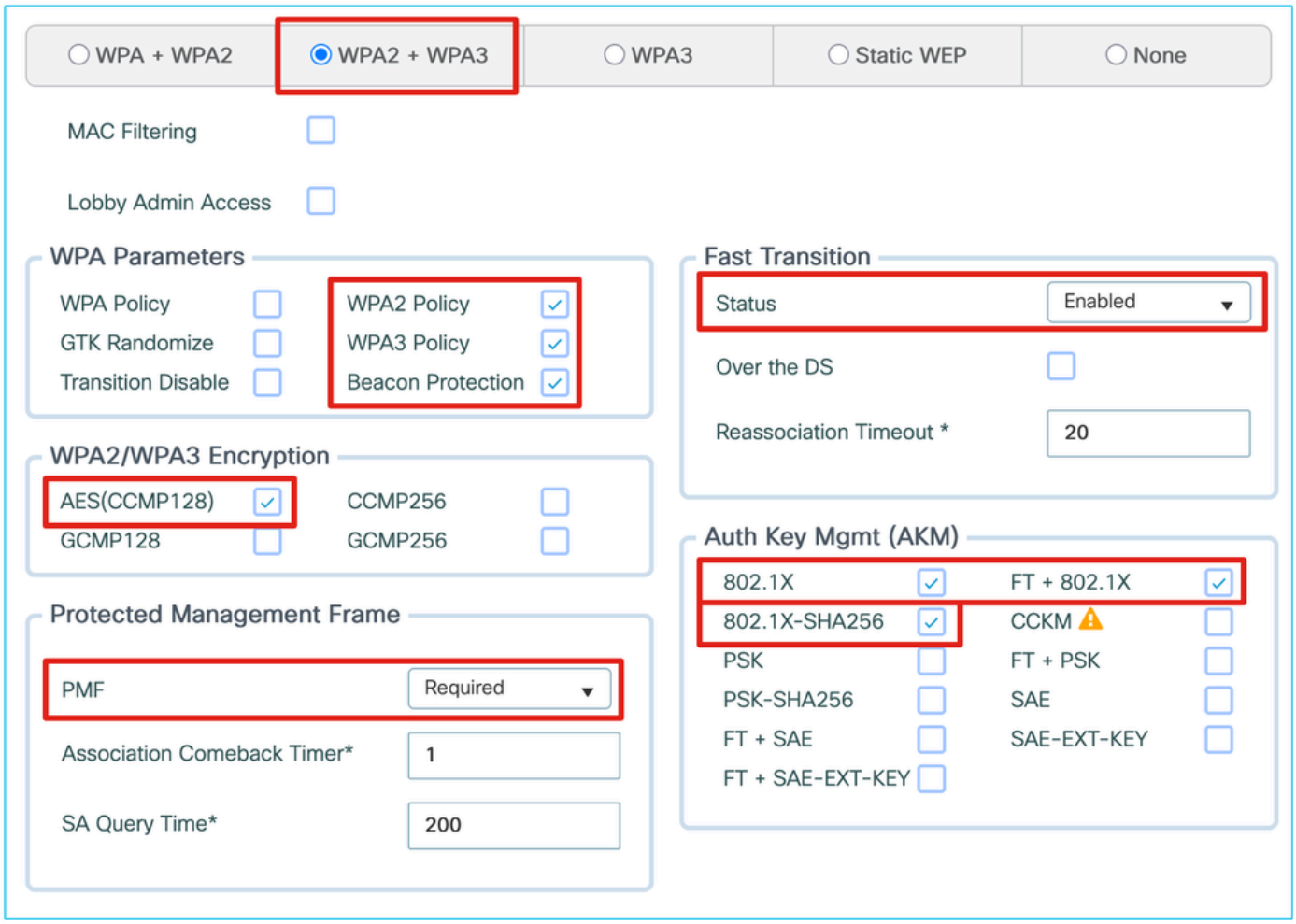
Podemos seguir ofreciendo WPA2 con 802.1X (SHA1) estándar en la misma WLAN. La

compatibilidad con Wi-Fi 7 requiere habilitar la protección de baliza y configurar PMF según sea necesario en lugar de opcionalmente. WPA2 802.1X (SHA1) puede permanecer presente en la WLAN como una opción de compatibilidad con versiones anteriores. Esto significa que puede tener todos los dispositivos corporativos bajo un solo SSID, siempre que sean compatibles con 802.11w/PMF, lo que es bastante común en las NIC inalámbricas actuales para portátiles y otros terminales móviles.

Desde un SSID WPA2 típico con estos parámetros de seguridad de capa 2:



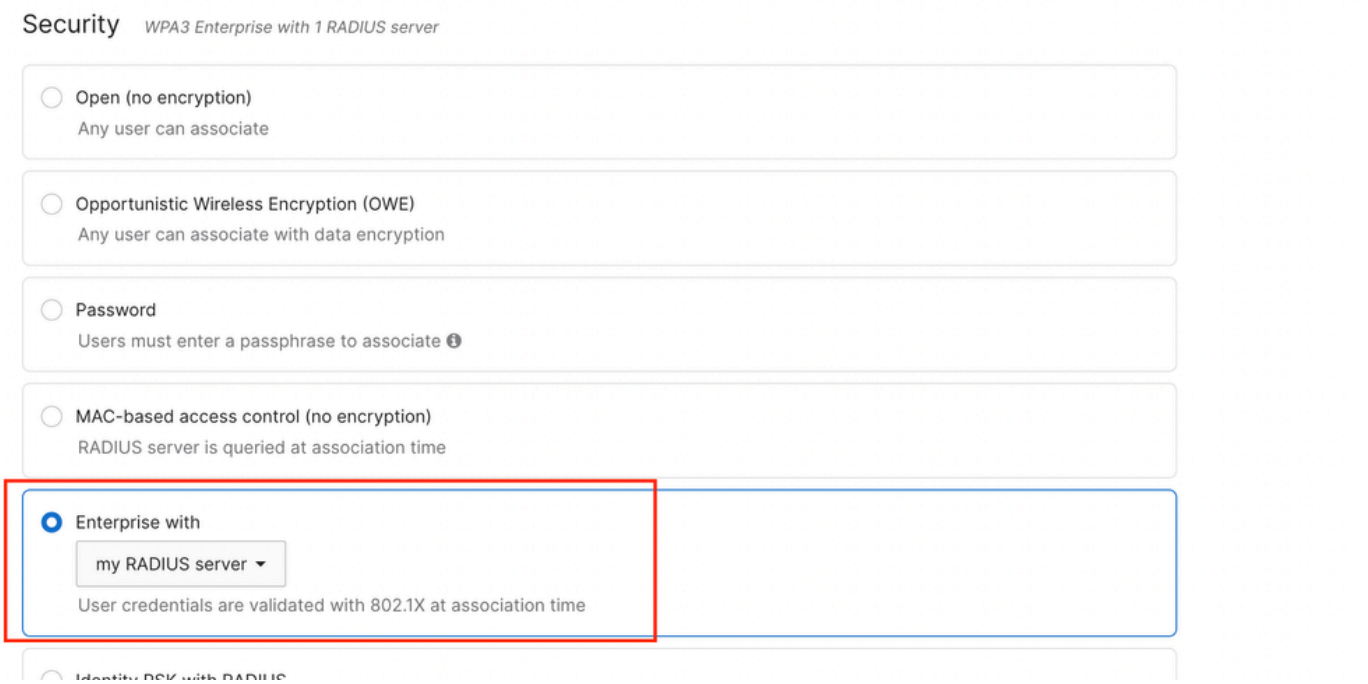
Podemos migrar la configuración para admitir WPA3, 6 GHz y Wi-Fi 7, tal y como se muestra a continuación:



