Wi-Fi Protected Access 2（WPA 2）の設定例

内容

概要

このドキュメントでは、Wireless LAN（WLAN; ワイヤレス LAN）で Wi-Fi Protected Access 2（WPA 2）を使用するメリットについて説明します。 このドキュメントでは、WLAN での WPA 2 の実装に関する 2 つの設定例について説明します。1 番目の例では WPA 2 を Enterprise モードで設定する方法、2 番目の例では WPA 2 を Personal モードで設定する方法を示します。

注：WPAは Extensible Authentication Protocol(EAP)と連動します。

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

- 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 Aironet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 IOS® ソフトウェア リリース 12.3(2)JA が稼働する Cisco Aironet 1310G Access Point（AP; アクセス ポイント）/ブリッジ
- ファームウェア 2.5 が稼働する Aironet 802.11a/b/g CB21AG クライアント アダプタ
- ファームウェア 2.5 が稼働する Aironet Desktop Utility（ADU）

注：Aironet CB21AGおよびPI21AGクライアントアダプタソフトウェアは、他のAironetクライアントアダプタソフトウェアと互換性がありません。ADU は、CB21AG カードおよび PI21AG カードで、Aironet Client Utility（ACU）はその他すべての Aironet クライアント アダプタで使用する必要があります。CB21AG カードおよび ADU をインストールする方法の詳細は、『クライアント アダプタのインストール』を参照してください。

注：このドキュメントでは、アンテナが内蔵されたAP/ブリッジを使用します。外部アンテナを必要とする AP/ブリッジを使用する場合は、アンテナが AP/ブリッジに接続されていることを確認します。そうでない場合は、AP/ブリッジはワイヤレス ネットワークに接続できません。特定の AP/ブリッジ モデルには一体型アンテナが装備されていますが、他のモデルでは一般的な操作に外部アンテナが必要です。内部アンテナまたは外部アンテナが付いている AP/ブリッジ モデルについての詳細は、適切なデバイスの注文ガイドまたは製品ガイドを参照してください。

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

WPA は Wi-Fi Alliance による標準ベースのセキュリティ ソリューションで、ネイティブ WLAN の脆弱性に対処するものです。WPA は、WLAN システムに対する拡張データ保護とアクセス コントロール機能を提供します。WPA は、従来の IEEE 802.11 によるセキュリティ実装における Wired Equivalent Privacy（WEP）の既知のすべての脆弱性に対処し、企業環境と Small Office, Home Office（SOHO; スモール オフィス、ホーム オフィス）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 2は、次世代のWi-Fiセキュリティです。WPA 2 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。WPA 2は、Counter Mode with Cipher Block Chaining Message Authentication Code Protocol(CCMP)を使用して、National Institute of Standards and Technology(NIST)が推奨するAdvanced Encryption Standard(AES)暗号化アルゴリズムを実装しています。AES カウンタ モードは、データの 128 ビットのブロックを 128 ビットの暗号化キーを使用して一度に暗号化する、ブロック暗号です。CCMP アルゴリズムでは、ワイヤレス フレームにデータ発信元の認証およびデータ整合性を提供する、Message Integrity Code（MIC）が生成されます。

注：CCMPはCBC-MACとも呼ばれます。

WPA2 では、AES により、Temporal Key Integrity Protocol（TKIP）よりも強力な暗号化が提供されるため、WPA よりも高いセキュリティ レベルが提供されます。TKIP は WPA で使用される暗号化アルゴリズムです。WPA2 では、関連付けごとに新たなセッション キーが作成されます。ネットワーク上のクライアントごとに使用される暗号化キーは、クライアントごとに一意で固有なものです。最終的に、無線で送信される各パケットは、一意のキーで暗号化されます。キーは再利用されないため、新しい一意の暗号化キーの使用によりセキュリティが強化されます。WPA は依然として安全であると考えられており、TKIP の仕組みはまだ破られていません。しかし、シスコでは WPA 2 へのできるだけ早急な移行を推奨しています。

WPA および WPA 2 では、次の 2 つの動作モードがサポートされています。

- エンタープライズ モード
- パーソナル モード

このドキュメントでは、WPA 2 でのこれらの 2 つのモードの実装方法について説明します。

Cisco Aironet 機器での WPA 2 のサポート

WPA 2 は、次の機器でサポートされています。

- Aironet 1130AG AP シリーズおよび 1230AG AP シリーズ
- Aironet 1100 AP シリーズ
- Aironet 1200 AP シリーズ
- Aironet 1300 AP シリーズ

注：**これらの**APに802.11g無線を装備し、Cisco IOSソフトウェアリリース12.3(2)JA以降を使用してください。

WPA 2 および AES は、次の機器でもサポートされています。

- 部品番号が AIR-RM21A および AIR-RM22A の Aironet 1200 シリーズの無線モジュール**注**：部品番号AIR-RM20AのAironet 1200無線モジュールでは、WPA 2はサポートされていません。
- ファームウェア バージョン 2.5 の Aironet 802.11a/b/g クライアント アダプタ

注：Cisco Aironet 350シリーズ製品は、無線でAESがサポートされていないため、WPA 2をサポートしていません。

注：Cisco Aironet 1400シリーズワイヤレスブリッジはWPA 2またはAESをサポートしていません。

エンタープライズ モードでの設定

Enterprise モードという用語は、Pre-Shared Key（PSK; 事前共有キー）動作モードと IEEE 802.1x 動作モードの両方で認証の相互運用が可能であることが確認された製品を指します。802.1x は、多様な認証メカニズムとより強固な暗号化アルゴリズムをサポートする柔軟性によって、従来のあらゆる認証用フレームワークよりも安全性が高いと考えられています。エンタープライズ モードの WPA 2 では、2 段階で認証が実行されます。オープン認証の設定は、最初の段階で行われます。2 番目のフェーズは、EAP 手法のいずれかを使用した 802.1x 認証です。暗号化メカニズムは AES により提供されます。

エンタープライズ モードでは、クライアントと認証サーバが EAP 認証方式を使用して互いに認証を行います。そして、クライアントとサーバが Pairwise Master Key (PMK) を生成します。WPA 2 では、サーバが PMK を動的に生成し、その PMK を AP に渡します。

このセクションでは、Enterprise 動作モードに WPA 2 を実装するために必要な設定について説明します。

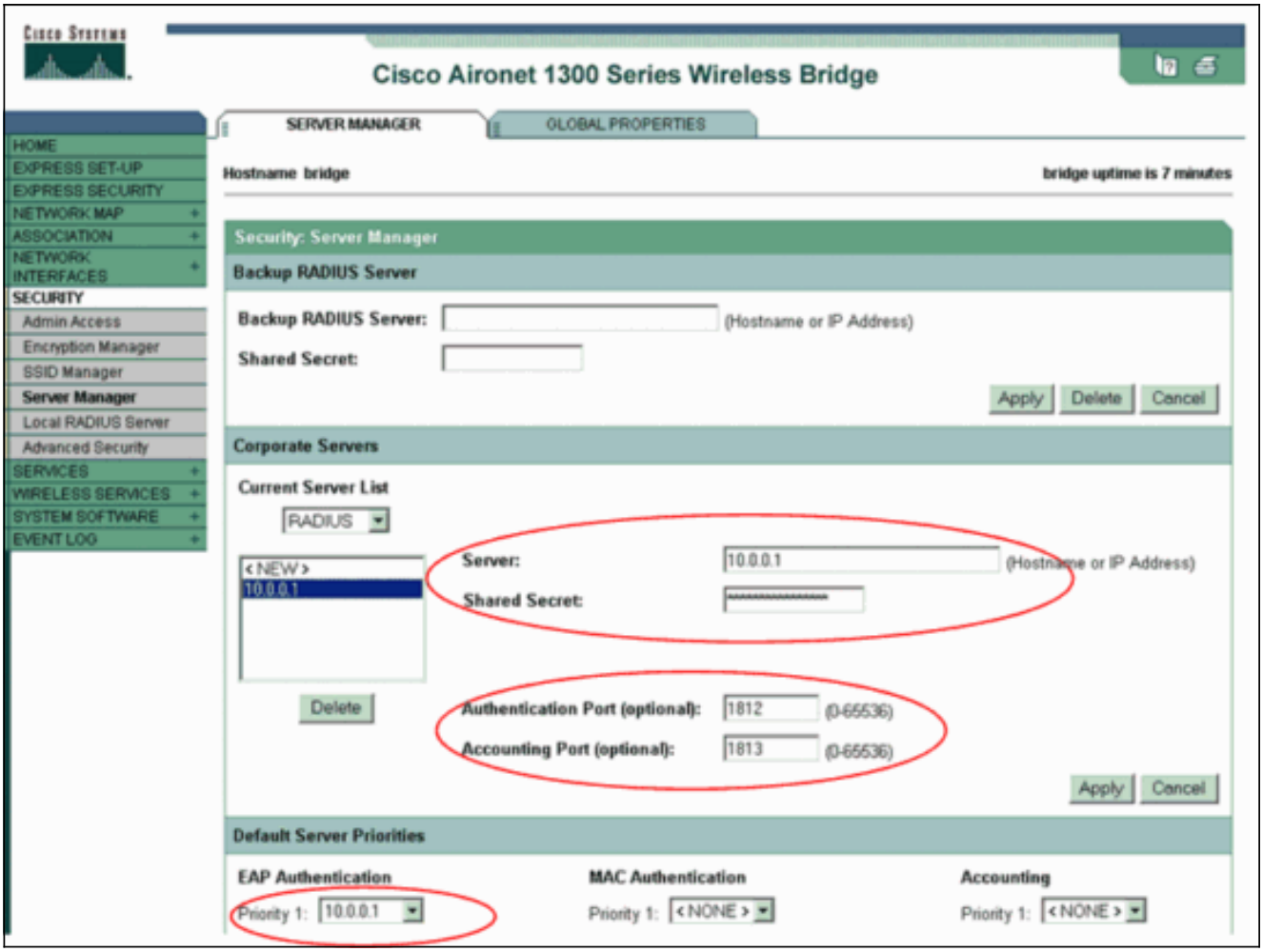
ネットワークのセットアップ

このセットアップでは、Cisco Lightweight Extensible Authentication Protocol (LEAP) が稼働する Aironet 1310G AP/ブリッジにより、WPA 2 互換のクライアント アダプタでユーザが認証されます。キー管理には、AES-CCMP 暗号化が設定された WPA 2 が使用されます。AP は、LEAP 認証を実行するローカル RADIUS サーバとして設定されます。このセットアップを実装するためには、クライアント アダプタおよび AP を設定する必要があります。「AP の設定」および「クライアント アダプタの設定」のセクションでは、AP とクライアント サーバでの設定について説明しています。

