Wi-Fi 保護存取 2 (WPA 2) 的組態範例

目錄

簡介

本文件說明在無線 LAN (WLAN) 中，使用 Wi-Fi 保護存取 2 (WPA 2) 的優點。 本文件提供如何在 WLAN 上實作 WPA 2 的兩個組態範例。第一個範例說明如何在企業模式中設定 WPA 2，第二個範例則是在個人模式中設定 WPA 2。

註：WPA與可擴展身份驗證協定(EAP)配合使用。

必要條件

需求

嘗試此組態之前，請確認您已瞭解以下主題的基本知識：

- WPA
- WLAN安全解決方案**註：有關**Cisco WLAN安全解決方案的資訊，請參閱Cisco Aironet無線

LAN安全概述。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 執行Cisco IOS®軟體版本12.3(2)JA的Cisco Aironet 1310G存取點(AP)/橋接器
- 運行韌體2.5的Aironet 802.11a/b/g CB21AG客戶端介面卡
- 執行韌體2.5的Aironet案頭公用程式(ADU)

注意：Aironet CB21AG和PI21AG客戶端介面卡軟體與其他Aironet客戶端介面卡軟體不相容。必須將ADU與CB21AG和PI21AG卡配合使用，並且必須使用Aironet客戶端實用程式(ACU)所有其他Aironet客戶端介面卡。有關如何安裝CB21AG卡和ADU的詳細資訊，請參閱安裝客戶端介面卡。

註：本文檔使用整合天線的AP/網橋。如果使用需要外部天線的AP/網橋，請確保天線已連線到AP/網橋。否則，AP/網橋無法連線到無線網路。某些型號的AP/網橋配備整合天線，而其他型號則需要外部天線才能正常工作。有關內建或外接天線的AP/網橋型號的資訊，請參閱相應裝置的訂購指南/產品指南。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

背景資訊

WPA是Wi-Fi聯盟提供的基於標準的安全解決方案，可解決本地WLAN中的漏洞。WPA為WLAN系統提供增強的資料保護和訪問控制。WPA解決了原始IEEE 802.11安全實施中的所有已知有線等效保密(WEP)漏洞，為企業和小型辦公室、家庭辦公室(SOHO)環境中的WLAN帶來了即時安全解決方案。

WPA 2是下一代Wi-Fi安全性。WPA 2是已批准的IEEE 802.11i標準的Wi-Fi聯盟互操作性實施。WPA 2使用計數器模式及密碼塊鏈結消息驗證代碼協定(CCMP)，實施美國國家標準與技術研究所(NIST)推薦的高級加密標準(AES)加密演算法。AES計數器模式是一種分組密碼，使用128位加密金鑰一次加密128位資料塊。CCMP演算法產生消息完整性代碼(MIC)，為無線幀提供資料來源驗證和資料完整性。

注意:CCMP也稱為CBC-MAC。

WPA 2比WPA提供更高級別的安全性，因為AES提供的加密比臨時金鑰完整性協定(TKIP)更強。TKIP是WPA使用的加密演算法。WPA 2會在每個關聯上建立新的會話金鑰。用於網路中每個客戶端的加密金鑰是唯一的並且特定於該客戶端。最後，通過無線方式傳送的每個資料包都使用唯一金鑰進行加密。使用新的唯一加密金鑰增強了安全性，因為沒有金鑰重複使用。WPA仍被視為安全，並且TKIP尚未被破壞。但是，思科建議客戶儘快過渡到WPA 2。

WPA和WPA 2都支援兩種操作模式：

- 企業模式
- 個人模式

本文討論這兩種模式在WPA 2中的實施。

Cisco Aironet裝置的WPA 2支援

以下裝置支援WPA 2:

- Aironet 1130AG AP系列和1230AG AP系列
- Aironet 1100 AP系列
- Aironet 1200 AP系列
- Aironet 1300 AP系列

註：為這些AP配備802.11g無線電並使用Cisco IOS軟體版本12.3(2)JA或更高版本。

以下裝置也支援WPA 2和AES:

- 部件號為AIR-RM21A和AIR-RM22A的Aironet 1200系列無線電模組**註：**部件號為AIR-RM20A的Aironet 1200無線電模組不支援WPA 2。
- 採用韌體版本2.5的Aironet 802.11a/b/g使用者端配接器

注意：Cisco Aironet 350系列產品不支援WPA 2，因為其無線電不支援AES。

註：Cisco Aironet 1400系列無線網橋不支援WPA 2或AES。

在企業模式下配置

術語**企業模式**是指經過測試，可在預共用金鑰(PSK)和IEEE 802.1x身份驗證操作模式下互操作的產品。802.1x被認為比任何傳統身份驗證框架更安全，因為它支援各種身份驗證機制和更強大的加密演算法。企業模式中的WPA 2分兩個階段執行身份驗證。開放式身份驗證的配置在第一階段進行。第二階段是使用其中一個EAP方法的802.1x身份驗證。AES提供加密機制。

在企業模式下，客戶端和身份驗證伺服器使用EAP身份驗證方法相互進行身份驗證，客戶端和伺服器生成成對主金鑰(PMK)。 通過WPA 2，伺服器動態生成PMK並將PMK傳遞到AP。

本節討論在企業運營模式下實施WPA 2所需的配置。

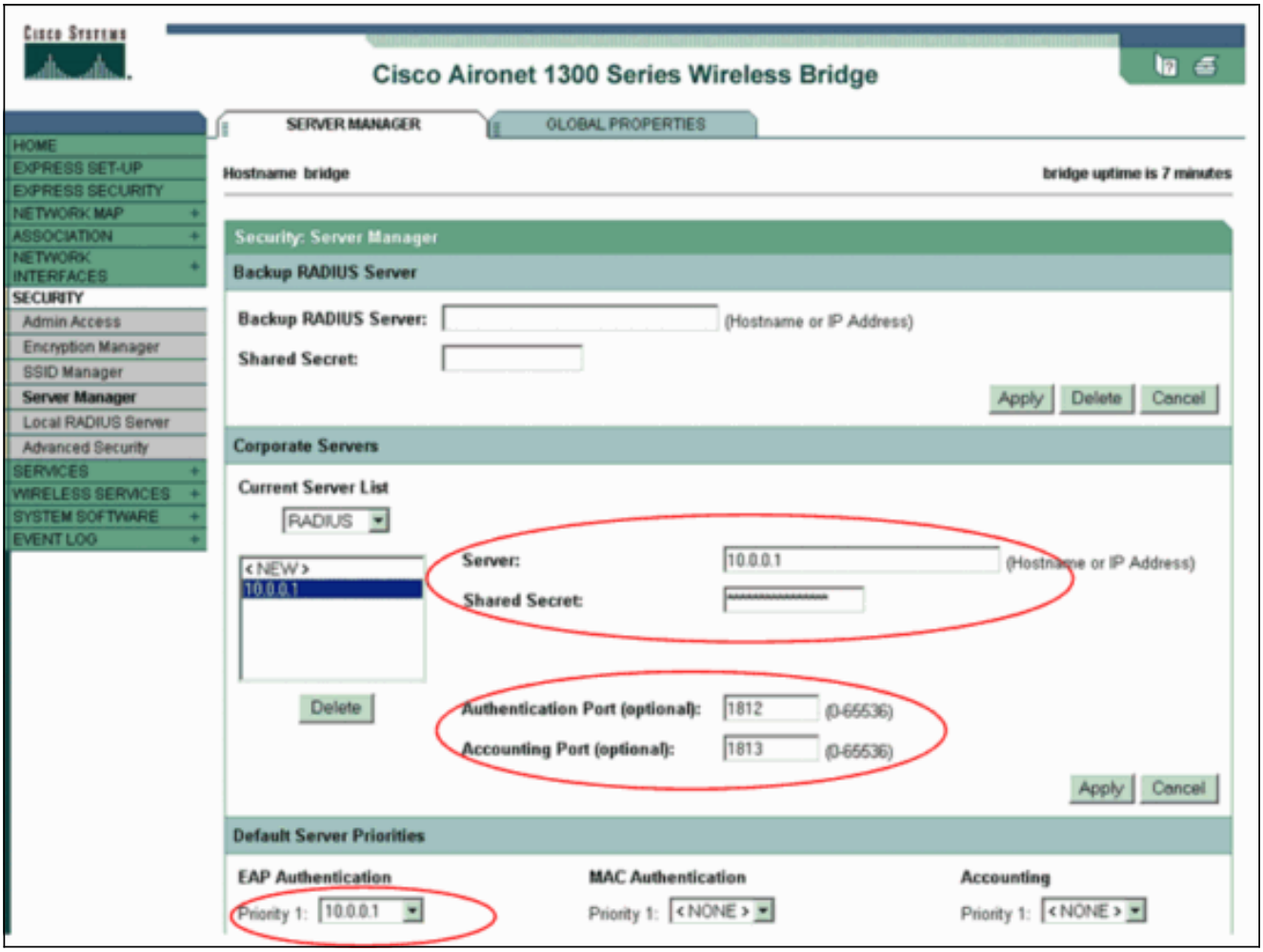
網路設定

在此設定中，運行Cisco輕型可擴展身份驗證協定(LEAP)的Aironet 1310G AP/網橋使用與WPA 2相容的客戶端介面卡對使用者進行身份驗證。使用WPA 2進行金鑰管理，其中配置了AES-CCMP加密。AP配置為運行LEAP身份驗證的本地RADIUS伺服器。您必須配置客戶端介面卡和AP才能實施此設定。配置AP和配置客戶端介面卡部分顯示AP和客戶端介面卡上的配置。

