

在固定ISR上配置無線身份驗證型別

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[背景資訊](#)

[設定](#)

[網路圖表](#)

[配置開放式身份驗證](#)

[配置整合路由和橋接\(IRB\)並設定網橋組](#)

[設定橋接虛擬介面\(BVI\)](#)

[配置SSID進行開放式身份驗證](#)

[為此VLAN的無線客戶端配置內部DHCP伺服器](#)

[配置802.1x/EAP身份驗證](#)

[配置整合路由和橋接\(IRB\)並設定網橋組](#)

[設定橋接虛擬介面\(BVI\)](#)

[配置本地RADIUS伺服器以進行EAP身份驗證](#)

[為802.1x/EAP身份驗證配置SSID](#)

[為此VLAN的無線客戶端配置內部DHCP伺服器](#)

[WPA金鑰管理](#)

[配置WPA-PSK](#)

[配置整合路由和橋接\(IRB\)並設定網橋組](#)

[設定橋接虛擬介面\(BVI\)](#)

[為WPA-PSK身份驗證配置SSID](#)

[為此VLAN的無線客戶端配置內部DHCP伺服器](#)

[配置WPA \(使用EAP \) 身份驗證](#)

[配置整合路由和橋接\(IRB\)並設定網橋組](#)

[設定橋接虛擬介面\(BVI\)](#)

[為WPA身份驗證配置本地RADIUS伺服器](#)

[為採用EAP身份驗證的WPA配置SSID](#)

[為此VLAN的無線客戶端配置內部DHCP伺服器](#)

[配置無線客戶端進行身份驗證](#)

[配置無線客戶端進行開放式身份驗證](#)

[配置無線客戶端進行802.1x/EAP身份驗證](#)

[配置無線客戶端進行WPA-PSK身份驗證](#)

[為WPA \(採用EAP \) 身份驗證配置無線客戶端](#)

[疑難排解](#)

[疑難排解指令](#)

[相關資訊](#)

簡介

本文檔提供配置示例，說明如何使用CLI命令在思科無線整合固定配置路由器上配置各種第2層身份驗證型別，以實現無線連線。

必要條件

需求

嘗試此組態之前，請確保符合以下要求：

- 瞭解如何配置思科整合多業務路由器(ISR)的基本引數
- 瞭解如何使用Aironet案頭實用程式(ADU)配置802.11a/b/g無線客戶端介面卡

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(8)YI1的Cisco 877W ISR
- 採用Aironet案頭實用程式版本3.6的筆記型電腦
- 運行韌體版本3.6的802.11 a/b/g客戶端介面卡

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

請參閱[思科技術提示慣例以瞭解更多有關文件慣例的資訊。](#)

背景資訊

思科整合服務固定配置路由器支援安全、經濟實惠且易於使用的無線區域網解決方案，該解決方案將移動性和靈活性與網路專業人員所需的企業級功能相結合。使用基於Cisco IOS軟體的管理系統，Cisco路由器充當接入點並符合Wi-Fi認證、符合IEEE 802.11a/b/g標準的無線LAN收發器。

您可以使用命令列介面(CLI)、基於瀏覽器的管理系統或簡單網路管理協定(SNMP)來配置和監控路由器。本文檔介紹如何使用CLI命令配置ISR的無線連線。

設定

此示例說明如何使用CLI命令在思科無線整合固定配置路由器上配置這些身份驗證型別。

- 開放式身份驗證

- 802.1x/EAP (可擴展身份驗證協定) 身份驗證
- Wi-Fi保護訪問預共用金鑰(WPA-PSK)身份驗證
- WPA (使用EAP) 身份驗證

注意：本文檔不關注共用身份驗證，因為它是安全性較低的身份驗證型別。

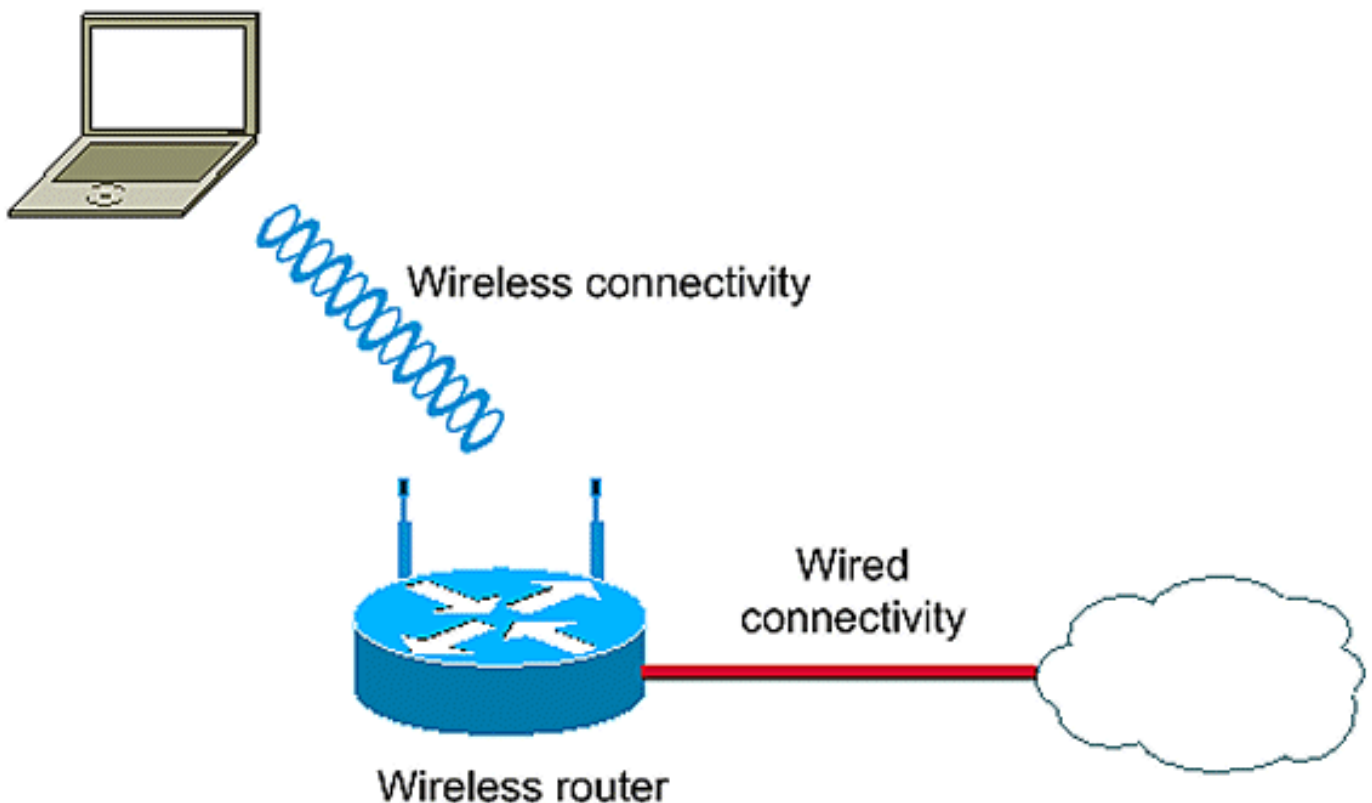
本節提供用於設定本文件中所述功能的資訊。

註：使用[Command Lookup Tool](#)(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

網路圖表

此文件使用以下網路設定：

Wireless LAN Client



此安裝程式使用無線ISR上的本地RADIUS伺服器通過802.1x身份驗證對無線客戶端進行身份驗證。

配置開放式身份驗證

開放式身份驗證是null身份驗證演算法。接入點會授予任何身份驗證請求。開放式身份驗證允許任何裝置訪問網路。如果在網路上未啟用加密，則任何知道接入點SSID的裝置都可以訪問該網路。在接入點上啟用WEP加密後，WEP金鑰本身就成為一種訪問控制手段。如果裝置沒有正確的WEP金鑰，即使身份驗證成功，裝置仍無法通過接入點傳輸資料。它也無法解密從接入點傳送的資料。

此示例配置僅說明了簡單的開放式身份驗證。WEP金鑰可以設為強制或可選。此示例將WEP金鑰配

置為可選金鑰，以便任何不使用WEP的裝置也能驗證和關聯此AP。

如需詳細資訊，請參閱[開放驗證](#)。

此示例使用此配置設定在ISR上配置開放式身份驗證。

- SSID名稱：「open」
- VLAN 1
- 內部DHCP伺服器範圍: 10.1.0.0/16

注意：為了簡便起見，此示例不會對經過身份驗證的客戶端使用任何加密技術。

在路由器上完成以下操作：

1. [配置整合路由和橋接\(IRB\)並設定網橋組](#)
2. [設定橋接虛擬介面\(BVI\)](#)
3. [配置SSID進行開放式身份驗證](#)
4. [為此VLAN的無線客戶端配置內部DHCP伺服器](#)

配置整合路由和橋接(IRB)並設定網橋組

完成以下操作：

1. 在路由器中啟用IRB。

```
router<configure>#bridge irb
```

注意：如果要在同一台路由器上配置所有安全型別，則僅可在路由器上全域性啟用IRB一次。不需要為每個單獨的身份驗證型別啟用它。

2. 定義網橋組。

此示例使用網橋組編號1。

```
router<configure>#bridge 1
```

3. 為網橋組選擇生成樹協定。

此處，為此網橋組配置了IEEE生成樹協定。

```
router<configure>#bridge 1 protocol ieee
```

4. 啟用BVI以接受和路由從其對應網橋組接收的可路由資料包。

此示例使BVI能夠接受和路由IP資料包。

```
router<configure>#bridge 1 route ip
```

設定橋接虛擬介面(BVI)

完成以下操作：

1. 配置BVI。

將網橋組的往來行號分配給BVI時配置BVI。每個網橋組只能有一個對應的BVI。此示例將網橋組編號1分配給BVI。

```
router<configure>#interface BVI <1>
```

2. 為BVI分配IP地址。

```
router<config-if>#ip address 10.1.1.1 255.255.0.0
```

```
router<config-if>#no shut
```

有關橋接的詳細資訊，請參閱[配置橋接](#)。

配置SSID進行開放式身份驗證

完成以下操作：

1. 啟用無線電介面

要啟用無線電介面，請轉到DOT11無線電介面配置模式並為介面分配SSID。

```
router<config>#interface dot11radio0
```

```
router<config-if>#no shutdown
```

```
router<config-if>#ssid open
```

