Configurazione dei tipi di autenticazione wireless su ISR fisso

Sommario

[Informazioni correlate]

Introduzione

Questo documento offre esempi di configurazione che spiegano come configurare vari tipi di autenticazione di layer 2 su un router a configurazione fissa integrato con Cisco Wireless per la connettività wireless con i comandi CLI.

Prerequisiti

Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- Conoscenza di come configurare i parametri di base di Cisco Integrated Services Router (ISR)
- Informazioni su come configurare l'adattatore client wireless 802.11a/b/g con Aironet Desktop Utility (ADU)

Componenti usati

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

- Cisco 877W ISR con software Cisco IOS® versione 12.3(8)YI1
- Notebook con Aironet Desktop Utility versione 3.6
- Scheda client 802.11 a/b/g con firmware versione 3.6

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

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Premesse

I router a configurazione fissa dei servizi integrati Cisco supportano una soluzione LAN wireless sicura, economica e di facile utilizzo che combina mobilità e flessibilità con le funzionalità di classe enterprise richieste dai professionisti delle reti. Con un sistema di gestione basato sul software Cisco IOS, i router Cisco fungono da punti di accesso e sono ricetrasmettitori LAN wireless

conformi allo standard IEEE 802.11a/b/g e certificati Wi-Fi.

È possibile configurare e monitorare i router tramite l'interfaccia della riga di comando (CLI), il sistema di gestione basato su browser o il protocollo SNMP (Simple Network Management Protocol). In questo documento viene descritto come configurare l'ISR per la connettività wireless con i comandi CLI.

Configurazione

Nell'esempio viene mostrato come configurare questi tipi di autenticazione su un router Cisco Wireless Integrated a configurazione fissa con comandi CLI.

- Autenticazione aperta
- Autenticazione 802.1x/EAP (Extensible Authentication Protocol)
- Autenticazione WPA-PSK (Wi-Fi Protected Access Pre-Shared Key)
- Autenticazione WPA (con EAP)

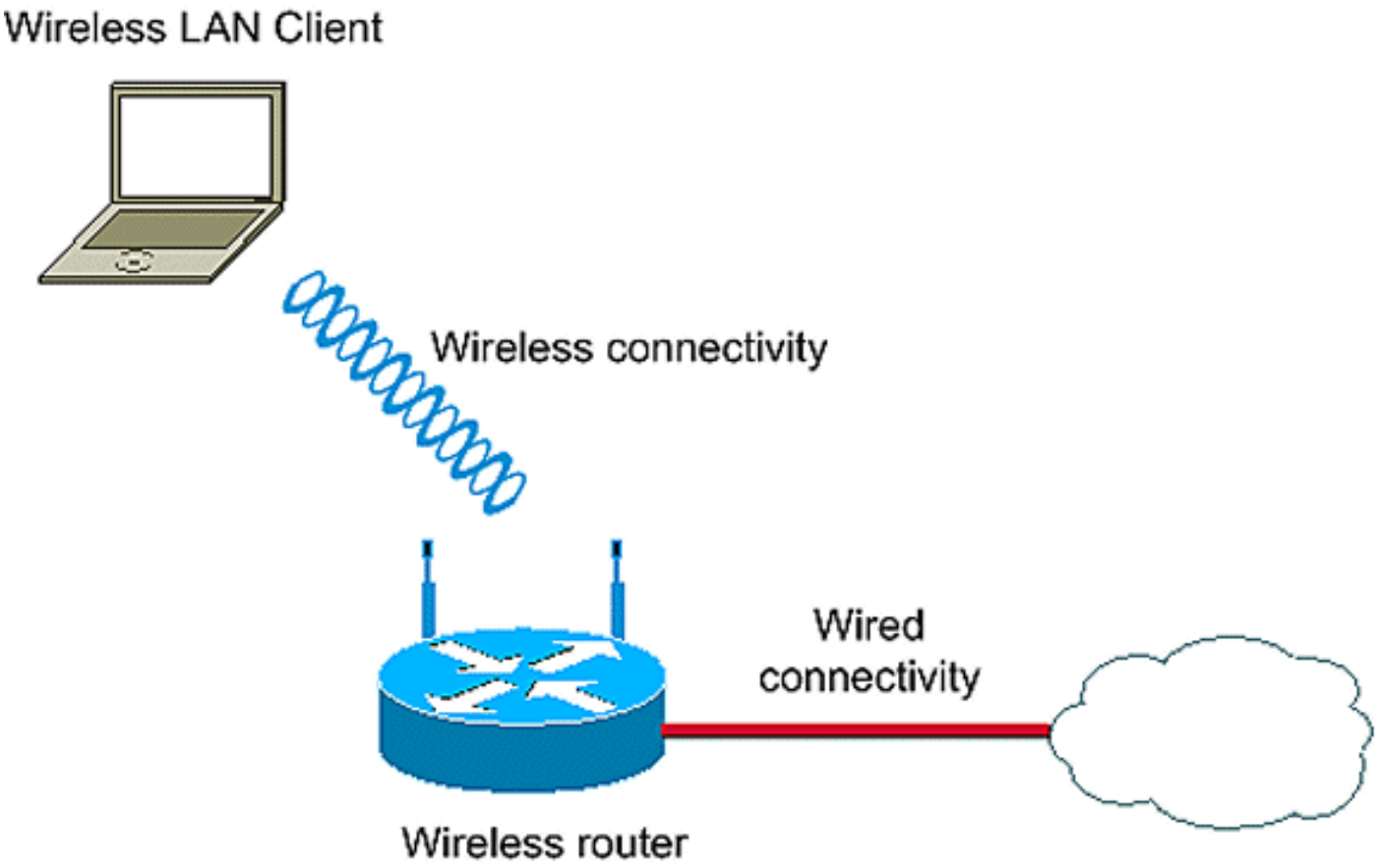
Nota: questo documento non si concentra sull'autenticazione condivisa in quanto si tratta di un tipo di autenticazione meno sicuro.

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Il documento usa la seguente configurazione di rete:



Il programma di installazione utilizza il server RADIUS locale dell'ISR wireless per autenticare i client wireless con l'autenticazione 802.1x.

Configura autenticazione aperta

L'autenticazione aperta è un algoritmo di autenticazione Null. Il punto di accesso concede qualsiasi richiesta di autenticazione. L'autenticazione aperta consente l'accesso alla rete a qualsiasi dispositivo. Se sulla rete non è attivata la crittografia, qualsiasi dispositivo che conosce l'SSID del punto di accesso può accedere alla rete. Se la crittografia WEP è attivata su un punto di accesso, la chiave WEP stessa diventa un mezzo di controllo dell'accesso. Se un dispositivo non dispone della chiave WEP corretta, anche se l'autenticazione ha esito positivo, il dispositivo non è in grado di trasmettere i dati attraverso il punto di accesso. Né può decrittografare i dati inviati dal punto di accesso.

In questo esempio di configurazione viene illustrata una semplice autenticazione aperta. La chiave WEP può essere resa obbligatoria o facoltativa. In questo esempio la chiave WEP viene configurata come facoltativa in modo che qualsiasi dispositivo che non utilizza WEP possa anche eseguire l'autenticazione e l'associazione a questo punto di accesso.

per ulteriori informazioni, fare riferimento a Autenticazione aperta.

In questo esempio viene utilizzata l'impostazione di configurazione per configurare l'autenticazione aperta sull'ISR.

- Nome SSID: "open"

- VLAN 1
- Intervallo server DHCP interno: 10.1.0.0/16

Nota: per semplicità, in questo esempio non viene utilizzata alcuna tecnica di crittografia per i client autenticati.

Completare queste azioni sul router:

1. Configurare l'IRB (Integrated Routing and Bridging) e impostare il gruppo di bridge
2. Configurazione dell'interfaccia virtuale con bridging (BVI)
3. Configurare il SSID per l'autenticazione aperta
4. Configurare il server DHCP interno per i client wireless della VLAN

Configurare l'IRB (Integrated Routing and Bridging) e impostare il gruppo di bridge

Eseguire le azioni seguenti:

1. Abilitare l'IRB nel router.

   router<configure>#bridge irb

   Nota: se tutti i tipi di sicurezza devono essere configurati su un singolo router, è sufficiente abilitare il protocollo IRB solo una volta a livello globale sul router. Non è necessario abilitarla per ogni singolo tipo di autenticazione.

2. Definire un gruppo di bridge.

   In questo esempio viene utilizzato il numero del gruppo di bridge 1.

   router<configure>#bridge 1

3. Scegliere il protocollo Spanning Tree per il gruppo bridge.

   Qui, il protocollo Spanning Tree IEEE è configurato per questo gruppo di bridge.

   router<configure>#bridge 1 protocol ieee

4. Abilitare una BVI ad accettare e indirizzare i pacchetti indirizzabili ricevuti dal suo gruppo di bridge corrispondente.

   In questo esempio, il BVI accetta e instrada il pacchetto IP.

   router<configure>#bridge 1 route ip

Configurazione dell'interfaccia virtuale con bridging (BVI)

Eseguire le azioni seguenti:

1. Configurare la BVI.

   Configurare la BVI quando si assegna il numero corrispondente del gruppo di bridge alla BVI. Ciascun gruppo di bridge può avere solo una BVI corrispondente. In questo esempio viene assegnato il numero di gruppo di bridge 1 al BVI.

   router<configure>#interface BVI <1>

2. Assegnare un indirizzo IP alla BVI.

   router<config-if>#ip address 10.1.1.1 255.255.0.0

   router<config-if>#no shut

Per informazioni dettagliate sul bridging, consultare il documento sulla configurazione del bridging.

Configurare il SSID per l'autenticazione aperta

Eseguire le azioni seguenti:

1. Attiva l'interfaccia radio

   Per abilitare l'interfaccia radio, passare alla modalità di configurazione dell'interfaccia radio DOT11 e assegnare un SSID all'interfaccia.

   router<config>#interface dot11radio0

   router<config-if>#no shutdown

   router<config-if>#ssid open

   È possibile configurare il tipo di autenticazione aperta in combinazione con l'autenticazione dell'indirizzo MAC. In questo caso, il punto di accesso forza tutti i dispositivi client a eseguire l'autenticazione dell'indirizzo MAC prima che possano unirsi alla rete.

   È inoltre possibile configurare l'autenticazione aperta insieme all'autenticazione EAP. Il punto di accesso impone a tutti i dispositivi client di eseguire l'autenticazione EAP prima che possano unirsi alla rete. Specificare l'elenco dei metodi di autenticazione per il nome elenco.

   Un punto di accesso configurato per l'autenticazione EAP impone a tutti i dispositivi client associati di eseguire l'autenticazione EAP. I dispositivi client che non utilizzano EAP non possono utilizzare il punto di accesso.

