

Cisco Wirelessによる6 GHzおよびWi-Fi 7への移行

内容

[はじめに](#)

[CX設計ガイド](#)

[6 GHzおよびWi-Fi 7を使用する理由](#)

[6 GHzの運用およびWi-Fi 7の基本要件](#)

[6 GHz帯域の要件](#)

[Wi-Fi 7の要件](#)

[IOS XE 17.15.3以降の17.15.xバージョン](#)

[IOS XE 17.18.1/17.18.2](#)

[IOS XE 17.18.3以降](#)

[6 GHzカバレッジの無線設計に関する考慮事項](#)

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

[Wi-Fi 7をグローバルに有効化](#)

[IOS XEでのWi-Fi 7のグローバルな有効化](#)

[Cisco MerakiダッシュボードでのWi-Fi 7のグローバルな有効化](#)

[使用例](#)

[802.1X/WPA3 – エンタープライズネットワーク](#)

[IOS XEでのWPA3-Enterpriseの設定](#)

[Cisco MerakiダッシュボードでのWPA3-Enterpriseの設定](#)

[パスフレーズ/WPA3パーソナル/IoTネットワーク](#)

[IOS XEでのWPA3-SAEの設定](#)

[Cisco MerakiダッシュボードでのWPA3-SAEの設定](#)

[オープン/拡張オープン/引き受け/ゲストネットワーク](#)

[IOS XEのLEAD設定](#)

[Cisco MerakiダッシュボードのLEAD設定](#)

[追加のWPA3および関連オプション](#)

[ビーコン保護](#)

[GCMP256](#)

[トラブルシューティングと検証](#)

[トラブルシューティングチェックリスト](#)

[参照資料](#)

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スペクトルを完全に活用するための設計および設定のガイドラインについて説明します。



CX設計ガイドは、Cisco CXのスペシャリストが他の部門のエンジニアと共同で作成し、シスコ内のエキスパートが相互にレビューします。ガイドは、シスコのベストプラクティスに加え、長年にわたってお客様が数多くの製品を導入してきた経験と知識に基づいています。このドキュメントの推奨事項に従って設計および設定されたネットワークは、一般的な落とし穴を回避し、ネットワーク運用を改善するのに役立ちます。

6 GHzおよびWi-Fi 7を使用する理由

2020年に6 GHz帯域がWLAN運用に使用可能になり、Wi-Fi 6E認定に必要になりました。Wi-Fi 6は2.4 GHzおよび5 GHz帯域で動作しますが、Wi-Fi 6Eは同じIEEE 802.11ax規格を使用しますが、特定の要件を満たすことを条件にその機能を6 GHz帯域に拡張します。

新しいWi-Fi 7認定は、IEEE 802.11be規格に基づいており、2.4 GHz、5 GHz、6 GHz帯域での運用をサポートします。また、Wi-Fi 7では、以前の認定と比べて新機能と拡張機能が導入されています。

6 GHz帯域および/またはWi-Fi 7をサポートするには特定の要件が伴い、特にWi-Fi 6を使用する2.4 GHzおよび5 GHz帯域の確立されたプラクティスと比較すると、新しい設定とRF設計が必要になる場合があります。

たとえば、旧式のWEPセキュリティを使用することで802.11規格の802.11a/b/gを超える導入を防ぐのと同様に、新しい規格では、よりセキュアなネットワークの展開を促進するために、さらに厳しいセキュリティ要件が課されます。

逆に、6 GHz帯域の導入により、よりクリーンな周波数へのアクセス、パフォーマンスの向上、新しいユースケースのサポートが提供されます。また、音声やビデオ会議などの既存のアプリケーションをよりシームレスに実装できます。

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のみが許可されます。つまり、次のいずれかのセキュリティオプションが有効になります。

- 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では交換を長くせずに済むため、実際の使用をお勧めします。
- 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の両方を、移行モードを有効にして設定することが技術的に可能です。これらはすべて、標準仕様に従わずに設定できます。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のデータレートとプロトコルの向上を使用できるものもあれば、マルチリンク動作(MLO)のサポートに固有のものもあり、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は次のいずれかのセキュリティタイプを必要とします。

- 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) 新しいWPA3仕様(3.4)では、クライアントがAES128の使用を引き続き許可されている場合でも、要件が「APはGCMP256アルゴリズムを提供する必要がある」に変わります。これにより、AES128を使用してWi-Fi 7 Enterpriseを実行しようとするクライアントと、すでにGCMP256を実行する必要があると予想されるクライアントの動作に違いが生じます。

- WPA3-Personal(GCMP256、SAE-EXT-KEY、FT + SAE-EXT-KEY (AKM 24または25))
Wi-Fi 6Eでは、WPA3 SAEまたはFT + SAE、あるいはその両方を通常のAES(CCMP128)で必須としますが、拡張キーは追加で使用されません。これは、Wi-Fi 7用に新しい暗号が導入されたことを意味します。
- 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をサポートしません。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、これは新しい、より強力な要件です。6 GHzのサポートに関しては、移行モードは許可されません。

選択したセキュリティタイプに関係なく、WLANでWi-Fi 7をサポートするには、Protected Management Frames(PMF)とビーコン保護が必要です。

Wi-Fi 7は、このドキュメントの執筆時点では最新の認定であり、可能な限り早期にリリースされているため、多くのベンダーは当初からこれらのセキュリティ要件をすべて適用していませんでした。

最近では、Wi-Fi 7認定に準拠するように構成オプションを段階的に適用しています。バージョン固有の動作を次に示します。

IOS XE 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でき、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、GCMP256などの初期のWi-Fi 7クライアントが、よりセキュア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の要件に一致しないWLANにWi-Fi 7 MLO対応として関連付けようとする、問題を引き起こす可能性があります。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。

