H3C iMC

WSM(ワイヤレスサービス管理)

管理者ガイド

New H3C Technologies Co.,Ltd.
http://www.h3c.com

ソフトウェアバージョン:IMC WSM 7.3(E0602)
ドキュメントバージョン:5W106-20190806

はじめに

『H3C IMC Wireless Service Manager Administrator Guide』には37の章があり、IMC WSMでのネットワークリソースの管理、一般的な設定手順、および重要なパラメーターについて説明しています。

ここでは、ドキュメントに関する次のトピックについて説明します。

- 対象読者
- 表記規則。
- ドキュメントに関するフィードバック。

対象読者

このマニュアルの対象読者は次のとおりです。

- ネットワークプランナー。
- フィールドテクニカルサポートおよびサービスエンジニア。
- H3C IMCで作業するネットワーク管理者。

表記規則

このセクションでは、マニュアルで使用されている表記規則について説明します。

例でのポート番号付け

マニュアルに記載されているポート番号は説明のためのものであり、デバイスで使用できない場合があります。

コマンドの表記法

規約	説明
太字	太字のテキストは、文字どおりに入力したコマンドとキーワードを表します。
斜体	斜体のテキストは、実際の値に置き換える引数を表します。
#	ポンド記号(#)で始まる行はコメントです。

GUIの規則

規約	説明
太字	ウィンドウ名、ボタン名、フィールド名およびメニュー項目は太字で示されています。たとえば、New Userウィンドウが表示されたら、OKをクリックします。
>	複数レベルのメニューは、山カッコで区切られます。たとえば、File > Create > folder

記号

規約	説明
△注意:	重要な情報に注意を喚起する警告であり、理解または従わないと、データの損失、データの破損、またはハードウェアやソフトウェアの損傷につながる可能性があります。
ⓘ重要:	重要な情報に注意を喚起する警告。
注:	追加または補足情報を含むアラート。

ドキュメントに関するフィードバック

製品ドキュメントに関するご意見は、info@h3c.comまで電子メールでお送りください。

ご意見をいただければ幸いです。

内容

Wireless Service Managerの概要

IMCプラットフォームをベースにしたWireless Service Manager(WSM)コンポーネントは、統合された有線および無線ネットワーク管理を実装するためのWLAN管理機能を提供します。WSMを使用すると、管理者は既存の有線ネットワーク管理システムに無線管理機能を追加できます。これにより、投資とメンテナンスのコストを節約できます。

WSMは、AC、FAT AP、FIT AP、およびクライアントの集中管理を提供します。WSMはまた、リソース管理およびワイヤレストポロジー管理機能も提供します。

他のIMCコンポーネントと連携することで、WSMは次の機能を提供します。

- パネル管理
- アラーム管理
- パフォーマンスの監視
- ソフトウェアのバージョン管理
- 構成ファイルの管理
- アクセスユーザー管理
- ユーザー認証管理機能

WSMは、SNMPを介してComwareベースのAC、FAT AP、およびFIT APを管理します。

より良いユーザー体験のために、IMCは、WSM機能を表示するために、異なるサービスおよびソリューションに対して異なるビューを提供致します。

デフォルトの画面

デフォルトの画面に入る手順は、次のとおりです:

1. **WSM Manager**にログインします。
2. トップナビゲーションバーの**Service**タブをクリックします。
3. 次のいずれかのタスクを実行します。
   - ナビゲーションツリーから、**WLAN Manager**を選択します。
   - **Value-Added Service Management**領域で、**WLAN Manager**をクリックします。このドキュメントでは、デフォルト画面でのWSM機能について説明します。

デスクトップビュー

デスクトップビューに入るには:

1. **WSM Manager**にログインします。
2. 次のいずれかのタスクを実行します。
   - IMCホームページの右上隅にある**Desktop**アイコン 

をクリックします。
   - IMCホームページの右上隅にある**View**リストから**Desktop View**を選択します。
3. デスクトップビューで、**Add application**をクリックします。

   必要に応じて、ワイヤレスアプリケーション管理をカスタマイズできます。デスクトップビューの詳細については、『H3C IMC v7.3 Enterprise and Standard Platform Administrator Guide』を参照してください。
4. デスクトップビューで、デスクトップの左にある**Start**アイコン 
をクリックするか、デスクトップを右クリックしてショートカットメニューから**Classic**を選択し、既定のパースペクティブに切り替えます。

WLAN Manage画面

WLAN Manager画面を開始するには、次の手順を実行します。

1. **WSM Manager**にログインします。
2. IMCホームページの右上隅にある**View**リストから**WLAN Manager Perspective**を選択します。
3. WLAN Managerパースペクティブで、右上隅にある**Switch Perspective**アイコン をクリックし、**Default Perspective**を選択してデフォルトのパースペクティブに切り替えます。

クイックサービスプロセス

クイックサービスプロセスに入る手順は、次のとおりです。

1. **WSM Manager**にログインします。
2. IMCホームページの右上隅にある**View**リストから**Quick Service Process**を選択します。
3. **Select Template Category**領域で、**WLAN Manager**を選択します。

   Quick Service Processについては、『H3C IMC v7.3 Enterprise and Standard Platform Administrator Guide』を参照してください。
4. クイックサービスプロセスで、右上隅にある**Default Perspective**をクリックしてデフォルトのパースペクティブに切り替えます。

WLANの迅速な導入

WSMを使用すると、WLANの基本設定とセキュリティ設定を1つのページで構成して、WLANを迅速に導入できます。

ワイヤレスリソース管理

WSMは、IMCで次のワイヤレスリソースを管理します。

- AC
- FAT AP
- FIT AP
- クライアント
- Radio
- WLAN
- APアクセスポート
- IoTモジュール

これらのワイヤレスリソースは、管理者によるリソースのメンテナンスを容易にします。WSMを使用すると、管理者は次のタスクを実行できます。

- 管理可能なすべてのComwareベースのワイヤレスデバイスに対して、さまざまなビューで、現在のデバイス情報の照会と表示、設定の同期、およびトポロジーロケーション、ping、ルートトレース、およびTelnet操作を実行します。
- クライアントビューで特定のクライアント情報を迅速にクエリー、表示およびエクスポートします。WSMを使用すると、管理者はクライアントオンライン履歴のクエリーと表示、クライアントローミング履歴の動的表示、およびWSMがUAMとコラボレーションするときのクライアント情報の同期化を行うことができます。
- 無線情報を照会および表示し、無線ビューのIMCで管理できるFAT APおよびFIT APのすべての

無線の無線パラメーターを変更します。

- 同じSSIDでワイヤレスサービスを提供するデバイスに関する情報を表示します。指定されたSSIDのFAT AP、FIT AP、およびクライアントに関する情報を表示します。WLANをバッチで変更および削除し、WLAN統計を表示します。
- IMC内のすべての管理可能なFAT AP、FIT AP、および不正APのアクセスポートに関する統計情報を収集します。APアクセスポートに関する情報を問い合せ、アクセスポートがPoEをサポートしているAPのPoE機能をイネーブルまたはディセーブルにします。
- IoTモジュールビューでIMCが管理するIoTモジュールをクエリーして表示する。

ワイヤレスサービスのアラーム

無線サービス警報機能は、IMCプラットフォームの警報機能をベースに実装されており、無線サービス警報は、オペレーターがネットワーク上の障害を迅速に検出して解決するのに役立ちます。

WSMがデプロイされると、IMCは次の機能を提供します。

- **Periodic polling**: ワイヤレスデバイスを定期的にポーリングしてその到達可能性をテストし、到達不能なデバイスに対してトラップを生成します。
- **Alarm**: **Alarm Management**モジュールのシステム定義およびユーザー定義のアラーム規則に従って、ACおよびFAT APから受信したトラップに基づいてアラームを生成します。
- **Syslog**: ACおよびFAT APからsyslogエントリーを受信し、システムおよびユーザー定義のアラーム規則に従って、syslogエントリーに基づいてアラームを生成します。
- **WLAN performance monitoring**: パフォーマンス管理モジュールでシステム定義のWLANパフォーマンスインデックスを提供し、WLANパフォーマンス監視用のユーザー定義のインデックスをサポートします。
- **Threshold settings**: WSMでのWLANパフォーマンスモニタリングのしきい値を設定できます。管理対象デバイスから収集されたパフォーマンスインデックスIMCが指定したしきい値を満たすと、WSMはアラームを生成します。

ワイヤレスパフォーマンス監視

WSMには、次のパフォーマンス監視機能があります。

- 基本的なパフォーマンス監視WSMパフォーマンス監視は、IMCプラットフォームのパフォーマンス管理に基づいて実装されます。WSMが正常にデプロイされると、IMCプラットフォームでは、CPUやメモリー使用量などのパフォーマンスインデックスの監視および表示がリアルタイムで開始されます。
- ワイヤレスパフォーマンス監視設定ワイヤレスサービスの概要ページ、およびIMCプラットフォームのホームページ上のワイヤレスサービス、ワイヤレスレポート、およびWebサービスウィジェットのパフォーマンスインデックスの設定に使用します。
- リアルタイム監視WSMは、オンラインのFAT AP、FIT AP、およびクライアントをリアルタイムで監視します。

ビューの管理

WSMには、次のビュー管理機能があります。

- **Location view**: 物理的な位置に従ってAPをグループ単位で管理します。
- **Custom view**: グループ内の同じACに接続されたFIT APを管理します。カスタムビューを使用すると、管理者はターゲットデバイスに簡単に集中できます。

- **GIS view**：ロケーションビュー内のホットスポットを既定のマップにマッピングし、次の項目を動的に表示します。
  - Address
  - Telephone number
  - Total number of APs
  - Total number of terminals for each location view

ワイヤレストポロジー管理

ワイヤレストポロジー管理は、IMCプラットフォームのトポロジー管理機能の拡張であり、次のトポロジーを提供します。

- **Wireless device topology**：WSM内のすべてのACおよびFAT APを表示します。トポロジー内のACまたはFAT APをダブルクリックすると、そのトポロジーを表示できます。
- **Location view topology**：ロケーションビューでAPおよび関連付けられたクライアントに関する情報を表示します。
- **Custom view topology**：特定のACによって管理されるFIT APおよび関連付けられたクライアントをカスタムビューで表示します。
- **Mesh topology**：メッシュネットワーク内のACおよびFAT AP、MPP、MP、およびMAP接続とクライアント情報を表示します。
- **Converged topology**：ネットワーク内のワイヤレスデバイスとワイヤードデバイス、およびそれらの接続を表示します。

WIDSコマンド

802.11ネットワークは、不正なAPやクライアント、アドホックネットワーク、DoS攻撃など、さまざまな脅威の影響を受けます。不正なデバイスは、企業のネットワークセキュリティに対する深刻な脅威です。WIDSは、ワイヤレスネットワークに対する悪意のある攻撃や侵入を早期に検出するために使用されます。

WIDSは、ComwareベースのACを管理します。

ComwareベースのAC上のWIDS

WSMで不正デバイスを検出できるようにするには、次のように設定します。

- 許可されるOUIリスト
- 許可SSIDリスト
- 許可MACアドレスリスト
- 攻撃MACアドレスリスト
- WIDS検出規則
- WIDS検出モード

検出された不正なAPおよび不正なクライアントを管理し、アタックデバイスリストまたは許可リストに追加したり削除したりできます。

WIPS

Wireless Intrusion Prevention System(WIPS)は、ユーザー定義のセキュリティポリシーに従って、企業ネットワークおよびユーザーを不正なワイヤレスアクセスから保護します。

WIPSを使用すると、WLANを複数の仮想セキュリティドメインに分割し、センサー(IPSが有効なAP)を

各仮想セキュリティドメインに追加できます。センサーは、定義した検出規則に従って、次のことを実行できます。

- ワイヤレスネットワーク内のAPの分類
- ワイヤレスネットワークに接続されているクライアントの分類
- ワイヤレスネットワークでのセキュリティイベントの検出
- チャネルを許可チャネルと禁止チャネルに分割し、チャネル使用率を検出する
- 不正なクライアントによるワイヤレスネットワークへのアクセスを禁止する
- 不正デバイス対策WIPSは、ComwareベースのACだけを管理します。

ネットワーク計画

WSMネットワークプランニングでは、ロケーショントポロジーに仮想APを追加してエリア内の信号カバレッジを分析することにより、APのロケーションと数を計画できます。

RF管理

RF管理では、無線の種類、伝送速度、およびコンクリート壁、窓、金属製バリアなどの障害物に基づいてヒートマップが作成されます。APは、信号強度、アクセスレート、チャネル、またはSSIDでソートできます。RF管理では、ロケーションビューに基づいて、部屋または床のワイヤレス信号カバレッジが表示されます。

RF管理を使用すると、管理者は弱い信号、アクセス速度の低さ、ネットワークアクセスの失敗、およびその他のワイヤレス信号の問題を特定できます。ユーザーは、APの展開、伝送速度、およびチャネル設定を調整して、最適で費用対効果の高いワイヤレス信号カバレッジを実装できます。

スペクトルガード管理

WSMスペクトル分析は、2.4GHzおよび5GHzの周波数帯域をスキャンして、干渉および影響を受けるチャネルを検出し、リアルタイムスペクトルデータを生成します。オペレーターは、現在の干渉データおよびリアルタイムスペクトルデータを表示することで、ワイヤレススペクトルのパフォーマンスおよびWLANセキュリティを判断できます。2.4GHz帯域で検出できる干渉には、次のものがあります。

- Microwave ovens
- Bluetooth devices
- Fixed frequency devices
- Video devices with fixed frequency
- Cordless phones using fixed frequency
- Microsoft Xbox

5GHz帯域で検出できる干渉には、Cordless phones using fixed frequency、Microsoft Xbox、およびその他のFixed frequency devicesが含まれます。

ワイヤレスロケーション管理

ワイヤレスロケーションは、オンラインクライアント、不正なクライアント、不正なAP、およびiNodeクライアントを検出し、オペレーターがワイヤレスクライアントと不正なデバイスの物理的な場所を特定できるようにします。ワイヤレスロケーションには、次の機能があります。

- **Location Aware locating**: ロケーション認識検索では、サンプリングを行わずにリアルタイムで複数のクライアントを同時に検索できます。ロケーション認識検索をサポートするAPでのみ実行できます。
- **Bluetooth Low Energy (BLE) locating**: BLE位置特定は、信号強度の三角測量を使用して、リアルタイムで正確なクライアント位置特定を実行できます。導入コストが低くなります。
- **X-Share locating**: X-Shareの検索は、X-Shareアンテナをサポートするapでのみ実行できます。X-Shareの検索では、サンプリングなしでクライアントを高速に検索できます。
- **AP-based wireless locating**: APは、ワイヤレス信号をスキャンして信号強度を分析することにより、サンプリングなしでワイヤレスデバイスを検出できます。この機能により、クライアント、不正なクライアント、および不正なAPを検出できます。
- **GIS locating**: この機能を使用すると、デフォルトマップ上でAPまたはモバイルクライアントのロケーションビューを検索できます。

エネルギーポリシー管理

エネルギーポリシー管理では、次のようなエネルギーポリシーを設定および管理できます。

- APまたはその無線の起動とシャットダウンのスケジューリング
- APの送信電力の自動調整
- SSIDサービスの開始と停止のスケジューリング。

エネルギーポリシーは、追加、変更、削除、コピー、一時停止、または復元できます。

メッシュ構成管理

メッシュ設定管理を使用すると、特定のワイヤレスデバイスのMPポリシー、メッシュプロファイル、メッシュインターフェース、およびピアMACアドレス設定を管理できます。

ネットワーク評価管理

ネットワーク評価を使用すると、エリア内のAPの動作ステータスを判断し、評価結果と記録に基づいてネットワークを最適化できます。

評価タスクを作成すると、WSMによって、指定したロケーションビューでAPおよびクライアントのデータが定期的に収集されます。データ収集が完了すると、WSMによって収集されたデータが要約され、事前定義されたしきい値に基づいてAPおよびクライアントが評価されます。評価レポートをエクスポートすると、APの全体的な評価情報、APおよびクライアントの履歴レコードと要約、および評価結果を表示できます。全体的な評価情報を使用して、ロケーション内のAPの全体的な動作ステータスを判断できます。

ワイヤレスサービスレポート

ワイヤレスサービスレポート機能は、WSMによって収集されたデータを分析します。また、APのパフォーマンス、利用率、サービスの可用性などのパフォーマンスデータを要約し、データを棒グラフ、折れ線グラフ、または円グラフで表示します。

構成管理

WSMには、次の一般的な構成管理機能があります。

- **Wireless Monitoring Settings**：レポート、Webサービス、およびWSMサービス概要ページの監視インデックスをバッチで開始または停止できます。
- **FIT AP Group Management**：IMCプラットフォームオペレーターは、IMCプラットフォームオペレーターが管理権限を持つACを介してFIT APを管理できます。WSM FIT APグループ管理を使用すると、管理者はFIT APレベルで操作権限を制御できます。FIT APを異なるグループに割り当て、FIT APグループベースで操作権限を付与することで、管理者は各オペレーターのFIT APの表示および保守権限を制御できます。
- **AP model Management**：APモデルの追加、変更、削除、およびAPモデルに関する基本情報の表示を行うことができます。
- **Antenna Management**：アンテナ情報を追加、変更、削除、および表示できます。
- **Threshold Configuration**：パフォーマンス索引しきい値を設定できます。収集されたデータが選択した索引のしきい値を超えると、WSMによってアラームが生成されます。
- **UAM Parameter Configuration**：UAMパラメーターを構成できます。UAMと連携する必要があるWSMモジュールは、構成されたパラメーターを介してUAMからデータを取得します。
- **Endpoint Identification Management**：ベンダー、タイプ、OS情報などのエンドポイントIDを一元的に管理できます。
- **Synchronization Configuration**：無線デバイスの同期トリガーメカニズムを管理できます。

WSMは、一般的な機能に加えて、Comwareベースのワイヤレスデバイスのバッチ設定およびバッチ管理をサポートします。

オペレーター権限管理

WSMには、次のオペレーター権限管理機能があります。

- オペレーターグループによる権限の割り当て
- 特定のオペレーターによる特権の割り当て

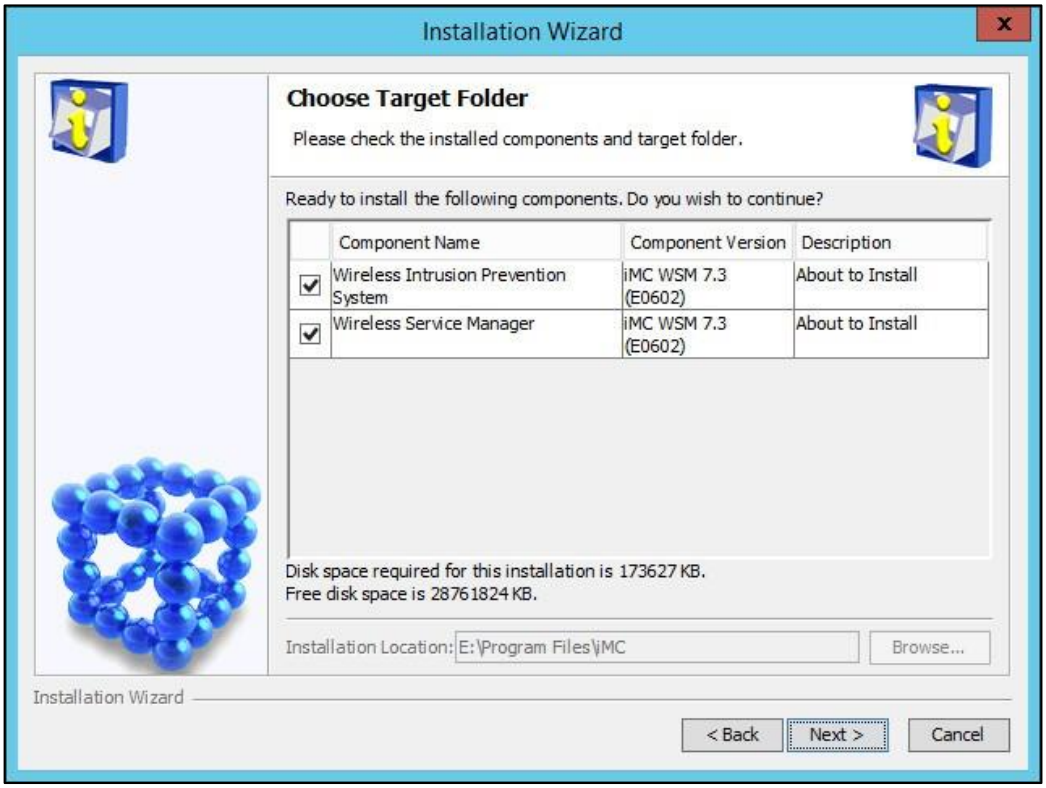
WSMは、IMCプラットフォームの特権割り当て機能を拡張します。WSMは、FIT APグループおよびロケーションビューに従って管理特権を割り当てることができます。

WSMインストール

WSMは、他のコンポーネントと同じ方法でインストールします。詳細については、H3C IMCデプロイメントガイドを参照してください。

図1に示すように、WIPS以外のすべてのモジュールをインストールする必要があります。WIPSはインストールするかどうかを選択できます。

図1 WSMのインストール



WSMライセンス

WSMでは、次のタイプのライセンスがサポートされています。

- **License of authorization**：WSMコンポーネントまたは特定のモジュールの使用を許可しますが、管理できるノード数は増加しません。たとえば、locating managementライセンスでは、locating managementモジュールの使用のみが許可されます。
- **Node license**: 管理対象ノードの数を増やします。ノードライセンスは、認可または拡張、あるいはその両方に使用できます。たとえば、FIT APノードライセンスは管理可能なFIT APの数を増やすだけであり、WIPSノードライセンスはWIPS管理モジュールを認可し、WIPSが管理できるセンサーの数を増やします。

基本WSMライセンスは、WSMが使用可能かどうかを決定します。このライセンスは、すべてのWSMモジュールを対象とするわけではありません。独立したライセンスを持つモジュールには、次のものがあります。

- WIPS管理
- 管理の検索
- ネットワーク評価

表2 WSMライセンスとモジュール固有のライセンスの説明

モジュール	ライセンス	説明
Wireless Service Manager	Basic WSM license	WSMを使用するには、ライセンスを登録する必要があります。デフォルトでは、基本WSMライセンスには50個のAPが含まれています。 管理可能なFAT APおよびACの数は、IMCプラットフォームノードライセンスによって制御されます。
	FIT AP node license	このライセンスを使用すると、管理可能なFIT APの数を増やすことができます。たとえば、FIT APが230あるネットワークの場合、基本WSMライセンスの50 APを除いて、200FIT APのFIT APノードライセンスを購入する必要があります。WSMは、ライセンス制限内でのみFIT APを管理できます。ネットワーク上のFIT APの数がライセンスで許可されている最大数を超えた場合、FIT APはWSMに追加できますが、表示されません。
	WTU license	このライセンスでは、WSMが管理するWTUsの数を制御できます。
Locating Management	Basic locating management license	このライセンスでは、X-Share検索機能、Wireless Locating Based on AP機能、およびGIS検索機能を使用できます。
	Real Time Location System (RTLS) node license	このライセンスでは、リアルタイム検索機能を使用して、リアルタイム検索用のAPの数を制御できます。たとえば、リアルタイム検索用のAPが80台あるネットワークでは、100ノードのライセンスを購入する必要があります。
WIPS Management	WIPS node license	このライセンスでは、WIPS管理モジュールを使用してセンサーの数を増やすことができます。たとえば、50個のセンサーのWIPSノードライセンスが登録されている場合は、すべてのWIPS機能を使用して最大50個のセンサーを管理できます。
Network Evaluation	Network evaluation license	このライセンスでは、ネットワーク評価モジュールを使用できます。

試用期間中

IMCの試行期間は45日間です。試行期間では、WSMのすべてのモジュールが使用可能ですが、ノード数は制限されます。

試用期間中にサポートされるノードの数を図2に示します。

図2 WSMライセンスの試用期間

Wireless Service Manager	iMC WSM 7.3 (E0508P11)	Max. APs: 5000	2554	Apr 30, 2019
		Max. Real-Time Location Nodes(AP): 10	0	Apr 30, 2019
		Max. Real-Time Location Nodes(Beacon): 10	0	Apr 30, 2019
		Network Evaluation	--	Apr 30, 2019
		Max. WIPS Sensors: 50	1	Apr 30, 2019
		Max. WTUs: 1000	0	Apr 30, 2019
		Supported IoT Modules quantity: 50	0	Apr 30, 2019

試用期間終了後

試用期間が終了すると、WSM基本ライセンスをアクティブ化しないとWSMを使用できません。モジュールのモジュール固有のライセンスがアクティブ化されていない場合、そのモジュールは使用できません。ナビゲーションツリーから**Service > WLAN Manager**にアクセスした場合、モジュール名は表示されません。モジュール固有のライセンスがアクティブ化されているモジュールは、引き続き使用できます。たとえば、ライセンスをアクティブ化しないとスペクトルガードを使用できませんが、ライセンスがアクティブ化されている場合は、検出管理モジュールを使用できます。ライセンスのアクティブ化の詳細については、H3C IMCの展開ガイドを参照してください。

注:

アクティブ化された永続ライセンスは削除できません。

WSMホームページウィジェット

WSMには、複数のワイヤレスサービスホームページウィジェットが用意されています。オペレーターは、IMCホームページにウィジェットを追加できます。詳細は、「H3C IMC v7.3 Enterprise and Standard Platform Administrator Guide」を参照してください。

次の情報では、各ウィジェットについて説明します。

基本機能

各ウィジェットにはいくつかの基本的な機能があります。

リフレッシュ間隔の設定

デフォルトでは、各ウィジェットのリフレッシュ間隔は5分です。ウィジェットごとに間隔を設定できます。

リフレッシュ間隔を設定する手順は、次のとおりです。

1. 右上隅にある**Set**アイコン をクリックします。

   ウィジェットに特定の機能が含まれていない場合は、**Setting**メニューが表示されます。ウィジェットに特定の機能が含まれている場合は、**Refresh Interval**を選択すると、**Setting**ダイアログボックスが開きます。
2. リフレッシュ間隔(分単位)を選択します。オプションは次のとおりです。
   - **No Refresh**
   - **1**
   - **5**
   - **10**
   - **30**

   デフォルトのリフレッシュ間隔は5分です。**No Refresh**は、Widgetが自動的にリフレッシュされないことを示します。手動でリフレッシュできます。
3. **OK**をクリックします。

最大表示

ウィジェットを最大化するには:

1. 右上隅にある**Maximize**アイコンをクリックします。
2. **Close**アイコン をクリックして、最大表示を閉じます。

ウィジェットの更新

デフォルトのリフレッシュ間隔は5分です。ウィジェットをリフレッシュするには、右上隅にある**Refresh**アイコン をクリックします。

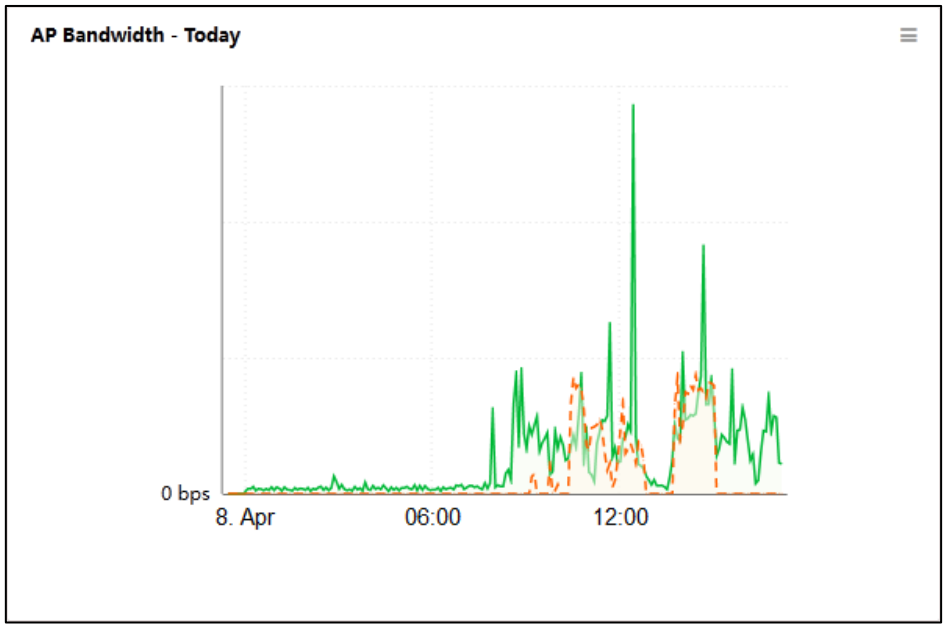
ウィジェットの削除

1. ウィジェットの右上隅にある**Delete** アイコン をクリックします。
2. 表示されたダイアログボックスで**OK**をクリックします。

AP帯域幅-現在

このウィジェットは、今日の00:00から現在の時間までの、ワイヤレス側のすべてのAPの合計送信レートと受信レートの変化をエリアグラフ(図3)で示します。横軸は時間を表し、縦軸は送信レートまたは受信レートの値を表します。送信レートと受信レートはグラフ上で異なる色で表されます。

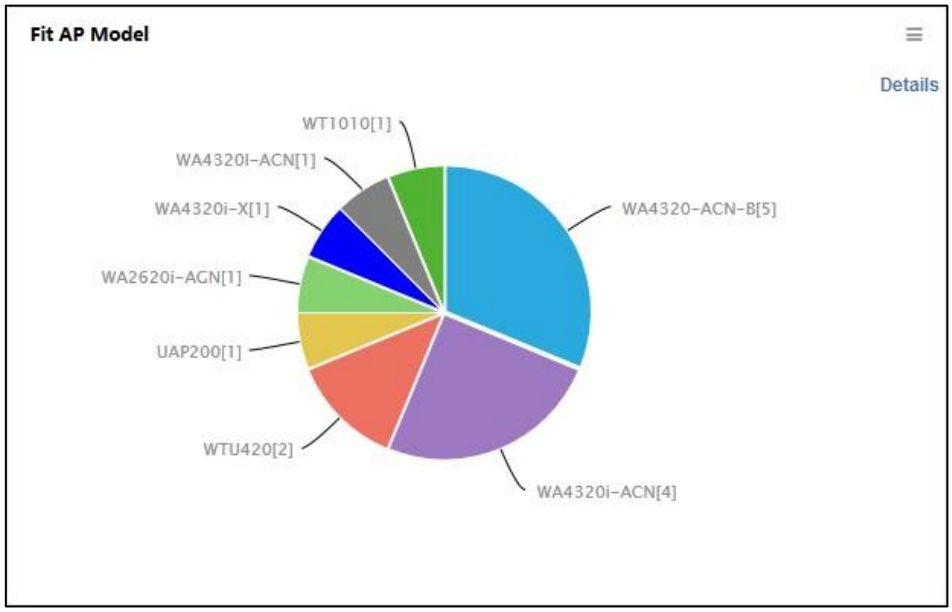
図3 AP Bandwidth-Todayトレンドグラフ



FIT APモデル

図4に示すように、円グラフは、FIT APモデルごとのFIT APの数を示しています。

図4 FIT APモデル



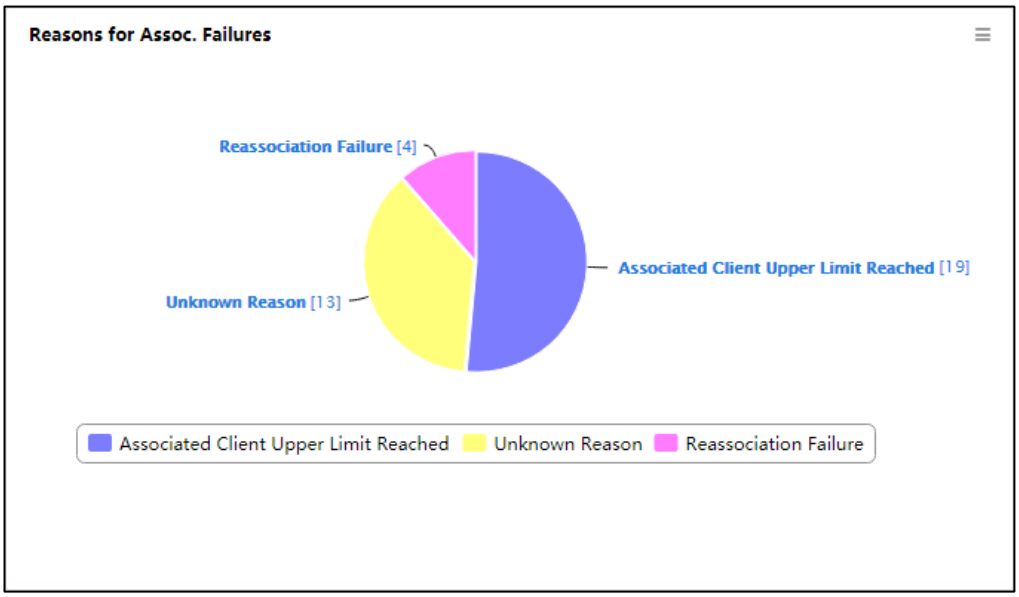
色はAPモデルを表します。

- カーソルを色の上に置くと、APモデルとそのモデルのAP数を示すヒントが表示されます。
- 色をクリックして、FIT APリストを入力します。リストには、APモデルのFIT APに関する情報が表示されます。
- 右上隅のDetailsをクリックすると、各モデルのAPの数とすべてのモデルに対する割合が表示されます。

アソシエーションの失敗の理由

このウィジェットは、今日のアソシエーションの失敗と失敗の理由を円グラフ(図5)で示します。理由は、**Associated client upper limit reached**、**Unsupported mandatory rate**、**Reassociation failure**、**Others(weak signal strength**や**blacklist**など)、および**Unknown reason**です。

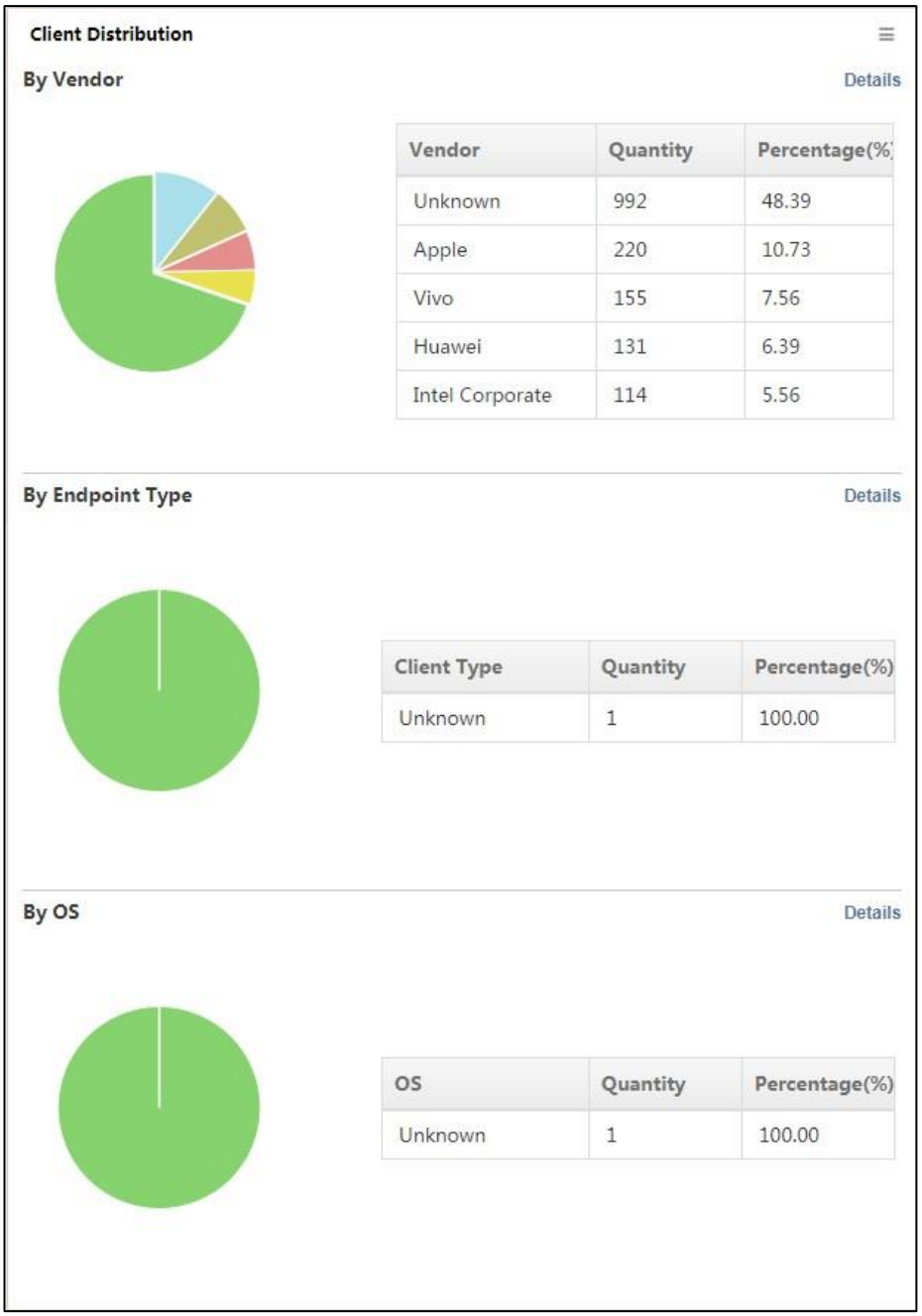
図5 アソシエーションの失敗の理由



クライアントの分布

このウィジェットは、ベンダー、エンドポイントタイプ、およびOS別のクライアント数を円グラフ(図6)で示します。

図6 クライアントの分布



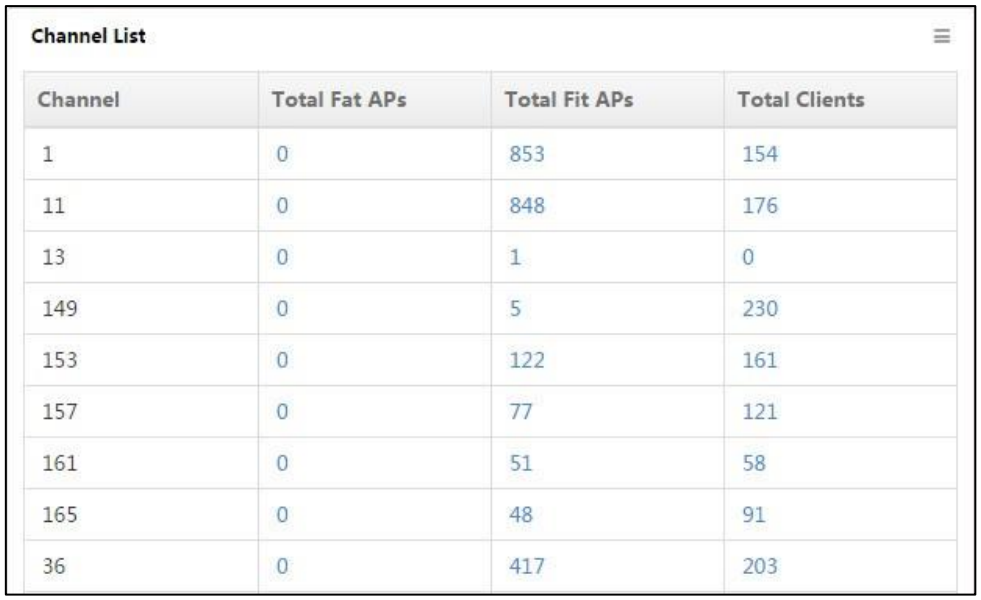
ベンダー別の統計を例にとると、ウィジェットは左側の円グラフに各ベンダーのクライアント数とクライアント総数の割合を表示し、右側に上位10のベンダーの割合を表示します。

右側の**Details**リンクをクリックします。**Details**ウィンドウに、クライアント数と各ベンダーの割合が表示されます。

チャネルリスト

このウィジェットは、ネットワーク上のFAT AP、FIT AP、およびクライアントをチャネル別にリストします(図7)。

図7 チャネルリスト



Channel List

Channel	Total Fat APs	Total Fit APs	Total Clients
1	0	853	154
11	0	848	176
13	0	1	0
149	0	5	230
153	0	122	161
157	0	77	121
161	0	51	58
165	0	48	91
36	0	417	203

このリストには次の情報が表示されます。

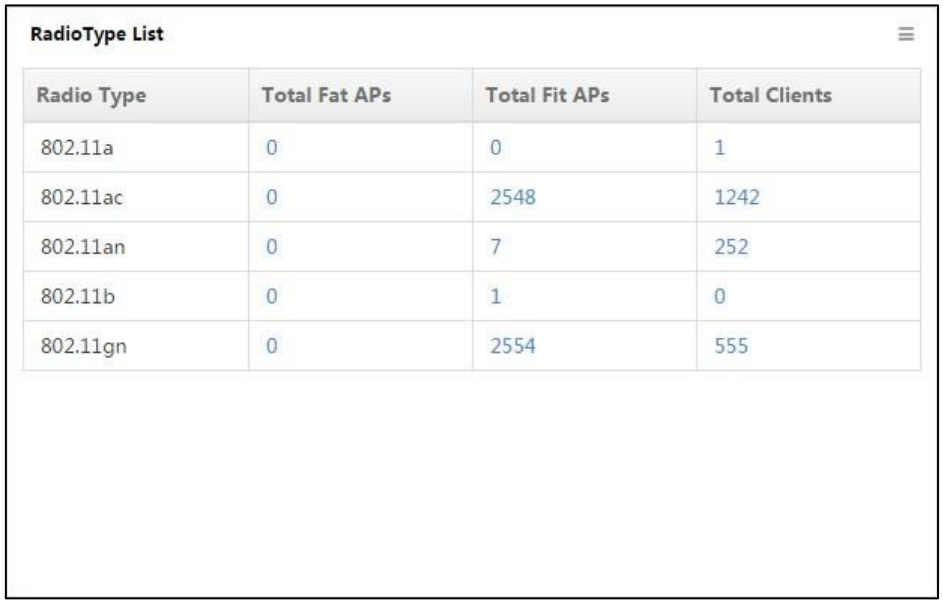
- **Channel**: ネットワーク上で設定されているチャネルの番号。
- **Total FAT APs**: チャネル上でサービスを提供するFAT APの数。
- **Total FIT APs**: チャネル上でサービスを提供するFIT APの数。
- **Total Clients**: チャネルを介してネットワークにアクセスするクライアントの数。

チャネルを使用するFAT AP、FIT AP、またはクライアントのリストを表示するには、チャネルの番号をクリックします。

無線タイプリスト

このウィジェットは、ネットワーク上のFAT AP、FIT AP、およびクライアントを無線タイプ別にリストします(図8)。

図8 無線の種類一覧



Radio Type	Total Fat APs	Total Fit APs	Total Clients
802.11a	0	0	1
802.11ac	0	2548	1242
802.11an	0	7	252
802.11b	0	1	0
802.11gn	0	2554	555

このリストには次の情報が表示されます。

- **Radio Type**: 無線のタイプ。
- **Total FAT APs**: この無線タイプでサービスを提供するFAT APの数。
- **Total FIT APs**: この無線タイプでサービスを提供するFIT APの数。
- **Total Clients**: この無線タイプでネットワークにアクセスするクライアントの数。

無線タイプを使用するFAT AP、FIT AP、またはクライアントのリストを表示するには、無線タイプの番号をクリックします。

AC

このウィジェットは、円グラフ(図9)のAC数を円グラフ(図9)に表示し、円グラフの下に到達可能性ステータス別のAC数を表示します。

図9 AC

円グラフの各セクターは、不明なAC、正常なAC、およびアラームを生成するACの数をアラームレベル別に示します。ACのアラームレベルは、ACの最も重大なアラームのレベルと同じです。対応する到達可能性ステータスでフィルタリングされたACリストを表示するには、円グラフの下にある合計、到達可能、または到達不能ACの数をクリックします。

FAT AP

このウィジェットは、アラームレベル別のFAT APの数を円グラフ(図10)に表示し、その下にFAT APの数を到達可能性ステータス別に表示します。

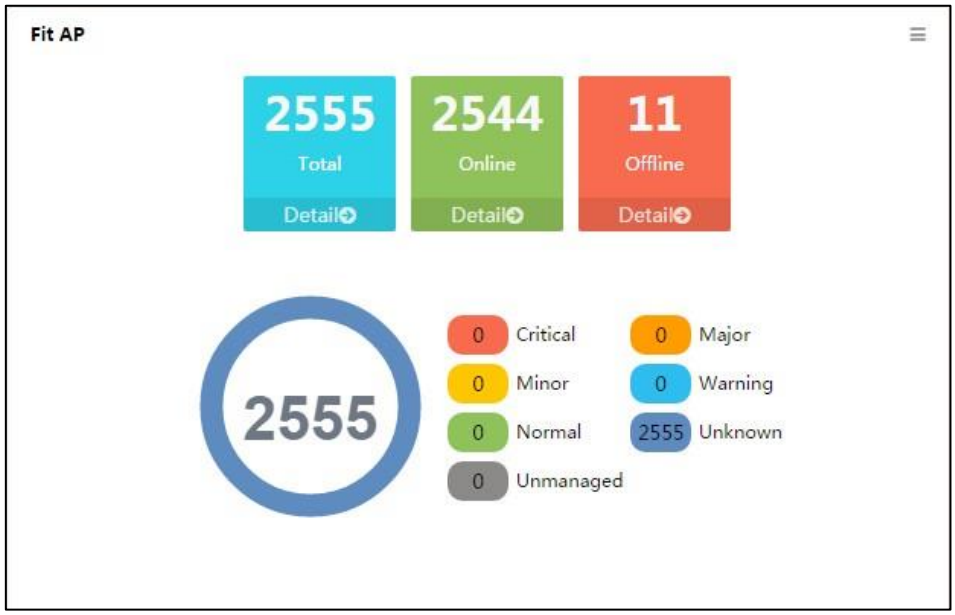
図10 FAT AP

円グラフのセクターは、アラームを生成する不明なFAT APの数をアラームレベル別に示します。FAT APのアラームレベルは、FAT APで最も重大なアラームのレベルと同じです。すべてのFAT AP、到達可能なFAT AP、または到達不能なFAT APのリストを表示するには、円グラフの下にある**Total**、**Reachable**、または**Unreachable**の数をクリックします。

FIT AP

このウィジェットは、円グラフ(図11)にアラームレベル別のFIT AP数を表示し、円グラフの下に到達可能性ステータス別のFIT AP数を表示します。

図11 FIT AP

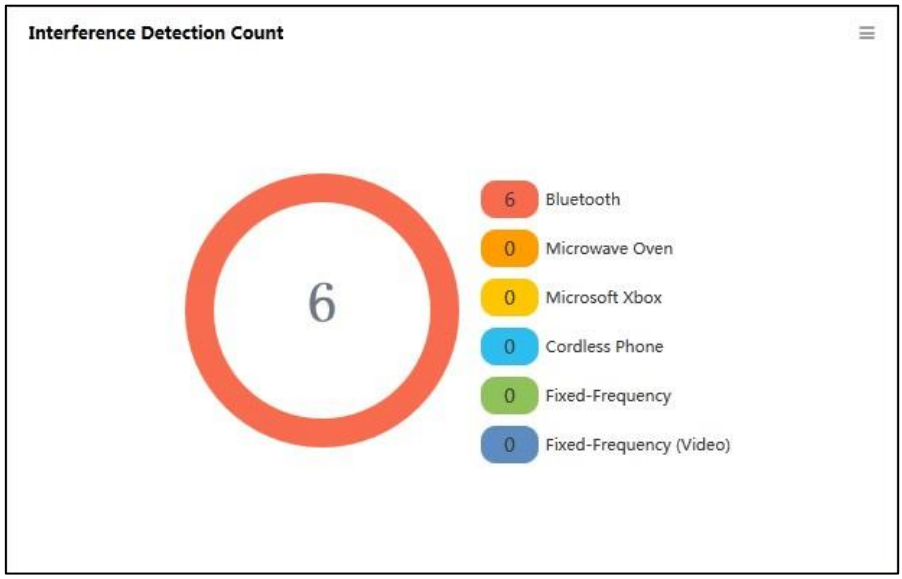


円グラフのセクターは、アラームを生成する不明なFIT APの数をアラームレベル別に示します。FIT APのアラームレベルは、FIT APで最も重大なアラームのレベルと同じです。すべてのFIT AP、オンラインFIT APまたはオフラインFIT APのリストを表示するには、円グラフの下にある合計、オンラインまたはオフラインの数をクリックします。

干渉検出数

このウィジェットは、スペクトル分析をサポートするComwareベースのFIT APによって検出された各タイプのデバイスの干渉時間を円グラフ(図12)で示します。

図12 干渉の検出数



異なるタイプの干渉デバイスは、異なる色で識別されます。WSMは、次のような様々なタイプの干渉デバイスを検出できます:

- Microwave ovens
- Bluetooth devices
- Fixed frequency transmit devices
- Fixed-frequency video transmit devices
- Cordless phones
- Microsoft Xbox

デバイスの横の番号をクリックすると、デバイスリストが表示されます。

不正APと不正クライアント

このウィジェットは、ComwareベースのFAT APとFIT APによって検出された不正なAPと不正なクライアントをリストします(図13)。

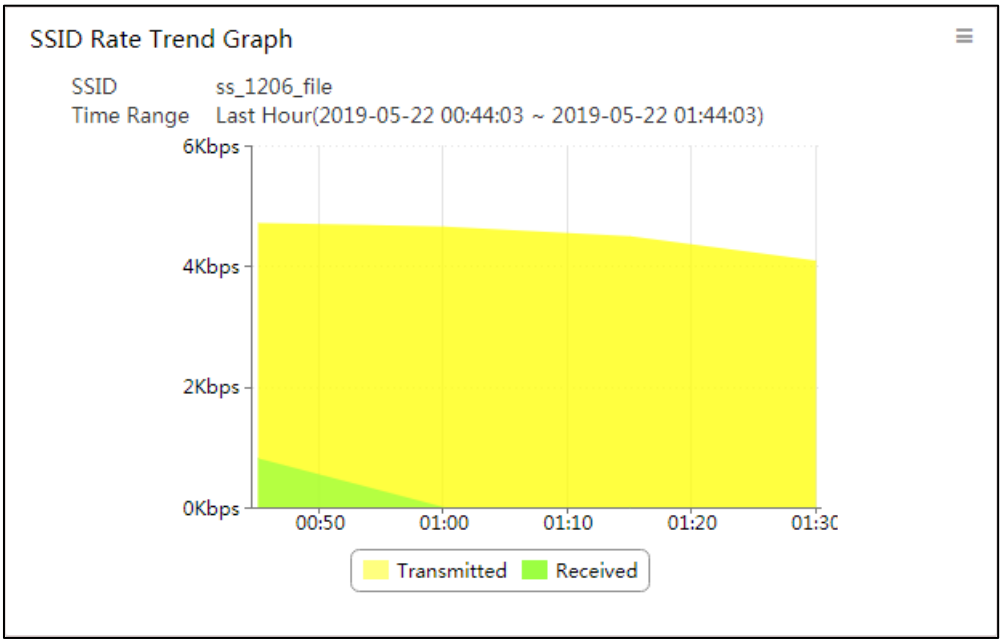
図13 不正なAPと不正なクライアント

このリストには、不正APおよび不正クライアントの数が表示されます。この数をクリックすると、不正APまたは不正クライアントのリストが表示されます。

SSIDレート トレンドグラフ

このウィジェットは、選択した時間範囲における無線側の指定されたSSIDを持つAPの送信レートと受信レートのエリアグラフ(図14)を示します。

図14 SSIDレートトレンドグラフ



選択したSSIDの名前と時間範囲がグラフの上部に表示されます。横軸は時間を表し、縦軸は送信レートまたは受信レートの値を表します。送信レートと受信レートはグラフ上で異なる色で表示されます。

SSID Rate Trend Graphウィジェットを設定するには:

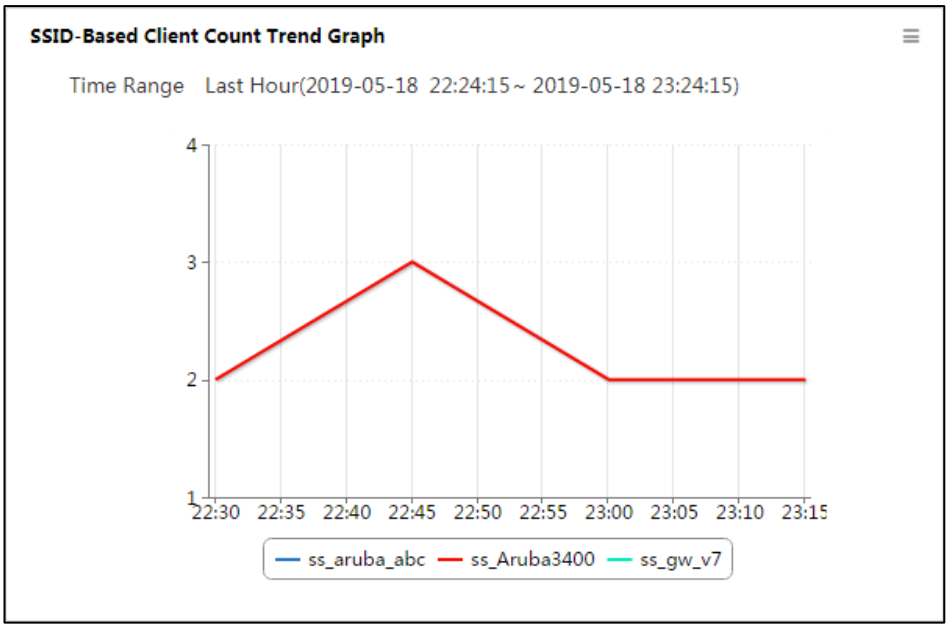
1. ウィジェットの右上にある**Set**アイコン をクリックし、設定を選択します。設定ウィンドウが開きます。
2. **Time Range**リストから時間範囲を選択します。オプションは次のとおりです。
   - **Last Hour**
   - **Last Day**
   - **Last Week**
   - **Last Month**
3. SSIDリストからSSIDを選択します。

   WSM内のすべての**SSID**が使用可能です。
4. **OK**をクリックします。

SSIDベースのクライアント数のトレンドグラフ

このウィジェットは、選択した時間範囲内で指定したSSIDにアクセスしたクライアントをエリアグラフ(図15)で表示します。

図15 SSIDベースのクライアント数のトレンドグラフ



時間範囲はグラフの上部に表示されます。横軸は時間を表し、縦軸はクライアント数を表します。

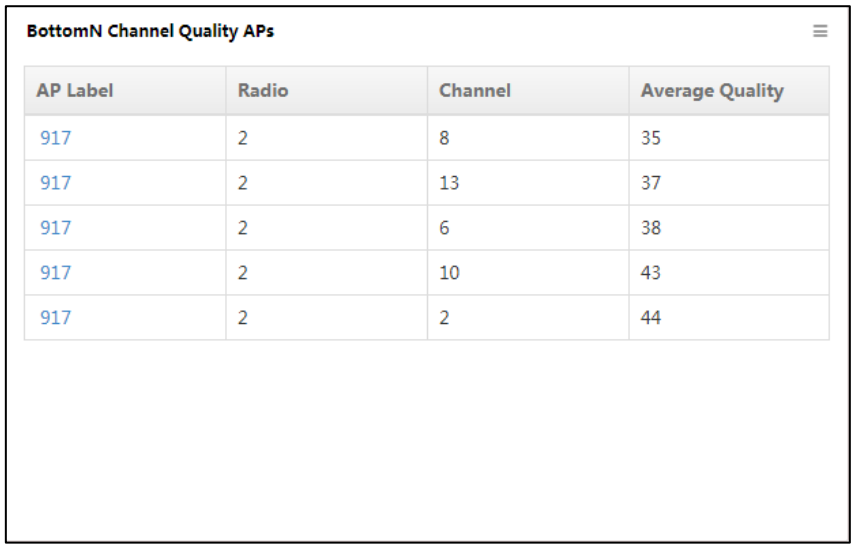
SSIDベースのClient Count Trend Graphウィジェットを設定するには:

1. グラフの右上にある**Set**アイコン をクリックし、**Setting**を選択します。**Setting**ウィンドウが開きます。
2. **Time Range**リストで、時間範囲を選択します。オプションは次のとおりです。
   - **Last Hour**
   - **Last Day**
   - **Last Week**
   - **Last Month**
3. **Select SSID**をクリックします。
   SSID Listが表示されます。
4. SSIDを選択します。最大5つまで選択できます。
5. **OK**をクリックします。
6. 選択したSSIDを**Setting**ウィンドウに表示します。
   SSIDを削除するには、ターゲットSSIDを選択してDeleteをクリックします。
7. **OK**をクリックします。

BottomN APのチャネル品質

このウィジェットは、BottomN APsチャネル品質を降順にリストします(図16)。また、チャネルを使用する無線、APラベル、および平均品質もリストします。

図16 BottomNチャネル品質のAP



AP Label	Radio	Channel	Average Quality
917	2	8	35
917	2	13	37
917	2	6	38
917	2	10	43
917	2	2	44

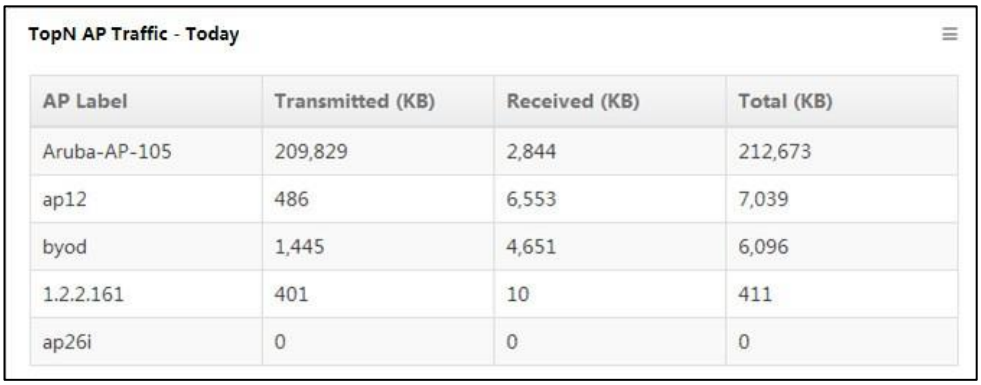
BottomN Channel Quality APsウィジェットを設定するには、次の手順に従います。

1. グラフの右上にある**Set**アイコンをクリックし、**Setting**を選択します。**Setting**ウィンドウが開きます。
2. **BottomN**リストから数値を選択します。オプションは次のとおりです。
   - **5**
   - **10**
   - **20**
   - **50**
   - **100**
3. **OK**をクリックします。

TopN APトラフィック - Today

このウィジェットは、今日の00:00から現在の時刻までのトラフィックが最も多いTopN APを降順にリストします(図17)。このリストには、各TopN APの送信トラフィック、受信トラフィック、および合計トラフィックも表示されます。

図17 TopN APトラフィック - Today



AP Label	Transmitted (KB)	Received (KB)	Total (KB)
Aruba-AP-105	209,829	2,844	212,673
ap12	486	6,553	7,039
byod	1,445	4,651	6,096
1.2.2.161	401	10	411
ap26i	0	0	0

TopN AP Traffic -Todayウィジェットを設定するには、次の手順を実行します。

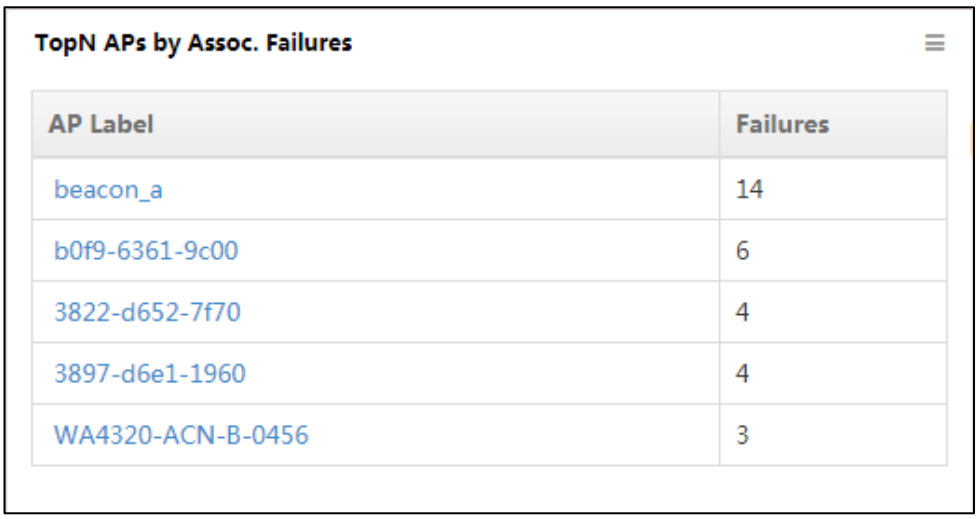
1. グラフの右上にある**Set**アイコン をクリックし、**Setting**を選択します。
   Settingウィンドウが開きます。
2. TopNリストから番号を選択します。オプションは次のとおりです。
   - **5**
   - **10**
   - **20**
   - **50**
   - **100**

   デフォルト値は5です。
3. **OK**をクリックします。

Assoc. FailuresごとのTopN AP

このウィジェットは、アソシエーション障害が最も多いTopN APとそれぞれの障害番号を、今日の00:00から現在の時刻まで降順にリストします(図18)。

図18 Assoc. FailureごとのTopN AP



APの詳細情報を表示するには、APラベルの名前をクリックします。**TopN APs by Assoc. Failures**ウィジェットを設定するには:

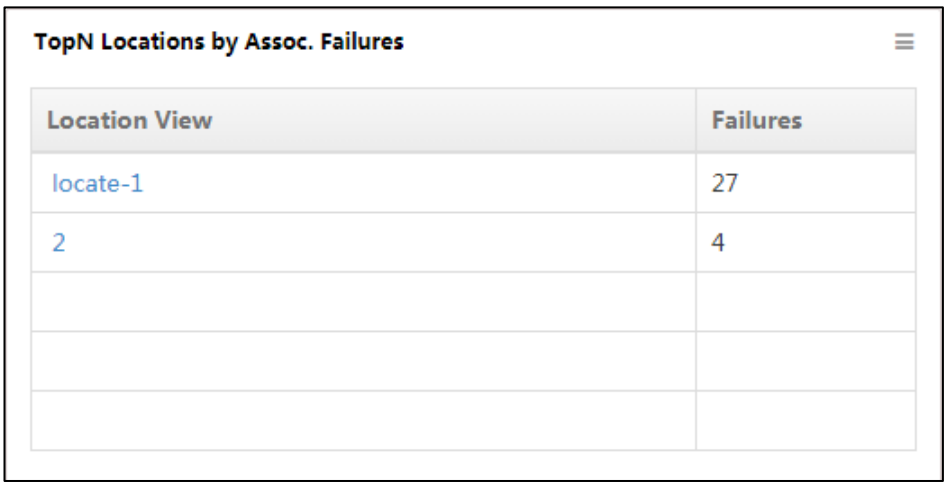
1. グラフの右上にある**Set**アイコン をクリックし、**Setting**を選択します。
   Settingウィンドウが開きます。
2. TopNリストから番号を選択します。オプションは次のとおりです。
   - **5**
   - **10**
   - **20**
   - **50**
   - **100**

   デフォルト値は5です。
3. **OK**をクリックします。

Assoc. FailuresごとのTopNロケーション

このウィジェットは、今日の00:00から現在の時刻までの間で、アソシエーションの失敗が最も多かったTopNロケーションビューとそれぞれの失敗番号を降順にリストします(図19)。

図19 Assoc. FailuresごとのTopNロケーション



ロケーションビューに含まれるサブビューとデバイスを表示するには、ロケーションビューの名前をクリックします。**As sociation.Failures Widget**による**TopN Locations**を設定するには:

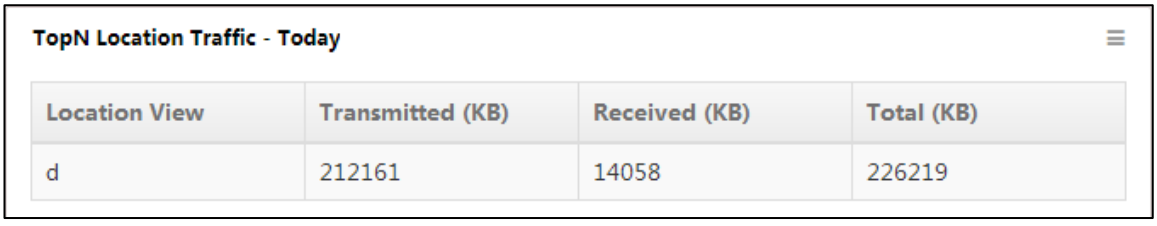
1. グラフの右上にある**Set**アイコンをクリックし、**Setting**を選択します。
   Settingウィンドウが開きます。
2. TopNリストから番号を選択します。オプションは次のとおりです。
   - **5**
   - **10**
   - **20**
   - **50**
   - **100**

   デフォルト値は5です。
3. OKをクリックします。

TopNロケーショントラフィック - Today

このウィジェットは、今日の00:00から現在の時刻までのトラフィックが最も多いTopNロケーションビューを降順にリストします(図20)。このリストには、各TopNロケーションビューの送信トラフィック、受信トラフィックおよび合計トラフィックも表示されます。

図20 TopNロケーショントラフィック - Today



TopN Location Traffic-Todayウィジェットを設定するには、以下の手順に従ってください。

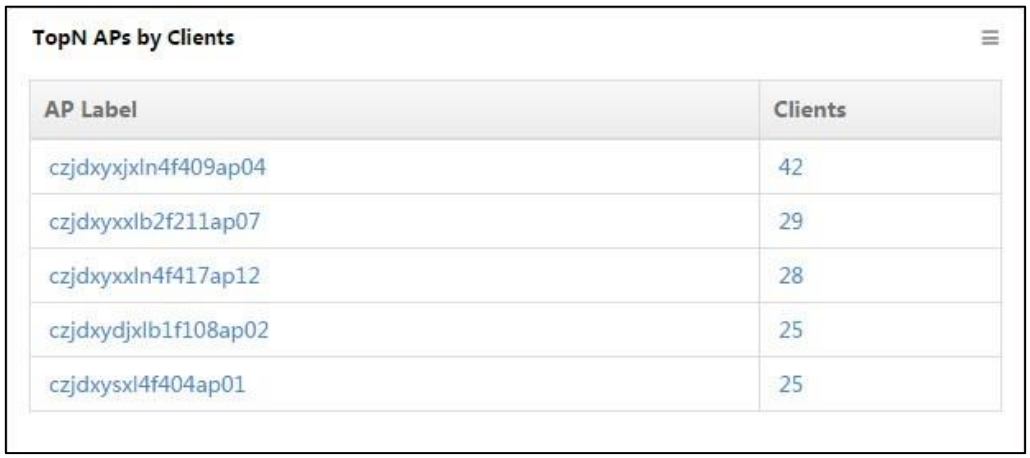
1. グラフの右上にある**Set**アイコン をクリックし、**Setting**を選択します。**Setting**ウィンドウが開きます。
2. TopNリストから番号を選択します。オプションは次のとおりです。
   - **5**
   - **10**
   - **20**
   - **50**
   - **100**

   デフォルト値は5です。
3. OKをクリックします。

クライアントごとのTopN AP

このウィジェットは、TopN AP(FAT APとFIT APを含む)を降順にリストし(図21)、最もオンラインなクライアントとそれぞれのクライアント番号を、今日の00:00から現在の時刻まで表示します。

図21 クライアントごとのTopN AP



APに関する詳細情報を表示するには、APラベルの名前をクリックします。APを介してワイヤレスネットワークにアクセスするクライアントのリストを表示するには、APのクライアント数をクリックします。

TopN APs by Clientsウィジェットを設定するには:

1. グラフの右上にある**Set**アイコン をクリックし、**Setting**を選択します。

   Settingウィンドウが開きます。
2. TopNリストから番号を選択します。オプションは次のとおりです。
   - **5**
   - **10**
   - **20**
   - **50**
   - **100**

   デフォルト値は5です。
3. **OK**をクリックします。

クライアントごとのTopNロケーション

このウィジェットは、今日の00:00から現在の時刻までの最もオンラインなクライアントとそれぞれのクライアント番号を含むTopNロケーションビューを降順にリストします(図22)。

図22 クライアントごとのTopNロケーション

ロケーションビューに含まれるサブビューおよびデバイスを表示するには、ロケーションビューの名前をクリックします。ロケーションビューでAPを介してワイヤレスネットワークにアクセスするクライアントのリストを表示するには、クライアントの数をクリックします。

TopN Locations by Clientsウィジェットを設定するには:

1. グラフの右上にある**Set**アイコン をクリックし、**Setting**を選択します。

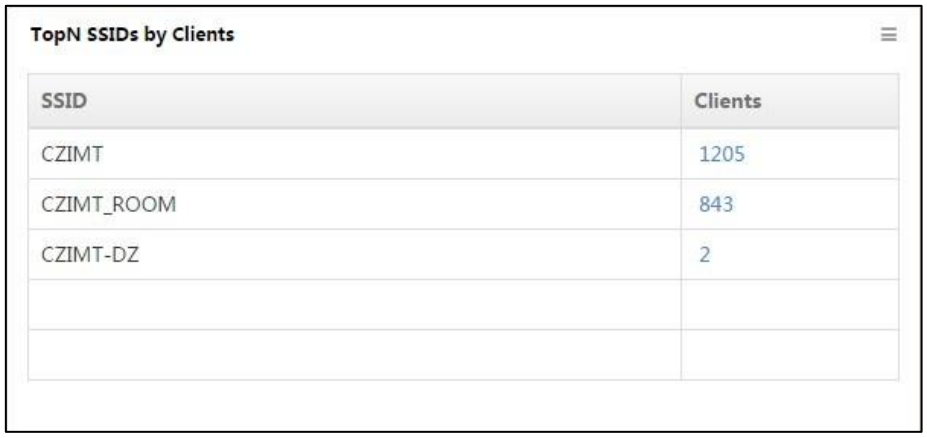
   Settingウィンドウが開きます。
2. TopNリストから番号を選択します。オプションは次のとおりです。
   - **5**
   - **10**
   - **20**
   - **50**
   - **100**

   デフォルト値は5です。
3. **OK**をクリックします。

クライアントごとのTopN SSID

このウィジェットは、オンラインクライアントが最も多いTopN SSIDとそれぞれのクライアント番号を、今日の00:00から現在の時刻まで降順にリストします(図23)。

図23 クライアントごとのTopN SSID



SSIDを使用してワイヤレスネットワークにアクセスするクライアントの一覧を表示するには、クライアント数をクリックします。

TopN SSID by Clientsウィジェットを設定するには、次の手順を実行します。

1. グラフの右上にある**Set**アイコン をクリックし、**Setting**を選択します。

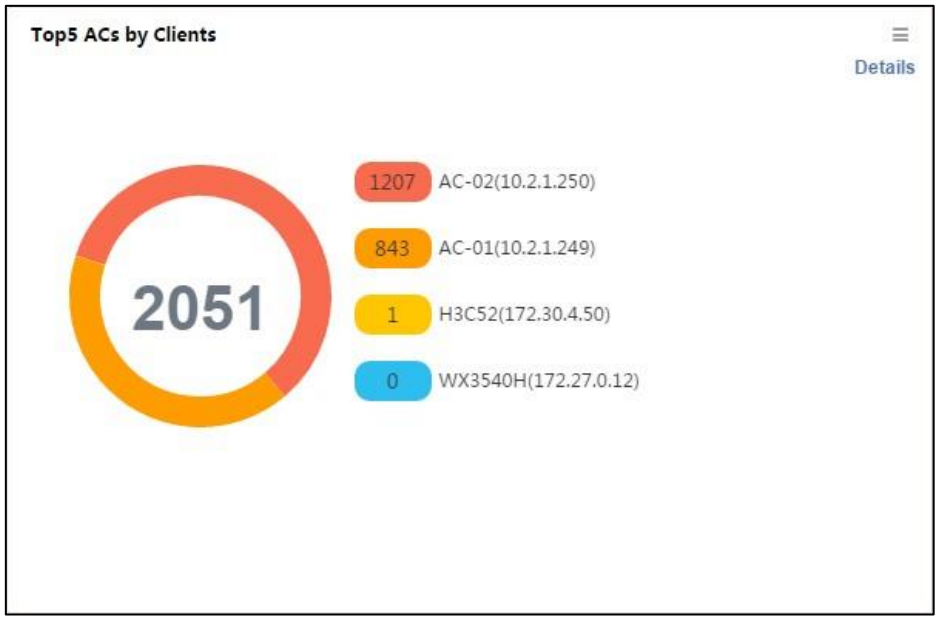
   Settingウィンドウが開きます。
2. TopNリストから番号を選択します。オプションは次のとおりです。
   - **5**
   - **10**
   - **20**
   - **50**
   - **100**

   デフォルト値は5です。
3. **OK**をクリックします。

クライアント別の上位5つのAC

このウィジェット(図24)は、オンラインクライアントが最も多い上位5つのACと、それぞれのクライアント番号を示しています。

図24 クライアントごとの上位5つのAC

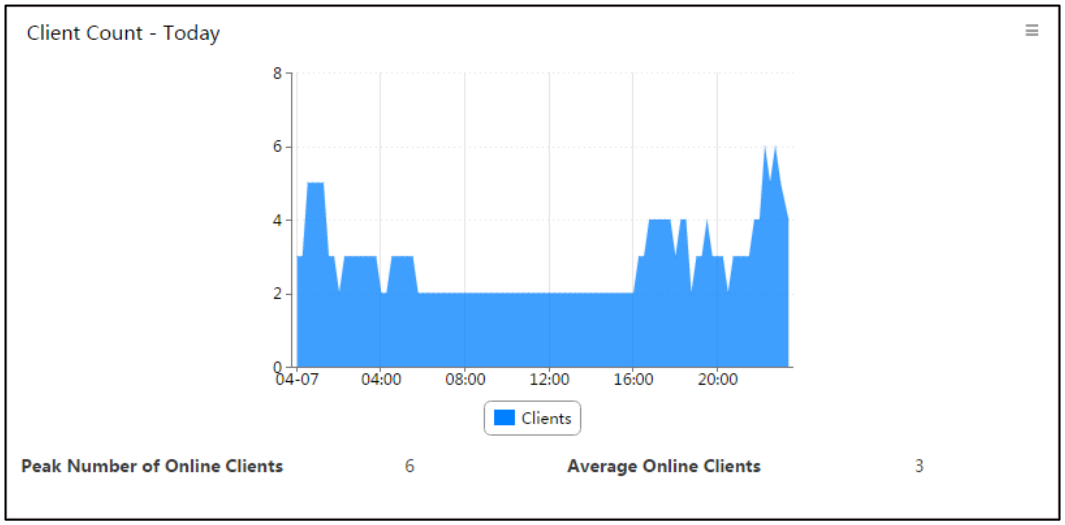


各ACに関連付けられているクライアントの数を一覧で表示するには、右上隅にある詳細をクリックします。

クライアント数 - Today

このウィジェットは、今日の00:00から現在の時刻までのオンラインクライアント数の変化をエリアグラフ(図25)で示しています。

図25 クライアント数 - Today

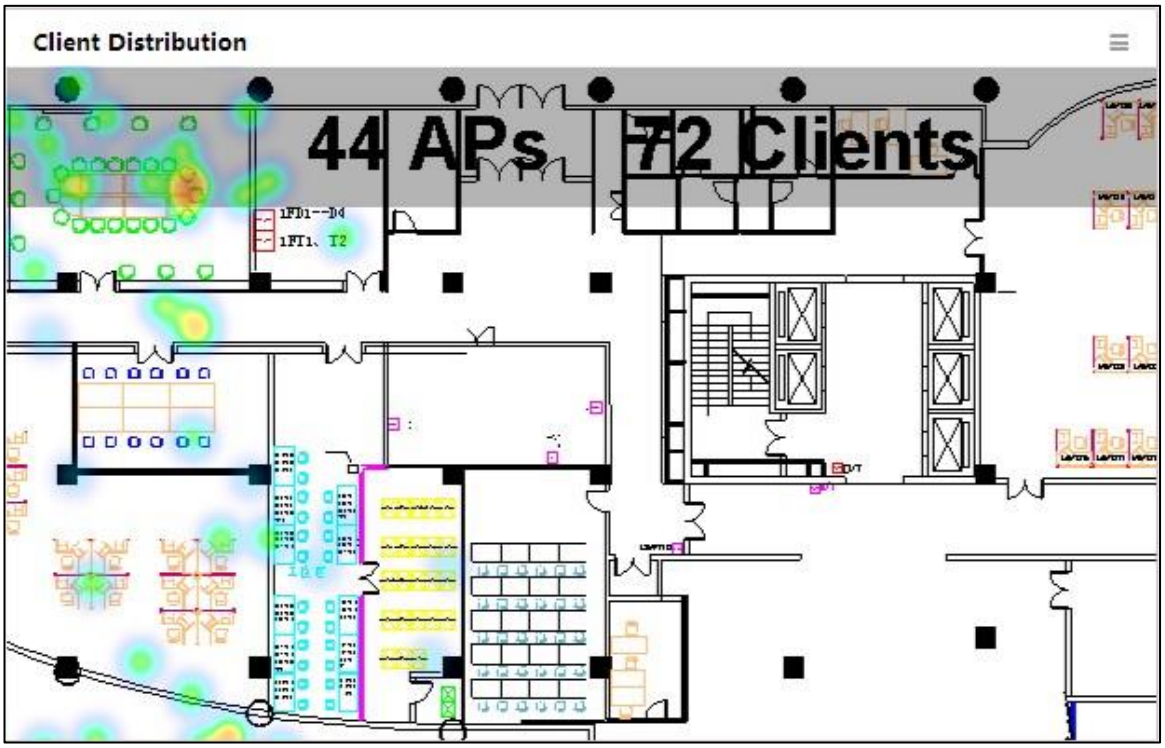


横軸は時間を表し、縦軸はオンラインクライアントの数を表します。横軸の時間間隔は、時間の長さに自動的に調整されます。

クライアントの分布

このウィジェットは、クライアントの分布を、指定されたロケーションビューに番号またはヒートマップで表示します(図26)。

図26 クライアントの分布



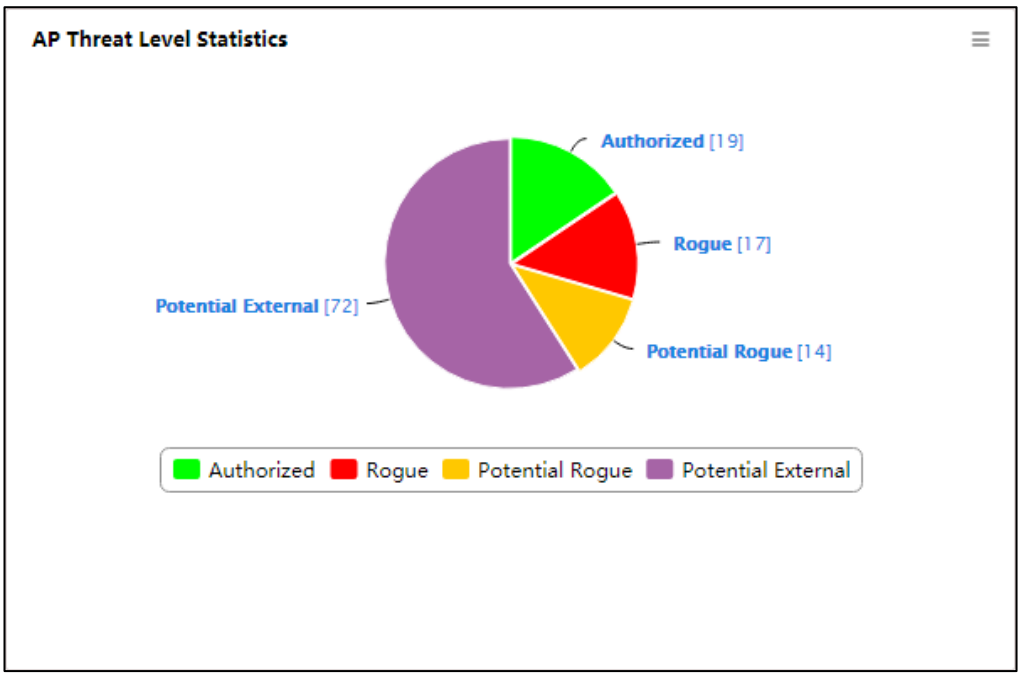
位置ビューと表示モードを指定するには、ウィジェットの上部にカーソルを置いて、表示される**Set**アイコン をクリックします。メニューから**Setting**を選択し、表示されるウィンドウで位置ビューと表示モードを選択します。

AP脅威レベルの統計情報

このウィジェットをカスタマイズする前に、WIPSモジュールを展開してください。

このウィジェットは、APごとの円グラフ(図27)で、WIPSによって検出されたすべてのAPを示します。

図27 AP脅威レベルの統計情報



APタイプは、次のようなWIPSモジュールによって定義されます。

- **Ad Hoc**(アドホック)
- **Authorized**(承認済み)
- **Rogue**(不正)
- **Misconfigured**(設定ミス)
- **External**(外部)
- **Potential-Authorized**(潜在 - 承認済み)
- **Potential-Rogue**(潜在的な不正)
- **Potential-External**(潜在的な外部)
- **Uncategorized**(未分類)

円グラフのAPタイプの領域をクリックすると、APs Detectedページにこのタイプのすべてのに関する情報が表示されます。

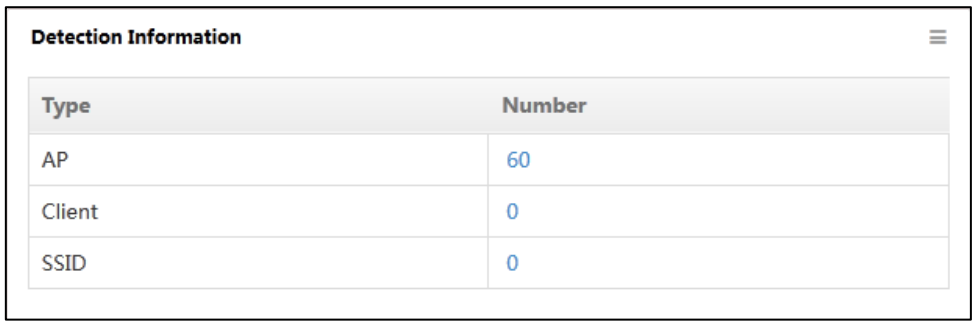
円グラフの下にあるAPタイプのIDをクリックすると、円グラフからAPが非表示になり、クリックすると再表示されます。

検出情報

このウィジェットをカスタマイズする前に、WIPSモジュールを展開してください。

このウィジェットは、WIPSによって検出されたAP、クライアント、およびSSIDの数を一覧表示します(図28)。

図28 検出情報



Type	Number
AP	60
Client	0
SSID	0

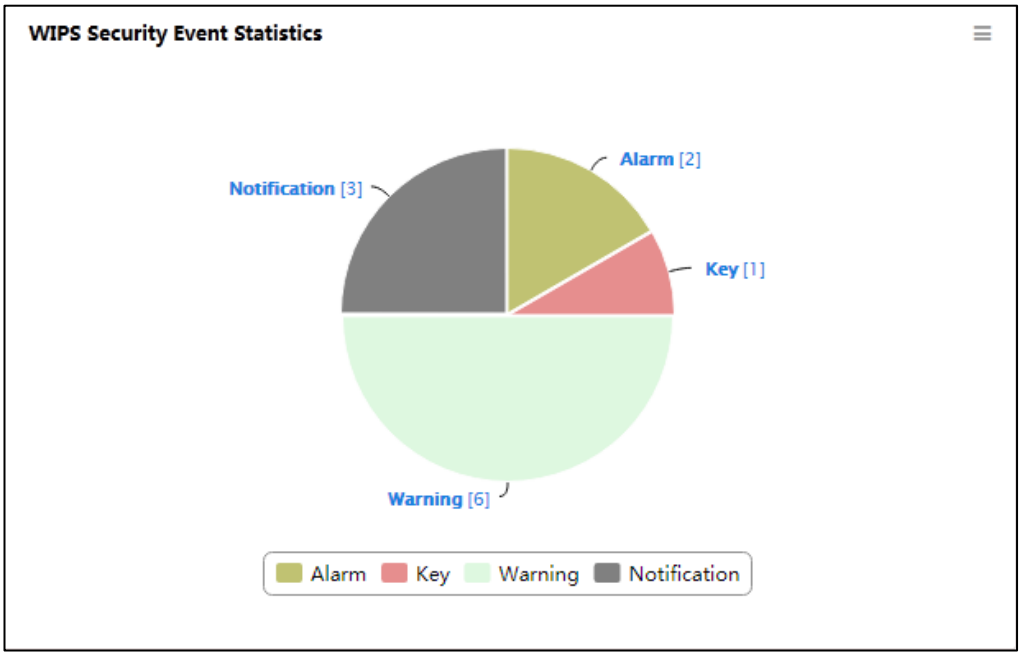
Numberカラムの番号リンクをクリックします。たとえば、APの番号リンクをクリックすると、WIPSによって検出されたAPがAPs Detectedページに表示されます。

WIPSセキュリティイベント統計情報

このウィジェットをカスタマイズする前に、WIPSモジュールを展開してください。

このウィジェットは、WIPSによって検出されたセキュリティイベントの数をセキュリティイベントレベル別に円グラフ(図29)で示します。

図29 WIPSセキュリティイベントの統計情報



円グラフでセキュリティイベントレベルの領域をクリックすると、そのレベルのすべてのセキュリティイベントに関する情報が表示されます。

円グラフの下にあるセキュリティイベントレベルをクリックすると、円グラフにセキュリティイベントレベルが表

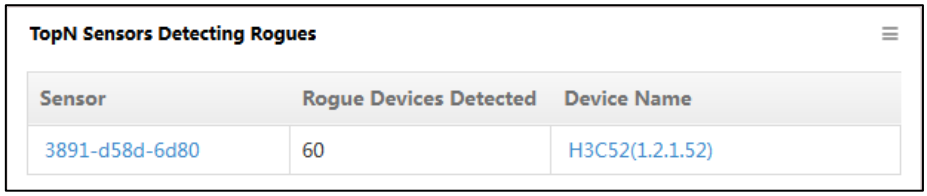
示されなくなります。もう一度表示するには、そのレベルをクリックします。

不正を検出するTopNセンサー

このウィジェットをカスタマイズする前に、WIPSモジュールを展開してください。

このウィジェットは、不正デバイスを検出しているTopNセンサーを降順にリストします(図30)。

図30 不正を検出するTopNセンサー



センサーのラベルリンクをクリックすると、センサーの詳細が表示されます。

デバイスリンクをクリックすると、ACに関する詳細情報が表示されます。**TopN Sensors Detecting Rogues**ウィジェットを設定するには、次の手順に従います。

1. グラフの右上にある**Set**アイコン をクリックし、**Setting**を選択します。
   Settingウィンドウが開きます。
2. TopNリストから番号を選択します。オプションは次のとおりです。
   - **5**
   - **10**
   - **20**
   - **50**
   - **100**

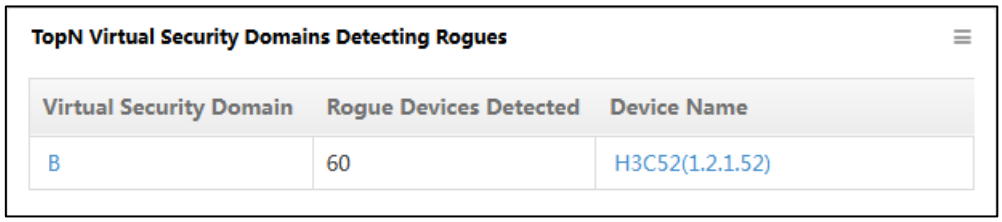
   デフォルト値は5です。
3. OKをクリックします。

TopN仮想セキュリティドメインによる不正の検出

このウィジェットをカスタマイズする前に、WIPSモジュールを展開してください。

このウィジェットは、不正デバイスを検出しているTopN仮想セキュリティドメインを降順にリストします(図31)。

図31 TopN仮想セキュリティドメインによる不正の検出



Virtual Security Domainカラムのドメインリンクをクリックすると、詳細情報が表示されます。

Device Nameカラムのデバイス名リンクをクリックすると、ACによって管理されているドメインに関する詳

細情報が表示されます。

TopN Virtual Security Domains Detecting Roguesウィジェットを設定するには、次の手順を実行します。

1. グラフの右上にある**Set**アイコンをクリックし、**Setting**を選択します。

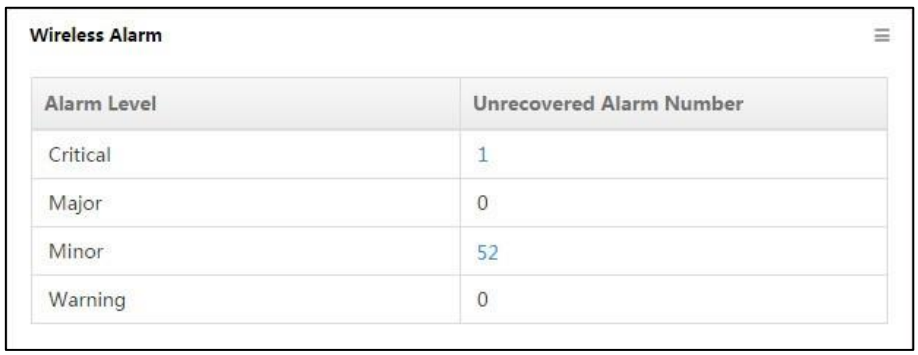
   Settingウィンドウが開きます。
2. TopNリストから番号を選択します。オプションは次のとおりです。
   - **5**
   - **10**
   - **20**
   - **50**
   - **100**

   デフォルト値は5です。
3. **OK**をクリックします。

ワイヤレスアラーム

このウィジェットは、現在のネットワーク上のワイヤレスサービスによって生成された未回復のアラームを一覧表示します(図32)。

図32 ワイヤレスアラーム



このリストには次の情報が表示されます。

- Alarm Level:アラームレベルは次のとおりです。
  - **Critical**
  - **Major**
  - **Minor**
  - **Warning**

Alarm Number:ネットワーク上の特定のアラームレベルの未回復アラームの数。IMCで特定のアラームレベルのすべての未回復アラームを表示するには、アラーム番号をクリックします。

WLANリスト

このウィジェットは、現在のネットワーク上のFAT AP、FIT AP、およびクライアントの分布をSSID別にリストします(図33)。

図33 WLANリスト

WLANリストWidgetを設定するには:

1. グラフの右上にある**Set**アイコンをクリックし、**Setting**を選択します。

   Settingウィンドウが開きます。
2. TopNリストから、WLANリストに表示するSSIDの数を選択します。
3. SSIDフィールドにSSIDの一部または全体を入力して、表示するSSIDをフィルタリングします。

   WLAN Listには、指定したSSID文字列を含むSSIDが表示されます。
4. OKをクリックします。

このリストには次の情報が表示されます。

- **SSID**: SSIDの名前
- **Total FAT APs**: SSIDで無線がバインドされているFAT APの数
- **Total FIT APs**: SSIDで無線がバインドされているFIT APsの数。
- **Total Clients**: SSIDを使用してネットワークにアクセスするクライアントの数

SSIDに関連付けられているFAT AP、FIT AP、またはクライアントを表示するには、リストの番号をクリックします。

WLANの概要

WSMはWLANの概要を提供し、ネットワーク上のワイヤレスデバイスとクライアントのステータスと統計情報をすばやく把握できるようにします。

WLAN Managerには、ワイヤレスサービスホームページウィジェットとしてさまざまなデータを表示するいくつかの領域があります。

WLANの概要ページにアクセスするには、次の手順を実行します。

1. トップナビゲーションバーの**Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Overview**を選択します。

   WLAN Overviewが開きます。このページには、ワイヤレスデバイスとクライアントに関する統計情報とステータス情報が表示されます。
3. **Overview**ページにウィジェットを追加するには、ページの右上隅にある**Overview Customization**をクリックし、ウィジェットを追加します。
4. **Overview**ページからウィジェットを削除するには、ウィジェットの右上隅にある**Delete**アイコン をクリックします。

次の情報では、WLAN Overviewページの領域について説明します。

Shop Entry/Exitクライアント

図34に示すように、棒グラフには、クライアント数が最も多いTopNショップとそれぞれのクライアント番号が表示されます。

図34 Shop Entry/Exitクライアント

店舗名を表示するには、ヒントが表示されるまでバーの上にカーソルを置きます。

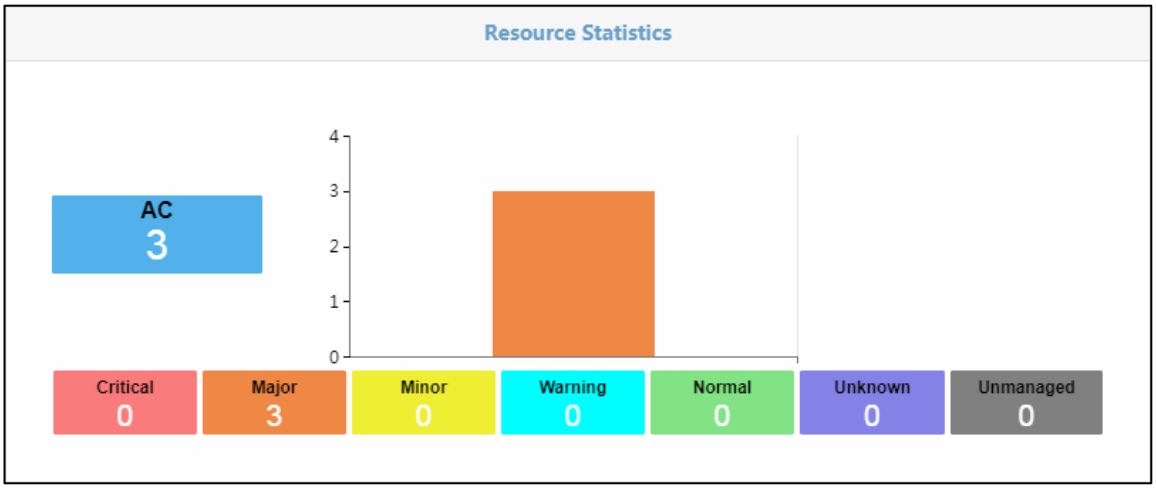
リソース統計情報

Resource Statistics領域には、AC、FIT AP、およびFAT APのアラーム統計情報が5秒間隔で1つずつヒストグラムで表示されます。

ACリソース統計情報

図35に示すように、ACリソース統計情報には、各アラームレベルのAC数が表示されます。

図35 リソース統計情報

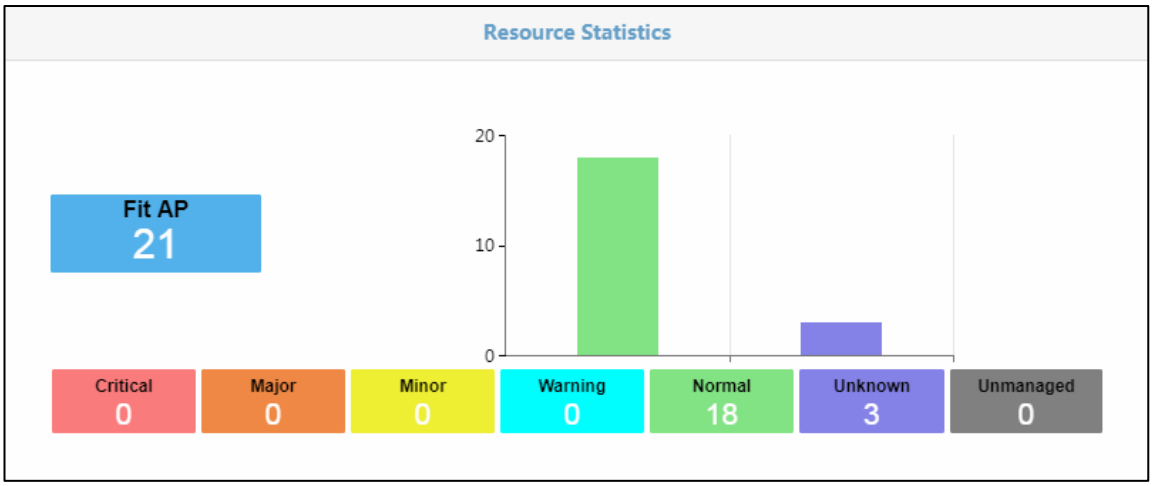


- 縦軸は、ワイヤレスネットワーク内のACの数を示します。ヒストグラムの下にある色付きの四角形は、各アラームレベルのACの数を示します。
- それぞれの色は、異なるアラームレベルを反映しています。
  - Critical
  - Major
  - Minor
  - Warning
  - Normal
  - Unknown
  - Unmanaged
- 色付きの四角形をクリックすると、そのアラームレベルのすべてのACを表示できます。

FIT APリソース統計情報

図36に示すように、FIT APリソース統計情報は、各アラームレベルにFIT APの数を示します。

図36 FIT APリソースの統計情報

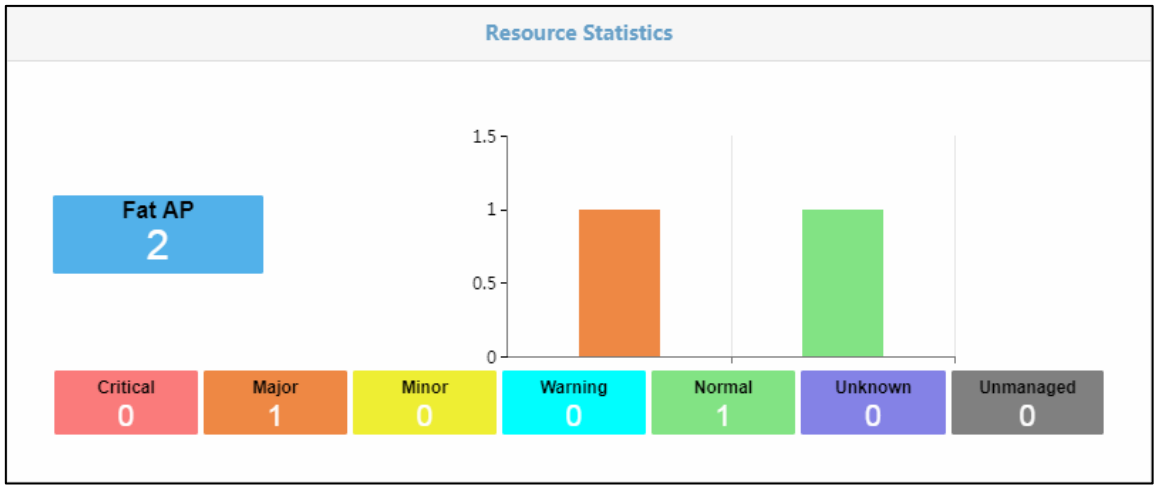


- 縦軸は、ワイヤレスネットワークにFIT APの数を示します。ヒストグラム内の色付きの正方形は、各アラームレベルにFIT APの数を示します。
- それぞれの色は、異なるアラームレベルを反映しています。
  - Critical
  - Major
  - Minor
  - Warning
  - Normal
  - Unknown
  - Unmanaged
- 色付きの四角形をクリックすると、そのアラームレベルに適合するすべてのAPを表示できます。

FAT APリソース統計情報

図37に示すように、FAT APリソース統計情報には、各アラームレベルのFAT APの数が表示されます。

図37 FAT APリソースの統計情報



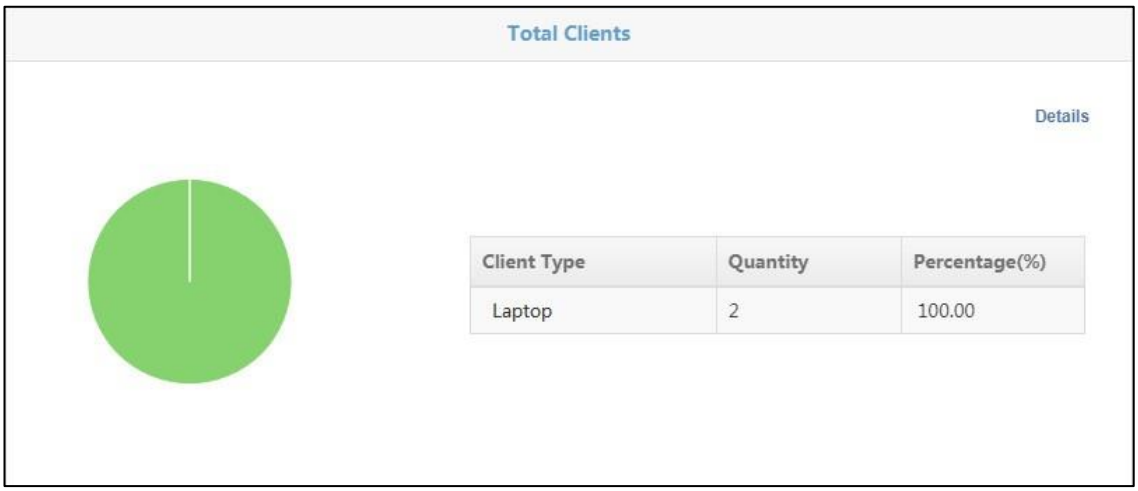
- 縦軸は、ワイヤレスネットワーク内のFAT APの数を示します。ヒストグラム内の色付きの正方形は、各アラームレベルのFAT APの数を示します。
- それぞれの色は、異なるアラームレベルを反映しています。
  - Critical
  - Major
  - Minor
  - Warning
  - Normal
  - Unknown
  - Unmanaged
- 色付きの四角形をクリックすると、そのアラームレベルのすべてのFAT APを表示できます。

クライアント合計

Total Clients領域には、タイプ、ベンダー、およびオペレーティングシステムごとのクライアントの合計が、5秒間隔で1つずつ円グラフとフォームに表示されます。

クライアントタイプ別のクライアント合計

図38 クライアントタイプ別のクライアントの合計



- 色はクライアントの種類を表します。
- フォームには次の情報が表示されます。
  - **Client Type**:クライアントのタイプ。
  - **Quantity**:タイプのクライアント数。
  - **Percentage**:タイプのクライアントの割合。
- このフォームには、最大5つのクライアントタイプを表示できます。すべてのクライアントタイプに関する情報を表示するには、右上隅の**Details**をクリックします。

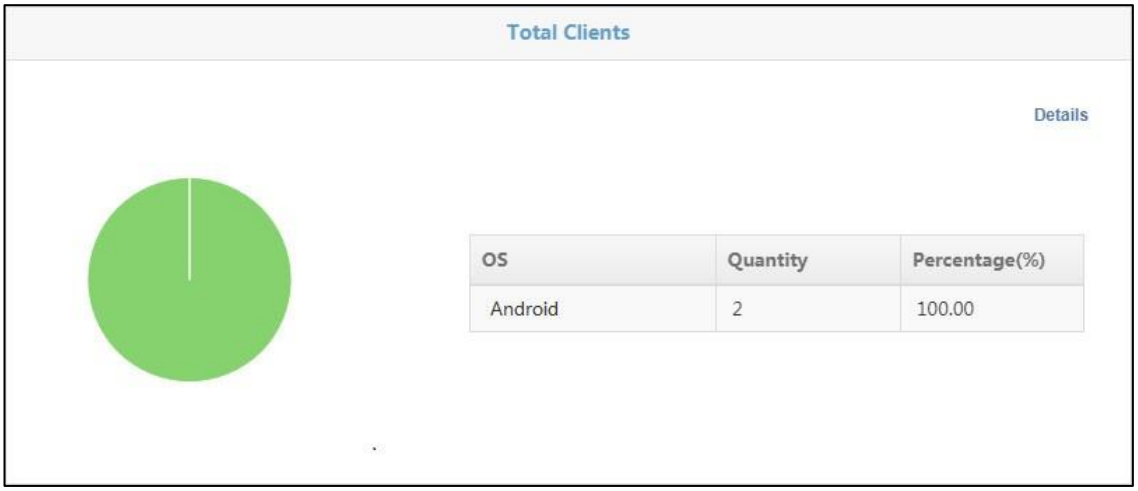
ベンダー別クライアント合計

図39 ベンダー別の総クライアント数

- 色はベンダーを表します。
- フォームには次の情報が表示されます。
  - **Vendor**:クライアントのベンダー。
  - **Quantity**:ベンダーのクライアント数。
  - **Percentage**:ベンダーのクライアントの割合。
- このフォームには、最大5つのベンダーを表示できます。すべてのベンダーに関する情報を表示するには右上隅に詳細が表示されます。

オペレーティングシステム別クライアント数

図40 オペレーティングシステム別のクライアントの合計



- 色はオペレーティングシステムを表します。
- フォームには次の情報が表示されます。

- **OS**:クライアントのオペレーティングシステム。
- **Quantity**:オペレーティングシステムを使用するクライアントの数。
- **Percentage**:オペレーティングシステムを使用するクライアントの割合。

- このフォームには、最大5つのオペレーティングシステムを表示できます。すべてのクライアントオペレーティングシステムに関する情報を表示するには、右上隅のDetailsをクリックします。

クライアント数

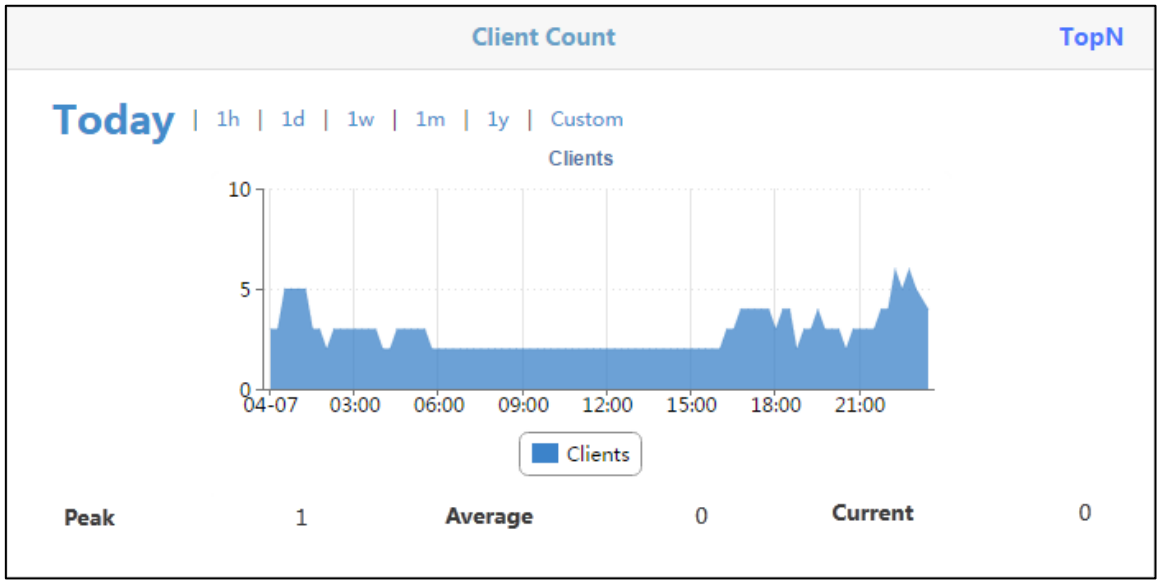
Client Count領域には、次の情報が表示されます。

- **Client count**
- **Client count details**
- **TopN clients**

クライアント数の表示

図41の傾向グラフは、特定の時間範囲内のオンラインクライアント数の変化を示しています。

図41 クライアント数



横軸は時間範囲を表し、縦軸はクライアント数を表します。横軸の時間間隔は、指定した時間範囲に自動的に調整されます。

特定の時間範囲内のオンラインクライアント数の変化を表示できます。オプションは次のとおりです。**Today**、**1h**、**1d**、**1w**、**1m**、**1y**、および**Custom**です。

Customを選択した場合は、開始時刻と終了時刻を設定します。

1. **Custom**をクリックします。
2. 表示された**Custom**ウィンドウで、開始時間と終了時間を入力するか、表示されたカレンダーから開始時間と終了時間を選択します(YYYY-MM-DD hh:mmフォーマット)。終了時間は開始時間より後である必要があります。
3. **Query**をクリックします。

   指定した時間範囲内のオンラインクライアント数の変化が、トレンドグラフに表示されます。

クライアント数の詳細の表示

1. **Client Count**トレンドグラフの上部にある**Clients**をクリックします。

   Detailsウィンドウが開きます。このウィンドウには、特定の時間におけるオンラインクライアントの数がリストで表示されます。

2. ウィンドウを閉じるには、**Close**アイコンをクリックします。

TopNクライアントの表示

TopN Clientsページを図42に示します。

TopN Clientsページには、次のリストがあります。

- **TopN Locations by Clients**

  このリストには、クライアント数が最も多いTopNロケーションビューが降順で表示されます。ロケーションビューの名前をクリックすると、ロケーションビューに含まれるサブビューおよびデバイスが表示されます。クライアントの数をクリックすると、ロケーションビューにクライアントのリストが表示されます。

- **TopN SSIDs by Clients**

  このリストには、クライアント数が最も多いTopN SSIDが降順で表示されます。クライアント数をクリックすると、そのSSIDを使用してネットワークにアクセスするクライアントのリストが表示されます。

- **TopN APs by Clients**

  このリストには、クライアント数が最も多いTopN APが降順で表示されます。APラベルをクリックすると、APに関する詳細情報が表示されます。クライアントの数をクリックすると、APを介してワイヤレスネットワークにアクセスするクライアントが表示されます。

- **TopN Locations by Association Failures**

  このリストには、過去24時間のアソシエーションの失敗数が最も多いTopNロケーションビューが降順で表示されます。ロケーションビューの名前をクリックすると、そのロケーションビューに含まれているサブビューおよびデバイスが表示されます。

- **TopN APs by Association Failures**

  このリストには、過去24時間のアソシエーション障害が最も多かったTopN APが降順で表示されます。APをクリックすると、そのAPに関する詳細情報が表示されます。

TopNクライアントに関する情報を表示するには、次の手順を実行します。

1. **Client Count**トレンドグラフの右上にあるTopNをクリックします。

   TopN Clientsページが開きます。

2. ページの右上にあるTopNリストから番号を選択します。オプションは次のとおりです。
   - **5**
   - **10**
   - **20**
   - **50**
   - **100**

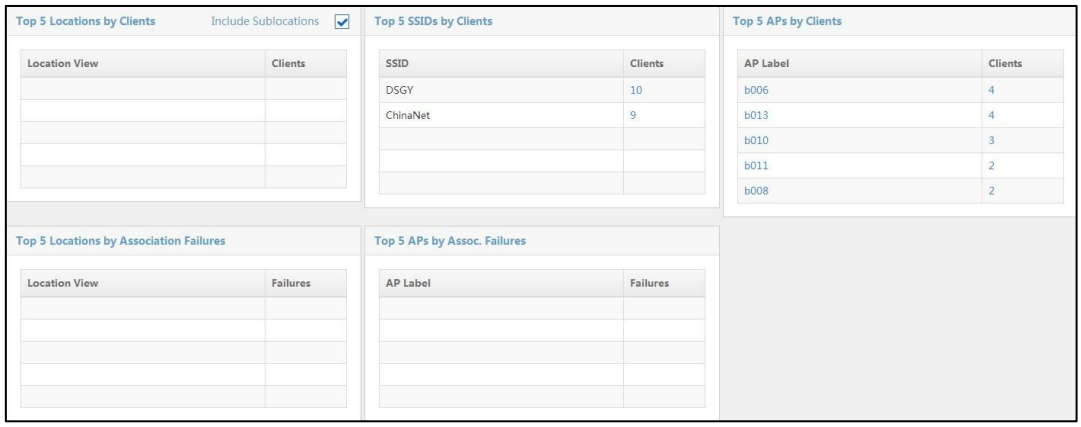
   デフォルト値は**20**です。ページがリフレッシュされ、クライアント数が最も多いTopNロケーションビュー、TopN SSID、およびTopN AP、アソシエーション失敗数が最も多いTopNロケーションビュー、およびアソシエーション失敗数が最も多いTopN APが表示されます。

3. すべてのサブロケーションビューでクライアントをカウントするには、**Top 5 Locations by**

Clientsリストの右上にある**Including Sublocations**を選択します。

4. リスト上のロケーションビューの名前をクリックすると、そのビューに含まれるサブビューとデバイスが表示されます。
5. **Back**をクリックして、**WLAN Overview**ページに戻ります。

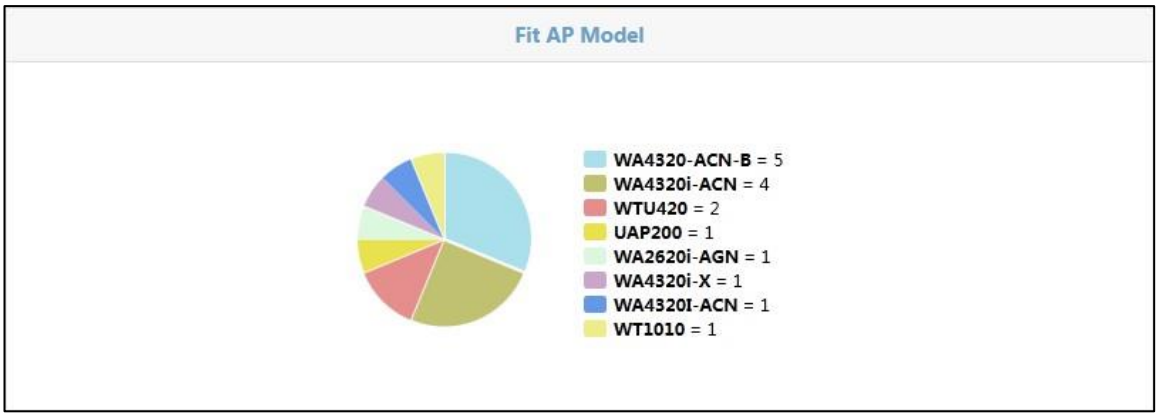
図42 TopNクライアント



FIT APモデル

図43に示すように、**FIT AP Model**領域には、WLAN内のすべてのAPモデルと各モデルのAPの数が表示されます。

図43 FIT APモデル



- 色はAPモデルを表します。モデルのAPの数は円グラフの右側に表示されます。
- カーソルを色の上に置くと、APモデルとそのモデルのAP数を示すヒントが表示されます。
- 色をクリックして、FIT APリストを入力します。リストには、APモデルのFIT APに関する情報が表示されます。

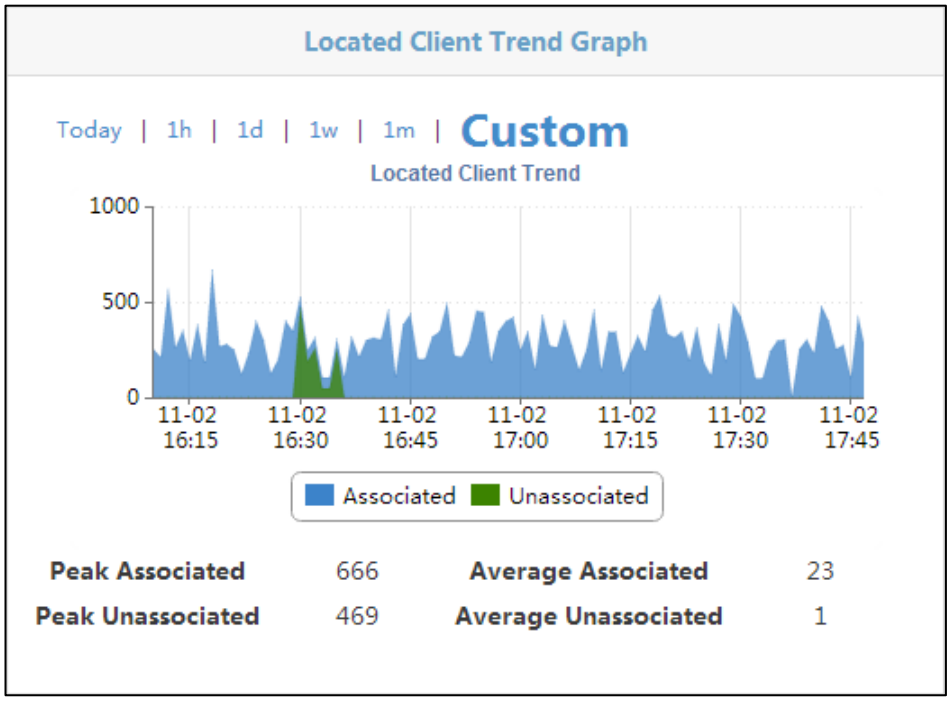
Located Client Trendグラフ

Located Client Trend Graphには、検出されたクライアントの傾向と詳細が表示されます。

トレンドグラフの表示

この領域には、図44に示すように、関連付けられているクライアントと関連付けられていないクライアントの合計数が面グラフで表示され、ピーク値と平均値が示されます。

図44 Located Client Trendグラフ



横軸は時間を表し、縦軸はクライアント数を表します。横軸の時間間隔は、指定した時間範囲に自動的に調整されます。

特定の時間範囲内で検出されたクライアント数の変化を表示できます。オプションは次のとおりです。**Today**、**1h**、**1d**、**1w**、**1m**、**1y**、および**Custom**です。

カスタムを選択した場合は、開始時刻と終了時刻を設定します。

1. **Custom**をクリックします。
2. 表示された「カスタム」ウィンドウで、開始時間と終了時間を入力するか、表示されたカレンダーから開始時間と終了時間を選択します(YYYY-MM-DD hh:mmフォーマット)。終了時間は開始時間より後である必要があります。
3. **Query**をクリックします。

   指定した時間範囲内で検出されたクライアント数の変化が、トレンドグラフに表示されます。

検索されたクライアントの詳細の表示

Located Client TrendグラフでLocated Client Trendsをクリックすると、選択した時間範囲に関連付けられているクライアントと関連付けられていないクライアントの詳細リストが表示されます。リストを閉じるには、Closeアイコンをクリックします。

APの帯域幅

APの帯域幅には次の情報が含まれます。

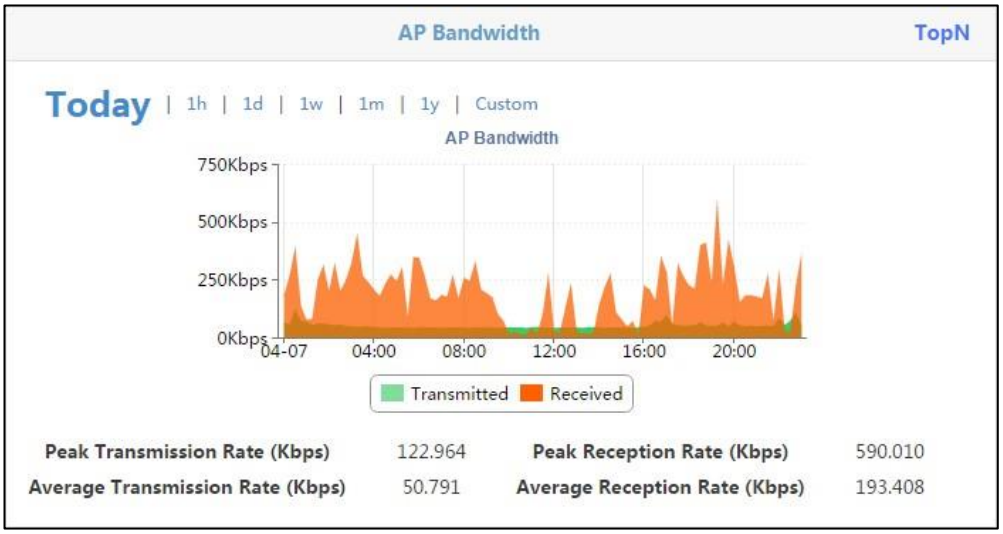
- AP Bandwidth
- AP Bandwidth details

- TopN traffic

APの帯域幅の表示

図45のトレンドグラフは、特定の時間範囲内における無線側のAPの送信レートと受信レートの変化を示しています。

図45 APの帯域幅



横軸は時間範囲を表し、縦軸はクライアント数を表します。横軸の時間間隔は、指定した時間範囲に自動的に調整されます。

特定の時間範囲内の無線側のAPの送信レートと受信レートの変化を表示できます。オプションは、**Today**、**1h**、**1d**、**1w**、**1m**、**1y**、**Custom**です。

Customを選択した場合は、開始時刻と終了時刻を設定します。

1. **Custom**をクリックします。

   表示された「カスタム」ウィンドウで、開始時間と終了時間を入力するか、表示されたカレンダーから開始時間と終了時間を選択します(YYYY-MM-DD hh:mmフォーマット)。終了時間は開始時間より後である必要があります。

2. **Query**をクリックします。

   トレンドグラフには、指定した時間範囲内での無線側のAPの送信レートと受信レートの変化が表示されます。

AP帯域幅の詳細の表示

1. トレンドグラフの上部にある**AP Bandwidth**をクリックします。

   Detailsウィンドウが開きます。このウィンドウには、特定の時刻におけるAPの送信レートと受信レートが表示されます。

2. ウィンドウを閉じるには、**Close**アイコンをクリックします。

TopNトラフィック統計情報の表示

TopN Trafficページを図46に示します。

TopN Trafficページには、次のリストがあります。

- **TopN AP Traffic – Today**

  このリストには、トラフィックが最も多いTopN APが降順で表示されます。このリストには、送信トラフィック、受信トラフィック、および合計トラフィックの統計情報が表示されます。
- **TopN Location Traffic – Today**

  このリストには、トラフィックが最も多いTopNロケーションビューが降順で表示されます。このリストには、送信トラフィック、受信トラフィック、および合計トラフィックの統計情報が表示されます。
- **Current AP Receive Rate TopN**

  このリストには、受信レートが最も高いTopN APと、それぞれの受信レートが降順で表示されます。
- **Current AP Transmit Rate TopN**

  このリストには、送信レートが最も高いTopN APと、それぞれの送信レートが降順で表示されます。

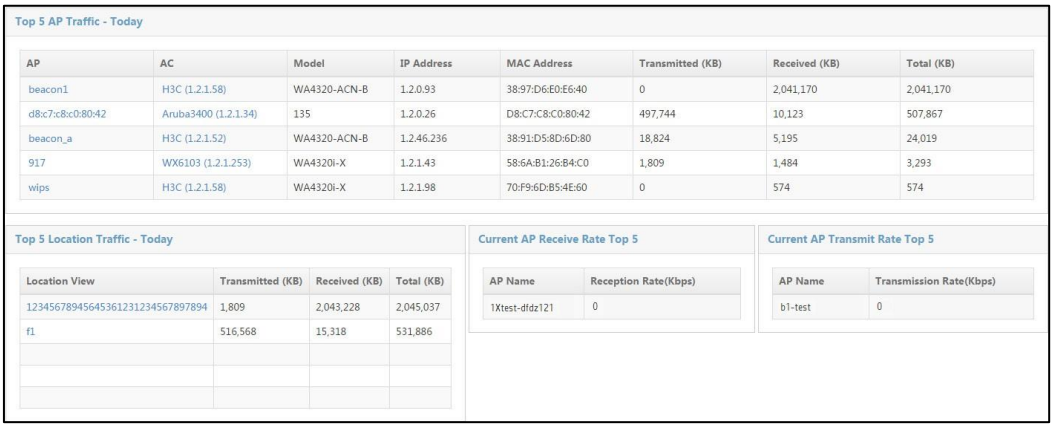
TopNトラフィック統計情報を表示するには、次の手順を実行します。

1. **AP Bandwidth**トレンドグラフの右上にある**TopN**をクリックします。

   TopN Trafficページが開きます。
2. ページの右上にある**TopN**リストから番号を選択します。

   使用可能なオプションは**5、10、20、50、および100**です。デフォルト値は20です。ページがリフレッシュされ、トラフィックが最も多いTopN APおよびロケーションビューが表示されます。
3. **Back**をクリックして、**WLAN Overview**ページに戻ります。

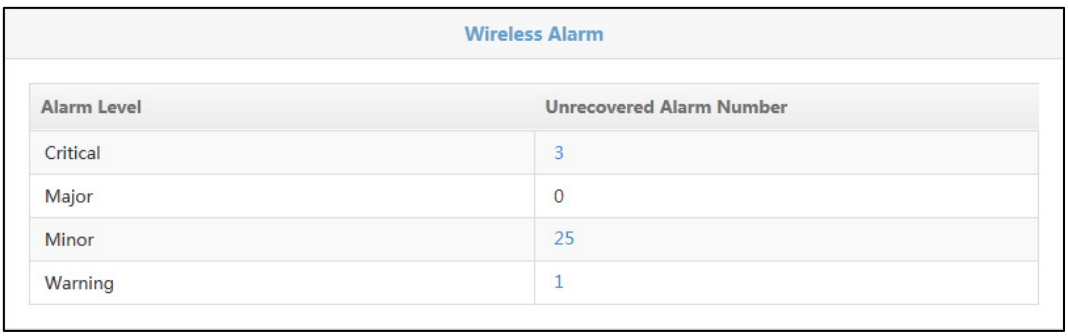
図46: TopNトラフィック



ワイヤレスアラーム

図47に、ワイヤレスアラームページを示します。このページには、現在のネットワーク上のワイヤレスサービスによって生成された未回復アラームに関するアラームレベルの統計情報が表示されます。

図47 ワイヤレスアラーム



このページには、次の情報が表示されます。

- **Alarm Level**: アラームレベルは次のとおりです。
  - **Critical**
  - **Major**
  - **Minor**
  - **Warning**
- **Alarm Number**: 特定のアラームレベルの未回復アラームの数。

アラーム番号をクリックすると、IMCの特定のアラームレベルのワイヤレスデバイス上のすべての未回復アラームが表示されます。

未回復のワイヤレスアラーム

Unrecovered Wireless Alarmsページを図48に示します。

このページには、次の情報が表示されます。

- **Alarm Level**:アラームレベルは次のとおりです。
  - **Critical**
  - **Major**
  - **Minor**
  - **Warning**
- **Alarm description**:アラームの説明。
- **Alarm time**:アラームが生成された時刻。

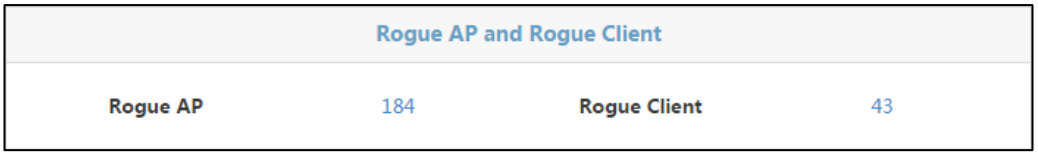
図48 未回復のワイヤレスアラーム

- ページの右上にある**TopN**リストから番号を選択します。オプションは5と10です。
- **More…**をクリックして、ワイヤレスサービスアラームページに入ります(「ワイヤレスサービスアラームの表示」を参照)。
- アラームの詳細情報を表示するには、アラームの説明をクリックします。アラーム情報ページの詳細については、「H3C IMC v7.3 Enterprise and Standard Platform Administrator Guide」を参照してください。

不正APと不正クライアント

Rogue AP and Rogue Clientページを図49に示します。

図49:不正なAPと不正なクライアント



このページには、不正なAPおよび不正なクライアントの数が表示されます。

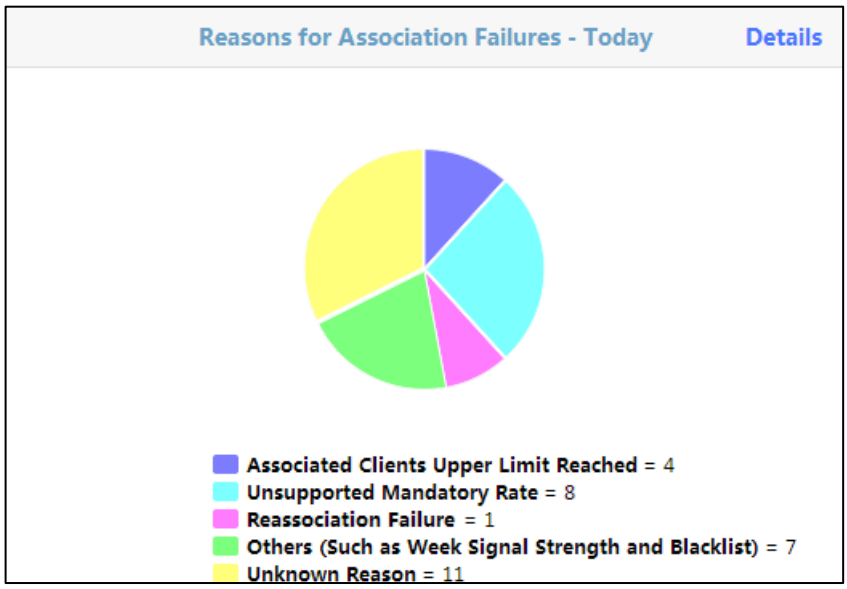
- **Rogue AP**の横の番号をクリックして、不正なAPのリストを表示します。
- **Rogue Client**の横の番号をクリックすると、不正クライアントのリストが表示されます。

関連付け失敗の理由 - Today

Reasons for Association Failures-Todayページを図50に示します。このページには、示します。このページには、アソシエーション失敗の理由が円グラフで表示されます。数値は、本日00:00から現在の時間までの各理由に関連付けられた失敗の数を表します。失敗の理由には次のものがあります。

- Associated client upper limit reached
- Unsupported mandatory rate
- Reassociation failure
- Others (such as weak signal strength and blacklist).
- Unknown reason

図50 アソシエーション失敗の理由 - Today



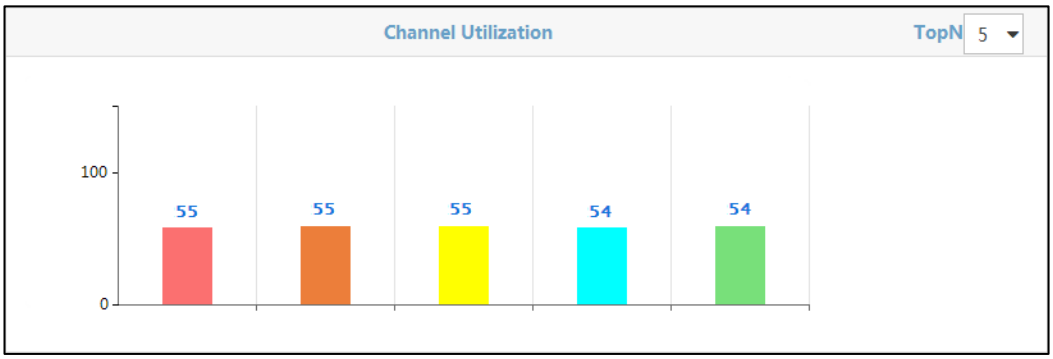
ページの右上隅にあるDetailsをクリックします。各理由に関連付けられた障害の数が、個々のAPについて表示されます。

図51 詳細ページ

チャネル使用率

図52に示すように、棒グラフはワイヤレスネットワークにおけるTopNチャネルの使用率を示しています。右上隅のTopNリストから5または10を選択できます。

図52 チャネル使用率

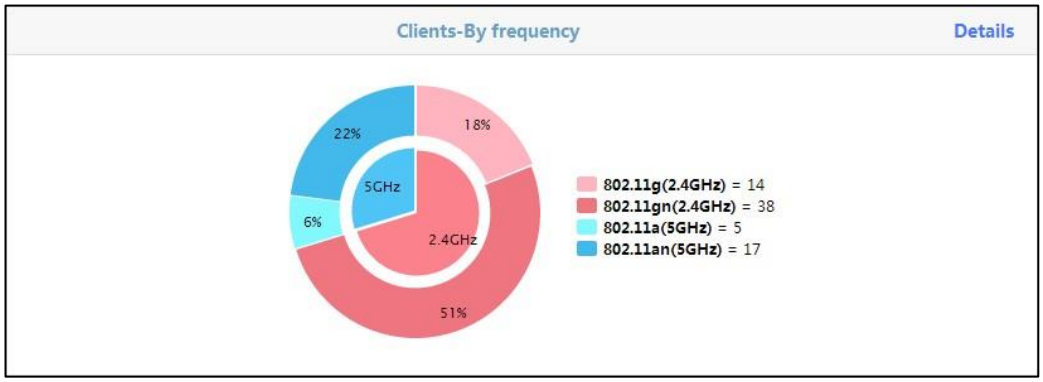


ページの右上にあるTopNリストから番号を選択します。オプションは5と10です。

クライアント - 頻度別

Clients-By Frequencyページには、5GHzおよび2.4GHz帯域と各無線タイプの分布がドーナツグラフで表示され、無線タイプごとに関連付けられたクライアントの数が表示されます。

図53 クライアント - 頻度別



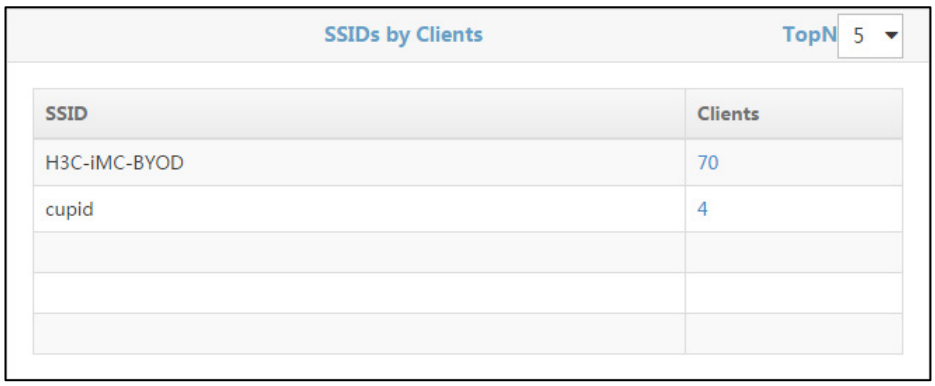
内側のリングは5GHzおよび2.4GHz帯域の分布を示します。外側のリングは各無線タイプの分布を示します。ドーナツグラフの右側のリストには、各無線タイプに関連付けられたクライアントの数が表示されます。

各無線タイプに関連付けられているクライアントの数を表示するには、右上隅にあるDetailsをクリックします。

クライアントごとのSSID

クライアントごとのSSIDページを図54に示します。このページには、最も多くのクライアントが関連付けられているSSIDと、各SSIDに関連付けられているクライアントの数が表示されます。

図54 クライアントごとのSSID



- ページの右上にあるTopNリストから番号を選択します。オプションは5と10です。
- このリストには次の情報が表示されます。
  - **SSID**: SSID名。
  - **Clients**: SSIDに関連付けられているクライアントの数。
- 番号をクリックすると、SSIDに関連付けられたクライアントに関する情報が表示されます。

フルスクリーンモニタ

フルスクリーンモニタでは、カスタマイズされたワイヤレスサービスの統計情報がダッシュボードに表示されます。これにより、ユーザーモニタの操作性が向上します。**WLAN Overview**ページをフルスクリーンで表示するには、ページの右上隅にあるフルスクリーンモニタをクリックします。

表示スタイルの設定

図55に示すように、WSMは、フルスクリーンモニタに対して、フラットスタイルと従来のスタイルの2つの表示スタイルを提供する。

図55 表示スタイルの設定

表示スタイルを設定するには:

1. 右上隅にある**Full Screen Configuration**をクリックします。
2. 表示内容のスタイルを選択して**OK**をクリックします。
3. 2番目のスタイル(従来のスタイル)が選択されている場合は、次の設定を行います。
   - **Title Name**: フルスクリーンページの名前を入力します。デフォルトの名前は**Wireless Device Monitoring**です。
   - **Selected Location Views**: 全画面表示ページのスクロール領域に表示するロケーションビューを選択します。
   - **Location**: 全画面表示ページの中央領域に表示する位置ビューを選択します。
   - **Include Sublocations**: サブロケーションビュー内のクライアントを、クライアント数(上位10位)のロケーションビュー領域に表示される統計に含めるかどうかを選択します。

フラットスタイルのフルスクリーンモニタ

クライアントのポジション分布

図56に示すように、クライアント位置分布は、ワイヤレスネットワーク内のクライアントの位置を表示します。クライアントのMACアドレス、ユーザー名、SSIDなどのクライアント情報を表示するには、クライアントのアイコンをクリックします。

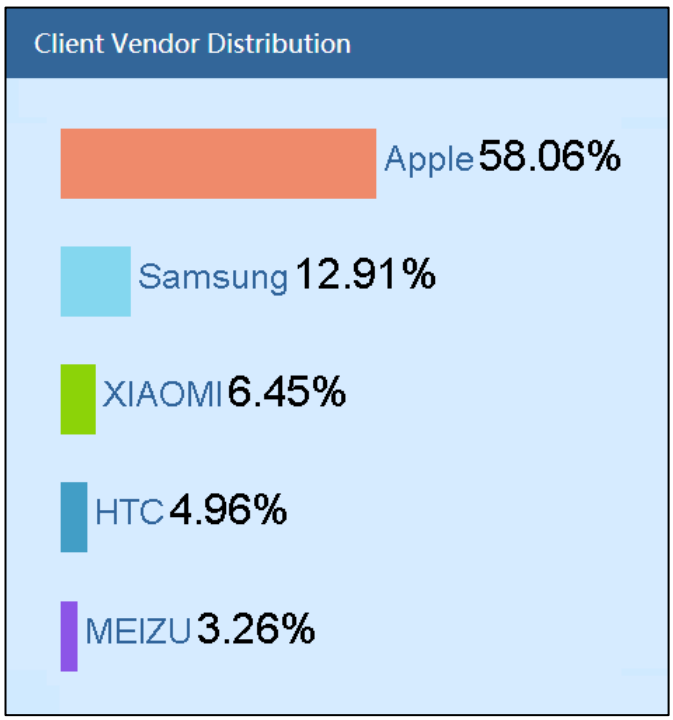
Setアイコンをクリックして、表示するロケーションビュートポロジーを選択します。

図56 クライアントの位置の分布

クライアントベンダーの分布

図57に示すように、クライアントベンダー分布は、ワイヤレスネットワーク内のクライアントに関するベンダー統計情報を提供します。

図57 クライアントベンダーの分布

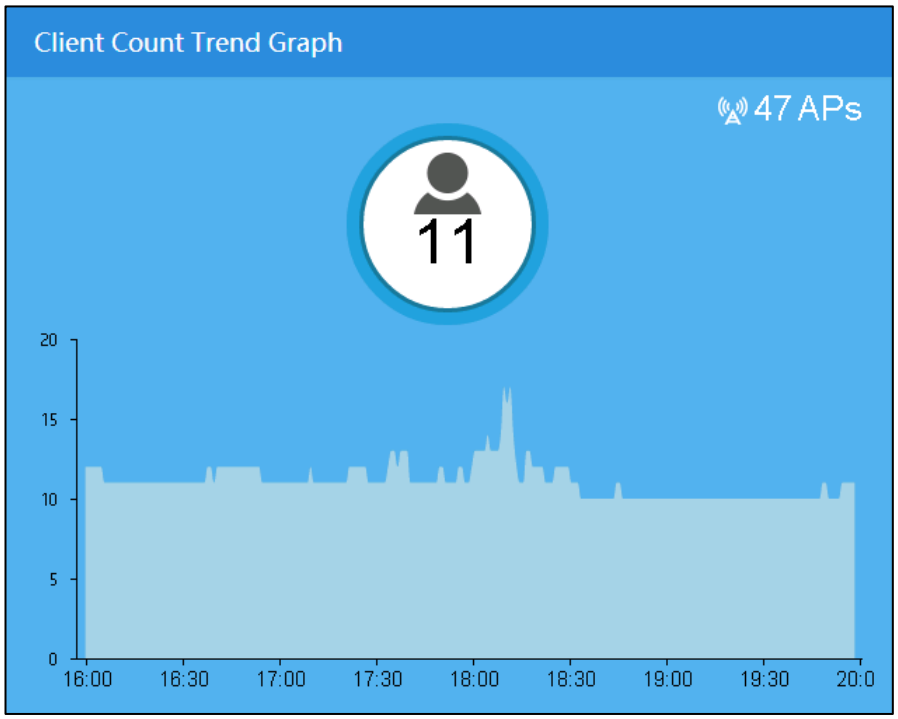


棒グラフは、ベンダー名とクライアントの割合を表します。

クライアント数のトレンドグラフ

図58に示すように、クライアント数トレンドグラフは、ワイヤレスネットワーク内のある期間におけるオンラインクライアント統計情報を提供します。

図58 クライアント数のトレンドグラフ

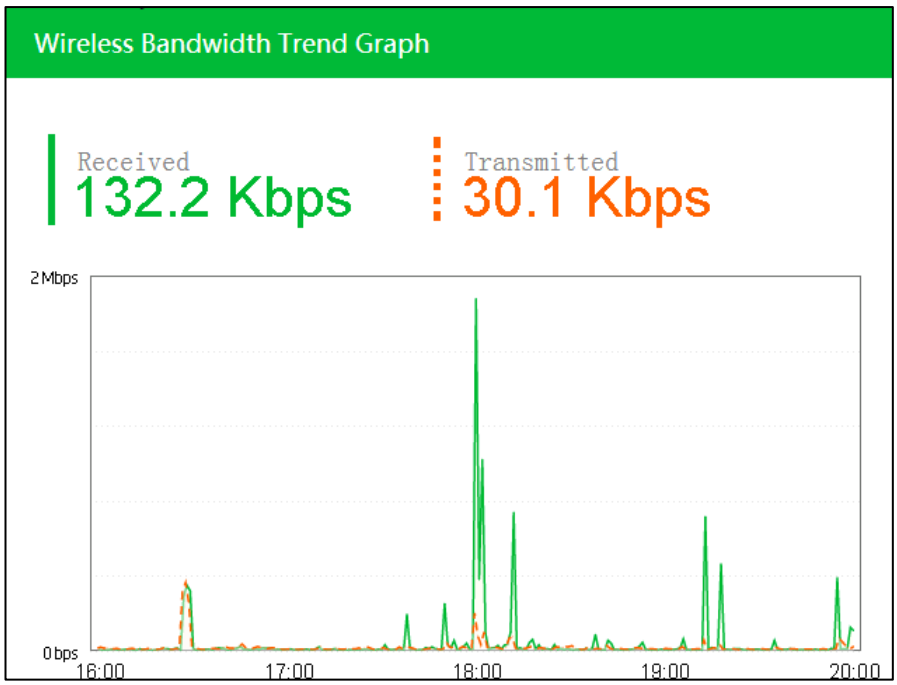


- 量座標は、現在のオンラインクライアントの数を表します。
- トレンドグラフの右上にある数字は、ワイヤレスネットワーク内のAPの数を表します。

ワイヤレス帯域幅のトレンドグラフ

図59に示すように、無線帯域幅トレンドグラフは、ある期間におけるAPの送受信レートを示します。

図59 Wireless Bandwidth Trendグラフ

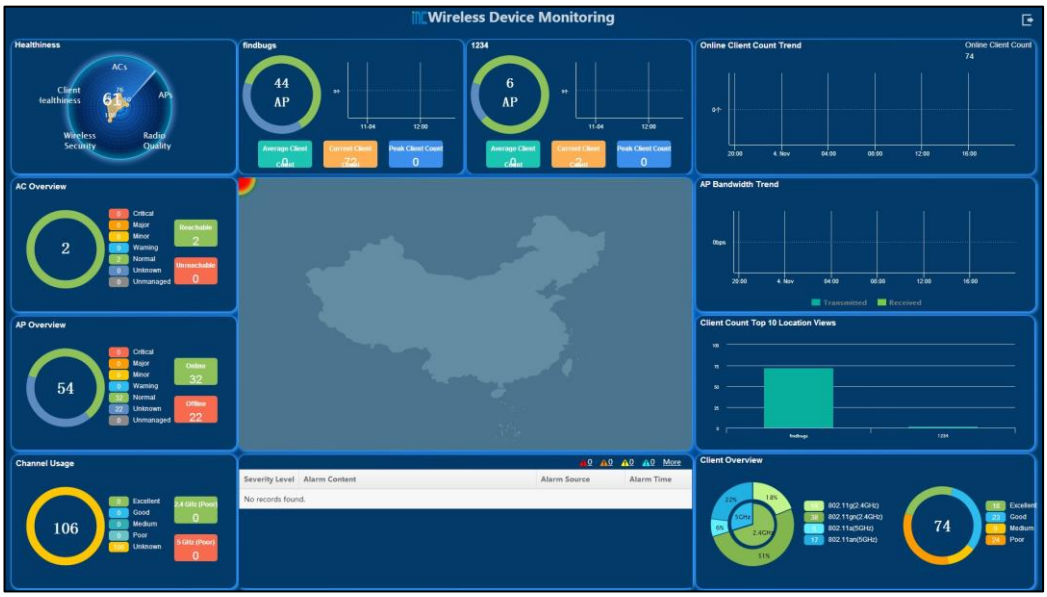


- 緑の数字は合計受信帯域幅を表し、緑の線はワイヤレスネットワーク内のある期間における受信レートの傾向を表します。
- 赤い数字は送信帯域幅の合計を表し、赤い線はワイヤレスネットワーク内のある期間における送信レートの傾向を表します。

従来型のフルスクリーンモニタ

図60に示すように、従来のスタイルのフルスクリーンモニタには、ネットワーク管理者がネットワーク動作ステータスを表示するために、ACおよびAPアラームとクライアント統計情報が表示されます。

図60 従来型のフルスクリーンモニタ



WLANの迅速な導入

WSMを使用すると、1つのページですべてのWLANパラメーターを設定して、WLANを迅速に展開できます。この機能は、Comwareベースをサポートします。

Comwareベースの高速WLAN展開

WLANパラメーターの設定

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Fast Deploy WLAN**を選択します。
3. **Comware Based**タブをクリックします。
4. **Fast Deploy WLAN**ページで、次のパラメーターを設定します。

   Basic Information

   - **SSID**: サービステンプレートの一意のSSIDを入力します。
   - 有効-サービステンプレートを有効にするには、このオプションを選択します。
   - **Bind Radio**: サービステンプレートがバインドされる無線タイプを選択します。オプションは次のとおりです。
     2.4GHz、**5GHz**、および**All**。
   - **Hide SSID**: このオプションを選択すると、FIT APによって送信されるビーコンフレーム内のSSIDが非表示になります。このパラメーターを選択すると、クライアントはビーコンフレームからSSIDを取得できず、ワイヤレスネットワークにアクセスする前にSSIDを設定する必要があります。このパラメーターを選択しないと、クライアントはビーコンフレームからSSIDを取得してワイヤレスネットワークにアクセスできます。
   - **VLAN**: サービステンプレートがバインドされるVLANを指定します。WLANにアクセスするクライアントは、自動的にVLANに参加します。

   Security Information

   Encryption Mode: 暗号化モードを選択します。オプションは、**Clear**、**WEP**、**WPA(Personal)**、**WPA2(Personal)**、**WPA(Enterprise)**、および**WPA2(Enterprise)**です。

   - **Clear**: データフレームは暗号化されません。
   - **WEP**: WEP暗号化が使用されます。次のパラメーターを設定します。
     - **Cipher Suite**: 暗号スイートを選択します。オプションはWEP40、WEP104、およびWEP128で、セキュリティ強度は昇順です。
     - **Key**: キーを入力します。キーの長さは暗号スイートによって異なります。キーの長さは、WEP40、WEP104およびWEP128キーに対して、それぞれ5文字、13文字および16文字の英数字です。
     - **Confirm Key**: キーを再入力します。
     - **Key Index**: キーインデックスを入力します。WEPは1～4個のキーインデックスをサポートします。
   - **WPA**(パーソナル)または**WPA2**(パーソナル)-PSK認証が使用されます。次のパラメーターを設定します。
     - **PSK**: 事前共有キーを8～63文字の範囲で入力します。
     - **Confirm PSK**: PSKを再入力します。

- **WPA**(エンタープライズ)または**WPA2**(エンタープライズ)-802.1X認証が使用されます。次のパラメーターを設定します。
  - **Domain**: ドメインを選択します。ドメインを構成するには、Domainをクリックします。詳細は、「ドメインの構成」を参照してください。

Extension Information

- **Max Clients**: WLANで許可される最大オンラインクライアント数を入力します。
- **Layer 2 Isolation**: レイヤ2分離を有効にするには、このオプションを選択します。このパラメーターは、ACで実行される**user-isolation vlan**コマンドと組み合わせて設定する必要があります。この機能が有効になっている場合、許可MACアドレスリスト内のクライアントは、同じVLAN内の他のクライアントと通信できます。

5. **AP List**フィールドで、**Add**をクリックします。
6. 表示されるダイアログボックスで、APをクエリーするための次のクエリー基準を1つまたは複数指定します。
   - **Device Label**: APのデバイスラベルを入力します。WSMは、このフィールドのファジーマッチングをサポートします。
   - **Location View**: APのロケーションビューを選択します。
   - **Serial Number**: FIT APのシリアル番号を入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
   - **Model**: APモデルを選択します。オプションは**Unlimited**で、すべてのAPモデルをWSMで使用できます。
   - **IP Address**: FIT APの部分的または完全なIPv4アドレスを入力します。WSMは、このフィールドのファジーマッチングをサポートします。
   - **Online Status**: FIT APのオンラインステータスを選択します。オプションは、**Unlimited**、**Online**、および**Offline**です。
   - **AC**: FIT APを管理するACを選択します。オプションは**Unlimited**およびWSM内のすべてのACです。空のフィールドまたは**Unlimited**に設定されたフィールドは、問合せ基準として機能しません。
7. **Query**をクリックします。

   リストには、クエリー基準に一致するすべてのAPが表示されます。

   クエリー基準をクリアして、別のサービステンプレートにバインドされていないすべてのAPを表示するには、**Reset**をクリックします。
8. 追加するAPを選択して、**OK**をクリックします。

   選択したすべてのAPがAPリストに表示されます。
9. **OK**をクリックします。

RADIUSポリシーの設定

次の情報では、RADIUSポリシーの設定について説明します。

RADIUSポリシーの追加

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Fast Deploy WLAN**を選択します。
3. **Security Information**フィールで、**Domain**をクリックします。
4. **Domain Configuration**ページで、**RADIUS Policy**をクリックします。
5. **RADIUS Policy**ページで、**Add**をクリックします。

6. **Add RADIUS Policy**ページで、次のパラメーターを設定します。
   - **RADIUS Policy** : RADIUSポリシー名を入力します。
   - **Server Type**: サーバータイプを選択します。オプションは**Extended**および**Standard**です。
   - **Primary Authentication**: プライマリ認証サーバーのIPアドレスを入力します。
   - **Secondary Authentication**: バックアップ認証サーバーのIPアドレスを入力します。
   - **Primary Accounting:** プライマリアカウンティングサーバーのアドレスを入力します。
   - **Secondary Accounting:** バックアップアカウンティングサーバーのアドレスを入力します。
   - **Authentication Key**: 認証用のキーを入力します。
   - **Confirm Authentication Key**: 認証用のキーを再入力します。
   - **Accounting Key**: アカウンティングのキーを入力します。
   - **Confirm Accounting Key**: アカウンティング用のキーを再入力します。
7. **OK**をクリックします。

RADIUSポリシーの変更

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Fast Deploy WLAN**を選択します。
3. **Security Information**フィールドで、**Domain**をクリックします。
4. **Domain Configuration**ページで、**RADIUS Policy**をクリックします。
5. **RADIUS Policy**ページで、RADIUSポリシーの**Modify**アイコンをクリックします。
6. 開いたページで、必要に応じてRADIUSポリシーパラメーターを変更します。「RADIUSポリシーの追加」を参照してください。
7. **OK**をクリックします。

RADIUSポリシーの削除

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Fast Deploy WLAN**を選択します。
3. **Security Information**フィールドで、**Domain**をクリックします。
4. **Domain Configuration**ページで、**RADIUS Policy**をクリックします。
5. **RADIUS Policy**ページで、RADIUSポリシーの**Delete**アイコンをクリックします。

   確認ダイアログボックスが開きます。
6. **OK**をクリックします。

ドメインの構成

次の情報は、ドメイン構成を示しています。

ドメインの追加

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Fast Deploy WLAN**を選択します。
3. **Security Information**フィールドで、**Domain**をクリックします。
4. **Domain Configuration**ページで、**Add**をクリックします。
5. **Add Domain**ページで、次のパラメーターを設定します。
   - **Domain Name**: ドメイン名を入力します。

- **RADIUS Policy**: RADIUSポリシーを選択します。詳細は、「RADIUSポリシーの構成」を参照してください。

6. **OK**をクリックします。

ドメインの変更

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Fast Deploy WLAN**を選択します。
3. **Security Information**フィールドで、**Domain**をクリックします。
4. **Domain Configuration**ページで、ドメインの**Modify**アイコンをクリックします。
5. 開いたページで、必要に応じてドメインパラメーターを変更します。「ドメインの追加」を参照してください。
6. **OK**をクリックします。

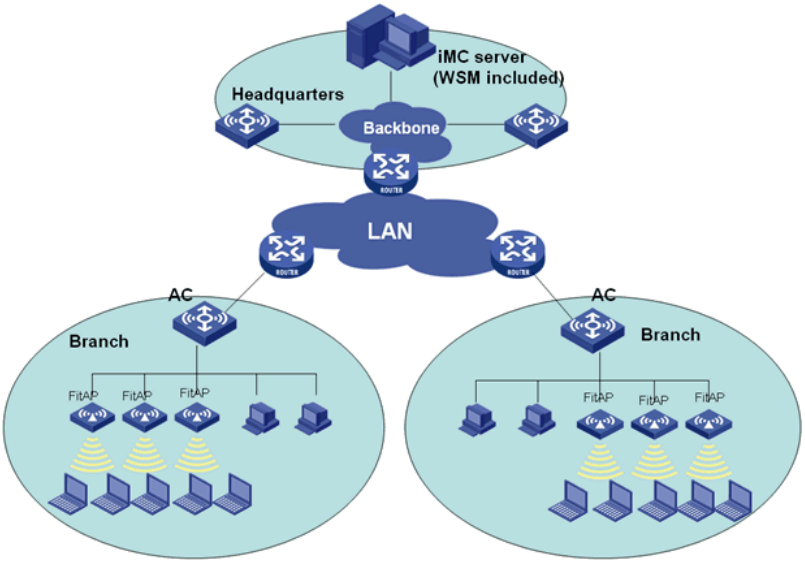
ドメインの削除

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Fast Deploy WLAN**を選択します。
3. **Security Information**フィールドで、**Domain**をクリックします。
4. **Domain Configuration**ページで、ドメインの**Delete**アイコンをクリックします。確認のダイアログボックスが開きます。
5. **OK**をクリックします。

Comwareベースのアクセスコントローラの管理

WSMを使用すると、管理者はACを介してAC+FIT APネットワークを作成および管理できます。IMC WSMは、IMCプラットフォームに追加されたすべてのACを自動的に管理します。

図62 AC+FIT APネットワーク



WSMで新しいAC+FIT APネットワークを作成する前に、次のタスクを実行します。

- ネットワークアクセスサービスを提供するようにACを設定します。
- FIT APをアクセスデバイスに接続し、FIT APとACが相互に到達できることを確認します。
- ACでSNMPコミュニティを設定し、ACをIMCプラットフォームに追加します。ベスト

プラクティスとして、次の手順を使用してAC+FIT APネットワークを管理します。

1. (任意)FIT APグループを追加し、FIT APをグループに分類します。の詳細については FIT APグループの設定については、「FIT APテンプレートの管理」を参照してください。
2. ACのグローバルパラメーターを構成します。詳細は、「ACグローバルパラメーターの構成」を参照してください。
3. (任意)ACの無線ポリシーを追加し、無線が正しく動作できるように各管理対象APの無線に無線ポリシーをバインドします。詳細については、「無線ポリシーの設定」を参照してください。
4. (任意)AC上の複数の無線に対して同じパラメーターをバッチで設定して、繰り返し操作を減らし、効率を向上させます。詳細については、「バッチでの無線の設定」を参照してください。
5. ACのWLAN論理インターフェースを追加し、それらのポートセキュリティモードおよびVLANを変更します。詳細については、「WLAN論理インターフェースの設定」を参照してください。
6. ACのサービスポリシーを追加し、サービスポリシーをACのWLAN論理インターフェースにバインドし、サービスポリシーをFIT APの無線にバインドして、FIT APが無線サービスを提供できるようにします。詳細については、「サービスポリシーの設定」を参照してください。

既存のワイヤレスネットワークを管理するには、WSMでAC+FIT APネットワークを作成せずに、WSMでACを管理するだけで済みます。現在のWSMバージョンでは、一部の機能のみがComware 7 ACで使用できます。

ACリストの表示

AC Listページには、IMC内のすべての管理対象ACに関する情報が表示

されます。AC Listページでは、次の機能にもアクセスできます。

- サービスポリシーの設定。
- 無線ポリシーの設定。
- ワイヤレス論理インターフェースの設定。
- MPポリシーの管理。
- メッシュプロファイルの管理
- メッシュインターフェースの管理

- ACリストを表示するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。

   AC ListページにすべてのACが表示されます。

   AC List

   - **Status** : ACの現在のアラームステータス。
   - **Device Label**: IMCプラットフォームでACを識別するデバイスラベル。ACのデバイスラベルをクリックすると、その詳細が表示されます。

     アイコンのラベルが付いたデバイスは、中央ACを表します。中央ACによって管理されているローカルACをその概要情報ページで表示したり、無線デバイストポロジー内の中央ACとローカルAC間の接続を表示したりできます。
   - **Model**: ACのモデル。
   - **IP Address**: ACの管理IPアドレス。
   - **Total APs**: ACによって管理されるFIT APの合計数。数値をクリックすると、すべての管理FIT APが表示されます。
   - **Online APs**: ACによって管理されているオンラインFIT APの数。この数をクリックすると、管理されているすべてのオンラインFIT APが表示されます。
   - **Online Clients**: ACによって管理されるFIT APに関連付けられているクライアントの数。この数をクリックすると、すべてのオンラインクライアントが表示されます。
   - **Last Sync Time**: AC設定が最後に同期された時刻。
   - **Sync Result**: 最後の同期結果: **Succeeded**、**Synchronizing**、または**Failed**。
   - **Operation**: ACの**Operation**アイコン…をクリックします。

     Operationメニューには、次の操作タスクがあります。

     - **Service Policy**
     - **Radio Policy**
     - **FIT AP List**
     - **Wireless Logical Interface Configuration**
     - **RADIUS Policy**
     - **MP Policy Management**
     - **Mesh Profile Management**
     - **Mesh Interface Management**
     - **View Topology**
     - **History Information**
     - **Threshold Configuration**

- **ping**
- **TraceRoute**
- **Open Web Manager**
- **Telnet**
- **SSH**

重要:

- **Threshold Configuration**オプションは、**Clients Associated with AC(Minor)**または**Clients Associated with AC(Major)**がイネーブルになっている場合にだけ表示されます。詳細については、「アラームしきい値の設定」を参照してください。

AC Listに十分なエントリーが含まれている場合は、次のナビゲーション支援が表示されます。

- **Next Page**アイコンをクリックして、**AC List**ページに移動します。
- **Last Page**アイコンをクリックすると、**AC List**の最後にページ送りされます。
- **Previous Page**アイコンをクリックして、**AC List**の前のページに戻ります。
- **First Page**アイコンをクリックすると、**AC List**の先頭に戻ることができます。

AC Listの右上にある**8、15、50、100、または200**をクリックして、各ページに表示する項目の数を指定します。

AC Listは、**Operation**フィールド以外のすべてのフィールドでソートできます。選択したフィールドでリストをソートするには、列ラベルをクリックします。列ラベルを使用すると、各フィールドに固有のソートオプションを切り替えることができます。

ACの同期化

WSMは、AC構成の同期化を自動または手動でサポートします。デフォルトでは、IMCは2時間ごとにACを自動的に同期化します(『HPEH3C IMC v7.3 Enterprise and Standard Platform Administrator Guide』を参照)。また、必要に応じてACを手動で同期化することもできます。

ACを手動で同期するには、次の手順を実行し

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。

   AC ListページにすべてのACが表示されます。
3. 同期させるACを選択します。
4. **Synchronize**をクリックして、選択したACの同期化を開始します。

   同期化プロセスには数分かかります。最後の同期化時刻と同期化結果を表示するには、ページをリフレッシュするか、同期化の完了後に再度ページを入力します。

ACの問い合わせ

WSMには、基本問合せと拡張問合せが用意されています。基本問合せ基準には、迅速な検索のためのキーパラメーターがいくつか含まれています。拡張問合せには、正確な照合のための様々な問合せ基準が用意されています。

詳細については、「ACの照会」を参照してください。

ACに関する概要情報の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。

   AC ListページにすべてのACが表示されます。
3. ACのデバイスラベルをクリックします。

   このページには、ACに関する簡単な情報が表示されます。

   Device Information
   - **Device Label**: ACのデバイスラベル。
   - **Device Status**: ACのアラームステータス。
   - **IP Address**: ACのIPv4アドレス。
   - **Device Model**: ACのデバイスモデル。

   Wireless Service Informationエリアには、ACのAP情報、クライアント情報、およびグローバルパラメーター情報が表示されます。詳細については、「ACに関する詳細情報の表示」を参照してください。

   Client Countグラフおよび**AP Bandwidth**グラフには、オンラインクライアントおよびAPの帯域幅のトレンドが表示されます。詳細は、「クライアント数」および「AP帯域幅」を参照してください。

   Local ACリストには、中央ACによって管理されるすべてのローカルACが表示されます。このリストは、中央ACに対してのみ表示されます。詳細は、「中央ACの構成」を参照してください。

   Wireless Service Alarm領域には、ACが生成するアラームに関する情報が表示されます。詳細については、「ワイヤレスサービスアラームの表示」を参照してください。

   Detected APs領域には、ACによって管理されているセンサーによって検出されたAPに関する情報が表示されます。詳細については、「検出されたAP」を参照してください。

ACに関する詳細情報の表示

1. **Service**をクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。

   AC ListページにすべてのACが表示されます。
3. ACのデバイスラベルをクリックします。
4. ACの簡単な情報ページの右上隅にある**More Detailed**をクリックします。

   ACの詳細ページが開きます。

   この情報には、ACに関するワイヤレスサービス情報のみが記載されています。ACの詳細ページに表示されるその他の情報については、『H3C IMC v7.3 Enterprise and Standard Platform Administrator Guide』を参照してください。
5. **Wireless Service Information**タブをクリックします。

   Global Parameter Information
   - **Max APs**: ACで管理できるFIT APの最大数。
   - **Max Clients**: ACによって管理されるAP全体に関連付けることができるクライアントの最大数。
   - **Control Channel Security Scheme**: CAPWAPコントロールトンネルパケットが暗号化されているかどうかを示します。オプションは**Plaintext**と**Ciphertext**です。

- **Data Channel Security Scheme**: CAPWAPデータトンネルパケットが暗号化されているかどうかを示します。オプションは**Plaintext**と**Ciphertext**です。
- **Traffic Load Balancing Threshold(%)**: ACでロードバランシングがイネーブルになっている場合に、ACによって管理されるFIT APの無線側のトラフィックしきい値。これは、APのスループットに対するFIT APの無線側のトラフィックの比率をパーセンテージで表したものです。

  ACによって管理されるFIT APのトラフィックがしきい値に達すると、FIT APはクライアントからの要求を拒否し、ACは別のFIT APにそれらの要求を受け入れるように通知します。このフィールドに**N/A**と表示されている場合、トラフィックモードのロードバランシングはディセーブルです。
- **Client Load Balancing Threshold**: ACで負荷分散が有効になっている場合に、ACによって管理されるFIT APのクライアントしきい値。ACによって管理されるFIT APに関連付けられているクライアントの数がしきい値に達すると、FIT APはクライアントからの要求を拒否し、ACは別のFIT APにそれらの要求を受け入れるように通知します。このフィールドにN/Aと表示されている場合、クライアントモードの負荷分散は無効です。
- **Auto AP**: 必要に応じて自動AP機能を選択します。オプションは**Enable**および**Disable**です。自動AP機能を使用すると、ACに構成されたテンプレートで指定されたモデルのFIT APにACを自動的に関連付けることができます。詳細は、「FIT APテンプレートの追加」を参照してください。
- **Scan Mode**: FIT APのチャネルスキャンモード。オプションは、**Active**および**Passive**です。

  Activeモードでは、スキャンプロセス中に、FIT APがクライアントとして動作し、別のFIT APにプローブ要求を送信できます。

  Passiveモードでは、スキャンプロセス中に、FIT APはプローブ要求を送信しません。
- **Scan Channel**: チャネルスキャンモード: **All**または**Auto**。**All**は、FIT APがすべてのチャネルをスキャンすることを示します。**Auto**は、接続されたACが属する国または地域で許可されているFIT APスキャンチャネルを示します。
- **Country/Region Code**: **US**(米国)や**JP**(日本)など、ACが属する国または地域のコード。無線の動作チャネルは国コードによって異なります。チャネルスキャンモードが**Auto**の場合、ACは国コードを使用して、FIT APをスキャンするチャネルを決定します。
- **MKD-ID**: ACがキー交換に使用するMKD MACアドレス。
- **Troubleshooting**: トラブルシューティング機能が有効かどうかを示します。詳細は、「トラブルシューティング」を参照してください。
- **Modify**: 必要に応じてACのグローバルパラメーターを変更するには、Modifyアイコンをクリックします。詳細は、「ACグローバルパラメーターの構成」を参照してください。

AP情報

- **Online FIT APs**: ACによって管理されるオンラインFIT APの数。この数をクリックすると、管理されているすべてのオンラインFIT APが表示されます。
- **Offline FIT APs**: ACによって管理されているオフラインFIT APの数。この数をクリックすると、管理されているすべてのオフラインFIT APが表示されます。
- **Online/P FIT APs**: 現在のACでプライマリトンネルを確立したFIT APの数。このようなFIT APはACによって管理されます。この数をクリックすると、現在のACでプライマリトンネルを確立したすべてのFIT APが表示されます。ACバックアップ環境では、FIT APは最大2つのACに接続して、一方のACでプライマリトンネルを確立し、もう一方のACでバックアップトンネルを確立できます。
- **Online/S FIT APs**: 現在のACでバックアップトンネルを確立したFIT APsの数。このようなFIT APsはACによって管理されません。番号をクリックすると、現在のACでバックアップトンネルを確立したすべてのFIT APsが表示されます。ACバックアップ環境では、FIT APsは最大2つのACに接続して、一方のACでプライマリトンネルを確立し、もう一方のACでバックアップトンネルを確立できます。

- **Auto FIT APs**: ACに関連付けられている自動FIT APの数。数字をクリックすると、すべての自動FIT APが表示されます。
- **View All**: **View All**をクリックすると、ACによって管理されているすべてのFIT APが表示されます。オペレーターは、**FIT AP List**で、FIT APの追加、削除、インポート、エクスポート、マップ上でのFIT APの検索、およびAPラベルの同期化を実行できます。詳細は、「FIT APリストの表示」を参照してください。

Client Information

- **Online Clients**: ACによって管理されるFIT APに関連付けられているクライアントの数。この数をクリックすると、すべてのオンラインクライアントが表示されます。
- **Associated Clients**: クライアントとFIT AP間で成功したアソシエーションの数。
- **Associated Failures**: クライアントとFIT AP間で失敗したアソシエーションの数。
- **Re-associated Clients**: クライアントとFIT AP間の再アソシエーションの数。
- **Rejected Clients**: クライアントとFIT AP間で拒否されたアソシエーションの数。
- **Exceptional Deauthenticated Clients**: クライアントとFIT AP間の例外的なアソシエーション解除の数。

ACグローバルパラメーターの設定

AC Parameter Configurationページには、ACの詳細ページまたは構成管理ページからアクセスできます。次の情報では、ACの詳細ページを例として使用しています。

ACグローバルパラメーターを設定するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。

   AC ListページにすべてのACが表示されます。
3. ACのデバイスラベルをクリックします。
4. ACパラメーターを設定するには、次のいずれかの方法を使用します。
   - グローバルパラメーター情報の**Modify**アイコンをクリックします。
   - ページの右側にある**AC Configuration**領域の**Global Configuration**リンクをクリックします。

   AC Global Parameter Configurationページが開きます。
5. 次のパラメーターを設定します。
   - **Load Balancing**: ロードバランシングを有効または無効にします。オプションは、**Traffic Threshold**、**Client Count Threshold**、**No Threshold**です。
     - **Traffic Threshold**を選択すると、トラフィックロードバランシングがイネーブルになります。APのトラフィックロードバランシングしきい値と、2つのAP間のトラフィックロードバランシングギャップを入力します。トラフィックロードバランシングしきい値は、APのスループットに対するFIT APの無線側のトラフィックの割合をパーセントで表したものです。FIT APがしきい値またはギャップのいずれかに達すると、FIT APは新しいクライアントからの要求を拒否し、ACは別のFIT APにこれらの要求を受け入れるように通知します。
     - **Client Count Threshold**を選択すると、クライアントロードバランシングがイネーブルになります。クライアントロードバランシングしきい値と、2つのAP間のクライアントロードバランシングギャップを入力します。FIT APがしきい値またはギャップのいずれかに達すると、FIT APは新しいクライアントからの要求を拒否し、ACは別のFIT APにこれらの要求を受け入れるように通知します。
     - **No Threshold**を選択すると、ロードバランシングはディセーブルになります。
   - **Auto AP**: 自動AP機能を使用可能または使用不可にします。オプションは**Enable**および

Disableです。

Enableを選択すると、ACは、ACに設定されたテンプレートで指定されたモデルのFIT APに自動的に関連付けられます。

Disableを選択すると、モデルを含むテンプレートがACに設定されていても、ACはFIT APに自動的に関連付けられません。

自動FIT APテンプレートの詳細については、「FIT APテンプレートの追加」を参照してください。

- **Scan Mode**: チャネルスキャンモードを選択します。オプションはActiveおよびPassiveです。
  - **Active**: FIT APは、スキャンプロセス中に他のFIT APにプローブ要求を送信するクライアントとして動作します。
  - **Passive**: FIT APはスキャンプロセス中にプローブ要求を送信しません。
- **Scan Channel**: スキャンするチャネルを選択します。オプションはAllおよびAutoです。
  - **All**: FIT APはすべてのチャネルをスキャンします。
  - **Auto**: FIT APは、接続されたACが属する国または地域で許可されているチャネルをスキャンします。デフォルトのオプションは**Auto**です。
- **Country/Region Code**: **US**(米国)や**JP**(日本)など、ACが属する国または地域のコードを選択します。無線の動作チャネルは国コードによって異なります。チャネルスキャンモードが**Auto**の場合、ACの国コードによって、FIT APによってスキャンされるチャネルが決まります。
- **MKD-ID**: キー交換用のMesh Key Distributor(MKD)を入力します。デフォルト値は000F-E200-0001です。設定されたMACアドレスが未使用であり、ベンダー固有の部分が正しいことを確認します。ACのMACアドレスは、MKD IDとして設定できません。
- **Synchronize AC Configuration**: 現在のACが属するACグループ内の他のACにグローバル構成を同期化します。現在のACにのみグローバル構成を適用するには、このオプションを選択しないでください。このオプションは、ACが1つ以上のACグループに属する場合にのみ使用できます。
- **AC Group**: ACグループを選択します。オプションには、現在のACが属するすべてのACグループが含まれます。このオプションは、**Synchronize AC Configuration**が選択されている場合にのみ使用できます。
- **Layer2 Isolation**: レイヤ2分離を有効または無効にします。このパラメーターは、ACで実行される**user-isolation vlan**コマンドと組み合わせて設定します。この機能を有効にすると、許可されたMACアドレスリスト内のクライアントは、同じVLAN内の他のクライアントと通信できます。たとえば、ACで**user-isolation vlan 1 permit-mac 0000-1111-2222**コマンドを実行し、レイヤ2分離を有効にすると、クライアント**0000-1111-2222**はVLAN 1内の他のクライアントにアクセスできますが、他のクライアントは相互にアクセスできません。
- **Troubleshooting**: トラブルシューティング機能を有効にするには、このオプションを選択します。WSMは、ACがトラブルシューティング分析のためにIMCプラットフォームに送信するsyslogを収集します。

注:

レイヤ2分離をイネーブルにした後にクライアントがネットワークにアクセスできるようにするには、まずゲートウェイのMACアドレスを許可MACアドレスリストに追加します。

6. **OK**をクリックします。

無線ポリシーの設定

無線ポリシーは無線パラメーターのコレクションであり、無線にバインドされた後に有効になります。

無線ポリシーの作成を容易にするために、WSMには無線ポリシーテンプレート管理機能が用意されています。詳細は、「無線ポリシーテンプレートの管理」を参照してください。

Radio Policy Managementページには、AC listページ、AC detailsページ、または設定管理ページからアクセスできます。次の情報では、例としてAC listページを使用しています。

無線ポリシーリストの表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。

   AC ListページにすべてのACが表示されます。
3. ACの**Operation**アイコン ⋯ をクリックします。
4. メニューから**Radio Policy**を選択します。

   Radio Policy Managementページが開きます。

   Radio Policy Listには、ACのすべての無線ポリシー情報が表示されます。

   Radio Policy List
   - **Policy Name**: 無線ポリシーの名前。
   - **Beacon Interval(TU)**: APがビーコンフレームを送信する間隔。
   - **DTIM Interval**: バッファリングされたマルチキャストフレームおよびブロードキャストフレームを送信する前にAPが待機するビーコン間隔の数。
   - **RTS Threshold(bytes)**: Request to Send(RTS;送信要求)方式が使用されるフレームの長さ。
   - **Fragment Threshold(bytes)**: フラグメンテーションなしで送信できるフレームの最大長。
   - **Rx Lifecycle(ms):** APが受信したフレームをバッファメモリーに保持する間隔。
   - **Operation**: 無線ポリシーの**Operation**アイコン ⋯ をクリックして、**Operation**メニューを表示します。

     Operationメニューで提供される操作タスクは、**Modify**、**Delete**、および**Bound Radios**です。

   Radio List
   - **Admin Status**: 無線の管理状態。オプションはUpおよびDownです。
   - **Radio ID**: 無線のID。
   - **AP Template Name**: 無線が属するAPで使用されるテンプレートの名前。
   - **Radio Type**: 無線タイプを選択します。オプションは次のとおりです。

     802.11a
     802.11b
     802.11g
     802.11bg
     802.11at
     802.11an
     802.11gn
     802.11n(2.4GHz)
     802.11bgn

802.11n

802.11n(5GHz)

- **Policy Name**: 無線にバインドされている無線ポリシーの名前。
- **Delete**: 無線を削除するには、**Delete**アイコンをクリックします。

5. **Related Operations**をクリックし、次のいずれかを選択して設定ページに入ります。
   - 構成管理
   - APの設定
   - バッチでの無線の設定
   - ワイヤレス論理インターフェースの設定
   - サービスポリシーの管理

Radio Policy Listに十分なエントリーがある場合は、次のナビゲーション支援が表示されます。

- **Next Page**アイコンをクリックして、**Radio Policy List**で次のページに進みます。
- **Last Page**アイコンをクリックして、**Radio Policy List**の最後のページに進みます。
- **Previous Page**アイコンをクリックして、**Radio Policy List**で前のページに戻ります。
- **First Page**アイコンをクリックして、**Radio Policy List**の先頭にページバックします。

無線ポリシーの詳細の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。

   AC ListページにすべてのACが表示されます。
3. ACの**Operation**アイコン をクリックします。
4. メニューから**Radio Policy**を選択します。

   Radio Policy Managementページが開き、すべての無線ポリシーとACのバインドされた無線が表示されます。
5. 詳細を表示するには、無線ポリシーの名前をクリックします。

   Radio Policy Details
   - **Policy Name**: 無線ポリシーの名前。
   - **Beacon Interval(TU)**: APがビーコンフレームを送信する間隔。
   - **DTIM Interval**: バッファリングされたマルチキャストフレームおよびブロードキャストフレームを送信する前にAPが待機するビーコン間隔の数。
   - **RTS Threshold(bytes)** :Request to Send(RTS)方式が使用されるフレームの長さ。
   - **Fragment Threshold(bytes)**: フラグメンテーションなしで送信できるフレームの最大長。
   - **Short Frame Retransmission Threshold**: RTSしきい値よりも短いフレームを送信する最大試行回数。
   - **Long Frame Retransmission Threshold**: RTSしきい値よりも大きいフレームを送信する最大試行回数。
   - **Rx Lifecycle(ms)**: APが受信したフレームをバッファメモリーに保持する間隔。
   - **Max Clients**: ポリシーを使用する無線に関連付けることができるクライアントの最大数。
6. **Close**をクリックします。

無線ポリシーの追加

次のいずれかの方法を使用して、ACの無線ポリシーを追加できます。

- **Normal method**: Radio Policy Managementで無線ポリシーを追加します。
- **Express method**: テンプレートを使用して、無線ポリシーを追加します。無線ポリシーテンプレートの詳細については、「無線ポリシーテンプレートの管理」を参照してください。

Normal method

通常の方法を使用して無線ポリシーを追加するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。

   AC ListページにすべてのACが表示されます。
3. ACの**Operation**アイコン ··· をクリックします。
4. メニューから**Radio Policy**を選択します。

   Radio Policy Managementページが開き、ACのすべての無線ポリシー情報が表示されます。
5. **Add Policy**をクリックします。

   無線ポリシーを追加するためのページが開きます。
6. 次のパラメーターを設定します。
   - **Policy Name**: ACの無線ポリシーを一意に識別する名前を入力します。
   - **Beacon Interval(TU)**: APがビーコンフレームを送信する間隔を入力します。
   - **DTIM Interval**: バッファされたマルチキャストフレームおよびブロードキャストフレームを送信する前にAPが待機するビーコン間隔の数を入力します。値の範囲は1～31です。デフォルト値は1で、102400マイクロ秒です。DTIMカウンタが設定値に達すると、APはバッファされたブロードキャスト/マルチキャストフレームを送信します。
   - **RTS Threshold (bytes)**: Request to Send(RTS;送信要求)方式を使用するフレームの長さを入力します。WLANでデータ送信の衝突を効果的に回避するには、有理値を設定します。値を小さく設定すると、RTSパケットが頻繁に送信され、使用可能な帯域幅をより多く消費します。ただし、システムは干渉や衝突から迅速に回復できます。
   - **Fragment Threshold(bytes)**: フラグメンテーションなしで送信できるフレームの最大長を入力します。指定したフラグメントしきい値を超えるパケットは、フラグメント化されます。
   - **Short Frame Retransmission Threshold**: RTSしきい値よりも短いフレームを送信する最大試行回数を入力します。
   - **Long Frame Retransmission Threshold**: RTSしきい値よりも大きいフレームを送信する最大試行回数を入力します。
   - **Rx Lifecycle(ms)**: APが受信したフレームをバッファメモリーに保持する間隔を入力します。
   - **Max Clients**: ポリシーを使用する無線に関連付けることができるクライアントの最大数を入力します。
   - **Synchronize AC Configuration**: 指定したACグループ内のすべてのACに無線ポリシーを適用します。現在のACにのみ無線ポリシーを適用するには、このオプションを選択しないでください。このオプションは、ACが少なくとも1つのACグループに属している場合にのみ使用できます。
   - **AC Group**: ACグループを選択します。オプションは、現在のACが属するすべてのACグループです。このオプションは、「AC構成の同期化」が選択されている場合にのみ使用できます。
7. **OK**をクリックします。

Express method

express方式を使用して無線ポリシーを追加するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。**AC List**ページにすべてのACが表示されます。
3. ACの**Operation**アイコン をクリックします。
4. メニューから**Radio Policy**を選択します。

   Radio Policy Managementページが開き、**Radio Policy List**にACのすべての無線ポリシー情報が表示されます。
5. **Select Template**をクリックします。

   WSM内のすべての無線ポリシーテンプレートが表示されます。

   Select Radio Policy Template
   - **Policy Name**: 無線ポリシーの名前。
   - **Beacon Interval**: APがビーコンフレームを送信する間隔。
   - **DTIM Interval**: バッファリングされたマルチキャストフレームおよびブロードキャストフレームを送信する前にAPが待機するビーコン間隔の数。
   - **RTS Threshold**: Request to Send(RTS;送信要求)方式が使用されるフレームの長さ。
   - **Fragment Threshold**: フラグメンテーションなしで送信できるフレームの最大長。
   - **Rx Lifecycle**: APが受信したフレームをバッファメモリーに保持する間隔。
6. 使用する無線ポリシーテンプレートを選択します。
7. **Next**をクリックします。
8. 必要に応じて、次のパラメーターを変更します。
   - **Policy Name**: 無線ポリシーの名前を入力します。デフォルト値は、選択した無線テンプレートの名前です。
   - **Synchronize AC Configuration**: 指定したACグループ内のすべてのACに無線ポリシーを適用します。現在のACにのみ無線ポリシーを適用するには、このオプションを選択しないでください。このオプションは、ACが少なくとも1つのACグループに属している場合にのみ使用できます。
   - **AC Group**: ACグループを選択します。オプションは、現在のACが属するすべてのACグループです。このオプションは、**Synchronize AC Configuration**が選択されている場合にのみ使用できます。
9. **OK**をクリックします。

   Result Listページが開き、無線ポリシーを追加するための操作結果が表示されます。
10. **Back**をクリックして、現在のACの**Radio Policy Management**ページに戻ります。

無線ポリシーの変更

デフォルトの無線ポリシー**default_rp**は変更できません。

ユーザー定義の無線ポリシーを変更するには、次の手順

を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。**AC List**ページにすべてのACが表示されます。
3. ACの**Operation**アイコン をクリックします。
4. メニューから**Radio Policy**を選択します。

