

# Esempio di configurazione di Wi-Fi Protected Access 2 (WPA 2)

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Premesse](#)

[Supporto WPA 2 con apparecchiature Cisco Aironet](#)

[Configura in modalità Enterprise](#)

[Installazione della rete](#)

[Configurare il punto di accesso](#)

[Configurazione CLI](#)

[Configurare l'adattatore client](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Configurazione in modalità personale](#)

[Installazione della rete](#)

[Configurare il punto di accesso](#)

[Configurare l'adattatore client](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

## [Introduzione](#)

In questo documento vengono spiegati i vantaggi derivanti dall'uso della funzionalità Wi-Fi Protected Access 2 (WPA 2) in una LAN wireless (WLAN). Il documento contiene due esempi su come implementare WPA 2 su una WLAN. Il primo esempio mostra come configurare WPA 2 in modalità enterprise, il secondo esempio come configurare WPA 2 in modalità Personal.

**Nota:** WPA funziona con EAP (Extensible Authentication Protocol).

## [Prerequisiti](#)

### [Requisiti](#)

Prima di provare la configurazione, accertarsi di avere una conoscenza di base di questi

argomenti:

- WPA
- Soluzioni per la sicurezza WLAN **Nota:** per informazioni sulle soluzioni di sicurezza WLAN di Cisco, consultare la [panoramica](#) della [sicurezza LAN wireless di Cisco Aironet](#).

## Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Access point (AP)/bridge Cisco Aironet 1310G con software Cisco IOS® versione 12.3(2)JA
- Aironet 802.11a/b/g CB21AG Client Adapter con firmware 2.5
- Aironet Desktop Utility (ADU) con firmware 2.5

**Nota:** i software per le schede client Aironet CB21AG e PI21AG non sono compatibili con altri software per schede client Aironet. È necessario utilizzare l'ADU con le schede CB21AG e PI21AG e l'Aironet Client Utility (ACU) per tutte le altre schede client Aironet. Per ulteriori informazioni su come installare la scheda CB21AG e l'ADU, fare riferimento a [Installazione della scheda client](#).

**Nota:** questo documento utilizza un access point/bridge con antenna integrata. Se si utilizza un punto di accesso/ponte che richiede un'antenna esterna, verificare che le antenne siano collegate al punto di accesso/ponte. In caso contrario, il punto di accesso/bridge non è in grado di connettersi alla rete wireless. Alcuni modelli AP/bridge sono dotati di antenne integrate, mentre altri necessitano di un'antenna esterna per il funzionamento generale. Per informazioni sui modelli AP/bridge forniti con antenne interne o esterne, consultare la Guida agli ordini/la Guida del prodotto della periferica appropriata.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento [Cisco sulle convenzioni nei suggerimenti tecnici](#).

## Premesse

WPA è una soluzione di sicurezza basata su standard di Wi-Fi Alliance che affronta le vulnerabilità nelle WLAN native. WPA offre protezione avanzata dei dati e controllo dell'accesso per i sistemi WLAN. WPA risolve tutte le vulnerabilità WEP (Wired Equivalent Privacy) conosciute nell'implementazione della sicurezza IEEE 802.11 originale e offre una soluzione di sicurezza immediata per le WLAN sia negli ambienti aziendali che in quelli di piccole aziende e uffici privati (SOHO).

WPA 2 è la nuova generazione di protezione Wi-Fi. WPA 2 è l'implementazione interoperabile Wi-Fi Alliance dello standard IEEE 802.11i ratificato. WPA 2 implementa l'algoritmo di crittografia AES (Advanced Encryption Standard) raccomandato dal NIST (National Institute of Standards and

Technology) con l'uso della modalità contatore con CCMP (Cipher Block Chaining Message Authentication Code Protocol). La modalità contatore AES è una cifratura a blocchi che cripta blocchi di dati a 128 bit alla volta con una chiave di cifratura a 128 bit. L'algoritmo CCMP produce un codice di integrità dei messaggi (MIC) che fornisce l'autenticazione dell'origine dei dati e l'integrità dei dati per il frame wireless.

**Nota:** il protocollo CCMP è anche noto come CBC-MAC.

WPA 2 offre un livello di sicurezza più elevato rispetto a WPA perché AES offre una crittografia più avanzata rispetto a TKIP (Temporal Key Integrity Protocol). TKIP è l'algoritmo di crittografia utilizzato da WPA. WPA 2 crea nuove chiavi di sessione per ogni associazione. Le chiavi di crittografia utilizzate per ogni client della rete sono univoche e specifiche per tale client. In ultima analisi, ogni pacchetto inviato via etere viene crittografato con una chiave univoca. La sicurezza è migliorata grazie all'utilizzo di una nuova chiave di crittografia univoca, che non consente il riutilizzo della chiave. WPA è ancora considerato sicuro e TKIP non è stato interrotto. Tuttavia, Cisco consiglia ai clienti di passare a WPA 2 il prima possibile.

WPA e WPA 2 supportano due modalità di funzionamento:

- Modalità Enterprise
- Modalità personale

Questo documento descrive l'implementazione di queste due modalità con WPA 2.

## [Supporto WPA 2 con apparecchiature Cisco Aironet](#)

WPA 2 è supportato da questa apparecchiatura:

- Aironet serie 1130AG AP e serie 1230AG AP
- Aironet serie 1100 AP
- Aironet serie 1200 AP
- Aironet serie 1300 AP

**Nota:** dotare questi access point di radio 802.11g e usare il software Cisco IOS versione 12.3(2)JA o successive.

WPA 2 e AES sono inoltre supportati su:

- Aironet serie 1200 moduli radio con i numeri di parte AIR-RM21A e AIR-RM22A **Nota:** il modulo radio Aironet 1200 con numero di parte AIR-RM20A non supporta WPA 2.
- Aironet 802.11a/b/g Client Adapter con firmware versione 2.5

**Nota:** i prodotti Cisco Aironet serie 350 non supportano WPA 2 perché le loro radio non supportano AES.

**Nota:** Cisco Aironet serie 1400 Wireless Bridge non supporta WPA 2 o AES.

## [Configura in modalità Enterprise](#)

Il termine **modalità enterprise** si riferisce a prodotti che sono stati testati per essere interoperabili sia in modalità PSK (Pre-Shared Key) che IEEE 802.1x per l'autenticazione. Lo standard 802.1x è considerato più sicuro di qualsiasi altro framework di autenticazione legacy a causa della sua flessibilità nel supporto di diversi meccanismi di autenticazione e algoritmi di crittografia più

avanzati. WPA 2 in modalità enterprise esegue l'autenticazione in due fasi. La configurazione dell'autenticazione aperta avviene nella prima fase. La seconda fase è l'autenticazione 802.1x con uno dei metodi EAP. AES fornisce il meccanismo di crittografia.

In modalità enterprise, i client e i server di autenticazione si autenticano reciprocamente utilizzando un metodo di autenticazione EAP e il client e il server generano una chiave master Pairwise (PMK). Con WPA 2, il server genera la chiave PMK in modo dinamico e la passa all'access point.

In questa sezione viene descritta la configurazione necessaria per implementare WPA 2 in modalità operativa enterprise.

## [Installazione della rete](#)

In questa configurazione, un access point/bridge Aironet 1310G con Cisco Lightweight Extensible Authentication Protocol (LEAP) autentica un utente con una scheda client compatibile con WPA 2. La gestione delle chiavi avviene con l'uso di WPA 2, su cui è configurata la crittografia AES-CCMP. Il punto di accesso è configurato come server RADIUS locale che esegue l'autenticazione LEAP. Per implementare questa configurazione, è necessario configurare l'adattatore client e l'access point. Le sezioni [Configurazione dell'access point](#) e [Configurazione dell'adattatore client](#) mostrano la configurazione sull'access point e sull'adattatore client.

