Esempio di connettività LAN wireless tramite ISR con crittografia WEP e autenticazione LEAP

Sommario

Introduzione

Questo documento spiega come configurare un Cisco serie 870 Integrated Services Router (ISR) per la connettività LAN wireless con crittografia WEP e autenticazione LEAP.

La stessa configurazione si applica a tutti gli altri modelli della serie Wireless Cisco ISR.

Prerequisiti

Requisiti

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

- Informazioni su come configurare i parametri di base dell'ISR Cisco serie 870.
- Informazioni su come configurare l'adattatore client wireless 802.11a/b/g con Aironet Desktop Utility (ADU).

Per informazioni su come configurare l'adattatore client LAN wireless Cisco Aironet 802.11a/b/g (CB21AG e PI21AG), consultare la guida all'installazione e configurazione degli adattatori client LAN wireless (CB21AG e PI21AG) della versione 2.5.

Componenti usati

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

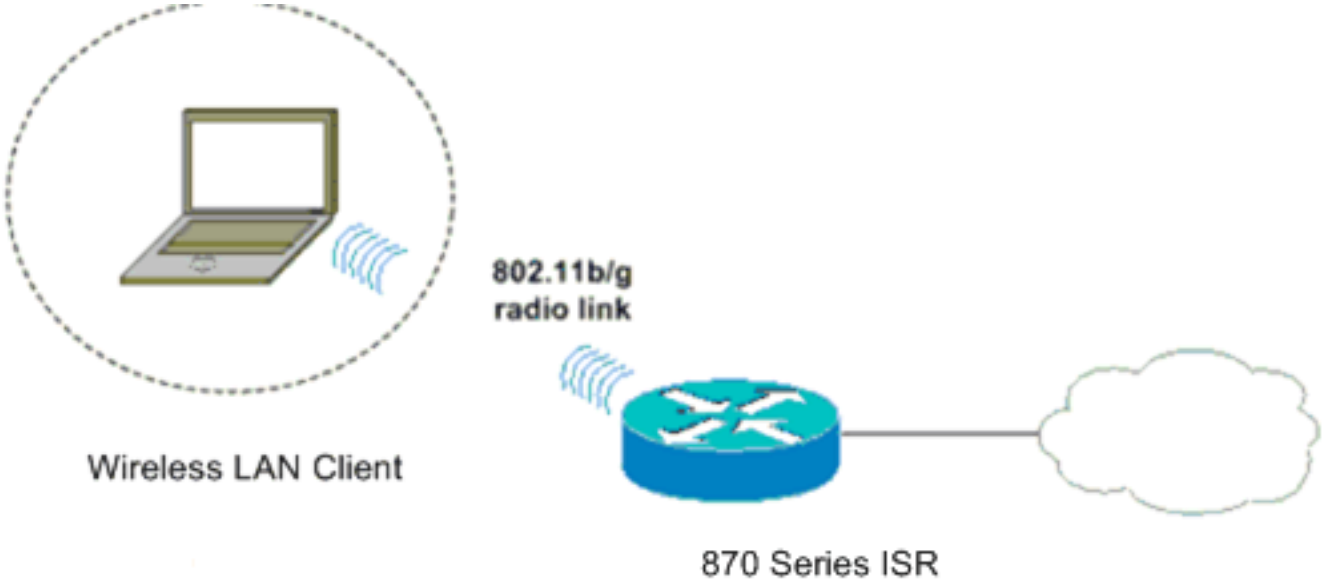
- Cisco 871W ISR con software Cisco IOS® versione 12.3(8)YI1
- Notebook con Aironet Desktop Utility versione 2.5
- Scheda client 802.11 a/b/g con firmware versione 2.5

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.

Esempio di rete

Nel documento viene usata questa impostazione di rete.

In questa configurazione, il client LAN wireless viene associato al router 870. Il server DHCP (Dynamic Host Configuration Protocol) interno sul router 870 viene utilizzato per fornire un indirizzo IP ai client wireless. La crittografia WEP è abilitata sull'ISR 870 e sul client WLAN. L'autenticazione LEAP viene utilizzata per autenticare gli utenti wireless e la funzionalità server RADIUS locale sul router 870 viene utilizzata per convalidare le credenziali.



Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Configurazione router 871W

Completare la procedura descritta di seguito per configurare l'ISR 871W come punto di accesso per accettare le richieste di associazione dai client wireless.

