6 GHzおよびWi-Fi 7への移行が必要

内容

はじめに

このドキュメントでは、Wi-Fi 7のパフォーマンスを最適化し、6 GHzスペクトルを最大限に活用するための設計と設定のガイドラインについて説明します。

6 GHzおよびWi-Fi 7を使用する理由

6 GHzは、2020年にWLAN運用に使用可能になった新しい帯域で、最初はWi-Fi 6E認定によって悪用されました。Wi-Fi 6Eは引き続き同じ802.11ax規格（2.4/5 GHz帯域のWi-Fi 6認定）に準拠していますが、特定の要件が満たされている場合は6 GHz帯域のみで動作するように拡張されています。

Wi-Fi 7はIEEE 802.11be規格の認定に対応しており、6 GHzのみに制限されているWi-Fi 6Eとは異なり、2.4、5、6 GHzの3つの帯域すべてで使用するように定義されています。Wi-Fi 7には、以前の認定と比べて新機能も備わっています。

6 GHzおよび/またはWi-Fi 7にはサポートが必要な特定の要件があるため、2.4/5 GHz帯域およびWi-Fi 6まで使用していた設計と比べると、新しい設定やRF設計が必要になることが多くなります。たとえば、WEPセキュリティを使用すると802.11a/b/g以外の802.11規格の使用ができなくな

るのと同様に、よりセキュアなネットワークの採用を推進するために、より新しい規格では高いセキュリティの前提条件が満たされています。

一方、最近の6 GHz帯とWi-Fi 6E/7などの最新の認定を組み合わせることで、よりクリーンな周波数、パフォーマンスの向上、新しい使用が可能になり、既存のユースケース（音声/ビデオ会議など）をより安心して導入できます。

6 GHzの運用およびWi-Fi 7の基本要件

これらは、6 GHzおよびWi-Fi 7運用の認定に記載されているセキュリティ要件です。

6 GHz帯域の要件

6 GHz帯域では、WPA3またはEnhanced Open WLANのみを許可します。つまり、次のいずれかのセキュリティオプションを意味します。

- WPA3-Enterprise（802.1X認証）
- パスフレーズを使用したWPA3同時認証の等号(SAE)（WPA3-Personalとも呼ばれます）。SAE-FT（Fast Transitionを使用したSAE）もAKMの一種であり、SAEハンドシェイクは単純なものではなく、FTでは長い交換をスキップできるため、実際に使用することが推奨されます。
- Opportunistic Wireless Encryptionによる拡張オープン(LEAN)

WPA3 v3.4の仕様（セクション11.2）では、6 GHzではEnhanced Open Transition(EOT)モードはサポートされていませんが、多くのベンダー(IOS® XE 17.18までのシスコを含む)では、まだ対応していません。したがって、たとえば5 GHz上のオープンSSIDと、5 GHzおよび6 GHz上の対応する拡張オープンSSIDを、移行モードを有効にして、これらすべてを標準仕様に従わずに設定することは技術的に可能です。ただし、このようなシナリオでは、通常のオープンSSIDを5 GHzに維持しながら、遷移モードなしで6 GHzのみで使用可能な拡張オープンSSID（6 GHzをサポートするクライアントは通常は拡張オープンもサポート）を設定することが想定される必要があります。

802.11w/Protected Management Frame(PMF)の適用を除き、WPA3-Enterpriseに固有の暗号やアルゴリズムに関する新しい要件はありません。シスコを含む多くのベンダーは、802.1X-SHA256または「FT + 802.1X」（実際にはSHA256を使用する802.1Xで上位にFast Transition）のみをWPA3準拠と見なし、単純な802.1X（SHA1を使用）をWPA2の一部と見なしているため、6 GHzには適合サポートされません。

Wi-Fi 7の要件

802.11be規格のWi-Fi 7認定により、Wi-Fi Allianceはセキュリティ要件を強化しました。802.11beデータレートとプロトコルの向上を使用できるプロトコルもあれば、マルチリンク動作(MLO)のサポートに固有のプロトコルもあり、互換性のあるデバイス（クライアントやAP）が同じアソシエーションを維持しながら複数の周波数帯域を使用できます。

一般に、Wi-Fi 7では次のいずれかのセキュリティタイプが必須です。

- AES(CCMP128)および802.1X-SHA256またはFT + 802.1Xを使用するWPA3-Enterprise（名前に明示されていない場合でもSHA256を使用） これは、6 GHz帯域に対する既存のWPA3セキュリティ要件との違いを表すものではありません。
- WPA3-Personal(GCMP256、SAE-EXT-KEY、FT + SAE-EXT-KEY（AKM 24または25））Wi-Fi 6Eは、通常のAES(CCMP128)を使用するだけでWPA3 SAEおよび/またはFT + SAEを必須とし、追加の拡張キーを使用しないため、これはWi-Fi 7専用に導入された新しい暗号です。
- GCMP256による拡張オープン/借入AES(CCMP128)は同じSSIDで設定できますが、AES 128を使用するクライアントはWi-Fi 7をサポートできません。Wi-Fi 7以前は、Enhanced Openをサポートするほとんどのクライアントが AES 128のみを使用していたため、これは新たに強化された要件です。6 GHzのサポートに関しては、移行モードは許容されません。

いずれの場合も、WLANでWi-Fi 7をサポートするには、Protected Management Frames(PMF)とビーコン保護も必要です。

このドキュメントの執筆時点ではWi-Fi 7はまだ新しく、可能な限り早期にリリースされたため、多くのベンダーはこれらすべてのセキュリティ要件を当初から適用していませんでした。

最近では、Wi-Fi 7認定に準拠するために、設定オプションを段階的に強化しています。バージョン固有の動作を次に示します。

17.18.1 以降

IOS XE 17.18以降のバージョンでは、Wi-Fi 7の要件に一致するセキュリティパラメータ（ビーコン保護、PMF、および前述のようにWLANの種類に応じて適切なAKM、LEANまたはSAE-EXTの場合にWi-Fi 7 MLOを実現するためのGCMP256の存在）がWLANにある場合にのみ、特定のWLANを有効としてアドバタイズします。 AES128の存在はSSIDで許容されますが、使用する場合はWi-Fi 6Eのみを提供し、Wi-Fi 7 MLOは提供しません。

クライアントはWi-Fi 7として関連付けられ、使用するセキュリティ方式に関係なくWi-Fi 7データレートを実現できます（WLANでサポートされている場合）。 ただし、クライアントは、Wi-Fi 7セキュリティの厳格な要件を満たしている場合、または拒否される場合にのみ、MLO対応（1つ以上の帯域）として関連付けることができます。

17.15.3以降の17.15.xバージョン

このブランチでは、セキュリティ設定に関係なくWi-Fi 7がグローバルに有効になっている限り、すべてのWLANがWi-Fi 7 SSIDとしてブロードキャストされます。

クライアントは、Wi-Fi 7対応として関連付けられ、WLANでサポートされていれば、使用するセキュリティ方式に関係なくWi-Fi 7データレートを実現できます。ただし、クライアントは、Wi-Fi 7セキュリティの厳格な要件を満たす場合にのみ（1つ以上の帯域で） MLO対応として関連付けることができ、それ以外の場合は拒否されます。