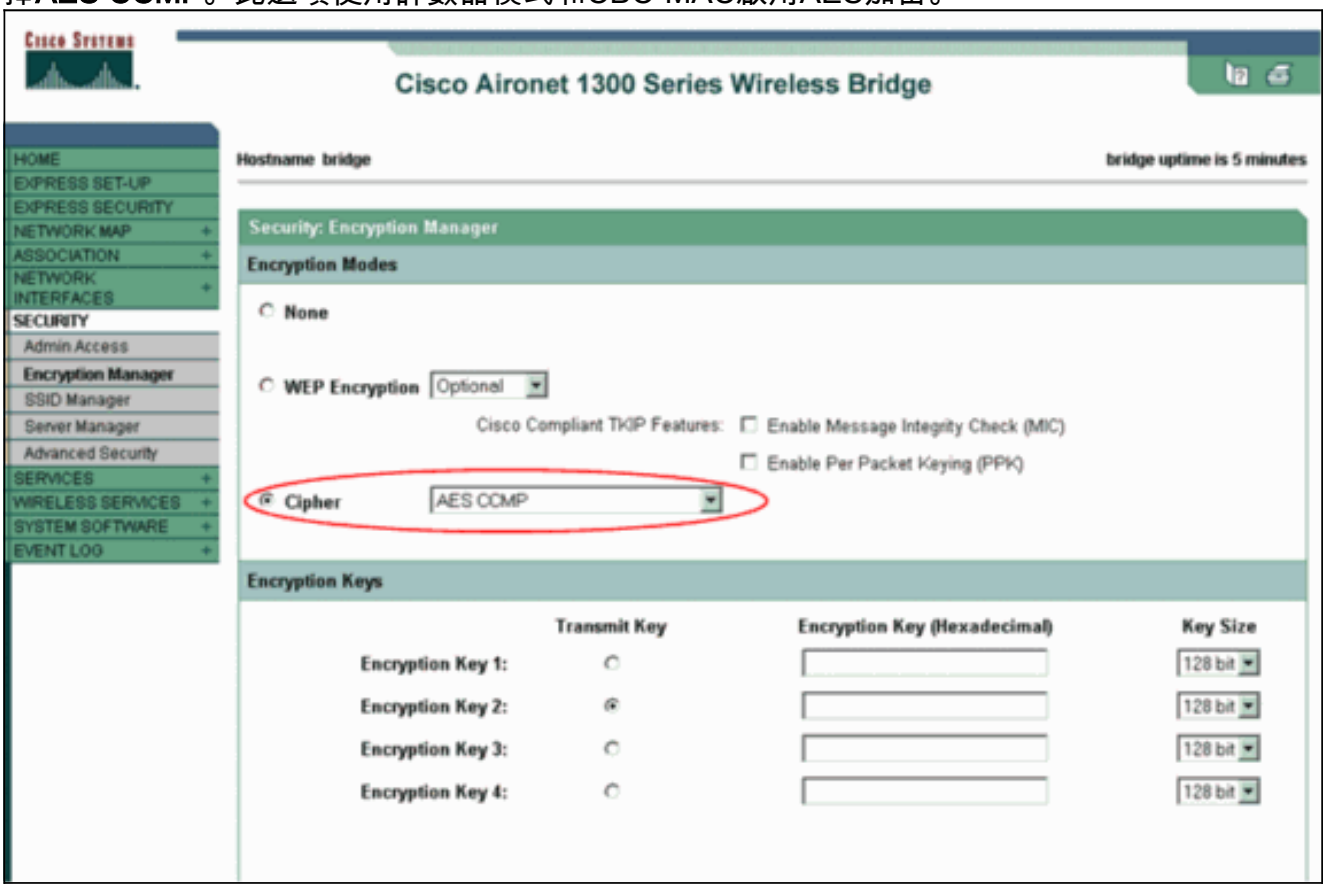
配置AP

完成以下步驟，使用GUI配置AP:

1. 將AP配置為運行LEAP身份驗證的本地RADIUS伺服器。在左側選單中選擇**Security > Server Manager**，並定義RADIUS伺服器的IP地址、埠和共用金鑰。由於此配置將AP配置為本地RADIUS伺服器，因此使用AP的IP地址。使用埠1812和1813進行本地RADIUS伺服器操作。在Default Server Priorities區域中，將預設EAP身份驗證優先順序定義為10.0.0.1。**注意**：10.0.0.1是本地RADIUS伺服器。



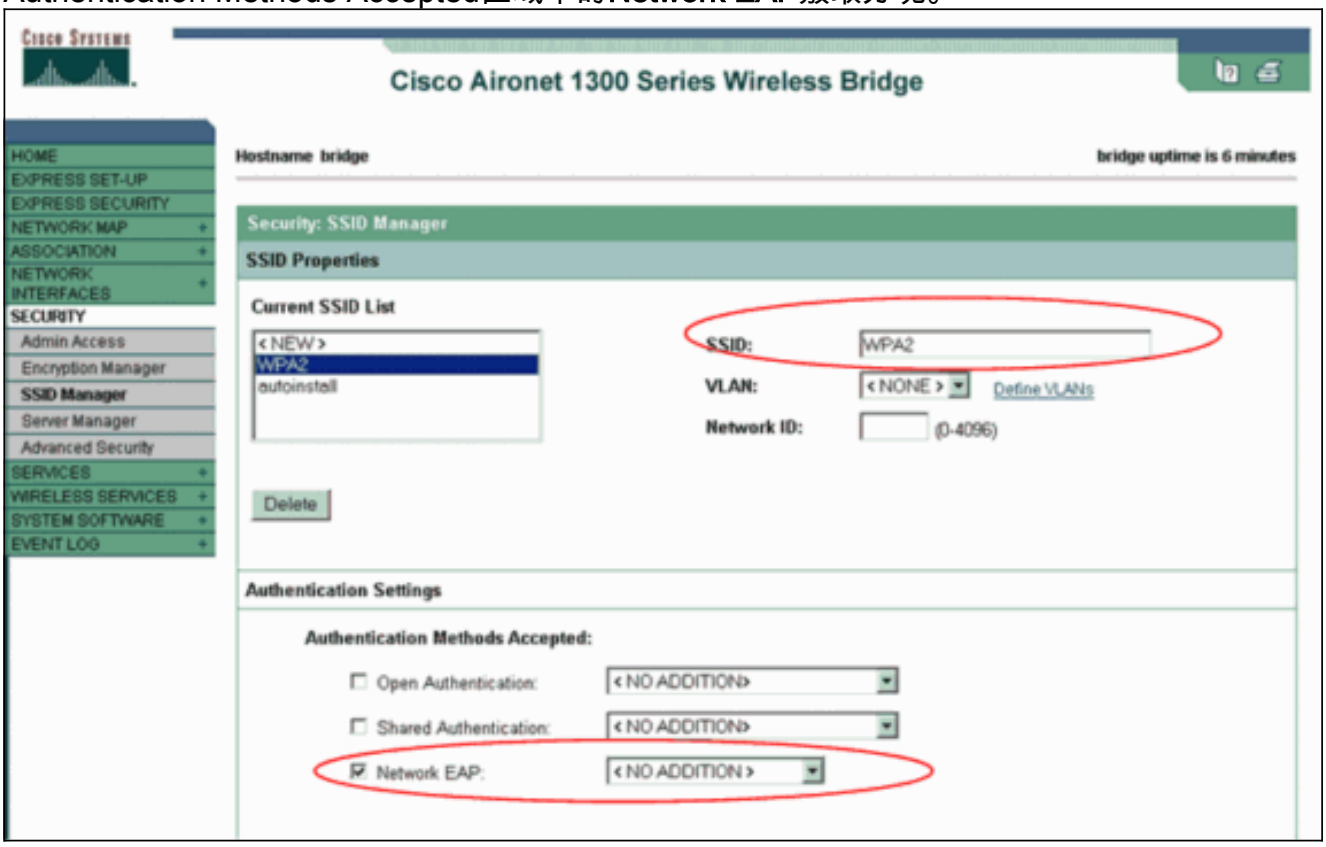
2. 從左側選單中選擇**Security > Encryption Manager**，並完成以下步驟：在「密碼」功能表中選擇**AES CCMP**。此選項使用計數器模式和CBC-MAC啟用AES加密。