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

abilitare IRB, digitare questi comandi dalla modalità di configurazione globale.

```
WirelessRouter<config>#bridge irb
!--- Enables IRB. WirelessRouter<config>#bridge 1 protocol ieee  !--- Defines the type of
Spanning Tree Protocol as ieee. WirelessRouter<config>#bridge 1 route ip
!--- Enables the routing of the specified protocol in a bridge group.
```

2. Configurare l'interfaccia virtuale con bridging (BVI).Assegnare un indirizzo IP alla BVI. Digitare questi comandi dalla modalità di configurazione globale.

```
WirelessRouter<config>#interface bvi1
!--- Enter interface configuration mode for the BVI. WirelessRouter<config-if>#ip address
172.16.1.100 255.255.0.0
```

Per ulteriori informazioni sulla funzionalità dei gruppi di bridge nei punti di accesso, consultare la sezione *Configurazione dei gruppi di bridge sui punti di accesso e sui bridge* in Uso di VLAN con apparecchiature wireless Cisco Aironet.

3. Configurare la funzione server DHCP interno su 871W ISR.La funzionalità server DHCP interno sul router può essere utilizzata per assegnare indirizzi IP ai client wireless che si associano al router. Completare questi comandi in modalità di configurazione globale.

```
WirelessRouter<config>#ip dhcp excluded-address 172.16.1.100 172.16.1.100
!--- Excludes IP addresses from the DHCP pool. !--- This address is used on the BVI
interface, so it is excluded. WirelessRouter<config>#ip dhcp pool 870-ISR
WirelessRouter<dhcp-config>#network 172.16.1.0 255.255.0.0
```

Nota: anche la scheda client deve essere configurata per accettare indirizzi IP da un server DHCP.

4. Configurare l'ISR 871W come server RADIUS locale.In modalità di configurazione globale, digitare questi comandi per configurare l'ISR 871W come server RADIUS locale.

```
WirelessRouter<config>#aaa new-model
!--- Enable the authentication, authorization, and accounting !--- (AAA) access control
model. WirelessRouter<config>#radius-server local
!--- Enables the 871 wireless-aware router as a local !--- authentication server and enters
into configuration !--- mode for the authenticator. WirelessRouter<config-radsrv)#nas
172.16.1.100 key Cisco
!--- Adds the 871 router to the list of devices that use !--- the local authentication
server. WirelessRouter<config-radsrv>#user ABCD password ABCD
WirelessRouter<config-radsrv)#user XYZ password XYZ
!--- Configure two users ABCD and XYZ on the local RADIUS server. WirelessRouter<config-
radsrv)#exit
WirelessRouter<config>#radius-server host 172.16.1.100 auth-port 1812 acct-port 1813 key
Cisco
!--- Specifies the RADIUS server host.
```

Nota: utilizzare le porte 1812 e 1813 per l'autenticazione e l'accounting per il server RADIUS locale.

```
WirelessRouter<config>#aaa group server radius rad_eap
!--- Maps the RADIUS server to the group rad_eap
.
WirelessRouter<config-sg-radius>#server 172.16.1.100 auth-port 1812 acct-port 1813
!--- Define the server that falls in the group rad_eap. WirelessRouter<config>#aaa
authentication login eap_methods group rad_eap
!--- Enable AAA login authentication.
```

5. Configurare l'interfaccia radio.La configurazione dell'interfaccia radio implica la configurazione di vari parametri wireless sul router, tra cui l'SSID, la modalità di crittografia, il tipo di autenticazione, la velocità e il ruolo del router wireless. In questo esempio viene utilizzato il SSID **Test**.Digitare questi comandi per configurare l'interfaccia radio nella modalità di configurazione globale.

```
WirelessRouter<config>#interface dot11radio0
!--- Enter radio interface configuration mode. WirelessRouter<config-if>#ssid Test
```

```
!--- Configure an SSID test. irelessRouter<config-ssid>#authentication open eap eap_methods
WirelessRouter<config-ssid>#authentication network-eap eap_methods
!--- Expect that users who attach to SSID 'Test' !--- are requesting authentication with
the type 128 !--- Network Extensible Authentication Protocol (EAP) !--- authentication bit
set in the headers of those requests. !--- Group these users into a group called
'eap_methods'. WirelessRouter<config-ssid>#exit
!--- Exit interface configuration mode. WirelessRouter<config-if>#encryption mode wep
mandatory
!--- Enable WEP encryption. WirelessRouter<config-if>#encryption key 1 size 128
1234567890ABCDEF1234567890
!--- Define the 128-bit WEP encryption key. WirelessRouter<config-if>#bridge-group 1
WirelessRouter<config-if>#no shut
!--- Enables the radio interface.
```

Una volta completata questa procedura, il router 870 accetta le richieste di associazione dai client wireless.Quando si configura il tipo di autenticazione EAP sul router, si consiglia di scegliere **Network-EAP e Open with EAP** come tipi di autenticazione per evitare problemi di autenticazione.