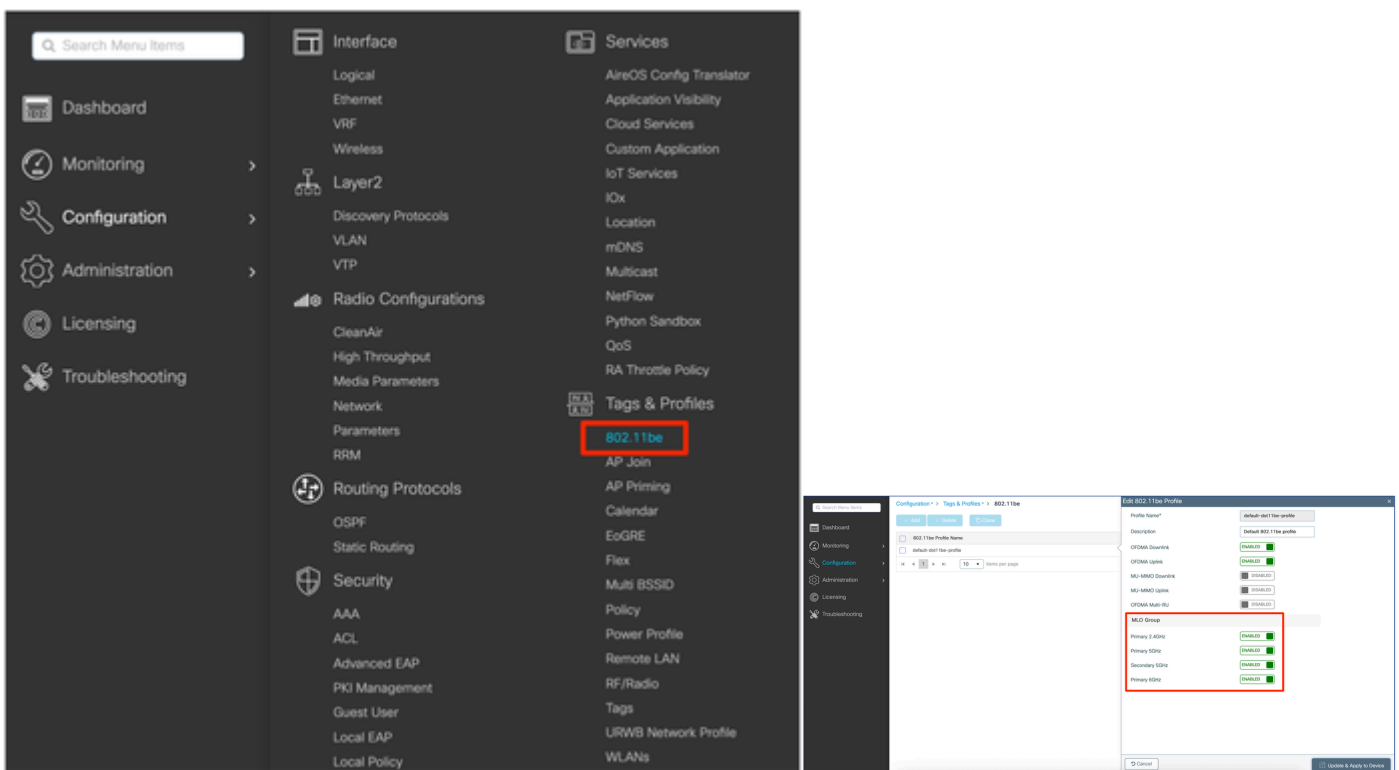
IOS XE 17.18.1/17.18.2

ビーコン保護は、WLANがWi-Fi 7に準拠している場合、チェックボックスをオンにしたかどうかにかかわらず、自動的に有効になります。

17.18.1以降のCisco IOS XEでは、WLAN設定で適切なセキュリティ要件が有効になっている場合、WLANをWi-Fi 7およびMLO対応としてのみアドバタイズします。たとえば、SAEのみをアドバタイズし、SAE-EXTをアドバタイズしないWLANは、MLO非対応としてブロードキャストされます。

17.18ブランチでは、WLANプロファイルに接続する802.11beプロファイルの機能を導入しています。このプロファイルにより、Wi-Fi 7のアクティブ化をSSID単位、さらには無線単位で制御できます。

Configuration > Tags & Profiles > 802.11beの下に、新しい専用メニューが追加されました。デフォルトでは、「default-dot11be-profile」という名前の下に、事前設定された802.11beプロファイルがすでに存在します。



Wi-Fi 7を有効または無効にするための4つの主な設定は、「MLOグループ」セクションにあります。これら4つをすべて無効にすることで、WLANプロファイルのすべての帯域に対してWi-Fi 7を無効にします。これは、802.11beプロファイルを接続するものです。それらのいくつか、またはすべてを有効にすることで、802.11beプロファイルを接続するWLANプロファイルの対応する帯域/無線でWi-Fi 7を有効にします。

「default-dot11be-profile」は、すべての無線でMLOとWi-Fi 7を有効にし、デフォルトではすべてのWLANプロファイルに適用されます。

たとえば、すべての「MLO Group」設定を無効にして新しい802.11beプロファイルを作成し、それを特定のWLANプロファイルに接続することで、一部のSSIDでWi-Fi 7を選択的に無効にすることができます。

各WLANプロファイルの「Advanced」設定タブに、対応する802.11beプロファイルが添付されています。

The screenshot shows the 'Edit WLAN' configuration interface. The '11be' profile is selected and highlighted with a red box. Below it, the '802.11be Profile' dropdown menu is set to 'default-dot11...'. The interface includes various configuration options with checkboxes and a 'Geolocation' section with a 'DISABLED' button. At the bottom, there are 'Cancel' and 'Update & Apply to Device' buttons.