これは問題を引き起こす可能性があります。初期のWi-Fi 7クライアントがGCMP256などのより安全な暗号をサポートできない場合、セキュリティ設定がWi-Fi 7要件に一致しないWLANにWi-Fi 7 MLO対応として関連付けようとすると、問題が発生します。このような状況では、クライアントは無効なセキュリティ設定（WLANで設定することは許可されている）のために拒否されます

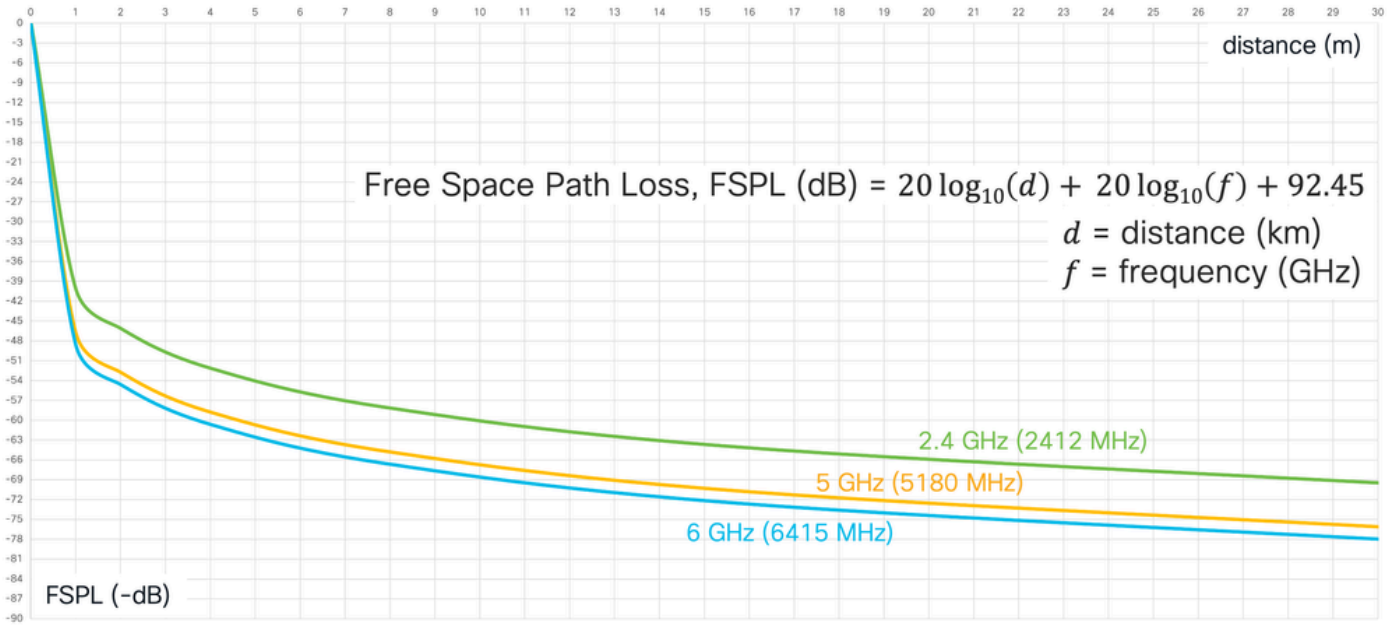
。

6 GHzカバレッジの無線設計に関する考慮事項

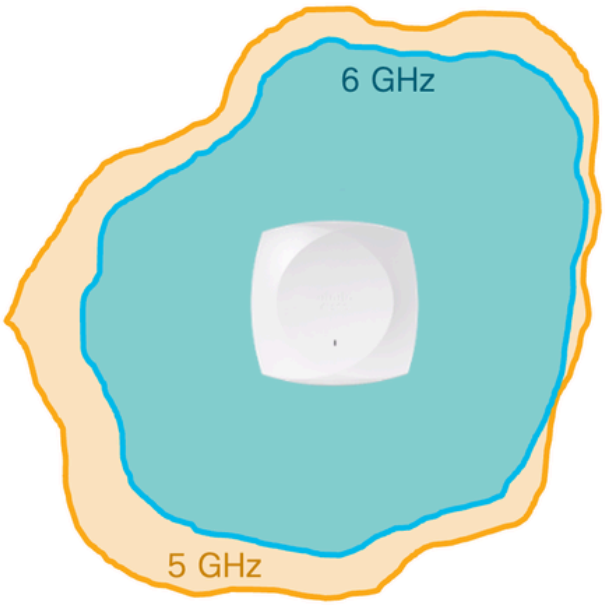
このセクションでは、サイト調査の完全な規範的なガイドになる意味はなく、6 GHzカバレッジを設計する際の基本的な考慮事項について簡単に説明します。特に、Wi-Fi 6Eまたは7に移行する2.4/5 GHz用の既存のインストールがある場合は重要です。
2.4または5 GHzで使用された新しいWi-Fiの導入に関しては、6 GHzの新しい無線プロジェクトに、対応する専用6 GHzサイト調査も含める必要があります。

Wi-Fi 6E/7以前のAPが特定の5 GHzカバレッジ用にすでに配置されていて、必要な場合には、Wi-Fi 6E/7対応APと交換でき、6 GHzでも良好なカバレッジを得られると予測できます。この理論が機能するためには、既存のAPが、目的のニーズ（データのみ、音声、特定のアプリケーションなど）に適した5 GHzカバレッジをすでに提供している必要があります。また、すでに最大限度の3 ~ 4送信電力レベルを満たしている必要があります。通常、APには7 ~ 8の電力レベルがあり、各電力レベルは送信電力を半分に割ります。これは、APが許可された送信電力範囲のメディアを使用している場合に、快適な場所になることを意味します。

空きスペース損失の計算によると、6 GHzの信号は5 GHzを超える2 dB減衰されます。さらに、6 GHzの信号は、同等の5 GHzの信号よりも障害物の影響を受けやすくなります。



Cisco APは、送信電力を1レベルずつ増減する場合、3 dBの「ジャンプ」によって増減します。たとえば、送信電力が11 dBmの電力レベル4から電力レベル3に移行したAPは、送信電力を14 dBmに増やします（電力レベル4の11 dBmと電力レベル3の14 dBmは、モデルや世代が異なれば、同じ電力レベル番号でも送信電力値がdBm単位でわずかに異なる場合があるため、一般的な例です）。



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.

たとえば、Wi-Fi 6E/7以前のAPが電力レベル4で5 GHzの良好なカバレッジをすでに提供している場合、同様の5 GHz無線パターンを持つ新しいWi-Fi 6E/7 APが、既存の5 GHzネットワークに大きな影響を与えることなく、以前のAPを置き換える可能性があります。

また、新しいWi-Fi 6E/7 APの6 GHz無線は、1つの送信電力レベル（つまり3 dB）を高くするだけで、5 GHz無線と同様の6 GHzカバレッジを提供できます。

APの5 GHz無線で5 GHzが既に最大未満の3 ~ 4電力レベルで正しくカバーされている場合、対応する6 GHz無線は、同等のカバー範囲を確保するために、最大未満の2 ~ 3電力レベルに設定できます。

また、6 GHz無線が最大出力より2 ~ 3電力レベル低い正しいカバレッジをすでに提供している場合、予期しない一時的なカバレッジホール（ネイバーAPの障害、未発表の障害、新しいRFニーズなど）を回避しようとするなど、数レベル高くても非常に高い可能性があります。

