Wi-Fi Protected Access 2（WPA 2）の設定例

目次

はじめに

このドキュメントでは、ワイヤレス LAN（WLAN）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）を使用します。

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:** 情報 WLAN セキュリティ ソリューションのための Cisco Aironet Wireless LAN セキュリティの概要を on Cisco 参照して下さい。

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くものです。

- Cisco IOS® ソフトウェア リリース 12.3(2)JA を実行する Cisco Aironet 1310G Access Point （ AP ） /Bridge
- ファームウェア 2.5 を実行する Aironet 802.11a/b/g CB21AG クライアントアダプタ
- Aironet デスクトップ ユーティリティ（ ADU ）その実行ファームウェア 2.5

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 ソフトウェアに対応しないです。 CB21AG および PI21AG カードと ADU を使用して下さい他のすべての Aironetクライアントアダプタ Aironet Client Utility （ ACU ）を使用して下さい。 CB21AG カードおよび ADU をインストールする方法で詳細についてはクライアントアダプタをインストールすることを参照して下さい。

注: この資料は統合されたアンテナがある AP/bridge を使用します。 外部アンテナを必要とする AP/bridge を使用したら、アンテナが AP/bridge に接続されるようにして下さい。 さもなければ、AP/bridge は無線ネットワークに接続することができません。 ある特定の AP/bridge モデルは統合されたアンテナが他が一般のオペレーションのための外部アンテナを必要とする一方、付いています。 内部か外部アンテナが付いている AP/bridge モデルの情報に関しては、適切なデバイスの発注 ガイド/製品ガイドを参照して下さい。

本書の情報は、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、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

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 はネイティブ WLAN の脆弱性に対処する Wi-Fi 同盟からの標準ベース セキュリティソリューションです。 WPA は WLANシステムに拡張 な データ 保護およびアクセスコントロールを提供します。 WPA はオリジナル IEEE 802.11 セキュリティインプリメンテーションのすべての既知 Wired Equivalent Privacy（ WEP ）脆弱性に対処し、エンタープライズおよび small office，home office （ SOHO ）両方環境の WLAN に即時セキュリティソリューションを持って来ます。

WPA2 は次世代の Wi-Fi セキュリティ機能です。 WPA 2 は批准された IEEE 802.11i 規格の Wi-Fi 同盟相互運用可能な実装です。 WPA 2 は国立標準技術研究所 （ NIST ）を- Cipher Block Chaining Message Authentication Code プロトコル（ CCMP ）のカウンター モードの使用の推奨される高度暗号化規格（ AES ）暗号化アルゴリズム設定します。 AES カウンター モードは 128 ビット暗号化キーとのデータの 128 ビット ブロックを一度に暗号化するブロック 暗号です。 CCMP アルゴリズムはワイヤレス フレームにデータ元の認証およびデータ統合を提供するメッセージの整合性コード（ MIC ）を生成 します。

注: CCMP はまた CBC-MAC と言われます。

AES が Temporal Key Integrity Protocol (TKIP) より強化暗号化を提供するので WPA 2 は WPA よりセキュリティの上位レベルを提供します。 TKIP は WPA が使用する暗号化アルゴリズムです。 WPA 2 は各アソシエーションの新しいセッションキーを作成します。 ネットワークの各クライアントのために使用する暗号化キーはそのクライアントにユニーク、特定です。 最終的に、各パケットは一意キーを使って送信 された 地上波である暗号化されます。 セキュリティは新しく、ユニークな暗号キーの使用と No 鍵再使用があるので強化されます。 WPA はまだセキュアと考慮され、ずっと TKIP は壊れていません。 ただし、Cisco は顧客が WPA 2 にできるだけ早く移行することを推奨します。

WPA および WPA は 2 両方 2 つの動作モードをサポートします:

- エンタープライズ モード
- 個人的なモード

この資料は WPA 2.とこれら二つのモードの実装を説明します。

Ciscoエアロネット 機器が付いている WPA 2 サポート

WPA 2 はこの機器でサポートされます:

- 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 をか以降使用して下さい。

WPA 2 および AES はまたサポートされます:

- 部品番号 AIR-RM21A および AIR-RM22A が付いている Aironet 1200 シリーズ無線モジュール**注:** 部品番号 AIR-RM20A が付いている Aironet 1200 無線モジュールは WPA 2.をサポートしません。
- ファームウェア バージョン 2.5 が付いている 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 WPA 2 をので無線欠乏 AES サポート サポートしません。

注: Cisco Aironet 1400 シリーズ ワイヤレスブリッジは WPA 2 か AES をサポートしません。

エンタープライズ モードの設定

条件 **エンタープライズ モードは**両方で相互運用可能認証における事前共有キー (PSK) および IEEE 802.1x であるために動作モード テストされる製品を示します。 802.1X はいろいろな認証機構および強化暗号化アルゴリズムを助けて柔軟性が理由でよりセキュアのレガシー 認証フレームワークであると考慮されます。 エンタープライズ モードの WPA 2 は 2 フェーズに認証を行います。 開いた認証の設定は序盤に発生します。 第 2 フェーズは EAP メソッドの 1 つの 802.1X 認証です。 AES は暗号化メカニズムを提供します。

エンタープライズ モードでは、クライアントおよび認証サーバは EAP 認証方式の使用と互い、およびクライアント および サーバ 生成するをマスター キー (PMK) 一対に認証します。 WPA 2 を使うと、サーバは PMK を動的に生成し、AP に PMK を渡します。

このセクションは設定を論議しますエンタープライズ 動作モードの WPA 2 を設定して必要であ

る。

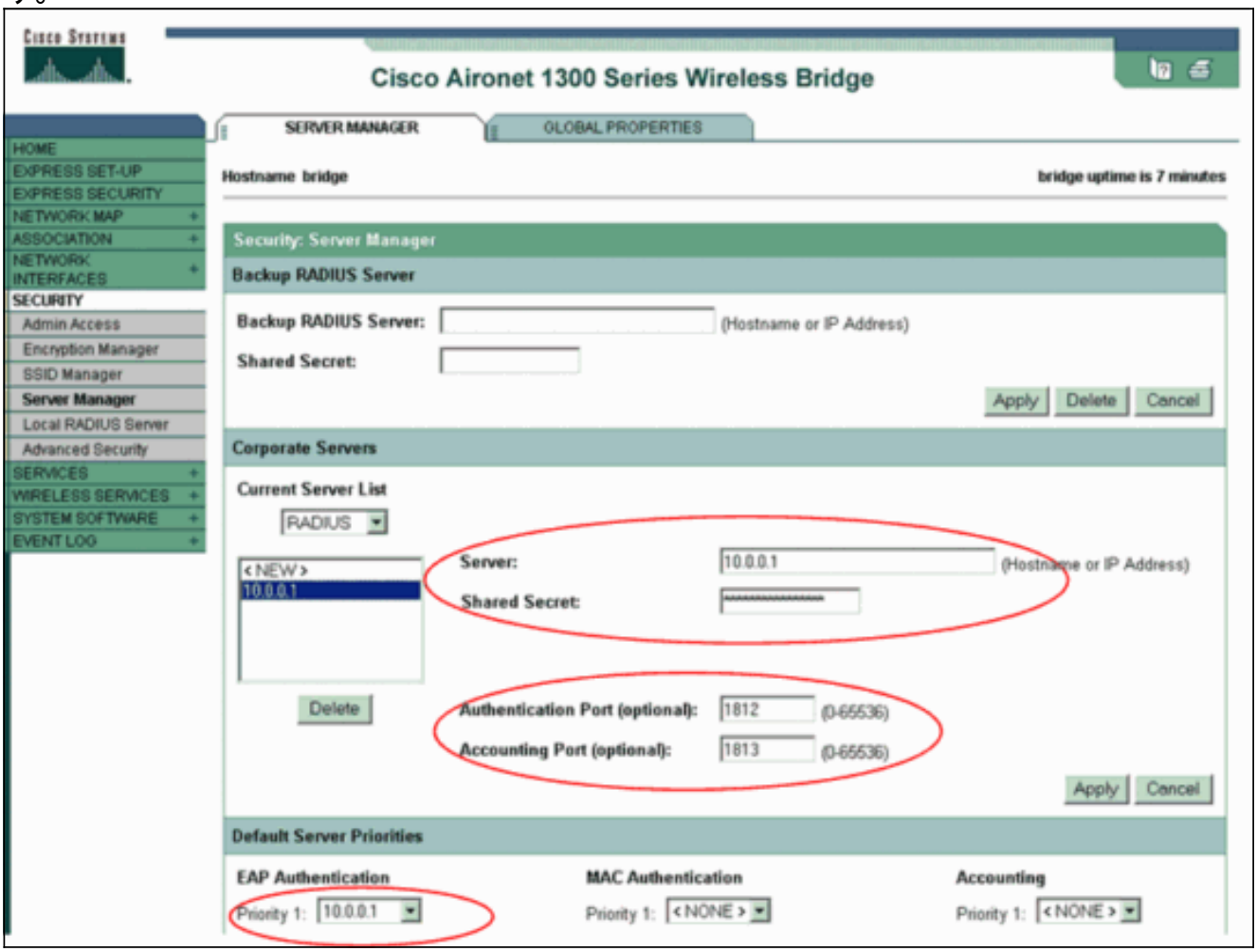
ネットワーク構成

動作するこの設定では、Aironet 1310G AP/Bridge は Cisco Lightweight Extensible Authentication Protocol （ LEAP ） WPA 2 互換性があるクライアントアダプタを持つユーザを認証します。 キー管理は AES-CCMP 暗号化が設定される WPA 2 の使用と行われます。 AP は LEAP 認証を動作するローカル RADIUSサーバで設定されます。 クライアントアダプタおよびこの設定を設定するために AP を設定して下さい。 セクションは AP を設定し、クライアントアダプタを示します AP およびクライアントアダプタの設定を設定します。

