固定 ISR でのワイヤレス認証タイプの設定

内容

はじめに

このドキュメントでは、CLI コマンドを使用してワイヤレス接続用のシスコ ワイヤレス統合型固定構成ルータのさまざまなレイヤ 2 認証タイプを設定する方法について説明する設定例を示します。

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。

- シスコ サービス統合型ルータ（ISR）の基本パラメータを設定する方法についての知識。
- Aironet Desktop Utility（ADU）を使用して 802.11a/b/g 無線クライアント アダプタを設定する方法についての知識。

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いています。

- Cisco IOS® ソフトウェア リリース 12.3(8)YI1 が稼働する Cisco 877W ISR
- Aironet Desktop Utility バージョン 3.6 がインストールされているラップトップ PC
- ファームウェア バージョン 3.6 が稼働する 802.11 a/b/g クライアント アダプタ

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、クリアな（デフォルト）設定で作業を開始しています。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。

背景説明

シスコのサービス統合型固定構成ルータは、モビリティと柔軟性をネットワーク技術者が必要とするエンタープライズクラスの機能と組み合わせた、セキュアかつ安価で使いやすいワイヤレス LAN ソリューションをサポートします。Cisco IOS ソフトウェアをベースとした管理システムにより、Cisco ルータはアクセス ポイントとして機能し、Wi-Fi 認定を受けた、IEEE 802.11a/b/g 準拠のワイヤレス LAN トランシーバとなります。

これらのルータは、コマンドライン インターフェイス（CLI）、ブラウザベースの管理システム、または簡易ネットワーク管理プロトコル（SNMP）を使用して設定およびモニタできます。こ

のドキュメントでは、CLI コマンドを使用してワイヤレス接続のために ISR を設定する方法について説明します。

設定

この例では、CLI コマンドを使用してシスコ ワイヤレス統合型固定構成ルータで次の認証タイプを設定する方法を示します。

- オープン認証
- 802.1x/EAP（拡張認証プロトコル）認証
- Wi-Fi Protected Access Pre-Shared Key（WPA-PSK）認証
- WPA（EAP を使用した）認証

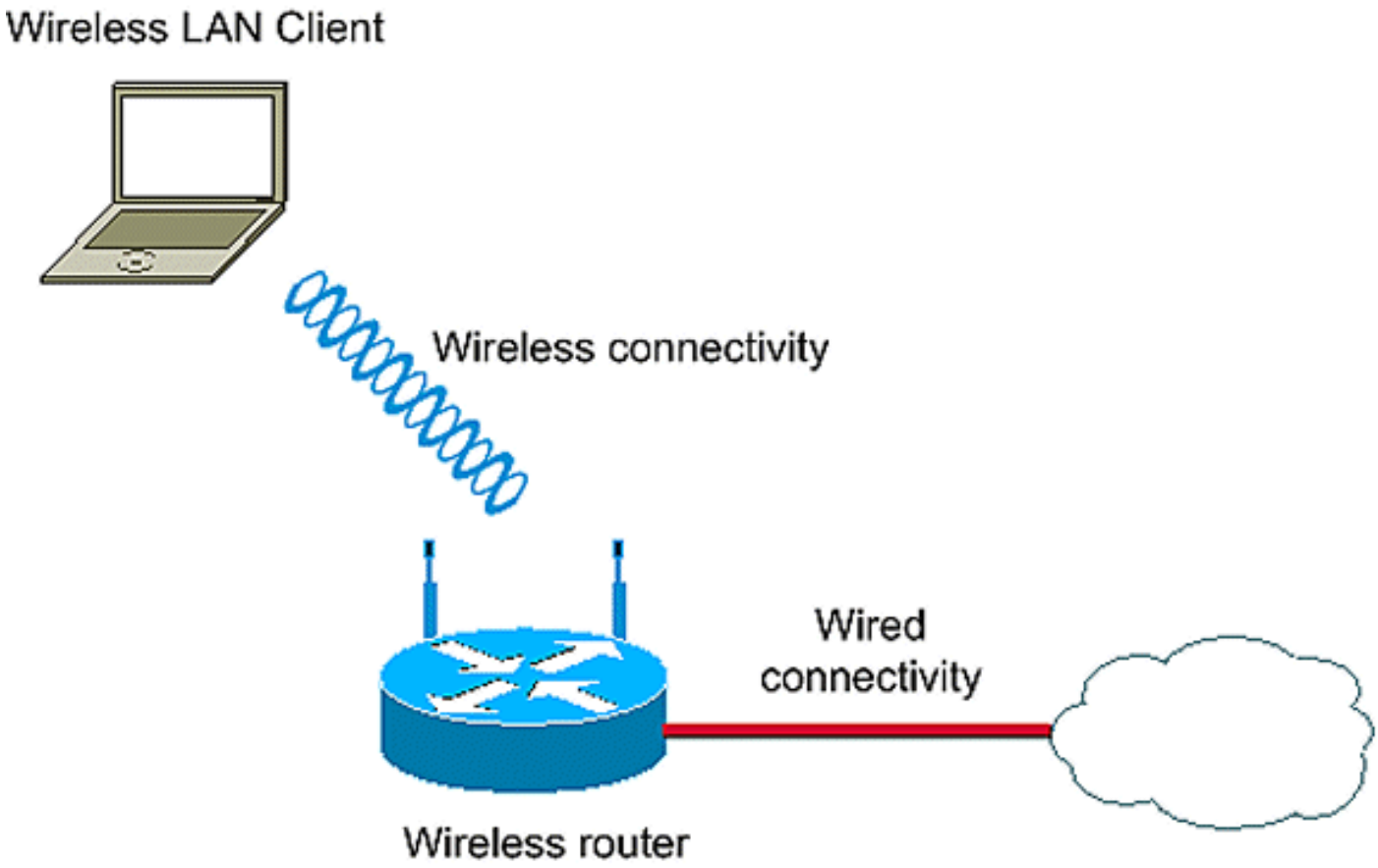
注：このドキュメントでは、安全性の低い認証タイプであるため、共有認証については詳しく説明しません。

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。

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）を参照してください。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことをご了承ください。

ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。



この設定は、802.1x 認証を使用してワイヤレス クライアントを認証するためにワイヤレス ISR でローカル RADIUS サーバを使用します。

オープン認証の設定

オープン認証は、ヌル認証アルゴリズムです。アクセス ポイントは、あらゆる認証の要求を認可します。オープン認証は、あらゆるデバイスのネットワーク アクセスを可能にします。ネットワークで暗号化がイネーブルになっていない場合、アクセス ポイントの SSID を知っているあらゆるデバイスが、このネットワークにアクセスできます。アクセス ポイントで WEP 暗号化がイネーブルになっている場合、WEP キー自体がアクセス コントロールの手段となります。デバイスが正しい WEP キーを持っていない場合、認証が成功した場合でもデバイスはアクセス ポイント経由でデータを送信できません。また、アクセス ポイントから送信されるデータの復号化も不可能です。

この設定例では、簡単なオープン認証のみについて説明します。WEP キーは、必須または任意にすることができます。この例では、WEP を使用しないあらゆるデバイスがこの AP で認証されて関連付けられるように、WEP キーを任意として設定します。

詳細については、「オープン認証」を参照してください。

この例では、ISR のオープン認証を設定するために、次の設定セットアップを使用します。

- SSID名：open
- VLAN 1

- 内部DHCPサーバの範囲：10.1.0.0/16

注：わかりやすくするために、この例では認証されたクライアントに対して暗号化テクニックを使用していません。

ルータで次の操作を行います。

1. Integrated Routing and Bridging（IRB）の設定とブリッジ グループのセットアップ
2. Bridged Virtual Interface（BVI）の設定
3. オープン認証の SSID の設定
4. VLAN のワイヤレス クライアントの内部 DHCP サーバの設定

Integrated Routing and Bridging（IRB）の設定とブリッジ グループのセットアップ

次の操作を行います。

1. ルータで IRB をイネーブルにします。

   router<configure>#bridge irb

   注：すべてのセキュリティタイプを1台のルータで設定する場合、ルータでIRBを一度だけグローバルに有効にすれば十分です。個々の認証タイプに対してイネーブルにする必要はありません。

2. ブリッジ グループを定義します。

   この例では、ブリッジ グループ番号 1 を使用しています。

   router<configure>#bridge 1

3. ブリッジ グループのスパニング ツリー プロトコルを選択します。

   ここでは、IEEE スパニング ツリー プロトコルが、このブリッジ グループに設定されます。

   router<configure>#bridge 1 protocol ieee

4. BVI を有効にして、対応するブリッジ グループから受信したルーティング可能なパケットを受け入れ、ルーティングします。

   この例では、IP パケットを受け入れ、パスを指定するように BVI を有効にします。

   router<configure>#bridge 1 route ip

Bridged Virtual Interface（BVI）の設定

次の操作を行います。

1. BVI を設定します。

   BVI にブリッジ グループの対応する番号を割り当てるときの BVI を設定します。各ブリッジ グループは、1 つの対応する BVI のみを持てます。次の例では、ブリッジ グループ番号 1 を BVI に割り当てています。

   router<configure>#interface BVI <1>

2. BVI に IP アドレスを割り当てます。

   router<config-if>#ip address 10.1.1.1 255.255.0.0

   router<config-if>#no shut

ブリッジングについての詳細は、『ブリッジングの設定』を参照してください。

オープン認証の SSID の設定

次の操作を行います。

1. 無線インターフェイスをイネーブルにします。

   無線インターフェイスをイネーブルにするには、DOT11 無線インターフェイスのコンフィギュレーション モードに進み、SSID をインターフェイスに割り当てます。

   router<config>#interface dot11radio0

   router<config-if>#no shutdown

   router<config-if>#ssid open

   オープン認証のタイプは、MAC アドレスの認証と組み合わせて設定できます。この場合、アクセス ポイントは、すべてのクライアント デバイスに対して、ネットワーク接続を許可される前に MAC アドレス認証の実行を強制します。

   オープン認証は、EAP 認証とともに設定できます。アクセス ポイントは、すべてのクライアント デバイスに対して、ネットワーク接続を許可される前に EAP 認証の実行を強制します。list-name には、認証方式リストを指定します。

   EAP 認証が設定されたアクセス ポイントは、アソシエートするすべてのクライアント デバイスに対して EAP 認証の実行を強制します。EAP を使用しないクライアント デバイスはアクセス ポイントを使用できません。

2. SSID を VLAN にバインドします。

   このインターフェイスで SSID をイネーブルにするには、SSID コンフィギュレーション モードで VLAN に SSID をバインドします。

   router<config-ssid>vlan 1

3. オープン認証を使用した SSID を設定します。

router<config-ssid>#authentication open

4. 任意選択 WEP キーの無線インターフェイスを設定します。

   router<config>#encryption vlan 1 mode WEP optional

5. 無線インターフェイスで VLAN を有効にします。

   router<config>#interface Dot11Radio 0.1

   router<config-subif>#encapsulation dot1Q 1

   router<config-subif>#bridge-group 1

VLAN のワイヤレス クライアントの内部 DHCP サーバの設定

この VLAN のワイヤレス クライアントの内部 DHCP サーバを設定するには、グローバル コンフィギュレーション モードで次のコマンドを入力してください。

- ip dhcp excluded-address 10.1.1.1 10.1.1.5
- ip dhcp pool open

DHCP プール設定モードで、次のコマンドを入力してください。

- network 10.1.0.0 255.255.0.0
- default-router 10.1.1.1

802.1x/EAP 認証の設定

この認証タイプは、無線ネットワークに最高レベルのセキュリティを提供します。拡張認証プロトコル（EAP）を使用して EAP 互換の RADIUS サーバと対話することにより、アクセス ポイントは、無線クライアント デバイスと RADIUS サーバが相互認証を行って動的なユニキャスト WEP キーを引き出す補助をします。RADIUS サーバはアクセス ポイントに WEP キーを送ります。アクセス ポイントはこのキーを、クライアントに対して送受信するすべてのユニキャスト データ信号に使用します。

