借助思科无线迁移至6 GHz和Wi-Fi 7

目录

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操作认证中写下的安全要求。

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
- WPA3对等同时身份验证(SAE)（也称为WPA3 — 个人）和密码。SAE-FT(SAE with Fast Transition)是另一种可能的AKM，实际上建议使用，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

虽然根据WPA3 v3.4规范(第11.2节),6 GHz不支持增强型开放式过渡模式，但许多供应商(包括最高支持IOS® XE 17.18的思科)尚未实施该模式。因此，在技术上，可以配置（例如）5 GHz上的开放

式SSID、5 GHz和6 GHz上的相应增强型开放式SSID（两者都启用了转换模式），并且所有这一切都不符合标准规范。但是，在此类场景中，必须预期我们宁愿配置不带转换模式且仅在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），同时保持常规的开放SSID在5 GHz上且不带转换模式。

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）认为802.1X-SHA256或“FT + 802.1X”（实际上是802.1X，上面有SHA256和Fast Transition）仅兼容WPA3，而普通802.1X（使用SHA1）则被认为是WPA2的一部分，因此不适合/不支持6 GHz。

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。其中一些允许使用802.11be数据速率和协议改进，而其他一些则专门支持多链路操作(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（仍使用SHA256，即使其命名不明确也是如此）。 与之前现有的6 GHz频段的WPA3安全必备条件相比，这并不是更改。
- WPA3 — 个人，带GCMP256和SAE-EXT-KEY和/或FT + SAE-EXT-KEY（AKM 24或25）。Wi-Fi 6E通过常规AES(CCMP128)强制使用WPA3 SAE和/或FT + SAE，且无需其他扩展密钥使用；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，并且尽早发布，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：

IOS XE 17.18.1及更高版本

如果WLAN具有与Wi-Fi 7要求相匹配的安全参数（信标保护、PMF和前面所述的正确AKM，这取决于WLAN类型以及是否存在GCMP256，以便在OWE或SAE-EXT的情况下实现Wi-Fi 7 MLO），则IOS XE 17.18及更高版本仅将给定WLAN通告为Wi-Fi 7。 SSID上允许存在AES128，但使用时，它仅提供Wi-Fi 6E而不是Wi-Fi 7 MLO。

客户端可以作为Wi-Fi 7进行关联，并实现Wi-Fi 7数据速率，而不管其使用的是何种安全方法（前提是WLAN仍支持它）。 但是，如果客户端遵守Wi-Fi 7安全的严格要求，或者被拒绝，则它只能关联为支持MLO的客户端（在一个或多个频段上）。

IOS XE 17.15.3及更高版本17.15.x

在此分支机构中，如果全局启用Wi-Fi 7，则所有WLAN都将广播为Wi-Fi 7 SSID，而不考虑安全设置。

客户端可以关联为支持Wi-Fi 7，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仍支持它。但是，如果客户端遵守Wi-Fi 7安全的严格要求，或者被拒绝，则它只能关联为支持MLO的客户端（在一个或多个频段上）。

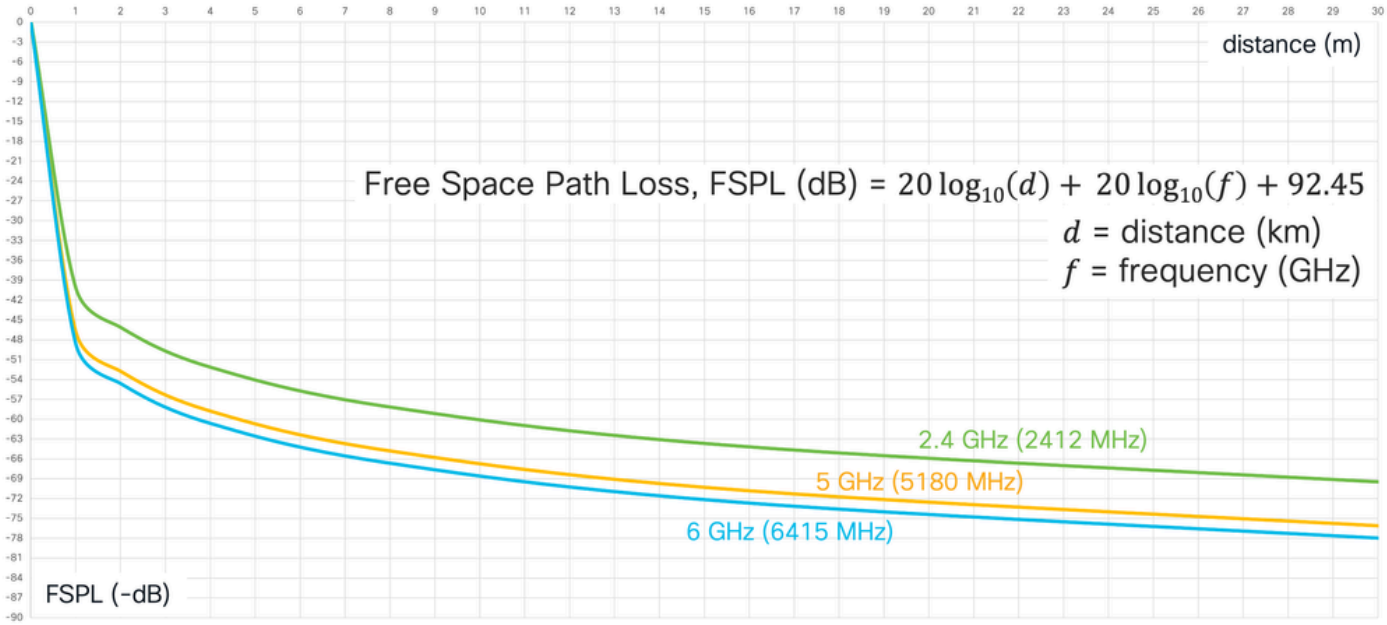
当一些早期的Wi-Fi 7客户端无法支持更安全的密码（如GCMP256）时，这可能会造成问题，这些客户端尝试将具有Wi-Fi 7 MLO功能的WLAN关联到安全设置与Wi-Fi 7要求不匹配的WLAN。在这种情况下，由于安全设置无效（仍允许在WLAN下配置），客户端被拒绝。

6 GHz覆盖的无线电设计注意事项

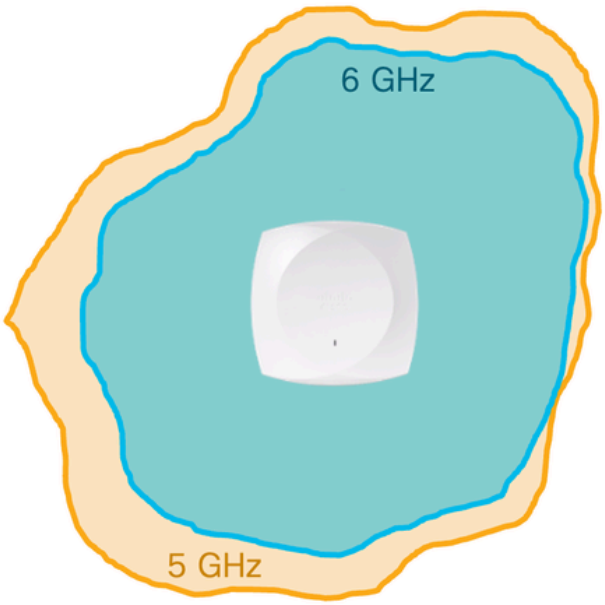
本部分无意成为现场勘测的完整规范指南，简要介绍设计6 GHz覆盖范围时的一些基本注意事项，特别是如果已经存在要迁移到Wi-Fi 6E或7的2.4/5 GHz安装。
对于我们过去在2.4和/或5 GHz频段采用的任何新Wi-Fi部署，6 GHz频段的新无线项目也必须包括相应的专用6 GHz站点勘察。

当Wi-Fi 6E/7以前的AP已针对特定的5 GHz覆盖范围和需求进行定位时，在某些情况下，我们可以期望能够将其替换为支持Wi-Fi 6E/7的AP，并且仍能在6 GHz上获得良好的覆盖范围。为了让此理论起作用，我们现有的AP必须已针对预期需求（仅数据、语音、特定应用等）提供正确的5 GHz覆盖范围，同时其最大传输功率水平至少已达到3-4级。AP通常有7到8个功率电平，每个功率电平将发射功率除一半。这意味着，当AP使用其允许的传输功率范围的介质时，可以有一个舒适的位置。

根据自由空间损失计算，6GHz信号比5GHz信号衰减2dB。此外，6 GHz信号受障碍的影响也比5 GHz信号更大。



当思科AP将发射功率增加/减少一个级别时，其发送功率增加/减少为3 dB。AP从功率级别4（例如，发射功率为11 dBm）上升到功率级别3，将其发射功率提高至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，因为不同型号/代的AP对于相同功率级别编号在dBm中的发射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，新型Wi-Fi 6E/7 AP的6 GHz无线电只需提高一个发射功率电平（所以3 dB），就可以提供与5 GHz无线电类似的6 GHz覆盖。

如果AP的5 GHz无线电已正确覆盖了5 GHz的最大功率以下的3-4个功率电平，则对应的6 GHz无线电可设置为最大功率以下的2-3个功率电平，以实现可比覆盖。

此外，如果6 GHz无线电在低于其最大功率水平的2-3个功率水平下已提供正确的覆盖范围，它仍可能会在特殊情况下提高几个电平，例如尝试绕过临时意外的覆盖盲区（邻居AP故障、未通告的障碍、新的RF需求等）。

在Wi-Fi 6E/7之前和Wi-Fi 6E/7 AP之间的漫游行为

在同一个覆盖区域部署支持不同标准和/或频段的AP始终不是推荐的做法，尤其是当这些不同代的AP以“盐和胡椒”方式（即，在同一区域中混合）安装时。

虽然无线控制器可以处理来自一组多个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），但在不同标准甚至不同频段之间移动的客户端并不总是能够正确处理这些操作，它们可能遇到漫游问题。