## [Configurare il punto di accesso](#)

Completare la procedura seguente per configurare l'access point con la GUI:

1. Configurare il punto di accesso come server RADIUS locale che esegue l'autenticazione LEAP. Scegliere **Sicurezza > Server Manager** nel menu a sinistra e definire l'indirizzo IP, le porte e il segreto condiviso del server RADIUS. Poiché questa configurazione configura il punto di accesso come server RADIUS locale, utilizzare l'indirizzo IP del punto di accesso. Usare le porte 1812 e 1813 per il funzionamento del server RADIUS locale. Nell'area Priorità predefinite server definire la priorità di autenticazione EAP predefinita come 10.0.0.1. **Nota:** 10.0.0.1 è il server RADIUS locale.

**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

< NEW >  
 10.0.0.1

Server:  (Hostname or IP Address)  
 Shared Secret:

Authentication Port (optional):  (0-65536)  
 Accounting Port (optional):  (0-65536)

Apply Cancel

**Delete**

**Default Server Priorities**

EAP Authentication MAC Authentication Accounting

Priority 1:  Priority 1:  Priority 1:

2. Scegliere **Sicurezza > Encryption Manager** dal menu a sinistra e completare i seguenti passaggi: Dal menu Cifratura, scegliere **AES CCMP**. Questa opzione abilita la crittografia AES con l'uso della modalità contatore con CBC-MAC.

**Cisco Aironet 1300 Series Wireless Bridge**

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)

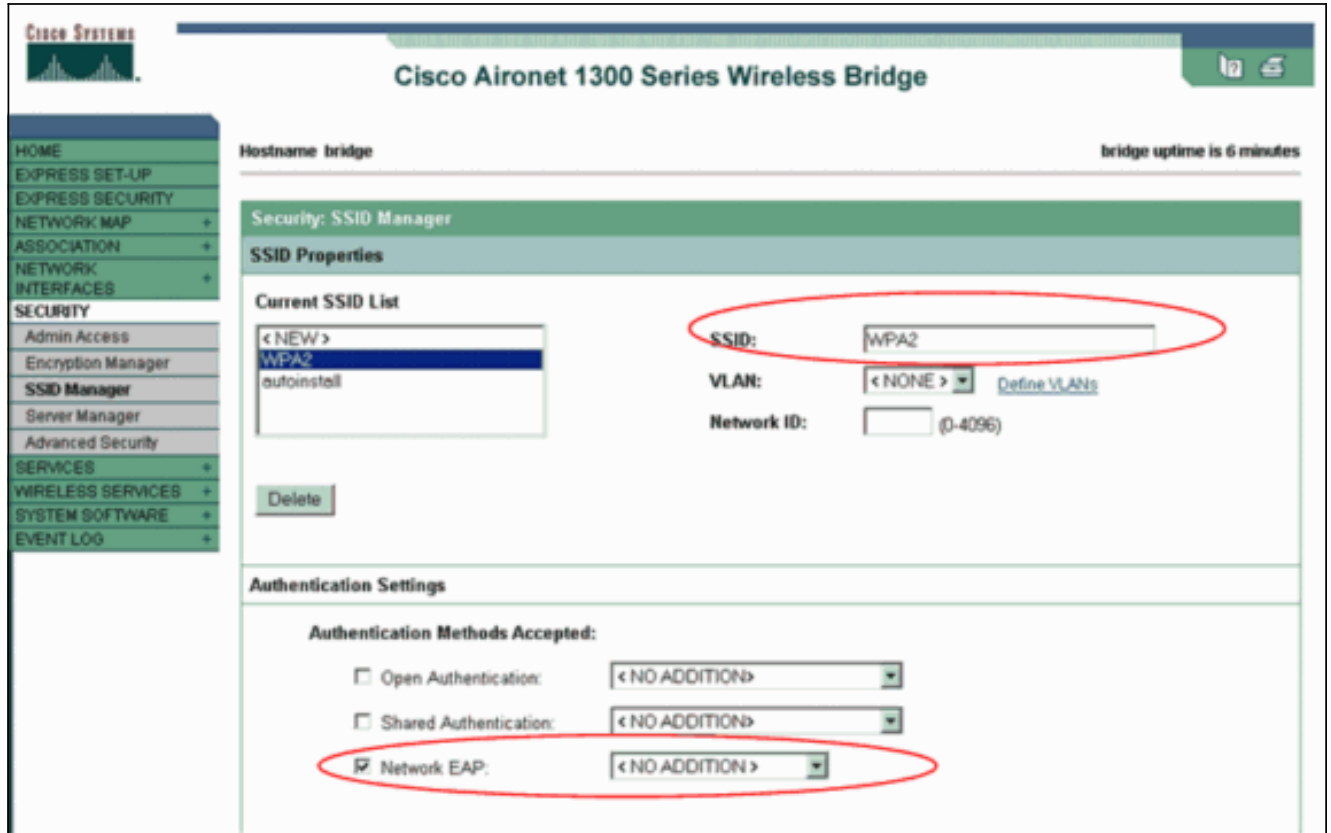
Cipher

**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 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"/>

Fare clic su **Apply** (Applica).

3. Scegliere **Protezione > Gestione SSID** e creare un nuovo SSID (Service Set Identifier) da utilizzare con WPA 2. Selezionare la casella di controllo **EAP rete** nell'area Metodi di autenticazione accettati.



**Nota:** attenersi alle seguenti linee guida quando si configura il tipo di autenticazione sull'interfaccia radio: Client Cisco: utilizzare Network EAP. Client di terze parti (che includono prodotti compatibili con Cisco Compatible Extensions [CCX]): utilizzare l'autenticazione aperta con EAP. Combinazione di client Cisco e di terze parti: scegliere sia Network EAP che Open Authentication con EAP. Scorrere la finestra Security SSID Manager fino all'area Authenticated Key Management e completare i seguenti passaggi: Dal menu Gestione chiavi, scegliere **Obbligatorio**. Selezionare la casella di controllo **WPA** a destra. Fare clic su **Apply** (Applica). **Nota:** la definizione delle VLAN è facoltativa. Se si definiscono le VLAN, i dispositivi client associati all'uso di questo SSID vengono raggruppati nella VLAN. Per ulteriori informazioni su come implementare le VLAN, consultare il documento sulla [configurazione delle VLAN](#).

**Authenticated Key Management**

**Key Management:**   CCCKM  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. Scegliere **Sicurezza > Server Radius locale** e completare i seguenti passaggi: Fare clic sulla scheda **General Set-Up (Impostazione generale)** nella parte superiore della finestra. Selezionare la casella di controllo **LEAP** e fare clic su **Applica**. Nell'area Server di accesso alla rete definire l'indirizzo IP e il segreto condiviso del server RADIUS. Per il server RADIUS locale, utilizzare l'indirizzo IP del punto di accesso.

The screenshot shows the configuration interface 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 shows the following configuration sections:

- 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
  - Apply** **Cancel**
- Network Access Servers (AAA Clients)**
  - Current Network Access Servers**
    - Input field: < NEW > (with 10.0.0.1 selected)
    - Input field: 10.0.0.1 (IP Address)
    - Input field: Shared Secret
    - Delete**
  - Apply** **Cancel**
- Individual Users**

Fare clic su **Apply** (Applica).

5. Scorrere la finestra Impostazione generale fino all'area Utenti singoli e definire i singoli utenti. La definizione dei gruppi di utenti è facoltativa.



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.
- Username:** A text field containing 'user1'.
- Password:** A password field with a red oval around it. To its right are radio buttons for 'Text' and 'NT Hash', with 'NT Hash' selected.
- Confirm Password:** An empty text field.
- Group Name:** A dropdown menu showing '<NONE >'. Below it is a checkbox for 'MAC Authentication Only'.
- Buttons:** 'Apply' and 'Cancel' buttons are at the bottom right.

