

# Wi-Fi Protected Access 2 ( WPA 2 ) 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](#)

[背景説明](#)

[Cisco Aironet 機器での WPA 2 のサポート](#)

[エンタープライズ モードでの設定](#)

[ネットワークのセットアップ](#)

[AP の設定](#)

[CLI での設定](#)

[クライアント アダプタの設定](#)

[確認](#)

[トラブルシューティング](#)

[パーソナル モードでの設定](#)

[ネットワークのセットアップ](#)

[AP の設定](#)

[クライアント アダプタの設定](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

## 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WPA2へのできるだけ早急な移行を推奨しています。

WPAおよびWPA2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、WPA2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

WPA2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。

WPA2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、WPA2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、WPA2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WPA2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WPA2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。

The screenshot shows the configuration page for the Server Manager. The left sidebar contains a menu with 'Security' > 'Encryption Manager' highlighted. The main content area is titled 'Security: Server Manager' and includes sections for 'Backup RADIUS Server', 'Corporate Servers', and 'Default Server Priorities'. In the 'Corporate Servers' section, a 'Current Server List' dropdown is set to 'RADIUS'. A table lists a server with IP '10.0.0.1'. Red circles highlight the 'Server' field (10.0.0.1), the 'Authentication Port' (1812), the 'Accounting Port' (1813), and the 'EAP Authentication' priority dropdown (10.0.0.1).

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。

The screenshot shows the configuration page for the Encryption Manager. The left sidebar contains a menu with 'Security' > 'Encryption Manager' highlighted. The main content area is titled 'Security: Encryption Manager' and includes sections for 'Encryption Modes' and 'Encryption Keys'. In the 'Encryption Modes' section, the 'Cipher' radio button is selected, and the 'AES CCMP' option is chosen from the dropdown menu. Red circles highlight the 'Cipher' radio button and the 'AES CCMP' dropdown. The 'Encryption Keys' section shows a table with four keys, each with a 'Transmit Key' radio button, an 'Encryption Key (Hexadecimal)' input field, and a 'Key Size' dropdown menu set to '128 bit'.

[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。

The screenshot displays the configuration interface for a Cisco Aironet 1300 Series Wireless Bridge. The page title is "Cisco Aironet 1300 Series Wireless Bridge" and the hostname is "bridge". The bridge uptime is 6 minutes. The left sidebar shows the navigation menu with "Security" expanded and "SSID Manager" selected. The main content area is titled "Security: SSID Manager" and "SSID Properties". Under "Current SSID List", there is a list with items: "< NEW >", "WPA2", and "autoinstall". The "WPA2" item is selected. To the right of the list, the "SSID:" field contains "WPA2", the "VLAN:" dropdown is set to "< NONE >", and the "Network ID:" field is empty. Below this, the "Authentication Settings" section is visible, with "Authentication Methods Accepted:" listed. The "Network EAP:" checkbox is checked, and the "Open Authentication:" and "Shared Authentication:" checkboxes are unchecked. Red circles highlight the "WPA2" SSID in the list and the "Network EAP:" checkbox in the authentication settings.

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。

**Authenticated Key Management**

**Key Management:**   CCMP  WPA

**WPA Pre-shared Key:**   ASCII  Hexadecimal

---

**Accounting Settings**

Enable Accounting

**Accounting Server Priorities:**

Use Defaults [Define Defaults](#)

Customize

Priority 1:

Priority 2:

Priority 3:

---

**General Settings**

Advertise Extended Capabilities of this SSID

- Advertise Wireless Provisioning Services (WPS) Support
- Advertise this SSID as a Secondary Broadcast SSID

Enable IP Redirection on this SSID

IP Address:

IP Filter (optional):  [Define Filter](#)

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。

The screenshot shows the configuration page for a Cisco Aironet 1300 Series Wireless Bridge. The page is titled "Cisco Aironet 1300 Series Wireless Bridge" and has three tabs: "STATISTICS", "GENERAL SET-UP", and "EAP-FAST SET-UP". The "GENERAL SET-UP" tab is active. The page displays the following information:

- Hostname: bridge
- bridge uptime is 0 minutes
- Security: Local RADIUS Server - General Set-Up
- Local Radius Server Authentication Settings
- Enable Authentication Protocols:
  - EAP FAST
  - LEAP
  - MAC
- Network Access Servers (AAA Clients)
- Current Network Access Servers
  - <NEW>
  - 10.0.0.1
- Network Access Server: 10.0.0.1 (IP Address)
- Shared Secret: [Redacted]

Red circles highlight the "LEAP" checkbox and the "Network Access Server" and "Shared Secret" fields.

[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。

**Individual Users**

**Current Users**

<NEW>  
user1

Delete

Username: user1

Password:   Text  NT Hash

Confirm Password:

Group Name: <NONE >

MAC Authentication Only

Apply Cancel

---

**User Groups**

**Current User Groups**

<NEW>

Delete

Group Name:

Session Timeout (optional):  (1-4294967295 sec)

Failed Authentications before Lockout (optional):  (1-4294967295)

Lockout (optional):  Infinite  Interval  (1-4294967295 sec)

VLAN ID (optional):

SSID (optional):  Add

Delete

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 nhash password1
group testuser
!--- Individual user user user2 nhash 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