Wi-Fi 6E/7以前のAPとWi-Fi 6E/7 APの間のローミング動作

同じカバレッジエリアで異なる標準や周波数帯域をサポートするAPを導入することは、常に推奨される方法ではありません。特に、異なる世代のAPが「ソルトアンドペッパー」方式（同じゾーンで互いに混在する方式）で設置されている場合には推奨されません。

ワイヤレスコントローラは、複数のAPモデルのグループからの操作（たとえば、ダイナミックチャネル割り当て、送信電力制御、PMKキャッシュの配布など）を処理できますが、異なる標準や異なる周波数帯域の間を移動するクライアントは必ずしも適切に処理できず、たとえばローミングの問題が発生する可能性があります。

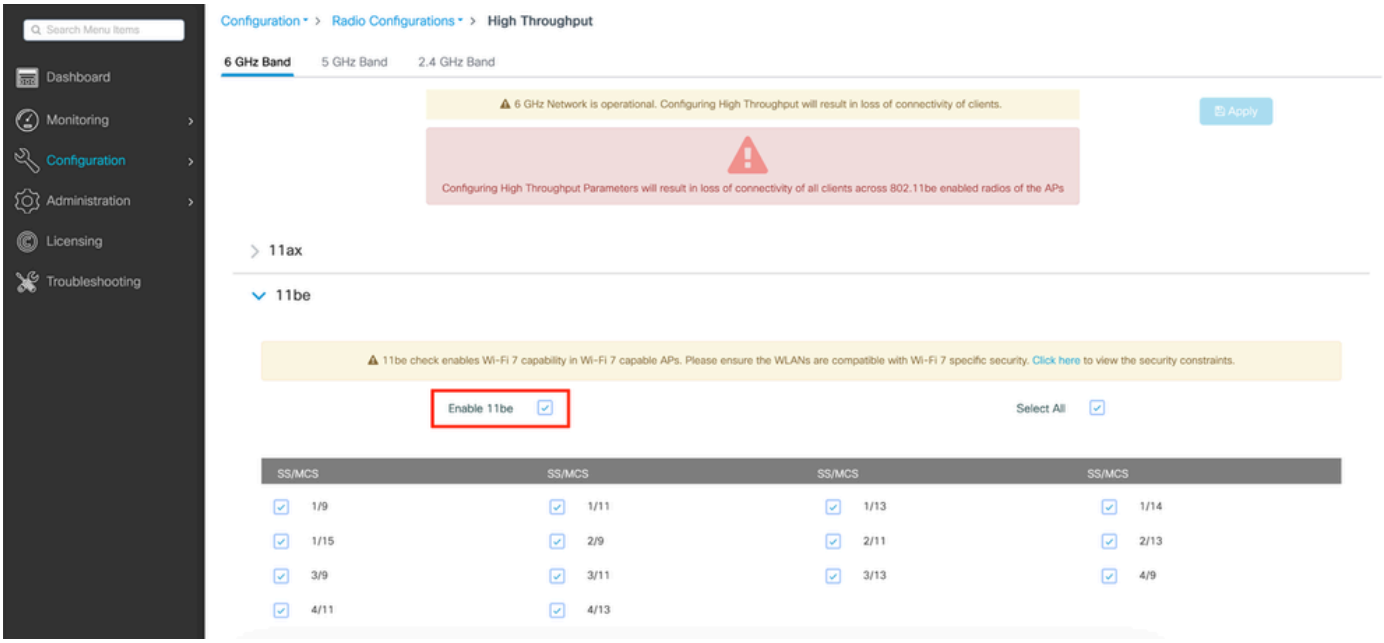
さらに、新しい標準のため、Wi-Fi 6E/7 APはWPA3のGCMP256暗号をサポートします。ただし、一部のWi-Fi 6 APおよびそれ以前のモデルでは、常に同じとは限りません。パスフレーズ/WPA3 – パーソナルSSIDおよび拡張Open/BORING SSIDの場合、AES(CCMP128)およびGCMP256暗号の両方の設定が必要、特定のWi-Fi 6（90など） 105、9115、および9120シリーズ)はGCMP256をサポートしておらず、Wi-Fi 6E/7対応クライアントを含むアソシエーションクラ

イアントにのみAES(CCMP128)暗号を提供できます。GCMP256をサポートする隣接するWi-Fi 6E/7 APとの間でローミングする必要があるこれらのWi-Fi 6E/7クライアントは、AES(CCMP128)とGCMP256の間の暗号の再ネゴシエーションがトランスペアレントローミングではサポートされていないため、まったく新しい関連付けを通過する必要があります。さらに、一般に、新しい機能を提供するAPと、これと同じ機能を提供しないAPを同じエリアに配置するのは最適ではありません。移動の際にクライアントがこれらの機能を安全に使用できず、スティッキ状態や切断が発生する可能性があります。
このシナリオは稀なケースですが、WLANでGCMP256暗号が設定されている場合、9105/9115/9120 APと9130/9124/916x/917x APの間でのWi-Fi 6E/7クライアントのローミングは不可能であり、後者のシリーズはGCMP256をサポートしていません。

6 GHz上で40 MHz以上のチャネル幅を使用すると、6 GHz対応のクライアントにスティッキ性が生じる可能性があり、他の帯域への再アソシエーションを拒否できます。これは、同じローミングエリアに6 GHz対応のAPと6 GHz非対応のAPを混在させないことのもう1つの理由です。

Wi-Fi 7をグローバルに有効化

Wi-Fi 7をサポートするIOS XEバージョンをインストールまたはアップグレードする際、デフォルトでWi-Fi 7のサポートはグローバルに無効になっています。
これを有効にするには、各2.4/5/6 GHz帯域のHigh Throughput設定メニューの下を移動し、チェックボックスをオンにして11beを有効にする必要があります。



別のオプションとして、ターミナルコンフィギュレーションモードでSSH/コンソールを使用して次の3つのコマンドラインを実行することもできます。

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

警告ノートに記載されているように、これらの設定を変更しようとする際に802.11beサポートのステータスを変更すると、Wi-Fi 7 APの無線ですべてのクライアントの接続が短時間失われます。MLO（複数の帯域に同時に接続するクライアント）を実行するには、クライアントが接続するすべての帯域で11beを有効にする必要があります。すべての帯域で有効にする必要はありませんが、単にパフォーマンスを向上させるためにお勧めします。