**User Groups:**

- Current User Groups:** A list box containing '<NEW>'. A 'Delete' button is below it.
- Group Name:** An empty text field.
- Session Timeout (optional):** A text field with '(1-4294967295 sec)' to its right.
- Failed Authentications before Lockout (optional):** A text field with '(1-4294967295)' to its right.
- Lockout (optional):** Radio buttons for 'Infinite' and 'Interval'. 'Interval' is selected, with a text field and '(1-4294967295 sec)' to its right.
- VLAN ID (optional):** An empty text field.
- SSID (optional):** A text field with an 'Add' button to its right.
- Buttons:** A 'Delete' button is at the bottom right.

Questa configurazione definisce un utente con il nome "utente1" e una password. Inoltre, la configurazione seleziona l'hash NT per la password. Al termine della procedura descritta in questa sezione, l'access point è pronto ad accettare le richieste di autenticazione dei client. Il passaggio successivo consiste nel configurare la scheda client.

## [Configurazione CLI](#)

### Access Point

```
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

```

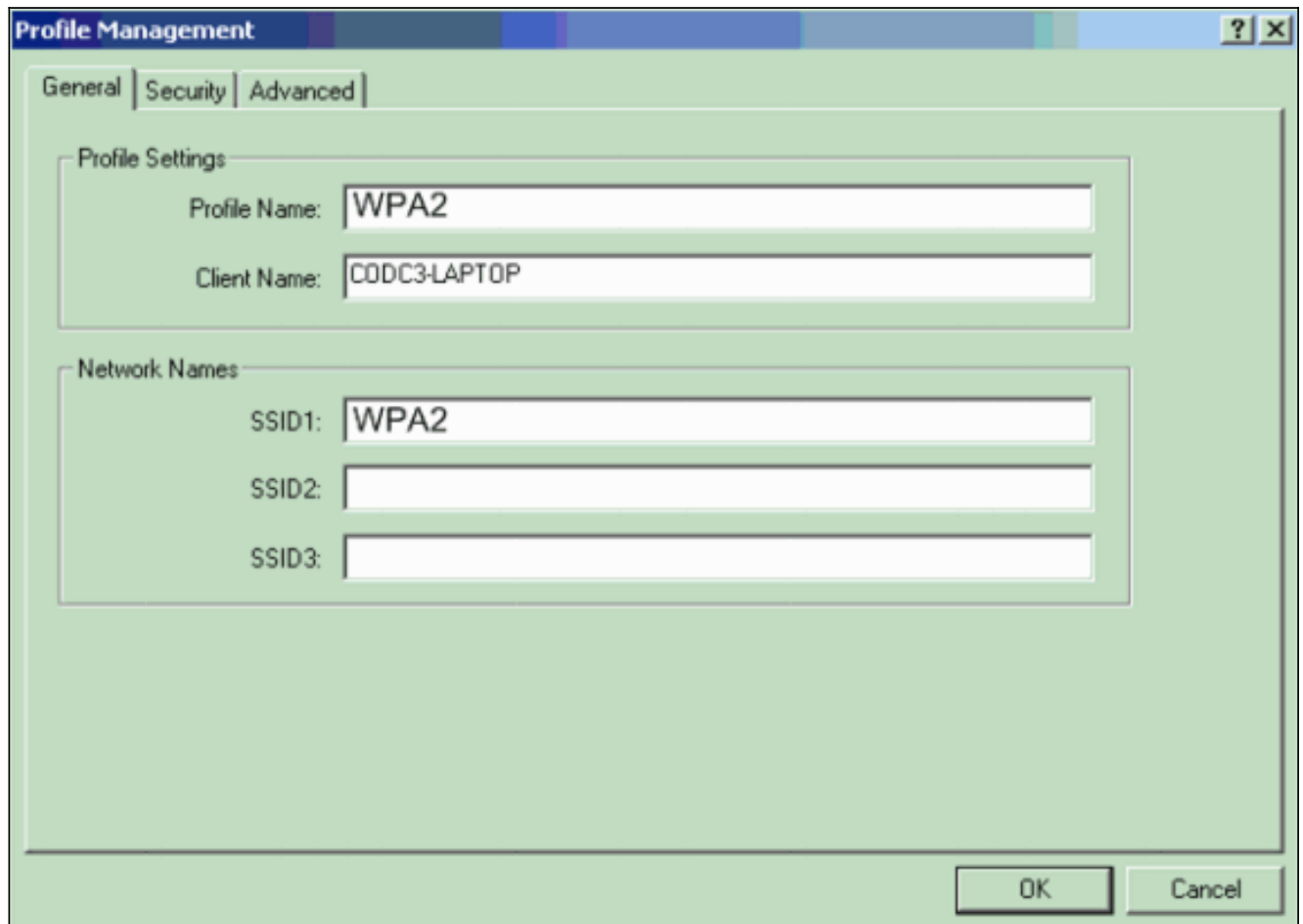
## Configurare l'adattatore client

Attenersi alla seguente procedura:

**Nota:** questo documento utilizza un adattatore client Aironet 802.11a/b/g con firmware 2.5 e illustra la configurazione dell'adattatore client con ADU versione 2.5.

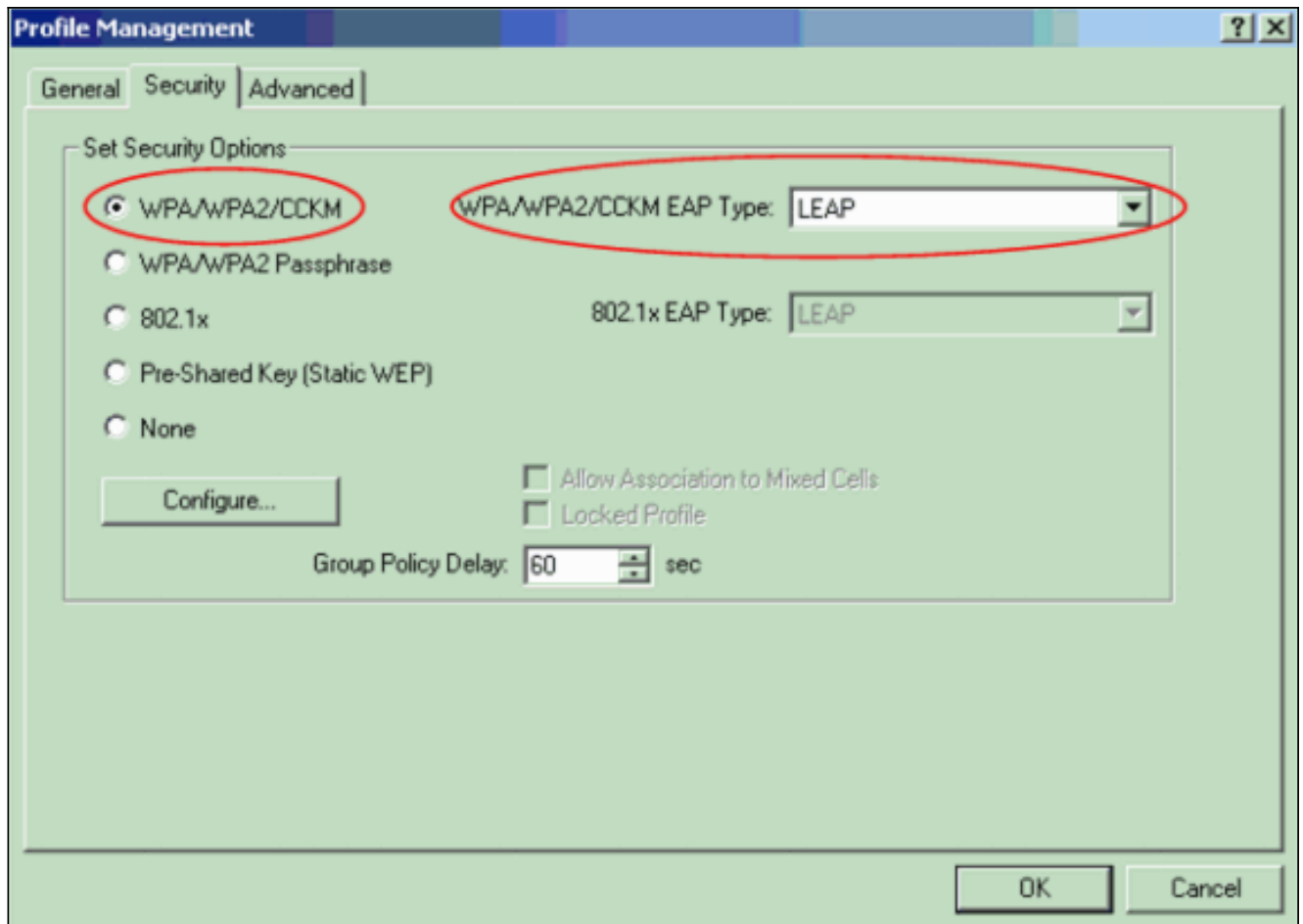
1. Nella finestra Gestione profili dell'ADU, fare clic su **Nuovo** per creare un nuovo profilo. Viene visualizzata una nuova finestra in cui è possibile impostare la configurazione per il funzionamento in modalità enterprise di WPA 2. Nella scheda Generale, immettere il Nome profilo e il SSID che verranno utilizzati dall'adattatore client. In questo esempio, il nome del profilo e il SSID sono WPA2: **Nota:** il SSID deve corrispondere al SSID configurato nell'access point per WPA