詳細は、「EAP 認証」を参照してください。

この例では、次の設定セットアップを使用しています。

- SSID名：leap
- VLAN 2
- 内部DHCPサーバの範囲：10.2.0.0/16

この例では、ワイヤレス クライアントを認証するメカニズムとして LEAP 認証を使用します。

注：EAP-TLSを設定するには、『EAP-TLSマシン認証が設定されたCisco Secure ACS for Windows v3.2』を参照してください。

注：PEAP-MS-CHAPv2を設定するには、『PEAP-MS-CHAPv2マシン認証が設定されたCisco Secure ACS for Windows v3.2』を参照してください。

注：これらのEAPタイプのすべての設定は、主にクライアント側と認証サーバ側の設定変更に関係することを理解してください。ワイヤレス ルータまたはアクセス ポイントの設定は多かれ少なかれ、これらの認証タイプと同じです。

注：最初に説明したように、このセットアップでは、ワイヤレスISR上のローカルRADIUSサーバを使用して、ワイヤレスクライアントを802.1x認証で認証します。

ルータで次の操作を行います。

1. Integrated Routing and Bridging（IRB）の設定とブリッジ グループのセットアップ
2. Bridged Virtual Interface（BVI）の設定
3. EAP 認証のためのローカル RADIUS サーバの設定
4. 802.1x/EAP 認証の SSID の設定
5. VLAN のワイヤレス クライアントの内部 DHCP サーバの設定

Integrated Routing and Bridging（IRB）の設定とブリッジ グループのセットアップ

次の操作を行います。

1. ルータで IRB をイネーブルにします。

   router<configure>#bridge irb

   注：すべてのセキュリティタイプを1台のルータで設定する場合、ルータでIRBを一度だけグローバルに有効にすれば十分です。個々の認証タイプに対してイネーブルにする必要はありません。

2. ブリッジ グループを定義します。

   この例では、ブリッジ グループ番号 2 を使用しています。

   router<configure>#bridge 2

3. ブリッジ グループのスパニング ツリー プロトコルを選択します。

   ここでは、IEEE スパニング ツリー プロトコルが、このブリッジ グループに設定されます。

   router<configure>#bridge 2 protocol ieee

4. ブリッジ グループのスパニング ツリー プロトコルを選択します。

ここでは、IEEE スパニング ツリー プロトコルが、このブリッジ グループに設定されます。

router<configure>#bridge 2 protocol ieee

5. BVI を有効にして、対応するブリッジ グループから受信したルーティング可能なパケットを受け入れ、ルーティングします。

この例では、IP パケットを受け入れ、パスを指定するように BVI を有効にします。

router<configure>#bridge 2 route ip

Bridged Virtual Interface（BVI）の設定

次の操作を行います。

1. BVI を設定します。

BVI にブリッジ グループの対応する番号を割り当てるときの BVI を設定します。各ブリッジ グループは、1 つの対応する BVI のみを持てます。次の例では、ブリッジ グループ番号 2 を BVI に割り当てています。

router<configure>#interface BVI <2>

2. BVI に IP アドレスを割り当てます。

router<config-if>#ip address 10.2.1.1 255.255.0.0

router<config-if>#no shut

EAP 認証のためのローカル RADIUS サーバの設定

上記のように、このドキュメントでは EAP の認証にワイヤレス認識ルータのローカル RADIUS サーバを使用します。

1. 認証、許可、アカウンティング（AAA）アクセス コントロール モデルをイネーブルにします。

router<configure>#aaa new-model

2. RADIUS サーバの rad eap サーバ グループを作成します。

router<configure>#aaa group server radius rad-eap server 10.2.1.1 auth-port 1812 acct-port 1813

3. AAA ログイン ユーザの認証に使用する認証方式をリストする、認証方式リスト eap_methods を作成します。このサーバ グループに認証方式リストを割り当てます。

router<configure>#aaa authentication login eap_methods group rad-eap

4. ルータをローカル認証サーバとしてイネーブルにし、オーセンティケータのコンフィギュレーション モードを開始します。

   router<configure>#radius-server local

5. RADIUS サーバの設定モードで、ローカル認証サーバの AAA クライアントとしてルータを追加します。

   router<config-radsrv>#nas 10.2.1.1 key Cisco

6. ローカル RADIUS サーバで、ユーザ user1 を設定します。

   router<config-radsrv>#user user1 password user1 group rad-eap

7. RADIUS サーバ ホストを指定します。

   router<config-radsrv>#radius-server host 10.2.1.1 auth-port 1812 acct-port 1813 key cisco

   注：このキーは、radius-server設定モードのnasコマンドで指定されたキーと同じである必要があります。

802.1x/EAP 認証の SSID の設定

802.1x/EAP の無線インターフェイスと関連 SSID の設定には、SSID、暗号化モード、認証タイプを含むルータのさまざまな無線パラメータの設定が含まれます。この例では、leap という名前の SSID を使用します。

1. 無線インターフェイスをイネーブルにします。

   無線インターフェイスをイネーブルにするには、DOT11 無線インターフェイスのコンフィギュレーション モードに進み、SSID をインターフェイスに割り当てます。

   router<config>#interface dot11radio0

   router<config-if>#no shutdown

   router<config-if>#ssid leap

2. SSID を VLAN にバインドします。

   このインターフェイスで SSID をイネーブルにするには、SSID コンフィギュレーション モードで VLAN に SSID をバインドします。

   router<config-ssid>#vlan 2

3. 802.1x/EAP 認証を使用した SSID の設定

   router<config-ssid>#authentication network-eap eap_methods

4. ダイナミック キー管理の無線インターフェイスを設定します。

router<config>#encryption vlan 2 mode ciphers wep40

5. 無線インターフェイスで VLAN を有効にします。

   router<config>#interface Dot11Radio 0.2

   router<config-subif>#encapsulation dot1Q 2

   router<config-subif>#bridge-group 2

VLAN のワイヤレス クライアントの内部 DHCP サーバの設定

この VLAN のワイヤレス クライアントの内部 DHCP サーバを設定するには、グローバル コンフィギュレーション モードで次のコマンドを入力してください。

- ip dhcp excluded-address 10.2.1.1 10.2.1.5
- ip dhcp pool leapauth

DHCP プール設定モードで、次のコマンドを入力してください。

- network 10.2.0.0 255.255.0.0
- default-router 10.2.1.1

WPA キー管理

Wi-Fi Protected Access（WPA）は、現在および将来の無線 LAN システムのデータ保護とアクセス コントロールの水準を大幅に向上させる、標準規格に基づく相互運用性のあるセキュリティ拡張です。

詳細は、「WPA キー管理」を参照してください。

WPAキー管理では、WPA-Pre-Shared Key(WPA-PSK)とWPA（EAPを使用）の2つの相互排他的な管理タイプがサポートされています。

WPA-PSK の設定

WPA-PSK は、802.1x ベース認証を使用できない無線 LAN のキー管理タイプとして使用されます。このようなネットワークでは、アクセス ポイントで事前共有キーを設定します。事前共有キーを ASCII 文字または 16 進数として入力できます。キーを ASCII 文字として入力する場合は、8 ~ 63 文字を入力します。アクセス ポイントはこのキーを、『Password-based Cryptography Standard（RFC2898）』に記載されているプロセスを使用して展開します。キーを 16 進数として入力する場合は、64 桁の 16 進数を入力する必要があります。

この例では、次の設定セットアップを使用しています。

- SSID名：wpa-shared

- VLAN 3
- 内部DHCPサーバの範囲：10.3.0.0/16

ルータで次の操作を行います。

1. Integrated Routing and Bridging（IRB）の設定とブリッジ グループのセットアップ
2. Bridged Virtual Interface（BVI）の設定
3. WPA-PSK 認証の SSID の設定
4. VLAN のワイヤレス クライアントの内部 DHCP サーバの設定

Integrated Routing and Bridging（IRB）の設定とブリッジ グループのセットアップ

次の操作を行います。

1. ルータで IRB をイネーブルにします。

   router<configure>#bridge irb

   注：すべてのセキュリティタイプを1台のルータで設定する場合、ルータでIRBを一度だけグローバルに有効にすれば十分です。個々の認証タイプに対してイネーブルにする必要はありません。

2. ブリッジ グループを定義します。

   この例では、ブリッジ グループ番号 3 を使用しています。

   router<configure>#bridge 3

3. ブリッジ グループのスパニング ツリー プロトコルを選択します。

   IEEE スパニング ツリー プロトコルが、このブリッジ グループに設定されます。

   router<configure>#bridge 3 protocol ieee

4. BVI を有効にして、対応するブリッジ グループから受信したルーティング可能なパケットを受け入れ、ルーティングします。

   この例では、IP パケットを受け入れ、パスを指定するように BVI を有効にします。

   router<configure>#bridge 3 route ip

Bridged Virtual Interface（BVI）の設定

次の操作を行います。

1. BVI を設定します。

BVI にブリッジ グループの対応する番号を割り当てるときの BVI を設定します。各ブリッジ グループは、1 つの対応する BVI のみを持てます。次の例では、ブリッジ グループ番号 3 を BVI に割り当てています。

router<configure>#interface BVI <2>

2. BVI に IP アドレスを割り当てます。

router<config-if>#ip address 10.3.1.1 255.255.0.0

router<config-if>#no shut

WPA-PSK 認証の SSID の設定

次の操作を行います。

1. 無線インターフェイスをイネーブルにします。

無線インターフェイスをイネーブルにするには、DOT11 無線インターフェイスのコンフィギュレーション モードに進み、SSID をインターフェイスに割り当てます。

router<config>#interface dot11radio0

router<config-if>#no shutdown

router<config-if>#ssid wpa-shared

2. WPA キー管理を有効にするには、まず VLAN インターフェイスに対して WPA 暗号キーを設定します。この例では、暗号キーとして tkip を使用しています。

無線インターフェイスで WPA キー管理タイプを指定するには、次のコマンドを入力します。

router<config>#interface dot11radio0

router(config-if)#encryption vlan 3 mode ciphers tkip

3. SSID を VLAN にバインドします。

このインターフェイスで SSID をイネーブルにするには、SSID コンフィギュレーション モードで VLAN に SSID をバインドします。

router<config-ssid>vlan 3

4. WPA-PSK 認証を使用して SSID を設定します。

WPA キー管理を有効にするには、まず SSID コンフィギュレーション モードでオープンまたはネットワーク EAP 認証を設定する必要があります。この例では、オープン認証を設定します。

router<config>#interface dot11radio0

router<config-if>#ssid wpa-shared

router<config-ssid>#authentication open

ここで、SSID で WPA キー管理をイネーブルにします。キー管理の暗号の tkip は、この VLAN ではすでに設定されています。

router(config-if-ssid)#authentication key-management wpa

SSID で WPA-PSK 認証を設定します。

router(config-if-ssid)#wpa-psk ascii 1234567890 !— 1234567890は、このSSIDの事前共有キー(PSK)の値です。同じキーが、クライアント側でこの SSID に指定されていることを確認します。