開放式身份驗證型別可以與MAC地址身份驗證結合配置。在這種情況下，接入點會強制所有客戶端裝置在獲准加入網路之前執行MAC地址身份驗證。

開放式身份驗證也可與EAP身份驗證一起配置。接入點會強制所有客戶端裝置執行EAP身份驗證，然後才允許它們加入網路。對於list-name，指定身份驗證方法清單。

為EAP身份驗證配置的接入點強制關聯的所有客戶端裝置執行EAP身份驗證。未使用EAP的客戶端裝置無法使用接入點。

2. 將SSID繫結到VLAN。

要在此介面上啟用SSID，請在SSID配置模式下將SSID繫結到VLAN。

```
router<config-ssid>vlan 1
```

3. 使用開放式身份驗證配置SSID。

```
router<config-ssid>#authentication open
```

4. 為WEP金鑰配置無線電介面 (可選)。

```
router<config>#encryption vlan 1 mode WEP可選
```

5. 在無線電介面上啟用VLAN。

```
router<config>#interface Dot11Radio 0.1
```

```
router<config-subif>#encapsulation dot1Q 1
```

```
router<config-subif>#bridge-group 1
```

為此VLAN的無線客戶端配置內部DHCP伺服器

在全域性配置模式下鍵入以下命令，為該VLAN的無線客戶端配置內部DHCP伺服器：

- ip dhcp excluded-address 10.1.1.1 10.1.1.5
- ip dhcp pool open

在DHCP池配置模式下，鍵入以下命令：

- network 10.1.0.0 255.255.0.0
- default-router 10.1.1.1

配置802.1x/EAP身份驗證

此身份驗證型別為您的無線網路提供最高級別的安全性。使用可擴展身份驗證協定(EAP)與相容EAP的RADIUS伺服器互動，接入點可幫助無線客戶端裝置和RADIUS伺服器執行相互身份驗證並派生動態單播WEP金鑰。RADIUS伺服器將WEP金鑰傳送到存取點，存取點會將其用於傳送至使用者端或從使用者端接收的所有單點傳播資料訊號。

有關詳細資訊，請參閱[EAP身份驗證](#)。

此示例使用以下配置設定：

- SSID名稱：leap
- VLAN 2
- 內部DHCP伺服器範圍: 10.2.0.0/16

此示例使用LEAP身份驗證作為驗證無線客戶端的機制。

注意：請參閱[適用於Windows v3.2的Cisco安全ACS採用EAP-TLS電腦身份驗證](#)，以配置EAP-TLS。

註：請參閱[使用PEAP-MS-CHAPv2電腦身份驗證配置Cisco Secure ACS for Windows v3.2](#)以配置PEAP-MS-CHAPv2。

注意：瞭解這些EAP型別的所有配置主要涉及客戶端和身份驗證伺服器端的配置更改。對於所有這些身份驗證型別，無線路由器或接入點上的配置或多或少保持相同。

注意：如最初所述，此設定使用無線ISR上的本地RADIUS伺服器通過802.1x身份驗證對無線客戶端進行身份驗證。

在路由器上完成以下操作：

1. [配置整合路由和橋接\(IRB\)並設定網橋組](#)
2. [設定橋接虛擬介面\(BVI\)](#)
3. [配置本地RADIUS伺服器以進行EAP身份驗證](#)
4. [為802.1x/EAP身份驗證配置SSID](#)
5. [為此VLAN的無線客戶端配置內部DHCP伺服器](#)

配置整合路由和橋接(IRB)並設定網橋組

完成以下操作：

1. 在路由器中啟用IRB。

```
router<configure>#bridge irb
```

注意：如果要在同一台路由器上配置所有安全型別，則僅可在路由器上全域性啟用IRB一次。不需要為每個單獨的身份驗證型別啟用它。

2. 定義網橋組。

此示例使用網橋組編號2。

```
router<configure>#bridge 2
```

3. 為網橋組選擇生成樹協定。

此處，為此網橋組配置了IEEE生成樹協定。

```
router<configure>#bridge 2 protocol ieee
```

4. 為網橋組選擇生成樹協定。

此處，為此網橋組配置了IEEE生成樹協定。

```
router<configure>#bridge 2 protocol ieee
```

5. 啟用BVI以接受和路由從其相應網橋組接收的可路由資料包。

此示例使BVI能夠接受和路由IP資料包。

```
router<configure>#bridge 2 route ip
```

設定橋接虛擬介面(BVI)

完成以下操作：

1. 配置BVI。

將網橋組的往來行號分配給BVI時配置BVI。每個網橋組只能有一個對應的BVI。此示例將網橋組編號2分配給BVI。

```
router<configure>#interface BVI <2>
```

2. 為BVI分配IP地址。

```
router<config-if>#ip address 10.2.1.1 255.255.0.0
```

```
router<config-if>#no shut
```

配置本地RADIUS伺服器以進行EAP身份驗證

如前所述，本文檔使用無線感知路由器上的本地RADIUS伺服器進行EAP身份驗證。

1. 啟用身份驗證、授權和記帳(AAA)訪問控制模型。

```
router<configure>#aaa new-model
```

2. 為RADIUS伺服器建立伺服器組rad-eap。

```
router<configure>#aaa group server radius rad-eap server 10.2.1.1 auth-port 1812 acct-port 1813
```

3. 建立方法清單eap_methods，列出用於驗證AAA登入使用者的驗證方法。將方法清單分配給此伺服器組。

```
router<configure>#aaa authentication login eap_methods group rad-eap
```

4. 啟用路由器作為本地身份驗證伺服器並進入身份驗證器的配置模式。

```
router<configure>#radius-server local
```

5. 在Radius伺服器配置模式下，將路由器新增為本地身份驗證伺服器的AAA客戶端。

```
router<config-radsrv>#nas 10.2.1.1 key Cisco
```

6. 在本地Radius服務器上配置使用者user1。

```
router<config-radsrv>#user user1 password user1 group rad-eap
```

7. 指定RADIUS伺服器主機。

```
router<config-radsrv>#radius-server host 10.2.1.1 auth-port 1812 acct-port 1813 keycisco
```


注意：此金鑰應與nas命令中在radius-server配置模式下指定的金鑰相同。

為802.1x/EAP身份驗證配置SSID

802.1x/EAP的無線電介面和相關SSID的配置涉及路由器上各種無線引數的配置，包括SSID、加密模式和身份驗證型別。此示例使用名為leap的SSID。

1. 啟用無線電介面。

要啟用無線電介面，請轉到DOT11無線電介面配置模式並為介面分配SSID。

```
router<config>#interface dot11radio0
```

```
router<config-if>#no shutdown
```

```
router<config-if>#ssid leap
```

2. 將SSID繫結到VLAN。

要在此介面上啟用SSID，請在SSID配置模式下將SSID繫結到VLAN。

```
router<config-ssid>#vlan 2
```

3. 使用802.1x/LEAP身份驗證配置SSID。

```
router<config-ssid>#authentication network-eap eap_methods
```

4. 配置用於動態金鑰管理的無線電介面。

```
router<config>#encryption vlan 2模式密碼wep40
```

5. 在無線電介面上啟用VLAN。

```
router<config>#interface Dot11Radio 0.2
```

```
router<config-subif>#encapsulation dot1Q 2
```

```
router<config-subif>#bridge-group 2
```

為此VLAN的無線客戶端配置內部DHCP伺服器

在全域性配置模式下鍵入以下命令，為該VLAN的無線客戶端配置內部DHCP伺服器：

- ip dhcp excluded-address 10.2.1.1 10.2.1.5
- ip dhcp pool leapauth

在DHCP池配置模式下，鍵入以下命令：

- network 10.2.0.0 255.255.0.0

- default-router 10.2.1.1

WPA金鑰管理

Wi-Fi Protected Access是一種基於標準的互操作性安全增強功能，可大大提高當前和未來無線LAN系統的資料保護和訪問控制級別。

有關詳細資訊，請參閱[WPA金鑰管理](#)。

WPA金鑰管理支援兩種互斥管理型別：WPA — 預共用金鑰(WPA-PSK)和WPA (使用EAP)。

配置WPA-PSK

WPA-PSK在基於802.1x的身份驗證不可用的無線LAN上用作金鑰管理型別。在此類網路中，您必須在接入點上配置預共用金鑰。您可以以ASCII或十六進位制字元的形式輸入預共用金鑰。如果輸入金鑰為ASCII字元，則輸入8到63個字元，然後接入點將使用基於密碼的加密標準(RFC2898)中所述的過程來擴展金鑰。如果輸入金鑰為十六進位制字元，則必須輸入64個十六進位制字元。

此示例使用以下配置設定：

- SSID名稱：wpa-shared
- VLAN 3
- 內部DHCP伺服器範圍: 10.3.0.0/16

在路由器上完成以下操作：

1. [配置整合路由和橋接\(IRB\)並設定網橋組](#)
2. [設定橋接虛擬介面\(BVI\)](#)
3. [為WPA-PSK身份驗證配置SSID](#)
4. [為此VLAN的無線客戶端配置內部DHCP伺服器](#)

配置整合路由和橋接(IRB)並設定網橋組

完成以下操作：

1. 在路由器中啟用IRB。

```
router<configure>#bridge irb
```

注意：如果要在同一台路由器上配置所有安全型別，則僅可在路由器上全域性啟用IRB一次。不需要為每個單獨的身份驗證型別啟用它。

2. 定義網橋組。

本示例使用網橋組編號3。

```
router<configure>#bridge 3
```

3. 為網橋組選擇生成樹協定。

為此網橋組配置了IEEE生成樹協定。

```
router<configure>#bridge 3 protocol ieee
```

4. 啟用BVI以接受和路由從其對應網橋組接收的可路由資料包。

此示例使BVI能夠接受和路由IP資料包。

```
router<configure>#bridge 3 route ip
```

設定橋接虛擬介面(BVI)

完成以下操作：

1. 配置BVI。

將網橋組的往來行號分配給BVI時配置BVI。每個網橋組只能有一個對應的BVI。此示例將網橋組編號3分配給BVI。

```
router<configure>#interface BVI <2>
```

2. 為BVI分配IP地址。

```
router<config-if>#ip address 10.3.1.1 255.255.0.0
```

```
router<config-if>#no shut
```

為WPA-PSK身份驗證配置SSID

完成以下操作：

1. 啟用無線電介面。

要啟用無線電介面，請轉到DOT11無線電介面配置模式並為介面分配SSID。

```
router<config>#interface dot11radio0
```

```
router<config-if>#no shutdown
```

```
router<config-if>#ssid wpa-shared
```

2. 要啟用WPA金鑰管理，首先為VLAN介面配置WPA加密密碼。此範例使用tkip作為加密密碼。

鍵入此命令以指定無線電介面上的WPA金鑰管理型別。

```
router<config>#interface dot11radio0
```

```
router(config-if)#encryption vlan 3 mode ciphers tkip
```

