Configurar tipos de autenticação sem fio em um ISR fixo

Contents

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Conventions
Informações de Apoio
Configurar
Diagrama de Rede
Configurar a autenticação aberta
Configurar o Integrated Routing and Bridging (IRB) e Configurar o Grupo de Bridge
Configurar a interface virtual com bridge (BVI)
Configurar o SSID para autenticação aberta
Configure o servidor DHCP interno para os clientes sem fio desta VLAN
Configurar a autenticação 802.1x/EAP
Configurar o Integrated Routing and Bridging (IRB) e Configurar o Grupo de Bridge
Configurar a interface virtual com bridge (BVI)
Configurar o servidor RADIUS local para autenticação EAP
Configurar o SSID para autenticação 802.1x/EAP
Configure o servidor DHCP interno para os clientes sem fio desta VLAN
Gerenciamento de chave WPA
Configuração do WPA-PSK
Configurar o Integrated Routing and Bridging (IRB) e Configurar o Grupo de Bridge
Configurar a interface virtual com bridge (BVI)
Configurar o SSID para autenticação WPA-PSK
Configure o servidor DHCP interno para os clientes sem fio desta VLAN
Configurar a autenticação WPA (com EAP)
Configurar o Integrated Routing and Bridging (IRB) e Configurar o Grupo de Bridge
Configurar a interface virtual com bridge (BVI)
Configurar o servidor RADIUS local para autenticação WPA
Configurar o SSID para WPA com autenticação EAP
Configure o servidor DHCP interno para os clientes sem fio desta VLAN
Configurar o cliente sem fio para autenticação
Configurar o cliente sem fio para a autenticação aberta
Configurar o cliente sem fio para a autenticação 802.1x/EAP
Configurar o cliente sem fio para a autenticação WPA-PSK
Configurar o cliente sem fio para a autenticação WPA (com EAP)
Troubleshooting
Comandos para Troubleshooting

[Informações Relacionadas](#)

Introdução

Este documento fornece um exemplo de configuração que explica como configurar vários tipos de autenticação de Camada 2 em um roteador de configuração fixo integrado sem fio da Cisco para conectividade sem fio com comandos CLI.

Pré-requisitos

Requisitos

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

- Conhecimento de como configurar os parâmetros básicos do Cisco Integrated Services Router (ISR)
- Conhecimento de como configurar o Adaptador Cliente Sem Fio 802.11a/b/g com o Aironet Desktop Utility (ADU)

Componentes Utilizados

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

- Cisco 877W ISR com Cisco IOS® Software Release 12.3(8)YI1
- Laptop com Utilitário de Desktop Aironet Versão 3.6
- Adaptador cliente 802.11 a/b/g que executa a versão 3.6 do firmware

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Conventions

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

Informações de Apoio

Os roteadores de configuração fixa dos serviços integrados da Cisco suportam uma solução LAN sem fio segura, acessível e fácil de usar que combina mobilidade e flexibilidade com os recursos de nível empresarial exigidos pelos profissionais de rede. Com um sistema de gerenciamento baseado no software Cisco IOS, os roteadores Cisco atuam como pontos de acesso e são transceptores LAN sem fio compatíveis com IEEE 802.11a/b/g, com certificação Wi-Fi.

Você pode configurar e monitorar os roteadores com a interface de linha de comando (CLI), o sistema de gerenciamento baseado em navegador ou o Simple Network Management Protocol (SNMP). Este documento descreve como configurar o ISR para conectividade sem fio com os comandos CLI.

Configurar

Este exemplo mostra como configurar esses tipos de autenticação em um roteador de configuração fixa Cisco Wireless Integrated com comandos CLI.

- Autenticação aberta
- Autenticação 802.1x/EAP (Extensible Authentication Protocol)
- Autenticação WPA-PSK (Wi-Fi Protected Access Pre-Shared Key)
- autenticação WPA (com EAP)

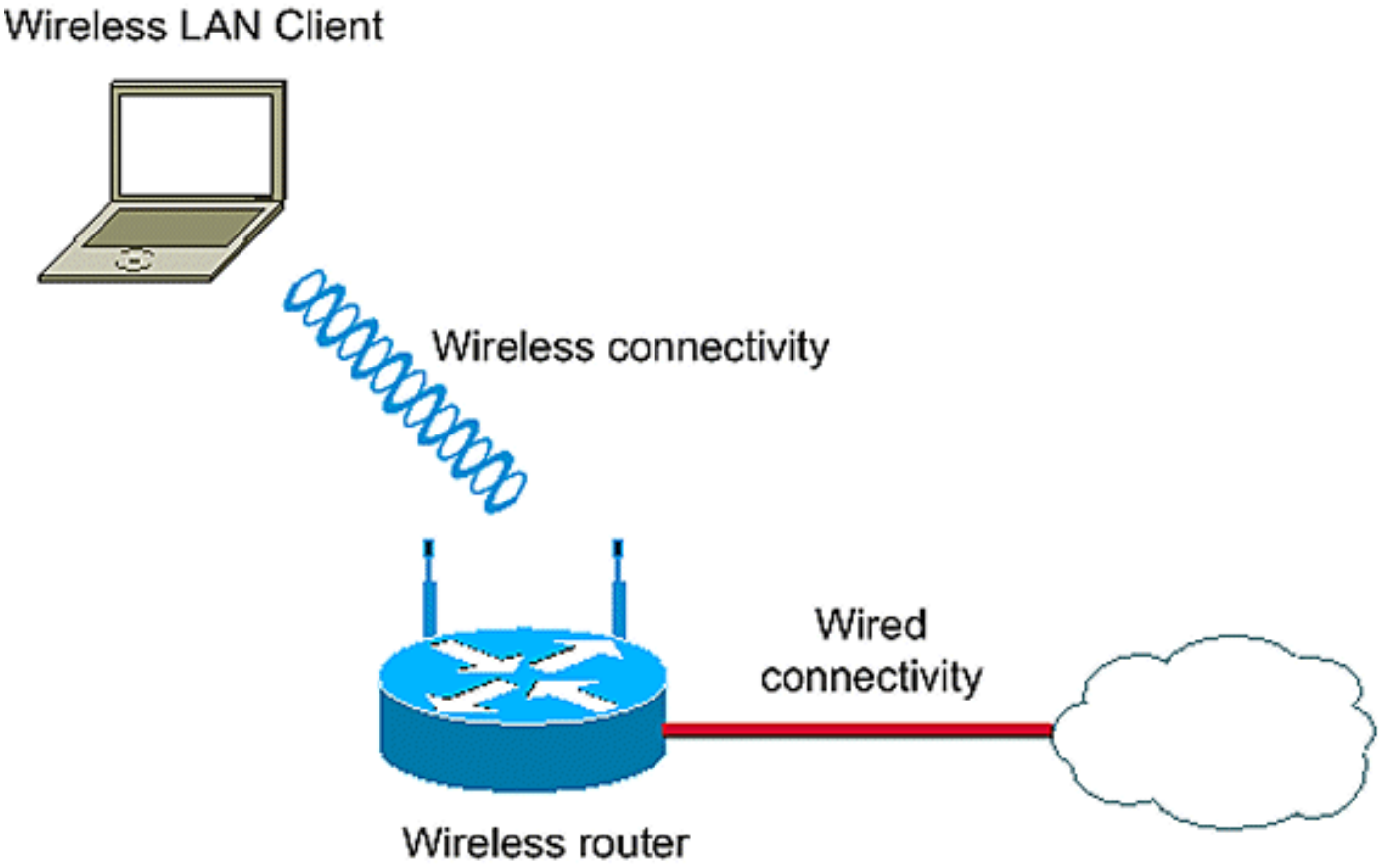
Observação: este documento não se concentra na autenticação compartilhada, pois é um tipo de autenticação menos seguro.

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Esta configuração usa o servidor RADIUS local no ISR Wireless para autenticar clientes Wireless com autenticação 802.1x.

Configurar a autenticação aberta

A autenticação aberta é um algoritmo de autenticação nulo. O ponto de acesso concede qualquer solicitação de autenticação. A autenticação aberta permite acesso à rede de qualquer dispositivo. Se nenhuma criptografia estiver habilitada na rede, qualquer dispositivo que conheça o SSID do ponto de acesso poderá obter acesso à rede. Com a criptografia WEP habilitada em um ponto de acesso, a própria chave WEP se torna um meio de controle de acesso. Se um dispositivo não tiver a chave WEP correta, mesmo que a autenticação seja bem-sucedida, o dispositivo não poderá transmitir dados através do ponto de acesso. Ele também não pode descriptografar os dados enviados do ponto de acesso.

Este exemplo de configuração explica apenas uma autenticação aberta simples. A chave WEP pode se tornar obrigatória ou opcional. Este exemplo configura a chave WEP como opcional de modo que qualquer dispositivo que não use WEP também possa autenticar e associar-se a este AP.

Consulte Autenticação Aberta para obter mais informações.

Este exemplo usa esta configuração para configurar a autenticação aberta no ISR.

- Nome SSID: "open"

- VLAN 1
- Intervalo do servidor DHCP interno: 10.1.0.0/16

Observação: para simplificar, este exemplo não usa nenhuma técnica de criptografia para clientes autenticados.

Conclua estas ações no roteador:

1. Configurar o Integrated Routing and Bridging (IRB) e Configurar o Grupo de Bridge
2. Configurar a interface virtual com bridge (BVI)
3. Configurar o SSID para autenticação aberta
4. Configure o servidor DHCP interno para os clientes sem fio desta VLAN

Configurar o Integrated Routing and Bridging (IRB) e Configurar o Grupo de Bridge

Conclua estas ações:

1. Ative o IRB no roteador.

   router<configure>#bridge irb

   Observação: se todos os tipos de segurança forem configurados em um único roteador, basta ativar o IRB globalmente apenas uma vez no roteador. Ele não precisa ser habilitado para cada tipo de autenticação individual.

2. Defina um grupo de bridge.

   Este exemplo usa o número de grupo de ponte 1.

   router<configure>#bridge 1

3. Escolha o protocolo spanning tree para o grupo de pontes.

   Aqui, o protocolo spanning tree IEEE é configurado para esse grupo de ponte.

   router<configure>#bridge 1 protocol ieee

4. Habilite um BVI para aceitar e rotear pacotes roteáveis recebidos de seu grupo de ponte correspondente.

   Este exemplo permite que o BVI aceite e roteie o pacote IP.

   router<configure>#bridge 1 route ip

Configurar a interface virtual com bridge (BVI)

Conclua estas ações:

1. Configure o BVI.

   Configure o BVI ao atribuir o número correspondente do grupo de pontes ao BVI. Cada grupo de bridge pode ter apenas um BVI correspondente. Este exemplo atribui o grupo de pontes número 1 ao BVI.

   router<configure>#interface BVI <1>

2. Atribua um endereço IP ao BVI.

   router<config-if>#ip address 10.1.1.1 255.255.0.0

   router<config-if>#no shut

Consulte Configurar Bridging para obter informações detalhadas sobre Bridging.

Configurar o SSID para autenticação aberta

Conclua estas ações:

1. Ativar a interface de rádio

   Para habilitar a interface de rádio, vá para o modo de configuração da interface de rádio DOT11 e atribua um SSID à interface.

   router<config>#interface dot11radio0

   router<config-if>#no shutdown

   router<config-if>#ssid open

   O tipo de autenticação aberta pode ser configurado em combinação com a autenticação do endereço MAC. Nesse caso, o ponto de acesso força todos os dispositivos clientes a executar a autenticação de endereço MAC antes de terem permissão para se unir à rede.