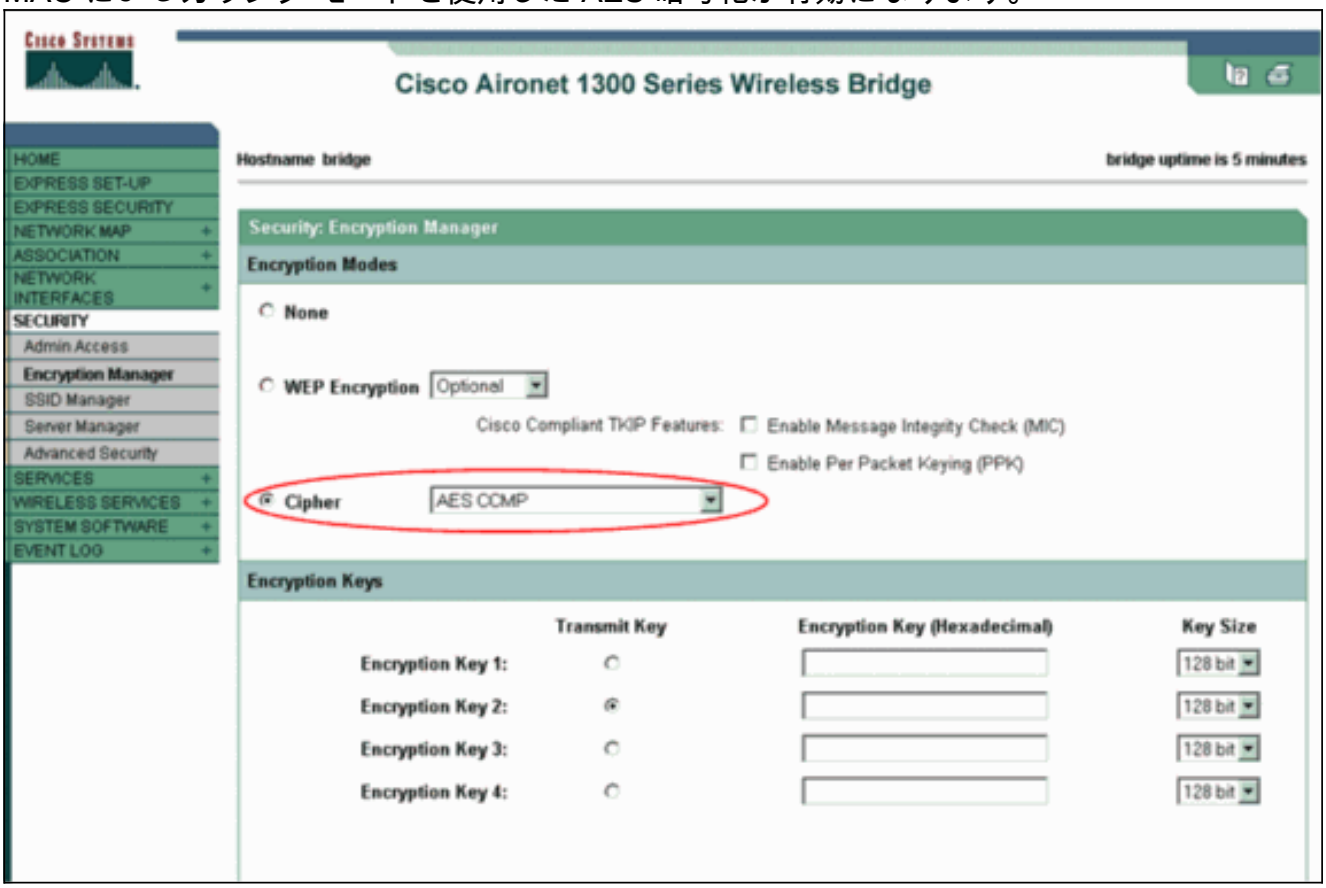
AP の設定

次の手順を実行して、GUI を使用して AP を設定します。

1. AP を、LEAP 認証が稼働するローカルの RADIUS サーバとして設定します。左側のメニューで [Security] > [Server Manager] を選択して、RADIUS サーバの IP アドレス、ポート、および共有秘密を定義します。この設定では、AP をローカルの RADIUS サーバとして設定するため、AP の IP アドレスを使用してください。ローカル RADIUS サーバの動作には、ポート 1812 および 1813 を使用します。[Default Server Priorities] エリアで、デフォルトの EAP 認証プライオリティを 10.0.0.1 に定義します。**注：**10.0.0.1はローカルRADIUSサーバです。

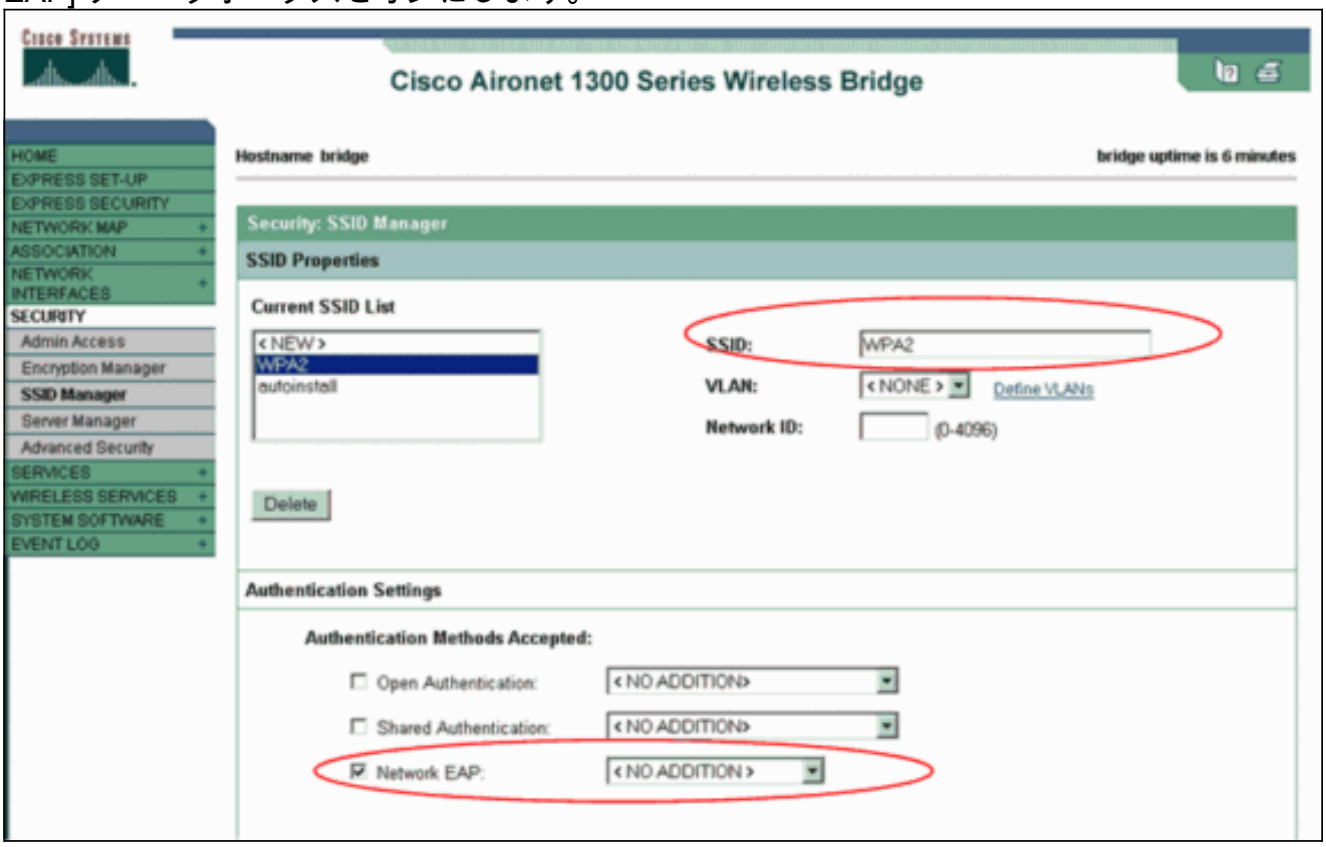


2. 左側のメニューで [Security] > [Encryption Manager] を選択して、次の手順を実行します。[Cipher] メニューで、[AES CCMP] を選択します。このオプションを選択すると、CBC-MAC によるカウンタ モードを使用した AES 暗号化が有効になります。



[Apply] をクリックします。

3. [Security] > [SSID Manager] を選択し、WPA 2 で使用する新しい Service Set Identifier（SSID）を作成します。[Authentication Methods Accepted] エリアの [Network EAP] チェックボックスをオンにします。