2.



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. Fare clic sulla scheda **Security**, fare clic su **WPA/WPA2/CCKM**, quindi selezionare **LEAP** dal menu WPA/WPA2/CCKM EAP Type. Questa azione consente di attivare WPA o WPA 2, a seconda di quale sia la configurazione sull'access point.



3. Per definire le impostazioni LEAP, fare clic su **Configura** (Configura).
4. Scegliere le impostazioni appropriate per il nome utente e la password, in base ai requisiti, e fare clic su **OK**. In questa configurazione viene selezionata l'opzione Richiedi automaticamente nome utente e password. Questa opzione consente di immettere manualmente il nome utente e la password quando viene eseguita l'autenticazione LEAP.

**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:

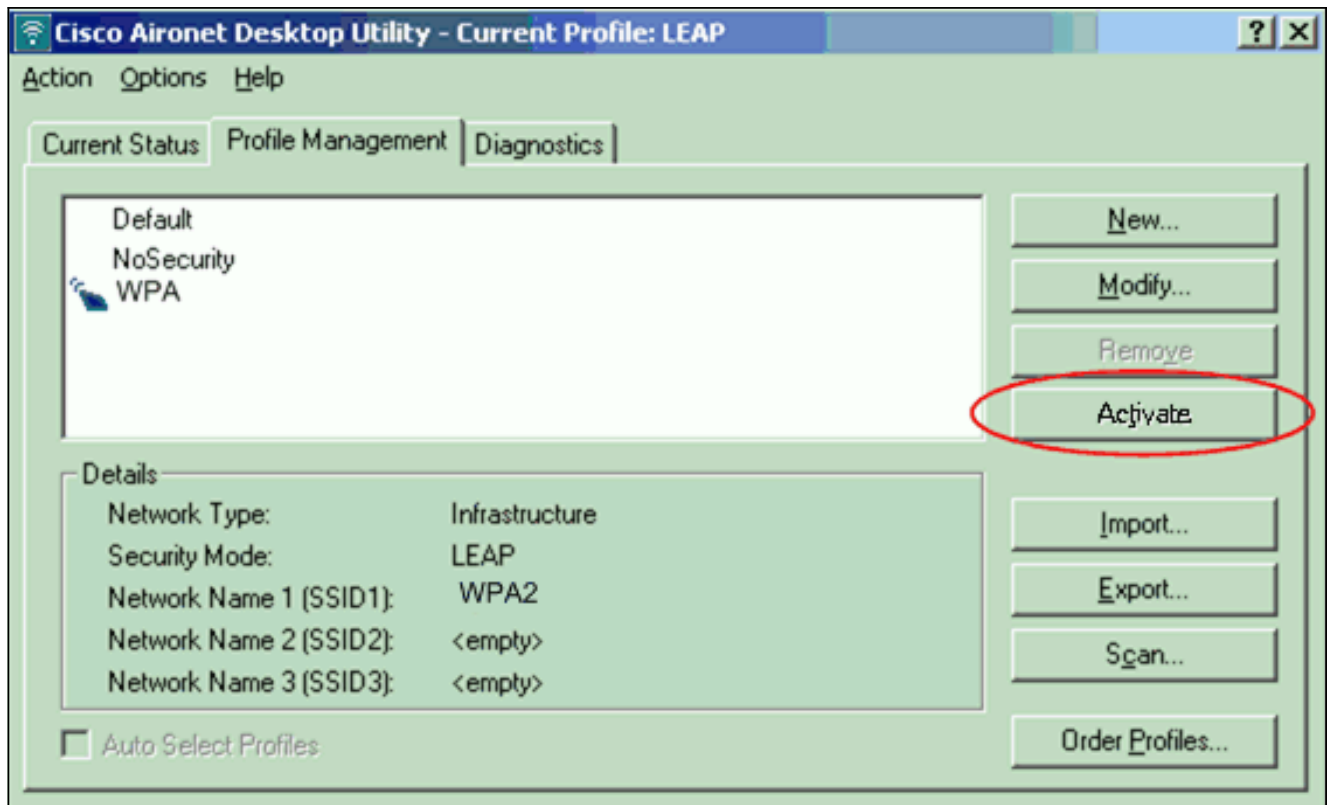
Include Windows Logon Domain with User Name

No Network Connection Unless User Is Logged In

Authentication Timeout Value (in seconds)

OK Cancel

5. Per uscire dalla finestra Gestione profili, fare clic su **OK**.
6. Fare clic su **Activate** (Attiva) per attivare questo profilo sull'adattatore client.



**Nota:** se si utilizza Microsoft Wireless Zero Configuration (WZC) per configurare la scheda client, per impostazione predefinita WPA 2 non è disponibile con WZC. Pertanto, per consentire ai client abilitati per WZC di eseguire WPA 2, è necessario installare un hot fix per Microsoft Windows XP. Per informazioni sull'installazione, vedere [Area download Microsoft - Aggiornamento per Windows XP \(KB893357\)](#). Dopo aver installato l'hot fix, è possibile configurare WPA 2 con WZC.

## Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

1. Quando viene visualizzata la finestra Enter Wireless Network Password (Immettere password rete wireless), immettere il nome utente e la

**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

password. La finestra successiva è Stato autenticazione LEAP. In questa fase vengono verificate le credenziali dell'utente rispetto al server RADIUS locale.

