Conectividade LAN sem fio usando um ISR com criptografia WEP e exemplo de configuração de autenticação LEAP

Contents

Introduction

Este documento explica como configurar um Cisco 870 Series Integrated Services Router (ISR) para a conectividade com LAN Wireless com criptografia e autenticação de LEAP.

A mesma configuração se aplica a qualquer outro modelo Cisco ISR Wireless Series.

Prerequisites

Requirements

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Conhecimento de como configurar os parâmetros básicos do Cisco 870 Series ISR.
- Conhecimento sobre como configurar o Adaptador de Cliente Wireless 802.11a/b/g usando o Aironet Desktop Utility (ADU).

Consulte o Guia de Instalação e Configuração do Cisco Aironet 802.11a/b/g Wireless LAN Client Adapters (CB21AG e PI21AG), Release 2.5, para obter informações sobre como configurar o Adaptador de Cliente 802.11a/b/g.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

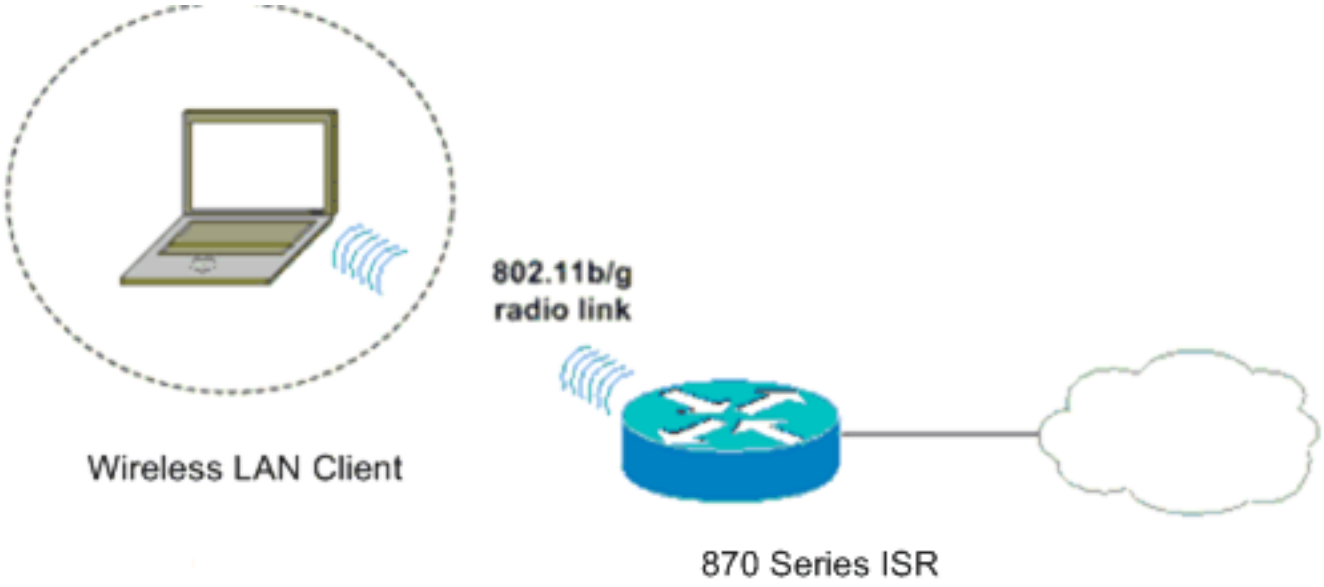
- Cisco 871W ISR que executa o Cisco IOS® Software Release 12.3(8)YI1
- Laptop com Aironet Desktop Utility versão 2.5
- Adaptador cliente 802.11 a/b/g que executa a versão de firmware 2.5

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede.

Nesta configuração, o cliente LAN sem fio se associa ao roteador 870. O servidor DHCP (Dynamic Host Configuration Protocol) interno no roteador 870 é usado para fornecer um endereço IP aos clientes sem fio. A criptografia WEP está habilitada no ISR 870 e no cliente WLAN. A autenticação LEAP é usada para autenticar os usuários sem fio e o recurso de servidor RADIUS local no roteador 870 é usado para validar as credenciais.



Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Configuração do roteador 871W

Conclua estes passos para configurar o ISR 871W como um ponto de acesso para aceitar solicitações de associação dos clientes sem fio.

