

# Wi-Fi Protected Access 2 ( WPA 2 ) の設定例

## 目次

[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](#)

[ネットワーク構成](#)

[AP の設定](#)

[CLI 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](#)

[ネットワーク構成](#)

[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、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 上で WPA 2 を実装する方法の 2 つの設定例を示します。最初の例では、エンタープライズ モードでの WPA 2 の設定方法について、また 2 つ目の例では、パーソナル モードでの WPA 2 の設定方法について説明します。

注: WPA は、Extensible Authentication Protocol ( EAP; 拡張認証プロトコル ) で動作します。

## 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くものです。

- 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、その他の Aironet クライアント アダプタ ソフトウェアとは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、一体型アンテナ装備の AP/ブリッジが使用されています。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、クリアな ( デフォルト ) 設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分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。

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 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、National Institute of Standards and Technology ( NIST; 国立標準技術研究所 ) が推奨する Advanced Encryption Standard ( AES; 高度暗号化規格 ) の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 無線を実装して、Cisco IOS ソフトウェア リリース 12.3(2)JA 以降を使用します。

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 シリーズの製品では AES がサポートされていないため、WPA 2 はサポートされません。

注: Cisco Aironet 1400 シリーズ ワイヤレスブリッジでは、WPA 2 または AES はサポートされていません。

## 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。

企業モードでは、クライアントおよび認証サーバは EAP 認証認証方法の使用と互い、およびクライアント および サーバ 生成するをマスタ鍵 (PMK) 一対に認証します。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。

## [ネットワーク構成](#)

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。

Cisco Systems  
Cisco Aironet 1300 Series Wireless Bridge

SERVER MANAGER GLOBAL PROPERTIES

Hostname bridge bridge uptime is 7 minutes

Security: Server Manager

Backup RADIUS Server

Backup RADIUS Server:  (Hostname or IP Address)

Shared Secret:

Apply Delete Cancel

Corporate Servers

Current Server List

RADIUS

<NEW>  
10.0.0.1

Delete

Server:  (Hostname or IP Address)

Shared Secret:

Authentication Port (optional):  (0-65536)

Accounting Port (optional):  (0-65536)

Apply Cancel

Default Server Priorities

EAP Authentication Priority 1:

MAC Authentication Priority 1:

Accounting Priority 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。

Cisco Systems  
Cisco Aironet 1300 Series Wireless Bridge

HOME

EXPRESS SET-UP

EXPRESS SECURITY

NETWORK MAP

ASSOCIATION

NETWORK INTERFACES

SECURITY

Admin Access

Encryption Manager

SSID Manager

Server Manager

Advanced Security

SERVICES

WIRELESS SERVICES

SYSTEM SOFTWARE

EVENT LOG

Hostname bridge bridge uptime is 5 minutes

Security: Encryption Manager

Encryption Modes

None

WEP Encryption

Cisco Compliant TKIP Features:  Enable Message Integrity Check (MIC)  
 Enable Per Packet Keying (PPK)

Cipher

Encryption Keys

	Transmit Key	Encryption Key (Hexadecimal)	Key Size
Encryption Key 1:	<input type="radio"/>	<input type="text"/>	<input type="text" value="128 bit"/>
Encryption Key 2:	<input checked="" type="radio"/>	<input type="text"/>	<input type="text" value="128 bit"/>
Encryption Key 3:	<input type="radio"/>	<input type="text"/>	<input type="text" value="128 bit"/>
Encryption Key 4:	<input type="radio"/>	<input type="text"/>	<input type="text" value="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" > "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" (highlighted), and "autoinstall". To the right of the list, the "SSID:" field contains "WPA2", "VLAN:" is set to "< NONE >", and "Network ID:" is empty. Below the list is a "Delete" button. The "Authentication Settings" section is titled "Authentication Methods Accepted:" and contains three options: "Open Authentication:" (unchecked), "Shared Authentication:" (unchecked), and "Network EAP:" (checked). The "Network EAP:" checkbox and its dropdown menu are circled in red.

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 interface for a Cisco Aironet 1300 Series Wireless Bridge. The page title is "Cisco Aironet 1300 Series Wireless Bridge". The navigation menu on the left includes: HOME, EXPRESS SET-UP, EXPRESS SECURITY, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, SECURITY (with sub-items: Admin Access, Encryption Manager, SSID Manager, Server Manager, Local RADIUS Server, Advanced Security), SERVICES, WIRELESS SERVICES, SYSTEM SOFTWARE, and EVENT LOG. The main content area is divided into three tabs: STATISTICS, GENERAL SET-UP (selected), and EAP-FAST SET-UP. The "GENERAL SET-UP" tab shows the "Security: Local RADIUS Server - General Set-Up" section. Under "Local Radius Server Authentication Settings", the "Enable Authentication Protocols" section has three options:  EAP FAST,  LEAP (circled in red), and  MAC. Below this are "Apply" and "Cancel" buttons. The "Network Access Servers (AAA Clients)" section shows "Current Network Access Servers" with a list containing "< NEW >" and "10.0.0.1". A "Delete" button is below the list. To the right, the "Network Access Server:" field contains "10.0.0.1" (IP Address) and the "Shared Secret:" field is empty. Both fields are circled in red. "Apply" and "Cancel" buttons are at the bottom right. The "Individual Users" section is partially visible at the bottom.

[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。

The screenshot shows a configuration interface with two main sections: 'Individual Users' and 'User Groups'.

**Individual Users:**

- Current Users:** A list box containing '<NEW>' and 'user1'. A 'Delete' button is below it.
- Form Fields:**
  - Username:** 'user1' (circled in red)
  - Password:** (circled in red)
  - Confirm Password:** (empty)
  - Group Name:** '<NONE >'
  - MAC Authentication Only
  - Radio buttons for  Text and  NT Hash
- Buttons:** 'Apply' and 'Cancel' at the bottom right.

