無線ドメイン サービス（WDS）の設定

目次

概要

このドキュメントでは、Wireless Domain Services（WDS; ワイヤレス ドメイン サービス）の概念を紹介します。 また、1 つのアクセス ポイントまたは Wireless LAN Services Module（WLSM; ワイヤレス LAN サービス モジュール）を WDS として設定し、別の 1 つ以上のアクセス ポイントをインフラストラクチャ アクセス ポイントとして設定する方法についても説明します。 このドキュメントに概要を示した手順に従えば、WDS を機能させて、WDS アクセス ポイントかインフラストラクチャ アクセス ポイントのどちらかにクライアントを関連付けられます。 このドキュメントの目的は、高速セキュア ローミングを設定するための基礎を確立すること、または Wireless LAN Solutions Engine（WLSE）をネットワークに導入して、その機能を使用できるようにすることです。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- ワイヤレス ネットワークとワイヤレスのセキュリティ問題に関する全般的な知識
- 現行の Extensible Authentication Protocol（EAP）セキュリティ方式に関する知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco IOS® ソフトウェアが稼動するアクセス ポイント（AP）
- Cisco IOS ソフトウェア リリース 12.3(2)JA2 以降
- Catalyst 6500 シリーズ ワイヤレス LAN サービス モジュール

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな状態（デフォルト）および BVI1 インターフェイスの IP アドレスを使用して設定作業を始めています。そのため、Cisco IOS ソフトウェアの GUI または Command Line Interface（CLI; コマンド ライン インターフェイス）からユニットにアクセスできます。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

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。

ワイヤレス ドメイン サービス

WDS は Cisco IOS ソフトウェアのアクセス ポイント用の新機能で、Catalyst 6500 シリーズ ワイヤレス LAN サービス モジュールの基盤となっています。 WDS は次のような機能を有効にするコア機能です。

- 高速セキュア ローミング
- Wireless LAN Solution Engine（WLSE）とのやり取り
- 無線管理

WDS と WLSM に参加するアクセス ポイント間の関係を確立しなければ、他の WDS ベースの機能は動作しません。 WDS の 1 つの目的は、認証サーバでのユーザ クレデンシャルの検証を不要にして、クライアントの認証に要する時間を削減することです。

WDS を使用するためには、1 つのアクセス ポイントまたは WLSM を WDS として指定する必要があります。 WDS のアクセス ポイントは、WDS のユーザ名とパスワードを使用した認証を行って、認証サーバと関係を確立する必要があります。 認証サーバとしては、外部 RADIUS サーバまたは WDS アクセス ポイントのローカル RADIUS サーバ機能のどちらかを使用できます。 WLSM はサーバの認証は必要としませんが、認証サーバとの関係は確立しておく必要があります。

インフラストラクチャ アクセス ポイントと呼ばれる他のアクセス ポイントは WDS と通信します。 インフラストラクチャ アクセス ポイントは、登録の前に、自分自身の認証を WDS で完了しておく必要があります。 このインフラストラクチャの認証は、WDS のインフラストラクチャ サーバ グループによって定義されています。

クライアントの認証は、WDS の 1 つ以上のクライアント サーバ グループによって定義されています。

クライアントがインフラストラクチャ アクセス ポイントへの関連付けを試みると、インフラストラクチャ アクセス ポイントから WDS にユーザ クレデンシャルが渡されて検証されます。 そのクレデンシャルが WDS に初めて渡された場合は、WDS は認証サーバにクレデンシャルの検証を依頼します。 次に WDS はそのクレデンシャルをキャッシュに保存し、ユーザが再び認証を試み

たときには、認証サーバに依頼しなくてもよいようにします。 再認証の例には次のものがあります。

- 鍵の再作成
- ローミング
- ユーザがクライアント デバイスを起動した場合

RADIUS ベースの EAP 認証プロトコルは WDS を使用したトンネリングが可能です。

- Lightweight EAP（LEAP）
- Protected EAP（PEAP）
- EAP-Transport Layer Security（EAP-TLS）
- EAP-Flexible Authentication through Secure Tunneling（EAP-FAST）

MAC アドレスの認証も、外部認証サーバまたは WDS アドレス ポイントのローカル リストのどちらかにトンネリングできます。 WLSM は MAC アドレスの認証をサポートしていません。

WDS とインフラストラクチャ アクセス ポイントは、Wireless LAN Context Control Protocol（WLCCP）というマルチキャスト プロトコルで通信しています。 これらのマルチキャスト メッセージはルーティングできないので、WDS とそれに関連付けられたインフラストラクチャ アクセス ポイントは同じ IP サブネット内および同じ LAN セグメント内に存在する必要があります。 WDS と WLSE の間では、WLCCP が TCP と User Datagram Protocol（UDP）をポート 2887 で使用しています。 WDS と WLSE が異なるサブネットにあると、Network Address Translation（NAT; ネットワーク アドレス変換）などのプロトコルではパケットを変換できません。

WDS デバイスとして設定された AP は、最大 60 の参加アクセス ポイントをサポートしています。 WDS デバイスとして設定された統合サービス ルータ（ISR）は 100 台までの参加アクセス ポイントに対応しています。 さらに、WLSM 装備のスイッチは 600 台までの参加アクセス ポイントおよび 240 までのモビリティ グループに対応しています。 1 つのアクセス ポイントで 16 までのモビリティ グループに対応しています。

注: インフラストラクチャ アクセス ポイントが同じバージョンの IOS を WDS デバイスとして実行することを推奨します。 旧バージョンの IOS を使用する場合、アクセス ポイントが WDS デバイスの認証に失敗する場合があります。 さらに、最新バージョンの IOS を使用することを推奨します。 最新バージョンの IOS は、ワイヤレス製品のダウンロード ページ（登録ユーザ専用）にあります。

WDS デバイスの役割

WDS デバイスは、ワイヤレス LAN 上で次のようないくつかのタスクを実行します。

- WDS 機能をアドバタイズして、ご使用のワイヤレス LAN に最適な WDS デバイスを選びます。 WDS 用にワイヤレス LAN を設定するときに、1 台のデバイスをメイン WDS 候補に設定し、1 台以上の追加のデバイスをバックアップ WDS 候補に設定します。 メイン WDS デバイスがオフラインになると、バックアップ WDS デバイスのいずれかがその役割を引き継ぎます。
- サブネット内のすべてのアクセス ポイントを認証して、それぞれのアクセス ポイントとのセキュリティ保護された通信チャネルを確立します。
- サブネット内のアクセス ポイントから無線データを収集し、データを集約して、ネットワーク上の WLSE デバイスに転送します。
- 参加アクセス ポイントに関連するすべての 802.1x 認証済みクライアント デバイスのパスス

ルーの役割を果たします。
- 動的な鍵作成を使用するサブネット内のすべてのクライアント デバイスを登録して、それらのセッション鍵を確立して、セキュリティ クレデンシャルをキャッシュします。 クライアントが別のアクセス ポイントにローミングするときに、WDS デバイスはそのクライアントのセキュリティ クレデンシャルを新しいアクセス ポイントに転送します。

WDS デバイスを使用するアクセス ポイントの役割

ワイヤレス LAN 上のアクセス ポイントは、次の動作において WDS デバイスと連携します。

- 最新の WDS デバイスを検出して追跡し、WDS アドバタイズメントをワイヤレス LAN にリレーする。
- WDS デバイスを認証し、WDS デバイスに対して、セキュリティ保護された通信チャネルを確立する。
- 関連クライアント デバイスを WDS デバイスに登録する。
- 無線データを WDS デバイスにレポートする。

設定

WDS では、整理されたモジュラ形式で設定が表示されます。 各コンセプトは、それよりも前のコンセプトの上に構築されています。 中心となる内容を明確に示すために、パスワード、リモート アクセス、無線設定など、他の設定項目は WDS から除外されています。

このセクションでは、この文書で説明する機能を設定するために必要な情報を提供します。

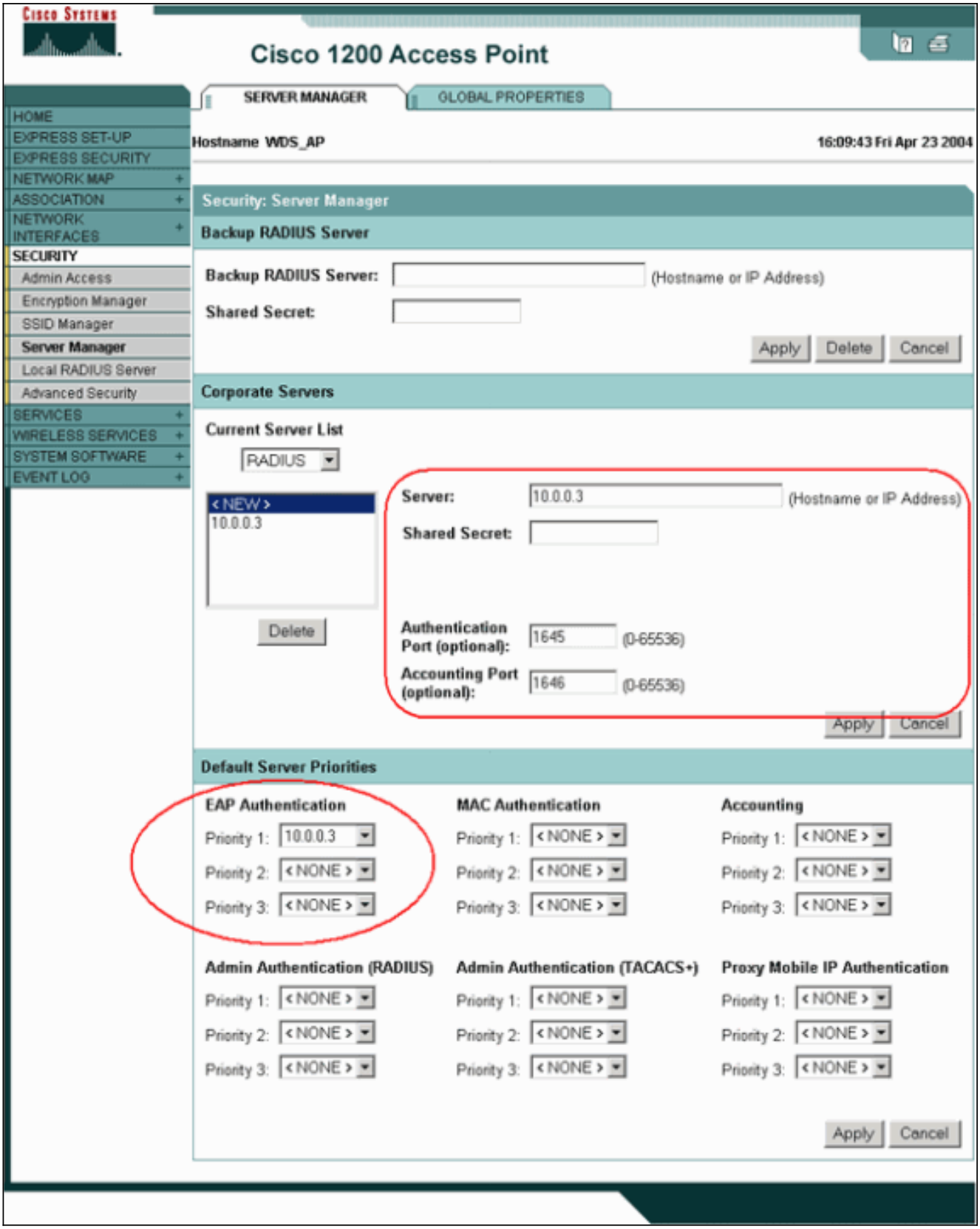
注: このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