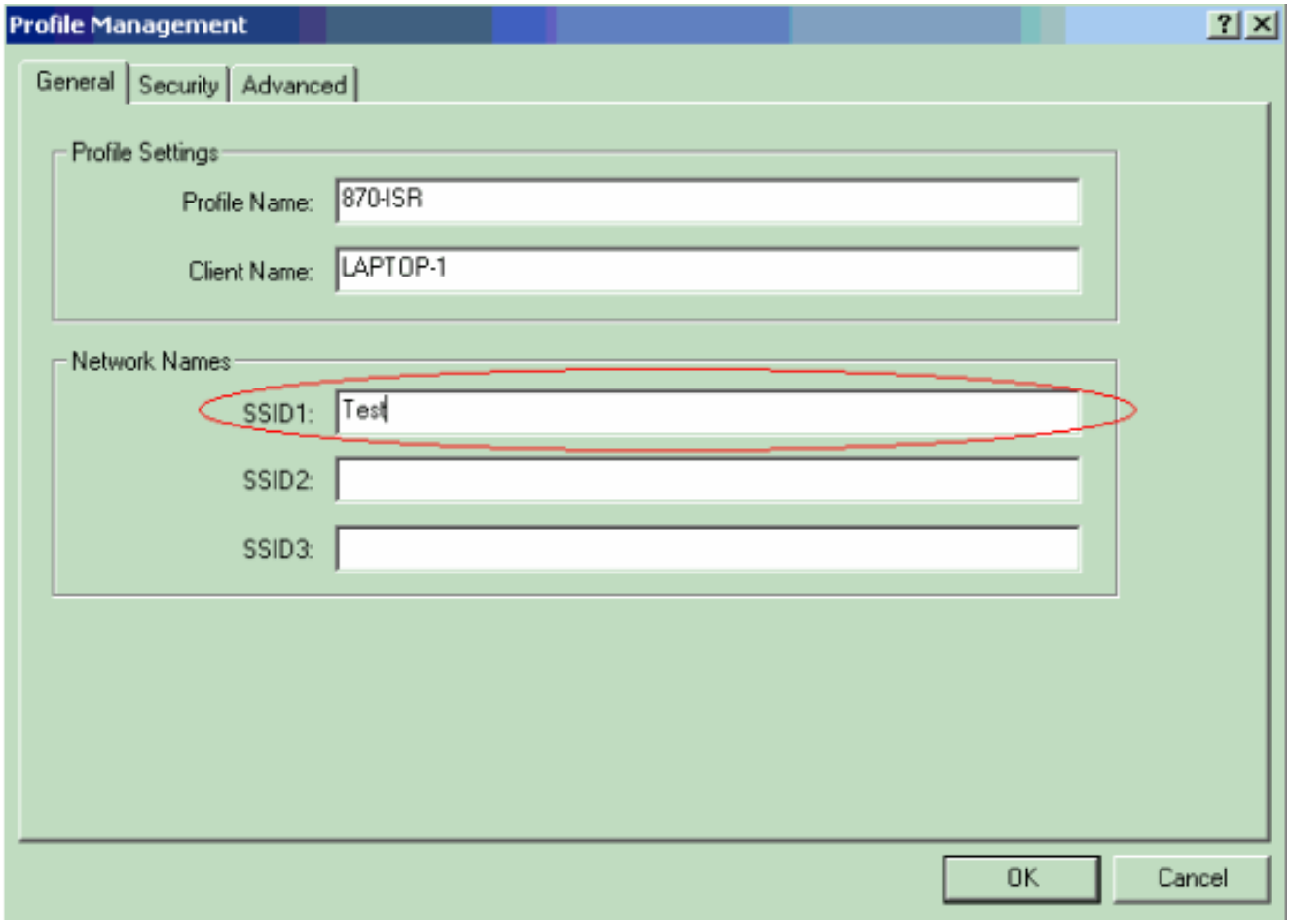
```
WirelessRouter<config-ssid>#authentication network-eap eap_methods
WirelessRouter<config-ssid>#authentication open eap eap_methods
```

Nota: in questo documento si presume che la rete abbia solo client Cisco Wireless.**Nota:** per ulteriori informazioni sui comandi menzionati in questo documento, usare lo strumento di ricerca dei comandi (solo utenti registrati).