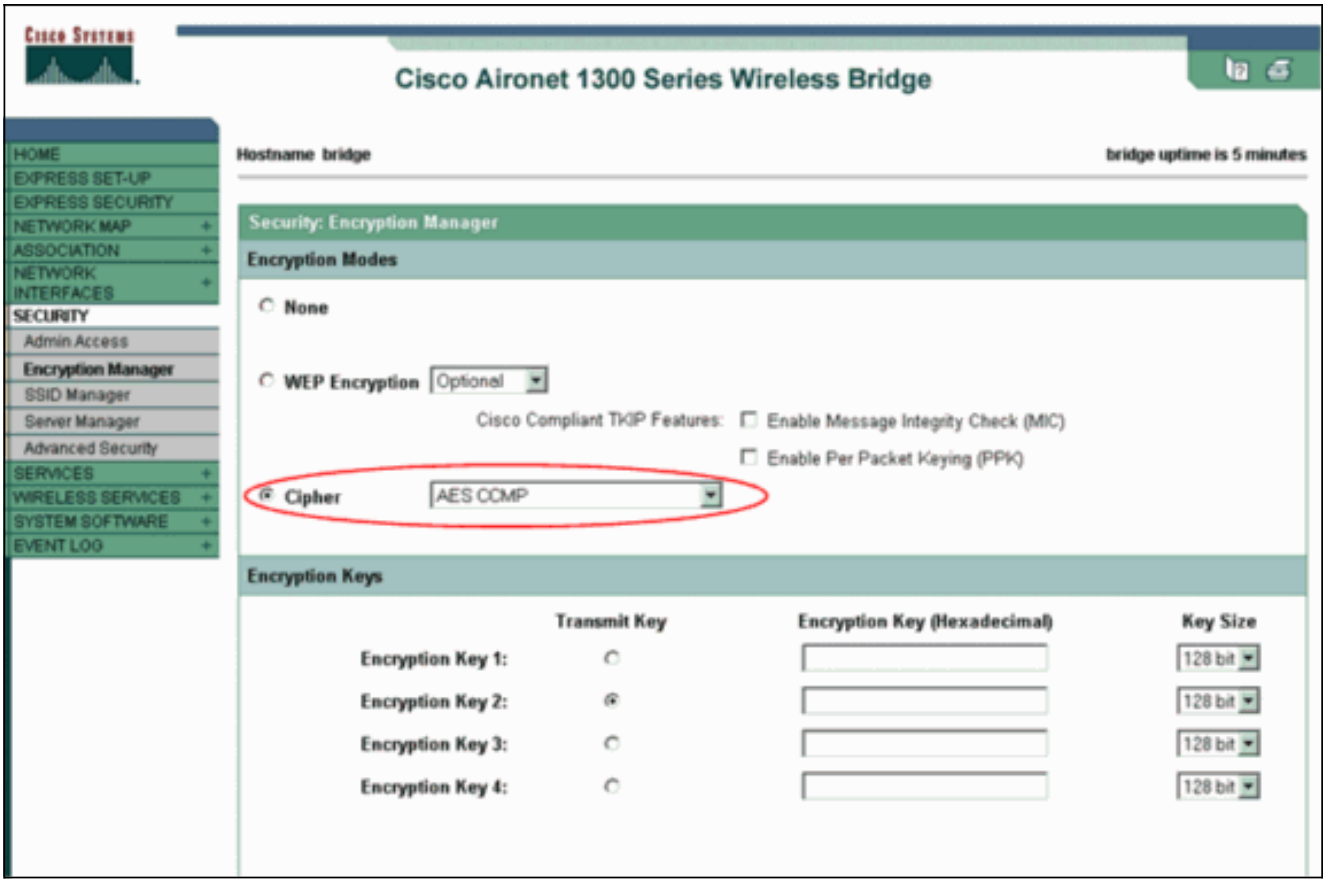
AP を設定して下さい

GUI を使用して AP を設定するためにこれらのステップを完了して下さい:

1. LEAP 認証を動作するローカル RADIUSサーバで AP を設定して下さい。左のメニューで Security > Server Manager の順に選択 し、RADIUSサーバの IP アドレス、ポートおよび共用シークレットを定義して下さい。この設定がローカル RADIUSサーバで AP を設定するので、AP の IP アドレスを使用して下さい。 ローカル RADIUSサーバ オペレーションのためのポート 1812 および 1813 を使用して下さい。既定のサーバー優先分野では、10.0.0.1 とデフォルト EAP 認証優先順位を定義して下さい。**注:** 10.0.0.1 はローカル RADIUSサーバです。

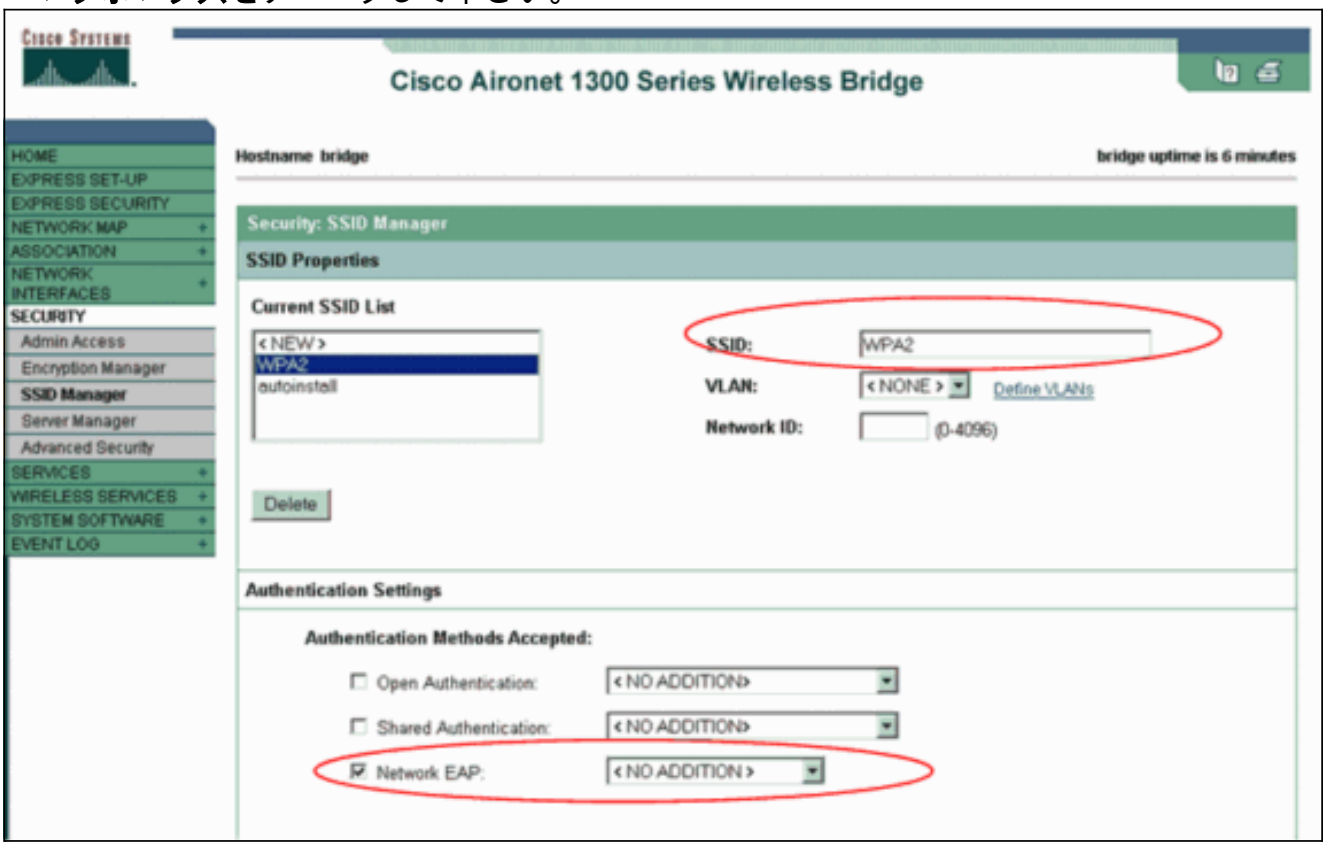


2. 左のメニューから Security > Encryption Manager の順に選択 し、これらのステップを完了して下さい:暗号メニューから、『AES CCMP』 を選択 して下さい。このオプションは CBC-MAC のカウンター モードの使用の AES 暗号化を有効に します。



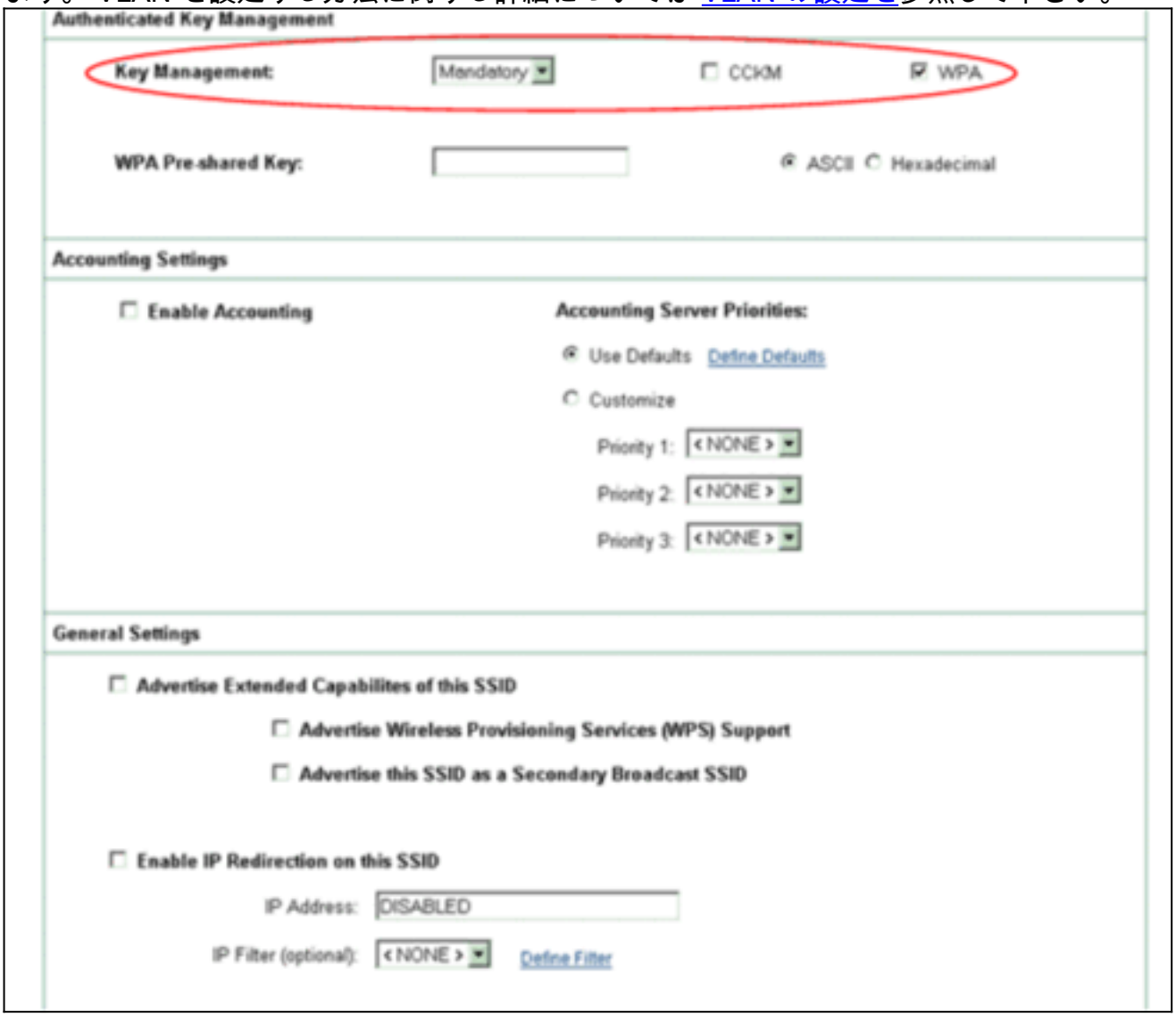
[Apply] をクリックします。

3. WPA 2.と併用するため新しいサービス セット ID（SSID）を Security > SSID Manager の順に選択 し、作成して下さい。認証方式によって受け入れられる領域の**ネットワーク Eap チェックボックスを**チェックして下さい。