此外，由于新标准，Wi-Fi 6E/7 AP支持WPA3的GCMP256密码。但是，一些Wi-Fi 6 AP和早期型号并非总是如此。对于需要同时配置AES(CCMP128)和GCMP256密码的口令/WPA3-Personal和增强型开放/OWE SSID，某些Wi-Fi 6（如9105、9115和9120系列）不支持GCMP256，并且只能为关联客户端（包括支持Wi-Fi 6E/7的客户端）提供AES(CCMP128)密码。如果这些Wi-Fi 6E/7客户端需要从支持GCMP256的相邻Wi-Fi 6E/7 AP漫游或漫游到相邻Wi-Fi 6E/7 AP，它们必须经历全新的关联，因为透明漫游不支持AES(CCMP128)和GCMP256之间的重新协商密码。此外，一般来说，AP在同一区域提供不同功能并不是最佳选择：此部署不允许客户端在移动时可靠地使用这些功能，并且可能导致粘滞或断开。

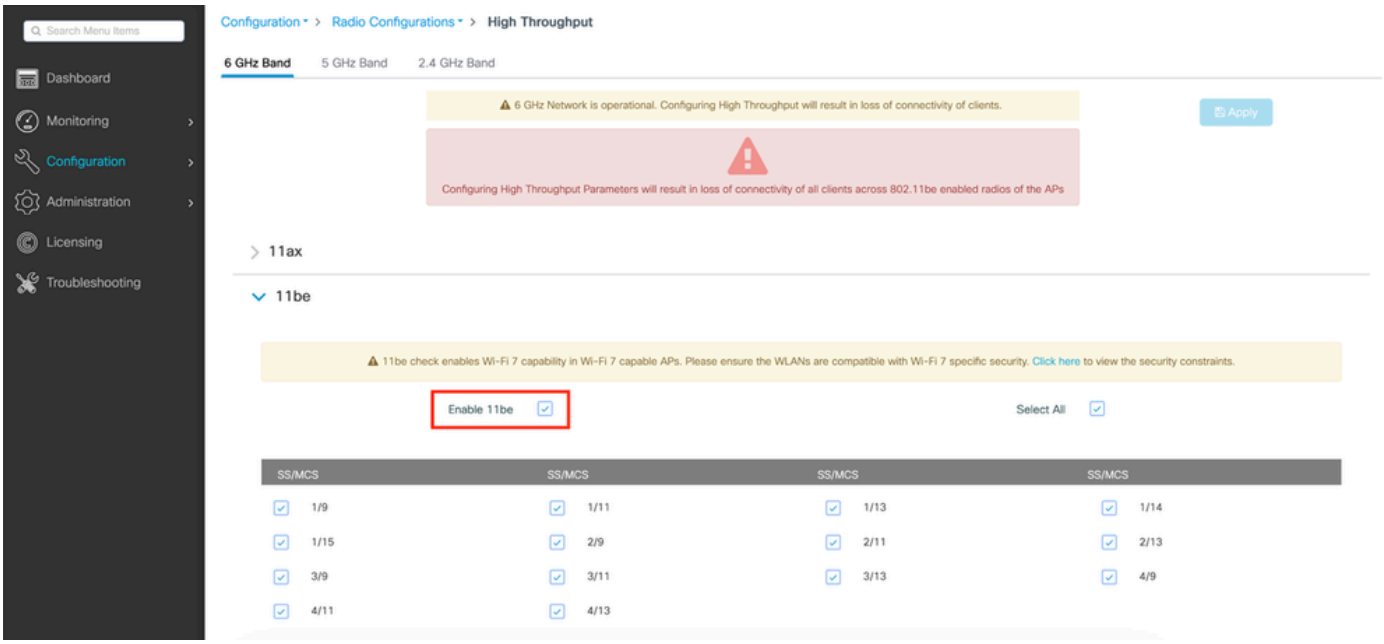
虽然此场景必须代表一个角落，但我们仍要记住，在WLAN下配置了GCMP256密码后，在9105/9115/9120和9130/9124/916x/917x AP之间漫游的Wi-Fi 6E/7客户端是不可能的，因为这些后一系列支持GCMP256，而前一个系列则不支持。

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，这些客户端可能会拒绝重新关联到其他频段。这肯定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IOS XE上全局启用Wi-Fi 7

当安装或升级到支持Wi-Fi 7的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 configuration菜单下，并选中启用11be的复选框。



