Wireless Control System のトラブルシューティング

目次

概要

このドキュメントでは、Cisco Wireless Control System（WCS）における基本的な問題のトラブルシューティング手順をについて説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco WCS の設定方法に関する知識
- WLAN Controller（WLC）と Lightweight アクセス ポイント（LAP）を使用した無線 LAN（WLAN）の設定方法に関する知識

使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

トラブルシューティング

WCS をインストールできない

WCS のインストール時に問題が発生した場合は、まず WCS のインストール先システムが最低限のシステム要件を満たしているかどうかを確認します。

Cisco WCS をインストールする前に使用する、前提条件のチェックリストを次に示します。

1. Cisco WCS のインストール先システムが、Cisco WCS の必要なハードウェアおよびソフトウェア要件を満たしているかどうかを確認する。 WCS をインストールするためのソフトウェアおよびハードウェアの最低要件については、『Cisco WCS コンフィギュレーション ガイド、リリース 4.0』の「*システム要件*」セクションを参照してください。
2. 必要とされる重要なアップデートとサービス パックでシステムをアップデートしてあるか確認する。 最新のリリース ノートを参照し、WCS の正しい稼働に必要なサービス パックとパッチに関する情報を入手します。**注:** Linux で WCS をインストールする前に、Red Hat Linux のフル インストールが必要です。
3. 既存の WCS データベースをバックアップする。 Windows バックアップの実施方法については、「WCS データベースのバックアップ」を参照してください。
4. 旧バージョンの WCS をアンインストールする。 アンインストールの実施方法については、「Cisco WCS のアンインストール」を参照してください。

前提条件を満たしていることが確認されたら、WCS をインストールできます。 Windows 用 Cisco WCS のインストール方法については、「Windows 用 WCS のインストール」を参照してください。

注: WCS は 32 ビット Windows でだけ稼働します。 64 ビット オペレーティング システムへのインストールはサポートされていません。

Linux に WCS をインストールする方法については、「Linux 用 WCS のインストール」を参照してください。

WLC と WCS のバージョン間の互換性に関する問題

WLC を管理するために WCS をインストールするときは、WCS と WLC のバージョンに互換性があることを確認してください。 この情報は、インストールする WCS バージョンのリリース ノートに記載されています。

たとえば、Cisco WCS 5.1.64.0 は、次のワイヤレス LAN コントローラの管理をサポートします。

- 4.2.61.0
- 4.2.99.0
- 4.2.112.0
- 4.2.130.0
- 5.0.148.0
- 5.1.151.0

この情報は、次のドキュメントに記載されています。 Cisco Wireless Control System 5.1.64.0 リリース ノート Windows 版または Linux 版

WCS と WLC の互換性のないバージョンを使用している場合は、WLC を WCS に追加できません。

英語以外の Windows 2003 オペレーティング システムでインストール後に WCS が起動しない

これは、WCS が英語または日本語バージョンの Windows 2003 でだけサポートされるためです

。 他の言語に翻訳されているオペレーティング システムを使用している場合、WCS はインストール後に失敗します。 これを回避するには、Windows 2003 英語または日本語バージョンで WCS を使用します。

WCS でサポートされていない国際的な文字

WCS とロケーション アプライアンスでは、一般に、国際化文字がサポートされません。 マップ名、資産情報などに英語以外の文字を使用すると、表示エラー (誤った文字を表示) と検索機能のエラーが生じることがあります。

破損したログ ファイルが原因で WCS を起動できない

場合によっては、WCS を起動できず、Web インターフェイスを開けません。 WCS\bin\ フォルダの「.exe」ファイルを使用して WCS を開こうとしても、失敗します。 WCS を開始しようとした際に次のメッセージが表示されることがあります。

```
Starting WCS

Checking for Port 21 availability... OK

Checking for Port 8456 availability... OK

Checking for Port 8457 availability... OK
.....................................
.....................................
.....................................
.....................................
.....................................

Starting database server ...

The Nms_Server service is starting........ The Nms_Server service could not be started. The
service did not report an error. More help is available by typing NET HELPMSG 3534. Failed to
start WCS server.
```

この問題の考えられる原因の 1 つは、Bug CSCse17963 (登録ユーザ専用) です。

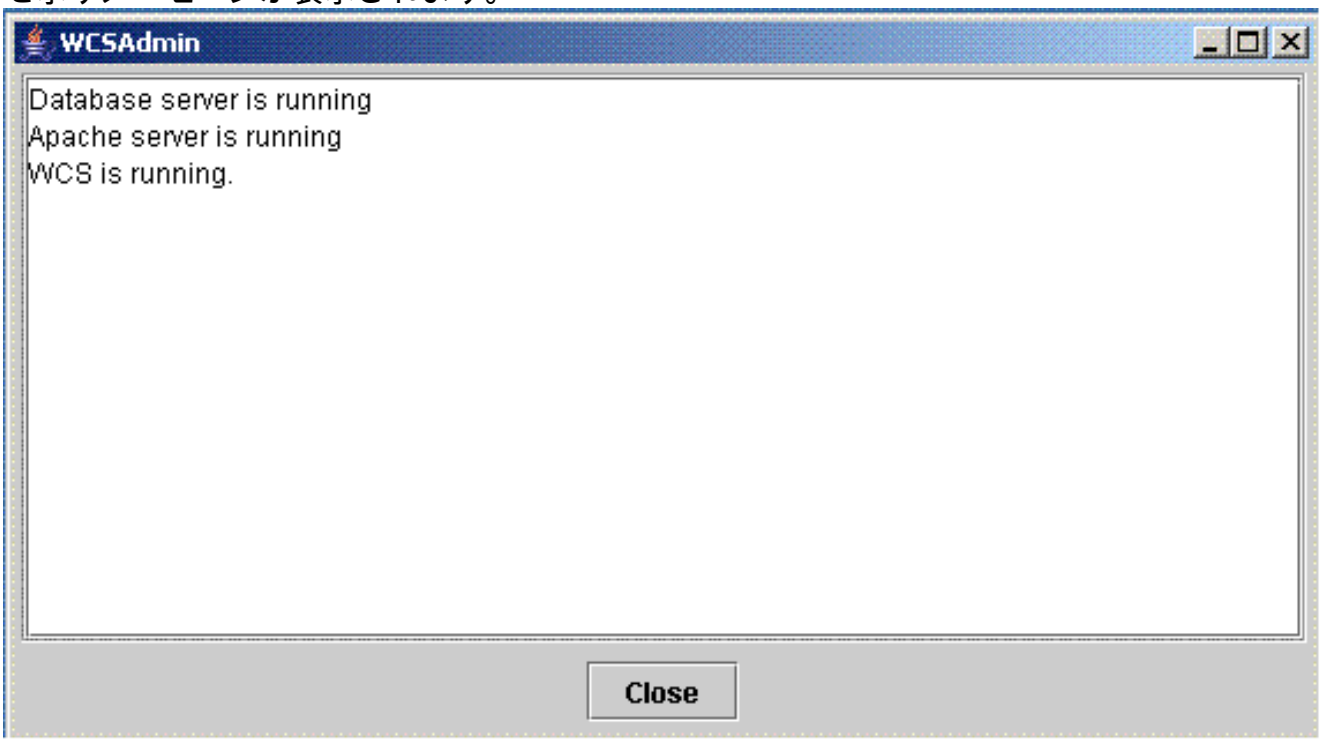
このバグが原因で、ログ ファイルが破損しているために WCS データベースの開始が失敗することがあります。 この問題を解決するには、WCS ディレクトリ内のパス **webnms\eval_kit\standalone** からサブディレクトリ **standalone** に移動します。 そのサブディレクトリで、最大の番号を持つ **sol####.log** ファイルを探します。ここで、**####** は 4 桁の数です。 これを削除し、サーバをリブートします。 WCS を起動してみます。 WCS が起動しない場合は、次の sol###.log ファイル、さらに次へと繰り返します。 この回避策で問題が解決します。

WCS のステータスの確認

WCS が期待通りに動作しない場合は、まず WCS のステータスを確認します。 WCS が Windows アプリケーションまたは Windows サービスとしてインストールされている場合、WCS のステータスを確認するには次の手順を実行します。 ステータスは任意の時点で確認できます。

1. システムに管理者として ログインします。
2. 次のいずれかのアクションを実行します。Windows の [Start] メニューに移動し、[Programs] > [Wireless Control System] > [WCSStatus] を選択します。コマンド プロンプトで、WCS のインストール ディレクトリ (C:\Program Files\WCS32\bin) へ移動し、**WCSAdmin status** と入力します。WCSAdmin ウィンドウが表示され、WCS のステータス

を示すメッセージが表示されます。



3. Close をクリックして、WCSAdmin ウィンドウを閉じます。

WCS が Linux システムにインストールされている場合、WCS のステータスを確認するには次の手順を実行します。

1. システムにルートでログインします。
2. Linux の CLI を使用して、次のタスクのいずれかを実行します。**/opt/WCS32** ディレクトリ（またはインストール時に選択したディレクトリ）へ移動し、**./WCSStatus** と入力します。**/opt/WCS32/bin** ディレクトリへ移動し、**WCSAdmin status** と入力します。CLI に WCS のステータスを示すメッセージが表示されます。

WLC への WCS の追加

新しい WLC を WCS に追加する場合は、コントローラに設定されている SNMP バージョンが WCS の SNMP バージョンと一致することを確認してください。 バージョンが異なると、WCS でコントローラが検出されず、WCS に次のエラーが表示されます。

```
No response from device, check SNMP.
```

また、コントローラで SNMP の書き込みアクセス権限が有効になっていることも確認してください。 読み取り専用アクセス パラメータを入力すると、コントローラは WCS に追加されますが、WCS でコントローラの設定の修正ができません。

要約すると、コントローラを WCS に追加するときに問題が発生した場合は、次の項目を確認します。

- コントローラ サービス ポートの IP アドレスが間違って設定されていないか。 コントローラ上のサービス ポートの設定をチェックします。
- WCS がコントローラに連絡できないのではないか。 WCS サーバからコントローラへ ping が行えることを確認します。
- コントローラ上の SNMP 設定が、WCS に入力した SNMP 設定と一致しないのではないか。コントローラに設定された SNMP 設定が、WCS に入力した設定と一致することを確認します。

- 最新バージョンの WCS にアップグレードするときは、Cisco からのライセンスが必要です。 WCS のライセンスを取得していない場合、新しい WLC を追加できません。 ライセンスを取得するには、TAC サポートに問い合わせる必要があります。

注: WCS で変更を加えた場合は、コントローラにこの変更を転送するようにしてください。 次に、最新にするためにコントローラの設定を更新します。 WCS から WLC を更新する方法については、このドキュメントの「WCS からの WLC 設定の更新」セクションを参照してください。

WCS からの WLC 設定の更新

WCS からコントローラの設定を更新するには、WCS で、次の手順を次の順序で実行します。

1. [Configure] > [Controllers] の順に選択します。
2. [Controllers] ページに追加されたすべての WLC が表示されます。 WLC のリストから、更新する WLC を選択します。
3. 結果のコントローラ ページで、[Select a command] ドロップダウン メニューから [save configuration to flash] を選択し、[Go] をクリックします。
4. 設定をフラッシュに保存した後、画面に成功を示すメッセージが表示されます。 成功画面が表示されたら、設定をフラッシュに保存した同じコントローラを選択し、[Select a command] で [Refresh config from controller] を選択します。
5. 古い設定を保持するのか削除するのかのプロンプトが示されます。 [Delete] を選択し、[OK] を押します。

WCS とコントローラ間または WCS と WCS ユーザ インターフェイスの間のファイアウォール

WCS サーバと WCS ユーザ インターフェイスがファイアウォールをはさんでいる場合、双方向トラフィック用にファイアウォールのポートがオープンされていなければ、それらは通信できません。

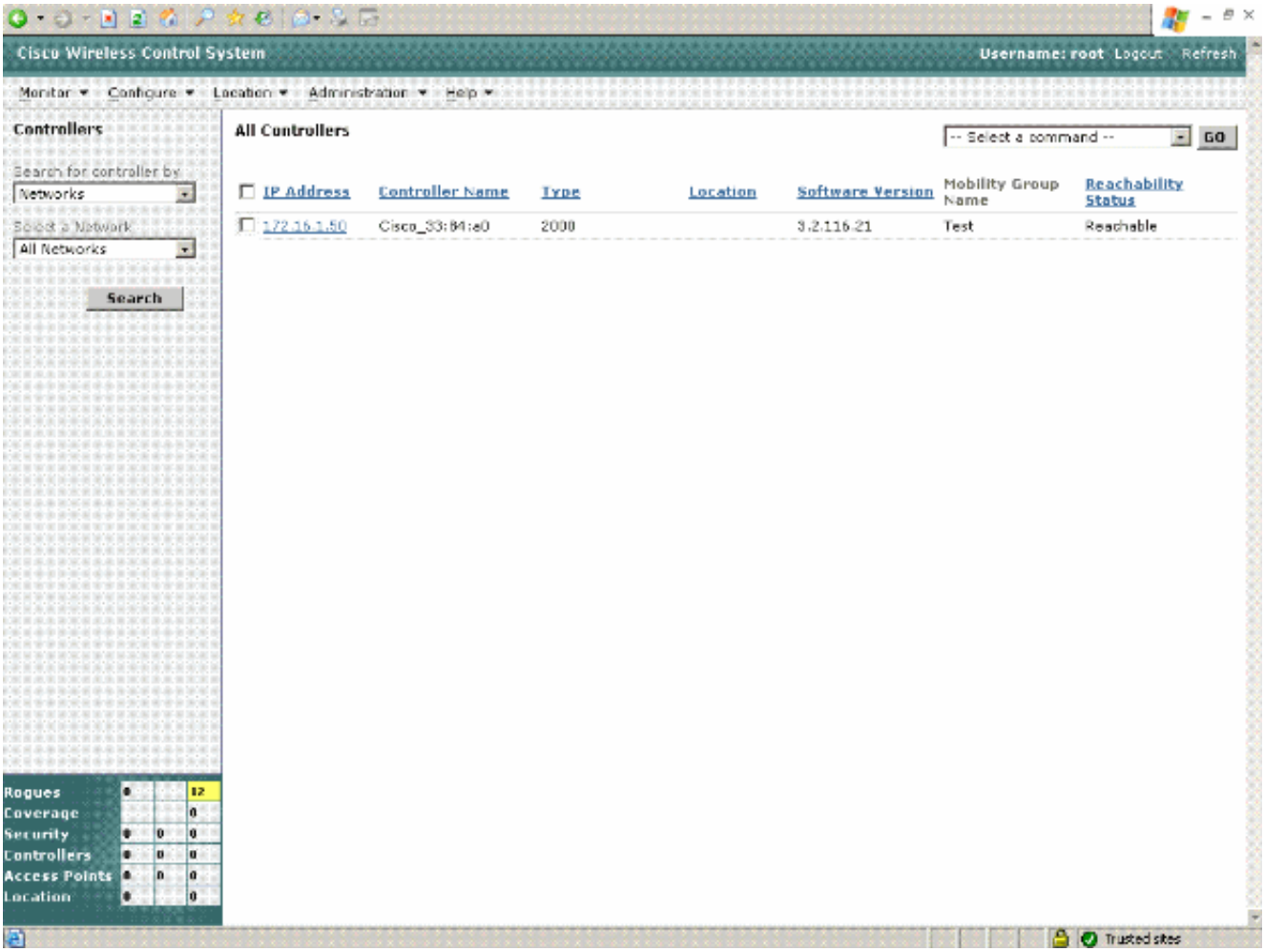
- 80（初期 http）
- 69（tftp）
- 162（トラップ ポート）
- 443（https）