注: 無線インターフェイスの認証種別を設定するときこれらのガイドラインを使用して下さい:Cisco クライアント—ネットワーク EAP を使用して下さい。（Cisco Compatible Extensions [CCX] -対応製品が）含まれているサード パーティ クライアント— EAP の使用

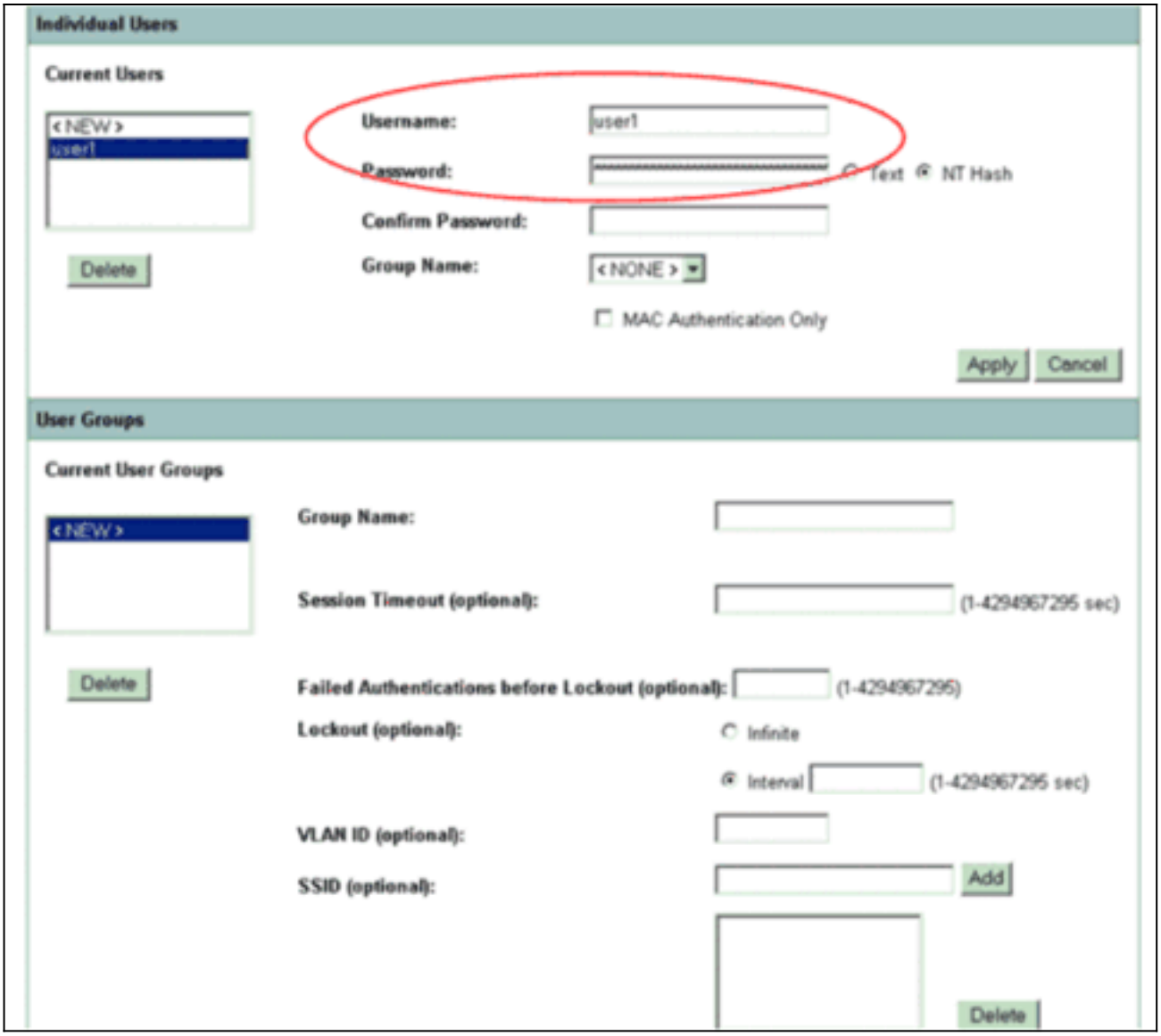
開いた認証。Cisco およびサード パーティ クライアント両方の組み合せ—ネットワーク EAP を選択し、EAP の認証を開いて下さい。セキュリティ SSID マネージャ ウィンドウを認証されたキー管理エリアにスクロールし、これらのステップを完了して下さい:キー管理メニューから、『Mandatory』 を選択 して下さい。右の **WPA チェックボックスを**チェックして下さい。[Apply] をクリックします。**注:** VLAN の定義はオプションです。 VLAN を定義する場合、この SSID の使用と関連付けるクライアントデバイスは VLAN にグループ化されます。 VLAN を設定する方法に関する詳細については VLAN の設定を参照して下さい。



4. これらのステップを Security > Local Radius Server の順に選択 し、完了して下さい:ウィンドウの上にある **General Set-up タブを**クリックして下さい。**LEAP チェックボックスを**チェックし、『Apply』 をクリック して下さい。ネットワーク アクセス サーバ エリアでは、RADIUSサーバの IP アドレスおよび共用シークレットを定義して下さい。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. General Set-up ウィンドウを個々の利用者域にスクロールし、個々のユーザを定義して下さい。ユーザグループの定義はオプションです。



この設定はネーム "user1" のユーザおよびパスワードを定義します。 また、設定はパスワードに NT ハッシュを選択します。 このセクションのプロシージャの完了が、AP クライアントからの認証要求を受け入れて準備ができていた後。 次のステップはクライアントアダプタを設定することです。

CLI 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
```

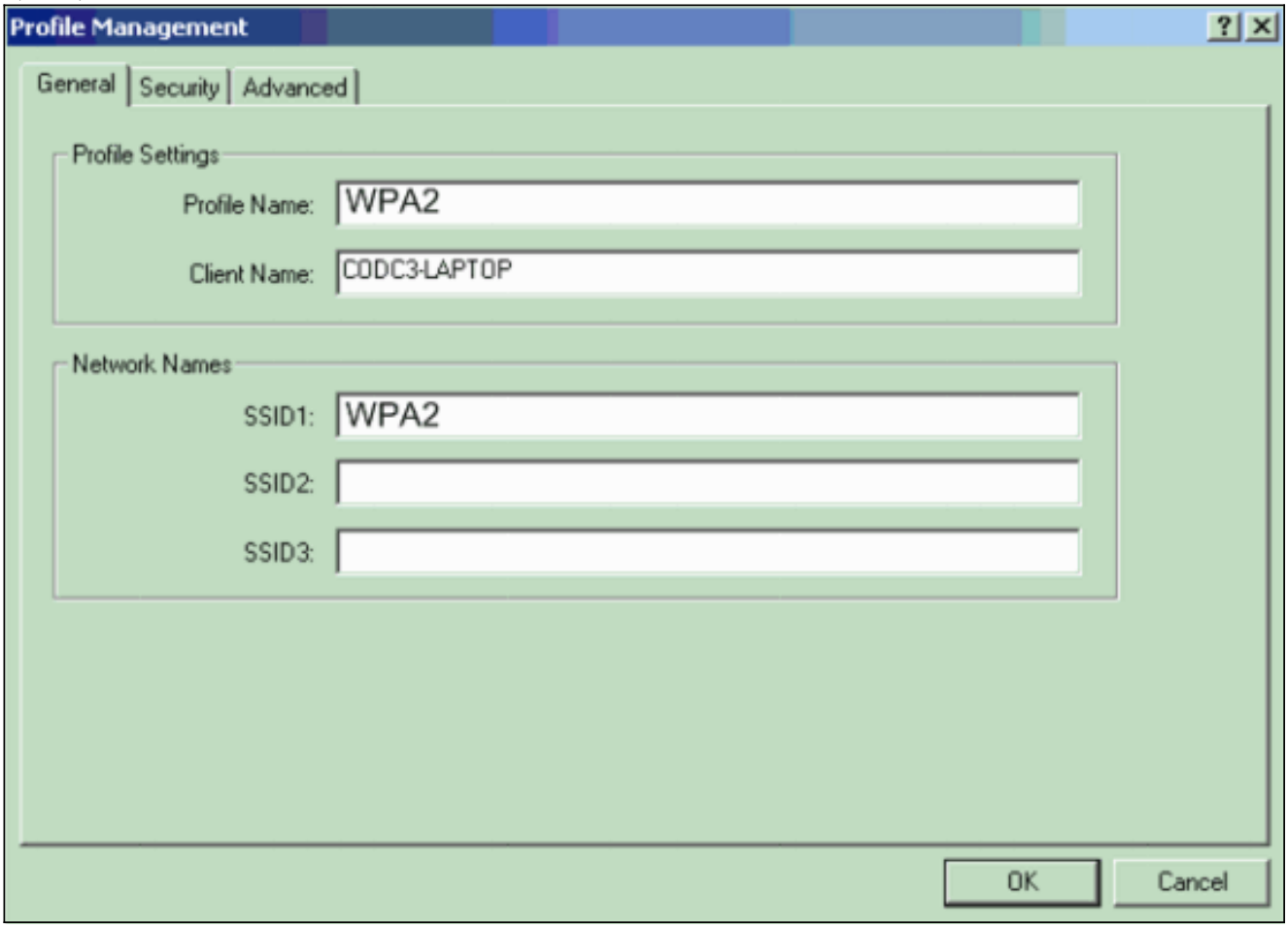
```
Dot11Radio0 no ip address no ip route-cache !
encryption vlan 1 key 1 size 128bit
   12345678901234567890123456 transmit-key
!---This step is optional !--- This value seeds the
initial key for use with !--- broadcast
[255.255.255.255] traffic. If more than one VLAN is !---
used, then keys must be 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を設定して下さい