5. 無線インターフェイスで VLAN を有効にします。

   router<config>#interface Dot11Radio 0.3

   router<config-subif>#encapsulation dot1Q 3

   router<config-subif>#bridge-group 3

VLAN のワイヤレス クライアントの内部 DHCP サーバの設定

この VLAN のワイヤレス クライアントの内部 DHCP サーバを設定するには、グローバル コンフィギュレーション モードで次のコマンドを入力してください。

- ip dhcp excluded-address 10.3.1.1 10.3.1.5
- ip dhcp pool wpa-psk

DHCP プール設定モードで、次のコマンドを入力してください。

- network 10.3.0.0 255.255.0.0
- default-router 10.3.1.1

WPA (EAP を使用した) 認証の設定

これは別の WPA キー管理タイプです。ここでは、クライアントと認証サーバは、EAP 認証方式で相互認証を行い、Pairwise Master Key (PMK) を生成します。WPA を使用すると、サーバは PMK を動的に生成し、アクセス ポイントに渡します、ただし、WPA-PSK を使用すると、クライアントとアクセス ポイントの両方の事前共有キーを設定し、その事前共有キーは PMK として使用されます。

詳細は、「WPA (EAP を使用した) 認証」を参照してください。

この例では、次の設定セットアップを使用しています。

- SSID名：wpa-dot1x
- VLAN 4
- 内部DHCPサーバの範囲：10.4.0.0/16

ルータで次の操作を行います。

1. Integrated Routing and Bridging（IRB）の設定とブリッジ グループのセットアップ
2. Bridged Virtual Interface（BVI）の設定
3. WPA 認証のためのローカル RADIUS サーバの設定
4. EAP 認証を使用した WPA の SSID の設定
5. VLAN のワイヤレス クライアントの内部 DHCP サーバの設定

Integrated Routing and Bridging（IRB）の設定とブリッジ グループのセットアップ

次の操作を行います。

1. ルータで IRB をイネーブルにします。

   router<configure>#bridge irb

   注：すべてのセキュリティタイプを1台のルータで設定する場合、ルータでIRBを一度だけグローバルに有効にすれば十分です。個々の認証タイプに対してイネーブルにする必要はありません。

2. ブリッジ グループを定義します。

   この例では、ブリッジ グループ番号 4 を使用しています。

   router<configure>#bridge 4

3. ブリッジ グループのスパニング ツリー プロトコルを選択します。

   ここでは、IEEE スパニング ツリー プロトコルが、このブリッジ グループに設定されます。

   router<configure>#bridge 4 protocol ieee

4. BVI を有効にして、対応するブリッジ グループから受信したルーティング可能なパケットを受け入れ、ルーティングします。

   この例では、IP パケットを受け入れ、パスを指定するように BVI を有効にします。

   router<configure>#bridge 4 route ip

Bridged Virtual Interface（BVI）の設定

次の操作を行います。

1. BVI を設定します。

   BVI にブリッジ グループの対応する番号を割り当てるときの BVI を設定します。各ブリッジ グループは、1 つの対応する BVI のみを持てます。次の例では、ブリッジ グループ番号 4 を BVI に割り当てています。

   router<configure>#interface BVI <4>

2. BVI に IP アドレスを割り当てます。

   router<config-if>#ip address 10.4.1.1 255.255.0.0

   router<config-if>#no shut

WPA 認証のためのローカル RADIUS サーバの設定

詳細な手順については、「802.1x/EAP 認証」の下の項を参照してください。

EAP 認証を使用した WPA の SSID の設定

次の操作を行います。

1. 無線インターフェイスをイネーブルにします。

   無線インターフェイスをイネーブルにするには、DOT11 無線インターフェイスのコンフィギュレーション モードに進み、SSID をインターフェイスに割り当てます。

   router<config>#interface dot11radio0

   router<config-if>#no shutdown

   router<config-if>#ssid wpa-dot1x

2. WPA キー管理を有効にするには、まず VLAN インターフェイスに対して WPA 暗号キーを設定します。この例では、暗号キーとして tkip を使用しています。

   無線インターフェイスで WPA キー管理タイプを指定するには、次のコマンドを入力します。

   router<config>#interface dot11radio0

   router(config-if)#encryption vlan 4 mode ciphers tkip

3. SSID を VLAN にバインドします。

   このインターフェイスで SSID をイネーブルにするには、SSID コンフィギュレーション モードで VLAN に SSID をバインドします。

   vlan 4

4. WPA-PSK 認証を使用して SSID を設定します。

   EAP 認証を使用した WPA の無線インターフェイスを設定するには、まずネットワーク EAP の関連 SSID を設定します。

   router<config>#interface dot11radio0

   router<config-if>#ssid wpa-shared

   router<config-ssid>#authentication network eap eap_methods

5. ここで、SSID で WPA キー管理をイネーブルにします。キー管理の暗号の tkip は、この VLAN ではすでに設定されています。

   router(config-if-ssid)#authentication key-management wpa

6. 無線インターフェイスで VLAN を有効にします。

   router<config>#interface Dot11Radio 0.4

   router<config-subif>#encapsulation dot1Q 4

   router<config-subif>#bridge-group 4

VLAN のワイヤレス クライアントの内部 DHCP サーバの設定

この VLAN のワイヤレス クライアントの内部 DHCP サーバを設定するには、グローバル コンフィギュレーション モードで次のコマンドを入力してください。

- ip dhcp excluded-address 10.4.1.1 10.4.1.5
- ip dhcp pool wpa-dot1shared

DHCP プール設定モードで、次のコマンドを入力してください。

- network 10.4.0.0 255.255.0.0
- default-router 10.4.1.1

認証のためのワイヤレス クライアントの設定

ISR を設定したら、ルータがこれらの無線クライアントを認証し、WLAN ネットワークへのアクセスを提供できるように、さまざまな認証タイプのために無線クライアントを説明したように設定します。このドキュメントでは、クライアント側の設定に Cisco Aironet Desktop Utility（ADU）を使用します。

オープン認証のためのワイヤレス クライアントの設定

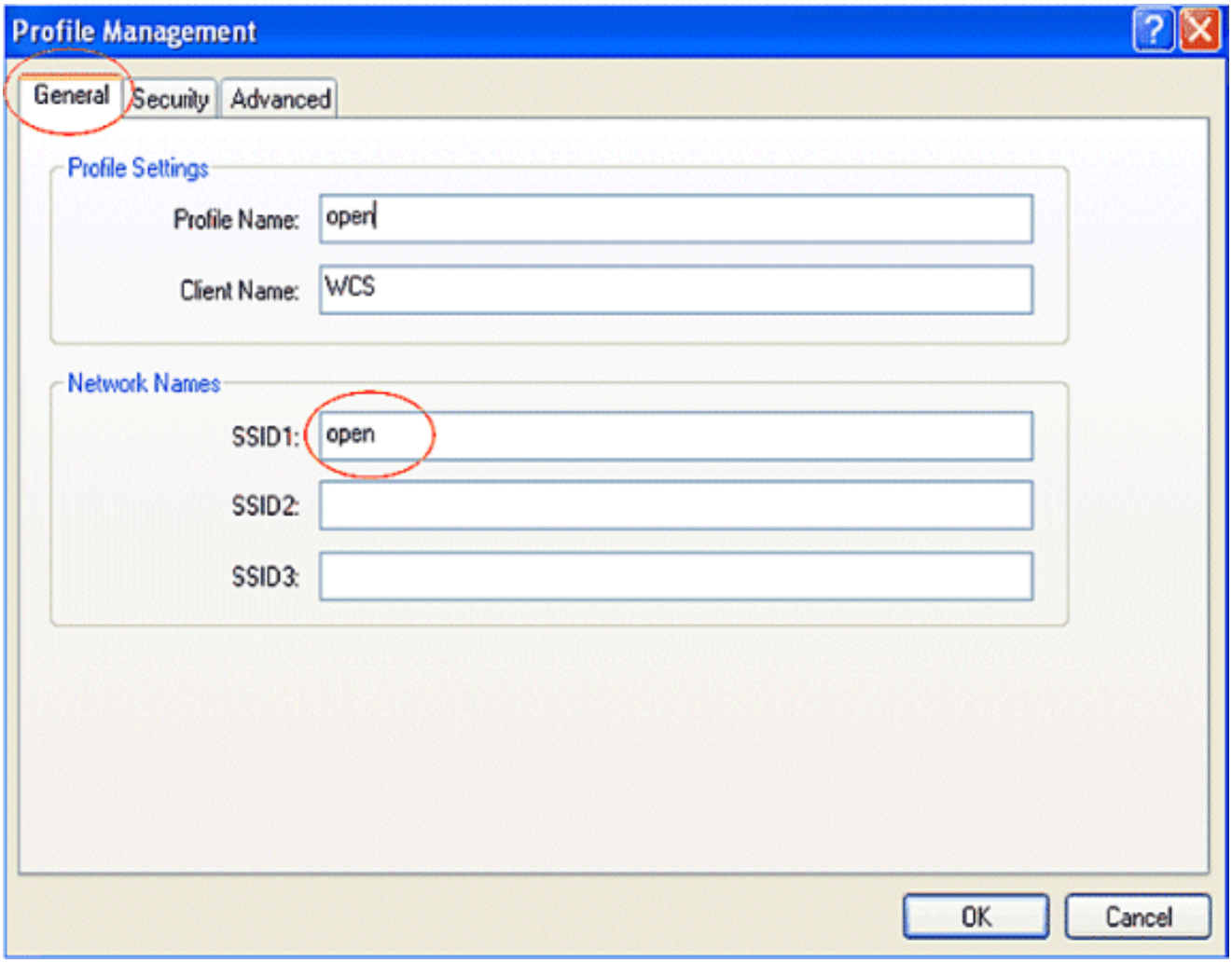
次のステップを実行します。

1. ADU の [Profile Management] ウィンドウで、[New] をクリックして新しいプロファイルを作成します。

   新しいウィンドウが表示されます。ここでオープン認証の設定を行います。[General] タブで、クライアント アダプタが使用する [Profile Name] と [SSID] を入力します。