アクセス ポイントを WDS として指定

まず最初にアクセス ポイントを WDS として指定します。 認証サーバとやり取りするのは WDS アクセス ポイントだけです。

アクセス ポイントを WDS として指定するために、次の手順を実行します。

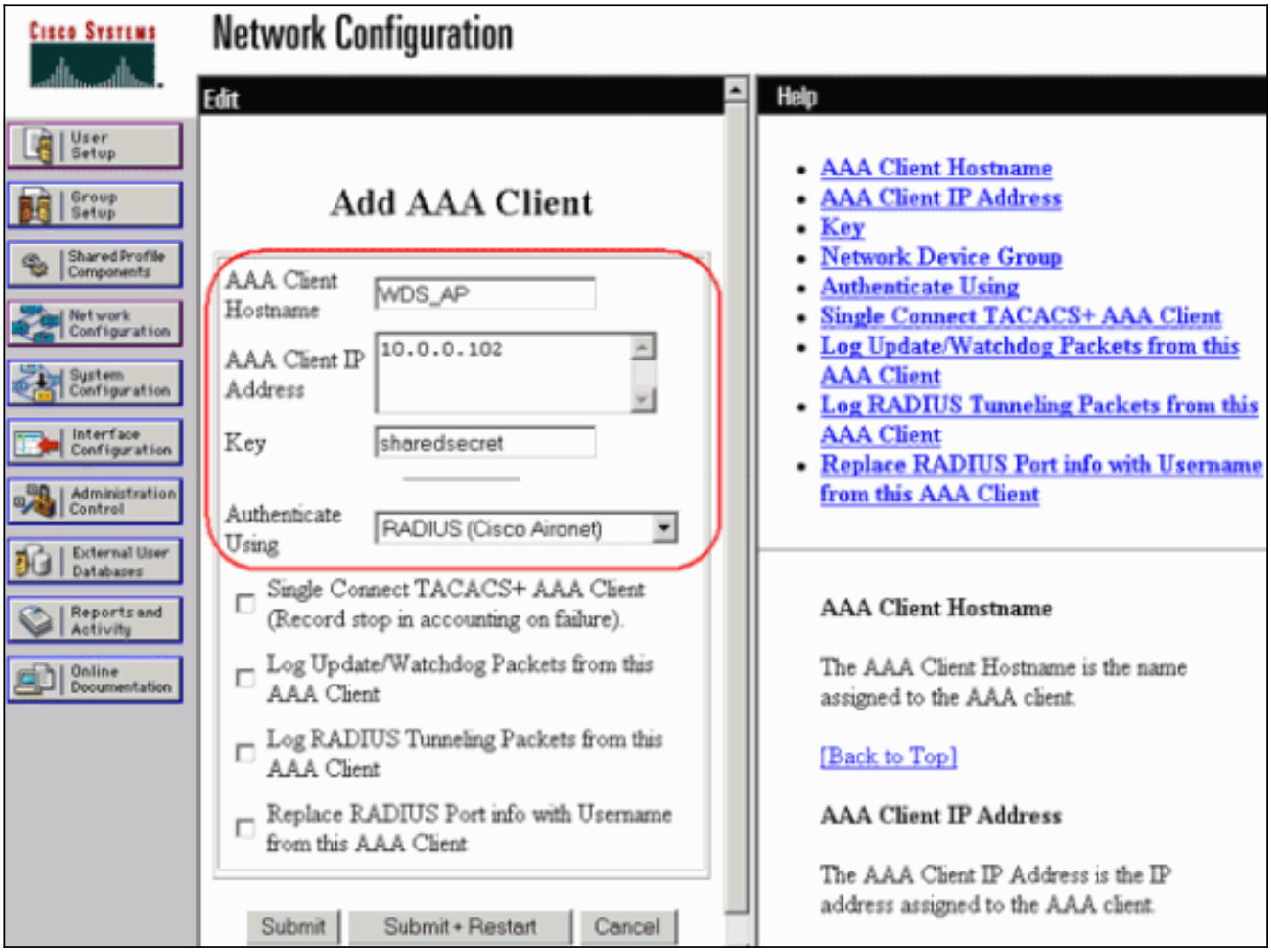
1. WDS アクセス ポイントで認証サーバを設定するには、[Security] > [Server Manager] の順に選択して、[Server Manager] タブに進みます。[Corporate Servers] の下で、[Server] フィールドに認証サーバの IP アドレスを入力します。共有秘密とポートを指定します。適切な認証タイプを使用して、[Default Server Priorities] の下で [Priority 1] フィールドをそのサーバ IP アドレスに設定します。



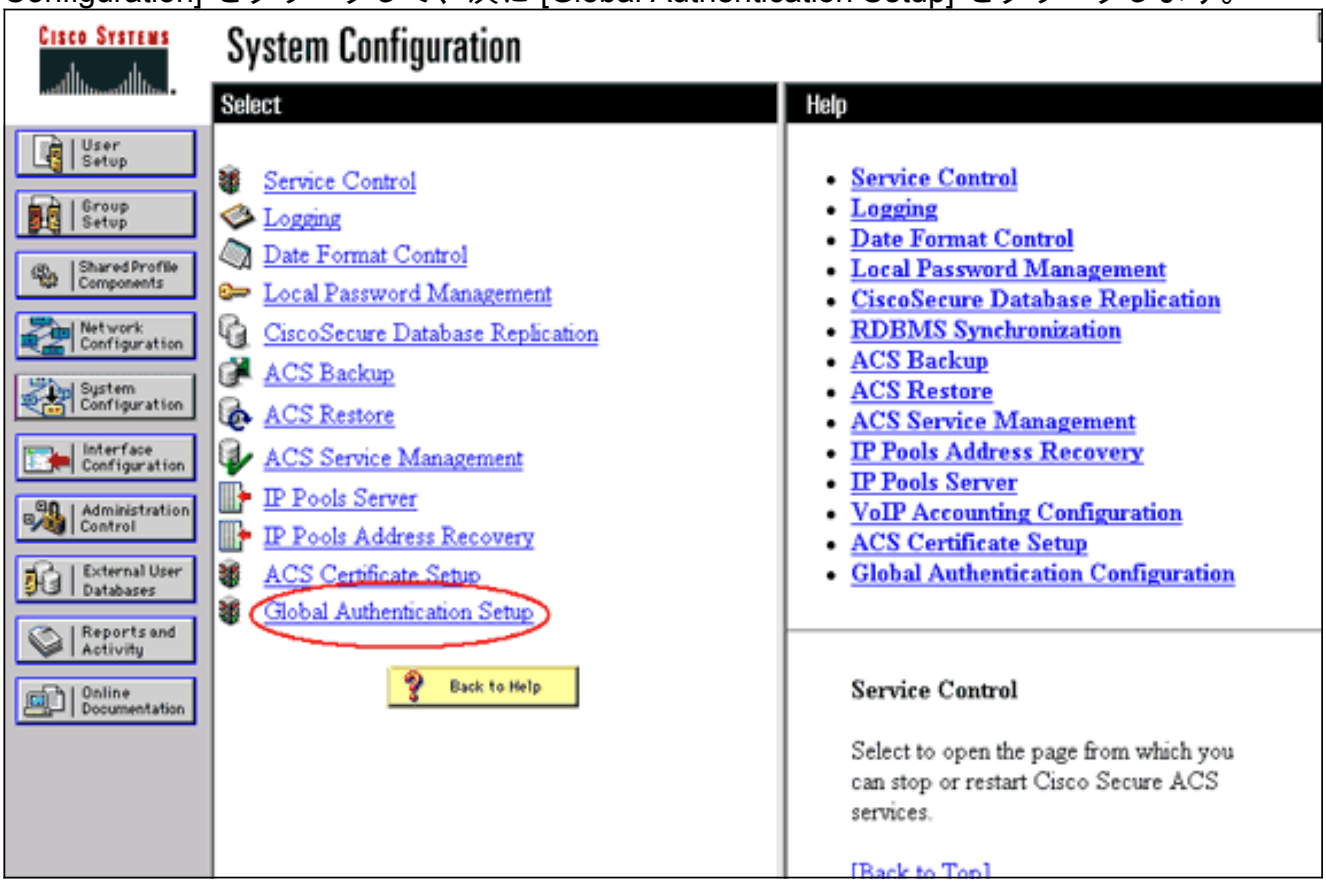
または、CLI で次のコマンドを実行します。

2. 次の手順は、WDS アクセス ポイントを認証サーバで認証、認定、およびアカウンティング（AAA）クライアントとして設定することです。 このためには、WDS アクセス ポイントを AAA クライアントとして追加する必要があります。 次の手順を実行します。**注:** このドキュメントでは、Cisco Secure ACS サーバを認証サーバとして使用します。Cisco Secure Access Control Server（ACS）では、この作業は [Network Configuration] ページで行います。WDS アクセス ポイント用に次の属性を定義します。名前IP アドレス共有秘密認証方式 RADIUS Cisco AironetRADIUS Internet Engineering Task Force（IETF）[Submit] をクリックします。ACS 以外の他の認証サーバについては、メーカーのマニュアルを参照してくだ

