Mobility Express ネットワークのモニタ

[ネットワークサマリー（Network Summary）] の表示

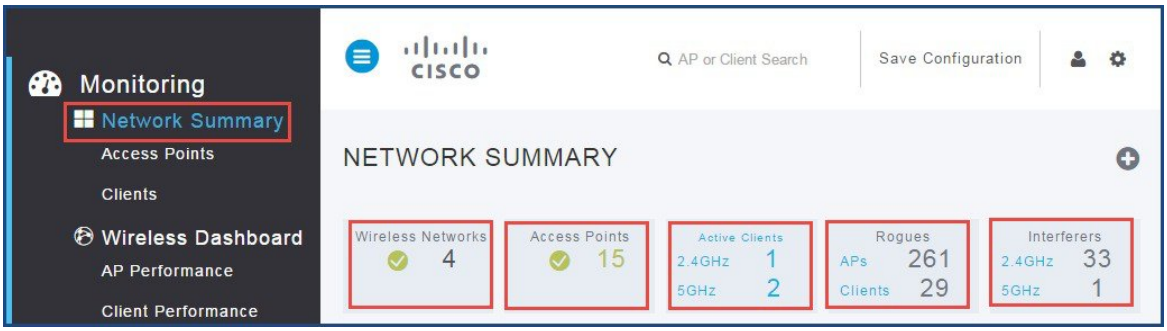
[モニタリング（Monitoring）] サービスを使用すれば、マスター AP で Cisco Mobility Express ネットワークをモニタすることができます。

監視ダッシュボード

[ネットワークサマリー（Network Summary）] ページの監視ダッシュボードには、次のものの数が表示されます。

1. 無線ネットワーク
2. アクセス ポイント
3. アクティブ クライアント（2.4 GHz および 5 GHz）
4. 不正な AP とクライアント
5. 干渉

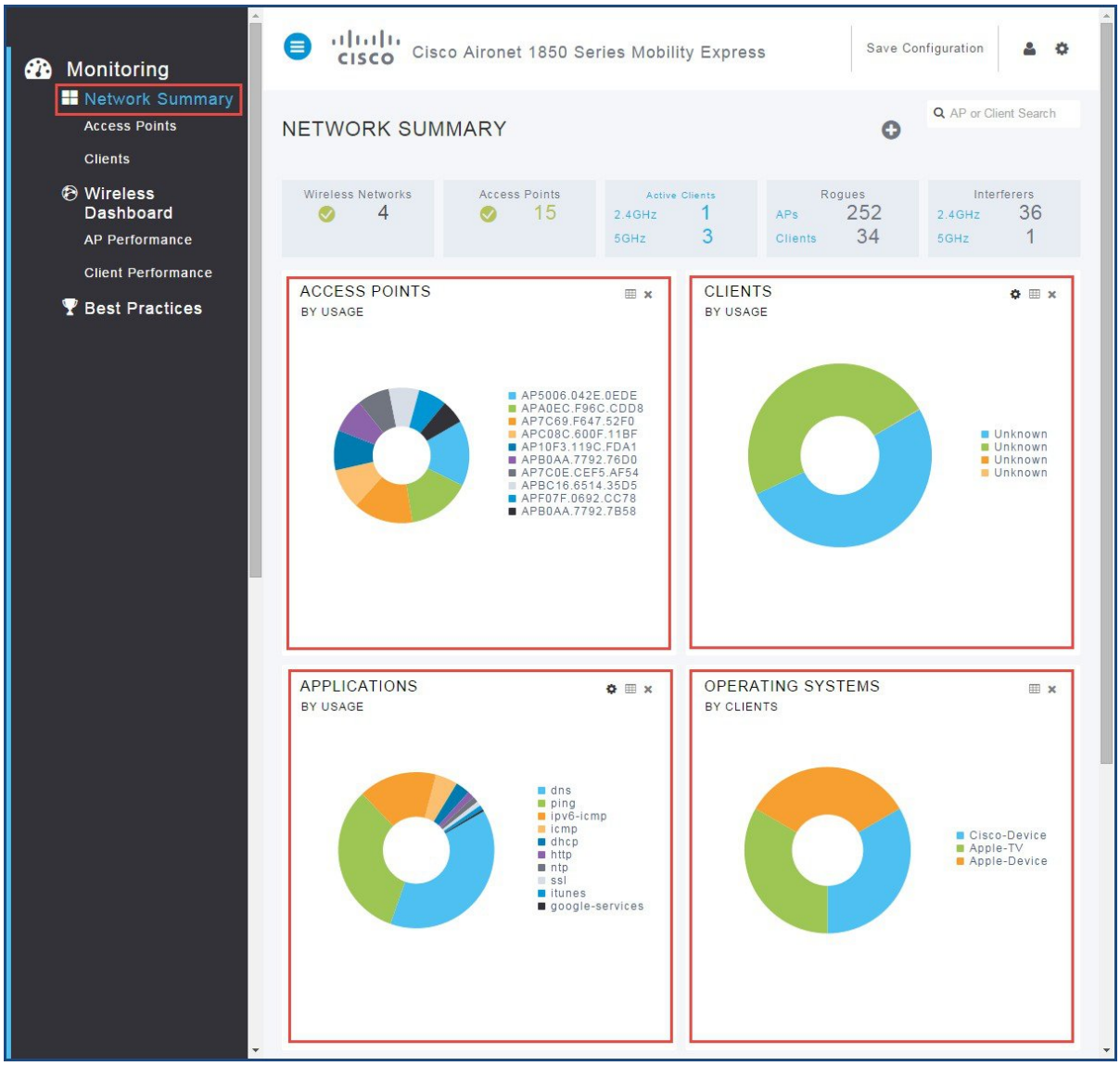
（注） [不正（Rogues）] と [干渉（Interferers）] は、クリック可能なリンクではありません。 数のみが表示されます。



[ネットワークサマリー（Network Summary）]ページには、次のものに関するデータを表形式とグラフ形式の両方で表示するカスタマイズ可能な 5 つのウィジェットが組み込まれています。

1. アクセス ポイント（使用 AP 別）
2. クライアント（使用クライアント別）
3. アプリケーション（使用アプリケーション別）
4. オペレーティング システム（クライアント別）
5. 上位 WLAN（使用数別）