   A autenticação aberta também pode ser configurada junto com a autenticação EAP. O ponto de acesso força todos os dispositivos clientes a executar a autenticação EAP antes que eles tenham permissão para ingressar na rede. Para o nome da lista, especifique a lista de métodos de autenticação.

   Um ponto de acesso configurado para autenticação EAP força todos os dispositivos clientes associados a executar a autenticação EAP. Os dispositivos clientes que não usam EAP não podem usar o ponto de acesso.

2. Vincule o SSID a uma VLAN.

   Para habilitar o SSID nessa interface, vincule o SSID à VLAN no modo de configuração de SSID.

   router<config-ssid>vlan 1

3. Configure o SSID com autenticação aberta.

   router<config-ssid>#authentication open

4. Configure a interface de rádio para a chave WEP como opcional.

   router<config>#encryption vlan 1 mode WEP optional

5. Ative a VLAN na interface de rádio.

   router<config>#interface Dot11Radio 0.1

   router<config-subif>#encapsulation dot1Q 1

   router<config-subif>#bridge-group 1

Configure o servidor DHCP interno para os clientes sem fio desta VLAN

Digite estes comandos no modo de configuração global para configurar o servidor DHCP interno para os clientes sem fio desta VLAN:

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

No modo de configuração do pool DHCP, digite estes comandos:

- rede 10.1.0.0 255.255.0.0
- default-router 10.1.1.1

Configurar a autenticação 802.1x/EAP

Esse tipo de autenticação fornece o mais alto nível de segurança para a sua rede sem fio. Com o Protocolo de Autenticação Extensível (EAP - Extensible Authentication Protocol) usado para interagir com um servidor RADIUS compatível com EAP, o ponto de acesso ajuda um dispositivo de cliente sem fio e o servidor RADIUS a executar autenticação mútua e derivar uma chave WEP unicast dinâmica. O servidor RADIUS envia a chave WEP ao ponto de acesso, que a usa para todos os sinais de dados unicast que envia para o cliente ou recebe dele.

Consulte Autenticação EAP para obter mais informações.

Este exemplo usa esta configuração:

- Nome do SSID: leap
- VLAN 2
- Intervalo do servidor DHCP interno: 10.2.0.0/16

Este exemplo usa a autenticação LEAP como o mecanismo para autenticar o cliente sem fio.

Observação: consulte Cisco Secure ACS for Windows v3.2 With EAP-TLS Machine Authentication para configurar o EAP-TLS.

Observação: consulte Configuração do Cisco Secure ACS para Windows v3.2 com autenticação de máquina PEAP-MS-CHAPv2 para configurar PEAP-MS-CHAPv2.

Observação: entenda que toda a configuração desses tipos de EAP envolve principalmente as alterações de configuração no lado do cliente e no lado do servidor de autenticação. A configuração no roteador sem fio ou no ponto de acesso permanece mais ou menos a mesma para todos esses tipos de autenticação.

Observação: como mencionado inicialmente, essa configuração usa o servidor RADIUS local no ISR sem fio para autenticar clientes sem fio com autenticação 802.1x.

Conclua estas ações no roteador:

1. Configurar o Integrated Routing and Bridging (IRB) e Configurar o Grupo de Bridge
2. Configurar a interface virtual com bridge (BVI)
3. Configurar o servidor RADIUS local para autenticação EAP
4. Configurar o SSID para autenticação 802.1x/EAP
5. Configure o servidor DHCP interno para os clientes sem fio desta VLAN

Configurar o Integrated Routing and Bridging (IRB) e Configurar o Grupo de Bridge

Conclua estas ações:

1. Ative o IRB no roteador.

   router<configure>#bridge irb

   Observação: se todos os tipos de segurança forem configurados em um único roteador, basta ativar o IRB globalmente apenas uma vez no roteador. Ele não precisa ser habilitado para cada tipo de autenticação individual.

2. Defina um grupo de bridge.

   Este exemplo usa o número 2 do grupo de pontes.

   router<configure>#bridge 2

3. Escolha o protocolo spanning tree para o grupo de pontes.

   Aqui, o protocolo de spanning tree IEEE é configurado para esse grupo de bridge.

   router<configure>#bridge 2 protocol ieee

4. Escolha o protocolo spanning tree para o grupo de pontes.

   Aqui, o protocolo de spanning tree IEEE é configurado para esse grupo de bridge.

   router<configure>#bridge 2 protocol ieee

5. Habilite um BVI para aceitar e rotear pacotes roteáveis que são recebidos de seu grupo de ponte correspondente.

   Este exemplo permite que o BVI aceite e roteie pacotes IP.

   router<configure>#bridge 2 route ip

Configurar a interface virtual com bridge (BVI)

Conclua estas ações:

1. Configure o BVI.

   Configure o BVI ao atribuir o número correspondente do grupo de pontes ao BVI. Cada grupo de bridge pode ter apenas um correspondente BVI. Este exemplo atribui o grupo de pontes número 2 ao BVI.

   router<configure>#interface BVI <2>

2. Atribua um endereço IP ao BVI.

   router<config-if>#ip address 10.2.1.1 255.255.0.0

   router<config-if>#no shut

Configurar o servidor RADIUS local para autenticação EAP

Como mencionado anteriormente, este documento usa o servidor RADIUS local no roteador com reconhecimento de conexão sem fio para autenticação EAP.

1. Ative o modelo de controle de acesso AAA (authentication, authorization, and accounting).

   router<configure>#aaa new-model

2. Crie um grupo de servidores read-eap para o servidor RADIUS.

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

3. Crie uma lista de métodos eap_methods que liste o método de autenticação usado para autenticar o usuário de logon AAA. Atribua a lista de métodos a este grupo de servidores.

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

4. Ative o roteador como um servidor de autenticação local e entre no modo de configuração

para o autenticador.

router<configure>#radius-server local

5. No modo de configuração do servidor Radius, adicione o roteador como um cliente AAA do servidor de autenticação local.

   router<config-radsrv>#nas 10.2.1.1 key Cisco

6. Configure o usuário user1 no servidor Radius local.

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

7. Especifique o host do servidor RADIUS.

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

   Observação: essa chave deve ser a mesma que a especificada no comando nas no modo de configuração radius-server.

Configurar o SSID para autenticação 802.1x/EAP

A configuração da interface de rádio e do SSID associado para 802.1x/EAP envolve a configuração de vários parâmetros sem fio no roteador, que incluem o SSID, o modo de criptografia e o tipo de autenticação. Este exemplo usa o SSID chamado leap.

1. Ative a interface de rádio.

   Para habilitar a interface de rádio, vá para o modo de configuração da interface de rádio DOT11 e atribua um SSID à interface.

   router<config>#interface dot11radio0

   router<config-if>#no shutdown

   router<config-if>#ssid leap

2. Vincule o SSID a uma VLAN.

   Para habilitar o SSID nessa interface, vincule o SSID à VLAN no modo de configuração de SSID.

   router<config-ssid>#vlan 2

3. Configure o SSID com autenticação 802.1x/LEAP.

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

4. Configure a interface de rádio para gerenciamento dinâmico de chaves.

   router<config>#encryption vlan 2 mode ciphers wep40

5. Ative a VLAN na interface de rádio.

   router<config>#interface Dot11Radio 0.2

   router<config-subif>#encapsulation dot1Q 2

   router<config-subif>#bridge-group 2

Configure o servidor DHCP interno para os clientes sem fio desta VLAN

Digite estes comandos no modo de configuração global para configurar o servidor DHCP interno para os clientes sem fio desta VLAN:

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

No modo de configuração do pool DHCP, digite estes comandos:

- rede 10.2.0.0 255.255.0.0
- default-router 10.2.1.1

Gerenciamento de chave WPA

O Wi-Fi Protected Access é uma melhoria de segurança interoperável baseada em padrões que aumenta significativamente o nível de proteção de dados e de controle de acesso para sistemas LAN sem fio atuais e futuros.

Consulte Gerenciamento de chaves WPA para obter mais informações.

O gerenciamento de chaves WPA suporta dois tipos de gerenciamento mutuamente exclusivos: WPA-Pre-Shared Key (WPA-PSK) e WPA (com EAP).

Configuração do WPA-PSK

A WPA-PSK é usada como um tipo de gerenciamento de chave em uma LAN sem fio onde a autenticação baseada em 802.1x não está disponível. Nessas redes, você deve configurar uma chave pré-compartilhada no ponto de acesso. Você pode inserir a chave pré-compartilhada como caracteres ASCII ou hexadecimais. Se você inserir a chave como caracteres ASCII, insira entre 8 e 63 caracteres, e o ponto de acesso expandirá a chave com o processo descrito no Padrão de Criptografia Baseado em Senha (RFC2898). Se você inserir a chave como caracteres hexadecimais, deverá inserir 64 caracteres hexadecimais.

Este exemplo usa esta configuração:

- nome SSID: wpa-shared
- VLAN 3

- Intervalo do servidor DHCP interno: 10.3.0.0/16

Conclua estas ações no roteador:

1. Configurar o Integrated Routing and Bridging (IRB) e Configurar o Grupo de Bridge
2. Configurar a interface virtual com bridge (BVI)
3. Configurar o SSID para autenticação WPA-PSK
4. Configure o servidor DHCP interno para os clientes sem fio desta VLAN

Configurar o Integrated Routing and Bridging (IRB) e Configurar o Grupo de Bridge

Conclua estas ações:

1. Ative o IRB no roteador.

   router<configure>#bridge irb

   Observação: se todos os tipos de segurança forem configurados em um único roteador, basta ativar o IRB globalmente apenas uma vez no roteador. Ele não precisa ser habilitado para cada tipo de autenticação individual.

2. Defina um grupo de bridge.

   Este exemplo usa o número de grupo de ponte 3.

   router<configure>#bridge 3

3. Escolha o protocolo spanning tree para o grupo de pontes.

   O protocolo de spanning tree IEEE está configurado para esse grupo de bridge.

   router<configure>#bridge 3 protocol ieee

4. Habilite um BVI para aceitar e rotear pacotes roteáveis recebidos de seu grupo de ponte correspondente.

   Este exemplo permite que o BVI aceite e roteie pacotes IP.

   router<configure>#bridge 3 route ip

Configurar a interface virtual com bridge (BVI)

Conclua estas ações:

1. Configure o BVI.

   Configure o BVI ao atribuir o número correspondente do grupo de pontes ao BVI. Cada grupo de bridge pode ter apenas um correspondente BVI. Este exemplo atribui o grupo de

ponte número 3 ao BVI.

router<configure>#interface BVI <2>

2. Atribua um endereço IP ao BVI.

   router<config-if>#ip address 10.3.1.1 255.255.0.0

   router<config-if>#no shut

Configurar o SSID para autenticação WPA-PSK

Conclua estas ações:

1. Ative a interface de rádio.

   Para habilitar a interface de rádio, vá para o modo de configuração da interface de rádio DOT11 e atribua um SSID à interface.

   router<config>#interface dot11radio0

   router<config-if>#no shutdown

   router<config-if>#ssid wpa-shared

2. Para habilitar o gerenciamento de chave WPA, primeiro configure a cifra de criptografia WPA para a interface VLAN. Este exemplo usa tkip como a cifra de criptografia..