例からわかるように、「default-dot11be-profile」はデフォルトで任意のWLANプロファイルに割り当てられています。



注：後述するように、コントローラでWi-Fi 7がグローバルに有効になっていない場合、Wi-Fi 7はすべてのWLANプロファイルで無効になり、802.11beプロファイルは適用されません。

17.18.2では、WLANがWi-Fi7に準拠しているかどうかを可視化し、欠落している情報を表示する小さなウィザードがWLAN編集ページに導入されています（図1を参照）。

Wi-Fi 7 Compatibility

3/3 requirements met

2/3 bands enabled

✓ WPA3 should be Enabled

Current Status: Enabled

✓ Supported Ciphers and AKMs are:

GCMP256 + SAE-EXT-KEY / FT-SAE-EXT-KEY / OWE

AES + 802.1X-SHA256 / FT-802.1X

GCMP256 + Suite-B-192

Current configured Cipher(s) + AKM(s):

CCMP128 / GCMP256 + SAE / FT-SAE / SAE-EXT-KEY / FT-SAE-EXT-KEY

✓ PMF state should be Optional or Required

Current Status: Required

Per Band Enablement Status

6 GHz

✓ Enabled

Dependencies:

- Global 11be
- MLO Primary

5 GHz

✓ Enabled

Dependencies:

- Global 11be
- MLO Primary
- MLO Secondary

2.4 GHz

✘ Disabled

Dependencies:

- Global 11be
- MLO Primary

✓ Enabled – band is enabled and all dependencies have been met

⚠ Downgraded – band is enabled but dependencies are not met

✘ Disabled – band is disabled as per the Radio Policy configuration

Click [here](#) to Enable/Disable global 802.11be configuration.

Click [here](#) to Enable/Disable MLO configuration on the associated 802.11be profile

17.18.2セキュリティウィザード

IOS XE 17.18.3以降

IOS 17.18.3では、802.1XエンタープライズSSIDに対してGCMP256暗号を設定できます。これは

以前のバージョンでは不可能でした。これは、AES128暗号に加えてGCMP256を提供するWi-Fi7エンタープライズSSIDを持つためのいくつかのクライアント要件を満たし、WPA 3.4仕様に準拠しています。

GCMP256が17.18.3で有効になっていない場合にWi-Fi 6E SSIDにデグレードするのを避けるため、アップグレード前にSSIDがWi-Fi 7に準拠していた場合、GCMP256がアップグレード時に自動的に設定に追加されます

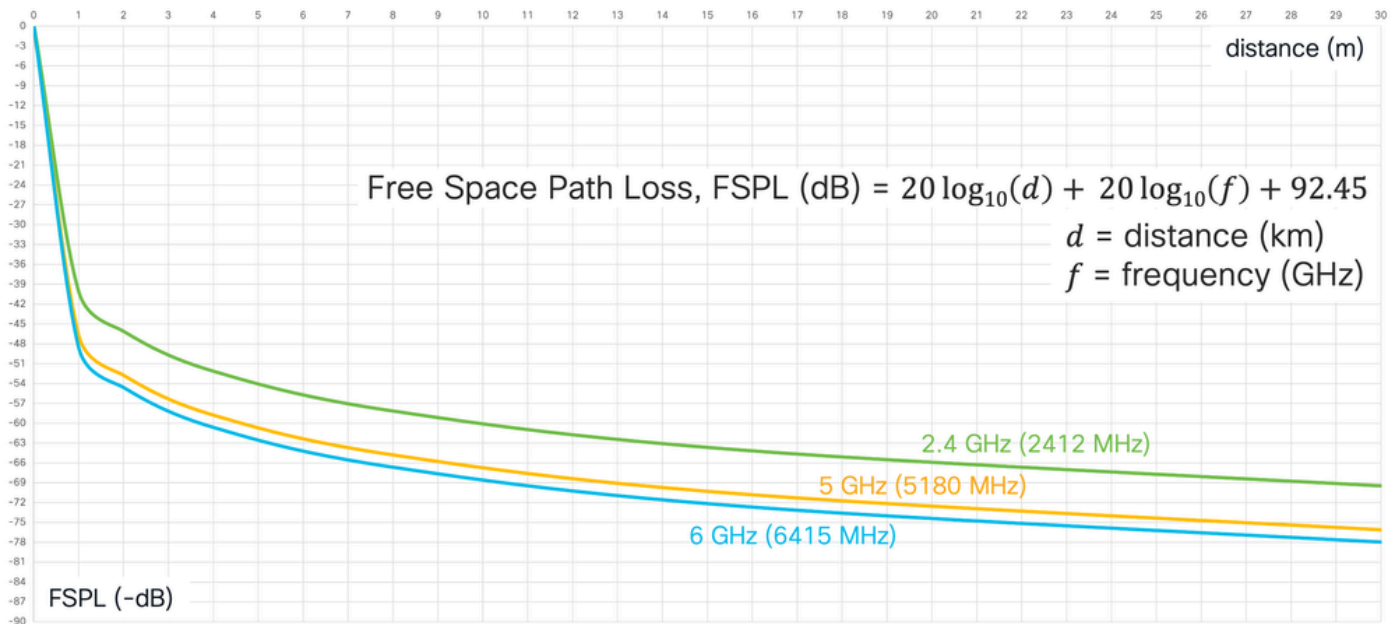
6 GHzカバレッジの無線設計に関する考慮事項

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。

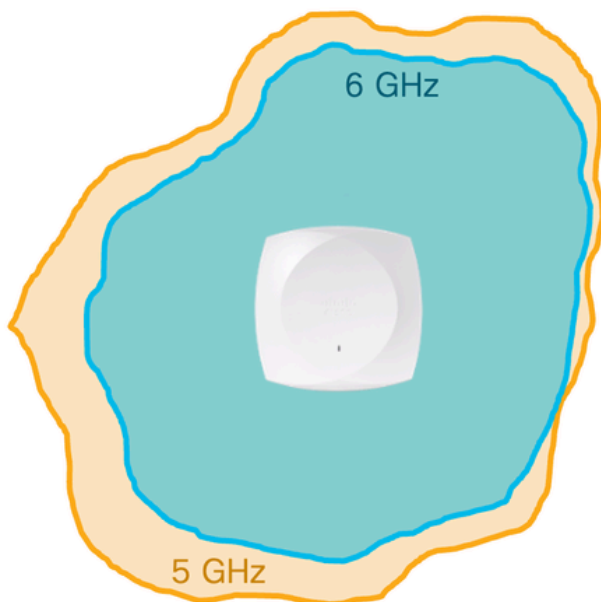
2.4または5 GHzで使用された新しいWi-Fiの導入に関しては、6 GHzの新しい無線プロジェクトに、対応する専用6 GHzサイト調査も含める必要があります。