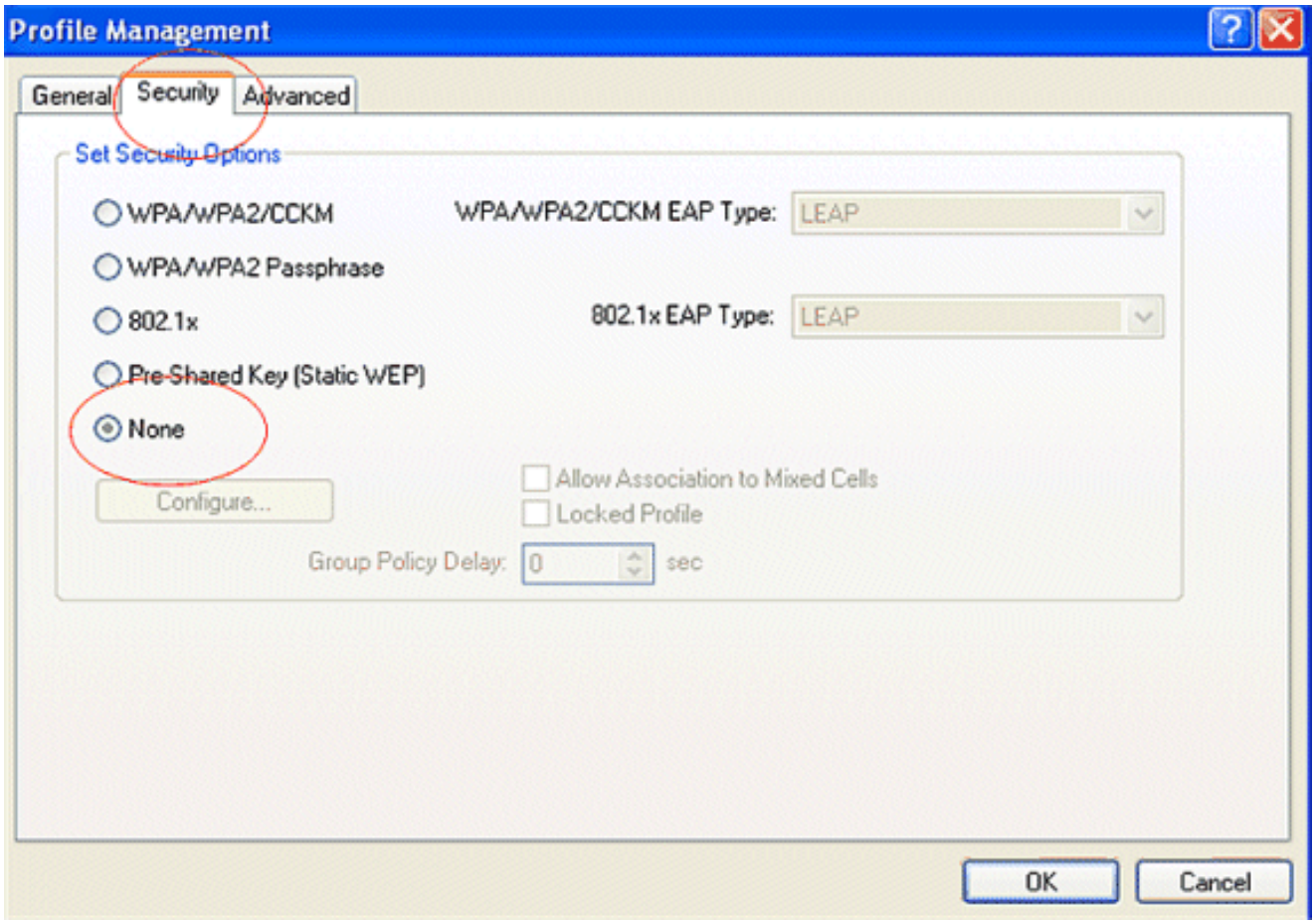
   この例では、プロファイル名と SSID は open です。

   注：SSIDは、オープン認証のためにISRで設定したSSIDと一致する必要があります。

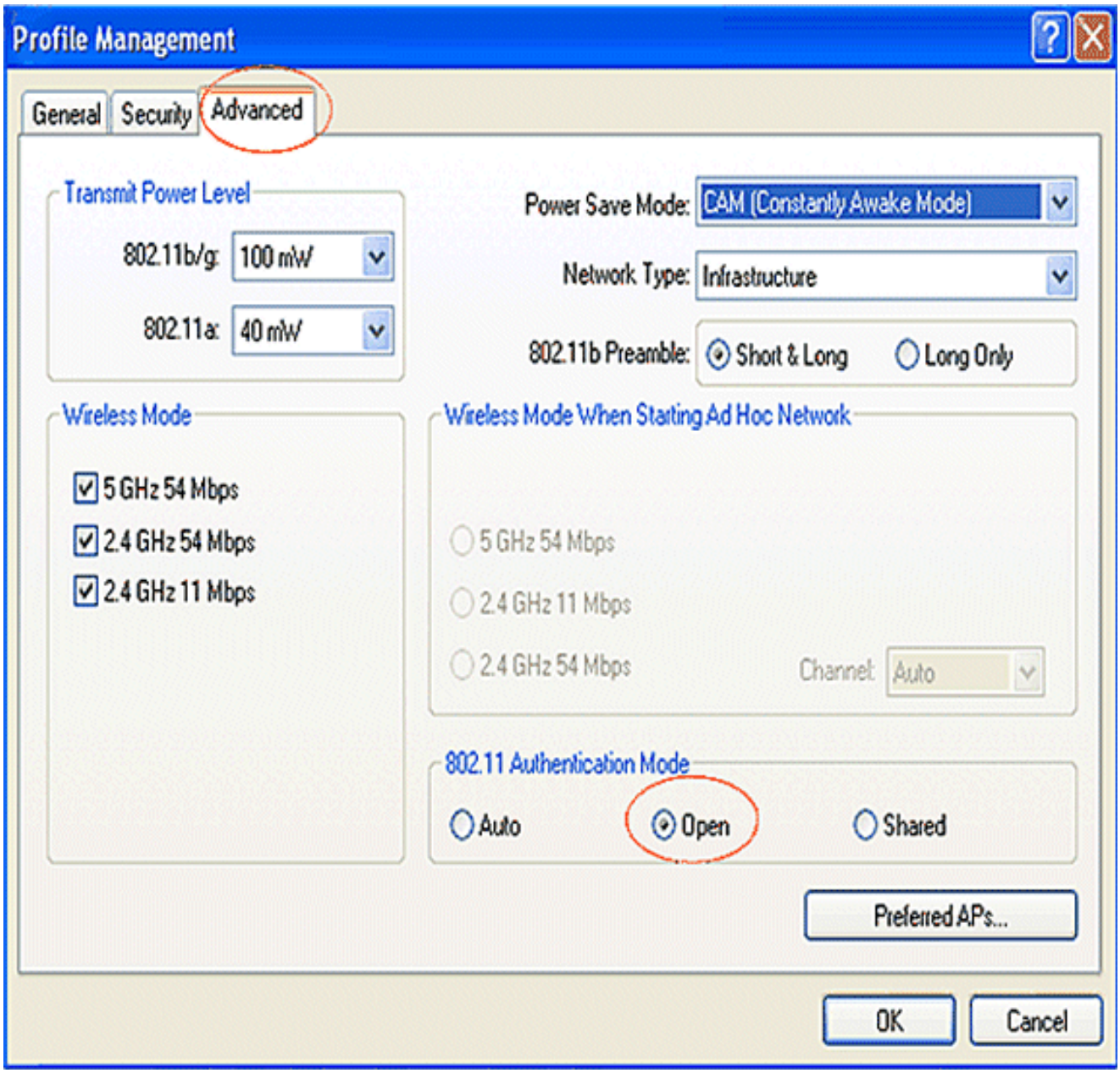


2. [Security] タブをクリックし、WEP 暗号化のセキュリティ オプションを [None] のままにします。この例は WEP キーを任意として使用するため、このオプションを [None] に設定することにより、クライアントは正常に WLAN ネットワークに関連付けられて通信できます。

   [OK] をクリックします。

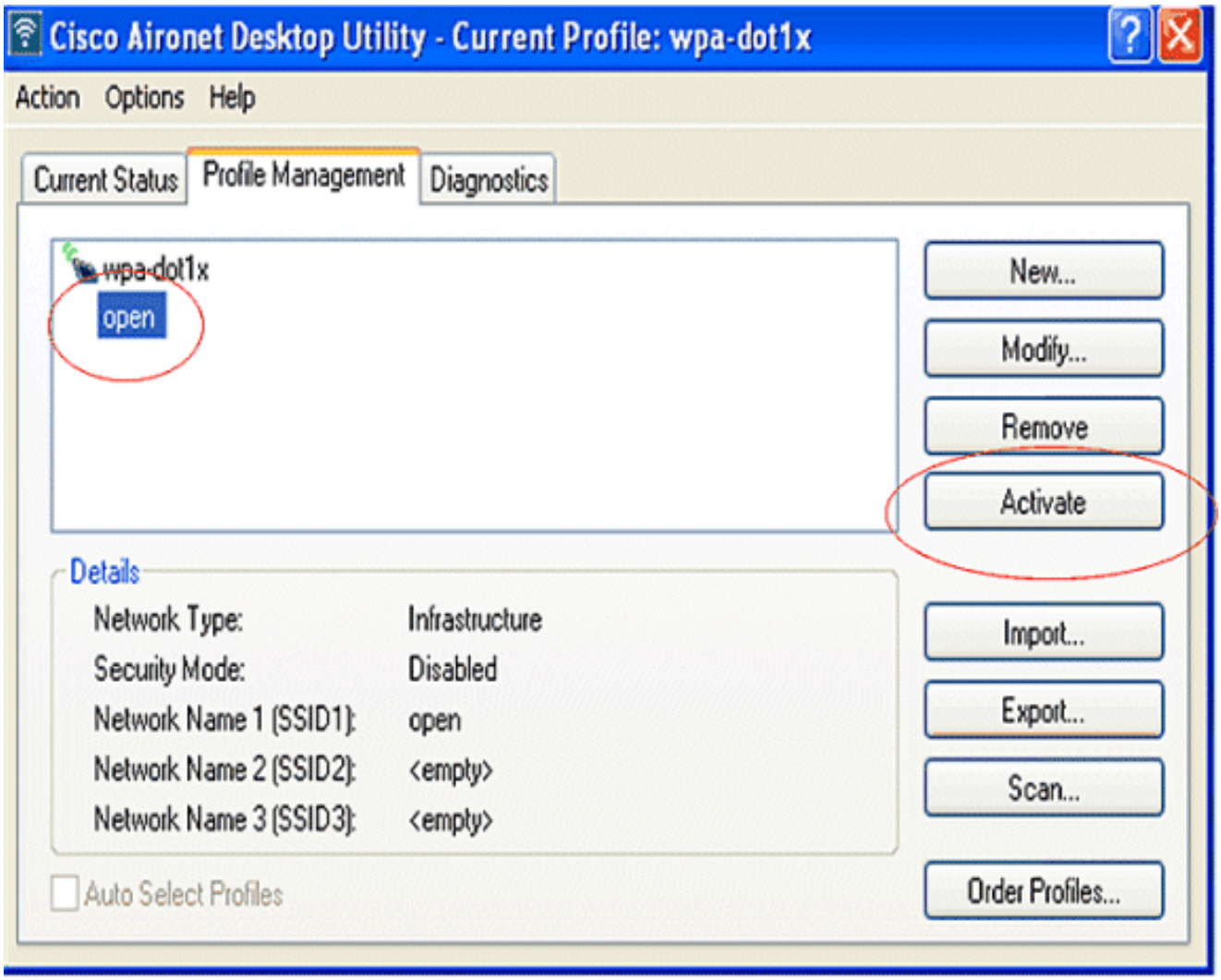


3. [Profile Management] タブから [Advanced] ウィンドウを選択し、オープン認証の場合は [802.11 Authentication Mode] を [Open] に設定します。