**User Groups:**

- Current User Groups:** A list box containing '<NEW>'. A 'Delete' button is below it.
- Form Fields:**
  - Group Name:** (empty)
  - Session Timeout (optional):** (empty) (1-4294967295 sec)
  - Failed Authentications before Lockout (optional):** (empty) (1-4294967295)
  - Lockout (optional):**
    - Infinite
    - Interval (empty) (1-4294967295 sec)
  - VLAN ID (optional):** (empty)
  - SSID (optional):** (empty) with an 'Add' button.
- Buttons:** 'Delete' at the bottom right.

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 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

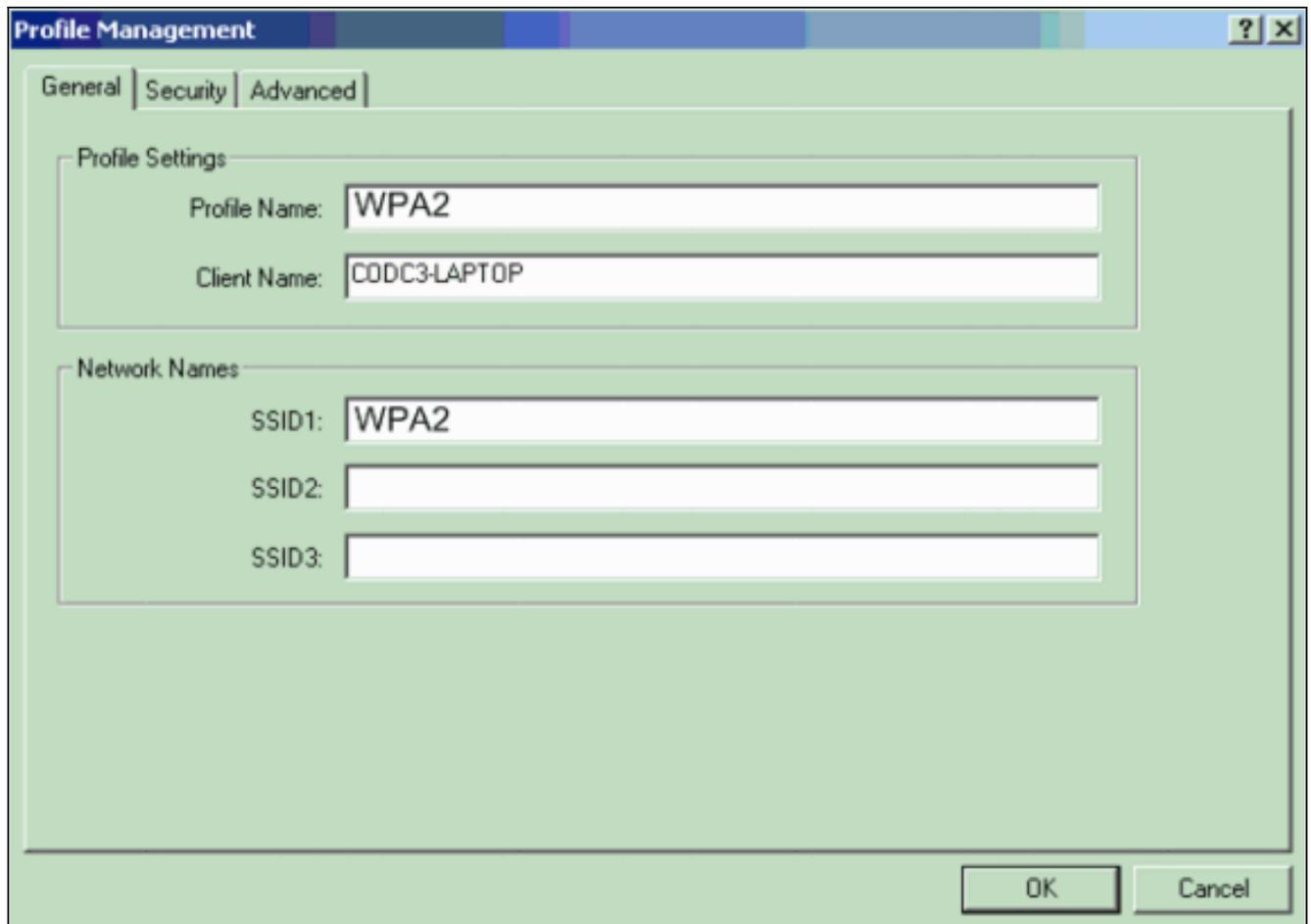
```

## クライアントアダプタの設定

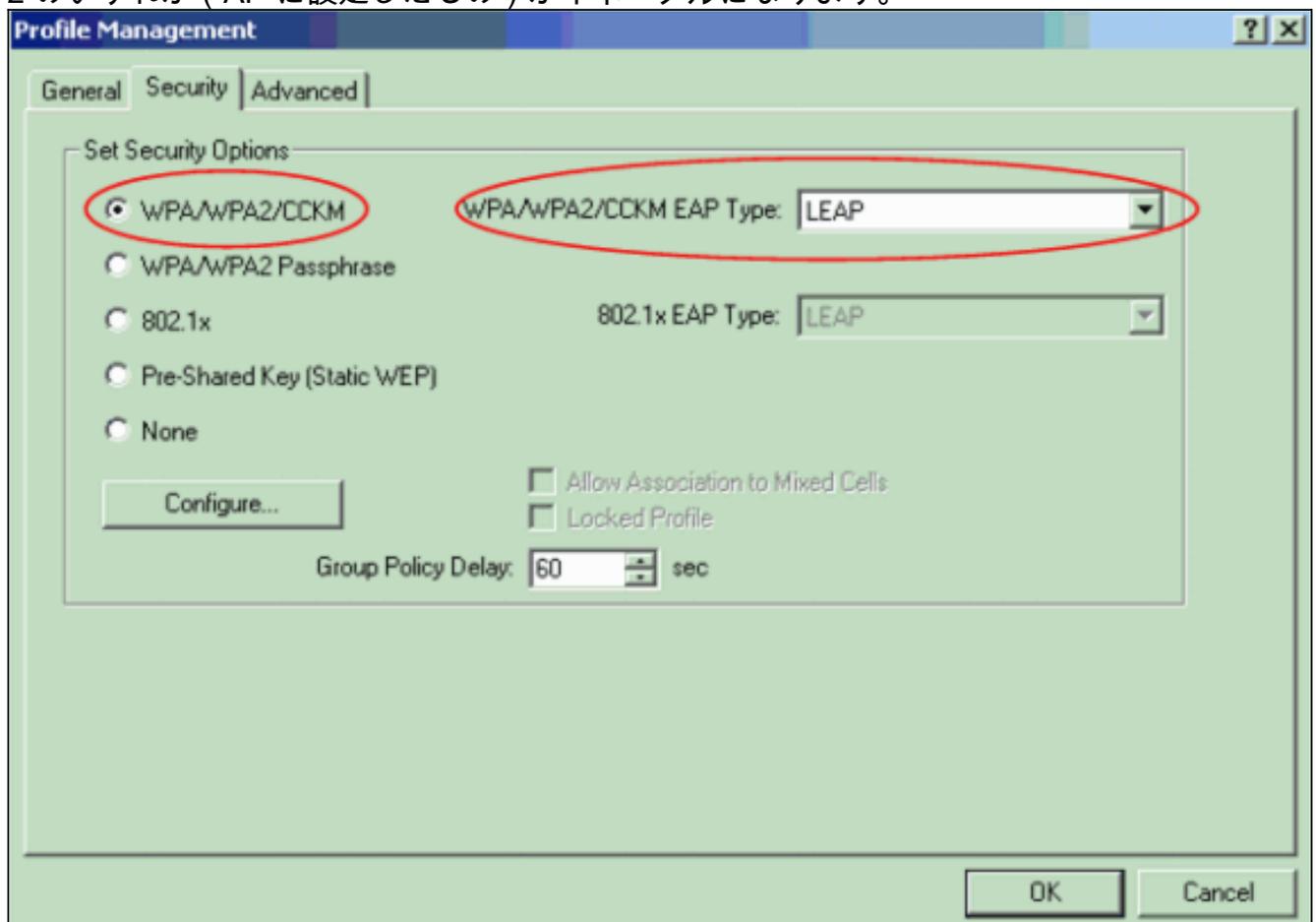