Radio Policy Managementページが開き、**Radio Policy List**にACのすべての無線ポリシー情報が表示されます。

5. 無線ポリシーの**Operation**アイコン･･･ をクリックします。
6. メニューから**Modify**を選択します。

   無線ポリシーを変更するためのページが開きます。
7. 必要に応じて、無線ポリシーパラメーターを設定します。詳細は、「無線ポリシーの追加」を参照してください。無線ポリシー名は変更できません。
8. **OK**をクリックします。

無線ポリシーにバインドされた無線の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。**AC List**ページにすべてのACが表示されます。
3. ACの**Operation**アイコン･･･ をクリックします。
4. メニューから**Radio Policy**を選択します。

   Radio Policy Managementページが開き、**Radio Policy List**にACのすべての無線ポリシー情報が表示されます。
5. 無線ポリシーの**Operation**アイコン･･･ をクリックします。
6. メニューから**Bound Radios**を選択します。

   Radio Listダイアログボックスが開きます。

   Bound radio Listには、現在の無線ポリシーにバインドされているすべての無線に関する情報が表示されます。オペレーターは、必要に応じて無線のバインドを解除し、最新のバインドされた無線リストをACグループ内のすべてのACに同期化できます。詳細については、「無線ポリシーの無線へのバインド」を参照してください。

無線への無線ポリシーのバインディング

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。**AC List**ページにすべてのACが表示されます。
3. ACの**Operation**アイコン･･ をクリックします。
4. メニューから**Radio Policy**を選択します。

   Radio Policy Managementページが開き、**Radio Policy List**にACのすべての無線ポリシー情報が表示されます。
5. バインドする無線ポリシーを選択します。
6. **Radio List**領域で**Add**をクリックします。

   Select Radiosダイアログボックスが開きます。
7. 設定する無線を検索するためのクエリー基準を指定して、設定する無線を検索します。
   - **AP Label**: 無線が属するFIT APのラベルを入力します。WSMは、このフィールドのファジーマッチングをサポートします。
   - **AP Name**: 無線が属するFIT APの名前を入力します。WSMは、このフィールドのファジーマッチングをサポートしています。
   - **Serial Number**: 無線が属するFIT APのシリアル番号を入力します。WSMは、このフィー

ルドのファジーマッチングをサポートします。

- **Radio Type**: 無線タイプを選択します。オプションは次のとおりです。
  - **802.11a**
  - **802.11b**
  - **802.11g**
  - **802.11bg**
  - **802.11at**
  - **802.11an**
  - **802.11gn**
  - **802.11n(2.4GHz)**
  - **802.11bgn**
  - **802.11n**
  - **802.11n(5GHz)**
- **Admin Status**: 無線の管理状態を選択します。オプションは、Unlimited、Up、および Downです。
- **Radio Policy Name**: 無線にバインドされた無線ポリシーの名前を入力します。 WSMは、このフィールドのファジーマッチングをサポートしています。
- **Location**: FIT APが属するロケーションビューの名前を入力または選択します。WSMは、このフィールドのファジーマッチングをサポートしています。

空のフィールドや**Unlimited**に設定されたフィールドは、クエリーの抽出条件にはなりません。

8. **Query**をクリックします。

   Radio Listには、クエリー基準に一致するすべての無線が表示されます。**Reset**をクリックすると、クエリー基準がクリアされ、すべての無線が表示されます。
9. 無線ポリシーにバインドする無線を選択します。
10. **OK**をクリックして、**Select Device**ウィンドウを閉じます。

    Radio Listに、選択したすべての無線が表示されます。
11. **Bind**をクリックします。

    Result Listページが開き、成功したバインド操作と失敗したバインド操作が表示されます。失敗した場合は、**Operation Result**列の**Details**アイコンをクリックして、失敗の原因を特定します。

無線からの無線ポリシーのアンバインド

デフォルトの無線ポリシー**default_rp**はすべての無線にバインドされており、バイン

ド解除できません。ユーザー定義の無線ポリシーから無線のバインドを解除するに

は、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。

   AC ListページにすべてのACが表示されます。
3. ACの**Operation**アイコン･･･ をクリックします。
4. メニューから**Radio Policy**を選択します。

   Radio Policy Managementページが開き、**Radio Policy List**にACのすべての無線ポリシー情報が表示されます。
5. 無線ポリシーの**Operation**アイコン･･･ をクリックします。

6. メニューから**Bound Radios**を選択します。

   Radio Listダイアログボックスが開きます。
7. バインド解除する無線を選択します。
8. 必要に応じて次のパラメーターを設定します。
   - **Synchronize AC Configuration**: 指定されたACグループ内のすべてのACの無線ポリシーから無線をアンバインドします。現在のACの無線ポリシーからのみ無線をアンバインドするには、このオプションを選択しないでください。このオプションは、ACが少なくとも1つのACグループに属している場合にだけ使用できます。
   - **AC Group**: ACグループを選択します。オプションは、現在のACが属するすべてのACグループです。このオプションは、**Synchronize AC Configuration**が選択されている場合にのみ使用できます。
9. **Unbind**をクリックします。

   Result Listページが開き、成功および失敗したアンバインド操作が表示されます。Operation列の**Details**アイコンをクリックして、失敗の原因を特定します。
10. **Back**をクリックして、ダイアログボックスを閉じます。

無線ポリシーの削除

無線ポリシーを削除すると、その無線ポリシーに関連するすべての情報が削除されます。デフォルトの無線ポリシー**default_rp**および無線にバインドされている無線ポリシーは削除できません。

無線ポリシーを削除するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > AC**sを選択します。

   AC ListページにすべてのACが表示されます。
3. ACの**Operation**アイコン ··· をクリックします。
4. メニューから**Radio Policy**を選択します。

   Radio Policy Managementページが開き、**Radio Policy List**にACのすべての無線ポリシー情報が表示されます。
5. 無線ポリシーの**Operation**アイコン ··· をクリックします。
6. メニューから**Delete**を選択します。

   確認ダイアログボックスが表示されます。
7. **OK**をクリックします。

バッチでの無線の設定

無線設定を容易にし、繰り返しの操作を減らすために、WSMでは、オペレーターは、ACによって管理されるFIT APの複数の無線のパブリックパラメーターをバッチで設定できます。

Radio Batch Configurationページには、ACの詳細ページまたは構成管理ページからアクセスできます。次の情報では、例としてACリストページを使用しています。

無線をバッチで設定するには、次の手順を実行します

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > AC**sを選択します。

   AC ListページにすべてのACが表示されます。
3. ACのデバイスラベルをクリックします。

4. ページの右側にある**Wireless Service**領域で、**Radio Batch Configuration**をクリックします。

   Radio Batch Configurationページが開きます。

5. 次のパラメーターを設定します。
   - Radio Type:無線タイプを選択します。オプションは次のとおりです。

     802.11a
     802.11b
     802.11g
     802.11bg
     802.11at
     802.11an
     802.11gn
     802.11n(2.4GHz)
     802.11bgn
     802.11n
     802.11n(5GHz)
     802.11ac
   - **Max Transmission Power(dBm)**: 無線の最大送信電力を入力します。
   - **Admin Status**: 無線の管理状態を選択します。オプションはUpおよびDownです。
   - 使用中のチャネル無線の動作チャネルを選択します。値の範囲は無線のタイプによって異なります。自動を選択すると、ACは無線に最適なチャネルを割り当てます。
   - **Preamble Type**: FIT APのプリアンブルタイプを選択します。オプションはShortとLongです。Shortは、FIT APがショートプリアンブルまたはロングプリアンブルのいずれかを含むフレームを送信することを意味します。Longは、FIT APがロングプリアンブルを含むフレームだけを送信することを意味します。このオプションは、無線タイプとして802.11b、802.11g、および802.11gnを選択した場合に設定できます。
   - **Radio Policy**: 無線にバインドする無線ポリシーを選択します。オプションは、WSM内のすべての既存の無線ポリシーです。
   - **Synchronize AC Configuration**: 現在のACが属するACグループ内の他のACにグローバル構成を同期化します。現在のACにのみグローバル構成を適用するには、このオプションを選択しないでください。このオプションは、ACが1つ以上のACグループに属する場合にのみ使用できます。
6. **Radio List**領域で**Add**をクリックします。

   Select Deviceダイアログボックスが開きます。
7. 設定する無線を検索するためのクエリー基準を指定して、設定する無線を検索します。
   - **AP Label**: 無線が属するFIT APのラベルを入力します。WSMは、このフィールドのファジーマッチングをサポートします。
   - **AP Name**: 無線が属するFIT APの名前を入力します。WSMは、このフィールドのファジーマッチングをサポートします。
   - **Serial Number**: 無線が属するFIT APのシリアル番号を入力します。WSMは、このフィールドのファジーマッチングをサポートしています。
   - **Radio Type**: 無線タイプを選択します。オプションは、**802.11a、802.11b、802.11g、802.11gn、および802.11an**
   - **Admin Status**: 無線の管理状態を選択します。オプションは、**Unlimited、Up**、および**Down**です。
   - **Radio Policy Name**: 無線にバインドされた無線ポリシーの名前を入力します。WSMは、この

フィールドのファジーマッチングをサポートしています。

- **Location**: FIT APが属するロケーションビューの名前を入力または選択します。WSMは、このフィールドのファジーマッチングをサポートしています。

空のフィールドや**Unlimited**に設定されたフィールドは、クエリーの抽出条件にはなりません。

8. **Query**をクリックします。

   Radio Listには、クエリー基準に一致するすべての無線が表示されます。**Reset**をクリックすると、クエリー基準がクリアされ、すべての無線が表示されます。
9. 設定する無線を選択します。
10. **OK**をクリックして、**Select Device**ウィンドウを閉じます。**Radio List**に、選択したすべての無線が表示されます。
11. **OK**をクリックします。

    Result Listページが開き、各無線の設定結果が表示されます。
12. **Back**をクリックして、無線バッチ設定ページに戻ります。

注:

設定エラーを回避するためのベストプラクティスとして、同じモデルのFIT APに無線をバッチで設定します。

WLAN論理インターフェースの設定

サービスポリシーは、ACのWLAN論理インターフェースにバインドされます。WLAN論理インターフェースは、1つのサービスポリシーだけにバインドできます。

WLAN Logical Interface Configurationページには、AC listページ、AC detailsページ、または設定管理ページからアクセスできます。次の情報では、例としてAC listページを使用しています。

WLAN論理インターフェースリストの表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。

   AC ListページにすべてのACが表示されます。
3. ACの**Operation**アイコン ··· をクリックします。
4. メニューから**Wireless Logical Interface Configuration**を選択します。

   Wireless Logical Interface Configurationページが開き、**Wireless Logical Interface List**にACのすべてのWLAN論理インターフェース情報が表示されます。

   WLAN Logical Interface List

   - **Description**: WLAN-ESSインターフェースID形式のインターフェースの説明。
   - **SSID**: WLAN論理インターフェースにバインドされたサービスポリシーの一意のSSID。名前をクリックすると、その詳細が表示されます。
   - **Port Security Mode**: WLAN論理インターフェースのポートセキュリティモード。オプションは次のとおりです。
     - **noRestrictions**
     - **mac-and-psk**
     - **MAC-authentication**

- **mac-else-userlogin-secure**
- **mac-else-userlogin-secure-ext**
- **psk**
- **userlogin-secure**
- **userlogin-secure-ext**
- **userlogin-secure-or-mac**
- **userlogin-secure-or-mac-ext**
- **userlogin-secure-ext-or-psk**
- **userlogin-with OUI**

o **VLAN**: WLAN論理インターフェースが属するVLAN。

o **Operation**: WLAN論理インターフェースの**Operation**アイコン ･･･ をクリックして、**Operation**メニューを表示します。

Operationメニューに表示される操作タスクは、**Delete Interface**、**Modify Port Security**、および**Modify VLAN**です。

5. **Related Operations**をクリックし、**Configuration Management**、**Configure Radio Batches**、または**Service Policy Management**を選択して、設定ページを開きます。

ワイヤレス論理インターフェースリストに十分な数のエントリーがある場合は、次のナビゲーションツールが表示されます。

- **Next Page**アイコンをクリックして、**Wireless Logical Interface List**で次のページに進みます。
- **Last Page**アイコンをクリックして、**Wireless Logical Interface List**の最後のページに進みます。
- **Previous Page**アイコンをクリックで**Wireless Logical Interface List**の前のページに戻ります。
- **First Page**アイコンをクリックして、**Wireless Logical Interface List**の先頭にページバックします。

各ページに表示する項目数を設定するには、**Wireless Logical Interface List**の右上にある**8**、**15**、**50**、**100**、または**200**をクリックします。

Wireless Logical Interface Listは、**Operation**フィールド以外のすべてのフィールドで並べ替えることができます。列ラベルをクリックすると、選択したフィールドでリストが並べ替えられます。列ラベルを使用すると、各フィールドに固有の並べ替えオプションを切り替えることができます。

WLAN論理インターフェースの照会

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。

   AC ListページにすべてのACが表示されます。
3. ACの**Operation**アイコン ･･･ をクリックします。
4. メニューから**Wireless Logical Interface Configuration**を選択します。

   Wireless Logical Interface Configurationページが開き、AC on WLAN Logical Interface Listのすべての WLAN論理インターフェース情報が表示されます。
5. 次の問合せ基準のいずれかまたは両方を指定します。

   o **Description**: インターフェースの説明を入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。

   o **SSID**: ACのSSIDを入力します。WSMでは、このフィールドのファジーマッチングがサポートさ

れています。空のフィールドまたは無制限に設定されたフィールドは、クエリー条件として機能しません。

6. **Query**をクリックします。

   Device Listには、クエリー基準に一致するすべての無線インターフェースが表示されます。**Reset**をクリックすると、クエリー基準がクリアされ、すべての無線インターフェースが表示されます。

WLAN論理インターフェースの追加

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。

   AC ListページにすべてのACが表示されます。
3. ACの**Operation**アイコン ··· をクリックします。
4. メニューから**Wireless Logical Interface Configuration**を選択します。

   Wireless Logical Interface Configurationページが開き、**Wireless Logical Interface List**にACのすべてのWLAN論理インターフェース情報が表示されます。
5. **Add Interface**をクリックします。

   WLAN論理インターフェースを追加するためのページが開きます。
6. 次のパラメーターを設定します。
   - **Interface ID**: WLAN論理インターフェースのIDを入力します。たとえば、ID 50のWLAN論理インターフェースを追加すると、そのインターフェースの説明はWLAN-ESS50になります。
   - **Synchronize AC Configuration**: WLAN論理インターフェース設定を、指定したACグループ内のすべてのACに適用します。WLAN論理インターフェース設定を現在のACにのみ適用するには、このオプションを選択しないでください。このオプションは、ACが少なくとも1つのACグループに属している場合にのみ使用できます。
   - **Cancel Shake Handshake**: このオプションを選択すると、802.1Xハンドシェーク機能が無効になります。
   - **AC Group**: ACグループを選択します。オプションは、現在のACが属するすべてのACグループです。このオプションは、**Synchronize AC Configuration**が選択されている場合にのみ使用できます。
7. **OK**をクリックします。

   Adding Interface Resultページが開き、WLAN論理インターフェースの追加操作の結果とAC同期化の結果が表示されます。
8. **Back**をクリックして、**WLAN Logical Interface Configuration**ページに戻ります。

WLAN論理インターフェースのポートセキュリティモードの変更

サービスポリシーにバインドされているWLAN論理インターフェースのポートセキュリティモードを変更するには、最初に**Modify Service Policy**ページでWLAN論理インターフェースの**Interface ID**を-1に設定します。

WLAN論理インターフェースのポートセキュリティモードを変更するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。

   AC ListページにすべてのACが表示されます。
3. ACの**Operation**アイコン ··· をクリックします。

4. メニューから**Wireless Logical Interface Configuration**を選択します。

   Wireless Logical Interface Configurationページが開き、Wireless Logical Interface ListにACのすべてのWLAN論理インターフェース情報が表示されます。

5. ポートセキュリティを変更するには、次のいずれかの方法を使用します。
   - WLAN論理インターフェースの**Operation**アイコン ･･･をクリックし、メニューからModify **Port Security**を選択します。
   - ポートセキュリティモードを変更するWLAN論理インターフェースを選択し、WLAN **Logical Interface List**で**Modify Port Security**をクリックします。

   Modify Port Securityページが開きます。

6. 次のパラメーターを設定します。
   - **Port Security Mode**: WLAN論理インターフェースのポートセキュリティモードを選択します。オプションは次のとおりです。
     - **noRestrictions**
     - **mac-and-psk**
     - **MAC-authentication**
     - **mac-else-userlogin-secure**
     - **mac-else-userlogin-secure-ext**
     - **psk**
     - **userlogin-secure**
     - **userlogin-secure-ext**
     - **userlogin-secure-or-mac**
     - **userlogin-secure-or-mac-ext**
     - **userlogin-secure-ext-or-psk**
     - **userlogin-with OUI**

     サービスポリシーの暗号化モードが**Clear**であるか、セキュリティIEが**None**である場合、ポートセキュリティモードWLAN論理インターフェースは、**mac-and-psk、psk、またはuserlogin-secure-ext-or-psk**にできません。

     サービスポリシーの暗号化モードが**Crypto**で、セキュリティIEが**RSNまたはWPA**の場合、ポートセキュリティモードのWLAN論理インターフェースは、**mac-and-psk、psk、userlogin-secure-ext-or-psk、またはuserlogin-secure-ext**だけになり、キーネゴシエーションタイプは**11Key**になります。

表7 ポートセキュリティモード

ポートセキュリティモード	キーパラメーター
noRestrictions	キーパラメーターは必要ありません。
mac-and-psk	• **Key negotiation type**: オプションは、**None**と**11key**です。 • **PSK type**: オプションは**None**、**Pass-Phrase**、および**Raw-Key**です。 • **PSK**: PSK値を入力します。PSKタイプに**None**を選択した場合、このフィールドは必要ありません。
MAC-authentication	キーパラメーターは必要ありません。
mac-else-userlogin-secure	キーパラメーターは必要ありません。
mac-else-userlogin-secure-ext	キーパラメーターは必要ありません。
psk	• **Key negotiation type**: オプションは、**None**と**11key**です。 • **PSK type**: オプションは**None**、**Pass-Phrase**、および**Raw-Key**です。 • **PSK**: PSK値を入力します。PSKタイプに**None**を選択した場合、このフィールドは必要ありません。
userlogin-secure	キーパラメーターは必要ありません。
userlogin-secure-ext	キーネゴシエーションタイプ。オプションは**None**および**11key**です。
userlogin-secure-or-mac	キーパラメーターは必要ありません。
userlogin-secure-or-mac-ext	キーパラメーターは必要ありません。
userlogin-secure-ext-or-psk	• **Key negotiation type**: オプションは、**None**と**11key**です。 • **PSK type**: オプションは**None**、**Pass-Phrase**、および**Raw-Key**です。 • **PSK**: PSK値を入力します。PSKタイプに**None**を選択した場合、このフィールドは必要ありません。
userlogin-with OUI	キーパラメーターは必要ありません。

- **Cancel Shake Handshake**: このオプションを選択すると、802.1Xハンドシェーク機能が無効になります。
- **Synchronize AC Configuration**: 指定したACグループ内のすべてのACにポートセキュリティモード設定を適用します。現在のACにのみポートセキュリティモード設定を適用するには、このオプションを選択しないでください。このオプションは、ACが1つ以上のACグループに属している場合にのみ使用できます。
- **AC Group**: ACグループを選択します。オプションは、現在のACが属するすべてのACグループです。このオプションは、**Synchronize AC Configuration**が選択されている場合にのみ使用できます。

7. **OK**をクリックします。

   Result Listページが開き、選択したWLAN論理インターフェースのポートセキュリティモードを変更する操作の結果と、AC同期化の結果が表示されます。

8. **Back**をクリックして、**WLAN Logical Interface Configuration**ページに戻ります。

WLAN論理インターフェースが属するVLANの変更

1. **Service**タブをクリックします。

2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。

   AC ListページにすべてのACが表示されます。

3. ACの**Operation**アイコン ⋯ をクリックします。
4. メニューから**Wireless Logical Interface Configuration**を選択します。

   Wireless Logical Interface Configurationページが開き、**AC on WLAN Logical Interface List**のすべてのWLAN論理インターフェース情報が表示されます。
5. VLANを変更するには、次のいずれかの方法を使用します。
   - WLAN論理インターフェースの**Operation**アイコン ⋯ をクリックし、メニューから**Modify VLAN**を選択します。
   - **VLAN**を変更するWLAN論理インターフェースを選択し、**WLAN Logical Interface List**で**Modify VLAN**をクリックします。

   Modify VLANページが開きます。
6. 次のパラメーターを設定します。
   - **VLAN**: VLANを選択します。オプションは、現在のACで作成されたすべてのVLANです。
   - **Synchronize AC Configuration**: 指定したACグループ内のすべてのACにVLAN設定を適用します。現在のACにのみVLAN設定を適用するには、このオプションを選択しないでください。このオプションは、ACが少なくとも1つのACグループに属している場合にのみ使用できます。
   - **AC Group**: ACグループを選択します。オプションは、現在のACが属するすべてのACグループです。このオプションは、**Synchronize AC Configuration**が選択されている場合にのみ使用できます。
7. **OK**をクリックします。

   Result Listページが開き、選択したインターフェースが属するVLANの変更操作の結果とAC同期化の結果が表示されます。
8. **Back**をクリックして、**WLAN Logical Interface Configuration**ページに戻ります。

WLAN論理インターフェースの削除

サービスポリシーにバインドされているWLAN論理インターフェースを削除するには、最初に**Modify Service Policy**ページでWLAN論理インターフェースの**Interface ID**を-1に設定します。

WLAN論理インターフェースを削除するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。

   AC ListページにすべてのACが表示されます。
3. ACの**Operation**アイコン ⋯ をクリックします。
4. メニューから**Wireless Logical Interface Configuration**を選択します。

   Wireless Logical Interface Configurationページが開き、**WLAN Logical Interface List**にACのすべてのWLAN論理インターフェース情報が表示されます。
5. 削除するWLAN論理インターフェースの**Operation**アイコン ⋯ をクリックし、メニューから**Delete Interface**を選択します。

   または削除するWLAN論理インターフェースを選択し、**WLAN Logical Interface List**の**Delete Interface**をクリックします。

   確認ダイアログボックスが表示されます。
6. **OK**をクリックします。

サービスポリシーの設定

サービスポリシーはWLANアクセスパラメーターの集まりであり、ポリシーがFIT APの無線にバインドされた後、FIT APがWLANアクセスサービスを提供できるようにします。異なる無線が同じサービスポリシーを使用でき、各無線は複数のサービスポリシーにバインドできます。

サービスポリシーの作成を容易にするために、WSMにはサービスポリシーテンプレート管理機能が用意されています。詳細は、「サービスポリシーテンプレートの管理」を参照してください。

Service Policy Managementページには、ACリストページ、AC詳細ページまたは構成管理ページからアクセスできます。次の情報では、ACリストページを例として使用しています。

サービスポリシーリストの表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。

   AC ListページにすべてのACが表示されます。
3. ACの**Operation**アイコン ··· をクリックします。
4. メニューから**Service Policy**を選択します。

   Service Policy Managementページが開きます。

   このページでは、ACのすべてのサービスポリシー情報を表示する**Service Policy List**と、サービスポリシーにバインドされているすべての無線を表示する**Radio List**の2つのリストを使用できます。

   Service Policy Listでは、サービスポリシーの追加と変更、サービスポリシーテンプレートの選択、サービスポリシーリストのリフレッシュ、サービスポリシーの削除、サービスポリシーにバインドされた無線の表示、およびサービスポリシーへの無線のバッチバインドを行うことができます。

   Service Policy List

   - **Policy ID**: サービスポリシーのID。
   - **SSID**: サービスポリシーのSSID。
   - **Encryption Mode**: サービスポリシーの暗号化モード。このフィールドは、Comware 7 ACには表示されません。オプションは次のとおりです。
     - **Clear Mode**: データパケットを暗号化する必要はありません。
     - **Crypto Mode**: すべてのデータパケットを暗号化する必要があります。
   - **Hide SSID**: APから送信されるビーコンフレームでSSIDを提供するかどうかを示します。このパラメーターを選択すると、クライアントはビーコンフレームからSSIDを取得できないため、ワイヤレスネットワークにアクセスする前にSSIDを設定する必要があります。このパラメーターを選択しないと、クライアントはビーコンフレームからSSIDを取得してワイヤレスネットワークにアクセスできます。
   - **Enable Status**: サービスポリシーが有効かどうかを示します。オプションは次のとおりです。
     - **Enable**: サービスポリシーがAC上でイネーブルであり、ACがサービスを提供できることを示します。
     - **Disable**: サービスポリシーがACでイネーブルになっておらず、ACがサービスを提供できないことを示します。
     - **Not Ready**: サービスポリシーがACに導入されていて、ACがサービスを提供できないことを示します。
   - **Authentication Mode**: サービスポリシーの認証モード。このフィールドは、Comware 7 ACでは表示されません。オプションは次のとおりです。

- **Open System**: 認証を要求するすべてのクライアントが直接認証を通過できるようにします。
- **Shared Key**: クライアントはデバイスに設定されているものと同じ共有キーを使用する必要があります。**Shared Key**は、暗号スイートとしてWEP40、WEP104、またはWEP128を選択した場合にだけ指定します。
- **All**: クライアントが必要に応じて**Open System**モードまたは**Shared Key**モードを使用できるようにします。

○ **Operation**: サービスポリシーの**Operation**アイコン ･･･ をクリックして、**Operation**メニューを表示します。

Operationメニューで提供される操作タスクは、指定されたサービスポリシーの変更と削除、および指定されたサービスポリシーにバインドされた無線に関する情報の表示です。

Radio Listでは、無線を追加または削除したり、すべての無線を削除したりできます。

Radio List

○ **Admin Status**: 無線の管理状態。オプションはUpおよびDownです。

○ **Radio ID**: 無線のID。

○ **AP Template Name**: 無線が属するAPのテンプレートの名前。

○ Radio Type:無線のタイプ。オプションは次のとおりです。

- **802.11a**
- **802.11b**
- **802.11g**
- **802.11gn**
- **802.11an**

○ **Policy Name**: 無線にバインドされている無線ポリシーの名前。

○ **Delete**: 無線を削除するには、**Delete**アイコン をクリックします。

5. **Related Operations**をクリックし、**Configuration Management**または**Wireless Logical Interface Configuration**を選択して、**Configuration**ページを開きます。

Service Policy Listに十分な数のエントリーが含まれている場合は、次のナビゲーションツールが表示されます。

- **Next Page**アイコンをクリックして、**Service Policy List**内で次のページに進みます。
- **Last Page**アイコンをクリックして、**Service Policy List**の最後のページに進みます。
- **Previous Page**アイコンをクリックして、**Service Policy List**のページを逆方向に表示します。
- **First Page**アイコンをクリックして、**Service Policy List**の前のページに戻ります。

各ページに表示する項目数を設定するには、**Service Policy List**の右上にある**8**、**15**、**50**、**100**、または**200**をクリックします。

サービスポリシーの詳細の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。

   AC ListページにすべてのACが表示されます。
3. ACの**Operation**アイコン ･･ をクリックします。
4. メニューから**Service Policy**を選択します。

   Service Policy Managementページには、**Service Policy List**上のACのすべてのサービス

ポリシー情報が表示されます。

5. サービスポリシーのIDをクリックすると、その基本情報が表示されます。Comware 5 ACの場合:

   Service policy basic information

   - **Policy ID**: サービスポリシーのID。
   - **SSID**: サービスポリシーのSSID。
   - **Encryption Mode**: サービスポリシーの暗号化モード。オプションは次のとおりです。
     - **Clear:** データパケットを暗号化する必要はありません。
     - **Crypto**: すべてのデータパケットを暗号化する必要があります。
   - **Hide SSID**: APから送信されるビーコンフレームでSSIDを提供するかどうかを示します。このパラメーターを選択すると、クライアントはビーコンフレームからSSIDを取得できないため、ワイヤレスネットワークにアクセスする前にSSIDを設定する必要があります。このパラメーターを選択しないと、クライアントはビーコンフレームからSSIDを取得してワイヤレスネットワークにアクセスできます。
   - **Enable Status**: サービスポリシーが有効かどうかを示します。オプションは次のとおりです。
     - **Enable**: サービスポリシーがAC上でイネーブルであり、ACがサービスを提供できることを示します。
     - **Disable**: サービスポリシーがACでイネーブルになっておらず、ACがサービスを提供できないことを示します。
     - **Not Ready**: サービスポリシーがACに導入されていて、ACがサービスを提供できないことを示します。
   - **Authentication Mode**: サービスポリシーの認証モード。オプションは次のとおりです。
     - **Open System**: 認証を要求するすべてのクライアントが直接認証を通過できるようにします。
     - **Shared Key**: クライアントはデバイスに設定されているものと同じ共有キーを使用する必要があります。Shared Keyは、暗号スイートとしてWEP40、WEP104、またはWEP128を選択した場合にだけ指定します。
     - **All**: クライアントがオープンシステムモードまたは共有キーモードのいずれかを使用できるようにします。
   - **Interface ID**: サービスポリシーがバインドされているWLAN論理インターフェースのID。
   - **Interface Type**: サービスポリシーにバインドされているインターフェースのタイプ。常に**WLAN-ESS**です。
   - **Max Clients**: サービスポリシーを使用してFIT APに関連付けることができるクライアントの最大数。
   - **Layer2 Isolation**: レイヤ2分離を有効または無効にします。このパラメーターは、ACで実行される**user-isolation vlan**コマンドと組み合わせて設定します。この機能を有効にすると、許可されたMACアドレスリスト内のクライアントは、同じVLAN内の他のクライアントと通信できます。たとえば、ACで**user-isolation vlan 1 permit-mac 0000-1111-2222**コマンドを実行し、レイヤ2分離を有効にすると、クライアント**0000-1111-2222**はVLAN 1内の他のクライアントにアクセスできますが、他のクライアントは相互にアクセスできません。

     注:

     レイヤ2分離をイネーブルにした後にクライアントがネットワークにアクセスするには、まずゲートウェイのMACアドレスを許可MACアドレスリストに追加します。

   - **Synchronize AC Configuration**: ACの指定されたACグループ内のすべてのACにサービスポリシーを適用します。このオプションを選択しない場合、サービスポリシーは現在の

ACにのみ適用されます。

- **AC Group**: サービスポリシーが適用されるACグループ。このフィールドは、**Synchronize AC Configuration**オプションが選択されていない場合は表示されません。

Security Information

- **Security IE**: FIT APによって送信されるビーコンフレームおよびプローブ応答で使用されるセキュリティIE。オプションは、**None**、**RSN**、**WPA**、および**All**です。

  Noneは、セキュリティIEが設定されていないことを示します。

  Allは、RSNとWPAの両方が構成されていることを示します。RSNとWPAの詳細については、関連するデバイスのマニュアルを参照してください。

- **Cipher Suite**: データレームの暗号化および復号化に使用される暗号スイート。オプションは次のとおりです:
  - **TKIP**
  - **CCMP**
  - **WEP40**
  - **WEP104**
  - **WEP128**
- **Key Index**: クライアントの認証キーインデックス。
- **Key**: クライアントの認証キー。

Comware 7 ACの場合:

Service policy basic information

- **Policy ID**: サービスポリシーのID。
- **SSID**: サービスポリシーのSSID。
- **Hide SSID**: FIT APによって送信されるビーコンフレームでSSIDを提供するかどうかを示します。このパラメーターが選択されている場合、クライアントはビーコンフレームからSSIDを取得できないため、ワイヤレスネットワークにアクセスする前にSSIDを設定する必要があります。このパラメーターが選択されていない場合

  選択すると、クライアントはビーコンフレームからSSIDを取得して、ワイヤレスネットワークにアクセスできます。

- **Enable Status**： サービスポリシーが有効かどうかを示します。オプションは次のとおりです。
  - **Enable**: サービスポリシーがAC上でイネーブルであり、ACがサービスを提供できることを示します。
  - **Disable**: サービスポリシーがACでイネーブルになっておらず、ACがサービスを提供できないことを示します。
  - **Not Ready**: サービスポリシーがACに導入されていて、ACがサービスを提供できないことを示します。
- **Max Clients**: サービスポリシーを使用してFIT APに関連付けることができるクライアントの最大数。
- **Synchronize AC Configuration**: ACの指定されたACグループ内のすべてのACにサービスポリシーを適用します。このオプションを選択しない場合、サービスポリシーは現在のACにのみ適用されます。
- **AC Group**: サービスポリシーが適用されるACグループ。このフィールドは、**Synchronize AC Configuration**オプションが選択されていない場合は表示されません。

Security Information

- **Security IE** :FIT APによって送信されるビーコンフレームおよびプローブ応答で使用されるセキュリティIE。オプションは、**None**、**RSN**、**WPA**、および**All**です。

NoneはセキュリティIEが設定されていないことを示します。

Allは、RSNとWPAの両方が構成されていることを示します。RSNとWPAの詳細については、関連するデバイスのマニュアルを参照してください。

- **Cipher Suite**: データフレームの暗号化および復号化に使用される暗号スイート。オプションは次のとおりです:
  - **TKIP**
  - **CCMP**
  - **WEP40**
  - **WEP104**
  - **WEP128**
- **Key**: クライアントの認証キー。このフィールドは、**Cipher Suite**が**WEP40**、**WEP104**、または**WEP128**に設定されている場合にのみ表示されます。
  AKM Mode: -認証およびキー管理モード。オプションは、**MAC**、**dot1x**、および**psk**です。
- **PSK**: 事前共有キー。このフィールドは、**AKM Mode**が**psk**に設定されている場合にのみ表示されます。

6. **Close**をクリックします。

サービスポリシーの追加

ACのサービスポリシーは、次の方法で追加できます。

- **Normal method**: サービスポリシー管理でサービスポリシーを追加します。
- **Express Method**: サービスポリシーテンプレートを選択し、そのテンプレートを使用してサービスポリシーを追加します。サービスポリシーテンプレートの詳細は、「サービスポリシーテンプレートの管理」を参照してください。

Comware 7 ACのサービスポリシーを追加するには、通常の方法しか使用できません。

サービスポリシーの設定を成功させるには、サービスポリシーのセキュリティ情報を設定する前に、CLIまたはWebインターフェースを使用してACのセキュリティIEおよび暗号スイートを設定します。

Using the normal method (Comware 5 AC)

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。
   AC ListページにすべてのACが表示されます。
3. ACの**Operation**アイコン ⋯ をクリックします。
4. メニューから**Service Policy**を選択します。
   Service Policy Managementページには、S**ervice Policy List**上のACのすべてのサービスポリシー情報が表示されます。
5. **Add Policy**をクリックします。
   サービスポリシーを追加するためのページが開きます。
6. 次のパラメーターを設定します。
   - **Policy ID**: サービスポリシーのIDを入力して、AC上のサービスポリシーを一意に識別します。
   - **Enable**: ACに適用された直後にサービスポリシーをイネーブルにする場合にだけ、このオプションを選択します。
   - **SSID**: サービスポリシーのSSIDを入力します。
   - **Coded Format:** SSIDのコード形式を選択します。オプションは、**default**、**GB2312**および

UTF-8。

- **Encryption Mode**: サービスポリシーの暗号化モードを選択します。オプションは次のとおりです。
  - **Clear**: データパケットを暗号化する必要はありません。
  - **Crypto**: すべてのデータパケットを暗号化する必要があります。
- **Hide SSID**: このオプションを選択すると、FIT APによって送信されるビーコンフレーム内のSSIDが非表示になります。このパラメーターを選択すると、クライアントはビーコンフレームからSSIDを取得できず、ワイヤレスネットワークにアクセスする前にSSIDを設定する必要があります。このパラメーターを選択しないと、クライアントはビーコンフレームからSSIDを取得できます。
- **Authentication Mode**: サービスポリシーの認証モードを選択します。暗号化モードが**Clear**の場合、認証モードは**Open System**だけです。暗号化モードが**Crypto**の場合、認証モードのオプションはOpen System、Shared Key、および**All**です。
  - **Open System**: 認証を要求するすべてのクライアントが直接認証を通過できるようにします。
  - **Shared Key**: クライアントはデバイスに設定されているものと同じ共有キーを使用する必要があります。**Shared Key**は、暗号スイートとして**WEP40**、**WEP104**、または**WEP128**を選択した場合にだけ指定します。
  - **All**: クライアントが必要に応じてオープンシステムモードまたは共有キーモードを使用できるようにします。
- **Binding Interface**: このパラメーターは強制的に選択され、追加するサービスポリシーにWLAN論理インターフェースをバインドする必要があります。
- **Interface ID**: サービスポリシーにバインドするインターフェースIDを入力します。IDが存在しないWLAN論理インターフェースを表す場合、WSMによってACのWLAN論理インターフェースが自動的に作成されます。サービスポリシーの設定を成功させるには、WLAN論理インターフェースが他のサービスポリシーにバインドされていないことを確認します。
- **Interface Type**: サービスポリシーにバインドするインターフェースのタイプを選択します。タイプは常に**WLAN-ESS**です。
- **Max Clients**: サービスポリシーを使用してFIT APに関連付けることができるクライアントの最大数。
- **Synchronize AC**: 指定したACグループ内のすべてのACにサービスポリシーを適用します。現在のACにのみサービスポリシーを適用するには、このオプションを選択しないでください。このオプションは、ACが少なくとも1つのACグループに属している場合にのみ使用できます。
- **AC Group**: ACグループを選択します。オプションは、現在のACが属するすべてのACグループです。このオプションは、**Synchronize AC Configuration**が選択されている場合にのみ使用できます。
- **Layer2 Isolation**: レイヤ2分離を有効または無効にします。このパラメーターは、AC上で実行される**user-isolation vlan**コマンドと組み合わせて設定する必要があります。この機能が有効な場合、許可されたMACアドレスリスト内のクライアントは、同じVLAN内の他のクライアントと通信できます。たとえば、AC上で**user-isolation vlan 1 permit-mac 0000-1111-2222**コマンドを実行してレイヤ2分離を有効にすると、クライアント**0000-1111-222**2はVLAN 1内の他のクライアントにアクセスできますが、他のクライアントは相互にアクセスできません。

注:

レイヤ2分離をイネーブルにした後にクライアントがインターネットにアクセスするには、まずゲートウェイのMACアドレスを許可MACアドレスリストに追加します。

- **Client Forwarding Mode**: リストから転送モードを選択します。オプションには、**remote**、

local、および**policy-based**があります。**remote**を選択すると、データパケットはACによって転送されます。**local**を選択すると、データパケットはACによって管理されるAPによって転送されます。**policy-based**を選択すると、データパケットは設定された転送ポリシーに基づいて転送されます。

7. **Encryption Mode**として**Crypto**を選択した場合は、必要に応じて次のセキュリティパラメーターを設定します。
   - **Security IE**: ビーコンフレームで使用されるセキュリティIEおよびFIT APによって送信されるプローブ応答を選択します。オプションは次のとおりです。
     - **None**: セキュリティIEが設定されていないことを示します。
     - **RSN**: 堅牢なセキュリティネットワークは、WPAよりも強力な保護を提供するために、堅牢なセキュリティネットワークアソシエーションの作成だけを可能にするセキュリティネットワークです。
     - **WPA**: WPAは、WPA-PSK(またはパーソナル)モードまたはWPA-802.1X(またはエンタープライズ)モードのいずれかで動作します。パーソナルモードでは、事前共有キーまたはパスフレーズが認証に使用されます。エンタープライズモードでは、802.1XおよびRADIUSサーバーとEAPが認証に使用されます。
     - **All**: RSNとWPAの両方が設定されていることを示します。

     RSNとWPAの詳細については、関連するデバイスのマニュアルを参照してください。
   - **Cipher Suite**: データフレームの暗号化および復号化に使用する暗号スイートを選択します。オプションは、**TKIP**、**CCMP**、**WEP40**、**WEP104**、および**WEP128**です。キーインデックスとキーは、**WEP40**、**WEP104**、または**WEP128**を選択した場合にのみ設定できます。**WEP40**、**WEP104**、および**WEP128**を同時に選択することはできません。
     - **WEP**: WEP40、WEP104、およびWEP128が含まれます。これらはすべて静的なWEP暗号化メカニズムです。WEP40キーは40ビット、WEP104キーは104ビット、およびWEP128キーは128ビットです。WEPはRC4暗号化を使用し、ワイヤレスネットワークにアクセスするすべてのクライアントが同じキーを使用する必要があります。
     - **TKIP**: Temporal Key Integrity Protocolは、WEPと同様にRC4アルゴリズムを使用しますが、WLANに対してより安全な保護を提供します。
     - **CCMP**: Counter mode with CBC-MAC Protocolは、Advanced Encryption Standard(AES;高度暗号化規格)にAES;高度暗号化規格)に基づくカウンタモード/CBC-MACメカニズムです。
   - **Key Index** :クライアントの認証キーインデックスを入力します。
   - **Key**: クライアントの認証キーを入力します。

     WEP40の場合、キーは5文字の英数字の文字列です。

     WEP104の場合、キーは13文字の英数字の文字列です。

     WEP128の場合、キーは16文字の英数字の文字列です。
8. **OK**をクリックします。

Using the normal method (Comware 7 AC)

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。

   AC ListページにすべてのACが表示されます。
3. ACの**Operation**アイコン ··· をクリックします。
4. メニューから**Service Policy**を選択します。

   Service Policy Managementページには、**Service Policy List**上のACのすべてのサービスポリシー情報が表示されます。

5. **Add Policy**をクリックします。

   サービスポリシーを追加するためのページが開きます。

6. 次のパラメーターを設定します。

   Basic Information

   - **Policy ID**: サービスポリシーのIDを入力して、AC上のサービスポリシーを一意に識別します。
   - **Enable**: ACに適用された直後にサービスポリシーをイネーブルにする場合にだけ、このオプションを選択します。
   - **SSID**: サービスポリシーのSSIDを入力します。
   - **Coded Format**: SSIDのコード形式を選択します。オプションは、デフォルト、GB2312およびUTF-8。
   - **Hide SSID**: このオプションを選択すると、FIT APによって送信されるビーコンフレーム内のSSIDが非表示になります。このパラメーターを選択すると、クライアントはビーコンフレームからSSIDを取得できず、ワイヤレスネットワークにアクセスする前にSSIDを設定する必要があります。このパラメーターを選択しないと、クライアントはビーコンフレームからSSIDを取得できます。
   - **Max Clients**: サービスポリシーを使用してFIT APに関連付けることができるクライアントの最大数を入力します。
   - **Synchronize AC**: 指定したACグループ内のすべてのACにサービスポリシーを適用します。現在のACのみにサービスポリシーを適用するには、このオプションを選択しないでください。このオプションは、ACが1つ以上のACグループに属している場合にのみ使用できます。
   - **AC Group**: ACグループを選択します。オプションは、現在のACが属するすべてのACグループです。このオプションは、**Synchronize AC Configuration**が選択されている場合にのみ使用できます。

   Security Information

   - **Security IE**: ビーコンフレームで使用されるセキュリティIEおよびFIT APによって送信されるプローブ応答を選択します。オプションは次のとおりです。
     - **None**: セキュリティIEが設定されていないことを示します。
     - **RSN**: 堅牢なセキュリティネットワークは、WPAよりも強力な保護を提供するために、堅牢なセキュリティネットワークアソシエーションの作成だけを可能にするセキュリティネットワークです。
     - **WPA**: Wi-Fi保護アクセス。WEPよりも高度な暗号化アルゴリズムを使用して、ワイヤレスネットワークを保護します。
     - **All**: RSNとWPAの両方が設定されていることを示します。

     表8に、セキュリティIEオプションと対応するセキュリティ情報パラメーターの設定を示します。

表8 セキュリティ情報の設定

セキュリティIE	セキュリティ情報パラメーター
なし	• **Cipher Suite**: データフレームの暗号化および復号化に使用する暗号スイートを選択します。オプションは、WEP40、**WEP104**および**WEP128**です。一度に選択できるオプションは1つのみです。 • **Key**:クライアントの認証キーを入力します。**WEP40**の場合、キーは5文字の英数字の文字列です。**WEP104**の場合、キーは13文字の英数字の文字列です。**WEP128**の場合、キーは16文字の英数字の文字列です。 • **AKM Mode**: ユーザーを認証し、キーを管理するための認証およびキー管理モードを選択します。オプションは**None**および**MAC**です。
RSN	• **Cipher Suite**: データフレームの暗号化および復号化に使用する暗号スイートを選択します。オプションは**TKIP**および**CCMP**です。**TKIP**と**CCMP**の両方を選択できます。
WPA	• **AKM Mode**: ユーザーを認証し、キーを管理するための認証およびキー管理モードを選択します。オプションは**dot1x**および**psk**です。
All	• **PSK**: **AKM**モードが**psk**に設定されている場合に事前共有キーを入力します。

高速メソッドを使用する

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。

   AC ListページにすべてのACが表示されます。
3. ACの**Operation**アイコン ··· をクリックします。
4. メニューから**Service Policy**を選択します。

   Service Policy Managementページには、**Service Policy List**上のACのすべてのサービスポリシー情報が表示されます。
5. **Select Template**をクリックします。

   WSM内のすべてのサービスポリシーテンプレートがリストに表示されます。

   Select Service Policy Template
   - **SSID**: サービスポリシーのSSID。
   - **Encryption Mode**: サービスポリシーの暗号化モード。**Clear**または**Crypto**。**Clear**モードは、データパケットを暗号化する必要がないことを意味します。**Crypto**モードは、すべてのデータパケットを暗号化する必要があることを意味します。
   - **Hide SSID**: FIT APによって送信されたビーコンフレームでSSIDが非表示になっているかどうかを示します。このパラメーターを選択すると、クライアントはビーコンフレームからSSIDを取得できず、ワイヤレスネットワークにアクセスする前にSSIDを設定する必要があります。このパラメーターを選択しないと、クライアントはビーコンフレームからSSIDを取得してワイヤレスネットワークにアクセスできます。
   - **Authentication Mode**: サービスポリシーの認証モード。オプションは次のとおりです。
     - **Open System**: 認証を要求するすべてのクライアントが直接認証を通過できるようにします。

- **Shared Key**: クライアントはデバイスに設定されているものと同じ共有キーを使用する必要があります。**Shared Key**は、暗号スイートとして**WEP40**、**WEP104**、または**WEP128**を選択した場合にだけ指定します。
- **All**: クライアントが必要に応じてオープンシステムモードまたは共有キーモードを使用できるようにします。

6. 使用するサービスポリシーテンプレートを選択します。
7. **Next**をクリックします。

   Select Service Policy Template contents

   - **Synchronize AC Configuration**: 指定したACグループ内のすべてのACにサービスポリシーを適用します。現在のACにのみグローバル構成を適用するには、このオプションを選択しないでください。このオプションは、ACが少なくとも1つのACグループに属している場合にのみ使用可能です。
   - **AC Group**: ACグループを選択します。オプションは、現在のACが属するすべてのACグループです。このオプションは、「AC構成の同期化」が選択されている場合にのみ使用できます。
   - **Policy ID**: サービスポリシーのIDを入力して、AC上のサービスポリシーを一意に識別します。
   - **Interface ID**: サービスポリシーにバインドされるインターフェースIDを入力します。IDが存在しないWLAN論理インターフェースを表す場合、WSMは自動的にWLAN論理インターフェースを作成します。

     サービスポリシーの設定を成功させるには、WLAN論理インターフェースが他のサービスポリシーにバインドされていないことを確認します。
8. **OK**をクリックします。

   Result Listページが開き、サービスポリシーを追加するための操作結果が表示されます。
9. 現在のACの**Service Policy Management**ページに戻るには、**Back**をクリックします。

サービスポリシーの変更

サービスポリシーの設定を成功させるには、サービスポリシーのセキュリティ情報を設定する前に、CLIまたはWebインターフェースを使用してACのセキュリティIEおよび暗号スイートを設定します。

サービスポリシーを変更するには

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。

   AC ListページにすべてのACが表示されます。
3. ACの**Operation**アイコン をクリックします。
4. メニューから**Service Policy**を選択します。

   Service Policy Managementページには、**AC on Service Policy List**のすべてのサービスポリシー情報が表示されます。
5. サービスポリシーの**Operation**アイコン をクリックします。
6. メニューから変更を選択します。

   Modify Service Policyページが開きます。
7. 必要に応じてサービスポリシーパラメーターを変更します。「通常の方法(Comware 5 AC)を使用する」および「通常の方法(Comware 7 AC)を使用する」を参照してください。

   サービスポリシーIDは変更できません。
8. **OK**をクリックします。

サービスポリシーにバインドされた無線の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。

   AC ListページにすべてのACが表示されます。
3. ACの**Operation**アイコン をクリックします。
4. メニューから**Service Policy**を選択します。

   Service Policy Managementページには、**Service Policy List**上のACのすべてのサービスポリシー情報が表示されます。
5. サービスポリシーの**Operation**アイコンをクリックします。
6. メニューから**Bound Radios**を選択します。

   Radio Listダイアログボックスが開きます。

   Bound Radiosリストには、現在のサービスポリシーにバインドされているすべての無線に関する情報が表示されます。

   Bound Radio List
   - **Radio ID**: 無線のID。
   - **Admin Status**: 無線の管理状態。オプションは**Up**および**Down**です。
   - **Radio Type**: 無線のタイプ。オプションは次のとおりです。
     802.11a
     802.11b
     802.11g
     802.11gn
     802.11an
   - **AP Label**: 無線が属するAPのラベル。
   - **AP Name**: 無線が属するAPの名前。
   - **SN**: 無線が属するAPのシリアル番号。
   - **Radio Policy Name**: 無線がバインドされている無線ポリシーの名前。
7. **Close**をクリックして、ダイアログボックスを閉じます。

サービスポリシーへの無線のバインド

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。

   AC ListページにすべてのACが表示されます。
3. ACの**Operation**アイコン をクリックします。
4. メニューから**Service Policy**を選択します。

   Service Policy Managementページには、**AC on Service Policy List**のすべてのサービスポリシー情報が表示されます。
5. ターゲットサービスポリシーを選択します。
6. **Radio List**領域で**Add**をクリックします。

   Select Deviceダイアログボックスが開きます。

7. 設定する無線を検索するためのクエリー基準を指定して、設定する無線を検索します。
   - **AP Label**: 無線が属するFIT APのラベルを入力します。WSMは、このフィールドのファジーマッチングをサポートします。
   - **AP Name**: 無線が属するFIT APの名前を入力します。WSMは、このフィールドのファジーマッチングをサポートします。
   - **Serial Number**: 無線が属するFIT APのシリアル番号を入力します。WSMは、このフィールドのファジーマッチングをサポートしています。
   - **Radio Type**: 無線タイプを選択します。オプションは次のとおりです。
     802.11a
     802.11b
     802.11g
     802.11gn
     802.11an
   - **Admin Status**: 無線の管理状態を選択します。オプションは**Up**および**Down**です。
   - **Radio Policy Name**: 無線にバインドされた無線ポリシーの名前を入力します。WSMは、このフィールドのファジーマッチングをサポートしています。
   - **Location**: FIT APが属するロケーションビューの名前を入力または選択します。WSMは、このフィールドのファジーマッチングをサポートしています。

   空のフィールドや**Unlimited**に設定されたフィールドは、クエリーの抽出条件にはなりません。
8. **Query**をクリックします。
   Radio Listには、クエリー基準に一致するすべての無線が表示されます。**Reset**をクリックすると、クエリー基準がクリアされ、すべての無線が表示されます。
9. サービスポリシーにバインドする無線を選択します。
10. **OK**をクリックして、**Select Device**ウィンドウを閉じます。**Radio List**に、選択したすべての無線が表示されます。
11. **Bind Policy**をクリックします。
    Result Listページが開き、サービスポリシーを無線にバインドする操作の結果が表示されます。

サービスポリシーからの無線のバインド解除

無線を複数のサービスポリシーにまとめてアンバインドすることも、1つのサービスポリシーにアンバインドすることもできます。アップ状態の無線をサービスポリシーからアンバインドすると、無線が提供するサービスが中断され、無線に関連付けられているすべてのクライアントがログオフされます。

複数のサービスポリシーから無線をバッチでアンバインドするには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Resource Management>ACs**を選択します。
   AC ListページにすべてのACが表示されます。
3. ACの**Operation**アイコン をクリックします。
4. メニューから**Service Policy**を選択します。
   Service Policy Managementページには、**Service Policy List**上のACのすべてのサービスポリシー情報が表示されます。
5. ターゲットサービスポリシーを選択します。
6. **Radio List**領域で**Add**をクリックします。

Select Deviceダイアログボックスが開きます。

7. 設定する無線を検索するためのクエリー基準を指定して、設定する無線を検索します。
   - **AP Label**: 無線が属するFIT APのラベルを入力します。WSMは、このフィールドのファジーマッチングをサポートします。
   - **AP Name**: 無線が属するFIT APの名前を入力します。WSMは、このフィールドのファジーマッチングをサポートします。たとえば、Bと入力すると、名前にBが含まれるFIT AP上のすべての無線が問い合せられます。
   - **Serial Number**: 無線が属するFIT APのシリアル番号を入力します。WSMは、このフィールドのファジーマッチングをサポートしています。
   - **Radio Type**: 無線タイプを選択します。オプションは次のとおりです。
     802.11a
     802.11b
     802.11g
     802.11gn
     802.11an
   - **Admin Status**: 無線の管理状態を選択します。オプションはUpおよびDownです。
   - **Radio Policy Name**: 無線にバインドされた無線ポリシーの名前を入力します。WSMは、このフィールドのファジーマッチングをサポートしています。
   - **Location**: FIT APが属するロケーションビューの名前を入力または選択します。WSMは、このフィールドのファジーマッチングをサポートしています。

   空のフィールドや無制限に設定されたフィールドは、クエリーの抽出条件にはなりません。
8. **Query**をクリックします。
   Radio Listには、クエリー基準に一致するすべての無線が表示されます。**Reset**をクリックすると、クエリー基準がクリアされ、すべての無線が表示されます。
9. サービスポリシーからバインド解除する無線を選択します。
10. **OK**をクリックして、**Select Radios**ウィンドウを閉じます。
    Radio Listに、選択したすべての無線が表示されます。
11. **Unbind**をクリックします。
    WSMはリスト内の無線を1つずつチェックします。サービスポリシーへのバインディングが検出されると、WSMはそのバインディングを削除します。プロセスが完了すると、**Result List**ページが開き、サービスポリシーと無線間のバインディングを削除するための操作結果が表示されます。

無線とサービスポリシー間のバインディングを削除するには、次の手順を実行します。

12. **Service**タブをクリックします。
13. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。
    AC ListページにすべてのACが表示されます。
14. ACの**Operation**アイコン ･･･ をクリックします。
15. メニューから**Service Policy**を選択します。
    Service Policy Managementページには、**Service Policy List**上のACのすべてのサービスポリシー情報が表示されます。
16. サービスポリシーの**Operation**アイコン ･･･をクリックします。
17. メニューから**Bound Radios**を選択します。
    Radio Listダイアログボックスが開きます。

18. バインド解除する無線を選択します。
19. 次のパラメーターを設定します。
    - **Synchronize AC Configuration**: 指定したACグループ内のすべてのACで、サービスポリシーから無線をアンバインドします。現在のACでのみサービスポリシーから無線をアンバインドするには、このオプションを選択しないでください。このオプションは、ACが少なくとも1つのACグループに属している場合にだけ使用できます。
    - **AC Group**: ACグループを選択します。オプションは、現在のACが属するすべてのACグループです。このオプションは、**Synchronize AC Configuration**が選択されている場合にのみ使用できます。
20. **Unbind**をクリックします。

    Result Listページが開き、サービスポリシーから無線をアンバインドする操作の結果が表示されます。
21. **Back**をクリックして、ダイアログボックスを閉じます。

サービスポリシーの削除

無線にバインドされているサービスポリシーを削除するには、まずサービスポリシーから無線のバインドを解除します。

サービスポリシーを削除するには

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。

   AC ListページにすべてのACが表示されます。
3. ACの**Operation**アイコン をクリックします。
4. メニューから**Service Policy**を選択します。

   Service Policy Managementページには、**Service Policy List**上のACのすべてのサービスポリシー情報が表示されます。
5. サービスポリシーの**Operation**アイコン をクリックします。
6. メニューから**Delete**を選択します。

   確認ダイアログボックスが表示されます。
7. **OK**をクリックします。

ACによって管理されるオンラインFIT APの表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。

   AC ListページにすべてのACが表示されます。
3. 次のいずれかの方法を使用します。
    - ACの**Online APs**列の番号をクリックします。
    - ACのデバイスラベルをクリックし、**Device Details**の**AP Information**エリアでページが表示されたら、**Online APs**の数をクリックします。

   FIT AP Listページには、ACによって管理されるすべてのオンラインFIT APが表示されます。FIT AP Listの詳細は、「FIT APリストの表示」を参照してください。

オンラインクライアントの表示

この機能を使用すると、ACによって管理されるFIT APに関連付けられたすべてのオンラインクライアントを表示できます。

オンラインクライアントを表示するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。

   AC ListページにすべてのACが表示されます。
3. 次のいずれかの方法を使用します。
   - ACの**Online Clients**列の番号をクリックします。
   - ACのデバイスラベルをクリックし、**Device Details**の**Client Information**領域でページが表示されたら、**Online Clients**の番号をクリックします。

   Online Client Listには、ACによって管理されているFIT APに関連付けられているすべてのオンラインクライアントが表示されます。**Online Client List**の詳細は、「クライアントリストの表示」を参照してください。

クライアント数量の監視

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。

   AC ListページにすべてのACが表示されます。
3. **Client Monitor**をクリックします。

   クライアントの数量を監視するページが開きます。
4. ページの右上隅にある**Select ACs**をクリックします。

   ACリストが表示されます。
5. 監視するACを最大5つ選択します。
6. **OK**をクリックします。

   折れ線グラフは、監視対象のACに接続されているクライアントの数をリアルタイムで示します。

ACのMPポリシーの表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。

   AC ListページにすべてのACが表示されます。
3. 次のいずれかの方法を使用します。
   - ACの**Operation**アイコン ··· をクリックし、メニューから**MP Policy Management**を選択します。
   - ACのデバイスラベルをクリックし、ページの右側にある**Mesh Management**領域で**MP Policy Management**リンクをクリックします。

     MP Policy Managementページが開きます。

   ACのすべてのメッシュポリシー情報がMPポリシーリストに表示されます。メッシュポリシーの追加、変更、削除、メッシュポリシーの詳細の表示、およびメッシュポリシーへの無線のバインドまたはバインド解除を行うことができます。詳細については、「MPポリシーの管理」を参照してください。

ACのメッシュプロファイルの表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。

   AC ListページにすべてのACが表示されます。
3. 次のいずれかの方法を使用します。
   - ACの**Operation**アイコン ··· をクリックし、メニューからメッシュプロファイルの管理を選択します。
   - ACのデバイスラベルをクリックし、ページの右側にある**Mesh Management**領域で**Mesh Profile Management**リンクをクリックします。

   Mesh Profile Managementページが開きます。

   ACのすべてのメッシュプロファイル情報がMesh Profile Listに表示されます。メッシュプロファイルの追加、変更、削除、メッシュプロファイル詳細の表示、およびメッシュプロファイルへの無線のバインドまたはバインド解除を行うことができます。詳細については、「MPポリシーの管理」を参照してください。

ACのメッシュインターフェースの表示

1. Serviceタブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。

   AC ListページにすべてのACが表示されます。
3. 次のいずれかの方法を使用します。
   - ACの**Operation**アイコン ··· をクリックし、**Mesh Interface Management**を選択します。の名前を変更します。
   - ACのデバイスラベルをクリックし、ページの右側にある**Mesh Management**領域で**Mesh Interface Management**リンクをクリックします。

   メッシュインターフェース管理ページが開きます。

   ACのすべてのメッシュインターフェース情報が**Mesh Interface List**に表示されます。メッシュインターフェースの追加、変更、削除、ポートセキュリティ設定の変更、またはメッシュインターフェースのVLANの変更を行うことができます。詳細については、「メッシュインターフェースの管理」を参照してください。

AC履歴情報の表示

この機能を使用すると、過去1時間、過去1日、過去1週間、過去1か月、またはユーザー定義の時間範囲におけるACトラフィックおよびレート履歴情報を表示できます。

- **Traffic statistics**: 統計情報収集の開始時刻と終了時刻、送信トラフィック、受信トラフィック、および合計トラフィックを表示します。
- **Rate statistics**: 指定した統計情報収集時間における送受信レートのトレンドグラフ、ピーク送信レート、ピーク受信レート、平均送信レート、および送受信レートを表示します。

ACの**History Information**ページには、ACリストページまたはAC詳細ページからアクセスできます。次の情報では、例としてACリストページを使用しています。

AC履歴情報を表示する手順は、次のとおりです。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。

   AC ListページにすべてのACが表示されます。
3. ComwareベースのACの**Operation**アイコン ⋯ をクリックしクリックし、**History Information**.を選択します。**History Information**.ダイアログボックスが開きます。
4. **Statistics**から統計タイプを選択します。

   オプションは**Traffic**と**Rate**です。デフォルトのオプションは**Traffic**です。
5. 統計収集の時間範囲を指定するには、**1h**、**1d**、**1w**、**1m**、または**1y**をクリックします。

   または、**Custom**をクリックします。開いた**Custom**ウィンドウで、開始時刻と終了時刻を入力するか、**Start Time/End Time**の横にあるフィールドをクリックして、表示されるカレンダーから開始時刻/終了時刻をYYYY-MM-DD hh:mm形式で選択します。

   指定した時間範囲内の統計情報が表示されます。
   - **Traffic Statistics**

     トラフィックの単位は、送受信されるトラフィックの量によって変化します。

     Trafficを選択すると、次の情報が表示されます。
     - **Start Time**: 統計情報収集の開始時刻。形式はYYYY-MM-DD hh:mm:ssです。
     - **End Time**: 統計情報収集の終了時刻。形式はYYYY-MM-DD hh:mm:ssです。
     - **Transmitted Traffic(B)**: 指定した時間範囲内にACによって送信されたトラフィックの合計。データが変更されると、測定単位も自動的に変更されます。
     - **Received Traffic(B)**: 指定した時間範囲内にACによって受信されたトラフィックの合計。測定単位は、データの変更に応じて自動的に変更されます。
     - **Total Traffic(B)**: 指定した時間範囲内にACによって送受信されたトラフィックの合計。この値は統計に基づいて計算され、実際の値とは若干異なる場合があります。測定単位はデータの変更に応じて自動的に変更されます。
   - **Rate Statistics**

     レートの単位は、レートの値によって変わります。**Rate**を選択すると、次の情報が表示されます。
     - **Transmission and Reception Rate Trend graph**: データ収集時間範囲内のACの送受信率のトレンド。x座標は時間を表し、y座標は送受信率を表します。
     - **Peak Transmission Rate(bps)**: 統計情報収集時間範囲内のACの最大送信レート。測定単位はデータの変更に応じて自動的に変更されます。
     - **Peak Reception Rate(bps)**: 統計情報収集時間範囲内のACの最大受信レート。測定単位はデータの変更に応じて自動的に変更されます。
     - **Average Transmission Rate(bps)**: 統計情報収集時間範囲内のACの平均送信レート。測定単位はデータの変更に応じて自動的に変更されます。
     - **Average Reception Rate(bps)**: 統計収集時間範囲内のACの平均受信レート。測定単位は、データの変更に応じて自動的に変更されます。
   - **Rate Details**

     トレンドグラフの上部にある**Rate**をクリックして、**Details**ウィンドウを表示します。
     - **Time**: 統計情報が収集される時刻。形式はYYYY-MM-DD hh:mm:ssです。
     - **Transmission Rate(bps)**: 指定した時刻のACの送信レート。
     - **Reception Rate(bps)**: 指定した時刻のACの受信レート。
6. **Close**をクリックします。

ロードバランシンググループの設定

WLANロードバランシングは主に高密度WLANネットワークに適用され、クライアントに適切な帯域幅を確保するためにAP間の負荷を動的に調整します。

異なるAPの無線間で負荷を分散するには、それらの無線を同じロードバランシンググループに追加します。ロードバランシンググループ内の無線は、設定に従ってセッションモードまたはトラフィックモードのロードバランシングを実行できます。

ロードバランシンググループ内の無線は、最大しきい値とギャップに達するとロードバランシングを開始します。無線は、負荷が最大しきい値を下回るか、またはギャップが最大ギャップより小さくならない限り、アソシエーション要求を受け入れません。

クライアントが指定された最大回数を超えて拒否された場合、APはクライアントが他のAPにアソシエートできないと判断し、クライアントからのアソシエーション要求を受け入れます。

ロードバランシンググループを有効にするには、ACのロードバランシンググループを設定する前に、Load Balancing Limitをイネーブルにし、関連するしきい値を設定します。どのロードバランシンググループにも追加されていない無線は、ロードバランシングを実行しません。

ロードバランシンググループリストの表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。

   AC ListページにすべてのACが表示されます。
3. ACのデバイスラベルをクリックします。
4. ページの右側にある**AC Configuration**領域で、**Load Balance Group**リンクをクリックします。**Load Balance Group List**ページが開きます。

   Load Balance Group List
   - **ID**: ロードバランシンググループのID。
   - **Description**: ロードバランシンググループの説明。
   - **Modify**: ロードバランシンググループを変更するには、**Modify**アイコンをクリックします。
   - **Delete**: ロードバランシンググループを削除するには、**Delete**アイコンをクリックします。

ロードバランスグループリストに十分なエントリーが含まれている場合は、次のナビゲーションエイドが表示されます:

- **Next Page**アイコンをクリックして、**Load Balance Group List**で次のページに進みます。
- **Last Page**アイコンをクリックして、**Load Balance Group List**の最後にページ転送します。
- **Previous Page**アイコンをクリックして、**Load Balance Group List**で前のページに戻ります。
- **First Page**アイコンをクリックすると、**Load Balance Group List**トの先頭に戻ります。

Load Balance Group Listの右上にある**8、15、50、100、または200**をクリックして、表示する1ページあたりの項目数を設定します。

Load Balance Group Listは、**ID**フィールドでソートできます。列ラベルをクリックすると、選択したフィールドでリストがソートされます。列ラベルを使用すると、各フィールドに固有の様々なソートオプションを切り替えることができます。

ロードバランシンググループの追加

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。
   AC ListページにすべてのACが表示されます。
3. ACのデバイスラベルをクリックします。
4. ページの右側にある**AC Configuration**領域で、**Load Balance Group**をクリックします。
   ACのロードバランシンググループ情報が**Load Balance Group List**に表示されます。
5. **Add**をクリックします。
   ロードバランシンググループを追加するためのページが開きます。
6. 次のパラメーターを設定します。
   - **ID**: ロードバランシンググループのIDを入力します。
   - **Description**: ロードバランシンググループの説明を入力します。
7. **OK**をクリックします。

ロードバランシンググループの変更

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。
   AC ListページにすべてのACが表示されます。
3. ACのデバイスラベルをクリックします。
4. ページの右側にある**AC Configuration**領域で、**Load Balance Group**をクリックします。
   ACのすべてのロードバランシンググループ情報が**Load Balance Group List**に表示されます。
5. ロードバランシンググループの**Modify**アイコンをクリックします。ロードバランシンググループを変更するためのページが開きます。
6. 次のパラメーターを変更します。
   - **ID**: 変更できません。
   - **Description**: ロードバランシンググループの説明を入力します。
7. **OK**をクリックします。

ロードバランシンググループの削除

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。
   AC ListページにすべてのACが表示されます。
3. ACのデバイスラベルをクリックします。
4. ページの右側にある**AC Configuration**領域で、**Load Balance Group**をクリックします。
   ACのすべてのロードバランシンググループ情報が**Load Balance Group List**に表示されます。
5. ロードバランシンググループの**Delete**アイコンをクリックします。確認ダイアログボックスが開きます。
6. **OK**をクリックします。

ロードバランシンググループ内の無線の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。

   AC ListページにすべてのACが表示されます。
3. ACのデバイスラベルをクリックします。
4. ページの右側にある**AC Configuration**領域で、**Load Balance Group**をクリックします。
   ACのすべてのロードバランシンググループ情報がLoad Balance Group Listに表示されます。
5. ターゲットロードバランシンググループのIDをクリックします。

   Radio Listページが開きます。

   Radio List
   - **AP Label**: 無線が属するFIT APのラベル。
   - **SN**: 無線が属するFIT APのシリアル番号。
   - **Radio ID**: 無線のID。
   - **Radio Type**: 無線のタイプ。オプションは次のとおりです。
     802.11a
     802.11b
     802.11g
     802.11gn
     802.11an
   - **Delete**: 無線を削除するには、**Delete**アイコンをクリックします。

ラジオリストに十分なエントリーが含まれている場合は、次のナビゲーション支援が表示されます。

- **Next Page**アイコンをクリックして、**Radio List**で次のページに進みます。
- **Last Page**アイコンをクリックして、**Radio List**の最後のページに進みます。
- **Previous Page**アイコンをクリックして、**Radio List**で前のページに戻ります。
- **First Page**アイコンをクリックすると、**Radio List**の先頭に戻ることができます。

Radio Listの右上にある**8、15、50、100、または200**をクリックして、表示する項目数を設定します。

Radio Listは、**Delete** fieldフィールド以外のすべてのフィールドで並べ替えることができます。列ラベルをクリックすると、選択したフィールドでリストが並べ替えられます。列ラベルを使用すると、各フィールドに固有の並べ替えオプションを切り替えることができます。

ロードバランシンググループへの無線の追加

ロードバランシンググループに追加された無線は、同じACによって管理されるFIT APに属します。ロードバランシンググループに無線を追加するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。

   AC ListページにすべてのACが表示されます。
3. ACのデバイスラベルをクリックします。
4. ページの右側にある**AC Configuration**領域で、**Load Balance Group**をクリックします。
   ACのすべてのロードバランシンググループ情報が**Load Balance Group List**に表示されます。
5. ロードバランシンググループのIDをクリックします。

ロードバランシンググループ内のすべての無線が**Load Balance Group Radio List**に表示されます。

6. **Radio List**領域で**Add**をクリックします。

   Select Deviceダイアログボックスが開きます。

7. 設定する無線を検索するためのクエリー基準を指定して、設定する無線を検索します。
   - **AP Label**: 無線が属するFIT APのラベルを入力します。WSMは、このフィールドのファジーマッチングをサポートします。
   - **AP Name**: 無線が属するFIT APの名前を入力します。WSMは、このフィールドのファジーマッチングをサポートしています。
   - **Serial Number**: 無線が属するFIT APのシリアル番号を入力します。WSMは、このフィールドのファジーマッチングをサポートしています。
   - Radio Type:無線タイプを選択します。オプションは次のとおりです。
     - **All**
     - **802.11a**
     - **802.11b**
     - **802.11g**
     - **802.11bg**
     - **802.11at**
     - **802.11gn**
     - **802.11an**
     - **802.11ac**
     - **802.11n(2.4GHz)**
     - **802.11bgn**
     - **802.11n**
     - **802.11n(5GHz)**
     - **802.11ac/n/a**
     - **wired**
   - **Admin Status**: 無線の管理状態を選択します。オプションはUpおよびDownです。
   - **Radio Policy Name**: 無線にバインドされた無線ポリシーの名前を入力します。WSMは、このフィールドのファジーマッチングをサポートしています。
   - **Location**: IT APが属するロケーションビューの名前を入力または選択します。WSMは、このフィールドのファジーマッチングをサポートしています。

   空のフィールドや**Unlimited**に設定されたフィールドは、クエリーの抽出条件にはなりません。

8. **Query**をクリックします。

   Radio Listには、クエリー基準に一致するすべての無線が表示されます。Resetをクリックすると、クエリー基準がクリアされ、すべての無線が表示されます。

9. ロードバランシンググループに追加する無線を選択します。
10. **OK**をクリックして、**Select Device**ウィンドウを閉じます。

    Radio Listに、選択したすべての無線が表示されます。

11. **OK**をクリックします。

ロードバランシンググループからの無線の削除

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > Resource Management > ACs**を選択します。
   AC Listページに、すべてのACが表示されます。
3. ACのデバイスラベルをクリックします。
4. ページの右側にある**AC Configuration**領域で、**Load Balance Group**をクリックします。
   ACのロードバランシンググループ情報が**Load Balance Group List**に表示されます。
5. 無線を削除するロードバランシンググループのIDをクリックします。ロードバランシンググループ内のすべての無線が**Radio List**に表示されます。
6. 次のいずれかの方法を使用します。
   - 削除する1つまたは複数の無線を選択し、**Delete**をクリックします。
   - 無線の**Delete**アイコンをクリックし、ダイアログボックスで**OK**をクリックします。
7. **OK**をクリックします。

サポートされているFIT APモデルの表示

この機能を使用すると、ACでサポートされているFIT APモデルを表示できます。FIT APモデルリストに表示される情報には、APモデル、名前、無線の数、無線に関連付けることができるクライアントの最大数、ベンダー、CPUモデルと周波数、メモリモデルとそのサイズ、およびフラッシュモデルとそのサイズが含まれます。この機能を使用すると、管理者は、ACでサポートされているすべてのFIT APモデルに関する情報をすばやく取得でき、ワイヤレスネットワークの計画をサポートできます。

サポートされているFIT APモデルを表示するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。
   AC ListページにすべてのACが表示されます。
3. ACのデバイスラベルをクリックします。
4. ページの右側にある**AC Configuration**領域で、**View Supported FIT AP Models**リンクをクリックします。
   List of Supported AP Modelsページが開き、現在のACでサポートされているすべてのFIT APモデルがリストに表示されます。
   List of Supported AP Models
   - **Model**: FIT APのモデル。
   - **Name**: FIT APモデルのエイリアス。
   - **Radios/Clients**: FIT AP上の無線の数と、FIT APに関連付けることができるクライアントの最大数。
   - **Vendor**: FIT APのベンダー。常にH3Cです。
   - **CPU Model/Frequency**: FIT APのCPUモデルおよび周波数。
   - **Memory Model/Size**: FIT APのメモリモデルと容量。
   - **Flash Model/Size**: フラッシュモデルおよびFIT APの容量。

注:

List of Supported AP Modelsは、モデル、別名、およびベンダー別にソートできます。列ラベルをクリックすると、選択したフィールド別にリストがソートされます。列ラベルを使用すると、各フィールドに固有の様々なソートオプションを切り替えることができます。

CAPWAPトンネル情報の表示

Control And Provisioning of Wireless Access Points(CAPWAP)は、APがACと通信する方法を定義します。APとAC間の一般的なカプセル化および転送メカニズムを提供します。

CAPWAPはUDPを採用し、IPv4とIPv6の両方をサポートします。CAPWAPは、データパケットを転送するためのデータトンネルと、APの設定および管理に使用される制御パケットを転送するための制御トンネルを提供します。使用すると、ACは管理者から提供された情報に基づいてAPを自動的に設定および管理できます。

CAPWAPトンネル情報を表示するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。**AC List**ページにすべてのACが表示されます。
3. ACのデバイスラベルをクリックします。
4. ページの右側にある**AC Configuration**領域で、**View CAPWAP Channel Information**リンクをクリックします。

   CAPWAP Channel Information Listが表示され、リスト内のACのすべてのCAPWAPトンネル情報が表示されます。

   CAPWAP Channel Information List

   - **FIT AP Name**: FIT APの名前。
   - **Control Channel Security Policy**: CAPWAPコントロールトンネルで使用されるセキュリティポリシー。
   - **Control Channel Startup Time**: CAPWAP制御トンネルの起動時間。
   - **Data Channel Security Policy**: CAPWAPデータトンネルで使用されるセキュリティポリシー。
   - **Data Channel Startup Time**: CAPWAPデータトンネルの起動時間。

APライセンス情報の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。

   AC ListページにすべてのACが表示されます。
3. ACのデバイスラベルをクリックします。

   ACの詳細ページが開きます。
4. ページの右側にある**AC Configuration**領域で**View AP License Information**をクリックします。**AP License Information**ウィンドウが開きます。

   AP License Information

   - **Associated AP**: ACで管理できるAPの数。APには、デフォルトでACで管理できるAPと、アクティブ化されたライセンスで許可されているAPが含まれます。
   - **Max AP Count**: ACで管理できるAPの最大数。
   - **Default AP Count**: デフォルトでACによって管理できるAPの数。次のリストに、ACに登録されているAPライセンスを示します。
   - **Number**: ライセンス番号。

- **License Key**: 標準ライセンスのライセンスキー。ライセンスキーを取得するには、ソフトウェアライセンス証明書を購入します。
- **Activation Key**: Webサイトでデバイスのライセンスキー、シリアル番号、および検証コードを提供することによって取得されるアクティベーションキー。
- **AP Limit**: ライセンスで許可されているAPの数。

5. **Close**をクリックします。

WLAN RRMの設定

WLAN Radio Resource Management(RRM)は、スケーラブルな無線リソース管理ソリューションです。APはリアルタイムで無線環境情報を収集し、分析のためにACに送信します。分析結果に基づいて、ACは無線リソース調整設定を行います。APは、無線リソース最適化のためにACによって行われた設定を実装します。したがって、WLAN RRMは、情報収集、情報分析、意思決定、および実装を通じて、リアルタイムでインテリジェントな統合無線リソース管理ソリューションを提供します。これにより、WLANネットワークは無線環境の変化に迅速に適応し、健全な状態を維持できます。

RRMグローバルパラメーターの設定

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。

   AC ListページにすべてのACが表示されます。
3. ACのデバイスラベルをクリックします。
4. ページの右側にある**RRM Management**領域の**RRM Configuration**リンクをクリックします。
5. 次のパラメーターを設定します。
   - **Radio Type**: 無線タイプを選択します。オプションは802.11aおよび802.11b/gです。
   - **Dynamic Channel Selection**: 動的チャネル選択をイネーブルまたはディセーブルにします。このパラメーターを使用すると、ACはリアルタイムでチャネルをスキャンできるため、各FIT APは最適なチャネルを使用し、レーダーや電子レンジなどの干渉が存在するチャネルの使用を回避できます。FIT APがACによる動的チャネル選択を受け入れるように設定するには、FIT AP無線設定のChannel Lockオプションとともにこのオプションを使用します。詳細については、「FIT APの無線パラメーターの変更」を参照してください。

     ダイナミックチャネル選択がイネーブルになっている場合は、CRC Error Threshold、Channel Interfere Threshold、およびTolerance Factorを設定する必要があります。CRCエラーしきい値またはチャネル干渉しきい値に達すると、ACはAPの新しいチャネルを選択します。ただし、APは、古いチャネルと新しいチャネルの差がTolerance factorを超えるまで、新しいチャネルを使用しません。
   - **Dynamic Power Selection**: 動的電力選択を有効または無効にします。このパラメーターにより、ACは無線環境に応じてFIT APの送信レートを動的に調整できます。FIT APの無線設定でPower Lockオプションとともにこのオプションを使用すると、FIT APがACによる動的電力選択を受け入れるように設定できます。詳細については、「FIT APの無線パラメーターの変更」を参照してください。
   - **Adjacency Factor**: ネイバーの最大数を設定します。ACによって管理されるAPの数が制限に達すると、ACはRRM設定に基づいてすべてのAPのチャネルと送信電力を自動的に調整します。たとえば、ネイバーの最大数が4の場合、ACによって管理されるAPの数が4に達すると、ACはすべてのAPのチャネルと送信電力を調整します。
   - **Calibration Interval(M)**: チャネル/電力の動的選択の調整間隔を入力します。チャネル/電力の動的選択がイネーブルの場合、ACはチャネル/電力の動的選択を実行し、調整間隔ごとに調整されたチャネル/電力をAPに適用します。

6. **OK**をクリックします。

RRM調整グループの設定

無線にDFSまたはTPCが設定されている場合、ACは調整間隔で無線のチャネル品質または電力を計算します。その結果がトリガー条件を満たすと、ACは無線の新しいチャネルまたは電力を選択します。

深刻な干渉環境では、チャネルまたは電力を頻繁に調整すると、WLANネットワークへのユーザーアクセスに影響する可能性があります。この場合、指定したホールドダウン時間内にグループ内の無線のチャネルまたは電力を変更しないように、RRM調整グループを設定できます。RRM調整グループ内にない無線のチャネルおよび電力は、通常どおり調整されます。

ホールドダウン時間が経過すると、ACはチャネルまたは電力を再計算します。結果がトリガー条件に一致すると、チャネルまたは電力が変更され、新しいチャネルまたは電力は指定されたホールドダウン時間内に変更されません。このメカニズムは継続します。

RRM調整グループリストの表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。

   AC ListページにすべてのACが表示されます。
3. ACのデバイスラベルをクリックします。
4. ページの右側にある**RRM Management**領域で、**RRM Calibration Group**をクリックします。

   RRM Calibration Group Listが表示されます。

   RRM Calibration Group List
   - **ID**: RRM調整グループのID。
   - **Channel Hold Time(M)**: RRM調整グループ内の無線のチャネルホールドダウン時間。
   - **Power Hold Time(M)**: RRM調整グループ内の無線の電力ホールドダウン時間。
   - **Description**: RRM調整グループの説明。
   - **Modify**: Modifyアイコンをクリックして、RRM調整グループを変更します。
   - **Delete**: Deleteアイコンをクリックして、RRM調整グループを削除します。

RRM Calibration Group Listに十分なエントリーが含まれている場合は、次のナビゲーション支援が表示されます。

- **Next Page**アイコンをクリックして、**RRM Calibration Group List**で次のページに進みます。
- **Last Page**アイコンをクリックして、**RRM Calibration Group List**の最後のページに進みます。
- **Previous Page**アイコンをクリックして、**RRM Calibration Group List**のページを逆方向に移動します。
- **First Page**アイコンをクリックすると、**RRM Calibration Group List**の先頭ページに戻ることができます。

RRM Calibration Group Listの右上にある**8、15、50、100、または200**をクリックして、表示する1ページあたりの項目数を設定します。

RRM Calibration Group Listは、**ID**、**Channel Hold Time**、および**Power Hold Time**の各フィールドでソートできます。選択したフィールドでリストをソートするには、列ラベルをクリックします。列ラベルを使用すると、各フィールドに固有のソートオプションを切り替えることができます。

RRM調整グループの追加

1. **Service**タブをクリックします。

2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。

   AC ListページにすべてのACが表示されます。
3. ACのデバイスラベルをクリックします。
4. ページの右側にある**RRM Management**領域で、**RRM Calibration Group**をクリックします。

   ACのすべてのRRM調整グループ情報は、**RRM Calibration Group List**に表示されます。
5. **Add**をクリックします。

   RRM調整グループを追加するためのページが開きます。
6. 次のパラメーターを設定します。
   - **ID**: RRM調整グループのIDを入力します。
   - **Channel Hold Time(M)**: RRM調整グループ内の無線のチャネルホールドダウン時間を入力します。
   - **Power Hold Time(M)**: RRM調整グループの無線の電力ホールドダウン時間を入力します。
   - **Description**: RRM調整グループの説明を入力します。
7. **OK**をクリックします。

RRM調整グループの変更

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。

   AC ListページにすべてのACが表示されます。
3. ACのデバイスラベルをクリックします。
4. ページの右側にある**RRM Management**領域で、**RRM Calibration Group**をクリックします。

   ACのすべてのRRM調整グループ情報は、**RRM Calibration Group List**に表示されます。
5. RRM調整グループの**Modify**アイコンをクリックします。

   Modify RRM Calibration Groupページが開きます。
6. 次のパラメーターを変更します。
   - **ID**: 変更できません。
   - **Channel Hold Time(M)**: RRM調整グループ内の無線のチャネルホールドダウン時間を入力します。
   - **Power Hold Time(M)**: RRM調整グループの無線の電力ホールドダウン時間を入力します。
   - **Description**: RRM調整グループの説明を入力します。
7. **OK**をクリックします。

RRM調整グループの削除

RRMキャリブレーショングループが削除されると、グループ内の無線はチャネルホールドダウン時間および電力ホールドダウン時間を調整しなくなります。

RRM調整グループを削除するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。

   AC ListページにすべてのACが表示されます。
3. ACのデバイスラベルをクリックします。
4. ページの右側にある**RRM Management**領域で、**RRM Calibration Group**をクリックします。

   ACのすべてのRRM調整グループ情報は、**RRM Calibration Group List**に表示されます。

5. RRM調整グループの**Delete**アイコンをクリックします。
   確認のダイアログボックスが開きます。
6. **OK**をクリックします。

RRM調整グループ内の無線の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。
   AC ListページにすべてのACが表示されます。
3. ACのデバイスラベルをクリックします。
4. ページの右側にある**RRM Management**領域で、**RRM Calibration Group**をクリックします。
   ACのすべてのRRM調整グループ情報は、**RRM Calibration Group List**に表示されます。
5. RRM調整グループのIDをクリックします。
   Radio List of RRM Calibrationページが開きます。
   RRMキャリブレーショングループの無線リスト
   - **AP Labe**l: 無線が属するFIT APのラベル。
   - **SN**: 無線が属するFIT APのシリアル番号。
   - **Radio ID**:無線のID。
   - **Radio Type**: 無線タイプを選択します。オプションは次のとおりです。
     802.11a
     802.11b
     802.11g
     802.11gn
     802.11an
   - **Delete**:無線を削除するには、**Delete**アイコンをクリックします。

RRM Calibration Group Radio Listに十分なエントリーが含まれている場合は、次のナビゲーション支援が表示されます。

- **Next Page**アイコンをクリックして、**RRM Calibration Group Radio List**で次のページに進みます。
- **Last Page**アイコンをクリックして、**RRM Calibration Group Radio List**の最後のページに進みます。
- **Previous Page**アイコンをクリックして**RRM Calibration Group Radio List**の前のページに戻ります。
- **First Page**アイコンをクリックすると、**RRM Calibration Group Radio List**の先頭ページに戻ることができます。

RRM Calibration Group Radio Listの右上にある**8、15、50、100、または200**をクリックして、表示する1ページあたりの項目数を設定します。

RRM調整グループへの無線の追加

RRM調整グループに追加された無線は、同じACによって管理されるFIT APに属します。RRM調整グループに無線を追加するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。

AC ListページにすべてのACが表示されます。

3. ACのデバイスラベルをクリックします。
4. ページの右側にある**RRM Management**領域で、**RRM Calibration Group**をクリックします。

   ACのすべてのRRM調整グループ情報は、**RRM Calibration Group List**に表示されます。
5. RRM調整グループのIDをクリックします。

   RRMキャリブレーショングループのすべての無線に関する情報は、R**adio List of RRM Calibration Group**に表示されます。
6. RRM領域の**Radio List**で**Add**をクリックします。

   Select Deviceダイアログボックスが開きます。
7. 設定する無線を検索するためのクエリー基準を指定して、設定する無線を検索します。
   - **AP Label**: 無線が属するFIT APのラベルを入力します。WSMは、このフィールドのファジーマッチングをサポートします。
   - **AP Name**: 無線が属するFIT APの名前を入力します。WSMは、このフィールドのファジーマッチングをサポートします。
   - **Serial Number**: 無線が属するFIT APのシリアル番号を入力します。WSMは、このフィールドのファジーマッチングをサポートしています。
   - **Radio Type**: 無線タイプを選択します。オプションは次のとおりです。

     802.11a

     802.11b

     802.11g

     802.11gn

     802.11an
   - **Admin Status**: 無線の管理状態を選択します。オプションはUpおよびDownです。
   - **Radio Policy Name**: 無線にバインドされた無線ポリシーの名前を入力します。WSMは、このフィールドのファジーマッチングをサポートしています。
   - **Location**: FIT APが属するロケーションビューの名前を入力または選択します。WSMは、このフィールドのファジーマッチングをサポートしています。

   空のフィールドや無制限に設定されたフィールドは、クエリーの抽出条件にはなりません。
8. **Query**をクリックします。

   Radio Listには、クエリー基準に一致するすべての無線が表示されます。**Reset**をクリックすると、クエリー基準がクリアされ、すべての無線が表示されます。
9. RRM調整グループに追加する無線を選択します。
10. **OK**をクリックして、デバイスの選択ウィンドウを閉じます。

RRM調整グループからの無線の削除

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。

   AC ListページにすべてのACが表示されます。
3. ACのデバイスラベルをクリックします。
4. ページの右側にある**RRM Management**領域で、**RRM Calibration Group**をクリックします。

   ACのRRM調整グループ情報は、**RRM Calibration Group List**に表示されます。
5. RRM調整グループのIDをクリックします。

   RRMキャリブレーショングループのすべての無線に関する情報は、**Radio List of RRM**

Calibration Groupに表示されます。

6. 次のいずれかの方法を使用します。
   - 削除する1つまたは複数の無線を選択し、**Delete**ボタンをクリックします。
   - 削除する無線の**Delete**アイコンをクリックし、確認ダイアログボックスで**OK**をクリックします。
7. OKをクリックします。

802.11レートの設定

この機能を使用すると、802.11a、802.11b、および802.11g 無線でサポートされるレート、必須レート、およびディセーブルレートを変更できます。

802.11レートを設定するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。

   AC ListページにすべてのACが表示されます。
3. ACのデバイスラベルをクリックします。
4. ページの右側にある**RRM Management**領域で、**Rate Set Configuration**をクリックします。
5. **802.11a Configuration**タブ、**802.11b Configuration**タブ、または**802.11g Configuration**タブを選択して、**Supported Rate**、**Mandatory Rate**、または**Disabled Rate**タイプの無線レートを設定します。
   - **802.11a Configuration**タブで、**Supported Rate**、**Mandatory Rate**、または**Disabled Rate**タイプには次のものがあります。
     - **6 Mbps**
     - **9 Mbps**
     - **12 Mbps**
     - **18 Mbps**
     - **24 Mbps**
     - **36 Mbps**
     - **48 Mbps**
     - **54 Mbps**
   - **802.11b Configuration**タブで、**Supported Rate**、**Mandatory Rate**、または**Disabled Rate**タイプには次のものがあります。
     - **1 Mbps**
     - **2 Mbps**
     - **5.5 Mbps**
     - **11 Mbps**
   - **802.11g Configuration**タブで、**Supported Rate**、**Mandatory Rate**、または**Disabled Rate**タイプには次のものがあります。
     - **1 Mbps**
     - **2 Mbps**
     - **5.5 Mbps**
     - **6 Mbps**
     - **9 Mbps**
     - **11 Mbps**
     - **12 Mbps**

- **18 Mbps**
- **24 Mbps**
- **36 Mbps**
- **48 Mbps**
- **54 Mbps**

6. レートタイプを選択して、対応するレートを設定します。
7. **OK**をクリックします。

MCSの設定

必須でサポート対象の802.11anまたは802.11gnレートを設定するには、最大Modulation and Coding Scheme(MCS)インデックスを指定します。MCSデータレートテーブルには、データレート、MCSインデックス、およびデータレートに影響するパラメーター間の関係が表示されます。

802.11レートは次のタイプに分類されます。

- Mandatory rates
- Supported rates
- Multicast rates。

WSMでは、必須レートとサポートされるレートがサポートされています。MCSを設定するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Resource Management>ACs**を選択します。

   AC ListページにすべてのACが表示されます。
3. ACのデバイスラベルをクリックします。
4. ページの右側にある**RRM Management**領域で、**MCS Set Configuration**をクリックします。
   - **Max Index of Mandatory MCS Set**: 最大必須MCSを入力します。FIT APは必須レートをサポートしている必要があります。クライアントは、必須レートをサポートしている場合にだけ、FIT APにアソシエートできます。
   - **Max Index of Support MCS Set**: サポートされる最大MCSを入力します。必須の最大MCSよりも小さくすることはできません。これらは、必須レート以外にAPでサポートされるより高いレートです。サポートされるレートにより、必須レートとサポートされるレートの両方をサポートする一部のクライアントは、APと通信するときにより高いレートを選択できます。
5. **OK**をクリックします。

注:

MCS Set Configurationリンクは、ACが802.11anまたは802.11gnをサポートしている場合にだけ表示されます。

AC階層の設定

AC階層型ネットワークには、中央AC、ローカルAC、およびAPが含まれます。中央ACはすべてのローカルACを管理し、ローカルACはAPへのWLANアクセスを提供し、クライアントトラフィックを処理します。

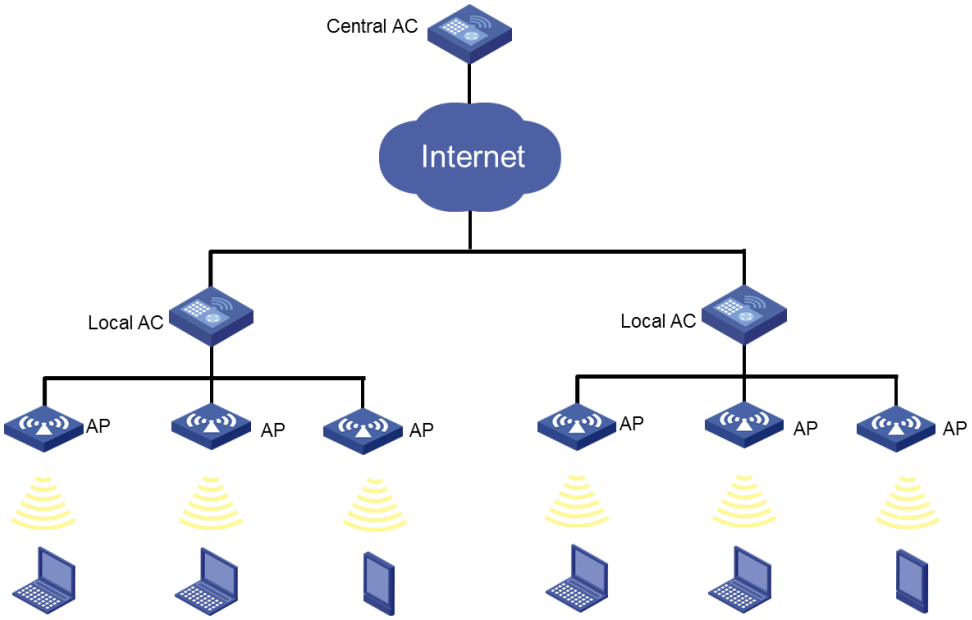
AC階層は、次のいずれかのシナリオで使用して、WLANのメンテナンスを簡素化し、WLANの拡張性を向上させることができます。

- 本社+支社のシナリオでは、本社に中央ACが導入され、支社にローカルACが導入されます。
- 中央のACがコアレイヤに配置され、ローカルACがアクセスレイヤに配置されている大規模な

企業ネットワーク。

AC階層をサポートするのは、Comware7ソフトウェアバージョンを実行するACだけです。

図63 AC階層



中央ACの設定

WSMを使用すると、中央ACに関連付けられたローカルACに関する情報を表示したり、ローカルACを追加、変更、または削除したりできます。

ローカルACリストの表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。

   AC ListページにすべてのACが表示されます。
3. ターゲット中央ACのデバイスラベルをクリックします。

   Local AC Listには、中央ACに関連付けられたすべてのローカルACが表示されます。

   Local AC List
   - **Status**: ローカルACのステータス。オプションはオンラインとオフラインです。
   - **Serial ID**: ローカルACのシリアルID。
   - **Local AC Name**: ローカルACの名前。オンラインローカルACの名前をクリックすると、その概要情報ページを表示できます。
   - **IP Address**: ローカルACの管理IPアドレス。このフィールドには、ローカルACがオフラインの場合に0.0.0.0と表示されます。
   - **Model**: ローカルACのモデル。
   - **Modify**: ローカルACを変更するには、**Modify**アイコンをクリックします。
   - **Delete**: **Delete**アイコンをクリックして、ローカルACを削除します。

ローカルACの追加

1. **Service**タブをクリックします。

2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。

   AC ListページにすべてのACが表示されます。
3. ターゲット中央ACのデバイスラベルをクリックします。

   Local AC Listには、中央ACに関連付けられたすべてのローカルACが表示されます。
4. **Add**をクリックします。

   Add Local ACページが開きます。
5. 次のパラメーターを設定します。
   - **Local AC Name**: ローカルAC名を1～63文字の文字列で入力します。名前に使用できるのは、文字、数字、およびアンダースコア(_)だけです。
   - **Serial ID**: ローカルACのシリアルIDを1～64文字の文字列で入力します。シリアルIDには、疑問符(?)、アポストロフィ(')、またはスペースを含めることはできません。
   - **Model**: ローカルACモデルを選択します。

6. **OK**をクリックします。

ローカルACの変更

この機能を使用すると、ローカルACのシリアルIDを変更できます。

ローカルACのシリアルIDを変更するには、以下の手順に従ってください。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。

   AC ListページにすべてのACが表示されます。
3. ターゲット中央ACのデバイスラベルをクリックします。

   Local AC Listには、中央ACに関連付けられたすべてのローカルACが表示されます。
4. ターゲットローカルACの**Modify**アイコンをクリックします。
5. ACのシリアルIDを変更します。
6. **OK**をクリックします。

ローカルACの削除

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。

   AC ListページにすべてのACが表示されます。
3. ターゲット中央ACのデバイスラベルをクリックします。

   Local AC Listには、中央ACに関連付けられたすべてのローカルACが表示されます。
4. ターゲットローカルACの**Delete**アイコンをクリックします。確認のダイアログボックスが開きます。
5. **OK**をクリックします。

ローカルACの設定

この関数を使用すると、ローカルAC機能を有効にして、ローカルACに中央ACを指定できます。

ローカルACを設定するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。

AC ListページにすべてのACが表示されます。

3. ターゲットローカルACのデバイスラベルをクリックします。
4. **AC Configuration**領域で**Configure Local AC Settings**をクリックします。
5. **Enable Local AC**を選択します。
6. メニューで中央ACのIPアドレスを選択します。
7. **OK**をクリックします。

サポートされているローカルACモデルの表示

この機能を使用すると、中央ACでサポートされているローカルACモデルを表示できます。

サポートされているローカルACモデルを表示するには、次の手順を実行します:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。

   AC ListページにすべてのACが表示されます。
3. ターゲット中央ACのデバイスラベルをクリックします。
4. **AC Configuration**領域で**View Supported Local AC Models**をクリックします。

   ローカルACリスト
   - **Model**: ローカルACモデル。
   - **Name**: ローカルAC名。
   - **Vendor**: ローカルACベンダー。
   - **CPU Model/Frequency**: ローカルACでサポートされているCPUモデルおよび周波数。
   - **Memory Model/Size**: ローカルACでサポートされているメモリーのモデルとサイズ。
   - **Flash Model/Size**: ローカルACでサポートされているフラッシュモデルおよびサイズ。

ACグループの管理

WSMは、プライマリ/セカンダリメカニズムを使用して高可用性を保証します。2つ以上のACを1つのACグループに追加し、1つ以上のACをプライマリ状態で動作するように構成できます。他のACはセカンダリ状態で動作します。

プライマリACがダウンすると、セカンダリACがすぐにプライマリACの役割を引き継ぎます。

同じACグループ内のACは相互にバックアップします。グループ内のすべてのACはアクティブに動作し、他のACのセカンダリACとして機能します。プライマリACとセカンダリACの設定は同じです。

ACグループリストの表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Configuration Management**を選択します。

   Configuration Managementページが開きます。
3. **Comware-Based**タブをクリックします。
4. **Network Management**領域で、**AC Group**をクリックします。**AC Group List**ページにすべてのACグループが表示されます。

   AC Group List

- **Group Name**: ACグループの名前。グループの名前をクリックすると、その詳細が表示されます。詳細は、「ACグループの詳細の表示」を参照してください。
- **Modify**: ACグループの名前を変更するには、**Modify**アイコン  をクリックします。詳細は、「ACグループの変更」を参照してください。
- **Delete**: ACグループを削除するには、**Delete**アイコン  をクリックします。詳細は、「ACグループの削除」を参照してください。

5. 最新のACグループリストを表示するには、**Refresh**をクリックします。

ACグループリストに十分な数のエントリーが含まれている場合は、次のナビゲーションツールが表示されます。

-  **Next Page**アイコンをクリックして、**AC Group List**で次のページに進みます。
-  **Last Page**アイコンをクリックして、**AC Group List**の最後のページに進みます。
- **Previous Page**アイコンをクリックして、**AC Group List**の前のページに戻ります。
-  **First Page**アイコンをクリックすると、**AC Group List**の先頭に戻ることができます。

ACグループリストの右上にある**8、15、50、100**、または**200**をクリックして、各ページに表示する項目数を指定します。

ACグループリストは、グループ名フィールドで並べ替えることができます。列のラベルをクリックすると、選択したフィールドを並べ替えることができます。

ACグループの詳細の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Configuration Management**を選択します。

   Configuration Managementページが開きます。
3. Comware-Basedタブをクリックします。
4. **Network Management**領域で、AC Groupをクリックします。

   AC Group Listページが開きます。
5. ACグループの名前をクリックすると、詳細が表示されます。

   AC Listには、グループ内のすべてのACが表示されます。

   AC List
   - **Status**: ACの現在のアラームステータス。
   - **Device Label**: ACのデバイスラベル。ターゲットACのラベルをクリックすると、その詳細が表示されます。
   - **Model** :ACのデバイスモデル。
   - **IP Address**: ACのIPアドレス。
   - **Online FIT APs**: ACによって管理されるオンラインFIT APの数。オンラインFIT APの数を示すリンクをクリックすると、**Fit AP Lis**が表示されます。
   - **Online Clients**: ACのFIT APにログインしているオンラインクライアントの合計数。オンラインクライアントの数を示すリンクをクリックすると、クライアントリストが表示されます。リストの詳細は、「クライアントリストの表示」を参照してください。
6. 最新のACリストを表示するには、**Refresh**をクリックします。

ACリストに十分なエントリーが含まれている場合は、次のナビゲーション支援が表示されます。

-  **Next Page**アイコンをクリックして、**AC List**の次のページに移動します。

- **Last Page**アイコンをクリックすると、**AC List**の最後に移動します。
- **Previous Page**アイコンをクリックして、**AC List**で前のページに戻ります。
- **First Page**アイコンをクリックすると、**AC List**の先頭に戻ることができます。

ACリストの右上にある**8**、**15**、**50**、**100**、または**200**をクリックして、各ページに表示する項目の数を指定します。

フィールドごとにACリストを並べ替えることができます。列ラベルをクリックすると、選択したフィールドごとにリストが並べ替えられます。列ラベルを使用すると、各フィールドに固有の並べ替えオプションを切り替えることができます。

ACグループの追加

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Configuration Management**を選択します。
   Configuration Managementページが開きます。
3. **Comware-Based**タブをクリックします。
4. **Network Management**領域で、**AC Group**をクリックします。**AC Group List**にすべてのACグループが表示されます。
5. **Add**をクリックします。
   Add AC Groupページが開きます。
6. 新しいACグループの名前を入力して、リスト内のグループを一意に識別します。
7. **OK**をクリックします。

ACグループの変更

この関数を使用すると、ACグループの名前を変更できます。

ACグループの名前を変更するには、次の手順を実行します:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Configuration Management**を選択します。
   Configuration Managementページが開きます。
3. **Comware-Based**タブをクリックします。
4. **Network Management**領域で、**AC Group**をクリックします。
   AC Group ListページにすべてのACグループが表示されます。
5. ACグループの**Modify**アイコンをクリックします。**Modify AC Group**ページが開きます。
6. ACグループの新しい名前を入力して、リスト内のグループを一意に識別します。
7. **OK**をクリックします。

ACグループの削除

この関数は、ACグループにACがあるかどうかにかかわらず、ACグループをWSMから削除します。ACグループを削除すると、ACはグループから削除されますが、WSMからは削除されません。

ACグループを削除するには、次のとおりです。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Configuration Management**を選択します。
   Configuration Managementページが開きます。
3. **Comware-Based**タブをクリックします。
4. **Network Management**領域で、**AC Group**をクリックします。
   AC Group ListにすべてのACグループが表示されます。
5. ACグループの**Delete**アイコンをクリックします。
   確認ダイアログボックスが開きます。
6. **OK**をクリックします。

デフォルトのAC同期動作の設定

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Configuration Management**を選択します。
   Configuration Managementページが開きます。
3. **Comware-Based**タブをクリックします。
4. **Network Management**領域で、**AC Group**をクリックします。AC Group Listにすべてのグループが表示されます。
5. デフォルトでAC構成を同期するには、次のいずれかを選択します。
   - **Yes**: ACの設定が変更されると、デフォルトでプライマリ/セカンダリAC間で設定が同期されます。
   - **No**: ACの設定が変更された場合、デフォルトではプライマリACとセカンダリACの間で設定が同期されません。
6. **OK**をクリックします。

ACグループへのACの追加

同じACを別のACグループに追加できます。

ACをACグループに追加するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Configuration Management**を選択します。
   Configuration Managementページが開きます。
3. **Comware-Based**タブをクリックします。
4. **Network Management**領域で、**AC Group**をクリックします。**AC Group List**にすべてのACグループが表示されます。
5. ターゲットACグループの名前をクリックします。
   AC Listページが開きます。
6. **Add AC**をクリックします。
   デバイスの選択ページが開きます。
7. 次の問合せ基準を1つ以上指定します。
   - **Device Label**: ACのデバイスラベルを入力します。WSMは、このフィールドのファジーマッチングをサポートします。

- **IP Address**: ACのIPv4アドレスの一部または全体を入力します。WSMは、このフィールドのファジーマッチングをサポートします。
- **Model**: ACモデルを選択します。オプションは**Unlimited**で、すべてのACモデルをWSMで使用できます。

空のフィールドや無制限に設定されたフィールドは、クエリーの抽出条件にはなりません。

8. **Query**をクリックします。

   AC Listには、クエリー基準に一致するすべてのACが表示されます。
9. ACグループに追加するACを選択します。
10. **OK**をクリックします。

    選択したACがグループに追加されます。

ACグループからのACの削除

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Configuration Management**を選択します。

   Configuration Managementページが開きます。
3. **Comware-Based**タブをクリックします。
4. **Network Management**領域で、**AC Group**をクリックします。**AC Group List**ページが開きます。
5. ACグループの名前をクリックすると、詳細が表示されます。AC Listページが開きます。
6. グループから削除するACを選択します。
7. **Remove AC**をクリックします。

   確認ダイアログボックスが表示されます。
8. **OK**をクリックします。

ポリシーテンプレートの管理

ACは、管理対象のFIT APに無線ポリシーとサービスポリシーを発行します。適切なポリシーテンプレートをACに適用すると、各ポリシーで同じパラメーターを繰り返し設定する必要がないため、手順が簡素化されます。Template Managementページでは、次のタイプのポリシーテンプレートを管理できます。

- Radio policy templates
- Service policy templates

無線ポリシーテンプレートの管理

適切な無線ポリシーテンプレートをACに適用すると、ポリシー名を変更するだけで済むため、無線ポリシーの設定手順が簡素化されます。

無線ポリシーテンプレートリストの表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Configuration Management**を選択します。

   Configuration Managementページが開きます。
3. **Comware-Based**タブをクリックします。
4. **Network Management**領域で、**Template Management**をクリックします。

   Template Managementページが開きます。デフォルトでは、**Radio Policy Template List**

が表示され、すべての無線ポリシーテンプレートが表示されます。

Radio Policy Template List

- **Policy Name**: 無線ポリシーテンプレートの名前。
- **Beacon Interval**: FIT APがビーコンフレームを送信する間隔。
- **DTIM Interval**: バッファリングされたマルチキャストフレームおよびブロードキャストフレームを送信する前にAPが待機するビーコン間隔の数。
- **RTS Threshold**: RTS方式が使用されるフレームの長さ。
- **Fragment Threshold**: フラグメンテーションなしで送信できるフレームの最大長。
- **Rx Lifecycle**: APが受信したフレームをバッファメモリーに保持する間隔。
- **Modify**: ターゲット無線ポリシーテンプレートの**Modify**アイコンをクリックして、そのパラメーターを変更します。詳細については、「無線ポリシーテンプレートの変更」を参照してください。
- **Delete**: ターゲット無線ポリシーテンプレートの**Delete**アイコンをクリックして、テンプレートを削除します。詳細については、「無線ポリシーテンプレートの削除」を参照してください。

無線ポリシーテンプレートの詳細の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Configuration Management**を選択します。

   Configuration Managementページが開きます。
3. **Comware-Based**タブをクリックします。
4. **Network Management**領域で、**Template Management**をクリックします。

   Template Managementページが開きます。デフォルトでは、**Radio Policy Template List**が表示され、すべての無線ポリシーテンプレートが表示されます。
5. ターゲットの無線ポリシーテンプレートの名前をクリックします。

   Radio Policy Template Detailsダイアログボックスが開きます。

   Radio Policy Template Details

   - **Policy Name**: 無線ポリシーテンプレートの名前。
   - **Beacon Interval**: FIT APがビーコンフレームを送信する間隔。
   - **DTIM Interval**: バッファされたマルチキャストフレームおよびブロードキャストフレームを送信する前に、FIT APが待機するビーコン間隔の数。
   - **RTS Threshold(bytes)**: RTS方式が使用されるフレームの長さ。
   - **Fragment Threshold(bytes)**: フラグメンテーションなしで送信できるフレームの最大長。
   - **Short Frame Retransmission Threshold**: RTSしきい値を超えないフレームの最大再送信回数。
   - **Long Frame Retransmission Threshold**: RTSしきい値よりも長いフレームの最大再送信回数。
   - **Rx Lifecycle(ms)**: APが受信したフレームをバッファメモリーに保持する間隔。
   - Max Clients: 無線ポリシーで許可されるクライアントの最大数。
6. **Close**をクリックします。

無線ポリシーテンプレートの追加

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Configuration Management**を選択します。

   Configuration Managementページが開きます。
3. **Comware-Based**タブをクリックします。

4. **Network Management**領域で、**Template Management**をクリックします。

   Template Managementページが開きます。デフォルトでは、**Radio Policy Template List**が表示され、すべての無線ポリシーテンプレートが表示されます。

5. **Add**をクリックします。

   Add Radio Policy Templateページが開きます。

6. 次のパラメーターを設定します。
   - **Policy Name**: 無線ポリシーテンプレートの名前を入力します。ポリシー名は15文字以内で、既存の無線ポリシー名と同じにはできません。英数字とアンダースコア(_)のみ使用できます。
   - **Beacon Interval(TU)**: FIT APがビーコンフレームを送信する間隔を入力します。間隔の値の範囲は32～8191(TU単位)で、デフォルト値は100です(1 TUは1024マイクロ秒に相当します)。
   - **DTIM Interval**: バッファされたマルチキャストフレームおよびブロードキャストフレームを送信する前に、FIT APが待機するビーコン間隔の数を入力します。DTIM Intervalの値の範囲は1～31で、デフォルト値は1で、1は100 TUに相当します。DTIM Intervalが0までカウントダウンされると、FIT APはバッファされたマルチキャストフレームおよびブロードキャストフレームを無線クライアントに送信します。
   - **RTS Threshold(bytes)**: RTS方式を使用するフレームの長さを入力します。値の範囲は0～2346で、デフォルト値は2346です。WLANでデータ送信の衝突を効果的に回避するには、rational値を設定します。小さい値を設定すると、RTSパケットが頻繁に送信され、使用可能な帯域幅をより多く消費しますが、システムは干渉または衝突から迅速に回復できます。
   - **Fragment Threshold(bytes)**: フラグメンテーションなしで送信できるフレームの最大長を入力します。値は256～2346の範囲の偶数で、デフォルト値は2346です。**Fragment Threshold**よりも長いフレームはフラグメント単位で送信されます。
   - **Short Frame Retransmission Threshold**: RTSしきい値を超えないフレームの最大再送信回数を入力します。値の範囲は1～15で、デフォルト値は7です。
   - **Long Frame Retransmission Threshold**: RTSしきい値よりも長いフレームの最大再送信回数を入力します。値の範囲は1～15で、デフォルト値は4です。
   - **Rx Lifecycle(ms)**: APが受信したフレームをバッファメモリーに保持する間隔を入力します。値の範囲は500～250000で、デフォルト値は2000です。
   - **Max Clients**: 無線ポリシーで許可されるクライアントの最大数を入力します。値の範囲は1～124で、デフォルト値は64です。

7. **OK**をクリックします。

無線ポリシーテンプレートの変更

既存の無線ポリシーテンプレートの名前は変更できません。

無線ポリシーテンプレートを変更するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Configuration Management**を選択します。

   Configuration Managementページが開きます。

3. **Comware-Based**タブをクリックします。
4. **Network Management**領域で、**Template Management**をクリックします。

   Template Managementページが開きます。デフォルトでは、Radio Policy Template Listが表示され、すべての無線ポリシーテンプレートが表示されます。

5. 無線ポリシーテンプレートの**Modify**アイコンをクリックします。**Modify Radio Policy Template**ペ

ージが開きます。

6. ポリシー名以外の無線ポリシーパラメーターを変更します。

   パラメーターの詳細については、「無線ポリシーテンプレートの追加」を参照してください。

7. **OK**をクリックします。

無線ポリシーテンプレートの削除

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Configuration Management**を選択します。

   Configuration Managementページが開きます。
3. **Comware-Based**タブをクリックします。
4. **Network Management**領域で、**Template Management**をクリックします。

   Template Managementページが開きます。デフォルトでは、Radio Policy Template List が表示され、すべての無線ポリシーテンプレートが表示されます。
5. 無線ポリシーテンプレートの**Delete**アイコンをクリックします。確認のダイアログボックスが開きます。
6. **OK**をクリックします。

サービスポリシーテンプレートの管理

適切なサービスポリシーテンプレートをACに適用すると、ポリシーIDとインターフェースIDを変更するだけで済むため、サービスポリシーの設定手順が簡素化されます。

サービスポリシーテンプレートリストの表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Configuration Management**を選択します。

   Configuration Managementページが開きます。
3. **Comware-Based**タブをクリックします。
4. **Network Management**領域で、**Template Management**をクリックします。

   Template Managementページが開きます。ポリシーテンプレートには次の2つのタイプがあります。
   - **Radio Policy Template**
   - **Service Policy Template**
5. **Service Policy Template**をクリックします。

   Service Policy Template Listページが開き、すべてのサービスポリシーテンプレートが表示されます。

   Service Policy Template List
   - **SSID**:サービスポリシーテンプレートのSSID。
   - **Encryption Mode**: サービスポリシーテンプレートの暗号化モード。オプションは次のとおりです。
     - **Clear**: クライアントはパスワードなしでワイヤレスネットワークにアクセスできます。
     - **Crypto**: クライアントがワイヤレスネットワークにアクセスするには、正しいパスワードを入力する必要があります。
   - **Hide SSID**: APから送信されるビーコンフレーム内のSSIDを提供するかどうかを示します。このパラメーターを選択すると、クライアントはビーコンフレームからSSIDを取得できないため、ワイヤレスネットワークにアクセスする前にSSIDを設定する必要があります。このパラメーターを選択しないと、クライアントはビーコンフレームからSSIDを取得してワイヤレスネットワークにアクセスできます。

- **Authentication Mode**: サービスポリシーテンプレートの認証モード。オプションは次のとおりです。
  - **Open System**: 認証を要求するすべてのクライアントが直接認証を通過できるようにします。
  - **Shared Key**: クライアントはデバイスに設定されているものと同じ共有キーを使用する必要があります。**Shared Key**は、暗号スイートとして**WEP40**、**WEP104**、または**WEP128**を選択した場合にだけ選択します。
  - **All**: クライアントが必要に応じて**Open System**モードまたは**Shared Key**モードを使用できるようにします。
- **Modify**: ターゲットサービスポリシーテンプレートの**Modify**アイコンをクリックして、そのパラメーターを変更します。詳細は、「サービスポリシーテンプレートの変更」を参照してください。
- **Delete**: ターゲットサービスポリシーテンプレートの**Delete**アイコンをクリックして、テンプレートを削除します。詳細は、「サービスポリシーテンプレートの削除」を参照してください。

サービスポリシーテンプレートの詳細の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Configuration Management**を選択します。

   Configuration Managementページが開きます。
3. **Comware-Based**タブをクリックします。
4. **Network Management**領域で、**Template Management**をクリックします。

   Template Managementページが開きます。ポリシーテンプレートには次の2つのタイプがあります。
   - **Radio Policy Template**
   - **Service Policy Template**
5. **Service Policy Template**をクリックします。

   Service Policy Template Listページが開き、すべてのサービスポリシーテンプレートが表示されます。
6. ターゲットサービスポリシーテンプレートのSSIDをクリックすると、**Basic Information**や**Security Information**などの詳細が表示されます。**Security Information**は、**Encryption Mode**が**Clear**に設定されているサービスポリシーテンプレートでは使用できません。

   Basic Information
   - **SSID**: サービスポリシーテンプレートのSSID。
   - **Encryption Mode**: サービスポリシーテンプレートの暗号化モード。オプションは次のとおりです。
     - **Clear**: クライアントはパスワードなしでワイヤレスネットワークにアクセスできます。
     - **Crypto**: クライアントがワイヤレスネットワークにアクセスするには、正しいパスワードを入力する必要があります。
   - **Hide SSID**: APから送信されるビーコンフレームでSSIDを提供するかどうかを示します。このパラメーターを選択すると、クライアントはビーコンフレームからSSIDを取得できないため、ワイヤレスネットワークにアクセスする前にSSIDを設定する必要があります。このパラメーターを選択しないと、クライアントはビーコンフレームからSSIDを取得してワイヤレスネットワークにアクセスできます。
   - **Authentication Mode**: サービスポリシーテンプレートの認証モード。オプションは次のとおりです。
     - **Open System**: 認証を要求するすべてのクライアントが直接認証を通過できるようにします。

- **Shared Key**: クライアントはデバイスに設定されているものと同じ共有キーを使用する必要があります。**Shared Key**は、暗号スイートとして**WEP40**、**WEP104**、または**WEP128**を選択した場合にだけ選択します。
- **All**: クライアントが必要に応じてオープンシステムモードまたは共有キーモードを使用できるようにします。

- **Max Clients**:サービスポリシーで許可されるクライアントの最大数。
- **Layer2 Isolation**: レイヤ2分離を有効または無効にします。このパラメーターは、ACで実行される**user-isolation vlan**コマンドと組み合わせて設定します。この機能を有効にすると、許可されたMACアドレスリスト内のクライアントは、同じVLAN内の他のクライアントと通信できます。たとえば、ACで**user-isolation vlan 1 permit-mac 0000-1111-222**2コマンドを実行し、レイヤ2分離を有効にすると、クライアント**0000-1111-2222**はVLAN 1内の他のクライアントにアクセスできますが、他のクライアントは相互にアクセスできません。

注:

レイヤ2分離をイネーブルにした後にクライアントがネットワークにアクセスできるようにするには、まずゲートウェイのMACアドレスを許可MACアドレスリストに追加します。

Security Information

- **Security IE**: ビーコンフレームで使用されるセキュリティIEと、FIT APによって送信されるプローブ応答。オプションは、**None** (デフォルト)、**RSN**、**WPA**および**All**です。**None**は、Security IEが構成されていないことを示します。**All**は、RSNとWPAの両方が構成されていることを示します。RSNとWPAの詳細は、関連するデバイスのマニュアルを参照してください。
- **Cipher Suite**: データフレームの暗号化および復号化に使用される暗号スイート。オプションは次のとおりです:
  - **TKIP**
  - **CCMP**
  - **WEP40**
  - **WEP104**
  - **WEP128**
- **Key Index**: クライアントの認証キーインデックス。
- **Key**: クライアントの認証キー。

7. **Close**をクリックします。

サービスポリシーテンプレートの追加

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Configuration Management**を選択します。

   Configuration Managementページが開きます。
3. **Comware-Based**タブをクリックします。
4. **Network Management**領域で、**Template Management**をクリックします。

   Template Managementページが開きます。ポリシーテンプレートには、**Radio Policy Template**と**Service Policy Template**の2種類があります。
5. **Service Policy Template**をクリックします。

   Service Policy Template Listページが開き、すべてのサービスポリシーテンプレートが表示されます。
6. **Add**をクリックします。

   サービスポリシーテンプレートを追加するためのページが開きます。

7. 次のパラメーターを設定します。
   - **SSID**: サービスポリシーテンプレートのSSIDを1～32文字の文字列で入力します。SSID文字列内の有効な文字については、「WLANの追加」を参照してください。
   - **Encryption Mode**: サービスポリシーテンプレートの暗号化モードを選択します。オプションは次のとおりです。
     - **Clear**: **Security Information**領域はサービスポリシーテンプレートでは使用できず、クライアントはパスワードなしでワイヤレスネットワークにアクセスできます。
     - **Crypto**: テンプレートの**Security Information**領域でパラメーターを設定する必要があります。また、クライアントがワイヤレスネットワークにアクセスするには、正しいパスワードを入力する必要があります。
   - **Hide SSID**: このオプションを選択すると、FIT APによって送信されるビーコンフレーム内のSSIDが非表示になります。このパラメーターを選択すると、クライアントはビーコンフレームからSSIDを取得できないため、ワイヤレスネットワークにアクセスする前にSSIDを設定する必要があります。このパラメーターを選択しないと、クライアントはビーコンフレームからSSIDを取得してワイヤレスネットワークにアクセスできます。
   - **Authentication Mode**: サービスポリシーの認証モードをリストから選択します。オプションは次のとおりです。
     - **Open System**: 認証を要求するすべてのクライアントが直接認証を通過できるようにします。
     - **Shared Key**: クライアントはデバイスに設定されているものと同じ共有キーを使用する必要があります。**Shared Key**は、暗号スイートとして**WEP40**、**WEP104**、または**WEP128**を選択した場合にだけ選択します。
     - **All**: クライアントが必要に応じてオープンシステムモードまたは共有キーモードを使用できるようにします。

     暗号化モードが**Clear**の場合、認証モードはOpen Systemのみです。暗号化モードが**Crypto**の場合、認証モードオプションは**Open System**、**Shared Key**、**All**です。
   - **Layer2 Isolation**: レイヤ2分離を有効または無効にします。このパラメーターは、ACで実行される**user-isolation vlan**コマンドと組み合わせて設定します。この機能を有効にすると、許可されたMACアドレスリスト内のクライアントは、同じVLAN内の他のクライアントと通信できます。たとえば、ACで**user-isolation vlan 1 permit-mac 0000-1111-2222**コマンドを実行し、レイヤ2分離を有効にすると、クライアント**0000-1111-2222**はVLAN 1内の他のクライアントにアクセスできますが、他のクライアントは相互にアクセスできません。

     注:

     レイヤ2分離をイネーブルにした後にクライアントがネットワークにアクセスできるようにするには、まずゲートウェイのMACアドレスを許可MACアドレスリストに追加します。

   - Max Clients:サービスポリシーで許可されるクライアントの最大数。
8. **Encryption Mode**として**Crypto**を選択した場合は、必要に応じて次のセキュリティパラメーターを設定します。
   - **Security IE**: ビーコンフレームで使用されるセキュリティIEおよびFIT APによって送信されるプローブ応答を選択します。オプションは次のとおりです。
   - **None**: セキュリティIEは設定されません。
   - **RSN**: 堅牢なセキュリティネットワークとは、WEPやWPAよりも強力な保護を提供するために、堅牢なセキュリティネットワークアソシエーションの作成だけを許可するセキュリティネットワークです。
   - **WPA**: WPAは、WPA-PSK(またはパーソナル)モードまたはWPA-802.1X(またはエンタープライズ)モードのいずれかで動作するWEPよりも優れています。パーソナルモードでは、事前

共有キーまたはパスフレーズが認証に使用されます。エンタープライズモードでは、802.1XおよびRADIUSサーバーとEAPが認証に使用されます。

- **All**: RSNとWPAの両方が設定されています。

  RSNとWPAの詳細については、関連するデバイスのマニュアルを参照してください。

- **Cipher Suite**: データフレームの暗号化および復号化に使用する暗号スイートを選択します。オプションは、**TKIP**、**CCMP**、**WEP40**、**WEP104**、および**WEP128**です。キーインデックスとキーは、**WEP40**、**WEP104**、または**WEP128**を選択した場合にのみ設定できます。**WEP40**、**WEP104**、および**WEP128**を同時に選択することはできません。
  - **WEP**: **WEP40**、**WEP104**、および**WEP128**が含まれます。これらはすべてstatic WEP暗号化メカニズムです。WEP40キーは40ビット、WEP104キーは104ビット、およびWEP128キーは128ビットです。WEPはRC4暗号化を使用し、ワイヤレスネットワークにアクセスするすべてのクライアントが同じキーを使用する必要があります。
  - **TKIP**: Temporal Key Integrity Protocolは、WEPと同様にRC4アルゴリズムを使用しますが、WLANに対してより安全な保護を提供します。TKIPは、802.11iより前のハードウェアのセキュリティを強化します。
  - **CCMP**: Counter mode with CBC-MAC Protocolは、高いセキュリティを提供するためにAESに基づいたCounter-Mode/CBC-MACメカニズムです。
- **Key Index**: クライアントの認証キーインデックスを入力します。
- **Key**: クライアントの認証キーを入力します。WEP40の場合、キーは5文字の英数字の文字列です。WEP104の場合、キーは13文字の英数字の文字列です。WEP128の場合、キーは16文字の英数字の文字列です。

9. **OK**をクリックします。

サービスポリシーテンプレートの変更

この機能では、既存のサービスポリシーテンプレートのSSIDを変更できません。

サービスポリシーテンプレートを変更するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Configuration Management**を選択します。

   Configuration Managementページが開きます。
3. **Comware-Based**タブをクリックします。
4. **Network Managemen**t領域で、**Template Management**をクリックします。

   Template Managementページが開きます。ポリシーテンプレートには次の2つのタイプがあります。
   - **Radio Policy Template**
   - **Service Policy Template**
5. **Service Policy Template**をクリックします。

   Service Policy Template Listページが開き、すべてのサービスポリシーテンプレートが表示されます。
6. サービスポリシーテンプレートの**Modify**アイコンをクリックします。

   Modify Service Policy Templateページが開きます。
7. サービスポリシーテンプレートのパラメーターを変更します。

   これらのパラメーターの詳細については、「サービスポリシーテンプレートの追加」を参照してください。
8. **OK**をクリックします。

サービスポリシーテンプレートの削除

1. **Service**タブをクリックします。

2. ナビゲーションツリーから、**WLAN Manager > Configuration Management**を選択します。
   Configuration Managementページが開きます。
3. **Comware-Based**タブをクリックします。
4. **Network Management**領域で、**Template Management**をクリックします。
   Template Managementページが開きます。ポリシーテンプレートには次の2つのタイプがあります。
   - **Radio Policy Template**
   - **Service Policy Template**
5. **Service Policy Template**をクリックします。
   Service Policy Template Listページが開き、すべてのサービスポリシーテンプレートが表示されます。
6. サービスポリシーテンプレートの**Delete**アイコンをクリックします。確認のダイアログボックスが開きます。
7. **OK**をクリックします。

一般的な管理機能

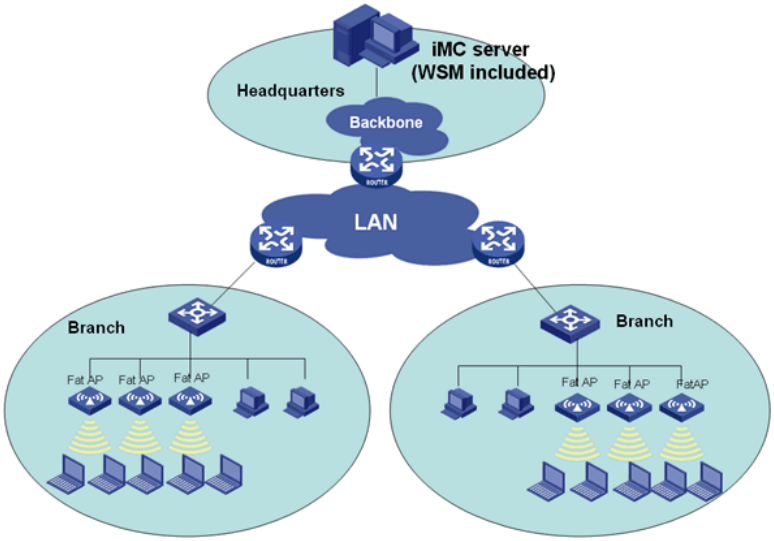
WSMは、Comwareベースのアクセスコントローラに次の一般的な管理機能を提供します。

- **Viewing Topology**
- **ping**
- **traceroute**
- **Open Web Manager**
- **Telnet**
- **SSH**

ComwareベースのFAT APの管理

WSMを使用すると、管理者はFAT APを介してワイヤレスネットワークを作成および管理できます。IMC WSMは、IMCプラットフォームに追加されたすべてのFAT APを自動的に管理します。図65は、FAT APネットワークを示しています。

図65 Fat APネットワーク



WSMで新しいFAT APネットワークを作成する前に、以下のタスクを実行します。

- ネットワークにアクセスできるように、FAT APを設定します。
- FAT APでSNMPコミュニティを設定し、FAT APをIMCプラットフォームに追加します。

WSMでFAT APネットワークを作成するには:

1. FAT AP用のWLAN BSSインターフェースをバッチで作成し、ポートセキュリティモードとバッチ内のWLAN BSSインターフェースのVLAN。

   詳細については、「バッチでのWLAN BSSインターフェースの設定」を参照してください。
2. FAT APのサービスポリシーをバッチで作成します。

   詳細については、「バッチでのサービスポリシーの設定」を参照してください。
3. (任意)FAT APの無線に対して同じパラメーターをバッチで設定します。詳細

   については、「バッチでの無線の設定」を参照してください。
4. 単一のFAT APの無線パラメーターを変更し、無線をサービスポリシーにバインドし、使用する無線論理インターフェースを指定します。

詳細については、「無線ポリシーの設定」を参照してください。

既存のワイヤレスネットワークを管理するには、WSMでFAT APネットワークを作成せずに、WSMでFAT APだけを管理する必要があります。現在のWSMバージョンでは、一部の機能のみがComware 7FAT APで使用できます。

FAT APリストの表示

Fat AP Listページには、IMCで管理されているすべてのFAT APに関する情報が表示されます。この情報には、FAT APのステータス、デバイスラベル、モデル、IPアドレス、オンラインクライアント数、最終同期時刻、同期結果などがあります。

FAT APリストを表示するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Fat APs**を選択します。

   Fat AP ListページにすべてのFat APが表示されます。

   Device List

   - **Status**: FAT APの現在のアラームステータス。
   - **Device Label**: IMCプラットフォームのFAT APを識別するデバイスラベル。FAT APのデバイスラベルをクリックすると、その詳細が表示されます。
   - **Model**: FAT APのモデル。
   - **IP Address**: FAT APの管理IPアドレス。
   - **Clients**: FAT APに関連付けられているクライアントの数。この数をクリックすると、すべてのオンラインクライアントが表示されます。
   - **Last Sync Time**: FAT AP設定が最後に同期された時刻。
   - **Sync Result**: 最後の同期結果(SuccessfulまたはFailed)。
   - Operation: FAT APのOperationアイコン をクリックして、**Operation**メニューを表示します。

Operationメニューに表示される操作タスクには、FAT APのサービスポリシー、ワイヤレス論理インターフェース、MPポリシー、メッシュプロファイル、およびメッシュインターフェースの表示、トポロジーおよびデフォルトマップ上でのFAT APの検索、ping、traceroute、およびTelnet操作の実行、FAT APのWebマネージャーの起動があります。

Fat APリストに十分な数のエントリーがある場合は、次のナビゲーションツールが表示されます。

- **Next Page**アイコンをクリックして、**Fat AP List**の次のページに進みます。
- **Last Page**アイコンをクリックして、**Fat AP List**の最後のページに進みます。
- **Previous Page**アイコンをクリックして、**Fat AP List**の前のページに戻る。
- **First Page**アイコンをクリックして、**Fat AP List**の先頭にページバックします。

Fat AP Listの右上にある**8、15、50、100、**または200をクリックして、各ページに表示する項目数を指定します。

Fat AP Listは、Operationフィールド以外のすべてのフィールドでソートできます。選択したフィールドでリストをソートするには、列ラベルをクリックします。列ラベルは、各フィールドのソートオプションを切り替えるためのトグルスイッチです。

FAT APのクエリー

WSMには、基本問合せと拡張問合せが用意されています。基本問合せ基準には、迅速な検索のためのキーパラメーターがいくつか含まれています。拡張問合せには、正確な照合のための様々な問合せ基準が用意されています。

詳細については、「FAT APのクエリー」を参照してください。

FAT APに関する詳細情報の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Fat APs**を選択します。

   Fat AP Listページにすべてのfat APが表示されます。

3. FAT APのデバイスラベルをクリックします。

   FAT APの詳細ページが開きます。

   この情報は、FAT APに関するワイヤレスサービス情報のみを示します。FAT APの詳細ページに表示されるその他の情報については、『H3C IMC v7.3 Enterprise and Standard Platform Administrator Guide』を参照してください。

4. ワイヤレスサービス情報タブをクリックします。

   FAT APのすべてのワイヤレスサービス情報が表示されます。

   Global Parameter Information

   - **Client Keep Alive Interval(s)**: クライアントのキープアライブインターバル。

     キープアライブメカニズムは、システムから分離されたクライアントを検出するために使用されます。FAT APはプローブ要求をクライアントに送信します。FAT APが応答を受信できない場合は、クライアントとの接続を終了します。

   - **Client Idle-Timeout Interval(s)**: FAT APとクライアント間のリンクがアイドル状態になる最大間隔。

     FAT APがクライアントから送信されたフレームを最大アイドルタイムアウト間隔内に受信しない場合、FAT APはクライアントとの接続を終了します。

   - **Country/Region Code**: US(米国)やJP(日本)など、FAT APが属する国または地域のコード。

   - **Work Mode**: FAT APの動作モード。オプションはNormal、Monitor、およびHybridです。

     Normalモードで動作するFAT APは、クライアントに対してWLANサービスだけを提供します。

     FAT APはモニターモードで動作し、WLAN内のすべてのデバイスを監視しますが、WLANサービスは提供しません。

     ハイブリッドモードで動作している場合、FAT APはWLAN内のデバイスをスキャンし、ワイヤレスアクセスポイントとして機能します。

     Global Parameter Information領域の右側にあるModifyリンクをクリックして、fat APパラメーター設定ページを表示し、fat APパラメーターを変更します。詳細については、「fat APグローバルパラメーターの設定」を参照してください。

   Client Information

   - **Online Clients**: FAT APに関連付けられているクライアントの数。この数をクリックすると、すべてのオンラインクライアントが表示されます。
   - **Associated Clients**: クライアントとFAT AP間で成功したアソシエーションの数。
   - **Associated Failures**: クライアントとFAT AP間で失敗したアソシエーションの数。
   - **Re-associated Clients**: クライアントとFAT AP間の再アソシエーションの数。
   - **Denied Registered Clients**: クライアントとFAT AP間で拒否されたアソシエーションの数。
   - **Exceptional Deauthenticated Clients**: クライアントとFAT AP間の例外的なアソシエーション解除の数。

   Radio Information

   - **ID**: 無線のID。
   - **Interface**: 無線をFAT APに接続する無線インターフェース。
   - **Radio** Type: 無線のタイプ。この値は、FAT APモデルによって異なります。
   - **Channel**: 無線の現用チャネル。値の範囲は無線タイプによって異なります。

     Autoを選択すると、FAT APはチャネル品質を評価し、最適なチャネルを現用チャネルとして選択します。

   - **Current Transmission Power(dBm)**: 無線の現在の送信電力(dBm)。

- **Operation:** Modify and Configure Mesh Peer MAC Addressオプションを提供します。

オペレーターはModifyアイコンをクリックして無線パラメーターを変更したり、Configure Mesh Peer MAC AddressアイコンをクリックしてのネイバーMACアドレスを設定したりできます。

fat AP。詳細については、「無線ポリシーの設定」および「fat APのメッシュピアMACアドレスの設定」を参照してください。

バッチでのWLAN BSSインターフェースの設定

FAT APのWLAN BSSインターフェースは、サービスポリシーにバインドされます。WSMを使用すると、オペレーターはWLAN BSSインターフェースをバッチで作成および削除したり、複数のFAT APのポートセキュリティモードおよびVLANをバッチで変更したりできます。

バッチでのWLAN BSSインターフェースの作成

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Configuration Management**を選択します。

   Configuration Managementページが開きます。
3. Comware-Basedタブをクリックします。
4. Fat AP Batch Configuration Management(H3C)領域で、BSS Interface Batch Configurationをクリックします。

   BSS Interface Batch Configurationページが開きます。
5. Add Interface領域のInterface IDボックスに、インターフェースIDまたはID範囲を入力します。

   ID範囲はハイフン(-)で区切る必要があります(例:5-12)。
6. Fat AP List領域で、Addをクリックします。

   Select Devicesダイアログボックスが開きます。
7. 次の1つ以上のクエリー基準を入力または指定して、設定するFAT APを検索します。
   - **Device Label**: FAT APのラベルを入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
   - **IP Address**: FAT APの部分的または完全なIPv4アドレスを入力します。WSMは、このフィールドのファジーマッチングをサポートしています。
   - **Model**: FAT APのモデルを入力します。WSMは、このフィールドのファジーマッチングをサポートします。
   - **Connectivity Status** :FAT APの接続状態を選択します。オプションは次のとおりです。
     - **Unlimited**
     - **Reachable**
     - **Unreachable**
   - **Location**: FAT APが属するロケーションビューの名前を入力または指定します。WSMは、このフィールドのファジーマッチングをサポートします。

     空のフィールドや無制限に設定されたフィールドは、クエリーの抽出条件にはなりません。
8. **Query**をクリックします。

   Fat AP Listには、クエリー基準に一致するすべてのFAT APが表示されます。クエリー基準をクリアしてすべてのFAT APを表示するには、Resetをクリックします。
9. 目的のFAT APを選択します。

10. **OK**をクリックしてSelect Deviceウィンドウを閉じます。

    Fat AP Listに、選択したすべてのFat APが表示されます。

11. OKをクリックします。

    Result Listページが開き、WLAN BSSインターフェースをバッチで作成した場合の操作結果が表示されます。

12. バッチでWLAN BSSインターフェースを作成するページに戻るには、Backをクリックします。

バッチでのWLAN BSSインターフェースのポートセキュリティモードの変更

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Configuration Management**を選択します。

   Configuration Managementページが開きます。

3. Comware-Basedタブをクリックします。
4. Fat AP Batch Configuration Management(H3C)領域で、BSS Interface Batch Configurationをクリックします。

   BSS Interface Batch Configurationページが開きます。

5. Modify Port Security in Batchesをクリックします。
6. Modify Port Security領域で、次のパラメーターを設定します。
   - **Interface ID**: 変更するWLAN BSSインターフェースのインターフェースIDまたはインターフェースID範囲を入力します。ID範囲はハイフン(-)で区切ります(例:5-12)。
   - **Port Security Mode**: 無線論理インターフェースのポートセキュリティモードを選択します。オプションは次のとおりです。
     - **noRestrictions**
     - **mac-and-psk**
     - **mac-authentication**
     - **mac-else-userlogin-secure**
     - **mac-else-userlogin-secure-ext**
     - **psk**
     - **userlogin-secure**
     - **userlogin-secure-ext**
     - **userlogin-secure-or-mac**
     - **userlogin-secure-or-mac-ext**
     - **userlogin-secure-ext-or-psk**
     - **userlogin-with OUI**

     サービスポリシーの暗号化モードがClearであるか、セキュリティIEが**None**である場合、ポートセキュリティモードの無線論理インターフェースは、**mac-and-psk**、**psk**、**userlogin-secure-ext-or-psk**にできません。

     サービスポリシーの暗号化モードがCryptoで、セキュリティIEがRSNまたはWPAの場合、ポートセキュリティモードのワイヤレス論理インターフェースは**mac-and-psk**、**psk**、**userlogin-secure-ext-or-psk**、または**userlogin-secure-ext**のいずれかになり、キーネゴシエーションタイプは**11Key**になります。ポートセキュリティモードの情報については、表16を参照してください。

表16 ポートセキュリティモード

ポートセキュリティモード	キーパラメーター
noRestrictions	なし
mac-and-psk	• **Key negotiation type**: オプションは、**None**と**11Key**です。 • **PSK type**: オプションは**None**、**Pass-Phrase**、および**Raw-Key**です。 • **PSK**: PSK値を入力します。PSKタイプに**None**を選択した場合は、このフィールドは不要です。
mac-authentication	なし
mac-else-userlogin-secure	なし
mac-else-userlogin-secureext	なし
psk	• **Key negotiation type**: オプションは、**None**と**11Key**です。 • **PSK type**: オプションは**None**、**Pass-Phrase**、および**Raw-Key**です。 • **PSK:** PSK値を入力します。PSKタイプに**None**を選択した場合は、このフィールドは不要です。
userlogin-secure	なし
userlogin-secure-ext	• **Key negotiation type**: オプションは、**None**と**11Key**です
userlogin-secure-or-mac	なし
userlogin-secure-or-macext	なし
userlogin-secure-ext-or-psk	• **Key negotiation type**: オプションは、**None**と**11Key**です。 • **PSK type**: オプションは**None**、**Pass-Phrase**、および**Raw-Key**です。 • **PSK**: PSK値を入力します。PSKタイプに**None**を選択した場合は、このフィールドは不要です。
userlogin-with OUI	なし

7. Fat AP List領域で、Addをクリックします。Select Deviceダイアログボックスが開きます。

8. 設定するFAT APを検索するために、次の設定するFAT APを検索します。

- **Device Label**: FAT APのラベルを入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
- **IP Address**: FAT APの部分的または完全なIPv4アドレスを入力します。WSMは、このフィールドのファジーマッチングをサポートしています。
- **Model**: FAT APのモデルを入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
- **Connectivity Status**: FAT APの接続状態を指定します。オプションは次のとおりです。
  - **Unlimited**
  - **Reachable**

- **Unreachable**

- **Location**: FAT APが属するロケーションビューの名前を入力または指定します。WSMは、このフィールドのファジーマッチングをサポートします。

  空のフィールドや無制限に設定されたフィールドは、クエリーの抽出条件にはなりません。

9. **Query**をクリックします。

   Fat AP Listには、クエリー基準に一致するすべてのFAT APが表示されます。クエリー基準をクリアしてすべてのFAT APを表示するには、Resetをクリックします。

10. ターゲットのFAT APを指定します。
11. OKをクリックしてSelect Deviceウィンドウを閉じます。Fat AP Listに、選択したすべてのFat APが表示されます。
12. OKをクリックします。

    Result Listページが開き、選択したWLAN BSSインターフェースのポートセキュリティモードを変更するための操作結果と、FAT AP同期化の結果が表示されます。

13. WLAN BSSインターフェースのポートセキュリティモードをバッチで変更するページに戻るには、Backをクリックします。

バッチでのWLAN BSSインターフェースの削除

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Configuration Management**を選択します。

   Configuration Managementページが開きます。

3. Comware-Basedタブをクリックします。
4. Fat AP Batch Configuration Management(H3C)領域で、BSS Interface Batch Configurationをクリックします。

   BSS Interface Batch Configurationページが開きます。

5. Delete BSS Interfaces in Batchesをクリックします。
6. Delete Interface領域のInterface IDボックスに、インターフェースIDまたはID範囲を入力します。

   ID範囲はハイフン(-)で区切る必要があります(例:5-12)。

7. Fat AP List領域で、Addをクリックします。

   Select Deviceダイアログボックスが開きます。

8. 設定するFAT APを検索するために、次の設定するFAT APを検索します。
   - **Device Label**: FAT APのラベルを入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
   - **IP Address** :FAT APの部分的または完全なIPv4アドレスを入力します。WSMは、このフィールドのファジーマッチングをサポートしています。
   - **Model**: FAT APのモデルを入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
   - **Connectivity Status**: FAT APの接続状態を指定します。オプションは次のとおりです。
     - **Unlimited**
     - **Reachable**
     - **Unreachable**
   - **Location**: FAT APが属するロケーションビューの名前を入力または指定します。WSMは、このフィールドのファジーマッチングをサポートします。

   空のフィールドや無制限に設定されたフィールドは、クエリーの抽出条件にはなりません。

9. **Query**をクリックします。

   Fat AP Listには、クエリー基準に一致するすべてのFAT APが表示されます。クエリー基準をクリアしてすべてのFAT APを表示するには、Resetをクリックします。

10. ターゲットのFAT APを指定します。
11. OKをクリックしてSelect Deviceウィンドウを閉じます。Fat AP Listに、選択したすべてのFat APが表示されます。
12. OKをクリックします。

    Result Listページが開き、各FAT APのWLAN BSSインターフェースを削除する操作の結果が表示されます。

13. バッチでWLAN BSSインターフェースを削除するページに戻るには、Backをクリックします。

バッチでのWLAN BSSインターフェースが所属するVLANの変更

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Configuration Management**を選択します。
3. Fat AP Batch Configuration Management(H3C)領域で、BSS Interface Batch Configurationをクリックします。

   BSS Interface Batch Configurationページが開きます。

4. Modify VLANs in Batchesをクリックします。
5. Modify VLAN領域で、次のパラメーターを設定します。
   - **Interface ID**: インターフェースIDまたはインターフェースID範囲を入力します。ID範囲はハイフン(-)で区切ります(例:5-12)。
   - **VLAN**: VLAN IDを入力します。

     VLAN変更操作を成功させるには、IDが選択したFAT AP上の既存のIDであることを確認します。

6. Fat AP List領域で、Addをクリックします。Select Deviceダイアログボックスが開きます。
7. 設定するFAT APを検索するために、次の設定するFAT APを検索します。
   - **Device Label**: FAT APのラベルを入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
   - **IP Address**: FAT APの部分的または完全なIPv4アドレスを入力します。WSMは、このフィールドのファジーマッチングをサポートしています。
   - **Model**: FAT APのモデルを入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
   - **Connectivity Status**: FAT APの接続状態を指定します。オプションは次のとおりです。
     - **Unlimited**
     - **Reachable**
     - **Unreachable**
   - **Location**: FAT APが属するロケーションビューの名前を入力または指定します。WSMは、このフィールドのファジーマッチングをサポートします。

   空のフィールドや無制限に設定されたフィールドは、クエリーの抽出条件にはなりません。

8. **Query**.をクリックします。

Fat AP Listには、クエリー基準に一致するすべてのFAT APが表示されます。クエリー基準をクリアしてすべてのFAT APを表示するには、Resetをクリックします。

9. ターゲットのFAT APを指定します。
10. OKをクリックしてSelect Deviceウィンドウを閉じます。Fat AP Listに、選択したすべてのFat APが表示されます。
11. OKをクリックします。

    Result Listページが開き、FAT APのVLANをバッチで変更した場合の操作結果が表示されます。
12. Backをクリックするページに戻るには、Backをクリックします。

バッチでのサービスポリシーの設定

サービスポリシーは、ポリシーがFAT APの無線にバインドされている場合に、FAT APがWLANアクセスサービスを提供できるようにするWLANアクセスパラメーターのコレクションです。異なる無線は同じサービスポリシーを使用でき、各無線は複数のサービスポリシーにバインドできます。

ワイヤレスサービスを提供するために、異なるFAT APに対して同じサービスポリシーを設定できます。サービスポリシーの設定を容易にするために、WSMを使用すると、オペレーターはFAT APのサービスポリシーをバッチで作成、変更、および削除できます。

バッチでのサービスポリシーの作成

オペレーターは、サービスポリシーをバッチで作成したり、既存のサービスポリシーテンプレートからサービスポリシーを選択したりできます。サービスポリシーテンプレートの管理の詳細については、「ポリシーテンプレートの管理」を参照してください。

サービスポリシーをバッチで作成するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Configuration Management**を選択します。

   Configuration Managementページが開きます。
3. Comware-Basedタブをクリックします。
4. Fat AP Batch Configuration Management(H3C)領域で、Service Policies Batch Configurationをクリックします。

   Service Policies Batch Configurationページが開きます。
5. 必要に応じて次のパラメーターを設定するか、既存のサービスポリシーテンプレートからサービスポリシーを指定します。

   サービスポリシーをバッチで作成するには、次の基本パラメーターとセキュリティパラメーターを設定します。

   Basic Information

   - **Policy ID**: FAT APでサービスポリシーを一意に識別するためのサービスポリシーのIDを入力します。
   - **Enable**: サービスポリシーがFAT APに適用されたときにすぐにイネーブルにする場合にだけ、このオプションを指定します。
   - **SSID**: サービスポリシーのSSIDを入力します。
   - **Encryption Mode**: サービスポリシーの暗号化モードを指定します。オプションは次のとおりです。
     - **Clear Mode**: データパケットを暗号化する必要はありません。
     - **Crypto Mode**: すべてのデータパケットを暗号化する必要があります。
   - **Hide SSID**: FAT APによって送信されるビーコンフレーム内のSSIDを非表示にするには、このオプションを指定します。このパラメーターを指定すると、クライアントはビーコンフレームか

らSSIDを取得できません。このパラメーターを指定しないと、クライアントはビーコンフレームからSSIDを取得できます。

- **Encryption Mode**: サービスポリシーの認証モードを指定します。オプションは次のとおりです。
  - **Open System**: 認証を要求するすべてのクライアントが直接認証を通過できるようにします。
  - **Shared Key**: クライアントはデバイスに設定されているものと同じ共有キーを使用する必要があります。Shared Keyは、暗号スイートとしてWEP40、WEP104、またはWEP128を選択した場合にだけ指定します。
  - **All**: クライアントが必要に応じてオープンシステムモードまたは共有キーモードを使用できるようにします。

  暗号化モードがClearの場合、認証モードはOpen Systemのみです。暗号化モードがCryptoの場合、認証モードオプションはOpen System、Shared Key、Allです。
- **Max Clients**: サービスポリシーを使用できるクライアントの最大数を入力します。

Security Information

Encryption ModeとしてCryptoを選択した場合は、必要に応じて次のセキュリティパラメーターを設定します。

- **Security IE**: FAT APによって送信されるビーコンフレームおよびプローブ応答で使用されるセキュリティIEを指定します。オプションは、None、RSN、WPA、およびAllです。
  - **None**: セキュリティIEが設定されていないことを示します。
  - **All**: RSNとWPAの両方が設定されていることを示します。
  - **RSN**: 堅牢なセキュリティネットワークは、WPAよりも強力な保護を提供するために、堅牢なセキュリティネットワークアソシエーションの作成だけを可能にするセキュリティネットワークです。
  - **WPA**: WPAは、WPA-PSK(パーソナル)モードまたはWPA-802.1X(エンタープライズ)モードで動作します。パーソナルモードでは、事前共有キーまたはパスフレーズが認証に使用されます。エンタープライズモードでは、802.1XおよびRADIUSサーバーとEAPが認証に使用されます。

    RSNとWPAの詳細については、関連するデバイスのマニュアルを参照してください。
- **Cipher Suite**: データフレームの暗号化および復号化に使用される暗号スイートを指定します。オプションは次のとおりです。
  - **WEP**: 静的WEP暗号化メカニズム。WEP40キーは40ビット、WEP104キーは104ビット、WEP128キーは128ビットです。WEPはRC4暗号化を使用し、ワイヤレスネットワークにアクセスするすべてのクライアントが同じキーを使用する必要があります。キーインデックスとキーは、WEP40、WEP104、またはWEP128を選択した場合にのみ設定できます。WEP40、WEP104、およびWEP128を同時に選択することはできません。
  - **TKIP**: Temporal Key Integrity Protocolは、WEPと同様にRC4アルゴリズムを使用しますが、WLANに対してより安全な保護を提供します。
  - **CCMP**: Counter mode with CBC-MAC Protocolは、高いセキュリティを提供するためにAESに基づいたCounter-Mode/CBC-MACメカニズムです。
- **Key Index**: クライアントの認証キーインデックスを入力します。
- **Key**: クライアントの認証キーを入力します。WEP40の場合、キーは5文字の英数字の文字列です。WEP104の場合、キーは13文字の英数字の文字列です。WEP128の場合、キーは16文字の英数字の文字列です。

  キーインデックスとキーは、WEP40、WEP104、またはWEP128を選択した場合にのみ設定できます。WEP40、WEP104、およびWEP128を同時に選択することはできません。

既存のサービスポリシーテンプレートからサービスポリシーを選択するには、次の手順を実行します。

a. テンプレートの選択をクリックします。

WSM内のすべてのサービスポリシーテンプレートが表示されます。

Service Policy List

- **SSID**: サービスポリシーのSSID。
- **Encryption Mode**: サービスポリシーの暗号化モード。オプションは次のとおりです。
  - Clear Mode: データパケットを暗号化する必要はありません。
  - Crypto Mode: すべてのデータパケットを暗号化する必要があります。
- **Hide SSID**: FAT APから送信されたビーコンフレームでSSIDを非表示にするかどうか。

  このパラメーターを指定すると、クライアントはビーコンフレームからSSIDを取得できないため、ワイヤレスネットワークにアクセスする前にSSIDを設定する必要があります。

  このパラメーターが指定されていない場合、クライアントはビーコンフレームからSSIDを取得してワイヤレスネットワークにアクセスできます。
- **Authentication Mode**: サービスポリシーの認証モードを指定します。オプションは次のとおりです。
  - **Open System**: 認証を要求するすべてのクライアントが直接認証を通過できるようにします。
  - **Shared Key**: クライアントは、デバイスに設定されているものと同じ共有キーを使用する必要があります。Shared Keyは、暗号スイートとしてWEP40またはWEP104を選択した場合にだけ指定します。
  - **All**: クライアントが必要に応じてオープンシステムモードまたは共有キーモードを使用できるようにします。

    暗号化モードがClearの場合、認証モードはOpen Systemのみです。暗号化モードがCryptoの場合、認証モードオプションはOpen System、Shared Key、Allです。

b. サービスポリシーテンプレートを指定します。

c. OKをクリックします。

d. サービスポリシーをバッチで作成するページの**Add Service Policy**領域で、サービスポリシーのIDを入力して、FAT AP上のサービスポリシーを一意に識別します。

e. **Fat AP List**領域で、Addをクリックします。Select Deviceダイアログボックスが開きます。

f. 設定するFAT APを検索するために、次の設定するFAT APを検索します。

- **Device Label**: FAT APのラベルを入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
- **IP Address**: FAT APの部分的または完全なIPv4アドレスを入力します。WSMは、このフィールドのファジーマッチングをサポートしています。
- **Model**: FAT APのモデルを入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
- **Connectivity Status**: FAT APの接続状態を指定します。オプションは次のとおりです。
  - **Unlimited**
  - **Reachable**
  - **Unreachable**
- **Location**: FAT APが属するロケーションビューの名前を入力または指定します。WSMは、このフィールドのファジーマッチングをサポートします。

  空のフィールドや無制限に設定されたフィールドは、クエリーの抽出条件にはなりません。

g. Queryをクリックします。

Fat AP Listには、クエリー基準に一致するすべてのFAT APが表示されます。クエリー基準を

クリアしてすべてのFAT APを表示するには、Resetをクリックします。

h. ターゲットのFAT APを指定します。

i. OKをクリックしてSelect Deviceウィンドウを閉じます。Fat AP Listに、選択したすべてのFat APが表示されます。

6. OKをクリックします。

Result Listページが開き、サービスポリシーをバッチで作成した場合の操作結果が表示されます。

7. バッチでサービスポリシーを作成するページに戻るには、Backをクリックします。

バッチでのサービスポリシーの変更

1. **Service**タブをクリックします。

2. ナビゲーションツリーから、**WLAN Manager > Configuration Management**を選択します。

Configuration Managementが表示されます。

3. **Comware-Based**タブをクリックします。

4. Fat AP Batch Configuration Management(H3C)領域で、Service Policies Batch Configurationをクリックします。

Service Policies Batch Configurationページが開きます。

5. Modify Service Policies in Batchesをクリックします。

6. 必要に応じて、サービスポリシーパラメーターを変更します。

詳細については、「バッチでのサービスポリシーの作成」を参照してください。

7. Fat AP List領域で、Addをクリックします。Select Deviceダイアログボックスが開きます。

8. 設定するFAT APを検索するために、次の設定するFAT APを検索します。

- **Device Label**: FAT APのラベルを入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
- **IP Address**: FAT APの部分的または完全なIPv4アドレスを入力します。WSMは、このフィールドのファジーマッチングをサポートしています。
- **Model**: FAT APのモデルを入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
- **Connectivity Status**: FAT APの接続状態を指定します。オプションは次のとおりです。
  - Unlimited
  - Reachable
  - Unreachable
- **Location**: FAT APが属するロケーションビューの名前を入力または指定します。WSMは、このフィールドのファジーマッチングをサポートします。

  空のフィールドや無制限に設定されたフィールドは、クエリーの抽出条件にはなりません。

9. **Query**をクリックします。

Fat AP Listには、クエリー基準に一致するすべてのFAT APが表示されます。クエリー基準をクリアしてすべてのFAT APを表示するには、Resetをクリックします。

10. ターゲットのFAT APを指定します。

11. OKをクリックしてSelect Deviceウィンドウを閉じます。Fat AP Listに、選択したすべてのFat APが表示されます。

12. OKをクリックします。

Result Listページが開き、サービスポリシーをバッチで変更した場合の操作結果が表示されます。

13. バッチでサービスポリシーを変更するページに戻るには、Backをクリックします。

バッチでのサービスポリシーの削除

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Configuration Management**を選択します。

   Configuration Managementページが開きます。
3. **Comware-Based**タブをクリックします。
4. Fat AP Batch Configuration Management(H3C)領域で、Service Policies Batch Configurationをクリックします。

   Service Policies Batch Configurationページが開きます。
5. Delete Service Policies in Batchesをクリックします。
6. 削除するサービスポリシーのSSIDを入力します。
7. Fat AP List領域で、Addをクリックします。Select Deviceダイアログボックスが開きます。
8. 設定するFAT APを検索するために、次の設定するFAT APを検索します。
   - **Device Label**: FAT APのラベルを入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
   - **IP Address**: FAT APの部分的または完全なIPv4アドレスを入力します。WSMは、このフィールドのファジーマッチングをサポートしています。
   - **Model**: FAT APのモデルを入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
   - **Connectivity Status**: FAT APの接続状態を指定します。オプションは次のとおりです。
     - Unlimited
     - Reachable
     - Unreachable

     空のフィールドや無制限に設定されたフィールドは、クエリーの抽出条件にはなりません。
9. **Query**をクリックします。

   Fat AP Listには、クエリー基準に一致するすべてのFAT APが表示されます。クエリー基準をクリアしてすべてのFAT APを表示するには、Resetをクリックします。
10. ターゲットのFAT APを指定します。
11. OKをクリックしてSelect Deviceウィンドウを閉じます。Fat AP Listに、選択したすべてのFat APが表示されます。
12. OKをクリックします。

    Result Listページが開き、サービスポリシーをバッチで削除したときの操作結果が表示されます。
13. Backをクリックして、戻るには、Backをクリックします。

バッチでのWLAN BSSインターフェースへのサービスポリシーのバインド

この機能を使用すると、同じSSIDを持つサービスポリシーを、FAT APのWLAN BSSインターフェースにバッチでバインドできます。

サービスポリシーをバッチでバインドするには

1. **Service**タブをクリックします。

2. ナビゲーションツリーから、**WLAN Manager > Configuration Management**を選択します。

   Configuration Managementページが開きます。
3. **Comware-Based**タブをクリックします。
4. **Fat AP Batch Configuration Management(H3C)**領域で、Service Policies Batch Configurationをクリックします。

   Service Policies Batch Configurationページが開きます。
5. Bind Service Policies in Batchesをクリックします。
6. バインドするサービスポリシーのSSIDを入力します。
7. Port Descriptionボックスに、BSSインターフェースIDをWLAN-BSSインターフェースIDの形式で入力します。

   デフォルト値はWLAN-BSS 1です。

   FAT AP上の既存または存在しないWLAN BSSインターフェースIDを入力できます。存在しないインターフェースIDを入力すると、WSMによってBSSインターフェースのインターフェースIDが自動的に作成されます。
   1つのサービスポリシーにバインドできるBSSインターフェースは1つだけです。入力したインターフェースIDがすでに他のサービスポリシーにバインドされている場合、バインド操作は失敗します。
8. Fat AP List領域で、Addをクリックします。

   Select Deviceダイアログボックスが開きます。
9. 設定するFAT APを検索するために、次の設定するFAT APを検索します。
   - **Device Label**: FAT APのラベルを入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
   - **IP Address**: FAT APの部分的または完全なIPv4アドレスを入力します。WSMは、このフィールドのファジーマッチングをサポートしています。
   - **Model**: FAT APのモデルを入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
   - **Connectivity Status**: FAT APの接続状態を指定します。オプションは次のとおりです。
     - **Unlimited**
     - **Reachable**
     - **Unreachable**

     空のフィールドや無制限に設定されたフィールドは、クエリーの抽出条件にはなりません。
10. **Query**をクリックします。

    Fat AP Listには、クエリー基準に一致するすべてのFAT APが表示されます。クエリー基準をクリアしてすべてのFAT APを表示するには、Resetをクリックします。
11. ターゲットのFAT APを指定します。
12. OKをクリックしてSelect Deviceウィンドウを閉じます。Fat AP Listに、選択したすべてのFat APが表示されます。
13. OKをクリックします。

    Result Listページが開き、サービスポリシーをバッチで変更した場合の操作結果が表示されます。
14. バッチでサービスポリシーを変更するページに戻るには、Backをクリックします。

バッチでの無線の設定

無線設定を容易にし、反復動作を削減するために、WSMは、オペレーターが、複数のFAT APの無線に対す

るパブリックパラメーターをバッチで設定することを可能にする。

パブリックパラメーターには次のものがあります。

- Radio type
- Maximum transmit power
- Admin status
- Channel in use
- Operating mode
- Description

無線をバッチで設定するには、次の手順を実行します

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Configuration Management**を選択します。

   Configuration Managementページが開きます。
3. **Comware-Based**タブをクリックします。
4. **Fat AP Batch Configuration Management(H3C)**領域で、**Radio Batch Configuration**をクリックします。

   Radio Batch Configurationページが開きます。
5. 次のパラメーターを設定します。
   - **Beacon Interval(TU)**: APがビーコンフレームを送信する間隔を入力します。
   - **DTIM Interval**: バッファリングされたマルチキャストフレームおよびブロードキャストフレームを送信する前にAPが待機するビーコン間隔の数を入力します。DTIMカウンタが設定値に達すると、APはバッファリングされたブロードキャスト/マルチキャストフレームを送信します。
   - **RTS Threshold(bytes)**: RTS方式が使用されるフレームの長さを入力します。値を小さくすると、RTSパケットの送信頻度が高くなり、使用可能な帯域幅をより多く消費します。ただし、RTSパケットの送信頻度が高くなると、システムは干渉または衝突からより迅速に回復できます。
   - **Fragment Threshold(bytes)**: フラグメンテーションなしで送信できるフレームの最大長を入力します。指定したフラグメントしきい値を超えるフレームは、フラグメント化されます。
   - **Short Frame Retransmission Threshold**: RTSしきい値よりも短いフレームを送信する最大試行回数を入力します。
   - **Long Frame Retransmission Threshold**: RTSしきい値よりも大きいフレームを送信する最大試行回数を入力します。
   - **Rx Lifecycle(ms)**: FAT APが受信したフレームをバッファメモリーに保持する間隔を入力します。
   - **Radio Type**: 無線タイプを指定します。オプションは次のとおりです。

     802.11a

     802.11b

     802.11g

     802.11gn

     802.11an
   - **Channels in Use**: 無線の動作チャネルを指定します。値の範囲は無線タイプによって異なります。Autoを指定すると、FAT APはアイドルチャネルを動作チャネルとして選択します。
   - **Max Transmit Power(dBm)**: 無線の最大送信電力を入力します。
   - **Preamble Type**: 802.11b、802.11g、または802.11gn無線タイプを指定する場合は、FAT APのプリアンブルタイプを指定します。オプションは次のとおりです。

- **Short**: Fat APは、ショートプリアンブルまたはロングプリアンブルのいずれかを使用してフレームを送信します。
- **Long**: Fat APは、長いプリアンブルを持つフレームだけを送信します。

6. Radio List領域で、Addをクリックします。Select Deviceダイアログボックスが開きます。
7. 設定する無線を検索するというクエリー基準を指定して、設定する無線を検索します。
   - **Device Label**: FAT APのラベルを入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
   - **IP Address**: FAT APの部分的または完全なIPv4アドレスを入力します。WSMは、このフィールドのファジーマッチングをサポートしています。
   - **Model**: FAT APのモデルを入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
   - **Radio Type**: 無線タイプを指定します。オプションは次のとおりです。
     - **802.11a**
     - **802.11b**
     - **802.11g**
     - **802.11gn**
     - **802.11an**
   - **Location**: FAT APが属するロケーションビューの名前を入力または指定します。WSMは、このフィールドのファジーマッチングをサポートします。

     空のフィールドや無制限に設定されたフィールドは、クエリーの抽出条件にはなりません。
8. Queryをクリックします。

Radio Listには、クエリー基準に一致するすべての無線が表示されます。Resetをクリックすると、クエリー基準がクリアされ、すべての無線が表示されます。

注:

設定エラーを回避するためのベストプラクティスとして、同じモデルのFAT AP上で無線をバッチで設定します。

9. 設定する無線を指定します。
10. OKをクリックして、Select Deviceウィンドウを閉じます。Radio Listに、選択したすべての無線が表示されます。
11. OKをクリックします。

    Result Listページが開き、各無線の設定結果が表示されます。
12. Backをクリックして、無線バッチ設定ページに戻ります。

FAT APの無線パラメーターの変更

この機能を使用すると、FAT APの無線パラメーターを変更し、無線をサービスポリシーにバインドおよびアンバインドできます。サービスポリシーを無線にバインドする場合は、無線論理インターフェースを指定して、クライアントの認証方式とVLANを決定する必要があります。

FAT APの無線パラメーターを変更するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management>Fat APs**を選択します。

   Fat AP Listページにすべてのfat APが表示されます。

3. FAT APのデバイスラベルをクリックします。
4. **Wireless Service Information**タブの**Radio Information**領域で、Modifyアイコンをクリックします。
5. 次のパラメーターを設定します。
   - **Radio ID**: このフィールドは変更できません。
   - **Beacon Interval(TU)**: FAT APがビーコンフレームを送信する間隔を入力します。
   - **DTIM Interval**: バッファされたマルチキャストフレームおよびブロードキャストフレームを送信する前にAPが待機するビーコン間隔の数を入力します。

     値の範囲は1～31です。デフォルト値は1(102,400マイクロ秒)です。DTIMカウンタが設定値に達すると、APはバッファされたブロードキャスト/マルチキャストフレームを送信します。
   - **RTS Threshold(bytes)**: RTS方式を使用するフレームの長さを入力します。

     WLANでのデータ送信の衝突を効果的に回避するために、合理的な値を設定します。値を小さく設定すると、RTSパケットが頻繁に送信され、使用可能な帯域幅をより多く消費します。ただし、システムは干渉や衝突から迅速に回復できます。
   - **Fragment Threshold(bytes)**: フラグメンテーションなしで送信できるフレームの最大長を入力します。指定したフラグメントしきい値を超えるフレームは、フラグメント化されます。
   - **Short Frame Retransmission Threshold**: RTSしきい値よりも短いフレームを送信する最大試行回数を入力します。
   - **Long Frame Retransmission Threshold**: RTSしきい値よりも大きいフレームを送信する最大試行回数を入力します。
   - **Rx Lifecycle(ms)**: FAT APが受信したフレームをバッファメモリーに保持する間隔を入力します。
   - **Radio Type**: 無線タイプを指定します。オプションは次のとおりです。

     802.11a

     802.11b

     802.11g

     802.11gn

     802.11an

     802.11gnまたは802.11 anを指定する場合は、次のパラメーターを設定します。
     - **Enable A-MPDU**
     - **Enable A-MSDU**
     - **Client 802.11n Only**
     - **Short GI**

     無線が有効なメッシュプロファイルにバインドされている場合、無線のタイプは変更できません。
   - 使用中のチャネル無線の動作チャネルを指定します。

     このフィールドにAutoと表示されている場合、FAT APはアイドルチャネルを現用チャネルとして選択します。

     注:

     メッシュプロファイルとサービスポリシーの両方を無線にバインドする場合は、チャネルモードをAutoに設定できません。
   - **Max Transmission Power(dBm)**: 無線の最大送信電力をdBm単位で入力します。
   - **Current Transmission Power(dBm)**: 無線の現在の送信電力(dBm)。
   - **MP Policy**: 無線にバインドされたMPポリシー(WSM内の既存のMPポリシーを含む)を

指定します。

- **Mesh Profile ID**: 無線にバインドされたメッシュプロファイルIDを指定します。

注:

モニターモードまたはハイブリッドモードでは、FAT APのメッシュプロファイルを指定できません。

6. 次のいずれかの手順を実行します。
   - 選択したサービスポリシーをオンにして、サービスポリシーを無線にバインド解除します。
   - サービスポリシーを指定し、リストから無線論理インターフェースを指定して、サービスポリシーを無線にバインドします。

   Service Policy List
   - **SSID**: サービスポリシーのSSID。
   - **Encryption Mode**: サービスポリシーの暗号化モード。オプションは次のとおりです。
     - **Clear Mode**: データパケットを暗号化する必要はありません。
     - **Crypto Mode**: すべてのデータパケットを暗号化する必要があります。
   - **Hide SSID**: FAT APから送信されたビーコンフレームでSSIDを非表示にするかどうか。
   - **Authentication Mode**: サービスポリシーの認証モードを指定します。オプションは次のとおりです。
     - **Open System**: 認証を要求するすべてのクライアントが直接認証を通過できるようにします。
     - **Shared Key**: クライアントは、デバイスに設定されているものと同じ共有キーを使用する必要があります。Shared Keyは、暗号スイートとしてWEP40またはWEP104を選択した場合にだけ指定します。
     - **All**: クライアントが必要に応じてオープンシステムモードまたは共有キーモードを使用できるようにします。

     暗号化モードがClearの場合、認証モードはOpen Systemのみです。暗号化モードがCryptoの場合、認証モードオプションはOpen System、Shared Key、Allです。
   - **Interface**:サービスポリシーのバインディングインターフェース。サービスポリシーを指定すると、Interfaceリストからバインディングインターフェースを選択できます。オプションはすべて、現在の無線が属するFAT APの無線論理インターフェースです。

     FAT APの1つのワイヤレス論理インターフェースは、1つのサービスポリシーに1つの無線だけをバインドできます。選択したワイヤレス論理インターフェースが使用中でないことを確認してください。
   - **Modify**: 現在の無線にバインドされているサービスポリシーを変更するには、**Modify**アイコン  をクリックします。詳細については、「サービスポリシーの変更」を参照してください。
7. OKをクリックします。

サービスポリシーの設定

サービスポリシーは、ポリシーがFAT APの無線にバインドされている場合に、FAT APがWLANアクセスサービスを提供できるようにするWLANアクセスパラメーターのコレクションです。異なる無線は同じサービスポリシーを使用でき、各無線は複数のサービスポリシーにバインドできます。

サービスポリシーの作成を容易にするために、WSMにはサービスポリシーテンプレート管理機能が用意されています。詳細は、「サービスポリシーテンプレートの管理」を参照してください。
Service Policy Configuration機能には、**Fat AP List**ページ、**fat AP details**ページまたは**Configuration Management**ページからアクセスできます。次の情報では、例として**Fat AP List**ページを使用しています。

サービスポリシーリストの表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management>Fat APs**を選択します。Fat AP Listページにすべてのfat APが表示されます。
3. FAT APの**Operation**アイコン ▪▪▪をクリックします。
4. メニューからService Policyを選択します。

   Service Policy Managementページが開きます。このページのリストを使用できます。

   - **Service Policy List**: FAT APのすべてのサービスポリシー情報を表示します。
   - **Radio Information area**: サービスポリシーにバインドされているすべての無線を表示します。

     Service Policy Listでは、サービスポリシーの追加と変更、サービスポリシーテンプレートの選択、Service Policy Listのリフレッシュ、サービスポリシーの削除、サービスポリシーにバインドされた無線の表示、およびサービスポリシーへの無線のバッチバインドを行うことができます。

   Service Policy List

   - **Policy ID**: サービスポリシーのID。
   - **SSID**: サービスポリシーのSSID。
   - **Encryption Mode**: サービスポリシーの暗号化モード。オプションは次のとおりです。
     - Clear Mode: データパケットを暗号化する必要はありません。
     - Crypto Mode: すべてのデータパケットを暗号化する必要があります。
   - **Hide SSID**: FAT APから送信されるビーコンフレーム内でSSIDを非表示にするかどうかを指定します。このパラメーターを選択すると、クライアントはビーコンフレームからSSIDを取得できず、ワイヤレスネットワークにアクセスする前にSSIDを設定する必要があります。このパラメーターを選択しないと、クライアントはビーコンフレームからSSIDを取得してワイヤレスネットワークにアクセスできます。
   - **Enable Status**: サービスポリシーが有効かどうか。オプションは次のとおりです:
     - **Enable**: サービスポリシーがFAT APでイネーブルであり、FAT APがサービスを提供できることを示します。
     - **Disable**: サービスポリシーがFAT APでイネーブルになっておらず、FAT APがサービスを提供できないことを示します。
     - **Not Ready**: サービスポリシーがFAT APに展開されており、FAT APがサービスを提供できないことを示します。
   - **Authentication Mode**: サービスポリシーの認証モード。オプションは次のとおりです。
     - **Open System**: 認証を要求するすべてのクライアントが直接認証を通過できるようにします。
     - **Shared Key**: クライアントは、デバイスに設定されているものと同じ共有キーを使用する必要があります。Shared Keyは、暗号スイートとしてWEP40またはWEP104を選択した場合にだけ指定します。
     - **All**: クライアントが必要に応じてオープンシステムモードまたは共有キーモードを使用できるようにします。

     暗号化モードがClearの場合、認証モードはOpen Systemのみです。暗号化モードがCryptoの場合、認証モードオプションはOpen System、Shared Key、Allです。

   - **Operation**: サービスポリシーのOperationアイコン ▪▪▪ をクリックして、**Operation**メニューを表示します。

     Operationメニューに表示される操作タスクには、指定したサービスポリシーの変更と削除、お

よび指定したサービスポリシーにバインドされた無線に関する情報の表示があります。

Radio Information領域では、無線を追加または削除したり、すべての無線を削除したりできます。

Radio Information

- **Interface**: 無線をFAT APに接続する無線インターフェースの名前。名前のリンクをクリックすると、その詳細およびバインドされたサービスポリシーが表示されます。
- **Radio Type**: 無線のタイプ。オプションは次のとおりです。
  - **802.11a**
  - **802.11b**
  - **802.1g**
  - **802.11gn**
  - **802.11an**
- **Channel**: 無線の現用チャネル。無線のタイプによって異なります。このフィールドにAutoと表示されている場合、FAT APはチャネル品質を評価し、最適なチャネルを現用チャネルとして選択します。
- **Max Transmission Power(dBm)**: 無線の最大送信電力。
- **Modify**: 無線パラメーターを変更するには、**Modify**アイコンをクリックします。詳細については、「FAT APの無線パラメーターの変更」を参照してください。

サービスポリシーの詳細の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Fat APs**を選択します。

   Fat AP Listページにすべての Fat APが表示されます。
3. FAT APの**Operation**アイコン をクリックします。
4. メニューからService Policyを選択します。

   Service Policy Managementページには、Service Policy ListにあるFAT APのすべてのサービスポリシー情報が表示されます。
5. サービスポリシーのIDをクリックすると、その基本情報が表示されます。

   Basic Information
   - **Policy ID**: サービスポリシーのID。
   - **Enable**: サービスポリシーがイネーブルかどうかを示します。イネーブルの場合、サービスポリシーを無線および無線論理インターフェースにバインドして、無線サービスを提供できます。
   - **SSID**: サービスポリシーのSSID。
   - **Encryption Mode**: サービスポリシーの暗号化モード。オプションは次のとおりです。
     - **Clear Mode**: データパケットを暗号化する必要はありません。
     - **Crypto Mode**: すべてのデータパケットを暗号化する必要があります。
   - **Hide SSID**: FAT APから送信されるビーコンフレーム内でSSIDを非表示にするかどうかを指定します。このパラメーターを選択すると、クライアントはビーコンフレームからSSIDを取得できず、ワイヤレスネットワークにアクセスする前にSSIDを設定する必要があります。このパラメーターを選択しないと、クライアントはビーコンフレームからSSIDを取得してワイヤレスネットワークにアクセスできます。
   - **Authentication Mode**: サービスポリシーの認証モード。オプションは次のとおりです。
     - **Open System**: 認証を要求するすべてのクライアントが直接認証を通過できるようにします。

- **Shared Key**: クライアントは、デバイスに設定されているものと同じ共有キーを使用する必要があります。Shared Keyは、暗号スイートとしてWEP40またはWEP104を選択した場合にだけ指定します。
- **All**: クライアントが必要に応じてオープンシステムモードまたは共有キーモードを使用できるようにします。

- **Max Clients**: サービスポリシーを使用できるクライアントの最大数。

Security Information

- **Security IE**: FAT APによって送信されるビーコンフレームおよびプローブ応答で使用されるセキュリティIE。オプションは、None、RSN、WPA、およびAllです。
  - **None**: セキュリティIEは設定されません。
  - **All**: RSNとWPAの両方が設定されています。

    RSNとWPAの詳細については、関連するデバイスのマニュアルを参照してください。
- **Cipher Suite**: データフレームの暗号化および復号化に使用される暗号スイート。オプションは次のとおりです:
  - **TKIP**
  - **CCMP**
  - **WEP40**
  - **WEP104**
- **Key Index**: クライアントの認証キーインデックス。
- **Key**: クライアントの認証キー。

6. **Close**をクリックします。

サービスポリシーの追加

次の方法を使用して、FAT APのサービスポリシーを追加できます。

- 通常の方法サービスポリシー管理でサービスポリシーを追加します。
- Expressメソッドサービスポリシーテンプレートを指定し、そのテンプレートを使用してサービスポリシーを追加します。サービスポリシーテンプレートの詳細は、「サービスポリシーテンプレートの管理」を参照してください。

サービスポリシーを正常に設定するには、サービスポリシーのセキュリティ情報を設定する前に、CLIまたはWebインターフェースを使用して、FAT APのセキュリティIEおよび暗号スイートを設定します。

通常の方法

通常の方法を使用してサービスポリシーを追加するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management>Fat APs**を選択します。

   Fat AP Listページにすべてのfat APが表示されます。
3. FAT APの**Operation**アイコン をクリックします。
4. メニューからService Policyを選択します。

   Service Policy Managementページには、Service Policy ListにあるFAT APのすべてのサービスポリシー情報が表示されます。
5. Add Policyをクリックします。

サービスポリシーを追加するためのページが開きます。

6. 次のパラメーターを設定します。

- **Policy ID**: FAT APでサービスポリシーを一意に識別するためのサービスポリシーのIDを入力します。
- **Enable**: サービスポリシーがFAT APに適用されたときにすぐにイネーブルにする場合にだけ、このオプションを指定します。
- **SSID**: サービスポリシーのSSIDを入力します。
- **Encryption Mode**: サービスポリシーの暗号化モードを指定します。オプションは、ClearとCryptoです。Clearモードでは、データパケットを暗号化する必要はありません。Cryptoモードでは、すべてのデータパケットを暗号化する必要があります。
- **Hide SSID**: FAT APから送信されるビーコンフレーム内のSSIDを非表示にするには、このオプションを指定します。このパラメーターを選択すると、クライアントはビーコンフレームからSSIDを取得できず、ワイヤレスネットワークにアクセスする前にSSIDを設定する必要があります。このパラメーターを選択しないと、クライアントはビーコンフレームからSSIDを取得してワイヤレスネットワークにアクセスできます。
- **Authentication Mode**: サービスポリシーの認証モードを選択します。オプションは次のとおりです。
  - **Open System**: 認証を要求するすべてのクライアントが直接認証を通過できるようにします。
  - **Shared Key**: クライアントは、デバイスに設定されているものと同じ共有キーを使用する必要があります。Shared Keyは、暗号スイートとしてWEP40またはWEP104を選択した場合にだけ指定します。
  - **All**: クライアントが必要に応じてオープンシステムモードまたは共有キーモードを使用できるようにします。

  暗号化モードがClearの場合、認証モードはOpen Systemのみです。暗号化モードがCryptoの場合、認証モードオプションはOpen System、Shared Key、Allです。
- **Max Client**s: サービスポリシーを使用できるクライアントの最大数を入力します。

7. Encryption Mode(暗号化モード)としてCryptoを選択した場合は、次のセキュリティパラメーターを設定します。

- **Security IE** :FAT APによって送信されるビーコンフレームおよびプローブ応答で使用されるセキュリティIEを指定します。オプションは、None、RSN、WPA、およびAllです。
  - **None**: セキュリティIEは設定されていません。すべては、RSNとWPAの両方が設定されていることを示します。
  - **RSN**: 堅牢なセキュリティネットワークは、WPAよりも強力な保護を提供するために、堅牢なセキュリティネットワークアソシエーションの作成だけを可能にするセキュリティネットワークです。
  - **WPA**: WPAは、WPA-PSK(またはパーソナル)モードまたはWPA-802.1X(またはエンタープライズ)モードのいずれかで動作します。パーソナルモードでは、事前共有キーまたはパスフレーズが認証に使用されます。エンタープライズモードでは、802.1XおよびRADIUSサーバーとEAPが認証に使用されます。

  RSNとWPAの詳細については、関連するデバイスのマニュアルを参照してください。
- **Cipher Suite**: データフレームの暗号化および復号化に使用する暗号スイートを指定します。オプションは、TKIP、CCMP、WEP40、およびWEP104です。キーインデックスおよびキーは、WEP40またはWEP104を選択した場合にのみ設定できます。WEP40とWEP104の両方を選択することはできません。
  - **WEP**: WEP40とWEP104が含まれます。どちらも静的なWEP暗号化メカニズムです。WEP40キーは40ビットで、WEP104キーは104ビットです。WEPはRC4暗号化を使用し、ワイヤレスネットワークにアクセスするすべてのクライアントが同じキーを使用する必要があります。

- **TKIP**: Temporal Key Integrity Protocolは、WEPと同様にRC4アルゴリズムを使用しますが、WLANに対してより安全な保護を提供します。
- **CCMP**: Counter mode with CBC-MAC Protocolは、高いセキュリティを提供するためにAESに基づいたCounter-Mode/CBC-MACメカニズムです。