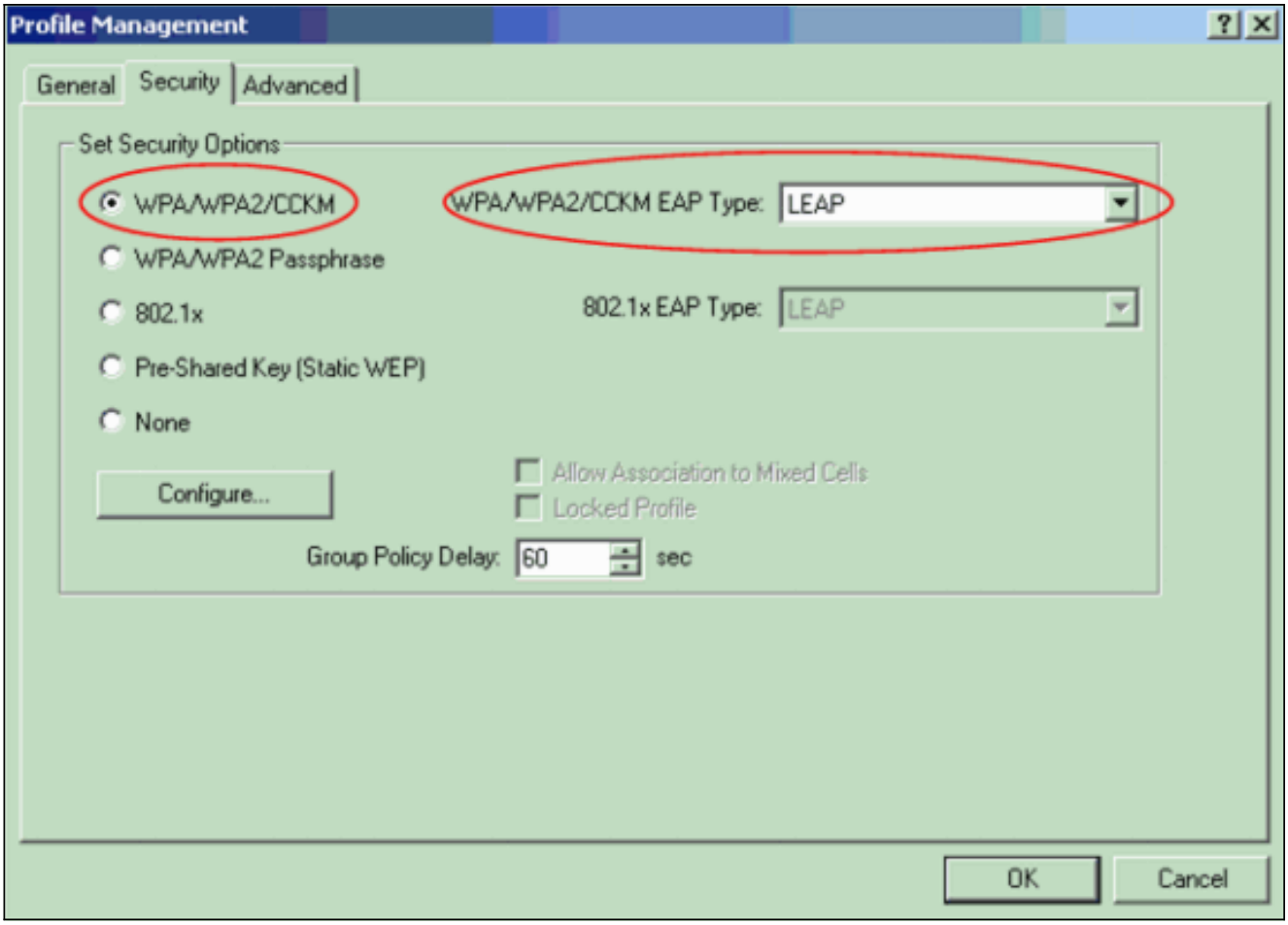
次の手順を実行します。

注: この資料はファームウェア 2.5 を実行し、ADU バージョン 2.5 が付いているクライアントアダプタの設定を説明する Aironet 802.11a/b/g クライアントアダプタを使用します。

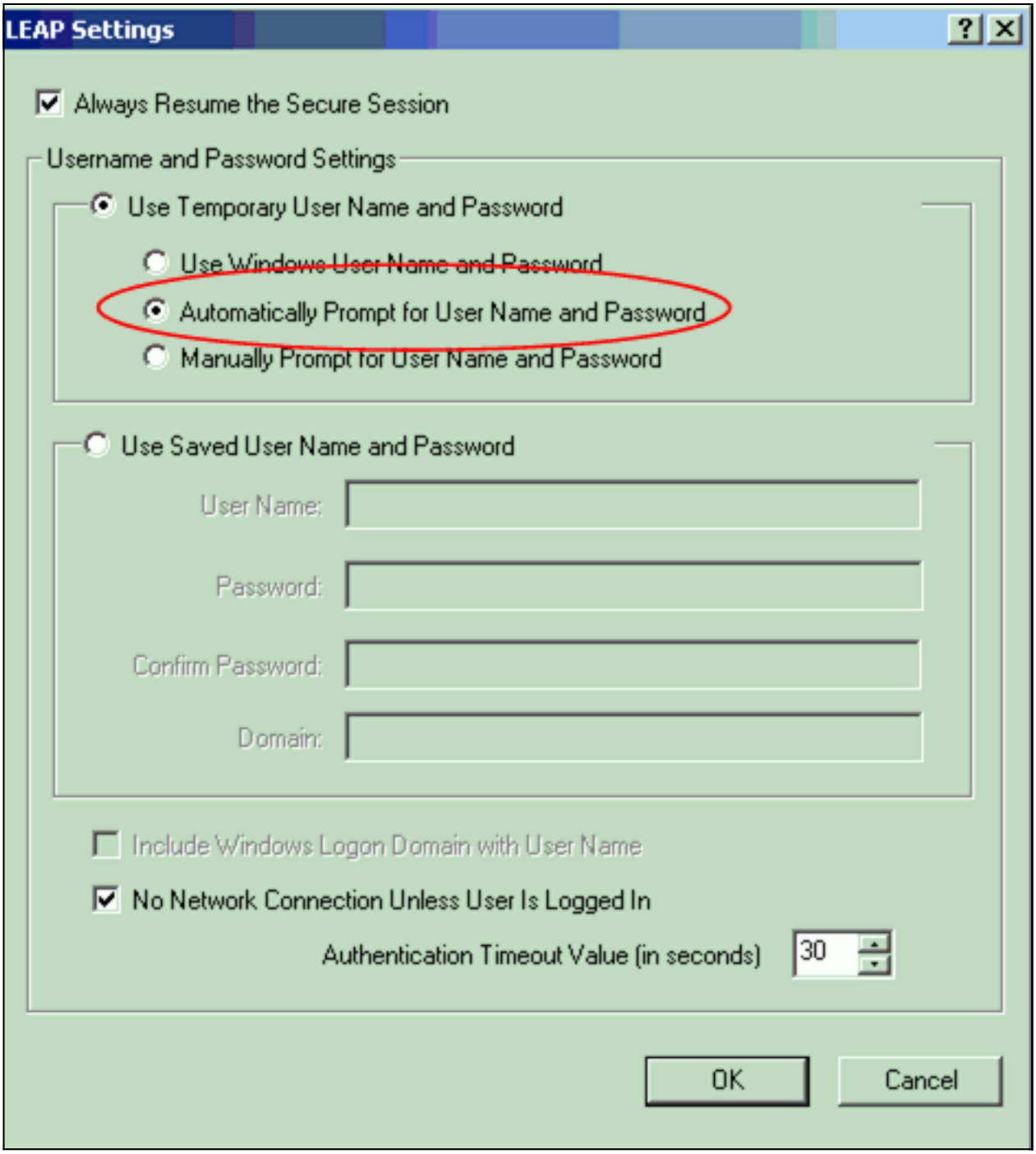
1. ADU の [Profile Management] ウィンドウで、[New] をクリックして新しいプロファイルを作成します。New ウィンドウは WPA 2 エンタープライズ モード オペレーションのための設定をどこに設定できるか表示します。 General タブの下で、クライアントアダプタが使用する SSID およびプロファイル名前を入力して下さい。この例では、プロファイル名および SSID は WPA2 です:**注:** SSID は WPA 2.のための AP で設定した SSID を一致する必要があります。



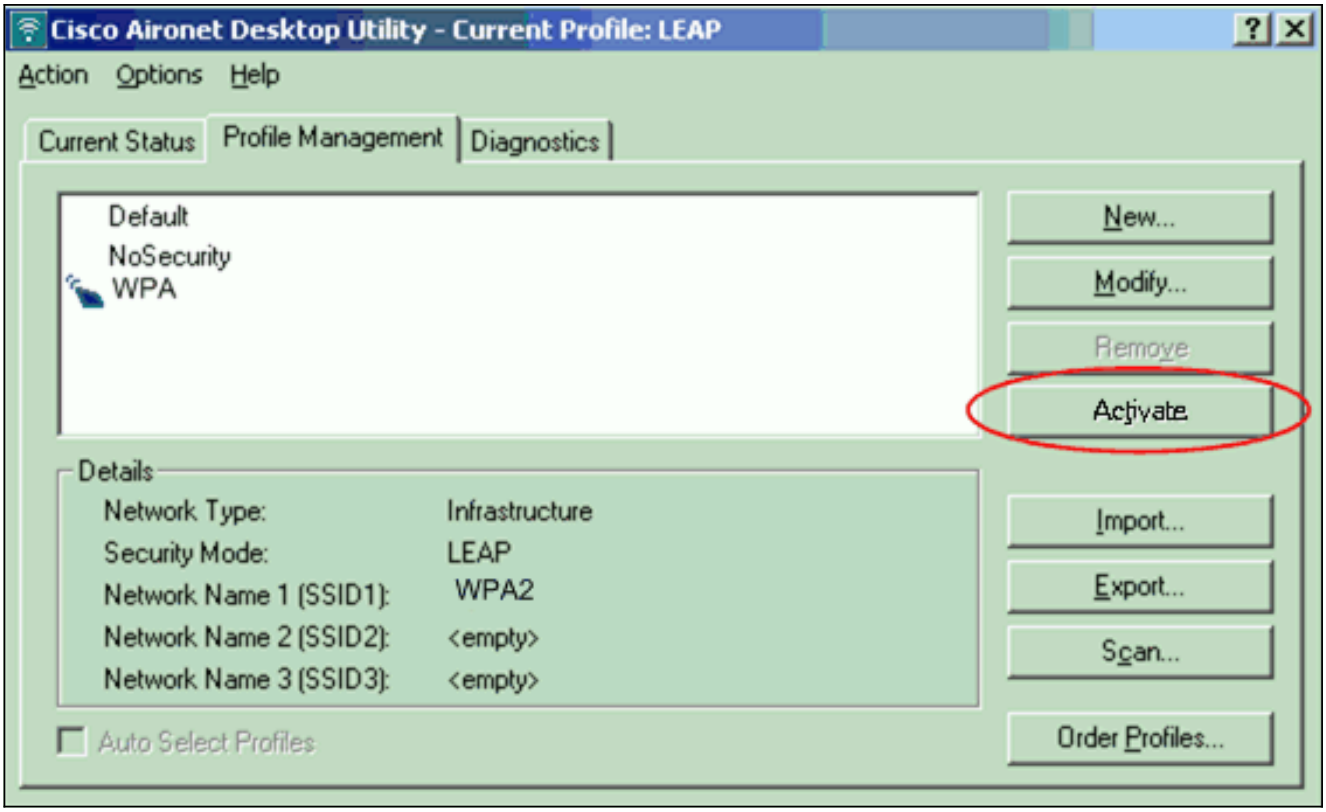
2. **Security タブを**クリックし、『WPA/WPA2/CCKM』 をクリック し、WPA/WPA2/CCKM EAP Type メニューから『LEAP』 を選択 して下さい。この操作は AP で設定するものはどれでも、WPA か WPA 2 を有効に します。



