CHAPTER 9

コントローラとアクセス ポイントの設定

この章では、Cisco WCS データベースでのコントローラとアクセス ポイントの設定方法について説明します。この章の内容は、次のとおりです。

- コントローラの追加（P. 9-2）
- 複数の国番号の設定（P. 9-4）
- コントローラの検索（P. 9-6）
- ユーザ認証の順序の管理（P. 9-7）
- Audit Status の表示（対コントローラ）（P. 9-8）
- 最新のネットワーク監査レポートの表示（P. 9-9）
- コントローラに対する負荷ベース CAC の有効化（P. 9-10）
- 高密度の有効化（P. 9-12）
- 802.3 ブリッジの設定（P. 9-16）
- RRM しきい値のコントローラの設定（802.11a/n または 802.11b/g/n 用）（P. 9-17）
- 個々のコントローラに対する EDCA パラメータの設定（P. 9-18）
- SNMPv3 の設定（P. 9-19）
- Autonomous の LWAPP への移行のサポート（P. 9-20）
- Autonomous の LWAPP への移行のサポート（P. 9-20）
- Audit Status の表示（対アクセス ポイント）（P. 9-29）
- アクセス ポイントの検索（P. 9-30）
- Spectrum Expert の設定（P. 9-31）
- 有線ゲストのアクセスの設定（P. 9-34）

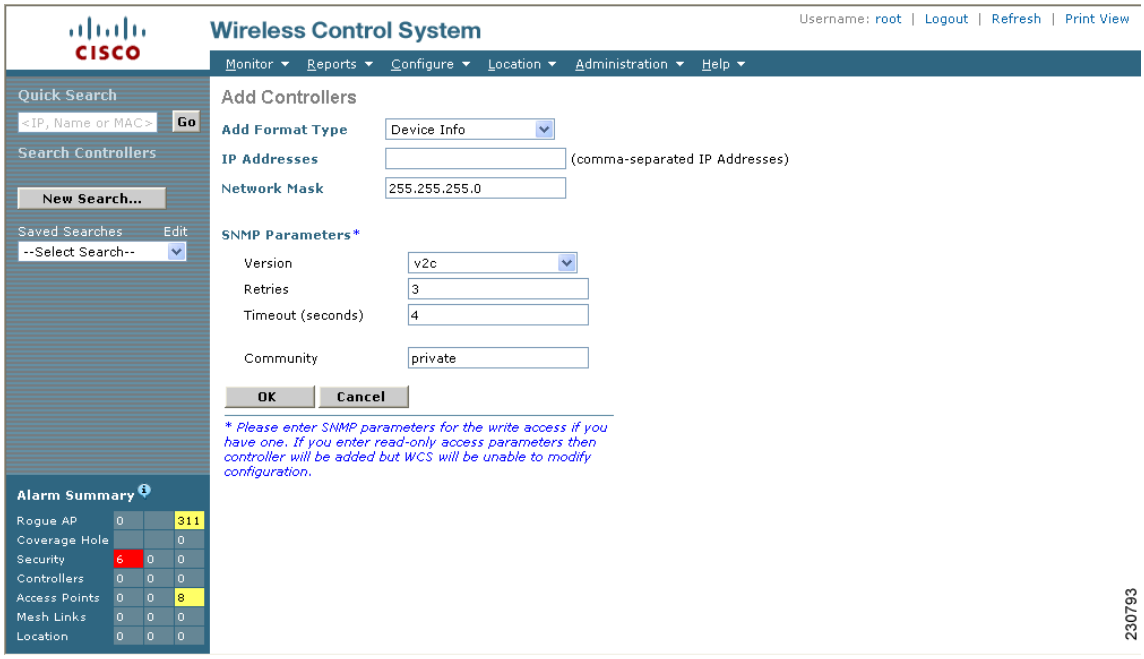
コントローラの追加

コントローラは 1 つずつまたはバッチで追加することができます。次の手順に従って、コントローラを追加します。

ステップ 1　**Configure > Controllers** の順に選択します。

ステップ 2　Select a command ドロップダウン メニューから **Add Controller** を選択し、**GO** をクリックします。Add Controller ウィンドウが表示されます（図 9-1 参照）。

図 9-1　Add Controller ウィンドウ



ステップ 3　次のいずれかを選択します。

1 つのコントローラを追加するか、カンマを使用して複数のコントローラを区切る場合は、Add Format Type ドロップダウン メニューを Device Info のままにします。

CSV ファイルのインポートにより複数のコントローラを追加する場合は、Add Format Type ドロップダウン メニューから **File** を選択します。CSV ファイルを使用すると、独自のインポート ファイルを生成して必要に応じてデバイスを追加できます。

（注）　IPsec を使用した GRE リンクや複数の断片を持つ下位の MTU リンクを超えて WCS にコントローラを追加している場合は、MaxVar Binds PerPDU の調整が必要な場合があります。設定されている値が高すぎる場合は、WCS へのコントローラの追加は失敗します。MaxVarBindsPerPDU の設定を調整する手順は、次のとおりです。1) WCS を停止します。2) WCS を実行しているサーバ上の Open SnmpParameters.properties ファイルの場所へ移動します。3) MaxVarBindsPerPDU を編集して 50 以下にします。4) WCS を再起動します。

ステップ 4　Device Info を選択した場合は、追加するコントローラの IP アドレスを入力します。複数のコントローラを追加するには、IP アドレスの文字列の間にカンマを使用します。

File を選択した場合は、**Browse...** をクリックしてインポートする CSV ファイルの場所を探します。

ステップ 5　**OK** をクリックします。

複数の国番号の設定

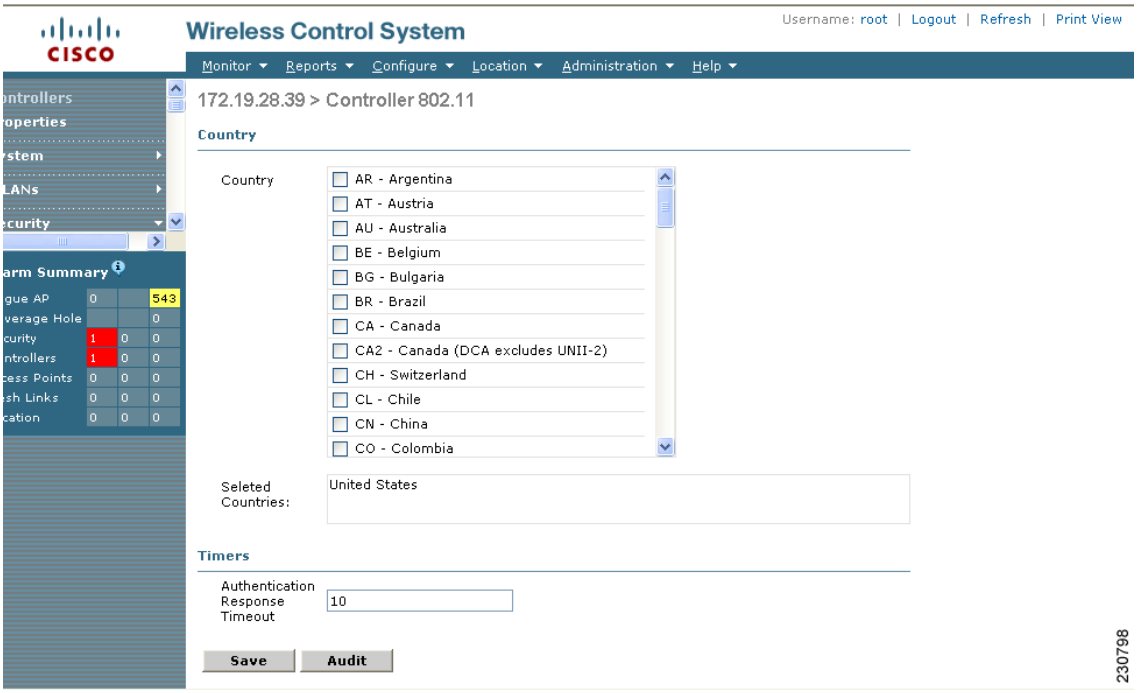
モビリティ グループの一部ではない単一のコントローラを複数の国をサポートするように設定する手順は、次のとおりです。

ステップ 1　**Configure > Controllers** の順に選択します。

ステップ 2　国を追加しているコントローラを選択します。

ステップ 3　左側のサイドバーのメニューから、**802.11 > General** の順に選択します。Controller 802.11 ウィンドウが表示されます（図 9-2 参照）。

図 9-2　Controller 802.11



ステップ 4　チェックボックスをクリックして、追加する国を選択します。アクセス ポイントは、さまざまな規制要件を持つ多くの国で使用できるように設計されています。国の規制に準拠するように国番号を設定できます。

（注）　操作する国向けに設計されていない場合は、アクセス ポイントは正しく動作しない場合があります。たとえば、米国規制区域に含まれる部分番号 AIR-AP1030-A-K9 のアクセス ポイントは、オーストラリアでは使用できません。必ず自国の規制区域に合ったアクセス ポイントを購入するようにしてください。製品ごとにサポートされている国番号の一覧については、http://www.cisco.com/warp/public/779/smbiz/wireless/approvals.html を参照してください。