2. Controllare l'area di stato per verificare il risultato dell'autenticazione.

**LEAP Authentication Status**

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

Profile Name: WPA2

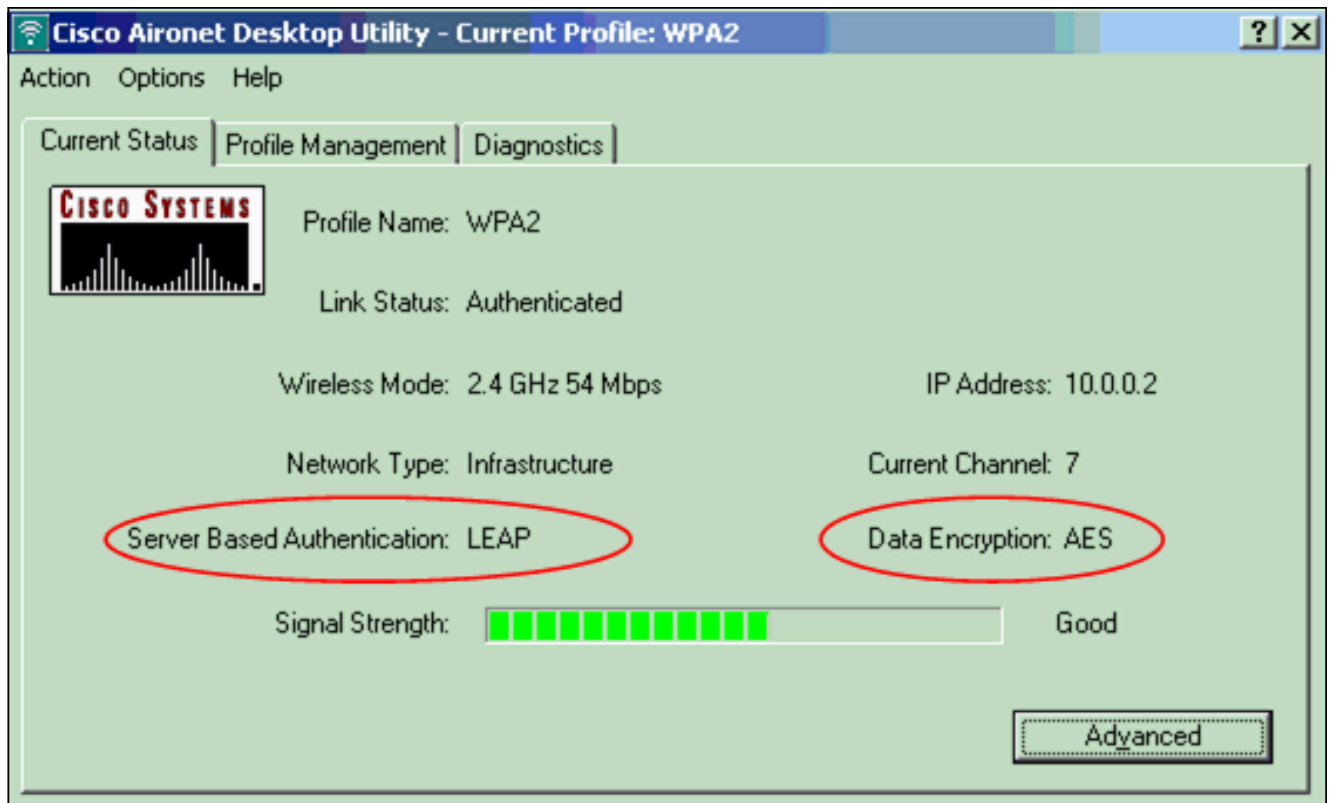
Steps	Status
1. Starting LEAP Authentication	Success
2. Checking Link Status	Success
3. Renewing IP address	Success
4. Detecting IPX Frame Type	Success
5. Finding Domain Controller	Success

Show minimized next time

Cancel

Quando l'autenticazione ha esito positivo, il client si connette alla LAN wireless.

3. Controllare lo stato corrente dell'ADU per verificare che il client utilizzi la crittografia AES e l'autenticazione LEAP. Ciò dimostra che è stata implementata la WPA 2 con autenticazione LEAP e crittografia AES nella WLAN.



4. Controllare il registro eventi AP/bridge per verificare che il client sia stato autentificato correttamente con WPA
- 2.



## Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

## Configurazione in modalità personale

Il termine **modalità personale** si riferisce a prodotti che sono stati testati per essere interoperabili



nella modalità di funzionamento solo PSK per l'autenticazione. Questa modalità richiede la configurazione manuale di una chiave già condivisa sull'access point e sui client. PSK autentica gli utenti tramite una password, o codice di identificazione, sia sulla stazione client che sull'access point. Non è necessario alcun server di autenticazione. Un client può accedere alla rete solo se la password del client corrisponde a quella del punto di accesso. La password fornisce anche il materiale per le chiavi usato da TKIP o AES per generare una chiave di crittografia per i pacchetti di dati. La modalità personale è destinata agli ambienti SOHO e non è considerata sicura per gli ambienti aziendali. In questa sezione viene fornita la configurazione necessaria per implementare WPA 2 in modalità di funzionamento personale.

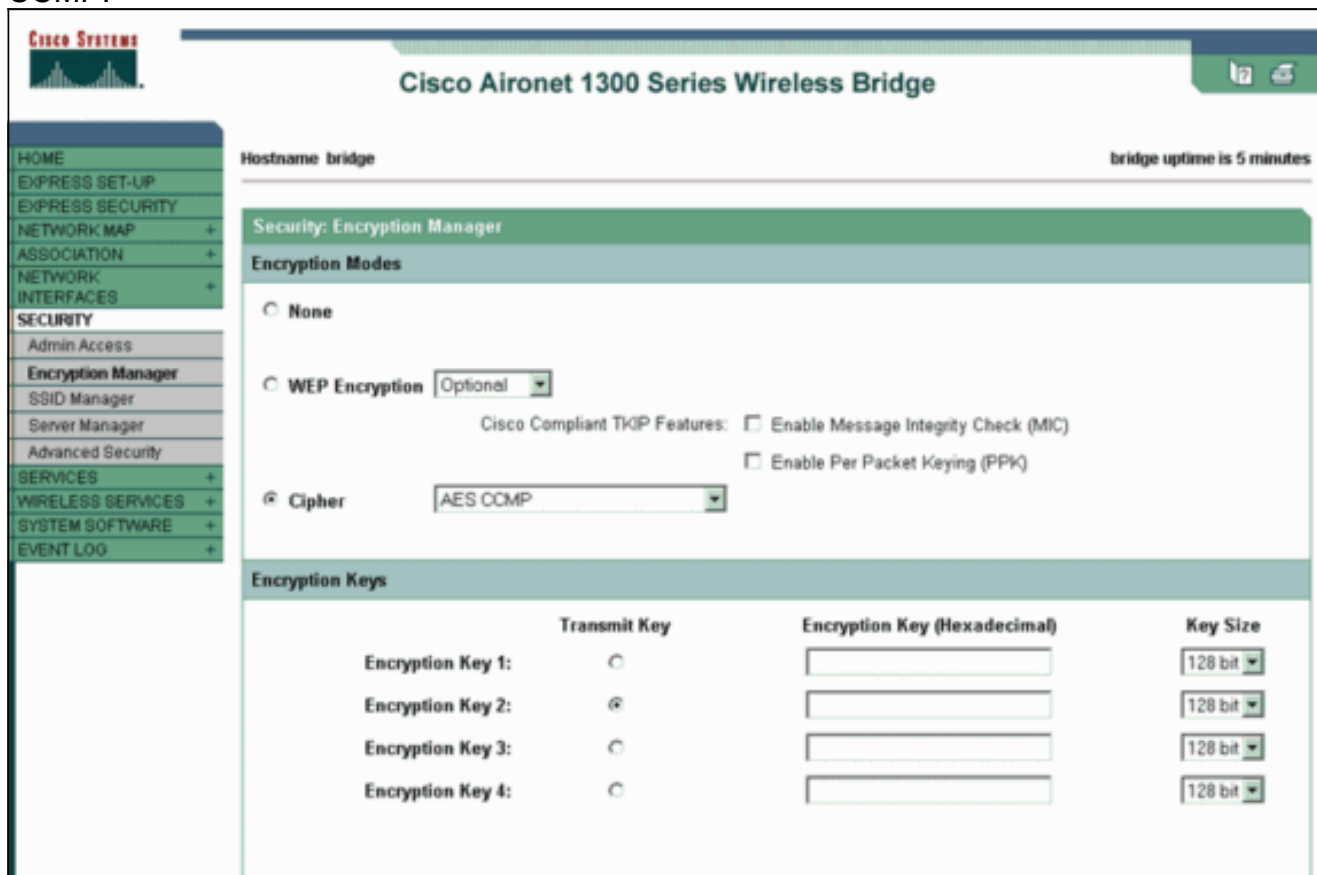
## [Installazione della rete](#)

In questa configurazione, un utente con un adattatore client compatibile con WPA 2 esegue l'autenticazione a un access point/bridge Aironet 1310G. La gestione delle chiavi avviene con l'uso di WPA 2 PSK, con la crittografia AES-CCMP configurata. Le sezioni [Configurazione dell'access point](#) e [Configurazione dell'adattatore client](#) mostrano la configurazione sull'access point e sull'adattatore client.