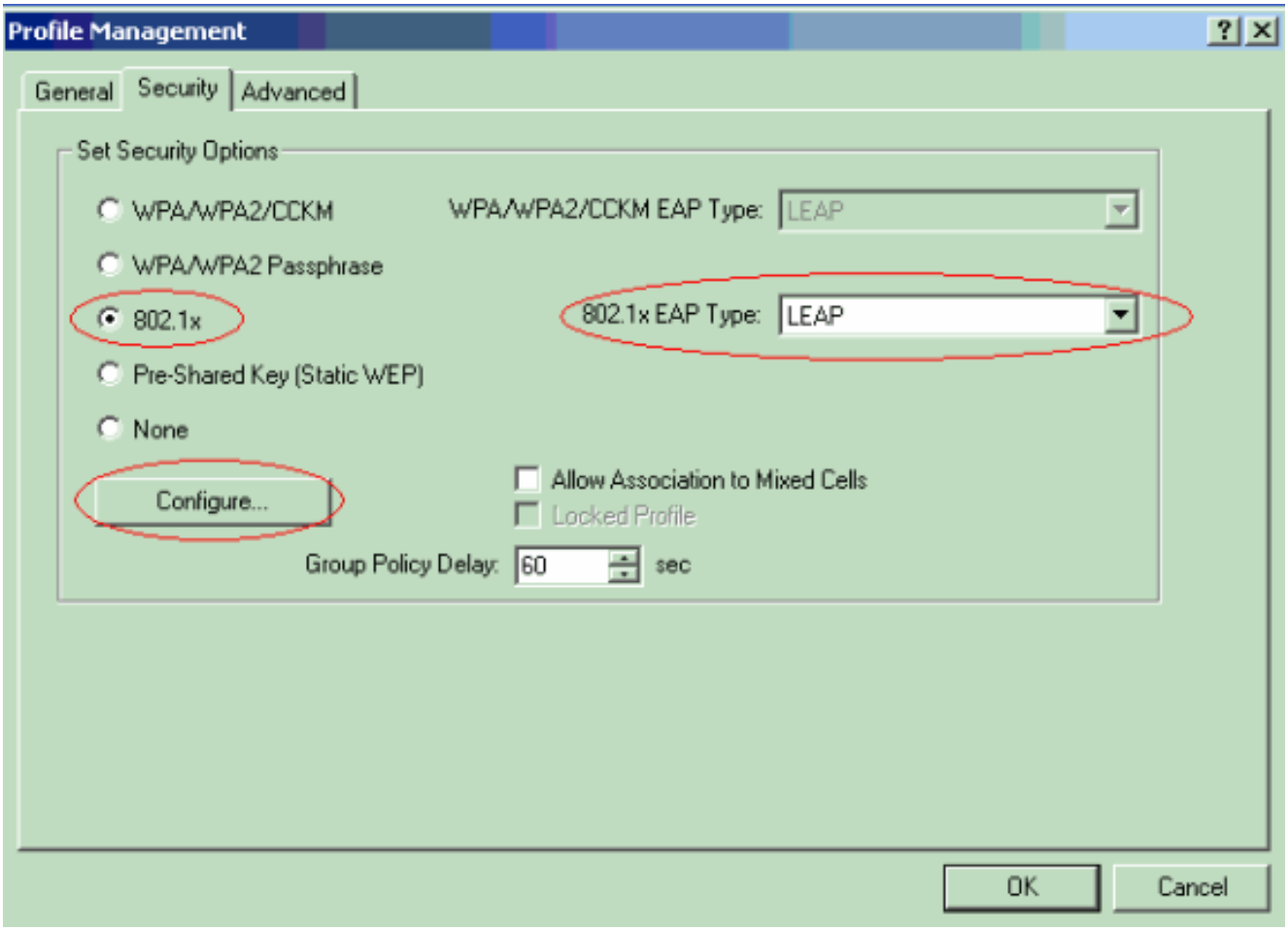
Configurazione adattatore client

Completare questa procedura per configurare la scheda client. Ad esempio, questa procedura consente di creare un nuovo profilo denominato **870-ISR** sull'unità ADU. Questa procedura utilizza anche Test come SSID e abilita l'autenticazione LEAP sulla scheda client.