（注） [ネットワークサマリー（Network Summary）] の下のウィジェットに、ワイヤレス ネットワークの集約データが表示されます。



GUI を使用したアクセス ポイントの要約の表示

GUI を使用してアクセス ポイントを表示するには、次の手順を実行します。

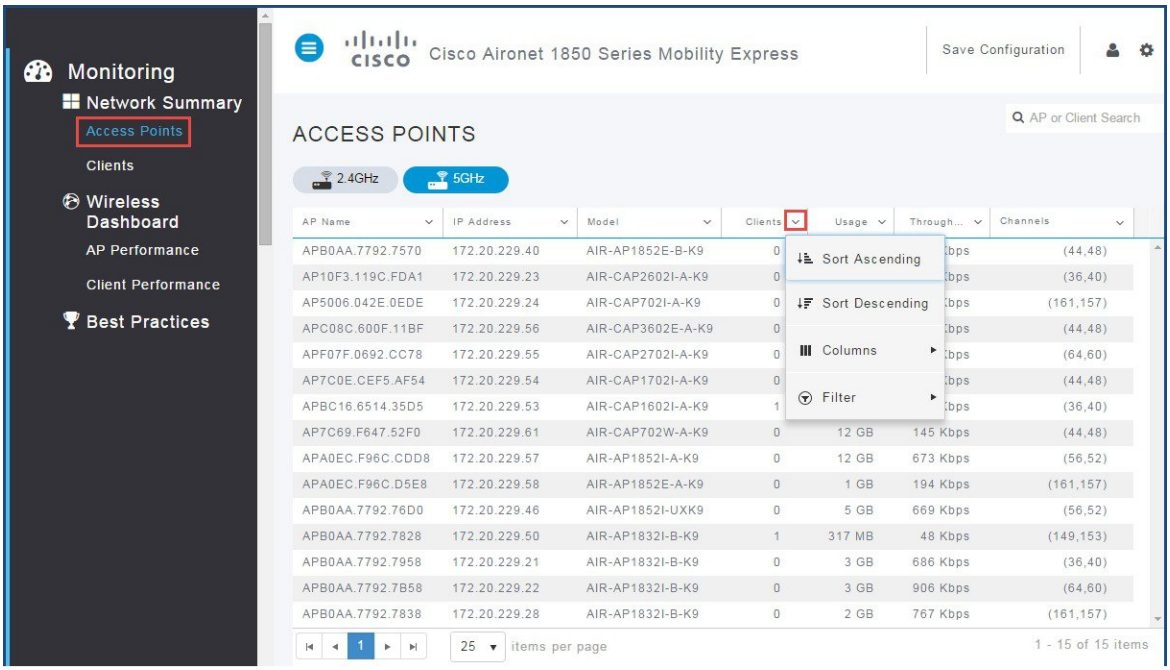
手順

ステップ 1 [モニタリング（Monitoring）] > [ネットワークサマリー（Network Summary）] > [アクセスポイント（Access Points）] をクリックします。

テーブルにアクセス ポイントのリストが表示されます。

ステップ 2 各無線周波数で動作するアクセス ポイントのリストを表示するには、[2.4 GHz] タブと [5 GHz] タブとの間で切り替えます。

ステップ 3 （任意）テーブル ビューで非表示または表示になるように列を選択するには、列ヘッダーの右上にある下矢印をクリックします。必要なパラメータに基づいてテーブル ビューをフィルタ処理するには、目的のフィールドを非表示または表示にします。



CLI を使用したアクセス ポイントの要約の表示

CLI を使用してアクセス ポイントの要約を表示するには、次の手順を実行します。

手順

次のコマンドを入力して、マスター AP に関連付けられているアクセス ポイントすべての要約を表示します。

```
show ap summary
```

```
(Cisco Controller) >show ap summary

Number of APs.................................... 15

Global AP User Name.............................. Not Configured
Global AP Dot1x User Name........................ Not Configured

AP Name             Slots  AP Model             Ethernet MAC       Location          Country    IP Address       Clients   DSE Location
------------------  -----  -------------------  -----------------  ----------------  ---------  ---------------  --------  -------------
APB0AA.7792.7570      2     AIR-AP1852E-B-K9     b0:aa:77:92:75:70  default location  US         172.20.229.40      0       [0 ,0 ,0 ]
AP10F3.119C.FDA1      2     AIR-CAP2602I-A-K9    10:f3:11:9c:fd:a1  CONF ROOM MARS    US         172.20.229.23      0       [0 ,0 ,0 ]
AP5006.042E.0EDE      2     AIR-CAP702I-A-K9     50:06:04:2e:0e:de  RESTROOM          US         172.20.229.24      0       [0 ,0 ,0 ]
APC08C.600F.11BF      2     AIR-CAP3602E-A-K9    c0:8c:60:0f:11:bf  CONF ROOM SATURN  US         172.20.229.56      1       [0 ,0 ,0 ]
APF07F.0692.CC78      2     AIR-CAP2702I-A-K9    f0:7f:06:92:cc:78  STORE ROOM        US         172.20.229.55      0       [0 ,0 ,0 ]
AP7C0E.CEF5.AF54      2     AIR-CAP1702I-A-K9    7c:0e:ce:f5:af:54  CONF ROOM PLUTO   US         172.20.229.54      0       [0 ,0 ,0 ]
APBC16.6514.35D5      2     AIR-CAP1602I-A-K9    bc:16:65:14:35:d5  LAB               US         172.20.229.53      2       [0 ,0 ,0 ]
AP7C69.F647.52F0      2     AIR-CAP702W-A-K9     7c:69:f6:47:52:f0  BREAK ROOM        US         172.20.229.61      0       [0 ,0 ,0 ]
APA0EC.F96C.CDD8      2     AIR-AP1852I-A-K9     a0:ec:f9:6c:cd:d8  MAIN OFFICE       US         172.20.229.57      0       [0 ,0 ,0 ]
APA0EC.F96C.D5E8      2     AIR-AP1852E-A-K9     a0:ec:f9:6c:d5:e8  MAIN OFFICE       US         172.20.229.58      0       [0 ,0 ,0 ]
APB0AA.7792.76D0      2     AIR-AP1852I-UXK9     b0:aa:77:92:76:d0  CONF ROOM NEPTUN  US         172.20.229.46      0       [0 ,0 ,0 ]
APB0AA.7792.7828      2     AIR-AP1832I-B-K9     b0:aa:77:92:78:28  default location  US         172.20.229.50      0       [0 ,0 ,0 ]
APB0AA.7792.7958      2     AIR-AP1832I-B-K9     b0:aa:77:92:79:58  default location  US         172.20.229.21      1       [0 ,0 ,0 ]
APB0AA.7792.7B58      2     AIR-AP1832I-B-K9     b0:aa:77:92:7b:58  default location  US         172.20.229.22      0       [0 ,0 ,0 ]
```