Configuración de WPA3-Enterprise en el panel de Cisco Meraki

En el momento de escribir este documento, el funcionamiento de WPA3-Enterprise sólo está disponible con un servidor RADIUS externo (también denominado "mi servidor RADIUS").

WPA3-Enterprise no está disponible con la autenticación de nube de Meraki.



A partir de MR 31.x, los tipos WPA son:

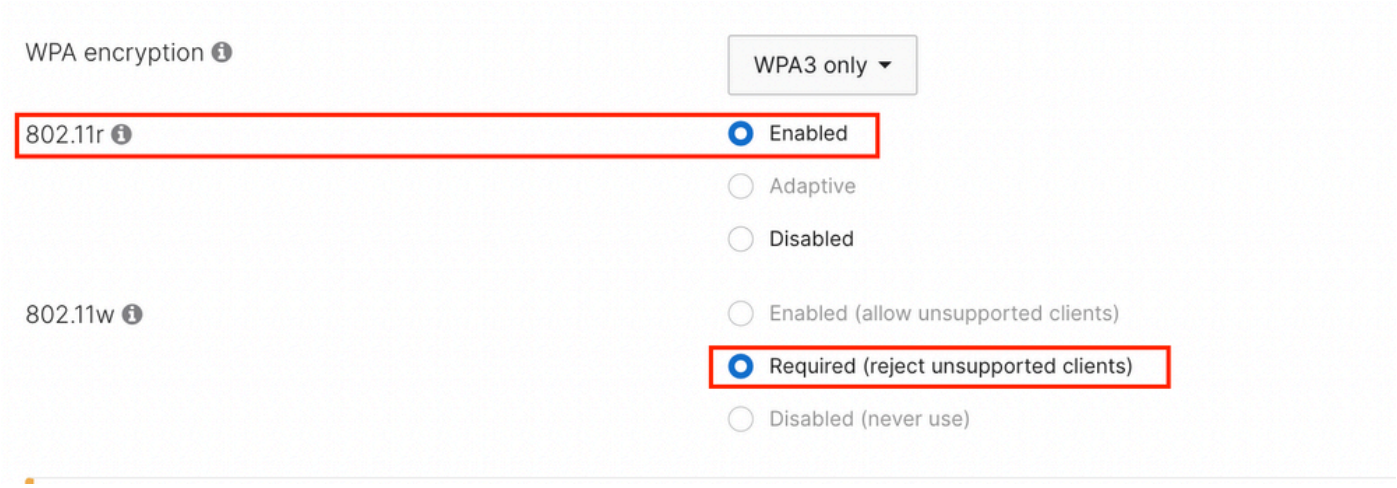
- 'Sólo WPA3', que utiliza los mismos cifrados que WPA2, pero requiere 802.11w (PMF).
- 'WPA3 de 192 bits', que sólo permite el método EAP-TLS con chips TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 o TLS_DHE_RSA_WITH_AES_256_GCM_SHA384. Este modo requiere la configuración de los mismos chips en el servidor RADIUS para habilitar este modo.
- 'Modo de transición WPA3' (también denominado modo mixto), que permite la coexistencia de clientes WPA2 en la misma WLAN utilizada para WPA3.

Al utilizar 'WPA3 only' (Sólo WPA3) o 'WPA3 192-bit Security' (Seguridad WPA3 de 192 bits), PMF es obligatorio para todos los clientes.

En la mayoría de las aplicaciones, FT (802.11r), aunque no es obligatorio, debe habilitarse mejor para mitigar el impacto de la latencia de itinerancia y reautenticación mientras se utiliza un

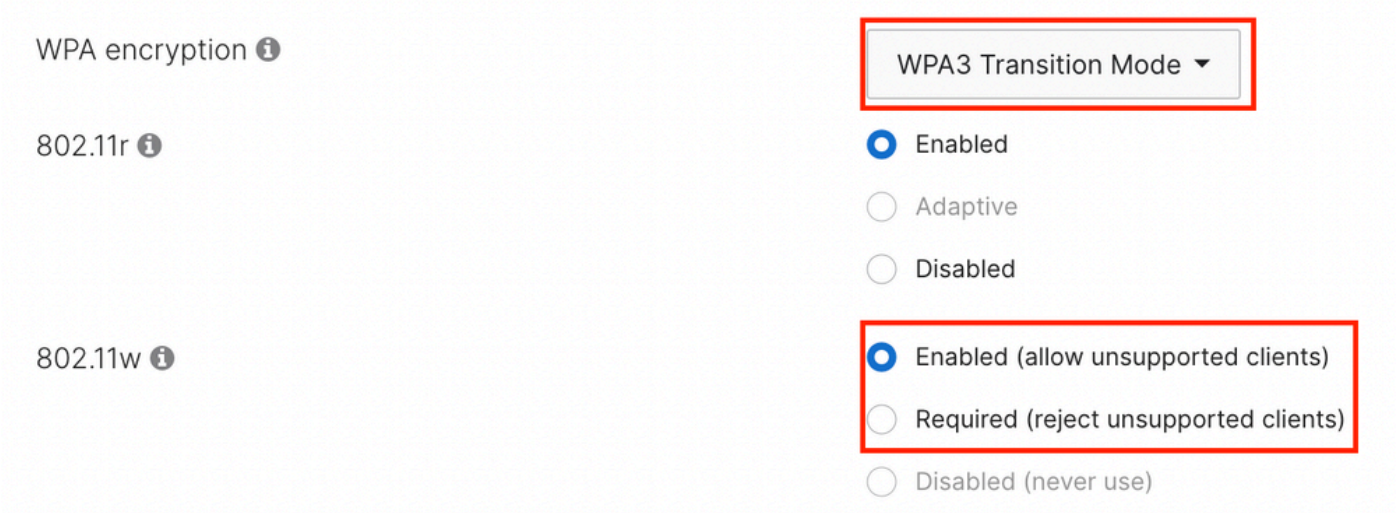
servidor RADIUS externo.