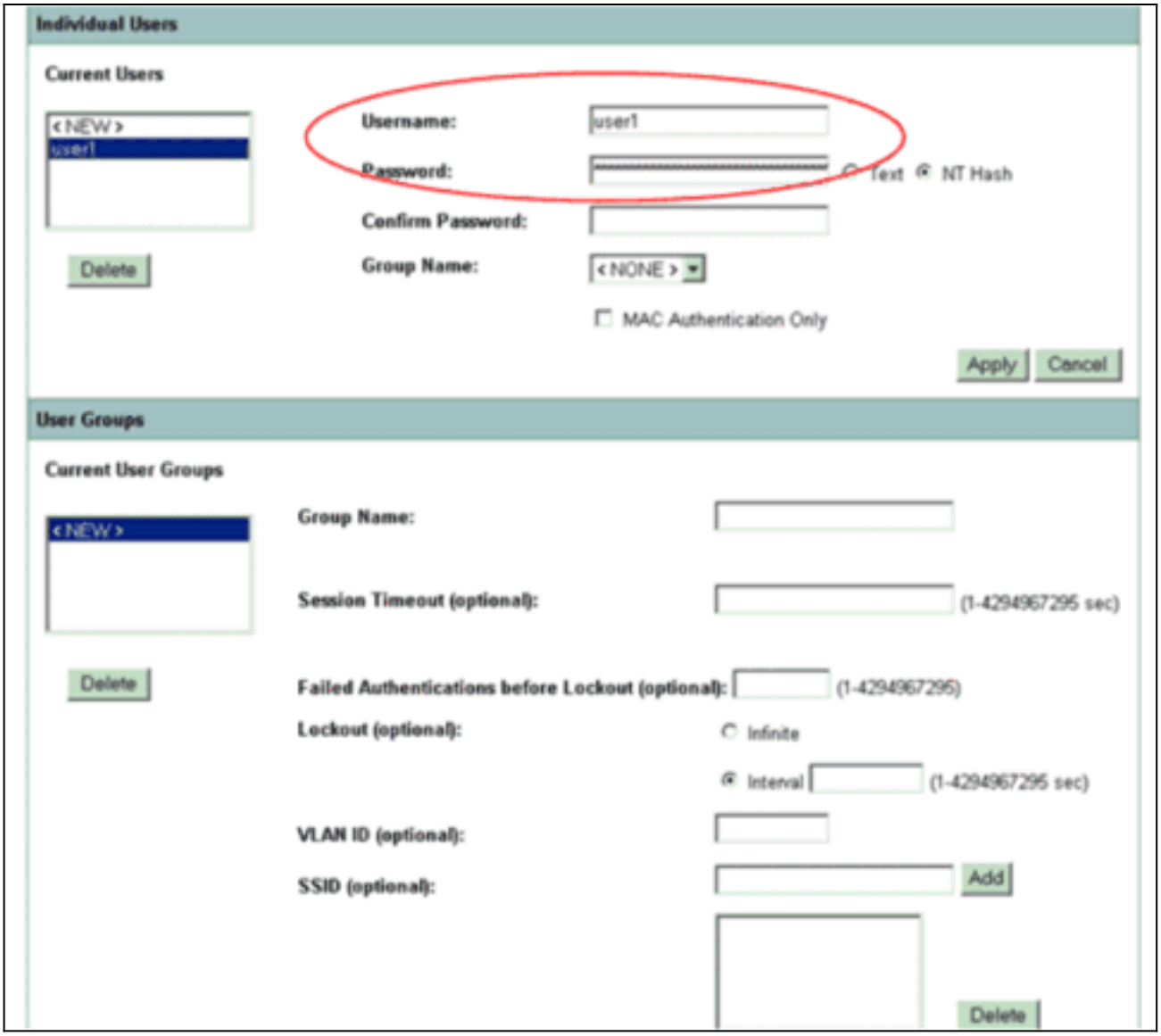


注：無線インターフェイスで認証タイプを設定する場合は、次のガイドラインに従ってください。Cisco クライアント：Network EAP を使用する。サードパーティのクライアント（Cisco Compatible Extensions（CCX）準拠の製品を含む）：EAP によるオープン認証を使用する。Cisco とサードパーティのクライアントの両方：Network EAP と EAP による Open Authentication の両方を選択する。[Authenticated Key Management] エリアまで [Security SSID Manager] ウィンドウを下にスクロールし、次の手順を実行します。[Key Management] メニューで、[Mandatory] を選択します。右側の [WPA] チェックボックスをオンにします。[Apply] をクリックします。**注：VLANの**定義はオプションです。VLAN を定義した場合、この SSID の使用に関連付けられたクライアント デバイスは、VLAN にグループ化されます。VLAN の実装方法に関する詳細は、『VLAN の設定』を参照してください。

4. [Security] > [Local Radius Server] を選択して、次の手順を実行します。ウィンドウ上部にある [General Set-Up] タブをクリックします。[LEAP] チェックボックスをオンにし、[Apply] をクリックします。[Network Access Servers] エリアで、RADIUS サーバの IP アドレスおよび共有秘密を定義します。ローカル RADIUS サーバの場合は、AP の IP アドレスを使用します。

[Apply] をクリックします。

5. [Individual Users] エリアまで [General Set-Up] ウィンドウを下にスクロールし、個々のユーザを定義します。ユーザ グループの定義はオプションです。



この設定では、ユーザに名前「user1」およびパスワードを定義します。また、この設定ではパスワードに NT ハッシュを選択します。このセクションでの手順を完了すると、AP ではクライアントからの認証要求を受け入れる準備が整います。次に、クライアント アダプタを設定します。

CLI での設定

アクセス ポイント

```
ap#show running-config
Building configuration...
.
.
.
aaa new-model !--- This command reinitializes the
authentication, !--- authorization and accounting
functions. ! ! aaa group server radius rad_eap
 server 10.0.0.1 auth-port 1812 acct-port 1813
!--- A server group for RADIUS is created called
"rad_eap" !--- that uses the server at 10.0.0.1 on ports
1812 and 1813. . . . aaa authentication login
eap_methods group rad_eap
!--- Authentication [user validation] is to be done for
!--- users in a group called "eap_methods" who use
server group "rad_eap". . . . ! bridge irb ! interface
Dot11Radio0 no ip address no ip route-cache !
```

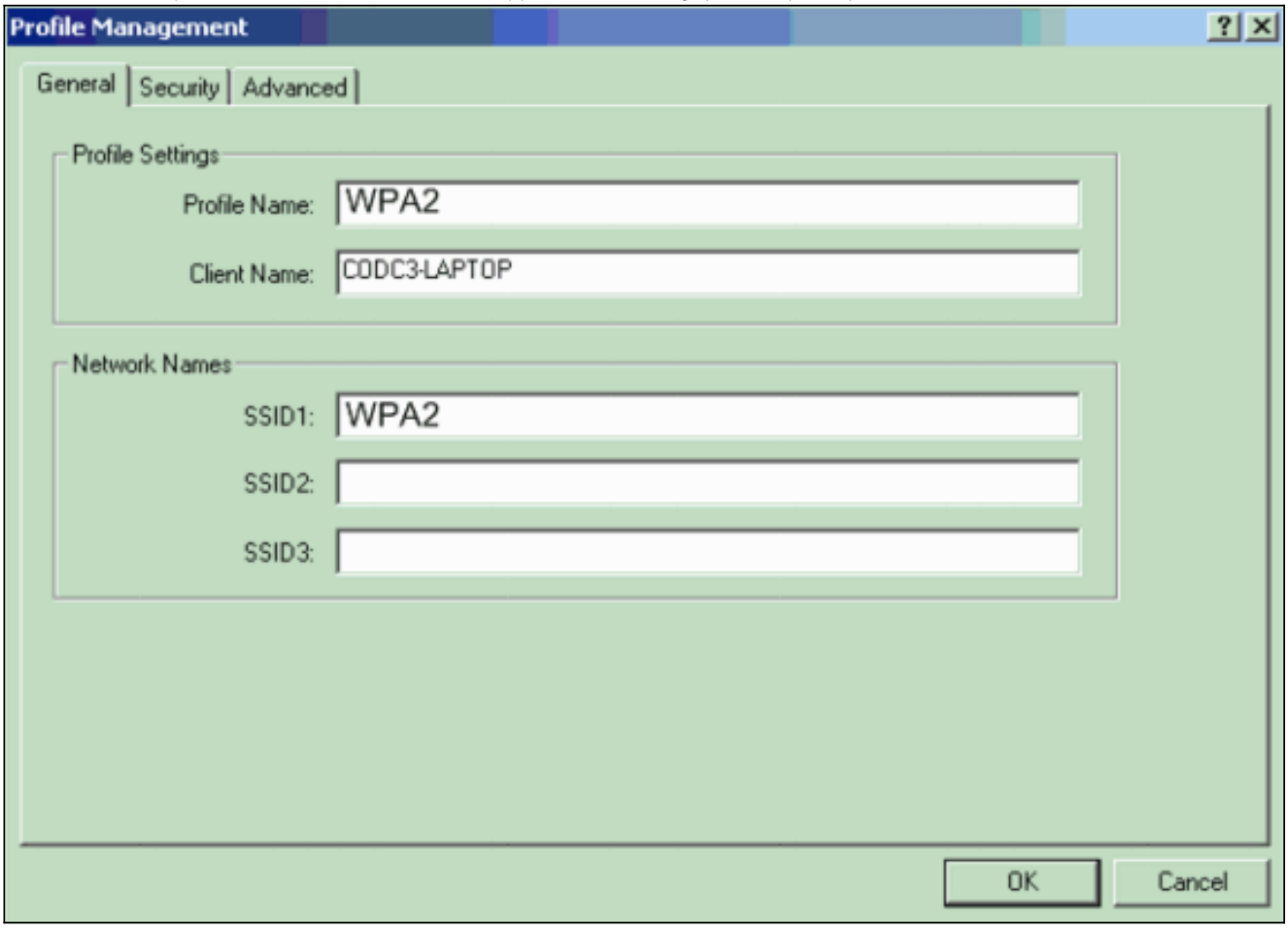
```
encryption vlan 1 key 1 size 128bit
   12345678901234567890123456 transmit-key
!---This step is optional !--- This value seeds the
initial key for use with !--- broadcast
[255.255.255.255] traffic. If more than one VLAN is !---
used, then keys must be set for each VLAN. encryption
vlan 1 mode wep mandatory
!--- This defines the policy for the use of Wired
Equivalent Privacy (WEP). !--- If more than one VLAN is
used, !--- the policy must be set to mandatory for each
VLAN. broadcast-key vlan 1 change 300
  !--- You can also enable Broadcast Key Rotation for
each vlan and Specify the time after which Brodacst key
is changed. If it is disabled Broadcast Key is still
used but not changed. ssid cisco vlan 1
!--- Create a SSID Assign a vlan to this SSID
authentication open eap eap_methods
 authentication network-eap eap_methods
 !--- Expect that users who attach to SSID "cisco" !---
request authentication with the type 128 Open EAP and
Network EAP authentication !--- bit set in the headers
of those requests, and group those users into !--- a
group called "eap_methods." ! speed basic-1.0 basic-2.0
basic-5.5 basic-11.0 rts threshold 2312 channel 2437
station-role root bridge-group 1 bridge-group 1
subscriber-loop-control bridge-group 1 block-unknown-
source no bridge-group 1 source-learning no bridge-group
1 unicast-flooding bridge-group 1 spanning-disabled . .
. interface FastEthernet0 no ip address no ip route-
cache duplex auto speed auto bridge-group 1 no bridge-
group 1 source-learning bridge-group 1 spanning-disabled
! interface BVI1 ip address 10.0.0.1 255.255.255.0 !---
The address of this unit. no ip route-cache ! ip
default-gateway 10.77.244.194 ip http server ip http
help-path
http://www.cisco.com/warp/public/779/smbiz/prodconfig/he
lp/eag/ivory/1100 ip radius source-interface BVI1 snmp-
server community cable RO snmp-server enable traps tty
radius-server local
!--- Engages the Local RADIUS Server feature. nas
10.0.0.1 key shared_secret
!--- Identifies itself as a RADIUS server, reiterates !-
-- "localness" and defines the key between the server
(itself) and the access point(itself). ! group testuser
!--- Groups are optional. ! user user1 nthash password1
group testuser
!--- Individual user user user2 nthash password2 group
testuser
!--- Individual user !--- These individual users
comprise the Local Database ! radius-server host
10.0.0.1 auth-port 1812 acct-port
   1813 key shared_secret
!--- Defines where the RADIUS server is and the key
between !--- the access point (itself) and the server.
radius-server retransmit 3 radius-server attribute 32
include-in-access-req format %h radius-server
authorization permit missing Service-Type radius-server
vsa send accounting bridge 1 route ip ! ! line con 0
line vty 5 15 ! end
```