- **Key Index**: クライアントの認証キーインデックスを入力します。
- **Key**: クライアントの認証キーを入力します。

  WEP40の場合、キーは5文字の英数字の文字列です。WEP104

  の場合、キーは13文字の英数字の文字列です。

8. OKをクリックします。

Expressメソッド

express方式を使用してサービスポリシーを追加するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management>Fat APs**を選択します。

   Fat AP Listページにすべてのfat APが表示されます。
3. FAT APの**Operation**アイコン をクリックします。
4. メニューからService Policyを選択します。

   Service Policy Managementページには、Service Policy List上のFAT APに関するすべてのサービスポリシー情報が表示されます。
5. テンプレートの選択をクリックします。

   WSM内のすべてのサービスポリシーテンプレートがリストに表示されます。

   Select Service Policy Template
   - SSID: サービスポリシーのSSID。
   - **Encryption Mode**: サービスポリシーの暗号化モード。ClearまたはCrypto。

     Clearモードは、データパケットを暗号化する必要がないことを意味します。

     暗号モードでは、すべてのデータパケットを暗号化する必要があります。
   - **Hide SSID**: FAT APから送信されるビーコンフレーム内でSSIDを非表示にするかどうかを指定します。このパラメーターを選択すると、クライアントはビーコンフレームからSSIDを取得できず、ワイヤレスネットワークにアクセスする前にSSIDを設定する必要があります。このパラメーターを選択しないと、クライアントはビーコンフレームからSSIDを取得してワイヤレスネットワークにアクセスできます。
   - **Authentication Mode**: サービスポリシーの認証モード。オプションは次のとおりです。
     - **Open System**: 認証を要求するすべてのクライアントが直接認証を通過できるようにします。
     - **Shared Key**: クライアントは、デバイスに設定されているものと同じ共有キーを使用する必要があります。Shared Keyは、暗号スイートとしてWEP40またはWEP104を選択した場合にだけ指定します。
     - **All**: クライアントが必要に応じてオープンシステムモードまたは共有キーモードを使用できるようにします。
6. 使用するサービスポリシーテンプレートを指定します。
7. **Next**をクリックします。
8. サービスポリシーのIDを入力して、FAT AP上のサービスポリシーを一意に識別します。
9. OKをクリックします。

   Result Listページが開き、サービスポリシーを追加するための操作結果が表示されます。

10. Backをクリックして、現在のFAT APのService Policy Managementページに戻ります。

サービスポリシーの変更

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management>Fat APs**を選択します。

   Fat AP Listページにすべての Fat APが表示されます。
3. FAT APの**Operation**アイコン をクリックします。
4. メニューからService Policyを選択します。

   Service Policy Managementページには、Service Policy ListにあるFAT APのすべてのサービスポリシー情報が表示されます。
5. サービスポリシーの**Operation**アイコン をクリックします。
6. メニューから変更を選択します。

   Modify Service Policyページが開きます。
7. サービスポリシーパラメーターを変更します。

   詳細については、「サービスポリシーの追加」を参照してください。

   サービスポリシーIDは変更できません。ポリシーIDとSSIDは一意である必要があります。
8. OKをクリックします。

サービスポリシーにバインドされた無線の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management>Fat APs**を選択します。

   Fat AP Listページにすべての Fat APが表示されます。
3. FAT APの**Operation**アイコン をクリックします。
4. メニューからService Policyを選択します。

   Service Policy Managementページには、Service Policy ListにあるFAT APのすべてのサービスポリシー情報が表示されます。
5. サービスポリシーの**Operation**アイコン をクリックします。
6. メニューからBound Radiosを選択します。Radio Listダイアログボックスが開きます。

   Bound radiosリストには、現在のサービスポリシーにバインドされているすべての無線に関する情報が表示されます。オペレーターは、必要に応じて無線のバインドを解除できます。詳細については、「バッチでのサービスポリシーからの無線のバインド解除」を参照してください。
7. キャンセルをクリックして、ダイアログボックスを閉じます。

無線のサービスポリシーのバインディングとバインド解除

無線からサービスポリシーをアンバインドすると、サービスポリシーによって提供されるサービスが中断され、サービスポリシーに関連付けられているすべてのクライアントがログオフされます。

無線のサービスポリシーをバインドおよびアンバインドするには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Fat APs**を選択します。

   Fat AP Listページにすべての Fat APが表示されます。

3. FAT APのデバイスラベルをクリックします。Device Detailsページが開きます。
4. **Wireless Service Information**タブの**Radio Information**領域で、Modifyアイコンをクリックします。

   Modify Fat AP Radio Parametersページが開きます。
5. 次のいずれかの手順を実行します。
   - 選択したサービスポリシーをオンにして、サービスポリシーを無線にバインド解除します。
   - サービスポリシーを指定し、リストから無線論理インターフェースを選択して、サービスポリシーを無線にバインドします。1つの無線論理インターフェースをバインドできるサービスポリシーは1つだけです。
6. OKをクリックします。

バッチでのサービスポリシーからの無線のアンバインド

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Fat APs**を選択します。

   Fat AP Listページにすべてのfat APが表示されます。
3. FAT APの**Operation**nアイコン をクリックします。
4. メニューからService Policyを選択します。

   Service Policy Managementページには、Service Policy ListにあるFAT APのすべてのサービスポリシー情報が表示されます。
5. サービスポリシーの**Operation**アイコン をクリックします。
6. メニューから**Bound Radios**を選択します。
7. サービスポリシーからアンバインドする無線を指定します。
8. **Unbind**をクリックします。

サービスポリシーの削除

無線にバインドされているサービスポリシーを削除するには、まず無線からサービスポリシーのバインドを解除します。

サービスポリシーを削除するには

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Fat APs**を選択します。

   Fat AP Listページにすべてのfat APが表示されます。
3. FAT APの**Operation**アイコン をクリックします。
4. メニューからService Policyを選択します。

   Service Policy Managementページには、Service Policy ListにあるFAT APのすべてのサービスポリシー情報が表示されます。
5. サービスポリシーの**Operation**アイコン をクリックします。
6. メニューから**Delete**を選択します。

   確認ダイアログボックスが表示されます。
7. OKをクリックします。

ワイヤレス論理インターフェースの設定

サービスポリシーは、FAT APの無線論理インターフェースにバインドされます。無線論理インターフェースは、1つのサービスポリシーだけにバインドできます。

Wireless Logical Interface Configurationページには、Fat AP Listページ、fat AP detailsページ、またはConfiguration Managementページからアクセスできます。次の情報では、例としてfat AP listページを使用しています。

ワイヤレス論理インターフェースリストの表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Fat APs**を選択します。

   Fat AP ListページにすべてのFat APが表示されます。
3. FAT APの**Operation**アイコン ··· をクリックします。
4. メニューからWireless Logical Interface Configurationを選択します。

   Wireless Logical Interface Configurationページが開き、Wireless Logical Interface List上のFAT APのすべての無線論理インターフェース情報が表示されます。

   WLAN Logical Interface List

   - **Description**: WLAN-ESSインターフェースID形式のインターフェース名。
   - **SSID**: ワイヤレス論理インターフェースにバインドされているサービスポリシーのSSID。名前をクリックすると、その詳細が表示されます。空のフィールドは、インターフェースがどのサービスポリシーにもバインドされていないことを示します。
   - **Port Security Mode**: 無線論理インターフェースのポートセキュリティモード。オプションは次のとおりです。
     - **noRestrictions**
     - **mac-and-psk**
     - **mac-authentication**
     - **mac-else-userlogin-secure**
     - **mac-else-userlogin-secure-ext**
     - **psk**
     - **userlogin-secure**
     - **userlogin-secure-ext**
     - **userlogin-secure-or-mac**
     - **userlogin-secure-or-mac-ext**
     - **userlogin-secure-ext-or-psk**
     - **userlogin-with OUI**
   - **VLAN**: 無線論理インターフェースが属するVLAN。
   - **Operation**: ワイヤレス論理インターフェースの**Operation**アイコン ··· をクリックして、**Operation**メニューを表示します。

     サービスポリシーにバインドされていないインターフェースの場合、Operationメニューのオプションは次のとおりです。
     Delete Interface、Modify Port Security、およびModify VLAN。

     サービスポリシーにバインドされているインターフェースの場合、Operationメニューオプションは次のとおりです。
     Modify Port Security、Modify Service Policy、およびModify VLAN。

Wireless Logical Interface Listに十分な数のエントリーがある場合は、次のナビゲーションツールが表示されます。

- **Next Page**アイコンをクリックして、**Wireless Logical Interface List**で次のページに進みます。
- **Last Page**アイコンをクリックして、**Wireless Logical Interface List**の最後のページに進みます。
- **Previous Page**アイコンをクリックして、**Wireless Logical Interface List**の前のページに戻ります。
- **First Page**アイコンをクリックして、**Wireless Logical Interface List**の先頭に戻ります。

Wireless Logical Interface Listの右上にある**8**、**15**、**50**、**100**、または**200**をクリックして、各ページに表示する項目数を指定します。

ワイヤレス論理インターフェースリストは、操作フィールド以外のすべてのフィールドで並べ替えることができます。列ラベルをクリックすると、選択したフィールドでリストが並べ替えられます。列ラベルを使用すると、各フィールドに固有の並べ替えオプションを切り替えることができます。

ワイヤレス論理インターフェースの照会

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Fat APs**を選択します。

   Fat AP Listページにすべての Fat APが表示されます。
3. FAT APの**Operation**アイコン をクリックします。
4. メニューからWireless Logical Interface Configurationを選択します。

   Wireless Logical Interface Configurationページが開き、Wireless Logical Interface List上のFAT APのすべての無線論理インターフェース情報が表示されます。
5. 次の問合せ基準のいずれかまたは両方を指定します。
   - **Description**: インターフェースの説明を入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
   - **SSID**: FAT APのSSIDを入力します。WSMは、このフィールドのファジーマッチングをサポートしています。空のフィールドまたは無制限に設定されたフィールドは、クエリー条件として機能しません。
6. **Query**をクリックします。

Device Listには、クエリー基準に一致するすべての無線インターフェースが表示されます。Resetをクリックすると、クエリー基準がクリアされ、すべての無線インターフェースが表示されます。

ワイヤレス論理インターフェースの追加

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Fat APs**を選択します。

   Fat AP Listページにすべての Fat APが表示されます。
3. FAT APの**Operation**アイコン をクリックします。
4. メニューからWireless Logical Interface Configurationを選択します。

   Wireless Logical Interface Configurationページが開き、Wireless Logical Interface List上のFAT APのすべての無線論理インターフェース情報が表示されます。
5. Add Interfaceをクリックします。

   ワイヤレス論理インターフェースを追加するためのページが開きます。

6. ワイヤレス論理インターフェースのIDを入力します。FAT APの他のワイヤレス論理インターフェースと同じにすることはできません。
7. OKをクリックします。

   Adding Interface Resultページが開き、ワイヤレス論理インターフェースを追加する操作の結果が表示されます。
8. **Back**をクリックして、ワイヤレス論理インターフェースの設定ページに戻ります。

ワイヤレス論理インターフェースのポートセキュリティモードの変更

サービスポリシーにバインドされている無線論理インターフェースのポートセキュリティモードを変更するには、まず無線論理インターフェースのインターフェースIDを-1に設定します。

ワイヤレス論理インターフェースのポートセキュリティモードを変更するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Fat APs**を選択します。

   Fat AP Listページにすべての Fat APが表示されます。
3. FAT APのOperationアイコン ▪▪▪ をクリックします。
4. メニューからWireless Logical Interface Configurationを選択します。

   Wireless Logical Interface Configurationページが開き、Wireless Logical Interface List上のFAT APのすべての無線論理インターフェース情報が表示されます。
5. ワイヤレス論理インターフェースのOperationアイコン ▪▪▪ をクリックします。
6. 次のいずれかの手順を実行します。
   - メニューからModify Port Securityを選択します。
   - ポートセキュリティモードを変更するワイヤレス論理インターフェースを指定し、Wireless Logical Interface ListでModify Port Securityをクリックします。

     Modify Port Securityページが開きます。
7. 次のパラメーターを設定します。

   Port Security Mode: ワイヤレス論理インターフェースのポートセキュリティモードを指定します。オプションは次のとおりです。
   - **noRestrictions**
   - **mac-and-psk**
   - **mac-authentication**
   - **mac-else-userlogin-secure**
   - **mac-else-userlogin-secure-ext**
   - **psk**
   - **userlogin-secure**
   - **userlogin-secure-ext**
   - **userlogin-secure-or-mac**
   - **userlogin-secure-or-mac-ext**
   - **userlogin-secure-ext-or-psk**
   - **userlogin-with OUI**

   ポートセキュリティモードでは、次の注意事項に従ってください。
   - サービスポリシーの暗号化モードが**Clear**であるか、セキュリティIEが**None**である場合、無線論理インターフェースのポートセキュリティモードをmac-and-psk、psk、またはuserlogin-

secure-ext-or-pskにすることはできません。

- サービスポリシーの暗号化モードがCryptoで、セキュリティIEがRSNまたはWPAの場合、無線論理インターフェースのポートセキュリティモードは、**mac-and-psk、psk、userlogin-secure-ext-or-psk、**または**userlogin-secure-ext**のいずれかになり、キーネゴシエーションタイプは11 Keyになります。

  必要なキーパラメーターは、ポートセキュリティモードによって異なります。詳細については、表16を参照してください。

8. OKをクリックします。

Modify Port Securityページが開き、選択したワイヤレス論理インターフェースのポートセキュリティモードを変更するための操作結果が表示されます。

9. Backをクリックして、**Wireless Logical Interface Configuration**の設定ページに戻ります。

ワイヤレス論理インターフェースのVLANの変更

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Fat APs**を選択します。

   Fat AP Listページにすべての Fat APが表示されます。
3. FAT APのOperationアイコン ··· をクリックします。
4. メニューからWireless Logical Interface Configurationを選択します。

   Wireless Logical Interface Configurationページが開き、Wireless Logical Interface List上のFAT APのすべての無線論理インターフェース情報が表示されます。
5. 次のいずれかの手順を実行します。

- ワイヤレス論理インターフェースのOperationアイコン ··· をクリックして、メニューから**Modify VLAN**を選択します。
- VLANを変更するワイヤレス論理インターフェースを指定して**Wireless Logical Interface List**で**Modify VLAN**をクリックします。

  Modify VLANページが開きます。
6. VLANリストからVLANを指定します。

   VLAN Listには、FAT AP上の既存のすべてのVLANが表示されます。
7. OKをクリックします。

Modify VLANページが開き、選択したインターフェースが属するVLANの変更操作の結果が表示されます。

8. Backをクリックして、ワイヤレス論理インターフェースの設定ページに戻ります。

ワイヤレス論理インターフェースの削除

サービスポリシーにバインドされている無線論理インターフェースを削除するには、まず無線論理インターフェースのインターフェースIDを-1に設定します。

ワイヤレス論理インターフェースを削除するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Fat APs**を選択します。

   Fat AP Listページにすべての Fat APが表示されます。
3. FAT APのOperationアイコン ··· をクリックします。

4. メニューからWireless Logical Interface Configurationを選択します。

   Wireless Logical Interface Configurationページが開き、Wireless Logical Interface List上のFAT APのすべての無線論理インターフェース情報が表示されます。

5. 次のいずれかの手順を実行します。

   - ワイヤレス論理インターフェースのOperationアイコン ··· をクリックし、Delete Interfaceを選択します。
   - 削除するワイヤレス論理インターフェースを指定し、**Wireless Logical Interface List** の**Delete Interface**をクリックします。

   確認ダイアログボックスが表示されます。

6. OKをクリックします。

FAT APの同期化

WSMは、FAT AP構成の自動または手動による同期化をサポートしています。デフォルトでは、IMCはFAT APを2時間ごとに自動的に同期化します(『IMC Base Platform Administrator Guide』を参照)。また、必要に応じて、FAT APを手動で同期化することもできます。

FAT APを手動で同期するには、次の手順を実行し

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Fat APs**を選択します。

   Fat AP Listページにすべてのの Fat APが表示されます。

3. FAT APを指定します。
4. Synchronizeをクリックして、選択したFAT APの同期化を開始します。

プロセスが完了すると、ページがリフレッシュされ、最新のFAT AP情報が表示されます。

すべてのFAT APのエクスポート

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management>Fat APs**を選択します。

   Fat AP Listページにすべてのの Fat APが表示されます。

3. **Export All**をクリックします。

   FAT APのエクスポートのページが開きます。

4. Export Resultをクリックして、**.csv**ファイルを保存します。

FAT APのMPポリシーの表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Fat APs**を選択します。

   Fat AP Listページにすべてのの Fat APが表示されます。

3. FAT APのOperationアイコン ··· をクリックし、メニューからMPポリシー管理を選択します。MPポリシー管理ページが開きます。

   FAT APのすべてのメッシュポリシー情報がMPポリシーリストに表示されます。メッシュポリシーの追加、変更、および削除、メッシュポリシーの詳細の表示、およびメッシュポリシーへの無線のバイ

ンドまたはバインド解除を行うことができます。詳細については、「MPポリシーの管理」を参照してください。

FAT APのメッシュプロファイルの表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management>Fat APs**を選択します。

   Fat AP Listページにすべてのfat APが表示されます。
3. FAT APのOperationアイコン ▪▪▪ をクリックし、メニューからMesh Profile Managementを選択します。

   Mesh Interface Managementページが開きます。

   FAT APのすべてのメッシュプロファイル情報がMesh Profile Listに表示されます。メッシュプロファイルの追加、変更、削除、メッシュプロファイルの詳細の表示、およびメッシュプロファイルへの無線のバインドまたはバインド解除を行うことができます。詳細については、「MPポリシーの管理」を参照してください。

FAT APのメッシュインターフェースの表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management>Fat AP**sを選択します。

   Fat AP Listページにすべてのfat APが表示されます。
3. FAT APのOperationアイコン▪▪▪をクリックし、メニューからMesh Interface Managementを選択します。

   メッシュインターフェース管理ページが開きます。

   FAT APのすべてのメッシュインターフェース情報がMesh Interface Listに表示されます。メッシュインターフェースの追加、変更、削除、ポートセキュリティ設定の変更、およびメッシュインターフェースのVLANの変更を行うことができます。詳細については、「メッシュインターフェースの管理」を参照してください。

デフォルトマップ上のFAT APの位置

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management>Fat APs**を選択します。

   Fat AP Listページにすべてのfat APが表示されます。
3. FAT APのOperationアイコン▪▪▪ をクリックします。
4. メニューからLocate to Mapを選択します。デフォルトのマップページが開きます。

選択したFAT APが既定のマップでハイライト表示されます。既定のマップでFAT APを検索する前に、ワイヤレス検索を設定してください。詳細については、「GIS検索」を参照してください。

FAT APグローバルパラメーターの設定

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management>Fat APs**を選択します。

Fat AP Listページにすべてのの Fat APが表示されます。

3. FAT APのデバイスラベルをクリックします。
4. 次のいずれかの方法でパラメーターを設定する準備をします。
   - Wireless Service Informationタブで、グローバルパラメーター情報のModifyアイコンをクリックします。
   - ページの右側のWireless Service領域で、Global Configurationリンクをクリックします。Fat AP Parameter Configurationページが開きます。
5. 必要に応じて次のパラメーターを設定します。
   - **Client Keep-Alive Interval(s)**: クライアントのキープアライブ間隔を入力します。キープアライブメカニズムは、システムから分離されたクライアントを検出するために使用されます。FAT APはプローブ要求をクライアントに送信します。FAT APが応答を受信できない場合、クライアントとの接続を終了します。
   - **Client Idle-Timeout Interval(s)**: FAT APとクライアント間のリンクがアイドル状態になる最大間隔を入力します。FAT APが最大間隔内にクライアントから送信されたフレームを受信しない場合、FAT APはクライアントとの接続を終了します。
   - **Country/Region Code**: US(米国)やJP(日本)など、FAT APが属する国または地域のコードを指定します。無線の動作チャネルは国コードによって異なります。チャネルスキャンモードがAutoの場合は、FAT APの国コードによって、FAT APがスキャンするチャネルが決まります。
   - **Work Mode**: 操作モードを指定します。オプションはNormal、MonitorおよびHybridです。
     - **Normal**: Fat APは、クライアントにWLANサービスだけを提供します。
     - **Monitor**: Fat APはWLAN内のすべてのデバイスを監視しますが、WLANサービスは提供しません。
     - **Hybrid**: FAT APは、WLAN内のデバイスをスキャンすることも、ワイヤレスアクセスポイントとして機能することもできます。
6. OKをクリックします。

FAT APの詳細な無線情報の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > Resource Management>Fat APs**を選択します。
   Fat AP Listページには、すべてのFAT APが表示されます。
3. FAT APのデバイスラベルをクリックします。
4. **Wireless Service Information**タブの**Radio Information**領域で、詳細情報を表示する無線のIDをクリックします。

無線の詳細情報を表示するページが開きます。

Fat AP Radio Details

- **Beacon Interval(TU)**: 無線ビーコンの送信間にFAT APが待機するTUの数。
- **DTIM Interval**: DTIM送信間のビーコン間隔の数。
- **RTS Threshold(bytes)**: RTS方式が使用されるフレームの長さ。
- **Fragment Threshold(bytes)**: フラグメンテーションなしで送信できるフレームの最大長。
- **Short Frame Retransmission Threshold**: 確認応答が受信されない場合に、RTS/CTSしきい値よりも小さいユニキャストフレームの再送信試行回数。
- **Long Frame Retransmission Threshold**: RTS/CTSしきい値よりも大きいユニキャストフレ

ームの再送信試行回数。

- **Rx Lifecycle(ms)**: FAT APが受信したフレームがバッファメモリー内に留まることができる間隔。
- **Radio Type**: 無線のタイプ。オプションは次のとおりです。
  - **802.11a**
  - **802.11b**
  - **802.11g**
  - **802.11gn**
  - **802.11an**
- **Channels in Use**: 無線の現用チャネル。このフィールドにAutoと表示されている場合、FAT APはアイドルチャネルを現用チャネルとして選択します。
- **Max Transmit Power(dBm)**: 無線の最大送信電力(dBm)。
- **Preamble Type**: FAT APのプリアンブルタイプ。オプションはショートとロングです。
  - Short: Fat APは、ショートプリアンブルまたはロングプリアンブルのいずれかを使用してフレームを送信します。
  - Long: Fat APは、長いプリアンブルを持つフレームだけを送信します。
- **MP Policy**: WSM内の既存のMPポリシーを含む、無線にバインドされたMPポリシー。
- **Mesh Profile ID**: 無線にバインドされているメッシュプロファイルID。

Service Policy

- **SSID**: サービスポリシーのSSID。
- **Encryption Mode**: サービスポリシーの暗号化モード。オプションはClearおよびCryptoです。
  - **Clear**: データパケットを暗号化する必要はありません。
  - **Crypto**: すべてのデータパケットを暗号化する必要があります。
- **Hide SSID**: FAT APから送信されたビーコンフレームでSSIDを非表示にするかどうか。
- **Authentication Mode**: サービスポリシーの認証モード。オプションは次のとおりです。
  - **Open System**: 認証を要求するすべてのクライアントが直接認証を通過できるようにします。
  - **Shared Key**: クライアントは、デバイスに設定されているものと同じ共有キーを使用する必要があります。Shared Keyは、暗号スイートとしてWEP40またはWEP104を選択した場合にだけ指定します。
  - **All**: クライアントが必要に応じてオープンシステムモードまたは共有キーモードを使用できるようにします。

5. **Back**をクリックして、Fat AP Detailsページに戻ります。

FAT APのメッシュピアMACアドレスの設定

許可されたメッシュピアのMACアドレスを各FAT APの無線に設定して、WIDSを実装できます。

メッシュピアMACアドレスリストの表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management>Fat APs**を選択します。

   Fat AP Listページにすべての Fat APが表示されます。

3. FAT APのデバイスラベルをクリックします。
4. **Wireless Service Information**タブの**Radio Information**領域で、ターゲット無線の**Configure Mesh Peer MAC Address**アイコンをクリックして、メッシュピアのMACアドレスを設定するページを開きます。

   オペレーターは、**Peer MAC Address L**の現在の無線のネイバーのメッシュピアMACアドレスを表示できます。
5. **Back**をクリックして、Device Detailsページに戻ります。

メッシュピアMACアドレスの追加

1つの無線には最大8つのメッシュピアMACアドレスを設定できます。メッシュピアMACアドレスを追加するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management>Fat APs**を選択します。

   Fat AP Listページにすべての Fat APが表示されます。
3. FAT APのデバイスラベルをクリックします。
4. Wireless Service InformationタブのRadio Information領域で、ターゲット無線の**Configure Mesh Peer MAC Address**アイコンをクリックして、メッシュピアMACアドレスを設定するページを開きます。
5. Peer MAC Addressボックスに、メッシュピアのMACアドレスをhh:hh:hh:hh:hh:hh:hh:hhの形式で入力します。
6. Addをクリックします。
7. Backをクリックして、Device Detailsページに戻ります。

メッシュピアMACアドレスの削除

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management>Fat APs**を選択します。

   Fat AP Listページにすべての Fat APが表示されます。
3. FAT APのデバイスラベルをクリックします。
4. Wireless Service InformationタブのRadio Information領域で、ターゲット無線の**Configure Mesh Peer MAC Address**アイコンをクリックして、メッシュピアMACアドレスを設定するページを開きます。
5. Peer MAC Address Listで、1つ以上のMACアドレスを選択し、Deleteをクリックします。

確認ダイアログボックスが表示されます。

6. OKをクリックします。
7. Backをクリックして、FAT APの詳細ページに戻ります。

802.11レートの設定

この機能を使用すると、802.11a、802.11b、および802.11g無線でサポートされるレート、必須レート、およびディセーブルレートを変更できます。

802.11レートを設定するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management>Fat APs**を選択します。

   Fat AP Listページにすべての Fat APが表示されます。
3. FAT APのデバイスラベルをクリックします。
4. ページの右側にあるRRM Management領域で、Rate Set Configurationをクリックします。
5. 802.11a構成タブ、802.11b構成タブ、または802.11g構成をクリックします。
   タブを使用して、Supported Rate、Mandatory Rate、またはDisabled Rateタイプの無線レートを設定します。
6. レートタイプを指定して、対応するレートを設定します。
   - **802.11a Configuration**タブでは、オペレーターは各タイプのレートを設定できます。オプションは次のとおりです。
     - 6 Mb/s
     - 9 Mb/s
     - 12 Mb/s
     - 18 Mb/s
     - 24 Mb/s
     - 36 Mb/s
     - 48 Mb/s
     - 54 Mb/s
   - **802.11b Configuration**タブでは、オペレーターは各タイプのレートを設定できます。オプションは次のとおりです。
     - 1 Mb/s
     - 2 Mb/s
     - 5.5 Mb/s
     - 11 Mb/s
   - **802.11g Configuration**タブでは、オペレーターは各タイプのレートを設定できます。オプションは次のとおりです。
     - 1 Mb/s
     - 2 Mb/s
     - 5.5 Mb/s
     - 6 Mb/s
     - 9 Mb/s
     - 11 Mb/s
     - 12 Mb/s
     - 18 Mb/s
     - 24 Mb/s
     - 36 Mb/s
     - 48 Mb/s
     - 54 Mb/s
7. レートタイプを指定して、対応するレートを設定します。
8. OKをクリックします。

MCSの設定

必須およびサポート対象の802.11anまたは802.11gnレートを設定するには、最大MCSインデックスを指定します。MCSデータレートテーブルには、データレート、MCSインデックス、およびデータレートに影響するパラメーター間の関係が示されます。

802.11レートには、必須レート、サポートされるレートおよびマルチキャストレートの3つのタイプがあります。WSMでは、必須レートおよびサポートされるレートがサポートされます。

MCSを設定するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management>Fat APs**を選択します。

   Fat AP Listページにすべてのfat APが表示されます。
3. FAT APのデバイスラベルをクリックします。
4. ページの右側にあるRRM Management領域で、MCS Set Configurationをクリックします。

   注:

   MCS Set Configurationリンクは、FAT APが802.11 anまたは802.11 gnをサポートしている場合にだけ表示されます。

   - **Max Index of Mandatory MCS Set**: 最大の必須MCSを入力します。FAT APは必須レートをサポートする必要があります。クライアントがFAT APに関連付けられるのは、必須レートをサポートしている場合だけです。
   - **Max Index of Support MCS Set**: サポートされる最大MCSを入力します。必須の最大MCSよりも小さくすることはできません。これらは、必須レート以外にAPでサポートされるより高いレートです。サポートされるレートにより、必須レートとサポートされるレートの両方をサポートする一部のクライアントは、APと通信するときにより高いレートを選択できます。
5. OKをクリックします。

一般的な管理機能

トポロジーを表示する

この機能を使用すると、ワイヤレストポロジー内のFAT APを特定できます。ワイヤレストポロジー内のFAT APを特定するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management>Fat APs**を選択します。

   Fat AP Listページにすべてのfat APが表示されます。
3. FAT APのOperationアイコン…をクリックします。
4. メニューからView Topologyを選択します。ワイヤレストポロジーページが開きます。

選択したFAT APがトポロジー内で強調表示されます。FAT APに対する操作は、ワイヤレストポロジーから実行できます。詳細については、「FAT APのデバイストポロジーの表示」を参照してください。

ping

この機能を使用すると、管理対象のFAT APのIMCサーバーからの到達可能性をテストできます。選択したFAT APをFat AP Listページからpingするには、次の手順を実行します。

1. **Service**タブをクリックします。

2. ナビゲーションツリーから、**WLAN Manager > Resource Management>Fat APs**を選択します。

   Fat AP Listページにすべてのfat APが表示されます。
3. FAT APのOperationアイコン･･･をクリックします。
4. メニューからPingを選択します。Pingダイアログボックスが開きます。
5. Buffer Sizeリストから、pingパケットのサイズ(バイト単位)を選択します。
6. Numberリストから、選択したFAT APにIMCが送信するpingパケットの数を選択します。
7. OKをクリックして変更を受け入れ、pingテストを開始します。

   pingテストの結果をpingダイアログボックスで確認します。
8. OKをクリックします。

traceroute

この機能を使用すると、管理対象のFAT APのIMCサーバーからの到達可能性をテストし、接続の問題をトラブルシューティングして特定できます。

Fat AP Listページから選択したFat APに対してtracerouteを実行するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management>Fat APs**を選択します。

   Fat AP Listページにすべてのfat APが表示されます。
3. FAT APのOperationアイコン･･ をクリックします。
4. メニューからTraceRouteを選択します。

Traceroutedialogボックスが開き、tracerouteの結果が表示されます。

5. OKをクリックします。

FAT APのWebマネージャーを開く

この機能を使用すると、管理対象のFAT APにすばやくWebアクセスできます。

Web Managerを使用して選択したFAT APにアクセスして管理するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management>Fat APs**を選択します。

   Fat AP Listページにすべてのfat APが表示されます。
3. Webマネージャーの**Operation**アイコン･･･をクリックします。
4. メニューから**Open Web Manager**を選択します。

   Web Managerのインターフェースが開きます。
5. **Web Manager**のユーザー名とパスワードを入力します。
6. OKをクリックします。

Telnet

この機能により、管理対象のFAT APへの迅速かつ集中的なアクセスが可能になります。この機能を使用するには、IMCへのアクセスに使用するコンピュータ上でTelnetをサポートするオペレーティングシステムまたはアプリケーションが必要です。

Fat AP Listページから選択したFat APにTelnet接続するには、次の手順を実行します。

1. **Service**タブをクリックします。

2. ナビゲーションツリーから、**WLAN Manager > Resource Management>Fat APs**を選択します。

   Fat AP Listページにすべてのfat APが表示されます。
3. FAT APのOperationアイコン ··· をクリックします。
4. メニューから**Telnet**を選択します。
5. オペレーティングシステムの指示に従って、選択したFAT APとのTelnetセッションを確立するために使用するTelnetアプリケーションをロードします。

SSH

この機能を使用すると、管理対象のFAT APに迅速かつ集中的にアクセスできます。この機能を使用するには、ローカルデバイスにSSHアプリケーションをインストールする必要があります。この機能を初めて使用する場合は、オペレーティングシステムの指示に従ってSSHアプリケーションをロードします。この機能では、エージェントとしてIMCを使用し、クライアントブラウザから直接SSHを介してデバイスにアクセスして管理できます。

Fat AP ListページからSSHを使用して選択したFat APにログインするには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management>Fat APs**を選択します。

   Fat AP Listページにすべてのfat APが表示されます。
3. FAT APのOperationアイコン ··· をクリックします。
4. メニューから**SSH**を選択します。
5. オペレーティングシステムの指示に従って、選択したFAT APとのSSHセッションを確立するために使用するSSHアプリケーションをロードします。

ComwareベースのFIT APの管理

WSMを使用すると、管理者は、ComwareベースのACを介してComwareベースのFIT APを管理できます。

WSMでは、各Fit APはFit APテンプレートに対応します。Fit APがACに接続できるようにするには、最初に対応するFit APテンプレートをACに追加します。

FIT AP名とシリアル番号をCompliance Centerでチェックして、同じシリアル番号で異なる名前のAP、同じ名前で異なるシリアル番号のAP、または同じ名前とシリアル番号のAPが異なるACに存在しないことを確認できます。また、ACに設定されたVLANを確認して、VLAN設定エラーを回避することもできます。

現在のWSMバージョンでは、Comware 7 FIT APで使用できる機能は一部のみです。

Fit APリストの表示

fit APリストページには、IMC内のすべての管理対象fit APに関する情報が表示されます。次の情報が含まれます。

- Online status
- Device status
- Device label
- Serial number
- IP address
- MAC address
- Model
- VLAN ID of fit APs
- ACs
- Clients

オペレーターは、ベンダー基準をH3Cに設定した後、Fit AP ListでComwareベースのfit APに関する情報を表示できます。

FIT APリストを表示するには、次の手順を実行します。

1. Serviceタブをクリックします。
2. ナビゲーションツリーから、WLAN Manager > Resource Management>Fit APsを選択します。Fit AP Listページには、全てのFIT APが表示されます。

   Fit AP Listでは、オンライン状態のFit APはオンラインFit APであり、オフライン状態のFit APはオフラインFit APです。
   IP AddressおよびMAC Addressフィールドが空の場合は、APテンプレートにFIT APです。

   IP AddressフィールドとMAC Addressフィールドが空ではないオフライン状態のFit APは、オフラインFIT APです。

   Fit AP List

   - **Online Status**: スFIT APのオンラインステータス。
   - **Online and Online(Primary)**: Fit APは、プライマリACに接続するオンラインFit APです。
   - **Online(Secondary)**: Fit APはセカンダリACに接続するオンラインFit APです。

     Offline: FIT APはオフラインです。

     デフォルトでは、高度なクエリーが実行された場合にだけ、Online(Secondary)fit APsがFit AP Listに表示されます。
   - **Status**: FIT APの現在のアラームステータス。

- **AP Label**: IMCプラットフォームにFIT APを識別するデバイスラベル。
  詳細を表示するには、FIT APのデバイスラベルをクリックします。
  - アイコンの付いたデバイスラベルは、IoT APを表します。
  - アイコンの付いたデバイスラベルはWTを表します。
  - アイコンの付いたデバイスラベルはWTUを表します。
- **SN**: FIT APのシリアル番号。
- **IP Address**: FIT APのIPv4アドレス。
- **MAC Address**: FIT APのMACアドレス。
- **Model**: FIT APのモデル。
- **VLAN ID**: FIT APにバインドされたサービスポリシーに対応するVLAN ID。
- **AC**: FIT APを管理するAC。ACラベルをクリックすると、詳細が表示されます。
- **Total Clients** :FIT APに関連付けられているクライアントの数。

  数字をクリックすると、すべてのオンラインクライアントが表示されます。
- **Operation**: FIT APのOperationアイコン をクリックして、Operationメニューを表示します。

Operationメニューには、次の操作タスクがあります。

- Modifying/deleting fit AP templates
- ping
- traceroute
- Locating fit APs on the default map
- Locating to topology
- Monitoring fit APs in real time
- Viewing history information for online/offline fit APs

Fit AP Listに十分なエントリーが含まれている場合は、次のナビゲーション支援が表示されます。

- **Next Page**アイコンをクリックして、Fit AP Listの次のページに進みます。
- **Last Page**アイコンをクリックして、Fit AP Listの最後のページに進みます。
- **Previous Page**アイコンをクリックして、Fit AP Listで前のページに戻ります。
- **First Page**アイコンをクリックして、Fit AP Listの前にページに戻ります。

FIT AP Listの右上にある**8**、**15**、**50**、**100**、または**200**をクリックして、各ページに表示する項目数を指定します。

Operationフィールド以外のすべてのフィールドで**FIT AP LIST**をソートできます。選択したフィールドでリストをソートするには、列ラベルをクリックします。列ラベルを使用すると、各フィールドに固有のソートオプションを切り替えることができます。

FIT APのクエリー

WSMには、基本問合せと拡張問合せが用意されています。基本問合せ基準には、迅速な検索のためのキーパラメーターがいくつか含まれています。拡張問合せには、正確な照合のための様々な問合せ基準が用意されています。

詳細については、「FIT APのクエリー」を参照してください。

FIT APに関する簡単な情報の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management>Fit APs**を選択します。

   Fit AP Listページには、すべてのFIT APが表示されます。
3. FIT APのデバイスラベルをクリックします。

簡易のFIT APの情報ページが開きます。

Basic Information領域とClient Statistics領域のフィールドについては、「FIT APに関する詳細情報の表示」を参照してください。

Evaluation Result

- **Index**: 品質評価の基準。Associated Clients、Associated Failures、Alarms、CPU Usage(%)、およびMemory usage(%)が含まれます。
- **Expected Value**: 予測値を変更するには、アイコンをクリックして、表示されるウィンドウで予測値を変更します。デフォルトの予測値の詳細は、表18を参照してください。
- **Obtained Value**: 取得した値が予測値に達した場合は緑色で表示され、予測値に達しなかった場合は赤色で表示されます。
- **Risk**: インデックス値が期待値に達しない場合に発生するネットワークの問題。表18には、WSMによって対処される問題のみがリストされています。
- **Suggestion**: 問題を解決するために実行されるメジャー。表18には、WSMによって提案されるメジャーのみがリストされています。

表18 評価結果

索引	期待値	リスク	提案
関連付けられたクライアント	15以下	新しいクライアントのアクセス障害。 ネットワーク速度が遅い。	ロードバランシングをイネーブルにするか、またはより多くのAPを展開します。
関連する障害	0	新しいクライアントのアクセス障害。 ネットワーク速度が遅い。	ロードバランシングをイネーブルにするか、またはより多くのAPを展開します。
アラーム	0	アラーム状態で実行されているAP。	詳細なアラーム情報に基づいてアラームをクリアします。
CPU使用率(%)	75%以下	パフォーマンスの低い不安定なAP。	APの設定を確認します。
メモリー使用率(%)	75%以下	パフォーマンスの低い不安定なAP。	APの設定を確認します。

Trend graph

- **AP Rate Trend Graph**: 指定した時間範囲にFIT APの送信レートまたは受信レートのトレンドグラフ。
- **Associated Client Trend Graph**: 指定した時間範囲内でFIT APに関連付けられているクライアントの数量トレンドグラフ。
- **Clients by Radio Type**: FIT APに関連付けられたクライアントの無線タイプの分布。
- **Client Type**: FIT APに関連付けられたクライアントのベンダーの分布。

FIT APに関する詳細情報の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Fit APs**を選択します。

   Fit AP Listページには、全てのFIT APが表示されます。
3. FIT APのデバイスラベルをクリックします。
4. 簡易なFit AP情報ページの右上隅にある**More Detail**をクリックします。Fit APの詳細ページが開きます。

   Basic Information
   - **AP Label:** FIT APを識別するデバイスラベル。

     FIT APのデバイスラベルを変更するには、**Modify**アイコンをクリックします。ダイアログボックスが開きます。
   - **Online Status**: FIT APのオンラインステータス。
     - **Online and Online(Primary)**: Fit APは、プライマリACに接続するオンラインFit APです。
     - **Online(Secondary)**: Fit APはセカンダリACに接続するオンラインFit APです。
     - **Offline**: FIT APはオンラインではありません。
   - **AP Name**: FIT APの名前。
   - **AP Alias**: FIT APのエイリアス。
   - **Serial Number**: FIT APのシリアル番号。
   - **WT**: WTUが属するWT。このフィールドはWTUsでのみ使用できます。
   - **AC**: FIT APを管理するAC。

     名前をクリックすると、その詳細が表示されます。
   - **Mode**l: FIT APのモデル。
   - **MAC Address**: FIT APのMACアドレス。
   - **IP Address**: FIT APのIPv4アドレス。
   - **MAC Mode**: FIT APのMACモード。オプションは次のとおりです。
     - **Split**
     - **Localtunnel**
     - **Localbridge**
     - **FAT AP**
   - **Mask**: FIT APのIPアドレスマスク。
   - **Operation Status**: FIT APの工程ステータス。オプションは次のとおりです。
     - **Join**
     - **Join Confirm**
     - **Download**
     - **Config**
     - **Run**
   - **IPv6 Address**: FIT APのIPv6アドレス。FIT APにIPv6アドレスがない場合、このフィールドは空です。
   - **Template Description:** FIT APのテンプレート摘要。
   - **Work Mode**: Fit APの動作モード。オプションは次のとおりです。

- **Normal:** FIT APはクライアントに対してWLANサービスだけを提供します。
- **Monitor**: Fit APはWLAN内のすべてのデバイスを監視しますが、WLANサービスは提供しません。
- **Hybrid**: 最適なAPは、WLAN内のデバイスをスキャンし、ワイヤレスアクセスポイントとして機能します。

- **Software Ver**: FIT APのソフトウェアバージョン。
- **AP Online Time**: FIT APの最新オンライン継続時間。
- **Software Name**: FIT APで実行されているソフトウェアのファイル名。
- **Location**: FIT APのロケーションビュー。名前リンクをクリックすると、その詳細が表示されます。トポロジーを表示するには、**View Location**アイコンをクリックします。FIT APがどのロケーションビューにも属していない場合、トポロジーは空です。
- **AC Port Index** :ACをFIT APに接続するポートのインデックス。
- **AC Port Description**: ACをFIT APに接続するポートの説明。
- **Radio Statistics Interval(s)**: APが無線統計情報をACにレポートする間隔。
- **Respond to Broadcast Probes**: FIT APがクライアントから送信されたブロードキャストに応答するかどうか。
- **Connection Priority**: FIT APの接続優先度。

  複数のACが使用可能な場合、最適なAPは最高の接続プライオリティでACに接続します。値の範囲は0～7です。値が大きいほど、プライオリティが高くなります。
- **Client Idle-Timeout Interval(s)**: FIT APとクライアント間のリンクがアイドル状態になる最大間隔。

  FIT APが最大間隔内にクライアントから送信されたフレームを受信しない場合、ACはFIT APとクライアント間の接続を終了します。
- **Client Keep-Alive Interval(s)**: クライアントのキープアライブインターバル。

  キープアライブメカニズムは、システムから分離されたクライアントを検出するために使用されます。FIT APはクライアントにプローブ要求を送信します。FIT APが応答を受信できない場合、ACはFIT APとクライアント間の接続を終了します。
- **Flash Free(Bytes)**: FIT AP上のフラッシュの空きメモリー。
- **Enable Mesh Portal Service**: メッシュポータルサービスは、FIT APで有効または無効になっています。
  - **Yes**: メッシュポータルサービスがイネーブルになっており、FIT APはメッシュネットワーク内でMPPとして動作できます。
  - **No**: メッシュポートサービスはイネーブルではありません。
- **Whether it is an engineered Fit AP**: Fit APが設計されたFit APかどうか。設計されたFit APは、インストールされているがデバッグ状態にあるFit APです。

Client Statistics

- オンラインクライアント:FIT APに関連付けられているクライアントの数。この数をクリックすると、すべてのオンラインクライアントが表示されます。
- **Associated Clients**: クライアントとFIT AP間で成功したアソシエーションの数。
- **Associated Failures**: クライアントとFIT AP間で失敗したアソシエーションの数。
- **Denied Registered Clients**: クライアントとFIT AP間で拒否されたアソシエーションの数。
- **Re-associated Clients**: クライアントとFIT AP間の再アソシエーションの数。
- **Exceptional Deauthenticated Clients**: クライアントとFIT AP間の例外的なアソシエーション解除の数。

Reason for Association Failures-Today

- **Associated client upper limit reached**: オンラインクライアントの上限に達したために、今日、FIT APとのアソシエートに失敗したクライアントの数。
- **Unsupported mandatory rate**: クライアントがfit APの必須レートをサポートしていないために、今日fit APとの関連付けに失敗したクライアントの数。
- **Re-Associate Failed**: 再アソシエーションの失敗のために、その日にFIT APとのアソシエートに失敗したクライアントの数。
- **Others (such as weak signal and blacklist)**: 信号強度が弱い、またはクライアントがブラックリストに載っているなどのその他の理由で、その日にFIT APとの関連付けに失敗したクライアントの数。
- **Unknown Reason**: 不明な理由により、今日、FIT APとの関連付けに失敗したクライアントの数。

  右上隅の**More**をクリックすると、アソシエーションの失敗に関するタイムテーブルが表示されます。

IoT Modules

この領域は、FIT APがIoT APの場合にのみ表示されます。IoTモジュールの詳細は、「IoTモジュールの管理」を参照してください。

- **ID**: FIT AP上のIoTモジュールのID。
- **Type**: FIT AP上のIoTモジュールのタイプ。
- **Status**: FIT AP上のIoTモジュールの管理ステータス。
- **Version**: FIT AP上のIoTモジュールのバージョン。
- **Sequence ID**: FIT AP上のIoTモジュールのシーケンス番号。

Wireless Service

- **BSSID** :FIT APのBSSID。FIT APのMACアドレスで表されます。
- **Radio ID**: FIT AP上の無線のID。

  IDをクリックすると、詳細な無線情報が表示されます。
- **Service Policy SSID** : FIT AP上の無線にバインドされたサービスポリシーに対応するSSID。

  名前をクリックすると、その詳細が表示されます。
- **VLAN ID**: 現在の無線にバインドされているサービスポリシーで設定されているVLAN ID。

Radios

- **ID**: 無線のID。

  IDをクリックすると、その詳細が表示されます。
- **Radio Type**: 無線のタイプを選択します。オプションは次のとおりです。
  - **802.11a**
  - **802.11b**
  - **802.11g**
  - **802.11bg**
  - **802.11at**
  - **802.11an**
  - **802.11gn**
  - **802.11n(2.4GHz)**
  - **802.11bgn**
  - **802.11n**
  - **802.11n(5GHz)**
- **Channel**: 無線の現用チャネル。値の範囲は無線タイプによって異なります。フィールドに

Autoと表示されている場合、FIT APはチャネル品質を評価し、最適なチャネルを現用チャネルとして選択します。

- **Current Transmission Power(dBm)**: 無線の現在の送信電力。
- **Admin Status**: 無線の管理状態。オプションはUpおよびDownです。
- **Operation Status**: 無線の現在の状態。オプションはUpおよびDownです。
- **Operation**: **Modify and Configure Mesh Peer MAC Address**オプションを提供します。

  オペレーターは、**Modify**アイコンをクリックして無線パラメーターを変更し、**Configure Mesh Peer MAC Address**アイコンをクリックして、FIT APのネイバーMACアドレスを設定できます。詳細については、「FIT APの無線パラメーターの変更」および「重要なAPのメッシュピアMACアドレスの設定」を参照してください。

X-Shareアンテナ

- **Antenna ID**: アンテナのID。
- **Radio**: アンテナの無線ID。
- **Attenuation**: アンテナの減衰値。
- **Description**: アンテナの説明。
- **Modify**: アンテナのパラメーターを変更するには、Modifyアイコンをクリックします。「Xシェアアンテナのパラメーターの変更」を参照してください。

Neighbor

作業モードがMonitorまたはHybridに設定されている場合、Fit APはネイバーAPを自動的にスキャンし、検出されたネイバーFit APをネイバーリストに表示します。

- **Radio ID**: ネイバーFIT AP上の無線のID。
- **MAC Address**: 無線にバインドされたサービスポリシーのBSSID。
- **AP Label**: ネイバーAPのデバイスラベル。
- **Channel**: 無線の現用チャネル。
- **Interference(%)**: チャネルのインターフェースレート。
- **Signal Strength(dBm)**: 無線の信号強度。

WTに関する詳細情報の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management>Fit APs**を選択します。

   Fit AP Listページには、全てのFIT APが表示されます。
3. WTのAPラベルをクリックします。

   Basic Information

   - **AP Label**: WTを識別するデバイスラベル。

     WTのデバイスラベルを変更するには、**Modify**アイコンをクリックします。ダイアログボックスが開きます。
   - オンラインステータスWTのオンラインステータス。
     - **Online and Online(Primary)**: WTは、プライマリACに接続するオンラインWTです。
     - **Online(Secondary)**: WTは、セカンダリACに接続するオンラインWTです。
     - **Offline**: WTはオンラインではありません。
   - **AP Name**: WTの名前。

- **AP Alias**: WTのエイリアス。
- **Serial Number**: WTのシリアル番号。
- **AC**: WTを管理するAC。名前をクリックすると、その詳細が表示されます。
- **Model**: WTのモデル。
- **MAC Address**: WTのMACアドレス。
- **IP Address**: WTのIPv4アドレス。
- **MAC Mode**: WTのMACモード。オプションは次のとおりです。
  - **Split**
  - **Localtunnel**
  - **Localbridge**
  - **FAT AP**
- **Mask**: WTのIPアドレスマスク。
- **Operation Status**: WTの工程ステータス。オプションは次のとおりです。
  - Join
  - Join Confirm
  - Download
  - Config
  - Run
- **IPv6 Address**: WTのIPv6アドレス。WTにIPv6アドレスがない場合、このフィールドは空です。
- **Template Description**: WTのテンプレートの説明。
- **Software Version**: WTのソフトウェアバージョン。
- **AP Online Time**: WTの最新オンライン継続時間。
- **Software Name**: WT上で実行されているソフトウェアのファイル名。
- **Location**: WTのロケーションビュー。名前リンクをクリックすると、その詳細が表示されます。トポロジーを表示するには、**View Location**アイコンをクリックします。WTがどのロケーションビューにも属していない場合、トポロジーは空です。
- **AC Port Index**: ACをWTに接続するポートのインデックス。
- **AC Port Description**: ACをWTに接続するポートの説明。

WTU

- **AP Label**: WTUを識別するデバイスラベル。
- **SN**: WTUのシーケンス番号。
- **IP Address**: WTUのIPアドレス。
- **MAC Address**: WTUのMACアドレス。
- **Model**: WTUのモデル。
- **Interfaces**: WTUをWTに接続するインターフェース。

Fit APテンプレートの管理

ACを介してFit APを管理するには、AC上のFit AP用にFit APテンプレートを作成する必要があります。

FIT APがACとの関連付けを試みると、ACはFIT APのシリアル番号とFIT APテンプレートのシリアル番号を比較します。一致するものが見つかると、ACはFIT APの関連付け要求を受け入れ、FIT APを管理します。一致するものが見つからない場合、ACはFIT APの関連付け要求を拒否します。

FIT AP/FIT APテンプレートリストの表示、FIT APテンプレートの追加、修正、削除、FIT APテンプレートのインポート、FIT APテンプレートのエクスポート、FIT APの再起動、およびFIT APラベルの同期を行うことができます。

Fit APまたはFit APテンプレートリストの表示

AP/fit APテンプレートリストは、ACリストページ、AC詳細ページまたは構成管理ページから表示できます。次の手順では、ACリストページを例として使用します。

fit APテンプレートリストを表示するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management>ACs**を選択します。

   AC Listページにすべてのが表示されます。
3. ACの**Operation**アイコン をクリックします。
4. メニューからFit AP Listを選択します。

   Fit AP Listページには、全てのFIT APが表示されます。

   Fit AP Listで、オンライン状態のFit APはオンラインFit APです。

   IP Addressフィールドと**MAC Address**フィールドが空のFit APは、Fit APテンプレートと一致するFit APです。

   IP Addressフィールドと**MAC Address**フィールドが空でないオフライン状態のFit APは、オフラインFIT APです。

   FIT AP List

   - **Online Status**: FIT APのオンラインステータス。
     - **Online and Online(Primary)**: Fit APは、プライマリACに接続するオンラインFit APです。
     - **Online(Secondary)**: Fit APはセカンダリACに接続するオンラインFit APです。

     Offline: FIT APはオンラインではありません。
   - **AP Name**: FIT AP/FIT APテンプレートの名前。

     名前をクリックすると、その詳細が表示されます。
   - **AP Alias**: FIT APテンプレートのエイリアス。
   - **SN**: FIT APのシリアル番号。
   - **IP Address**: FIT APのIPv4アドレス。
   - **MAC Address**: FIT APのMACアドレス。
   - **Model**: Fit AP/fit APテンプレートのモデル。
   - **Clients**: FIT APに関連付けられているクライアントの数。この数をクリックすると、すべてのオンラインクライアントが表示されます。

     Fit AP Listに十分なエントリーが含まれている場合は、次のナビゲーション支援が表示されます。

- **Next Page**アイコンをクリックして、Fit AP Listで次のページに進みます。
- **Last Page**アイコンをクリックして、Fit AP Listの最後のページに進みます。
- **Previous Page**アイコンをクリックして、Fit AP Listで前のページに戻ります。
- **First Page**アイコンをクリックして、Fit AP Listの前にページに戻ります。

FIT AP Listの右上にある**8、15、50、100**、または**200**をクリックして、各ページに表示する項目数を指定します。

Operationフィールド以外のすべてのフィールドで**Fit AP List**をソートできます。選択したフィールドでリストをソートするには、列ラベルをクリックします。列ラベルを使用すると、各フィールドに固有のソートオプションを切り替えることができます。

Fit APテンプレートの追加

Fit APテンプレートには、共通テンプレートと自動テンプレートの2種類があります。

- **Common fit AP template**

  ACに共通のFit APテンプレートを追加すると、Fit APがACに接続しようとしたときに、ACはFit APのシリアル番号をFit APテンプレートのシリアル番号と照合します。一致するものが見つかると、Fit APはACに接続できます。一致するものが見つからないと、Fit APはACに接続できません。

- **Auto fit AP template**

  自動APを有効にして、AC上のFIT APモデルに対応する自動FIT APテンプレートを追加すると、FIT APがACに接続しようとするときに、ACはFIT APのシリアル番号をFIT APテンプレートのシリアル番号と照合します。共通のFIT APテンプレートが存在しないか、一致するものが見つからない場合、ACはFIT APモデルを自動FIT APテンプレートのモデルと照合します。一致するものが見つかると、FIT APはACに接続できます。一致するものが見つからない場合、FIT APはACに接続できません。

  自動FIT APテンプレートを使用してFIT APがACに自動的に接続すると、ACは一時的なFIT APテンプレートを生成します。このテンプレートは現在のACのFIT APリストに表示されます。オペレーターは、CLIで一時的なFIT APテンプレートの名前を変更して、共通のFIT APテンプレートに変更できます。一時的なFIT APテンプレートが共通のテンプレートに変更されない場合、一時的なFIT APテンプレートは、自動的に接続されたFIT APがオフラインになった後で自動的に削除されます。詳細については、ACのコンフィギュレーションガイドを参照してください。

Fit APテンプレートを追加するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management>ACs**を選択します。

   AC Listページにすべてのが表示されます。
3. ACの**Operation**アイコン▪▪▪をクリックします。
4. メニューからFit AP Listを選択します。

   Fit AP Listページには、全てのFIT APが表示されます。
5. **Add**をクリックします。
6. 次のパラメーターを設定します。
   - **AP Name** :FIT APテンプレートを一意に識別するためのFIT APテンプレートの名前を入力します。
   - **AP Alias**: FIT APテンプレートのエイリアスを入力します。
   - **Serial Number**: FIT APのシリアル番号を入力するか、**Auto**(大文字と小文字は区別されます)と入力します。**Auto** と入力すると、auto FIT AP テンプレートが追加されます。**AC Parameter Configuration**で**Auto AP** を有効にすると(「AC グローバル パラメーターの設定」を参照)、auto FIT AP テンプレートで設定されたものと同じデバイス モデルを持つすべてのFIT AP が AC に自動的に接続でき、FIT AP に表示されます。AP name_001、AP name_002、AP name_00N という名前でリストします (AP name はauto FIT AP テンプレート名です)。Fit AP がオフラインになると、Fit AP リストに表示されません。オペレーターは AC にログインして、auto FIT AP テンプレートを共通のものに切り替え、FIT AP の名前を変更できます。

- **Model**: FIT APのモデルを選択します。オプションは、現在のACでサポートされているすべてのFIT APモデルです。
- **Work Mode**: Fit APの動作モードを選択します。オプションは次のとおりです。
  - **Normal**: FIT APはクライアントにWLANサービスだけを提供します。
  - **Monitor** :Fit APはWLAN内のすべてのデバイスを監視しますが、WLANサービスは提供しません。
  - **Hybrid**: 最適なAPは、WLAN内のデバイスをスキャンし、ワイヤレスアクセスポイントとして機能します。
- **Respond to Broadcast Probes**: クライアントから送信されたブロードキャストに応答するAPを有効または無効にします。
- **Connection Priority**: FIT APの接続プライオリティを入力します。

  複数のACが使用可能な場合、最適なAPは最高の接続プライオリティでACに接続します。値の範囲は0～7です。値が大きいほど、プライオリティが高くなります。
- **Client Idle-Timeout Interval(s)**: FIT APとクライアント間のリンクがアイドル状態になる最大間隔を入力します。

  FIT APが最大間隔内にクライアントから送信されたフレームを受信しない場合、ACはFIT APとクライアント間の接続を終了します。
- **Client Keep-Alive Interval(s)**: クライアントのキープアライブインターバルを入力します。

  キープアライブメカニズムは、システムから分離されたクライアントを検出するために使用されます。FIT APはクライアントにプローブ要求を送信します。FIT APが応答を受信できない場合、ACはFIT APとクライアント間の接続を終了します。
- **Description**: FIT APの説明を入力します。
- **Enable Mesh Portal Service**: FIT APのメッシュポータルサービスを有効または無効にします。オプションは次のとおりです。
  - **Yes**: メッシュポータルサービスがイネーブルになっており、Fit APはメッシュネットワーク内でMPPとして動作できます。
  - **No**: メッシュポータルサービスは有効ではありません。

    このパラメーターを設定する前に、fit APがメッシュをサポートしていることを確認してください。fit APがメッシュをサポートしていない場合、設定は失敗します。詳細については、fit APのデバイスマニュアルを参照してください。
- **Synchronize AC Configuration**: Fit APテンプレート内の設定を、指定したACグループ内のすべてのACに適用します。

  Fit APテンプレートの設定を現在のACだけに適用する場合は、このオプションを選択しないでください。このオプションは、ACが少なくとも1つのACグループに属している場合にのみ使用できます。
- **AC Group**: ACグループを選択します。

  オプションは、現在のACが属するすべてのACグループです。このオプションは、AC構成の同期が選択されている場合にのみ使用できます。
- **Other Connection Priority**: ACグループ内の他のACへの接続に適したAPの接続プライオリティを入力します。

  複数のACが使用可能な場合、最適なAPは最高の接続プライオリティでACに接続します。値の範囲は0～7です。値が大きいほど、プライオリティが高くなります。

7. **OK**をクリックします。

Fit APテンプレートのインポート

WSMでは、FIT APテンプレートをインポートするときに、FIT APのシリアル番号がキーワードとして使用されます。インポートファイルは.csvファイルである必要があります。WSMでは、インポートファイルの最初の行もFIT APテンプレート情報としてインポートされます。インポートファイルに3,000行を超える行が含まれている場合、WSMでは最初の3,000行のみがインポートされます。

Fit APテンプレートをインポートするには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management>ACs**を選択します。

   AC ListページにすべてのACが表示されます。
3. ACの**Operation**アイコン をクリックします。
4. メニューからFit AP Listを選択します。

   Fit AP Listページには、全てのFIT APが表示されます。
5. **Import**をクリックします。
6. 次のいずれかの方法で手順を続行します。
   - **Source File**フィールドに、インポートするファイルのフルパスを入力します。
   - インポートするファイルのローカルコンピュータのファイルシステムを参照します。参照するには、**Source File**フィールドの右にある**Browse**ボタンをクリックします。ブラウザの指示に従ってファイルを検索します。
7. **Next**をクリックします。

   Fit AP Template Listには、ソースファイルに含まれているすべてのFit APテンプレートが表示されます。

   Fit AP Template List
   - **AP Name**: FIT APテンプレートの名前。
   - **AP Alias**: FIT APテンプレートのエイリアス。
   - **Serial Number**: FIT APのシリアル番号。
   - **Model**: FIT APのモデル。
   - **Work Mode**: Fit APの動作モード。オプションは、Normal、Monitor、およびHybridです。
     - **Normal**: FIT APはクライアントにWLANサービスだけを提供します。
     - **Monitor**: Fit APはWLAN内のすべてのデバイスを監視しますが、WLANサービスは提供しません。
     - **Hybrid**: 最適なAPは、WLAN内のデバイスをスキャンし、ワイヤレスアクセスポイントとして機能します。
8. (任意)インポートする必要のないfit APテンプレートを削除するか、fit APテンプレートの動作モードを変更します。

   Fit APテンプレートを削除するには:

   a. ターゲットFIT APテンプレートを選択し、**Delete**をクリックします。確認のダイアログボックスが開きます。

   b. OKをクリックします。

   FIT APテンプレートの動作モードを変更するには、ターゲットのFIT APテンプレートを選択し、**Monitor**, **Normal**, または **Hybrid**をクリックします。
9. OKをクリックします。

結果リストには、FIT APテンプレートのインポート結果が表示されます。

AP Template Import
- **AP Name**: FIT APテンプレートの名前。

- **SN**: Fit APテンプレートのシリアル番号。
- **Result**: FIT APテンプレートをインポートしたときの操作結果。詳細については、表19を参照してください。
- **Failure Cause**: このオプションは、FIT APテンプレートのインポートに失敗した場合にだけ使用できます。

表19 Fit APテンプレートのインポートの操作結果

運転結果	理由
APテンプレートが正常に追加されました	Fit APテンプレートが正常にインポートされました。
APテンプレートが正常に変更されました	インポートされたFIT APテンプレートのシリアル番号とAP名が既存のFIT APテンプレートと同じ場合、WSMはインポートされたFIT APテンプレートの情報に従って既存のFIT APテンプレートの情報を修正します。
APテンプレートの追加に失敗しました	WSMでは、FIT APテンプレートはインポートされず、インポートされるFIT APテンプレートのシリアル番号が既存のFIT APテンプレートと同じでもAP名が異なる場合は、"AP name cannot be modified"と表示されます。
	インポートされたFIT APテンプレートのモデルは、現在のACではサポートされていません。
	インポートされた自動FIT APテンプレートのモデルは、現在のACの既存の自動FIT APテンプレートのモデルと同じです。
	インポートファイル内の値の形式が無効です。
	インポートファイルがNULLです。

10. Backをクリックして、Fit AP Listページに戻ります。

ACのすべてのFit APまたはFit APテンプレートのエクスポート

この機能を使用すると、ACによって管理されるすべてのFit APまたはFit APテンプレートを.csvファイルにエクスポートして保存できます。

すべてのFit APまたはFit APテンプレートをエクスポートするには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。

   AC Listページにすべてのacが表示されます。
3. ACの**Operation**アイコン をクリックします。
4. メニューからFit AP Listを選択します。

   Fit AP Listページには、全てのFIT APが表示されます。
5. **Export All**をクリックします。
6. **AP Template Export Result**をクリックして、ファイルをローカルコンピュータにダウンロードします。

Fit APまたはFit APテンプレートの変更

1. Serviceタブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。

AC Listページにすべてのacが表示されます。

3. acの**Operation**アイコン をクリックします。
4. メニューからFit AP Listを選択します。

   Fit AP Listには、全てのFIT APが表示されます。
5. fit APのデバイスラベルをクリックします。

   fit APの詳細ページが開きます。
6. ページの右側にあるActionメニューで、Modify AP Templeを選択します。

   Modify AP Templateページが開きます。
7. 必要に応じて、次のパラメーターを変更します。
   - **AP Name**: このフィールドは変更できません。
   - **AP Alias**: FIT APテンプレートのエイリアスを入力します。
   - **Serial Number**: このフィールドは変更できません。
   - **Model**: このフィールドは変更できません。
   - **Work Mode**: Fit APの動作モードを選択します。オプションは次のとおりです。
     - **Normal** :FIT APはクライアントにWLANサービスだけを提供します。
     - **Monitor**: Fit APはWLAN内のすべてのデバイスを監視しますが、WLANサービスは提供しません。
     - **Hybrid**: FIT APは、WLAN内のデバイスをスキャンし、ワイヤレスアクセスポイントとして機能します。
   - **Respond to Broadcast Probes**: クライアントから送信されたブロードキャストに応答するようにFIT APをイネーブルにするか、クライアントから送信されたブロードキャストに応答しないようにFIT APをディセーブルにします。
   - **Connection Priority**: FIT APの接続プライオリティを入力します。

     複数のacが使用可能な場合、最適なAPは最高の接続プライオリティでacに接続します。値の範囲は0～7です。値が大きいほど、プライオリティが高くなります。
   - **Client Idle-Timeout Interval(s)**: FIT APとクライアント間のリンクがアイドル状態になる最大間隔を入力します。FIT APが最大間隔内にクライアントから送信されたフレームを受信しない場合、acはFIT APとクライアント間の接続を終了します。
   - **Client Keep-Alive Interval(s)**: クライアントのキープアライブインターバルを入力します。

     キープアライブメカニズムは、システムから分離されたクライアントを検出するために使用されます。FIT APはクライアントにプローブ要求を送信します。FIT APが応答を受信できない場合、acはFIT APとクライアント間の接続を終了します。
   - **Description**: FIT APの説明を入力します。
   - **Enable Mesh Portal Service**: FIT APのメッシュポータルサービスを有効または無効にします。オプションは次のとおりです。
     - **Yes**: メッシュポータルサービスがイネーブルになっており、Fit APはメッシュネットワーク内でMPPとして動作できます。
     - **No**: メッシュポータルサービスは有効ではありません。

     このパラメーターを設定する前に、fit APがメッシュをサポートしていることを確認してください。fit APがメッシュをサポートしていない場合、設定は失敗します。詳細については、fit APのデバイスマニュアルを参照してください。
8. OKをクリックします。

APの再起動

オンラインFIT APのみを再起動できます。

FIT APを再起動するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > AC**sを選択します。

   AC Listページにすべてのacが表示されます。
3. ACのOperationアイコン をクリックします。
4. メニューからFit AP Listを選択します。

   Fit AP Listページには、全てのFIT APが表示されます。
5. 再起動するFit APのデバイスラベルをクリックします。

   fit APの詳細ページが開きます。
6. ページの右側にある**Action**メニューで、**Reset**アイコンをクリックします。確認ダイアログボックスが開きます。
7. OKをクリックします。

Fit APまたはFit APテンプレートの削除

オンラインFit APに対応するFit APテンプレートは削除できません。テンプレートを削除するには、Fit APを再起動してください。

Fit APまたはFit APテンプレートを削除するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。

   AC Listページにすべてのacが表示されます。
3. ACのOperationアイコン をクリックします。
4. メニューからFit AP Listを選択します。

   Fit AP Listページには、全てのFIT APが表示されます。
5. FIT APテンプレートを選択します。
6. **Delete**をクリックします。

確認ダイアログボックスが表示されます。

7. OKをクリックします。

FIT APラベルの同期化

WSMでは、ラベルを使用してAPを一意に識別します。

この機能を使用すると、同じACによって管理されているFIT APのラベルを同期化できます。FIT APラベルは、AP名、エイリアス、または説明から同期化できます。

FIT APラベルを同期するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > AC**sを選択します。

   AC Listページにすべてのacが表示されます。
3. ACのOperationアイコン をクリックします。
4. メニューからFit AP Listを選択します。

   Fit AP Listページには、全てのFIT APが表示されます。

5. FIT APを選択します。
6. Synchronize AP Labelをクリックし、From AP Name、From AP Alias、またはFrom AP Descriptionを選択します。

同期が完了すると、同期結果を表示できます。

FIT APの同期化

WSMでは、Fit AP構成の手動同期化がサポートされています。

Fit APを手動で同期化する手順は、次のとおりです

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Fit APs**を選択します。

   Fit AP Listページには、全てのFIT APが表示されます。
3. Fit APを選択します。
4. **Synchronize**をクリックして、選択したFIT APの同期化を開始します。

プロセスが完了すると、ページが更新され、最新のFit AP情報が表示されます。

すべてのFIT APのエクスポート

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Fit APs**を選択します。

   Fit AP Listページには、全てのFIT APが表示されます。
3. **Export All**をクリックします。

FIT APをエクスポートするためのページが開きます。

4. **Export Result**をクリックして、**.csv**ファイルを保存します。

トポロジーを検索しています

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Fit APs**を選択します。

   Fit AP Listページには、全てのFIT APが表示されます。
3. FIT APのOperationアイコン･･･をクリックします。
4. メニューから、**Locate to Topology**を選択します。

   APのロケーションビュートポロジーが表示されます。

デフォルトマップ上でのFIT APの検索

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Fit APs**を選択します。

   Fit AP Listページには、全てのFIT APが表示されます。
3. FIT APのOperationアイコン･･･ をクリックします。
4. メニューから**Locate to GIS Map**を選択します。

既定のマップページが開きます。

選択したFIT APが既定のマップでハイライト表示されます。既定のマップでFIT APを検索する前に、ワイヤレス検索を設定してください。詳細については、「GIS検索」を参照してください。

FIT APをリアルタイムで監視

この機能を使用すると、FIT APをAPおよび無線でリアルタイムに監視できます。オンラインFIT APのみを監視できます。

- CPU使用率、メモリー使用率、AP温度、オンラインクライアント、正常に関連付けられたクライアント数、関連付けの失敗数、再関連付けられたクライアント数、拒否されたクライアント数、および例外的に認証解除されたクライアント数をAPごとにリアルタイムで監視できます。CPU使用率とメモリー使用率は、トレンドグラフに表示されます。
- 送信トラフィック、受信トラフィック、送信レート、受信レート、および無線による再送信レートをリアルタイムで監視できます。送信レートと受信レートはトレンドグラフに表示されます。無線タブの数は、FIT APの無線の数と同じです。

Fit AP Listページまたは**fit AP details**ページから**Fit AP Monitoring**機能にアクセスできます。次の手順では、例として**Fit AP List**ページを使用します。

FIT APをリアルタイムで監視するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Fit APs**を選択します。

   Fit AP Listページには、すべてのFIT APが表示されます。
3. FIT APの**Operation**アイコン をクリックします。
4. メニューからMonitorを選択します。

   AP Monitorダイアログボックスが開きます。
5. APタブをクリックします。

次の情報が表示されます。

- **AP**: FIT APの名前とシリアル番号。
- **CPU and Memory Usage Trend graph**: 最後の150秒間のFIT APのCPUおよびメモリー使用率のトレンド。x座標は時間を表し、y座標はCPUおよびメモリー使用率を表します。
- **CPU Used(%)**: 該当するAPの現在のCPU使用率。
- **Memory Used(%)**: 取り付けたAPの現在のメモリー使用率。
- **AP Temperature(°C)**: FIT APの現在の温度。
- Online Clients: FIT APに関連付けられているクライアントの数。
- **Associated Clients**: クライアントとFIT AP間で成功したアソシエーションの数。
- **Associated Failures**: クライアントとFIT AP間で失敗したアソシエーションの数。
- **Re-associated Clients**: クライアントとFIT AP間の再アソシエーションの数。Denied **Registered Clients**: クライアントとFIT AP間で拒否されたアソシエーションの数。
- **Exceptional Deauthenticated Clients**: クライアントとFIT AP間の例外的なアソシエーション解除の数。

6. **Radio**タブをクリックします。

Radioタブの名前は、FIT APの無線IDに対応します。たとえば、IDが1の無線のリアルタイムモニタリング情報を照会するには、Radio 1タブをクリックします。

レートの単位は、レートの値によって変わります。

- **AP**: FIT APの名前とシリアル番号。
- **Transmission and Reception Rate Trend**: グラフ過去150秒間の無線の送信レートと受信レートのトレンド。x座標は時間を表し、y座標は送信レートと受信レートを表します。
- **Transmitted(Bytes)**: 無線によって送信された合計トラフィック。
- **Tx Speed**: 無線の現在の送信レート。
- **Received(Bytes)**: 無線で受信された合計トラフィック。
- **Rx Speed**: 無線の現在の受信レート。
- **Tx Retry Rate(%)**: 無線によって送信された合計トラフィックに対する再送信トラフィックの割合(%)。

7. **Close**をクリックします。

FIT AP履歴情報の表示

この機能を使用すると、過去1時間、過去1日、過去1週間、過去1か月、またはユーザー定義の時間におけるオンラインクライアントの数、レート、トラフィック、アソシエーション、および接続の履歴情報を表示できます。

- オンラインクライアント数統計情報の場合は、オンラインクライアント数のトレンドグラフ、ピークおよび平均オンラインクライアント、および統計収集時間内のオンラインクライアントを表示できます。
- レート統計情報では、送受信レートのトレンドグラフ、ピーク送信レート、ピーク受信レート、平均送信レート、平均受信レート、および指定した時間範囲の送受信レートを表示できます。
- トラフィック統計情報では、統計情報収集の開始時刻と終了時刻、送信トラフィック、受信トラフィック、および合計トラフィックを表示できます。
- アソシエーション統計情報では、アクセス要求、アクセス応答、成功したログイン、異常なログオフ、アソシエーションの成功率、関連するブロッキング率、およびドロップ率を表示できます。
- 接続統計情報では、クライアントのログオフ時間、リカバリ時間、およびログオフ時間を表示できます。

FIT AP LISTページまたはFIT AP detailsページから、fit AP history informationを表示できます。次の手順では、例としてFIT AP Listページを使用します。

Fit AP履歴情報を表示する手順は、次のとおりです。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Fit APs**を選択します。

   Fit AP Listページには、全てのFIT APが表示されます。
3. FIT APの**Operation**アイコン をクリックします。
4. メニューから履歴情報を選択します。

   履歴情報ダイアログボックスが表示されます。
5. 統計タイプを選択します。オプションは次のとおりです。
   - **Online clients**
   - **Rate**
   - **Traffic**
   - **Association**
   - **Connectivity**
6. 時間範囲を選択します。オプションは次のとおりです。
   - **1h**
   - **1d**
   - **1w**

- **1m**
- **1y**
- **Custom**

7. 表示される**Custom**ウィンドウで、開始時間と終了時間を入力するか、**Start Time/End Time**の横のフィールドをクリックして、表示されるカレンダーから開始時間/終了時間をYYYY-MM-DD hh:mm形式で選択します。終了時間は開始時間より後である必要があります。

指定した時間範囲の統計情報が表示されます。

Online Clients Statistics

Online Clientsを選択すると、次の情報が表示されます。

- **Online Client Trend graph**: データ収集時間内にFIT APのオンラインクライアントのトレンド。x座標は時間を表し、y座標はクライアントの送信と数を表します。
- **Peak Number of Online Clients**: 統計情報収集時間範囲にFIT APの最大クライアント数。
- **Average Online Clients**: 統計収集の時間範囲にFIT APの平均クライアント数。

Client Details

- **Time**: 統計情報が収集される時刻。形式はYYYY-MM-DD hh:mm:ssです。
- **Clients**: 統計情報収集の時間範囲にFIT APに関連付けられているオンラインクライアントの数。

Rate Statistics

レートの単位は、レートの値によって変わります。**Rate**を選択すると、次の情報が表示されます。

- **Transmission and Reception Rate Trend graph**: データ収集時間範囲内のFIT APの送信および受信率のトレンド。x座標は時間を表し、y座標は送信および受信率を表します。
- **Peak Transmission Rate(bps)**: 統計情報収集時間範囲にFIT APの最大送信レート。データが変更されると、測定単位も自動的に変更されます。
- **Peak Reception Rate(bps)**: 統計情報収集時間範囲にFIT APの最大受信レート。測定単位はデータの変更に応じて自動的に変更されます。
- **Average Transmission Rate(bps)**: 統計情報収集時間範囲にFIT APの平均送信レート。データが変更されると、測定単位も自動的に変更されます。
- **Average Reception Rate(bps)**: 統計情報収集時間範囲にFIT APの平均受信レート。データが変更されると、測定単位も自動的に変更されます。

Rate Details

- **Time**: 統計情報が収集される時刻。形式はYYYY-MM-DD hh:mm:ssです。
- **Transmission Rate(bps)**: 指定した時間のFIT APの伝送レート。データが変更されると、測定単位も自動的に変更されます。
- **Reception Rate(bps)**: 指定した時間のFIT APの受信レート。測定単位は、データの変更に応じて自動的に変更されます。

Traffic Statistics

trafficの単位は、送受信されるトラフィックの量によって変化します。

trafficを選択すると、次の情報が表示されます。

- **Start Time**: 統計情報収集の開始時刻。形式はYYYY-MM-DD hh:mm:ssです。
- **End Time**: 統計情報収集の終了時刻。形式はYYYY-MM-DD hh:mm:ssです。
- Transmitted Traffic(MB): 指定した時間範囲内にFIT APによって送信された合計トラフィック。測定単位は、データの変更に応じて自動的に変更されます。
- **Received Traffic(MB)**: 指定した時間範囲内にFIT APによって受信された合計トラフィック。測定単位は、データの変更に応じて自動的に変更されます。

- **Total Traffic(B)**: 指定された時間範囲内にFIT APによって送受信されたトラフィックの合計。この値は統計に基づいて計算され、実際の値とは若干異なる場合があります。測定単位はデータの変更に応じて自動的に変更されます。

Association Statistics

Associationを選択すると、次の情報が表示されます。

- **Access Requests**: 指定された時間範囲内にFIT APが受信したアソシエーション要求の数。
- **Response Requests**: 指定された時間範囲内にFIT APによって送信されたアソシエーション応答の数。
- **Successful Logins**: 指定された時間範囲内で成功したアソシエーションの数。
- **Abnormal Logoffs**: 指定された時間内に正常に関連付けられたクライアントの異常なオフライン数。
- **Association Success Rate**: 指定された時間範囲内で、FIT APによって送信されたアソシエーション要求の数に対するクライアントのアソシエーションの成功数(パーセンテージ)。
- **Relevant Blocking Rate**: 指定された時間範囲内の成功したアソシエーションの数に対するFIT AP リソースの不足が原因で失敗したクライアントのアソシエーションの数のパーセンテージ。
- **Dropping Rate**: 指定した時間範囲内のクライアントの正常なアソシエーション数に対する異常オフライン数の割合(%)。

Connectivity Statistics

Connectivityを選択すると、次の情報が表示されます。

- **Logoff Tim**e: FIT APのオフライン時間(YYYY-MM-DD hh:mm:ss形式)。
- **Recovery Time**: FIT APが再びオンラインになる時刻。形式はYYYY-MM-DD hh:mm:ssです。
- **Logoff Duration**: FIT APのオフライン期間(YYYY-MM-DD hh:mm:ssの形式)。

8. **Close**をクリックします。

FIT APに関連付けられたクライアントの表示

FIT APに関連付けられたクライアントは、**Fit AP List**ページから表示できます。FIT APに関連付けられたクライアントを表示するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、WLAN Manager > Resource Management>Fit APsを選択します。

   Fit AP Listページには、全てのFIT APが表示されます。
3. FIT APのTotal Clientsリンクをクリックします。

クライアントリストには、現在のFIT APに関連付けられているすべてのオンラインクライアントが表示されます。クライアントリストの詳細は、「クライアントリストの表示」を参照してください。

FIT APの無線パラメーターの表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Fit APs**を選択します。

   Fit AP Listページには、全てのFIT APが表示されます。
3. FIT APのデバイスラベルをクリックします。

fit APの詳細ページには、現在のfit APの基本情報、クライアント情報、および無線情報が表示されます。

4. Radios領域で、ターゲット無線のIDをクリックします。

   Radio Informationダイアログボックスが開きます。

   Radio Information

   - **Radio ID**: 無線のID。
   - **Radio Type**: 無線のタイプ。オプションは次のとおりです。

     802.11a
     -802.11b
     -802.11g
     -802.1gn
     -802.11an
     -802.11ac
   - **Admin Status**: 無線の管理状態。オプションは**Up**および**Down**です。
   - **Operation Status**: 無線の動作状態。オプションは**Up**および**Down**です。
   - **Preamble Type**: Fit APのプリアンブルタイプ。オプションは次のとおりです。
     - **Short**: FIT APは、ショートプリアンブルまたはロングプリアンブルのいずれかを使用してフレームを送信します。
     - **Long**: FIT APは、長いプリアンブルを含むフレームだけを送信します。**802.11b、802.11g、**または**802.11gn**無線タイプを選択した場合は、このオプションを設定できます。
   - **Channels in Use**: 無線の現用チャネル。値の範囲は無線タイプによって異なります。**Auto**を選択した場合、Fit APはアイドルチャネルを現用チャネルとして選択します。
   - **Max Transmission Power(dBm)**: 無線の最大送信電力。
   - **Current Transmission Power(dBm)**: 無線の現在の送信電力。
   - **Radio Policy**: 無線にバインドされた無線ポリシー。
   - **MP Policy**: 無線にバインドされたMPポリシー。
   - **Mesh Profile ID**:メッシュプロファイルにバインドされている無線のID。このオプションは、無線がどのメッシュプロファイルにもバインドされていない場合は表示されません。
   - **Channel Calibration Lock down**: 無線の現在の動作チャネルがロックされています。オプションは次のとおりです。
     - **Yes**: FIT APが現在の作業チャネルをロックしており、その作業チャネルはACによって自動的に調整されません。
     - **No**: 無線の動作チャネルはACによって自動的に調整されます。
   - **Power Calibration Lock down**: 無線の現在のロック送信電力。オプションは次のとおりです。
     - **Yes**: FIT APは現在の送信電力をロックしており、その送信電力はACによって自動的に調整されません。
     - **No**: 無線の送信電力はACによって自動的に調整されます。
   - **WMM Enable**: WMMがイネーブルかどうかを示します。

     WMMは、優先度の高いパケットを優先的に送信するように設計されたワイヤレスQoSプロトコルであり、ワイヤレスネットワーク内の音声およびビデオアプリケーションに対してより優れたQoSサービスを保証します。WMMプロトコルは、802.11nプロトコルの基盤です。関連付けられた802.11nクライアントが通信するには、無線が802.11 anまたは802.11 gn無線モードで動作しているときにWMMを有効にします。
   - **CAC ChannelUtilization(%)**: チャネル使用率ベースのアドミッションポリシー、または単位時間内の有効時間に対する、受け入れられたAC-VOおよびAC-VIトラフィックのメディア時間の割

合。有効時間は、データが送信された合計時間です。このオプションは、CACポリシーが**ChannelUtilization**に設定されている場合に表示されます。

- **CAC UserNumber**: ネットワークへのアクセスを許可されるクライアントの最大数。このオプションは、CACポリシーが**UserNumber**に設定されている場合に表示されます。
- **Service Policy**: 無線にバインドされたサービスポリシーのSSID。

5. **Close**をクリックします。

FIT APの無線パラメーターの変更

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Fit AP**sを選択します。

   Fit AP Listページには、全てのFIT APが表示されます。
3. FIT APのデバイスラベルをクリックします。
4. **Radios**領域で、無線の**Modify**アイコンをクリックします。無線パラメーターを変更するためのページが開きます。
5. 必要に応じて、次の無線パラメーターを変更します。
   - **Radio ID**: このフィールドは変更できません。
   - **Radio Type**: 無線タイプを選択します。オプションは次のとおりです。

     802.11a
     802.11b
     802.11g
     802.11gn
     802.11an
     802.11ac

     無線が有効なメッシュプロファイルにバインドされている場合、無線のタイプは変更できません。
   - **Admin Status**: 無線の管理状態を選択します。オプションはUpおよびDownです。
   - **Channels in Use**: 無線の動作チャネルを選択します。

     値の範囲は無線タイプによって異なります。Autoを選択した場合、FIT APはチャネル品質を評価し、最適なチャネルを作業チャネルとして選択します。このシナリオでは、FIT APをメッシュプロファイルにバインドできないため、Mesh Profile IDリストからNoneを選択する必要があります。

     注:

     メッシュプロファイルとサービスポリシーの両方を無線にバインドしている場合は、チャネルモードをautoに設定できません。

   - **Max Transmission Power(dBm):** 無線の最大送信電力を入力します。
   - **Current Transmission Power(dBm)**: 無線の現在の送信電力を入力します。
   - **Radio Policy**: 無線にバインドする無線ポリシーを選択します。オプションは、WSM内のすべての既存の無線ポリシーです。
   - **MP Policy**: 無線にバインドするMPポリシーを選択します。オプションは、WSM内の既存のすべてのMPポリシーです。
   - **Mesh Profile ID**: 無線にバインドするメッシュプロファイルを選択します。オプションは、None

とWSM内の既存のすべてのメッシュプロファイルです。

注:

モニターモードまたはハイブリッドモードでは、FAT APのメッシュプロファイルを指定できません。

- **Dot11n Channelband**: Dot11nチャネルバンドを選択します。オプションは20 MHzおよび40 MHzです。このパラメーターは、無線タイプが802.11 anまたは802.11gnの場合にのみ使用できます。
- **A-MPDU Enable**: A-MPDUをイネーブルまたはディセーブルにします。このオプションは、無線タイプが802.11 anまたは802.11gnの場合にだけ使用できます。
- **A-MSDU Enable**: A-MSDUをイネーブルまたはディセーブルにします。このオプションは、無線タイプが802.11 anまたは802.11gnの場合にだけ使用できます。
- **Client Dot11n only**: このオプションを選択すると、FIT APがdot11クライアントだけに関連付けられるように制限されます。このオプションは、無線タイプが802.11 anまたは802.11gnの場合にだけ使用できます。
- **Short GI Enable**: ショートGIをイネーブルまたはディセーブルにします。このオプションは、無線タイプが**802.11an**または**802.11gn**の場合にだけ表示されます。

注:

ショートGIをイネーブルにする前に、必須MCSセットを設定します。

- **Channel Calibration Lock down**: 無線の動作チャネルをロックまたはロックしません。オプションは**No**と**Yes**です。

  Yesを選択すると、FIT APは現在の作業チャネルをロックし、その作業チャネルはACによって自動的に調整されません。

  Noを選択すると、無線の動作チャネルがACによって自動的に調整されます。

  このオプションを設定する前に、FIT APが接続されているACでDFSを有効にします。詳細については、「WLAN RRMの設定」を参照してください。DFSを有効にすると、ACは各APに最適なチャネルをリアルタイムで選択して、同一チャネル干渉および他の無線ソースからの干渉を回避します。
- **Power Calibration Lock down**: 無線の現在の送信電力をロックまたはロックしない。オプションは**Yes**と**No**です。

  Yesを選択すると、Fit APは現在の送信電力をロックし、その送信電力はACによって自動的に調整されません。

  Noを選択すると、無線の送信電力はACによって自動的に調整されます。

  このオプションを設定する前に、Fit APが接続されているACでTPCを有効にします。詳細については、「RRMキャリブレーショングループの設定」を参照してください。TPCを有効にすると、ACは各Fit APの送信電力を動的に調整します。
- **WMM Enable**: 無線のWMMを有効または無効にします。

  WMMは、優先度の高いパケットを優先的に送信するように設計されたワイヤレスQoSプロトコルであり、ワイヤレスネットワーク内の音声およびビデオアプリケーションに対してより優れたQoSサービスを保証します。WMMプロトコルは、802.11nプロトコルの基盤です。関連付けられた802.11nクライアントが通信するには、無線が802.11 anまたは802.11 gn無線モードで動作しているときにWMMを有効にします。
- **CAC Policy**: 無線のCACポリシーを選択して、ハイプライオリティアクセスカテゴリ(AC-VOおよびAC-VI)を使用するクライアントの数を制限し、既存のハイプライオリティトラフィックに十分な帯域幅を保証します。オプションは**ChannelUtilization**および**UserNumber**です。**ChannelUtilization**を選択した場合は、**CAC ChannelUtilization**を設定します。

UserNumberを選択した場合は、**CAC UserNumber**を設定します。

- **CAC ChannelUtilization**: ユニット時間内の有効時間に対する、受け入れられたAC-VOおよびAC-VIトラフィックのメディア時間のレートを入力します。有効時間は合計時間です。

  データが送信される間。Fit APは、CACチャネル使用率が最大値に達したときにアソシエートするクライアントの数を制限します。CACポリシーが**ChannelUtilization**に設定されている場合は、このオプションを設定します。

- **CAC UserNumber**: ネットワークへのアクセスが許可されるクライアントの最大数を設定します。CACポリシーが**UserNumber**に設定されている場合は、このオプションを設定します。

- **Service Policy**: 無線にバインドするサービスポリシーを選択します。Service Policy Listには、現在の無線が属するAPのすべてのサービスポリシーが表示されます。

Service Policy List contents

- **SSID**: サービスポリシーのSSID。
- **Encryption Mode**: 暗号化モードを選択します。オプションは**Clear**および**Crypto**です。
- **Hide SSID**: サービスポリシーのビーコンフレームでのSSIDの非表示を有効または無効にします。
- **Authentication Mode**: サービスポリシーの認証モードを選択します。オプションは次のとおりです。
  - **Open System**: 認証を要求するすべてのクライアントが直接認証を通過できるようにします。
  - **Shared Key**: クライアントは、デバイスに設定されているものと同じ共有キーを使用する必要があります。Shared Keyは、暗号スイートとしてWEP40またはWEP104を選択した場合にだけ指定します。
  - **All**: クライアントが必要に応じてオープンシステムモードまたは共有キーモードを使用できるようにします。

オペレーターは、現在の無線にバインドするサービスポリシーを選択できます。

- **Synchronize AC Configuration**: Fit APテンプレート内の設定を、指定したACグループ内のすべてのACに適用します。

  Fit APテンプレートの設定を現在のACだけに適用する場合は、このオプションを選択しないでください。このオプションは、ACが少なくとも1つのACグループに属している場合にのみ使用できます。

- **AC Group**: ACグループを選択します。オプションは、現在のACが属するすべてのACグループです。このオプションは、**Synchronize AC Configuration**が選択されている場合にのみ使用できます。

6. **OK**をクリックします。

   確認ダイアログボックスが表示されます。

7. **OK**をクリックします。

FIT APのメッシュピアMACアドレスの設定

許可されたメッシュピアのMACアドレスは、WDSを実装する各FIT APの無線で設定できます。

メッシュピアMACアドレスリストの表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Fit APs**を選択します。

   Fit AP Listページには、全てのFIT APが表示されます。
3. FIT APのデバイスラベルをクリックします。
4. **Radio Interface**領域でターゲット無線の**Configure Mesh Peer MAC Address**アイコンをクリックして、メッシュピアMACアドレスを設定するページを表示します。

   オペレーターは、**Peer MAC Address List**の現在の無線のネイバーのmesh peer MACアドレスを表示できます。
5. **Back**をクリックして、fit AP detailsページに戻ります。

メッシュピアMACアドレスの追加

1つの無線には最大8つのメッシュピアMACアドレスを設定できます。メッシュピアMACアドレスを追加するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Fit APs**を選択します。

   Fit AP Listページには、全てのFIT APが表示されます。
3. FIT APのデバイスラベルをクリックします。
4. **Radio Interface**領域で、ターゲット無線の**Configure Mesh Peer MAC Address**アイコンをクリックして、メッシュピアMACアドレスを設定するページを開きます。
5. **Peer MAC Address**ボックスに、メッシュピアのMACアドレスをhh:hh:hh:hh:hh:hh:hhの形式で入力します。
6. **Add**をクリックします。
7. **Back**をクリックして、fit AP detailsページに戻ります。

メッシュピアMACアドレスの削除

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management>Fit APs**を選択します。

   Fit AP Listページには、全てのFIT APが表示されます。
3. FIT APのデバイスラベルをクリックします。
4. **Wireless Service Information**タブの**Radio Information**領域で、ターゲット無線の**Configure Mesh Peer MAC Address**アイコンをクリックして、メッシュピアMACアドレスを設定するページを開きます。
5. **Peer MAC Address List**から1つ以上のMACアドレスを選択し、**Delete**をクリックします。

   確認のダイアログボックスが開きます。
6. **OK**をクリックします。

7. **Back**をクリックして、Fit APの詳細ページに戻ります。

X-shareアンテナのパラメーターの変更

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management>Fit APs**を選択します。

   Fit AP Listページには、全てのFIT APが表示されます。
3. FIT APのデバイスラベルをクリックします。
4. **X-Share Antenna**領域で、無線の**Modify**アイコンをクリックします。
5. **Modify X-Share Antenna**ダイアログボックスで、次のパラメーターを設定します。
   - **Antenna ID**: このパラメーターは変更できません。
   - **Attenuation**: 減衰値を入力します。
   - **Description**: アンテナの説明を入力します。
6. **OK**をクリックします。

engineered fit APの管理

エンジニアリングされたFIT APは、インストールされているがデバッグ状態にあるFIT APです。IMCにトラップを送信したり、クライアントにワイヤレスサービスを提供したりすることはできません。

設計されたFIT APを標準FIT APに切り替えることができます。また、その逆も可能です。設計されたFIT APを標準FIT APにバッチで切り替えることができます。

engineered fit APリストの表示

Engineered Fit AP Listページには、IMCで管理されているすべてのエンジニアリングAPに関する情報が表示されます。この情報には、エンジニアリングFIT APのステータス、デバイスラベル、シリアル番号、IPアドレス、MACアドレス、モデル、およびACが含まれます。

設計されたFIT APリストを表示するには、次の手順に従います。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management>Fit APs**を選択します。

   Fit AP Listページには、全てのFIT APが表示されます。
3. **Related Operations**をクリックして、**Engineered Fit AP List**を選択します。

   Engineered Fit AP Listには、すべてのEngineered Fit APが表示されます。

   Engineered Fit AP List
   - **Online Status**: engineered fit APのオンライン状態。
     - **Online** and **Online(Primary)**: engineered fit APは、プライマリACに接続するオンラインFIT APです。
     - **Online(Secondary)**: Engineered Fit APは、セカンダリACに接続するオンラインFIT APです。
     - **Offline**: engineered fit APはオフラインです。
   - **AP Label**: IMCプラットフォーム内のエンジニアリングされたFIT APを識別するデバイスラベル。

     FIT APのデバイスラベルをクリックすると、詳細が表示されます。

- **Serial Number**: engineered fit APのシリアル番号。
- **IP Address**: engineered fit APのIPv4アドレス。
- **MAC Address**: engineered fit APのMACアドレス。
- **Model**: engineered fit APのモデル。
- **AC**: 設計されたFIT APを管理するAC。ACラベルをクリックすると、詳細が表示されます。

Engineered Fit AP Listに十分なエントリーがある場合は、次のナビゲーション支援が表示されます。

- **Next Page**アイコンをクリックして、**Engineered Fit AP List**で次のページに進みます。
- **Last Page**アイコンをクリックして、**Engineered Fit AP List**の最後のページに進みます。
- **Previous Page**アイコンをクリックして、**Engineered Fit AP List**の前のページに戻ります。
- **First Page**アイコンをクリックして、**Engineered Fit AP List**の前にページに戻ります。
- **Engineered Fit AP List**の右上にある8、15、50、100、または200をクリックして、各ページに表示する項目数を指定します。

フィールドごとにFit APリストをソートできます。選択したフィールドでリストをソートするには、列ラベルをクリックします。列ラベルを使用すると、各フィールドに固有のソートオプションを切り替えることができます。

engineered fit APのクエリー

WSMは、基本問合せと拡張問合せを提供します。基本問合せでは、高速検索の唯一の基準としてMACアドレスが使用されます。拡張問合せでは、正確な照合のための様々な問合せ基準が提供されます。

engineered fit APをクエリーするには、次の手順を実行し

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management>Fit APs**を選択します。

   Fit AP Listページには、全てのFIT APが表示されます。
3. **Related Operations**をクリックし、**Engineered Fit AP List**を選択します。Engineered Fit AP Listには、すべてのEngineered Fit APが表示されます。
4. 基本問合せまたは拡張問合せを実行します。

Basic query

a. ページ右側の**Query**フィールドに、MACアドレスを入力します。

b. **Query**アイコンをクリックします。

   Engineered Fit AP Listに、基準に一致するすべてのFIT APが表示されます。

c. Queryフィールドをクリアして、**Query**アイコンをクリックします。**Engineered Fit AP List**には、全てのFIT APが表示されます。

Advanced query

d. Queryフィールドの右にある**Expand**アイコンをクリックします。

e. 次の問合せ基準を1つ以上指定します。

- **AP Label**: 設計されたFIT APのデバイスラベルを入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
- **AP Name**: 設計FIT APの名前を入力します。WSMでは、このフィールドのファジーマッチがサポートされています。
- **Serial Number**: 設計されたFIT APのシリアル番号を入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。

- **Online Status**: 設計されたFIT APのオンラインステータスを選択します。オプションは次のとおりです。
  - Unlimited
  - Online
  - Online (Primary)
  - Online (Secondary)
  - Offline

  Onlineを選択すると、**Primary**と**Secondary**を含むすべてのオンラインのengineered fit APsが表示されます。

  空のフィールドや**Unlimited**に設定されたフィールドは、クエリーの抽出条件にはなりません。

f. **Query**.をクリックします。

Device Listには、クエリー基準に一致するすべてのエンジニアリングされたFIT APが表示されます。

g. **Reset**をクリックしてクエリー基準をクリアし、設計されたすべてのFIT APを表示します。

FIT APの切り替え

この機能を使用すると、標準FIT APと設計FIT APの間で切り替えるか、または標準FIT APを設計FIT APにバッチで切り替えることができます。**Switching Fit APs**機能には、「FIT AP詳細」ページからアクセスできます。

Switch between a normal fit AP and an engineered fit AP

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management>Fit APs**を選択します。

   Fit AP Listページには、全てのFIT APが表示されます。
3. fit APのデバイスラベルをクリックします。

   fit APの詳細ページが開きます。
4. **Set as Engineered Fit AP**アイコンまたはページの右側にある**Action**メニューにある**Set as Normal Fit AP**アイコンをクリックします。
   - **Set As Engineered Fit AP**アイコンがページの右側の**Action**領域に表示されている場合は、現在のFIT APを設計されたFIT APに切り替えることができます。
   - ページの右側にある**Action**領域に**Set As Normal Fit AP**アイコンが表示されている場合は、現在の**Fit APを**Normal Fit AP**に切り替えることができます。
   - **Set As Engineered Fit AP**アイコンまたは**Set As Normal Fit AP**アイコンがページの右側の**Action**領域に表示されない場合は、現在のFIT APを切り替えることはできません。

Switching engineered fit APs to normal fit APs in batches

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management>Fit APs**を選択します。

   Fit AP Listページには、全てのFIT APが表示されます。
3. **Related Operations**をクリックし、**Engineered Fit AP List**を選択します。

   Engineered Fit AP Listページには、すべての**Engineered Fit AP**が表示されます。
4. 目的の**engineered fit AP**を選択します。
5. **Set as Normal Fit AP**をクリックします。

IoT APのサーバー設定の構成

WSMを使用すると、オペレーターはIoT APのサーバー設定を構成して、IoTモジュールによって監視されたデータパケットをサーバーに送信できる。

IoT APのサーバー設定を構成するには、以下の手順に従ってください。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management>Fit APs**を選択します。

   Fit AP Listページには、全てのFIT APが表示されます。
3. FIT APのデバイスラベルをクリックします。
4. ページの右側にある**Action**メニューの**Server Settings**アイコン  をクリックします。

   Server Settingsダイアログボックスが開きます。
5. サーバーのIPアドレスとポート番号を設定します。
6. OKをクリックします。

FIT APの拡張プロパティの設定

WSMを使用すると、オペレーターはFIT APのプロパティ(拡張プロパティと呼ばれます)を定義できます。オペレーターは、FIT APの拡張プロパティを定義した後でのみ、拡張プロパティを変更およびインポートできます。

FIT APの拡張プロパティを定義する

オペレーターは、WSM(**<Installation path>/client/conf/wlan/extendproperty.xml**)で提供される設定ファイルを編集して、FIT APの拡張プロパティを定義できます。1つのFIT APに対して最大10個の拡張プロパティを定義できます。

拡張プロパティを定義するには:

1. IMCがインストールされているサーバーにログインします。
2. **<installation path>/client/conf/wlan**にある**extendproperty.xml**ファイルを開きます。

   次の情報が表示されます。

   ```
   <?xml version="1.0" encoding="GB2312"?>
   <properties>
   <!-- propertyitem id="1" propertyname="Hotspot Type" export="true" / -->
   <!-- propertyitem id="2" propertyname="Hotspot AP Code" export="true"/ -->
   </property>
   ```
3. **extendproperty.xml**ファイルを編集します。

   ファイルには、拡張プロパティを定義するためのサンプルが含まれています。演算子は、文のコメント文字を削除した後でサンプルを使用できます。たとえば、サンプル文を次のように変更します:

   ```
   <!-- propertyitem id="1" propertyname="Hotspot Type" export="true" / -->
   ```

   から

   ```
   <propertyitem id="1" propertyname="Hotspot Type" export="true" />
   ```

   ここで

   - **propertyitem id**: プロパティの番号。システムはプロパティをIMCに表示します。
     プロパティの番号に従います。番号は連続している必要があり、重複することはできません。

- **propertyname**: IMCに表示されるプロパティの名前。
- **export**: すべてのFIT APがエクスポートされるときにプロパティをエクスポートするかどうか。オプションはtrueです。
  偽です
  - **true**: プロパティをエクスポートできます。
  - **false**: プロパティをエクスポートできません。

4. **extendproperty.xml**ファイルを保存して閉じます。
5. 次のいずれかの方法で手順を続行します。
   - **Intelligent Deployment Monitoring Agent**で、**Monitor**タブのIMCを再起動します。
   - **Process**タブで、**jserver**プロセスを再起動します。
6. IMCにログインします。
7. **Service**タブをクリックします。
8. ナビゲーションツリーから、**WLAN Manager > Resource Management>Fit APs**を選択します。

   Fit AP Listページには、全てのFIT APが表示されます。
9. ターゲットFIT APのデバイスラベルをクリックします。
   定義されている拡張プロパティを表示するには、ワイヤレス情報タブをクリックします。

FIT APの拡張プロパティを修正する

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management>Fit APs**を選択します。

   Fit AP Listページには、全てのFIT APが表示されます。
3. FIT APのデバイスラベルをクリックします。
4. 拡張プロパティの**Modify**アイコンをクリックします。

   Modify Extended Propertiesページには、定義されているすべての拡張プロパティが表示されます。
5. **extended properties**を修正します。
6. OKをクリックします。

拡張プロパティの拡張プロパティのインポート

この機能を使用すると、FIT APの拡張プロパティをバッチでインポートできます。WSMでは、拡張プロパティのIPアドレスがキーワードとして使用されます.csvファイルのみがサポートされており、.csvファイルの各行の列数は同じである必要があります。WSMでは、最初の行が列名とみなされ、この行はインポートされません。

拡張プロパティをバッチでインポートするには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Fit APs**を選択します。

   Fit AP Listページには、全てのFIT APが表示されます。
3. **Import**をクリックします。
4. **Browse**をクリックしてファイルを選択するか、インポートするファイルのURLを入力します。
5. **Next**をクリックします。

Import Informationページが開きます。

6. 拡張プロパティは、インポートしたファイルから読み込むことも、手動で指定することもできます。ファイル内の指定した列番号を拡張プロパティとして選択するか、**Not select in the file**を選択して拡張プロパティを入力します。
7. **Preview**をクリックします。

   ダイアログボックスが開きます。オペレーターはインポートされた情報をプレビューできます。**Not Imported**拡張プロパティは表示されません。
8. **Cancel**をクリックして、ダイアログボックスを閉じます。
9. OKをクリックします。

Import Resultには、各FIT APの拡張プロパティの読み込み結果が表示されます。

一般的な管理機能

ping

この機能を使用すると、IMCサーバーからの管理対象Fit APの到達可能性をテストできます。選

択したFit APをFit AP Listページからpingするには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Fit APs**を選択します。

   Fit AP Listページには、全てのFIT APが表示されます。
3. FIT APの**Operation**アイコン･･･をクリックします。
4. メニューから**Ping**を選択します。

   Pingダイアログボックスが開きます。
5. **Buffer Size**リストから、pingパケットのサイズ(バイト単位)を選択します。
6. **Number**リストから、選択したFIT APにIMCが送信するpingパケットの数を選択します。
7. **OK**をクリックして変更を受け入れ、pingテストを開始します。

   Pingダイアログボックスでpingテストの結果を確認します。
8. **OK**をクリックします。

traceroute

この機能を使用すると、IMCサーバーからのManaged Fit APの到達可能性をテストし、接続の問題をトラブルシューティングして特定できます。

Fit AP Listページから選択したFit APに対してtracerouteを実行するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management>Fit APs**を選択します。

   Fit AP Listページには、全てのFIT APが表示されます。
3. FIT APの**Operation**アイコン･･をクリックします。
4. メニューから**TraceRoute**を選択します。

Tracerouteダイアログボックスが開きます。tracerouteの結果を表示します。

5. **OK**をクリックします。

クライアントの管理

WSMを使用すると、オンラインクライアント、クライアントオンライン履歴、およびクライアント情報を管理できます。

オンラインクライアント管理

WSMは、WLANに接続されているすべてのオンラインクライアントをクライアントリストに表示して、管理を容易にします。これには次のものが含まれます。

- クエリークライアント
- 詳細なクライアント情報の表示
- クライアント情報のエクスポート
- クライアント情報の変更
- リアルタイムのクライアント監視情報およびクライアント履歴情報を表示するロケーションビューまたはデフォルトマップを使用してクライアントを検索することもできます。

クライアントリストの表示

クライアントリストページには、WSMのすべてのオンラインクライアントに関する情報が表示されます。クライアントに関する次の情報を表示できます。

- Status
- Radio type
- Signal strength
- Endpoint identification
- MAC address
- User name
- IP address
- SSID
- Channel
- Rx rate
- Total traffic
- Online duration
- AP

クライアントリストを表示するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Clients**を選択します。

   Client Listページにすべてのクライアントが表示されます。

   Client List

   - **Client Status**: クライアントの現在のステータス。このアイコンはクライアントが正常に関連付けられたことを示し、このアイコンはクライアントが正常に認証されたことを示します。
   - **Radio Type**: アクセスAPの無線タイプ。表21に、無線タイプのアイコンを示します。

表21 アイコンで表される無線の種類

アイコン	無線の種類
a	802.11a
b	802.11b
g	802.11g
bg	802.11bg
at	802.11at
an	802.11an
ac	802.11ac
gn	802.11gn
n	802.11n(2.4GHz) 802.11bgn 802.11n 802.11n(5GHz)

- **Signal Strength**: クライアントの信号強度。表22に、アイコンで表された信号強度とSNRを示します。

  表22 アイコンで表された信号強度とSNR

Icon	Signal strength	SNR
	Signal strength > –57 dBm	SNR > 40 dB
	–67 dBm < signal strength ≤ –57 dBm	32 dB < SNR ≤ 40 dB
	–71 dBm < signal strength ≤ –67 dBm	25 dB < SNR ≤ 32 dB
	–81 dBm < signal strength ≤ –71 dBm	15 dB < SNR ≤ 25 dB
	Signal strength < –81 dBm	10 dB < SNR ≤ 15 dB
	None	SNR ≤ 10 dB

- **Endpoint Identification**: エンドポイントタイプ、ベンダー、およびOSを含むエンドポイント識別情報。エンドポイント識別の詳細は、「ネットワーク管理の構成」を参照してください。
- **MAC Address**: クライアントのMACアドレス。
- **Username**: クライアントがワイヤレスネットワークにアクセスするために使用するユーザー名。次のいずれの条件も満たさない場合、このフィールドは空白になります。
  - **ComwareベースのFAT AP/FIT AP**を介してオンラインになるクライアントの場合、802.1X認証がイネーブルになっていると、ユーザー名(ACまたはFAT APから取得)が表示されます。このようなユーザー名は変更できません。
  - WSMがUAMと統合されている場合、またはユーザー情報がWSMに追加されている場合は、ユーザー名が表示されます。このようなユーザー名は、クライアント情報の変更ページで変更できます。
- **IP Address**: クライアントのIPアドレス。
  - **ComwareベースのfatAPまたはfit AP**: クライアントがiNodeを使用してワイヤレスネットワークにアクセスする場合、またはアクセスfat AP/ACでIPスヌーピングが有効になっている場合、IPアドレスは使用可能です。クライアントのIPアドレスが使用できない場合、このフィールドには0.0.0.0と表示されます。

- **SSID**: クライアントがネットワークにアクセスするために使用するSSID名。
- **Channel**: クライアントによって使用されるチャネル。
- **Rx Rate(Mbps)**: クライアントの現在の受信レート。
- **Total Traffic(KB)**: クライアントが受信および送信したトラフィックの合計量。
  受信トラフィックと送信トラフィックの詳細な値を表示するには、**Total Traffic**をクリックします。
- **Online Duration**: クライアントの最新のオンライン期間。
- **AP**: クライアントに関連付けられたAP。
  - **Fit AP**: [management AC device label->[fit AP device label]と表示されます。該当するリンクをクリックすると、詳細なfit AP情報が表示されます。
  - **Fat AP**: Fat APデバイスラベルが表示されます。対応するリンクをクリックすると、Fat APの詳細情報が表示されます。

- **Operation**: **Operation**アイコン ▪▪▪ は、関連付けられたクライアントの操作タスクへのリンクを表示します。

– **ComwareのFAT APまたはFIT AP**: クライアント情報の変更、リアルタイム監視情報と履歴情報の表示、トラブルシューティングの実行、RF Pingの実行、クライアントトラフィック分析の表示、および**Operation**メニュー ▪▪▪ のLocation Viewまたはデフォルトマップを使用したクライアントの検索を行います。

Client Listに十分な数のエントリーがある場合は、次のナビゲーションツールが表示されます。

- **Next Page**アイコンをクリックして、**Client List**でページを進めます。
- **Last Page**アイコンをクリックして、**Client List**の最後にページを移動します。
- **Previous Page**アイコンをクリックして、**Client List**で前のページに戻ります。
- **First Page**アイコンをクリックして、**Client List**の前にページを戻します。

クライアントリストの右上にある**8**、**15**、**50**、**100**、または**200**をクリックして、各ページに表示する項目数を指定します。

Client Listは、**Operation**フィールド以外のすべてのフィールドでソートできます。列ラベルをクリックすると、選択したフィールドでリストをソートできます。列ラベルを使用すると、各フィールドに固有の様々なソートオプションを切り替えることができます。

クライアント リストのカスタマイズ

Client Listをカスタマイズして、**Online Duration**列などの列を削除できます。**Client Status**、**Radio Type**、**Signal Strength**および**Operation**列以外のすべての列をカスタマイズできます。デフォルトでは、すべての列がカスタマイズされます。

client listをカスタマイズするには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Clients**を選択します。
   Clientsページにすべてのクライアントが表示されます。
3. **Custom Columns**をクリックします。
4. 必要な列をカスタマイズします。
5. **Default**をクリックします。

すべての列が選択されます。

6. OKをクリックします。

カスタマイズされた列のみが**client list**に表示されます。

クライアントのクエリー

WSMには、基本問合せと拡張問合せが用意されています。基本問合せ基準には、迅速な検索のためのキーパラメーターがいくつか含まれています。拡張問合せには、正確な照合のための様々な問合せ基準が用意されています。

クライアントにクエリーを実行するには

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Clients**を選択します。

   Clientsページにすべてのクライアントが表示されます。
3. 基本的なクエリーを実行します。
   a. クライアントのMACアドレスを入力します。WSMは、このフィールドのファジーマッチングをサポートしています。
   b. **Query**アイコンをクリックします。**Client List**に、問合せ基準に一致するすべてのクライアントが表示されます。
   c. **Query**フィールドをクリアし、**Query**アイコンをクリックしてすべてのクライアントを表示します。
4. 高度なクエリーを実行します。
   a. **Query**フィールドの横にある**Expand**アイコンをクリックして**Query**領域を拡張します。再度クリックすると**Query**領域が非表示になります。
   b. 次の問合せ基準を1つ以上指定します。
   - **Username**:クライアントがワイヤレスネットワークにアクセスするために使用するユーザー名を入力します。WSMは、このフィールドのファジーマッチングをサポートします。
   - **MAC Address**:クライアントのMACアドレスを入力します。WSMは、このフィールドのファジーマッチングをサポートします。
   - **Device Type**:クライアントのデバイスタイプを選択します。オプションは次のとおりです。
     - **Unlimited**
     - **AC**
     - **FIT AP**
     - **FAT AP**
   - **Device Label**: クライアントのデバイスラベルを入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。**Device Type**がUnlimitedに設定されている場合、**Device Label**は問合せ基準として機能しません。
   - **Radio Type**: アクセスAPの無線タイプを選択します。オプションは次のとおりです。
     - **All**
     - **802.11a**
     - **802.11b**
     - **802.11g**
     - **802.11bg**
     - **802.11at**
     - **802.11an**
     - **802.11gn**
     - **802.11ac**
     - **802.11n(2.4GHz)**
     - **802.11n**

- **802.11n(5GHz)**
- **802.11ag**
- **Wired**

- **Channel**: クライアントが使用するチャネルを入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
- **SSID**: クライアントがネットワークに接続するために使用するSSID名を入力します。WSMは、このフィールドのファジーマッチングをサポートしています。
- **IP Address**: クライアントのIPアドレスを入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
- **Location**: クライアントのロケーションビュー名を入力または選択します。WSMでは、このフィールドのファジーマッチングがサポートされています。

  空のフィールドや**Unlimited**に設定されたフィールドは、クエリーの抽出条件にはなりません。

c. **Query**をクリックすると、クエリー条件に一致するすべてのクライアントがクライアントリストに表示されます。

d. **Reset**をクリックして、クエリー基準をクリアし、すべてのクライアントを表示します。

クライアントのエクスポート

この関数を使用すると、.csvファイル内の特定の基準に一致するクライアントをエクスポートできます。クライアントをエクスポートするには、次の手順に従います:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Clients**を選択します。

   Clientsページにすべてのクライアントが表示されます。
3. **Export**をクリックします。
4. **Export Content**ダイアログボックスで、必要に応じて**Export Custom Columns**または**Export Custom Columns**を選択します。

   Download Exported Template Fileのダウンロードウィンドウが開きます。
5. **Export Result**をクリックして、エクスポートされた.csvファイルをダウンロードします。

クライアント情報の変更

この関数を使用すると、クライアントの基本情報を変更できます。クライアント情報を変更するには、次の手順を実行します:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Clients**を選択します。

   Clientsページにすべてのクライアントが表示されます。
3. クライアントの**Operation**アイコン ··· をクリックします。
4. メニューから**Modify Client Info**を選択します。

オペレーターは、必要に応じてクライアント情報を変更できます。クライアント情報の変更の詳細は、「クライアント情報の変更」を参照してください。

ターゲットクライアントに情報がない場合は、**Modify Client Info**を選択し、必要に応じて基本的なクライアント情報を追加します。クライアント情報の追加の詳細は、「クライアント情報の変更」を参照してください。

クライアントの検索

WSMを使用すると、クライアントリストでクライアントを検索できます。結果はロケーションビュー トポロジーに表示されます。クライアントを検索するには、次の手順を実行します:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Clients**を選択します。
   Clientsページにすべてのクライアントが表示されます。
3. クライアントの**Operation**アイコン ⋯ をクリックします。
4. メニューから、**Locate to Topology**を選択します。

ロケーションビュー トポロジー内でクライアントがハイライト表示されます。クライアントを検索する前に、関連する構成を実行してください。詳細は、「ワイヤレス検索の管理」を参照してください。

マッピングするクライアントの検索

この関数を使用すると、デフォルトマップへのクライアントをすぐに検索できます。

マッピングするクライアントを検索するには、次の手順を実行します:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Clients**を選択します。
   Clientsページにすべてのクライアントが表示されます。
3. クライアントの**Operation**アイコン ⋯ をクリックします。
4. メニューから、**Locate to GIS Map**を選択します。

クライアントの場所がデフォルトマップ上にハイライト表示されます。マッピングするクライアントを検索する前に、関連する構成を実行してください。詳細は、「GISの検索」を参照してください。

クライアントのリアルタイム監視の実行

WSMは、クライアントリスト上のオンラインクライアントにリアルタイム監視機能を提供します。表23に、クライアントのリアルタイム監視情報を示します。

表23クライアントのリアルタイム監視情報

アクセスAP	リアルタイム監視情報
ComwareベースのFAT AP/FIT AP	• 送受信レートトレンドグラフ • 信号強度トレンドグラフ • 受信ノイズトレンドグラフ • 信号ノイズ比トレンドグラフ • 受信トラフィック • Rx速度 • 送信トラフィック • Tx速度 • Txリトライバイト • Txリトライバイト • 信号強度(dBm) • 受信ノイズ • オンライン時間 • 信号ノイズ比

クライアントリアルタイムモニタリングページには、最後の150秒間のモニタリング情報が表示されます。この情報は5秒ごとに更新されます。

クライアントのリアルタイム監視を実行する手順は、次のとおりです。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Clients**を選択します。

   Clientsページにすべてのクライアントが表示されます。
3. クライアントの**Operation**アイコン･･･をクリックします。
4. メニューから**Monitor**を選択します。

クライアントのリアルタイム監視ページが開きます。

Realtime Monitoring Information

x座標は150秒の特定の時間に従って変化します。

- **Reception and transmission rate trend graph**: 直前の150秒間のクライアントの受信および送信率のトレンド。x座標は時間を表し、y座標は受信および送信率を表します。
- **Signal strength (dBm) trend graph**: 直前の150秒間にアクセスAPによって取得されたクライアントの信号強度トレンド。x座標は時間を表し、y座標は信号強度を表します。
- **Received noise trend graph**: 直前の150秒間のクライアントの受信ノイズ傾向。x座標は時間を表し、y座標は受信ノイズを表します。
- **Signal noise ratio trend graph**: 直前の150秒間のクライアントの信号ノイズ比のトレンド。x座標は時間を表し、y座標は信号ノイズ比を表します。
- **Received(Bytes)**: モニタリング時間内に受信したトラフィックの合計量。
- **Rx Speed**: クライアントの現在の受信レート。
- **Transmitted(Bytes)**: モニタリング時間内に送信されたトラフィックの合計量。
- **Tx Speed**: クライアントの現在の送信速度。
- **Signal Strength(dBm)**: クライアントの現在の信号強度。
- **Received Noise(dBm)**: クライアントの現在の受信ノイズ。
- **Online Time**: クライアントのオンライン期間(hh:mm:ss形式)。
- **Signal Noise Ratio(dBm)**: クライアントの現在の信号ノイズ比。

クライアントトラフィック分析の表示

この関数は、NTAサーバーからクライアントトラフィック情報を取得し、クライアントトラフィック情報をトレンドグラフに表示し、WSMにリストします。この関数は、NTAがIMCサーバーにデプロイされている場合にのみ使用できます。

クライアントトラフィック分析を表示するには、次の手順を実行します

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Clients**を選択します。

   Clientsページにすべてのクライアントが表示されます。
3. クライアントの**Operation**アイコン ··· をクリックし、ショートカットメニューから**Station Traffic Analysis**を選択します。

クライアントトラフィック分析ページには、上位5つのアプリケーション速度、トラフィックごとの上位10のアプリケーション、およびトラフィックごとの上位10のホストのトレンドグラフが表示されます。

静的ブラックリストからのクライアントの削除

静的ブラックリストの詳細は、「静的ブラックリストの構成」を参照してください。静的ブラックリストからクライアントを削除するには、次のようにします。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Clients**を選択します。

   Clientsページにすべてのクライアントが表示されます。
3. クライアントの**Operation**アイコン ··· をクリックし、**Remove MAC address from the static blacklist**を選択します。
4. **OK**をクリックします。

クライアント履歴情報の表示

この機能を使用すると、過去1時間、過去1日、過去1週間、過去1か月、またはユーザー定義の時間におけるオンラインクライアントのレート、トラフィックおよびオンラインデータの統計を表示できます。この機能は、ComwareベースのFAT APまたはFIT APを介してオンラインになるクライアントにのみ適用されます。

- **Traffic statistics**: 情報収集の開始時刻と終了時刻、送信トラフィック、受信トラフィック、および合計トラフィック。
- **Rate statistics**: 指定した統計情報収集時刻における送信および受信レートのトレンドグラフ、ピーク送信レート、ピーク受信レート、平均送信レート、平均受信レート、および送信および受信レート。
- **Online data statistics**: クライアントのオンライン数と合計オンライン期間、および各オンライン期間の特定のオンライン時間、オフライン時間、関連するAP、およびオンライン期間。

クライアント履歴情報を表示するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Clients**を選択します。

   Clientsページにすべてのクライアントが表示されます。
3. クライアントの**Operation**アイコン ··· をクリックします。
4. メニューから**History In**を選択します。

History Inダイアログボックスが表示されます。

5. **Query**領域で、**Statistics**リストから統計タイプを選択します。オプションは、**Traffic**, **Rate**,および**Online Data**です。デフォルトのオプションは**Traffic**です。
6. リストから時間範囲を選択します。オプションは次のとおりです。
   - **1h**
   - **1d**
   - **1w**
   - **1m**
   - **1y**
   - **Custom**

   Customを選択した場合は、開いたCustomウィンドウに開始時間と終了時間を入力するか、**Start Time/End Time**の横のフィールドをクリックして、表示されるカレンダーから開始時間/終了時間をYYYY-MM-DD hh:mm形式で選択します。終了時間は開始時間より後である必要があります。

   指定した時間範囲の統計情報が表示されます。

   - **Traffic Statistics**

     トラフィックの単位は、送受信されるトラフィックの量に応じて変化します。**Traffic**を選択すると、次の情報が表示されます。

     - **Start Time**: 統計情報収集の開始時刻。YYYY-MM-DD hh:mm:ss形式で指定します。
     - **End Time**: 統計情報収集の終了時刻。YYYY-MM-DD hh:mm:ss形式で指定します。
     - **Transmitted Traffic(B)**: 指定した時間範囲内にクライアントによって送信されたトラフィックの合計。データが変更されると、測定単位も自動的に変更されます。
     - **Received Traffic(B)**: 指定した時間範囲内にクライアントが受信したトラフィックの合計。データが変更されると、測定単位も自動的に変更されます。
     - **Total Traffic(B)**: 指定した時間範囲内にクライアントによって送信および受信された合計トラフィック。この値は統計に基づいて計算され、実際の値と多少異なる場合があります。測定単位はデータの変更に応じて自動的に変更されます。
   - **Rate Statistics**

レートの単位は、レートの値によって変わります。**Rate**を選択すると、次の情報が表示されます。

- **Transmission and Reception Rate Trend graph**: データ収集時間内のクライアントの送信および受信率のトレンド。x座標は時間を表し、y座標は送信および受信率を表します。x座標上の時間間隔は、統計収集時間内で変化します。
  - **Peak Transmission Rate**: 統計情報収集時間内のクライアントの最大送信レート。測定単位は、データの変更に応じて自動的に変更されます。
  - **Peak Reception Rate**: 統計情報収集時間範囲内のクライアントの最大受信レート。測定単位は、データの変更に応じて自動的に変更されます。
  - **Average Transmission Rate**: 統計情報収集時間範囲内のクライアントの平均送信レート。データが変更されると、測定単位も自動的に変更されます。
  - **Average Reception Rate**: 統計収集時間範囲内のクライアントの平均受信率。測定単位はデータの変更に応じて自動的に変更されます。
- **Rate Details**

トレンドグラフの上部にある**Rate**をクリックして、**Details**ウィンドウを表示します。

  - **Time**: 送信または受信統計情報が収集される時刻。YYYY-MM-DD hh:mm:ss形式で指定します。
  - **Transmission Rate**: 指定した時刻のクライアントの転送レート。

- **Reception Rate**: 指定された時刻のクライアントの受信レート。
- **Online Data Statistics**

Online Dataを選択すると、次の情報が表示されます。

- **Online Count**: 統計情報収集時間範囲内でのクライアントの正常なアソシエーション時間。
- **Total Online Duration**: 統計収集時間範囲内のクライアントの合計オンライン時間。
- Online Data Details
  - **Online Time**: クライアントのオンライン時間(YYYY-MM-DD hh:mm:ss形式)。
  - **Offline Time**: クライアントのオフライン時間(YYYY-MM-DD hh:mm:ss形式)。
  - **AP**: クライアントに関連付けられたAPのデバイスラベル。
  - **Online Duration**: クライアントが関連付けられている期間(hh:mm:ss形式)。

7. **Close**をクリックします。

同期間隔の設定

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Clients**を選択します。**Clients**ページにすべてのクライアントが表示されます。
3. **Set Sync Interval**をクリックします。
4. **Set Sync Interval**ダイアログボックスで、間隔を選択します。
   オプションは、**30 Sec.**, **1 Min.**, **3 Min.**, **5 Min.**, および **Custom**です。デフォルトの間隔は3分です。**Custom**を選択した場合は、5から1000000秒の範囲で間隔を入力します。
5. **OK**をクリックします。

パフォーマンス収集パラメーターの設定

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Clients**を選択します。Clientsページにすべてのクライアントが表示されます。
3. **Performance Collection Parameters**をクリックします。
4. 開いたページで、次のパラメーターを設定します。
   - **Collection Status**: 収集ステータスを選択します。オプションは**Off**および**On**です。
   - **Collection Interval**:収集間隔を60～86400秒の範囲で入力します。
5. **OK**をクリックします。

クライアントのオンライン履歴管理

WSMには、クライアントオンライン履歴情報リストを介してWSMにアクセスするすべてのクライアントに関する情報が表示されます。WSMでは、クライアントオンライン履歴情報の問合せおよびクライアントローミングトラックの表示もできます。

クライアントのオンライン履歴情報リストの表示

この機能を使用すると、クライアントの詳細なオンライン履歴情報を表示できます。クライアントオンライン履歴

情報リストでは、次の情報を表示できます。

- MAC address
- User name
- SSID
- Online time
- Offline time
- Online duration
- Total traffic
- AP location
- AP name of clients

クライアントのオンライン履歴情報リストを表示するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Clients**を選択します。

   Clientsページにすべてのクライアントが表示されます。
3. **Client Online History**をクリックします。

すべてのクライアントのオンライン履歴情報は、クライアントオンライン履歴情報リストに表示されます。

Client Online History Information List

- **MAC Address**: クライアントのMACアドレス。
- **Username**: クライアントがワイヤレスネットワークにアクセスするために使用するユーザー名。
  - **ComwareベースのAP**: ユーザー名は、WSMがUAMとコラボレーションされた場合、またはユーザー情報がWSMに追加された場合にのみ表示されます。
- **IP Address**: クライアントのIPアドレス。
- **SSID**: クライアントがネットワークにアクセスするために使用するSSID名。
- **Online Time**: クライアントのオンライン時間(YYYY-MM-DD hh:mm:ss形式)。
- **Offline Time**: クライアントのオフライン時間(YYYY-MM-DD hh:mm:ss形式)。
- **Online Duration**: クライアントがオンラインであった期間(hh:mm:ss形式)。

注:

クライアントのポーリング間隔はデフォルトで3分に設定されているため、オンライン時間、オフライン時間、およびオンライン時間には3分のエラーが発生する場合があります。

- **Total Traffic(KB)**: クライアントがオンラインのときに生成されたトラフィックの合計。
- **AP Location**: クライアントに関連付けられているアクセスAPのロケーションビュー名。
- **AP Name**: クライアントに関連付けられたアクセスAPのデバイスラベル。
- **Operation**: **Operation**アイコン は、関連付けられたクライアントの操作タスクへのリンクを表示します。

Operationメニューから、クライアントローミングトラックを表示できます。

Client Online History Information Listに十分なエントリーが含まれている場合は、次のナビゲーションツールが表示されます。

- **Next Page**アイコンをクリックすると、**Client Online History Information List**のページが次に進みます。
- **Last Page**アイコンをクリックすると、**Client Online History Information List**の最後のペ

ージに移動します。

- **Previous Page**アイコンをクリックすると、**Client Online History Information List**のページが逆方向に表示されます。
- **First Page**アイコンをクリックすると、**Client Online History Information List**の先頭ページに戻ることができます。

Client Online History Information Listの右上にある**8**、**15**、**50**、**100**、または**200**をクリックします。
各ページに表示する項目数を指定します。

Client Online History Information Listは、**Operation**フィールド以外のすべてのフィールドでソートできます。選択したフィールドでリストをソートするには、列ラベルをクリックします。列ラベルを使用すると、各フィールドに固有の様々なソートオプションを切り替えることができます。

4. **Back**をクリックして、クライアントリストページに戻ります。

注:

Resourceタブから履歴情報リストにアクセスすることもできます。**Resource**タブをクリックし、ナビゲーションツリーから**Terminal Access>History Access Log**を選択して、**Client Online History**をクリックします。

クライアントのオンライン履歴情報の照会

WSMには、基本問合せと拡張問合せが用意されています。基本問合せ基準には、迅速な検索のためのキーパラメーターがいくつか含まれています。拡張問合せには、正確な照合のための様々な問合せ基準が用意されています。

クライアントのオンライン履歴を照会する手順は、次のとおりです。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Clients**を選択します。
   Clientsページにすべてのクライアントが表示されます。
3. Client Online Historyをクリックします。
   すべてのクライアントに関するオンライン履歴情報は、Client Online Historyページに表示されます。
4. 基本的なクエリーを実行します。
   a. クライアントのMACアドレスを入力します。WSMは、このフィールドのファジーマッチングをサポートしています。
   b. **Query**アイコンをクリックします。**Client Online History**ページに、問合せ基準に一致するすべてのクライアントのオンライン履歴が表示されます。
   c. **Query**フィールドをクリアしてQueryアイコンをクリックすると、すべてのクライアントのオンライン履歴が表示されます。
5. 高度なクエリーを実行します。
   a. Queryフィールドの横にある**Expand**アイコンをクリックしてQuery領域を拡張します。再度クリックするとQuery領域が非表示になります。
   b. 次の問合せ基準を1つ以上指定します。
      - **MAC Address**: クライアントのMACアドレスを入力します。WSMは、このフィールドのファジーマッチングをサポートします。
      - **SSID**: クライアントがネットワークに接続するために使用するSSID名を入力します。WSMは、このフィールドのファジーマッチングをサポートしています。

- **Online from/to**: 開始時刻と終了時刻を入力して、オンライン履歴がクエリー基準の範囲内にあるすべてのクライアントのオンライン履歴情報をクエリーします。または、Start Time/End Timeの横にあるフィールドをクリックして、表示されるカレンダーから開始時刻と終了時刻をYYYY-MM-DD hh:mm形式で選択できます。終了時刻は開始時刻より後である必要があります。
- **Online more than**: クライアントのオンライン時間を分単位で入力して、オンライン時間が指定した値よりも長いすべてのクライアントのオンライン履歴情報を照会します。
- **AP Location**: クライアントに関連付けられたアクセスAPのロケーションビュー。WSMは、このフィールドのファジーマッチングをサポートします。
- **AP Name**: クライアントに関連付けられたアクセスAPのデバイスラベル。WSMは、このフィールドのファジーマッチングをサポートします。
- **Username**: クライアントがワイヤレスネットワークにアクセスするために使用するユーザー名。WSMは、このフィールドのファジーマッチングをサポートします。
- **IP Address**: クライアントのIPアドレスを入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。

空のフィールドは、クエリー条件として使用できません。

c. **Query**をクリックして、クライアントオンライン履歴情報リストの問合せ基準と一致するエントリーを表示します。

d. **Reset**をクリックすると、クエリー基準がクリアされ、すべてのクライアントのオンライン履歴情報が表示されます。

クライアントローミングトラックの表示

この機能を使用すると、クライアントローミングトラックを表示できます。ローミングトラックは、クライアントのアクセスAPが存在するロケーションビュー トポロジーに動的に表示されます。

クライアントのローミングトラックを表示する前に、クライアントに関連付けられているすべてのAPがロケーションビューに追加されていることを確認してください。追加されていない場合、ローミングトラックは完全には表示されません。

クライアントローミングトラックを表示するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Clients**を選択します。

   Clientsページにすべてのクライアントが表示されます。
3. Client Online Historyをクリックします。

すべてのクライアントのオンライン履歴情報は、クライアントオンライン履歴情報リストに表示されます。

4. クライアントの**Operation**アイコン ⋯ をクリックします。
5. メニューから**View Roaming track**を選択します。

オペレーターは、ロケーションビュー トポロジーでクライアントローミングトラックの動的な表示を確認できます。

顧客情報管理

クライアント情報管理機能を使用すると、クライアントのMACアドレスからユーザー名へのマッピングを管理できます。クライアント情報を1つずつ追加したり、テキストファイルを使用してクライアント情報をバッチでインポートできます。WSMがUAMと連携している場合、オペレーターはUAMからユーザー情報をインポートできます。

クライアント情報リストの表示

WSMは、クライアント情報リストの問合せ機能を提供します。クライアントのMACアドレス、クライアント名、クライアントID、アドレス、電話番号、電子メールおよび更新時刻を表示できます。

クライアント情報リストを表示するには、次のとおりです。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Clients**を選択します。
   Clientsページにすべてのクライアントが表示されます。
3. Client Info Managementをクリックします。
   すべてのクライアント情報は、Client Info Managementページに表示されます。
   Client Info List
   - **MAC Address**: クライアントのMACアドレス。
   - **Username**: クライアントがワイヤレスネットワークにアクセスするために使用するユーザー名。
   - **Account Name**: 認証に使用されるアカウント名。
   - **Client Type**: iPhoneやPCなどのクライアントタイプ。
   - **Vendor**: エンドポイントのベンダー。
   - **OS**: エンドポイントが使用するオペレーティングシステム。
   - **Update Time**: クライアントの基本情報の最新更新時刻。
   - **Status**: クライアントのステータス。オプションはLockedとUnlockedです。WSMでは、Locked状態のクライアントの情報は同期されません。
   - **Modify**:クライアントに関する情報を変更するには、**Modify**アイコンをクリックします。

Client Info Listに十分なエントリーがある場合は、次のナビゲーションツールが表示されます。

- **Next Page**アイコンをクリックして、Client Info Listで次のページに進みます。
- **Last Page**アイコンをクリックすると、Client Info Listの最後のページに移動します。
- **Previous Page**アイコンをクリックして、Client Info Listのページを逆方向に表示します。
- **First Page**アイコンをクリックすると、Client Info Listの先頭に戻ることができます。

クライアント情報リストの右上にある**8**、**15**、**50**、**100**、または**200**をクリックして、各ページに表示する項目数を指定します。

Client Info Listは、Operationフィールド以外のすべてのフィールドでソートできます。選択したフィールドでリストをソートするには、列ラベルをクリックします。列ラベルを使用すると、各フィールドに固有の様々なソートオプションを切り替えることができます。

4. **Back**をクリックして、クライアントリストページに戻ります。

クライアント情報の照会

WSMには、特定のクライアント情報を取得するための問合せ機能が用意されています。クライアント情報を問い合せるには、次の手順を実行します:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Clients**を選択します。
   Clientsページにすべてのクライアントが表示されます。
3. Client Info Managementをクリックします。

すべてのクライアント情報がクライアント情報リストに表示されます。

4. 次の問合せ基準を1つ以上指定します。
   - **MAC Address**: クライアントのMACアドレスを入力します。WSMは、このフィールドのファジーマッチングをサポートします。
   - **Username**: クライアントの名前を入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。空のフィールドは、問合せ基準として機能しません。
5. Queryをクリックして、クライアント情報リストのクエリー基準に一致するエントリーを表示するか、Resetをクリックしてクエリー基準をクリアし、すべてのクライアントに関する情報を表示します。

クライアント情報の追加

この関数を使用すると、クライアント情報を手動で追加できます。

クライアント情報を追加するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Clients**を選択します。
   Clientsページにすべてのクライアントが表示されます。
3. Client Info Managementをクリックします。
   すべてのクライアント情報がクライアント情報リストに表示されます。
4. **Add**をクリックします。
   クライアント情報を追加するためのページが開きます。
5. 次のパラメーターを設定します。
   - **MAC Address**: クライアントのMACアドレスを入力します。このアドレスはWSM内で一意である必要があります。
   - **Username**: クライアントの名前を入力します。
   - **Account Name**: アカウント名を入力します。
   - **Client Type**: モバイルやiPhoneなどのクライアントタイプを入力します。
   - **Vendor**: エンドポイントのベンダーを入力します。
   - **OS**: エンドポイントで使用されるオペレーティングシステムを入力します。
   - **Client ID**: クライアントのIDを入力します。
   - **Address:** クライアントの連絡先アドレスを入力します。
   - **Email**: クライアントの電子メールを入力します。有効な電子メールアドレスのフォーマットは、yourname@domain.comです。
   - **Tel**: クライアントの電話番号を入力します。
6. OKをクリックします。

クライアント情報のインポート

この関数を使用すると、テキストファイルを介してクライアント情報をWSMにインポートできます。テキストファイルは次の要件を満たす必要があります。

- csvまたは.txtファイルである必要があり、そのサイズは5 MBを超えることはできません。
- ファイル内の各行の列数は同じです。
- 列間の区切り文字としてスペースが使用されている場合、2つの列の間には1つのスペースしか使用できません。スペースをさらに入力すると、インポートに失敗する可能性があります。

クライアント情報をインポートするには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Clients**を選択します。
   Clientsページにすべてのクライアントが表示されます。
3. Client Info Managementをクリックします。
   すべてのクライアント情報がクライアント情報リストに表示されます。
4. **import**をクリックします。
   クライアント情報をインポートするページが開きます。
5. **Source File**ボックスの横にある**Browse**をクリックします。
6. インポートするファイルを選択し、OKをクリックします。
7. **Delimiter** listトから区切り記号を選択します。オプションは次のとおりです。
   - **space**
   - **TAB**
   - **comma (,)**
   - **pound sign (#)**
   - **dollar sign ($)**
8. **Next**をクリックします。
   プロパティ列を選択するページが開きます。
9. ファイルからインポートするプロパティ列を選択します。オプションは次のとおりです。
   Not selected in the file:インポートされたすべてのクライアント情報のプロパティ値はNULLです。
   Overwrite Duplicate: インポートされたコンテンツによって既存のクライアント情報が上書きされます。Overwrite Duplicateを選択しないと、WSMは既存のクライアント情報を変更しません。
10. OKをクリックします。
    クライアント情報管理ページで、WSMはインポート結果を表示します。これには、インポートされた数、複製された数、失敗した数が含まれます。

クライアント情報の変更

この関数は、基本的なクライアント情報の変更に役立ちます。クライアント情報を変更するには、次の手順を実行します:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Clients**を選択します。
   Clientsページにすべてのクライアントが表示されます。
3. **Client Info Management**をクリックします。

すべてのクライアント情報がクライアント情報リストに表示されます。

4. クライアントの**Modify**アイコンをクリックします。

クライアント情報を変更するためのページが開きます。

5. 必要に応じてクライアント情報を変更します。詳細は、「クライアント情報の追加」を参照してください。
6. OKをクリックします。

クライアント情報の削除

この関数を使用すると、1つ以上のクライアント情報を削除できます。クライアント情報を削除するには、次の

手順を実行します:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Clients**を選択します。
   Clientsページにすべてのクライアントが表示されます。
3. **Client Info Management**をクリックします。
   すべてのクライアント情報がクライアント情報リストに表示されます。
4. 削除するクライアントの横にあるボックスを選択します。
5. **Delete**をクリックします。
   確認ダイアログボックスが表示されます。
6. OKをクリックします。

UAMクライアント情報の同期

この機能は、UAMクライアント情報を同期するのに役立ちます。

クライアント情報を同じIMCプラットフォームに基づいてインストールされたUAMと同期するために、オペレーターはUAMクライアント情報を直接同期できます。

異なるIMCプラットフォームに基づいてインストールされたUAMとクライアント情報を同期化するには、オペレーターは最初にUAMが提供するWebサービスパラメーターを構成する必要があります。詳細は、「UAMパラメーターの構成」を参照してください。

UAMクライアント情報を同期するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Clients**を選択します。
   Clientsページにすべてのクライアントが表示されます。
3. Client Info Managementをクリックします。

すべてのクライアント情報がクライアント情報リストに表示されます。

4. **Sync All**をクリックします。

同期処理には時間がかかるため、最新のクライアント情報は後で表示してください。

クライアントのロック

WSMは、ロック状態のクライアントの情報を同期化しません。クライアントをロックするには、次の手順に従います:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Clients**を選択します。
   Clientsページにすべてのクライアントが表示されます。
3. Client Info Managementをクリックします。

すべてのクライアント情報がクライアント情報リストに表示されます。

4. ロックするクライアントを選択して、**Lock**をクリックします。

クライアントのロック解除

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Clients**を選択します。

Clientsページにすべてのクライアントが表示されます。

3. Client Info Managementをクリックします。

クライアント情報リストには、すべてのクライアント情報が表示されます。

4. ロック解除するクライアントを選択し、Unlockをクリックします。

関連付けられていないクライアントの管理

この機能を使用すると、検出されたがどのAPにも関連付けられていないクライアントを管理できます。WSMは、異なるAPからの検出結果を計算してクライアントを検索します。管理者は、関連付けられていないクライアントの履歴を問い合せて、検出されたAPの詳細を表示できます。

関連付けられていないクライアントの表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Clients**を選択します。
   Clientsページにすべてのクライアントが表示されます。
3. Unassociated Clientをクリックします。
   関連付けられていないクライアントの情報はすべて、Unassociated Clientページに表示されます。
   Unassociated Client List
   - **MAC Address**: アソシエートされていないクライアントのMACアドレス。
   - **Location**: 関連付けられていないクライアントが存在するロケーションビューの名前。
   - **First Detected at**: 関連付けられていないクライアントが最初に検出された時刻。
   - **Last Located at**: 関連付けられていないクライアントが最後に検出された時刻。
   - **Detecting AP**:アソシエートされていないクライアントからの最も強い信号を検出するAP。

   Unassociated Client Listに十分な数のエントリーがある場合は、次のナビゲーションツールが表示されます。

- **Next Page**アイコンをクリックして、Unassociated Client Listのページを進めます。
- **Last Page**アイコンをクリックして、Unassociated Client Listの最後のページに進みます。
- **Previous Page**アイコンをクリックして、Unassociated Client Listのページを逆方向に移動します。
- **First Page**アイコンをクリックして、Unassociated Client Listの前にページバックします。

Unassociated Client Listの右上にある**8**、**15**、**50**、**100**、または**200**をクリックして、各ページに表示する項目数を指定します。

Unassociated Client Listは、Operationフィールド以外のすべてのフィールドでソートできます。列ラベルをクリックすると、選択したフィールドでリストをソートできます。列ラベルを使用すると、各フィールドに固有の様々なソートオプションを切り替えることができます。

関連付けられていないクライアントのクエリー

WSMには、基本問合せと拡張問合せが用意されています。基本問合せ基準には、迅速な検索のためのキーパラメーターがいくつか含まれています。拡張問合せには、正確な照合のための様々な問合せ基準が用意されています。

関連付けられていないクライアントを照会するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Clients**を選択します。
   Clientsページにすべてのクライアントが表示されます。
3. Unassociated Clientをクリックします。
   関連付けられていないクライアントの情報はすべて、Unassociated Clientページに表示されます。
4. 基本的なクエリーを実行します。
   a. 関連付けられていないクライアントのMACアドレスを入力します。WSMは、このフィールドのファジーマッチングをサポートします。
   b. **Query**アイコンをクリックします。Unassociated Clientページには、問合せ基準に一致するすべての関連付けられていないクライアントが表示されます。
   c. **Query**フィールドをクリアし、**Query**アイコンをクリックして、関連付けられていないすべてのクライアントを表示します。
5. 高度なクエリーを実行します。
   a. **Query**フィールドの横にある**Expand**アイコンをクリックして、**Query**領域を拡張します。
   b. 次の問合せ基準を1つ以上指定します。
      - **MAC Address**: アソシエートされていないクライアントのMACアドレスを入力します。WSMは、このフィールドのファジーマッチングをサポートします。
      - **Location**: 検出しているAPが配置されているロケーションビューを選択します。空のフィールドはクエリー条件として使用できません。
   c. **Query**をクリックすると、関連付けられていないクライアント情報リストのクエリー基準に一致するエントリーが表示されます。
   d. **Reset**をクリックして、クエリー基準をクリアし、関連付けられていないすべてのクライアントを表示します。

検出APの詳細の表示

検出APは、アソシエートされていないクライアントからの最も強い信号を検出するAPです。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Clients**を選択します。
   Clientsページにすべてのクライアントが表示されます。
3. Unassociated Clientをクリックします。
   関連付けられていないクライアントの情報はすべて、Unassociated Clientページに表示されます。
4. アソシエートされていないクライアントのdetecting APリンクをクリック検出APの詳細が表示されます。

関連付けられていないクライアントの履歴の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Clients**を選択します。
   Clientsページにすべてのクライアントが表示されます。
3. Unassociated Clientをクリックします。
   関連付けられていないクライアントの情報はすべて、Unassociated Clientページに表示されます。
4. Unassociated Client Historyをクリックします。
   Unassociated Client Historyページが開きます。

Unassociated Client History List

- **MAC Address**: アソシエートされていないクライアントのMACアドレス。
- **Location**: 関連付けられていないクライアントが存在するロケーションビューの名前。
- **First Detected at**: 関連付けられていないクライアントが最初に検出された時刻。
- **Continued for**: アソシエートされていないクライアントが最初に検出されてから、最後に検出されるまでの期間。
- **Detecting AP**: アソシエートされていないクライアントからの最も強い信号を検出するAP。

5. Backをクリックします。

トラブルシューティング

このトラブルシューティング機能は、ComwareベースのAP(FAT APまたはFIT AP)に関連付けられたクライアントに適用できます。

トラブルシューティング機能を使用すると、クライアントアクセスの障害または不安定なリンクステータスのトラブルシューティングを行うことができます。また、NQA操作を実行して、ACとWebサイト、AAAサーバー、DNSサーバー、またはポータルサーバーとの間のリンクをテストし、問題の原因が外部ネットワークの障害であるかどうかを判断できます。

チャネル使用状況、チャネル品質、RSSI、干渉デバイスなどのスペクトル分析データをトラブルシューティングページで表示できます。スペクトル分析データに基づいて、干渉デバイスを見つけるなど、WLAN内の問題を特定できます。

前提条件

トラブルシューティング機能を使用する前に、次の作業を完了してください。

- アラーム管理モジュールとsyslog管理モジュールがインストールされ、展開されていることを確認します。

トラブルシューティング機能では、ACからIMCプラットフォームに送信されるsyslogを使用して、クライアントのアクセスステータスをリアルタイムでトラブルシューティングします。トラブルシューティング機能を有効にするには、syslog管理モジュールとアラーム管理モジュールをインストールして展開してから、この機能を使用します。

- フィルタリング規則**Filter Trap**をディセーブルにして、ACまたはFAT APから送信されたsyslogをフィルタリングしないようにIMCプラットフォームを設定します。
- ACまたはFAT APでトラブルシューティング機能を有効にします。

WSMは、トラブルシューティング機能がイネーブルになった後にだけ、ACまたはFAT APから送信されたsyslogを収集します。

アラーム管理モジュールとsyslog管理モジュールのインストールと展開

1. **System**タブをクリックします。
2. ナビゲーションツリーから、**System Configuration** > **Deploy Component**を選択します。

   Deploy Componentページが開きます。

   IMC Platform – Alarm Management および **IMC Platform – Syslog Management** の **Status** フィールドに Deployed と表示されることを確認します。

   アラーム管理モジュールまたはsyslog管理モジュールのStatusフィールドにUndeployedと表示されている場合は、最初にモジュールをインストールしてデプロイします。詳細は、「H3C IMCデプロイメントガイド」を参照してください。

フィルタートラップ規則を無効にする

1. **Alarm**タブをクリックします。
2. ナビゲーションツリーから、Syslog Management>Filtering Ruleを選択します。

   Filtering Ruleページが開きます。
3. **Filter Trap**ルールの**Modify**アイコンをクリックします。**Modify Rule**ページが開きます。
4. StatusフィールドでDisabledを選択します。
5. OKをクリックします。

ACまたはFAT APでのトラブルシューティングのイネーブル化

ACまたはFAT APでトラブルシューティング機能が無効になっている場合、トラブルシューティングページにはTroubleshooting Conclusion領域は表示されません。

ACまたはFAT APでトラブルシューティングをイネーブルにするには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management**を選択します。

   Resource Managementリストが表示されます。
3. 次のいずれかの操作を実行します。
   - ACを表示するには、リストの**ACs**をクリックします。
   - FAT APを表示するには、リストの**Fat APs**をクリックします。

   ACsページまたはFat APsページが開きます。
4. ACまたはFAT APの名前をクリックします。

   デバイスの詳細ページが開きます。
5. ページの右側の操作領域で、次の操作を行います。
   - ACを変更するには、AC Configuration > Global Configurationを選択します。
   - FAT APを変更するには、Fat AP Configuration > Global Configurationを選択します。

   AC Global Parameter ConfigurationページまたはFat AP Global Parameter Configurationページが開きます。
6. **Troubleshooting**を選択します。
7. OKをクリックします。

クライアントのトラブルシューティング

クライアントのトラブルシューティングを行う場合、クライアントのトラブルシューティングが完了するまで、他のオペレーターは他のブラウザまたはPC上で同じクライアントのトラブルシューティングを行うことができません。

トラブルシューティング設定ページから、またはクライアントのMACアドレス、IPアドレス、またはユーザー名を照会して、トラブルシューティングプロセスを開始します。

トラブルシューティングプロセスを開始するには、次のクイッククエリー機能を使用します。

- **By querying the MAC address of a client**: クライアントリストにないクライアントがWLANにアクセスできない場合は、クライアントのMACアドレスを問い合わせる方法でしかクライアントのトラブルシューティングを実行できません。
- **By querying the IP address of a client**: クライアントリスト内のクライアントがWLANに正常に接続されている場合は、IPアドレスでクライアントを照会できます。
- **By querying the username of a client**: ユーザーがどのクライアントを使用しているかわからない場合は、ユーザー名を照会してトラブルシューティングプロセスを開始できます。

クライアントのMACアドレスを照会する

トラブルシューティングプロセスを開始するには:

1. ページの右上隅にある問合せボックスの**Expand**アイコンをクリックします。操作リストが表示されます。
2. **Troubleshooting**アイコンをクリックします。
3. **Query**ボックスにクライアントのMACアドレスをxx:xx:xx:xx:xx:xx:xx形式で入力します。
4. **Query**アイコンをクリックします。

   トラブルシューティングパラメーターの設定ページが開きます。

5. トラブルシューティングパラメーターを設定します。
   - リアルタイムアクセスプロセスのトラブルシューティングを行うには、Configure TimeでReal Timeを選択します。
   - 履歴アクセスプロセスのトラブルシューティングを行うには、Configure TimeフィールドでHistoryを選択します。

     Historyを選択した場合は、トラブルシューティングプロセスの開始時刻と終了時刻を設定する必要があります。
     - **Start Time**: Start Timeの横のフィールドをクリックして、表示されるカレンダーから開始時間を選択します。
     - **End Time**: End Timeの横にあるフィールドをクリックして、表示されるカレンダーから終了時間を選択します。終了時間は開始時間より後である必要があり、開始時間と終了時間の間隔は24時間を超えることはできません。

   注:

   WSMは、ACでトラブルシューティング機能が有効になるまで、ACによって送信されたsyslogを収集しません。ACでトラブルシューティング機能が無効になっている履歴期間にアクセスプロセスのトラブルシューティングを行うと、Troubleshooting Conclusion領域に内容が表示されません。

クライアントリストにないクライアントがWLANにアクセスできない場合、トラブルシューティングページにはNQA情報が表示されません。そのため、Webサイトおよびサーバーの IPアドレスを入力する必要はありません。

6. **Start Troubleshooting**をクリックします。トラブルシューティングページが開きます。
7. クライアントのアクセスステータスを表示します。

   Troubleshooting Conclusion領域には、syslogに基づいたクライアントのリアルタイムアクセスステータスが表示されます。失敗の理由を分析するには、アクセスステータスと推奨事項を使用します。問題が解決したら、後で参照できるように、トラブルシューティングプロセスを推奨事項に記録します。

   注:

   ベストプラクティスとして、問題が解決するまで推奨事項を変更しないでください。

8. 推奨事項を変更します。
   a. **Troubleshooting Conclusion**領域で、**Modify Recommendations**をクリックします。

      Modify Recommendationsウィンドウが開きます。
   b. フィールドにrecommendationsを入力します。
   c. OKをクリックします。
9. トラブルシューティング情報を表示します。

   Troubleshooting Conclusion領域には、クライアントがアソシエートしようとするAPに関連するすべてのsyslogが表示されます。障害の原因を分析するには、syslogを使用します。

   トラブルシューティングsyslogは、レベルおよび詳細な説明でフィルタリングできます。トラブルシューティングsyslogをフィルタリングするには、次の手順を実行します。

   a. 1つ以上のsyslogレベルを選択します。オプションは次のとおりです。
      - **Emergency**
      - **Alert**
      - **Critical**
      - **Error**

- **Warning**
- **Notification**
- **Information**
- **Debugging**

b. 詳細説明ボックスにsyslogキーワードを入力します。

WSMでは、このフィールドのファジーマッチングがサポートされています。たとえば、詳細説明ボックスにDHCPと入力すると、DHCPに関連するsyslogのみが表示されます。このボックスにキーワードを入力しないと、WSMはレベルのみでsyslogをフィルタします。

c. アイテムのフィルタをクリックします。

syslogリストには、フィルタリング基準に一致するすべてのsyslogが表示されます。

Syslog List

- **Level** : Syslogレベル。
- **Result**: syslogの分析結果。
- **Description**: syslogの詳細な説明。
- **Time**: syslogを受信した時刻。

10. トラブルシューティングプロセスを停止するには、ページの下部にある**Stop**をクリックします。

By querying the IP address of a client

クライアントをIPアドレスで問い合せるには、WSMに記録されている(クライアントリストに表示されている)クライアントIPアドレスを入力する必要があります。たとえば、クライアントのIPアドレスが1.2.6.6で、WSMがそのIPアドレスを0.0.0.0として記録している場合、IPアドレス1.2.6.6でクライアントを問い合せることはできません。

WSMは、ComwareベースのAPに関連付けられたクライアントのIPアドレスを次のように記録します。

- WSMは、次のいずれかの条件でクライアントのIPアドレスを取得できる場合に、クライアントの実際のIPアドレスを記録します。
  - クライアントはiNodeを介してWLANにアクセスします。
  - IPスヌーピングはACまたはFAT APでイネーブルです。IPスヌーピングがイネーブルの場合、ACまたはFAT APはクライアントのMACアドレスとIPアドレスのマッピングを記録します。
- WSMは、クライアントのIPアドレスを取得できない場合、クライアントのIPアドレスを0.0.0.0として記録します。

クライアントのIPアドレスを照会してトラブルシューティングプロセスを開始するには、次の手順を実行します。

1. ページの右上隅にある問合せボックスの**Expand**アイコンをクリックします。操作リストが表示されます。

2. **Troubleshooting**アイコンをクリックします。

3. queryボックスにクライアントのIPアドレスをx.x.x.xの形式で入力します。

4. **Query**アイコンをクリックします。

次のいずれかのページが開きます。

- クライアントリストにクライアントの実際のIPアドレス(0.0.0.0以外の一意のIPアドレス)を入力すると、**Configure Troubleshooting Parameters**ページが開きます。
- 0.0.0.0を入力すると、WSMによって2つ以上のクライアントのIPアドレスが0.0.0.0として記録され、**Client List**ページが開きます。

  クライアントリストでターゲットクライアントを選択し、OKをクリックして**Configure Troubleshooting Parameter**ページに入ります。
- 照会されたクライアントがクライアントリストにない場合は、エラーページが開きます。

5. トラブルシューティングパラメーターを設定します。
   - **Configure Time**: リアルタイムアクセスプロセスのトラブルシューティングを行うには、**Configure Time**フィールドでReal Timeを選択します。履歴アクセスプロセスのトラブルシューティングを行うには、**Configure Time**フィールドでHistoryを選択します。

     Historyを選択した場合は、トラブルシューティングプロセスの開始時刻と終了時刻を設定する必要があります。
     - **Start Time**: Start Timeの横のフィールドをクリックして、表示されるカレンダーから開始時間を選択します。
     - **End Time**: End Timeの横にあるフィールドをクリックして、表示されるカレンダーから終了時間を選択します。終了時間は開始時間より後にする必要があり、開始時間と終了時間の間隔は24時間を超えることはできません。

     注:

     WSMは、ACでトラブルシューティング機能が有効になるまで、ACによって送信されたsyslogを収集しません。ACでトラブルシューティング機能が無効になっている履歴期間にアクセスプロセスのトラブルシューティングを行うと、Troubleshooting Conclusion領域に内容が表示されません。
   - **Website IP**: WebサイトIPボックスを選択し、WebサイトのIPアドレスを入力します。WSMは、ACとWebサイト間のリンクに対してNQA操作を実行します。
   - **AAA Server IP**: AAA server IPボックスを選択し、AAAサーバーのIPアドレスを入力します。WSMは、ACとAAAサーバー間のリンク上でNAT操作を実行します。
   - **DNS Server IP**: **DNS Server IP**ボックスを選択し、DNSサーバーのIPアドレスを入力します。WSMは、ACとDNSサーバー間のリンクでNAT操作を実行します。
   - **Portal Server IP**: ポータルサーバーIPボックスを選択し、ポータルサーバーのIPアドレスを入力します。WSMは、ACとポータルサーバー間のリンクに対してNAT操作を実行します。
6. **Start Troubleshooting**をクリックします。

   トラブルシューティングページが開きます。

   ページの上部には、クライアント、SSID、Fit AP、AC、またはFat AP、およびワイヤレスネットワークの品質評価レベルに関する情報が表示されます。品質評価レベルは次のように分類されます。
   - **Good**: 緑色の5つの星で表されます。
   - **Medium**: オレンジ色の2つ半の星で表されます。
   - **Poor**: 赤の1つ半の星で表されます。

     APがスイッチに接続され、スイッチがIMCプラットフォームに追加されている場合、WSMはスイッチに関する情報も表示します。ただし、WSMはスイッチの品質を評価しません。
7. クライアントのアイコンをクリックすると、クライアントに関する情報が表示されます。

   Basic Information
   - **Username**: クライアントがワイヤレスネットワークにアクセスするために使用するユーザー名。
   - **Channel**: クライアントによって使用されるチャネル。
   - **MAC Address**: クライアントのMACアドレス。
   - **SSID**: ワイヤレスネットワークのSSID。
   - **IP Address**: クライアントのIPアドレス。
   - **Authentication Type**: ワイヤレスネットワークの認証タイプ: **Open System**または**Shared Key**。
   - **Vendor**: クライアントのベンダー。WSMでは、不明なベンダーについて**Others**が表示されます。
   - **Encryption Mode**: ワイヤレスネットワークの暗号化モード(ClearまたはCrypto)。

- **Online Duration**: クライアントがオンラインであった合計期間。
- **Signal Noise Ratio(dB)**: クライアントの信号ノイズ比(dB単位)。
- **VLAN ID**: クライアントに割り当てられたVLAN ID。
- **RSSI**: ワイヤレス接続の受信信号強度インジケータ。
- **Location**: クライアントが存在するロケーションビュー。
- **Transmission Traffic(KB)**: クライアントが受信した合計トラフィック(KB単位)。
- **Radio Type**: クライアントがAPに接続するために使用する無線のタイプ。
- **Reception Traffic(KB)**: クライアントによって送信された合計トラフィック(KB単位)。

Trend Graph

- **Reception Rate/Transmission Rate**: クライアントのリアルタイムの受信レートおよび送信レートのトレンド。
- **Signal Strength(dBm)**: リアルタイムでのクライアントの信号強度のトレンド。
- **Received Noise(dBm)**: クライアントの受信ノイズのリアルタイムの傾向。
- **Signal Noise Ratio(dB)**: リアルタイムでのクライアントの信号ノイズ比のトレンド。

Evaluation Result

- **Index:** 信号ノイズ比および信号強度を含む品質評価の基準。
- **Expected Value**: **Configure**アイコン  をクリックして、期待値を設定します。デフォルトの期待値の詳細は、表24を参照してください。
- **Obtained Value**: 取得されたインデックス値。取得された値は、期待値に達すると緑色で表示され、期待値に達しないと赤色で表示されます。
- **Risk**: インデックス値が期待値に達しない場合に発生するネットワークの問題。表24には、WSMによって対処される問題のみがリストされています。
- **Suggestion**: 問題を解決するために実行されるメジャー。表24には、WSMによって提案されるメジャーのみがリストされています。

表24評価結果

索引	期待値	リスク	提案
信号強度	20 dB以上	不安定なネットワーク。	APの展開を確認します。
信号ノイズ比	-65 dBm ～ -40 dBm	クライアントのアクセスに失敗しました。ネットワークの速度が低下します。	APの展開を確認します。

Troubleshooting Conclusion

Troubleshooting Conclusion領域には、クライアントクライアントのリアルタイムネットワークアクセス情報が表示されます。ネットワークアクセスの問題が発生した場合は、アクセスステータスの問題が発生した場合は、アクセスステータスおよび提案に基づいて障害の理由を分析できます。問題が解決した後は、将来の参照用に、提案としてトラブルシューティングプロセスを記録できます。

提案を変更するには:

a. **Troubleshooting Conclusion**領域で、**Modify Recommendations**をクリックします。

   Modify Recommendationsウィンドウが開きます。

b. フィールドに候補を入力します。

c. OKをクリックします。

Troubleshooting Conclusion領域には、クライアントがアソシエートしようとするAPに関連するすべてのsyslogが表示されます。syslogはトラブルシューティングに使用でき、**Level**および**Detailed Description**でフィルタリングできます。

トラブルシューティングsyslogをフィルタリングするには、次の手順を実行します

a. 1つ以上のsyslogレベルを選択します。オプションは次のとおりです。

   - **Emergency**
   - **Alert**
   - **Critical**
   - **Error**
   - **Warning**
   - **Notification**
   - **Information**
   - **Debugging**

b. **detailed description**ボックスにsyslogキーワードを入力します。

   WSMでは、このフィールドのファジーマッチングがサポートされています。たとえば、detailed descriptionボックスにDHCPと入力すると、DHCPに関連するsyslogのみが表示されます。このボックスにキーワードを入力しないと、WSMはレベルのみでsyslogをフィルタします。

c. **Filter Item**をクリックします。

   syslogリストには、フィルタリング基準に一致するすべてのsyslogが表示されます。

   Syslogリスト

   - **Level**: Syslogレベル。
   - **Result**: syslogの分析結果。
   - **Description**: syslogの詳細な説明。
   - **Time**: syslogを受信した時刻。

8. クライアントがアクセスするWLANに関する情報を表示するには、SSIDアイコンをクリックします。Comwareベースのデバイスの場合は、SSIDアイコンをクリックしてサービスポリシー情報を表示しま

す。

Basic Information

- **SSID**: サービスポリシーのSSIDの名前。
- **Enable**: サービスポリシーのステータス: Enable、Disable、またはNot Ready。
- **Policy ID**: サービスポリシーのID。
- **Interface ID**: サービスポリシーにバインドされているWLAN論理インターフェースのID。
- **Encryption Mode**ド: サービスポリシーの暗号化モード(ClearまたはCrypto)。
- **Authentication Type**: サービスポリシーが無線にバインドされている場合に設定されるリンク認証タイプ(**Open System**または**Shared Key**)。
- **Interface Type**: サービスポリシーにバインドされているインターフェースのタイプ。デフォルトはWLAN-ESSです。
- **Max Clients**: WLANアクセスのサービスポリシーによって許可されるクライアントの最大数。

Trend Graph

- **Associated Clients**: トラブルシューティングの開始以降にサービスポリシーに関連付けられたクライアントの数量トレンド。
- **Reception Rate/Transmission Rate**ト: トラブルシューティングが開始されてからの、WLANのサービスポリシーの受信レートと送信レートの傾向。

Evaluation Result

- **Index**: 品質評価の基準であり、関連クライアントです。
- **Expected Value**: **Configure**アイコン  をクリックして、期待値を設定します。デフォルトの期待値の詳細は、表25を参照してください。
- **Obtained Value**: 取得されたインデックス値。取得された値は、期待値に達すると緑色で表示され、期待値に達しないと赤色で表示されます。
- **Risk**: インデックス値が期待値に達しない場合に発生するネットワークの問題。表25には、WSMによって対処される問題のみがリストされています。
- **Risk**: 題を解決するために実行される手段。表25には、WSMによって提案される手段のみがリストされています。

表25 評価結果

索引	期待値	リスク	提案
関連付けられたクライアント	15以下	新しいクライアントへのアクセスに失敗しました。ネットワークが低速です。	ロードバランシングをイネーブルにするか、またはより多くのAPを展開します。

9. APアイコンをクリックすると、クライアントに関連付けられているAPに関する情報が表示されます。

Basic Information

- **AP Label**: APのデバイスラベル。
- **IP Address**: APのIPアドレス。
- **Associated Clients**: APにアソシエートされているクライアントの総数。
- **Online Duration**: APがオンラインであった期間の合計。

Trend Graph

- **CPU Usage(%)**: リアルタイムでのAPのCPU使用率のトレンド。
- **Memory Usage(%)**: リアルタイムでのAPのメモリー使用率の。
- **Associated Clients**: トラブルシューティングの開始以降にAPに関連付けられたクライアントの数量トレンド。

- **Reception Rate/Transmission Rate**: トラブルシューティングを開始してからのWLAN内のAPの受信レートと送信レートの傾向。

Evaluation Result

- **Index**: 品質評価の基準。**Associated Clients**、**Associated Failures**、**Alarms**、**CPU Usage(%)**、および**Memory usage(%)**が含まれます。
- **Expected Value**: **Configure**アイコンをクリックして、期待値を設定します。デフォルトの期待値の詳細は、表26を参照してください。
- **Obtained Value**: 取得されたインデックス値。取得された値は、期待値に達すると緑色で表示され、期待値に達しないと赤色で表示されます。
- **Risk**: インデックス値が期待値に達しない場合に発生するネットワークの問題。表26には、WSMによって対処される問題のみがリストされています。
- **Suggestion**: 問題を解決するために実行されるメジャー。表26には、WSMによって提案されるメジャーのみがリストされています。

表26 評価結果

索引	期待値	リスク	提案
Associated Clients	≤ 15	新規クライアントのアクセス障害。 遅いネットワーク。	ロード バランシングを有効にするか、より多くの AP を展開します。
Alarms	0	AP がアラーム状態で動作しています。	詳細なアラーム情報に基づいてアラームをクリアします。
Associated Failures	0	新規クライアントのアクセス障害。 遅いネットワーク。	ロード バランシングを有効にするか、より多くの AP を展開します。
CPU Usage (%)	≤ 75%	パフォーマンスの低い不安定な AP。	AP 構成を確認します。
Memory Usage (%}	≤ 75%	パフォーマンスの低い不安定な AP。	AP 構成を確認します。

Detection Information

- **Clients Detected**: ワイヤレスネットワークで検出されたすべてのクライアントを表示するには、**Clients Detected**タブをクリックします。詳細については、「検出されたクライアントの一覧」を参照してください。
- **SSIDs Detected**: ワイヤレスネットワークで検出されたすべてのSSIDを表示するには、**SSIDs Detected**タブをクリックします。詳細については、「検出されたSSID」を参照してください。
- **APs Detected**: **APs Detected**タブをクリックして、ワイヤレスネットワークで動作しているすべてのAPを表示します。詳細については、「検出されたAP」を参照してください。

RF pingの結果

WSMはクライアントに対してRF pingテストを実行し、RF Ping Result領域にRF pingデータを表示します。

RF ping結果リスト

- **No.**: RF pingパケットのシーケンス番号。
- **Rate(Mbps)**: テストパケットの伝送レート(Mbps単位)。

- **TxCnt**: 送信されたパケットの数。
- **RxCnt**: 受信したパケット数。
- **RSSI**: クライアントのRSSI。クライアントが受信した信号の強度を示します。値が大きいほど、信号が強いことを示します。
- **RTT(ms)**: パケット応答時間(ミリ秒単位)。

  5秒ごとに5回のRF pingテストを実行すると、ワイヤレスリンクのステータスの結果が表示されます。ステータスには、**failed**, **very poor**, **poor**, **good**, または **excellent**.があります。リンクのステータスが**very poor** または **poor**の場合は、スペクトル分析情報を表示して問題を特定します。

Spectrum Analysis

スペクトル分析情報を表示するには、次のすべての条件が満たされていることを確認します。

- APは、スペクトル分析機能をサポートし、ハイブリッドモードで動作します。
- スペクトル分析は、APのACと無線の両方でイネーブルになります。
- スペクトル分析ライセンスがACにインストールされています。
- クライアントに関連付けられたAPがロケーションビューに追加されます。スペクトル分析情報を

表示するには、次の手順を実行します。

a. **Spectrum Analysis**をクリックします。

b. **Spectrum Analysis Monitor**をクリックします。

   Spectrum Analysis Monitorウィンドウが開き、クライアントがアソシエートしているAPに関するスペクトル分析情報(チャネル使用状況、チャネル使用状況の傾向、チャネル品質、チャネル品質の傾向など)が表示されます。詳細については、「スペクトル分析モニターの管理」を参照してください。

c. 干渉デバイスを表示します。

   干渉デバイスリストには、クライアントがアソシエートしているAPによって検出されたすべての干渉デバイスが表示されます。

   Interference device list

   - **Interference Type**: 電子レンジやBluetoothデバイスなどの干渉デバイスタイプ。
   - **Sensitivity**: 干渉デバイスによって発生する干渉の重大度レベル。オプションは0～100の整数です。値が大きいほど、干渉の重大度が高いことを示します。
   - **RSSI**: Received Signal Strength Indicator(受信信号強度インジケータ)
   - **Duty Cycle (%)**: 干渉のデューティサイクル。デューティサイクルは、干渉デバイスがアクティブであった時間です。デバイスのデューティサイクルを表示できます。
   - **Affected Channel**: 干渉デバイスの影響を受けるチャネル。

d. スペクトル分析を停止するには、**Stop Spectrum Analysis**をクリックします。

10. スイッチアイコンをクリックすると、APに直接接続されているスイッチに関する情報が表示されます。

    スイッチアイコンが表示されるのは、スイッチがIMCプラットフォームに追加されている場合だけです。

    Basic Information

    - **Device Label**: スイッチのデバイスラベル。
    - **IP Address**: スイッチのIPアドレス。
    - **System Name**: スイッチソフトウェアのシステム名。
    - **Device Model**: スイッチのデバイスモデル。
    - **Device Status**: スイッチのアラームステータス。
    - **Runtime**: スイッチが動作していた合計時間。

NQA Information

トラブルシューティングプロセスには、APと直接接続されたスイッチ間の有線リンク、およびACとスイッチ間のリンクでのNQA操作が含まれます。

- **Link Information**: デバイスラベル(IPアドレス)-デバイスラベル(IPアドレス)によってリンクを識別します。
- **Packet Loss Rate(%)**: テストパケットの損失率。
- **Source to Destination Average Delay(ms)**: 送信元から宛先までの平均遅延(ミリ秒単位)。
- **Destination to Source Average Delay(ms)**: 宛先から送信元までの平均遅延(ミリ秒単位)。
- **Remarks**: NQA操作が失敗した場合に、失敗の理由を表示します。

11. APに接続されているACに関する情報を表示するには、ACアイコンをクリックします。

Basic Information

- **Device Label**: ACのデバイスラベル。
- **IP Address**: ACのIPアドレス。
- **Model**: ACのデバイスモデル。
- **Runtime**: ACが実行されている合計時間。
- **Status**: ACのアラームステータス。
- **Contacts**: ACの連絡先情報。
- **Online APs**: ACによって管理されているオンラインFIT APの数。
- **Total APs**: ACによって管理されているFIT APの総数。
- **Associated Clients**: ACによって管理されているFIT APに関連付けられているクライアントの数。

Trend Graph

- **Associated Clients**: トラブルシューティングの開始以降、ACによって管理されているFIT APに関連付けられているクライアントの数量傾向。

Evaluation Result

- **Index**: 品質評価の基準。**Associated Clients**です。
- **Expected Value**: 期待値を設定するには、**Configure**アイコンをクリックします。デフォルトの期待値については、表27を参照してください。
- **Obtained Value**: 取得されたインデックス値。取得された値は、期待される値に達した場合は緑色で表示され、期待される値に達しなかった場合は赤色で表示されます。
- **Risk**: インデックス値が期待値に達しない場合に発生するネットワークの問題。表27は、WSMによって対処される問題のみを示しています。
- **Suggestion**: 問題を解決するために実行される措置。表27には、WSMによって提案される措置のみがリストされています。

表27評価結果

索引	期待値	リスク	提案
関連付けられたクライアント	15以下	新しいクライアントのアクセスの失敗。 ネットワークの速度が遅い。	ロードバランシングをイネーブルにするか、より多くのAPを配置します。

NQA Information

トラブルシューティングプロセスには、ACとIMCプラットフォームによって管理される直接接続されたスイッチ間の有線リンク、およびACとfit AP間のリンクでのNQA操作が含まれます。Web

サイトのIPアドレスまたはサーバーのIPアドレスが設定されている場合、WSMはACとWebサイトまたはサーバー間のリンクでNATテストも実行します。

NQA information list

- Link Information: デバイスラベル(IPアドレス)-デバイスラベル(IPアドレス)によってリンクを識別します。
- **Packet Loss Rate(%)**: テストパケットの損失率。
- **Source to Destination Average Delay(ms)**: 送信元から宛先までの平均遅延(ミリ秒単位)。
- **Destination to Source Average Delay(ms)**: 宛先から送信元までの平均遅延(ミリ秒単位)。
- **Source to Destination Positive Jitter(ms)**: 送信元から宛先への正のジッタ(ミリ秒単位)。
- **Destination to Source Positive Jitter(ms)**: 宛先から送信元への正のジッタ(ミリ秒単位)。
- **Source to Destination Negative Jitter(ms)**: 送信元から宛先への負のジッタ(ミリ秒単位)。
- **Destination to Source Negative Jitter(ms)**: 宛先から送信元への負のジッタ(ミリ秒単位)。
- **Remarks**: NQA操作が失敗した場合に、失敗の理由を表示します。たとえば、**One or both of the devices on the two ends of the link do not support NQA**.

