借助思科无线迁移至6 GHz和Wi-Fi 7

目录

简介

- CX设计指南

为什么选择6 GHz和Wi-Fi 7

6 GHz操作和Wi-Fi 7的基本要求

- 6 GHz频段要求
- Wi-Fi 7要求
  - Cisco IOS® XE 17.15.3及更高版本17.15.x
  - Cisco IOS XE 17.18.1/17.18.2
  - Cisco IOS XE 17.18.3及更高版本

6 GHz覆盖的无线电设计注意事项

- 在Wi-Fi 6E/7之前和Wi-Fi 6E/7 AP之间的漫游行为

全局启用Wi-Fi 7

- 在Cisco IOS XE上全局启用Wi-Fi 7
- 在Cisco Meraki控制面板上全局启用Wi-Fi 7

使用案例

- 802.1X / WPA3 — 企业网络
  - Cisco IOS XE上的WPA3-Enterprise配置
  - Cisco Meraki控制面板上的WPA3-Enterprise配置
- 口令/ WPA3 — 个人/ IoT网络
  - Cisco IOS XE上的WPA3-SAE配置
  - Cisco Meraki控制面板上的WPA3-SAE配置
- 开放/增强型开放/OWE/访客网络
  - Cisco IOS XE上的OWE配置
  - Cisco Meraki控制面板上的OWE配置

其他WPA3和相关选项

- 信标保护
- GCMP256

故障排除和验证

- 故障排除核对表

参考

简介

本文档介绍设计和配置指南，以优化Wi-Fi 7的性能并充分利用6 GHz频谱。

CX设计指南



CX设计指南由思科CX的专家与其他部门的工程师协作编写，并由思科内部的专家进行同行审查；这些指南基于思科领先实践，以及多年来从无数客户实施中获得的知识和经验。按照本文档的建议设计和配置网络有助于避免常见缺陷并改善网络运行。

为什么选择6 GHz和Wi-Fi 7

2020年，6 GHz频段开始可用于WLAN运营，Wi-Fi 6E认证需要该频段。虽然Wi-Fi 6在2.4 GHz和5 GHz频段中运行，但Wi-Fi 6E使用相同的IEEE 802.11ax标准，但将其功能扩展至6 GHz频段，前提是满足特定要求。

新的Wi-Fi 7认证基于IEEE 802.11be标准，支持2.4 GHz、5 GHz和6 GHz频段的操作。与之前的认证相比，Wi-Fi 7还引入了新的功能和增强功能。

支持6 GHz频段和/或Wi-Fi 7具有特定要求，通常需要新的配置和RF设计，尤其是与采用Wi-Fi 6的2.4 GHz和5 GHz频段的既定做法相比。

例如，正如使用过时的WEP安全阻止在802.11a/b/g之后采用802.11标准一样，新标准也会强制实施更严格的安全必备条件，以鼓励部署更安全的网络。

相反，6 GHz频段的引入提供了更清洁的频率、改进的性能以及对新使用案例的支持。它还可以更无缝地实施现有应用，例如语音和视频会议。

6 GHz操作和Wi-Fi 7的基本要求

这些是6 GHz和Wi-Fi 7运营认证规定的安全要求。

6 GHz频段要求

6 GHz频段仅允许WPA3或增强型开放式WLAN，这意味着以下安全选项之一：

- 采用802.1X身份验证的WPA3-Enterprise
- 带有密码的WPA3对等同时身份验证(SAE)（也称为WPA3 — 个人）。SAE-FT(SAE with Fast

Transition)是另一种可能的AKM，建议使用SAE握手，因为SAE握手并非无关紧要，并且FT允许跳过更长的交换。
- 通过机会无线加密(OWE)增强开放性

尽管WPA3 v3.4规范（第11.2节）指出6 GHz不支持增强型开放式过渡模式，但许多供应商（包括思科至Cisco IOS XE 17.18）尚未实施此限制。因此，在技术上，可以配置（例如）5 GHz的开放式SSID和5 GHz和6 GHz的相应增强型开放式SSID，两者都启用转换模式，而不遵守标准规范。但是，在这种情况下，请改为配置无转换模式且仅在6 GHz上可用的增强型开放SSID（支持6 GHz的客户端通常也支持增强型开放），同时保持我们的常规开放SSID在5 GHz上且无转换模式。

除了802.11w/保护管理帧(PMF)实施外，WPA3-Enterprise没有新的特定密码或算法要求。许多供应商（包括思科）只认为802.1X-SHA256或“FT + 802.1X”（802.1X采用SHA256和快速过渡）符合WPA3。普通802.1X（使用SHA1）被认为是WPA2的一部分，因此不适用于6 GHz或受支持。

Wi-Fi 7要求

通过802.11be标准的Wi-Fi 7认证，Wi-Fi联盟提高了安全要求。其中一些要求允许使用802.11be数据速率和协议改进，而其他要求支持多链路操作(MLO)，允许兼容设备（客户端和/或AP）使用多个频段，同时保持相同的关联。

一般来说，Wi-Fi 7要求使用以下安全类型之一：

- WPA3-Enterprise，带AES(CCMP128)和802.1X-SHA256或FT + 802.1X（仍然使用SHA256，即使其名称不明确也是如此）。 较新的WPA3规范(v3.4)将要求更改为“AP必须提供GCMP256算法”，即使客户端仍允许使用AES128。这会导致客户端行为差异：有些客户端尝试将Wi-Fi 7企业版与AES128配合使用，而另一些客户端则已期望GCMP256。
- WPA3 — 个人，带GCMP256和SAE-EXT-KEY和/或FT + SAE-EXT-KEY（AKM 24或25）。Wi-Fi 6E要求使用常规AES(CCMP128)的WPA3 SAE和/或FT + SAE，且无需额外的扩展密钥使用；这意味着专门为Wi-Fi 7引入了一个新密码。
- GCMP256的增强型开放/OWE。虽然AES(CCMP128)仍然可以在同一个SSID上配置，但使用AES 128的客户端不支持Wi-Fi 7。在Wi-Fi 7之前，大多数支持增强型开放的客户端仅使用AES 128，因此这是一个新的、更强大的要求。对于6 GHz支持，不允许转换模式。

无论选择哪种安全类型，都需要受保护管理帧(PMF)和信标保护来支持WLAN上的Wi-Fi 7。

由于Wi-Fi 7在撰写本文时仍属于最新认证，因此许多供应商从一开始就没有强制执行这些安全要求。

最近，思科逐步实施了符合Wi-Fi 7认证要求的配置选项。以下是版本特定的行为：

Cisco IOS® XE 17.15.3及更高版本17.15.x

在此分支机构中，所有WLAN均以Wi-Fi 7 SSID形式广播，前提是Wi-Fi 7全局启用，无论安全设置如何。

客户端可以关联为支持Wi-Fi 7的设备，并实现Wi-Fi 7数据速率，无论其使用何种安全方法，前提是WLAN支持该方法。但是，客户端只有在满足严格的Wi-Fi 7安全要求时，才能够关联为支持MLO的（在一个或多个频段上）；否则，将被拒绝。

当早期不支持更安全密码的Wi-Fi 7客户端（例如GCMP256）尝试与其安全设置不符合Wi-Fi 7要求的WLAN建立MLO关联时，可能会导致问题。在这种情况下，客户端会因为无效的安全设置而被拒绝，即使这些设置仍可以在WLAN上配置。

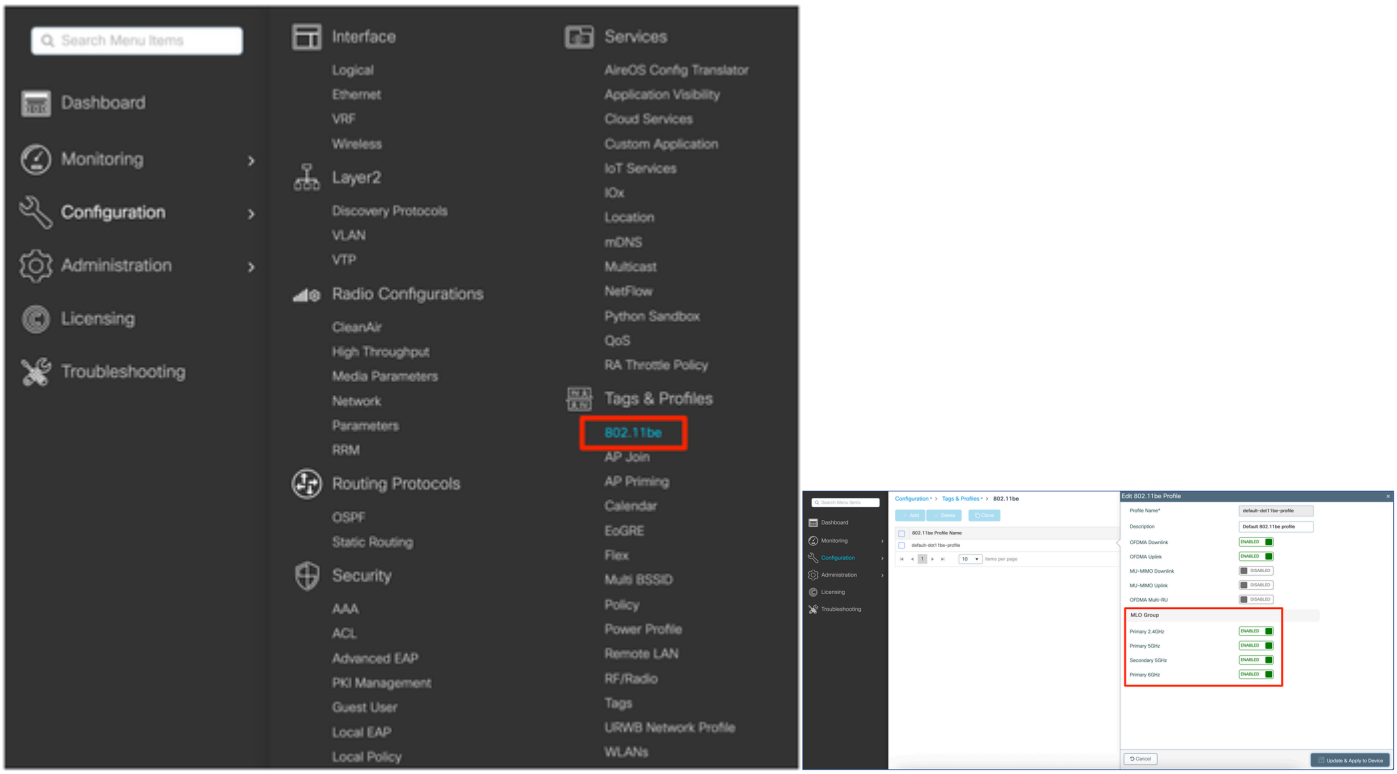
Cisco IOS XE 17.18.1/17.18.2

如果WLAN符合Wi-Fi 7，则自动启用信标保护，无论您是否启用该复选框。

只有在WLAN设置中启用了适当的安全要求时，Cisco IOS XE 17.18.1及更高版本才会将WLAN通告为Wi-Fi 7和MLO。例如，仅通告SAE而非SAE-EXT的WLAN将广播为MLO不支持。