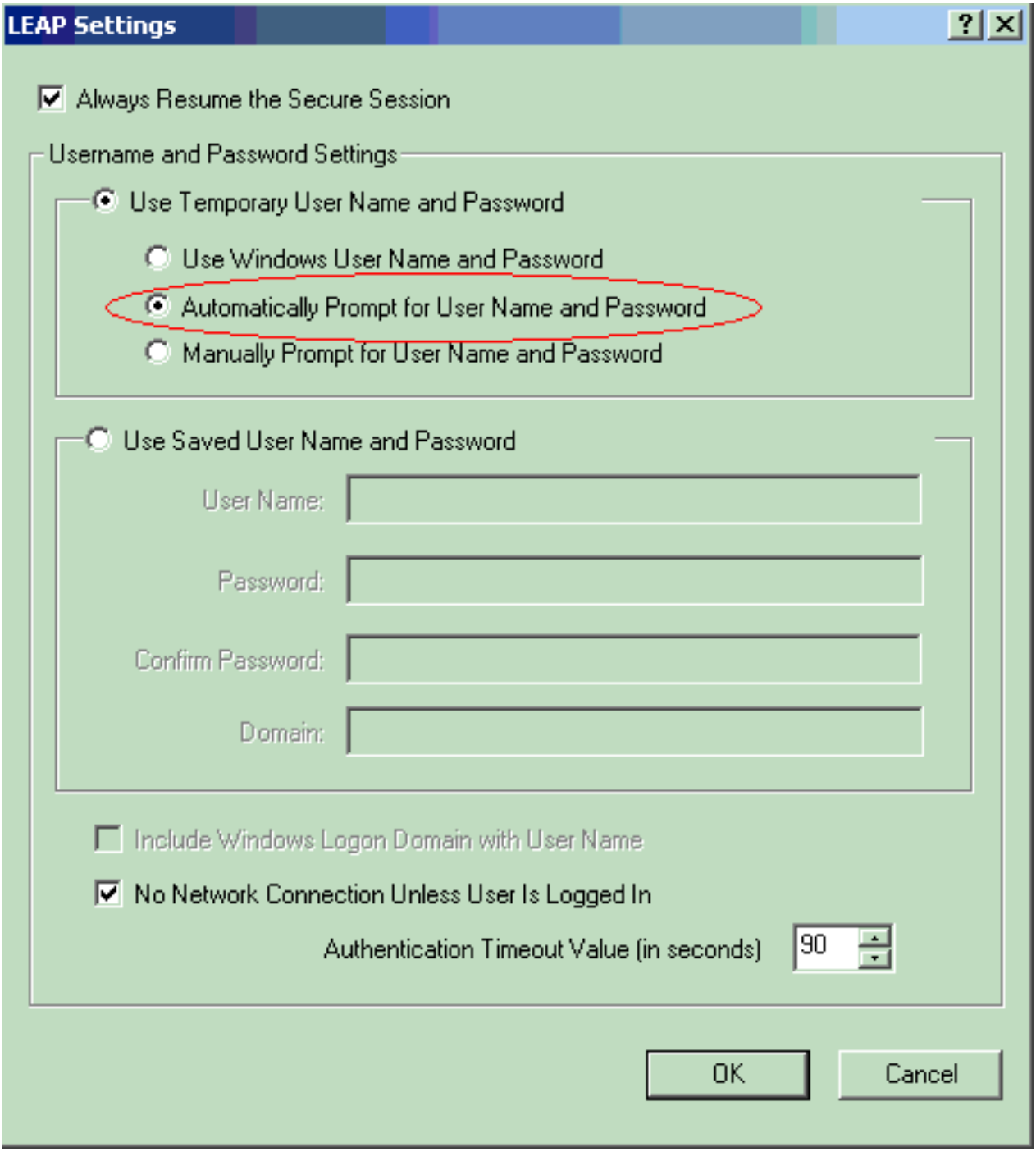
1. Fare clic su **Nuovo** per creare un nuovo profilo nella finestra Gestione profili dell'ADU. Immettere il Nome profilo e l'SSID utilizzati dall'adattatore client nella scheda Generale.Nell'esempio, il nome del profilo è **870-ISR** e il SSID è **Test**.