2. Associare il SSID a una VLAN.

   Per abilitare il SSID su questa interfaccia, associare il SSID alla VLAN in modalità di configurazione SSID.

   router<config-ssid>vlan 1

3. Configurare il SSID con l'autenticazione aperta.

router<config-ssid>#authentication open

4. Configurare l'interfaccia radio per la chiave WEP (facoltativo).

   router<config>#encryption vlan 1 mode WEP facoltativo

5. Abilitare la VLAN sull'interfaccia radio.

   router<config>#interface Dot11Radio 0.1

   router<config-subif>#encapsulation dot1Q 1

   router<config-subif>#bridge-group 1

Configurare il server DHCP interno per i client wireless della VLAN

Digitare questi comandi in modalità di configurazione globale per configurare il server DHCP interno per i client wireless della VLAN:

- indirizzo ip dhcp escluso 10.1.1.1 10.1.1.5
- pool dhcp ip aperto

In modalità di configurazione pool DHCP, digitare i comandi seguenti:

- network 10.1.0.0 255.255.0.0
- default-router 10.1.1.1

Configurazione dell'autenticazione 802.1x/EAP

Questo tipo di autenticazione offre il livello di protezione più elevato per la rete wireless. Grazie al protocollo EAP (Extensible Authentication Protocol) utilizzato per interagire con un server RADIUS compatibile con EAP, il punto di accesso consente a un dispositivo client wireless e al server RADIUS di eseguire l'autenticazione reciproca e di derivare una chiave WEP unicast dinamica. Il server RADIUS invia la chiave WEP al punto di accesso, che la utilizza per tutti i segnali di dati unicast che invia o riceve dal client.

per ulteriori informazioni, fare riferimento a Autenticazione EAP.

In questo esempio viene utilizzata la configurazione seguente:

- Nome SSID: leap
- VLAN 2
- Intervallo server DHCP interno: 10.2.0.0/16

In questo esempio viene utilizzata l'autenticazione LEAP come meccanismo per autenticare il client wireless.

Nota: per configurare EAP-TLS, consultare il documento Cisco Secure ACS for Windows v3.2 With EAP-TLS Machine Authentication (Cisco Secure ACS per Windows v3.2 con autenticazione computer EAP-TLS).

Nota: per configurare PEAP-MS-CHAPv2, consultare il documento sulla configurazione di Cisco Secure ACS per Windows v3.2 con l'autenticazione del computer PEAP-MS-CHAPv2.

Nota: comprendere che tutte le configurazioni di questi tipi EAP implicano principalmente modifiche della configurazione sul lato client e sul lato server di autenticazione. La configurazione del router o del punto di accesso wireless rimane più o meno la stessa per tutti questi tipi di autenticazione.

Nota: come accennato in precedenza, questa installazione utilizza il server RADIUS locale sull'ISR wireless per autenticare i client wireless con l'autenticazione 802.1x.

Completare queste azioni sul router:

1. Configurare l'IRB (Integrated Routing and Bridging) e impostare il gruppo di bridge
2. Configurazione dell'interfaccia virtuale con bridging (BVI)
3. Configurare il server RADIUS locale per l'autenticazione EAP
4. Configurare il SSID per l'autenticazione 802.1x/EAP
5. Configurare il server DHCP interno per i client wireless della VLAN

Configurare l'IRB (Integrated Routing and Bridging) e impostare il gruppo di bridge

Eseguire le azioni seguenti:

1. Abilitare l'IRB nel router.

   router<configure>#bridge irb

   Nota: se tutti i tipi di sicurezza devono essere configurati su un singolo router, è sufficiente abilitare il protocollo IRB solo una volta a livello globale sul router. Non è necessario abilitarla per ogni singolo tipo di autenticazione.

2. Definire un gruppo di bridge.

   In questo esempio viene utilizzato il numero 2 del gruppo di bridge.

   router<configure>#bridge 2

3. Scegliere il protocollo Spanning Tree per il gruppo bridge.

   In questo caso, il protocollo IEEE Spanning Tree è configurato per questo gruppo di bridge.

   router<configure>#bridge 2 protocol ieee

4. Scegliere il protocollo Spanning Tree per il gruppo bridge.

   In questo caso, il protocollo IEEE Spanning Tree è configurato per questo gruppo di bridge.

   router<configure>#bridge 2 protocol ieee

5. Abilitare una BVI per accettare e indirizzare i pacchetti instradabili ricevuti dal gruppo bridge corrispondente.

   In questo esempio il BVI accetta e instrada i pacchetti IP.

   router<configure>#bridge 2 route ip

Configurazione dell'interfaccia virtuale con bridging (BVI)

Eseguire le azioni seguenti:

1. Configurare la BVI.

   Configurare la BVI quando si assegna il numero corrispondente del gruppo di bridge alla BVI. Ogni gruppo di bridge può avere un solo corrispondente BVI. In questo esempio viene assegnato il numero 2 del gruppo di bridge al BVI.

   router<configure>#interface BVI <2>

2. Assegnare un indirizzo IP alla BVI.

   router<config-if>#ip address 10.2.1.1 255.255.0.0

   router<config-if>#no shut

Configurare il server RADIUS locale per l'autenticazione EAP

Come accennato in precedenza, in questo documento viene utilizzato il server RADIUS locale sul router abilitato per il wireless per l'autenticazione EAP.

1. Abilitare il modello di controllo di accesso autenticazione, autorizzazione e accounting (AAA).

   router<configure>#aaa new-model

2. Creare un gruppo di server read-eap per il server RADIUS.

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

3. Creare un elenco di metodi eap_methods che elenchi il metodo di autenticazione utilizzato per autenticare l'utente che ha eseguito l'accesso AAA. Assegnare l'elenco dei metodi a questo gruppo di server.

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

4. Abilitare il router come server di autenticazione locale e accedere alla modalità di configurazione per l'autenticatore.

   router<configure>#radius-server local

5. In modalità di configurazione server Radius, aggiungere il router come client AAA del server di autenticazione locale.

   router<config-radsrv>#nas 10.2.1.1 chiave Cisco

6. Configurare l'utente user1 sul server Radius locale.

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

7. Specificare l'host del server RADIUS.

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

   Nota: questa chiave deve essere uguale a quella specificata nel comando nas in modalità di configurazione radius-server.

Configurare il SSID per l'autenticazione 802.1x/EAP

La configurazione dell'interfaccia radio e del SSID associato per 802.1x/EAP implica la configurazione di vari parametri wireless sul router, tra cui il SSID, la modalità di crittografia e il tipo di autenticazione. In questo esempio viene utilizzato il SSID leap.

1. Attivare l'interfaccia radio.

   Per abilitare l'interfaccia radio, passare alla modalità di configurazione dell'interfaccia radio DOT11 e assegnare un SSID all'interfaccia.

   router<config>#interface dot11radio0

   router<config-if>#no shutdown

   router<config-if>#ssid leap

2. Associare il SSID a una VLAN.

   Per abilitare il SSID su questa interfaccia, associare il SSID alla VLAN in modalità di configurazione SSID.

   router<config-ssid>#vlan 2

3. Configurare il SSID con l'autenticazione 802.1x/LEAP.

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

4. Configurare l'interfaccia radio per la gestione dinamica delle chiavi.

   router<config>#encryption vlan 2 mode ciphers wep40

5. Abilitare la VLAN sull'interfaccia radio.

   router<config>#interface Dot11Radio 0.2

   router<config-subif>#encapsulation dot1Q 2

   router<config-subif>#bridge-group 2

Configurare il server DHCP interno per i client wireless della VLAN

Digitare questi comandi in modalità di configurazione globale per configurare il server DHCP interno per i client wireless della VLAN:

- indirizzo ip dhcp escluso 10.2.1.1 10.2.1.5
- ip dhcp pool leapauth

In modalità di configurazione pool DHCP, digitare i comandi seguenti:

- network 10.2.0.0 255.255.0.0
- default-router 10.2.1.1

Gestione chiavi WPA

L'accesso protetto Wi-Fi è un miglioramento della sicurezza interoperabile basato su standard che aumenta notevolmente il livello di protezione dei dati e il controllo dell'accesso per i sistemi LAN wireless attuali e futuri.

Per ulteriori informazioni, fare riferimento a Gestione chiavi WPA.

La gestione delle chiavi WPA supporta due tipi di gestione reciprocamente esclusivi: WPA-Pre-Sshared key (WPA-PSK) e WPA (con EAP).

Configurazione di WPA-PSK

WPA-PSK viene utilizzato come tipo di gestione delle chiavi in una LAN wireless in cui non è disponibile l'autenticazione basata su 802.1x. In tali reti, è necessario configurare una chiave già condivisa sul punto di accesso. È possibile immettere la chiave precondivisa come caratteri ASCII o esadecimali. Se si immette la chiave come caratteri ASCII, si immette un numero di caratteri compreso tra 8 e 63 e il punto di accesso espande la chiave seguendo il processo descritto in RFC2898 (Password-based Cryptography Standard). Se si immette la chiave come caratteri esadecimali, è necessario immettere 64 caratteri esadecimali.

In questo esempio viene utilizzata la configurazione seguente:

- Nome SSID: wpa-shared
- VLAN 3
- Intervallo server DHCP interno: 10.3.0.0/16

Completare queste azioni sul router:

1. Configurare l'IRB (Integrated Routing and Bridging) e impostare il gruppo di bridge
2. Configurazione dell'interfaccia virtuale con bridging (BVI)
3. Configurare il SSID per l'autenticazione WPA-PSK
4. Configurare il server DHCP interno per i client wireless della VLAN

Configurare l'IRB (Integrated Routing and Bridging) e impostare il gruppo di bridge

Eseguire le azioni seguenti:

1. Abilitare l'IRB nel router.

   router<configure>#bridge irb

   Nota: se tutti i tipi di sicurezza devono essere configurati su un singolo router, è sufficiente abilitare il protocollo IRB solo una volta a livello globale sul router. Non è necessario abilitarla per ogni singolo tipo di autenticazione.

2. Definire un gruppo di bridge.

   In questo esempio viene utilizzato il numero 3 del gruppo di bridge.

   router<configure>#bridge 3

3. Scegliere il protocollo Spanning Tree per il gruppo bridge.

   Il protocollo Spanning Tree IEEE è configurato per questo gruppo di bridge.

   router<configure>#bridge 3 protocol ieee

4. Abilitare una BVI ad accettare e indirizzare i pacchetti indirizzabili ricevuti dal suo gruppo di bridge corrispondente.

   In questo esempio il BVI accetta e instrada i pacchetti IP.

   router<configure>#bridge 3 route ip

Configurazione dell'interfaccia virtuale con bridging (BVI)

Eseguire le azioni seguenti:

1. Configurare la BVI.

   Configurare la BVI quando si assegna il numero corrispondente del gruppo di bridge alla BVI. Ogni gruppo di bridge può avere un solo corrispondente BVI. In questo esempio viene assegnato il numero 3 del gruppo di bridge al BVI.

   router<configure>#interface BVI <2>

2. Assegnare un indirizzo IP alla BVI.

   router<config-if>#ip address 10.3.1.1 255.255.0.0

   router<config-if>#no shut

Configurare il SSID per l'autenticazione WPA-PSK

Eseguire le azioni seguenti:

1. Attivare l'interfaccia radio.

   Per abilitare l'interfaccia radio, passare alla modalità di configurazione dell'interfaccia radio DOT11 e assegnare un SSID all'interfaccia.

   router<config>#interface dot11radio0

   router<config-if>#no shutdown

   router<config-if>#ssid wpa-shared

2. Per abilitare la gestione delle chiavi WPA, configurare innanzitutto la crittografia WPA per l'interfaccia VLAN. In questo esempio viene utilizzato tkip come cifratura di crittografia..

   Digitare questo comando per specificare il tipo di gestione delle chiavi WPA sull'interfaccia radio.

   router<config>#interface dot11radio0

   router(config-if)#encryption vlan modalità 3 tkip

3. Associare il SSID a una VLAN.

   Per abilitare il SSID su questa interfaccia, associare il SSID alla VLAN in modalità di configurazione SSID.

   router<config-ssid>vlan 3

4. Configurare il SSID con l'autenticazione WPA-PSK.

   Per abilitare la gestione delle chiavi WPA, è necessario configurare prima l'autenticazione EAP aperta o di rete in modalità di configurazione SSID. In questo esempio viene configurata l'autenticazione aperta.

router<config>#interface dot11radio0

router<config-if>#ssid wpa-shared

router<config-ssid>#authentication open

Abilitare ora la gestione delle chiavi WPA sull'SSID. La cifratura di gestione delle chiavi è già configurata per questa VLAN.