ステップ 5　認証応答がタイムアウトするまでの時間を秒単位で入力します。

ステップ 6　**Save** をクリックします。

コントローラの検索

左側のサイドバーのコントロールを使用して、カスタム検索を作成および保存します。

- **New Search** ドロップダウン メニュー：Search Controllers ウィンドウを開きます。Search Controllers ウィンドウを使用して、検索を設定、実行および保存します。
- **Saved Searches** ドロップダウン メニュー：保存済みのカスタム検索を一覧表示します。保存済みの検索を開くには、Saved Searches リストから選択します。
- **Edit Link**：Edit Saved Searches ウィンドウを開きます。保存済みの検索を Edit Saved Searches ウィンドウで削除できます。

Search Controllers ウィンドウで、次のパラメータを設定できます。

- Search for controller by：すべてのコントローラ、IP アドレス、またはコントローラ名を選択します。
- Select a Network：すべてのネットワークまたは個々のネットワークを選択します。
- Save Search：Save Search チェックボックスをオンにして Save Search テキスト フィールドに名前を入力し、Saved Searches ドロップダウン リストに検索を保存します。
- Search by Audit Status：次の監査ステータスで検索します。
  - Not Available：監査ステータスは使用できない。
  - Identical：最新の監査で、設定の相違は検出されなかった。
  - Mismatch：最新の監査で、WCS とコントローラ間の設定の相違が検出された。
- Items per page : Search Results ウィンドウに表示する、検出済み項目の数を選択します。範囲は、ウィンドウごとに 10 ～ 100 項目です。デフォルトは 20 です。

GO をクリックすると、コントローラ検索結果が表示されます。

表 9-1　検索結果

パラメータ	オプション
IP Address	コントローラ管理インターフェイスのローカル ネットワーク IP アドレス。タイトルをクリックすると、昇順から降順に並べ替えられます。リストの IP アドレスをクリックすると、コントローラ詳細の概要が表示されます。
WCS	ユーザ定義の WCS 名。
Controller Name	タイトルをクリックすると、昇順から降順に並べ替えられます。
タイプ	コントローラの種類。Cisco 2000 Series、Cisco 4100 Series、Cisco 4400 Series など。
Location	地理的位置（キャンパスやビルディングなど）。タイトルをクリックすると、昇順から降順に並べ替えられます。
Mobility Group Name	コントローラまたは WPS グループの名前。
Reachability Status	到達可能または到達不能。タイトルをクリックすると、昇順から降順に並べ替えられます。

ユーザ認証の順序の管理

コントローラの管理ユーザの認証に使用する認証サーバの順序を制御できます。

ステップ 1　**Configure > Controllers** の順に選択します。

ステップ 2　IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、**Management > Authentication Priority** の順に選択します。

ステップ 4　最初にローカル データベースが検索されます。RADIUS または TACACS+ のどちらかを次の検索対象に選択します。ローカル データベースを使用した認証に失敗した場合に、コントローラは次の種類のサーバを使用します。

ステップ 5　**Save** をクリックします。

Audit Status の表示（対コントローラ）

Configure > Controllers ウィンドウの Audit Status 列には、最新の監査に基づいた各コントローラの監査ステータスが表示されます。選択したコントローラのネットワーク監査レポートも確認できます。レポートには、監査の時刻、選択したコントローラの IP アドレス、および同期ステータスが表示されます。

ステップ 1　**Configure > Controllers** の順に選択します。

ステップ 2　最新の監査レポートは、次の 2 種類のいずれかの方法で表示できます。

監査レポートが必要なコントローラのチェックボックスをオンにします。Select a Command ドロップダウン メニューから **Audit Now** を選択し、**GO** をクリックします。この方法では、ネットワーク監査タスクからのレポートが表示され、コントローラごとのオンデマンドの監査は表示されません。

または

Audit Status 列の値をクリックして、選択したコントローラの最新の監査詳細ページへ移動します。この方法で表示される情報は、Reports メニューの Network Audit レポートと似ていますが、このレポートはインタラクティブでコントローラごとになっています。

（注）　マウスを Audit Status 列の値の上に置くと、最新監査の時刻が表示されます。

Audit Report には、デバイス名、設定名、監査の時刻、各設定に対する監査ステータス（Mismatch または Identical）、各設定に対する属性（AP Group Name、IP アドレス）、WCS の値、およびコントローラの値が表示されます。

オンデマンドの監査レポートを実行するには、レポートを実行させるコントローラを選択し、Select a command ドロップダウン メニューから **Audit Now** を選択します。オンデマンド監査レポートを実行して設定の相違が検出されると、既存のコントローラの値か WCS の値のどちらを保持するかを選択できます。

ステップ 3　監査の結果、設定の相違が検出された場合、コントローラ上の WCS 値を復元するか、コントローラの値を更新して WCS をコントローラに同期させるかのどちらかが可能になります。**Restore WCS Values** または **Refresh Controller Values** を選択します。

最新のネットワーク監査レポートの表示

Network Audit Report には、監査の時刻、選択したコントローラの IP アドレス、および同期ステータスが表示されます。

（注）　この方法では、ネットワーク監査タスクからのレポートが表示され、コントローラごとのオンデマンドの監査は表示されません。

選択したコントローラに対する最新のネットワーク監査レポートを表示する手順は、次のとおりです。

ステップ 1　**Configure > Controllers** の順に選択します。

ステップ 2　該当するコントローラのチェックボックスをオンにします。

ステップ 3　Select a command ドロップダウン メニューから、**View Latest Network Audit Report** を選択します。

ステップ 4　**Go** をクリックします。

Audit Summary には、監査の時刻、選択したコントローラの IP アドレス、および監査ステータスが表示されます。設定の相違がある場合、その詳細が表示されます。

General and Schedule タブを使用して、Audit Report パラメータを変更します。

（注）　**All Controllers** ページから、**Audit Status** 列の値をクリックして、選択したコントローラの最新の監査詳細ページを表示します。この方法で表示される情報は、Reports メニューの Network Audit レポートと似ていますが、このレポートはインタラクティブでコントローラごとになっています。

（注）　オンデマンドの監査レポートを実行するには、レポートを実行させるコントローラを選択し、Select a command ドロップダウン メニューから **Audit Now** を選択します。オンデマンド監査レポートを実行して設定の相違が検出されると、既存のコントローラの値か WCS の値のどちらを保持するかを選択できます。

コントローラに対する負荷ベース CAC の有効化

負荷ベースの Call Admission Control（CAC; コール アドミッション制御）で取り入れられている測定方式では、それ自体からのすべてのトラフィック タイプによって共同チャネル アクセス ポイントで消費される帯域幅や、共同設置チャネルの干渉によって消費される帯域幅が考慮されています。また、負荷ベース CAC では PHY やチャネル障害から生じる帯域幅の消費もカバーされます。

負荷ベース CAC では、RF チャネル、チャネル干渉、およびアクセス ポイントが許容できるその他のコールが、アクセス ポイントによって定期的に測定および更新されます。そのコールをサポートするための未使用の帯域幅がチャネルに十分ある場合のみ、アクセス ポイントによって新しいコールが許容されます。そうすることにより、負荷ベース CAC はチャネルの加入過多を防ぎ、WLAN の負荷および干渉のすべての条件の下で QoS を維持します。

コントローラ テンプレートに対して負荷ベース CAC を有効にするには、「音声パラメータ テンプレートの設定（802.11a/n または 802.11b/g/n 用）」の項（P. 10-61）を参照してください。

WCS Web インターフェイスを使用してコントローラに対して負荷ベース CAC を有効にする手順は、次のとおりです。

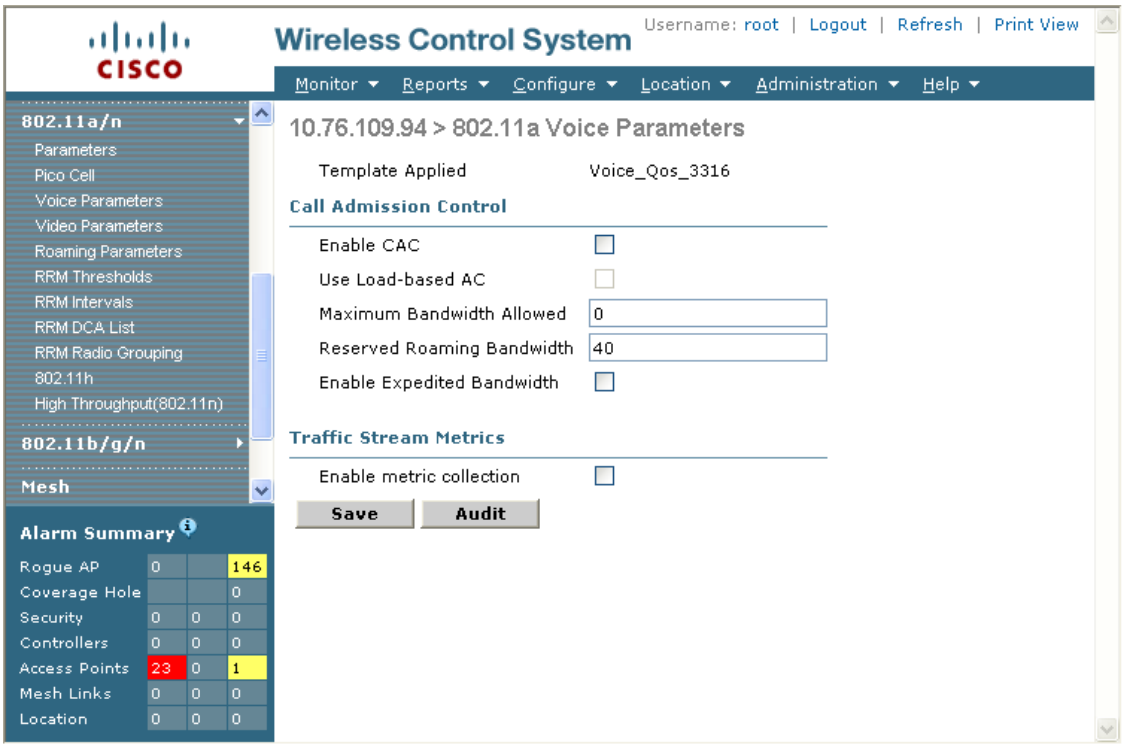
ステップ 1　**Configure > Controllers** の順に選択します。