**Nota:** l'SSID deve corrispondere esattamente a quello configurato sull'ISR 871W. SSID fa distinzione tra maiuscole e
minuscole.



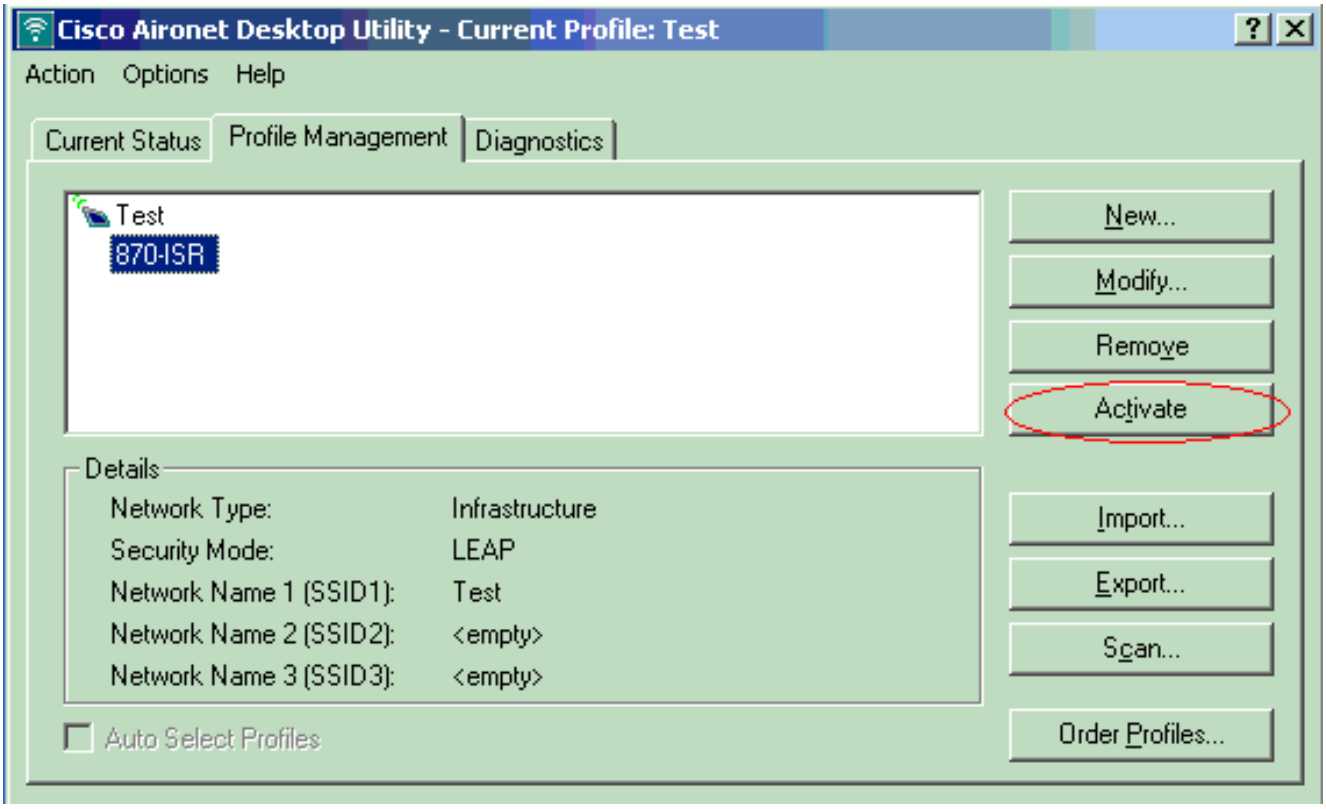
2. Andare alla scheda Security (Sicurezza), selezionare **802.1x** e scegliere **LEAP** dal menu 802.1x EAP Type (Tipo EAP 802.1x).Questa azione abilita l'autenticazione LEAP sulla scheda
client.



