



## ワイヤレス モビリティの使用

- モビリティとは
- 新しいモビリティ
- Mobility Work Center
- モビリティ ドメインの作成
- モビリティ アンカー

### モビリティとは

モビリティ (ローミング) とは、安全かつ最小限の遅延で、あるアクセス ポイントから別のアクセス ポイントへアソシエーションをシームレスに維持するワイヤレス クライアントの機能です。より柔軟なローミングを可能にし、トラフィックのトンネル カプセル化の必要性を最小限にするために、Cisco Prime Infrastructure は、ネットワーク デバイス全体にモビリティ機能を提供する堅固なモビリティ アーキテクチャを用意しています。

モビリティ アーキテクチャの主要要素は次のとおりです。

- モビリティ コントローラ (MC) : MC (Cisco 5700 シリーズ ワイヤレス コントローラなど) は 1 つ以上の MA またはスイッチ ピア グループを受け持ち、その制御範囲内でのローミングと、MA 間または MC 間 (または MA と MC 間) を移動するトラフィックを処理します。
- モビリティ エージェント (MA) : MA (Catalyst 3650 や Catalyst 3850 スイッチなど) は、WAP が直接接続されるアクセス スイッチまたはエッジ スイッチに配置され、WAP との通信用 CAPWAP トンネルの終端となります。
- モビリティ オラクル (MO) : MO は大規模展開において複数の MC またはモビリティ サブドメインを接続する最上位のコントロール エンティティであり、非常に大きな物理領域でのローミングを可能にします。
- モビリティ ドメイン (ローミング ドメイン) : モバイル ユーザは、このドメイン (WAP とそれに関連するすべての制御エンティティ) のデバイス全体をローミングできます。通常、これには MA と MC が含まれますが、MO が含まれる場合もあります (複数のサブドメインを結合するため)。
- モビリティ サブドメイン : WAP とそれに関連する複数の MA および 1 つの MC。大規模なモビリティ ドメインの一部を担います (複数のサブドメイン間のローミングは MO によって調整されます)。

- **スイッチ ピア グループ (SPG)**: スwitchのグループ (MA として機能)。SPG は、グループ メンバー間にフル メッシュのモビリティ トンネルを確立し、グループ内のスイッチに関連する WAP 全体にわたって効率的なローミングをサポートします。また、SPG は、ハンドオフ中のスイッチ間のインタラクションの範囲を制限するためにも使用されます。SPG はモビリティ コントローラによって設定され、スイッチ ピア グループ内のすべてのスイッチがメンバーシップに対して同一のビューを持ちます。SPG 内のスイッチは、一連のダイレクト トンネルによって相互接続される場合もあります。同じスイッチ ピア グループ内であるスイッチから別のスイッチにステーションがローミングする際に、Point of Presence が元のスイッチまたはアンカー スwitchにとどまる場合は、MTE を使用せずに、トラフィックを直接トンネリングしてアンカー スwitchに戻すことができます。この直接トンネリング メカニズムはデータ パスの最適化であり、オプションです。
- **モビリティ グループ**: モビリティ グループは一連の MC (および関連する MA/スイッチ ピア グループ) です。
- **モビリティ トンネル エンドポイント**: モビリティ トンネル エンドポイント (MTE) は、トンネリングを使用してモバイル デバイスにデータ プレーン サービスを提供します。これにより、ネットワーク上のユーザの Point of Presence を一定に保ち、ローミング イベントのネットワークへの影響を最小化します。ローミング対象のクライアントの VLAN またはサブネットを MTE で使用可能な場合、MTE は Point of Presence となることができます。使用できない場合、MTE は単なるトンネル スwitchング エンティティとして機能し、Point of Presence であるアクセス スwitchまたは MTE にローミング対象のクライアントを接続します。

#### 関連項目

- [Mobility Work Center](#)
- [モビリティ ドメインの作成](#)