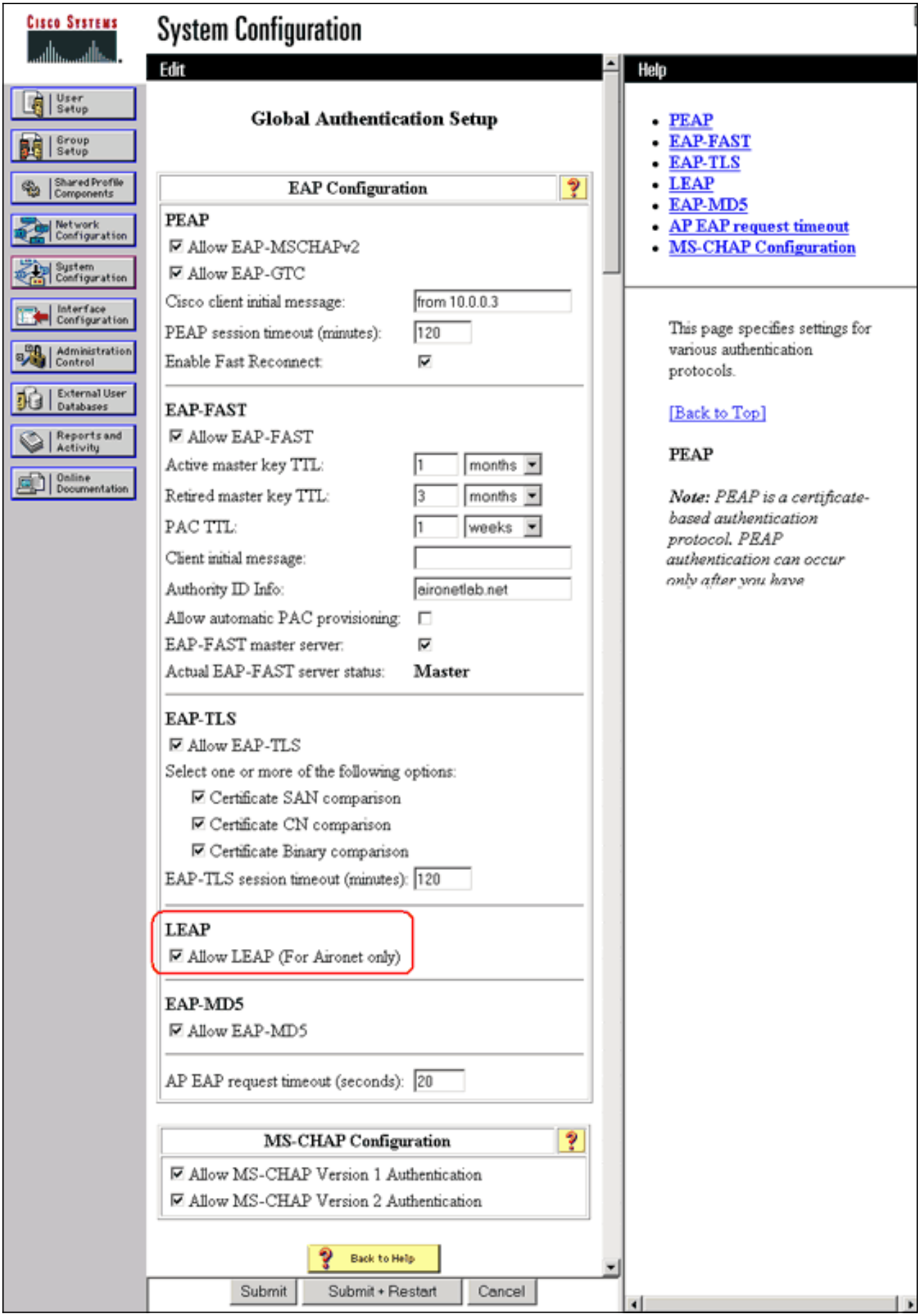
さい。



また、Cisco Secure ACS では、ACS が LEAP の認証を行うように、[System Configuration] - [Global Authentication Setup] ページで必ず設定してください。 まず、[System Configuration] をクリックして、次に [Global Authentication Setup] をクリックします。



次に、LEAP の設定までページを下にスクロールします。 ボックスにチェックマークを付けると、ACS で LEAP の認証が行われます。

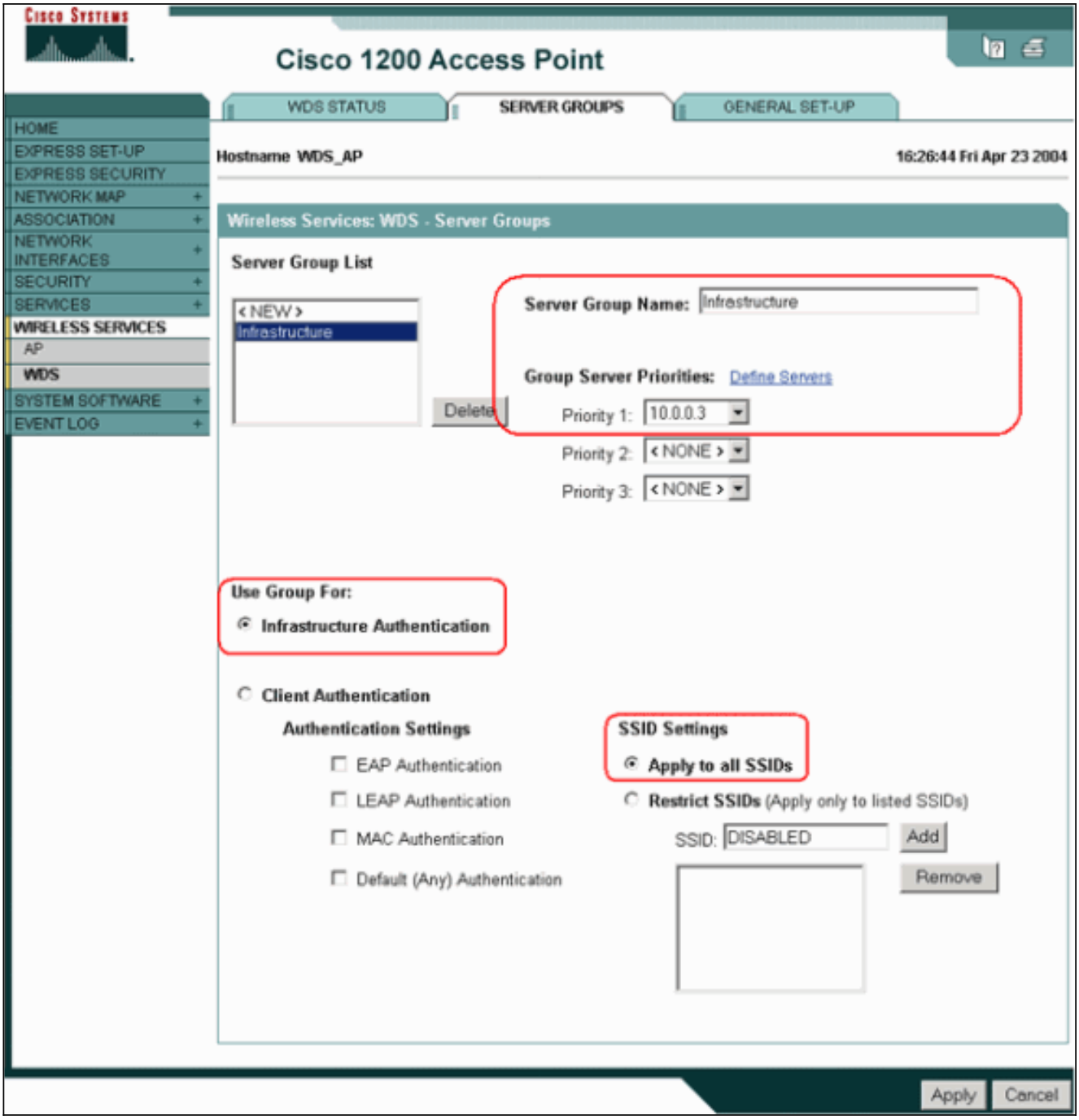


3. WDS アクセス ポイントで WDS 設定を行うには、WDS アクセス ポイントで [Wireless

Services] > [WDS] を選択し、[General Set-Up] タブをクリックします。 次の手順を実行します。[WDS - Wireless Domain Services - Global Properties] で、[Use this AP as Wireless Domain Services] をオンにします。これが最初の設定なので、[Wireless Domain Services Priority] の値を **254** 程度の値に設定します。 1 つ以上のアクセス ポイントまたはスイッチを WDS を提供する候補として設定できます。 最も優先度の高いデバイスが WDS を提供します。