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

Configurare l'autenticazione WPA-PSK sul SSID.

router(config-if-ssid)#wpa-psk ascii 1234567890 !— 1234567890 è il valore della chiave precondivisa per questo SSID. Verificare che per questo SSID sia specificata la stessa chiave sul lato client.

5. Abilitare la VLAN sull'interfaccia radio.

   router<config>#interface Dot11Radio 0.3

   router<config-subif>#encapsulation dot1Q 3

   router<config-subif>#bridge-group 3

Configurare il server DHCP interno per i client wireless della VLAN

Digitare questi comandi in modalità di configurazione globale per configurare il server DHCP interno per i client wireless della VLAN:

- indirizzo ip dhcp escluso 10.3.1.1 10.3.1.5
- pool dhcp ip wpa-psk

In modalità di configurazione pool DHCP, digitare i comandi seguenti:

- network 10.3.0.0 255.255.0.0
- default-router 10.3.1.1

Configurazione dell'autenticazione WPA (con EAP)

Si tratta di un altro tipo di gestione delle chiavi WPA. In questo caso, i client e il server di autenticazione si autenticano reciprocamente tramite un metodo di autenticazione EAP e il client e il server generano una chiave master pairwise (PMK). Con WPA, il server genera la chiave PMK in modo dinamico e la passa al punto di accesso, ma con WPA-PSK si configura una chiave già condivisa sia sul client che sul punto di accesso e tale chiave viene utilizzata come chiave PMK.

per ulteriori informazioni, fare riferimento a WPA con autenticazione EAP.

In questo esempio viene utilizzata la configurazione seguente:

- Nome SSID: wpa-dot1x
- VLAN 4
- Intervallo server DHCP interno: 10.4.0.0/16

Completare queste azioni sul router:

1. Configurare l'IRB (Integrated Routing and Bridging) e impostare il gruppo di bridge
2. Configurazione dell'interfaccia virtuale con bridging (BVI)
3. Configurare il server RADIUS locale per l'autenticazione WPA.
4. Configurare il SSID per WPA con autenticazione EAP
5. Configurare il server DHCP interno per i client wireless della VLAN

Configurare l'IRB (Integrated Routing and Bridging) e impostare il gruppo di bridge

Eseguire le azioni seguenti:

1. Abilitare l'IRB nel router.

   router<configure>#bridge irb

   Nota: se tutti i tipi di sicurezza devono essere configurati su un singolo router, è sufficiente abilitare il protocollo IRB solo una volta a livello globale sul router. Non è necessario abilitarla per ogni singolo tipo di autenticazione.

2. Definite un gruppo Bridge.

   In questo esempio viene utilizzato il numero 4 del gruppo di bridge.

   router<configure>#bridge 4

3. Selezionare il protocollo Spanning Tree per il gruppo bridge.

   In questo caso, il protocollo IEEE Spanning Tree è configurato per questo gruppo di bridge.

   router<configure>#bridge 4 protocol ieee

4. Abilitare una BVI ad accettare e indirizzare i pacchetti instradabili ricevuti dal suo gruppo di bridge corrispondente.

   In questo esempio il BVI accetta e instrada i pacchetti IP.

   router<configure>#bridge 4 route ip

Configurazione dell'interfaccia virtuale con bridging (BVI)

Eseguire le azioni seguenti:

1. Configurare la BVI.

   Configurare la BVI quando si assegna il numero corrispondente del gruppo di bridge alla BVI. Ciascun gruppo di bridge può avere solo una BVI corrispondente. In questo esempio viene assegnato il numero 4 del gruppo di bridge al BVI.

   router<configure>#interface BVI <4>

2. Assegnare un indirizzo IP alla BVI.

   router<config-if>#ip address 10.4.1.1 255.255.0.0

   router<config-if>#no shut

Configurare il server RADIUS locale per l'autenticazione WPA

Per la procedura dettagliata, consultare la sezione in Autenticazione 802.1x/EAP.

Configurare il SSID per WPA con autenticazione EAP

Eseguire le azioni seguenti:

1. Attivare l'interfaccia Radio.

   Per abilitare l'interfaccia radio, passare alla modalità di configurazione dell'interfaccia radio DOT11 e assegnare un SSID all'interfaccia.

   router<config>#interface dot11radio0

   router<config-if>#no shutdown

   router<config-if>#ssid wpa-dot1x

2. Per abilitare la gestione delle chiavi WPA, configurare innanzitutto la crittografia WPA per l'interfaccia VLAN. In questo esempio viene utilizzato tkip come cifratura di crittografia..

   Digitare questo comando per specificare il tipo di gestione delle chiavi WPA sull'interfaccia radio.

   router<config>#interface dot11radio0

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

3. Associare il SSID a una VLAN.

   Per abilitare il SSID su questa interfaccia, associare il SSID alla VLAN nella modalità di

configurazione SSID.

vlan 4

4. Configurare il SSID con l'autenticazione WPA-PSK.

   Per configurare l'interfaccia radio per WPA con autenticazione EAP, configurare innanzitutto l'SSID associato per la rete EAP.

   router<config>#interface dot11radio0

   router<config-if>#ssid wpa-shared

   router<config-ssid>#authentication network eap eap_methods

5. Abilitare ora la gestione delle chiavi WPA sull'SSID. La cifratura di gestione delle chiavi è già configurata per questa VLAN.

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

6. Abilitare la VLAN sull'interfaccia radio.

   router<config>#interface Dot11Radio 0.4

   router<config-subif>#encapsulation dot1Q 4

   router<config-subif>#bridge-group 4

Configurare il server DHCP interno per i client wireless della VLAN

Digitare questi comandi in modalità di configurazione globale per configurare il server DHCP interno per i client wireless della VLAN:

- indirizzo ip dhcp escluso 10.4.1.1 10.4.1.5
- pool dhcp ip wpa-dot1shared

In modalità di configurazione pool DHCP, digitare i comandi seguenti:

- network 10.4.0.0 255.255.0.0
- default-router 10.4.1.1

Configura client wireless per l'autenticazione

Dopo aver configurato l'ISR, configurare il client wireless per diversi tipi di autenticazione come spiegato in modo che il router possa autenticare i client wireless e fornire accesso alla rete WLAN. In questo documento viene usata Cisco Aironet Desktop Utility (ADU) per la configurazione sul lato client.

Configurazione del client wireless per l'autenticazione aperta

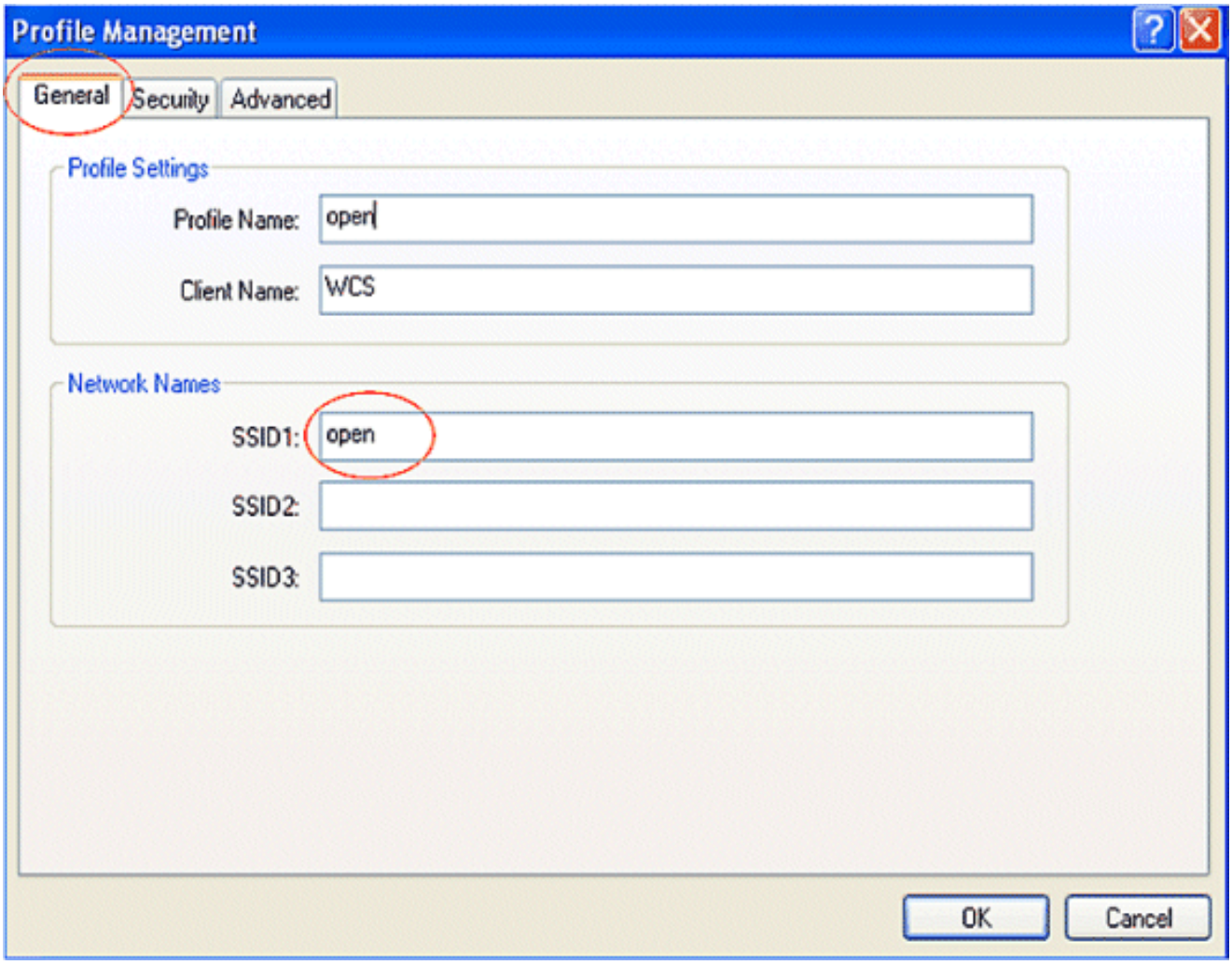
Attenersi alla seguente procedura:

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 l'autenticazione aperta. Nella scheda General (Generale), immettere il Nome profilo e l'SSID utilizzati dall'adattatore client.