17.18分支引入可以连接到WLAN配置文件的802.11be配置文件，以控制每个SSID甚至每个无线电的Wi-Fi 7激活。

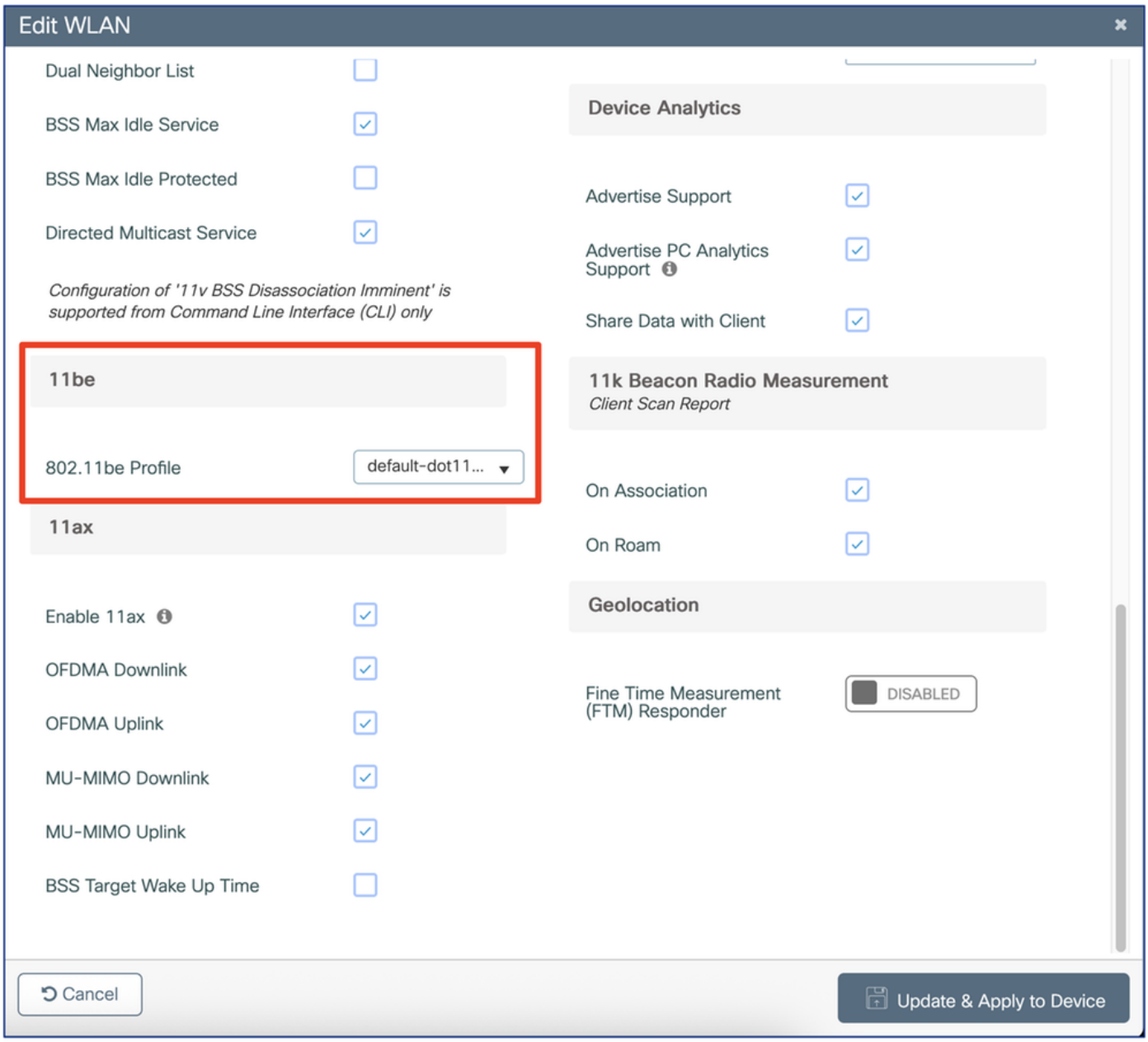
默认情况下，名为“default-dot11be-profile”的预配置802.11be配置文件在新的Configuration > Tags & Profiles > 802.11be菜单下可用。



启用或禁用Wi-Fi 7的四个主要设置位于“MLO组”部分下。禁用所有四个设置会禁用802.11be配置文件所连接的任何WLAN配置文件中的每个频段上的Wi-Fi 7。启用部分或全部这些功能可在所连接的WLAN配置文件的相应频段/无线电上启用Wi-Fi 7。

“default-dot11be-profile”在所有无线电上启用MLO和Wi-Fi 7，并且默认连接到每个WLAN配置文件。
通过创建一个新的802.11be配置文件，禁用所有“MLO组”设置，并将其连接到特定的WLAN配置文件，例如，我们可以为我们的某些SSID选择性地禁用Wi-Fi 7。

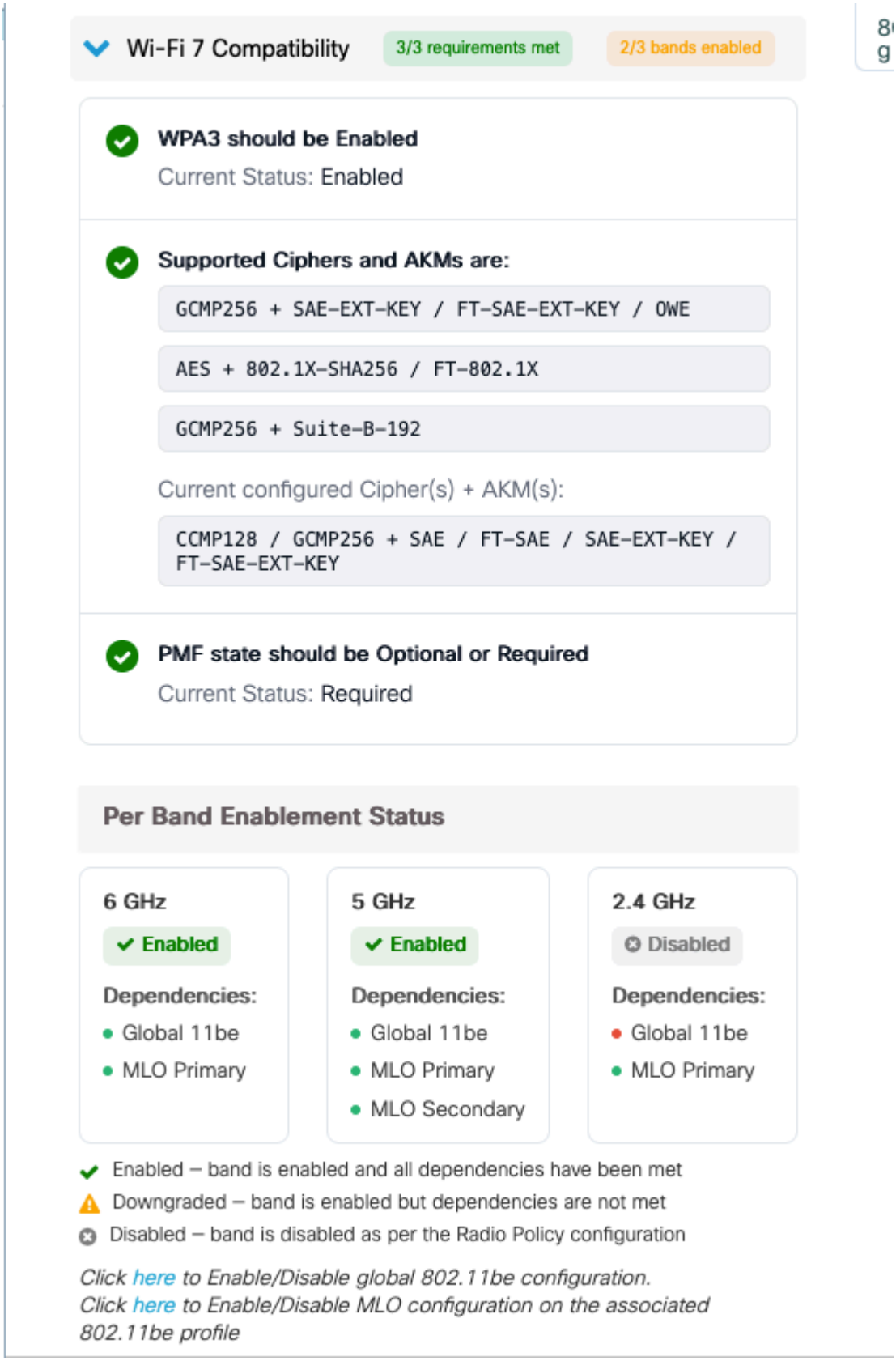
在每个WLAN配置文件的“高级”设置选项卡下，会附加相应的802.11be配置文件：



如示例所示，“default-dot11be-profile”默认附加到任何WLAN配置文件。

注意：如果在控制器上未全局启用Wi-Fi 7（如后所述），则所有WLAN配置文件均禁用Wi-Fi 7，且未应用802.11be配置文件。

17.18.2在WLAN编辑页面中引入了一个小型向导，可帮助您查看WLAN是否符合Wi-Fi 7标准，并显示缺少的内容：



17.18.2安全向导

Cisco IOS XE 17.18.3及更高版本

Cisco IOS 17.18.3允许您为802.1X企业SSID配置GCMP256密码，这在早期版本中是不可能的。这

满足了某些客户端对Wi-Fi 7企业SSID的要求，以便除AES128密码外提供GCMP256，并符合WPA3 v3.4规范。

如果在升级之前您的SSID符合Wi-Fi 7,GCMP256会在升级时自动添加到您的配置中，以避免在升级到17.18.3后未启用GCMP256时，SSID降级为Wi-Fi 6E SSID。

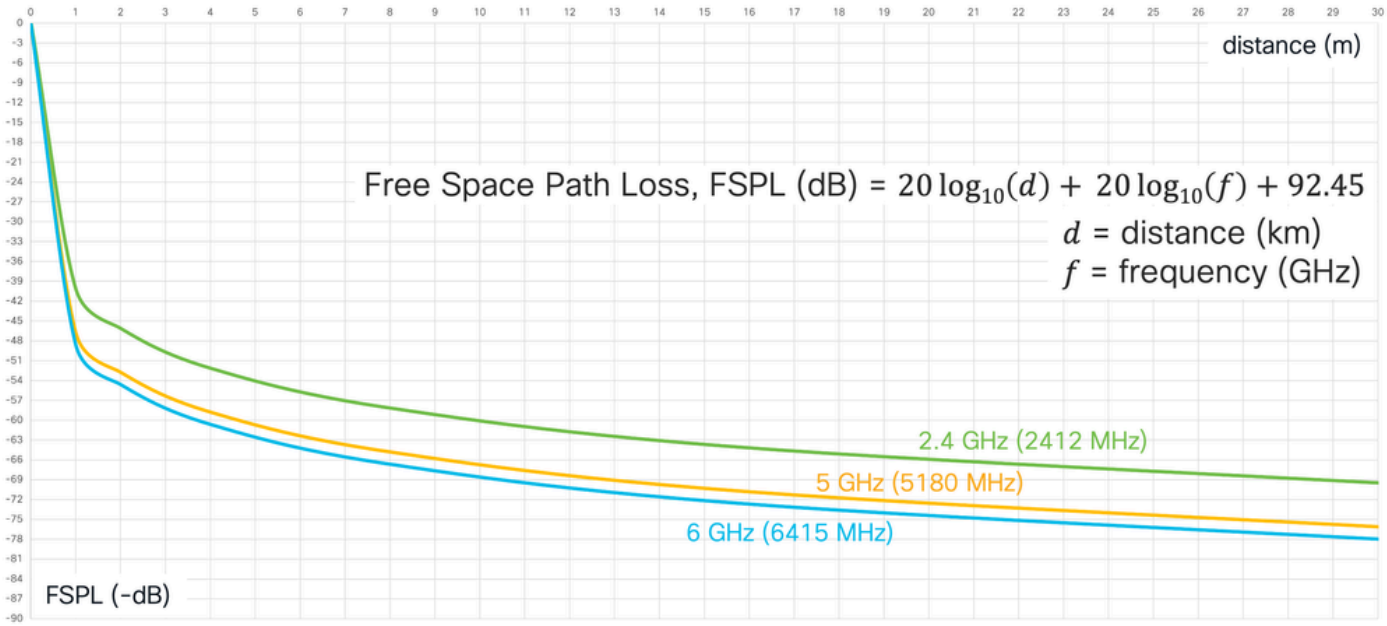
6 GHz覆盖的无线电设计注意事项

本部分简要介绍设计6 GHz覆盖范围时的一些基本注意事项，特别是将2.4/5 GHz现有安装迁移到Wi-Fi 6E或7时，本部分并未尝试作为现场勘测的完全规范指南。

