Cisco Unified Wireless Network での Wi-Fi Protected Access（WPA）の設定例

内容

概要
前提条件
要件
使用するコンポーネント
表記法
WPA および WPA2 のサポート
ネットワークのセットアップ
WPA2 Enterprise モード向けのデバイスの設定
外部 RADIUS サーバによる RADIUS 認証用の WLC の設定
WPA2 Enterprise 動作モード向けの WLAN の設定
WPA2 Enterprise モード認証向けの RADIUS サーバの設定（EAP-FAST）
WPA2 Enterprise 動作モード向けのワイヤレス クライアントの設定
WPA2 Personal モード向けのデバイスの設定
トラブルシュート
関連情報

概要

このドキュメントでは、Cisco Unified Wireless Network で Wi-Fi Protected Access（WPA）を設定する方法について説明します。

前提条件

要件

この設定を開始する前に、次の項目に関する基本的な知識を必ず取得しておきます。

- WPA
- ワイヤレス LAN（WLAN）セキュリティ ソリューション**注**：Cisco WLANセキュリティソリューションの詳細については、『CiscoワイヤレスLANセキュリティの概要』を参照してください。

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いています。

- Cisco 1000 シリーズ Lightweight アクセス ポイント（LAP）
- ファームウェア 4.2.61.0 が稼働する Cisco 4404 ワイヤレス LAN コントローラ（WLC）
- ファームウェア 4.1 が稼働する Cisco 802.11a/b/g クライアント アダプタ
- ファームウェア 4.1 が稼働する Aironet Desktop Utility（ADU）
- Cisco Secure ACS サーバ バージョン 4.1

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ました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実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については、『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。

WPA および WPA2 のサポート

Cisco Unified Wireless Network は、Wi-Fi Alliance 認定の WPA および WPA2 をサポートしています。WPA は 2003 年に Wi-Fi Alliance によって導入されました。WPA2 は 2004 年に Wi-Fi Alliance によって導入されました。WPA2 の Wi-Fi 認定を受けたすべての製品は、WPA の Wi-Fi 認定を受けた製品と相互運用できることが求められています。

WPA および WPA2 は、データが公開されないこと、およびネットワークへのアクセスが認可ユーザに限定されるということを、エンド ユーザおよびネットワーク管理者に対して高いレベルで保証します。どちらの規格にも Personal 動作モードと Enterprise 動作モードがあり、これら 2 つの市場セグメント特有のニーズに応えます。これらは Enterprise モードでは、認証に IEEE 802.1X および EAP を使用します。これらは Personal モードでは、認証に事前共有キー（PSK）を使用します。Personal モードではユーザ認証に PSK を使用するため、ビジネスまたは官公庁への導入の場合、Cisco では Personal モードを推奨しません。企業環境では PSK は安全ではありません。

WPA は、従来の IEEE 802.11 によるセキュリティ実装における WEP の既知のすべての脆弱性に対処し、企業環境とスモール オフィス、ホーム オフィス（SOHO）環境の両方において、WLAN に即座に適用できるセキュリティ ソリューションです。WPA では暗号化に TKIP を使用します。

WPA2 は次世代の Wi-Fi セキュリティ機能です。これは批准された IEEE 802.11i 標準を Wi-Fi Alliance と相互運用できるように実装したものです。WPA2 では、Counter Mode with Cipher Block Chaining Message Authentication Code Protocol（CCMP）を使用して、国立標準技術研究所（NIST）が推奨する AES の暗号化アルゴリズムを実装しています。WPA2 によって、官公庁の FIPS 140-2 への準拠が促進されます。

WPA モードと WPA2 モードのタイプの比較

	WPA	WPA2
Enterprise モード（ビジネス、官公庁、教育）	• 認証：IEEE 802.1X/EAP • 暗号化：TKIP/	• 認証：IEEE 802.1X/EAP • 暗号化：AES-

	MIC	CCMP
Personal モード（SOHO、家庭または個人）	• 認証：PSK • 暗号化：TKIP/MIC	• 認証：PSK • 暗号化：AES-CCMP

Enterprise 動作モードでは、WPA も WPA2 も両方とも認証に 802.1X/EAP を使用します。802.1X により、WLAN でクライアントと認証サーバの間の高性能な相互認証が利用できます。また、802.1X によってユーザ単位かつセッション単位の動的な暗号キーが提供されるため、静的な暗号キーに伴う管理上の負担やセキュリティ上の問題がなくなります。

802.1X の場合、認証に使用されるログオン パスワードなどのクレデンシャルが平文で、つまり暗号化されずにワイヤレス メディア経由で送信されることはありません。802.1X の認証タイプはワイヤレス LAN に対して高性能な認証方式を提供しますが、標準的な 802.11 WEP 暗号化はネットワーク攻撃に対して脆弱であるため、暗号化のためには 802.1X 以外に TKIP または AES が必要です。

いくつかの 802.1X 認証タイプが存在し、これらはそれぞれ認証の方式が異なりますが、クライアントとアクセス ポイントの間の通信については同じフレームワークおよび EAP に依存しています。Cisco Aironet 製品では、他のどの WLAN 製品よりも多くの種類の 802.1X EAP 認証をサポートしています。サポートされるタイプには、次のものがあります。

- Cisco LEAP
- EAP-Flexible Authentication via Secure Tunneling（EAP-FAST）
- EAP-Transport Layer Security（EAP-TLS）
- Protected Extensible Authentication Protocol（PEAP）
- EAP-Tunneled TLS（EAP-TTLS）
- EAP-Subscriber Identity Module（EAP-SIM）

802.1X 認証のもう 1 つのメリットは、WLAN ユーザ グループの集中管理で、これにはポリシーベースのキー ローテーション、動的キー割り当て、動的 VLAN 割り当て、SSID 制限などがあります。これらの機能では、暗号キーがローテーションされます。

Personal 動作モードでは、認証に事前共有キー（パスワード）が使用されます。Personal モードでは、アクセス ポイントおよびクライアント デバイスのみが必要ですが、Enterprise モードでは通常、RADIUS サーバなどの認証サーバがネットワーク上に必要になります。

このドキュメントでは、Cisco Unified Wireless Network 上に WPA2（Enterprise モード）および WPA2-PSK（Personal モード）を設定する例を示します。

ネットワークのセットアップ

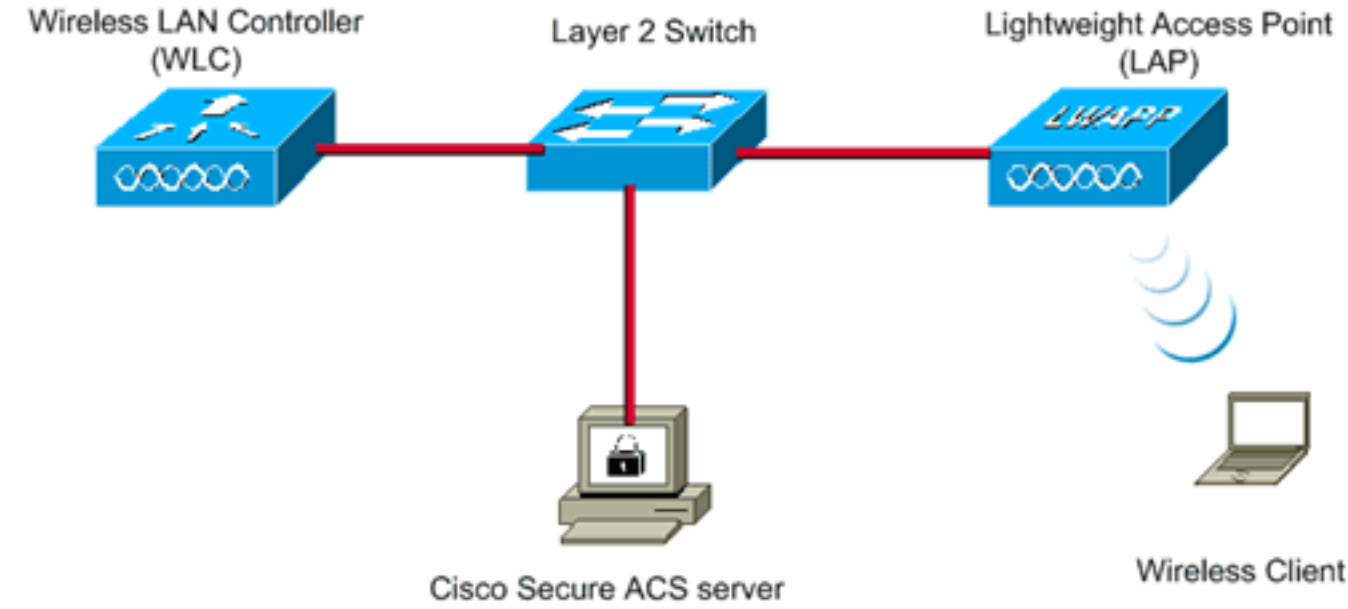
この構成では、Cisco 4404 WLC と Cisco 1000 Series LAP がレイヤ 2 スイッチを介して接続されています。外部 RADIUS サーバ（Cisco Secure ACS）も同じスイッチに接続します。すべてのデバイスは同じサブネット内にあります。アクセス ポイント（LAP）はコントローラに最初から登録されています。ワイヤレス LAN は、1 つを WPA2 Enterprise モード用に、もう 1 つを WPA2 Personal モード用に 2 つ作成する必要があります。

WPA2-EnterpriseモードのWLAN(SSID:WPA2-Enterprise)では、ワイヤレスクライアントの認証にEAP-FASTを使用し、暗号化にAESを使用します。ワイヤレス クライアントの認証用の外部

RADIUS サーバとして、Cisco Secure ACS サーバを使用します。

WPA2-PersonalモードWLAN(SSID:WPA2-PSK)は、事前共有キー「abcdefghijk」を使用した認証にWPA2-PSKを使用します。

この構成に合わせてデバイスを設定する必要があります。



WLC Management IP address:	10.77.244.204
WLC AP Manager IP address:	10.77.244.205
Wireless Client IP address:	10.77.244.221
Cisco Secure ACS server IP address	10.77.244.196
Subnet Mask used in this example	255.255.255.224

WPA2 Enterprise モード向けのデバイスの設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

WPA2 Enterprise 動作モード用にデバイスを設定するには、次の手順を実行します。

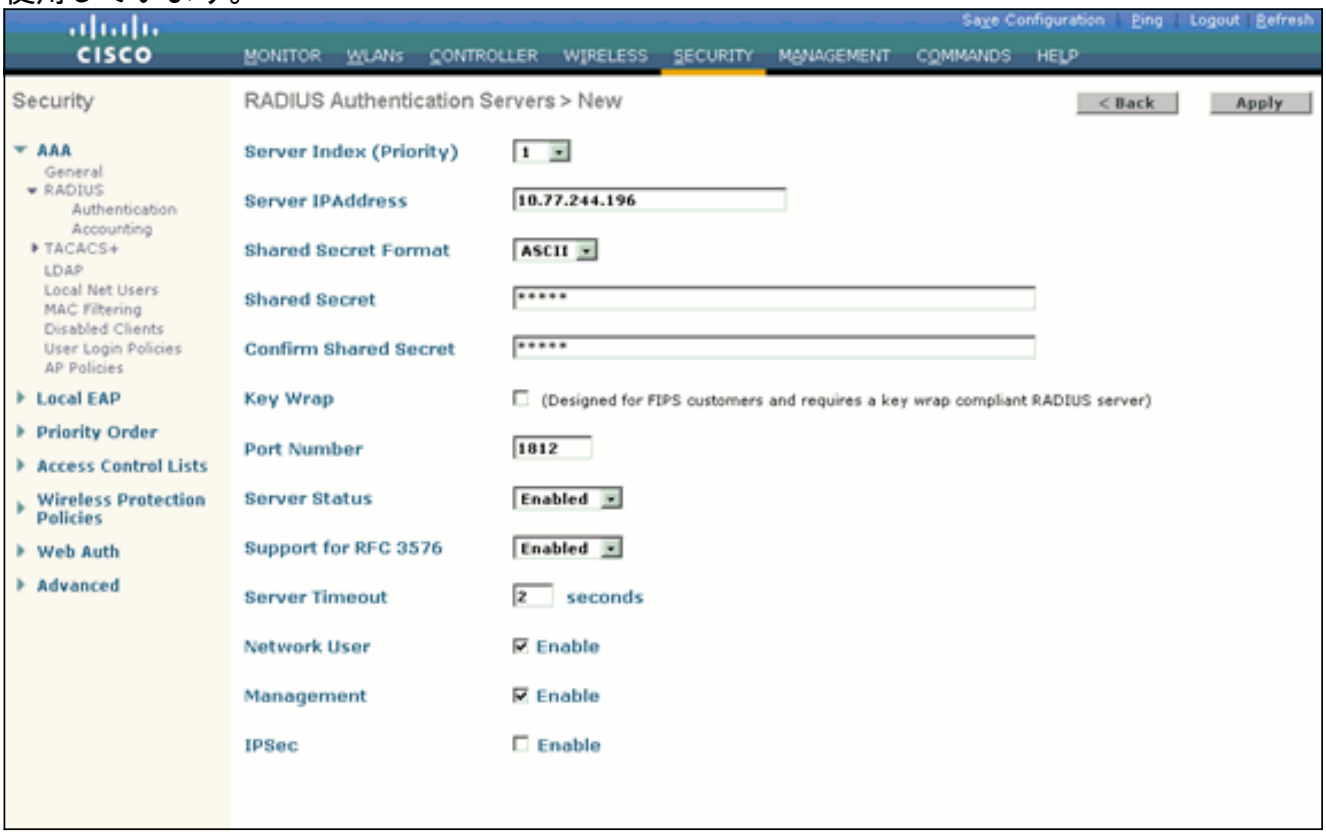
1. 外部 RADIUS サーバによる RADIUS 認証用の WLC の設定
2. WPA2 Enterprise モード認証向けの WLAN の設定（EAP-FAST）
3. WPA2 Enterprise モード向けのワイヤレス クライアントの設定

外部 RADIUS サーバによる RADIUS 認証用の WLC の設定

ユーザ クレデンシャルを外部 RADIUS サーバに転送するには、WLC を設定する必要があります。そうすると、外部 RADIUS サーバは、EAP-FAST を使用してユーザのクレデンシャルを検証し、ワイヤレス クライアントにアクセス権を付与します。