3. LEAP 設定を定義するために『Configure』 をクリック して下さい。
4. 適切なユーザ名 および パスワード設定を、必要条件に基づいて選択し、『OK』 をクリック して下さい。この設定はユーザネームおよびパスワードのためにオプションを自動的にプロンプト表示します選択します。 このオプションは LEAP 認証が起こるとき手動で ユーザネームおよびパスワードを入力することを可能にします。



5. プロファイル 管理ウィンドウを終了するために『OK』 をクリック して下さい。
6. クライアントアダプタのこのプロファイルを有効に するために『Activate』 をクリック して下さい。

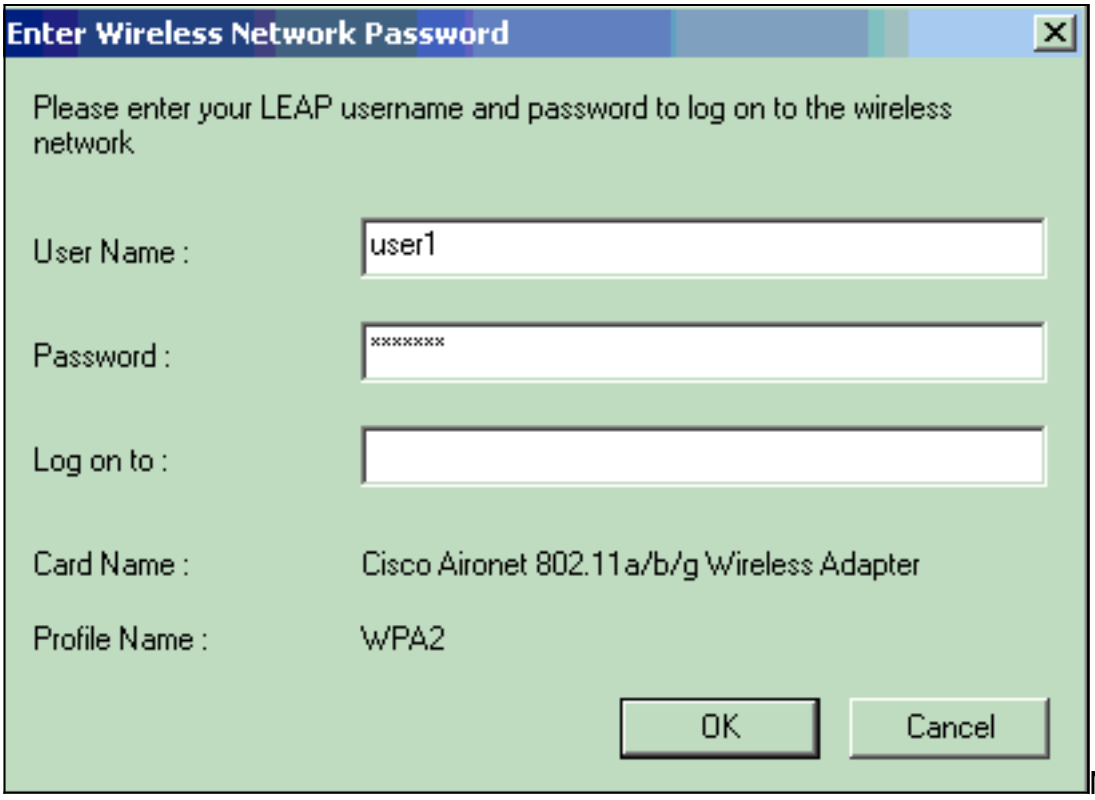


注: クライアントアダプタを、デフォルトで設定すればのに、Microsoft ワイヤレス ゼロ設定（WZC）を WPA 2 でなければ WZC と利用可能使用すれば。 このように、WZC 有効に されたクライアントを WPA 2 を実行することを許可するために Microsoft Windows XP 用の熱い修正をインストールして下さい。 参照して下さい Microsoft ダウンロード センター-インストールの Windows XP （KB893357 ）のためのアップデート。熱い修正をインストールした後、WZC で WPA 2 を設定できます。

確認

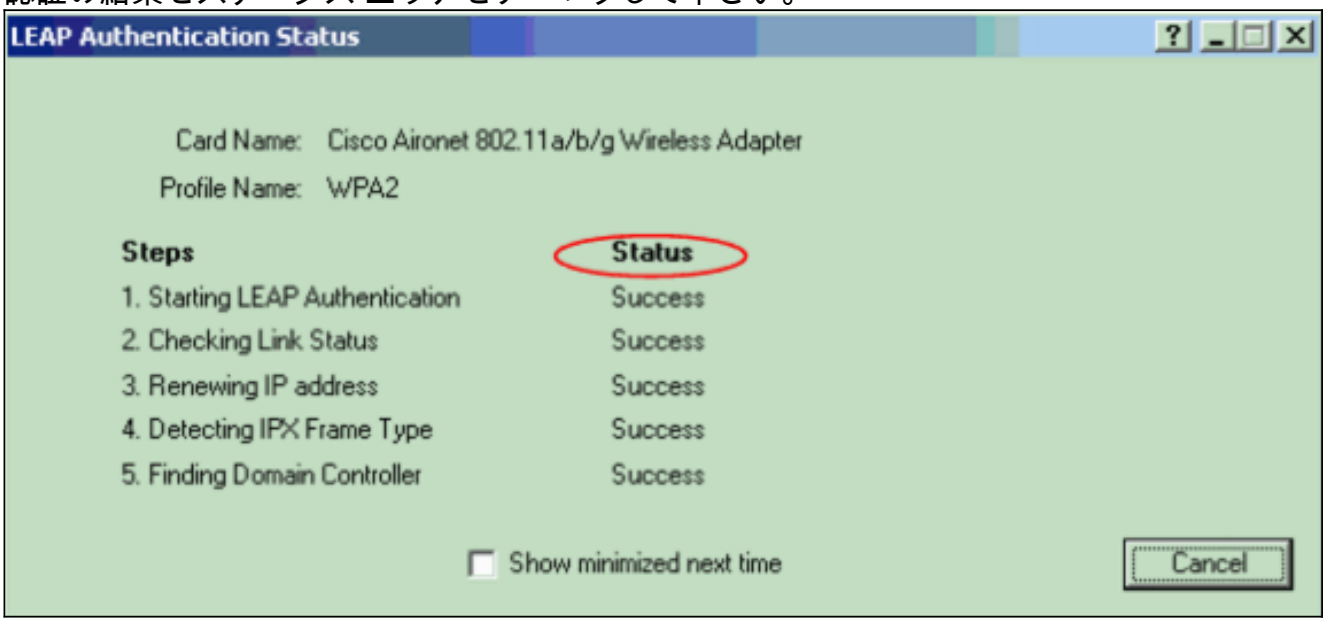
ここでは、設定が正常に動作していることを確認します。

1. 入力無線ネットワーク Password ウィンドウが表示するとき、ユーザネームおよびパスワードを入力して下さい。



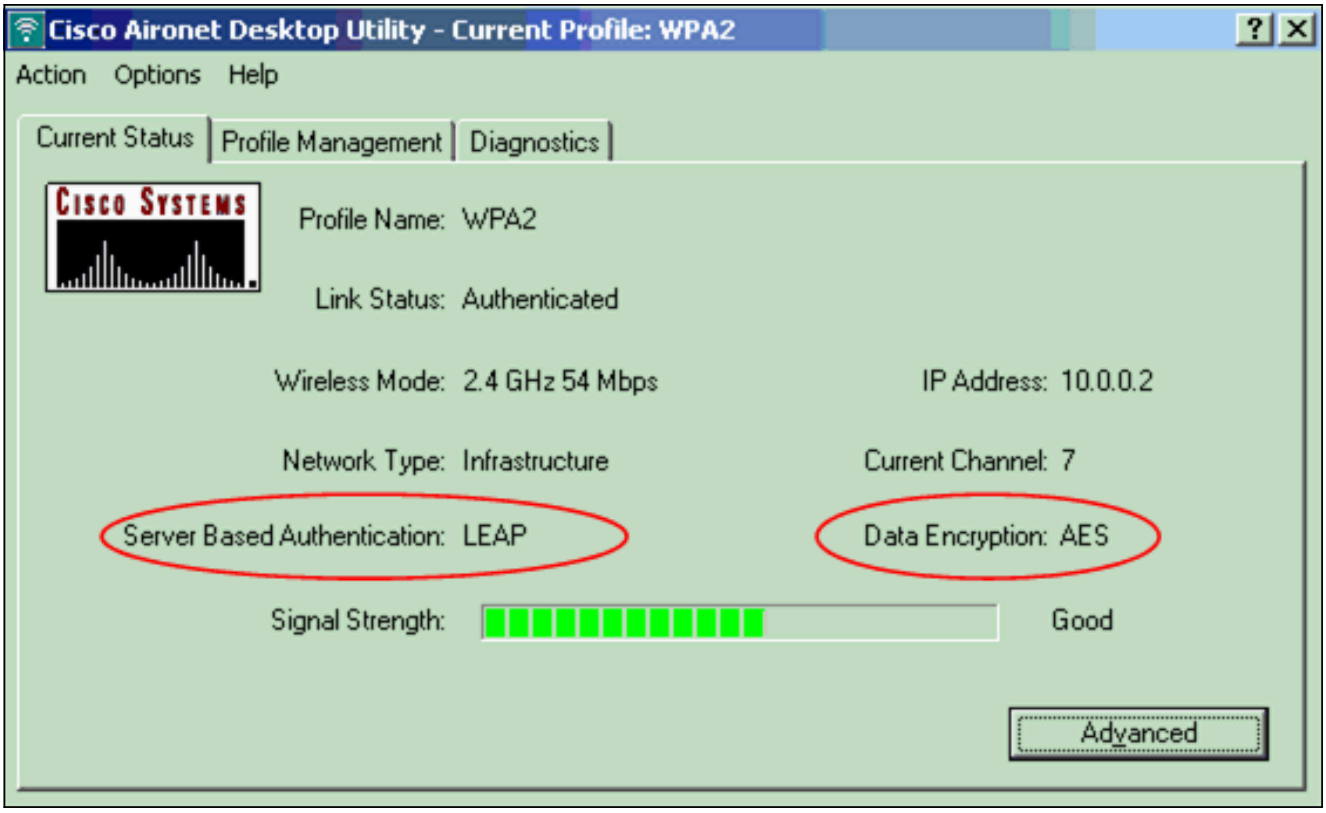
Next ウィンドウは LEAP 認証状況です。 このフェーズはローカル RADIUSサーバに対してユーザーの資格情報を確認します。