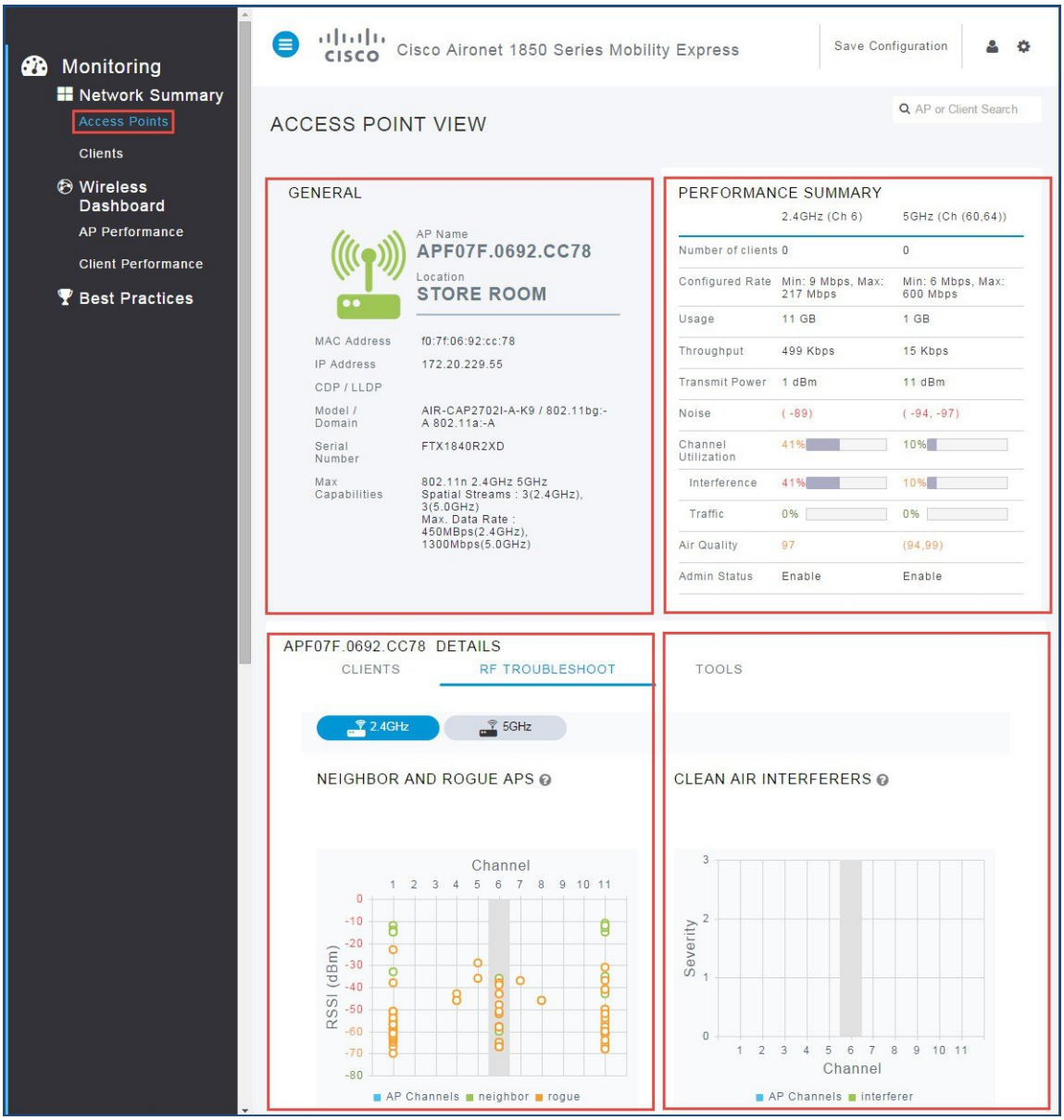
GUI を使用したアクセス ポイントの詳細の表示

GUI を使用してアクセス ポイントの詳細を表示するには、次の手順を実行します。

手順

ステップ 1 リストで任意のアクセス ポイントをクリックして、その AP に関する詳細情報を表示します。 デフォルトのタブは [RF トラブルシュート（RF Troubleshoot）] タブで、次の情報が表示されます。

1. 全般的な AP のパラメータ
2. 2 つの無線（2.4 GHz と 5 GHz）のパフォーマンスの要約
3. ネイバー AP と不正 AP
4. Clean Air の干渉
5. 使用数別のクライアントの分布
6. とデータ レート別のクライアントの分布



ステップ 2 [ツール（Tools）] をクリックして、AP を再起動するか、または AP の設定をクリアします。

CLI を使用したアクセス ポイントの詳細の表示

CLI を使用してアクセス ポイントを表示するには、次の手順を実行します。

手順

ステップ 1　次のコマンドを入力して、アクセス ポイントを表示します。
```
show ap <option>
```

ステップ 2　AP を再起動するには、次のコマンドを入力します。
```
(Cisco Controller) >config ap reset <Cisco AP>
```

GUI を使用したクライアントの要約の表示

GUI を使用してクライアントの要約を表示するには、次の手順を実行します。

手順

ステップ 1　[モニタリング（Monitoring）] > [ネットワークサマリー（Network Summary）] > [クライアント（Clients）] をクリックします。

ステップ 2　（任意）テーブル ビューで非表示または表示になるように列を選択するには、列ヘッダーの右上にある下矢印をクリックします。
必要なパラメータに基づいてテーブル ビューをフィルタ処理するには、目的のフィールドを非表示または表示にします。

CLI を使用したクライアントの要約の表示

CLI を使用してクライアントの要約を表示するには、次の手順を実行します。

手順

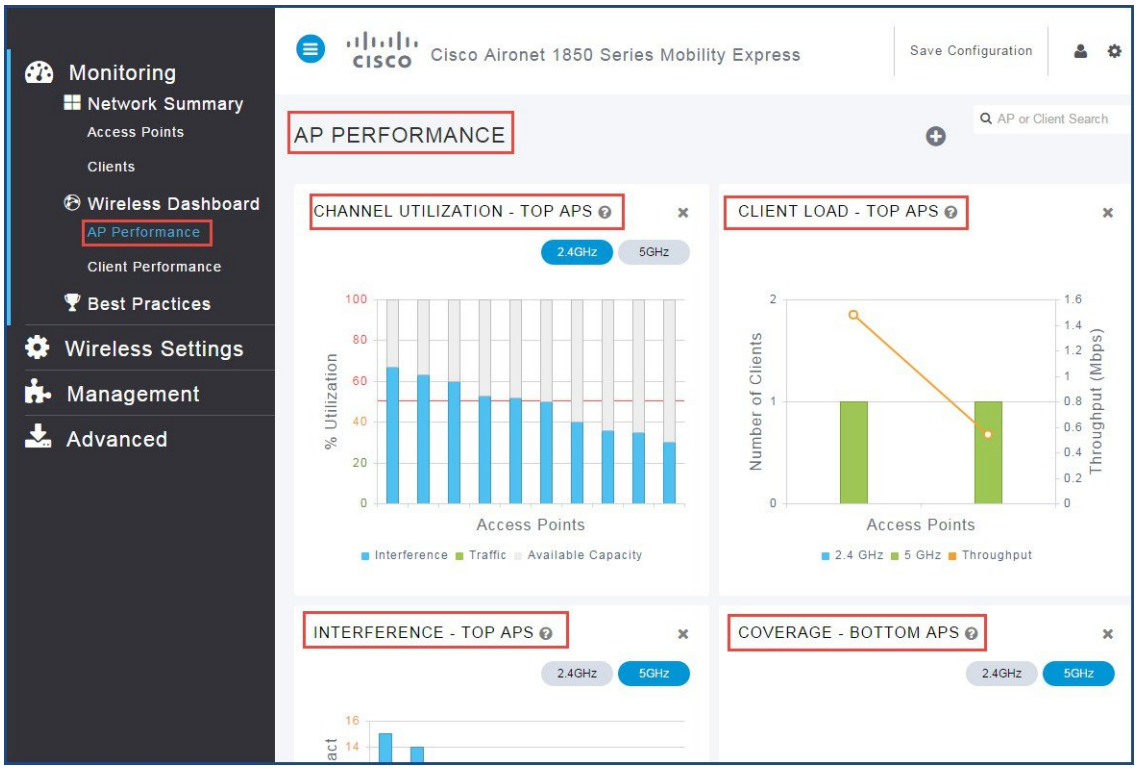
次のコマンドを入力して、Mobility Express ネットワークに接続されているアクセス ポイントすべての要約を表示します。
```
show client summary
```

[ワイヤレス ダッシュボード（Wireless Dashboard）] の表示

[ワイヤレス ダッシュボード（Wireless Dashboard）] には、AP およびクライアントのパフォーマンスの詳細が表示されます。

[AP パフォーマンス（AP Performance）] の表示

[AP パフォーマンス（AP Performance）] ダッシュボードは、ユーザが Mobility Express の問題を特定してトラブルシューティングするために役立ちます。



[AP パフォーマンス（AP Performance）] ダッシュボードにアクセスするには、[モニタリング（Monitoring）] > [AP パフォーマンス（AP Performance）] を選択します。