外部 RADIUS サーバ用に WLC を設定するには、次の手順を実行します。

1. コントローラの GUI から [Security]、[RADIUS]、[Authentication] を選択して、[RADIUS Authentication Servers] ページを表示します。次に、[New] をクリックして、RADIUS サーバを定義します。
2. [RADIUS Authentication Servers] > [New] ページで RADIUS サーバのパラメータを定義します。次のパラメータがあります。RADIUS サーバの IP アドレス共有秘密ポート番号サーバステータスこのドキュメントでは、10.77.244.196 という IP アドレスを持つ ACS サーバを使用しています。



3. [Apply] をクリックします。

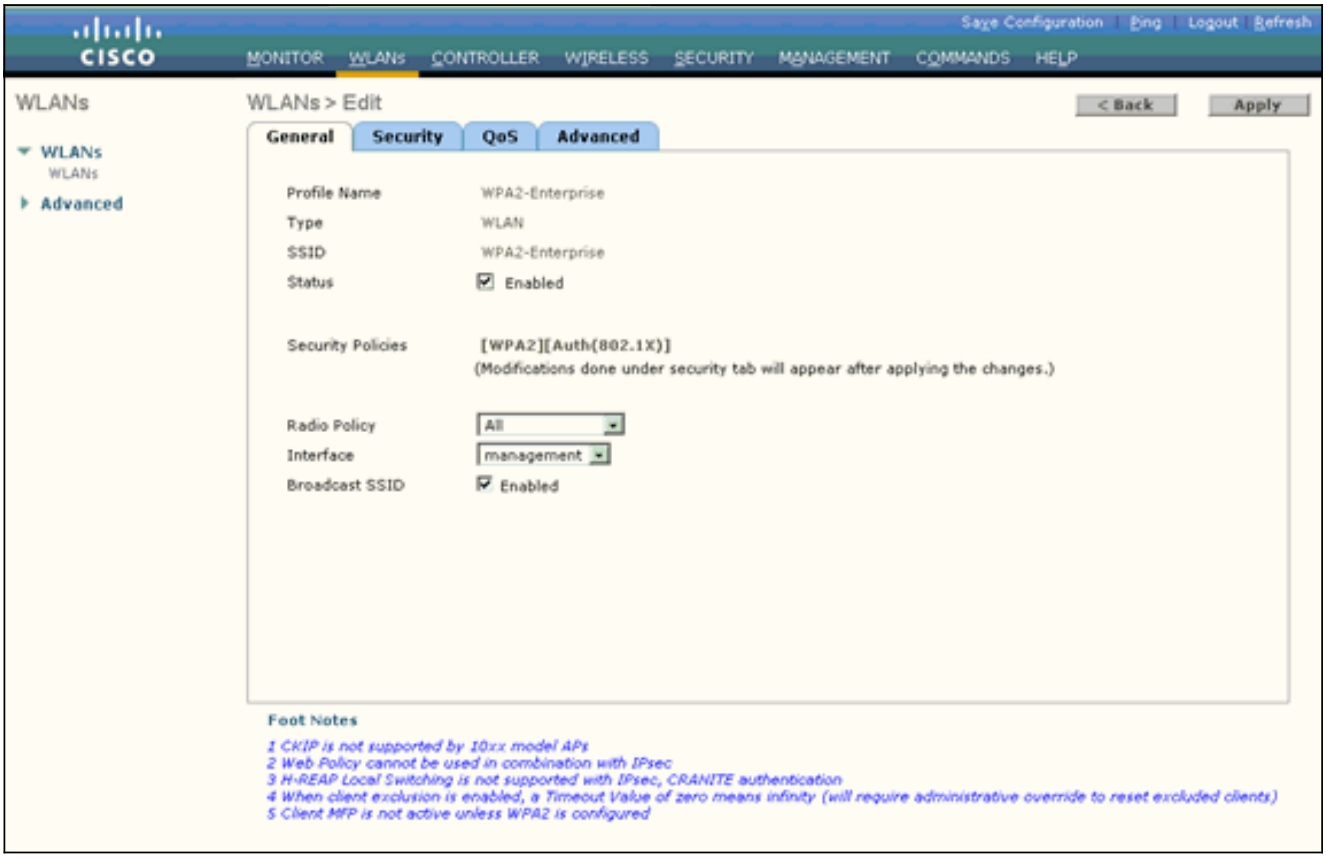
WPA2 Enterprise 動作モード向けの WLAN の設定

次に、クライアントがワイヤレス ネットワークに接続するために使用する WLAN を設定します。WPA2 Enterprise モード用の WLAN SSID は、WPA2-Enterprise です。この例では、この WLAN を管理インターフェイスに割り当てます。

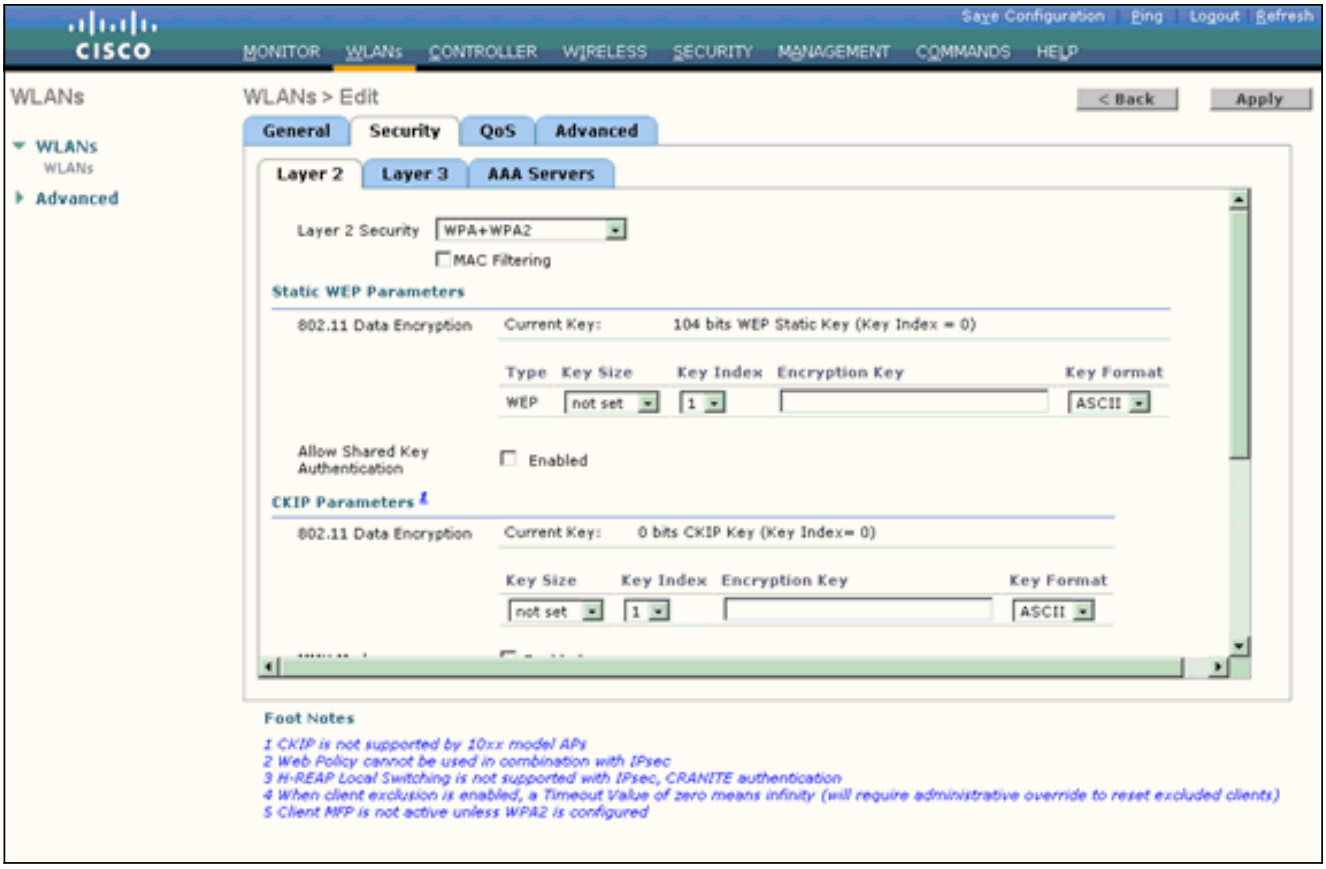
WLAN と関連するパラメータを設定するために、次の手順を実行します。

1. コントローラの GUI で [WLANs] をクリックして、[WLANs] ページを表示します。このページには、コントローラに存在する WLAN の一覧が表示されます。
2. [New] をクリックして新規の WLAN を作成します。
3. [WLANs] > [New] ページで WLAN SSID 名とプロファイル名を入力します。次に、[Apply] をクリックします。この例では、SSID として **WPA2-Enterprise** を使用しています。

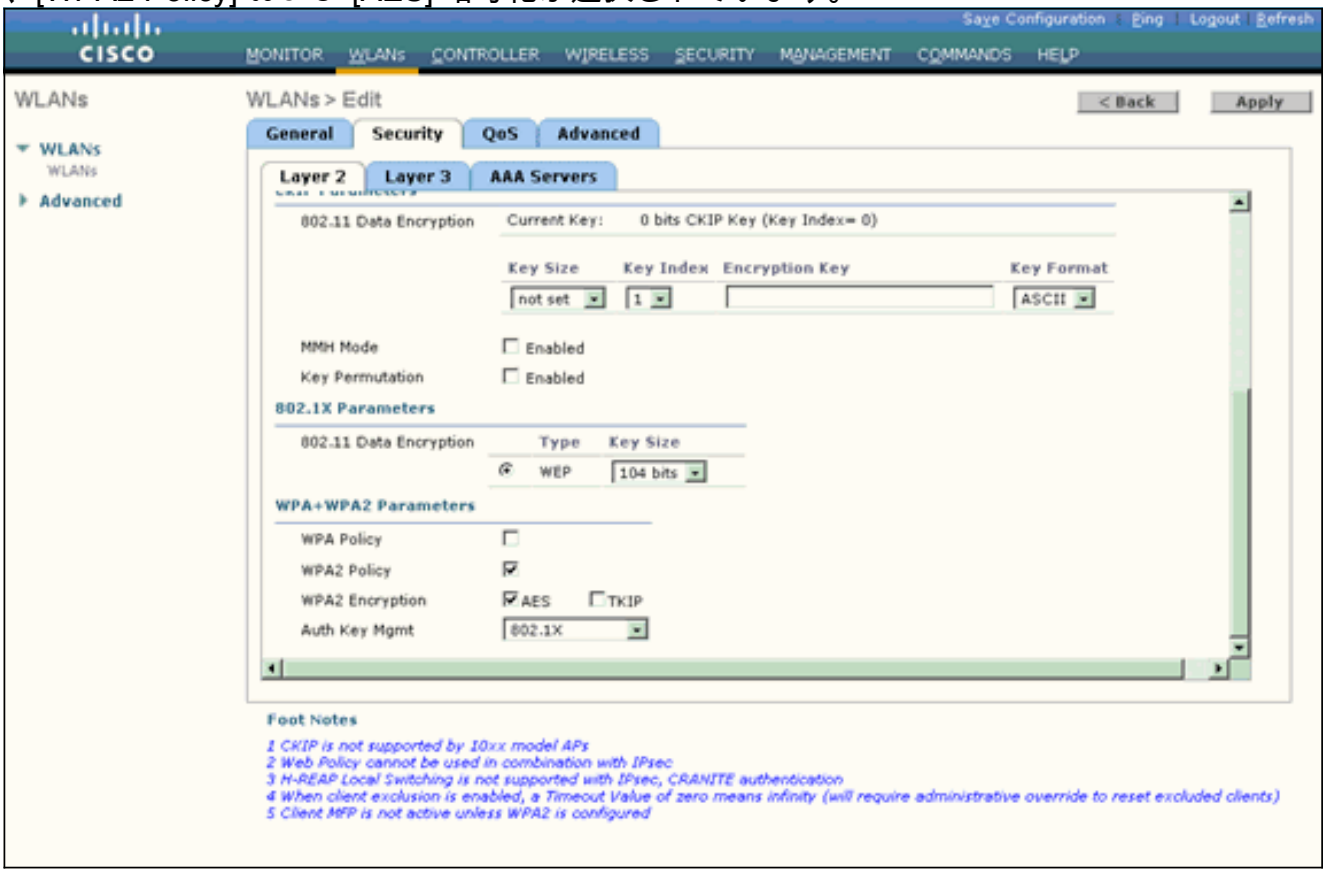
4. 新しい WLAN を作成すると、新しい WLAN に対する [WLAN] > [Edit] ページが表示されます。このページでは、その WLAN に固有のさまざまなパラメータを定義できます。これには、全般ポリシー、セキュリティ ポリシー、QOS ポリシー、および高度なパラメータが含まれます。
5. WLAN を有効にするには、[General Policies] で [Status] チェック ボックスをオンにします。