クライアント アダプタの設定

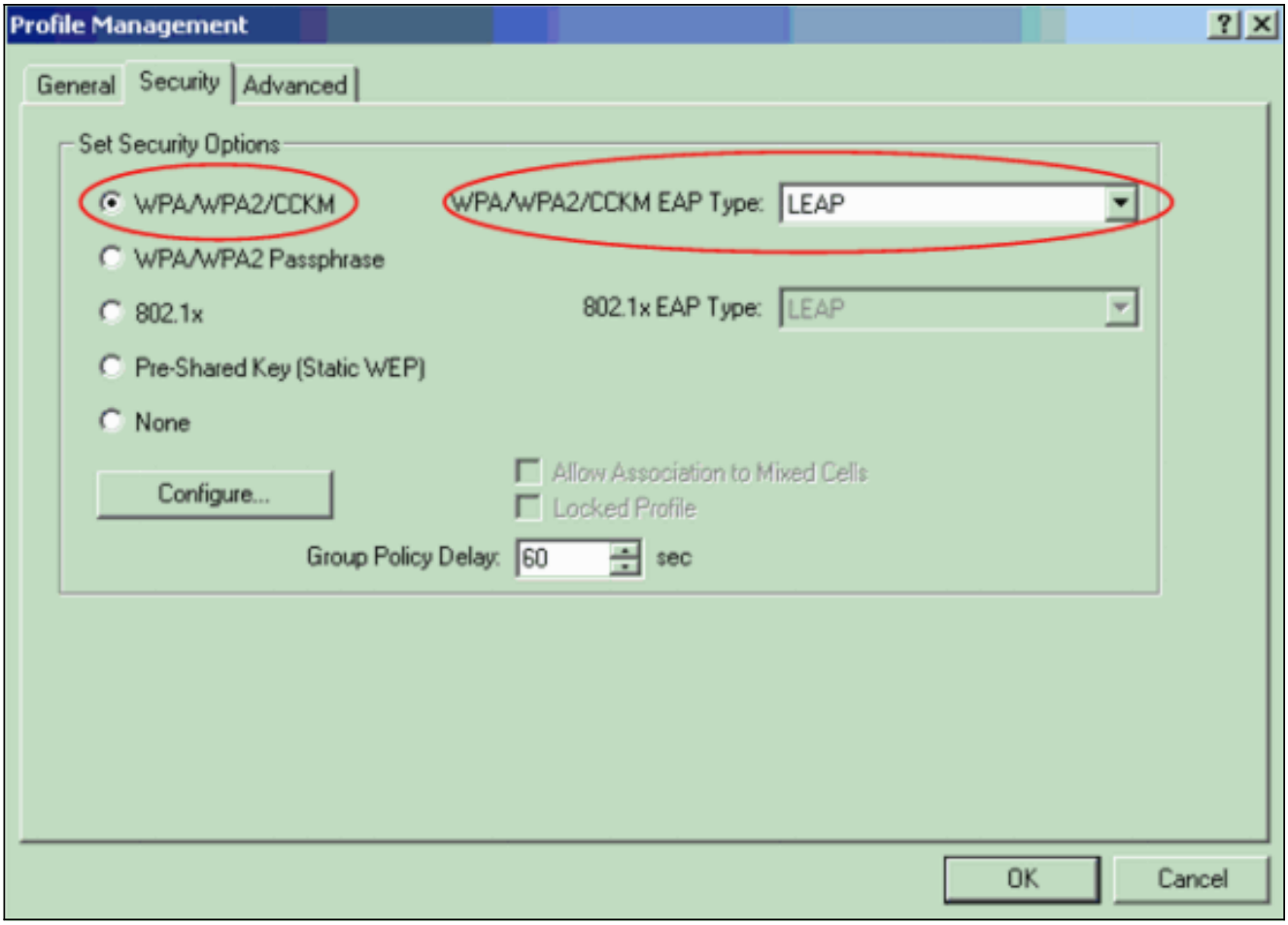
次のステップを実行します。

注：このドキュメントでは、ファームウェア2.5が稼働するAironet 802.11a/b/gクライアントアダプタを使用し、ADUバージョン2.5でのクライアントアダプタの設定について説明します。

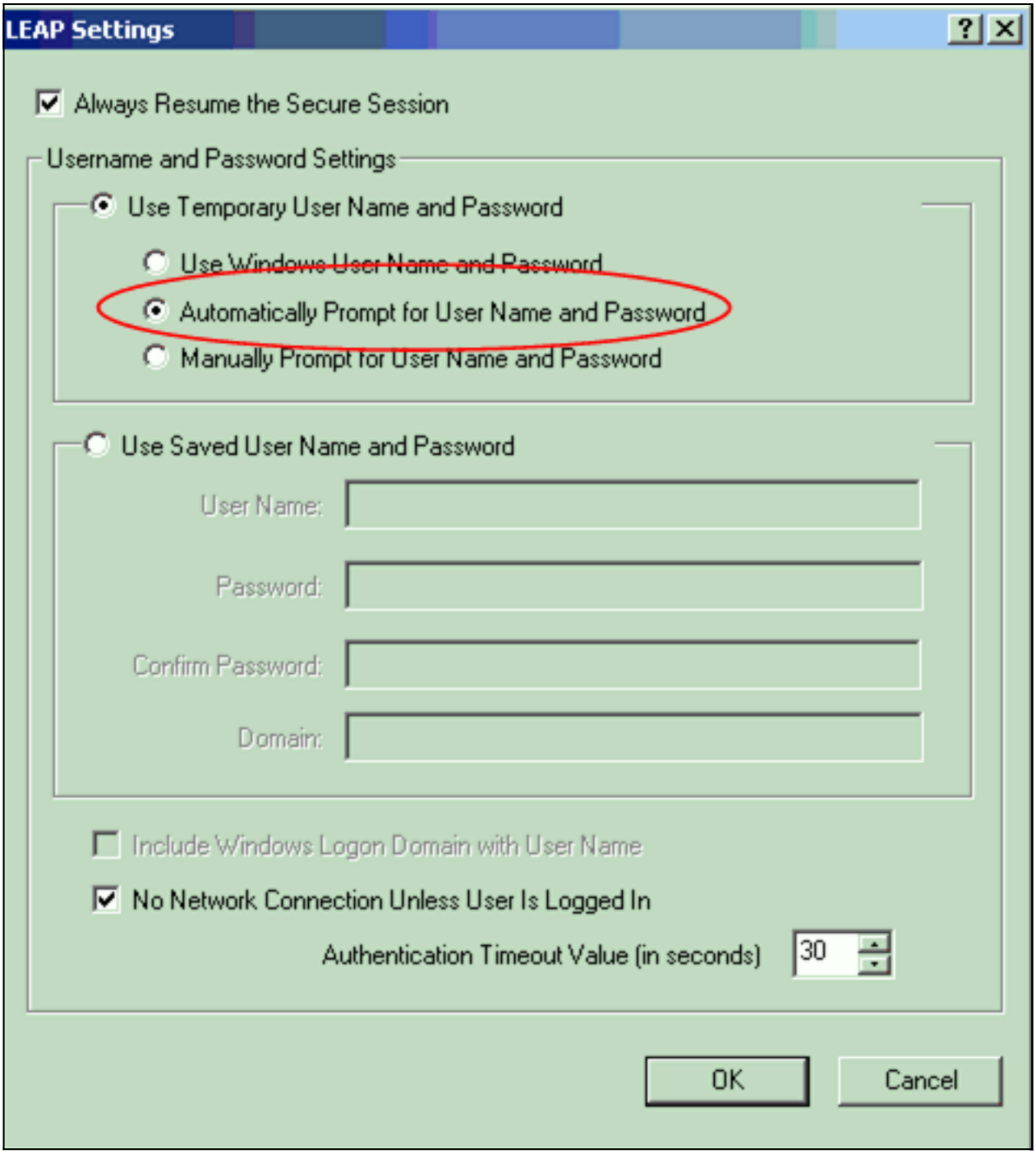
1. ADU の [Profile Management] ウィンドウで、 **[New]** をクリックして新しいプロファイルを作成します。新しいウィンドウに、WPA 2 Enterprise モード動作設定の設定場所が表示されます。[General] タブで、クライアント アダプタが使用するプロファイル名と SSID を入力します。この例では、プロファイル名と SSID に WPA2 を使用しています。**注：**SSIDは、APでWPA 2用に設定したSSIDと一致している必要があります。



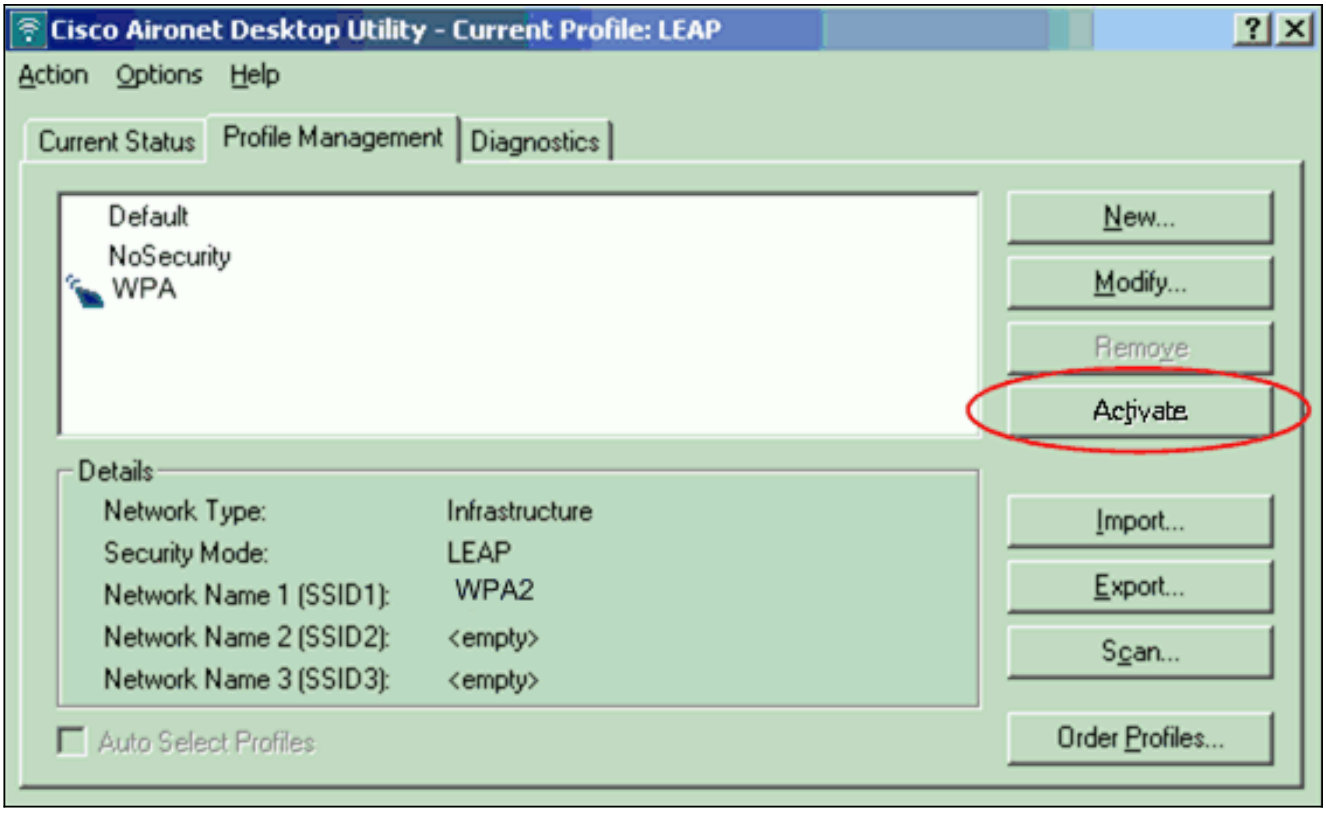
2. [Security] タブをクリックし、[WPA/WPA2/CCKM] をクリックして、[WPA/WPA2/CCKM EAP Type] メニューから [LEAP] を選択します。このアクションにより、WPA または WPA 2 のいずれか（AP に設定したもの）がイネーブルになります。