Wi-Fi 6E/7以前のAPがすでに特定の5 GHzカバレッジ用に配置されていて、場合によっては、それらをWi-Fi 6E/7対応APに置き換えても6 GHzで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、すでに最大限の3 ~ 4送信電力レベルを満たしている必要があります。APには通常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分割します。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。

5 GHzがAPの5 GHz無線ですでに最大未満の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。この前提条件は、5 GHzと6 GHzのカバレッジが展開されている国の規制では、6 GHz無線とEIRPを5 GHzよりも高い電力に設定できるという条件の下で機能します (チャンネル集約と特定のAPモデルも考慮する可能性があります。国別の情報については、各APモデルの電力設定の表を参照してください)。

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を展開することは、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」方式でインストールされている (つまり、同じゾーンに混在している) 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、ダイナミックチャンネル割り当て、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、同じエリア内に異なる機能を提供するAPを配置することは最適ではありません。この配置では、クライアントが移動中にこれらの機能を実際に使用することはできず、スティッキ性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以上のチャン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

IOS XEでのWi-Fi 7のグローバルな有効化

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場合、デフォルトでは、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。

The screenshot shows the Cisco Meraki dashboard configuration page for High Throughput. The breadcrumb trail is Configuration > Radio Configurations > High Throughput. There are three tabs for 6 GHz Band, 5 GHz Band, and 2.4 GHz Band. A warning message states: "6 GHz Network is operational. Configuring High Throughput will result in loss of connectivity of clients." Below this, a red warning box says: "Configuring High Throughput Parameters will result in loss of connectivity of all clients across 802.11be enabled radios of the APs". Under the "11ax" section, there is a "11be" section with a warning: "11be check enables Wi-Fi 7 capability in Wi-Fi 7 capable APs. Please ensure the WLANs are compatible with Wi-Fi 7 specific security. Click here to view the security constraints." The "Enable 11be" checkbox is checked and highlighted with a red box. A "Select All" checkbox is also checked. Below this is a table of SS/MCS values for each band.

SS/MCS	SS/MCS	SS/MCS	SS/MCS
<input checked="" type="checkbox"/> 1/9	<input checked="" type="checkbox"/> 1/11	<input checked="" type="checkbox"/> 1/13	<input checked="" type="checkbox"/> 1/14
<input checked="" type="checkbox"/> 1/15	<input checked="" type="checkbox"/> 2/9	<input checked="" type="checkbox"/> 2/11	<input checked="" type="checkbox"/> 2/13
<input checked="" type="checkbox"/> 3/9	<input checked="" type="checkbox"/> 3/11	<input checked="" type="checkbox"/> 3/13	<input checked="" type="checkbox"/> 4/9
<input checked="" type="checkbox"/> 4/11	<input checked="" type="checkbox"/> 4/13		

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。すべての帯域を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。

Cisco MerakiダッシュボードでのWi-Fi 7のグローバルな有効化

Wi-Fi 7対応AP (CW9178I、CW9176I/D1など) をCisco Merakiダッシュボードネットワークに初めて追加する際、802.11be動作のサポートはデフォルトのRFプロファイルで行われます。これをアクティブにするには、Wireless > Radio Settingsの順に選択し、RF Profileタブをクリックして、APに割り当てられているプロファイル (デフォルト : 屋内APの基本屋内プロファイル) を選択します。

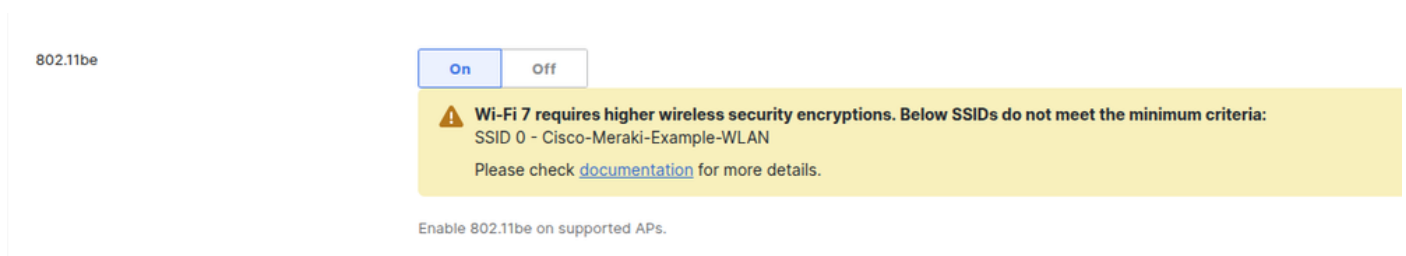
Generalセクションで、次のスクリーンショットに示すように、802.11be(on)を有効にします。



1つ以上のWLANがWi-Fi 7仕様で必要とされるセキュリティ設定よりも弱いセキュリティ設定で設定されている場合、以下に示すように、ダッシュボードにユーザに警告するバナーが表示されます。

ダッシュボードでは設定を保存できませんが、Wi-Fi 7要件への準拠が保証されるまで、フラグが付いたSSIDではWi-Fi 7は有効になりません。

このドキュメントの作成時点で、ネットワークで有効になっているすべてのWLANは、ファームウェアバージョンMR 31.1.x以降で有効にされるには、Wi-Fi 7仕様の要件を満たす必要があります (この動作は、ファームウェアMR 32.1.xの将来のバージョンでは変更されます) 。



SSIDの設定がWi-Fi 7の最小基準を満たすと、バナーが消えます。

同じRFプロファイルで、AP上で6 GHzの動作が有効になっていることを確認します。

これは、すべてのSSIDに対して一括で、または個々のSSIDごとに実行できます。

バンドステアリングは、2.4 GHzと5 GHzの間でのみ使用できます。

すべてのSSIDに対して6 GHzを有効にする例。

General

Band selection

All SSIDs

Per SSID

Enable operation on 2.4 GHz band

SSID will be broadcast on 2.4 GHz. This band does not support 802.11a devices.

