CHAPTER 11

WDS、高速で安全なローミング、および無線管理の設定

この章では、Wireless Domain Services（WDS）、クライアント デバイスの高速で安全なローミング、および無線管理のために、アクセス ポイントを設定する方法を説明します。この章の内容は、次のとおりです。

WDS の概要

次の項では、ブリッジがアクセス ポイントとして設定されている場合であっても WDS サーバとして設定できない場合の WDS について説明します。ただし、アクセス ポイントとして設定されている場合、ブリッジは WDS サーバを使用でき、WDS 認証サーバ（クライアント）として動作できます。

WDS を提供するようにアクセス ポイントを設定した場合、無線 LAN 上のその他のアクセス ポイント（アクセス ポイントとして設定されている場合のブリッジなど）は、WDS アクセス ポイントを使用してクライアント デバイスに高速で安全なローミングを提供し、無線管理に参加します。

高速で安全なローミングによって、クライアント デバイスが 1 つのアクセス ポイントから別のアクセス ポイントにローミングする際に迅速な再認証が行われます。これによって音声などの時間に敏感なアプリケーションにおける遅延を防ぐことができます。

無線管理に参加するアクセス ポイントは、無線環境の情報（潜在的な不正アクセス ポイントやクライアントのアソシエーションおよびアソシエーション解除など）を WDS アクセス ポイントに転送します。WDS アクセス ポイントは情報を集約し、これをネットワーク上の Wireless LAN Solution Engine（WLSE）デバイスに転送します。

WDS アクセス ポイントの役割

WDS アクセス ポイントは無線 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、無線 LAN に最適な WDS アクセス ポイントの選択に参加します。WDS 用に無線 LAN を設定する場合、メインの WDS アクセス ポイントの候補として 1 つアクセス ポイントを設定し、バックアップ WDS アクセス ポイント候補として 1 つ以上のアクセス ポイントを設定します。
- サブネット中の全アクセス ポイントを認証して、そのうちのそれぞれと安全な通信チャネルを設定します。
- サブネットのアクセス ポイントから無線データを収集して集約した後、これをネットワーク上の WLSE デバイスに転送します。
- サブネット中の全クライアント デバイスを登録して、それにセッション キーを設定し、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場合、WDS アクセス ポイントは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 アクセス ポイントを使用したアクセス ポイントの役割

無線 LAN 上のアクセス ポイントは、次の動作において WDS アクセス ポイントと対話します。

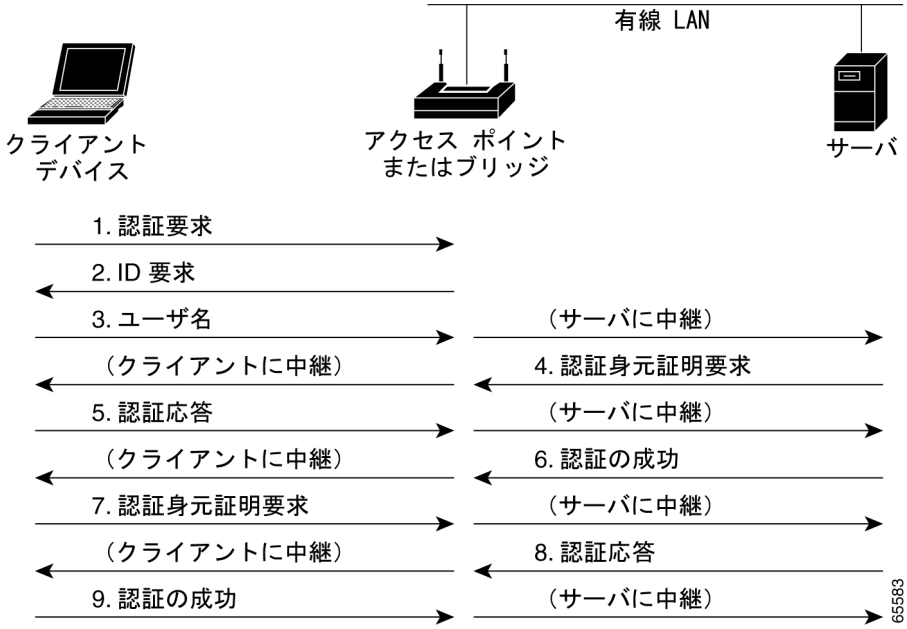
- 現在の WDS アクセス ポイントを検出、トラッキングし、WDS アドバタイズメントを無線 LAN に中継します。
- WDS アクセス ポイントを認証して、WDS アクセス ポイントと安全な通信チャネルを設定します。
- WDS アクセス ポイントとアソシエートしたクライアント デバイスを登録します。
- 無線データを WDS アクセス ポイントに報告します。