WCS サーバと WCS ユーザ インターフェイスが通信できるようにファイアウォールを設定するには、これらのポートをオープンする必要があります。

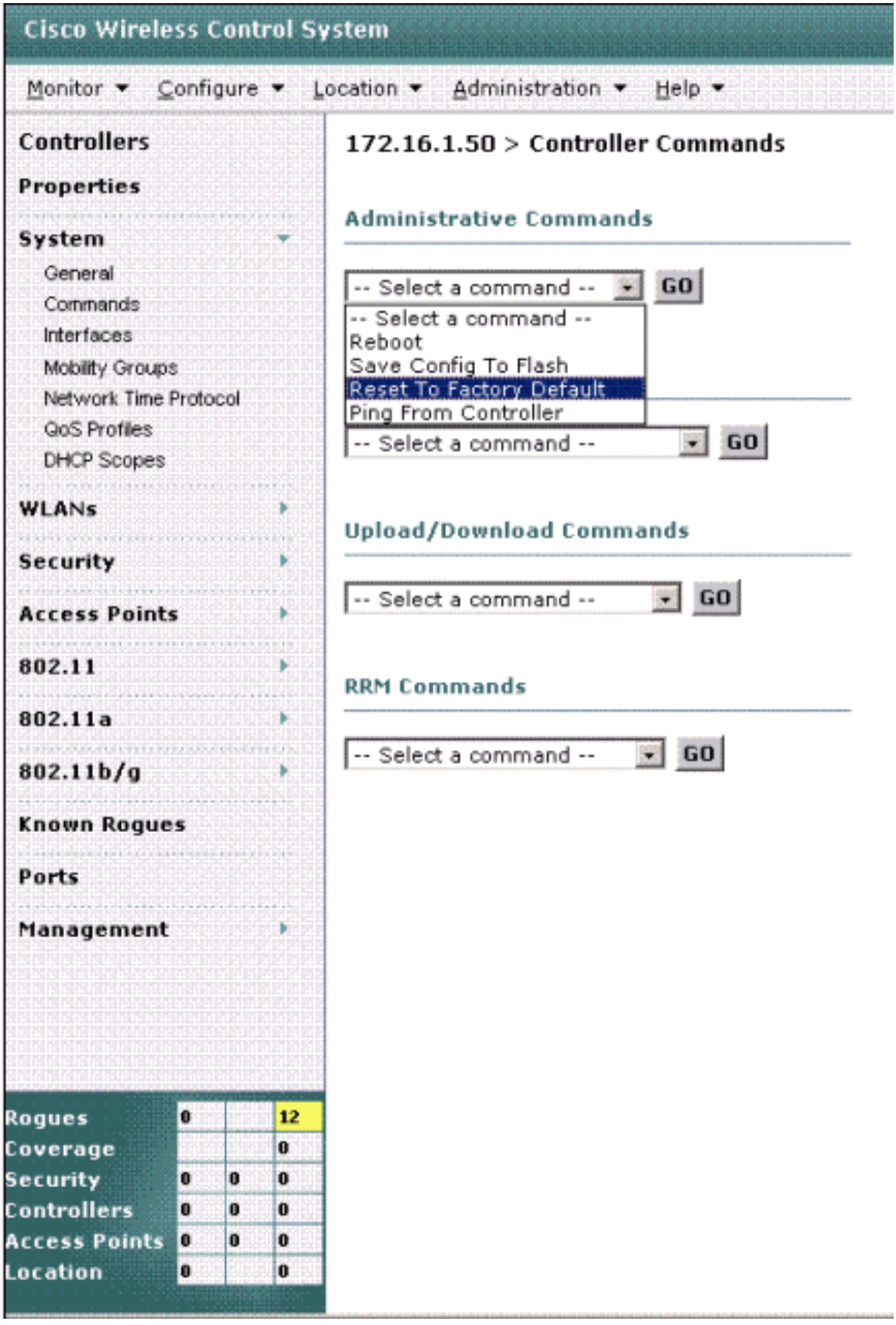
WCS を使用した、コントローラの工場出荷時デフォルトへのリセット

WCS を使用して、コントローラを工場出荷時のデフォルトにリセットするには、次の手順を実行します。

1. [All Controllers] ページを表示するには、[Configure] > [Controllers] を選択します。 このページには、WCS が検出するすべてのコントローラがリストアップされます。



2. エ場出荷時のデフォルトにリセットするコントローラの IP アドレスをクリックします。Controller Properties ウィンドウが表示されます。
3. 左側のメニューから、[System] > [Commands] の順に選択します。Controller Commands ウィンドウが表示されます。



4. [Administrative commands] で [Reset to factory default] を選択し、[Go] をクリックします。
5. Administrative Commands メニューから Reboot を選択し、コントローラの設定を保存せずにコントローラをリブートします。 これでコントローラは工場出荷時のデフォルトにリセットされます。**注:** コントローラが工場出荷時のデフォルトにリセットされると、コントローラが管理 IP アドレスで設定されない限り、WCS はそのコントローラを検出できません。検出できるようにするには、コントローラ上でスタートアップ コンフィギュレーション ウィザードを使用して、コントローラを設定する必要があります。

WCS データベースの最適化

アラームの削除、イベント、コントローラの追加/削除など、すべての通常の WCS 操作には、WCS データベース（DB）との SQL 操作が内部的に伴います。 このような、内部的な SQL 操作によって通常はデータベース サイズが大きくなり、その結果、WCS のパフォーマンスに影響を与えます。

たとえば、WCS での削除操作によってデータベースの削除された部分に空のスペースが残ります。 これにより、データベースにデータが不連続になった場所が発生することがあり、これが WCS のパフォーマンスに影響を与えます。 この問題を解決するには WCS データベースを最適化します。

最適化によってすべての使用領域と未使用領域が連続します。 使用領域および未使用領域が連続的であれば、パフォーマンスが向上します。 データベースを最適化すると、割り当て済みで未使用のディスク領域を解放できます。 データベースの最適化は、データベース サイズが大きいためにシステムの空きディスク領域が少なくなるか、データを要求したときの WCS アプリケーションの応答時間が顕著に遅い場合に有効なことがあります。

WCS で最適化を手動で実行するには、WCS アプリケーションを停止します。 これを行うには、[Start] > [Programs] > [Wireless Control System] > [Stop WCS] の順にクリックします。 次に、コマンドライン ボックスを開き、**C:\Program Files\WCS4.0\bin** ディレクトリ（WCS がインストールされているデフォルト ディレクトリ）に移動して、コマンド **DBAdmin defrag** を実行します。 最適化プロセスが開始されます。 プロセスが完了したら、[Start] > [Programs] > [Wireless] > [Control System] > [Start WCS operation] を使用して WCS を再起動します。

注: 最適化は、データベースの復元後に自動的に動作します。 ただし、場合によっては、ディスク領域を解放するために手動で最適化を行います。 手動の最適化は実際には必要ありません。 この領域は、通常は、WCS がアラームの作成と削除を開始する数日以内に取り戻されます。

WCS ソフトウェアのライセンスが適切であるかどうかの確認

Cisco Unified Wireless Network ソフトウェア リリース 4.0 は、ソフトウェア ベースのライセンス形式をとります。 新しいすべての Cisco WCS SKU ファミリ（Cisco WCS デモンストレーション ライセンスを除く）では、お客様はライセンス証明書を入力することが求められます。 現在のお客様がリリース 4.0 へ移行する場合も、ライセンス条件が適用されます。 Cisco WCS ライセンスの適用は、次のパラメータに密接に関連付けられています。

- **Host name**：登録プロセス時に、Cisco WCS サーバのホスト名を必要とするようになりました。 発行されるライセンスは、登録プロセスで指定された元のホスト名で割り当てられます。
- **Feature option**：購入した Cisco WCS 機能オプション（[Base] または [Location]）は、Cisco WCS ライセンスのシステムによって追跡されるようになりました。
- **Access points**：設定された増分（50、100、500、1000、または 2500）によるサポートされるアクセス ポイントの数は、Cisco WCS ライセンスのシステムによって追跡されるようになりました。
- **Demonstration license**：この無償の口ケーション対応 Cisco WCS デモンストレーション用ライセンスは、10 アクセス ポイントを最大 30 日間サポートします。

Cisco WCS ライセンスと利用可能なさまざまなライセンス タイプの詳細については、『Cisco WCS ライセンスおよび発注ガイド』を参照してください。

導入の状況、サポートされるアクセス ポイント数、および Cisco WCS のオプション（Base また

は Location) によって、適切なライセンスを選択してください。 SKU ファミリのすべての SKU は、Base と Base、Location と Location など同等のオプション レベルどうしで組み合わせることができます。 異なるオプション レベル (Base と Location) は混合できません。 WCS では、同時に 1 つのタイプのライセンスだけを使用できます。

たとえば、コンピュータに Location ライセンスがある場合は、Base ライセンスを追加できません。 ライセンスを購入して現在のライセンスに追加することで、アクセス ポイントを増やすことができます。 たとえば、アクセス ポイント数 50 の Location ライセンスを持っていて、1 年以内にアクセス ポイントがさらに必要になった場合、アクセス ポイント数 100 の Location ライセンスをもう 1 つ購入し、WCS に適用することで、アクセス ポイント数 150 の WCS Location ライセンスにすることができます。 ライセンスを追加することで増やすことのできるアクセス ポイント数は、50、100、500、1000、2500、または無制限です。

Base ライセンスを持っていて、Location ライセンスへアップグレードしたい場合は、Location アップグレード ライセンスを購入する必要があります。 Base ライセンスと同じ合計アクセス ポイント数の Location アップグレード ライセンスを購入する必要があります。 たとえば、50、100、および 200 のアクセス ポイント (合計 350 アクセス ポイント) をサポートする 3 つの Base ライセンスを持っている場合は、350 のアクセス ポイントをサポートする Location アップグレード ライセンスを 1 つ購入します。

Cisco WCS ライセンスを登録するには、すべての Cisco WCS SKU に PAK 証明書が必要です。 PAK は、Cisco WCS ライセンスの購入時にシスコから郵送される書面による証明書です。 お客様は PAK 証明書によって、Cisco WCS のライセンスを受け取ることができます。 この証明書は、Cisco WCS の登録とライセンス ファイルの生成に使用されます。 すべてのお客様は、PAK 証明書に記載されている PAK 登録サイトへアクセスし、Cisco WCS の登録を完了させる必要があります。 PAK 証明書には、Cisco WCS のライセンス プロセスの完了手順が明確に記載されています。