与2.4 GHz和/或5 GHz频段中的任何新Wi-Fi部署一样，新的6 GHz无线项目也必须包括专门6 GHz站点勘察。

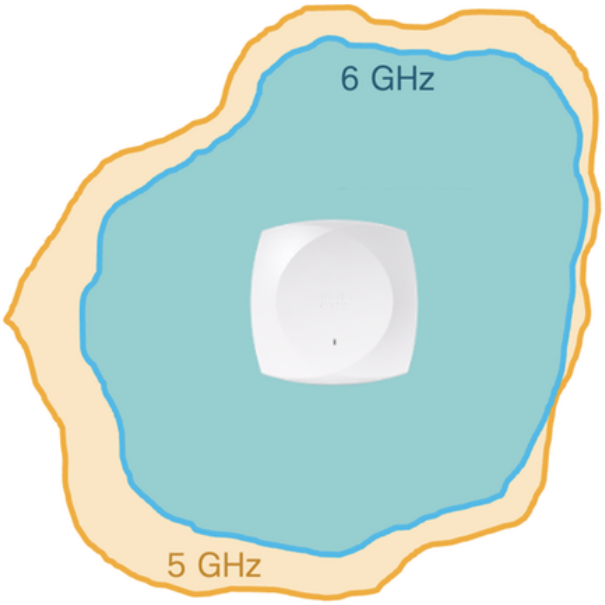
当Wi-Fi 6E/7以前的AP已经定位为满足特定的5 GHz覆盖需求时，在某些情况下，我们可以期望将其替换为支持Wi-Fi 6E/7的AP，并且仍能在6 GHz上获得良好的覆盖范围。要使用此方法，我们现有的AP必须已提供满足预期需求（仅数据、语音、特定应用等）的足够5 GHz覆盖范围，同时运行至少比其最大传输功率水平低3-4个传输功率水平。AP通常有7到8个功率电平，每个连续功率电平将发射功率减半。因此，舒适的工作点靠近允许的发射功率范围的中间位置。

根据自由空间损耗计算，6 GHz信号的衰减比5 GHz信号多2 dB。此外，6 GHz信号可能比其5 GHz信号更易受到障碍物的影响。



当思科AP将发射功率增加或降低一个级别时，其发射功率会以3 dB“跳跃”的方式增加。例如，AP从发射功率为11 dBm的功率级别4移动到功率级别3，其发射功率增加到14 dBm。功率级别4为11

dBm，功率级别3为14 dBm，这只是一般示例，因为对于相同功率级别编号，不同AP型号和代的dBm传输功率值可能稍有不同。



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.

例如，如果之前的Wi-Fi 6E/7 AP已经在5GHz的功率水平4上提供良好的覆盖范围，那么具有类似5GHz无线电模式的较新Wi-Fi 6E/7 AP可以取代之前的AP，而不会对现有的5GHz网络产生任何重大影响。

此外，新的Wi-Fi 6E/7 AP的6 GHz无线电可以通过提高一个发射功率电平(3 dB)来提供与5 GHz无线电类似的覆盖范围。

如果AP 5 GHz无线电在小于其最大功率水平的3-4个功率水平下已经提供了足够的5 GHz覆盖范围，则相应的6 GHz无线电可以被设置为小于其最大功率水平的2-3个功率水平来进行类似的覆盖范围。假设在部署国家/地区的法规允许6 GHz无线电和EIRP级别使用比5 GHz更高的功率时有效。还需要考虑信道聚合和特定AP模型；请参阅每个AP型号的电源设置表了解国家/地区特定的信息。

此外，如果6 GHz无线电已提供低于其最大功率水平2-3的足够覆盖范围，在特殊情况下，它仍然可以增加几个级别，例如，解决由相邻AP故障、未宣布的障碍、新的RF要求等引起的临时意外的覆盖盲点。

在Wi-Fi 6E/7之前和Wi-Fi 6E/7 AP之间的漫游行为

从未建议在同一覆盖区域部署支持不同标准和/或频段的AP，特别是如果以“盐和胡椒”方式（即在同一区域混合）安装不同代的AP。

虽然无线控制器可以处理一组多个AP型号的操作（例如，动态信道分配、传输功率控制、PMK缓存

分配等），但在不同标准和频带之间移动的客户端有时无法正确处理这些转换，并且可能会遇到漫游问题。

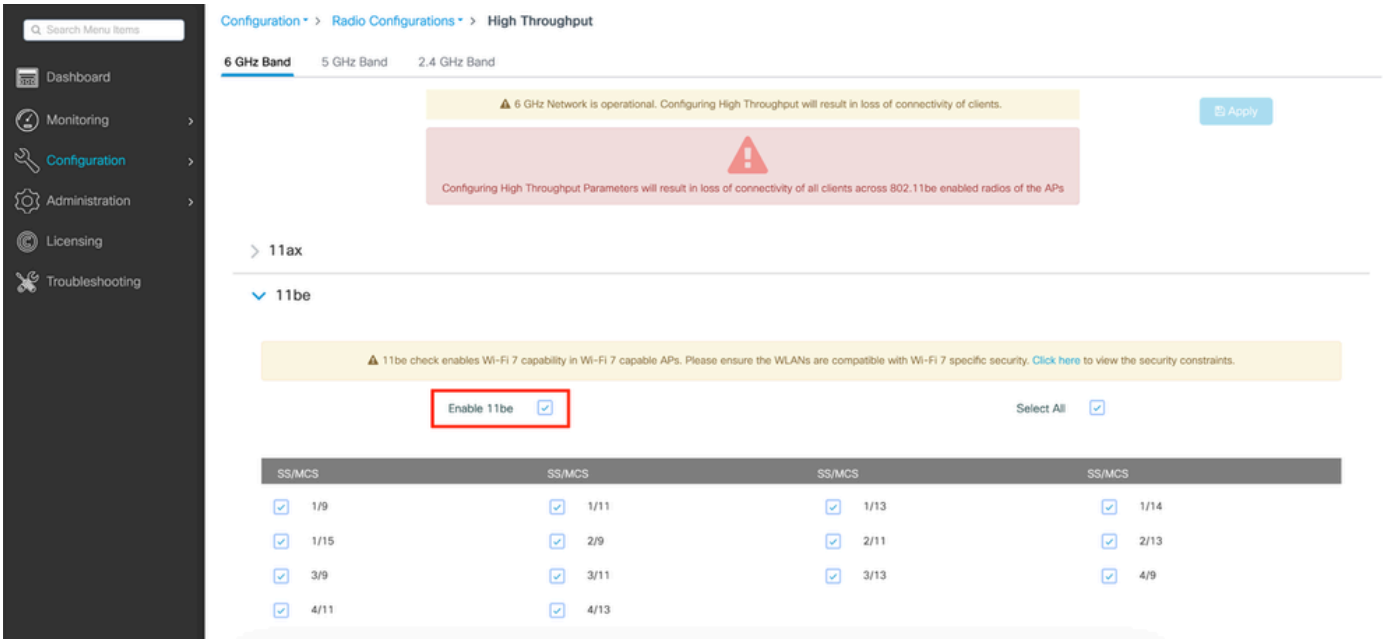
此外，Wi-Fi 6E/7 AP支持WPA3的GCMP256密码，但某些Wi-Fi 6和更早的AP型号并非总是如此。对于同时需要AES(CCMP128)和GCMP256密码的口令/WPA3-Personal和增强型开放/OWE SSID，某些Wi-Fi 6个AP（例如9105、9115和9120系列以及802.11ac Wave 2 x800系列AP）不支持GCMP256且只能提供AES(CCMP) 128)，用于关联客户端，包括支持Wi-Fi 6E/7的客户端。如果这些Wi-Fi 6E/7客户端需要在支持GCMP256的相邻Wi-Fi 6E/7 AP之间漫游，它们必须完成新的关联，因为透明漫游不支持AES(CCMP128)和GCMP256之间的重新协商密码。此外，AP在同一区域提供不同功能通常不是最佳选择：这样的部署不允许客户端在移动时可靠地使用这些功能，并且可能导致粘性和断开连接。
虽然此场景属于角落，但请记住，在WLAN上配置GCMP256密码后，在9105/9115/9120和9130/9124/916x/917x AP之间漫游Wi-Fi 6E/7客户端是不可能的，因为后一个系列支持GCMP256，而前一个系列不支持。

6 GHz上40 MHz或更大的信道宽度也会导致支持6 GHz的客户端粘性，这可能导致拒绝在其他频段上重新关联。这是不在同一漫游区域混合使用6个GHz功能的AP和非6个GHz功能的AP的另一个原因。

全局启用Wi-Fi 7

在Cisco IOS XE上全局启用Wi-Fi 7

当安装或升级到支持Wi-Fi 7的Cisco IOS XE版本时，默认情况下全局禁用对Wi-Fi 7的支持。
要激活它，我们需要导航到每个2.4/5/6 GHz频段的High Throughput配置菜单，并选中复选框以启用11be。



或者，在终端配置模式下通过SSH或控制台运行以下三个命令：

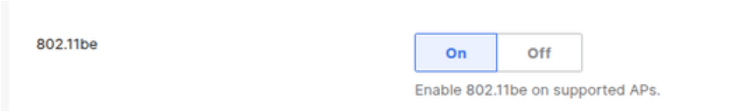
```
ap dot11 24ghz dot11be
ap dot11 5ghz dot11be
ap dot11 6ghz dot11be
```

如警告说明中所述，当尝试修改这些设置时，更改802.11be支持状态会导致Wi-Fi 7 AP无线电上的所有客户端短暂失去连接。如果要执行MLO（这意味着客户端同时连接到多个频段），则需要在希望客户端连接的所有频段上启用11be。不必启用所有频段，但建议仅用于性能。