   Digite este comando para especificar o tipo de gerenciamento de chave WPA na interface de rádio.

   router<config>#interface dot11radio0

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

3. Vincule o SSID a uma VLAN.

   Para habilitar o SSID nessa interface, vincule o SSID à VLAN no modo de configuração de SSID.

   router<config-ssid>vlan 3

4. Configure o SSID com autenticação WPA-PSK.

   Você precisa configurar a autenticação EAP aberta ou de rede primeiro no modo de configuração SSID para habilitar o gerenciamento de chave WPA. Este exemplo configura a autenticação aberta.

   router<config>#interface dot11radio0

   router<config-if>#ssid wpa-shared

router<config-ssid>#authentication open

Agora, habilite o gerenciamento de chave WPA no SSID. O tkip de cifra de gerenciamento de chave já está configurado para esta VLAN.

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

Configure a autenticação WPA-PSK no SSID.

router(config-if-ssid)#wpa-psk ascii 1234567890 !— 1234567890 é o valor da chave pré-compartilhada para este SSID. Certifique-se de que a mesma chave seja especificada para este SSID no lado do cliente.

5. Ative a VLAN na interface de rádio.

   router<config>#interface Dot11Radio 0.3

   router<config-subif>#encapsulation dot1Q 3

   router<config-subif>#bridge-group 3

Configure o servidor DHCP interno para os clientes sem fio desta VLAN

Digite estes comandos no modo de configuração global para configurar o servidor DHCP interno para os clientes sem fio desta VLAN:

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

No modo de configuração do pool DHCP, digite estes comandos:

- rede 10.3.0.0 255.255.0.0
- default-router 10.3.1.1

Configurar a autenticação WPA (com EAP)

Este é outro tipo de gerenciamento de chave WPA. Aqui, os clientes e o servidor de autenticação autenticam-se entre si com um método de autenticação EAP, e o cliente e o servidor geram uma chave mestra em pares (PMK). Com a WPA, o servidor gera a PMK dinamicamente e a passa para o access point, mas, com a WPA-PSK, você configura uma chave pré-compartilhada no cliente e no access point, e essa chave pré-compartilhada é usada como a PMK.

Consulte WPA com autenticação EAP para obter mais informações.

Este exemplo usa esta configuração:

- Nome SSID: wpa-dot1x

- VLAN 4
- Intervalo do servidor DHCP interno: 10.4.0.0/16

Conclua estas ações no roteador:

1. Configurar o Integrated Routing and Bridging (IRB) e Configurar o Grupo de Bridge
2. Configurar a interface virtual com bridge (BVI)
3. Configure o servidor RADIUS local para a autenticação WPA.
4. Configurar o SSID para WPA com autenticação EAP
5. Configure o servidor DHCP interno para os clientes sem fio desta VLAN

Configurar o Integrated Routing and Bridging (IRB) e Configurar o Grupo de Bridge

Conclua estas ações:

1. Ative o IRB no roteador.

   router<configure>#bridge irb

   Observação: se todos os tipos de segurança forem configurados em um único roteador, basta ativar o IRB globalmente apenas uma vez no roteador. Ele não precisa ser habilitado para cada tipo de autenticação individual.

2. Defina um grupo de Bridge.

   Este exemplo usa o número de grupo de ponte 4.

   router<configure>#bridge 4

3. Selecione o protocolo spanning tree para o grupo de pontes.

   Aqui, o protocolo de spanning tree IEEE é configurado para esse grupo de bridge.

   router<configure>#bridge 4 protocol ieee

4. Habilite um BVI para aceitar e rotear os pacotes roteáveis recebidos de seu grupo de ponte correspondente.

   Este exemplo permite que o BVI aceite e roteie pacotes IP.

   router<configure>#bridge 4 route ip

Configurar a interface virtual com bridge (BVI)

Conclua estas ações:

1. Configure o BVI.

   Configure o BVI ao atribuir o número correspondente do grupo de pontes ao BVI. Cada grupo de bridge pode ter apenas um BVI correspondente. Este exemplo atribui o grupo de pontes número 4 ao BVI.

   router<configure>#interface BVI <4>

2. Atribua um endereço IP ao BVI.

   router<config-if>#ip address 10.4.1.1 255.255.0.0

   router<config-if>#no shut

Configurar o servidor RADIUS local para autenticação WPA

Consulte a seção em Autenticação 802.1x/EAP para obter o procedimento detalhado.

Configurar o SSID para WPA com autenticação EAP

Conclua estas ações:

1. Ative a interface do rádio.

   Para habilitar a interface de rádio, vá para o modo de configuração da interface de rádio DOT11 e atribua um SSID à interface.

   router<config>#interface dot11radio0

   router<config-if>#no shutdown

   router<config-if>#ssid wpa-dot1x

2. Para habilitar o gerenciamento de chave WPA, primeiro configure a cifra de criptografia WPA para a interface VLAN. Este exemplo usa tkip como a cifra de criptografia..

   Digite este comando para especificar o tipo de gerenciamento de chave WPA na interface de rádio.

   router<config>#interface dot11radio0

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

3. Vincule o SSID a uma VLAN.

   Para habilitar o SSID nessa interface, vincule o SSID à VLAN no modo de configuração de SSID.

   vlan 4

4. Configure o SSID com a autenticação WPA-PSK.

Para configurar a interface de rádio para WPA com autenticação EAP, primeiro configure o SSID associado para EAP de rede.

router<config>#interface dot11radio0

router<config-if>#ssid wpa-shared

router<config-ssid>#authentication network eap eap_methods

5. Agora, habilite o gerenciamento de chave WPA no SSID. O tkip de cifra de gerenciamento de chave já está configurado para esta VLAN.

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

6. Ative a VLAN na interface de rádio.

   router<config>#interface Dot11Radio 0.4

   router<config-subif>#encapsulation dot1Q 4

   router<config-subif>#bridge-group 4

Configure o servidor DHCP interno para os clientes sem fio desta VLAN

Digite estes comandos no modo de configuração global para configurar o servidor DHCP interno para os clientes sem fio desta VLAN:

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

No modo de configuração do pool DHCP, digite estes comandos:

- rede 10.4.0.0 255.255.0.0
- default-router 10.4.1.1

Configurar o cliente sem fio para autenticação

Depois de configurar o ISR, configure o cliente sem fio para diferentes tipos de autenticação, conforme explicado, de modo que o roteador possa autenticar esses clientes sem fio e fornecer acesso à rede WLAN. Este documento usa o Cisco Aironet Desktop Utility (ADU) para a configuração do lado do cliente.

Configurar o cliente sem fio para a autenticação aberta

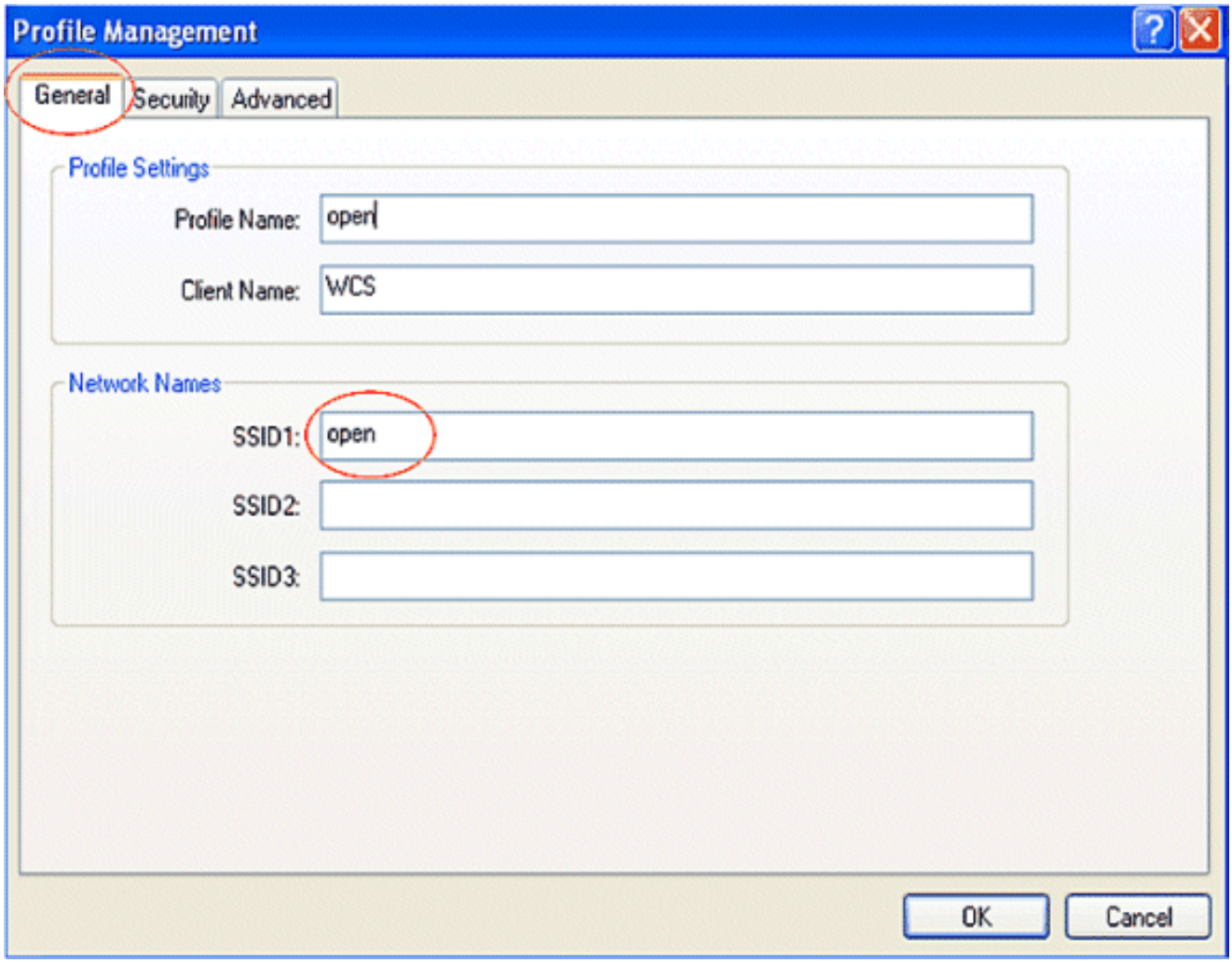
Conclua estes passos:

1. Na janela Gerenciamento de perfil na ADU, clique em Novo para criar um novo perfil.

Uma nova janela é exibida, na qual você pode definir a configuração da autenticação aberta. Na guia Geral, insira o Nome do perfil e o SSID que o adaptador cliente usa.