## [Configurare il punto di accesso](#)

Attenersi alla seguente procedura:

1. Scegliere **Sicurezza > Encryption Manager** nel menu a sinistra e completare i seguenti passaggi: Dal menu Cifratura, scegliere **AES CCMP**. Questa opzione abilita la crittografia AES con l'uso della modalità contatore con CCMP.



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 hostname is "bridge" and the bridge uptime is 5 minutes. The left sidebar contains a navigation menu with categories: HOME, EXPRESS SET-UP, EXPRESS SECURITY, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, SECURITY (with sub-items: Admin Access, Encryption Manager, SSID Manager, Server Manager, Advanced Security), SERVICES, WIRELESS SERVICES, SYSTEM SOFTWARE, and EVENT LOG. 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": "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 radio button for "Transmit Key", an input field for "Encryption Key (Hexadecimal)", and a dropdown menu for "Key Size" (all set to 128 bit).

	Transmit Key	Encryption Key (Hexadecimal)	Key Size
Encryption Key 1:	<input type="radio"/>	<input type="text"/>	128 bit
Encryption Key 2:	<input checked="" type="radio"/>	<input type="text"/>	128 bit
Encryption Key 3:	<input type="radio"/>	<input type="text"/>	128 bit
Encryption Key 4:	<input type="radio"/>	<input type="text"/>	128 bit

Fare clic su **Apply** (Applica).

2. Scegliere **Protezione > Gestione SSID** e creare un nuovo SSID da utilizzare con WPA

2. Selezionare la casella di controllo **Apri** autenticazione.

Cisco Systems  
Cisco Aironet 1300 Series Wireless Bridge  
bridge uptime is 7 minutes

Hostname bridge

Security: SSID Manager

SSID Properties

Current SSID List

< NEW >  
WPA2PSK  
tsunami

Delete

SSID: WPA2PSK  
VLAN: < NONE > Define VLANs  
Network ID: (0-4096)

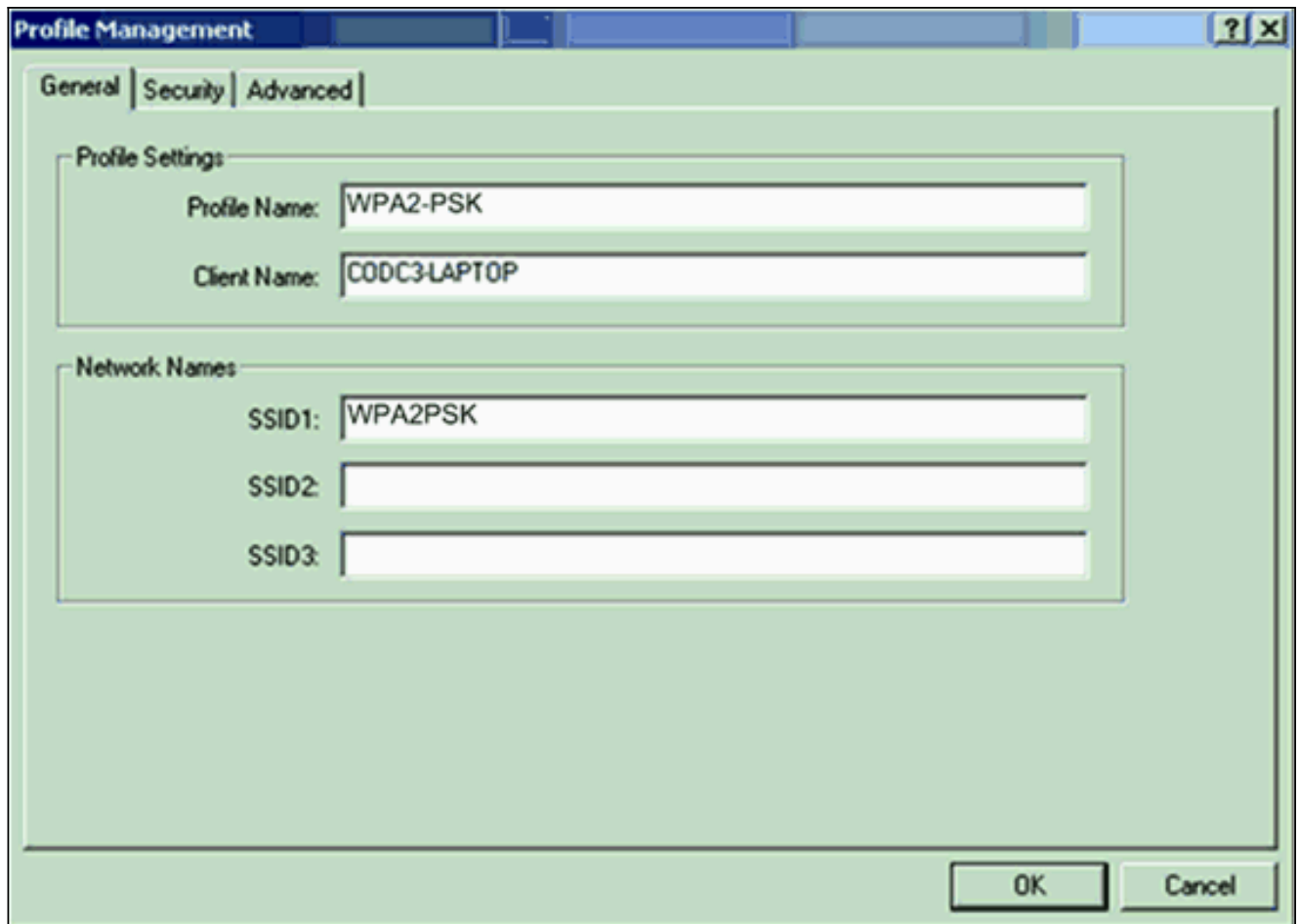
Authentication Settings

Authentication Methods Accepted:

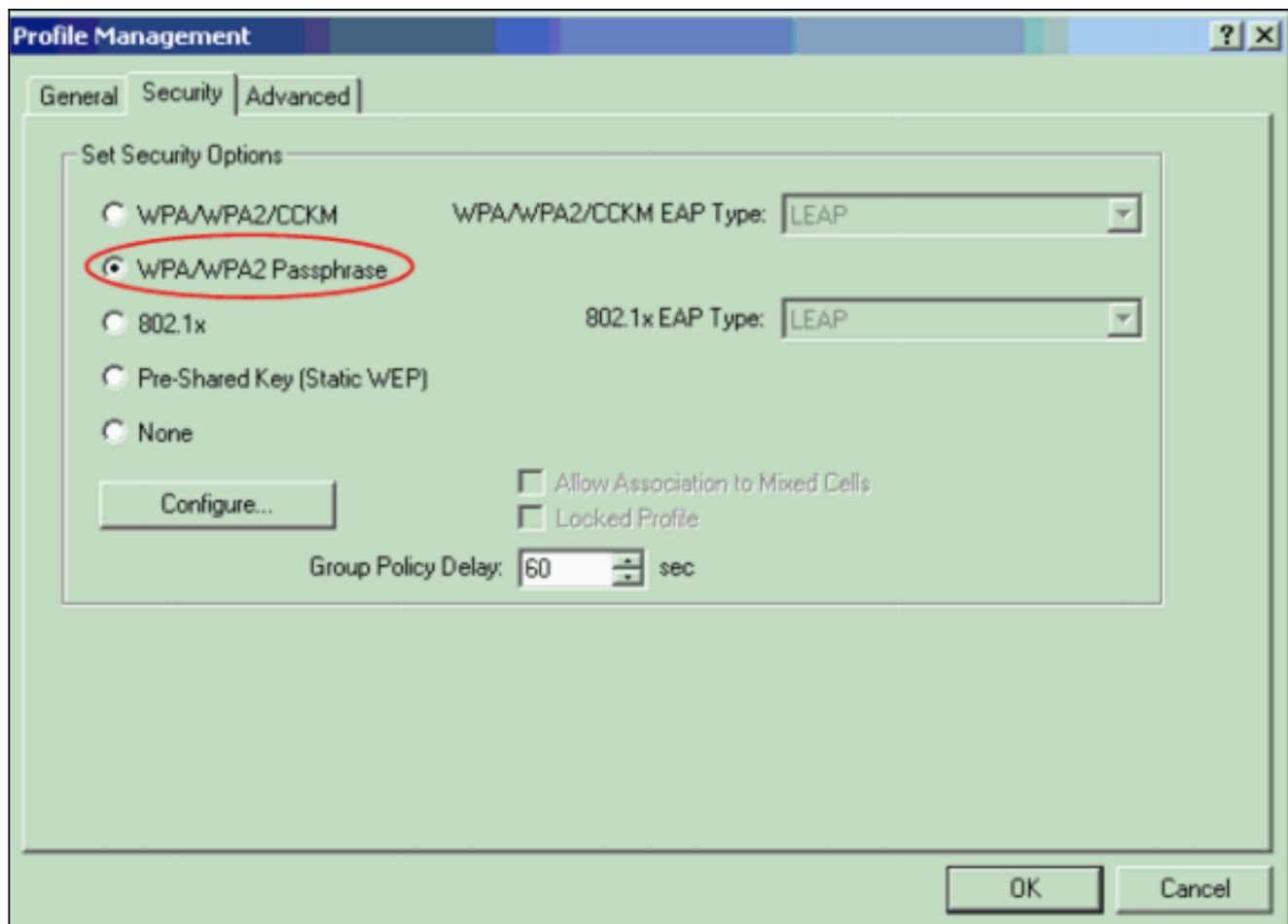
Open Authentication: < NO ADDITION >  
 Shared Authentication: < NO ADDITION >  
 Network EAP: < NO ADDITION >

Scorrere verso il basso la scheda Protezione: Aprire la finestra Gestione SSID nell'area Gestione chiavi autenticate e completare i seguenti passaggi: Dal menu Gestione chiavi, scegliere **Obbligatorio**. Selezionare la casella di controllo **WPA** a destra.

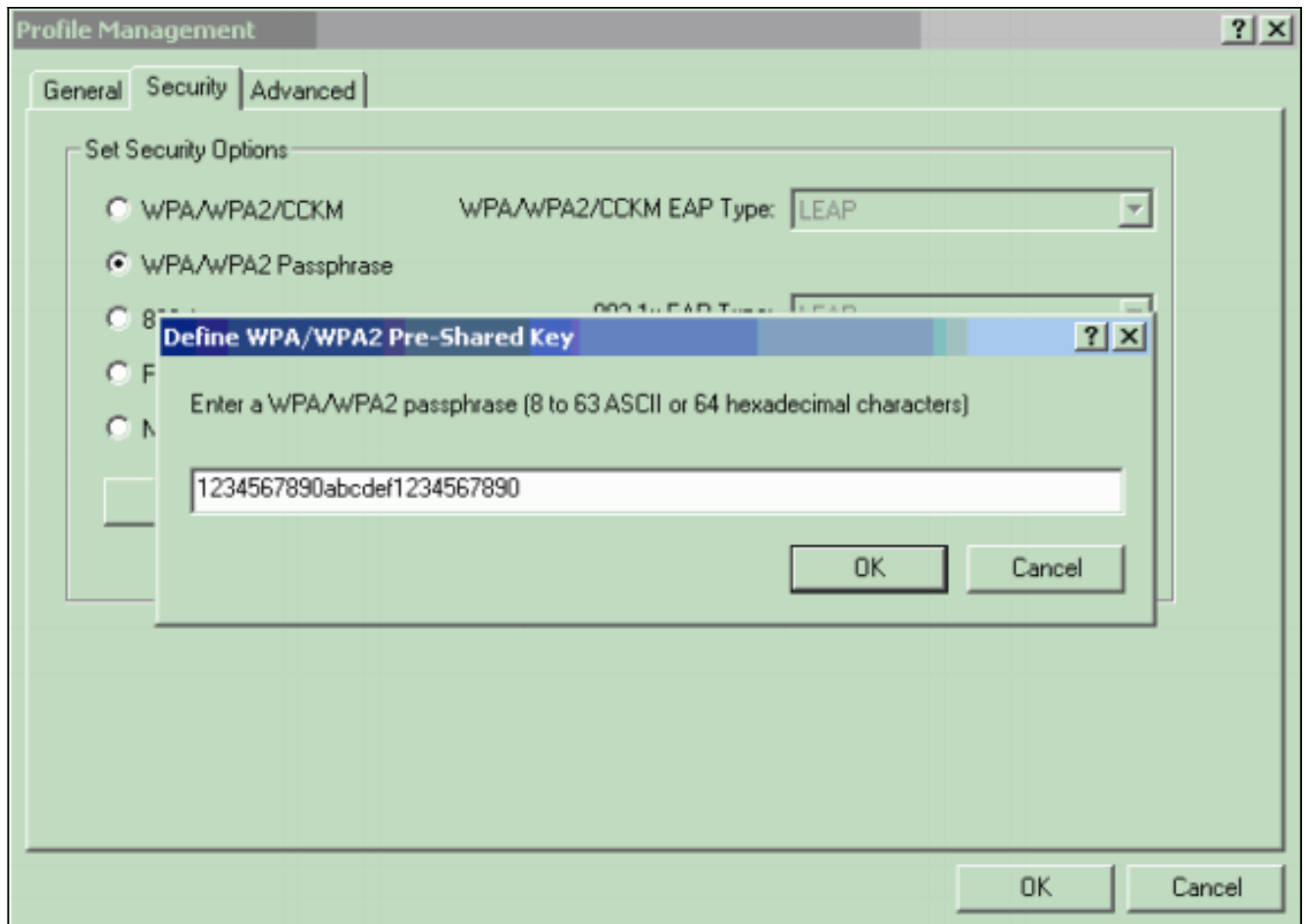




2. Fare clic sulla scheda **Protezione** e selezionare **Passphrase WPA/WPA2**. Questa azione consente di abilitare WPA PSK o WPA 2 PSK, a seconda di quale sia la modalità configurata nell'access point.



3. Fare clic su **Configura**. Viene visualizzata la finestra Definisci chiave già condivisa WPA/WPA2.
4. Ottenere la passphrase WPA/WPA2 dall'amministratore di sistema e immetterla nel campo passphrase WPA/WPA2. Ottenere la passphrase per l'access point in una rete di infrastruttura o la passphrase per altri client in una rete ad hoc. Per immettere una passphrase, attenersi alle seguenti linee guida: Le passphrase WPA/WPA2 devono contenere da 8 a 63 caratteri di testo ASCII o 64 caratteri esadecimali. La passphrase WPA/WPA2 della scheda client deve corrispondere alla passphrase dell'access point con cui si intende comunicare.