1. Configure o Integrated Routing and Bridging (IRB) e configure o grupo de pontes.Digite esses comandos no modo de configuração global para ativar o IRB.

```
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. Configure a interface virtual com bridge (BVI).Atribua um endereço IP à BVI. Digite estes comandos no modo de configuração global.

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

   Consulte a seção *Bridge Group Configuration on Access Points and Bridges* de Using VLANs with Cisco Aironet Wireless Equipment para obter mais informações sobre a funcionalidade dos Bridge Groups em access points.

3. Configure o recurso interno do servidor DHCP no ISR 871W.O recurso interno do servidor DHCP no roteador pode ser usado para atribuir endereços IP a clientes sem fio que se associam ao roteador. Complete estes comandos no modo de configuração global.

```
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
```

   Observação: o adaptador cliente também deve ser configurado para aceitar endereços IP de um servidor DHCP.

4. Configure o ISR 871W como um servidor RADIUS local.No modo de configuração global, digite estes comandos para configurar o 871W ISR como um servidor RADIUS local.

```
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.
```

   Observação: use as portas 1812 e 1813 para autenticação e contabilização do servidor RADIUS local.

```
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. Configure a interface de rádio.A configuração da interface de rádio envolve a configuração de vários parâmetros sem fio no roteador, incluindo o SSID, o modo de criptografia, o tipo de autenticação, a velocidade e a função do roteador sem fio. Este exemplo usa o SSID chamado **Test**.Digite estes comandos para configurar a interface de rádio no modo de configuração global.

```
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.
```

O roteador 870 aceita solicitações de associação dos clientes sem fio assim que esse procedimento for concluído.Ao configurar o tipo de autenticação EAP no roteador, é recomendável escolher **Network-EAP e Open with EAP** como tipos de autenticação para evitar quaisquer problemas de autenticação.

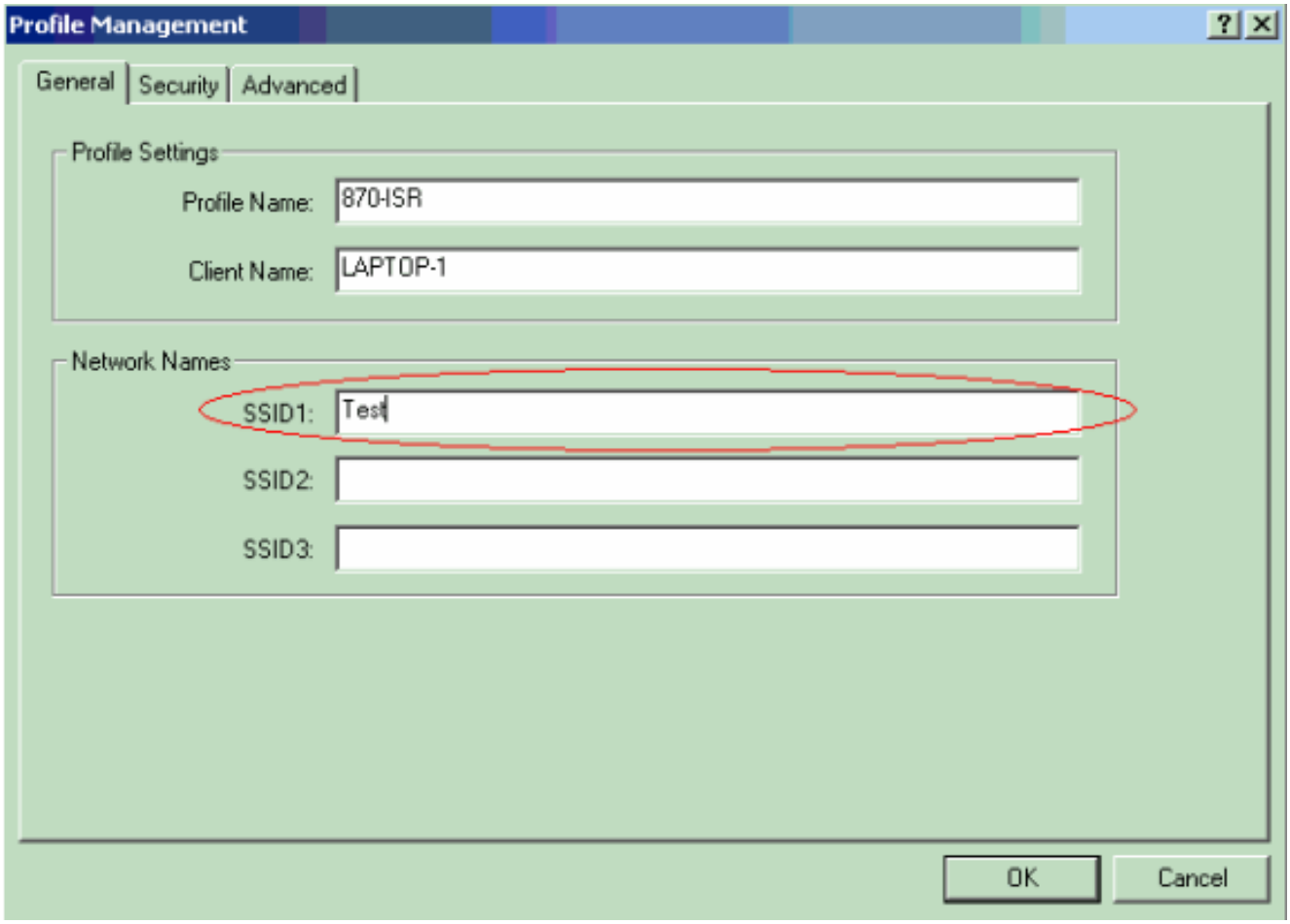
```
WirelessRouter<config-ssid>#authentication network-eap eap_methods
WirelessRouter<config-ssid>#authentication open eap eap_methods
```