次の手順を実行します。

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。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 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 WPA2 を使用しています。注: この SSID は、AP で WPA 2 に設定されている SSID と一致している必要があります。



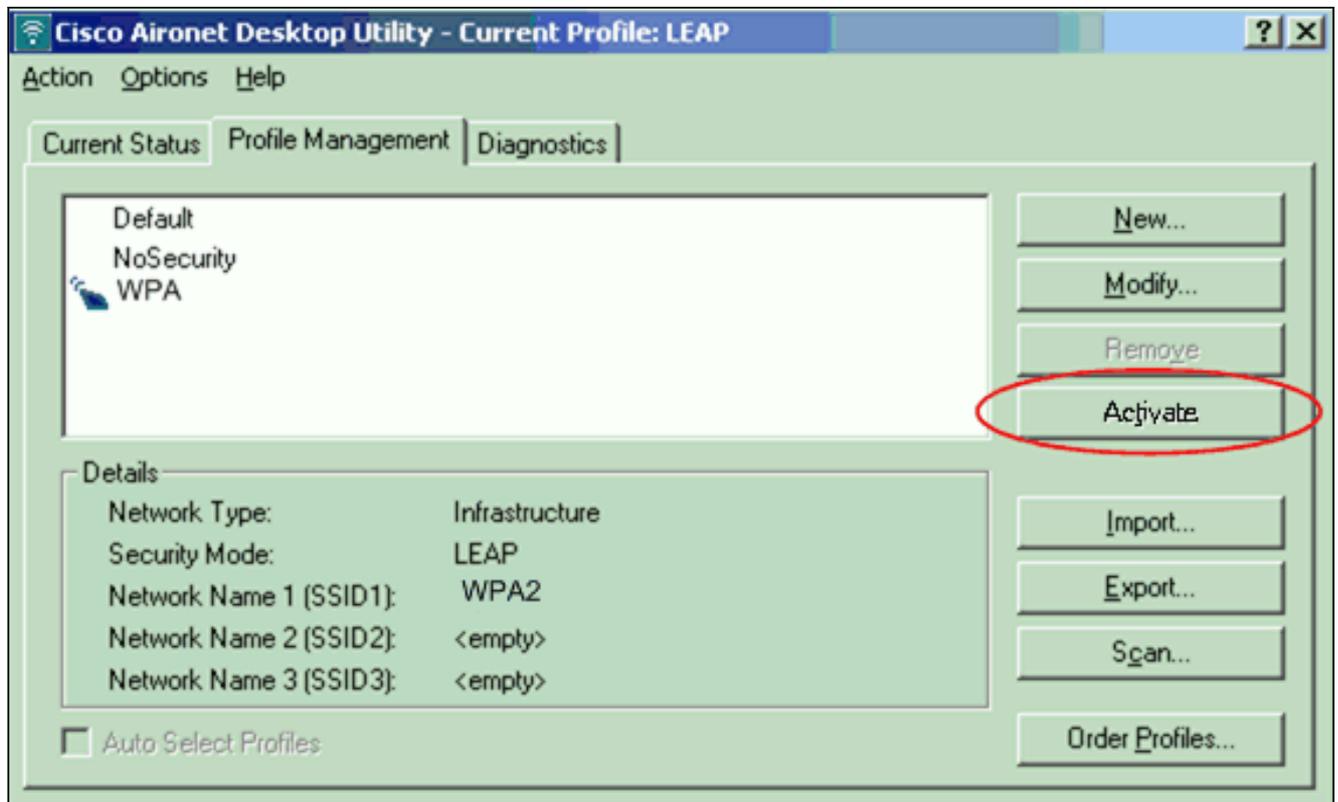
2. [Security] タブをクリックし、[WPA/WPA2/CCKM] をクリックして、[WPA/WPA2/CCKM EAP Type] メニューから [LEAP] を選択します。このアクションにより、WPA または WPA 2 のいずれか ( AP に設定したもの ) がイネーブルになります。



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。

The image shows a screenshot of the 'LEAP Settings' dialog box. The window title is 'LEAP Settings'. At the top, there is a checked checkbox labeled 'Always Resume the Secure Session'. Below