3. 將SSID繫結到VLAN。

要在此介面上啟用SSID，請在SSID配置模式下將SSID繫結到VLAN。

```
router<config-ssid>vlan 3
```

4. 使用WPA-PSK身份驗證配置SSID。

您需要首先在SSID配置模式下配置開放或網路EAP身份驗證，以啟用WPA金鑰管理。此示例配置開放式身份驗證。

```
router<config>#interface dot11radio0
```

```
router<config-if>#ssid wpa-shared
```

```
router<config-ssid>#authentication open
```

現在，在SSID上啟用WPA金鑰管理。已為此VLAN配置金鑰管理密碼tkip。

```
router(config-if-ssid)#authentication key-management wpa
```

在SSID上配置WPA-PSK身份驗證。

```
router(config-if-ssid)#wpa-psk ascii 1234567890 !— 1234567890是此SSID的預共用金鑰值。  
確保在客戶端為此SSID指定相同的金鑰。
```

5. 在無線電介面上啟用VLAN。

```
router<config>#interface Dot11Radio 0.3
```

```
router<config-subif>#encapsulation dot1Q 3
```

```
router<config-subif>#bridge-group 3
```

為此VLAN的無線客戶端配置內部DHCP伺服器

在全域性配置模式下鍵入以下命令，為該VLAN的無線客戶端配置內部DHCP伺服器：

- ip dhcp excluded-address 10.3.1.1 10.3.1.5
- ip dhcp pool wpa-psk

在DHCP池配置模式下，鍵入以下命令：

- network 10.3.0.0 255.255.0.0
- default-router 10.3.1.1

配置WPA (使用EAP) 身份驗證

這是另一個WPA金鑰管理型別。在這裡，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，並且客戶端和伺服器生成成對主金鑰(PMK)。使用WPA時，伺服器會動態生成PMK並將其傳遞到接入點，但使用WPA-PSK時，您可在客戶端和接入點上配置預共用金鑰，該預共用金鑰將用作PMK。

有關詳細資訊，請參閱[具有EAP身份驗證的WPA](#)。

此示例使用以下配置設定：

- SSID名稱：wpa-dot1x
- VLAN 4
- 內部DHCP伺服器範圍：10.4.0.0/16

在路由器上完成以下操作：

1. [配置整合路由和橋接\(IRB\)並設定網橋組](#)
2. [設定橋接虛擬介面\(BVI\)](#)
3. [為WPA身份驗證配置本地RADIUS伺服器。](#)
4. [為採用EAP身份驗證的WPA配置SSID](#)
5. [為此VLAN的無線客戶端配置內部DHCP伺服器](#)

配置整合路由和橋接(IRB)並設定網橋組

完成以下操作：

1. 在路由器中啟用IRB。

```
router<configure>#bridge irb
```

注意：如果要在同一台路由器上配置所有安全型別，則僅可在路由器上全域性啟用IRB一次。不需要為每個單獨的身份驗證型別啟用它。

2. 定義網橋組。

本示例使用網橋組編號4。

```
router<configure>#bridge 4
```

3. 為網橋組選擇生成樹協定。

此處，為此網橋組配置了IEEE生成樹協定。

```
router<configure>#bridge 4 protocol ieee
```

4. 啟用BVI以接受和路由從其對應網橋組接收的可路由資料包。

此示例使BVI能夠接受和路由IP資料包。

```
router<configure>#bridge 4 route ip
```

設定橋接虛擬介面(BVI)

完成以下操作：

1. 配置BVI。

將網橋組的往來行號分配給BVI時配置BVI。每個網橋組只能有一個對應的BVI。此示例將網橋組編號4分配給BVI。

```
router<configure>#interface BVI <4>
```

2. 為BVI分配IP地址。

```
router<config-if>#ip address 10.4.1.1 255.255.0.0
```

```
router<config-if>#no shut
```

為WPA身份驗證配置本地RADIUS伺服器

如需詳細程式，請參閱[802.1x/EAP驗證](#)一節。

為採用EAP身份驗證的WPA配置SSID

完成以下操作：

1. 啟用無線電介面。

要啟用無線電介面，請轉到DOT11無線電介面配置模式並為介面分配SSID。

```
router<config>#interface dot11radio0
```

```
router<config-if>#no shutdown
```

```
router<config-if>#ssid wpa-dot1x
```

2. 要啟用WPA金鑰管理，首先為VLAN介面配置WPA加密密碼。此範例使用tkip作為加密密碼。

鍵入此命令以指定無線電介面上的WPA金鑰管理型別。

```
router<config>#interface dot11radio0
```

```
router(config-if)#encryption vlan 4 mode ciphers tkip
```

3. 將SSID繫結到VLAN。

要在此介面上啟用SSID，請在SSID配置模式下將SSID繫結到VLAN。

```
vlan 4
```

4. 使用WPA-PSK身份驗證配置SSID。

要配置無線介面以使用EAP身份驗證WPA，首先配置網路EAP的關聯SSID。

```
router<config>#interface dot11radio0
```

```
router<config-if>#ssid wpa-shared
```

```
router<config-ssid>#authentication network eap eap_methods
```

5. 現在，在SSID上啟用WPA金鑰管理。已為此VLAN配置金鑰管理密碼tkip。

```
router(config-if-ssid)#authentication key-management wpa
```

6. 在無線電介面上啟用VLAN。

```
router<config>#interface Dot11Radio 0.4
```

```
router<config-subif>#encapsulation dot1Q 4
```

```
router<config-subif>#bridge-group 4
```

為此VLAN的無線客戶端配置內部DHCP伺服器

在全域性配置模式下鍵入以下命令，為該VLAN的無線客戶端配置內部DHCP伺服器：

- ip dhcp excluded-address 10.4.1.1 10.4.1.5
- ip dhcp pool wpa-dot1shared

在DHCP池配置模式下，鍵入以下命令：

- network 10.4.0.0 255.255.0.0
- default-router 10.4.1.1

配置無線客戶端進行身份驗證

配置ISR後，按照說明為不同的身份驗證型別配置無線客戶端，以便路由器可以對這些無線客戶端進行身份驗證並提供對WLAN網路的訪問。本文檔使用Cisco Aironet案頭實用程式(ADU)進行客戶端配置。

配置無線客戶端進行開放式身份驗證

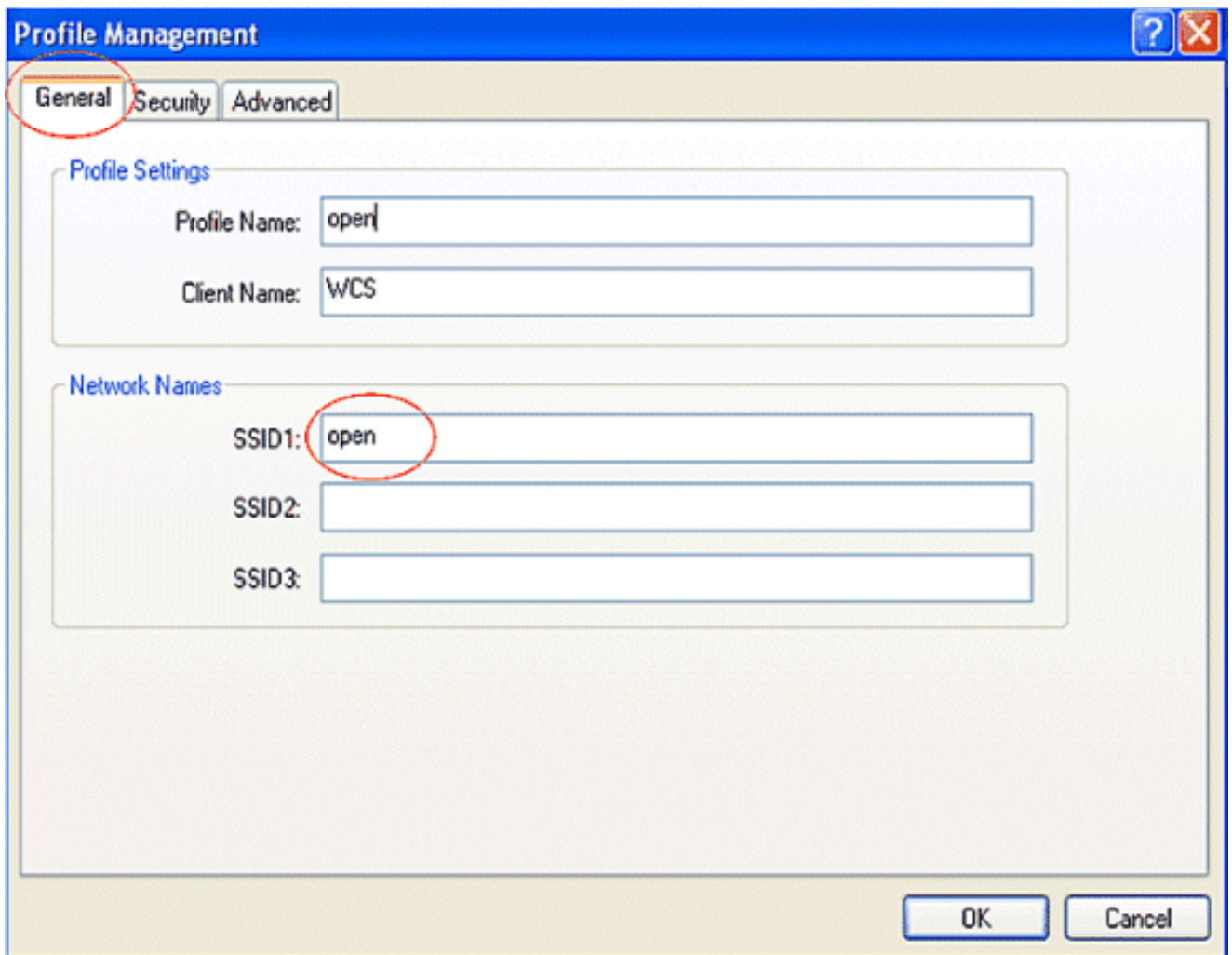
請完成以下步驟：

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，您可以在其中設定開放式身份驗證的配置。在General索引標籤下，輸入使用者端配接器使用的設定檔名稱和SSID。