高速で安全なローミングの概要

多くの無線 LAN 内のアクセス ポイントは、システム全体においてアクセス ポイントからアクセス ポイントへローミングするモバイル クライアント デバイスに対応します。クライアント デバイスで稼働するアプリケーションの中には、異なるアクセス ポイントにローミングする場合、高速な再アソシエーションを必要とするものがあります。たとえば、音声アプリケーションでは、会話の遅延やギャップを防ぐために、シームレスなローミングが必要です。

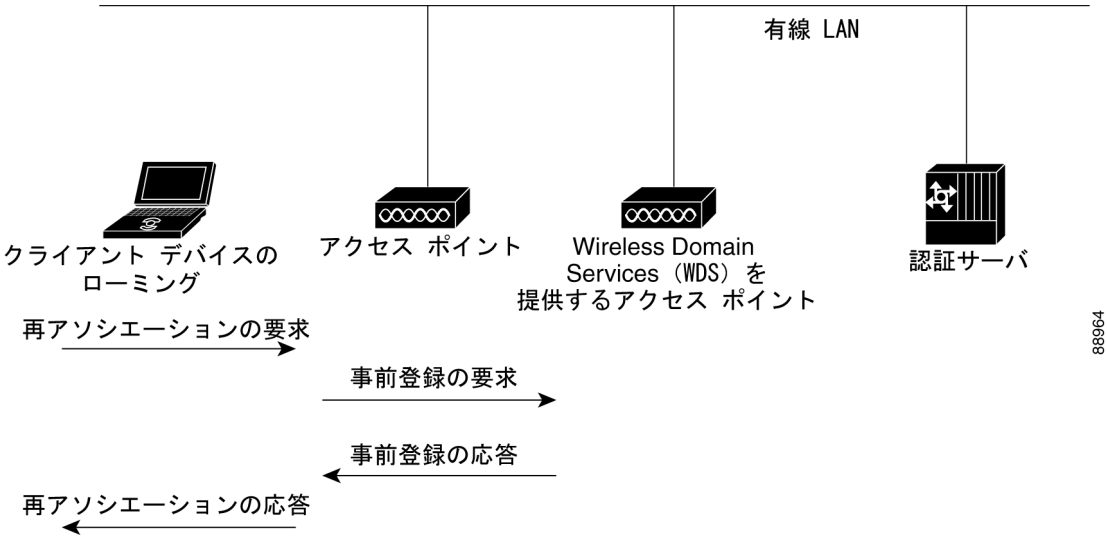
正常稼働時は、LEAP 使用可能クライアント デバイスは、図 11-1 に示すように、完全な LEAP 認証を実行することによって、メイン RADIUS サーバとの会話を含めて、新しいアクセス ポイントを相互に認証します。

図 11-1　RADIUS サーバを使ったクライアント認証



しかし、無線 LAN に高速で安全なローミングの設定を行えば、LEAP 使用可能クライアント デバイスは、メイン サーバを利用することなく、あるアクセス ポイントから別のアクセス ポイントへのローミングを行います。Cisco Centralized Key Management（CCKM）を使用すると、Wireless Domain Services（WDS）を提供するように設定されているアクセス ポイントは、RADIUS サーバの代わりにクライアントを非常に速く認証するので、音声や他の時間に敏感なアプリケーションにほとんど遅延が発生することはありません。図 11-2 は、CCKM を使用するクライアント認証を示しています。