El funcionamiento a 6 GHz requiere la activación de PMF (802.11w).



Al seleccionar el modo de transición WPA3, todos los clientes que pueden utilizar WPA3 utilizan PMF de forma predeterminada. Todos los clientes que funcionan a 6 GHz utilizan WPA3.

En este modo, puede seleccionar si el cliente heredado que utiliza WPA2 debe utilizar PMF (se requiere 802.11w) o si esa función es opcional (802.11w habilitado).



Independientemente de la selección de WPA3, los puntos de acceso Cisco Meraki requieren que el conjunto de cifrado GCMP 256 esté habilitado para funcionar en modo Wi-Fi 7.

Además, la protección de baliza está activada de forma predeterminada en 2,4, 5 y 6 GHz cuando los puntos de acceso funcionan en modo Wi-Fi 7.

Frase de paso/redes WPA3-Personal/IoT

La activación de un SSID de frase de paso para 6 GHz, hasta la compatibilidad con Wi-Fi 6E, es sencilla y requiere SAE y/o FT + SAE, junto con otros AKM PSK WPA2 si es necesario. Sin embargo, para la compatibilidad con Wi-Fi 7, la certificación exige agregar AKM SAE-EXT-KEY y/o FT + SAE-EXT-KEY, junto con el cifrado GCMP256. Por lo tanto, no es posible tener una WLAN basada en una frase de contraseña con compatibilidad máxima para clientes más antiguos y rendimiento Wi-Fi 7.

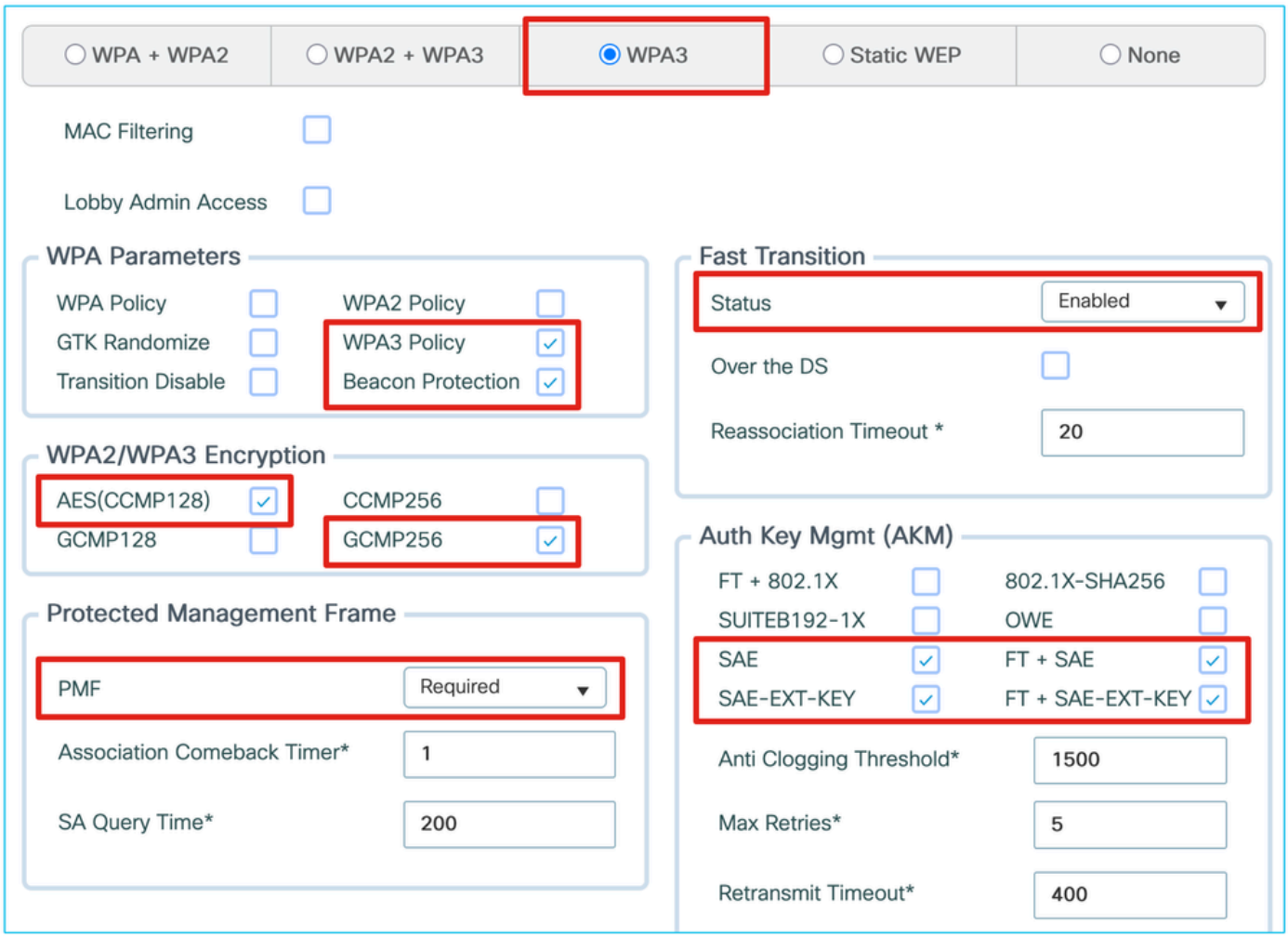
En estos casos, podemos configurar un SSID exclusivo para WPA3 con SAE, FT + SAE, SAE-EXT-KEY y FT + SAE-EXT-KEY, que ofrezca cifrado AES (CCMP128) y GCMP256, para clientes Wi-Fi 6E y Wi-Fi 7 más recientes.