在此示例中，配置檔名稱和SSID為open。

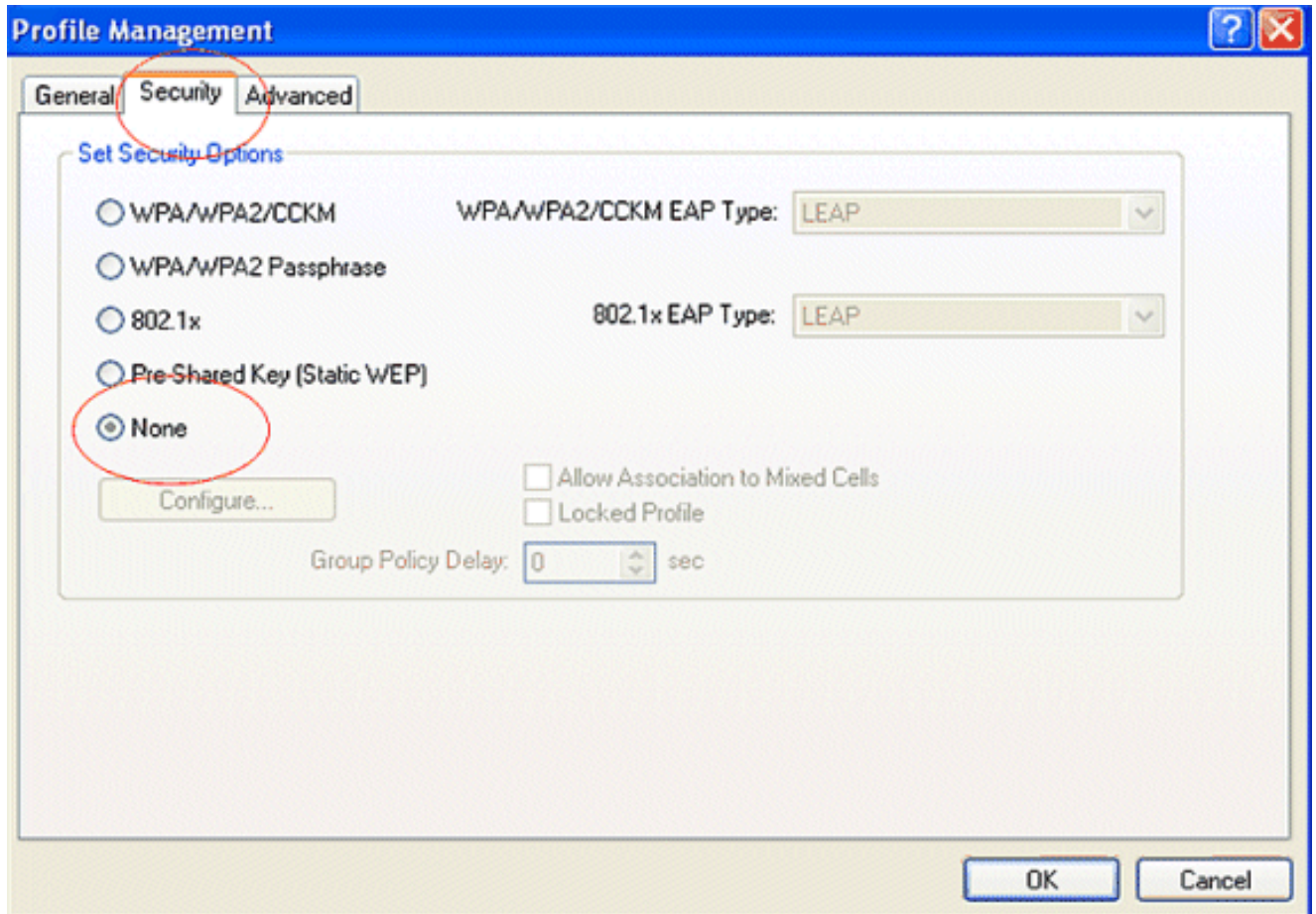
注意：SSID必須與您在ISR上為開放式身份驗證配置的SSID匹配。



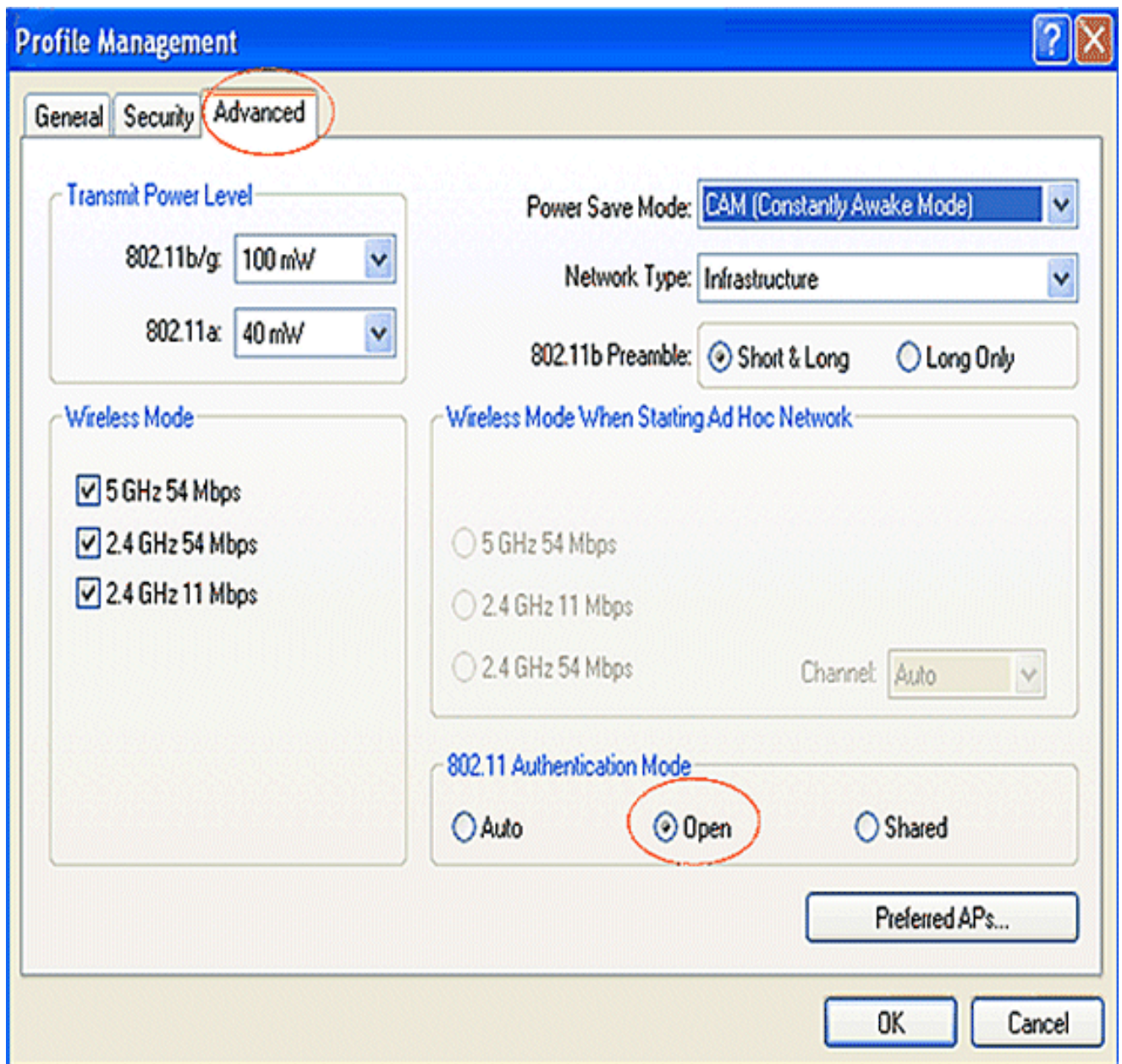
The screenshot shows the 'Profile Management' dialog box with the 'General' tab selected. The 'Profile Settings' section contains two text boxes: 'Profile Name' with the value 'open' and 'Client Name' with the value 'WCS'. The 'Network Names' section contains three text boxes: 'SSID1' with the value 'open', 'SSID2' which is empty, and 'SSID3' which is empty. The 'General' tab is circled in red, and the 'SSID1' text box is also circled in red. At the bottom right, there are 'OK' and 'Cancel' buttons.

2. 按一下Security頁籤，將WEP加密的安全選項保留為None。由於此示例將WEP用作可選的，將此選項設定為None將允許客戶端成功與WLAN網路關聯和通訊。

按一下「OK」

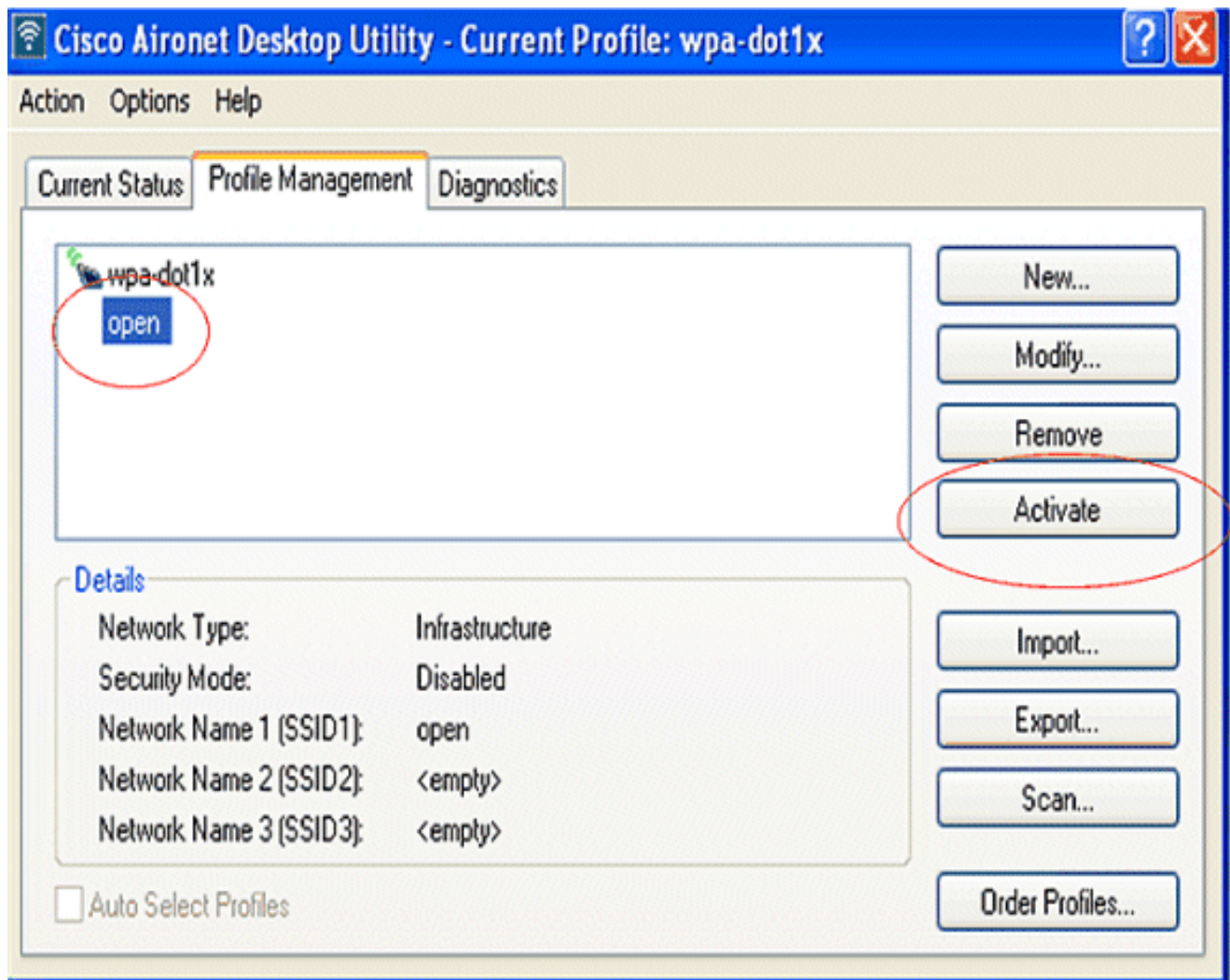


3. 從Profile Management頁籤中選擇Advanced視窗，並將802.11 Authentication Mode設定為Open以進行開放式身份驗證。