ステップ 2　コントローラの IP アドレス リンクをクリックします。

ステップ 3　802.11a/n または 802.11b/g/n の下の **Voice Parameters** をクリックします。

802.11a/n (or 802.11b/g/n) Voice Parameters ページが表示されます（図 9-3 参照）。

図 9-3　802.11a/n Voice Parameters ページ



ステップ 4　チェックボックスをオンにして、帯域幅の CAC を有効にします。VoIP 通話中にエンド ユーザが許容できる音声品質と感じるよう、パケットはエンドポイントから別のエンドポイントまで低遅延、低パケット損失で配送される必要があります。異なるネットワーク負荷の下で QoS を維持するには、Call Admission Control（CAC; コール アドミッション制御）が必要です。アクセス ポイントでの CAC により、アクセス ポイントは、ネットワークの輻輳時でも QoS が制御された状態を維持し、許容する最大の通話数を許容できる数に保つことができます。

ステップ 5　負荷ベース CAC をこの無線帯域で有効にするかどうかを指定します。それにより、それ自体からのすべてのトラフィック タイプによって共同チャネル アクセス ポイントで消費される帯域幅や、共同設置チャネルの干渉によって消費される帯域幅を考慮した測定方式を取り入れます。

ステップ 6　許容する最大帯域幅のパーセンテージを入力します。

ステップ 7　予約するローミング帯域幅のパーセンテージを入力します。

ステップ 8　緊急コール用に CAC の拡張として緊急帯域幅を有効にする場合は、チェックボックスをオンにします。より高い優先度が Traffic Specification（TSPEC; トラフィック仕様）の要求に与えられるように、Cisco Compatible Extensions バージョン 5（CCXv5）準拠の優先帯域幅の Information Element（IE; 情報要素）が必要となります。

ステップ 9　メトリック収集を有効にする場合は、Enable metric collection チェックボックスをオンにします。トラフィック ストリーム メトリックは、無線 LAN での VoIP に関する一連の統計で、無線 LAN の QoS について報告します。アクセス ポイントで測定値を収集するには、トラフィック ストリーム メトリックが有効であることが必要です。これを有効にすると、コントローラは 802.11b/g/n インターフェイスに対して 90 秒ごとにアソシエートされたすべてのアクセス ポイントからの統計データの収集を開始します。VoIP またはビデオを使用している場合は、この機能を有効にします。

ステップ 10　**Save** をクリックします。

高密度の有効化

高密度展開は、Cisco および Intel の Business Class Suite Version 2 のイニシアチブとともに Cisco Unified Wireless Network Software Release 4.1 を使用することで可能になります。

高密度ネットワーク機能は、大規模な、マルチセルの高密度無線ネットワーク向けに設計されています。そのようなネットワークでは、多数の Lightweight アクセス ポイントを含むサイトを実装して帯域幅の累積負荷を管理しながら、アクセス ポイント間のコンテンションを減らし、サービスの質を維持することは困難な場合があります。RF チャネルのキャパシティを最適化し、ネットワークのパフォーマンスを向上させるには、高密度（またはピコ セル）モードのパラメータを導入します。

この機能を使用すると、最適な高密度展開を作成するために、Intel のクライアント デバイスと Cisco Aironet lightweight アクセス ポイントの送信電力、受信感度のしきい値、およびクリア チャネル評価感度のしきい値を手動で設定できます。高密度をサポートするクライアントが高密度対応アクセス ポイントにアソシエートするときは、アクセス ポイントでアドバタイズされた受信感度のしきい値、CCA 感度のしきい値、および送信電力レベルに従うようにクライアントに指示する、特定の 802.11 Information Element（IE; 情報要素）が交換されます。これらの 3 つのパラメータにより、アクセス ポイントとクライアントがパケットの転送に利用できるチャネルと見なす前に、受信信号強度を調整して、有効なセルのサイズを縮小します。このように高密度領域全体にわたり、すべてのアクセス ポイントとクライアントで信号標準が上がると、アクセス ポイントは互いの干渉を最小限に抑え、周囲や遠隔の不正信号を管理して、近接して展開されます。

（注） 高密度はデフォルトではオフになっています。あらかじめ定められている値を変更する場合は、展開の際にリスクを伴います。シスコのテクニカル サポートからのアドバイスを受けずに無線 LAN 内でピコ セル機能を設定しようとしないでください。標準以外のインストールはサポートされていません。

これらの設定変更とともにさらに最適化できるピコ セル展開は、次のとおりです。

要件

高密度に関する制約事項は、次のとおりです。

- Cisco lightweight アクセス ポイント（AP1030 および 1500 シリーズのメッシュ アクセス ポイント以外）と、Intel PRO/Wireless 3945ABG および Intel Wireless WiFi Link 4965AGN クライアントのみがサポートされています。
- 高密度展開を備えた 802.11a/n ネットワークのみがサポートされています。

（注） すべてのクライアントと lightweight アクセス ポイントで高密度機能がサポートされている、新しい WLAN 展開でのみ高密度を使用することをお勧めします。

高密度をサポートするためのコントローラの最適化

高密度をサポートするようにコントローラを最適化するには、ピコ セル モード v2 を有効にする必要があります。高密度ネットワークでセル間のコンテンションの問題を緩和するには、比較的調和が取れるように、アクセス ポイントとクライアント レシーバの感度、CCA の感度、送信電力パラメータを調整します。これらの変数を調整することで、アクセス ポイントとクライアントがチャネルをパケット転送のために十分クリアであると見なす前に、送信電力を下げずに必要な受信電力を

上げて有効なセルのサイズを縮小できます。これらの類似値は、GUI の Controller Templates 部分で設定できます。コントローラ テンプレートの追加（P. 10-2）を参照してください。高密度を設定する手順は、次のとおりです。

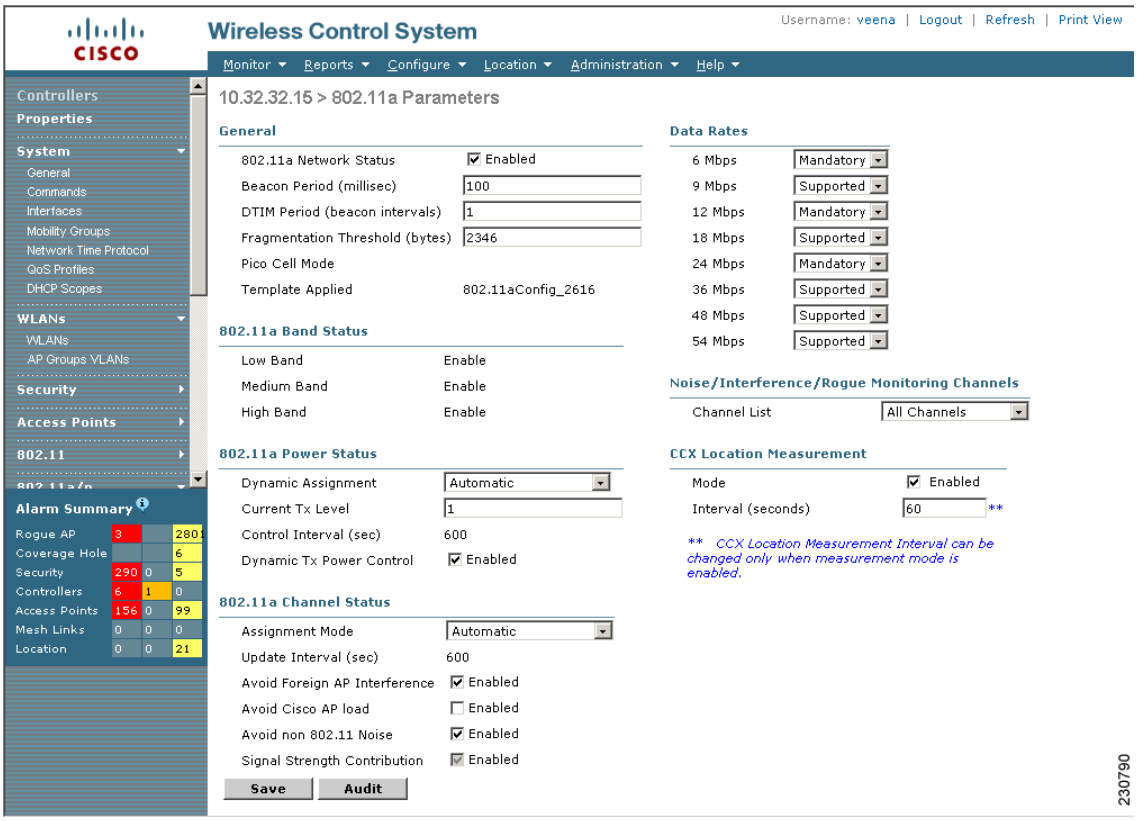
（注）　ピコ セルを有効にする場合は、自動 RF のデフォルト値は、Intel 3945ABG クライアント向けに示された値に合わせて変更されます。送信電力は 10dBm、CCA 感度のしきい値は -65dBm、レシーバ感度のしきい値は -65dBm に設定されます。