[AP パフォーマンス（AP Performance）] ダッシュボードには、次のグラフが表示されます。

- [チャネル使用率の上位 AP（Channel Utilization Top APs）]：AP で割り当てられているチャネルを介したデータと干渉を含むトラフィックのレベル。 干渉には、Wi-Fi 信号および非 Wi-Fi 信号の両方が含まれています。 チャネルの高い使用率（たとえば、50％以上）は、同じチャネル上の近くの AP/クライアント/不正からのノイズなどの干渉が高いレベルであることを示しています。この場合、クライアントのパフォーマンスは低下します。
- [クライアント負荷の上位 AP（Client Load TOP APs）]：負荷インジケータには、各アクセスポイント上で接続されている現在のクライアント数が表示されます。 高い負荷はパフォーマンスに影響を与えるおそれがあります。クライアント ロード バランシングを使用すれば、ワイヤレス ネットワークでのクライアントの分散を向上させることができます。
- [干渉の上位 AP （Interference Top APs）]：RF 干渉には、正常な無線運用を妨害し、潜在的なネットワーク遅延およびクライアントのパフォーマンスの低下を生じさせる、望ましくな

い RF 信号の干渉が含まれています。 干渉する RF 信号には、Wi-Fi 信号と非 Wi-Fi 信号の両方が含まれています。

- [カバレッジ下位 AP（Coverage BOTTOM APs）]：カバレッジ ホールとは、クライアントがワイヤレス ネットワークから信号を受信できないエリアのことです。 カバレッジホールは、クライアントの SNR があらかじめ決められたレベルを下回った場合に発生したとみなされます。 カバレッジ ホール イベントとは、いくつかのクライアントが同じカバレッジ ホールに留まっている状態を意味しています。

[クライアント パフォーマンス（Client Performance）] の表示

[クライアント パフォーマンス（Client Performance）] ダッシュボードは、ユーザが Mobility Express ネットワークへの接続障害の原因を特定して、クライアント関連の問題をトラブルシューティングするために役立ちます。

[クライアント パフォーマンス（Client Performance）] ダッシュボードにアクセスするには、[モニタリング（Monitoring）] > [クライアント パフォーマンス（Client Performance）] を選択します。

[クライアント パフォーマンス（Client Performance）] ダッシュボードには、次のグラフが表示されます。

- [信号強度（Signal Strength）]：信号強度が高くなると、接続の信頼性がより高くなり、高速になります。 信号強度は -dBm 形式で表され、0 ~ -100 dBm の範囲です。 値が 0 に近づくほど、信号はより強くなります。 クライアントの要約を表示するには、クリックします。
- [接続レート（Connection Rate）]：各クライアントのスループットは、どの時点でも、使用されるデータ レート（802.11 a/b/n/ac）によって異なります。このデータ レートは常に変化する可能性があります。 RSSI 値、RF 干渉などのさまざまな要因が、クライアント デバイスの瞬間的なデータ レートに影響を与える可能性があります。
- [信号品質（Signal Quality）]：信号対雑音比（SNR）とは、信号強度とノイズ レベル間の強さの比率です。 この値は +dBm 値で表されます。 通常、最低でも +25 dBm の信号対雑音比が必要です。 値が +25 dBm よりも小さくなると、パフォーマンスと速度が低下します。
- [クライアント接続（Client Connections）]：アクセス ポイントに関連付けられている、すべての接続タイプのクライアントを表示します。

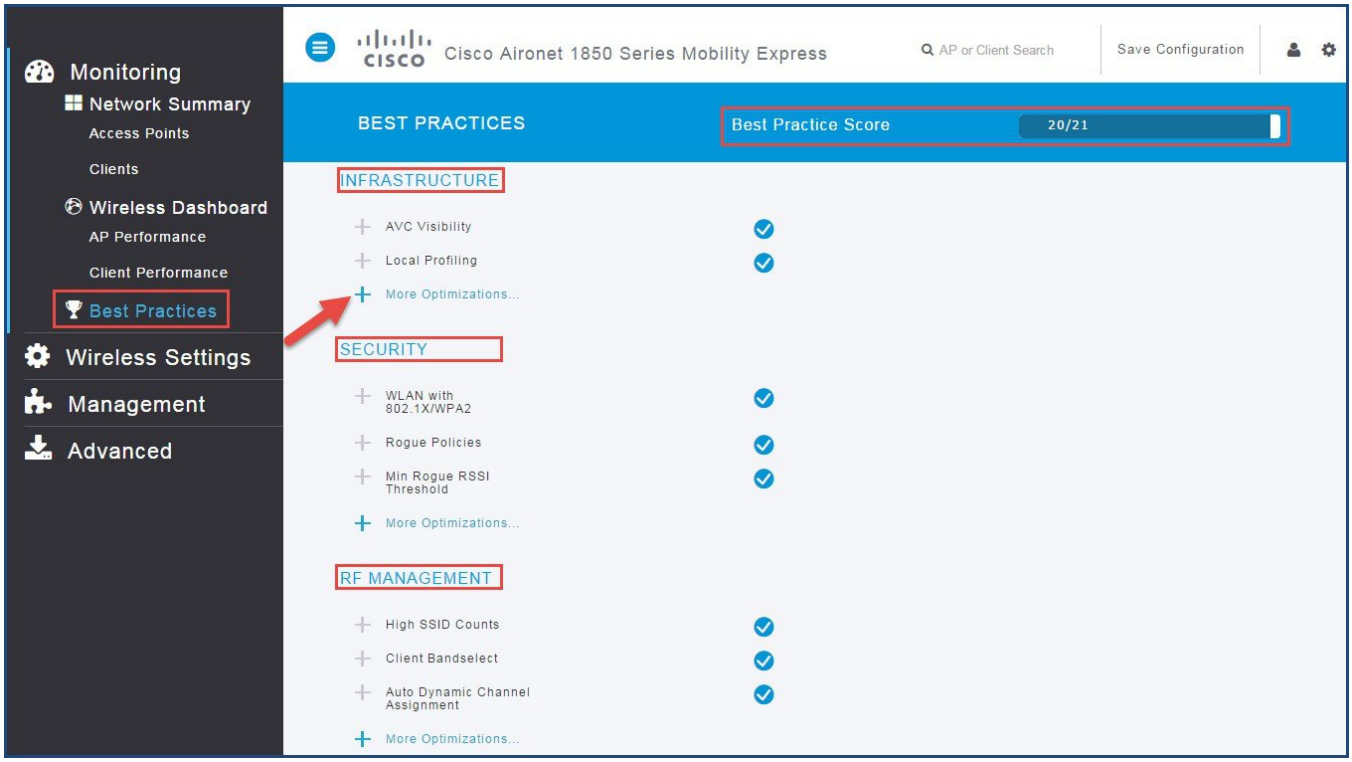
ベスト プラクティス

[ベストプラクティス（Best Practices）] ページには、Mobility Express の [インフラストラクチャ（Infrastructure）]、[セキュリティ（Security）]、および [RF 管理（RF Management）] に対して有効になっているデフォルトの機能が表示されます。

[ベストプラクティス（Best Practices）] は、GUI から無効にすることはできません。 [ベストプラクティス（Best Practices）] のいずれかが CLI から無効にされると、ユーザは無効になったベスト

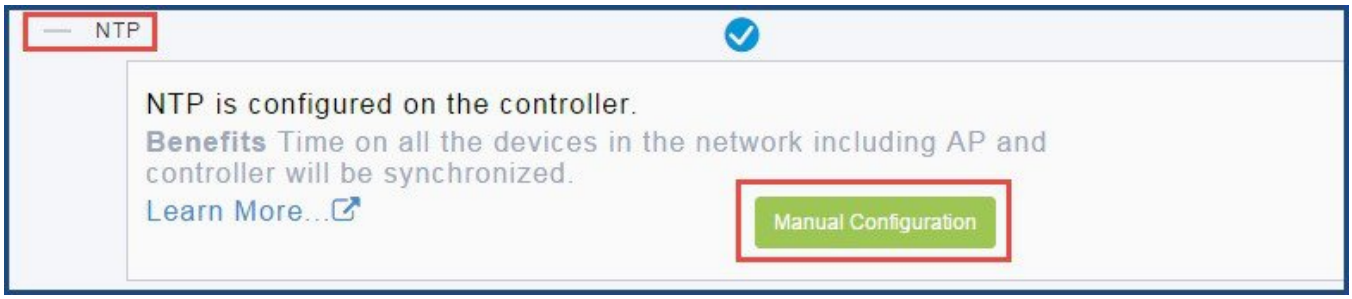
プラクティスを展開して [デフォルトの復元（Restore Default）] ボタンをクリックすることで、GUI から有効にできます。