另一种方法也可以是通过SSH/控制台在终端配置模式下运行以下三条命令行：

```
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

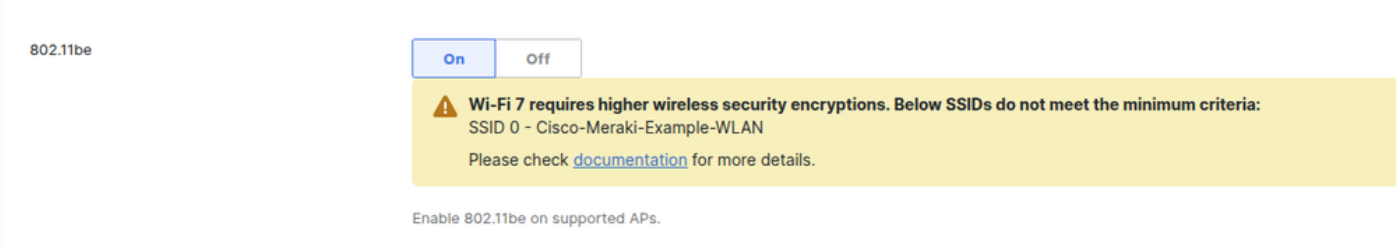
首次将支持Wi-Fi 7的AP（例如CW9178I、CW9176I/D1）添加到Cisco Meraki控制面板网络时，在

其默认RF配置文件中支持802.11be操作。
要激活它，我们需要在Wireless > Radio Settings下导航，点击RF Profile选项卡，并选择分配给AP的配置文件(默认值："基本室内配置文件"（适用于室内AP）。

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配置的安全设置比Wi-Fi 7规范要求的安全设置弱，控制面板将显示一个标语警告用户，如下图所示。

虽然控制面板允许保存配置，但在确保符合Wi-Fi 7要求之前，不会在标记的SSID上启用Wi-Fi 7。写本文时，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（此行为将在未来版本的固件MR 32.1.x中更改）。



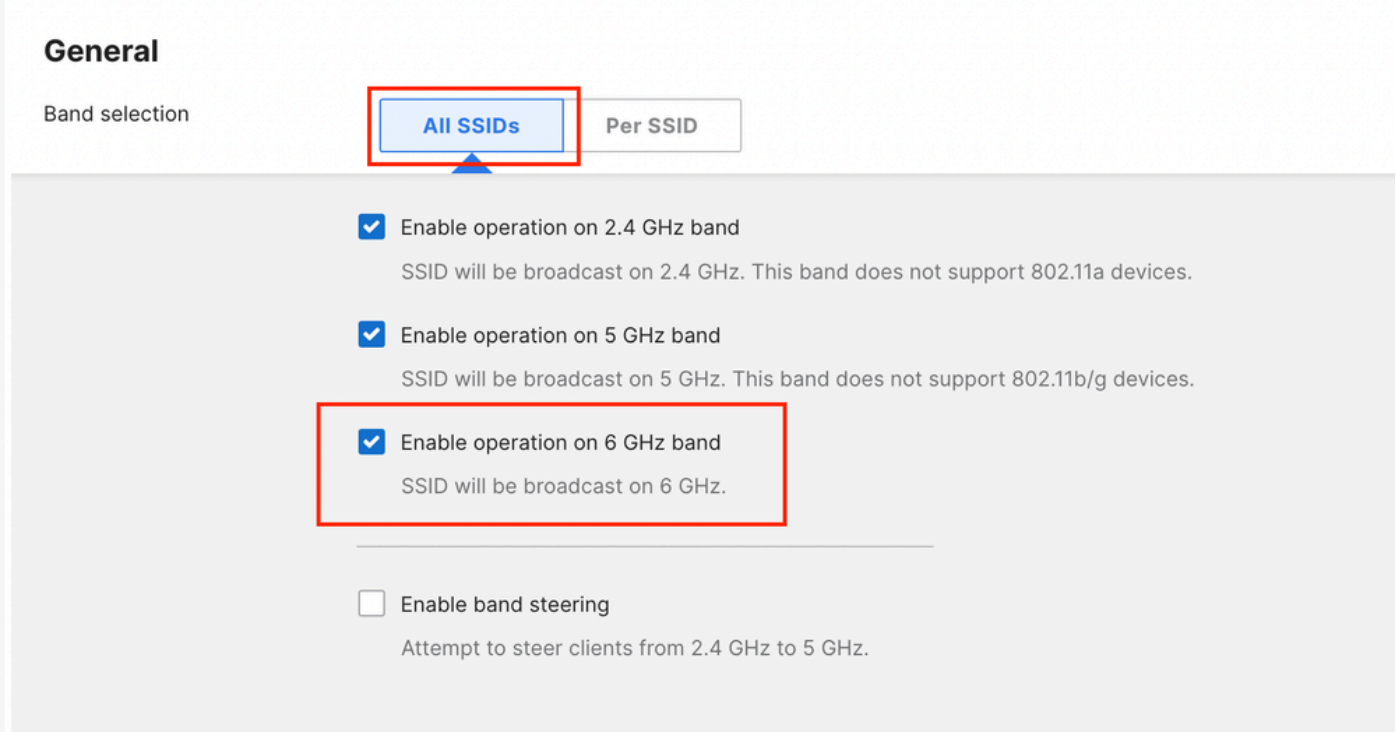
一旦SSID配置满足Wi-Fi 7最低标准，标语即消失。

在同一个RF配置文件中，确保在AP上启用6 GHz操作。

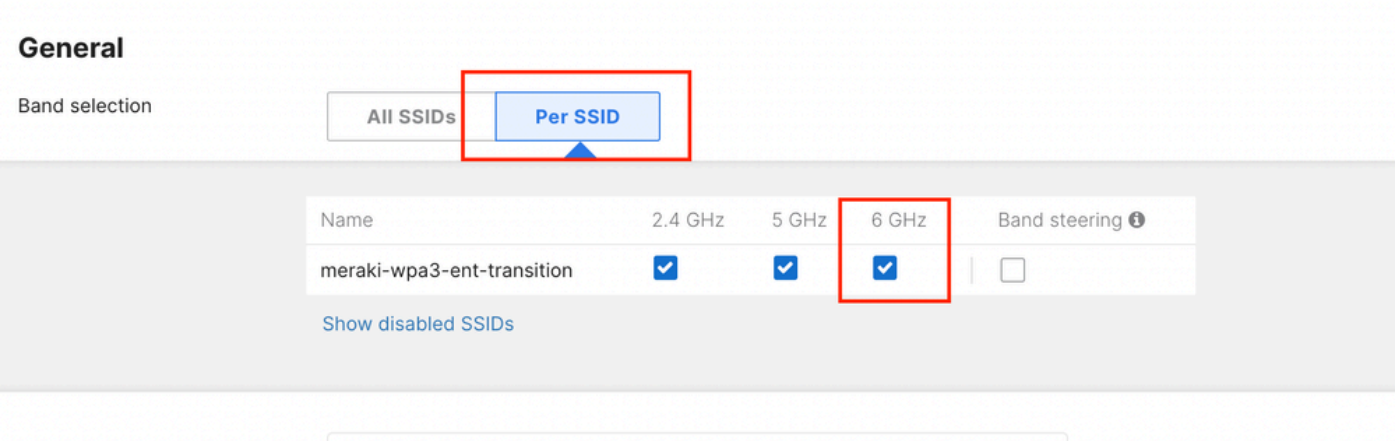
这可以批量或按单个SSID对所有SSID执行。

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

IOS XE上的WPA3-Enterprise配置

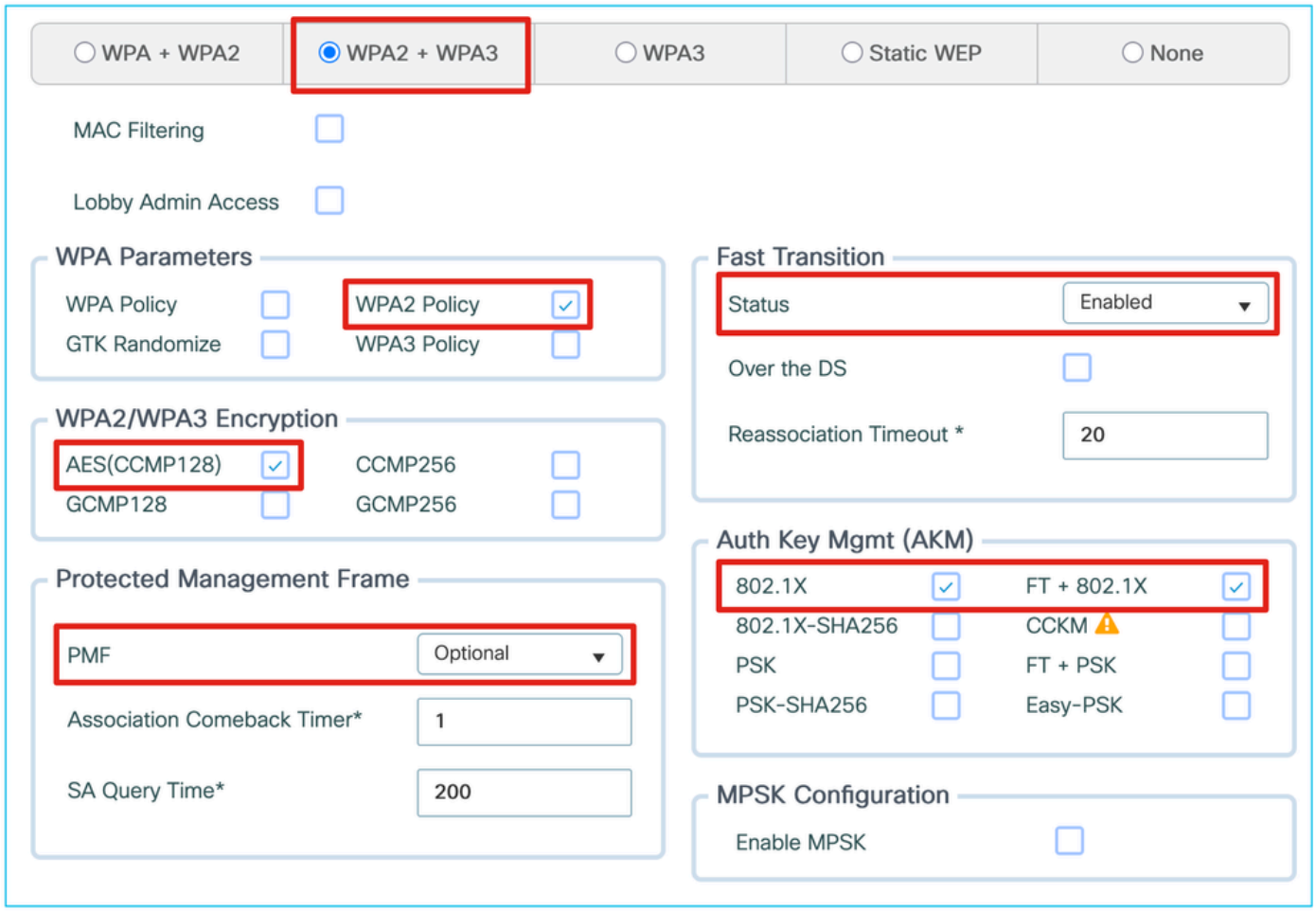
基于采用802.1X身份验证的WPA2/3的企业WLAN最容易迁移至6 GHz和/或Wi-Fi 7。

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