this is a section titled 'Username and Password Settings'. Inside this section, there are four radio button options: 'Use Temporary User Name and Password', 'Use Windows User Name and Password', 'Automatically Prompt for User Name and Password' (which is selected and circled in red), and 'Manually Prompt for User Name and Password'. Below the radio buttons is another section with a radio button option 'Use Saved User Name and Password'. This section contains four text input fields: 'User Name:', 'Password:', 'Confirm Password:', and 'Domain:'. Below these fields are two checkboxes: 'Include Windows Logon Domain with User Name' (unchecked) and 'No Network Connection Unless User Is Logged In' (checked). At the bottom of this section is a label 'Authentication Timeout Value (in seconds)' followed by a spin box set to '30'. At the very bottom of the dialog are two buttons: 'OK' and '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。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。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、設定が正常に動作していることを確認します。

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

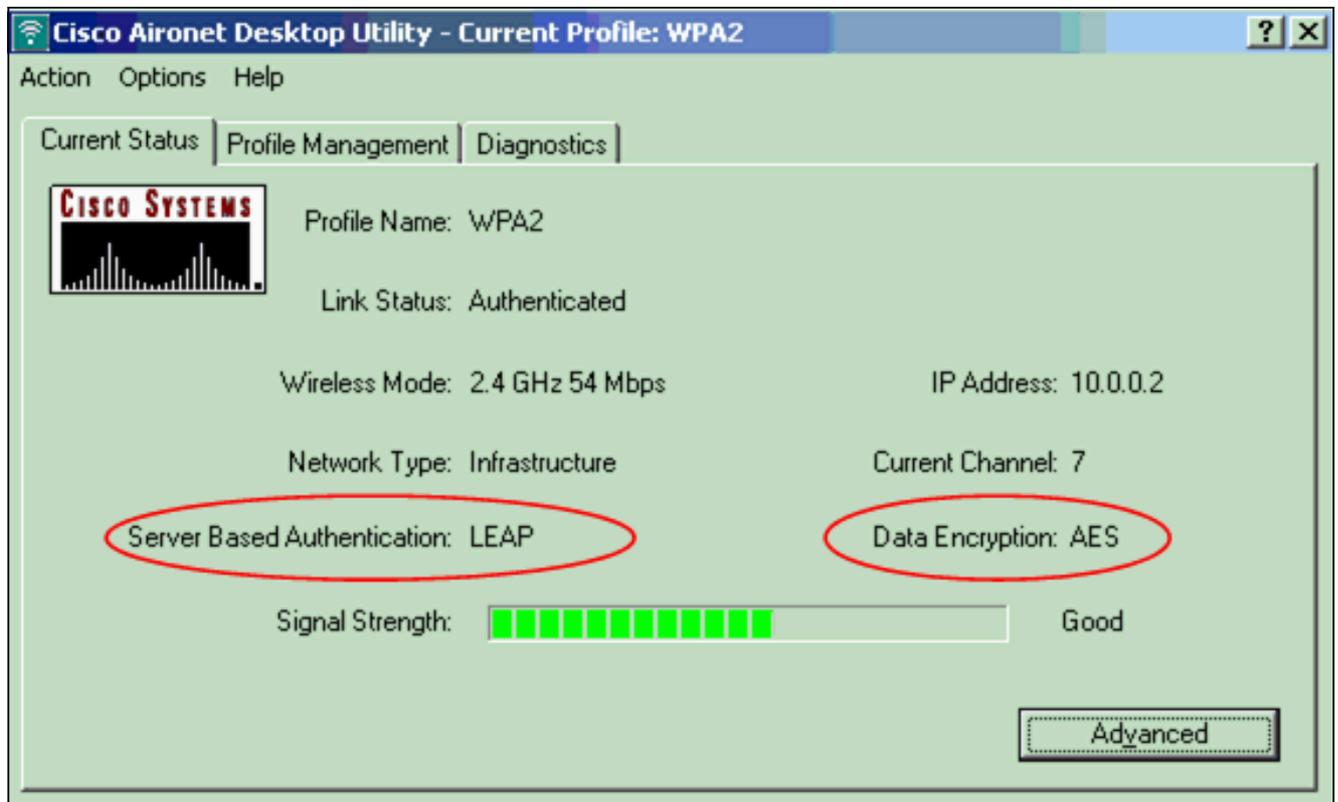
Steps	Status
1. Starting LEAP Authentication	Success
2. Checking Link Status	Success
3. Renewing IP address	Success
4. Detecting IPX Frame Type	Success
5. Finding Domain Controller	Success

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。