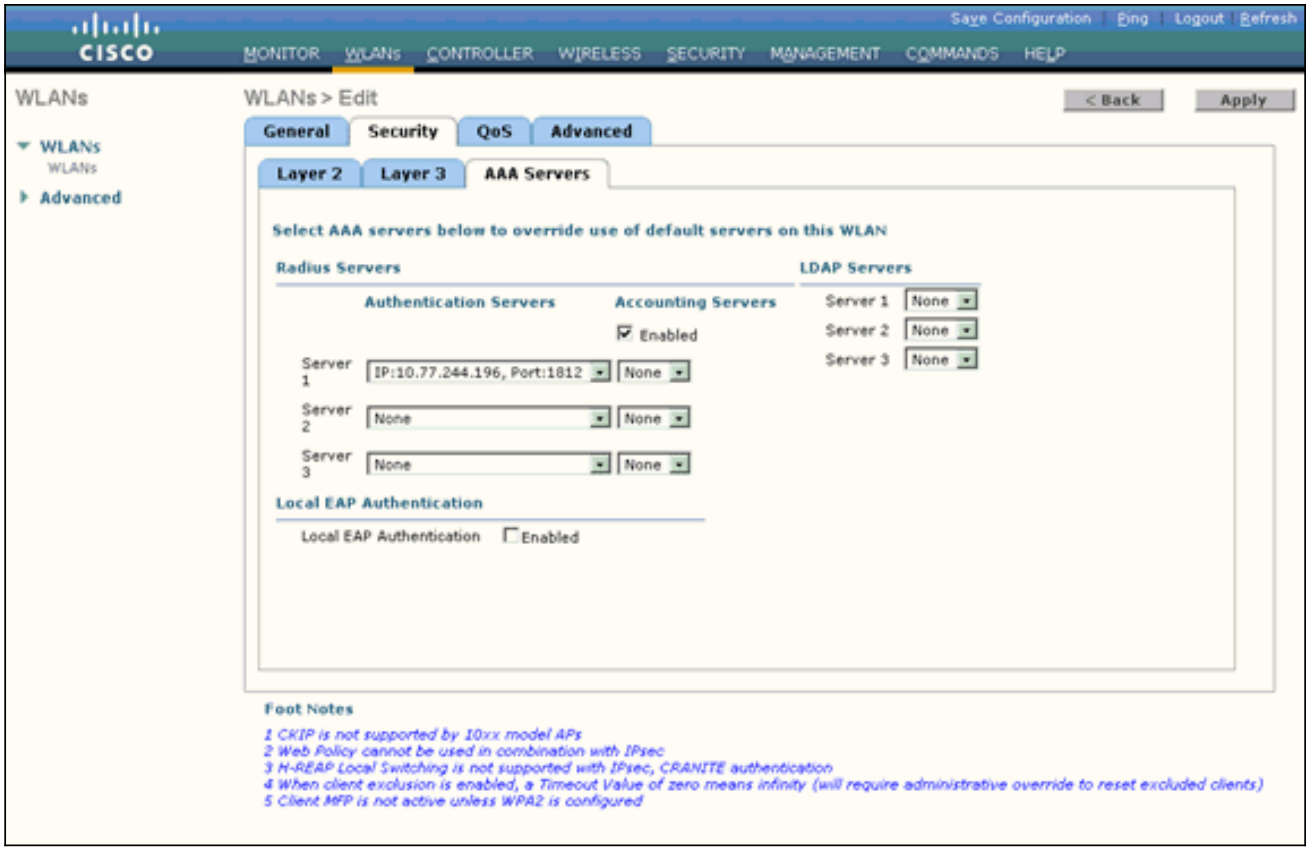
6. AP にビーコン フレームで SSID をブロードキャストさせる場合は、[Broadcast SSID] にチェックボックスをオンにします。
7. [Security] タブをクリックします。[Layer 2 Security] で、[WPA+WPA2] を選択します。これにより、WLAN に対して WPA 認証が有効になります。



8. [WPA+WPA2 Parameters] を変更するために、ページを下にスクロールします。この例では、[WPA2 Policy] および [AES] 暗号化が選択されています。



9. [Auth Key Mgmt] で [802.1x] を選択します。これで、802.1x/EAP 認証と AES 暗号化を使用する WPA2 が WLAN に対して有効になります。
10. [AAA Servers] タブを選択します。[Authentication Servers] から、適切なサーバ IP アドレスを選択します。この例では、10.77.244.196 が RADIUS サーバとして使用されます。



11. [Apply] をクリックします。**注**：これは、EAP認証用にコントローラで設定する必要がある唯一のEAP設定です。EAP-FAST に固有なその他すべての設定は、RADIUS サーバおよび認証が必要なクライアントで行う必要があります。

WPA2 Enterprise モード認証向けの RADIUS サーバの設定（EAP-FAST）

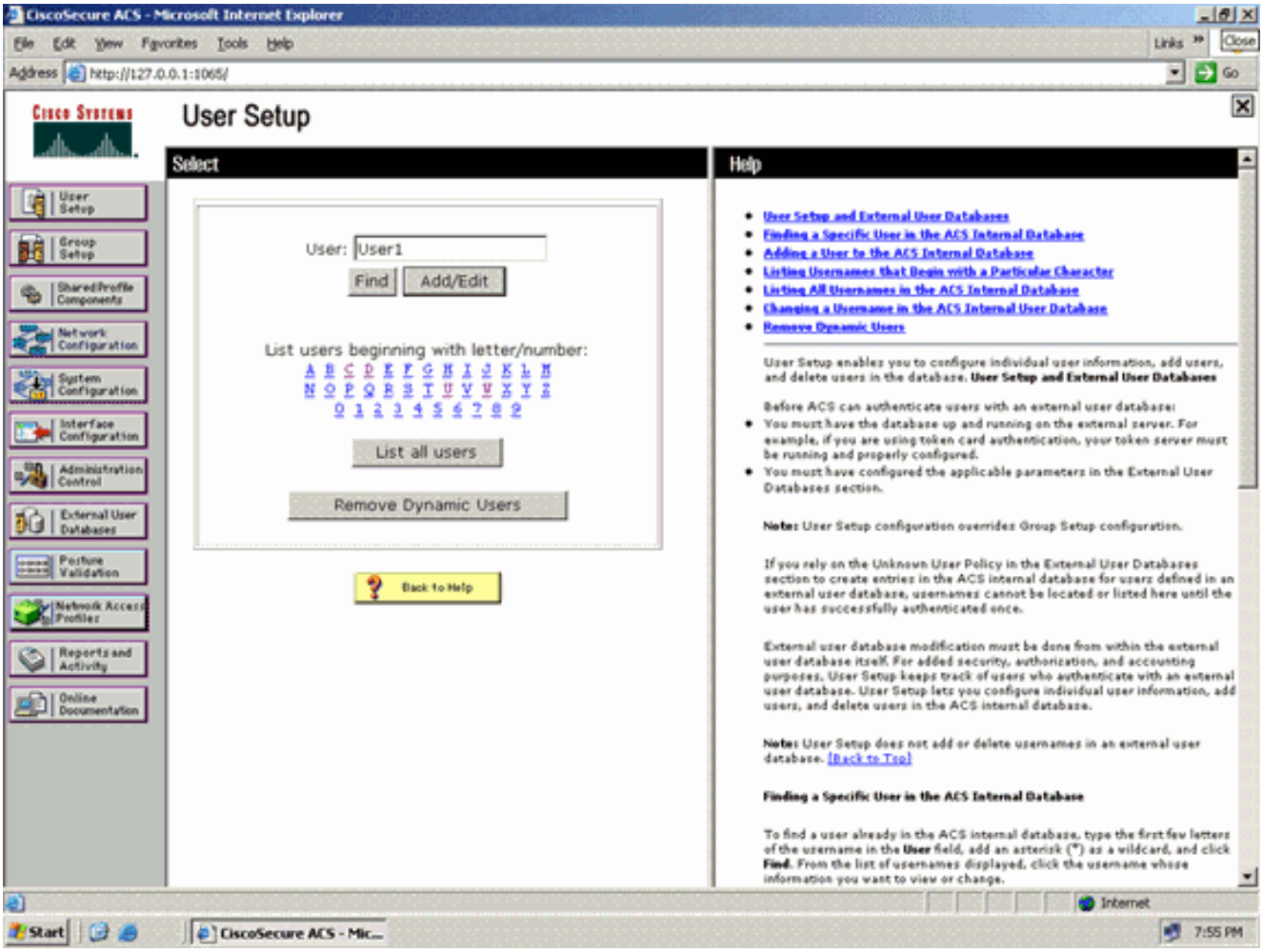
この例では、外部 RADIUS サーバとして Cisco Secure ACS サーバを使用しています。RADIUS サーバの EAP-FAST 認証を設定するには、次の手順を実行します。

1. クライアント認証用のユーザ データベースの作成
2. AAA クライアントとしての WLC の RADIUS サーバへの追加
3. 匿名インバンド PAC プロビジョニングによる RADIUS サーバへの EAP-FAST 認証の設定
   注：EAP-FASTは、匿名インバンドPACプロビジョニングまたは認証済みインバンドPACプロビジョニングのいずれかで設定できます。この例では匿名インバンド PAC プロビジョニングを使用します。EAP-FAST を匿名インバンド PAC プロビジョニングおよび認証済みインバンド PAC プロビジョニングで設定することについての詳細な情報および設定例については『ワイヤレス LAN コントローラおよび外部 RADIUS サーバを使用する EAP-FAST 認証の設定例』を参照してください。

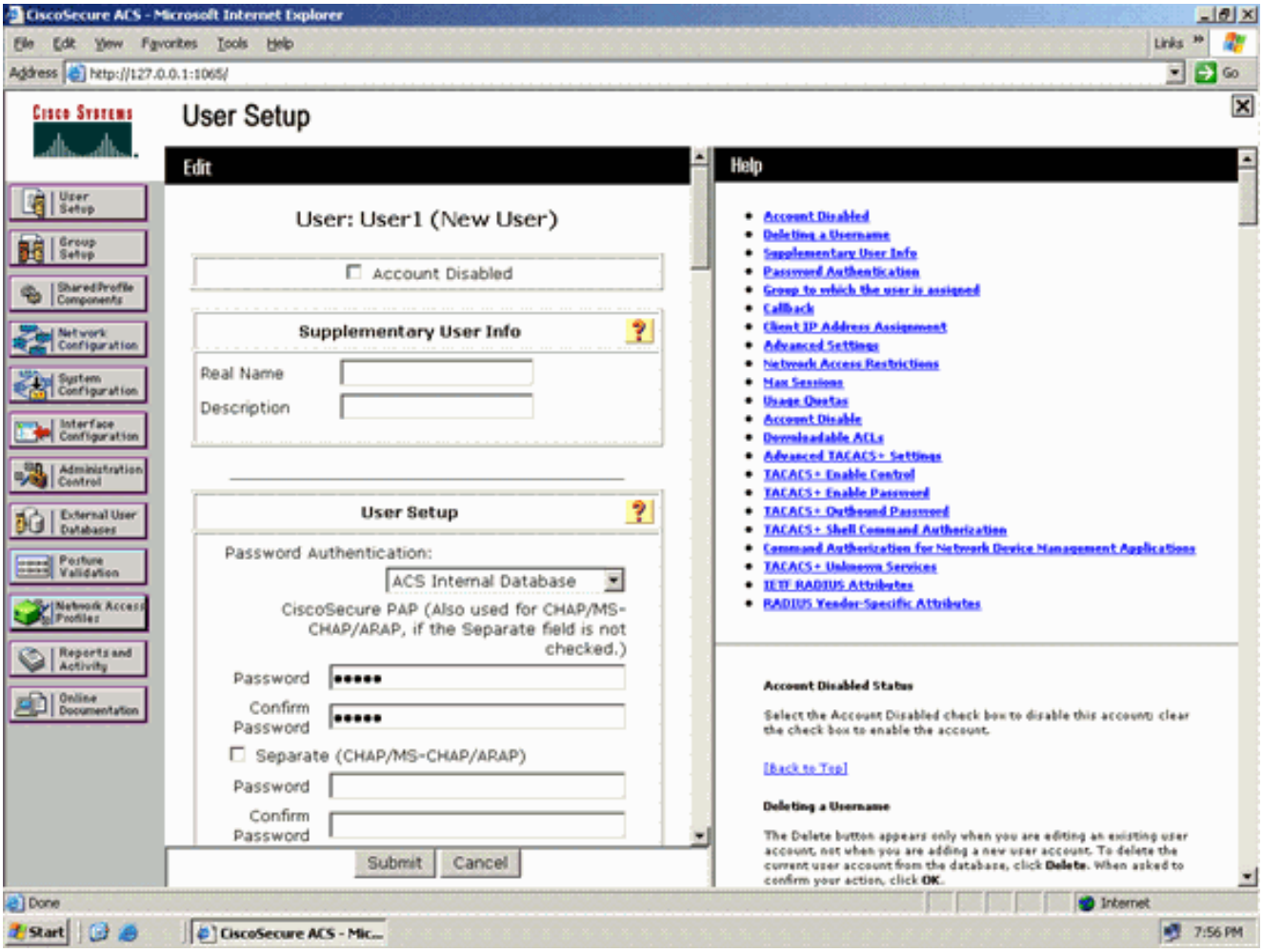
EAP-FAST クライアント認証用のユーザ データベースの作成

ACS で EAP-FAST クライアント用のユーザ データベースを作成するには、次の手順を実行します。この例では、EAP-FAST クライアントのユーザ名およびパスワードをそれぞれ User1、User1 に設定します。

1. ナビゲーション バーの ACS GUI から、[User Setup] を選択します。新しいワイヤレス ユーザを作成し、[Add/Edit] をクリックして、このユーザの編集ページに移動します。



2. [User Setup] の [Edit] ページで、この例に示すように、[Real Name]、[Description]、[Password] を設定します。このドキュメントでは、[Password Authentication] オプションで [ACS Internal Database] を使用しています。

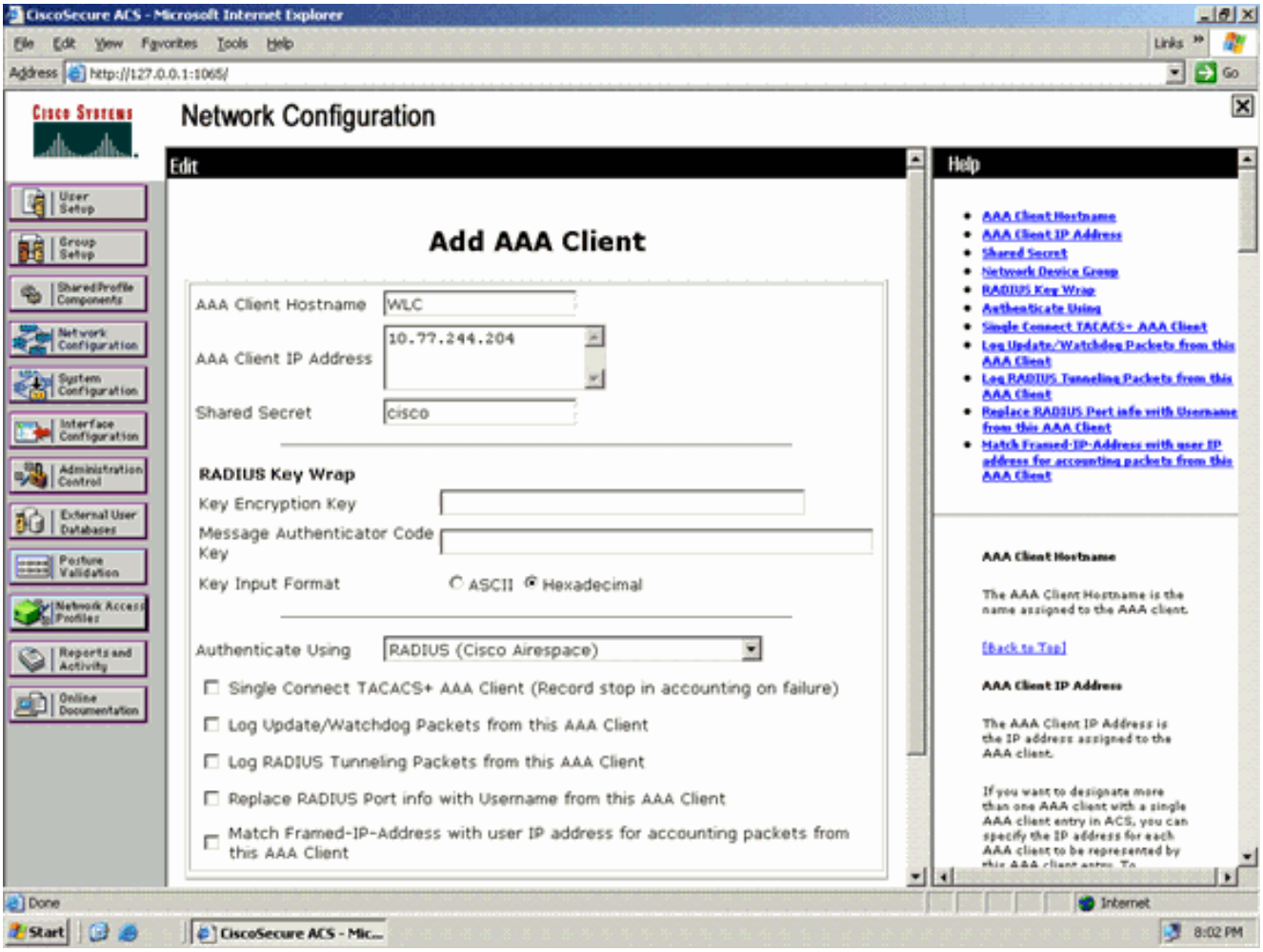


3. [Password Authentication] ドロップダウン ボックスから [ACS Internal Database] を選択します。
4. その他の必須パラメータをすべて設定して [Submit] をクリックします。