3. [Configure] をクリックして LEAP 設定を定義します。
4. 要件に応じて適切なユーザ名およびパスワードの設定を選択し、[OK] をクリックします。この設定では、[Automatically Prompt for User Name and Password] オプションを選択します。このオプションにより、LEAP 認証が実行されたときに、ユーザ名およびパスワードを手動入力できるようになります。



5. [OK] をクリックして [Profile Management] ウィンドウを閉じます。
6. [Activate] をクリックして、クライアント アダプタ上でこのプロファイルをイネーブルにします。

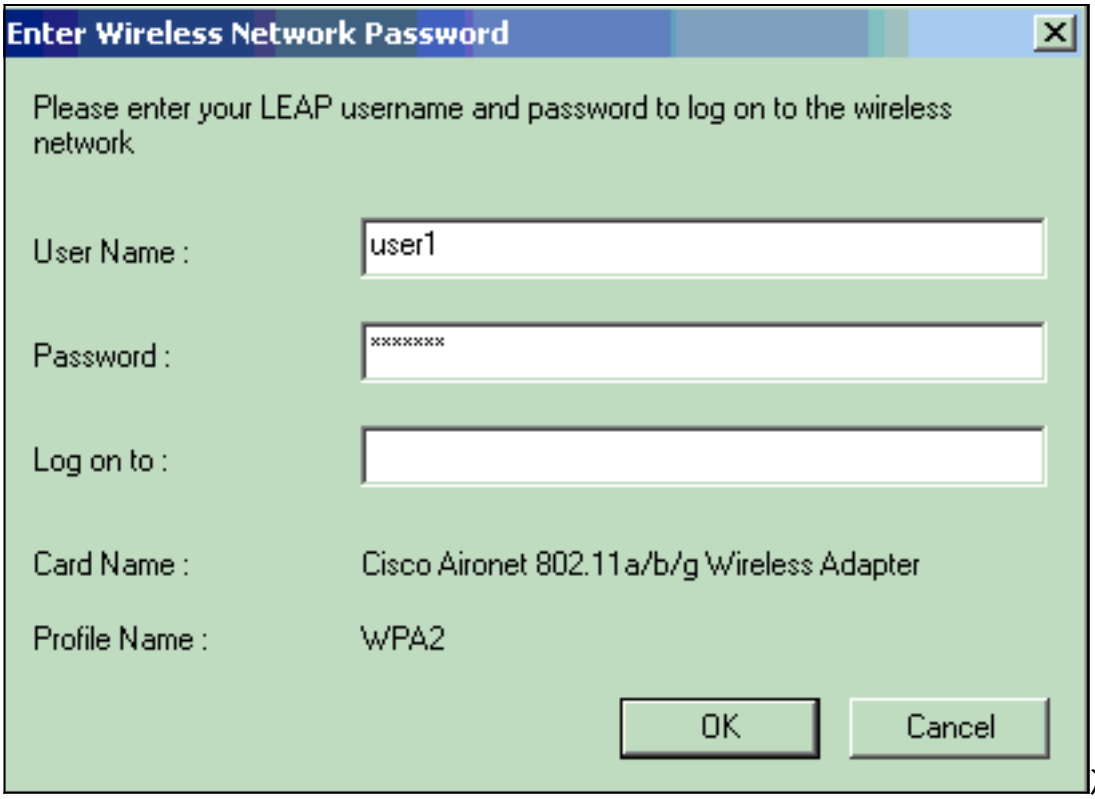


注：Microsoft Wireless Zero Configuration(WZC)を使用してクライアントアダプタを設定する場合、デフォルトではWZCではWPA 2は使用できません。そのため、WZC をイネーブルにしたクライアントで WPA 2 を稼働するためには、Microsoft Windows XP のホット フィックスをインストールする必要があります。インストールに関[しては、Microsoft Download Center - Update for Windows XP (KB893357)を参照して](#)ください 。ホット フィックスをインストールすれば、WZC で WPA 2 を設定できます。

確認

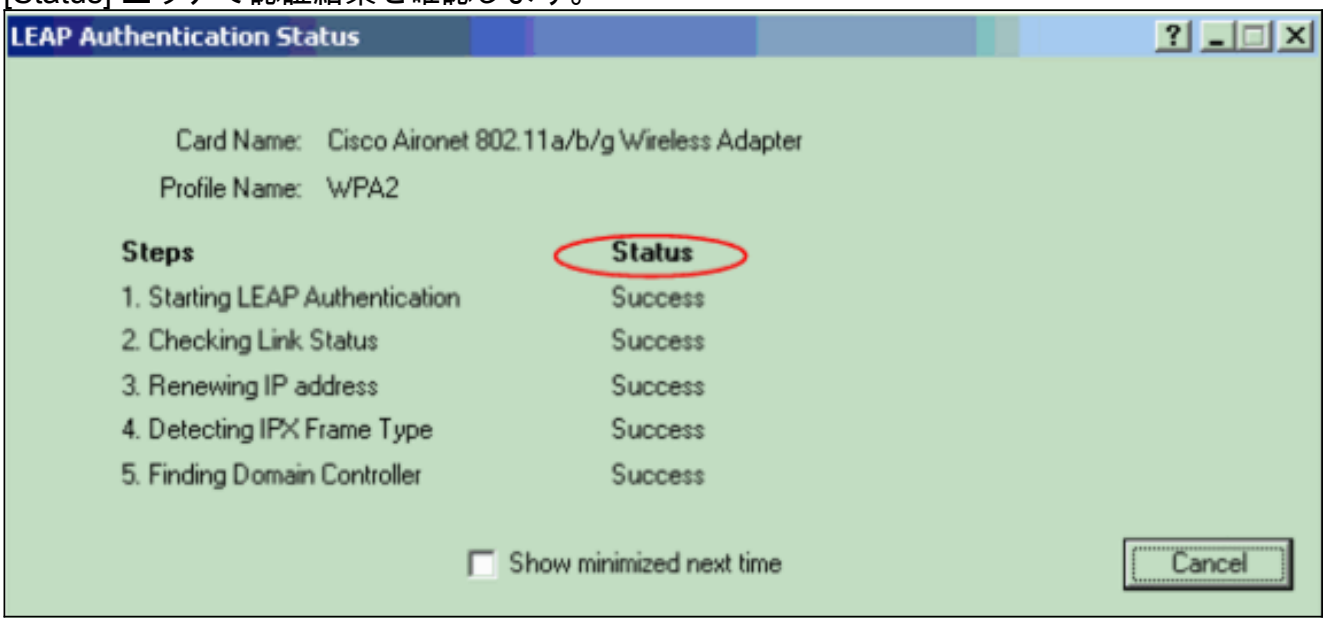
ここでは、設定が正常に機能しているかどうかを確認します。

1. [Enter Wireless Network Password] ウィンドウが表示されたら、ユーザ名とパスワードを入



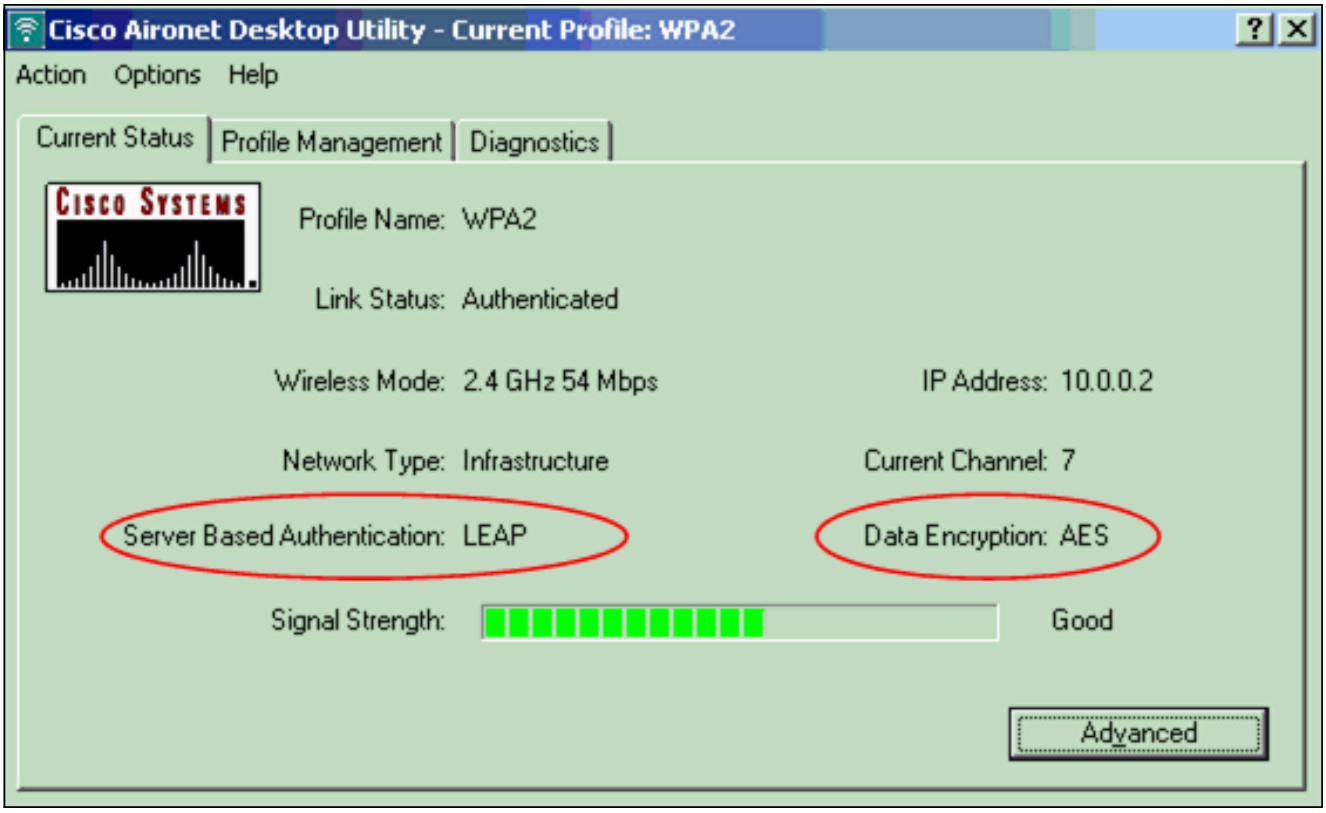
カします。次のウィンドウは [LEAP Authentication Status] です。このフェーズでは、ユーザのクレデンシャルがローカル RADIUS サーバに照会されます。