按一下「**Apply**」。

3. 選擇**Security > SSID Manager**，並建立一個新的服務集識別符號(SSID)以用於WPA 2。選中

Authentication Methods Accepted區域中的**Network EAP**覈取方塊。

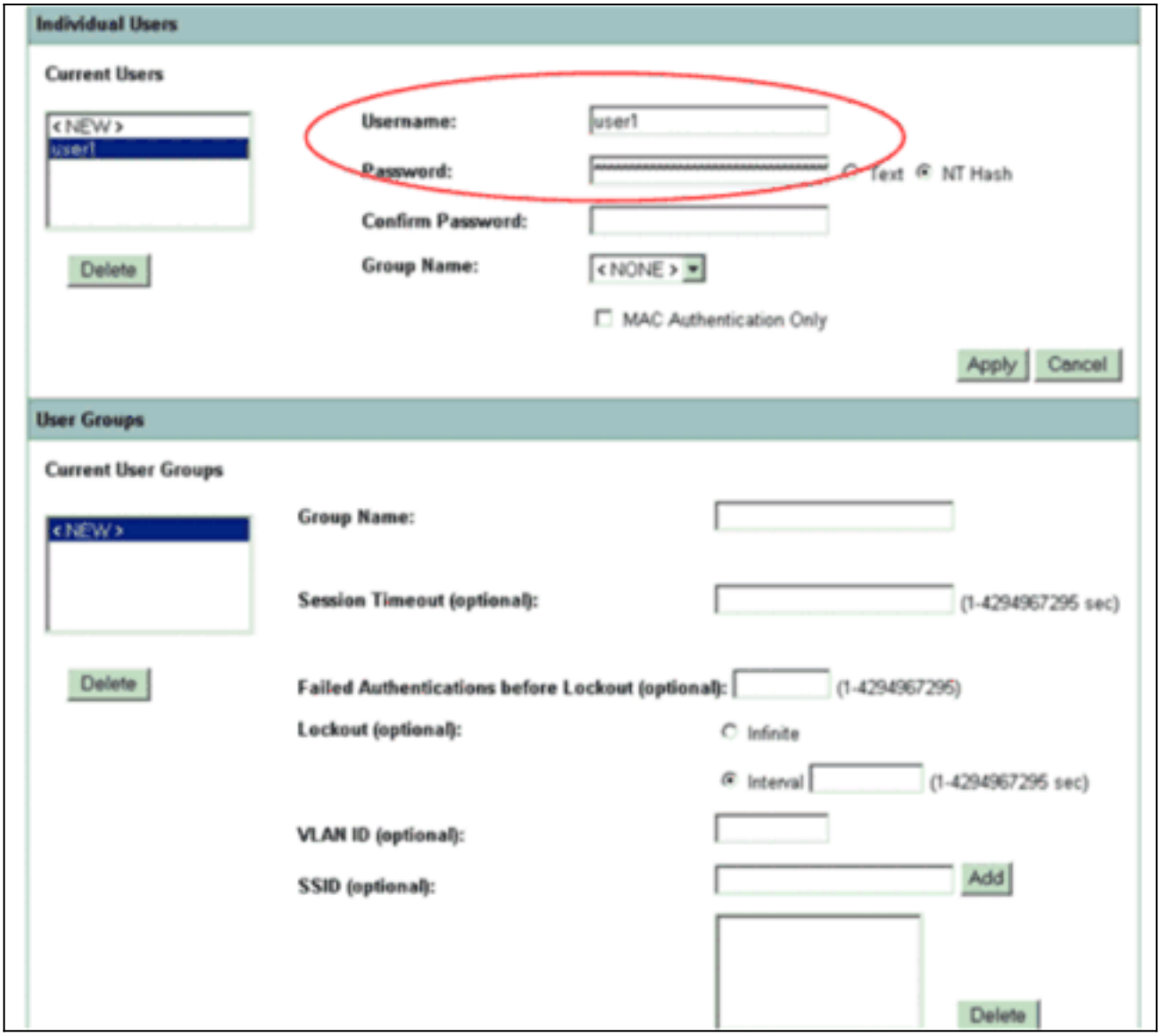


注意：在無線電介面上配置身份驗證型別時，請使用以下准則：Cisco clients — 使用網路EAP。第三方客戶端（包括符合Cisco Compatible Extensions [CCX]標準的產品）— 使用Open Authentication with EAP。思科和第三方客戶端的組合 — 選擇網路EAP和使用EAP的開放式身份驗證。向下滾動Security SSID Manager視窗至Authenticated Key Management區域並完成以下步驟：在「金鑰管理」選單中，選擇**必填**。選中右側的**WPA**覈取方塊。按一下「**Apply**」。**注意**：VLAN的定義是可選的。如果定義VLAN，則與此SSID的使用相關聯的客戶端裝置將分組到VLAN中。有關如何實施VLAN的詳細資訊，請參閱配置VLAN。

4. 選擇**Security > Local Radius Server**，然後完成以下步驟：按一下位於視窗頂部的**General Set-Up**頁籤。選中**LEAP**覈取方塊並按一下**Apply**。在Network Access Servers區域中，定義RADIUS伺服器的IP地址和共用金鑰。對於本地RADIUS伺服器，使用AP的IP地址。

按一下「Apply」。

5. 向下滾動「常規設定」視窗至「單個使用者」區域，並定義單個使用者。使用者組的定義是可選的。



此組態會定義名稱為「user1」且密碼的使用者。此外，配置還會為密碼選擇NT雜湊。完成本節中的過程後，AP準備接受來自客戶端的身份驗證請求。下一步是配置客戶端介面卡。

CLI組態

存取點

```
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
```

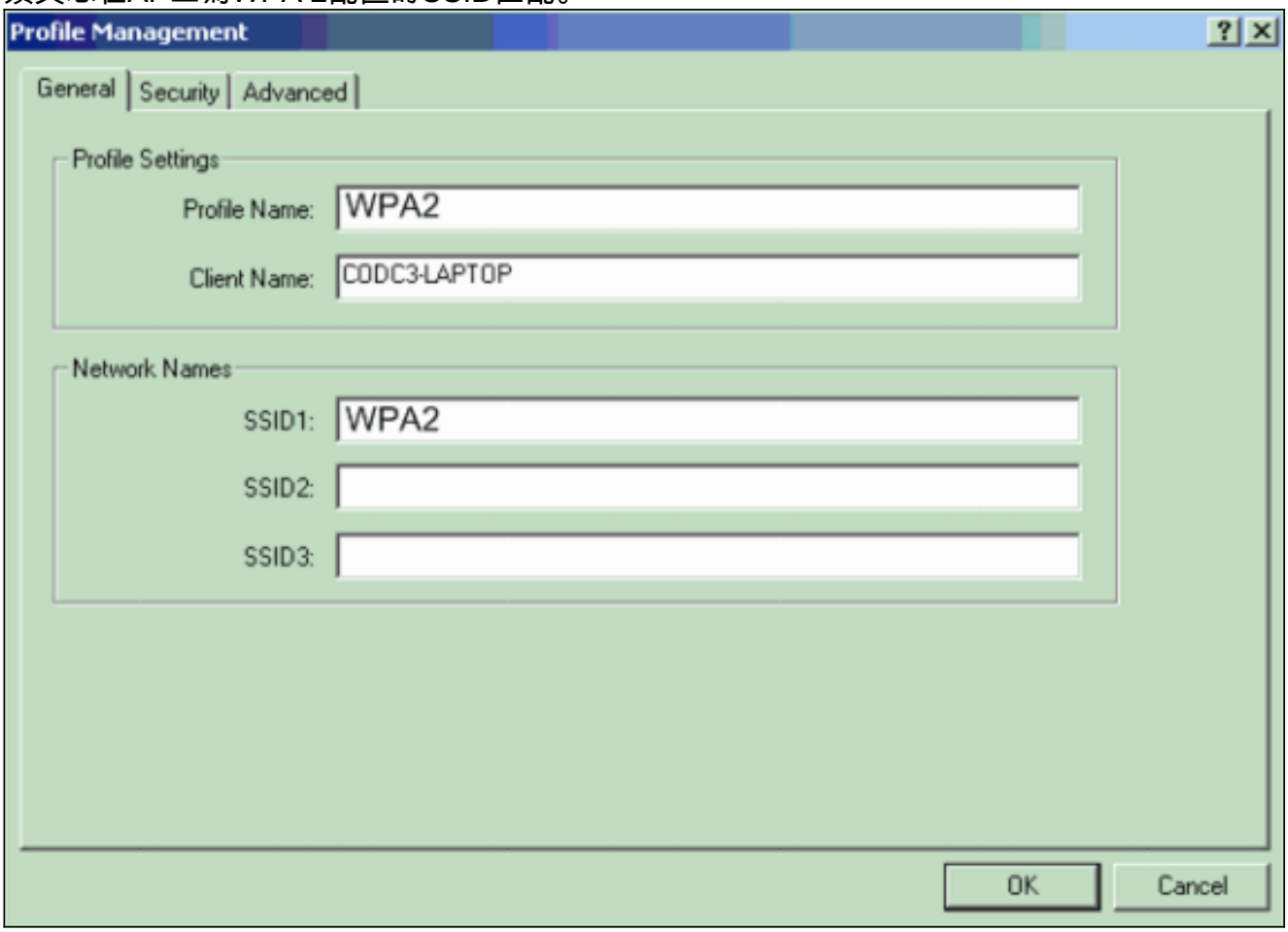
```
   12345678901234567890123456 transmit-key
!---This step is optional !--- This value seeds the
initial key for use with !--- broadcast
[255.255.255.255] traffic. If more than one VLAN is !---
used, then keys must be set for each VLAN. encryption
vlan 1 mode wep mandatory
!--- This defines the policy 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
```