AAA クライアントとしての WLC の RADIUS サーバへの追加

ACS サーバでコントローラを AAA クライアントとして定義するには、次の手順を実行します。

1. ACS の GUI で [Network Configuration] をクリックします。[Network Configuration] ページの [Add AAA client] セクションで、[Add Entry] をクリックして、AAA クライアントとして WLC を RADIUS サーバに追加します。
2. [AAA Client] ページで、WLC の名前、IP アドレス、共有秘密、および認証方式（RADIUS または Cisco Airespace）を定義します。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。



注：WLCとACSサーバで設定する共有秘密キーは一致している必要があります。共有秘密では、大文字と小文字が区別されます。

3. [Submit+Apply] をクリックします。

匿名インバンド PAC プロビジョニングによる RADIUS サーバへの EAP-FAST 認証の設定

匿名インバンド プロビジョニング

これは、2 つのインバンド プロビジョニング方式の 1 つです。これにより、ACS は、クライアントに新しい PAC を提供するために、エンドユーザ クライアントとセキュア接続を確立します。このオプションでは、エンドユーザ クライアントと ACS の間で匿名の TLS ハンドシェイクが可能になります。

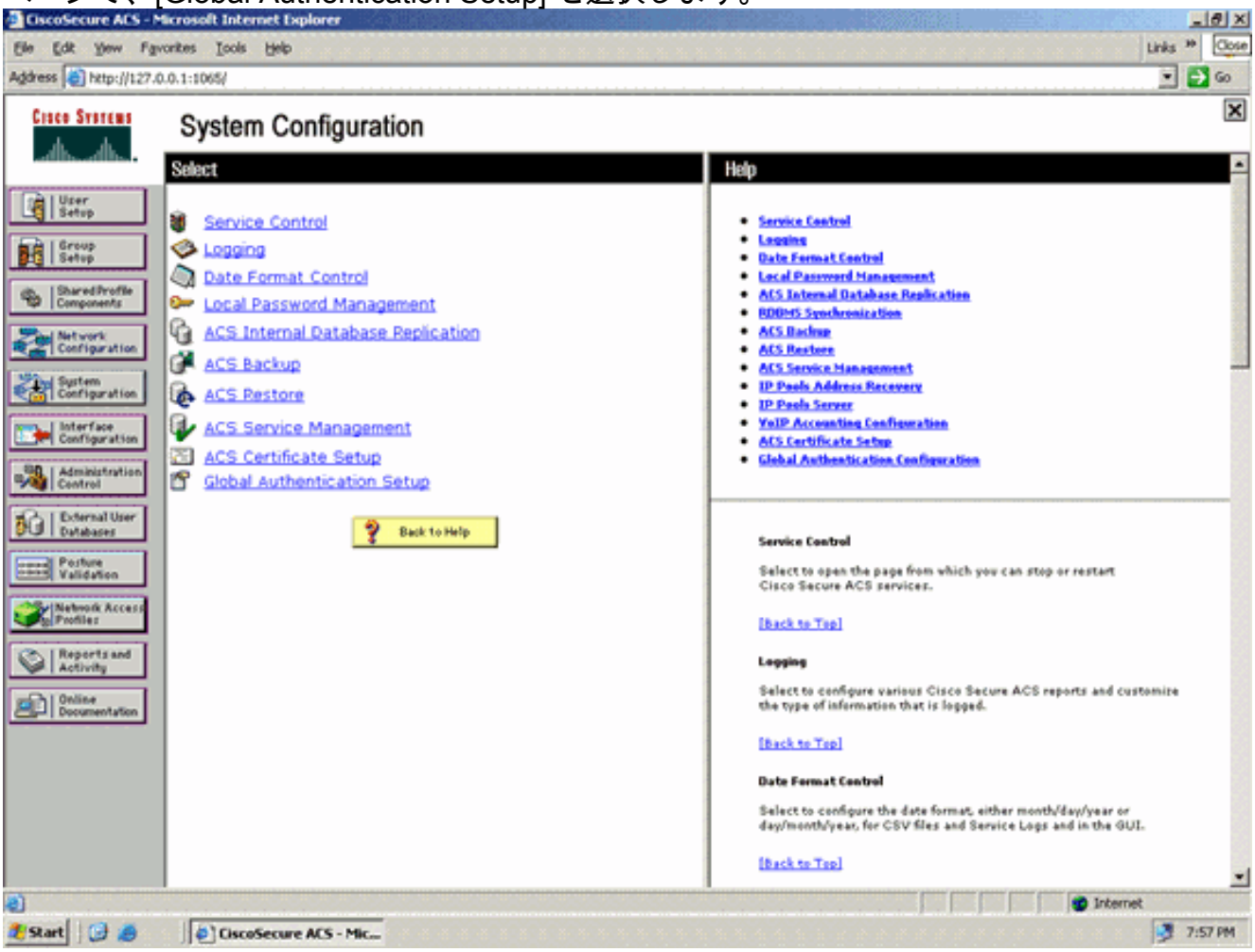
この方式は、ピアが ACS サーバを認証する前に、Authenticated Diffie-HellmanKey Agreement Protocol（ADHP）トンネル内で機能します。

ACS では、ユーザの EAP-MS-CHAPv2 認証が必要です。ユーザ認証が成功すると、ACS はエンドユーザ クライアントとの Diffie-Hellman トンネルを確立します。ACS はユーザ用の PAC を生成し、この ACS に関する情報とともにこのトンネル内でエンドユーザ クライアントに送信します。このプロビジョニング方式は、認証方式としてフェーズ 0 で EAP-MSCHAPv2、フェーズ 2 で EAP-GTC を使用します。

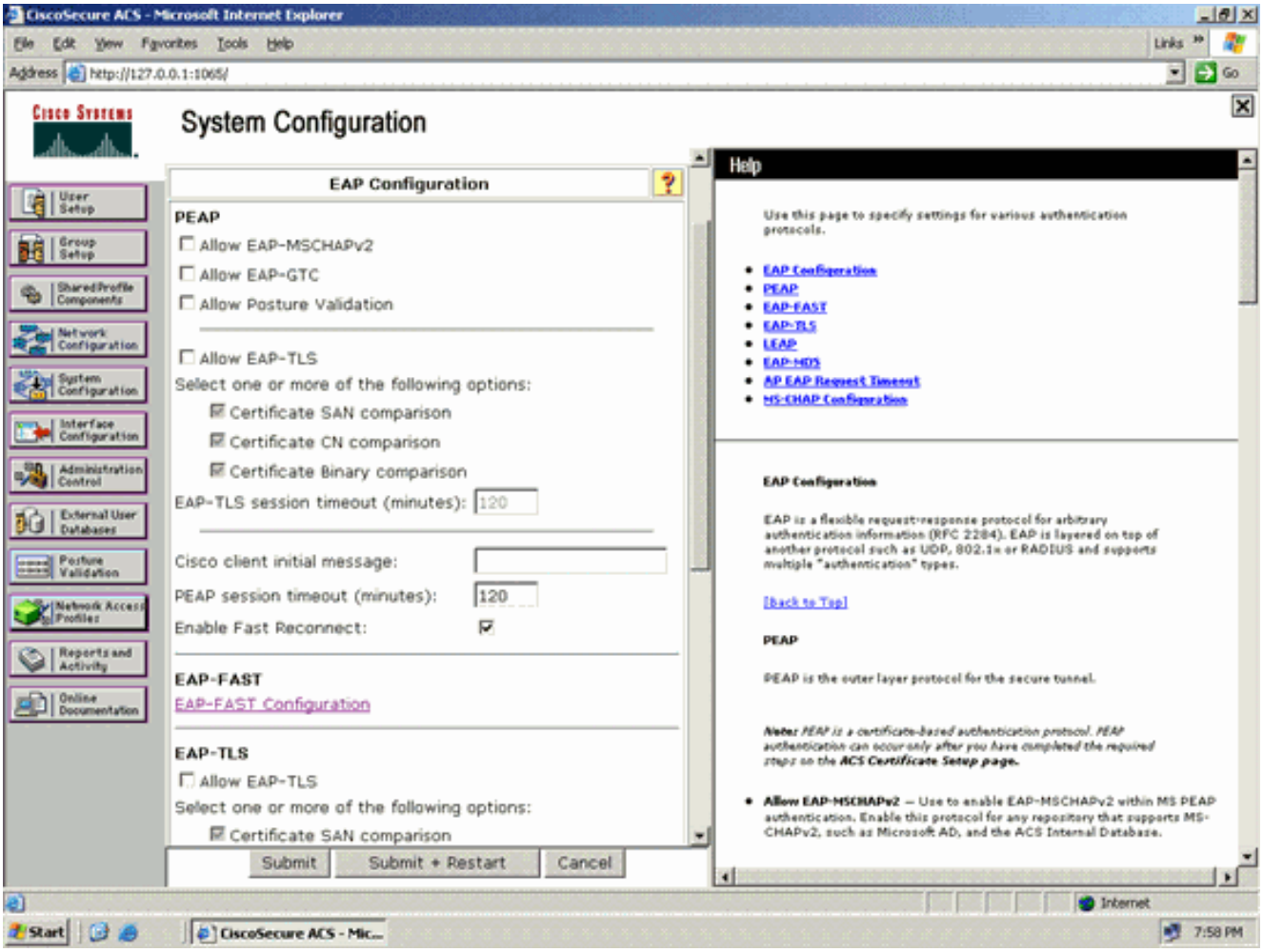
非認証サーバがプロビジョニングされるため、プレーン テキスト パスワードは使用できません。そのため、トンネル内では MS-CHAP クレデンシャルだけを使用できます。MS-CHAPv2 は、その後の認証セッションのためにピアの ID をプローブし、PAC を受け取るときに使用されます（EAP-MS-CHAP は内部方式としてのみ使用されます）。

RADIUS サーバ内で匿名インバンド プロビジョニング用に EAP-FAST 認証を設定するには、次の手順を実行します。

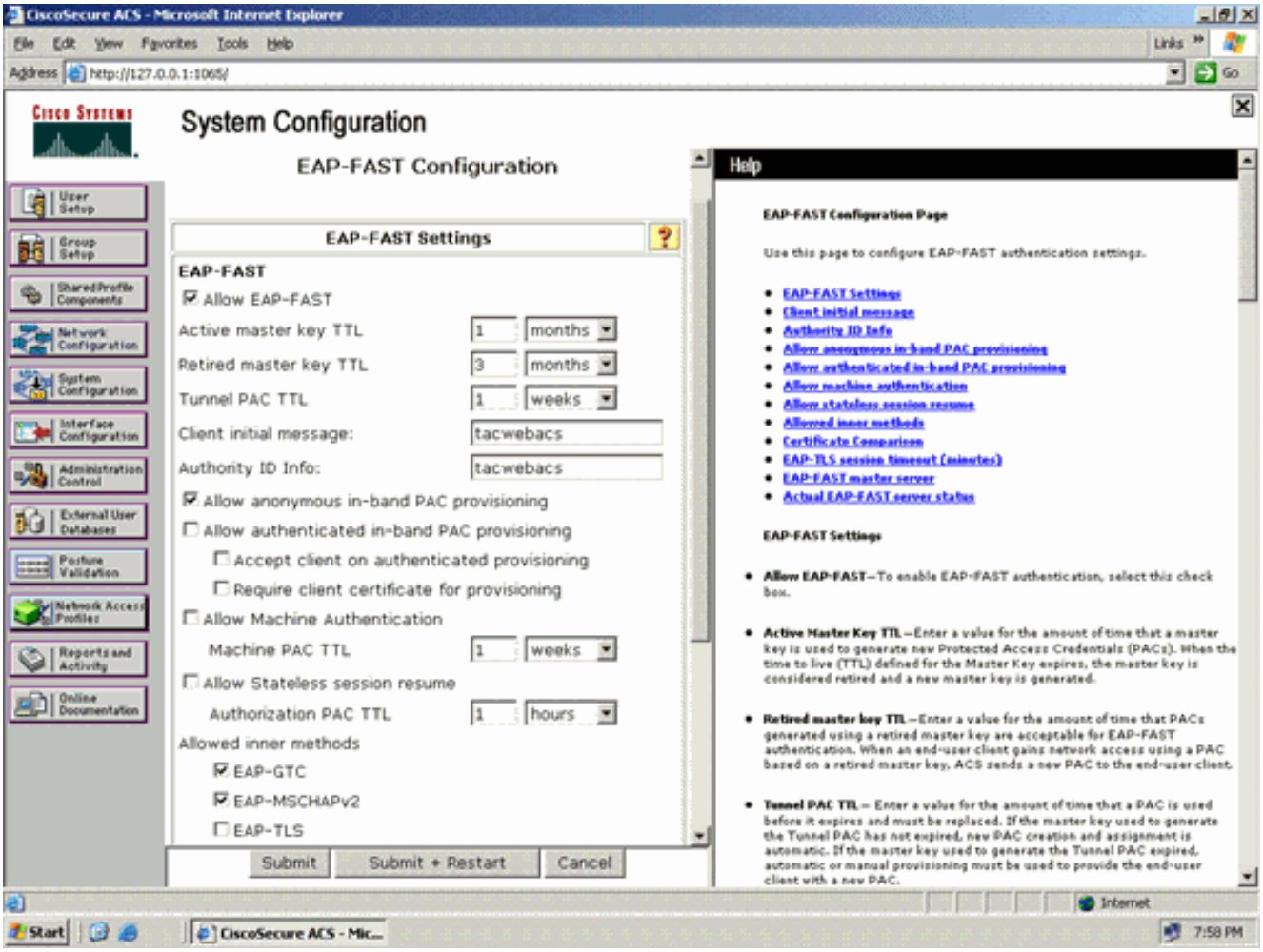
1. RADIUS サーバの GUI で [System Configuration] をクリックします。[System Configuration] ページで、[Global Authentication Setup] を選択します。