次の図に示すように、そのカテゴリのすべてのベスト プラクティスを表示するには、[+その他の最適化（+ More Optimizations）] をクリックします。



次の 3 つのベスト プラクティスでは、次の図で強調表示しているように、[手動設定（Manual Configuration）] が必要になる場合があります。

1. [インフラストラクチャ（Infrastructure）] > [NTP]。
2. [セキュリティ（Security）] > [WLAN with 802.1x/WPA2]。
3. [最大 SSID 数（High SSID Count）]。



インフラストラクチャ

[インフラストラクチャ（Infrastructure）] には、次のベスト プラクティスが一覧表示されます。

アプリケーションの表示

[アプリケーションの表示（Application Visibility）]（制御なし）では、Network-Based Application Recognition（NBAR）エンジンによるシスコの ディープ パケット インスペクション（DPI）技術を使用してアプリケーションを分類し、Wi-Fi ネットワークに関するアプリケーション レベルの可視性を提供します。 アプリケーションの可視性を使用すれば、コントローラで 1000 を超えるアプリケーションを検出できます。 このアプリケーションを使用すれば、リアルタイム分析を行うことができます。

[アプリケーションの表示（Application Visibility）] は、デフォルトではすべての WLAN で有効になっています。 [アプリケーションの表示（Application Visibility）] が無効になっている場合、[デフォルトの復元（Restore Default）] をクリックして、すべての WLAN で [アプリケーションの表示（Application Visibility）] を有効にします。

ステータス：

- 選択済み：すべての WLAN で有効になっています。
- 未選択：1 つ以上の WLAN で無効になっています。

CLI のオプション：

WLAN で [アプリケーションの表示（Application Visibility）] を有効にするには、次のコマンドを入力します。

```
(Cisco Controller) >config wlan avc wlan-id visibility enable
```

ローカル プロファイリング

Cisco Mobility Express のコントローラでは、クライアント デバイスがコントローラに関連付けられている場合、受信した情報からクライアントタイプを判別できます。 このコントローラは情報のコレクタとして機能し、収集した情報を Cisco Mobility Express の GUI ダッシュボードに直接表示するか、または ISE に必要なデータを最も適切に送信します。 [ローカル プロファイリング（Local Profiling）] は、デフォルトではすべての WLAN で有効になっています。

[ローカル プロファイリング（Local Profiling）] は、デフォルトでは有効になっています。 これが無効になっている場合、[デフォルトの復元（Restore Default）] をクリックして、Cisco Mobility Express のコントローラでローカル プロファイリング（DHCP/HTTP）を有効にします。この有効化は、その特定の時点でサービスに影響を与える場合があります。

ステータス：

- 選択済み：すべての WLAN で有効になっています。 これは、RADIUS プロファイルが有効な場合、緑の状態で表示されます。
- 未選択：無効になっています。

CLI のオプション：

すべての WLAN で ローカル プロファイリング（DHCP/HTTP）を有効にするには、次のコマンドを入力します。

```
(Cisco Controller) >config wlan profiling local all enable
```

NTP

Mobility Express コントローラの日付と時刻を同期するには、NTP サーバを使用する必要があります。 場所、SNMPv3 の機能のいずれかを使用する場合、Mobility Express のいくつかの機能で NTP 同期を使用することが重要かつ必須です。

NTP サーバが設定されていない場合、[手動設定（Manual Configuration）] > [管理（Management）] > [時刻（Time）] をクリックして、NTP サーバの詳細を設定します。

ステータス：

- 選択済み：設定済みです。
- 未選択：無効になっています。

CLI のオプション：

NTP サーバを有効にするには、次のコマンドを入力します。

```
(Cisco Controller) >config time ntp server ntp-server-index ntp-server-ip-address
```

高速 SSID

高速 SSID 変更が有効になっている場合、コントローラではクライアントが SSID 間でより高速に移動できるようにします。 高速 SSID が有効になっている場合、クライアント エントリがクリアされず、遅延は適用されません。 [高速 SSID（Fast SSID）] は、Apple iOS デバイスをサポートするために重要です。

[高速 SSID（Fast SSID）] は、デフォルトでは有効になっています。 これが無効になっている場合、[デフォルトの復元（Restore Default）] をクリックして [高速 SSID（Fast SSID）] を有効にします。

ステータス：

- 選択済み：有効になっています。
- 未選択：無効になっています。

CLI のオプション：

[高速 SSID（Fast SSID）] を有効にするには、次のコマンドを入力します。

```
(Cisco Controller) >config network fast-ssid-change
```

管理用 HTTPS

[管理用 HTTPS（HTTPS for Management）] では、セキュアなアクセスを可能にすることで、セキュリティが向上します。 Mobility Express のコントローラを管理するには、[HTTPS アクセス（HTTPS Access）] を有効にする必要があります。 Web アクセス（HTTP）を無効にする必要があります。

ステータス：

- 選択済み：HTTPS が有効になっています。つまり、HTTP が無効になっています。
- 未選択：HTTPS が有効で HTTP が有効、または HTTPS が無効で HTTP が有効になっています。

CLI のオプション：

ユーザによる *http://ip-address* を使用した Mobility Express のコントローラ GUI へのアクセスを拒否するために Web モードを無効にするには、次のコマンドを入力します。

```
(Cisco Controller) >config network webmode disable
```

ユーザによる *https://ip-address* を使用した Mobility Express のコントローラ GUI へのアクセスを許可するために [管理用 HTTPS（HTTPS for Management）] を有効にするには、次のコマンドを入力します。

```
(Cisco Controller) >config network secureweb enable
```

Aironet IE

Aironet IE とは、接続性の向上のためにシスコのデバイスで使用されるシスコ独自の属性です。この属性には、アクセス ポイント（AP）から WLAN のビーコン応答とプローブ応答で送信される、アクセス ポイント名、負荷、関連付けられたクライアントの数などの情報が含まれています。 Cisco Client Extensions（CCX）クライアントでは、この情報を使用して関連付けるために最適な AP を選択します。

CCX ソフトウェアは、サードパーティ製クライアントデバイスの製造業者およびベンダーに対してライセンスされます。 これらのクライアント上にある CCX コードにより、サードバーティ製クライアント デバイスは、シスコ製の AP と無線で通信できるようになり、他のクライアント デバイスでサポートしていないシスコの機能もサポートできるようになります。 これらの機能は、セキュリティの強化、パフォーマンスの向上、高速ローミング、および電源管理に関連しています。

Aironet IE は CCX ベースのクライアントで任意ですが、一部のタイプのワイヤレス クライアントとの互換性の問題の原因となる可能性があります。 WGB および Cisco 音声を有効にすることを推奨しますが、通常の実稼働ネットワークの場合、テスト後に Aironet IE を無効にすると役立つ可能性があります。

CCX Aironet IE 機能は、無効にする必要があります。 この機能が有効になっている場合、[デフォルトの復元（Restore Default）] をクリックして無効にします。

ステータス：

- 選択済み：すべての WLAN で CCX Aironet IE が無効になっています。
- 未選択：すべての WLAN で CCX Aironet IE が有効になっています。