12. クライアントが関連付けられているFAT APに関する情報を表示するには、FAT APアイコンをクリックします。

Basic Information

- **Device Label**: FAT APのデバイスラベル。
- **IP Address**: FAT APのIPアドレス。
- **Model**: FAT APのデバイスモデル。
- **Runtime**: FAP FATが実行されている合計時間。
- **Status**: FAT APのアラームステータス。
- **Contacts**: FAT APの連絡先情報。
- **Associated Clients**: FAT APに関連付けられているクライアントの数。

Trend Graph

- **Associated Clients**ト: トラブルシューティング開始以降の、FAT APに関連付けられたクライアントの数の傾向。

Evaluation Result

- **Index**: 品質評価の基準。関連クライアントです。
- **Expected Value**: 期待値を設定するには、**Configur**アイコン  をクリックします。デフォルトの期待値については、表28を参照してください。
- **Obtained Va**: 取得されたインデックス値。取得された値は、期待される値に達した場合は緑色で表示され、期待される値に達しなかった場合は赤色で表示されます。
- **Risk**: インデックス値が期待値に達しない場合に発生するネットワークの問題。表28は、WSMによって対処される問題のみを示しています。
- **Suggestion**: 問題を解決するために実行される措置。表28には、WSMによって提案される措置のみがリストされています。

表28 評価結果

索引	期待値	リスク	提案
関連付けられたクライアント	15以下	新しいクライアントのアクセスの失敗。 ネットワークの速度が遅い。	ロードバランシングをイネーブルにするか、より多くのAPを配置します。

Detection Information

- **Clients Detected**: ワイヤレスネットワークで検出されたすべてのクライアントを表示するには、**Clients Detected**タブをクリックします。詳細については、「検出されたクライアントの一覧」を参照してください。
- **SSIDs Detected**: ワイヤレスネットワークで検出されたすべてのSSIDを表示するには、**SSIDs Detected**タブをクリックします。詳細については、「検出されたSSID」を参照してください。

RF ping Result

WSMはクライアント上でRF pingテストを実行し、RF Ping Result領域にRF pingデータを表示します。

RF ping Result List

- **No.**: RF pingパケットのシーケンス番号。
- **Rate(Mbps)**: テストパケットの伝送レート(Mbps単位)。
- **TxCnt**: 送信されたパケットの数。
- **RxCnt**: 受信したパケット数。
- **RSSI**: クライアントのRSSI。クライアントが受信した信号の強度を示します。値が大きいほど、信号が強いことを示します。
- **RTT(ms)**: パケット応答時間(ミリ秒単位)。

  5秒ごとに5回のRF pingテストを実行すると、ワイヤレスリンクのステータスの結果が表示されます。ステータスには、**failed**, **very poor**, **poor**, **good**, または **excellent**.があります。リンクのステータスが**very poor** または **poor**の場合は、スペクトル分析情報を表示して問題を特定します。

NQA Information

トラブルシューティングプロセス中に、WebサイトIPアドレスまたはサーバーIPアドレスが設定されている場合、WSMはFAT APとWebサイトまたはサーバー間の有線リンクでNQA操作を実行します。

NQA Information List

- **Link Information**: デバイスラベル(IPアドレス)-デバイスラベル(IPアドレス)によってリンクを識別します。
- **Packet Loss Rate(%)**: テストパケットの損失率。
- **Source to Destination Average Delay(ms)**: 送信元から宛先までの平均遅延(ミリ秒単位)。
- **Destination to Source Average Delay(ms)**: 宛先から送信元までの平均遅延(ミリ秒単位)。
- **Source to Destination Positive Jitter(ms)**: 送信元から宛先への正のジッタ(ミリ秒単位)。
- **Destination to Source Positive Jitter(ms)**: 宛先から送信元への正のジッタ(ミリ秒単位)。
- **Source to Destination Negative Jitter(ms)**: 送信元から宛先への負のジッタ(ミリ秒単位)。
- **Destination to Source Negative Jitter(ms):** 宛先から送信元への負のジッタ(ミリ秒単位)。
  - **Remarks**: NQA操作が失敗した場合に、失敗の理由を表示します。たとえば、**One or both of the devices on the two ends of the link do not support NQA By**

querying the username of a client

Client Info Managementページで、ComwareベースのAPに関連付けられたクライアントのユーザー名を設定できます。または、WSMは次の方法でユーザー名を取得できます。

- 802.1X認証ユーザーの場合、WSMは自動的にACまたはFAT APからユーザー名を取得します。
- UAMサーバーで認証されたユーザーの場合、Client Info Managementページで同期操作を実行すると、WSMによってUAMからのユーザー名が同期されます。

クライアントのユーザー名を照会してトラブルシューティングプロセスを開始するには、次の手順を実行します。

1. ページの右上隅で、問合せボックスの**Expand**アイコンをクリックします。
   操作リストが表示されます。
2. **Troubleshooting**アイコンをクリックします。
3. クライアントのユーザー名を入力します。
   WSMでは、このフィールドのファジー一致がサポートされています。
4. **Query**アイコンをクリックします。
   次のいずれかのページが開きます。
   - クエリーユーザー名に一致するクライアントが1つだけの場合は、**Configure Troubleshooting Parameters**ページが開きます。
   - 複数のクライアントがクエリーユーザー名に一致する場合は、**Client List**ページが開きます。

   クライアントリストでターゲットクライアントを選択し、OKをクリックして、そのクライアントのConfigure Troubleshooting Parametersページに移動します。

   トラブルシューティングパラメーターの設定およびトラブルシューティングプロセスについて詳しくは、「クライアントのIPアドレスを照会する」を参照してください。

Starting the troubleshooting process from the troubleshooting configuration page

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > Resource Management**を選択します。
   Resource Managementリストが表示されます。
3. **Clients**をクリックします。
   Clientsページが開きます。
4. クライアントの**Operation**アイコンをクリックします。

操作リストが表示されます。

5. **Troubleshooting**をクリックします。
   Configure Troubleshooting Parametersページが開きます。

トラブルシューティングパラメーターの設定およびトラブルシューティングプロセスについて詳しくは、「クライアントのIPアドレスを照会する」を参照してください。

RF ping

重要:

RF pingテストは、スリープ状態のクライアントでは失敗します。

ネットワークが不安定な場合や低速で動作している場合は、RF ping機能を使用してワイヤレスリンクの問題を検出できます。

クライアントでRF pingテストを実行するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > Resource Management**を選択します。

   Resource Managementリストが表示されます。
3. **Clients**をクリックします。

   Clientsページが開きます。
4. クライアントの**Operation**アイコン･･･をクリックします。

操作リストが表示されます。

5. RF Pingをクリックします。

   RF pingウィンドウが開きます。

   WSMはRF pingテスト情報を5秒ごとにACに送信し、RF pingデータをRF ping結果リストに表示します。

   RF ping Result List
   - **No**: RF pingパケットのシーケンス番号。
   - **Rate(Mbps)**: テストパケットの伝送レート(Mbps単位)。
   - **TxCnt:** 送信されたパケットの数。
   - **RxCnt**: 受信したパケット数。
   - **RSSI**: クライアントのRSSI。クライアントが受信した信号の強度を示します。RSSIが高いほど、信号が強いことを示します。
   - **RTT(ms)**: パケットへの応答時間(ミリ秒単位)。
6. RF pingテストを停止するには、RF pingウィンドウを閉じます。

無線の管理

無線リストには、WSMによって管理されているFAT APおよびFIT APのすべての無線に関する情報が表示されます。無線リストから、無線の詳細の表示、特定の無線のクエリー、および無線設定の変更を行うことができます。

無線リストを表示する

1. Serviceタブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > Resource Management > Radios**を選択します。Radio Listページに、すべての無線が表示されます。

   ラジオリスト

   - **Admin Status**: 無線の管理ステータス。緑のアイコン🟢は管理ステータスがUpであることを示し、グレーのアイコン⚫は管理ステータスがDownであることを示します。
   - **AP**: 無線が属するAPのデバイスラベル。デバイスラベルをクリックすると、APの詳細情報を表示できます。FIT APの場合、このフィールドにはAPを管理するACのデバイスラベルも表示されます。
   - **Radio ID** :-無線のID。詳細を表示するには、無線IDをクリックします。
   - **Radio Type** :無線のタイプ。オプションは次のとおりです。
     - **802.11a**
     - **802.11b**
     - **802.11g**
     - **802.11bg**
     - **802.11at**
     - **802.11an**
     - **802.11gn**
     - **802.11ac**
     - **802.11n(2.4GHz)**
     - **802.11bgn**
     - **802.11n**
     - **802.11n(5GHz)**
     - **802.11ac/n/a**
   - **Vendor**: 無線がバインドされているAPのベンダー。オプションは、H3C。
   - **Current Transmission Power(dBm)**: 無線の現在の送信電力(dBm単位)。
   - **Channe**l: 無線の動作チャネル。このフィールドにAutoが表示されている場合、ACまたはFAT APは無線ネットワーク上で検出されたすべてのチャネルを評価し、最適なチャネルを動作チャネルとして選択します。
   - **Channel Assignment Mode**: 無線のチャネル割り当てモード。オプションは、**Manual**および**Auto**です。モードがAutoの場合、Channelフィールドには Autoが表示されます。モードがManualの場合、Channelフィールドには無線の動作チャネルが表示されます。
   - **Number of Neighbor APs**: 無線によって検出されたネイバーAPの数。
   - **Operation Status**: 無線の動作状態。オプションはUpおよびDownです。
   - **Modify**: 無線の設定を変更するか、無線の管理ステータスを変更します。
     - **Modify**アイコン📝をクリックして、無線設定を変更します。

– アイコンをクリックして、無線管理ステータスを変更します。

Radio Listに十分なエントリーが含まれている場合は、次のナビゲーションが表示されます。

- **Next Page**アイコンをクリックして、**Radio List**で次のページに進みます。
- **Last Page**アイコンをクリックして、**Radio List**の最後までページを進めます。
- **Previous Page**アイコンをクリックして、**Radio List**のページを逆方向に移動します。
- **First Page**アイコンをクリックして、**Radio List**の先頭に戻ります。

Radio Listの右上にある**8**、**15**、**50**、**100**、または**200**をクリックして、各ページに表示する項目の数を指定します。

Radio Type、**Admin Status**、**Operation Status**および**Modify**フィールドを除くすべてのフィールドで無線リストをソートできます。選択したフィールドでリストをソートするには、列ラベルをクリックします。列ラベルを使用すると、各フィールドに固有のソートオプションを切り替えることができます。

無線のクエリー

WSMには、基本問合せと拡張問合せが用意されています。基本問合せ基準には、迅速な検索のためのキーパラメーターがいくつか含まれています。拡張問合せには、正確な照合のための様々な問合せ基準が用意されています。

無線をクエリーするには、次の手順を実行

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > Resource Management > Radios**を選択します。Radio Listページに、すべての無線が表示されます。
3. 基本的なクエリーを実行します。
   a. 無線IDを入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
   b. **Query**アイコンをクリックします。Radio Listに、クエリー基準に一致するすべての無線が表示されます。
   c. **Query**フィールドをクリアし、**Query**アイコンをクリックしてすべての無線を表示します。
4. 高度なクエリーを実行します。
   a. **Query**フィールドの横にある**Expand**アイコンをクリックして、Query領域を展開します。再度クリックすると、Query領域が非表示になります。
   b. 次の問合せ基準を1つ以上指定します。
   - **AC Label**: ACのデバイスラベルを入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。この基準は、FIT APにバインドされている無線にだけ適用されます。
   - **AP Label**: 無線がバインドされているAPのデバイスラベルを入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
   - **Radio ID**: 無線のIDを入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
   - **Vendor**: 無線がバインドされているAPのベンダーを選択します。オプションは次のとおりです。
     – Unlimited
     – H3C
   - Radio Type: 無線のタイプを選択します。オプションは次のとおりです。
     – **All**

- **802.11a**
- **802.11b**
- **802.11g**
- **802.11bg**
- **802.11at**
- **802.11an**
- **802.11gn**
- **802.11ac**
- **802.11n(2.4GHz)**
- **802.11bgn**
- **802.11n**
- **802.11n(5GHz)**
- **802.11ac/n/a**
- **Wired**

o **Channel**: 無線の作業チャネルを入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。

o **Operation Status**: 無線の動作状態を選択します。オプションは次のとおりです。

- **All**
- **Down**
- **Up**

空のフィールドや制限なしに設定されたフィールドは、クエリーの抽出条件として使用できません。

c. **Query**をクリックします。

Radio Listには、クエリー基準に一致するすべての無線が表示されます。

d. クエリー基準をクリアしてすべての無線を表示するには、**Reset**をクリックします。

無線設定の変更

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > Resource Management > Radios**を選択します。Radio Listページに、すべての無線が表示されます。
3. 無線の**Modify**アイコンをクリックします。

ComwareベースのFAT APの無線設定を変更する方法については、「FAT APの無線パラメーターの変更」を参照してください。

ComwareベースのFIT APの無線設定の変更については、「FIT APの無線パラメーターの変更」を参照してください。

無線管理ステータスの変更

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > Resource Management > Radios**を選択します。Radio Listページに、すべての無線が表示されます。
3. 無線のアイコンをクリックします。

確認ダイアログボックスが表示されます。

4. OKをクリックします。

WLANの管理

WLANは、ACまたはFAT APに設定されるワイヤレスサービスで、SSIDによって識別されます。APはWLANを使用して、クライアントにワイヤレスアクセスサービスを提供します。管理の便宜上、ComwareベースのACに設定されるサービスポリシーは、WLAN管理ではWLANと呼ばれます。

WLAN Managementから、WLANリストの表示、WLANのクエリー、同じSSIDを持つWLANの表示、WLAN履歴情報の表示、WLANのバッチでの変更および削除を実行できます。

WLANリストの表示

WLANリストには、ネットワーク内のすべてのWLANに関する情報が表示されます。SSIDにバインドされたFAT APとFIT AP、およびSSIDを介してネットワークにアクセスするクライアントを表示できます。

WLANリストを表示するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > WLANs**を選択します。WLAN Listには、すべてのWLANが表示されます。

   WLAN List

   - **SSID**: SSIDの名前。SSIDで設定されたすべてのWLANに関する情報を表示するには、名前のリンクをクリックします。
   - **Total Fat APs**: ComwareベースのFat APの場合、このフィールドには、サービスポリシーにバインドされているFat APの数が表示されます。数値リンクをクリックすると、Fat APの詳細情報が表示されます。
   - **Total Fit AP**: ComwareベースのFit APの場合、このフィールドには、サービスポリシーにバインドされているFit APの数が表示されます。数値リンクをクリックすると、Fit APの詳細情報が表示されます。
   - **Total Clients**: SSIDを使用してネットワークにアクセスするクライアントの数。数値をクリックすると、その詳細が表示されます。
   - **Operation**: **Operation**メニューを表示するには、WLANの**Operation**アイコン ⋯ をクリックします。

Operationメニューの操作タスクには、バッチでのWLANの変更と削除、およびWLAN履歴の表示が含まれます。

WLAN Listに十分なエントリーが含まれている場合は、次のナビゲーション支援が表示されます。

- **Next Page**アイコンをクリックして、WLAN Listで次のページに進みます。
- **Last Page**アイコンをクリックして、WLAN Listの最後までページを進めます。
- **Previous Page**アイコンをクリックして、WLAN Listで前のページに戻ります。
- **First Page**アイコンをクリックして、WLAN Listの先頭に戻ります。

WLAN Listの右上にある**8**、**15**、**50**、**100**、または**200**をクリックして、各ページに表示する項目の数を指定します。

WLAN Listは、**Operation**フィールドを除くすべてのフィールドで並べ替えることができます。選択したフィールドでリストを並べ替えるには、列ラベルをクリックします。列ラベルを使用すると、各フィールドに固有の並べ替えオプションを切り替えることができます。

WLANのクエリー

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > WLANs**を選択します。

   WLAN Listには、すべてのWLANが表示されます。
3. SSIDを入力します(大文字と小文字は区別されません)。WSMでは、このフィールドのファジーマッチングがサポートされています。
4. **Query**アイコン  をクリックします。

Device Listには、クエリー基準に一致するすべてのWLANが表示されます。

5. **Query**フィールドをクリアし、**Query**アイコンをクリックしてすべてのWLANを表示します。

同じSSIDを使用するWLANのリストの表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > WLANs**を選択します。

   WLAN Listには、すべてのWLANが表示されます。
3. WLANのSSID名をクリックします。

   WLAN Listには、このSSIDを使用するすべてのWLANが表示されます。

   WLAN List
   - **Status**: ComwareベースのACおよびFat APの場合、このフィールドには、サービスポリシーがイネーブルになっているかどうかが表示されます。
   - **SSID**: SSIDの名前。名前のリンクをクリックすると、詳細が表示されます。
   - **Device Label**: IMCプラットフォームでWLANがバインドされているデバイスを識別するデバイスラベル。デバイスラベルをクリックすると、その詳細が表示されます。ACグループおよびグループメンバー情報は、AC detailsページで表示できます。
   - **Device Type**: WLANがバインドされているデバイスのタイプ。オプションはACおよびFat APです。
   - **Encryption Mode**: ComwareベースのACおよびFAT APの場合、このフィールドにはサービスポリシーの暗号化モードが表示されます。オプションは、ClearおよびCryptoです。Clearモードは、データパケットを暗号化する必要がないことを意味します。Cryptoモードは、すべてのデータパケットを暗号化する必要があることを意味します。
   - **Authentication Mode**: ComwareベースのACおよびFAT APの場合、このフィールドにはサービスポリシーの認証モードが表示されます。オプションは、**Open-System**、**Shared-Key**、および**All**です。
   - **Vendor**: WLANがバインドされているACまたはFat APのベンダー。オプションはH3Cです。
   - **Client Forwarding Mode**: ComwareベースのACおよびFat APの場合、このフィールドにはデータパケットの転送モードが表示されます。オプションは、リモート、ローカル、およびポリシーベースです。その他のデバイスの場合、このフィールドは空です。
   - **Modify**: WLANを変更するには、**Modify**アイコン  をクリックします。
     - ComwareベースのACおよびFAT APの場合は、Modifyアイコンをクリックしてサービスポリシーを変更します。詳細については、Comwareベースのアクセスコントローラの「サービスポリシーの変更」またはComwareベースのFAT APの「サービスポリシーの変更」を参照してください。
4. **WLAN List**ページに戻るには、**Back**をクリックします。

WLAN履歴情報の表示

この機能を使用すると、WLANトラフィック、クライアント数、およびクライアントのオンライン期間の履歴情報を表示できます。

- **Traffic**: 統計情報収集の開始時刻と終了時刻、送信トラフィック、受信トラフィック、および合計トラフィック。
- **Online Clients**: 統計情報の収集時間範囲内のオンラインクライアントのトレンドグラフ、ピークおよび平均オンラインクライアント、およびオンラインクライアント数。
- **Client Online Duration**: 指定された時間範囲内にWLANにアクセスしているクライアントに関するオンライン情報。すべてのクライアントの合計および平均オンライン時間、単一クライアントのオンライン時間、オフライン時間、およびオンライン時間が含まれます。

WLAN履歴情報を表示するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > WLANs**を選択します。

   WLAN Listには、すべてのWLANが表示されます。
3. WLANのOperationアイコン ･･･をクリックします。
4. メニューから**History Information**を選択します。

   History Informationダイアログボックスが開きます。
5. Statisticsリストから統計タイプを選択します。オプションは次のとおりです。
   - **Traffic (default)**
   - **Online Clients**
   - **Client Online Duration**
6. 時間範囲を設定します。オプションは次のとおりです。
   - **1h**
   - **1d**
   - **1w**
   - **1m**
   - **1y**
   - **Custom**
7. **Custom**を選択します。

   開いたCustomウィンドウで、開始時刻と終了時刻を入力するか、**Start Time/End Time**の横にあるフィールドをクリックして、表示されたカレンダーから開始時刻と終了時刻をYYYY-MM-DD hh:mm形式で選択します。

   指定された時間範囲の統計情報が表示されます。
   - **Traffic Statistics**

     トラフィックの単位は、送受信されたトラフィックの量によって変化し

     ます。**Traffic**を選択すると、次の情報が表示されます。
     - **Start/End Time**: 統計情報収集の開始時刻または終了時刻(YYYY-MM-DD hh:mm:ss形式)。
     - **Transmitted Traffic(B)**: 指定された時間範囲内にWLANによって送信されたトラフィックの合計。
     - **Received Traffic(B)**: 指定された時間範囲内にWLANが受信したトラフィックの合計。
     - **Total Traffic(B)**: 指定された時間範囲内にWLANが送受信したトラフィックの合計。この

値は統計に基づいて計算され、実際の値とは若干異なる場合があります。

- **Online Clients Statistics**

  時間の単位は、時間範囲の値によって変化します。

  Online Clientsを選択した場合は、次の情報が表示されます。

  - **Online Clients Trend Graph**: データコレクション時間範囲内でWLANにアクセスしているクライアントの傾向。x軸は時間を表し、y軸はクライアントの数を表します。
  - **Peak Number of Online Clients**: 統計情報の収集時間範囲内でWLANにアクセスするオンラインクライアントの最大数。
  - **Average Online Clients**: 統計情報収集時間範囲内でWLANにアクセスするオンラインクライアントの平均数。

    トレンドグラフの上部にある**Online Clients**をクリックして、Detailsウィンドウを表示します。
  - **Time**: 統計情報が収集された時刻(YYYY-MM-DD hh:mm:ss形式)。
  - **Clients**: 統計情報の収集時間範囲内でWLANにアクセスするオンラインクライアントの数。

- **Client Online Duration Statistics**
  - **Total Online Duration** :指定された時間範囲内にWLANにアクセスしたクライアントの合計オンライン時間。
  - **Average Online Duration**: 指定された時間範囲内にWLANにアクセスしたクライアントの平均オンライン時間。

  Details領域には、指定した時間範囲内にWLANにアクセスする各クライアントに関する次の情報が表示されます。
  - **Online Time**: クライアントがWLANにアクセスするためにオンラインになった時刻(YYYY-MM-DD hh:mm:ss形式)。
  - **Offline Time**: クライアントがオフラインになった時刻(YYYY-MM-DD hh:mm:ss形式)。
  - **MAC**: クライアントのMACアドレス。
  - **Online Duration**: WLANにアクセスするクライアントのオンライン継続時間(hh:mm:ss形式)。

8. **Close**をクリックして、ダイアログボックスを閉じます。

バッチでのWLANの変更

WLAN Listページで WLANを変更できます。

- 複数のデバイス上の指定されたSSIDを持つWLANをバッチで変更します。デバイスが同じベンダーのものであることを確認してください。
- 同じSSIDを持つWLANがバインドされているデバイスが異なるベンダーのものである場合は、1つのWLANだけを変更します。

WLANをバッチで変更するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > Resource Management > WLANs**を選択します。

   WLAN Listには、すべてのWLANが表示されます。
3. WLANのOperationアイコン ... をクリックします。
4. メニューから**Modify**を選択します。

バッチでWLANを変更するためのページが開きます。

WLAN **List**には、次の基準に一致するWLANがACまたはFat APごとに表示されます。

- 以前に選択したWLANと同じSSIDを使用するWLAN。
- WLANが属するACまたはFAT APは、同じベンダーのものです。

5. ターゲットWLANを選択します。

WSMでは、デフォルト設定が設定されているデバイスを確認するプロンプトが表示されます。

6. 次のパラメーターを設定します。

表29セキュリティ情報

暗号化モード	セキュリティ情報
None	セキュリティパラメーターは必要ありません。
Static WEP	· key Length: リストからキーの長さを選択します。オプションは64ビットと128ビットです。 · Key Type: リストからキータイプを選択します。オプションはASCIIおよびHEX · Key Index: リストからキー索引を選択します。オプションは1、2、3および4です。 · Key: キー値を入力します。64ビットキーの場合は、5文字の英数字文字列または10桁の16進数を入力します。128ビットキーの場合は、13文字の英数字文字列または26桁の16進数を入力します。
Dynamic WEP	セキュリティパラメーターは必要ありません。
WPA Pre-Shared key	Version: リストからWPAバージョンを選択します。オプションは、WPA、WPA2、およびWPAまたはWPA2です。 Cipher: リストから暗号化モードを選択します。オプションは次のとおりです。 TKIP、CCMP(AES)、およびTKIP+CCMP(AES)。 Key Type: このフィールドは常にASCIIで、変更できません。 Pre-Shared Key: 事前共有キーを入力します。
WPA Dynamic	· Version: リストからWPAバージョンを選択します。オプションは、WPA、WPA2、およびWPAまたはWPA2です。 · Cipher: リストから暗号化モードを選択します。オプションは次のとおりです。 TKIP、CCMP(AES)、およびTKIP+CCMP(AES)。

Comwareベースのデバイスに関する**Basic information**:

- **SSID**:サービスポリシーのSSIDを入力します。これは一意である必要があります。nullにはできません。文字列には、次の大文字と小文字が区別される文字、数字、および特殊文字を含めることができます。
  - チルダ(~)
  - 感嘆符(!)
  - アットマーク(@)
  - シャープ記号(#)
  - ドル記号($)
  - パーセント記号(%)

- キャレット(^)
- アンパサンド記号(&)
- アスタリスク(*)
- 左中かっこ({)
- 右中かっこ(})
- 左かっこ(()
- 右括弧())
- 左角カッコ(
- 右角かっこ(
- 左山カッコ(<)
- 右山カッコ(>)
- ハイフン(-)
- 下線(_)
- プラス記号(+)
- 等号(=)
- 縦棒(
- バックスラッシュ(\)
- コロン(:)
- セミコロン(;)
- 引用符(")
- アポストロフィ(')
- カンマ(,)
- ドット(.)
- スラッシュ(/)
- スペース

- **Enable**: ACまたはFat APに適用されたサービスポリシーをイネーブルまたはディセーブルにします。
- **Encryption Mode**: このフィールドは変更できません。
- **Hide SSID**: APによって送信されるビーコンフレーム内のSSIDを非表示にするには、このオプションを選択します。このパラメーターが選択されている場合、クライアントはビーコンフレームからSSIDを取得できないため、ワイヤレスネットワークにアクセスする前にSSIDを設定する必要があります。このパラメーターが選択されていない場合、クライアントはビーコンフレームからSSIDを取得してワイヤレスネットワークにアクセスできます。
- **Authorization Mode**: リストからサービスポリシーの認可モードを選択します。オプションは次のとおりです。
  - **Open System**: 認証を要求するクライアントに対しては、認証は実行されません。
  - **Shared Key**: クライアントは、デバイスと同じ共有キーで設定されている必要があります。このオプションは、暗号スイートがWEP40、WEP104、またはWEP128の場合にだけ使用できます。
  - **All**: オープンシステムと共有キーの両方が構成されています。

  暗号化モードがクリアの場合、認証モードはオープンシステムである必要があります。暗号化モードが暗号化の場合、認証モードのオプションはオープンシステム、共有キー、すべてです。

- **Binding Interface**: サービスポリシーを無線論理インターフェースにバインドするかしないかを指定します。このオプションは、サービスポリシーを追加するときに選択する必要があります。サービスポリシーを変更するときに、このオプションを選択するかどうかを指定できます。
- **Interface ID**: サービスポリシーにバインドされるインターフェースIDを入力します。IDが存在しないWLAN論理インターフェースを表す場合、WSMはACまたはFAT APのWLAN論理インターフェースを自動的に作成します。サービスポリシー設定の失敗を回避するには、WLAN論理インターフェースが他のサービスポリシーにバインドされていないことを確認します。
- **Interface Type**: サービスポリシーにバインドされているインターフェースのタイプを選択します。常にWLAN-ESSです。
- **Max Clients**: サービスポリシーを使用できるクライアントの最大数を入力します。

Comwareベースのデバイスの**Security information**:

Encryption Modeで**Crypto**が選択されている場合は、次のセキュリティパラメーターを設定します。

- **Security IE**: FIT APによって送信されるビーコンフレームおよびプローブ応答で使用されるセキュリティIEを選択します。オプションは、**None**、**RSN**、**WPA**、および**All**です。
  - **None**: セキュリティIEは設定されていません。
  - **All**: RSNとWPAの両方が設定されています。
  - **RSN**: 堅牢なセキュリティネットワークは、WPAよりも強力な保護を提供するために、堅牢なセキュリティネットワークアソシエーションの作成のみを可能にするセキュリティネットワークです。
  - **WPA**: **WPAは、WPA-PSK**(パーソナル)モードまたはWPA-802.1X(エンタープライズ)モードのいずれかで動作します。パーソナルモードでは、認証に事前共有キーまたはパスフレーズが使用されます。エンタープライズモードでは、802.1Xサーバー、RADIUSサーバー、およびEAPが認証に使用されます。

RSNおよびWPAの詳細については、関連するデバイスのマニュアルを参照してください。

- **Cipher Suite**: データフレームの暗号化および復号化に使用する暗号スイートを選択します。オプションは次のとおりです。
  - **WEP**: **WEP40**、**WEP104**、および**WEP128**を含みます。どちらも静的なWEP暗号化メカニズムです。**WEP40**キーは40ビット、**WEP104**キーは104ビット、**WEP128**キーは128ビットです。WEPはRC4暗号化を使用し、ワイヤレスネットワークにアクセスするすべてのクライアントが同じキーを使用することを要求します。キーインデックスとキーを設定できるのは、**WEP40**、**WEP104**、または**WEP128**を選択した場合だけです。**WEP40**、**WEP104**、および**WEP128**を同時に選択することはできません。
  - **TKIP**: TKIPは、WEPと同様にRC4アルゴリズムを使用しますが、WLANに対してより安全な保護を提供します。
  - **CCMP**: MACプロトコルを使用したCCMP-Counterモードは、AESに基づくCBC-MACメカニズムを使用したカウンタモードで、高いセキュリティを提供します。
- **Key Index**: クライアントの認証キーインデックスを入力します。
- **Key**: クライアントの認証キーを入力します。WEP40の場合、キーは5文字の英数字の文字列です。WEP104の場合、キーは13文字の英数字の文字列です。WEP128の場合、キーは16文字の英数字の文字列です。

7. OKをクリックします。

WLANの削除

この関数を使用すると、同じSSIDを持つすべてのWLANを削除できます。ComwareベースのACおよびFat APの場合、この関数はACおよびFat AP上のサービスポリシーを削除します。

WLANを削除するには、次の手順を実行し

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > WLANs**を選択します。WLAN Listには、すべてのWLANが表示されます。
3. WLANの**Operation**アイコン をクリックします。
4. メニューから**Delete**を選択します。

バッチでWLANを削除するためのページが開きます。

5. WLANを削除するACまたはFAT APを選択します。
6. **OK**をクリックします。

Result Listには、各デバイスのWLANを削除した結果が表示されます。削除操作が失敗した場合は、操作結果をクリックして失敗の理由を表示します。

7. バッチでWLANを削除するためのページに戻るには、**Back**をクリックします。

APアクセスポートの管理

WSMを使用すると、オペレーターはAPアクセスポートを管理できます。APアクセスポートは、アクセスデバイスをAPに直接または間接的に接続します。WSMでのAPアクセスポート管理により、オペレーターは、FIT AP、FAT AP、および不正APのアクセス情報を表示し、次の管理機能を実行できます。

- **Collecting Data**: APアクセスポートからアクセスデータを収集できます。アクセスデバイスがすでにIMCに追加されていることを確認してください。
- **Managing PoE**: APアクセスポートのPoE機能をイネーブルまたはディセーブルにして、接続されたAPでコールドスタートアップまたはシャットダウンをリモートで実行できます。この機能は、PoE対応のAPアクセスポートだけでサポートされます。
- **Configuring Auto Rogue AP Isolation**: 不正なAPアクセスポートを起動またはシャットダウンし、直接接続された不正なAPのすべてのアップリンクアクセスポートを自動的にシャットダウンするように設定できます。

FIT APアクセスポートの管理

WSMでは、AP Access PortsページでFIT APアクセスポートを管理できます。

fit APアクセスポートの表示

WSMで管理されているすべてのFIT APアクセスポート、および関連するFIT APに関する情報(ステータス、名前、SN、IPアドレス、MACアドレス、アクセスデバイス、アクセスインターフェース、収集時間など)を表示できます。

fit APアクセスポートを表示するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > Resource Management > AP Access Ports**を選択します。

   AP Access Portsページが開きます。
3. **Fit AP**タブをクリックします。

Device Listページには、すべてのFIT APアクセスポートと、関連するFIT AP情報が表示されます。

Device List

- **Status**: fit APのステータス、fit APとアクセスデバイス間の接続、およびアクセスデバイスのPoEステータスを表示します。
  - **Online/Primary**アイコンは、オンラインFIT APがマスターACに接続され、マスターACによって管理されていることを示します。
  - **Online/Secondary**アイコンは、オンラインFIT APがバックアップACに接続され、バックアップACによって管理されていることを示します。
  - **Offline**アイコンは、オンラインFIT APがオフラインであることを示します。
  - **Direct Link**アイコンは、FIT APがアクセスデバイスに直接接続されていることを示します。
  - **Indirect Link**アイコンは、FIT APがアクセスデバイスに直接または間接的に接続されていることを示します。
  - **PoE Enable**アイコンは、APアクセスポートでPoEがイネーブルになっていることを示します。

- **PoE Disable**アイコン  は、APアクセスポートがPoEでディセーブルになっていることを示します。WSMにAPアクセスポートのPoEステータスが表示されるのは、アクセスデバイスがFIT APに直接接続され、アクセスデバイスがPoEをサポートしている場合だけです。
  - **AP Label**: FIT APのラベル。詳細を表示するには、デバイスラベルのリンクをクリックします。
  - **SN**: FIT APのシリアル番号。
  - **IP Address**: FIT APのIPv4アドレス。
  - **MAC Address**: FIT APのMACアドレス。
  - **Access Device**: FIT APが接続されているアクセスデバイスのラベル。詳細を表示するには、アクセスデバイスのラベルをクリックします。
  - **Access Interface**: アクセスデバイスをFIT APに接続するAPアクセスポートの名前。
  - **Collect Time** :FIT APに接続されているAPアクセスポート経由でIMCが最後にデータを収集した時刻。
  - **Operation**: Fit APのOperationアイコン  をクリックして、Operationメニューを表示します。このアイコンは、Fit APがアクセスデバイスに直接接続されている場合にだけ表示されます。

Operationメニューから、FIT APアクセスポートでPoE機能をイネーブルまたはディセーブルにできます。詳細については、「FIT APアクセスポートでのPoEの設定」を参照してください。

Device Listに十分な数のエントリーが含まれている場合は、次のナビゲーションが表示されます。

-  **Next Page**アイコンをクリックして、**Device List**の次のページに進みます。
-  **Last Page**アイコンをクリックして、**Device List**の最後までページを進めます。
-  **Previous Page**アイコンをクリックして、**Device List**で前のページに戻ります。
-  **First Page**アイコンをクリックして、**Device List**の先頭にページを戻します。

Device Listの右上にある**8**、**15**、**50**、**100**、または**200**をクリックして、各ページに表示する項目の数を指定します。

Statusおよび**Operation**フィールドを除くすべてのフィールドでDevice Listをソートできます。選択したフィールドでリストをソートするには、列ラベルをクリックします。列ラベルを使用すると、各フィールドのソートオプションを切り替えることができます。

fit APアクセスポートに関する情報の収集

この機能を使用すると、APアクセスポートに関する情報を手動で収集し、統計情報をデバイスリストに同期化できます。さらに、WSMは毎日14:00にAPアクセスポートに関する情報を自動的に収集します。

fit APアクセスポートに関する情報を収集するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > Resource Management > AP Access Ports**を選択します。

   AP Access Portsページが開きます。
3. **Fit AP**タブをクリックします。

Device Listページには、すべてのFIT APアクセスポートと、関連するFIT AP情報が表示されます。

4. **Collect Data**をクリックします。

WSMは、適合するすべてのAPアクセスポートからデータの収集を開始します。後でページを更新して、結果を表示します。

fit APアクセスポートのクエリー

この機能を使用すると、FIT APアクセスポートを特定の基準でフィルタリングできます。FIT APアクセスポートを照会するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > Resource Management > Fit AP Access Ports**を選択します。

   AP Access Portsページが開きます。
3. **Fit AP**タブをクリックします。

Device Listページには、すべてのFIT APアクセスポートと、関連するFIT AP情報が表示されます。

4. 次の問合せ基準を1つ以上指定します。
   - **AP Label**: FIT APのラベルを入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
   - **IP Address**: FIT APのIPv4アドレスの一部または全体を入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
   - **Online Status**: リストからfit AP stateを選択します。オプションは次のとおりです。
     - **Unlimited**
     - **Online**
     - **Online/Primary**
     - **Online/Secondary**
     - **Offline**

     Onlineオプションは、**Online/Primary**および**Online/Secondary**と同じです。
   - **MAC Address**: FIT APのMACアドレスの一部または全体を入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
   - **Serial Number**: FIT APのシリアル番号の一部または全体を入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
   - **Vendor**: FIT APのベンダーを選択します。オプションは次のとおりです。
   - Unlimited
     - **H3C**
   - **AC**: FIT APが接続するACを選択します。オプションはUnlimitedで、すべてのACはWSMによって管理されます。

     空のフィールドや制限なしに設定されたフィールドは、クエリーの抽出条件として使用できません。
5. **Query**をクリックします。

   Device Listには、クエリー基準に一致するすべてのFIT APアクセスポートが表示されます。
6. **Reset**をクリックしてクエリー基準をクリアし、すべてのFIT APアクセスポートを表示します。

FIT APアクセスポートの追加

この機能を使用すると、ポートがシステムによって自動的に検出されない場合に、fit APアクセスポートを手動で追加できます。

FIT APアクセスポートを追加するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > Resource Management > AP Access Ports**を選択します。

   AP Access Portsページが開きます。
3. **Fit AP**タブをクリックします。

Device Listページには、すべてのFIT APアクセスポートと、関連するFIT AP情報が表示されます。

4. **Manual Add**をクリックします。
5. **Select AP**をクリックします。開いたウィンドウで、追加するAPを選択し、OKをクリックします。選択したAPがAdd AP Access Portsリストに表示されます。
6. ターゲットAPの**Configure Access Port**アイコンをクリックします。
7. ターゲットアクセスポートを選択し、OKをクリックします。
   アクセスデバイスとアクセスポートが**Add AP Access Ports**リストに表示されます。
8. OKをクリックします。

FIT APアクセスポートのエクスポート

この機能を使用すると、デバイスリスト内のすべてのFIT APアクセスポートを.csvファイルにエクスポートし、そのファイルをローカルに保存できます。

すべてのFIT APアクセスポートをエクスポートするには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > Resource Management > AP Access Ports**を選択します。
   AP Access Portsページが開きます。
3. **Fit AP**タブをクリックします。

Device Listページには、すべてのFIT APアクセスポートと、関連するFIT AP情報が表示されます。

4. **Export**をクリックします。
5. **Export Result**アイコンをクリックして、ローカルホストでエクスポートファイルを開くか、保存します。

FIT APアクセスポートでのPoEの設定

アクセスデバイスがFIT APに直接接続され、APアクセスポートがPoE機能をサポートしている場合は、APアクセスポートでPoE機能をイネーブルまたはディセーブルにできます。

PoEテクノロジーにより、デバイスは、イーサネット銅線ポートを介して、ツイストペアケーブル接続された受電装置にリモートで電力を供給できます。

fit APアクセスポートでPoEをディセーブルにすると、外部電源を使用しない接続されたfit APは動作を停止します。

fit APアクセスポートでPoEをディセーブルまたはイネーブルにするには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > Resource Management > AP Access Ports**を選択します。
   AP Access Portsページが開きます。
3. **Fit AP**タブをクリックします。

Device Listページには、すべてのFIT APアクセスポートと、関連するFIT AP情報が表示されます。

4. PoEをイネーブルまたはディセーブルにするfit APの**Operation**アイコンをクリックします。
5. FIT APでPoEをイネーブルにするには、表示されるメニューの**Enable PoE**アイコンをクリックします。
6. fit APでPoEをディセーブルにするには、表示されるメニューの**Disable PoE**アイコンをクリックします。

FAT APアクセスポートの管理

WSMでは、AP Access PortsページでFAT APアクセスポートを管理できます。

FAT APアクセスポートの表示

WSMで管理されているすべてのFAT APアクセスポート、および関連するFAT APに関する次のような情報を表示できます。

- **Status**
- **Name**
- **SN**
- **IP address**
- **MAC address**
- **Access Device**
- **Access Interface**
- **Collect time**

FAT APアクセスポートを表示するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > Resource Management > AP Access Ports**を選択します。

   AP Access Portsページが開きます。
3. **Fat AP**タブをクリックします。

Device Listページには、すべてのFAT APアクセスポートと、関連するFAT AP情報が表示されます。

Device List

- **Status**: FAT APとアクセスデバイス間の接続、およびアクセスデバイスのPoEステータスを表示します。
  - **Direct Reality**アイコンは、FAT APがアクセスデバイスに直接接続されていることを示します。
  - **Indirect Link**アイコンは、FAT APがアクセスデバイスに直接または間接的に接続されていることを示します。
  - **PoE Enable**アイコンは、APアクセスポートでPoEがイネーブルになっていることを示します。
  - **PoE Disable**アイコンは、APアクセスポートがPoEでディセーブルになっていることを示します。

WSMは、アクセスデバイスがPoEをサポートし、FAT APに直接接続されている場合に限り、APアクセスポートのPoEステータスを表示します。

- **Device Label**: FAT APのラベル。名前をクリックすると、その詳細が表示されます。
- **SN**: FAT APのシリアル番号。
- **IP Address**: FAT APのIPv4アドレス。
- **MAC Address**: FAT APのMACアドレス。
- **Access Device**: FAT APが接続されているアクセスデバイスのラベル。ラベルをクリックすると、その詳細が表示されます。
- **Access Interface**: アクセスデバイスをFAT APに接続するAPアクセスポートの名前。

- **Collect Time**: Collect Time :IMCが、FAT APに接続されているAPアクセスポートを介して最後にデータを収集した時刻。
- **Operation**: FAT APのOperationアイコン ⋯ をクリックすると、Operationメニューが表示されます。このアイコンは、FAT APがアクセスデバイスに直接接続されている場合にだけ表示されます。

Operationメニューから、FAT APアクセスポートのPoE機能を有効または無効にできます。詳細については、「FAT APアクセスポートでのPoEの設定」を参照してください。

Device Listに十分な数のエントリーが含まれている場合は、次のナビゲーションが表示されます。

- **Next Page**アイコンをクリックして、**Device List**の次のページに進みます。
- **Last Page**アイコンをクリックして、**Device List**の最後までページを進めます。
- **Previous Page**アイコンをクリックして、**Device List**で前のページに戻ります。
- **First Page**アイコンをクリックして、**Device List**の先頭にページを戻します。

Device Listの右上にある**8**、**15**、**50**、**100**、または**200**をクリックして、各ページに表示する項目の数を指定します。

StatusおよびOperationフィールドを除くすべてのフィールドでDevice Listをソートできます。選択したフィールドでリストをソートするには、列ラベルをクリックします。列ラベルを使用すると、各フィールドに固有の様々なソートオプションを切り替えることができます。

FAT APアクセスポートに関する情報の収集

この機能を使用すると、FAT APとAPアクセスデバイス間の接続を表示し、FAT APアクセスポートに関する情報を収集できます。

FAT APアクセスポートのクエリー

この機能を使用すると、特定の基準でFAT APアクセスポートをフィルタリングできます。FAT APアクセスポートを照会するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > Resource Management > AP Access Ports**を選択します。

   AP Access Portsページが開きます。
3. **Fat AP**タブをクリックします。

Device Listページには、すべてのFAT APアクセスポートと、関連するFAT AP情報が表示されます。

4. 次の問合せ基準を1つ以上指定します。
   - **Device Label**: FAT APのラベルを入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
   - **IP Address**: FAT APのIPv4アドレスの一部または全体を入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
   - **MAC Address**: FAT APのMACアドレスの一部または全体を入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
   - **Serial Number**: FAT APのシリアル番号の一部または全体を入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
   - **Vendor**: FAT APのベンダーを選択します。オプションは次のとおりです。
     - Unlimited

– H3C

空のフィールドや**Unlimited**に設定されたフィールドは、クエリーの抽出条件として使用できません。

5. **Query**をクリックします。

Device Listには、クエリー基準に一致するすべてのFAT APアクセスポートが表示されます。

6. クエリー基準をクリアしてすべてのFAT APアクセスポートを表示するには、**Reset**をクリックします。

FAT APアクセスポートのエクスポート

この機能を使用すると、デバイスリスト内のすべてのFAT APアクセスポートを.csvファイルにエクスポートし、ファイルをローカルに保存できます。詳細については、「FIT APアクセスポートのエクスポート」を参照してください。

FAT APアクセスポートでのPoEの設定

アクセスデバイスがFAT APに直接接続され、APアクセスポートがPoE機能をサポートしている場合は、APアクセスポートでPoE機能をイネーブルまたはディセーブルにできます。詳細については、「FIT APアクセスポートでのPoEの設定」を参照してください。

不正なAPアクセスポートの管理

WSMでは、AP Access Portsページで不正なAPアクセスポートを管理できます。

不正なAPアクセスポートの表示

WSMで管理されているすべての不正APアクセスポートと、関連する不正APに関する次のような情報を表示できます。

- **Status**
- **MAC address**
- **vendor**
- **SSID**
- **Access device**
- **Access Interface**
- **Collect time**

不正なAPアクセスポートを表示するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > Resource Management > AP Access Ports**を選択します。

   AP Access Portsページが開きます。
3. **Rogue AP**タブをクリックします。

Device Listページには、すべての不正APアクセスポートと、関連する不正AP情報が表示されます。

Device List

- **Status**: 不正APのステータス、不正APとアクセスデバイス間の接続、およびアクセスデバイスのPoEステータスを表示します。
- 不正APの状態は、次のいずれかになります。
  - **Online/Primary**: オンラインの不正なAPがマスターACに接続され、マスターACによ

って管理されていることを示します。

- **Online/Secondary**は、オンラインの不正なAPがバックアップACに接続され、バックアップACによって管理されていることを示します。
- **Offline**

- **Direct Link**アイコンは、不正なAPがアクセスデバイスに直接接続されていることを示します。
- **Indirect Link**アイコンは、不正なAPがアクセスデバイスに直接または間接的に接続されていることを示します。
- **PoE Enable**アイコンは、APアクセスポートでPoEがイネーブルになっていることを示します。
- **PoE Disable**アイコンは、APアクセスポートがPoEでディセーブルになっていることを示します。

WSMは、アクセスデバイスがPoEをサポートし、FAT APに直接接続されている場合に限り、APアクセスポートのPoEステータスを表示します。

- **MAC Address**: 不正APのMACアドレス。MACアドレスをクリックすると、その詳細が表示されます。
- **Vendor**: 不正APのベンダー。
- **SSID**: 不正APがアクセスするWLANのSSID。
- **Access Device**: 不正なAPが接続されているアクセスデバイスのアクセスデバイスラベル。詳細を表示するには、アクセスデバイスラベルをクリックします。
- **Access Interface**:アクセスデバイスを不正なAPに接続するAPアクセスポートの名前。
- **Collect Time**:不正なAPに接続されているAPアクセスポート経由でIMCが最後にデータを収集した時刻。
- **Operation**:不正APの**Operation**アイコン をクリックして、Operationメニューを表示します。このアイコンは、不正APがアクセスデバイスに直接接続されている場合にだけ表示されます。

Operation メニューでは、アソシエートされた不正APアクセスポートのPoE機能をイネーブルまたはディセーブルにできます。

Device Listに十分な数のエントリーが含まれている場合は、次のナビゲーションが表示されます。

- **Next Page**アイコンをクリックして、**Device List**の次のページに進みます。
- **Last Page**アイコンをクリックして、**Device List**の最後までページを進めます。
- **Previous Page**アイコンをクリックして、**Device List**で前のページに戻ります。
- **First Page**アイコンをクリックして、**Device List**の先頭にページを戻します。

Device Listの右上にある**8**、**15**、**50**、**100**、または**200**をクリックして、各ページに表示する項目の数を指定します。

Statusおよび**Operation**フィールドを除くすべてのフィールドでDevice Listをソートできます。選択したフィールドでリストをソートするには、列ラベルをクリックします。列ラベルを使用すると、各フィールドに固有の様々なソートオプションを切り替えることができます。

不正なAPアクセスポートに関する情報の収集

この機能を使用すると、不正なAPとアクセスデバイス間の接続を表示し、APアクセスポートに関する情報を収集できます。詳細については、「FIT APアクセスポートに関する情報の収集」を参照してください。

不正なAPアクセスポートのクエリー

この機能を使用すると、不正なAPアクセスポートを特定の基準でフィルタリングでき

ます。不正なAPアクセスポートを照会するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > Resource Management > Rogue AP Access Ports**を選択します。

   AP Access Portsページが開きます。
3. Rogue APタブをクリックします。

Device Listページには、すべての不正APアクセスポートと、関連する不正AP情報が表示されます。

4. 次の問合せ基準を1つ以上指定します。
   - **MAC Address**: 不正APのMACアドレスの一部または全体を入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
   - **SSID**: 不正APがアクセスするWLANのSSIDの一部または全体を入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。

空のフィールドや制限なしに設定されたフィールドは、クエリーの抽出条件として使用できません。

5. **Query**をクリックします。

Device Listには、クエリー基準に一致するすべての不正なAPアクセスポートが表示されます。

6. クエリー基準をクリアしてすべての不正APアクセスポートを表示するには、**Reset**をクリックします。

不正なAPアクセスポートのエクスポート

この機能を使用すると、デバイスリスト内のすべての不正なAPアクセスポートを.csvファイルにエクスポートし、そのファイルをローカルに保存できます。詳細については、「FIT APアクセスポートのエクスポート」を参照してください。

不正なAPアクセスポートでのPoEの設定

アクセスデバイスが不正なAPに直接接続され、APアクセスポートがPoE機能をサポートしている場合は、APアクセスポートでPoE機能をイネーブルまたはディセーブルにできます。詳細については、「FIT APアクセスポートでのPoEの設定」を参照してください。

自動不正AP隔離の設定

セキュリティを強化するために、WSMは自動不正AP分離機能を提供します。この機能をイネーブルにすると、WSMは不正APに直接接続されているすべてのAPアクセスポートを自動的にシャットダウンします。

不正APの自動隔離を設定するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > Resource Management > Access Ports**を選択します。AP Access Portsページが開きます。
3. **Rogue AP**タブをクリックします。

Device Listページには、すべての不正APアクセスポートと、関連する不正AP情報が表示されます。

4. 不正APの自動隔離機能をイネーブルにするには、次の手順を実行します。
   a. リストの右上にある**Auto Rogue AP Isolation**をクリックします。
   b. 確認ダイアログボックスでOKをクリックします。
5. 不正APの自動隔離機能をディセーブルにするには、次の手順を実行します。

a. リストの右上にある**Cancel Rogue AP Isolation**をクリックします。
b. 確認ダイアログボックスでOKをクリックします。

IoTモジュールの管理

IoTモジュールリストには、各IoTモジュールのID、タイプ、ステータス、バージョン、シーケンスID、および各IoTモジュールが存在するIoT APが表示される。

IoTモジュールリストは、WSMにIoTモジュールが存在する場合にのみ表示されます。

IoTモジュール一覧の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > Resource Management > IoT Module List**を選択します。

   IoTモジュールリストには、すべてのIoTモジュールが表示されます。

IoTモジュール一覧

- ID-IoTモジュールのID。
- **Type**: IoTモジュールのタイプ(BluetoothまたはIoT)。IoTモジュールタイプを変更するには、**Modify**アイコンをクリックします。
- **Status**: IoTモジュールの管理ステータスUpまたはDown。IoTモジュールの管理ステータスを変更するには、**Modify**アイコンをクリックします。
- **Version**: IoTモジュールのバージョン。
- **Sequence ID**: IoTモジュールのシーケンスID。
- **AP Name**: IoTモジュールが配置されているAPの名前。AP名は、管理ACデバイスラベル->FIT APデバイスラベル形式です。IoT APの名前をクリックすると、詳細が表示されます。
- **Restart**: IoTモジュールを再起動するには、**Restart**アイコンをクリックします。
- 係数にリセットIoTモジュールのデフォルト設定を復元するには、係数に**Reset**アイコンをクリックします。

IoTモジュールのクエリー

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > Resource Management > IoT Module List**を選択します。

   IoTモジュールリストには、すべてのIoTモジュールが表示されます。
3. 次の問合せ基準のいずれかを指定します。
   - **Module Type**: モジュールタイプを入力します。
   - **AP Name**: IoTモジュールが配置されているAPの名前の一部または全体を入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。

空のフィールドは、クエリー条件として機能しません。

4. **Query**アイコンをクリックします。

   IoTモジュールリストには、クエリー基準に一致するすべてのIoTモジュールが表示されます。

ワイヤレスサービストラップを管理する

WSMを使用すると、IMCプラットフォームのトラップ管理コンポーネントを介してワイヤレストラップを一元的に管理および表示できます。ワイヤレストラップを使用すると、ワイヤレスデバイスの動作とステータスを迅速に識別し、ネットワークの問題をトラブルシューティングできます。

IMCには、定義済みのワイヤレストラップとトラップルールが用意されています。ワイヤレストラップとトラップルールはカスタマイズすることもできます。詳細については、『H3C IMC v7.3 Enterprise and Standard Platform Administrator Guide』を参照してください。

WSMでは、合計クライアント数や無線レートなどのパラメーターのトラップしきい値を構成できます。指定したしきい値に達すると、トラップが生成されます。しきい値の構成の詳細は、「アラームしきい値の設定」を参照してください。

次の情報では、Comwareベースワイヤレスデバイスの定義済みトラップについて説明します。

ワイヤレスサービスアラームの表示

1. Serviceタブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Wireless Service Alarm**を選択します。アラームリストには、すべてのワイヤレスサービスアラームが表示されます。

   ワイヤレスサービスアラームの一覧

   - **Level**: アラームのレベル: **Critical**、**Major**、**Minor**、または**Warning**。
   - **AP Source**: アラームを生成するAPのラベル。TopN Unrecovered wireless alarmsを表示するには、AP labelリンクをクリックします。
   - **Recovery Status**: アラームの回復ステータス: **Recovered**または**Unrecovered**。
   - **Alarm Description**: アラームの説明。アラームの詳細情報を表示するには、アラームの説明リンクをクリックします。詳細については、『H3C IMC v7.3 Enterprise and Standard Platform Administrator Guide』を参照してください。
   - **Alarm Time**: アラームが生成された時刻。

   ワイヤレスサービスアラームリスト(Wireless Service Alarms List)に十分なエントリーが含まれている場合は、次のナビゲーションが表示されます。

   - **Next Page**アイコンをクリックして、**Wireless Service Alarms**リストの次のページに進みます。
   - **Last Page**アイコンをクリックして、**Wireless Service Alarms List**の最後までページを進めます。
   - **Previous Page**アイコンをクリックして、**Wireless Service Alarms**リストで前のページに戻ります
   - **First Page**アイコンをクリックして、**Wireless Service Alarms**リストの先頭に戻ります。

   Wireless Service Alarms Listの右上にある**8**、**15**、**50**、**100**、または**200**をクリックして、各ページに表示する項目の数を指定します。

Wireless Service Alarms Listは、Levelフィールドを除くすべてのフィールドで並べ替えることができます。選択したフィールドでリストを並べ替えるには、列ラベルをクリックします。列ラベルを使用すると、各フィールドの並べ替えオプションを切り替えることができます。

ワイヤレスサービスアラームのクエリー

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > Wireless Service Alarm**を選択します。

このページには、すべてのワイヤレスサービスアラームが表示されます。

3. 問合せ領域で、次の問合せ基準を1つ以上指定します。
   - **Level**: アラームレベルを選択します。オプションは、**Critical**、**Major**、**Minor**および**Warning**です。
   - **Recovery Status**: リカバリステータスを選択します。オプションは、**All**、**Recovered**および**Unrecovered**。
4. **Query**をクリックします。

リストには、クエリー基準に一致するすべての無線サービスアラームが表示されます。

5. クエリー基準をクリアしてすべてのワイヤレスサービスアラームを表示するには、**Reset**をクリックします。

Comwareベースのワイヤレスデバイスの定義済みトラップ

表31に、ACトラップ、APトラップ、クライアントトラップ、セキュリティトラップ、およびNMS定義トラップを含む、Comwareベースのデバイスのすべての定義済みトラップを示します。NMS定義トラップはNMSによって生成され、その他のトラップはデバイスによって生成されます。

表31 Comwareベースのワイヤレスデバイストラップ

トラップタイプ	トラップ名	説明
ACトラップ	ACロードバランスの有効化	ACロードバランシングがイネーブルになります。
ACトラップ	時間の同期の失敗	APが時刻の同期に失敗しました。
APトラップ	AP作業モードが変更されました	APの作業モードが変更されました。
APトラップ	AP設定エラー	AP無線で設定エラーが発生しました。
APトラップ	APの干渉がなくなる	チャネル上の周囲APによる干渉がなくなりました。
APトラップ	APがチャネルに干渉する	APがチャネルに干渉しました。
APトラップ	フラッシュへのデータの書き込みに失敗しました	APがフラッシュへのデータの書き込みに失敗しました。
APトラップ	APのリブート	APがリブートしました。
APトラップ	CAPWAPトンネルダウン	ACとAP間のCAPWAPトンネルがダウンしています。
APトラップ	CAPWAPトンネルUP	ACとAP間のCAPWAPトンネルがアップしています。
APトラップ	無線ダウン	APの無線の動作ステータスがダウンです。
APトラップ	無線の回復	APの無線の動作ステータスはアップです。
APトラップ	無線チャネルが変更されました	APの無線チャネルが変更されました。
APトラップ	不正なデバイスが表示されなくなる	不正なデバイスが認識されなくなった。
セキュリティトラップ	アドホックデバイスの検出	APが不正なアドホックデバイスを検出しました。
セキュリティトラップ	不正なデバイスの検出	APが不正なAPを検出しました。
セキュリティトラップ	弱いIV攻撃の検出	ワイヤレスデバイスが弱いIV攻撃を開始しています。
セキュリティトラップ	フラッド攻撃の検出	ワイヤレスデバイスがネットワークにフラッディングしています。
セキュリティトラップ	不正なワイヤレスの検出-	APの無線で不正なデバイスが検出されました。

トラップタイプ	トラップ名	説明
	ブリッジ	不正なワイヤレスブリッジとして分類されます。
セキュリティトラップ	スプーフィング攻撃の検出	ワイヤレスデバイスがスプーフィング攻撃を開始しています。
セキュリティトラップ	未認可SSIDの検出	APが不正なSSIDを検出しました。
セキュリティトラップ	クライアントの干渉がなくなる	チャネル上のアンビエントクライアントによる干渉が解消されました。
セキュリティトラップ	クライアントがチャネルに干渉する	クライアントがチャネルに干渉しました。
セキュリティトラップ	他のデバイスの干渉がなくなる	チャネル上の周辺機器による干渉がなくなりました。
セキュリティトラップ	他のデバイスがチャネルに干渉しています	チャネル上の周辺機器による干渉が発生しました。
クライアントトラップ	ワイヤレスクライアントのアソシエーションの失敗	APの無線に接続されているクライアントでアソシエーション障害が発生しました。
クライアントトラップ	ワイヤレスクライアントの関連付け解除	APの無線に接続されているクライアントでアソシエーション解除が発生しました。
クライアントトラップ	ワイヤレスクライアント認証エラー	APの無線に接続されているクライアントで認証エラーが発生しました。
クライアントトラップ	ワイヤレスクライアント認証の成功	APの無線に接続されているクライアントが認可されます。
クライアントトラップ	ワイヤレスクライアント認証の失敗	APの無線に接続されているクライアントを認証できませんでした。
クライアントトラップ	ワイヤレスクライアントがいっぱいです	APに関連付けられたクライアントの数が、BSSの制限、無線の制限、無線の同時接続の制限、無線ポリシーで設定された制限、ACの制限、ACの同時接続の制限、またはプロトコルの制限のいずれかに達しました。
クライアントトラップ	ワイヤレスクライアントの完全復旧	APに関連付けられたクライアントの数が、BSSの制限、無線の制限、無線の同時接続の制限、無線ポリシーで設定された制限、ACの制限、ACの同時接続の制限、またはプロトコルの制限のいずれかの制限を下回る値に回復しました。
クライアントトラップ	クライアントステーションのアソシエーション解除に成功しました。	APの無線に接続されているクライアントが、APからアソシエート解除されました。
クライアントトラップ	ワイヤレスクライアントのMICエラー	AP無線に接続されているワイヤレスクライアントでMIC障害が発生しました。
NMS定義のトラップ	APデバイスオンライン	NMSが、APがオンラインであることを検出しました。
NMS定義のトラップ	APデバイスがオフライン	NMSが、APがオフラインであることを検出しました。
NMS定義のトラップ	iNodeクライアントがアクセスポリシーに従わない	NMSは、iNodeユーザーが領域のアクセスポリシーに従わなかったことを検出しました。

WLANパフォーマンスの監視

WSMは、次のWLANパフォーマンスモニタリング機能を提供します。

- 基本的なパフォーマンス監視インデックス

  ワイヤレスデバイスのパフォーマンスを監視するには、WSMをIMCプラットフォーム上のパフォーマンス管理モジュールと統合する必要があります。WSMが展開されると、IMCプラットフォームはワイヤレスデバイスのCPU、メモリー、およびその他のパフォーマンスインデックスをリアルタイムで監視し、監視情報をグラフで表示できます。

  WLANパフォーマンス監視タスクを作成して、Comwareベースのワイヤレスデバイスのこれらのインデックスタイプを監視できます。

- WSMに組み込まれた設定可能なモニタリングインデックス

  WSMには、WLANパフォーマンス監視用の組み込みの監視インデックスが用意されています。これらのインデックスは、WLANサービス概要ページ、IMCホームページのWLANウィジェット、WLANサービスレポート、Webサービス、およびネットワーク評価ページで設定できます。WLANパフォーマンスインデックスの監視は、WLANサービス概要ページ、WLANサービスレポート、Webサービスインターフェース、およびネットワーク評価ページで開始および停止できます。

- WSMでのリアルタイム監視

  WSMは、管理可能なComwareベースのFIT AP、およびオンラインクライアントのリアルタイムモニタリングを提供します。

  ここでは、WSMでのWLANパフォーマンスモニタリングの主要な管理機能について説明します。

基本的なパフォーマンス監視インデックス

WSMが展開されると、IMCプラットフォームはWLANパフォーマンス監視インデックス(表32)をサポートします。これらのインデックスを追加して、IMCプラットフォームのパフォーマンス管理モジュールでワイヤレスデバイスのパフォーマンスを監視できます。

表32 WLANパフォーマンス監視インデックス

索引の種類	インデックスの監視
WLAN-AC統計情報	• ACに接続しているAPの数 • ACに接続するステーションの数 • ACでユーザーソシエーションが成功した回数 • ACでユーザーソシエーションが失敗した回数 • ACでユーザーソシエーションが拒否された回数 • ACでのユーザー再関連付けの数 • ACでの例外的なクライアント認証解除の数
WLAN-Radio Rate Statistics	• 無線受信重複フレーム率(フレーム/秒) • 無線受信レート(フレーム/秒) • 無線受信ブロードキャストレート(フレーム/秒) • 無線受信マルチキャストレート(フレーム/秒) • 無線受信レート(b/s) • 無線受信管理フレームレート(フレーム/秒) • 無線受信制御フレームレート(フレーム/秒) • 無線受信データフレームレート(フレーム/秒) • 無線送信レート(フレーム/秒) • 無線送信ブロードキャストレート(フレーム/秒)

	• 無線送信マルチキャストレート(フレーム/秒) • 無線送信レート(b/s)
WLAN-Radio Traffic Statistics	• 無線で受信された重複フレームの数 • 無線で受信されたフレーム数 • 無線で受信されたブロードキャストフレームの数 • 無線で受信されたマルチキャストフレームの数 • 無線によって廃棄されたフレームの数 • 無線で受信されたFCSエラーのあるフレームの数 • 無線で受信された管理フレームの数 • 無線で受信されたバイト数 • 無線で受信された制御フレームの数 • 無線で受信されたデータフレームの数 • 無線復号化エラーフレーム数 • 無線で送信されるフレーム数 • 無線で送信されるブロードキャストフレームの数 • 無線で送信されるマルチキャストフレームの数 • 無線で送信された廃棄フレームの数 • 無線で送信されるバイト数 • 無線によって廃棄されるフレームのバイト数 • 受信したデータフレームのバイト数 • 送信されたデータフレームのバイト数 • 無線で受信されたエラーフレームの数
WLAN-Radio PerformanceStatistics	• 廃棄された受信フレームの割合(%) • 受信したFCSフレームの割合(%) • 無線復号化エラーの割合(%) • 破棄された送信フレームの割合(%) • 成功したRTS送信の数 • 失敗したRTS送信の数 • 失敗したACK送信の数 • 無線送信障害数 • 無線送信の再試行回数 • エラーフレームの受信率(%) • 送信された関連フレームの数 • 受信した関連フレームの数 • 物理受信エラー数 • MIC検証エラーの数 • 無線リソース使用率(%)
WLAN-Radio Statistics(SSID)	• このBSS(SSID)で受信されたフレームの数 • このBSS(SSID)で受信されたフレームのバイト数 • このBSS(SSID)で受信されたデータフレームの数 • このBSS(SSID)で受信されたフレームのバイト数 • このBSS(SSID)で送信されたフレーム数 • このBSS(SSID)で送信されたデータフレームのバイト数 • このBSS(SSID)で送信されたデータフレームの数 • このBSS(SSID)で送信されたフレームのバイト数 • このBSS(SSID)とのユーザーソシエーションの総数 • このBSS(SSID)でのユーザー受信の数 • このBSS(SSID)でのユーザーソシエーションの成功率 • このBSS(SSID)での例外的なクライアントの認証解除率 • このBSS(SSID)に関連付けられている現在のクライアント数

	• このBSS(SSID)のバイト受信レート(ビット/秒) • このBSS(SSID)の送信バイトレート(ビット/秒)
WLAN-Station Traffic Statistics	• ステーション受信レート(フレーム/秒) • ステーション送信レート(フレーム/秒) • ステーションドロップフレームレート(フレーム/秒) • ステーション受信レート(b/s) • ステーション送信レート(b/s) • ステーションのコマ落ち率(b/s) • ステーションが受信したフレーム数 • ステーション別送信フレーム数 • ステーションが受信したバイト数 • 送信バイト数(ステーション別) • ステーションの信号強度(dBm) • ユーザーが受信した合計バイト数 • 受信フレームの信号強度とノイズ強度の比率(%) • ステーション送信レート(Mb/秒) • ステーション受信レート(Mb/s)
WLAN-Fit AP Statistics	CPU使用率(%)
WLAN-AP Accumulate Statistics	• オンラインユーザー数 • ユーザー関連付けの成功回数 • 失敗したユーザーソシエーションの回数 • ユーザー関連付けの拒否回数 • ユーザーの再関連付け回数 • このAPでの例外的なクライアント認証解除の数 • 全ユーザーの継続時間の合計
WLAN-Fit AP Eth Interface Statistics	• 受信したパケット数 • 受信された廃棄パケット数 • バイト受信レート(b/s) • バイト送信レート(b/s) • 受信バイト数 • 送信バイト数

WSMでの組み込みモニタリングインデックスの設定

この情報では、Comwareベースのワイヤレスデバイスの設定可能な監視インデックスについて説明します。WLAN監視設定の詳細については、「ネットワーク管理の設定」を参照してください。

Comwareベースのワイヤレスデバイス用に設定可能な監視インデックス

Comwareベースのワイヤレスデバイスでは、次の設定可能なモニタリングインデックスを使用できます。

- WLANサービスレポートの監視インデックス(表37)
- Webサービスインターフェースの索引の監視(表38)
- WLANサービスの概要ページの監視インデックス(表39)
- ネットワーク評価のためのモニターインデックス(表40)

表37 WLANサービスレポートの監視インデックス

索引の種類	インデックスの監視
AP Association Summary report/AP Association Detail report	• 無線で受信されたアソシエーションフレームの数 • 無線で送信されるアソシエーションフレームの数 • 成功した関連付けの数 • 異常なアソシエーション解除の数
AP Traffic Summary report/AP Traffic Detail report	• インターフェース(AC/Fat AP)で受信されたエラーパケットの数 • インターフェースが受信したバイト数(AC/Fat AP) • インターフェース(AC/Fat AP)によって送信されたバイト数 • インターフェース(AC/Fat AP)によって送信されたパケット数 • 無線で受信されたフレーム数 • 無線で受信されたバイト数 • 無線で送信されるバイト数 • 無線で受信されたエラーパケットの数 • インターフェースが受信したパケット数(Fit AP) • Number of Discarded Packets Received by the Interface(Fit AP)(インターフェースが受信した廃棄パケットの数(Fit • インターフェースが受信したバイト数(Fit AP) • インターフェースによって送信されたバイト数(Fit AP)
AP Speed Report/Radio Speed Report	• 無線受信レート • 無線伝送レート
Radio Traffic Report	• 無線で受信されたバイト数 • 無線で送信されるバイト数
Radio Error Report	• 無線で受信されたFCSエラーのあるフレームの数 • 無線のエラーフレーム比 • 無線で受信された物理エラーのあるフレームの数 • MICチェックエラーの数
Radio Resource Usage Report	• 無線リソース使用率
Client Number Trendline Report	• オンラインユーザー

SSID Statistic Report (hour report)	• SSIDが受信したバイト数 • SSIDによって送信されたバイト数 • このBSS(SSID)に現在関連付けられているクライアントの数
AC Statistic Report	• インターフェース受信レート(AC/Fat AP) • インターフェース伝送レート(AC/Fat AP) • インターフェースが受信したバイト数(AC/Fat AP) • インターフェース(AC/Fat AP)によって送信されたバイト数 • 無線伝送レート • 無線のエラーフレーム比 • 無線で受信されたアソシエーションフレームの数 • パケット再送信率 • 成功した関連付けの数 • オンラインユーザー • 異常なアソシエーション解除の数 • アソシエーションの失敗の理由
Hotspot Statistic Report	• 無線受信レート • 無線伝送レート • 無線で受信されたバイト数 • 無線で送信されるバイト数 • 無線のエラーフレーム比 • 無線で受信されたアソシエーションフレームの数 • パケット再送信率 • 成功した関連付けの数 • オンラインユーザー • 異常なアソシエーション解除の数 • アソシエーションの失敗の理由
AP Statistic Report (hour report)	• インターフェースが受信したバイト数(AC/Fat AP) • インターフェース(AC/Fat AP)によって送信されたバイト数 • 無線受信レート • 無線伝送レート • 無線で受信されたバイト数 • 無線で送信されるバイト数 • 無線のエラーフレーム比 • 無線で受信されたアソシエーションフレームの数 • 無線で送信されるアソシエーションフレームの数 • パケット再送信率 • 成功した関連付けの数 • オンラインユーザー • 異常なアソシエーション解除の数 • インターフェースが受信したバイト数(Fit AP) • インターフェースによって送信されたバイト数(Fit AP) • アソシエーションの失敗の理由

表38 Webサービスインターフェースの索引の監視

索引の種類	インデックスの監視
AC Performance	• インターフェース受信レート(AC/Fat AP) • インターフェース伝送レート(AC/Fat AP) • インターフェース(AC/Fat AP)によって廃棄される入力パケットの数 • インターフェース(AC/Fat AP)によって廃棄される出力パケットの数 • インターフェースが受信したバイト数(AC/Fat AP) • インターフェース(AC/Fat AP)によって送信されたバイト数 • ACに接続されているAPの数 • インターフェース(AC/Fat AP)によって送信されたユニキャストの数 • インターフェース(AC/Fat AP)によって送信されたブロードキャストの数 • インターフェース(AC/Fat AP)で受信されたユニキャストの数 • インターフェース(AC/Fat AP)で受信されたブロードキャストの数
AC Performance By SSID	• 無線で受信されたフレームの数(SSID) • 無線で送信されたフレーム数(SSID) • 無線のバイト受信レート(SSID) • 無線のバイト伝送レート(SSID)
AP Performance	• インターフェース受信レート(AC/Fat AP) • インターフェース受信レート(AC/Fat AP) • インターフェース(AC/Fat AP)によって廃棄される入力パケットの数 • インターフェースが受信したバイト数(AC/Fat AP) • インターフェースが受信したバイト数(AC/Fat AP) • インターフェースで受信されたパケット数(AC/Fat AP) • 無線受信レート • 無線伝送レート • 無線で受信されたフレーム数 • 無線で受信されたバイト数 • 無線で送信されたフレーム数 • 無線によって廃棄された送信フレームの数 • 無線で送信されるバイト数 • 成功した関連付けの数 • アソシエーションの失敗の数 • アソシエーションの失敗の数 • 再関連付けの数 • ユーザー接続時間 • インターフェースが受信したパケット数(Fit AP) • Number of Discarded Packets Received by the Interface(Fit AP)(インターフェースが受信した廃棄パケットの数(Fit • インターフェースのバイト受信レート(Fit AP) • インターフェースのバイト伝送レート(Fit AP) • インターフェースが受信したバイト数(Fit AP) • インターフェースによって送信されたバイト数(Fit AP) • 再関連付けの総数 • 無線送信エラーフレーム • 認証に合格したクライアントの数 • 認証要求の数 • 成功した認証の数

索引の種類	インデックスの監視
AP Performance By SSID	• SSIDが受信したバイト数 • 無線で送信されたフレーム数(SSID) • 無線リソース使用率(SSID)の比率

表39 WLANサービスの概要ページの監視インデックス

索引の種類	インデックスの監視
Online History	オンラインユーザー
AP Bandwidth	• 無線受信レート • 無線伝送レート
Reasons for Association Failures	アソシエーションの失敗の理由
Association Failures	アソシエーションの失敗の数

表40 ネットワーク評価のためのモニターインデックス

索引の種類	インデックスの監視
AP Monitor Items	• 無線受信レート • 無線伝送レート • 無線で受信されたバイト数 • 無線で送信されるバイト数 • 発信パケット損失率 • 無線のエラーフレーム比 • 無線で受信されたアソシエーションフレームの数 • パケット再送信率 • 成功した関連付けの数 • アソシエーションの失敗の数 • 拒否された関連付けの数 • 再関連付けの数 • オンラインユーザー • 異常なアソシエーション解除の数 • 異常なアソシエーション解除の数

WSMでのリアルタイム監視

この情報では、デバイスタイプに基づいてワイヤレスデバイスのリアルタイムモニタリングを設定する方法について説明します。

FIT APをリアルタイムで監視

WSMは、ComwareベースのFit APをリアルタイムで監視し、APタブとRadioタブに監視情報を表示します。ComwareベースのFit APをリアルタイムで監視する方法については、「Fit APをリアルタイムで監視する」を参照してください。

リアルタイムでのクライアントの監視

WSMは、クライアントのリアルタイム監視を提供します。監視されるオブジェクトは、クライアントにWLANアクセスを提供するAPのベンダーによって異なります(表41を参照)。リアルタイムでのクライアントの監視については、「クライアントのリアルタイム監視の実行」を参照してください。

表41 クライアントのリアルタイム監視オブジェクト

APベンダー	リアルタイム監視オブジェクト
Comwareベース	• 送受信レートトレンドグラフ • 信号強度トレンドグラフ • 受信ノイズトレンドグラフ • 信号/雑音強度比トレンドグラフ • パケットの受信 • 受信レート • パケットの送信 • 送信速度 • 受信した再送信バイト数 • 送信された再送信バイト数 • 信号強度(dBm) • 受信ノイズ • ユーザー接続時間 • 信号とノイズの強度比

ワイヤレス表示の管理

WSMには、次のビュー管理機能があります。

- **Location view**: APを物理的な場所に従ってグループで管理します。これは、RFおよびワイヤレスロケーションを含むワイヤレス管理の基盤です。
- **Cuatom view**: 同じACにグループで接続されたFIT APを管理します。カスタムビューを使用すると、ターゲットデバイスに焦点を当て、そのトポロジーを表示できます。
- **GIS view**: ロケーションビュー上の位置をデフォルトマップにマッピングし、各ロケーションビューのアドレス、電話番号、APの総数、および端末の総数を動的に表示します。

ロケーションビューを管理する

この機能を使用すると、ロケーションビューを作成し、そのビューにデバイスを追加できます。ロケーションビューには、デバイスビューとサブロケーションビューが含まれます。各サブロケーションビューには、さらに無制限のレベルのデバイスビューとサブロケーションビューが含まれます。ロケーションビューはルートディレクトリに類似しており、サブロケーションビューはサブディレクトリに類似しています。

この機能では、ロケーションビューまたはサブロケーションビューをホットスポットとして設定することもできます。

ロケーションリストを表示する

ロケーションリストには、ステータス、名前、トポロジーなど、IMCで管理されているすべてのロケーションビューに関する情報が表示されます。ロケーションビューは、Location Viewsページで変更および削除できます。

ロケーションリストを表示するには、次の手順を実行します。

1. Serviceタブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>View Management > Location Views**を選択します。ロケーションリストには、すべてのロケーションビューが表示されます。

   Location List contents:

   - **Status**: ロケーションビューのステータス。アラームレベルが最も高いAPのステータスによって異なります。ロケーションビューにデバイスが含まれていない場合、ステータスは**Unmanaged**になります。ステータスアイコンをクリックすると、Top 10 unrecoveredアラームが表示されます。
   - **Location Name**: IMCプラットフォーム上のロケーションビューを識別するロケーション名。詳細を表示するには、ロケーションビューの名前をクリックします。
   - **Total APs**: APの総数。
   - **Online Fit APs**: Online Fit APの総数。
   - **Offline Fit AP**: オフラインFit APの合計数。
   - **Clients**: ロケーションビュー内のAPに関連付けられているクライアントの総数。
   - **View Topology**: 位置ビューの**View Topology**アイコンをクリックして、トポロジーを表示します。
   - **Modify**: 位置ビューの**Modify**アイコンをクリックして、パラメーターを修正します。
   - **Delete**: ロケーションビューを削除するには、**Delete**アイコンをクリックします。

Location Listに十分な数のエントリーが含まれている場合は、次のナビゲーション支援が表示されます。

- **Next Page**アイコンをクリックすると、Location Listの次のページに進みます。

- **Last Page**アイコンをクリックして、Location Listの最後までページを進めます。
- **Previous Page**アイコンをクリックして、Location Listで前のページに戻ります。
- **First Page**アイコンをクリックして、Location Listの前面にページを移動します。

位置リストの右上にある**8**、**15**、**50**、**100**、または**200**をクリックして、各ページに表示する項目の数を指定します。

Statusおよび**Location Name**フィールドで**Location List**をソートできます。選択したフィールドでリストをソートするには、列ラベルをクリックします。列ラベルを使用すると、各フィールドに固有のソートオプションを切り替えることができます。

ロケーションビューのクエリー

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > Location Views**を選択します。ロケーションリストには、すべてのロケーションビューが表示されます。
3. ロケーションビューを入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
4. **Query**アイコンをクリックします。**Device List**に、クエリー基準に一致するすべてのロケーションビューが表示されます。
5. **Query**フィールドをクリアし、**Query**アイコンをクリックしてすべてのロケーションビューを表示します。

ロケーションビューの詳細の表示

この機能を使用すると、ロケーションビューおよびサブロケーションビューでFIT APおよびFAT APを表示できます。ロケーションビューに関する詳細情報を表示するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > Location Views**を選択します。**Location List**には、すべてのロケーションビューが表示されます。
3. ターゲットロケーションビューの名前をクリックして、詳細を表示します。

   このページの上部には、**Client Count**グラフと**Count Clients**領域が表示されます。

   - **Client Count:** 指定した時間範囲内のオンラインクライアント数の傾向を表示します。
   - **Count Clients**: ベンダー別のクライアントの数と割合。

   Sub-location/Device Listには、ロケーションビューのすべてのサブロケーションとデバイスが表示されます。

   Sub-location/Device List contents:

   - **Status**:サブロケーションビューでのAPの最高アラームステータス、またはAPのオンラインステータス。オプションは次のとおりです。
     - **Online**アイコン: Fit APはオンラインです。
     - **Offline**アイコン: Fit APはオンラインではありません。

     サブロケーションビューでTop 10 unrecovered alarmsを表示するには、サブロケーションビューのステータスアイコンをクリックします。
   - **Device Status**: サブロケーションビューの場合、このフィールドには、ビュー内のAPによって生成されたアラームの最高レベルが表示されます。APの場合、このフィールドに

はAPのアラームレベルが表示されます。

- **Locating AP**: APがロケーションAPであるかどうかを示します。オプションには、**Yes** および**No**があります。ロケーション認識ロケーションに参加できるのは、ロケーション APのみです。ロケーション認識ロケーションの詳細は、「ロケーション認識ロケーション」を参照してください。
- **Device List**: サブロケーションビューまたはAPの名前。デフォルトでは、AP名はAPのシステム名です。サブロケーションビューまたはAPの名前をクリックすると、その詳細が表示されます。
- **SN**: APのシリアル番号。サブロケーションの場合、このフィールドは空です。
- **Model:** APのモデル。サブロケーションの場合、このフィールドは空です。
- **IP Address**: APのIPアドレス。サブロケーションの場合、このフィールドは空です。
- **IPv6 Address**: APのIPv6アドレス。サブロケーションの場合、このフィールドは空です。
- **MAC Address**: APのMACアドレス。サブロケーションの場合、このフィールドは空です。
- **Online Clients**: ロケーションビューでAPに関連付けられているオンラインクライアントの数。すべてのオンラインクライアントを表示するには、この数をクリックします。サブロケーションの場合、このフィールドは空です。
- **Operation**: **Operation**メニューを表示するには、サブロケーションまたはAPの**Operation**アイコン ▪▪▪ をクリックします。

サブロケーションの場合、Operationメニューには次の操作タスクが表示されます。

- **Modify**
- **Delete**
- **View Topology**

APの場合、**Operation**メニューに表示される操作タスクは次のとおりです。

- **View Topology**
- **Ping**
- **TraceRoute**
- **Locate to Map**

Sub-location/Device Listに十分なエントリーが含まれている場合は、次のナビゲーションツールが表示されます。

- **Next Page**アイコンをクリックして、**Sub-location/Device List**で次のページに進みます。
- **Last Page**アイコンをクリックして、**Sub-location/Device List**の最後に進みます。
- **Previous Page**アイコンをクリックして、**Sub-location/Device List**で前のページに戻ります。
- **First Page**アイコンをクリックして、**Sub-location/Device List**の先頭に戻ります。

Sub-location/Device Listの右上にある**8**、**15**、**50**、**100**、または**200**をクリックして、各ページに表示する項目の数を指定します。

Sub-location/Device Listは、Operationフィールドを除くすべてのフィールドでソートできます。選択したフィールドでリストをソートするには、列ラベルをクリックします。列ラベルを使用すると、各フィールドに固有のソートオプションを切り替えることができます。

ロケーションビューを追加する

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > Location Views**を選択します。**Location List**には、すべてのロケーションビューが表示されます。

3. **Add**をクリックします。

   Add Locationページが開きます。

4. 必要に応じて、次のパラメーターを設定します。
   - **Location Name**: ロケーションビューを一意に識別する名前を入力します。
   - **Location Type**: ロケーションビューのタイプを選択します。オプションは次のとおりです:
     - Area
     - Building
     - Floor
     - Room
   - **Hotspot**: ロケーションビューがGISホットスポットであるかどうかを設定します。ホットスポットは、それに属するすべてのAPを管理します。サブロケーションビューを含めることはできません。サブロケーションビューは、ホットスポットが関連付けられていないロケーションビューにのみ追加できます。

   ホットスポットの拡張プロパティを構成する必要があります。詳細については、「ロケーションビューに関連付けられたホットスポットの拡張プロパティの構成」を参照してください。
   - **Automatically Match Virtual AP**: 仮想APと同じ名前を持つAPをロケーションビューに自動的に追加するには、このオプションを選択します。APは仮想APと同じ場所に配置されます。
   - **Set to Locating AP**: このオプションを選択すると、ビューに追加されたAPが自動的にロケーションAPとして設定されます。
   - **Automatically Add AP**: ロケーションビューにAPを自動的に追加するには、このオプションを選択します。AP一致ルールを設定する必要があります。
     - **Start IP Address/End IP Address**: APのIPアドレス範囲を入力します。開始IPアドレスと終了IPアドレスは、同じ形式にする必要があります。
     - **AP Model**: APモデルを入力します。
     - **AP Name**: AP名を入力します。

   一致ルールをさらに追加するには、**Add**をクリックします。一致ルールを削除するには、**Delete**をクリックします。
5. **OK**をクリックします。

位置ビューを修正する

この機能を使用すると、ロケーションの名前とタイプを変更し、そのロケーションをホットスポットとして設定するかどうかを選択できます。

サブロケーションビューを含むロケーションビューは、ホットスポットとして設定できません。ロケーションビュー

ーを変更するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > Location Views**を選択します。**Location List**には、すべてのロケーションビューが表示されます。
3. ターゲットロケーションビューの**Modify**アイコンをクリックします。**Modify Location**ページが開きます。
4. 必要に応じてロケーションビューのパラメーターを設定します。

   詳細については、「ロケーションビューを追加する」を参照してください。
5. **OK**をクリックします。

ロケーションビューを削除する

ロケーションビューを削除すると、そのサブロケーションビューがすべて削除されます。ロケーションビューおよびそのサブロケーションビュー上のデバイスはビューから削除されますが、WSMからは削除されません。

GISホットスポットに関連付けられたロケーションビューを削除すると、GISビュー上の対応するホットスポットが削除されます。

ロケーションビューを削除する手順は、次のとおりです。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > Location Views**を選択します。

   Location Listには、すべてのロケーションビューが表示されます。
3. ロケーションビューの**Delete**アイコンをクリックします。
4. 確認ダイアログボックスで、**OK**をクリックします。

サブロケーションビューを追加する

この機能を使用すると、ロケーションビューまたはサブロケーションビューにサブロケーションビューを追加できます。ホットスポットに関連付けられたロケーションビューにサブロケーションビューを追加することはできません。

サブロケーションビューを追加するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > Location Views**を選択します。

   Location Listには、すべてのロケーションビューが表示されます。
3. 次のいずれかの方法で手順を続行します。
   - ターゲットロケーションビューの名前をクリックします。

     Sub-location/Device Listページが開きます。
   - **Sub-location/Device List**ページで、ターゲットサブロケーションビューの名前をクリックします。

     Sub-location/Device Listページが開きます。
4. **More**をクリックし、**Add Sub-location**を選択します。

   Add Location」ページが開きます。
5. 次のパラメーターを設定します。
   - **Location Name**: サブロケーションビューを一意に識別する名前を入力します。
   - **Location Type**: サブロケーションビューのロケーションタイプを選択します。オプションは次のとおりです。
     - **Area**
     - **Building**
     - **Floor**
     - **Room**

オプションは、ロケーションタイプによって異なります。

- **Hotspot**: サブロケーションビューがGISホットスポットであるかどうかを設定します。ホットスポットは、それに属するすべてのAPを管理します。サブロケーションビューを含めることはできません。サブロケーションビューは、ホットスポットが関連付けられていないロケーションビューにのみ追加できます。

ホットスポットに定義されている拡張プロパティを構成する必要があります。詳細については、「ロケーションビューに関連付けられたホットスポットの拡張プロパティの構成」を参照してください。

- **Automatically Add AP**: サブロケーションビューにAPを自動的に追加するには、このオプションを選択します。

APー致ルールを設定する必要があります。

- **Start IP Address/End IP Address**: APのIPアドレス範囲を入力します。開始IPアドレスと終了IPアドレスは、同じ形式にする必要があります。
- **AP Model**: APモデルを入力します。
- **AP Name**: AP名を入力します。

APー致ルールをさらに追加するには、**Add**をクリックします。APー致ルールを削除するには、Deleteをクリックします。

6. **OK**をクリックします。

サブロケーションビューの変更

この機能を使用すると、ロケーションビューのサブロケーションビューを変更できます。サブロケーションビューにサブロケーションビューが含まれている場合、ホットスポットとして設定することはできません。

サブロケーションビューを変更する手順は、次のとおりです。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > Location Views**を選択します。**Location List**には、すべてのロケーションが表示されます。
3. 次のいずれかの方法で手順を続行します。
   - ターゲットロケーションビューの名前をクリックします。

     Sub-location/Device Listページが開きます。
   - **Sub-location/Device List**ページで、ターゲットサブロケーションビューの名前をクリックします。

     Sub-location/Device Listページが開きます。
4. 変更するサブロケーションビューの**Operation**アイコン ··· をクリックします。
5. メニューから**Modify**アイコンを選択します。

   Modify Locationページが開きます。
6. サブロケーションビューのパラメーターを設定します。

詳しくは、『サブロケーションビューの追加』を参照してください。

7. **OK**をクリックします。

サブロケーションビューの削除

サブロケーションビューを削除すると、そのサブロケーションビューがすべて削除されます。サブロケーションビューおよびそのサブロケーションビュー上のAPは、他のロケーションビューまたはWSMからではなく、サブロケーションビューから削除されます。

ホットスポットに関連付けられたサブロケーションビューを削除すると、GISビュー上のホットスポットが削除されます。サブロケーションビューを削除するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > Location Views**を選択します。**Location List**には、すべてのロケーションビューが表示されます。
3. 次のいずれかの方法で手順を続行します。
   - ターゲットロケーションビューの名前をクリックします。

     Sub-location/Device Listページが開きます。
   - **Sub-location/Device List**ページで、ターゲットサブロケーションビューの名前をクリックします。

     Sub-location/Device Listページが開きます。
4. 次のいずれかの方法で手順を続行します。
   - 削除するサブロケーションビューを選択し、**Remove**をクリックします。
   - 削除するサブロケーションビューの**Operation**アイコン をクリックしショートカットメニューから**Delete**アイコンをクリックします。
5. 確認ダイアログボックスで、**OK**をクリックします。

ロケーションビューまたはサブロケーションビューへのAPの追加

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > Location Views**を選択します。**Location List**には、すべてのロケーションビューが表示されます。
3. 次のいずれかの方法で手順を続行します。
   - ターゲットロケーションビューの名前をクリックします。

     Sub-location/Device Listページが開きます。
   - **Sub-location/Device List**ページで、ターゲットサブロケーションビューの名前をクリックします。

     Sub-location/Device Listページが開きます。
4. **Add**をクリックします。

   Select Devicesページが開きます。
5. APをクエリーするには、次のクエリー基準を1つ以上入力または選択します。
   - **Device Label:** APのデバイスラベルを入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
   - **Device Type**: APタイプを選択します。オプションは、Fat APおよびFit APです。
   - **Serial Number**: FIT APのシリアル番号を入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
   - **IP Address**: FIT APのIPv4アドレスの一部または全体を入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
   - **Model**: APモデルを選択します。オプションはUnlimitedで、すべてのAPモデルをWSMで使用できます。
   - **Online Status**: FIT APのオンラインステータスを選択します。オプションは次のとおりです。
     - **Unlimited**
     - **Online**
     - **Offline**

- **AC**: FIT APを管理するACを選択します。オプションは**Unlimited**およびWSMのすべてのACです。空のフィールドまたはUnlimitedに設定されたフィールドは、クエリー条件として機能しません。

6. **Query**をクリックします。**Device List**には、クエリー基準に一致するすべてのAPが表示されます。クエリー基準をクリアし、現在のロケーションビューまたはサブロケーションビューにすべてのAPを表示するには、**Reset**をクリックします。
7. 追加するAPを選択します。
8. **OK**をクリックして、選択したAPをロケーションビューまたはサブロケーションビューに追加します。選択したすべてのAPが**Sub-location/Device List**に表示されます。

注:

APを追加できるのは、1つのロケーションビューだけです。

ロケーションビューからのAPまたはサブロケーションビューの削除

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > Location Views**を選択します。**Location List**には、すべてのロケーションビューが表示されます。
3. ターゲットロケーションビューの名前をクリックします。
   Sub-location/Device Listページが開きます。
4. ロケーションビューから削除するAPまたはサブロケーションを選択します。
5. **Remove**をクリックします。
6. 確認ダイアログボックスで、**OK**をクリックします。

注:

ロケーションビューからデバイスを削除すると、デバイスはロケーションビューからのみ削除され、他のロケーションビューまたはWSMからは削除されません。デバイスを削除すると、WSMからデバイスが削除されますが、IMCはデバイスを管理します。

APを配置APまたは非配置APとして設定する

ロケーションビューでAPをロケーションAPまたは非ロケーションAPとして設定するには、次の作業を実行します。ロケーション認識ロケーションに参加できるのは、ロケーションAPだけです。非ロケーションAPには、リアルタイムロケーションライセンスは必要ありません。ロケーション認識ロケーションの詳細については、「ロケーション認識ロケーション」を参照してください。

ロケーションリストまたはロケーションビュー トポロジーから、APをロケーションAPまたは非ロケーションAPとして設定できます。

APを配置APまたは非配置APとして設定するには、次の手順を実行します。

Method 1:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > Location Views**を選択します。**Location List**には、すべてのロケーションビューが表示されます。

3. 次のいずれかの方法で手順を続行します。
   - ターゲットロケーションビューの名前をクリックします。

     Sub-location/Device Listページが開きます。
   - **Sub-location/Device List**ページで、ターゲットサブロケーションビューの名前をクリックします。

     Sub-location/Device Listページが開きます。
4. ターゲットAPを選択し、**Set to Locating AP/Set to Non-Locating AP**をクリックします。

ページの右上隅に、操作が成功したかどうかを示すプロンプトが表示されます。

Method 2:

1. ナビゲーションツリーから、**WLAN Manager > Wireless Topology**を選択します。ワイヤレスデバイストポロジーウィンドウが開きます。
2. 左側のナビゲーションツリーから、**Topology > Wireless Topology > Location View**の順に選択します。ロケーションビュー トポロジーには、すべてのロケーションビューが表示されます。
3. ターゲットのロケーションビューのアイコンをダブルクリックするか、ロケーションビューのアイコンを右クリックして、ショートカットメニューから**Open Topology**を選択します。
4. ツールバーの**Set AP locating mode**アイコンをクリックします。
5. ターゲットAPを選択し、**Set to Locating AP**または**Set to Non-Locating AP**ボタンをクリックします。操作の結果は、ページ下部のメッセージフィールドに表示されます。

ロケーションビューの履歴情報の照会

この関数を使用すると、指定したデータ収集期間内の次の情報を問い合わせることができます。

- **Online client statistics**: オンラインクライアントトレンドグラフ、オンラインクライアントのピーク数と平均数、および統計収集時間範囲内のオンラインクライアントの詳細情報。
- **Rate statistics**: データを収集したときの送受信レートの傾向グラフ、ピーク送信レート、ピーク受信レート、平均送信レート、平均受信レート、送受信レート。
- **Traffic statistics**: 統計情報収集の開始時刻と終了時刻、送信トラフィック、受信トラフィック、および合計トラフィック。
- **Association statistics**: AP番号、オフライン率、アソシエーション要求、アソシエーション応答、正常なアクセス、異常なオフライン数、アソシエーションの成功率、およびアソシエーションの失敗率に関する統計情報。
- **Connectivity statistics**: クライアントのオフライン時間、リカバリ時間、オフライン時間。

ロケーションビューの履歴情報を問い合せる手順は、次のとおりです。

1. Serviceタブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > Location Views**を選択します。

   Location Listには、すべてのロケーションビューが表示されます。
3. 次のいずれかの方法で手順を続行します。
   - ターゲットロケーションビューの名前をクリックします。

     Sub-location/Device Listページが開きます。
   - **Sub-location/Device List**ページで、ターゲットサブロケーションビューの名前をクリックします。

     Sub-location/Device Listページが開きます。

4. **More**をクリックし、**History Information**アイコン  を選択します。

   History Informationページが開きます。

5. 統計タイプを選択します。オプションは次のとおりです。
   - **Online Clients (default)**
   - **Rate**
   - **Traffic**
   - **Association**
   - **Connectivity**
6. 時間範囲を選択します。オプションは次のとおりです。
   - **1h**
   - **1d**
   - **1w**
   - **1m**
   - **1y**
   - **Custom**

   Customを選択した場合は、開いた**Custom**ウィンドウに開始時刻と終了時刻を入力するか、**Start Time/End Time**の横にあるフィールドをクリックして、表示されるカレンダーから開始時刻と終了時刻を**YYYY-MM-DD hh:mm**形式で選択します。終了時刻は、開始時刻より後の時刻にする必要があります。

   指定した時間範囲の統計情報が表示されます。

   Online Clients Statistics contents:

   Online Clientsを選択すると、次の情報が表示されます。

   - **Online Client Trend graph**: Trendグラフロケーションビューまたはサブロケーションビューにおける、データ収集時間範囲内のオンラインクライアントのトレンド。x座標は時間を表し、y座標はオンラインクライアントの数を表します。x座標の単位は、統計収集時間範囲に応じて変化します。
   - **Peak Number of Online Cl**: 統計情報収集時のロケーションビューまたはサブロケーションビューでのAPのオンラインクライアントの最大数。
   - **Average Online Clients**: 統計情報の収集時における、ロケーションビューまたはサブロケーションビュー上のAPの平均オンラインクライアント数。

   Client Details contents:

   トレンドグラフの上部にあるOnline Clientsをクリックして、**Details**ウィンドウを表示します。

   - **Time**: 統計情報が収集された時刻(**YYYY-MM-DD hh:mm:ss**の形式)。
   - **Clients**: 統計情報収集時間範囲内のロケーションビューまたはサブロケーションビューのAPに関連付けられているオンラインクライアントの数。

   Rate Statistics cont:

Rateの単位は、**Rate**の値によって変わります。

Rateを選択すると、次の情報が表示されます。

- **Transmission and Receiving rate Trend graph**: グラフロケーションビューまたはサブロケーションビューでの、データ収集時間範囲内のAPの送信レートおよび受信レートの傾向。x座標は時間を表し、y座標は送信レートおよび受信レートを表します。x座標の単位は、統計情報収集時間範囲によって変化します。
- **Peak Transmission Rate(Kbps)**: 統計情報収集時のロケーションビューまたはサブロケーションビューでのAPの最大伝送レート。測定単位は、データの変更に応じて自動的に変更されます。
- **Peak Receiving rate(Kbps)**: 統計情報収集時のロケーションビューまたはサブロケーション

ビューでのAPの最大受信レート。測定単位は、データの変更に応じて自動的に変更されます。

- **Average Transmission Rate(Kbps)**: 統計情報収集時のロケーションビューまたはサブロケーションビューでのAPの平均伝送レート。測定単位は、データの変更に応じて自動的に変更されます。
- **Average Receiving rate(Kbps)**: 統計情報収集時のロケーションビューまたはサブロケーションビューでのAPの平均受信レート。測定単位は、データの変更に応じて自動的に変更されます。

Rate Details contents:

トレンドグラフの上部にある**Rate**をクリックして、**Details**ウィンドウを表示します。

- **Time**: 統計情報が収集された時刻(YYYY-MM-DD hh:mm:ssの形式)。
- **Transmission Rate(bps)**: 指定された時間におけるロケーションビューまたはサブロケーションビュー上のAPの伝送レート。測定単位は、データの変更に応じて自動的に変更されます。
- **Receiving rate(bps)**: 指定された時間のロケーションビューまたはサブロケーションビューでのAPの受信レート。測定単位は、データの変更に応じて自動的に変更されます。

Traffic Statistics con:

トラフィックの単位は、送受信されたトラフィックの量によって変わります。トラフィッ

クを選択すると、次の情報が表示されます。

- **Start Time**: 統計情報収集の開始時刻(YYYY-MM-DD hh:mm:ssの形式)。
- **End Time**: 統計情報収集の終了時刻(YYYY-MM-DD hh:mm:ssの形式)。
- Transmitted Traffic(MB): 指定された時間範囲内にロケーションビューまたはサブロケーションビューでAPによって送信されたトラフィックの合計。測定単位は、データの変更に応じて自動的に変更されます。
- **Received Traffic(MB)**: 指定された時間範囲内にロケーションビューまたはサブロケーションビューでAPによって受信されたトラフィックの合計。測定単位は、データの変更に応じて自動的に変更されます。
- **Total Traffic(MB)**: 指定された時間範囲内にロケーションビューまたはサブロケーションビューでAPによって送受信されたトラフィックの合計。この値は統計情報に基づいて計算され、実際の値とは若干異なる場合があります。測定単位は、データの変更に応じて自動的に変更されます。

Association Statistics contents:

関連付けを選択すると、次の情報が表示されます。

- **APs**: 指定された時刻におけるロケーションビューまたはサブロケーションビュー内のAPの数。
- **Dropping Rate**: 指定された時間範囲内の正常なログインに対する異常なログオフの比率をパーセンテージで示します。
- **Access Requests**: 指定された時間範囲内にAPによって受信されたアクセス要求の数。
- **Response Count**: 指定された時間範囲内にAPによって送信された応答の数。
- **Successful Logins**: 指定された時間範囲内で成功したログインの数。
- **Abnormal Logoffs**: 指定された時間範囲内で正常にログインしたクライアントの異常ログオフ数。
- **Association Success Rate**: 指定された時間範囲内にAPによって送信されたアクセス応答の数に対する、成功したログインクライアントの数の割合。
- **Relevant Blocking Rate**: 指定された時間範囲内で、成功したログインクライアントの数に対してAPリソースが不足しているためにAPへのアクセスに失敗したクライアントの数の割合。

Connectivity Statistics contents:

Connectivityを選択すると、次の情報が表示されます。

- **AP Name**:ロケーションビューまたはサブロケーションビューのAPの名前。
- **Logoff Time**: WSMによって検出されたFIT APのログオフ時間、またはFAT AP障害時間(YYYY-MM-DD hh:mm:ss形式)。
- **Recovery Time**: FIT APが再びオンラインになった時刻、またはWSMがFAT APの再接続を検出した時刻。形式はYYYY-MM-DD hh:mm:ssです。
- **Logoff Duration**: YYYY-MM-DD hh:mm:ssの形式で、FIT APのログオフ期間、またはWSMによって検出されたFAT APの障害期間。

7. **Close**をクリックします。

ロケーションビューでのAPのネットワーク接続のテスト

この機能を使用すると、IMCサーバーからの管理対象APの到達可能性をテストし、接続の問題をトラブルシューティングして特定できます。

Sub-location/Device Listページから選択したAPに対してpingまたはtracerouteを実行するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > Location Views**を選択します。ロケーションリストには、すべてのロケーションビューが表示されます。
3. 次のいずれかの方法で手順を続行します。
   - ターゲットロケーションビューの名前をクリックします。
   - **Sub-location/Device List**ページが開きます。
   - **Sub-location/Device List**ページで、ターゲットサブロケーションビューの名前をクリックします。

   Sub-location/Device Listページが開きます。
4. pingまたはtracerouteを実行するAPの**Operation**アイコン ･･･をクリックします。
5. メニューから、**Ping**アイコンまたは**TraceRoute**アイコンを選択します。

pingまたは**traceroute**ダイアログボックスが開きます。pingまたはtraceroute操作の結果を表示します。

6. **OK**をクリックします。

ロケーションビューでFAT APのWebマネージャーを開く

Web Managerを使用すると、管理されたFAT APへの迅速なWebアクセスが可能になります

Webマネージャーを使用して、Sub-location/Device Listページから選択したFAT APにアクセスして管理するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > Location Views**を選択します。ロケーションリストには、すべてのロケーションビューが表示されます。
3. 次のいずれかの方法で手順を続行します。
   - ターゲットロケーションビューの名前をクリックします。

     Sub-location/Device Listページが開きます。
   - **Sub-location/Device List**ページで、ターゲットサブロケーションビューの名前をクリックします。

     Sub-location/Device Listページが開きます。
4. Webマネージャーを開くFAT APの**Operation**アイコン をクリックします。
5. メニューから、**Open Web Manager**アイコンを選択します。

Web Managerインターフェースが開きます。

6. Webマネージャーのユーザー名とパスワードを入力します。
7. **Login**をクリックします。

ロケーションビュー上のFAT APへのTelnet接続

この機能により、管理されたFAT APへの迅速かつ集中的なアクセスが可能になります。IMCへのアクセスに使用するコンピュータには、Telnetをサポートするオペレーティングシステムまたはアプリケーションが必要です。Telnetを使用して、Sub-location/Device Listページから選択したFAT APにアクセスするには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > Location Views**を選択します。ロケーションリストには、すべてのロケーションビューが表示されます。
3. 次のいずれかの方法で手順を続行します。
   - ターゲットロケーションビューの名前をクリックします。

     Sub-location/Device Listページが開きます。
   - **Sub-location/Device List**ページで、ターゲットサブロケーションの名前をクリックします。
   - **Sub-location/Device List**ページが開きます。
4. アクセスするFAT APの**Operation**アイコン ･･･をクリックします。
5. メニューから**Telnet**アイコンを選択します。
6. オペレーティングシステムの指示に従ってアプリケーションをロードし、選択されたFAT APとのTelnetセッションを確立します。

ロケーション トポロジーを表示する

この機能を使用すると、ロケーションビューおよびそのサブロケーションビューのトポロジーを表示できます。ロケーションビューのトポロジーを表示するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > Location Views**を選択します。

   ロケーションリストには、すべてのロケーションビューが表示されます。
3. 次のいずれかの方法で手順を続行します。
   - トポロジーを表示するロケーションビューの**View Topology**アイコンをクリックします。
   - ターゲットロケーションビューの名前をクリックし、**Sub-location/Device List**の後にページが表示されます。
   - **More**をクリックして**View Topology**アイコンを選択するか、**Operation**アイコン･･･をクリックして**View Topology**アイコンを選択します。

     ロケーションビューに含まれるすべてのサブロケーションビューおよびAPがトポロジーに表示されます。
4. サブロケーションビューのラベルをダブルクリックします。

   トポロジーを表示するページが開きます。

ロケーションビュー トポロジーには、すべてのサブロケーションビューとロケーションビュー上のAPが表示さ

れます。トポロジーは必要に応じて変更できます。詳細については、「ワイヤレストポロジーを管理する」を参照してください。

ロケーションビューでのAPの検索

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > Location Views**を選択します。

   ロケーションリストには、すべてのロケーションビューが表示されます。
3. 次のいずれかの方法で手順を続行します。
   - ターゲットロケーションビューの名前をクリックします。**Sub-location/Device List**ページが開きます。
   - **Sub-location/Device List**ページで、ターゲットのサブロケーションビューの名前をクリックします。ターゲットのサブロケーションビューの**Sub-location/Device List**ページが開きます。
4. 検索するAPの**Operation**アイコン をクリックします。
5. メニューから**View Topology**アイコンを選択します。トポロジーを表示するページが開きます。

選択したAPが、ロケーションビューのトポロジーで強調表示されます。

デフォルトマップに対するロケーションビューでのAPの検索

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > Location Views**を選択します。ロケーションリストには、すべてのロケーションビューが表示されます。
3. 次のいずれかの方法で手順を続行します。
   - ターゲットロケーションビューの名前をクリックします。

     Sub-location/Device Listページが開きます。
   - **Sub-location/Device List**ページで、ターゲットサブロケーションビューの名前をクリックします。**Sub-location/Device List**ページが開きます。
4. デフォルトマップを検索するAPの**Operation**アイコン をクリックします。
5. メニューから、**Locate to Map**アイコンを選択します。デフォルトのマップページが開きます。

APが選択されているロケーションビューは、デフォルトマップ上で強調表示されます。デフォルトマップに対してAPを検索する前に、ワイヤレス検索を設定します。詳細については、「GIS検索」を参照してください。

すべてのロケーションビューのホットスポット情報をエクスポートする

この関数を使用すると、すべてのホットスポットの基本的なホットスポット情報と拡張プロパティを.csvファイルにエクスポートできます.csvファイル内のホットスポット情報をWSMにインポートできます。

ホットスポット情報をエクスポートするには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > Location Views**を選択しま

す。ロケーションリストには、すべてのロケーションビューが表示されます。

3. **Export Hotspot**をクリックします。

   Export Resページが開きます。

4. **Export Res**をクリックします。

ファイルをダウンロードするためのダイアログボックスが開きます。

5. **Save**をクリックして、.csvファイルをローカルコンピュータに保存します。

   CSVファイルの内容

   - **Symbol Id**: WSMデータベース内のホットスポットの一意の識別子。
   - **Location Name**: ホットスポットが関連付けられているロケーションビュー。
   - **AP Count**: ホットスポット上のAPの数。

ホットスポットに拡張プロパティが定義されている場合、WSMはこれらの拡張プロパティを**SymbolId**に基づいてホットスポットごとにバッチでインポートします。

オフラインAPの元の場所の復元

WSMは、オフラインAPのロケーション履歴を管理し、APが再びオンラインになったときに元のロケーションビューを復元するかどうかを制御できます。

オフラインAPの元の場所を復元するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > View Management > Location View**を選択します。

   Location Viewページが開きます。

3. **Location History**をクリックします。

   Location Historyページが開きます。

4. 必要に応じて、**Restore Offline APs' Original Location**オプションを選択します。
   - このオプションを選択すると、WSMはオフラインAPのロケーション情報を保存し、APが再びオンラインになったときに元のロケーションビューに自動的に追加します。
   - このオプションがクリアされている場合、WSMはオフラインAPの保存済みロケーション情報を削除し、オフラインAPのロケーション情報は保存しません。デフォルトでは、このオプションはクリアされています。

   Location History contents

   - **SN/MAC Address**: オフラインAPのMACアドレス又はシーケンス番号。
   - **Location View**: オフラインAPが配置されたロケーションビュー。
   - **X Coordinate/Y Coordinate**: ロケーションビューでのオフラインAPのロケーション座標。
   - **Offline Time**: APがオフラインになった時刻。
5. ロケーションリスト内のAPのロケーション情報エントリーを手動で削除するには、1つまたは複数のエントリーを選択し、**Delete**をクリックします。

エントリーが削除された後、APが再びオンラインになっても、そのAPはロケーションビューに自動的に追加されません。

ロケーションビューに関連付けられたホットスポットの拡張プロパティの設定

WSMを使用すると、オペレーターは必要に応じてホットスポットのプロパティ(拡張プロパティと呼ばれる)を

定義できます。オペレーターは、ホットスポットの拡張プロパティを定義した後にのみ、そのプロパティを変更およびインポートできます。ホットスポットの拡張プロパティを定義するには、構成ファイルを変更します。

オペレーターは、ホットスポットを追加または変更するときにこれらの拡張プロパティを設定できます。また、すべてのホットスポットの拡張プロパティをバッチでエクスポートまたはインポートすることもできます。

ホットスポット拡張プロパティの定義

オペレーターは、WSMによって提供される設定ファイル(**IMC installation path/client/conf/wlan/hotspotExtendProperty.xml**)を編集することによって、ホットスポットの拡張プロパティを定義できます。ホットスポットには、最大10個の拡張プロパティを定義できます。

拡張プロパティを定義するには

1. IMCがインストールされているサーバーにログインします。
2. **Installation path/client/conf/wlan**にある**hotspotExtendProperty.xml**ファイルを開きます。次の情報が表示されます。

```
<?xml version="1.0" encoding="GB2312"?>
<config>
<global>
<property name="enableNotify" value="false" />
<property name="serverType" value="jxtele" />
<property name="endPointAddress"
value="http://134.224.4.69:18089/infHotspot/services/infhotspot" />
< property name ="enableResume" value="true"/>
< property name ="resumeInterval" value="10"/>
</global>
<extendProperties>
- <!-- propertyitem id="1" displayName="lanCode "wsName="lanCode" unique="false"
inheritLast="false" /-->
- <!-- propertyitem id="2" displayName="hotSpotCode" wsName="hotSpotCode"
unique="true" inheritLast="false" /-->
- <!-- propertyitem id="3" displayName="OrgName" wsName="OrgName" unique="false"
inheritLast="true" /-->
- <!-- propertyitem id="4" displayName="hotSpotType "wsName="hotSpotType"
unique="false" inheritLast="false" /-->
- <!-- propertyitem id="5" displayName="cityName" wsName="cityName"
unique="false" inheritLast="false" /-->
- <!-- propertyitem id="6" displayName="Memo" wsName="memo" unique="false"
inheritLast="false" / -->
</extendProperties>
</config>
```

3. **hotspotExtendProperty.xml**ファイルを編集します。

このファイルには、拡張プロパティを定義するためのサンプルが含まれています。このサンプルは、文中のコメント文字を削除してから使用できます。たとえば、次の行を変更します:

- <!--propertyitem id="1" displayName="lanCode" wsName="lanCode" unique="false"
inheritLast="false"/
--> to
- <propertyitem id="1" displayName="lanCode" wsName="lanCode" unique="false"

inheritLast="false" />

ここで

- **propertyitem id**: プロパティのID。IMCでは、プロパティIDに基づいて昇順でプロパティが表示されます。IDは連続している必要があり、重複することはできません。
- **displayName**: IMCに表示されるプロパティの名前。
- **wsName**: 3番目のネットワーク管理者に拡張プロパティ名を通知して、拡張プロパティの値の変更を同期させます。このフィールドはNULLでもかまいません。
- **unique**: 拡張プロパティの値を一意に設定します。trueが設定されている場合、この拡張プロパティの値は、異なるホットスポットに対して一意である必要があります。falseが設定されている場合、この拡張プロパティの値は、異なるホットスポットに対して同じにすることができます。一意の設定は、構成後は変更できません。
- **inheritLast**: このホットスポットのプロパティ値がNULLの場合に、ホットスポットが前のホットスポットの対応するプロパティ値を継承するかどうかを設定します。この関数は、ホットスポット情報をWSMにインポートするときに有効になります。**true**が設定されている場合、WSMはプロパティをインポートします

  後続のホットスポットの対応する値がnullの場合、後続のホットスポットの前のホットスポットの値。最初にインポートされたホットスポットの値がnullの場合でも、WSMはホットスポットのnull値をインポートします。**false**が設定されている場合、WSMはプロパティ値をそのままインポートします。

4. **hotspotExtendProperty.xml**ファイルを保存して閉じます。
5. **Intelligent Deployment Monitor Agent**でIMCを再起動するか、または**process**タブの**jserver**処理を再起動します。
6. IMCにログインします。
7. **Service**タブをクリックします。
8. ナビゲーションツリーから、**WLAN Manager > View Management > Location Views**を選択します。ロケーションリストには、すべてのロケーションビューが表示されます。
9. ホットスポット情報をエクスポートまたはインポートするには、**Export Hotspot**または**Import Hotspot**をクリックします。新しく追加されたホットスポットに対して、これらの拡張プロパティを構成する必要があります。

ホットスポット情報のエクスポート

WSMでは、すべてのホットスポットの基本情報および拡張プロパティをバッチでエクスポートできます。ホットスポットの新しい拡張プロパティを定義した後、オペレーターはそれらをexport.csvファイルで設定し、.csvファイルをインポートすることによって拡張プロパティをWSMに適用できます。

ホットスポット情報をエクスポートするには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > Location Views**を選択します。ロケーションリストには、すべてのロケーションビューが表示されます。
3. **Export Hotspot**をクリックします。

ホットスポット情報をインポートするためのページが開きます。

4. **Export Res**をクリックします。

ファイルをダウンロードするためのダイアログボックスが開きます。

5. **Save**をクリックして、.csvファイルをローカルコンピュータに保存します。

   export.csvファイルには、**SymbolId**、**Location Name**、**AP Count**、およびすべてのホットスポットの拡張プロパティが含まれています。WSMでは、**SymbolId**をデータベース内のホットスポットの一意の識別子として使用します。

ホットスポット情報のインポート

WSMでは、すべてのホットスポットの基本情報および拡張プロパティのバッチでのエクスポートがサポートされています。ホットスポットの新しい拡張プロパティを定義した後、オペレーターはそれらをexport.csvファイルで構成し、.csvファイルをインポートすることによって拡張プロパティをWSMに適用できます。詳細は、「ホットスポット情報のエクスポート」を参照してください。

WSMは、インポートされた.csvファイルの最初の行をプロパティ名として識別します。最初の列は各ホットスポットの一意の識別子として使用されるため、ファイルの最初の列はインポートされません。

ホットスポット情報をインポートするには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > Location Views**を選択します。ロケーションリストには、すべてのロケーションビューが表示されます。
3. **Import Hotspot**をクリックします。

ホットスポット情報をインポートするためのページが開きます。

4. 次のいずれかの方法で手順を続行します。
   - インポートするファイルの絶対パスを入力します。
   - **Browse**をクリックします。

ブラウザの指示に従ってファイルを検索します。

5. **Next**をクリックします。

   Result Listページが開き、ロケーションビューにインポートされたホットスポットと、ロケーションビューへのインポートに失敗したホットスポットが表示されます。失敗が発生した場合は、**Operation Result**列の**Detail**アイコンをクリックして、失敗の理由を識別します。
6. **Location List**ページに戻るには、**Back**をクリックします。

ワイヤレスカスタムビューを管理する

ACに対して1つまたは複数のワイヤレスカスタムビューを作成できます。ワイヤレスカスタムビューは、ACとACに接続された複数のAPで構成されます。ワイヤレスカスタムビューを使用すると、トポロジー上で目的のデバイスを簡単に検索し、デバイスを管理できます。

ワイヤレスカスタムビューリストの表示

Wireless Custom View Listページには、すべてのワイヤレスカスタムビューのステータス、名前、トポロジーなど、WSMで管理されているすべてのワイヤレスカスタムビューに関する情報が表示されます。ワイヤレスカスタムビューを変更または削除することもできます。

ワイヤレスカスタムビューリストを表示するには、以下の手順に従ってください。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > Custom Views**を選択します。Wireless Custom View Listページには、すべてのワイヤレスカスタムビューが表示されます。

   Wireless Custom View List contents:
   - **Status**: ロケーションビューのステータス。アラームレベルが最も高いFIT APのステータスによって異なります。ワイヤレスカスタムビューにデバイスが含まれていない場合、そのステータスは**Unmanaged**です。ワイヤレスカスタムビューにオンラインFIT APが含まれていない場合、そのステータスは**Unknown**です。
   - **Location View**: ロケーションビューの名前。詳細を表示して管理するには、ロケーションビュ

ーの名前をクリックします。

- **View Topology** :トポロジーの表示ワイヤレスカスタムビューのトポロジーを表示するには、**View Topology**をクリックします。
- **Modify** :設定を変更するには、ワイヤレスカスタムビューの**Modify**アイコンをクリックします。
- **Delete**: ワイヤレスカスタムビューを削除するには、**Delete**アイコンをクリックします。

ワイヤレスカスタムビューリストに十分な数のエントリーが含まれている場合は、次のナビゲーションツールが表示されます。

- **Next Page**アイコンをクリックして、**Wireless Custom View List**で次のページに進みます。
- **Last Page**アイコンをクリックして、**Wireless Custom View List**の最後までページを進めます。
- **Previous Page**アイコンをクリックして、**Wireless Custom View List**で前のページに戻ります。
- **First Page**アイコンをクリックして、**Wireless Custom View List**の先頭に移動します。

ワイヤレスカスタムビューリストの右上にある**8**、**15**、**50**、**100**、または**200**をクリックして、各ページに表示する項目の数を指定します。

ワイヤレスカスタムビューリストを状態フィールドとワイヤレスカスタムビューフィールドで並べ替えることができます。列のラベルをクリックすると、選択したフィールドでリストが並べ替えられます。この列では、各フィールドに固有の並べ替えオプションを切り替えることができます。

ワイヤレスカスタムビューの詳細を表示する

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > Custom Views**を選択します。Wireless Custom View Listページには、すべてのワイヤレスカスタムビューが表示されます。
3. ターゲットのワイヤレスカスタムビューの名前をクリックして、その詳細を表示します。

   Device Listには、ワイヤレスカスタムビューのすべてのデバイスが表示されます。

ワイヤレスカスタムビューには、ACおよびACに接続されたすべてのFIT APが含まれています。ACエントリーは常にデバイスリストの最初の行に配置され、FIT APエントリーはすべてACエントリーの下に配置されます。

Device List contents:

- **Status**: ACまたはFIT APの現在のアラームステータス。
- **Device List**: ACまたはfit APの名前。デフォルトでは、ACまたはfit APの名前は、ACまたはfit APのシステム名です。
- **SN**: FIT APのシリアル番号。ACの場合、このフィールドは空です。
- **Type**: デバイスタイプ(ACまたはfit AP)。
- **Model**: ACまたはFIT APのモデル。
- **IP Address**: ACまたはfit APの管理IPアドレス。
- **IPv6 Address**: ACまたはfit APの管理IPv6アドレス。
- **MAC Address**: ACまたはfit APのMACアドレス。
- **Online Clients**: ACの場合、このフィールドには、無線カスタムビューでfit APに関連付けられているクライアントの総数が表示されます。fit APの場合、このフィールドには、fit APに関連付けられているクライアントの数が表示されます。数値をクリックすると、すべてのオンラインクライアントが表示されます。
- **Operation**: **Operation**メニュー ･･･を表示するには、ACまたはFIT APの**Operation**アイコンをクリックします。

ACの場合、**Operation**メニューに表示される操作タスクは次のとおりです。

- View Topology
- **ping、TraceRoute**
- Open Web Manager
- Telnet

FIT APの場合、Operationメニューに表示される操作タスクは次のとおりです。

- View Topology
- ping
- TraceRoute
- Locate to Map

Device Listに十分な数のエントリーが含まれている場合は、次のナビゲーションが表示されます。

- **Next Page**アイコンをクリックして、**Device List**の次のページに進みます。
- **Last Page**アイコンをクリックして、**Device List**の最後までページを進めます。
- **Previous Page**アイコンをクリックして、**Device List**で前のページに戻ります。
- **First Page**アイコンをクリックして、**Device List**の先頭にページを戻します。

Device Listの右上にある**8、15、50、100**、または**200**をクリックして、各ページに表示する項目の数を指定します。

Operationフィールドを除くすべてのフィールドで**Device List**をソートできます。選択したフィールドでリストをソートするには、列ラベルをクリックします。列ラベルを使用すると、ソートオプションを切り替えることができます。

各フィールド固有のACは、指定したソート基準に関係なく、常にリストの最初の行に表示されます。

ワイヤレスカスタムビューを追加する

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > View Management > Custom Views**を選択します。
3. ワイヤレスカスタムビューリストページには、すべてのワイヤレスカスタムビューが表示されます。
4. **Add**をクリックします。

ワイヤレスカスタムビューを追加するためのページが開きます。

5. ワイヤレスカスタムビューの名前を入力します。
6. **OK**をクリックします。

ワイヤレスカスタムビューを変更する

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > View Management > Custom Views**を選択します。
3. **Wireless Custom View List**ページには、すべてのワイヤレスカスタムビューが表示されます。
4. ターゲットワイヤレスカスタムビューの**Modify**アイコン  をクリックします。

   ビューを変更するためのページが開きます。
5. ワイヤレスカスタムビューの名前を変更します。
6. **OK**をクリックします。

ワイヤレスカスタムビューを削除する

ワイヤレスカスタムビューを削除すると、ACおよびすべてのFIT APがワイヤレスカスタムビューから削除されますが、WSMからは削除されません。

ワイヤレスカスタムビューを削除するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > Custom Views**を選択します。**Wireless Custom View List**ページには、すべてのワイヤレスカスタムビューが表示されます。
3. ワイヤレスカスタムビューの**Delete**アイコンをクリックします。
4. 確認ダイアログボックスで、**OK**をクリックします。

ワイヤレスカスタムビューへのFIT APの追加

この機能を使用すると、ACの複数のFit APをワイヤレスカスタムビューに追加できます。Fit

APをワイヤレスカスタムビューに追加するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > Custom Views**を選択します。**Wireless Custom View List**ページには、すべてのワイヤレスカスタムビューが表示されます。
3. ターゲットのワイヤレスカスタムビューの名前をクリックして、その詳細を表示します。**Device List**ページには、ワイヤレスカスタムビュー上のすべてのデバイスが表示されます。
4. **Add**をクリックします。
5. **Select Devices**ダイアログボックスが開きます。
6. 次のクエリー基準を1つ以上入力または選択して、追加するAPを検索します。
   - **AC**: FIT APのACを選択します。オプションはすべて、WSMで使用可能なACです。
   - **Device Labe**l: FIT APのラベルを入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
   - **IP Address**: FIT APのIPv4アドレスの一部または全体を入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。

空のフィールドは、クエリー条件として機能しません。

7. **Query**をクリックします。

   Device Listには、クエリー基準に一致するすべてのFIT APが表示されます。クエリー基準をクリアしてFIT APをすべて表示するには、**Reset**をクリックします。
8. ワイヤレスカスタムビューに追加するfit APを選択します。
9. **OK**をクリックします。

選択したすべてのFIT APが、ワイヤレスカスタムビューの**Device List**に表示されます。

注:

- FIT APをワイヤレスカスタムビューに初めて追加すると、対応するACが自動的にビューに追加されます。次回は、ACの他のFIT APのみを追加できます。
- **FIT APは、複数のワイヤレスカスタムビューに追加できます。**

ワイヤレスカスタムビューからのFIT APの削除

ワイヤレスカスタムビューからデバイスを削除すると、現在のビューからのみデバイスが削除され、他のビューやWSMからは削除されません。デバイスを削除すると、WSMからデバイスが完全に削除されます。

ビューに適合するすべてのAPが削除されると、WSMはワイヤレスカスタムビューのデバイスリストからACを自動的に削除します。

ワイヤレスカスタムビューからFit APを削除するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > Custom Views**を選択します。**Wireless Custom View List**ページには、すべてのワイヤレスカスタムビューが表示されます。
3. ターゲットのワイヤレスカスタムビューの名前をクリックします。**Device List**ページが開きます。
4. 削除するFit APを選択し、**Remove**をクリックします。
5. 確認ダイアログボックスで、**OK**をクリックします。

ワイヤレスカスタムビューでのACまたはオンラインFIT APのネットワーク接続のテスト

この機能を使用すると、IMCサーバーからの管理対象ACまたはOnline Fit APの到達可能性をテストし、接続の問題をトラブルシューティングして特定できます。

Device ListページからACまたはオンラインFIT APに対してpingまたはtracerouteを実行するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > Custom Views**を選択します。**Wireless Custom View List**ページには、すべてのワイヤレスカスタムビューが表示されます。
3. ターゲットのワイヤレスカスタムビューの名前をクリックします。

   Device Listページが開きます。
4. pingまたはtracerouteを実行するACまたはオンラインFIT APの**Operation**アイコン をクリックします。
5. メニューから、**Ping**アイコンまたは**TraceRoute**アイコンを選択します。

pingまたはtracerouteダイアログボックスが開きます。pingまたはtracerouteの結果を表示します。

6. **OK**をクリックします。

ワイヤレスカスタムビューでACのWebマネージャーを開く

この機能により、管理対象ACへの迅速なWebアクセスが可能になります。

Web Managerを使用して、Device Listから選択したACにアクセスして管理するには、次の手順を実行します。

1. Serviceタブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > Custom Views**を選択します。**Wireless Custom View List**ページには、すべてのワイヤレスカスタムビューが表示されます。
3. ターゲットのワイヤレスカスタムビューの名前をクリックします。デバイスリストページが開きます。
4. Web Managerを開くACの**Operation**アイコン をクリックします。
5. メニューから、**Open Web Manager**アイコンを選択します。

   Web Managerインターフェースが開きます。
6. Webマネージャーのユーザー名とパスワードを入力します。

7. **Login**をクリックします。

Telnetを使用してワイヤレスカスタムビュー上のACにアクセスする

この機能により、管理対象ACへの迅速かつ集中的なアクセスが可能になります。

この機能を使用するには、IMCへのアクセスに使用するコンピュータでTelnetをサポートするオペレーティングシステムまたはアプリケーションが必要です。

Telnetを使用して、Devices Listページから選択したACにアクセスするには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > Custom Views**を選択します。**Wireless Custom View List**ページには、すべてのワイヤレスカスタムビューが表示されます。
3. ターゲットのワイヤレスカスタムビューの名前をクリックします。デバイスリストページが開きます。
4. Telnetを使用してアクセスするACの**Operation**アイコン をクリックします。
5. メニューから**Telnet**アイコンを選択します。
6. オペレーティングシステムの指示に従ってアプリケーションをロードし、選択したACとのTelnetセッションを確立します。

ワイヤレスカスタムビュートポロジーを表示する

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > Custom Views**を選択します。**Wireless Custom View List**ページには、すべてのワイヤレスカスタムビューが表示されます。
3. 次のいずれかの方法で手順を続行します。
   - トポロジーを表示するワイヤレスカスタムビューの**View Topology**アイコンをクリックします。
   - ターゲットのワイヤレスカスタムビューの名前をクリックし、デバイスリストページで**View Topology**アイコン をクリックします。

トポロジーを表示するためのページが開きます。

トポロジーには、ワイヤレスカスタムビューのACおよびすべてのFIT APが表示されます。トポロジーは必要に応じて変更できます。詳細については、「ワイヤレスカスタムビューを変更する」を参照してください。

ワイヤレスカスタムビューでのACまたはFIT APの位置確認

この機能を使用すると、ワイヤレスカスタムビューのトポロジー内でACまたはFIT APを検索できます。

ACまたはFIT APを検索するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > Custom Views**を選択します。**Wireless Custom View List**には、すべてのワイヤレスカスタムビューが表示されます。
3. ターゲットのワイヤレスカスタムビューの名前をクリックします。

   Device Listページが開きます。
4. 検索するACまたはFit APの**Operation**アイコン をクリックします。

5. メニューから**View Topology**アイコンを選択します。トポロジーを表示するページが開きます。

ACまたはFIT APが選択されているロケーションビューが、トポロジー内で強調表示されます。

デフォルトマップに対するワイヤレスカスタムビューでのFIT APの検索

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > Custom Views**を選択します。**Wireless Custom View List**には、すべてのワイヤレスカスタムビューが表示されます。
3. ターゲットのワイヤレスカスタムビューの名前をクリックします。

   Device Listページが開きます。
4. デフォルトマップに配置するFIT APの**Operation**アイコン ･･･をクリックします。
5. メニューから、**Locate to Map**アイコンを選択します。

   デフォルトのマップページが開きます。

FIT APが選択されているロケーションビューは、デフォルトマップで強調表示されます。デフォルトマップにFIT APを検索する前に、ワイヤレス検索を設定します。詳細については、「GIS検索」を参照してください。

GISビューを管理する

ロケーションビュー トポロジーに基づいて、小規模ワイヤレスネットワークの地理的範囲を簡単に表示できます。ただし、ロケーションビュー トポロジーは、大都市内または大都市間のAPなどの大規模ワイヤレスネットワークの地理的範囲を表示するには十分ではありません。

GISビューでは、ロケーションビューまたは単一のAPをデフォルトマップにマッピングできます。デフォルトマップでは、APの配置がマクロレベルで表示されます。GISビューを使用すると、各ロケーションビューまたはAPはデフォルトマップ上で正確にラベル付けされ、ヒントメッセージボックスが各ロケーションビューまたはAPに添付されます。ヒント情報には、コンタクトアドレス、電話番号、およびロケーションビューまたはAPのアクセス端末が含まれます。GISロケーティングでは、マップ上の各APの位置を正確に特定できます。

デフォルトのマップはMapbarマップです。

GISビューを使用するには、次のガイドラインに従います。

- ネットワーク接続が異常な場合は、マップが正しくロードされません。
- マーカーのステータスは、それに関連付けられたロケーションビューまたはAPによって決定されます。
- 管理者およびマップを管理する人は、GISビューでマップを編集できます。ビューアはマップの表示のみが可能です。

GISビューでマーカーを表示する

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > GIS View**を選択します。

   GIS Viewページには、マップ上および**Marker List**内のすべてのマーカーが表示されます。

   現在のGISビュー上のマーカー、AP、およびオンラインクライアントの数がマップの上に表示されます。

   既定のマップの左側にあるナビゲーションコントロールを使用して、任意のマーカーとそのマップ上の位置を参照できます。マーカーの画像またはアイコンをクリックすると、ヒントのメッセージボックスが表示されます。
3. location viewの場合は、APの合計数を示すリンクをクリックして、マーカーのデバイス情報を表示します。
4. location viewの場合は、**View Topology**アイコンをクリックしてマーカートポロジーを表示します。
5. APの場合は、クライアントの合計数を示すリンクをクリックして、クライアント情報を表示します。

注:

デフォルトマップ上のナビゲーションコントロール:北、南、東および西のナビゲーション矢印をクリックしてマップを別の方向にドラッグし、ズームの+記号または-記号をクリックするか、ズームスライダをドラッグしてマップをズームインまたはズームアウトします。マップ上で直接ドラッグ、ズームインまたはズームアウトすることもできます。

Marker Listには、GISビュー上のすべてのマーカーが表示されます。**Marker List**には、各マーカーの名前、**Modify**アイコン、および**Delete**アイコンが含まれています。既定のマップ上のマーカーの名前をクリックすると、ヒントメッセージボックスが開きます。

マーカーの詳細を表示する

この機能を使用すると、アドレス、電話番号、オンラインモバイルクライアントの数など、マーカーの詳細を

表示できます。

マーカーの詳細を表示するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > GIS View**を選択します。**Marker List**にはすべてのマーカーが表示されます。
3. マップ上で、マーカーの画像またはアイコンをクリックします。

   ヒントメッセージボックスが開き、マーカーの詳細が表示されます。マーカーの詳細には、次の情報が含まれます:

   - **location view**の場合:
     - 関連付けられたロケーションビュー。
     - ロケーションビューの連絡先アドレスと電話番号。
     - ロケーションビュー内のAPの数。
     - オンラインクライアントの数。

     ロケーションビューでAPに関する情報を表示するには、APの合計数を示すリンクをクリックします。

     View Topologyアイコンをクリックすると、ロケーションビュートポロジーを表示できます。
   - **AP**の場合:
     - アソシエートされたAP。
     - APの連絡先アドレスと電話番号。
     - APのIPアドレス。
     - シリアルID (FIT APだけに表示されます)。
     - オンラインクライアントの数。

     クライアントの合計数を示すリンクをクリックすると、APに関連付けられているクライアントに関する情報が表示されます。

位置ビューマーカーを追加する

位置ビューを位置ビューマーカーとして既定のマップに追加し、マップ上のマーカーの経度と緯度を指定できます。位置ビューは1つのマーカーにのみ関連付けることができ、位置ビューの親または子の位置は他のマーカーに関連付けることはできません。位置ビュー内の各APは、APマーカーに関連付けることができます。

位置ビューマーカーを追加するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > GIS View**を選択します。

   Marker Listにはすべてのマーカーが表示されます。
3. **Add Marker**をクリックし、リストから**Add Location View**を選択します。
4. **Location View**トから位置ビューを選択します。
5. **Select Picture**リストから、マップ上のマーカーを表すラベルを選択します。
6. 次のいずれかの方法で手順を続行します。
   - **Label**をクリックして、マップ上のマーカーの地理的位置を設定します。
     Longitude/Latitudeフィールドには、マーカーの経度と緯度が自動的に表示されます。
   - **Longitude/Latitude**フィールドに、マーカーの緯度と経度を入力します。
7. **Telephone**フィールドにマーカーの電話番号を入力します。

8. **Address**フィールドにマーカーのアドレスを入力します。
9. OKをクリックします。

APマーカーの追加

APは1つのAPマーカーだけに関連付けることができ、APが存在するロケーションビューは1つのロケーションビューマーカーに関連付けることができます。

APマーカーを追加するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > GIS View**を選択します。

   Marker Listにはすべてのマーカーが表示されます。
3. **Add Marker**をクリックし、リストから**Add AP**を選択します。
4. **Select Devices**をクリックして、APを選択します。
5. 次のいずれかの方法で手順を続行します。
   - **Label**をクリックして、マップ上のマーカーの地理的位置を設定します。

     Longitude/Latitudeフィールドには、マーカーの経度と緯度が自動的に表示されます。
   - **Longitude/Latitude**フィールドに、マーカーの緯度と経度を入力します。
6. **Telephone**フィールドにマーカーの電話番号を入力します。
7. **Address**フィールドにマーカーのアドレスを入力します。
8. OKをクリックします。

マーカーを変更する

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > GIS View**を選択します。

   Marker Listにはすべてのマーカーが表示されます。
3. 変更するマーカーの**Modify**アイコンをクリックします。**Modify Marker**ページが開きます。
4. 「位置ビューマーカーの追加」および「APマーカーの追加」に示すように、必要に応じてパラメーターを変更します。
5. OKをクリックします。

注:

マップ上のマーカーにラベルを付けたり、マーカーを修正した後、マーカーの座標を入力したり、マップ上のマーカーのラベルをドラッグしてマーカーの座標を修正することができます。ドラッグ操作の後、マーカーの新しい座標が自動的に記録されます。

マーカーを削除する

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > GIS View**を選択します。

   Marker Listにはすべてのマーカーが表示されます。
3. 削除するマーカーの**Delete**アイコンをクリックします。

確認ダイアログボックスが表示されます。

4. OKをクリックします。

デフォルト位置の保存

この機能を使用すると、GISビューを開始するときに、マップ上の既定の位置を保存できます。

既定の位置を保存するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > GIS View**を選択します。

   Marker Listにはすべてのマーカーが表示されます。
3. マップ上でドラッグおよびズーム機能を使用して、マップ上の適切な表示位置を選択し、**Save Position**をクリックして現在の位置を既定の位置として保存します。

ワイヤレストポロジーを管理する

WSMは、次の種類のワイヤレストポロジーをサポートしています。

- **Wireless device topology**: WSM内のすべての管理対象ACおよびFAT APを表示します。また、ACデバイストポロジーを通じてACによって管理されるFIT APを表示したり、FAT APデバイストポロジーを通じてFAT APに関連付けられたクライアントを表示したりできます。
- **Location view topology**: ロケーションビューに含まれるAPとその関連クライアントを表示します。
- **Wireless custom view topology**: カスタムビューに含まれるACとその管理対象FIT APを表示し、FIT APに関連付けられたクライアントを表示できます。

さらに、コンバージドトポロジーでは、ワイヤレスデバイスとワイヤードデバイス、およびネットワーク内のそれらの接続も表示できます。

ネイバートポロジーは、指定されたホップ内のデバイスとそのネイバーを含むレイヤ2トポロジーです。これは、物理接続、リンクステータス、デバイスステータスなど、デバイスのネットワーク構造とステータス情報を表示します。詳細については、『H3C IMC v7.3 Enterprise and Standard Platform Administrator Guide』を参照してください。

Open Device Panel、**Tools**、**Root Alarms**、**Find**、**Reload**、**Device Label**などの基本的な機能は、IMCプラットフォームトポロジーと同じです。このドキュメントでは、ワイヤレストポロジーに固有の機能だけを説明します。基本的なトポロジー操作については、『H3C IMC v7.3 Enterprise and Standard Platform Administrator Guide』を参照してください。

ワイヤレスデバイストポロジー

ワイヤレスデバイストポロジーには、WSM内のすべての管理対象ACおよびFAT APが表示されます。これにより、ACデバイストポロジーを介してACによって管理されるFIT APを表示したり、FAT APデバイストポロジーを介してFAT APに関連付けられたクライアントを表示したりできます。

ワイヤレスデバイストポロジーは、さらに次のタイプに分類されます。

- **AC device topology**: ACによって管理されるFIT APと中央ACによって管理されるローカルACを表示します。また、FIT APに関連付けられたクライアントを表示できます。
- **Fat AP device topology**: FAT APに関連付けられたクライアントを表示します。
- **Physical topology**: ACから指定されたFit APへの接続に関与するネットワークデバイスを表示します。このトポロジーは、ACとFit APの両方がComwareベースのデバイスである場合にのみ使用できます。

ワイヤレスデバイストポロジーの表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Wireless Topology**を選択します。

   無線デバイストポロジーには、すべてのACとFAT APが表示されます。

トポロジーから、ACに対して次の操作を実行します。

- ACのアイコンをクリックします。ヒントウィンドウには、ACに関する次の情報が表示されます。
  - **Device Label**: IMCプラットフォームでACを識別するデバイスラベル。ACのデバイスラベルをクリックすると、その詳細が表示されます。
  - **IP Address**: ACの管理IPアドレス。

- **Device Status**: ACの現在のアラームステータス。
- **SysName**: ACに設定されている名前。
- **Vendor**: ACのベンダー。
- **System Up**: ACのシステムアップタイム。
- **Online APs**: ACによって管理されるFit APの合計数。この数をクリックすると、すべての管理対象Fit APのリストが表示されます。
- **Associated Wireless Clients**: ACによって管理されるFIT APに関連付けられているクライアントの数。この数をクリックすると、すべてのオンラインクライアントのリストが表示されます。クライアントリストの詳細は、「クライアントリストの表示」を参照してください。

- ACのアイコンを右クリックします。

  メニューには、ACに適用できる次のオプションが表示されます。

  - **Open Topology**: ACのデバイストポロジーを開くことができます。このトポロジーから、ACによって管理されるFIT AP、およびFIT APに関連付けられたクライアントを表示できます。
  - **Open Mesh Topology**: ACのメッシュ トポロジーを開くことができます。メッシュ トポロジーの詳細については、「メッシュ トポロジー」を参照してください。
  - **Neighbor Topology**: ACのネイバートポロジーを表示できます。詳細については、『H3C IMC v7.3 Enterprise and Standard Platform Administrator Guide』を参照してください。

トポロジーから、FAT APに対して次の操作を実行します。

- FAT APのアイコンをクリックします。ヒントウィンドウには、FAT APに関する次の情報が表示されます。
  - **Device Label**: IMCプラットフォームのFAT APを識別するデバイスラベル。FAT APのデバイスラベルをクリックすると、その詳細が表示されます。
  - **IP Address**: FAT APの管理IPアドレス。
  - **Device Status**: FAT APの現在のアラームステータス。
  - **SysName**: FAT APに設定されている名前。
  - **Vendor**: FAT APのベンダー。
  - **Clients**: FAT APに関連付けられているクライアントの数。数をクリックすると、すべてのオンラインクライアントのリストが表示されます。オンラインクライアントリストの詳細は、「クライアントリストの表示」を参照してください。
- FAT APのアイコンを右クリックします。

  メニューには、FAT APに適用できる次のオプションが表示されます。

  - **Open Topology**: FAT APのデバイストポロジーを開くことができます。このトポロジーから、FAT APに関連付けられているすべてのクライアントを表示できます。
  - **Neighbor Topology**: ACのネイバートポロジーを表示できます。詳細については、『H3C IMC v7.3 Enterprise and Standard Platform Administrator Guide』を参照してください。

ACのデバイストポロジーの表示

1. **Service**タブをクリックします。
2. 次のいずれかの方法を使用して、ターゲットACを特定します。

   Method 1

   a. ナビゲーションツリーから、**WLAN Manager > Wireless Topology**を選択します。

   b. 空白領域を右クリックして、ショートカットメニューの**Find**を選択します。クエリーデバイスウィンドウが開きます。

c. **Content**ボックスに、ターゲットACのデバイスラベルを入力します。

d. **Query**をクリックします。

ターゲットACがFind Resultウィンドウに表示されます。

e. ACを選択して、デバイストポロジーを表示します。

Method 2

a. ナビゲーションツリーで、**WLAN Manager > Resource Management > ACs**を選択します。

b. ターゲットACのOperationアイコン をクリックします。

c. ショートカットメニューから**View Topology**アイコンを選択します。

システムは、表示されたワイヤレスデバイストポロジー上でACを自動的に検出します。

3. ACのアイコンをダブルクリックするか、ACアイコンを右クリックして、ショートカットメニューから**Open Topology**を選択します。

ACのデバイストポロジーが表示され、選択したACとその管理対象APがすべて表示されます。中央ACの場合、デバイストポロジーには、中央ACによって管理されているローカルACも表示されます。

ACデバイストポロジーから、ACで次の操作を実行します。

- ACのアイコンをクリックします。ヒントウィンドウには、デバイスラベル、IPアドレス、デバイスステータス、システム名、ベンダー、システム稼働時間、オンラインAPおよび関連付けられたワイヤレスクライアントなど、ACに関する基本情報が表示されます。これらのパラメーターの詳細は、「ワイヤレスデバイストポロジーの表示」を参照してください。

ACデバイストポロジーから、FIT APで次の操作を実行します。

- FIT APのアイコンをクリックします。ヒントウィンドウには、FIT APに関する次の情報が表示されます。
  - **Device Label**: WSM内のFIT APを識別するデバイスラベル。FIT APのデバイスラベルをクリックすると、その詳細が表示されます。
  - **IP Address**: ACによって取得されたFit APのIPアドレス。
  - デバイスステータス:FIT APの状態。オプションはオンラインまたはオフラインです。
  - **Associated Wireless Clients**: FIT APに関連付けられているクライアントの数。この数をクリックすると、すべてのオンラインクライアントのリストが表示されます。オンラインクライアントリストの詳細は、「クライアントリストの表示」を参照してください。
- FIT APのアイコンを右クリックします。

  このメニューには、FIT APに適用できる次のオプションが表示されます。
  - **Device Information**: FIT APに関する詳細情報を表示できます。
  - **View Physical Topology**: FIT APとACの間の物理接続を表示できます。このオプションは、FIT APとACの両方がComwareベースのデバイスである場合にのみ使用できます。
  - **Lock/Unlock**: トポロジー上のFIT APの位置をロックまたはロック解除できます。FIT APは、ロック後は移動できません。

ACと指定されたFit AP間のリンクで次の操作を実行します。

- ACとFit AP間のプライマリリンクを右クリックし、ショートカットメニューからLink Informationを選択します。

  ヒントウィンドウには、次のリンク情報が表示されます。
  - **Control Channel Security Policy**: ACとAP間のCAPWAPトンネルで使用されるコントロールチャネルのセキュリティポリシー。
  - **Control Channel Startup Time**: ACとAP間のCAPWAPトンネルで使用される制御チャネルの開始時間。
  - **Data Channel Security Policy**: ACとAP間のCAPWAPトンネルで使用されるデータチャネル

のセキュリティポリシー。

- **Data Channel Startup Time**: ACとAP間のCAPWAPトンネルで使用されるデータチャネルの開始時間。

注:

ショートカットメニューのリンク情報オプションは、ACとFit APの両方がComwareベースのデバイスである場合にのみ使用できます。

トポロジー上の空白領域を右クリックすると、ペイン設定のメニューが表示されます。

- **Show Devices**を選択し、次のいずれかのオプションを選択して、トポロジーに表示するデバイスのタイプを決定します。
  - **Show Onlines Only**: オンライン状態の管理対象APだけを表示します。
  - **Show Offlines Only**: オフライン状態の管理対象APだけを表示します。
  - **Show Rogues**: 検出に使用されたFIT APに接続されている不正APおよび不正クライアントを表示します。
  - **Show All Clients**: ACによって管理されているFIT APに関連付けられているすべてのクライアントを表示します。
- **Client Link Label**を選択し、次のいずれかのオプションを選択して、FIT APとクライアント間のリンクのラベルを決定します。
  - **Show Radio Type**: APの無線タイプをリンクラベルとして使用します。
  - 信号強度を表示ワイヤレスクライアントの信号強度をリンクラベルとして使用します。
  - **Show RSSI**: ワイヤレスクライアントの受信信号強度インジケータをリンクラベルとして使用します。
  - **Show Channel**: ワイヤレスクライアントで使用されるチャネルをリンクラベルとして使用します。
  - **No Label**: リンクラベルを使用しません。

右クリックメニューから**Show Devices>Show All Clients**を選択して、ACによって管理されるFIT APに関連付けられたすべてのクライアントを表示するようにACデバイストポロジーを設定すると、トポロジーからクライアントに対してさらに次の操作を実行できます。

- クライアントのアイコンをクリックします。

  ヒントウィンドウには、クライアントに関する次の情報が表示されます。
  - **MAC Address**: クライアントのMACアドレス。クライアントのMACアドレスをクリックすると、クライアントの詳細が表示されます。
  - **Username**: クライアントの名前。
  - **SSID Name**: クライアントがネットワークにアクセスするために使用するSSID。
  - **Radio Type**: クライアントがネットワークにアクセスするときに使用するAPの無線タイプ。
  - **Signal Strength**: クライアントの信号強度。
  - **RSSI**: クライアントの信号のRSSI値。
  - **Channel**: クライアントによって使用されるチャネル。
- クライアントのアイコンを右クリックします。

  メニューには、クライアントに適用できる次のオプションが表示されます。
  - **Client Information**: MACアドレス、クライアント名、接続時間、信号強度、SSID、チャネルなど、クライアントに関する詳細情報を表示できます。Comwareベースのデバイスの場合は、認可モード、AKMタイプ、暗号化モード、およびデータレートを表示できます。クライアントの詳細の詳細は、「クライアントの詳細情報の表示」を参照してください。
  - **Locate**: ロケーションビュー トポロジーを開き、そのトポロジー上でクライアントを検索

できます。詳細は、「ワイヤレス検索の管理」を参照してください。

- **Lock/Unlock**: トポロジー上のクライアントの位置をロックまたはロック解除できます。クライアントは、ロック後は移動できません。

トポロジー上の空白領域を右クリックし、メニューから**Show Devices > Show Rogues**を選択して、ACデバイストポロジー上の不正デバイスを表示します。

次の操作を実行できます。

- 不正デバイスのアイコンをクリックします。

  ヒントウィンドウには、デバイスに関する次の情報が表示されます。

  - **MAC Address**: 不正デバイスのMACアドレス。不正デバイスのMACアドレスをクリックすると、デバイスの詳細が表示されます。不正デバイスの詳細については、「不正クライアントの詳細情報の表示」を参照してください。
  - **Vendor Name**: 不正デバイスのベンダー名。
  - **SSID Name**: 不正なデバイスが無線サービスを提供するために使用するSSID。不正なAPでのみ使用できます。
  - **Last Detect Time**: 不正デバイスが最後に検出された時刻。
  - **Beacon Interval**: 不正デバイスがビーコンフレームを送信する間隔。不正APだけで使用できます。
  - **Max Signal Strength**: 不正デバイスの最大信号強度。
  - **Attack Status**: 不正デバイスがネットワークを攻撃したかどうか。
- 不正なデバイスのアイコンを右クリックします。メニューには次のオプションが表示されます。
  - **Locate**: Location Viewトポロジーを開いて、トポロジー上の不正デバイスを特定できます。
  - **Lock/Unlock**: トポロジー上の不正デバイスの位置をロックまたはロック解除できます。不正デバイスをロックすると、移動できなくなります。

FAT APのデバイストポロジーの表示

1. **Service**タブをクリックします。
2. 次のいずれかの方法を使用して、ターゲットのFAT APを特定します。

   Method 1

   a. ナビゲーションツリーから、**WLAN Manager > Wireless Topology**を選択します。

   b. 空白の領域を右クリックし、ショートカットメニューから**Find**を選択します。

   Query Devicesウィンドウが開きます。

   c. ターゲットFAT APのデバイスラベルをContentボックスに入力します。

   d. **Query**をクリックします。

   ターゲットのFAT APがFind Resultウィンドウに表示されます。

   Method 2

   a. ナビゲーションツリーで、**WLAN Manager > Resource Management > Fat APs**を選択します。

   b. ターゲットFAT APの**Operation**アイコン ･･･をクリックします。

   c. ショートカットメニューから**View Topology**アイコンを選択します。

   システムは、表示されたワイヤレスデバイストポロジー上のFAT APを自動的に特定します。
3. Fat APアイコンをダブルクリックするか、右クリックしてOpen Topologyを選択します。Fat APのデバイストポロジーが表示され、Fat APとそれに関連付けられたすべてのクライアントが表示され

ます。

4. FAT APアイコンをクリックします。

   ヒントウィンドウには、デバイスラベル、IPアドレス、デバイスステータス、システム名、ベンダー、クライアントなど、FAT APに関する基本情報が表示されます。これらのパラメーターの詳細については、「ワイヤレスデバイストポロジーの表示」を参照してください。

5. FAT APデバイストポロジーから、クライアント上で次の操作を実行します。

   - クライアントのアイコンをクリックします。

     ヒントウィンドウには、MACアドレス、クライアント名、無線タイプ、信号強度、RSSIなど、クライアントに関する基本情報が表示されます。これらのパラメーターの詳細については、「ACのデバイストポロジーの表示」を参照してください。

   - クライアントのアイコンを右クリックします。

     このメニューには、クライアントに適用できる管理オプション: **Client Information**、**Locate**、および**Lock/Unlock**が表示されます。これらの管理オプションの詳細については、「ACのデバイストポロジーの表示」を参照してください。

6. トポロジー上の空白領域を右クリックし、ショートカットメニューからUser Link Labelを選択して、クライアントとFAT AP間のリンクのラベルを設定します。オプションは次のとおりです。

   - **Show Radio Type**
   - **Show Signal Strength**
   - **Show RSSI**
   - **Show Channel**
   - **No Label**

   リンクラベルの設定の詳細については、「ACのデバイストポロジーの表示」を参照してください。

物理トポロジーの表示

物理トポロジーには、指定したFit APへのACの接続に関与するネットワークデバイスが表示されます。このトポロジーは、ACとFit APの両方がComwareベースのデバイスである場合にのみ使用できます。

ACと指定されたFit AP間の物理トポロジーを表示するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. 次のいずれかの方法で、ターゲットACを特定します。

   Method 1

   a. ナビゲーションツリーから、**WLAN Manager > Wireless Topology**を選択します。
   b. 空白の領域を右クリックし、ショートカットメニューから**Find**を選択します。

      Query Devicesウィンドウが開きます。

   c. ContentボックスにターゲットAC APのデバイスラベルを入力します。
   d. **Query**をクリックします。

      ターゲットACがFind Resultウィンドウに表示されます。

   Method 2

   a. ナビゲーションツリーで、**WLAN Manager > Resource Management > ACs**を選択します。
   b. ターゲットACのOperationアイコン⋯をクリックします。
   c. メニューからView Topologyアイコンを選択します。

      システムは、表示されるワイヤレスデバイストポロジー上のACを自動的に特定します。

3. ACのアイコンをダブルクリックするか、ACアイコンを右クリックして、ショートカットメニューから**Open Topology**を選択します。

ACデバイストポロジーが表示され、ACとその管理対象のすべてのAPが示されます。

4. FIT APのアイコンを右クリックし、ショートカットメニューから**View Physical To**を選択します。

   Physical Topology(Snapshot)ウィンドウが開き、ACとFIT AP間の物理接続が表示されます。

位置ビュー トポロジー

ロケーションビュー トポロジーには、ロケーションビューに含まれるすべてのFit APとFat AP、およびそれらに関連付けられたクライアントが表示されます。同じロケーションビューに近接して配置されたAPを追加し、ロケーションビュー トポロジーから直接それらに対して集中化された視覚化された管理を実行できます。

ロケーションビュー トポロジーには、ワイヤレスロケーティングおよびワイヤレスRF管理機能もあります。詳細は、「ワイヤレスロケーティングの管理」および「RFの管理」を参照してください。

ロケーションビューの詳細は、「ロケーションビューの管理」を参照してください。

ロケーションビューのトポロジーを表示する手順は、次のとおりです:

1. **Service**タブをクリックします。
2. 次のいずれかの方法を使用して、位置ビュートポロジーを入力します。

   Method 1

   a. ナビゲーションツリーから**WLAN Manager > Wireless Topology**を選択します。

      ワイヤレスデバイストポロジーウィンドウが開きます。

   b. 左側のナビゲーションツリーで、**Topology > Wireless Topology > Location View**を選択します。ロケーションビュー トポロジーには、すべてのロケーションビューが表示されます。

   c. ターゲットロケーションビューのアイコンをダブルクリックするか、ロケーションビューアイコンを右クリックしてショートカットメニューから**Open Topology**を選択します。

      ロケーションビューのトポロジーが表示され、そのロケーションビューに含まれるすべてのサブロケーションビュー、Fit AP、およびFat APが表示されます。

   Method 2

   a. ナビゲーションツリーから、**WLAN Manager > View Management>Location View**を選択します。Location Listには、すべてのロケーションビューが表示されます。

   b. トポロジーを表示するロケーションビューの**View Topology icon**をクリックします。

      ロケーションビューのトポロジーが表示され、そのロケーションビューに含まれるすべてのサブロケーションビュー、Fit AP、およびFat APが表示されます。

サブロケーションビューでは、次のタスクを実行できます。

- ロケーションビューのアイコンをクリックします。ヒントウィンドウには、ロケーションビューに関する次の情報が表示されます。
  - **View Name**: ビューの名前。
  - **View Status**: ビューおよびそのサブビュー内のデバイスの最高アラームレベル。ビューおよびそのサブビューにデバイスが含まれていないか、管理されていないデバイスしか含まれていない場合、このフィールドには**Unmanaged**と表示されます。
- ロケーションビューのアイコンを右クリックします。メ

  ニューには次のオプションが表示されます。
  - **Open Topology**: 位置ビューのトポロジーを開くことができます。
  - **Delete**: ロケーションビューを削除できます。ロケーションビューを削除すると、そのすべて

のサブビューが除去され、これらのビューからすべてのデバイスも除去されますが、WSMからは除去されません。

- **Modify Label**: ューのラベルを修正できます。
- **Lock/Unlock**: トポロジー上のロケーションビューの位置をロックまたはロック解除できます。ロケーションビューは、ロック後は移動できません。

FIT APの場合は、次のタスクを実行できます。

- FIT APのアイコンをクリックします。ヒントウィンドウには、デバイスラベル、IPアドレス、デバイスステータス、クライアントなど、FIT APに関する基本情報が表示されます。これらのパラメーターの詳細は、「ACのデバイストポロジーの表示」を参照してください。
- FIT APのアイコンを右クリックします。

  メニューには、次のオプションが表示されます。

  - **View Physical Topology**: FIT APとAC間の物理接続を表示できます。このオプションは、ACとFIT APの両方がComwareベースのデバイスである場合にのみ使用できます。
  - **Device Information**: FIT APに関する詳細情報を表示できます。
  - **Modify AP**: FIT APの無線のアンテナタイプと角度を変更して、カバレッジエリアを調整できます。詳細については、「RFの管理」を参照してください。
  - **Show Rogue Devices/Hide Rogue Devices**: APによって検出された不正デバイスを表示または非表示にできます。一度に1つのAPによって検出された不正デバイスを表示するようにWSMを設定できます。
  - **Delete Device from this Location**: 現在のロケーションビューからFIT APを削除できます。
  - **Lock/Unlock**: トポロジー上のFIT APの位置をロックまたはロック解除できます。FIT APは、ロック後は移動できません。

FAT APでは、次のタスクを実行できます。

- FAT APのアイコンをクリックします。ヒントウィンドウには、デバイスラベル、IPアドレス、デバイスステータス、システム名、ベンダー、クライアントなど、FAT APに関する基本情報が表示されます。これらのパラメーターについては、「ワイヤレスデバイストポロジーの表示」を参照してください。
- FAT APのアイコンを右クリックします。

  メニューには、次のオプションが表示されます。

  - **Device Information**: FAT APに関する詳細情報を表示できます。
  - **Modify AP**: FAT APの無線のアンテナタイプと角度を変更して、そのカバレッジエリアを調整できます。詳細については、「RFの管理」を参照してください。
  - **Delete Device from this Location**: 現在のロケーションビューからFAT APを削除できます。
  - **Lock/Unlock**: トポロジー上のFAT APの位置をロックまたはロック解除できます。FAT APは、ロック後は移動できません。
- トポロジー上の空白領域を右クリックすると、ペイン設定のメニューが表示されます。
  - **Add Location**: 現在のロケーションビューにサブロケーションビューを追加できます。
  - **Add Devices**: ロケーションビューにデバイスを追加できます。
  - **Add Virtual APs**: 仮想APをロケーションビューに追加できます。仮想APはネットワークプランニングに使用されます。
  - **Modify Virtual AP Labels**: 仮想APのラベルをバッチで変更できます。このオプションは、仮想APがロケーションビューに存在する場合にのみ表示されます。
  - **Delete All Virtual APs**: ロケーションビューからすべての仮想APを削除できます。このオ

プションは、ロケーションビューに仮想APが含まれていない場合は表示されません。

- **Show Interference Devices**: トポロジー上の干渉デバイスを表示するには、このオプションを選択します。
- **Show Channel Quality**: **Show Channel Quality > 802.11 a/an** または **Show Channel Quality > 802.11b/g/gn** を選択して、5GHz 周波数帯域または 2.4GHz 周波数帯域のチャネルの品質を表示します。FIT AP またはFAT AP のチャネル品質はデバイス アイコンの右側に表示され、チャネル品質が低下するにつれて色が薄くなります。

  WSM は、RF 分析をサポートするFIT AP またはFAT AP のチャネル品質のみを表示できます。
- **Hide Channel Quality**: このオプションを選択すると、トポロジーのチャネル品質が非表示になります。
- **Generate Network Planning Report**: ロケーションビューのネットワークプランニングレポートを生成できます。このオプションは、ロケーションビューに仮想APが含まれていない場合は表示されません。
- **Display Coverage Area**: 信号強度、データレート、チャネル、またはSSID別に信号カバレッジエリアを表示できます。
- **Show/Hide Mesh Link**: 現在のロケーションビューでAPメッシュリンクを表示または非表示にできます。詳細については、「メッシュネットワークの管理」を参照してください。
- **Area Policy Configuration**: アクセスエリアコンフィギュレーションモードを開始できます。
- **Color Settings**: APの信号強度、データレート、およびチャネルの色を設定できます。詳細については、「色の設定」を参照してください。
- **Show/Hide Clients**: 現在のロケーションビューで、APに関連付けられたクライアントの表示/非表示を切り替えることができます。
- **Display Client Quantity**: クライアント数量の表示モードを設定できます。オプションは、**Star**, **Number**および**Star**, **Number**です。**Star**, **Number**を選択して、1つの星で表されるクライアントの数と星の色を設定します。**Region Mgt**を選択して、クライアントの数量が表示される範囲を設定します。
- **Show/Hide Radio Information**: APのチャネルおよび伝送パワーを表示または非表示にします。
- **Generate BOM File**: ロケーションビューのBOMファイルを生成できます。BOMファイルには、APの数、APモデル、APの場所、信号強度などの情報が含まれています。ツールバーの**Download BOM File**アイコン をクリックすると、生成されたBOMファイルをダウンロードできます。

クライアントの場合は、トポロジーから次のタスクを実行できます。

- クライアントのアイコンをクリックします。ヒントウィンドウには、MACアドレス、クライアント名、SSID、無線タイプ、信号強度、RSSIなど、クライアントに関する基本情報が表示されます。これらのパラメーターの詳細については、「ACのデバイストポロジーの表示」を参照してください。
- クライアントのアイコンを右クリックすると、オプションが表示されます: **Client Information**、**Locate**、および**Lock/Unlock**。詳細については、「ACのデバイストポロジーの表示」を参照してください。

ロケーションビューの上にあるツールバーでは、次のタスクを実行できます。

- 背景画像を追加するには、**Add Background**アイコンをクリックします。「背景の追加」を参照してください。
  写真」
- 背景画像を削除するには、**Remove Background**アイコンをクリックします。

- 背景ピクチャのスケールを設定するには、**Set Scale**アイコンをクリックします。「スケールの設定」を参照してください。
- 障害物を描画するには、**Add Obstacle**アイコンをクリックします。「障害物の描画」を参照してください。
- AP Calculatorを使用するには、**AP Calculator**アイコンをクリックします。「**AP Calculator**」を参照してください。
- ロケーションビュー情報をエクスポートするには、**Export Location**アイコンをクリックします。ロケーションビュー情報には背景画像と障害物が含まれますが、AP情報は含まれません。
- ロケーションビュー情報をインポートするには、**Import Location**アイコンをクリックします。ロケーションビュー情報には背景画像と障害が含まれますが、AP情報は含まれません。
- BOMファイルをダウンロードするには、**Download BOM File**アイコンをクリックします。表示されたウィンドウで、BOMファイルが生成された時刻を確認し、生成されたファイルをサーバーから削除できます。
- APの検索モードを設定するには、ツールバーの**Set AP locating mode**アイコンをクリックします。表示されるウィンドウで、ターゲットAPを選択し、Set to Locating APまたはSet to Non-Locating APボタンをクリックします。

ワイヤレスカスタムビュートポロジー

ワイヤレスカスタムビュートポロジーでは、ワイヤレスカスタムビューに基づいて、カスタムビューに含まれるACによって管理されるFIT AP、FIT APに関連付けられたクライアント、およびFIT APによって検出された不正デバイスが表示されます。ワイヤレスカスタムビュートポロジーは主に次のシナリオで使用されます。多数のFIT APが同じACに接続されている場合、特別な注意が必要なFIT APをカスタムビューに追加できます。その後、カスタムビューのトポロジーから関連するFIT APを直接検索して管理できます。

ワイヤレスカスタムビューの詳細は、「ワイヤレスカスタムビューの管理」を参照してください。

ワイヤレスカスタムビューのトポロジーを表示するには、次の手順を実行します:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから**WLAN Manager > Wireless Topology**を選択します。

   ワイヤレスデバイストポロジーウィンドウが開きます。
3. 左側のナビゲーションツリーで、**WLAN Manager** > **Wireless Topology**を選択します。

   カスタムビュートポロジーには、すべてのカスタムビューが表示されます。

   カスタムビューでは、次のタスクを実行できます。
   - カスタムビューのアイコンをクリックします。

     ヒントウィンドウには、ビューに関する次の情報が表示されます。
     - **View Name**: ビューの名前。
     - **View Status**: ビューのステータス。ステータスは、ビュー内で最も高いアラームレベルを持つデバイスによって決定されます。ビューにデバイスが含まれていない場合、または管理されていないデバイスのみが含まれている場合、このフィールドには**Unmanaged**と表示されます。
   - カスタムビューのアイコンを右クリックします。メニューには次のオプションが表示されます。
     - **Open Topology**: カスタムビューのトポロジーを開くことができます。
     - **Delete**: カスタムビューを削除できます。ビューを削除すると、すべてのデバイスがビューから削除されますが、WSMからは削除されません。

Modify Label: ビューのラベルを修正できます。

Lock/Unlock: トポロジー上のカスタムビューの位置をロックまたはロック解除できます。カスタムビューは、ロック後は移動できません。

- 新しいカスタムビューを作成するには、空白の領域を右クリックし、ショートカットメニューから**Add Wireless Custom View**を選択します。

4. カスタムビューのアイコンをダブルクリックするか、カスタムビューアイコンを右クリックして、ショートカットメニューから**Open Topology**を選択します。カスタムビューのトポロジーには、ビューに含まれるACとその管理されたFIT APが表示されます。

ACの場合は、トポロジーから次の作業を実行できます。

- ACのアイコンをクリックします。

  ヒントウィンドウには、デバイスラベル、IPアドレス、デバイスステータス、システム名、ベンダー、システム稼動時間、合計AP数、クライアント数など、ACに関する基本情報が表示されます。詳細については、「ACのデバイストポロジーの表示」を参照してください。

FIT APの場合は、トポロジーから次のタスクを実行できます。

- FIT APのアイコンをクリックします。

  ヒントウィンドウには、デバイスラベル、IPアドレス、デバイスステータス、クライアントなど、FIT APに関する基本情報が表示されます。これらのパラメーターの詳細については、「ACのデバイストポロジーの表示」を参照してください。

- FIT APのアイコンを右クリックします。

  メニューには、次のオプションが表示されます。

  - **Device Information**: FIT APに関する詳細情報を表示できます。
  - **View Physical Topology**: FIT APとAC間の物理トポロジーを表示できます。このオプションは、ACとFIT APの両方がComwareベースのデバイスである場合にのみ使用できます。
  - **Delete Device from this View**: 現在のカスタムビューからFIT APを削除できます。
  - **Lock/Unlock**: トポロジー上のFIT APの位置をロックまたはロック解除できます。FIT APは、ロック後は移動できません。

カスタムビュートポロジーからアクセスできるその他のオプションは次のとおりです。

- FIT APのアイコンをダブルクリックすると、そのAPに関連付けられているすべてのクライアントが表示されます。クライアントを非表示にするには、FIT APアイコンをもう一度ダブルクリックします。

  トポロジーからクライアントに対して次の操作を実行できます。

  - クライアントのアイコンをクリックします。

    ヒントウィンドウには、MACアドレス、ユーザー名、SSID名、無線タイプ、信号強度、RSSIなど、クライアントに関する基本的な情報が表示されます。これらのパラメーターについては、「ACのデバイストポロジーの表示」を参照してください。

  - クライアントのアイコンを右クリックします。

    ショートカットメニューには、クライアントに適用できる管理オプション(**Client Information**、**Locate**、および**Lock/Unlock**)があります。これらの管理オプションの詳細については、「ACのデバイストポロジーの表示」を参照してください。

- ACとFIT AP間のプライマリリンクを右クリックし、ショートカットメニューからリンク情報を選択します。

  ウィンドウが開き、リンクに関する次のような情報が表示されます。

  - **Control Channel Security Policy**
  - **Control Channel Startup Time**
  - **Data Channel Security Policy**
  - **Data Channel Startup Time**

これらのパラメーターについては、「ACのデバイストポロジーの表示」を参照してください。

注:

右クリックメニューの**Link Information**オプションは、ACとFit APの両方がComwareベースのデバイスである場合にのみ使用できます。

- トポロジー上の空白領域を右クリックし、ショートカットメニューから**Add Devices to this View**を選択します。
- **Select Devices**ウィンドウで、ビューに追加するFIT APを選択し、OKをクリックします。

  ワイヤレスカスタムビュートポロジーから不正デバイスを監視および管理することもできます。詳細については、「ACのデバイストポロジーの表示」を参照してください。

コンバージド トポロジー

集約されたトポロジーには、ワイヤレスデバイスとワイヤードデバイス、およびネットワーク内のそれらの接続が表示されます。必要に応じてデバイスをトポロジーに追加して、トポロジーからワイヤレスデバイスを直接監視および管理できます。

ベストプラクティスとして、クラウドを使用してWLANを管理し、サブビューを使用してワイヤレスサービスを管理します。

ここでは、ワイヤレスデバイスの基本的な操作だけを説明します。コンバージドトポロジーの詳細については、『H3C IMC v7.3 Enterprise and Standard Platform Administrator Guide』を参照してください。

集約されたトポロジーを表示するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから**WLAN Manager > Wireless Topology**を選択します。

   ワイヤレスデバイストポロジーウィンドウが開きます。
3. 左側のナビゲーションツリーで、**Topology** > **Converged Topology**を選択します。集約トポロジーには、すべての集約ビューが表示されます。
4. 収束ビューのアイコンをダブルクリックします。

   統合ビューには、有線デバイスと無線デバイスが表示されます。
5. ワイヤレスデバイスをビューに追加するには、**Add Wireless Device to this View**アイコン  をクリックします。ACまたはFAT APの場合は、トポロジーから次のタスクを実行できます。

- ACまたはFAT APのアイコンをクリックします。

  ヒントウィンドウには、デバイスラベル、IPアドレス、デバイスステータス、システム名、ベンダー、実行時間、最後のポーリング時間など、ACまたはFAT APに関する基本情報が表示されます。これらのパラメーターの詳細については、『IMC Base Platform Administrator Guide』を参照してください。
- ACまたはFAT APのアイコンを右クリックします。

  メニューには次のオプションが表示されます。

  - Performance at a Glance
  - Create Performance View
  - Real-Time Monitor
  - Create Subview
  - Device Information
  - Tools

- Delete Device from This View
- Synchronize

これらのパラメーターについては、『H3C IMC v7.3 Enterprise and Standard Platform Administrator Guide』を参照してください。

FIT APの場合は、トポロジーから次のタスクを実行できます。

- FIT APのアイコンをクリックします。

  ヒントウィンドウには、Fit APに関する次の基本情報が表示されます。

  - **Device Label** :APのラベル。デバイスラベルをクリックすると、APに関する詳細情報が表示されます。
  - **AP Name**: APの名前。
  - **AP Alias**: APのエイリアス。
  - **MAC Address**: APのMACアドレス。
  - **IP Address**: APのIPアドレス。
  - **Location**: APが存在するロケーションビュー。
  - **Device Status**: APのステータス(OnlineまたはOffline)。
  - **Associated Wireless Clients**: APにアソシエートされているクライアントの数。この数をクリックすると、APのクライアントリストが表示されます。
- FIT APのアイコンを右クリックします。

  メニューには、次のオプションが表示されます。

  - **Energy Policy Management** :Energy Policy Managementページを表示できます。
  - **Reset**: FIT APをリセットできます。
- トポロジー上の空白領域を右クリックすると、ペイン設定のメニューが表示されます。
  - **Display Client Quantity**: クライアント数量の表示モードを設定できます。オプションは**Star**および**Number**.です。

ワイヤレスネットワークのセキュリティを管理する

ワイヤレスネットワークは、不正または悪意のあるAPやクライアント(この章では不正APおよび不正クライアントと呼びます)など、さまざまな脅威の影響を受けます。WIDSモデルを使用して、不正なAPおよびクライアントを監視および管理できます。

IDS機能の概要

ComwareベースのACのIDS機能について説明します。

ComwareベースのAC上のIDS

ComwareベースのACでは、WIDS検出規則を使用して、FIT APが認証されたAPか不正なAPかを判断します。

WIDS検出規則を設定すると、次のリストが維持されます。

- **Permitted-OUI list**: OUIリスト信頼できるベンダーのOUIで構成されます。
- **Permitted-SSID list**: 信頼されたワイヤレスネットワークのSSIDで構成されます。
- **Permitted-MAC address list**ト: 信頼できるAPおよび信頼できるクライアントのMACアドレスで構成されます。
- **MAC-to-attack List**: 不正なAPおよび不正なクライアントのMACアドレスで構成されます。ACは、

WIDS検出規則に基づいて、デバイスを不正デバイスおよび許可デバイスとして分類します。

- 許可リストのいずれかにあるすべてのAPおよびクライアントは、正当なデバイスと見なされます。ACは許可します。
  これらのAPとクライアントは、サービスを提供したり、ワイヤレスネットワークにアクセスしたりするために使用されます。
- 許可リストにないAPまたはクライアントは、それぞれ**Rogue APs**モジュールおよび**Rogue Clients**モジュールから管理できる不正なAPまたはクライアントと見なされます。
- MAC-to-attackリスト上のAPおよびクライアントに対しては、無線ネットワークへの影響を防ぐために、ACに対して攻撃を開始するようにACを設定できます。

WIDS Configページへのアクセス

WIDS Configページには、WSM内のすべての管理対象ACがリストされます。このページから、次の操作を実行できます。

- ComwareベースのACのWIDS検出規則を設定します。
- 不正なAPを検出するための、ACによって管理されるFit APのイネーブル化またはディセーブル化。

WIDS Configページにアクセスするには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIDS Management > WIDS Config**を選択します。ACsリストには、WSM内のすべてのACが表示されます。

   AC List content

   - **Status**: ACのIDS機能の状態(🔴Disableまたは🟢Enable)。このフィールドには、Comwareベ

ースのACの場合は常に Enableと表示されます。

- **Device Label**: ACのデバイスラベル。ラベルをクリックすると、ACの詳細が表示されます。
- **Model**: ACモデル。
- **IP Address**: ACのIPアドレス。
- **Detector**: **Network Detector**でイネーブルにされた、ACによって管理されるFIT APの数。

  番号をクリックすると、Detect Fit AP Listページが表示されます。

  - **Comware-based AC**: **Detect Fit AP List**ページには、作業モードがHybridまたはMonitorのManaged Fit APが表示されます。このページでは、Fit APの作業モードをバッチ単位で設定できます。
- **Operation**: **Operation**アイコン をクリックすると、**Operation**メニューが表示されます。
  - **Comware-based AC**: OperationメニューにはWIDS Detection Ruleオプションがあります。このオプションを使用すると、ACに対してWIDSの検知ルールを設定できます。

ACリストに十分なエントリーが含まれている場合は、次のナビゲーション支援が表示されます。

- **Next Page**アイコンをクリックして、AC Listの次のページに移動します。
- **Last Page**アイコンをクリックすると、AC Listの最後にページ送りされます。
- **Previous Page**アイコンをクリックして、AC Listで前のページに戻ります。
- **First Page**アイコンをクリックすると、AC Listの先頭に戻ることができます。

ACリストの右上にある**8**、**15**、**50**、**100**、または200をクリックして、1ページに表示する項目数を設定します。

注:

AC Listは、**Operation**フィールド以外のすべてのフィールドでソートできます。列ラベルをクリックすると、選択したフィールドでリストをソートできます。列ラベルを使用すると、各フィールドに固有のソートオプションを切り替えることができます。ACは、指定したソート基準にかかわらず、常にリストの最初の行に表示されます。

WIDS Configページでの ACのクエリー

WSMには、基本問合せと拡張問合せが用意されています。基本問合せ基準には、迅速な検索のためのキーパラメーターがいくつか含まれています。拡張問合せには、正確な照合のための様々な問合せ基準が用意されています。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manage r> WIDS Management > WIDS Config**を選択します。ACsリストには、WSM内のすべての管理対象ACが表示されます。
3. 基本的なquery:を実行します。
   a. ACのデバイスラベル(大/小文字を区別)またはIPアドレスを入力します。WSMは、このフィールドのファジーマッチングをサポートします。たとえば、19と入力すると、デバイスラベルまたはIPアドレスに19が含まれるすべてのACが問い合せられます。
   b. **Query**アイコンをクリックします。**AC List**」に、問合せ基準に一致するすべてのACが表示されます。
   c. **Query**フィールドをクリアして**Query**アイコンをクリックすると、すべてのACが表示されます。
4. 高度なクエリーを実行します。
   a. **Query**フィールドの横にある**Expand**アイコンをクリックして**Query**領域を拡張します。再度

クリックするとQuery領域が非表示になります。

b. **Query**領域で、次の問合せ基準を1つ以上入力または選択します。
   - **Device Label**: ACのデバイスラベルを入力します。WSMは、このフィールドのファジーマッチングをサポートします。
   - **IP Address**: ACのIPアドレスを入力します。WSMは、このフィールドのファジーマッチングをサポートします。
   - **WIDS Status**: ACのWIDS状態を選択します。オプションは、Unlimited、Enable、および無効にします。
   - **Vendor**: Cのベンダーを選択します。オプションは、無制限、H3Cです。

c. **Query**をクリックします。ACリストに、問合せ基準に一致するすべてのACが表示されます。

d. **Reset**をクリックして、クエリー基準をクリアし、すべてのACを表示します。

不正なAPを検出するためのFit APのイネーブル化とディセーブル化

ACによって管理されるFit APをイネーブルまたはディセーブルにして、不正なAPを検出できます。

- ComwareベースのFit APで不正なAPを検出できるのは、その作業モードがMonitorまたは**Hybrid**。

Detect Fit APページへのアクセス

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIDS Management > WIDS Config**を選択します。

   ACsリストには、WSM内のすべての管理対象ACが表示されます。
3. ComwareベースのACの**Detector**カラムにある番号リンクをクリックします。

   Device Listには、ACによって管理され、作業モードが**Monitor**または**Hybrid**。

   Device List content
   - **Online Status**: FIT APのオンライン状態(Onlineアイコンとofflineアイコン)。
   - デバイスステータス:FIT APのアラームまたは管理状態。オプションは次のとおりです。
     - **Critical**
     - **Major**
     - **Minor**
     - **Warning**
     - **Normal**
     - **Unknown**
     - **Unmanaged**
   - **AP Label**: FIT APのラベル。ラベルをクリックすると、FIT APの詳細が表示されます。
   - **AP Name**: FIT AP名。
   - **SN**: FIT APのシリアル番号。
   - **IP Address**: FIT APのIPアドレス。
   - **MAC Address** :FIT APのMACアドレス。
   - **Model**: Fit APモデル。

- **Work Mode**: Fit APの作業モード。常に**Hybrid**または**Monitor**です。このカラムは、Comwareベースの Fit APでのみ使用できます。
- **AC**: FIT APを管理するACのデバイスラベル。ラベルをクリックすると、ACの詳細が表示されます。デバイスリストに十分なエントリーが含まれている場合は、次のナビゲーションエイドが表示されます:

- **Next Page**アイコンをクリックして、**Device List**で次のページに進みます。
- **Last Page**アイコンをクリックして、**Device List**の最後のページに進みます。
- **Previous Page**アイコンをクリックして、**Device List**で前のページに戻ります。
- **First Page**アイコンをクリックすると、**Device List**の先頭にページバックします。

デバイスリストの右上にある**8**、**15**、**50**、**100**、または**200**をクリックして、1ページに表示する項目数を設定します。

注:

デバイスリストをフィールドごとにソートできます。列ラベルをクリックすると、選択したフィールドごとにリストがソートされます。列ラベルを使用すると、各フィールドに固有のソートオプションを切り替えることができます。ACは、指定したソート基準にかかわらず、常にリストの最初の行に表示されます。

FIT APの検出のクエリー

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIDS Management > WIDS Config**を選択します。
   ACsリストには、WSM内のすべての管理対象ACが表示されます。
3. ACの**Detector**カラムの番号リンクをクリックします。
   Device Listには、ACによって管理され、作業モードが**Monitor**または**Hybrid**。
4. **Device Query**領域で、次のクエリー基準を1つ以上入力または選択します。
   - **AP Label**: APのデバイスラベルの一部または全部を入力します。
   - **AP Name**: APのデバイス名の一部または全部を入力します。
   - **Serial Number**: APのシリアル番号の一部または全部を入力します。
   - **IP Address**: APのIPアドレスの一部または全体を入力します。
   - **AC**: このフィールドには、AC名が表示されます。
5. **Query**.をクリックします。
   Device Listには、クエリー基準に一致するすべてのACが表示されます。クエリー基準をクリアしてすべてのACを表示するには、Resetをクリックします。

不正なAPを検出するためのFit APのイネーブル化とディセーブル化

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIDS Management > WIDS Config**を選択します。ACsリストには、WSM内のすべての管理対象ACが表示されます。
3. ACのDetectorカラムの番号リンクをクリックします。
   Detect Fit AP Listページが開きます。

4. Device List領域で**Enable Detecting Fit AP**をクリックします。

   Enable Detecting Fit APページが開きます。

5. ACベンダーに応じて、次のいずれかを実行します。
   - **Comware-based AC**: Configure AP Work Mode領域で、FIT APの作業モードを選択します。オプションは**Normal**、**Monitor**、および**Hybrid**です。FIT APが不正なAPを検出できるようにするには、このフィールドをMonitorまたはHybridに設定します。

6. Fit AP List領域でAddをクリックします。

   Select Devicesダイアログボックスが開き、ACによって管理されているすべてのAPが表示されます。

7. 設定を適用する1つ以上のFIT APを選択し、OKをクリックします。選択したFIT APがFit AP Listに表示されます。

8. OKをクリックします。

   WSMは、選択されたFIT APのモニタリングステータスの設定を開始し、操作が完了すると結果リストページを表示します。

9. **Back**をクリックして、**Detect Fit AP**ページに戻ります。

   Device Listには、不正なAPを検出するためにイネーブルにされたすべてのFit APが表示されます。

許可されたAPのエクスポート

ComwareベースのACにはManaged Fit APをエクスポートできます。

許可されたAPをエクスポートするには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIDS Management > WIDS Config**を選択します。ACsリストには、WSM内のすべての管理対象ACが表示されます。
3. 次のいずれかの方法で、**Export Authorized AP List**ページに移動します。
   - 1つまたは複数のACを選択し、ACリスト領域でExport Authorized APをクリックします。
   - ACの**Operation**アイコン ⋯ をクリックして、ショートカットメニューから**Export Authorized AP List**を選択します。

   Options of Exporting Authorized APウィンドウが開きます。

4. エクスポートするAPのタイプを選択します。オプションは次のとおりです。
   - **Management AP**: エクスポートは、ACによって管理されるFIT AP。
   - **Manually Authorized AP**: 手動で許可されたAPをエクスポートします。

   ComwareベースのACの場合は、Management Fit APだけをエクスポートできます。

5. **Export**.をクリックします。

エクスポートされたテンプレートファイルをダウンロードするためのページが開きます。

6. **Export Result**をクリックして、許可APリストを保存または開きます。

許可されたAPのインポート

1つのACまたは複数のACについて、.csvファイルから認可APリストをインポートできます。認可APリストは、MACアドレス別のAPのリストを示します。ACは、検出された不正なAPのMACアドレスを、認可APリスト内のMACアドレスと照合します。一致する場合、ACは検出された不正なAPを認可APとして分類します。

許可されたAPリストファイルは.csv形式である必要があり、次のカラムだけを含めることができます。

- **BSSID**: FIT APのMACアドレス(フォーマットはhh:hh:hh:hh:hh:hh)。
- **Mask**: BSSIDのマスクサイズ。有効な値の範囲は0～8です。

  マスクサイズは、IPマスクサイズと逆方向に機能します。マスクサイズを4ビットに指定すると、最後の4ビットがベースBSSIDからそれを共有するBSSIDに変更されます。たとえば、マスクサイズが4のベースBSSID 0e:1f:3a:4d:5e:01には、0e:1f:3a:4d:5e:02、0e:1f:3a:4d:5e:03、0e:1f:3a:4d:5e:04、および0e:1f:3a:4d:5e:0fのBSSIDが関連付けられます。
- **Last Discovery Time**: FIT APが最後に検出された(YYYY-MM-DDまたはMM-DD-YYYY形式)。

許可されたAPリストファイルの最初の行は、APデータまたは列見出しのいずれかです。最初の行が列見出しの場合は、BSSIDの左側にポンド記号(#)が追加されていることを確認してください。データ形式が正しくないと、インポートに失敗する可能性があります。

許可APリストをインポートするには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIDS Management > WIDS Config**を選択します。ACsリストには、WSM内のすべての管理対象ACが表示されます。
3. 次のいずれかの方法で、Import Authorized AP MAC Addressページに移動します。
   - 1つまたは複数のACを選択し、ACリスト領域でImport Authorized APをクリックします。
   - ACの**Operation**アイコンを･･･ クリックし、ショートカットメニューからImport Authorized AP Listを選択します。
4. **Browse**をクリックして、インポートするファイルを選択します。
5. **Next**.をクリックします。

   Import Authorized AP Listページが開き、インポートされた認可APリストに含まれるすべてのFIT APが表示されます。
6. OKをクリックして、FIT APのインポートを開始します。

   操作が完了すると、Result Listページにインポート結果が表示されます。

   Result List content
   - **AC**: ACのラベル。
   - **IP Address**: ACのMACアドレス。
   - **Result**: FIT APのインポート結果。
7. OKをクリックして、WIDS Configページに戻ります。

ComwareベースのACのWIDS検出規則の設定

WSMを使用すると、ComwareベースのACに対してWIDS検出規則を設定できます。WIDS検出規則は、不正なAPおよびクライアントを判別するために、ACによって管理されるFIT APによって使用されます。

次のいずれかの方法で、WIDS検出規則を設定するためのページにアクセスできます。

Method 1:

AC detailsページで、ページの右側にあるRRM Management領域のWIDS Detection Ruleをクリックします。

Method 2:

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > WIDS Management > WIDS Config**を選択します。

3. **Operation**メニューからWIDS Detection Ruleを選択し

   ます。WIDS Detection Ruleページが開きます。

次の情報では、方法2を使用しています。

ACの許可されたOUIリストの保守

ベンダーのワイヤレスデバイスがワイヤレスネットワークにアクセスできるようにするには、ベンダーのOUIを許可OUIリストに追加します。

許可されたOUIを追加するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIDS Management > WIDS Config**を選択します。

   WIDS Configページにすべてのacが表示されます。
3. ComwareベースのACのOperationアイコン ･･･をクリックし、ショートカットメニューからWIDS Detection Ruleを選択します。

   WIDS Detection Ruleページが開きます。
4. **Permitted OUI**タブをクリックします。
5. **Permitted OUI**フィールドに、許可されるOUIをhh:hh:hhの形式で入力します。
6. **Add**をクリックします。

   許可されたOUIを削除するには、Permitted OUI ListからOUIを選択してDeleteをクリック。

ACの許可されたSSIDリストの維持

ワイヤレスネットワークがユーザーにサービスを提供できるようにするには、そのSSIDを許可された

SSIDリストに追加します。許可されたSSIDを追加するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIDS Management > WIDS Config**を選択します。

   WIDS Configページにすべてのacが表示されます。
3. ComwareベースのACの**Operation**アイコン ･･･ をクリックし、ショートカットメニューからWIDS Detection Ruleを選択します。

   WIDS Detection Ruleページが開きます。
4. **Permitted SSID**タブをクリックします。
5. Permitted SSIDフィールドに許可されるSSIDを入力します。
6. **Add**.をクリックします。

   許可されたSSIDを削除するには、Permitted SSID ListからSSIDを選択し、Deleteをクリックします。

ACの許可されたMACアドレスリストの保守

APがサービスを提供したり、モバイルユーザがワイヤレスネットワークにアクセスしたりできるようにするには、MACアドレスを許可MACアドレスリストに追加します。

許可MACアドレスを追加するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIDS Management > WIDS Config**を選択します。