在Cisco Meraki控制面板上全局启用Wi-Fi 7

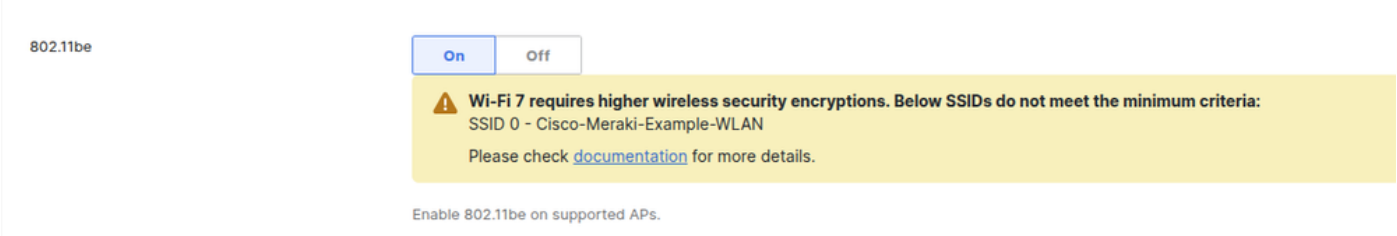
首次将支持Wi-Fi 7的AP（例如，CW9178I或CW9176I/D1）添加到Cisco Meraki控制面板网络时，在其默认RF配置文件中启用对802.11be操作的支持。
要激活它，请导航到Wireless > Radio Settings，单击RF Profile选项卡，然后选择分配给AP的配置文件（室内AP的默认值为“Basic Indoor Profile”）。

在常规部分中，启用802.11be(on)，如下屏幕截图所示：



如果一个或多个WLAN配置的安全设置低于Wi-Fi 7规范要求的安全设置，控制面板将显示警报标语，如下图所示。

虽然控制面板允许保存配置，但标记的SSID上不会启用Wi-Fi 7，直到它们符合Wi-Fi 7要求。至撰写本文时止，要使固件版本MR 31.1.x及更高版本启用Wi-Fi 7，网络中启用的所有WLAN必须满足Wi-Fi 7规范要求（此行为将在未来版本的固件MR 32.1.x中更改）。



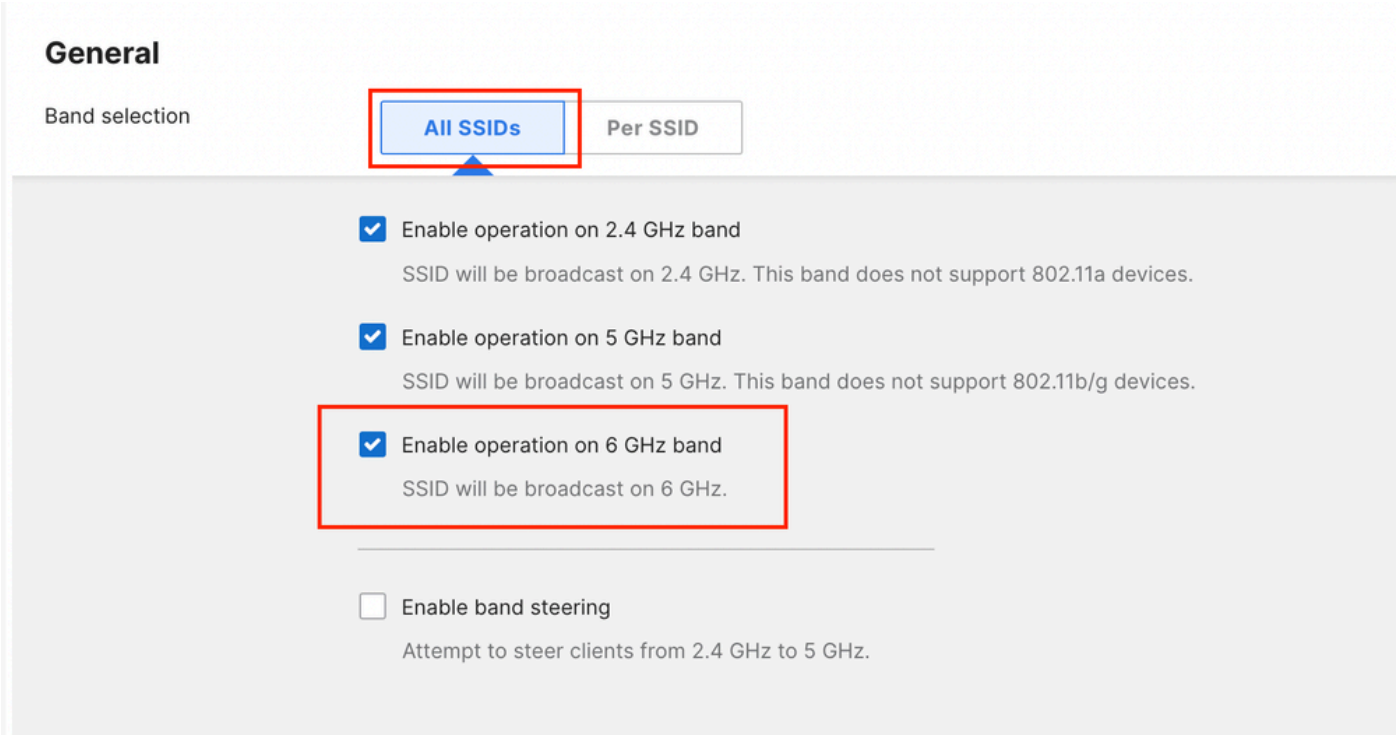
一旦SSID配置满足Wi-Fi 7最低标准，标语即消失。

在同一个RF配置文件中，确保在AP上启用6 GHz操作。

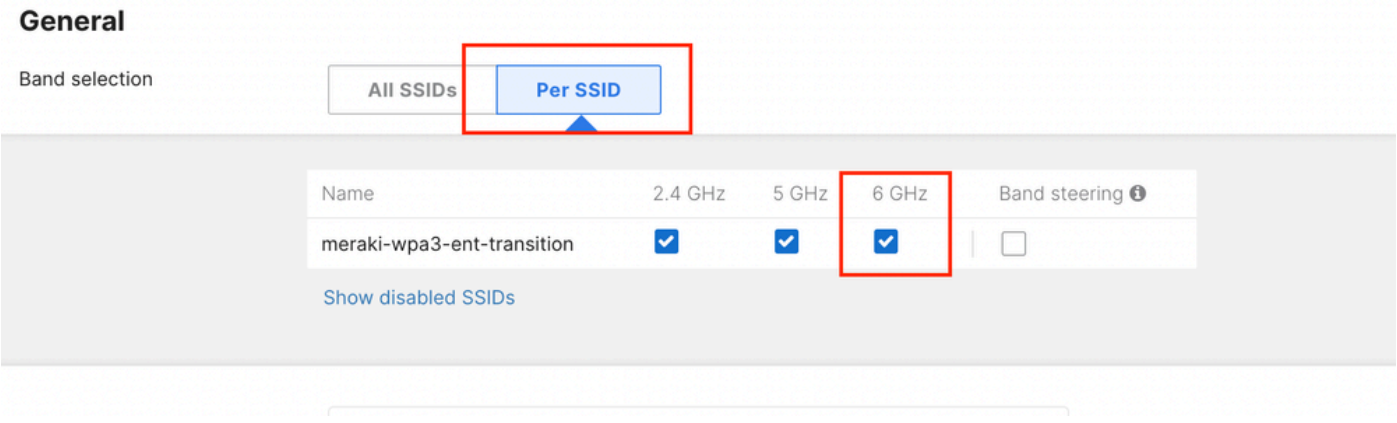
这可以批量或按单个SSID对所有SSID执行。

请注意，频段控制仅在2.4至5 GHz之间可用。

为所有SSID启用6 GHz的示例。



单SSID的6 GHz支持示例。



使用案例

802.1X / WPA3 — 企业网络

Cisco IOS XE上的WPA3-Enterprise配置

基于采用802.1X身份验证的WPA2/3的企业WLAN最容易迁移至6 GHz。

启用6 GHz的802.1X SSID需要启用PMF支持（即使它是可选的），以及802.1X-SHA256和/或FT + 802.1X AKM（两者均符合WPA3）。

我们可以在同一WLAN上继续提供具有标准802.1X(SHA1)的WPA2，仅在5 GHz频段上通告。

Wi-Fi 7支持需要启用Beacon保护；WPA2 802.1X(SHA1)可以作为向后兼容选项保留在WLAN上。

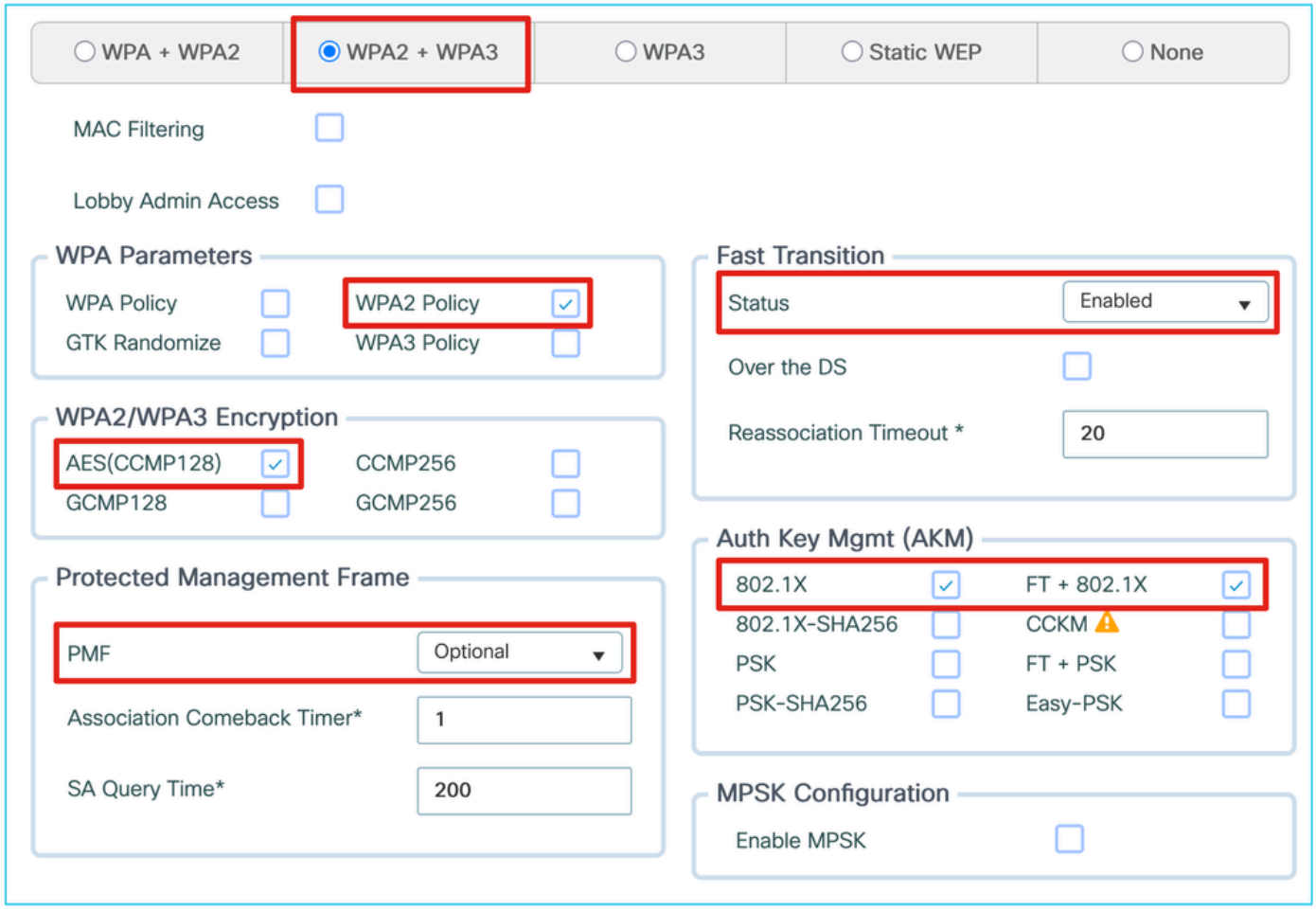
启用AES128和GCMP256、将PMF设置为可选以及允许常规802.1X等WPA2 AKM可能支持许多设备以实现兼容性。但是，这给客户端提供了许多选择。如果客户端通告Wi-Fi 7支持，但选择了不符合Wi-Fi 7的安全配置，则AP必须拒绝这些配置，这可能导致兼容性问题。