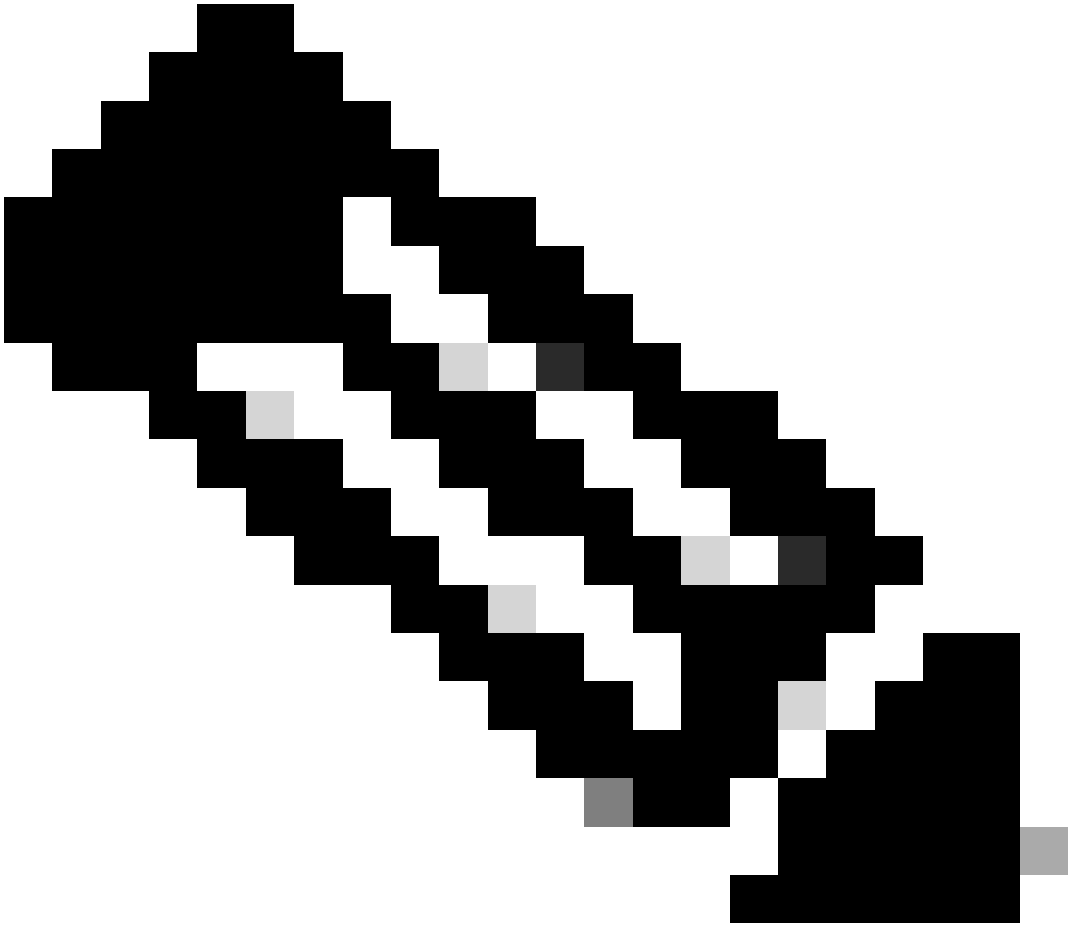
Es posible tener una WLAN de modo de transición que permita WPA2 PSK, además de WPA3 SAE y SAE-EXT, pero esto representa 6 AKM (si se utiliza FT) y algunos clientes de derecha podrían potencialmente tener un problema con eso. Le recomendamos que pruebe esta posibilidad con sus clientes si decide optar por el modo de transición WPA2-PSK+WPA3-SAE+SAE-EXT + FT.

En todos estos casos, se recomienda encarecidamente habilitar FT al utilizar SAE. El intercambio de tramas SAE es costoso en términos de recursos y más largo que el protocolo de enlace de 4 vías WPA2 PSK.

Algunos fabricantes de dispositivos como Apple esperan utilizar SAE solo cuando FT está habilitado y pueden negarse a conectarse si no está disponible.

Configuración de WPA3-SAE y WPA2-Personal en IOS XE

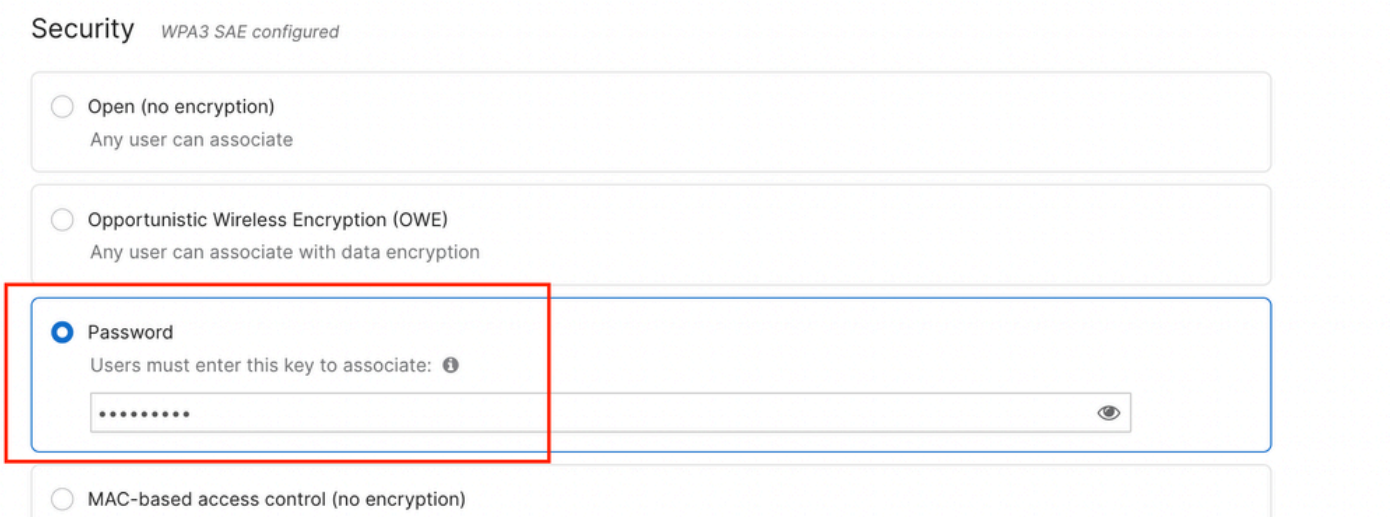

WPA + WPA2
WPA2 + WPA3
WPA3
Static WEP
None
MAC Filtering
Lobby Admin Access
WPA Parameters
WPA Policy
WPA2 Policy
GTK Randomize
WPA3 Policy
Transition Disable
Beacon Protection
WPA2/WPA3 Encryption
AES(CCMP128)
CCMP256
GCMP128
GCMP256
Protected Management Frame
PMF
Required
Association Comeback Timer*
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



Nota: Si (FT +) SAE está activado en la WLAN y un cliente Wi-Fi 7 intenta asociarse con él en lugar de (FT +) SAE-EXT-KEY, se rechaza. Siempre que (FT +) SAE-EXT-KEY también esté habilitado, los clientes Wi-Fi 7 deben utilizar este último AKM, y este problema no debe ocurrir.