図 11-2　CCKM と WDS アクセス ポイントを使用するクライアント再アソシエーション



WDS アクセス ポイントは、無線 LAN 上の CCKM 利用可能クライアント デバイスに対するクレデンシャルのキャッシュを維持します。CCKM 利用可能クライアントは、1 つのアクセス ポイントから別のアクセス ポイントへローミングする場合、クライアントが新しいアクセス ポイントへ再アソシエーションの要求を送信し、新しいアクセス ポイントはその要求を WDS アクセス ポイントへ中継します。WDS アクセス ポイントはクライアントのクレデンシャルを新しいアクセス ポイントへ転送し、新しいアクセス ポイントは再アソシエーション応答をクライアントに送信します。クライアントと新しいアクセス ポイントとの間で渡されるパケットは 2 つだけなので、再アソシエーションの時間が大幅に短縮されます。クライアントは再アソシエーション応答をユニキャスト キーの生成にも使用します。

無線管理の概要

無線管理に参加しているアクセス ポイントは、無線環境をスキャンして、潜在的な不正アクセス ポイント、アソシエートされているクライアント、クライアントの信号強度、他のアクセス ポイントからの無線信号などの無線情報の報告を WDS アクセス ポイントに送信します。WDS アクセス ポイントは、ネットワーク上の WLSE デバイスに、集約した無線データを転送します。また、無線管理に参加しているアクセス ポイントは自己修復無線 LAN を補助します。このようなアクセス ポイントは、近くのアクセス ポイントに障害が発生した場合に、そのカバレッジを補うよう自動的に設定を調整します。無線管理を設定する方法の詳細は、「デバッグ メッセージの使用」の項（P.11-12）を参照してください。

WDS と高速で安全なローミングの設定

この項では、WDS と高速で安全なローミングを無線 LAN 上に設定する方法を説明します。この項の内容は、次のとおりです。

WDS のガイドライン

次の WDS ガイドラインに注意する必要があります。

- ブリッジを WDS アクセス ポイントとして設定することはできません。ただし、ブリッジをアクセス ポイントとして設定する場合は、ブリッジが WDS アクセス ポイントを使用するように設定することもできます。
- リピータ アクセス ポイントは WDS をサポートしません。

WDS と高速で安全なローミングの要件

ブリッジが常駐する無線 LAN は、次の要件を満たす必要があります。

- WDS アクセス ポイントとして設定できる 1 つ以上のアクセス ポイント
- 認証サーバ（またはローカル認証サーバとして設定されているアクセス ポイント）
- Cisco クライアント ファームウェア バージョン 5.20.17 以降を実行する Cisco Aironet クライアント デバイス

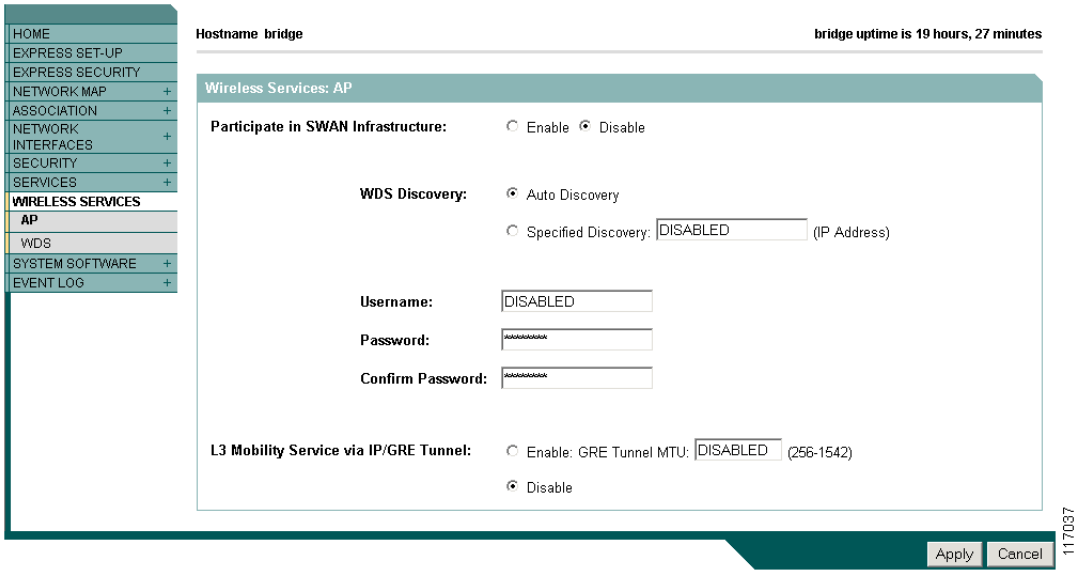
ブリッジを WDS アクセス ポイントを使用するように設定する

ブリッジが WDS を使用するように設定するには、まずブリッジをアクセス ポイントとして設定する必要があります。WDS アクセス ポイントを通じて認証し、CCKM に参加するようにブリッジを設定するには、次の手順に従います。