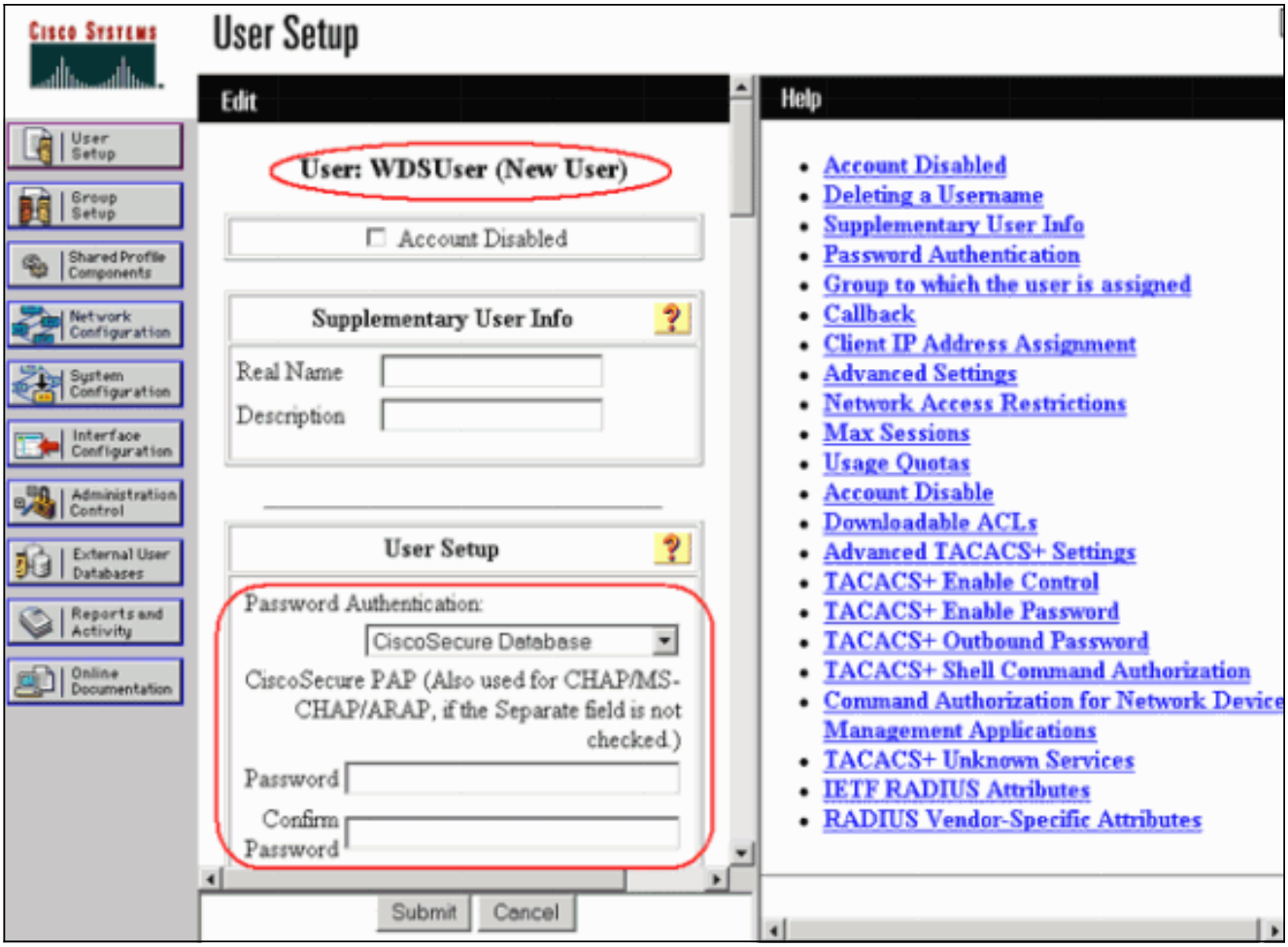
または、CLI で次のコマンドを実行します。

4. [Wireless Services] > [WDS] を選択し、[Server Groups] タブに進みます。他のアクセス ポイント、インフラストラクチャ グループを認証するサーバ グループ名を定義します。前に設定した認証サーバに [Priority 1] を設定します。[Use Group For: Infrastructure Authentication] ラジオ ボタンをクリックします。設定を関連 Service Set Identifier (SSID; サービスセット ID) に適用します。



または、CLI で次のコマンドを実行します。

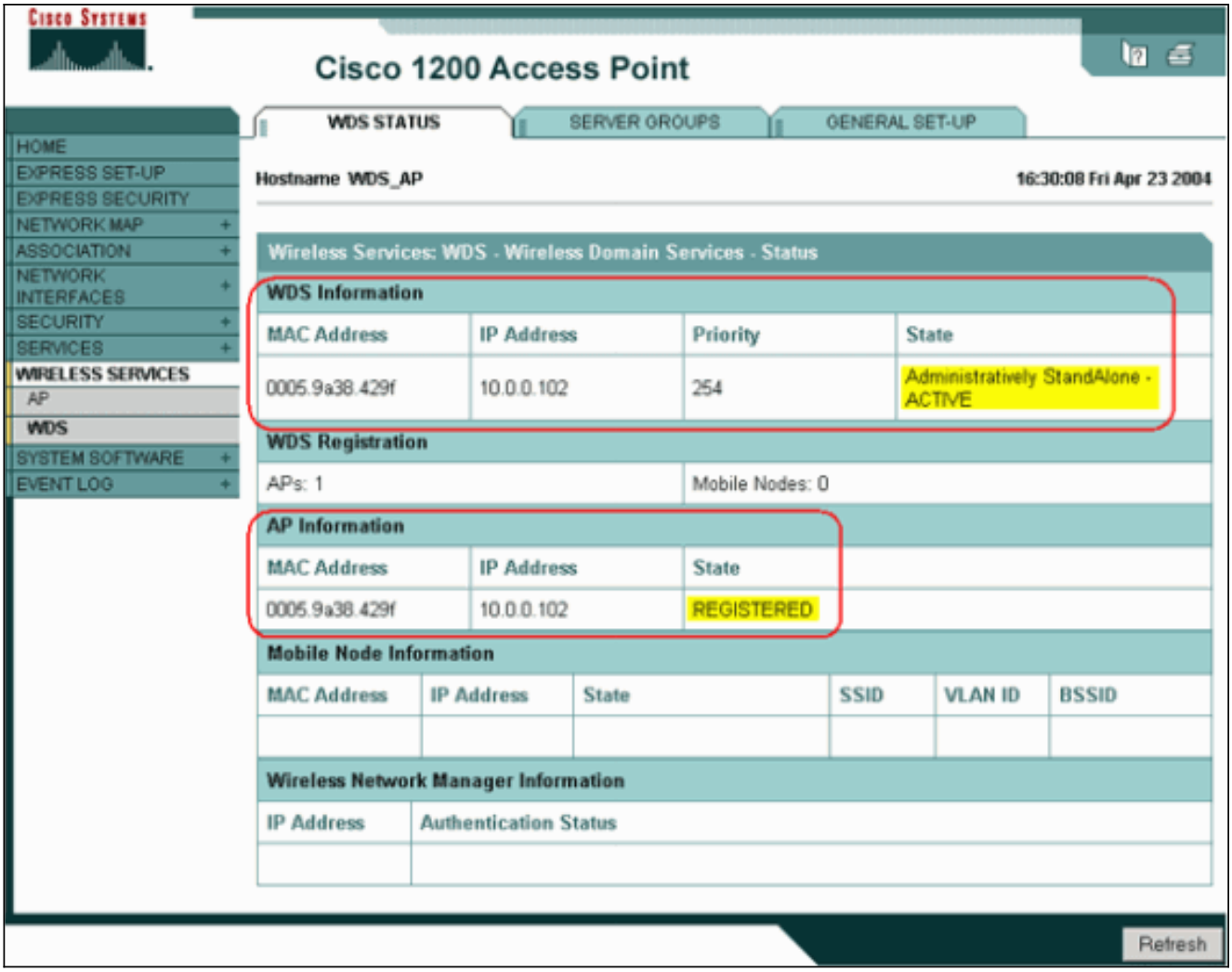
5. WDS のユーザ名とパスワードを自分の認証サーバのユーザとして設定します。Cisco Secure ACS の場合は、WDS のユーザ名とパスワードを定義する [User Setup] ページでこの作業を行います。 ACS 以外の他の認証サーバについては、メーカーのマニュアルを参照してください。**注:** WDS ユーザは多くの権限や特権が割り当てられているグループには入れないでください。WDS に必要なのは限られた権限だけです。



6. [Wireless Services] > [AP] の順に選択し、[Participate in SWAN infrastructure] オプションで [Enable] をクリックします。 次に WDS のユーザ名とパスワードを入力します。WDS のメンバに指定したすべてのデバイスについて、WDS のユーザ名とパスワードを認証サーバに指定しておく必要があります。

または、CLI で次のコマンドを実行します。

7. [Wireless Services] > [WDS] を選択します。 WDS アクセス ポイントの [WDS Status] タブで、WDS アクセス ポイントが [WDS Information] エリアにアクティブ状態と表示されているか確認します。 アクセス ポイントが [AP Information] エリアに [REGISTERED] と表示される必要があります。アクセス ポイントが [REGISTERED] または [ACTIVE] と表示されない場合は、認証サーバでエラーや認証の失敗がないか確認してください。アクセス ポイントが正しく登録されたら、WDS のサービスを使用するためにインフラストラクチャ アクセス ポイントを追加します。



または、CLI で次のコマンドを実行します。**注:** クライアント認証にはまだプロビジョニングされていないので、クライアントの関連付けはテストできません。

WLSM を WDS として指定

このセクションでは、WLSM を WDS として設定する方法を説明します。 認証サーバとやり取りするデバイスは WDS だけです。

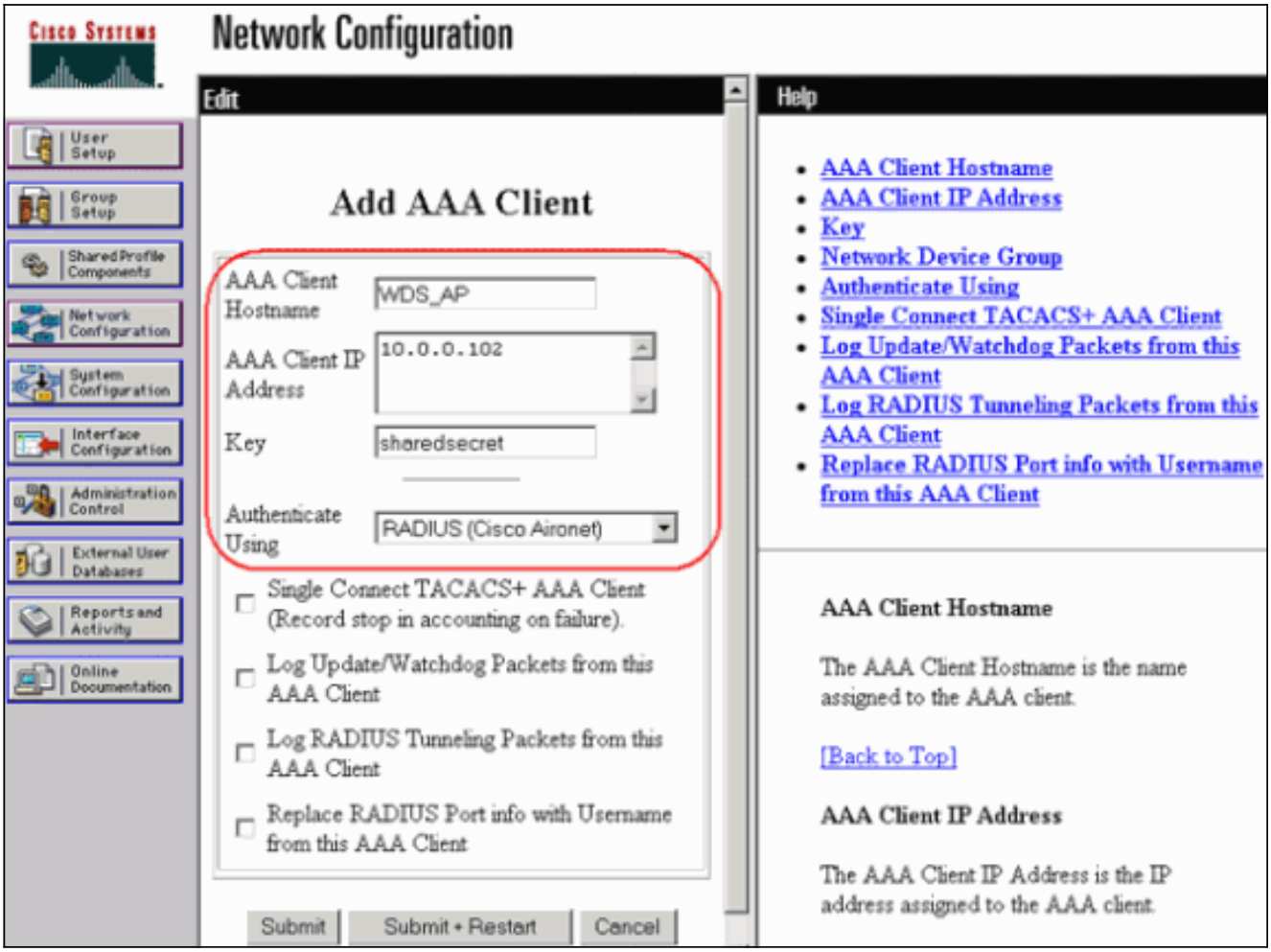
注: 次のコマンドは、Supervisor Engine 720 のコマンド プロンプトではなく、WLSM の enable コマンド プロンプトで実行してください。 WLSM のコマンド プロンプトを表示するには、Supervisor Engine 720 の enable コマンド プロンプトで次のコマンドを実行します。

```
c6506#session slot x proc 1
!--- In this command, x is the slot number where the
WLSM resides. The default escape character is Ctrl-^,
then x. You can also type 'exit' at the remote prompt to
end the session Trying 127.0.0.51 ... Open User Access
Verification Username: <username> Password: <password>
wlan>enable
Password: <enable password>
wlan#
```