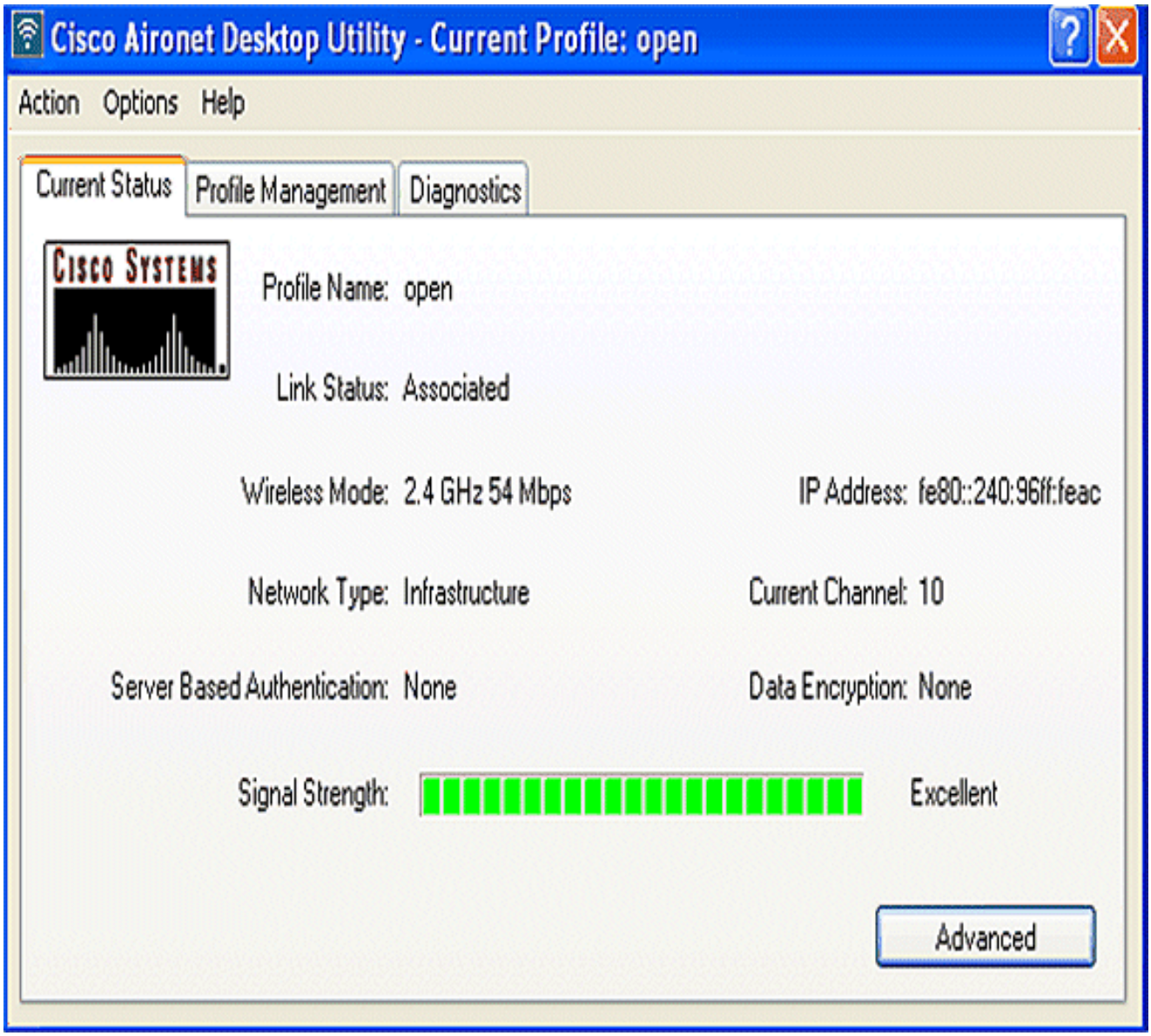


このセクションでは、設定が正常に動作していることを確認します。

1. クライアント プロファイルが作成された後、プロファイルをアクティブにするには、[Profile Management] タブで [Activate] をクリックします。



2. 正常な認証のために ADU の状態を確認します。



802.1x/EAP 認証のためのワイヤレス クライアントの設定

次のステップを実行します。

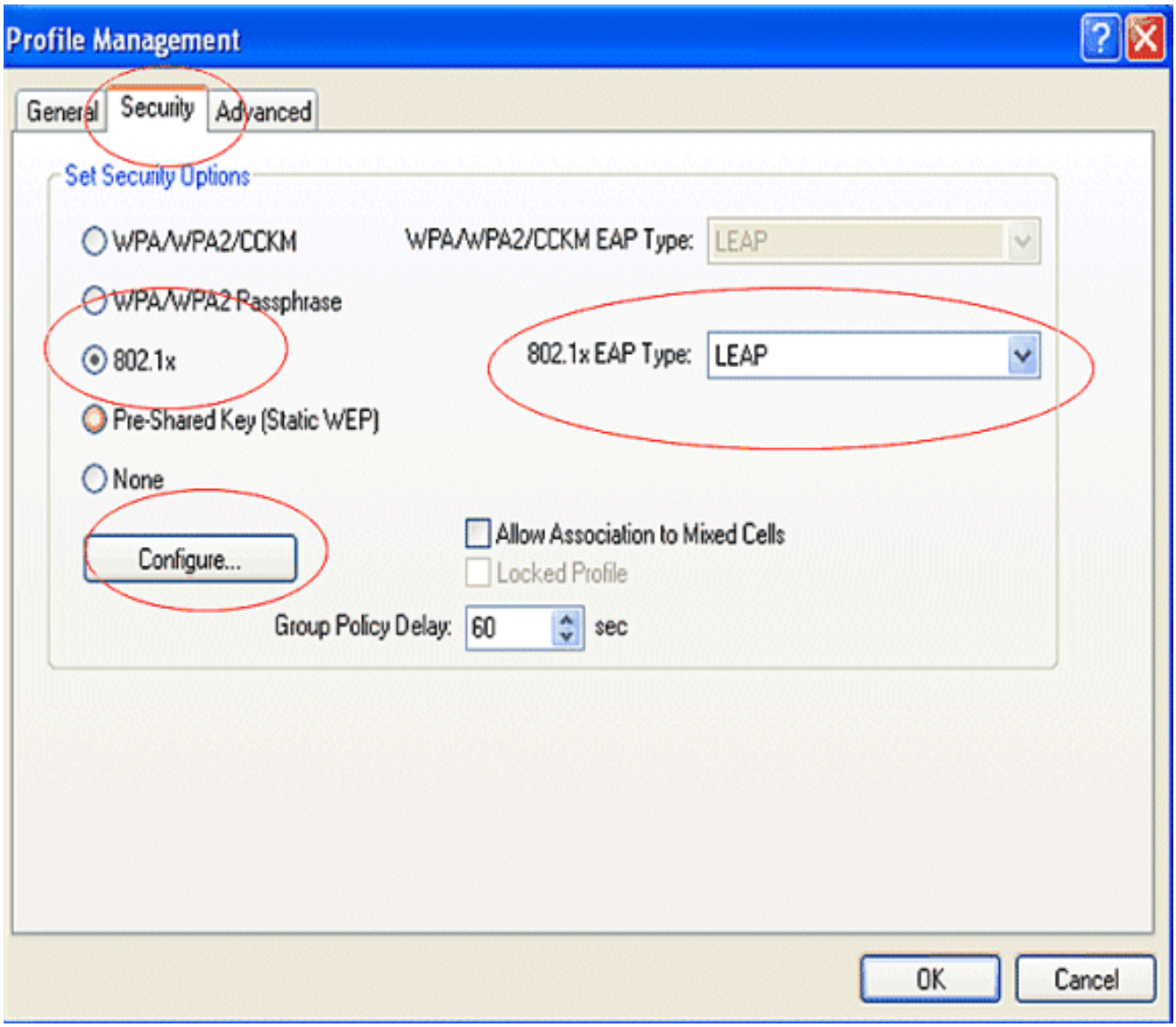
1. ADU の [Profile Management] ウィンドウで、[New] をクリックして新しいプロファイルを作成します。

   新しいウィンドウが表示されます。ここでオープン認証の設定を行います。[General] タブで、クライアント アダプタが使用する [Profile Name] と [SSID] を入力します。

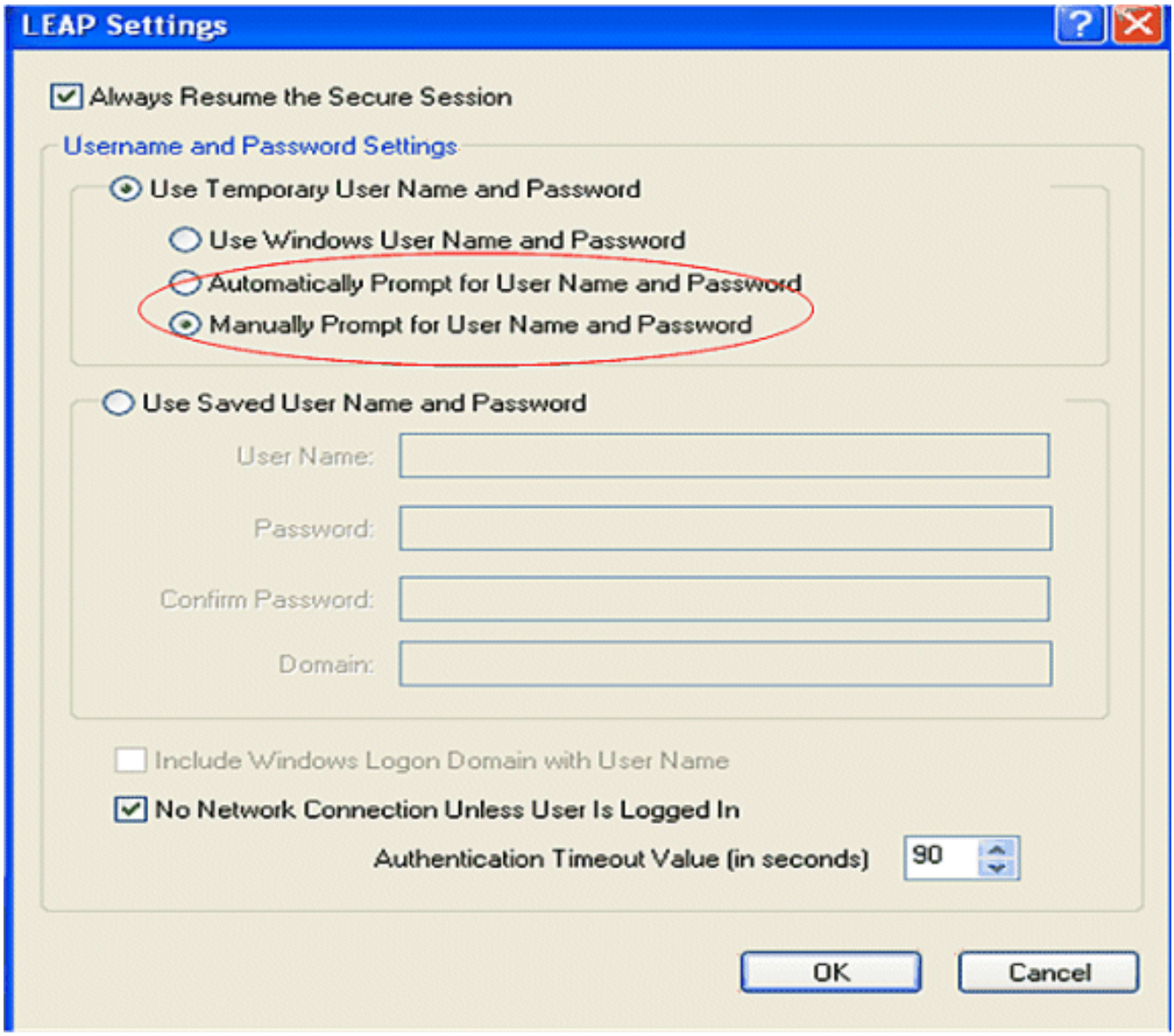
   この例では、プロファイル名と SSID は leap です。

2. [Profile Management] で [Security] タブをクリックし、セキュリティ オプションを 802.1x として設定し、適切な EAP の種類を選択します。このドキュメントでは、認証の EAP のタイプとして [LEAP] を使用しています。ここで、LEAP のユーザ名とパスワードを設定するには、[Configure] をクリックします。