ステップ 1　Wireless Services Summary ページを表示します。

ステップ 2　**AP** をクリックして、Wireless Services AP ページを表示します。図 11-3 は、Wireless Services AP ページを示しています。

図 11-3　Wireless Services AP ページ



ステップ 3　Participate in SWAN Infrastructure フィールドの **Enabled** をクリックします。

ステップ 4　WDS Discovery フィールドの次のオプションのいずれかを選択します。

a. Auto Discovery：ブリッジは、WDS アクセス ポイントを自動的に検索します。

b. Specified Discovery：ブリッジは、入力された IP アドレスに基づいて WDS アクセス ポイントを検出します。

ステップ 5　Username フィールドにブリッジのユーザ名を入力します。このユーザ名は、認証サーバ上でブリッジ用に作成したユーザ名と一致する必要があります。

ステップ 6　Password フィールドにブリッジのパスワードを入力し、Confirm Password フィールドに同じパスワードをもう一度入力します。このパスワードは、認証サーバ上でブリッジ用に作成したパスワードと一致する必要があります。

ステップ 7　L3 Mobility Service via IP/GRE Tunnel フィールドに GRE Tunnel MTU の値を入力します。

ステップ 8　**Apply** をクリックします。

設定が完了すると、ブリッジは WDS と対話し、自動的に次の手順を実行します。

- 現在の WDS アクセス ポイントを検出、トラッキングし、WDS アドバタイズメントを無線 LAN に中継します。
- WDS アクセス ポイントを認証して、WDS アクセス ポイントに対する安全な通信チャネルを確立します。
- WDS アクセス ポイントとアソシエートしたクライアント デバイスを登録します。

CLI の設定例

次に、「ブリッジを WDS アクセス ポイントを使用するように設定する」の項（P.11-5）に記載された手順と同じ働きをする CLI コマンドの例を示します。

```
AP# configure terminal
AP(config)# wlccp ap username APWestWing password 7 wes7win8
AP(config)# end
```

この例では、ブリッジは WDS アクセス ポイントと対話できるように設定されており、ユーザ名に *APWestWing*、パスワードに *wes7win8* を使用して認証サーバに対する認証を行います。認証サーバ上でクライアントとしてアクセス ポイントを設定するときには、同じユーザ名とパスワードの組み合わせで設定する必要があります。

この例で使用されているコマンドの詳細は、『Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges』を参照してください。

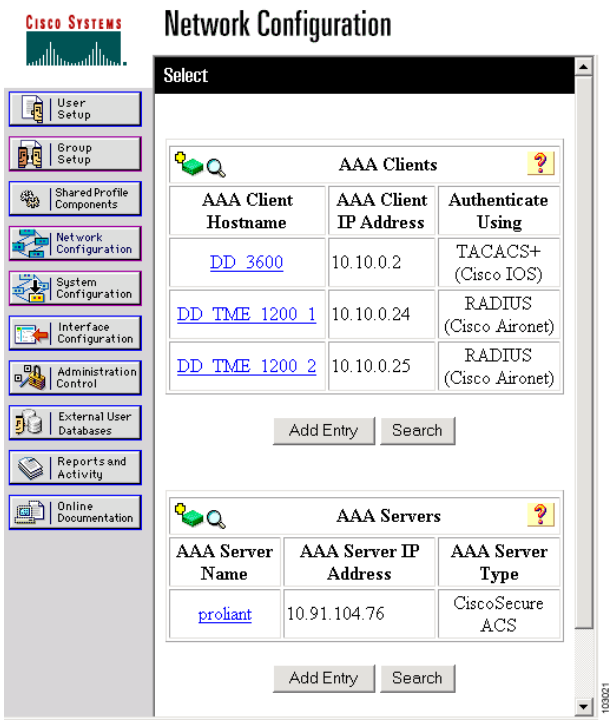
認証サーバが高速で安全なローミングをサポートするように設定する

WDS アクセス ポイントと CCKM に参加している全アクセス ポイントは、認証サーバに対する認証を行う必要があります。サーバ上で、アクセス ポイント用のユーザ名とパスワードと、WDS アクセス ポイント用のユーザ名とパスワードを設定します。