   WIDS Configページにすべてのacが表示されます。

3. ComwareベースのACの**Operation**アイコン ⋯ をクリックし、ショートカットメニューからWIDS Detection Ruleを選択します。

   WIDS Detection Ruleページが開きます。

4. Permitted MACタブをクリックします。
5. 許可MACアドレスを追加するには、次のいずれかの方法を使用します。
   a. Permitted MACフィールドに、許可されるMACアドレスをhh:hh:hh:hh:hh:hh:hhの形式で入力し、Addをクリックします。
   b. Select Rogue Listをクリックし、許可するMACアドレスを選択して、OKをクリックします。

   許可されたMACアドレスを削除するには、Permitted MAC ListからMACアドレスを選択して、**Delete**をクリックします。

ACのMAC-to-attackリストの保守

不正なクライアントまたはAPがネットワークにアクセスしたり、ワイヤレスサービスを提供したりしないようにするには、そのMACアドレスをMAC-to-attackリストに追加します。ACは、MAC-to-attackリストにある不正なAPだけを攻撃できます。

攻撃対象のMACアドレスを追加するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIDS Management > WIDS Config**を選択します。WIDS Configページにすべてのacが表示されます。
3. ComwareベースのACの**Operation**アイコン ⋯ をクリックし、ショートカットメニューからWIDS Detection Ruleを選択します。

   WIDS Detection Ruleページが開きます。

4. MAC to Attackタブをクリックします。
5. 次のいずれかの方法を使用して、攻撃対象のMACアドレスを追加します。
   a. **MAC to Attack**フィールドに、MACアドレスをhh:hh:hh:hh:hh:hh:hh:hhの形式で入力し、**Add**をクリックします。
   b. **Select Rogue List**をクリックし、攻撃するMACアドレスを選択して、OKをクリックします。

   攻撃対象のMACアドレスを削除するには、MAC-to-Attack ListからMACアドレスを選択し、**Delete**をクリックします。

静的ブラックリストの設定

スタティックブラックリストのクライアントは、WLANにアクセスできません。

この機能は、Comware V5ソフトウェアバージョンを実行するH3C ACでのみサポートされます。スタティックブラックリストを設定するには、次の手順を実行します。

1. 次のいずれかの方法を使用して、Set Static Blacklistページを表示します。

   Method 1
   a. **Service**タブをクリックします。
   b. ナビゲーションツリーで、**WLAN Manager > WIDS Management > WIDS Config**を選択します。
   c. WIDS Configページに、すべてのACが表示されます。
   d. ComwareベースのACの**Operation**アイコン ⋯ をクリックし、メニューからSet Static Blacklistを選択します。

Method 2

a. **Service**タブをクリックします。

b. ナビゲーションツリーから、**WLAN Manager > Resource Management > ACs**を選択します。

AC Listページにすべてのが表示されます。

c. 詳細情報を表示するComwareベースのACのデバイスラベルをクリックします。

ACの詳細ページが開きます。

d. ページの右側にあるAC Configuration領域でSet Static Blacklistを選択します。

2. 次のいずれかの方法を使用して、クライアントをかの方法を使用します。
   - クライアントのMACアドレスを入力し、**Add**をクリックします。
   - **Select Rogue Clients List**をクリックし、1つまたは複数のMACアドレスを選択して、OKをクリックします。

   ブラックリストからクライアントを削除するには、静的ブラックリストから1つ以上のMACアドレスを選択し、**Delete**をクリックします。

不正なAPの管理

WSMは、不正なAPを管理するための一連の機能を提供します。

不正APリストの表示

検出されたすべての不正APは、不正APリストに追加されます。不正APリストを表示するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIDS Management > Rogue APs**を選択します。

   Rogue APsページが開き、検出されたすべての不正APが表示されます。

   不正APの情報には、次のフィールドがあります。
   - **MAC Address**: 不正APのMACアドレス。不正APの詳細情報を表示するには、MAC addressリンクをクリックします。詳細情報のフィールドの説明については、「Comwareベースの不正APに関する詳細情報の表示」を参照してください。
   - **Class**: 不正APが属するクラス。Unlimited、Rogue、External、Forced Authorized、Controlled Authorized、およびUnclassifiedがあります。
   - **Vendor**: 不正APのベンダー。不正APのベンダーが検出できない場合、このフィールドにはOthersと表示されます。
   - **BSSID**: 不正APのサービスSSID。
   - **Channel**: 不正なAPが無線サービスを提供するために使用するチャネル。
   - 信号強度:不正APの信号強度(dBm)。
   - **Detected by**: 不正なAPを検出したAC。ACに関する詳細情報を表示するには、ACリンクをクリックします。ACの詳細情報に関するフィールドの説明については、「Managing Comware-based access controllers」を参照してください。
   - **Last Discovered a**t: 不正APが最後に検出された時刻。
   - **Operation**:不正なAPの**Operation**アイコン ⋯ をクリックして、**Operation**メニューを表示します。

     Comwareベースの不正APの場合、許可MACアドレスリストまたはMAC-to-attackリストに

不正APを追加し、MAC-to-attackリストから削除して、トポロジー上で不正APを特定できます。

注:

Rogue AP Listは、Operationフィールド以外のすべてのフィールドでソートできます。選択したフィールドでリストをソートするには、列ラベルをクリックします。列ラベルを使用すると、各フィールドに固有のさまざまなソートオプションを切り替えることができます。

不正なAPのクエリー

WSMには、基本問合せと拡張問合せが用意されています。基本問合せ基準には、迅速な検索のためのキーパラメーターがいくつか含まれています。拡張問合せには、正確な照合のための様々な問合せ基準が用意されています。

不正なAPをクエリーするには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > WIDS Management > Rogue APs**を選択します。
3. 基本的なQueryを実行します。
   a. 不正APのデバイスラベル(大文字と小文字を区別)またはIPアドレスを入力します。WSMは、このフィールドのファジーマッチングをサポートします。たとえば、**19**と入力すると、デバイスラベルまたはIPアドレスに**19**が含まれるすべての不正APが照会されます。
   b. **Query**アイコンをクリックします。**Rogue AP List**には、クエリー基準に一致するすべての不正APが表示されます。
   c. **Query**フィールドをクリアして**Query**アイコンをクリックすると、すべての不正なAPが表示されます。
4. 高度なクエリーを実行します。
   a. Queryフィールドの横にある**Expand**アイコンをクリックしてQuery領域を拡張します。再度クリックするとQuery領域が非表示になります。
   b. ページのクエリー領域で、1つ以上のクエリー条件を入力または選択します。
      - **MAC Address**: 不正APのMACアドレスを入力します。ファジーマッチングがサポートされています。たとえば、0と入力すると、MACアドレスに0が含まれるすべての不正APが表示されます。
      - **SSID**: 不正APのサービスSSIDを入力します。ファジーマッチングがサポートされています。たとえば、Wと入力すると、SSIDにWが含まれるすべての不正APが表示されます。
      - **Last Discovered at**: ドロップダウンリストから、時間範囲を選択します。オプションは、Last Day、Last 3 Days、Last 7 Days、Last MonthおよびUnlimitedです。
      - **Class**: 不正APが属するクラスを選択します。オプションは、Unlimited、Rogue、External、Authorized、およびUnclassifiedです。

        空のフィールドや無制限に設定されたフィールドは、Queryの抽出条件にはなりません。
   c. **Query**をクリックします。

      Rogue AP Listには、クエリー基準に一致するすべての不正APが表示されます。
   d. **Reset**をクリックして不正APを表示するには、Resetをクリックします。

Comwareベースの不正APに関する詳細情報の表示

Comwareベースの不正APの詳細情報ページには、不正APに関するすべての情報(不正APの場所と不正APを検出したAPを含む)が表示され、ページの右側にあるAction領域で不正APに対して実行できるすべてのアクションが示されます。

不正なAPに関する詳細情報を表示するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > WIDS Management > Rogue APs**を選択します。
3. 不正なAPのMACアドレスリンクをクリックします。

   不正APの詳細情報ページが開き、次の情報が表示されます。

   不正APの情報

   - **MAC Address**: 不正APのMACアドレス。
   - **Detected by**: 不正なAPを検出したAC。ACに関する詳細情報を表示するには、ACリンクをクリックします。ACの詳細情報に関するフィールドの説明については、「Managing Comware-based access controllers」を参照してください。
   - **Vendor**: 不正なAPのベンダー。
   - **SSID**: 不正なAPのサービスSSID。
   - **First Discovered at**: 不正APが最初に検出された時刻。
   - **Last Discovered at:** 不正APが最後に検出された時刻。
   - **Max Signal Strength(dBm)**: 不正APの最大信号強度。
   - **Channel with Max Signal Strength**: 不正なAPが最大信号強度で最後に検出されたチャネル。
   - **Attacked Status**: 値はAttackedとNot Attackedです。不正なAPがACによって攻撃された場合、値はアイコンで表される**Attacked**またはアイコンで表される**Not Attacked**です。
   - **Crypto**: 値はYesおよびNoです。不正なAPが暗号化されたワイヤレスネットワークサービスを提供している場合、値はYesとなり、アイコンで示されます。Noの場合、値はNoです。

   検出されたAPの情報

   - **Detected by**: 不正なAPを検出したディテクタAP。ディテクタAPに関する詳細情報を表示するには、ディテクタAPリンクをクリックします。APの詳細情報に関するフィールドの説明については、「Managing Comware-based Access Controllers」を参照してください。
   - **First Discovered at**: ディテクタAPが最初に不正APを検出した時刻。
   - **Last Discovered at**: 最後にディテクタAPが不正APを検出した時刻。
   - **Signal Strength**: 不正なAPの信号強度。
   - **Channel**: 不正なAPが無線ネットワークサービスを提供するチャネル。
   - **Attacked Status**: ディテクタAPが不正なAPを攻撃したかどうか。YESの場合、値は**Attacked**です。
     攻撃されている。攻撃されていない場合、値は**Not Attacked**.」です。
   - **Radio ID**: 不正なAPを検出した無線。

   場所

   - **Location**: 不正なAPが存在するロケーションビュー。ロケーションビューでデバイスを表示するには、ロケーションリンクをクリックします。
   - **Open Topology**: 不正APが属するトポロジーを開きます。トポロジー上の不正APの位置を表示するには、**View Topology**アイコンをクリックします。

注:

ロケーションエリアは、ディテクタAPがロケーションビューに追加された場合にのみ表示されます。ロケーションビューにAPを追加する方法については、「ロケーションビューまたはサブロケーションビューへのAPの追加」を参照してください。

Action

- **Refresh**: 不正APおよびディテクタAPの情報をリフレッシュします。
- **Add to Attack List**: 不正APをMAC-to-attackリストに追加します。このアクションの使用方法の詳細については、「Adding Comware-based rogue APs to the MAC-to-attack list」を参照してください。
- **Remove from Attack List**: MAC-to-attackリストから不正APを削除します。このアクションの使用方法の詳細については、「Removing Comware-based rogue APs from the MAC-to-attack list」を参照してください。
- **Add to Permit List**: 不正APを許可MACアドレスリストに追加します。このアクションの使用方法の詳細については、「許可MACアドレスリストへのComwareベースの不正APの追加」を参照してください。

MAC-to-attackリストへのComwareベースの不正APの追加

不正APのMACアドレスをMAC-to-attackリストに追加すると、Comwareベースの不正APをACで攻撃できます。

MAC-to-attackリストへのComwareベースの不正アクセスポイントの追加

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > WIDS Management > Rogue AP**sを選択します。
3. 不正APをMAC-to-attackリストに追加するには、次のいずれかの方法を使用します。
   a. Operationフィールドの**Operation**アイコン ⋯ をクリックし、ショートカットメニューからAdd to Attack Listをクリックします。
   b. 不正APのMACアドレスリンクをクリックし、ページの右側にあるAction領域でAdd to Attack Listリンクをクリックします。

   Add to Attack Listリンクは、不正なAPがMAC-to-attackリストにない場合にだけ表示されます。
4. OKをクリックします。

MAC-to-attackリストへのComwareベースの不正APのバッチ追加

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > WIDS Management > Rogue APs**を選択します。
3. 1つまたは複数の不正なAPを選択し、Add to Attack Listをクリックします。
4. 確認ダイアログボックスで、OKをクリックします。

   Add to Attack List Resultページが開きます。
   - **MAC Address**: APのMACアドレス。
   - **AC**: APを管理するACのラベル。
   - **Result**: 操作の結果。

MAC-to-attackリストからのComwareベースの不正APの削除

攻撃対象MACリストからComwareベースの不正APを削除すると、ACはそのAPを攻撃しなくなります。

MAC-to-attackリストからのComwareベースの不正APの削除

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > WIDS Management > Rogue APs**を選択します。
3. 次のいずれかの方法を使用して、APを削除するには、次のいずれかの方法を使用します。
   a. Operationフィールドの**Operation**アイコン ⋯ をクリックしてから、Remove from Attack Listリンクをクリックします。
   b. 不正なAPのMACアドレスリンクをクリックし、Remove from Attack Listをクリックします。
   リンクをクリックします。

   Remove from Attack Listリンクは、不正なAPがMAC-to-attackリストにある場合にだけ表示されます。
4. OKをクリックします。

MAC-to-attackリストからのComwareベースの不正APのバッチ削除

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > WIDS Management > Rogue APs**を選択します。
3. 1つまたは複数の不正なAPを選択し、Remove from Attack Listをクリックします。
4. 確認ダイアログボックスで、OKをクリックします。

   Remove from Attack List Resultページが開きます。
   - **MAC Address**: APのMACアドレス。
   - **AC**: APを管理するACのラベル。
   - **Result:** 操作の結果。

許可MACアドレスリストへのComwareベースの不正APの追加

許可MACアドレスリストに追加することで、Comwareベースの不正なAPがワイヤレスネットワークサービスを提供できるようになります。この機能は、Comwareベースの不正なAPだけで使用できます。

許可MACアドレスリストへのComwareベースの不正APの追加

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > WIDS Management > Rogue APs**を選択します。
3. 次のいずれかの方法を使用して、不正なAPを許可MACアドレスリストに追加します。
   - Operationフィールドの**Operation**アイコン ⋯をクリックし、Add to Permit Listをクリックします。

- 不正なAPのMACアドレスリンクをクリックし、ページの右側にある**Action**領域で**Add to Permit List**リンクをクリックします。

4. OKをクリックします。

許可MACアドレスリストへのComwareベースの不正APのバッチ追加

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > WIDS Management > Rogue APs**を選択します。
3. 1つまたは複数の不正なAPを選択し、Add to Permit Listをクリックします。
4. 確認ダイアログボックスで、OKをクリックします。

   Add to Permit List Resultページが開きます。

   - **MAC Address**: APのMACアドレス。
   - **AC**: APを管理するACのラベル。
   - **Result**: 操作の結果。

MAC-to-attackリスト上の不正APは、許可MACアドレスリストに追加できません。許可MACアドレスリストに不正APを追加すると、不正APリストから削除されます。

許可MACアドレスリストからAPを削除する方法の詳細については、「ACの許可MACアドレスリストの保守」を参照してください。

不正なAPの特定

ロケーションビューを使用して、不正なAPを特定します。不正なAPを特定するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > WIDS Management > Rogue APs**を選択します。
3. Operationフィールドの**Operation**アイコン…をクリックします。
4. **Locate**リンクをクリックします。

   トポロジーウィンドウがポップアップ表示され、不正なAPが赤い円で囲まれたロケーションビューが表示されます。

不正なAPは、ディテクタAPがロケーションビューに追加された場合にだけ検出できます。詳細については、「ワイヤレス検索の管理」を参照してください。

不正なクライアントの管理

WSMは、不正なクライアントを管理するための一連の機能を提供します。

不正クライアントリストの表示

検出されたすべての不正クライアントは、不正クライアントリストに追加されます。不正クライアントリストを表示するには、次の手順を実行します。

1. **Service**タブをクリックします。

2. ナビゲーションツリーから、**WLAN Manager > WIDS Management > Rogue Clients**を選択します。Rogue Clientsページが開き、検出されたすべての不正クライアントが表示されます。

   不正クライアント情報には、次のフィールドがあります。

   - **MAC Address**: 不正クライアントのMACアドレス。不正クライアントの詳細情報を表示するには、MAC addressリンクをクリックします。詳細情報のフィールドの説明は、「不正クライアントの詳細情報の表示」を参照してください。
   - **Class**: 不正クライアントの分類。Unclassified、Rogue、External、およびForced Authorizedがあります。
   - **Vendor**: 不正なクライアントのネットワークアダプタのベンダー。
   - **BSSID**: 不正クライアントにワイヤレスネットワークサービスを提供しているデバイスのMACアドレス。
   - **Signal Strength**: クライアントの信号強度。
   - **Associated Type**: クライアントのアソシエーションタイプ。BSSとAd-Hocがあります。
   - **Detected by**: 不正なクライアントを検出したAPが属するAC。ACの詳細情報を表示するには、ACリンクをクリックします。ACの詳細情報のフィールドの説明については、「Managing Comware-based access controllers」を参照してください。
   - **Last Discovered at**: 不正クライアントが最後に検出された時刻。
   - **Operation**: このフィールドには、不正クライアントの運用タスクへのリンクを表示する**Operation**アイコン ▪▪▪ があります。
   - Comwareベースの不正なAPに関連付けられた不正なクライアントの場合、許可MACアドレスリストまたはMAC-to-attackリストに不正なクライアントを追加したり、MAC-to-attackリストから削除したりできます。また、不正なクライアントを特定することもできます。これらの各操作の使用方法の詳細については、これらの各設定機能の詳細情報を参照してください。

注:

Rogue Client Listは、Operationフィールド以外のすべてのフィールドでソートできます。選択したフィールドでリストをソートするには、列ラベルをクリックします。列ラベルを使用すると、各フィールドに固有のソートオプションを切り替えることができます。

不正なクライアントのクエリー

WSMには、基本問合せと拡張問合せが用意されています。基本問合せ基準には、迅速な検索のためのキーパラメーターがいくつか含まれています。拡張問合せには、正確な照合のための様々な問合せ基準が用意されています。

不正なクライアントにクエリーを実行するには

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > WIDS Management > Rogue Clients**を選択します。
3. 基本的なQueryを実行します。
   a. ACのMACアドレスを入力します。WSMは、このフィールドのファジーマッチングをサポートしています。
   b. **Query**アイコン🔍をクリックします。Rogue Client Listには、クエリー基準に一致するすべての不正クライアントが表示されます。
   c. Queryフィールドをクリアして**Query**アイコン🔍をクリックすると、すべての不正クライアントが表示されます。

4. 高度なクエリーを実行します。

   a. Queryフィールドの横にある**Expand**アイコンをクリックしてQuery領域を拡張します。再度クリックするとQuery領域が非表示になります。

   b. ページの問合せ領域で、1つ以上の問合せ条件を入力または選択します。問合せオプションは次のとおりです。

   - **MAC Address**: 不正クライアントのMACアドレスを入力します。ファジーマッチングがサポートされています。たとえば、0を入力すると、MACアドレスに0が含まれるすべての不正クライアントが表示されます。
   - **Last Discovered at**: ドロップダウンリストから、時間範囲を選択します。オプションは、**Last Day**、**Last 3 Days**、**Last 7 Days**、**Last Month**および**Unlimited**です。
   - **Class**: 不正なクライアントが属するクラスを選択します。オプションは、**Unclassified**、**Rogue**、**External**、および**Forced Authorized**です。

     空のフィールドや無制限に設定されたフィールドは、Queryの抽出条件にはなりません。

   c. **Query**をクリックします。

     Rogue Client Listには、クエリー基準に一致するすべての不正クライアントが表示されます。

   d. **Reset**をクリックして、クエリー基準をクリアし、すべての不正クライアントを表示します。

不正なクライアントに関する詳細情報の表示

不正クライアントの詳細情報ページには、不正クライアントに関するすべての情報(不正クライアントの場所および不正クライアントを検出したAPを含む)が表示され、ページの右側にあるAction領域で不正クライアントに対して実行できるすべてのアクションが示されます。

不正クライアントに関する詳細情報を表示するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > WIDS Management > Rogue Clients**を選択します。
3. 詳細情報を表示する不正なクライアントのMACアドレスリンクをクリックします。不正なクライアントの詳細情報ページが開きます。

   ComwareベースのAPに関連付けられた不正クライアントの場合、不正クライアントの詳細の内容は次のとおりです。

   不正クライアントの情報

   - **MAC Address**: 不正クライアントのMACアドレス。
   - **Detected by**: 不正なクライアントを検出したAPが属するAC。ACの詳細情報を表示するには、ACリンクをクリックします。ACの詳細情報のフィールドの説明については、「Managing Comware-based access controllers」を参照してください。
   - **Vendor**:不正なクライアントのネットワークアダプタのベンダー。
   - **BSS MAC**: 不正なクライアントにワイヤレスネットワークサービスを提供しているデバイスのMACアドレス。
   - **First Discovered at** :不正クライアントが最初に検出された時刻。
   - **Last Discovered at**: 不正クライアントが最後に検出された時刻。
   - **Max Signal Strength(dBm)**: 不正クライアントの最大信号強度。
   - **Channel with Max Signal Strength**: 不正クライアントが最大信号強度で最後に検出されたチャネル。
   - **Ad Hoc**: 不正なクライアントがアドホックモードで動作しているかどうかを示します。
   - **Attacked Status**: 値は**Attacked**と**Not Attacked**です。不正なクライアントがACによって攻

撃された場合、値は**Attacked**であり、**Attacked**アイコン  で表されます。攻撃されていない場合、値は**Not Attacked**であり、**Not Attacked**アイコン  で表されます。

検出されたAP情報

- **Detected by**: 不正なクライアントを検出したディテクタAP。ディテクタAPに関する詳細情報を表示するには、ディテクタAPリンクをクリックします。APの詳細情報に関するフィールドの説明については、「Managing Comware-based Access Controllers」を参照してください。
- **First Discovered at**: ディテクタAPが不正クライアントを最初に検出した時刻。
- **Last Discovered at**: 最後にディテクタAPが不正クライアントを検出した時刻。
- **Signal Strength**: ディテクタAPの信号強度。
- チ**Channel**: 不正なクライアントのアクセスワイヤレスネットワークがサービスを提供するチャネル。
- **Attacked Status**: 値は**Attacked**と**Not Attacked**です。不正なクライアントがACによって攻撃された場合、値は**Attacked**であり、**Attacked**アイコン  で表されます。攻撃されていない場合、値はNot Attackedであり、**Not Attacked**アイコン  で表されます。
- **Radio ID**: 不正クライアントを検出した無線。

位置情報

- **Location**: 不正なクライアントが存在するロケーションビュー。ロケーションビューでデバイスを表示するには、ロケーションリンクをクリックします。デバイスリストのフィールドの説明については、「ワイヤレスビューの管理」を参照してください。
- **Open Topology**: 不正なクライアントが存在するトポロジーを開きます。トポロジー上の不正なクライアントの場所を表示するには、**View Topology**アイコンをクリックします。

注:

Locationエリアは、ディテクタAPがロケーションビューに追加された場合にのみ表示されます。ロケーションビューにAPを追加する方法については、「ワイヤレストポロジーの管理」を参照してください。

Action

- **Re fresh**: 不正クライアントおよびディテクタAPの情報をリフレッシュします。
- **Add to Attack List**: 不正クライアントをMAC-to-attackリストに追加します。このアクションの使用方法の詳細については、「不正クライアントのMAC-to-attackリストへの追加」を参照してください。
- **Remove from Attack List**: MAC-to-attackリストから不正クライアントを削除します。このアクションの使用方法の詳細については、MAC-to-attackリストからの不正クライアントの削除」を参照してください。
- **Add to Permit List**: 不正クライアントを許可MACアドレスリストに追加します。このアクションの使用方法の詳細については、「不正クライアントの許可MACアドレスリストへの追加」を参

不正クライアントのMAC-to-attackリストへの追加

不正なクライアントを攻撃するには、不正なクライアントのMACアドレスをMAC-to-attackリストに追加します。

MAC-to-attackリストへの不正クライアントの追加

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > WIDS Management > Rogue Clients**を選択します。
3. 次のいずれかの方法を使用して、不正に追加するには、次のいずれかの方法を使用します。
   - Operationフィールドの**Operation**アイコン ··· をクリックしてから、Add to Attack Listをクリックします。
   - 不正クライアントのMACアドレスリンクをクリックし、ページの右側にあるAction領域の**Add to Attack List**リンクをクリックします。

   Add to Attack Listリンクが表示されるのは、不正クライアントがMAC-to-attackリストにない場合だけです。
4. OKをクリックします。

MAC-to-attackリストへの不正クライアントのバッチ追加

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > WIDS Management > Rogue Clients**を選択します。
3. 1つまたは複数の不正クライアントを選択し、Add to Attack Listをクリックします。
4. 確認ダイアログボックスで、OKをクリックします。

   Add to Attack List Resultページが開きます。
   - **MAC Address**: クライアントのMACアドレス。
   - **AC**: クライアントが関連付けられているACのラベル。
   - **Result**: 操作の結果。

MAC-to-attackリストからの不正クライアントの削除

MAC-to-attackリストから不正なクライアントを削除すると、ACはそのクライアントを攻撃しなくなります。

MAC-to-attackリストからの不正クライアントの削除

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > WIDS Management > Rogue Clients**を選択します。
3. **MAC-to-attack**リストから不正クライアントを削除するには、次のいずれかの方法を使用します。
   - **Operation**フィールドの**Operation**アイコン ··· をクリックしてから、Remove from Attack Listリンクをクリックします。
   - 不正クライアントのMACアドレスリンクをクリックし、ページの右側にあるAction領域で**Remove from Attack List**リンクをクリックします。

   Remove from Attack Listリンクは、不正なクライアントがMAC-to-attackリストにある場合にだけ表示されます。
4. OKをクリックします。

MAC-to-attackリストからの不正クライアントのバッチ削除

1. **Service**タブをクリックします。

2. ナビゲーションツリーで、**WLAN Manager > WIDS Management > Rogue Clients**を選択します。
3. 1つまたは複数の不正クライアントを選択し、Remove from Attack Listをクリックします。確認ダイアログボックスが開きます。
4. 確認ダイアログボックスで、OKをクリックします。
   Remove from Attack List Resultページが開きます。
   - **MAC Address**: クライアントのMACアドレス。
   - **AC**: クライアントが関連付けられているACのラベル。
   - **Result**: 操作の結果。

許可MACアドレスリストへの不正なクライアントの追加

クライアントがワイヤレスネットワークにアクセスできるようにするには、クライアントを許可MACアドレスリストに追加します。

許可MACアドレスリストへの不正なクライアントの追加

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > WIDS Management > Rogue Clients**を選択します。
3. 次のいずれかの方法を使用して、するには、次のいずれかの方法を使用します。
   - **Operation**フィールドの**Operation**アイコン ••• をクリックし、ショートカットメニューからAdd to Permit Listを選択します。
   - 不正なクライアントのMACアドレスリンクをクリックし、ページの右側にあるAction領域で**Add to Permit List**リンクをクリックします。
4. OKをクリックします。

許可MACアドレスリストへの不正クライアントのバッチ追加

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > WIDS Management > Rogue Clients**を選択します。
3. 1つまたは複数の不正クライアントを選択し、Add to Permit Listをクリックします。
4. 確認ダイアログボックスで、OKをクリックします。
   Add to Permit List Resultページが開きます。
   - **MAC Address**: クライアントのMACアドレス。
   - **AC**: クライアントが関連付けられているACのラベル。
   - **Result**: 操作の結果。

MAC-to-attackリスト上の不正クライアントは、許可されたMACアドレスリストに追加できません。許可されたMACアドレスリストに不正クライアントを追加すると、不正クライアントリストから削除されます。

許可MACアドレスリストからAPを削除する方法の詳細については、「ACの許可MACアドレスリストの保守」を参照してください。

不正なクライアントの特定

ロケーションビューで不正なクライアントを検索できます。不正なクライアントを検索するには、次の手順を実行します:

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > WIDS Management > Rogue Clients**を選択します。
3. **Operation**フィールドの**Operation**アイコン ▪▪▪ をクリックし、ショートカットメニューから**Locate**を選択します。

   トポロジーウィンドウがポップアップ表示され、不正なクライアントが赤い円で囲まれたロケーションビューが表示されます。

不正なクライアントを検出できるのは、ディテクタAPがロケーションビューに追加されている場合だけです。詳細については、「ワイヤレスビューの管理」を参照してください。

WLAN IPSの設定

概要

802.11ネットワークは、干渉、攻撃者、不正なクライアント、およびアンビエントワイヤレスデバイスなど、さまざまな脅威の影響を受けます。ワイヤレス侵入防止システム(WIPS)は、ユーザーが定義したセキュリティポリシーに従って、企業ネットワークおよびユーザーを不正なワイヤレスアクセスから保護します。

WIPS対応ネットワークでは、センサーがチャネルを監視して攻撃を検出してアラームを生成し、その情報をACに報告して管理者に通知します。また、センサーは検出された不正デバイスに対して対策を講じることもできます。

注:

このモジュールは、Comwareベースのワイヤレスデバイスのみをサポートします。

用語

- **Virtual security domain**: WLANは、仮想セキュリティドメインと呼ばれる複数のドメインに分割できます。仮想セキュリティドメインには、センサー、APカテゴリ化規則、対策ポリシー、シグニチャポリシー、および攻撃検出ポリシーが含まれます。WIPSは、各仮想セキュリティドメインに異なるセキュリティ検出および保護ポリシーを適用します。
- **Sensor**: センサーは、WIPSが有効なAPです。WLANチャネルを監視し、WLAN情報を収集し、802.11フレームを送信して不正デバイスの関連付けを解除します。センサーは次のモードで動作できます。
- **Monitor mode**ド: センサー上の1つまたは複数の無線がWIPSサービスを提供しますが、アクセスサービスは提供しません。
- **Hybrid mode**: センサー上の1つまたは複数の無線が、WIPSとアクセスサービスの両方を提供します。ハイブリッドモードで動作するセンサーは、次のポリシーを採用します。
  - **Access first**: アクセス時間が長く、WIPS監視時間が短く、パケット損失が少なく、アクセス効率が良好。検出能力が低い。
  - **Scanning first**: WIPS監視時間が長く、アクセス時間が短く、パケット損失が多く、アクセス効率が低い。検出能力が高い。
  - **Balanced**: アクセス優先ポリシーとスキャン優先ポリシーの間で調整されます。
- **Trusted address list**: 信頼できるアドレスリストには、許可されたAPまたはクライアントのMACアドレスが含まれています。ワイヤレスデバイスのMACアドレスは、手動または動的に許可されたデバイスリストに追加できます。動的モードはクライアントに適用できます。WIPSは、クライアントが暗号化された認証方式によって許可されたAPに関連付けられていることを検出すると、そのクライアントを許可されたデバイスリストに追加します。
- **Static-trusted OUI list**ト: スタティックに信頼されたOUIリストには、信頼できる無線デバイスのOUIが含まれています。これは許可されたデバイスリストの補足です。
- **Blocked address list**: ブロックアドレスリストには、禁止されたAPまたはクライアントのMACアドレスが含まれています。WIPSはこのリストを使用してAPとクライアントを分類します。また、WIPSはリスト内のクライアントがWLANにアクセスすることを禁止することもできます。

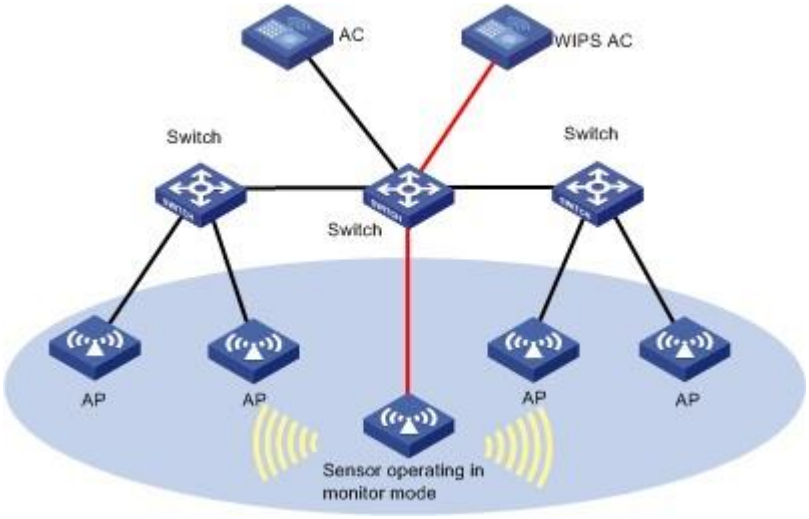
WIPSネットワーキング

WIPSは、独立して動作することも、既存のWLAN内で動作することもできます。

独立したネットワーク

モニターモードで動作するACおよびセンサー(FIT AP)は、図66に示すように、WIPSネットワークを形成します。WIPSネットワークは、保護されるWLANから独立しています。

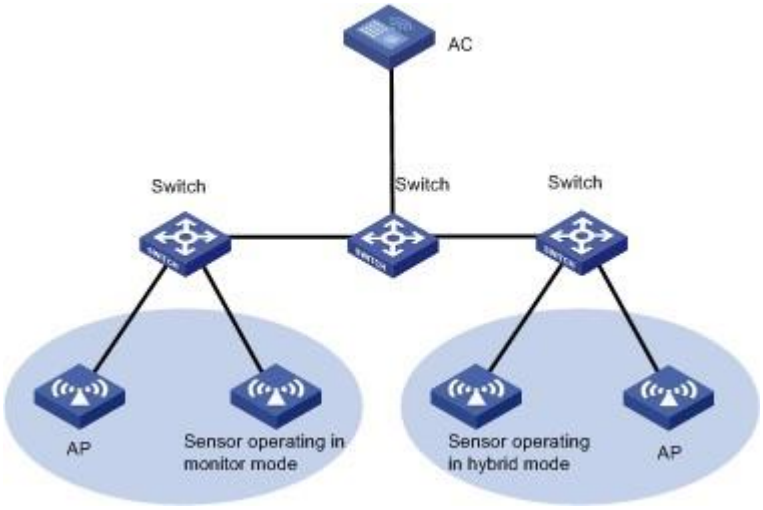
図66 ネットワーク図



既存のWLANでの動作

図67に示すように、WLAN内のACおよびAPでWIPSをAPでWIPSを有効にして、センサーがモニターモードまたはハイブリッドモードで動作するように設定します(図67を参照)。

図67 ネットワーク図



基本的なWIPS設定

WIPS Managementページへのアクセス

WIPS Managementページからは、基本的なWIPS設定にアクセスできます。WIPS Managementページにアクセスするには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > WIPS Configuration**を選択します。

   WIPS Managementページにすべての機能が表示されます。
3. 設定するACを選択します。

   WIPS Managementページには、ACに関する情報が表示されます。

WIPSのイネーブル化

デフォルトでは、WIPSはAC上でディセーブルです。

WIPSをイネーブルにするには、次の手順を実行します。

1. **WIPS Management**ページにアクセスします。
2. ACリストからターゲットACを選択します。
3. **Enable WIPS**を選択します。
4. **OK**をクリックします。

注:

ACでWIDSとWIPSを同時にイネーブルにしたり、WIDSが設定されているComwareベースのACでWIDSをディセーブルにしたりすることはできません。WIDSがすでにイネーブルになっているACでWIPSをイネーブルにするには、最初にすべてのWIDS設定を削除し、すべてのAPテンプレートを通常モードで動作するように設定します。

時間パラメーターの設定

1. **WIPS Management**ページにアクセスします。
2. **Time Parameters**タブをクリックします。
3. ACの次の時間パラメーターを設定します。
   - **Time in seconds for the AP to change to inactive status**: WIPSがAPを非アクティブ状態に切り替えるまでの待機時間を指定します。WIPSは、FIT APが指定された時間内にパケットを送信しないことを検出すると、APの状態をアクティブから非アクティブに切り替えます。有効な時間範囲は60～600秒で、デフォルトは300秒です。
   - **Time in seconds for the client to change to inactive status**: WIPSがクライアントを非アクティブ状態に切り替えるまでの待機時間を指定します。WIPSは、クライアントが指定された時間内にパケットを送信しないことを検出すると、クライアントの状態をアクティブから非アクティブに切り替えます。有効な時間範囲は120～1200秒で、デフォルトは600秒です。
   - **Aging time in seconds for inactive devices**: 非アクティブなワイヤレスデバイスのエージングタイマーを指定します。WIPSは、ワイヤレスデバイスが指定された時間内にパケットを送信しないことを検出すると、そのワイヤレスデバイスを削除します。有効な時間の範囲は60～2592000秒で、デフォルトは86400秒です。
   - **Re-categorization period(s)**: 検出されたAPをWIPSが再分類する時間間隔を指定します。有効な時間範囲は10～36000秒で、デフォルトは600秒です。
   - **Traffic statistics periods(s)**: APが収集したトラフィックデータをACに送信する間隔を指

定します。有効な時間範囲は60～86400秒で、デフォルトは900秒です。

- **Dynamic Trust List Aging Time(s)**: ダイナミック信頼リスト内の無線デバイスのエージングタイムを60～3600秒の範囲で指定します。デフォルトは60秒です。リスト内のデバイスのエージングタイムが経過すると、WIPSはそのデバイスを検出できなくなると、リストからそのデバイスを削除します。このパラメーターは、ダイナミック信頼リストに対してだけ有効です。
- **Device Status Update Interval(s)**: ワイヤレスデバイスの情報更新間隔を設定します。この間隔を設定すると、ワイヤレスデバイスの情報が変化しない場合に、センサーが指定された間隔でワイヤレスデバイスの現在の状態をACに通知し、ACがワイヤレスデバイスの状態を時間内に取得できるようになります。

4. **OK**をクリックします。

許可チャネルリストの設定

WLANで許可チャネルリストを設定できます。WIPSは、許可チャネルリストにないチャネルでのパケット送信を検出すると、アラームを生成します。

許可チャネルリストを設定するには、次の手順を実行します。

1. **WIPS Management**ページにアクセスします。
2. **Permitted Channel List**タブをクリックします。

   許可チャネルリストには、802.11でサポートされているすべてのチャネルが表示されます。異なる国コードをサポートしているため、異なるACを選択すると、一部のチャネルはグレー表示されます。
3. 許可されたチャネルリストに追加するチャネルを選択します。サポートされているすべてのチャネルを許可されたチャネルリストに追加するには、**Select All**を選択します。
4. OKをクリックします。

スタティック信頼アドレスリストの設定

スタティック信頼アドレスリストには、手動で設定されたすべての信頼できるデバイスのMACアドレスが含まれます。

スタティック信頼アドレスリストの表示

1. **WIPS Management**ページにアクセスします。
2. Static Trusted Address Listタブをクリックします。

   スタティック信頼アドレスリストには、手動で設定されたすべての信頼できるMACアドレスが表示されます。

   - **MAC Address**: デバイスのMACアドレス。
   - **Vendor**: デバイスまたはNICのベンダー。IMCはMACアドレスを使用してデバイスまたはNICのベンダーを識別します。MACアドレスがOUI MACアドレスまたは有効なMACアドレスでない場合、フィールドにはUnknownと表示されます。
   - **Delete**: MACアドレスを削除できます。

   スタティックに信頼されたアドレスリストに十分なエントリーが含まれている場合は、次のナビゲーション支援が表示されます。

   - **Next Page**アイコンをクリック)アイコンをクリックして、static-trusted addressリストでページを進めます。
   - **Last Page**アイコンをクリックすると、static-trusted addressリストの最後にページ転送されます。

- **Previous Page**アイコンをクリックすると、static-trusted addressリストのページが逆方向に表示されます。
- **First Page**アイコンをクリックすると、static-trusted addressリストの先頭にページバックします。

静的に信頼されたアドレス一覧の右上にある**8**、**15**、**50**、**100**、または**200**をクリックして、各ページに表示する項目数を指定します。

注:

スタティック信頼アドレスリストは、MAC AddressフィールドとVendorフィールドでソートできます。選択したフィールドでリストをソートするには、列ラベルをクリックします。列ラベルを使用すると、各フィールドに固有のソートオプションを切り替えることができます。

スタティック信頼アドレスリストの同期化

IMCは、スタティック信頼アドレスリストの自動または手動による同期化をサポートしています。デフォルトでは、IMCはスタティック信頼アドレスリストを2時間ごとに自動的に同期化します。

スタティック信頼アドレスリストを手動で同期化するには、次の手順を実行します。

1. **WIPS Management**ページにアクセスします。
2. Static Trusted Address Listタブをクリックします。
3. **Synchronize**をクリックして、スタティック信頼アドレスリストの同期化を開始します。

   同期プロセスが完了すると、ページがリフレッシュされ、最新のデータが表示されます。

スタティックに信頼されたMACアドレスの照会

1. **WIPS Management**ページにアクセスします。
2. Static Trusted Address Listタブをクリックします。
3. **Query**フィールドに、MACアドレスの一部または全体をxx:xx:xx:xx:xx:xx:xx形式で入力します。
4. **Query**アイコン🔍をクリックします。

   スタティック信頼アドレスリストには、一致するすべてのスタティック信頼MACアドレスが表示されます。
5. **Reset**をクリックしてクエリー基準をクリアし、すべてのスタティック信頼できるMACアドレスを表示します。

信頼できるMACアドレスの追加

1. **WIPS Management**ページにアクセスします。
2. Static Trusted Address Listタブをクリックします。
3. **Add**をクリックします。

   Add MAC Addressダイアログボックスが開きます。
4. 追加するMACアドレスをxx:xx:xx:xx:xx:xx:xxの形式で入力します。
5. OKをクリックします。

信頼できるMACアドレスのインポート

WIPSでは、静的信頼アドレスリストへのMACアドレスのバッチインポートがサポートされています.csvファイルのみがサポートされています。ファイルにはMACアドレスのみを含めることができ、行見出しや行見出しは必要ありません。

信頼できるMACアドレスをインポートするには:

1. **WIPS Management**ページにアクセスします。
2. Static Trusted Address Listタブをクリックします。
3. **Import**をクリックします。

   Select Fileページが開きます。
4. **Browse**またはフィールドをクリックしてファイルを選択します。
5. Nextをクリックします。

   Import MAC Address Informationページが開き、次の情報が表示されます。
   - **MAC Address**: デバイスのMACアドレス。
   - **Vendor**: デバイスまたはNICのベンダー。IMCはMACアドレスを使用してデバイスまたはNICのベンダーを識別します。MACアドレスがOUI MACアドレスまたは有効なMACアドレスでない場合、フィールドにはUnknowと表示されます。

   特定のMACアドレスをインポートしない場合は、それらを選択してDeleteをクリックします。
6. OKをクリックします。

   Imported MAC Address Resultページが開き、MACアドレス情報のインポート結果が表示されます。
7. OKをクリックして、Static Trusted Address Listページに戻ります。

スタティック信頼MACアドレスの削除

1. **WIPS Management**ページにアクセスします。
2. Static Trusted Address Listタブをクリックします。
3. 1つのMACアドレスを削除するか、複数のMACアドレスをまとめて削除します。
   - 削除するMACアドレスを選択して、Deleteをクリックします。
   - 削除するMACアドレスの**Delete**アイコンをクリックします。
4. 確認ダイアログボックスで、OKをクリックします。

アラーム無視アドレスリストの設定

アラーム無視アドレスリストには、手動で設定されたすべてのAPまたはクライアントのMACアドレスが含まれています。アラーム無視アドレスリスト内のワイヤレスデバイスの場合、WIPSはそれらを監視するだけで、それらの動作に対するアラームは生成しません。

アラーム無視アドレス一覧を表示する

1. **WIPS Management**ページにアクセスします。
2. アラーム-無視されたアドレス一覧タブをクリックします。

   alarm-ignoredアドレスリストには、アクションWIPSがアラームを生成しないすべてのデバイスのMACアドレスが表示されます。
   - **MAC Address**: デバイスのMACアドレス。
   - **Vendor**: デバイスまたはNICのベンダー。IMCはMACアドレスを使用してデバイスまたはNICのベンダーを識別します。MACアドレスがOUI MACアドレスまたは有効なMACアドレス

でない場合、フィールドにはUnknowと表示されます。

- **Delete**: MACアドレスを削除できます。

アラーム無視アドレスリストに十分なエントリーが含まれている場合は、次のナビゲーション支援が表示されます。

- **Next Page**アイコンをクリックして、**alarm-ignored address**リスト内でページを進めます。
- **Last Page**アイコンをクリックして、**alarm-ignored address**リストの最後にページ移動します。
- **Previous Page**アイコンをクリックして、**alarm-ignored address**リストの前のページに戻ります。
- **First Page**アイコンをクリックすると、**alarm-ignored address**リストの先頭にページ戻ります。

アラーム無視アドレスリストの右上にある**8**、**15**、**50**、**100**、または**200**をクリックして、各ページに表示する項目数を指定します。

注:

アラームが無視されたアドレスリストは、MAC AddressフィールドとVendorフィールドでソートできます。選択したフィールドでリストをソートするには、列ラベルをクリックします。列ラベルを使用すると、各フィールドに固有のソートオプションを切り替えることができます。

アラーム無視アドレス一覧の同期

IMCは、アラーム無視アドレスリストの自動または手動による同期化をサポートしています。デフォルトでは、IMCはアラーム無視アドレスリストを2時間ごとに自動的に同期化します。

アラーム無視アドレスリストを手動で同期するには、次の手順を実行します。

1. **WIPS Management**ページにアクセスします。
2. **Alarm-Ignored Address List**リストタブをクリックします。
3. Synchronizeをクリックして、アラーム無視アドレスリストの同期化を開始します。

   同期プロセスが完了すると、ページがリフレッシュされ、最新のデータが表示されます。

アラーム無視アドレス一覧の問い合わせ

1. **WIPS Management**ページにアクセスします。
2. **Alarm-Ignored Address List**タブをクリックします。
3. MACアドレスの一部または全部をxx:xx:xx:xx:xx:xx:xx形式で入力します。
4. **Query**をクリックします。

Alarm-Ignored Address Listリストには、一致するアラーム無視MACアドレスがすべて表示されます。

5. **Reset**をクリックして、クエリー基準をクリアし、アラームが無視されたすべてのMACアドレスを表示します。

アラームを無視したMACアドレスの追加

1. **WIPS Management**ページにアクセスします。
2. **Alarm-Ignored Address**リストタブをクリックします。
3. **Add**をクリックします。

   Add MAC Addressウィンドウが開きます。

4. 追加するMACアドレスをxx:xx:xx:xx:xx:xx:xxの形式で入力します。
5. OKをクリックします。

アラームが無視されたMACアドレスのインポート

WIPSでは、アラーム無視アドレスリストへのMACアドレスのバッチインポートがサポートされています.csvファイルのみがサポートされています。これらのファイルにはMACアドレスのみを含めることができ、行見出しや行見出しは必要ありません。

アラームが無視されたMACアドレスをインポートするには:

1. **WIPS Management**ページにアクセスします。
2. **Alarm-Ignored Address**リストタブをクリックします。
3. **Import**をクリックします。

   ファイルの選択ページが開きます。
4. **Browse**またはフィールドをクリックしてファイルを選択します。
5. **Next**をクリックします。

   Import MAC Address Informationページが開き、次の情報が表示されます。
   - **MAC Address**: デバイスのMACアドレス。
   - **Vendor**: デバイスまたはNICのベンダー。IMCはMACアドレスを使用してデバイスまたはNICのベンダーを識別します。MACアドレスがOUI MACアドレスまたは有効なMACアドレスでない場合、フィールドにはUnknownと表示されます。

   特定のMACアドレスをインポートしない場合は、それらを選択してDeleteをクリックします。
6. OKをクリックします。

   Imported MAC Address Resultページが開き、MACアドレス情報のインポート結果が表示されます。
7. OKをクリックします。

アラームを無視したMACアドレスの削除

この機能を使用すると、アラーム無視アドレスリストから1つ以上のMACアドレスを削除できます。

アラームが無視されたMACアドレスを削除するには:

1. **WIPS Management**ページにアクセスします。
2. **Alarm-Ignored Address**リストタブをクリックします。
3. 1つのMACアドレスまたは複数のMACアドレスをバッチで削除します。
   - 削除するMACアドレスを選択して、Deleteをクリックします。
   - 削除するMACアドレスの**Delete**アイコンをクリックします。
4. 確認ダイアログボックスで、OKをクリックします。

スタティックブロックアドレスリストの設定

スタティックブロックアドレスリストには、手動で設定されたすべての不正デバイスのMACアドレスが含まれています。

静的ブロックアドレス一覧の表示

1. **WIPS Management**ページにアクセスします。
2. **Static Blocked Address**リストタブをクリックします。

スタティックブロックアドレスリストには、ブロックされたすべてのMACアドレスが表示されます。

静的ブロックアドレス一覧

- **MAC Address**: デバイスのMACアドレス。
- **Vendor**: デバイスまたはNICのベンダー。IMCはMACアドレスを使用してデバイスまたはNICのベンダーを識別します。MACアドレスがOUI MACアドレスまたは有効なMACアドレスでない場合、フィールドにはUnknownと表示されます。
- **Delete**: MACアドレスを削除できます。

スタティックブロックアドレスリストに十分なエントリーが含まれている場合は、次のナビゲーション支援が表示されます。

- **Next Page**アイコンをクリックして、**static-blocked address**リストで次のページに移動します。
- **Last Page**アイコンをクリックして、**static-blocked address**の最後のページに移動します。
- **Previous Page**アイコンをクリックして、**static-blocked address**リストのページを逆方向に表示します。
- **First Page**アイコンをクリックして、**static-blocked address**リストの先頭に戻ります。

静的ブロックアドレス一覧の右上にある8、15、50、100、または200をクリックして、各ページに表示する項目数を指定します。

注:

静的ブロックアドレスリストは、MAC AddressフィールドとVendorフィールドでソートできます。選択したフィールドでリストをソートするには、列ラベルをクリックします。列ラベルを使用すると、各フィールドに固有のソートオプションを切り替えることができます。

静的ブロックアドレス一覧の同期

IMCは、静的ブロックアドレスリストの自動または手動による同期化をサポートしています。デフォルトでは、IMCは静的ブロックアドレスリストを2時間ごとに自動的に同期化します。

スタティックブロックアドレスリストを手動で同期するには、次の手順を実行します。

1. **WIPS Management**ページにアクセスします。
2. **Static Blocked Address**リストタブをクリックします。
3. Synchronizeをクリックして、**Static Blocked Address**リストの同期を開始します。

   同期プロセスが完了すると、ページがリフレッシュされ、最新のデータが表示されます。

静的にブロックされたアドレスの問い合わせ

1. **WIPS Management**ページにアクセスします。
2. **Static Blocked Address**リストタブをクリックします。
3. MACアドレスの一部または全部をxx:xx:xx:xx:xx:xx:xx形式で入力します。
4. **Query**をクリックします。

Static Blocked Addressリストには、一致するすべてのスタティックブロックMACアドレスが表示されます。

5. **Reset**をクリックすると、クエリー基準がクリアされ、すべてのスタティックブロックMACアドレスが表示されます。

スタティックブロックMACアドレスの追加

1. **WIPS Management**ページにアクセスします。
2. **Static Blocked Address**リストタブをクリックします。
3. **Add**をクリックします。

   Add MAC Addressウィンドウが開きます。
4. 追加するMACアドレスをxx:xx:xx:xx:xx:xx:xxの形式で入力します。

スタティックブロックされたMACアドレスのインポート

WIPSは、静的ブロックアドレスリストへのMACアドレスのバッチインポートをサポートしています.csvファイルのみがサポートされています。ファイルにはMACアドレスのみを含めることができ、行見出しや行見出しは必要ありません。

スタティックブロックMACアドレスをインポートするには:

1. **WIPS Management**ページにアクセスします。
2. **Static Blocked Address**タブをクリックします。
3. **Import**をクリックします。

   ファイルの選択ページが開きます。
4. **Browse**をクリックしてファイルを選択するか、インポートするURLまたはファイルを入力します。
5. Nextをクリックします。

   Import MAC Address Informationページが開き、次の情報が表示されます。
   - **MAC Address**: デバイスのMACアドレス。
   - **Vendor**: デバイスまたはNICのベンダー。IMCはMACアドレスを使用してデバイスまたはNICのベンダーを識別します。MACアドレスがOUI MACアドレスまたは有効なMACアドレスでない場合、フィールドにはUnknownと表示されます。

   特定のMACアドレスをインポートしない場合は、それらを選択してDeleteをクリックします。
6. OKをクリックします。

   Imported MAC Address Resultページが開き、MACアドレス情報のインポート結果が表示されます。
7. OKをクリックします。

スタティックブロックされたMACアドレスの削除

この機能を使用すると、静的ブロックアドレスリストから1つ以上のデバイスを削除できます。静的ブロックMACアドレスを削除するには、次の手順を実行します。

1. **WIPS Management**ページにアクセスします。
2. 静的ブロックアドレス一覧タブをクリックします。
3. 1つのMACアドレスを削除するか、複数のMACアドレスをまとめて削除します。
   - 削除するMACアドレスを選択して、Deleteをクリックします。
   - 削除するMACアドレスの**Delete**アイコンをクリックします。
4. 確認ダイアログボックスで、OKをクリックします。

ブロックされたクライアントのWLANへのアクセスを許可する

デフォルトでは、WIPSは、静的ブロックアドレスリスト内のクライアントがWLANにアクセスすることを禁止します。ブロックされたクライアントがWLANにアクセスすることを許可するようにWIPSを設定できま

す。

ブロックされたクライアントがWLANにアクセスできるようにするには、次の手順を実行します

1. **WIPS Management**ページにアクセスします。
2. **Static Blocked Address**リストタブをクリックします。
3. ブロックされたデバイスの許可を選択します。
4. OKをクリックします。

静的対策アドレスリストの設定

スタティックな対策アドレスリストには、手動で設定されたすべての不正デバイスのMACアドレスが含まれています。WIPSは、次の方法を使用して、リスト内の不正デバイスに対して対策を実行します。

- 不正なクライアントを防止するための許可されたAPの制御。
- センサーが802.11フレームを送信して不正なために、センサーがフレームを送信できるようにします。

静的対策アドレス一覧の表示

1. **WIPS Management**ページにアクセスします。
2. Static Countermeasures Address Listタブをクリックします。

   静的対策アドレスリストには、対策が実行されるすべてのデバイスのMACアドレスが表示されます。
   - **MAC Address**: デバイスのMACアドレス。
   - **Vendor**: デバイスまたはNICのベンダー。IMCはMACアドレスを使用してデバイスまたはNICのベンダーを識別します。MACアドレスがOUI MACアドレスまたは有効なMACアドレスでない場合、フィールドにはUnknownと表示されます。
   - **Delete**: MACアドレスを削除できます。

静的対策アドレスリストに十分なエントリーが含まれている場合は、次のナビゲーション支援が表示されます。

- **Next Page**アイコンをクリックして、**static countermeasures address**リスト内でページを進めます。
- **Last Page**アイコンをクリックして、**static countermeasures address**リストの最後にページ転送します。
- **Previous Page**アイコンをクリックして、**static countermeasures address**リストのページを逆方向に移動します。
- **First Page**アイコンをクリックして、**static countermeasures address**リストの先頭にページを戻します。

静的対策アドレスリストの右上にある8、15、50、100、または200をクリックして、各ページに表示する項目数を指定します。

注:

static countermeasures addressリストは、MAC AddressフィールドとVendorフィールドでソートできます。列ラベルをクリックすると、選択したフィールドでリストがソートされます。列ラベルを使用すると、各フィールドに固有のソートオプションを切り替えることができます。

静的対策アドレス一覧の同期

IMCは、静的対抗措置アドレスリストの自動または手動による同期化をサポートしています。デフォルトでは、IMCは静的対抗措置アドレスリストを2時間ごとに自動的に同期化します。

静的対抗措置のアドレスリストを手動で同期化するには:

1. **WIPS Management**ページにアクセスします。
2. Static Countermeasures Address Listタブをクリックします。
3. **Synchronize**をクリックして、静的対抗措置アドレスリストの同期化を開始します。
   同期プロセスが完了すると、ページがリフレッシュされ、最新のデータが表示されます。

静的対策MACアドレスの照会

1. **WIPS Management**ページにアクセスします。
2. Static Countermeasures Address Listタブをクリックします。
3. MACアドレスの一部または全部をxx:xx:xx:xx:xx:xx:xx形式で入力します。
4. **Query**をクリックします。
   静的対策アドレスリストには、一致するすべてのMACアドレスが表示されます。
5. **Reset**をクリックして、クエリー基準をクリアし、すべてのスタティックな対策MACアドレスを表示します。

静的対策MACアドレスの追加

1. **WIPS Management**ページにアクセスします。
2. Static Countermeasures Address Listタブをクリックします。
3. **Add**をクリックします。
   Add MAC Addressウィンドウが開きます。
4. 追加するMACアドレスをxx:xx:xx:xx:xx:xx:xxの形式で入力します。
5. OKをクリックします。

静的対策MACアドレスのインポート

WIPSでは、静的対策アドレスリストへのMACアドレスのバッチインポートがサポートされています.csvファイルのみがサポートされています。ファイルにはMACアドレスのみを含めることができ、行見出しや行見出しは必要ありません。

静的対策のMACアドレスをインポートするには:

1. **WIPS Management**ページにアクセスします。
2. Static Countermeasures Address Listタブをクリックします。
3. **Import**をクリックします。
   Select Fileページが開きます。
4. **Browse**をクリックしてファイルを選択するか、インポートするURLまたはファイルを入力します。
5. **Next**をクリックします。
   Import MAC Address Informationページが開き、次の情報が表示されます。
   - **MAC Address**: デバイスのMACアドレス。
   - **Vendor**: デバイスまたはNICのベンダー。IMCはMACアドレスを使用してデバイスまたはNICのベンダーを識別します。MACアドレスがOUI MACアドレスまたは有効なMACアドレスでない場合、フィールドにはUnknownと表示されます。

   特定のMACアドレスをインポートしない場合は、それらを選択して**Delete**をクリックします。

6. OKをクリックします。

   Imported MAC Address Resultページが開き、MACアドレス情報のインポート結果が表示されます。

7. OKをクリックします。

静的対策MACアドレスの削除

1. **WIPS Management**ページにアクセスします。
2. Static Countermeasures Address Listタブをクリックします。
3. 1つのMACアドレスまたは複数のMACアドレスをバッチで削除します。
   - 削除するMACアドレスを選択して、Deleteをクリックします。
   - 削除するMACアドレスの**Delete**アイコンをクリックします。
4. 確認ダイアログボックスで、OKをクリックします。

静的に信頼されたOUIリストの構成

static-trusted OUIリスト内のすべてのMACアドレスは、信頼できるMACアドレスと見なされます。

静的に信頼されたOUIリストの表示

1. **WIPS Management**ページにアクセスします。
2. Static Trusted OUIリストタブをクリックします。

   static-trusted OUIリストには、すべての信頼できるOUIが表示されます。
   - OUI-xx:xx:xx形式のOUI。
   - **Vendor**: OUIが属するベンダー。
   - **Delete**: OUIを削除できます。

static-trusted OUIリストに十分なエントリーが含まれている場合は、次のナビゲーション支援が表示されます。

- **Next Page**アイコンをクリックして、static-trusted OUIリストでページを進めます。
- **Last Page**アイコンをクリックすると、static-trusted OUリストの最後にページ転送されます。
- **Previous Page**アイコンをクリックして、static-trusted OUIリストで前のページに戻ります。
- **First Page**アイコンをクリックして、static-trusted OUIリストの先頭に戻ります。

static-trusted OUIリストの右上にある8、15、50、100または200をクリックして、各ページに表示するアイテム数を指定します。

注:

static-trusted OUI Iリストは、**OUI**フィールドと**Vendor**フィールドでソートできます。列ラベルをクリックすると、選択したフィールドでリストラベルをクリックします。列ラベルを使用すると、各フィールドに固有のソートオプションを切り替えることができます。

静的に信頼されたOUIリストの同期化

IMCは、静的に信頼されたOUIリストの自動または手動による同期化をサポートしています。デフォルトでは、IMCは静的に信頼されたOUIリストを2時間ごとに自動的に同期化します。

静的に信頼されたOUIリストを手動で同期化するには、次のようにし

1. **WIPS Management**ページにアクセスします。
2. Static Trusted OUI Listタブをクリックします。
3. Synchronizeクリックして、静的に信頼されたOUIリストの同期化を開始します
   同期プロセスが完了すると、ページがリフレッシュされ、最新のデータが表示されます。

OUIのクエリー

1. **WIPS Management**ページにアクセスします。
2. Static Trusted OUI Listタブをクリックします。
3. 右上隅の問合せフィールドに、OUIの一部または全部をxx:xx:xx形式で入力します。
4. **Query**アイコンをクリックします。OUIリストに、問合せ基準に一致するすべてのOUIが表示されます。
5. Queryフィールドをクリアし、**Query**アイコンをクリックしてすべてのOUIを表示します。

OUIの追加

静的に信頼されたOUIリストにOUIを1つずつ追加するか、WSMからOUIを選択できます。

OUIを手動で追加するには、次のようにします。

1. **WIPS Management**ページにアクセスします。
2. Static Trusted OUIリストタブをクリックします。
3. **Add**をクリックします。Add an OUIダイアログボックスが開きます
4. 完全なOUIをxx:xx:xx形式で入力します。
5. OKをクリックします。

WSMからOUIを選択するには:

1. **WIPS Management**ページにアクセスします。
2. Static Trusted OUI リストタブをクリックします。
3. **Select**をクリックします。OUIを選択するためのダイアログボックスが開きます。
4. OUIの**Query**:
   a. **Query**領域で問合せ基準を設定します。
      - **OUI**: OUIの一部または全部をxx:xx:xx形式で入力します。
      - **Vendor Name**: ベンダー名の一部または全部を入力します。
   b. **Query**アイコンをクリックします。OUIリストに、問合せ基準に一致するすべてのOUIが表示されます。
   c. Queryフィールドをクリアし、**Query**アイコンをクリックしてすべてのOUIを表示します。
   d. **Reset**をクリックして、クエリー基準をクリアし、すべてのOUIを表示します。
5. OUIリストから1つ以上のOUIを選択します。
6. OKをクリックします。

OUIの削除

スタティックに信頼されたOUIリストからOUIを削除すると、再分類時間に達した後に、WIPSによって関連デバイスが再分類されます。

OUIを削除するには:

1. **WIPS Management**ページにアクセスします。
2. Static Trusted OUIリストタブをクリックします。
3. ターゲットOUIの**Delete**アイコンをクリックして1つのOUIを削除するか、複数のOUIを選択してDeleteをクリックしてバッチで削除します。
4. 確認ダイアログボックスで、OKをクリックします。

関数セットの設定

1. **WIPS Management**ページにアクセスします。
2. **Function Set**タブをクリックします。
3. 必要に応じて**Function Set**を設定します。
   - **Enable ADOS**: ADOSはWIPSが攻撃されないようにします。この機能がイネーブルになっている場合、WIPSは自身に対する攻撃を検出し、パケットレート制限やフィルタリングなどの対策を実行します。
   - **Enable WIPS for a hybrid sensor that provides access services**: この機能を使用すると、WIPS検出および攻撃防止のパフォーマンスは向上しますが、センサーのアクセスパフォーマンスは低下します。
   - **Function set supported by the attack detection policy**: オプションには、**Ad Hoc Network**、**Spoofing AP**、**Spoofing Client**、**AP Flood Attack**、**EAPOL-Start DoS Attack**、**Authentication DoS Attack**、**Association DoS Attack**、**Reassociation DoS Attack**、**Weak IV**、および**Invalid OUI**があります。
   - **Function set supported by the countermeasures policy**: オプションには、**Misconfigured AP**、**Rogue AP**、**Unauthorized Client**、**External AP**、**Misassociated Client**、**Potential-rogue AP**、**Potential-external AP**、**Uncategorized AP**、**Uncategorized Client**、および**Potential-authorized AP**があります。
4. OKをクリックします。

注:

アタック検出ポリシーでサポートされる関数セットを設定した後は、アタック検出ポリシーを設定するときに、設定された関数セットだけを選択できます。この規則は、対策ポリシーでサポートされる関数セットにも適用されます。

センサーの設定

センサーリストの表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Sensor Management**を選択します。

   センサーリストにはすべてのセンサーが表示されます。
   - **Status**:センサーのオンラインステータス(**Online**および**Offline**)。
   - **AP Label**: センサーのラベル。センサーのラベルをクリックすると、その詳細が表示されます。
   - Radio 1:無線の管理ステータスおよび検出モード。**Down**アイコンは無線がダウン管理ステータスであることを示し、**Up**アイコンは無線がアップ管理ステータスであることを示します。

     次の検出モードを使用できます。

- **Access First**: アクセスサービスを優先します。アクセス時間はWIPS時間よりも長くなります。
- **Detection First**: WIPSを優先します。WIPSの期間がアクセス期間よりも長くなっています。
- **Hybrid Mode**: アクセス優先と検出優先の動作モードの間で調整されます。
- **Detection Only**: WIPSサービスを提供します。アクセスサービスは提供しません。無線の

動作モードを変更するには、**Modify**アイコンをクリックします。

無線でWIPSがイネーブルになっていない場合、またはセンサーにRadio 1がない場合、フィールドには2つの連続したハイフン(--)が表示されます。

- **Radio 2**: 無線でWIPSがイネーブルになっていない場合、またはセンサーにRadio 2がない場合、フィールドには2つの連続したハイフン(--)が表示されます。

  Radio 2の管理状態および検出モードの説明は、Radio 1と同じです。
- **Radio 3**: 無線でWIPSがイネーブルになっていない場合、またはセンサーにRadio 3がない場合、フィールドには2つの連続したハイフン(--)が表示されます。

  Radio 3の管理状態および検出モードの説明は、Radio 1と同じです。
- **Virtual Security Domain**: センサーがバインドされている仮想セキュリティドメインの名前。
- **AC**: センサーが関連付けられているACのラベル。ACのラベルをクリックすると、その詳細が表示されます。
- **Operation**: センサーの**Operation**アイコン ･･･をクリックすると、**Operation**メニューが表示されます。

メニューリストに表示される操作タスクには、センサーおよびセンサーがバインドされている仮想セキュリティドメインの削除が含まれます。

センサーリストに十分なエントリーが含まれている場合は、次のナビゲーション支援が表示されます。

- **Next Page**アイコンをクリックして、**sensor**リストでページを進めます。
- **Last Page**アイコンをクリックして、**sensor**リストの最後のページに進めます。
- **Previous Page**アイコンをクリックして、**sensor**リストの前のページに戻ります。
- **First Page**アイコンをクリックして、**sensor**リストの先頭に戻ります。

センサーリストの右上にある**8**、**15**、**50**、**100**、または**200**をクリックして、各ページに表示する項目数を指定します。

注:

Operationフィールド以外のすべてのフィールドでセンサーリストをソートできます。選択したフィールドでリストをソートするには、列ラベルをクリックします。列ラベルを使用すると、各フィールドに固有のソートオプションを切り替えることができます。

センサーリストの同期

IMCは、センサーリストの自動または手動での同期化をサポートしています。デフォルトでは、IMCはセンサーリストを2時間ごとに自動的に同期化します。

センサーリストを手動で同期するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Sensor Management**を

選択します。

センサーリストにはすべてのセンサーが表示されます。

3. **Synchronize**をクリックして、センサーリストの同期化を開始します。

同期プロセスが完了すると、ページがリフレッシュされ、最新のデータが表示されます。

センサーの照会

WSMには、基本問合せと拡張問合せが用意されています。基本問合せ基準には、迅速な検索のためのキーパラメーターがいくつか含まれています。拡張問合せには、正確な照合のための様々な問合せ基準が用意されています。

センサーを照会するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Sensor Management**を選択します。

   センサーリストにはすべてのセンサーが表示されます。
3. 基本的な**Query**を実行します。
   a. 仮想セキュリティドメインの名前を入力します。WSMは、このフィールドのファジーマッチングをサポートしています。
   b. **Query**アイコンをクリックします。センサーリストには、問合せ基準に一致するすべてのセンサーが表示されます。
4. Queryボックスをクリアし、**Query**アイコンをクリックしてすべてのセンサーを表示します。
5. 高度なクエリーを実行します。
   a. Queryフィールドの横にある**Expand**アイコンをクリックしてQuery領域を拡張します。再度クリックするとQuery領域が非表示になります。
   b. 次の問合せ基準を1つ以上入力または選択します。
      - **AP Label**: APラベルの一部または全部を入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
      - **Virtual Security Domain**: 仮想セキュリティドメイン名の一部または全体を入力して、ドメインにバインドされているすべてのセンサーを表示します。WSMは、このフィールドのファジーマッチングをサポートします。
      - **Status**: センサーのオンラインステータスを選択します。オプションはAll、OnlineおよびOfflineです。
      - **Detection Mode**: 無線の検出モードを選択します。オプションは、All、Access First、Detection First、Hybrid Mode、およびDetection Onlyです。
      - **AC**: センサーがアソシエートするACを選択します。
   c. **Query**をクリックします。

      センサーリストには、一致するすべてのセンサーが表示されます。
   d. **Reset**をクリックしてクエリー基準をクリアし、すべてのセンサーを表示します。

センサーの追加

この関数を使用すると、センサーを追加し、無線の検出モードを指定できます。センサーを追加するには、次の手順を実行します。

1. **Service**タブをクリックします。

2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Sensor Management**を選択します。

   センサーリストにはすべてのセンサーが表示されます。

3. **Add**をクリックします。

   Add Sensorページが開きます。

4. Detection Modeリストから無線の検出モードを選択します。オプションは、Access First、Detection First、Hybrid Mode、およびDetection Onlyです。

   検出モードの詳細については、「センサーリストの表示」を参照してください。

5. 無線リストの下にあるSelectをクリックし、次の手順に従ってAdd Sensorページから無線を選択します。

   a. QueryフィールドにAPラベルの一部または全部を入力し、**query**アイコンをクリックします。または

      次の問合せ基準を1つ以上選択または入力します。

      - **Radio ID**: 無線IDを選択します。オプションはAll、Radio 1、Radio 2、Radio 3です。
      - **Radio Type**: 無線タイプを選択します。オプションはAll、802.11a、802.11b、802.11g、802.11gn、および802.11 anです。
      - **AP Label**: 無線が属するAPのラベルを入力します。WSMは、このフィールドのファジーマッチングをサポートしています。
      - **AC**: ACを選択します。

   b. **Query**をクリックします。

      Radio Listには、一致するすべての無線が表示されます。

   c. 1つまたは複数の無線を選択します。

   d. OKをクリックして、Add Sensorページに戻ります。

6. OKをクリックします。

仮想セキュリティドメインへのセンサーのバインド

デフォルトでは、センサーはDefaultという名前の仮想セキュリティドメインにバインドされます。センサーは別の仮想セキュリティドメインにバインドできます。1つのセンサーをバインドできる仮想セキュリティドメインは1つのみです。

センサーを仮想セキュリティドメインにバインドするには、以下の手順に従ってください。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Sensor Management**を選択します。

   Sensor Listにすべてのセンサーが表示されます。

3. 複数のセンサーを仮想セキュリティドメインにバインドするか、またはセンサーを仮想セキュリティドメインにバインドします。

   - 仮想セキュリティドメインにバインドするセンサーを選択し、Bindをクリックします。

     Bind to Virtual Security Domainウィンドウが開きます。

   - 仮想セキュリティドメインにバインドするセンサーの**Operation**アイコンをクリックします。

     Bind to Virtual Security Domainウィンドウが開きます。

4. 仮想セキュリティドメインリストから仮想セキュリティドメインを選択します。

   仮想セキュリティドメインリストの内容:

- **Name**: 仮想セキュリティドメインの名前。
- **AP Categorization Rule**: 仮想セキュリティドメインに追加されたAPカテゴリ化規則の名前。

5. OKをクリックします。

センサーの削除

センサーを削除すると、センサー上のすべての無線のWIPSがディセーブルになります。センサーを削除するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Sensor Management**を選択します。

   センサーリストにはすべてのセンサーが表示されます。
3. 1つまたは複数のセンサーをバッチで削除します。
   - 削除するセンサーを選択して、Deleteをクリックします。
   - 削除するセンサーの**Operation**アイコン ··· をクリックし、ショートカットメニューから削除を選択します。
4. 確認ダイアログボックスで、OKをクリックします。

仮想セキュリティドメインの管理

APカテゴリ化規則の設定

WIPSは、検出されたAPを分類するか、APを分類するか、または検出されたAPの脅威レベルを指定します。検出されたすべてのAPのタイプまたは脅威レベルは、APs Detectedページで確認できます。

WIPSは、AP分類規則を使用して、検出されたAPを次のタイプに分類します。

- **Authorized AP**: WLANで許可されたAP。
- **External AP**: 隣接するワイヤレスネットワーク内のAP。たとえば、近くのカフェのWLAN内のAP。
- **Misconfigured AP**: ワイヤレスネットワークで使用できるが、設定が間違っているAPAPの設定ミス。たとえば、許可されたデバイスリスト内のAPで、SSIDが間違っている。
- **Rogue AP**: 無線ネットワークで使用できないAP。
- **None**: カテゴリを判別できないAP。

APカテゴリ化規則には、次のサブ規則を1つ以上含めることができます。

- **SSID**: SSIDを照合します。
- **Data Security**: APで使用されるセキュリティ方式を照合します。
- **Authentication method**: APで使用される認証方式を照合します。
- **RSSI**: APのRSSIを照合します。
- **Running time of the AP**: APの実行時間と一致します。
- **Number of associated clients**: APのアソシエートされたクライアントの数と一致します。
- **Number of APs detected by the sensor**: センサーによって検出されたAPの数と一致します。
- **Vendor**: APのOUIまたはベンダー名を照合します。

APの脅威レベルは、許可されたAP、不正なAP、外部AP、または認識されていないAPのWLANへの影響を示します。脅威レベルが高いほど、WLANへの影響が深刻であることを示します。APのカテゴリ化

ルールに一致するAPの脅威レベルは、0～100の範囲で指定できます。

複数のAPカテゴリ化規則が存在する場合は、優先順位を指定できます。WIPSは、優先順位の順に規則を照合します。一致するものが見つかると、WIPSは次の基準に従ってアクションを実行します。

- 規則でAPタイプを設定した場合、WIPSは検出されたAPをそのAPタイプに割り当て、検出されたAPを次のAP分類規則と照合しません。
- 規則でAPタイプを設定していない場合、WIPSは検出されたAPに脅威レベルを割り当て、検出されたAPを次のAPカテゴリ化規則と照合します。

APカテゴリ化規則リストの表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Virtual Security Domain**を選択します。
3. **AP Categorization Rule**タブをクリックします。

   AP分類規則リストには、すべてのAP分類規則が表示されます。

   APカテゴリ化規則リストの内容

   - **Name**: APカテゴリ化ルールの名前。APカテゴリ化ルールの名前をクリックすると、その詳細が表示されます。
   - **Category**: AP分類ルールに一致するAPのタイプ。
   - **Threat Level**: AP分類ルールに一致するAPの脅威レベル。WIPSは、Categoryフィールドに Noneと表示されている場合にだけ、検出されたAPに脅威レベルを割り当てます。
   - **AC**: APカテゴリ化ルールが設定されているACのラベル。ACのラベルをクリックすると、その詳細が表示されます。
   - **Operation**: AP分類ルールの**Operation**アイコン をクリックして、**Operation**メニューを表示します。

   メニューに表示される操作タスクには、APカテゴリ化規則の変更、およびAPカテゴリ化規則がバインドされている仮想セキュリティドメインの表示が含まれます。

APカテゴリ化規則リストに十分なエントリーが含まれている場合は、次のナビゲーション支援が表示されます。

- **Next Page**アイコンをクリックして、**AP Categorization Rule**リスト内でページを進めます。
- **Last Page**アイコンをクリックして、**AP Categorization Rule**リストの最後にページ送りします。
- **Previous Page**アイコンをクリックすると、**AP Categorization Rule**リストのページが逆方向に表示されます。
- **First Page**アイコンをクリックすると、**AP Categorization Rule**リストの先頭にページバックします。

APカテゴリ化規則リストの右上にある**8**、**15**、**50**、**100**、または**200**をクリックして、各ページに表示する項目数を指定します。

注:

APカテゴリ化規則リストは、Operationフィールド以外のすべてのフィールドでソートできます。列ラベルをクリックすると、選択したフィールドでリストがソートされます。列ラベルを使用すると、各フィールドに固有のソートオプションを切り替えることができます。

AP分類ルールリストの同期化

IMCは、APカテゴリ化ルールリストの自動または手動による同期化をサポートしています。デフォルトでは、IMCはAPカテゴリ化ルールリストを2時間ごとに自動的に同期化します。

APカテゴリ化規則リストを手動で同期するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Virtual Security Domain**を選択します。
3. AP Categorization Ruleタブをクリックします。

   AP分類規則リストには、すべてのAP分類規則が表示されます。
4. **Synchronize**をクリックして、APカテゴリ化ルールリストの同期化を開始します。

   同期プロセスが完了すると、ページがリフレッシュされ、最新のデータが表示されます。

AP分類ルールの照会

基本問合せを実行する手順は、次のとおりです。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Virtual Security Domain**を選択します。
3. **AP Categorization Rule**タブをクリックします。

   AP分類規則リストには、すべてのAP分類規則が表示されます。
4. 右上隅のQueryフィールドに、APカテゴリ化規則の名前の一部または全体を入力します。
5. **Query**アイコンをクリックします。AP分類リストに、クエリー基準と一致するすべてのAP分類ルールが表示されます。
6. Queryフィールドをクリアして**Query**アイコンをクリックすると、すべてのAPカテゴリ化ルールが表示されます。

高度なクエリーを実行するには、次の手順を実行します。

1. Serviceタブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>WIPS Management>Virtual Security Domain**を選択します。
3. AP Categorization Ruleタブをクリックします。

   AP分類規則リストには、すべてのAP分類規則が表示されます。
4. Queryフィールドの右にある展開アイコンをクリックします。
5. 次の問合せ基準を1つ以上入力または選択します。
   - **Name**: APカテゴリ化ルールの名前を入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
   - **AC**: AP分類ルールが設定されているACを選択します。
6. **Query**をクリックします。

   AP分類規則リストには、一致するすべてのAP分類規則が表示されます。
7. クエリー基準をクリアしてすべてのAPカテゴリ化規則を表示するには、**Reset**をクリックします。

APカテゴリ化規則の追加

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Virtual Security Domain**を選択します。
3. AP Categorization Ruleタブをクリックします。

AP分類規則リストには、すべてのAP分類規則が表示されます。

4. **Add**をクリックします。

   Add AP Categorization Ruleページが開きます。

5. APカテゴリ化規則の次の基本パラメーターを設定します。
   - **Name**: AP分類ルールの名前を1～32文字の文字列で入力します。有効な文字は、整数、文字、およびアンダースコア(_)です。
   - **AC**: AP分類ルールを作成するACを選択します。
   - **Category**: A P分類ルールに一致するAPのタイプを選択します。オプションは次のとおりです。None、Authorized、External、Misconfigured、およびRogueです。
   - **Threat Level**: 脅威レベルを入力します。有効値の範囲は1～100です。Categoryフィールドでを選択すると、WIPSによって、検出されたAPに脅威レベルが割り当てられます。
   - **Sub-Rule Match Criteria**: サブルールの一致基準を選択します。
   - **AND**: すべてのサブルールに一致するAPは、APカテゴリ化ルールに一致します。
   - **OR**: サブルールの1つに一致するAPがAPカテゴリ化ルールに一致します。
   - **Sub rules**: 有効にするサブルールを選択します。選択したサブルールのパラメーターが表示されます。サブルールには、認証方法、データセキュリティ、SSID、RSSI、操作時間、クライアント数、検出AP数およびデバイスベンダーが含まれます。
6. Authentication Methodリストから、APと照合する認証方式を選択します。
   a. **Match Criteria**を選択します。オプションは**Include**です。
   b. 認証方式を選択します。オプションは**None**、**PSK**、**802.1X**、および**Others**です。
7. APを照合するセキュリティ方式を設定します。
   a. **Match Criteria**を選択します。オプションは**Include**および**Equal to**です。
      - **Include**: 指定したセキュリティメソッドを含むセキュリティメソッドを照合します。
      - **Equal to**: 指定したセキュリティメソッドと同じセキュリティメソッドを照合します。
   b. セキュリティ方式を選択します。オプションは、Clear、WEP、WPA、およびWPA2です。
8. APと一致するようにSSIDを設定します。
   a. **Match Criteria**を選択します。オプションは、**Include**, **Exclude**, **Equal to**, 及び **Not Equal to** です。
      - **Include**: 指定されたSSID文字列を含むSSIDを照合します。
      - **Exclude**: 指定したSSID文字列を含まないSSIDを照合します。
      - **Equal to**: 指定したSSID文字列と同じSSIDを照合します。
      - **Not Equal to**: 指定したSSID文字列と異なるSSIDを照合します。
   b. SSID文字列を入力します。
   c. Case SensitiveリストからYesまたはNoを選択します。
9. APと一致するようにRSSIを設定します。
   a. **Match Criteria**を選択します。オプションは、**Greater than**、**Smaller than**および**Between**です。
   b. **Start Value**: RSSIを0～89の範囲で入力します。
   c. **End Value**: RSSIを入力します。開始値よりも大きい値を指定する必要があります。有効な値の範囲は1～90です。一致基準がBetweenに指定されている場合、このフィールドは必須です。
10. APと一致するように動作時間を設定します。

a. **Match Criteria**を選択します。オプションは、**Greater than**、**Smaller than**および**Between**です。
   - **Greater than**: 指定した実行時間以上の値に一致します。
   - **Smaller than**: 指定した実行時間よりも小さい値に一致します。
   - **Between**: 指定した継続時間範囲内の値を照合します。

b. Start Valueに0～2591999秒の範囲で値を入力します。

c. **End Value**を入力します。開始値より大きい値を入力する必要があります。有効な値の範囲は1から2592000秒です。このフィールドは、一致基準が**Between**に指定されている場合は必須です。

11. APと一致するアソシエートされたクライアントの数を設定します。
    a. **Match Criteria**を選択します。オプションは、**Greater than**, **Smaller than**, および**Between**です。
       - **Greater than**: 指定した値以上の値に一致します。
       - **Smaller than**: 指定した値より小さい値に一致します。
       - **Between**: 指定した値の範囲内の値を照合します。

    b. **Start Value**を入力します。関連付けられたクライアントの数。範囲は0～127です。

    c. **End Value**を入力します。関連付けられたクライアントの数で、開始値より大きい値である必要があります。有効な値の範囲は1から128です。このフィールドは、一致基準が「範囲」に指定されている場合は必須です。

12. 検出されたAPの数をAPと一致するように設定します。
    a. **Match Criteria**を選択します。オプションは、**Greater than**, **Smaller than**, および**Between**です。
       - **Greater than**: 指定した値以上の値に一致します。
       - **Smaller than**: 指定した値より小さい値に一致します。
       - **Between**: 指定した値の範囲内の値を照合します。

    b. **Start Value**を入力します。検出されたAPの数。範囲は0～127です。

    c. **End Value**を入力します。検出されたAPの数。開始値より大きい値を指定する必要があります。有効な値の範囲は1から128です。このフィールドは、一致基準が**Between**に指定されている場合は必須です。

13. デバイスベンダーを設定します。WIPSは、APのベンダーまたはAPのMACアドレスが属するOUIを照合します。
    a. **Device Vendor**を選択します。

    b. リストから**OUI** 又は **Vendor Name**を選択します。

    c. xx:xx:xx形式でOUIを入力するか、ベンダー名を入力します。ベンダー名に使用できる文字については、ページのベンダー名に関するヒントを参照してください。

14. OKをクリックします。

APカテゴリ化規則の変更

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Virtual Security Domain**を選択します。
3. **AP Categorization Rule**タブをクリックします。

   AP分類規則リストには、すべてのAP分類規則が表示されます。
4. 変更するAPカテゴリ化規則の**Operation**アイコン ... をクリックしてショートカットメニューから

Modifyを選択します。

APカテゴリ化規則を変更するためのページが開きます。

5. APカテゴリ化規則のパラメーターを変更します。

   APカテゴリ化規則とACの名前は変更できません。他のパラメーターの設定の詳細については、「APカテゴリ化規則の追加」を参照してください。

6. OKをクリックします。

APカテゴリ化ルールの削除

APカテゴリ化ルールを削除すると、APカテゴリ化ルールのすべての設定が削除されます。

APカテゴリ化規則を削除するには、次の手順を実行します

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Virtual Security Domain**を選択します。
3. AP Categorization Ruleタブをクリックします。

   AP分類規則リストには、すべてのAP分類規則が表示されます。
4. 1つのAPカテゴリ化ルールまたは複数のAPカテゴリ化ルールをまとめて削除する:
   - 削除するAPカテゴリ化規則を1つ以上選択して、**Delete**をクリックします。
   - 削除するAPカテゴリ化規則の**Operation**アイコン をクリックしてショートカットメニューの**Delete**を選択。
5. 確認ダイアログボックスで、OKをクリックします。

攻撃検出ポリシーの設定

WIPSは、WIPSシステム上での攻撃検出をサポートします。WIPSは、検出された攻撃に対してアラームを生成し、攻撃を記録します。WIPSは、次の攻撃検出ポリシーをサポートします。

- **Ad hoc network**: アドホックネットワークは、直接通信できるクライアントで構成されるため、攻撃されやすいネットワークです。
- **Spoofing AP**: APスプーフィング攻撃では、潜在的な攻撃者がACに接続して、別の許可されたAPの代わりにアクセスサービスを提供できます。
- **Spoofing client**: クライアントスプーフィング攻撃では、潜在的な攻撃者が、別の許可されたクライアントの代わりにWLANにアクセスできます。
- **AP flood a**: Fake APツールは、多数の偽造APを模倣してビーコンフレームを生成します。これにより、帯域幅の消費、正当なクライアントの誤認、WIPSとの干渉などの問題が発生します。
- **EAPOL – start DoS attack**: 攻撃者は、EAPOL-startフレームでAPをフラッディングすることによって、APの内部リソースを使い果たすことができます。
- **Authentication DoS attack**: 認証DoS攻撃は、認証要求をAPに送信する多数のクライアントを模倣することによって、APのアソシエーションテーブルをフラッディングします。テーブル内のエントリー数が上限に達すると、APは正規のクライアントからの認証要求を処理できなくなります。
- **Association/reassociation DoS attack**: アソシエーション/再アソシエーションDoS攻撃は、APが正規のクライアントを受け入れられないように、大量のスプーフィングされたクライアントアソシエーションでAPをフラッディングすることによって、APのクライアントアソシエーションテーブルを枯渇させます。
- **Weak IV**: WEPセキュリティプロトコルで使用されるRC4暗号化アルゴリズムで安全でないIVが使用されている場合、WEPキーが解読される可能性が高くなります。

- **Invalid OUI**: WIPSのOUIライブラリには、有効なOUIを持つデバイスに関する情報が含まれています。Invalid OUI Detectionは、OUIがライブラリ内にないデバイスを検出します。

アタック検出ポリシーリストの表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Virtual Security Domain**を選択します。
3. **Attack Detection Policy**タブをクリックします。

   アタック検出ポリシーリストには、すべての攻撃検出ポリシーが表示されます。

   Attack Detection Policy Listの内容

   - **Name**: アタック検出ポリシーの名前。
   - **AC**: アタック検出ポリシーが設定されているACのラベル。ACのラベルをクリックすると、その詳細が表示されます。
   - **Operation**: AP分類ルールの**Operation**アイコン ...をクリックして、**Operation**メニューを表示します。

   このメニューで提供される操作タスクには、アタック検出ポリシーの変更、およびアタック検出ポリシーがバインドされている仮想セキュリティドメインの表示が含まれます。

アタック検出ポリシーリストに十分なエントリーが含まれている場合は、次のナビゲーション支援が表示されます。

- **Next Page**アイコンをクリックして、**Attack Detection Policy List**トのページを進めます。
- **Last Page**アイコンをクリックして、**Attack Detection Policy List**の最後のページに進みます。
- **Previous Page**アイコンをクリックして、**Attack Detection Policy List**で前のページに戻ります
- **First Page**アイコンをクリックして、**Attack Detection Policy List**の先頭に戻ります。

アタック検出ポリシーリストの右上にある**8**、**15**、**50**、**100**、または**200**をクリックして、各ページに表示する項目数を指定します。

注:

アタック検出ポリシーリストは、NameフィールドとACフィールドでソートできます。選択したフィールドでリストをソートするには、列ラベルをクリックします。列ラベルを使用して、各フィールドに固有のソートオプションを切り替えることができます。

同期アタック検出ポリシーリスト

IMCは、アタック検出ポリシーリストの自動または手動による同期化をサポートしています。デフォルトでは、IMCはアタック検出ポリシーリストを2時間ごとに自動的に同期化します。

アタック検出ポリシーリストを手動で同期するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Virtual Security Domain**を選択します。
3. **Attack Detection Policy**タブをクリックします。

   アタック検出ポリシーリストには、すべての分類規則が表示されます。
4. **Synchronize**をクリックして、アタック検出ポリシーリストの同期化を開始します。

   同期プロセスが完了すると、ページがリフレッシュされ、最新のデータが表示されます。

攻撃検出ポリシーの照会

基本問合せを実行する手順は、次のとおりです。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Virtual Security Domain**を選択します。
3. **Attack Detection Policy**タブをクリックします。

   アタック検出ポリシーリストには、すべての攻撃検出ポリシーが表示されます。
4. アタック検出ポリシーの名前の一部または全部を、右上隅のQueryフィールドに入力します。
5. **Query**アイコンをクリックします。アタック検出ポリシーリストには、クエリー基準に一致するすべての攻撃検出ポリシーが表示されます。
6. Queryフィールドをクリアして**Query**アイコンをクリックすると、すべての攻撃検出ポリシーが表示されます。拡張クエリーを実行するには、次の手順を実行します。
7. **Service**タブをクリックします。
8. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Virtual Security Domain**を選択します。
9. **Attack Detection Policy**タブをクリックします。

   アタック検出ポリシーリストには、すべての攻撃検出ポリシーが表示されます。
10. Queryフィールドの右にある**Expand**アイコンをクリックします。
11. 次の問合せ基準を1つ以上入力または選択します。
    - **Name**: アタック検出ポリシーの名前の一部または全部を入力します。
    - **AC**: アタック検出ポリシーが設定されているACを選択します。
12. **Query**をクリックします。

アタック検出ポリシーリストには、一致するすべての攻撃検出ポリシーが表示されます。

13. **Reset**をクリックすると、クエリー基準がクリアされ、すべての攻撃検出ポリシーが表示されます。

攻撃検出ポリシーの追加

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Virtual Security Domain**を選択します。
3. **Attack Detection Policy**タブをクリックします。

   アタック検出ポリシーリストには、すべての攻撃検出ポリシーが表示されます。
4. **Add**をクリックします。

   Add Attack Detection Policyページが開きます。
5. Nameフィールドにアタック検出ポリシーの名前を1から32文字の文字列で入力します。有効な文字は、整数、文字およびアンダースコア(_)です。
6. アタック検出ポリシーを設定するACをACリストから選択します。
7. 検出項目を設定します。
   a. ターゲットの検出項目を選択するか、**Select All**を選択してすべての項目を検出します。
   b. 検出項目のパラメーターを設定します。
   - **Quiet Time(s)**: 攻撃が検出され、アラームが生成された後の待機時間を設定します。値の範囲は5～604800秒で、デフォルト値は600秒です。このオプションは、Detected Ad hocおよび

Invalid OUIを除くすべての検出時間に必要です。

- **Action**: WIPSが無効なOUIを検出したときに実行するアクションを設定します。このパラメーターは、Invalid OUIを選択した場合に必要です。オプションは**Rogue**および**None**です。

8. OKをクリックします。

攻撃検出ポリシーの変更

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Virtual Security Domain**を選択します。
3. **Attack Detection Policy**タブをクリックします。

   アタック検出ポリシーリストには、すべての攻撃検出ポリシーが表示されます。
4. 変更するアタック検出ポリシーの**Operation**アイコン ▪▪▪ をクリックしてショートカットメニューから**Modify**を選択します。

   攻撃検出ポリシーを変更するためのページが開きます。
5. アタック検出ポリシーのパラメーターを変更します。

   アタック検出ポリシーの名前acの名前は変更できません。パラメーターの設定の詳細については、「攻撃検出ポリシーの追加」を参照してください。

攻撃検出ポリシーの削除

デフォルトの攻撃検出ポリシーおよび仮想セキュリティドメインにバインドされている攻撃検出ポリシーは削除できません。仮想セキュリティドメインにバインドされている攻撃検出ポリシーを削除するには、最初にバインドを削除します。

攻撃検出ポリシーを削除するには、次の手順を実行します

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Virtual Security Domain**を選択します。
3. **Attack Detection Policy**タブをクリックします。

   アタック検出ポリシーリストには、すべての攻撃検出ポリシーが表示されます。
4. 1つの攻撃検出ポリシーを削除するか、複数の攻撃検出ポリシーをまとめて削除します。
   - 削除するアタック検出ポリシーを選択して、**Delete**をクリックします。
   - 削除するアタック検出ポリシーの**Operation**アイコン ▪▪▪ をクリックしてショートカットメニューの**Delete**をクリックします。
5. 確認ダイアログボックスで、OKをクリックします。

バインドされた仮想セキュリティドメインの表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Virtual Security Domain**を選択します。
3. **Attack Detection Policy**タブをクリックします。

   アタック検出ポリシーリストには、すべての攻撃検出ポリシーが表示されます。
4. ターゲット攻撃検出ポリシーの**Operation**アイコン ▪▪▪をクリックし、ショートカットメニューから**Display Bound Virtual Security Domains**を選択します。

   Bound virtual security domainウィンドウが開き、アタック検出ポリシーが仮想セキュリティドメインリ

ストにバインドされているすべての仮想セキュリティドメインが表示されます。

仮想セキュリティドメインリスト

- **Attack Detection Policy**: アタック検出ポリシーの名前。
- **Virtual Security Domain**: バインドされた仮想セキュリティドメインの名前。

5. Backをクリックして、アタックDetection Policyページに戻ります。

シグニチャポリシーの設定

シグニチャポリシーには、一連のシグニチャルールが含まれています。シグニチャルールは、802.11パケットの特性を識別し、一致するパケットに対して対応するアクション(シグニチャイベントの生成など)を実行するために使用されます。フレームタイプ、MACアドレス、SSID、およびSSIDの長さを指定できます。

さらに、特殊な特性を持つ802.11パケットを識別するようにサブ規則を設定できます。

シグニチャポリシーリストの表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Virtual Security Domain**を選択します。
3. **Signature Policy**タブをクリックします。

   シグニチャポリシーリストには、すべてのシグニチャポリシーが表示されます。

   - **Name**: シグネチャポリシーの名前。名前のリンクをクリックすると、その詳細が表示されます。
   - **AC**: シグニチャポリシーが設定されているACのラベル。ラベルのリンクをクリックすると、AC管理ページが表示されます。
   - **Operation**: シグニチャポリシーの**Operation**アイコン ... をクリックして、**Operation**メニューを表示します。
   - このメニューで提供される操作タスクには、署名ポリシーの変更と削除、および署名ポリシーがバインドされている仮想セキュリティドメインの表示が含まれます。

シグニチャポリシーリストに十分なエントリーが含まれている場合は、次のナビゲーションツールが表示されます。

- **Next Page**アイコンをクリックして、**signature policy**リストの次のページに進みます。
- **Last Page**アイコンをクリックして、**signature policy**リストの最後に進みます
- **Previous Page**アイコンをクリックして、**signature policy**リストの前のページに戻ります。
- **First Page**アイコンをクリックして、**signature policy**リストの最初のページに戻ります。

シグニチャポリシーリストの右上にある**8**、**15**、**50**、**100**、または**200**をクリックして、各ページに表示する項目数を指定します。

注:

シグニチャポリシーリストは、Operationフィールド以外のすべてのフィールドでソートできます。選択したフィールドでリストをソートするには、列ラベルをクリックします。列ラベルを使用すると、各フィールドに固有のソートオプションを切り替えることができます。

シグニチャポリシーの詳細の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Virtual Security Domain**を選択します。
3. **Signature Policy**タブをクリックします。

   シグニチャポリシーリストには、すべてのシグニチャポリシーが表示されます。
4. ターゲットシグニチャポリシーの名前リンクをクリックすると、その詳細が表示されます。

   基本的な情報
   - **Policy Name**: シグニチャポリシーの名前。
   - **AC**: シグニチャポリシーが設定されているACのラベル。

   署名ルール一覧
   - **Rule ID**: シグニチャルールのID。
   - **Rule Name**: シグニチャルールの名前。
   - **Rule Priority**: シグニチャルールのプライオリティ。
5. **Back**をクリックして、シグニチャポリシーリストページに戻ります。

シグニチャポリシーリストの同期

IMCは、シグニチャポリシーリストの自動または手動による同期化をサポートしています。デフォルトでは、IMCはシグニチャポリシーリストを2時間ごとに自動的に同期化します。

シグニチャポリシーリストを手動で同期するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Virtual Security Domain**を選択します。
3. **Signature Policy**タブをクリックします。

   シグニチャポリシーリストには、すべてのシグニチャポリシーが表示されます。
4. **Synchronize**をクリックして、シグニチャポリシーリストの同期化を開始します。

   同期プロセスが完了すると、ページがリフレッシュされ、最新のデータが表示されます。

シグニチャポリシーのクエリー

基本問合せを実行する手順は、次のとおりです。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Virtual Security Domain**を選択します。
3. **Signature Policy**タブをクリックします。

   シグニチャポリシーリストには、すべてのシグニチャポリシーが表示されます。
4. 右上隅のQueryフィールドに、シグニチャポリシーの名前の一部または全部を入力します。
5. **Query**アイコン🔍をクリックします。シグニチャポリシーリストには、クエリー基準に一致するすべてのシグニチャポリシーが表示されます。
6. 問合せポリシーを表示するには、**Query**フィールドをクリアして**Query**アイコン🔍をクリックします。

高度なクエリーを実行するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Virtual Security Domain**を選択します。

3. **Signature Policy**タブをクリックします。

   シグニチャポリシーリストには、すべてのシグニチャポリシーが表示されます。

4. 問合せフィールドの右にある**Expand**アイコンをクリックします。この操作により、問合せフィールドも消去されます。

5. クエリー基準を設定します。
   - **Policy Name**: シグニチャポリシー名の一部または全部を入力します。
   - **AC**: シグニチャポリシーが設定されているACを選択します。Allを選択した場合、このフィールドはクエリー基準として使用されません。

6. **Query**をクリックします。

   Signature Policyリストには、クエリー基準に一致するすべてのシグニチャポリシーが表示されます。

7. クエリー基準をクリアしてすべてのシグニチャポリシーを表示するには、**Reset**をクリックします。

シグニチャポリシーの追加

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Virtual Security Domain**を選択します。
3. **Signature Policy**タブをクリックします。

   シグニチャポリシーリストには、すべてのシグニチャポリシーが表示されます。

4. **Add**をクリックします。
5. 基本的な情報を設定します。
   - **Policy Name**: シグニチャポリシー名を1～32文字の文字列で入力します。この文字列には、文字、数字、および下線だけを含めることができます。
   - **AC**: シグニチャポリシーを作成するACを選択します。
6. シグニチャポリシーのシグニチャ規則を選択し、シグニチャ規則のプライオリティを変更します。
   a. **Select**.をクリックします。
   b. **Query**領域にシグネチャルール名の一部または全部を入力し、**Query**をクリックします。**Signature Rule**リストには、問合せ基準と一致するすべてのシグネチャルールが表示されます。**Reset**をクリックすると、問合せ基準が消去され、すべてのシグネチャルールが表示されます。

      署名ルール一覧

      Rule ID: シグニチャルールのID。

      Rule Name: シグニチャルールの名前。

      AC: シグニチャルールが設定されているACのラベル。

   c. 1つ以上のシグニチャルールを選択します。
   d. **OK**をクリックして**Add Signature Policy**ページに戻ります。Signature Ruleリストに、選択したすべての署名ルールが表示されます。

      署名ルール一覧

      – **Rule Priority**: シグニチャルールのプライオリティを1～64の範囲で入力します。デフォルト値は1です。

        センサーはフレームを受信すると、プライオリティ順にシグニチャルールを照合します。一致が見つかると、センサーはルールで指定されたアクションを実行します。シグニチャルールのプライオリティが同じ場合、センサーはIDに従ってシグニチャルールを昇順に照合します。

      – **Delete**アイコンをクリックすると、シグネチャルールが削除されます。

すべてのシグネチャルールを削除するには、**Remove All**をクリックします。

7. OKをクリックします。

シグニチャポリシーの変更

署名ポリシーが構成されている署名ポリシー名およびACは変更できません。他のパラメーターの変更の詳細は、「署名ポリシーの追加」を参照してください。

シグニチャポリシーを変更するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Virtual Security Domain**を選択します。
3. **Signature Policy**タブをクリックします。

   シグニチャポリシーリストには、すべてのシグニチャポリシーが表示されます。
4. 変更するシグニチャポリシーの**Operation**アイコン ･･･ をクリックし、ショートカットメニューから**Modify**を選択します。

バインドされた仮想セキュリティドメインの表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Virtual Security Domain**を選択します。
3. **Signature Policy**タブをクリックします。

   シグニチャポリシーリストには、すべてのシグニチャポリシーが表示されます。
4. ターゲットのシグニチャポリシーの**Operation**アイコン ･･･ をクリックし、ショートカットメニューからDisplay Bound Virtual Security Domainsを選択します。

   Bound Virtual Security Domainダイアログボックスが開きます。
   - **Signature Policy**: 署名ポリシーの名前。
   - **Virtual Security Domain**: バインドされた仮想セキュリティドメインの名前。
5. **Close**をクリックします。

シグニチャポリシーの削除

デフォルトの署名ポリシーおよび仮想セキュリティドメインにバインドされている署名ポリシーは削除できません。仮想セキュリティドメインにバインドされている署名ポリシーを削除するには、最初にバインドを削除します。署名ルールおよびサブルールは削除されません。

シグニチャポリシーを削除するには

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Virtual Security Domain**を選択します。
3. **Signature Policy**タブをクリックします。

   シグニチャポリシーリストには、すべてのシグニチャポリシーが表示されます。
4. 1つまたは複数のシグニチャポリシーをバッチで削除します。
   - 削除するシグニチャポリシーの**Operation**アイコン ･･･ をクリックし、ショートカットメニューの **Delete**を選択。
   - 削除するシグニチャポリシーを選択し、**Delete**をクリックします。
5. 確認ダイアログボックスで、OKをクリックします。

署名ルール一覧の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Virtual Security Domain**を選択します。
3. **Signature Policy**タブをクリックします。
4. **Signature Rule**をクリックします。

   シグニチャルールリストには、すべてのシグニチャルールが表示されます。

   署名ルール一覧

   - **Rule ID**: シグネチャルールのID。IDリンクをクリックすると、その詳細が表示されます。
   - **Rule Name**: シグニチャルールの名前。
   - **AC**: シグニチャルールが設定されているACのラベル。デバイスラベルのリンクをクリックすると、AC管理ページが表示されます。
   - **Operation**: シグネチャルールの**Operation**アイコン をクリックすると、**Operation**メニューが表示されます。メニューに表示される操作タスクには、シグネチャルールの変更と削除、およびシグネチャルールが属するシグネチャポリシーの表示が含まれます。

     システム定義のシグニチャルールは削除できません。シグニチャポリシーに属するシグニチャルールは、変更および削除できません。

   シグニチャルールリストに十分なエントリーが含まれている場合は、次のナビゲーションツールが表示されます。

   - **Next Page**アイコンをクリックして、**Signature Rule**リストの次のページに進みます。
   - **Last Page**アイコンをクリックして、**Signature Rule**リストの最後に進みます。
   - **Previous Page**アイコンをクリックして、**Signature Rule**リストで前のページに戻ります。
   - **First Page**アイコンをクリックして、**Signature Rule**リストの先頭に戻ります。

   シグニチャルールリストの右上にある8、15、50、100、または200をクリックして、各ページに表示する項目数を指定します。

   注:

   シグネチャルールリストは、Operationフィールド以外のすべてのフィールドでソートできます。選択したフィールドでリストをソートするには、列ラベルをクリックします。列ラベルを使用すると、各フィールドに固有のソートオプションを切り替えることができます。

5. **Back**をクリックして、シグニチャポリシーリストページに戻ります。

シグニチャルールリストの同期

IMCは、シグニチャルールリストの自動または手動による同期化をサポートしています。デフォルトでは、IMCはシグニチャルールリストを2時間ごとに自動的に同期化します。

シグニチャルールリストを手動で同期するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Virtual Security Domain**を選択します。
3. **Signature Policy**タブをクリックします。

   シグニチャポリシーリストには、すべてのシグニチャ規則が表示されます。
4. **Signature Rule**をクリックします。

5. **Synchronize**をクリックして、シグニチャルールリストの同期化を開始します。
   同期プロセスが完了すると、ページがリフレッシュされ、最新のデータが表示されます。

シグニチャルールの詳細の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Virtual Security Domain**を選択します。
3. **Signature Policy**タブをクリックします。
4. **Signature Rule**をクリックします。
   シグニチャルールリストには、すべてのシグニチャルールが表示されます。
5. ルールIDリンクをクリックすると、その詳細が表示されます。
   ルール情報
   - **Rule ID**: シグニチャルールのID。
   - **Rule Name**: シグニチャルールの名前。
   - **AC**: シグニチャルールが設定されているACのラベル。
   - **Alarm Event Level**: シグニチャルールが一致した後に生成されるアラームイベントのレベル。範囲は0～7です。レベルが高いほど、より深刻なイベントを表します。
   - **Tracking Mode**: 署名ルールの追跡モード。オプションは、**Signature, MAC**, 及び **Signature and MAC**。
   - **Threshold For MAC Address Tracking**: このオプションは、**MAC**又は**Signature and MAC** 追跡モード。
   - **Threshold For Signature Tracking** : このオプションは、**Signature**または**Signature and MAC** 追跡モード。
   - **Statistics Collection Interval(s)**: WIPSは、成功したシグニチャルールまたはMACアドレスの一致に関する統計情報を定期的に収集します。
   - **Quiet Time(s)**: シグニチャルールまたはMACアドレスの一致カウントが上限に達すると、シグニチャルールのMACアドレスは待機時間に入り、それ以上一致しません。
   - **Matching Relations**: 各アイテムの一致リレーション。オプションは**AND**と**OR**です。
     下の領域には、一致項目とその値が表示されます。一致項目が使用可能でない場合、値は**None**と表示されます。
     一致フレームタイプ
     - **frame type**: **Control Frame**、**Management Frame**、および**Data Frame**のオプションがあります。
     - **Match Frame Sub Type**: オプションには、**None**、**Dis-association**、**Probe Request**、**Beacon**、**Association Response**、**De-authentication**、**Association Request**、および**Authentication**があります。**None**を選択すると、WIPSはどのフレームサブタイプとも一致しません。

     802.11フレームは、事前定義された値と一致する場合、この項目と一致すると見なされます。
     MACアドレスの一致
     - **MAC address**
     - **Match MAC Address Type**: オプションは、Source Address、Destination Address、およびBSSIDです。

     802.11フレームは、事前定義された値と一致する場合、この項目と一致すると見なされます。
     パケットシーケンス番号の照合

- **Match Criteria**: オプションには、Greater than、Smaller than、Between、およびEqual toがあります。
- **Start Value**: このフィールドは、一致基準が**Greater than**または**Between**.の場合に表示されます。
- **End Value**: このフィールドは、一致基準が**Smaller than**または**Between**の場合に表示されます。
- **Value**: このフィールドは、一致基準が**Equal to**の場合に表示されます。

802.11フレームは、事前定義された値と一致する場合、この項目と一致すると見なされます。

SSIDの長さの一致

- **Match Criteria**: オプションには、**Greater than**、**Smaller than**、**Between**、および**Equal to**があります。
- **Start Value**: このフィールドは、一致基準が**Greater than**または**Between**の場合に表示されます。
- **End Value**: このフィールドは、一致基準がSmaller than または**Between**の場合に表示されます。
- **Value**: このフィールドは、一致基準が**Equal to**の場合に表示されます。

802.11フレームは、事前定義された値と一致する場合、この項目と一致すると見なされます。

SSIDの一致

- **Match Criteria**: オプションには、**Greater than**、**Smaller than**、**Between**、および**Equal to**があります。
- **Value**。
- **Case Sensitive**: オプションは、YesとNoです。

802.11フレームは、事前定義された値と一致する場合、この項目と一致すると見なされます。

6. **Back**をクリックします。

シグニチャルールのクエリー

基本問合せを実行する手順は、次のとおりです。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Virtual Security Domain**を選択します。
3. **Signature Policy**タブをクリックします。
4. **Signature Rule**をクリックします。

   シグニチャルールリストには、すべてのシグニチャルールが表示されます。
5. 右上隅のQueryフィールドに、シグニチャルールの名前の一部または全部を入力します。
6. **Query**アイコンをクリックします。

   シグニチャルールリストには、クエリー基準と一致するすべてのシグニチャルールが表示されます。
7. Queryフィールドを消去して**Query**アイコンをクリックすると、すべてのシグネチャ

ルールが表示されます。拡張問合せを実行する手順は、次のとおりです。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Virtual Security Domain**を選択します。
3. **Signature Policy**タブをクリックします。
4. **Signature Rule**をクリックします。

シグニチャルールリストには、すべてのシグニチャルールが表示されます。

5. 問合せフィールドの右にある**Expand**アイコンをクリックします。この操作により、問合せフィールドも消去されます。
6. クエリー基準を設定します。
   - **Rule Name**: シグニチャルール名の一部または全部を入力します。
   - **AC**: -シグネチャルールが構成されているACを選択します。**All**を選択すると、このフィールドは問合せ基準として使用されません。
7. **Query**をクリックします。

   シグニチャルールリストには、クエリー基準と一致するすべてのシグニチャルールが表示されます。
8. クエリー基準をクリアしてすべてのシグニチャルールを表示するには、**Reset**をクリックします。

シグニチャルールの追加

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Virtual Security Domain**を選択します。
3. **Signature Policy**タブをクリックします。
4. **Signature Rule**をクリックします。

   シグニチャルールリストには、すべてのシグニチャルールが表示されます。
5. **Add**をクリックします。
6. シグニチャルール情報を設定します。
   - **AC**: ACを選択します。IMCはACにシグニチャルールを作成します。
   - **Rule ID**: シグニチャルールIDを選択します。ルールIDはシグニチャルールを一意に識別します。IMCがデバイスと時間内に同期しない場合、シグニチャルールを追加するときにエラーが発生することがあります。たとえば、ID 50のシグニチャルールを作成したが、IMCがデバイスと時間内に同期しない場合、IMCでID 50のシグニチャルールを追加すると失敗します。
   - **Rule Name**: シグネチャルールの名前を1から32文字の文字列で入力します。名前には、文字、数字および下線を使用できます。ルール名は一意である必要があります。
   - **Alarm Event Level**: アラームイベントレベルを選択します。レベルが高いほど、より重大なイベントを表します。シグニチャルールの一致数が上限に達すると、センサーはアラームイベントを生成し、ACに報告します。
   - **Tracking Mode**: シグニチャルールのトラッキングモードを選択します。オプションはMAC、**Signature**、および**MAC and Signature**です。
     - **MAC**: 国コードでサポートされているすべてのチャネルについて、シグニチャルールに対する各MACアドレスの一致数を記録します。MACアドレスの一致数がしきい値に達すると、センサーはアラームイベントを生成し、そのイベントをACに報告します。
     - **Signature**: 国コードでサポートされているチャネルごとに、802.11フレームに対する各シグニチャルールの一致数を記録します。シグニチャルールの一致数がしきい値に達すると、センサーはアラームイベントを生成し、そのイベントをACに報告します。
     - **MAC and Signature**: 両方のトラッキングモードを使用します。
   - **Threshold For MAC Address Tracking**: MACアドレストラッキングのしきい値を1～32000の範囲で設定します。デフォルト値は1000です。MACアドレスの一致数がしきい値に達すると、センサーはアラームイベントを生成します。このオプションは、トラッキングモードが**MAC**または**MAC and Signature**の場合に必要です。
   - **Threshold For Signature Tracking**: シグニチャトラッキングのしきい値を1～32000の範囲で設定します。デフォルト値は1000です。シグニチャルールの一致数がしきい値に達す

ると、センサーはアラームイベントを生成します。このオプションは、トラッキングモードが**Signature**または**MAC and Signature**の場合に必要です。

- **Statistics Collection Interval(s)**: センサーがシグニチャルール照合統計情報を収集する間隔を1～3600の範囲で設定します。デフォルト値は60です。
- **Quiet Time(s)**: トラッキングモードに応じて、シグニチャルールまたはMACアドレスの待機時間を設定します。トラッキングモードがMACの場合、このオプションはMACアドレスに対して有効です。トラッキングモードがシグニチャの場合、このオプションはシグニチャルールに対して有効です。トラッキングモードがMACおよびシグニチャの場合、このオプションは両方に対して有効です。MACアドレスおよびシグニチャルール。MACおよびシグニチャトラッキングモードを選択したとします。MACアドレスの一致カウントがしきい値に達し、WIPSがアラームイベントを生成すると、MACアドレスは待機時間に入り、待機時間が終了するまでどのシグニチャルールにも一致しません。WIPSは、一致カウントがしきい値に達するまで、シグニチャルールを802.11フレームと照合し続けます。その後、シグニチャルールは待機時間に入ります。
- **Matching Relations**: 各一致項目の一致関係を設定します。オプションは**AND**と**OR**です。ANDは、802.11フレームがすべての項目と一致する場合にのみシグニチャルールと一致することを示します。**OR**は、802.11フレームが1つの項目と一致する限りシグニチャルールと一致することを示します。

7. 一致項目を設定します。オプションは、**Match Frame Type**、**Match MAC Address**、**Match SSID**、**Match SSID Length**、および**Match Packet Sequence Number**です。

一致項目のパラメーターは、一致項目を選択した場合にのみ表示されます。一致項目の構成の詳細は、表42を参照してください。

表42照合項目の構成

アイテムの一致	説明	パラメーター
マッチフレームタイプ	この項目が有効な場合、WIPSはフレームタイプとサブタイプを検出します。マッチングのために受信する802.11フレーム。	• **Frame type**: フレームタイプを選択します。オプションは、**Management Frame**、**Control Frame**および**Data Frame**です。 • **Match Frame Sub Type**: フレームサブタイプを選択します。オプションは、**None**、**Dis-association**、**Probe Request**、**Beacon**、**Association Response**、**De-authentication**、**Association Request**および**Authentication**です。このパラメーターは、フレームタイプが**Management Frame**の場合に必要です。**None**を選択すると、フレームサブタイプは一致しません。
MACアドレスの一致	この項目が有効になっている場合、WIPSは受信した802.11フレームごとにMACアドレスを検出して一致します。	• **MAC address**: xx:xx:xx:xx:xx:xx形式でMACアドレスを入力します。 • **MAC Address Type**: MACアドレスタイプを選択します。オプションは、**Source Address**、**Destination Address**、および**BSSID**です。
SSIDの一致	この項目が有効になっている場合、WIPSは各マッチングのために受信する802.11フレーム。	• **Match Criteria**: **Match Criteria**を選択します。オプションには、**Include**、**Exclude**、**Equal to**および**Not Equal to**があります。 • **Value**: SSID(1～32文字の文字列)を入力します。文字、数字、および下線だけを含めることができます。 • **Case Sensitive**: **Yes**または**No**を選択して、SSIDを照合するときに大文字と小文字を区別するかどうかを指定します。
		• **Match Criteria**: 一致基準を選択します。オプションは、**Greater than**、**Smaller than**、**Between**および**Equal to**です。

SSIDの長さの一致	この項目が有効になっている場合、WIPSは受信した802.11フレームごとにSSIDの長さを検出して一致します。	• **Start Value**: 開始値を0～の範囲で入力します。31.このパラメーターは、一致基準が**Greater than**または**Between**である場合に必要です。 • **End Value**: -開始値を1～の範囲で入力します。32.このパラメーターは、一致基準が**Smaller than**または**Between**の場合に必要です。 • **Value**: SSIDの長さを0～の範囲で入力します。32.このパラメーターは、一致基準が**Equal to**の場合に必要です。
パケットシーケンス番号の照合	この項目が有効になっている場合、WIPSは受信する各802.11フレームのシーケンス番号を検出して一致させます。	• **Match Criteria**: 一致基準を選択します。オプションは、**Smaller than**、**Smaller than**、**Between**および**Equal to**です。 **Start Value**: 開始値を 0 から 4094 の範囲で入力します。このパラメーターは、一致基準が**Greater** または **Between** の場合に必要です。 • **End Value**: 1～4095の範囲の終了値を入力します。このパラメーターは、一致基準が**Smaller than**または**Between**の場合に必要です。 • **Value**: 0～4095の範囲のパケットシーケンス番号を入力します。このパラメーターは、一致基準が**Equal to**の場合に必要です。

8. **OK**をクリックします。

シグニチャルールの変更

署名ポリシーにバインドされている署名規則は変更できません。署名規則を変更するには、次の手順を

実行します:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Virtual Security Domain**を選択します。
3. **Signature Policy**タブをクリックします。
4. **Signature Rule**をクリックします。

   シグニチャルールリストには、AC上のすべてのシグニチャルールが表示されます。
5. 変更するシグニチャルールの**Operation**アイコン ･･･をクリックし、ショートカットメニューから**Modify**を選択します。

   AC、**Rule ID**および**Rule Name**は変更できません。他のパラメーターの変更方法の詳細は、「シグネチャルールの追加」を参照してください。

シグニチャルールの削除

システムでは署名ルールが定義されており、署名ポリシーにバインドされている署名ルールは削除できません。署名ポリシーにバインドされている署名ルールを削除するには、最初にバインドを削除してください。

署名ルールを削除するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Virtual Security Domai**nを選択します。
3. **Signature Policy**タブをクリックします。
4. 単一のシグネチャルールまたはバッチ内の複数のシグネチャルールを削除します。
   - 削除するシグニチャルールの**Operation**アイコン ･･･ をクリックし、ショートカットメニューから

Deleteを選択します。

- 削除するシグニチャルールを選択し、**Delete**をクリックします。

5. 確認ダイアログボックスで、**OK**をクリックします。

下位規則リストの表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Virtual Security Domain**を選択します。
3. **Signature Policy**タブをクリックします。
4. **Signature Rule**をクリックします。
5. **Sub Rule**をクリックします。

   サブルールリストには、すべてのサブルールが表示されます。

   - **Sub Rule ID**: サブルールのID。IDリンクをクリックすると、その詳細が表示されます。
   - **Sub Rule Name**: サブルールの名前。この列は、サブルールに名前がない場合に表示されます。
   - **Rule ID**:サブルールが属するシグニチャルールのID。
   - **Rule Name**:サブ規則が属するシグニチャ規則の名前。
   - **AC**: サブルールが設定されているACのラベル。ラベルのリンクをクリックすると、AC管理ページが表示されます。
   - **Modify**: 変更するサブルールの**Modify**アイコン をクリックします。署名ルールが署名ポリシーにバインドされているサブルールは変更できません。このタイプのサブルールにはアイコンが表示されます。
   - **Delete**: 削除するサブルールの**Delete**アイコンをクリックします。署名ルールが署名ポリシーにバインドされているサブルールは削除できません。このタイプのサブルールには -- アイコンが表示されます。

   サブ規則リストに十分な数のエントリーが含まれている場合は、次のナビゲーションツールが表示されます。

   - **Next Page**アイコンをクリックして、サブルールリスト内で次のページに進みます。
   - **Last Page**アイコンをクリックして、サブルールリストの最後にページを移動します。
   - **Previous Page**アイコンをクリックして、サブ規則リストのページを逆方向に移動します。
   - **First Page**アイコンをクリックして、サブ規則リストの先頭にページバックします。

   サブ規則リストの右上にある**8**、**15**、**50**、**100**、または**200**をクリックして、各ページに表示する項目数を指定します。

   注:

   変更フィールドと削除フィールド以外のすべてのフィールドで、サブルールの一覧を並べ替えることができます。選択したフィールドで一覧を並べ替えるには、列見出しをクリックします。列見出しを使用すると、各フィールドに固有の並べ替えオプションを切り替えることができます。

6. **Back**をクリックして、シグニチャルールリストに戻ります。

下位規則リストの同期化

IMCは、サブルールリストの自動または手動による同期化をサポートしています。デフォルトでは、IMCは

サブルールリストを2時間ごとに自動的に同期化します。

サブ規則リストを手動で同期するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Virtual Security Domain**を選択します。
3. **Signature Policy**タブをクリックします。

   シグニチャルールリストには、すべてのシグニチャルールが表示されます。
4. **Signature Rule**をクリックします。
5. **Sub Rule**をクリックします。
6. **Synchronize**をクリックして、サブ規則リストの同期化を開始します。

   同期プロセスが完了すると、ページがリフレッシュされ、最新のデータが表示されます。

サブルールの詳細の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Virtual Security Domain**を選択します。
3. **Signature Policy**タブをクリックします。
4. **Signature Rule**をクリックします。
5. **Sub Rule**をクリックします。

   サブルールリストには、すべてのサブルールが表示されます。
6. subrule IDリンクをクリックして、その詳細を表示します。
   - **AC**: サブルールが設定されているACのラベル。
   - **Rule Name**: サブ規則が属するシグニチャ規則の名前。
   - **Sub Rule ID**: サブ規則のID。
   - **Offset Value**: 指定した開始ビットからのフレームを一致させます。
   - **Mask Value**: 指定したマスクとフレームを一致させます。
   - **Match from Payload**: フレームボディから始まるフレームをマッチングします。
   - **Sub Rule Name**: サブルールの名前。サブルールに名前がない場合、このフィールドには**None**と表示されます。
   - **Pattern Value**: 指定されたパターンに基づいてフレームを照合します。マスク値と802.11フレームを使用してWIPSが計算する値がパターン値の範囲内にある場合、802.11フレームはサブルールに一致します。パターン値のパラメーターには次のものがあります。
     - **Match criteria**: オプションには、**Greater than**, **Smaller than**, **Between**および**Equal to**があります。
     - **Pattern value**:このフィールドは、一致基準が**Equal to**の場合にだけ使用できます。
     - **Min.Pattern Value**: このフィールドは、一致基準が**Between**の場合にだけ使用できます。またはより大きい。
     - **Max.Pattern Value**: このフィールドは、一致基準が**Between**の場合にだけ使用できます。またはより小さい。
7. **Back**をクリックしてサブ規則リストに戻ります。

サブルールのクエリー

基本問合せを実行する手順は、次のとおりです。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Virtual Security Domain**を選択します。
3. **Signature Policy**タブをクリックします。
4. **Signature Rule**をクリックします。
5. **Sub Rule**をクリックします。

   サブルールリストには、すべてのサブルールが表示されます。
6. 右上隅のQueryフィールドに、サブ規則の名前の一部または全体を入力します。
7. **Query**アイコンをクリックします。下位ルールリストに、問合せ基準と一致するすべての下位ルールが表示されます。
8. **Query**フィールドを消去して**Query**アイコンをクリックすると、すべてのサブルールが表示されます。

拡張問合せを実行する手順は、次のとおりです。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Virtual Security Domain**を選択します。
3. **Signature Policy**タブをクリックします。
4. **Signature Rule**をクリックします。
5. **Sub Rule**をクリックします。

   サブルールリストには、すべてのサブルールが表示されます。
6. Queryフィールドの右にある**Expand**アイコンをクリックします。
7. クエリー基準を設定します。
   - **Sub Rule Name**: サブルール名を入力します。WSMは、このフィールドのファジーマッチングをサポートしています。
   - **AC**: シグネチャルールが構成されているACを選択します。**All**を選択すると、このフィールドは問合せ基準として使用されません。
8. **Query**をクリックします。

   サブルールリストには、**Query**条件に一致するすべてのサブルールが表示されます。
9. **Reset**をクリックしてクエリー基準をクリアし、すべてのサブ規則を表示します。

サブルールの追加

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Virtual Security Domain**を選択します。
3. **Signature Policy**タブをクリックします。
4. **Signature Rule**をクリックします。
5. **Sub Rule**をクリックします。

   サブルールリストには、すべてのサブルールが表示されます。
6. **Add**をクリックします。
7. サブルール情報を設定します。
   - **AC**: ACを選択します。IMCはAC上にサブルールを作成します。
   - **Rule Name**: サブ規則が属するシグニチャ規則の名前を選択します。
   - **Rule ID**: 1～27の範囲でサブルールIDを選択します。選択したIDがデバイスですでに使用され

ている場合、サブルールの追加は失敗します。

- **Offset Value**: オフセット値を0～2364の範囲で入力します。オフセット値は、どのビットからWIPSがフレームを開始するビットを決定します。
- **Mask Value**: 0～65535の範囲のマスク値を入力します。WIPSは、マスク値と802.11フレームの一部を使用して値を計算します。次に、その値をパターン値と比較します。この値がパターン値の範囲内にある場合、802.11フレームは下位規則と一致します。
- **Match from Payload**: フレームボディから始まるフレームをマッチングするには、このパラメーターを選択します。
- **Sub Rule Name**: サブルールに名前を付ける必要はありません。サブルールに名前を付けるには、Sub Rule Nameを選択し、1から32文字の文字列を入力します。文字列には、文字、数字および下線を使用できます。名前は一意である必要があります。
- **Pattern Value**: 以下のパラメーターを含む、サブ規則のパターン値を設定します。
  - 一致基準オプションには、**Greater than**、**Smaller than**、**Between**および**Equal to**があります。
  - **Pattern value**: このフィールドは、一致基準が**Equal to**の場合にだけ必要です。
  - **Min.Pattern Value**: このフィールドは、一致基準が**Between**の場合にだけ必要です。またはより大きい。
  - **Max.Pattern Value**: このフィールドは、一致基準が**Between**の場合にだけ必要です。またはより小さい。

8. **OK**をクリックします。

サブルールの変更

システム定義のサブルールおよび署名ルールが署名ポリシーにバインドされているサブルールは変更できません。後者のサブルールを変更するには、最初にバインドを削除します。

サブルールを変更するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Virtual Security Domain**を選択します。
3. **Signature Policy**タブをクリックします。
4. **Signature Rule**をクリックします。
5. **Sub Rule**をクリックします。

   サブルールリストには、すべてのサブルールが表示されます。
6. 変更するサブ規則の**Modify**アイコンをクリックします。

   AC、ルール名、サブルールIDおよびサブルール名は変更できません。他のパラメーターを変更する方法の詳細は、「サブルールの追加」を参照してください。
7. OKをクリックします。

サブルールの削除

システム定義のサブルールおよび署名ルールが署名ポリシーにバインドされているサブルールは削除できません。後者のサブルールを削除するには、最初にバインドを削除します。

サブルールを削除するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Virtual Security**

Domainを選択します。

3. **Signature Policy**タブをクリックします。
4. **Signature Rule**をクリックします。
5. **Sub Rule**をクリックします。

   サブルールリストには、すべてのサブルールが表示されます。
6. 1つまたは複数のサブルールをバッチで削除します。
   - 削除するサブルールの**Delete**アイコンをクリックします。
   - 削除するシグニチャルールを選択し、**Delete**をクリックします。
7. 確認ダイアログボックスで、OKをクリックします。

対策ポリシーの設定

WIPSは、不正なAPまたはクライアントに対して次の対策を講じることができます。

- 不正クライアントの防止。
- 不正なワイヤレスデバイスの関連付けを解除するようにセンサーに通知します。

対策ポリシーは、仮想セキュリティドメインにバインドされている場合にのみ有効になります。1つの対策ポリシーは、複数の仮想セキュリティドメインにバインドできます。

対策方針一覧の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Virtual Security Domain**を選択します。
3. **Countermeasure Policy**タブをクリックします。

   対策ポリシーリストには、すべての対策ポリシーが表示されます。
   - **Name** : 対抗措置ポリシーの名前。名前のリンクをクリックすると、その詳細が表示されます。
   - **AC**: 対策ポリシーが設定されているACのラベル。ラベルのリンクをクリックすると、AC管理ページが表示されます。
   - **Operation**: **Operation**メニューを表示するには、対策ポリシーの**Operation**アイコンをクリックします。

   このメニューで提供される操作タスクには、署名ポリシーの変更と削除、および署名ポリシーがバインドされている仮想セキュリティドメインの表示が含まれます。

対策ポリシーリストに十分なエントリーが含まれている場合は、次のナビゲーションツールが表示されます。

- **Next Page**アイコンをクリックして、**Countermeasure Policy**リストの次のページに進みます。
- **Last Page**アイコンをクリックして、**Countermeasure Policy**リストの最後にページを移動します。
- **Previous Page**アイコンをクリックして、**Countermeasure Policy**リストのページを逆方向に移動します。
- **First Page**アイコンをクリックすると、**Countermeasure Policy**リストの先頭に戻ることができます。

対策ポリシーリストの右上にある**8**、**15**、**50**、**100**、または**200**をクリックして、各ページに表示する項目数を指定します。

注:

Operationフィールド以外のすべてのフィールドで、対策ポリシーリストをソートできます。選択したフィールドでリストをソートするには、列ラベルをクリックします。列ラベルを使用して、各フィールドに固有のソートオプションを切り替えることができます。

対策方針リストの同期

IMCは、対策ポリシーリストの自動または手動による同期化をサポートしています。デフォルトでは、IMCは2時間ごとに対策ポリシーリストを自動的に同期化します。

対策ポリシーリストを手動で同期するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Virtual Security Domain**を選択します。
3. **Countermeasure Policy**タブをクリックします。

   対策ポリシーリストには、すべての対策ポリシーが表示されます。
4. **Synchronize**をクリックして、対抗措置ポリシーリストの同期化を開始します

   同期プロセスが完了すると、ページがリフレッシュされ、最新のデータが表示されます。

対策方針の詳細の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Virtual Security Domain**を選択します。
3. **Countermeasure Policy**タブをクリックします。

Countermeasure Policyリストには、すべての対策ポリシーが表示されます。

4. ターゲット対策ポリシーの名前リンクをクリックすると、その詳細が表示されます。

   対策方針情報
   - **Name**: 対策ポリシーの名前。
   - **AC**: 対策ポリシーが設定されているACのラベル。
   - **Enable Countermeasures on a Fixed Channel**: オプションはYesとNoです。
   - 対策方針で支援する機能
     - **Item**: 対抗措置アイテムがサポートされているかどうか。オプションは**Yes**および**No**です。
     - **Priority**: 0から9の範囲の対策項目の優先度。値が大きいほど優先度が高くなります。
5. **Close**をクリックします。

対抗措置ポリシーの照会

基本問合せを実行する手順は、次のとおりです。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Virtual Security Domain**を選択します。
3. **Countermeasure Policy**タブをクリックします。

   Countermeasure Policyリストには、すべての対策ポリシーが表示されます。
4. 右上隅のQueryフィールドに、対策ポリシーの名前の一部または全部を入力します。

5. **Query**アイコンをクリックします。サブルールリストには、問合せ基準に一致するすべての対策ポリシーが表示されます。
6. **Query**フィールドを消去して**Query**アイコンをクリックすると、すべての対抗措置ポリシーが表示されます。

拡張問合せを実行する手順は、次のとおりです。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Virtual Security Domain**を選択します。
3. **Countermeasure Policy**タブをクリックします。

   Countermeasure Policyリストには、すべての対策ポリシーが表示されます。
4. Queryフィールドの右にある**Expand**アイコンをクリックします。
5. クエリー基準を設定します。
   - **Name**: 対抗策ポリシー名を入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
   - **AC**: 対策ポリシーが設定されているACを選択します。**All**を選択した場合、このフィールドはクエリー基準として使用されません。
6. **Query**をクリックします。

   対策ポリシーリストには、クエリー基準に一致するすべての対策ポリシーが表示されます。
7. クエリー基準をクリアしてすべての対策ポリシーを表示するには、**Reset**をクリックします。

対策方針の追加

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Virtual Security Domain**を選択します。
3. **Countermeasure Policy**タブをクリックします。

   Countermeasure Policyリストには、すべての対策ポリシーが表示されます。
4. **Add**をクリックします。
5. 対策ポリシー情報を設定します。
   - **Name**: 対抗措置ポリシーの名前を1～32文字の範囲で入力します。名前には、文字、数字、および下線を使用できます。
   - **AC**: 対抗措置ポリシーを作成するACを選択します。
   - **Enable Countermeasures on a Fixed Channel**: このオプションを選択すると、固定チャネルでの対策が有効になります。この機能を有効にすると、センサーは、対策が成功するまで、デバイスが存在するチャネル上のワイヤレスデバイスに対して継続的に対策を実行します。
   - **Select All**: すべての対策項目を有効にするには、このオプションを選択します。
   - **Configure countermeasure items**: 必要な対策項目またはすべての対策項目を有効にし、対策項目の優先度を0～9の範囲で設定します。値が大きいほど優先度が高くなります。ワイヤレスデバイスを検出すると、センサーは常に優先度の高いワイヤレスデバイスに対して対策を実行します。優先度が同じ場合、センサーはワイヤレスデバイスが静的な対策リストに追加された順序で対策を実行します。
6. **OK**をクリックします。

対策方針の変更

仮想セキュリティドメインにバインドされている対策ポリシーは変更できます。対策ポリシーを変更す

るには、次の手順を実行します:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Virtual Security Domain**を選択します。
3. **Countermeasure Policy**タブをクリックします。

   Countermeasure Policyリストには、すべての対策ポリシーが表示されます。
4. 変更する対抗措置ポリシーの**Operation**アイコン ... をクリックしてショートカットメニューから変更します。

   ACおよび対策ポリシー名は変更できません。他のパラメーターを変更する方法の詳細については、「対策ポリシーの追加」を参照してください。
5. OKをクリックします。

対策ポリシーの削除

デフォルトの対策ポリシーおよび仮想セキュリティドメインにバインドされている対策ポリシーは削除できません。仮想セキュリティドメインにバインドされている対策ポリシーを削除するには、最初にバインドを削除してください。

対策ポリシーを削除するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Virtual Security Domain**を選択します。
3. **Countermeasure Policy**タブをクリックします。

   Countermeasure Policyリストには、すべての対策ポリシーが表示されます。
4. 1つまたは複数の対抗措置ポリシーをバッチで削除します。
   - 削除する対抗措置ポリシーの**Operation**アイコン ･･･をクリックします。
   - 削除する対抗措置ポリシーを選択して、**Delete**.をクリックします。
5. 確認ダイアログボックスで、OKをクリックします。

仮想セキュリティドメインの構成

WLANは、ロケーションとセキュリティ要件に基づいて複数の仮想セキュリティドメインに分割できます。

たとえば、ある企業に4階建ての建物があるとします。各階にWLANを監視するセンサーがある場合は、各階にセキュリティドメインを設定できます。

セキュリティ要件の異なる複数のWLANを監視する2つのセンサーがフロアにある場合は、次の操作を実行できます。

- センサーを2つの仮想セキュリティドメインにバインドします。
- セキュリティドメインに異なるAPカテゴリ化規則と攻撃検出ポリシーを設定します。

仮想セキュリティドメインリストの表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Virtual Security Domain**を選択します。
3. **Virtual Security Domain**タブをクリックします。

   仮想セキュリティドメインリストには、すべての仮想セキュリティドメインが表示されます。

仮想セキュリティドメインリスト

- **Name**: 仮想セキュリティドメインの名前。仮想セキュリティドメインの名前をクリックすると、その詳細が表示されます。
- **Attack Detection Policy**: 仮想セキュリティドメインにバインドされているアタック検出ポリシーの名前。
- **Countermeasure Policy**: 仮想セキュリティドメインにバインドされている対策ポリシーの名前。
- **Signature Policy**: 仮想セキュリティドメインにバインドされている署名ポリシーの名前。
- **AC**: 仮想セキュリティドメインが構成されているACのラベル。ACのラベルをクリックすると、その詳細が表示されます。
- **Operation**: 仮想セキュリティドメインの**Operation**アイコン をクリックして、**Operation**メニューを表示します。

仮想セキュリティドメインリストに十分な数のエントリーが含まれている場合は、以下のナビゲーションガイドが表示されます。

- **Next Page**アイコンをクリックして、**virtual security domain**リスト内で次のページに進みます。
- **Last Page**アイコンをクリックすると、**virtual security domain**リストの最後に進むことができます。
- **Previous Page**アイコンをクリックすると、**virtual security domain**リスト内のページが逆方向に表示されます。
- **First Page**アイコンをクリックして、**virtual security domain**リストの先頭に戻ります。

virtual security domainリストの右上にある**8**、**15**、**50**、**100**、または**200**をクリックして、各ページに表示する項目数を指定します。

注:

仮想セキュリティドメインリストは、Operationフィールド以外のすべてのフィールドでソートできます。選択したフィールドでリストをソートするには、列ラベルをクリックします。列ラベルを使用すると、各フィールドに固有のソートオプションを切り替えることができます。

仮想セキュリティドメインリストの同期

IMCは、仮想セキュリティドメインリストの自動または手動による同期化をサポートします。デフォルトでは、IMCは仮想セキュリティドメインリストを2時間ごとに自動的に同期化します。

仮想セキュリティドメインリストを手動で同期するには、以下の手順に従ってください。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>WIPS Management>Virtual Security Domain**を選択します。
3. **Virtual Security Domain**タブをクリックします。

   仮想セキュリティドメインリストには、すべての仮想セキュリティドメインが表示されます。
4. **Synchronize**をクリックして、仮想セキュリティドメインリストの同期化を開始します。

   同期プロセスが完了すると、ページがリフレッシュされ、最新のデータが表示されます。

仮想セキュリティドメインのクエリー

基本問合せを実行する手順は、次のとおりです。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Virtual Security Domain**を選択します。
3. **Virtual Security Domain**タブをクリックします。

   仮想セキュリティドメインリストには、すべての仮想セキュリティドメインが表示されます。
4. 右上隅のQueryフィールドに、仮想セキュリティドメインの名前の一部または全体を入力します。
5. **Query**アイコンをクリックします。仮想セキュリティドメインリストに、問合せ基準に一致するすべての仮想セキュリティドメインが表示されます。
6. **Query**フィールドの選択を解除し、**Query**アイコンをクリックしてすべての仮想セキュリティドメインを表示します。拡張問合せを実行するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Virtual Security Domain**を選択します。
3. **Virtual Security Domain**タブをクリックします。

   仮想セキュリティドメインリストには、すべての仮想セキュリティドメインが表示されます。
4. Queryフィールドの右にある**Expand**アイコンをクリックします。
5. クエリー基準を設定します。
   - **Name**: 仮想セキュリティドメイン名を入力します。
   - **AC**: セキュリティドメインが構成されているACを選択します。**All**を選択した場合、このフィールドは問合せ基準として使用されません。
6. **Query**アイコンをクリックします。仮想セキュリティドメインリストに、問合せ基準に一致するすべての仮想セキュリティドメインが表示されます。
7. Queryフィールドをクリアして**Query**アイコンをクリックすると、すべての仮想セキュリティドメインが表示されます。

仮想セキュリティドメインの追加

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Virtual Security Domain**を選択します。
3. **Virtual Security Domain**タブをクリックします。

   仮想セキュリティドメインリストには、すべての仮想セキュリティドメインが表示されます。
4. **Add**をクリックします。

   Add Virtual Security Domainページが開きます。
5. 仮想セキュリティドメインの次のパラメーターを構成します。
   - **Name**: 仮想セキュリティドメインの名前を1から32文字の文字列で入力します。有効な文字は、整数、文字およびアンダースコア(_)です。
   - **AC**: 仮想セキュリティドメインの展開先となるACを選択します。
   - **Attack Detection Policy**: 攻撃検出ポリシーを選択します。1つの仮想セキュリティドメインに含めることができる攻撃検出ポリシーは1つだけです。仮想セキュリティドメインは、デフォルトではデフォルトの攻撃検出ポリシーにバインドされます。
   - **Countermeasure Policy**: 対策ポリシーを選択します。仮想セキュリティドメインは、デフォルトではデフォルトの対策ポリシーにバインドされます。

- **Signature Policy**: シグニチャポリシーを選択します。仮想セキュリティドメインは、デフォルトでデフォルトのシグニチャポリシーにバインドされます。

6. APカテゴリ化規則を仮想セキュリティドメインにバインドします。
   a. AP Categorization Rule領域で、**Select**をクリックします。

      AP Categorization Ruleウィンドウが開きます。
   b. 1つまたは複数のAPカテゴリ化規則を選択します。
   c. **OK**をクリックします。

      選択したAP分類ルールが**AP Categorization Rule List**に表示されます。
      - **Name**: AP分類ルールの名前。
      - **Threat Level**: AP分類ルールの脅威レベル。脅威レベルが設定されていない場合は、フィールドに -- が表示されます。
      - **Match Priority**: APカテゴリ化ルールのプライオリティを入力するか、**Move up**アイコン 又は**Move down**アイコン で優先順位を調整します。

        特定のAPカテゴリ化規則を仮想セキュリティドメインにバインドしない場合は、規則を選択して**Delete**をクリックします。
7. **Sensor**を選択して、センサーを仮想セキュリティドメインにバインドします。
   a. **Sensor List**領域で**Select**をクリックします。**Sensor**ウィンドウが開きます。
   b. 1つまたは複数のセンサーを選択します。
   c. **OK**をクリックします。

      選択したセンサーが**Sensor List**に表示されます。

   センサーリスト
   - **Status**:センサーのステータス。 Onlineおよび Offline。
   - **AP Label**: センサーのラベル。

   特定のセンサーを仮想セキュリティドメインにバインドしない場合は、センサーを選択して**Delete**をクリック。
8. OKをクリックします。

   Resultページが開き、結果リストに操作結果が表示されます。

   結果リスト
   - **Configuration Item**: 構成の説明。
   - **Configuration Item Details**: 構成の詳細。
   - **Configuration Result**: 構成の実行結果。
9. **OK**をクリックします。

仮想セキュリティドメインの変更

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Virtual Security Domain**を選択します。
3. **Virtual Security Domain**タブをクリックします。

   仮想セキュリティドメインリストには、すべての仮想セキュリティドメインが表示されます。
4. 変更する仮想セキュリティドメインの**Operation**アイコンをクリックしてショートカットメニューから**Modify**を選択します。

   仮想セキュリティドメインを変更するためのページが開きます。

5. 仮想セキュリティドメインのパラメーターを変更します。

   仮想セキュリティドメインおよびACの名前は変更できません。他のパラメーターの構成の詳細は、「仮想セキュリティドメインの追加」を参照してください。

仮想セキュリティドメインの削除

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Virtual Security Domain**を選択します。
3. **Virtual Security Domain**タブをクリックします。

   仮想セキュリティドメインリストには、すべての仮想セキュリティドメインが表示されます。
4. 1つの仮想セキュリティドメインまたは複数の仮想セキュリティドメインをバッチで削除します。
   - 削除する仮想セキュリティドメインを選択し、**Delete**をクリックします。
   - 削除する仮想セキュリティドメインの**Operation**アイコン…をクリックしてショートカットメニューの**Delete**をクリック。
5. 確認ダイアログボックスで、**OK**をクリックします。

WIPS動的検出情報

WSMは、Comware 5およびComware 7ワイヤレスデバイスのWIPS動的検出情報を表示および管理します。

WSMは、次のリストにあるすべての管理対象Comware 5 ACから収集された動的検出情報を要約します。

- 検出されたチャネルリスト
- 信頼できるアドレス一覧
- アラーム無視アドレス一覧
- ブロックするアドレス一覧
- 対策アドレス一覧

WIPSは、Comware 7ワイヤレスデバイスに関する次の攻撃情報を監視および収集します。

- **Classification information**: セキュリティレベル別にAPおよびクライアントを識別および分類します。AP分類の詳細については、「検出されたAP」を参照してください。クライアント分類の詳細については、「検出されたクライアントのリスト」を参照してください。
- **Countermeasure information**: 不正セキュリティを保護するために、不正なデバイスを無効にし、他のデバイスが不正なデバイスに関連付けられないようにするために取られる対策。
- **Unauthorized proxy**: 不正なプロキシ情報を検出し、イントラネットのセキュリティを保護するための対策を行います。
- **Attack detection**: センサーによって検出されたネットワーク攻撃の種類を提供します。

検出されたチャネルリスト

Detected Channel Listには、センサーによって検出されたチャネルと、そのチャネルが許可されているかどうかが表示されます。

センサーが検出できるのは、国番号または地域番号でサポートされているチャネルだけです。

検知したチャンネル一覧の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Dynamic Detection Information**を選択します。
3. **V5 Device**を選択します。
4. **Detected Channel List**タブをクリックします。

   Detected Channel Listには、検出されたすべてのチャネルが表示されます

   検出されたチャネルリスト

   - **Channel Number**: チャネル番号。
   - **Radio Type**: チャネルで動作する無線のタイプ。オプションは、802.11a、802.11b、802.11g、802.11gn、または802.11anです。
   - **Last Detection Time**: チャネルが最後に使用中であることが検出された時刻。
   - **Permitted Channel**: チャネルが許可されているかどうか(YesまたはNo)。
   - **Detecting AC**: チャネルを検出したセンサーが関連付けられているACのラベル。ACラベルをクリックすると、その詳細が表示されます。
5. **Detected Channel List**に十分な数のエントリーがある場合は、次のナビゲーションツールが表示されます。
   - **Next Page**アイコンをクリックして、**Detected Channel List**で次のページに進みます。
   - **Last Page**アイコンをクリックすると、**Detected Channel List**の最後のページに移動します。
   - **Previous Page**アイコンをクリックすると、**Detected Channel List**内で前のページに戻ります。
   - **First Page**アイコンをクリックすると、**Detected Channel List**の先頭にページバックします。
6. リストの右上にある**8**、**15**、**50**、**100**、または**200**をクリックして、各ページに表示する項目数を指定します。

注:

Detected Channel Listは、Channel Number、Radio Type、Last Detection Time、およびDetecting ACフィールドでソートできます。選択したフィールドでリストをソートするには、列ラベルをクリックします。列ラベルを使用すると、各フィールドに固有のさまざまなソートオプションを切り替えることができます。

ACから検出されたチャネル情報の同期化

デフォルトでは、IMCは管理対象ACからの最新のチャネル情報を2時間ごとに同期化します。手動で同期化操作を実行することもできます。

検出されたチャネル情報を管理対象ACからIMCに手動で同期化するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Dynamic Detection Information**を選択します。
3. **V5 Device**を選択します。
4. **Detected Channel List**タブをクリックします。

Detected Channel Listには、検出されたすべてのチャネルが表示されます

5. **Synchronize**をクリックします。

   同期プロセスが完了すると、ページが更新され、最後に検出されたチャネルアドレスリストが表示されます。

検出されたチャネルリスト上のチャネルの照会

基本問合せを実行する手順は、次のとおりです。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Dynamic Detection Information**を選択します。
3. **V5 Device**を選択します。
4. **Detected Channel List**タブをクリックします。

   Detected Channel Listには、検出されたすべてのチャネルが表示されます
5. 問合せフィールドの横にラジオタイプを入力します。WSMは、このフィールドのファジーマッチングをサポートします。
6. **Query**アイコンをクリックします。**Detected Channel List**に、クエリー基準に一致するすべてのチャネルが表示されます。
7. **Query**フィールドをクリアして**Query**アイコンをクリックすると、すべてのチャネルが表示されます。

拡張問合せを実行する手順は、次のとおりです。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Dynamic Detection Information**を選択します。
3. **Detected Channel List**タブをクリックします。

   Detected Channel Listには、検出されたすべてのチャネルが表示されます
4. **Query**フィールドの右にある**Expand**アイコンをクリックします。
5. **Query Criteria**領域で、次の問合せ条件を1つ以上指定します。
   - **Radio Type**: リストから無線タイプを選択します。オプションは、**802.11a**、**802.11b**、**802.11g**、**802.11gn**、および**802.11an**です。
   - **AC**: チャネルを検出するセンサーが関連付けられているACを選択します。
6. **Query**をクリックします。

   Detection Channel Listに、クエリー基準に一致するすべてのチャネルが表示されます。
7. クエリー基準をクリアしてすべてのチャネルを表示するには、**Reset**をクリックします。

信頼できるアドレス一覧

Trusted Address Listには、各ACのStatic Trusted Address Listで手動で指定された信頼できるAPとクライアント、およびWIPSによって検出された信頼できるクライアントを含む、各ACの信頼できるアドレスリスト上のすべての信頼できるデバイスが表示されます。

信頼できるアドレス一覧の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Dynamic Detection Information**を選択します。

3. **V5 Device**を選択します。
4. 信頼されたアドレス一覧タブをクリックします。

   Trusted Address Listには、すべての信頼できるデバイスのMACアドレスが表示されます。

   信頼されたアドレス一覧

   - **MAC Address**: 信頼できるデバイスのMACアドレス。
   - **Address Type**: 信頼できるアドレスのタイプ。
     - **Static**: 信頼できるアドレスがACの信頼できるアドレスリストに手動で追加され、センサーがデバイスを検出していないことを示します。
     - **Dynamic**: 信頼できるアドレスが信頼できるアドレスリストにないが、センサーがデバイスを検出したことを示します。
     - **Static and Dynamic**: 信頼できるアドレスが信頼できるアドレスリストにあり、センサーがデバイスを検出したことを示します。
   - **Detecting AC**: Address Typeが**Static**の場合、このフィールドには、そのアドレスが属する**Trusted Address List**を持つACのデバイスラベルが表示されます。**Address Type**が**Dynamic**または**Static and Dynamic**の場合、検出された信頼できるデバイスはクライアントであり、このフィールドには、クライアントを検出したACのデバイスラベルが表示されます。詳細を表示するには、ACラベルをクリックします。
   - **Operation**: **Operation**アイコン ⋯をクリックすると、**Operation**メニューが表示されます。このメニューには、信頼できるデバイスを信頼できるアドレスリストから削除するためのオプションがあります。

   信頼できるアドレス一覧に十分な数のエントリーがある場合は、次のナビゲーションツールが表示されます。

   - **Next Page**アイコンをクリックして、**Trusted Address List**でページを進めます。
   - **Last Page**アイコンをクリックして、**Trusted Address List**の最後のページに進みます。
   - **Previous Page**アイコンをクリックすると、**Trusted Address List**のページが逆方向に表示されます。
   - **First Page**アイコンをクリックして、**Trusted Address List**の先頭に戻るページを表示します。
5. リストの右上にある**8**、**15**、**50**、**100**、または**200**をクリックして、各ページに表示する項目数を指定します。

注:

信頼できるアドレス一覧は、MACアドレス、アドレスの種類、および検出されたACの各フィールドで並べ替えることができます。列ラベルをクリックすると、選択したフィールドで一覧が並べ替えられます。列ラベルを使用すると、各フィールドに固有のさまざまな並べ替えオプションを切り替えることができます。

信頼できるアドレスの同期

デフォルトでは、IMCは管理対象ACからのスタティック信頼アドレスリストを2時間ごとに同期します。手動で同期操作を実行することもできます。

管理対象ACからスタティック信頼アドレスリストを手動で同期化するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Dynamic Detection Information**を選択します。
3. **V5 Device**を選択します。

4. **Trusted Address List**タブをクリックします。

   Trusted Address Listには、すべての信頼できるAPおよびクライアントのMACアドレスが表示されます。

5. **Synchronize**をクリックします。

   同期プロセスが完了すると、ページが更新され、最新の信頼できるアドレスリストが表示されます。

信頼できるアドレスの照会

基本問合せを実行する手順は、次のとおりです。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Dynamic Detection Information**を選択します。
3. **V5 Device**を選択します。
4. **Trusted Address List**タブをクリックします。

   Trusted Address Listには、すべての信頼できるデバイスのMACアドレスが表示されます。

5. Queryフィールドの横に信頼できるアドレスを入力します。WSMは、このフィールドのファジーマッチングをサポートしています。
6. **Query**アイコンをクリックします。信頼できるアドレスリストに、問合せ基準に一致するすべての信頼できるアドレスが表示されます。
7. **Query**フィールドを消去して**Query**アイコンをクリックすると、すべての信頼できるアドレスが表示されます。

拡張問合せを実行する手順は、次のとおりです。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Dynamic Detection Information**を選択します。
3. **Trusted Address List**タブをクリックします。

   Trusted Address Listには、すべての信頼できるデバイスのMACアドレスが表示されます。

4. **Query**フィールドの右にある**Expand**アイコンをクリックします。
5. **Query criteria**領域で、次の1つ以上のクエリー基準を指定します。
   - **MAC Address**: MACアドレスの一部または全体をxx:xx:xx:xx:xx:xx形式で入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
   - **Address Type**: デバイスタイプを選択します。オプションは、All、Static、Dynamic、Static and Dynamicです。
   - **AC**: Static Trusted Device Listを照会するACを選択します。
6. **Query**をクリックします。

   Trusted Address Listには、問合せ基準に一致するすべての信頼できるアドレスが表示されます。
   Resetをクリックし、クエリー基準をクリアし、すべての信頼できるアドレスを表示します。

信頼できるアドレス一覧から信頼できるアドレスを削除する

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Dynamic Detection Information**を選択します。
3. **V5 Device**を選択します。
4. **Trusted Address List**タブをクリックします。

Trusted Address Listには、すべての信頼できるデバイスのMACアドレスが表示されます。

5. 削除する信頼できるアドレスの**Operation**アイコン ··· をクリックします。
6. ショートカットメニューから**Delete from Static Trusted Address List**を選択します。
7. 確認ダイアログボックスで、**OK**をクリックします。

アラーム無視アドレス一覧

Alarm-Ignored Address Listには、各ACの**Alarm-Ignored Address List**上のアラームで無視されたデバイスに関する情報がMACアドレス別に表示されます。この情報には、アドレスが最初に検出された時刻と最後に検出された時刻、デバイスによって生成されたアラームが無視された回数、検出したACなどが含まれます。

アラーム無視アドレス一覧を表示する

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Dynamic Detection Information**を選択します。
3. **V5 Device**を選択します。
4. **Alarm Ignored Address List**タブをクリックします。

   Alarm Ignored Address Listには、アラームが無視されたすべてのアドレスが表示されます。

   アラーム無視アドレス一覧

   - **MAC Address**: アラームが無視されたデバイスのMACアドレス。
   - **First Detection Time**: アドレスがワイヤレスネットワークで最初に検出された時刻。アドレスが検出されなかった場合、このフィールドには2つの連続したハイフン(--)が表示されます。
   - **Last Detection Time**: アドレスが無線ネットワークで最後に検出された時刻。アドレスが検出されなかった場合、このフィールドには2つの連続したハイフン(--)が表示されます。
   - **Alarm Ignoring Count**: デバイスによって生成されたアラームが無視された回数。数値が0の場合、このフィールドには2つの連続したハイフン(--)が表示されます。
   - **Detecting AC**: アドレスを検出したセンサーが関連付けられているACのデバイスラベル。ACラベルをクリックすると、その詳細が表示されます。
   - **Operation**: **Operation**アイコンをクリックすると、**Operation**メニュー ···が表示されます。このメニューには、アラームが無視されたデバイスを**Alarm Ignored Address List**から削除するためのオプションがあります。

アラーム無視アドレス一覧に十分な数のエントリーがある場合は、次のナビゲーションツールが表示されます。

- **Next Page**アイコンをクリックして、**Alarm Ignored Address List**のページを進めます。
- **Last Page**アイコンをクリックして、**Alarm Ignored Address List**の最後のページに進みます。
- **Previous Page**アイコンをクリックすると、**Alarm Ignored Address List**のページが逆方向に表示されます。
- **First Page**アイコンをクリックして、**Alarm Ignored Address List**の先頭にページバックします。

リストの右上にある**8**、**15**、**50**、**100**、または**200**をクリックして、各ページに表示する項目数を指定します。

注:

Alarm Ignored Address Listは、**MAC Address**、**First Detection Time**、**Last Detection Time**、**Alarm Ignored Count**および**AC Detected AC**フィールドでソートできます。列ラベルをクリックすると、選択したフィール

ドでリストをソートできます。列ラベルを使用すると、各フィールドに固有の様々なソートオプションを切り替えることができます。

アラーム無視アドレスの同期

デフォルトでは、IMCは管理対象ACからのアラーム無視アドレスリストを2時間ごとに同期します。手動で同期操作を実行することもできます。

管理対象ACからアラーム無視アドレスリストを手動で同期化するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Dynamic Detection Information**を選択します。
3. **V5 Device**を選択します。
4. **Alarm Ignored Address List**タブをクリックします。

   Alarm Ignored Address Listには、アラームで無視されたすべてのデバイスが表示されます。
5. **synchronize**.をクリックします。

   同期プロセスが完了すると、ページがリフレッシュされ、最新のアラーム無視アドレスリストが表示されます。

アラームが無視されたアドレスの問い合わせ

基本問合せを実行する手順は、次のとおりです。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Dynamic Detection Information**を選択します。
3. **V5 Device**を選択します。
4. **Alarm Ignored Address List**タブをクリックします。

   アラーム無視アドレス一覧には、アラームが無視されたすべてのアドレスが表示されます。
5. 問合せフィールドの横に、アラームが無視されたアドレスを入力します。WSMは、このフィールドのファジーマッチングをサポートします。
6. **Query**アイコンをクリックします。**Alarm Ignored Address List**には、問合せ基準に一致するアラーム無視アドレスがすべて表示されます。
7. **Query**フィールドの選択を解除し、**Query**アイコンをクリックして、すべてのアラーム無視アドレスを表示します。

拡張問合せを実行する手順は、次のとおりです。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Dynamic Detection Information**を選択します。
3. **Alarm Ignored Address List**タブをクリックします。

   アラーム無視アドレス一覧には、アラームが無視されたすべてのアドレスが表示されます。
4. **Query**フィールドの右にある**Expand**アイコンをクリックします。
5. **Query Criteria**領域で、次の問合せ基準のいずれかまたは両方を指定します。
   - **MAC Address**: MACアドレスの一部または全体をxx:xx:xx:xx:xx:xx形式で入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
   - **AC**: **Alarm Ignored Address List**を照会するACを選択します。
6. **Query**をクリックします。

Alarm Ignored Address Listには、問合せ基準に一致するすべてのアラームが無視されたアドレスが表示されます。問合せ基準を消去してすべてのアラームが無視されたアドレスを表示するには、Resetをクリック

アラーム無視アドレス一覧からアドレスを削除する

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Dynamic Detection Information**を選択します。
3. **V5 Device**を選択します。
4. **Alarm Ignored Address List**タブをクリックします。

   Alarm Ignored Address Listには、アラームで無視されたすべてのデバイスが表示されます。
5. 削除するアラーム無視アドレスの**Operation**アイコン･･･ をクリックします。
6. ショートカットメニューから**Delete from Alarm Ignored Address List**を選択します。
7. 確認ダイアログボックスで、**OK**をクリックします。

ブロックするアドレス一覧

Blocked Address Listには、各ACのStatic-Blocked Address List上のブロックされたデバイスに関する情報がMACアドレス別に表示されます。この情報には、アドレスタイプ(アドレスがネットワーク内で検出されたかどうか)および検出中のACが含まれます。

禁止アドレス一覧を表示する

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Dynamic Detection Information**を選択します。
3. **V5 Device**を選択します。
4. ブロックするアドレス一覧タブをクリックします。

   ブロックされたアドレス一覧には、ブロックされたすべてのアドレスが表示されます。

   ブロックするアドレス一覧
   - **MAC Address**: ブロックされたデバイスのMACアドレス。
   - **Address Type**: ブロックされたデバイスのタイプ。
     - **Static**: ブロックされたアドレスがACの**Blocked Address List**に手動で追加されているが、センサーがデバイスを検出していないことを示します。
     - **Dynamic**: ブロックされたアドレスがブロックされたアドレスリストにないが、センサーがデバイスを検出したことを示します。
     - **Static and Dynamic**: ブロックされたアドレスがブロックされたアドレスリストにあり、センサーがデバイスを検出したことを示します。
   - **Detecting AC**: **Address Type**が**Static**の場合、このフィールドには、アドレスが属する**Blocked Address List**のACのデバイスラベルが表示されます。**Address Type**が**Dynamic**またはStatic and Dynamicの場合、このフィールドには、アドレスを検出したセンサーが関連付けられているACのデバイスラベルが表示されます。ACラベルをクリックすると、その詳細が表示されます。
   - **Operation**: **Operation**アイコン･･･ をクリックすると、**Operation**メニューが表示されます。このメニューには、ブロックされたデバイスを**Blocked Address List**から削除するためのオプションがあります。

ブロックされたアドレス一覧に十分な数のエントリーがある場合は、次のナビゲーションツールが表示されます。

- **Next Page**アイコンをクリックして、**Blocked Address List**内で次のページに
- **Last Page**アイコンをクリックして、**Blocked Address List**の最後のページに進みます。
- **Previous Page**アイコンをクリックして、**Blocked Address List**内で前のページ
- **First Page**アイコンをクリックして、**Blocked Address List**の先頭に戻るページを表示します。

5. リストの右上にある**8**、**15**、**50**、**100**、または**200**をクリックして、各ページに表示する項目数を指定します。

注:

Blocked Address Listは、**MAC Address**、**Address Type**および**Detected AC**フィールドでソートできます。選択したフィールドでリストをソートするには、列ラベルをクリックします。列ラベルを使用して、各フィールドに固有の様々なソートオプションを切り替えることができます。

ブロックされたアドレスの同期

デフォルトでは、IMCは管理対象ACからのスタティックブロックアドレスリストを2時間ごとに同期します。手動で同期操作を実行することもできます。

ブロックされたアドレスを同期するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Dynamic Detection Information**を選択します。
3. **V5 Device**を選択します。
4. **Blocked Address List**タブをクリックします。

   Blocked Address Listには、ブロックされたすべてのアドレスが表示されます。
5. **Synchronize**をクリックします。

   同期プロセスが完了すると、ページがリフレッシュされ、最新のブロックされたアドレスリストが表示されます。

ブロックされたアドレスのクエリー

基本問合せを実行する手順は、次のとおりです。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Dynamic Detection Information**を選択します。
3. **V5 Device**を選択します。
4. **Blocked Address List**タブをクリックします。

   Blocked Address Listには、ブロックされたすべてのアドレスが表示されます。
5. Queryフィールドの横にブロックされたアドレスを入力します。WSMは、このフィールドのファジーマッチングをサポートします。
6. **Query**アイコンをクリックします。**Blocked Address List**に、問合せ基準に一致するすべてのブロック済所在地が表示されます。
7. **Query**フィールドを消去し、**Query**アイコンをクリックして、すべてのブロックされた所在地を表示し

ます。拡張問合せを実行する手順は、次のとおりです。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Dynamic Detection Information**を選択します。
3. **Blocked Address List**をクリックします。

   Blocked Address Listには、ブロックされたすべてのアドレスが表示されます。
4. **Query**フィールドの右にある**Expand**アイコンをクリックします。
5. **Query Criteria**領域で、次の1つ以上のクエリー基準を指定します。
   - **MAC Address**: MACアドレスの一部または全体をxx:xx:xx:xx:xx:xx:xx形式で入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
   - **Address Type**: リストからアドレスタイプを選択します。オプションは**All**、**Static**、**Dynamic**、**Static** と **Dynamic**です。
   - **AC**: Static Blocked Address Listを照会するACを選択します。
6. **Query**をクリックします。

   Blocked Address Listには、問合せ基準に一致するすべてのブロック済アドレスが表示されます。**Reset**をクリックして、クエリー基準をクリアして、ブロックされたすべてのアドレスを表示します。

静的ブロックアドレス一覧からのアドレスの削除

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Dynamic Detection Information**を選択します。
3. **V5 Device**を選択します。
4. **Blocked Address List**タブをクリックします。

   Blocked Address Listには、ブロックされたすべてのアドレスが表示されます。
5. 削除するブロックアドレスの**Operation**アイコン をクリックし、ショートカットメニューから**Delete from Static Blocked Address List**を選択します。
6. 確認ダイアログボックスで、**OK**をクリックします。

対策アドレス一覧

Countermeasures Address Listには、対策を実施した機器やその状態、その他の対策情報が表示されます。

Countermeasures Address Listには、リストに手動で追加されたデバイスと、WIPSによって検出されたデバイスが含まれています。リスト内のデバイスに対して、WIPSは、センサーがそれらを検出する限り、それらに対して対抗措置を実行します。WIPSによって検出されたデバイスに対して、WIPSは、APの分類規則、スタティックな信頼アドレスリスト、スタティックに信頼されたOUIリスト、およびスタティックにブロックされたアドレスリストに従ってデバイスを分類します。その後、デバイスタイプが事前定義された対抗措置ポリシーと一致する場合、WIPSはデバイスに対して対抗措置を実行します。

対策アドレス一覧画面の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Dynamic Detection Information**を選択します。
3. **V5 Device**を選択します。

4. **Countermeasures Address List**タブをクリックします。

   Countermeasures Address Listには、すべての対策アドレスが表示されます。

   対策アドレス一覧

   - **MAC Address**: 対策が実行されるデバイスのMACアドレス。
   - **Virtual Security Domain**: **Static**デバイスの場合、このカラムにはデバイスが属する仮想ドメイン名が表示されます。**Static**デバイスの場合、このカラムにはデバイスを検出したセンサーが属する仮想ドメインが表示されます。
   - **Type**: 対抗措置の対象となるデバイスのタイプ。オプションは次のとおりです。
     静的、動的、および静的と動的。
     - **Static**: デバイスはスタティックな対策アドレスリストに含まれていますが、センサーによって検出されていません。
     - **Dynamic**: デバイスがセンサーによって検出され、WIPSがデバイスに対して対策を実行します。
     - **Static and Dynamic**: デバイスはスタティックな対策アドレスリストにあり、センサーによって検出されています。WIPSはデバイスに対して対策を実行します。
   - **Status**: デバイスの現在の状態。オプションは**Countermeasure**、**Idle**および**Pending**です。
     - **Countermeasure**: デバイスに対して対策がとられています。
     - **Idle**: デバイスは対策アドレスリストに手動で追加されていますが、センサーがデバイスを検出していません。
     - **Pending**: WIPSが対抗措置を取るデバイス。
   - **Start Time**: WIPSがデバイスに対して初めて対策を実行した時刻。
   - **Category**: デバイスのカテゴリ。
   - **Channel**: デバイスが動作しているチャネル。センサーはこのチャネル上のデバイスに対して対策を実行します。
   - **Countermeasure Priority**: デバイスの対策優先度。対策ポリシーによって決定されます。**Category**フィールドが空の場合、このフィールドは空になります。
   - **AC**: **Static**デバイスの場合、この列には、デバイスが関連付けられているACのデバイスラベルが表示されます。**Dynamic**デバイスの場合、この列には、デバイスを検出したセンサーが関連付けられているACのデバイスラベルが表示されます。ラベルのリンクをクリックすると、AC管理ページが表示されます。

Countermeasures Address Listに十分なエントリーがある場合は、次のナビゲーションツールが表示されます。

-  **Next Page**アイコンをクリックして、**Countermeasures Address List**でページを進めます。
-  **Last Page**アイコンをクリックして、**Countermeasures Address List**の最後にページフォワードします。
-  **Previous Page**アイコンをクリックして、**Countermeasures Address List**で前のページに戻ります
-  **First Page**アイコンをクリックして、**Countermeasures Address List**の前にページを戻します。

リストの右上にある**8**、**15**、**50**、**100**、または**200**をクリックして、各ページに表示する項目数を指定します。

注:

Countermeasures Address Listは、すべてのフィールドで並べ替えることができます。列見出しをクリックすると、選択したフィールドで一覧が並べ替えられます。列見出しを使用すると、各フィールドに固有のさまざまな並べ替えオプションを切り替えることができます。

対策アドレスの同期

デフォルトでは、IMCは管理対象ACからのスタティックな対策アドレスリストを2時間ごとに同期します。手動で同期操作を実行することもできます。

管理対象ACからスタティックな対策アドレスリストを手動で同期化するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Dynamic Detection Information**を選択します。
3. **V5 Device**を選択します。
4. **Countermeasures Address List**タブをクリックします。

   Countermeasures Address Listには、すべての対策アドレスが表示されます。
5. **Synchronize**をクリックします。

   同期プロセスが完了すると、ページが更新され、最新の対策アドレスリストが表示されます。

対抗策アドレスの照会

基本問合せを実行する手順は、次のとおりです。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Dynamic Detection Information**を選択します。
3. **V5 Device**を選択します。
4. **Countermeasures Address List**タブをクリックします。

   Countermeasures Address Listには、すべての対策アドレスが表示されます。
5. 問合せフィールドの横に対策アドレスを入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
6. **Query**アイコンをクリックします。**Countermeasures Address List**に、問合せ基準に一致するすべての対抗措置所在地が表示されます。
7. **Query**フィールドを消去して**Query**アイコンをクリックすると、すべての対抗措置アドレスが表示されます。

拡張問合せを実行する手順は、次のとおりです。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Dynamic Detection Information**を選択します。
3. **V5 Device**を選択します。
4. **Countermeasures Address List**タブをクリックします。

   Countermeasures Address Listには、すべての対策アドレスが表示されます。
5. Queryフィールドの横にある**Expand**アイコンをクリックして、領域を展開します。
6. **Query Criteria**領域で、次の1つ以上のクエリー基準を指定します。
   - **MAC Address**: MACアドレスの一部または全体をxx:xx:xx:xx:xx:xx:xx形式で入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
   - **AC**: **Static Countermeasures Address List**を照会するACを選択します。
7. **Query**をクリックします。

   Countermeasures Address Listには、問合せ基準に一致するすべての対策アドレスが表示されます。問合せ基準を消去してすべての対策アドレスを表示するには、**Reset**をクリックします。

APおよびクライアント検出情報

WIPSは、検出されたAPおよびクライアントに関する分類情報を検出して提供します。

APおよびクライアント検出情報の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Detected Information**を選択します。
3. **V7 Device**を選択します。
4. **AP and Client Detection Information**タブをクリックして、**AP and Client Detection Information**ページを開きます。

   APおよびクライアント検出情報

   - **Virtual Security Domain**: APおよびクライアント情報を検出したセンサーの仮想セキュリティドメインの名前。
   - **Detecting AC**:センサーが搭載されているACのラベル。
   - **Detail**: 詳細なAPとクライアントの分類情報を表示するには、**Detail**リンクをクリックします。

APおよびクライアント検出情報のクエリー

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Detected Information**を選択します。
3. **V7 Device**を選択します。
4. **AP and Client Detection Information**タブをクリックして、**AP and Client Detection Information**ページを開きます。
5. 基本的なQueryを実行します。
   a. 仮想セキュリティドメイン名を入力します。WSMは、このフィールドのファジーマッチングをサポートしています。
   b. **Query**アイコンをクリックします。

      このページには、クエリー基準と一致する検出情報が表示されます。
   c. **Query**フィールドをクリアして**Query**アイコンをクリックすると、すべての検出情報が表示されます。
6. 高度なQueryを実行します。
   a. **Query**フィールドの横にある**Expand**アイコンをクリックして、**Query**領域を拡張します。
   b. 次の問合せ基準を1つ以上指定します。
      - **Detecting AC**: **Detecting AC**リストからACラベルを選択するか、**All**を選択します。WSMは、選択したACまたはすべてのACの検出情報を表示します。
      - **Virtual Security Domain**: 仮想セキュリティドメイン名を入力します。WSMは、このフィールドのファジーマッチングをサポートしています。

      空のフィールドは、Query条件として使用できません。
   c. **Query**をクリックします。

      このページには、クエリー基準と一致する検出情報が表示されます。
   d. **Reset**をクリックすると、クエリー基準がクリアされ、すべての検出情報が表示されます。

詳細なAPおよびクライアント検出情報の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Detected Information**を選択します。
3. **V7 Device**を選択します。
4. **AP and Client Detection Information**タブをクリックして、**AP and Client Detection Information**ページを開きます。
5. **Detail**リンクをクリックして、詳細なAPおよびクライアント検出情報ページを開きます。

   詳細なAPおよびクライアント検出情報

   - **Total APs**: 検出されたAPの合計数。
   - **Total Clients**: 検出されたクライアントの合計数。
   - **Authorized APs**: WLANで許可されているAPの合計数。
   - **Misconfigured APs**: WLANサービス設定が正しくなく、WLANで許可されているAPの合計数。
   - **Rogue APs**: WLANで使用できないAPの合計数。
   - **External APs**: 隣接WLAN内にあるAPの合計数。
   - **Ad Hoc APs**:アドホックモードで動作しているAPの合計数。
   - **Mesh APs**: メッシュネットワークを構築するAPの合計数。
   - **Potential-Authorized APs**: 許可される可能性のあるAPの合計数。
   - **Potential-Rogue APs**: 不正デバイスである可能性があるAPの合計数。
   - **Potential-External APs**: 外部ネットワークからの可能性があるAPの合計数。
   - **Uncategorized APs**: カテゴリを判別できないAPの合計数。
   - **Authorized Clients**: WLANで許可されているクライアントの数。
   - **Unauthorized Clients**: WLANで許可されていないクライアントの数。
   - **Misassociated Clients**: 許可されたデバイスリスト内にあるが、許可されていないAPに関連付けられているクライアントの数。
   - **Uncategorized Clients**: カテゴリを判別できないクライアントの合計数。
6. **Back**をクリックします。

APクライアント対策情報

WSMは、WIPSが対策を講じるAPおよびクライアントに関する情報を提供します。クライアントは、WIPSが対策を講じたAPに関連付けることはできません。

APおよびクライアントの対策情報の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Detected Information**を選択します。
3. **V7 Device**を選択します。
4. **AP and Client Countermeasurement Information**タブをクリックして、**AP and Client Countermeasurement Information**ページを開きます。

   APクライアント対策情報

   - **Virtual Security Domain**: センサーが存在する仮想セキュリティドメインの名前。

- **Detecting AC**: センサーが配置されているACのラベル。
- **Detail**: **Detail**リンクをクリックすると、APおよびクライアントの詳細な対策情報が表示されます。

APおよびクライアントの対策情報の照会

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Detected Information**を選択します。
3. **V7 Device**を選択します。
4. **AP and Client Countermeasurement Information**タブをクリックして、**AP and Client Countermeasurement Information**ページを開きます。
5. 基本的なQueryを実行します。
   a. 仮想セキュリティドメイン名を入力します。WSMは、このフィールドのファジーマッチングをサポートしています。
   b. **Query**アイコンをクリックします。
      このページには、クエリー基準と一致する対策情報が表示されます。
   c. **Query**フィールドの選択を解除し、**Query**アイコンをクリックすると、すべての対応策情報が表示されます。
6. 高度なQueryを実行します。
   a. **Query**フィールドの横にある**Expand**アイコンをクリックして、**Query**領域を拡張します。
   b. 次の問合せ基準を1つ以上指定します。
      - **Detecting AC**: **Detecting AC**リストからACラベルを選択するか、**All**を選択します。WSMは、選択したACまたはすべてのACの検出情報を表示します。
      - **Virtual Security Domain**: 仮想セキュリティドメイン名を入力します。WSMは、このフィールドのファジーマッチングをサポートしています。

      空のフィールドは、Query条件として使用できません。
   c. **Query**をクリックします。
      このページには、query criteriaと一致する対策情報が表示されます。
   d. クエリー基準をクリアしてすべての対応策情報を表示するには、**Reset**をクリックします。

APおよびクライアントの詳細な対策情報の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Detected Information**を選択します。
3. **V7 Device**を選択します。
4. **AP and Client Countermeasurement Information**タブをクリックして、**AP and Client Countermeasurement Information**ページを開きます。
5. **Detail**リンクをクリックして、APおよびクライアントの詳細な対策情報ページを開きます。

   APおよびクライアントの詳細な対策情報
   - **Total APs**: WIPS対策が実行されたAPの合計数。
   - **Total Clients**: WIPS対策が実行されたクライアントの合計数。
   - **Misconfigured APs**: WIPS対策が実行された設定ミスのあるAPの合計数。
   - **Rogue APs**: WIPS対策が実行された不正APの合計数。

- **External APs**: WIPS対策が実行された外部APの合計数。
- **Potential-Authorized APs**: WIPS対策が実行された潜在的認可APの合計数。
- **Potential-Rogue APs**: WIPS対策が実行された潜在的な不正APの合計数。
- **Potential-External APs**: WIPS対策が実行された外部APの合計数。
- **Uncategorized APs**: WIPS対策が実行された未分類のAPの合計数。
- **Authorized Clients**: WIPS対策が実行されている許可されたクライアントの数。
- **Misassociated Clients**: WIPS対策が実行された、誤関連付けされたクライアントの数。
- **Uncategorized Clients**: WIPS対策が実行された、分類されていないクライアントの合計数。
- **Attack Countermeasure Operations**: 対抗ポリシーに基づく動的対抗操作の合計数。
- **Manual Countermeasure Operations**: 手動対策操作の合計数。
- **Client Countermeasure Operations Caused by AP Countermeasure**: WIPS対策が実行されたAPに関連付けられているクライアント上の対策操作の合計数。

6. **Back**をクリックします。

不正プロキシ検出情報

WSMは、他のデバイスに不正な有線またはワイヤレスネットワークアクセスを提供する不正なプロキシデバイスを検出します。

不正なプロキシ検出情報の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Detected Information**を選択します。
3. **V7 Device**を選択します。
4. **Unauthorized Proxy Detection Information**タブをクリックして、**Unauthorized Proxy Detection Information**ページを開きます。

   不正プロキシ検出情報

   - **Client MAC**: 無許可プロキシのMACアドレス。
   - **First Detection Time**: 不正なプロキシが最初に検出された時刻。
   - **Last Detection Time**: 不正なプロキシが最後に検出された時刻。
   - **Duration(Seconds)**: 最初の検出時刻から最後の検出時刻までの期間(秒単位)。
   - **Detecting AC**: センサーが配置されているACのラベル。

不正プロキシ検出情報の問い合わせ

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Detected Information**を選択します。
3. **V7 Device**を選択します。
4. **Unauthorized Proxy Detection Information**タブをクリックして、**Unauthorized Proxy Detection Information**ページを開きます。
5. 基本的なQueryを実行します。
   a. MACアドレスを入力します。WSMは、このフィールドのファジーマッチングをサポートしています。

b. **Query**アイコンをクリックします。

このページには、query criteriaと一致する検出情報が表示されます。

c. **Query**フィールドをクリアして**Query**アイコンをクリックすると、すべての検出情報が表示されます。

6. 高度なQueryを実行します。

a. **Query**フィールドの横にある**Expand**アイコンをクリックして、**Query**領域を拡張します。

b. 次のquery criteriaを1つ以上指定します。

- **Detecting AC**: **Detecting AC**リストからACラベルを選択するか、**All**を選択します。WSMは、選択したACまたはすべてのACの検出情報を表示します。
- **Client MAC**: MACアドレスを入力します。WSMは、このフィールドのファジーマッチングをサポートします。空のフィールドは、クエリー条件として機能しません。

c. **Query**をクリックします。

このページには、query criteriaと一致する検出情報が表示されます。

d. **Reset**をクリックすると、クエリー基準がクリアされ、すべての検出情報が表示されます。

攻撃検出情報

センサーから報告された攻撃情報に基づいて、WSMはタイプ別の攻撃統計情報を提供し、管理者に通知するアラームを生成します。

攻撃検出情報の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Detected Information**を選択します。
3. **V7 Device**を選択します。
4. **Attack Detection Information**タブをクリックして、アタック検出情報ページを開きます。

攻撃検出情報

- **Sensor Name**: アタック情報を検出したセンサーの名前。
- **Detecting AC**: アタック情報を検出したセンサーのACのラベル。
- **Detail**: detailed attack detection informationを表示するにはDetailリンクをクリックします。

攻撃検出情報のクエリー

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Detected Information**を選択します。
3. **V7 Device**を選択します。
4. **Attack Detection Information**タブをクリックして、アタック検出情報ページを開きます。
5. 基本的なQueryを実行します。

a. センサー名を入力します。WSMは、このフィールドのファジーマッチングをサポートしています。

b. **Query**アイコンをクリックします。

このページには、クエリー基準と一致する攻撃検出情報が表示されます。

c. **Query**フィールドをクリアして**Query**アイコンをクリックすると、すべての攻撃検出情報が表示

されます。

6. 高度なQueryを実行します。
   a. **Query**フィールドの横にある**Expand**アイコンをクリックして、**Query**領域を拡張します。
   b. 次のquery criteriaを1つ以上指定します。
      - **Detecting AC**: **Detecting AC**リストからACラベルを選択するか、**All**を選択します。WSMは、選択したACまたはすべてのACのアタック検出情報を表示します。
      - **Sensor**: センサー名を入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。空のフィールドは、問合せ基準として使用されません。
   c. **Query**をクリックします。
      このページには、query criteriaと一致する攻撃検出情報が表示されます。
   d. **Reset**をクリックすると、query criteriaがクリアされ、すべての攻撃検出情報が表示されます。

詳細な攻撃検出情報の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Detected Information**を選択します。
3. **V7 Device**を選択します。
4. **Attack Detection Information**タブをクリックして、アタック検出情報ページを開きます。
5. Detailリンクをクリックして、詳細な攻撃検出情報ページを開きます。表43に、詳細な攻撃検出情報を示します。