## 新しいモビリティ

階層型モビリティは、ワイヤレス LAN コントローラ構成において新しいモビリティと呼ばれます。Prime Infrastructure 2.0 は、Cisco WLC 7.6 を実行している Cisco 5508 と WiSM2 プラットフォームに新しいモビリティ機能を提供します。

Prime Infrastructure の新しいモビリティ機能の主要機能は、次のとおりです。

- **Mobility Work Center** は、Cisco WLC 7.6 を実行している Cisco 5508 と WiSM 2 プラットフォームを検出し、階層型モビリティ アーキテクチャの構築に必要な操作を提供します。このアーキテクチャには、2 つのデバイス タイプ (Cisco 5508 と WiSM2) とモビリティ エージェントとして展開されている Cisco 3650/3850 が含まれます。
- 階層型モビリティ アーキテクチャを展開する際に、LifeCycle ビューを使用して、WLAN、VLAN、セキュリティ、ゲスト アンカーなどの無線機能を Cisco 5508 と WiSM2 に設定できます。
- Cisco 5508 および WiSM2 でのプラットフォーム モビリティ アーキテクチャの展開は、クラシックビューでのみサポートされ、ワイヤレス設定全体はクラシックおよび LifeCycle ビューのままになります。
- Infrastructure 2.0 の場合、IOS ベースのデバイス (3850 と 5760) では、一部の無線機能 (VLAN インターフェイスの作成など) は引き続き CLI テンプレートを使用して設定されます。

新しいモビリティ機能の詳細については、次の URL にあるリリース ノート『Cisco Wireless LAN Controllers and Lightweight Access Points for Release 7.3.112.0』の「Hierarchical Mobility (New Mobility)」を参照してください。

[http://www.cisco.com/c/en/us/td/docs/wireless/controller/release/notes/crn7\\_3\\_112\\_0.html#wp1054557](http://www.cisco.com/c/en/us/td/docs/wireless/controller/release/notes/crn7_3_112_0.html#wp1054557)

# Mobility Work Center

Mobility Work Center を使用するには、[サービス (Services)] > [モビリティ サービス (Mobility Services)] > [モビリティ ドメイン (Mobility Domains)] を選択します。

次の情報が表示されます。

- [デバイス名 (Device Name)]: MC の名前。
- [管理 IP (Management IP)]: MC の管理 IP アドレス。
- [ワイヤレス インターフェイス IP (Wireless Interface IP)]: モビリティ プロトコルで使用される MC の IP アドレス。
- [モビリティ グループ (Mobility Group)]: MC が属しているモビリティ グループの名前。
- [モビリティ ロール (Mobility Role)]: 管理および動作のモビリティ モードを表示します。[管理 (Admin)] と [運用 (Operational)] の値が異なる場合は、管理モードを有効にするためにデバイスを再起動する必要があります。モビリティ オラクルが有効な場合は、モビリティ モードに加えて MO が表示されます。

このページでは、次のタスクを実行できます。

- モビリティ ドメインの作成: [モビリティ ドメインの作成](#)を参照してください。
- スイッチ ピア グループの作成: MC にスイッチ ピア グループを作成します。
- モビリティ ロールの変更: MA から MC にコントローラを変更します。
- ドメインの削除: ドメインのみを削除します。コントローラは Prime Infrastructure から削除されません。
- メンバーの削除: 選択したドメインから選択した MC を削除します。
- モビリティ オラクルとして設定: 選択した MC をドメイン全体の MO として動作させる場合は、その MC で MO を有効にします。ドメインごとに 1 つの MO のみが存在できます。Cisco 5760 シリーズのコントローラのみが MO 機能をサポートしています。
- スイッチ ピア グループへのメンバーの追加: スイッチ ピア グループにメンバーを追加します。
- スイッチ ピア グループからのメンバーの削除: スイッチ ピア グループからメンバーを削除します。



(注)