配置客戶端介面卡

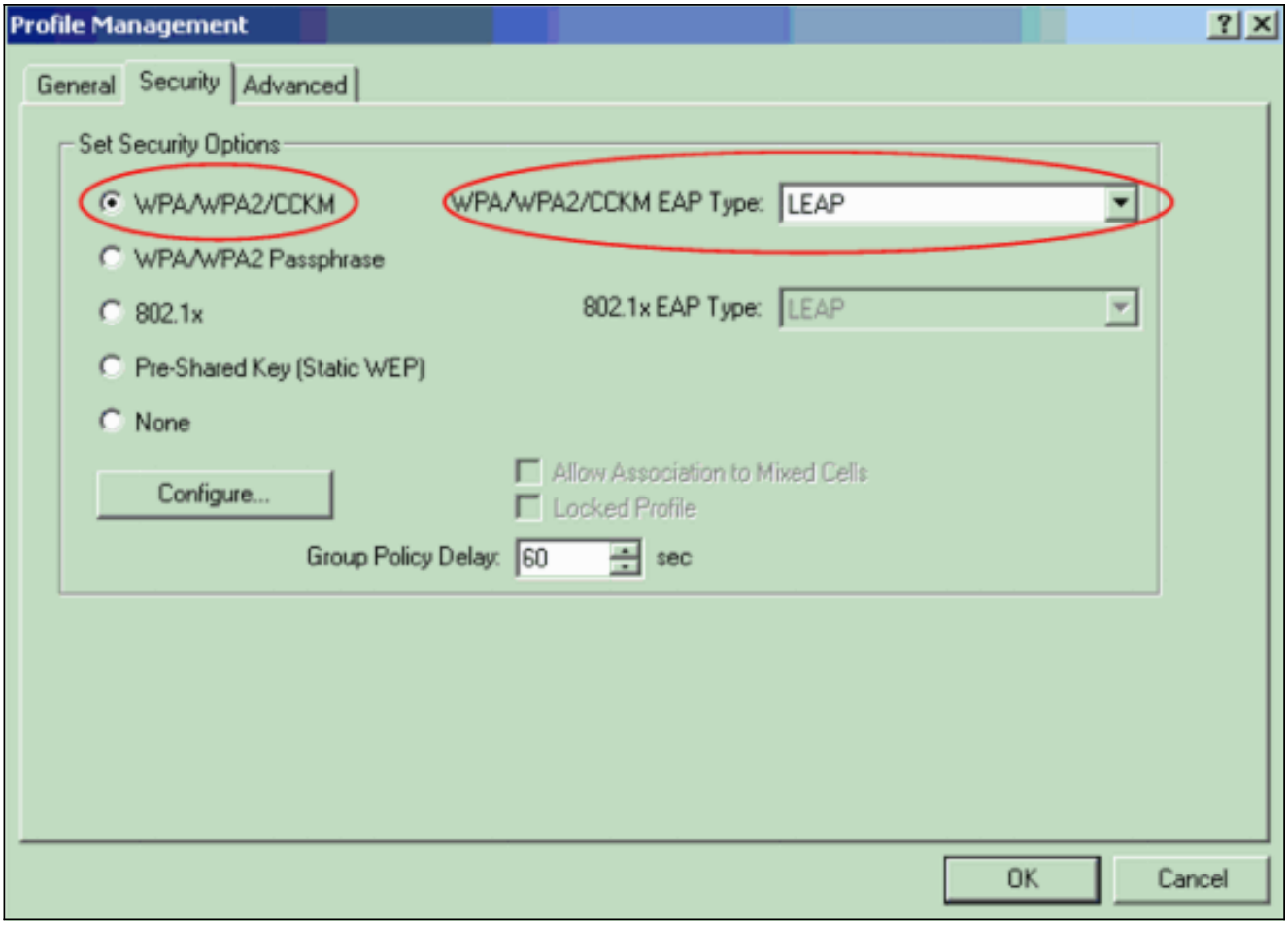
請完成以下步驟：

註：本文檔使用運行韌體2.5的Aironet 802.11a/b/g客戶端介面卡，並解釋使用ADU 2.5版配置客戶端介面卡。

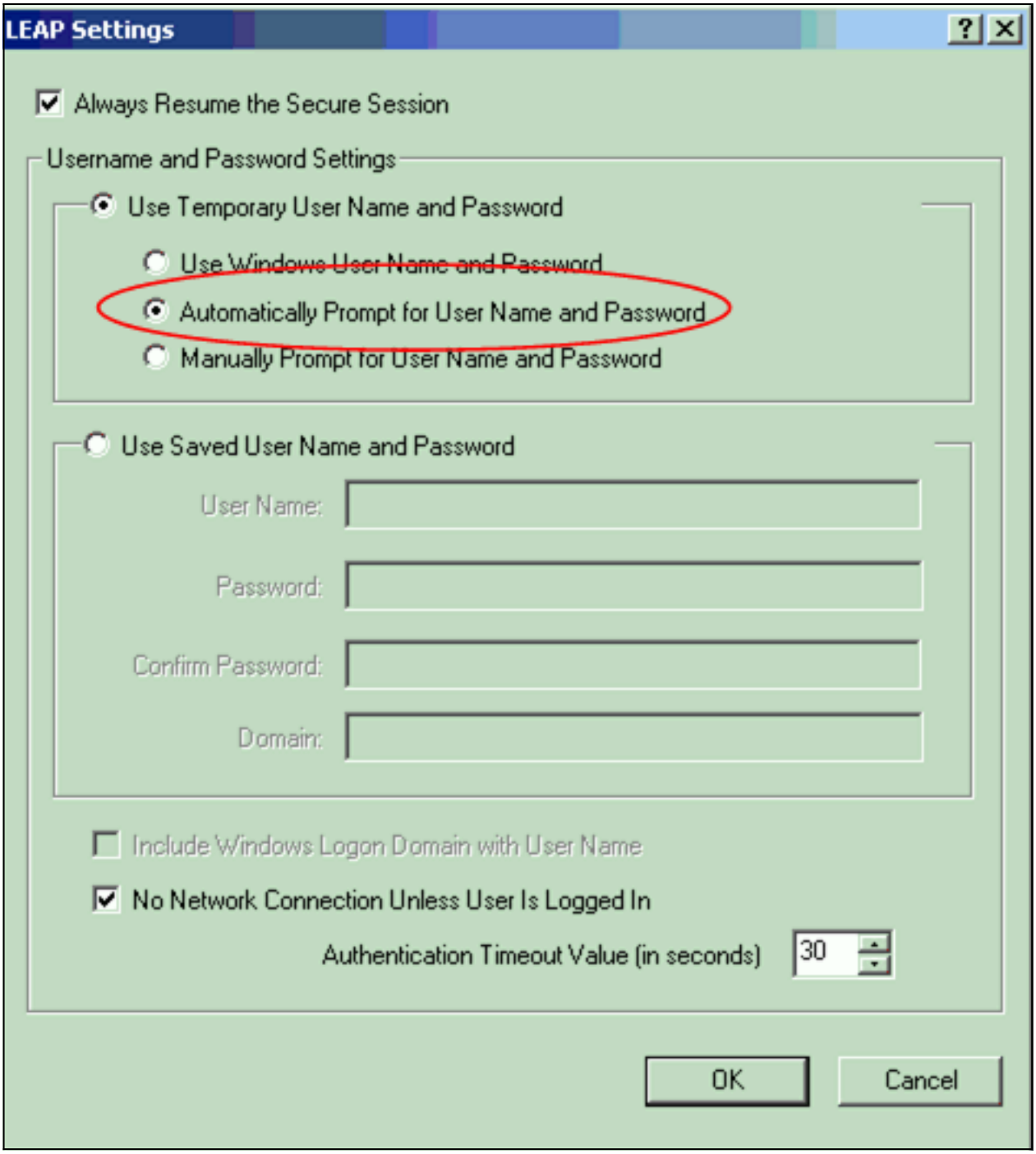
1. 在ADU的Profile Management視窗中，按一下**New**以建立新的配置檔案。將顯示一個新視窗，您可以在其中設定WPA 2企業模式操作的配置。在「General（常規）」頁籤下，輸入客戶端介面卡將使用的配置檔名稱和SSID。在此示例中，配置檔名稱和SSID為WPA2:**註：**SSID必須與您在AP上為WPA 2配置的SSID匹配。



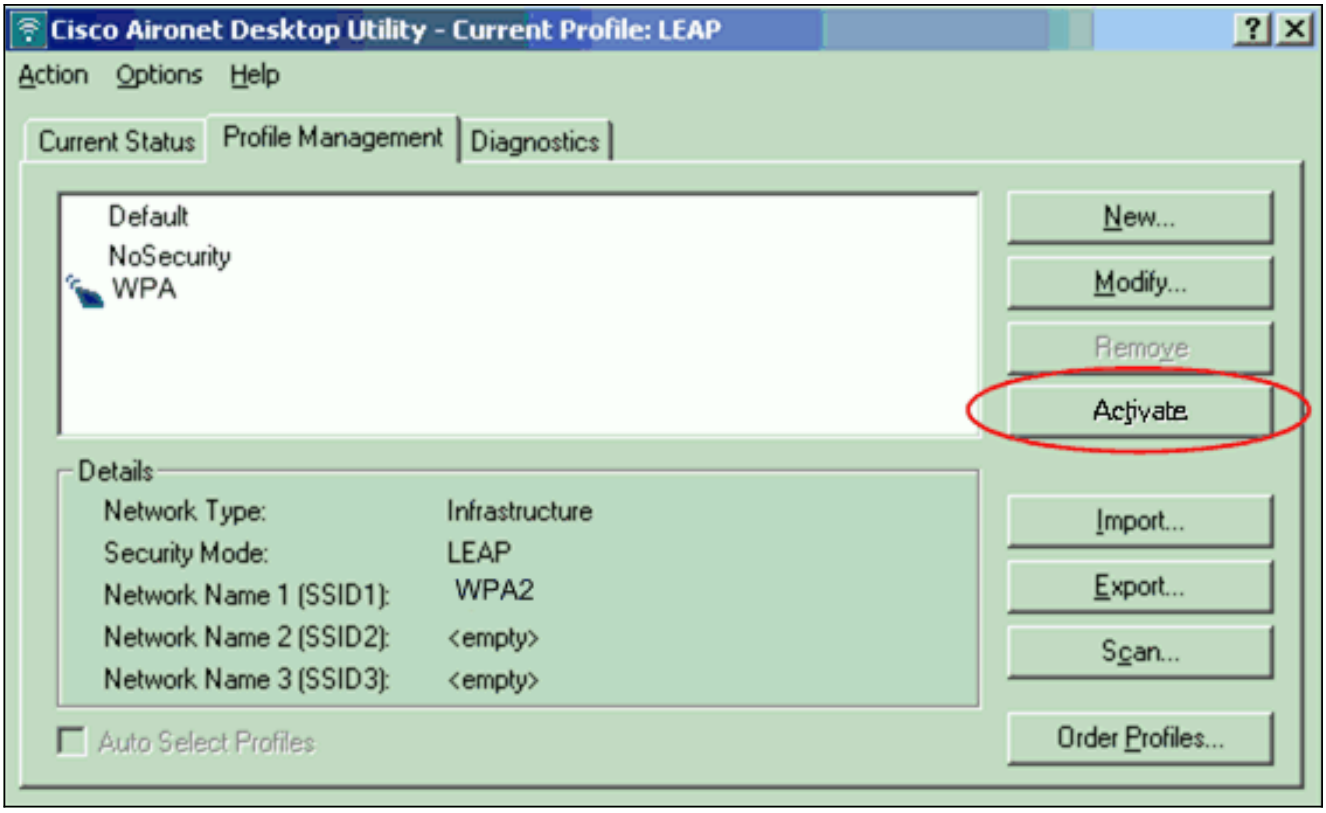
2. 按一下**Security**頁籤，按一下**WPA/WPA2/CCKM**，然後從WPA/WPA2/CCKM EAP Type選單中選擇**LEAP**。此操作將啟用WPA或WPA 2，無論您在AP上配置哪一個。



3. 按一下**Configure**以定義LEAP設定。
4. 根據要求選擇適當的使用者名稱和密碼設定，然後按一下**確定**。此配置選擇Automatically Prompt for User Name and Password選項。此選項可讓您在LEAP身份驗證發生時手動輸入使用者名稱和密碼。



5. 按一下「**OK**」以退出「Profile Management」視窗。
6. 按一下**Activate**以在客戶端介面卡上啟用此配置檔案。

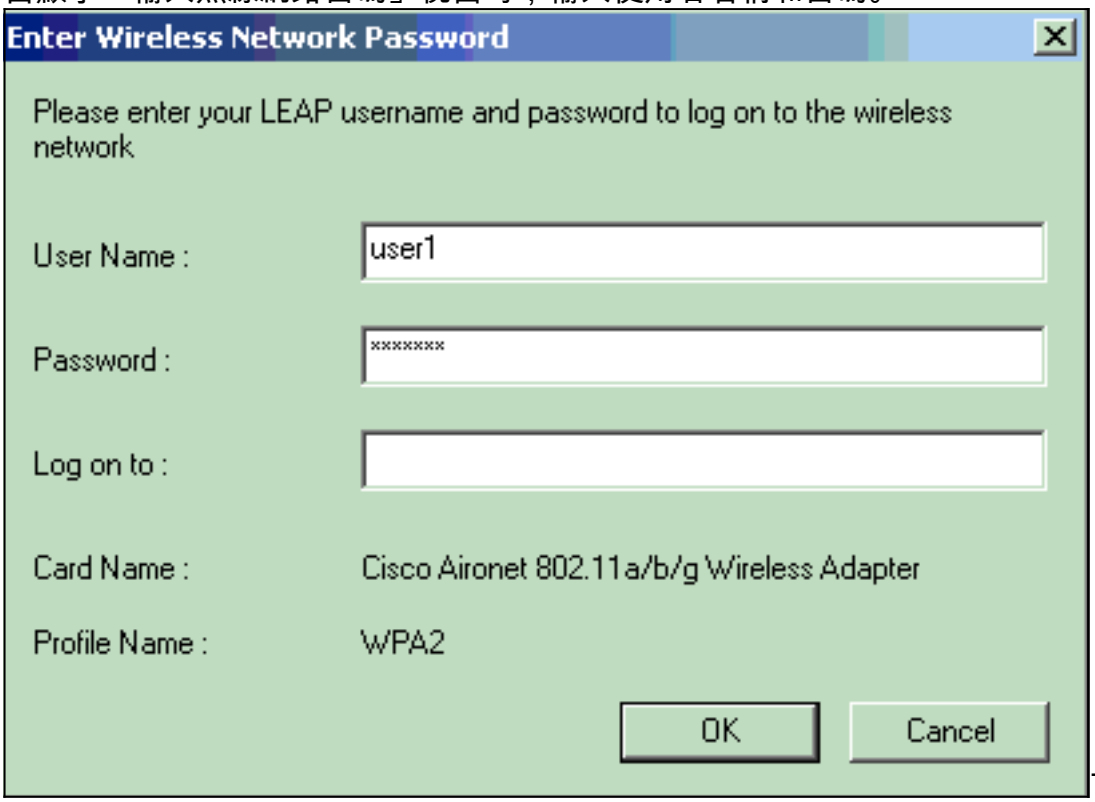


注意：如果使用Microsoft無線零配置(WZC)配置客戶端介面卡，預設情況下，WPA 2不適用於WZC。因此，為了允許啟用了WZC的客戶端運行WPA 2，您必須為Microsoft Windows XP安裝熱修復。請參閱Microsoft下載中心 — Windows XP更新(KB893357) ，瞭解安裝。安裝熱修復程式後，可以使用WZC配置WPA 2。