ステップ 1　**Configure > Controllers** の順に選択します。

ステップ 2　**802.11a/n > Parameters** に移動して、802.11a/n Network Status チェックボックスが有効になっていないことを確認します。

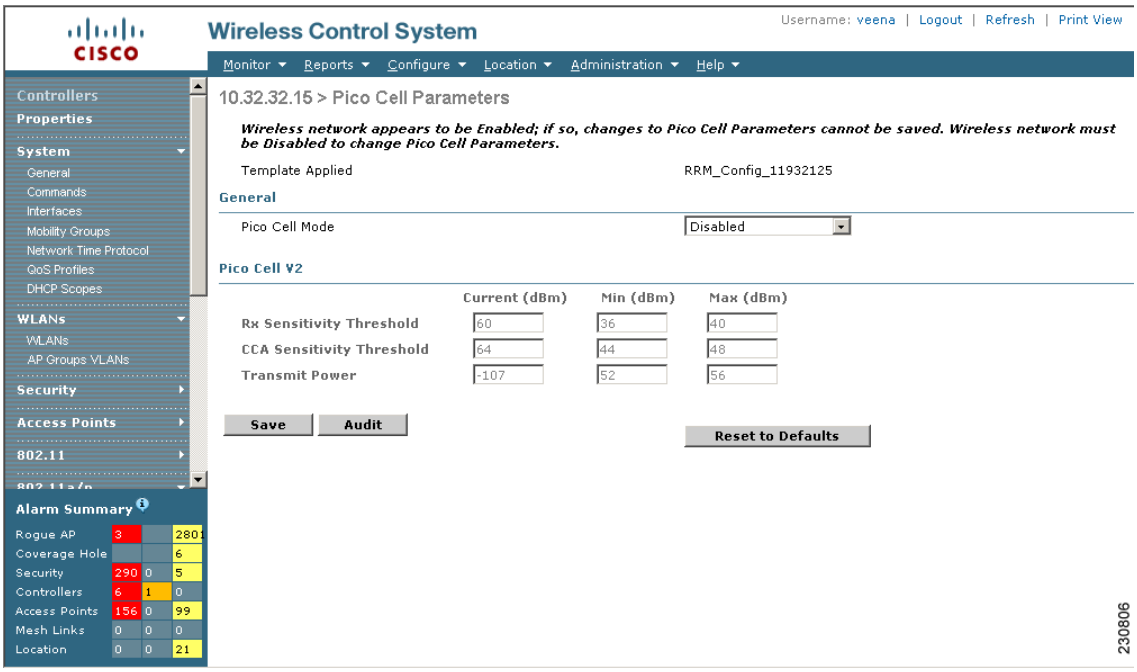
ステップ 3　左側のサイドバーのメニューから、**802.11a/n > Parameters** の順に選択します。図 9-4 に示すウィンドウが表示されます。

図 9-4　ピコ セル パラメータ



ステップ 4　このウィンドウの General 部分に Pico Cell Mode パラメータが表示されます。このパラメータの辺りにマウスを置いて表示されたリンクをクリックすると、図 9-5 のようなウィンドウが表示されます。左側のサイドバーのメニューから直接 **802.11a/n > Pico Cell** を選択しても、このウィンドウを表示できます。

図 9-5　Pico Cell Parameters ウィンドウ



（注）　Pico Cell Mode パラメータが Disabled または V1 に設定されている場合、Pico Cell V2 パラメータは灰色になっています。

ステップ 5　Pico Cell Mode ドロップダウン メニューから **V2** を選択します。V2 を選択すると、アクセス ポイントとクライアントの高密度パラメータが同じ値を共有し、通信を対称にします。ほとんどのネットワークでデフォルトの Rx 感度、CCA 感度、送信電力の最大値と最小値はシスコの推奨値を示していますが、この選択によってこれらの値を入力することもできます。

（注）　シスコによる買収前に購入したレガシーの Airespace ブランドの製品を使用している場合は、V1 を選択してください。ピコ セル モードを有効にする場合は、V2 を選択することをお勧めします。

ステップ 6　Rx 感度のしきい値は、802.11a/n 無線通信機の目的のレシーバ感度に基づいて設定します。Current 列は、アクセス ポイントとクライアントで現在設定されているものを示し、Min 列と Max 列は、アクセス ポイントとクライアントが適応する範囲を示します。Current、Min、Max 列の有効範囲は -127 ～ 127dBm です。デフォルトは -65dBm（Current）、-127dBm（Min）、127dBm（Max）です。この範囲外のレシーバ信号強度値はブロックされます。

ステップ 7　CCA 感度のしきい値は、アクセス ポイントまたはクライアントがチャネルをアクティビティのために十分クリアであると見なすときに基づいて設定します。Current 列は、アクセス ポイントとクライアントで現在設定されているものを示し、Min 列と Max 列は、アクセス ポイントとクライア

ントが適応する範囲を示します。Current、Min、Max 列の有効範囲は -127 ～ 127dBm です。デフォルトは -65dBm（Current）、-127dBm（Min）、127dBm（Max）です。この範囲外の CCA 値はブロックされます。

ステップ 8　クライアントによって使用される無線の送信電力を指定します。Current、Min、Max 列の有効範囲は -127 ～ 127dBm です。デフォルトは 10dBm（Current）、0dBm（Min）、17dBm（Max）です。

ステップ 9　**Save** をクリックして、これらの値を保存します。WCS の設定がコントローラの設定とどのくらい合っているかの比較を表示するには、**Audit** をクリックします。**Reset to Defaults** を選択する前に、802.11a/n ネットワークをオフにする必要があります。

ステップ 10　**802.11a/n > Parameters** に戻り、802.11a /n Network Status チェックボックスをオンにしてネットワークをオンに戻します。

802.3 ブリッジの設定

コントローラは、一般的にレジやレジ サーバで使用されるような 802.3 フレームおよびそれらを使用するアプリケーションをサポートしています。ただし、これらのアプリケーションはコントローラと連動させるには、802.3 フレームをコントローラ上にブリッジする必要があります。

未加工の 802.3 フレームのサポートにより、コントローラを、IP 上で実行していないアプリケーション用の IP 以外のフレームにブリッジできるようになります。この未加工の 802.3 フレームの形式のみが、現在サポートされています。

WCS Release 4.1 以降を使用して、802.3 ブリッジを設定できます。手順は次のとおりです。

ステップ 1　**Configure > Controllers** の順に選択します。

ステップ 2　**System > General** の順にクリックして、General ページに移動します。

ステップ 3　802.3 Bridging ドロップダウン メニューから **Enable** を選択してコントローラ上の 802.3 ブリッジを有効にするか、**Disable** を選択してこの機能を無効にします。デフォルト値は Disable です。

ステップ 4　**Save** をクリックして、変更内容を確定します。

RRM しきい値のコントローラの設定（802.11a/n または 802.11b/g/n 用）

802.11a/n または 802.11b/g/n の RRM しきい値のコントローラを設定する手順は、次のとおりです。

ステップ 1　**Configure > Controller** の順に選択します。

ステップ 2　該当するコントローラの **IP address** をクリックして、**Controller Properties** ページを開きます。

ステップ 3　左側のサイドバー メニューから **802.11a/n > RRM Thresholds** または **802.11b/g/n > RRM Thresholds** を選択します。

ステップ 4　Coverage Thresholds、Load Thresholds、Other Thresholds、および Noise/Interference/Rogue Monitoring Channels に対して変更が必要な場合には、変更します。

（注）　Coverage Thresholds Min SNR Level (dB) パラメータを調整すると、Signal Strength (dB) の値が自動的にこの変更に反映されます。Signal Strength (dB) パラメータにより、SNR 値を調整する際のカバレッジのしきい値の対象範囲に関する情報が提供されます。

ステップ 5　**Save** をクリックします。

個々のコントローラに対する EDCA パラメータの設定

802.11a/n および 802.11b/g/n に対する EDCA パラメータ（EDCA プロファイル設定と Streaming MAC Enable 設定）は、個々のコントローラまたはコントローラ テンプレートのいずれかを使用して、音声 QoS サポートを向上させるように設定できます。コントローラ テンプレートの設定の手順については、「コントローラ テンプレートによる EDCA パラメータの設定」の項（P. 10-64）を参照してください。