Enable operation on 5 GHz band

SSID will be broadcast on 5 GHz. This band does not support 802.11b/g devices.

Enable operation on 6 GHz band

SSID will be broadcast on 6 GHz.

Enable band steering

Attempt to steer clients from 2.4 GHz to 5 GHz.

シングルSSIDに対する6 GHzの有効化の例。

General

Band selection

All SSIDs

Per SSID

Name	2.4 GHz	5 GHz	6 GHz	Band steering ⓘ
meraki-wpa3-ent-transition	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Show disabled SSIDs

使用例

802.1X/WPA3 – エンタープライズネットワーク

IOS XEでのWPA3-Enterpriseの設定

6 GHzへの移行が最も簡単なのは、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用に802.1X SSIDを有効にするには、PMFのサポートを有効にする必要があるだけで、オプションの場合と同様に、802.1X-SHA256およびFT + 802.1X AKM (両方ともWPA3に準拠) も有効にする必要があります。

同じWLANで、5GHz帯域でのみアドバタイズされる標準の802.1X(SHA1)を使用したWPA2を引き続き提供できます。

Wi-Fi 7をサポートするには、ビーコン保護を有効に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。

AES128とGCMP256を有効にすることで、多くのデバイスに対して「互換性のために」ドアを開いたままにすることができますが、PMFをオプションとして設定し、通常の802.1XなどのWPA2 AKMを許容することで、クライアントは多くの可能性に直面し、Wi-Fi7をサポートしていると宣言した場合、Wi-Fi7に準拠していないセキュリティ設定のこの組み合わせを選択したクライアントは拒否拒否します。

ただし、IOS XE 17.18.2以前のバージョンでは、エンタープライズSSIDのGCMP256をサポートしていません。主な推奨事項は、主にWindows11ラップトップを実行するエンタープライズ環境でこのようなユースケースを維持することです。

17.18.3以降を実行すると、GCMP256を有効にし、より広範なモバイルデバイスのカテゴリを適切にサポートできます (一部のクライアントは、SSIDがWi-Fi7であると主張する場合に接続を拒否しますが、AES128のみをサポートします)。

MerakiクラウドダッシュボードはGCMP256をサポートしており、SSIDでWi-Fi7を有効にするために必要です。Wi-Fi7クライアントはAES128のみをサポートしても問題ありませんが、認定Wi-Fi 7 APはAES128とGCMP256の両方を提供する必要があります。

次のL2セキュリティ設定を使用する一般的なWPA2 SSIDから：

WPA + WPA2
 WPA2 + WPA3
 WPA3
 Static WEP
 None

MAC Filtering

Lobby Admin Access

WPA Parameters

WPA Policy
 WPA2 Policy
 WPA3 Policy

GTK Randomize

WPA2/WPA3 Encryption

AES(CCMP128)
 CCMP256
 GCMP128
 GCMP256

Protected Management Frame

PMF

Association Comeback Timer*

SA Query Time*

Fast Transition

Status

Over the DS

Reassociation Timeout *

Auth Key Mgmt (AKM)

802.1X
 FT + 802.1X
 802.1X-SHA256
 CCKM ⚠
 PSK
 FT + PSK
 PSK-SHA256
 Easy-PSK

MPSK Configuration

Enable MPSK

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

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
 Association Comeback Timer*
 SA Query Time*

Fast Transition
 Status
 Over the DS
 Reassociation Timeout *

Auth Key Mgmt (AKM)
 802.1X FT + 802.1X
 802.1X-SHA256 CCKM ⚠️
 PSK FT + PSK
 PSK-SHA256 SAE
 FT + SAE SAE-EXT-KEY
 FT + SAE-EXT-KEY

この最後のスクリーンキャプチャには、適切なWi-Fi7サポートのためのGCMP256が含まれていません。また、クライアントがこの多数の異なる暗号を提供し、AES128+GCMP256を使用して完全なWPA3 WLANにできるだけ早く移行することを検討することは、潜在的に問題となります。

Cisco MerakiダッシュボードでのWPA3-Enterpriseの設定

このドキュメントの執筆時点では、WPA3-Enterprise動作は外部RADIUSサーバ（別名「my RADIUS server」）でのみ使用できます。

WPA3-EnterpriseはMerakiクラウド認証では使用できません。

Security WPA3 Enterprise with 1 RADIUS server

Open (no encryption)
Any user can associate

Opportunistic Wireless Encryption (OWE)
Any user can associate with data encryption

Password
Users must enter a passphrase to associate ⓘ

MAC-based access control (no encryption)
RADIUS server is queried at association time

Enterprise with
my RADIUS server ▾
User credentials are validated with 802.1X at association time

Identity-based access control with RADIUS

MR 31.x以降のWPAタイプは次のとおりです。

- 「WPA3 only」では、WPA2と同じ暗号を使用しますが、802.11w(PMF)が必要です。
- 「WPA3 192ビット」では、cipher TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, TLS_ECDSAを使用するEAP-TLS方式のみが許可されます。
dhe_RSA_WITH_AES_256_GCM_SHA384または
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384です。このモードを有効にするには、RADIUSサーバで同じチップを設定する必要があります。
- 「WPA3移行モード」(別名「混合モード」)では、WPA3に使用される同じWLAN上にWPA2クライアントを共存させることができます。

WPA encryption ⓘ

802.11r ⓘ

802.11w ⓘ

WPA3 only ▾

WPA2 only

WPA1 and WPA2

WPA3 only

WPA3 192-bit Security

WPA3 Transition Mode

clients)

clients)