デフォルトでは、[Mobility Work Center] ページには、管理対象ネットワークに設定されているすべてのモビリティ ドメインが表示されます。モバイル デバイスのリストを表示するには、左側のサイドバーから [すべてのモビリティ デバイス (All Mobility Devices)] を選択します。

## 関連項目

- [モビリティとは](#)
- [モビリティ ドメインの作成](#)

## モビリティドメインの作成

モビリティドメインは互いの IP アドレスが設定されたコントローラの集合であり、クライアントはモビリティドメイン内のコントローラ間でローミングできます。

[Mobility Work Center] には、Prime Infrastructure によって管理対象ネットワーク内に設定されたすべてのモビリティドメインが表示されます。左側のサイドバーメニューには以下が表示されます。

- ドメイン
- 各ドメインの MC
- 各 MC 上の SPG
- 各 SPG 内の MA

左側のサイドバーメニューからノードを選択すると、右側のペインに詳細が表示されます。左側のサイドバーメニューからドメインノードを選択すると、右側のペインにドメイン内の MC が表示されます。

モビリティドメインを作成するには、次の手順を実行します。

- 
- ステップ 1 [サービス (Services)] > [モビリティ サービス (Mobility Services)] > [モビリティドメイン (Mobility Domains)] の順に選択します。
  - ステップ 2 左側のサイドバーメニューをクリックします。
  - ステップ 3 グループ化する一連の MC のモビリティドメインの名前を入力します。  
選択した MC が別のドメインに存在している場合、MC はそのドメインから削除され、新しいドメインに追加されます。
  - ステップ 4 モビリティドメインのメンバーデバイスを選択します。  
デバイスは 1 つのドメインまたは SPG にのみ属することができます。
  - ステップ 5 [適用 (Apply)] をクリックします。
- 

## スイッチピアグループの作成

MC にはスイッチピアグループ (SPG) を含めることができ、スイッチピアグループには MA を含めることができます。管理対象ネットワークの MA は [スイッチピアグループ (Switch Peer Group)] ページに表示されます。すでに存在しているスイッチピアグループを作成すると、古いスイッチピアグループから新しいスイッチピアグループに MC が移動され、すべての MA に MC ワイヤレスインターフェイスの IP アドレスが設定されます。

スイッチピアグループを作成するには、次の手順を実行します。

- 
- ステップ 1 [サービス (Services)] > [モビリティ サービス (Mobility Services)] > [モビリティドメイン (Mobility Domains)] の順に選択します。
  - ステップ 2 左側のサイドバーから MC を選択します。
  - ステップ 3 [スイッチピアグループの作成 (Create Switch Peer Group)] をクリックします。

- ステップ 4** 選択した MC でグループ化する、一連の MA を含めるスイッチ ピア グループの名前を入力します。
- 選択した MA が別のスイッチ ピア グループに存在している場合、MA はそのグループから削除され、新しいグループ追加されます。MC に複数のスイッチ ピア グループを作成できます。
- ステップ 5** モビリティ エージェントを選択します。
- デバイスは 1 つのドメインまたは SPG にのみ属することができます。
- ステップ 6** [適用(Apply)] をクリックします。
- 作成した SPG が左側のサイド バーに表示されます。そこに移動して、選択したスイッチ ピア グループのモビリティ エージェントを表示できます。

## モビリティ ロールの変更

デフォルトでは、Cisco 3850 コントローラは MA として動作します。ネットワークで MC が必要な場合は、これらのコントローラを MC に変換できます。

モビリティ ロールを変更するには、次の手順を実行します。

- ステップ 1** [サービス (Services)] > [モビリティ サービス (Mobility Services)] > [モビリティ ドメイン (Mobility Domains)] の順に選択します。
- ステップ 2** [すべてのモビリティ デバイス (All Mobility Devices)] を選択します。
- ステップ 3** 変更先のロールとデバイスを選択します。
- [モビリティ コントローラへのロールの変更 (Change Role To Mobility Controller)]: 選択したコントローラでモビリティ コントローラ機能を有効にします。
  - [モビリティ エージェントへのロールの変更 (Change Role To Mobility Agent)]: 選択したコントローラでモビリティ エージェント機能を有効にします。これを実行すると、MC 機能が無効化されます。
- MA から MC (またその逆) への変換は、3850 デバイスでのみ行うことができます。ロールの変更を有効にするには、デバイスを再起動する必要があります。
- [モビリティ グループの割り当て (Assign Mobility Group)]: 選択したデバイスの新しいモビリティ グループ名を入力します。
- ステップ 4** [適用(Apply)] をクリックします。