   注：注：SSIDは、ISRで802.1x/EAP認証に設定したSSIDと一致する必要があります。

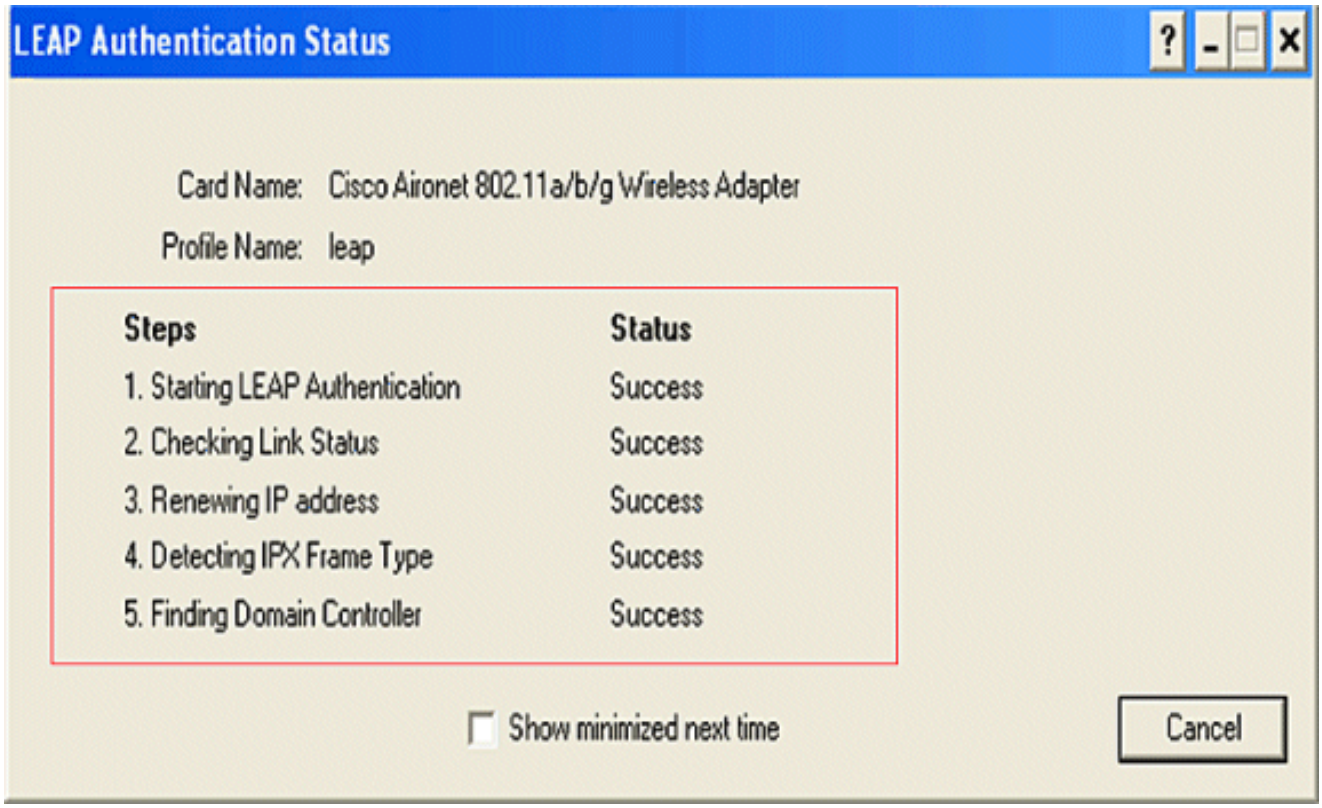


3. ユーザ名とパスワードの設定で、この例では [Manually Prompt for User Name and Password] を選択し、クライアントがネットワークへの接続を試みるときに、正しいユーザ名およびパスワードの入力が求められるようにします。[OK] をクリックします。



このセクションでは、設定が正常に動作していることを確認します。

- クライアント プロファイルが作成された後、プロファイル leap をアクティブにするには、[Profile Management] タブで [Activate] をクリックします。leap のユーザ名とパスワードが求められます。この例では、ユーザ名とパスワードに user1 を使用しています。[OK] をクリックします。
- クライアントが正常に認証されて、ルータで設定された DHCP サーバから IP アドレスが割り当てられることを確認できます。



WPA-PSK 認証のためのワイヤレス クライアントの設定

次のステップを実行します。

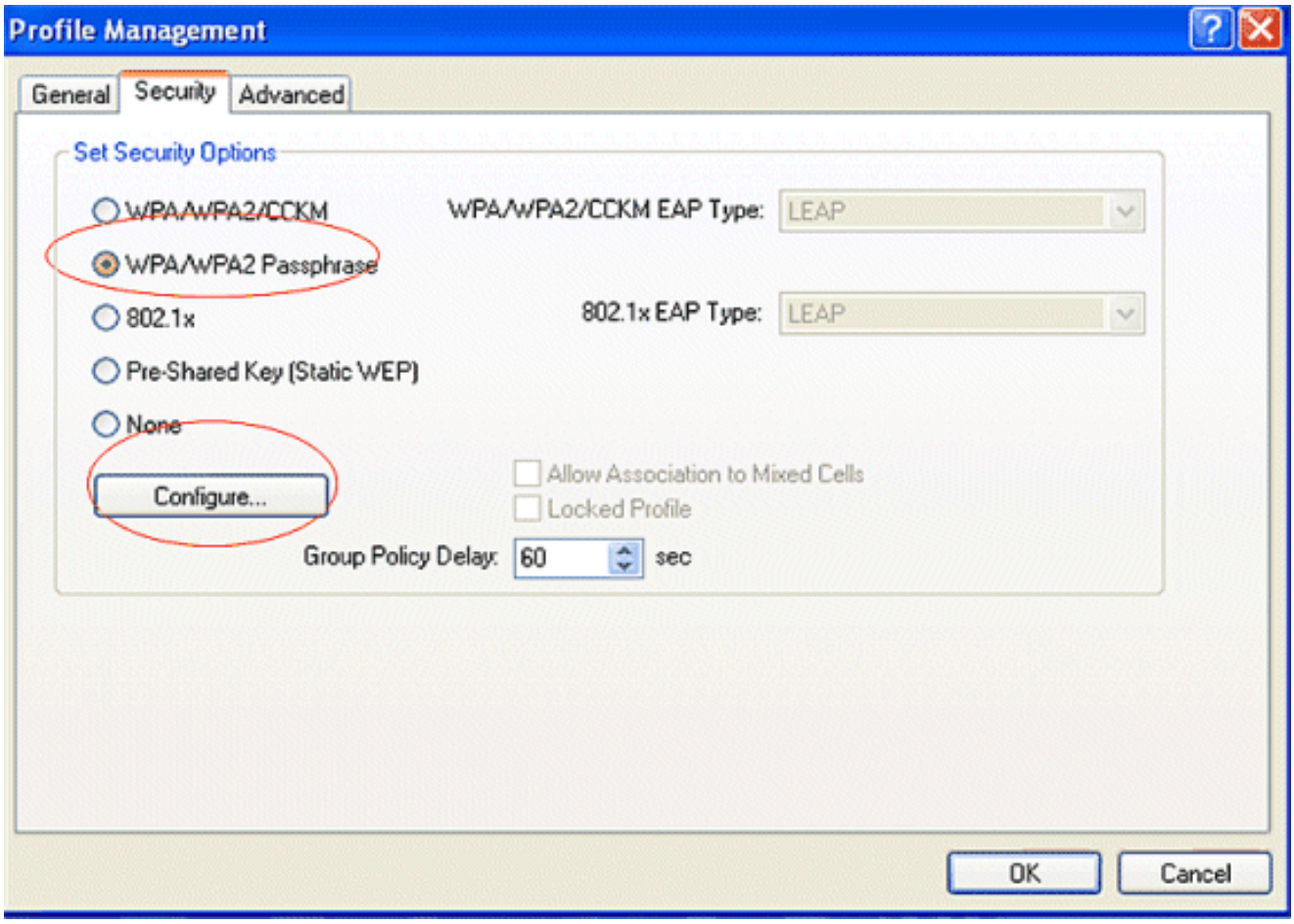
1. ADU の [Profile Management] ウィンドウで、[New] をクリックして新しいプロファイルを作成します。

   新しいウィンドウが表示されます。ここでオープン認証の設定を行います。[General] タブで、クライアント アダプタが使用する [Profile Name] と [SSID] を入力します。

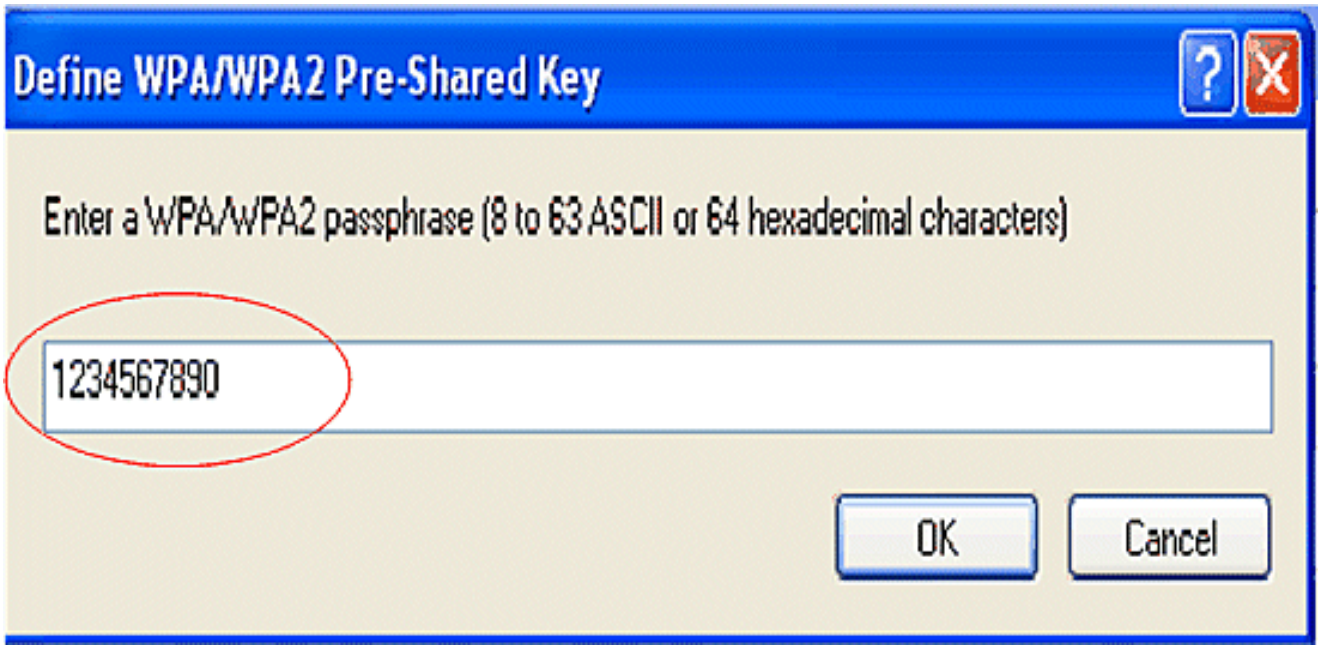
   この例では、プロファイル名と SSID に wpa-shared が使用されています。