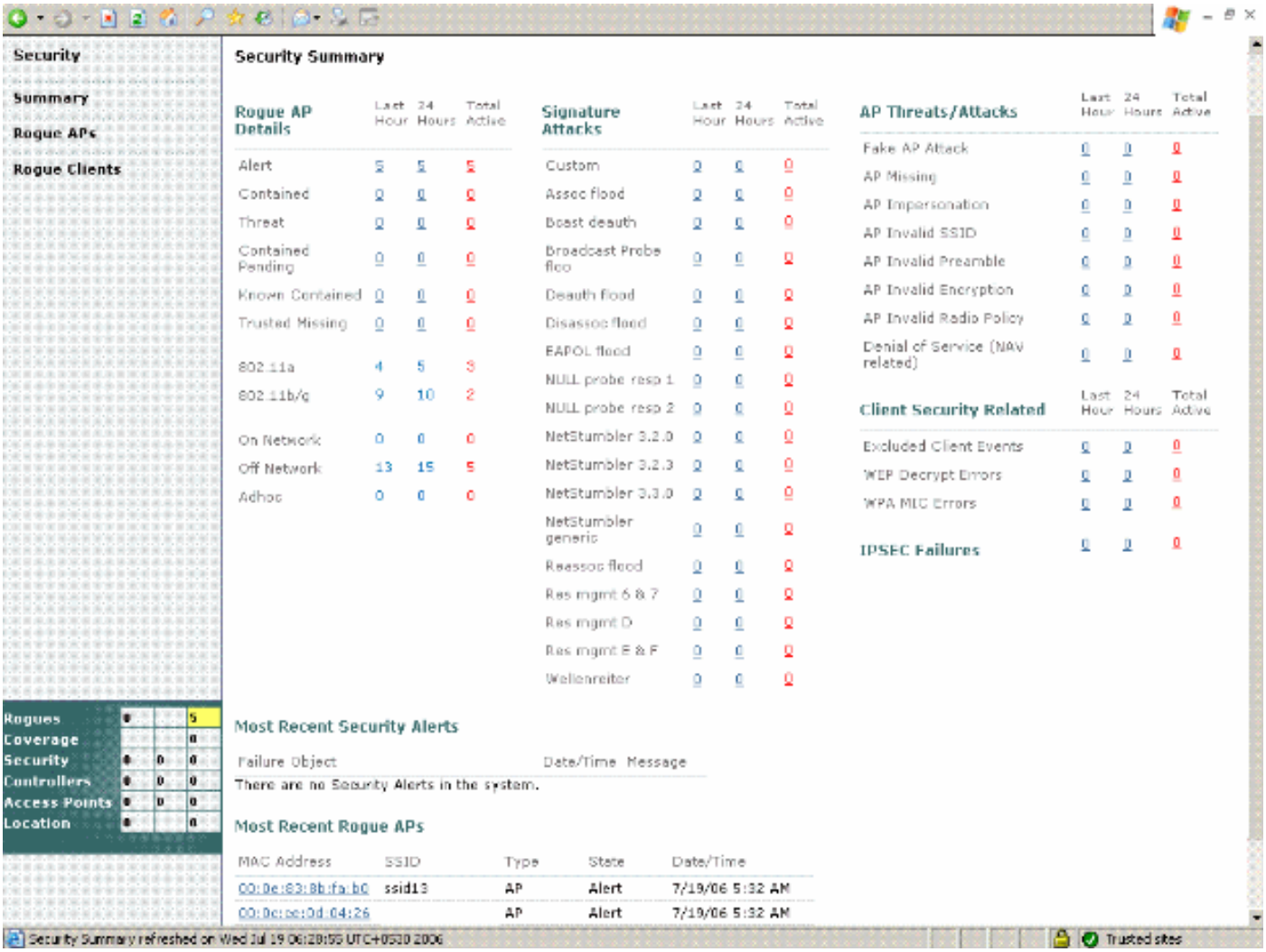
Cisco.com からのダウンロードまたは CD で Cisco WCS を購入されたお客様はすべて、PAK サイトでの登録により Cisco WCS のライセンスをアクティブ化する必要があります。 お客様は米国の郵便で PAK を受け取ります。 Cisco WCS は、PAK 登録プロセスが完了するまでアクティブ化されません。 WCS ライセンスのインストールと管理の方法については、「WCS のライセンス」を参照してください。

トラブルシューティングのための Security Summary ページ

Security Summary ページは、あらゆるセキュリティ関連のイベント情報をユーザに提供します。このページには、不正なアクセス ポイントに関する情報、シグニチャの攻撃に関する情報、アクセス ポイントへの攻撃に関する情報、およびクライアントのセキュリティに関する情報が含まれています。

このページは、とりわけセキュリティの脅威に関連した問題への効果的なトラブルシューティング ツールになります。 また、このページは最新のセキュリティの警告に関する情報も提供します。

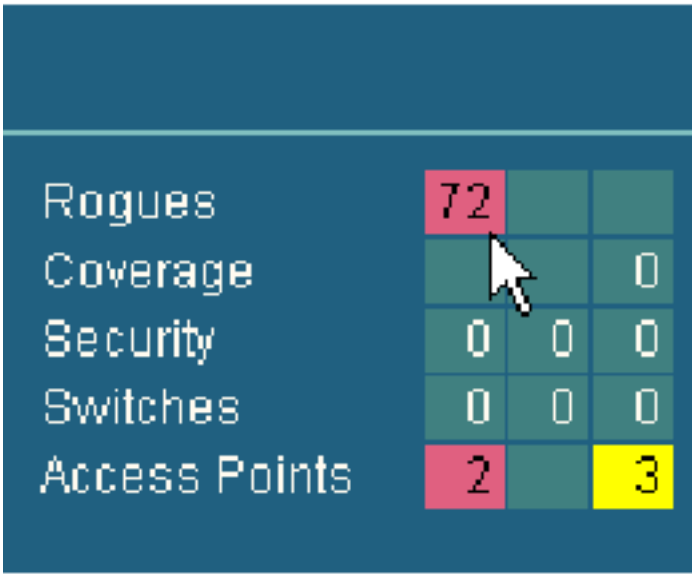
Security Summary ページの例を次に示します。



不正なアクセス ポイントの検出と場所の特定

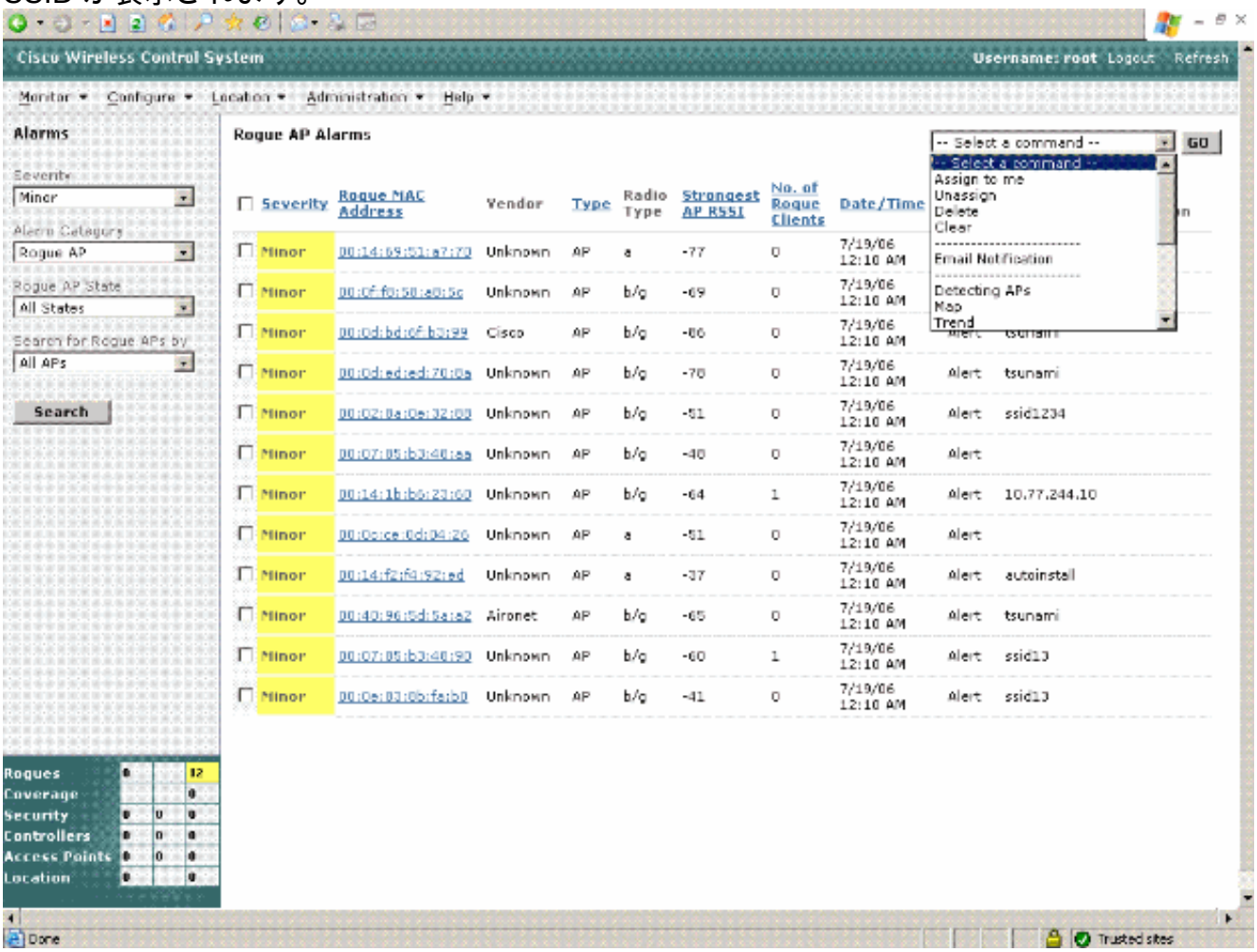
Cisco LAP がアップし、Cisco WLC に関連付けられると、オペレーティング システムに組み込まれている Cisco WCS はすぐに不正なアクセス ポイントのリッスンを開始します。 Cisco WLC は不正なアクセス ポイントを検出すると、それをすぐに Cisco WCS へ知らせ、Cisco WCS は不正アクセス ポイントのアラームを作成します。 WCS は、無線ネットワークの一部ではないアクセス ポイントをすべて不正なアクセス ポイントと見なします。

Cisco WCS が不正なアクセス ポイントのメッセージを Cisco WLC から受け取ると、Cisco WCS はアラームを生成し、すべての Cisco WCS ユーザ インターフェイスのページの左下隅にインジケータが表示されます。 次の例は、Cisco WCS による不正なアクセス ポイントのアラームが 72 件表示されています。

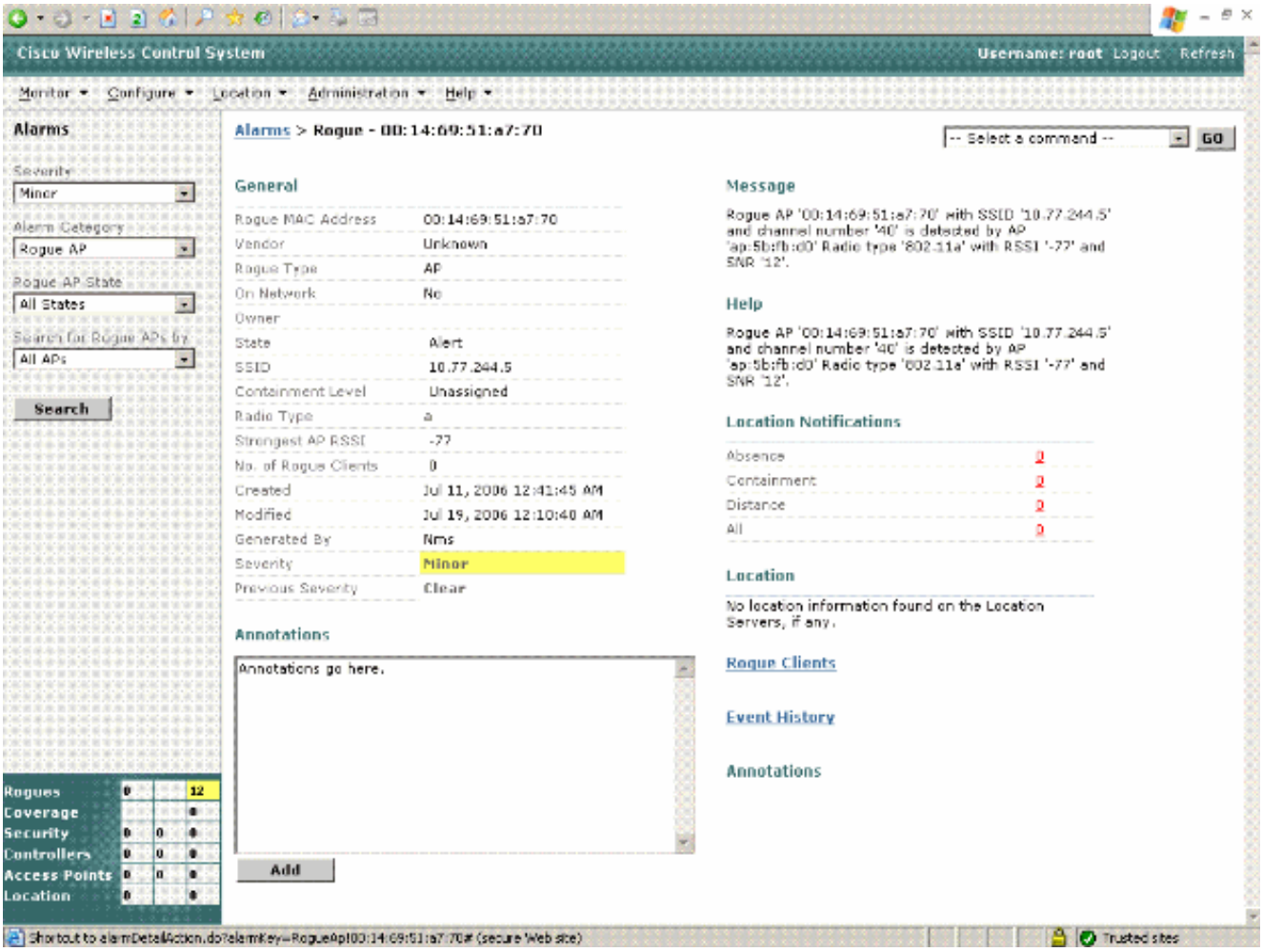


不正なアクセス ポイントを検出し、その場所を特定するには、次の手順を実行します。

1. [Rogues] インジケータをクリックして、[Rogue AP Alarms] ページを表示します。 このページには、アラームの重大度、不正なアクセス ポイントの MAC アドレス、不正なアクセス ポイントのタイプ、不正なアクセス ポイントが初めて検出された日時、および、それらの SSID が表示されます。