## モビリティ アンカー

モビリティ アンカーは、WLAN のアンカー コントローラとして指定されたモビリティ グループのサブセットです。この機能を使用すると、クライアントのネットワーク エントリ ポイントに関係なく、WLAN を 1 つのサブネットに制限できます。これにより、ユーザは企業全体のパブリック WLAN やゲスト WLAN にアクセスできますが、引き続き特定のサブネットに制限されません。また、WLAN は建物の特定のセクション (ロビー、レストランなど) を表すことができるため、ゲスト WLAN を使って地理的ロード バランシングを実現することもできます。

クライアントが WLAN のモビリティ アンカーとして事前設定されているモビリティ グループのコントローラに最初に関連付けると、クライアントはローカルでそのコントローラに関連付けし、クライアントのローカルセッションが作成されます。クライアントは、WLAN の事前設定されたアンカー コントローラにのみアンカーできます。指定された WLAN の場合、モビリティグループのすべてのコントローラ上で同じセットのアンカー コントローラを設定する必要があります。

クライアントが、WLAN のモビリティ アンカーとして設定されていないモビリティ グループのコントローラに最初に関連付けると、クライアントはローカルでそのコントローラに関連付けし、ローカルセッションがクライアントのために作成され、コントローラは同じモビリティグループの別のコントローラへ通知されます。その通知に対する回答がない場合、コントローラは WLAN に設定されたいずれかのアンカー コントローラに連絡をとり、ローカルスイッチ上のクライアントに対する外部セッションを作成します。クライアントからのパケットは EtherIP を使用してモビリティ トンネルを介してカプセル化され、アンカー コントローラに送信されます。ここでカプセル化が解除されて有線ネットワークへ配信されます。クライアントへのパケットは、アンカー コントローラで受信され、EtherIP を使用してモビリティ トンネルを介して外部コントローラへ転送されます。外部コントローラはパケットのカプセル化を解除し、クライアントへ転送します。

## WLAN のゲスト アンカー コントローラの設定

ゲストアンカー コントローラはゲスト トラフィック専用のコントローラであり、非武装地帯 (DMZ) とも呼ばれる非保護ネットワーク領域に配置されます。トラフィック発信元の他の内部 WLAN コントローラは、エンタープライズ LAN に配置されます。



(注) Cisco 5760 コントローラはゲストアンカーとして指定できますが、Catalyst 3850 スイッチはゲストアンカーとして指定できません。ただし、外部コントローラとして指定できます。

ロード バランシングのために WLAN のモビリティ アンカーとしてゲスト コントローラを設定できます。

### はじめる前に

- Prime Infrastructure でワイヤレス デバイスが設定されていることを確認します。ワイヤレス デバイスの設定方法については、「[無線機能の設定](#)」を参照してください。
- WLAN のモビリティ アンカーとして設定するワイヤレス デバイスが、同じモビリティ ドメイン内にあることを確認します。

WLAN のゲストアンカー コントローラを設定するには、次の手順を実行します。

- 
- ステップ 1 [インベントリ (Inventory)] > [デバイス管理 (Device Management)] > [ネットワーク デバイス (Network Devices)] を選択します。
  - ステップ 2 [デバイス グループ (Device Group)] 領域で、[デバイス タイプ (Device Type)] を展開し、次に [ワイヤレス コントローラ (Wireless Controller)] を展開します。
  - ステップ 3 ゲスト モビリティ アンカーとして指定するコントローラを選択します。デバイスの詳細が、ページの下部に表示されます。
  - ステップ 4 [設定 (Configuration)] タブをクリックします。
  - ステップ 5 左側のサイドバーのメニューから、[WLANs] > [WLAN 設定 (WLAN Configuration)] の順に選択します。[WLAN コンフィギュレーション (WLAN Configuration)] ページが表示されます。