Observação: este documento pressupõe que a rede tem apenas clientes Cisco Wireless.Nota:Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados neste documento.

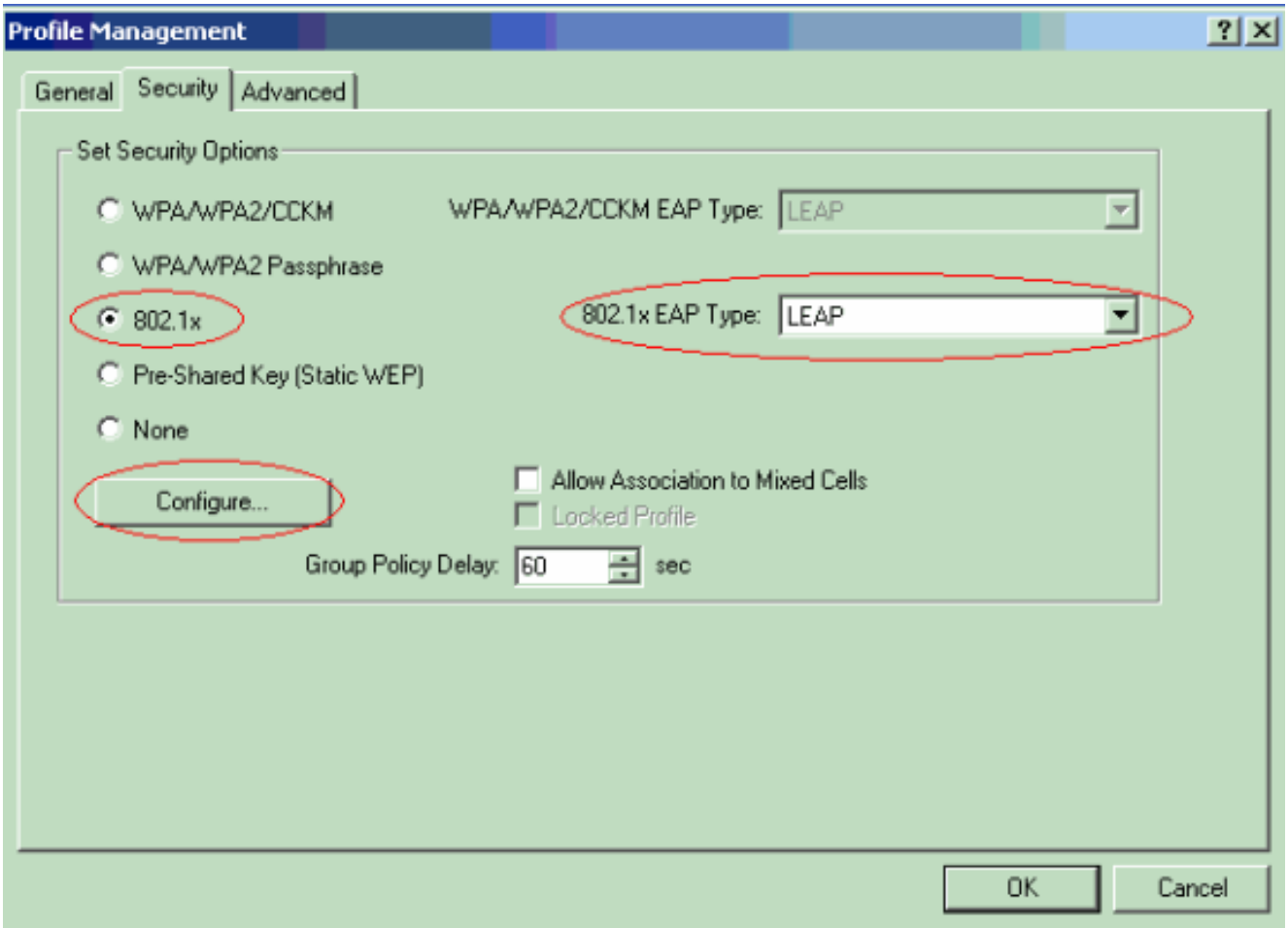
Configuração do adaptador cliente

Conclua estes passos para configurar o adaptador cliente. Este procedimento cria um novo perfil chamado **870-ISR** no ADU, como exemplo. Este procedimento também usa Testar como SSID e habilita a autenticação LEAP no adaptador cliente.