CLI のオプション：

特定の WLAN に対して Aironet IE のサポートを無効にするには、次のコマンドを入力します。

```
(Cisco Controller) >config wlan ccx aironetIeSupport disable wlan-id
```

セキュリティ

[セキュリティ（Security）] には、次のベスト プラクティスが一覧表示されます。

WLAN の 802.1X

WLAN では、802.1X セキュリティを使用する必要があります。デイゼロ（Wireless Express のセットアップ）は、デフォルトでは 802.1X を要求しません。

ステータス：

- 選択済み：少なくとも 1 つの WLAN で 802.1X を使用している場合、有効になっています。
- 未選択：無効になっています。

不正ポリシー

不正なワイヤレス デバイスは、企業のワイヤレス ネットワークにとって常に脅威となっています。ネットワークの所有者は、不明なデバイスをスキャンするだけでなく、それ以上のことを実施する必要があります。所有者は、不正や侵入者の脅威の検出、無効化、特定、および管理をリアルタイムで自動的に実行できる必要があります。

不正 AP は、正規のクライアントをハイジャックし、プレーン テキスト、サービス妨害攻撃、または中間者攻撃を使用することによって、無線 LAN の運用を妨害します。つまり、ハッカーは不正 AP を使用して、パスワードやユーザ名などの機密情報を取得できます。これに成功すると、ハッカーは一連の Clear To Send（CTS; クリア ツー センド）フレームを送信できるようになります。このフレームでは AP を模倣し、特定の無線 LAN クライアント アダプタに送信を通知し、他のすべてのアダプタには待機を通知します。このシナリオでは、正規のクライアントは、無線 LAN リソースに接続できなくなります。このため、無線 LAN のサービス プロバイダーは、その無線周波数帯で不正 AP を禁止する方法を探し求めています。

ベストプラクティスは、不正検出を使用して、たとえば、ある企業の環境内でセキュリティリスクを最小限に抑えることです。ただし、OEAP 導入、オープンエアーの会場やスタジアム、市全域、屋外など、不正検出が不要な特定のシナリオがあります。屋外のメッシュ AP を使用して不正を検出しても、分析するリソースが増えるばかりでメリットはほとんどありません。さらに、不正の自動封じ込めを評価する（または完全に止める）ことがきわめて重要です。これは、不正の自動封じ込めを動作させておくと法的な問題や責任が生じる可能性があるためです。ポリシーは、少なくとも [高（High）] である必要があります。

[不正ポリシー（Rogue Policies）] は、デフォルトで [高（High）] に設定されます。[不正ポリシー（Rogue Policies）] が [カスタム（Custom）] に設定されている場合、[デフォルトの復元（Restore Default）] をクリックして [高（High）] に変更します。

ステータス：

- 選択済み：ポリシーは [高（High）] 以上に設定されています。
- 未選択：ポリシーは [カスタム（Custom）] に設定されています。

CLI のオプション：

不正検出のセキュリティ レベルを [高（High）] に設定するには、次のコマンドを入力します。
```
(Cisco Controller) >config rogue detection security-level high
```

最小不正 RSSI しきい値

この基準は通常、不明な不正 AP が設備の境界の内側にあることを示し、ワイヤレス ネットワークに対する干渉の原因となる可能性があります。

このルールは、小売業のお客様、またはすべての無線利用者からの WiFi 信号が一般的には互いに混在している、さまざまなテナントによって共有される会場には推奨しません。

AP で不正を検出し、不正のエントリがコントローラで作成されるために必要な最小 RSSI 値を指定します。推奨値は -80 dBm です。

[最小不正 RSSI しきい値（Min Rogue RSSI Threshold）] は、-80 dBm に設定されます。この値がこれよりも低く設定されている場合、[デフォルトの復元（Restore Default）] をクリックして最小 RSSI 値を -80 dBm に変更します。

ステータス：

- 選択済み：-80 dBm に設定されています。
- 未選択：-80 dBm 未満に設定されています。

CLI のオプション：

不正を検出するために必要な最小 RSSI 値を設定するには、次のコマンドを入力します。
```
(Cisco Controller) >config rogue detection min-rssi rssi-in-dBm
```

SSH/Telnet アクセス

Mobility Express のコントローラに対する SSH は、デフォルトで有効にする必要があり、Telnet は無効にする必要があります。

SSH が無効で Telnet が有効、または SSH が有効で Telnet も有効な場合、[デフォルトの復元（Restore Default）] をクリックして SSH を有効にし、Telnet を無効にします。

ステータス：

- 選択済み：SSH が有効になっています。つまり、Telnet が無効になっています。
- 未選択：SSH が有効で Telnet も有効（または） SSH が無効で Telnet が有効になっています。

CLI のオプション：

SSH を有効にするには、次のコマンドを入力します。
```
(Cisco Controller) >config network ssh enable
```

Telnet を無効にするには、次のコマンドを入力します。
```
(Cisco Controller) >config network telnet disable
```

クライアント除外

ユーザが認証に失敗すると、コントローラによってそのクライアントが除外されます。そのクライアントは、除外タイマーが期限切れになるか、または管理者によって除外タイマーが手動でオーバーライドされるまで、そのネットワークに接続できません。

クライアント除外では、単一のデバイスによる認証の試みが検出されます。そのデバイスが失敗の最大数を超えると、その MAC アドレスの、コントローラへの関連付けはそれ以上許可されなくなります。

[クライアント除外（Client Exclusion）] は Mobility Express のコントローラでデフォルトで有効になっており、コントローラは上記のイベントの間、それらのクライアントによるコントローラへの参加を除外できます。これが無効になっている場合、[デフォルトの復元（Restore Default）] ボタンをクリックして、すべてのイベントに対して [クライアント除外（Client Exclusion）] 機能を有効にします。

ステータス：

- 選択済み：クライアント除外がすべてのイベントに対して有効になっています。
- 未選択：クライアント除外がすべてのイベントに対して無効になっています。

CLI のオプション：

すべてのイベントに対してクライアント除外を有効にするには、次のコマンドを入力します。

```
(Cisco Controller) >config wps client-exclusion all enable
```

レガシー IDS

Cisco Mobility Express のコントローラでは、接続されたすべての AP を使用して WLAN の IDS 分析を実行し、検出された攻撃を仮想コントローラに報告します。無線 IDS 分析は、別の状況では有線ネットワーク IDS システムで実行される場合がある分析を補完するものです。Cisco Mobility Express コントローラの組み込みの無線 IDS 機能では、有線ネットワーク IDS システムで入手できない 802.11 および Cisco Mobility Express コントローラ固有の情報を分析します。

これによって、無線 IDS 機能および 17 の組み込みのシグニチャで侵入攻撃を防止できます。これが無効になっている場合、[デフォルトの復元（Restore Default）] をクリックして、無線 IDS 機能を有効にし、17 の組み込みのシグニチャに対する検査を有効にすることで、侵入攻撃を防止できます。

ステータス：

- 選択済み：標準のすべてのシグニチャの検査が有効になっています。
- 未選択：標準のすべてのシグニチャの検査が無効になっています。

CLI のオプション：

シグニチャの検査を有効にするには、次のコマンドを入力します。

```
(Cisco Controller) >config wps signature enable
```

ローカル管理パスワード ポリシー

強力なパスワードを使用する必要があります。パスワード ポリシーを使用すると、コントローラおよびアクセス ポイントの追加の管理ユーザ用に新しく作成されたパスワードに対して、強力なパスワード チェックを実行できます。新規パスワードに適用される要件は次のとおりです。