## 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。

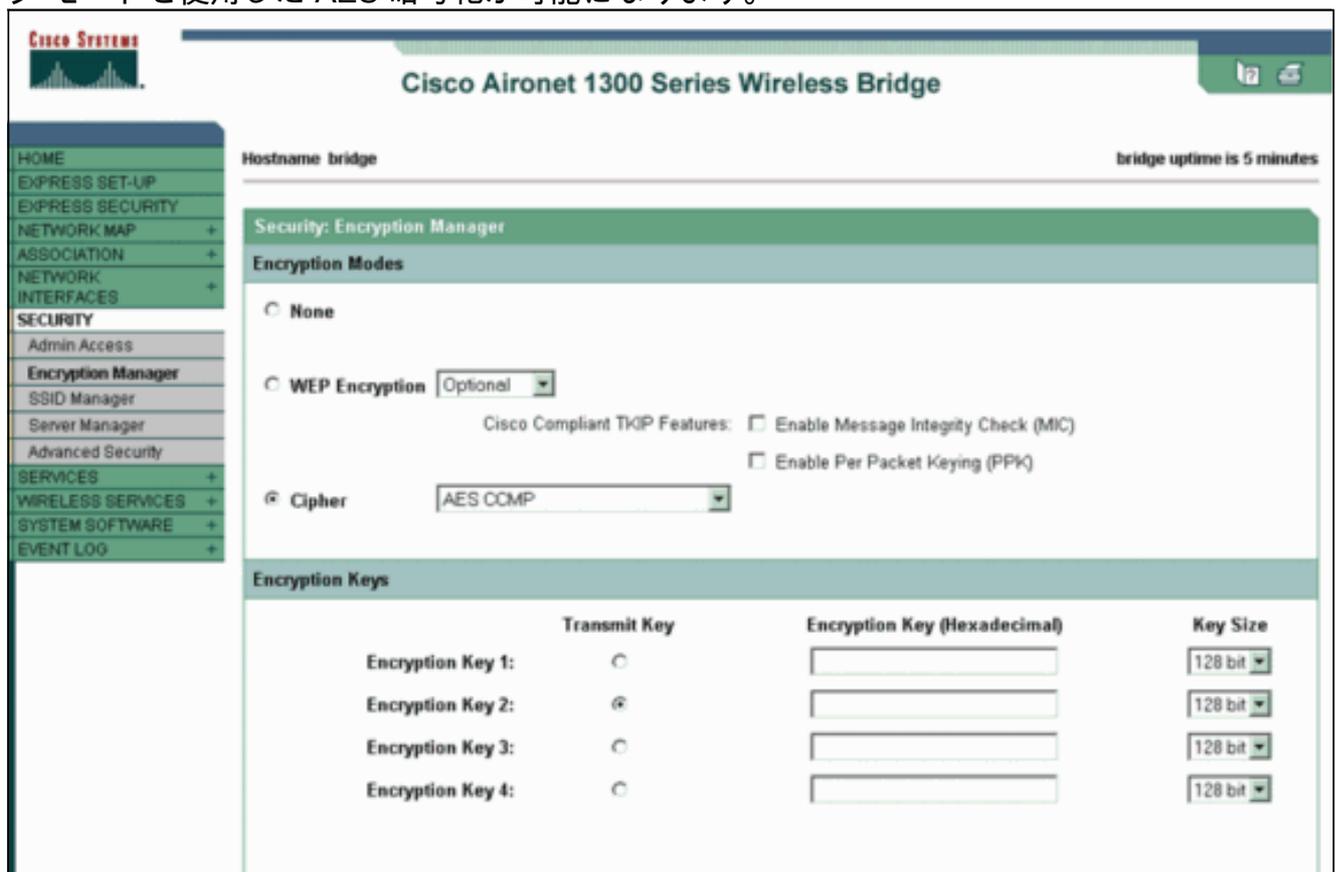
## ネットワーク構成

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

次の手順を実行します。

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 left sidebar contains a navigation menu with categories like HOME, EXPRESS SET-UP, SECURITY, and SERVICES. The main content area is titled 'Security: Encryption Manager' and includes the following sections:

- Encryption Modes:** Radio buttons for 'None', 'WEP Encryption' (with an 'Optional' dropdown), and 'Cipher' (selected). Under 'Cipher', a dropdown menu shows 'AES CCMP'. There are also checkboxes for 'Cisco Compliant TKIP Features' such as 'Enable Message Integrity Check (MIC)' and 'Enable Per Packet Keying (PPK)'.