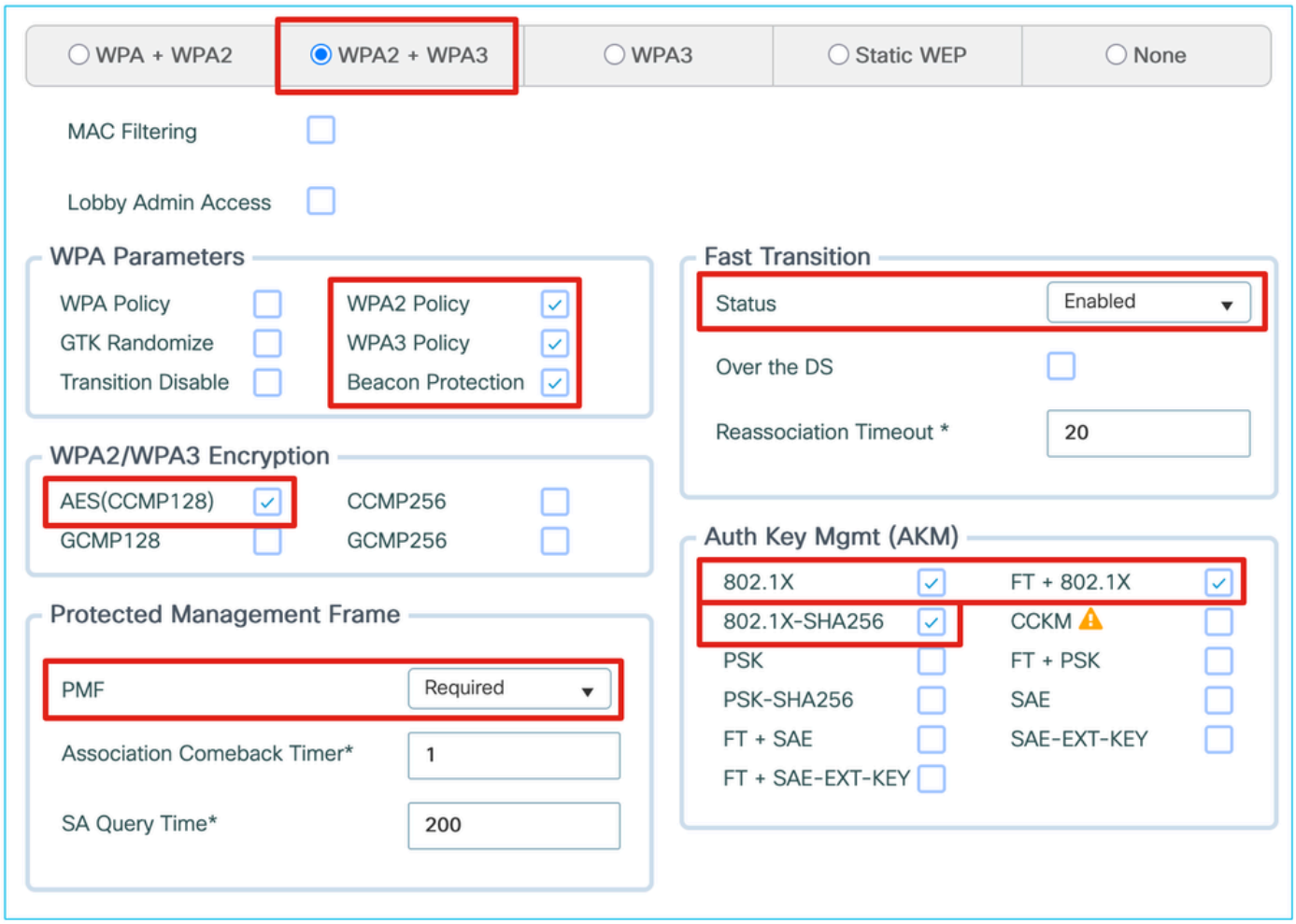
我们可以在同一WLAN上继续提供具有标准802.1X(SHA1)的WPA2。Wi-Fi 7支持需要启用Beacon Protection并根据需要设置PMF，而不是可选的；WPA2 802.1X(SHA1)可以作为向后兼容选项保留在WLAN上。这意味着您可以在单个SSID下拥有所有企业设备，前提是它们支持802.11w/PMF，这

在用于笔记本电脑和其他移动终端的当前无线网卡上非常常见。

从具有以下L2安全设置的典型WPA2 SSID:



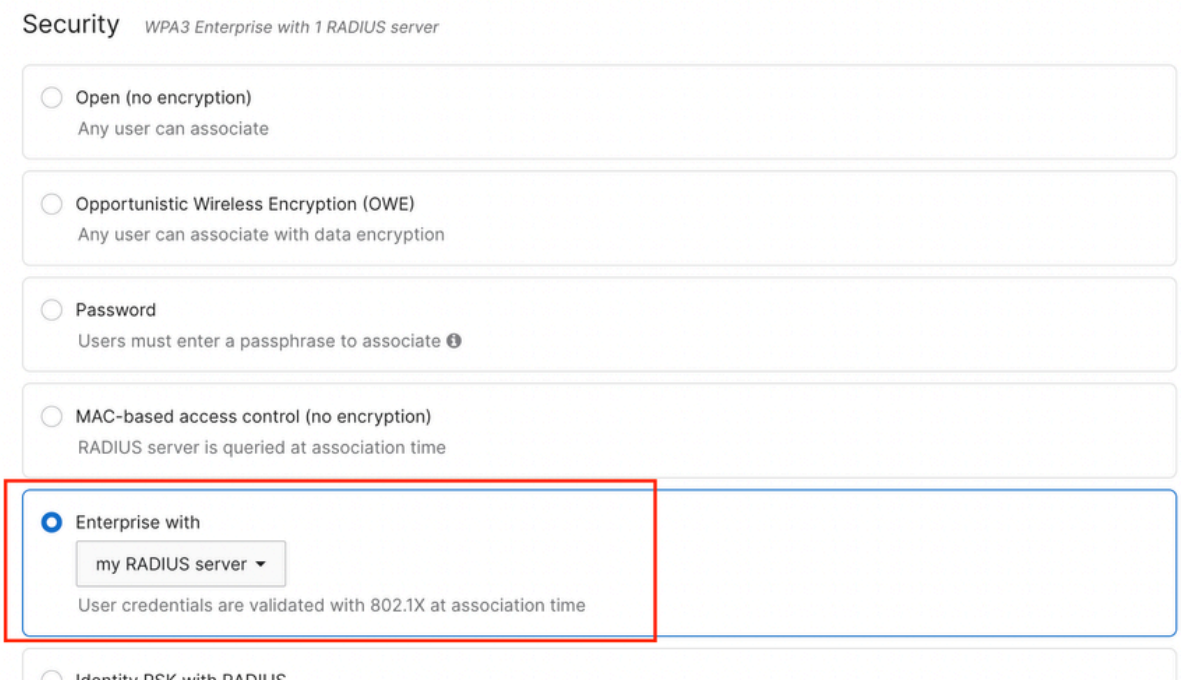
我们可以迁移WPA3、6 GHz和Wi-Fi 7支持的配置，如下所示：



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。



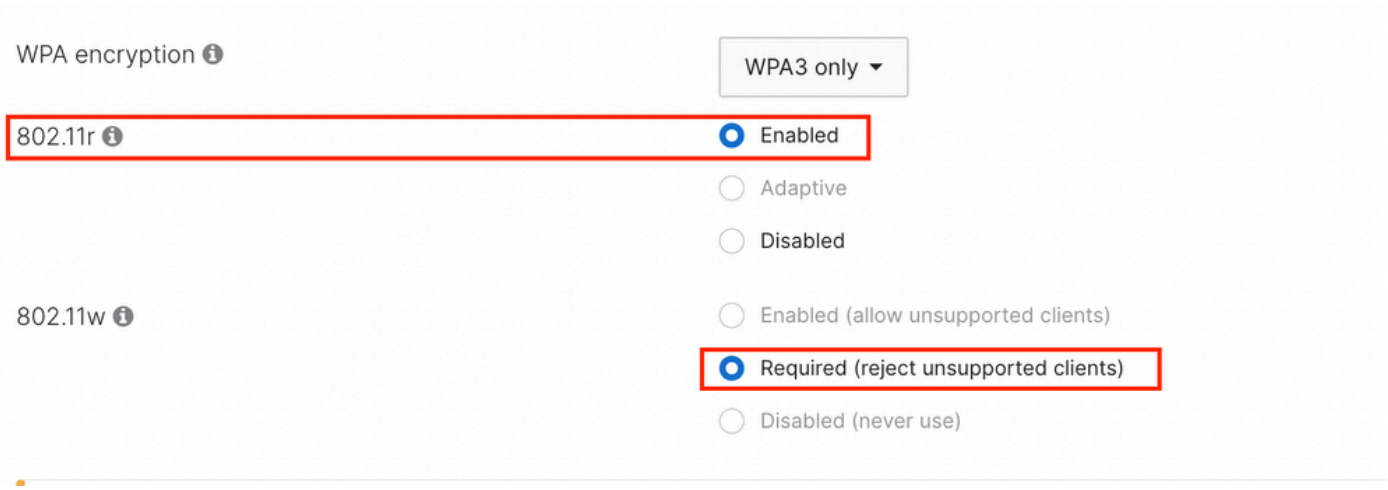
从MR 31.x开始，WPA类型包括：

- “仅WPA3”，与WPA2使用相同的密码，但需要802.11w(PMF)。
- 'WPA3 192位'，它仅允许使用包含切片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。此模式需要在RADIUS服务器上配置相同的清道夫才能启用此模式。
- “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。

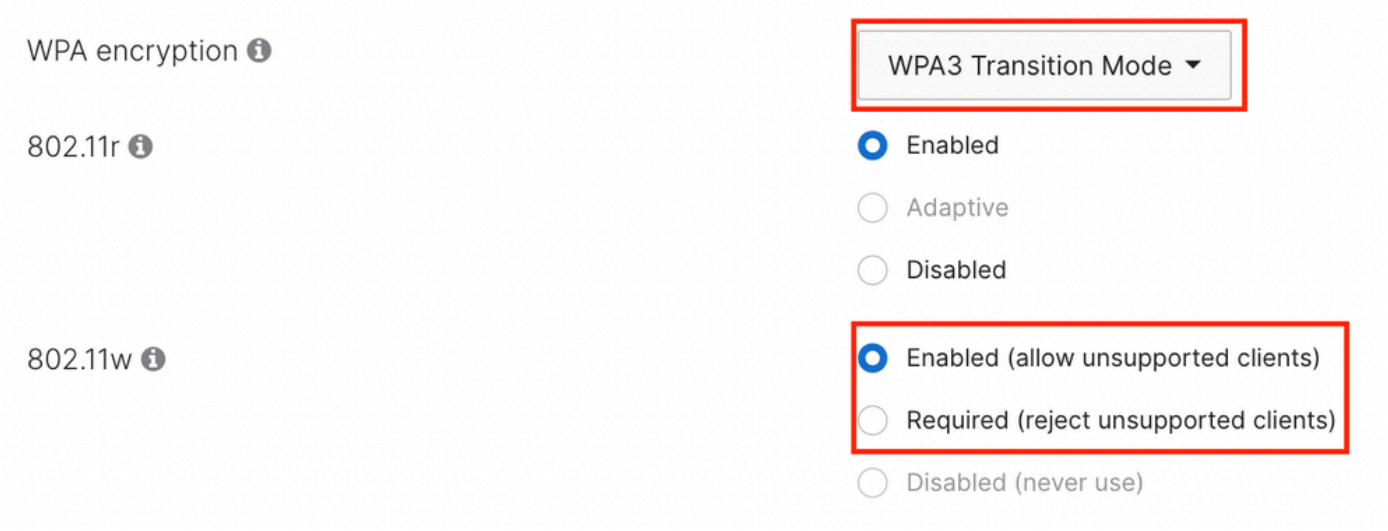
在大多数应用中，FT(802.11r)虽然不是强制性的，但是在使用外部RADIUS服务器时，必须更好地启用FT，以缓解漫游和重新身份验证延迟的影响。

6 GHz操作需要启用PMF(802.11w)。



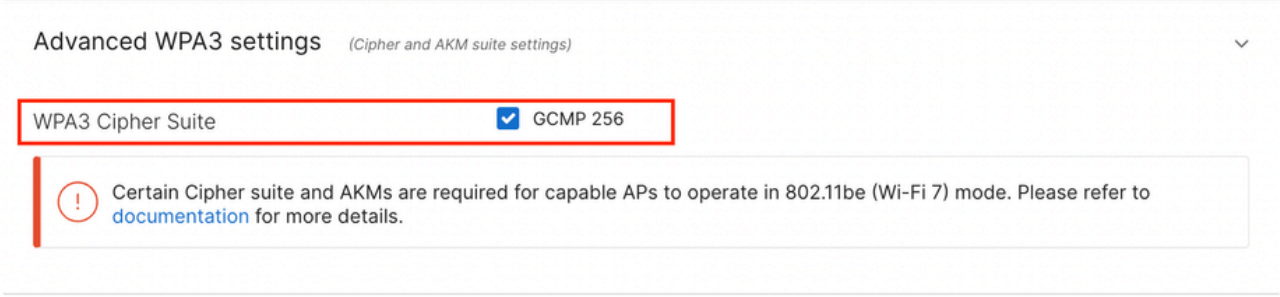
选择WPA3过渡模式时，所有能够使用WPA3的客户端都默认使用PMF。所有在6 GHz上运行的客户端都使用WPA3。