2. [Status] エリアで認証結果を確認します。



認証が成功した場合は、クライアントはワイヤレス LAN に接続します。

3. ADU の現在の状態をチェックして、クライアントが AES 暗号化と LEAP 認証を使用していることを確認します。この例では、WLAN で LEAP 認証と AES 暗号化を使用する WPA 2 が実装されていることを示しています。



4. AP/ブリッジ イベント ログをチェックして、クライアントが WPA 2 で正常に認証されたことを確認します。

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

パーソナル モードでの設定

Personal モードという用語は、PSK のみの動作モードで認証の相互運用が可能であることが確認された製品を指します。このモードでは、AP およびクライアント上での PSK の手動設定が必要です。PSK は、パスワードまたは認証コードをクライアント ステーションおよび AP の両方で使

用して、ユーザを認証します。認証サーバは不要です。クライアントは、クライアント パスワードが AP パスワードに一致した場合のみ、ネットワークにアクセスできます。また、このパスワードにより提供されるキー関連情報を使用して、TKIP または AES はデータ パケットの暗号化に使用する暗号化キーを生成します。パーソナル モードは SOHO 環境を対象としており、エンタープライズ環境では安全と見なされていません。このセクションでは、Pnterprise 動作モードに WPA 2 を実装するために必要な設定について説明します。

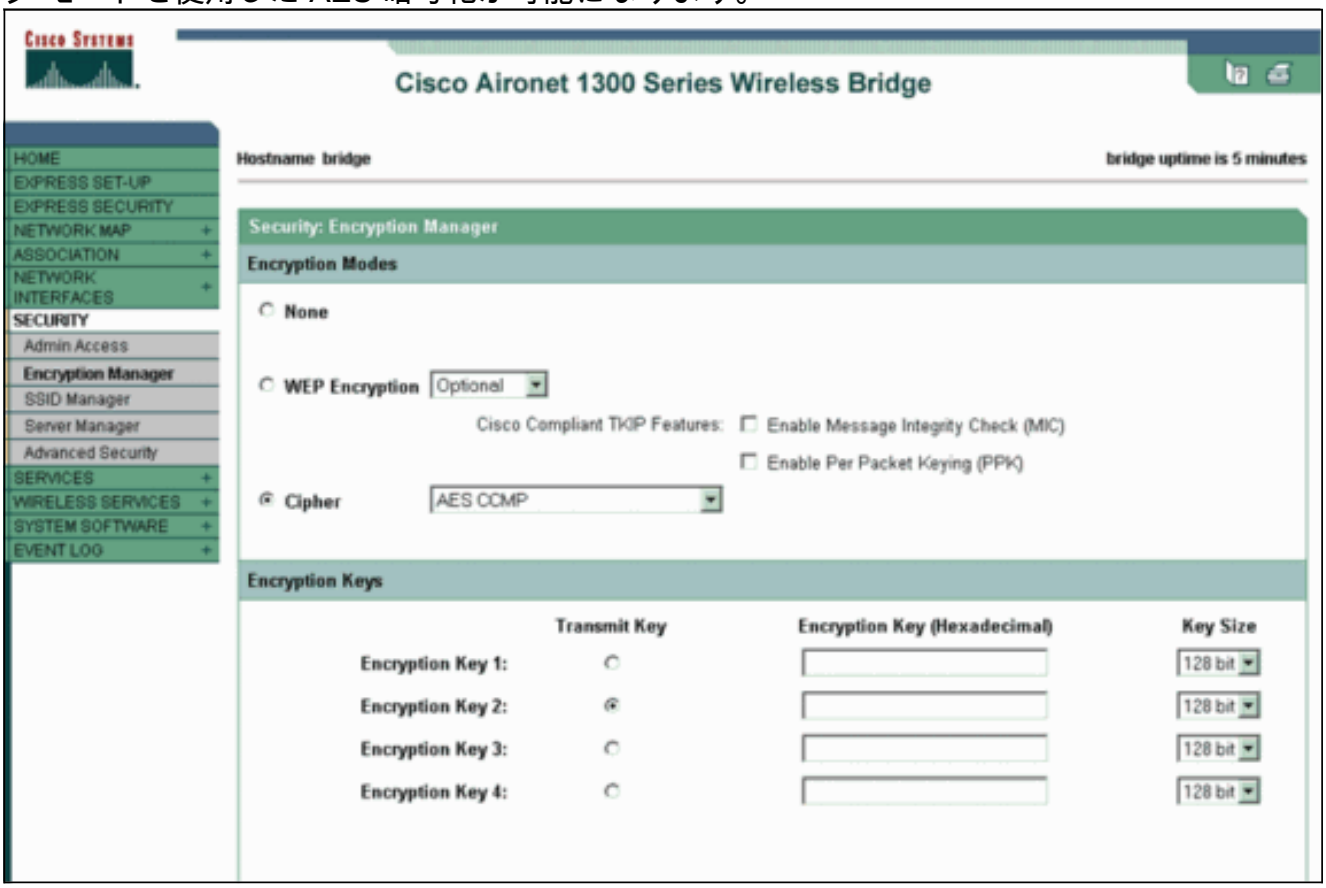
ネットワークのセットアップ

このセットアップでは、Aironet 1310G AP/ブリッジにより、WPA 2 互換のクライアント アダプタでユーザが認証されます。キー管理には、AES-CCMP 暗号化が設定された WPA 2 PSK が使用されます。「AP の設定」および「クライアント アダプタの設定」のセクションでは、AP とクライアント サーバでの設定について説明しています。

AP の設定

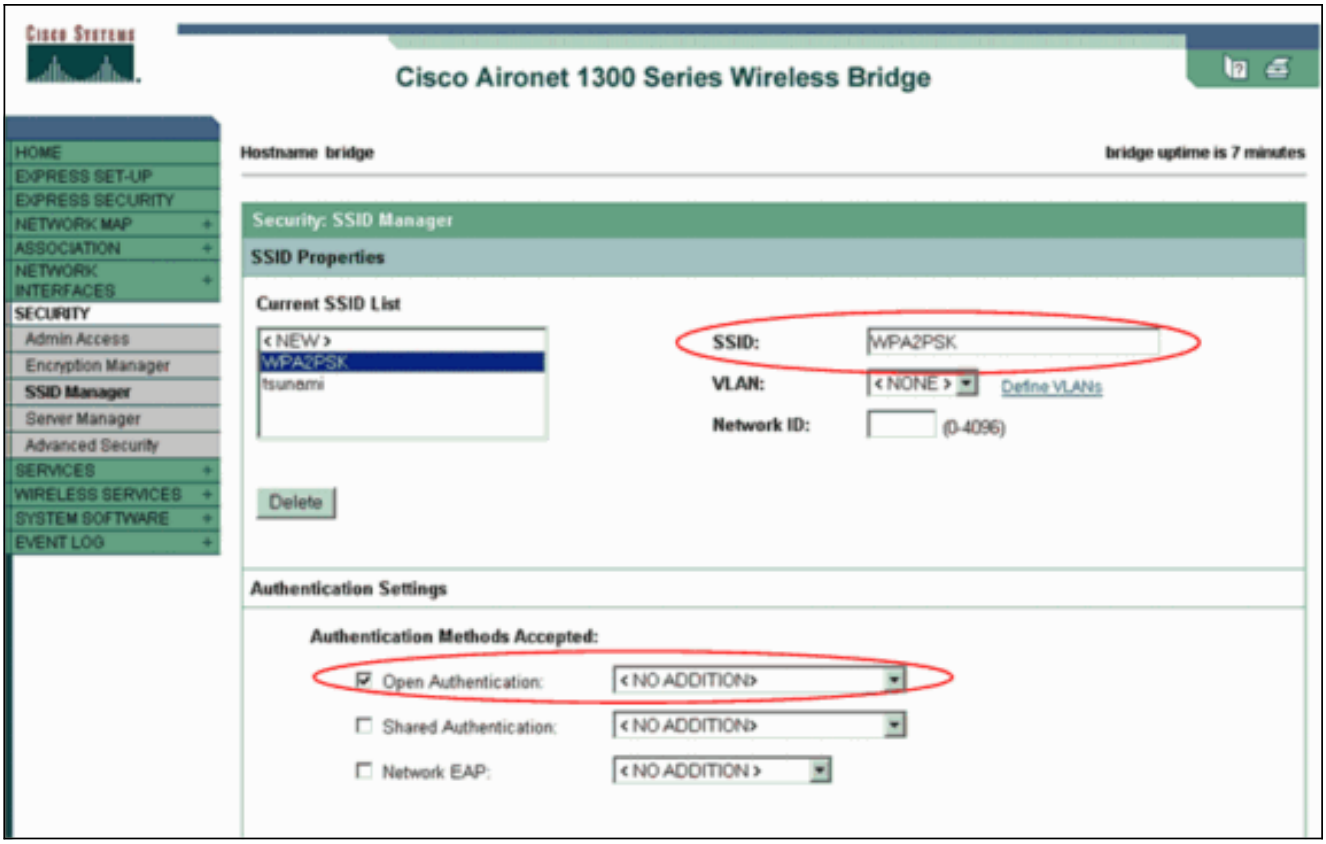
次のステップを実行します。

1. 左側のメニューで [Security] > [Encryption Manager] を選択して、次の動作を実行します。[Cipher] メニューで、[AES CCMP] を選択します。これを選択すると、CCMP によるカウンタ モードを使用した AES 暗号化が可能になります。