使用例

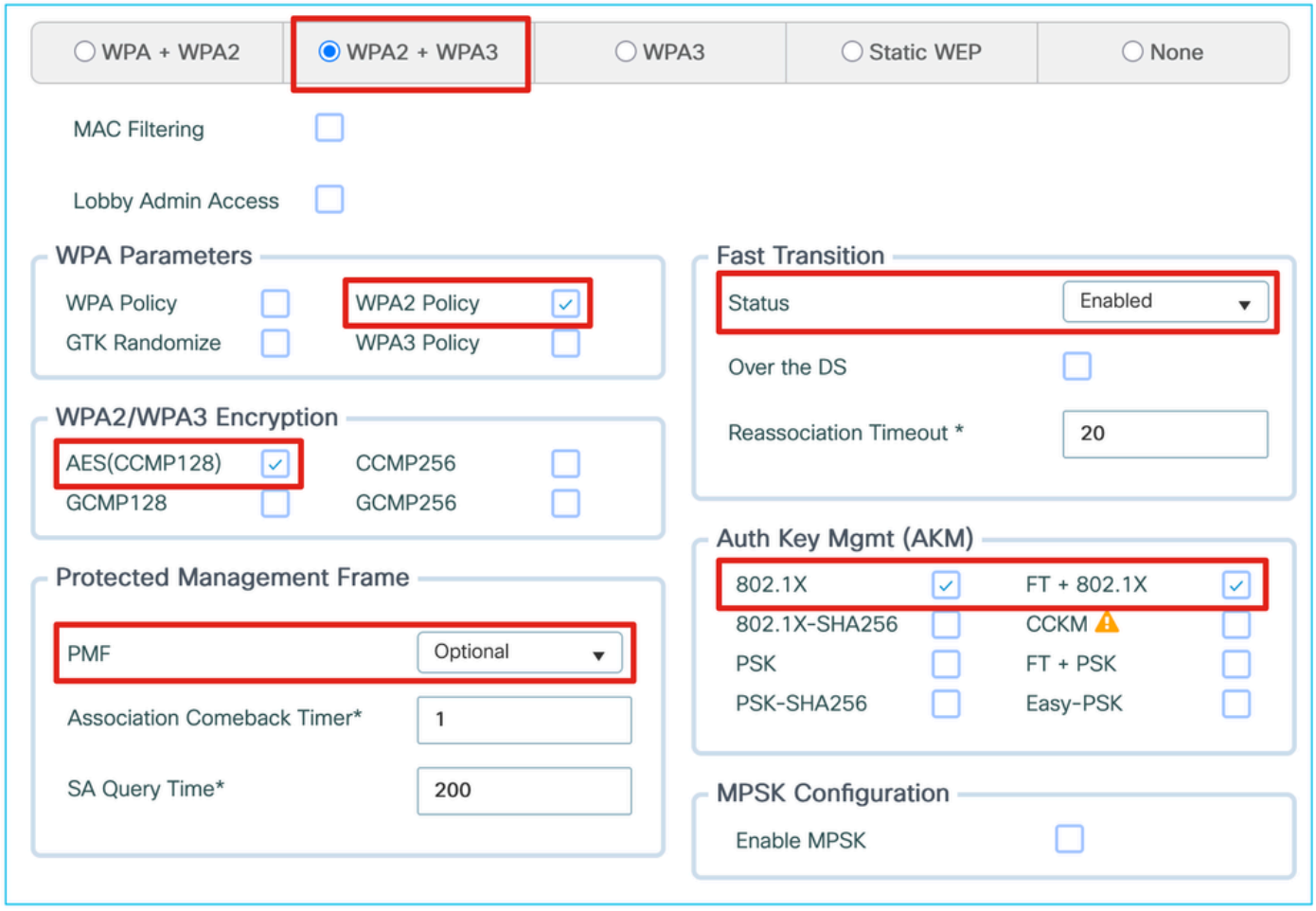
802.1X/WPA3 – エンタープライズネットワーク

6 GHzまたはWi-Fi 7への最も簡単な移行は、802.1X認証を使用するWPA2/3に基づくエンタープライズWLANです。

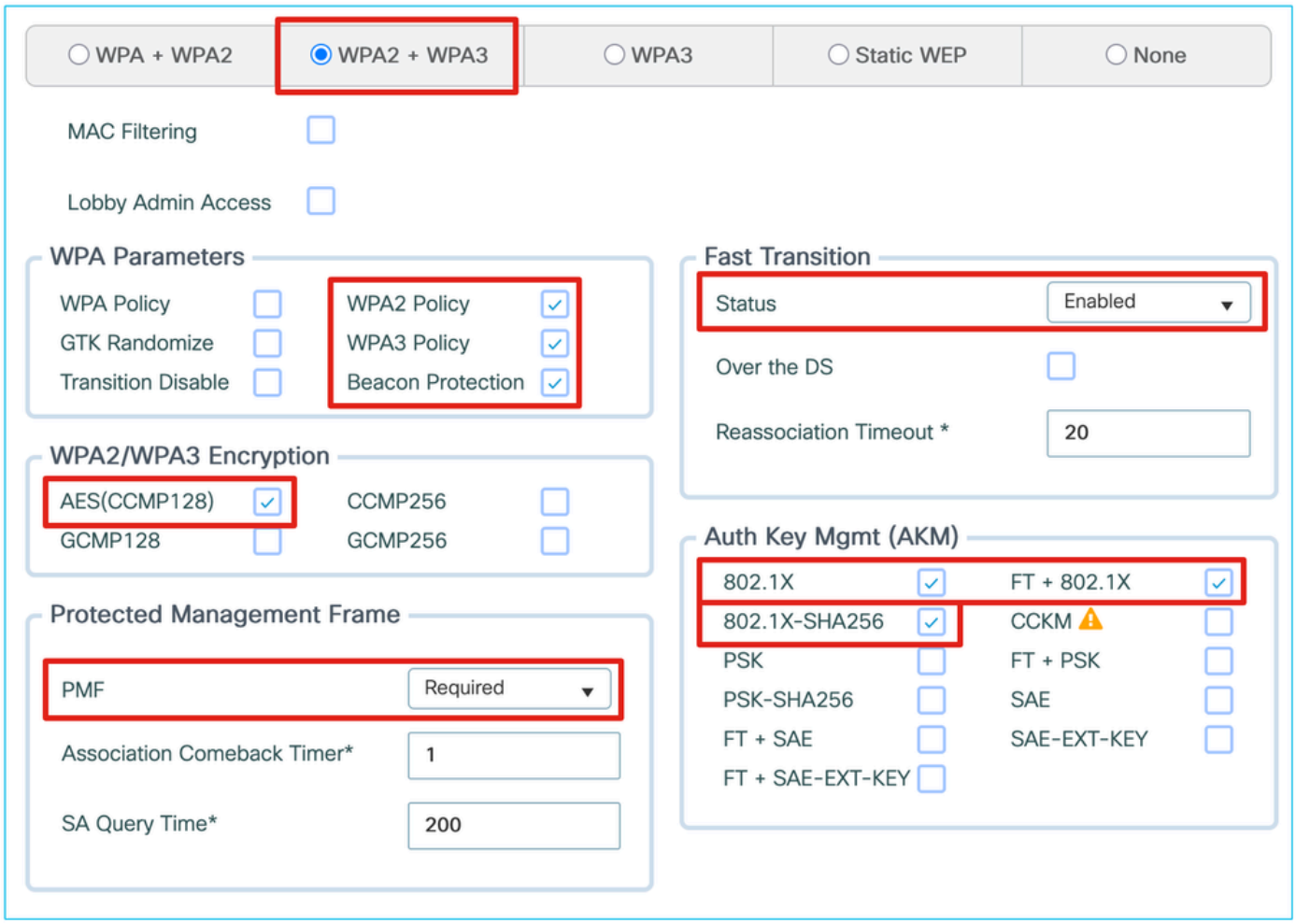
6 GHzの802.1X SSIDを有効にするには、PMFのサポートを有効にするだけでなく、オプションであっても、802.1X-SHA256および/またはFT + 802.1X AKMを有効にする必要があります。これらはどちらもWPA3に準拠しています。