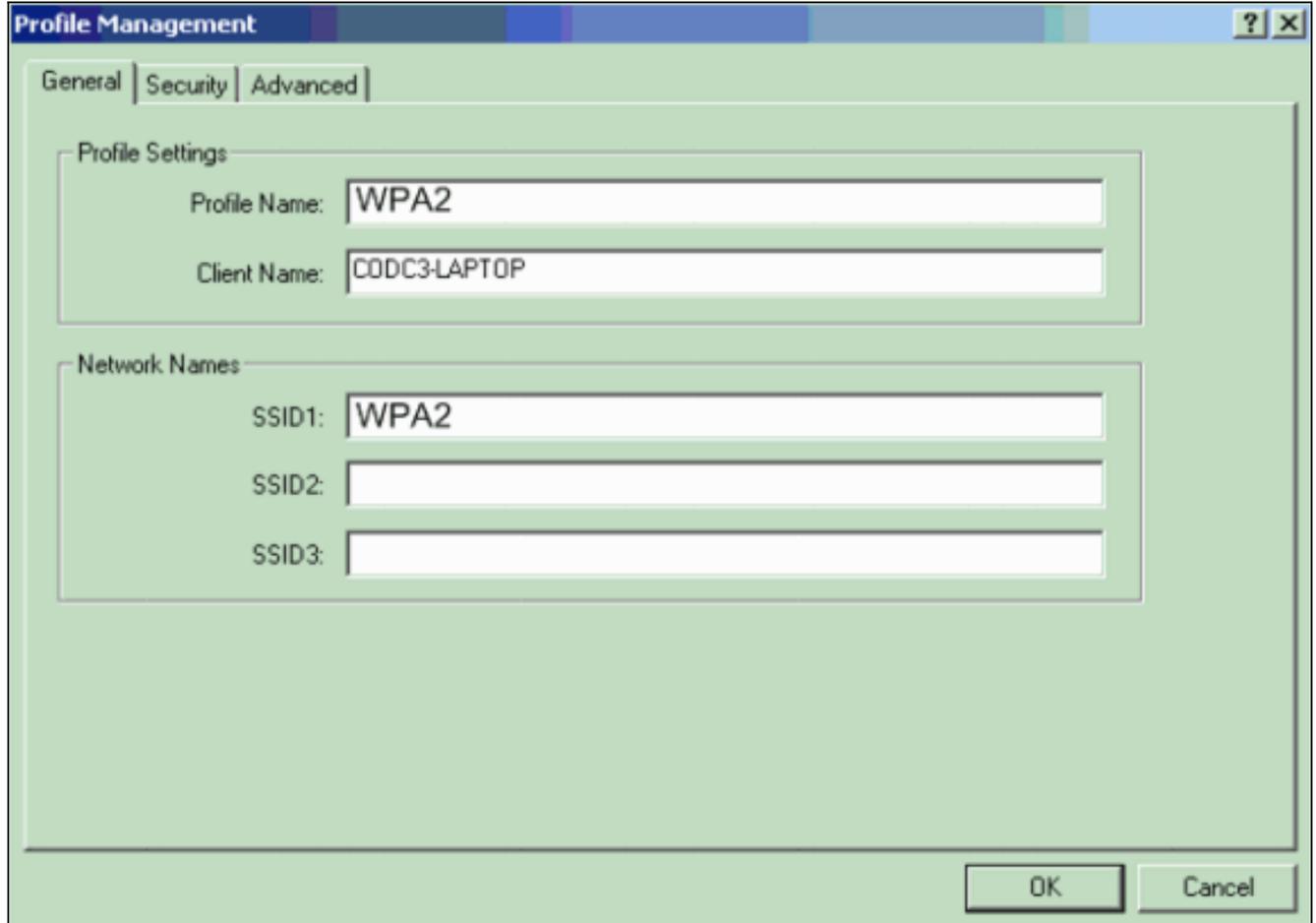
```

## 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。

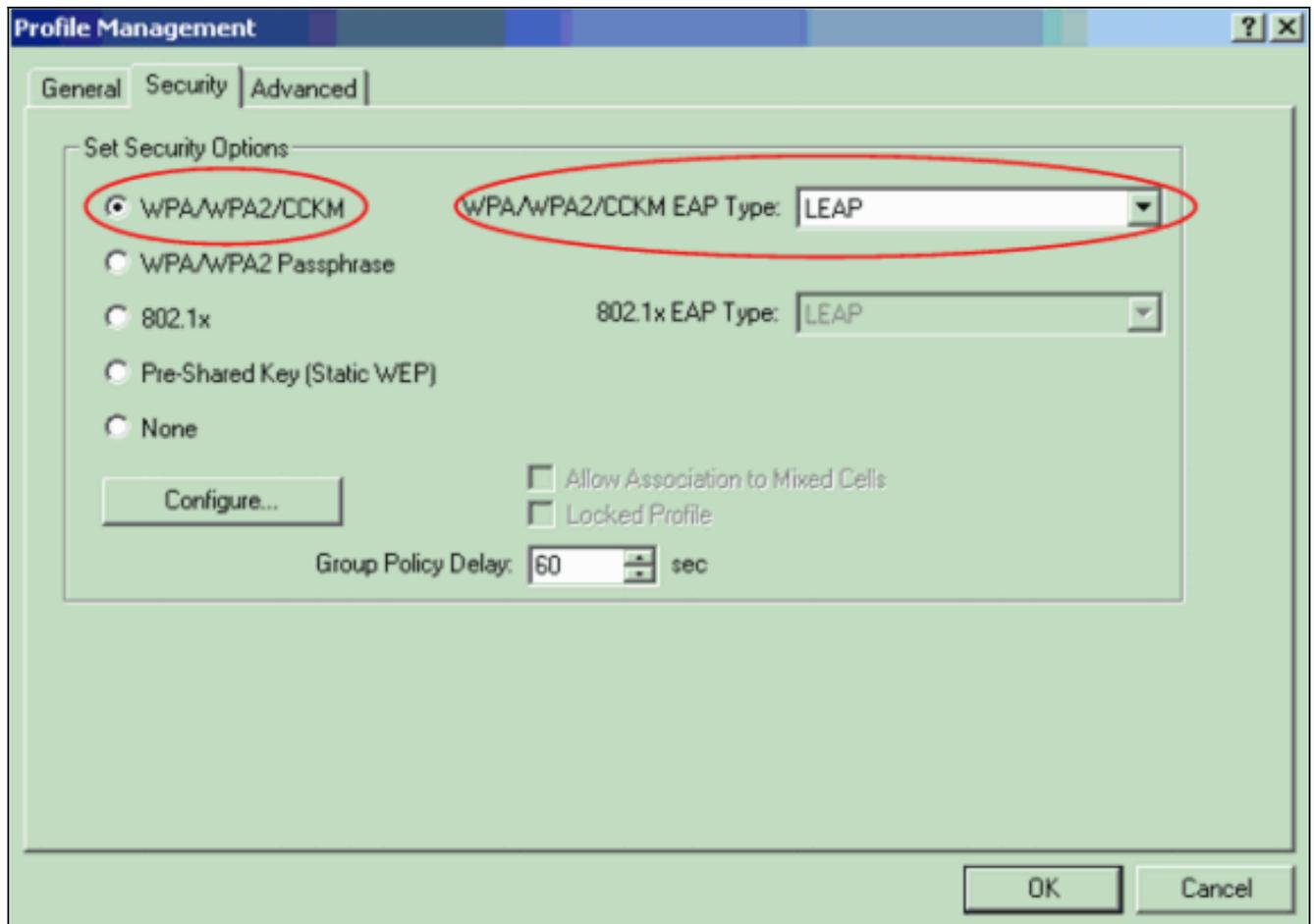
注：このドキュメントでは、ファームウェア2.5が稼働するAironet 802.11a/b/gクライアントアダプタを使用し、ADUバージョン2.5でのクライアントアダプタの設定について説明します。

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。



The screenshot shows the 'Profile Management' dialog box with the 'General' tab selected. The 'Profile Settings' section contains two text input fields: 'Profile Name' with the value 'WPA2' and 'Client Name' with the value 'C0DC3-LAPTOP'. The 'Network Names' section contains three text input fields: 'SSID1' with the value 'WPA2', 'SSID2' which is empty, and 'SSID3' which is empty. At the bottom right, there are 'OK' and 'Cancel' buttons.

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。

**LEAP Settings** [?] [X]

Always Resume the Secure Session

Username and Password Settings

Use Temporary User Name and Password