2. [Global Authentication setup] ページで [EAP-FAST Configuration] をクリックし、EAP-FAST 設定のページに進みます。



3. [EAP-FAST Settings] ページから、[Allow EAP-FAST] チェックボックスをオンにして、RADIUS サーバで EAP-FAST を有効にします。



4. アクティブおよびリタイア マスター キーの TTL（存続可能時間）の値を目的に合わせて設定するか、この例で示すようにデフォルト値に設定します。アクティブおよびリタイア マスター キーについては、「マスター キー」を参照してください。また、詳細については、「マスター キーおよび PAC TTLs」を参照してください。[Authority ID Info] フィールドは、この ACS サーバのテキスト ID を表し、認証先の ACS サーバをエンド ユーザが判別するために使用できます。このフィールドの入力は必須です。[Client initial display message] フィールドは、EAP-FAST クライアントを使用して認証するユーザに送信するメッセージを指定します。最大長は 40 文字です。ユーザに初期メッセージが示されるのは、エンドユーザ クライアントがその表示をサポートしている場合だけです。
5. ACS で匿名インバンド PAC プロビジョニングを実行する場合、[Allow anonymous in-band PAC provisioning] チェックボックスをオンにします。
6. **[Allowed inner methods]：このオプションにより、EAP-FAST TLS トンネル内で実行できる内部 EAP 方式が決まります。**匿名インバンド プロビジョニングを実行する場合は、下位互換性を確保するために EAP-GTC と EAP-MS-CHAP を有効にする必要があります。[Allow anonymous in-band PAC provisioning] を選択する場合は、EAP-MS-CHAP（フェーズ 0）および EAP-GTC（フェーズ 2）を選択する必要があります。

WPA2 Enterprise 動作モード向けのワイヤレス クライアントの設定

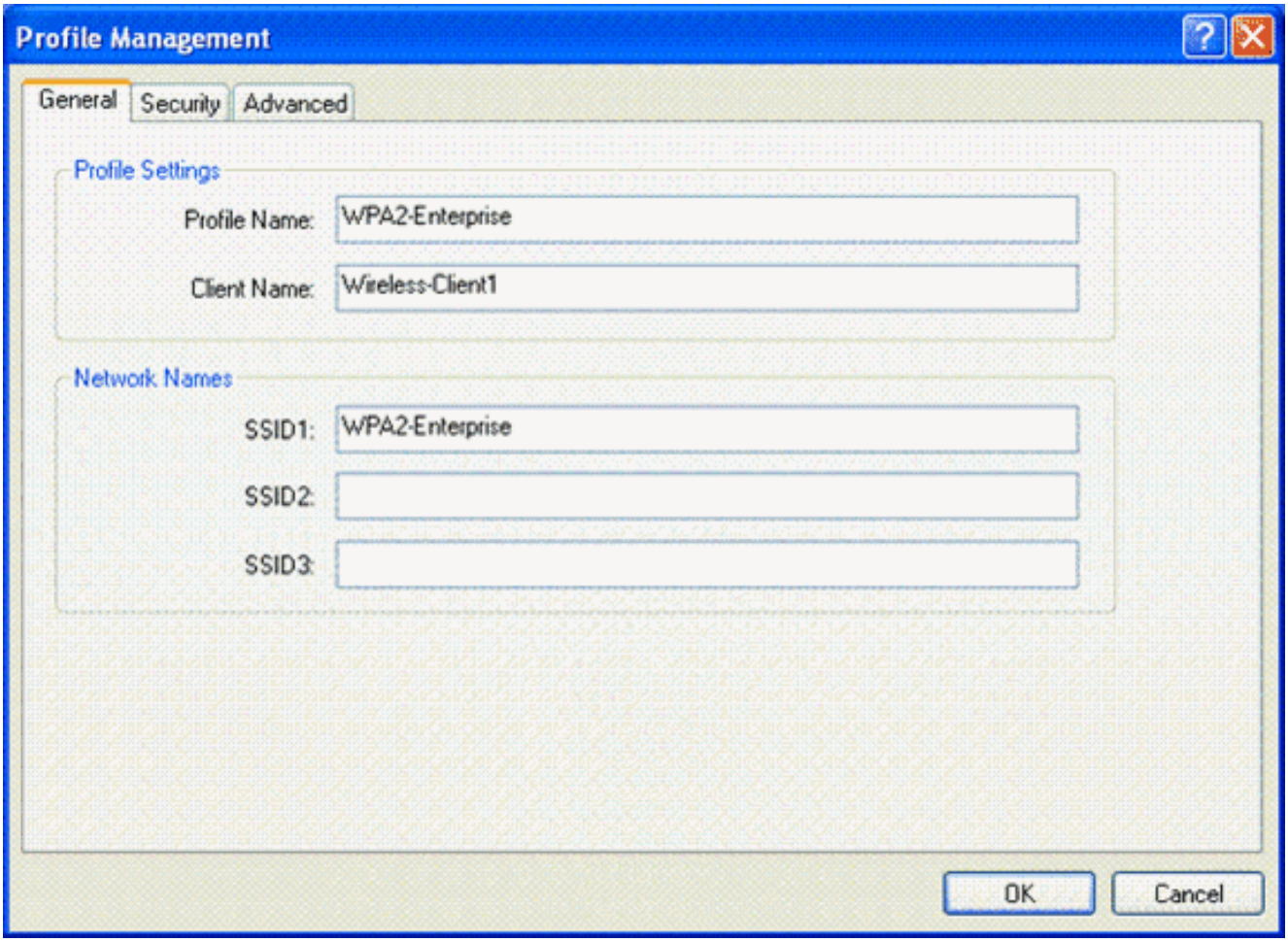
次の手順では、WPA2 Enterprise 動作モード用にワイヤレス クライアントを設定します。

WPA2 Enterprise モード用にワイヤレス クライアントを設定するには、次の手順を実行します。

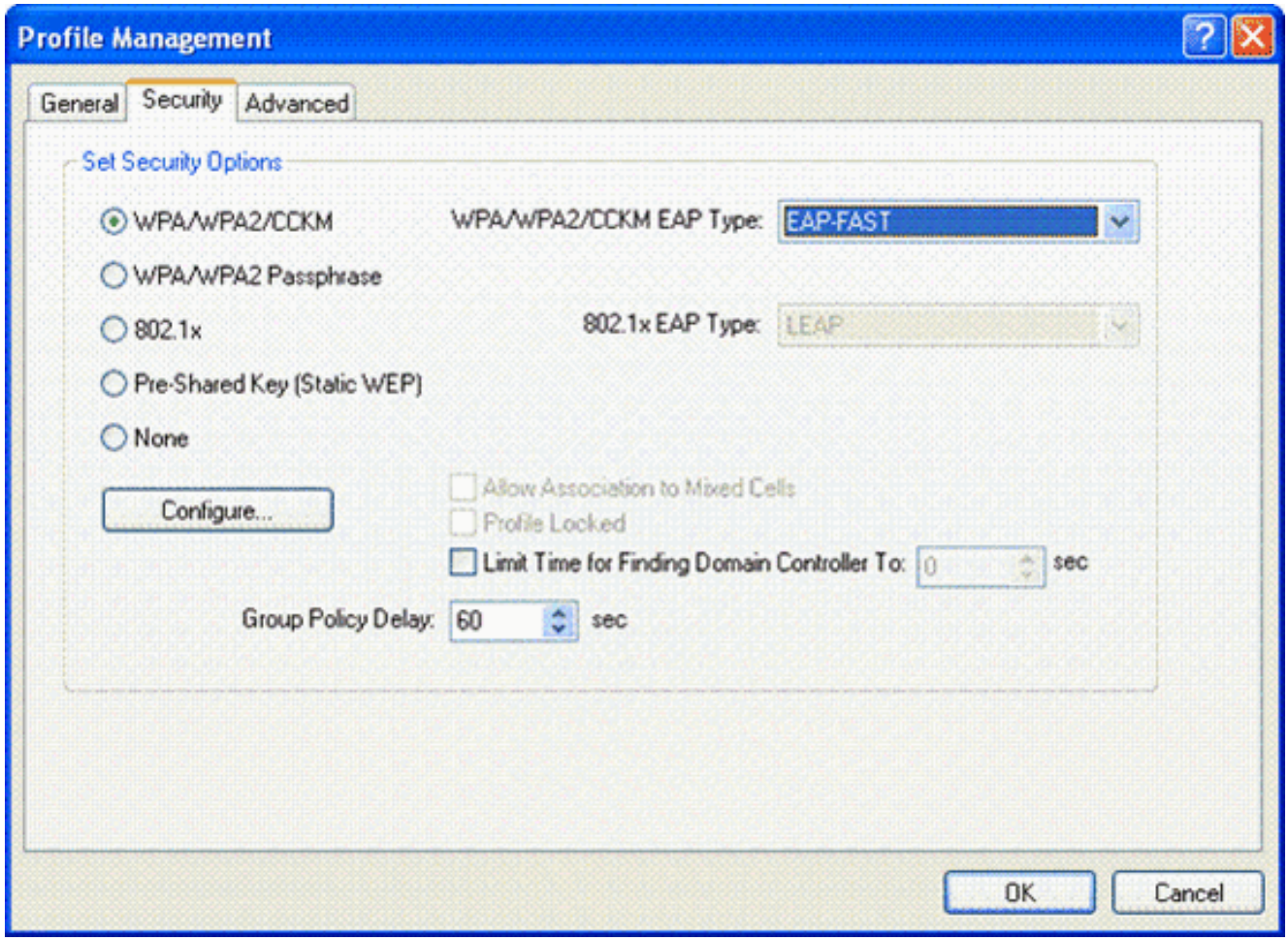
1. [Aironet Desktop Utility] ウィンドウで、[Profile Management] > [New] をクリックして、WPA2-Enterprise WLAN ユーザのプロファイルを作成します。すでに説明したように、この

ドキュメントでは、ワイヤレス クライアントの WLAN/SSID 名として **WPA2-Enterprise** を使用します。

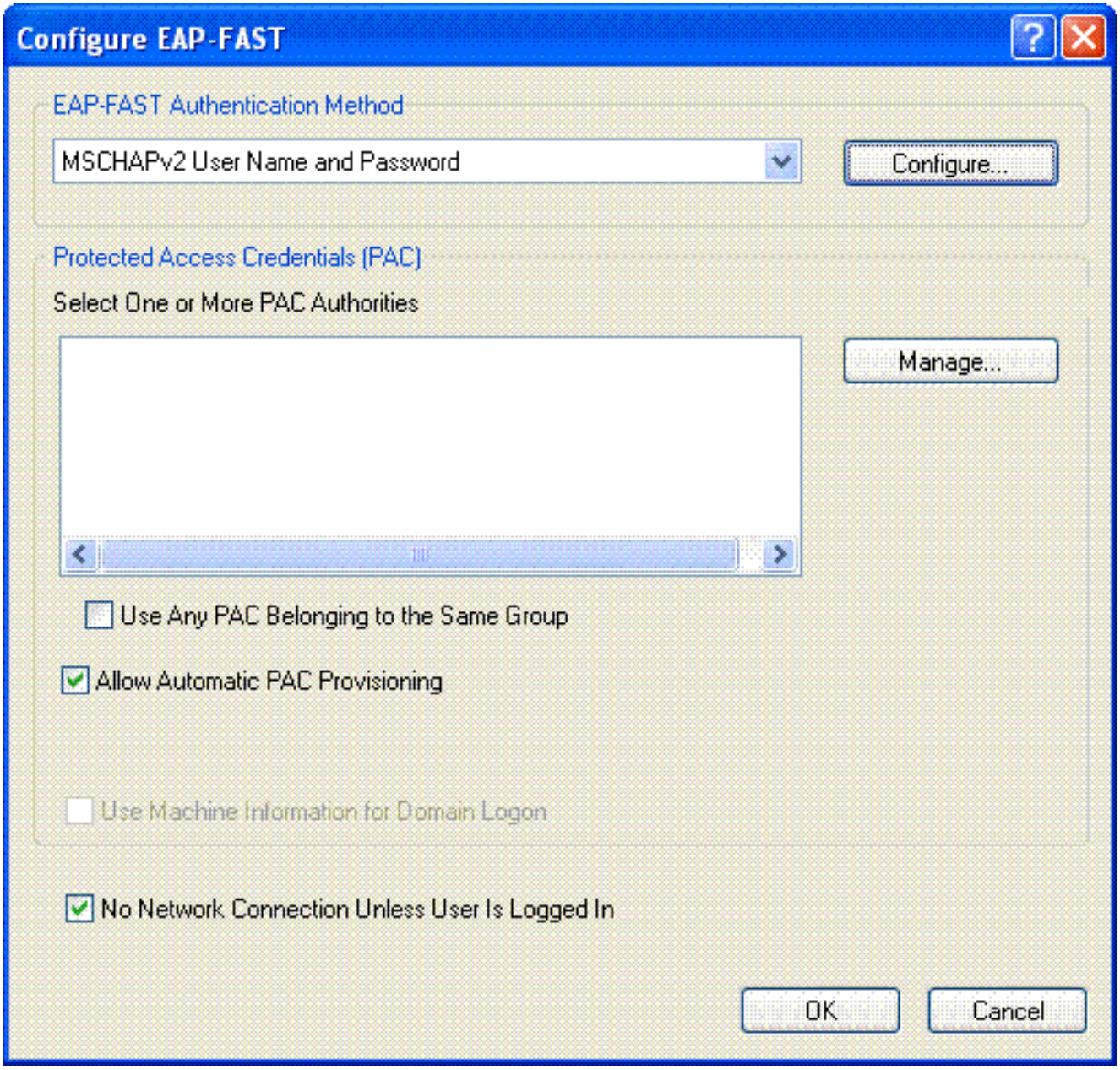
2. [Profile Management] ウィンドウの [General] タブをクリックし、この例に示すように、プロファイル名、クライアント名、および SSID 名を設定します。次に、[OK] をクリックします。