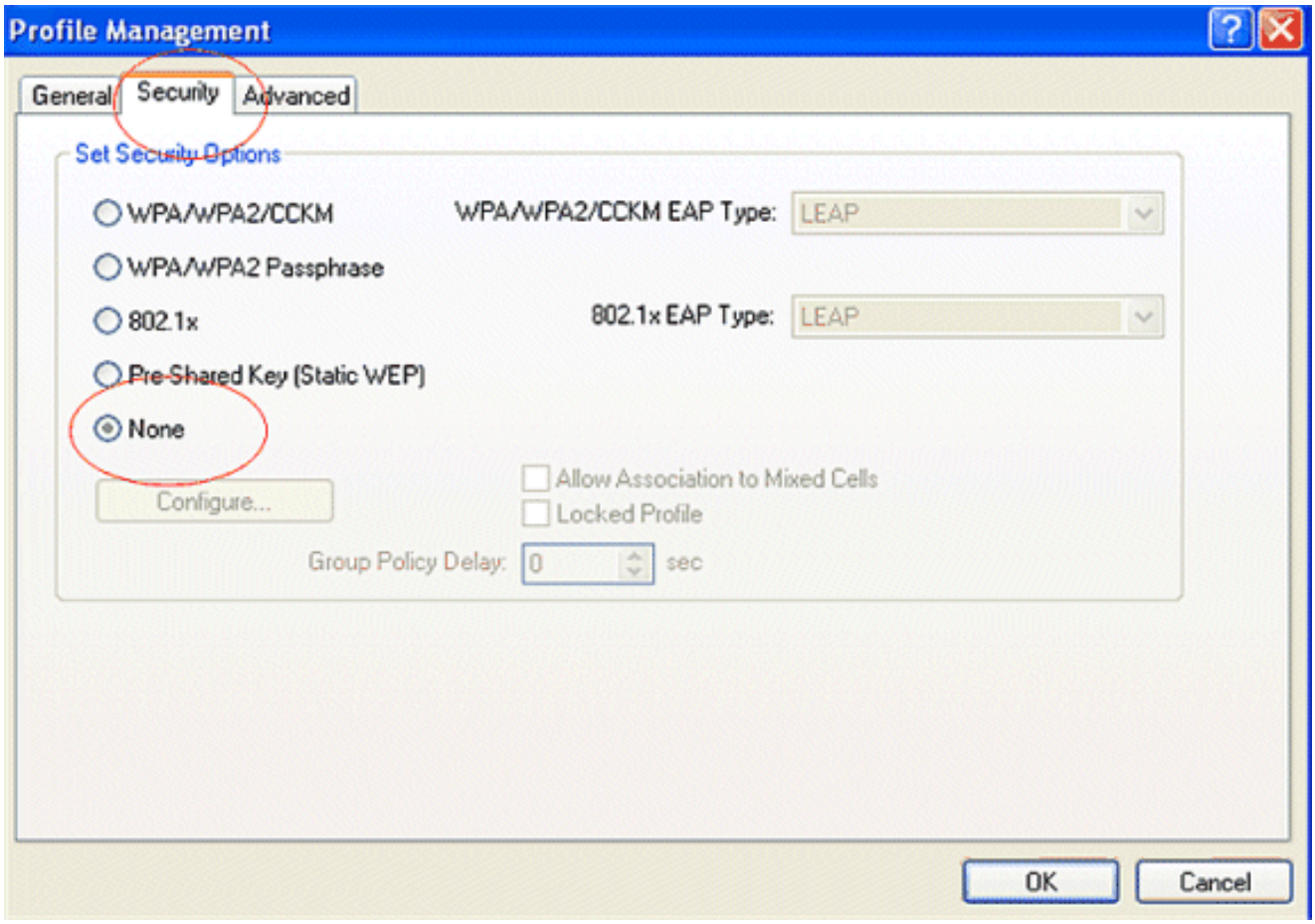
Neste exemplo, o nome do perfil e o SSID são abertos.

Observação: o SSID deve corresponder ao SSID configurado no ISR para autenticação aberta.

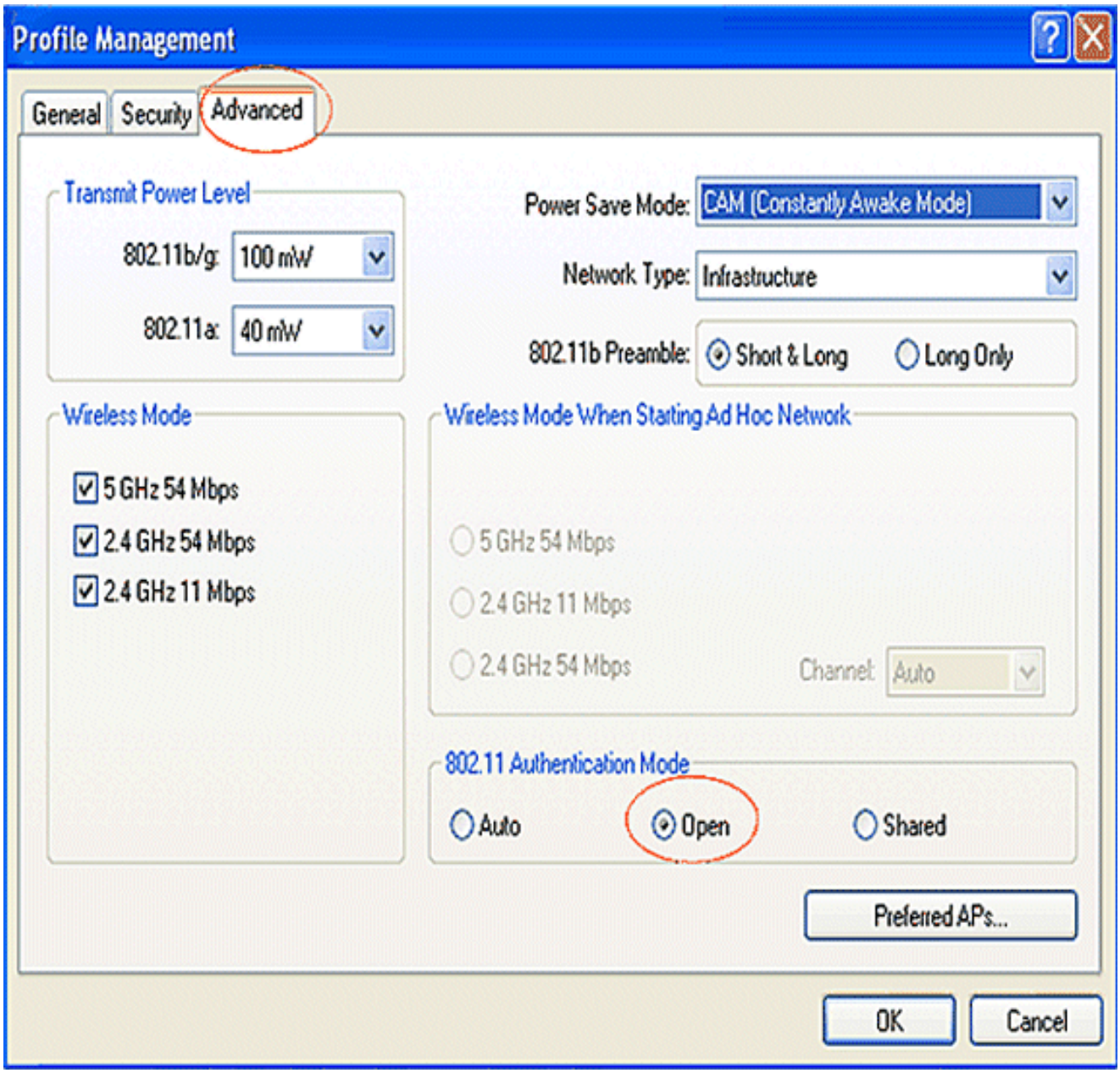


2. Clique na guia Security e deixe a opção de segurança como None para criptografia WEP. Como este exemplo usa a WEP como opcional, a definição desta opção como None permitirá que o cliente se associe e se comunique com êxito com a rede WLAN.

   Clique em OK.

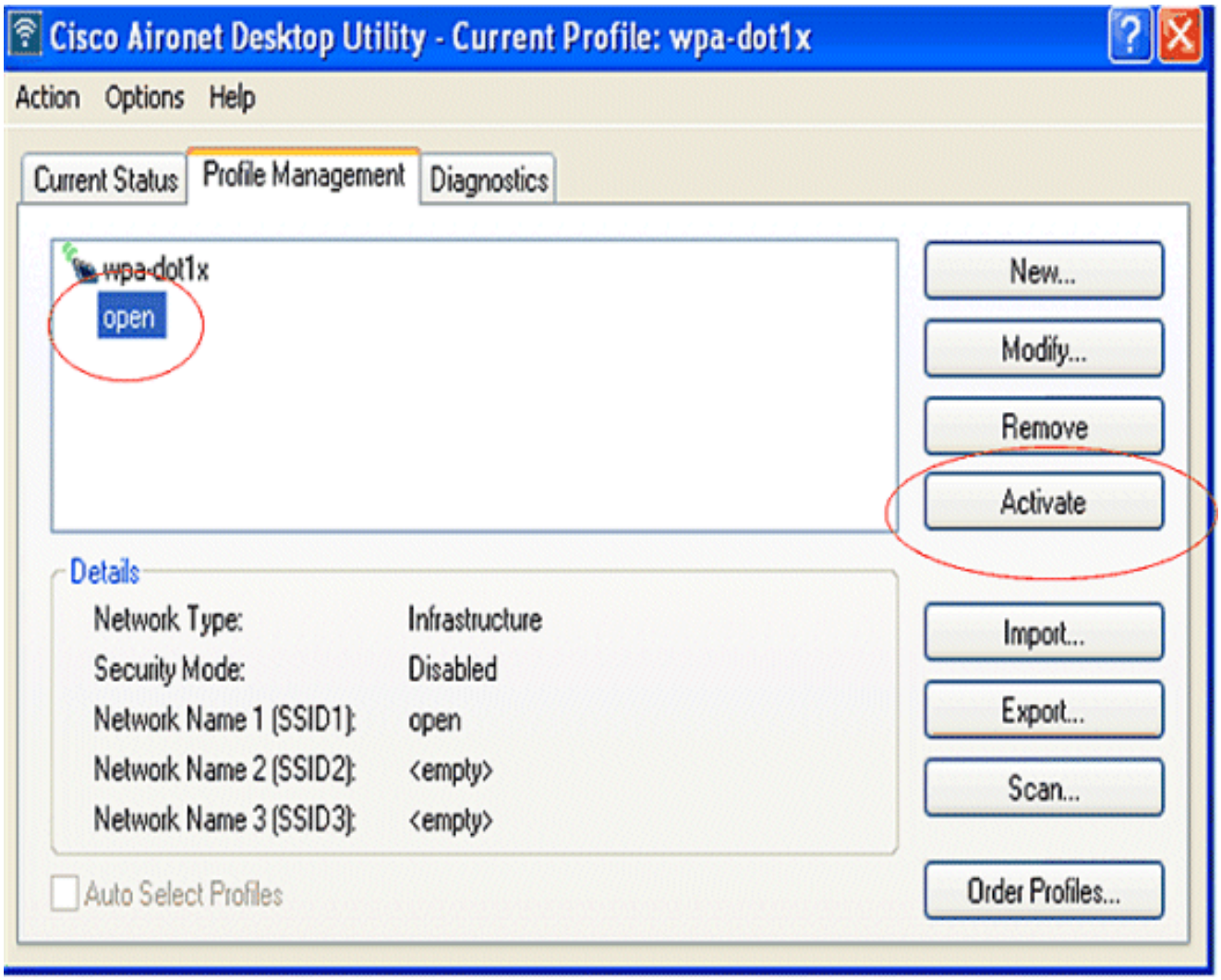


3. Selecione a janela Avançado na guia Gerenciamento de perfil e defina o Modo de autenticação 802.11 como Abrir para a autenticação aberta.