2. 認証の結果をステータス エリアをチェックして下さい。



認証が正常なとき、クライアントは Wireless LAN に接続します。

3. クライアントが AES 暗号化および LEAP 認証を使用することを確認するために ADU 現在のステータスをチェックして下さい。これは WLAN の LEAP 認証および AES 暗号化を用いる WPA 2 を設定したことを示します。



4. クライアントの WPA 2.と認証に成功されたことを確認するために AP/bridge イベント ログイン順序をチェックして下さい。

トラブルシューティング

現在のところ、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。

個人的なモードの設定

条件**個人的なモードは**認証における PSK だけ動作モードで相互運用可能であるためにテストされる製品を示します。 このモードは AP およびクライアントの PSK の手動設定を必要とします。 PSK はパスワードによってユーザ、かクライアント ステーションおよび AP 両方の識別コードを

、認証します。 認証サーバは必要ではないです。 クライアントはネットワークへのクライアントパスワードが AP パスワードとマッチするときだけアクセス権を得ることができます。 パスワードはまたデータパケットの暗号化のための暗号化キーを生成するのに TKIP か AES が使用する主な材料を提供します。 個人的なモードは SOHO 環境に目標とされ、エンタープライズ環境のためにセキュアと考慮されません。 このセクションは個人的な動作モードの WPA 2 を設定することを必要とする設定を提供します。

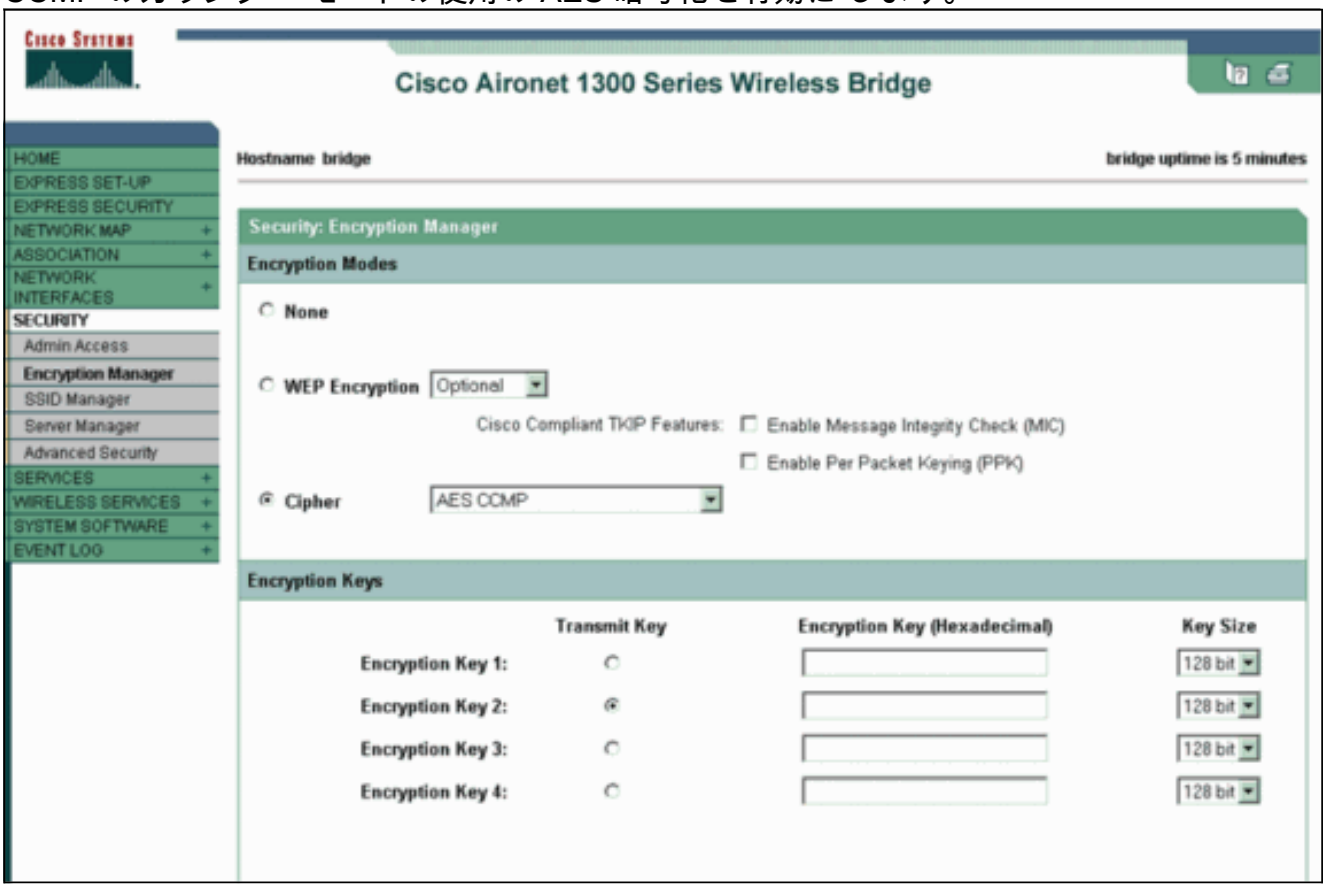
ネットワーク構成

この設定では、WPA 2 互換性があるクライアントアダプタを持つユーザは Aironet 1310G AP/Bridge に認証を受けます。 キー管理は AES-CCMP 暗号化が設定されている WPA 2 PSK の使用と、行われます。 セクションは AP を設定し、クライアントアダプタを示します AP およびクライアントアダプタの設定を設定します。

AP を設定して下さい

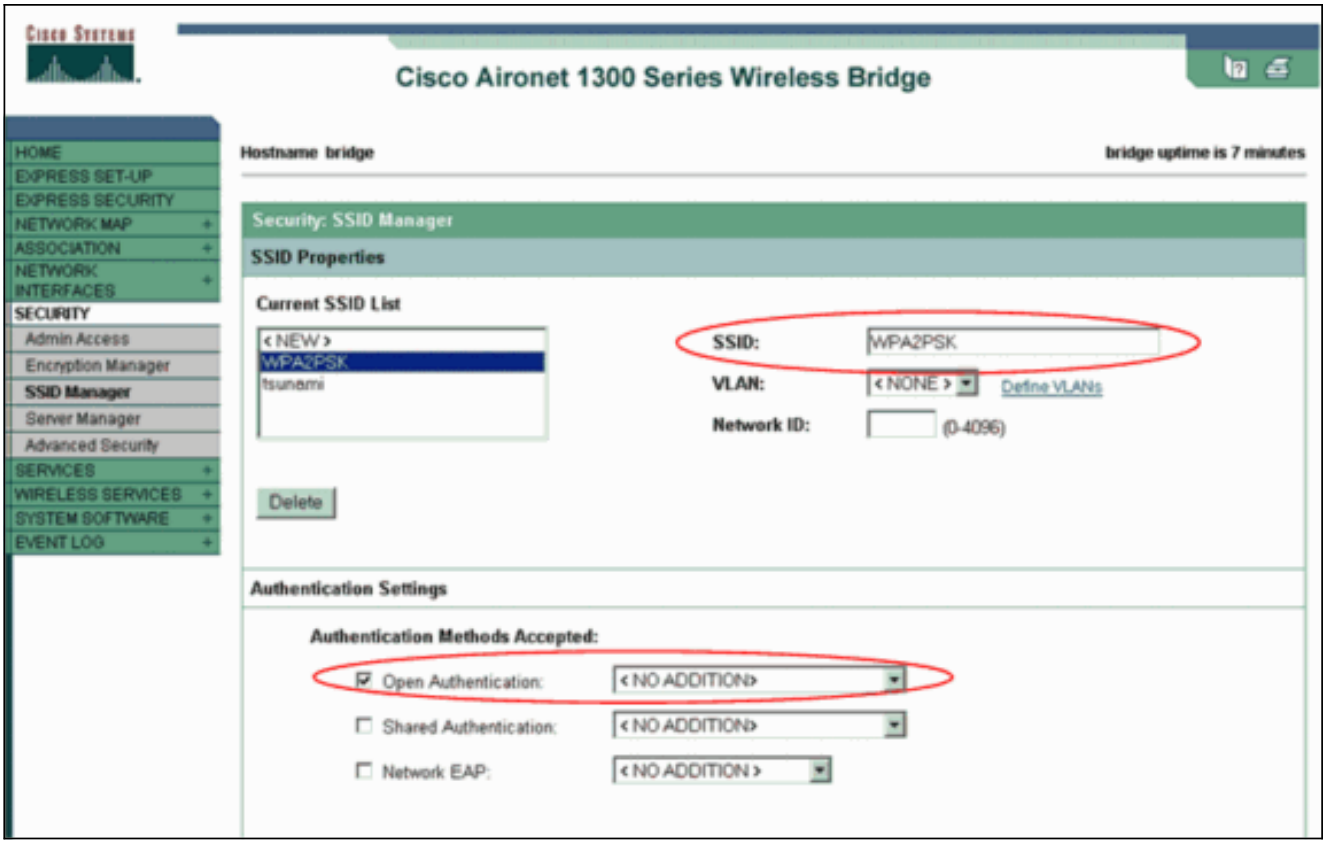
次の手順を実行します。

1. 左のメニューで Security > Encryption Manager の順に選択 し、これらのステップを完了して下さい:暗号メニューから、『AES CCMP』 を選択 して下さい。このオプションは CCMP のカウンター モードの使用の AES 暗号化を有効に します。