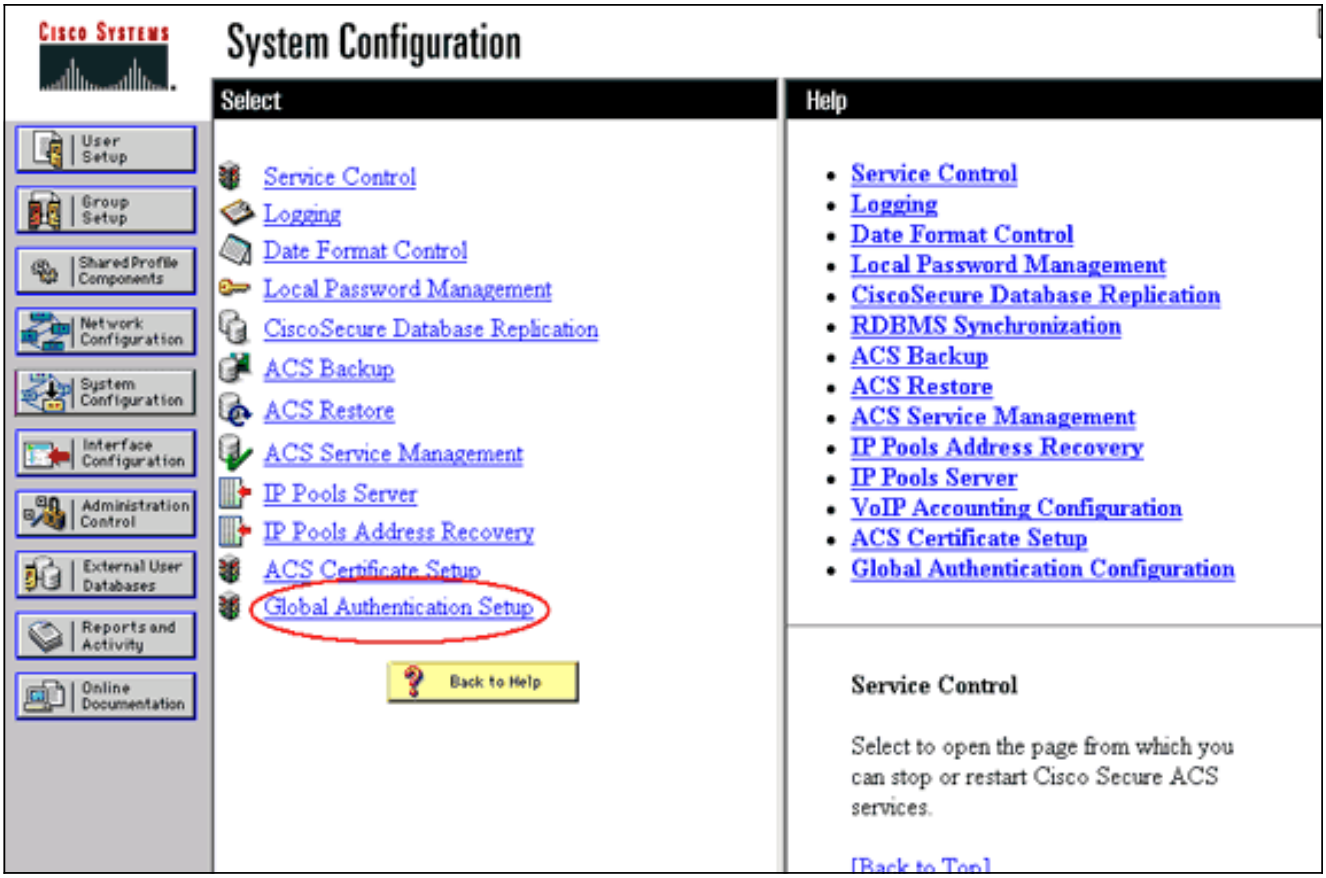
注: WLSM のトラブルシューティングとメンテナンスをさらに簡単にするために、Telnet によるリモート アクセスを WLSM に対して設定します。 『Telnet によるリモート アクセスの設定』を参照してください。

WLSM を WDS として指定するには次の操作を行います。

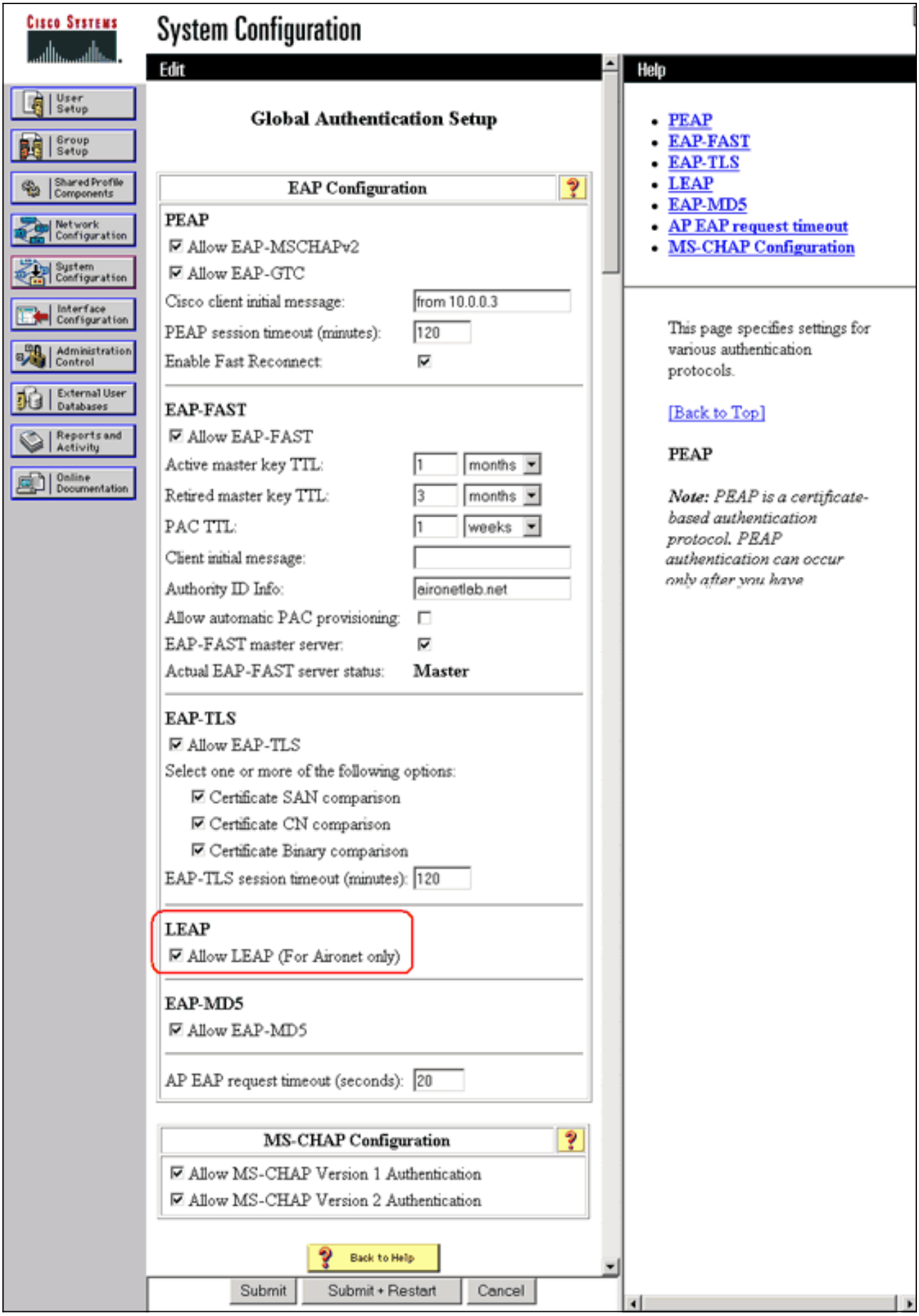
1. WLSM を WDS として指定するには、WLSM の CLI で次のコマンドを実行して、認証サーバとの関係を確立します。**注:** WLSM では優先順位を制御できません。 ネットワークに複数の WLSM モジュールがある場合、WLSM では冗長設定を使用してプライマリ モジュールが決定されます。
2. 認証サーバで WLSM を AAA クライアントとして設定します。ACS では、この作業は [Network Configuration] ページで行います。WLSM 用に次の属性を定義します。名前IP アドレス共有秘密認証方式RADIUS Cisco AironetRADIUS IETFACS 以外の他の認証サーバについては、メーカーのマニュアルを参照してください。