3. Fare clic su **Configura** per definire le impostazioni LEAP.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.



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

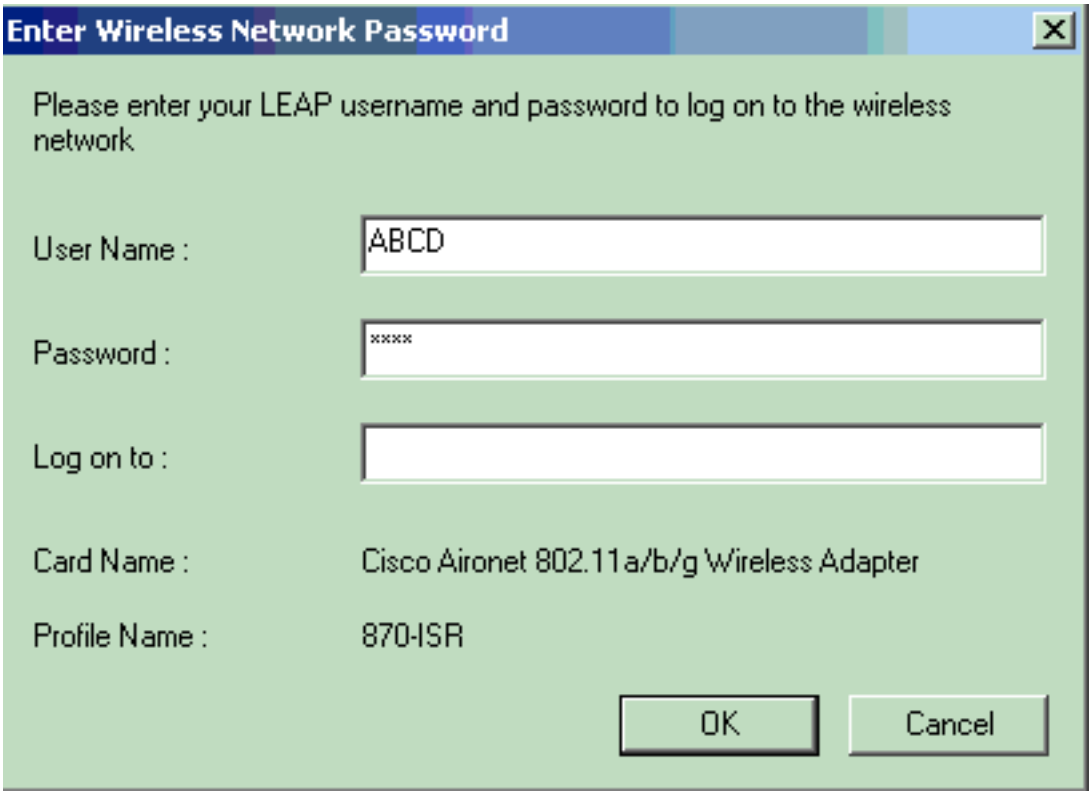


Verifica

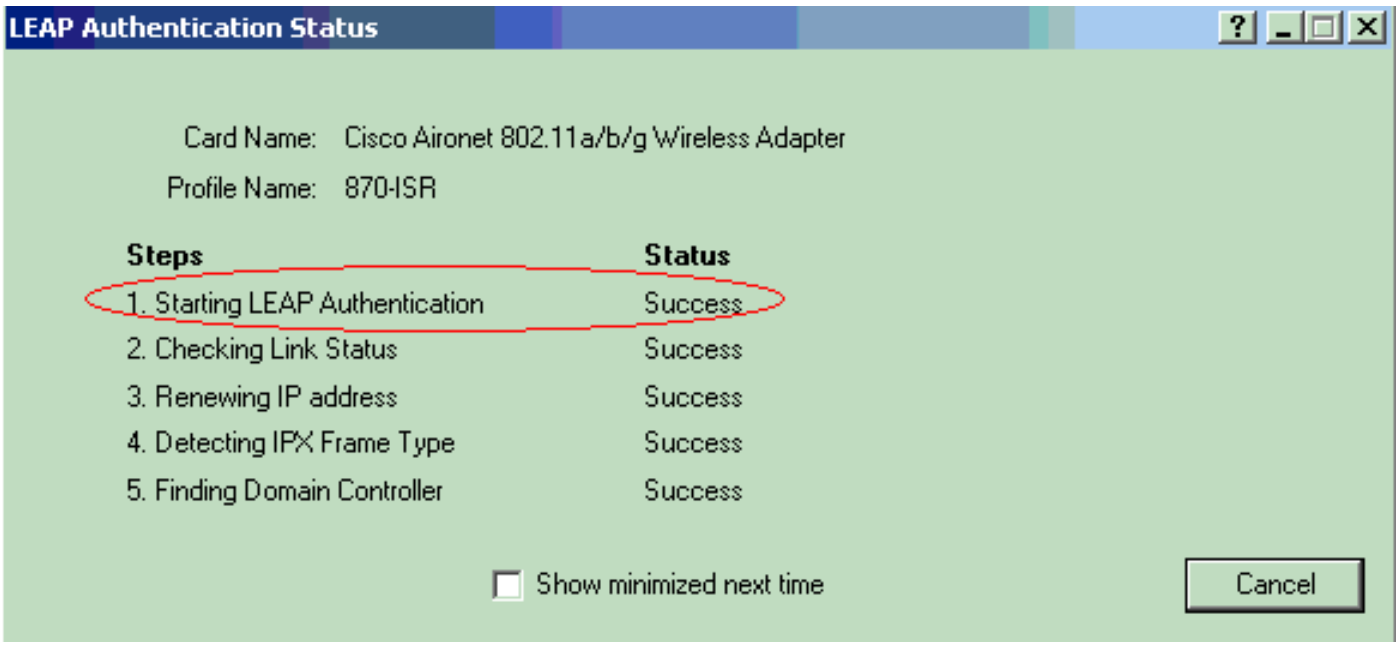
Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Una volta configurati l'adattatore client e il router 870, attivare il profilo 870-ISR sull'adattatore client per verificare la configurazione.