サーバが Cisco ACS を実行している場合は、次の手順に従ってサーバ上でアクセス ポイントを設定します。

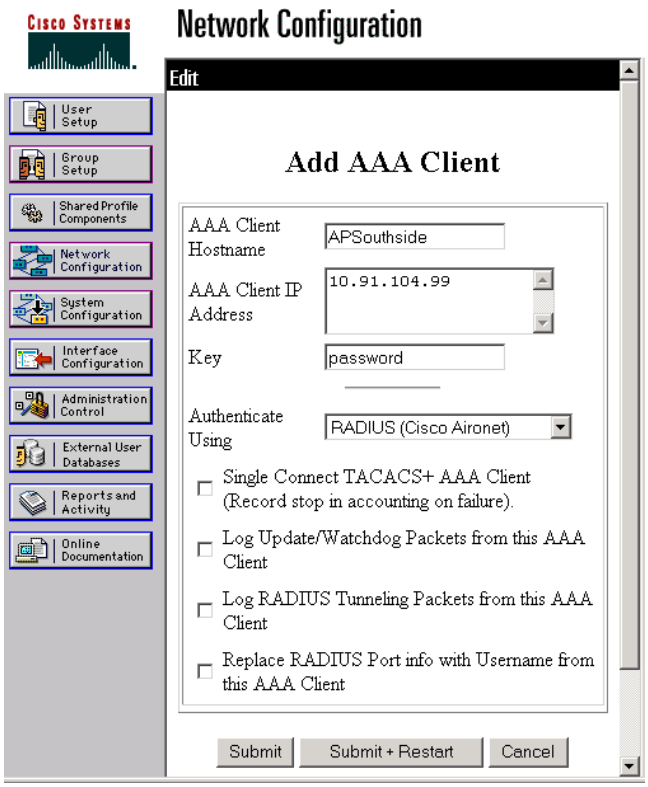
ステップ 1　Cisco Secure ACS にログインし、**Network Configuration** をクリックして Network Configuration ページを表示します。WDS アクセス ポイント用のエントリを作成するには、Network Configuration ページを使用する必要があります。図 11-4 は、Network Configuration ページを示しています。

図 11-4　Network Configuration ページ



ステップ 2　AAA Clients テーブルで、**Add Entry** をクリックします。Add AAA Client ページが表示されます。図 11-5 は、Add AAA Client ページを示しています。

図 11-5　Add AAA Client ページ



ステップ 3　AAA Client Hostname フィールドに、WDS アクセス ポイントの名前を入力します。

ステップ 4　AAA Client IP Address フィールドに、WDS アクセス ポイントの IP アドレスを入力します。

ステップ 5　Key field フィールドに、WDS アクセス ポイントで設定したのとまったく同じパスワードを入力します。

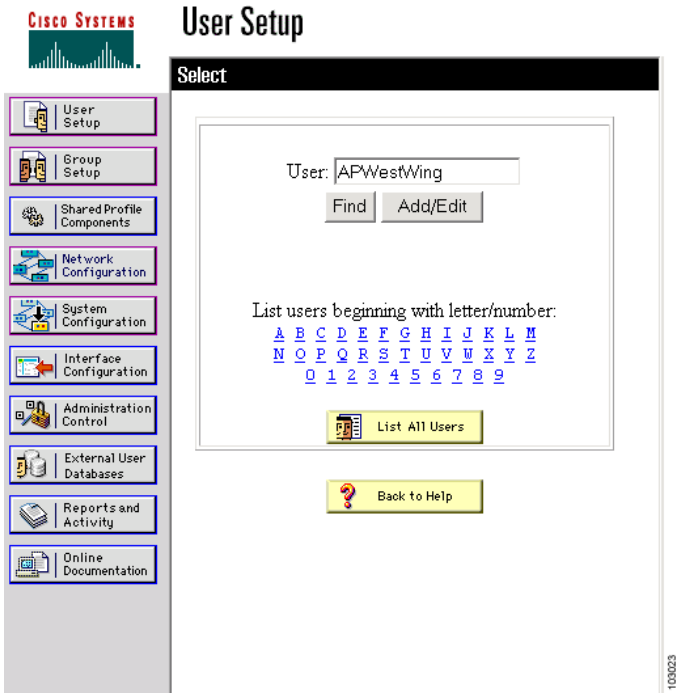
ステップ 6　Authenticate Using ドロップダウン メニューから、**RADIUS (Cisco Aironet)** を選択します。