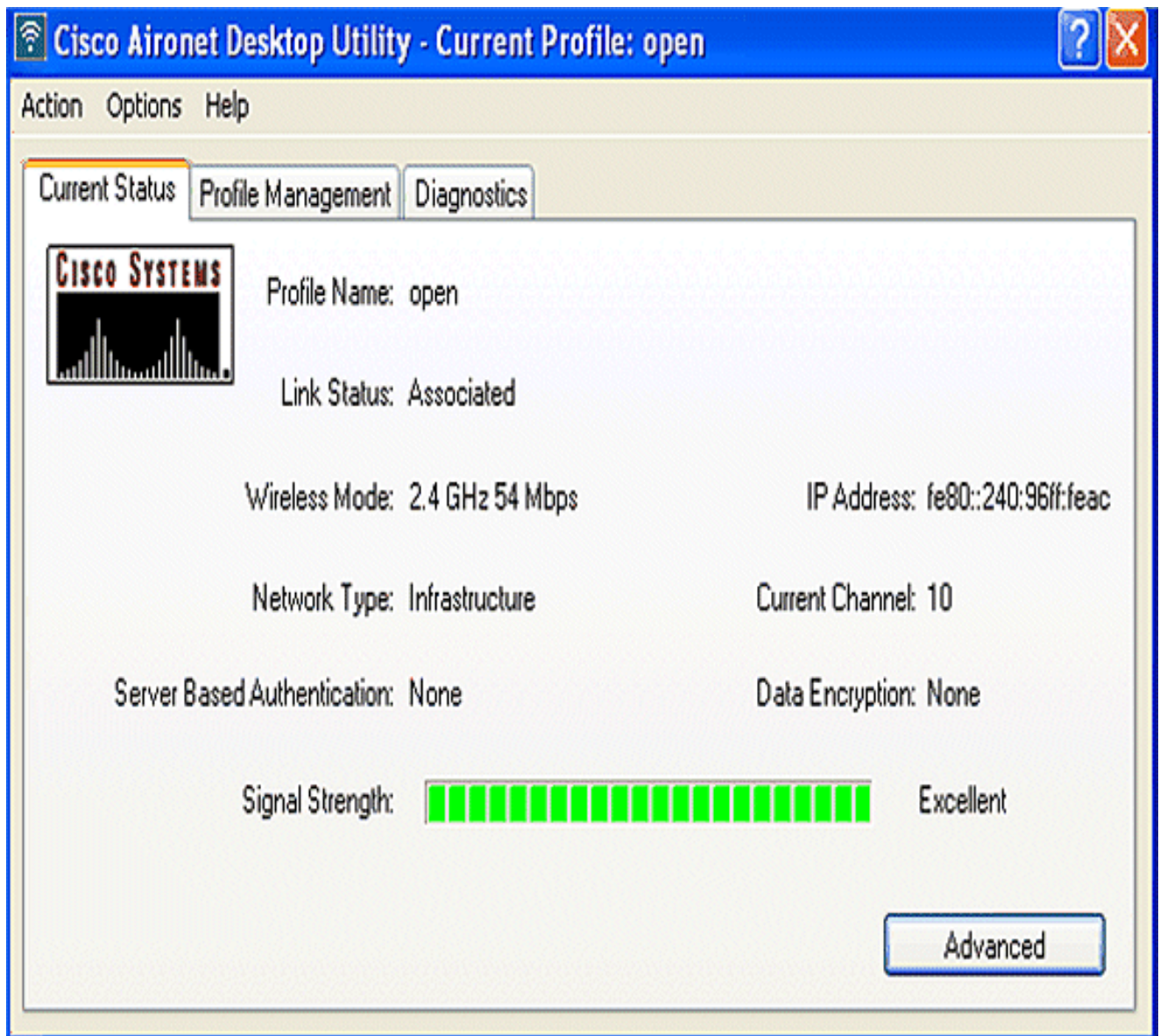


使用本節內容，確認您的組態是否正常運作。

1. 建立客戶端配置檔案後，點選Profile Management頁籤下的Activate以啟用該配置檔案。



2. 檢查ADU狀態以確認身份驗證成功。



配置無線客戶端進行802.1x/EAP身份驗證

請完成以下步驟：

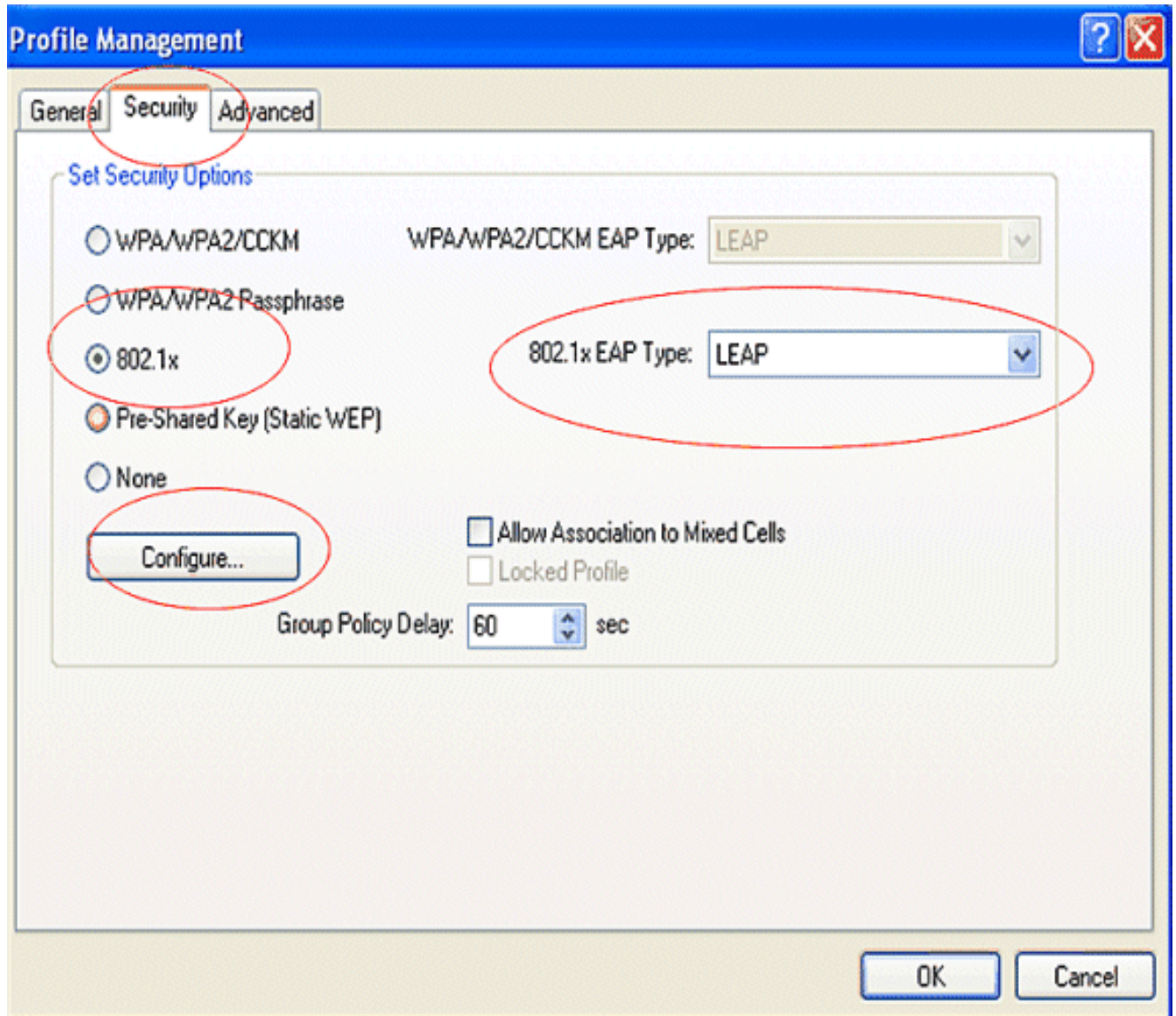
1. 在ADU的Profile Management視窗中，按一下New以建立新的配置檔案。