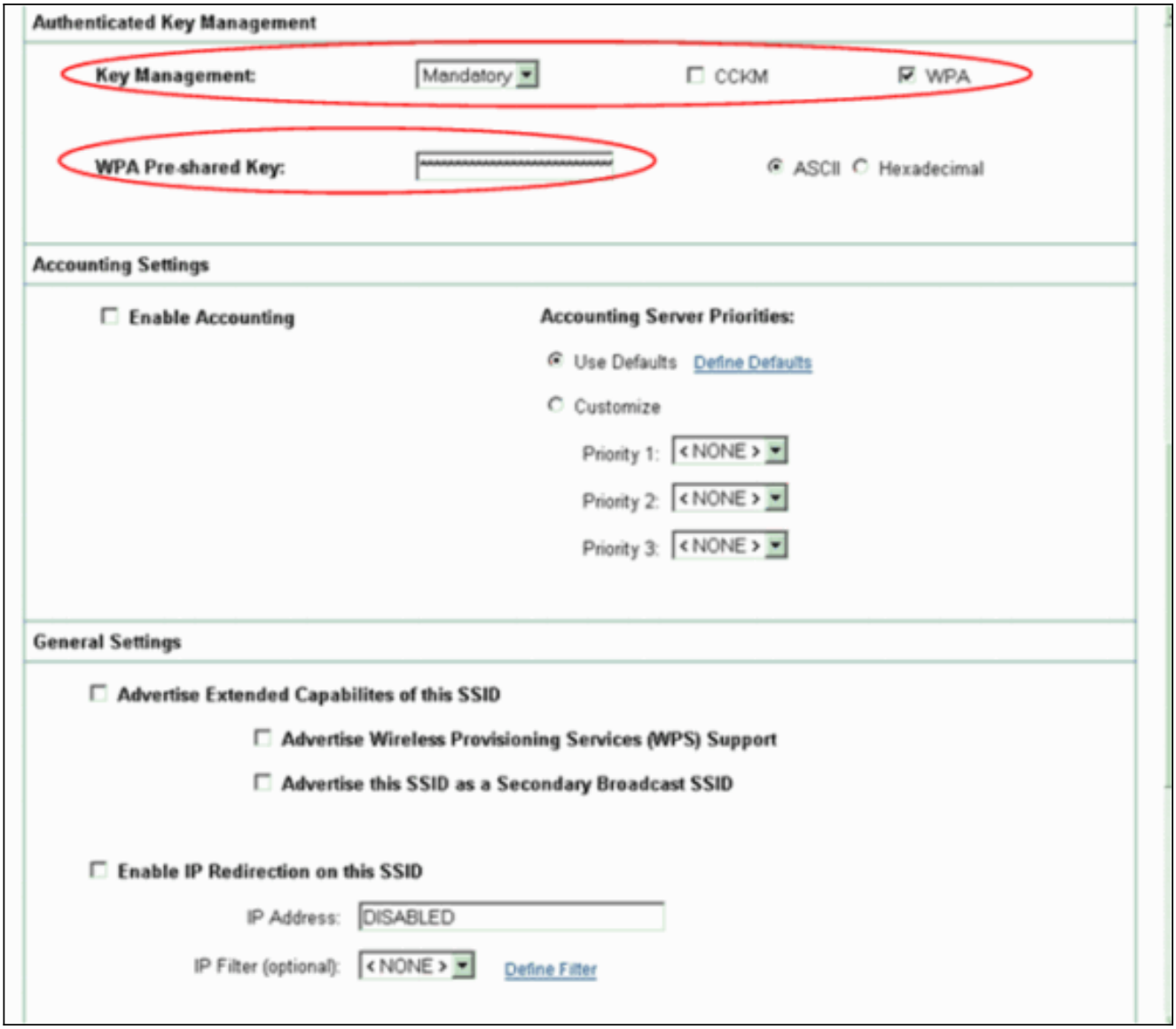


[Apply] をクリックします。

2. [Security] > [SSID Manager] を選択し、WPA 2 で使用する新しい SSID を作成します。[Open Authentication] チェックボックスをオンにします。



[Authenticated Key Management] エリアまで、[Security: SSID Manager] ウィンドウを下にスクロールし、次の手順を実行します。[Key Management] メニューで、[Mandatory] を選択します。右側の [WPA] チェックボックスをオンにします。



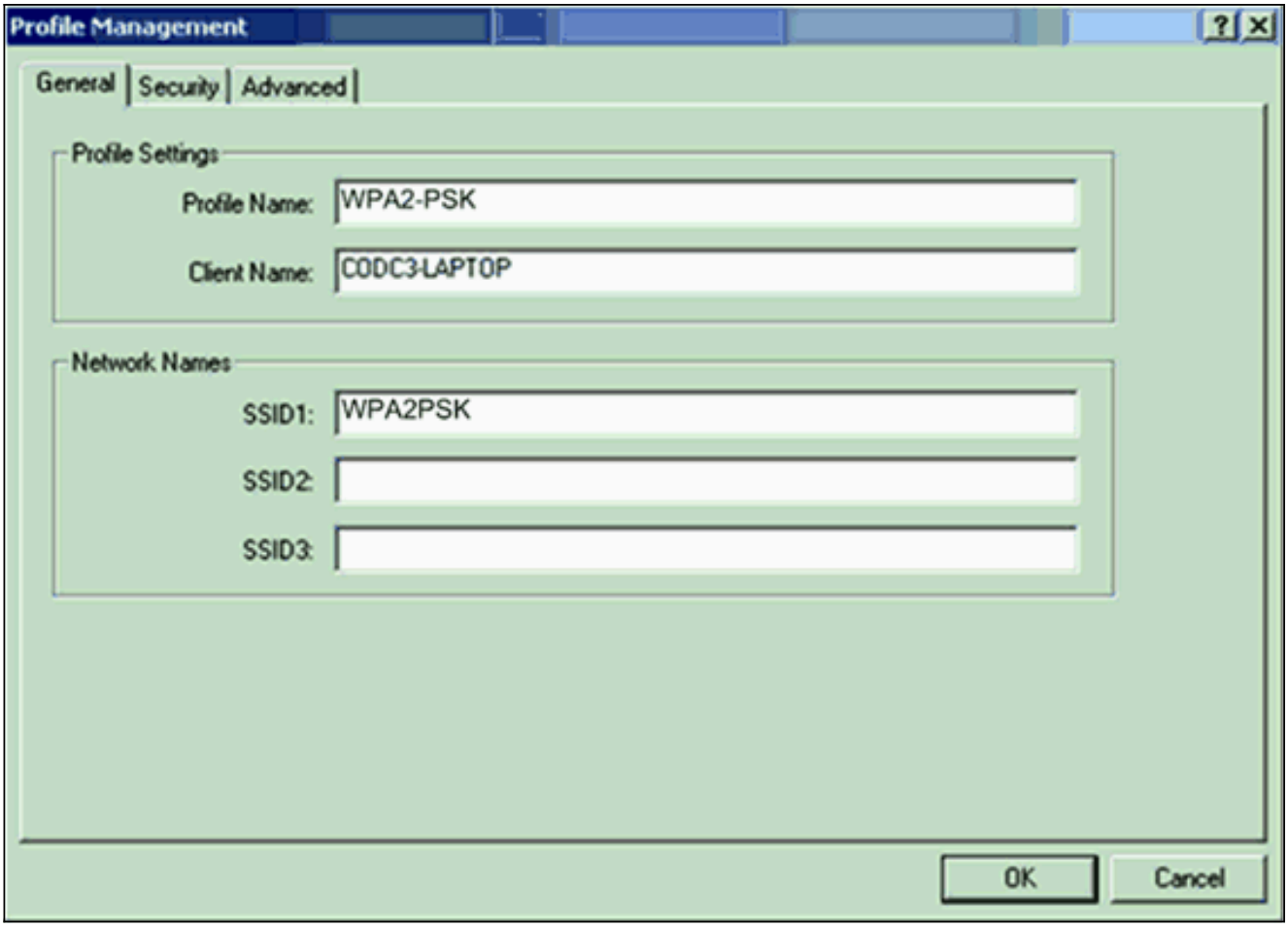
WPA PSK 共有秘密キーまたは WPA PSK パスフレーズ キーを入力します。このキーは、クライアント アダプタで設定されている WPA PSK キーと一致する必要があります。[Apply] をクリックします。

これで、AP はワイヤレス クライアントからの認証要求を受け付けることができるようになりました。

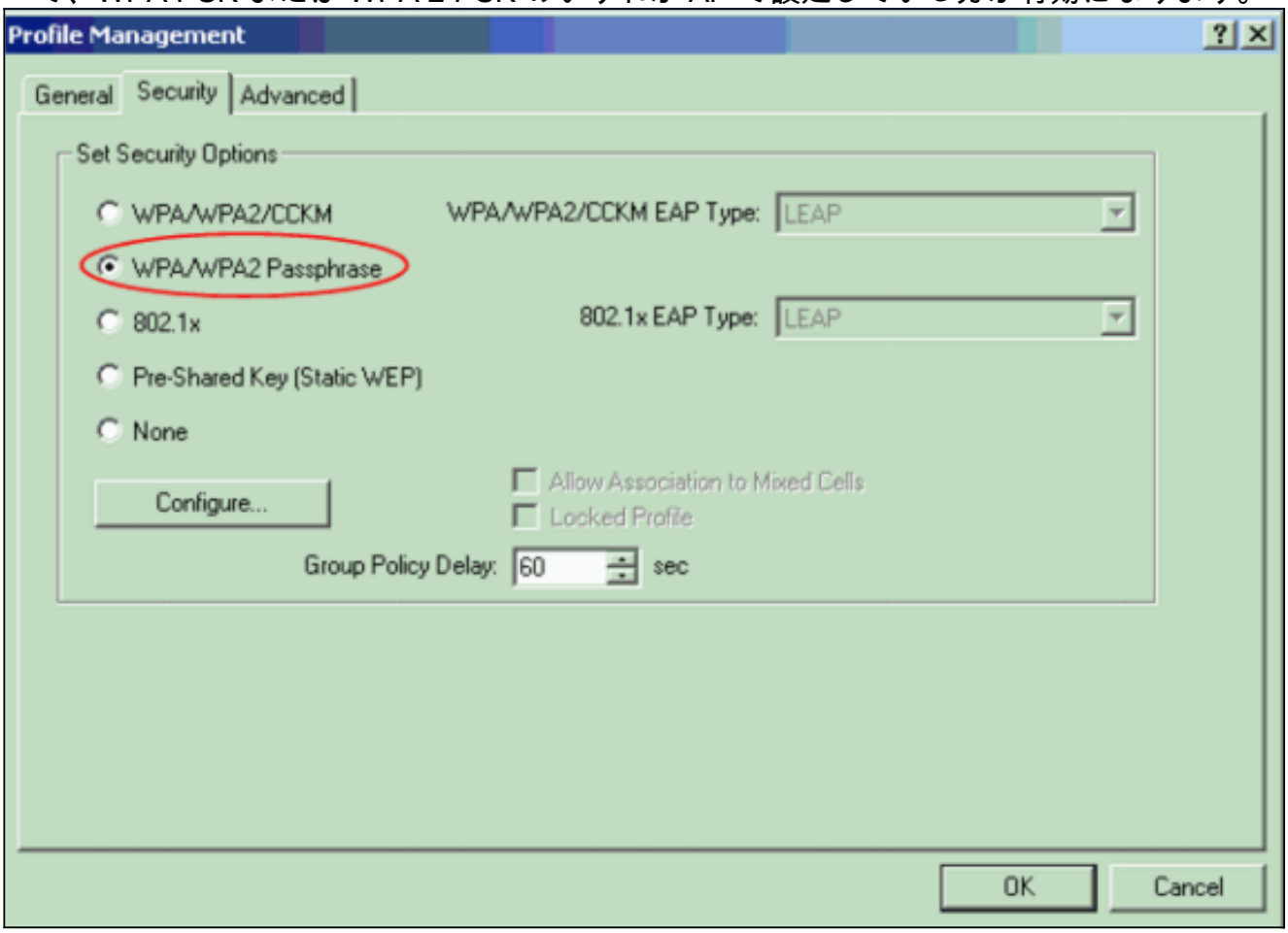
クライアント アダプタの設定

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。新しいウィンドウに、WPA 2 PSK モード動作設定の設定場所が表示されます。[General] タブで、クライアント アダプタが使用するプロファイル名と SSID を入力します。この例では、プロファイル名は WPA2-PSK、SSID は WPA2PSK です。**注**：SSIDは、APでWPA 2 PSK用に設定したSSIDと一致している必要があります。