驗證

使用本節內容，確認您的組態是否正常運作。

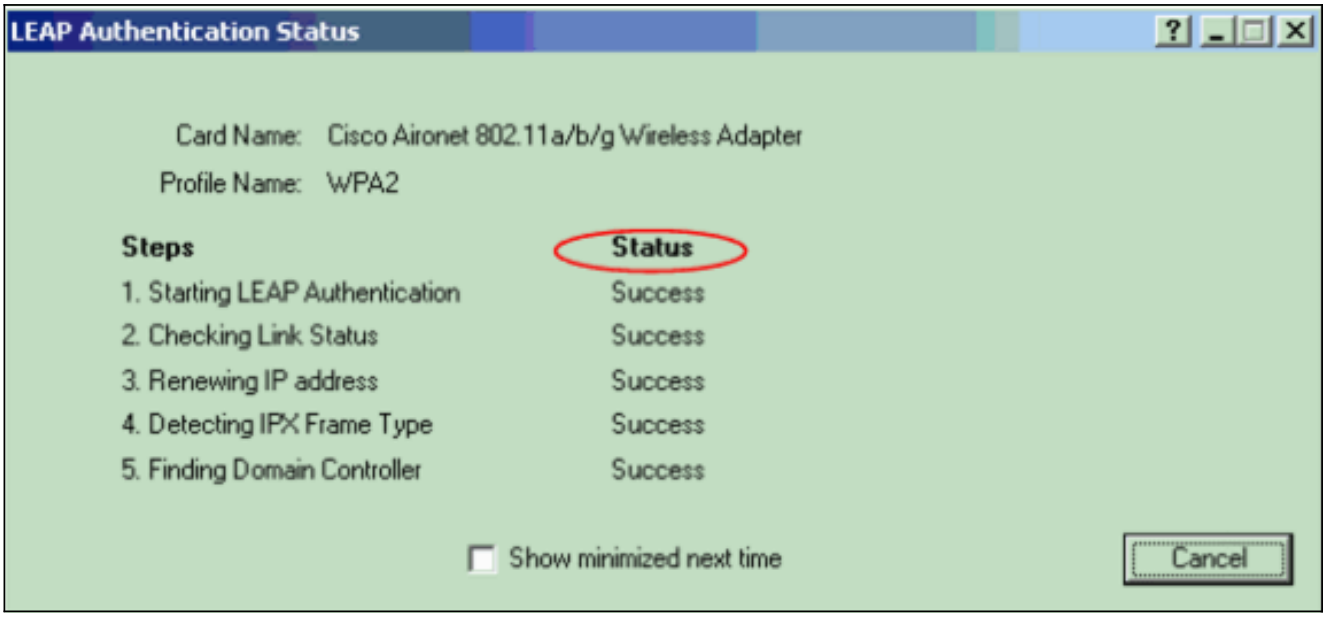
1. 當顯示「輸入無線網路密碼」視窗時，輸入使用者名稱和密碼。



下一個視窗是

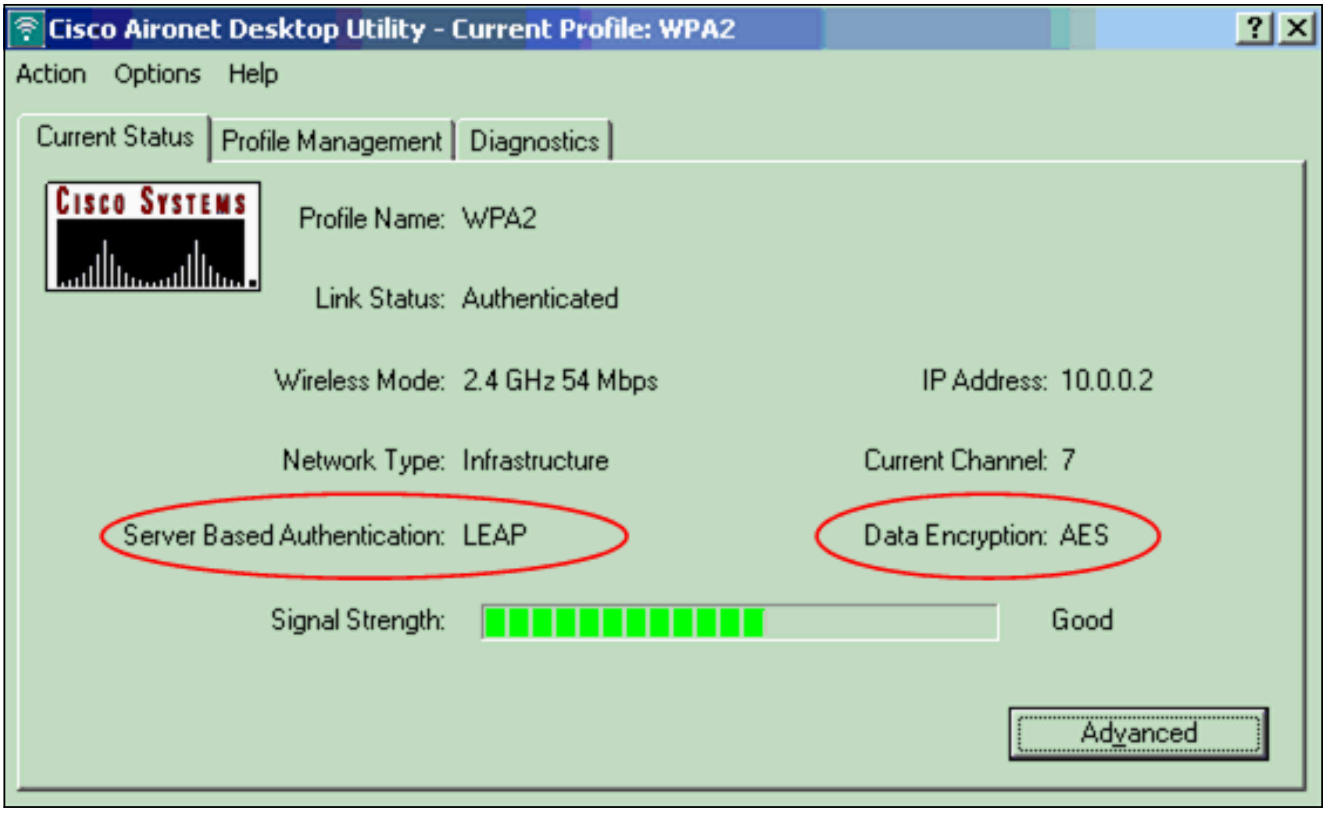
LEAP身份驗證狀態。此階段會驗證本地RADIUS伺服器的使用者憑證。

2. 檢查Status區域以檢視身份驗證的結果。



身份驗證成功後，客戶端連線到無線LAN。

3. 檢查ADU當前狀態以驗證客戶端是否使用AES加密和LEAP身份驗證。這表示您已在WLAN中實作WPA 2及LEAP驗證和AES加密。



4. 檢查AP/bridge事件日誌以驗證客戶端是否已成功通過WPA 2驗證。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

在個人模式下配置

術語**個人模式**是指經過測試，在僅PSK操作模式下可互操作的產品進行身份驗證。此模式要求在AP和客戶端上手動配置PSK。PSK通過客戶端工作站和AP上的密碼或標識代碼對使用者進行身份驗證。無需身份驗證伺服器。僅當客戶端密碼與AP密碼匹配時，客戶端才能訪問網路。密碼還提供TKIP或AES用來生成加密金鑰以對資料包進行加密的金鑰材料。個人模式針對SOHO環境，對於企業環境來說不安全。本節提供在個人操作模式下實施WPA 2所需的配置。