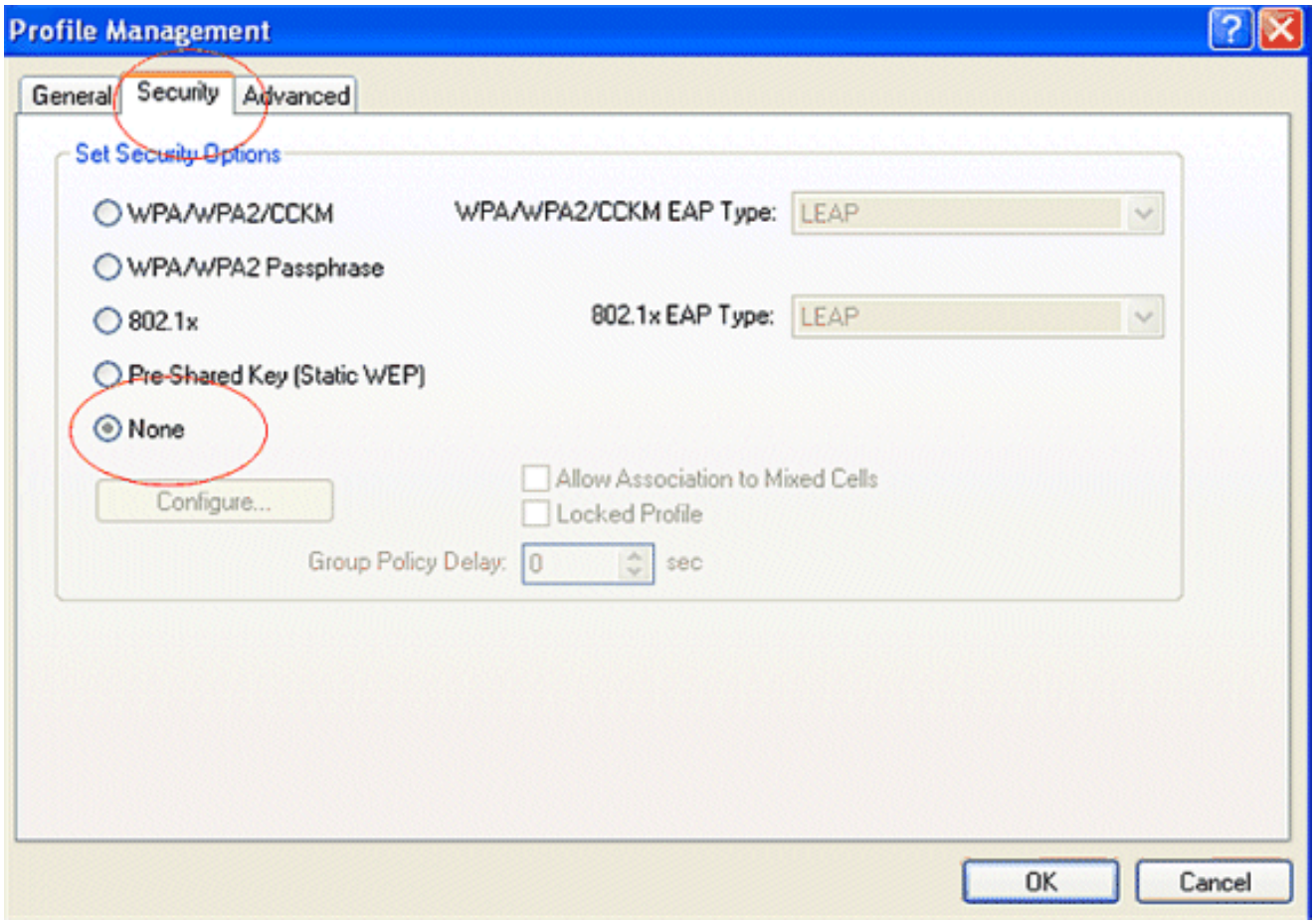
   In questo esempio, il nome del profilo e il SSID sono aperti.

   Nota: il SSID deve corrispondere al SSID configurato nell'ISR per l'autenticazione aperta.

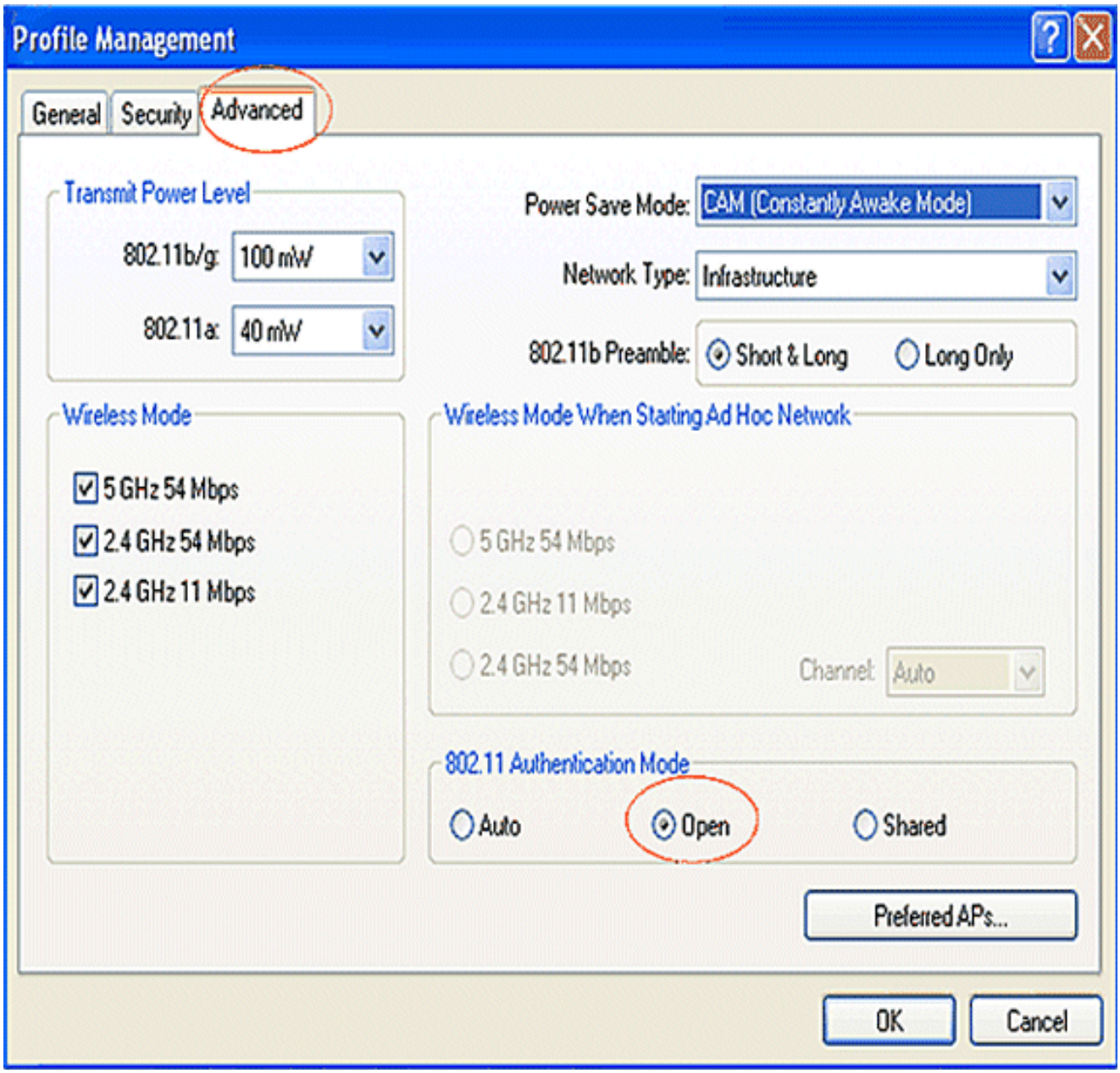


2. Fare clic sulla scheda Protezione e lasciare l'opzione di protezione Nessuna per la crittografia WEP. Poiché in questo esempio WEP viene utilizzato come opzione facoltativa, impostando questa opzione su None il client sarà in grado di associarsi e comunicare con la rete WLAN.

   Fare clic su OK.

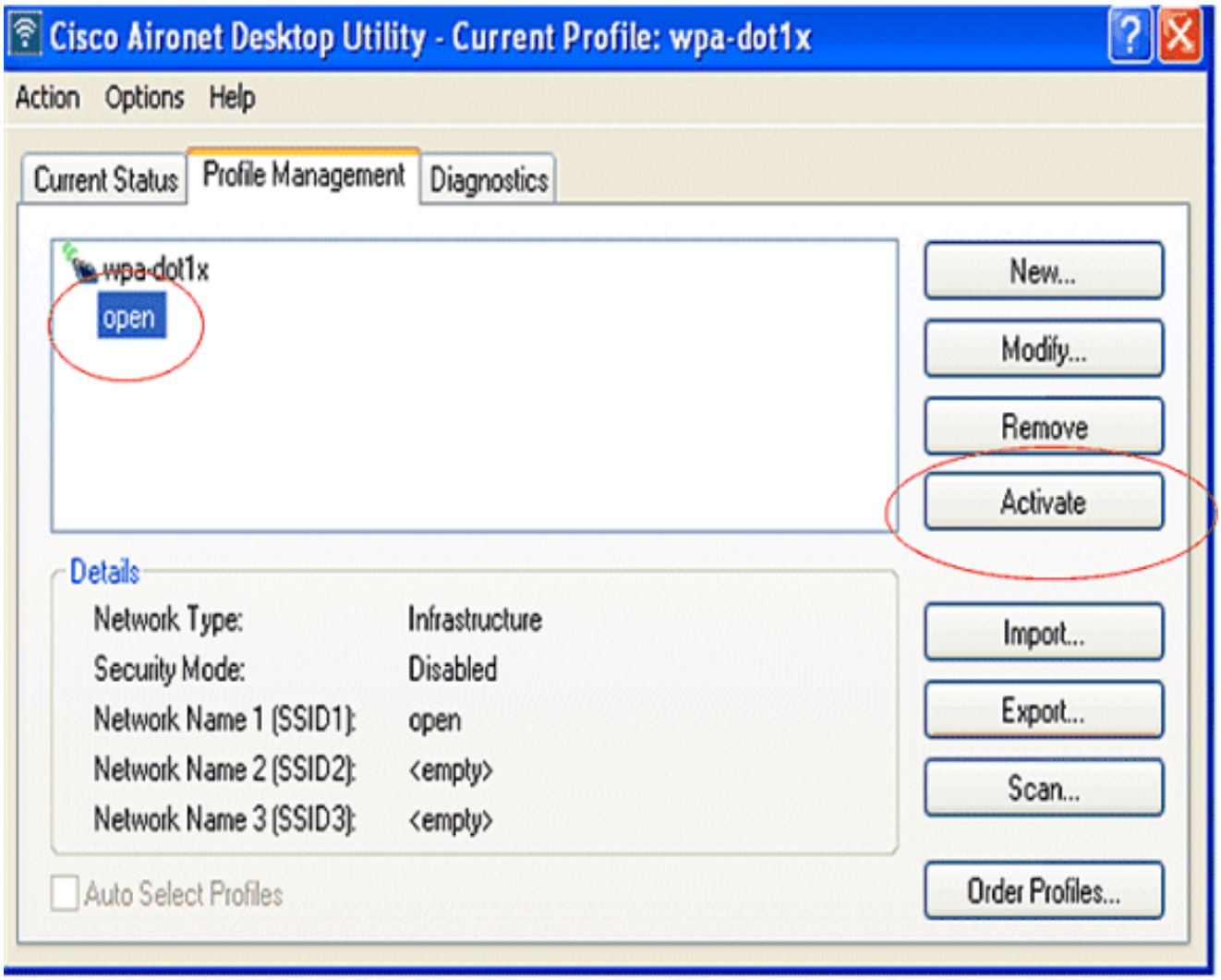


3. Selezionare Advanced window (Avanzate) dalla scheda Profile Management (Gestione profili) e impostare 802.11 Authentication Mode (Modalità di autenticazione 802.11) su Open (Apri) per l'autenticazione aperta.