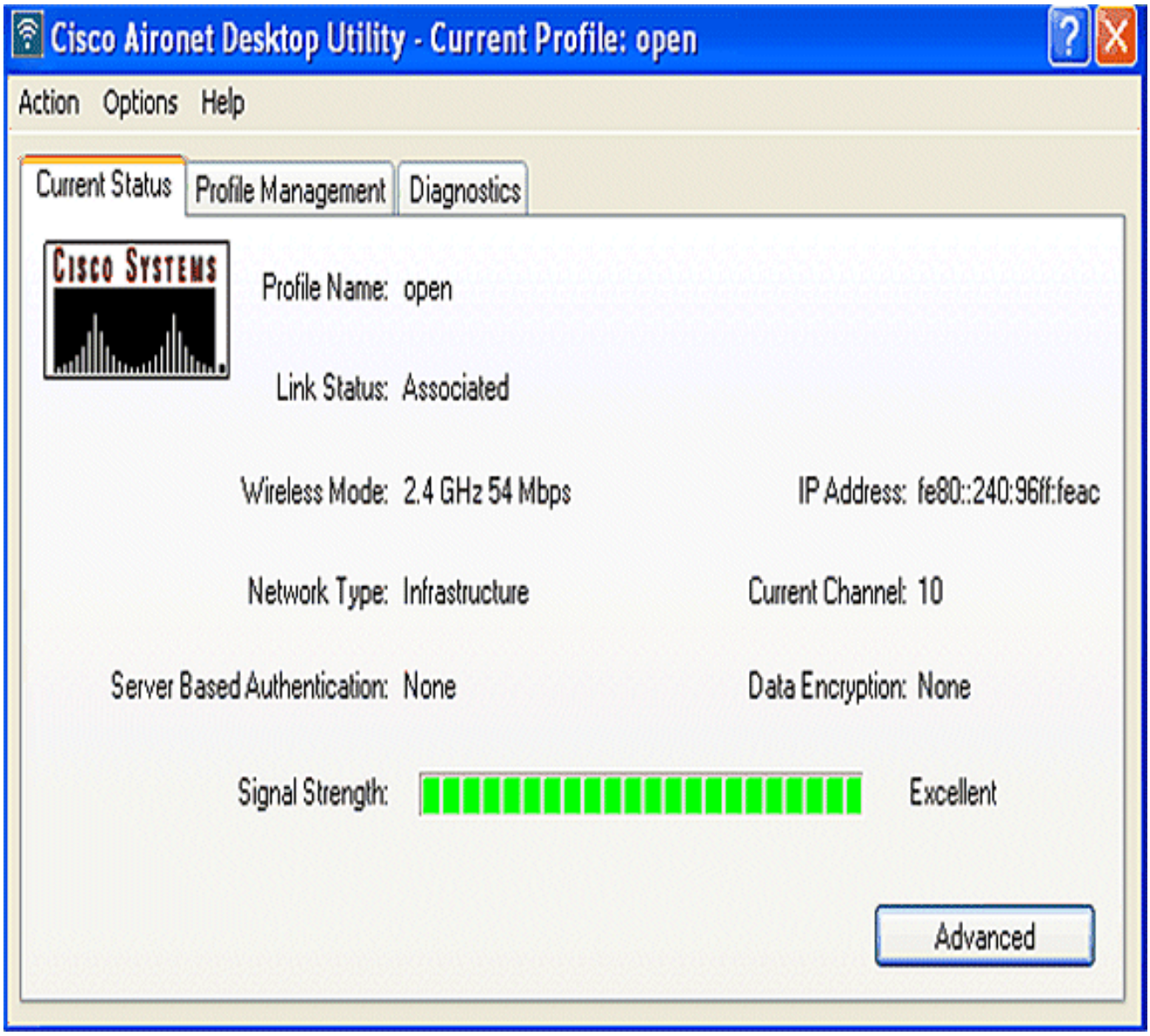


Use esta seção para confirmar se a sua configuração funciona corretamente.

1. Depois que o perfil do cliente for criado, clique em Ativate na guia Profile Management para ativar o perfil.



2. Verifique o status ADU para uma autenticação bem-sucedida.



Configurar o cliente sem fio para a autenticação 802.1x/EAP

Conclua estes passos:

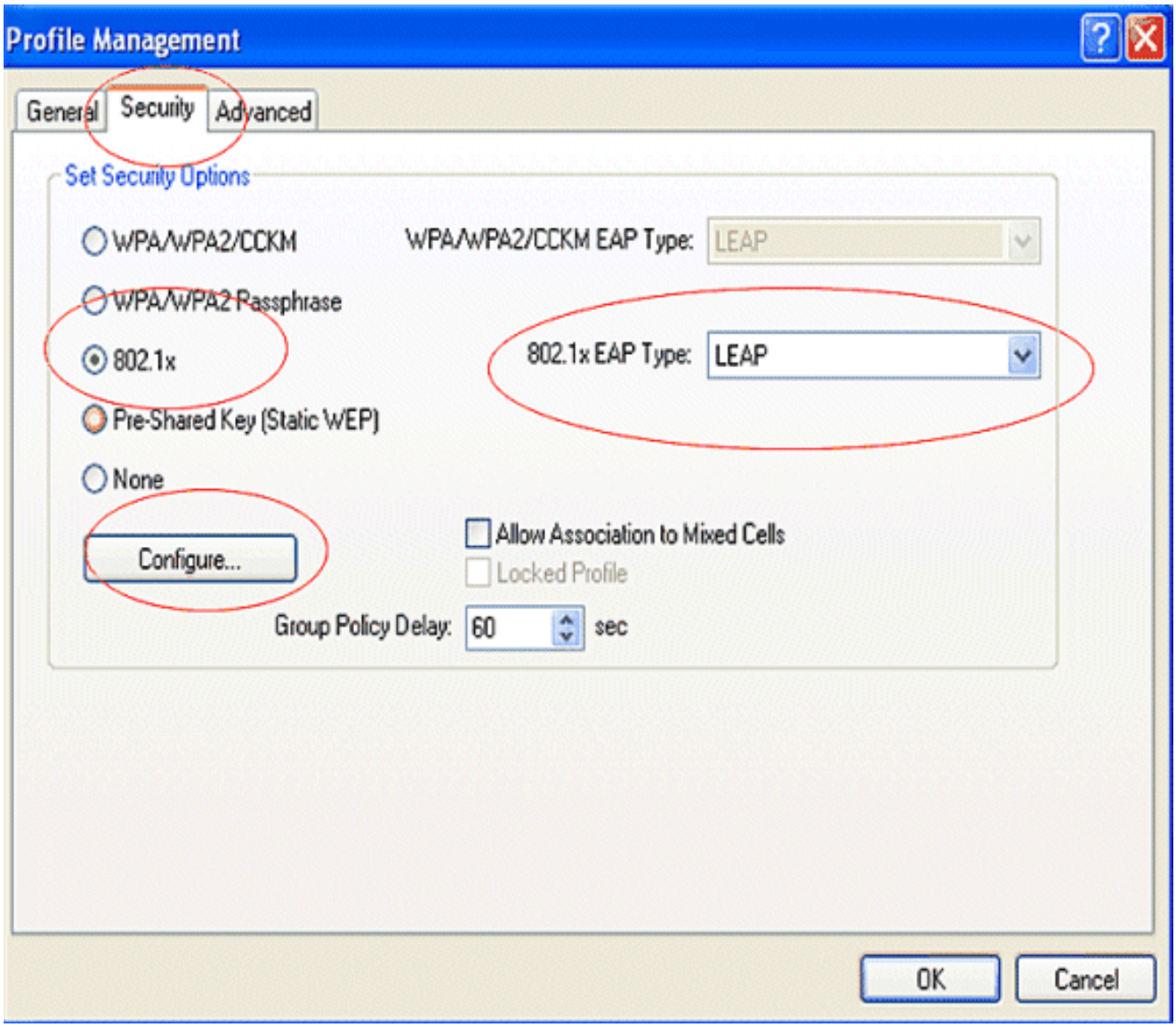
1. Na janela Gerenciamento de perfil na ADU, clique em Novo para criar um novo perfil.

   Uma nova janela é exibida, na qual você pode definir a configuração da autenticação aberta. Na guia Geral, insira o Nome do perfil e o SSID que o adaptador cliente usa.

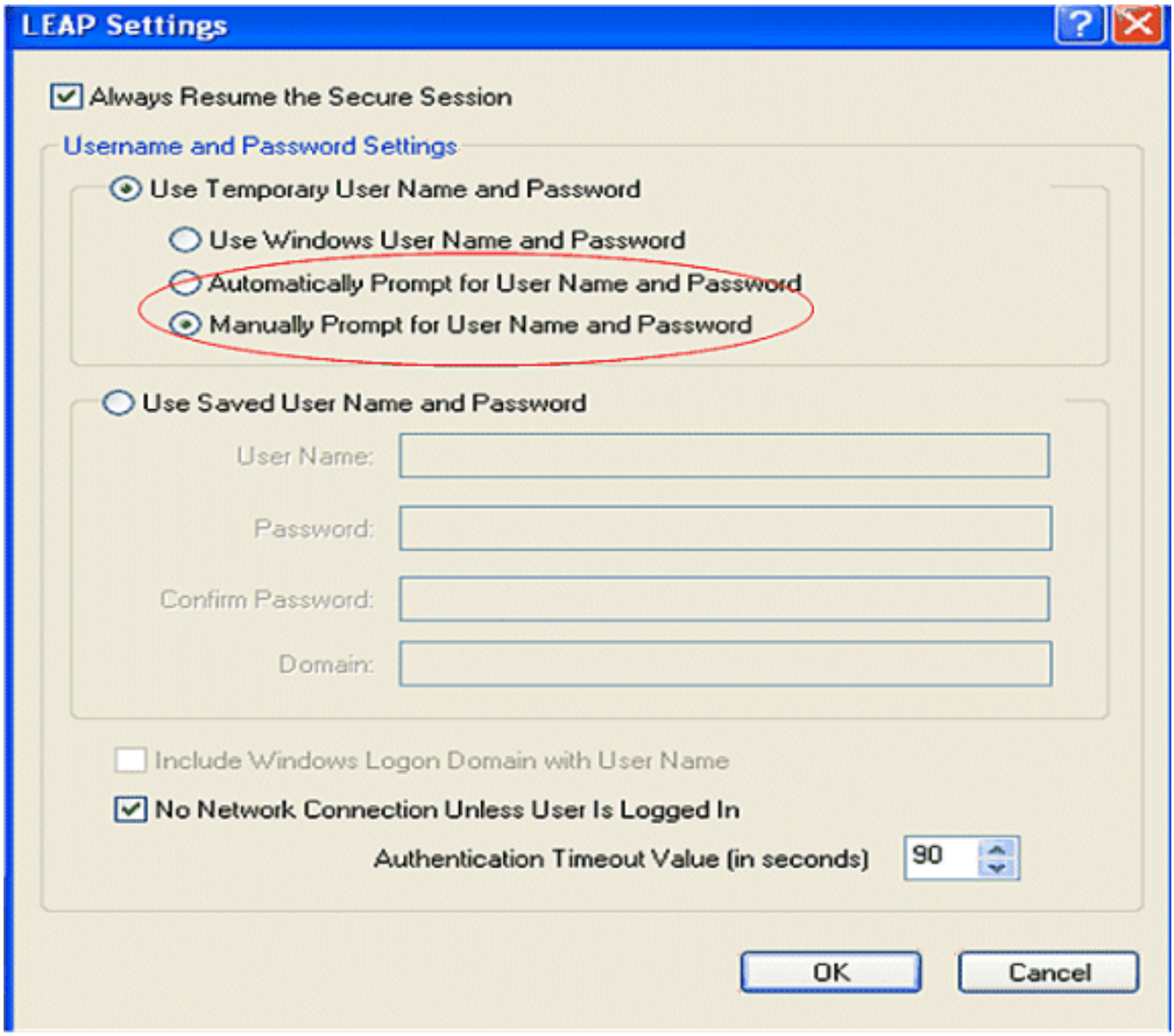
   Neste exemplo, o nome do perfil e o SSID são leap.