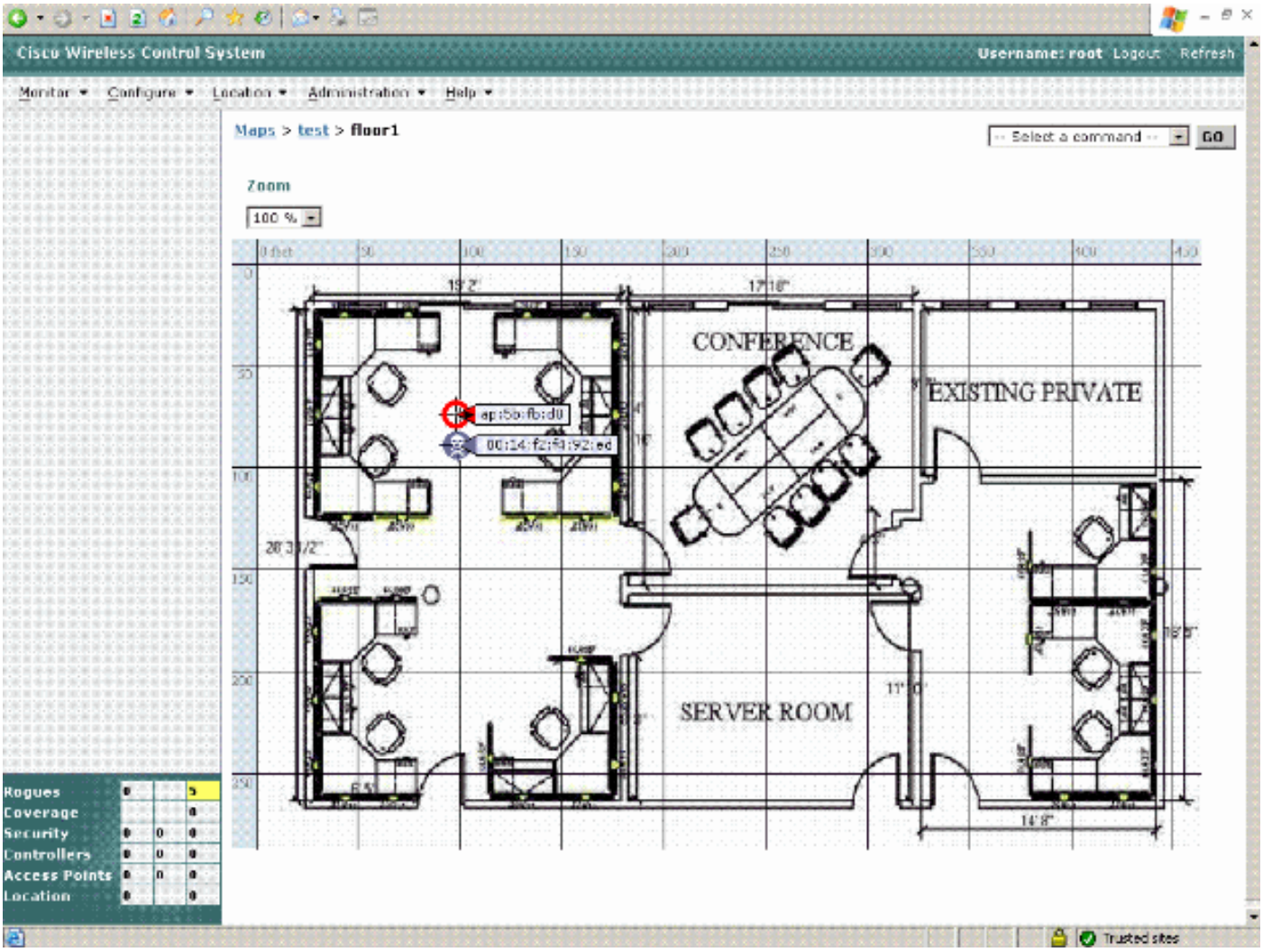
2. 任意の [Rogue MAC Address] リンクをクリックして、関連付けられた [Alarms > Rogue - AP MAC Address] ページを表示します。 次のページは、不正なアクセス ポイントのアラームの詳細を示しています。



3. Select a Command メニューからコマンドを 1 つ選択し、GO をクリックしてアラームを修正します。[Assign to me]：選択したアラームを現在のユーザに割り当てます。[Unassign]：選択したアラームの割り当てを解除します。[Delete]：選択したアラームを削除します。[Clear]：選択したアラームをクリアします。[Event History]：不正アラームのイベントを表示できます。[Detecting APs]（無線帯域、ロケーション、SSID、チャネル番号、Wired Equivalent Privacy（WEP）の状態、短いプリアンブルまたは長いプリアンブル、受信信号強度インジケータ（RSSI）、および SNR）：現在不正アクセス ポイントを検出しているアクセス ポイントを表示できます。[Rogue Clients]：この不正アクセス ポイントと関連付けられているクライアントを表示できます。[Set State to 'Unknown - Alert']：不正アクセス ポイントを最も低い脅威としてタグ付けして不正アクセス ポイントの監視を続行し、隔離機能をオフにします。[Set State to 'Known - Internal']：不正アクセス ポイントを内部としてタグ付けして既知の不正アクセス ポイント リストに追加し、隔離機能をオフにします。[Set State to 'Known - External']：不正アクセス ポイントを外部としてタグ付けして既知の不正アクセス ポイント リストに追加し、隔離機能をオフにします。[1 AP Containment] ~ [4 AP Containment]：level 1 containment を選択した場合は、不正な機器の近辺にある 1 つのアクセス ポイントが、その不正な機器に関連付けられたクライアント デバイスに認証解除とアソシエート解除のメッセージを送信します。 レベル 2 の封じ込めを選択すると、不正な装置の付近にあるアクセス ポイントのうち 2 つが、不正な装置のクライアントへ認証解除と関連付け解除のメッセージを送信します。これはレベル 4 まで、同様にルールが適用されます。したがって、封じ込めに選択されたアクセス ポイントは、クライアントが不正なアクセス ポイントと通信するのを防ぎます。 これにより、不正なアクセス ポイントの機能が効果的に無力化されます。
4. [Select a Command] ドロップダウン メニューに移動し、[Map (High Resolution)] を選択して、[GO] をクリックすることにより、[Map] > [Building Name] > [Floor Name] ページに計

算された現在の不正アクセス ポイントのロケーションを表示しま。
WCS Location を使用する場合、WCS は 2 つ以上のアクセス ポイントからの RSSI 信号強度を比較することで、不正なアクセス ポイントである可能性が最も高い場所を見つけ出し、小さなどくろマークをその場所に付けます。 1 つのアクセス ポイントと 1 つの全方向性アンテナだけを備えた場所にある導入途上のネットワークの場合、最も可能性の高い場所はアクセス ポイントを囲むリングのどこかですが、最も疑いが強いのは、そのアクセス ポイントです。

地図上に不正なアクセス ポイントを表示した例を示します。



WCS Base を使用する場合、WCS は不正なアクセス ポイントからの RSSI 信号強度によって、不正な装置から最も強い RSSI 信号を受信しているアクセス ポイントの隣に、小さなどくろマークを付けます。

ロケーション アプライアンスを使用している場合は、[Monitor] > [Map] ドロップダウン メニューで表示されるように、不正を追跡でき、[Show Rogue AP] オプションと [Rogue Clients] オプションがあります。 ロケーション アプライアンスを使用していない場合は、これらのオプションはなく、不正アラームを表示し、ドロップダウン メニューから [MAP (high resolution)] コマンドを選択することによってのみ不正の場所を表示できます。

WCS Base では、不正は、ロケーション情報なしで検出中の AP の横（直近ではない）に表示されます。 WCS Base および WCS Location でサポートされている機能の詳細については、「WCS Base と WCS Location の比較」を参照してください。

注: ファームウェア リリース 4.0 には、Cisco Bug ID CSCse96812（登録ユーザ専用）および CSCsf17545（登録ユーザ専用）があり、不正アクセス ポイントのリストで不正クライアント カ

ウントが常にゼロになります。 この問題の回避策は、コントローラ上の不正アクセス ポイント リストを直接参照して正しいカウントを確認することです。

WCS のアクセス ポイント（AP）偽装機能の使用

AP の偽装機能により、有効な Cisco 1000 Series LAP への偽装を試みる不正な AP の検出が改善されます。 この機能は無線周波数（RF）のネットワーク グループを作成するもので、同じグループにある Cisco 1000 Series LAP どうしが、互いに Radio Resource Management（RRM）のネイバー パケットを配信し合います。 Cisco 1000 シリーズ LAP が、別の Cisco 1000 シリーズ LAP からパケットを受信したにもかかわらず、同じ LAP から RRM ネイバー パケットを受信していない場合、新しい AP が Cisco 1000 シリーズ LAP に偽装していると想定できるため、それは不正な AP として報告されます。

WCS が WLAN 内の別の AP に偽装している AP を見つけると、次のアラートが WCS サーバに表示されます。

```
AP Impersonation with MAC '00:14:1b:62:4e:42' is detected by authenticated
AP '00:14:1b:62:4e:40' on '802.11b/g' radio and Slot ID '0'
```

コントローラでは、次のトラップ ログ メッセージに問題の発生元の MAC アドレスが表示されます。

```
Apr 10 11:21:16 <SomeIPAddress> [WARNING] apf_rogue.c 1890: Possible AP
impersonation of 00:14:1b:62:4e:42, using source
address of 00:90:4b:8a:de:c3, detected by 00:14:1b:62:4e:40 on slot 0.
```

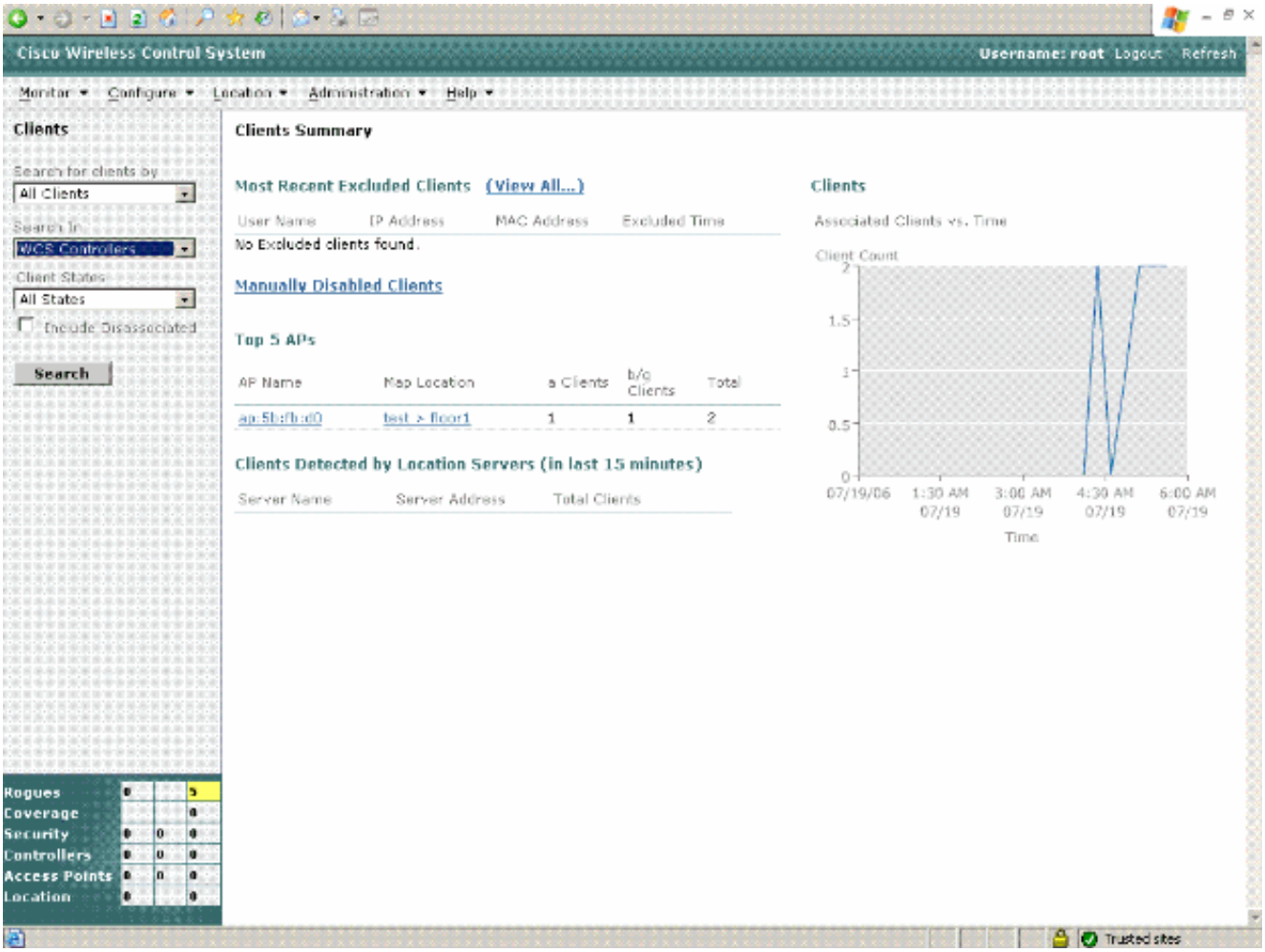
AP の偽装に関連する WCS エラーログの詳細は、Cisco Bug ID CSCsb90622（登録ユーザ専用）を参照してください。

AP の偽装は、Lightweight Access Point Protocol（LWAPP）や Wireless LAN Context Control Protocol（WLCCP）で通信を行わない Cisco MAC アドレスをアドバタイズする AP が見つかった場合に、IDS によってレポートされます。 LWAPP モデルでは、WCS はコントローラによるすべての AP 示数の解釈から、不正な AP のおおよその場所を特定できます。