「WPA3のみ」または「WPA3 192ビットセキュリティ」を使用する場合、PMFはすべてのクラ

クライアントで必須です。

ほとんどのアプリケーションでは、外部RADIUSサーバを使用する際のローミングや再認証遅延の影響を緩和するために、必須ではありませんが、FT(802.11r)を有効にする必要があります。

6 GHzの運用では、PMF(802.11w)を有効にする必要があります。

WPA encryption ⓘ WPA3 only ▾

802.11r ⓘ Enabled
 Adaptive
 Disabled

802.11w ⓘ Enabled (allow unsupported clients)
 Required (reject unsupported clients)
 Disabled (never use)

WPA3 Transition Modeを選択すると、WPA3を使用できるすべてのクライアントは、デフォルトでPMFを使用します。6 GHzで動作するすべてのクライアントはWPA3を使用します。

このモードでは、WPA2を使用するレガシークライアントでPMFを使用する必要があるか(802.11wが必須)、またはその機能がオプションか(802.11wが有効)を選択できます。

WPA encryption ⓘ WPA3 Transition Mode ▾

802.11r ⓘ Enabled
 Adaptive
 Disabled

802.11w ⓘ Enabled (allow unsupported clients)
 Required (reject unsupported clients)
 Disabled (never use)

WPA3の選択にかかわらず、Cisco Meraki APをWi-Fi 7モードで動作させるには、GCMP 256暗号スイートを有効にする必要があります。

さらに、APがWi-Fi 7モードで動作している場合、2.4、5、および6 GHzではビーコン保護がデフォルトで有効になっています。

Advanced WPA3 settings (Cipher and AKM suite settings)

WPA3 Cipher Suite GCMP 256



Certain Cipher suite and AKMs are required for capable APs to operate in 802.11be (Wi-Fi 7) mode. Please refer to [documentation](#) for more details.

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、認定はGCMP256暗号とともにSAE-EXT-KEYおよび/またはFT + SAE-EXT-KEY AKMを追加することを義務付けています。

Cisco IOS XE 17.18.1以降では、前述の4つのSAE AKMの上にWPA2-PSKを設定できます。ただし、これは同じSSID上に多数のAKMが存在する可能性があるという懸念を生み出します（これは標準でサポートされているため、クライアントドライバの不良という観点のみです）。WPA2クライアントがWLANで有効になっているすべてのAKMに対応できるかどうかを実際に確認することをお勧めします。この状況では、WPA2として接続することを決定したクライアントはMLOまたはWi-Fi7を実行できませんが、SAE-EXTで接続するクライアントはMLOおよびWi-Fi7を実行できます。WLAN自体は、引き続きWi-Fi 7およびMLO機能をアドバタイズします。

このような場合、SAE、FT + SAE、SAE-EXT-KEY、およびFT + SAE-EXT-KEYを使用して専用のWPA3専用SSIDを設定し、最新のWi-Fi 6EおよびWi-Fi 7クライアント用にAES(CCMP128)とGCMP256の両方の暗号を提供できます。

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お勧めします。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場合にのみSAEを使用することを想定しており、使用できない場合は接続を拒否できます。

IOS XEでのWPA3-SAEの設定

<input type="radio"/> WPA + WPA2	<input type="radio"/> WPA2 + WPA3	<input checked="" type="radio"/> WPA3	<input type="radio"/> Static WEP	<input type="radio"/> None
MAC Filtering	<input type="checkbox"/>			
Lobby Admin Access	<input type="checkbox"/>			
WPA Parameters				
WPA Policy	<input type="checkbox"/>	WPA2 Policy	<input type="checkbox"/>	
GTK Randomize	<input type="checkbox"/>	WPA3 Policy	<input checked="" type="checkbox"/>	
Transition Disable	<input type="checkbox"/>	Beacon Protection	<input checked="" type="checkbox"/>	
WPA2/WPA3 Encryption				
AES(CCMP128)	<input checked="" type="checkbox"/>	CCMP256	<input type="checkbox"/>	
GCMP128	<input type="checkbox"/>	GCMP256	<input checked="" type="checkbox"/>	
Protected Management Frame				
PMF	<input type="checkbox"/>	Required	<input type="checkbox"/>	
Association Comeback Timer*	<input type="text" value="1"/>			
SA Query Time*	<input type="text" value="200"/>			
Fast Transition				
Status	<input type="text" value="Enabled"/>			
Over the DS	<input type="checkbox"/>			
Reassociation Timeout *	<input type="text" value="20"/>			
Auth Key Mgmt (AKM)				
FT + 802.1X	<input type="checkbox"/>	802.1X-SHA256	<input type="checkbox"/>	
SUITEB192-1X	<input type="checkbox"/>	OWE	<input type="checkbox"/>	
SAE	<input checked="" type="checkbox"/>	FT + SAE	<input checked="" type="checkbox"/>	
SAE-EXT-KEY	<input checked="" type="checkbox"/>	FT + SAE-EXT-KEY	<input checked="" type="checkbox"/>	
Anti Clogging Threshold*	<input type="text" value="1500"/>			
Max Retries*	<input type="text" value="5"/>			
Retransmit Timeout*	<input type="text" value="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。

WPA-3のみのWLAN上でPSKのみを使用するレガシーWLANを使用すると、合計SSIDの量が増加しますが、1つのSSID上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る可能性がある他の高度な機能を無効にし、多くのIoTシナリオに役立つ可能性がある一方で、他のSSIDを使用して最新の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。図の中に古いIoTデバイスや機密の高いIoTデバイスがある場合は、このシナリオを推奨できます。IoTデバイスがない場合は、1つのSSIDのみをアドバタイズするため、単一の移行モードのWLANを選択する方が効率的です。

Cisco MerakiダッシュボードでのWPA3-SAEの設定

Security WPA3 SAE configured

Open (no encryption)
Any user can associate

Opportunistic Wireless Encryption (OWE)
Any user can associate with data encryption

Password
Users must enter this key to associate: ⓘ
.....