   注：SSIDは、ISRでWPA-PSK認証に設定したSSIDと一致する必要があります。

2. [Profile Management] で [Security] タブをクリックし、セキュリティ オプションを [WPA/WPA2 Passphrase] として設定します。ここで、[WPA Passphrase] を設定するには、[Configure] をクリックします。



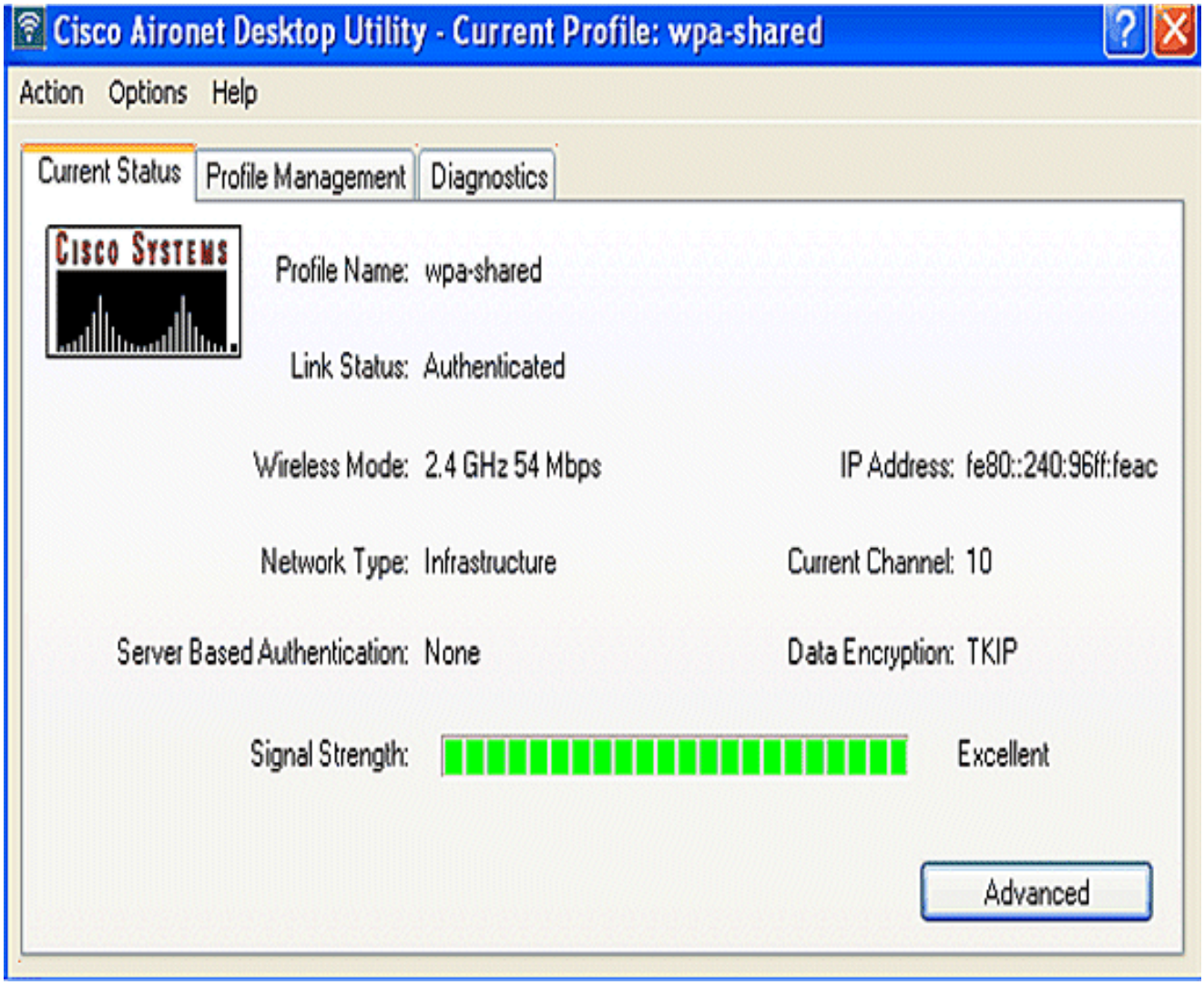
3. WPA 事前共有キーを定義します。キーの長さは 8 ~ 63 文字の ASCII 文字である必要があります。[OK] をクリックします。



このセクションでは、設定が正常に動作していることを確認します。

- クライアント プロファイルが作成された後、プロファイル wpa-shared をアクティブにするには、[Profile Management] タブで [Activate] をクリックします。

- 正常な認証のために ADU を確認します。



WPA（EAP を使用した）認証のためのワイヤレス クライアントの設定

次のステップを実行します。

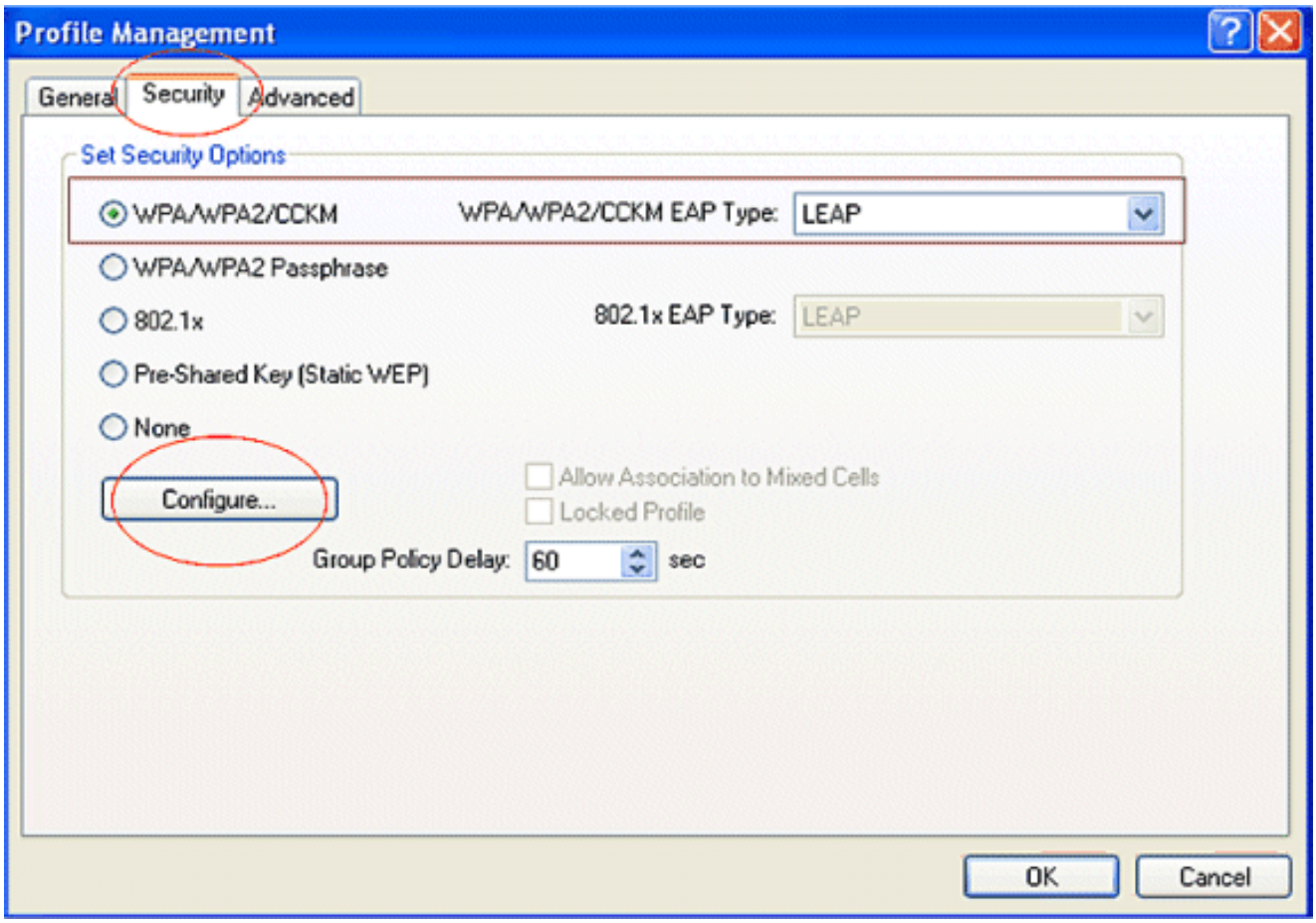
1. ADU の [Profile Management] ウィンドウで、[New] をクリックして新しいプロファイルを作成します。

   新しいウィンドウが表示されます。ここでオープン認証の設定を行います。[General] タブで、クライアント アダプタが使用する [Profile Name] と [SSID] を入力します。

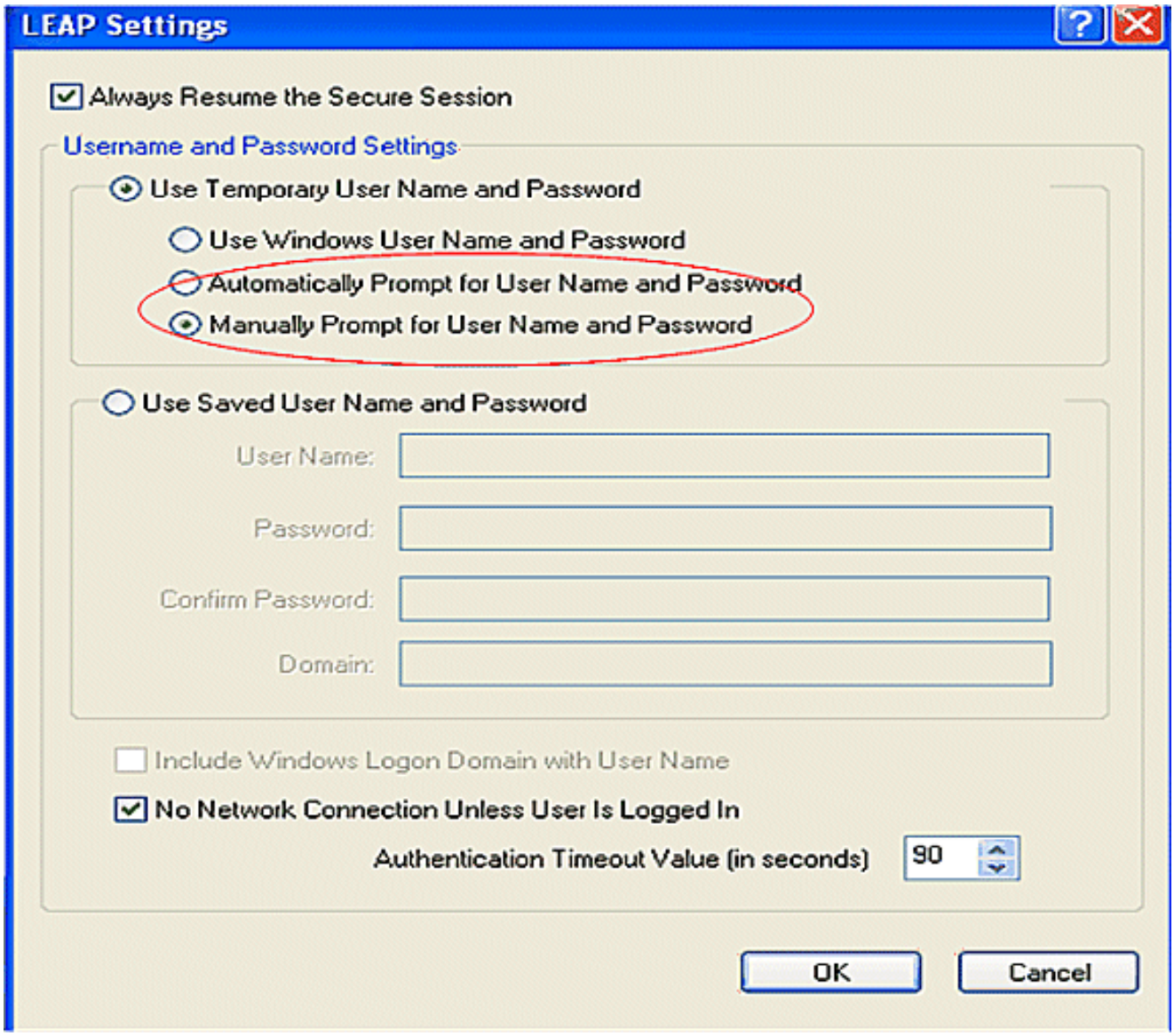
   この例では、プロファイル名と SSID に wpa-dot1x が使用されています。