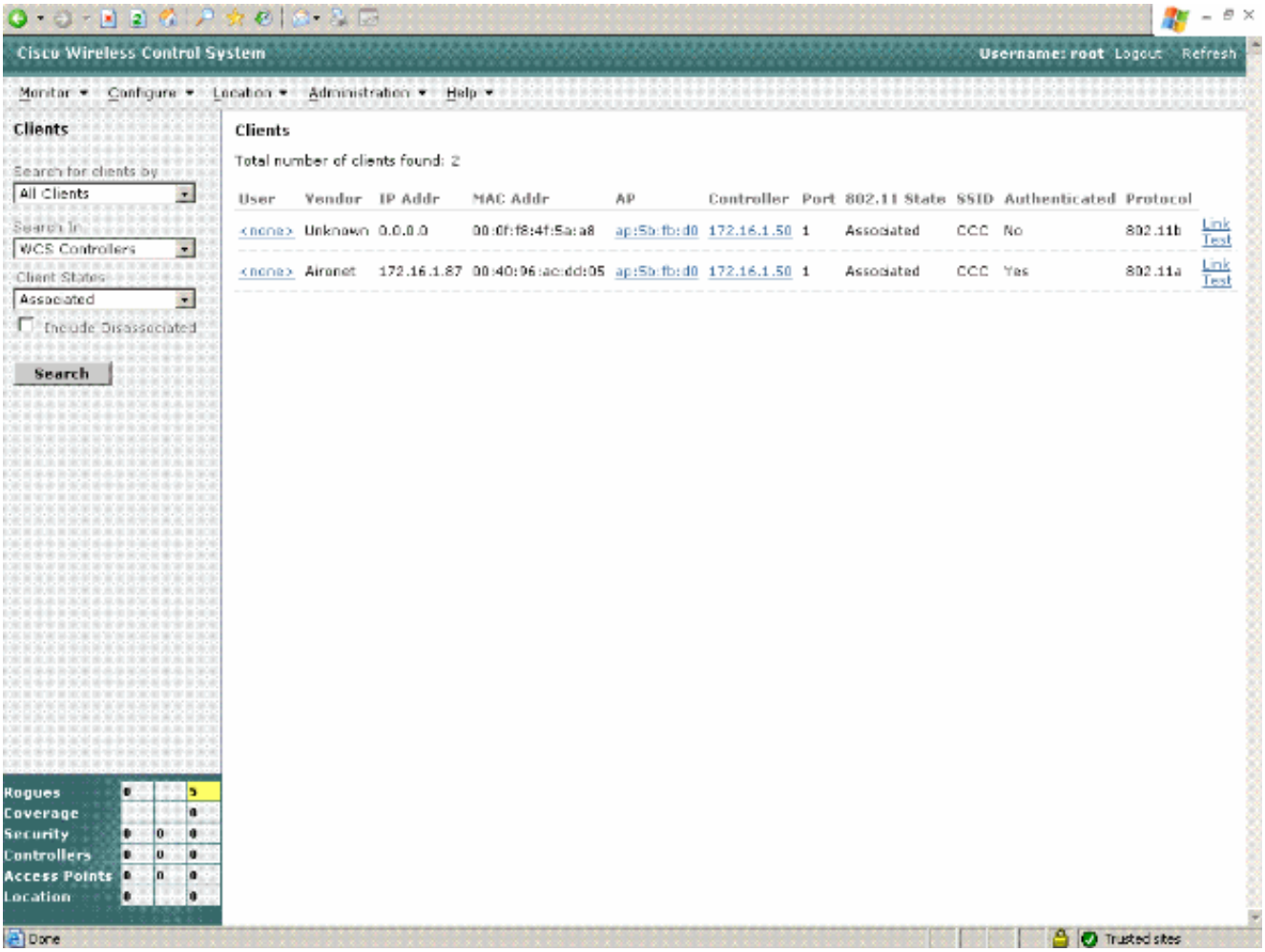
クライアントの場所の特定

Cisco WCS では、システム オペレータは企業内のクライアントの場所を特定できます。 次の手順を実行します。

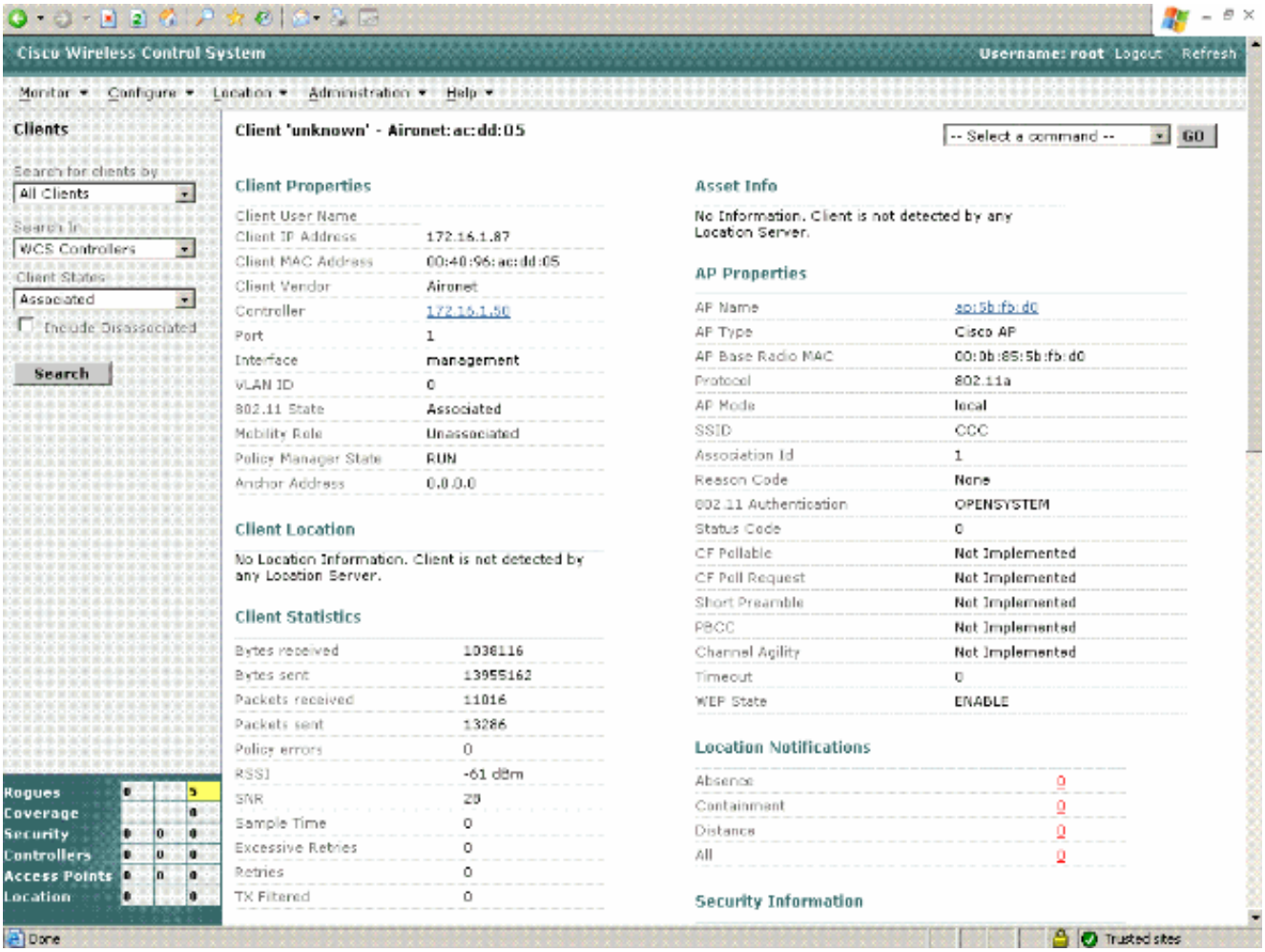
1. [Monitor] > [Devices] > [Clients] の順に選択して、[Clients Summary] ページに移動します。



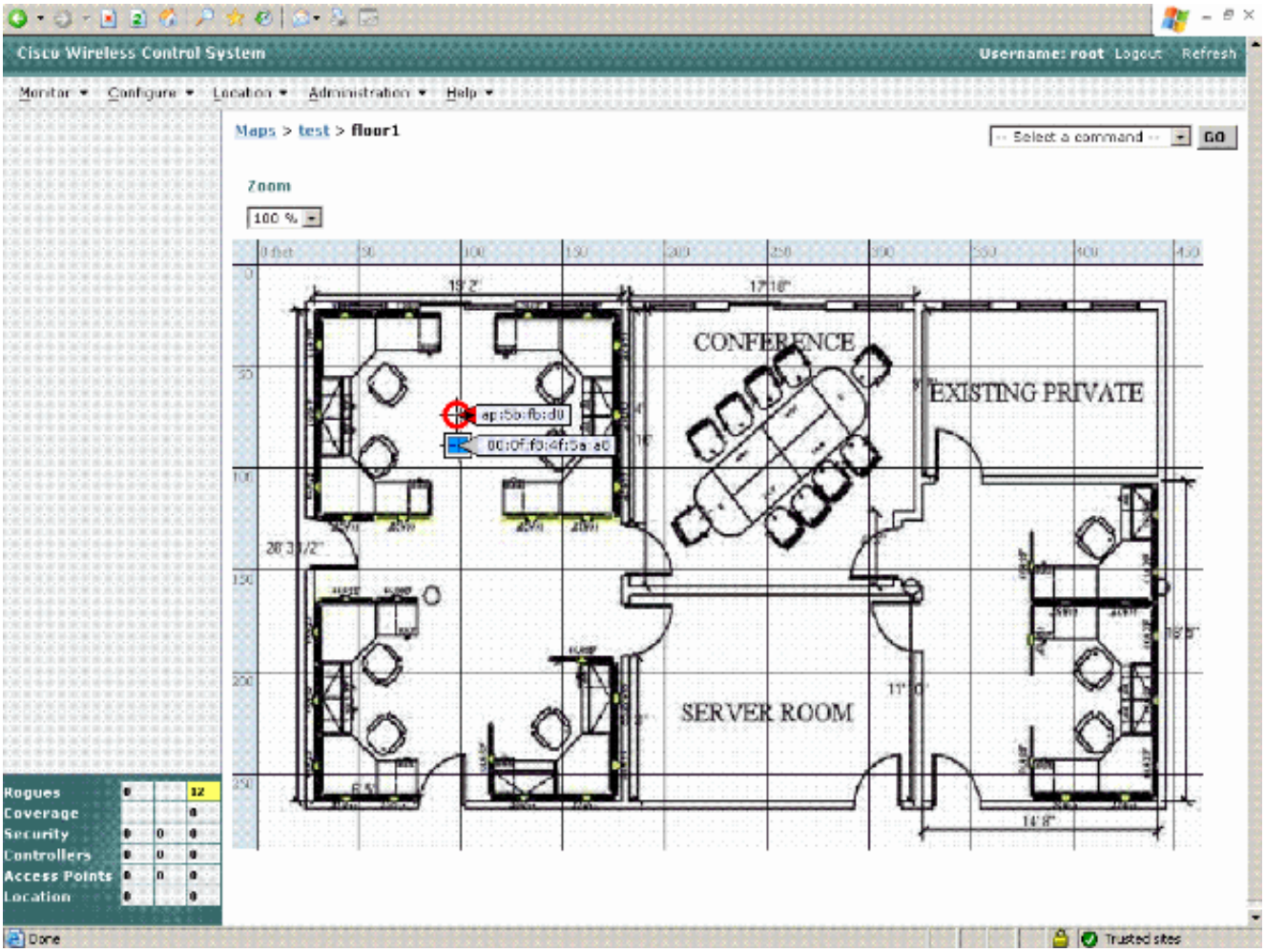
2. [Clients Summary] ページの左側のサイドバーで [All Clients] を検索して、Cisco WCS に [Clients] ページを表示します。



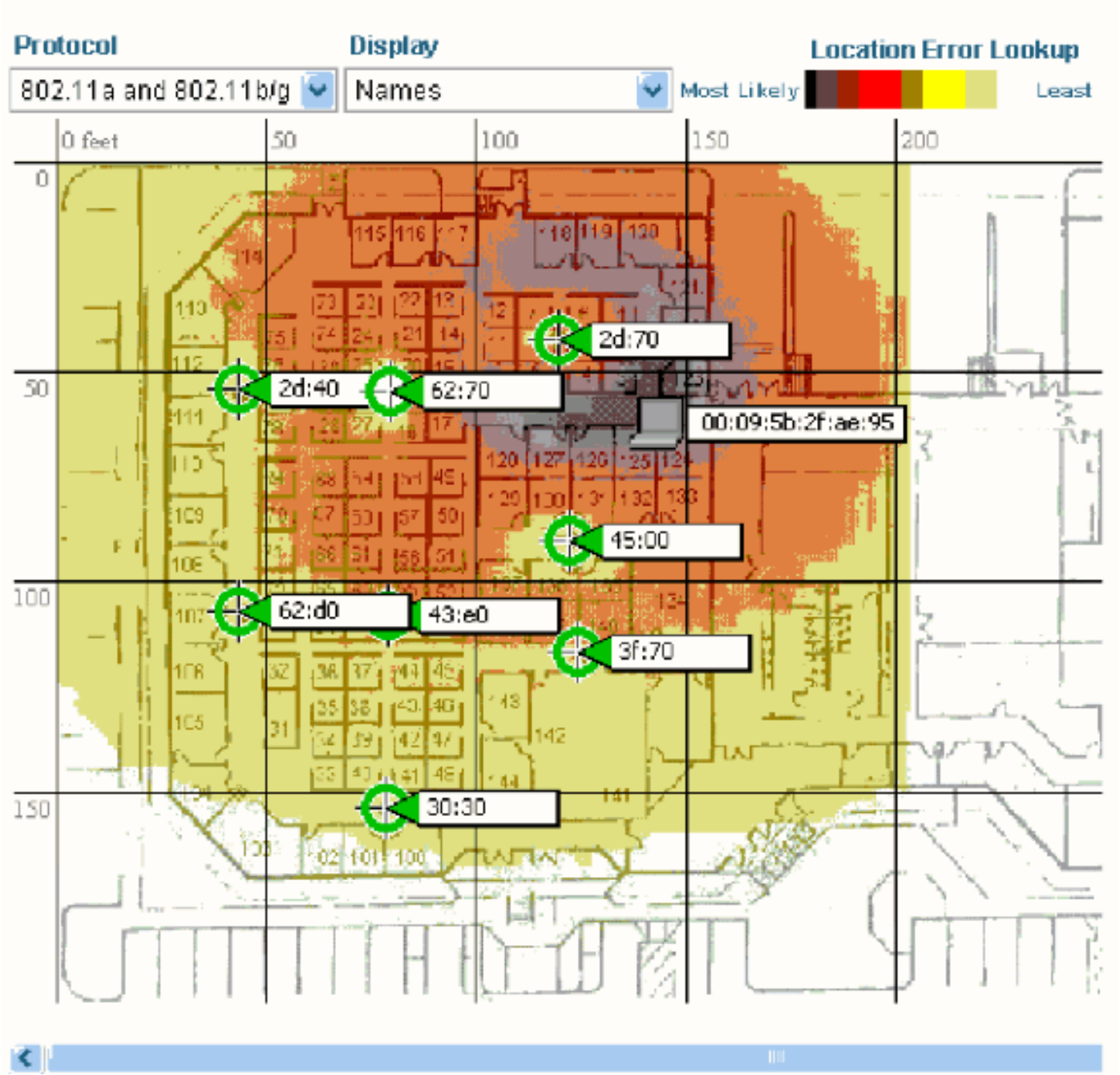
3. [Clients] ページから、場所を確認するクライアントの [User Name] をクリックします。Cisco WCS に対応する [Clients <client name>] ページが表示されます。