2. Em Gerenciamento de perfil, clique na guia Segurança, defina a opção de segurança como 802.1x e escolha o tipo de EAP apropriado. Este documento usa LEAP como o tipo de EAP para autenticação. Agora, clique em Configure para configurar as definições de nome de usuário e senha LEAP.

   Observação: Observação: o SSID deve corresponder ao SSID configurado no ISR para autenticação 802.1x/EAP.

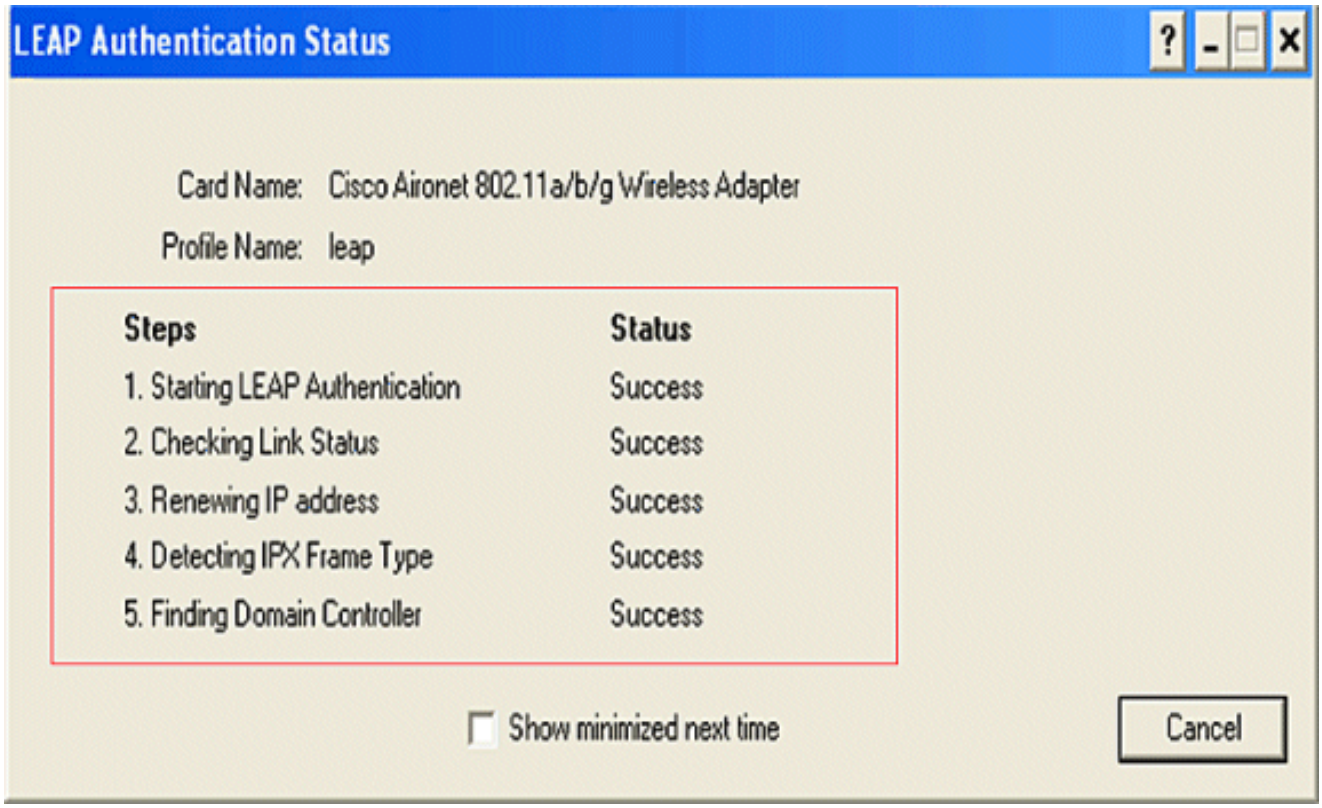


3. Nas configurações de nome de usuário e senha, este exemplo opta por Solicitar manualmente o nome de usuário e a senha para que o cliente seja solicitado a inserir o nome de usuário e a senha corretos enquanto o cliente tenta se conectar à rede. Click OK.



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

- Depois que o perfil do cliente for criado, clique em Ativate na guia Profile Management para ativar o perfil leap. Você será solicitado a fornecer o nome de usuário e a senha do leap. Este exemplo usa o nome de usuário e a senha user1. Click OK.
- Você pode observar o cliente se autenticar com êxito e receber um endereço IP do servidor DHCP configurado no roteador.



Configurar o cliente sem fio para a autenticação WPA-PSK

Conclua estes passos:

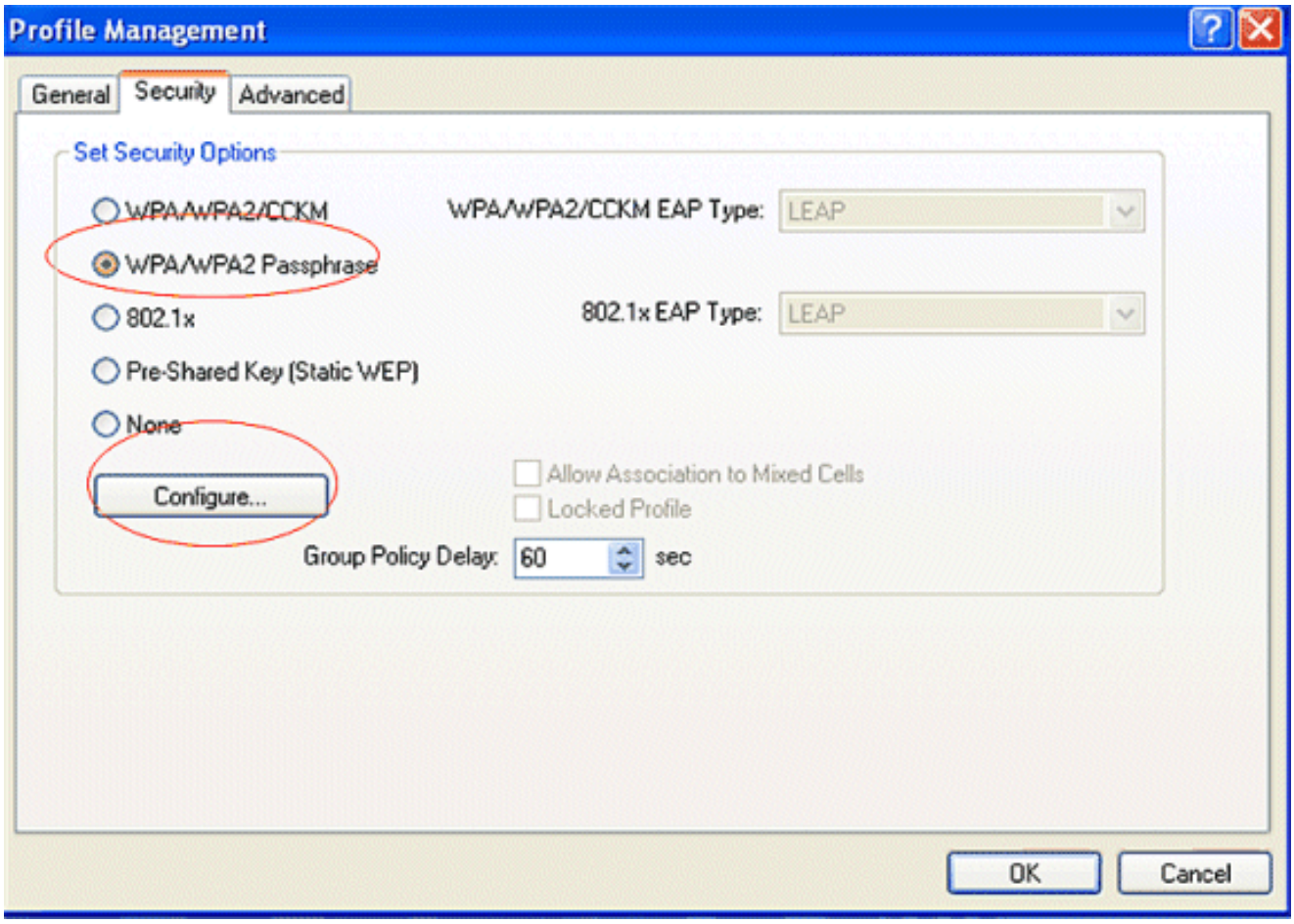
1. Na janela Gerenciamento de perfil na ADU, clique em Novo para criar um novo perfil.

   Uma nova janela é exibida, na qual você pode definir a configuração da autenticação aberta. Na guia General, insira o Profile Name e o SSID que o adaptador cliente usa.

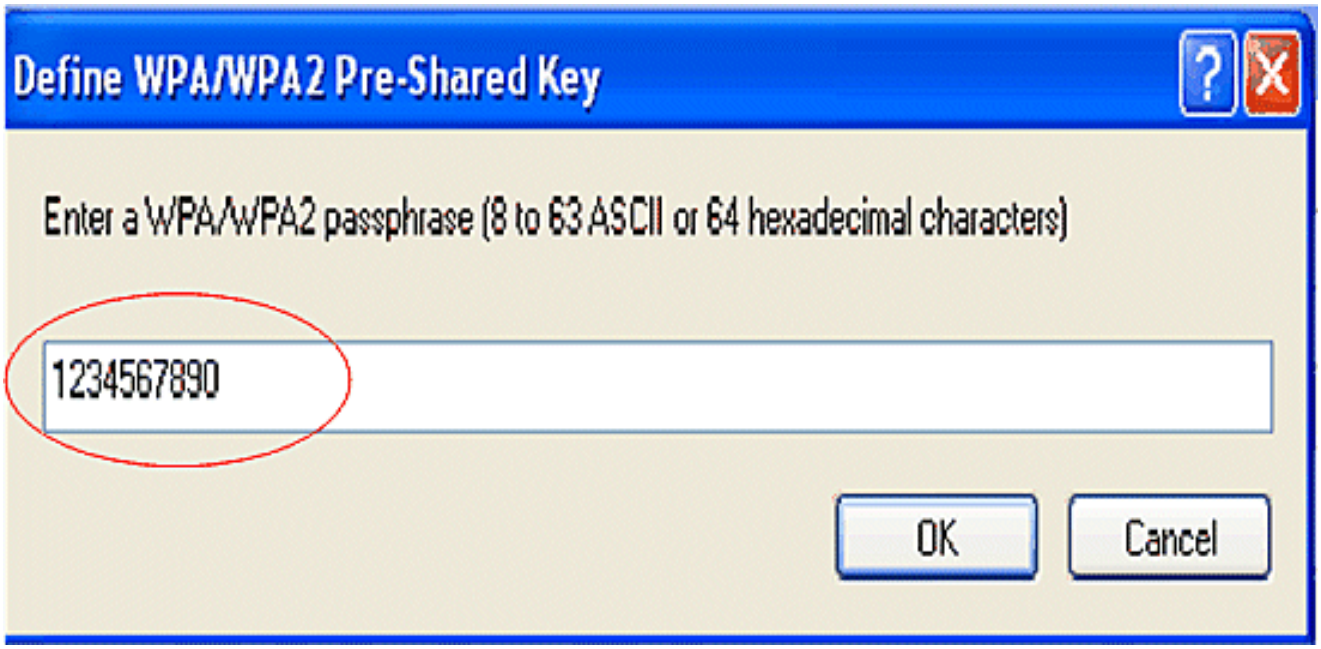
   Neste exemplo, o nome do perfil e o SSID são wpa-shared.