同じWLANで、標準の802.1X(SHA1)を使用したWPA2を引き続き提供できます。Wi-Fi 7サポートでは、ビーコン保護を有効にし、オプションではなく必要に応じてPMFを設定する必要があります。WPA2 802.1X(SHA1)は、下位互換性オプションとしてWLAN上に残ることができます。つまり、802.11w/PMFをサポートすれば、すべての企業デバイスを1つのSSIDで管理できます。802.11w/PMFは、ラップトップやその他のモバイルエンドポイントの現在の無線NICによく使用されます。

次のL2セキュリティ設定を使用する一般的なWPA2 SSIDから：



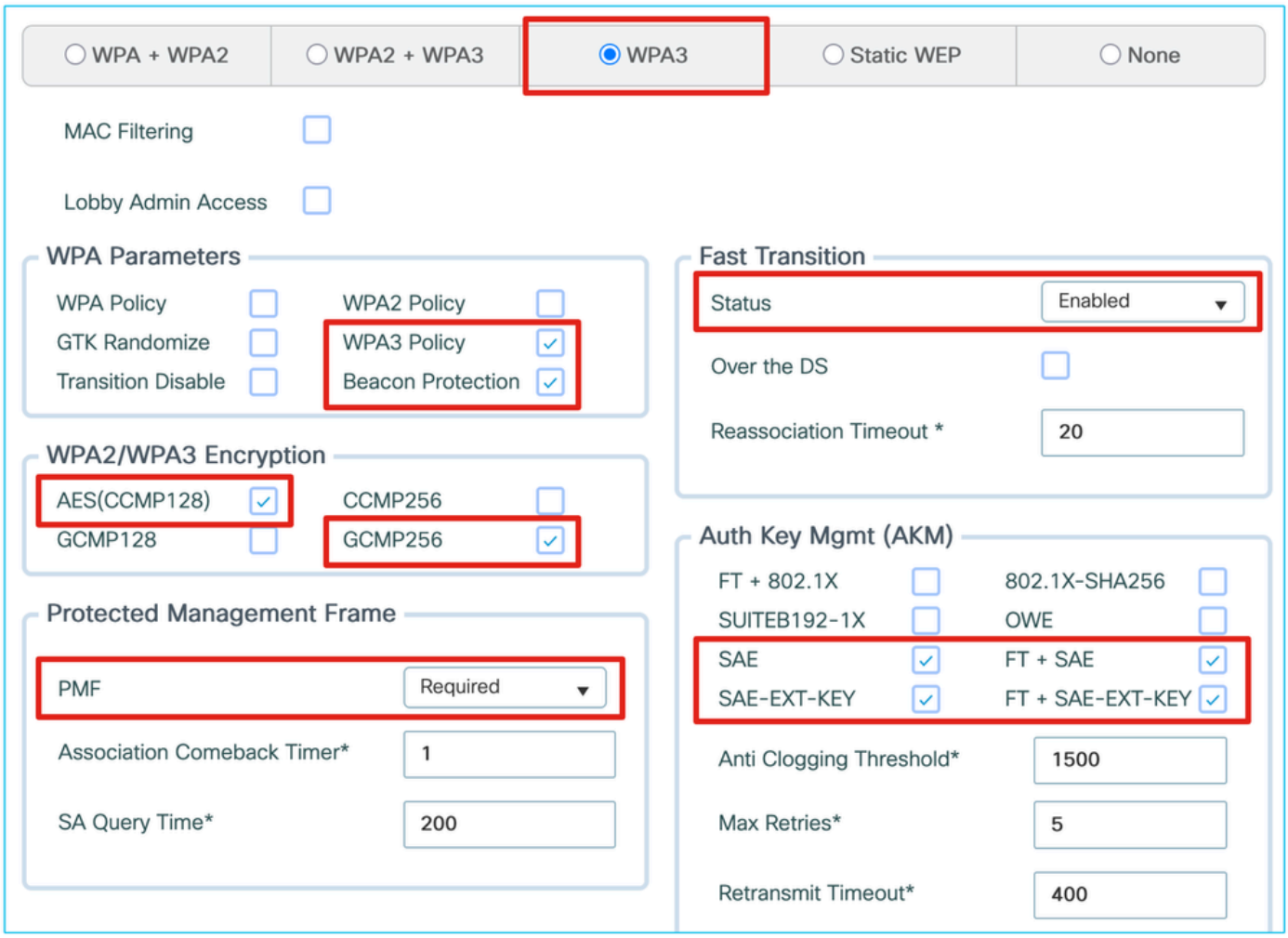
次に示すように、WPA3、6 GHz、およびWi-Fi 7サポートの設定を移行できます。