4. [Clients <client name>] ページからクライアントを検索する方法は 2 通りあります。ドロップダウン メニューで [Recent Map (high/low resolution)] を選択してクライアントの関連付けを解除せずにクライアントの場所を特定する。ドロップダウン メニューで [Present Map (high/low resolution)] を選択してクライアントの関連付けを解除し、再度関連付けた後にクライアントの場所を特定する。 これを選択した場合、Cisco WCS の警告メッセージが表示され、続行するかどうかが確認されます。 次に例を示します。



次の図で、クライアントの位置を示す Heat Map を参照してください。



注: Cisco WCS Location は、2 つ以上の Cisco 1000 シリーズ LAP からの RSSI 信号強度を比較することで、最も可能性の高いクライアントの場所を特定し、その場所に小さなラップトップのアイコンを付けます。 Cisco WCS Base はクライアントからの RSSI 信号強度を比較し、クライアントから最も強い RSSI 信号を受信している Cisco 1000 シリーズ LAP の隣に小さなラップトップのアイコンを付けます。

注: 通常、ラップトップをシャット ダウンすると、WLC または WCS がクライアントのリストからクライアントを削除する前に長時間かかります (分単位)。 引き続き「associated」と表示されます。 これは、ユーザ アソシエーション情報を制御するタイマーが、アイドル タイムアウトとセッション タイムアウトの 2 種類あるためです。 この両方のタイマーを変更できます。 次にデフォルト タイマーを示します。

- [Idle Timeout]：300 秒。
- [Session Timeout]：1800 秒

WLAN ネットワークのカバレッジ ホール

カバレッジ ホールとは、クライアントが無線ネットワークからの信号を受信できない領域です。 Operating System Radio Resource Management（RRM）は、このようなカバレッジ ホールの領域を見つけ出し、Cisco WCS へ報告します。 これにより、IT 管理者はユーザの要求に応じてホールを埋めることができます。

Cisco WCS に [Top 5 Coverage Holes] が表示されたら、Cisco WCS ユーザ インターフェイス ページの左下にある [Coverage] インジケータをクリック（または [Monitor] > [Alarms] を選択し、[Alarm Category - Coverage] を検索）して、Cisco WCS に [Coverage Hole Alarms] ページを表示します。 [Coverage Hole Alarms] ページで、[Monitor] > [Maps] を選択し、Cisco 1000 シリーズ LAP の名前で、アクセス ポイントを検索します（この検索ツールは大文字と小文字が区別されます）。 Cisco WCS に、Cisco 1000 シリーズ LAP 配置されている場所のフロアまたは屋外のエリアをリストする [Maps > Search Results] ページが表示されます。 リンクをクリックして関連する [Maps > <building name> > <floorname>] ページを表示します。

[Maps > <building name> > <floor name>] ページで、カバレッジ ホールを報告した Cisco 1000 シリーズ LAP の近辺にある低信号強度エリアを探します。 これらが、カバレッジ ホールである可能性が最も高い場所です。 信号強度の弱い領域がなさそうならば、フロア プランのマップが正しいことを確認します。 また、Floor Plan Editor を使用して .FPE ファイルを作成した場合は、金属製の物、たとえば壁、エレベーターシャフト、階段室、本棚などを見落としていないことを確認します。 もしある場合はそれらを .FPE フロア プラン ファイルに追加し、古いフロア プランを新しいフロア プランに替えます。

マップのインポートが困難な場合

Cisco WCS では、ユーザは管理対象の WLAN ネットワークを、臨場感のあるキャンパス、建物、およびフロア プラン マップ上に表示できます。 フロア、キャンパス、または建物のプランをイメージ ファイルとして Cisco WCS にインポートし、適切な場所にデバイスを追加できます。 Cisco WCS では、次のタイプのイメージをサポートしています。

- .PNG 形式
- .JPG 形式
- .JPEG 形式
- .GIF 形式

マップを Cisco WCS にインポートする際に問題が発生する場合は、サポート外のイメージ形式が原因である可能性があります。 この問題を解決するには、Microsoft Paint でイメージを開き、**<filename>.GIF** としてファイルを保存します。 その後、もう一度イメージをインポートしてみます。

場合によっては、元のイメージ ファイルが高品質でも、インポートしたイメージ ファイルが WCS では非常に低品質で表示されます。 この問題の考えられる原因の 1 は、イメージ自体にあります。 WCS では、マップの一部であると想定してイメージを囲む空白文字 1 字を組み込みます。 この結果、WCS のマップ エディタで低表示品質になる可能性があります。 イメージ ファイルをトリミングして空白文字を削除し、WCS に新しいイメージをインポートしてみてください。

Cisco WCS に対するマップの追加についての詳細は、「マップの追加および使用」を参照してください。

Cisco WLC からネットワーク デバイスへの ping

Cisco WLC から他のデバイスへ ping を行うには、次の手順を実行します。

1. [Configure] > [Controllers] を選択し、[IP Address] 列の下の IP アドレスをクリックして、Cisco WCS に [<IPaddress> > Controller Properties] ページを表示します。
2. [<IPaddress> > Controller Properties] ページで左側のサイドバーに移動し、[System] > [Commands] を選択して、Cisco WCS に [<IPaddress> > Controller Commands] ページを表示します。
3. [<IPaddress> > Controller Commands] ページで、[Switch] から [Administrative Commands] > [Ping] を選択し、[GO] をクリックします。
4. Enter an IP Address (x.x.x.x) to Ping ウィンドウで、Cisco WLC が ping を行うネットワーク デバイスの IP アドレスを入力し、OK をクリックします。
5. Cisco WCS の Ping Results ウィンドウに、送受信されたパケットが表示されます。 Restart をクリックして、もう一度ネットワーク デバイスに ping を行うか、または Close をクリックして、ネットワーク デバイスへの ping を終了し、Ping Results ウィンドウを閉じます。

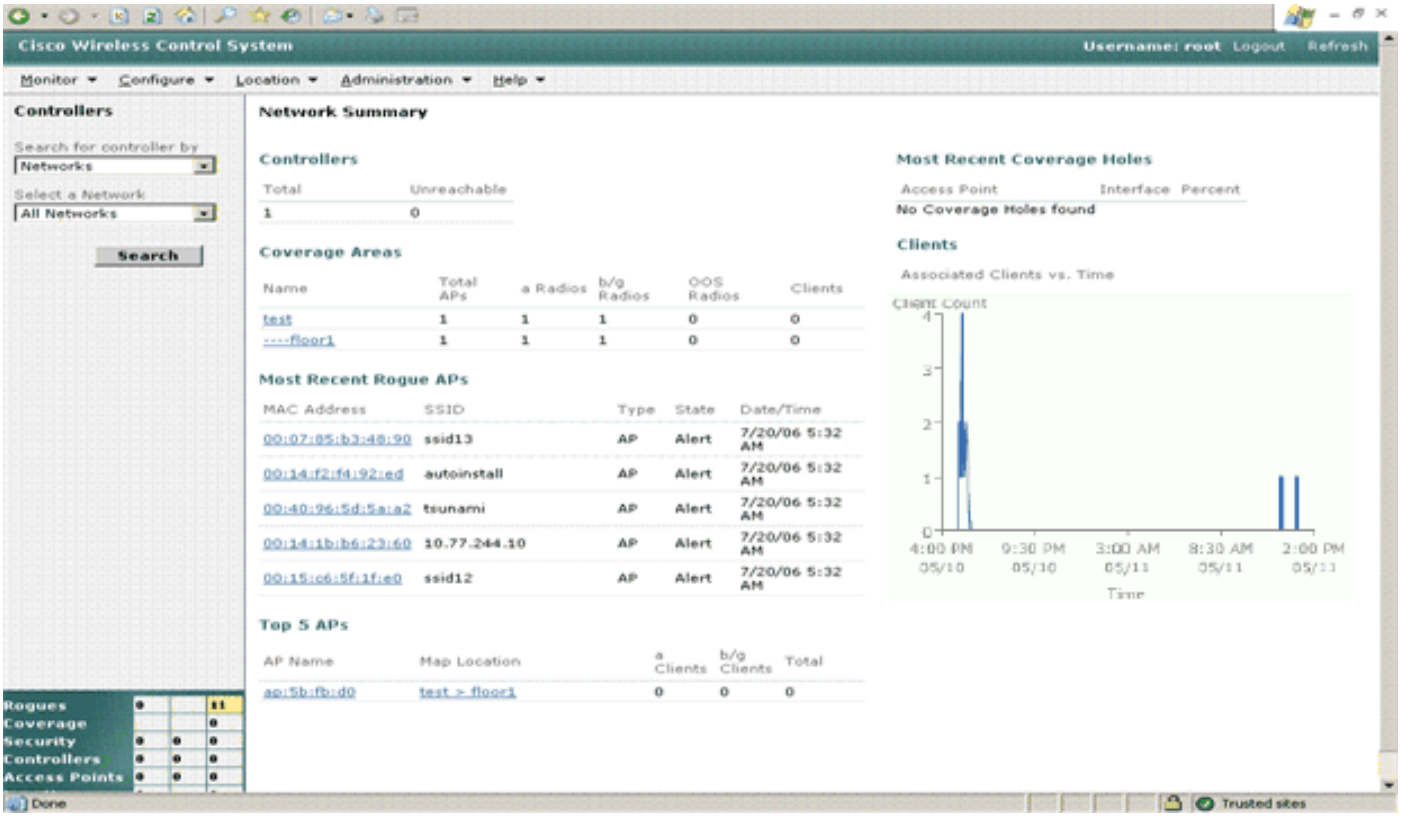
現在の Cisco WLC のステータス、設定、および統計の表示

Cisco WLC および Cisco 1000 シリーズの IEEE 802.11a/b/g LAP を Cisco WCS データベースに追加した後、Cisco WLAN Solution のステータスを表示できます。

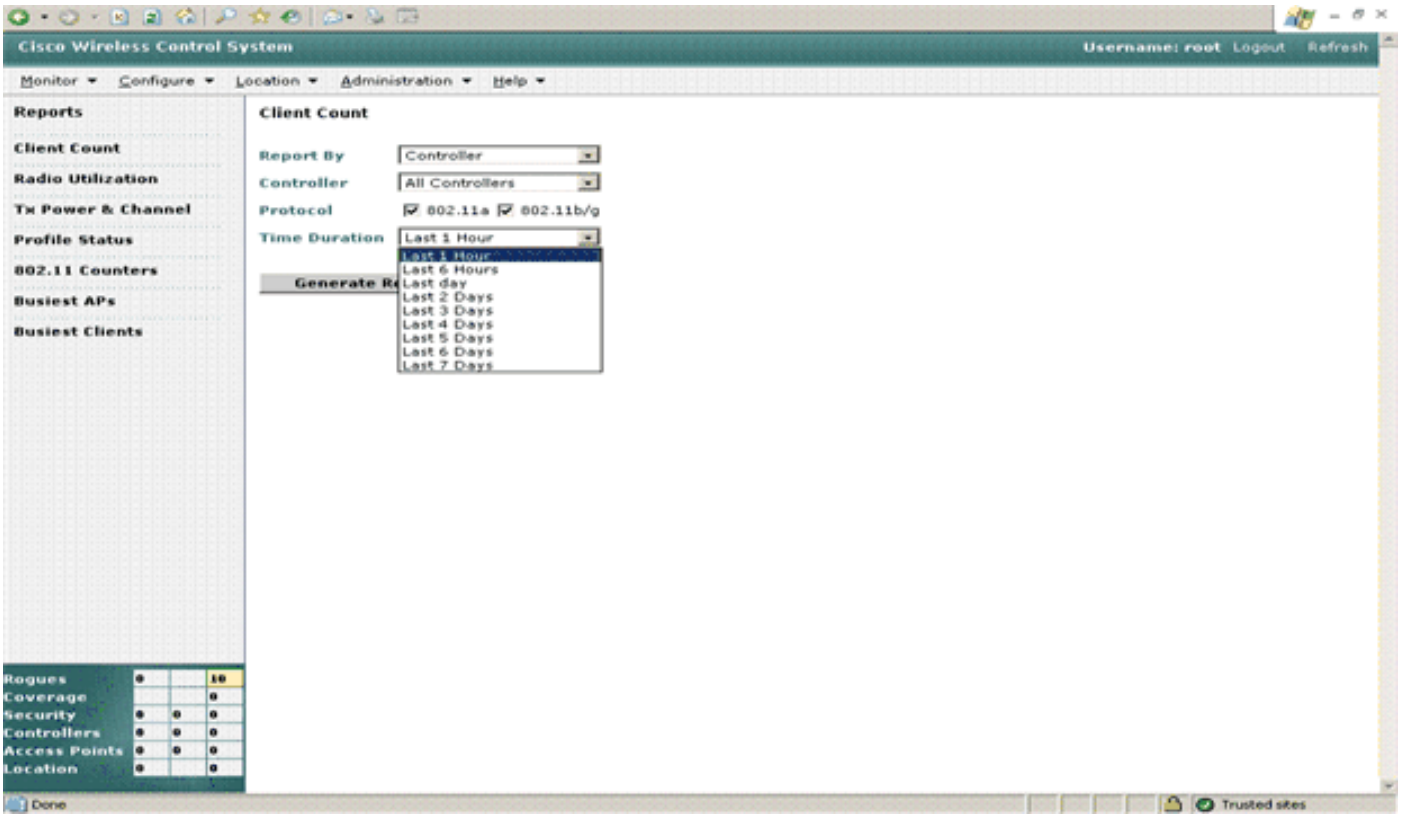
注: ロケーション アプライアンスなしでクライアントまたはタグを検索する際は、WCS データベースに WLC のコントローラを指定する必要があります。 これは、WCS がデフォルトで常に「ロケーション サーバ」を設定するためです。