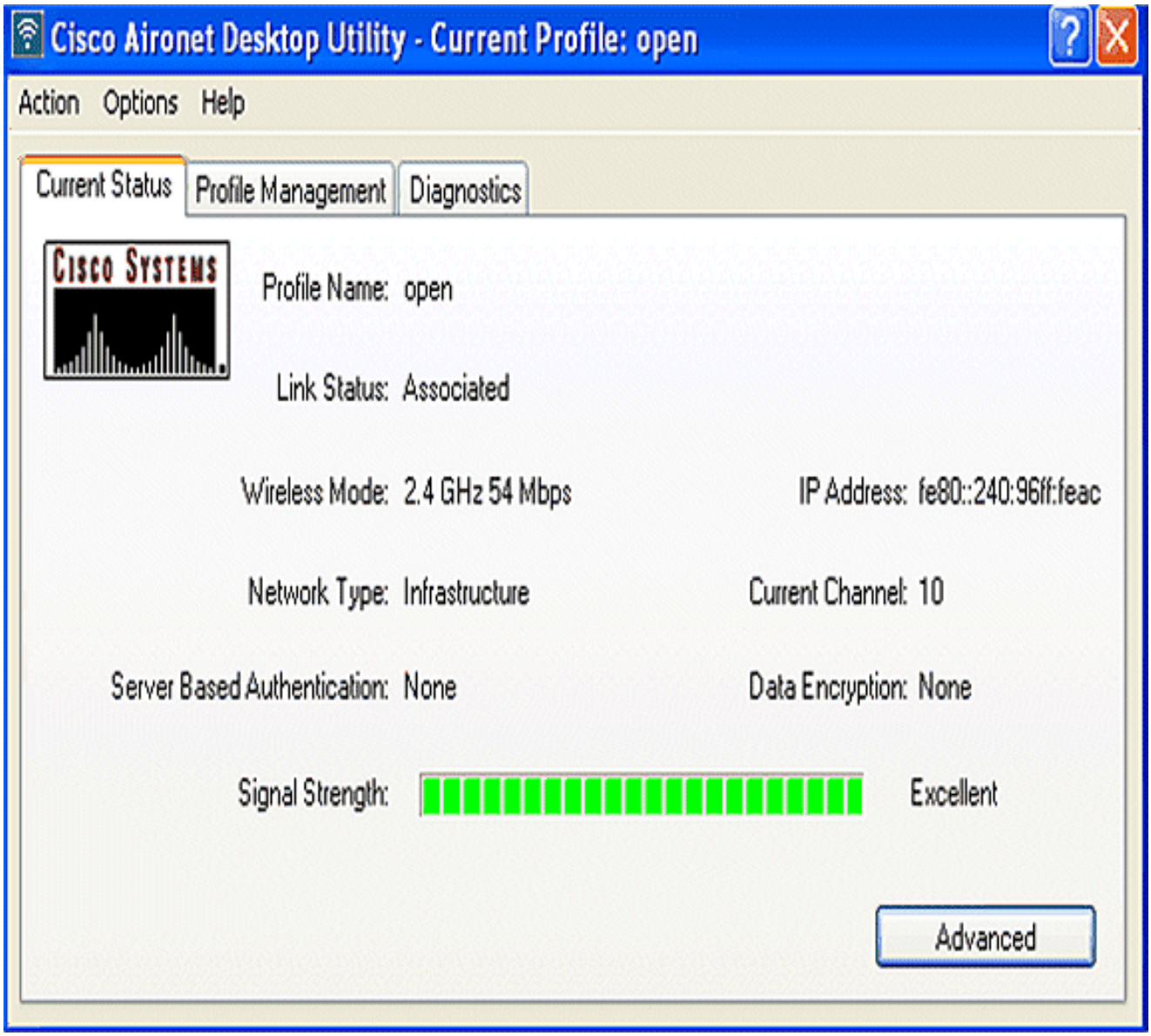


Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

1. Una volta creato il profilo client, fare clic su Attiva nella scheda Gestione profili per attivarlo.



2. Verificare lo stato ADU per un'autenticazione riuscita.



Configurazione del client wireless per l'autenticazione 802.1x/EAP

Attenersi alla seguente procedura:

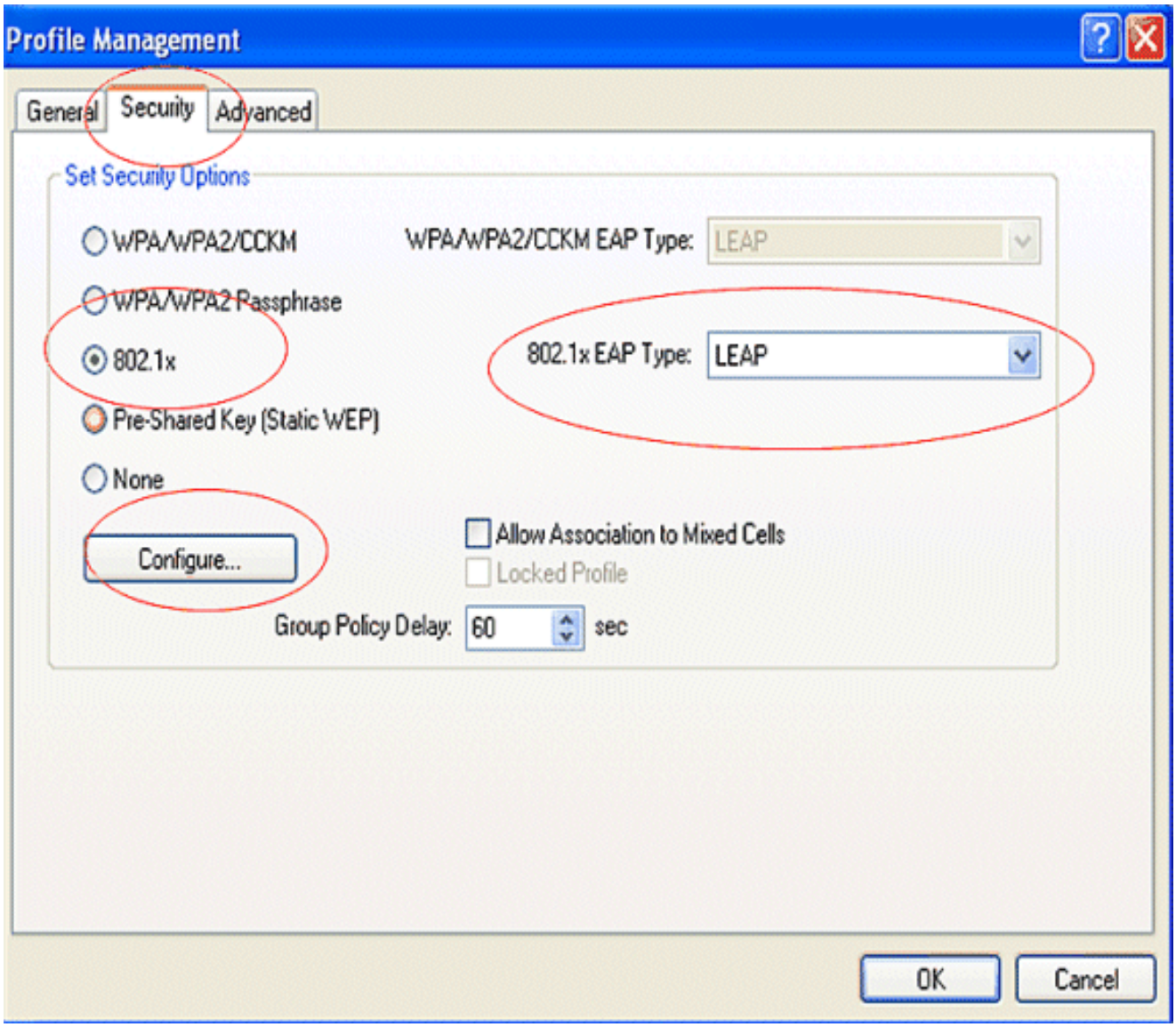
1. Nella finestra Gestione profili dell'ADU, fare clic su Nuovo per creare un nuovo profilo.

   Viene visualizzata una nuova finestra in cui è possibile impostare la configurazione per l'autenticazione aperta. Nella scheda General (Generale), immettere il Nome profilo e l'SSID utilizzati dall'adattatore client.

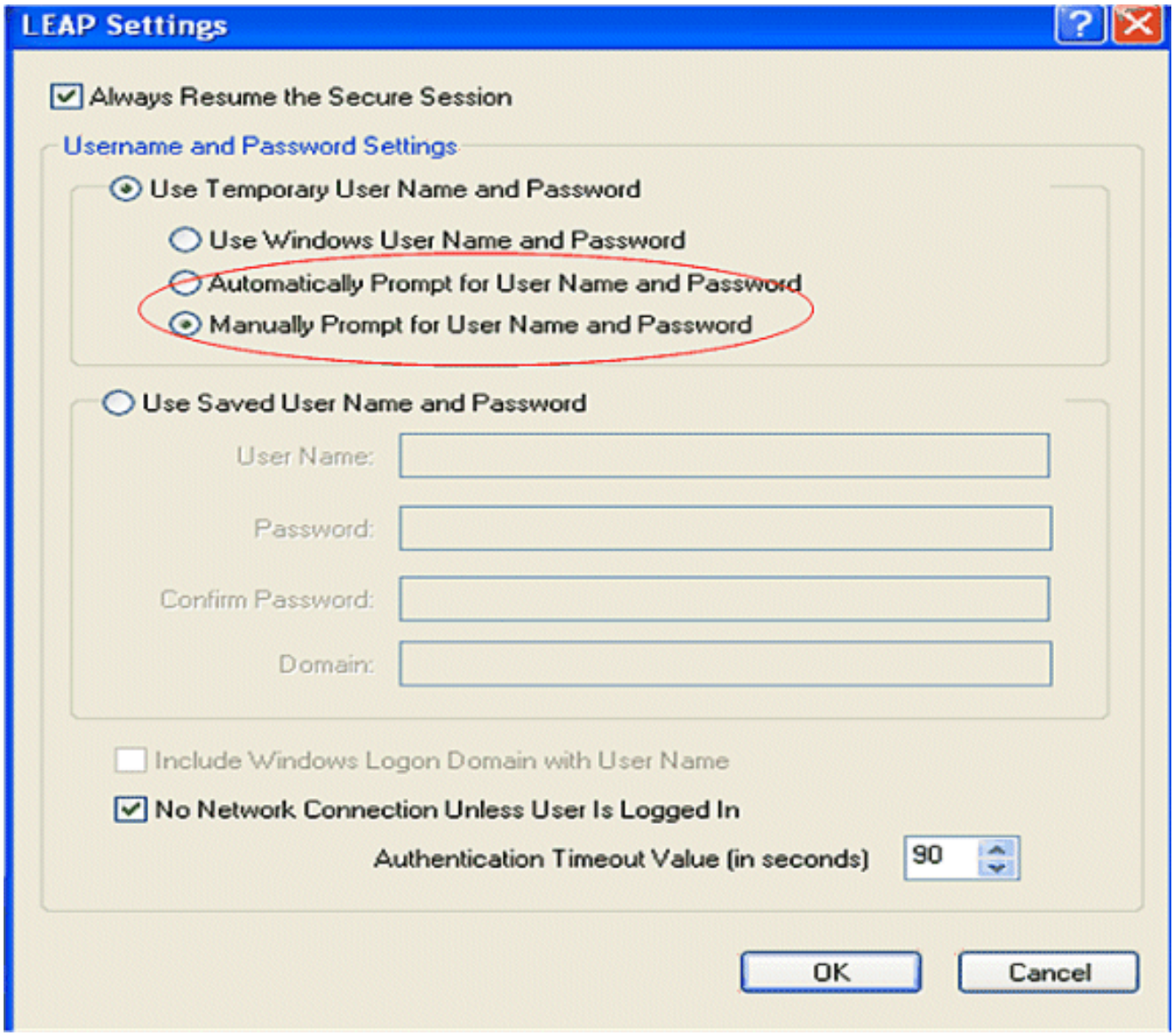
   In questo esempio, il nome del profilo e l'SSID sono leap.