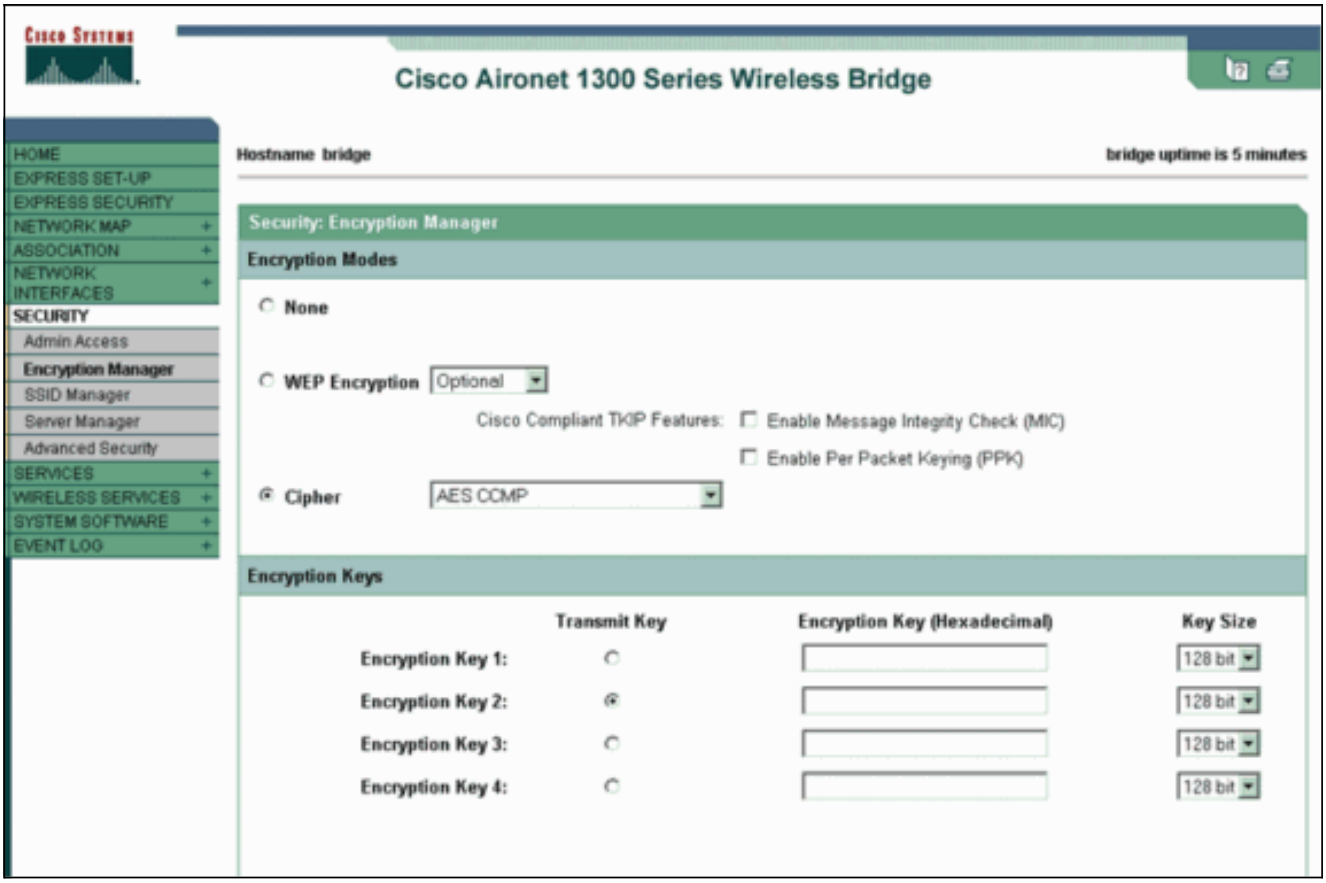
網路設定

在此設定中，具有WPA 2相容客戶端介面卡的使用者對Aironet 1310G AP/網橋進行身份驗證。使用WPA 2 PSK並配置AES-CCMP加密進行金鑰管理。配置AP和配置客戶端介面卡部分顯示AP和客戶端介面卡上的配置。

配置AP

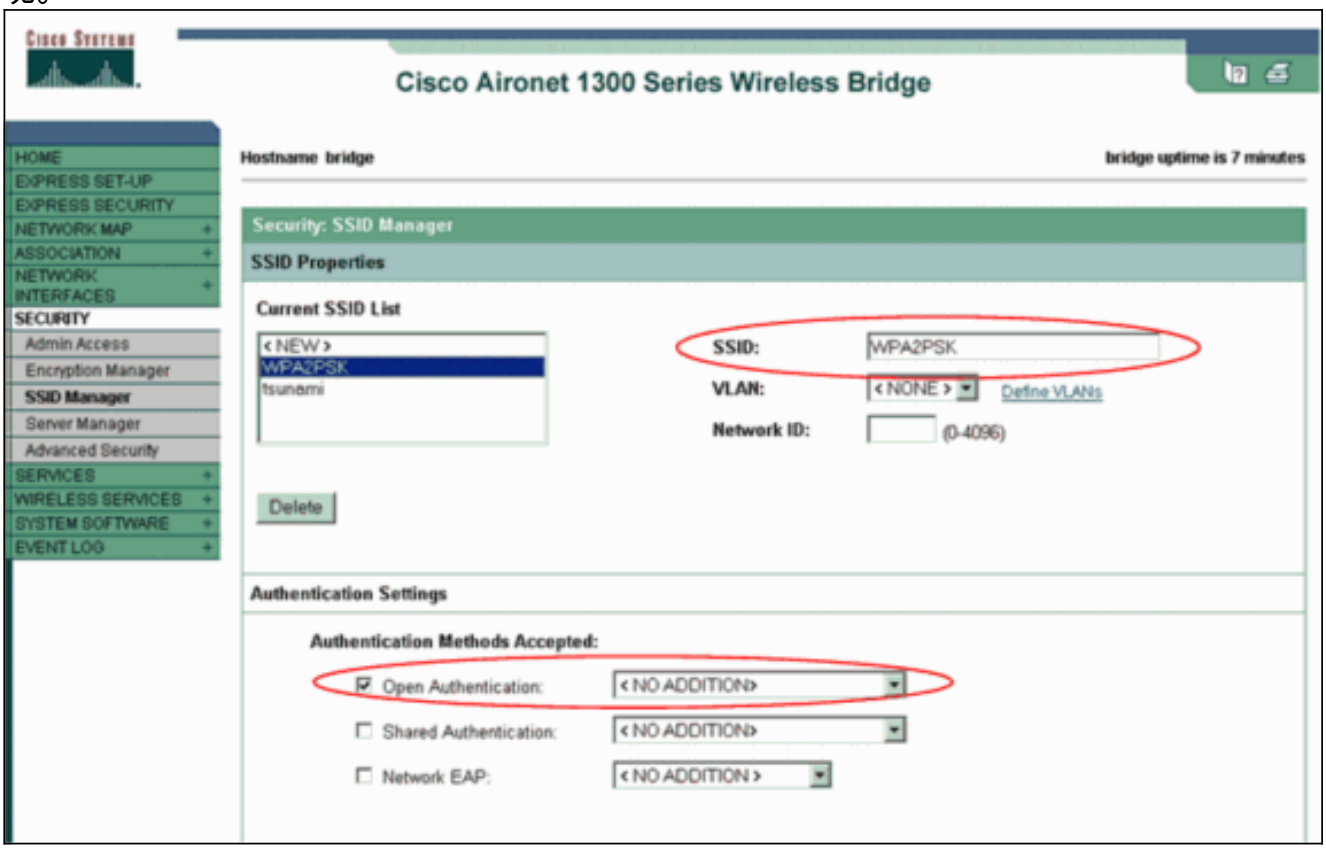
請完成以下步驟：

1. 在左側選單中選擇**Security > Encryption Manager**，並完成以下步驟：在「密碼」功能表中選擇**AES CCMP**。此選項使用計數器模式和CCMP啟用AES加密。

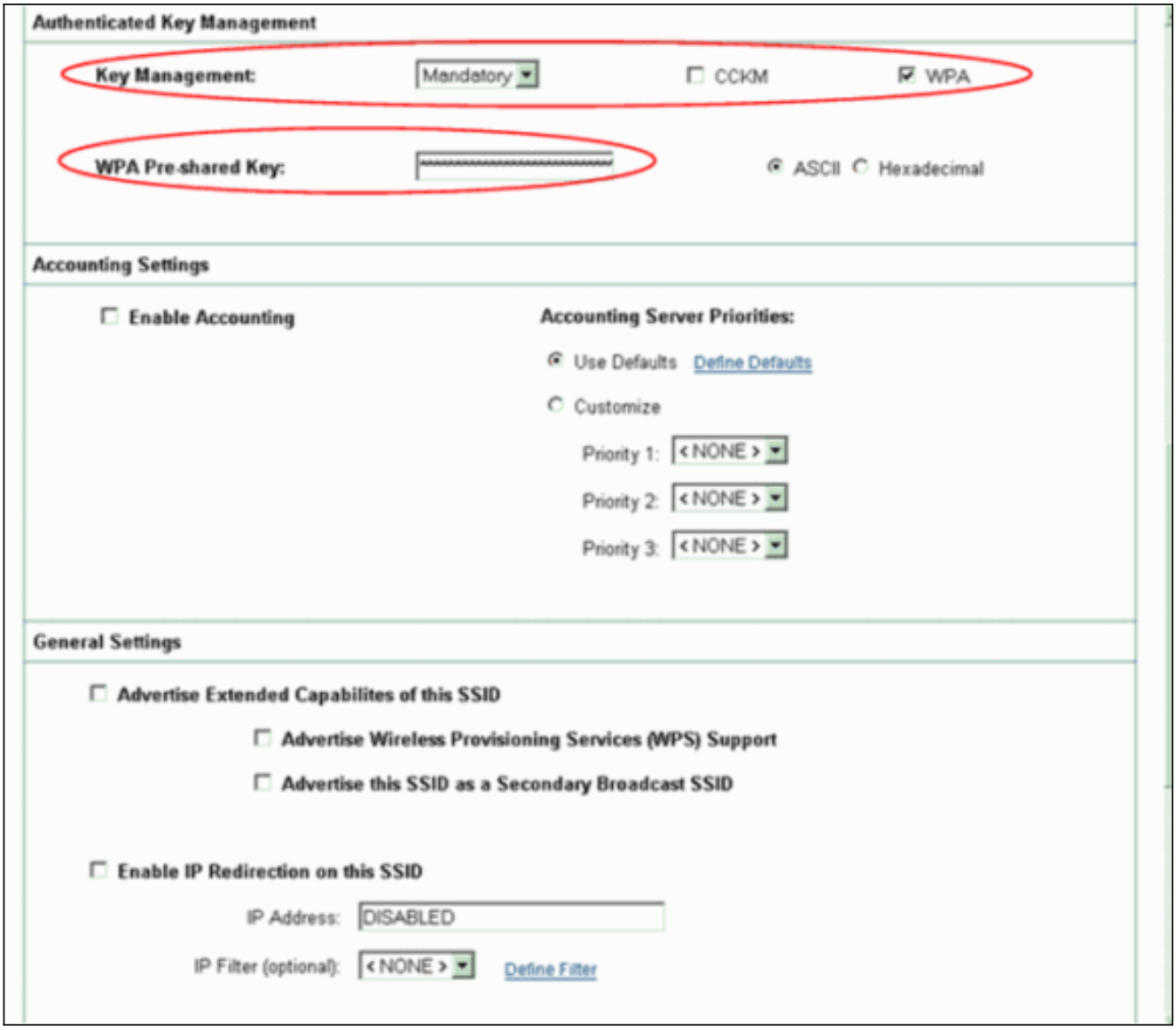


按一下「Apply」。

2. 選擇Security > SSID Manager並建立用於WPA 2的新SSID。選中Open Authentication覈取方塊。



向下滾動Security:SSID Manager視窗進入Authenticated Key Management區域並完成以下步驟：在「金鑰管理」選單中，選擇**必填**。選中右側的**WPA**覈取方塊。