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

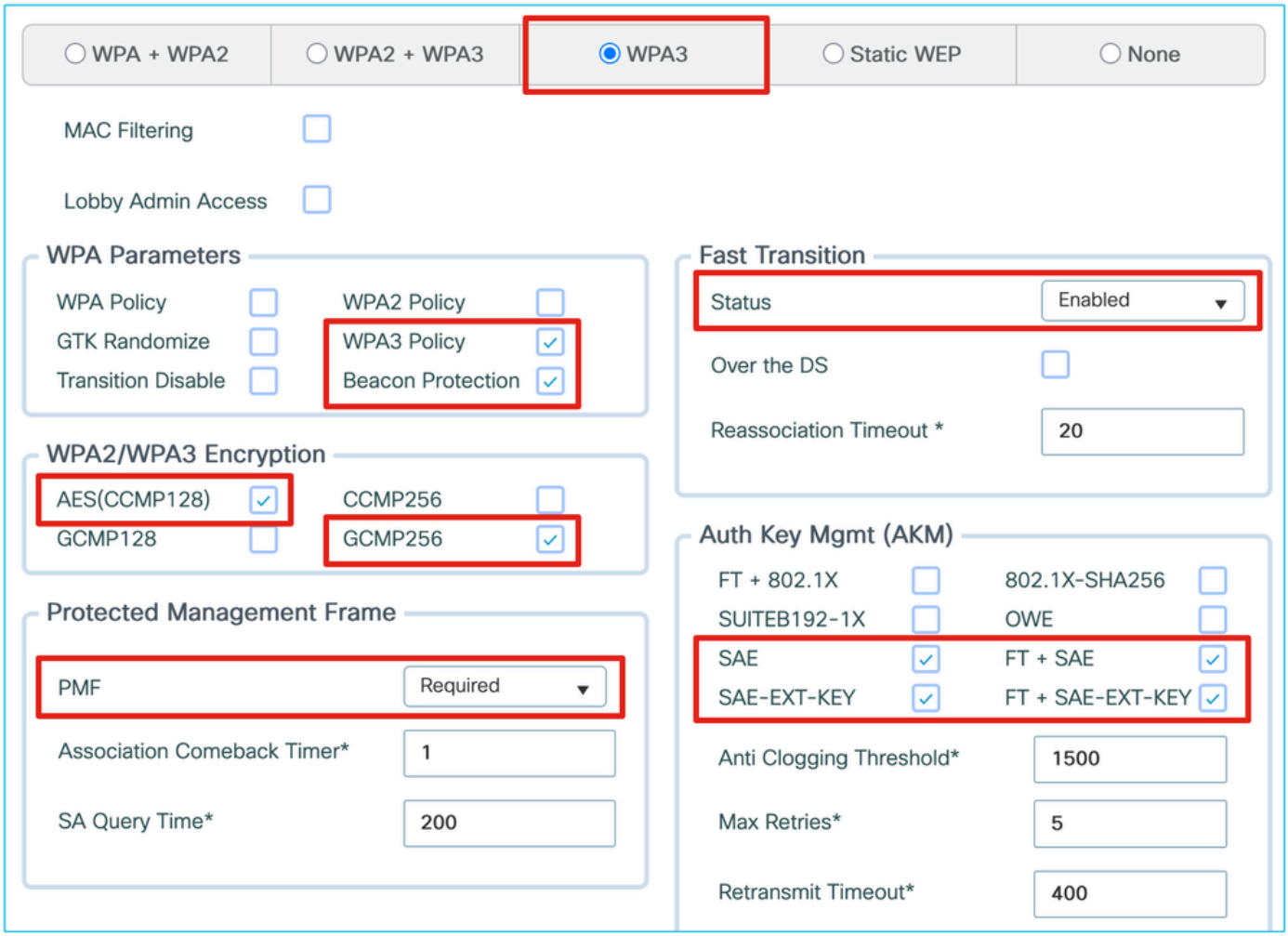
为6 GHz启用口令SSID（最多支持Wi-Fi 6E）非常简单，并且需要SAE和/或FT + SAE，以及其他WPA2 PSK AKM（如果需要）。但是，对于Wi-Fi 7支持，认证要求删除任何WPA2 PSK选项，并添加SAE-EXT-KEY和/或FT + SAE-EXT-KEY AKM以及GCMP256密码。因此，基于口令的WLAN不可能同时具有对于较旧客户端的最大兼容性和Wi-Fi 7性能。

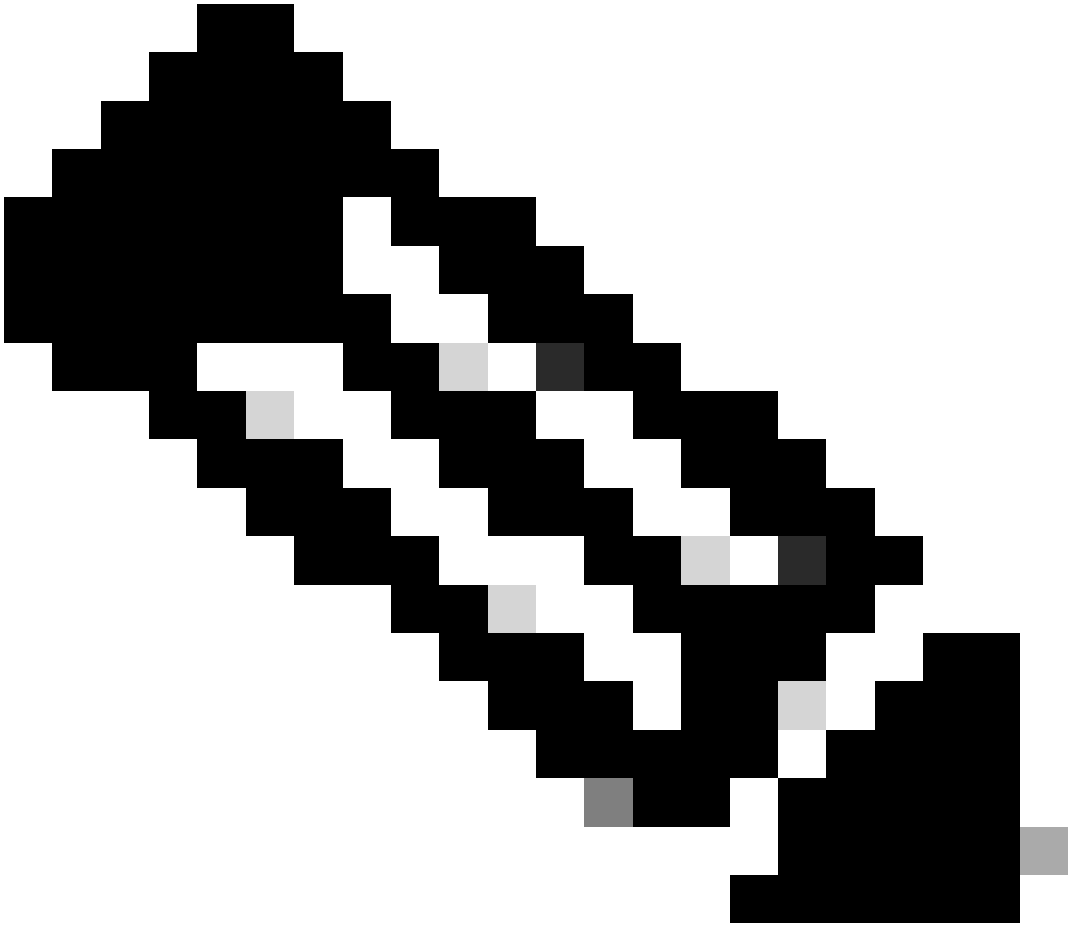
在这种情况下，我们需要为Wi-Fi 6E和Wi-Fi 7客户端配置SAE、FT + SAE、SAE-EXT-KEY和FT + SAE-EXT-KEY的专用WPA3专用SSID，提供AES(CCMP128)和GCMP256密码。

在所有这些情况下，我们强烈建议使用SAE时启用FT。SAE帧交换在资源方面成本高昂，并且比WPA2 PSK 4次握手更长。

一些设备制造商，如苹果，期望仅在启用FT时使用SAE，如果无法连接，可以拒绝连接。

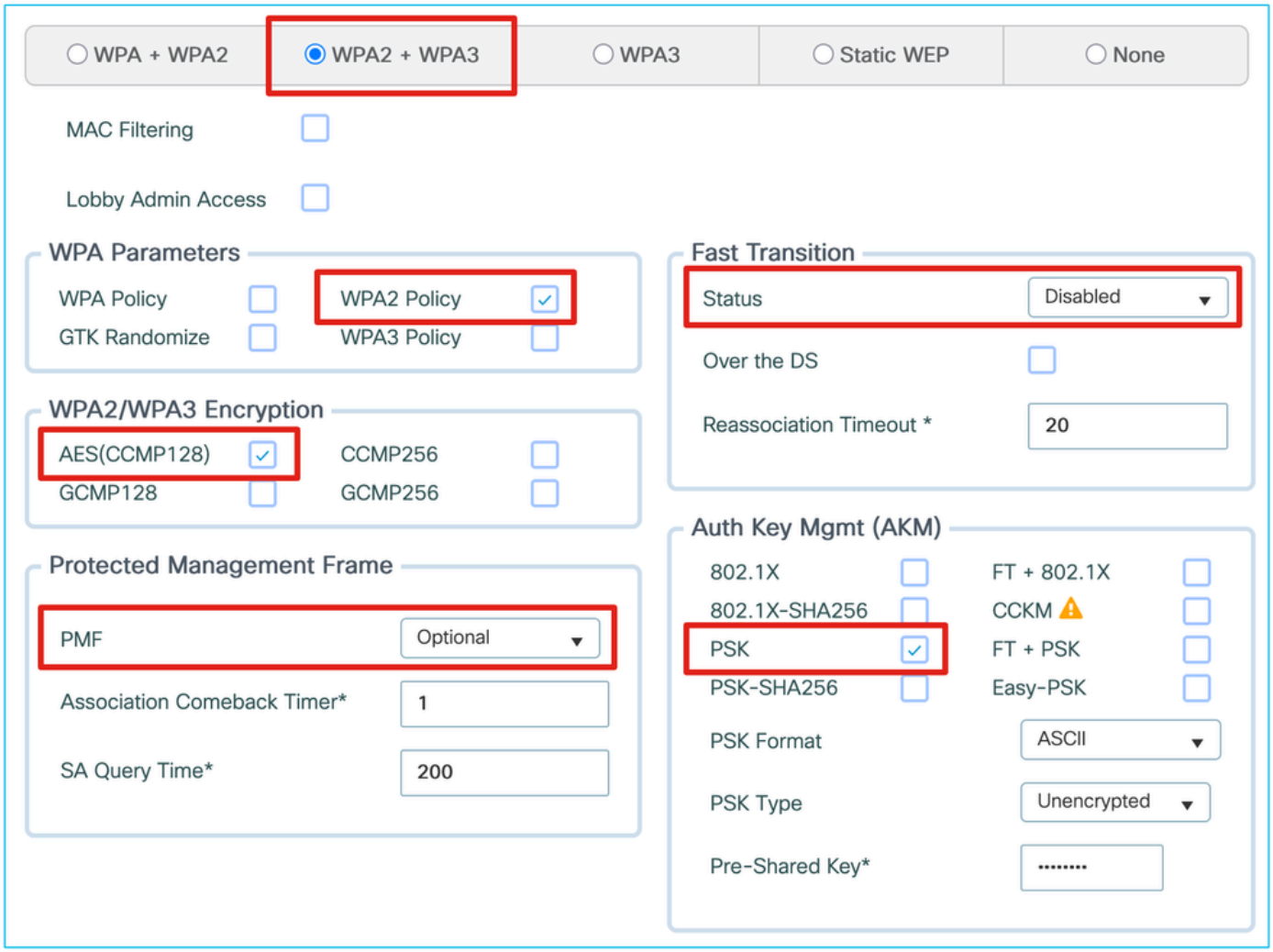
IOS XE上的WPA3-SAE和WPA2-Personal配置





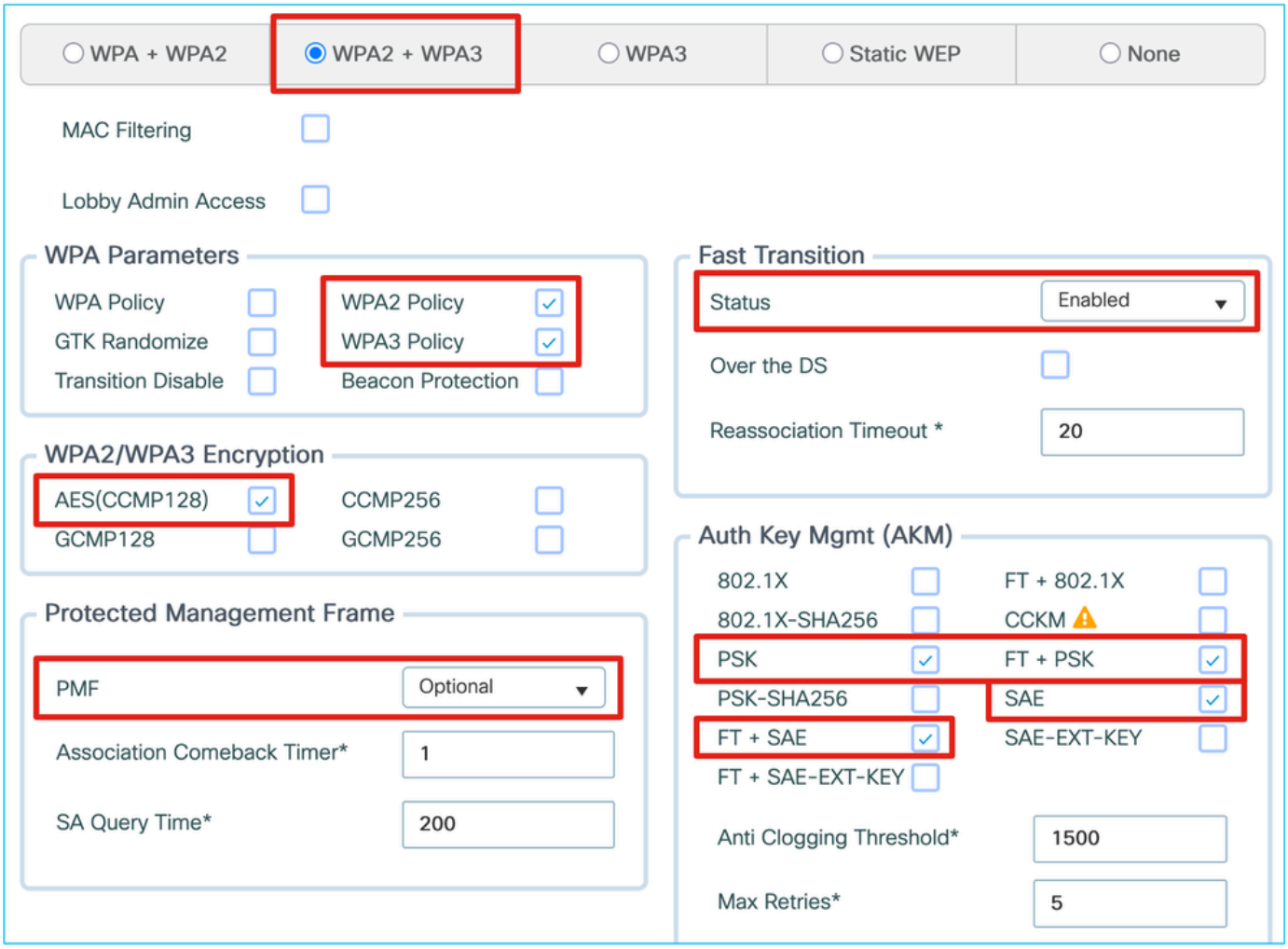
注意：如果在WLAN上启用了(FT +)SAE，并且Wi-Fi 7客户端尝试与其关联，而不是(FT +)SAE-EXT-KEY，则会拒绝该请求。只要(FT +)SAE-EXT-KEY也启用，Wi-Fi 7客户端无论如何都必须使用后一个AKM，并且此问题一定不会发生。

另一方面，另一个常规WPA2 SSID仍可容纳剩余的旧版客户端。

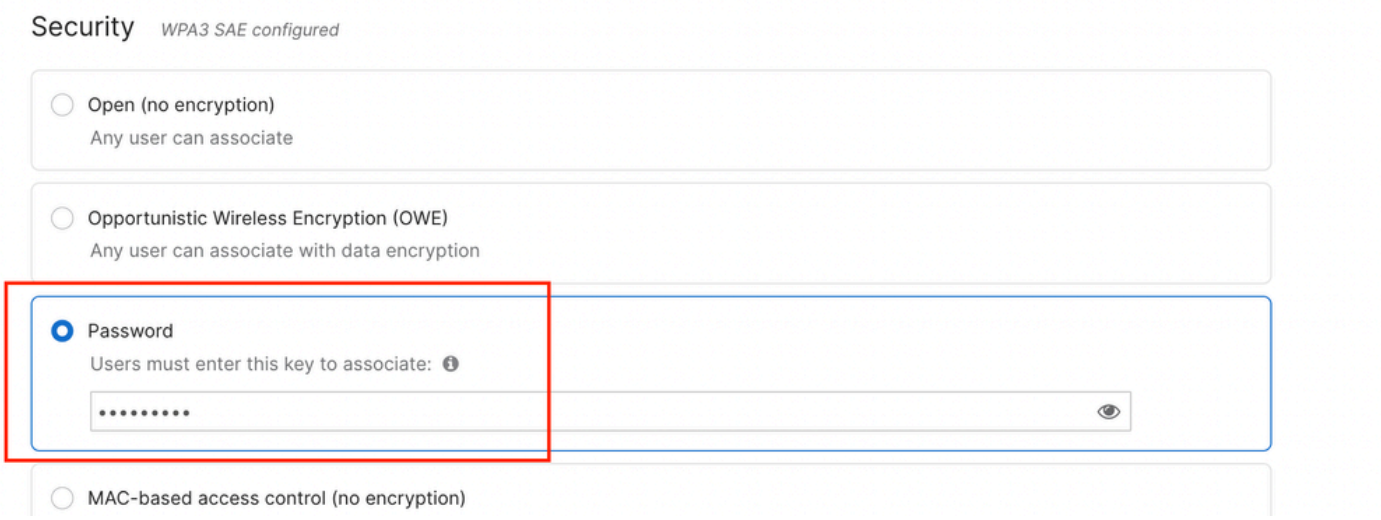


虽然此组合会增加总SSID的数量，但它允许保持一个SSID的最大兼容性，这样我们可能也会禁用其他可能影响兼容性且对许多IoT场景有帮助的高级功能，同时通过另一个SSID为较新的设备提供最大功能和性能。