此時將顯示一個新視窗，您可以在其中設定開放式身份驗證的配置。在General索引標籤下，輸入使用者端配接器使用的設定檔名稱和SSID。

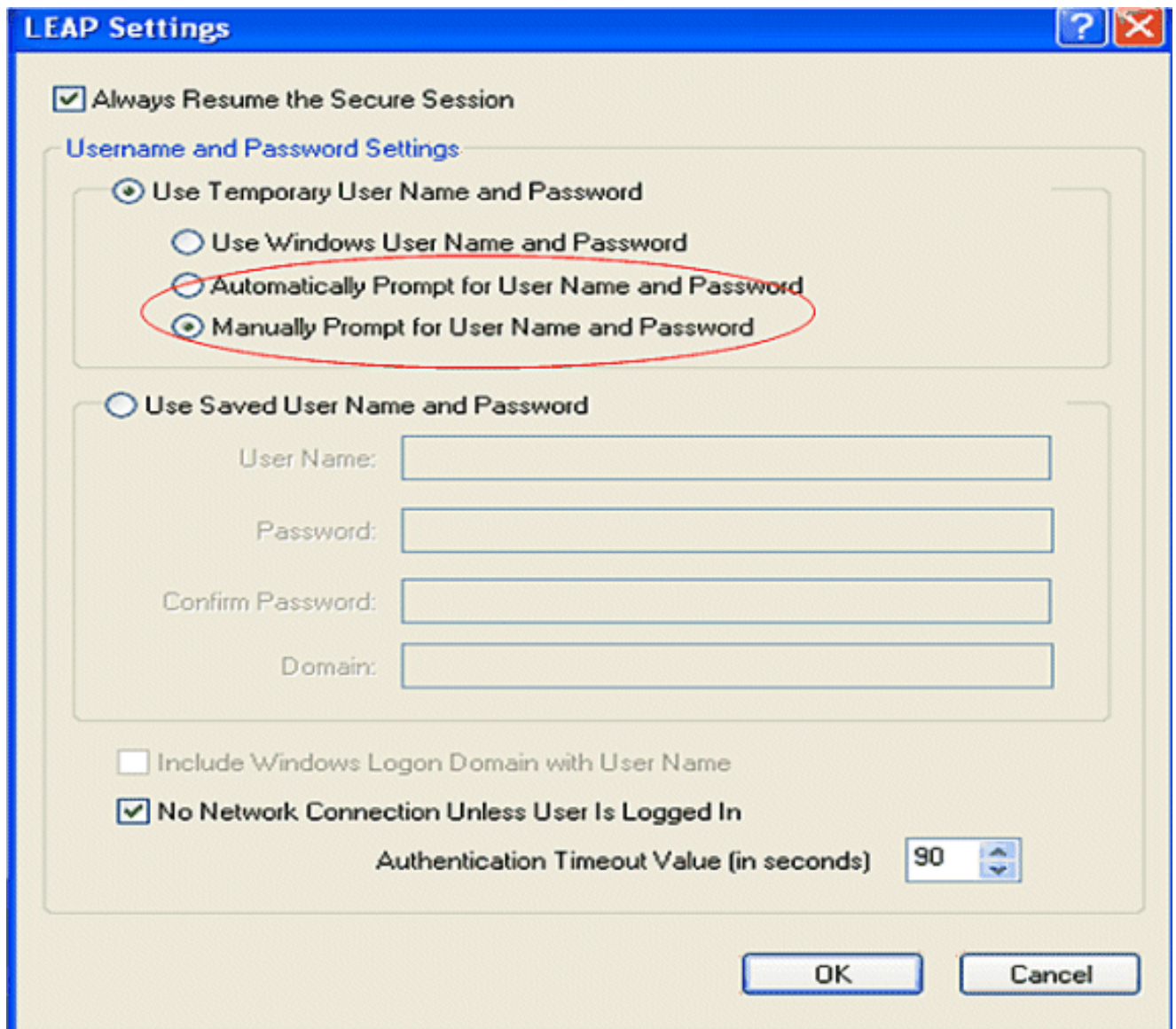
在本示例中，配置檔名稱和SSID是leap。

2. 在Profile Management下，按一下Security頁籤，將安全選項設定為802.1x，然後選擇適當的EAP型別。本文檔使用LEAP作為EAP型別進行身份驗證。現在，按一下Configure以配置LEAP使用者名稱和密碼設定。

注意：注意：SSID必須與您在ISR上為802.1x/EAP身份驗證配置的SSID匹配。

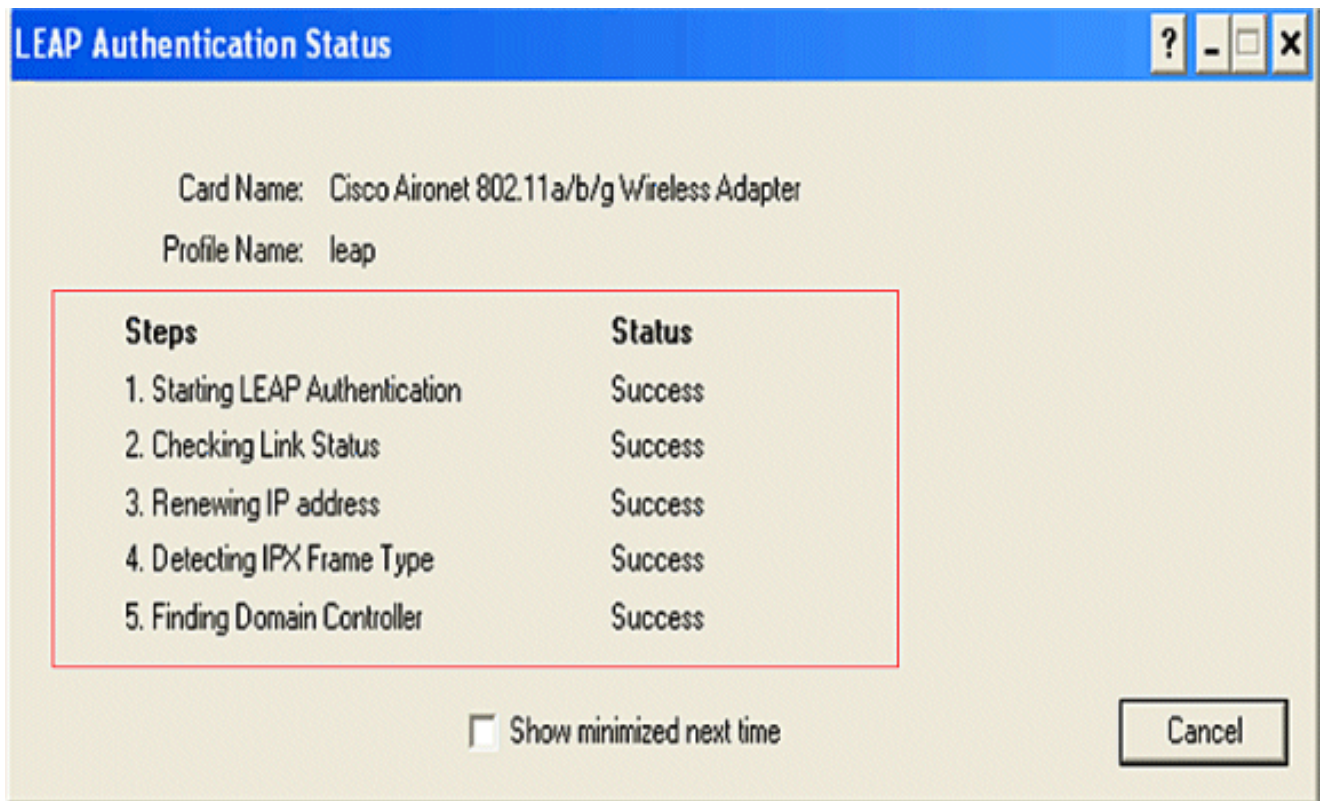


3. 在使用者名稱和密碼設定下，此示例選擇Manually Prompt for User Name and Password，以便在客戶端嘗試連線到網路時提示客戶端輸入正確的使用者名稱和密碼。按一下「OK」（確定）。



使用本節內容，確認您的組態是否正常運作。

- 建立客戶端配置檔案後，按一下Profile Management頁籤下的Activate以啟用配置檔案跳躍。系統將提示您輸入leap使用者名稱和密碼。此示例使用使用者名稱和密碼user1。按一下「OK」（確定）。
- 您可以監視客戶端身份驗證成功，並從路由器上配置的DHCP伺服器分配一個IP地址。



配置無線客戶端進行WPA-PSK身份驗證

請完成以下步驟：

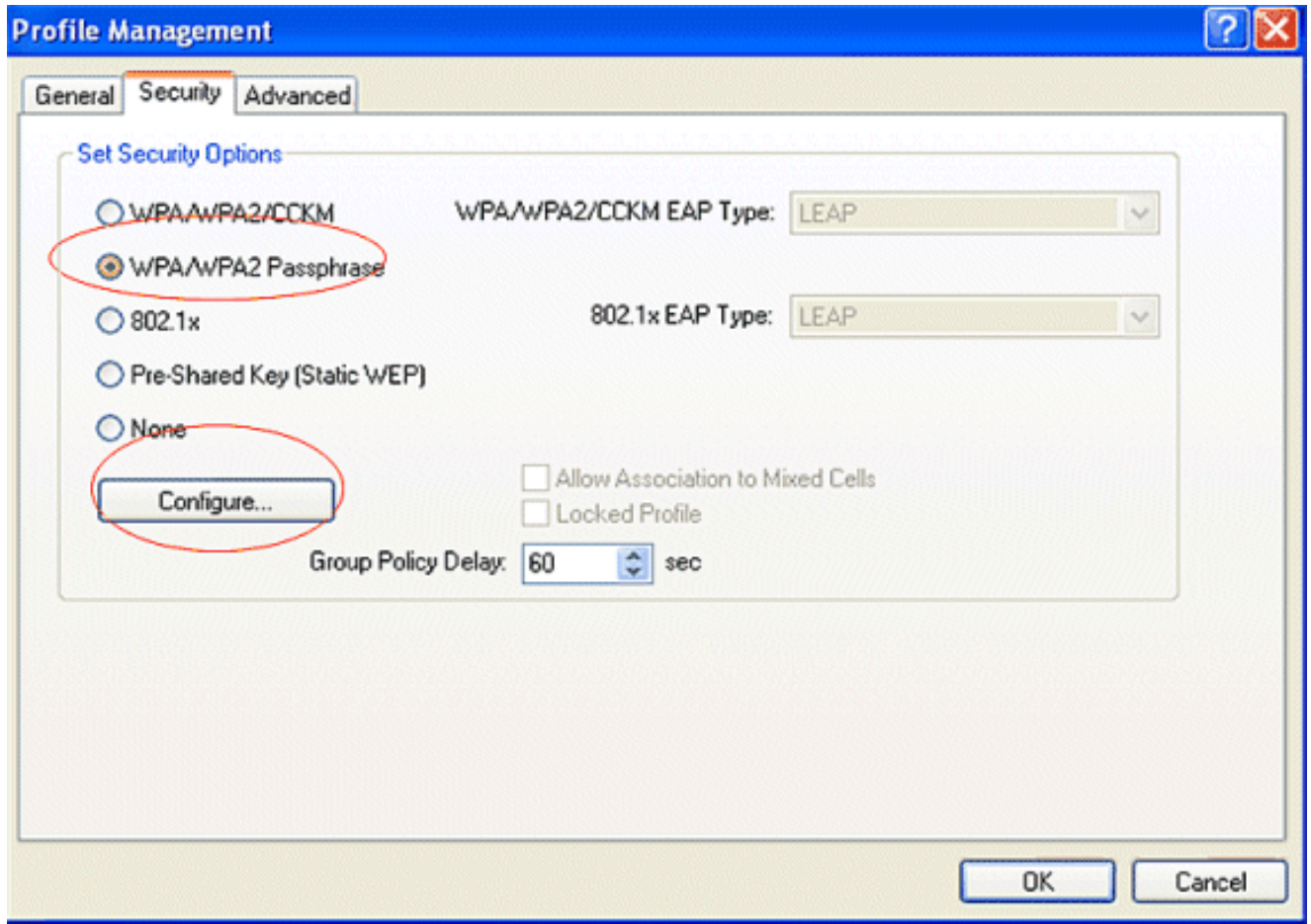
1. 在ADU的Profile Management視窗中，按一下New以建立新的配置檔案。