- **case-check**：同じ文字が 3 回連続して使用されているかを確認します。
- **consecutive-check**：デフォルト値またはそのバリアントが使用されているかを確認します。
- **default-check**：ユーザ名またはそれを逆にした文字が使用されているかを確認します。
- **all-checks**：強力なパスワード チェックをすべて有効または無効にします。
- **position-check**：古いパスワードからの 4 文字の流用を確認します。
- **case-digit-check**：小文字、大文字、数字、および特殊文字の 4 つすべての組み合わせが含まれているかを確認します。

強力なパスワードポリシーを適用します。これが変更されている場合、[デフォルトの復元（Restore Default）] をクリックして強力なパスワード ポリシーを有効にします。

ステータス：

- 選択済み：すべての強力なパスワード ポリシーが有効になっています。
- 未選択：一部のパスワード ポリシーが有効になっているか、またはすべてのパスワード ポリシーが無効になっています。

CLI のオプション：

すべての強力なパスワード ポリシーを有効にするには、次のコマンドを入力します。

```
(Cisco Controller) >config switchconfig strong-pwd all-checks enable
```

ユーザ ログイン ポリシー

[ユーザ ログイン ポリシー（User Login Policies）] では、コントローラのローカル ネット ユーザの同時ログイン数を制限するための詳細が用意されています。同時ログイン数は制限できます。ゼロより大きい数を指定することを推奨します。デフォルト値はゼロです。

[ユーザ ログイン ポリシー（User Login Policies）] は、デフォルトで設定されています。これらが設定されていない場合、[デフォルトの復元（Restore Default）] をクリックして [ユーザ ログイン ポリシー（User Login Policies）] を設定します。

ステータス：

- 選択済み：設定済みです。
- 未選択：ユーザ ログイン ポリシーがありません。

CLI のオプション：

ネット ユーザ数の制限を確認するには、次のコマンドを入力します。

```
(Cisco Controller) >show netuser summary
```

ユーザ ログイン ポリシーを設定するには、次のコマンドを入力します。

```
(Cisco Controller) >config netuser maxUserLogin count
```

RF 管理

[RF 管理（RF Management）] には、次のベスト プラクティスが一覧表示されます。

最大 SSID 数

WLAN の数は 4 未満にする必要があります。

コントローラで設定するサービス セット識別子（SSID）の数を制限することを推奨します。 16 個の同時 SSID を設定できます（各 AP の無線ごとに）が、それぞれの WLAN または SSID で個別のプローブ応答とビーコンが必要なため、SSID がさらに追加されるにつれて、RF 環境が低下します。 さらに、PDA、WiFi 電話機、バーコード スキャナなどの小型ワイヤレス ステーションの一部では、大量の基本 SSID（BSSID）情報を管理できません。 この結果、ロックアップ（動作停止）、リロード、または関連付けの失敗が発生します。 また、SSID の数が増えるほど必要なビーコンも増えるため、実際のデータ送信に利用できる RF 時間が減少します。 たとえば、企業の場合は 1 ~ 3 個の SSID を設定し、高密度設計の場合は 1 個の SSID を設定することを推奨します。 単一の SSID シナリオでは、ユーザごとの VLAN または設定に AAA オーバーライドを利用できます。

4 個以上の SSID を有効にする場合は、有効にする WLAN を少なくできるように、[手動設定（Manual Configuration）] をクリックして [ワイヤレス設定（Wireless Settings）] > [WLAN（WLANs）] ページに移動します。

ステータス：

- 選択済み：4 個未満です。
- 未選択：4 個以上です。

CLI のオプション：

WLAN の数を確認するには、次のコマンドを入力します。

```
(Cisco Controller) >show wlan summary
```

不要な WLAN を無効にするには、次のコマンドを入力します。

```
(Cisco Controller) >config wlan disable wlan-id
```

クライアント帯域選択

帯域選択によって、デュアルバンド（2.4 GHz および 5 GHz）動作が可能なクライアントの無線を、混雑の少ない 5 GHz AP に移動できます。 2.4 GHz 帯域は、混雑していることがよくあります。 2.4 GHz 帯域のクライアントは、Bluetooth デバイス、電子レンジ、およびコードレス電話機からの干渉を受けるだけでなく、他の AP からの同一チャネル干渉も受けます。これは、802.11b/g では、重複しないチャネルが 3 つに制限されるためです。 これらの干渉源を回避して、ネットワーク全体のパフォーマンスを向上させるために、コントローラで帯域選択を設定できます。

帯域選択は、デフォルトではグローバルに有効または無効になっています。 帯域選択のしくみは、クライアントへのプローブ応答を規制するというものです。 5 GHz チャネルへクライアントを誘導するために、2.4 GHz チャネルでのクライアントへのプローブ応答を遅らせます。

音声の帯域選択を評価する場合は、特にローミングのパフォーマンスに焦点を当ててください。 AP の 5 GHz 信号が 2.4 GHz 信号と同じかより強い場合、最近のほとんどのモデルのクライアントでは、デフォルトで 5 GHz を優先します。

高密度設計では、帯域選択を有効にする必要があります。 また、高密度設計では、使用可能な UNII-2 チャネルを調査する必要があります。 レーダーによる影響を受けず、クライアントベースで使用可能なチャネルは、RRM DCA リストに使用可能チャネルとして追加する必要があります。

デュアルバンドローミングは、クライアントによっては低速になる可能性があります。 大部分の音声クライアントの基本部分でローミング動作が低速な場合は、それらのクライアントが 2.4 GHz に留まっている可能性が高くなります。 この場合、5 GHz でスキャンの問題が発生しています。 一般に、クライアントがローミングすることを決定した場合、現在のチャネルと帯域を最初にスキャンします。 クライアントでは、通常信号レベルがより高い（およそ 20 dB 程度、またはより高い SNR、あるいはその両方の）AP があるか確認するためにスキャンします。 そのような接続が使用できない場合、クライアントは現在の AP にとどまる可能性があります。 この場合、2.4 GHz の CU が低く、コール品質が悪くない場合、選択した帯域を無効にする方が良い場合があります。 ただし、推奨の設計は、すべてのデータ レートを有効にし、6 Mbps を必須にして、5 GHz で帯域選択を有効にすることです。 この後、5 GHz RRM の最小 Tx 電力レベルを、RRM によって設定される 2.4 GHz の平均電力レベルよりも 6 dBm 高く設定します。

この推奨設定の目的は、クライアントで、SNR と Tx 電力がより良好な帯域とチャネルを最初に獲得できるようにすることです。 一般に、クライアントがローミングすることを決定した場合、現在のチャネルと帯域を最初にスキャンします。 このため、クライアントが最初に 5 GHz 帯域に参加した場合、5 GHz の電力レベルが良好であれば、その帯域にとどまる可能性が高くなります。 5 GHz の SNR レベルは、通常 2.4 GHz よりも高くなります。これは、2.4 GHz には Wi-Fi チャネルが 3 つしかなく、Bluetooth、iBeacon、電子レンジなどの信号の干渉の影響を受けやすいためです。

デュアルバンド レポーティングでは、802.11k を有効にすることを推奨します。 これにより、すべての 11k 対応クライアントが、経由ローミングのメリットを享受できます。 デュアルバンド レポーティングを有効にすると、クライアントでは、クライアントから指示された要求時に、最良の 2.4 GHz および 5 GHz AP のリストを受け取ります。 ここで、クライアントは、ほとんどの場合同じチャネル上の上位 AP のリストをチェックし、その後クライアントが現在使用している帯域と同じ帯域上の上位 AP のリストをチェックします。 このロジックにより、スキャン時間が短縮され、バッテリーの電力が節約されます。 WLC で 802.11k を有効にしても、802.11k 以外のクライアントに悪影響を与えません。