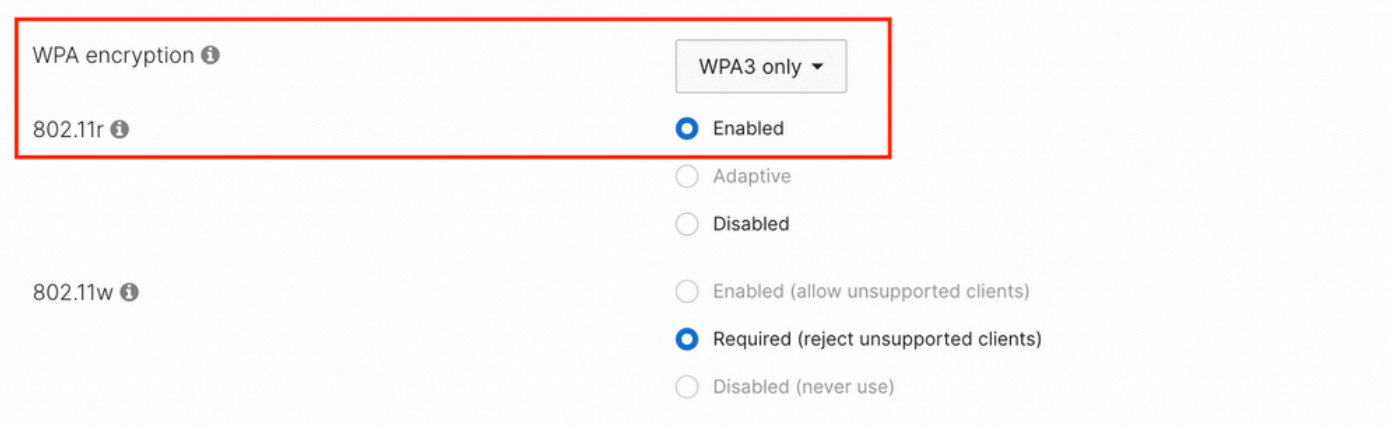
Aunque el uso de una WLAN heredada con solo PSK en una WLAN solo WPA-3 aumenta la cantidad total de SSID, permite mantener la máxima compatibilidad en un SSID, donde también podemos deshabilitar otras funciones avanzadas que podrían afectar a la compatibilidad y que podrían ser útiles para muchos escenarios de IoT, al tiempo que ofrece las máximas características y rendimiento a los dispositivos más recientes a través del otro SSID. Este puede ser el escenario preferido si tiene dispositivos de IoT más antiguos o más sensibles en la imagen. Si no tiene dispositivos IoT, optar por una WLAN de modo de transición único puede ser más eficiente, ya que solo se anuncia un SSID.

Configuración de WPA3-SAE en el panel de Cisco Meraki



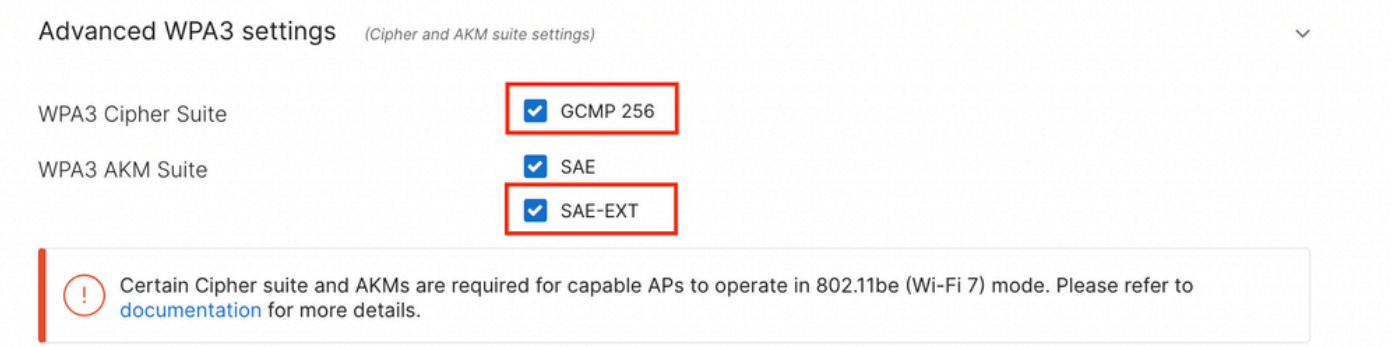
Hasta el firmware MR 30.x, el único tipo WPA admitido es 'Sólo WPA3' y el panel no permite seleccionar un método diferente.

PMF es obligatorio en esta configuración, mientras que FT (802.11r) se recomienda que esté habilitado cuando se utilice SAE.



Para permitir el funcionamiento de Wi-Fi 7, el conjunto de chips GCMP 256 y el conjunto AKM SAE-EXT deben activarse tras la configuración del SSID.

Están desactivados de forma predeterminada y se pueden activar en 'Configuración avanzada de WPA3'.



En el momento de escribir esto, todas las WLAN habilitadas en la red deben cumplir con los

requisitos de la especificación Wi-Fi 7 para poder habilitarse en la versión de firmware MR 31.1.x y posteriores.

Esto significa que un SSID Wi-Fi 7 configurado como se ha descrito anteriormente no puede coexistir con otro SSID mediante el modo de transición WPA2-Personal o WPA3-SAE.

Si se configura un SSID WPA2-Personal en la red del panel de control, todos los puntos de acceso Wi-Fi 7 volverían al funcionamiento Wi-Fi 6E.

Este comportamiento cambia en una versión futura del firmware MR 32.1.x.