表43 攻撃検出情報の詳細

攻撃検出名	備考
• アソシエーション要求のフラッド攻撃 • 認証要求のフラッド攻撃 • ビーコンフラッド攻撃 • ブロックAckフラッド攻撃 • CTS フラッド攻撃 • 認証解除フラッド攻撃 • Disassociation フラッド攻撃 • EAPOL-Startフラッド攻撃 • ヌルデータフラッド攻撃 • プローブ要求フラッド攻撃 • 再アソシエーション要求によるフラッド攻撃 • RTSフラッド攻撃 • EAPOL-Logoffフラッド攻撃 • EAP-Failure フラッド攻撃 • EAP-Successフラッド攻撃	フラッド攻撃です。 ワイヤレスデバイスは、短期間に同じタイプのフレームを大量に受信すると、フラッド攻撃を受ける可能性があります。次に例を示します。 • **Association request flood attack**: APにアソシエーション要求を送信する多数のクライアントを模倣して、APのアソシエーションテーブルをフラッドします。 • **Deauthentication flood attack**: APからアソシエートされたクライアントに送信される認証解除フレームをスプーフィングして、クライアントとAPのアソシエーションを解除します。 • **Null data flood attack**: クライアントからAPに送信されるヌルデータフレームをスプーフィングします。APはクライアントが省電力モードであることを確認し、クライアントのためにフレームをバッファします。エージングタイムが経過すると、APはバッファされたフレームを破棄します。これにより、クライアントとAPとの通信が中断されます。
• IEが重複している不正な形式のパケット • FATA-Jack不正な形式のパケット • 異常なIBSSおよびESS設定を持つ不正な形式のパケット	不正な形式のパケット攻撃です。 不正な形式のパケットは、クライアントプロセッサをクラッシュさせる可能性があります。次に例を示します。

攻撃検出名	備考
• 不正な送信元アドレスを持つ不正な形式のパケット • 不正なアソシエーション要求パケット • 不正な形式の認証要求パケット • 不正な認証解除コードを含む不正な形式のパケット • 無効なアソシエーション解除コードを持つ不正な形式のパケット • 無効なHT IEを含む不正な形式のパケット • 不正なIE長を持つ不正な形式のパケット • 無効なパケット長を持つ不正な形式のパケット • 期間が長すぎる不正な形式のパケット • 不正なNullプローブ応答パケット • 過大なEAPOLキーを持つ不正な形式のパケット • SSIDが大きすぎる不正な形式のパケット • 冗長IEでの不正な形式のパケット	• **Malformed packet with duplicate IE**: パケットに重複するIEがあります。 • **Malformed packet with invalid disassociation code**:アソシエーション解除パケットには、理由コード0または67～65535が含まれています。 • **Malformed packet with oversized duration:** パケット期間の値が指定されたしきい値よりも大きい。
• APスプーフィング(APスプーフィングAP)攻撃 • クライアントスプーフィング(APスプーフィングクライアント)攻撃 • アドホックスプーフィング(AP Spoof Ad Hoc)攻撃 • APスプーフィング(Ad Hoc Spoof AP)攻撃 • APスプーフィング(クライアントがAPをスプーフィングする)攻撃	これらはなりすまし攻撃です。 他のデバイスの代わりにスプーフィングされたフレームを送信すると、ネットワークセキュリティが侵害されます。たとえば、クライアントが許可されたAPのふりをしている場合、クライアントをAPから切断するために、認証解除またはアソシエーション解除フレームを送信できます。次に例を示します。 • **AP spoofing (AP spoofs AP) attack**: 許可されていないAPが、クライアントと通信するために許可されたAPのMACアドレスを含むフレームを偽造します。 • **AP spoofing (client spoofs AP) attacks**: クライアントは、クライアントと通信するために許可されたAPのMACアドレスを含むフレームを偽造します。
弱いIVパケット	弱いIV攻撃は,不安定なIVにより引き起こされる。 WEPセキュリティプロトコルで使用されるRC4暗号化アルゴリズムで安全でないIVが使用されている場合、WEPキーは解読される可能性が高くなります。
• APエントリー攻撃 • クライアントエントリー攻撃	これらはデバイスエントリー攻撃です。 攻撃者は、無効なパケットを送信してWIPSの処理オーバーヘッドを増加させる可能性があります。指定された間隔内に学習されたAPまたはクライアントエントリーの数がしきい値を超えると、WIPSはアラームをトリガーし、新しいエントリーの学習を停止します。
シグニチャベースの攻撃	WIPSはユーザー定義のシグニチャを使用して攻撃を検出します。パケットがユーザー定義のシグニチャと一致すると、システムはアラームを送信します。

40 MHz帯域幅モードでディセーブルにされたクライアント	802.11nデバイスは、20 MHzと40 MHzの両方の帯域幅モードをサポートします。40 MHzの帯域幅モードがクライアントで無効になっている場合、そのクライアントと同じAPに関連付けられている他のクライアントも20 MHzの帯域幅を使用する必要があります。これにより、ネットワークのスループットと効率が低下します。
省電力攻撃	攻撃者は、AP宛てのPower Saving Onフレームでクライアントの MACアドレスをスプーフィングします。APはクライアントが省電力モードであると判断し、フレームをキャッシュします。その後、キャッシュされたフレームは期限切れとなり、廃棄されます。
Windowsブリッジ攻撃	有線ネットワークに接続されたワイヤレスクライアントが、有線NICを介してWindowsブリッジを確立すると、クライアントは外部APを内部ネットワークにブリッジできます。これにより、内部ネットワークにセキュリティ上の問題が発生する可能性があります。
オメルタアタック	Omertaは、802.11プロトコルに基づくDoS攻撃ツールであり、アソシエーション解除フレームを送信してクライアントのアソシエーションを解除します。
ソフトAP	ソフトAPとは、APとして動作し、ワイヤレスサービスを提供するクライアントのことです。攻撃者はソフトAPを介して内部ネットワークにアクセスし、さらなる攻撃を開始することができます。
• ブロードキャストアソシエーション解除攻撃 • ブロードキャスト再認証攻撃	攻撃者は正規のAPをスプーフィングして、ブロードキャストアソシエーション解除または認証解除フレームを送信し、APに関連付けられているすべてのクライアントをログオフします。
APなりすまし攻撃	正規のAPと同じBSSIDおよびESSIDを持つ悪意のあるAPは、クライアントを誘導してAPに関連付けさせます。その後、この偽装APがホットスポット攻撃を開始するか、検出システムを欺きます。
HT:未開拓のAP	HT-greenfieldモードで動作しているAPは、802.11a/b/gデバイスと通信できないため、衝突、エラー、および再送信を引き起こす可能性があります。
ワイヤレスブリッジ攻撃	攻撃者は、ワイヤレスブリッジを介して内部ネットワークに侵入します。
APフラッド攻撃	WIPSはWLAN内のAPの数を検出し、APの数が指定されたしきい値を超えると、APフラッド攻撃のアラームをトリガーします。
アソシエーション/再アソシエーションDoS攻撃	アソシエーション/再アソシエーションDoS攻撃は、APにアソシエーション要求を送信する多数のクライアントを模倣することによって、APのアソシエーションテーブルをフラッディングします。テーブル内のエントリー数が上限に達すると、APは正規のクライアントからの要求を処理できなくなります。

6. **Back**をクリックします。

検出されたAP

WIPSはワイヤレスネットワーク内のAPを監視し、検出された各APをAP分類規則に従って分類するか、またはAPに脅威レベルを割り当てます。

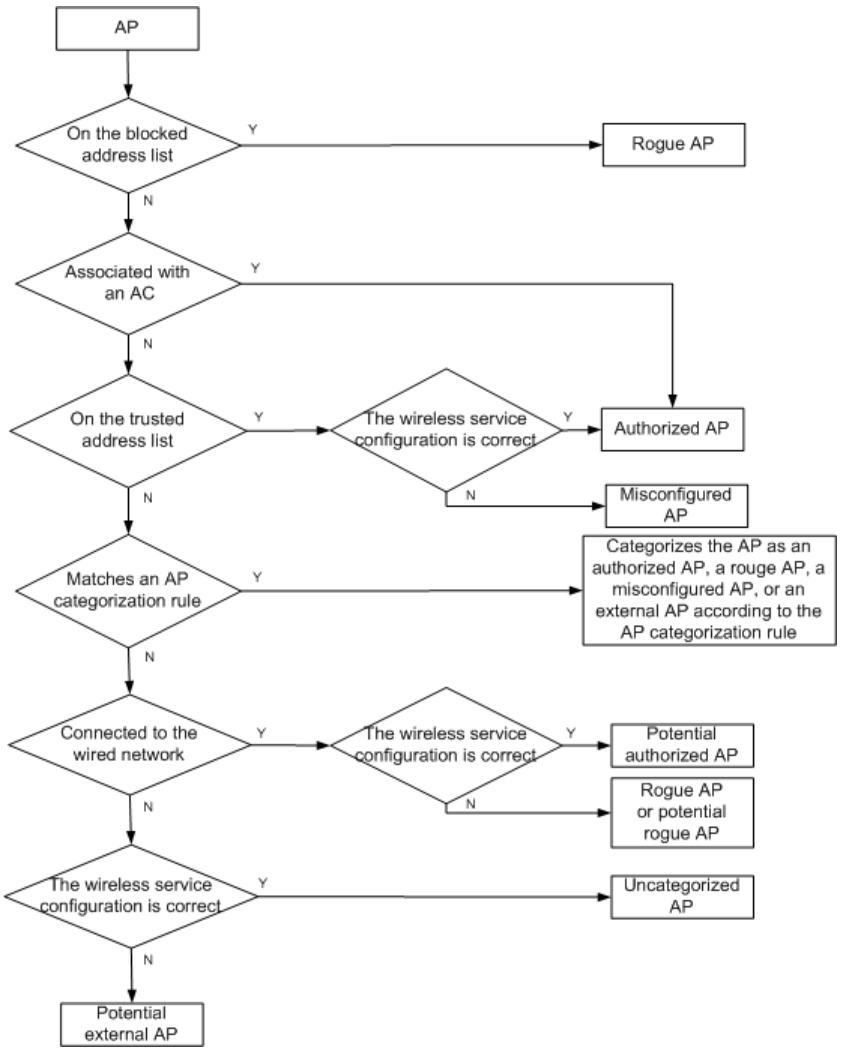
WIPSは、検出されたAPを次のタイプに分類します。

- **Authorized**: WLANで許可されているAP。次のAPがあります。
  - ACに関連付けられているAP。
  - 信頼されたアドレスリスト内にあり、ワイヤレス設定が正しいAP。
  - 許可されたAP分類ルールに一致するAP。
- **Rogue**: WLANで禁止されているAP。次のものがあります。
  - ブロックされたアドレスリスト内のAP。
  - WIPS攻撃検出ポリシーに準拠していないAP。
  - 不正APの分類ルールに一致するAP。
- **Misconfigured**: WLANで許可されているが、正しく設定されていないAP。たとえば、信頼できるアドレスリストにあるが、(AP分類ルールに従って)無効なSSIDを使用しているAP。
- **External**: 隣接無線ネットワーク内のAP。
- **Ad Hoc**:アドホックモードで動作するAP。
- **Potentia**l: 許可されている可能性のある許可されたAP。APが許可されたアドレスリストにもブロックされたアドレスリストにもないのに、無線サービスの設定が正しく、有線ポートがネットワークに接続されている場合、そのAPは許可されたAPである可能性があります。
- **Potential**: 不正APの可能性がある不正AP。APが許可デバイスリストにも禁止デバイスリストにもなく、無線サービス設定が正しくなく、有線ポートがネットワークに接続されている場合、そのAPは不正APである可能性があります(攻撃者APなど)。
- **Possible**: 外部APの可能性がある外部AP。APが許可アドレスリストにもブロックアドレスリストにもなく、無線サービスの設定が正しく、有線ポートがネットワークに接続されていない場合、そのAPは外部APである可能性があります。
- **Uncategorized**: カテゴリを判別できない、未分類のAP。

APが分類ルールに一致するが、そのルールに対してAPカテゴリが指定されていない場合、WIPSは、ルールで指定された脅威レベルをAPに割り当てます。値が大きいほど、脅威レベルが高くなります。

WIPSは、図68に示すワークフローを使用してAPを分類します。

図68 APの分類プロセス



検出されたAPリストの表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > APs Detected**を選択します。**Detected AP List**には、検出されたすべてのAPが表示されます。

   検出されたAPリストの内容
   - **Status**: APの状態: Onlineまたは Offline。
   - **BSSID**: APのBSSID(MACアドレス)。BSSIDをクリックすると、APの詳細が表示されます。
   - **SSID**: APで使用されるSSID。SSIDをクリックすると、SSIDの詳細が表示されます。
   - **Virtual Security Domain**: APを検出したセンサーが属する仮想セキュリティドメイン。
   - **Category**: APのカテゴリ。オプションは、**Authorized**、**Rogue**、**Ad hoc**、**Misconfigured**、**External**、**Potential-Authorized**、**Potential-Rogue**、**Potential-External**、および**Uncategorized**です。APカテゴリを変更するには、**Modify**アイコンをクリックします。
   - **Threat Level**: APの脅威レベル。
   - **Detecting AC**: APを検出したセンサーが関連付けられているACのデバイスラベル。ラベルをクリックすると、ACの詳細が表示されます。
   - **Device vendor info**: 検出されたAPのベンダー。センサーがAPに関するベンダー情報

を取得しない場合、このフィールドにはnullが表示されます。

- **Last Detection Time**: APが最後に検出された時刻。
- **Static List Status**: APがAC の**Static Trusted Address List**、**Alarm-Ignored Address List**、**Static Blocked Address List**、および**Countermeasures Address List**にあるかどうか。

  緑色のアイコンは、APがリストにあることを示します。アイコンをクリックすると、リストから削除されます。

  グレーのアイコンは、APがリストにないことを示します。アイコンをクリックすると、APがリストに追加されます。

  APは、**Static Trusted Address List**と**Static Blocked Address List**に同時に存在することはできません。
- **Locate**: **Locate**アイコンをクリックすると、APを検出したセンサーが存在するロケーションビューにAPが表示されます。センサーがロケーションビューにない場合、操作は失敗します。

検出されたAPリストに十分な数のエントリーがある場合は、次のナビゲーションツールが表示されます。

- **Next Page**アイコンをクリックして、**Detected AP List**のページを進めます。
- **Last Page**アイコンをクリックして、**Detected AP List**の最後のページに進みます。
- **Previous Page**アイコンをクリックして、**Detected AP List**のページを逆方向に移動します。
- **First Page**アイコンをクリックして、**Detected AP List**の先頭にページバックします。

リストの右上にある8、15、50、100、または200をクリックして、各ページに表示する項目数を指定します。

注:

検出されたAPリストは、BSSID、SSID、カテゴリ、および検出されたACフィールドでソートできます。列ラベルをクリックすると、選択したフィールドでリストをソートできます。列ラベルを使用すると、各フィールドに固有のさまざまなソートオプションを切り替えることができます。

検出されたAPの同期化

デフォルトでは、IMCは管理対象ACから検出された最新のAPリストを2時間ごとに同期化します。手動で同期化操作を実行することもできます。

検出されたAPを手動で同期するには、次の手順を

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > APs Detected**を選択します。**Detected AP List**には、検出されたすべてのAPが表示されます。
3. **Synchronize**をクリックします。

   同期プロセスが完了すると、ページが更新され、検出された最新のAPリストが表示されます。

検出されたAPのクエリー

WSMには、基本問合せと拡張問合せが用意されています。基本問合せ基準には、迅速な検索のためのキーパラメーターがいくつか含まれています。拡張問合せには、正確な照合のための様々な問合せ基準が用意されています。

検出されたAPを照会するには、次の手順を

1. **Service**タブをクリックします。

2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > APs Detected**を選択します。**Detected AP List**には、検出されたすべてのAPが表示されます。
3. 基本的なQueryを実行します。
   a BSSID(大文字と小文字を区別しない)、SSID(大文字と小文字を区別しない)または仮想セキュリティドメインを入力します。WSMは、このフィールドのファジーマッチングをサポートします。
   b **Query**アイコンをクリックします。**Detected AP List**に、クエリー基準に一致するすべてのAPが表示されます。
   c **Query**フィールドをクリアし、**Query**アイコンをクリックして、すべてのAPを表示します。
4. 高度なクエリーを実行します。
   a **Query**フィールドの横にある**Expand**アイコンをクリックして**Query**領域を拡張します。再度クリックすると**Query**領域が非表示になります。
   b Query領域で、次の1つ以上のクエリー基準を指定します。
      - **AC**: 検出ACを選択します。
      - **BSSID**: APの部分的または完全なBSSID(MACアドレス)をxx:xx:xx:xx:xx:xx:xx形式で入力します。WSMは、このフィールドのファジーマッチングをサポートしています。
      - **SSID**: APで使用されるSSIDの一部または全体を入力します。WSMは、このフィールドのファジーマッチングをサポートします。
      - **Virtual Security Domain**: APを検出したセンサーが属する仮想セキュリティドメインの名前を入力します。
      - **Category**: APのカテゴリを選択します。オプションは、**Authorized**、**Rogue**、**Ad hoc**、**Misconfigured**、**External**、**Potential-Authorized**、**Potential-Rogue**、**Potential-External**、および**Uncategorized**です。
      - **Last Detection Time**: APが最後に検出された時間範囲を選択します。オプションは、**All**、**Last Day**、**Last Three Days**、**Last Week**、および**Last Month**です。
   c **Query**をクリックします。

      Detected AP Listには、クエリー基準に一致する検出されたすべてのAPが表示されます。
   d クエリー基準をクリアし、検出されたすべてのAPを表示するには、**Reset**をクリックします。

APのカテゴリの変更

デフォルトでは、WIPSは、ユーザー定義およびシステム定義のAP分類ルールに従ってAPを分類します。APのカテゴリは手動で変更できます。

APのカテゴリを変更するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > APs Detected**を選択します。**Detected AP List**には、検出されたすべてのAPが表示されます。

   カテゴリを変更する1つまたは複数のAPを選択し、**Detected AP List**領域にある**Modify AP Category**をクリックします。

   または、ターゲットAPのCategory列にある**Modify**アイコンをクリックします。**Modify AP Category**ウィンドウが開きます。
3. **Category**リストから新しいAPカテゴリを選択します。
4. **AP Categorization Mode**リストからカテゴリ化モードを選択します。オプションには、**Manual**、**Automatic Categorization by NMS**、および**Automatic Categorization by Device**がありま

す。

5. **OK**をクリックします。

スタティックリストへのAPの割り当てまたはスタティックリストからのAPの削除

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > APs Detected**を選択します。**Detected AP List**には、検出されたすべてのAPが表示されます。
3. ターゲットAPを選択して、**Detected AP List**領域で**Operation**をクリックし、ショートカットメニューから**Add to Static Trusted Address List**、**Add to Alarm Ignored Address List**、**Add to Static Blocked Address List**、または**Add to Static Countermeasures List**を選択します。

   または、APの**Static List Status**カラムにあるスタティックリストの**Add to list**アイコンをクリックして、スタティックリストに追加します。スタティックリストから削除するには、APの**Static List Status**カラムにあるスタティックリストの**Remove from list**アイコンをクリックします。

   APが**Static Trusted Address List**および**Static Blocked Address List**に同時には存在できません。いずれかのリストにAPを追加するには、まずそのAPをもう一方のリストから削除します。

検出されたAP履歴の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > APs Detected**を選択します。**Detected AP List**には、検出されたすべてのAPが表示されます。
3. **Detected AP List**の右にある**History**アイコンをクリックします。

   Detected AP History Listには、検出されたすべてのAP履歴レコードが表示されます。

   検出されたAPの履歴リスト

   - **MAC Address**: 検出されたAPのMACアドレス。MACアドレスをクリックすると、APの詳細が表示されます。
   - **SSID**: APで使用されるSSID。
   - **Last Detection Time**: APが最後に検出された時刻。
   - **Disappeared At**: APが検出されなくなった時間。
   - **Virtual Security Domain**: APを検出したセンサーが属する仮想セキュリティドメイン。
   - **Category**: APのカテゴリ。**Authorized**、**Rogue**、**Ad hoc**、**Misconfigured**、**External**、**Potential-Authorized**、**Potential-Rogue**、**Potential-External**、または**Uncategorized**です。
   - **Device vendor info**: 検出されたAPのベンダー。センサーがAPに関するベンダー情報を取得しない場合、このフィールドにはnullが表示されます。
   - **Threat Level**: APの脅威レベル。値が大きいほど、脅威レベルが高くなります。
   - **Detecting AC**: APを検出したセンサーが関連付けられているACのデバイスラベル。ラベルをクリックすると、ACの詳細が表示されます。
4. **Back**アイコンをクリックして、**Detected AP List**に戻ります。

検出されたAP履歴の照会

検出されたAPのクエリー基準を使用して、検出されたAPの履歴レコードをクエリーできます。詳細については、「検出されたAPのクエリー」を参照してください。

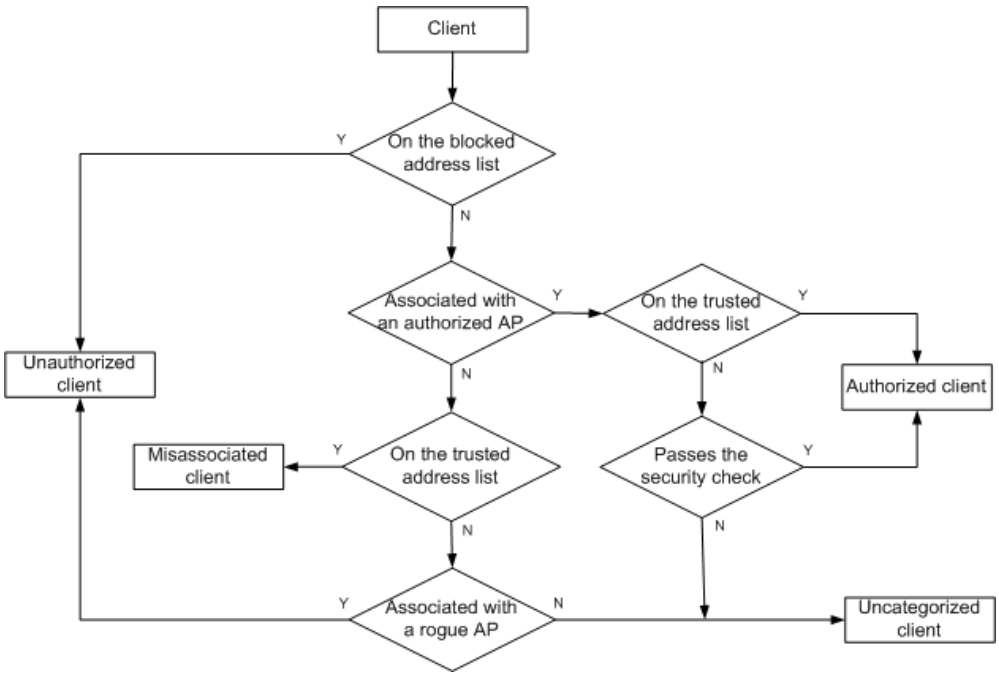
検出されたクライアントリスト

Detected Clientリストには、すべてのセンサーによって検出されたクライアントが表示されます。クライアントは次のカテゴリに分類されます。

- **Authorized**: WLANで許可されているクライアント。次のクライアントが含まれます。
  - 許可されたAPに関連付けられている許可デバイスリスト内のクライアント。
  - 認証と暗号化を渡すことによって許可されたAPに関連付けられているクライアント。
- **Rogue**: WLANで禁止されているクライアント。次のものがあります。
  - ブロックされたアドレスリスト上のクライアント。
  - 不正なAPに関連付けられたクライアント。
  - **Misassociated**: 信頼されたアドレスリスト上が、不正なAPに関連付けられているクライアントの誤やまった関連付け。
  - **Uncategorized**: カテゴリを判別できないクライアント。

WIPSは、図69に示すプロセスを使用して、検出されたクライアントを分類します。

図69 クライアントのクラス分けプロセス



検出されたクライアントリストの表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Clients Detected**を選択します。**Detected Client List**には、検出されたすべてのクライアントが表示されます。
   検出されたクライアントリストの内容
   - **Status**:クライアントのオンライン状態: ●Onlineまたは●Offline。

- **MAC Address**: クライアントのMACアドレス。
- **BSSID**:クライアントがアソシエートされているAPのBSSID(MACアドレス)。BSSIDをクリックすると、APの詳細が表示されます。
- **Virtual Security Domain**: を検出したセンサーが属する仮想セキュリティドメイン。
- **Category**: クライアントのカテゴリ。**Authorized**、**Unauthorized**、**Misassociated**、および**Uncategorized**があります。
- **Detecting AC**: クライアントを検出したセンサーが関連付けられているACのデバイスラベル。ラベルをクリックすると、ACの詳細が表示されます。
- **Last Detection Time**: クライアントが最初に検出された時刻。
- **Static List Status**: クライアントが**Static Trusted Address List**、**Alarm-Ignored Address List**、**Static Blocked Address List**、および**Countermeasures Address List**にあるかどうか。

  緑色のアイコンは、クライアントがリストにあることを示します。アイコンをクリックすると、リストからクライアントが削除されます。

  グレーのアイコンは、クライアントがリストにないことを示します。アイコンをクリックすると、クライアントがリストに追加されます。

  APは、**Static Trusted Address List**と**Static Blocked Address List**に同時に存在することはできません。
- **Locate**: クライアントを検出したセンサーが存在するロケーションビューにクライアントを表示するには、**Locate**アイコンをクリックします。センサーがロケーションビューに存在しない場合、操作は失敗します。

Detected Client Listに十分な数のエントリーがある場合は、次のナビゲーションツールが表示されます。

- **Next Page**アイコンをクリックして、**Detected Client List**のページを進めます。
- **Last Page**アイコンをクリックして、**Detected Client List**の最後のページに進みます。
- **Previous Page**アイコンをクリックすると、**Detected Client List**のページが逆に表示されます。
- **First Page**アイコンをクリックすると、**Detected Client List**の先頭にページバックします。

リストの右上にある8、15、50、100、または200をクリックして、各ページに表示する項目数を指定します。

注:

「検出されたクライアントリスト」は、「静的リストステータス」フィールド以外のすべてのフィールドでソートできます。選択したフィールドでリストをソートするには、列ラベルをクリックします。列ラベルを使用すると、各フィールドに固有の様々なソートオプションを切り替えることができます。

検出されたクライアントの同期

デフォルトでは、IMCは、管理対象ACからWIPSによって検出された最新のクライアント情報を2時間ごとに同期します。手動で同期操作を実行することもできます。

管理対象ACから検出されたクライアント情報を手動で同期するには、次の手順を実行します

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Clients Detected**を選択します。**Detected Client List**には、検出されたすべてのクライアントが表示されます。
3. **Synchronize**をクリックします。

   同期プロセスが完了すると、ページが更新され、最後に検出されたクライアントのリストが表示されます。

検出されたクライアントのクエリー

WSMには、基本問合せと拡張問合せが用意されています。基本問合せ基準には、迅速な検索のためのキーパラメーターがいくつか含まれています。拡張問合せには、正確な照合のための様々な問合せ基準が用意されています。

検出されたクライアントを照会するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Clients Detected**を選択します。**Detected Client List**には、検出されたすべてのクライアントが表示されます。
3. 基本的な**Query**を実行します。
   a. MACアドレスまたは仮想セキュリティドメイン名を入力します。WSMは、このフィールドのファジーマッチングをサポートします。
   b. **Query**アイコンをクリックします。**AC List**に、問合せ基準に一致するすべてのACが表示されます。
   c. **Query**フィールドをクリアして**Query**アイコンをクリックすると、すべてのACが表示されます。
4. 高度なQueryを実行します。
   a. **Query**フィールドの横にある**Expand**アイコンをクリックして**Query**領域を拡張します。再度クリックすると**Query**領域が非表示になります。
   b. **Query**領域で、次の1つ以上のクエリー基準を指定します。
      - **AC**: クライアントを検出したセンサーが関連付けられているACを選択します。
      - **MAC Address**: クライアントのMACアドレスの一部または全体をxx:xx:xx:xx:xx:xx形式で入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
      - **Virtual Security Domain**: クライアントを検出したセンサーが属する仮想セキュリティドメインの名前を入力します。
      - **BSSID**: クライアントがアソシエートされているAPのBSSID(MACアドレス)の一部または全部を入力します。WSMは、このフィールドのファジーマッチングをサポートしています。
      - **Category**: リストからクライアントカテゴリを選択します。オプションは**All**、**Authorized**、**Unauthorized**、**Misassociated**および**Uncategorized**です。
      - **Last Detection Time**: クライアントが最後に検出された時間範囲を選択します。オプションは、**All**、**Last Day**、**Last Three Days**、**Last Week**、および**Last Month**です。
   c. **Query**をクリックします。

      Detected Client Listには、query criteriaに一致するすべての検出されたクライアントが表示されます。
   d. **Reset**をクリックしてquery criteriaをクリアし、検出されたすべてのクライアントを表示します。

検出されたクライアントの詳細の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Clients Detected**を選択します。**Detected Client List**には、検出されたすべてのクライアントが表示されます。
3. 詳細情報を表示するクライアントのMACアドレスをクリックします。Client Detailsページが開きます。

   基本的なクライアント情報
   - **MAC Address**: クライアントのMACアドレス。

- **Detecting AC**: クライアントを検出したセンサーが関連付けられているACのデバイスラベル。ラベルをクリックすると、ACの詳細が表示されます。
- **Virtual Security Domain**: クライアントを検出したセンサーが属する仮想セキュリティドメインの名前。
- **Whether Countermeasures Are Taken**: WIPSがクライアントに対して対策を実施したかどうか、**Yes**または**No**。
- **Sensors That Have Detected the Clients**: クライアントを検出したセンサーの数。
- **BSSID**: クライアントがアソシエートされているAPのBSSID(MACアドレス)。
- **First Detection Time**: クライアントが最初に検出された時刻。
- **Last Detection Time**: クライアントが最後に検出された時刻。
- **Status**: クライアントの現在のオンライン状態。
- **Station Status**: 最後に検出されたときにクライアントがAPに関連付けられていたかどうか。**Associated**または**Disassociated**。
- **Channel**: クライアントとAPが相互に通信するために使用するチャネル。
- **Category**: クライアントのカテゴリ。**Authorized**、**Unauthorized**、**Misassociated**、または**Uncategorized**。
- **Radio Type**: クライアントが関連付けられている無線のタイプ: **802.11a**、**802.11b**、**802.11g**、**802.11an**、**または802.11gn**。

センサーリスト

Sensor Listには、クライアントを検出したすべてのセンサーが表示されます。

- **Status**: センサーの現在の状態: Onlineまたは Offline。
- **AP Label**: センサーのデバイスラベル。ラベルをクリックすると、センサーの詳細が表示されます。
- **Last Detection Time**: センサーが最後にクライアントを検出した時刻。
- **RSSI(dBm)**: センサーのRSSI値。
- **Radio ID**: クライアントを検出した無線のID。

最新のWIPSセキュリティベントリスト

Latest WIPS Security Event Listには、クライアントに関連するすべてのセキュリティベントが表示されます。

- **Level**: セキュリティベントの重大度レベル。セキュリティレベルには、**Emergency**、**Alarm**、**Key**、**Error**、**Warning**、**Notification**、**Prompt**および**Debugging**があります。
- **Sensor MAC Address**: クライアントを検出したセンサーのMACアドレス。
- **Virtual Security Domain**: クライアントを検出したセンサーが属する仮想セキュリティドメイン。
- **Event Type**: セキュリティベントタイプ。
- **Description**: セキュリティベントの説明。
- **Generated At**: セキュリティベントが発生した時刻。

検出されたクライアントの静的リストへの割り当てまたは静的リストからの削除

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Clients Detected**を選択します。**Detected Client List**には、検出されたすべてのクライアントが表示されます。

3. ターゲットクライアントを選択し、**Detected AP List**領域で**Operation**をクリックして、ショートカットメニューから**Add to Static Trusted Address List**、**Add to Alarm Ignored Address List**、**Add to Static Blocked Address List**、または**Add to Static Countermeasures List**を選択します。

   または

   クライアントをリストに追加するには、クライアントの**Static List Status**列にある静的リストの**Add to list**アイコンをクリックします。リストからクライアントを削除するには、**Remove from list**アイコンをクリックします。

   クライアントは、**Static Trusted Address List**および**Static Blocked Address List**に登録できません。同時に。いずれかのリストにクライアントを追加するには、最初にもう一方のリストからクライアントを削除します。

検出されたクライアントの履歴の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Clients Detected**を選択します。**Detected Client List**には、検出されたすべてのクライアントが表示されます。
3. **Detected Client History**リストの右にある**History**アイコンをクリックします。

   Detected Client Historyリストには、検出されたすべてのクライアント履歴レコードが表示されます。

   Detected Client Historyリストの内容

   - **Client MAC**: クライアントのMACアドレス。MACアドレスをクリックすると、クライアントの詳細が表示されます。
   - **BSSID**: クライアントがアソシエートされているAPのBSSID(MACアドレス)。
   - **Last Detection Time**: クライアントが最後に検出された時刻。
   - **Disappeared At**: クライアントがログオフした時刻。
   - **Virtual Security Domain**: クライアントを検出したセンサーが属する仮想セキュリティドメイン。
   - **Category**: クライアントのカテゴリ。オプションは、**Authorized**、**Unauthorized**、**Misassociated**、および**Uncategorized**です。
   - **Detecting AC**: APを検出したセンサーが関連付けられているACのデバイスラベル。ラベルをクリックすると、ACの詳細が表示されます。
4. **Detected Clients History List**の右上隅にある**Back**アイコンをクリックして、**Detected Client List**ページに戻ります。

検出されたクライアント履歴の照会

検出されたクライアント履歴の問合せは、検出されたクライアントの問合せと同様です。詳細は、「検出されたクライアントの問合せ」を参照してください。

検出されたSSID

センサーは国コードでサポートされているチャネルをスキャンし、そのチャネルで使用されているSSIDに関する統計情報を収集します。

検出されたSSID一覧の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > SSID Detected**を選択します。**Detected SSID List**には、検出されたすべてのSSIDが表示されます。

   検出されたSSIDリスト

   - **Status**: SSIDの状態: **Inactive**または**Active**。アクティブなSSIDは、指定された時間内にSSIDを伝送するフレームが送信されない場合に非アクティブになります。非アクティブなSSIDは、そのライフタイムが指定されたエージングタイムを超えると、**Detected SSID List**から削除されます。
   - **SSID**: SSIDをクリックすると、その詳細が表示されます。
   - **Virtual Security Domain**: SSIDを検出したセンサーが属する仮想セキュリティドメイン。
   - **Hide SSID**: APから送信されたビーコンフレーム内でSSIDを非表示にするかどうか。
   - **AP Count**: SSIDを使用するAPの数。
   - **Detecting AC**: SSIDを検出したセンサーが関連付けられているACのデバイスラベル。ラベルをクリックすると、ACの詳細が表示されます。
   - **Last Detection Time**: SSIDが最後に検出された時刻。

   検出されたSSIDリストに十分な数のエントリーがある場合は、次のナビゲーションツールが表示されます。

   - **Next Page**アイコンをクリックして、**Detected SSID List**で次のページに
   - **Last Page**アイコンをクリックして、**Detected SSID List**の最後のページに進みます。
   - **Previous Page**アイコンをクリックして、**Detected SSID List**のページを逆に表示します。
   - **First Page**アイコンをクリックして、**Detected SSID List**の先頭にページバックします。
3. 検出されたSSIDリストの右上にある**8**、**15**、**50**、**100**、または**200**をクリックして、各ページに表示する項目数を指定します。

注:

Detected SSID Listは、**SSID**、**AP Count**、および**Detected AC**フィールドでソートできます。列ラベルをクリックすると、選択したフィールドでリストをソートできます。列ラベルを使用すると、各フィールドに固有のさまざまなソートオプションを切り替えることができます。

検出されたSSIDの同期

デフォルトでは、IMCは管理対象ACからWIPSによって検出されたSSIDを2時間ごとに同期します。手動で同期操作を実行することもできます。

ACからSSIDを手動で同期化するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Clients Detected**を選択します。**Detected SSID List**には、検出されたすべてのSSIDが表示されます。
3. **Synchronize**をクリックします。

   同期プロセスが完了すると、ページがリフレッシュされ、最後に検出されたSSIDアドレスリストが表示されます。

検出されたSSIDのクエリー

WSMには、基本問合せと拡張問合せが用意されています。基本問合せ基準には、迅速な検索のためのキーパラメーターがいくつか含まれています。拡張問合せには、正確な照合のための様々な問合せ基準が用意されています。

検出されたSSIDを照会するには、次の手順を

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > SSID Detected**を選択します。**Detected SSID List**には、検出されたすべてのSSIDが表示されます。
3. 基本的なQueryを実行します。
   a. SSID(大文字と小文字を区別)または仮想セキュリティドメイン名を入力します。WSMでは、このフィールドのファジーマッチングがサポートされます。
   b. **Query**アイコンをクリックします。**Detected SSID List**に、query criteriaに一致するすべてのSSIDが表示されます。
   c. **Query**フィールドをクリアして**Query**アイコンをクリックすると、すべてのSSIDが表示されます。
4. 高度なQueryを実行します。
   a. Queryフィールドの横にある**Expand**アイコンをクリックしてQuery領域を拡張します。再度クリックするとQuery領域が非表示になります。
   b. **Query Criteria**領域で、次の1つ以上の**Query Criteria**を指定します。
      - **AC**: SSIDを検出したセンサーが関連付けられているACを選択します。
      - **SSID**: 照会するSSIDの一部または全体を入力します。
      - **Virtual Security Domain**: SSIDを検出したセンサーが属する仮想セキュリティドメインの名前を入力します。
      - **Status**: SSIDの状態を選択します。オプションには、**Active**、**Inactive**、および**All**があります。
      - **Last Detection Time**: SSIDが最後に検出された時間範囲を選択します。オプションは、**All**、**Last Day**、**Last Three Days**、**Last Week**、および**Last Month**です。
   c. **Query**をクリックします。
      Detected SSID Listには、クエリー基準に一致する検出されたすべてのSSIDが表示されます。
   d. Query criteriaをクリアし、検出されたすべてのSSIDを表示するには、**Reset**をクリックします。

検出されたSSIDの詳細の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Clients Detected**を選択します。**Detected SSID List**には、検出されたすべてのSSIDが表示されます。
3. 詳細情報を表示するSSIDをクリックします。SSIDの詳細ページが開きます。
   基本的なSSID情報
   - **SSID**: SSID。
   - **Detecting AC**: SSIDを検出したセンサーが関連付けられているACのデバイスラベル。ラベルをクリックすると、ACの詳細が表示されます。
   - **Number of APs of the SSID**: SSIDを使用するAPの合計数。
   - **Virtual Security Domain**: SSIDを検出したセンサーが属する仮想セキュリティドメイン。

- **Hide SSID**: APから送信されたビーコンフレーム内でSSIDを非表示にするかどうか。
- **First Detection Time**: SSIDが最初に検出された時刻。
- **Last Detection Time**: SSIDが最後に検出された時刻。
- **Status**: SSIDの状態: **Active**または**Inactive**。デフォルトでは、検出されたSSIDは**Active**状態です。指定された時間内にSSIDを含むフレームが送信されない場合、SSIDの状態は**Inactive**に設定されます。
- **Security Method**: SSIDを伝送するフレームで使用されるセキュリティ方式。
- **Encryption Method**: SSIDを伝送するフレームで使用される暗号化方式。
- **Authentication Method** :SSIDを伝送するフレームで使用される認証方式。

SSIDのAP

SSID領域のAPには、SSIDを使用しているすべてのAPが表示されます。

- **BSSID**: SSIDを使用しているAPのBSSID(MACアドレス)。
- **Channel**: SSIDで使用されるチャネル。
- **Client Count**: SSIDを使用してワイヤレスネットワークにアクセスしているクライアントの合計数。

検出されたSSID履歴の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > SSID Detected**を選択します。**Detected SSID List**には、検出されたすべてのSSIDが表示されます。
3. **Detected SSID List**の右にある**History**アイコンをクリックします。

   Detected SSID History Listには、検出されたSSIDのすべての履歴レコードが表示されます。

   検出されたSSID履歴一覧の内容

   - **SSID**: SSIDをクリックすると、その詳細が表示されます。SSIDの詳細については、「検出されたSSIDの詳細の表示」を参照してください。
   - **Virtual Security Domain**: SSIDを検出したセンサーが属する仮想セキュリティドメイン。
   - **Last Detection Time**: SSIDが最後に検出された時刻。
   - **Disappeared at**: SSIDが検出されなくなった時刻に消失しました。
   - **Security Method**: SSIDで使われるセキュリティ方法。**Clear**、**WEP**、**WPA**、**WPA2**、または**WPA/WPA2**。
   - **Detecting AC**: SSIDを検出したセンサーが関連付けられているACのデバイスラベル。ラベルをクリックすると、ACの詳細が表示されます。

検出されたSSID履歴の照会

検出されたSSIDのクエリー基準を使用して、検出されたSSID履歴をクエリーできます。詳細については、「検出されたSSIDのクエリー」を参照してください。

セキュリティイベント

セキュリティイベントは、syslogメッセージに記録されるワイヤレスネットワーク内のイベントまたは動作です。APは検出された情報を定期的にACに報告します。ACはsyslogに情報を記録し、syslogをIMCに送信します。WIPSセキュリティイベントリストでsyslogを表示できます。

WIPSセキュリティイベントリストを表示するには、次の条件が満たされていることを確認します。

- Syslog Managementモジュールがインストールされ、展開されている。
- **info-center loghost xxxx**コマンドを使用して、IMCサーバー(IPアドレス)をACのログホストとして設定します。xxxxは、プライマリIMCサーバーのIPアドレスです。

WIPSセキュリティベントリストの表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Security Event**を選択します。**WIPS Security Event List**には、すべてのセキュリティベントが表示されます。

   WIPSセキュリティベントリストの内容

   - **Security Level**: セキュリティベントの重大度レベル。

     オプションは、**Emergency**, **Alarm**,**Key**, **Error**, **Warning**, **Notification**, **Prompt**,および**Debugging**です。
   - **Detected Device MAC**: イベントが発生したデバイスのMACアドレス。
   - **Detecting Device MAC**: セキュリティベントを検出したデバイスのMACアドレス。
   - **Virtual Security Domain**: セキュリティベントを検出したセンサーが属する仮想セキュリティドメイン。
   - **Event Type**: セキュリティベントタイプ。たとえば、vsd-client-delまたはvsd-ap-addです。
   - **Detecting AC**: セキュリティベントを検出したセンサーが関連付けられているACのデバイスラベル。ACラベルをクリックすると、その詳細が表示されます。
   - **Description**: セキュリティベントの説明。
   - **Receive Time**: セキュリティベントを記録したsyslogを受信した時刻。
   - **Locate**: **Locate**アイコンをクリックすると、デバイスを検出したセンサーが存在するロケーションビューにデバイスが表示されます。センサーがロケーションビューにない場合、操作は失敗します。

   WIPSセキュリティベントリストに十分な数のエントリーがある場合は、次のナビゲーションツールが表示されます。

   - **Next Page**アイコンをクリックして、**WIPS Security Event List**で次のページに進みます。
   - **Last Page**アイコンをクリックして、**WIPS Security Event List**の最後のページに進みます。
   - **Previous Page**アイコンをクリックすると、**WIPS Security Event List**のページが逆方向に表示されます。
   - **First Page**アイコンをクリックして、**WIPS Security Event List**の前のページに戻ります。
3. WIPS Security Event Listの右上にある**8**、**15**、**50**、**100**、または**200**をクリックして、各ページに表示する項目数を指定します。

注:

WIPS Security Event Listは、すべてのフィールドでソートできます。選択したフィールドでリストをソートするには、列ラベルをクリックします。列ラベルを使用すると、各フィールドに固有のさまざまなソートオプションを切り替えることができます。

セキュリティベントの照会

WSMには、基本問合せと拡張問合せが用意されています。基本問合せ基準には、迅速な検索のための

キーパラメーターがいくつか含まれています。拡張問合せには、正確な照合のための様々な問合せ基準が用意されています。

セキュリティイベントを問い合せる手順は、次のとおりです

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Security Event**を選択します。**WIPS Security Event List**には、すべてのセキュリティイベントが表示されます。
3. 基本的なQueryを実行します。
   a. 仮想セキュリティドメイン名またはセキュリティイベントを入力します。WSMでは、このフィールドのファジーマッチングがサポートされます。
   b. **Query**アイコンをクリックします。**WIPS Security Event List**に、Query criteriaに一致するすべてのセキュリティイベントが表示されます。
   c. **Query**フィールドを消去し、**Query**アイコンをクリックして、すべてのセキュリティイベントを表示します。
4. 高度なQueryを実行します。
   a. **Query**フィールドの横にある**Expand**アイコンをクリックして**Query**領域を拡張します。再度クリックすると**Query**領域が非表示になります。
   b. 次の問合せ基準を1つ以上指定します。
      - **Detected Device MAC**: セキュリティイベントが発生したデバイスの部分的または完全なMACアドレスをxx:xx:xx:xx:xx:xx:xx形式で入力します。WIPSは、このフィールドのファジーマッチングをサポートします。
      - **Detecting Device MAC**: セキュリティイベントを検出するデバイスの部分的または完全なMACアドレスをxx:xx:xx:xx:xx:xx:xx形式で入力します。WIPSは、このフィールドのファジーマッチングをサポートします。
      - **Virtual Security Domain**: セキュリティイベントを検出したセンサーが属するセキュリティドメイン名の一部または全部を入力します。
      - Receive Time: セキュリティイベントが発生した時間範囲を選択します。オプションは**All**、**Last Day**、**Last Three Days**、**Last Week**および**Last Month**です。
      - Event Type: セキュリティイベントタイプを入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
      - Severity Level: セキュリティイベントの重大度レベルを選択します。オプションは、**Emergency**, **Alarm**, **Key**, **Error**, **Warning**, **Notification**, **Prompt**および**Debugging**です。
   c. **Query**をクリックします。

      WIPS Security Event Listには、クエリー基準に一致するすべてのセキュリティイベントが表示されます。
   d. **Reset**をクリックすると、クエリー基準が消去され、すべてのセキュリティイベントが表示されます。

セキュリティイベントの削除

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Security Event**を選択します。

   WIPS Security Event Listにすべてのセキュリティイベントが表示されます。
3. 削除するセキュリティイベントを1つ以上選択します。
4. **Delete**をクリックします。
5. 確認ダイアログボックスで、**OK**をクリックします。

WLANプローブ

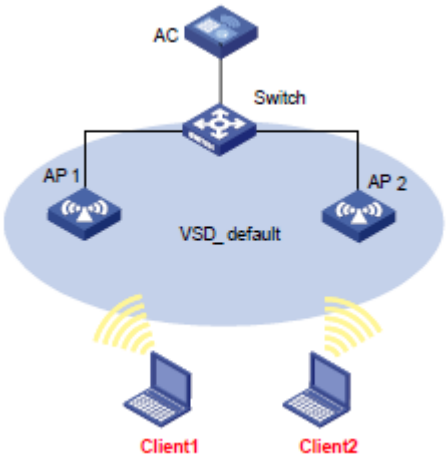
WLANプローブを使用すると、APはチャネルをスキャンしてデバイス情報を収集し、デバイスの数量と位置をリアルタイムで分析するためにその情報をWSMに送信できます。WLANプローブは、関連付けられていないクライアントを検索できます。

WLANプローブとWIPSを同時に使用することはできません。

WLANプローブネットワーク

図70に示すように、APをモニターモードまたはハイブリッドモードで動作するように設定できます。APのWLANプローブ設定の詳細については、関連するデバイスのマニュアルを参照してください。

図70 WLANプローブネットワーク



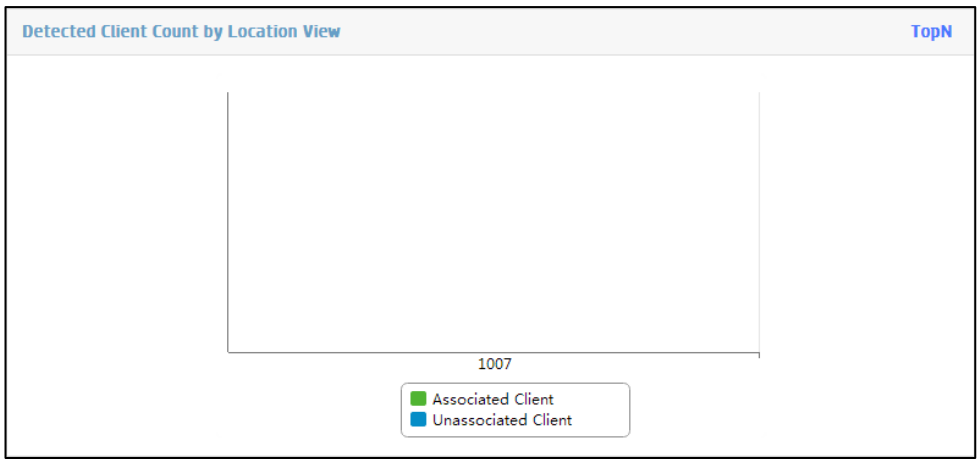
検出されたクライアントグラフ

検出されたクライアントグラフには、ロケーションビュー別のクライアント数またはトレンドが表示されます。特定のロケーションビューの検出されたクライアントグラフを表示するには、最初にロケーションビューをカスタマイズする必要があります。ロケーションビューまたはサブロケーションビューのカスタマイズの詳細は、「ロケーションビューのカスタマイズ」を参照してください。

ロケーションビューによって検出されたクライアントの数

このグラフには、ロケーションビューごとに、関連付けられているクライアントと関連付けられていないクライアントの数が表示されます。サブロケーション内のクライアントは含まれません。

図71 ロケーションビュー別に検出されたクライアント数



グラフの右上にある**TopN**をクリックします。**TopN Location Views by Client Count**ページが開きます。

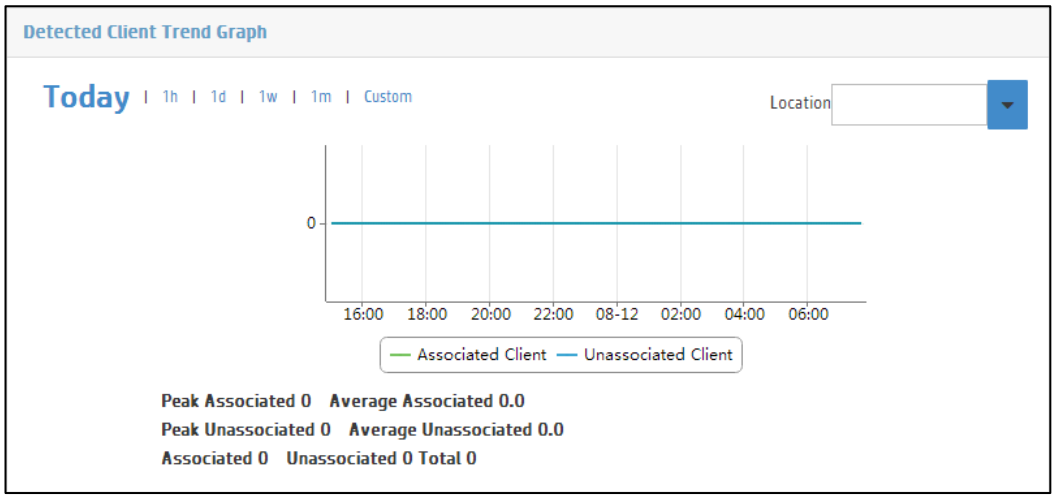
図72 クライアント数別のTop N Locationビュー

- 図の右上にある**TopN**リストから番号を選択します。オプションは**5**、**10**、**20**、**50**および**100**です。
- **Top N Location Views by Client Count List**のサブロケーションにあるクライアントを含めるには**Including sublocations**を選択します。

検出されたクライアントのトレンドグラフ

グラフには、オンラインクライアントのトレンド、ピーク、および平均オンラインクライアント数が表示されます。

図73 検出されたクライアントのトレンドグラフ



横軸は時間を表し、縦軸はクライアント数を表します。左上にある時間範囲リンクをクリックすると、特定の

時間範囲内でのオンラインクライアント数の変化を表示できます。オプションには、Today、1h, 1d, 1w,1wおよびCustomがあります。別の時間範囲リンクをクリックすると、横軸の時間増分が変化します。

グラフの右上にある**Location**リストからロケーションまたはサブロケーションを選択すると、そのロケーションまたはサブロケーションのクライアントトレンドを表示できます。

プローブ情報の表示

Probing Infoページには、検出されたすべてのデバイス(APおよびクライアントを含む)に関する情報が

表示されます。プローブ情報を表示する手順は、次のとおりです。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Probing Info**を選択します。

   Probing Infoページには、検出されたクライアントグラフおよび検出されたデバイスのリストが表示されます。検出されたクライアントグラフの詳細は、「検出されたクライアントグラフ」を参照してください。

   検出されたデバイスリスト

   - **MAC Address**: デバイスのMACアドレス。
   - **Category**: デバイスのタイプ。オプションには、**Related Detection of AP Clients**、**Associated With Other AP Clients**、**Non Associated Clients**、および**Neighbor AP**があります。
   - **SSID**: 接続されたネットワークのSSID。関連付けられていないクライアントの場合、このフィールドは空です。
   - **BSSID**: アソシエートされたAPのMACアドレス。アソシエートされていないクライアントまたはネイバーAPの場合、このフィールドは空です。
   - **Channel**: デバイスの動作チャネル。
   - **Detected AP**: デバイスを検出したAPの名前。
   - **Location**: 検出中のAPが存在するロケーションビューの名前。
   - **RSSI**: デバイスのRSSI。
   - **Noise**: 検出APによって検出されたノイズフロア。ノイズフロアはチャネル品質に影響し、温度によって変化します。
   - **Encryption Method**: デバイスで使用される暗号化方式。
   - **First Detection Time**: デバイスが最初に検出された時刻。
   - **Last Detection Time**: デバイスが最後に検出された時刻。
   - **Online Time**: デバイスの合計オンライン時間。
   - **Detecting AC**: 検出中のAPが関連付けられているACの名前。

プローブ情報の照会

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Probing Info**を選択します。**Detected Device List**には、検出されたすべてのデバイスが表示されます。
3. 基本的なQueryを実行します。
   a. MACアドレスを入力します。WSMは、このフィールドのファジーマッチングをサポートしています。
   b. **Query**アイコン🔍をクリックします。**Detected Device List**に、query criterialに一致するすべてのデバイスが表示されます。

c. **Query**フィールドをクリアして**Query**アイコンをクリックすると、検出されたすべてのデバイスが表示されます。

4. 高度なQueryを実行します。
   a. Queryフィールドの横にある**Expand**アイコンをクリックしてQuery領域を拡張します。再度クリックするとQuery領域が非表示になります。
   b. Query criteria領域で、次の1つ以上のクエリー基準を指定します。
      - **AC**: 検出ACを選択します。
      - **MAC Address**: デバイスのMACアドレスを入力します。
      - **Location**: 検出しているAPがあるロケーションビューを選択します。
      - **Device Type**: デバイスタイプを選択します。オプションは、**All**、**Related Detection of AP Clients**、**Associated With Other AP Clients**、**Non Associated Clients**、および**Neighbor AP**です。
      - **Last Detection Start Time**: クエリー時間範囲の開始時間を選択します。
      - **Last Detection End Time**: クエリー時間範囲の終了時間を選択します。
      - **Duplicate MAC Filter**: 重複するデバイスをフィルタリングするかどうかを選択します。オプションは**Yes**と**No**です。Yesを選択すると、WSMは同じMACアドレスを持つデバイスをフィルタリングし、最後に検出されたデバイスだけを表示します。
      - **Detected AP**: 検出しているAPを選択します。
   c. Queryをクリックします。

      Detected Device Listには、query criteriaに一致するすべてのデバイスが表示されます。
   d. **Reset**をクリックしてquery criteriaをクリアし、検出されたすべてのデバイスを表示します。

位置ビューをカスタマイズする

検出されたクライアントグラフのロケーションビューをカスタマイズするには、次の作業を実行します。ロケーションビューをカスタマイズするには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Probing Info**を選択します。
3. ページの**Customize Location Views**をクリックします。
4. 1つ以上のロケーションビューを選択します。デフォルトでは、ロケーションビュー内のすべてのサブロケーションビューが選択されます。サブロケーションビューのグラフをカスタマイズすることもできます。
5. **OK**をクリックします。

APの検出されたデバイスの表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Probing Info**を選択します。
3. **Detected Device**リストで、検出しているAPの名前をクリックします。**Detected Device**リストには、APによって検出されたすべてのデバイスが表示されます。

   Detected Device List
   - **MAC Address**: デバイスのMACアドレス。
   - **Category**: デバイスのタイプ。オプションには、**Related Detection of AP Clients**、**Associated With Other AP Clients**、**Non Associated Clients**、および**Neighbor AP**があ

ります。

- **SSID**: 接続されたネットワークのSSID。関連付けられていないクライアントの場合、このフィールドは空です。
- **BSSID**: アソシエートされたAPのMACアドレス。アソシエートされていないクライアントまたはネイバーAPの場合、このフィールドは空です。
- **Channel**: デバイスの動作チャネル。
- **RSSI**: デバイスのRSSI。
- **Noise**: 検出APによって検出されたノイズフロア。ノイズフロアはチャネル品質に影響し、温度によって変化します。
- **Encryption Method**: デバイスで使用される暗号化方式。
- **First Detection Time**: デバイスが最初に検出された時刻。
- **Last Detection Time**: デバイスが最後に検出された時刻。
- **Online Time**: デバイスの合計オンライン時間。

4. **Close**アイコンをクリックして、ウィンドウを閉じます。

プローブ情報履歴の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIPS Management > Probing Info**を選択します。
3. **History**をクリックします。

   Probing Info Historyページが開きます。

   プローブ情報の履歴リスト

   - **MAC Address**: デバイスのMACアドレス。
   - **Category**: デバイスのタイプ。オプションには、**Related Detection of AP Clients**、**Associated With Other AP Clients**、**Non Associated Clients**、および**Neighbor A**Pがあります。
   - **SSID**: 接続されたネットワークのSSID。関連付けられていないクライアントの場合、このフィールドは空です。
   - **BSSID**: アソシエートされたAPのMACアドレス。アソシエートされていないクライアントまたはネイバーAPの場合、このフィールドは空です。
   - **Channel**: デバイスの動作チャネル。
   - **Detected AP**: デバイスを検出したAPの名前。
   - **Location**: 検出中のAPが存在するロケーションビューの名前。
   - **RSSI**: デバイスのRSSI。
   - **Noise**: 検出APによって検出されたノイズフロア。ノイズフロアはチャネル品質に影響し、温度によって変化します。
   - **Encryption Method**: デバイスで使用される暗号化方式。
   - **First Detection Time**: デバイスが最初に検出された時刻。
   - **Last Detection Time**: デバイスが最後に検出された時刻。
   - **Online Time**: デバイスの合計オンライン時間。
   - **Detecting AC**: 検出中のAPが関連付けられているACの名前。
4. **Back**をクリックして、**Probing Info**ページに戻ります。

データのエクスポート

WSMでは、データベースのワークロードを削減するためのデータエクスポートがサポートされています。エクスポート可能なデータには、検出されたAP、検出されたクライアント、検出されたSSID、セキュリティイベントおよびWLANプローブ情報が含まれます。データエクスポートの詳細は、H3C IMC v7.3 Enterprise and Standard Platform Administrator Guideを参照してください。

データエクスポートを構成するには:

1. **System**タブをクリックします。
2. ナビゲーションツリーから、**System Configuration** > **Data Export**を選択します。**Data Export Settings**ページが開きます。
3. ターゲットタブをクリックして、設定ページを開きます。
4. 次のパラメーターを設定します。
   - トリガー方法を選択します。
   - **By Quantity**: データベースに保存されているエントリーの数がしきい値に達した場合、データをエクスポートします。**Export but the last** 値を設定して、データベースで最近生成された指定された数のエントリーを保存し、他のエントリーをエクスポートするように WSM を構成します。
   - **By Time**: しきい値より長いエントリーがデータベースに保存されている場合にデータをエクスポートします。指定した時間内に生成されたエントリーを保存し、その他のエントリーをエクスポートするようにWSMを構成するには、**Export but those in last**の値を設定します。

     By Quantityと**By Time**の両方を選択した場合、WSMはデータベースがより多くのエントリーを保存できる方法を使用します。
   - エクスポート設定を構成します。
   - **Target File Type**: ターゲットファイルタイプを選択します。オプションはCSVおよびHTMLです。
   - **Save File for**: エクスポートしたファイルを保存できる日数を入力します。
   - **Execute Command After Export**: GUI操作を必要としないコマンドを指定します。コマンドには、実行可能コマンドまたはバッチコマンドを使用できます。
     - **Target File Path**: このフィールドには、エクスポートされたファイルを保存するディレクトリが表示されます。ディレクトリを変更するには、ページの右上にある**Change Export Directory**をクリックします。
     - **Last Export**: このフィールドには、最後にエクスポートされた時刻が表示されます。
5. **OK**をクリックします。WSMは毎日午前2時にデータベースを検査して、データエクスポートを実行するかどうかを決定します。WSMがデータベースを即時に検査できるようにするには、ページの右上にある**Export Immediately**をクリックします。

ネットワーク計画の設定

WSMネットワーク計画では、WLANを展開または拡張する前に、APモデル、伝送パワー、およびオンサイト条件に従って、ネットワーク内のAPの場所と数を計画できます。次に、WSMによってネットワーク計画レポートが生成されます。この機能により、WLANの展開効率が向上します。

ワイヤレスネットワークを計画するには、次の情報を参照してください。

- ロケーションビューを作成します。詳細については、「ワイヤレスビューの管理」を参照してください。
- 位置ビュー トポロジーを入力する
- 背景画像を追加する
- 尺度を設定する
- 障害物を描画する
- ネットワーク計画の有効化
- 仮想APの信号カバレッジを表示して、信号カバレッジを完了する
- 仮想APの展開
- ネットワーク計画レポートの生成

この章のすべての操作は、位置ビューで実行されます。

位置ビュー トポロジーを入力する

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management>Location View**を選択します。**Location List**には、すべてのロケーションビューが表示されます。
3. 次のいずれかの方法でロケーションビューを入力します。
   - トポロジーを表示するロケーションの**View Topology**アイコンをクリックします。
   - ターゲットロケーションビューの名前リンクをクリックし、開いたページの右上にある**View Topology**アイコンをクリックします。

   ロケーションビュー トポロジーには、現在のロケーションビュー内のすべてのサブロケーションとAPが表示されます。

背景画像を追加する

1. Topologyページの上部にあるツールバーで、**Add background**アイコンをクリックします。**Topo Background-Picture Setting**ウィンドウが開きます。
2. 次のいずれかの方法を使用して、背景画像を選択します。ローカル画像を使用するには:
   a. ページで**Upload Image**を選択し、**Choose File**をクリックします。ウィンドウが開きます。
   b. 画像を選択し、**Open**をクリックします。
   c. **Topo Background-Picture Setting**ウィンドウで、**Preview**をクリックします。選択した画像がウィンドウに表示されます。

   別の画像を選択するには、**Exit**をクリックします。
   a. **Set**をクリックします。ロケーションビューに背景ピクチャが表示されます。

サーバーの画像を使用するには、次の手順を実行します:

b. **Select from Gallery**を選択します。

c. 画像を選択し、**Set**をクリックします。

選択した画像がロケーションビューに表示されます。

CADファイルを使用するには:

a. **Upload CAD File**を選択し、ページで**Choose File**をクリックします。

ウィンドウが開きます。

b. CADファイルを選択し、**Open**をクリックします。

c. **Topo Background-Picture Setting**ウィンドウで、**Merge into Picture**をクリックします。選択した画像がロケーションビューに表示されます。

GISマップを使用するには:

a. **Use GIS Map**を選択します。

b. 経度と緯度を設定し、**Set**をクリックします。

GISマップは、指定した経度と緯度を中心として位置ビューに表示されます。

3. **Close**をクリックします。

スケールを設定する

適切なスケールを設定して、信号のカバレッジをテストしたり、ワイヤレスネットワークを計画したりします。

尺度を設定するには:

1. トポロジー ページの上部にあるツールバーで、**Set Scale**アイコンをクリックします。
2. 背景画像に線を引きます。

Specify the actual distanceウィンドウが開きます。

3. **Actual Distance**フィールドに値を入力し、測定単位を選択します。オプションは**Meter**と**Feet**。
4. **OK**をクリックします。

障害物を描画する

WSMには、ドア、窓、エレベータなどの障害物が事前に定義されています。障害物は位置ビューに追加できます。

障害物を追加する

1. Topologyページの上部にあるツールバーで、**Add Obstacle**アイコンをクリックします。**Add Obstacle**ウィンドウが開きます。
2. 次のパラメーターを設定します。
   - **Shape**: 次の中から障害物の形状を選択します。
     - **Line**
     - **Polyline**
     - **Rectangle**
     - **Polygon**
     - **Rectangle Area**

- **Type**: 次の中から障害物のタイプを選択します。
  - **Concrete (24dB/m)**
  - **Concrete (24dB/m)**
  - **Dry Wall (30dB/m)**
  - **Window (200dB/m)**
  - **Elevator Shaft (150dB/m)**
  - **Cubical (10dB/m)**
  - **Thin Door (25dB/m)**
  - **Bookshelf (24dB/m)**
- **Thickness(m)**: 障害物の厚さをメートル単位で入力します。
- **Attenuation(dB)**:障害物のタイプと厚さに基づいて自動的に計算されます。

3. **OK**をクリックします。

描画モードになっています。

4. カーソルをドラッグして障害物を描画します。
5. 障害物の描画を終了するには、ダブルクリックします。

作成モードでは、カーソルをドラッグアンドドロップして、同じタイプの障害物をさらに追加できます。

6. トポロジー ページの上部にあるツールバーで、**Pointer**アイコンをクリックして描画モードを終了します。

障害物を修正する

1. 修正する障害物を右クリックし、ショートカットメニューの**Modify**を選択します。
2. 次のパラメーターを変更します。
   - **Serial**: 変更できません。
   - **Shape**: 変更できません。
   - **Type**: 障害物のタイプを修正します。
     - **Concrete (24dB/m)**
     - **Brick Wall (33dB/m)**
     - **Dry Wall (30dB/m)**
     - **Window (200dB/m)**
     - **Elevator Shaft (150dB/m)**
     - **Cubical (10dB/m)**
     - **Thin Door (25dB/m)**
     - **Bookshelf (24dB/m)**
   - **Thickness(m)**: 障害物の厚みをメートル単位で修正します。
   - **Attenuation(dB)**:障害物のタイプと厚さに基づいて自動的に計算されます。
3. **OK**をクリックします。

   修正された障害物がロケーションビューに表示されます。

障害物を削除する

描画モードでは障害物を削除することはできません。障害物を削除する前にトポロジー ページのトップに**Hand**アイコンより**pointer**アイコンが表示されるようにしてください。

障害を削除するには、次の手順に従います。

1. 削除する障害物を右クリックします。
2. 確認ダイアログボックスで、**OK**をクリックします。

ネットワーク計画の有効化

ネットワーク計画を有効にすると、WSMはネットワーク内のAPの数と場所を自動的に計画し、ネットワーク計画レポートを生成します。

ネットワークプランニングをイネーブルにする前に、ロケーションビューですべての仮想APを削除します(存在する場合)。新しい領域を描画することも、古い領域を使用することもできます。

ネットワークプランニングを有効にするには:

1. 空白の領域を右クリックし、ショートカットメニューから**Plan Network** > **Draw Covered Area**の順に選択します。

   Auto Plan Parametersウィンドウがオープンします。
2. 次のパラメーターを設定します。
   - **2.4G**: 2.4GHz無線を有効にするには、このオプションを選択します。このオプションを選択した場合は、無線タイプを選択する必要があります。オプションは**802.11b**、**802.11g**、および**802.11gn**です。
   - **5G**: 5GHz無線を有効にするには、このオプションを選択します。このオプションを選択した場合は、無線タイプを選択する必要があります。オプションは**802.11a**および**802.11an**です。
   - **AP Vendor**: 仮想APのベンダーを選択します。オプションはH3Cです。
   - **AP Model**: 仮想APモデルを選択します。APモデルは、APベンダーとの整合性を保つために自動的にリフレッシュされます。
   - **Minimum Signal Strength(dBm)**: 最小信号強度値を入力します。デフォルトは-70 dBmです。デバイスは-75 dBmを超える信号で検出される必要があります。3つ以上のアクセスポイントの信号検出レベルが-75 dBm未満である必要があります。
   - **Concurrent Online User Count**: 同時オンラインユーザーの許容最大数を入力します。このオプションにより、計画リージョン内の各ユーザーの帯域幅が保証されます。
   - **Per-User Bandwidth(Mbps)**: ユーザーごとの最小帯域幅を入力します。計画リージョン内のユーザーの平均帯域幅は、ユーザーごとの最小帯域幅以上である必要があります。
   - **Power Usage(%)**: 2.4GHzロケーションビュー内のすべてのAPについて、リストから2.4GHz帯域の消費電力値を選択します。このパラメーターはロケーション全体に影響します。たとえば、ロケーションビュー内のあるエリアの消費電力を変更すると、別のエリアの消費電力値も変更されます。
   - **Power Usage(%)**: 5GHzロケーションビュー内のすべてのAPについて、リストから5GHz帯域の電力消費量の値を選択します。このパラメーターはロケーション全体に有効です。たとえば、ロケーションビュー内のあるエリアの電力消費量を変更すると、別のエリアの電力値も変更されます。
3. **OK**をクリックします。

   ネットワーク領域プランニングモードになっています。
4. 背景画像上でカーソルをクリックアンドドラッグし、目的の位置をクリックしてネットワークプランニン

グエリアを描画します。

5. ネットワークリージョンプランニングモードを手動で終了するには、トポロジー ページの上部にあるツールバーの**Pointer**アイコンをクリックします。
6. ダブルクリックして、ネットワークプランニングエリアの描画を終了します。

   システムはネットワーク領域計画モードを自動的に終了します。ネットワーク計画領域は背景画像で強調表示されます。
7. 空白の領域を右クリックし、ショートカットメニューから**Plan Network > Auto Lay APs**を選択します。
8. 青色のAPアイコンは、APを展開する場所を示します。

仮想APの信号カバレッジの表示

ネットワーク計画後、仮想APの信号カバレッジを表示し、カバレッジに基づいてAP番号またはAPロケーションを調整できます。信号カバレッジを表示するには、「信号カバレッジ領域マップの表示」、「色の設定」および「信号カバレッジパラメーターの構成」を参照してください。

仮想APの展開

信号のカバレッジに基づいてAPの展開を調整できます。

現在のロケーションへの仮想APの追加

ネットワークプランニング機能をイネーブルにしたら、1つまたは複数の仮想APをロケーションに手動で追加して、信号展開を完了できます。

現在のロケーションに仮想APを追加するには、次の手順を実行します。

1. 空白の領域を右クリックし、ショートカットメニューから**Add Virtual APs**を選択します。

   Select AP Modelウィンドウが開きます。
2. APモデルを選択し、OKをクリックします。

   ロケーションビューに戻り、**adding virtual AP mode**に入ります。
3. 仮想APを追加する場所をクリックします。追加された仮想APがその場所に表示されます。
4. **ESC**キーを押して、モードを終了します。

仮想APの変更

1. 変更する仮想APを右クリックし、ショートカットメニューから**Modify Virtual AP**を選択します。
2. **AP Label**フィールドに新しいAPラベルを入力します。
3. 無線設定を変更します。

   仮想APモデルによっては、1つまたは複数の無線設定タブが表示される場合があります。設定方法はすべての無線で同じです。この例では、**Radio 1**のパラメーターを変更します。
   - **Model**: 変更できません。
   - **Enable**: 無線を有効または無効にします。
   - **Radio Type**: 無線タイプを次の中から選択します。

     802.11a

     802.11b

802.11g

802.11an

802.11gn

- **Channel**: 無線が動作しているチャネルを選択します。
- **Power(dBm)**: 無線電力をdBm単位で入力します。
- **Bandwidth Mode**: 帯域幅モードを選択します。オプションは**20MHz**および**40MHz**です。このオプションは、無線タイプ**802.11an**および**802.11gn**だけで使用できます。
- **A-MPDU**: A-MPDUを有効または無効にします。このオプションは、無線タイプ**802.11an**および**802.11gn**にのみ使用できます。
- **A-MSDU**: A-MSDUを有効または無効にします。このオプションは、無線タイプ**802.11an**および**802.11gn**でのみ使用できます。
- **Short GI**: ショートGIを有効または無効にします。このオプションは無線タイプ**802.11an**および**802.11gn**だけで使用できます。
- **Antenna**: アンテナを選択します。
- **Angle**: アンテナ角度を0～359の範囲で入力します。**Refresh**をクリックして、仮想APの信号カバレッジエリアを表示します。

4. **OK**をクリックします。

仮想APの削除

1. 削除する仮想APを右クリックし、ショートカットメニューから**Delete Device from this Location**を選択します。
2. 確認ダイアログボックスで、**OK**をクリックします。

すべての仮想APの削除

1. 空白の領域を右クリックし、ショートカットメニューから**Delete All Virtual APs**を選択します。
2. 確認ダイアログボックスで、**OK**をクリックします。

ネットワークプランニングは、ロケーションビューですべての仮想APが削除された後にだけ実行できます。

ネットワーク計画レポートの生成

ネットワーク計画レポートは、ネットワーク計画と信号カバーシミュレーションテストが完了した後に表示するために生成できます。ネットワーク計画レポートは、選択したAPとアンテナの番号と説明、AP導入マップ、および信号カバレッジ予測ヒートマップを含むHTMLファイルです。

ネットワーク計画レポートを生成する手順は、次のとおりです。

1. ネットワークプランニングを有効にした後、トポロジーページの上部にあるツールバーで**Pointer**アイコンをクリックして、ネットワーク領域プランニングモードを終了します。
2. 空白の領域を右クリックし、ショートカットメニューから**Generate Network Planning Report**を選択します。
3. 開いたウィンドウで、レポートを保存するディレクトリを選択し、レポート名を入力して、**OK**をクリックします。

APカリキュレーター

WSMには、特定のパラメーターに基づいてエリア内の必要なAPの数を迅速に計算するためのAPカリキュレーターが用意されています。ネットワーク計画と比較すると、APカリキュレーターには複雑な計画プロセスは必要ありません。

APカリキュレーターを使用するには:

1. ロケーションビュー トポロジーの上にあるツールバーで、**Calculator**アイコン  をクリックしてAP Calculatorを開きます。
2. 表示されるダイアログボックスで、次のパラメーターを設定します。
   - **2.4G**: 2.4GHz無線を有効にするには、このオプションを選択します。このオプションを選択した場合は、無線タイプを選択する必要があります。オプションは、**802.11b**、**802.11g**、および**802.11gn**です。
   - **5G**: 5GHz無線をイネーブルにするには、このオプションを選択します。このオプションを選択した場合は、無線タイプを選択する必要があります。オプションは、**802.11a**、**802.11an**、および**802.11ac/n/a**です。
   - **AP Vendor**: APベンダーを選択します。オプションはH3Cです。
   - **AP Model**: APモデルを選択します。オプションはAPベンダーによって異なります。
   - **Minimum Signal Strength(dBm)**: 対象リージョンで必要な最小信号強度を入力します。デフォルト値は-70 dBmです。
   - **Total Area(m^2)**: 計画領域の総面積を入力します。ワイヤレス信号は領域全体をカバーする必要があります。
   - **Concurrent Online User Count**: 予想される同時オンラインユーザー数を入力します。各ユーザーの帯域幅が同時に確保されている場合は、計画領域内の同時オンラインユーザー数が予想数以上であることを確認してください。
   - **Per-User Bandwidth(Mbps)**: ユーザーごとの最小帯域幅を入力します。計画リージョン内のユーザーの平均帯域幅は、ユーザーごとの最小帯域幅以上である必要があります。
3. 計算をクリックします。**Recommended AP Count**フィールドには、上記の要件を満たすために必要なAPの数が表示されます。
4. 計算をキャンセルするには、**Cancel**をクリックします。

RFの管理

WSM RF管理を使用すると、保守のためにワイヤレス信号カバレッジ領域を表示できます。ワイヤレス信号カバレッジ領域を表示するには、次の情報を参照してください:

- 位置ビュート ポロジーを入力する
- 背景画像を追加する
- スケールを設定する
- 障害物を描画する
- 電波の届く範囲の地図を表示する

注:

APの無線をイネーブルにしているかどうかに関係なく、APの信号カバレッジエリアを信号カバレッジエリアマップに表示できます。

位置ビュー トポロジーを入力する

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > Location View**を選択します。**Location List**には、すべてのロケーションビューが表示されます。
3. 次のいずれかの方法でロケーションビューを入力します。
   - トポロジーを表示するロケーションの**View Topology**アイコンをクリックします。
   - ターゲットロケーションビューの名前リンクをクリックし、開いたページの右上にある**View Topology**アイコンをクリックします。

   ロケーションビュー トポロジーには、現在のロケーションビュー内のすべてのサブロケーションとAPが表示されます。

背景画像を追加する

1. **Topology**ページの上部にあるツールバーで、**Add background**アイコンをクリックします。**Topo Background-Picture Setting**ウィンドウが開きます。
2. 次のいずれかの方法を使用して、背景画像を選択します。ローカル画像を使用するには:
   a. ページで**Upload Image**を選択し、**Choose File**をクリックします。
      ウィンドウが開きます。
   b. 画像を選択し、**Open**.をクリックします。
   c. **Topo Background-Picture Setting**ウィンドウで、Previewをクリックします。選択した画像がウィンドウに表示されます。

   別の画像を選択するには、**Exit**.をクリックします。

   a. **Set**をクリックします。ロケーションビューに背景ピクチャが表示されます。サーバーのピクチャを使用するには、次の手順を実行します:
   a. **Select from Gallery**を選択します。
   b. 画像を選択し、**Set**をクリックします。

選択した画像がロケーションビューに表示されます。

CADファイルを使用するには:

a. **Upload CAD File**を選択し、ページで**Choose File**をクリックします。ウィンドウが開きます。
b. CADファイルを選択し、**Open**をクリックします。
c. **Topo Background-Picture Setting**ウィンドウで、**Merge into Picture**をクリックします。選択した画像がロケーションビューに表示されます。

GISマップを使用するには:

a. **Use GIS Map**を選択します。
b. 経度と緯度を設定し、**Set**をクリックします。
GISマップは、指定した経度と緯度を中心として位置ビューに表示されます。

3. **Close**をクリックします。

スケールを設定する

適切なスケールを設定して、信号のカバレッジをテストしたり、ワイヤレスネットワークを計画したりします。

スケールを設定するには:

1. トポロジー ページの上部にあるツールバーで、**Set Scale**アイコンをクリックします。
2. カーソルが**Plus**記号＋に変わったら、背景ピクチャに線を引きます。**Specify the actual distance**ウィンドウが開きます。
3. **Actual Distance**フィールドに値を入力し、測定単位を選択します。オプションは**Meter**と**Feet**。
4. **OK**をクリックします。

障害物を描画する

WSMには、ドア、窓、エレベータなどの障害物が事前に定義されています。障害物は位置ビューに追加できます。

障害物を追加する

1. **Topology**ページの上部にあるツールバーで、**Add Obstacle**アイコンをクリックします。**Add Obstacle**ウィンドウが開きます。
2. 次のパラメーターを設定します。
   - **Shape**: 次の中から障害物の形状を選択します。
     - **Line**
     - **Polyline**
     - **Rectangle**
     - **Polygon**
     - **Rectangle Area**
   - **Type**: 次の中から障害物のタイプを選択します。
     - **Concrete (24dB/m)**
     - **Brick Wall (33dB/m)**
     - **Dry Wall (30dB/m)**

        - **Window (200dB/m)**
        - **Elevator Shaft (150dB/m)**
        - **Cubical (10dB/m)**
        - **Thin Door (25dB/m)**
        - **Bookshelf (24dB/m)**
    - **Thickness(m)**: 障害物の厚さをメートル単位で入力します。
    - **Attenuation(dB)**: に基づいて自動的に計算されます。
3. **OK**をクリックします。

   描画モードになっています。
4. カーソルをドラッグして障害物を描画します。
5. 障害物の描画を終了するには、ダブルクリックします。

   作成モードでは、カーソルをドラッグアンドドロップして、同じタイプの障害物をさらに追加できます。
6. トポロジー ページの上部にあるツールバーで、**Pointer**アイコンをクリックして描画モードを終了します。

障害物を修正する

1. 修正する障害物を右クリックし、ショートカットメニューの**Modify**を選択します。
2. 次のパラメーターを変更します。
    - **Serial**: 変更できません。
    - **Shape**: 変更できません。
    - **Type**: 障害物のタイプを修正します。
        - **Concrete (24dB/m)**
        - **Brick Wall (33dB/m)**
        - **Dry Wall (30dB/m)**
        - **Window (200dB/m)**
        - **Elevator Shaft (150dB/m)**
        - **Cubical (10dB/m)**
        - **Thin Door (25dB/m)**
        - **Bookshelf (24dB/m)**
    - **Thickness(m)**: 害物の厚みをメートル単位で修正します。
    - **Attenuation(dB)**: に基づいて自動的に計算されます。
3. **OK**をクリックします。

   修正された障害物がロケーションビューに表示されます。

障害物を削除する

描画モードでは障害物を削除することはできません。障害物を削除する前に、トポロジー ページの上部にあるツールバーにポインタ アイコンではなく手のアイコンが表示されていることを確認してください。

障害を削除するには、次の手順に従います。
1. 削除する障害物を右クリックします。
2. 確認ダイアログボックスで、**OK**をクリックします。

電波の届く範囲の地図を表示する

管理者は、信号カバレッジエリアに基づいてAPの展開を調整できます。

信号強度を地図上に表示する

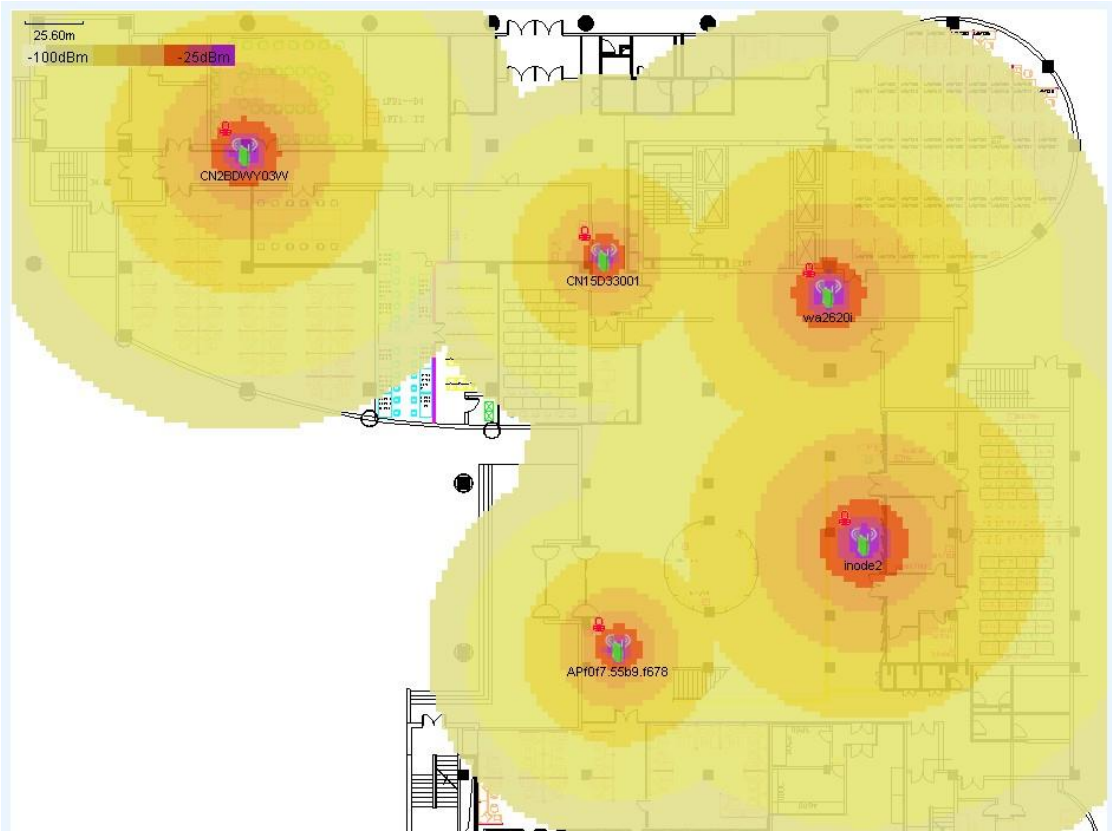
次の方法で、マップ上に信号強度を表示できます。

空白領域を右クリックして、ショートカットメニューから次のいずれかを選択します。

- **Show Signal Coverage > By Signal > 2.4GHz**
- **Show Signal Coverage > By Signal > 5GHz**

マップには、各APの信号カバレッジエリアが表示されます。クリックすると、図74に示すように、信号強度が表示されます。

図74 信号強度の表示(2.4GHz)



マップ上の伝送速度の表示

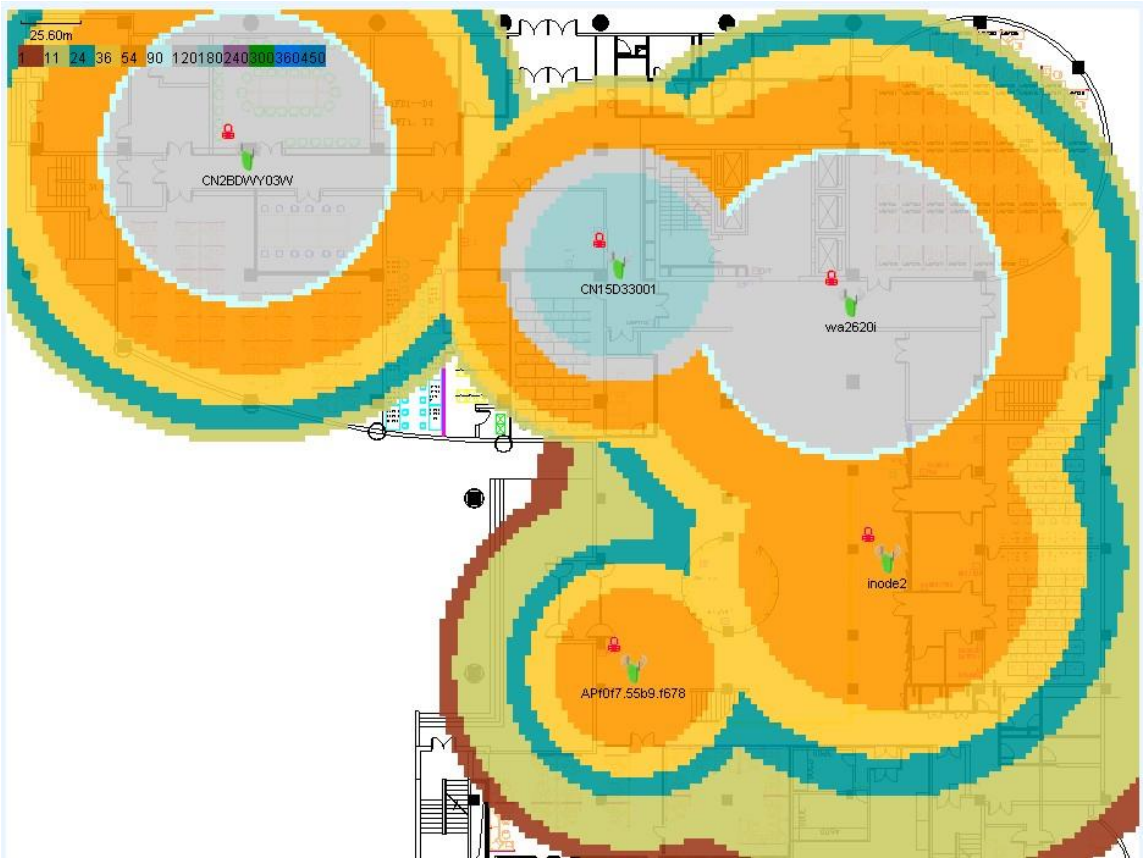
次の方法で、マップ上に伝送速度を表示できます。

空白の領域を右クリックし、ショートカットメニューから次のいずれかを選択します。

- **Show Signal Coverage > By Rate > 2.4GHz**
- **Show Signal Coverage > By Rate > 5GHz**

マップには、各APの信号カバレッジエリアが表示されます。クリックすると、図75に示すように、伝送レートが表示されます。

図75 伝送速度の表示(2.4GHz)



マップ上のAP動作チャネルの表示

次の方法で、マップ上にAP動作チャネルを表示できます。

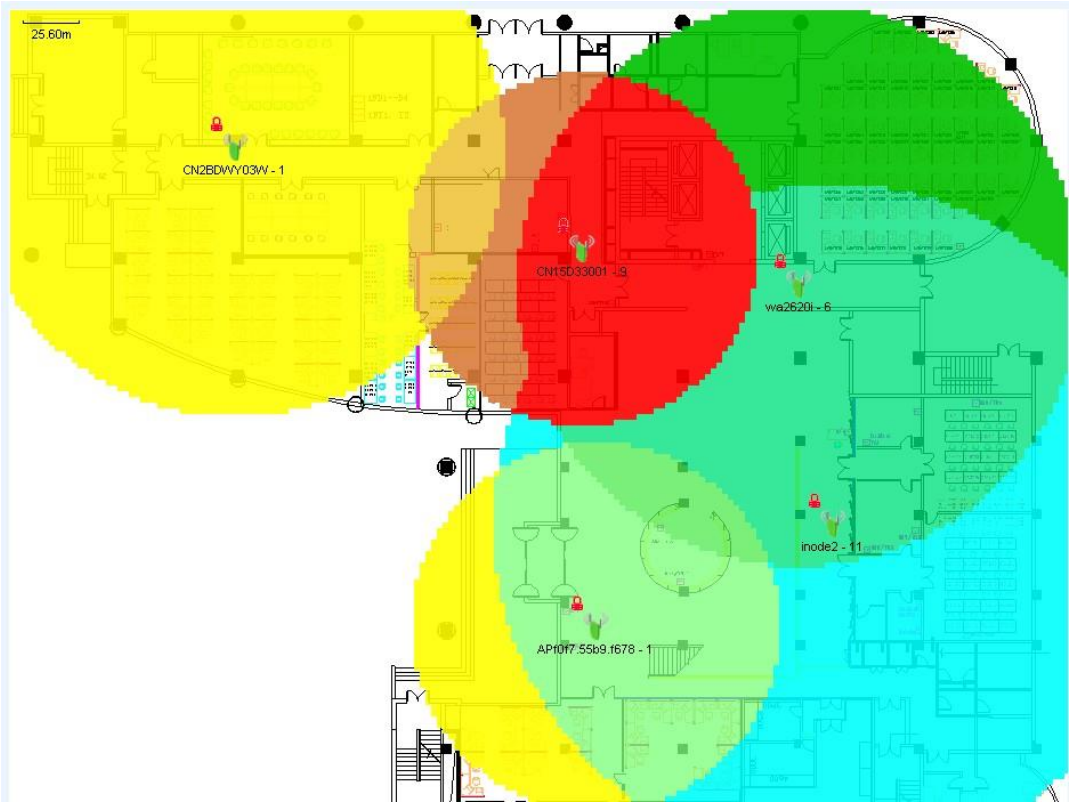
空白領域を右クリックして、ショートカットメニューから次のいずれかを選択します。

- **Show Signal Coverage > By Channel > 2.4GHz**
- **Show Signal Coverage > By Channel > 5GHz**
- **Show Signal Coverage > By Channel > Single Channel**

Single Channelを選択した場合は、Set Channelウィンドウが表示されますので、チャンネル番号を入力して
わかりました。

マップには、各APの信号カバレッジエリアが表示されます。クリックすると、図76に示すように、APの動作
チャネルが表示されます。

図76 動作中のチャネル(2.4GHz)の表示



マップ上の特定のSSIDを使用したAPの表示

次の方法で、マップ上の特定のSSIDを使用してAPを表示できます。

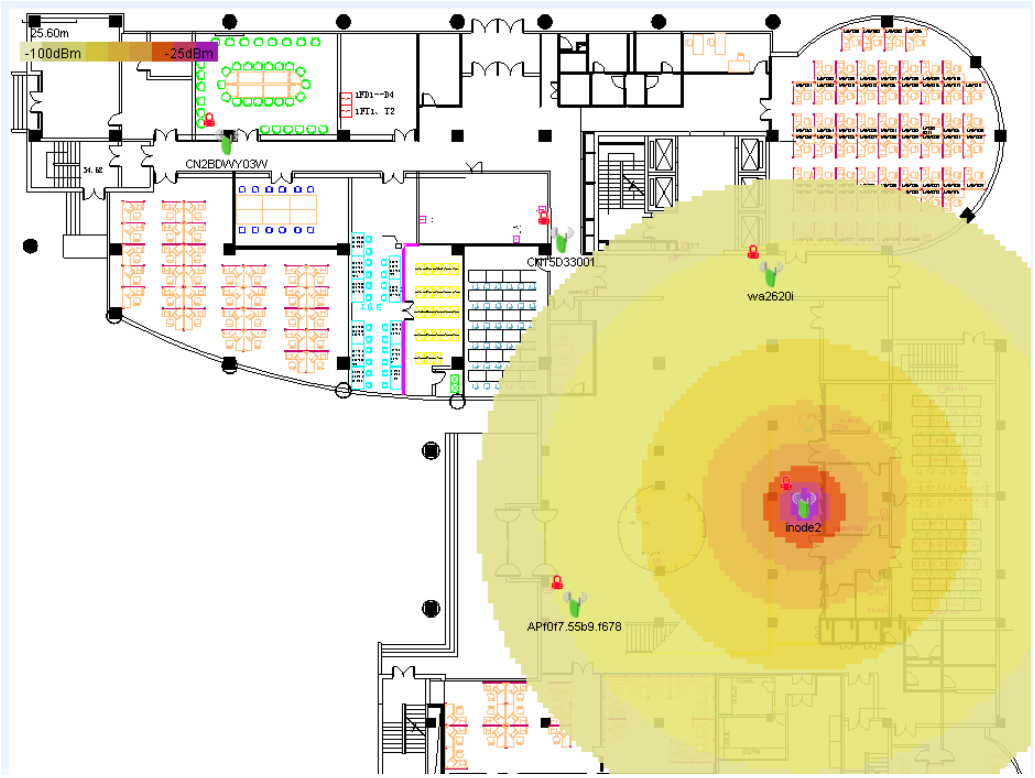
空白領域を右クリックして、ショートカットメニューから次のいずれかを選択します。

- **Show Signal Coverage > By SSID > 2.4GHz**
- **Show Signal Coverage > By SSID > 5GHz**

表示されたウィンドウのSSIDリストからSSIDを選択します。

マップには、選択したSSIDを使用するAPの信号カバレッジエリアが表示されます。クリックすると、図77に示すように、信号強度が表示されます。

図77 特定のSSID(2.4GHz)を使用したAPの表示



RFヒートマップの更新

ツールバーの**Refresh**アイコンをクリックします。

電波の届く範囲を隠す

空白領域を右クリックし、ショートカットメニューの**Hide Signal Cover Area** を選択します。

色を設定する

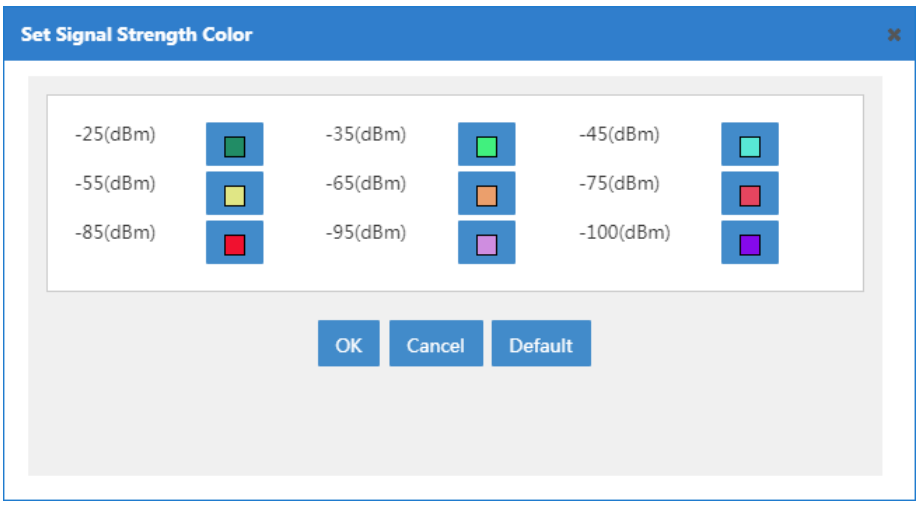
信号カバレッジ予測マップでは、さまざまな信号強度、レート、およびチャネルの色を設定できます。

信号強度の色を設定する

1. 空白の領域を右クリックし、ショートカットメニューから**Color Settings** > **Set Signal Strength Color**を選択します。

   信号強度の色を設定するウィンドウが開き、図78に示すように、信号強度の値とそれに関連する色が表示されます。

図78 信号強度の色の設定

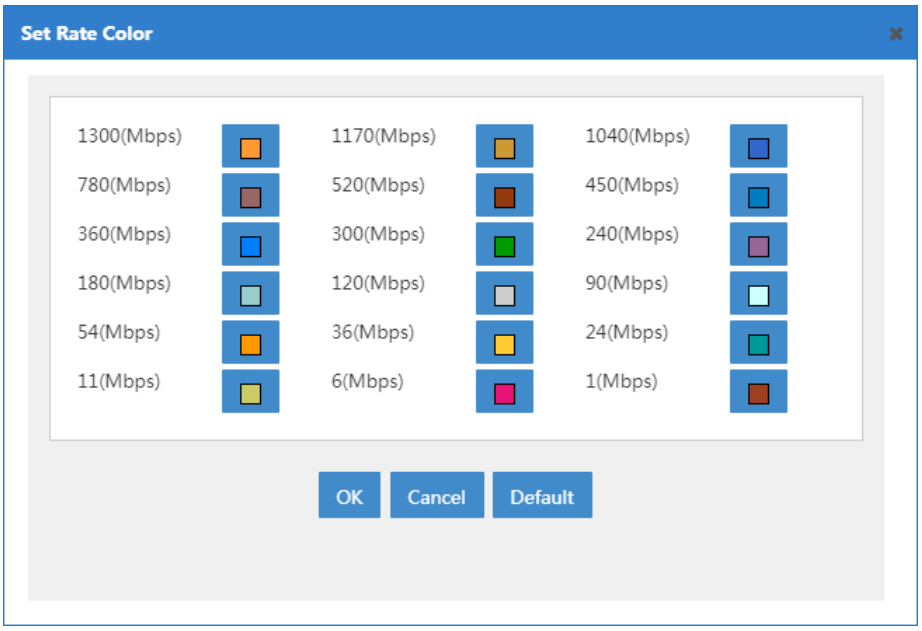


2. 変更するカラーブロックをクリックします。
   色を変更するためのウィンドウが開きます。
3. 色を選択します。
4. **OK**をクリックします。

レートの色を設定する

1. 空白の領域を右クリックし、ショートカットメニューからカラー設定/レートカラーを設定、を選択します。
   図79に示すように、レートカラーを設定するためのウィンドウが開き、レート値とそれに関連するカラーが表示されます。

   図79 レートカラーの設定



2. 変更する色ブロックをクリックします。色
   を変更するためのウィンドウが開きます。
3. 色を選択します。

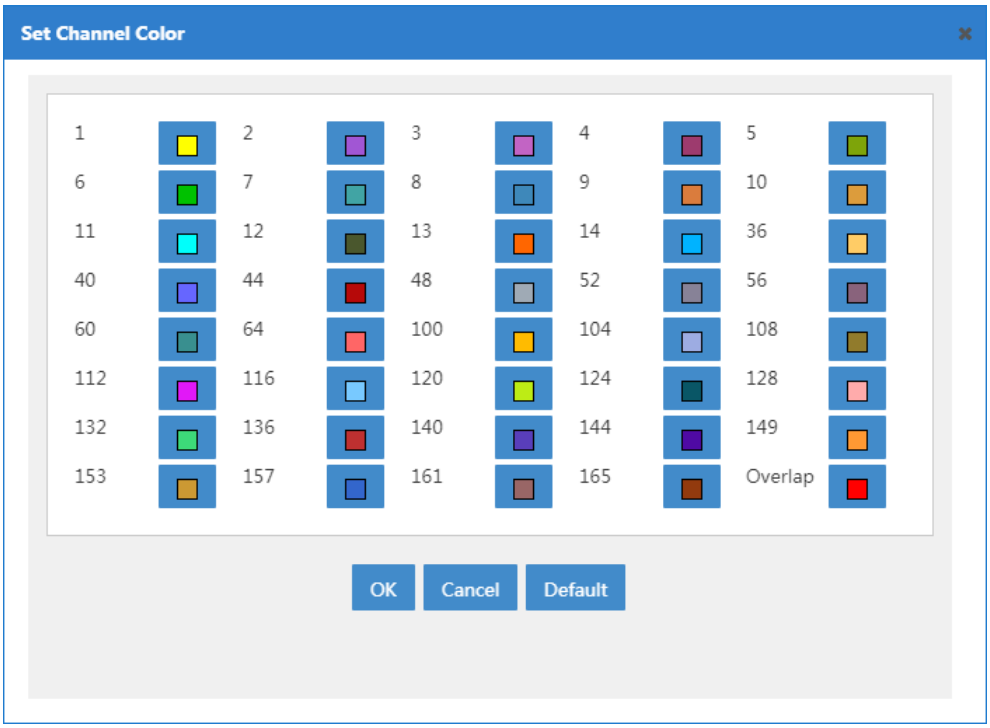
4. **OK**をクリックします。

チャンネルのカラーを設定する

1. 空白の領域を右クリックし、ショートカットメニューからカラー設定/チャンネルカラーの設定を選択します。

   チャンネルカラーを設定するためのウィンドウが開き、図80に示すように、チャンネル値とそれに関連するカラーが表示されます。

   図80 チャンネルカラーの設定



2. 変更する色ブロックをクリックします。色

   を変更するためのウィンドウが開きます。

3. 色を選択します。
4. **OK**をクリックします。

信号カバレッジパラメーターの設定

WSMを使用すると、位置ビューの信号受信感度と消費電力を設定できます。

- **Receive sensitivity**: ロケーションビューでの最小AP信号強度。WSMでは、APと仮想APの両方の**Show Signal Coverage**パラメーターで指定した値よりも弱い信号はロケーションビューに表示されません。
- **Power Usage(%)**: ロケーションビュー内のAPおよび仮想APの帯域内の電力消費量。信号カバレッジパラメーターを設定するには、次の手順を実行します。

1. トポロジーのツールバーで、**Signal Coverage Parameters**アイコンをクリックします。

   Signal Coverage Parametersダイアログボックスが開きます。

2. 次のパラメーターを設定します。

- **Cut Off Signal**: 値を入力するか、スクロールバーを移動して、ロケーションビューに表示する最小信号強度を設定します。
- **Power Usage(%)**: 2.4GHzロケーションビューで2.4GHz帯域の電力消費量の値を入力します。
- **Power Usage(%)**: 5GHzロケーションビューで5GHz帯域の電力消費量の値を入力します。

3. OKをクリックします。

スペクトルガードの管理

スペクトルガードを使用するには、まずスペクトル分析を有効にします。スペクトル分析では、チャネル品質が評価され、監視対象チャネル上の干渉が検出されます。次の干渉を検出できます。

- **Microwave ovens**
- **Bluetooth**
- **Fixed frequency (video)**
- **Cordless phone**
- **Microsoft Xbox**

スペクトルガードモジュールは、次の機能を提供します。

- 無線が常に最適なチャネルで動作するように、チャネル品質に基づいて無線の動作チャネルを自動的に切り替えます。
- スペクトル解析データを要約してグラフおよびチャートに表示します。設定またはWLANレイアウトを調整して、ネットワークパフォーマンスを向上させることができます。

この章では、スペクトルガードモジュールの設定および使用方法について説明します。

APの動作モードの設定

スペクトル分析を使用するには、APがハイブリッドモードまたはモニターモードで動作していることを確認します。APが通常モードで動作している場合、無線は動作チャネルだけを検出します。

APの動作モードを設定するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Fit APs**を選択します。

   Fit **AP List**ページが開きます。
3. APのラベルをクリックします。

   fit AP detailsページが開きます。
4. ページの右側にある**Action**メニューで、**Modify AP Template**アイコンをクリックします。

   Modify AP Templateページが開きます。
5. 動作モードをハイブリッドまたはモニターに設定します。

注:

- ハイブリッドモードとモニターモードを切り替えるには、まず動作モードを通常モードに変更します。
- **Signal Strength by SSID**統計情報を表示するには、APがモニターモードで動作するように設定します。

スペクトル解析の設定

ComwareベースのACでスペクトル分析を設定するには、ACがrfpライセンスを登録していることを確認します。

2.4GHz帯と5GHz帯のスペクトル分析を個別に設定します。スペクトル分析を設定するには、次の手順を実行します:

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > Spectrum Guard**を選択します。

   Spectrum Guardページが開きます。
3. **Device Configuration**リストからACを選択します。
4. **Spectrum Analysis Configuration**をクリックします。

   2.4GHz帯域の**Spectrum Analysis Configuration**ページが開きます。
5. 2.4GHz帯域に次のパラメーターを設定します。
   - **Spectrum Analysis**: スペクトル分析を有効にすると、APは2.4GHz帯域のスペクトル分析を実行できます。
   - **Select interferences**: 検出するデバイスのタイプを次のオプションから選択します。
     - **Microwave Oven**
     - **Bluetooth**
     - **Fixed-Frequency**
     - **Cordless Phone**
     - **Microsoft Xbox**
   - **Interference Alarm**: 干渉に対するアラームの生成を有効または無効にします。干渉アラームを有効にすると、無線が干渉を検出したときにACがIMCにトラップを送信します。
   - **Select interferences**: アラームを生成する干渉デバイスのタイプを選択します。無線が指定された干渉を検出した場合にだけ、ACはIMCにトラップを送信します。次のオプションから選択します。
     - **Microwave Oven**
     - **Bluetooth**
     - **Fixed-Frequency**
     - **Fixed Frequency (Video)**
     - **Cordless Pho**
     - **Microsoft Xbox**

     このフィールドは、干渉アラームをイネーブルにした場合にだけ使用できます。
   - **Channel Quality Alarm**: チャネル品質アラームを有効または無効にします。チャネル品質アラームを有効にすると、チャネル品質が指定したしきい値を下回ると、ACからIMCにトラップが送信されます。
   - **Channel Quality Alarm Threshold**: チャネル品質アラームのトリガー値を1～100の範囲で入力します。このフィールドは、チャネル品質アラームをイネーブルにした場合にだけ使用できます。
   - **Automatic Channel Selection**: 自動チャネル選択をイネーブルまたはディセーブルにします。自動チャネル選択をイネーブルにすると、現在動作しているチャネルの品質が指定したしきい値を下回ると、ACでチャネル調整がトリガーされます。

     現在のチャネルの品質がしきい値を下回ると、ACはAPに新しいチャネルを選択します。ただし、新しいチャネルと古いチャネルのチャネル品質の差が許容レベルを超えるまで、APは新しいチャネルを使用しません。詳細については、関連するデバイスのマニュアルを参照してください。

     自動チャネルスイッチオーバーは、無線が自動モードを採用している場合にだけ実行できます。詳細については、関連するデバイスのマニュアルを参照してください。
   - **Sensitivity Level:** 干渉が検出されたときの自動チャネル選択の感度レベルを選択します。オプションには、Low、Medium、およびHighがあります。感度レベルが高いほど、チャネル切り替えの頻度が高くなります。
6. **OK**をクリックします。

OKをクリックして設定を保存してから、別のページに切り替えます。

7. **5GHz**タブをクリックして、5GHz帯域のパラメーターを設定します。

   5GHz帯域の設定は、検出できる干渉タイプを除いて、2.4GHz帯域の設定と同じです。

8. **OK**をクリックします。

無線の設定

WSMを使用すると、無線設定ページで次の項目を設定できます。

- スペクトル解析の有効化と無効化
- FFTモニタリングの有効化と無効化
- モニタリング用のチャネルの設定。
- スペクトル分析データを表示します。詳細は、「スペクトル分析モニターの管理」を参照してください。

チャネルをスキャンし、チャネル品質を検出し、各チャネルで動作する干渉を検出するには、まず無線のスペクトル分析をイネーブルにする必要があります。

FFT、FFTデューティサイクル、およびスイープスペクトログラムデータを表示するには、まずFFTモニタリングを有効にする必要があります。2.4GHz帯域では、無線はチャネル1～14だけを監視できます。

5GHz帯域の場合、無線はデフォルトでチャネル149～165を監視します。5GHz帯域の監視対象チャネルは変更できます。

無線リストの表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Spectrum Guard > Radio Config**を選択します。

   Radio Listにすべての無線が表示されます。

   Radio List

   - **AP Label**: 無線が属するAPのラベル。APのラベルをクリックすると、詳細が表示されます。
   - **AP SN**: 無線が属するAPのシリアル番号。
   - **AP Model**: 無線が属するAPのモデル。
   - **Radio ID**: APによって割り当てられた無線のID。
   - **Radio Type**: 次のオプションがあります。
     - **802.11a**
     - **802.11b**
     - **802.11g**
     - **802.11an**
     - **802.1gn**
   - **Analysis Status**: 無線のスペクトル分析ステータス。
   - **FFT State**: 無線のFFTイネーブルステータス。
   - **Channels to Monitor**: 無線によって監視されるチャネル。2.4GHz帯域では、無線はチャネル1～14を監視できます。5GHz帯域では、無線はチャネル36～64、100～140、および149～165を監視できます。
   - **Location**: 無線が属するAPのロケーションビューの名前。トポロジーを表示するには、ロケーションビューの名前をクリックします。

- **AC**: (無線が属する)APがアソシエートされているACの名前。ACの名前をクリックすると、その詳細が表示されます。
- **Operation**: 無線が検出したスペクトル分析情報を表示するには、**Operation**アイコン をクリックします。

  Operationメニュー からスペクトル解析モニターを選択して**スペクトル解析モニター履歴。**

Radio Listに十分なエントリーが含まれている場合は、次のナビゲーション支援が表示されます。

- **Next Page**アイコンをクリックして、**Radio List**で次のページに進みます。
- **Last Page**アイコンをクリックして、**Radio List**の最後のページに進みます。
- **Previous Page**アイコンをクリックして、**Radio List**の前のページに戻ります。
- **First Page**アイコンをクリックすると、**Radio List**の先頭に戻ることができます。

ラジオリストの右上にある**8**、**15**、**50**、**100**、または**200**をクリックして、各ページに表示する項目数を指定します。

注:

Radio Listは、**Operation**フィールド以外のすべてのフィールドでソートできます。選択したフィールドでリストをソートするには、列ラベルをクリックします。列ラベルを使用すると、各フィールドに固有の様々なソートオプションを切り替えることができます。

無線の問い合わせ

WSMには、基本問合せと拡張問合せが用意されています。基本問合せ基準には、迅速な検索のためのキーパラメーターがいくつか含まれています。拡張問合せには、正確な照合のための様々な問合せ基準が用意されています。

無線を照会するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Spectrum Guard > Radio Config**を選択します。

   Radio Configページが開きます。
3. 基本的な問い合わせを実行します。
   a. APのデバイスラベルを入力します(大文字と小文字は区別されません)。WSMは、このフィールドのファジーマッチングをサポートします。
   b. **Query**アイコンをクリックします。**Radio Config**ページに、クエリー基準に一致するすべてのAPが表示されます。
4. **Query**フィールドをクリアし、**Query**アイコンをクリックして、すべてのAPを表示します。
5. 高度なクエリーを実行します。
   a. **Query**フィールドの横にある**Expand**アイコンをクリックして**Query**領域を拡張します。再度クリックすると**Query**領域が非表示になります。
   b. 次の問合せ基準を1つ以上入力または選択します。
   - **AP Label**: APラベルを入力します。WSMは、このフィールドのファジーマッチングをサポートします。
   - **Serial Number**: APのシリアル番号を入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
   - **AP Model**: APモデルを入力します。WSMでは、このフィールドのファジーマッチングがサポート

されます。

- **Radio Type**: 無線タイプを入力します。オプションは次のとおりです。
  - **All**
  - **802.11a**
  - **802.11b**
  - **802.11g**
  - **802.11an**
  - **802.11gn**
- **Analysis Status**: 無線のスペクトル分析ステータスを選択します。オプションはAll、Enable、およびDisableです。
- **FFT State**: 無線のFFTステータスを選択します。オプションは、All、Enable、およびDisableです。
- **Location**: 次のいずれかの方法でロケーションを選択します。
  - 無線を使用するAPのロケーションビューを入力します。
  - フィールドをクリックして、表示されるリストからロケーションビューを選択します。
- **AC**: ACを選択します。ACによって管理されるAPのすべての無線がクエリーされます。空のフィールドまたはAllに設定されたフィールドは、クエリー条件として機能しません。

c. **Query**をクリックします。
Radio Listには、クエリー基準に一致するすべての無線が表示されます。

d. **Reset**をクリックして無線を表示するには、**Reset**をクリックします。

スペクトル解析/FFTモニタリングの有効化

無線で干渉をスキャンしたり、APチャネルの品質を監視したり、その他の操作を実行したりするには、まず無線のスペクトル分析を有効にします。FFT、FFTデューティサイクル、またはスイープスペクトログラムのデータを監視、記録、または保存するには、まずFFTモニタリングを有効にする必要があります。

スペクトル分析またはFFTモニタリングを有効にするには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Spectrum Guard > Radio Config**を選択します。
Radio Configページが開きます。
3. **Radio List**から、スペクトル分析またはFFTモニタリングをイネーブルにするAPを選択します。
4. **Enable Analysis**または**Enable FFT**をクリックします。
Result Listページには、各無線の操作結果が表示されます。
5. **Back**をクリックして、**Radio Config**ページに戻ります。

スペクトル解析/FFTモニタリングの無効化

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Spectrum Guard > Radio Config**を選択します。
Radio Configページが開きます。
3. **Radio List**から、スペクトル分析/FFTモニタリングをディセーブルにするAPを選択します。
4. **Disable Analysis**にするまたは**Disable FFT**にする、をクリックします。
Result Listページには、各無線の動作結果が表示されます。
5. **Back**をクリックして、**Radio Config**ページに戻ります。

監視対象チャネルの設定

5GHz帯域では、無線が監視するチャネルを変更できます。チャネルを監視対象として設定するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Spectrum Guard > Radio Config**を選択します。
   Radio Configページが開きます。
3. **Radio List**から、チャネルモニタリングを設定する無線を選択します。
   複数の無線が選択されている場合は、無線が同じ周波数で動作していることを確認します。
4. **Monitor Channels**をクリックします。
   Monitor Channelsウィンドウが開きます。
5. チャンネルレンジを選択します。
   適用されるチャネル範囲は、地域によって異なります。
6. **OK**をクリックします。

現在の干渉の表示

WLAN上の現在の干渉を表示、照会、および検索して、干渉を除去できます。ACでは、次の干渉を検出できます。

- **Microwave Oven**
- **Bluetooth**
- **Fixed-Frequency**
- **Fixed Frequency (Video)**
- **Cordless Phone**
- **Microsoft Xbox**

現在の干渉リストを表示する

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Spectrum Guard > Interference**を選択します。
   Interferenceページが開きます。
3. **Synchronize**をクリックします。
4. 同期化後に、**Interferences**ページを再度開きます。

   Current Interference Listには、すべての干渉が表示されます。

   Current Interference List
   - **Interference Type**: 干渉のタイプ。干渉タイプは次のとおりです。
     - **Microwave Oven**
     - **Bluetooth**
     - **Fixed-Frequency**
     - **Fixed-Frequency (Video)**
     - **Cordless Phone**

  - **Microsoft Xbox**
- **Sensitivity**: 干渉の重大度レベル。範囲は0～100です。値が大きいほど、干渉が大きくなります。
- **RSSI**: 干渉の信号強度。
- **Duty Cycle (%)**: 干渉のデューティサイクル。デューティサイクルは、干渉デバイスがアクティブだった時間です。デバイスのデューティサイクルを表示できます。
- **Affected Channel**: 干渉の影響を受けるチャネル。
- **AP Label**: (干渉を検出した)無線が属するAPのラベル。APのラベルをクリックすると、詳細が表示されます。
- **Location**: 干渉が属する位置ビュー。WSMは、干渉を検出したAPの位置ビューに干渉を配置します。位置ビューのトポロジーを表示するには、位置ビュー名をクリックします。
- **Detected Time**: APが干渉を検出した時間。
- **Operation**:干渉の**Operation**アイコン⋯をクリックして、**Operation**メニューを表示します。**Operation**メニューから**View Topology**を選択して、トポロジー内の干渉を特定できます。

Current Interference Listに十分なエントリーがある場合は、次のナビゲーションツールが表示されます。

- **Next Page**アイコンをクリックして、**Current Interference List**内で次のページに進みます。
- **Last Page**アイコンをクリックすると、**Current Interference List**の最後に進むことができます。
- **Previous Page**アイコンをクリックすると、**Current Interference List**内で前のページに戻ります。
- **First Page**アイコンをクリックすると、**Current Interference List**の先頭に戻ることができます。

現在の干渉リストの右上にある**8**、**15**、**50**、**100**、または**200**をクリックして、各ページに表示する項目数を指定します。

注:

現在の干渉リストは、操作フィールド以外のすべてのフィールドで並べ替えることができます。列ラベルをクリックすると、選択したフィールドでリストを並べ替えることができます。列ラベルを使用すると、各フィールドに固有のさまざまな並べ替えオプションを切り替えることができます。

現在の干渉の照会

WSMには、基本問合せと拡張問合せが用意されています。基本問合せ基準には、迅速な検索のためのキーパラメーターがいくつか含まれています。拡張問合せには、正確な照合のための様々な問合せ基準が用意されています。

現在の干渉をクエリーするには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Spectrum Guard > Interference**を選択します。

   Interferenceページが開きます。
3. 基本的なクエリーを実行します。
   a. APのデバイスラベルを入力します(大文字と小文字は区別されません)。WSMは、このフィールドのファジーマッチングをサポートします。
   b. **Query**アイコンをクリックします。**Interference List**」に、問合せ基準に一致するすべての干渉が表示されます。
4. **Query**フィールドをクリアし、**Query**アイコンをクリックしてすべての干渉を表示します。
5. 高度なクエリーを実行します。

a. **Query**フィールドの横にある**Expand**アイコンをクリックして**Query**領域を拡張します。再度クリックするとQuery領域が非表示になります。

b. 次の問合せ基準を1つ以上入力または選択します。

- **AP Label**: APラベルを入力します。WSMは、このフィールドのファジーマッチングをサポートします。
- **Affected Channel**: 影響を受けるチャンネルを入力します。このチャンネルの干渉はすべて照会されます。WSMでは、このフィールドのファジーマッチングはサポートされていません。
- **Interference Type**: 干渉のタイプを選択します。オプションは次のとおりです。
  - **Unlimited**
  - **Microwave Oven**
  - **Bluetooth**
  - **Fixed-Frequency (Video)**
  - **Cordless Phone**
  - **Microsoft Xbox**
- **Location**: 干渉の位置を入力します。またはフィールドをクリックして、表示されるリストから干渉の位置を選択します。

  空のフィールドや**Unlimited**に設定されたフィールドは、クエリーの抽出条件にはなりません。

c. **Query**をクリックします。

Current Interference Listには、クエリー基準に一致するすべての干渉が表示されます。

d. クエリー基準をクリアしてすべての干渉を表示するには、**Reset**をクリックします。

干渉を検出する

この機能を使用すると、干渉を検出したAPのトポロジー ビューで干渉を特定できます。

干渉を検出するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Spectrum Guard > Interference**を選択します。

   Interferenceページが開きます。
3. ターゲット干渉の**Operation**アイコン をクリックし、ショートカットメニューの**View Topology**を選択します。

   トポロジーウィンドウが開き、位置ビューで干渉が赤いボックスで囲まれます。

干渉履歴を管理する

WSMを使用すると、干渉タイプ、感度、検出時間、位置などの干渉履歴を表示できます。

干渉履歴の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Spectrum Guard > Interfere Data**を選択します。

   Interfere Dataページが開きます。

   Interference History List
   - **Interference Type**: 干渉のタイプ。オプションは次のとおりです。

  - **Microwave Oven**
  - **Bluetooth**
  - **Fixed-Frequency (Video)**
  - **Cordless Phone**
  - **Microsoft Xbox**
- **Sensitivity**:干渉の重大度レベル。範囲は0～100です。値が大きいほど、干渉が大きくなります。
- **RSSI**: 干渉の信号強度。
- **Duty Cycle (%)**: 干渉のデューティサイクル。デューティサイクルは、干渉デバイスがアクティブだった時間です。デバイスのデューティサイクルを表示できます。
- **Affected Channel:** 干渉の影響を受けるチャネル。
- **AP Label**: (干渉を検出した)無線が属するAPのラベル。
- **Location**: 干渉が属する位置ビュー。
- **Detected Time**: APが干渉を検出した時間。
- **Last Disappeared**: 干渉が消失した時刻。

干渉履歴リストに十分なエントリーがある場合は、次のナビゲーション支援が表示されます。

- **Next Page**アイコンをクリックして、**Interference History List**で次のページに進みます。
- **Last Page**アイコンをクリックして、**Interference History List**の最後に進みます。
- **Previous Page**アイコンをクリックして、**Interference History List**で前のページに戻ります。
- **First Page**アイコンをクリックして、**Interference History List**の先頭に戻ります。

干渉履歴リストの右上にある**8**、**15**、**50**、**100**、または**200**をクリックして、各ページに表示する項目の数を指定します。

干渉履歴の照会

WSMには、基本問合せと拡張問合せが用意されています。基本問合せ基準には、迅速な検索のためのキーパラメーターがいくつか含まれています。拡張問合せには、正確な照合のための様々な問合せ基準が用意されています。

干渉履歴を照会するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Spectrum Guard > Interfere Data**を選択します。

   Interfere Dataページが開きます。
3. 基本的なクエリーを実行します。
   a. APのデバイスラベルを入力します(大文字と小文字は区別されません)。WSMは、このフィールドのファジーマッチングをサポートします。
   b. **Query**アイコンをクリックします。**Interfere Data**ページに、問合せ基準に一致するすべての干渉データが表示されます。
4. **Query**フィールドをクリアして**Query**アイコンをクリックすると、すべての干渉データが表示されます。
5. 高度なクエリーを実行します。
   a. **Query**フィールドの横にある**Expand**アイコンをクリックして**Query**領域を拡張します。再度クリックすると**Query**領域が非表示になります。
   b. 次の問合せ基準を1つ以上入力または選択します。

- **AP Label**: APのラベルを入力します。WSMは、このフィールドのファジーマッチングをサポートします。
- **Affected Channel**: 影響を受けるチャンネルを入力します。このチャンネルの干渉はすべて照会されます。WSMでは、このフィールドのファジーマッチングはサポートされていません。
- I**nterference Type**: 干渉のタイプを選択します。オプションは次のとおりです。
  - **Unlimited**
  - **Microwave Oven**
  - **Bluetooth**
  - **Fixed Frequency (Video)**
  - **Cordless Phone**
  - **Microsoft Xbox**

  空のフィールドや**Unlimited**に設定されたフィールドは、クエリーの抽出条件にはなりません。

c. **Query**をクリックします。

Interferences History Listには、クエリー基準に一致するすべての干渉履歴が表示されます。

d. クエリー基準をクリアしてすべての干渉履歴を表示するには、**Reset**をクリックします。

APチャネル品質の管理

APチャネル品質とは、チャネルの品質を指します。チャネル品質が高いほど、干渉が少なくなり、チャネル上のクライアントのWLANアクセスが改善されます。

APチャネル品質リストの表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Spectrum Guard > Channel Quality**を選択します。**Channel Quality**ページが開きます。
3. 同期をクリックします。

   AP Channel Quality List
   - **AP Label**: チャネルを監視するAPのラベル。APのラベルをクリックすると、その詳細が表示されます。
   - **Radio ID**: チャネルを監視するAPの無線のID。
   - **Monitored Channel**: APが監視するチャネル。
   - **Average Quality**: チャネル評価の平均スコア。範囲は1～100です。値が大きいほど品質が高いことを示します。
   - **Worst Quality**: チャネルの最低品質スコア(1～100)。
   - **Interference Count**: チャネル上の干渉の数。
   - **Noise Floor**: 無線のノイズフロア(dBm単位)。ノイズフロアはチャネル品質に影響し、温度によって変化します。

AP Channel Quality Listに十分なエントリーがある場合は、次のナビゲーションツールが表示されます。

- **Next Page**アイコンをクリックして、**AP Channel Quality List**で次のページに進みます。
- **Last Page**アイコンをクリックして、**AP Channel Quality List**の最後のページに進みます。
- **Previous Page**アイコンをクリックして、**AP Channel Quality List**の前のページに戻ります。
- **First Page**アイコンをクリックすると、**AP Channel Quality List**の先頭ページに戻ることができ

ます。

AP Channel Quality Listの右上にある**8**、**15**、**50**、**100**、または**200**をクリックして、各ページに表示する項目数を指定します。

APチャネル品質のクエリー

WSMには、基本問合せと拡張問合せが用意されています。基本問合せ基準には、迅速な検索のためのキーパラメーターがいくつか含まれています。拡張問合せには、正確な照合のための様々な問合せ基準が用意されています。

APチャネル品質を照会するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Spectrum Guard > Channel Quality**を選択します。**Channel Quality**ページが開きます。
3. 基本的なクエリーを実行します。
   a. APのデバイスラベルを入力します(大文字と小文字は区別されません)。WSMは、このフィールドのファジーマッチングをサポートします。
   b. **Query**アイコンをクリックします。**Channel Quality**ページに、問合せ基準に一致するすべてのチャネルが表示されます。
   c. **Query**フィールドをクリアし、**Query**アイコンをクリックしてすべてのチャネルを表示します。
4. 高度なクエリーを実行します。
   a. **Query**フィールドの横にある**Expand**アイコンをクリックして**Query**領域を拡張します。再度クリックすると**Query**領域が非表示になります。
   b. 次の問合せ基準を1つ以上入力します。
   - **AP Label**:チャネルをモニタリングする無線を使用するAPのラベルを入力します。WSMは、このフィールドのファジーマッチングをサポートします。
   - **Channel:** チャンネルの番号を入力します。WSMでは、このフィールドのファジーマッチングはサポートされていません。

     空のフィールドは、クエリー条件として使用できません。

   c. **Query**.をクリックします。

      AP Channel Quality Listには、クエリー基準に一致するすべてのAPチャネル品質が表示されます。
   d. クエリー基準をクリアしてすべてのAPチャネル品質を表示するには、Resetをクリックします。

スペクトル解析モニターの管理

スペクトル分析モニターは統計情報を収集し、チャネル使用率、チャネル品質、干渉信号強度、FFT、スイープスペクトログラム、およびSSID別の信号強度のトレンドグラフと棒グラフを描画します。

スペクトル解析モニターデータの表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Spectrum Guard > Radio Config**を選択します。

   Radio Configページが開きます。
3. 干渉の**Operation**アイコン をクリックし、スペクトル解析モニターをクリックします。
タブを選択します。

スペクトル解析モニターウィンドウが開きます。

4. 次のモニターパラメーターを設定します。
   - **Statistics**: スペクトラム解析モニター情報の種類を選択します。オプションは:
     - **Channel Usage**
     - **Channel Usage Trend**
     - **Channel Quality**
     - **Channel Quality Trend**
     - **Interference Signal Strength**
     - **FFT**
     - **FFT Duty Cycle**
     - **Swept Spectrogram**
     - **Signal Strength by SSID**
   - Radio ID: チャネルの監視に使用する無線を選択します。

図81 チャネル使用棒グラフ

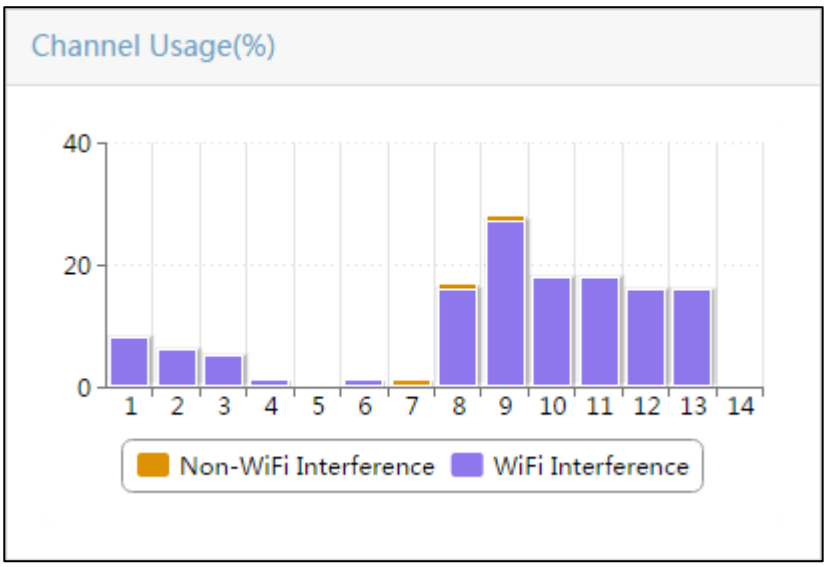
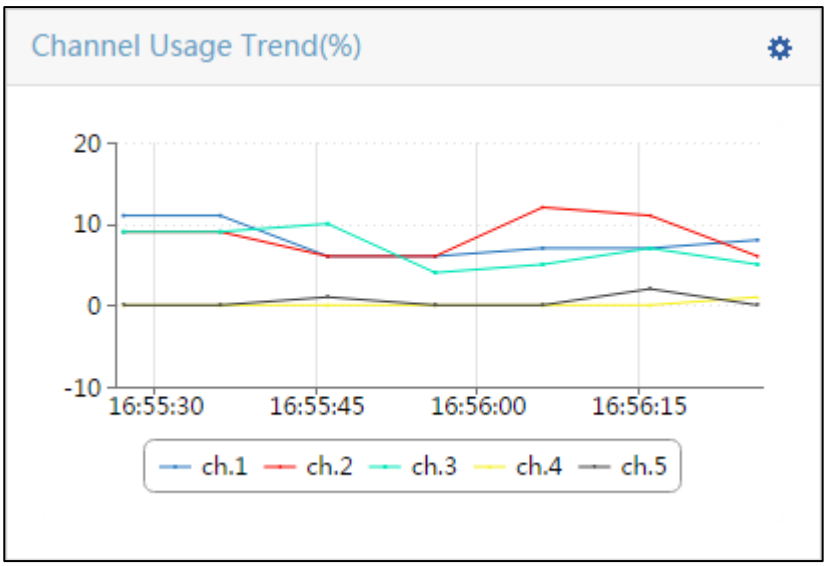


図82は、チャネル使用率のトレンドグラフを示しています。

図82 Channel Usage Trendグラフ



チャネルを指定するには:

a. グラフの右上にある**Select Channel**アイコンをクリックします。
Select Channel ウィンドウが開きます。

b. 監視するチャネルを指定するには、チャネルを選択して をクリックします。監視を停止するチャネルを指定するには、チャネルを選択して をクリックします。すべてのチャネルを監視するには、をクリックします。すべてのチャネルの監視を停止するには、をクリックします。

c. **OK**をクリックします。

図83は、チャネル品質の棒グラフを示しています。

図83 チャネル品質の棒グラフ

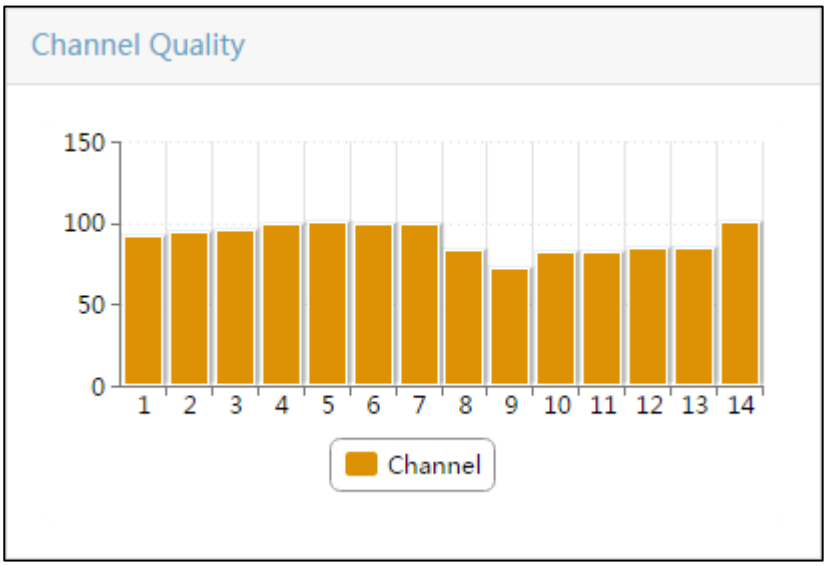
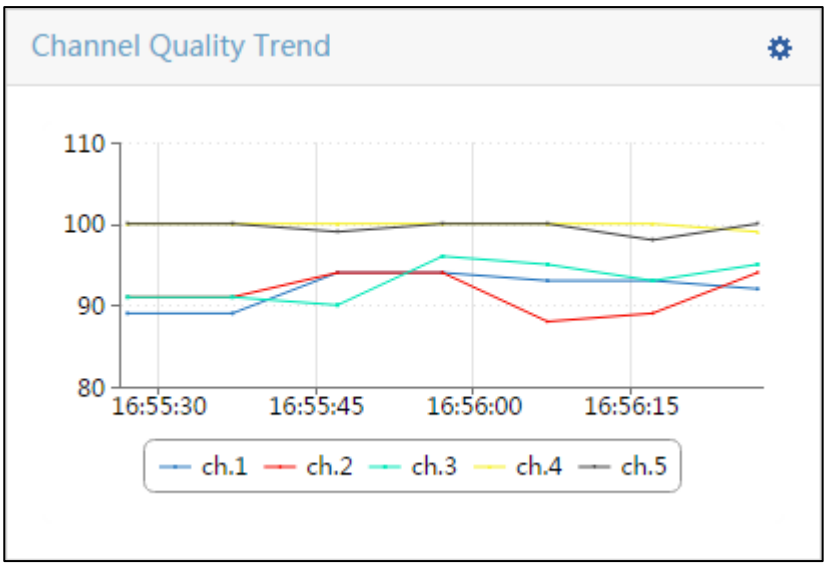


図84は、チャネル品質トレンドグラフを示しています。

図84 チャネル品質の傾向グラフ



チャネルを指定するには:

a. **Select Channel**アイコンをクリックします。

   Select Channelウィンドウが開きます。

b. 監視するチャネルを指定するには、チャネルを選択してをクリックします。監視を停止するチャネルを指定するには、チャネルを選択してをクリックします。すべてのチャネルを監視するには、をクリックします。すべてのチャネルの監視を停止するには、をクリックします。

c. **OK**をクリックします。

   図85に干渉信号強度のグラフを示します。

   図85 干渉信号強度グラフ

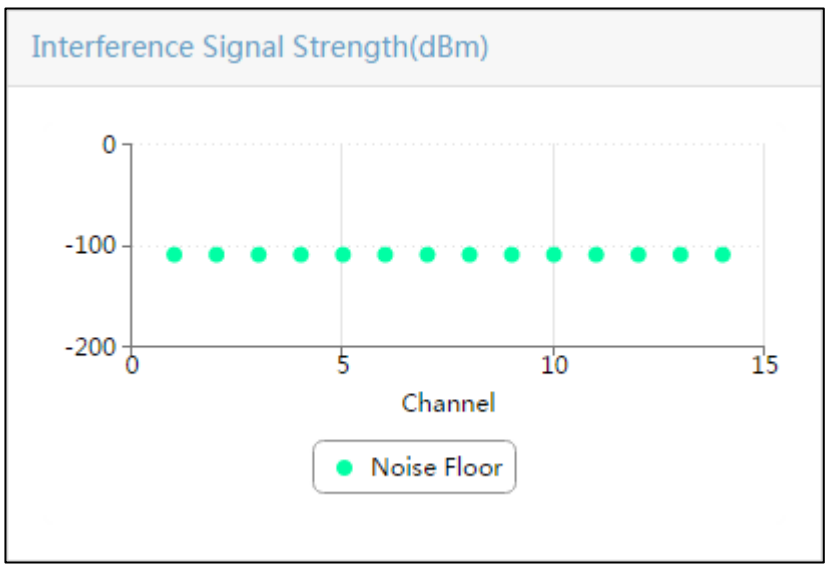
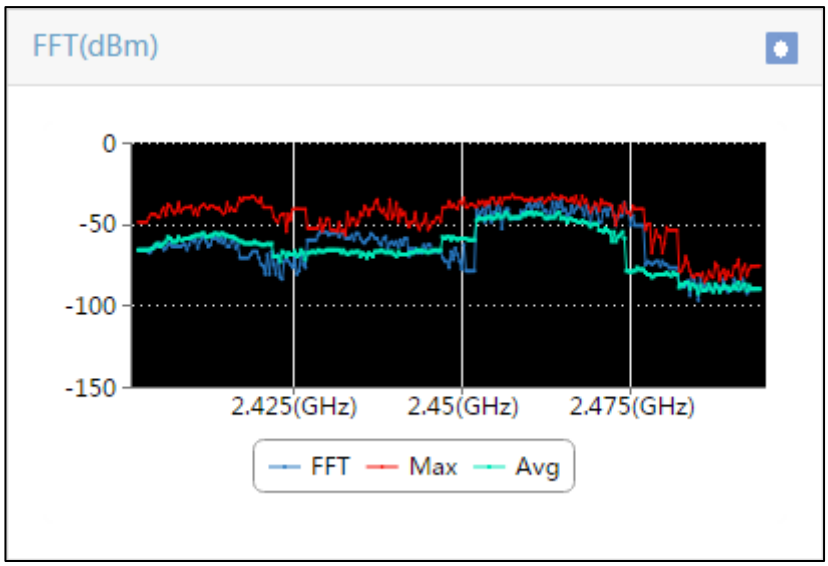


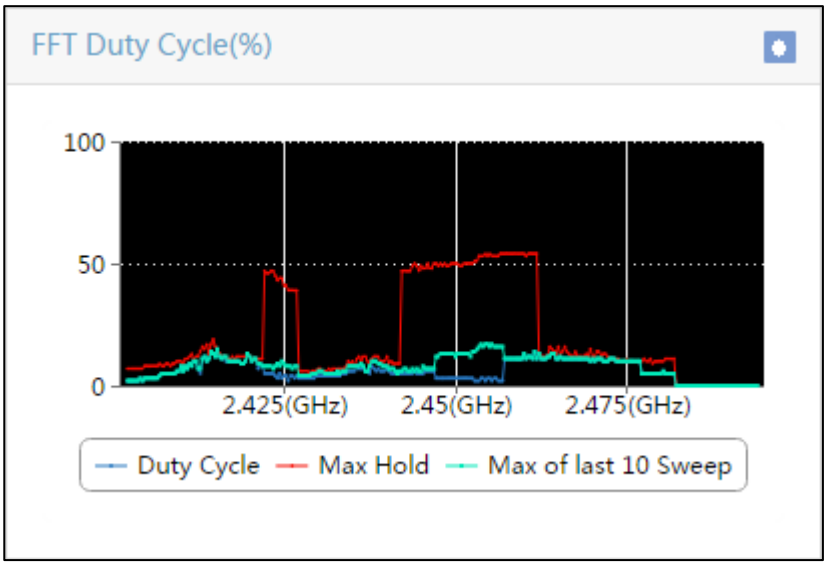
図86は、FFTモニターのトレンドグラフを示しています。

図86 FFTモニターのトレンドグラフ



- FFTのモニターデータを記録およびエクスポートするには、「スペクトル分析モニターデータの記録とエクスポート」を参照してください。
  - **FFT**: 周波数での干渉信号強度。
  - **Max**: 周波数での最大干渉信号強度。
  - **Avg**: 周波数での干渉信号の平均強度。図87は、FFTデューティサイクルのトレンドグラフを示しています。

図87 FFTデューティサイクルの傾向グラフ

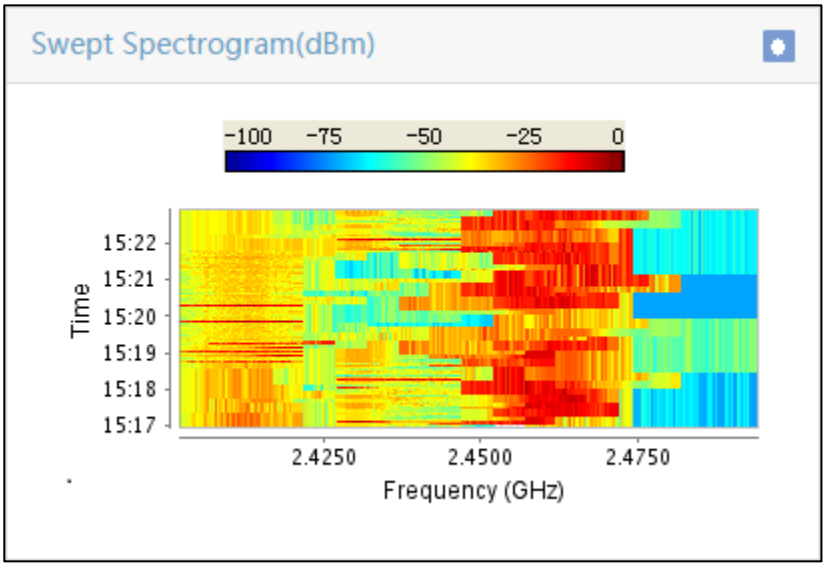


FFT Duty Cycleのモニターデータを記録およびエクスポートするには、「スペクトル分析モニターデータの記録とエクスポート」を参照してください。

- **Duty Cycle**: 周波数上の干渉信号のデューティサイクル。
- **Max Hold**: 周波数上の干渉信号の最大デューティサイクル。
- **Max of last 10 Sweep**: 最後の10回のスイープにおける周波数上の干渉信号の最大デューティサイクル。

図88は掃引スペクトログラムグラフを示す。

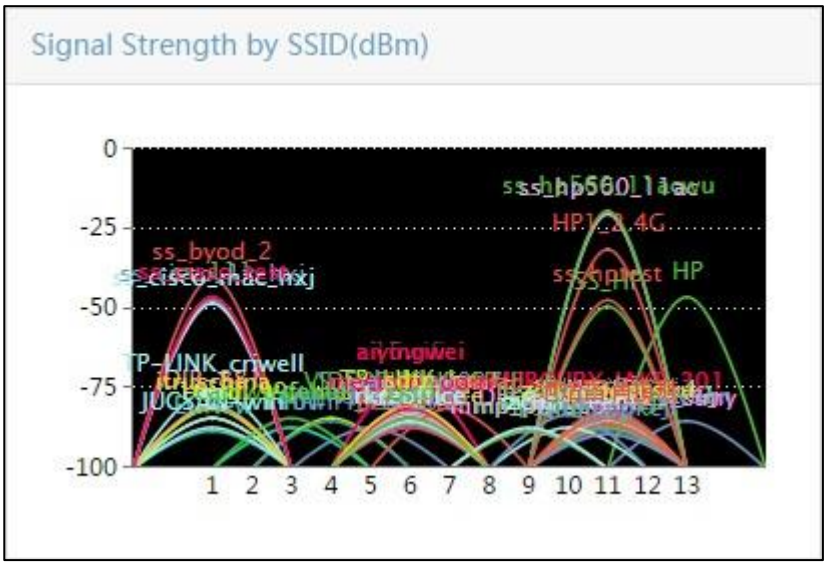
図88 掃引スペクトログラムグラフ



FFTのモニターデータを記録およびエクスポートするには、「スペクトル分析モニターデータの記録とエクスポート」を参照してください。

図89は、SSIDグラフによる信号強度を示しています。

図89 SSID別の信号強度(dBm)



5. **Monitor**.をクリックします。

   WSMは、モニターの統計情報を収集し、グラフやチャートで表示します。

6. **Stop Monitor**をクリックします。

   グラフとチャートには、最後に更新されたモニターデータが表示されます。

スペクトル分析モニターデータの記録と書き出し

1. **Service**タブをクリックします。

2. ナビゲーションツリーで、**WLAN Manager > Spectrum Guard > Radio Config**を選択します。

   Radio Configページが開きます。
3. 干渉の**Operation**アイコン をクリックし、**Spectrum Analysis Monitor**タブをクリックします。

   Spectrum Analysis Monitorウィンドウが開きます。
4. 次のパラメーターを設定します。
   - **Statistics**: 記録およびエクスポートするスペクトル分析モニター情報のタイプを選択します。オプションは、**FFT**、**FFT Cycle**および**Swept Spectrogram**です。
   - **Radio ID**:スペクトル分析モニタリングの無線のIDを選択します。
5. **Monitor**.をクリックします。

   WSMは、モニターの統計情報を収集し、グラフやチャートで表示します。
6. グラフの右上にある**Start Recording**アイコン をクリックします。
7. グラフの右上にある**Stop Recording**アイコン をクリックします。
8. グラフの右上にある**Save Recordings**アイコン をクリックします。

   Download Exported Template Fileダイアログボックスが開きます。

注:
Internet Explorerブラウザを使用している場合は、**Tools** > **Internet Options** > **Security** > **Internet** > **Custom level** > **Downloads**,を選択し、ファイルをエクスポートする前に**Automatic Prompting for file downloads**を有効にします。

9. **Export Result**をクリックします。

   Download Exported Template Fileダイアログボックスが開きます。
10. **Save**をクリックします。
11. **OK**をクリックします。

スペクトル分析モニターの履歴の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > Spectrum Guard**を選択します。

   Spectrum Guardページが開きます。
3. **AP Spectrum Analysis**リストで、**Spectrum Analysis Monitor History**リンクをクリックします。

   Spectrum Analysis Monitor Historyウィンドウが開きます。
4. 次のパラメーターを設定します。
   - **Statistics**:スペクトル分析モニター情報のタイプを選択します。
   - **Select File**: **Select File**で、次のいずれかの操作を行います。
     - ファイルの絶対パスを入力します。
     - **Browse**をクリックしてファイルを開きます。
   - **Start Time**: **Start Time**で、次のいずれかを実行します。
     - 履歴データの開始時刻をYYYY-MM-DD hh:mm形式で入力します。
     - 開始時刻を選択するには、**Calendar**アイコンをクリックします。
   - **Stop Time**: **Stop Time**で、次のいずれかを実行します。
     - 履歴データの終了時刻をYYYY-MM-DD hh:mm形式で入力します。

– 終了時刻を選択するには、**Calendar**アイコン  をクリックします。

開始時刻も停止時刻も指定しない場合は、ファイルのすべてのデータが表示されます。

5. **Query**をクリックします。

   グラフには、指定した期間のデータが表示されます。

6. **Close**をクリックします。

ワイヤレス位置確認の管理

WSMワイヤレスロケーティングを使用すると、802.11ネットワーク内のワイヤレスクライアント(WiFi携帯電話、PDA、iNodeクライアントがインストールされた端末、およびラップトップ)およびAPの位置を特定できます。

概要

検索モード

WSMは、Location Awareロケーティング、BLEロケーティング、コンバージドLocation AwareおよびBLEロケーティング、X-Shareロケーティング、APベースのロケーティング、およびGISロケーティングをサポートしています。

リアルタイム検索(BLE検索、Location Aware検索、およびLocation AwareとBLEを統合した検索)、X-Share検索、およびAPベースの検索によって取得されたロケーションの優先順位は、降順になっています。上記のすべての検索方法でクライアントの検索に失敗した場合、WSMは、クライアントが関連付けられたAPの近くにあると想定します。

Location Awareによる検索

Location Awareによる検索では、Round Trip Time(RTT)を使用して、クライアントをリアルタイムで検索します。

Location Aware検索に使用できるのは、Location Aware検索をサポートするAPだけです。Location

Aware検索は、クライアントの検索に加えて、次の機能をサポートしています。

- ロケーションビューでクライアントをリアルタイムで追跡する。
- ロケーションビューで線を使用してクライアントトラックを表示する。
- ロケーションビューにクライアントトラックを動的に表示する。
- 指定した期間の各クライアントのヒートマップをロケーションビューで表示できます。
- デジタルフェンスを描画して、エリア内の位置を収集できます。

BLE位置確認

BLE位置特定は、WLAN内のビーコンによって検出された相対的な信号強度をリアルタイムで三角測量することによって、クライアントの位置を決定します。位置認識位置特定と比較して、BLE位置特定はコストが低く、より正確です。

BLE位置確認を実行する前に、ビーコンを展開する必要があります。

クライアントの検索に加えて、BLE検索は次の機能をサポートしています。

- ロケーションビューでクライアントをリアルタイムで追跡する。
- ロケーションビューで線を使用してクライアントトラックを表示する。
- ロケーションビューにクライアントトラックを動的に表示する。
- 指定した期間の各クライアントのヒートマップをロケーションビューで表示できます。

X-Shareの場所

X-Shareロケーティングに使用できるのは、X-Shareアンテナをサポートするだけです。X-Shareロケーティングを使用するには、実際の状況に応じてロケーションビューの正しい場所にX-Shareアンテナア

イコンを配置します。APは、クライアントの大まかなロケーションを取得できます。X-Shareロケーティングが失敗した場合、WSMはクライアントがX-Shareアンテナの近くにあると想定します。

APベースのワイヤレス位置確認

APベースのワイヤレスロケーティングでは、APがワイヤレス信号をスキャンして、ワイヤレスクライアント(不正なクライアントを含む)および不正なAPの位置を特定します。たとえば、サンプリングAPは、クライアントと各AP間の距離を推定します。その後、WSMはクライアントの大まかな位置を取得し、それをロケーションビューに表示できます。

GIS検索

GIS検索は、GISビューで実行されます。GIS検索を実行する前に、GISビューに位置ビューを追加し、経度と緯度を設定します。その後、WSMは、位置ビューに従って、GISビューでFIT AP、FAT AP、またはクライアントを検索できます。

既定では、Map WorldはGISビューにロードされます。Map worldをロードできるように、IMCがインターネットに接続できることを確認してください。

GISによる位置特定は、通常、複数の支店を持つ企業に適用されます。

用語

- **Received Signal Strength Indicator**: RSSIは、受信信号強度を示します。WSMは、RSSIを使用してワイヤレス位置確認を実装します。
- **Location view**: 無線ロケーションおよびRF管理用にWSMで定義されたビュー。無線ロケーション機能を使用する前に、ロケーションビューを作成し、バックグラウンドピクチャを設定し、ロケーションビューでスケーリングする必要があります。
- **GIS view**: GIS検索用にWSMで定義されたビュー。
- **Background picture**: バックグラウンドピクチャは、トポロジー上の実際のネットワーク環境を反映します。位置特定のパフォーマンスを確保するには、バックグラウンドピクチャに正しいスケールを設定し、サンプリングAPとサンプリングポイントをバックグラウンドピクチャ上の正しい位置に配置します。

ロケーションビューを設定する

この設定は、ワイヤレスロケーティングの基本です。

ロケーションビューを作成する

ロケーションビューの作成については、「ロケーションビューを管理する」を参照してください。

背景画像を設定する

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager** > **Wireless Topology**を選択します。

   ワイヤレストポロジーウィンドウが開きます。
3. 左側のナビゲーションツリーから、背景ピクチャを設定するロケーションビューを入力します。
4. Topologyページの上部にあるツールバーで、**Add background**アイコンをクリックします。**Topo**

Background-Picture Settingウィンドウが開きます。

5. 背景画像を選択:
   a. ローカルの画像またはIMCデータベースのギャラリーの画像を使用できます。

      To use a local picture: **User Upload Picture**を選択し、**Browse**をクリックしてローカル画像を選択します。画像の名前に使用できるのは、文字、数字、ハイフン(-)、アンダースコア(_)、およびスペースだけです。画像に関するその他の制限については、プロンプト情報を参照してください。

      To use a picture from the gallery on the IMC database: ギャラリーのプレビュー領域からピクチャを選択し、Select Pictureをクリックします。デフォルトでは、プレビュー領域には、名前のアルファベット順に表示されるに従って、最初の背景ピクチャが表示されます。

   b. **Set**をクリックします。
   c. **Close**をクリックします。
6. (オプション)背景画像の位置とサイズを調整します。
   a. 空白領域を右クリックし、ショートカットメニューの**Adjust Background** > **Manual Adjust**の順に選択します。

      背景画像調整モードになっています。

   b. 背景画像の調整モードを終了するには、空白領域を右クリックし、ショートカットメニューから**Exit Adjust Background**を選択します。

スケールの設定

トポロジーのスケールは、対応する実際の距離に対する背景画像の距離の比率です。

スケールを設定するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager** > **Wireless Topology**を選択します。

   ワイヤレスデバイストポロジーウィンドウが開きます。
3. 左側のナビゲーションツリーから、尺度を設定する位置ビューを入力します。
4. **Set Scale**アイコンをクリックします。
5. カーソルが＋に変わったら、背景ピクチャに線を描画します。**Specify the actual distance**ウィンドウが開きます。
6. **Actual Distance**フィールドに値を入力し、計測単位を選択します。
7. **OK**をクリックします。

位置ビューの右上コーナーに尺度が表示されます。

共通パラメーターの設定

FTPサーバーの設定

ワイヤレス位置確認のためのFTPサーバー設定を構成します。生成された位置確認データは、定期的にFTPサーバーにアップロードされます。

FTPサーバーの設定を構成するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > Locating Management**を選択します。

Locating Managementページが開きます。

3. **Common Parameter Configuration**領域で、**FTP Server Settings**をクリックします。
4. **FTP Server Settings**ページで、次のパラメーターを設定します。
   - **Enable FTP**: 位置情報データをFTPサーバーにアップロードするには、このオプションを選択します。
   - **FTP Server**: FTPサーバーのIPアドレスを入力します。
   - **Port Number**: FTPサーバーのポート番号を入力します。
   - **User Name**: FTPサーバーにログインするためのユーザー名を入力します。
   - **Password**: FTPサーバーにログインするためのパスワードを入力します。
   - **FTP Directory**: FTPサーバー上の検索ファイルを保存する相対パスを入力します。たとえば、**iMC\location**のようになります。
5. **OK**をクリックします。

主要なクライアント設定の構成

キークライアントリストにクライアントを追加するには、次の作業を実行します。キークライアントのロケーションビューが変更されると、マイナーアラームが生成されます。

主要なクライアント設定を構成するには、次の手順に従います

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > Locating Management**を選択します。

   Locating Managementページが開きます。
3. **Common Parameter Configuration**領域で、**Key Client Settings**をクリックします。
4. 単一のクライアントまたはクライアントのバッチをキークライアントリストに追加します。
   - 単一のクライアントを追加するには、**Add**.をクリックします。表示されるウィンドウで、クライアントのMACアドレスをhh:hh:hh:hh:hh:hhの形式で入力します。
   - クライアントをバッチで追加するには、インポートをクリックし、クライアントのMACアドレスを含む.csvファイルをインポートします。
5. **OK**をクリックします。

Location Awareによる検索

Location Awareロケーティングは、時間値を使用してクライアントと複数のAP間の距離を計算します。APの位置に基づいて、クライアントの位置を正確に特定し、ロケーションビュートポロジーにクライアントを表示できます。

Location Awareロケーティングに参加できるのは、ロケーティングAPだけです。APをロケーティングAPとして設定する方法の詳細については、「ロケーティングAPまたは非ロケーティングAPとしてのAPの設定」を参照してください。

位置決めパラメーターの設定

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > Locating Management**を選択します。

   Locating Managementページが開きます。
3. **Location Aware Locating**領域で、**Location Parameter Configuration**をクリックします。

4. **Location Parameter Configuration**ページで、次のパラメーターを設定します。
   - **Location Request Interval(1-5 s)**: ロケーション要求を送信する間隔を入力します。
   - **Locating Packet Quantity in One Locating Request**: 各位置特定要求で送信される位置特定パケットの数を入力します。
   - **Client Locating Interval(1-10 s)** :クライアントの検索間隔を入力します。APは、クライアントの検索間隔中に複数の検索要求を送信します。
   - **Client Locating Idle Interval(20-60 s)**: クライアント検索のアイドル間隔を入力します。APがアイドル間隔内にクライアントに関する検索情報を受信しない場合、APはクライアントがオフラインであると判断します。
   - **Locating AP Mounting Height(m)**: APの取り付け高さを入力します。
5. **OK**をクリックします。

クライアント カウント設定の構成

ロケーションビューページでクライアントがカウントされるロケーションビューおよびサブビューを設定するには、次の作業を実行します。

クライアント数の設定を構成するには、次の手順に従います

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > Locating Management**を選択します。

   Locating Managementページが開きます。
3. **Location Aware Locating**領域で、**Client Counting Settings**をクリックします。
4. クライアントのカウント設定ページで、クライアントがカウントされるロケーションビューおよびサブビューを選択します。
5. **OK**をクリックします。

位置領域の管理

正確なLocation Aware検索のために、WSMはLocation Aware検索領域を管理する次の機能を提供します。

- 配置領域を描画する
- 障害領域を描画する
- デジタルフェンスを描画する

Location Aware位置領域を描画する

Location Awareロケーティングリージョンを描画すると、Location Awareロケーティングはそのリージョン内のクライアントを検索します。

Location Aware位置特定領域を描画するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management>Location Views**を選択します。

   Location Listページが開きます。
3. ロケーションビューの**View Topology**アイコンをクリックします。

   ロケーションビューのトポロジーページが開き、すべてのサブロケーションビュー、FIT AP、およびFAT APが表示されます。

4. 空白領域を右クリックし、ショートカットメニューから**Locating Region Mgt**を選択します。ロケーション対応のロケーション領域管理モードになっています。
5. 空白領域を右クリックして、ショートカットメニューの**Draw Locating Region**を選択します。
6. 位置指定リージョンタイプを選択します。オプションは次のとおりです。
   - **Plane**: プレーン領域内のクライアントの場合、WSMは領域内の正確な位置にクライアントを配置します。
   - **Room**: ルーム領域内のクライアントの場合、WSMはクライアントをルーム内の正確な位置ではなく、ルームに配置します。
   - **Line**: 回線領域内のクライアントの場合、WSMはRSSI強度に基づいて、クライアントRSSIが最も強い2つのAP間の場所にクライアントを配置します。
7. ロケーション領域の各頂点を1つずつクリックし、ダブルクリックして終了します。WSMは、特定の距離にある領域内のロケーションポイントを自動的に水色でマークします。
   位置決め領域に有効な位置決め点が含まれていることを確認してください。
8. 描画モードを終了するには、**Pointer**アイコンをクリックします。

障害領域の描画

APは障害領域内のクライアントを検出できません。

障害領域を描画するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > Location Views**を選択します。
   Location Listページが開きます。
3. ロケーションビューの**View Topology**アイコンをクリックします。
   Location View Topologyページが開き、すべてのサブロケーションビュー、Fit AP、およびFat APが表示されます。
4. 空白領域を右クリックし、ショートカットメニューから**Locating Region Mgt**を選択します。ロケーション対応のロケーション領域管理モードになっています。
5. 空白の領域を右クリックし、ショートカットメニューから**Draw Obstacle**を選択します。
6. 障害物領域の各頂点を1つずつクリックし、ダブルクリックして終了します。
7. 描画モードを終了するには、**Pointer**アイコンをクリックします。

デジタルフェンスを描画する

デジタルフェンスは、クライアントの検索には影響しません。WSMは、統計分析のためにデジタルフェンスにアクセスするクライアントの場所を記録します。

デジタルフェンスを描画するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > Location Views**を選択します。
   Location Listページが開きます。
3. ロケーションビューの**View Topology**アイコンをクリックします。
   ロケーションビューのトポロジーページが開き、すべてのサブロケーションビュー、FIT AP、およびFAT APが表示されます。
4. 空白領域を右クリックし、ショートカットメニューから**Locating Region Mgt**を選択します。ロケーション対応のロケーション領域管理モードになっています。

5. 空白の領域を右クリックし、ショートカットメニューから**Draw Digital Fence**を選択します。
6. デジタルフェンス上の各頂点を1つずつクリックし、ダブルクリックして終了します。
7. 描画モードを終了するには、**Pointer**アイコンをクリックします。

クライアントの検索

この関数は、クライアントを検索し、ロケーションビューにロケーションを表示できます。システムは、クライアントの検索後にクライアントのロケーションを調整します。

クライアントの検索

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > Location Views**を選択します。**Location List**ページが開きます。
3. ロケーションビューの**View Topology**アイコンをクリックします。

   Location View Topologyページが開き、すべてのサブロケーションビュー、Fit AP、およびFat APが表示されます。
4. 空白の領域を右クリックし、ショートカットメニューから**Show Clients**を選択します。開いたページには、ACによって管理されているFIT APに関連付けられたすべてのクライアントが表示されます。
5. クライアントアイコンを右クリックし、ショートカットメニューから**Locate**を選択して、クライアントの場所を表示します。
6. 空白領域を右クリックし、ショートカットメニューから**Stop Locate**を選択します。

複数のクライアントを検索する

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > Location Views**を選択します。

   Location Listページが開きます。
3. ロケーションビューの**View Topology**アイコンをクリックします。

   Location View Topologyページが開き、すべてのサブロケーションビュー、Fit AP、およびFat APが表示されます。
4. 空白領域を右クリックし、ショートカットメニューから**Locate**を選択します。
5. 表示される**Showing Clients Configuration**ダイアログボックスで、ユーザー名、アカウント名、またはMACアドレスによって検索されるクライアントを照会します。
6. **Query**をクリックします。リストに、基準に一致するすべてのクライアントが表示されます。
7. 検索するクライアントを選択し、**OK**をクリックします。

クライアントの追跡

この関数は、ロケーションビューでクライアントをリアルタイムで追跡します。WSMは、ロケーションビュー トポロジーでクライアントの現在のロケーションをリアルタイムで表示します。ロケーションビューが変更されると、WSMは新しいロケーションビューにクライアントのロケーションを表示します。1つのロケーションビューで追跡できるクライアントは1つだけです。

クライアントを追跡するには:

1. クライアントを検索します。

   詳細については、「クライアントの検索」を参照してください。

2. クライアントアイコンを右クリックし、ショートカットメニューから**Track**を選択してクライアントを追跡します。クライアントアイコンの色が青に変わります。
   WSMは、トポロジー上のクライアントの場所をリアルタイムで表示します。

位置トラックの表示

このファンクションは、ロケーションビューに青い線を使用してクライアントトラックを表示します。クライアントのロケーショントラックを表示するには、次のステップを実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > Location Views**を選択します。
   Location Listページが開きます。
3. ロケーションビューの**View Topology**アイコンをクリックします。
   Location View Topologyページが開き、すべてのサブロケーションビュー、Fit AP、およびFat APが表示されます。
4. 空白の領域を右クリックし、ショートカットメニューから**Display Locating Track**を選択します。
5. 開いた位置トラックを表示ダイアログボックスで、次のパラメーターを設定します。
   - **Start Time**: 開始時間を入力します。
   - **End Time**: 終了時間を入力します。
   - **MAC**: 表示するクライアントのMACアドレスを入力します。
6. **OK**をクリックします。
   によって開始され、 によって終了する青い線であるクライアントトラックがトポロジーに表示されます。

ロケーションビュー トポロジーでクライアントトラックを動的に表示する

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > Location Views**を選択します。**Location List**ページが開きます。
3. ロケーションビューの**View Topology**アイコンをクリックします。
   Location View Topologyページが開き、すべてのサブロケーションビュー、Fit AP、およびFat APが表示されます。
4. ツールバーの**Locating Result Dynamic Display**アイコンをクリックします。
5. 開いた**Locating Result Dynamic Display**ダイアログボックスで、以下のパラメーターを設定します。
   - **Start Time**: 開始時間を入力します。
   - **End Time**: 終了時間を入力します。
   - **MAC**: 表示するクライアントのMACアドレスを入力します。
6. **OK**をクリックします。
   クライアントトラックは、トポロジーに動的に表示されます。

   動的表示を一時停止するには、**Pause**アイコンをクリックします。

   動的表示を続行するには、**Continue**アイコンをクリックします。

動的表示を停止するには、**Stop**アイコン■をクリックします。

Location Aware位置特定ヒートマップの表示

この関数は、ヒートマップ内の位置指定領域にある期間中のクライアントの位置を表示します。

Location Aware位置指定ヒートマップを表示するには、次の手順を実行します:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > Location Views**を選択します。**Location List**ページが開きます。
3. ロケーションビューの**View Topology**アイコンをクリックします。
   ロケーションビューのトポロジーページが開き、すべてのサブロケーションビュー、FIT AP、およびFAT APが表示されます。
4. 空白の領域を右クリックし、ショートカットメニューから**Show Locating Heat Map**を選択します。
5. 開いた**Show Locating Heat Map**ダイアログボックスで、次のパラメーターを設定します。
   - **Start Time**: 開始時間を入力します。
   - **End Time**: 終了時間を入力します。
   - **MAC**: 表示するクライアントのMACアドレスを入力します。複数のMACアドレスがある場合は、カンマで区切ります。このパラメーターを指定しない場合は、すべてのクライアントのヒートマップ情報が表示されます。
6. **OK**をクリックします。

BLE位置確認

BLE位置確認では、ビーコンによって検出されたクライアントのRSSIを使用してクライアントの位置を確認します。この方法では、クライアントの位置をリアルタイムで表示および監視できます。

ビーコンの管理

WSMのビーコンには、APによって検出されたビーコンと、ロケーションビュートポロジーに手動で追加されたビーコンが含まれます。WSMで管理できるのは、検出されたAPと一致するビーコンだけです。

ロケーションビューにAPを追加すると、APの一致するすべてのビーコンがロケーションビューに表示されます。

ビーコンリストの表示

ビーコンリストには、APによって検出されたビーコンに関する情報が表示されます。ビーコンリストを表示するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > Locating Management**を選択します。
   Locating Managementページが開きます。
3. **iBeacon Locating**領域で、**Beacon List**をクリックします。
   ビーコンリスト
   - **Status**: ビーコンのステータス。●アイコンは、ビーコンが検出中のAPと一致しないことを示します。●アイコンは、ビーコンが検出中のAPと一致することを示します。

- **Beacon MAC**: ビーコンのMACアドレス。
- **Beacon UUID**: ビーコンの**Universally Unique Identifier(UUID)**。
- **AP**: ビーコンと一致するAPの名前。
- **Beacon Name**: ビーコンの名前。
- **RSSI(dBm)**: ビーコンのRSSI。クライアントとビーコンの間の距離を計算するために使用されます。
- **Major ID**: ビーコンが属するグループのメジャーID。ビーコングループの識別に使用されます。
- **Minor ID**: ビーコンのマイナーID。グループ内のビーコンの識別に使用されます。
- **Measured Power(dBm)**: ビーコンの送信電力。クライアントとビーコンの間の距離を計算するために使用されます。
- **Battery(%)**: ビーコンのバッテリ残量。
- **Operation**: ビーコンのパスワードまたはパラメーターを変更するには、**Operation**アイコン をクリックします。

ビーコンUUID、メジャーIDおよびマイナーIDはすべて、ビーコンを識別します。たとえば、チェーンストアの場合、UUIDを使用してチェーンのストアブランドを識別し、メジャーIDを使用してストアを識別し、マイナーIDを使用してビーコンを識別できます。

ビーコンの詳細情報の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > Locating Management**を選択します。

   Locating Managementページが開きます。
3. **iBeacon Locating**領域で、Beacon Listをクリックします。
4. ビーコンの詳細情報を表示するには、ビーコンのMACアドレスをクリックします。

ビーコン情報のインポート

ビーコン情報をバッチでインポートするには、このタスクを実行します。ビーコン情報をインポートするには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager>Locating Management**を選択します。

   Locating Managementページが開きます。
3. iBeacon Locating領域で、Beacon Listをクリックします。
4. **Import**をクリックします。

   Importページが開きます。
5. ソースファイルとして.csvファイルを選択し、Location Viewリストからロケーションビューを選択します。
6. **Next**をクリックし、パラメーターの順序を設定します。指定する順序は、選択したファイル内の順序と同じである必要があります。
7. **OK**をクリックします。
8. **Back**をクリックします。

ビーコン情報のエクスポート

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > Locating Management**を選択します。

Locating Managementページが開きます。

3. **iBeacon Locating**領域で、**Beacon List**をクリックします。
4. **Export**.をクリックします。

   Export Resultページが開きます。
5. 結果のエクスポートをクリックします。WSMによって.csvファイルが生成され、デフォルトのディレクトリに保存されます。

ビーコンパラメーターの変更

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager>Locating Management**を選択します。

   Locating Managementページが開きます。
3. **iBeacon Locating**領域で、**Beacon List**をクリックします。
4. ターゲットビーコンの**Operation**アイコン ･･･ をクリックし、**Modify Parameter**を選択します。**Modify Beacon Parameter Settings**ページが開きます。
5. 必要に応じてビーコンパラメーターを変更します。
6. **OK**をクリックします。

パスワードの変更

このタスクは、APと一致するビーコンに対してのみ実行できます。ビーコンは、同じパスワードを持つAPと一致します。

パスワードを変更するには、次の手順に従います

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > Locating Management**を選択します。

   Locating Managementページが開きます。
3. **iBeacon Locating**領域で、**Beacon List**をクリックします。
4. ターゲットビーコンの操作**Operation**アイコン･･･をクリックし、**Change Password**を選択します。

   Change Beacon Configuration Passwordページが開きます。
5. **Change Password on**リストから**AP and Beacon**または**AP Only**を選択します。
6. **Configuration Password**フィールドと**Confirm Password**フィールドの両方にパスワードを入力します。
7. **OK**をクリックします。

変更履歴の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > Locating Management**を選択します。

   Locating Managementページが開きます。
3. **iBeacon Locating**領域で、**Beacon List**をクリックします。
4. 履歴の変更をクリックします。履歴リストの変更
   - **Beacon Name**: ビーコンの名前。
   - **Beacon MAC**: ビーコンのMACアドレス。
   - **AP Name**: ビーコンと一致するAPの名前。

- **Modified at**: ビーコンが変更された時刻。
- **Modified Type**: Modified Typeオプションは、**Modify Attribute**, **Change Password**,そして**Change Attribute and Password**です。
- **Modified Status**: 変更ステータス。オプションは、**Success**, **Failure**および**Modifying**です。
- **Operator**: 変更するオペレーターの名前。

ビーコンの追加

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > View Management > Location Views**を選択します。

   Location Listページが開きます。
3. ロケーションビューの**View Topology**アイコンをクリックします。

   ロケーションビューのトポロジー ページが開き、すべてのサブロケーションビュー、FIT AP、およびFAT APが表示されます。
4. 空白の領域を右クリックし、表示されるリストから**Beacon Mgt**を選択して、ビーコン管理モードを開始します。
5. 空白の領域を右クリックし、表示されるリストから**Add beacon**を選択します。
6. 表示されるダイアログボックスで、次のパラメーターを設定します。
   - **MAC**: ビーコンのMACアドレスを入力します。
   - **UUID**: ビーコンのUUIDを入力します。
   - **Major ID**: ビーコンのメジャーIDを0～65535の範囲で入力します。
   - **Minor ID**: ビーコンのマイナーIDを0～65535の範囲で入力します。
7. **OK**をクリックします。

   新たに追加されたビーコンがトポロジーに表示されます。
8. ビーコンをトポロジー内の適切な場所にドラッグし、**Save**アイコンをクリックします。
9. 空白の領域を右クリックし、リストから**Exit Beacon Management**を選択して、ビーコン管理モードを終了します。

位置領域の管理

詳細については、「位置領域を管理する」を参照してください。

クライアントの検索

この関数は、クライアントを検索し、ロケーションビューにロケーションを表示できます。システムは、クライアントの検索後にクライアントのロケーションを調整します。

クライアントの検索

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > Location Views**を選択します。**Location List**ページが開きます。
3. ロケーションビューの**View Topology**アイコンをクリックします。

   Location View Topologyページが開き、すべてのサブロケーションビュー、Fit AP、およびFat APが表示されます。

4. 空白の領域を右クリックし、ショートカットメニューからクライアントの表示を選択します。開いたページには、ACによって管理されているFIT APに関連付けられたすべてのクライアントが表示されます。
5. クライアントアイコンを右クリックし、ショートカットメニューから**Locate**を選択して、クライアントの場所を表示します。
6. 空白領域を右クリックし、ショートカットメニューから**Stop Locate**を選択します。

複数のクライアントを検索する

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > Location Views**を選択します。**Location List**ページが開きます。
3. ロケーションビューの**View Topology**アイコンをクリックします。

   Location View Topologyページが開き、すべてのサブロケーションビュー、Fit AP、およびFat APが表示されます。
4. 空白領域を右クリックし、ショートカットメニューから**Locate**.を選択します。
5. 表示される**Showing Clients Configuration**ダイアログボックスで、ユーザー名、アカウント名、またはMACアドレスによって検索されるクライアントを照会します。
6. **Query**をクリックします。リストに、基準に一致するすべてのクライアントが表示されます。
7. 検索するクライアントを選択し、**OK**をクリックします。

クライアントの追跡

この関数は、ロケーションビューでクライアントをリアルタイムで追跡します。WSMは、ロケーションビュー トポロジーでクライアントの現在のロケーションをリアルタイムで表示します。ロケーションビューが変更されると、WSMは新しいロケーションビューにクライアントのロケーションを表示します。1つのロケーションビューで追跡できるクライアントは1つだけです。

クライアントを追跡するには:

1. クライアントを検索します。

   詳細については、「クライアントの検索」を参照してください。
2. クライアントアイコンを右クリックし、ショートカットメニューから**Track**を選択してクライアントを追跡します。クライアントアイコンの色が青に変わります。

   WSMは、トポロジー上のクライアントの場所をリアルタイムで表示します。

位置トラックの表示

このファンクションは、ロケーションビューに青い線を使用してクライアントトラックを表示します。クライアントのロケーショントラックを表示するには、次のステップを実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > Location Views**を選択します。**Location List**ページが開きます。
3. ロケーションビューの**View Topology**アイコンをクリックします。

   Location View Topologyページが開き、すべてのサブロケーションビュー、Fit AP、およびFat APが表示されます。
4. 空白の領域を右クリックし、ショートカットメニューから**Display Locating Track**を選択します。

5. 開いた位置トラックを表示ダイアログボックスで、次のパラメーターを設定します。
   - **Start Time**: 開始時間を入力します。
   - **End Time**: 終了時間を入力します。
   - **MAC**: 表示するクライアントのMACアドレスを入力します。
6. OKをクリックします。

   によって開始され、 によって終了する青い線であるクライアントトラックがトポロジーに表示されます。

ロケーションビュー トポロジーでクライアントトラックを動的に表示する

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > Location Views**を選択します。**Location List**ページが開きます。
3. ロケーションビューの**View Topology**アイコンをクリックします。

   Location View Topologyページが開き、すべてのサブロケーションビュー、Fit AP、およびFat APが表示されます。
4. ツールバーの**Locating Result Dynamic Display**アイコンをクリックします。
5. 開いた**Locating Result Dynamic Display**ダイアログボックスで、以下のパラメーターを設定します。
   - **Start Time**: 開始時間を入力します。
   - **End Time**: 終了時間を入力します。
   - **MAC**: 表示するクライアントのMACアドレスを入力します。
6. OKをクリックします。

   クライアントトラックは、トポロジーに動的に表示されます。

   動的表示を一時停止するには、**Pause**アイコンをクリックします。

   動的表示を続行するには、**Continue**アイコンをクリックします。

   動的表示を停止するには、**Stop**アイコンをクリックします。

Location Aware位置特定ヒートマップの表示

この関数は、ヒートマップ内の位置指定領域にある期間中のクライアントの位置を表示します。

Location Aware位置指定ヒートマップを表示するには、次の手順を実行します:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > Location Views**を選択します。**Location List**ページが開きます。
3. ロケーションビューの**View Topology**アイコンをクリックします。

   ロケーションビューのトポロジー ページが開き、すべてのサブロケーションビュー、FIT AP、およびFAT APが表示されます。
4. 空白の領域を右クリックし、ショートカットメニューから**Show Locating Heat Map**を選択します。
5. 開いた**Show Locating Heat Map**ダイアログボックスで、次のパラメーターを設定します。
   - **Start Time**: 開始時間を入力します。

- **End Time**: 終了時間を入力します。
- **MAC**: 表示するクライアントのMACアドレスを入力します。複数のMACアドレスがある場合は、カンマで区切ります。このパラメーターを指定しない場合は、すべてのクライアントのヒートマップ情報が表示されます。

6. **OK**をクリックします。

X-Shareの場所

X-Share検索を実行できるのは、X-Shareアンテナをサポートするだけです。X-Shareアンテナに近い場所にクライアントを配置します。

X-Shareアンテナの管理

X-Share位置確認を実装するには、最初にX-Shareアンテナの位置とパラメーターを設定します。

X-Shareアンテナを追加する

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > Location Views**を選択します。**Location List**ページが開きます。
3. ロケーションビューの**View Topology**アイコンをクリックします。

   ロケーションビューのトポロジー ページが開き、すべてのサブロケーションビュー、FIT AP、およびFAT APが表示されます。
4. 空白の領域を右クリックし、ショートカットメニューから**X-Share Antenna Mgt**を選択します。
5. X-Shareアンテナをサポートするを右クリックし、ショートカットメニューからAdd X-Share Antennaを選択します。
6. **Add X-Share Antenna**ダイアログボックスで、次のパラメーターを設定します。
   - **Antenna ID**: アンテナIDを選択します。オプションは**Ant-1**、**Ant-2**、**Ant-3**および**Ant-4**です。
   - **Attenuation**: 減衰値を入力します。
   - **Description**: アンテナの説明を入力します。
7. **OK**をクリックします。
8. X-Shareアンテナアイコンを、実際の位置に従ってトポロジー内の正しい場所にドラッグします。

X-Shareアンテナを変更する

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > Location Views**を選択します。**Location List**ページが開きます。
3. ロケーションビューの**View Topology**アイコンをクリックします。

   ロケーションビューのトポロジー ページが開き、すべてのサブロケーションビュー、FIT AP、およびFAT APが表示されます。
4. 空白の領域を右クリックし、ショートカットメニューから**X-Share Antenna Mgt**を選択します。
5. 修正するX-Shareアンテナを右クリックし、ショートカットメニューから**Modify**を選択します。
6. **Modify X-Share Antenna**ダイアログボックスで、次のパラメーターを設定します。
   - **Antenna ID**: このパラメーターは変更できません。

- **Attenuation**: 減衰値を入力します。
- **Description**: アンテナの説明を入力します。

7. **OK**をクリックします。
8. X-Shareアンテナアイコンを、実際の位置に従ってトポロジー内の正しい場所にドラッグします。

X-Shareアンテナの削除

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > Location Views**を選択します。

   Location Listページが開きます。
3. ロケーションビューの**View Topology**アイコンをクリックします。

   Location View Topologyページが開き、すべてのサブロケーションビュー、Fit AP、およびFat APが表示されます。
4. 空白の領域を右クリックし、ショートカットメニューから**X-Share Antenna Mgt**を選択します。
5. 削除するX-Shareアンテナを右クリックし、ショートカットメニューから**Delete**を選択します。
6. 確認ダイアログボックスで、**OK**をクリックします。

X-Shareアンテナの保存

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>View Management>Location Views**を選択します。**Location List**ページが開きます。
3. ロケーションビューの**View Topology**アイコンをクリックします。

   Location View Topologyページが開き、すべてのサブロケーションビュー、Fit AP、およびFat APが表示されます。
4. 空白の領域を右クリックし、ショートカットメニューから**X-Share Antenna Mgt**を選択します。
5. 空白の領域を右クリックし、ショートカットメニューから**Save**を選択します。

クライアントの検索

1つまたは複数のワイヤレスクライアントを検索できます。検索結果はロケーションビューに表示されます。

クライアントの検索

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > Location Views**を選択します。

   Location Listページが開きます。
3. ロケーションビューの**View Topology**アイコンをクリックします。

   Location View Topologyページが開き、すべてのサブロケーションビュー、Fit AP、およびFat APが表示されます。
4. 空白領域を右クリックし、ショートカットメニューから**Show Clients**を選択します。

   開いたページには、ACに接続されているAPに関連付けられているすべてのクライアントが表示されます。
5. ターゲットクライアントを右クリックし、ショートカットメニューから**Locate**を選択します。

複数のクライアントを検索する

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > View Management > Location Views**を選択します。**Location List**ページが開きます。
3. ロケーションビューの**View Topology**アイコンをクリックします。

   Location View Topologyページが開き、すべてのサブロケーションビュー、Fit AP、およびFat APが表示されます。
4. 空白の領域を右クリックし、ショートカットメニューから検索を選択します。
5. 表示される**Showing Clients Configuration**ダイアログボックスで、ユーザー名、アカウント名、またはMACアドレスによって検索されるクライアントを照会します。
6. **Query**をクリックします。リストに、基準に一致するすべてのクライアントが表示されます。
7. 検索するクライアントを選択し、**OK**をクリックします。

APに基づいたワイヤレスでの位置特定

APベースの無線位置特定では、無線信号をスキャンして、クライアント(不正なクライアントを含む)および不正なAPの位置を特定します。

APベースのワイヤレスロケーティングを実装するには、APの動作モードをモニターまたはハイブリッドに設定します。

ワイヤレスクライアントの検索

クライアントをクライアント名で検索するには、次の手順に従います。

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > Resource Management > Clients**を選択します。**Client List**ページにすべてのクライアントが表示されます。
3. 検索するクライアントの**Operation**アイコン をクリックし、ショートカットメニューから**Locate**を選択します。

   ロケーションビュー トポロジーにクライアントが表示され、強調表示されます。

トポロジーによってクライアントを検索するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager** > **Wireless Topology**を選択します。

   ワイヤレスデバイス トポロジーページが開き、すべてのACとFAT APが表示されます。
3. ACまたはFat APアイコンをダブルクリックするか、ACまたはFat APアイコンを右クリックして**Open Topology**を開きます。

   ACまたはFAT APのトポロジー ページが開きます。

   ACトポロジーにはクライアントは表示されません。
4. ACによって管理されているfit APに関連付けられているすべてのクライアントを表示するには、空白領域を右クリックし、ショートカットメニューから**Show Devices** > **Show All Clients**を選択します。
5. クライアントアイコンを右クリックし、ショートカットメニューから**Locate**を選択します。ロケーションビュ