個々のコントローラに対する 802.11a/n または 802.11b/g/n EDCA パラメータを設定する手順は、次のとおりです。

ステップ 1　**Configure > Controllers** の順に選択します。

ステップ 2　該当するコントローラの **IP Address** をクリックします。

ステップ 3　左側のサイドバー メニューから **802.11a/n > EDCA Parameters** または **802.11b/g/n > EDCA Parameters** を選択します。

ステップ 4　ドロップダウン メニューから **EDCA Profile** を選択します。

（注）　プロファイルには、Wi-Fi Multimedia (WMM)、Spectralink Voice Priority (SVP)、Voice Optimized、および Voice & Video Optimized が含まれます。WMM がデフォルトの EDCA プロファイルです。

（注）　無線インターフェイスをシャットダウンしてから、EDCA パラメータを設定してください。

ステップ 5　**Enable Streaming MAC** チェックボックスをオンにして、この機能を有効にします。

（注）　ネットワーク上のすべてのクライアントが WMM 準拠の場合には、Streaming MAC を有効にするのみです。

SNMPv3 の設定

コントローラを設定する場合、SNMPv3 設定を追加したり、以前に追加したコントローラから作成した設定（およびその他の設定）を変更できます。SNMPv3 を設定する手順は、次のとおりです。

ステップ 1　**Configure > Controllers** の順に選択します。

ステップ 2　該当するコントローラの **IP Address** をクリックするか、Select a command ドロップダウン メニューから **Add Controller** を選択します。

ステップ 3　ウィンドウの SNMP Parameters 部分で、Version ドロップダウン メニューから **v3** を選択します。

ステップ 4　このコントローラに対して実行された再試行およびタイムアウト値を、必要に応じて変更できます。

ステップ 5　Privacy Type ドロップダウン メニューで、**None**、**CBC-DES**、または **CFB-AES-128** を選択します。Advanced Encryption Standard（高度暗号化規格 ; AES）は、National Institute of Standards and Technology（国立標準技術研究所 ; NIST）によって制定された Advanced Encryption Standard アルゴリズムを参照します。これは、従来の Digital Encryption Standard（デジタル暗号化規格 ; DES）アルゴリズムより安全です。Cipher Feedback（CFB）は、AES がパケットを暗号化するために使用する方法を参照し、128 はキーの長さ（128 ビット）を参照します。

ステップ 6　128　を使用するアルゴリズムの暗号化キーを得るには、任意のパスワードを使用します。ただし、パスワードには 12 文字以上が含まれている必要があります。この基準に適合するパスワードを入力します。

ステップ 7　**OK** をクリックします。

Autonomous の LWAPP への移行のサポート

Autonomous の LWAPP への移行サポート機能には、現在の LWAPP アクセス ポイントと共に IOS アクセス ポイントの基本的な監視を実行できる共通のアプリケーション（WCS）が備わっています。次の Autonomous アクセス ポイントがサポートされています。

- Cisco Aironet 1100 Access Point
- Cisco Aironet 1130 Access Point
- Cisco Aironet 1200 Access Point
- Cisco Aironet 1240 Access Point
- Cisco Aironet 1240 Access Point
- Cisco Aironet 1310 Bridge

IOS アクセス ポイントの LWAPP への変換も選択できます。

WCS から、IOS アクセス ポイントを管理する際に次の機能を使用できます。

- IOS アクセス ポイントの追加
- IOS アクセス ポイントの設定
- Monitor > Access Points ページでの現在の IOS アクセス ポイントの表示（詳細は「Monitoring Access Points」参照）
- Monitor > Maps ページでの IOS アクセス ポイントの追加と表示（詳細は「Maps」参照）
- アソシエートされているアラームの監視
- Autonomous アクセス ポイントのバックグラウンド タスクの実行
  - WCS によって管理される IOS アクセス ポイントのステータスを確認します。
  - 到達不能の IOS アクセス ポイントが検出された場合に、重大なアラームを生成します。
  - 詳細は、「Background Task」を参照してください。
- IOS アクセス ポイントのレポートの実行
  - 詳細は、Reports > Inventory Reports および Reports > Client Reports > Client Count を参照してください。
- Work Group Bridge（WGB）モードにおける IOS アクセス ポイントのサポート
- IOS アクセス ポイントの LWAPP アクセス ポイントへの移行

IOS アクセス ポイントの WCS への追加

WCS から IOS アクセス ポイントを追加するには、次の方法が使用できます。

- Device 情報（IP アドレスおよびクレデンシャル）により IOS アクセス ポイントを追加します。
- CSV ファイルにより IOS アクセス ポイントを追加します。

Device 情報による IOS アクセス ポイントの追加

Device 情報によって IOS アクセス ポイントを WCS に追加するには、カンマ区切りの IP アドレスとクレデンシャルを使用します。

Device 情報を使用して IOS アクセス ポイントを追加する手順は、次のとおりです。

ステップ 1　**Configure > Access Points** の順に選択します。

ステップ 2　Select a command ドロップダウン メニューから、**Add Autonomous APs** を選択します。

ステップ 3　**Go** をクリックします。

ステップ 4　Add Format Type ドロップダウン リストから **Device Info** を選択します。

ステップ 5　IOS アクセス ポイントのカンマ区切り IP アドレスを入力します。

ステップ 6　バージョン番号、再試行の回数、タイムアウトの秒数などの SNMP パラメータを入力します。

ステップ 7　移行に対する Telnet クレデンシャルを入力します（オプション）。

（注）　Telnet クレデンシャルは、アクセス ポイントを Autonomous から Unified へ変換するのに必要です。

（注）　Autonomous アクセス ポイントが既に存在する場合には、WCS はクレデンシャル（SNMP および Telnet）を既存のデバイスへアップデートします。

ステップ 8　**OK** をクリックします。

CSV ファイルによる Autonomous アクセス ポイントの追加

Autonomous アクセス ポイントを WCS に追加するには、WLSE からエクスポートした CSV ファイルを使用します。

CSV ファイルを使用して Autonomous アクセス ポイントを追加する手順は、次のとおりです。

ステップ 1　**Configure > Access Points** の順に選択します。

ステップ 2　**Select a Command** ドロップダウン メニューから、**Add Autonomous APs** を選択します。

ステップ 3　**Go** をクリックします。

ステップ 4　**Add Format Type** ドロップダウン リストから **File** を選択します。

ステップ 5　該当する CSV ファイルを入力するか、参照して選択します。

（注）　CSV ファイルには、Adding Controllers と同じ形式が含まれますが、telnet_username、telnet_password、enable_password などの追加行（オプション）が含まれます。

ステップ 6　**OK** をクリックします。

Autonomous アクセス ポイントを WCS から削除する手順は、次のとおりです。

ステップ 1　該当するアクセス ポイントのチェックボックスをオンにします。

ステップ 2　**Select a Command** ドロップダウン リストから、**Remove APs** を選択します。

WCS での Autonomous アクセス ポイントの表示

Autonomous アクセス ポイントが追加されると、**Monitor > Access Points** ページに表示されます。

Autonomous アクセス ポイントをクリックすると、次のような詳細が表示されます。

- アクセス ポイントの操作ステータス
- 無線情報、チャネル、電力、無線上のクライアント数などの主要な属性
- CDP 近隣情報

Autonomous アクセス ポイントは、**Monitor > Maps** でも表示できます。

Autonomous アクセス ポイントをフロア領域に追加するには、**Monitor Maps > <floor area>** を選択して、**Select a Command** ドロップダウン リストから **Add Access Points** を選択します。

Work Group Bridge（WGB）モード

Wireless Group Bridge（WGB）モードは、Autonomous アクセス ポイントが無線クライアントのように機能して、LWAPP アクセス ポイントに接続する特殊なモードです。WGB およびその有線クライアントは、WCS のクライアントとして一覧に記載されています。

Monitor > WGBs を選択して、WGB 内にあるすべての WCS クライアントの一覧を表示します。**User** をクリックして、特定の WGB とその有線クライアントに関する詳細な情報を表示します。

（注） WCS には、Autonomous アクセス ポイントを WCS が管理するかどうかについて WGB クライアントの情報が備わっています。WGB アクセス ポイントも WCS によって管理されている場合には、WCS は他の Autonomous アクセス ポイントに類似したアクセス ポイントに対する基本的な監視機能を提供します。

Autonomous アクセス ポイントの LWAPP アクセス ポイントへの移行

Autonomous ソリューションから Unified アーキテクチャへ移行するには、Autonomous アクセス ポイントを LWAPP アクセス ポイントへ変換する必要があります。移行ユーティリティは、既存テンプレートが一覧に記載されている **Configure > Migration Templates** ページから使用できます。

Select a command ドロップダウン リストから、次の機能を実行できます。

- Add Template：移行に関する必要な情報を提供できます。
- Delete Templates：現在のテンプレートを削除できます。
- View Migration Report：AP アドレス、移行ステータス、タイムスタンプ、詳細なログへのリンクなどの情報を表示できます。
- View Current Status：現在の移行の進捗状況を表示できます（3 秒ごとに更新）。

（注）　既に管理されている Autonomous アクセス ポイントを LWAPP へ移行する場合には、その位置とアンテナの情報も移行されます。情報を再入力する必要はありません。WCS では、移行後に Autonomous アクセス ポイントが自動的に削除されます。