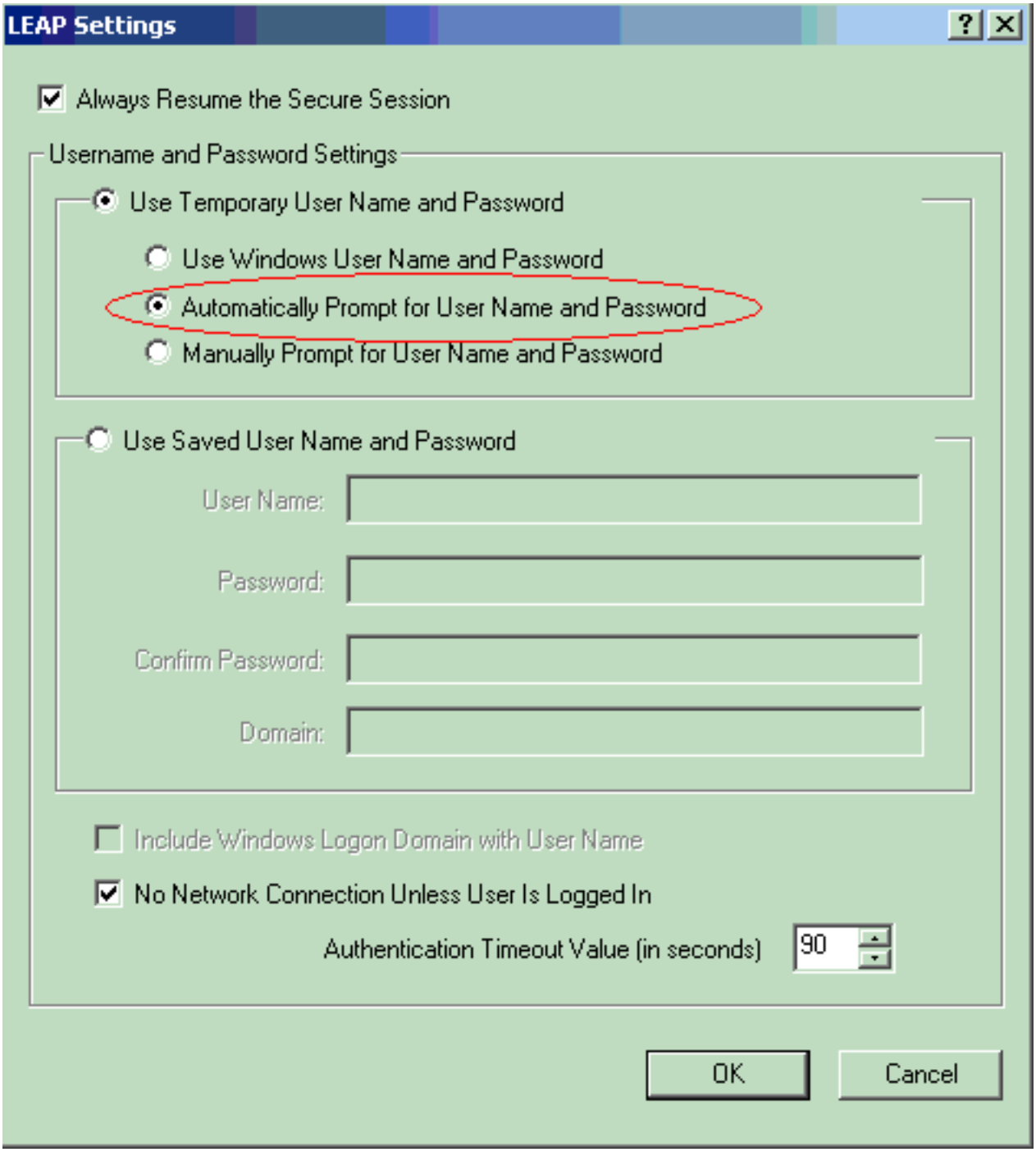
1. Clique em **Novo** para criar um novo perfil na janela Gerenciamento de perfis no ADU. Insira o Nome do perfil e o SSID que o adaptador cliente usa na guia Geral.Neste exemplo, o nome do perfil é **870-ISR** e o SSID é **Test**.**Observação:** o SSID deve corresponder exatamente ao SSID que você configurou no ISR 871W. SSID diferencia maiúsculas de minúsculas.