また、Cisco Secure ACS では、ACS が LEAP の認証を行うように、[System Configuration] - [Global Authentication Setup] ページで設定してください。 まず、[System Configuration] をクリックして、次に [Global Authentication Setup] をクリックします。



次に、LEAP の設定までページを下にスクロールします。 ボックスにチェックマークを付けると、ACS で LEAP の認証が行われます。



3. 他の AP（インフラストラクチャ サーバ グループ）を認証する方法を WLSM で定義します。
4. クライアント デバイス（クライアント サーバ グループ）を認証する方法およびそれらのク

ライアントがどの EAP タイプを使用するかを WLSM で定義します。**注:** このステップを実行すると、「クライアントの認証方式の定義」の手順を行う必要がなくなります。

5. Supervisor Engine 720 と WLSM の間に独自の VLAN を定義して、WLSM がアクセス ポイントや認証サーバなどの外部エンティティと通信できるようにします。 この VLAN はネットワークのどこでも、この目的以外に使用されることはありません。 まず Supervisor Engine 720 にこの VLAN を作成してから、次のコマンドを実行します。スーパーバイザ エンジン 720 の場合：WLSM の場合：
6. 次のコマンドを使用して WLSM の機能を確認します。WLSM の場合：スーパーバイザ エンジン 720 の場合：

アクセス ポイントをインフラストラクチャとして指定

この時点で、少なくとも 1 つのインフラストラクチャ アクセス ポイントを指定して、WDS に関連付ける必要があります。 クライアントはインフラストラクチャ AP に関連付けられます。 インフラストラクチャ アクセス ポイントは、WDS アクセス ポイントまたは WLSM にクライアントの認証を要求します。

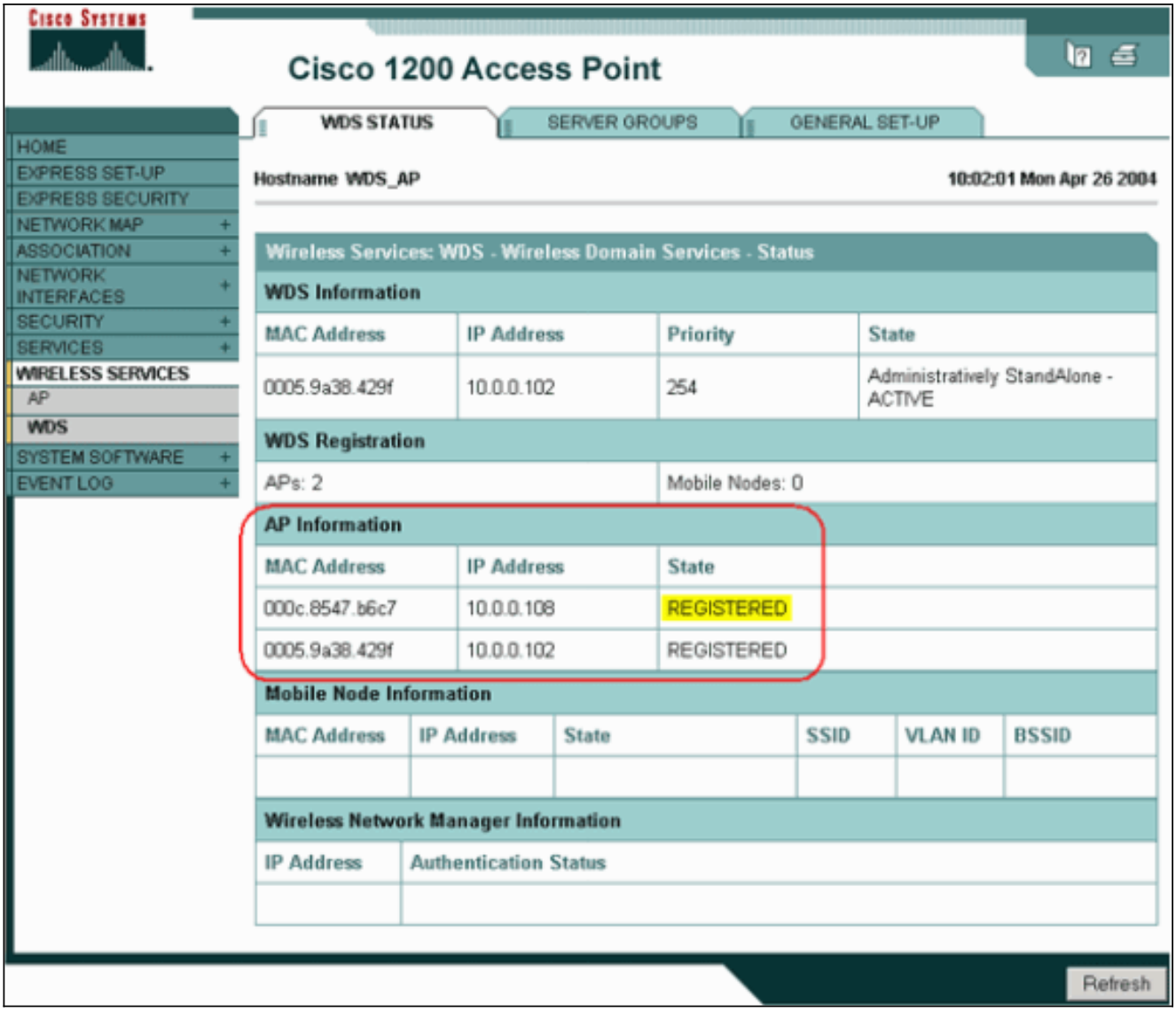
WDS のサービスを使用するインフラストラクチャ AP を追加するには、次の手順を実行します。

注: この設定はインフラストラクチャ アクセス ポイントにのみ該当し、WDS アクセス ポイントには該当しません。

1. [Wireless Services] > [AP] を選択します。 インフラストラクチャ アクセス ポイントで、[Wireless Services] オプションの [Enable] を選択します。 次に WDS のユーザ名とパスワードを入力します。WDS のメンバとなるすべてのデバイスについて、WDS のユーザ名とパスワードを認証サーバに指定しておく必要があります。

または、CLI で次のコマンドを実行します。

2. [Wireless Services] > [WDS] を選択します。 WDS アクセス ポイントの [WDS Status] タブで、新しいインフラストラクチャ アクセス ポイントの [WDS Information] エリアの [State] に [ACTIVE] が表示され、[AP Information] エリアの [State] に [REGISTERED] が表示されます。アクセス ポイントが [ACTIVE] または [REGISTERED] と表示されない場合は、認証サーバでエラーや認証の失敗がないか確認してください。アクセス ポイントが [ACTIVE] または [REGISTERED] と表示されたら、クライアント認証方式を WDS に追加します。



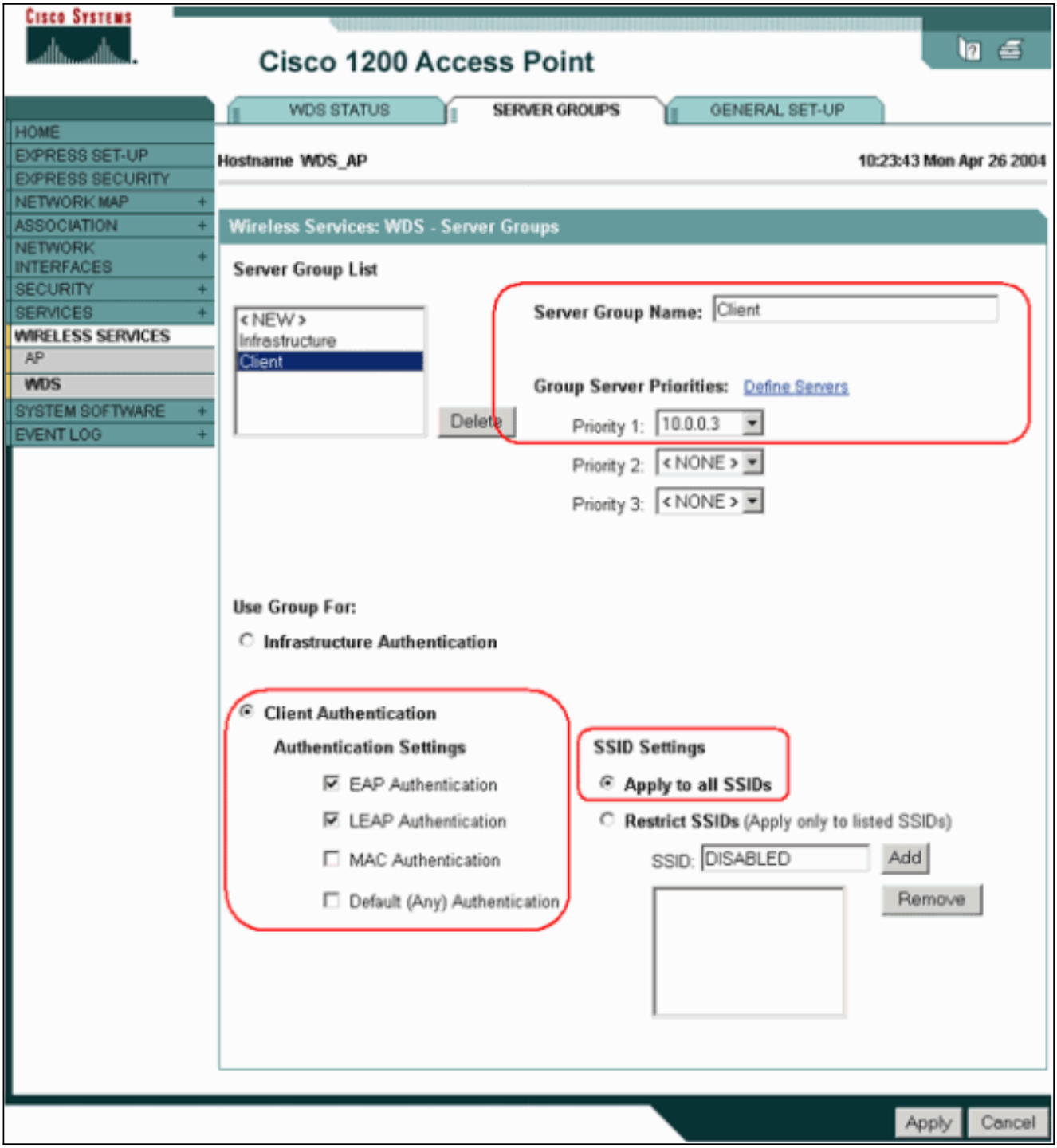
または、CLI で次のコマンドを実行します。または、WLSM で次のコマンドを実行します。次に、インフラストラクチャ アクセス ポイントで次のコマンドを実行します。**注:** クライアント認証にはまだプロビジョニングされていないので、クライアントの関連付けはテストできません。