- Encryption Keys:** A table with four rows for 'Encryption Key 1' through 'Encryption Key 4'. Each row has a radio button for 'Transmit Key', a text input field for 'Encryption Key (Hexadecimal)', and a dropdown menu for 'Key Size' (all set to '128 bit').

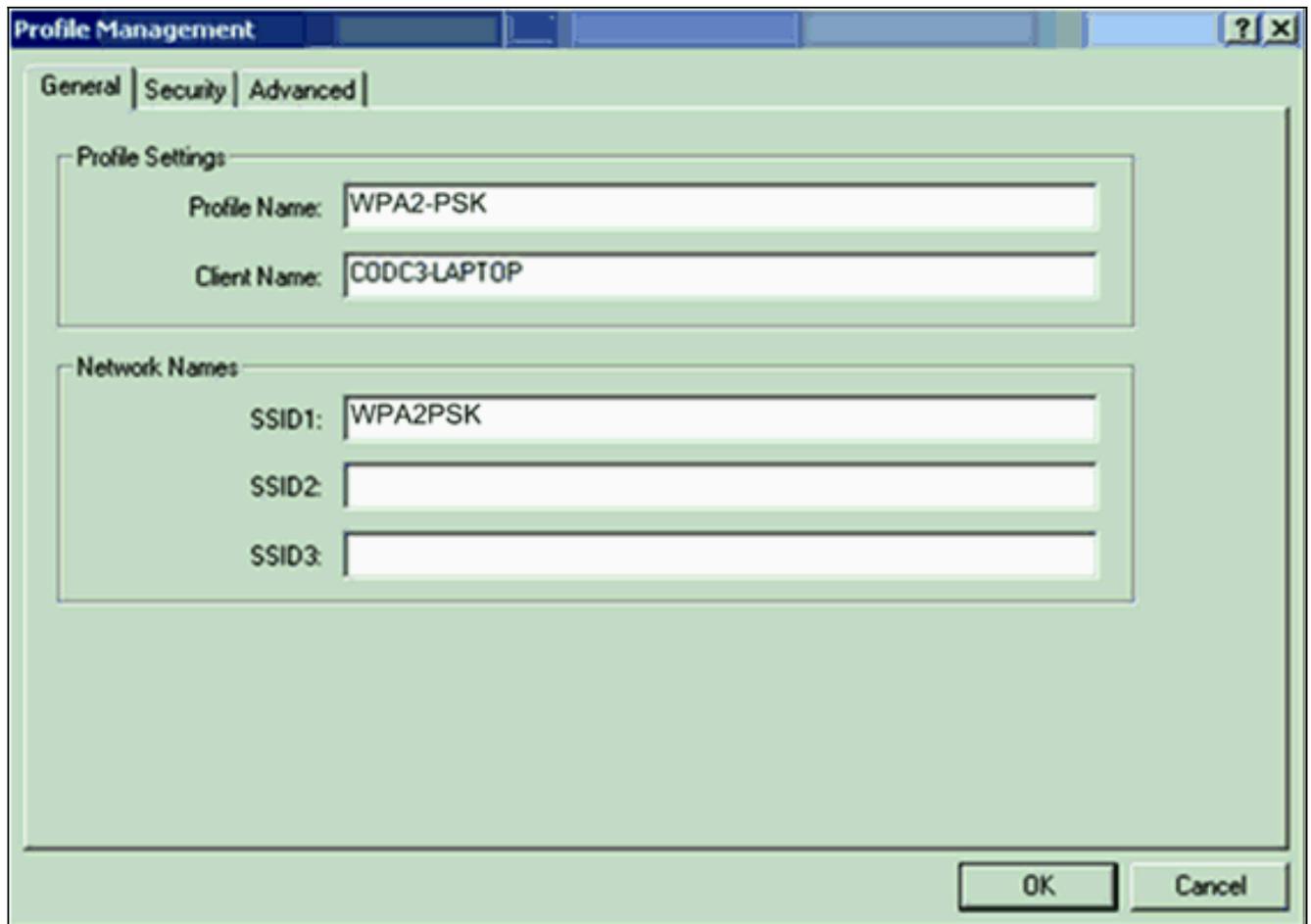
[Apply] をクリックします。

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。

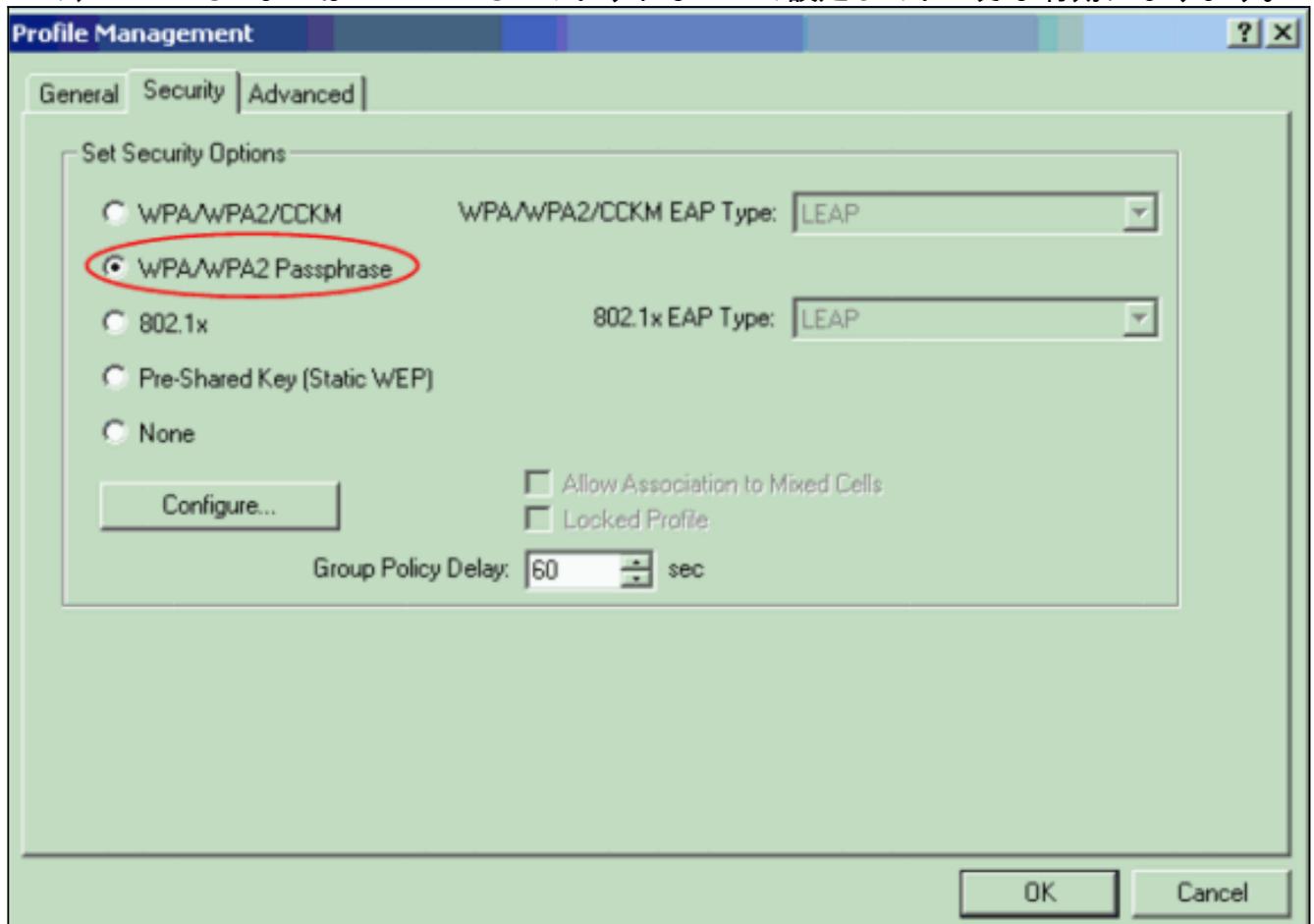
The screenshot displays the configuration interface for a Cisco Aironet 1300 Series Wireless Bridge. The page title is "Cisco Aironet 1300 Series Wireless Bridge" and the hostname is "bridge". The