2. In Gestione profili, fare clic sulla scheda Protezione, impostare l'opzione di protezione su 802.1x e scegliere il tipo EAP appropriato. Nel documento viene usato il tipo LEAP per l'autenticazione. A questo punto, fare clic su Configure (Configura) per configurare le impostazioni di nome utente e password LEAP.

   Nota: il SSID deve corrispondere al SSID configurato sull'ISR per l'autenticazione 802.1x/EAP.

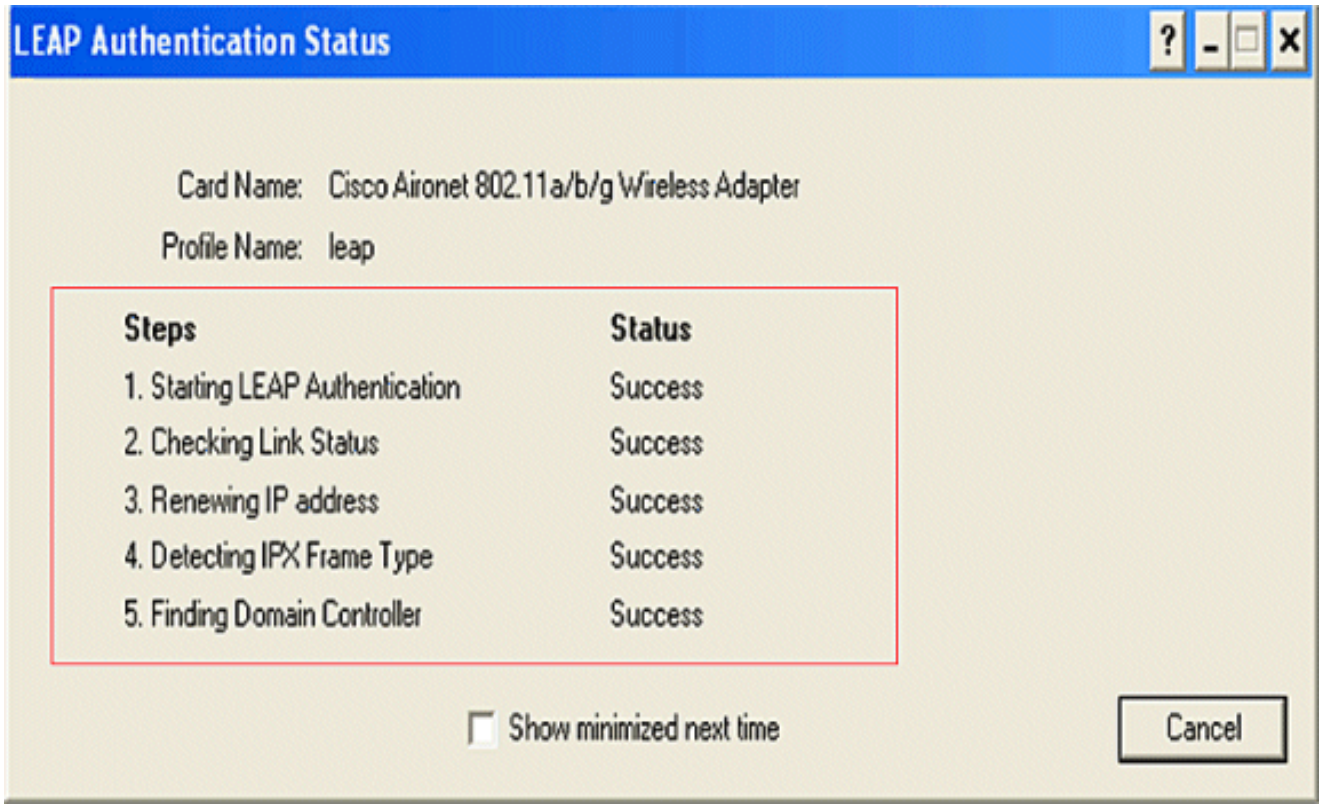


3. In Impostazioni nome utente e password, in questo esempio viene scelto di richiedere manualmente il nome utente e la password in modo che venga richiesto al client di immettere il nome utente e la password corretti durante il tentativo di connessione alla rete. Fare clic su OK.



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

- Una volta creato il profilo client, fare clic su Attiva nella scheda Gestione profili per attivare il salto del profilo. Vengono richiesti il nome utente e la password leap. In questo esempio vengono utilizzati il nome utente e la password user1. Fare clic su OK.
- È possibile controllare l'autenticazione del client e ottenere un indirizzo IP dal server DHCP configurato sul router.



Configurazione del client wireless per l'autenticazione WPA-PSK

Attenersi alla seguente procedura:

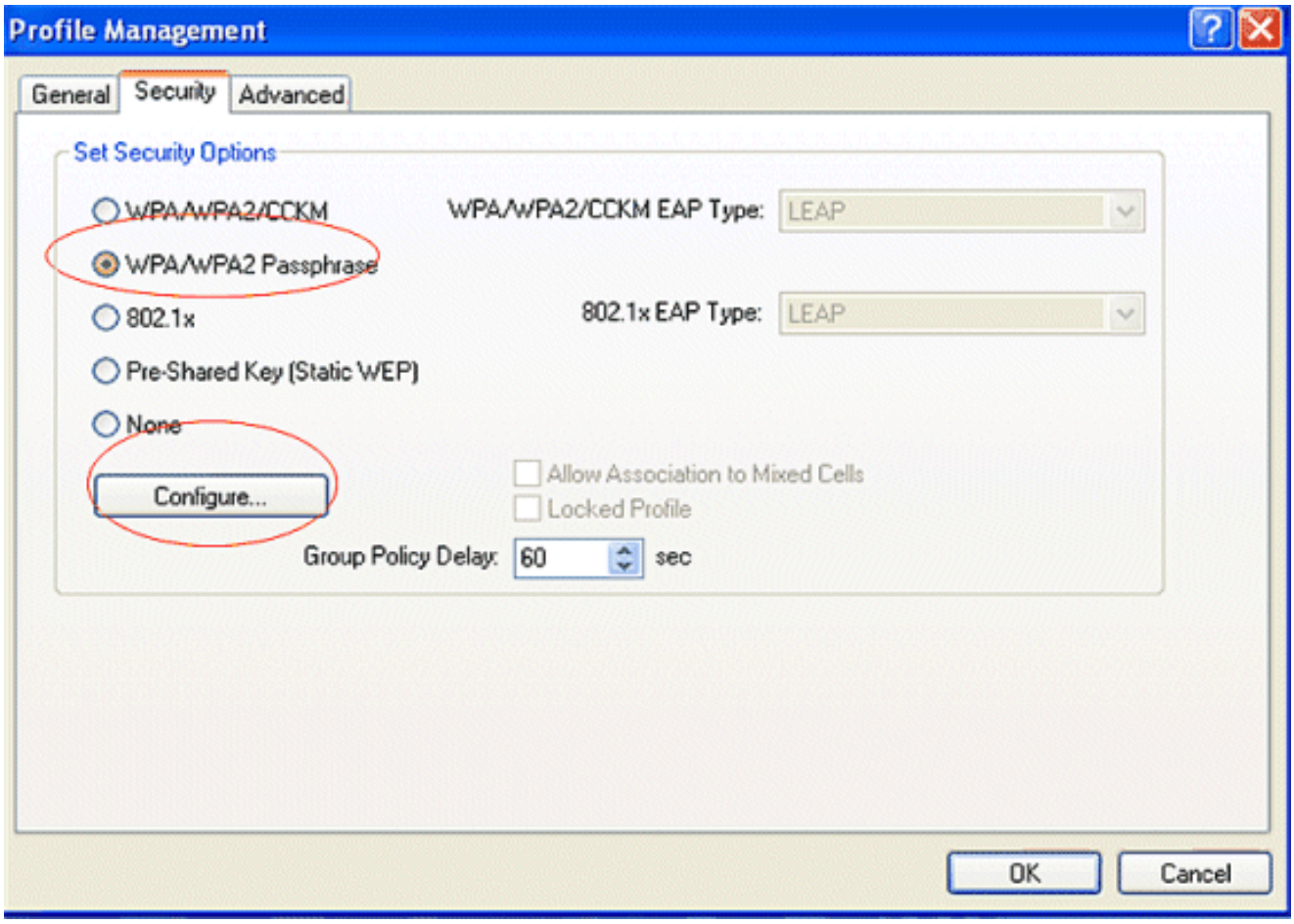
1. Nella finestra Gestione profili dell'ADU, fare clic su Nuovo per creare un nuovo profilo.

   Viene visualizzata una nuova finestra in cui è possibile impostare la configurazione per l'autenticazione aperta. Nella scheda Generale, immettere il Nome profilo e l'SSID utilizzati dall'adattatore client.

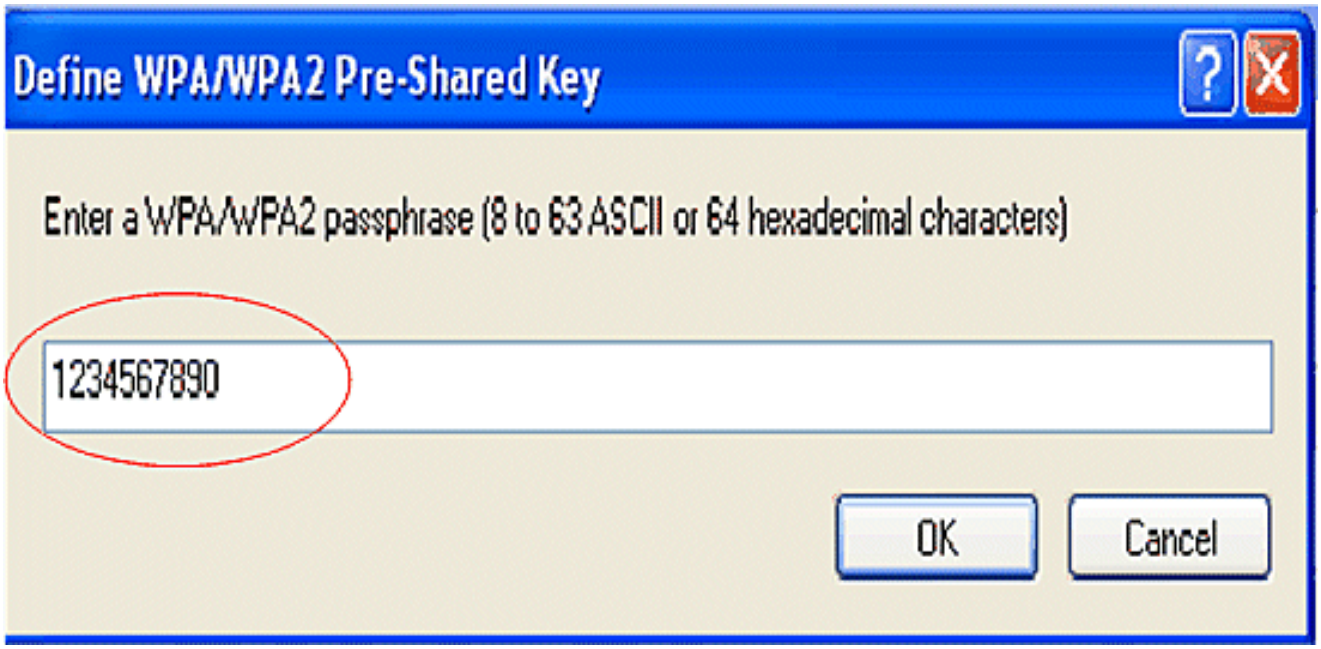
   In questo esempio, il nome del profilo e il SSID sono wpa-shared.