ステップ 7　**Submit** をクリックします。

ステップ 8　WDS アクセス ポイント候補それぞれに対して、ステップ 2 から ステップ 7 の手順を繰り返します。

ステップ 9　**User Setup** をクリックして User Setup ページを表示します。WDS アクセス ポイントを使用するアクセス ポイント用のエントリを作成するには、User Setup ページを使用する必要があります。図 11-6 は、User Setup ページを示しています。

図 11-6　User Setup ページ

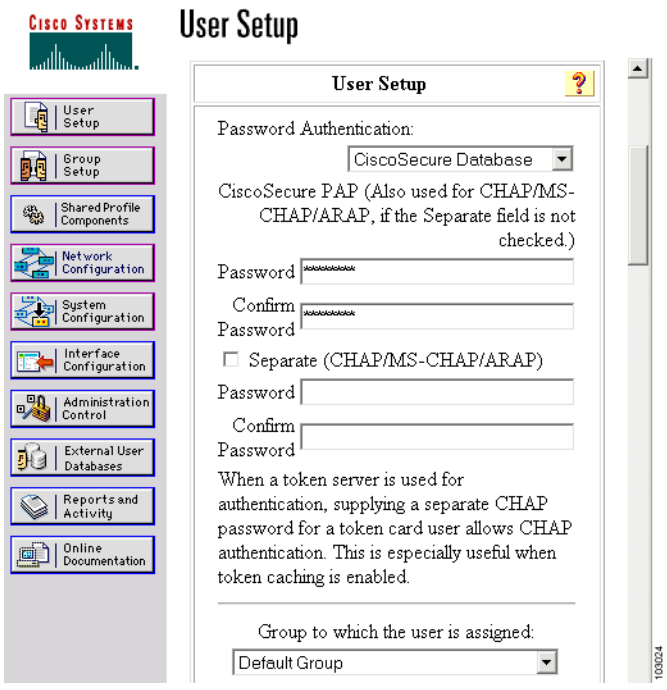


ステップ 10　User フィールドに、アクセス ポイントの名前を入力します。

ステップ 11　**Add/Edit** をクリックします。

ステップ 12　User Setup ボックスが表示されるまで、画面を下にスクロールします。図 11-7 は、User Setup ボックスを示しています。

図 11-7　ACS User Setup ボックス



ステップ 13　Password Authentication ドロップダウン メニューから **CiscoSecure Database** を選択します。

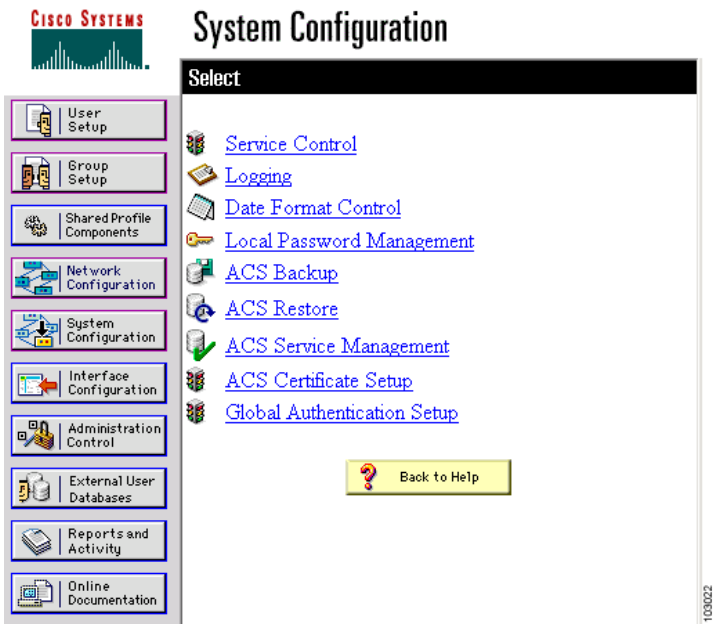
ステップ 14　Password フィールドと Confirm Password フィールドに、Wireless Services AP ページでアクセス ポイントに対して入力したのとまったく同じパスワードを入力します。