   注：SSIDは、ISRでWPA（EAPを使用）認証用に設定したSSIDと一致する必要があります。

2. [Profile Management] で [Security] タブをクリックし、セキュリティ オプションを [WPA/WPA2/CCKM] として設定し、適切な WPA/WPA2/CCKM EAP の種類を選択します。このドキュメントでは、認証の EAP のタイプとして [LEAP] を使用しています。ここで、LEAP のユーザ名とパスワードを設定するには、[Configure] をクリックします。

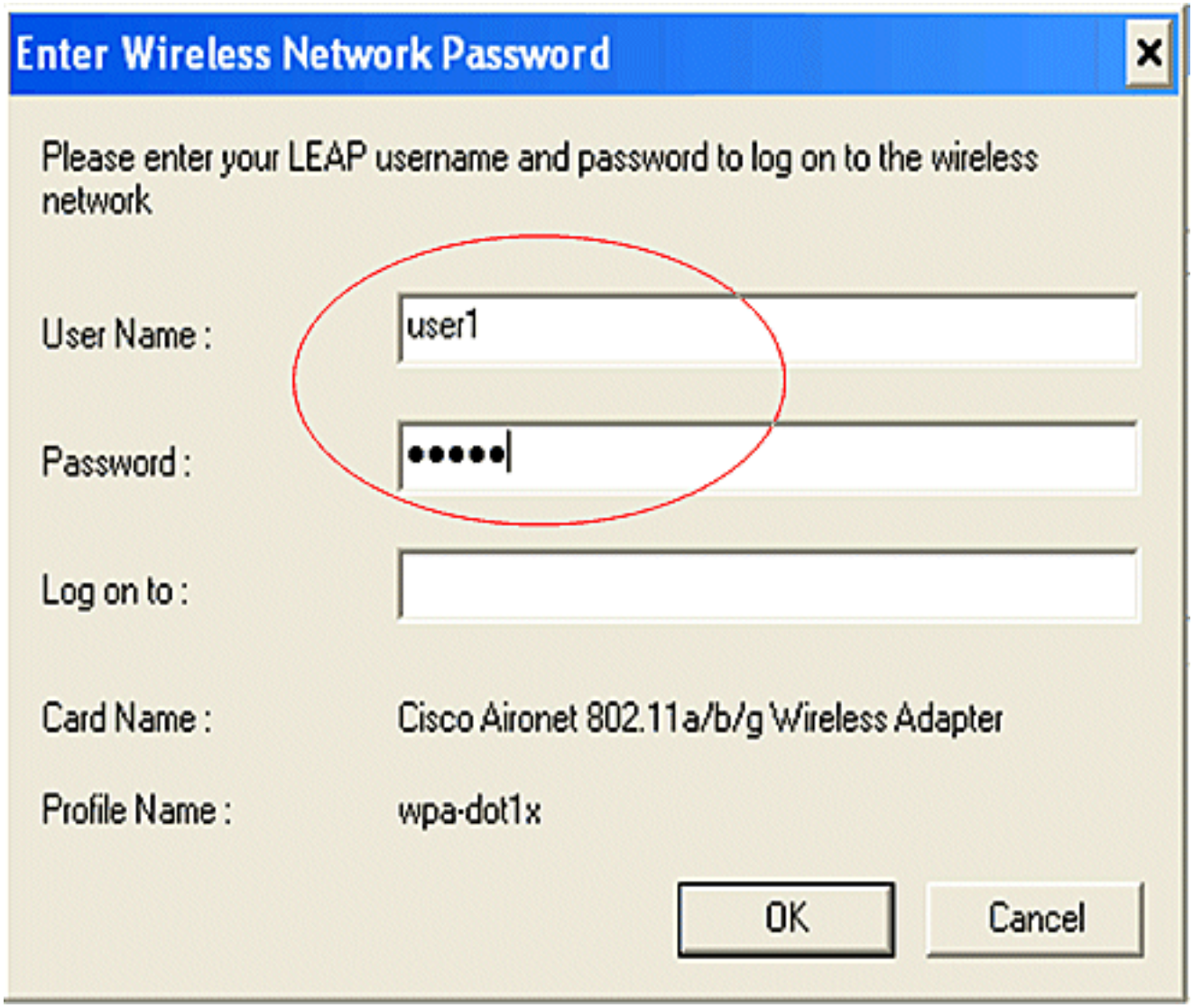


3. [Username and Password Settings] で、この例では [Manually Prompt for User Name and Password] を選択し、クライアントがネットワークへの接続を試みるときに、正しいユーザ名およびパスワードの入力が求められるようにします。[OK] をクリックします。

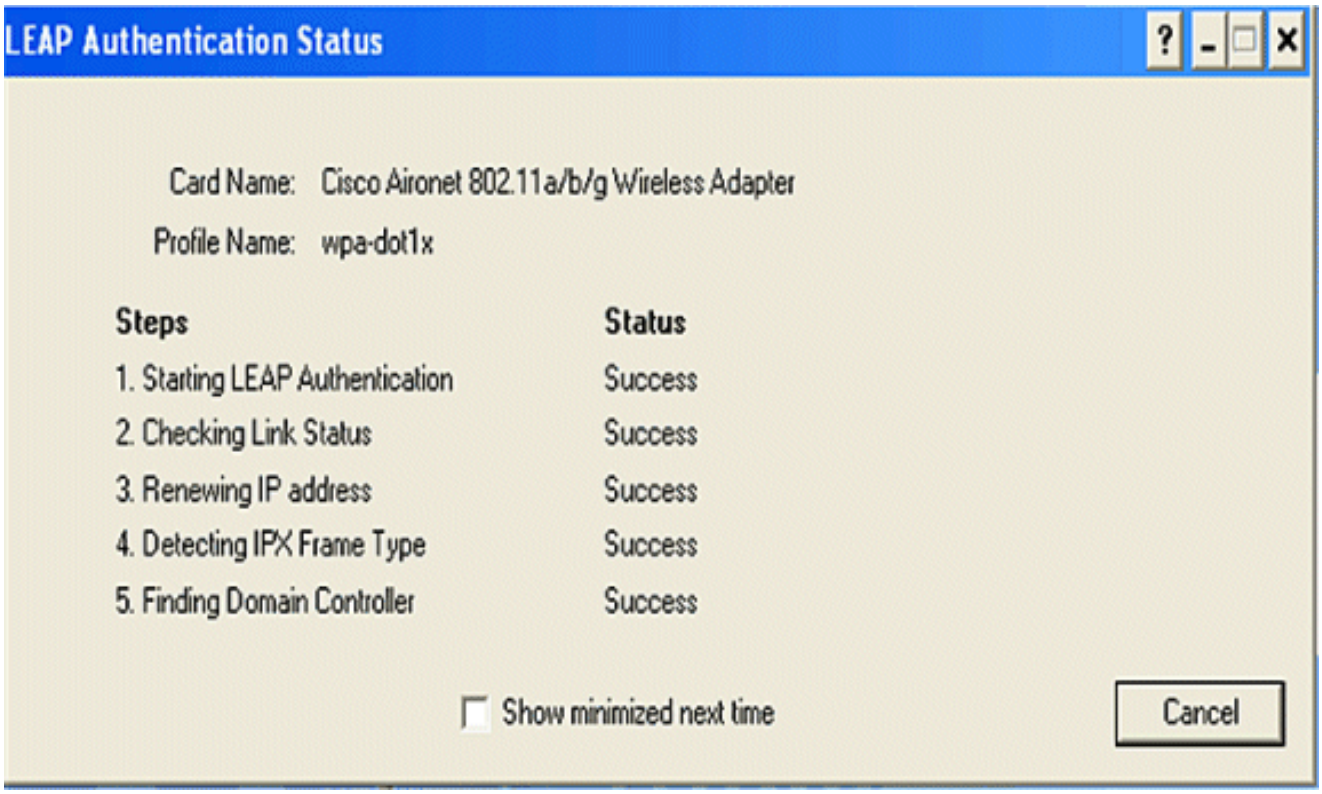


このセクションでは、設定が正常に動作していることを確認します。

1. クライアント プロファイルが作成された後、プロファイル wpa-dot1x をアクティブにするには、[Profile Management] タブで [Activate] をクリックします。leap のユーザ名とパスワードが求められます。この例では、ユーザ名とパスワードとして user1 を使用しています。[OK] をクリックします。



2. クライアントが正常に認証するのを確認できます。



ルータの CLI からのコマンド show dot11 associations は、クライアントのアソシエーション ステータスの詳細を表示します。次に例を示します。

Router#show dot11 associations

<#root>

```
802.11 Client Stations on Dot11Radio0:

SSID [leap] :

MAC Address    IP address      Device        Name            Parent        State
0040.96ac.e657 10.3.0.2        CB21AG/PI21AG WCS             self        EAP-Assoc


SSID [open] :

SSID [pre-shared] : DISABLED, not associated with a configured VLAN

SSID [wpa-dot1x] :

SSID [wpa-shared] :


Others:  (not related to any ssid)
```

トラブルシュート

トラブルシューティングのためのコマンド

次の debug コマンドを使用して、設定のトラブルシューティングを行うことができます。

- debug dot11 aaa authenticator all:MACおよびEAP認証パケットのデバッグをアクティブにします。
- debug radius authentication：サーバとクライアント間の RADIUS ネゴシエーションを表示します。
- debug radius local-server packets：送受信される RADIUS パケットの内容を表示します。
- debug radius local-server client：失敗したクライアント認証に関するエラー メッセージを表示します。

関連情報

- ワイヤレス LAN コントローラでの認証の設定例
- アクセス ポイントでの VLAN の設定
- 内部 DHCP とオープン認証を使用する 1800 ISR ワイヤレス ルータの設定例
- シスコ ワイヤレス ISR と HWIC アクセス ポイント構成ガイド
- ISR と WEP 暗号化および LEAP 認証を使用するワイヤレス LAN 接続の設定例
- テクニカル サポートとドキュメント - Cisco Systems
- 認証タイプの設定
- ISR と WEP 暗号化および LEAP 認証を使用するワイヤレス LAN 接続の設定例

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。