(注) クラシック ビューを使用している場合は、[設定 (Configure)] > [コントローラ (Controllers)] > [コントローラの IP アドレス (Ctrl IP addr)] > [WLANs] > [WLAN コンフィギュレーション (WLAN Configuration)] の順に選択して、[WLAN コンフィギュレーション (WLAN Configuration)] 詳細ページにアクセスします。

ステップ 6 必要な WLAN ID の URL を選択します。タブ付きのページが表示されます。

ステップ 7 [詳細 (Advanced)] タブをクリックし、ページ下部にある [モビリティ アンカー (Mobility Anchors)] リンクをクリックします。[モビリティ アンカー (Mobility Anchors)] ページが表示されます。



(注) また、[WLAN コンフィギュレーション (WLAN Configuration)] ページから [モビリティ アンカー (Mobility Anchors)] ページにアクセスすることもできます。目的の WLAN ID のチェックボックスをオンにします。[コマンドの選択 (Select a command)] ドロップダウンリストから、[モビリティ アンカー (Mobility Anchors)] を選択し、[移動 (Go)] をクリックします。[モビリティ アンカー (Mobility Anchors)] ページが表示されます。

ステップ 8 モビリティ アンカーとして指定するコントローラの [IP アドレス (IP address)] チェックボックスをオンにして、[保存 (Save)] をクリックします。

## Spectrum Expert の設定

Spectrum Expert クライアントは、リモート干渉センサーとして機能し、動的な干渉データを Prime Infrastructure に送信します。この機能により、Prime Infrastructure はネットワーク内の Spectrum Expert から詳細な干渉データを収集、モニタ、およびアーカイブできます。

Spectrum Expert を設定するには、[サービス (Services)] > [モビリティ サービス (Mobility Services)] > [Spectrum Expert (Spectrum Experts)] の順に選択します。このページには、次の項目を含むすべての Spectrum Expert の一覧が表示されます。

- [ホスト名 (Hostname)]: Spectrum Expert ラップトップのホスト名または IP アドレス。
- [MAC アドレス (MAC Address)]: ラップトップのスペクトラム センサー カードの MAC アドレス。
- [到達可能性ステータス (Reachability Status)]: Spectrum Expert が正常に稼働し、情報を Prime Infrastructure に送信しているかどうかを指定します。ステータスは、[到達可能 (Reachable)] または [到達不能 (Unreachable)] と表示されます。
- [Spectrum Experts の概要の表示 \(45-8 ページ\)](#)
- [Spectrum Experts の概要の表示 \(45-8 ページ\)](#)

## Spectrum Expert の追加

Spectrum Expert を追加するには、次の手順を実行します。

- 
- ステップ 1 [サービス (Services)] > [モビリティ サービス (Mobility Services)] > [Spectrum Expert (Spectrum Experts)] の順に選択します。
- ステップ 2 [コマンドの選択 (Select a command)] ドロップダウン リストから、[Spectrum Expert の追加 (Add Spectrum Expert)] を選択します。このリンクは、Spectrum Expert が 1 つも追加されていない場合にのみ表示されます。[コマンドの選択 (Select a command)] ドロップダウン リストから [Spectrum Expert の追加 (Add a Spectrum Expert)] を選択しても、[Spectrum Expert の追加 (Add a Spectrum Expert)] ページにアクセスできます。
- ステップ 3 Spectrum Expert のホスト名または IP アドレスを入力します。ホスト名を使用する場合、Spectrum Expert を Prime Infrastructure に追加するには DNS に登録する必要があります。
- Spectrum Expert として正しく追加するには、Spectrum Expert クライアントが稼働しており、Prime Infrastructure に通信するように設定されていなければなりません。
- 