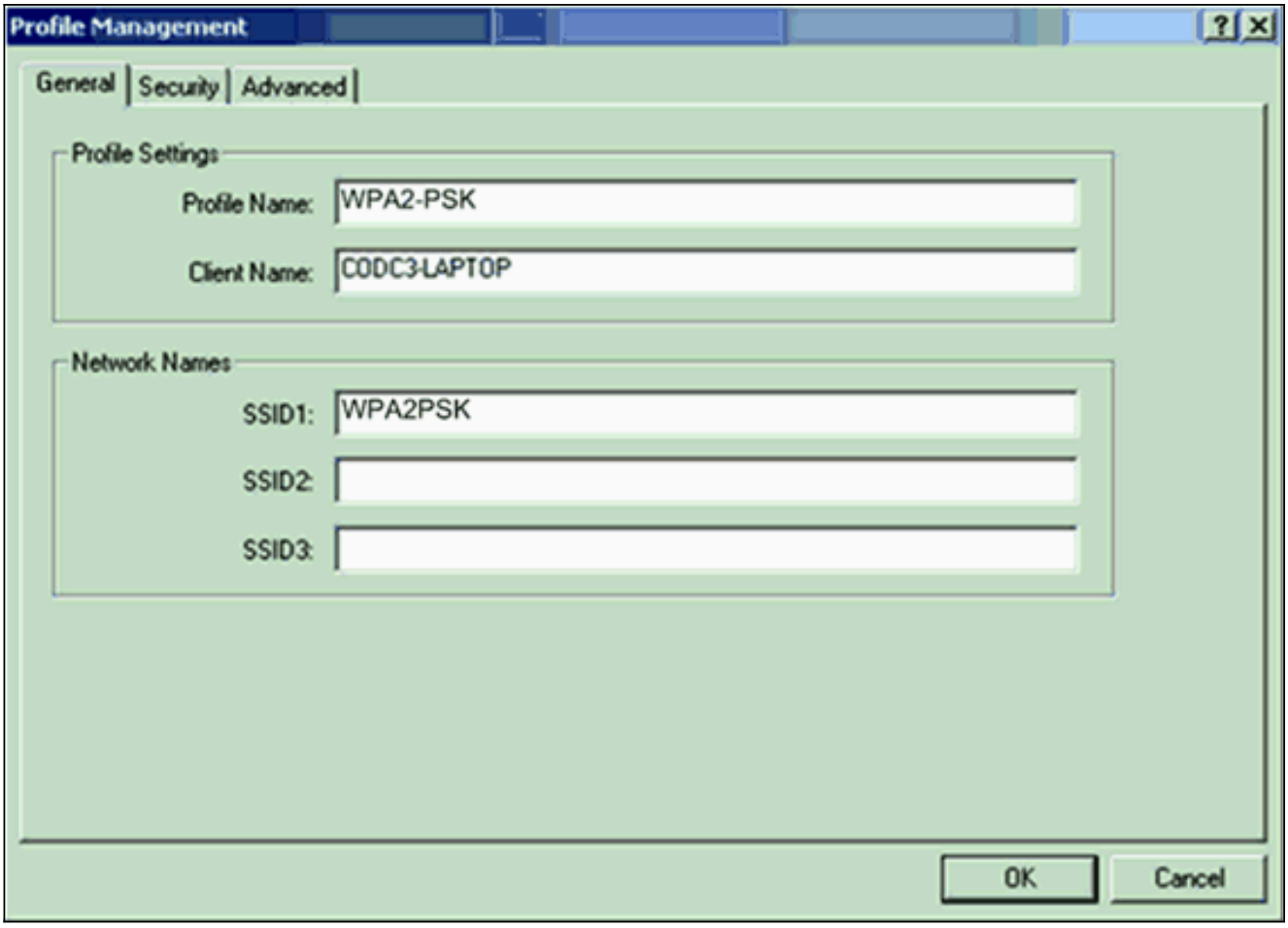
輸入WPA PSK共用金鑰或WPA PSK口令金鑰。此金鑰必須與您在客戶端介面卡上配置的WPA PSK金鑰匹配。按一下「**Apply**」。

AP現在可以從無線客戶端接收身份驗證請求。

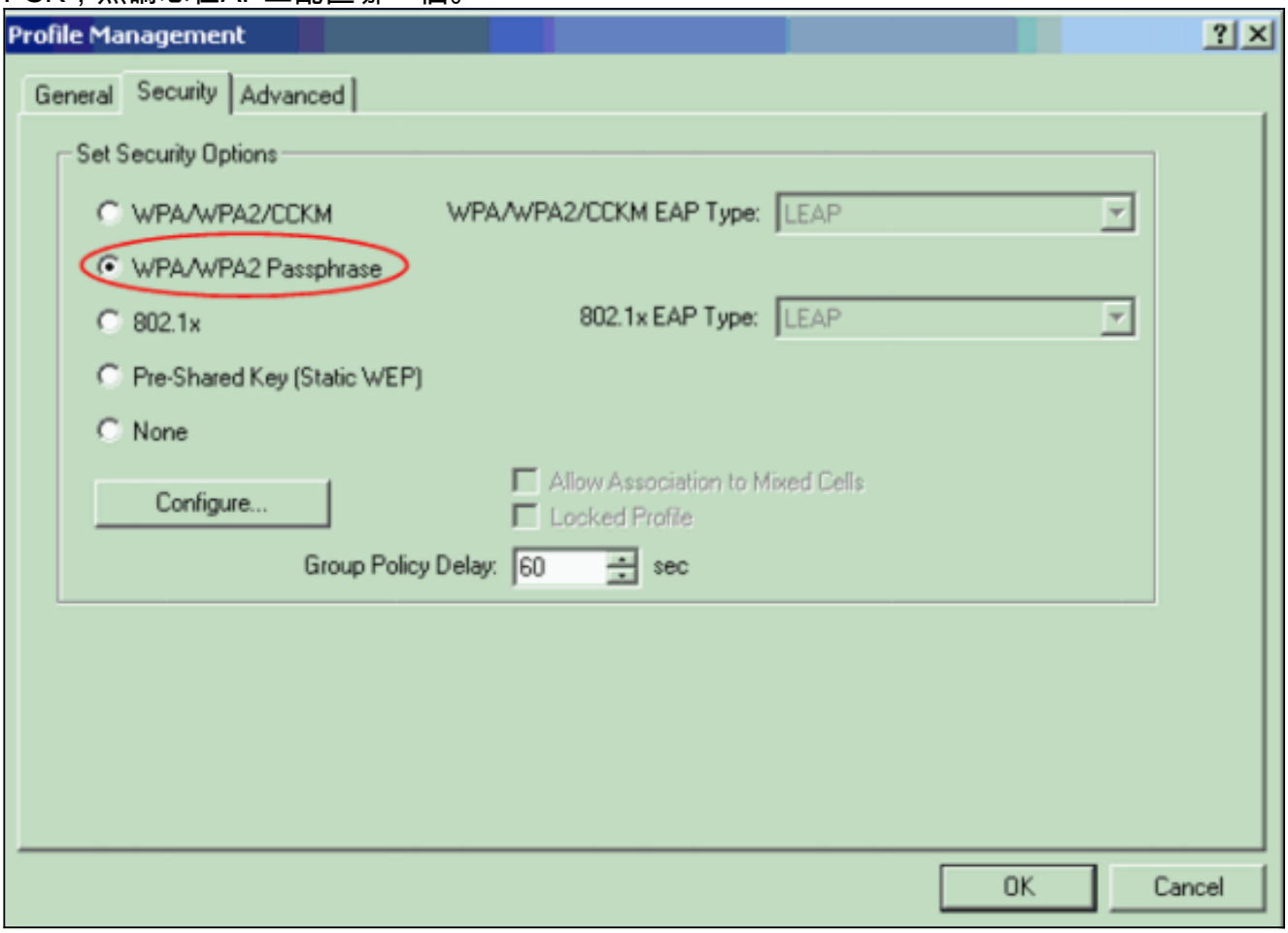
配置客戶端介面卡

請完成以下步驟：

1. 在ADU的Profile Management視窗中，按一下**New**以建立新的配置檔案。此時將顯示一個新視窗，您可以在其中設定WPA 2 PSK操作模式的配置。在「General（常規）」頁籤下，輸入客戶端介面卡將使用的配置檔名稱和SSID。在本示例中，配置檔名稱為WPA2-PSK，SSID為WPA2PSK:**註**：SSID必須與您在AP上為WPA 2 PSK配置的SSID匹配。