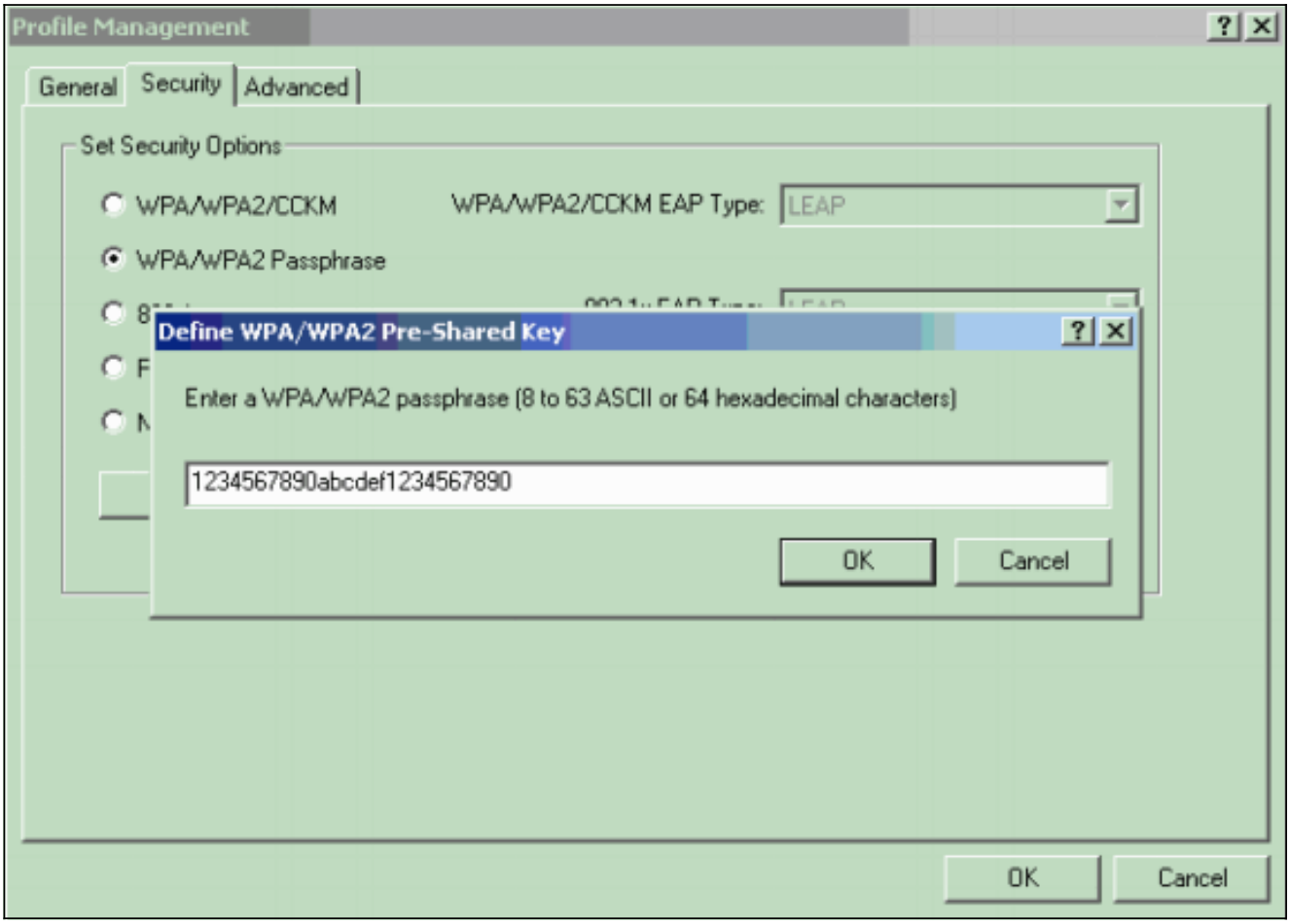
2. **[Security]** タブをクリックして、**[WPA/WPA2 Passphrase]** をクリックします。この操作によって、WPA PSK または WPA 2 PSK のいずれか AP で設定している方が有効になります。



3. [Configure] をクリックします。[Define WPA/WPA2 Pre-Shared Key] ウィンドウが表示され

ます。

4. システム管理者から WPA/WPA2 パスフレーズを入手し、[WPA/WPA2 passphrase] フィールドにパスフレーズを入力します。インフラストラクチャ ネットワーク内の AP 用のパスフレーズか、アドホック ネットワーク内の他のクライアント用のパスフレーズを入手します。パスフレーズを入力する場合は、次のガイドラインに従ってください。WPA/WPA2 パスフレーズには 8 ~ 63 文字の ASCII テキスト文字または 64 桁の 16 進数が含まれている必要があります。クライアント アダプタの WPA/WPA2 のパスフレーズは、通信に使用する AP のパスフレーズに一致している必要があります。



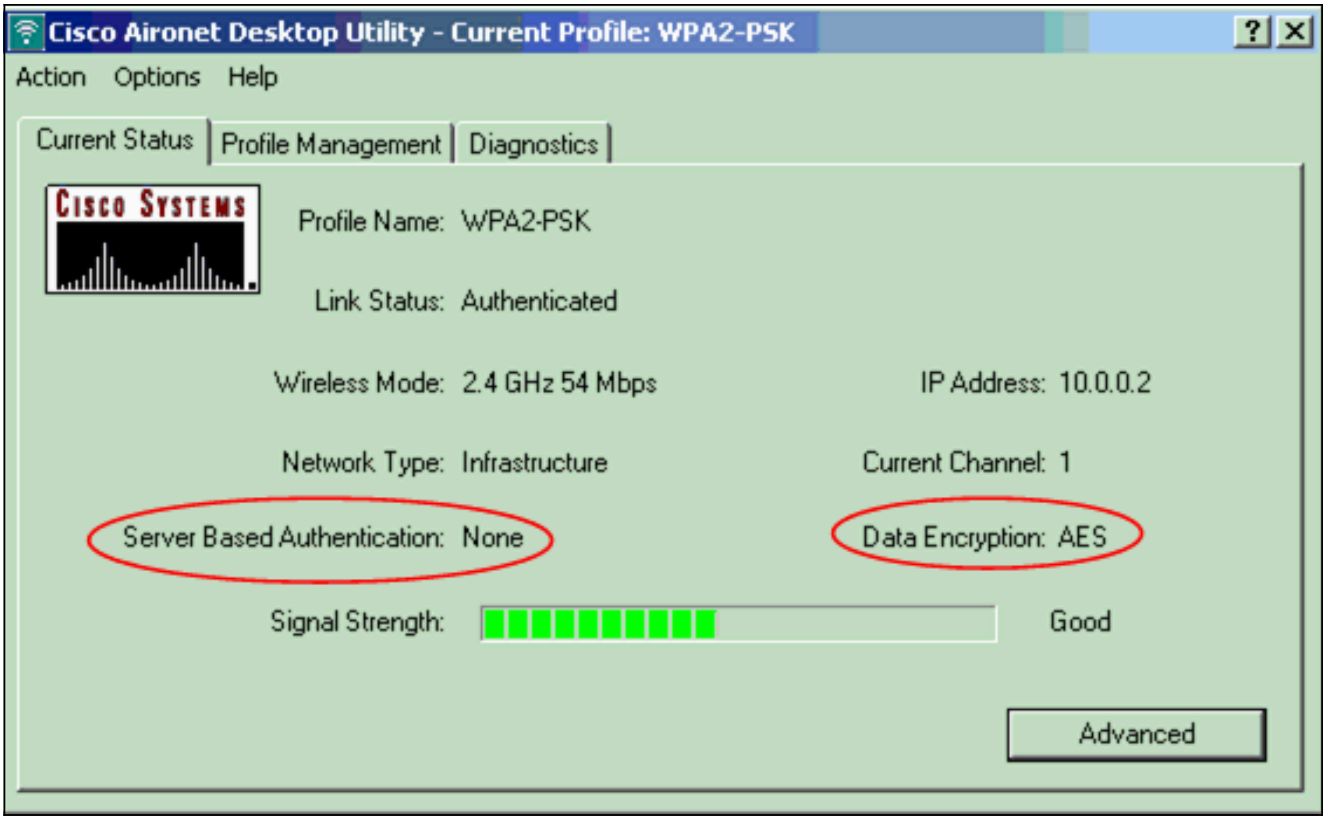
5. [OK] をクリックしてパスフレーズを保存し、[Profile Management] ウィンドウに戻ります。

確認

ここでは、設定が正常に機能しているかどうかを確認します。

WPA 2 PSK プロファイルをアクティブにした後、AP は WPA 2 パスフレーズ (PSK) に基づいてクライアントを認証し、WLAN へのアクセスを提供します。

1. ADU の現在の状態をチェックして、正常に認証されたことを確認します。このウィンドウは一例です。このウィンドウは、使用されている暗号化は AES であり、サーバベースの認証は実行されていないことを示します。



2. AP/ブリッジ イベント ログをチェックして、クライアントが WPA 2 PSK 認証モードで正常に認証されたことを確認します。

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- 暗号スイートと WEP の設定
- 認証タイプの設定

- WPA 設定の概要
- WPA2 - Wi-Fi Protected Access 2
- WPA混合モードの動作とは何ですか。また、APでWPA混合モードを設定するにはどうすればよいのですか。
- 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

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。