## Spectrum Experts の概要の表示

[Spectrum Experts] ページには、システムに追加されている Spectrum Expert のテーブルが表示されます。このテーブルには、次の Spectrum Expert の情報が記載されています。

[ホスト名 (Hostname)]: ホスト名または IP アドレス。

[アクティブな干渉源 (Active Interferers)]: Spectrum Expert により検出された現在の干渉源の数。

[アラーム AP (Alarms APs)]: 検出された干渉源が潜在的な影響を及ぼしていると Spectrum Expert により確認されたアクセス ポイントの数。

[アラーム (Alarms)]: Spectrum Expert から送信されたアクティブな干渉トラップの数。クリックすると、この Spectrum Expert のアクティブ アラームに対してフィルタリングされている [アラーム (Alarm)] ページへアクセスします。

[到達可能性ステータス (Reachability Status)]: Spectrum Expert が稼働しており、データを Prime Infrastructure に送信している場合は、緑色で [到達可能 (Reachable)] と表示されます。それ以外の場合は、[到達不能 (Unreachable)] と赤で表示されます。

[場所 (Location)]: Spectrum Expert が無線クライアントの場合、場所へのリンクが使用できます。それによって、Spectrum Expert の場所が有効範囲を示す赤いボックス付きで表示されます。

## [干渉源の概要 (Interferers Summary)] の表示

[干渉源 - SE (Interferers-SEs)] ページには、30 日間隔で検出されたすべての干渉源の一覧が表示されます。このテーブルには、次のような干渉源の情報が記載されています。

- [干渉源 ID (Interferer ID)]: 異なる Spectrum Expert 間で一意の ID。これは、疑似乱数によって生成される ID です。MAC アドレスに似ていますが、実際のアドレスではなく、干渉デバイスの検出に使用できます。
- [カテゴリ (Category)]: 干渉源のカテゴリ。カテゴリには、[Bluetooth]、[コードレス電話 (cordless phones)]、[電子レンジ (microwave ovens)]、[802.11 FH]、[その他一般: 周波数ホッピング (generic: frequency-hopped)]、[その他一般: 連続 (generic: continuous)]、および [アナログビデオ (analog video)] があります。



- [タイプ(Type)]:[アクティブ(Active)] は、干渉源が現在 Spectrum Expert で検出されていることを示します。[非アクティブ(Inactive)] は、干渉源が検出されなくなったこと、または Prime Infrastructure が到達できる干渉源はなくなったと Spectrum Expert が確認したことを示します。
- [検出時刻(Discover Time)]: 干渉源が発見された時刻を示します。
- [影響を受けるチャンネル(Affected Channels)]: 影響を受けるチャンネルを示します。
- [影響を受ける AP の数(Number of APs Affected)]: Spectrum Expert が検出した Prime Infrastructure により管理されるアクセス ポイントの数、または Spectrum Expert がアクセス ポイントのチャンネル上で検出した干渉源の数。アクティブな干渉源のみが表示されます。次の条件のすべてが適合する場合、そのアクセス ポイントには [影響を受ける(affected)] とラベルが付けられます。
  - アクセス ポイントが Prime Infrastructure で管理されている。
  - Spectrum Expert がアクセス ポイントを検出している。
  - Spectrum Expert がアクセス ポイントの稼働チャンネル上の干渉源を検出している。
- [電力(Power)]: dBm で示されます。
- [デューティ サイクル(Duty Cycle)]: パーセントで示されます。100 % は最低値です。
- [重大度(Severity)]: 干渉源の重大度ランキングを示します。100 は最低値、0 は干渉がないことを表しています。

## Spectrum Experts の詳細の表示

[Spectrum Expert] ページには、単一の Spectrum Expert からの干渉の詳細がすべて表示されます。このページは 20 秒ごとに更新され、リアルタイムにリモートの Spectrum Expert を確認できます。このページに表示される項目は、次のとおりです。