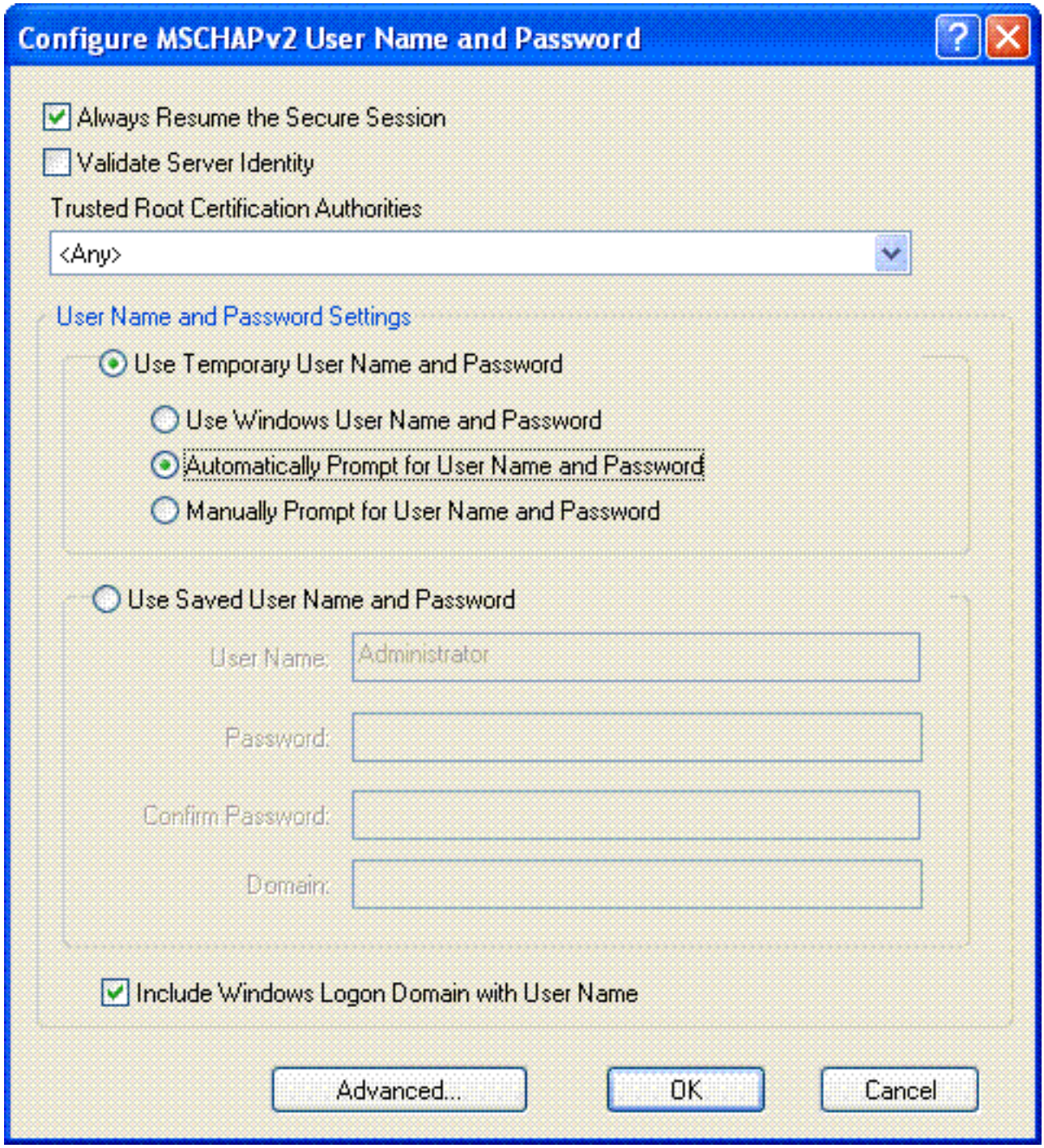
3. [Security] タブをクリックし、[WPA/WPA2/CCKM] を選択して WPA2 動作モードを有効にします。[WPA/WPA2/CCKM EAP Type] で、[EAP-FAST] を選択します。[Configure] をクリックして、EAP-FAST を設定します。



4. [Configure EAP-FAST] ウィンドウから、[Allow Automatic PAC Provisioning] チェック ボックスをオンにします。匿名 PAC プロビジョニングを設定する場合、EAP-MS-CHAP は、フェーズ 0 の内部方式だけで使用されます。



5. [EAP-FAST Authentication Method] ドロップダウン ボックスから、認証方式として [MSCHAPv2 User Name and Password] を選択します。[Configure] をクリックします。
6. [Configure MSCHAPv2 User Name and Password] ウィンドウから、適切なユーザ名とパスワード設定を選択します。この例では、[Automatically Prompt for User Name and Password] を選択しています。



同じユーザ名およびパスワードを ACS に登録する必要があります。すでに説明したように、この例ではユーザ名およびパスワードとしてそれぞれ User1、User1 を使用します。また、これは匿名インバンド プロビジョニングであることに注意してください。そのため、クライアントは、サーバ証明書を確認できません。[Validate Server Identity] チェックボックスがオフになっていることを確認します。

7. [OK] をクリックします。

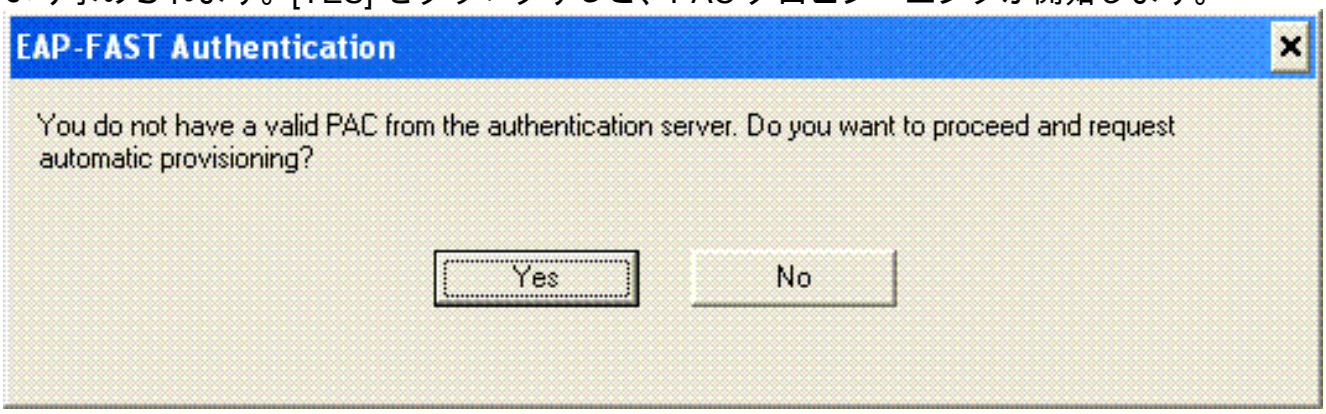
WPA2 Enterprise 動作モードの確認

WPA2 Enterprise 動作モード設定が正しく機能するかどうかを確認するには、次の手順を実行します。

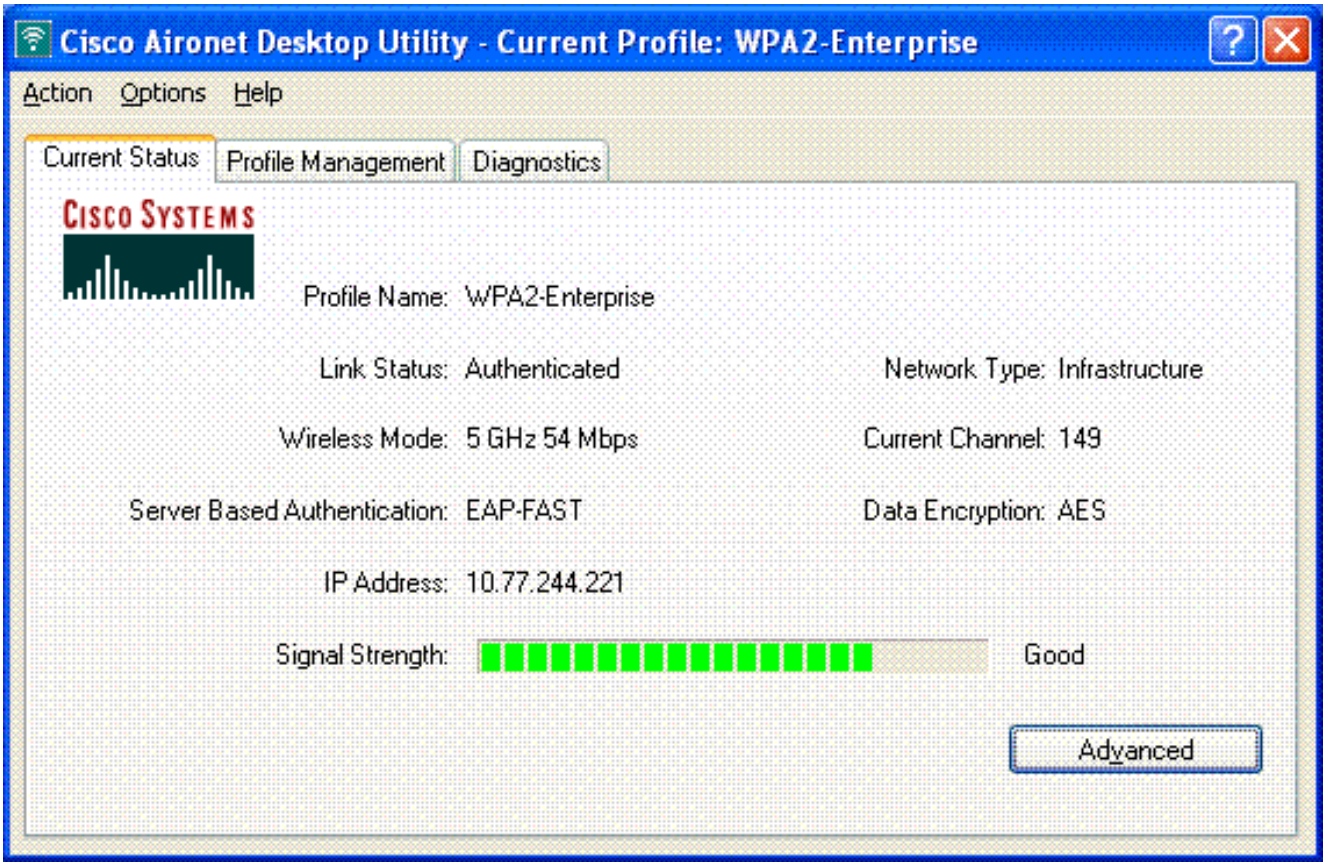
1. [Aironet Desktop Utility] ウィンドウで、[WPA2-Enterprise] プロファイルを選択して [Activate] をクリックし、ワイヤレス クライアント プロファイルをアクティブ化します。
2. MS-CHAP ver2 認証を有効にしている場合、ユーザ名およびパスワードを求めるプロンプト

がクライアントに表示されます。

3. ユーザの EAP-FAST 処理中、RADIUS サーバから PAC を要求するように、クライアントにより求められます。[YES] をクリックすると、PAC プロビジョニングが開始します。



4. フェーズ 0 で PAC プロビジョニングに成功した後、フェーズ 1 および 2 が実行され、認証手順が正常に実行されます。認証に成功すると、ワイヤレス クライアントは WLAN WPA2-Enterprise に関連付けられます。次にスクリーンショットを示します。



また、RADIUS サーバがワイヤレス クライアントから認証要求を受信して検証するかどうかも確認できます。そのためには、ACS サーバで Passed Authentications レポートと Failed Attempts レポートを調べます。これらのレポートは、ACS サーバの [Reports and Activities] で見ることができます。

WPA2 Personal モード向けのデバイスの設定

WPA2-Persona 動作モード用にデバイスを設定するには、次の手順を実行します。

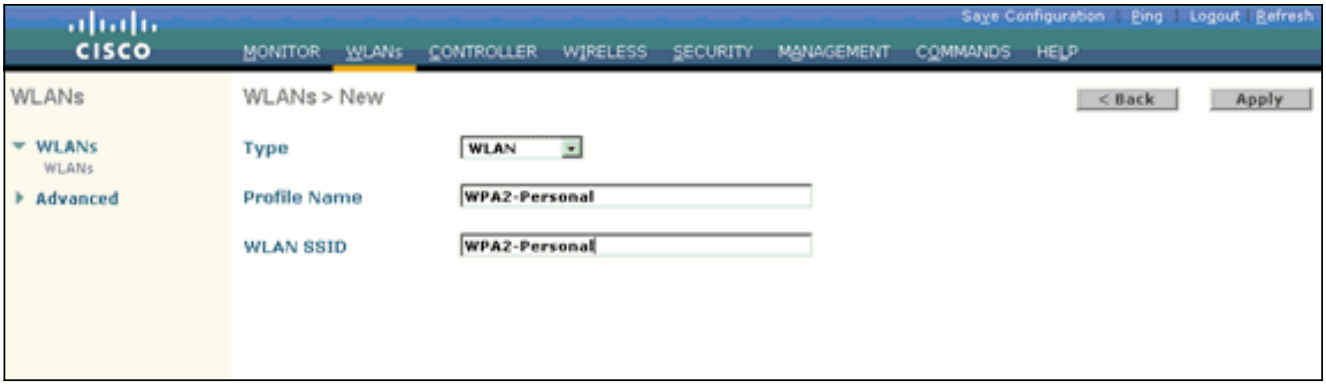
1. WPA2 Personal モード認証向けの WLAN の設定
2. WPA2 Personal モード向けのワイヤレス クライアントの設定