ートポロジーにクライアントが表示され、強調表示されます。

WSMはロケーション結果を継続的に調整するため、最初に配置されたロケーションが最終的に配置されたロケーションと異なる場合があります。10分後にロケーション結果が表示されない場合、ロケーション操作は自動的に停止し、失敗を示すプロンプトがメッセージバーに表示されます。

6. 検索操作を停止するには、空白領域を右クリックし、ショートカットメニューから**Stop Locate**を選択します。

不正なクライアントの検出

不正なクライアントをクライアント名で特定するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIDS Management > Rogue Clients**を選択します。**Rogue Client List**には、すべての不正クライアントが表示されます。
3. 検索する不正なクライアントの**Operation**アイコン ▪▪▪ をクリックし、ショートカットメニューから**Locate**を選択します。

   不正なクライアントがロケーションビュートポロジーに表示され、強調表示されます。

不正なクライアントをトポロジーで特定するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager** > **Wireless Topology**を選択します。ワイヤレスデバイストポロジーページが開き、すべてのACとFAT APが表示されます。
3. ACアイコンをダブルクリックするか、ACアイコンを右クリックして、ショートカットメニューから**Open Topology**を選択します。

   ACのトポロジーページが開きます。
4. 空白の領域を右クリックし、ショートカットメニューから**Show Devices > Show Rogues**を選択します。

   すべての不正なAPおよびクライアントが表示され、それらを検出したFIT APに関連付けられます。
5. クライアントアイコンを右クリックし、ショートカットメニューから**Locate**を選択します。ロケーションビュートポロジーにクライアントが表示され、強調表示されます。

   WSMはロケーション結果を継続的に調整するため、最初に配置されたロケーションが最終的に配置されたロケーションと異なる場合があります。10分後にロケーション結果が表示されない場合、ロケーション操作は自動的に停止し、失敗を示すプロンプトがメッセージバーに表示されます。
6. 検索操作を停止するには、空白領域を右クリックし、ショートカットメニューから**Stop Locate**を選択します。

不正なAPの検出

不正なAPをAP名で特定するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > WIDS Management > Rogue APs**を選択します。**Rogue AP List**には、すべての不正APが表示されます。
3. 検出する不正なAPの**Operation**アイコン ▪▪▪をクリックし、ショートカットメニューからLocateを選択します。

   不正なAPがロケーションビュー トポロジーに表示され、強調表示されます。

不正なAPをトポロジーで特定するには、次の手順を実行します。

4. **Service**タブをクリックします。
5. ナビゲーションツリーから、**WLAN Manager** > **Wireless Topology**を選択します。ワイヤレスデバイストポロジーページが開き、すべてのACとFAT APが表示されます。
6. ACアイコンをダブルクリックするか、ACアイコンを右クリックして、ショートカットメニューから**Open Topology**を選択します。
   ACのトポロジーページが開きます。
7. 空白の領域を右クリックし、ショートカットメニューから**Show Devices > Show Rogues**を選択します。
   すべての不正なAPおよびクライアントが表示され、それらを検出したFIT APに関連付けられます。
8. 不正APアイコンを右クリックし、ショートカットメニューから**Locate**を選択します。不正APがロケーションビュートポロジーに表示され、強調表示されます。
   WSMはロケーション結果を継続的に調整するため、最初に配置されたロケーションが最終的に配置されたロケーションと異なる場合があります。10分後にロケーション結果が表示されない場合、ロケーション操作は自動的に停止し、失敗を示すプロンプトがメッセージバーに表示されます。
9. 検索操作を停止するには、空白領域を右クリックし、ショートカットメニューから**Stop Locate**を選択します。

GIS検索

GIS検索は、GISビューでAPまたはクライアントを検索するために使用されます。これは通常、複数の支店を持つ企業に適用されます。

GISの検索を実行する前に、GISビューにロケーションビューを追加します。その後、WSMはAPのロケーションビューに従ってAPを検索し、クライアントが関連付けられているAPのロケーションビューに従ってクライアントを検索できます。

GISビューに位置ビューを追加する方法については、「GISビューを管理する」を参照してください。

注:

- 管理者およびメンテナはGISビューでマップを編集できますが、ビューアはマップの表示のみが可能です。
- マップをダブルクリックするとマップが拡大ズームされ、マップを右ダブルクリックするとマップが縮小ズームされます。

APの検索

1. **Service**タブをクリックします。
2. デバイスリストページを表示するには、次のいずれかの手順を実行します。
   ナビゲーションツリーで、WLAN Manager > Resource Management > Fat APsまたはWLAN Manager>Resource Management>Fit APsを選択します。
   Fat AP ListページまたはFit AP Listページが開きます。
   a. ナビゲーションツリーから、**WLAN Manager > View Management > Location Views**を選択します。**Location List**ページが開きます。
   b. ロケーションビューの名前をクリックします。
      Sub-location/Device Listページが開きます。
3. デフォルトマップを検索するAPの**Operation**アイコン ▪▪▪ をクリックしショートカットメニューから **Locate to Map**を選択します。

オンラインクライアントの検索

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Resource Management > Clients**を選択します。

   Client Listページが開きます。
3. デフォルトマップを検索するクライアントの**Operation**アイコン をクリックしショートカットメニューから**Locate to Map**を選択します。

ショップ管理

ショップ管理を使用すると、ショップマウント型AP統計情報を収集して、クライアントがショップに入ったか出たかを判別できます。ショップは1つのロケーションビューにのみ配置でき、ロケーションビューには複数のショップを含めることができます。

ショップリストの管理

ショップリストを表示する

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > Locating Management**を選択します。

   Locating Managementページが開きます。
3. **Shop Management**領域で、**Shop List**をクリックします。

   ショップリスト
   - **Shop Name**: ショップの名前。
   - **Shop Description**: ショップの説明。
   - **Location View**: ショップが存在するロケーションビュー。
   - **Modify**: ショップ情報を修正するには、**Modify**アイコンをクリックします。
   - **Delete**: **Delete**アイコンをクリックして、ショップを削除します。

ショップの追加

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > Locating Management**を選択します。

   Locating Managementページが開きます。
3. **Shop Management**領域で、**Shop List**をクリックします。
4. **Add**をクリックします。

   Add Shopウィンドウが開きます。
5. ショップの次のパラメーターを設定します。
   - **Location**: ショップが配置されているロケーションビューを選択します。
   - **Shop Name**: ショップの名前を入力します。
   - **Shop Description**: ショップの説明を入力します。
6. OKをクリックします。

ショップ情報の変更

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > Locating Management**を選択します。
   Locating Managementページが開きます。
3. **Shop Management**領域で、**Shop List**をクリックします。
4. ターゲットショップの**Modify**アイコンをクリックします。
5. 開いたウィンドウで、ショップの名前と説明を変更します。
6. **OK**をクリックします。

ショップの削除

ロケーションビューが削除されると、ロケーションビュー内のショップも削除されます。ショップを削除する手順は、次のとおりです。

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager>Locating Management**を選択します。
   Locating Managementページが開きます。
3. **Shop Management**領域で、**Shop List**をクリックします。
4. ターゲットショップの**Delete**アイコンをクリックします。
5. 表示された確認ダイアログボックスで、**OK**をクリックします。

ショップマウント型APの管理

この機能を使用すると、ショップマウントAPを追加、削除、および設定したり、ショップエントリーおよびショップエグジットのしきい値を設定したりできます。

ショップマウント型APリストの表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > Locating Management**を選択します。
   Locating Managementページが開きます。
3. **Shop Management**領域で、**Shop List**をクリックします。
4. ショップの名前をクリックします。
   ショップマウント型APリスト
   - **Status**: APのステータス。オプションは、**Online**および**Offline**です。
   - **Type**: APのタイプ。オプションは、**Shop-Entry**および**Shop-Exit**です。
   - **SN**: APのシリアル番号。
   - **Model**: APのモデル。
   - **IP Address**: APのIPアドレス。APにIPv4アドレスがない場合、このフィールドは空です。
   - **IPv6 Address**: APのIPv6アドレス。APにIPv6アドレスがない場合、このフィールドは空です。
   - **MAC Address**: APのMACアドレス。WSMがAPのMACアドレスの取得に失敗した場合、このフィールドは空です。
   - **Entry by RSSI**: RSSIしきい値によるエントリー。**Global Parameters**が使用されている場合、このフィールドにはGlobal Parametersが表示されます。

- **Exit by RSSI**: RSSIしきい値で終了します。**Global Parameters**が使用されている場合、このフィールドにはGlobal Parametersが表示されます。
- **Entry by Distance(1-50 m)**: 距離しきい値による入力。**Global Parameters**が使用されている場合、このフィールドにはGlobal Parametersが表示されます。
- **Exit by Distance(1-50 m)**: 距離しきい値で終了します。Global Parametersが使用されている場合、このフィールドには**Global Parameters**が表示されます。

5. **Shop List**ページに戻るには、**Back**をクリックします。

ショップマウント型APの追加

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager>Locating Management**を選択します。

   Locating Managementページが開きます。
3. **Shop Management**領域で、**Shop List**をクリックします。
4. ショップの名前をクリックします。
5. **Add**.をクリックします。
6. 表示されるダイアログボックスで、1つまたは複数のAPを選択します。クエリー機能を使用すると、APを迅速に検索できます。
7. **OK**をクリックします。

ショップマウント型APの削除

ロケーションビューが削除されると、ロケーションビュー内のショップマウント型ショップも削除されます。ショップマウント型APを削除するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager>Locating Management**を選択します。

   Locating Managementページが開きます。
3. **Shop Management**領域で、**Shop List**をクリックします。
4. ショップの名前をクリックします。
5. 1つまたは複数のAPを選択し、**Delete**をクリックします。
6. 表示された確認ダイアログボックスで、**OK**をクリックします。

工場出荷時のAPタイプの設定

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > Locating Management**を選択します。

   Locating Managementページが開きます。
3. **Shop Management**領域で、**Shop List**をクリックします。
4. ショップの名前をクリックします。
5. ターゲットAPを選択し、**Configure as Shop-Entry AP**または**Configure as Shop-Exit AP**をクリックします。
   をクリックしてAPタイプを設定します。

   ウィンドウが開き、操作が成功したかどうかが示されます。

ショップマウント型APのしきい値の設定

APにしきい値を設定しない場合は、グローバルしきい値が使用されます。ショップマウント型APにしきい値を設定するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager>Locating Management**を選択します。

   Locating Managementページが開きます。
3. **Shop Management**領域で、**Shop List**をクリックします。
4. ショップの名前をクリックします。
5. ターゲットAPを選択し、**Set Thresholds**をクリックします。
6. 開いたウィンドウで、開始および終了のしきい値を設定するか、**Use Global Parameters**を選択してグローバルパラメーターを使用します。

グローバルしきい値の設定

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > Locating Management**を選択します。

   Locating Managementページが開きます。
3. **Shop Management**領域で、**Shop Entry/Exit Thresholds**をクリックします。
4. 次のパラメーターを設定します。
   - **Entry by RSSI(1～95 dBm)**: WSMは、ショップマウント型APによって検出されたクライアントのRSSIがしきい値よりも高い場合に、クライアントがショップに入ったと判断します。
   - **Exit by RSSI(1-95 dBm)**: WSMは、ショップマウント型APによって検出されたクライアントのRSSIがしきい値より低い場合に、クライアントがショップを終了したと判断します。
   - **Entry by Distance(1-50 m)**: WSMは、クライアントとショップマウントAPとの間の距離がしきい値より小さい場合に、クライアントがショップに入ったと判断します。
   - **Exit by Distance(1-50 m)**: WSMは、クライアントとショップマウントAPの間の距離がしきい値よりも大きい場合に、クライアントがショップを終了したと判断します。
   - **Length of Stay(1-600 s)**: WSMは、クライアントの店舗滞在時間がしきい値より短い場合に、そのクライアントが店舗に入っていないと判断します。
5. OKをクリックします。

エネルギーポリシーの設定

エネルギーポリシー管理を使用すると、ワイヤレスデバイスにポリシーを適用して、省エネルギーとコスト削減を実現できます。管理可能なワイヤレスデバイスは、AP、無線、およびSSIDです。

たとえば、週末にワイヤレスデバイスの電源を自動的にオフにするようにWSMでエネルギーポリシーを設定するには、次の手順を実行します。

- 毎週月曜日の午前6:00にAPの動作を開始し、毎週金曜日の午後8:00にAPの動作を停止するようにエネルギーポリシーを設定します。
- ターゲットのワイヤレスデバイスまたは無線を選択します。
- ポリシーをWSMに保存します。

エネルギーポリシーリストの表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Energy Policy Management**を選択します。

   Energy Policy Listページには、すべてのエネルギーポリシーが表示されます。

   エネルギー政策リストの内容

   - **Status**--**Operation Result**: エネルギーポリシーのステータスおよび実行結果。エネルギーポリシーのステータスは、次のいずれかです:
     - **Waiting**
     - **Executing**
     - **Suspended**
     - **Finished**
     - **Expired**

     実行結果は次のようになります。
     - **Succeeded**
     - **Failed**
     - **Partially succeeded**
     - **Unknown**
   - **Policy Name**: エネルギーポリシーの名前。名前をクリックすると詳細情報が表示されます。
   - **Policy Type**: エネルギーポリシーの操作タイプ。エネルギーポリシーの操作タイプは、次のいずれかです。
     - **Start/Stop AP**
     - **Start/Stop Radio**
     - **Modify Radio Power**
     - **Start/Stop SSID**
   - **Execution Mode**: エネルギーポリシーが実行されるモード。エネルギーポリシーの実行モードは、次のいずれかです。
     - **One-off**
     - **Periodical**
   - **Creator**: エネルギーポリシーを作成したオペレーターの名前。
   - **Created Time**: エネルギーポリシーが作成された時刻。
   - **Copy**: **Copy**アイコンをクリックして、エネルギーポリシーをコピーします。コピーのパラメーターを変更し、別のエネルギーポリシーとして保存できます。
   - **Modify**: エネルギーポリシーを変更するには、**Modify**アイコンをクリックします。
   - **Delete**: エネルギーポリシーを削除するには、**Delete**アイコンをクリックします。

Energy Policy Listに十分なエントリーが含まれている場合は、次のナビゲーションが表示されます。

- **Next Page**アイコンをクリックして、**Energy Policy List**の次のページに進みます。
- **Last Page**アイコンをクリックして、**Energy Policy List**の最後のページに進みます。
- **Previous Page**アイコンをクリックして、**Energy Policy List**で前のページに戻ります。
- **First Page**アイコンをクリックして、**Energy Policy List**の前のページに戻ります。

Energy Policy Listの右上にある8、15、50、100、または200をクリックして、各ページに表示する項目の数を指定します。

エネルギーポリシーの照会

WSMを使用すると、特定の基準でエネルギーポリシーをフィルタ処理できます。エネルギーポリシーを問い合せるには、次の手順を実行します:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Energy Policy Management**を選択します。

   Energy Policy Listページには、すべてのエネルギーポリシーが表示されます。
3. 次の問合せ基準を1つ以上入力または選択します。
   - **Policy Name**: エネルギーポリシーの名前を入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
   - **Execution Mode**: エネルギーポリシーを実行するモードを選択します。オプションは次のとおりです。
     - **One-off**
     - **Periodical**
     - **All**
   - **Policy Type**: エネルギーポリシーの操作タイプを選択します。オプションは次のとおりです。
     - **Start/Stop AP**
     - **Start/Stop Radio**
     - **Modify Radio Power**
     - **Start/Stop SSID**
   - **Policy Status**: エネルギーポリシーの状態を選択します。オプションは次のとおりです。
     - **Waiting**
     - **Executing**
     - **Suspended**
     - **Finished**
     - **Expired**
     - **All**
   - 実行結果エネルギーポリシーの実行結果を選択します。オプションは次のとおりです。
     - **Succeeded**
     - **Failed**
     - **Partially succeeded**
     - **Unknown**
     - **All**

   空のフィールドやすべてに設定されたフィールドは、クエリーの抽出条件として使用できません。
4. クエリーをクリックします。

   Energy Policy Listには、クエリー基準に一致するすべてのエネルギーポリシーが表示されます。
5. クエリー基準をクリアしてすべてのエネルギーポリシーを表示するには、Resetをクリックします。

エネルギーポリシーの詳細の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Energy Policy Management**を選択します。

   Energy Policy Listページには、すべてのエネルギーポリシーが表示されます。
3. 詳細情報を表示するエネルギーポリシーの名前をクリックします。ポリシーの詳細ページが開きます。

   このページには、基本情報領域とAPまたは無線リストが表示されます。エネルギーポリシーの基本

   内容

   - **Policy Name**: エネルギーポリシーの名前。
   - **Policy Type**: エネルギーポリシーの動作タイプ。
   - **Creator**: エネルギーポリシーを作成したオペレーターの名前。
   - **Created Time**: エネルギーポリシーが作成された時刻。
   - **SSID**: エネルギーが適用されるSSID。このフィールドは、ポリシータイプがStart/Stop SSIDの場合にだけ表示されます。
   - **Execution Mode**: エネルギーポリシーが実行されるモード。**One-off**または**Periodic**。
   - **Execution Period**: エネルギーポリシーが実行される間隔。このフィールドは、実行モードがPeriodicalの場合にのみ表示されます。
   - **Stopped at**: WSMがAP、無線、またはSSIDの電源をオフにする時刻。
   - **Started at**: WSMがAP、無線、またはSSIDの電源をオンにする時刻。
   - **Restore at**: WSMが無線の電力を復元する時刻。このフィールドは、ポリシータイプがModify Radio Powerの場合にだけ表示されます。
   - **Changed at**: WSMが無線の電力を変更する時刻。このフィールドは、ポリシータイプがModify Radio Powerの場合にだけ表示されます。
   - **Restored Power**: 無線が復元する電力値。範囲は1～27 dBmです。このフィールドが表示されるのは、ポリシータイプがModify Radio Powerの場合だけです。
   - **Changed Power**: 無線が変更される電力値。範囲は1～27 dBmです。このフィールドは、ポリシータイプが**Modify Radio Power**の場合にだけ表示されます。
   - **Always Effective**: エネルギーポリシーが常に有効であるかどうかを示します: **Yes**または**No**。このフィールドは、実行モードが**Periodical**の場合にのみ表示されます。
   - **Validated at**: エネルギーポリシーが有効になる時刻(YYYY-MM-DD hh:mm:ss形式)。このフィールドが表示されるのは、実行モードが**Periodic**で、**Always Effective**オプションが選択されていない場合だけです。
   - **Expired at**: エネルギーポリシーの有効期限が切れる時刻(YYYY-MM-DD hh:mm:ss形式)。このフィールドが表示されるのは、実行モードが**Periodic**で、**Always Effective**オプションが選択されていない場合だけです。
   - **Description**: エネルギーポリシーの説明。

   エネルギーポリシーが**Start/Stop AP**の場合、このページには、エネルギーポリシーが適用されるすべてのAPを表示するAPリストが含まれます。

   APリストの内容

   - **Status**: APのステータス(OnlineまたはOffline)。
   - APラベル/デバイスラベル: APのデバイスラベル。
   - **SN**: APのシリアル番号。
   - **IP Address** :APのIPアドレス。
   - **Model**: APのモデル。
   - **Access Device**: FIT APが接続されるACのモデル。

- **Access Interface**: fit APに接続するアクセスデバイスのポート番号。
- **Location**: APのロケーション。

エネルギーポリシーが**Start/Stop AP**でない場合、ページには**Fit AP Radio List**と**Fat AP Radio List**:エネルギーポリシーが適用されるすべての無線を表示します。

FIT APラジオリストの内容

- **Admin Status**: fit APがWSMによって管理されているかどうかを示します。Upはfit APがWSMによって管理されていることを示し、Downはfit APがWSMによって管理されていないことを示します。
- **Radio ID**: 無線のID。
- **AP Template Nam**e: 無線がイネーブルになっているfit APに適用されるAPテンプレートの名前。
- **Radio Type**: 無線タイプ:802.11a、802.11b、802.11g、802.11an、または802.11gn。Fat AP無線リストの内容
- **Interface**: 無線に接続するFAT APのインターフェース。
- **AP Alias**: 無線がイネーブルになっているFAT APの名前。
- **Radio Type**: 無線タイプ:802.11a、802.11b、802.11g、802.11an、または802.11gn。

エネルギーポリシーを追加する

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Energy Policy Management**を選択します。**Energy Policy List**ページには、すべてのエネルギーポリシーが表示されます。
3. 追加をクリックします。

   Add Energy Policyページが開きます。
4. エネルギーポリシーの次の基本パラメーターを設定します。
   - **Policy Name**: 固有のエネルギーポリシー名を入力します。
   - **Policy Type**: エネルギーの操作タイプを選択します。オプションは次のとおりです。
     - **Start/Stop AP**: アクセスデバイス(通常はスイッチ)上のPoE対応APアクセスポートでPoEをイネーブルまたはディセーブルにして、APの電源をオンまたはオフにします。
     - **Start/Stop Radio**: 無線の管理ステータスをアップまたはダウンに変更して、無線の電源をオンまたはオフにします。
     - **Modify Radio Power**: 無線送信電力を変更または復元します。
     - **Start/Stop SSID**: SSIDを無線にバインドするか、無線からバインド解除します。Comwareベースのデバイスの場合、SSIDはサービスポリシーです。
   - **SSID**: ターゲットSSIDを選択します。このフィールドが表示されるのは、ポリシータイプが**Start/Stop SSID**の場合だけです。ターゲットSSIDを選択するには、次の手順を実行します。

   a. **Select SSID**をクリックします。

      Select Deviceウィンドウが開きます。

   b. query criterionを入力します。

   c. **Query**をクリックします。

   d. **SSID List**には、クエリー基準に一致するすべてのSSIDが表示されます。

   e. 管理するSSIDを選択します。

   f. **OK**をクリックします。

選択したすべてのSSIDがSSIDボックスに表示されます。

- **Execution Mode**: エネルギーポリシーを実行するモードを選択します。オプションは、**One-off**および**Periodic**です。

  One-offが選択されている場合は、次のパラメーターを設定します。

  - **One-off**ボックスの右側のリストから、WSMで実行する操作を選択します。操作オプションは、開始/停止タイプのエネルギーポリシーの場合は**Start/Stop**、**Start**、および**Stop**で、無線電力の変更タイプのエネルギーポリシーの場合は**Change/Restore**、**Change**、および**Restore**です。
  - **Stopped at**: WSMでAP、無線、またはSSIDの電源をオフにする時刻を、スケジュールされた時刻に、またはエネルギーポリシーが追加された直後に選択します。**Scheduled**を選択した場合は、**Scheduled**ボックスの右側のボックスにスケジュールされた時刻をYYYY-MM-DD hh:mm:ss形式で入力するか、カレンダーイコンをクリックしてスケジュールされた時刻を選択します。このパラメーターは、**One-off**ボックスで**Start/Stop**または**Stop**を選択した場合にのみ表示されます。停止時刻は、開始時刻と同じにすることはできません。また、現在の時刻より前にすることはできません。
  - **Started at**: WSMでAP、無線、またはSSIDの電源をオンにする時刻を、スケジュールされた時刻に、またはエネルギーポリシーが追加された直後に選択します。**Scheduled**を選択した場合は、**Scheduled**ボックスの右側のボックスにスケジュールされた時刻をYYYY-MM-DD hh:mm:ss形式で入力するか、カレンダーイコンをクリックしてスケジュールされた時刻を選択します。このパラメーターは、**One-off**ボックスで**Start/Stop**または**Start**を選択した場合にのみ表示されます。開始時刻を終了時刻と同じにすることはできません。また、開始時刻を現在の時刻より前にすることはできません。
  - **Recovered at:** WSMで無線の電力を復元する時刻を、スケジュールされた時刻、またはエネルギーポリシーが追加された直後から選択します。**Scheduled**を選択した場合は、**Scheduled**ボックスの右側のボックスにスケジュール時刻をYYYY-MM-DD hh:mm:ss形式で入力するか、カレンダーイコンをクリックしてスケジュール時刻を選択します。このパラメーターは、**One-off**ボックスで**Change/Restore**または**Restore**を選択した場合にのみ表示されます。リストア時刻は、変更時刻と同じにすることはできません。また、現在の時刻より前にすることはできません。
  - **Modified at**: WSMで無線の電力を変更する時刻を、スケジュールされた時刻に、またはエネルギーポリシーが追加された直後に選択します。**Scheduled**を選択した場合は、**Scheduled**ボックスの右側のボックスにスケジュール時刻をYYYY-MM-DD hh:mm:ss形式で入力するか、カレンダーイコンをクリックしてスケジュール時刻を選択します。このパラメーターは、**One-off**ボックスで**Change/Restore**または**Change**を選択した場合にのみ表示されます。変更時刻を復元時刻と同じにすることはできません。また、変更時刻を現在の時刻より前にすることはできません。
  - **Restored Power**: WSMで無線に対して復元する電力値を入力します。値の範囲は1～27 dBmです。このパラメーターは、**One-off**ボックスで**Change/Restore**または**Restore**が選択されている場合にだけ表示されます。
  - 変更された電力WSMで無線に対して変更する電力値を入力します。値の範囲は1～27 dBmです。このパラメーターは、**One-off**ボックスで**Change/Restore**または**Change**が選択されている場合にだけ表示されます。

  Periodicalを選択した場合は、次のパラメーターを設定します。

  - **Execution Period**: タスクが実行される間隔を選択します。オプションは次のとおりです: **Every Day, Every Week**、および**Every Month**。
  - **Stopped at**: WSMでAP、無線、またはSSIDの電源を切断する時刻をhh:mm:ss形式で入力します。停止時刻は、開始時刻と同じにすることはできません。また、現在の時刻より前にすることはできません。
  - **Started at**: WSMでAP、無線、またはSSIDの電源をオンにする時刻をhh:mm:ss形式で入力します。開始時刻は、終了時刻と同じにすることはできません。また、現在の時刻より前

にすることはできません。

- **Recovered at**: WSMが無線の電力を復元する時刻をhh:mm:ss形式で入力します。復元時刻を変更時刻と同じにすることはできません。また、現在の時刻より前の時刻にすることはできません。
- **Modified at**: WSMで無線の電力を変更する時刻をhh:mm:ss形式で入力します。変更時刻は、復元時刻と同じにすることはできません。また、現在の時刻より前にすることはできません。
- **Restored Power**: WSMで無線に対して復元する電力値を入力します。値の範囲は1～27 dBmです。
- **Changed Power**: WSMで無線に対して変更する電力値を入力します。値の範囲は1～27 dBmです。
- **Always Effective**: 変更されるまでエネルギーポリシーを有効にする場合は、このオプションを選択します。
- **Validated at**: エネルギーポリシーが有効になる時刻をYYYY-MM-DD hh:mm:ss形式で入力するか、カレンダーイコンをクリックして有効な時刻を選択します。このパラメーターは、**Always Effective**オプションが選択されていない場合にのみ表示されます。有効な時刻は、有効期限より前である必要があり、現在の時刻より前にすることはできません。
- **Expired at:** エネルギーポリシーの有効期限が切れる時刻をYYYY-MM-DD hh:mm:ss形式で入力するか、カレンダーイコンをクリックして有効期限を選択します。このパラメーターが表示されるのは、**Always Effective**オプションが選択されていない場合だけです。有効期限は、有効期限よりも後にする必要があり、現在の時刻よりも前にすることはできません。

- **Description**: エネルギーポリシーの説明を入力します。

5. エネルギーポリシーを適用するデバイスを選択します。

選択するデバイスは、エネルギーポリシーの動作タイプによって異なります。エネルギーポリシーのポリシータイプが**Start/Stop AP**の場合は、APを選択します。そうでない場合は、fit AP無線とfat AP無線の両方を選択します。

APを追加するには:

a 次の手順を実行し**AP List**領域の**Add**をクリックします。

Select Deviceウィンドウが開きます。

b 問合せ基準を入力します。

c **Query**をクリックします。

Device Listには、クエリー基準に一致するすべてのAPが表示されます。

d 管理するAPを選択します。

e **OK**をクリックします。

選択したすべてのAPがAPリストに表示されます。

fit AP無線を追加するには、次の手順を実行します。

a. **Fit AP Radio List**領域の**Add**をクリックします。

Select Deviceウィンドウが開きます。

b. 問合せ基準を入力します。

c. **Query**をクリックします。

Radio Listには、基準に一致するすべての無線が表示されます。

d. 管理するfit AP無線を選択します。

e. **OK**をクリックします。

選択したすべての無線がFit AP Radio Listに表示されます。

FAT AP無線を追加するには、次の手順を実行します。

a. **Fat AP Radio List**領域の**Add**をクリックします。

   Select Deviceウィンドウが開きます。

b. 問合せ基準を入力します。

c. **Query**をクリックします。

   Radio Listには、クエリー基準に一致するすべての無線が表示されます。

d. 管理するFAT AP無線を選択します。

e. **OK**をクリックします。

   選択したすべての無線が Fat AP Radio List に表示されます。

6. **OK**をクリックします。

   新しいエネルギーポリシーが Energy Policy List に表示されます。

既存のエネルギーポリシーのコピー

エネルギーポリシーを追加する設定を簡略化するために、既存のエネルギーポリシーをコピーし、必要に応じてパラメーターを変更できます。WSMを使用すると、認可されたユーザーは、ポリシータイプを除くコピーされたエネルギーポリシーのすべての基本アトリビュートを変更し、デバイスを再選択できます。

既存のエネルギーポリシーをコピーするには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Energy Policy Management**を選択します。

   Energy Policy Listページには、すべてのエネルギーポリシーが表示されます。
3. コピーするエネルギーポリシーの**Copy**アイコンをクリックします。

   Copy Energy Policyページが開きます。
4. エネルギーポリシーのパラメーターを変更します。

   既存のエネルギーポリシーのポリシー名は、一意の名前に置き換える必要があります。ポリシータイプは変更できません。その他のパラメーターの構成については、「エネルギーポリシーの追加」を参照してください。
5. エネルギーポリシーが適用されるデバイスを変更します。

   デバイスの選択について詳しくは、「エネルギーポリシーの追加」を参照してください。
6. **OK**をクリックします。

新しいエネルギーポリシーが Energy Policy List に表示されます。

エネルギーポリシーの変更

WSMでは、権限のあるユーザーが、ステータスが実行中でないエネルギーポリシーを変更できます。エネルギーポリシーを変更するには、次の手順を実行します:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Energy Policy Management**を選択します。

   Energy Policy Listページには、すべてのエネルギーポリシーが表示されます。
3. 変更するエネルギーポリシーの**Modify**アイコンをクリックします。**Modify Energy Policy**ページが開きます。

4. エネルギーポリシーのパラメーターを変更します。

   ポリシー名、ポリシータイプ、および選択したデバイスは変更できません。その他のパラメーターの設定については、「エネルギーポリシーの追加」を参照してください。

5. **OK**をクリックします。

エネルギーポリシーの削除

WSMを使用すると、許可されたユーザーは、期限切れまたは不要なエネルギーポリシーを削除できます。

エネルギーポリシーを削除するには、次の手順を実行し

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Energy Policy Management**を選択します。

   Energy Policy Listページには、すべてのエネルギーポリシーが表示されます。

3. 削除する各エネルギーポリシーの**Delete**アイコンをクリックします。または、削除するエネルギーポリシーを選択し、**Energy Policy List**領域の上部にある**Delete**をクリックします。
4. 確認ダイアログボックスで、**OK**をクリックします。

   選択したエネルギーポリシーが**Energy Policy List**から削除されます。

エネルギーポリシーの停止

WSMを使用すると、許可されたユーザーは、実行を待機している通常のエネルギーポリシーを一時的に一時停止できます。そのためには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Energy Policy Management**を選択します。**Energy Policy List**ページには、すべてのエネルギーポリシーが表示されます。
3. 一時停止するエネルギーポリシーを選択します。
4. **Suspend**をクリックします。
5. 確認ダイアログボックスで、**OK**をクリックします。

   Energy Policy Listで、選択したエネルギーポリシーの状態が**Suspended**に変わります。

中断していたエネルギーポリシーの再開

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Energy Policy Management**を選択します。

   Energy Policy Listページには、すべてのエネルギーポリシーが表示されます。

3. 再開する一時停止中のエネルギーポリシーを選択します。
4. **Resume**をクリックします。
5. 確認ダイアログボックスで、**OK**をクリックします。

エネルギーポリシーの実行結果の表示

WSMを使用すると、許可されたユーザーは、各APまたは無線での結果を含む、エネルギーポリシーの詳細な実行結果を表示できます。

エネルギーポリシーの詳細な実行結果を表示する手順は、次のとおりです。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager > Energy Policy Management**を選択します。**Energy Policy List**ページには、すべてのエネルギーポリシーが表示されます。
3. **Status--Operation Result**フィールドで、実行結果を表示するエネルギーポリシーの内容をクリックします。

   Policy Execution Resultページが開きます。
4. **Policy Execution Time**リストから、エネルギーポリシーが実行された時刻を選択します。

   エネルギーポリシーが**Start/Stop AP**の場合、**Policy Execution Result**ページに**AP List**が表示されます。表示されない場合は、**Fit AP Radio List**および**Fat AP Radio List**が表示されます。

   APリストの内容

   - **AP Label/Device Label**: APのデバイスラベル。
   - **AP SN**: APのシリアル番号。
   - **IP Address**: APのIPアドレス。
   - **Start Time**: WSMがエネルギーポリシーの実行を開始する時刻。
   - **End Time**: WSMがエネルギーポリシーの実行を停止する時刻。
   - **Status**: エネルギーポリシーの実行ステータス。オプションは、**Waiting**、**Executing**、**Suspended**および**Finished**です。
   - **Result**: エネルギーポリシーの実行結果。オプションは**Succeeded**および**Failed**です。
   - **Failure Reason**: 実行結果が**Failed**の場合、このフィールドには失敗理由が表示されます。失敗した場合、このフィールドは空白になります。

   FIT APラジオの内容

   - **AP SN**: 無線がイネーブルになっているAPのシリアル番号。
   - **Radio ID**: 無線のID。
   - **AP Template Name**: 無線がイネーブルになっているfit APに適用されるAPテンプレートの名前。
   - **Start Time**: WSMがエネルギーポリシーの実行を開始する時刻。
   - **End Time**: WSMがエネルギーポリシーの実行を停止する時刻。
   - **Status**: エネルギーポリシーの実行ステータス。オプションは、**Waiting**、**Executing**、**Suspended**および**Finished**です。
   - **Result**: エネルギーポリシーの実行結果。オプションは**Succeeded**および**Failed**です。
   - **Failure Reason**: 実行結果がFailedの場合、このフィールドには失敗理由が表示されます。失敗した場合、このフィールドは空白になります。

   Fat AP Radioコンテンツ

   - **Interface**: 無線に接続するFAT APのインターフェース。
   - **AP Alias**: 無線がイネーブルになっているFAT APの名前。
   - **Radio Type**: オプションは、802.11a、802.11b、802.11g、802.11an、および802.11gnです。
   - **Start Time**: WSMがエネルギーポリシーの実行を開始する時刻。
   - **End Time**: WSMがエネルギーポリシーの実行を停止する時刻。
   - **Status**: エネルギーポリシーの実行ステータス。オプションは、**Waiting**、**Executing**、**Suspended**および**Finished**です。
   - **Result**: エネルギーポリシーの実行結果。オプションはSucceedおよびFailedです。
   - **Failure Reason**: 実行結果がFailedの場合、このフィールドには失敗理由が表示されま

す。失敗した場合、このフィールドは空白になります。メッシュネットワークを管理する従来のWLANとは異なり、WLANメッシュネットワークではAP間のワイヤレス接続が可能であるため、WLANのモバイル性と柔軟性が向上します。さらに、AP間にマルチホップワイヤレスリンクを確立できます。

WLANメッシュには次の利点があります。

- 低コストで高性能
- 新しい配線やアクセスポイントを必要としない拡張性
- メトロ、企業、オフィス、大規模倉庫、製造、港湾、ウォーターフロントなどのエリアに適用できます。
- マルチパス可用性によるシングルポイント障害の回避図90および図91は、一般的なWLANメッシュネットワークのアプリケーションを示しています。

図90 一般的なWLANメッシュネットワーク(ACアプリケーション)

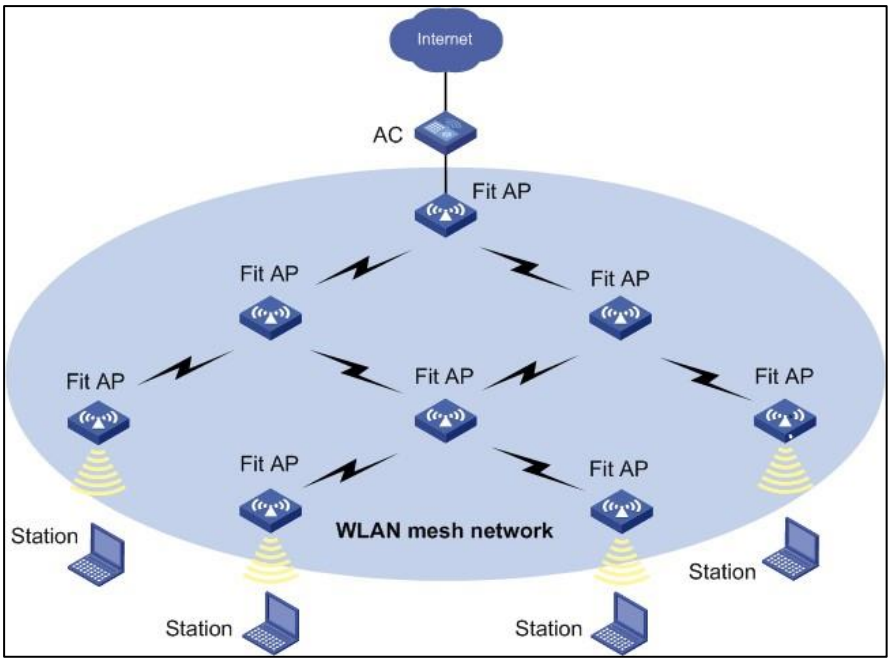
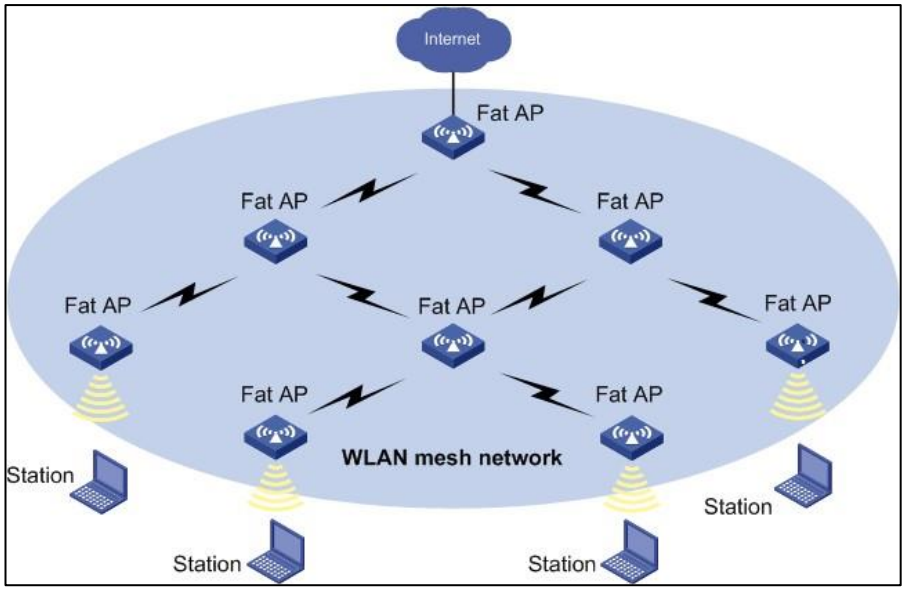


図91 一般的なWLANメッシュネットワーク(FAT APアプリケーション)



メッシュ管理は、メッシュネットワークの確立と維持に使用されます。メッシュ管理には、次のオブジェクトが含まれます。

- メッシュプロファイル
- メッシュポリシー
- メッシュインターフェース
- ピアAPのMACアドレス
- メッシュトポロジ

メッシュ管理をサポートしているのは、ComwareベースのACおよびAPだけです。

メッシュプロファイルの管理

メッシュプロファイルはMesh Point(MP)にマッピングされ、同じメッシュプロファイルがマッピングされた他のMPにメッシュサービスを提供できます。次の情報では、メッシュプロファイルの管理操作について説明します。

メッシュプロファイルリストの表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager > Resource Management > ACs**または**WLAN Manager > Resource Management > Fat APs**を選択します。
3. ACまたはFAT APのデバイスラベルをクリックして、デバイス情報ページを表示します。
4. ページの右下隅にある**Mesh Management**メニューで、**Mesh Profile Management**をクリックします。

   Mesh Profile Managementには、すべてのメッシュプロファイルが表示されます。

   メッシュプロファイルリストの内容

   - **Mesh Profile ID**: メッシュプロファイルのID。
   - **Mesh ID**: メッシュネットワークのID。
   - **Link Keep Alive Interval**: キープアライブを送信する間隔(秒数)。キープアライブの送信を3回試行してもAPがピアAPから応答を受信しない場合、メッシュリンクは切断されます。

- **Link Backhaul Rate**: メッシュリンクのバックホールレート。この値は無線タイプによって異なり、1つのメッシュネットワーク内で同じである必要があります。
- **Enable Mesh Profile**: メッシュプロファイルが有効かどうかを示します。メッシュプロファイルは、ポートセキュリティが設定されたメッシュインターフェースにバインドされている場合にだけ有効にできます。
- **Enable MKD Service**: メッシュプロファイルのMKDサービスがイネーブルかどうかを示します。これはACだけでサポートされます。

- **Operation**: メッシュプロファイルを変更または削除し、メッシュプロファイルにバインドされた無線を表示するには、**Operation**アイコン をクリックします。

ACの**Mesh Profile Management**ページに、メッシュプロファイルにバインドされる無線が表示されます。

ラジオ一覧の内容

- **Admin Status**: 無線の管理状態。オプションは**Up**および**Down**です。
- **Radio ID**:無線のID。
- **AP Template Name**: 無線が属するAPで使用されるテンプレートの名前。
- **Radio Type**: リストから無線のタイプを選択します。オプションは次のとおりです。
  - **802.11a**
  - **802.11b**
  - **802.11g**
  - **802.11gn**
  - **802.11an**
- **Mesh Profile ID**: 無線がバインドされているメッシュプロファイルのID。無線がどのメッシュプロファイルにもバインドされていない場合、このフィールドには0と表示されます。
- **Delete**: メッシュプロファイルにバインドする必要のない無線を削除するには、**Delete**アイコンをクリックします。

FAT APの**Mesh Profile Management**ページには、FAT APのすべての無線が表示されます。

ラジオ情報の内容

- **Interface**: メッシュプロファイルにバインドされる無線インターフェース。インターフェースリンクをクリックすると、FAT AP無線の詳細ページが表示されます。
- **Radio Type**: リストから無線のタイプを選択します。オプションは次のとおりです。
  - **802.11a**
  - **802.11b**
  - **802.11g**
  - **802.11bg**
  - **802.11**
  - **802.11an**
  - **802.11gn**
  - **802.11n(2.4GHz)**
  - **802.11bgn**
  - **802.11n**
  - **802.11n(5GHz)。**
- **Channel**: 無線のチャネル。無線のタイプによって異なります。
- **Max Transmission Power**: 無線の最大送信電力。
- **Modify**: **Modify**アイコンをクリックして、FAT APの無線パラメーターを変更します。詳細については、「FAT APの無線パラメーターの変更」を参照してください。

5. **Related Operations**をクリックし、表示されるメニューで**MP Policy Management**または

Mesh Interface Managementを選択します。

メッシュプロファイルの詳細の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager>Resource Management>ACs**または**WLAN Manager>Resource Management>Fat APs**を選択します。
3. ACまたはFAT APのデバイスラベルをクリックして、デバイス情報ページを表示します。
4. ページの右下隅にあるメッシュ管理メニューで、メッシュプロファイル管理をクリックしてメッシュプロファイルリストページを表示します。
5. メッシュプロファイルリンクをクリックします。

   ダイアログボックスが開き、**Mesh Profile ID**、**Mesh ID**、**Mesh Interface ID**、**Link Keep Alive Interval(s)**、**Link Backhaul Rate(Mb/s)**、**Enable Mesh Profile**、および**Enable MKD Service**に関する情報が表示されます。

   パラメーターリストの内容

   - **Mesh Interface ID**: メッシュプロファイルにバインドされているインターフェースのID。1つのインターフェースは1つのメッシュプロファイルにのみバインドできます。

その他のパラメーターについては、「メッシュプロファイルリストの表示」を参照してください。

6. **Close**をクリックします。

メッシュプロファイルの追加

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager>Resource Management>ACs**または**WLAN Manager>Resource Management>Fat APs**を選択します。
3. ACまたはFAT APのデバイスラベルをクリックして、デバイス情報ページを表示します。
4. ページの右下隅にある**Mesh Management**メニューで、**Mesh Profile Management**をクリックします。

   Mesh Profile Managementページが開きます。
5. メッシュプロファイルの追加をクリックします。
6. メッシュプロファイルの次のパラメーターを設定します。
   - **Mesh Profile ID**: メッシュプロファイルのIDを入力します。メッシュプロファイルIDは、同じデバイス上で一意である必要があります。
   - **Mesh ID**: メッシュネットワークのIDを入力します。既存のIDと同じIDは使用できません。
   - **Binding Mesh Interface**: このオプションを選択した場合は、**Mesh Interface ID**を設定する必要があります。このオプションを選択しないと、メッシュプロファイルを有効にできません。
   - **Mesh Interface ID**: メッシュプロファイルにバインドされるメッシュインターフェースのID。1つのメッシュインターフェースは1つのメッシュプロファイルにのみバインドできます。
   - **Link Backhaul Rate**: メッシュリンクのバックホールレート。この値は無線タイプによって異なり、1つのメッシュネットワーク内で同じである必要があります。
   - **Link Keep Alive Interval**: キープアライブを送信する間隔(秒数)。キープアライブの送信を3回試行してもAPがピアAPから応答を受信しない場合、メッシュリンクは切断されます。
   - **Enable Mesh Profile**: メッシュプロファイルを有効にします。メッシュプロファイルは、ポートセキュリティが設定されたメッシュインターフェースにバインドされている場合にだけ有効にできます。
   - **Enable MKD Service**: ACをメッシュプロファイルのMKDデバイスとして設定します。これは

ACでのみサポートされます。

7. OKをクリックします。

メッシュプロファイルの変更

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager>Resource Management>ACs**または**WLAN Manager>Resource Management>Fat APs**を選択します。
3. ACまたはFAT APのデバイスラベルをクリックして、デバイス情報ページを表示します。
4. ページの右下隅にあるメ**Mesh Management**メニューで、**Mesh Profile Management**をクリックします。

   Mesh Profile Management ページが開きます。
5. ターゲットメッシュプロファイルの**Operation**アイコン をクリックし、**Modify**アイコンをクリックします。
6. メッシュプロファイルのパラメーターを修正してください。**Mesh Profile ID**は修正できません。
   他のパラメーターの詳細については、「メッシュプロファイルの追加」を参照してください。
7. OKをクリックします。

メッシュプロファイルの削除

メッシュプロファイルが無線にバインドされている場合は、削除できません。メッシュプロファイルを削除する前に、無線のバインドを解除する必要があります。無線のバインド解除の詳細については、「メッシュプロファイルのバインド解除」を参照してください。

メッシュプロファイルを削除するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager>Resource Management>ACs**または**WLAN Manager>Resource Management>Fat APs**を選択します。
3. ACまたはFAT APのデバイスラベルをクリックして、デバイス情報ページを表示します。
4. ページの右下隅にある**Mesh Management**メニューで、**Mesh Profile Management**をクリックします。

   Mesh Profile Managementページが開きます。
5. ターゲットメッシュプロファイルの**Operation**アイコンをクリックし、ショートカットメニューの**Delete**を選択します。
6. **OK**をクリックします。

メッシュプロファイルのバインド

この機能を使用すると、メッシュプロファイルを複数の無線にバインドして、ACとFit AP間、およびFat AP間でメッシュサービスを提供できます。

FIT AP上の無線へのメッシュプロファイルのバインド

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager>Resource Management>ACs**を選択します。
3. ACのデバイスラベルをクリックします。
4. ページの右下隅にある**Mesh Management**メニューで、**Mesh Profile Management**をクリックします。

Mesh Profile Managementページが開きます。

5. **Radio List**領域で、**Add**をクリックします。

   無線を選択するためのウィンドウが開きます。

6. 無線を選択します。無線信号が強いほど、メッシュリンクは安定します。ベストプラクティスとして、802.11a無線を選択します。

   または、次のように検索基準を設定して、無線を選択する前に無線を照会することもできます。

   a. 次のいずれかの検索条件を入力します。
      - **AP Label**, **AP Name**
      - **Serial Number**
      - **Radio Type**
      - **Admin Status**
      - **Mesh Profile ID**
      - **Location**

      空のフィールドや無制限に設定されたフィールドは、クエリーの抽出条件にはなりません。

   b. **Query**をクリックします。

      無線リストには、一致するすべての無線が表示されます。

7. **Reset**をクリックして無線を表示するには、Resetをクリックします。OKをクリックすると、選択した無線が表示されます。
8. **Mesh Profile List**領域で、バインドするメッシュプロファイルを選択します。
9. **Bind Mesh Profile**をクリックします。

   操作結果ページにバインド結果が表示されます。

メッシュプロファイルをFAT AP上の無線にバインドする

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager>Resource Management>Fat APs**を選択します。
3. FAT APの名前リンクをクリックして、デバイス情報ページを表示します。
4. ページの右下隅にある**Mesh Management**メニューで、**Mesh Profile Management**をクリックします。

   Mesh Profile Managementページが開きます。

5. 無線情報領域で、バインドする無線の**Modify**アイコンをクリックします。無線信号が強いほど、メッシュリンクは安定します。ベストプラクティスとして、802.11a無線を使用します。
6. **Mesh Profile ID**リストからメッシュプロファイルIDを選択します。FAT APに追加されたメッシュプロファイルがリストに表示されます。
7. **Channels in Use**リストからチャネルを選択します。

   チャネルは無線の種類によって異なります。このオプションを**Auto**に設定することはできません。

8. OKをクリックします。

   操作結果ページにバインド結果が表示されます。

メッシュプロファイルのバインド解除

メッシュプロファイルのバインドを解除した後、メッシュプロファイルを削除できます。

FIT AP上の無線からのメッシュプロファイルのアンバインド

1. **Service**タブをクリックします。

2. **WLAN Manager>Resource Management>ACs**を選択します。
3. ACの名前リンクをクリックして、デバイス情報ページを表示します。
4. ページの右下隅にある**Mesh Management**メニューで、**Mesh Profile Management**をクリックします。

   Mesh Profile Managementページが開きます。
5. **Radio List**領域で、**Add**をクリックします。

   無線を選択するためのダイアログボックスが開きます。
6. プロファイルのバインドを解除する無線を選択します。

   または、次のように検索基準を設定して、無線を選択する前に無線を照会することもできます。

   a. 次の検索条件を入力します。
      - **AP Label**
      - **AP Name**
      - **Serial Number**
      - **Radio Type**
      - **Admin Status**
      - **Mesh Profile ID**
      - **Location**.

   空のフィールドや**Unlimited**に設定されたフィールドは、Queryの抽出条件にはなりません。

   b. **Query**をクリックします。

      無線リストには、一致するすべての無線が表示されます。

      Resetをクリックして検索条件をクリアして、全ての無線を表示します。
7. **OK**をクリックします。

   選択した無線が表示されます。
8. メ**Mesh Profile List**領域で、メッシュプロファイルを選択します。
9. **Unbind Mesh Profile**をクリックします。

操作結果ページに結果が表示されます。

FAT AP上の無線からのメッシュプロファイルのアンバインド

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager>Resource Management>Fat APs**を選択します。
3. FAT APの名前リンクをクリックして、デバイス情報ページを表示します。
4. ページの右下隅にある**Mesh Management**メニューで、**Mesh Profile Management**をクリックします。

   Mesh Profile Managementページが開きます。
5. **Modify**アイコンをクリックします。
6. **Mesh Profile ID**リストから**None**を選択します。
7. **OK**をクリックします。

メッシュプロファイルにバインドされた無線の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager>Resource Management>ACs**または**WLAN Manager>Resource Management>Fat APs**を選択します。

3. ACまたはFAT APのデバイスラベルをクリックして、デバイス情報ページを表示します。
4. ページの右下隅にある**Mesh Management**メニューで、**Mesh Profile Management**をクリックします。

   Mesh Profile Managementページが開きます。
5. メッシュプロファイルの**Operation**アイコン をクリックし、ショートカットメニューから**Bound Radios**アイコンを選択します。

   Radio Listダイアログボックスが開き、メッシュプロファイルにバインドされた無線が表示されます。次の操作を実行できます。
   - **Unbind**: メッシュプロファイルからアンバインドする無線を選択し バインドを解除して、バインドを削除します。
   - **Close**: **Close**をクリックして、ダイアログボックスを閉じます。

MPポリシーの管理

リンクの形成と維持は、MPポリシーで指定された属性によって駆動されます。MPポリシー管理では、次の操作を実行できます。

MPポリシーの表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Resource Management>ACs**または**WLAN Manager>Fat APs**を選択します。
3. ACまたはFAT APのデバイスラベルをクリックして、デバイス情報ページを表示します。
4. ページの右下隅にある**Mesh Management**メニューで、**MP Policy Management**をクリックします。

   MP Policy Managementページが開きます。

   MPポリシーリストの内容
   - **Policy Name**: MPポリシーの名前。
   - **Enable Link Initiation**: MPポリシーのリンク開始ステータス。オプションは**Enable**および**Disable**。リンク開始がイネーブルの場合、APはそのピアAPを検索します。
   - **Link Maximum Number**: APの無線が他のAPと確立できるメッシュリンクの最大数。
   - **Link Hold RSSI**: リンクを形成と保持を可能にする最小RSSI。アクティブリンクのRSSIがこの値よりも小さくなると、リンクスイッチが実行されます。
   - **Link Hold Time**: アクティブリンクをアップ状態に維持する最小時間。リンクホールドタイム内では、リンクスイッチのマージンに達してもアクティブリンクはアップ状態のままです。リンクスイッチのマージンおよびリンクスイッチングの優先度の詳細は、「MPポリシーの追加」を参照してください。
   - **Link Saturation RSSI**: アクティブなリンクの最大RSSI。この値に達すると、リンクが切り替えられます。
   - **Probe Request Interval**: APによるプローブ要求の送信間隔。APはプローブ要求を送信してピアAPをスキャンし、応答に応答して、ネイバーテーブルを確立します。
   - **Operation**: MPポリシーを変更または削除し、MPポリシーにバインドされた無線を表示するには、MPポリシーの**Operation**アイコンをクリックします。デフォルトのMPポリシー**default_mp_plcy**は変更または削除できません。
5. **More**をクリックし、**AP Configuration**、**Mesh Interface Management**、または**Mesh Profile Management**を選択して、設定ページを開きます。

   MP Policy Listに十分なエントリーが含まれている場合は、次のナビゲーション支援が表示されます。

MP Policy Listのナビゲート

- **Next Page**アイコンをクリックして、**MP Policy List**で次のページに進みます。
- **Last Page**アイコンをクリックすると、**MP Policy List**の最後にページ送りされます。
- **Previous Page**アイコンをクリックして、**MP Policy List**で前のページに戻ります。
- **First Page**アイコンをクリックすると、**MP Policy List**の先頭に戻ることができます。
- MPポリシーリストの右上にある8、15、50、100、または200をクリックして、各ページに表示する項目数を指定します。

6. ACの**MP Policy Management**ページには、MPポリシーにバインドされる無線が表示されます。

ラジオ一覧の内容

- **Admin Status**: 無線の管理状態。オプションはUpおよびDownです。
- **Radio ID**: 無線のID。
- **AP Template Name**: 無線が属するAPで使用されるテンプレートの名前。
- **Radio Type**: リストから無線のタイプを選択します。オプションは次のとおりです。
  - **802.11a**
  - **802.11b**
  - **802.11g**
  - **802.11gn**
  - **802.11an**
- **MP Policy Name**: 無線がバインドされるMPポリシーの名前。デフォルトでは、デフォルトのMPポリシー**default_mp_plcy**がすべての無線にバインドされます。
- **Delete**: MPポリシーにバインドする必要がない無線を削除するには、**Delete**アイコンをクリックします。

7. FAT APの**MP Policy Management**ページには、FAT APのすべての無線が表示されます。

ラジオ一覧の内容

- **Interface**: MPポリシーにバインドされた無線インターフェース。インターフェースリンクをクリックすると、FAT AP無線の詳細ページが表示されます。
- **Radio Type**: リストから無線のタイプを選択します。オプションは次のとおりです。
  - **802.11a**
  - **802.11b**
  - **802.11g**
  - **802.11bg**
  - **802.11at**
  - **802.11an**
  - **802.11gn**
  - **802.11n(2.4GHz)**
  - **802.11bgn**
  - **802.11n**
  - **802.11n(5GHz)**
- **Channel**: 無線のチャネル。無線タイプによって異なります。
- **Max Transmission Power**: 無線の最大送信電力。
- **Modify**: **Modify**アイコンをクリックして、FAT AP無線のパラメーターを変更します。無線パラメーターの変更の詳細については、「FAT APの無線パラメーターの変更」を参照してください。

8. **Related Operations**をクリックして、表示されるメニューから**Mesh Profile Management**または**Mesh Interface Management**を選択します。

MPポリシーの詳細の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager>Resource Management>ACs**または**WLAN Manager>Resource Management>Fat APs**を選択します。
3. ACまたはFAT APのデバイスラベルをクリックして、デバイス情報ページを表示します。
4. ページの右下隅にある**Mesh Management**メニューで、**MP Policy Management**をクリックします。

   MP Policy Managementページが開きます。
5. ターゲットMPポリシー名のリンクをクリックします。

   ダイアログボックスが開き、MPポリシーに関する詳細情報が表示されます。

   MPポリシーの詳細

   - **Policy Name**: MPポリシーの名前。
   - **Enable Link Initiation**: MPポリシーのリンク開始ステータス。オプションは**Enable**と**Disable**。リンク開始がイネーブルの場合、APはそのピアAPを検索します。
   - **Link Maximum Number**: APの無線が他のAPと確立できるメッシュリンクの最大数。
   - **Link Rate Mode**: メッシュリンクのコストを計算する方法。オプションは次のとおりです。
     - **Fixed**: 現在の無線の最大固定レートを使用して、メッシュリンクのコストを計算します。
     - **Realtime**: リアルタイムRSSIを使用してメッシュリンクのコストを計算します。
   - **Probe Request Interval**: APによるプローブ要求の送信間隔。APはプローブ要求を送信してピアAPをスキャンし、応答に応答して、ネイバーテーブルを確立します。
   - **Link Hold RSSI**: リンクを形成と保持を可能にする最小RSSI。アクティブリンクのRSSIがこの値よりも小さくなると、リンクスイッチが実行されます。
   - **Link Hold Time**: アクティブリンクをアップ状態に維持する最小時間。リンクホールドタイム内では、リンクスイッチのマージンに達してもアクティブリンクはアップ状態のままです。
   - **Link Saturation RSSI**: アクティブなリンクの最大RSSI。この値に達すると、リンクが切り替えられます。
   - **Link Switch Margin**: 新しいリンクのRSSIが現在のアクティブリンクのRSSIよりもリンクスイッチマージン分だけ大きい場合、アクティブリンクスイッチが発生します。この機能は、ACアプリケーションのメッシュネットワークでのみサポートされています。
   - **Enable Role Authenticator**: ロールオーセンティケータが有効かどうかを示します。メッシュリンクを確立するには、2つのAPのいずれかでロールオーセンティケータを有効にする必要があります。この機能は、ACアプリケーションのメッシュネットワークでのみサポートされています。
   - **Enable MLSP**: MLSPプロトコルがイネーブルかどうかを示します。MLSPは、列車の移動中にリンクを作成および切断するために使用され、アクティブなリンクがいつでも列車MPで使用できるようにします。この機能は、ACアプリケーションのメッシュネットワークでのみサポートされています。
   - **MLSP Proxy MAC Address**: MLSP対応FIT APに接続しているデバイスのMACアドレス。地下鉄メッシュネットワークでリンクスイッチオーバーが発生すると、列車MPは、MLSPプロキシが設定されている場合、トラフィックの中断を回避するためにレールMPに接続しているスイッチがARPエントリーを迅速に更新できるように、gratuitous ARPパケットを送信します。この機能は、ACアプリケーションのメッシュネットワークだけでサポートされています。この項目は、MLSPがイネーブルでプロキシMACアドレスが設定されている場合に、ACアプリケーションの

メッシュネットワークに対して表示されます。

6. **Close**をクリックします。

MPポリシーの追加

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager>Resource Management>ACs**または**WLAN Manager>Resource Management>Fat APs**を選択します。
3. ACまたはFAT APのデバイスラベルをクリックして、デバイス情報ページを表示します。
4. ページの右下隅にあるメッシュ管理メニューで、MPポリシー管理をクリックします。

   MPポリシー管理ページが開きます。
5. Add Policyをクリックして、Add MP Policyページを開きます。
6. 次のパラメーターを設定します。
   - **Policy Name**: MPポリシーの名前を入力します。MPポリシー名は、同じデバイス上で一意である必要があります。
   - リンク開始の有効化: リンク開始を有効にするオプションを選択します。リンク開始が有効な場合、APはそのピアAPを検索します。
   - **Link Maximum Number**: APの無線が他のAPと確立できるメッシュリンクの最大数を設定します。
   - **Link Rate Mode**: メッシュリンクのコストを計算する方法を選択します。オプションは次のとおりです。
     - **Fixed**: 現在の無線の最大固定レートを使用して、メッシュリンクのコストを計算します。
     - **Realtime**: リアルタイムRSSIを使用してメッシュリンクのコストを計算します。
   - プローブ要求間隔: APがプローブ要求を送信する間隔を設定します。APはプローブ要求を送信してピアAPをスキャンし、応答に応答して、ネイバーテーブルを確立します。
   - リンクホールドRSSI: リンクが形成され、保持されるように最小RSSIを設定します。アクティブリンクのRSSIがこの値より小さくなると、リンクスイッチが発生します。
   - **Link Hold Time**: アクティブリンクをアップ状態に維持する最小時間を設定します。リンクホールドタイム内では、リンクスイッチのマージンに達してもアクティブリンクはアップ状態のままです。
   - **Link Saturation RSSI**: アクティブリンクの最大RSSIを設定します。この値に達すると、リンクスイッチが実行されます。
   - リンクスイッチマージン: リンクスイッチマージンを設定します。新しいリンクのRSSIが現在のアクティブリンクのRSSIよりもリンクスイッチマージンだけ大きい場合は、アクティブリンクスイッチが発生します。この機能は、ACアプリケーションのメッシュネットワークでのみサポートされています。

   注:

   昇順でリンクスイッチを決定するパラメーターの優先順位は、リンクスイッチマージン、リンクホールドタイム、およびリンク飽和RSSI/リンクホールドRSSIです。

   - リンクホールドタイムが経過すると、新しいリンクのRSSIが現在のアクティブリンクのRSSIよりもリンクスイッチマージン分だけ大きい場合、アクティブリンクスイッチが実行されます。
   - リンクホールド時間内では、アクティブリンクRSSIがリンク飽和RSSIを超えた場合、またはリンクホールドRSSIを下回った場合を除き、アクティブリンクの切り替えは発生しません。

- **Enable Role Authenticator**: ロール認証を有効にするオプションを選択します。メッシュリンクを確立するには、2つのAPのいずれかでロール認証を有効にする必要があります。この機能は、ACアプリケーションのメッシュネットワークでのみサポートされています。
- **Enable MLSP**: MLSPプロトコルをイネーブルにするオプションを選択します。MLSPをイネーブルにする前に、リンクの開始をイネーブルにする必要があります。MLSPは、列車の移動中にリンクを作成および切断して、アクティブリンクがいつでも列車MPで使用できるようにするために使用されます。無線でMLSPがディセーブルの場合、現在のMPポリシーで設定されたMLSPプロキシMACアドレスは削除されます。この機能は、ACアプリケーションのメッシュネットワークでのみサポートされています。
- **MLSP Proxy**: MACアドレスMLSP対応のFit APに接続しているデバイスのMACアドレスを設定します。

  MLSP Proxy MAC Addressフィールドに MACアドレスを入力し、Addをクリックして MLSPプロキシMACアドレスリストにアドレスを追加します。この手順を繰り返して、さらにMACアドレスを追加できます。

  アドレスリストからMACアドレスを削除するには、ターゲットMACアドレスを選択し、Deleteをクリックします。

  地下鉄メッシュネットワークでリンクスイッチオーバーが発生すると、列車MP(MLSPプロキシが設定されている場合)はgratuitous ARPパケットを送信します。これにより、レールMPに接続するスイッチはARPエントリーを迅速に更新してトラフィックの中断を回避できます。この機能は、ACアプリケーションのメッシュネットワークでだけサポートされています。

7. **OK**をクリックします。

MPポリシーの変更

無線にバインドされているデフォルトのMPポリシーdefault_mp_plcyは変更できません。デフォルト以外のMPポリシーを変更するには、まず無線からバインドを解除します。無線を使用したMPポリシーのバインド解除の詳細については、「MPポリシーにバインドされている無線の表示とバインドの削除」を参照してください。

MPポリシーを変更するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager>Resource Management>ACs**または**WLAN Manager>Resource Management>Fat APs**を選択します。
3. ACまたはFAT APのデバイスラベルをクリックして、デバイス情報ページを表示します。
4. ページの右下隅にあるメッシュ管理メニューで、MPポリシー管理をクリックします。

   MPポリシー管理ページが開きます。
5. MPポリシーの**Operation**アイコン をクリックし、ショートカットメニューから**Modify**アイコン を選択します。
6. 必要に応じてMPポリシーパラメーターを変更します。ポリシー名は変更できません。その他のパラメーターの詳細は、「MPポリシーの追加」を参照してください。
7. OKをクリックします。

MPポリシーの削除

無線にバインドされているデフォルトのMPポリシーdefault_mp_plcyは削除できません。デフォルト以外のMPポリシーを削除するには、まず無線からバインドを解除します。無線を使用したMPポリシーのバインド解除の詳細については、「MPポリシーにバインドされている無線の表示とバインドの削除」を参照してください。

MPポリシーを削除するには:

1. **Service**タブをクリックします。

2. ナビゲーションツリーで、**WLAN Manager>Resource Management>ACs**または**WLAN Manager>Resource Management>Fat APs**を選択します。
3. ACまたはFAT APのデバイスラベルをクリックして、デバイス情報ページを表示します。
4. ページの右下隅にあるメッシュ管理メニューで、MPポリシー管理をクリックします。

   MPポリシー管理ページが開きます。
5. MPポリシーの**Operation**アイコン をクリックし、表示されるメニューの**Delete**アイコン をクリックします。
6. OKをクリックします。

MPポリシーのバインド

1つのMPポリシーを複数の無線にバインドできます。MPポリシーの設定によって、無線のメッシュリンクの確立とメンテナンスがトリガーされます。デフォルトでは、デフォルトのMPポリシーdefault_mp_plcyが無線にバインドされます。

FIT AP上の無線へのMPポリシーのバインディング

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager>Resource Management>ACs**を選択します。
3. ACのデバイスラベルをクリックすると、デバイス情報ページが表示されます。
4. ページの右下隅にあるメッシュ管理メニューで、MPポリシー管理をクリックします。

   MPポリシー管理ページが開きます。
5. Radio List領域でAddをクリックします。

無線を選択するためのダイアログボックスが開きます。

6. MPポリシーをバインドする無線を選択します。無線信号が強いほど、メッシュリンクはより安定します。ベストプラクティスとして、802.11a無線を選択します。

または、次のように検索基準を設定して、無線を選択する前に無線を照会することもできます。

a. 次の選択条件を入力します。
   - APラベル
   - AP名
   - シリアル番号
   - 無線タイプ
   - 管理ステータス
   - MPポリシー名
   - 場所。

   空のフィールドや無制限に設定されたフィールドは、クエリーの抽出条件にはなりません。

b. **Query**をクリックします。

   無線リストには、一致するすべての無線が表示されます。

   Resetをクリックして無線を表示するには、Resetをクリックします。

7. OKをクリックします。

   選択した無線が表示されます。
8. MP Policy List領域で、無線にバインドするMPポリシーを選択します。
9. **Bind**をクリックします。

   操作結果ページにバインド結果が表示されます。

MPポリシーをFAT AP上の無線にバインドする:

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager>Resource Management>Fat APs**を選択します。
3. FAT APのラベルリンクをクリックすると、デバイス情報ページが表示されます。
4. ページの右下隅にあるメッシュ管理メニューで、MPポリシー管理をクリックします。

   MPポリシー管理ページが開きます。
5. Radio Information領域で、バインドする無線のModifyアイコンをクリックします。無線信号が強いほど、メッシュリンクは安定します。ベストプラクティスとして、802.11a無線を使用します。
6. 使用中のチャネルリストからチャネルを選択します。チャネル番号は無線の種類によって異なります。このオプションを自動に設定することはできません。
7. 無線にバインドするMPポリシーをMP Policyリストから選択します。FAT APに追加されたMPポリシーがリストに表示されます。
8. OKをクリックします。

MPポリシーにバインドされた無線の表示とバインディングの削除

WSMを使用すると、MPポリシーにバインドされた無線を表示して、そのバインドを削除できます。また、バインドなしでMPポリシーを変更および削除することもできます。無線からMPポリシーのバインドを解除すると、デフォルトのMPポリシーdefault_mp_plcyが無線にバインドされます。

MPポリシーにバインドされた無線を表示するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager>Resource Management>ACs**または**WLAN Manager>Resource Management>Fat APs**を選択します。
3. ACまたはFAT APのデバイスラベルをクリックして、デバイス情報ページを表示します。
4. ページの右下隅にあるメッシュ管理メニューで、MPポリシー管理をクリックします。

   MPポリシー管理ページが開きます。
5. MPポリシーの**Operation**アイコンをクリックし、ショートカットメニューから**Bound Radios**アイコンを選択します。

   Radio Listダイアログボックスが開き、MPポリシーにバインドされた無線が表示されます。次の操作を実行できます。

   - **Unbind**: MPポリシーのバインドを解除する無線を選択しバインドを解除して、バインドを削除します。
   - **Close**: Closeをクリックして、ダイアログボックスを閉じます。

メッシュインターフェースの管理

メッシュインターフェース管理では、次の操作を実行できます。

メッシュインターフェースリストの表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager>Resource Management>ACs**または**WLAN Manager>Resource Management>Fat APs**を選択します。

3. ACまたはFAT APのデバイスラベルをクリックして、デバイス情報ページを表示します。
4. ページの右下隅にあるメッシュ管理メニューで、メッシュインターフェース管理をクリックします。

   メッシュインターフェース管理ページが開きます。

   メッシュインターフェースリストの内容

   - **Description**: WLAN-MESHおよびインターフェースIDで構成されるインターフェースの説明。
   - **Mesh Profile ID**: インターフェースにバインドされているメッシュプロファイルのID。
   - **Port Security Mode**: インターフェースのポートセキュリティモード。PSKだけがサポートされます。ポートセキュリティが設定されていない場合、noRestrictionsが表示されます。このモードのメッシュインターフェースは無効です。
   - **VLAN**: インターフェースが属するVLANのID。
   - **Operation**: メッシュインターフェースの**Operation**アイコン ･･･をクリックすると、Operationメニューが表示されます。

   メッシュインターフェースの削除、ポートセキュリティの変更、VLANの変更、およびメッシュプロファイルの変更を行うことができます。これらの操作の詳細については、「メッシュインターフェースのポートセキュリティの設定」、「メッシュインターフェースが属するVLANの変更」、「メッシュインターフェースの削除」、および「メッシュプロファイルの変更」を参照してください。
5. **More**をクリックし、**MP Policy Management**または**Mesh Profile Management**を選択して設定ページに入ります。

   メッシュインターフェースリストに十分な数のエントリーがある場合は、以下のナビゲーションツールが表示されます。

   - **Next Page**アイコンをクリックして、**Mesh Interface List**内で次のページに進みます。
   - **Last Page**アイコンをクリックして、**Mesh Interface List**の最後のページに進みます。
   - **Previous Page**アイコンをクリックして、**Mesh Interface List**で前のページに戻ります。
   - **First Page**アイコンをクリックして、**Mesh Interface List**の前にページバックします。

   Mesh Interface Listの右上にある8、15、50、100、または200をクリックして、1ページに表示するアイテム数を設定します。

   注:

   メッシュインターフェースリストは、Operationフィールド以外のすべてのフィールドでソートできます。列ラベルをクリックすると、選択したフィールドでリストをソートできます。列ラベルを使用すると、各フィールドに固有の様々なソートオプションを切り替えることができます。
6. 関連操作をクリックし、ショートカットメニューからメッシュプロファイル管理またはMPポリシー管理を選択して、対応するページを表示します。

メッシュインターフェースの照会

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager>Resource Management>ACs**または**WLAN Manager>Resource Management>Fat APs**を選択します。
3. ACまたはFAT APのデバイスラベルをクリックして、デバイス情報ページを表示します。
4. ページの右下隅にあるメッシュ管理メニューで、メッシュインターフェース管理をクリックします。

   メッシュインターフェース管理ページが開きます。
5. **Query**領域に、次の問合せ基準を1つ以上入力します。

- **Description**: メッシュインターフェースの説明。WSMは、このフィールドのファジーマッチングをサポートしています。
- **Mesh Profile ID**: メッシュインターフェースにバインドされているメッシュプロファイルのID。WSMは、このフィールドのファジーマッチングをサポートします。

  空のフィールドや無制限に設定されたフィールドは、クエリーの抽出条件にはなりません。

6. **Query**アイコンをクリックします。**Mesh Interface Managemen**tページに、問合せ基準に一致するすべてのメッシュインターフェースが表示されます。
7. **Query**ィールドをクリアして**Query**アイコンをクリックすると、すべてのメッシュインターフェースが表示されます。

メッシュインターフェースの追加

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager>Resource Management>ACs**または**WLAN Manager>Resource Management>Fat APs**を選択します。
3. ACまたはFAT APのデバイスラベルをクリックして、デバイス情報ページを表示します。
4. ページの右下隅にあるメッシュ管理メニューで、メッシュインターフェース管理をクリックします。

   メッシュインターフェース管理ページが開きます。
5. Add Interfaceをクリックして、Add Interfaceページを表示します。
6. インターフェースIDを入力します。

   インターフェースIDに基づいて説明が生成されます。たとえば、インターフェースIDとして10を入力すると、インターフェースの説明はWLAN-MESH10になります。
7. **OK**をクリックします。

   操作結果が表示されます。操作が失敗した場合は、失敗の理由が表示されます。
8. **Back**をクリックして、メッシュインターフェース管理ページに戻ります。

メッシュインターフェースのポートセキュリティの設定

メッシュインターフェースを追加したら、インターフェースのポートセキュリティを設定する必要があります。インターフェースのポートセキュリティを設定しない場合は、メッシュインターフェースリストでインターフェースのポートセキュリティモードに対してnoRestrictionsが表示されます。

メッシュインターフェースのポートセキュリティを設定するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager>Resource Management>ACs**または**WLAN Manager>Resource Management>Fat APs**を選択します。
3. ACまたはFAT APのデバイスラベルをクリックして、デバイス情報ページを表示します。
4. ページの右下隅にあるメッシュ管理メニューで、メッシュインターフェース管理をクリックします。

   メッシュインターフェース管理ページが開きます。
5. 次のいずれかの方法を使用して、Modifying Port Securityページを表示します。

方法1: 1つのインターフェースのポートセキュリティを変更する:

- **a.** メッシュインターフェースの**Operation**アイコンをクリックします。
- **b.** メニューから**Modify Port Security**アイコンを選択します。

方法2: 複数のインターフェースのポートセキュリティを変更する:

- **a.** ポートセキュリティモードを変更するメッシュインターフェースを選択します。

b. Modifying Port Securityをクリックします。

6. 次のパラメーターを設定します。

- **Description**:メッシュインターフェースの説明。WLAN-MESHおよびインターフェースIDで構成されます。このフィールドは変更できません。また、複数のインターフェースのポートセキュリティモードを変更した場合は表示されません。
- **Port Security Mode**:このフィールドはPSKに設定されており、変更できません。PSKだけがサポートされています。PSKは2つのAP間のネゴシエーションキーです。ローカルAPとピアAPで同じPSKを設定する必要があります。
- **Key Type**: リストからタイプを選択します。オプションは**11Key**と空白です。
- **PSK Mode**: PSKモードを選択します。オプションは、パスフレーズ、rawキー、および空白です。
- **PSK**: PSK文字列を入力します。PSK Modeが空白のオプションに設定されている場合は、値を入力しないでください。

7. **OK**をクリックします。

操作結果が表示されます。操作が失敗した場合は、失敗の理由が表示されます。

8. **Back**をクリックして、メッシュインターフェース管理ページに戻ります。

メッシュインターフェースが属するVLANの変更

1つ以上のメッシュインターフェースが属するVLANを変更できます。インターフェースがメッシュプロファイルにバインドされている場合、インターフェースが属するVLANは変更できません。VLANを変更する前に、メッシュプロファイルからインターフェースをアンバインドします。メッシュプロファイルからインターフェースをアンバインドする方法の詳細については、「メッシュプロファイルの変更」を参照してください。

メッシュインターフェースが属するVLANを変更するには、次の手順を実行します。

1. **Service**タブをクリックします。

2. ナビゲーションツリーで、**WLAN Manager>Resource Management>ACs**または**WLAN Manager>Resource Management>Fat APs**を選択します。

3. ACまたはFAT APのデバイスラベルをクリックして、デバイス情報ページを表示します。

4. ページの右下隅にあるメッシュ管理メニューで、メッシュインターフェース管理をクリックします。

メッシュインターフェース管理ページが開きます。

5. 次のいずれかの方法を使用して、**Modify VLAN**ページを表示します。

方法1: 1つのインターフェースのVLANを変更します。

a. メッシュインターフェース**Operation**アイコン ··· をクリックします。

b. メニューから**Modify VLAN**アイコンを選択します。

方法2: 複数のインターフェースのVLANを変更します。

a. VLANを変更するメッシュインターフェースを選択します。

b. Modify VLANをクリックします。

6. VLANリストからVLAN IDを選択します。デバイス上で作成されたVLANがリストに表示されます。

7. OKをクリックします。

操作結果が表示されます。操作が失敗した場合は、失敗の理由が表示されます。

8. **Back**をクリックして、メッシュインターフェース管理ページに戻ります。

メッシュインターフェースの削除

1つ以上のメッシュインターフェースを削除できます。インターフェースがメッシュプロファイルにバインドされて

いる場合、インターフェースは削除できません。インターフェースを削除する前に、メッシュプロファイルからインターフェースをアンバインドしてください。メッシュプロファイルからインターフェースをアンバインドする方法の詳細は、「メッシュプロファイルの変更」を参照してください。

メッシュインターフェースを削除するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーで、**WLAN Manager>Resource Management>ACs**または**WLAN Manager>Resource Management>Fat APs**を選択します。
3. ACまたはFAT APのデバイスラベルをクリックして、デバイス情報ページを表示します。
4. ページの右下隅にあるメッシュ管理メニューで、メッシュインターフェース管理をクリックします。
   メッシュインターフェース管理ページが開きます。
5. 1つまたは複数のメッシュインターフェースを削除するには、次のいずれかの方法を使用します。
   方法1: 1つのメッシュインターフェースを削除する:
   a. メッシュインターフェースの**Operation**アイコン をクリックします。
   b. メニューから**Delete Interface**アイコンを選択し、操作を確認します。
   方法2: 複数のメッシュインターフェースを削除する
   a. 削除するメッシュインターフェースを選択します。
   b. メッシュインターフェースの削除をクリックして、操作を確認します。

ピアのMACアドレスの指定

APがそのピアとだけメッシュネットワークを確立できるように、APのピアのMACアドレスを指定できます。APのピアMACアドレスを指定しない場合、APはすべてのAPとメッシュネットワークを確立します。

AP間にメッシュネットワークを配置する場合は、APの無線ごとにピアMACアドレスを設定できます。

ピアのMACアドレスを指定するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Resource Management>Fat APs**を選択するか**WLAN Manager>Resource Management>Fit APs**を選択します。
3. APのデバイスラベルをクリックすると、デバイス情報ページが表示されます。
4. **Radio Information**領域(または、FIT AP情報ページのRadio Interface領域で、**Configure Mesh Peer MAC Address**アイコンをクリックします。
   Configure Mesh Peer MAC Addressページが開きます。
5. ピアのMACアドレスを追加するには、次の手順を実行します。
   a. Peer MAC AddressフィールドにMACアドレスをhh:hh:hh:hh:hh:hh:hh:hh形式で入力します。
   b. 追加をクリックします。
   ピアのMACアドレスを削除するには、次の手順を実行します。
   a. Peer MAC Address Listから削除するMACアドレスを1つ以上選択します。
   b. **Delete**をクリックします。
6. **Back**をクリックして、デバイスの詳細ページに戻ります。

注:

無線には、最大8つのピアMACアドレスを設定できます。

メッシュトポロジ

ワイヤレスデバイストポロジーを介してACメッシュトポロジを表示し、ロケーションビュートポロジーを介してFAT APメッシュトポロジを表示できます。

ACメッシュトポロジを表示する

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Wireless Topology**を選択します。

   ワイヤレストポロジウィンドウが開き、すべてのACおよびFAT APが表示されます。ACまたはAPのアイコンをクリックすると、デバイスの基本情報を表示できます。
3. ACのアイコンを右クリックして、ショートカットメニューから**Open Mesh Topology**を選択します。

   ACのメッシュトポロジが表示されます。
4. ACのアイコンをクリックすると、基本情報が表示されます。
5. ACに接続するFIT APでは、次の操作を実行できます。
   - FIT APのアイコンをクリックすると、基本情報が表示されます。

     詳細については、「ACのデバイストポロジーの表示」を参照してください。
   - FIT APのアイコンを右クリックし、ショートカットメニューから操作を選択します。

     Device Informationにはデバイスの詳細が表示され、**Display Physical Topology**にはACとFIT AP間の物理接続が表示されます。
6. ACとFIT AP間のリンク(緑色の実線)を右クリックし、ショートカットメニューから**Link Information**を選択します。実線はACとFIT AP間の物理的な接続を表します。点線はFIT AP間のワイヤレス接続を表します。

   ACとFIT AP間の物理接続のリンク情報:
   - **Control Channel Security Policy**: ACとAP間のCAPWAPチャネルで使用されるコントロールチャネルのセキュリティポリシー。
   - **Control Channel Startup Time**: ACとAP間のCAPWAPチャネルで使用されるコントロールチャネルの起動時間。
   - **Data Channel Security Policy**: ACとAP間のCAPWAPチャネルで使用されるデータチャネルのセキュリティポリシー。
   - **Data Channel Startup Time**: ACとAP間のCAPWAPチャネルで使用されるデータチャネルの起動時間。
7. FIT AP間のリンク(緑の点線)を右クリックし、ショートカットメニューから**Link Information**を選択します。

   Mesh Link Informationダイアログボックスが開きます。

   基本情報タブ
   - **Left Node**: メッシュリンクの左ノードの名前。
   - **Left Radio ID**: メッシュリンク内の左ノードの無線ID。
   - **Right Node**: メッシュリンク内の右ノードの名前。
   - **Right Radio ID**: メッシュリンク内の右ノードの無線ID。
   - **Mesh ID**: メッシュネットワークのID。
   - **Duration**: メッシュリンクのアクティブ時間。

   左ノードタブ

- **Device Label**: メッシュリンク内の左ノードデバイスのラベル。
- **BSSID**: メッシュリンク内の左ノードデバイスのMACアドレス。
- **Channel**: メッシュリンク内の左側のノードデバイスで使用されるチャネル。
- **RSSI**: メッシュリンク内の左側のノードデバイスのRSSI。
- **SNR**: メッシュリンク内の左側のノードデバイスのSNR。

右ノードタブ

- **Device Label**: メッシュリンク内の右ノードデバイスのラベル。
- **BSSID**: メッシュリンク内の右ノードデバイスのMACアドレス。
- **Channel**: メッシュリンク内の右側のノードデバイスで使用されるチャネル。
- **RSSI**: メッシュリンク内の右ノードデバイスのRSSI。
- **SNR**: メッシュリンク内の右ノードデバイスのSNR。

FAT APメッシュトポロジの表示

1. **Service**タブをクリックします。
2. 位置ビューのトポロジーを入力します。

   方法1:

   a. ナビゲーションツリーから、**WLAN Manager>Wireless Topology**を選択します。

   b. ナビゲーションツリーから、**Topology>Wireless Topology>Location View**を選択します。ロケーションビュートポロジーが表示されます。

   c. ナビゲーションツリーのロケーションビューアイコンをダブルクリックするか、トポロジー上のロケーションビューアイコンの右クリックメニューから**Open Topology**を選択します。

   トポロジマップが表示され、このレベルのロケーションビューでリダイレクトされるすべてのサブロケーションビュー、Fit AP、およびFat APが表示されます。

   方法2:

   a. ナビゲーションツリーから、**WLAN Manager>View Management>Location View**を選択します。**Location List**には、すべてのロケーションビューが表示されます。

   b. 位置ビューの**View Topology**アイコンをクリックします。

   トポロジマップが表示され、このレベルのロケーションビューでリダイレクトされるすべてのサブロケーションビュー、Fit AP、およびFat APが表示されます。
3. 空白の領域を右クリックし、ショートカットメニューから**Show Mesh Link**を選択します。

   トポロジマップには、FAT AP間のメッシュリンクが表示されます。

注:

ロケーションビューに、メッシュリンクによって相互に接続されているFit APが含まれている場合、Locationビュートポロジーには、Fit AP間のメッシュリンクが表示されます。

---

4. FAT AP間のリンク(緑の点線)を右クリックし、ショートカットメニューから**Link Information**を選択します。

   Mesh Link Informationダイアログボックスが開きます。

   基本情報タブ

   - **Left Node**: メッシュリンクの左ノードの名前。
   - **Left Radio ID**: メッシュリンク内の左ノードの無線ID。

- **Right Node**: メッシュリンク内の右ノードの名前。
- **Right Radio ID**: メッシュリンク内の右ノードの無線ID。
- **Mesh ID**: メッシュネットワークのID。
- **Duration**: メッシュリンクのアクティブ時間。

左ノードタブ

- **Device Label**:メッシュリンク内の左ノードデバイスのラベル。
- **BSSID**:メッシュリンク内の左ノードデバイスのMACアドレス。
- **Channel**:メッシュリンク内の左側のノードデバイスで使用されるチャネル。
- **RSSI**:メッシュリンク内の左側のノードデバイスのRSSI。
- **SNR**:メッシュリンク内の左側のノードデバイスのSNR。

右ノードタブ

- **Device Label**:メッシュリンク内の右ノードデバイスのラベル。
- **BSSID**:メッシュリンク内の右ノードデバイスのMACアドレス。
- **Channel**:メッシュリンク内の右側のノードデバイスで使用されるチャネル。
- **RSSI**:メッシュリンク内の右ノードデバイスのRSSI。
- **SNR**:メッシュリンク内の右側のノードデバイスのSNR。

ワイヤレスネットワーク品質の評価

ネットワーク評価モジュールは、WSM基本バージョンでは使用できず、ComwareベースのACおよびAPでのみサポートされます。

ネットワーク評価モジュールを使用すると、AC+FIT AP WLANの品質と動作ステータスを評価し、評価統計情報と結果に基づいて問題を特定できます。

ネットワーク評価には、次の部分が含まれます。

- **Evaluation task**: 最初に評価タスクを作成し、評価オブジェクト、評価日およびデータ収集時間を設定する必要があります。評価タスクを作成すると、WSMはデータ収集時間内にACから定期的にデータを収集します。
- **Evaluation report**: データ収集の完了後、WSMは収集されたデータを要約し、事前定義されたしきい値に基づいてAPとクライアントを評価し、評価レポートを生成します。

評価タスクの設定

△注意:

評価タスクを作成して実行するときに、評価タスクに関連付けられたロケーションビューを変更すると、評価データの正確性に影響し、評価タスクが失敗する可能性があります。

評価オブジェクトに基づいて、評価タスクは次のタイプに分類できます。

- **Location view-based evaluation task**: 建物の床など、エリア内のWLANを評価します。
- **AC-based evaluation task**: FIT APが同じACによって管理されているWLANを評価します。

評価タスクリストの表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Network Evaluation**を選択します。**Task List**ページには、すべての評価タスクが表示されます。

   タスクリストの内容

   - **Task Name**: 評価タスクの名前。
   - **Task Type**: 評価タスクタイプ(**Location View**または**AC**)。
   - **Task Status**: 評価タスクの状態。オプションは次のとおりです:
     - **Waiting**: タスクが作成されてから最初のデータ収集が開始される1時間前まで、評価タスクは**Waiting**状態です。
     - **Collecting**: 評価タスクは、設定されたデータ収集の開始時刻に達する1時間前から設定されたデータ収集の終了時刻に達した15分後まで、**Collecting**状態にあります。

       1時間はデータ収集の準備のために予約され、15分はデータの整合性を確保するために予約されています。
     - **Waiting for collection**: 評価タスクは、**Collecting**状態が終了してから次の収集状態が開始されるまで、**Waiting for collection**状態にあります。評価タスクの開始日と終了日が現在の日付の場合、この状態は使用できず、**Collecting**状態が終了するとすぐに評価タスクは**Evaluating**状態になります。
     - **Evaluating**: 最後のデータ収集が終了すると、評価タスクは**Evaluating**状態になります。

たとえば、評価タスクが3日間続く場合、3日目のデータ収集が終了すると、タスクはEvaluating状態になります。

- **Completed**: WSMがデータ分析を完了し、評価レポートを生成すると、評価タスクは**Completed**状態になります。
- **Suspended**: 評価タスクを手動で中断すると、評価タスクは**Suspended**状態になります。
- **Expired** :評価タスクが再開されたが、現在の時間がタスクの設定された終了時間よりも遅い場合、評価タスクはExpired状態になります。

- **Start Date**: タスクが開始される日付。
- **End Date**: タスクが完了する日付。
- **Data Collection Time Range**: 範囲データが収集される時間範囲。
- **Created by**: タスクを作成するオペレーター。
- **Created at**: タスクが作成された時刻。
- **Operation**: 評価タスクを変更するには、**Waiting**状態の評価タスクまたは**Waiting**状態から**Suspending**状態に変更している評価タスクの**Operation**アイコンをクリックします。評価レポートを表示するには、Collecting、Waiting for collection、Completed、Suspendedまたは**Expired**状態の評価タスクの**View Evaluation Report**アイコンをクリックします。
  表44に、タスクの状態と使用可能な操作を示します。

表44タスクの状態と使用可能な操作

Task state		**Modify**	**Delete**	**Suspend**	**View evaluation report**	**Set task thresholds**	**Reevaluate**
Waiting		Yes	Yes	Yes	No	Yes	no
Collecting		No	No	No	Yes	Yes	no
Waiting for collection		No	Yes	Yes	Yes	Yes	No
Evaluating		No	No	No	No	No	no
Completed		No	Yes	No	Yes	Yes	yes
suspended	From Waiting to Suspended	Yes	Yes	N/A	No	Yes	No
	From Waiting for collection to Suspended	No	Yes	N/A	Yes	Yes	no
expired		No	Yes	No	Yes	Yes	yes

- **Threshold Settings**: **Threshold Settings**アイコンをクリックして、**Evaluating**状態ではない評価タスクのしきい値を設定します。詳細は、「評価タスクのしきい値の設定」を参照してください。

Task Listに十分な数のエントリーがある場合は、次のナビゲーションツールが表示されます。

- **Next Page**アイコンをクリックして、**Task List**の次のページに進みます。
- **Last Page**アイコンをクリックして、**Task List**の最後にページを移動します。

- **Previous Page**アイコンをクリックして、**Task List**で前のページに戻ります。
- **First Page**アイコンをクリックして、**Task List**の前のページに戻ります。

Task Listの右上にある**8**、**15**、**50**、**100**、または**200**をクリックして、1ページに表示する項目数を設定します。

注:

Task Listは、**Operation**および**Threshold Settings**フィールド以外のすべてのフィールドでソートできます。列ラベルをクリックすると、選択したフィールドでリストをソートできます。列ラベルを使用すると、各フィールドに固有の様々なソートオプションを切り替えられます。

評価タスクの照会

WSMには、基本問合せと拡張問合せが用意されています。基本問合せ基準には、迅速な検索のためのキーパラメーターがいくつか含まれています。拡張問合せには、正確な照合のための様々な問合せ基準が用意されています。

評価タスクを問い合せる手順は、次のとおりです:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Network Evaluation**を選択します。**Task List**ページには、すべての評価タスクが表示されます。
3. 基本的なクエリーを実行します。
   a. タスク名を入力します。WSMは、このフィールドのファジーマッチングをサポートしています。
   b. **Query**アイコンをクリックします。**Task List**に、問合せ基準に一致するすべてのタスクが表示されます。
   c. **Query**フィールドの選択を解除し、**Query**アイコンをクリックしてすべてのタスクを表示します。
4. 高度なクエリーを実行します。
   a. **Query**フィールドの横にある**Expand**アイコンをクリックして**Query**領域を拡張します。再度クリックすると**Query**領域が非表示になります。
   b. 次の問合せ基準を1つ以上入力または選択します。
   - **Task Name**: 評価タスクの名前を入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
   - **Task Status**: 評価タスクの状態を選択します。オプションは次のとおりです。
     - **Waiting**
     - **Collecting**
     - **Waiting for collection**
     - **Evaluating**
     - **Suspended**
     - **Completed**
     - **Expired**
   - **Task type**: 評価タスクのタイプを選択します。オプションは次のとおりです:
     - **Unlimited**
     - **Location View**
     - AC

   空のフィールドや**Unlimited**に設定されたフィールドは、クエリーの抽出条件にはなりません。

c. **Query**をクリックします。**Task List**に、問合せ基準に一致するすべての評価タスクが表示されます。

d. **Reset**をクリックすると、クエリー基準が消去され、すべての評価タスクが表示されます。

評価タスクに関する詳細情報の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Network Evaluation**を選択します。**Task List**ページには、すべての評価タスクが表示されます。
3. 詳細情報を表示するには、評価タスクの名前リンクをクリックします。

   ネットワーク評価タスクの詳細

   - **Task Name**: 評価タスクの名前。
   - **Evaluation Object**: 評価するロケーションビューの名前。
   - **Task Type**: 評価タスクのタイプ。
   - **Created by**: タスクを作成するオペレーター。
   - **Created at**: タスクが作成された時刻。
   - **Start Time**: タスクが開始された時刻。
   - **End Time** : タスクが完了した時刻。
   - **Data Collection Time Range**: データが収集される時間範囲。
   - **Task Description**: 評価タスクの説明。
4. **Close**をクリックします。

評価タスクの追加

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Network Evaluation**を選択します。**Task List**ページには、すべての評価タスクが表示されます。
3. **Add**をクリックします。**Add Evaluation Task**ページが開きます。
4. 次のパラメーターを設定します。

   基本的な評価タスク情報

   - **Task Name**: 評価タスクの名前を入力します。
   - **Task Type**: 評価タスクのタイプ**Location View** または **AC**を選択します。評価タスクタイプによって、パラメーター**Evaluation Object**の設定が決まります。
   - **Evaluation Object**: タスクタイプが**Location Vi**の場合、ロケーションビュー名の最初の数文字またはスペースを入力し、表示されるリストからロケーションビューを選択します。タスクタイプがACの場合は、リストからACを選択します。
   - **Task Description**: 評価タスクの説明を入力します。
   - **Start Date**: 評価タスクの開始日をYYYY-MM-DD形式で入力するか、**Calendar**アイコンをクリックして選択します。開始日を現在の日付より前にすることはできません。
   - **End Date**: 評価タスクの終了日をYYYY-MM-DD形式で入力するか**Calendar**アイコンをクリックして選択します。終了日を開始日より前にすることはできません。

   日次データ収集の時間範囲

   評価タスクを追加または変更する場合、選択した評価オブジェクトが現在の評価オブジェクトと重複している場合は、重複するデータ収集時間範囲を設定しないでください。

   たとえば、ロケーションビューAの評価タスクがすでに存在するとします。AC Bの評価タスクを作

成し、AC Bが管理するAPがロケーションビューAに追加された場合、2つのタスクのデータ収集時間範囲は重複できません。時間範囲が重複すると、AC Bの評価タスクは作成できません。

注:

WLANの品質がワイヤレスサービスの安定性に直接影響する可能性があるため、データ収集時間はサービスが最もビジー状態になる時間に設定することをお勧めします。

データ収集時間の範囲は次のとおりです。

- **Start Time**: 毎日のデータ収集の開始時間を選択します。データ収集が今日開始される場合、開始時間は現在の時間より1時間後である必要があります。
- **End Time**: 毎日のデータ収集の終了時間を選択します。終了時間は開始時間より後である必要があります。

5. **OK**をクリックします。

評価タスクの変更

Waitingの評価タスク、または**Waiting**状態から**Suspended**状態に変化した評価タスクを変更できます。

評価タスクを変更するには、次の手順に従います。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Network Evaluation**を選択します。**Task List**ページには、すべての評価タスクが表示されます。
3. ターゲット評価タスクの**Operation**アイコンをクリックします。
4. 必要に応じて、基本情報およびデータ収集時間範囲を変更します。詳細は、「評価タスクの追加」を参照してください。

   タスク名は変更できません。
5. OKをクリックします。

評価タスクの削除

評価タスクを削除すると、そのタスクに関連するすべてのデータが削除されます。**Collecting**または**Evaluating**状態は削除できません。評価タスクを削除するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Network Evaluation**を選択します。**Task List**ページには、すべての評価タスクが表示されます。
3. ターゲット評価タスクを選択します。
4. **Delete**をクリックします。
5. 確認ダイアログボックスで、OKをクリックします。

評価タスクの中断

Waitingまたは**Waiting for collection**状態の評価タスクのみを一時停止できます。評価タスクを一時停止する手順は、次のとおりです。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Network Evaluation**を選択します。**Task List**ページには、すべての評価タスクが表示されます。

3. ターゲット評価タスクを選択します。
4. **Suspend**をクリックします。
5. 確認ダイアログボックスで、**OK**をクリックします。

評価タスクの再開

評価タスクを再開した後、現在の時刻がタスクの終了時刻より前である場合、評価タスクは続行されます。現在の時刻がタスクの終了時刻より後である場合、評価タスクは期限切れの状態になり、終了されます。

評価タスクを再開するには、次の手順に従います。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Network Evaluation**を選択します。**Task List**ページには、すべての評価タスクが表示されます。
3. ターゲット評価タスクを選択します。
4. **Resume**をクリックします。

グローバルしきい値の設定

評価索引のグローバルしきい値を設定できます。WSMは、評価索引を使用してAPおよびクライアントを評価し、全体的な評価情報の円グラフの一部を表示します。

グローバルしきい値を設定するには、次の手順を

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Network Evaluation**を選択します。**Task List**ページには、すべての評価タスクが表示されます。
3. **Set Global Threshold**をクリックします。**Global Threshold Settings**ページが開きます。
4. 高レートパケットのしきい値を設定します。設定したしきい値よりもレートが高いパケットは、高レートパケットです。WSMでは、高レートパケットの数を使用して、高レートパケット比率が計算されます。
   a. High-Rate Packet SettingsのSettingリンクをクリックします。
   b. 次の各インデックスのしきい値を選択します。
      - **802.11aパケットレート(Mbps)**
      - **802.11 anパケットレート(Mbps)**
      - **802.11bパケットレート(Mbps)**
      - **802.11gパケットレート(Mbps)**
      - **802.11gnパケットレート(Mbps)**

      対応するタイプの無線によって送信されるパケットのレートがしきい値に達すると、そのパケットは高レートパケットと見なされます。
   c. OKをクリックします。
5. AP評価索引のしきい値を設定します。WSMでは、評価タスクでAPの動作ステータスを評価するためにしきい値が使用されます。評価レポートでは、AP評価情報全体の評価結果を表示できます。
   a. AP Evaluation Index SettingsのSettingリンクをクリックします。
   b. 各インデックスのしきい値を入力します。

      WSMでは、各索引に対して次のしきい値レベルが定義されています:**Excellent、Good、Fair**および**Poor**。各レベルの必要に応じて値を入力できます(Fairレベルに達しないデータの評価結果はPoorとみなされます)。APのデータがレベルに達すると、索引の評価結果は対

応するレベルの値になります。

インデックスには次のものがあります。

- **High-Rate Outgoing Packet Ratio(%)**: APによって送信された合計パケット数に対する、APによって送信された高レートパケット数の割合。
- **High-Rate Incoming Packet Ratio(%)**: APで受信された合計パケット数に対する、APで受信された高レートパケット数の割合。
- **Average Number of Online Clients**: APのオンラインクライアントの平均数。
- **Incoming Packet Error Ratio(%):** APで受信された合計パケット数に対する、APで受信されたエラーパケット数。
- **Association Success Ratio(%)**: APで受信されたアソシエーション要求の数に対する、APで成功したアソシエーションの数。
- **Client Dropping Ratio(%)**: 正常なアソシエーションとオンラインになったクライアントの合計数に対する、APにアソシエートされているクライアントの異常なオフライン時間の数。この数を超えるとデータ収集が開始されます。
- **Weight(%)**: 1つのAPを評価する際の各索引の重みを入力します。この重みは、APの履歴評価結果(データ収集期間ごとの評価結果)の計算に使用されます。履歴計算結果に基づいて、総合評価結果が計算されます。

c. OKをクリックします。

6. クライアント評価索引のしきい値を設定します。WSMでは、しきい値を使用して、評価タスクにおけるクライアントの動作ステータスが評価されます。評価レポートでは、クライアント評価情報全体の評価結果を表示できます。

a. **Client Evaluation Index Settings**の**Setting**リンクをクリックします。

b. 次の索引に対して、**Excellent**, **Good**, **Fair**および**Weight**のしきい値を入力します。

- **RSSI**: クライアントのRSSI。
- **High**: Rate Outgoing Packet Ratio(%):クライアントが送信した合計パケット数に対する、クライアントが送信した高レートパケット数の割合。
- **High-Rate Incoming Packet Ratio(%)**: クライアントが受信した合計パケット数に対する、クライアントが受信した高レートパケット数の割合。
- **Power Save Mode Percentage**: データ収集の合計回数に対する、データ収集期間内にクライアントがパワーセーブモードを使用した回数。
- **Weight(%)**: 1つのクライアントを評価する際の各索引の重みを入力します。この重みは、クライアントの履歴評価結果(各データ収集期間の評価結果)を計算するために使用されます。全体の評価結果は、履歴計算結果に基づいて計算されます。

c. OKをクリックします。

7. 円グラフのしきい値を設定します。

a. **Pie Chart Index Settings**の**Setting**リンクをクリックします。

b. 円グラフに表示する部品の数と、次の円グラフのしきい値を設定します。

- **High-Rate Outgoing Packet Ratio Distribution**
- **High-Rate Incoming Packet Ratio Distribution**
- **User Signal Strength**

表45に示すように、円グラフのしきい値を設定します。ここでは、高速発信パケット比率分布円グラフを例として取り上げます。

c. OKをクリックします。

表45 高レート発信パケットのパラメーター比率円グラフ

項目	説明
円グラフに表示されるPart番号	円グラフに表示するパーツの数を設定します。 WSMは、事前定義された基準に一致するAPをカウントし、異なる部分のAP数の比率に基づいて円グラフを生成します。 数値を2に設定すると、円グラフにはpart 1とpart 2のみが表示されます。part 1とpart 2のしきい値がそれぞれ80%と60%であり、高速発信パケットの割合が60%を超えたAPが10台あり、高速発信パケットの割合が80%を超えたAPが6台ある場合、円グラフのpart 1は6/10、part 2は4/10になります。
Part I(%)>=	part 1のAPの高レート発信パケットの比率を0～100の範囲で設定します。 デフォルトの値は80%です。 高速発信パケットの比率がこの値を超えるAPは、part 1に属します。
Part II(%)>=	part 2のAPの高レート発信パケット比率を0～100の範囲で設定します。この値はpart 1の値よりも小さくする必要があります。 デフォルトでは、値は60%です。 高速発信パケットの比率がpart 1の値を超え、part 2の値よりも小さいAPは、part 2に属します。
PartトIII(%)>=	part 3のAPの高レート発信パケット比率を0～100の範囲で設定します。この値はpart 2の値よりも小さくする必要があります。 デフォルトの値は40%です。 高速発信パケットの比率がpart 2の値を超え、part 2の値よりも小さいAPは、part 3に属します。
Part IV(%)>=	part 4のAPの高レート発信パケット比率を0～100の範囲で設定します。この値はpart 3の値よりも小さくする必要があります。 デフォルトの値は20%です。 高速発信パケットの比率がpart 3の値を超え、part 3の値よりも小さいAPは、part 4に属します。
Part V(%)>=	前の4つの部分に属さないAPは、部分5に属します。

8. **Restore the Defaults**をクリックして、グローバルしきい値をデフォルトしきい値に戻します。
9. **Back**をクリックして、**Task List**ページに戻ります。

評価タスクのしきい値の設定

デフォルトでは、評価タスクにしきい値を設定するまで、評価タスクはグローバルなしきい値を使用します。

この関数は、現在の評価タスクに対してのみ有効であり、評価中状態の評価タスクには有効ではありません。

評価タスクのしきい値を設定するには、次の手順を実行します:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Network Evaluation**を選択します。**Task List**ページには、すべての評価タスクが表示されます。
3. ターゲット評価タスクの**Threshold Settings**アイコン  をクリックします。
4. 索引タイプの**Setting**リンクをクリックし、表示されたウィンドウで索引のしきい値を設定します。詳細は、「グローバルしきい値の設定」を参照してください。
5. **Save As Global Threshold**をクリックするか、現在の評価タスクのしきい値をグローバルし

きい値として保存します。

または、**Restore Global Threshold**をクリックして、現在の評価タスクにグローバルしきい値を使用します。

または、**Re-Evaluate**をクリックして、現在のしきい値に従って、完了または期限切れの評価タスクを再評価します。

6. **Back**をクリックして、**Task List**ページに戻ります。

評価結果の計算

最後のデータ収集が終了すると、評価タスクは**Evaluating**状態になります。評価状態では、WSMは収集されたデータを分析し、しきい値を使用してWLANの品質を評価し、APおよびクライアントの評価結果を生成します。

WSMは15分ごとにデータを収集します。WSMは、次の手順に従ってAPおよびクライアントを評価します(例として、APベースの評価タスクがあります)。

1. 収集されたデータを評価します。
   a. 高速パケットの比率を計算します。

      WSMは、事前定義されたしきい値に従って、高レートの発信パケットと着信パケットの比率を計算します。

      802.11bパケット比率しきい値が5.5 Mbpsで、APが1000個の802.11bパケットを送信し、800パケットの送信レートが5.5 Mbpsを超えた場合、高速パケット比率は80%になります。

   b. 各インデックスのスコアを計算します。

      WSMでは、各AP指数の評価結果が計算されます。この評価結果には、excellent, good, fairおよび不可の4つのクラスが含まれています。各クラスのスコアは次のとおりです。

      - **Excellent** -100
      - **Good** -80
      - **Fair** -60
      - **Bad** -40

      高レート発信パケットの比率が95%で、**Excellent**のしきい値が90%の場合、評価結果は**Excellent**となり、高レート発信パケットのスコアは100になります。

   c. レコードの評価結果を計算します。

      各インデックスのスコアに基づいて、WSMは次の式を使用してレコードのスコアを計算します。

      Weight 1 × **Index 1's score** + **Weight 2** × **Index 2's score** +……

      WSMでは、最終スコアがシステム定義の標準と比較されます。標準は次のとおりです。

      - **Excellent >=85.00**
      - **Good >=70.00**
      - **Fair >=55.00**
      - **Poor <55.00**

      次に、各レコードの評価プロセスを示す簡単な例を示します。AP評価インデックスのしきい値が次のように設定されているとします。

      - **High-Rate Outgoing Packet Ratio(%)**: Excellent>=90.00、Good>=80.00、Fair>=60.00、およびWeight(%)10.00。
      - **High-Rate Incoming Packet Ratio(%)**: Excellent>=65.00、Good>=50.00、Fair>=30.00、およびWeight(%)10.00。
      - **Average Number of Online Clients**: Excellent<=15.00、Good<=20.00、Fair<=25.00、およびWeight(%)20.00。

- **Incoming Packet Error Ratio(%)**: Excellent<=5.00、Good<=9.00、Fair<=15.00、およびWeight(%)20.00。
- 関**Association Success Ratio (%**): Excellent>=90.00、Good>=75.00、Fair>=60.00、およびWeight(%)20.00。
- **Client Dropping Ratio(%)**: Excellent<=10.00、Good<=20.00、Fair<=30.00、およびWeight(%)20.00。

WSMは、次の手順に従って各レコードを評価します。

d. 各索引のスコアを計算します。

索引の評価結果は次のとおりです:

- **High-Rate Outgoing Packet Ratio**—Good (85%)
- **High-Rate Incoming Packet Ratio**—Excellent (70%)
- **Average Number of Online Clients**—Excellent (1
- **Incoming Packet Error Ratio**—Excellent (3%)
- **Association Success Ratio**—Fair (70%)
- **Client Dropping Ratio**—Good (15

評価結果によれば、各指標の得点は、**80、100、100、100、60、80**です

e. レコードのスコアを計算します。

80×10%+100×10%+100×20%+100×20%+60×20%+80×20%=86

システムで定義された基準に従って、このレコードの評価結果は**Excellent**です。

2. 全体的な評価結果を計算します。

WSMでは、APおよびクライアントの履歴評価結果の**excellent, good, fair、poor**の割合に従って、全体的な評価結果が計算されます。

- **Excellent**: 履歴評価結果のExcellentとGoodの割合は55%を超え、履歴評価結果のExcellentの割合は40%を超えている必要があります。
- **Good**: ExcellentおよびGoodの履歴評価結果の割合は55%を超えている必要があります。
- **Fair**: Excellent、GoodおよびFairの履歴評価結果の割合は、70%を超えている必要があります。
- **Poor**: 前の条件のいずれにも一致しない履歴評価結果。

評価レポートの管理

WSM評価レポートには、次の部分が含まれます。

- 総合評価情報
- トポロジー情報
- AP情報
- クライアント情報
- ラジオ情報
- チャネル情報

ロケーションビューベースのタスクの評価レポートには、6つの部分がすべて含まれています。ACベースのタスクの評価レポートには、トポロジー情報はありません。

評価レポートの最初のページを表示する

待機中または評価中の状態の評価タスクの評価レポートは表示できません。評価レポートの最初のページ

を表示するには、次の手順を実行します:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Network Evaluation**を選択します。**Task List**ページには、すべての評価タスクが表示されます。
3. **View Evaluation Report**アイコン  をクリックします。評価レポートの最初のページが表示され、次の情報が示されます。
   - **Report Name**: 評価レポートの名前。デフォルトの名前は**Network Evaluation**です。レポート名の変更の詳細は、「評価オブジェクトの選択」を参照してください。
   - **Cover Picture**: 評価レポートの表紙。表紙ピクチャの変更の詳細は、「評価オブジェクトの選択」を参照してください。
   - **Evaluation Object**: 評価するロケーションビューまたはACの名前。名前のリンクをクリックすると、全体的な評価情報が表示されます。詳細は、「全体的な評価情報の表示」を参照してください。
   - **Total Number of APs**: サブロケーションビュー内のAPを含む、評価されたAPの合計。評価タスクが作成されると、WSMは事前定義済の評価オブジェクトに基づいてAPの合計数を計算します。WSMは、評価中にオンラインになったAPを評価しません。評価中にAPがオフラインになった場合でも、APは評価されます。
   - **Evaluation Date**: 評価タスクの開始日と終了日。
   - **Current Status**: 評価タスクの現在の状態。

   完了または期限切れの評価タスクについては、評価レポートの最初のページで次の操作を実行できます。
   - **Select Evaluation Object**: 評価オブジェクトがロケーションビューの場合オブジェクトがロケーションビューの場合、そのサブロケーションビューの1つをオブジェクトとして選択して、サブロケーションビューの評価レポートを表示できます。詳細は、「評価オブジェクトの選択」を参照してください。
   - **Parameter Settings**: **Parameter Settings**リンクをクリックして、評価レポートの名前、表紙ピクチャ、評価日および説明を設定します。詳細は、「評価オブジェクトの選択」を参照してください。
   - **Export Report**: 現行の評価レポートをPDF形式でエクスポートするには、**Export Report**リンクをクリックします。詳細は、「評価レポートのエクスポート」を参照してください。

評価オブジェクトの選択

評価オブジェクトがロケーションビューの場合は、そのサブロケーションビューの1つをオブジェクトとして選択して、サブロケーションビューの評価レポートを表示できます。たとえば、評価オブジェクトが建物の場合は、1つのフロアをオブジェクトとして選択できます。

評価オブジェクトを設定するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Network Evaluation**を選択します。**Task List**ページには、すべての評価タスクが表示されます。
3. ターゲット評価タスクの**View Evaluation Report**アイコンをクリックします。評価レポートの最初のページが表示されます。
4. **Select Evaluation Object**をクリックします。
5. 表示されたダイアログボックスで、サブロケーションビューを選択します。
6. **OK**をクリックします。

評価レポートパラメーターの設定

レポートパラメーターは、完了済または期限切れの評価タスクに対してのみ設定できます。評価レポートパラメーターを設定する手順は、次のとおりです。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Network Evaluation**を選択します。**Task List**ページには、すべての評価タスクが表示されます。
3. ターゲット評価タスクの**View Evaluation Report**アイコンをクリックします。評価レポートの最初のページが表示されます。
4. **Parameter Settings**リンクをクリックします。
5. 必要に応じて次のパラメーターを設定します。
   - パラメーター設定
     - **Report Name**: 評価レポートの名前を入力します。評価レポートの最初のページに表示されます。デフォルトでは、名前は**Network Evaluation**です。
     - **Cover Picture**: **Browse**をクリックし、ダイアログボックスで画像を選択します。画像は、**.jpg**、**.bmp**、または**.gif**形式で、サイズは2 M以下です。画像は、評価レポートの最初のページに表示されます。
   - **Evaluation Time**: 評価日を選択して**OK**をクリックします。WSMは、選択した時間範囲でネットワーク品質を再評価し、元の評価レポートを置き換える新しい評価レポートを生成します。
   - **Report Template Description**: エクスポートされた評価レポートに表示される次の評価項目の説明を入力します。
     - **Overview**
     - **Overall Evaluation for the Hotspots**
     - **Overall AP and Client Evaluation**
     - **History AP and Client Information**
     - **Summary**
6. OKをクリックします。

評価レポートのエクスポート

評価レポートは、完了した評価タスクまたは期限切れの評価タスクについてのみエクスポートできます。

評価レポートは、Excel、PDFまたはWordフォーマットでエクスポートできます。Excelフォーマットの評価レポートは、PDFおよびWordフォーマットのレポートとは異なります。ロケーションビューベースの評価レポートは、ACベースの評価レポートとは異なります。詳細は、表46を参照してください。

表46評価報告書の内容

タスクの種類	レポートの形式	レポートの内容
Location view	Excel	• 履歴AC情報 • クライアント情報の履歴 • 総合チャネル評価記録 • 無線評価履歴記録無線
	PDFおよびMS Word	• 全体的なホットスポット評価 • AP、クライアント、無線、およびチャネル全体の評価 • AP、クライアント、無線、およびチャネルの履歴情報

タスクの種類	*レポートの形式*	*レポートの内容*
AC	Excel	• AP詳細 • RRMチャネル • RRM AP関係 • クライアント情報 • Ping詳細 • ping統計情報 • AP ChannelBusy詳細 • AP ChannelBusy統計
	PDFおよびMS Word	• AC統計情報 • 無線ベースの統計情報 • クライアントベースの統計情報 • AC-APリンクステータスの分析 • AP動作チャネル統計情報

評価レポートをエクスポートする手順は、次のとおりです。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Network Evaluation**を選択します。**Evaluation Task List**ページに、すべての評価タスクが表示されます。
3. **View Evaluation Report**アイコンをクリックします。評価レポートの最初のページが表示されます。
4. **Export Report**リンクをクリックします。確認ダイアログボックスが表示されます。
5. APおよびクライアントの履歴情報を含む評価レポートを生成するかどうかを確認します。オプションは**Yes**および**No**です。

   ロケーションビューまたはAPの数が多い場合、APおよびクライアントの履歴情報を含む評価レポートの生成には時間がかかり、システムリソースを占有します。ベストプラクティスとして、ロケーションビューまたはAPの数が比較的少ない場合は**Yes**を選択し、数が多い場合は**No**を選択します。
6. **OK**をクリックします。
7. **Export Report**をクリックします。ダイアログボックスが開きます。
8. **Save**をクリックします。レポートを保存するディレクトリを選択し、ダイアログボックスで**OK**をクリックします。

評価レポートの表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Network Evaluation**を選択します。E**valuation Task List**ページに、すべての評価タスクが表示されます。
3. ターゲット評価タスクの**View Evaluation Report**アイコンをクリックします。評価レポートの最初のページが表示されます。
4. 評価オブジェクトの名前をクリックします。
5. **Overall Evaluation**、**Topology**、**AP**、または**Client**タブをクリックして、全体、トポロジー、AP、またはクライアントの評価情報を表示します。

総合評価情報の表示

完了したタスクの全体的な評価情報のみを表示できます。

データは、構成されたしきい値に従って異なる色で表示されます。緑は良好、赤は不良、黒はその他のレベルを表します。しきい値を設定するには、「グローバルしきい値の設定」または「評価タスクのしきい値の設定」を参照してください。

基本的な情報

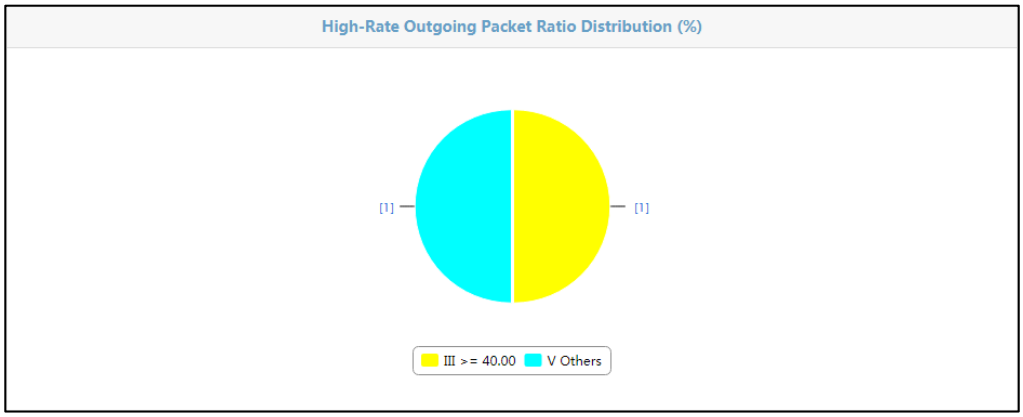
- **Number of APs**: 評価オブジェクト内のAPの数(オブジェクトのサブロケーション内のAPを含む)。
- **Number of APs Not Evaluated**: 評価タスクの完了後にデータが取得されなかったAPとロケーションから削除されたAPの合計。
- **Evaluation Duration (Hour)**: 評価タスクでデータを収集するために必要な合計時間。
- **Total AP Traffic(MB)**: 評価オブジェクト内のすべてのAPのトラフィックの合計。
- **Average Traffic Per AP(MB)**: 評価オブジェクトの各APの平均トラフィック。
- **Average Number of Online Clients**: 評価オブジェクト内の各APの平均オンラインクライアント数。
- **Average Traffic Per Client(MB)**: ロケーション内のAPに関連付けられた各クライアントの平均トラフィック。
- **Association Success Ratio(%)**: アソシエーションの総数に対する、ロケーション内で成功したクライアントのアソシエーションの数(パーセンテージ)。
- **High-Rate Outgoing Packet Ratio(%)**: ロケーション内の各APの送信パケットの平均高レートパケット比率。
- **High-Rate Incoming Packet Ratio(%)**: ロケーション内の各APの受信パケットの平均高レートパケット比率。
- **Packet Retransmission Ratio(%)**: ロケーション内の各APの平均再送信レート。
- **Incoming Packet Error Ratio(%)**: ロケーション内の各APで受信したパケットの平均エラーパケット率。
- **Outgoing Packet Loss Ratio(%)**: ロケーション内の各APの送信パケットの平均パケット損失率。
- **Client Dropping Ratio(%)**: ロケーション内のAP上の各端末の平均ドロップ率。
- **Radio Count**: 評価された無線の合計。
- **Run Client Count**: 評価されたクライアントの合計。

円グラフ

各索引の円グラフは、索引設定に従って表示されます。円グラフの索引を設定するには、「グローバルしきい値の設定」および「評価タスクのしきい値の設定」を参照してください。

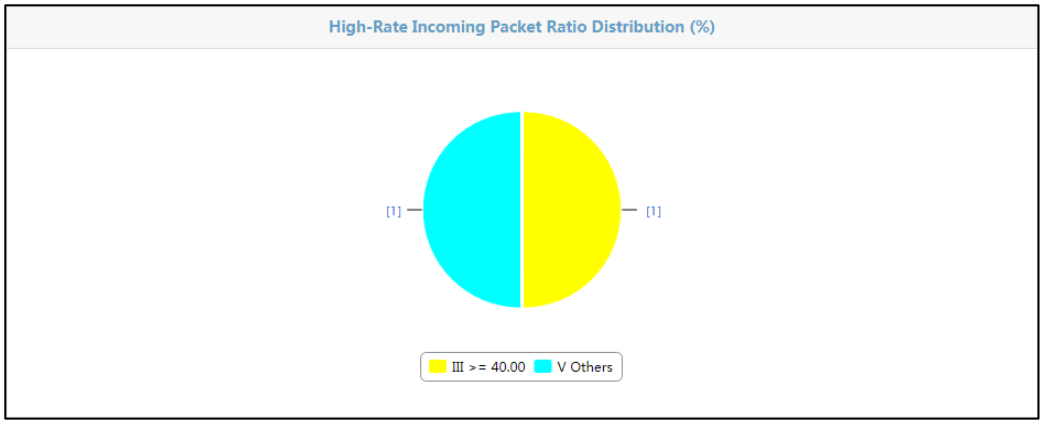
- **High-Rate Outgoing Packet Ratio Distribution**: 図92に示すように、評価対象APの**High-Rate Outgoing Packet Ratio Distribution**を表示します。

  図92:高レート発信パケット比率の分布



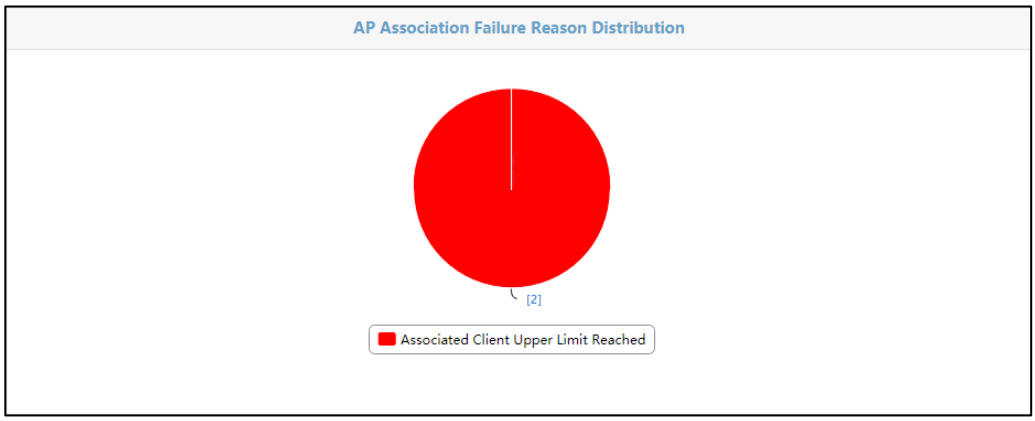
- **High-Rate Outgoing Packet Ratio Distribution**: 図93に示すように、評価対象APの高レート着信パケットの比率分布を表示します。

図93 高レート着信パケット比率の分布



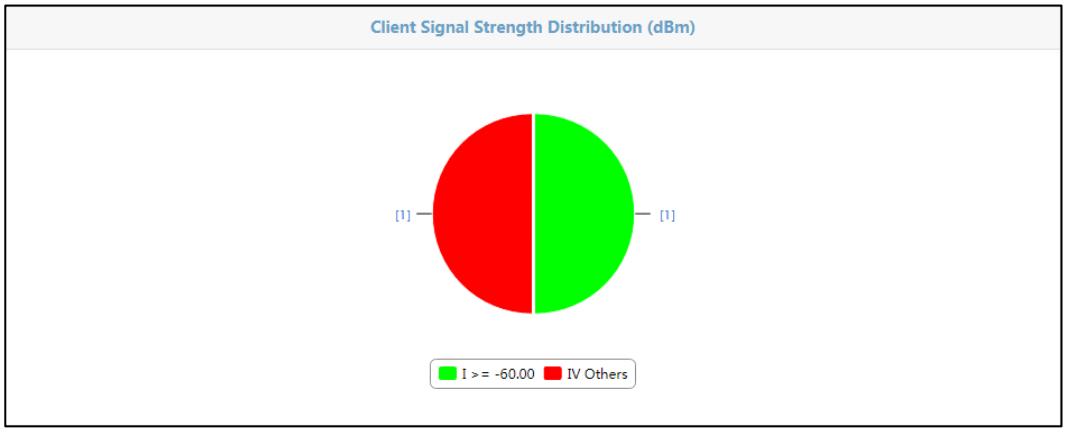
- **AP Association Failure Reason Distribution**:すべてのAPのアソシエーション障害の理由を表示します。これには、アソシエートされているクライアントの上限に達したこと、サポートされていない必須レート、associationの障害、その他(弱い信号強度やブラックリストなど)、および不明な理由が含まれます(図94を参照)。

図94 APアソシエーションの失敗理由の分布



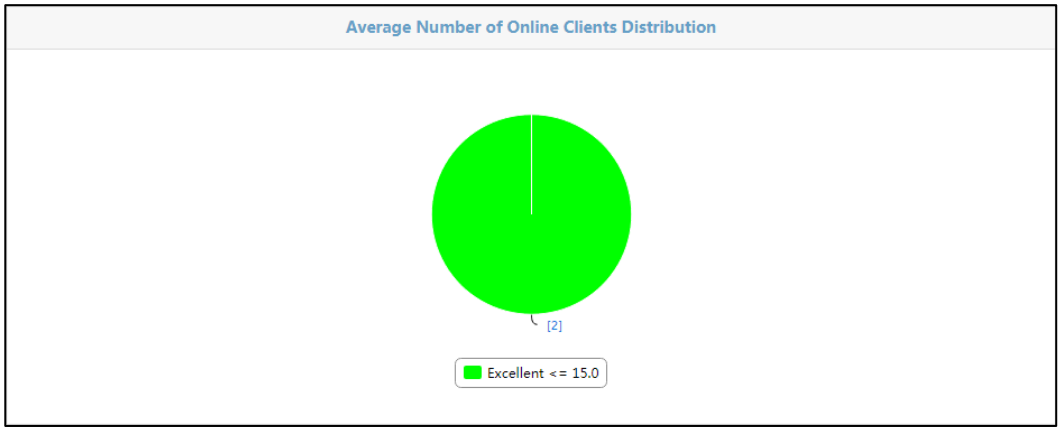
- **Client Signal Strength Distribution**: 図95に示すように、ロケーション内のAPに関連付けられたすべてのクライアントの信号強度分布を表示します。

図95 クライアント信号強度分布



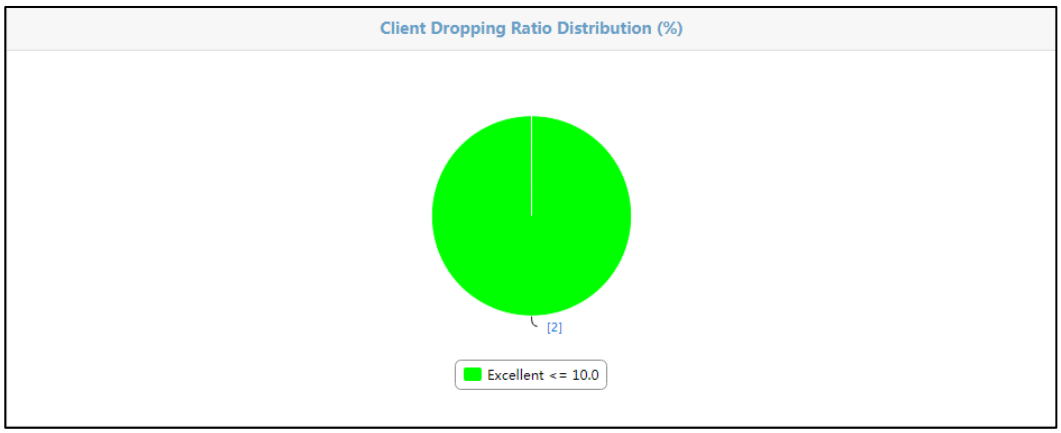
- **Average Number of Online Clients Distribution**: 図96に示すように、ロケーション内のAPに関連付けられたすべてのクライアントの信号強度分布を表示します。

図96 平均オンラインクライアント数の分布



- **Client Dropping Ratio Distribution**: 図97に示すように、ロケーション内のAPに関連付けられているクライアントのドロップ率を表示します。

図97 クライアントのドロップ率分布



AP評価情報の表示

完了または期限切れの評価タスクについてのみ、履歴と全体的な評価情報の両方を表示できます。また、他の状態の評価タスクについては、AP履歴の評価情報だけを表示できます。

総合的なAP評価情報

デバイスリストのデータは、構成されたしきい値に従って異なる色で表示されます。緑は良好、赤は不良、黒はその他のレベルを表します。しきい値を設定するには、「グローバルしきい値の設定」または「評価タスクのしきい値の設定」を参照してください。

デバイスリストの内容

- **AP Label**: APのラベル。ラベルのリンクをクリックすると、その詳細が表示されます。
- **Average Number of Online Clients**: APの平均オンラインクライアント数。
- **Average Transmission Rate(Mbps)**: APの平均伝送レート。
- **Average Receive Rate(Mbps)**: APの平均受信レート。
- **High-Rate Outgoing Packet Ratio(%)**: ロケーション内の各APの送信パケットの平均高レートパケット比率。
- **High-Rate Incoming Packet Ratio(%)**: ロケーション内の各APの受信パケットの平均高レートパケット比率。
- **Association Success Ratio**: アソシエーションの総数に対する、ロケーション内で成功したクライアントのアソシエーションの数(パーセント)。
- **Incoming Packet Error Ratio(%)** :ロケーション内の各APで受信したパケットの平均エラーパケット率。
- **Client Dropping Ratio(%)**: ロケーション内のAP上の各端末の平均ドロップ率。
- **Evaluation Result**: APの評価結果。

デバイスリストに十分なエントリーが含まれている場合は、次のナビゲーションツールが表示されます。

- **Next Page**アイコンをクリックして、**Device List**で次のページに進みます。
- **Last Page**アイコンをクリックして、**Device List**の最後のページに進みます。
- **Previous Page**アイコンをクリックして、**Device List**で前のページに戻ります。
- **First Page**アイコンをクリックすると、**Device List**の先頭にページバックします。

デバイスリストの右上にある**8**、**15**、**50**、**100**、または**200**をクリックして、各ページに表示する項目数を指定します。

注:

Device Listは、**Operation**フィールド以外のすべてのフィールドでソートできます。選択したフィールドでリストをソートするには、列ラベルをクリックします。列ラベルを使用すると、各フィールドに固有のソートオプションを切り替えることができます。

評価対象APのクエリー

1. **Query Criteria**領域に、次の**Query Criteria**を1つ以上入力します。
   - **AP Label**: APのラベルを入力します。WSMは、このフィールドのファジーマッチングをサポートします。
   - **Evaluation Result**: APをフィルタリングするには、**Excellent**、**Good**、**Fair**、または**Poor**を選択します。
   - **View History Records**: このオプションを選択すると、APの履歴評価情報が表示されます。**Evaluation Date**: 評価履歴レコードの日付を選択します。このオプションは、**View History Records**を選択した場合にのみ使用できます。
   - **Evaluation Indexes**: 評価索引を選択し、一致基準を選択して、基準の値を入力します。オプションの索引は次のとおりです。
     - **Average Number of Online Clients**

- **Average Transmission Rate (Mbps)**
- **Average Reception Rate (Mbps)**
- **High-Rate Outgoing Packet Ratio (%)**
- **High-Rate Incoming Packet Ratio (%)**
- **Association Success Ratio (%)**
- **Incoming Packet Error Ratio (%)**
- **Client Offline Ratio (%)**

オプションの一致基準は、**=**、**>=**、**>**、**<=**、および<です。

空のフィールドや**Unlimited**に設定されたフィールドは、クエリーの抽出条件にはなりません。

2. **Query**をクリックします。**Device List**に、クエリー基準に一致するすべてのAPが表示されます。
3. クエリー基準をクリアしてすべてのAPを表示するには、**Reset**をクリックします。

APの履歴評価情報のクエリー

1. **Query Criteria**領域で**View History Records**を選択し、評価日を選択して、必要に応じて他の問合せ基準を設定します。詳細は、「AP評価情報の表示」を参照してください。
2. **Query**をクリックします。**Device List**に、クエリー基準に一致するすべてのAPが表示されます。

   デバイスリストの内容

   - **AP Label**: APのラベルを入力します。WSMは、このフィールドのファジーマッチングをサポートします。
   - **Average Number of Online Clients**: APの平均オンラインクライアント数。
   - **Average Transmission Rate(Mbps)**: APの平均伝送レート。
   - **Average Reception Rate(Mbps)**: APの平均受信レート。
   - **High-Rate Outgoing Packet Ratio(%)**: ロケーション内の各APの送信パケットの平均高レートパケット比率。
   - **High-Rate Incoming Packet Ratio(%)**: ロケーション内の各APの受信パケットの平均高レートパケット比率。
   - **Association Success Ratio**: アソシエーションの総数に対する、ロケーション内で成功したクライアントのアソシエーションの数(パーセント)。
   - **Incoming Packet Error Ratio(%)**: ロケーション内の各APで受信したパケットの平均エラーパケット率。
   - **Client Offline Ratio(%)**: ロケーション内のAPの各端末の平均オフライン率。
   - **Evaluation Date**: APの評価日。
   - **Evaluation Result**: APの評価結果。

デバイスリストに十分なエントリーが含まれている場合は、次のナビゲーションツールが表示されます。

- **Next Page**アイコンをクリックして、**Device List**で次のページに進みます。
- **Last Page**アイコンをクリックして、**Device List**の最後のページに進みます。
- **Previous Page**アイコンをクリックして、**Device List**で前のページに戻ります。
- **First Page**アイコンをクリックすると、**Device List**の先頭にページバックします。

デバイスリストの右上にある**8**、**15**、**50**、**100**、または**200**をクリックして、各ページに表示する項目数を指定します。

注:

Device Listは、**Operation**フィールド以外のすべてのフィールドでソートできます。選択したフィール

ドでリストをソートするには、列ラベルをクリックします。列ラベルを使用すると、各フィールドに固有の様々なソートオプションを切り替えることができます。

APの詳細な評価情報の表示

APの詳細な評価情報を表示するには、のターゲットAPのラベルリンクをクリックします。

基本情報

- **AP Label**: APのラベル。
- **Evaluation Result**: APの評価結果。
- **IP Address**: APの管理IPアドレス。
- **AP Model**: APのモデル。
- **Mask**: APのマスク。
- **Location**: APが属するロケーションビュー。ロケーションの名前リンクをクリックして、ロケーションの総合評価ページに入ります。総合評価の詳細は、「総合評価情報の表示」を参照してください。

パケット統計情報

- **Average Transmission Rate(Mb/s)**: APの平均伝送レート。
- **Average Reception Rate(Mb/s)**: APの平均受信レート。
- **High-Rate Outgoing Packet Ratio(%)**: ロケーション内の各APの送信パケットの平均高レートパケット比率。
- **High-Rate Incoming Packet Ratio(%)**: ロケーション内の各APの受信パケットの平均高レートパケット比率。
- **Association Success Ratio**: アソシエーションの総数に対する、ロケーション内で成功したクライアントのアソシエーションの数(パーセント)。
- **Incoming Packet Error Ratio(%)**: ロケーション内の各APで受信したパケットの平均エラーパケット率。
- **Client Dropping Ratio(%)**: ロケーション内のAP上の各クライアントの平均ドロップ率。

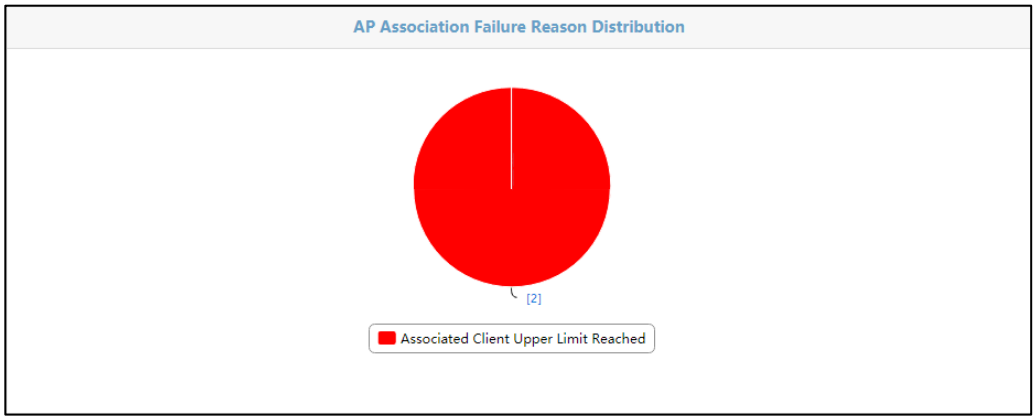
クライアント情報

- **Average Number of Online Clients**: APの平均オンラインクライアント数。
- **Total Number of Associations**: APに正常にアソシエートされたクライアントの合計数。
- **Total Number of Failed Associations**: APとのアソシエーションに失敗したクライアントの合計数。
- **Total Number of Rejected Associations**: APの拒否されたクライアントの合計数。
- **Total Number of Re-Associated**: APに再アソシエートされたクライアントの合計数。
- **Total Number of Abnormal Logouts**: APの例外的にアソシエート解除されたクライアントの合計数。
- **Association Success Ratio(%)**: アソシエーション要求の総数に対する成功したアソシエーションの数。
- **Relevant Blocking Rate(%)**: アソシエーション要求の総数に対するリソース不足が原因で失敗したアソシエーションの数。

円グラフ

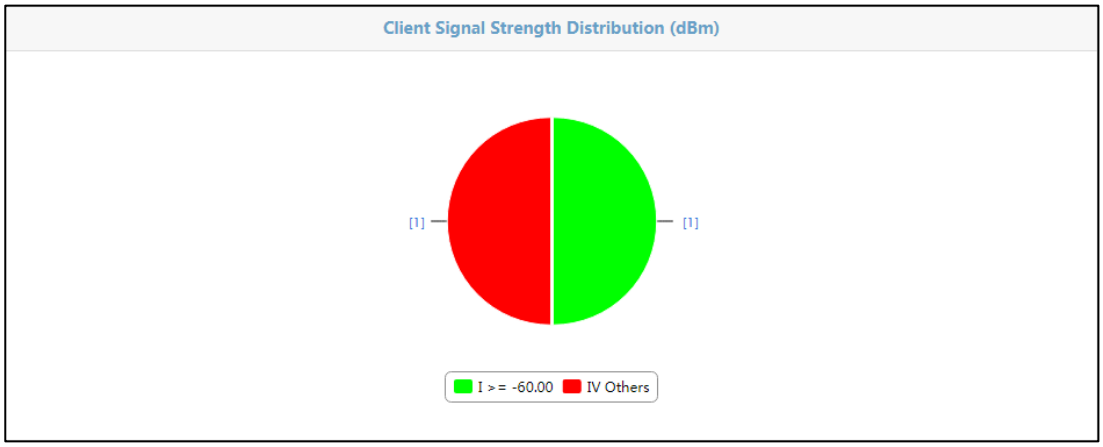
- **AP Association Failure Reason Distribution**: 図98に示すように、すべてのAPのアソシエーション障害理由を表示します。これには、アソシエートされているクライアントの上限に達したこと、サポートされていない必須レート、associationの障害、その他(弱い信号強度やブラックリストなど)、および不明な理由が含まれます。

図98 APアソシエーションの失敗理由の分布



- **Client Signal Strength Distribution**: 図99に示すように、ロケーション内のAPに関連付けられたすべてのクライアントの信号強度分布を表示します。

  図99 クライアント信号強度分布



デバイスリスト

APの履歴評価情報を表示します。

クライアント評価情報の表示

完了または期限切れの評価タスクについてのみ、履歴と全体的な評価情報の両方を表示できます。また、他の状態の評価タスクについては、クライアント履歴の評価情報のみを表示できます。

クライアントリストのデータは、構成されたしきい値に従って異なる色で表示されます。緑は良好、赤は不良、黒はその他のレベルを表します。しきい値を設定するには、「グローバルしきい値の設定」または「評価タスクのしきい値の設定」を参照してください。

クライアントリストの内容

- **MAC Address**: クライアントのMACアドレス。アドレスリンクをクリックすると、クライアントに関する詳細な評価情報が表示されます。
- **Username**: クライアントの名前。
- **Total Traffic(MB)**: クライアントが送受信したトラフィックの合計。
- **Average Transmission Rate(Mb/s)**: クライアントの平均伝送レート。
- **Average Reception Rate(Mb/s)**: クライアントの平均受信レート。

- **Power Save Mode Percentage**: データ収集回数の合計に対する、クライアントが省電力モードで動作する回数。
- **Average RSSI**: クライアントの平均RSSI。
- **High-Rate Outgoing Packet Ratio(%)**: クライアントの送信パケットの平均高レートパケット比率。
- **High-Rate Incoming Packet Ratio(%)**: クライアントの受信パケットの平均高レートパケット比率。
- **Evaluation Result**: APの評価結果。

クライアントリストに十分な数のエントリーがある場合は、次のナビゲーションツールが表示されます。

- **Next Page**アイコンをクリックして、**Client List**でページを進めます。
- **Last Page**アイコンをクリックして、**Client List**の最後にページを移動します。
- **Previous Page**アイコンをクリックして、**Client List**で前のページに戻ります。
- **First Page**アイコンをクリックして、**Client List**の前にページを戻します。

クライアントリストの右上にある8、15、50、100、または200をクリックして、各ページに表示する項目数を指定します。

注:

Client Listは、**Operation**フィールド以外のすべてのフィールドでソートできます。列ラベルをクリックすると、選択したフィールドでリストをソートできます。列ラベルを使用すると、各フィールドに固有の様々なソートオプションを切り替えることができます。

評価されたクライアントの照会

1. **Query Criteria**」領域に、次の問合せ基準を1つ以上入力します。
   - **Username**: クライアントの名前を入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
   - **MAC Address**: クライアントのMACアドレスを入力します。WSMは、このフィールドのファジーマッチングをサポートします。
   - **Evaluation Result**: クライアントをフィルタするには、**Excellent**、**Good**、**Fair**、または**Poor**を選択します。
   - **View History Records**: APの履歴評価情報を表示するには、このオプションを選択します。**Evaluation Date**:評価履歴レコードの日付を選択します。このオプションは、**View History Records**を選択した場合にのみ使用できます。
   - **Evaluation Indexes**: 評価索引を選択し、一致基準を選択して、基準の値を入力します。オプションの索引は次のとおりです。
     - **Total Traffic (MB)**
     - **Average Transmission Rate (Mb/s)**
     - **Average Reception Rate (Mb/s)**
     - **Power Save Mode Percentage (%)**
     - **Average RSSI**
     - **High-Rate Outgoing Packet Ratio (%)**
     - **High-Rate Incoming Packet Ratio(%)**

     オプションの一致基準は、**=**、**>=**、**>**、**<=**、および**<**です。

     空のフィールドや無制限に設定されたフィールドは、クエリーの抽出条件にはなりません。
2. **Query**をクリックします。**Client List**に、問合せ基準に一致するすべてのクライアントが表示されま

す。

3. **Reset**をクリックして、クエリー基準をクリアし、すべてのクライアントを表示します。

クライアントの履歴評価情報の表示

1. **Query Cri**領域で**View History Records**を選択し、評価日を選択して、必要に応じて他の問合せ基準を設定します。
2. **Query**をクリックします。**Client List**に、問合せ基準に一致するすべてのクライアントが表示されます。

   クライアントリストのデータは、構成されたしきい値に従って異なる色で表示されます。緑は良好、赤は不良、黒はその他のレベルを表します。しきい値を設定するには、「グローバルしきい値の設定」または「評価タスクのしきい値の設定」を参照してください。

   クライアントリストの内容

   - **MAC Address**: クライアントのMACアドレス。アドレスリンクをクリックすると、クライアントの詳細な評価情報が表示されます。
   - **Username**: クライアントの名前。
   - **Total Traffic(MB)**: クライアントが送受信したトラフィックの合計。
   - **Average Transmission Rate(Mb/s)**: クライアントの平均伝送レート。
   - **Average Reception Rate(Mb/s)**: クライアントの平均受信レート。
   - **Power Save Mode Percentage(%)**: データ収集回数の合計に対する、クライアントが省電力モードで動作する回数。
   - **Average RSSI**: クライアントの平均RSSI。
   - **High-Rate Outgoing Packet Ratio(%)**: クライアントの送信パケットの平均高レートパケット比率。
   - **High-Rate Incoming Packet Ratio(%)**: クライアントの受信パケットの平均高レートパケット比率。
   - **Evaluation Date**: クライアントの評価日。
   - **Evaluation Result**: クライアントの評価結果。

クライアントリストに十分な数のエントリーがある場合は、次のナビゲーションツールが表示されます。

- **Next Page**アイコンをクリックして、**Client List**でページを進めます。
- **Last Page**アイコンをクリックして、**Client List**の最後にページを移動します。
- **Previous Page**アイコンをクリックして、**Client List**で前のページに戻ります。
- **First Page**アイコンをクリックして、**Client List**の前にページを戻します。

クライアントリストの右上にある8、15、50、100、または200をクリックして、各ページに表示する項目数を指定します。

注:

Client Listは、**Operation**フィールド以外のすべてのフィールドでソートできます。列ラベルをクリックすると、選択したフィールドでリストをソートできます。列ラベルを使用すると、各フィールドに固有の様々なソートオプションを切り替えることができます。

クライアントの詳細な評価情報の表示

クライアントの詳細な評価を照会するには、でターゲットクライアントのMACアドレスリンクをクリックします。
クライアントリスト。

データは、構成されたしきい値に従って異なる色で表示されます。緑は良好、赤は不良、黒はその他のレベルを表します。しきい値を設定するには、「グローバルしきい値の設定」または「評価タスクのしきい値の設定」を参照してください。

詳細

クライアントの基本情報と評価情報を表示します。

- **Signal Noise Ratio**: クライアントの信号対ノイズ比。
- **Average Signal Strength(dBm)**: クライアントの平均信号強度。
- **AP Outgoing Packet Loss Ratio(%)**: クライアントが受信したパケットの平均パケット損失率。
- **Incoming Packet Error Ratio(%)**: クライアントが受信したパケットの平均エラーパケット率。
- **Packet Retransmission Ratio**: クライアントの平均パケット再送信率。

その他のパラメーターは、総合評価情報と同じです。詳細については、「クライアントのオンライン履歴情報リストの表示」を参照してください。

履歴レコード

クライアントの履歴評価情報を表示します。詳細は、「クライアントのオンライン履歴情報の問合せ」を参照してください。

無線評価情報の表示

無線評価情報には、無線の送信トラフィック、チャネルパケットエラー率、およびチャネルパケット使用率が含まれます。評価情報を表示すると、無線の動作ステータスを確認できます。

無線評価情報を表示するには、Radioタブをクリックします。

ラジオ一覧の内容

- **Radio ID**: 無線ID。
- **Radio Type**: 無線のタイプ。オプションは、**11a**、**11b**、**11g**、**11n**、**11gn**、および**11an**です。
- **AP Label**: 無線が属するAPのラベル。
- **Tx.Unicasts(MB)**: 送信されたユニキャストトラフィック。
- **Tx.Multicasts/Broadcasts(MB)**: 送信されたマルチキャストおよびブロードキャストトラフィック。
- **Tx.Traffic(MB)**: 送信トラフィックの合計。
- **Rx.Unicasts(MB)**: 受信したユニキャストトラフィック。
- **Rx.Multicasts/Broadcasts(MB)**: 受信したマルチキャストおよびブロードキャストトラフィック。
- **Rx.Traffic(MB)**: 受信トラフィックの合計。
- **Channel Packet Error Ratio(%)**: 動作チャネルのパケットエラー率。
- **Channel Usage(%)**: 動作チャネルの利用率。

ラジオリストに十分なエントリーが含まれている場合は、次のナビゲーション支援が表示されます。

- **Next Page**アイコンをクリックして、**Radio List**で次のページに進みます。
- **Last Page**アイコンをクリックして、**Radio List**の最後のページに進みます。
- **Previous Page**アイコンをクリックして、**Radio List**で前のページに戻ります。
- **First Page**アイコンをクリックすると、**Radio List**の先頭に戻ることができます。

Radio Listの右上にある8、15、50、100、または200をクリックして、各ページに表示する項目数を指定します。

注:

Radio Listをフィールドごとにソートすることはできません。

評価された無線のクエリー

WSMは、基本問合せと拡張問合せを提供します。基本問合せでは、高速検索の唯一の基準として無線IDが使用されます。拡張問合せでは、正確な照合のための様々な問合せ基準が提供されます。

基本クエリー

1. **Radio**タブをクリックします。
2. 右上隅の**Query**フィールドに無線IDを入力します。
3. **Query**アイコンをクリックします。無線リストには、基準に一致するすべての無線の評価情報が表示されます。

高度なクエリー

1. **Radio**タブをクリックします。
2. **Expand**アイコンをクリックします。次のように問合せ基準を設定します。
   - **AP Label**: 無線が属するAPのラベルを入力します。WSMは、このフィールドのファジーマッチングをサポートします。
   - **Radio Type**: 無線タイプを選択します。オプションには、**Unlimited**、**11a**、**11b**、**11g**、**11n**、**11gn**、**11 an**があります。
   - **View History Records**: 履歴レコードを表示するかどうかを選択します。すべての履歴レコードまたは1日の履歴レコードを表示できます。15分ごとに収集されたデータが1つのレコードを形成します。このオプションを選択する場合は、評価日を選択する必要があります。
   - **Evaluation Date**: **View History Records**オプションを選択した場合は、日付を選択してその日の履歴レコードを表示するか、**Unlimited**を選択してすべての履歴レコードを表示します。
   - **Radio ID**: 無線IDを入力します。
   - **Evaluation Indexes**: 問合せの評価索引を設定します。たとえば、チャネル使用率が20%未満の無線の評価情報を表示できます。この問合せ基準には、評価索引、比較演算子および値の3つの部分があります。

評価指標は次のとおりです。

- **Tx. Traffic (MB)**
- **Rx. Traffic (MB)**
- **Channel Packet Error Ratio (%)**
- **Channel Usage (%)**

比較演算子には次のものがあります。

- **等号(=)**
- **右山カッコと等号(>=)**
- **右山カッコ(>)**
- **左山カッコと等号(<=)**
- **左山カッコ(<)**

3. **Query**をクリックします。無線リストには、基準に一致するすべての無線の評価情報が表示されます。
4. すべての基準をクリアするには、**Reset**をクリックします。無線リストには、すべての無線の評価情報が表示されます。

チャネル評価情報の表示

チャネル評価情報を使用してチャネル使用率を表示できます。チャネル評価情報を表示するには、**Channel**

タブをクリックします。

チャンネルリストの内容

- **Radio Type**: このチャネルで動作している無線のタイプ。
- **AP Label**: 無線が属するAPのラベル。
- **IP Address** :APのIPアドレス。
- **Radio ID**: 無線ID。
- **Channel**: チャネル。
- **Channel Bandwidth(MHz)**: チャネル帯域幅(22 MHzまたは44 MHz)。
- **Avg.Channel Usage(%)**: 平均チャネル使用率。
- **Avg.Packet Rx.Channel Usage(%)**: チャネルでのパケット受信の平均使用率。
- **Avg.Packet Tx.Channel Usage(%)**: チャネルでのパケット送信の平均使用率。

チャネルリストに十分な数のエントリーがある場合は、次のナビゲーションツールが表示されます。

- **Next Page**アイコンをクリックして、**Channel List**内で次のページに進みます。
- **Last Page**アイコンをクリックすると、**Channel List**の最後にページ送りされます。
- **Previous Page**アイコンをクリックすると、**Channel List**内で前のページに戻ります。
- **First Page**アイコンをクリックすると、**Channel List**の先頭にページバックします。

チャネルリストの右上にある8、15、50、100、または200をクリックして、各ページに表示する項目の数を指定します。

注:

Channel Listをフィールドごとに並べ替えることはできません。

評価されたチャネルの照会

WSMでは、基本問合せと拡張問合せが提供されます。基本問合せでは、クイック検索の唯一の基準としてチャネルが使用されます。拡張問合せでは、正確な照合のための様々な問合せ基準が提供されます。

基本クエリー

1. **Channel**タブをクリックします。
2. 右上隅の**Query**フィールドにチャネル番号を入力します。
3. **Query**アイコンをクリックします。チャネルリストに、問合せ基準に一致するチャネルの評価情報が表示されます。

高度なクエリー

1. **Query**タブをクリックします。
2. 問合せフィールドの右にある**Expand**アイコンをクリックします。次のように問合せ基準を設定します。
   - **APラベルAP Label**: APラベルを入力します。WSMは、このフィールドのファジーマッチングをサポートします。
   - **Channel**: チャネル番号を入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
   - **View History Records**: 履歴レコードを表示するかどうかを選択します。すべての履歴レコードまたは1日の履歴レコードを表示できます。15分ごとに収集されたデータが1つのレコードを形成します。このオプションを選択する場合は、評価日を選択する必要があります。
   - **Evaluation Date**: **View History Records**オプションを選択した場合は、日付を選択してその

日の履歴レコードを表示するか、**Unlimited**を選択してすべての履歴レコードを表示します。

- **AP Channel Analysis**: 問合せの評価索引を設定します。たとえば、使用率が20%未満のチャネルの評価情報を表示できます。この問合せ基準には、評価索引、比較演算子および値の3つの部分があります。

評価指標は次のとおりです。

- **Avg. Channel Usage (%)**
- **Avg. Packet Rx. Channel Usage (%)**
- **Avg. Packet Tx. Channel Usage (%)**

比較演算子には次のものがあります。

- **等号(=)**
- **右山カッコと等号(>=)**
- **右山カッコ(>)**
- **左山カッコと等号(<=)**
- **左山カッコ(<)**

3. **Query**をクリックします。チャネルリストには、基準に一致するすべてのチャネルの評価情報が表示されます。
4. **Reset**をクリックすると、すべての基準がクリアされます。チャネルリストには、すべてのチャネルの評価情報が表示されます。

ワイヤレスサービスレポート

WSMレポートには、WSMサービス統計が表とグラフで表示されます。

WSMには、多数のリアルタイムレポートおよびスケジュール済レポートが事前定義されています。オペレーターはレポートをカスタマイズすることもできます。レポートをカスタマイズするには、IMC iARコンポーネントを使用する必要があります。

- **Realtime report**: オペレーターは、デバイス、クライアント、およびサービスに関する現在の統計情報または特定の時間範囲の統計情報を表示したり、レポートを印刷したり、後で表示およびダウンロードできるようにWSMサーバーに保存したりできます。
- **Scheduled report**: オペレーターが生成期間とレポートテンプレートを事前定義できるようにします。オペレーターは、データ比較とトレンド分析のために、異なる期間に生成されたレポートを表示できます。WSMます。WSMでは、レポートをオペレーターに電子メールで送信することができます。

ショートカットの追加、WSMレポートの変更、削除、エクスポートまたは印刷などの基本機能は、IMCプラットフォームレポートと同じです。このドキュメントでは、スケジュール済レポートの追加機能とリアルタイム/スケジュール済レポートの表示機能のみを説明します。基本レポート操作については、『H3C IMC v7.3 Enterprise and Standard Platform Administrator Guide』を参照してください。

リアルタイムレポート

リアルタイムレポートを使用すると、オペレーターは現在の統計情報または特定の時間範囲の統計情報を表示できます。

リアルタイムレポートの表示

1. **Report**タブをクリックします。
2. ナビゲーションツリーからレポート**Reports** > **Report Template List**の順に選択して、**Report Template List**ページを表示します。
3. **Query Template**領域で、**Type**リストから**Wireless Service Report**を選択し、**Query**をクリック。
   Report Template Listには、すべてのワイヤレスサービスレポートが表示されます。
4. 表示するレポートテンプレートの名前を指定するリンクをクリックします。

レポートを生成するためのパラメーターを設定するページが開きます。

5. 必要なパラメーターを設定し、**OK**をクリックします。

パラメーターは、レポートテンプレートによって異なります。次の情報では、各レポートおよびレポートコンテンツの表示に必要なパラメーターについて説明します。

AC統計レポート

AC統計情報レポートを表示するには、次のパラメーターを設定します。

- **Parameter "Begin Time and End Time"**: 統計収集の時間範囲をリストから選択します。**Last Hour**、**Last Day**、**Last Week**または**Last Month**など特定の時間範囲を選択するか、Custom Rangeを選択して開始時間と終了時間を手動で指定できます。
- **Begin Time/End Time**: は、カスタム範囲を選択した場合にのみ表示されます。
  Begin Time/End Timeの横にあるフィールドをクリックして、表示されるカレンダーから開始時間/終了時間をYYYY-MM-DD hh:mm形式で選択します。終了時間は開始時間より後である必要が

あります。

AC統計情報レポートのフィールド:

- **Report Period**: 統計情報が収集された期間。
- **AC Name**: ACの名前。
- **IP Address**: ACのIPv4アドレス。
- **AP Number** :ACによって管理されているAPの合計数。
- **Online/M APs**: ACによって管理されているマスターAPの数。
- **Online/B APs**: ACによって管理されているバックアップオンラインAPの数。
- **Availability(%)**: ACによって管理されているAPが使用可能な時間の割合。
- **Busy APs**: ACによって管理されているビジー状態のAPの数。APは、関連付けられているクライアント番号または伝送速度が指定したしきい値に達するとビジー状態と見なされます。詳細については、**Busy AP statistics report**を参照してください。
- **Idle APs** :ACによって管理されるアイドル状態のAPの数。APは、関連付けられたクライアント番号または伝送レートが指定したしきい値以下の場合にアイドル状態と見なされます。の詳細については、「アイドル状態のAP統計情報レポート」を参照してください。
- **Worst APs** :ACによって管理されるワーストAPの数。アウトオブサービスレートまたはアソシエーション輻輳レートが指定したしきい値に達すると、APはワーストと見なされます。
- **Transmitted Traffic(MB)**: ACによって送信されたトラフィックの合計。
- **Received Traffic(MB)**: ACが受信したトラフィックの合計。
- **Packet Retransmit Ratio(%)**: 送信されたパケットの総数に対する再送信されたパケットの数の割合。
- **Error Frame Ratio(%)** :ACで受信された合計フレーム数に対するエラーフレーム数の割合。
- **(Mb/s)**: ACの最大転送速度。
- **Avg Transmit Speed (Mb/s)**: ACの平均転送速度です。
- **Max Receive Speed(Mb/s)**: ACの最大受信速度。
- **Avg Receive Speed(Mb/s)**:ACの平均受信速度。
- **Max Online Client Number**: AC上のオンラインクライアントの最大数。
- **Avg Online Client Number**: AC上のオンラインクライアントの平均数。
- **AP Average Utilization(%)**: ACによって管理されるAP全体の平均使用率。Avg Online Client Number/Xとして計算されます(Xはコンフィギュレーションファイルで指定されているAP使用率の値)。
- **AP Peak Utilization(%)**: ACによって管理されるAP全体のピーク使用率。**Max Online Client Number/X**として計算されます(Xはコンフィギュレーションファイルで指定されたAP使用値)。
- **Total Client Online Duration**: クライアントの合計オンライン時間。
- **Avg Client Online Duration**: クライアントの平均オンライン時間。
- **Successful Accesses**: クライアントがACによって管理されているAPに正常にアソシエートした合計回数。
- **Success Rate(%)**: アクセス要求の合計数に対する成功したアクセスの割合。
- **Association Congestion Rate(%)**: ACのクライアントアソシエーションの輻輳率。アソシエーション要求の総数に対するアソシエーションの失敗数の比率です。
- **Client Dropping Rate(%)**: ACのクライアントドロップレート。これは、オンラインクライアントの合計数に対するクライアントの異常ログアウトの割合です。

APアソシエーションサマリーレポート

このレポートには、すべてのAPまたはロケーションビュー内のAPのクライアントアソシエーション統計情報のサマリーが表示されます。ロケーションビューにサブロケーションがある場合、レポートには、ロケーションビューとそのサブロケーションのクライアントアソシエーション統計情報のサマリーと上位10位までも表示されます。

APアソシエーションサマリーレポートを表示するには、次のパラメーターを設定します。

- **Parameter** "**Begin Time and End Time**": 統計収集の時間範囲をリストから選択します。**Last Hour**、**Last Week**または**Last Month**などの特定の時間範囲を選択するか、**Custom Range**を選択して開始時間と終了時間を手動で指定できます。
- **Location**: 統計情報収集用の特定のロケーションビューを選択するか、**All AP Devices**を選択します。
- **Begin Time/End Time**: これらの2つのパラメーターは、**Custom Range**を選択した場合にのみ表示されます。
  Begin Time/End Timeの横にあるフィールドをクリックして、表示されるカレンダーから開始時間/終了時間をYYYY-MM-DD hh:mm形式で選択します。終了時間は開始時間より後である必要があります。

APアソシエーションサマリーレポートのパラメーター:

- **Report Period**: 統計情報が収集される期間。
- **Location**: 統計情報が収集されるロケーションビューの名前、または**All AP Devices**

AP association summary reportフィールド:

- **Location**: ロケーションビュー名または**All AP Devices**。
- **AP Number**: ロケーションビューに含まれているAPの数、またはすべてのAPの合計数。
- **Access Requests**: クライアントアクセス要求の合計数。
- **Access Responses**: APから要求元クライアントに送信された応答の合計数。
- **Successful Accesses**: クライアントがAPに正常にアソシエートされた合計回数。
- **Abnormal Logouts**: APに関連付けられているクライアントが異常ログアウトした合計回数。
- **Client Dropping Rate(%)**: APのクライアントドロップレート。これは、オンラインクライアントの総数に対するクライアントの異常なログアウトの割合です。
- **Success Rate(%)**: APのクライアントアクセス成功率。これは、アクセス要求の総数に対する成功したアクセスの割合です。
- **Association Congestion Rate(%)**: APのクライアントアソシエーションの輻輳率。アソシエーション要求の総数に対するアソシエーション失敗の割合です。

APアソシエーション詳細レポート

このレポートには、個々のAPの詳細なクライアントアソシエーション統計情報が表示されます。このレポートを使用すると、ユーザーは個々のAPのアクセス品質と所属するロケーションビューを確認できます。

APアソシエーションの詳細レポートを表示するには、次のパラメーターを設定します。

- **Parameter "Begin Time and End Time"**: 統計収集の時間範囲をリストから選択します。**Last Hour**、**Last Day**、**Last Week**または**Last Month**など特定の時間範囲を選択するか、**Custom Range**を選択して開始時間と終了時間を手動で指定できます。
- **Location**: 統計情報収集用の特定のロケーションビューを選択するか、All AP Devicesを選択します。
- **Begin Time/End Time**: これらの2つのパラメーターは、**Custom Range**を選択した場合にのみ表示されます。
  Begin Time/End Timeの横にあるフィールドをクリックして、表示されるカレンダーから開始時間/終了時間をYYYY-MM-DD hh:mm形式で選択します。終了時間は開始時間より後である必要が

あります。

APアソシエーション詳細レポートのパラメーター:

- **Report Period**: 統計情報が収集される期間。
- **Location**: 統計情報が収集されるロケーションビューの名前または**All AP Devices**

AP association detail reportの各フィールド

- **AP Label**: アクセスポイント名。
- **AP Location**: APが属するロケーションビュー。
- **Access Requests**: APが受信したクライアントアクセス要求の合計数。
- **Access Responses**: APが要求元クライアントに送信した応答の合計数。
- **Successful Accesses**: クライアントがAPに正常にアソシエートした合計回数。
- **Abnormal Logouts**: APに関連付けられているクライアントが異常ログアウトした合計回数。
- **Client Dropping Rate(%)**: APのクライアントドロップレート。これは、APに関連付けられているクライアントの合計数に対する異常ログアウトの割合です。
- **Success Rate(%)**: APのクライアントアソシエーションの成功率。これは、アクセス要求の総数に対する成功したアクセスの割合です。
- **Association Congestion Rate(%)**: APのクライアントアソシエーションの輻輳率。アソシエーション要求の総数に対するアソシエーションの失敗数の比率です。

AP可用性概要レポート

このレポートには、すべてのAPまたはロケーションビュー内のAPの可用性統計のサマリーが表示されます。ロケーションビューにサブロケーションがある場合、レポートには、ロケーションビューおよびそのサブロケーションの可用性統計のサマリーと上位10位までも表示されます。

APアベイラビリティサマリーレポートを表示するには、次のパラメーターを設定します。

- **Parameter "Begin Time and End Time"**: 統計収集の時間範囲をリストから選択します。**Last Hour**、**Last Day**、**Last Week**または**Last Month**など特定の時間範囲を選択するか、**Custom Rang**eを選択して開始時間と終了時間を手動で指定できます。
- **Location**: 統計情報収集用の特定のロケーションビューを選択するか、**All AP Devices**を選択します。
- **Begin Time/End Time**: これらの2つのパラメーターは、**Custom Range** を選択した場合にのみ表示されます。開始時刻、終了時刻の横にあるフィールドをクリックして、表示されるカレンダーから開始時刻と終了時刻をYYYY-MM-DD hh:mm形式で選択します。終了時刻は開始時刻よりも後である必要があります。

AP可用性概要レポートのパラメーター:

- **Report Period**: 統計情報が収集された期間。
- **Location**: 統計情報が収集されるロケーションビューの名前または**All AP Devices**

AP Availability Summaryレポートのフィールド:

- **Availability Highest Top 10**: 可用性が最も高い上位10位のロケーションビューを表示します。棒グラフで表示されます。
- **Availability Lowest Top 10** 最下位可用性が最も低い上位10位のロケーションビューを棒グラフで表示します。
- **Location**: ロケーションビュー名またはAll AP Devices。
- **AP Number**: APの合計数。

- **Total Unavailable Time**: APの合計使用不能時間。
- **Total Available Time**: APの合計使用可能時間。
- **Availability**: APが使用可能な時間の割合。

AP可用性詳細レポート

このレポートには、個々のAPの詳細なアベイラビリティ統計情報が表示されます。

AP可用性詳細レポートを表示するには、次のパラメーターを設定します。

- **Parameter "Begin Time and End Time"**: 統計収集の時間範囲をリストから選択します。**Last Hour**、**Last Day**、**Last Week**または**Last Month**など特定の時間範囲を選択するか**Custom Range**を選択して開始時間と終了時間を手動で指定できます。
- **Location**: 統計情報収集用の特定のロケーションビューを選択するか、**All AP Devices**を選択します。
- **Begin Time/End Time**: これらの2つのパラメーターは、**Custom Range**を選択した場合にのみ表示されます。
  Begin Time/End Timeの横にあるフィールドをクリックして、表示されるカレンダーから開始時間/終了時間をYYYY-MM-DD hh:mm形式で選択します。終了時間は開始時間より後である必要があります。

AP可用性詳細レポートのフィールド:

- **Report Period**: 統計情報が収集される期間。
- **Location**: 統計情報が収集されるロケーションビューの名前または**All AP Devices**。
- **AP Name**: アクセスポイントの名前。
- **AP Location**: APが属するロケーションビュー。
- **IP Address**: APのIPv4アドレス。
- **Model:** APモデル。
- **Available Time**: APが使用可能な合計時間。
- **Unavailable Time**: APが使用できない合計時間。
- **Availability**: A Pが使用可能な時間の割合。

APトラフィック要約レポート

このレポートには、すべてのAPまたはロケーションビュー内のAPのサマリートラフィック統計が表示されます。ロケーションビューにサブロケーションがある場合、レポートには、サブロケーションのサマリートラフィック統計と、有線/無線トラフィックボリュームが最も大きい上位10のロケーションビューも表示されます。これらの統計は、将来のスケーラビリティニーズに対するキャパシティプランニングに役立ちます。

APトラフィックサマリーレポートを表示するには、次のパラメーターを設定します。

- **Parameter "Begin Time and End Time"**: 統計収集の時間範囲をリストから選択します。**Last Hours**、**Last Day**、**Last Week**または**Last Month**など特定の時間範囲を選択するか、Self-Definedを選択して開始時間と終了時間を手動で指定できます。
- **Location**: 統計情報収集用の特定のロケーションビューを選択するか、**All AP Devices**を選択します。
- **Begin Time/End Time**: これらの2つのパラメーターは、**Custom Range**を選択した場合にのみ表示されます。
  Begin Time/End Timeの横にあるフィールドをクリックして、表示されるカレンダーから開始時間/終了時間をYYYY-MM-DD hh:mm形式で選択します。終了時間は開始時間より後である必要があります。

AP Traffic Summaryレポートのパラメーター:

- **Report Period**: 統計情報が収集される期間。
- **Position**: 統計情報が収集されるロケーションビューの名前または**All AP Devices**

AP Traffic Summaryレポートのグラフ:

- **Core Traffic Top 10**: 有線トラフィックが最も高い上位10のロケーションビューを表示します。
  棒グラフのボリューム。
- **Radio Traffic Top 10**: 無線トラフィック量が最も多い上位10位のロケーションビューを棒グラフで表示します。
- **Core Traffic Trend**
- **Radio Traffic Trend**
- **Position**: ロケーションビュー名またはAll AP Devices。
- **AP Number**: ロケーションビューに含まれているAPの数、またはすべてのAPの合計数。
- **Core Frames Reception**: APが有線ネットワークから受信したフレームの合計数。
- **Core Errors Reception** APが有線ネットワークから受信したエラーパケットの合計数。
- **Core Traffic Reception(MB)**: APが有線ネットワークから受信したトラフィックの合計。
- **Core Traffic Transmission(MB)**: APから有線ネットワークに送信されたトラフィックの合計。
- **Radio Frames Reception**: APが無線ネットワークから受信したフレームの合計数。
- **Radio Errors Reception**: APが無線ネットワークから受信したエラーパケットの合計数。
- **Radio Traffic Reception(MB)**: 無線ネットワークからAPが受信したトラフィックの合計。
- **Radio Traffic Transmission(MB)**: APからワイヤレスネットワークに送信されたトラフィックの合計。

APトラフィック詳細レポート

このレポートには、個々のAPと、有線および無線トラフィック量が最も多い上位10のAPのトラフィック統計情報が表示されます。これらの統計情報は、将来のスケーラビリティのニーズに対応するキャパシティプランニングに役立ちます。

APトラフィックの詳細レポートを表示するには、次のパラメーターを設定します。

- **Parameter "Begin Time and End Time"**: 統計収集の時間範囲をリストから選択します。**Last Hour**、**Last Day**、**Last Week**または**Last Month**など特定の時間範囲を選択するか、Custom Rangeを選択して開始時間と終了時間を手動で指定できます。
- **Location**: 統計情報収集用の特定のロケーションビューを選択するか、**All AP Devices**を選択します。
- **Begin Time/End Time**: これらの2つのパラメーターは、カスタム範囲を選択した場合にのみ表示されます。
  Begin Time/End Timeの横にあるフィールドをクリックして、表示されるカレンダーから開始時間/終了時間をYYYY-MM-DD hh:mm形式で選択します。終了時間は開始時間より後である必要があります。

APトラフィック詳細レポートのパラメーター:

- **Report Period**: 統計情報が収集される期間。
- **Location**: 統計情報が収集されるロケーションビューの名前、または**All AP Devices**

AP traffic detail reportフィールド:

- Core Traffic Top 10有線トラフィック量が最も多い上位10のAPをバーで表示します。
  グラフ
- **Core Traffic Top 10**: ワイヤレストラフィック量が最も多い上位10のAPを棒グラフで表示しま

す。

- **AP Name**: アクセスポイントの名前。
- **Location**: APが属するロケーションビュー。
- **IP Address**: APのIPv4アドレス。
- **Core Frames Reception**: APが有線ネットワークから受信したフレームの総数。
- **Core Errors Reception**: APが有線ネットワークから受信したエラーパケットの合計数。
- **Core Bytes Reception**: APが有線ネットワークから受信したバイト数の合計。
- **Core Bytes Transmission**: APから有線ネットワークに送信された合計バイト数。
- **Radio Frames Reception**: APが無線ネットワークから受信したフレームの総数。
- **Radio Errors Reception**: APが無線ネットワークから受信したエラーパケットの総数。
- **Radio Bytes Reception**: APが無線ネットワークから受信した総バイト数。
- **Radio Bytes Transmission**: APから無線ネットワークに送信された総バイト数。

AP速度レポート

このレポートには、個々のAPのデータ送受信速度が表示されます。また、特定の期間におけるすべてのAPの集約データを使用して、データ送受信速度の全体的な傾向が折れ線グラフで示されます。

AP速度レポートを表示するには、次のパラメーターを設定します。

- **Parameter "Begin Time and End Time"**: 統計収集の時間範囲をリストから選択します。**Last Hours**、**Last Day**、**Last Week**または**Last Month**など特定の時間範囲を選択するか、**Custom Range**を選択して開始時間と終了時間を手動で指定できます。
- **Location**: 統計情報収集用の特定のロケーションビューを選択するか、**All AP Devices**を選択します。
- **Begin Time/End Time**: これらの2つのパラメーターは、**Custom Range**を選択した場合にのみ表示されます。
  Begin Time/End Timeの横にあるフィールドをクリックして、表示されるカレンダーから開始時間/終了時間をYYYY-MM-DD hh:mm形式で選択します。終了時間は開始時間より後である必要があります。

AP速度レポートのパラメーター:

- **Report Period**: 統計情報が収集される期間。
- **Location**: 統計情報が収集されるロケーションビューの名前または**All AP Devices**。

AP速度レポートのフィールド:

- トレンドグラフ-受信速度、送信速度、および合計の変化を表示します。
  指定したレポート期間中のすべてのAPの速度を折れ線グラフで表示します。すべてのAPの受信速度、送信速度、および合計速度の最大値と平均値がグラフの上部に表示されます。
- **AP Label**: FIT APのラベル。
- **Location**: APが属するロケーションビュー。
- **Max Reception Speed**: APの最大受信速度。
- 平均受信速度: APの平均受信速度。
- **Max Transmission Speed**: APの最大伝送速度。
- **Avg Transmission Speed**: APの平均伝送速度。
- **Max Total Speed**: APの最大合計速度。
- **Avg Total Speed**: APの平均合計速度。

APログオフ要約レポート

このレポートには、すべてのAPまたはロケーションビュー内のAPの要約ログオフ統計が表示されます。ロケーションビューにサブロケーションがある場合、レポートには、ロケーションビューとそのサブロケーションの要約および上位10のログオフ統計も表示されます。

APオフラインサマリーレポートを表示するには、次のパラメーターを設定します。

- **Parameter "Begin Time and End Time"**: 統計収集の時間範囲をリストから選択します。**Last Hours**、**Last Day**、**Last Week**または**Last Month**など特定の時間範囲を選択するか、**Custom Range**を選択して開始時間と終了時間を手動で指定できます。
- **Position**: 統計情報収集用の特定のロケーションビューを選択するか、**All AP Devices**を選択します。
- **Begin Time/End Time**: これらの2つのパラメーターは、**Custom Range**を選択した場合にのみ表示されます。
  Begin Time/End Timeの横にあるフィールドをクリックして、表示されるカレンダーから開始時間/終了時間をYYYY-MM-DD hh:mm形式で選択します。終了時間は開始時間より後である必要があります。
- **Logoff Time(Hour)**: オフライン期間を時間単位で指定します。値は整数である必要があります。レポートには、APオフライン期間が指定した値に達した回数が表示されます。

APログオフ要約レポートのパラメーター:

- **レポート期間**: 統計情報が収集される期間。
- **Location**: 統計情報が収集されるロケーションビューの名前、または**All AP Devices**

AP offline summary reportフィールド:

- **Logoff Count Top 10**: APオフライン数が最も多い上位10のロケーションビューを表示します。
- **Count of Logoff(Duration>=0 Hour)Top 10**: 期間が0時間に達するAPオフライン数が最も多い上位10のロケーションビューを表示します。ここで、0は指定したログオフ時間です。
- **Position**: ロケーションビュー名または**All AP Devices**。
- **AP Number**: ロケーションビューに含まれているAPの数、またはすべてのAPの合計数。
- **Total Logoff Count**: ロケーションビューに含まれるAPまたはすべてのAPのオフラインカウントの合計。
- **Count of Logoff(Duration>=0 Hour)**: APのオフライン期間が0時間に達した合計回数。**Logoff Time**には0が指定されています。
- **Total Logoff Duration**: ロケーションビューに含まれるAPまたはすべてのAPの合計オフライン期間。

APログオフ詳細レポート

このレポートには、指定したクエリー基準に基づく詳細なAPログオフ統計情報が表示されます。

APオフライン詳細レポートを表示するには、次のパラメーターを設定します。

- **Parameter "Begin Time and End Time"**: 統計情報収集の時間範囲をリストに表示されます。**Last Hour**、**Last Day**、**Last Week**、Last Monthなどの特定の時間範囲を選択するか、または**Custom Range**を選択して、開始時刻と終了時刻を手動で指定できます。
- **Location**: 統計情報収集用の特定のロケーションビューを選択するか、**All AP Devices**を選択します。
- **Begin Time/End Time**: これらの2つのパラメーターは、**Custom Range**を選択した場合にのみ表

示されます。
Begin Time/End Timeの横にあるフィールドをクリックして、表示されるカレンダーから開始時間/終了時間をYYYY-MM-DD hh:mm形式で選択します。終了時間は開始時間より後である必要があります。

- **Logoff Time(Hour)**: オフライン期間を時間単位で指定します。値は整数である必要があります。このレポートでは、オフライン期間が指定した値に達したAPに関する統計のみが収集されます。

APログオフ詳細レポートのフィールド:

- **Report Period**: 統計情報が収集される期間。
- **Location**: 統計情報が収集されるロケーションビューの名前または**All AP Devices**。
- **AP Name**: アクセスポイントの名前。
- **Location**: APが属するロケーションビュー。
- **IP Address**: APのIPv4アドレス。
- **Model**: APモデル。
- **Logoff Time**: APがログオフした時刻。
- **Recovery Time**: APが回復した時間。
- **Logoff Duration** APのログオフ期間。

無線エラーレポート

このレポートには、AP無線で受信されたエラーフレームの数が表示されます。

無線エラーレポートを表示するには、次のパラメーターを設定します。

- **Parameter "Begin Time and End Time"**: 統計情報収集の時間範囲をリストに表示されます。**Last Hour**、**Last Day**、**Last Week**、**Last Month**などの特定の時間範囲を選択するか、または**Custom Range**を選択して、開始時刻と終了時刻を手動で指定できます。
- **Location**: 統計情報収集用の特定のロケーションビューを選択するか、**All AP Devices**を選択します。
- **Begin Time/End Time**: これらの2つのパラメーターは、**Custom Range**を選択した場合にのみ表示されます。
Begin Time/End Timeの横にあるフィールドをクリックして、表示されるカレンダーから開始時間/終了時間をYYYY-MM-DD hh:mm形式で選択します。終了時間は開始時間より後である必要があります。

無線エラーレポートのフィールド:

- **Report Period**: 統計情報が収集される期間。
- **Location**: 統計情報が収集されるロケーションビューの名前または**All AP Devices**。
- **AP Name**:アクセスポイントの名前。
- **Radio ID:** 無線ID。
- **AP Location**: APが属するロケーションビュー。
- **FCS Error Frames**: AP無線が受信したFCSエラーフレームの数。
- **PHY Error Frames**: AP無線が受信したPHYエラーフレームの数。
- **MIC Error Frames**: AP無線が受信したMICエラーフレームの数。
- **Error Ratio**: AP無線で受信された合計フレーム数に対する、FCS、PHY、およびMICエラーフレームの合計数の比率。

ラジオトラフィックレポート

このレポートには、AP無線のトラフィック統計情報が表示されます。

無線トラフィックレポートを表示するには、次のパラメーターを設定します。

- **Parameter "Begin Time and End Time"**: 統計収集の時間範囲をリストから選択します。**Last Hour**、**Last Day**、**Last Week**または**Last Month**など特定の時間範囲を選択するか、Custom Rangeを選択して開始時間と終了時間を手動で指定できます。
- **Location**:統計情報収集用の特定のロケーションビューを選択するか、**All AP Devices**を選択します。
- **Begin Time/End Time**: これらの2つのパラメーターは、カスタム範囲を選択した場合にのみ表示されます。
  Begin Time/End Timeの横にあるフィールドをクリックして、表示されるカレンダーから開始時間/終了時間をYYYY-MM-DD hh:mm形式で選択します。終了時間は開始時間より後である必要があります。