移行テンプレートの追加と変更

新しいテンプレートを追加するには、**Select a command** ドロップダウン リストから **Add Template** を選択します。

既存テンプレートを変更するには、概要リストのテンプレート名をクリックします。

次の移行パラメータを入力または変更します。

General

- Template Name：この移行テンプレートのユーザ定義の名前。
- Description：移行テンプレートを識別できるような簡単な説明。

Upgrade Options

- DHCP Support：変換後にすべてのアクセス ポイントが DHCP サーバから IP を取得したことを確認します。
- Retain AP HostName：このアクセス ポイントに対して同じホスト名を保持できます。
- Migrate over WANLink：アクセス ポイント上で実行される CLI コマンドに対するデフォルトのタイムアウトを延長します。
- DNS Address
- Domain Name

Controller Details

（注）　アクセス ポイントの認証情報（SSC）をこのコントローラ上で設定でき、変換されたアクセス ポイントが接続できることを確認してください。

- Controller IP
- User Name
- Password

TFTP Details

- TFTP Server IP
- File Path
- File Name

テンプレートを WCS に追加すると、次の追加ボタンが表示されます。

- **Select APs**：このオプションを選択すると、変換のためのアクセス ポイントを選択する WCS の Autonomous アクセス ポイントの一覧が表示されます。
- **Select File**：変換用のアクセス ポイントの CSV 情報が表示されます。

アクセス ポイントの設定

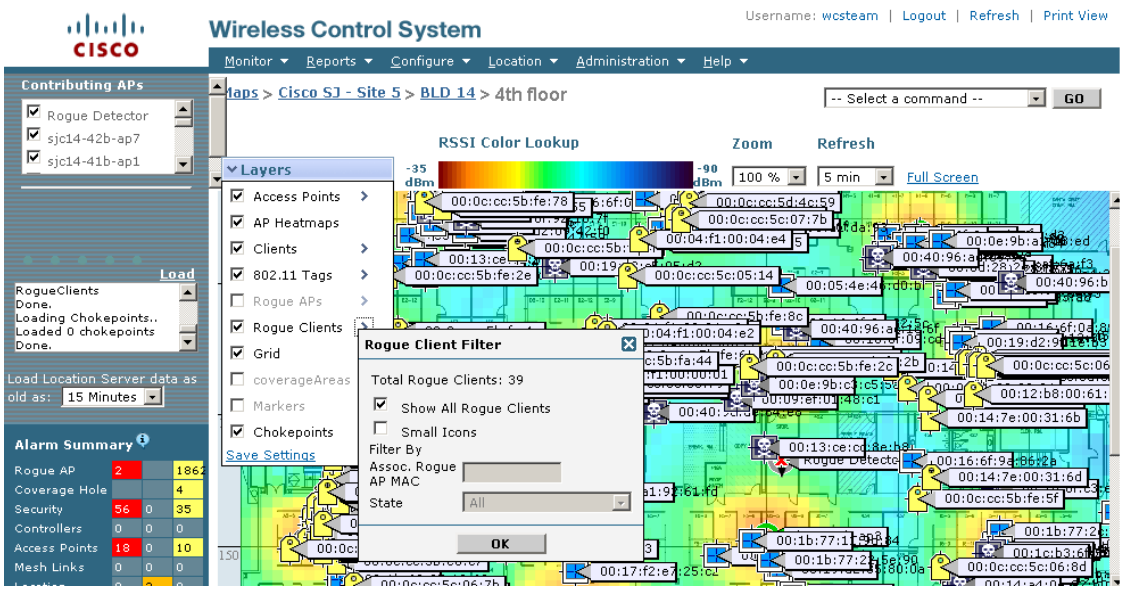
Configure > Access Points の順に選択して、Cisco WCS データベース内のすべてのアクセス ポイントの概要を表示します。表示される概要は、次のとおりです。

- Ethernet MAC
- IP Address
- Radio
- Map Location
- AP Type
- Controller
- Operation Status
- Alarm Status
- Audit Status

（注）　マウスを Audit Status の値の上に置くと、最新監査の時刻が表示されます。

ステップ 1　AP Name の下のリンクをクリックして、そのアクセス ポイント名についての詳細情報を表示します。次のようなウィンドウが表示されます（図 9-6 参照）。

図 9-6　アクセス ポイント詳細情報



（注）　アクセス ポイントを Cisco WCS データベースに追加する必要はありません。オペレーティング システムのソフトウェアによってアクセス ポイントが自動的に検出され、Cisco WCS データベース内の既存のコントローラとアソシエートしているかのように Cisco WCS データベースに追加されます。

ウィンドウ内のいくつかのパラメータは提供されます。

- General 部分には、イーサネット MAC、ベース無線の MAC、IP アドレスが表示されます。
- ウィンドウの Versions 部分には、ソフトウェア バージョンとブート バージョンが表示されます。
- Inventory Information 部分には、モデル、IOS バージョン、アクセス ポイントのシリアル番号と種類、必要な証明書の種類、H-REAP モードがサポートされるかどうかが表示されます。
- Radio Interfaces 部分には、admin ステータス、チャネル番号、電力レベル、アンテナ モード、アンテナ ダイバーシティ、アンテナの種類など、802.11a/n 無線と 802.11b/g/n 無線の現在のステータスが表示されます。

設定可能なパラメータを設定する手順は、次のとおりです。

ステップ 1　アクセス ポイントに割り当てられた名前を入力します。

ステップ 2　ドロップダウン メニューから国番号を選択して複数国のサポートを定義します。アクセス ポイントは、さまざまな規制要件を持つ多くの国で使用できるように設計されています。国の規制にアクセス ポイントが準拠するように国番号を設定できます。国番号を設定する際には、次の内容を考慮してください。

- コントローラごとに 20 までの国を設定できます。
- 自動 RF エンジンが 1 つと、使用可能なチャネルの一覧が 1 つしか存在しないため、複数国の設定は、共通チャネル内で自動 RF が使用できるチャネルに制限されます。共通チャネルとは、設定したすべての国において合法的なものです。
- 複数の国用にアクセス ポイントを設定する場合は、自動 RF チャネルは、設定したすべての国で使用できる最も高い電力レベルに制限されます。特定のアクセス ポイントはこれらの制限を越えて設定される場合があります（または、これらの制限を越えるレベルに手動で設定する場合があります）。ただし、自動 RF が自動で共通チャネル以外を選択することや、すべての国で使用できるレベルを超えた電力レベルに上げることはありません。

（注）　操作する国向けに設計されていない場合は、アクセス ポイントは正しく動作しない場合があります。たとえば、（-A）米国規制区域に含まれる部分番号 AIR-AP1030-A-K9 のアクセス ポイントは、ヨーロッパ （-E）では使用できません。必ず自国の規制区域に合ったアクセス ポイントを購入するようにしてください。製品ごとにサポートされている国番号の一覧については、http://www.cisco.com/warp/public/779/smbiz/wireless/approvals.html を参照してください。

ステップ 3　管理目的でアクセス ポイントを有効にする場合は、**Enabled** チェックボックスをオンにします。

ステップ 4　AP Static IP チェックボックスの **Enabled** をオンにする場合は、リブート時に動的に IP アドレスを取得するのではなく、常に静的 IP アドレスがアクセス ポイントに割り当てられます。

ステップ 5　AP Mode ドロップダウン メニューからアクセス ポイントのロールを選択します。モードの変更後にリブートする必要はありません。使用できるモードは、次のとおりです。

- Local：アクセス ポイントの通常動作であり、AP Mode のデフォルト値です。このモードでは、設定したチャネルをスキャンしてノイズと不正を探す間、データ クライアントが提供されます。アクセス ポイントは 50 ミリ秒間、チャネルの不正をリッスンします。Auto RF 設定の下で指定された期間の間、各チャネルを巡回します。

- Monitor：無線受信のみのモードであり、設定したすべてのチャネルをアクセス ポイントが 12 秒ごとにスキャンできるようになります。このように設定されたアクセス ポイントのある空間では認証解除のパケットのみが送信されます。監視モードのアクセス ポイントは不正を検出しますが、RLDP パケットの送信準備のために不審なものにクライアントとして接続することはできません。
- Rogue Detector：このモードでは、アクセス ポイントの無線がオフに切り替わり、アクセス ポイントは有線トラフィックのみをリッスンします。このモードで動作するコントローラは、不正アクセス ポイントを監視します。コントローラはすべての不正アクセス ポイントとクライアントの MAC アドレスのリストを不正検出器に送信して、不正検出器がこの情報を WLC に転送します。MAC アドレスの一覧は、WLC アクセス ポイント が予測した内容と比較されます。MAC アドレスが一致する場合は、どの不正アクセス ポイントが有線ネットワークに接続されるかを判別できます。
- Sniffer Mode：スニファ モードで動作し、アクセス ポイントは特定チャネル上のすべてのパケットを取得して、Airopeek を実行するリモート マシンへ転送します。これらのパケットには、タイムスタンプ、信号強度、パケット サイズなどの情報が含まれます。この機能は、データ パケットのデコードをサポートする、サードパーティ製のネットワーク分析ソフトウェアである Airopeek を実行する場合のみ有効になります。Airopeek の詳細は、www.wildpackets.com/products/airopeek/overview を参照してください。
- HREAP：AP Mode ドロップダウン メニューから **HREAP** を選択して、6 つまでのアクセス ポイントのハイブリッド REAP を有効にします。HREAP アクセス ポイントは、コントローラへの接続を失ったとき、クライアント データ トラフィックをローカルに切り替え、クライアント認証をローカルで実行できます。