Use Windows User Name and Password

Automatically Prompt for User Name and Password

Manually Prompt for User Name and Password

Use Saved User Name and Password

User Name:

Password:

Confirm Password:

Domain:

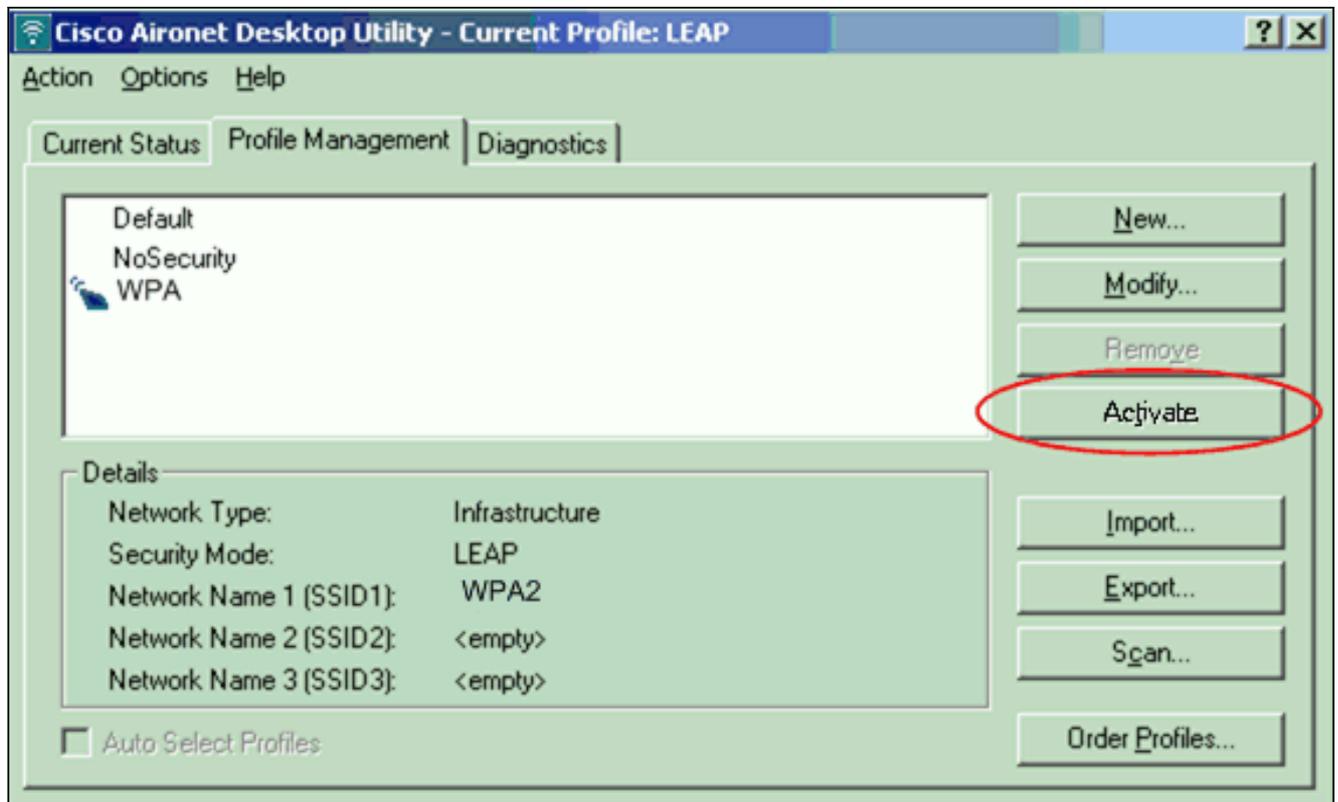
Include Windows Logon Domain with User Name

No Network Connection Unless User Is Logged In

Authentication Timeout Value (in seconds)

OK Cancel

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

**Enter Wireless Network Password**

Please enter your LEAP username and password to log on to the wireless network

User Name : user1

Password : xxxxxxx

Log on to :

Card Name : Cisco Aironet 802.11 a/b/g Wireless Adapter

Profile Name : WPA2

OK Cancel

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。

**LEAP Authentication Status**

Card Name: Cisco Aironet 802.11 a/b/g Wireless Adapter

Profile Name: WPA2

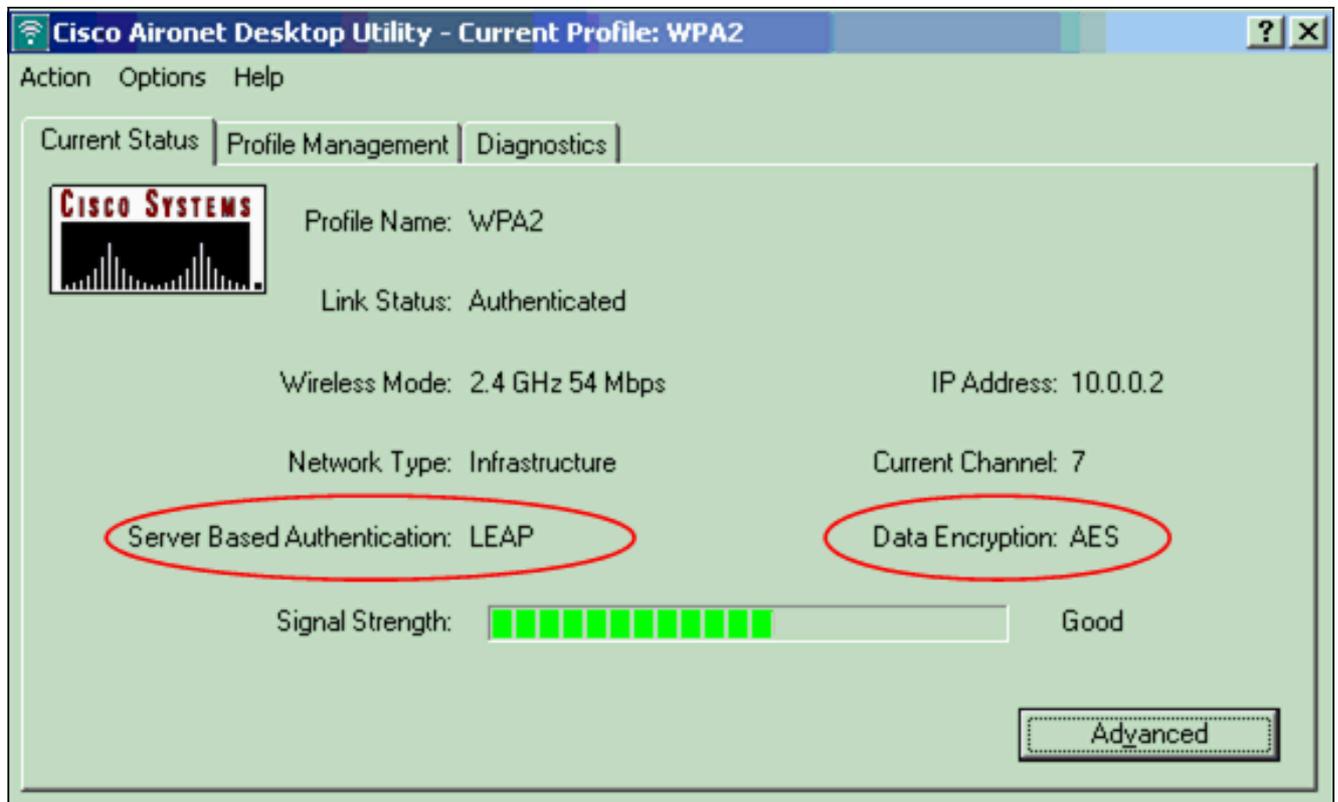