- [干渉源の合計数(Total Interferer Count)]: 特定の Spectrum Expert から取得されます。
- [アクティブな干渉源の数のチャート(Active Interferers Count Chart)]: 干渉源をカテゴリごとにグループ化した円グラフを表示します。
- [チャンネルあたりのアクティブな干渉源の数(Active Interferer Count Per Channel)]: 異なるチャンネル上の干渉源をカテゴリごとにグループ化して干渉源の数を表示します。
- [AP リスト(AP List)]: Spectrum Expert によって検出されたアクセス ポイントの一覧を表示します。これらのアクセス ポイントは、アクティブな干渉源が検出されたチャンネル上にあります。
- [影響を受けるクライアントのリスト(Affected Clients List)]: アクセス ポイントに現在認証されているクライアントの一覧を表示します。外部認証を行う場合は、[セキュリティ(Security)] > [AAA] ページで特定の RADIUS サーバまたは LDAP サーバを選択できます。

## wIPS プロファイルの作成

Prime Infrastructure にはいくつかの定義済みプロファイルが用意されており、そこから選択できます。これらのプロファイル(カスタマー タイプ、ビルディング タイプ、業界タイプなどに基づきます)を使用すると、Cisco Adaptive wIPS を通じて使用可能な追加のワイヤレスの脅威保護をすばやくアクティブにできます。プロファイルは「そのまま」使用することも、要件に合わせてカスタマイズすることもできます。

定義済みプロファイルには次のものがあります。

- [教育 (Education)]
- [EnterpriseBest]
- [EnterpriseRogue]
- [金融 (Financial)]
- [医療 (HealthCare)]
- [HotSpotOpen]
- [Hotspot8021x]
- [軍 (Military)]
- [小売 (Retail)]
- [トレードショー (Tradeshaw)]
- [ウェアハウス (Warehouse)]




[wIPS プロファイル (wIPS Profiles)] > [プロファイル リスト (Profile List)] ページでは、現在の wIPS プロファイルの表示、編集、適用、削除を行ったり、新しいプロファイルを追加したりできます。[プロファイル リスト (Profile List)] には、各プロファイルの次の情報が表示されます。

- [プロファイル名 (Profile Name)]: 現在のプロファイルのユーザ定義名を示します。プロファイルの詳細を表示または編集するには、プロファイル名をクリックします。  
マウス カーソルをプロファイル名に移動すると、プロファイル ID とバージョンが表示されます。
- [適用されている MSE (MSE(s) Applied To)]: このプロファイルが適用されている Mobility Services Engine (MSE) の数を示します。MSE 数をクリックすると、プロファイルの割り当ての詳細が表示されます。
- [適用されているコントローラ (Controller(s) Applied To)]: このプロファイルが適用されているコントローラの数を示します。コントローラ数をクリックすると、プロファイルの割り当ての詳細が表示されます。

wIPS プロファイルを作成するには、次の手順を実行します。

- 
- ステップ 1 [サービス (Services)] > [モビリティ サービス (Mobility Services)] > [wIPS プロファイル (wIPS Profiles)] の順に選択します。
  - ステップ 2 [コマンドの選択 (Select a command)] ドロップダウン リストから、[プロファイルの追加 (Add Profile)] を選択し、[移動 (Go)] をクリックします。
  - ステップ 3 [プロファイル パラメータ (Profile Parameters)] ページの [プロファイル名 (Profile Name)] テキスト ボックスにプロファイル名を入力します。
  - ステップ 4 ドロップダウン リストから該当する定義済みのプロファイルを選択するか、[デフォルト (Default)] を選択します。
  - ステップ 5 [保存 (Save)] > [次へ (Next)] を選択します。

[保存 (Save)] を選択すると、Mobility Services Engine またはコントローラの割り当てや変更なしで、プロファイルが Prime Infrastructure データベースに保存されます。プロファイルはプロファイル リストに表示されます。