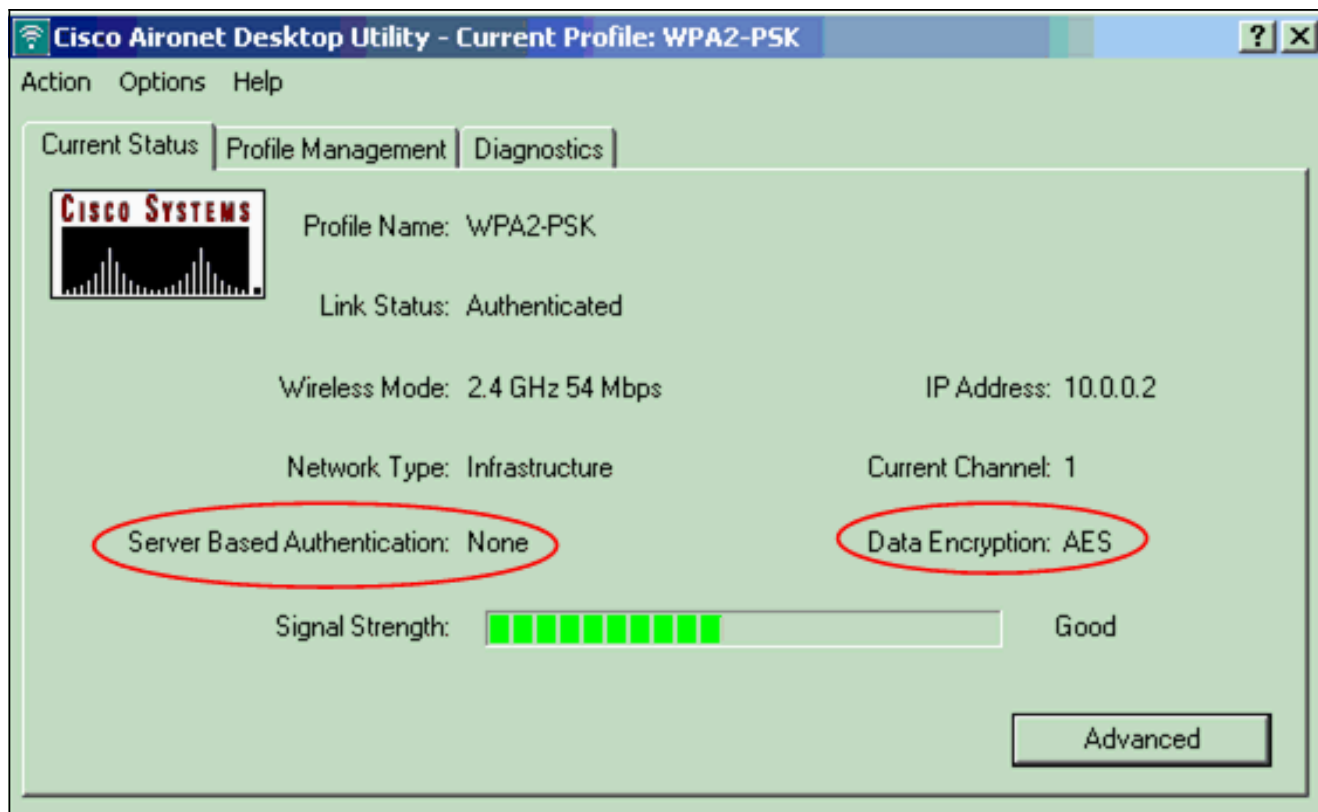
5. Per salvare la passphrase e tornare alla finestra Gestione profili, fare clic su **OK**.

## Verifica

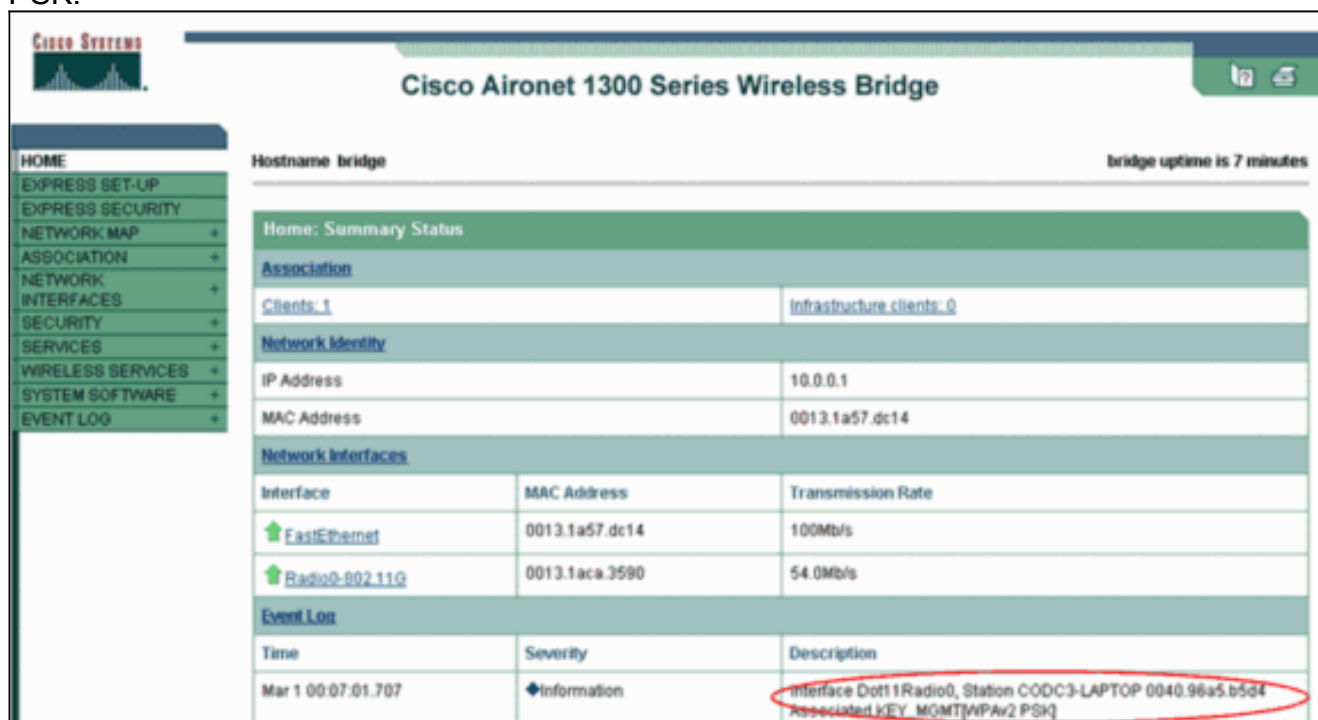
Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Dopo l'attivazione del profilo WPA 2 PSK, l'access point autentica il client in base alla passphrase WPA 2 (PSK) e fornisce l'accesso alla WLAN.

1. Per verificare la riuscita dell'autenticazione, controllare lo stato corrente dell'ADU. In questa finestra viene illustrato un esempio. La finestra mostra che la crittografia utilizzata è AES e che non viene eseguita alcuna autenticazione basata su server:



- Controllare il registro eventi AP/bridge per verificare che il client sia stato autenticato correttamente con la modalità di autenticazione WPA 2 PSK.



## [Risoluzione dei problemi](#)

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

## [Informazioni correlate](#)

- [Configurazione di suite di cifratura e WEP](#)
- [Configurazione dei tipi di autenticazione](#)
- [Panoramica della configurazione WPA](#)
- [WPA2 - Accesso protetto Wi-Fi 2](#)
- [Che cos'è il funzionamento in modalità mista WPA e come configurarlo nel punto di accesso](#)
- [Pagina di supporto wireless](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)