MAC-based access control (no encryption)

ファームウェアMR 30.xまでは、サポートされているWPAタイプは「WPA3のみ」であり、ダッシュボードでは別の方式を選択できません。

この設定ではPMFが必須ですが、SAEの使用時にはFT(802.11r)を有効にすることをお勧めします。

WPA encryption ⓘ WPA3 only ▾

802.11r ⓘ Enabled
 Adaptive
 Disabled

802.11w ⓘ Enabled (allow unsupported clients)
 Required (reject unsupported clients)
 Disabled (never use)

Wi-Fi 7の動作を許可するには、SSIDの設定時にGCMP 256チップスイートとSAE-EXT AKMスイートを有効にする必要があります。

これらはデフォルトで無効になっており、「Advanced WPA3 settings」で有効にできます。

Advanced WPA3 settings (Cipher and AKM suite settings)

WPA3 Cipher Suite

GCMP 256

WPA3 AKM Suite

SAE

SAE-EXT



Certain Cipher suite and AKMs are required for capable APs to operate in 802.11be (Wi-Fi 7) mode. Please refer to [documentation](#) for more details.

このドキュメントの作成時点で、ネットワークで有効になっているすべてのWLANは、ファームウェアバージョンMR 31.1.x以降で有効にされるためには、Wi-Fi 7仕様の要件を満たす必要があります。

つまり、前述のように設定されたWi-Fi 7 SSIDは、WPA2-PersonalまたはWPA3-SAE移行モードを使用して別のSSIDと共存できません。

ダッシュボードネットワークでWPA2-Personal SSIDが設定されている場合、すべてのWi-Fi 7 APはWi-Fi 6E動作に戻ります。

この動作は、ファームウェアMR 32.1.xの将来のバージョンで変更されます。

オープン/拡張オープン/引き受け/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ワードは必要なく、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。

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ワード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でパスワードが必要でなくても、パスワード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。802.11規格の定義では、クライアントがシームレスにローミングできるすべてのBSSを識別するためにSSID名が使用されるため、異なるSSID名を使用する必要がある点に注意してください。したがって、同じSSID名を持つ異なるセキュリティ設定のSSIDを使用することは違法であり、危険です。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。

IOS XEのLEAD設定

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。

現時点では、多くのモバイルクライアントが部分的な、またはそれほど使いやすくないLEAN/Enhanced Openのサポートを提供しています。クライアントとテストを行い、サポートを測定します。

2つの異なるゲストWLAN (1つのオープンWLANと1つのLEAD/EnhancedオープンWLAN) を持つことは、解決策のように見えますが (特に、LEADセキュアゲストを6 GHzのみに保持し、完全にオープンなゲストWLANを5 GHzのみに保持する場合)、この2つのゲストWLANを異なるサブネットに分離する必要があります。そうしないと、同じサブネットで暗号化解除されてされます。

WPA + WPA2
 WPA2 + WPA3
 WPA3
 Static WEP
 None

MAC Filtering
 Lobby Admin Access

Needed if using CWA or other web portal techniques requiring MAC filtering

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 Disabled

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

Transition Mode WLAN ID 0-4096

Cisco MerakiダッシュボードのLEAD設定

IOS XEと同様に、Cisco Merakiダッシュボードの6 GHzで動作する拡張オープン/LEANを使用して別のゲストSSIDを作成することを推奨します。

この設定はWireless > Access Controlで再度行うことができ、セキュリティ方式として「Opportunistic Wireless Encryption (LEAN)」を選択します。

Security Opportunistic Wireless Encryption

Open (no encryption)
 Any user can associate

Opportunistic Wireless Encryption (OWE)
 Any user can associate with data encryption

Password
 Users must enter a passphrase to associate ⓘ

MR31までのファームウェアを実行している場合、サポートされているWPAタイプは「WPA3のみ」であり、ダッシュボードでは別の方法を選択できません。

FT(802.11r)を有効にすることはできませんが、この設定ではPMFは必須です。

「WPA3のみ」というラベルはLEANがWPA3標準の一部ではないため過負荷になっていますが、この設定はLEANを遷移モードなしで使用することを示しています。

MR 32.1.xの今後のリリースの一部として、LEAD移行モードが使用可能になります。

WPA encryption ⓘ WPA3 only ▾

802.11r ⓘ Enabled Adaptive Disabled

802.11w ⓘ Enabled (allow unsupported clients) Required (reject unsupported clients) Disabled (never use)

AES(CCMP128)暗号は、Wi-Fi 6Eクライアントまでの互換性を最大にするためにデフォルトで有効になっています。

GCMP256ビットをCCMP128とともに有効にすると、Wi-Fi 7要件に準拠できます。

Advanced WPA3 settings (Cipher and AKM suite settings) ▾

WPA3 Cipher Suite GCMP 256

ⓘ Certain Cipher suite and AKMs are required for capable APs to operate in 802.11be (Wi-Fi 7) mode. Please refer to [documentation](#) for more details.

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（管理MIC）であり、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。ビーコンの正当性を検証できるのは、WPA3暗号キーに関連付けられたクライアントだけです。プローブクライアントには、ビーコンを検証する手段がありません。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クライアントを指します）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引き起こしません（不適切にプログラムされたクライアントドライバを除く）。

17.18以降では、WLANがWi-Fi 7に準拠している場合は、ビーコン保護チェックボックスを有効にするかどうかに関係なく、ビーコン保護要素が自動的に有効になります

次のスクリーンショットは、管理MIC情報要素の内容の例を示しています。

```
  Tag: Management MIC
    Tag Number: Management MIC (76)
    Tag length: 16
    KeyID: 6
    IPN: 350200000000
    MIC: c0105301ca902ff1
```

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エーションです。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、それでもGCMP256暗号化を実装していない場合があります。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できない場合に問題になる可能性があります。

GCMP256が有効な場合、WLANのビーコンフレームのRobust Security Network Element(RSNE)は、次に示すようにPairwise Cipher Suite Listの機能をアドバタイズします。