[クライアント帯域選択（Client Bandselect）] は、デフォルトでは有効になっています。 [クライアント帯域選択（Client Bandselect）] が無効になっている場合、[デフォルトの復元（Restore Default）] をクリックして [クライアント帯域選択（Client Bandselect）] を有効にします。

ステータス：

- 選択済み：すべての WLAN で有効になっています。
- 未選択：無効になっています。

CLI のオプション：

帯域選択を確認するには、次のコマンドを入力します。
```
(Cisco Controller) >show band-select
```

WLAN で帯域選択を有効にするには、次のコマンドを入力します。
```
(Cisco Controller) >config wlan band-select allow enable wlan-id
```

自動動的チャネル割り当て

[自動動的チャネル割り当て（Auto Dynamic Channel Assignment）]（DCA） は、RRM を許可し、無線ごとに適したチャネルを選択するために有効にする必要があります。

ワイヤレス ネットワークが初期化される際、参加するすべての無線で、干渉なしで動作するためにチャネルの割り当てが必要になります。これは、チャネルの割り当てを最適化して、干渉のない運用を可能にして行います。ワイヤレスネットワークでは、このチャネルの割り当てを、各無線によってできる限り多くのチャネルについて報告された電波メトリックを使用して、チャネルの帯域幅を最大化し、すべての原因（当該ネットワーク（信号）、他のネットワーク（外部干渉）、ノイズ（その他すべて））からの RF 干渉を最小化する解決策を提供して行います。

DCA はデフォルトで有効になっており、対象のネットワークに予定しているチャネルにグローバルな解決策を提供します。 これが無効になっている場合、[デフォルトの復元（Restore Default）] をクリックして ADS を有効にします。

ステータス：

- 選択済み：DCA が 802.11a/b で有効になっています。
- 未選択：DCA が無効になっているか、または 1 つの DCA が有効になっています。

CLI のオプション：

自動 DCA を有効にするには、次のコマンドを入力します。
```
(Cisco Controller) >config 802.11a channel global auto
(Cisco Controller) >config 802.11b channel global auto
```

自動伝送パワー コントロール

[自動伝送パワー コントロール（Auto Transmit Power Control）]（TPC）は、RRM で無線ごとに最適な送信電力を選択できるようにするために有効にします。 コントローラでは、リアルタイムの無線 LAN 状況に基づいて、アクセス ポイントの送信電力を動的に制御します。 TPCv1 および TPCv2 の 2 つのバージョンの送信電力制御から選択できます。 TPCv1 では、電力を低く維持することでキャパシティを増やし、干渉を減らすことができます。 TPCv2 では、干渉を最小にするために、送信電力を動的に調整します。 TPCv2 は、高密度のネットワークに適しています。 このモードでは、ローミングの遅延およびカバレッジ ホールのインシデントが多く発生する可能性があります。

送信電力制御（TPC）アルゴリズムでは、RF 環境での変化に応じてアクセス ポイント（AP）の電力を増やしたり減らしたりします。 ほとんどの場合、TPC では干渉を低減するために AP の電力を減らそうとします。 ただし、RF カバレッジに急激な変化が生じた場合（たとえば、AP で障害が発生したり、AP が無効になったりした場合）、TPC では周囲の AP の電力を増やす可能性もあります。この機能は、主にクライアントに関係するカバレッジホールの検出とは異なります。

TPC では AP 間のチャネルの干渉を防止しながら、必要なカバレッジ レベルを達成するために、十分な RF 電力を供給します。

（注） 最適なパフォーマンスを得るには、無線ごとに最適な送信電力を許可するための [自動（Automatic）] 設定を使用します。 [自動送信電力（Auto Transmit power）] は無線でデフォルトで有効になっています。 これが無効になっている場合、[デフォルトの復元（Restore Default）] をクリックして有効にします。

ステータス：

- 選択済み：TPC が 802.11a/b で有効になっています。
- 未選択：無効になっているか、または 1 つが有効になっています。

CLI のオプション：

自動 TPC を有効にするには、次のコマンドを入力します。

```
(Cisco Controller) >config 802.11a txPower global auto
(Cisco Controller) >config 802.11b txPower global auto
```

自動カバレッジホール検出

コントローラでは、AP から報告されたクライアントの信号レベルの品質を使用して、AP の電力レベルを増やす必要があるかどうかを判断します。 カバレッジ ホールの検出（CHD）はコントローラに依存しないため、RF グループ リーダーはこれらの計算に関与しません。 コントローラでは、特定の AP に関連付けられているクライアント数、およびクライアントごとの信号対雑音比（SNR）の値を明らかにします。

クライアントの SNR 値がコントローラに設定されたしきい値を下回った場合、AP ではクライアントを補うためにその電力レベルを増やします。 SNR のしきい値は、AP の送信電力とコントローラのカバレッジ プロファイル設定に基づいて設定されます。

自動 CHD を設定する方法の詳細については、『*Cisco Wireless LAN Controller Configuration Guide*』を参照してください。

Auto CHD は、デフォルトでは有効になっています。 これが無効になっている場合、[デフォルトの復元（Restore Default）] をクリックして有効にします。

ステータス：

- 選択済み：CHD が有効になっています。
- 未選択：無効になっているか、または 1 つが有効になっています。

CleanAir

RF 干渉を効果的に検出して緩和するために、必要な場合は必ず [CleanAir] を有効にする必要があります。 汎用の DECT 電話、電波妨害装置など、セキュリティ アラートをトリガーするさまざまな干渉源に対する推奨事項があります。

[CleanAir] は、デフォルトで有効になっています。 これが無効になっている場合、[デフォルトの復元（Restore Default）] をクリックして有効にします。

ステータス：

- 選択済み：有効になっています。
- 未選択：無効になっています。

CLI のオプション：

ネットワークの CleanAir の設定を確認するには、次のコマンドを入力します。

```
(Cisco Controller) >show 802.11{a|b} cleanair config
```

ネットワークで CleanAir 機能を有効にするには、次のコマンドを入力します。

```
(Cisco Controller) >config 802.11{a|b} cleanair enable network
```

特に電波妨害装置による干渉の検出を有効にするように設定するには、次のコマンドを入力します。

```
(Cisco Controller) >config 802.11{a|b} cleanair device enable jammer
```

イベント駆動型無線リソース管理

Y：自然発生的な干渉は、ネットワーク上に突然発生する干渉であり、特定のチャネルまたは特定の範囲のチャネルが完全にブロックされる可能性があります。 Cisco CleanAir のスペクトル イベント駆動型無線リソース管理機能を使用すると、電波品質（AQ）に対してしきい値を設定できます。このしきい値を超えた場合、影響を受けたアクセス ポイントに対してチャネル変更がただちにトリガーされます。 ほとんどの RF 管理システムでは干渉を回避できますが、この情報がシステム全体に伝搬するには時間を要します。 Cisco CleanAir では AQ 測定値を使用してスペクトルを連続的に評価しているため、措置を 30 秒以内にトリガーできます。 たとえば、アクセス ポイントでビデオ カメラからの干渉を検出した場合、そのカメラが動作し始めてから 30 秒以内のチャネル変更によってアクセス ポイントを回復させることができます。 Cisco CleanAir では干渉源の識別と位置の特定も行うため、後でそのデバイスの永続的なさらなる緩和措置も実行できます。

イベント駆動型 RRM は、デフォルトでは有効になっています。 これが無効になっている場合、[デフォルトの復元（Restore Default）] をクリックして有効にします。

ステータス：

- 選択済み：有効になっています。
- 未選択：無効になっています。