Steps	Status
1. Starting LEAP Authentication	Success
2. Checking Link Status	Success
3. Renewing IP address	Success
4. Detecting IPX Frame Type	Success
5. Finding Domain Controller	Success

Show minimized next time

Cancel

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。



## トラブルシューティング

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、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。

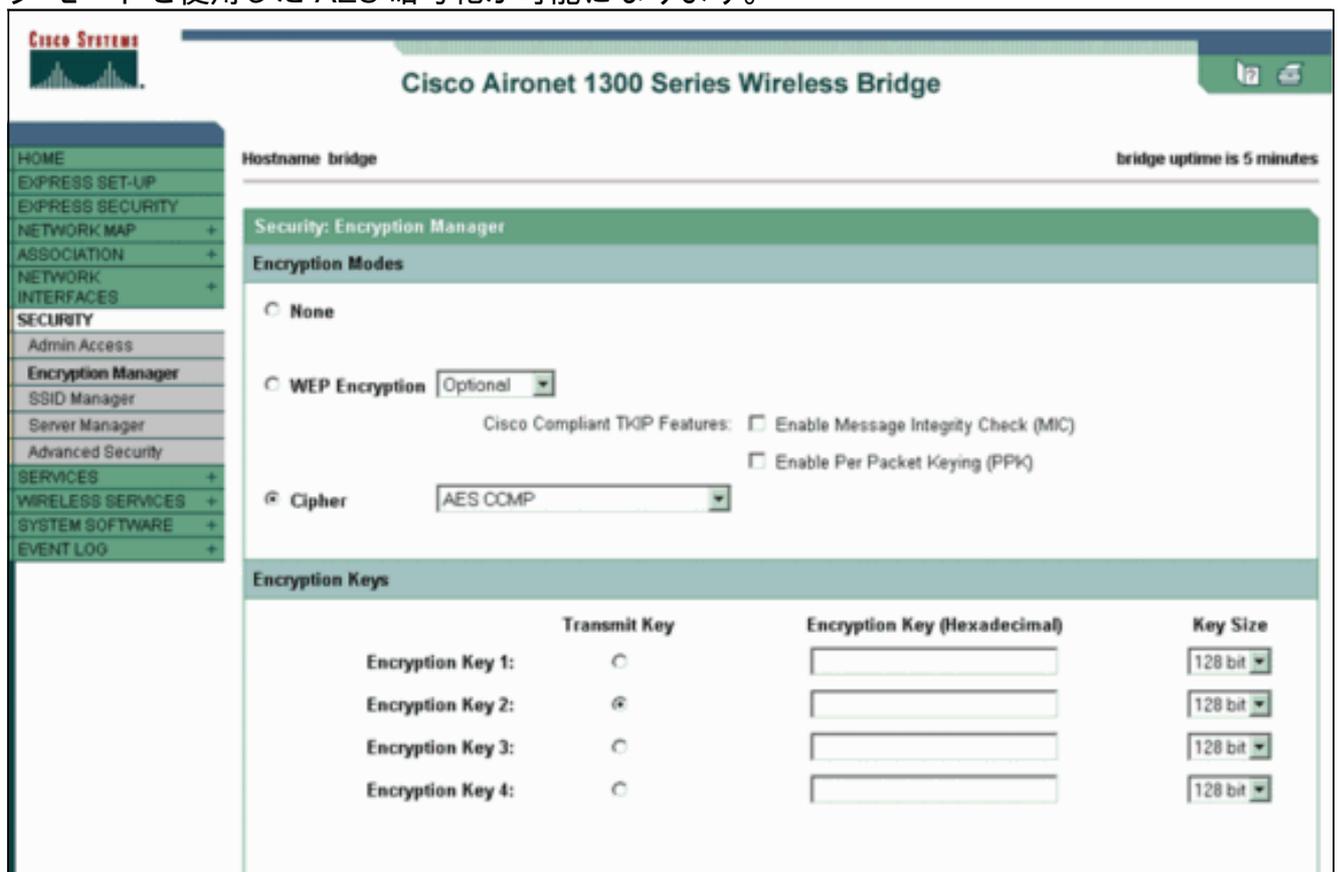
## ネットワークのセットアップ

このセットアップでは、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。



The screenshot shows the configuration interface for the Cisco Aironet 1300 Series Wireless Bridge. The page title is "Cisco Aironet 1300 Series Wireless Bridge". The hostname is "bridge" and the bridge uptime is 5 minutes. The left sidebar contains a navigation menu with categories like HOME, EXPRESS SET-UP, SECURITY, SERVICES, and WIRELESS SERVICES. The main content