   Observação: o SSID deve corresponder ao SSID configurado no ISR para autenticação WPA-PSK.

2. Em Gerenciamento de perfil, clique na guia Segurança e defina a opção de segurança como Senha WPA/WPA2. Agora, clique em Configure para configurar a senha WPA.



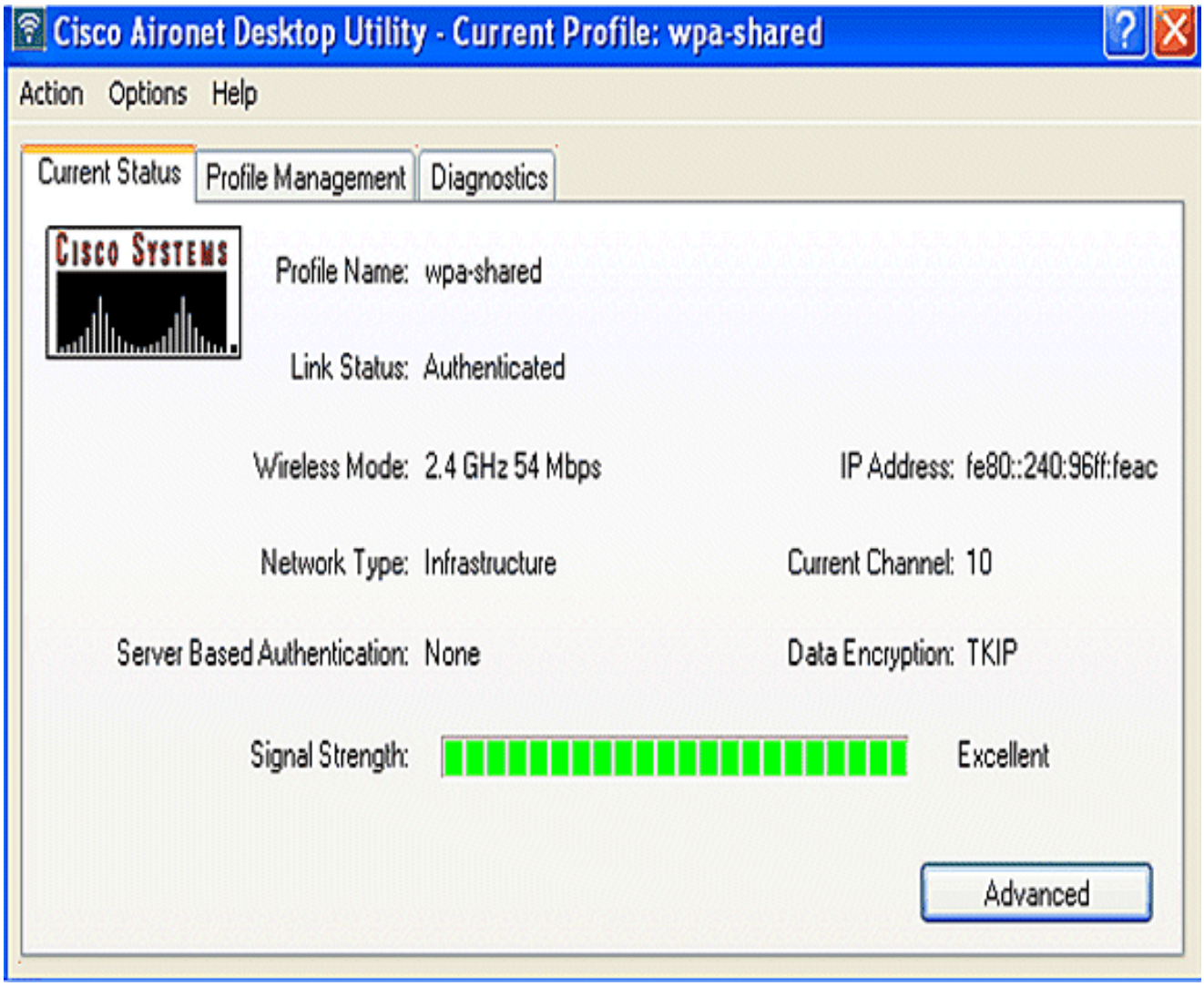
3. Defina uma chave pré-compartilhada WPA. A chave deve ter de 8 a 63 caracteres ASCII. Click OK.



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

- Depois que o perfil do cliente for criado, clique em Ativate na guia Profile Management para ativar o perfil wpa-shared.

- Verifique o ADU para obter uma autenticação bem-sucedida.



Configurar o cliente sem fio para a autenticação WPA (com EAP)

Conclua estes passos:

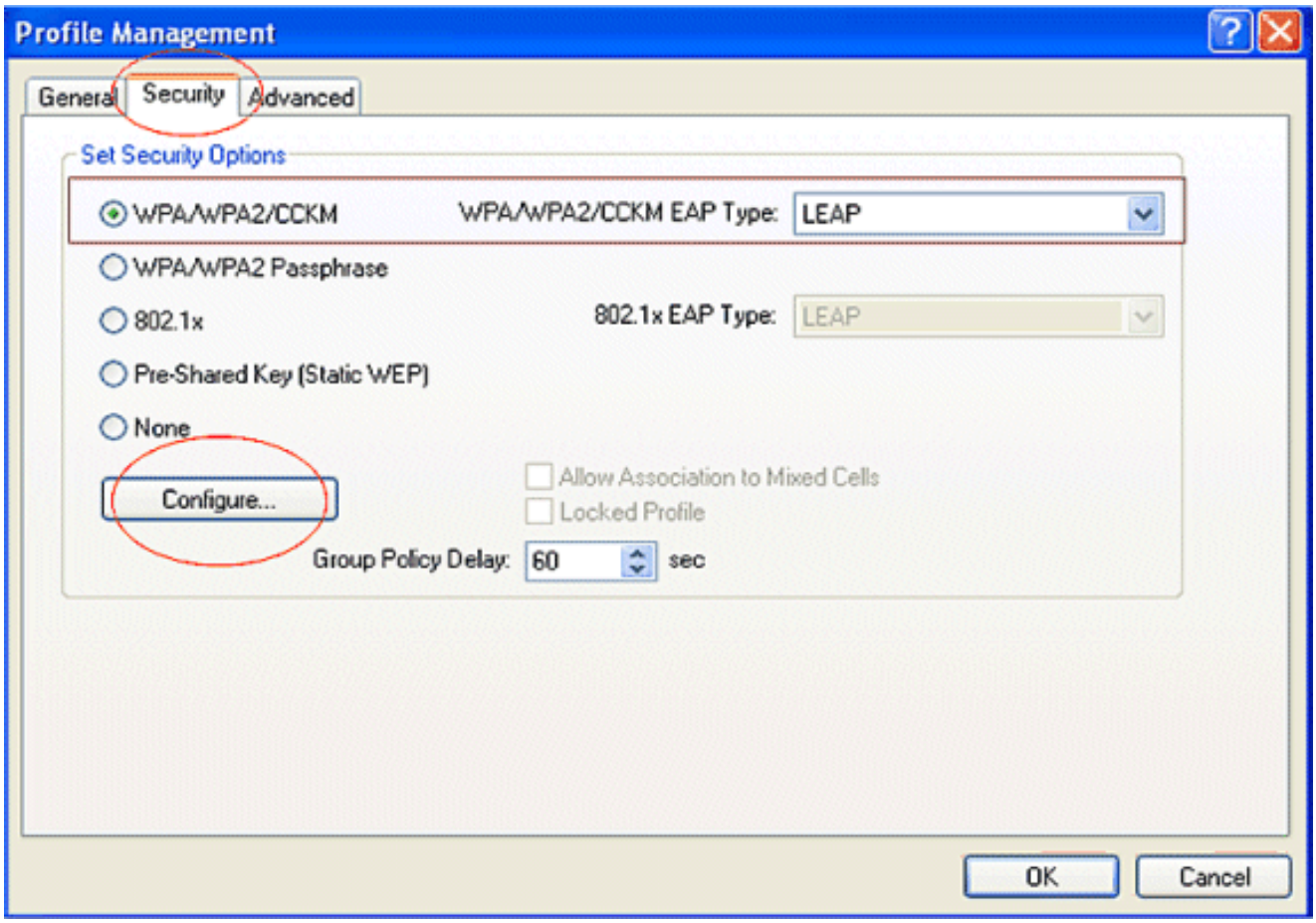
1. Na janela Gerenciamento de perfil na ADU, clique em Novo para criar um novo perfil.

   Uma nova janela é exibida, na qual você pode definir a configuração da autenticação aberta. Na guia General, insira o Profile Name e o SSID que o adaptador cliente usa.