ステップ 6　Primary Controller フィールド、Secondary Controller フィールド、および Tertiary Controller フィールドで、アクセスするコントローラの順序を定義できます。

ステップ 7　AP Group Name ドロップダウン メニューには、WLANS > AP Group VLANs を使用して定義されているすべてのアクセス ポイント グループ名が表示されます。また、このアクセス ポイントが任意ののグループに関連付いているかどうかを指定できます。

ステップ 8　アクセス ポイントが配置されている物理位置の説明を入力します。

ステップ 9　Stats Collection Period パラメータには、アクセス ポイントが .11 の統計をコントローラに送信する時間を入力します。有効範囲は 0 ～ 65535 秒です。値 0 は統計を送信しないことを意味します。

ステップ 10　単一のクライアント デバイスまたはアクセス ポイントで発信されるか終了するすべてのトラフィックを（別のポートに）複製する場合は、**Mirror Mode** で Enabled を選択します。ミラー モードは特定のネットワーク問題を診断する際には役立ちますが、このポートへの接続には反応しなくなるため、使用されていないポートのみで有効にする必要があります。

ステップ 11　コントローラ上でグローバルに Management Frame Protection（MFP; 管理フレーム保護）を設定できます。その場合、管理フレームの保護と検証は、接続している各アクセス ポイントに対してデフォルトで有効になります。また、アクセス ポイント認証は自動で無効になります。MFP をコントローラ上でグローバルに有効にした後は、個々の WLAN とアクセス ポイントに対してそれを無効にすることや再度有効にすることができます。

クリックして MFP Frame Validation を有効にする場合は、次の 3 つの主要な機能が実行されます。

- 管理フレーム保護：管理フレーム保護を有効にすると、アクセス ポイントは Message Integrity Check Information Element（MIC IE; メッセージ整合性チェック情報要素）を各フレームに追加することにより、送信する管理フレームを保護します。フレームのコピー、変更、または再生を試みると、MIC が無効となり、MFP フレームを検出するように設定された受信アクセス ポイントはその矛盾を報告します。

- 管理フレーム検証 : 管理フレーム検証が有効な場合、アクセス ポイントは、ネットワーク内の他のアクセス ポイントから受信するすべての管理フレームを検証します。発信側が MFP フレームを送信するよう設定されている場合、MIC IE が存在し、管理フレームの中身が一致していることを確認できます。有効な MIC IE が含まれていないフレームを受信した場合は、その矛盾がネットワーク管理システムに報告されます。この矛盾を報告するには、アクセス ポイントは MFP フレームを送信するように設定されている必要があります。同様に、タイムスタンプが適切に機能するには、すべてのコントローラで Network Time Protocol（NTP; ネットワーク タイム プロトコル）が同期されている必要があります。
- イベント報告 : アクセス ポイントは異常を検出するとコントローラに通知し、コントローラは受信した異常イベントを集積して、ネットワーク マネージャに警告するために SNMP トラップ経由で結果を報告できます。

ステップ 12 有効にするには、**Cisco Discovery Protocol** チェックボックスをオンにします。CDP は、Cisco で製造されたルータ、ブリッジ、通信サーバなどのすべての機器で実行されるデバイス検出プロトコルです。各デバイスは、隣接デバイスについて知るために、マルチキャスト アドレスに定期メッセージを送信して、ほかのデバイスが送信したメッセージをリッスンします。デバイスの起動時には、要求した電力が供給されるように、デバイスがインライン パワーに対応するかどうかを指定する CDP パケットを送信します。

（注） アクセス ポイント パラメータを変更すると、一時的にアクセス ポイントが無効になり、いくつかのクライアントへの接続を失う場合があります。

ステップ 13 AP Role ドロップダウン メニューからメッシュ アクセス ポイントのロールを選択します。デフォルトの設定は MAP です。

（注） メッシュ ネットワークのアクセス ポイントは、ルート アクセス ポイント（RAP）またはメッシュ アクセス ポイント（MAP）として機能します。

ステップ 14 アクセス ポイントが属するブリッジ グループの名前を入力します。名前には最大 10 文字が使用できます。

（注） ブリッジ グループは、メッシュ アクセス ポイントを論理的にグループ化して、同一チャネル上の 2 つのネットワークが互いに通信しないようにするために使用されます。

（注） メッシュ アクセス ポイントが通信するためには、同じブリッジ グループ名が付いている必要があります。

（注） 複数の RAP を使用する設定の場合は、ある RAP から別の RAP へフェールオーバーできるように、すべての RAP に同じブリッジ グループ名が付いていることを確認してください。

（注） 別々のセクタが必要な設定の場合は、各 RAP およびそれがアソシエートしている MAP に別々のブリッジ グループ名が付いていることを確認してください。

Type パラメータには、メッシュ アクセス ポイントが屋内または屋外のどちらのアクセス ポイントかが表示されます。また、Backhaul Interface パラメータには、アクセス ポイントのバックホールとして使用されている、アクセス ポイントの無線が表示されます。

ステップ 15 ドロップダウン メニューから、バックホール インターフェイスのデータ レートを選択します。使用可能なデータ レートは、バックホール インターフェイスによって指示されます。デフォルトのレートは 18Mbps です。

（注） このデータ レートは、メッシュ アクセス ポイント間で共有され、メッシュ ネットワーク全体に対して固定されます。

（注） 展開したメッシュ ネットワーク ソリューションに対してデータ レートを変更しないでください。

ステップ 16 Ethernet Bridging ドロップダウン メニューから Enable オプションを選択し、メッシュ アクセス ポイントに対してイーサネット ブリッジを有効にします。

ステップ 17 このアクセス ポイント上でハードウェアのリセットを実行する必要がある場合は、**Reset AP Now** をクリックします。

ステップ 18 アクセス ポイントの設定をクリアする必要がある場合や、すべての値を工場出荷時の設定にリセットする必要がある場合は、**Clear Config** をクリックします。

Audit Status の表示（対アクセス ポイント）

Configure > Access Points ウィンドウの Audit Status 列には、各アクセス ポイントの監査ステータスが表示されます。選択したアクセス ポイントの監査レポートも確認できます。レポートには、監査の時刻、選択したアクセス ポイントの IP アドレス、および同期ステータスが表示されます。

ステップ 1　**Configure > Access Points** の順に選択します。

ステップ 2　Audit Status 列の値をクリックして、選択したアクセス ポイントの最新の監査詳細ページへ移動します。このレポートは、インタラクティブでアクセス ポイントごとになっています。

（注）　マウスを Audit Status 列の値の上に置くと、最新監査の時刻が表示されます。

アクセス ポイントのオンデマンドの監査レポートを実行するには、レポートを実行させる目的のアクセス ポイントを選択し、Select a command ドロップダウン メニューから **Audit Now** を選択します。4.1 以前のバージョンでは、監査は AP Details and AP Interface Details ページ上のパラメータに限られていました。リリース 4.1 では、この監査レポートはアクセス ポイント全体レベルの監査を対象としています。監査結果はデータベースに保存されるので、もう一度監査を実行しなくても最新の監査レポートを確認できます。

（注）　監査は、コントローラにアソシエートされているアクセス ポイント上でのみ実行できます。

アクセス ポイントの検索

左側のサイドバーのコントロールを使用して、カスタム検索を作成および保存します。

- **New Search** ドロップダウン メニュー：Search Access Points ウィンドウを開きます。Search Access Points ウィンドウを使用して、検索を設定、実行および保存します。
- **Saved Searches** ドロップダウン メニュー：保存済みのカスタム検索を一覧表示します。保存済みの検索を開くには、Saved Searches リストから選択します。
- **Edit Link**：Edit Saved Searches ウィンドウを開きます。保存済みの検索を Edit Saved Searches ウィンドウで削除できます。

Search Access Points ウィンドウで、次のパラメータを設定できます。

- Search By
- Radio Type
- Search in
- Save Search
- Items per page

GO をクリックすると、アクセス ポイントの検索結果が表示されます。

表 9-2　アクセス ポイントの検索結果

パラメータ	オプション
AP Name	アクセス ポイントに割り当てられた名前。詳細を表示するには、アクセス ポイント名の項目をクリックします。
WCS	アクセス ポイントが検出された WCS の名前。
Ethernet MAC	アクセス ポイントの MAC アドレス。
IP Address	アクセス ポイントの IP アドレス。
Radio	アクセス ポイントのプロトコルは、802.11a/n または 802.11b/g/n のどちらかです。
Map Location	キャンパス、ビルディング、またはフロアの位置。
Controller	コントローラの IP アドレス。
Admin Status	アクセス ポイントの管理サイト（Enabled または Disabled）。
AP Type	アクセス ポイントの無線周波数の種類。
Operational Status	シスコ製無線通信機の動作ステータスを表示します（Up または Down）。
Alarm Status	アラームのカラー コードは、次のとおりです。 • 透明 = アラームなし • 赤 = 重大なアラーム • オレンジ = 主要なアラーム • 黄 = 比較的重大でないアラーム