area is titled "Security: Encryption Manager". Under "Encryption Modes", the "Cipher" option is selected, and the dropdown menu shows "AES CCMP". Below this, there are checkboxes for "Cisco Compliant TKIP Features" including "Enable Message Integrity Check (MIC)" and "Enable Per Packet Keying (PPK)". The "Encryption Keys" section contains a table with four rows for "Encryption Key 1" through "Encryption Key 4". Each row has a "Transmit Key" radio button (Key 2 is selected), an "Encryption Key (Hexadecimal)" input field, and a "Key Size" dropdown menu set to "128 bit".

[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。

The screenshot displays the configuration interface for a Cisco Aironet 1300 Series Wireless Bridge. The page title is "Cisco Aironet 1300 Series Wireless Bridge" and the hostname is "bridge". The bridge uptime is 7 minutes. The left sidebar shows the navigation menu with "SECURITY" expanded to "SSID Manager". The main content area is titled "Security: SSID Manager" and "SSID Properties". Under "Current SSID List", there is a table with columns for SSID and Name. The first row is "< NEW >" and the second row is "WPA2PSK" with the name "tsunami". A "Delete" button is below the list. To the right, the "SSID:" field is set to "WPA2PSK", the "VLAN:" dropdown is set to "< NONE >", and the "Network ID:" field is empty. Below this, the "Authentication Settings" section is titled "Authentication Methods Accepted:". It has three rows: "Open Authentication:" with a checked checkbox and a dropdown set to "< NO ADDITION >", "Shared Authentication:" with an unchecked checkbox and a dropdown set to "< NO ADDITION >", and "Network EAP:" with an unchecked checkbox and a dropdown set to "< NO ADDITION >".

[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。

Authenticated Key Management	