当然，还有一个选项也可能是不提供Wi-Fi 7 SSID，只保留一个配置用于WPA2 PSK和WPA3 SAE的SSID。其背后的理念可能是，IoT设备无论如何都不需要Wi-Fi 7性能。

此方法仍然支持6 GHz的Wi-Fi 6E和Wi-Fi 7客户端，这些客户端最多能连接Wi-Fi 6E性能。

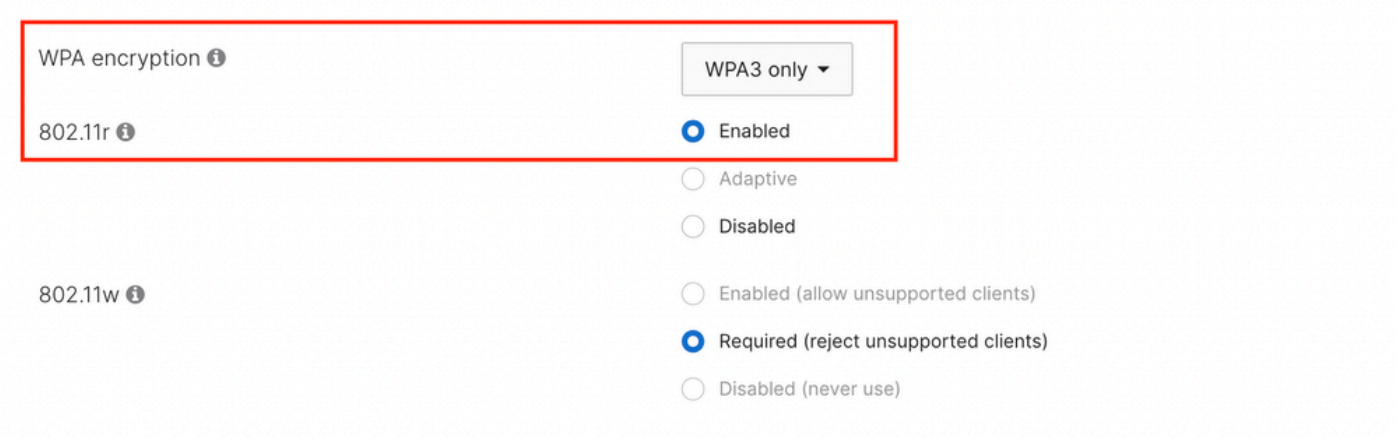


Cisco Meraki控制面板上的WPA3-SAE配置



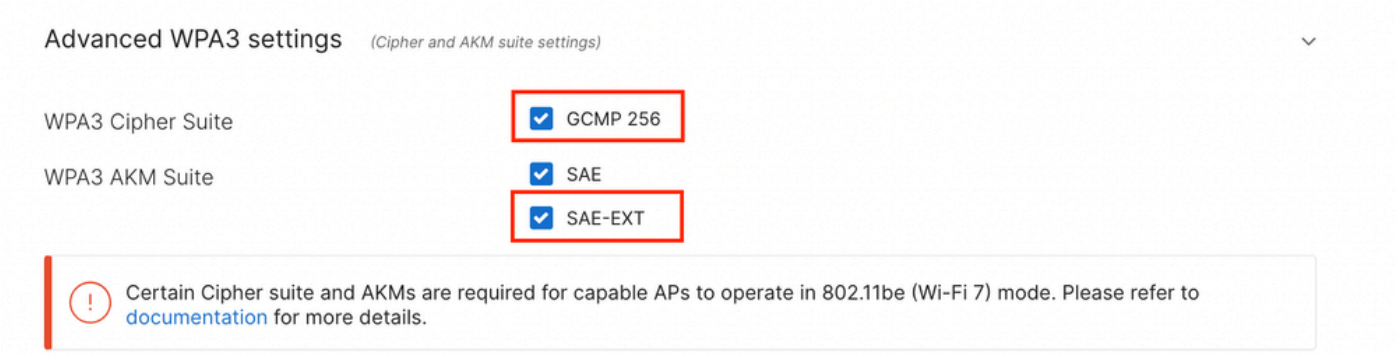
对于固件MR 30.x，唯一支持的WPA类型为“仅WPA3”，控制面板不允许您选择其他方法。

PMF在此配置中是必需的，而建议使用SAE时启用FT(802.11r)。



要允许Wi-Fi 7操作，必须在配置SSID时启用GCMP 256 chiper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

访客网络具有多种风格。通常，它们不需要802.1X凭证或密码短语进行连接，并且可能意味着启动页或门户，可能需要凭证或代码。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。

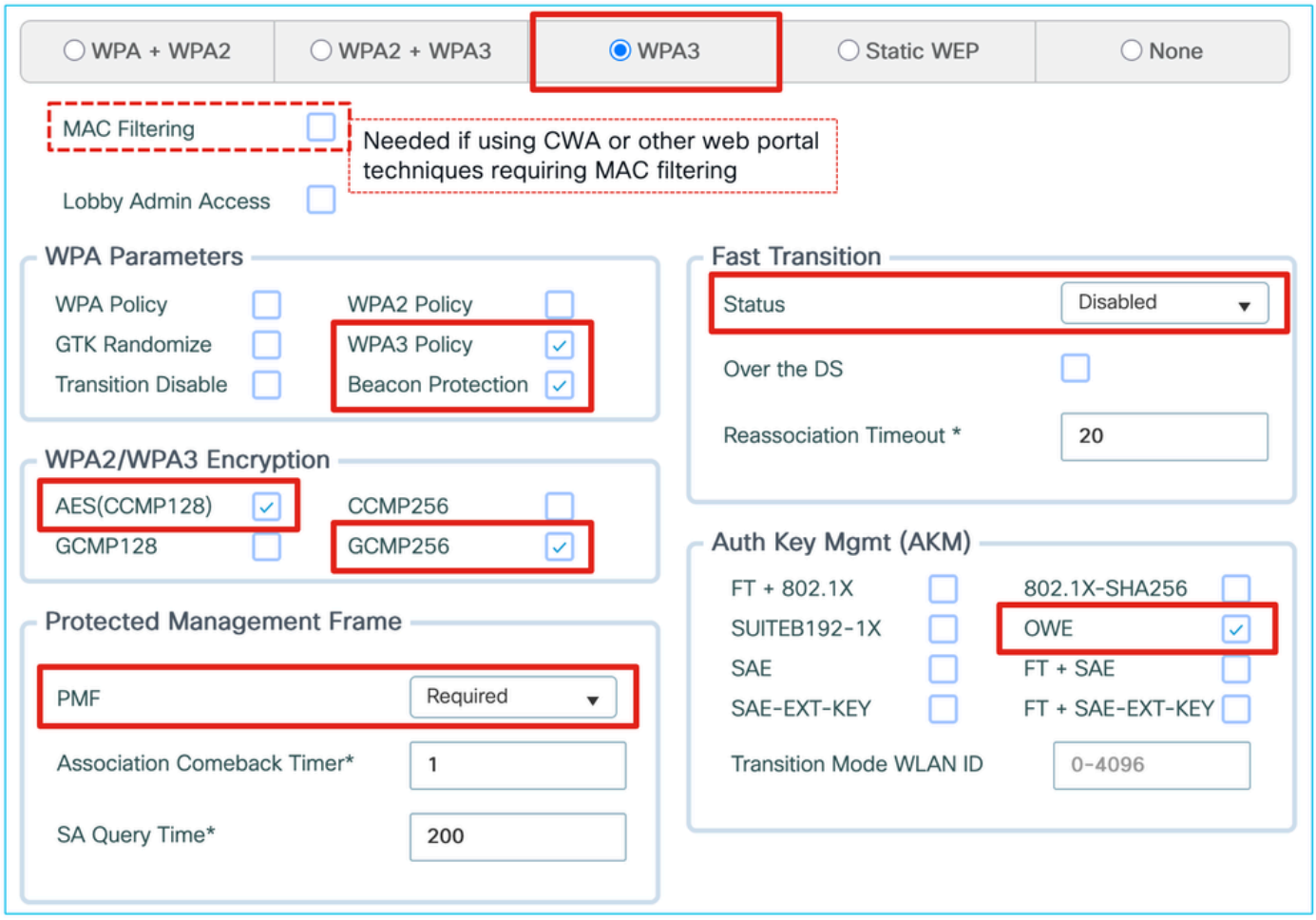
第一个非常保守的方法是最多将访客网络专用于5 GHz频段和Wi-Fi 6。这就为企业设备保留了6 GHz频段，解决了复杂性问题并带来了最大兼容性，尽管其性能不高达Wi-Fi 6E/7。

如果一方面增强型开放是提供隐私的出色安全方法，同时保持“开放”体验（最终用户无需输入任何802.1X凭证或密码），那么直到今天，它在终端之间的支持仍然有限。一些客户端仍然不支持它，即使它们支持，这种技术也并非总是能够顺利处理（设备可以将连接显示为非安全，而实际上它是安全的，或者可以将其显示为受密码保护的，即使不需要使用OWE的密码）。访客网络需要在所