クライアントの認証方式の定義

最後に、クライアントの認証方式を定義します。

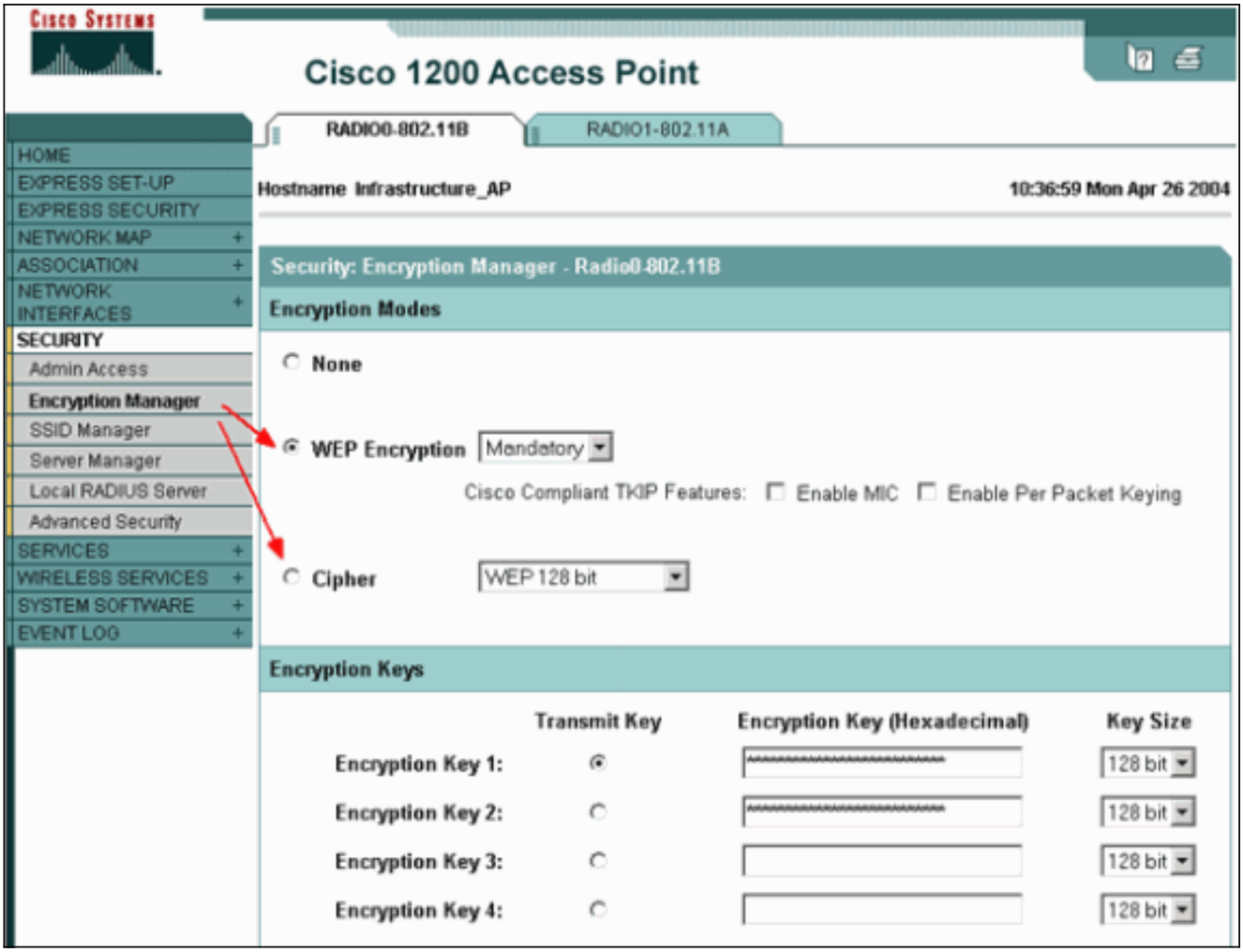
クライアントの認証方式を追加するには、次の手順を実行します。

1. [Wireless Services] > [WDS] を選択します。 WDS アクセス ポイントの [Server Groups] タブで次の手順を実行します。クライアント（クライアント グループ）の認証を行うサーバ グループを定義します。前に設定した認証サーバに [Priority 1] を設定します。該当する認証タイプ（LEAP、EAP、MAC など）を設定します。設定を関連する SSID に適用します。

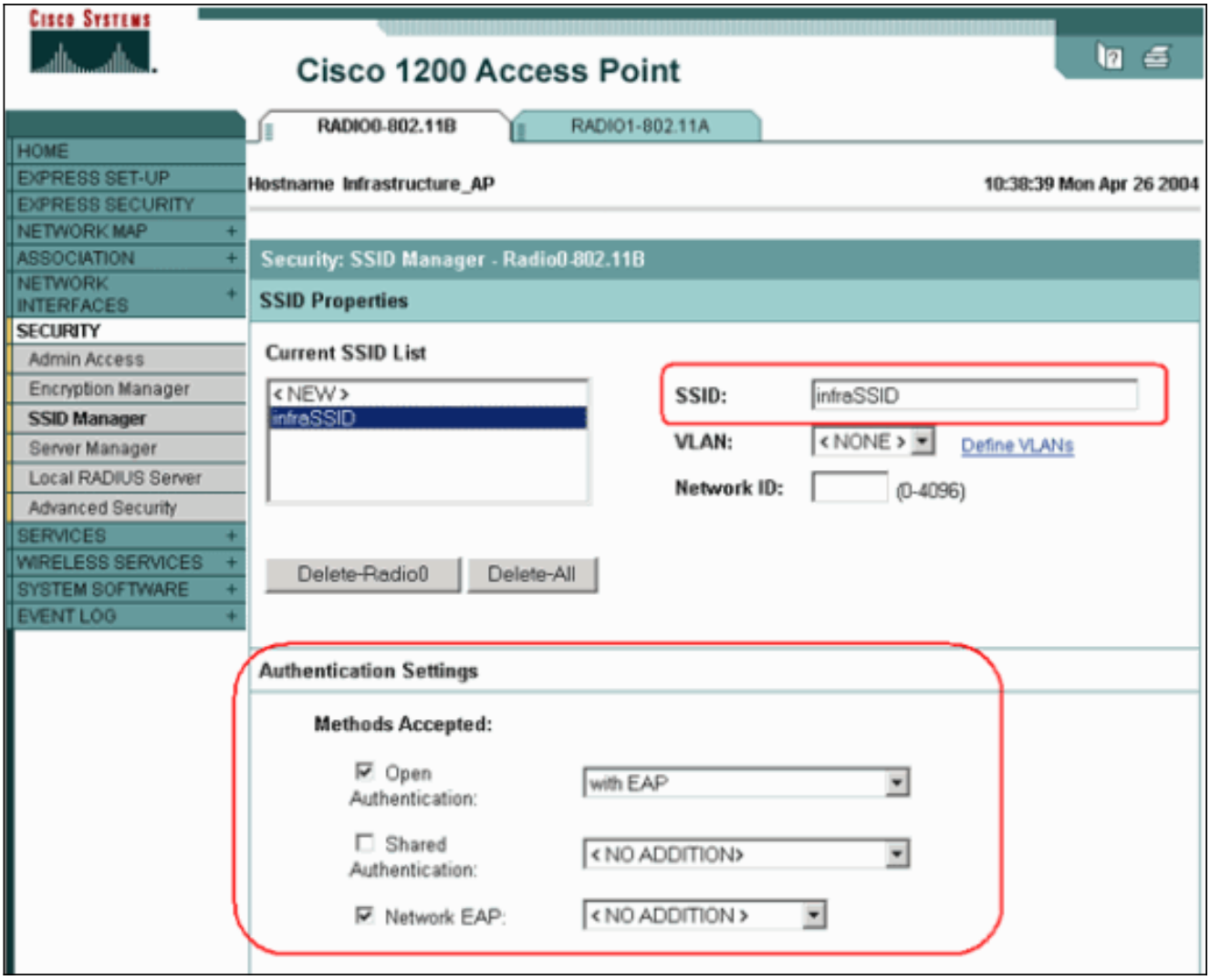


または、CLI で次のコマンドを実行します。**注:** この例では、WDS アクセス ポイントは専用で、クライアントの関連付けは受け付けません。**注:** インフラストラクチャ アクセス ポイントでは、サーバ グループ用には設定しないでください。 インフラストラクチャ アクセス ポイントはすべての要求の処理を WDS に転送するためです。