此時將顯示一個新視窗，您可以在其中設定開放式身份驗證的配置。在General索引標籤下，輸入使用者端配接器使用的Profile Name和SSID。

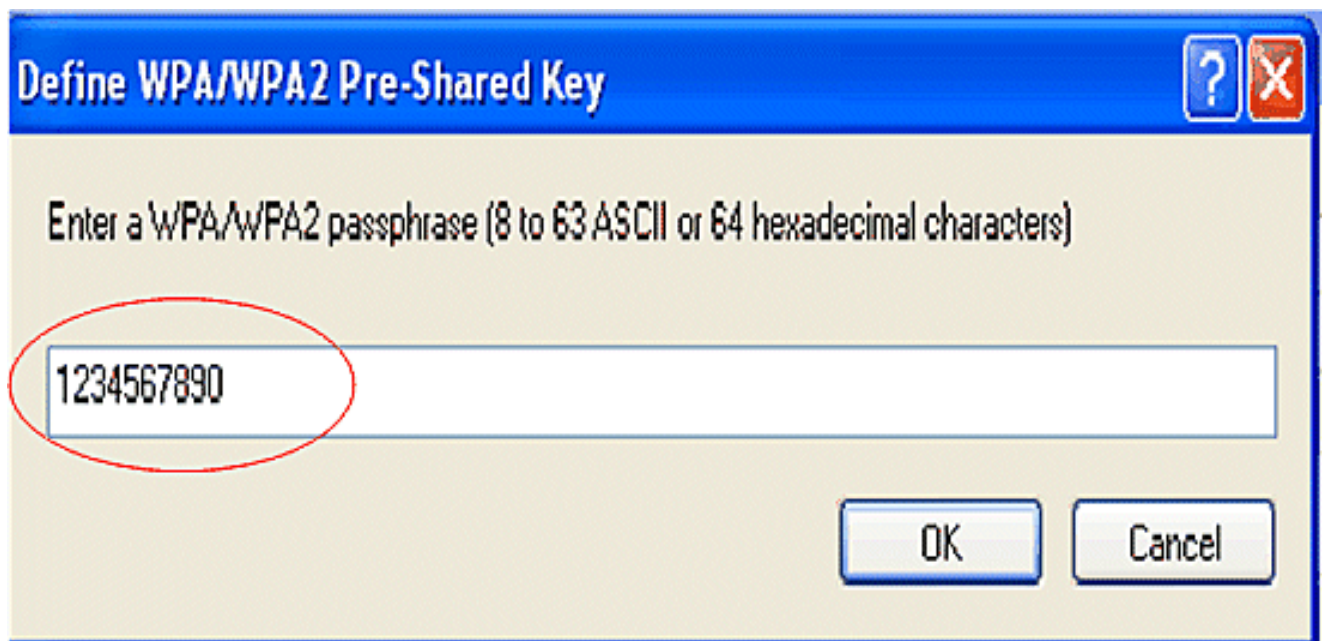
在本示例中，配置檔名稱和SSID是wpa-shared。

註：SSID必須與您在ISR上為WPA-PSK身份驗證配置的SSID匹配。

2. 在Profile Management下，按一下Security頁籤，將安全選項設定為WPA/WPA2密碼。現在，按一下Configure以配置WPA口令。

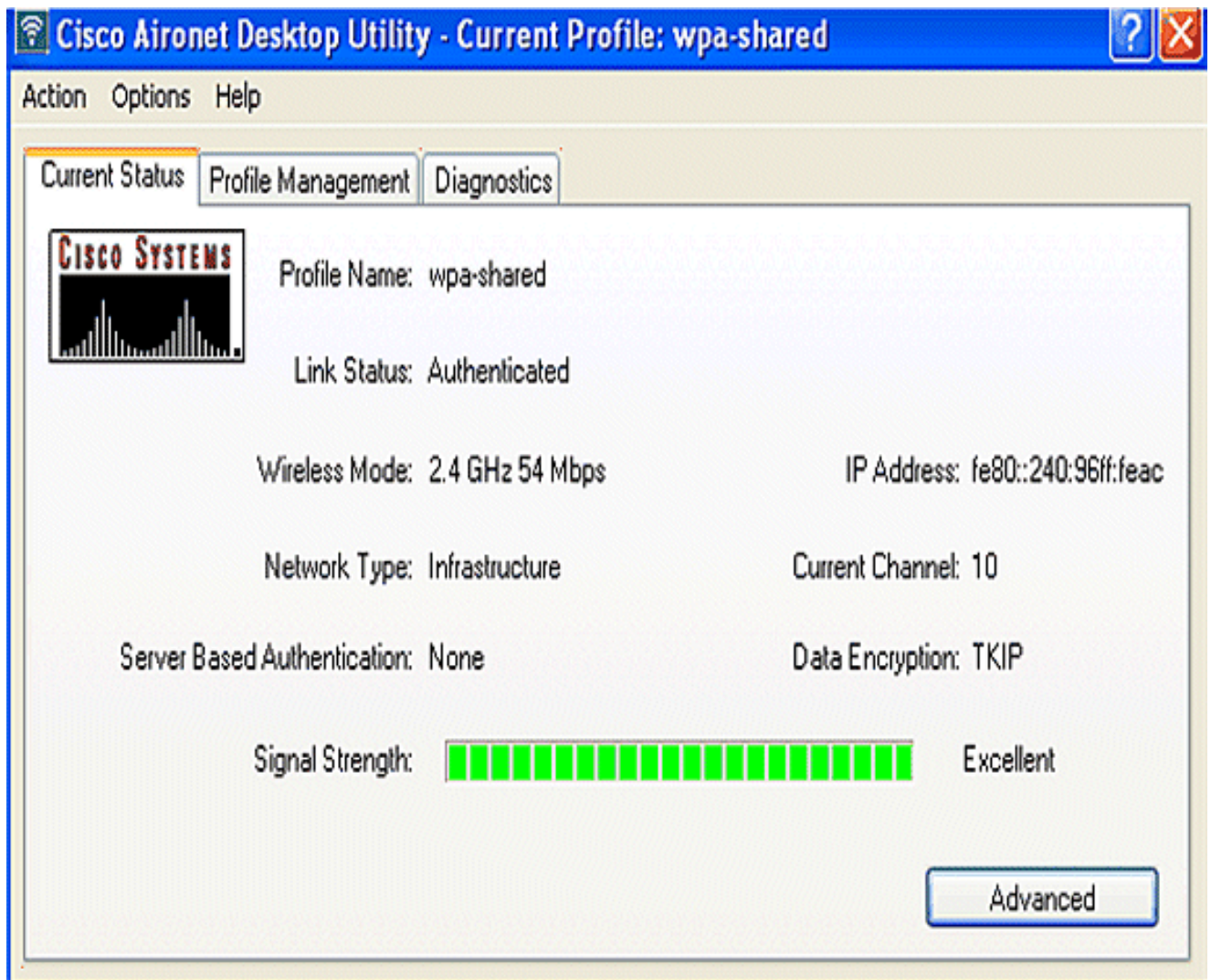


3. 定義WPA預共用金鑰。金鑰長度必須為8到63個ASCII字元。按一下「OK」（確定）。



使用本節內容，確認您的組態是否正常運作。

- 建立客戶端配置檔案後，按一下Profile Management頁籤下的Activate以啟用配置檔案wpa-shared。
- 檢查ADU驗證是否成功。



為WPA (採用EAP) 身份驗證配置無線客戶端

請完成以下步驟：

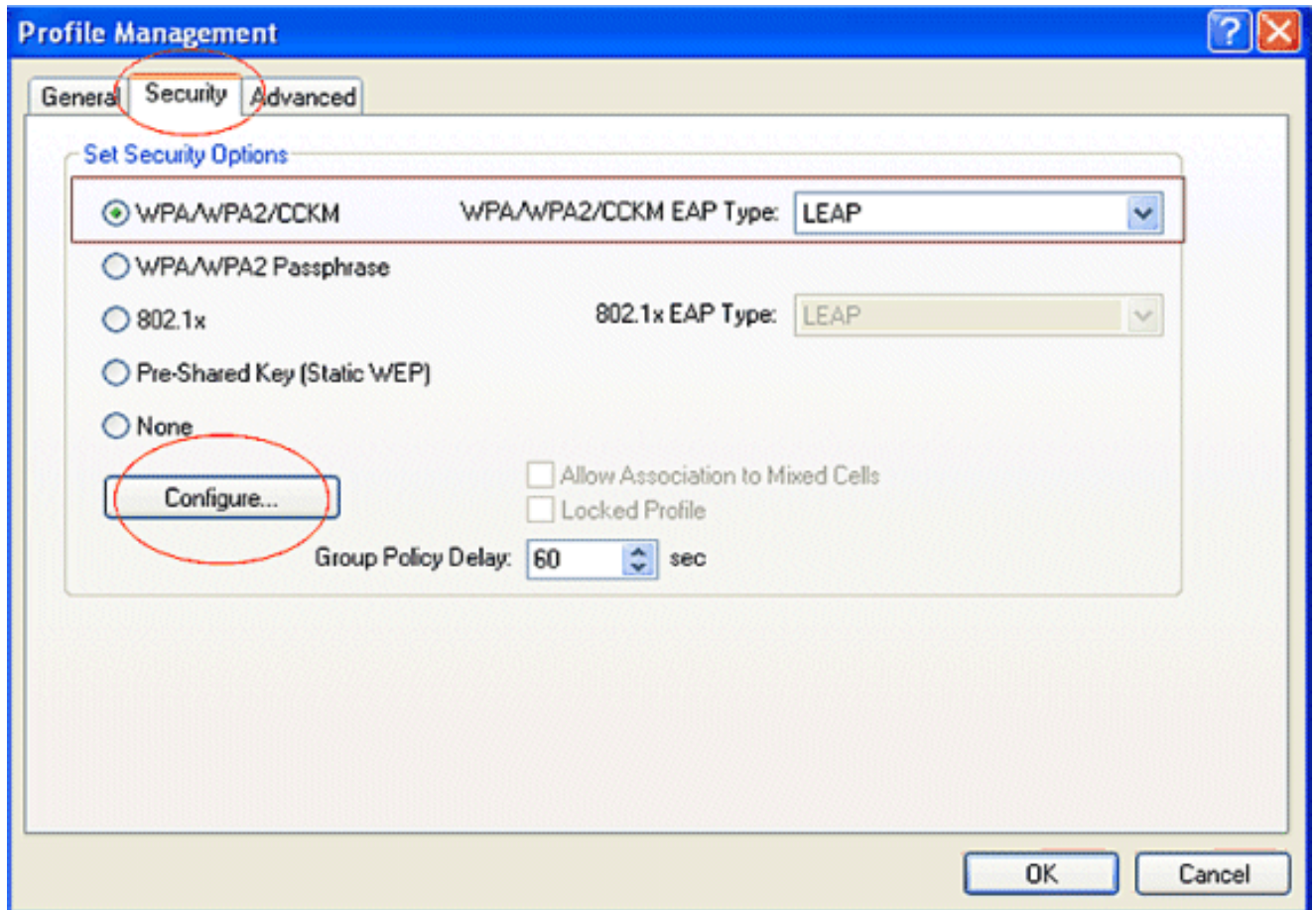
1. 在ADU的Profile Management視窗中，按一下New以建立新的配置檔案。