WPA2 Personal 動作モード向けの WLAN の設定

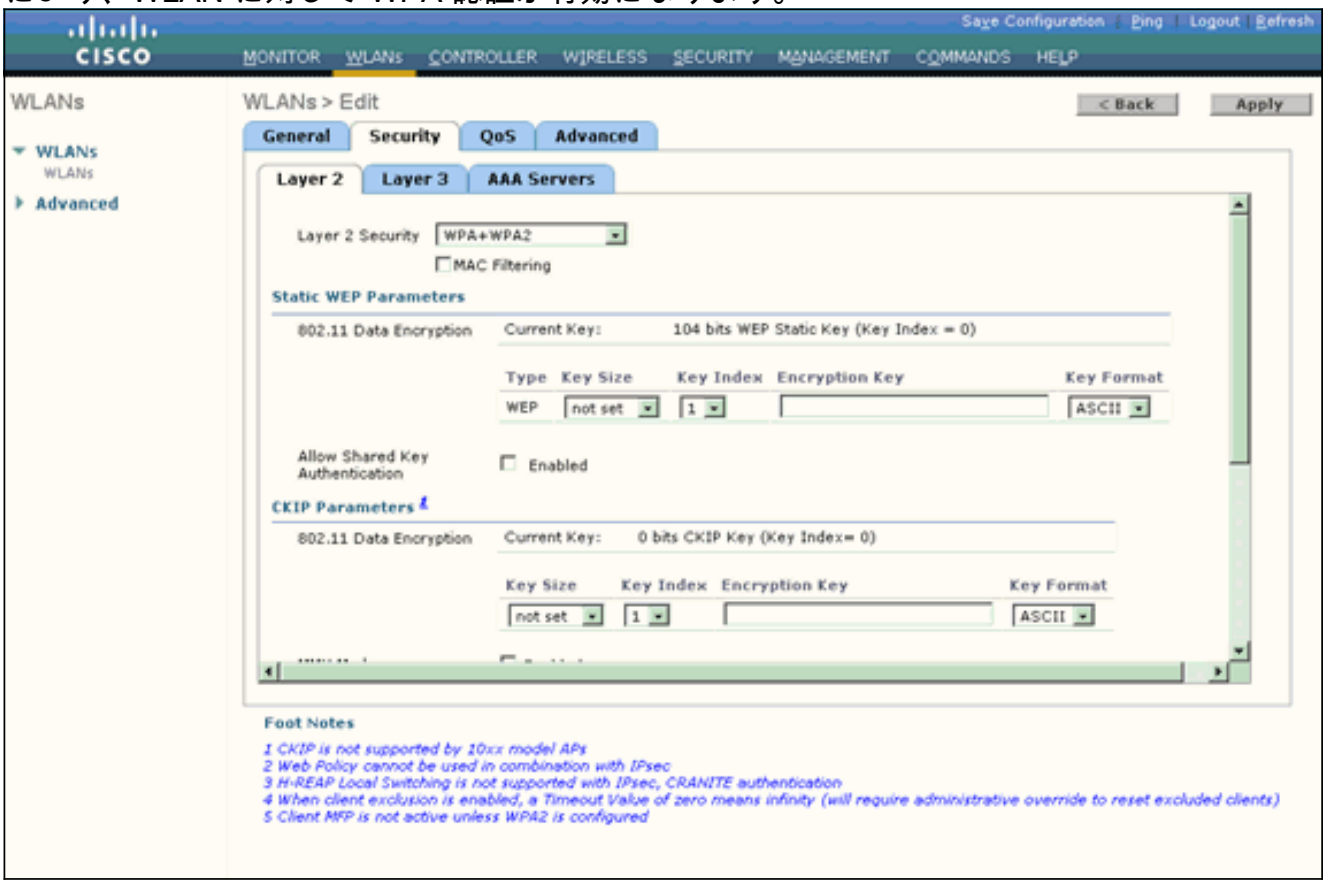
クライアントがワイヤレス ネットワークに接続するために使用する WLAN を設定する必要があります。WPA2 Personal モード用の WLAN SSID は、WPA2-Personal です。この例では、この WLAN を管理インターフェイスに割り当てます。

WLAN と関連するパラメータを設定するために、次の手順を実行します。

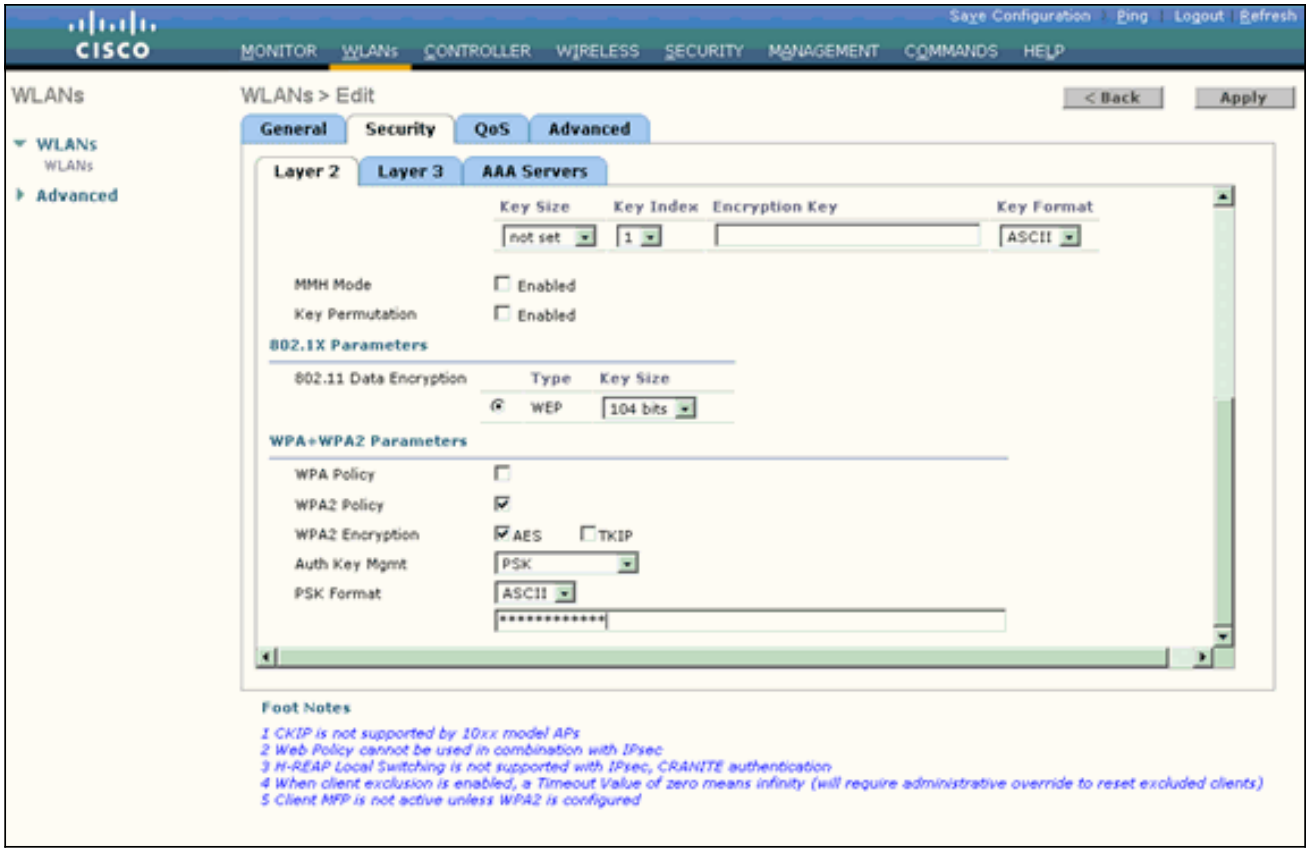
1. コントローラの GUI で [WLANs] をクリックして、[WLANs] ページを表示します。このページには、コントローラに存在する WLAN の一覧が表示されます。
2. [New] をクリックして新規の WLAN を作成します。
3. [WLANs] > [New] ページで WLAN SSID 名、プロファイル名、および WLAN ID を入力します。次に、[Apply] をクリックします。この例では、SSID として **WPA2-Personal** を使用しています。



4. 新しい WLAN を作成すると、新しい WLAN に対する [WLAN] > [Edit] ページが表示されます。このページでは、その WLAN に固有のさまざまなパラメータを定義できます。これには、全般ポリシー、セキュリティ ポリシー、QOS ポリシー、および高度なパラメータが含まれます。
5. WLAN を有効にするには、[General Policies] で [Status] チェック ボックスをオンにします。
6. AP にビーコン フレームで SSID をブロードキャストさせる場合は、[Broadcast SSID] にチェックボックスをオンにします。
7. [Security] タブをクリックします。[Layer 2 Security] で、[WPA+WPA2] を選択します。これにより、WLAN に対して WPA 認証が有効になります。



8. [WPA+WPA2 Parameters] を変更するために、ページを下にスクロールします。この例では、[WPA2 Policy] および [AES] 暗号化が選択されています。
9. [Auth Key Mgmt] で [PSK] を選択して、WPA2-PSK を有効にします。
10. 以下に示す適切なフィールドに事前共有キーを入力します。