Spectrum Expert の設定

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

Spectrum Experts を設定するには、Configure > Spectrum Experts の順に選択します。このページには、次の項目を含むすべての Spectrum Experts の一覧が表示されます。

- Hostname：Spectrum Expert ラップトップのホスト名または IP アドレス。
- MAC Address：ラップトップのスペクトラム センサー カードの MAC アドレス。
- Reachability Status : Spectrum Expert が正常に稼動し、情報を WCS に送信しているかどうかを示します。ステータスは、Reachable または Unreachable と表示されます。

Spectrum Expert の追加

Spectrum Expert を追加する手順は、次のとおりです。

ステップ 1　**Configure > Spectrum Experts** の順に選択します。

ステップ 2　**Add a Spectrum Expert** をクリックします。

（注） このリンクは、Spectrum Expert が 1 つも追加されていない場合にのみ表示されます。Select a command ドロップダウン メニューから Add a Spectrum Expert を選択しても、Add a Spectrum Expert ページにアクセスできます。

ステップ 3　Spectrum Expert のホスト名 または IP アドレスを入力します。ホスト名を使用する場合、Spectrum Expert を WCS に追加するには DNS で登録する必要があります。

（注） Spectrum Expert として正しく追加するには、Spectrum Expert クライアントが稼動しており、WCS に通信できるように設定されていなければなりません。

Spectrum Expert の監視

Spectrum Expert を監視するためのオプションもあります。Spectrum Expert を監視する手順は、次のとおりです。

ステップ 1　**Monitor > Spectrum Experts** の順に選択します。

ステップ 2　左側のサイドバーのメニューから、**Spectrum Experts > Summary** ページと **Interferers > Summary** ページにアクセスできます。

Spectrum Experts > Summary

Spectrum Experts Summary ページには、システムに追加された Spectrum Expert の表が表示されます。この表には、次の Spectrum Expert の情報が記載されています。

Hostname：ホスト名または IP アドレス。

Active Interferers：Spectrum Expert により検出された現在の干渉の数。

Alarms APs : 検出された干渉が潜在的な影響を及ぼしていると Spectrum Expert により確認されたアクセス ポイントの数。

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

Reachability Status：Spectrum Expert が稼動してデータを WCS へ送信してる際に表示される、緑の「Reachable」の表示。それ以外の場合は、「Unreachable」と赤で表示されます。

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

Interferers > Summary

Interferers Summary ページには、30 日間隔で検出されたすべての干渉の一覧が表示されます。この表には、次のような干渉の情報が記載されています。

- Interferer ID：異なる Spectrum Expert 間で一意の ID。
- Category：干渉のカテゴリ。カテゴリには、次のものが含まれます。Bluetooth、コードレス電話、電子レンジ、802.11 FH、その他一般：固定周波数、妨害装置、その他一般：周波数ホッピング、その他一般：連続、およびアナログ ビデオ。
- Type : Active は、干渉が現在 Spectrum Expert で検出されていることを示します。Inactive は、干渉が検出されなくなったこと、または WCS が到達できる干渉はなくなったと Spectrum Expert が 確認したことを示します。
- Discover Time：干渉が発見された時刻を示します。
- Affected Channels：影響を受けるチャネルを示します。
- Number of APs Affected：Spectrum Expert が検出した WCS により管理されるアクセス ポイントの数、または Spectrum Expert がアクセス ポイントのチャネル上で検出した干渉の数。アクティブな干渉のみが表示されます。次の条件のすべてが適合する場合、そのアクセス ポイントには *affected* とラベルが付けられます。
  - アクセス ポイントが WCS で管理されている。
  - Spectrum Expect がアクセス ポイントを検出している。
  - Spectrum Expect がアクセス ポイントの稼動チャネル上の干渉を検出している。
- Power：dBm で示されます。
- Duty Cycle：パーセントで示されます。100% は最低値です。
- Severity：干渉の重大度ランキングを示します。100 は最低値、0 は干渉がないことを表しています。

Spectrum Experts の詳細

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

- Total Interferer Count：特定の Spectrum Expert から報告されます。
- Active Interferers Count Chart：カテゴリごとの干渉をグループ化した円グラフを表示します。
- Active Interferer Count Per Channel：別々のチャネル上のカテゴリごとにグループ化された干渉の数を表示します。
- AP List : Spectrum Expert によって検出されたアクセス ポイントの一覧を表示します。これらのアクセス ポイントは、アクティブな干渉が検出されたチャネル上にあります。
- Affected Clients List：アクセス ポイントの一覧内のアクセス ポイントに、現在認証されているクライアントの一覧を表示します。

有線ゲストのアクセスの設定

Wired Guest Access では、ゲスト ユーザがゲスト アクセス用に指定および設定された有線イーサネット接続からゲスト アクセス ネットワークへ接続できます。有線ゲスト アクセス ポートは、ゲストのオフィスまたは会議室の特定のポートで使用できます。

無線ゲスト ユーザ アカウントのように、有線ゲスト アクセス ポートが Lobby Ambassador 機能を使用するネットワークに追加されます。「ゲスト ユーザ アカウントの作成」の項（P. 7-13）を参照してください。

Wired Guest Access は、スタンドアロン設定、またはアンカーおよび外部のコントローラを配置したデュアル コントローラ設定で設定することができます。後者の設定は、有線ゲストのアクセス トラフィックをさらに分離する際に使用しますが、有線ゲストのアクセスを展開する必要はありません。

Wired Guest Access ポートは、最初、レイヤ 2 アクセス スイッチか、有線ゲストのアクセス トラフィック用 VLAN インターフェイスで設定されたスイッチ ポートで終端します。

有線ゲスト トラフィックは、その後、アクセス スイッチから無線 LAN コントローラへトランキングされますこのコントローラは、アクセス スイッチ上で有線ゲストのアクセス VLAN へマップされたインターフェイスで設定されています。

2 つのコントローラが使用されている場合、外部コントローラがスイッチから有線ゲスト トラフィックを受信し、次に有線ゲスト トラフィックをアンカーコントローラへ転送します。アンカーコントローラも有線ゲストのアクセスに対して設定されています。有線ゲスト トラフィックがアンカー コントローラへ正常に渡されると、外部コントローラとアンカー コントローラ間に双方向の Ethernet over IP（EoIP）トンネルが確立され、このトラフィックを処理します。

（注）　2 つのコントローラが展開されている場合、アンカーと外部のコントローラが有線ゲストのアクセスを管理しますが、有線ゲスト アクセス クライアントのモビリティはサポートされていません。この場合、クライアントの DHCP および Web の認証はアンカー コントローラが処理します。

（注）　ロールと帯域幅コントラクトを設定して割り当てることで、ネットワーク内の有線ゲスト ユーザに割り当てる帯域幅の量を指定できます。これらの機能に関する詳細は、「ゲスト ユーザ アカウントの作成」の項（P. 7-13）を参照してください。

ネットワークの有線ゲスト ユーザのアクセスを設定して有効化する手順は、次のとおりです。

ステップ 1　有線ゲスト ユーザのアクセスに対する動的インターフェイスを設定するには、特定の IP アドレスを選択して **Configure > Controllers** の順にクリックし、**System > Interfaces** の順に選択します。Interfaces Summary ウィンドウが表示されます。

ステップ 2　Select a command ドロップダウン メニューから **Add Interface** を選択し、**GO** をクリックします。

ステップ 3　新しいインターフェイスの名前と VLAN ID を入力します。

ステップ 4　Guest LAN チェックボックスをオンにします。

ステップ 5　インターフェイスの IP アドレス、ネットマスク、およびゲートウェイ アドレスを入力します。

ステップ 6　プライマリおよびセカンダリ DHCP サーバの IP アドレスを入力します。

ステップ 7　**Save** をクリックします。これで、ゲスト アクセス用の有線 LAN を作成できるようになりました。

ステップ 8　ゲスト ユーザ アクセス用の有線 LAN を設定するには、左側のサイドバーのメニューから **WLANs > WLAN** をクリックします。

ステップ 9　Select a command ドロップダウン メニューから **Add WLAN** を選択し、**GO** をクリックします。

ステップ 10　このコントローラに適用する作成済みのテンプレートがある場合には、ドロップダウン メニューからゲスト LAN テンプレート名を選択します。そうでない場合には、**click here** リンクをクリックして新しいテンプレートを作成します。

ステップ 11　Profile Name フィールドにゲスト LAN を識別する名前を入力します。入力する名前には、スペースを使用しないでください。

ステップ 12　SSID フィールドにゲスト LAN を識別する名前を入力します。入力する名前には、スペースを使用しないでください。

ステップ 13　目的の WLAN Status パラメータに対して **Enabled** チェックボックスをオンにします。

ステップ 14　Web Authentication (web auth) がデフォルトのセキュリティ ポリシーです。これを Web パススルーに変更する場合には、Security タブと Layer 3 を選択します。

ステップ 15　ドロップダウン メニューから認証方法を選択します。オプションは、IPSEC、VPN Passthrough、および none（オープン）です。

（注）　VPN Passthrough オプションを選択した場合、VPN Gateway Address オプションが表示されます。

ステップ 16　**Save** をクリックします。