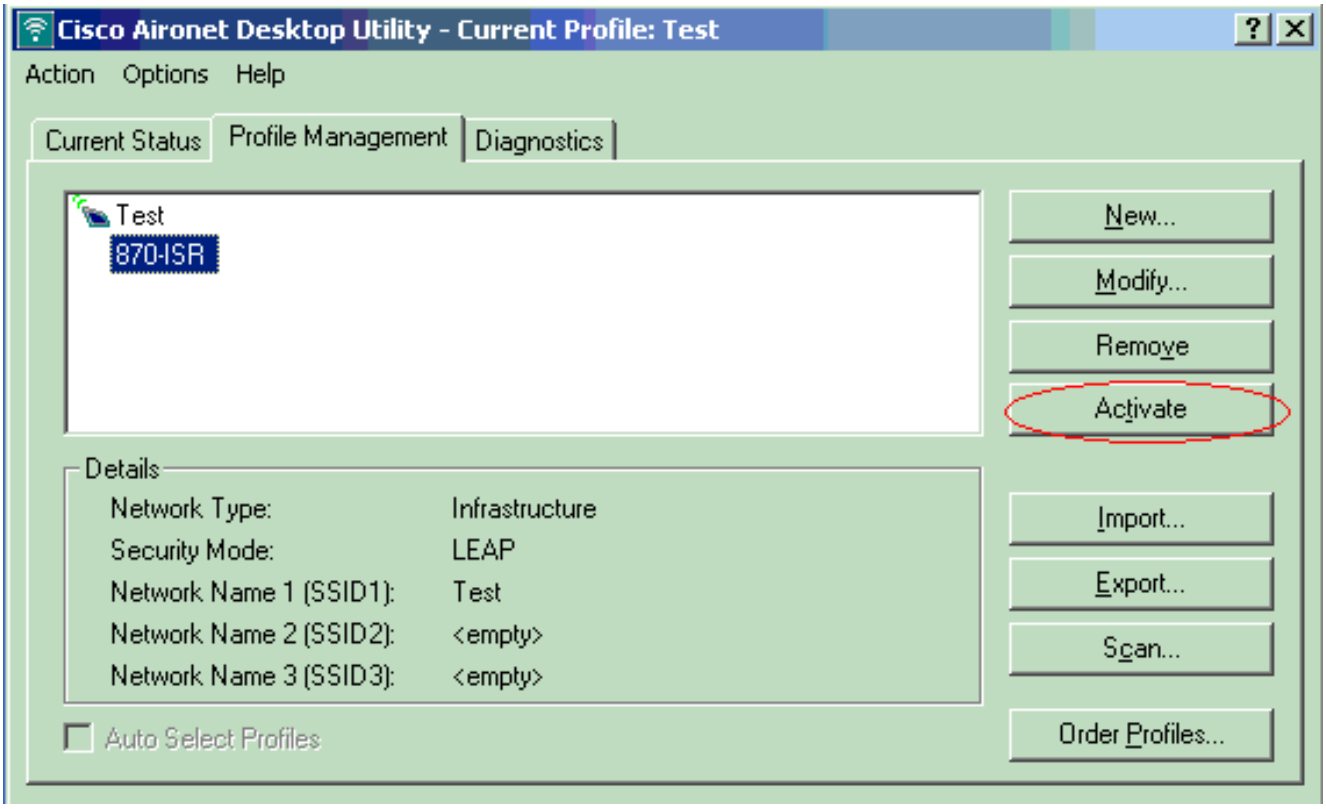
2. Vá até a guia Segurança, selecione **802.1x** e escolha **LEAP** no menu 802.1x EAP Type.Esta ação ativa a autenticação LEAP no adaptador cliente.