有访客不受控制的设备上运行，仅提供增强型开放SSID可能为时过早，建议通过单独的SSID提供两种选项：5 GHz的开放端口和5 GHz和6 GHz的OWE端口，如果这也需要的话，两者后面都有相同的强制网络门户。过渡模式在Wi-Fi 6E、6 GHz（即使软件上仍允许过渡模式）或Wi-Fi 7上不受支持，因此不建议采用此解决方案。OWE仍支持所有门户重定向技术（内部或外部Web身份验证、中央Web身份验证……）。

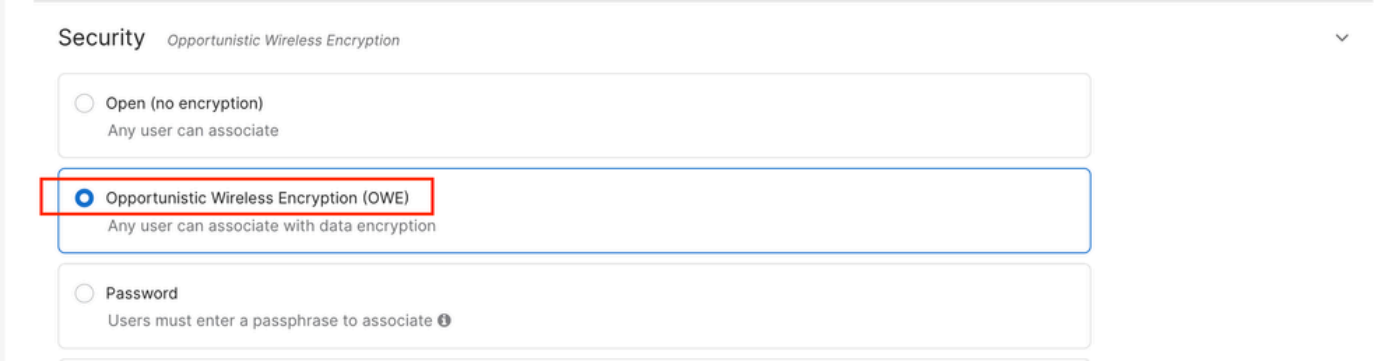
IOS XE上的OWE配置

如果我们想向访客提供6 GHz服务，建议创建具有增强型开放/OWE（机会无线加密）的独立SSID。 它可以同时提供AES(CCMP128)加密技术，最大兼容至Wi-Fi 6E客户端，并为支持Wi-Fi 7的客户端提供GCMP256位。



Cisco Meraki控制面板上的OWE配置

与在IOS XE上执行的操作类似，建议在Cisco Meraki控制面板上创建单独的访客SSID，在6 GHz上使用增强型开放/OWE操作。
可以在Wireless > Access Control中再次配置此密钥，然后选择“Opportitional Wireless Encryption(OWE)”作为安全方法。

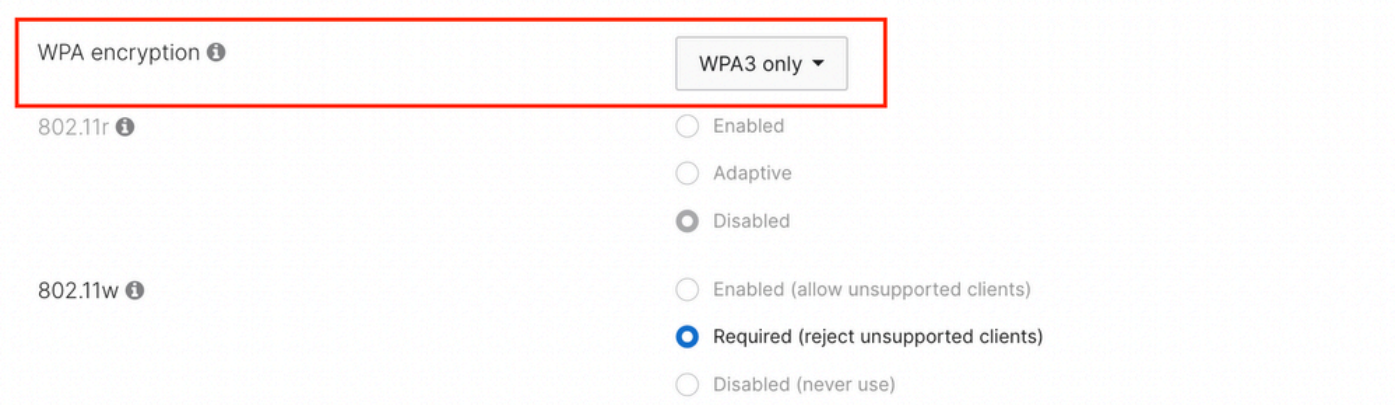


当运行固件至MR 31时，唯一支持的WPA类型是“仅WPA3”，控制面板不允许您选择其他方法。

PMF在此配置中是必需的，而FT(802.11r)无法启用。

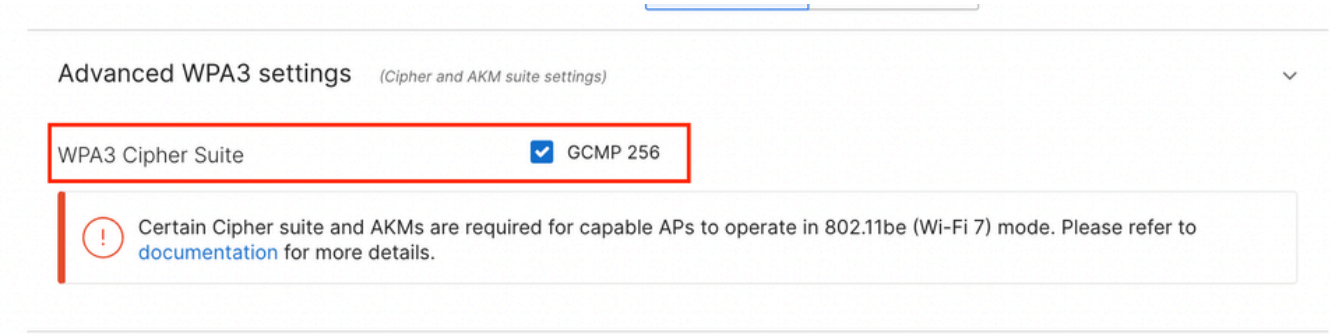
请注意，由于OWE不是WPA3标准的一部分，标记“WPA3 only”会过载；但是，此配置是指不带过渡模式的OWE。

OWE转换模式作为MR 32.1.x未来版本的一部分提供。



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位可与CCMP128一起启用，以符合Wi-Fi 7要求。



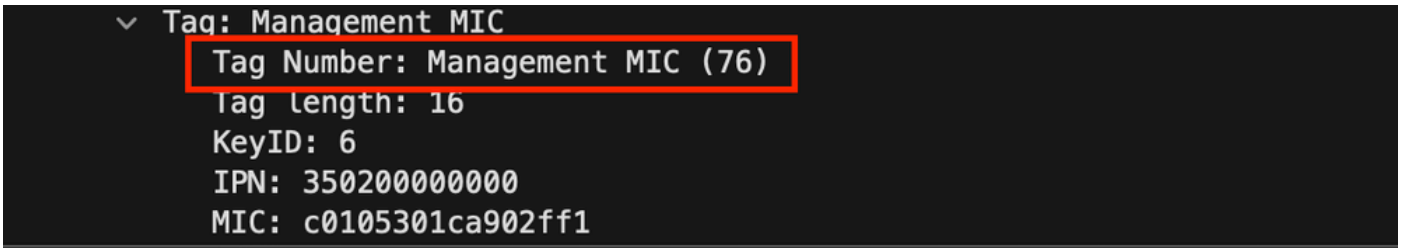
其他WPA3和相关选项