注：WLCで使用される事前共有キーは、ワイヤレスクライアントで設定されているものと一致する必要があります。

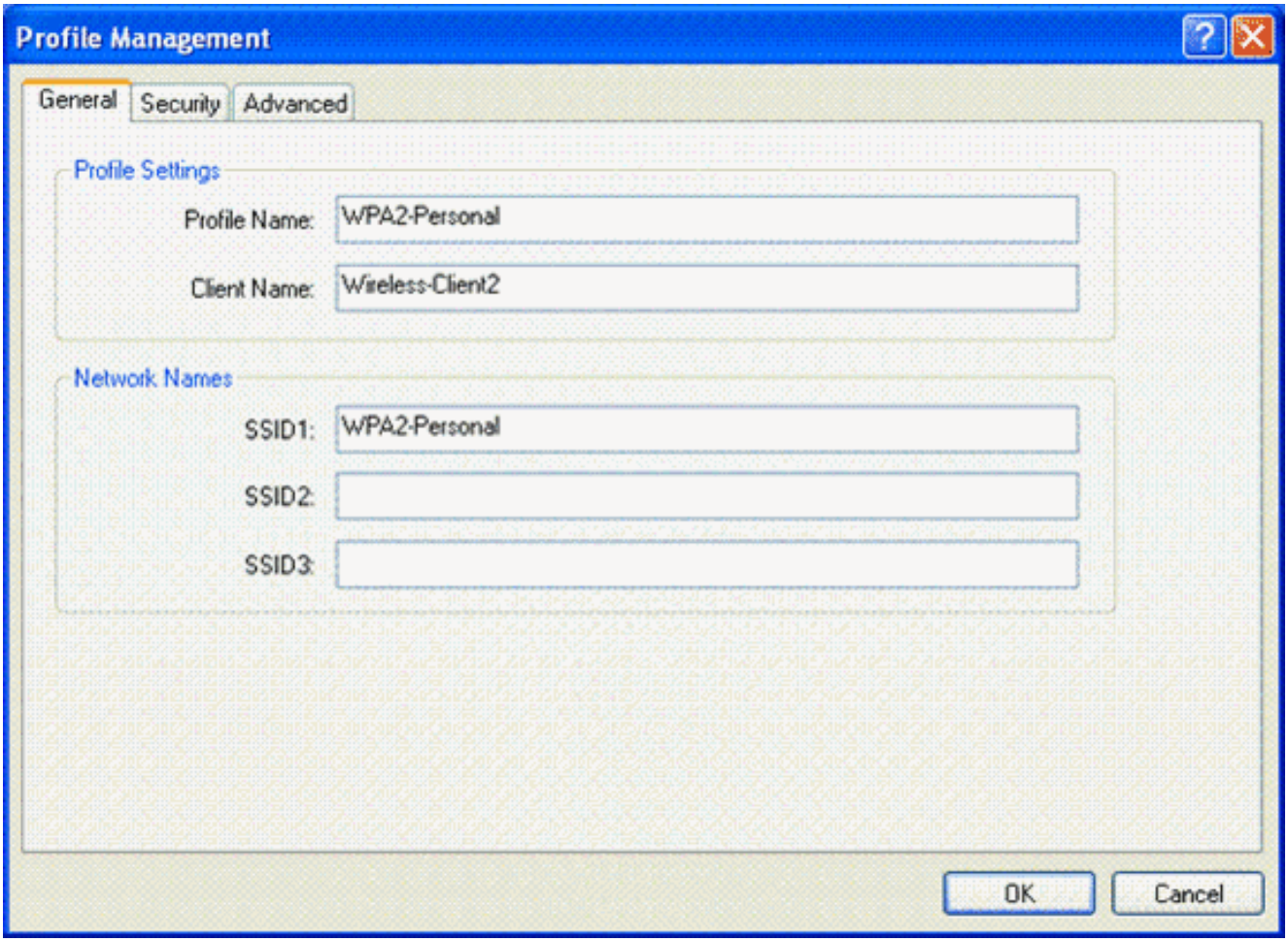
11. [Apply] をクリックします。

WPA2 Personal モード向けのワイヤレス クライアントの設定

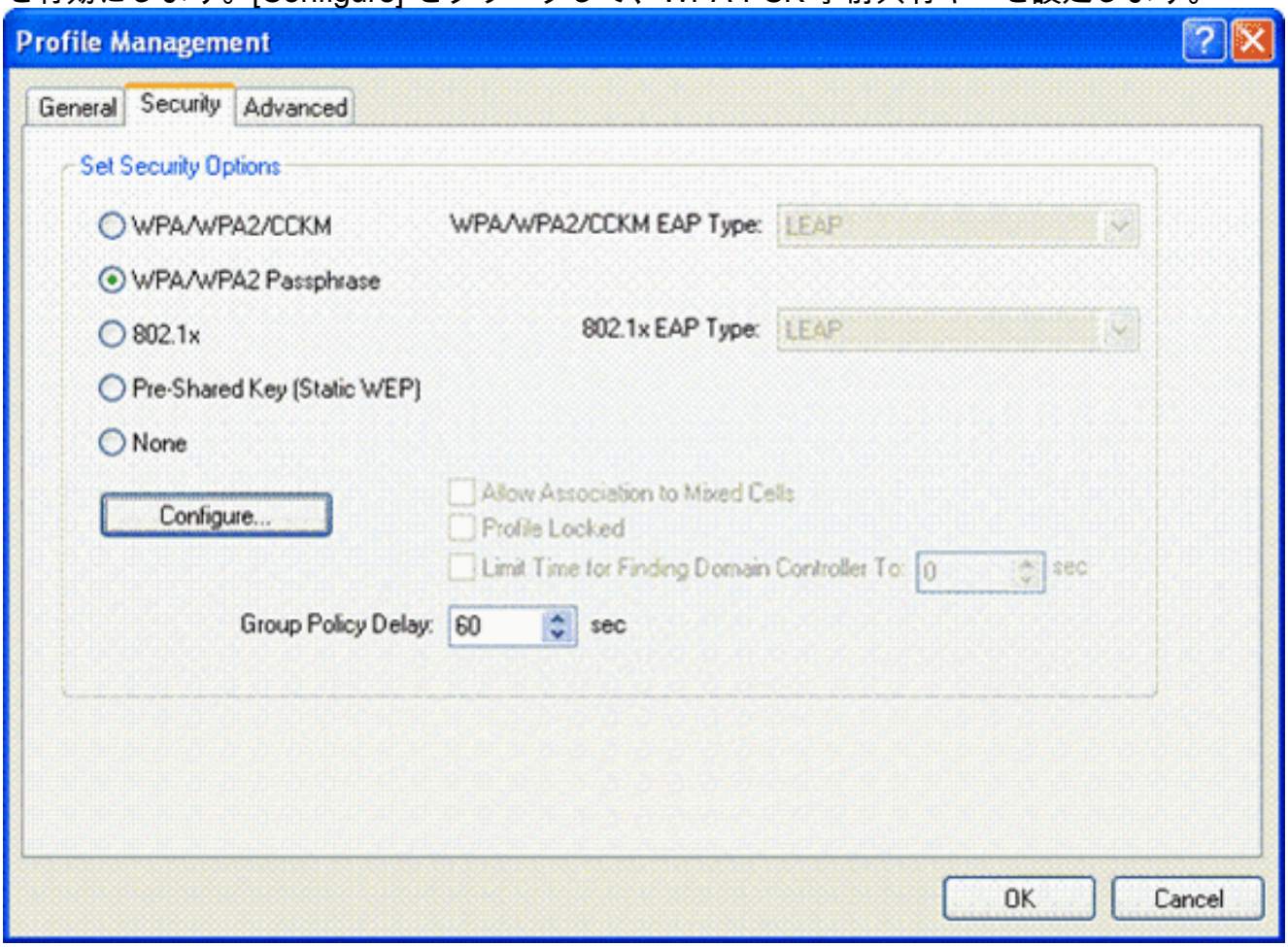
次の手順では、WPA2-Personal 動作モード用にワイヤレス クライアントを設定します。

WPA2-Personal モード用にワイヤレス クライアントを設定するには、次の手順を実行します。

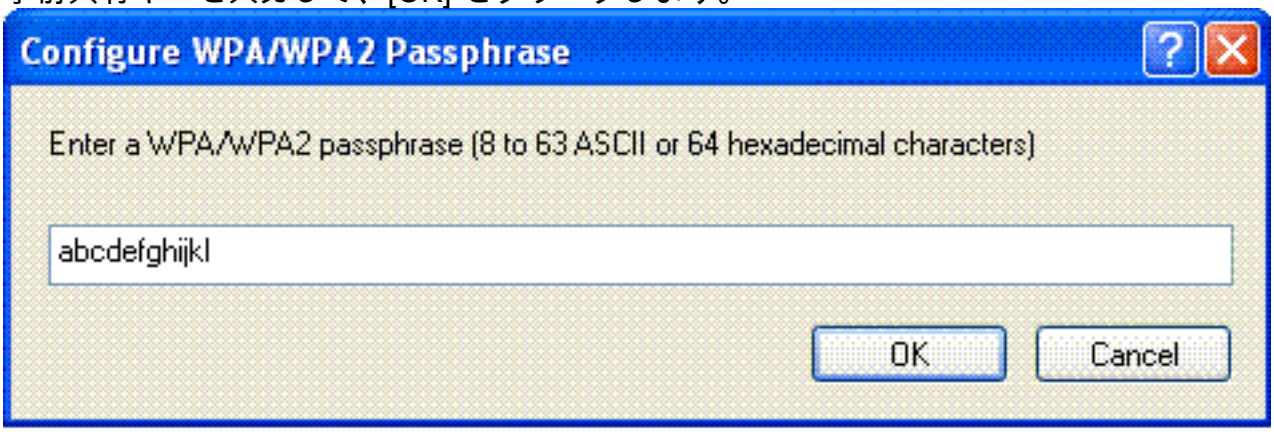
1. [Aironet Desktop Utility] ウィンドウで、[Profile Management] > [New] をクリックして、WPA2-PSK WLAN ユーザのプロファイルを作成します。
2. [Profile Management] ウィンドウの [General] タブをクリックし、この例に示すように、プロファイル名、クライアント名、および SSID 名を設定します。次に、[OK] をクリックします。



3. [Security] タブをクリックし、[WPA/WPA2 Passphrase] を選択して WPA2-PSK 動作モードを有効にします。[Configure] をクリックして、WPA-PSK 事前共有キーを設定します。



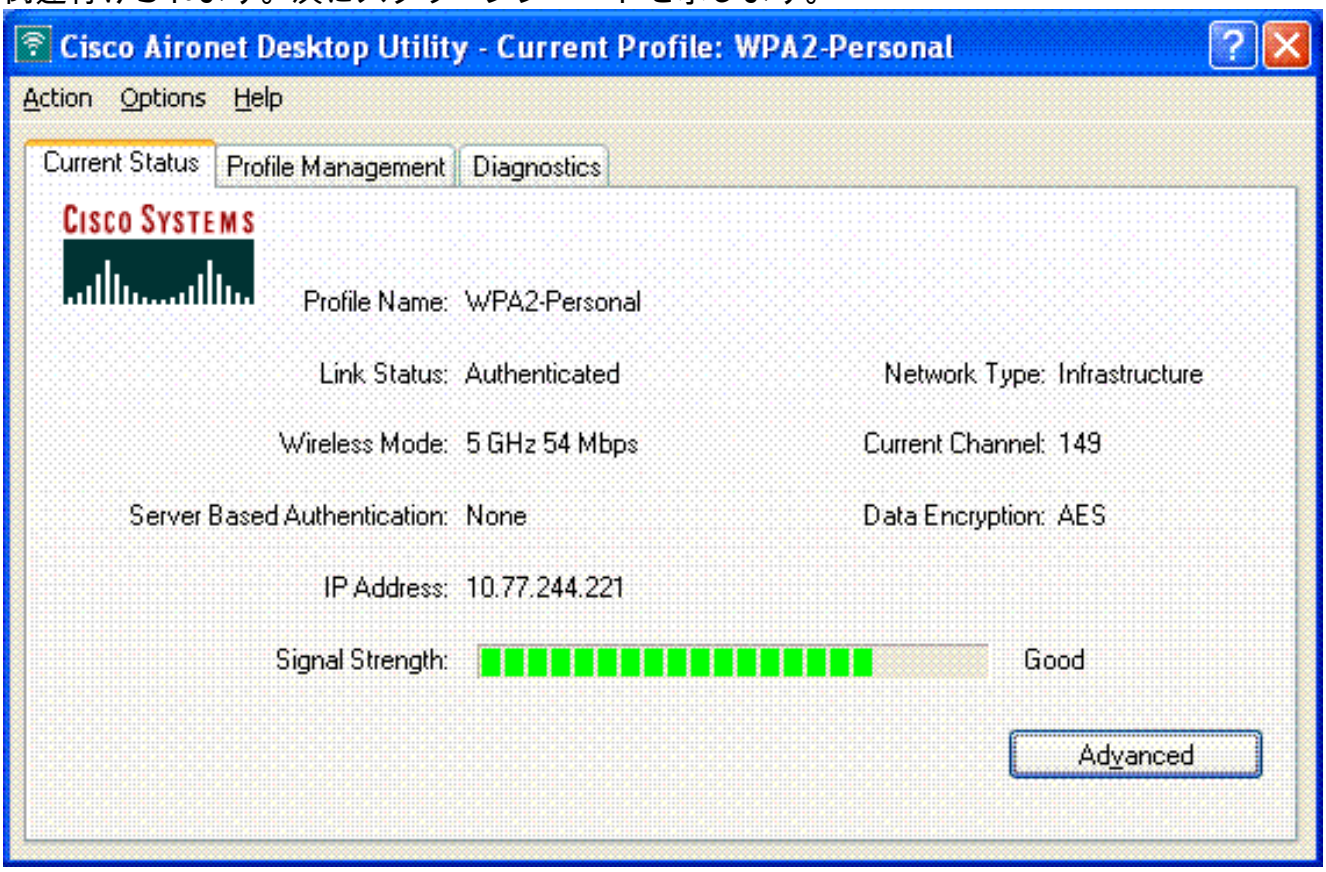
4. 事前共有キーを入力して、[OK] をクリックします。



WPA2-Personal 動作モードの確認

WPA2-Enterprise 動作モード設定が正しく機能するかどうかを確認するには、次の手順を実行します。

1. [Aironet Desktop Utility] ウィンドウで、[WPA2-Personal] プロファイルを選択して [Activate] をクリックし、ワイヤレス クライアント プロファイルをアクティブ化します。
2. プロファイルがアクティブになると、ワイヤレス クライアントは認証に成功後、WLAN に関連付けられます。次にスクリーンショットを示します。



トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

次に示す **debug** コマンドは、設定のトラブルシューティングに役立ちます。

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。

- **debug dot1x events enable**：すべての dot1x イベントのデバッグを有効にします。これは、正常な認証に基づくデバッグ出力の例です。**注：この**出力の一部の行は、スペースの制約により2行目に移動されています。

```
(Cisco Controller)>debug dot1x events enable
Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Sending EAP -Request/Identity
to mobile 00:40:96:af:3e:93 (EAP Id 1)
Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Received EAPOL START from
mobile 00:40:96:af:3e:93
Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity
to mobile 00:40:96:af:3e:93 (EAP Id 2)
Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Received EAP Response packet with
mismatching id (currentid=2, eapid=1) from mobile 00:40:96:af:3e:93
Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Received Identity Response
(count=2) from mobile 00:40:96:af:3e:93
Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Processing Access-Challenge
for mobile 00:40:96:af:3e:93
.....................................................................
.....................................................................
.....................................................................
.....................................................................

Wed Feb 20 14:20:00 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 19, EAP Type 43)
Wed Feb 20 14:20:00 2007: 00:40:96:af:3e:93 Processing Access-Challenge
for mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:00 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA
to mobile 00:40:96:af:3e:93 (EAP Id 20)
Wed Feb 20 14:20:01 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 20, EAP Type 43)
Wed Feb 20 14:20:29 2007: Creating dot1x interface with key 00:0b:85:91:c3:c0 -0
Wed Feb 20 14:20:29 2007: Resetting the group key timer for 3689 seconds on
AP 00:0b:85:91:c3:c0
Wed Feb 20 14:20:29 2007: Creating dot1x interface with key 00:0b:85:91:c3:c0 -1
Wed Feb 20 14:20:29 2007: Resetting the group key timer for 3696 seconds on
AP 00:0b:85:91:c3:c0
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received EAPOL START from
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to
mobile 00:40:96:af:3e:93 (EAP Id 22)
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received Identity Response (count=3)
from mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Processing Access-Challenge for
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 WARNING: updated EAP-Identifer 22 ===>
19 for STA 00:40:96:af:3e:93
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to
mobile 00:40:96:af:3e:93 (EAP Id 19)
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 19, EAP Type 3)
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Processing Access-Challenge for
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to
mobile 00:40:96:af:3e:93 (EAP Id 20)
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 20, EAP Type 43)
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Processing Access-Challenge for
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to
mobile 00:40:96:af:3e:93 (EAP Id 21)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from
```

```
mobile 00:40:96:af:3e:93 (EAP Id 21, EAP Type 43)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to
mobile 00:40:96:af:3e:93 (EAP Id 22)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 22, EAP Type 43)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to
mobile 00:40:96:af:3e:93 (EAP Id 23)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 23, EAP Type 43)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to
mobile 00:40:96:af:3e:93 (EAP Id 24)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 24, EAP Type 43)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to
mobile 00:40:96:af:3e:93 (EAP Id 25)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 25, EAP Type 43)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to
mobile 00:40:96:af:3e:93 (EAP Id 26)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 26, EAP Type 43)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to
mobile 00:40:96:af:3e:93 (EAP Id 27)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 27, EAP Type 43)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Reject for
mobile00:40:96:af:3e:93
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Failure to
mobile 00:4096:af:3e:93 (EAP Id 27)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Setting quiet timer for 5 seconds
for mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to
mobile 00:40:96:af:3e:93 (EAP Id 1)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to
mobile 00:40:96:af:3e:93 (EAP Id 1)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAPOL START from
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to
mobile 00:40:96:af:3e:93 (EAP Id 2)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received Identity Response (count=2)
from mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 WARNING: updated EAP-Identifer 2 ===>
20 for STA 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to
mobile 00:40:96:af:3e:93 (EAP Id 20)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 20, EAP Type 3)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to
```

```
mobile 00:40:96:af:3e:93 (EAP Id 21)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 21, EAP Type 43)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to
mobile 00:40:96:af:3e:93 (EAP Id 22)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 22, EAP Type 43)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 WARNING: updated EAP-Identifer 22 ===>
24 for STA 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to
mobile 00:40:96:af:3e:93 (EAP Id 24)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 24, EAP Type 43)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge
for mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA
to mobile 00:40:96:af:3e:93 (EAP Id 25)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 25, EAP Type 43)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Accept for
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Creating a new PMK Cache Entry for
tation 00:40:96:af:3e:93 (RSN 0)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP-Success to
mobile 00:40:96:af:3e:93 (EAP Id 25)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending default RC4 key to
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending Key-Mapping RC4 key to
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received Auth Success while in
Authenticating state for mobile 00:40:96:af:3e:93
```

- **debug dot1x packet enable**：802.1x パケット メッセージのデバッグを有効にします。
- **debug aaa events enable**：すべての aaa イベントのデバッグ出力を有効にします。

関連情報

- WPA2 - Wi-Fi Protected Access 2
- ワイヤレス LAN コントローラおよび外部 RADIUS サーバを使用する EAP-FAST 認証の設定例
- EAP 認証と WLAN コントローラ (WLC) の設定例
- WPA 設定の概要
- ワイヤレス製品に関するサポート
- テクニカル サポートとドキュメント – Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。