但是，Cisco IOS XE 17.18.2及更早版本不支持企业SSID的GCMP256。主要建议是为主要运行Windows 11笔记本电脑的企业环境保留此使用案例。

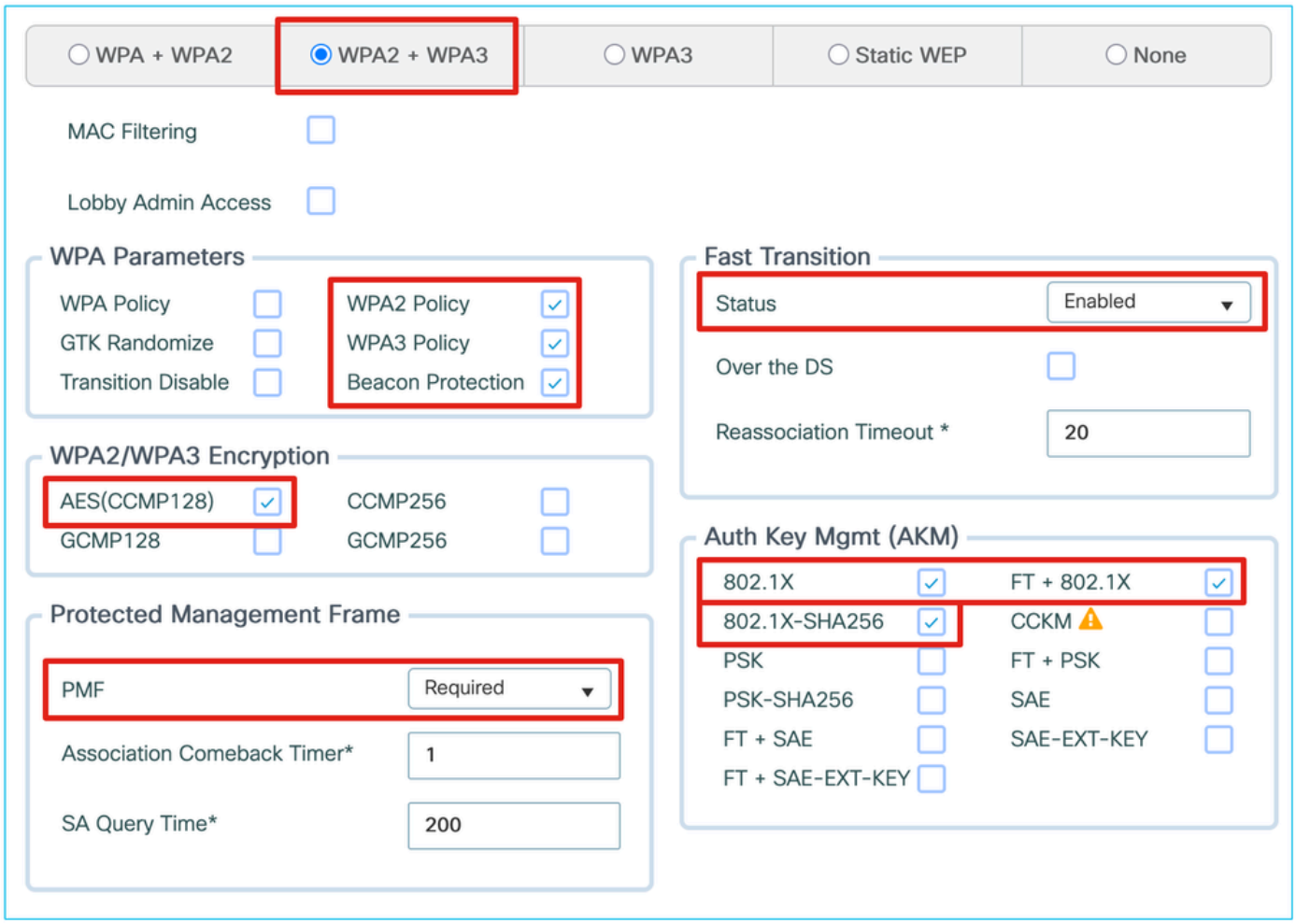
当运行17.18.3或更高版本时，您可以启用GCMP256并正确支持更广泛的移动设备类别（如果SSID声称是Wi-Fi 7，但仅支持AES128，则某些客户端会拒绝连接）。

Meraki云控制面板支持GCMP256，并要求其在SSID上启用Wi-Fi 7。虽然Wi-Fi 7客户端只能支持AES128，但经过认证的Wi-Fi 7 AP必须同时提供AES128和GCMP256。

从具有以下L2安全设置的典型WPA2 SSID:



我们可以迁移WPA3、6 GHz和部分Wi-Fi 7支持的配置，如下所示：

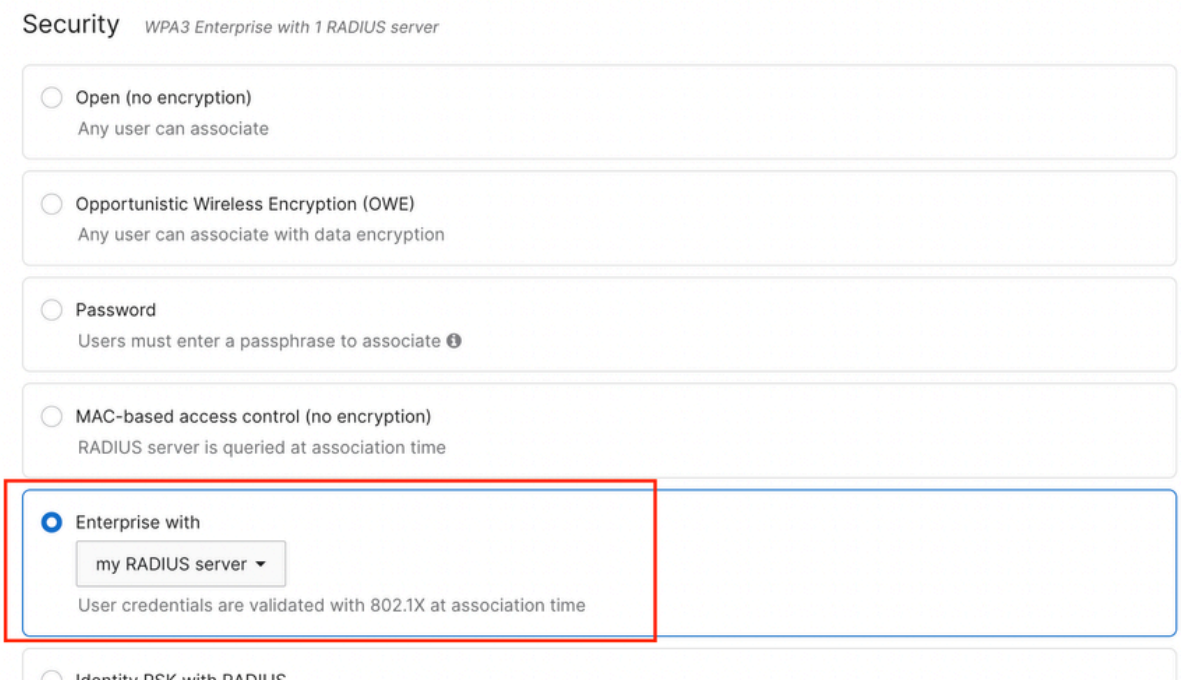


最后一个屏幕截图缺少GCMP256，无法提供合适的Wi-Fi 7支持。提供这么多不同的密码也会导致客户端兼容性问题，因此请考虑尽快迁移到采用AES128+GCMP256的完整WPA3 WLAN。

Cisco Meraki控制面板上的WPA3-Enterprise配置

在撰写本文时，WPA3-Enterprise操作仅适用于外部RADIUS服务器（也称为“我的RADIUS服务器”）。

WPA3-Enterprise不适用于Meraki云身份验证。



从MR 31.x开始，WPA类型包括：

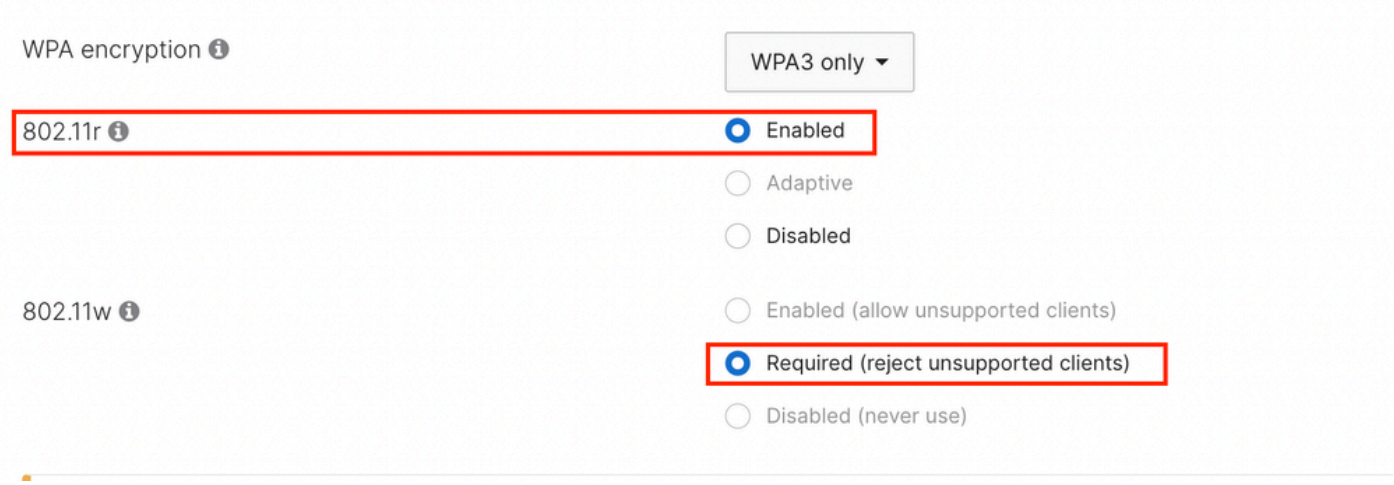
- “仅WPA3”，与WPA2使用相同的密码，但需要802.11w(PMF)。
- 'WPA3 192位'，仅允许使用密码TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384、TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384或TLS_DHE_RSA_WITH_AES_256_GCM_SHA384的EAP-TLS-TLS-TLS。必须在RADIUS服务器上配置相同的密码才能启用此模式。
- “WPA3过渡模式”（也称为混合模式），它允许WPA2客户端在用于WPA3的相同WLAN上共存。