Key Management:	Mandatory <input type="checkbox"/> CCKM <input checked="" type="checkbox"/> WPA
WPA Pre-shared Key:	<input type="text"/> ASCII <input type="radio"/> Hexadecimal
Accounting Settings	
<input type="checkbox"/> Enable Accounting	Accounting Server Priorities:
	<input checked="" type="radio"/> Use Defaults <a href="#">Define Defaults</a>
	<input type="radio"/> Customize
	Priority 1: <input type="text" value="&lt; NONE &gt;"/>
	Priority 2: <input type="text" value="&lt; NONE &gt;"/>
	Priority 3: <input type="text" value="&lt; NONE &gt;"/>
General Settings	
<input type="checkbox"/> Advertise Extended Capabilities of this SSID	
	<input type="checkbox"/> Advertise Wireless Provisioning Services (WPS) Support
	<input type="checkbox"/> Advertise this SSID as a Secondary Broadcast SSID
<input type="checkbox"/> Enable IP Redirection on this SSID	
	IP Address: <input type="text" value="DISABLED"/>
	IP Filter (optional): <input type="text" value="&lt; NONE &gt;"/> <a href="#">Define Filter</a>

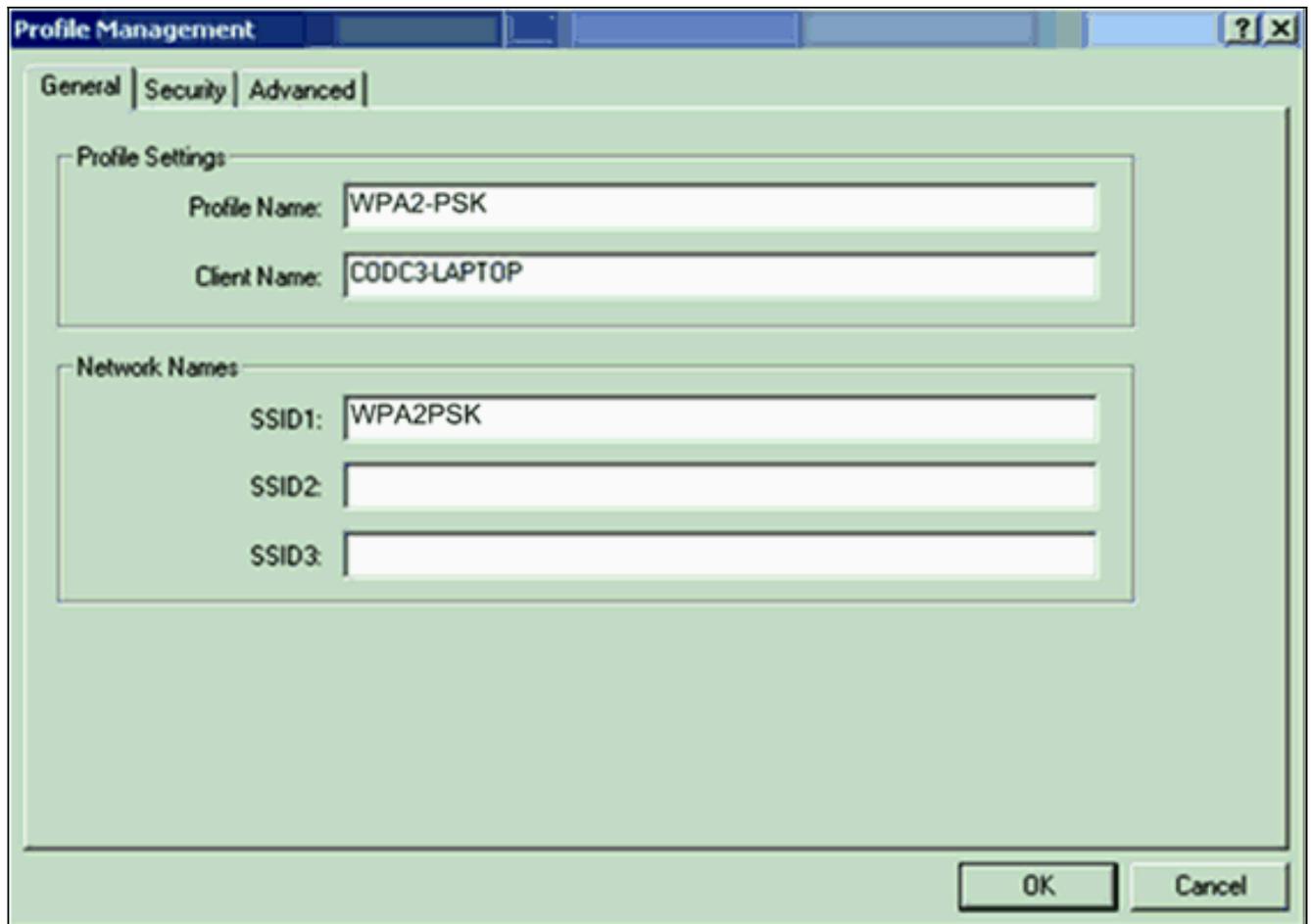
WPA PSK 共有秘密キーまたは WPA PSK パスフレーズ キーを入力します。このキーは、クライアント アダプタで設定されている WPA PSK キーと一致する必要があります。[Apply] をクリックします。

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。

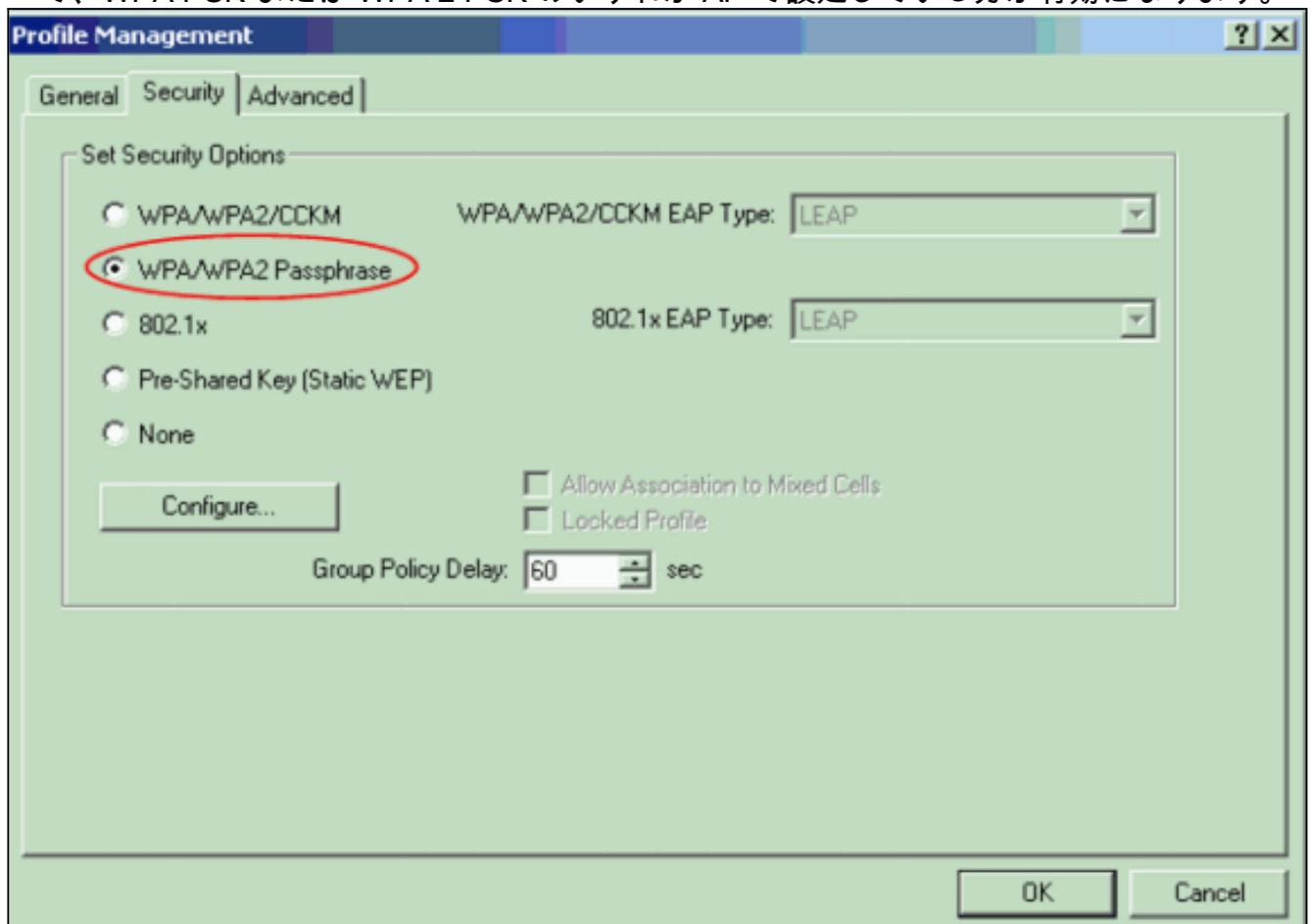
## クライアント アダプタの設定

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。



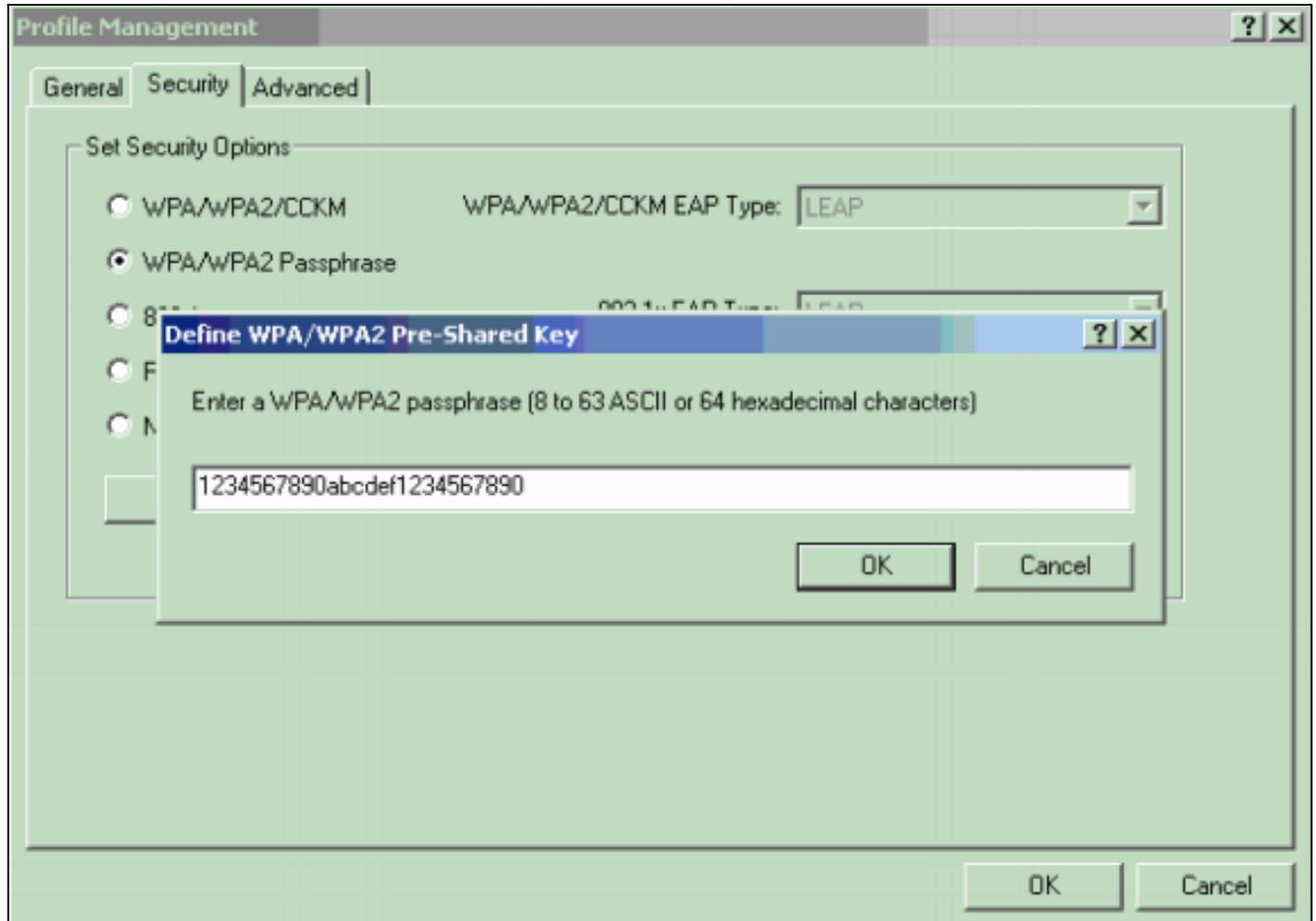
2. [Security] タブをクリックして、[WPA/WPA2 Passphrase] をクリックします。この操作によって、WPA PSK または WPA 2 PSK のいずれか AP で設定している方が有効になります。



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。



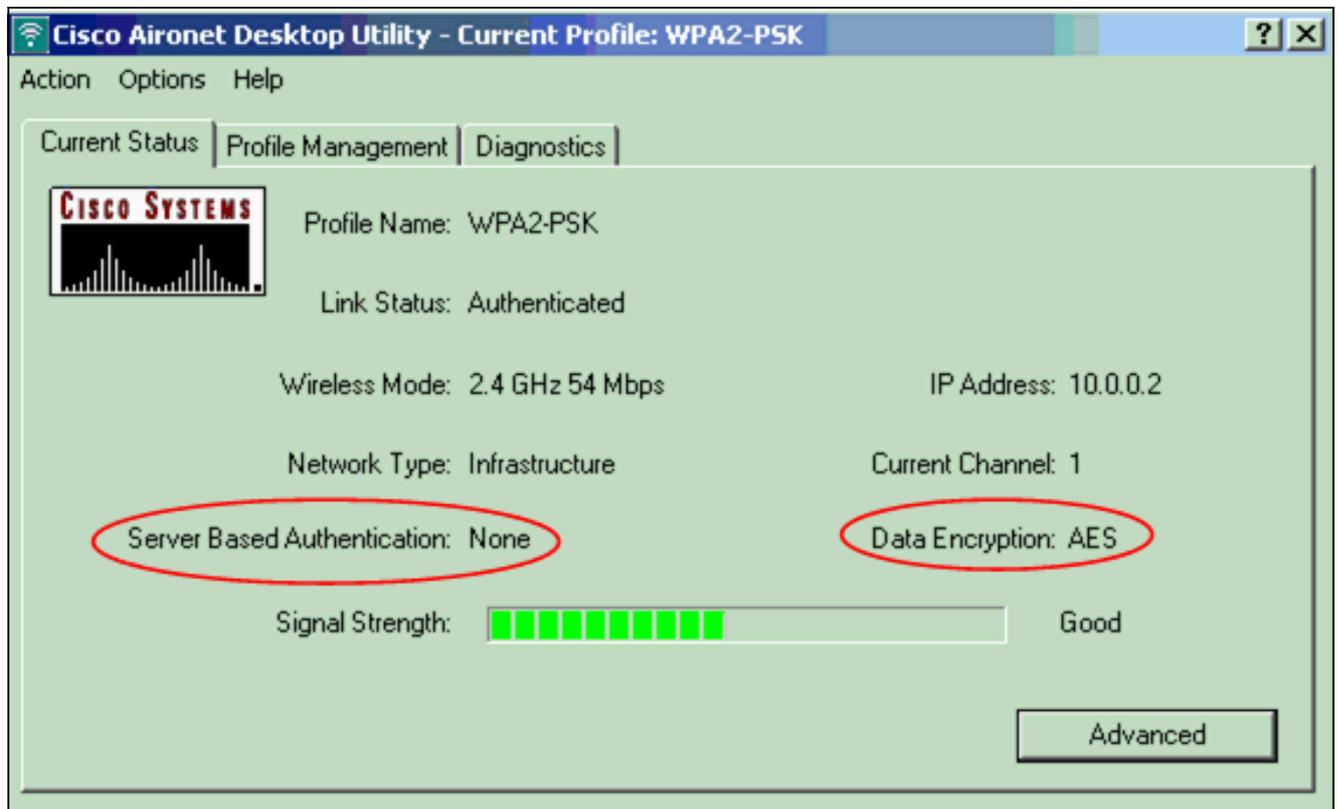
5. [OK] をクリックしてパスフレーズを保存し、[Profile Management] ウィンドウに戻ります。

## 確認

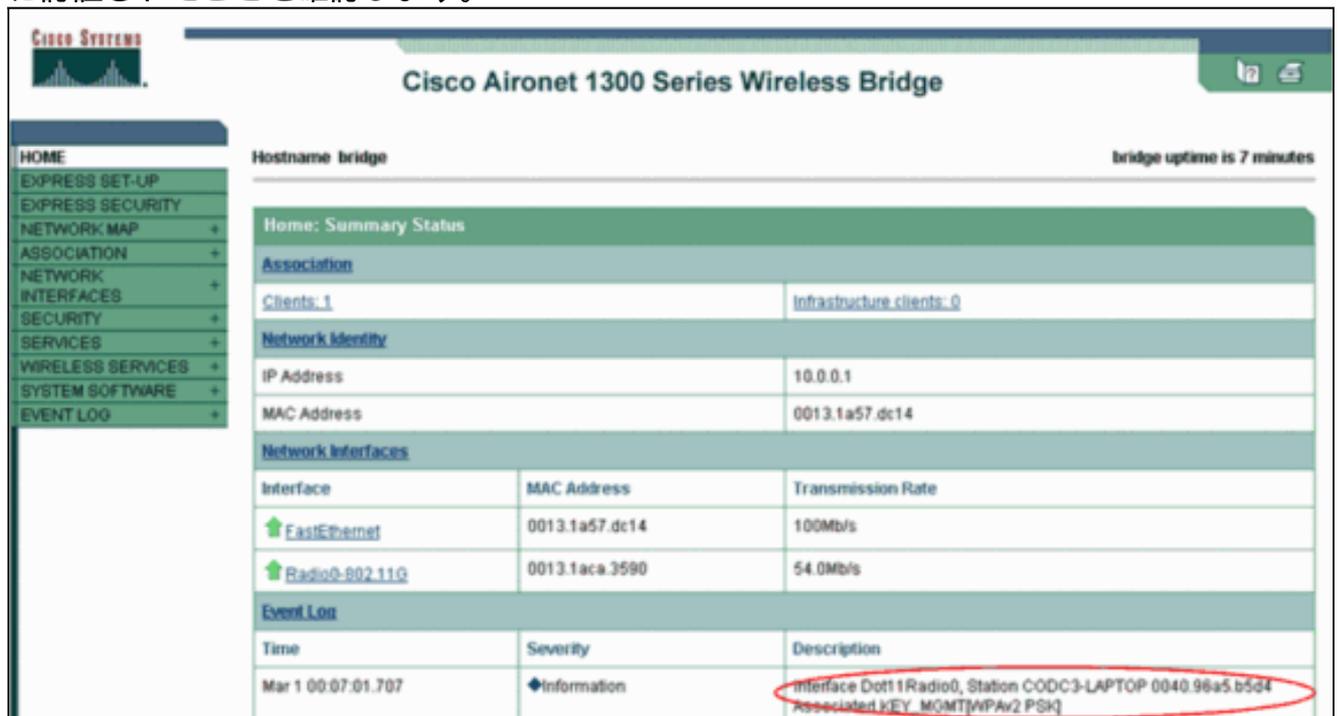
ここでは、設定が正常に機能しているかどうかを確認します。

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。



## トラブルシューティング

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。