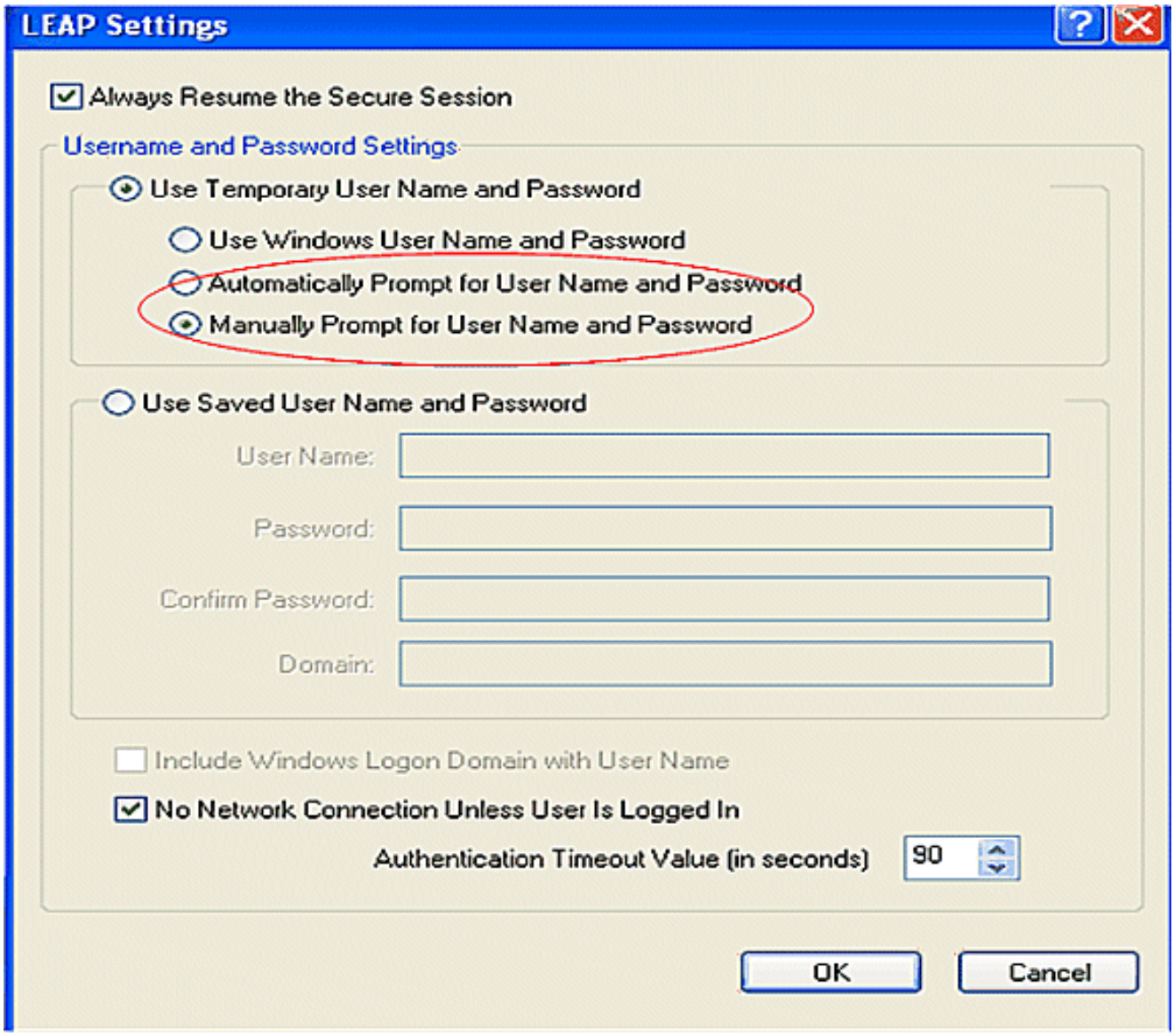
   Neste exemplo, o nome do perfil e o SSID são wpa-dot1x.

   Observação: o SSID deve corresponder ao SSID configurado no ISR para autenticação WPA (com EAP).

2. Em Gerenciamento de perfil, clique na guia Segurança, defina a opção de segurança como WPA/WPA2/CCKM e escolha o tipo de EAP WPA/WPA2/CCKM apropriado. Este documento usa LEAP como o tipo de EAP para autenticação. Agora, clique em Configure para configurar as definições de nome de usuário e senha LEAP.

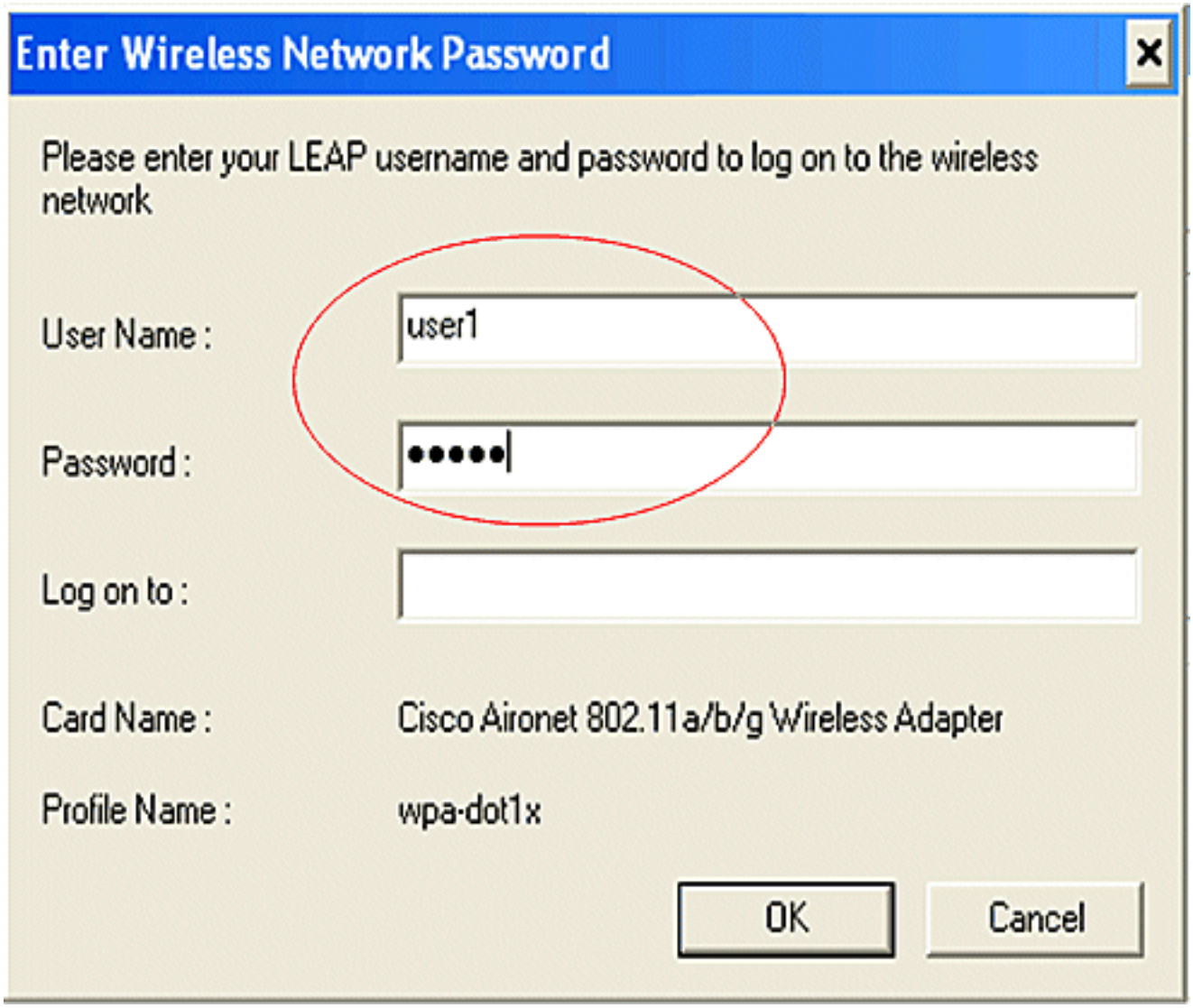


3. Na área Configurações de Nome de Usuário e Senha, este exemplo opta por Solicitar Manualmente Nome de Usuário e Senha para que o cliente seja solicitado a inserir o nome de usuário e a senha corretos enquanto o cliente tenta se conectar à rede. Click OK.

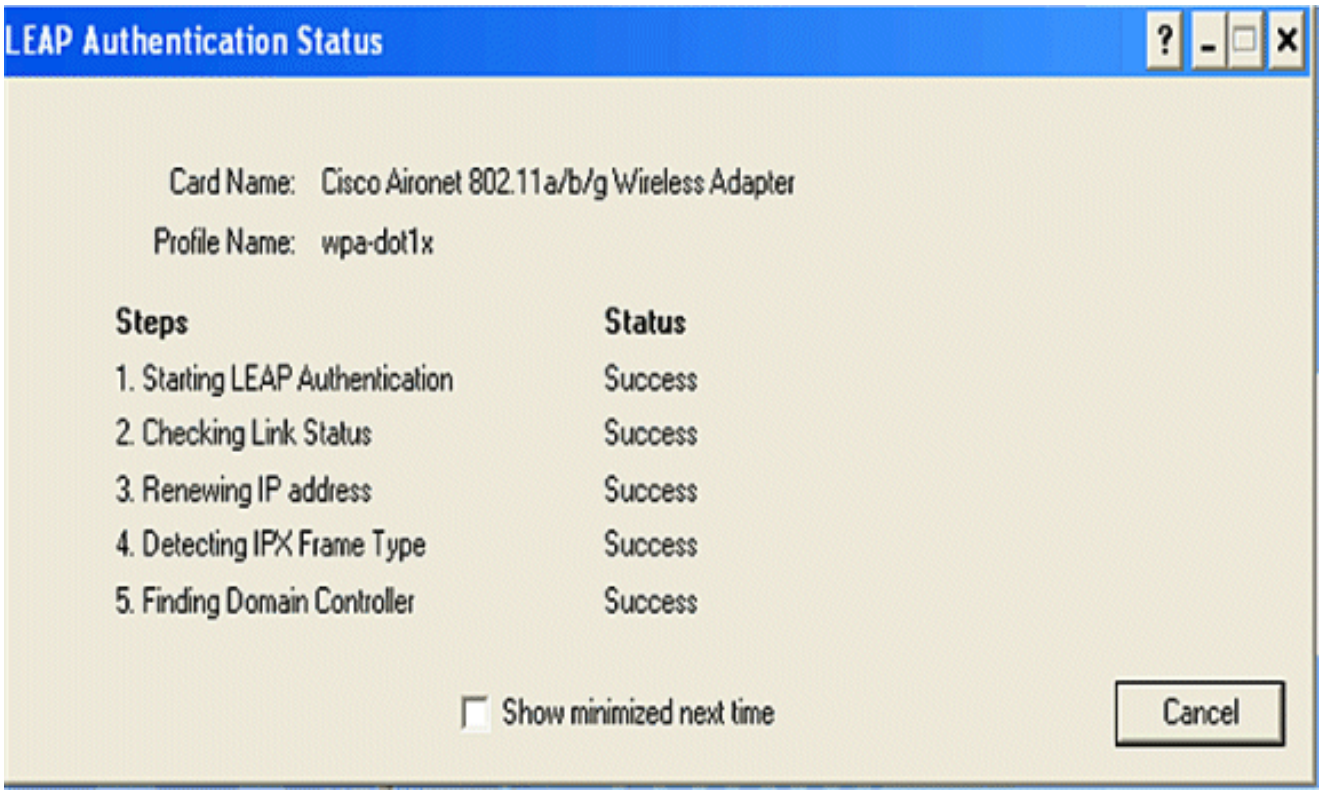


Use esta seção para confirmar se a sua configuração funciona corretamente.

1. Depois que o perfil do cliente for criado, clique em Ativate na guia Profile Management para ativar o perfil wpa-dot1x. Você será solicitado a fornecer o nome de usuário e a senha LEAP. Este exemplo usa nome de usuário e senha como user1. Click OK.



2. Você pode observar o cliente se autenticar com êxito.



O comando show dot11 associations da CLI do roteador exibe detalhes completos sobre o status de associação do cliente. Exemplo:

Roteador#mostrar associações dot11

<#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)
```

Troubleshooting

Comandos para Troubleshooting

Você pode usar esses comandos de depuração para solucionar problemas de 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 as autenticações de cliente com falha.

Informações Relacionadas

- Exemplos de Configuração de Autenticação em Controladores Wireless LAN
- Configurando VLANs em pontos de acesso
- Exemplo de configuração de roteador sem fio ISR 1800 com DHCP interno e autenticação aberta
- Guia de configuração do Cisco Wireless ISR e do ponto de acesso HWIC
- Exemplo de configuração de conectividade de LAN sem fio usando um ISR com criptografia WEP e autenticação LEAP
- Suporte Técnico e Documentação - Cisco Systems
- Configurando tipos de autenticação
- Exemplo de configuração de conectividade de LAN sem fio usando um ISR com criptografia WEP e autenticação LEAP

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.