Redes abiertas/abiertas mejoradas/OWE/invitados

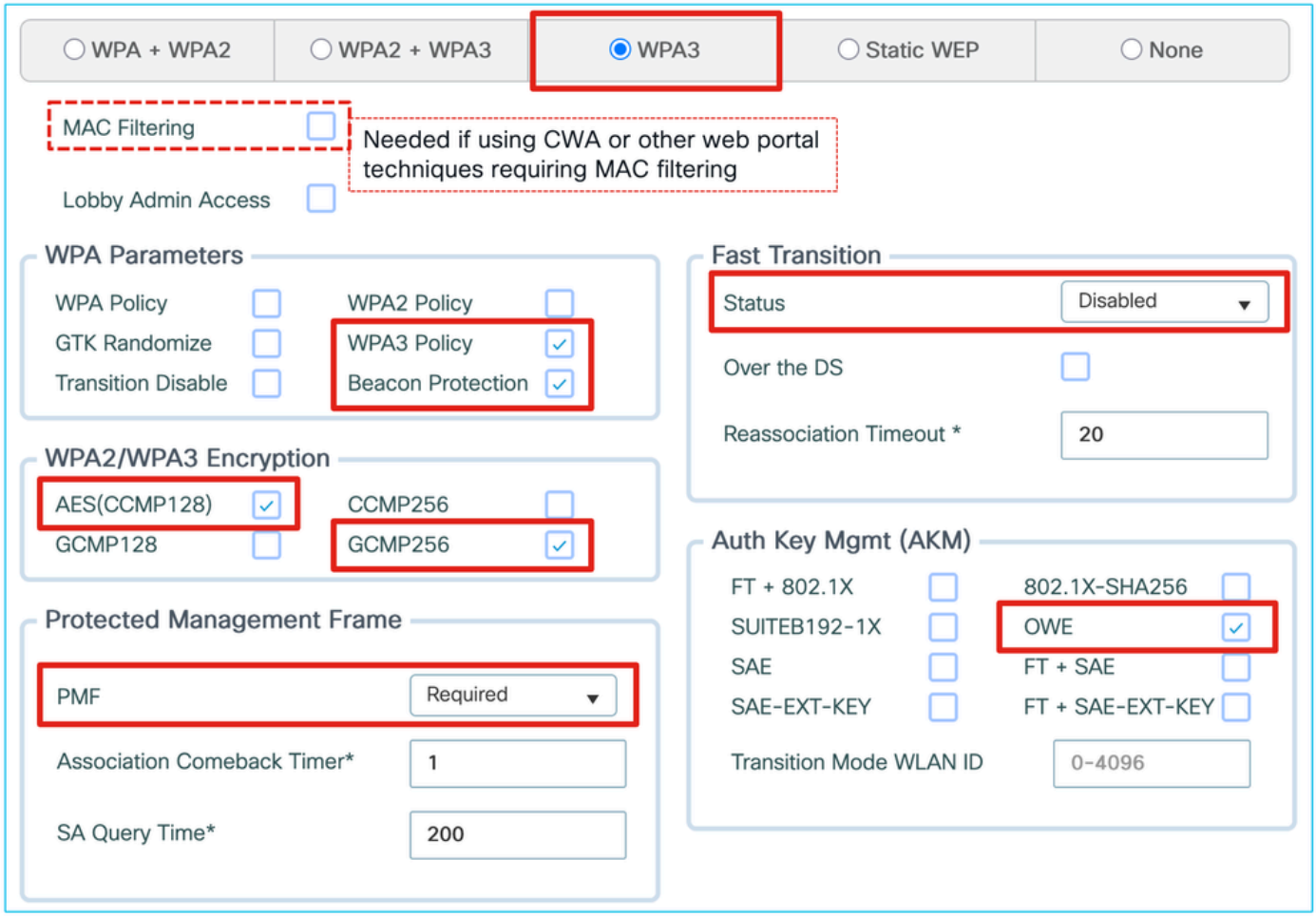
Las redes para invitados tienen muchos sabores. Normalmente, no requieren credenciales ni frase de contraseña 802.1X para conectarse y posiblemente implican una página de bienvenida o un portal, que pueden requerir credenciales o un código. Tradicionalmente, esto se gestiona con un SSID abierto y soluciones de portal de invitados locales o externos. Sin embargo, los SSID con seguridad abierta (sin encriptación) no están permitidos en 6 GHz ni son compatibles con Wi-Fi 7.

Un primer enfoque muy conservador sería dedicar las redes de invitados a la banda de 5 GHz y Wi-Fi 6, en el mejor de los casos. Esto deja la banda de 6 GHz reservada para los dispositivos corporativos, soluciona el problema de complejidad y ofrece la máxima compatibilidad, aunque no llega hasta el rendimiento de Wi-Fi 6E/7.

Si, por un lado, Enhanced Open es un excelente método de seguridad que ofrece privacidad mientras mantiene la experiencia de "apertura" (los usuarios finales no necesitan introducir ninguna frase de contraseña o credencial 802.1X), hasta el día de hoy sigue teniendo una compatibilidad limitada entre los terminales. Algunos clientes siguen sin admitirlo e, incluso cuando lo hacen, esta técnica no siempre se gestiona sin problemas (el dispositivo puede mostrar la conexión como no segura, mientras que en realidad es segura, o puede mostrarla como protegida por una frase de paso, incluso si no se necesita ninguna frase de paso con OWE). Se espera que una red para invitados funcione en todos los dispositivos no controlados para invitados. Puede que sea demasiado pronto para proporcionar un SSID abierto mejorado y se recomienda proporcionar ambas opciones a través de SSID independientes: una abierta a 5 GHz y una OWE habilitada a 5 y 6 GHz, ambas con el mismo portal cautivo detrás si esto también es un requisito. El modo de transición no es compatible con Wi-Fi 6E, 6 GHz (aunque todavía se puede permitir en el software) o Wi-Fi 7, por lo que no es una solución recomendada. Todas las técnicas de redirección del portal (autenticación web interna o externa, autenticación web central, ...) siguen siendo compatibles con OWE.