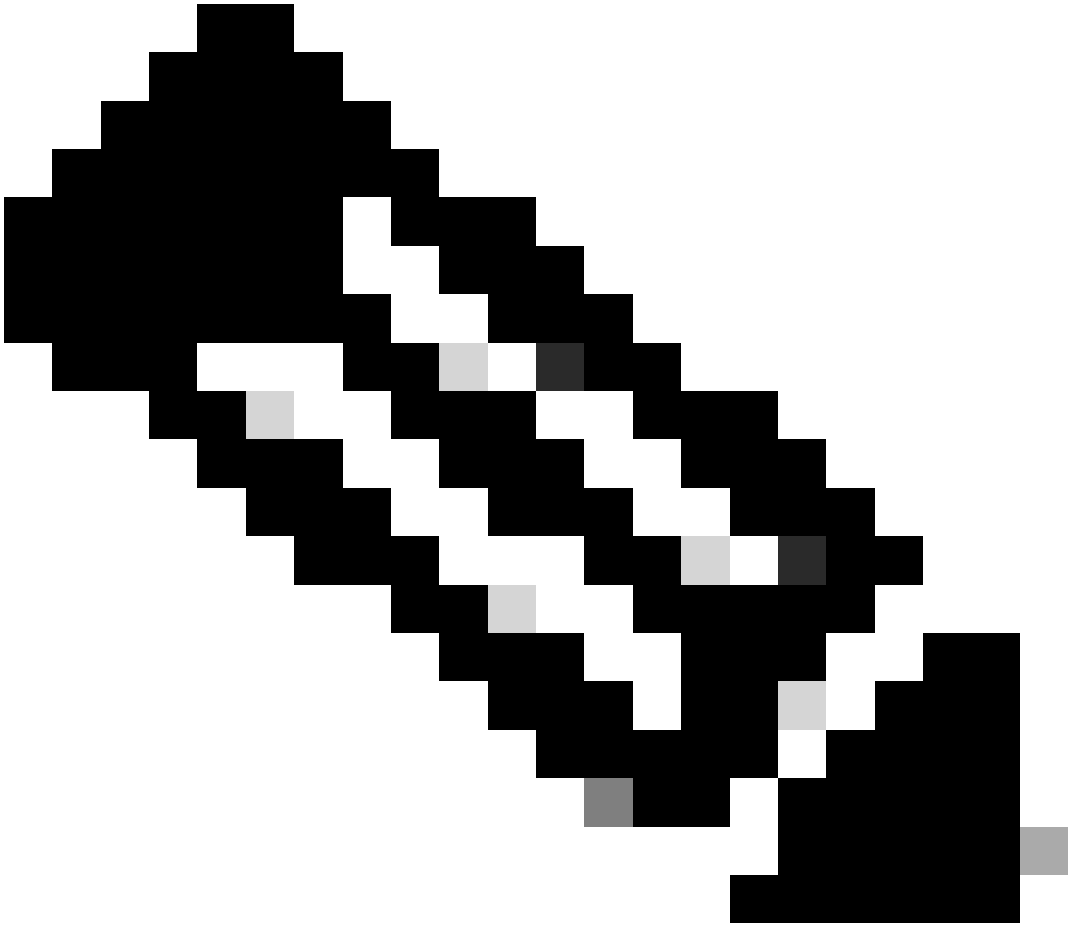


パスフレーズ/WPA3パーソナル/IoTネットワーク

6 GHz、Wi-Fi 6Eサポートまでのパスフレーズ SSIDを有効にするのは簡単で、必要に応じて他のWPA2 PSK AKMと一緒にSAEまたはFT + SAE、あるいはその両方が必要です。ただし、Wi-Fi 7をサポートする場合、認定ではWPA2 PSKオプションを削除し、SAE-EXT-KEYおよび/またはFT + SAE-EXT-KEY AKMをGCMP256暗号とともに追加することが義務付けられています。したがって、パスフレーズベースのWLANを古いクライアントとWi-Fi 7のパフォーマンスの両方に対して最大限の互換性を持つことは不可能です。

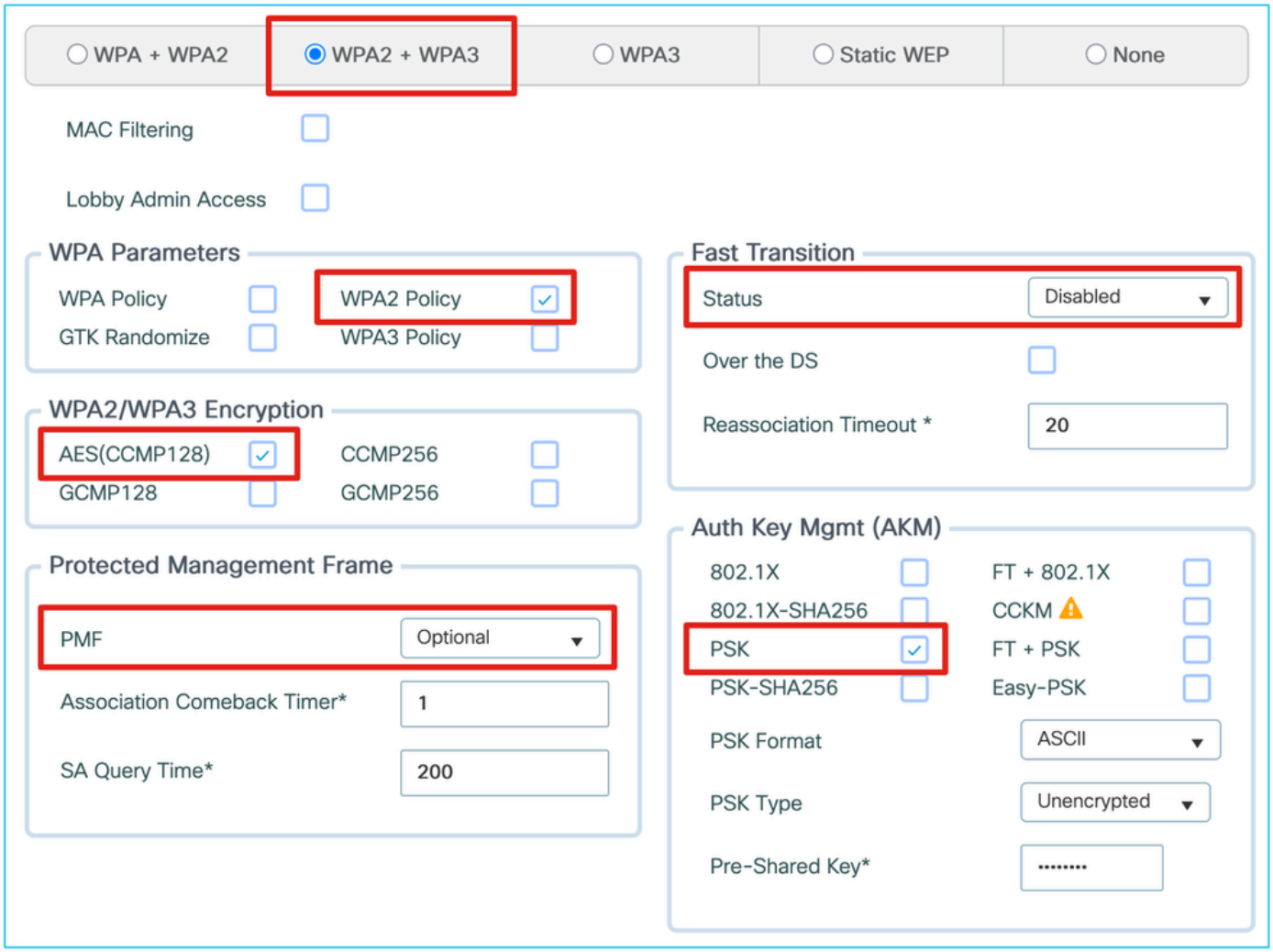
このような場合は、SAE、FT + SAE、SAE-EXT-KEY、およびFT + SAE-EXT-KEYを使用してWPA3専用のSSIDを設定する必要があります。これにより、最新のWi-Fi 6EおよびWi-Fi 7クライアント用に、AES(CCMP128)とGCMP256の両方の暗号が提供されます。