注: サーバの IP アドレスを変更する前に、WCS アプリケーションを手動で停止し、シャットダウンにする必要があります。 アプリケーションを停止しないでサーバをリブートすると、データベースが破損するおそれがあります。

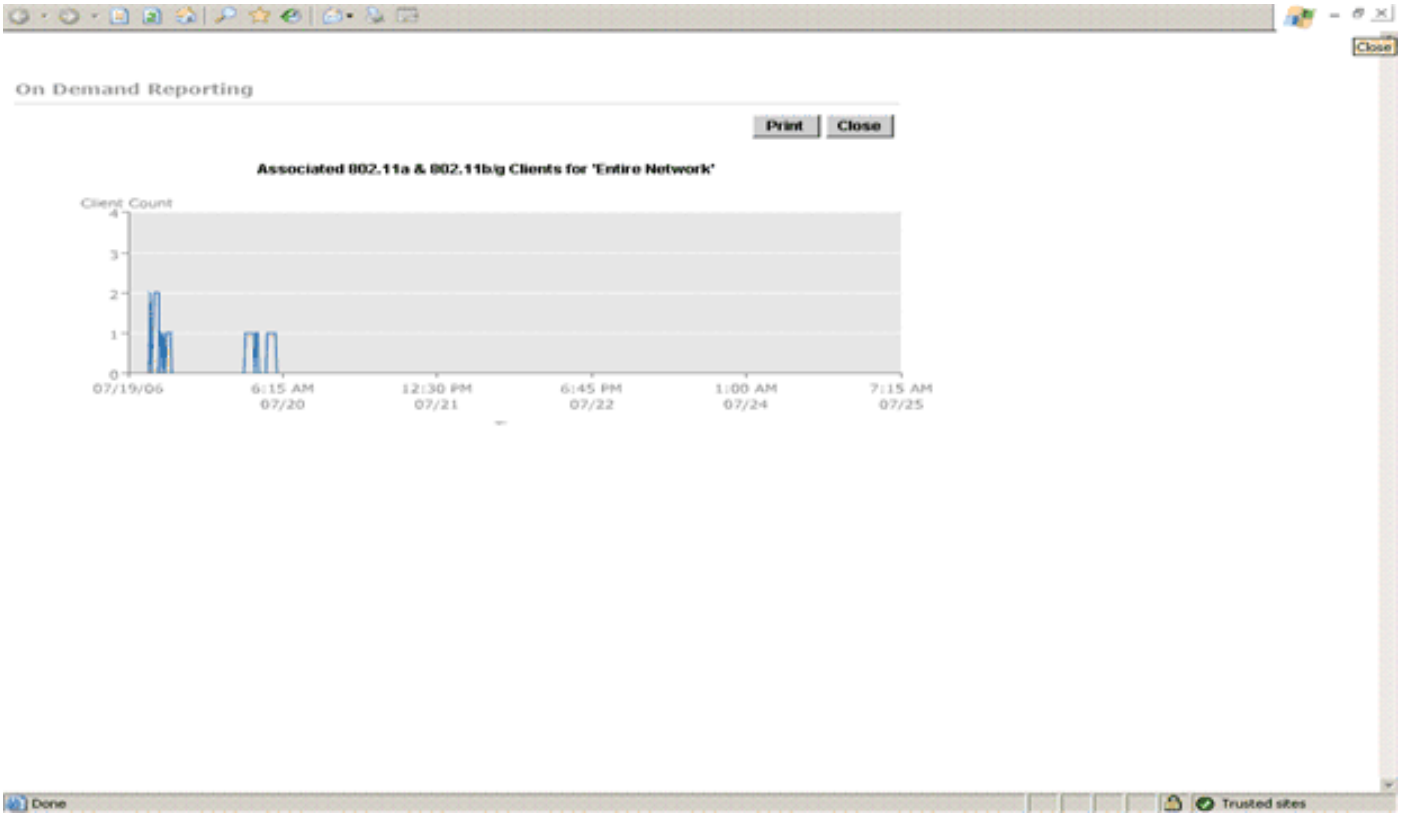
Cisco WCS ユーザ インターフェイスで、[Monitor] > [Network] の順に選択して、[Monitor Network Summary] を表示します。 次に例を示します。



Cisco WCS は、RSSI、SNR、プロファイルの障害、クライアント数、不正なアクセス ポイントの傾向、ビジー クライアントなどの統計情報を定期的に収集し、それらをレポートにまとめます。 これらのレポートを表示するには、[Monitor] > [Reports] のウィンドウを使用します。



802.11a/b/g クライアントの最近 7 日間におけるクライアント数のレポートの例を、次に示します。



これらのレポートは、効果的なトラブルシューティング ツールとしても使用できます。

位置の準備状態の調査

位置の準備状態の調査は、Location Appliance バージョン 2.1.34.0 で導入された機能です。 この機能を使用すると、少なくとも 90 % の時間、10 m 以内の要素の真の場所を推定する、既存のアクセス ポイント導入の機能を WCS で検証できます。 位置の準備状態の計算は、アクセス ポイントの数と配置に基づいています。

WCS から位置の準備状態を確認するには、[Monitor > Maps] ページにあるメニューから [Inspect Location Readiness] を選択します。 10 m、90 % の ロケーションの仕様を満たすエリア（Yes）および満たさないエリア（No）を示す色分けされたマップが表示されます。

WCS とロケーション サーバの同期に関する問題

ロケーション アプライアンスと同期する WCS に関する問題があることがあります。 WCS のネットワーク ダイアグラムは、ロケーション アプライアンスと同期していない可能性があります。この同期の問題には、かなりの多くの原因があります。

- ネットワーク設計のサイズが 30 Mb の最大限度を超えている可能性があります。 Cisco Bug ID CSCse60657（登録ユーザ専用）でこの問題をより明確に扱ってあります。したがって、キャンパスにある建物の数と各建物のフロア数を含む全体的なサイズが 30 Mb の最大制限を超える可能性があるキャンパスの図を同期しようとすると、この同期プロセスは失敗します。この問題は、ロケーション アプライアンスのログを調べてこのメッセージを確認することによってさらに検証できます。`TRACE[com.aes] THROW com.aes.server.cmn.AesServerException: Server Exception: Message sizeexceeded: 37176782` このサイズの制限は、次の WCS バージョンで解決されます。
- もう 1 つの考えられる原因は WCS にロードされるイメージの解像度が高すぎることであり、おそらく、1024x768 の有効な解像度を超えていることです。 ロケーション アプライアンスとこのようなイメージを同期する際に、同期プロセスは失敗します。 このような場合、この問題を軽減するには、解像度を低くします。
- 最新バージョンの WCS およびロケーション サーバを実行していることを確認します。 すべてのデバイスで時間と日付が正確に一致にしていることも確認します。これは、次の出力を見ると確認できます。WCS での **date and time** コマンドの出力locserver での **date** の出力 WLC での **show time** コマンドの出力
- もう一つの可能性のある解決策は、ロケーション サーバを停止し、ロケーション サーバのコンソールで次のコマンドを使用してデータベースを削除することです。**rm -rf /opt/locserver/db/linux/server-eng.db** ここで、**/opt/locserver/db/linux/server-eng.db** はロケーション サーバ データベースのディレクトリです。コマンド **/etc/rc.d/init.d/locserver restart** を使用してロケーション サーバを再起動します。次に、デバイスを再同期化してみます。

WCS と WLC の同期に関する問題

同期の問題が WCS と WLC の間で発生する可能性があります。 この問題が原因で、アクティブ クライアントの数が WLC と WCS で異なる場合があります。 コントローラと WCS を同期するには、次の手順を実行します。

1. [Configure] > [Controllers] を選択し、[IP Address] リストの上部にあるチェックボックスをクリックしてすべてのコントローラを選択します。
2. [Select a Command] ドロップダウン リストから、[Save Config to Flash] を選択します。
3. [OK] をクリックします。これは、SNMP が適切に機能すること、コントローラが WCS の

支持どおりに動作することを確認する、基本的なテストになります。
4. [Configure] > [Controllers] を選択し、[IP Address] リストの上部にあるチェックボックスをクリックしてすべてのコントローラを選択します。
5. [Select a Command] ドロップダウン リストで、[Refresh Config from Controllers] を選択します。
6. [OK] をクリックします。このアクションにより、WCS では、これまでに得たどんな情報よりもコントローラからの新情報を信用するようになります。

テンプレートを WCS から WiSM にプッシュしたときに、DHCP 設定が破損

汎用テンプレートが WCS から Wireless Services Module（WiSM）へプッシュされると、コントローラの Dynamic Host Configuration Protocol（DHCP）設定が破損する可能性があります。 このテンプレートは、WiSM とまったく同じオプションを保持できます。

主な影響は、DHCP オファー メッセージがドロップされることであり、したがってクライアントは DHCP アドレスを受け取りません。 次のメッセージがコントローラに記録されます。

```
Thu Jul 13 05:05:07 2006 [VERBOSE] dhcpd.c 164: Dropping packet from
192.168.80.23 (unable to match to a dhcp scope)
```

この問題は Cisco Bug ID CSCse98623（登録ユーザ専用）が原因で発生します。 WCS で汎用テンプレートを使用しないでください。 DHCP の転送を回復するためには、設定を手動で復元する必要があります。 このバグは、WCS ファームウェア バージョン 4.0.87.0 以降で修正されています。

WCS ヒートマップに誤った正方形カバレッジ ホールが表示される

WCS ヒートマップに誤った正方形カバレッジ ホールが表示されます。 カバレッジ ホールが正方形または長方形になることはありません。 ヒート マップの放射パターンは円形です。 この問題は、ありえない特定の四角形のホールがマップ上に示されることにあります。 トレースの編集はマップで実行されていません。 サイト調査ツールを使用して、カバレッジ ホールが存在しないことが確認されています。 この接続は、次の領域で非常に強力です。

これは、Cisco Bug ID CSCsf19291（登録ユーザ専用）に関連しています。 ドロップダウン メニューから [Recompute Prediction] オプションを選択し、予測を再計算します。 ヒート マップが円形になり、正方形のカバレッジ ホールは存在しません。 この問題はバージョン 4.0 で修正されていますが、バージョン 3.0 から移行であれば、小規模フロアでこの問題がある可能性があります。

不正 AP テンプレートは、どのような場合に WLC に適用されますか。

不正アクセス ポイント（AP）のテンプレートは、次の 2 つの条件が満たされる場合のみコントローラに適用されます。

- コントローラの AP が不正 AP を検出した。
- 不正 AP スケジュール作業が完了している。

WCS サーバのポート

WCS アプリケーションが実行されているサーバでファイアウォールを実行する場合は、WLC と通信するために複数のポートを開ける必要があります。 Apache.exe、JavaService.exe、

Solid.exe など、WCS サーバで実行されるサービスがあります。 TCPView では、出力は次のように表示されます。

```
Apache.exe:1712 TCP 0.0.0.0:443 0.0.0.0:0 LISTENING
JavaService.exe:1680 TCP 0.0.0.0:21 0.0.0.0:0 LISTENING
solid.exe:2672 TCP 0.0.0.0:1315 0.0.0.0:0 LISTENING

Apache.exe:208 TCP 127.0.0.1:1268 127.0.0.1:8009 ESTABLISHED
JavaService.exe:1680 TCP 127.0.0.1:1067 127.0.0.1:1315 ESTABLISHED
JavaService.exe:1680 TCP 127.0.0.1:1068 127.0.0.1:1315 ESTABLISHED
solid.exe:2672 TCP 127.0.0.1:1315 127.0.0.1:1083 ESTABLISHED
solid.exe:2672 TCP 127.0.0.1:1315 127.0.0.1:1082 ESTABLISHED
```

WLC で作業するには、UDP 161 (SNMP)、UDP 162 (SNMP トラップ)、TCP 443 (HTTPS) など、いくつかのポートのみを開けます。 次の表は、トラフィックの一部がブロックされる場合に、有用である可能性のあるポートのリストを示します。

サービス	ポート	Port Numbers
SNMP	UDP	161
SNMP トラップ	UDP	162
HTTPS	TCP	443
Advent Net	TCP	2000
データベース	TCP	1315
FTP	TCP	21
HTTP コネクタ	TCP	8457
HTTP コネクタのリダイレクト	TCP	8457
HTTP	TCP	80
RMI	TCP	1299
TFTP	UDP	69
Web コンテナ	TCP	8009

WLAN で除外リストが有効に設定されていることを確認

WLAN で**除外リストが有効**に設定されていることを確認するには、次の手順を実行します。

1. [Configure] > [Controller] の順に選択します。
2. [IP Address] 列で IP アドレスをクリックします。
3. 左側の [WLAN] をクリックします。
4. 各 WLAN ID をクリックして [Checked] に設定されていないことを確認します。