3. Clique em **Configurar** para definir as configurações LEAP.Esta configuração escolhe a opção **Solicitar automaticamente nome de usuário e senha**. Essa opção permite que você insira manualmente o nome do usuário e a senha no momento da autenticação LEAP.



4. Clique em **OK** para sair da janela Gerenciamento de perfis.
5. Clique em **Ativar** para ativar este perfil no adaptador cliente.

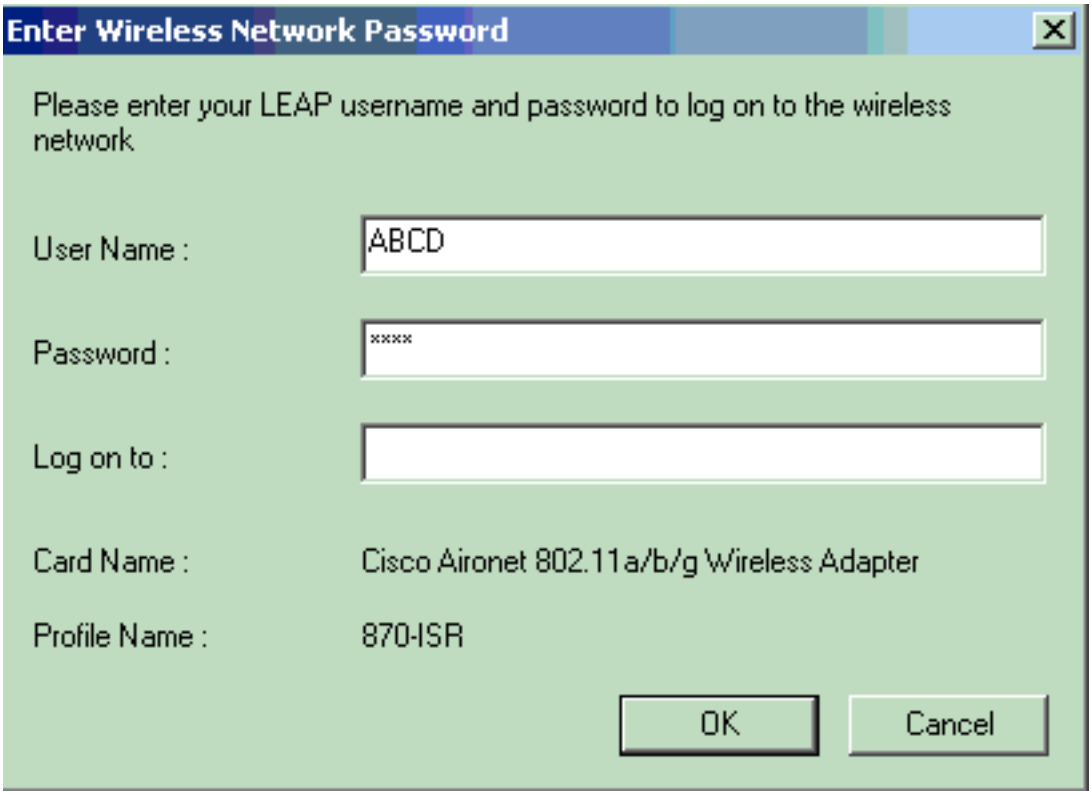


Verificar

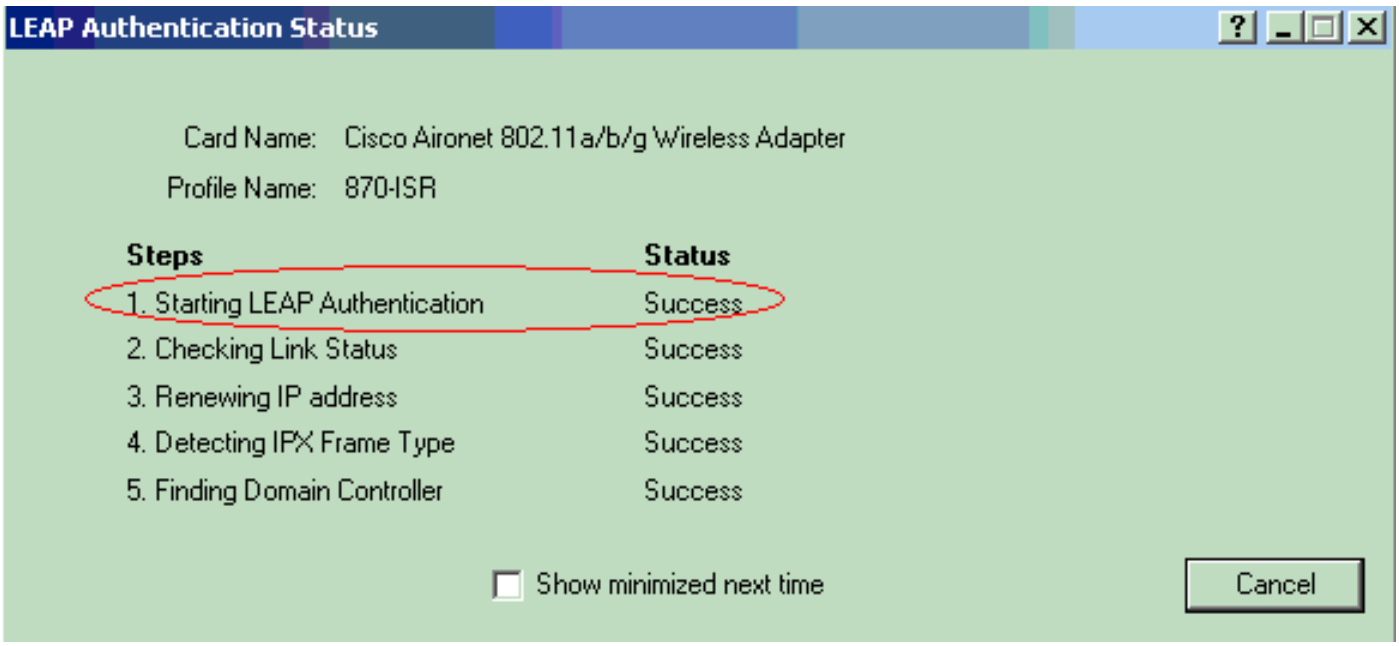
Use esta seção para confirmar se a sua configuração funciona corretamente.

Quando o adaptador cliente e o roteador 870 estiverem configurados, ative o perfil 870-ISR no adaptador cliente para verificar a configuração.