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



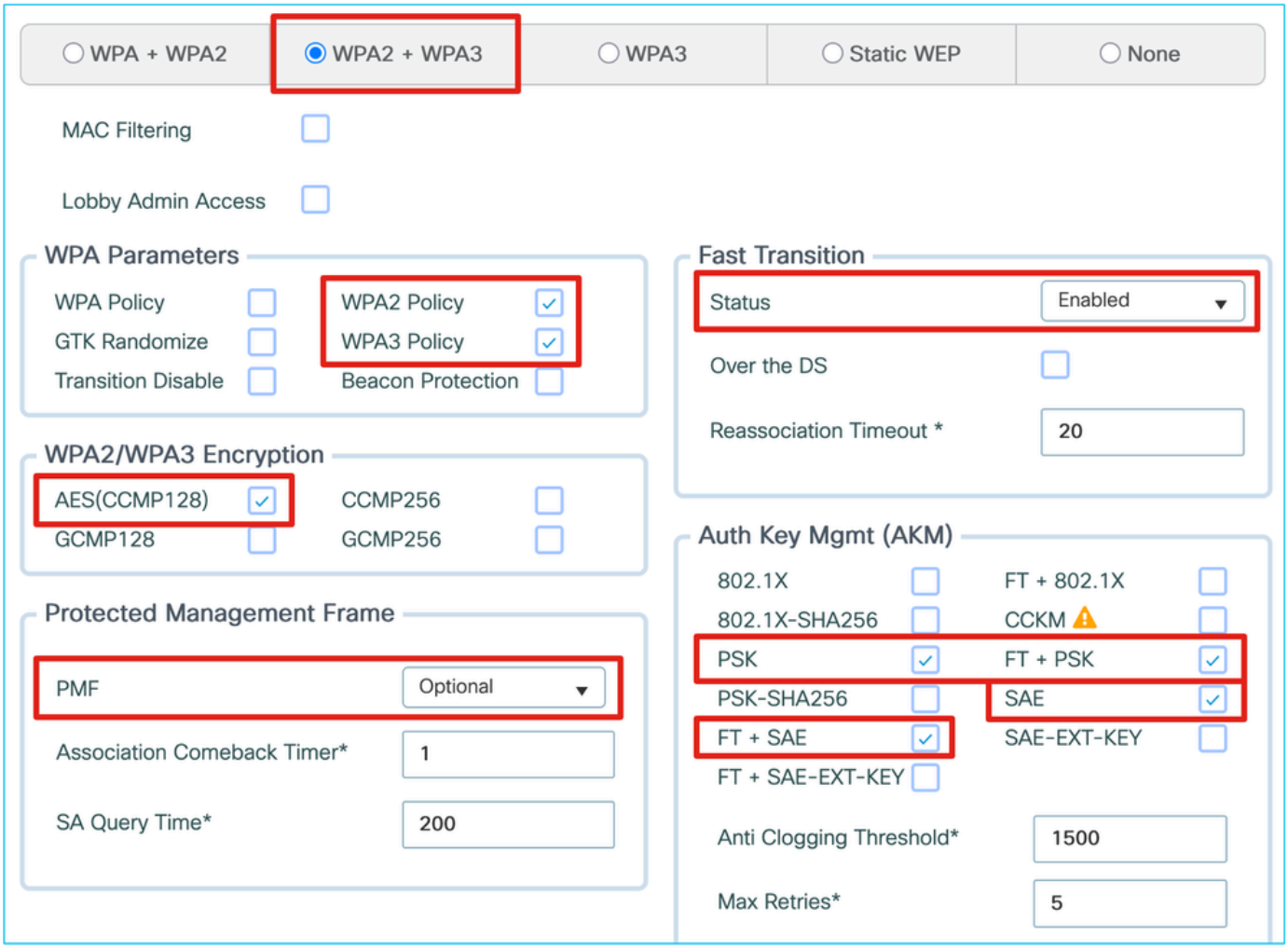
注:(FT +)SAEがWLANで有効な場合、Wi-Fi 7クライアントが(FT +)SAE-EXT-KEYの代わりに、このクライアントとの関連付けを試みると、拒否されます。(FT +)SAE-EXT-KEYが有効になっている限り、Wi-Fi 7クライアントは後者のAKMを使用する必要があり、この問題は発生しません。

一方、別の通常のWPA2 SSIDは、引き続き残りのレガシークライアントに対応できます。



この組み合わせによってSSIDの総量は増加しますが、1つのSSIDで最大の互換性を維持できます。また、互換性に影響を与え、多くのIoTシナリオで役立つ可能性がある他の高度な機能を無効にする可能性がある一方で、他のSSIDを通じて最新のデバイスに最大の機能とパフォーマンスを提供できます。
もう1つのオプションは、Wi-Fi 7 SSIDを提供せず、WPA2 PSKおよびWPA3 SAE用に1つだけ設定するというものです。その背景には、IoTデバイスはWi-Fi 7パフォーマンスを必要としないという考え方があります。

このアプローチは、Wi-Fi 6EおよびWi-Fi 7対応クライアントの6 GHzを引き続きサポートし、Wi-Fi 6Eパフォーマンスに最適に接続できます。



これらすべてのシナリオにおいて、SAEを使用する場合はFTを有効にすることを強く推奨します。SAEフレーム交換は、リソースの点でコストがかかり、WPA2 PSKの4方向ハンドシェイクよりも長くなります。

Appleなどの一部のデバイスメーカーは、FTが有効になっているときにのみSAEを使用することを期待しており、利用できない場合は接続を拒否できます。

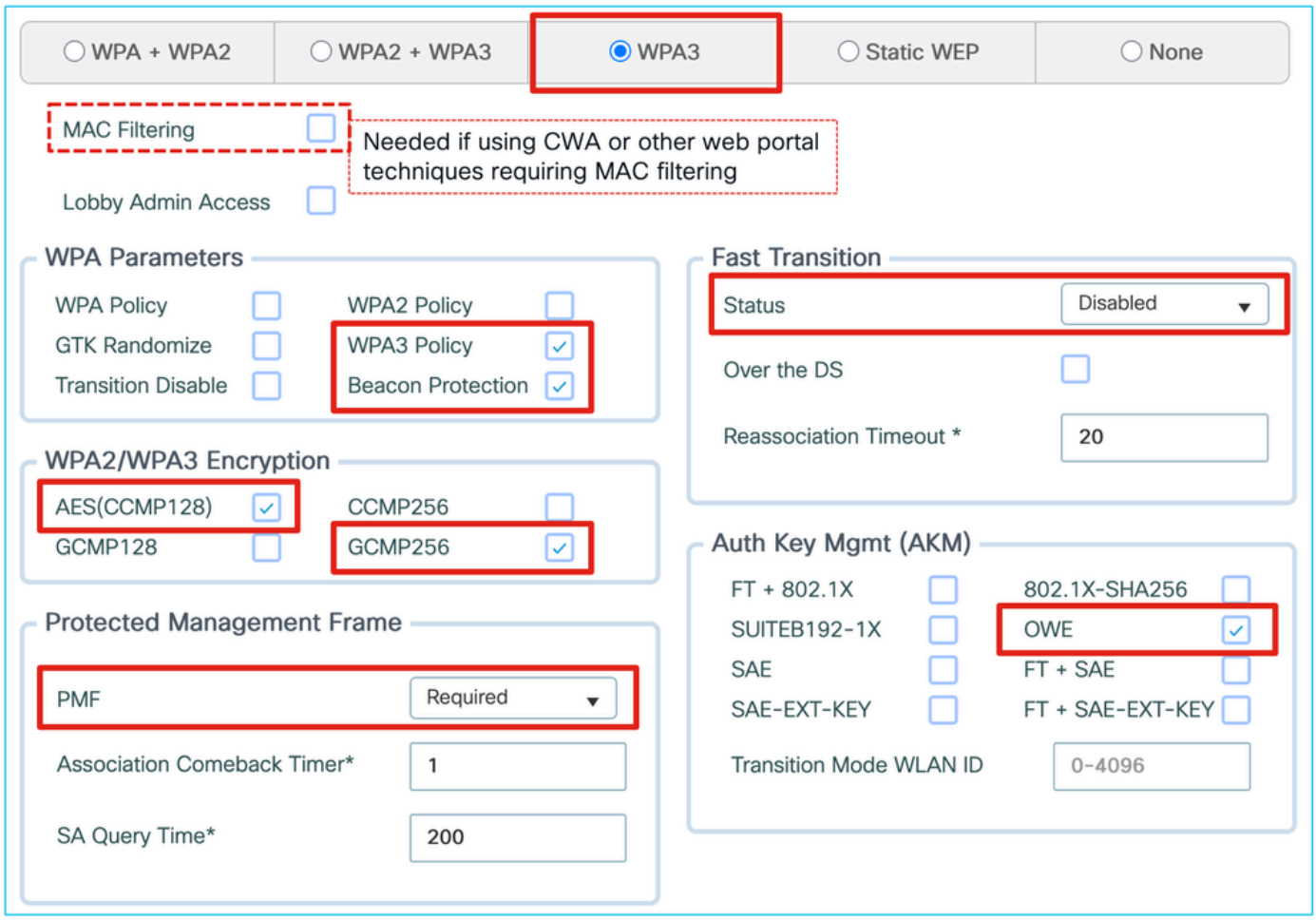
オープン/拡張オープン/負担/ゲストネットワーク

ゲストネットワークにはさまざまな種類があります。通常、接続に802.1Xのクレデンシャルやパスフレーズは必要なく、クレデンシャルやコードが必要なスプラッシュページやポータルを意味する可能性があります。従来は、オープンSSIDと、ローカルまたは外部のゲストポータルソリューションを使用して処理されます。ただし、オープンセキュリティ（暗号化なし）を備えたSSIDは、6 GHzまたはWi-Fi 7サポートでは許可されません。