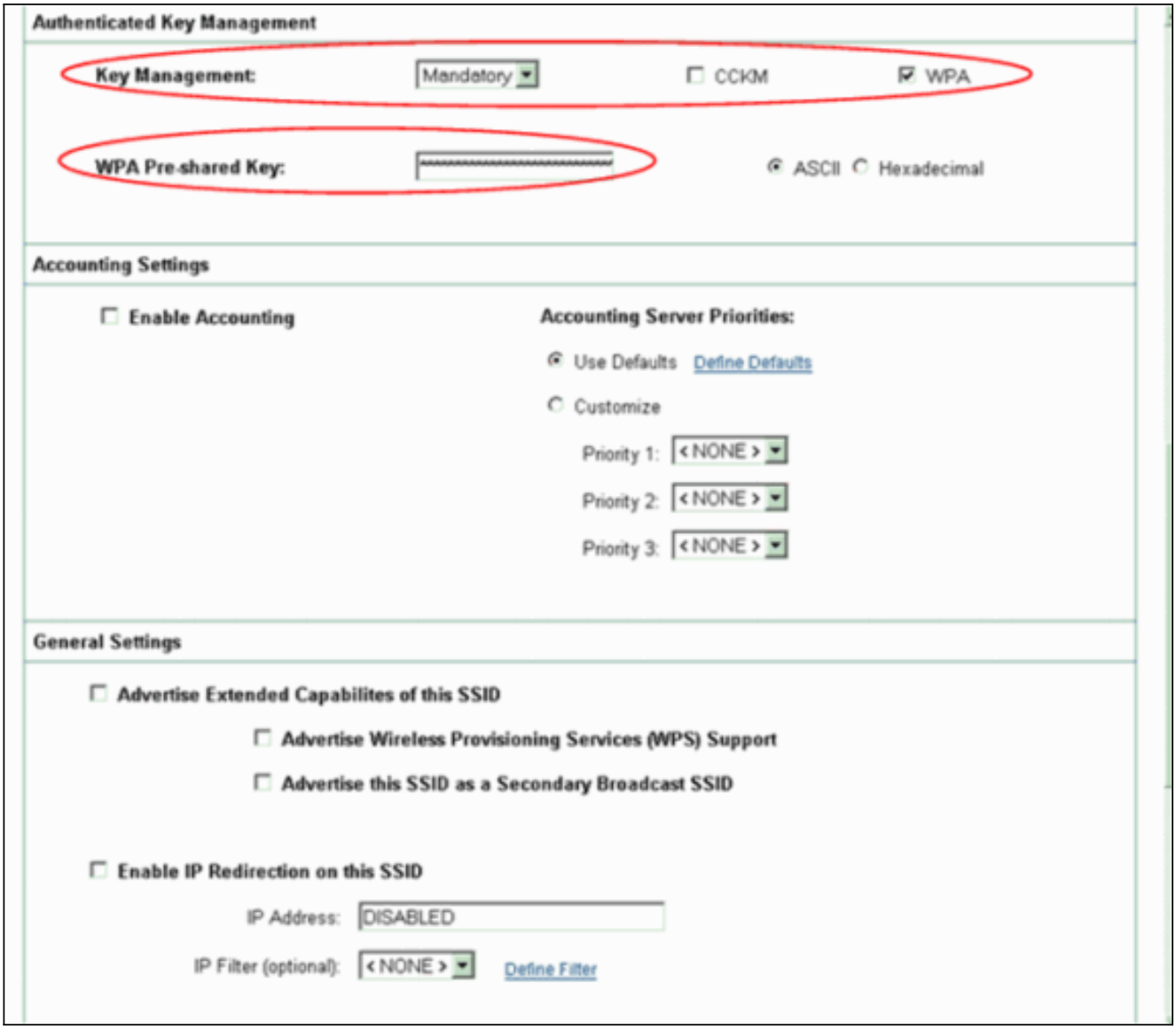


[Apply] をクリックします。

2. WPA 2.と併用するため新しい SSID を Security > SSID Manager の順に選択 し、作成して下さい。**Open Authentication チェックボックスを**チェックして下さい。



セキュリティをスクロールして下さい: 認証されたキー管理エリアへの SSID マネージャ ウィンドウはこれらのステップを完了し、:キー管理メニューから、『Mandatory』 を選択 して下さい。右の **WPA チェックボックスを**チェックして下さい。



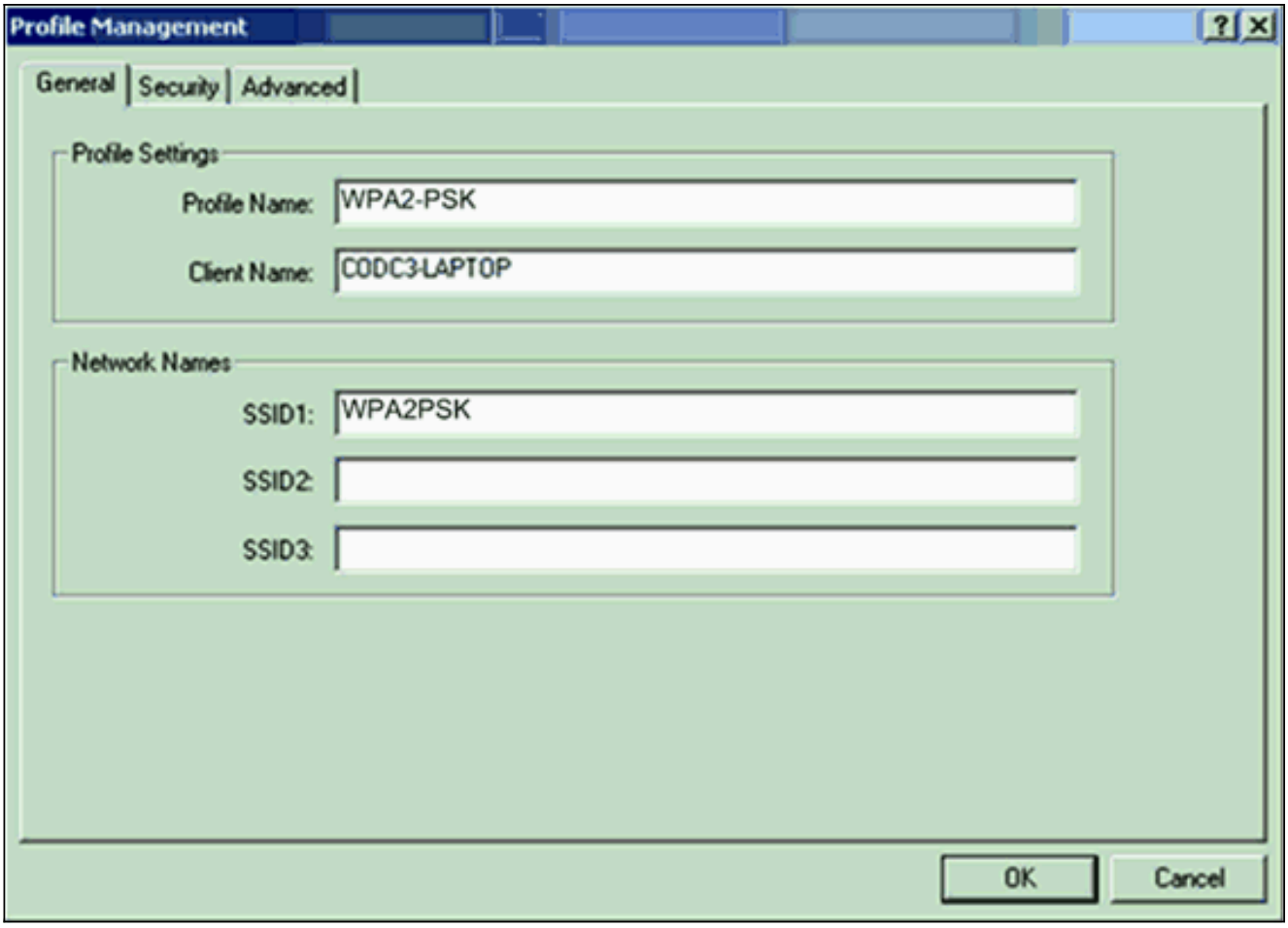
WPA PSK 共用秘密鍵か WPA PSK パスフレーズ キーを入力して下さい。このキーはクライアントアダプタで設定する WPA PSK キーを一致する必要があります。[Apply] をクリックします。

AP は無線クライアントから今認証要求を受け取ることができます。

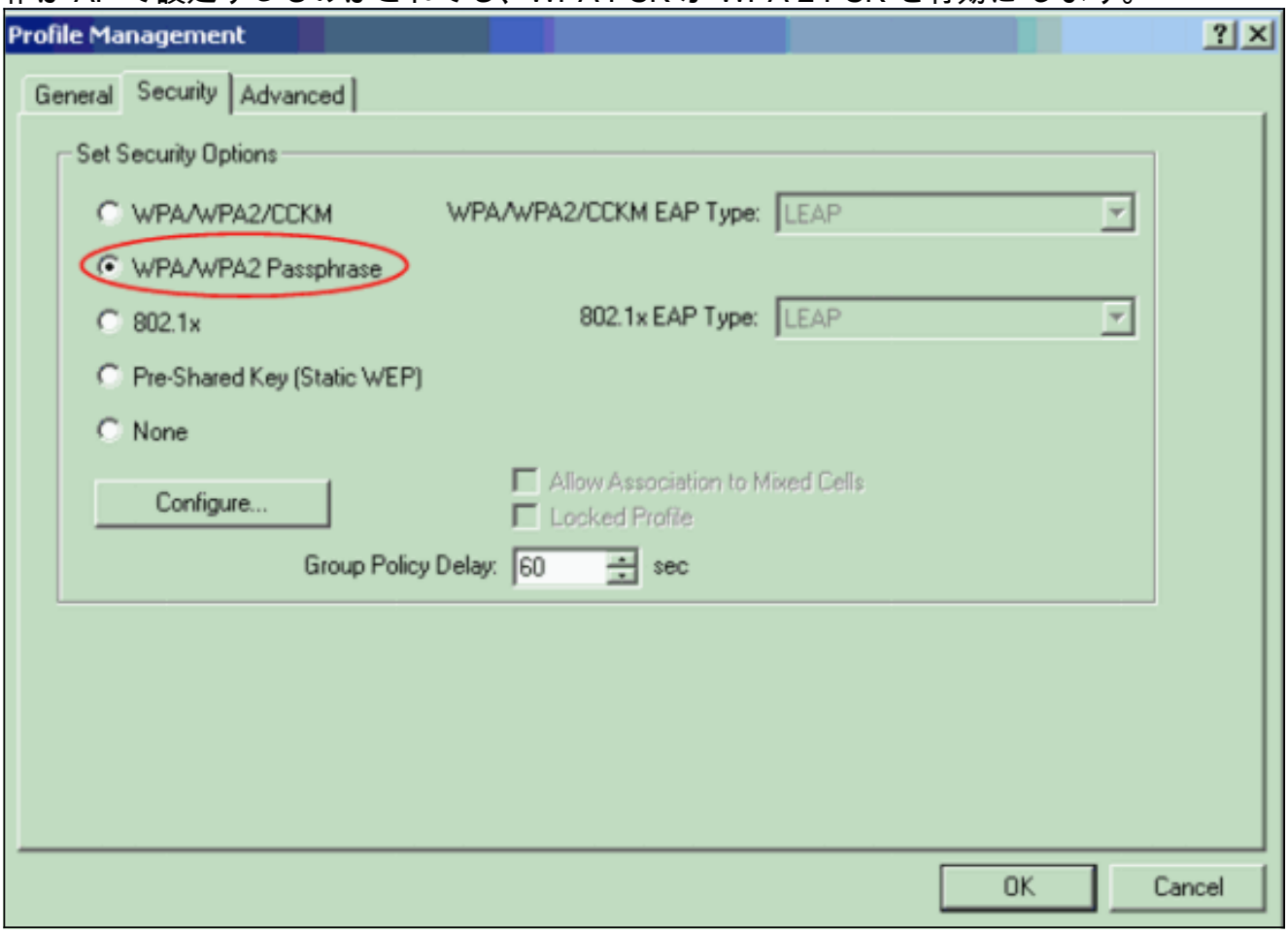
クライアントアダプタを設定して下さい

次の手順を実行します。

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。New ウィンドウは WPA 2 PSK 動作モードのための設定をどこに設定できるか表示します。 General タブの下で、クライアントアダプタが使用する SSID およびプロファイル名前を入力して下さい。この例では、プロファイル名は WPA2-PSK であり、SSID は WPA2PSK です:**注:** SSID は WPA 2 PSK のための AP で設定した SSID を一致する必要があります。