- ステップ 6** 既存グループを編集または削除したり、新しいグループを追加するには、次の手順を実行します。
- a. [SSID グループ リスト (SSID Group List)] ページの [コマンドの選択 (Select a command)] ドロップダウン リストから、[グループの追加 (Add Group)] または [グローバル リストからグループを追加 (Add Groups from Global List)] を選択し、[移動 (Go)] をクリックします。
  - b. グループ名と 1 つ以上の SSID グループを入力し、[保存 (Save)] をクリックします。
- ステップ 7** 現在のプロファイルに含めるポリシーを指定するには、[プロファイル コンフィギュレーション (Profile Configuration)] を選択します。ポリシー ツリーのチェックボックス (左側の [ポリシーの選択 (Select Policy)] ペインにあります) は、現在のプロファイルで有効または無効になっているポリシーを示します。このページでは次の操作を実行できます。
- 該当するブランチまたはポリシーのチェックボックスをオン/オフすることで、ブランチ全体や個別のポリシーを有効化または無効化することができます。  
デフォルトでは、すべてのポリシーが選択されています。
  - ポリシーの説明を表示するには、個々のポリシーをクリックします。[ポリシー ルール (Policy Rules)] ページを使用して、現在のポリシー ルールの設定を追加、編集、削除、並べ替えることができます。
-  **(注)** 1 つ以上のポリシー ルールが存在する必要があります。リスト内に 1 つしかない場合、そのポリシー ルールは削除できません。
-  **(注)** プロファイルがコントローラに適用されている場合、そのプロファイルは削除できません。
- 次を設定します。
    - [しきい値 (Threshold)] (すべてのポリシーに適用されるわけではありません) : 選択したポリシーに関連付けられたしきい値または上限を示します。すべてのポリシーに 1 つ以上のしきい値が含まれている必要があるため、標準的なワイヤレス ネットワークの問題に基づいて、各ポリシーにデフォルトのしきい値が定義されています。しきい値オプションは、選択したポリシーに応じて異なります。  
ポリシーのしきい値に達すると、アラームがトリガーされます。Cisco Adaptive wIPS DoS およびセキュリティ ペネトレーション攻撃からのアラームは、セキュリティ アラームとして分類されます。これらの攻撃の要約は [セキュリティ サマリ (Security Summary)] ページに表示されます。このページにアクセスするには [モニタ (Monitor)] > [セキュリティ (Security)] を選択します。wIPS の攻撃は [脅威および攻撃 (Threats and Attacks)] セクションにあります。
    - [重大度 (Severity)] : 選択したポリシーの重大度を示します。パラメータとしては、[重大 (critical)]、[やや重大 (major)]、[情報 (info)]、および [警告 (warning)] があります。このフィールドの値は、ワイヤレス ネットワークに応じて変わります。
    - [通知 (Notification)] : しきい値に関連付けられた通知の種類を示します。
    - [ACL/SSID グループ (ACL/SSID Group)] : このしきい値が適用される ACL または SSID グループを示します。
-  **(注)** 選択されたグループのみポリシーをトリガーします。

**ステップ 8** プロファイル設定が完了したら、[次へ (Next)] を選択して [MSE/コントローラ (MSE/Controller)] ページに進みます。

**ステップ 9** [プロファイルの適用 (Apply Profile)] ページで、現在のプロファイルを適用する Mobility Services Engine とコントローラを選択し、[適用 (Apply)] をクリックして、選択した Mobility Services Engine/コントローラに現在のプロファイルを適用します。

また、プロファイル リストから直接プロファイルを適用することもできます。[プロファイル リスト (Profile List)] ページで、適用するプロファイルを選択し、[コマンドの選択 (Select a command)] ドロップダウン リストで [プロファイルの適用 (Apply Profile)] をクリックします。次に、[移動 (Go)] をクリックして [プロファイルの適用 (Apply Profile)] ページにアクセスします。

---