   Nota: l'SSID deve corrispondere all'SSID configurato sull'ISR per l'autenticazione WPA-PSK.

2. In Gestione profili, fare clic sulla scheda Protezione e impostare l'opzione di protezione come passphrase WPA/WPA2. A questo punto, fare clic su Configure (Configura) per configurare la passphrase WPA.



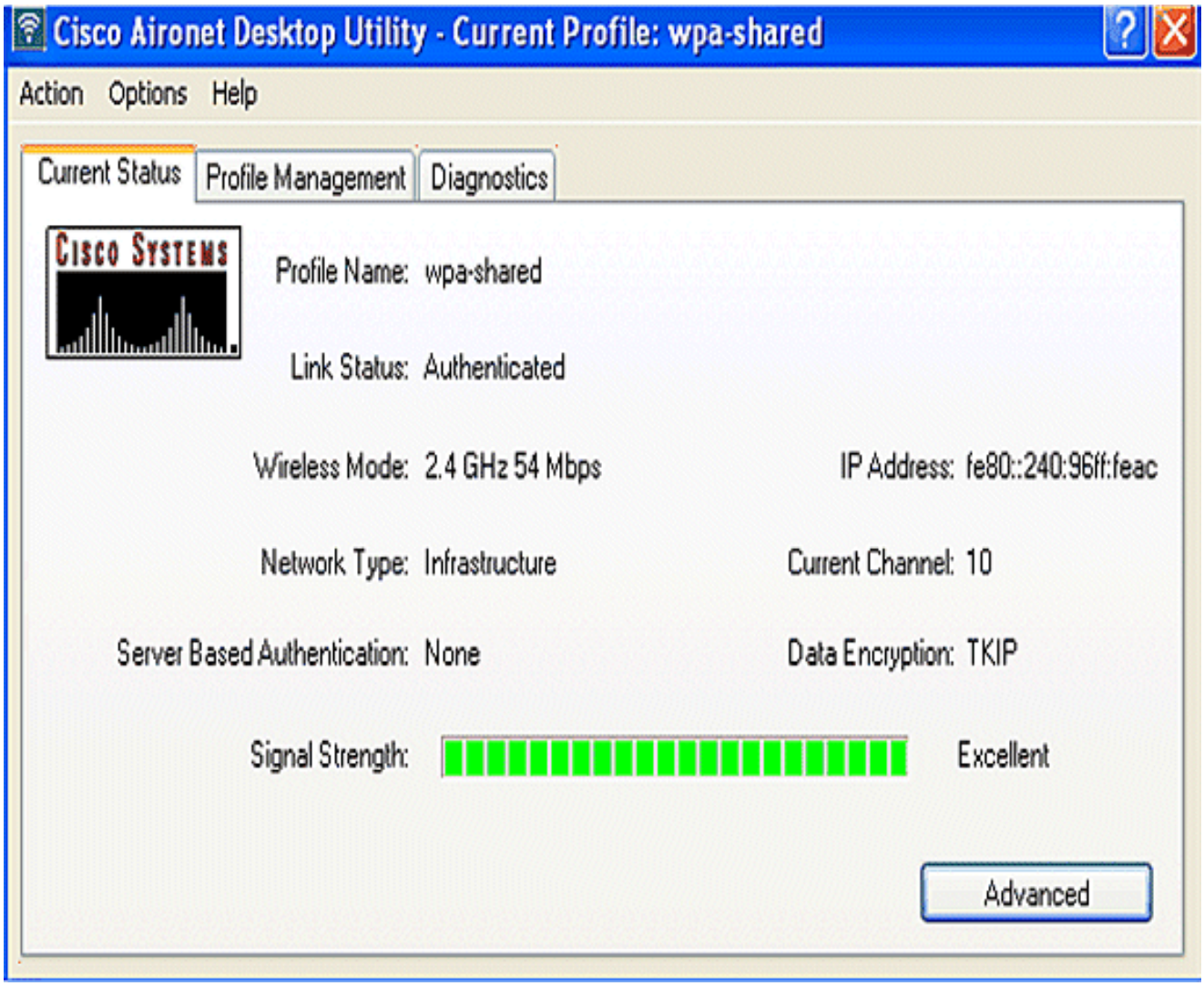
3. Definire una chiave già condivisa WPA. La lunghezza della chiave deve essere compresa tra 8 e 63 caratteri ASCII. Fare clic su OK.



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

- Una volta creato il profilo client, fare clic su Attiva nella scheda Gestione profili per attivare il profilo wpa-shared.

- Verificare che l'autenticazione dell'ADU sia riuscita.



Configurazione del client wireless per l'autenticazione WPA (con EAP)

Attenersi alla seguente procedura:

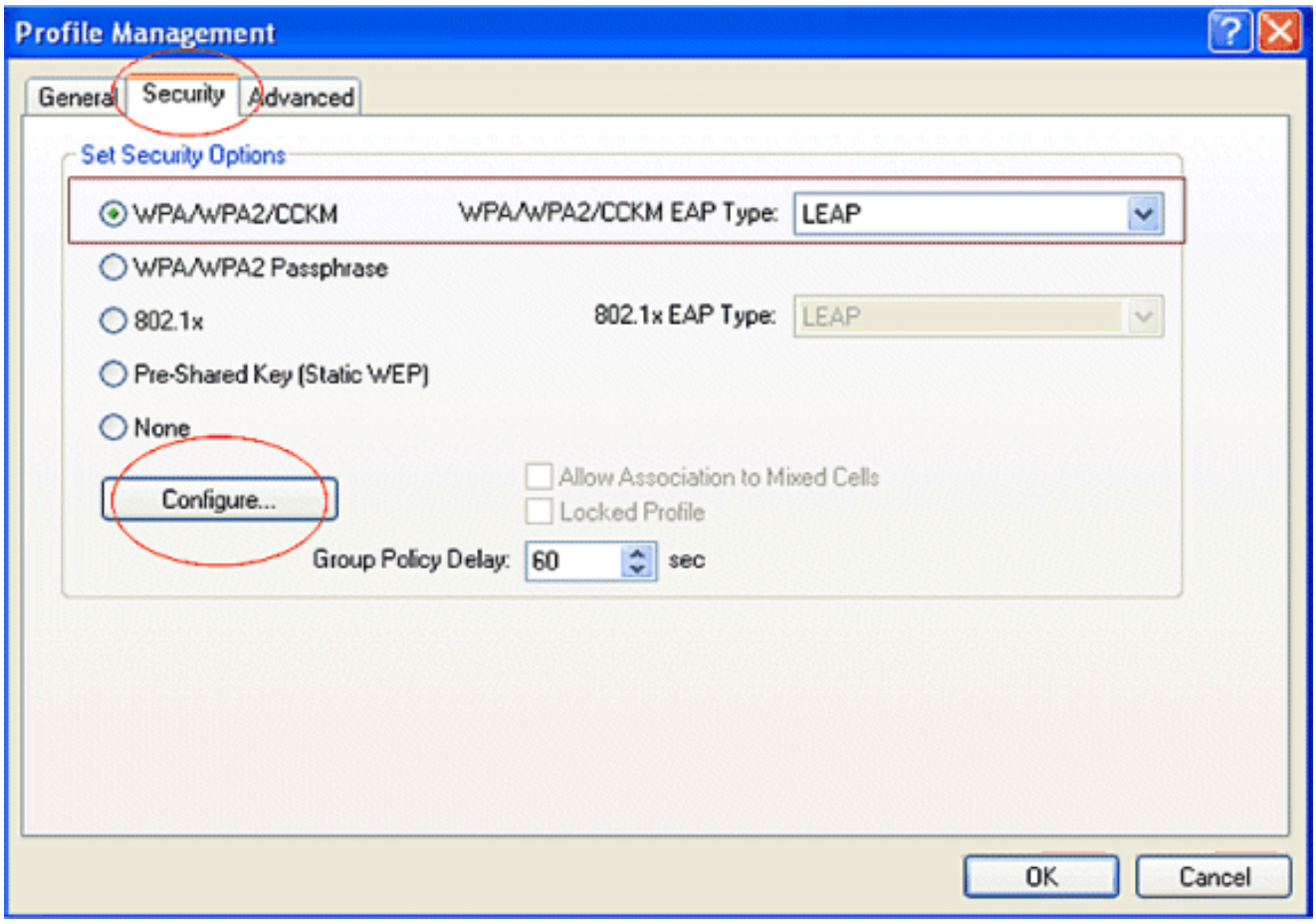
1. Nella finestra Gestione profili dell'ADU, fare clic su Nuovo per creare un nuovo profilo.

   Viene visualizzata una nuova finestra in cui è possibile impostare la configurazione per l'autenticazione aperta. Nella scheda General (Generale), immettere il Nome profilo e l'SSID utilizzati dall'adattatore client.

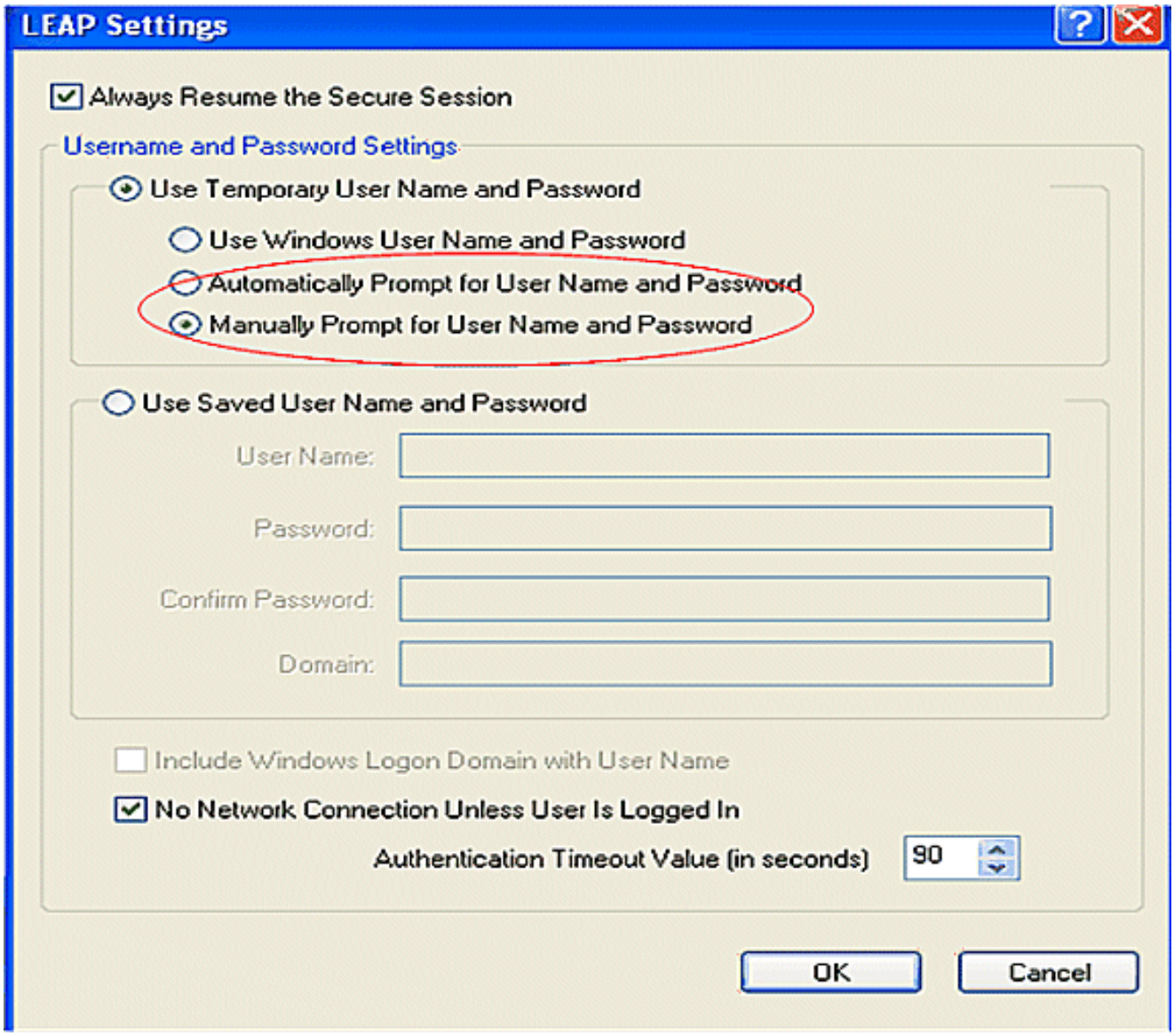
   In questo esempio, il nome del profilo e il SSID sono wpa-dot1x.