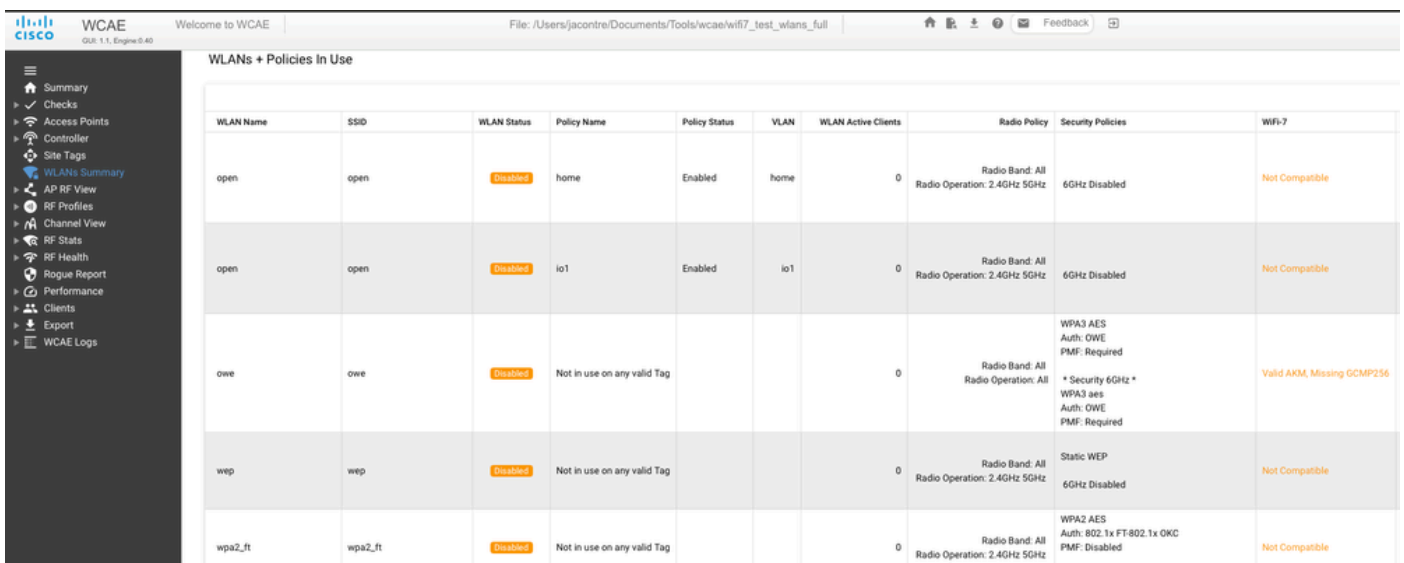
```
Pairwise Cipher Suite Count: 2
  Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) GCMP (256) 00:0f:ac (Ieee 802.11) AES (CCM)
    Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) GCMP (256)
      Pairwise Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
      Pairwise Cipher Suite type: GCMP (256) (9)
    Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
      Pairwise Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
      Pairwise Cipher Suite type: AES (CCM) (4)
```

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の設定を前述のすべての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対応かどうか疑問が残る場合は、WCAEを使用して何が間違っているかを知ることができます。



WLAN Name	SSID	WLAN Status	Policy Name	Policy Status	VLAN	WLAN Active Clients	Radio Policy	Security Policies	WiFi-7
open	open	Disabled	home	Enabled	home	0	Radio Band: All Radio Operation: 2.4GHz 5GHz	6GHz Disabled	Not Compatible
open	open	Disabled	io1	Enabled	io1	0	Radio Band: All Radio Operation: 2.4GHz 5GHz	6GHz Disabled	Not Compatible
owe	owe	Disabled	Not in use on any valid Tag			0	Radio Band: All Radio Operation: All	WPA3 AES Auth: OWE PMF: Required * Security 6GHz * WPA3 aes Auth: OWE PMF: Required	Valid AKM, Missing GCMP256
wep	wep	Disabled	Not in use on any valid Tag			0	Radio Band: All Radio Operation: 2.4GHz 5GHz	Static WEP 6GHz Disabled	Not Compatible
wpa2_ft	wpa2_ft	Disabled	Not in use on any valid Tag			0	Radio Band: All Radio Operation: 2.4GHz 5GHz	WPA2 AES Auth: 802.1x FT-802.1x OKC PMF: Disabled	Not Compatible

トラブルシューティングチェックリスト

- Web UI (R32または17.18.2以降) は、WLANがWi-Fi 7規格に準拠しているかどうかを示します。セキュリティ設定がこのドキュメントのヘルプに準拠していることを確認します。
- クライアントがWi-Fi7をサポートしていることを確認します。Windowsラップトップの場合は、Windows 11 24h2が最低限必要です。ワイヤレスアダプタのドライバがアップデートされていることを確認します。
- Windowsのコマンド「netsh wlan show drivers」は、ワイヤレスアダプタの機能を一覧表示し、そのステータスを確認するのに非常に便利です。
- ラップトップの場合は、アダプタ設定に移動して、11beモードが有効になっていることを確認します。互換性のために、多くのアダプタが最初の日に無効になった11beで、11axとして動作しました。
- 疑問がある場合は、Over-the-Airパケットキャプチャを使用して、以下の点を確認します。
 - APはビーコンでEHT情報要素をブロードキャストしています。ビーコンはレガシーレートで送信されるため、これはWi-Fi 7をサポートする必要のない任意のスニファでキャプチャできます。
 - APがEHTを正しくブロードキャストしている場合、クライアントは関連付け要求でEHT要素を送信している必要があります。そうでない場合は、クライアントがWi-Fi

7に準拠するAPセキュリティ設定を見つけられなかったか、またはアダプタのプロパティでクライアントの802.11be設定が無効になっていることを示します

参照資料

1. [Cisco Systems. 『WPA3暗号化および設定ガイド』](#)
2. [Meraki WPA3ガイド](#)

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。