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

该功能可解决该漏洞，恶意攻击者可在该漏洞中传输信标而非合法接入点，同时修改某些字段以更改已关联客户端的安全性或其他设置。信标保护是信标中的一个额外信息元素（管理MIC），充当信标本身的签名，以证明它是合法接入点发送的，并且未被篡改。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。信标中的其他信息元素必须被不支持它的客户端忽略（这是指非Wi-Fi 7客户端），并且通常不会导致兼容性问题（除非客户端驱动程序编程不佳）。

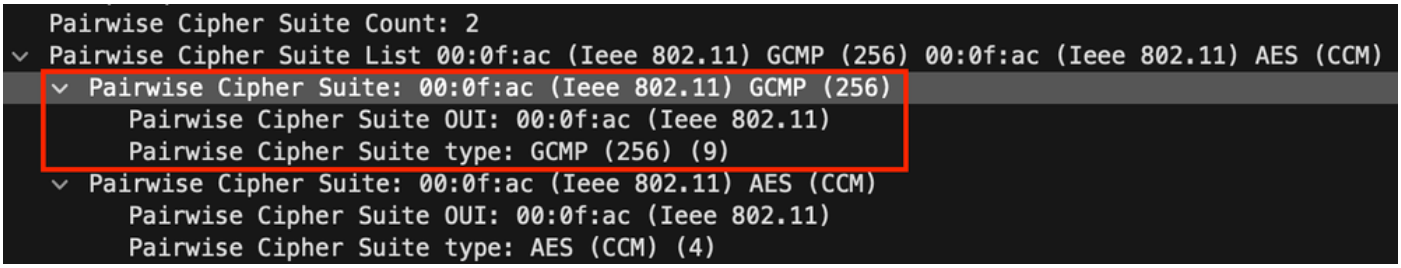
此屏幕截图显示管理MIC信息元素内容的示例：



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相关的非常具体的变体。虽然市场上的某些第一代Wi-Fi 7客户端声称Wi-Fi 7支持，但是他们有时仍然不实施GCMP256加密，如果按预期实施标准的Wi-Fi 7 AP阻止这些客户端在没有适当的GCMP256支持的情况下进行连接，则可能会出现此问题。

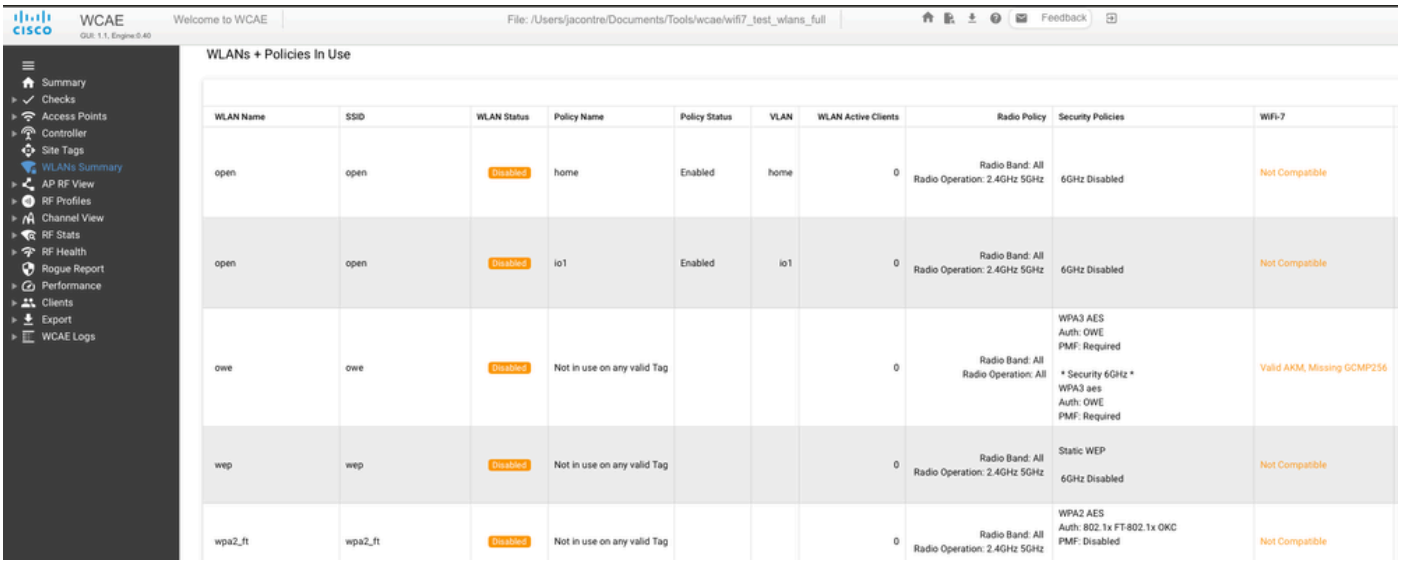
启用GCMP256后，WLAN信标帧中的稳健安全网络元素(RSNE)会在Pairwise Chiper套件列表中通告此功能，如下所示。



故障排除和验证

无线配置分析器Express最新版本(https://developer.cisco.com/docs/wireless-troubleshooting-tools/wireless-config-analyzer-express-gui/)具有一个Wi-Fi 7就绪性检查，可评估您的9800配置，以满足前面提到的所有Wi-Fi 7要求。

如果您仍然怀疑您的配置是否为Wi-Fi 7就绪，WCAE会让您知道问题所在。



参考

1. Cisco Systems。"WPA3加密和配置指南。"
2. 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）。