   Nota: il SSID deve corrispondere al SSID configurato nell'ISR per l'autenticazione WPA (con EAP).

2. In Gestione profili, fare clic sulla scheda Sicurezza, impostare l'opzione di sicurezza su WPA/WPA2/CCKM e scegliere il tipo di EAP WPA/WPA2/CCKM appropriato. Nel documento viene usato il tipo LEAP per l'autenticazione. A questo punto, fare clic su Configure (Configura) per configurare le impostazioni di nome utente e password LEAP.

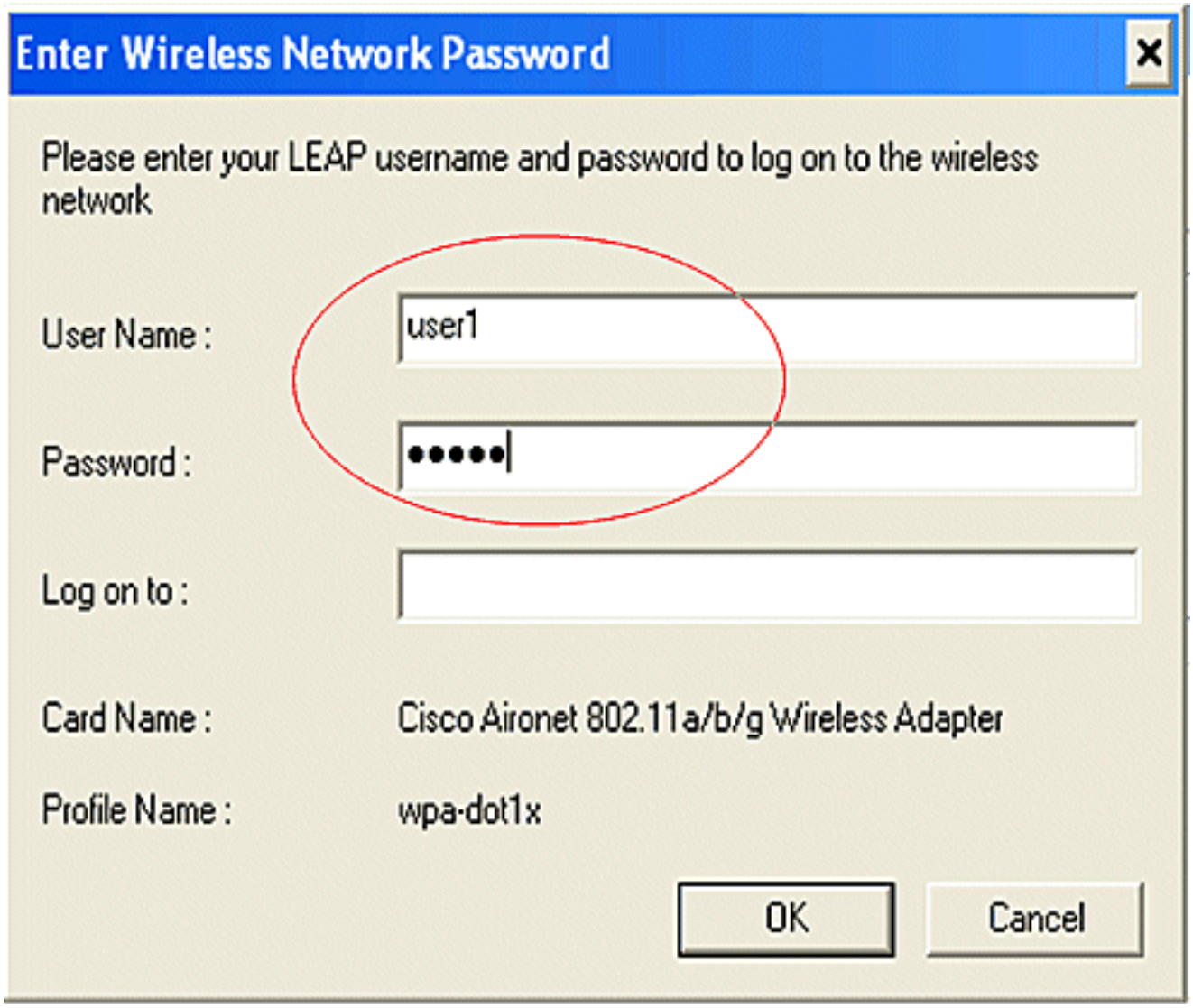


3. Nell'area Impostazioni nome utente e password, in questo esempio viene scelto di richiedere manualmente il nome utente e la password in modo che venga richiesto al client di immettere il nome utente e la password corretti durante il tentativo di connessione alla rete. Fare clic su OK.

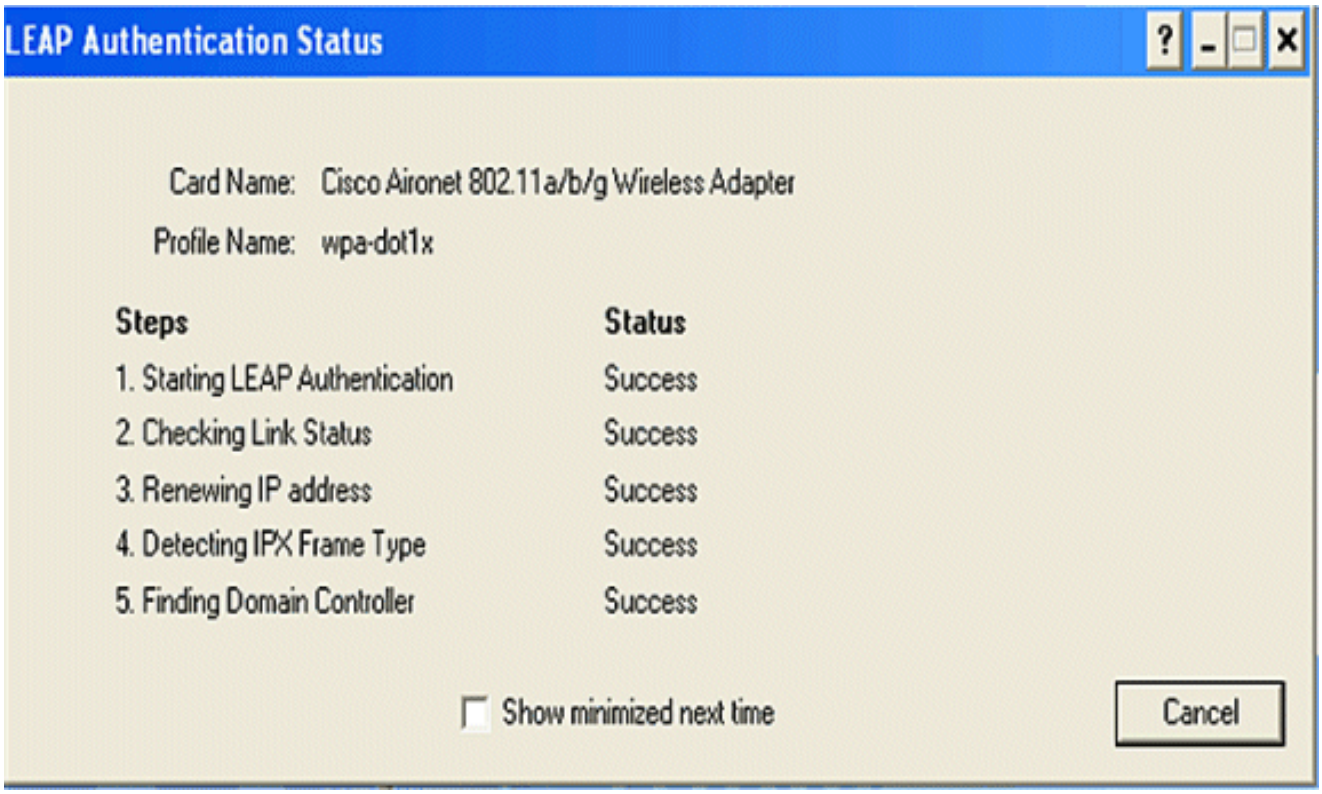


Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

1. Una volta creato il profilo client, fare clic su Activate (Attiva) nella scheda Profile Management (Gestione profili) per attivare il profilo wpa-dot1x. Vengono richiesti il nome utente e la password LEAP. In questo esempio vengono utilizzati il nome utente e la password user1. Fare clic su OK.



2. È possibile controllare l'autenticazione del client.



Il comando show dot11 association dalla CLI del router visualizza i dettagli completi sullo stato dell'associazione del client. Ecco un esempio.

Router#show dot11 associazioni

<#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)
```

Risoluzione dei problemi

Comandi per la risoluzione dei problemi

È possibile utilizzare questi comandi di debug per risolvere i problemi relativi alla configurazione.

- debug dot11 aaa authenticator all: attiva il debug dei pacchetti di autenticazione MAC ed EAP.
- debug radius authentication: visualizza le negoziazioni RADIUS tra il server e il client.
- debug radius local-server packets: visualizza il contenuto dei pacchetti RADIUS inviati e ricevuti.
- debug radius local-server client: visualizza i messaggi di errore relativi alle autenticazioni client non riuscite.

Informazioni correlate

- Esempi di configurazione dell'autenticazione sui controller LAN wireless
- Configurazione delle VLAN sui punti di accesso
- Esempio di router wireless 1800 ISR con DHCP interno e configurazione dell'autenticazione aperta
- Guida alla configurazione di Cisco Wireless ISR e HWIC Access Point
- Esempio di connettività LAN wireless tramite un ISR con crittografia WEP e autenticazione LEAP
- Documentazione e supporto tecnico – Cisco Systems
- Configurazione dei tipi di autenticazione
- Esempio di connettività LAN wireless tramite un ISR con crittografia WEP e configurazione dell'autenticazione LEAP

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).