当使用“仅WPA3”或“WPA3 192位安全”时，PMF对于所有客户端都是强制性的。

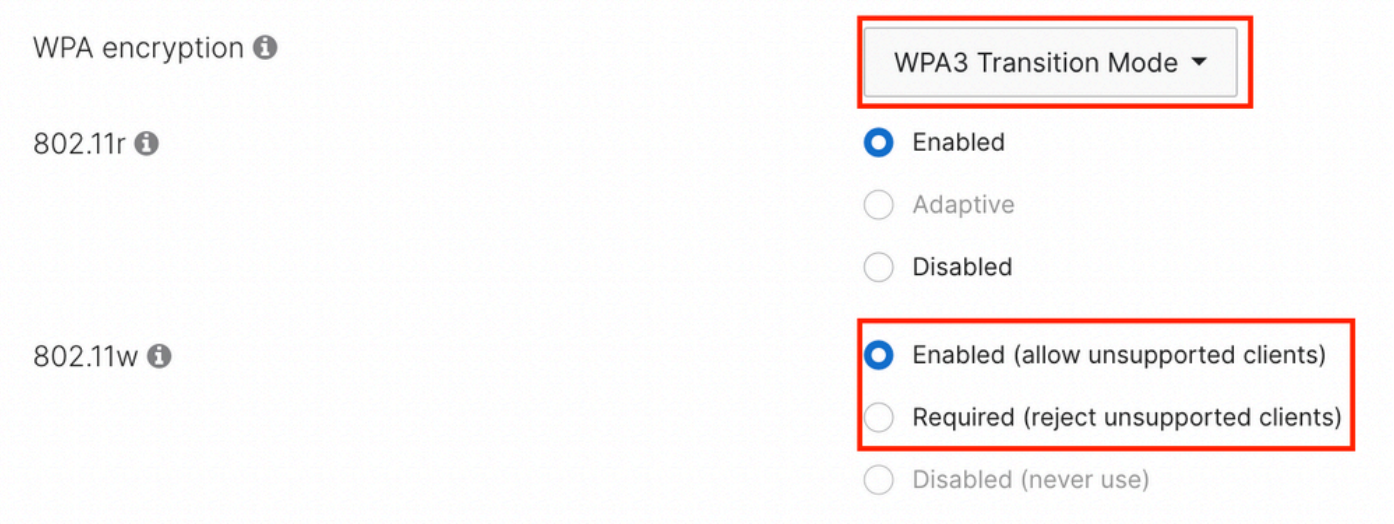
在大多数应用中，建议启用FT(802.11r)（虽然不是强制性的），以减轻使用外部RADIUS服务器时漫游和重新身份验证延迟的影响。

6 GHz操作需要启用PMF(802.11w)。



选择WPA3过渡模式时，所有能够使用WPA3的客户端都默认使用PMF。所有在6 GHz上运行的客户端都使用WPA3。

在此模式下，您可以选择使用WPA2的旧版客户端是否必须使用PMF（需要802.11w），或者该功能是否可选（启用802.11w）。



无论WPA3选择如何，Cisco Meraki AP都要求启用GCMP 256密码套件才能在Wi-Fi 7模式下运行。

此外，当AP在Wi-Fi 7模式下运行时，默认情况下在2.4、5和6 GHz上启用信标保护。



口令/ WPA3 — 个人/ IoT网络

为6 GHz启用口令SSID（最多支持Wi-Fi 6E）非常简单，并且需要SAE和/或FT + SAE，以及其他WPA2 PSK AKM（如果需要）。但是，对于Wi-Fi 7支持，认证要求添加SAE-EXT-KEY和/或FT + SAE-EXT-KEY AKM以及GCMP256密码。

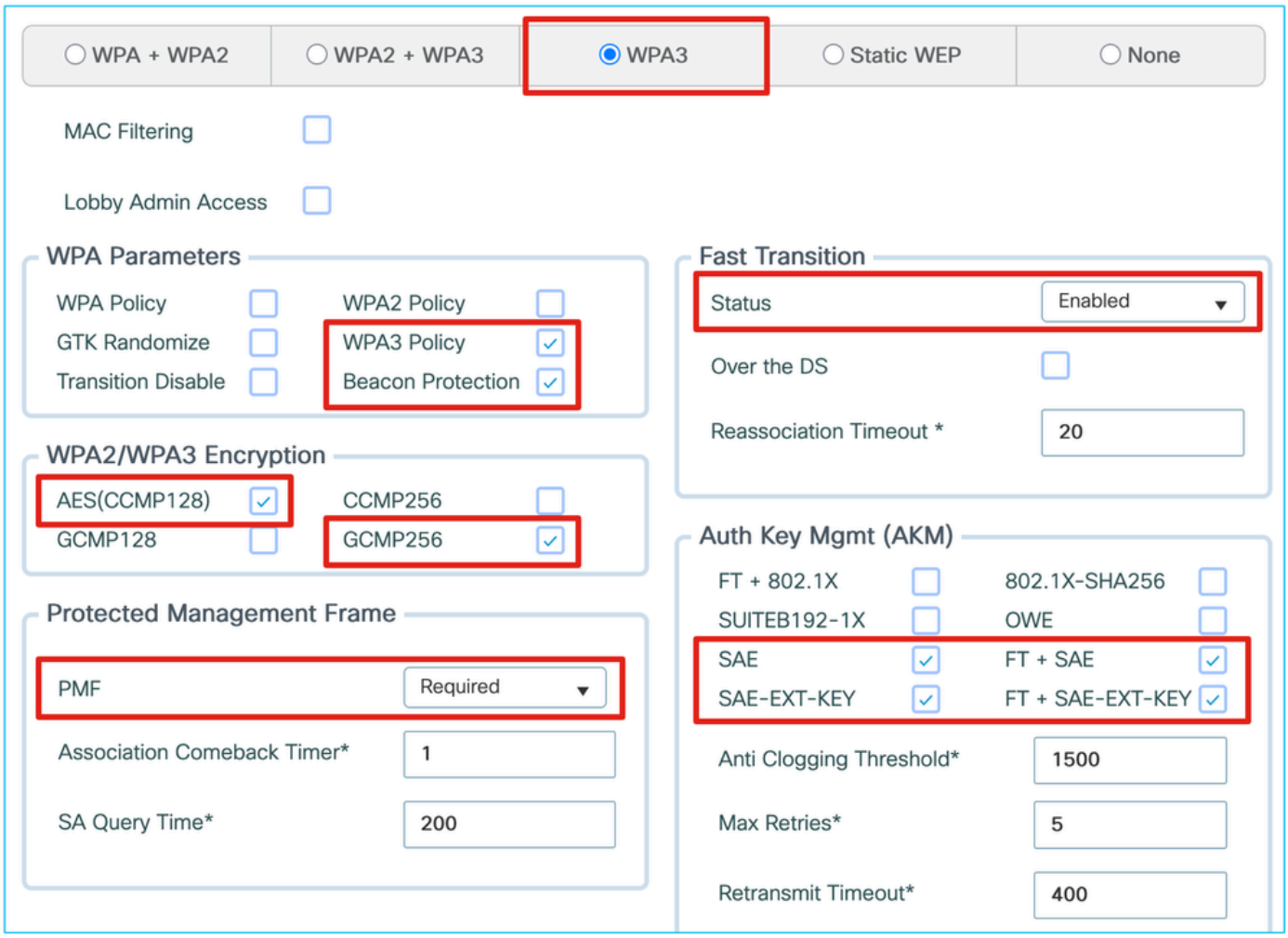
除了上述四个SAE AKM之外，Cisco IOS XE 17.18.1及更高版本还允许您配置WPA2-PSK。但是，即使标准支持配置，这也会向实施不当的客户端驱动程序提供过多的AKM。我们建议在实践中验证您的WPA2客户端是否可以处理WLAN上启用的所有AKM。在这种情况下，使用WPA2连接的客户端不能使用MLO或Wi-Fi 7，但使用SAE-EXT连接的客户端可以。WLAN本身仍会通告Wi-Fi 7和MLO功能。

在这种情况下，我们可以使用SAE、FT + SAE、SAE-EXT-KEY和FT + SAE-EXT-KEY配置专用仅WPA3的SSID，为更近的Wi-Fi 6E和Wi-Fi 7客户端提供AES(CCMP128)和GCMP256密码。

在所有这些情况下，我们强烈建议使用SAE时启用FT。SAE帧交换会占用更多的资源，并且比WPA2 PSK四次握手所需的时间更长。

一些设备制造商（例如苹果）期望在使用SAE时启用FT，并且如果FT不可用，其设备可以拒绝连接。

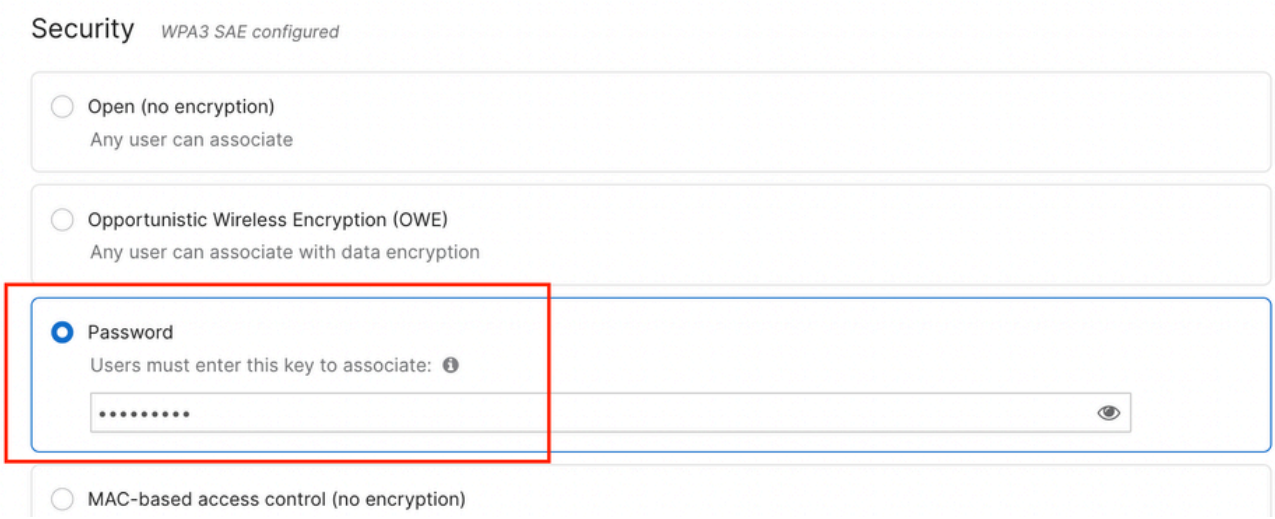
Cisco IOS XE上的WPA3-SAE配置



注意：如果在WLAN上启用了(FT +)SAE，并且Wi-Fi 7客户端尝试与其关联，而不是(FT +)SAE-EXT-KEY，则会拒绝该请求。只要(FT +)SAE-EXT-KEY也启用，Wi-Fi 7客户端就必须使用后一个AKM，因此不会出现此问题。