最初の非常に保守的なアプローチは、ゲストネットワークを5 GHz帯域とWi-Fi 6に割り当てることでした。これにより、企業デバイス用に6 GHz帯域が確保され、複雑さの問題が解決され、互換性が最大になりますが、Wi-Fi 6E/7のパフォーマンスには対応できません。

ゲストに6 GHzのサービスを提供する場合は、Enhanced Open/LEAN(Opportunistic Wireless Encryption)を使用して別のSSIDを作成することを推奨します。 Wi-Fi 6Eクライアントまでの互換性を最大化するためのAES(CCMP128)暗号と、Wi-Fi 7対応クライアント用のGCMP256ビットの

両方を提供できます。



一方で、Enhanced Openが「オープン」なエクスペリエンスを維持しながらプライバシーを提供する優れたセキュリティ方式である場合（エンドユーザが802.1Xのクレデンシャルやパスフレーズを入力する必要がない）、現在でもエンドポイント間のサポートは限定的です。一部のクライアントは引き続きこれをサポートしておらず、サポートしている場合でも、このテクニックは常に円滑に処理されません（デバイスは、実際にはセキュアである一方で、セキュアではない接続を表示したり、LEANでパスフレーズが必要でなくても、パスフレーズが保護されたものとして表示したりできます）。 ゲストネットワークは、すべてのゲスト非制御デバイスで動作することが想定されますが、拡張オープンSSIDだけを提供するのは時期尚早である可能性があります。また、5 GHzでオープンなSSIDと5 GHzおよび6 GHzでLEAD対応のSSIDの両方を別々のSSIDで提供することを推奨します。要件の場合はどちらも同じキャプティブポータルを使用します。移行モードは、Wi-Fi 6E、6 GHz（ソフトウェアで許可されていても）、またはWi-Fi 7ではサポートされていないため、推奨される解決策ではありません。すべてのポータルリダイレクション技術（内部または外部のWeb認証、中央Web認証など）は、引き続きLEANでサポートされています。

追加のWPA3および関連オプション

WPA3オプションはWPA3導入ガイドで最も適切に説明および説明されていますが、このセクションでは、特に6 GHzおよびWi-Fi 7のサポートに関連するWPA3のその他の推奨事項についても説明します。

ビーコン保護

これは、悪意のある攻撃者が正当なアクセスポイントの代わりにビーコンを送信し、一部のフィールドを変更してセキュリティや既に関連付けられているクライアントのその他の設定を変更する可能性があるという脆弱性を解決する機能です。ビーコン保護は、ビーコン自体のシグニチャとして機能するビーコン内の追加の情報要素で、正当なアクセスポイントから送信されたものであり、改ざんされていないことを証明します。WPA3暗号キーに関連付けられたクライアントだけがビーコンの正当性を検証でき、プローブ中のクライアントはそれを検証する手段を持ちません。ビーコンの付加情報要素は、それをサポートしていないクライアント（非Wi-Fi 7クライアント）によって単に無視される必要があり、通常は互換性の問題を表しません（プログラムが不十分なクライアントドライバの場合を除く）。

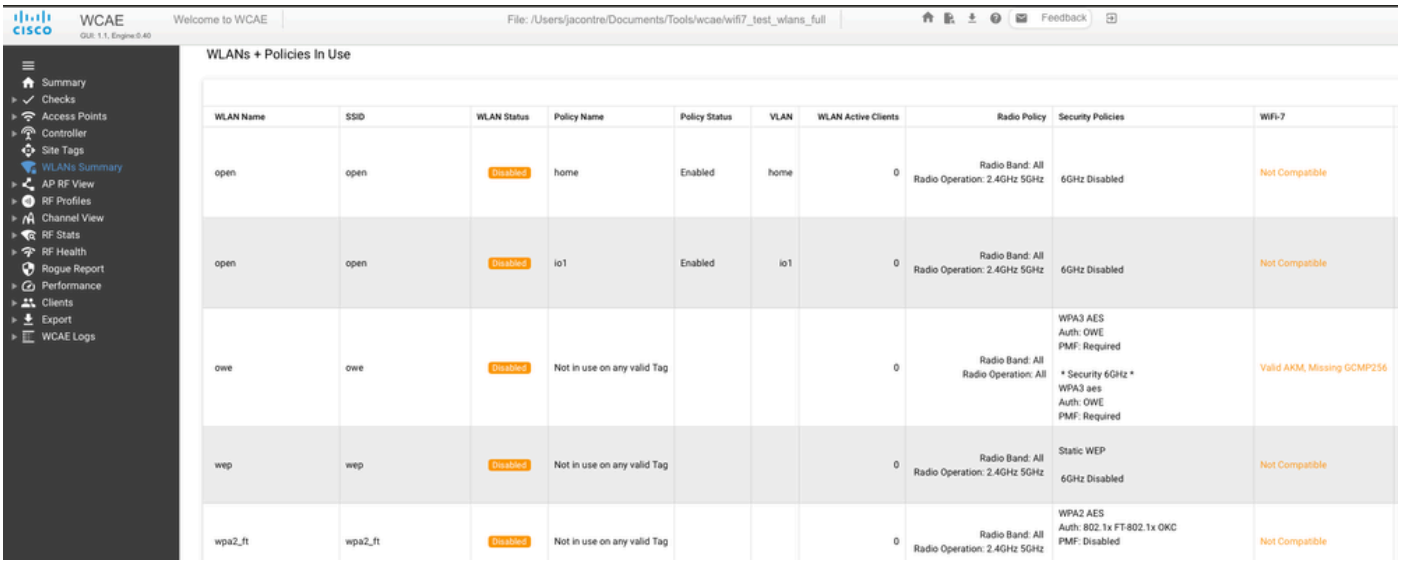
GCMP256

Wi-Fi 7認定まで、ほとんどのクライアントはAES(CCMP128)暗号暗号化を実装していました。CCMP256とGCMP256は、SUITE-B 802.1X AKMに関連する非常に特殊なバリアントです。市場に出回っている一部の第一世代のWi-Fi 7クライアントはWi-Fi 7サポートを主張していますが、まだGCMP256暗号化を実装していない可能性があります。これは、標準を期待どおりに適用しているWi-Fi 7 APがこれらのクライアントを適切なGCMP256サポートなしで接続することを妨げている場合に問題になる可能性があります。

トラブルシューティングと検証

最新バージョンのWireless Configuration Analyzer Express(https://developer.cisco.com/docs/wireless-troubleshooting-tools/wireless-config-analyzer-express-gui/)には、9800の設定を上記のすべてのWi-Fi 7要件について評価するWi-Fi 7レディネスチェックがあります。

設定がWi-Fi 7に対応しているかどうかにまだ疑問がある場合は、WCAEを使用して問題を把握できます。



参考資料

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。