bridge uptime is 7 minutes. The left sidebar shows the navigation menu with "SECURITY" expanded to "SSID 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。





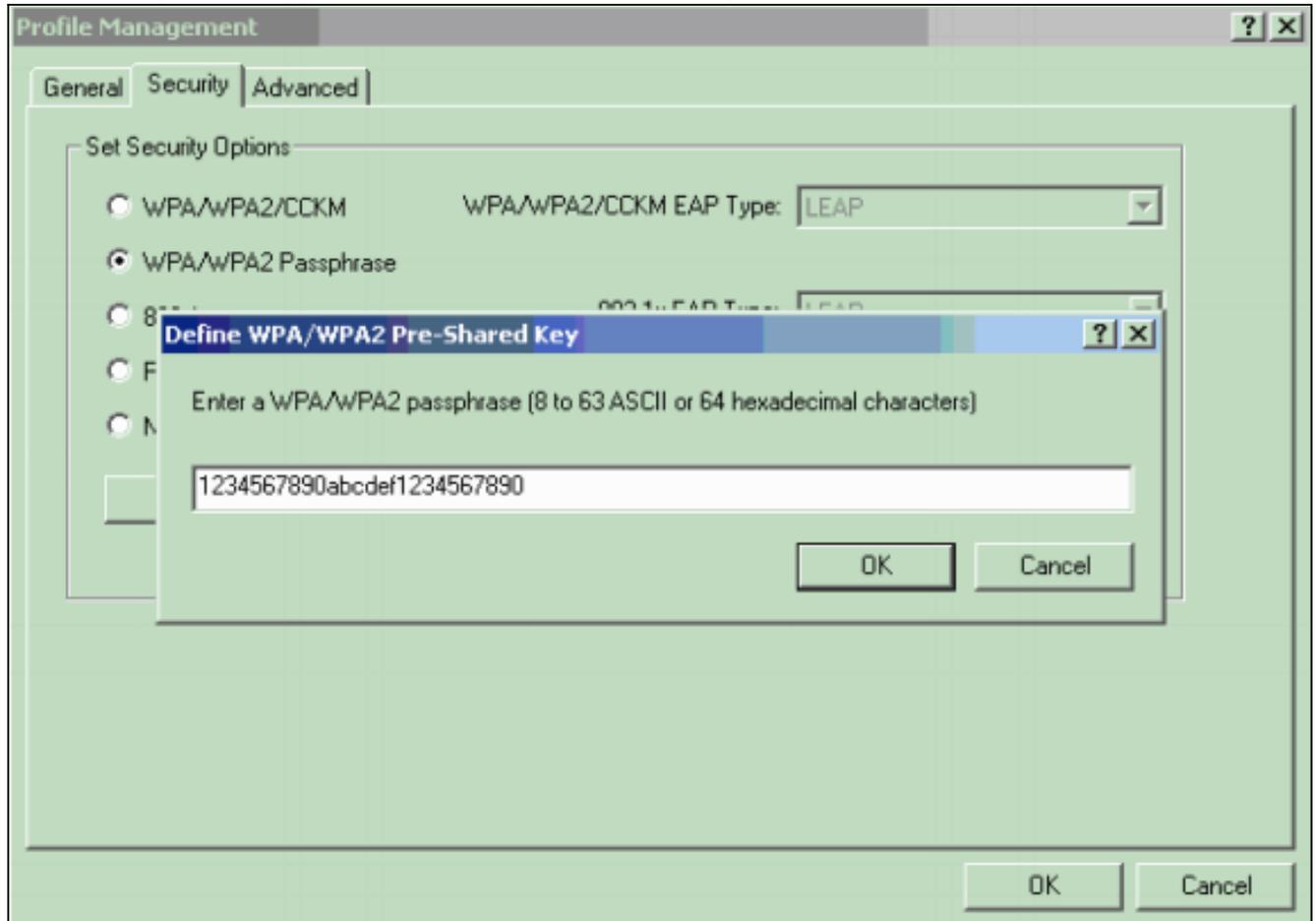
2. [Security] タブをクリックして、[WPA/WPA2 Passphrase] をクリックします。この操作によって、WPA PSK または WPA 2 PSK のいずれか AP で設定している方が有効になります。



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。



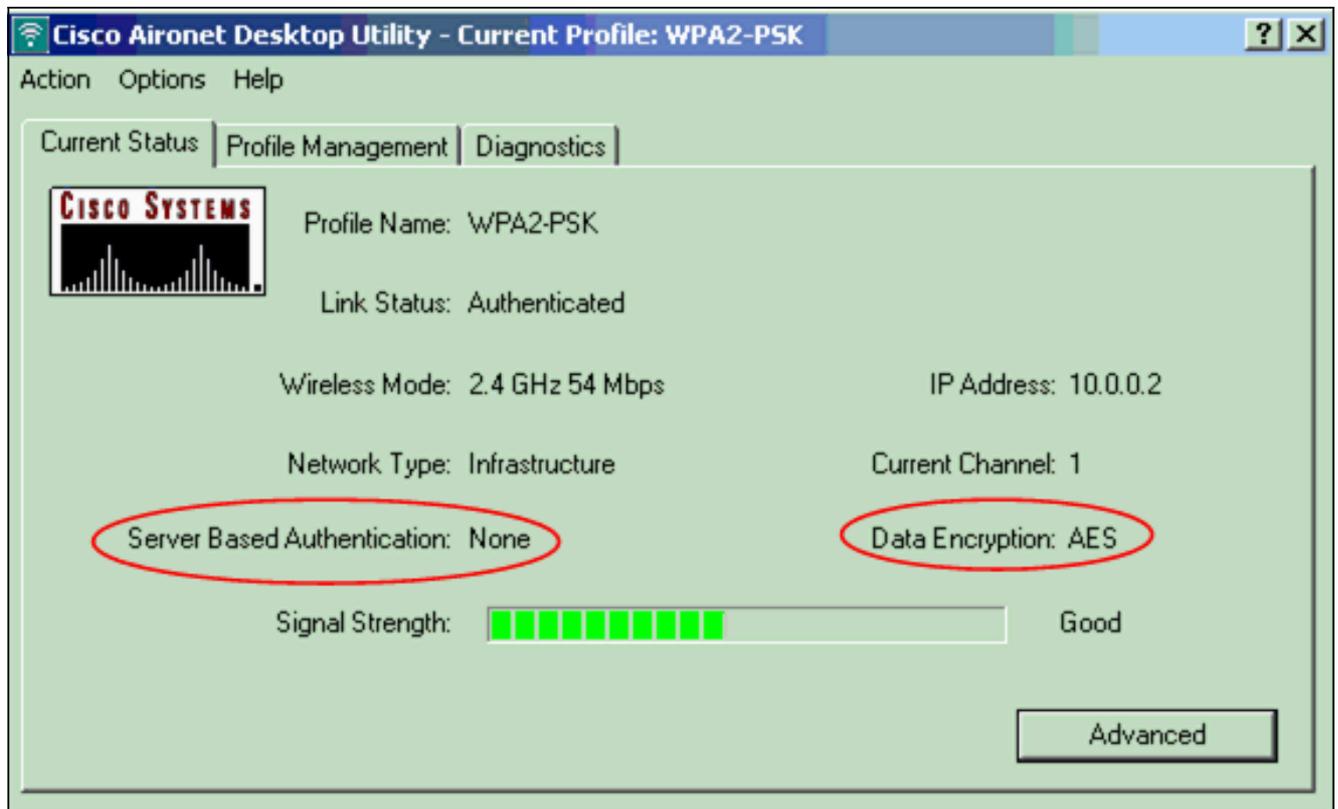
5. [OK] をクリックしてパスフレーズを保存し、[Profile Management] ウィンドウに戻ります。

## 確認

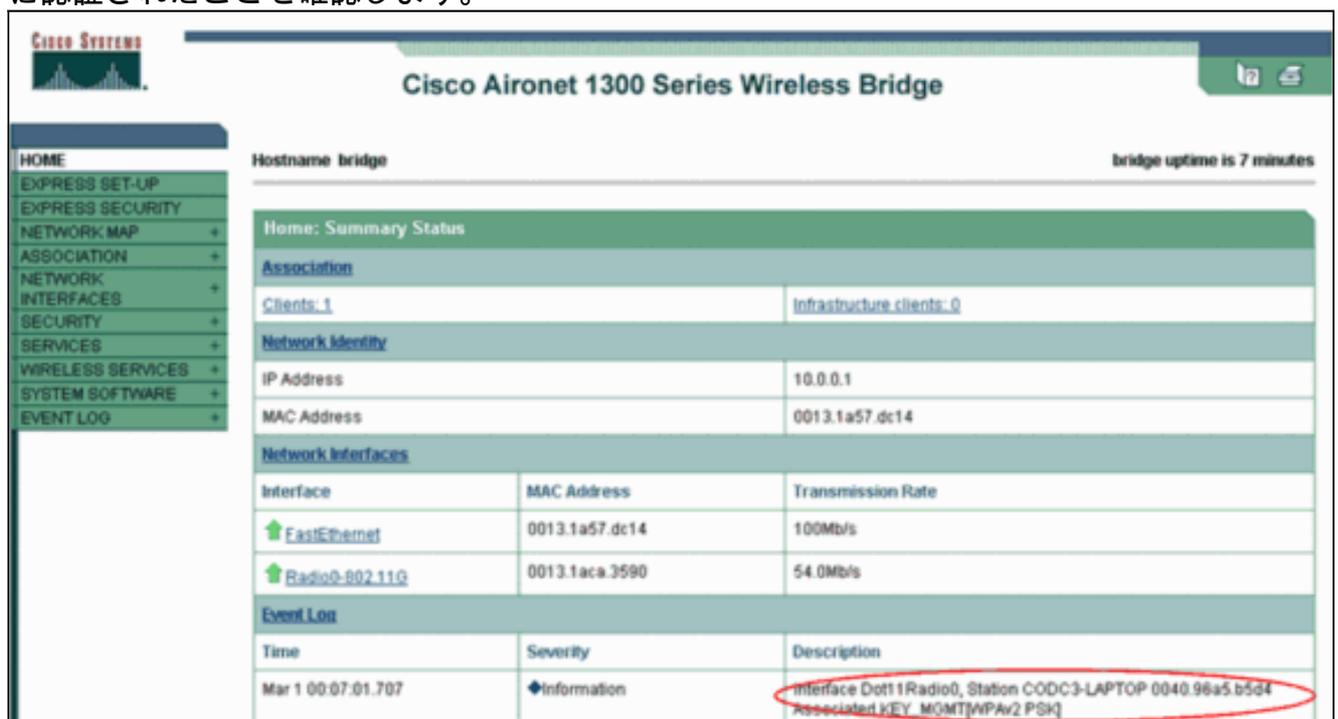
ここでは、設定が正常に動作していることを確認します。

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](#)
- [認証タイプの設定 \(英語\)](#)

- [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](#)