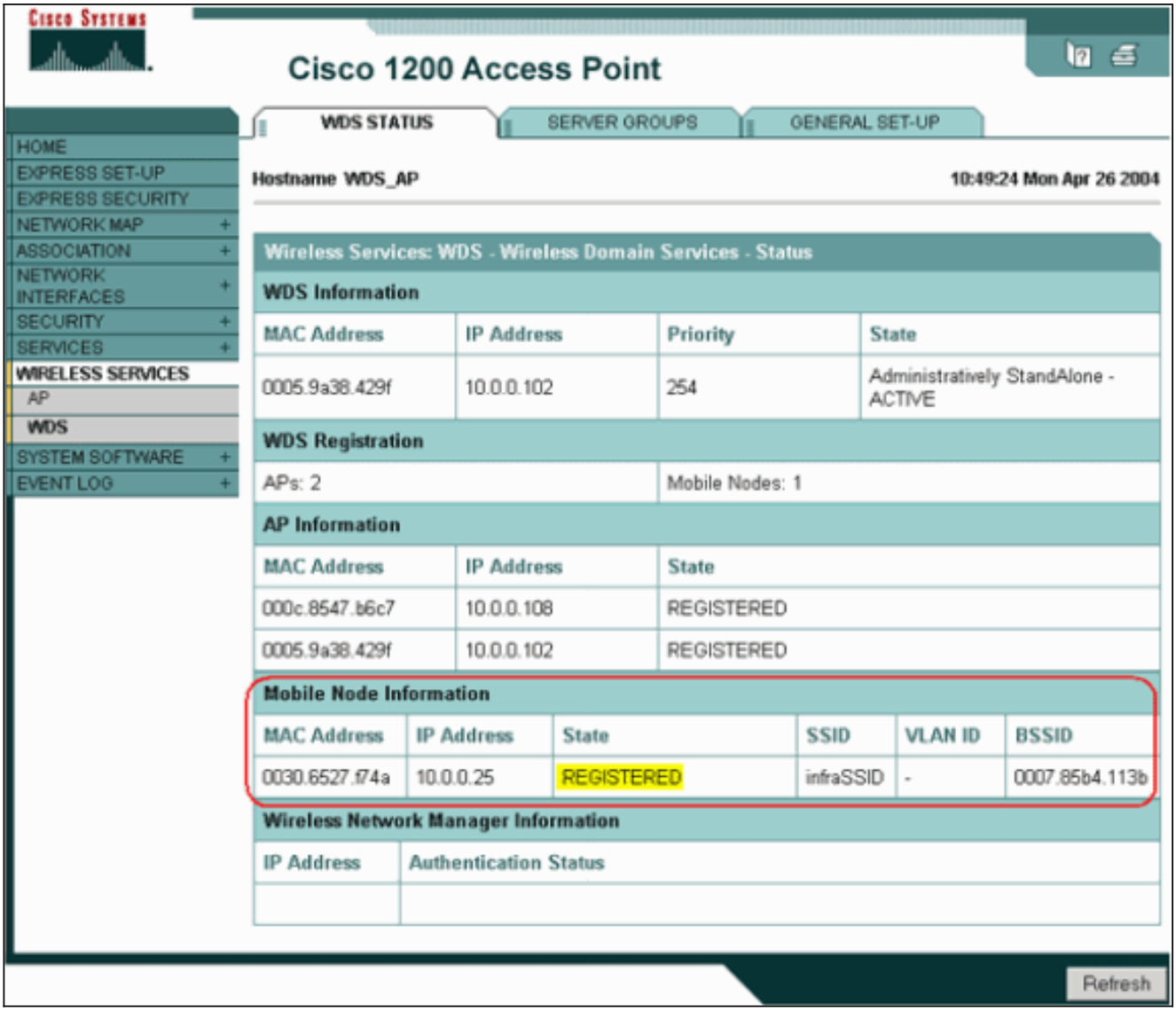
2. インフラストラクチャ アクセス ポイントまたはアクセス ポイントでは、次のようにします。[Security] > [Encryption Manager] メニューで、使用する認証プロトコルの要件に応じて、[WEP Encryption] または [Cipher] をクリックします。



[Security] > [SSID Manager] メニューで、使用する認証プロトコルの要件に応じて、認証方式を選択します。



3. この時点で、インフラストラクチャ アクセス ポイントでのクライアントの認証が正常にテストできるようになります。 [WDS Status] タブ（[Wireless Services] >> [WDS] の順で開いたメニュー項目内）の WDS の AP の [Mobile Node Information] エリアには、クライアントが [REGISTERED] 状態になっていることが表示されます。クライアントが表示されない場合は、認証サーバでエラーやクライアントによる認証の失敗がないか確認してください。



または、CLI で次のコマンドを実行します。**注:** 認証のデバッグが必要な場合は、WDS アクセス ポイントでデバッグを行ってください。認証サーバとやり取りをするのは WDS アクセス ポイントであるためです。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

このセクションでは、設定のトラブルシューティングに役立つ情報を紹介します。 以下では、WDS コマンドの使いやすさをさらに明らかにするために、WDS コマンドに関するよくある質問を示しています。

- **質問： WDS アクセス ポイントで、次の項目の推奨設定はどのようになりますか。**radius-server timeoutradius-server deadtimeTemporal Key Integrity Protocol (TKIP) Message Integrity Check (MIC) **障害ホールドオフ タイムクライアント ホールドオフ タイムEAP または MAC 再認証間隔EAP クライアントのタイムアウト (オプション) 回答：** これらの特別な設定に関してはデフォルト設定のままにし、タイミングに問題がある場合にのみ、これらの設定を使用することを推奨します。WDS アクセス ポイントの推奨設定は次のとおりです。

radius-server timeout を無効にします。 これは、アクセス ポイントが要求を再送信するまでに、RADIUS 要求に対する応答を待つ秒数です。 デフォルトは、5 秒です。**radius-server deadtime** を無効にします。 RADIUS は、すべてのサーバが障害とマークされない限り、追加の要求によってスキップされます。TKIP MIC 障害ホールドオフ タイムは、デフォルトで 60 秒で有効になっています。 ホールドオフ タイムを有効にしている場合、間隔を秒単位で入力できます。 アクセス ポイントが 60 秒以内に 2 つの MIC 障害を検出すると、そのインターフェイスのすべての TKIP クライアントをここで指定したホールドオフ タイムの間、ブロックします。クライアント ホールドオフ タイムは、デフォルトでは、無効にする必要があります。 ホールドオフを有効にした場合は、認証失敗後、次の認証要求が処理されるまで、アクセス ポイントが待機する秒数を入力します。EAP または MAC 再認証間隔は、デフォルトでは無効になっています。 再認証を有効にした場合、間隔を指定するか、認証サーバによって定められた間隔を受け入れることができます。 間隔を指定することを選択する場合、アクセス ポイントが認証されたクライアントに再認証を強制するまで待機する間隔を秒単位で入力します。EAP クライアント タイムアウト (オプション) はデフォルトでは、120 秒です。 アクセス ポイントで、ワイヤレス クライアントが EAP 認証要求に応答するまで待機する時間を入力します。

- **質問： TKIP ホールドオフ タイムについて、100 ms に設定すべきで、60 秒に設定すべきではないと書かれているのを読みました。 しかし、1 秒が選択できる最小の値なので、1 秒にしか設定できないと思うのですが。回答：** TKIP ホールドオフ タイムを増やすことが唯一の解決策になる障害が報告されていない限り、この時間を 100 ms に設定するという特定の推奨事項はありません。 1 秒が最小設定です。
- **質問： 次の 2 つのコマンドは何らかの方法でクライアント認証に役立ちますか。また、これらのコマンドは WDS またはインフラストラクチャ アクセス ポイントで必要ですか。**radius-server attribute 6 on-for-login-authradius-server attribute 6 support-multiple**回答：** これらのコマンドは、認証プロセスの役には立たず、WDS またはアクセス ポイントでは不要です。
- **質問： インフラストラクチャ アクセス ポイントで、アクセス ポイントは WDS から情報を受け取るため、サーバ マネージャやグローバル プロパティの設定は必要ないと思います。次の特定のコマンドのいずれかが、インフラストラクチャ アクセス ポイントに必要ですか。**radius-server attribute 6 on-for-login-authradius-server attribute 6 support-multipleradius-server timeoutradius-server deadtime**回答：** インフラストラクチャ アクセス ポイントには、サーバ マネージャやグローバル プロパティは不要です。 WDS がこれらのタスクを実行するため、次の設定を行う必要はありません。**radius-server attribute 6 on-for-login-authradius-server attribute 6 support-multipleradius-server timeoutradius-server deadtimeradius-server attribute 32 include-in-access-req format %h** 設定はデフォルトのまま残り、必要です。

アクセス ポイントは、レイヤ 2 デバイスです。 このため、アクセス ポイントが WDS デバイスの役割を果たすように設定されると、アクセス ポイントはレイヤ 3 モビリティに対応しません。WLSM を WDS デバイスとして設定する場合にのみ、レイヤ 3 モビリティを実現できます。 詳細については、「*レイヤ 3 モビリティ アーキテクチャ*」セクション (『Cisco Catalyst 6500 シリーズ ワイヤレス LAN サービス モジュール：ホワイト ペーパー』) を参照してください。

このため、アクセス ポイントを WDS デバイスとして設定する場合は、**mobility network-id** コマンドを使用しないでください。 このコマンドはレイヤ 3 モビリティに適用され、レイヤ 3 モビリティを正しく設定するには、WLSM を WDS デバイスとして設定する必要があります。 **mobility network-id** コマンドを誤って使用すると、次のいくつかの症状が現れます。

- ワイヤレス クライアントを AP と関連付けることができない。
- ワイヤレス クライアントをアクセス ポイントに関連付けることはできるが、DHCP サーバから IP アドレスを受け取らない。
- WLAN 上で音声を展開する場合に、無線電話が認証されない。

- EAP 認証が実行されない。 **mobility network-id** を設定すると、アクセス ポイントが Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）トンネルを構築して、EAP パケットを転送しようとします。 トンネルが確立されない場合、EAP パケットはどこにも転送されません。
- WDS デバイスとして設定されている AP は想定どおりに機能せず、WDS 設定も機能しない。**注:** Cisco Aironet 1300 AP/ブリッジを WDS マスターとして設定できません。 1300 AP/ブリッジはこの機能に対応していません。 1300 AP/ブリッジは、他のいくつかの AP または WLSM が WDS マスターとして設定されているインフラストラクチャ デバイスとして WDS ネットワークに参加します。

トラブルシューティングのためのコマンド

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

注: debug コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください。

- **全デバッグ dot11 AAA オーセンティケータは**クライアントがクライアント関連として行き、802.1X か EAP プロセスによって認証を受けることをさまざまなネゴシエーションに示します。 このデバッグは Cisco IOS ソフトウェア リリース 12.2(15)JA で導入されました。 上記以降のリリースでは、このコマンドが **debug dot11 aaa dot1x all** に代わるコマンドとして使用されています。
- **debug aaa authentication**：汎用 AAA パースペクティブからの認証プロセスを表示します。
- **debug wlccp ap**：AP が WDS に加入するときに関わる WLCCP ネゴシエーションを表示します。
- **debug wlccp packet**：WLCCP ネゴシエーションに関する詳細情報を表示します。
- **debug wlccp leap-client**：インフラストラクチャ デバイスが WDS に加入するときに詳細を表示します。

関連情報

- **WDS、高速セキュアローミング、および無線管理の設定**
- **Catalyst 6500 シリーズ ワイヤレス LAN サービス モジュール コンフィギュレーション ガイド**
- **暗号スイートと WEP の設定**
- **認証タイプの設定（英語）**
- **ワイヤレス LAN 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**