無線トラフィックレポートのフィールド:

- **Report Period**: 統計情報が収集される期間。
- **Location**: 統計情報が収集されるロケーションビューの名前または**All AP Devices**。
- **AP Name**: アクセスポイントの名前。
- **Radio ID**: 無線のID。
- **AP Location**: APが属するロケーションビュー。
- **Reception(bytes)**: AP無線が受信した合計トラフィック。
- **Transmission(bytes)**: AP無線によって送信された合計トラフィック。
- **Total Traffic(bytes)**: AP無線で送受信されたトラフィックの合計。

無線速度レポート

このレポートには、AP無線の最大および平均の受信速度と送信速度が表示されます。無線速度レポートを

表示するには、次のパラメーターを設定します。

- **Parameter "Begin Time and End Time"**: 統計情報収集の時間範囲をリストに表示されます。**Last Hour**、**Last Day**、**Last Week**、**Last Month**などの特定の時間範囲を選択するか、または**Custom Range**を選択して、開始時刻と終了時刻を手動で指定できます。
- **Location**: 統計情報収集用の特定のロケーションビューを選択するか、**All AP Devices**を選択します。
- **Begin Time/End Time**: これらの2つのパラメーターは、**Custom Range**を選択した場合にのみ表示されます。
  Begin Time/End Timeの横にあるフィールドをクリックして、表示されるカレンダーから開始時間/終了時間をYYYY-MM-DD hh:mm形式で選択します。終了時間は開始時間より後である必要があります。

無線速度レポートのフィールド:

- **Report Period**: 統計情報が収集される期間。
- **Location**: 統計情報が収集されるロケーションビューの名前または**All AP Devices**。
- **AP Label**: アクセスポイント名。
- **Radio ID**: 無線のID。
- **AP Location**: APが属するロケーションビュー。
- **Max Reception Speed(bits/s)**: 無線の最大受信速度。
- **Average Reception Speed (bits/s)**: 無線の平均受信速度。
- **Max Transmission Speed(bits/s)**: 無線の最大伝送速度。

- **Avg Transmission Speed(bits/s)**: 無線の平均伝送速度。

無線リソース使用状況レポート

このレポートには、AP無線のリソース使用状況の統計情報が表示されます。

無線リソース使用状況レポートを表示するには、次のパラメーターを設定します。

- **Parameter "Begin Time and End Time"**: 統計収集の時間範囲をリストから選択します。**Last Hour**、**Last Day**、**Last Week**または**Last Month**など特定の時間範囲を選択するか、**Custom Range**を選択して開始時間と終了時間を手動で指定できます。
- **Location**: 統計情報収集用の特定のロケーションビューを選択するか、**All AP Devices**を選択します。
- **Begin Time/End Time**: これらの2つのパラメーターは、**Custom Range**を選択した場合にのみ表示されます。
  Begin Time/End Timeの横にあるフィールドをクリックして、表示されるカレンダーから開始時間/終了時間をYYYY-MM-DD hh:mm形式で選択します。終了時間は開始時間より後である必要があります。

無線リソース使用状況レポートのフィールド:

- **Report Period**: 統計情報が収集される期間。
- **Location**: 統計情報が収集されるロケーションビューの名前または**All AP Devices**。
- **AP Name**: アクセスポイントの名前。
- **Radio ID**: 無線のID。
- **AP Location**: APが属するロケーションビュー。
- **IP Address**: APのIPv4アドレス。
- **Model**: APモデル。
- **Usage**: 無線の使用率。

無線チャネル使用状況レポート

このレポートには、無線ごとの無線チャネル使用状況の統計情報が表示されます。

無線リソース使用状況レポートを表示するには、次のパラメーターを設定します。

- **Location**: 統計情報収集用の特定のロケーションビューを選択するか、**All AP Devices**を選択します。

  Radio Channel Usage Top 10: グラフには、チャネル使用率が最も高い上位10台の無線が表示されます。横軸はAPラベルと無線IDを表し、縦軸はチャネル使用率の値を表します。

次に、無線チャネル使用状況レポートのフィールドを示します。

- **AP Label**: APのデバイスラベル。
- **AP IP**: APのIPアドレス。
- **AP Serial ID**: APのシリアルID。
- **Location**: APが属するロケーションビューの名前。
- **Radio ID**: 無線のID。
- **Channel Usage**: 無線のチャネル使用状況。

Rogue AP履歴レポート

このレポートには、検出された不正APの履歴レコードがMACアドレス別に表示されます。

不正APの履歴レポートを表示するには、次のパラメーターを設定します。

- **Parameter "Begin Time and End Time"**: 統計情報収集の時間範囲を
リストに表示されます。**Last Hour、Last Day、Last Week、Last Month**などの特定の時間範囲を選択するか、または**Custom Range**を選択して、開始時刻と終了時刻を手動で指定できます。
- **Begin Time/End Time**: これらの2つのパラメーターは、カスタム範囲を選択した場合にのみ表示されます。**Begin Time/End Time**の横にあるフィールドをクリックして、表示されるカレンダーから開始時刻と終了時刻をYYYY-MM-DD hh:mm形式で選択します。終了時刻は開始時刻よりも後である必要があります。

Rogue AP Historyレポートのフィールド:

- **Report Period**: 統計情報が収集される期間。
- **MAC Address**:不正APのMACアドレス。
- **Vendor**: 不正なAPのベンダー。
- **SSID**: 不正なAPのSSID。
- **Max Signal Strength**:不正APの最大信号強度。
- **Channel**: 不正APで使用されているチャネル。
- **Detected by**: 不正なAPを検出したACによって検出されました。
- **Detected AP**:不正なAPを検出したFit AP。
- **Last Discovered Time**: 不正なAPが最後に検出された時刻。
- **Status**:不正APの状態。オプションはAttackedとNot Attackedです。

Rogue APレポート

このレポートには、新たに検出されたすべての不正APがMACアドレス別に表示されます。

不正APレポートを表示するために特定のパラメーターは必要ありません。

Rogue APレポートのフィールド:

- **MAC Address**: 不正APのMACアドレス。
- **Vendor**: 不正なAPのベンダー。
- **SSID**: 不正なAPのSSID。
- **Max Signal Strength**: APの最大信号強度。
- **Channel**:不正APで使用されているチャネル。
- **Detected by**: 不正なAPを検出したACによって検出されました。
- **Last Discovered Time**: 不正なAPが最後に検出された時刻。
- **Attacked Status**: 不正なAPの状態。オプションは**Attacked**と**Not Attacked**です。

Rogue Client Historyレポート

このレポートには、検出された不正クライアントの履歴レコードがMACアドレス別に表示さ

れます。不正クライアントの履歴レポートを表示するには、次のパラメーターを設定します。

- **Parameter "Begin Time and End Time"**: 統計情報収集の時間範囲がリストに表示されます。**Last Hour、Last Day、Last Week、Last Month**などの特定の時間範囲を選択するか、または**Custom Range**を選択して、開始時刻と終了時刻を手動で指定できます。

- **Begin Time/End Time**: これらの2つのパラメーターは、カスタム範囲を選択した場合にのみ表示されます。
  Begin Time/End Timeの横にあるフィールドをクリックして、表示されるカレンダーから開始時間/終了時間をYYYY-MM-DD hh:mm形式で選択します。終了時間は開始時間より後である必要があります。

Rogue Client Historyレポートのフィールド:

- **Report Period**: 統計情報が収集される期間。
- **MAC Address**: 不正クライアントのMACアドレス。
- **SSID**:
- **Vendor**: 不正クライアントのベンダー。
- **Max Signal Strength**: 不正なクライアントの最大信号強度。
- **Channel**: 不正なクライアントが使用するチャネル。
- **Detected by**: ACによって検出されました。
- **Detected AP**:不正なクライアントを検出したAPを適合させます。
- **Last Discovered Time**: 不正クライアントが最後に検出された時刻。
- **Attacked Status**: 不正なクライアントの状態。オプションは**Attacked**と**Not Attacked**です。

不正クライアントレポート

このレポートには、最初に検出されたすべての新しい不正クライアントがMACアドレス別に表示されます。不正クライアントレポートを表示するために特定のパラメーターは必要ありません。

不正クライアントレポートのフィールド:

- **MAC Address**: 不正クライアントのMACアドレス。
- **Vendor**: 不正クライアントのベンダー。
- **Max Signal Strength**: 不正なクライアントの最大信号強度。
- **Channel**: 不正なクライアントが使用するチャネル。
- **Detected by**: ACによって検出されました。
- **Last Discovered Time**: 不正クライアントが最後に検出された時刻。
- **Attacked Status**: 不正なクライアントの状態。オプションは**Attacked**と**Not Attacked**です。

現在関連付けられているクライアント統計レポート

このレポートには、現在アソシエートされているクライアントに関する情報が、MACアドレス別、およびアソシエート期間が最も長い上位10クライアント別に表示されます。

現在関連付けられているクライアント統計情報レポートを表示するには、次のパラメーターを設定します。

- **Location**: 統計情報収集用の特定のロケーションビューを選択するか、**All AP Devices**を選択します。現在関連付けられているクライアント統計レポートのフィールド:

- **Position**: 統計情報が収集されるロケーションビューの名前または**All AP Devices**。
- **Associated Duration Top 10**: クライアントMACアドレス別に、関連付けられている期間が最も長い上位10クライアントを表示します。
- **MAC Address**: 関連付けられたクライアントのMACアドレス。
- **Client Name**: 関連付けられたクライアントの名前。

- **IP Address**: 関連付けられたクライアントのIPアドレス。
- **SSID**: 関連付けられたクライアントによって使用されるSSID。
- **Channel**: 関連付けられたクライアントによって使用されるチャネル。
- **AP Name**: クライアントがアソシエートされているアクセスポイントの名前。
- **AP Position**: APが属するロケーションビュー。
- **Session Duration**: クライアントに関連付けられている現在の継続時間。
- **Received Traffic(MB)**: 関連付けられたクライアントが受信したトラフィックの合計。
- **Transmitted Traffic(MB)**: 関連付けられたクライアントによって送信されたトラフィックの合計。
- **Total Traffic(MB)**: 関連付けられたクライアントが送受信したトラフィックの合計。

AP別のホットスポット統計レポート

このレポートには、ホットスポットとして設定されているロケーションに含まれるAPに関する統計情報が表示されます。ロケーションにサブロケーションがある場合は、ホットスポットとして設定されているサブロケーションのAP統計情報も表示されます。

ホットスポット統計レポートをAP別に表示するには、次のパラメーターを設定します。

- **Location**: 統計情報収集用の特定のロケーションビューを選択するか、**All AP Devices**を選択します。

Hotspot statistics report by APフィールド:

- **Location**: 統計情報が収集されるロケーションビューの名前または**All AP Devices**。
- **Myltest:** ホットスポットとして設定されているロケーションビューの名前。**myltest**は、このラボ環境で使用されるホットスポットロケーションビューの名前です。実際のロケーションビューの名前は、特定のネットワーク環境に依存します。ホットスポットロケーションビューが使用できない場合、このフィールドは空です。
- **test**: ホットスポットとして設定されているロケーションビューの名前。**test**は、このラボ環境で使用されるホットスポットロケーションビューの名前です。実際のロケーションビューの名前は、特定のネットワーク環境によって異なります。ホットスポットロケーションビューが使用できない場合、このフィールドは空です。
- **AP Number**: ホットスポットロケーションビューに含まれるAPの数。
- **Online AP Number**: ホットスポット位置ビューに含まれるオンラインAPの数。
- **AP Name**: ホットスポットロケーションビューに含まれるアクセスポイントの名前。
- **Status**: APの状態(OnlineまたはOffline)。
- **Serial ID**: APのシリアルID。
- **Model**: APのモデル。
- **IP Address**: APのIPv4アドレス。

ワイヤレス資産統計レポート

このレポートには、WSMの管理対象ワイヤレスデバイスの資産統計が円グラフで表示されます。ワイヤレス資産統計レポートを表示するために特定のパラメーターは必要ありません。

円グラフには、デバイスカテゴリ別の資産の数と、合計に対する各デバイスカテゴリの貢献度が表示されます。特定の資産カテゴリのデバイスリストを表示するには、グラフ上で対応するスライスをクリックします。

クライアント要約レポート

このレポートには、クライアントの関連付けられた合計時間と期間がMACアドレス別に表示されます。また、関連付けられた合計期間が最も長い上位10クライアントも表示されます。

クライアントサマリーレポートを表示するには、次のパラメーターを設定します。

- **Parameter "Begin Time and End Time"**: 統計収集の時間範囲をリストから選択します。**Last Hour**、**Last Day**、**Last Week**または**Last Month**など特定の時間範囲を選択するか、**Custom Range**を選択して開始時間と終了時間を手動で指定できます。
- **Location**: 統計情報収集用の特定のロケーションビューを選択するか、**All AP Devices**を選択します。
- **Begin Time/End Time**: これらの2つのパラメーターは、**Custom Range**を選択した場合にのみ表示されます。
  Begin Time/End Timeの横にあるフィールドをクリックして、表示されるカレンダーから開始時間/終了時間をYYYY-MM-DD hh:mm形式で選択します。終了時間は開始時間より後である必要があります。
- **Online Duration**: 収集するクライアントのオンライン期間を入力します。このレポートでは、オンライン期間が指定した時間より長いクライアントに関する統計が収集されます。
- **Column name**: レポートをソートする列を選択します。
- **Order**: ソート順序を選択します。オプションは**Ascending**および**Descending**です。クライアントサ

マリーレポートのパラメーター:

- **Report Period**: 統計情報が収集される期間。
- **Position**: 統計情報が収集されるロケーションビューの名前または**All AP Devices**。クライアン

ト要約レポートのフィールド:

- **Total Associated Duration Top 10**: 最も長く関連付けられている上位10クライアントを表示します。
  継続時間
- **MAC Address**: クライアントのMACアドレス。
- **Client Name**: クライアントの名前。
- **Online Times**: クライアントがオンライン接続を開始した合計回数。
- **Total Associated Duration**: クライアントに関連付けられた合計期間。
- **Avg Associated Duration**: クライアントに関連付けられている平均期間。
- **Received Traffic(MB)**: クライアントが受信したトラフィックの合計。
- **Sent Traffic(MB)**: クライアントによって送信されたトラフィックの合計。
- **Total Traffic(MB)**: クライアントが送受信したトラフィックの合計。

クライアント詳細レポート

このレポートには、クライアントの詳細なアソシエーションレコードがMACアドレス別に表示されます。

クライアント詳細レポートを表示するには、次のパラメーターを設定します。

- **Parameter "Begin Time and End Time"**: 統計収集の時間範囲をリストから選択します。**Last Hour**、**Last Day**、**Last Week**または**Last Month**など特定の時間範囲を選択するか、Custom Rangeを選択して開始時間と終了時間を手動で指定できます。
- **Location**: 統計情報収集用の特定のロケーションビューを選択するか、**All AP Devices**を選択しま

す。

- **Begin Time/End Time**: これらの2つのパラメーターは、**Custom Range**を選択した場合にのみ表示されます。
  Begin Time/End Timeの横にあるフィールドをクリックして、表示されるカレンダーから開始時間/終了時間をYYYY-MM-DD hh:mm形式で選択します。終了時間は開始時間より後である必要があります。
- **Online Duration**: 収集するクライアントのオンライン期間を入力します。このレポートでは、オンライン期間が指定した時間より長いクライアントに関する統計が収集されます。

クライアント詳細レポートのフィールド:

- **Report Period**: 統計情報が収集される期間。
- **Position**: 統計情報が収集されるロケーションビューの名前または**All AP Devices**。
- **MAC Address**: クライアントのMACアドレス。
- **Client Name**: クライアントの名前。
- **IP Address**: クライアントのIPv4アドレス。
- **Radio Type**: 無線のタイプ。
- **SSID**: クライアントが使用するSSID。
- **AP Name**: クライアントがアソシエートされているAPの名前。
- **Position**: APが属するロケーションビュー。
- **Online Time**: クライアントがAPに正常に関連付けられた時刻。
- **Session Duration**: クライアントセッションの期間。
- **Received Traffic(MB)**: クライアントが受信したトラフィックの合計。
- **Sent Traffic(MB)**: クライアントによって送信されたトラフィックの合計。
- **Total Traffic(MB)**: クライアントが送受信したトラフィックの合計。

顧客番号トレンドラインレポート

このレポートには、すべてのAPまたはロケーションビュー内のAPに関するクライアントアソシエーション統計情報の概要と詳細の両方が表示されます。このレポートには、すべてのAPの集約データと個々のAPの詳細な統計情報を使用して、アソシエートされているクライアント番号の変化の全体的な傾向が表示されます。

クライアント番号の近似曲線レポートを表示するには、次のパラメーターを設定します。

- **Parameter "Begin Time and End Time"**: 統計収集の時間範囲をリストから選択します。**Last Hour**、**Last Day**、**Last Week**または**Last Month**など特定の時間範囲を選択するか、**Custom Range**を選択して開始時間と終了時間を手動で指定できます。
- **Location**: 統計情報収集用の特定のロケーションビューを選択するか、**All AP Devices**を選択します。
- **Begin Time/End Time**: これらの2つのパラメーターは、**Custom Range**を選択した場合にのみ表示されます。
  Begin Time/End Timeの横にあるフィールドをクリックして、表示されるカレンダーから開始時間/終了時間をYYYY-MM-DD hh:mm形式で選択します。終了時間は開始時間より後である必要があります。
- **Column name**: レポートをソートする列を選択します。
- **Order**: ソート順序を選択します。オプションは**Ascending**および**Descending**です。

クライアント番号トレンドラインレポートパラメーター:

- **Report Period**: 統計情報が収集される期間。

- **Location**: 統計情報が収集されるロケーションビューの名前または**All AP Devices**。クライアント番号の近似曲線レポートのフィールド:

- **Global Statistics**: 指定したレポート期間中にすべてのAPに関連付けられたクライアントの合計数の変化を折れ線グラフで表示します。グラフの左上にある**Max online client number**および**Avg online client number**は、すべてのAPに関連付けられたクライアントの最大数と平均数を示します。
- **AP Name**: アクセスポイントの名前。
- **Location**: APが属するロケーションビュー。
- **Max Online Client Number**: APにアソシエートされているクライアントの最大数。
- **Avg Online Client Number**: APにアソシエートされているクライアントの平均数。
- **Total Client Associated Duration**: クライアントに関連付けられた合計期間。
- **Avg Client Associated Duration**: クライアントに関連付けられている平均継続時間。
- **AP Peak Utilization(%)**: APのピーク使用率。Max Online Client Number/X(Xはコンフィギュレーションファイルで指定されたAP使用値)として計算されます。
- **AP Average Utilization(%)**: APの平均使用率。Avg Online Client Number/Xとして計算されます。Xは、コンフィギュレーションファイルで指定されているAP使用率の値です。

Busy AP統計情報レポート

このレポートには、APのピークオンラインクライアント数、ピーク伝送レート、アウトオブサービスレート、アソシエーション輻輳レート、およびクライアントドロップレートなど、総使用量が最も高いAPに関する統計情報が表示されます。

ビジーAP統計情報レポートを表示するには、次のパラメーターを設定します。

- **Parameter "Begin Time and End Time"**: 統計収集の時間範囲をリストから選択します。**Last Hour**、**Last Day**、**Last Week**または**Last Month**など特定の時間範囲を選択するか、Custom Rangeを選択して開始時間と終了時間を手動で指定できます。
- **Location**: 統計情報収集用の特定のロケーションビューを選択するか、**All AP Devices**を選択します。
- **Begin Time/End Time**: これらの2つのパラメーターは、**Custom Range**を選択した場合にのみ表示されます。
  Begin Time/End Timeの横にあるフィールドをクリックして、表示されるカレンダーから開始時間/終了時間をYYYY-MM-DD hh:mm形式で選択します。終了時間は開始時間より後である必要があります。
- **Peak Number of Online Clients**: APのオンラインクライアントしきい値のピーク数を指定します。オンラインクライアント数が指定したしきい値に達すると、APはビジー状態であると見なされます。デフォルトは20です。**Save**をクリックしてデフォルト値として保存します。
- **Peak Transmission Rate**: APのピーク伝送レートしきい値をMb/s単位で指定します。伝送レートが指定したしきい値に達すると、APはビジー状態と見なされます。デフォルトは6 Mb/sです。**Save**をクリックして、デフォルト値として保存します。

  ビジー状態のAPを判別するための**Peak Number of Online Clients**と**Peak Transmission Rate**の条件は、"OR"の関係にあります。つまり、いずれかの条件を満たす限り、APはビジー状態であると見なされます。**Peak Number of Online Clients**と**Peak Transmission Rate**の横にある**Save**をクリックして、現在の設定を以降のアクセスのデフォルトとして保存します。
- **Column name**: レポートをソートする列を選択します。
- **Orde**r: ソート順序を選択します。オプションは**Ascending**および**Descending**です

Busy AP統計情報レポートのフィールド:

- **Report Period**: 統計情報が収集される期間。
- **Location**: 統計情報が収集されるロケーションビューの名前または**All AP Devices**。
- **AP Name**: アクセスポイントの名前。
- **AP Location**: APが属するロケーションビュー。
- **Peak Number of Online Clients**: APにアソシエートされているクライアントの最大数。
- **Peak Transmission Rate(Mbps mbps)**: APの最大伝送レート。
- **Out of Service Rate(%)**: APが使用できない時間の割合。
- **Association Congestion Rate(%)**: APのアソシエーション輻輳率。アソシエーション要求の総数に対するクライアントアソシエーションの失敗数の比率です。
- **Client Dropping Rate(%)**: APのクライアントドロップレート。これは、APに関連付けられているクライアントの合計数に対する異常なログオフの比率です。

アイドルAP統計情報レポート

このレポートには、ピークオンラインクライアント数、ピーク伝送レート、アウトオブサービスレート、アソシエーション輻輳レート、およびクライアントドロップレートなど、総使用量が最も低いAPに関する統計情報が表示されます。

アイドルAP統計情報レポートを表示するには、次のパラメーターを設定します。

- **Parameter "Begin Time and End Time"**: 統計収集の時間範囲をリストから選択します。**Last Hour**、**Last Day**、**Last Week**または**Last Month**など特定の時間範囲を選択するか、**Custom Range**を選択して開始時間と終了時間を手動で指定できます。
- **Location**: 統計情報収集用の特定のロケーションビューを選択するか、**All AP Devices**を選択します。
- **Begin Time/End Time**: これらの2つのパラメーターは、**Custom Range**を選択した場合にのみ表示されます。
  Begin Time/End Timeの横にあるフィールドをクリックして、表示されるカレンダーから開始時間/終了時間をYYYY-MM-DD hh:mm形式で選択します。終了時間は開始時間より後である必要があります。
- **Peak Number of Online Clients**: APのピークオンラインクライアント数の閾値を指定します。オンラインクライアント数が指定したしきい値以下の場合、APはアイドル状態と見なされます。デフォルトは0です。デフォルト値として保存するには、Saveをクリックします。
- **Peak Transmission Rate**: APの最大伝送レートしきい値をMb/s単位で指定します。伝送レートが指定したしきい値以下の場合、APはアイドル状態と見なされます。デフォルトは1Mb/sです。**Save**をクリックして、デフォルト値として保存します。

  アイドル状態のAPを判別するための**Peak Number of Online Clients**および**Peak Transmission Rate**の条件は、OR関係にあります。つまり、APはいずれかの条件を満たすかぎりアイドル状態とみなされます。**Peak Number of Online Client**sおよび**Peak Transmission Rate**の横にある**Save**をクリックすると、現在の設定が保存され、以降のアクセスのデフォルトとして使用されます。
- **Column name**: レポートをソートする列を選択します。
- **Order**: ソート順序を選択します。オプションは**Ascending**および**Descending**です。アイドルAP統

計情報レポートのフィールド:

- **Report Period**: 統計情報が収集される期間。
- **Location**: 統計情報が収集されるロケーションビューの名前または**All AP Devices**。
- **AP Name**: アクセスポイントの名前。

- **AP Location**: APが属するロケーションビュー。
- **Peak Number of Online Clients**: APにアソシエートされているクライアントの最大数。
- **Peak Transmission Rate(Mbps mbps)**: APの最大伝送レート。
- **Out of Service Rate(%)**: APが使用できない時間の割合。
- **Association Congestion Rate(%)**: APのアソシエーション輻輳率。アソシエーション要求の総数に対するクライアントアソシエーションの失敗数の比率です。
- **Client Dropping Rate(%)**: APのクライアントドロップレート。これは、APに関連付けられているクライアントの合計数に対する異常なログオフの比率です。

ワーストAP統計レポート

このレポートには、ピークオンラインクライアント数、ピーク伝送レート、アウトオブサービスレート、アソシエーション輻輳レート、およびクライアントドロップレートなど、最悪のAPに関する統計情報が表示されます。

最悪のAP統計情報レポートを表示するには、次のパラメーターを設定します。

- **Parameter** "**Begin Time and End Time**": 統計収集の時間範囲をリストから選択します。**Last Hour**、**Last Day**、**Last Week**または**Last Month**など特定の時間範囲を選択するか、**Custom Range**を選択して開始時間と終了時間を手動で指定できます。
- **Location**: 統計情報収集用の特定のロケーションビューを選択するか、**All AP Devices**を選択します。
- **Begin Time/End Time** これらの2つのパラメーターは、**Custom Range**を選択した場合にのみ表示されます。
  Begin Time/End Timeの横にあるフィールドをクリックして、表示されるカレンダーから開始時間/終了時間をYYYY-MM-DD hh:mm形式で選択します。終了時間は開始時間より後である必要があります。
- **Out of Service Rate**: APのアウトオブサービスレートしきい値を指定します。アウトオブサービスレートが指定したしきい値に達すると、APは最悪のAPとして分類されます。**Save**をクリックして、デフォルト値として保存します。
- **Relevant Blocking Rate**: APに関連するブロッキングレートしきい値を指定します。関連するブロッキングレートが指定したしきい値以上の場合、APは最悪と見なされます。値の範囲は0.0～100.0で、デフォルトは5%です。**Save**をクリックしてデフォルト値として保存します。
- **Dropping Rat**e: APのドロップレートしきい値を指定します。ドロップレートが指定したしきい値に達すると、APは最悪と見なされます。値の範囲は0.0～100.0で、デフォルトは3%です。**-1**を入力すると、このパラメーターは最悪のAP統計情報レポートを生成する条件として使用されません。デフォルト値として保存するには、**Save**をクリックします。

  Out of Service Rate、**Relevant Blocking Rate**、および**Dropping Rate**の各条件は、OR関係にあります。つまり、3つの条件のいずれかを満たすAPは最悪と見なされます。**Out of Service Rate**、**Relevant Blocking Rate**、および**Dropping Rate**の横にある**Save**をクリックすると、現在の設定が保存され、以降のアクセスのデフォルトとして使用されます。

Worst AP statisticsレポートのフィールド:

- **Report Period**: 統計情報が収集される期間。
- **Position**: ロケーションビュー名またはAll AP Devices。
- **AP Name**: アクセスポイントの名前。
- **AP Location**: APが属するロケーションビュー。
- **Peak Number of Online Clients**: APにアソシエートされているクライアントの最大数。
- **Peak Transmission Rate(Mbps mbps)**: APの最大伝送レート。
- **Out of Service Rate(%)**: APが使用できない時間の割合。

- **Association Congestion Rate(%)**: APのアソシエーション輻輳率。アソシエーション要求の総数に対するクライアントアソシエーションの失敗数の比率です。
- **Client Dropping Rate(%)**: APのクライアントドロップレート。これは、APに関連付けられているクライアントの合計数に対する異常なログオフの比率です。

AP統計レポート

AP統計情報レポートを表示するには、次のパラメーターを設定します。

- **Parameter "Begin Time and End Time"**: 統計収集の時間範囲をリストから選択します。**Last Hour**、**Last Day**、**Last Week**または**Last Month**など特定の時間範囲を選択するか、Custom Rangeを選択して開始時間と終了時間を手動で指定できます。
- **Location**: 統計情報収集用の特定のロケーションビューを選択するか、**All AP Devices**を選択します。
- **Begin Time/End Time**: これらの2つのパラメーターは、カスタム範囲を選択した場合にのみ表示されます。
  Begin Time/End Timeの横にあるフィールドをクリックして、表示されるカレンダーから開始時間/終了時間をYYYY-MM-DD hh:mm形式で選択します。終了時間は開始時間より後である必要があります。
- **Column name**: レポートをソートする列を選択します。
- **Order**: ソート順序を選択します。オプションは**Ascending**および**Descending**です。

AP統計レポートのフィールド:

- **Report Period**: 統計情報が収集される期間。
- **Location**: 統計情報が収集されるロケーションビューの名前または**All AP Devices**。
- **AP Name**: アクセスポイントの名前。
- **Location**: APが属するロケーションビュー。
- **Availability(%)**: APが使用可能な時間の割合。
- **Transmitted Core Traffic(MB)**: APから有線ネットワークに送信されたトラフィックの合計。
- **Received Core Traffic(MB)**: APが有線ネットワークから受信したトラフィックの合計。
- **Transmitted Radio Traffic(MB)**: APからワイヤレスネットワークに送信されたトラフィックの合計。
- **Received Radio Traffic(MB)**: APがワイヤレスネットワークから受信したトラフィックの合計。
- **Packet Retransmit Ratio(%)**: APによって送信された合計パケット数に対する再送信されたパケットの割合。
- **Error Frame Ratio(%)**: APで受信された合計フレーム数に対するエラーフレームの割合。
- **Max Transmit Speed(Mb/s)**: APの最大伝送速度。
- **Avg Transmit Speed(Mb/s)**: APの平均伝送速度。
- **Max Receive Speed(Mb/s)**: APの最大受信速度。
- **Avg Receive Speed(Mb/s)**: APの平均受信速度。
- **Max Online Client Number**: APにアソシエートされているクライアントの最大数。
- **Avg Online Client Number**: A Pにアソシエートされているクライアントの平均数。
- **AP Average Utilization(%)**: APの平均使用率。Avg Online Client Number/Xとして計算されます。Xは、コンフィギュレーションファイルで指定されているAP使用率の値です。
- **AP Peak Utilization(%)**: APのピーク使用率。Max Online Client Number/Xとして計算されます。Xは、コンフィギュレーションファイルで指定されているAP使用値です。
- **Total Client Online Duration**: APに関連付けられているクライアントの合計オンライン時間。

- **Avg Client Online Duration**: APに関連付けられているクライアントの平均オンライン時間。
- **Successful Accesses**: クライアントがAPに正常にアソシエートした合計回数。
- **Success Rate(%)**: APのクライアントアクセス成功率。これは、クライアントによって行われたアクセス要求の総数に対する、成功したアクセスの割合です。
- **Association Congestion Rate(%)**: APのクライアントアソシエーションの輻輳率。クライアントアソシエーション要求の総数に対するアソシエーションの失敗数の比率です。
- **Client Dropping Rate(%)**: APのクライアントドロップレート。これは、APに関連付けられているオンラインクライアントの総数に対する異常なログオフの割合です。

SSID Online Client Number Statisticsレポート

このレポートには、SSID別の最大オンラインクライアント数と平均オンラインクライアント数が表示されます。

SSIDオンラインクライアント番号統計情報レポートを表示するには、次のパラメーターを設定します。

- **Parameter "Begin Time and End Time"**: 統計収集の時間範囲をリストから選択します。**Last Hour**、**Last Day, Last Week**または**Last Month**など特定の時間範囲を選択するか、**Custom Range**を選択して開始時間と終了時間を手動で指定できます。
- **Begin Time/End Time**: これらの2つのパラメーターは、**Custom Range**を選択した場合にのみ表示されます。
  Begin Time/End Timeの横にあるフィールドをクリックして、表示されるカレンダーから開始時間/終了時間をYYYY-MM-DD hh:mm形式で選択します。終了時間は開始時間より後である必要があります。

SSIDオンラインクライアント番号統計情報レポートのフィールド:

- **Report Period**: 統計情報が収集される期間。
- **SSID**: Service Set Identifier(サービスセットID)。
- **Max Online Client Number**: SSIDを使用するAPにアソシエートされているクライアントの最大数。
- **Avg Online Client Number**: SSIDを使用するAPにアソシエートされているクライアントの平均数。

SSID統計情報レポート

このレポートには、SSID別のAPトラフィックおよびオンラインクライアント統計情報のサマリーが表示されます。SSID統計情報レポートを表示するには、次のパラメーターを設定します。

- **Parameter "Begin Time and End Time"**: 統計情報収集の時間範囲をリストに表示されます。**Last Hour**、**Last Day**、**Last Week**、**Last Month**などの特定の時間範囲を選択するか、または**Custom Range**を選択して、開始時刻と終了時刻を手動で指定できます。
- **Location**: 統計情報収集用の特定のロケーションビューを選択するか、**All AP Devices**を選択します。
- **Begin Time/End Time**: これらの2つのパラメーターは、**Custom Range**を選択した場合にのみ表示されます。
  Begin Time/End Timeの横にあるフィールドをクリックして、表示されるカレンダーから開始時間/終了時間をYYYY-MM-DD hh:mm形式で選択します。終了時間は開始時間より後である必要があります。

SSID統計情報レポートのフィールド:

- **Report Period**: 統計情報が収集される期間。
- **Location**: 統計情報が収集されるロケーションビューの名前または**All AP Devices**。
- **SSID**: Service Set Identifier(サービスセットID)。

- **Transmitted Radio Traffic(MB)**: SSIDを使用するAPによって送信されたトラフィックの合計。
- **Received Radio Traffic(MB)**: SSIDを使用するAPが受信したトラフィックの合計。
- **Max Online Client Number**: SSIDを使用するAPにアソシエートされているクライアントの最大数。
- **Avg Online Client Number**: SSIDを使用するAPにアソシエートされているクライアントの平均数。
- **Availability(%)**: SSIDを使用するAPが使用可能な時間の割合。

ホットスポット別のホットスポット統計レポート

このレポートには、ホットスポットとして設定されているロケーションビューが表示されます。

ホットスポット統計レポートをホットスポット別に表示するには、次のパラメーターを設定します。

- **Parameter "Begin Time and End Time"**: 統計収集の時間範囲をリストから選択します。**Last Hour**、**Last Day**、**Last Week**または**Last Month**など特定の時間範囲を選択するか、**Custom Range**を選択して開始時間と終了時間を手動で指定できます。
- Location: 統計情報収集用の特定のロケーションビューを選択するか、**All AP Devices**を選択します。
- **Begin Time/End Time**: これらの2つのパラメーターは、**Custom Range**を選択した場合にのみ表示されます。
  Begin Time/End Timeの横にあるフィールドをクリックして、表示されるカレンダーから開始時間/終了時間をYYYY-MM-DD hh:mm形式で選択します。終了時間は開始時間より後である必要があります。

ホットスポット統計レポート(ホットスポットフィールド別):

- **Report Period**: 統計情報が収集される期間。
- **Location**: 統計情報が収集されるロケーションビューの名前または**All AP Devices**。
- **Hotspot Name**: ホットスポットとして設定されているロケーションビューの名前。
- **AP Number**: ホットスポットロケーションビューに含まれるAPの数。
- オンラインAP数: ホットスポット位置ビューに含まれるオンラインAPの数。
- **Availability(%)**: APが使用可能な時間の割合。Busy APsホットスポット位置ビュー内のビジー状態のAPの数。オンラインクライアントのピーク数またはピーク伝送速度が指定したしきい値に達すると、APはビジー状態と見なされます。
- **Idle APs**: ホットスポットロケーションビュー内のアイドル状態のAPの数。オンラインクライアントのピーク数またはピーク伝送レートが、指定したしきい値以下になると、APはアイドル状態と見なされます。
- **Worst APs**: ホットスポットロケーションビュー内の最悪のAPの数。アウトオブサービスレートまたはアソシエーション輻輳レートが指定したしきい値に達すると、APは最悪と見なされます。
- **Transmitted Traffic(MB)**: ホットスポットロケーションビューでAPが送信したトラフィックの合計。
- **Received Traffic(MB)**: ホットスポットロケーションビューでAPが受信したトラフィックの合計。
- **Packet Retransmit Ratio(%)**: ホットスポットロケーションビューでAPによって送信された合計パケット数に対する、再送信されたパケット数の割合。
- **Error Frame Ratio(%)**: ホットスポットロケーションビューでAPが受信した合計フレーム数に対するエラーフレーム数の割合。
- **Max Transmit Speed(Mb/s)**: ホットスポットロケーションビューでのAPの最大送信速度。
- **Avg Transmit Speed(Mb/s)** :ホットスポットロケーションビューでのAPの平均送信速度。
- **Max Receive Speed(Mb/s)**: ホットスポットロケーションビューでのAPの最大受信速度。

- **Avg Receive Speed(Mb/s)**: ホットスポットロケーションビューでのAPの平均受信速度。
- **Max Online Client Number**: ホットスポットロケーションビュー内のオンラインクライアントの最大数。
- **Avg Online Client Number**: ホットスポットロケーションビュー内のオンラインクライアントの平均数。
- **AP Average Utilization(%)**: APの平均使用率。Avg Online Client Number/Xとして計算されます。Xはコンフィギュレーションファイルで指定されているAP使用率の値です。
- **AP Peak Utilization(%)**: APのピーク使用率。Max Online Client Number/Xとして計算されます。Xは、コンフィギュレーションファイルで指定されているAP使用値です。
- **Total Client Online Duration**: クライアントの合計オンライン時間。
- **Avg Client Online Duration**: クライアントの平均オンライン時間。
- **Successful Accesses**: クライアントがホットスポットロケーションビューに含まれるAPに正常にアソシエートした合計回数。
- **Success Rate(%)**: クライアントによって実行されたアクセス要求の総数に対する、成功したアクセスの割合。
- **Association Congestion Rate(%)**: アソシエーション要求の総数に対するクライアントアソシエーションの失敗数の割合。
- **Client Dropping Rate(%)**: オンラインクライアントの総数に対するクライアントの異常なログアウトの割合。

サイトアクセスポイントとネイバーレポート

このレポートには、すべてのAPまたはロケーションビュー内のAPのネイバー統計情報が表示されます。

サイトアクセスポイントとネイバーのレポートを表示するには、次のパラメーターを設定します。

- **Location**: 統計情報収集用の特定のロケーションビューを選択するか、**All AP Devices**を選択します。サイトアクセスポイントおよびネイバーレポートのフィールド:

- **Location**: 統計情報が収集されるロケーションビューの名前または**All AP Devices**。
- **Radio BSSID**: 検出されたネイバーAPの無線BSSID。
- **SSID**: 検出されたネイバーAPのSSID。
- **Wireless Mode**: 検出されたネイバーAPのワイヤレスモード。
- **Channel**: 検出されたネイバーAPのチャネル。
- **SNR(dB)**: 検出されたネイバーAPのSignal-to-Noise Ratio(SNR;信号対雑音比)。
- **Signal(dBm)**: 検出されたネイバーAPの信号強度。
- **Noise(dBm)**: 検出されたネイバーAPのノイズレベル。
- **Detected By**: ネイバーAPが検出されたアクセスポイントの名前。

APチャネル品質統計情報レポート

APチャネル品質統計情報レポートを表示するには、次のパラメーターを設定します。

- **Parameter "Begin Time and End Time"**: 統計収集の時間範囲をリストから選択します。**Last Hour**、**Last Day**、**Last Week**または**Last Month**など特定の時間範囲を選択するか、Custom Rangeを選択して開始時間と終了時間を手動で指定できます。
- **Location**: 統計情報収集用の特定のロケーションビューを選択するか、**All AP Devices**を選択します。
- **Begin Time/End Time**: これらの2つのパラメーターは、カスタム範囲を選択した場合にのみ表示されます。
  Begin Time/End Timeの横にあるフィールドをクリックして、表示されるカレンダーから開始時

間/終了時間をYYYY-MM-DD hh:mm形式で選択します。終了時間は開始時間より後である必要があります。

APチャネル品質統計情報レポート:

- **Report Period**: 統計情報が収集される期間。
- **Location**: 統計情報が収集されるロケーションビューの名前または**All AP Devices**。
- **AP Name**: アクセスポイントの名前。
- **AP Location**: APが属するロケーションビュー。
- **Radio ID**: 無線ID。
- **Monitored Channel**: APで使用されているチャネル。
- 平均品質平均チャネル品質。高い値はチャネルの通信品質が高いことを示し、その逆も同様です。

Detected APsレポート

このレポートには、WLANで検出されたAPの各カテゴリの数量と詳細が表示されます。検出されたAPレポートを表示するためにパラメーターを設定する必要はありません。

Detected AP Category円グラフには、検出されたAPの各カテゴリの割合が表示されます。このグラフには、次のAPカテゴリが含まれる場合があります。

- **Authorized APs**: WLANで許可されているAPの合計数。
- **Misconfigured APs**: WLANサービスの設定が正しくなく、WLANで許可されているAPの総数。
- **Rogue APs**: WLANで使用できないAPの合計数。
- **External APs**: 隣接WLAN内にあるAPの合計数。
- **Ad Hoc APs**: アドホックモードで動作しているAPの合計数。
- **Potential-Authorized APs**: 許可される可能性のあるAPの合計数。
- **Potential-Rogue APs**: 不正デバイスである可能性があるAPの合計数。
- **Potential-External APs**: 外部ネットワークからの可能性があるAPの合計数。
- **Uncategorized APs**: カテゴリを判別できないAPの合計数。

検出されたAPリストには、各カテゴリのAPの合計数とその詳細が表示されます。

- **Status**: APの状態(OnlineまたはOffline)。
- **BSSID**: APのBSSID(MACアドレス)。
- **SSID**: APで使用されるSSID。
- **Virtual Security Domain**: APを検出したセンサーが属する仮想セキュリティドメイン。
- **Category**: APのカテゴリ。オプションは、**Authorized**、**Rogue**、**Ad hoc**、**Misconfigured**、**External**、**Potential-Authorized**、**Potential-Rogue**、**Potential-External**、および**Uncategorized**です。
- **Threat Level**: APの脅威レベル。
- **Detecting AC**: APを検出したセンサーがアソシエートされているACのデバイスラベル。
- **Device Vendor**: 検出されたAPのベンダー。センサーがAPに関するベンダー情報を取得しない場合、このフィールドにはnullが表示されます。
- **First Detection**: APが最初に検出された時刻。
- **Last Detection**: APが最後に検出された時刻。
- **Trust**: APが信頼できるデバイスリストにあるかどうか。オプションはYesおよびNoです。

- **Alarm**: APがアラーム無視デバイスリストにあるかどうか。オプションはYesおよびNoです。
- **Block**: APがブロックデバイスリストにあるかどうか。オプションはYesおよびNoです。
- **Countermeasure**: APが対策デバイスリストにあるかどうかを示します。オプションは**Yes**と**No**です。

検出されたAP履歴レポート

このレポートには、WLANで検出された各カテゴリのAPの履歴数量と詳細が表示されます。検出されたAP履歴レポートを表示するためにパラメーターを設定する必要はありません。

Detected AP History Category円グラフには、検出されたAPの各カテゴリの割合が表示されます。このグラフには、次のAPカテゴリが含まれる場合があります。

- **Authorized APs**: WLANで許可されているAPの合計数。
- **Misconfigured APs**: WLANサービスの設定が正しくなく、WLANで許可されているAPの総数。
- **Rogue APs**: WLANで使用できないAPの合計数。
- **External APs**: 隣接WLAN内にあるAPの合計数。
- **Ad Hoc APs**: アドホックモードで動作しているAPの合計数。
- **Potential-Authorized APs**: 許可される可能性のあるAPの合計数。
- **Potential-Rogue APs**: 不正デバイスである可能性があるAPの合計数。
- **Potential-External APs**: 外部ネットワークからの可能性があるAPの合計数。
- **Uncategorized APs**: カテゴリを判別できないAPの合計数。

検出されたAPの履歴リストには、各カテゴリのAPの合計数とその詳細が表示されます。

- **MAC Address**: 検出されたAPのMACアドレス。MACアドレスをクリックすると、APの詳細が表示されます。
- **SSID**: APで使用されるSSID。
- **Last Detection Time**: APが最後に検出された時刻。
- **Disappeared At**: APが検出されなくなった時間。
- **Virtual Security**: APを検出したセンサーが属する仮想セキュリティドメイン。
- **Category**: APのカテゴリ。**Authorized**、**Rogue**、**Ad hoc**、**Misconfigured**、**External**、**Potential-Authorized**、**Potential-Rogue**、**Potential-External**、または**Uncategorized**です。
- **Device Ven**: 検出されたAPのベンダー。センサーがAPに関するベンダー情報を取得しない場合、このフィールドにはnullが表示されます。
- **Threat Level**: APの脅威レベル。値が大きいほど、脅威レベルが高くなります。
- **Detecting AC**: APを検出したセンサーが関連付けられているACのデバイスラベル。ラベルをクリックすると、ACの詳細が表示されます。

プローブ情報レポート

このレポートには、デバイスの数量と、WLAN内のデバイスの各カテゴリの詳細が表示されます。プローブ情報レポートを表示するには、次のパラメーターを設定します。

- **Parameter "Begin Time and End Time"**: 統計情報収集の時間範囲をリストに表示されます。**Last Hour**、**Last Day**、**Last Week**、**Last Month**などの特定の時間範囲を選択するか、または**Custom Range**を選択して、開始時刻と終了時刻を手動で指定できます。
- **Location**:統計情報収集用の特定のロケーションビューを選択するか、**All AP Devices**を選択します。

- **Begin Time/End Time**: これらの2つのパラメーターは、**Custom Range**を選択した場合にのみ表示されます。
  Begin Time/End Timeの横にあるフィールドをクリックして、表示されるカレンダーから開始時間/終了時間をYYYY-MM-DD hh:mm形式で選択します。終了時間は開始時間より後である必要があります。
- **Filter MAC**: 重複デバイスをフィルタするかどうかを選択します。オプションはYesおよびNoです。**Yes**を選択すると、WSMは同じMACアドレスを持つデバイスをフィルタし、最後に検出されたデバイスのみを表示します。

Detected Device Category円グラフには、検出されたデバイスの各カテゴリの割合が表示されます。このグラフには、**Related Detection of AP Client**、**Associated With Other AP Client**、**Non Associated Clients**および**Neighbor AP**カテゴリが含まれます。

Detected Deviceリストには、各カテゴリのデバイスの合計数とその詳細が表示されます。

- **MAC Address**: デバイスのMACアドレス。
- **Category**: デバイスのタイプ。オプションには、**Related Detection of AP Clients**、**Associated With Other AP Clients**、**Non Associated Clients**、および**Neighbor AP**があります。
- **SSID**: 接続されたネットワークのSSID。関連付けられていないクライアントの場合、このフィールドは空です。
- **BSSID**: アソシエートされたAPのMACアドレス。アソシエートされていないクライアントまたはネイバーAPの場合、このフィールドは空です。
- **Channel**: デバイスの動作チャネル。
- **Detecting AP**: デバイスを検出したAPの名前。
- **Location**: 検出中のAPが存在するロケーションビューの名前。
- **RSSI**: デバイスのRSSI。
- **Noise**: 検出APによって検出されたノイズフロア。ノイズフロアはチャネル品質に影響し、温度によって変化します。
- **Encryption Method**: デバイスで使用される暗号化方式。
- **First Detection Time**: デバイスが最初に検出された時刻。
- **Last Detection Time**: デバイスが最後に検出された時刻。
- **Online Time**: デバイスの合計オンライン時間。
- **Detecting AC**: 検出中のAPが関連付けられているACの名前。

プローブ情報履歴レポート

このレポートには、WLAN内のデバイスのWLAN内の各デバイスカテゴリの詳細が表示されます。プローブ情報履歴レポートを表示するには、次のパラメーターを設定します。

- **Parameter "Begin Time and End Time"**: 統計情報収集の時間範囲をリストに表示されます。**Last Hour**、**Last Day**、**Last Week**、**Last Month**などの特定の時間範囲を選択するか、または**Custom Range**を選択して、開始時刻と終了時刻を手動で指定できます。
- **Location**: 統計情報収集用の特定のロケーションビューを選択するか、**All AP Devices**を選択します。
- **Begin Time/End Time**: これらの2つのパラメーターは、**Custom Range**を選択した場合にのみ表示されます。
  Begin Time/End Timeの横にあるフィールドをクリックして、表示されるカレンダーから開始時間/終了時間をYYYY-MM-DD hh:mm形式で選択します。終了時間は開始時間より後である必要があります。

- **Filter MAC**: 重複デバイスをフィルタするかどうかを選択します。オプションは**Yes**および**No**です。**Yes**を選択すると、WSMは同じMACアドレスを持つデバイスをフィルタし、最後に検出されたデバイスのみを表示します。

Device Category Statistics円グラフには、検出されたデバイスの各カテゴリの割合が表示されます。このグラフには、**Related Detection of AP Clients**、**Associated With Other AP Clients**、**Non Associated Clients**および**Neighbor AP**などのカテゴリが含まれます。

検出されたクライアントのトレンドラインには、指定したレポート期間中の関連付けられたクライアントと関連付けられていないクライアントの合計数の変化が折れ線グラフで表示されます。横軸の時間増分は1時間です。

Detected Deviceリストには、各カテゴリのデバイスの合計数とその詳細が表示されます。

- **MAC Address**: デバイスのMACアドレス。
- **Category**: デバイスのタイプ。オプションには、**Related Detection of AP Clients**、**Associated With Other AP Clients**、**Non Associated Clients**、および**Neighbor A**Pがあります。
- **SSID**: 接続されたネットワークのSSID。関連付けられていないクライアントの場合、このフィールドは空です。
- **BSSID**: アソシエートされたAPのMACアドレス。アソシエートされていないクライアントまたはネイバーAPの場合、このフィールドは空です。
- **Channel**: デバイスの動作チャネル。
- **Detecting AP**: デバイスを検出したAPの名前。
- **Location**: 検出中のAPが存在するロケーションビューの名前。
- **RSSI**: デバイスのRSSI。
- **Noise**: 検出APによって検出されたノイズフロア。ノイズフロアはチャネル品質に影響し、温度によって変化します。
- **Encryption Method**: デバイスで使用される暗号化方式。
- **First Detection Time**: デバイスが最初に検出された時刻。
- **Last Detection Time**: デバイスが最後に検出された時刻。
- **Online Time**: デバイスの合計オンライン時間。
- **Detecting AC**: 検出中のAPが関連付けられているACの名前

Located Client Statisticsレポート

このレポートには、ロケーションビュー別に、検出されたクライアントの統計情報が表示されます。

検出されたクライアント統計情報レポートを表示するには、次のパラメーターを設定します。

- **Parameter "Begin Time and End Time"**: 統計収集の時間範囲をリストから選択します。**Last Hour**、**Last Day**、**Last Week**または**Last Month**など特定の時間範囲を選択するか、**Custom Range**を選択して開始時間と終了時間を手動で指定できます。
- **Location**: 統計情報収集用の特定のロケーションビューを選択するか、**All AP Devices**を選択します。
- **Begin Time/End Time**: これらの2つのパラメーターは、**Custom Range**を選択した場合にのみ表示されます。
  Begin Time/End Timeの横にあるフィールドをクリックして、表示されるカレンダーから開始時間/終了時間をYYYY-MM-DD hh:mm形式で選択します。終了時間は開始時間より後である必要があります。
- **Show Sublocations**: サブロケーションビューに統計を表示するかどうかを選択します。オプションは**Yes**と**No**です。

Client Trend Graphには、指定したレポート期間中の関連付けられたクライアントおよび関連付けられて

いないクライアントの合計数の変化が線グラフで表示されます。水平軸上の時間増分は1分です。

クライアント統計リストの検索

- **Location view**: ロケーションビューの名前。
- **Associated clients**: ロケーションビュー内のアソシエートされたクライアントの数。
- **Disassociated clients**: ロケーションビュー内のアソシエーション解除されたクライアントの数。
- **Total clients**: ロケーションビュー内のクライアントの合計数。

入出庫統計レポート

このレポートには、顧客フロー統計がショップ別に表示されます。

ショップEntry/Exit統計レポートを表示するには、次のパラメーターを設定します。

- **Parameter "Begin Time and End Time"**: 統計収集の時間範囲をリストから選択します。**Last Hour**、**Last Day**、**Last Week**または**Last Month**など特定の時間範囲を選択するか、**Custom Range**を選択して開始時間と終了時間を手動で指定できます。
- **Location**: 統計情報収集用の特定のロケーションビューを選択するか、All AP Devicesを選択します。
- **Begin Time/End Time**: これらの2つのパラメーターは、**Custom Range**を選択した場合にのみ表示されます。
  Begin Time/End Timeの横にあるフィールドをクリックして、表示されるカレンダーから開始時間/終了時間をYYYY-MM-DD hh:mm形式で選択します。終了時間は開始時間より後である必要があります。
- **Shop Name**: 1つまたはすべてのショップを選択します。
- **MAC Address of Client**: クライアントのMACアドレスをhh:hh:hh:hh:hh:hh:hhの形式で入力します。このパラメーターが設定されている場合、レポートには指定したクライアントに関する統計情報だけが表示されます。

Shop Entry/Exist Count Top 10には、ショップエントリー/エグジットカウントが最も多い上位10店舗が表示されます。横軸は店舗名を表し、縦軸はショップエントリー/エグジットカウントを表します。

以下は、ショップの入口/出口統計リストです。

- **Shop Name**: ショップの名前。
- **Client MAC**: クライアントのMACアドレス。
- **Entered At**: クライアントがショップに入った時刻。
- **Left at**: クライアントが店を出た時刻。
- **Length of Stay**: クライアントがストアに滞在していた時間(秒単位)。

PCIレポート

WSMは、PCIデータセキュリティ基準に基づいてワイヤレスネットワークのセキュリティコンプライアンス情報を収集し、企業のセキュリティリスクを防止するためにPCIレポートを生成します。

PCIレポートを表示するためにパラメーターを設定する必要はありません。

PCIレポート:

- **Generated**: PCIレポートが生成された時刻。
- **Requirement**: DSS要件のシーケンス番号。ワイヤレスネットワークでは、要件のシーケンス番号は4.1.1または11.1です。
- **Description**: 要件の説明。

- **Status**: ワイヤレスネットワークのセキュリティチェックの結果が**Fail** または **Pass**になります。
- **SSID**: WLANのSSID。
- **Enable Status**: WLANがイネーブルかディセーブルかを示します。
- **Encryption Mode**: WLANの暗号化モード(**Clear**または**Crypto**)。
- **Authentication Type**: WLANのリンク認証モード(**Open System**、**Shared Key**、または**All**)。

定期レポート

スケジュール済レポートを使用すると、オペレーターは生成期間とレポートテンプレートを事前定義できます。オペレーターは、異なる期間から生成されたレポートを表示できます。WSMでは、レポートをオペレーターに電子メールで送信することもできます。

スケジュールレポートの追加

1. 次のいずれかの方法で、スケジュールレポートを追加するページを入力します。
   a. **Report**タブをクリックします。ナビゲーションツリーから、**Reports** > **Add Scheduled Report**の追加を選択してスケジュールされたレポートを追加するページを入力するか、**Scheduled Reports > All Scheduled Report**sを選択して**All Scheduled Reports**を入力します。
   b. **Add**をクリックして、スケジュール済レポートを追加するためのページを入力します。
2. テンプレートの選択:
   a. **Template Name**の右にある**Select**をクリックします。
   b. **Query Template**領域の**Type**リストから**Wireless Service Report**を選択し、**Query**をクリックします。
   c. ターゲットレポートテンプレートを選択し、**OK**をクリックします。
3. **Scheduled Report Name**フィールドにレポート名を入力します。
4. レポートを表示できるオペレーターグループを選択します。
   a. 演算子グループを選択します。

      グループ内のすべてのオペレーターがレポートを表示できます。管理者グループが強制的に選択されています。
   b. オペレーターグループ内のオペレーターを表示するには、ターゲットオペレーターグループの右にある**Operator Group Information**アイコンをクリックします。

   Operator Group Informationウィンドウが開きます。
   c. **Group Name**領域でオペレーターグループを選択します。

      演算子グループに含まれる演算子が右側に表示されます。
   d. レポートを追加するページに戻るには、**Close**をクリックします。
5. レポートを生成する期間を指定します。

スケジュールされたレポート期間は、次のスケジュールタイプと時間設定によって決まります。

- **Schedule Type**: **Daily**、**Weekly**、**Monthly**、**Quarterly**、**Half Yearly**、および**Yearly**などのフィールドがあります。
- **Report Start Dat**e: **Report Start Date**の横にあるフィールドをクリックして、表示されるカレンダーから時間を選択します(YYYY-MM-DD hh:mm形式)。
- **End By**: **End by**ボックスを選択し、終了時刻を入力するか、表示されたカレンダーから終了時刻をYYYY-MM-DD hh:mm形式で選択します。

  WSMは、指定した時刻からスケジュールされたレポートの生成を停止します。

6. レポートファイルフォーマットの設定: **Report File Format**リストからファイルフォーマットを選択します。オプションは次のとおりです。
   - **PDF**
   - **CSV**
   - **MS EXcel**
   - **MS Excel(データ専用)**
7. レポートを電子メールで送信するには(オプション)、**Send by Email**ボックスを選択し、受信者の電子メールアドレスを入力します。

   レポートを送信できる電子メールアドレスは1つだけです。
8. **Parameter Value**領域でレポートのパラメーターを指定します。

   スケジュールレポートを追加するために必要なパラメーターは、レポートテンプレートによって異なります。レポートテンプレートについては、次の情報で説明します。
9. **OK**をクリックします。

スケジュールされたレポートの表示

1. **Report**タブをクリックします。
2. ナビゲーションツリーから、**Scheduled Reports > All Scheduled Reports**を選択して**All Scheduled Reports**ページに入ります。
3. 表示するスケジュール済レポートの**History Report**アイコンをクリックします。

   History Reportページが開きます。
4. **View**リンクをクリックしてレポートを開きます。

AC統計レポート

AC統計情報レポートのフィールド:

- レポート期間:統計情報が収集される期間。
- **AC Name** :ACの名前。
- **IP Address**: ACのIPv4アドレス。
- **AP Number**: ACによって管理されているAPの合計数。
- **Online/M APs**: ACによって管理されているマスターAPの数。
- **Online/B APs**: ACによって管理されているバックアップオンラインAPの数。
- **Availability(%)**: APがACを管理していた時間の割合(%)。
- **Busy APs**: ACによって管理されているビジー状態のAPの数。APに関連付けられているクライアント番号または伝送レートが指定したしきい値に達すると、そのAPはビジー状態と見なされます。
- **Idle APs**: ACによって管理されるアイドル状態のAPの数。APは、関連付けられているクライアント番号または伝送レートが指定したしきい値以下の場合に、アイドル状態と見なされます。
- **Worst APs**: ACによって管理されるワーストAPの数。アウトオブサービスレートまたはアソシエーション輻輳レートが指定したしきい値に達すると、APはワーストと見なされます。
- **Transmitted Traffic(MB)**: ACによって送信されたトラフィックの合計。
- **Received Traffic(MB)**: ACが受信したトラフィックの合計。
- **Packet Retransmit Ratio(%)**: 送信されたパケットの総数に対する再送信されたパケットの数の割合。

- **Error Frame Ratio(%)**: ACで受信された合計フレーム数に対するエラーフレーム数の割合。
- **Max Transmit Speed (Mb/s)**: ACの最大転送速度。
- **Avg Transmit Speed (Mb/s)**: ACの平均転送速度です。
- **Max Receive Speed(Mb/s)**: ACの最大受信速度。
- **Avg Receive Speed(Mb/s)**: ACの平均受信速度。
- **Max Online Client Number**: AC上のオンラインクライアントの最大数。
- **Avg Online Client Number**: AC上のオンラインクライアントの平均数。
- AP Average Utilization(%): ACによって管理されるAP全体の平均使用率。**Avg Online Client Number/X**として計算されます(Xはコンフィギュレーションファイルで指定されているAP使用率の値)。
- **AP Peak Utilization(%)**: ACによって管理されるAP全体のピーク使用率。**Max Online Client Number/X**として計算されます(Xはコンフィギュレーションファイルで指定されたAP使用値)。
- **Total Client Online Duration**: クライアントの合計オンライン時間。
- **Avg Client Online Duration**: クライアントの平均オンライン時間。
- **Successful Accesses**: クライアントがACによって管理されているAPに正常にアソシエートした合計回数。
- **Success Rate(%)**: アクセス要求の合計数に対する成功したアクセスの割合。
- **Association Congestion Rate(%)** :ACのクライアントアソシエーションの輻輳率。アソシエーション要求の総数に対するアソシエーションの失敗数の比率です。
- **Client Dropping Rate(%)**: ACのクライアントドロップレート。これは、オンラインクライアントの合計数に対するクライアントの異常ログアウトの割合です。

APアソシエーションサマリーレポート

このレポートには、すべてのAPまたはロケーションビュー内のAPのクライアントアソシエーション統計情報のサマリーが表示されます。ロケーションビューにサブロケーションがある場合、レポートには、ロケーションビューとそのサブロケーションのクライアントアソシエーション統計情報のサマリーと上位10位までも表示されます。

APアソシエーションサマリーレポートのパラメーター:

- **Report Period**: 統計情報が収集される期間。
- **Location**: 統計情報が収集されるロケーションビューの名前、または**All AP Devices**

AP association summary reportフィールド:

- **Location**: ロケーションビュー名または**All AP Devices**。
- **AP Number**: ロケーションビューに含まれているAPの数、またはすべてのAPの合計数。
- **Access Requests**: クライアントアクセス要求の合計数。
- **Access Responses**: APから要求元クライアントに送信された応答の合計数。
- **Successful Accesses**:クライアントがAPに正常にアソシエートした合計回数。
- **Abnormal Logouts**: APに関連付けられているクライアントが異常ログアウトした合計回数。
- **Client Dropping Rate(%)**: APのクライアントドロップレート。これは、オンラインクライアントの総数に対するクライアントの異常なログアウトの割合です。
- **Success Rate(%)**: APのクライアントアクセス成功率。これは、アクセス要求の総数に対する成功したアクセスの割合です。
- **Association Congestion Rate(%)**: APのクライアントアソシエーションの輻輳率。アソシエー

ション要求の総数に対するアソシエーション失敗の割合です。

APアソシエーション詳細レポート

このレポートには、個々のAPの詳細なクライアントアソシエーション統計情報が表示されます。このレポートを使用すると、ユーザーは個々のAPのアクセス品質と所属するロケーションビューを確認できます。

APアソシエーション詳細レポートのパラメーター:

- **Report Period**: 統計情報が収集される期間。
- **Location**: 統計情報が収集されるロケーションビューの名前または**All AP Devices**

AP association detail reportの各フィールド

- **AP Name**: アクセスポイントの名前。
- **Location**: APが属するロケーションビュー。
- **Access Requests**: APが受信したクライアントアクセス要求の合計数。
- **Access Responses**: APが要求元クライアントに送信した応答の合計数。
- **Successful Accesses**: クライアントがAPに正常にアソシエートした合計回数。
- **Abnormal Logouts**: APに関連付けられているクライアントが異常ログアウトした合計回数。
- **Client Dropping Rate(%)**: APのクライアントドロップレート。これは、APに関連付けられているクライアントの合計数に対する異常ログアウトの割合です。
- **Success Rate(%)**: APのクライアントアソシエーションの成功率。これは、アクセス要求の総数に対する成功したアクセスの割合です。
- **Association Congestion Rate(%)**: APのクライアントアソシエーションの輻輳率。アソシエーション要求の総数に対するアソシエーションの失敗数の比率です。

AP可用性概要レポート

このレポートには、すべてのAPまたはロケーションビュー内のAPの可用性統計のサマリーが表示されます。ロケーションビューにサブロケーションがある場合、レポートには、ロケーションビューおよびそのサブロケーションの可用性統計のサマリーと上位10位までも表示されます。

AP可用性概要レポートのパラメーター:

- **Report Period**: 統計情報が収集される期間。
- **Location**: 統計情報が収集されるロケーションビューの名前または**All AP Devices**.

AP Availability Summaryレポートのフィールド:

- **Availability Highest Top 10**: 可用性が最も高い上位10位のロケーションビューを棒グラフで表示します。
- **Availability Lowest Top 10**: 最下位可用性が最も低い上位10位のロケーションビューを棒グラフで表示します。
- **Location** :ロケーションビュー名またはAll AP Devices。
- **AP Number**: APの合計数。
- **Total Unavailable Time**: APの合計使用不能時間。
- **Total Available Time**: APの合計使用可能時間。
- **Availability**: APが使用可能な時間の割合。

AP可用性詳細レポート

このレポートには、個々のAPの詳細な可用性統計情報が表示されます。

AP可用性詳細レポートのフィールドは次のとおりです。

- **Report Period**: 統計情報が収集される期間。
- **Location**: 統計情報が収集されるロケーションビューの名前または**All AP Devices**。
- **AP Name**: アクセスポイントの名前。
- **AP Location**: APが属するロケーションビュー。
- **IP Address**: APのIPv4アドレス。
- Model: APモデル。
- **Available Tim**e: APが使用可能な合計時間。
- **Unavailable Time**: APが使用できない合計時間。
- **Availability**: APが使用可能な時間の割合。

APトラフィック要約レポート

このレポートには、すべてのAPまたはロケーションビュー内のAPのサマリートラフィック統計が表示されます。ロケーションビューにサブロケーションがある場合、レポートには、サブロケーションのサマリートラフィック統計と、有線/無線トラフィックボリュームが最も大きい上位10のロケーションビューも表示されます。これらの統計は、将来のスケーラビリティニーズに対するキャパシティプランニングに役立ちます。

AP Traffic Summaryレポートのパラメーター:

- **Report Period**: 統計情報が収集される期間。
- **Position**: 統計情報が収集されるロケーションビューの名前、または**All AP Device**

AP traffic summary reportフィールド:

- **Core Traffic Top 10**: 有線トラフィックが最も高い上位10のロケーションビューを表示します。棒グラフのボリューム。
- **Radio Traffic Top 10**: 無線トラフィック量が最も多い上位10位のロケーションビューを棒グラフで表示します。
- **Location**: ロケーションビュー名またはAll AP Devices。
- **AP Number**: ロケーションビューに含まれているAPの数、またはすべてのAPの合計数。
- **Core Frames Reception**: APが有線ネットワークから受信したフレームの合計数。
- **Core Errors Reception**: APが有線ネットワークから受信したエラーパケットの合計数。
- **Core Traffic Reception(MB**): APが有線ネットワークから受信したトラフィックの合計。
- **Core Traffic Transmission(MB)**: APから有線ネットワークに送信されたトラフィックの合計。
- **Radio Frames Reception**: APが無線ネットワークから受信したフレームの合計数。
- **Radio Errors Reception**: APが無線ネットワークから受信したエラーパケットの合計数。
- **Radio Traffic Reception(MB)**: 無線ネットワークからAPが受信したトラフィックの合計。
- **Radio Traffic Transmission(MB)**: APからワイヤレスネットワークに送信されたトラフィックの合計。

APトラフィック詳細レポート

このレポートには、個々のAPと、有線および無線トラフィック量が最も多い上位10のAPのトラフィック統計情報が表示されます。これらの統計情報は、将来のスケーラビリティのニーズに対応するキャパシティプランニングに役立ちます。

APトラフィック詳細レポートのパラメーター:

- **Report Period**: 統計情報が収集される期間。
- **Location**: 統計情報が収集されるロケーションビューの名前、または**All AP Devices**

AP traffic detail reportフィールド:

- **Core Traffic Top 10**: 有線トラフィック量が最も多い上位10のAPをバーで表示します。
グラフ
- **Core Traffic Top 10**: ワイヤレストラフィック量が最も多い上位10のAPを棒グラフで表示します。
- **AP Name**: アクセスポイントの名前。
- **Location**: APが属するロケーションビュー。
- **IP Address**: APのIPv4アドレス。
- **Core Frames Reception**: APが有線ネットワークから受信したフレームの総数。
- **Core Errors Reception**: APが有線ネットワークから受信したエラーパケットの合計数。
- **Core Bytes Re**: APが有線ネットワークから受信したバイト数の合計。
- **Core Bytes Transmission**: APから有線ネットワークに送信された合計バイト数。
- **Radio Frames Reception**: APが無線ネットワークから受信したフレームの総数。
- **Radio Errors Reception**: APが無線ネットワークから受信したエラーパケットの総数。
- **Radio Bytes Reception**: APが無線ネットワークから受信した総バイト数。
- **Radio Bytes Transmission**: APから無線ネットワークに送信された総バイト数。

AP速度レポート

このレポートには、個々のAPのデータ送受信速度が表示されます。また、特定の期間におけるすべてのAPの集約データを使用して、データ送受信速度の全体的な傾向が折れ線グラフで示されます。

AP速度レポートのパラメーター:

- **Report Period**: 統計情報が収集される期間。
- **Location**: 統計情報が収集されるロケーションビューの名前または**All AP Devices**

AP速度レポートのフィールド:

- **Trend graph**: 指定したレポート期間における全APの**Reception Speed**, **Transmission Speed**、**Total Speed**の変化を折れ線グラフで表示します。トレンドグラフの上段には、全APの受信速度、送信速度、合計速度の最大値と平均値が表示されます。
- **AP Name**: アクセスポイントの名前。
- **Location**: APが属するロケーションビュー。
- **Max Reception Speed**: APの最大受信速度。
- **Avg Reception Speed**: APの平均受信速度。
- **Max Transmission Speed**: APの最大伝送速度。
- **Avg Transmission Speed**: APの平均伝送速度。
- **Max Total Speed**: APの最大合計速度。
- **Avg Total Speed**: APの平均合計速度。

APログオフ要約レポート

このレポートには、すべてのAPまたはロケーションビュー内のAPの要約ログオフ統計が表示されます。ロケーションビューにサブロケーションがある場合、レポートには、ロケーションビューとそのサブロケーション

の要約および上位10のログオフ統計も表示されます。

APログオフ要約レポートのパラメーター:

- **Report Period**: 統計情報が収集される期間。
- **Location**: 統計情報が収集されるロケーションビューの名前、または**All AP Devices**

AP offline summary reportフィールド:

- **Offline Count Top 10**: APオフライン数が最も多い上位10のロケーションビューを表示します。
- **Count of Offline(Duration>=1 Hour)Top 10**: 期間が0時間に達するAPオフライン数が最も多い上位10のロケーションビューを表示します。ここで、0は指定した**Logoff Time**です。
- **Position**: ロケーションビュー名または**All AP Devices**。
- **AP Number**: ロケーションビューに含まれているAPの数、またはすべてのAPの合計数。
- **Total Offline Count**: ロケーションビューに含まれるAPまたはすべてのAPのオフラインカウントの合計。
- **Count of Offline(Duration>=1 Hour)**: APのオフライン期間が0時間に達した合計回数。1は指定した**Logoff Time**です。
- **Total Offline Duration**: ロケーションビューに含まれるAPまたはすべてのAPの合計オフライン時間。

APログオフ詳細レポート

このレポートには、指定した問合せ基準に基づいた詳細なAPログオフ統計が表示されます。

APログオフ詳細レポートのフィールドは次のとおりです。

- **Report Period**: 統計情報が収集される期間。
- **Location**: 統計情報が収集されるロケーションビューの名前または**All AP Devices**。
- **AP Name**: アクセスポイントの名前。
- **Location**: APが属するロケーションビュー。
- **IP Address**: APのIPv4アドレス。
- **Model**: APモデル。
- **Logoff Time**: APがログオフした時刻。
- **Recovery Time**: APが回復した時間。
- **Logoff Duration**: APのログオフ期間。

無線エラーレポート

このレポートには、AP無線で受信されたエラーフレームの数が表示されます。

無線エラーレポートのフィールド:

- **Report Period**: 統計情報が収集される期間。
- **Location**: 統計情報が収集されるロケーションビューの名前または**All AP Devices**。
- **AP Name**: アクセスポイントの名前。
- **Radio ID** :無線ID。
- **AP Location**: APが属するロケーションビュー。
- **FCS Error Frames**: AP無線が受信したFCSエラーフレームの数。

- **PHY Error Frames**: AP無線が受信したPHYエラーフレームの数。
- **MIC Error Frames**: AP無線が受信したMICエラーフレームの数。
- **Error Ratio**: AP無線で受信された合計フレーム数に対する、FCS、PHY、およびMICエラーフレームの合計数の比率。

ラジオトラフィックレポート

このレポートには、AP無線のトラフィック統計情報が表示されます。

無線トラフィックレポートのフィールド:

- **Report Period**: 統計情報が収集される期間。
- **Location**: 統計情報が収集されるロケーションビューの名前または**All AP Devices**。
- **AP Name**: アクセスポイントの名前。
- **Radio ID** :無線のID。
- **AP Location**: APが属するロケーションビュー。
- **Reception(bytes)**: AP無線が受信した合計トラフィック。
- **Transmission(bytes)**: AP無線によって送信された合計トラフィック(バイト単位)。
- **Total Traffic(bytes)**: AP無線で送受信されたトラフィックの合計。

無線速度レポート

このレポートには、AP無線の最大および平均の受信速度と送信速度が表示されます。

無線速度レポートのフィールド:

- **Report Period**: 統計情報が収集される期間。
- **Location**: 統計情報が収集されるロケーションビューの名前または**All AP Devices**。
- **AP Name**: アクセスポイントの名前。
- **Radio ID**: 無線のID。
- **AP Location**: APが属するロケーションビュー。
- **Max Reception Speed(bits/s)**: 無線の最大受信速度。
- **Average Reception Speed (bits/s)**: 無線の平均受信速度。
- **Max Transmission Speed(bits/s)**: 無線の最大伝送速度。
- **Avg Transmission Speed(bits/s)**: 無線の平均伝送速度。

無線リソース使用状況レポート

このレポートには、AP無線のリソース使用状況統計が表示されます。

無線リソース使用状況レポートのフィールドは次のとおりです。

- **Report Period**: 統計情報が収集される期間。
- **Location**: 統計情報が収集されるロケーションビューの名前または**All AP Device**s。
- **AP Name**: アクセスポイントの名前。
- **Radio ID**: 無線のID。

- **AP Location**: APが属するロケーションビュー。
- **IP Address**: APのIPv4アドレス。
- **Model**: APモデル。
- **Usage**: 無線の使用率。

Rogue AP履歴レポート

このレポートには、検出された不正なAPの履歴レコードがMACアドレス別に表示されます。

Rogue AP historyレポートのフィールドは次のとおりです。

- **Report Period**: 統計情報が収集される期間。
- **MAC Address**: 不正APのMACアドレス。
- **Vendor**: 不正なAPのベンダー。
- **SSID**: 不正なAPのSSID。
- **Max Signal Strength**: 不正APの最大信号強度。
- **Channel**: 不正APで使用されているチャネル。
- **Detected by**: 不正なAPを検出したAC。
- **Detected AP** :不正なAPを検出したFit AP。
- **Last Discovered Time**: 不正なAPが最後に検出された時刻。
- **Status**: 不正なAPの状態(**Attacked**または**Not Attacked**)。

Rogue APレポート

このレポートには、新たに検出されたすべての不正APがMACアドレス別に表示されます。

Rogue APレポートのフィールドは次のとおりです。

- **MAC Address**: 不正APのMACアドレス。
- **Vendor:** 不正なAPのベンダー。
- **SSID**: 不正なAPのSSID。
- **Max Signal Strength**: 不正APの最大信号強度。
- **Channel**: 不正APで使用されているチャネル。
- **Detected by**: 不正なAPを検出したAC。
- **Last Discovered Time**: 不正なAPが最後に検出された時刻。
- **Attacked Status**: 不正なAPの状態(AttackedまたはNot Attacked)。

Rogue Client Historyレポート

このレポートには、ネットワーク上で検出された不正なクライアントの履歴レコードがクライアントMACアドレス別に表示されます。

Rogue Client Historyレポートのフィールド:

- レポート期間:統計情報が収集される期間。
- **MAC Address**: 不正クライアントのMACアドレス。
- **Vendor**: 不正クライアントのベンダー。

- **Max Signal Strength**: 不正なクライアントの最大信号強度。
- **Channel**: 不正なクライアントが使用するチャネル。
- **Detected by**: 不正なクライアントを検出した
- **Detected AP**:不正なクライアントを検出したAPを適合させます。
- **Last Discovered Time**:不正クライアントが最後に検出された時刻。
- **Status**:不正クライアントの状態(**Attacked**または**Not Attacked**)。

不正クライアントレポート

このレポートには、初めて検出されたすべての新しい不正クライアントがMACアドレス別に表示されます。Rogue Clientレポートのフィールドは次のとおりです。

- **MAC Address**: 不正クライアントのMACアドレス。
- **Vendor**: 不正クライアントのベンダー。
- **Max Signal Strength**: 不正なクライアントの最大信号強度。
- **Channel**: 不正なクライアントが使用するチャネル。
- **Detected by**: 不正なクライアントを検出したAC。
- **Last Discovered Time**:不正クライアントが最後に検出された時刻。
- **Attacked Status**:不正クライアントの攻撃状態(AttackedまたはNot Attacked)。

現在関連付けられているクライアント統計レポート

このレポートには、現在アソシエートされているクライアントに関する情報が、MACアドレス別、およびアソシエート期間が最も長い上位10クライアント別に表示されます。

現在関連付けられているクライアント統計レポートのフィールド:

- **Position**: 統計情報が収集されるロケーションビューの名前または**All AP Devices**。
- **Associated Duration Top 10**: クライアントMACアドレス別に、関連付けられている期間が最も長い上位10クライアントを表示します。
- **MAC Address**: 関連付けられたクライアントのMACアドレス。
- **Client Name**: 関連付けられたクライアントの名前。
- **IP Address**: 関連付けられたクライアントのIPアドレス。
- **SSID**: 関連付けられたクライアントによって使用されるSSID。
- **Channel**: 関連付けられたクライアントによって使用されるチャネル。
- **AP Name**: クライアントがアソシエートされているアクセスポイントの名前。
- **AP Position**: APが属するロケーションビュー。
- **Session Duration**: クライアントに関連付けられている現在の継続時間。
- **Received Traffic(MB)**: 関連付けられたクライアントが受信したトラフィックの合計。
- **Sent Traffic(MB)**: 関連付けられたクライアントによって送信されたトラフィックの合計。
- **Total Traffic(MB)**: 関連付けられたクライアントが送受信したトラフィックの合計。

AP別のホットスポット統計レポート

このレポートには、ホットスポットとして設定されているロケーションに含まれるAPに関する統計情報が表示されます。ロケーションにサブロケーションがある場合は、ホットスポットとして設定されているサブロケーショ

ンのAP統計情報も表示されます。

APフィールド別のホットスポット統計レポート:

- **Location**: 統計情報が収集されるロケーションビューの名前または**All AP Devices**。
- **Myltest**: ホットスポットとして設定されているロケーションビューの名前。**myltest**は、このラボ環境で使用されるホットスポットロケーションビューの名前です。実際のロケーションビューの名前は、特定のネットワーク環境に依存します。ホットスポットロケーションビューが使用できない場合、このフィールドは空です。
- **test**: ホットスポットとして設定されているロケーションビューの名前。**test**は、このラボ環境で使用されるホットスポットロケーションビューの名前です。実際のロケーションビューの名前は、特定のネットワーク環境によって異なります。ホットスポットロケーションビューが使用できない場合、このフィールドは空です。
- **AP Numbe**r: ホットスポットロケーションビューに含まれるAPの数。
- **Online AP Number**: ホットスポット位置ビューに含まれるオンラインAPの数。
- **AP Name**: ホットスポットロケーションビューに含まれるアクセスポイントの名前。
- **Status**: APの状態(**Online**または**Offline**)。
- **Serial ID**: APのシリアルID。
- **Model**: APのモデル。

ワイヤレス資産統計レポート

このレポートには、WSM内の管理対象ワイヤレスデバイスに関する資産情報が円グラフで表示されます。

円グラフには、デバイスカテゴリ別の資産の数と、合計に対する各デバイスカテゴリの貢献度が表示されます。特定の資産カテゴリのデバイスリストを表示するには、グラフ上で対応するスライスをクリックします。

クライアント要約レポート

このレポートには、クライアントに関連付けられている時間と期間がMACアドレス別に表示されます。また、関連付けられている期間の合計が最も長い上位10クライアントが棒グラフで表示されます。

クライアント要約レポートのパラメーター:

- **Report Period**: 統計情報が収集される期間。
- **Position**: 統計情報が収集されるロケーションビューの名前または**All AP Devices**。

クライアント要約レポートのフィールド:

- **Total Associated Duration Top 10**: 最も長く関連付けられている上位10クライアントを表示します。
  継続時間
- **MAC Address**: クライアントのMACアドレス。
- **Client Name**: クライアントの名前。
- **Online Times**: クライアントがオンライン接続を開始した合計回数。
- **Total Associated Duration**: クライアントに関連付けられた合計期間。
- **Total Associated Duration**: クライアントに関連付けられている平均期間。
- **Received Traffic(MB)**: クライアントが受信したトラフィックの合計。
- **Sent Traffic(MB)**: クライアントによって送信されたトラフィックの合計。
- **Total Traffic(MB)**: クライアントが送受信したトラフィックの合計。

クライアント詳細レポート

このレポートには、クライアントの詳細なアソシエーションレコードがMACアドレス別

に表示されます。クライアント詳細レポートのフィールドは次のとおりです:

- **Report Period**: 統計情報が収集される期間。
- **Position**: 統計情報が収集されるロケーションビューの名前または**All AP Devices**。
- **MAC Address**: クライアントのMACアドレス。
- **Client Name**: クライアントの名前。
- **IP Address**: クライアントのIPv4アドレス。
- **Radio Type**: 無線のタイプ。
- **SSID**: クライアントが使用するSSID。
- **AP Name**: クライアントがアソシエートされているアクセスポイントの名前。
- **Position**: APが属するロケーションビュー。
- **Online Time**: クライアントがオンライン接続を開始した時刻。
- **Session Duration**: クライアントのセッション期間。
- **Received Traffic(MB)**: クライアントが受信したトラフィックの合計。
- **Sent Traffic(MB)**: クライアントによって送信されたトラフィックの合計。
- **Total Traffic(MB)**: クライアントが送受信したトラフィックの合計。

顧客番号トレンドラインレポート

このレポートでは、すべてのAPまたはロケーションビュー内のAPに関するクライアントアソシエーション統計情報の概要と詳細の両方が提供されます。このレポートでは、すべてのAPの集約データに基づいて、関連付けられたクライアント番号の全体的な変化傾向が表示され、個々のAPに関する詳細な統計情報が提供されます。

クライアント番号の近似曲線レポートのパラメーター:

- **Report Period**: 統計情報が収集される期間。
- **Location**: 統計情報が収集されるロケーションビューの名前または**All AP Devices**。

クライアント番号の近似曲線レポートのフィールド:

- **Global Statistics**: すべてに関連付けられているクライアントの合計数の変化を表示します。グラフの左上にある**Max online client number**と**Avg online client number**は、すべてのAPに関連付けられているクライアントの最大数と平均数を示します。
- **AP Name**: アクセスポイントの名前。
- **Location**: APが属するロケーションビュー。
- **Max Online Client Number**: APにアソシエートされているクライアントの最大数。
- **Avg Online Client Numbe**r: APにアソシエートされているクライアントの平均数。
- **Total Client Associated Duration**: クライアントに関連付けられた合計期間。
- **Avg Client Associated Duration**: クライアントに関連付けられている平均継続時間。
- **AP Peak Utilization(%)**: APのピーク使用率。Max Online Client Number/Xとして計算されます。Xは、コンフィギュレーションファイルで指定されているAP使用値です。
- **AP Average Utilization(%)**: APの平均使用率。Avg Online Client Number/Xとして計算されます。Xは、コンフィギュレーションファイルで指定されているAP使用率の値です。

Busy AP統計情報レポート

このレポートには、APのピークオンラインクライアント数、ピーク伝送レート、アウトオブサービスレート、アソシエーション輻輳レート、およびクライアントドロップレートなど、総使用量が最も高いAPに関する統計情報が表示されます。

Busy AP統計情報レポートのフィールド:

- **Report Period**: 情報が収集される期間。
- **Location**: 統計情報が収集されるロケーションビューの名前または**All AP Devices**。
- **AP Name**: アクセスポイントの名前。
- **AP Location**: APが属するロケーションビュー。
- **Peak Number of Online Clients**: APにアソシエートされているクライアントの最大数。
- **Peak Transmission Rate(Mb/s)**: APの最大伝送レート。
- **Out of Service Rate(%)**: APが使用できない時間の割合。
- **Association Congestion Rate(%)**: APのアソシエーション輻輳率。アソシエーション要求の総数に対するクライアントアソシエーションの失敗数の比率です。
- **Client Dropping Rate(%)**: APのクライアントドロップレート。これは、APに関連付けられているクライアントの合計数に対する異常なログオフの比率です。

アイドルAP統計情報レポート

このレポートには、総使用量が最も低いAPに関する統計情報が表示されます。統計情報には、APのピークオンラインクライアント数、ピーク伝送レート、アウトオブサービスレート、アソシエーション輻輳レート、およびクライアントドロップレートが含まれます。

アイドルAP統計情報レポートのフィールド:

- **Report Period**: 統計情報が収集される期間。
- **Location**: 統計情報が収集されるロケーションビューの名前または**All AP Devices**。
- **AP Name**: アクセスポイントの名前。
- **AP Location**: APが属するロケーションビュー。
- **Peak Number of Online Clients**: APにアソシエートされているクライアントの最大数。
- **Peak Transmission Rate(Mb/s)**:A Pの最大伝送レート。
- **Out of Service Rate(%)**: APが使用できない時間の割合。
- **Association Congestion Rate(%)**: APのアソシエーション輻輳率。アソシエーション要求の総数に対するクライアントアソシエーションの失敗数の比率です。
- **Client Dropping Rate(%)**: APのクライアントドロップレート。これは、APに関連付けられているクライアントの合計数に対する異常なログオフの比率です。

ワーストAP統計レポート

このレポートには、ピークオンラインクライアント数、ピーク伝送レート、アウトオブサービスレート、アソシエーション輻輳レート、およびクライアントドロップレートなど、最悪のAPに関する統計情報が表示されます。

Worst AP statisticsレポートのフィールド:

- **Report Period**: 統計情報が収集される期間。
- **Position**: ロケーションビュー名または**All AP Devices**。
- **AP Name**: アクセスポイントの名前。

- **AP Location**: APが属するロケーションビュー。
- **Peak Number of Online Clients**: APにアソシエートされているクライアントの最大数。
- **Peak Transmission Rate(Mb/s)**: APの最大伝送レート。
- **Out of Service Rate(%)**: APが使用できない時間の割合。
- **Association Congestion Rate(%)**: APのアソシエーション輻輳率。アソシエーション要求の総数に対するクライアントアソシエーションの失敗数の比率です。
- **Client Dropping Rate(%)**: APのクライアントドロップレート。これは、APに関連付けられているクライアントの合計数に対する異常なログオフの比率です。

AP統計レポート

AP統計情報レポートのフィールド:

- **Report Period**: 統計情報が収集される期間。
- **Location**: 統計情報が収集されるロケーションビューの名前またはAll AP Devices。
- **AP Name**: アクセスポイントの名前。
- **Location**: APが属するロケーションビュー。
- **Availability(%)**: APが使用可能な時間の割合。
- **Transmitted Core Traffic(MB)**: APから有線ネットワークに送信されたトラフィックの合計。
- **Received Core Traffic(MB)**: APが有線ネットワークから受信したトラフィックの合計。
- **Transmitted Radio Traffic(MB)**: APからワイヤレスネットワークに送信されたトラフィックの合計。
- **Received Radio Traffic(MB)**: APがワイヤレスネットワークから受信したトラフィックの合計。
- **Packet Retransmit Ratio(%)**: APによって送信された合計パケット数に対する再送信されたパケットの割合。
- **Error Frame Ratio(%)**: APで受信された合計フレーム数に対するエラーフレームの割合。
- **Max Transmit Speed(Mb/s)**: APの最大送信速度。
- **Avg Transmit Speed(Mb/s)**: APの平均伝送速度。
- **Max Receive Speed(Mb/s)**: APの最大受信速度。
- **Avg Receive Speed(Mb/s)**: APの平均受信速度。
- **Max Online Client Number**: APにアソシエートされているクライアントの最大数。
- **Avg Online Client Number**: APにアソシエートされているクライアントの平均数。
- **AP Average Utilization(%)**:APの平均使用率。Avg Online Client Number/Xとして計算されます。Xは、コンフィギュレーションファイルで指定されているAP使用率の値です。
- **AP Peak Utilization(%)**: APのピーク使用率。Max Online Client Number/Xとして計算されます。Xは、コンフィギュレーションファイルで指定されているAP使用値です。
- **Total Client Online Duration**: APに関連付けられているクライアントの合計オンライン時間。
- **Avg Client Online Duration**: APに関連付けられているクライアントの平均オンライン時間。
- **Successful Accesses**: クライアントがAPに正常にアソシエートした合計回数。
- **Success Rate(%)**: APのクライアントアクセス成功率。これは、クライアントによって行われたアクセス要求の総数に対する、成功したアクセスの割合です。
- **Association Congestion Rate(%)**: APのクライアントアソシエーションの輻輳率。クライアントアソシエーション要求の総数に対するアソシエーションの失敗数の比率です。
- **Client Dropping Rate(%)**: APのクライアントドロップレート。これは、APに関連付けられているオンラインクライアントの総数に対する異常なログオフの割合です。

SSID別オンラインクライアント数統計情報レポート

このレポートには、SSID別の最大オンラインクライアント数と平均オンラインクライアント数が表示されます。

SSIDオンラインクライアント番号統計レポートを表示するには、**parameter configuration icon** をクリックして開始/終了時間を指定します。終了時間は開始時間より後である必要があります。

SSIDオンラインクライアント番号統計情報レポートのフィールド:

- **Report Period**: 統計情報が収集される期間。
- **SSID**: Service Set Identifier。
- **Max Online Client Number**: SSIDを使用するAPにアソシエートされているクライアントの最大数。
- **Avg Online Client Number**: SSIDを使用するAPにアソシエートされているクライアントの平均数。

SSID統計情報レポート

このレポートには、SSID別のAPトラフィックおよびオンラインクライアント統計情報のサマ

リーが表示されます。SSID統計情報レポートのフィールド:

- **Report Period**: 統計情報が収集される期間。
- **Location**: 統計情報が収集されるロケーションビューの名前または**All AP Devices**。
- **SSID**: Service Set Identifier(。
- **Transmitted Radio Traffic(MB)**: SSIDを使用するAPによって送信されたトラフィックの合計。
- **Received Radio Traffic(MB)**: SSIDを使用するAPが受信したトラフィックの合計。
- **Max Online Client Number**: SSIDを使用するAPにアソシエートされているクライアントの最大数。
- **Avg Online Client Number**: SSIDを使用するAPにアソシエートされているクライアントの平均数。
- **Availability(%)**: SSIDを使用するAPが使用可能な時間の割合。

ホットスポット別のホットスポット統計レポート

このレポートには、ホットスポットとして設定されているロケーションビ

ューが表示されます。ホットスポット統計レポートは、ホットスポットフ

ィールド別に次のように表示されます。

- **Report Period**:統計情報が収集される期間。
- **Location** :統計情報が収集されるロケーションビューの名前または**All AP Devices**。
- **Hotspot Name**: ホットスポットとして設定されているロケーションビューの名前。
- **AP Number**: ホットスポットロケーションビューに含まれるAPの数。
- オンラインAP数: ホットスポット位置ビューに含まれるオンラインAPの数。
- **Availability(%)**: APが使用可能な時間の割合。
- **Busy APs**: ホットスポットの位置ビューに表示されるビジー状態のAPの数。オンラインクライアントのピーク数またはピーク伝送速度が指定したしきい値に達すると、APはビジー状態と見なされます。
- **Idle APs**: ホットスポットロケーションビュー内のアイドル状態のAPの数。オンラインクライアント

のピーク数またはピーク伝送レートが指定したしきい値を下回ると、APはアイドル状態とみなされます。これらのしきい値の構成の詳細は、「アイドル状態のAP統計レポート」を参照してください。

- **Worst APs**: ホットスポットロケーションビュー内の最悪のAPの数。アウトオブサービスレートまたはアソシエーション輻輳レートが指定したしきい値に達すると、APは最悪と見なされます。
- **Transmitted Traffic(MB)**: ホットスポットロケーションビューでAPが送信したトラフィックの合計。
- **Received Traffic(MB)**: ホットスポットロケーションビューでAPが受信したトラフィックの合計。
- **Packet Retransmit Ratio(%)**: ホットスポットロケーションビューでAPによって送信された合計パケット数に対する、再送信されたパケット数の割合。
- **Error Frame Ratio(%)**: ホットスポットロケーションビューでAPが受信した合計フレーム数に対するエラーフレーム数の割合。
- **Max Transmit Speed(Mb/s)**: ホットスポットロケーションビューでのAPの最大伝送速度。
- **Avg Transmit Speed(Mb/s)**: ホットスポットロケーションビューでのAPの平均伝送速度。
- **Max Receive Speed(Mb/s)**: ホットスポットロケーションビューでのAPの最大受信速度。
- **Avg Receive Speed(Mb/s)**: ホットスポットロケーションビューでのAPの平均受信速度。
- **Max Online Client Number**: ホットスポットロケーションビュー内のオンラインクライアントの最大数。
- **Avg Online Client Number**: ホットスポットロケーションビュー内のオンラインクライアントの平均数。
- **AP Average Utilization(%)**: APの平均使用率。Avg Online Client Number/Xとして計算されます。Xはコンフィギュレーションファイルで指定されているAP使用率の値です。
- **AP Peak Utilization(%)**: APのピーク使用率。Max Online Client Number/Xとして計算されます。Xは、コンフィギュレーションファイルで指定されているAP使用値です。
- **Total Client Online Duration**: クライアントの合計オンライン時間。
- **Avg Client Online Duration**: クライアントの平均オンライン時間。
- **Successful Accesse**s: クライアントがホットスポットロケーションビューに含まれるAPに正常にアソシエートした合計回数。
- **Success Rate(%)**: クライアントによって実行されたアクセス要求の総数に対する、成功したアクセスの割合。
- **Association Congestion Rate(%)**: アソシエーション要求の総数に対するクライアントアソシエーションの失敗数の割合。
- **Client Dropping Rate(%)**: オンラインクライアントの総数に対するクライアントの異常なログアウトの割合。

サイトアクセスポイントとネイバーレポート

このレポートには、すべてのAPまたはロケーションビュー内のAPのネイバー統計情

報が表示されます。サイトアクセスポイントおよびネイバーレポートフィールド:

- **Location**: 統計情報が収集されるロケーションビューの名前または**All AP Devices**。
- **Radio BSSID**: 検出されたネイバーAPの無線BSSID。
- **SSID**: 検出されたネイバーAPのSSID。
- **Wireless Mode**: 検出されたネイバーAPのワイヤレスモード。
- **Channel**: 検出されたネイバーAPのチャネル。
- **SNR(dB)**: 検出されたネイバーAPのSignal-to-Noise Ratio(SNR;信号対雑音比)。
- **Signal(dBm)**: 検出されたネイバーAPの信号強度。
- **Noise(dBm)**:検出されたネイバーAPのノイズレベル。

- **Detected By**: ネイバーAPが検出されたアクセスポイントの名前。

APチャネル品質統計情報レポート

APチャネル品質統計情報レポート:

- **Report Period**:統計情報が収集される期間。
- **Location**: 統計情報が収集されるロケーションビューの名前またはAll AP Devices。
- **AP Name**: アクセスポイントの名前。
- **AP Location**: APが属するロケーションビュー。
- **Radio ID**: 無線ID。
- **Monitored Channel**: APで使用されているチャネル。
- **Average Quality**: 平均品質平均チャネル品質。高い値はチャネルの通信品質が高いことを示し、その逆も同様です。

検出されたAPレポート

このレポートには、WLANで検出されたAPの各カテゴリの数量と詳細が表示されます。検出されたAPレポートを表示するためにパラメーターを設定する必要はありません。

Detected AP Category円グラフには、検出されたAPの各カテゴリの割合が表示されます。このグラフには、次のAPカテゴリが含まれる場合があります。

- **Authorized APs**: WLANで許可されているAPの合計数。
- **Misconfigured APs**: WLANサービスの設定が正しくなく、WLANで許可されているAPの総数。
- **Rogue APs**: WLANで使用できないAPの合計数。
- **External APs**: 隣接WLAN内にあるAPの合計数。
- **Ad Hoc APs**: アドホックモードで動作しているAPの合計数。
- **Potential-Authorized Aps**: 許可される可能性のあるAPの合計数。
- **Potential-Rogue Aps**: 不正デバイスである可能性があるAPの合計数。
- **Potential-External Aps**: 外部ネットワークからの可能性があるAPの合計数。
- **Uncategorized APs**: カテゴリを判別できないAPの合計数。検出されたAPリストには、各カテゴリのAPの合計数とその詳細が表示されます。

- **Status** :APの状態(OnlineまたはOffline)。
- **BSSID**: APのBSSID(MACアドレス)。
- **SSID**: APで使用されるSSID。
- **Virtual Security Domain**: APを検出したセンサーが属する仮想セキュリティドメイン。
- **Category**: APのカテゴリ。オプションは、Authorized、Rogue、Ad hoc、Misconfigured、External、Potential-Authorized、Potential-Rogue、Potential-External、およびUncategorizedです。
- **Threat Level**: APの脅威レベル。
- **Detecting AC**: APを検出したセンサーがアソシエートされているACのデバイスラベル。
- **Device Vendor**: 検出されたAPのベンダー。センサーがAPに関するベンダー情報を取得しない場合、このフィールドにはnullが表示されます。
- **First Detection**: APが最初に検出された時刻。

- **Last Detection**: APが最後に検出された時刻。
- **Trust**: APが信頼できるデバイスリストにあるかどうか。オプションはYesおよびNoです。
- **Alarm**: APがアラーム無視デバイスリストにあるかどうか。オプションはYesおよびNoです。
- **Block**: APがブロックデバイスリストにあるかどうか。オプションはYesおよびNoです。
- : 対策APが対策デバイスリストにあるかどうかを示します。オプションは**Yes**または**No**です。

検出されたAP履歴レポート

このレポートには、WLANで検出された各カテゴリのAPの履歴数量と詳細が表示されます。検出されたAP履歴レポートを表示するためにパラメーターを設定する必要はありません。

検出されたAP History Category円グラフは、検出されたAPの各カテゴリの割合を示します。このグラフには、次のAPカテゴリが含まれている場合があります。

- **Authorized APs**: WLANで許可されているAPの合計数。
- **Misconfigured Aps** :WLANサービスの設定が正しくなく、WLANで許可されているAPの総数。
- **Rogue APs**: WLANで使用できないAPの合計数。
- **External APs**: 隣接WLAN内にあるAPの合計数。
- **Ad Hoc APs**: アドホックモードで動作しているAPの合計数。
- **Potential-Authorized Aps**: 許可される可能性のあるAPの合計数。
- **Potential-Rogue Aps**: 不正デバイスである可能性があるAPの合計数。
- **Potential-External Ap**s: 外部ネットワークからの可能性があるAPの合計数。
- **Uncategorized Aps**: カテゴリを判別できないAPの合計数。

検出されたAPの履歴リストには、各カテゴリのAPの合計数とその詳細が表示されます。

- **MAC Address**: 検出されたAPのMACアドレス。MACアドレスをクリックすると、APの詳細が表示されます。
- **SSID**: APで使用されるSSID。
- **Last Detection Time**: APが最後に検出された時刻。
- **Disappeared At**: APが検出されなくなった時間。
- **Virtual Security Domain**: APを検出したセンサーが属する仮想セキュリティドメイン。
- **Categor**y: APのカテゴリ。**Authorized、Rogue、Ad hoc、Misconfigured、External、Potential-Authorized、Potential-Rogue、Potential-External**、またはUncategorizedです。
- **Device Vendor**: 検出されたAPのベンダー。センサーがAPに関するベンダー情報を取得しない場合、このフィールドにはnullが表示されます。
- **Threat Level**: APの脅威レベル。値が大きいほど、脅威レベルが高くなります。
- **Detecting AC**: APを検出したセンサーが関連付けられているACのデバイスラベル。ラベルをクリックすると、ACの詳細が表示されます。

プローブ情報レポート

このレポートには、WLAN内のデバイスの数量と各カテゴリのデバイスの詳細が表示されます。

Detected Device Category円グラフには、検出されたデバイスの各カテゴリの割合が表示されます。このグラフには、R**elated Detection of AP Clients、Associated With Other AP Clients、Non**

Associated Clientsおよび**P Neighbor AP**カテゴリが含まれます。

Detected Deviceリストには、各カテゴリのデバイスの合計数とその詳細が表示されます。

- **MAC Address**: デバイスのMACアドレス。
- Category: デバイスのタイプ。オプションには、**Related Detection of AP Clients**、**Associated With Other AP Clients**、**Non Associated Clients**、および**Neighbor AP**があります。
- **SSID**: 接続されたネットワークのSSID。関連付けられていないクライアントの場合、このフィールドは空です。
- **BSSID**: アソシエートされたAPのMACアドレス。アソシエートされていないクライアントまたはネイバーAPの場合、このフィールドは空です。
- **Channel**: デバイスの動作チャネル。
- **Detecting AP**: デバイスを検出したAPの名前。
- **Location**: 検出中のAPが存在するロケーションビューの名前。
- **RSSI**: デバイスのRSSI。
- **Noise**: 検出APによって検出されたノイズフロア。ノイズフロアはチャネル品質に影響し、温度によって変化します。
- **Encryption Method**: デバイスで使用される暗号化方式。
- **First Detection Time**: デバイスが最初に検出された時刻。
- **Last Detection Time**: デバイスが最後に検出された時刻。
- **Online Time**: デバイスの合計オンライン時間。
- **Detecting AC**: 検出中のAPが関連付けられているACの名前。

プローブ情報履歴レポート

このレポートには、WLAN内のデバイスのWLAN内のデバイスの各カテゴリの詳細が表示されます。

Device Category Statistics円グラフには、検出されたデバイスの各カテゴリの割合が表示されます。このグラフには、**Related Detection of AP Clients**、**Associated With Other AP Clients**、**Non Associated Clients**および**AP Neighbor AP**などのカテゴリが含まれます。

検出されたクライアントのトレンドラインには、指定したレポート期間中の関連付けられたクライアントと関連付けられていないクライアントの合計数の変化が折れ線グラフで表示されます。横軸の時間増分は1時間です。

Detected Deviceリストには、各カテゴリのデバイスの合計数とその詳細が表示されます。

- **MAC Address**: デバイスのMACアドレス。
- **Category**: デバイスのタイプ。オプションには、**Related Detection of AP Clients**、**Associated With Other AP Clients**、**Non Associated Clients**、および**Neighbor AP**があります。
- **SSID**: 接続されたネットワークのSSID。関連付けられていないクライアントの場合、このフィールドは空です。
- **BSSID**: アソシエートされたAPのMACアドレス。アソシエートされていないクライアントまたはネイバーAPの場合、このフィールドは空です。
- **Channel**: デバイスの動作チャネル。
- **Detecting AP**: デバイスを検出したAPの名前。
- **Location**: 検出中のAPが存在するロケーションビューの名前。
- **RSSI**: デバイスのRSSI。
- **Noise**: 検出APによって検出されたノイズフロア。ノイズフロアはチャネル品質に影響し、温度によって変化します。

- **First Detection Time**: デバイスで使用される暗号化方式。
- **First Detection Time**: デバイスが最初に検出された時刻。
- **Last Detection Time**: デバイスが最後に検出された時刻。
- **Online Time**: デバイスの合計オンライン時間。
- **Detecting AC**:検出中のAPが関連付けられているACの名前

Located Client Statisticsレポート

このレポートには、ロケーションビュー別に、検出されたクライアントの統計情報が表示されます。

クライアントトレンドグラフには、指定したレポート期間中の関連付けられたクライアントおよび関連付けられていないクライアントの合計数の変化が線グラフで表示されます。水平軸上の時間増分は1分です。

クライアント統計リストの検索

- **Location view**: ロケーションビューの名前。
- **Associated clients**: ロケーションビュー内のアソシエートされたクライアントの数。
- **Disassociated clients**: ロケーションビュー内のアソシエーション解除されたクライアントの数。
- **Total clients**: ロケーションビュー内のクライアントの合計数。

入出庫統計レポート

このレポートには、顧客フロー統計がショップ別に表示されます。

Shop Entry/Exist Count Top 10には、ショップエントリー/エグジットカウントが最も多い上位10店舗が表示されます。横軸は店舗名を表し、縦軸はショップエントリー/エグジットカウントを表します。

以下は、ショップの入口/出口統計リストです。

- **Shop Name**: ショップの名前。
- **Client MAC**: クライアントのMACアドレス。
- **Entered At**: クライアントがショップに入った時刻。
- **Left at**: クライアントが店を出た時刻。
- **Length of Stay**: クライアントがストアに滞在していた時間(秒単位)。

PCIレポート

PCIレポートは、WLANのセキュリティコンプライアンスチェック情報を提供しま

す。PCIレポート:

- **Generated**: PCIレポートが生成された時刻。
- **Requirement**: DSS要件のシーケンス番号。ワイヤレスネットワークでは、要件のシーケンス番号は4.1.1または11.1です。
- **Description**: 要件の説明。
- **Status**: ワイヤレスネットワークのセキュリティチェックの結果が失敗または成功になります。
- **SSID**: WLANのSSID。
- **Enable Status**: WLANがイネーブルかディセーブルかを示します。
- **Encryption Mode**: WLANの暗号化モード(ClearまたはCrypto)。
- **Authentication Type**: WLANのリンク認証モード(**Open System**、**Shared Key**、または**All**)。

ワイヤレスサービスレポートテンプレートリストの表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Report Template List**を選択します。
   Report Template Listには、すべての無線サービスレポートテンプレートが表示されます。
   - **Template Name**: テンプレートの名前。
   - **Sub-Type**: テンプレートのサブタイプ。

ワイヤレスサービスレポートテンプレートの照会

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Report Template List**を選択します。
   Report Template Listには、すべての無線サービスレポートテンプレートが表示されます。
3. **Report Template List**ページで、Queryフィールドに1つ以上のクエリー基準を入力または選択します。
   - **Template Name**: テンプレートの名前を入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
   - **Sub-Type**: テンプレートのサブタイプを選択します。オプションは、**AP Statistics Report**、**Radio Statistics Report**、**Client Statistics Report**、**WLAN Statistics Report**、**Wireless Asset Statistics Report**、および**Security Statistics Report**です。
4. **Query**をクリックします。**Query**に、問合せ基準に一致するすべてのレポートテンプレートが表示されます。
5. **Reset**をクリックしてクエリー基準をクリアし、すべてのレポートテンプレートを表示します。

ワイヤレスサービスレポートテンプレートの設定

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Report Template List**を選択します。
   Report Template Listには、すべての無線サービスレポートテンプレートが表示されます。
3. **Report Template List**ページで、テンプレートの名前リンクをクリックします。
4. 開いた設定ページで、レポートテンプレートを設定します。

   設定はレポートテンプレートによって異なります。詳細は、「リアルタイムレポート」を参照してください。
5. **OK**をクリックします。

ネットワーク管理の設定

WSMには、次のネットワーク管理機能があります。

- **Wireless Monitoring Settings**: 無線ネットワークで監視するパフォーマンスインデックスを選択できます。
- **Fit AP Group**: 管理者がAPグループに適合する操作権限を割り当てることができます。
- **AP Model Management**: システム定義およびユーザー定義のAPモデルを管理します。
- **Antenna Management**: AP無線のシステム定義およびユーザー定義のアンテナモデルを管理します。
- **Threshold Configuration**: ワイヤレスパフォーマンスインデックスのしきい値を設定できます。収集されたデータが選択したアイテムのしきい値を超えると、WSMはアラームを生成します。
- **UAM Parameter Configuration**: WSMがUAMサーバーにログインしてオンラインクライアントのアカウント情報を取得できるようにします。
- **Endpoint Identification Management**: WSMがクライアントのIDを管理して、クライアントリストに製造元、タイプ、およびオペレーティングシステム情報を表示できるようにします。
- **Synchronization Configuration**: WSMによって管理されるワイヤレスデバイスの同期トリガーメカニズムを設定します。

WSMは、一般的な構成管理機能に加えて、Comwareベースの次の構成管理機能をサポートしています。

- Comwareベース:
  - **Network Management**: プライマリACとバックアップACをグループ化し、ポリシーテンプレートを管理できます。
  - **AC Configuration Management**: 次の項目を設定できます。
    - **Basic settings**
    - **AP templates**
    - **Radio policies**
    - **Radios in batches**
    - **Wireless logical interfaces**
    - **Service templates**
  - **Fat AP Configuration Management**: 次のタスクを実行できます(それぞれをバッチで実行)。
    - **Create BSS interfaces**
    - **Modify VLANs**
    - **Modify port security**
    - **Create service policies**
    - **Bind service templates**
    - **Configure radios**

  詳細については、「Comwareベースのアクセスコントローラの管理」および「Comwareベースの FAT APの管理」を参照してください。

ワイヤレス監視設定の指定

この機能を使用すると、ワイヤレスネットワークのパフォーマンスを監視するためのワイヤレスパフォーマン

スインデックスを有効または無効にできます。次のタブでインデックスを有効にできます:

- **By Report**
- **By Web Service**
- **By Overview**
- **By Network Evaluation**

パフォーマンス索引は複数のタブに表示される場合があります。索引の監視を停止するには、すべてのタブで索引が無効になっていることを確認してください。

ワイヤレス監視設定を構成するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Configuration Management**を選択します。

   Configuration Managementページが開きます。
3. **Common**をクリックします。
4. **Network Management**領域で、**Wireless Monitoring Settings**リンクをクリックします。

   Wireless Monitoring Settingsページが開きます。
5. **By Report**、**By Web Service**、**By Overview**、または**By Network Evaluation**の各タブをクリックし、WSMで監視するパフォーマンスインデックスを各タブの**Monitor Items**リストから選択します。
6. **OK**をクリックします。

   WSMは、タブ上で選択したパフォーマンスインデックスの監視を開始します。
7. カウンタをリセットするには、ページの右上にある**Re-collect**リンクをクリックします。

   WSMは、ページ上の**Monitored Item Number**フィールドと**Monitored Instance Number**フィールドをリセットします。

FIT APグループの管理

この機能を使用すると、特定のFit APグループにFIT APを追加することによって、1つ以上のFit APの管理権限をオペレーターに対して設定できます。

オペレーターは、管理者、保守担当者、またはビューアです。管理者はすべてのFIT APを管理でき、保守担当者は特定のFIT APを管理でき、ビューアは特定のFIT APのみを表示できます。

オペレーターがFit APグループを管理できるようにするには、Fit AP ManagementモジュールのADMINロールと管理権限をオペレーターに割り当てる必要があります。詳細については、『H3C IMC v7.3 Enterprise and Standard Platform Administrator Guide』を参照してください。

FIT APグループの管理の詳細については、「FIT APグループの管理」を参照してください。

APモデルの管理

この機能を使用すると、WSM上のすべてのシステム定義およびユーザー定義のAPモデルを管理できます。ユーザー定義のAPモデルを追加、変更および削除したり、すべてのAPモデルに関する基本情報または詳細情報を表示したりできます。

APモデルリストの表示

1. **Service**タブをクリックします。

2. ナビゲーションツリーから、**WLAN Manager>Configuration Management**を選択します。**Configuration Management**ページが開きます。
3. **Common**タブをクリックします。
4. **Network Management**領域で、**AP Model Management**リンクをクリックします。**AP Model List**にすべてのAPモデルが表示されます。

   APモデルリストの内容

   - **Model**: APのデバイスモデル。ターゲットAPのモデルをクリックすると、APの詳細が表示されます。詳細は、「APモデルの詳細の表示」を参照してください。
   - **Vendor**: APのベンダー。
   - **Radio Number**: AP上の無線の数。
   - **Type**: APモデルのタイプ。オプションはSystem-definedおよびUser-definedです。
   - **Delete**: ユーザー定義APモデルを削除するには、**Delete**アイコンをクリックします。システム定義APモデルは削除できません。詳細は、「APモデルの削除」を参照してください。

AP Model Listに十分なエントリーが含まれている場合は、次のナビゲーション支援が表示されます。APモデルリストのナビゲート

- **Next Page**アイコンをクリックして、**AP Model List**で次のページに進みます。
- **Last Page**アイコンをクリックして、**AP Model List**の最後のページに進みます。
- **Previous Page**アイコンをクリックして**AP Model List**の前のページに戻ります。
- **First Page**アイコンをクリックして、**AP Model List**の先頭にページバックします。

AP Model Listの右上にある8、15、50、100、または200をクリックして、各ページに表示する項目数を指定します。

注:

AP Model Listは、**Delete**フィールド以外のすべてのフィールドで並べ替えることができます。列ラベルをクリックすると、選択したフィールドでリストが並べ替えられます。列ラベルを使用すると、各フィールドに固有のさまざまな並べ替えオプションを切り替えることができます。

APモデルのクエリー

WSMには、基本問合せと拡張問合せが用意されています。基本問合せ基準には、迅速な検索のためのキーパラメーターがいくつか含まれています。拡張問合せには、正確な照合のための様々な問合せ基準が用意されています。

APモデルを照会するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Configuration Management**を選択します。**Configuration Management**ページが開きます。
3. **Common**タブをクリックします。
4. **Network Management**領域で、**AP Model Management**リンクをクリックします。**AP Model Management**ページが開きます。
5. 基本的なクエリーを実行します。
   a. APのモデルを入力します。WSMは、このフィールドのファジーマッチングをサポートします。
   b. **Query**アイコンをクリックします。**AP Model Management**ページに、クエリー基準

にー致するすべてのAPモデルが表示されます。

c. **Query**フィールドをクリアして**Query**アイコンをクリックすると、すべてのAPモデルが表示されます。

6. 高度なクエリーを実行します。

a. **Query**フィールドの横にある**Expand**アイコンをクリックし**Query**領域を拡張します。再度クリックすると**Query**領域が非表示になります。

b. APモデルを照会するには、次の1つ以上の照会基準を入力または選択します。

- **Model:** APモデルを入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
- **Vendor**: APのベンダーを入力します。WSMは、このフィールドのファジーマッチングをサポートしています。
- **Radio Number**: AP上の無線の数を入力します。
- **Type**: APモデルのタイプを選択します。オプションは次のとおりです。
  - **Unlimited**
  - **System-defined**
  - **User-defined**

空のフィールドや無制限に設定されたフィールドは、クエリーの抽出条件にはなりません。

c. **Query**をクリックします。

AP Model Listには、クエリー基準に一致するすべてのAPモデルが表示されます。

d. **Reset**をクリックしてクエリー基準をクリアし、すべてのAPモデルを表示します。

APモデルの詳細の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Configuration Management**を選択します。

   Configuration Managementページが開きます。
3. 共通タブをクリックします。
4. **Network Management**領域で、**AP Model Management**リンクをクリックします。**AP Model Management**ページが開きます。

   AP Model Listには、すべてのAPモデルが表示されます。
5. ターゲットAPのモデルをクリックして、その詳細を表示します。

   基本情報の内容

   - **Model**: APのモデル。
   - **Vendor**: APのベンダー。
   - **Type**: APモデルのタイプ。オプションはSystem-definedおよびUser-definedです。

   ラジオリストの内容

   - **ID**: AP上の無線のID。
   - **Radio Type**: 無線のタイプ。オプションは次のとおりです。

     802.11a
     802.11b
     802.11g
     802.11an
     802.11gn

- **Default Transmission Power(dBm)**: 無線のデフォルト送信電力。
- **Antenna**: アンテナのモデル。詳細は、「アンテナモデルの管理」を参照してください。
- **Modify**: ターゲット無線の**Modify**アイコンをクリックして、そのパラメーターを変更します。詳細については、「APモデルの変更」を参照してください。

X-Shareアンテナの画像

このフィールドには、Xシェアアンテナの画像が表示されます。

APモデルの追加

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Configuration Management**を選択します。

   Configuration Managementページが開きます。
3. **Common**タブをクリックします。
4. **Network Management**領域で、**AP Model Management**リンクをクリックします。**AP Model Management**ページが開きます。

   AP Model Listには、すべてのAPモデルが表示されます。
5. **Add**をクリックします。

   Add AP Modelダイアログボックスが開きます。
6. 基本情報を設定します。
   - APモデルとベンダーを入力します。
   - **Browse…**をクリックして、X-shareアンテナの画像を選択します。
7. **OK**をクリックします。

APモデルの詳細を表示するページが開きます。

8. **Radio List**領域で、**Add**をクリックします。

   Add Radioダイアログボックスが開きます。
9. 次のクエリー基準を1つ以上入力または選択して、**Add Radio**ダイアログボックスから追加する無線を検索します。
   - **Radio ID**: 無線IDを1～9の範囲で入力します。
   - **Radio Type**: 無線タイプを選択します。オプションは次のとおりです。

     802.11a

     802.11b

     802.11g

     802.11an

     802.11gn
   - **Default Transmission Power(dBm)**: 無線のデフォルト送信電力を1～30の範囲で入力します。
   - **Antenna**: 無線のアンテナタイプを選択します。
   - **Bandwidth Mode**: 無線信号の帯域幅を選択します。オプションは20 MHzおよび40 MHz。このフィールドは、Radio Typeが802.11 anまたは802.11gnの場合にだけ使用できます。
   - **A-MPDU**: インターフェースでA-MPDUをイネーブルにするかどうかを設定します。このフィールドは、Radio Typeが802.11 anまたは802.11 gnに設定されている場合にだけ使用できます。

- **A-MSDU**: インターフェースでA-MSDUをイネーブルにするかどうかを設定します。このフィールドは、Radio Typeが802.11 anまたは802.11gnに設定されている場合にだけ使用できます。
- **Short GI**: ショートGIを有効にするかどうかを設定します。ショートGIは、遅延による干渉からデータを保護します。このフィールドは、Radio Typeが設定されている場合にだけ使用できます。802.11anまたは802.11gn。

10. **OK**をクリックします。

    無線がAPモデルに追加されます。

11. **Back**をクリックして、**AP Model Management**ページに戻ります。

    APモデルが**AP Model List**に追加されます。

APモデルの変更

この機能を使用すると、既存のAPモデルを変更できます。システム定義のAPモデルの場合は、無線パラメーターだけを変更できます。ユーザー定義のAPモデルの場合は、APモデルのモデル、ベンダー、および無線パラメーターを変更できます。

APモデルを変更するには、次のとおりです。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Configuration Management**を選択します。

   Configuration Managementページが開きます。
3. **Common**タブをクリックします。
4. **Network Management**領域で、**AP Model Management**リンクをクリックします。

   AP Model Managementページが開きます。

   AP Model Listには、すべてのAPモデルが表示されます。
5. ターゲットAPモデルの名前をクリックすると、その詳細が表示されます。
6. ユーザー定義APモデルの基本情報を変更します。
   a. **Basic Information**フィールドの**Modify**アイコンをクリックします。

      Modify AP Model Informationダイアログボックスが開きます。
   b. 新しいモデルまたはベンダーを入力します。
7. X-Share Antenna Pictureを変更する:
   a. **X-Share Antenna Picture**フィールドで**Modify**をクリックします。
   b. **Browse…**をクリックして、画像を選択します。
   c. OKをクリックします。
8. APモデルの無線パラメーターを変更します。
   a. **Radio List**で、ターゲット無線の**Modify**アイコンをクリックします。
   b. **Radio ID**以外のすべての無線パラメーターを変更します。
   c. OKをクリックします。
9. 選択した無線を削除します。
   a. **Radio List**で、**Delete**アイコンをクリックしてターゲット無線を削除します。
   b. 確認ダイアログボックスで、OKをクリックします。

削除できるのは、ユーザー定義のAPモデルの無線だけです。

APモデルの削除

この関数を使用すると、ユーザー定義のAPモデルを削除できます。ユ

ーザー定義のAPモデルを削除するには、次の手順に従います。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Configuration Management**を選択します。

   Configuration Managementページが開きます。
3. **Common**タブをクリックします。
4. **Network Management**領域で、**AP Model Management**リンクをクリックします。**AP Model Management**ページが開きます。

   AP Model Listには、すべてのAPモデルが表示されます。
5. APモデルを削除するには、次のいずれかの方法を使用します。
   - ターゲットユーザ定義APモデルの**Delete**アイコンをクリックします。
   - ユーザー定義のAPモデルを選択します。**AP Model List**の上部にある**Delete**をクリックします。
6. 確認ダイアログボックスで、OKをクリックします。

アンテナモデルの管理

この機能を使用すると、ユーザー定義のAPモデルに新しく追加された無線のアンテナモデルを選択できます。WSMには、システム定義のアンテナモデルとユーザー定義のアンテナモデルが含まれています。ユーザー定義のアンテナモデルを追加、変更、および削除したり、方向、周波数、最大ゲインなどのアンテナパラメーターを設定したりできます。

アンテナー覧の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Configuration Management**を選択します。

   Configuration Managementページが開きます。
3. **Common**タブをクリックします。
4. **Network Management**領域で、**Antenna Management**リンクをクリックします。**Antenna List**にすべてのアンテナモデルが表示されます。

   アンテナー覧の内容
   - **Model**: アンテナのモデル。
   - **Vendor**: アンテナモデルのデバイスのベンダー。
   - **Direction**: アンテナモデルの信号送信方向。オプションは次のとおりです。**Omnidirectional**と**Directional**
   - **Frequency**: アンテナモデルの信号周波数。オプションは2.4GHzおよび5GHzです。
   - **Max.Ga**in: アンテナモデルの信号の最大ゲイン。
   - **Type**: アンテナモデルのタイプ。オプションは**System-defined**および**User-defined**.です。
   - **Modify**: ユーザー定義のアンテナモデルの**Modify**アイコンをクリックして、そのパラメーターを修正します。システム定義のアンテナモデルのパラメーターは修正できません。
   - **Delete**: ユーザー定義のアンテナモデルの**Delete**アイコンをクリックして、アンテナモデルを削除します。削除できるのは、ユーザー定義のアンテナモデルのみです。

Antenna Listに十分なエントリーが含まれている場合は、次のナビゲーション支援が表示されます。アンテナリストのナビゲート

- **Next Page**アイコンをクリックして、**Antenna List**で次のページに進みます。
- **Last Page**アイコンをクリックして、**Antenna List**の最後のページに進みます。
- **Previous Page**アイコンをクリックして、**Antenna List**で前のページに戻ります。
- **First Page**アイコンをクリックして、**Antenna List**の先頭に戻ります。

アンテナリストの右上にある**8**、**15**、**50**、**100**、または**200**をクリックして、各ページに表示する項目数を指定します。

注:

Antenna Listは、**Modify**フィールドと**Delete**フィールド以外のすべてのフィールドで並べ替えることができます。列ラベルをクリックすると、選択したフィールドでリストが並べ替えられます。列ラベルを使用すると、各フィールドに固有のさまざまな並べ替えオプションを切り替えることができます。

アンテナモデルのクエリー

WSMには、基本問合せと拡張問合せが用意されています。基本問合せ基準には、迅速な検索のためのキーパラメーターがいくつか含まれています。拡張問合せには、正確な照合のための様々な問合せ基準が用意されています。

アンテナモデルをクエリーするには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Configuration Management**を選択します。

   Configuration Managementページが開きます。
3. **Common**タブをクリックします。
4. **Network Management**領域で、**Antenna Management**リンクをクリックします。**Antenna List**にすべてのアンテナモデルが表示されます。
5. 基本的なクエリーを実行します。
   a. アンテナのモデルを入力してください。WSMは、このフィールドのファジーマッチングをサポートしています。
   b. **Query**アイコンをクリックします。**Antenna List**に、問合せ基準に一致するすべてのアンテナモデルが表示されます。
   c. **Query**フィールドをクリアし、**Query**アイコンをクリックしてすべてのアンテナモデルを表示します。
6. 高度なクエリーを実行します。
   a. **Query**フィールドの横にある**Expand**アイコンをクリックして**Query**領域を拡張します。再度クリックするとQuery領域が非表示になります。
   b. アンテナモデルをクエリーするには、次のクエリー基準を1つ以上入力または選択します。
   - **Model**: アンテナのモデルを入力します。WSMは、このフィールドのファジーマッチングをサポートします。
   - **Vendor**: アンテナモデルのベンダーを入力します。WSMは、このフィールドのファジーマッチングをサポートします。
   - **Direction**: アンテナモデルの信号送信方向を選択します。オプションは次のとおりです。

- **Unlimited**
- **Omnidirectional**
- **Directional**

- **Frequency**: アンテナモデルの信号周波数を選択します。オプションは次のとおりです。
  - **Unlimited**
  - **2.4GHz**
  - **5GHz**
- **Type**: アンテナのモデルタイプを選択します。オプションは次のとおりです:
  - **Unlimited**
  - **System-defined**
  - **User-defined**

空のフィールドや**Unlimited**に設定されたフィールドは、クエリーの抽出条件にはなりません。

c. **Query**をクリックします。

Antenna Listには、クエリー基準に一致するすべてのアンテナモデルが表示されます。

d. query criteriaをクリアしてすべてのアンテナモデルを表示するには、**Reset**をクリックします。

ユーザー定義のアンテナモデルを追加する

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Configuration Management**を選択します。

   Configuration Managementページが開きます。
3. **Common**タブをクリックします。
4. **Network Management**領域で、**Antenna Management**リンクをクリックします。**Antenna List**にすべてのアンテナモデルが表示されます。
5. **Add**をクリックします。

   Add Antennaページが開きます。
6. 必要に応じて次のパラメーターを設定します。
   - **Model**: アンテナのモデルを入力します。英数字、スペース、アンダースコア(_)、およびハイフン(-)だけを使用できます。
   - **Vendor**: アンテナモデルのベンダーを入力します。
   - **Frequency**: アンテナモデルの信号周波数を選択します。オプションは**2.4GHz**と**5GHz**です。
   - **Direction**: アンテナモデルの信号送信方向を選択します。オプションは次のとおりです。**Omnidirectional**と**Directional**
   - **Max.Gain**: アンテナモデルのRF信号の最大ゲインを設定します。値の範囲は1.0～30.0です。このフィールドは、**Direction**フィールドが**Omnidirectional**に設定されている場合にのみ使用できます。
   - **Gain Information File**: ファイルシステムをブラウズしてゲイン情報ファイルを選択するには、**Browse**をクリックします。ゲイン情報をインポートするには、**Import Gain Info**をクリックします。このフィールドは、**Direction**フィールドが**Directional**に設定されている場合にのみ使用できます。ゲイン情報ファイルは、アンテナ角度とゲインに関する情報を含む.CSVファイルです。ゲイン情報をインポートすると、WSMはインポートされた情報に基づいて、**Add Antenna**ページの下部に角度-ゲイングラフをグラフ化します。

Antenna Listのアンテナモデルは、**Model**、**Vendor**および**Frequency**で識別されます。**Antenna List**の既存のアンテナモデルと同じモデル、ベンダーおよび周波数を持つアンテナモデルは追加できません。

7. OKをクリックします。

ユーザー定義のアンテナモデルの修正

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Configuration Management**を選択します。
   Configuration Managementページが開きます。
3. **Common**タブをクリックします。
4. **Network Management**領域で、**Antenna Management**リンクをクリックします。**Antenna List**にすべてのアンテナモデルが表示されます。
5. ターゲットのユーザー定義アンテナモデルの**Modify**アイコンをクリックします。
   Modify Antennaページが開きます。
6. 必要に応じて、アンテナパラメーターを変更します。

アンテナパラメーターの詳細については、「ユーザー定義のアンテナモデルの追加」を参照してください。

7. OKをクリックします。

ユーザー定義のアンテナモデルの削除

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Configuration Management**を選択します。
   Configuration Managementページが開きます。
3. **Common**タブをクリックします。
4. **Network Management**領域で、**Antenna Management**リンクをクリックします。**Antenna List**にすべてのアンテナモデルが表示されます。
5. 次のいずれかの方法を使用して手順を続行します。
   - ターゲットのユーザー定義アンテナモデルの**Delete**アイコンをクリックします。
   - 削除するユーザー定義のアンテナモデルを選択して、**Delete**をクリックします。
6. 確認ダイアログボックスで、OKをクリックします。

アラームしきい値の設定

この機能は、ワイヤレスパフォーマンスインデックスのしきい値の設定に役立ちます。収集されたデータが選択したパフォーマンスインデックスのしきい値を超えると、WSMはアラームを生成します。

しきい値を設定するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Configuration Management**を選択します。
   Configuration Managementページが開きます。
3. **Common**タブをクリックします。
4. **Network Management**領域で、**Threshold Configuration**リンクをクリックします。

   Threshold Configurationページが開きます。

   しきい値設定の内容

   - **Client Count>**: 同じAPにアソシエートされているクライアントの数。**Client Count>**を選択し

て、0～200の範囲の数を入力します。APにアソシエートされているクライアントの数がこの値を超えると、アラームが生成されます。

- **Radio Rate(%)>**: サポートされている最大レートに対する無線のレートの割合。**Radio Rate(%)>**を選択し、1～100の範囲の値を入力します。割合がこの値を超えると、アラームが生成されます。
- **Radio Channel Utilization**: メインチャネルの最大使用率。デフォルトで選択され、選択解除はできません。20から100の範囲の値を入力します。使用率がこの値を超えると、アラームが生成されます。
- **Clients Associated with AC(Minor))**: 同じACに関連付けられているクライアントの数。**Clients Associated with AC(Minor)**を選択し、1～50000の範囲の値を入力します。ACに関連付けられているクライアントの数がこの値を超えると、マイナーアラームが生成されます。
- **Clients Associated with AC(Major)**: 同じACにアソシエートされているクライアントの数。**Clients Associated with AC(Major)**を選択し、1～50000の範囲の値を入力します。ACにアソシエートされているクライアントの数がこの値を超えると、メジャーアラームが生成されます。

5. OKをクリックします。

UAMパラメーターの設定

デフォルトでは、WSMはオンラインクライアントの名前ではなくMACアドレスを表示します。ネットワークにUAMがデプロイされている場合は、WSMがオンラインクライアントのアカウント情報をUAMサーバーから取得できるように設定できます。UAMとWSMが同じサーバーにデプロイされているかどうかにかかわらず、UAMサービスパラメーターを構成します。

UAMサービスパラメーターを設定するには、次の手順を実行します。

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Configuration Management**を選択します。

   Configuration Managementページが開きます。
3. **Common**タブをクリックします。
4. **Network Management**領域で**UAM Parameter Configuration**リンクをクリックします。

   UAM Parameter Configurationページが開きます。
5. 次のUAMサービスパラメーターを設定します。
   - **IMC Master Server IP Address**s: UAMが属するプライマリIMCサーバーのIPアドレスを入力します。UAMとWSMが同じサーバーに展開されている場合は、127.0.0.1を入力します。
   - **Login Port**: UAMサーバーへのログインに使用するポートを入力します。
   - **Login Type**: UAMサーバーへのログインに使用するプロトコルを選択します。オプションは次のとおりです。
     HTTPおよびHTTPS。
   - **Login Name**: ログインユーザ名を入力します。
   - **Password** :ログインパスワードを入力します。
   - **Confirm Password**: ログインパスワードを再入力します。
   - **Automatically Obtain Client Information from UAM**: クライアントがネットワークに接続するときに、WSMがクライアントのアカウント名をUAMサーバーから自動的に取得するかどうかを設定します。WSMは、クライアントのMACアドレスによってアカウント名を問い合せます。このオプションはデフォルトでは選択されていません。
6. OKをクリックします。

エンドポイントIDの管理

エンドポイントID管理を使用すると、エンドポイントベンダー、エンドポイントタイプ、およびOSを含む基本的なエンドポイントID情報をWSMに追加できます。これにより、クライアントがWLANを介してネットワークにアクセスするときに、WSMはクライアントリストにクライアントの情報を表示できます。

クライアントの管理については、「クライアントの管理」を参照してください。

エンドポイントベンダーの管理

Vendor Listページでは、ベンダーの照会、追加、変更、および削除を行うことができます。

Vendor List**ページへのアクセス**

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Configuration Management**を選択します。

   Configuration Managementページが開きます。
3. **Common**タブをクリックします。
4. **Network Management**領域で、**Endpoint Identification Management**リンクをクリックします。

   Endpoint Identification Managementページが開きます。
5. **Vendor**をクリックします。

   Vendor Listには、WSMに追加されたすべてのベンダーが表示されます。

   ベンダーリストの内容

   - **Vendor**: ベンダー名。
   - **Description**: ベンダーの説明。
   - **Modify**: **Modify**アイコンをクリックして、**Modify Vendor**ページが表示されます。
   - **Delete**: ベンダーを削除するには、**Delete**アイコンをクリックします。

Vendor Listに十分なエントリーが含まれている場合は、次のナビゲーションエイドが表示されます。ベンダーリストのナビゲート

- **Next Page**アイコンをクリックして、**Vendor List**内で次のページに進みます。
- **Last Page**アイコンをクリックして、**Vendor List**の最後のページに進みます。
- **Previous Page**アイコンをクリックして、**Vendor List**で前のページに戻ります。
- **First Page**アイコンをクリックすると、**Vendor List**の先頭に戻ることができます。

ベンダーリストの右上にある8、15、50、100、または200をクリックして、各ページに表示する項目数を指定します。

注:

Vendor Listは、**Modify**フィールドと**Delete**フィールド以外のすべてのフィールドで並べ替えることができます。列ラベルをクリックすると、選択したフィールドでリストを並べ替えることができます。列ラベルを使用すると、各フィールドに固有のさまざまな並べ替えオプションを切り替えることができます。

ベンダーの照会

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Configuration Management**を選択します。

Configuration Managementページが開きます。

3. **Common**タブをクリックします。
4. **Network Management**領域で、**Endpoint Identification Management**リンクをクリックします。

   Endpoint Identification Managementページが開きます。
5. **Vendor**をクリックします。

   Vendor Listには、WSMに追加されたすべてのベンダーが表示されます。
6. ページ右側の**Query**フィールドに、ベンダー名の一部または全部を入力します。
7. **Query**アイコンをクリックします。**Vendor List**に、問合せ基準に一致するすべてのベンダーが表示されます。
8. 問合せフィールドを消去して**Query**アイコンをクリックします。**Vendor List**にすべてのベンダーが表示されます。

ベンダーの追加

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Configuration Management**を選択します。

   Configuration Managementページが開きます。
3. **Common**タブをクリックします。
4. **Network Management**領域で、**Endpoint Identification Management**リンクをクリックします。

   Endpoint Identification Managementページが開きます。
5. **Vendor**をクリックします。

   Vendor Listには、WSMに追加されたすべてのベンダーが表示されます。
6. **Add**.をクリックします。

   Add Vendorページが開きます。
7. **Vendor**フィールドにベンダー名を入力します。
8. **Description**フィールドにベンダーの説明を入力します。
9. OKをクリックします。

ベンダーの変更

変更できるのはベンダーの説明のみです。ベンダーを

変更するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Configuration Management**を選択します。

   Configuration Managementページが開きます。
3. **Common**タブをクリックします。
4. **Network Management**領域で、**Endpoint Identification Management**リンクをクリックします。

   Endpoint Identification Managementページが開きます。
5. **Vendor**をクリックします。

   Vendor Listには、WSMに追加されたすべてのベンダーが表示されます。
6. 変更するベンダーの**Modify**アイコンをクリックします。

   Modify Vendorページが開きます。
7. **Description**フィールドでベンダーの説明を変更します。
8. OKをクリックします。

ベンダーの削除

エンドポイントクライアント情報の記述に使用されたベンダーを削除する前に、まずクライアント情報を削除する必要があります。クライアント情報の削除の詳細は、「クライアント情報の削除」を参照してください。

ベンダーを削除するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Configuration Management**を選択します。
   Configuration Managementページが開きます。
3. **Common**タブをクリックします。
4. **Network Management**領域で、**Endpoint Identification Management**リンクをクリックします。
   Endpoint Identification Managementページが開きます。
5. **Vendor**.をクリックします。
   Vendor Listには、WSMに追加されたすべてのベンダーが表示されます。
6. 削除するベンダーの**Delete**アイコンをクリックします。
7. 確認ダイアログボックスで、OKをクリックします。

エンドポイントタイプの管理

Endpoint Type Listページから、エンドポイントタイプのクエリー、追加、変更、および削除ができます。

エンドポイントタイプリストページへのアクセス

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Configuration Management**を選択します。
   Configuration Managementページが開きます。
3. **Common**タブをクリックします。
4. **Network Management**領域で、**Endpoint Identification Management**リンクをクリックします。
   Endpoint Identification Managementページが開きます。
5. **Endpoint Type**をクリックします。
   Endpoint Typeプリストには、WSMに追加されたすべてのエンドポイントタイプが表示されます。
   エンドポイントタイプリストの内容
   - **Endpoint Type**: エンドポイントタイプの名前。
   - **Description**: エンドポイントタイプの説明。
   - **Modify**: **Modify**アイコンをクリックして、**Modify Endpoint Type**ページを開きます。
   - **Delete**: エンドポイントタイプを削除するには、**Delete**アイコンをクリックします。

Endpoint Type Listに十分な数の項目がある場合は、以下のナビゲーションエイドが表示されます。**Endpoint Type List**のナビゲート

- **Next Page**アイコンをクリックして**Endpoint Type List**で次のページ次のページに進みます。
- **Last Page**アイコンをクリックして、**Endpoint Type List**の最後のページに進みます。
- **Previous Page**アイコンをクリックして、**Endpoint Type List**の前のページに移動します。
- **First Page**アイコンをクリックして、**Endpoint Type List**の先頭にページバックします。

Endpoint Type Listの右上にある8、15、50、100、または200をクリックして、各ページに表示する項目数を指定します。

注:

Endpoint Type Listは、**Modify**および**Delete**フィールドを除くすべてのフィールドでソートできます。列ラベルをクリックすると、選択したフィールドでリストをソートできます。列ラベルを使用すると、各フィールドに固有の様々なソートオプションを切り替えることができます。

エンドポイントタイプの照会

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Configuration Management**を選択します。
   Configuration Managementページが開きます。
3. **Common**タブをクリックします。
4. **Network Management**領域で、**Endpoint Identification Management**リンクをクリックします。
   Endpoint Identification Managementページが開きます。
5. **Endpoint Type**をクリックします。
   Endpoint Type Listには、WSMに追加されたすべてのエンドポイントタイプが表示されます。
6. ページの右側の**Query**フィールドに、エンドポイントタイプ名の一部または全部を入力します。
7. **Query**アイコンをクリックします。**Endpoint Type List**に、問合せ基準に一致するすべてのエンドポイントタイプが表示され
8. **Query**フィールドを消去して、**Query**アイコンをクリックします。**Endpoint Type List**には、すべてのエンドポイントタイプが表示されます。

エンドポイントタイプの追加

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Configuration Management**を選択します。
   Configuration Managementページが開きます。
3. **Common**タブをクリックします。
4. **Network Management**領域で、**Endpoint Identification Management**リンクをクリックします。
   Endpoint Identification Managementページが開きます。
5. **Endpoint Type**をクリックします。
   Endpoint Type Addをクリックします。
   Add Endpoint Typeページが開きます。
6. **Endpoint Type**フィールドにエンドポイントタイプ名を入力します。
7. エンドポイントタイプの説明を**Description**フィールドに入力します。
8. OKをクリックします。

エンドポイントタイプの変更

エンドポイントタイプの説明のみ変更できます。エンドポイントタ

イプを変更する手順は、次のとおりです:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Configuration Management**を選択します。
   Configuration Managementページが開きます。
3. **Common**タブをクリックします。
4. **Network Management**領域で、**Endpoint Identification Management**リンクをクリックします。
   Endpoint Identification Managementページが開きます。

5. **Endpoint Type**をクリックします。
   Endpoint Typeリストには、WSMに追加されたすべてのエンドポイントタイプが表示されます。
6. 変更するエンドポイントタイプの**Modify**アイコンをクリックします。
   Modify Endpoint Typeページが開きます。
7. **Description**フィールドでエンドポイントタイプの説明を変更します。
8. OKをクリックします。

エンドポイントタイプの削除

エンドポイントクライアント情報の記述に使用されたエンドポイントタイプを削除する前に、まずクライアント情報を削除する必要があります。クライアント情報の削除の詳細は、「クライアント情報の削除」を参照してください。

エンドポイントタイプを削除するには、次のようにします

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Configuration Management**を選択します。
   Configuration Managementページが開きます。
3. **Common**タブをクリックします。
4. **Network Management**領域で、**Endpoint Identification Management**リンクをクリックします。
   Endpoint Identification Managementページが開きます。
5. **Endpoint Type**をクリックします。
   Endpoint Type Listには、WSMに追加されたすべてのエンドポイントタイプが表示されます。
6. 削除するエンドポイントタイプの**Delete**アイコンをクリックします。
7. 確認ダイアログボックスで、OKをクリックします。

OSの管理

OS Listページから、OSの照会、追加、変更、および削除を行うことができます。

OSリストページへのアクセス

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Configuration Management**を選択します。
   Configuration Managementページが開きます。
3. **Common**タブをクリックします。
4. **Network Management**領域で、**Endpoint Identification Management**リンクをクリックします。
   Endpoint Identification Managementページが開きます。
5. **OS**をクリックします。
   OSリストには、WSMに追加されたすべてのOSが表示されます。
   OSリストの内容
   - **OS**: Operating System(オペレーティングシステム)。
   - **Description**: オペレーティングシステムの説明。
   - **Modify**: **Modify**アイコンをクリックして、OSの変更ページに入ります。
   - **Delete**: **Delete**アイコンをクリックして、オペレーティングシステムを削除します。

OS Listに十分なエントリーが含まれている場合は、次のナビゲーション支援が表示されます。

OSリストのナビゲート

- **Next Page**アイコンをクリックして、**OS List**で次のページに進みます。
- **Last Page**アイコンをクリックすると、**OS List**の最後にページ送りされます。
- **Previous Page**アイコンをクリックして、**OS List**で前のページに戻ります。
- **First Page**アイコンをクリックすると、**OS List**の先頭に戻ることができます。

OSリストの右上にある8、15、50、100、または200をクリックして、各ページに表示する項目数を指定します。

注:

OS List byは、**Modify**および**Delete**フィールドを除くすべてのフィールドでソートできます。選択したフィールドでリストをソートするには、列ラベルをクリックします。列ラベルを使用すると、各フィールドに固有の様々なソートオプションを切り替えることができます。

OSのクエリー

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Configuration Management**を選択します。
   Configuration Managementページが開きます。
3. **Common**ブをクリックします。
4. **Network Management**領域で、**Endpoint Identification Management**リンクをクリックします。
   Endpoint Identification Managementページが開きます。
5. OSをクリックします。

OSリストには、WSMに追加されたすべてのOSが表示されます。

6. ページ右側の**Query**フィールドに、OS名の一部または全部を入力します。
7. **query**アイコンをクリックします。**OS List**に、問合せ基準に一致するすべてのOSが表示されます。
8. **Query**フィールドをクリアして、**Query**アイコンをクリックします。**OS List**にすべてのOSが表示されます。

OSの追加

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Configuration Management**を選択します。
   Configuration Managementページが開きます。
3. **Common**タブをクリックします。
4. **Network Management**領域で、**Endpoint Identification Management**リンクをクリックします。
   Endpoint Identification Managementページが開きます。
5. OSをクリックします。

OSリストには、WSMに追加されたすべてのOSが表示されます。

6. **Add**をクリックします。
7. **Add OS**ページが開きます。
8. **OS**フィールドにOS名を入力します。
9. **Description**フィールドにOSの説明を入力します。
10. OKをクリックします。

OSを変更する

変更できるのはOSの説明のみです。OSを変更す

るには、次の手順を実行します:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Configuration Management**を選択します。

   Configuration Managementページが開きます。
3. **Common**タブをクリックします。
4. **Network Management**領域で、**Endpoint Identification Managemen**tリンクをクリックします。

   Endpoint Identification Managementページが開きます。
5. **OS**をクリックします。

OS Listには、WSMに追加されたすべてのOSが表示されます。

6. 変更するOSの**Modify**アイコンをクリックします。**Modify OS**ページが開きます。
7. **Description**フィールドでOSの説明を変更します。
8. OKをクリックします。

OSの削除

エンドポイントクライアント情報の記述に使用されたOSを削除する前に、まずクライアント情報を削除する必要があります。クライアント情報の削除の詳細は、「クライアント情報の削除」を参照してください。

OSを削除するには:

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Configuration Management**を選択します。

   Configuration Managementページが開きます。
3. **Common**タブをクリックします。
4. **Network Management**領域で、**Endpoint Identification Management**リンクをクリックします。

   Endpoint Identification Managementページが開きます。
5. **OS**をクリックします。

OS Listには、WSMに追加されたすべてのOSが表示されます。

6. 削除するOSの**Delete**アイコンをクリックします。
7. 確認ダイアログボックスで、OKをクリックします。

同期構成

この機能を使用すると、ワイヤレスデバイスの同期トリガーメカニズムを設定できます。1つ以上の同期トリガーメカニズムを無効にして、パフォーマンス消費を削減できます。

同期パラメーターを設定するには、次の手順に従います

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Configuration Management**を選択します。

   Configuration Managementページが開きます。
3. **Common**タブをクリックします。
4. **Network Management**領域で、**Synchronization Configuration**リンクをクリックします。

   Synchronization Configurationページが開きます。

   同期構成の内容
   - **Synchronize Device Upon Alarm**: デバイスがアラームを受信したときにすぐ

にデバイスを同期するには、このオプションを選択します。

- **Synchronize Device Upon Configuration Deployment**: 設定がデバイスに展開されたときにデバイスをただちに同期するには、このオプションを選択します。
- **Synchronize Device Upon Polling Message from Platform**: このオプションを選択すると、デバイスがIMCプラットフォームからポーリングメッセージを受信したときに、ただちにデバイスが同期化されます。

5. **OK**をクリックします。

Fit APグループの管理

WSMを使用すると、管理者はFIT APをグループ化して管理を容易にすることができます。FIT APグループは、ユーザー グループおよび特定のユーザーごとに権限を割り当てるための基礎となります。

次の条件が満たされている場合、ユーザーは、FIT APリストのACリンクなしでFIT AP情報を表示できます。

- ユーザーには、FIT APグループ内のFIT AP情報を表示する権限が付与されます。
- ユーザーには、デバイスグループ内のFit APを管理するACを表示する権限が付与されていません。

FIT APグループリストの表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Configuration Management**を選択します。
3. **Common**タブをクリックします。
4. **Network Management**領域で、Fit AP Groupをクリックします。

   Fit AP Group Listに次の情報が表示されます。

   APグループリストに合わせる

   - **Group Na**: -FIT APグループの名前。FIT APグループの名前をクリックすると**Fit AP Group Details Information**ページが表示されます。
   - **Description**: Fit APグループの説明。
   - **Fit AP List**: **Fit AP List**アイコンをクリックして、Fit AP Listページを表示します。
   - **Modify**: FIT APグループを変更するには、**Modify**アイコンをクリックします。
   - **Delete**: FIT APグループを削除するには、**Delete**アイコンをクリックします。
5. 最新のFit APグループを表示するには、**Refresh**をクリックします。

FIT APグループに関する詳細情報の表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Configuration Management**を選択します。
3. **Common**タブをクリックします。
4. **Network Management**領域で、**Fit AP Group**をクリックします。

   Fit AP Group Listには、すべてのFIT APグループが表示されます。
5. グループFIT APグループの名前をクリックすると、そのグループの詳細情報が表示されます。

   Fit AP Group Details Informationページには、次の情報が表示されます。

   Fit AP Group Basic Information

   - **Group Name**: Fit APグループの名前。
   - **Description**: Fit APグループの説明。
   - **Group Type**: Fit APグループのタイプ。

   グループを管理できるオペレーター

   オペレーターの詳細については、『H3C IMC v7.3 Enterprise and Standard Platform Administrator Guide』を参照してください。

   - **Username**: IMCにログインするためのユーザー名。

- **Full Name**: オペレーターのフルネーム。
- **Role**: オペレーターは、管理者、保守担当者、またはビューアになります。管理者はすべてのFIT APグループを管理でき、保守担当者は特定のFIT APグループを管理でき、ビューアは特定のFIT APグループのみを表示できます。
- **Manage All Groups**: オペレーターの特権レベルを表示します。
  - **Yes**: オペレーターには、適合するすべてのAPグループを管理する特権レベルがあります。
  - **No**: オペレーターには、FIT APグループを管理または表示するための特権レベルがありません。
- **Description**: オペレーターの説明。

FIT APリスト

この領域には、グループ内のすべてのFIT APが表示されます。

- **Status**: FIT APのオンラインステータス。アイコンにポインタを置くと、ステータスの詳細が表示されます。
  - **Online(Primary)**: Fit APは、プライマリACに接続するComwareベースのFit APで、Fit APはオンラインです。
  - **Online(Secondary)**: Fit APはセカンダリACに接続するFit APであり、Fit APはオンラインです。
  - **Offline**: FIT APはオンラインではありません。
- **AP Label**: FIT APのラベル。
- **SN**: FIT APのシリアル番号。
- **IP Address**: FIT APのIPv4アドレス。
- **MAC Address**: FIT APのMACアドレス。
- **Model**: FIT APのデバイスモデル。

6. **Close**をクリックして、**Fit AP Group List**に戻ります。

FIT APグループの追加

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Configuration Management**を選択します。
3. **Common**タブをクリックします。
4. **Network Management**領域で、**Fit AP Group**をクリックします。

   Fit AP Group Listには、すべてのFIT APグループが表示されます。
5. **Add**をクリックします。
6. FIT APグループの基本情報を指定します。
   - **Group Name**: IT APグループの名前を入力します。名前は一意である必要があります。
   - **Description**: APグループ全体の説明を入力します。
   - **Group Type**: FIT APグループのタイプを選択します。オプション**Unlimited**、**Attendance**および**Access Deny**です。**Attendance**を選択すると、WSMにより各クライアントの最初の接続時間およびオフライン時間が記録されます。**Access Deny**を選択すると、クライアントがこのグループ内のFIT APにアクセスするとアラームがトリガーされ、WSMによりクライアントの拒否情報が記録されます。この機能はサードパーティソフトウェアで使用されます。
7. **Operators that can manage the group**領域で、該当するAPグループを管理または表示するための権限を割り当てるオペレーターを選択します。

- デフォルトでは、システム管理者adminは常にすべてのFIT APグループを管理する権限を持っています。**admin**の前のボックスはクリアできません。
- すべてのグループを管理する権限を持って作成された管理者は、新しいAPグループを管理できます。この権限を持つ管理者のボックスをクリアすることができます。
- すべてのグループを表示する権限で作成されたビューアは、新しいfit APグループを表示できます。この権限を持つビューアのボックスをクリアできます。

8. OKをクリックします。

FIT APグループの変更

1. **Service**タブをクリックします。
2. ナビゲーションツリーから**WLAN Manager** > **Configuration Management**を選択します。
3. **Common**タブをクリックします。
4. **Network Management**領域で、**Fit AP Group**をクリックします。

   Fit AP Group Listには、すべての**Fit AP Group**が表示されます。
5. 変更するFit APグループの**Modify**アイコンをクリックします。
6. 次のように変更します。
   - **Group Name**: このフィールドは変更できません。
   - **Description**: Fit APグループの説明を変更します。
7. FIT APグループを管理できるオペレーターを再選択します。

adminの前のボックスはグレー表示され、変更できません。

8. OKをクリックします。

FIT APグループの削除

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Configuration Management**を選択します。
3. **Common**タブをクリックします。
4. **Network Management**領域で、Fit AP Groupをクリックします。

   Fit AP Group Listには、すべてのFIT APグループが表示されます。
5. 削除するFit APグループの**Delete**アイコンをクリックします。
6. 確認ダイアログボックスで、OKをクリックします。

FIT APグループ内のFIT APの表示

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Configuration Management**を選択します。
3. **Common**タブをクリックします。
4. **Network Management**領域で、**Fit AP Group**をクリックします。

   Fit AP Group Listには、すべてのFIT APグループが表示されます。
5. APを追加するFit APグループの**Fit AP List**アイコンをクリックします。**Fit AP List**には、現

在のグループ内のすべてのFit APが表示されます。

FIT APリスト

- **Status**: FIT APのステータス。アイコンは、APがオンラインであることを示します。アイコンは、APがオフラインであることを示します。
- **AP Label**: FIT APのラベル。
- **SN**: FIT APのシリアル番号。
- **IP Address**: FIT APのIPアドレス。APがオフラインの場合、このフィールドはヌルです。
- **MAC Address**: FIT APのMACアドレス。APがオフラインの場合、このフィールドはヌルです。
- **Model**: FIT APのモデル。

6. 複数のFIT APが同じシリアル番号を持つ場合、**Fit AP List**には、デフォルトでこれらのすべてのAPが表示されます。ページの右側で**Fit AP List**オプションを選択すると、WSMフィルタにより、同じシリアル番号を持つAPが適合され、1つのFIT APのみが表示されます。フィルタルールは次のとおりです。
   - オンラインのAPが1つだけの場合、WSMはこのオンラインAPを表示します。
   - すべてのAPがオフラインの場合、WSMは最初のAPを表示します。

Fit AP Listに十分なエントリーが含まれている場合は、次のナビゲーション支援が表示されます。

Fit AP Listのナビゲート

- Next Pageアイコンをクリックして、**Fit AP List**で次のページに進みます。
- **Last Page**アイコンをクリックして、**Fit AP List**の最後のページに進みます。
- **Previous Page**アイコンをクリックして、**Fit AP List**で前のページに戻ります。
- **First Page**アイコンをクリックして、**Fit AP List**の前にページバックします。

APリストに合わせるの右上にある**8、15、50、100**、または**200**をクリックして、各ページに表示する項目数を指定します。

注:

AP Model Listはフィールドごとにソートできます。列ラベルをクリックすると、選択したフィールドごとにリストがソートされます。列ラベルを使用すると、各フィールドに固有のさまざまなソートオプションを切り替えることができます。

FIT APグループへのFIT APの追加

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Configuration Management**を選択します。
3. **Common**タブをクリックします。
4. **Network Management**領域で、**Fit AP Group**をクリックします。

   Fit AP Group Listには、すべてのFIT APグループが表示されます。
5. APを追加したいAPグループのために**Fit AP List**アイコンをクリックします。
6. **Add**をクリックします。

   ダイアログボックスが開き、FIT APを選択できます。
7. 次の1つ以上の検索基準を指定します。

   空のフィールドや無制限に設定されたフィールドは、検索条件として使用できません。

- **Device Label**: FIT APのデバイスラベルを入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
- **Device Type**: リストからFIT APを選択します。
- **Serial Number**: FIT APのシリアル番号を入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
- **IP Address**: FIT APのIPv4アドレスの一部または全体を入力します。WSMは、このフィールドのファジーマッチングをサポートします。
- **Model**: FIT APのモデルを入力します。WSMでは、このフィールドのファジーマッチングがサポートされています。
- **Online Status**: FIT APのオンライン状態を選択します。オプションは次のとおりです。
  - **Unlimited**
  - **Online**
  - **Offline**
- **AC**: ACを選択します。オプションはUnlimitedおよびすべての管理対象ACです。
- **Location View**: FIT APが属するロケーションビューの名前を入力または選択します。WSMは、このフィールドのファジーマッチングをサポートします。

8. **Query**をクリックします。

   Fit AP Listには、クエリー基準に一致するすべてのFIT APが表示されます。
9. FIT APグループに追加するfit APを選択します。
10. OKをクリックします。

FIT APグループからのFIT APの削除

1. **Service**タブをクリックします。
2. ナビゲーションツリーから、**WLAN Manager>Configuration Management**を選択します。
3. **Common**タブをクリックします。
4. **Network Management**領域で、**Fit AP Group**をクリックします。

   Fit AP Group Listには、すべてのFIT APグループが表示されます。
5. APを削除するfit APグループの**Fit AP List**アイコンをクリックします。
6. 削除する1つを1つ以上選択して、**Remove**をクリックします。
7. 確認ダイアログボックスで、**OK**をクリックします。

オペレーター権限の管理

WSMは、IMCプラットフォームの権限割当て機能を拡張します。WSMは、オペレーターグループごとに権限を割り当て、特定のFIT APグループおよびレベル1ロケーションビューのオペレーターへの割当てをサポートします。

概要

ロケーションビューを使用すると、地理的な場所に基づいてAPを管理できます。現在、オペレーターにはレベル1のロケーションビューのみが割り当てられています。ロケーションビューの詳細については、「ワイヤレスビューの管理」を参照してください。

オペレーター管理では、オペレーターの役割を指定し、そのオペレーターを管理可能なAPグループとレベル1ロケーションビューに割り当てることができます。役割には、管理者、メンテナ、およびビューアがあります。各役割には、異なる権限があります。

設定手順

オペレーター権限を管理するには、次の手順に従います

1. **System**タブをクリックします。
2. ナビゲーションツリーから、**Operator Management>Operator**を選択します。
3. 権限を変更するオペレーターの**Add**または**Modify**アイコンをクリックします。
4. **Operator Group**リストで、**Maintainer Group**または**Viewer Group**を選択します。
5. **WSM Privilege Management**エリアで、オペレーターの管理可能FIT APグループとレベル1ロケーションビューを指定します。

   管理しやすいAPグループ

   - **Manage all Fit AP groups**: オペレーターは既存のすべてのFit APグループを管理できます。デフォルトでは、新しく作成されたFit APグループを管理するように割り当てられます。
   - **Specify manageable Fit AP groups**: このオプションを選択すると、Fit AP Group Listが表示されます。オペレーターが管理または表示するグループを選択します。

   管理可能なレベル1ロケーションビュー

   - **Manage all Level 1 location views**: オペレーターは既存のレベル1をすべて管理できます。既定では、新しく作成されたレベル1の位置ビューを管理するために割り当てられます。
   - **Specify manageable Level 1 location views**: このオプションを選択した場合は、**Add**をクリックしてロケーションビューの問合せページを開きます。基準を入力して**Query**をクリックします。一致するすべてのロケーションビューが表示されます。オペレーターが管理または表示するレベル1ロケーションビューを選択します。
6. OKをクリックします。

よくある質問

デバイスはワイヤレスデバイスとしてIMCプラットフォームに追加されますが、WSMには表示されません。なぜでしょう?

WSMは、MIB内の特定のオブジェクトを読み取ることによってワイヤレスデバイスを識別します。WSMがMIB内のワイヤレスデバイスのオブジェクトを読み取れない場合、管理用のデバイスは追加されません。

この問題を解決するには:

- デバイスのソフトウェアバージョンがWSMと互換性があることを確認します。
- 互換性がない場合は、ソフトウェアバージョンまたはWSMバージョンを更新します。

WSMライセンスで許可される管理可能なノードの数には、AC、FAT AP、およびFIT APが含まれますか?

ACは、購入したIMCプラットフォームライセンスで許可される管理可能ノードの数に含まれます。

FIT APは、購入したWSMライセンスで許可される管理可能ノードの数に含まれます。

FAT APは、購入したIMCプラットフォームライセンスで許可される管理可能なノード数と、購入したWSMライセンスで許可される管理可能なノード数の両方に含まれます。

マネージドFIT APの数は、ACに設定されたAPテンプレートの数またはオンラインFIT APの数によって計算されますか?

FIT APのライセンス数は、ACで異なるシリアル番号を使用して設定されたAPテンプレートのライセンス数です。

ACに設定されているAPテンプレートの数が、購入したWSMライセンスの上限を超えた場合はどうなりますか?

ACはWSMに追加できますが、WSMには余分なAPは表示されません。

リアルタイムレポートで現在の時間データを表示できません。なぜですか?

日次リアルタイムレポートのデータ統計は、時間に基づいて収集されます。リアルタイムレポートには、過去1時間またはそれ以前のデータが表示されますが、現在の1時間のデータは表示されません。

シリアル操作を実行するとエラーが発生するのはなぜですか? たとえば、サービスポリシーテンプレートを無線からバインド解除した直後に削除しようとすると、サービスポリシーが無線にバインドされていて削除できないことがWSMから通知されることがあります。

WSMに多数のAPテンプレートまたはVLANが含まれている場合は、情報をデバイスと同期させるために時間がかかります。この期間にシリアル操作を実行すると、エラーが発生することがあります。

特定のカスタムビューのWLANサービスレポートに重複するエントリーが含まれています。なぜですか?

重複するエントリーは、複数のカスタムビューに表示される同じデバイスのデータです。このような問題を回避するには、WLANサービスレポートを表示する複数のカスタムビューに各デバイスが表示されないようにします。

すべてのWSMプロセスが1時間前後にIntelligent Deployment Monitoring AgentのProcessタブで停止された場合、集約されたパフォーマンスデータはWSMデータベースで見つかりません。なぜですか?

WSMでは、1時間ごとにパフォーマンスデータが結合されます。その時点でWSMプロセスを停止すると、操作が中断されます。この中断は、収集されたパフォーマンスデータが集計されず、1時間ごとおよび1日ごとのレポートに表示されないことを意味します。WSMプロセスは1時間ごとに再起動しないことをお薦めします。

ワイヤレスパフォーマンス統計が実際のデータと一致していません。なぜですか?

ワイヤレスパフォーマンス統計情報には、データパケットのトラフィック、合計数、およびレートだけが含まれます。ただし、これらの統計情報には、プロトコル層または物理層の制御パケットの統計情報は含まれません。

クライアントの履歴データが空です。なぜですか?

クライアントのパフォーマンスデータの収集機能が有効になっていることを確認してください。この機能は、既定では無効になっています。この機能を有効にするには、インストールパスの**server/conf**ディレクトリにある**qvdm_wlan.conf**ファイルに**startStaPerfColl=true**という内容を追加し、**imcwlan.exe**プロセスを再起動します。

干渉の場所はAPの場所と同じです。なぜですか?

干渉は通常APの近くに現れ、APとほぼ同じ場所にあります。

複数のAPの帯域幅統計レポートを表示すると、先週の同じ時間と最近3日間の帯域幅統計が異なります。なぜですか。

IMCでは、レポートデータをrawデータ、時間単位データ、および日単位データとして保存できます。AP

帯域幅統計情報レポートの場合、データは次の方法で生成されます。

- **raw data**: IMCは15分ごとにトラフィックデータを収集します。特定の時間のrawデータは2つの統計情報収集操作間で収集されたトラフィックデータの差を統計情報収集間隔(15分)で除算した値。
- **Hourly data**: 時間ごとに、IMCは過去1時間に収集された未加工データの最大値を1時間ごとのデータとして取得します。
- **Daily data**: 毎日00:00に、IMCは、最後の日に収集された1時間ごとのデータの最大値を毎日のデータとして取得します。

ワイヤレストラフィック統計情報レポートの場合、データは次の方法で生成されます。

- **raw data**: IMCは15分ごとにトラフィックデータを収集します。raw dataは、2つの統計情報収集期間に収集されたトラフィックデータ間の差です。
- **Hourly data**: IMCは、最近1時間以内に収集された未加工データの合計を1時間ごとのデータとして取得します。
- **Daily data**: 毎日00:00に、IMCは、最後の日に収集された時間ごとのデータの合計を日次データとして取得します。

過去3日間の履歴データを照会すると、IMCはrawデータを読み取ります。過去1週間の履歴データを照会すると、IMCは時間単位のデータを読み取ります。過去1か月などの長期間の履歴データを照会すると、IMCは日単位のデータを読み取ります。

そのため、次の問題が発生する可能性があります。

- 先週と最近3日間の同じ時間の帯域幅統計は異なります。これは、各APの最大帯域幅が異なる時間に発生するためです。特定の時間のデータは、最近3日間の統計における各APの未処理データの合計であり、最近1週間の統計における各APの1時間ごとのデータの合計です。1時間ごとのデータは、常に最近1時間以内に収集された未処理データの最大値であるため、最近1週間の特定の時間の帯域幅が最近3日間の時間の帯域幅より大きい場合があります。
- 最後の1日のトラフィックの合計が、最後の1週間のトラフィックの合計よりも大きい。これは、最後の1時間に1時間ごとのデータが生成されないためです。最後の1日のトラフィックの合計には最後の1時間のトラフィックが含まれますが、最後の1週間のトラフィックの合計には含まれません。したがって、IMCが1週間未満で導入され、最後の1時間のトラフィックが大きい場合、最後の1日のトラフィックの合計は、最後の1週間のトラフィックの合計よりも大きくなります。
- 先週のトラフィックの合計は、先月のトラフィックの合計よりも大きくなります。これは、毎日のデータが最後の日に生成されないためです。先週のトラフィックの合計には、最後の日のトラフィックが含まれますが、最後の月のトラフィックの合計には含まれません。したがって、IMCのデプロイが1

か月未満で、最後の日のトラフィックが大きい場合、最後の週のトラフィックの合計は、最後の月のトラフィックの合計よりも大きくなります。

用語

AC	アクセスコントローラ。WLANに適合するすべてのAPを制御および管理します。
AC group	2つ以上のACのグループ。1つ以上のACがプライマリ状態で動作してサービスを提供し、他のACがセカンダリ状態で動作しています。プライマリACがダウンすると、セカンダリACがプライマリになってサービスを提供します。
AC port index	ACをFIT APに接続するポートのインデックス。
AC topology	ACと、ACによって管理されるFit AP間の論理接続、およびFit APに接続されているクライアントに関する情報を表示します。
Admin status	デバイスがIMC(ManagedまたはUnmanaged)によって管理されているかどうかを指定します。
AES	Advanced Encryption Standard(AES)。対称的な128ビットブロックデータ暗号化技術です。
AKM type	802.11iでクライアント用に定義されたパスワード管理タイプ。AKMタイプは、none、PSK、または802.1Xです。
A-MPDU	集約MACプロトコルデータユニット。複数のMPDUを結合し、1つのPHYヘッダーだけを持つ。
A-MSDU	集約MACサービスデータユニット。複数のMSDUを結合し、1つのPHYヘッダーだけを持つ。
Antenna gain	空間のある領域に無線エネルギーを向けたり、集中させたりするアンテナの能力の尺度。
AP	アクセスポイント。一方のワイヤレスリンクを他方の有線ネットワークにブリッジします。
AP access port	アクセスデバイスをAPに直接または間接的に接続するポート。
Area access control policy	関係するユーザーグループのエリアへのアクセスを許可または拒否します。
Association	APとクライアント間のアソシエーションは、APによって指定されたSSIDを使用して、ワイヤレスネットワークを介したAPリンクを介して確立されます。
Association congestion rate	アソシエーション要求の総数に対する、リソース不足が原因で失敗したアソシエーションの数の割合。
Attack list	ACに設定されたブラックリスト。ACが攻撃を実行できるデバイスを一覧表示します。
Authentication mode	ComwareベースのACおよびFAT APは、サービスポリシーで設定されたリンク認証モードを使用します。このモードには、Open-System、Shared-Key、またはallがあります。
Authorization mode	802.11でクライアント用に定義された認証モードは、オープンシステムと共有キーです。オープンシステムモードでは、クライアントはワイヤレスアクセス要求がある場合に認証を直接渡します。共有キーモードでは、クライアントはワイヤレスアクセスを提供するデバイスと同じ共有キーを使用する必要があります。
Basic Performance monitoring	WSMは、IMCプラットフォームのパフォーマンス管理機能に基づいて、ワイヤレスデバイスの基本的なパフォーマンスインデックスを監視します。パフォーマンス管理機能は、ワイヤレスデバイスのCPU、メモリー、およびその他のパフォーマンスインデックスをリアルタイムで監視し、監視データをグラフで表示します。

Beacon interval	APがビーコンフレームを送信する時間間隔。
Broadcast SSID	WLANにバインドされたFIT APはSSIDをブロードキャストし、クライアントはこのSSIDを検索してワイヤレスアクセスを行うことができます。
BSS	基本サービスセット。AP無線信号の範囲を指定します。
BSS MAC	基本サービスセットMAC。BSSを識別します。
Built-in monitoring indexes	WSMは、WLANサービス概要ページでのWLANパフォーマンス監視用の組み込み監視インデックス、IMCホームページでのWLANウィジェット、WLANサービスレポート、およびWebサービスとネットワーク評価ページを提供します。
Busy AP	ピークオンラインユーザおよびピーク送信レートの上限に達したか、上限を超えたAP。
CAC	Connect Admission Control(接続アドミッションacキューを使用するクライアントの数を制限して、既存の高プライオリティトラフィックに十分な帯域幅を保証します。
CAPWAP	ワイヤレスアクセスポイントの制御とプロビジョニング。
CCMP	CBC-MACプロトコルを使用したカウンタモード。
Channel	情報または信号が送信者(または送信機)から受信者に送信される一方向の電気通信リンクまたは伝送媒体。
Channel quality	スペクトル保護でモニタチャネルに対して生成される通信品質スコア。
Channels to monitor	スペクトル保護のために無線が監視されるチャネル範囲。
Cipher suite	データの暗号化と復号化に適しています。
Clear	無線通信における全てのデータパケットは暗号化されない。
Client dropping rate	成功したアソシエーションと初期オンラインユーザーの合計に対するクライアントドロップ数の比率。
Client historical track	関係するクライアントの履歴ロケーション情報を表示し、ロケーショントポロジー上のクライアントのトラックを動的に表示します。
Concerned user group	リアルタイムでロケーションを監視するUAMユーザアカウントのグループが含まれます。
Crypto	ワイヤレス通信では、すべてのデータパケットを暗号化する必要があります。
Custom view	1つのACに対してグループ内のFIT APを管理し、トポロジビューで表示できます。
DFS	動的周波数選択は、動作周波数を動的に選択および/または変更して、他のシステムとの干渉(または他のシステムからの干渉)を回避するチャネル割り当て方式です。
DoS	サービス拒否。
DTIM	配信トラフィック通知メッセージ。
Dual-Radio behavior	Fit APでサポートされる無線モード。Both Radios、Radio 1 Only、またはRadio 2 Onlyです。ACにバインドされた出力ネットワークVLAN。
Encryption mode	ワイヤレスネットワーク上で転送するためのデータの処理方法を指定します。暗号化モードは、クリアと暗号化です。
Energy policy	ワイヤレスデバイスの電源を制御します。
ESS	拡張サービスセット。同じSSIDを使用する複数の基本サービスセットで構成されます。

Evaluation report	指定したインデックスの統計情報に従って、特定のエリア、建物、床、または部屋にあるAPおよびクライアントの履歴、要約、および評価結果を表示します。
Evaluation task	スケジュールされた日時に特定のロケーションビューにあるすべてのAPおよびクライアントのロケーションデータを収集します。
FAT AP	クライアントにワイヤレスサービスとセキュリティ認証を提供し、有線ネットワークとワイヤレスネットワーク間のフレームをブリッジします。
Fat AP topology	FAT APおよびそれらに接続されているクライアントを表示します。
FCS error	フレームチェックシーケンスエラーが発生したパケット
FFT	高速フーリエ変換。スペクトルを変化させる方法。
Fit AP	ACによって制御および管理されます。
Fit AP group	オペレーターが特定の権限を割り当てることができる、FIT APのグループが含まれます。
GIS locating	デフォルトマップ上でAPとオンラインクライアントの位置を確認します。
GIS view	既定のマップアイコンを作成して既定のマップに配置し、ワイヤレスホットスポットの物理的な分布をロケーションビューに表示します。
Hotspot	位置ビューは、ホットスポットに関連付けられている場合に、GISマップに表示できます。
Idle AP	ピークオンラインユーザおよびピーク送信レートの下限に達したか、またはそれを超えたAP。
iMC	Intelligent Management Center(IMC)は、H3Cの新世代ネットワーク運用管理プラットフォームです。ネットワーク管理者が統合プラットフォーム上でアプリケーション、リソース、およびユーザーを管理できるように設計されています。
Inter-Client blocking	クライアントが同じWLAN内で相互にアクセスできないようにします。
Level 1 location view	ルートディレクトリと同様に、レベル1ロケーションビューにはデバイスビューとサブロケーションビューが含まれます。
Load balance group	ロードバランシングのためにワークロードが分散される無線のグループ。
Load balancing	ACが管理対象のFIT AP間でワークロードを分散できるようにして、最適なリソース使用率を実現し、過負荷を回避します。
Location view	物理的な位置に基づいて、異なるグループ内のAPを管理します。ロケーションビューは、ワイヤレスの位置特定と無線管理のための基本的なフレームワークを提供します。
Location view topology	APおよびAPに接続されているすべてのクライアントに関するロケーション情報を表示します。
MAC	メディアアクセス制御。
MAC to attack	ACが攻撃を実行できるデバイスのMACアドレス。
MAP	メッシュアクセスポイント。1つまたは複数のアクセスポイントと同じ場所にあるメッシュポイントです。
Max RSSI	最大受信信号強度インジケータ。
MCS set	802.11anまたは802.11gnタイプの無線レートを設定するために使用される変調および符号化スキームセット。

Mesh	マルチチップ無線リンクを介して相互に通信する2つ以上のAPで構成される無線LAN。
Mesh interface	メッシュプロファイルがバインドされるワイヤレス論理インターフェース。メッシュネットワークを確立するには、メッシュインターフェースにポートセキュリティ設定が必要です。
Mesh link	メッシュネットワーク上の2つのAP間のワイヤレスリンク。
Mesh peer MAC	ローカルAPとのメッシュリンクを確立したピアAPのMACアドレス。
Mesh profile	メッシュプロファイルは、ACとAPが相互にメッシュサービスを提供できる1つまたは複数の無線にバインドできます。
Mesh topology	メッシュネットワーク上のデバイス接続を表示します。メッシュトポロジには、ACとFit AP間の接続を表示するACメッシュトポロジと、FAT AP間の接続を表示するFAT APメッシュトポロジがあります。
MIC check error	メッセージ完全性チェックエラーが発生したパケット。
MKD	メッシュキーディストリビュータ。
Monitored channel	スペクトル保護のために無線が監視されるチャネル。
Monitoring clients	関連するユーザーグループのオンラインユーザアカウントとそのロケーションを表示し、ロケーショントポロジー上のロケーション変更をリアルタイムで追跡します。
MP	メッシュポイント。メッシュネットワーク上のノードです。
MP policy	操作メッシュポイントに適用されるポリシー。
MPDU	MACプロトコルデータユニット。
MPP	メッシュポータルポイント。1つまたは複数のポータルと同じ位置にあるメッシュポイントです。
MSDU	MACサービスデータユニット。
Obstacle	コンクリート壁、窓、金属バリアなど、無線信号の伝送をブロックまたは妨害する物体。
Operation status	デバイスのオンライン状態(OnlineまたはOffline)を指定します。
OUI	Organizationally Unique Identifier(組織固有識別子)。所有者を識別するためにIEEEによって割り当てられた6桁の16進数で構成されます。
PD	受電装置。イーサネット経由の電源装置が必要です。
Periodical report	比較と分析のためのデータを提供するために、定義された期間とテンプレートに従ってレポートが生成されます。
Permit list	許可されたOUI、SSID、およびMACアドレスを含む、ACに設定されたホワイトリスト。
Permitted area	ロケーションビューでは、オペレーターはエリアアクセスコントロールポリシーが適用されるエリアを編集および設定できます。
Permitted MAC	ACによって許可されるワイヤレスデバイスのMACアドレス。
Permitted OUI	ACによって許可されているワイヤレスデバイスベンダーのOUI。
Permitted SSID	ACによって許可されたSSID。
PHY error	物理層エラーがあるパケット。

Physical topology	ComwareベースのACと特定のComwareベースのfit AP間の物理接続を表示します。
PoE	Power over Ethernet。ツイストペア上のイーサネット銅線ポートを介して、リモートの受電装置に電源を供給します。
Preamble type	Fit APのプリアンブルタイプ:ShortまたはLong。Shortタイプは、Fit APがショートまたはロングプリアンブルフレームを送信することを示します。Longタイプは、Fit APがロングプリアンブルフレームだけを送信することを示します。
PSE	受電装置に電力を供給する電力供給装置。
QoS	サービス品質。
Radio policy	無線パラメーターのセットを定義します。
Radio port	無線信号を送信するためにアンテナが設置されているポート。APには通常、2つの無線ポートがあります。
Radio type	無線で使用される無線プロトコル。WSMは、802.11a、802.11b、802.11g、802.11bg、802.11at、802.11an、802.11gn、802.11n(2.4GHz)、802.11bgn、802.11nおよび802.11n(5GHz)の無線プロトコルをサポートしています。
RADIUS	リモート認証ダイヤルインユーザーサービス。クライアント/サーバーモデルを使用する分散情報対話プロトコルです。不正アクセスからネットワークを保護できます。高度なセキュリティとリモートユーザーアクセスの両方を必要とするネットワーク環境でよく使用されます。
Rate set	無線タイプ802.11a、802.11b、および802.11gで使用される、サポートされるレート、必須レート、およびディセーブルレートのセットが含まれます。
Realtime monitoring	WSMは、管理可能なComwareベースのFIT AP、およびオンラインクライアントをリアルタイムで監視します。
Realtime report	最新の統計情報、または特定の期間の統計情報を表示します。
RF	無線周波数。
Rogue AP	ネットワーク上の無許可または悪意のあるAP。
Rogue client	ネットワーク上の許可されていないクライアントまたは悪意のあるクライアント。
RRM	**Radio Resource Management**: RRM設定、RRM調整グループ、レートセット、MCSセット、およびWIDS検出ルールを管理します。
RRM calibration group	無線チャネルパラメーターと電力を計算することによって、チャネルのライフタイムと電力のライフタイムを自動的に変更できる無線のグループが含まれます。
RSN	RSNアソシエーションを確立できる堅牢なセキュリティネットワーク。
RSSI	無線信号強度インジケータ。
RTS	送信要求。通信回線上でのデータ送信を要求するEIA/TIA-232制御信号。
Rx lifecycle	FIT APがフレームをキャッシュに保持する最大時間。
Scale	建物の実際の長さに対する背景イメージの比率を指定します。
Scan channel	Fit APはチャネルをアクティブまたはパッシブにスキャンできます。アクティブスキャンでは、Fit APはクライアントをシミュレートしてプローブ要求を他のFit APに送信します。パッシブスキャンでは、Fit APはプローブ要求を送信しません。

Security IE	セキュリティ情報要素。FIT APによって送信されるビーコンおよびプローブ応答フレームに含まれます。セキュリティIEには、RSNおよびWPAが含まれます。
Short GI	短いガードインターバル。送信が相互に干渉しないことを保証します。
SN	APの製品シリアル番号。
SNR	信号ノイズ比。
Spectrum analysis	ワイヤレス信号の周波数スペクトルを分析します。
SSH	Secure Shell。強力な認証と安全な通信を使用して、ネットワーク経由で別のコンピュータにログインするためのユーティリティです。
SSID	サービスセット識別子。ワイヤレスネットワークサービスのセットを識別します。
Sublocation	レベル1の位置ビューに直接または間接的にアタッチされます。
Swept spectrogram	スペクトル保護のためにスペクトルをスキャンします。
Synchronize fit AP	最新のFit AP構成をACからWSMに同期化します。
Team	サービスを提供する仮想ACとして動作する複数のACが含まれます。チーム内のACの役割は、スレーブ、マスター、優先マスター、または不明です。
TKIP	Temporal Key Integrity Protocol(一時キー完全性プロトコル)。
TopN	指定したインデックスを持つ上位N個のアイテム。
TPC	送信電力制御。ワイヤレスネットワーク間の不要な干渉を防止するメカニズムです。
traceroute	IMCサーバーからの管理対象ACの到達可能性をテストし、接続の問題をトラブルシューティングします。
TU	時間単位。1,024マイクロ秒に相当します。
UAM	User Access Manager。ネットワークへのユーザアクセスを制御するIMCのサービスコンポーネントです。
Virtual AP	WSMは、ComwareベースのAPをシミュレートして、ワイヤレスネットワーク信号を送信できます。シミュレーション結果は、自動ネットワークプランニングに使用できます。
VSC	仮想サービスコミュニティ。ACによって管理されるFIT APによって提供される無線ネットワークサービスのセットを指定します。
WDS	無線分散システム。IEEE 802.11ネットワーク内のアクセスポイントの無線相互接続を可能にします。
WIDS	不正なワイヤレスアクセスを検出するWireless Intrusion Detection System(ワイヤレス侵入検知システム)。
WIDS detection rule	ACは、この規則を使用してワイヤレスデバイスの有効性を確認します。
Wireless custom topology	ワイヤレスカスタムビューでのAC、これらのACによって管理されるFit AP、およびFit APに接続されているクライアントに関する情報を表示します。
Wireless device topology	WSMで管理されているすべてのACとFAT AP、およびAC、FAT AP、FIT AP、クライアント間の論理接続を表示します。

WMM	WiFiマルチメディアは、優先度の高いパケットを優先的に送信するように設計されたワイヤレスQoSプロトコルであり、ワイヤレスネットワーク内の音声およびビデオアプリケーションに対してより優れたQoSサービスを保証します。
Work mode	Fit APが動作しているモード。Workモードには、Normal、Monitor、およびHybridがあります。Normalモードでは、Fit APはワイヤレスアクセスを提供し、不正侵入を検出しません。Monitorモードでは、Fit APは不正侵入を検出し、ワイヤレスアクセスを提供しません。Hybridモードでは、Fit APはワイヤレスアクセスを提供し、不正侵入を検出します。
Worst AP	アウトオブサービスレート、アソシエーション輻輳レート、またはクライアントドロップレートのしきい値に達したか、しきい値を超えたAP。
WPA	WiFi Protected Accessは、ワイヤレスセキュリティソリューションです。WPA-PSKモード(パーソナルモードとも呼ばれます)またはWPA-802.1Xモード(WPA-エンタープライズモードとも呼ばれます)で動作します。WPA-PSKモードでは、WPAは事前共有キーまたはパスワードに基づいて認証を実行します。WPA-802.1Xモードでは、WPAは802.1X RADIUSサーバーとEAPを使用して認証を行います。
WSM	Wireless Service Manager。WLAN管理機能を提供しネットワーク管理を実装するためのWLAN管理機能を提供します。