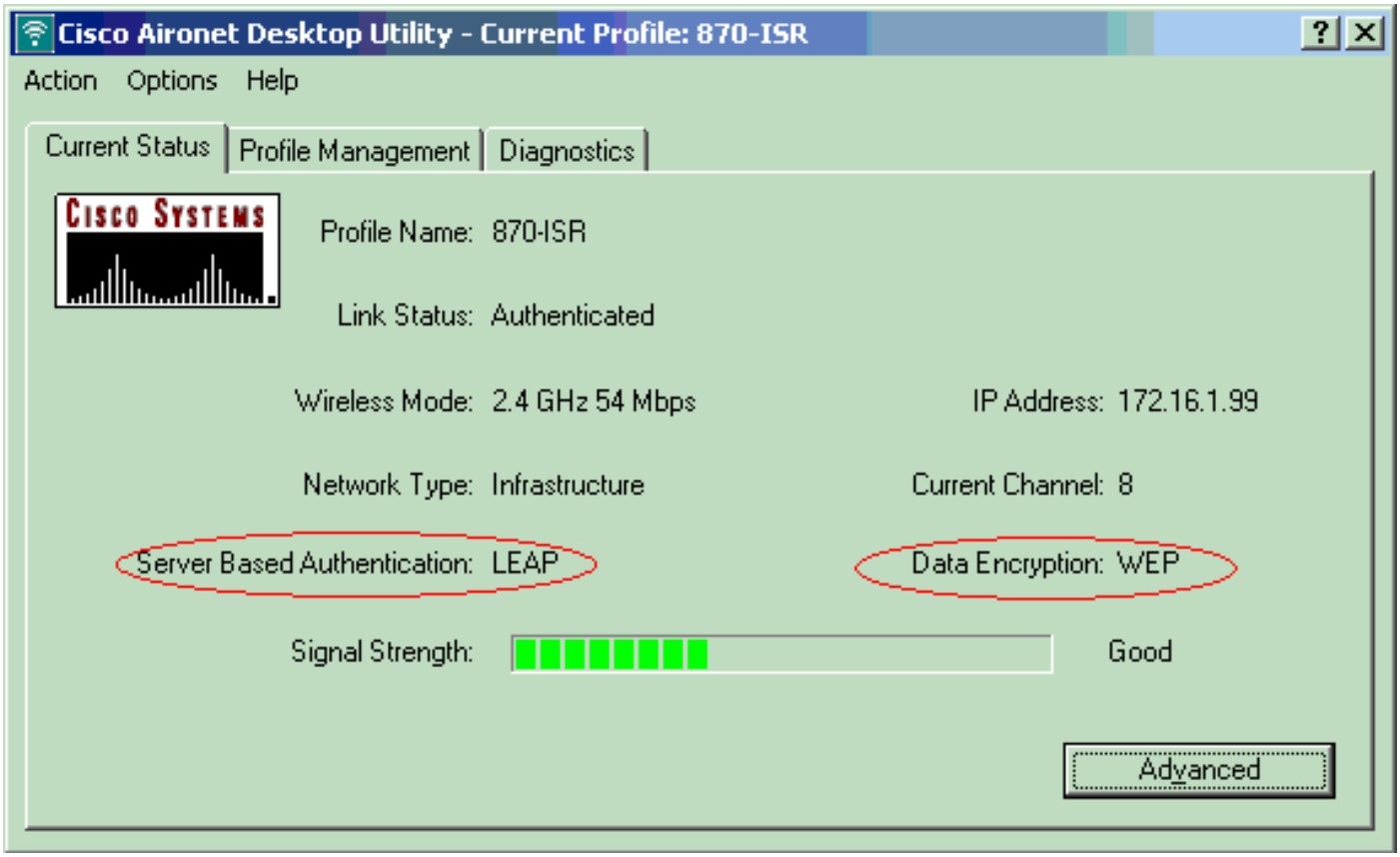
Digite o nome de usuário e a senha quando a janela Enter Wireless Network Password (Inserir senha da rede sem fio) for exibida. Eles devem corresponder aos configurados no ISR 871W. Um dos perfis usados neste exemplo é Nome de usuário **ABCD** e **ABCD** de senha.



A janela LEAP Authentication Status (Status da autenticação LEAP) é exibida. Essa janela verifica as credenciais do usuário em relação ao servidor RADIUS local.



Verifique o status atual do ADU para verificar se o cliente usa criptografia WEP e autenticação LEAP.



A Output Interpreter Tool (somente clientes registrados) (OIT) oferece suporte a determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

- **show dot11 association** —Verifica a configuração no roteador 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 se o cliente tem um endereço IP através do servidor 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
```

Troubleshoot

Esta seção fornece informações de solução de problemas relevantes para esta configuração.

1. Defina o método no SSID como **Open (Abrir)** para desabilitar temporariamente a autenticação.Isso elimina a possibilidade de problemas de radiofrequência (RF) que impeçam a autenticação bem-sucedida.Use os comandos **no authentication open eap eap_methods**, **no authentication network-eap eap_methods** e **authentication open** da CLI.Se o cliente se associar com êxito, o RF não contribui para o problema de associação