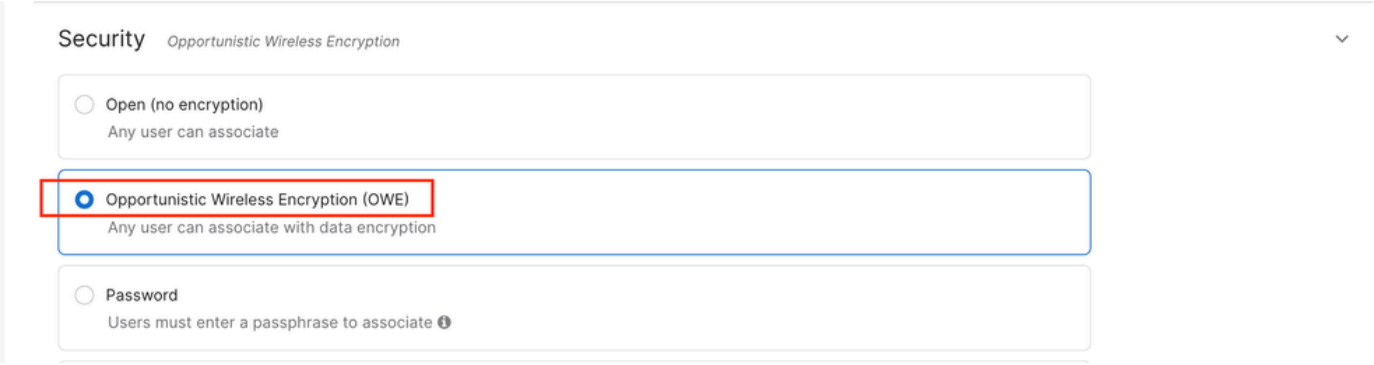
Configuración OWE en IOS XE

Si deseamos proporcionar un servicio de 6 GHz a los invitados, se recomienda crear un SSID independiente con Enhanced Open / OWE (cifrado inalámbrico oportunista). Podría ofrecer cifrado AES (CCMP128), para una compatibilidad máxima hasta clientes Wi-Fi 6E, así como bits GCMP256 para clientes con capacidad Wi-Fi 7.



Configuración OWE en el panel de Cisco Meraki

De forma similar a lo que se hizo en IOS XE, se recomienda crear un SSID de invitado independiente con apertura/OWE mejorada que funcione a 6 GHz en el panel de Cisco Meraki. Esto se puede configurar nuevamente en Wireless > Access Control, y seleccionando 'Opportunistic Wireless Encryption (OWE)' como el método de seguridad.



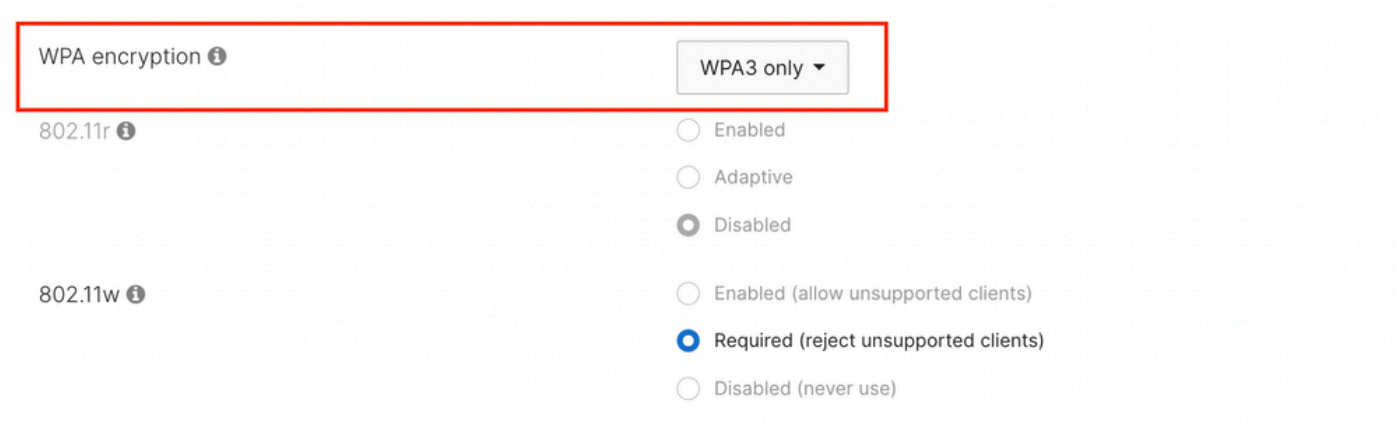
Cuando se ejecuta firmware hasta MR 31, el único tipo WPA admitido es 'Sólo WPA3' y el panel no permite seleccionar un método diferente.

PMF es obligatorio en esta configuración, mientras que FT (802.11r) no se puede habilitar.

Tenga en cuenta que la etiqueta 'Solo WPA3' está sobrecargada, ya que OWE no forma parte del

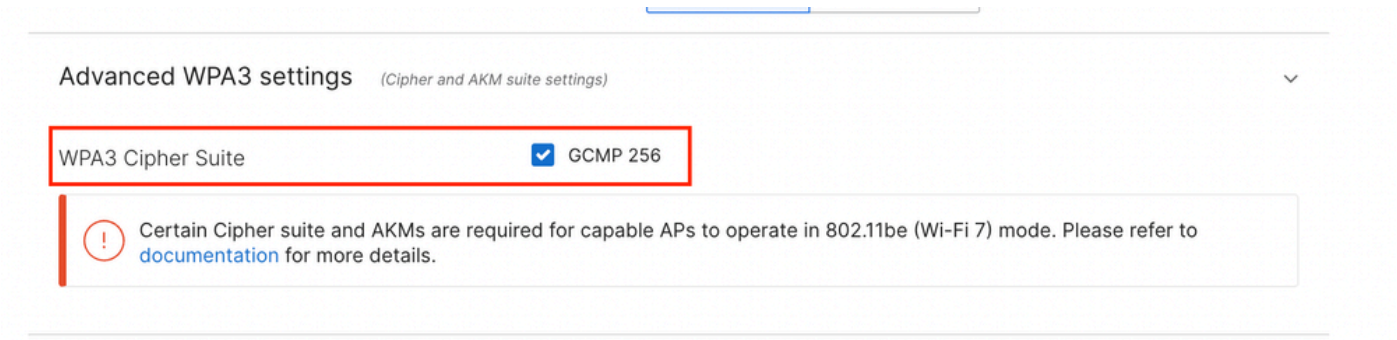
estándar WPA3; sin embargo, esta configuración se refiere a OWE sin modo de transición.

El modo de transición OWE está disponible como parte de una futura versión de MR 32.1.x.



El cifrado AES (CCMP128) está activado de forma predeterminada para ofrecer la máxima compatibilidad hasta los clientes Wi-Fi 6E.

Los bits GCMP256 se pueden habilitar junto con CCMP128 para cumplir con los requisitos de Wi-Fi 7.



WPA3 adicional y opciones relacionadas

Aunque las opciones de WPA3 se describen mejor y se tratan en la guía de implementación de WPA3, en esta sección se tratan algunas recomendaciones adicionales para WPA3 relacionadas específicamente con la compatibilidad con 6 GHz y Wi-Fi 7.