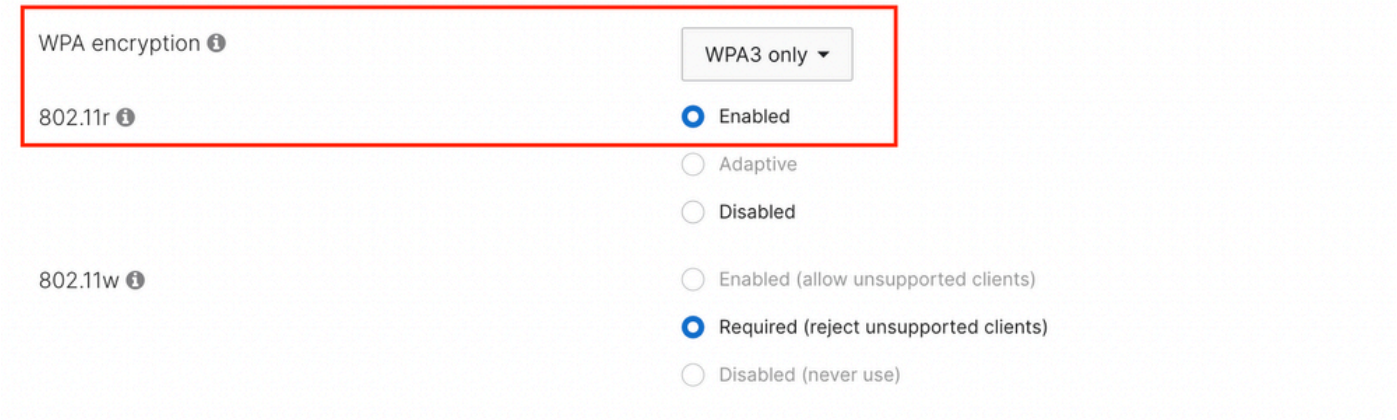
尽管除了仅WPA3的WLAN外，还使用传统PSK的WLAN会增加SSID的总数，但我们仍可以在一个SSID上保持最大兼容性。我们还可以禁用可能影响兼容性的高级功能，这在许多物联网场景中都有帮助，同时通过其他SSID为较新的设备提供最大的功能和性能。如果您部署了较旧或更敏感的IoT设备，这可以成为首选方法。如果您没有IoT设备，使用单一过渡模式WLAN会更有效，因为您只通告一个SSID。

Cisco Meraki控制面板上的WPA3-SAE配置



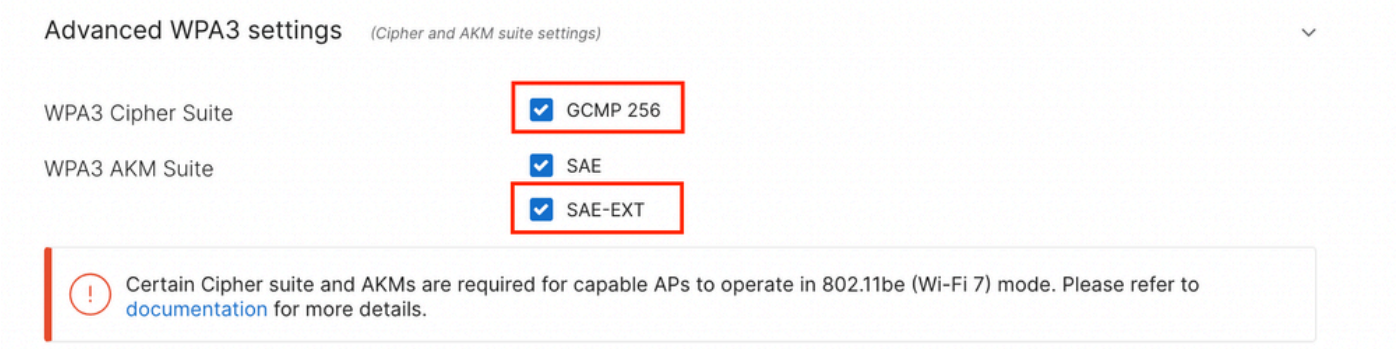
对于固件MR 30.x，唯一支持的WPA类型为“仅WPA3”，控制面板不允许您选择其他方法。

在此配置中，PMF是必需的，而使用SAE时，最好启用FT(802.11r)。



要允许Wi-Fi 7操作，必须在配置SSID时启用GCMP 256密码套件和SAE-EXT AKM套件。

默认情况下禁用这些设置，并且可以在“高级WPA3设置”下启用。



至撰写本文时止，网络中启用的所有WLAN必须满足Wi-Fi 7规范要求，才能在固件版本MR 31.1.x及更高版本上启用。

这意味着之前配置的Wi-Fi 7 SSID不能与使用WPA2-Personal或WPA3-SAE转换模式的其他SSID共存。

如果在控制面板网络中配置了WPA2-Personal SSID，则所有Wi-Fi 7 AP将恢复为Wi-Fi 6E操作。

此行为在未来的固件MR 32.1.x版本中更改。

开放/增强型开放/OWE/访客网络

访客网络有多种形式。通常，它们不需要802.1X凭证或密码短语进行连接，并且可以包含需要凭证或代码的启动页或门户。这通常通过开放式SSID以及本地或外部访客门户解决方案来处理。但是，在6 GHz或Wi-Fi 7支持中不允许使用具有开放安全（无加密）的SSID。

保守的方法是最多将访客网络专用于5 GHz频段和Wi-Fi 6。这保留了6 GHz频段供企业设备使用，降低了复杂性，并提供了最大的兼容性，但它不提供Wi-Fi 6E/7性能。

尽管增强型开放是一种强大的安全方法，可在保留开放体验的同时提供隐私保护（最终用户无需输入802.1X凭证或密码），但终端支持仍然有限。一些客户仍不支持它，即使支持，体验也并不总是流畅：当连接安全时，设备可将连接显示为不安全，或即使不需要OWE的口令，设备也可将连接显示为受口令保护的连接。由于访客网络需要与所有非托管访客设备配合使用，因此仅提供增强型开放SSID可能为时过早。我们建议通过单独的SSID提供两种选项：5 GHz的开放式SSID和5 GHz和6 GHz的启用OWE的SSID，两者均使用相同的强制网络门户（如果需要）。这两个网络必须使用不同的SSID名称，因为根据802.11标准，SSID名称标识客户端可以无缝漫游的所有BSS。因此，将同一SSID名称用于不同的安全设置是无效和危险的。过渡模式在Wi-Fi 6E、6 GHz（即使软件仍然允许它）或Wi-Fi 7上不受支持，因此不建议使用。OWE仍支持所有门户重定向技术（内部或外部Web身份验证、集中Web身份验证等）。

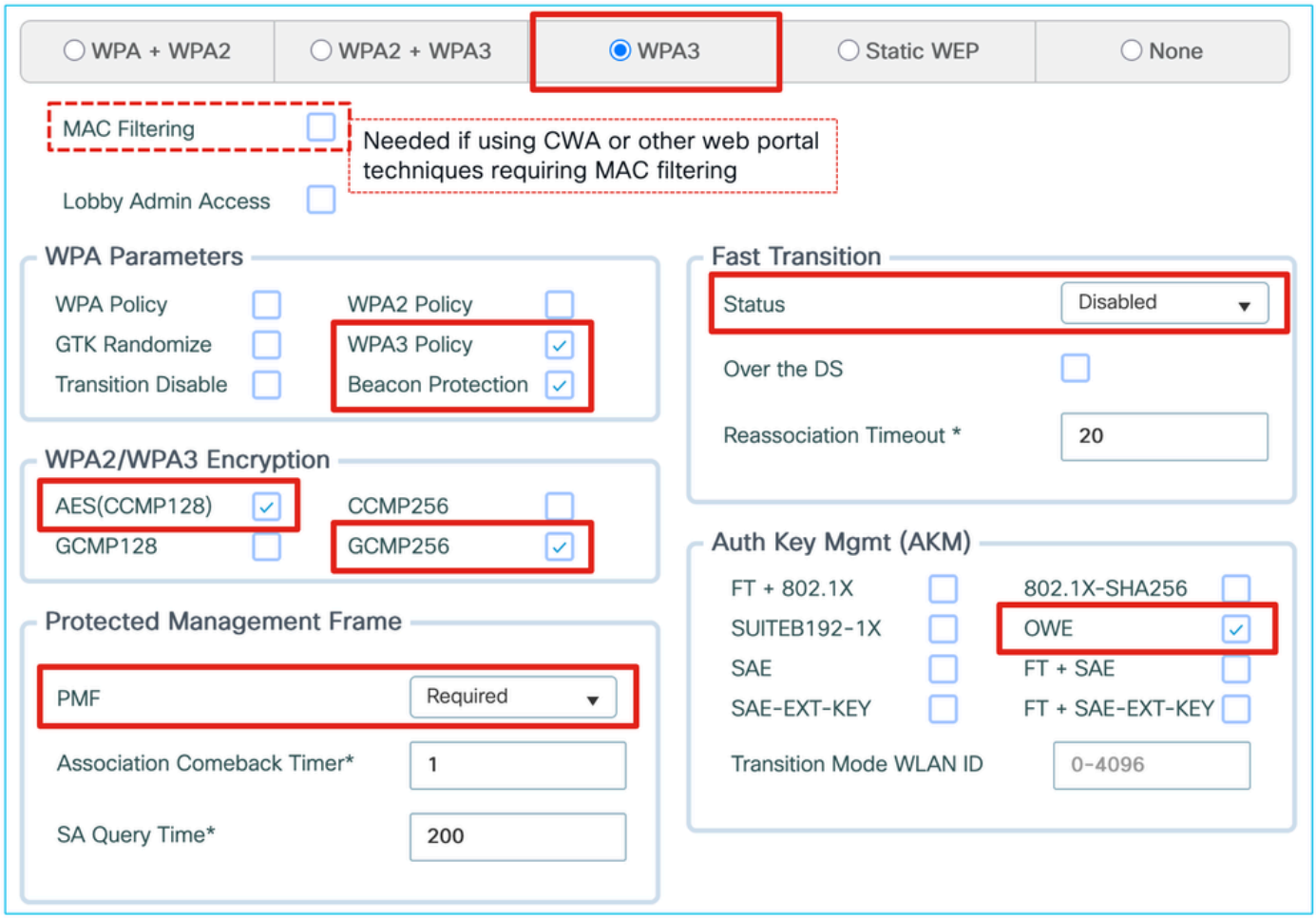
Cisco IOS XE上的OWE配置

要向访客提供6 GHz服务，我们建议使用增强型开放/OWE（随机无线加密）创建单独的SSID。 它可以同时提供AES(CCMP128)密码，以便与最高可支持Wi-Fi 6E的客户端实现最大兼容性，并为支持Wi-Fi 7的客户端提供GCMP256。