ステップ 15　**Submit** をクリックします。

ステップ 16　WDS アクセス ポイントを使用するアクセス ポイントそれぞれに対して、ステップ 10 からステップ 15 の手順を繰り返します。

ステップ 17　System Configuration ページを表示して **Service Control** をクリック、ACS を再始動してエントリ内容を適用します。図 11-8 は、System Configuration ページを示しています。

図 11-8　　ACS System Configuration ページ



WDS 情報の表示

Web ブラウザのインターフェイスでは、Wireless Services Summary ページを参照して WDS ステータスの概要を表示します。

イネーブル EXEC モードの CLI では、次のコマンドを使って、現在の WDS アクセス ポイントと CCKM に参加している他のアクセス ポイントについて情報を表示します。

コマンド	説明
show wlccp ap	CCKM に参加する任意のアクセス ポイント上で、このコマンドを使用して、WDS アクセス ポイントの MAC アドレス、WDS アクセス ポイントの IP アドレス、アクセス ポイントの状態（認証中、認証済み、登録済み）、インフラストラクチャ認証サーバの IP アドレス、クライアント デバイス（MN）認証サーバの IP アドレスを表示することができます。
show wlccp wds { **ap** | **mn** } [**detail**] [**mac-addr** *mac-address*]	WDS アクセス ポイントでのみ、このコマンドを使って、アクセス ポイントとクライアント デバイスに関するキャッシュ情報を表示できます。 • **ap**：このオプションを使用して、CCKM に参加するアクセス ポイントを表示します。このコマンドは、各アクセス ポイントの MAC アドレス、IP アドレス、状態（認証中、認証済み、または登録済み）、有効期間（アクセス ポイントが再認証を必要とするまでの秒数）を表示します。**mac-addr** オプションを利用して、特定のアクセス ポイントに関する情報を表示します。 • **mn**：このオプションはモバイル ノードとも呼ばれるクライアント デバイスに関するキャッシュされた情報を表示する場合に使用します。このコマンドにより、各クライアントの MAC アドレス、IP アドレス、クライアントにアソシエートされているアクセス ポイント（cur-AP）、および状態（認証中、認証済み、または登録済み）が表示されます。**detail** オプションを使用して、クライアントの有効期間（アクセス ポイントが再認証を必要とするまでの残りの秒数）、SSID、VLAN ID を表示します。**mac-addr** オプションを使用して、特定のクライアント デバイスに関する情報を表示します。 **show wlccp wds** のみを入力する場合、そのコマンドは、アクセス ポイントの IP アドレス、MAC アドレス、優先順位、インターフェイス状態（管理上スタンドアロン、アクティブ、バックアップ、または候補）を表示します。状態がバックアップの場合、コマンドは現在の WDS のアクセス ポイントの IP アドレス、MAC アドレス、および優先順位も表示します。

デバッグ メッセージの使用

イネーブル EXEC モードでは、デバッグ コマンドを使って、WDS アクセス ポイントと対話するデバイス用のデバッグ メッセージの表示を制御します。

コマンド	説明
debug wlccp ap { **mn** | **mobility** | **rm** | **state** |**wds-discovery** }	このコマンドを使って、クライアント デバイス（**mn**）、WDS 検出プロセス、WDS アクセス ポイント（**state**）に対するアクセス ポイントの認証に関連するデバッグ メッセージの表示をオンにします。
debug wlccp leap-client	このコマンドを使って、LEAP 使用可能クライアント デバイスに関連するデバック メッセージの表示をオンにします。
debug wlccp packet	このコマンドを使用して、WDS アクセス ポイントとやりとりするパケットの表示をオンにします。
debug wlccp wds [**state** | **statistics**]	このコマンドと **state** オプションを使って、WDS デバックと状態のメッセージの表示をオンにします。**statistics** オプションを使って、障害統計情報の表示をオンにします。