Protección de baliza

Se trata de una función que soluciona la vulnerabilidad, en la que un atacante malintencionado puede transmitir balizas en lugar del punto de acceso legítimo, al tiempo que modifica algunos campos para cambiar la seguridad u otras configuraciones de clientes ya asociados. La protección de baliza es un elemento de información adicional (Management MIC) de la baliza que actúa como firma de la propia baliza para demostrar que la ha enviado el punto de acceso legítimo y que no se ha manipulado. Sólo los clientes asociados con una clave de cifrado WPA3 pueden verificar la legitimidad de la baliza; los clientes de sondeo no tienen medios para verificarlo. Los clientes que no lo admitan simplemente deben ignorar el elemento de información

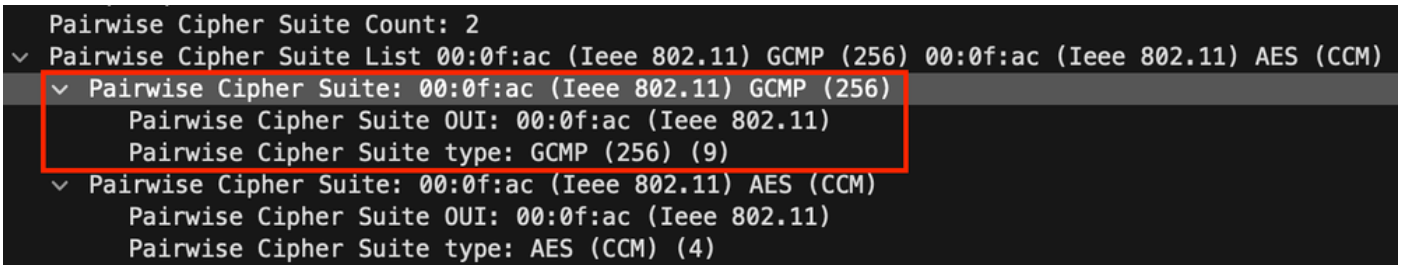
adicional de la baliza (esto se refiere a clientes que no son Wi-Fi 7) y, normalmente, no causa problemas de compatibilidad (a menos que se trate de un controlador de cliente mal programado).

Esta captura de pantalla muestra un ejemplo del contenido del elemento de información Management MIC:

GCMP256

Hasta la certificación Wi-Fi 7, la mayoría de los clientes implementaban el cifrado AES (CCMP128). CCMP256 y GCMP256 son variantes muy específicas relacionadas con SUITE-B 802.1X AKM. Aunque algunas primeras generaciones de clientes Wi-Fi 7 en el mercado afirman que son compatibles con Wi-Fi 7, a veces siguen sin implementar el cifrado GCMP256, que puede convertirse en un problema si los puntos de acceso Wi-Fi 7 que aplican el estándar como se esperaba impiden que estos clientes se conecten sin el soporte GCMP256 adecuado.

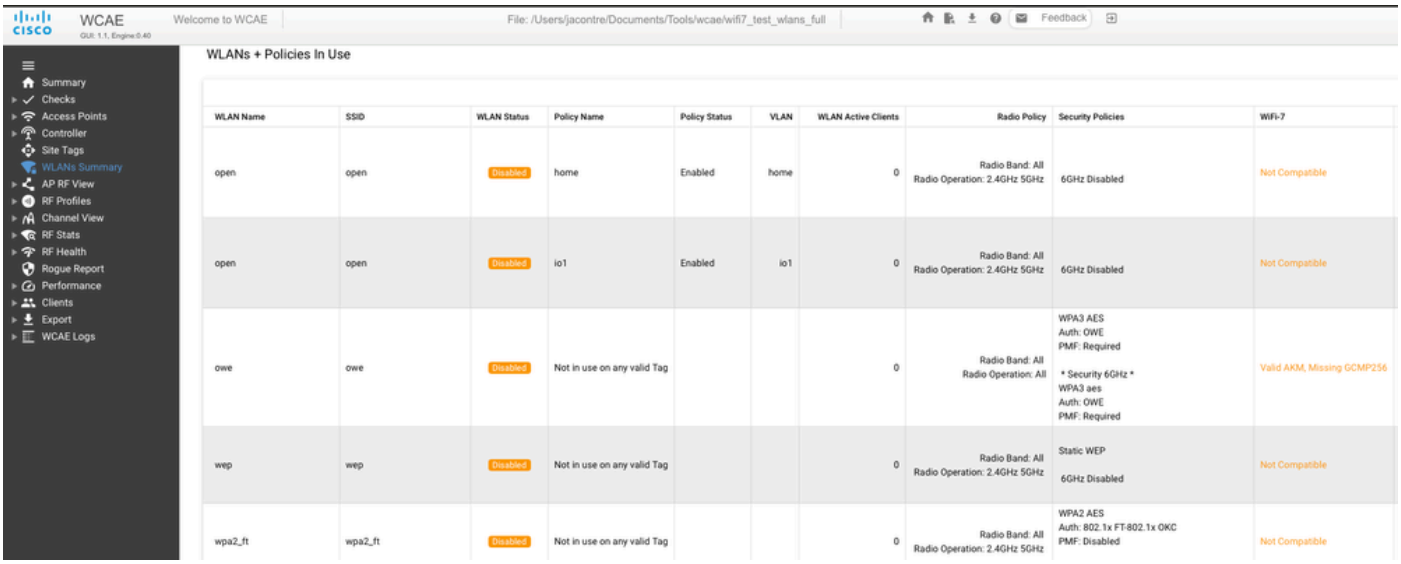
Cuando se habilita GCMP256, el Elemento de red de seguridad robusto (RSNE) en las tramas de baliza para la WLAN anuncia la capacidad en la Lista de conjuntos de chips de pares como se muestra aquí.



Solucionar problemas y comprobar

La última versión de Wireless Configuration Analyzer Express (https://developer.cisco.com/docs/wireless-troubleshooting-tools/wireless-config-analyzer-express-gui/) incluye una comprobación de preparación para Wi-Fi 7 que evalúa la configuración 9800 para todos los requisitos de Wi-Fi 7 mencionados anteriormente.

Si todavía tiene dudas sobre si su configuración está preparada para Wi-Fi 7, WCAE le permite saber qué es lo que está mal.



Referencias

1. Cisco Systems. "Guía de configuración y cifrado WPA3".
2. Guía de Meraki WPA3

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).