2. Verifique se as chaves WEP configuradas no roteador wireless correspondem às chaves WEP configuradas nos clientes.Se houver uma incompatibilidade nas chaves WEP, os clientes não poderão se comunicar com o roteador sem fio.
3. Verifique se as senhas secretas compartilhadas estão sincronizadas entre o roteador wireless e o servidor de autenticação.

Você também pode usar esses comandos debug para solucionar problemas de sua configuração.

- **debug dot11 aaa authenticator all** — Ativa a depuração de pacotes de autenticação MAC e EAP.
- **debug radius authentication** — Exibe as negociações RADIUS entre o servidor e o cliente.
- **debug radius local-server packets** — Exibe o conteúdo dos pacotes RADIUS enviados e recebidos.
- **debug radius local-server client** — Exibe mensagens de erro sobre falhas de autenticação de cliente.

Informações Relacionadas

- Algoritmos de criptografia e tipos de autenticação
- Exemplo de configuração de tipos de autenticação sem fio em ISR fixo por meio de SDM
- Exemplo de Tipos de Autenticação Wireless em uma Configuração de ISR Fixo
- Guia de configuração sem fio do Cisco Access Router
- Exemplo de configuração do roteador sem fio 1800 ISR com DHCP interno e autenticação aberta
- Página de Suporte Wireless
- Suporte Técnico e Documentação - Cisco Systems