目前，许多移动客户端都为OWE/增强型开放提供部分或不那么方便的用户支持。与您的客户一起测试以衡量支持情况。

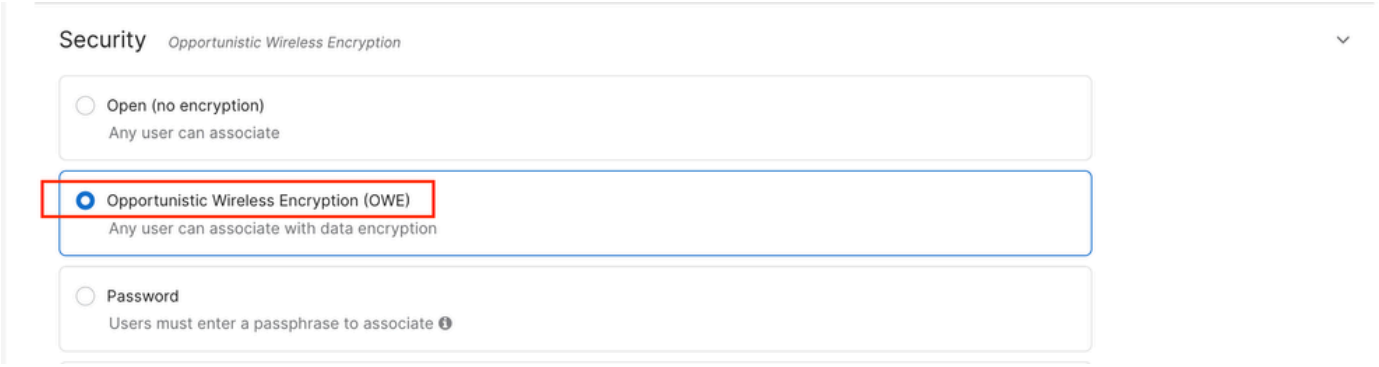
有两个独立的访客WLAN（一个开放式WLAN和一个增强型OWE/开放式WLAN）可以作为一个解决

方案，尤其是在您仅将OWE安全的访客WLAN保持在6 GHz和完全开放的5 GHz时。但是，您必须将两个访客WLAN划分为不同的子网；否则，开放式WLAN会提供对相同子网的未加密访问，从而抵消安全WLAN的安全优势。



Cisco Meraki控制面板上的OWE配置

与Cisco IOS XE一样，我们建议使用在6 GHz上运行的增强型开放/OWE创建单独的访客SSID。在Cisco Meraki控制面板的Wireless > Access Control下，通过选择“Opportitional Wireless Encryption(OWE)”作为安全方法配置此设置。

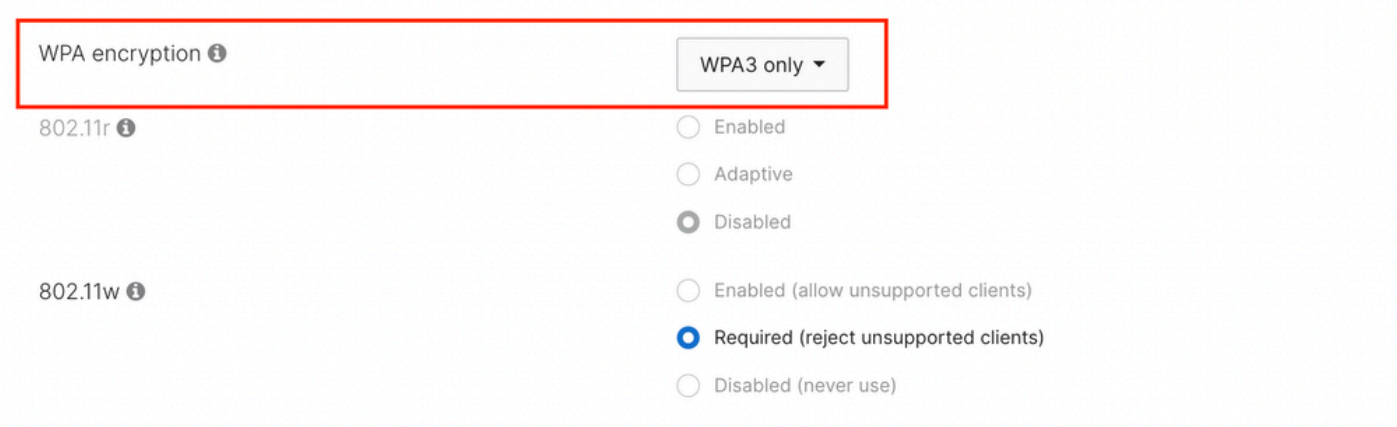


运行固件至MR 31时，唯一支持的WPA类型为“仅WPA3”，控制面板不允许您选择其他方法。

PMF在此配置中是必需的，而FT(802.11r)无法启用。

请注意，标签“WPA3 only”具有误导性，因为OWE不是WPA3标准的一部分；但是，此配置是指不带过渡模式的OWE。

未来MR 32.1.x版本中将提供OWE转换模式。



默认情况下，AES(CCMP128)密码已启用，以便最大兼容至Wi-Fi 6E客户端。

GCMP256可与CCMP128一起启用，以符合Wi-Fi 7要求。



其他WPA3和相关选项

虽然WPA3选项在WPA3部署指南中进行了最详细的描述和介绍，但本节介绍一些有关WPA3的额外建议，具体涉及6 GHz和Wi-Fi 7支持。

信标保护

此功能解决了以下漏洞：攻击者可以传输模拟合法接入点的信标，并修改字段以更改已关联客户端的安全设置或其他设置。Beacon protection会向该信标添加一个信息元素（管理MIC），该元素用作签名，以证明合法接入点发送了该信标，并且该信标未被篡改。只有具有WPA3加密密钥的关联客户端可以验证信标的合法性；探测客户端无法对其进行验证。不支持附加信息元素的客户端（即非Wi-Fi 7客户端）必须忽略它，通常不会导致兼容性问题，除非客户端的驱动程序编程不正确。

在17.18之后，如果您的WLAN兼容Wi-Fi 7，则自动启用信标保护元素，无论您是否启用信标保护复选框。

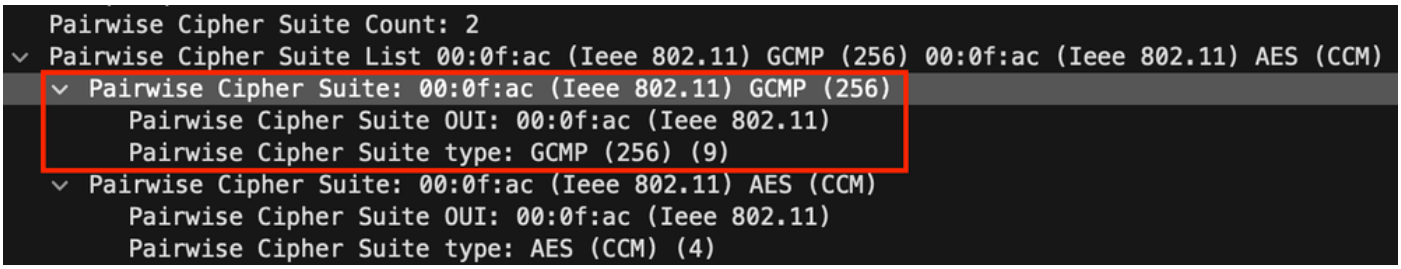
此屏幕截图显示管理MIC信息元素内容的示例：



GCMP256

在Wi-Fi 7认证之前，大多数客户端都实施AES(CCMP128)密码加密。CCMP256和GCMP256是与SUITE-B 802.1X AKM相关的特定变体。虽然市场上有一些早期的Wi-Fi 7客户端声称支持Wi-Fi 7，但它们并不总是实施GCMP256加密。当Wi-Fi 7 AP实施标准并阻止没有适当GCMP256支持的客户端连接时，这可能成为一个问题。

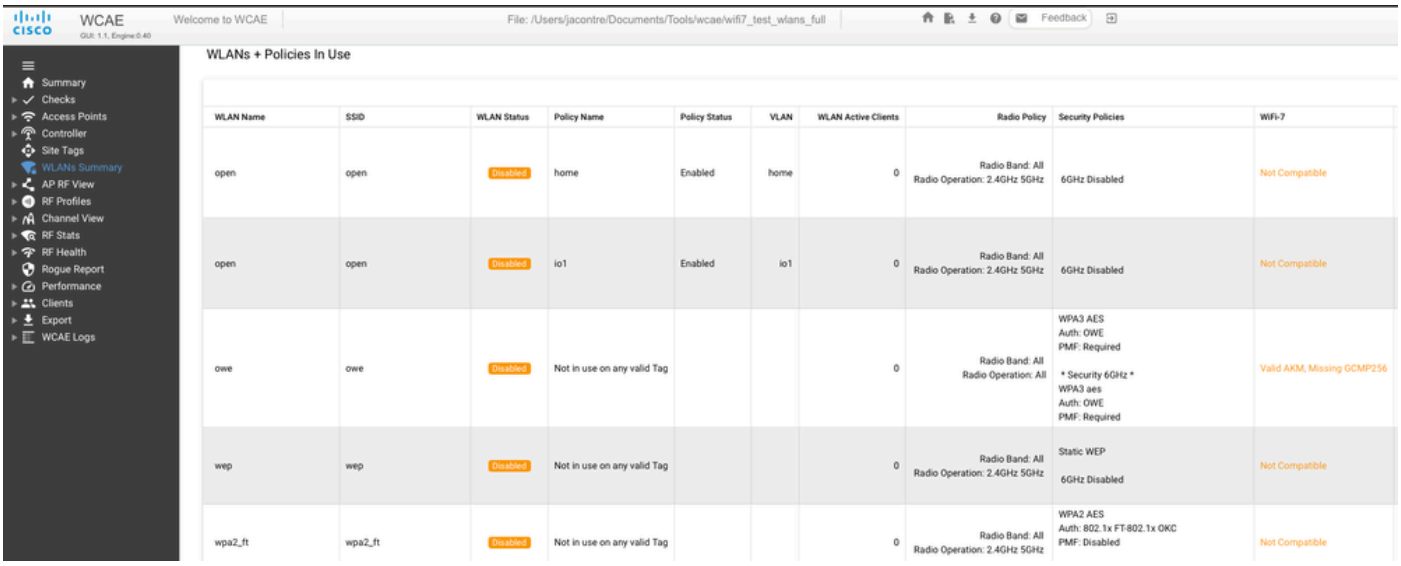
启用GCMP256时，WLAN信标帧中的稳健安全网络元素(RSNE)会通告成对密码套件列表中的功能，如下所示。



故障排除和验证

最新版本的Wireless Configuration Analyzer Express具有Wi-Fi 7就绪性检查，根据前面提到的所有Wi-Fi 7要求评估您的9800配置。

如果您仍然不确定您的配置是否为Wi-Fi 7就绪，WCAE会确定问题所在。



故障排除核对表

- Web UI（在R32或17.18.2及更高版本中）告诉您您的WLAN是否符合Wi-Fi 7标准。使用本文档验证安全设置是否合规。
- 请确保客户端支持Wi-Fi 7。Windows笔记本电脑至少需要Windows 11 24H2。请确保无线适配器驱动程序是最新的。
- Windows中的“netsh wlan show drivers”命令在列出无线适配器的功能并检验其状态时非常有用。
- 对于笔记本电脑，请转至适配器设置并验证适配器是否已启用11be模式。许多最初随11一起提供的适配器被禁用，并作为11ax运行，以实现兼容性。
- 如有疑问，请执行无线数据包捕获以验证：
  - AP正在信标中广播EHT信息元素。这可以通过任何嗅探器捕获；它不需要支持Wi-Fi 7，因为信标以传统速率发送。
  - 如果AP正确广播了EHT，则客户端必须在其关联请求中发送EHT元素。如果没有，则客户端认为与Wi-Fi 7兼容的AP安全设置或者在适配器属性中禁用了802.11be。

参考

- WPA3加密和配置指南
- Meraki WPA3指南

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。