除外リストの有効のトラブルシュート

除外リスト有効のトラブルシューティングを行うには、次の手順を実行します。

1. クライアントを追跡します。
2. 除外クライアントの WLAN を確認します。
3. **削除**する除外クライアントを選択します。
4. 指定されたコントローラの下の除外リストからクライアントを削除します。

グローバルで無効なクライアントの表示および削除

グローバルで無効化されているクライアントを表示して削除するには、次の手順を実行します。

1. [Monitor] > [Devices] > [Clients] の順に選択します。
2. [Manually Disabled Clients] をクリックします。
3. このページにアクセスする MAC アドレスを選択します。
4. [Delete] をクリックします。

コントローラごとの手動で無効にしたクライアントの表示および削除

セキュリティなど複数の理由により、特定のクライアントは「手動で無効化したクライアント」としてブラックリストに載せることができます。

WCS に追加された各コントローラで、手動で無効化されたクライアントを個別に表示するには、次の手順を実行します。

1. WCS GUI に移動します。
2. [Configure] > [Controllers] の順に選択します。
3. 手動で無効にされたクライアントを表示する必要のあるコントローラの [IP Address] 列の下で IP アドレスをクリックします。
4. 表示されるページで、[Security] を選択し、[Manually Disabled Clients] をクリックして、この特定のコントローラに対する [Manually Disabled Clients] のリストを表示します。

左のドロップダウン メニューから、[Delete Manually Disabled Clients] を選択して手動で無効にしたクライアントを削除します。

建物ごとのクライアントの WCS 検索が機能しない

この問題は Cisco Bug ID CSCse97619（登録ユーザ専用）が原因で発生する可能性があります。1 つの建物の 1 フロアのクライアントを対象とする WCS 検索は正しく機能しますが、1 つの建物の全フロアのクライアントを検索すると機能しません。 このバグに対する修正は、WLS バージョン 4.0.87.0 で提供されています。 4.0.87.0 よりも前の WCS バージョンを使用する場合、回避策は、フロア エリアのクライアントを検索することです。

H-REAP モードでは WCS が報告する AP に関連付けられたクライアント数が不正確

この問題は Cisco Bug ID CSCsg48059（登録ユーザ専用）が原因で発生します。 H-REAP がコントローラで有効になっている場合、WCS は多すぎるクライアント数をレポートします。 AP または特定のコントローラに関連付けられているクライアントの数を調べるための回避策は、[WCS Monitor] > [Clients] 機能を使用し、AP またはコントローラで検索し、検索された項目の合計数を正しいクライアント数として使用することです。この検索は、重複を防ぐため、無線のタイプによって限定されています。 bsnMobileStation テーブルには、クライアントの数に対する正しい数の行もあります。 また、WLC を使用して、正しいクライアント数を確認することもできます。

サーバ/ホストに名アンダースコアが設定されていると WCS が起動しない

アンダースコア文字「_」は、WCS サーバ名ではサポートされていません。 WCS インストール

でサーバ/ホスト名にアンダースコアを使用すると、WCS は起動しません。 ソフトウェアのインストールで問題が報告されず、通常どおりにインストールされる一方で、RFC-952 ではアンダースコアがサポートされていない文字であることを示しています。これが WCS ソフトウェアが失敗する理由です。

ERROR[location] Failed to Create Heat Map for MAC: xx: xx: xx: xx: xx: xx Reason: Failed as the RSSI List is Empty After Time Pruning

正確なローカル時間を保証するために、コントローラ、ロケーション サーバ、および WCS のすべてで、Network Time Protocol（NTP）を使用する必要があります。 ロケーション サーバでは、15 分のウィンドウに入らない、コントローラからのすべての日付をドロップします。

コントローラでは内部的に 1 種類の時刻のみを保持しますが、オフセットが指定されると表示用に変更します。 オフセットを指定すると、入力される時間が UTC 時間（英国ロンドンの現地時間）であり、コントローラで表示するときはオフセットを追加して現地時間を表示するようにコントローラに通知します。 NTP は常に UTC 時間であるため、コントローラで現地時間を表示するにはオフセットが必要です。 たとえば、EST のオフセットは -5 です。 NTP が設定されている場合、コントローラは UTC 時刻を取得しますが、ログのタイムスタンプ用にオフセットを追加して現地時間を得ます。

コントローラ、ロケーション サーバ、および WLC は、いずれも、WCS の内部時刻（オフセットを加えた内部時刻であるローカル時刻ではない）の差はすべて 15 分以内で**なければならず**、そうでない場合、ロケーション サーバではクライアントを表示も追跡もしません。 代わりに、ロケーション サーバのログに次のエラー メッセージが示されます。

```
3/08/07 00:46:59 ERROR[location] Failed to create heat map for MAC: xx:xx:xx:xx:xx:xx Reason:
Failed as the RSSI list is empty after time pruning
```

ロケーション サーバのリアルタイム ストレージは 15 分前までのデータしか保存することができません。 ロケーション サーバではリアルタイムでクライアントを追跡する一方で、WCS ではこのデータを長期間アーカイブすることに注意してください。 WCS はクライアントを追跡しますが、更新はリアルタイムではなく数分おきのみです。 デバイス間でクロックがオフに設定されている場合、ロケーション サーバがリクエストで指定された時間間隔以外のクライアント データを削除するため、データを参照できなくなります。 実際に、ロケーション サーバが内部時刻と 15 分を超える差異のある内部タイムスタンプのデータをコントローラから受け取ると、そのデータをビット バケットへ投げてしまいます。

WLC、WCS、ロケーション サーバの内部時刻を UTC に自動的に同期するには、NTP をオンにする必要があります。

エラー メッセージ「The Procedure Entry Point_FIIfexp_Could Not be Located in the Dynamic Link Library DFORRT.DLL」の表示

WCS で MATLAB コンパイラなどのサード パーティ アプリケーションを使用しており、MATLAB で特定のバージョンの DFORRT.dll ライブラリを使用する場合に、アプリケーションで c:\windows\system32 に DFORRT.dll ライブラリをすでにインストールしてあると、WCS が正しくインストールされていません。 その結果、WCS を起動すると、このエラー メッセージが表示されます。

```
The procedure entry point _FIIfexp_ could not be located in the dynamic link library DFORRT.DLL
```

この問題を修正するには、DFORRT.dll ファイルを c:\windows\system32 から削除して WCS を再インストールします。

3 台のデバイスを同期する手順

ロケーション サーバの場合： 初期設定内については、『インストレーション コンフィギュレーション ガイド』を参照してください。

日付、時刻、タイム ゾーンを変更するには、アプライアンスの起動後に、ロケーション サーバを停止する必要があります。 次の手順に従ってください。

1. ロケーション アプライアンスのタイム ゾーンを変更するには、/etc/localtime に適切なタイム ゾーン ファイルをコピーします。`# cp /usr/share/zoneinfo/<your country>/<your timezone> /etc/localtime`
2. 次のように ZONE の指定なしでファイル /etc/sysconfig/clock が定義されていることを確認してください。`# more /etc/sysconfig/clock`

   ```
   UTC=true
   ARC=false
   ```
3. ロケーション サーバの CLI で **date** コマンドを使用して日時を確認します。`# date`
4. http://www.cisco.com/en/US/products/ps6386/products_qanda_item09186a008078ece3.shtml#qa13 にある手順を参照してロケーション サーバを再起動します

注: ロケーション アプライアンスに NTP サーバを使用する場合は、「NTP サーバの設定」を参照してください。

WCS の場合： WCS は Windows から正確な時刻を取得します。 24 時間ごとに Windows OS を調べてシステム時刻を確認します。 WCS サーバを停止して再起動しなければ、システム時刻の変更について即座に認識しません。 クロックを右クリックし、[change time/date] を選択します。 NTP 時刻源を使用して、クロックを設定し、現地のタイム ゾーンに合わせてオフセットを手動で設定します。 通常は、すでに設定されています。

コントローラの場合： コントローラで時刻およびオフセットを確認するには、CLI コマンド **show clock** を使用します。 GUI からも実施できます。 [DST] チェックボックスをオフにするか、コマンド **config time timezone disable -8 0** -8 0 を使用します。

デバイス間の時刻の同期が完了したら、ロケーション サーバを WCS と同期する必要があります（[location-server] > [synchronize] を使用）。 これは、同じタイムスタンプと同じデータにするための作業です。

WCS コントローラおよびロケーション ソフトウェアが同じ日付にリリースされていることに注意してください。

WLAN テンプレートで WLC の正しい [Broadcast SSID] 設定が適用されない

WLAN テンプレートを作成し、WCS から WLC にロードすると、WCS WLAN テンプレートの設定に関係なく、個々のコントローラ WLAN 設定画面で [Broadcast SSID] フィールドがオンのままになっています。 この結果、WLAN SSID 情報が常にブロードキャストされます。

WCS を使用して現在の WLAN テンプレートのブロードキャスト SSID を無効にするには、4.1.83 よりも前のバージョンの WCS で次の手順を実行します。

注: WCS をバージョン 4.1.83 にアップグレードするのであれば、結果として、この問題も解決します。 また、このような問題は、主に、コントローラと WCS が同期していないために発生します。 このような場合は、WLC と WCS を同期します。

1. WCS WLAN テンプレートで、[Admin status] ボックスを無効にするかオフにし、[Broadcast SSID] がオフであることを確認します。
2. テンプレートを保存します。
3. コントローラにテンプレートを適用します。
4. この WLAN の管理ボックスを再度有効にします。
5. テンプレートを保存します
6. コントローラにテンプレートを再度適用します。

これで、コントローラの個々の WLAN 設定での [Broadcast SSID] フィールドがオフになっていることを確認できます。

WLAN テンプレートに正しい 7920 CAC のチェックボックス設定が表示されない

コントローラに WLAN をプッシュする WLAN テンプレートを作成するとき、[7920 CAC] チェックボックスをオンにして機能を有効にし、保存して同じ WLAN を再度表示します。 このテンプレートは、実際にはオンされており、コントローラにプッシュされたときにこの機能が有効になりますが、オフで表示されます。

これは、この問題に関連するバグ CSCsi77521 が原因です。

この問題を解決するにはバージョン 4.1 に WCS をアップグレードします。

WCS バージョン 3.2.51.0 からオフラインのコントローラを削除できない

場合によっては、すでに使用されていない WLC をユーザが WCS から削除できません。 これは、バージョン 3.2.51.0 の WCS のデータベース構造に関する問題によります。 その結果、WCS はリソースをロックアップする傾向があります。 バージョン 4.0 ではデータベース全体が再構成されており、パフォーマンス レベルが向上しました。

この問題には 2 つの回避策があります。

- 監査レポートを削除してからコントローラを削除する、**または**
- WCS 4.0.87.0 以降にアップグレードします

最初のオプションの場合に、オフラインのコントローラを削除するには、この操作を実行します。

1. WCS がコントローラの非常に大きなプールをモニタする場合は、最良の方法は、まず、これらのコントローラの監査レポートを 1 つずつ削除し、次に、これらのコントローラの削除を試行します。 監査レポートを削除するには、次の手順を実行します。[Configure Controller] に移動します。目的のコントローラのボックスをオンにします。 1 度に 1 台のコントローラのみ処理できます。ドロップダウン ボックスからコマンド [View Audit Reports] を選択します。[Go] ボタンをクリックします。監査レポートを削除します。次に、コントローラの削除を試行します。
2. 他のすべてのコントローラでこの手順を試行します。 これらのタスクを実行するために使用するユーザ アカウントがスーパーユーザ グループに属することを確認します。場合によっては、特定のコントローラに関する一部の監査レポートが削除される一方で一部のレポートは残ることがあります。
3. 同期ステータスが [Same in WCS and Controller] である監査レポートは正常に削除できますが、同期ステータスが [Different in WCS and Controller] である監査レポートは削除できません。

4. ステータスが [Different in WCS and Controller] である監査レポートは削除しようとすると次のエラー メッセージが表示されることがあります。`The resource you are trying to delete seems to be busy`
5. この場合、コントローラは削除できません。 このエラー メッセージは、データベースがリソースをロックしたことを意味します。 これは、ユーザが [delete] ボタンをクリックし、十分待たないで [Back] をクリックして前のページに移動することによって発生することがあります。 これはバージョン 3.2 の問題でした。 そのまま待ち、リソースが解放されたかどうかを確認します。

または、4.0.87.0 以降に WCS をアップグレードする第 2 のオプションを採用できます。このバージョンには、WCS データベースの再構造化により、パフォーマンスに関して 3.2 からの大幅な強化があります。

WCS からタイプ Default Internal で Web 認証テンプレートを追加できない

テンプレートをプッシュしようとすると、デバイスにエラー メッセージ「**SNMP operation to Device failed**」が表示されます。

これはバグ CSCsh89306 が原因で発生します。 WCS では、バージョン 4.0.206.0 が稼働するコントローラに Web 認証テンプレートをプッシュすると、SNMP エラーを示します。

回避策は、コントローラに Web 認証を直接設定することです。

1. Web 認証カスタマイゼーション テンプレートのページに移動します。
2. Web 認証タイプで [External] を選択します。
3. ダミーの URL のテキストを入力します。
4. Web 認証タイプを [Default Internal] に変更します。
5. カスタム リダイレクト URL を入力します。
6. テンプレートを保存し、適用します。

基本的に、現在の Web 認証アプリケーション タイプに関連していない場合でも、外側およびカスタム リダイレクト URL のページを空白にしておくことはできません。

関連情報

- Wireless Control System (WCS) のトラブルシューティングに関する FAQ
- Cisco Wireless Control System コンフィギュレーション ガイド、リリース 4.0
- Cisco Wireless Control System
- ワイヤレスに関するサポート ページ
- テクニカルサポートとドキュメント - Cisco Systems