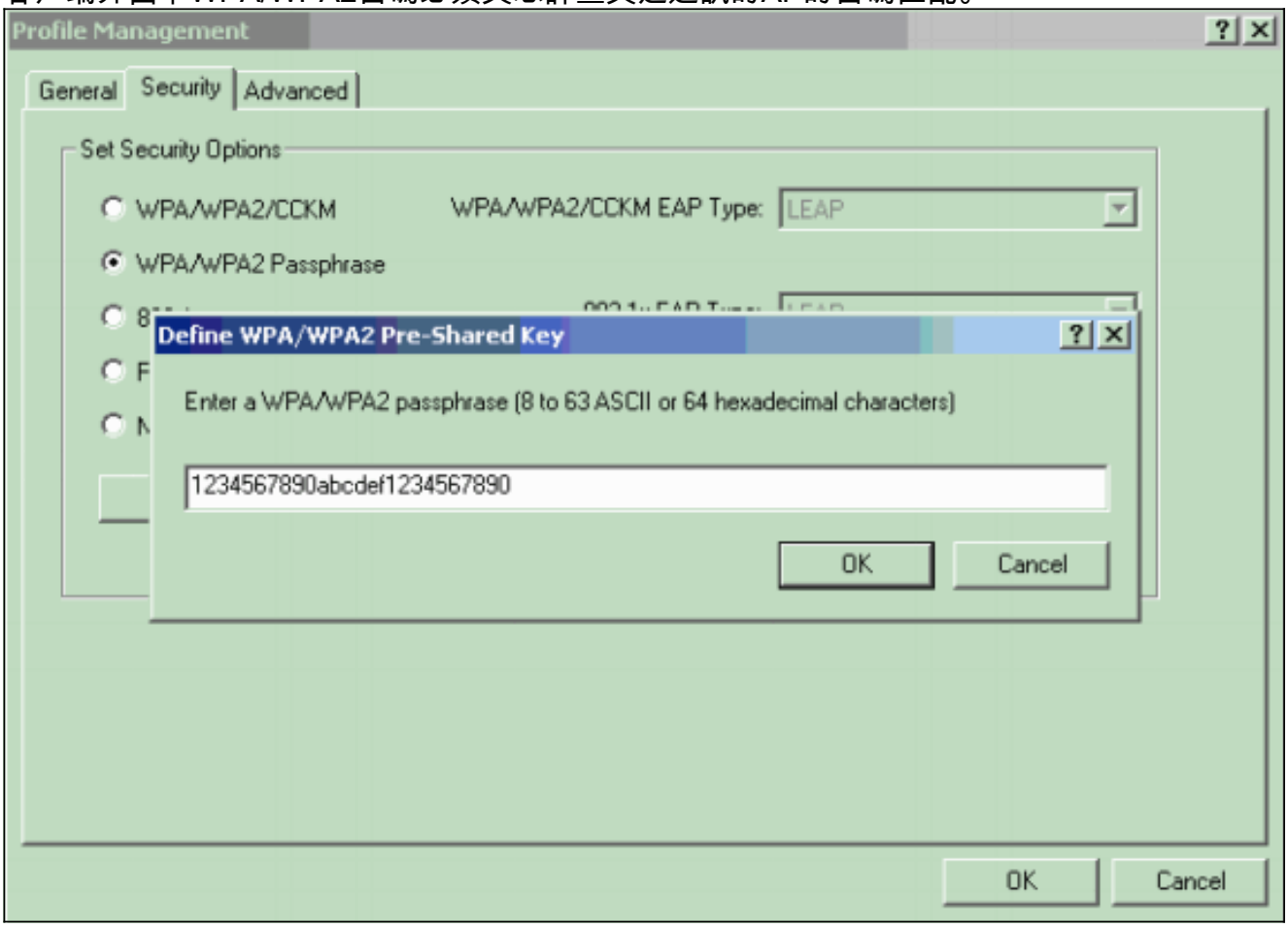


2. 按一下**Security**頁籤，然後按一下**WPA/WPA2密碼**。此操作將啟用WPA PSK或WPA 2 PSK，無論您在AP上配置哪一個。



3. 按一下「**Configure**」。將顯示「定義WPA/WPA2預共用金鑰」視窗。

4. 從系統管理員處獲取WPA/WPA2密碼短語，然後在WPA/WPA2密碼短語欄位中輸入該密碼。獲得基礎架構網路中AP的密碼或點對點網路中其他使用者端的密碼短語。使用以下准則以輸入密碼短語：WPA/WPA2密碼必須包含8到63個ASCII文本字元或64個十六進位制字元。您的客戶端介面卡WPA/WPA2密碼必須與您計畫與之通訊的AP的密碼匹配。



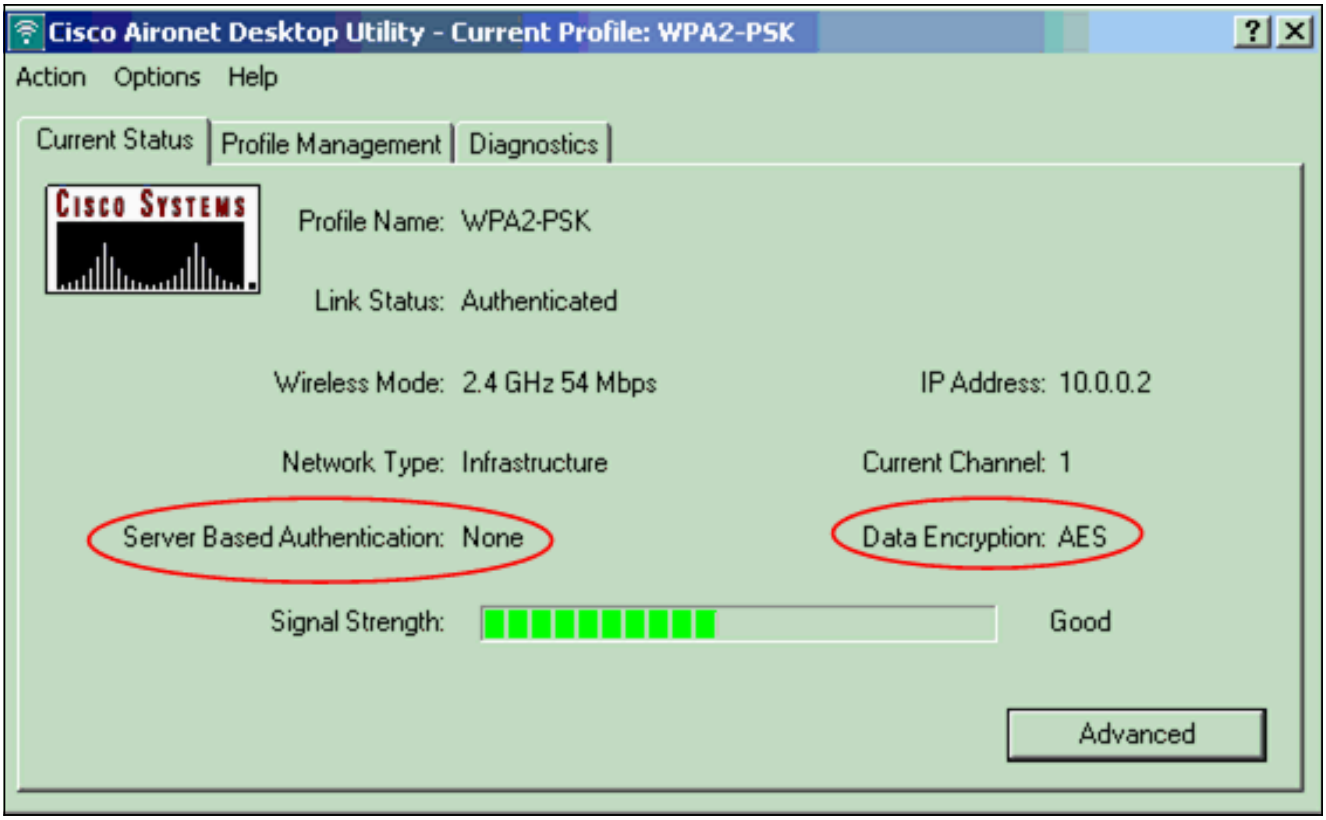
5. 按一下**OK**以儲存密碼並返回「設定檔管理」視窗。

驗證

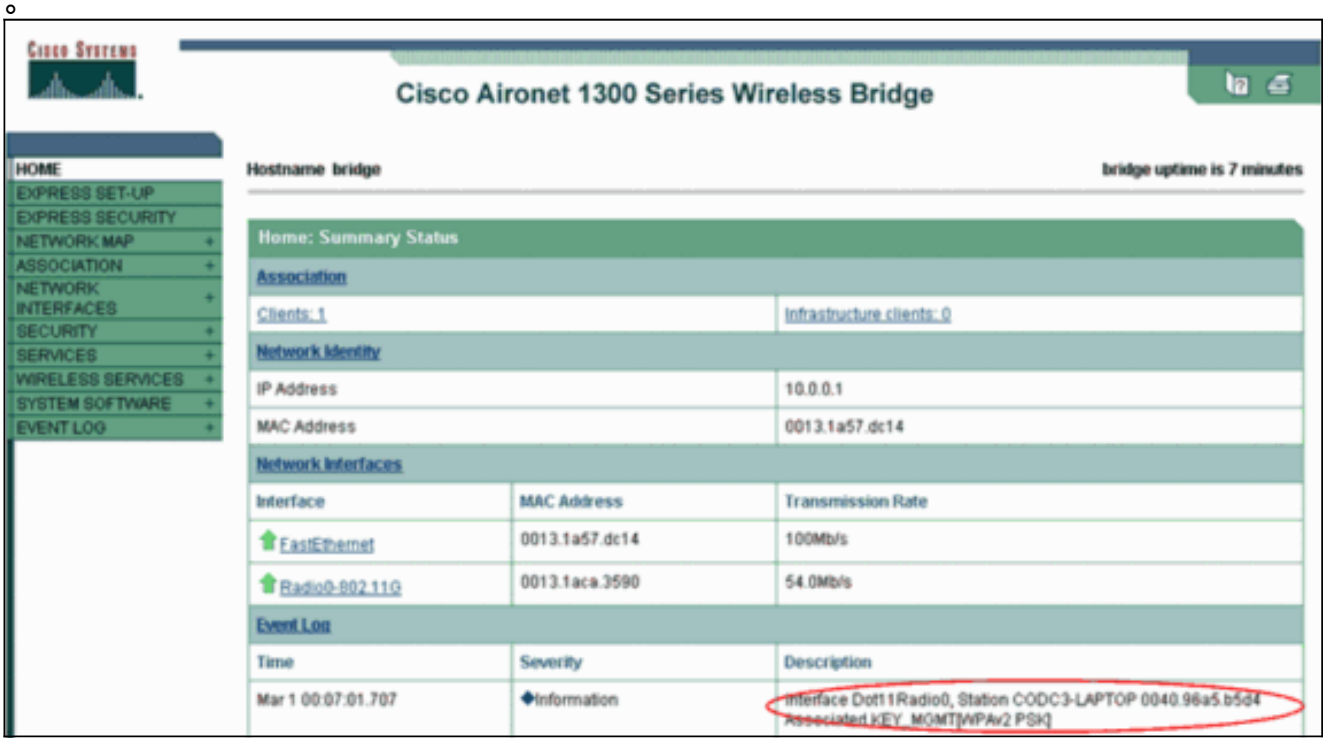
使用本節內容，確認您的組態是否正常運作。

啟用WPA 2 PSK配置檔案後，AP會根據WPA 2密碼短語(PSK)對客戶端進行身份驗證，並提供對WLAN的訪問。

1. 檢查ADU當前狀態以驗證身份驗證成功。此視窗提供了一個示例。此視窗顯示使用的加密是AES，並且未執行任何基於伺服器的身份驗證
：



2. 檢查AP/bridge事件日誌以驗證客戶端是否已成功通過WPA 2 PSK身份驗證模式進行身份驗證。



疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- 配置密碼套件和WEP
- 配置身份驗證型別

- WPA配置概述
- WPA2 - Wi-Fi保護訪問2
- 什麼是WPA混合模式操作，以及如何在AP中配置它
- 無線支援頁面
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。