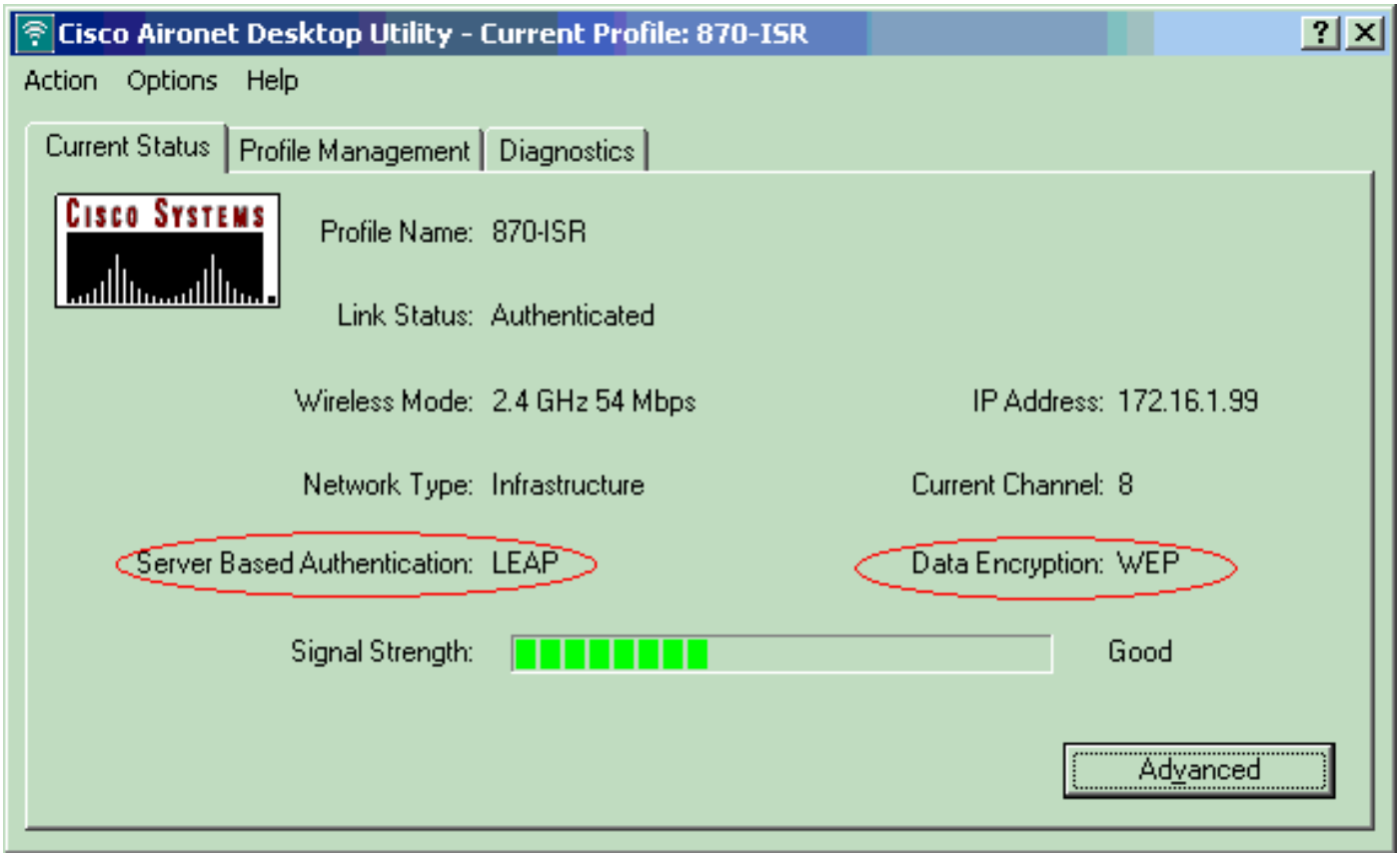
Immettere il nome utente e la password quando viene visualizzata la finestra Enter Wireless Network Password (Immettere password di rete wireless). Questi devono corrispondere a quelli configurati nell'ISR 871W. Uno dei profili utilizzati in questo esempio è **Nome** utente **ABCD** e Password **ABCD**.



Viene visualizzata la finestra Stato autenticazione LEAP. In questa finestra vengono verificate le credenziali dell'utente rispetto al server RADIUS locale.



Controllare lo stato corrente ADU per verificare che il client utilizzi la crittografia WEP e l'autenticazione LEAP.



Lo [strumento Output Interpreter](#) (solo utenti [registrati](#)) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

- **show dot11 association**: verifica la configurazione sul router 870.

```
WirelessRouter#show dot11 association

802.11 Client Stations on Dot11Radio0:

SSID [Test]:

MAC Address     IP Address     Device          Name     Parent    State
0040.96ac.dd05   172.16.1.99   CB21AG/PI21AG   LAPTOP-1  self    EAP-Associated

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

- **show ip dhcp binding**: verifica che il client disponga di un indirizzo IP tramite il server DHCP.

```
WirelessRouter#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address        Client-ID/       Lease expiration      Type
                 Hardware address/
                 User name
172.16.1.99      0040.96ac.dd05     Feb 6 2006 10:11 PM  Automatic
```

Risoluzione dei problemi

In questa sezione vengono fornite informazioni utili per risolvere eventuali problemi con questa configurazione.

1. Impostare il metodo sull'SSID su **Open** per disabilitare temporaneamente l'autenticazione.In questo modo non è più possibile che si verifichino problemi di radiofrequenza (RF) che impediscono la riuscita dell'autenticazione.Usare i comandi **no authentication open eap_methods**, **no authentication network-eap_methods** e **authentication open** dalla CLI.Se il

client viene associato correttamente, RF non contribuisce al problema di associazione
2. Verificare che le chiavi WEP configurate sul router wireless corrispondano alle chiavi WEP configurate sui client.In caso di mancata corrispondenza delle chiavi WEP, i client non saranno in grado di comunicare con il router wireless.
3. Verificare che le password segrete condivise siano sincronizzate tra il router wireless e il server di autenticazione.

Èpossibile usare questi comandi di debug anche 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

- Algoritmi di crittografia e tipi di autenticazione
- Tipi di autenticazione wireless su ISR fisso tramite configurazione SDM
- Tipi di autenticazione wireless su una configurazione ISR fissa Esempio
- Guida alla configurazione wireless di Cisco Access Router
- Esempio di router wireless 1800 ISR con DHCP interno e configurazione dell'autenticazione aperta
- Pagina di supporto wireless
- Documentazione e supporto tecnico – Cisco Systems