此時將顯示一個新視窗，您可以在其中設定開放式身份驗證的配置。在General頁籤下，輸入客戶端介面卡使用的配置檔名稱和SSID。

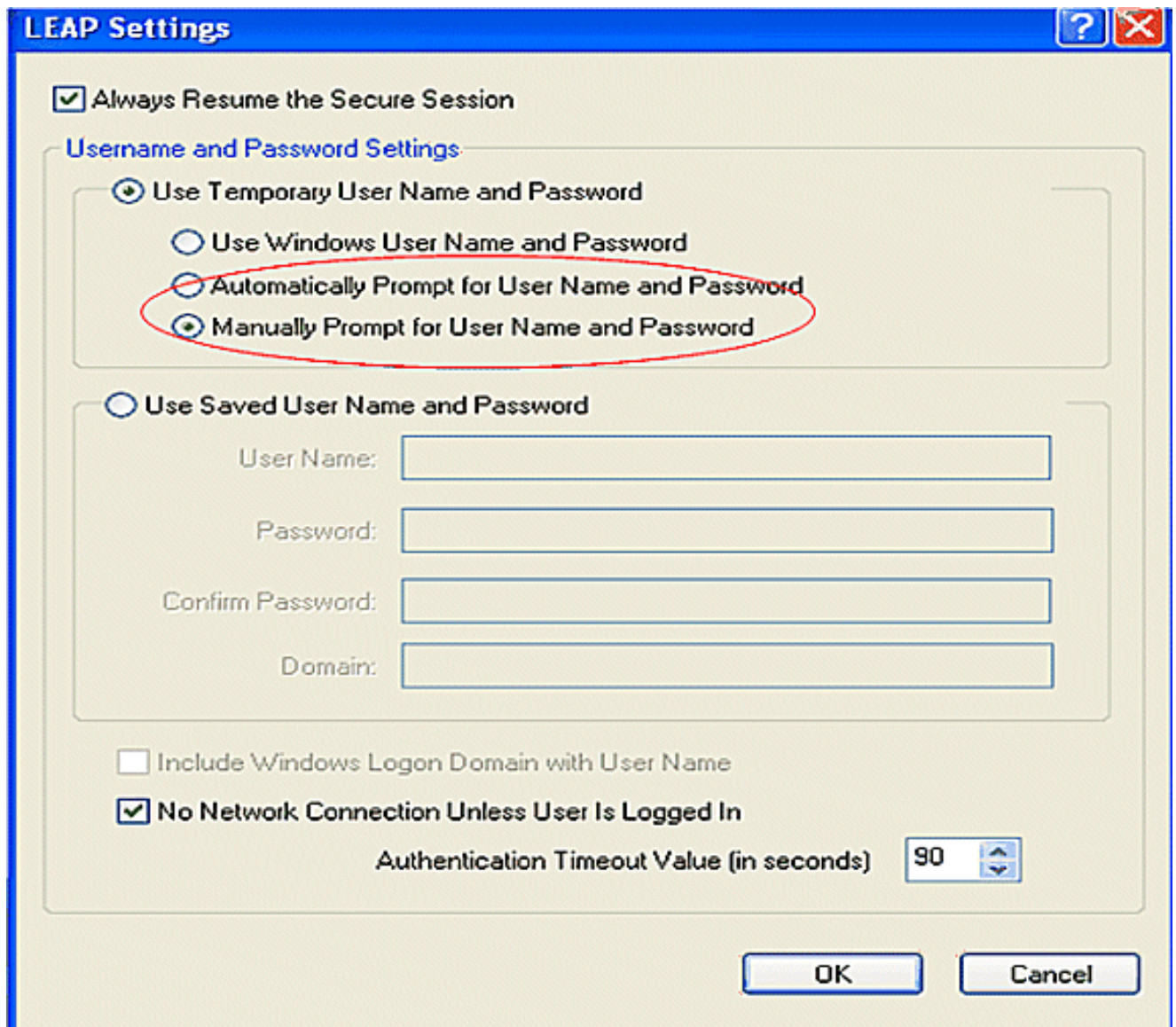
在本示例中，配置檔名稱和SSID是wpa-dot1x。

註：SSID必須與您在ISR上為WPA (使用EAP) 身份驗證配置的SSID匹配。

2. 在Profile Management下，按一下Security頁籤，將安全選項設定為WPA/WPA2/CCKM，然後選擇適當的WPA/WPA2/CCKM EAP型別。本文檔使用LEAP作為EAP型別進行身份驗證。現在，按一下Configure以配置LEAP使用者名稱和密碼設定。



3. 在Username and Password Settings區域下，此示例選擇Manually Prompt for User Name and Password，以便在客戶端嘗試連線到網路時提示客戶端輸入正確的使用者名稱和密碼。按一下「OK」（確定）。



使用本節內容，確認您的組態是否正常運作。

1. 建立客戶端配置檔案後，按一下Profile Management頁籤下的Activate以啟用配置檔案wpa-dot1x。系統將提示您輸入LEAP使用者名稱和密碼。此示例將使用者名稱和密碼用作user1。按一下「OK」（確定）。

Enter Wireless Network Password



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

User Name :

user1

Password :

•••••

Log on to :

Card Name :

Cisco Aironet 802.11 a/b/g Wireless Adapter

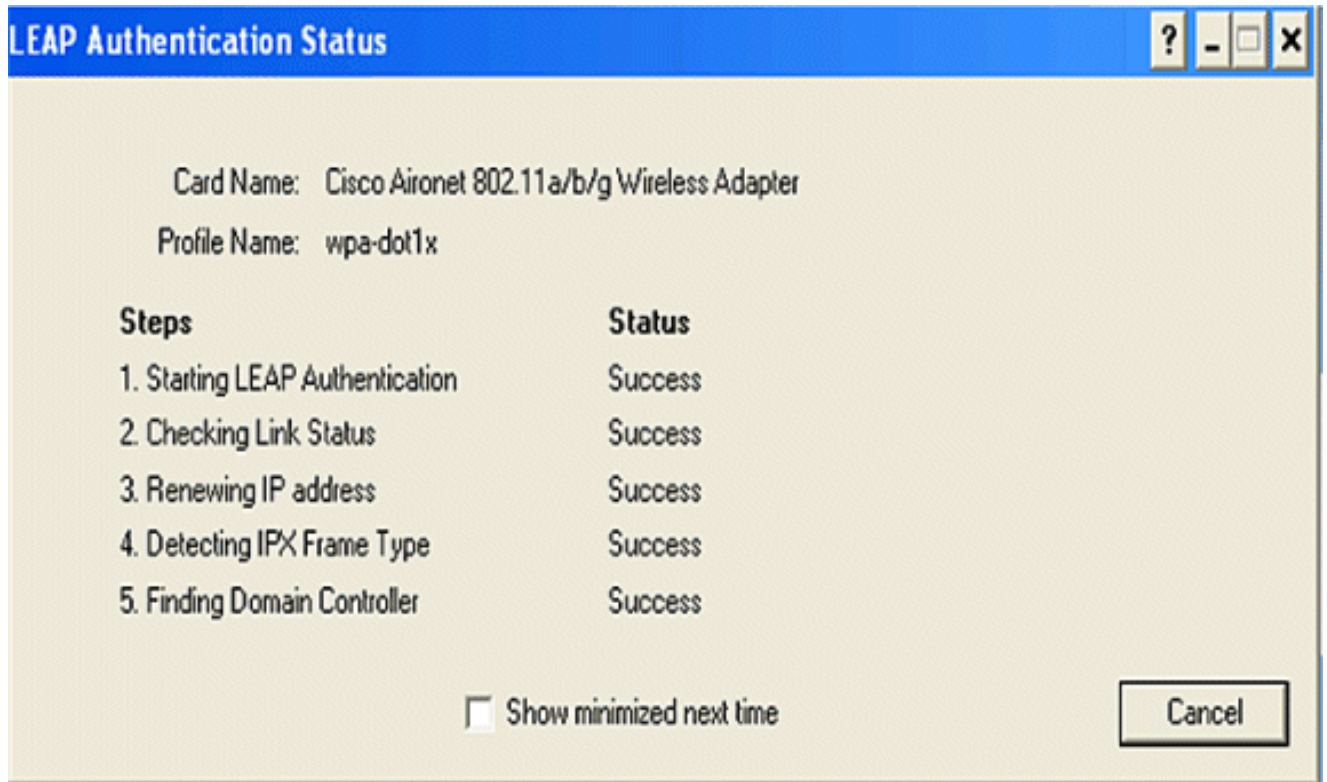
Profile Name :

wpa-dot1x

OK

Cancel

2. 您可以成功觀察使用者端進行驗證。



來自路由器CLI的show dot11 associations命令會顯示有關客戶端關聯狀態的完整詳細資訊。以下提供範例。

```
Router#show dot11 associations
```

```
<#root>
```

```
802.11 Client Stations on Dot11Radio0:
```

```
SSID [leap] :
```

MAC Address	IP address	Device	Name	Parent	State
0040.96ac.e657	10.3.0.2	CB21AG/PI21AG	WCS	self	EAP-Assoc

```
SSID [open] :
```

```
SSID [pre-shared] : DISABLED, not associated with a configured VLAN
```

```
SSID [wpa-dot1x] :
```

```
SSID [wpa-shared] :
```

```
Others: (not related to any ssid)
```

疑難排解

疑難排解指令

您可以使用這些debug指令對組態進行疑難排解。

- debug dot11 aaa authenticator all — 啟用MAC和EAP身份驗證資料包的調試。
- debug radius authentication — 顯示伺服器和客戶端之間的RADIUS協商。
- debug radius local-server packets — 顯示傳送和接收的RADIUS資料包的內容。
- debug radius local-server client — 顯示有關客戶端身份驗證失敗的錯誤消息。

相關資訊

- [無線LAN控制器上的驗證組態範例](#)
- [在接入點上配置VLAN](#)
- [具有內部DHCP和開放式身份驗證的1800 ISR無線路由器配置示例](#)
- [Cisco無線ISR和HWIC接入點配置指南](#)
- [使用帶WEP加密的ISR和LEAP身份驗證的無線區域網連線配置示例](#)
- [技術支援與文件 - Cisco Systems](#)
- [配置身份驗證型別](#)
- [使用帶WEP加密的ISR和LEAP身份驗證的無線區域網連線配置示例](#)

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）。