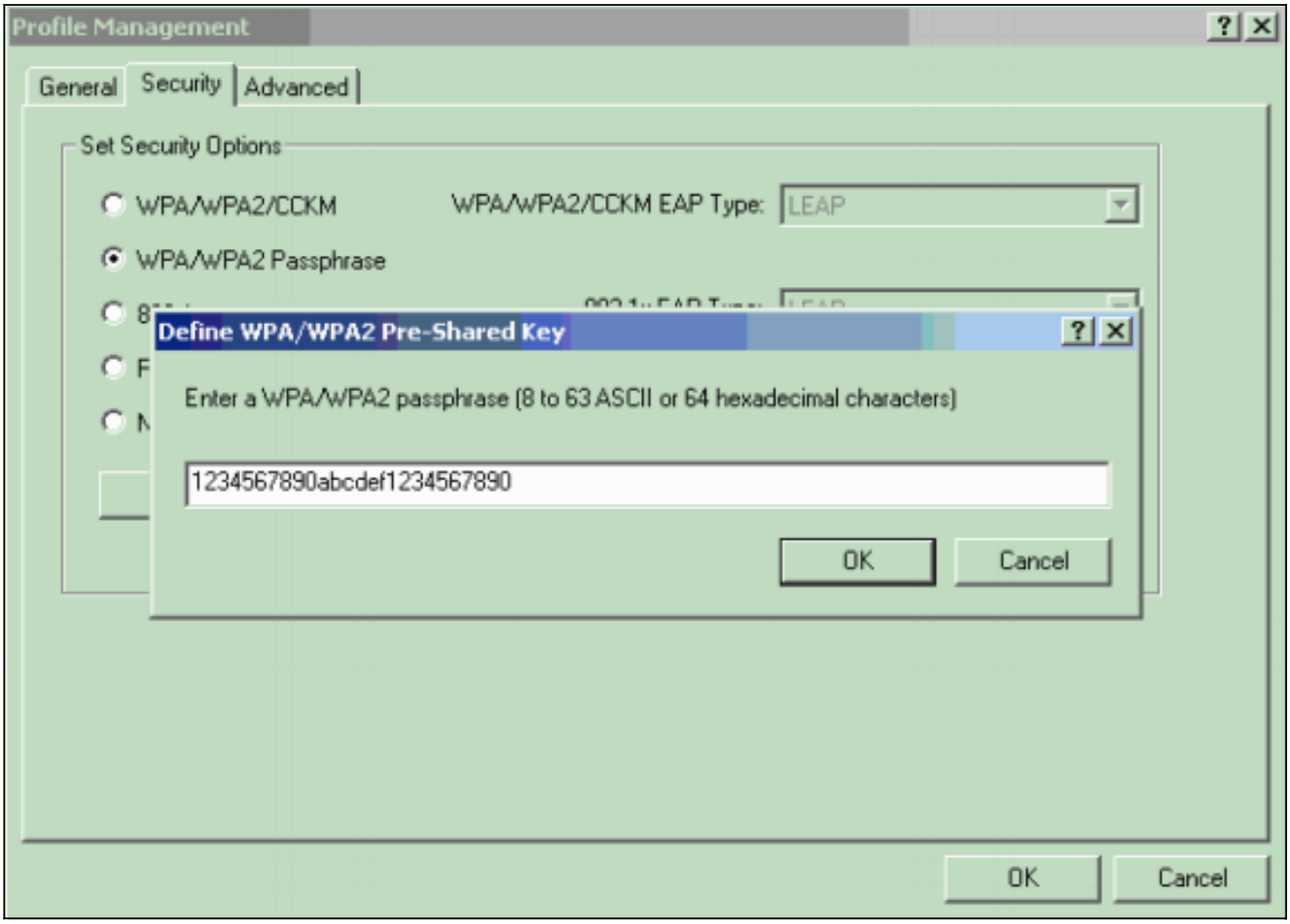
2. **Security タブを**クリックし、『WPA/WPA2 Passphrase』 をクリック して下さい。この操作は AP で設定するものはどれでも、WPA PSK か WPA 2 PSK を有効に します。



3. [Configure] をクリックします。定義 WPA/WPA2 Pre-Shared Key ウィンドウは表示します

。

4. システム アドミニストレータからの WPA/WPA2 パスフレーズを得、WPA/WPA2 Passphrase フィールドでパスフレーズを入力して下さい。インフラストラクチャ ネットワークの AP のためのパスフレーズかアド ホックなネットワークの他のクライアントのためのパスフレーズを得て下さい。パスフレーズを入力するためにこれらのガイドラインを使用して下さい:WPA/WPA2 パスフレーズは 8 人および 63 人の ASCII テキスト文字か 64 の 16 進法文字の間で含まれている必要があります。クライアントアダプタ WPA/WPA2 パスフレーズは通信することを計画する AP のパスフレーズを一致する必要があります。



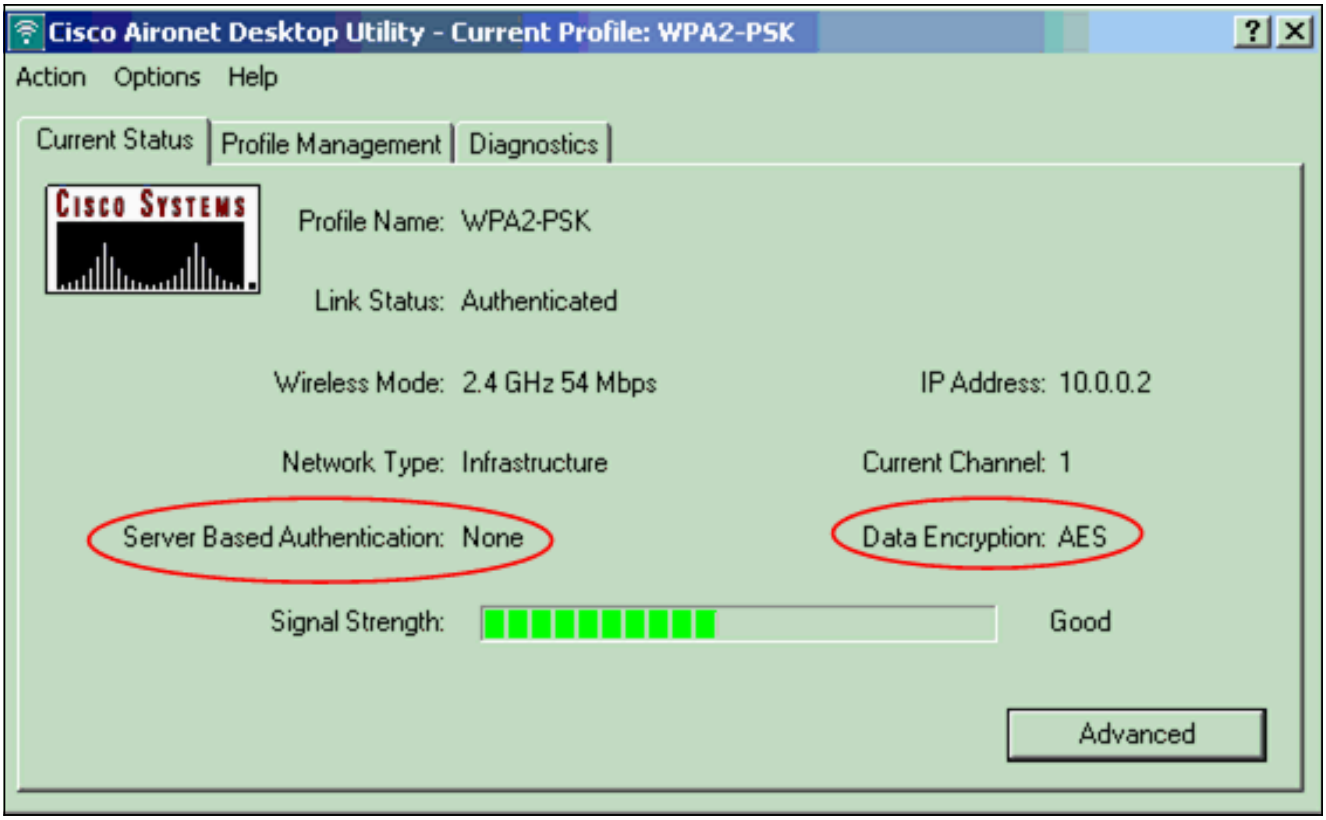
5. パスフレーズを保存し、プロファイル 管理ウィンドウに戻るために『OK』 をクリック して下さい。

確認

ここでは、設定が正常に動作していることを確認します。

WPA 2 PSK の後でプロファイルはアクティブになります、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. 認証の成功を確認するために ADU 現在のステータスをチェックして下さい。このウィンドウは例を提供します。 ウィンドウはことサーバベース認証は実行されたことを使用する暗号化が AES、そしてである表示します
:



2. クライアントの認証の WPA 2 PSK モードと認証に成功されたことを確認するために AP/bridge イベント ログイン順序をチェックして下さい。

トラブルシューティング

現在のところ、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
- 設定

- WPA 設定の概要
- WPA2 - Wi-Fi Protected Access 2
- WPA ミックス モード オペレーションはである何、そしてそれを設定するどのように AP で
- 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