Exemplo de configuração do acesso protegido por wi-fi 2 (WPA2)

Índice

Introdução

Este documento explica as vantagens do uso do Wi-Fi Protected Access 2 (WPA 2) em uma LAN Wireless (WLAN). O documento fornece dois exemplos de configuração sobre como executar o WPA 2 em uma WLAN. O primeiro exemplo mostra como configurar o WPA 2 no modo corporativo e o segundo exemplo configura o WPA 2 no modo pessoal.

Nota: O WPA trabalha com Extensible Authentication Protocol (EAP).

Pré-requisitos

Requisitos

Assegure-se de que você tenha o conhecimento básico destes assuntos antes que você tente

esta configuração:

- WPA
- Soluções da Segurança de WLAN**Nota:** Refira a Visão Geral de Segurança do Cisco Aironet Wireless LAN para obter informações sobre das soluções da Segurança de WLAN de Cisco.

Componentes Utilizados

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

- Access Point (AP) /Bridge do Cisco Aironet 1310G que executa o Software Release 12.3(2)JA de Cisco IOS®
- Adaptador cliente de Aironet 802.11a/b/g CB21AG que executa o firmware 2.5
- Utilitário de Desktop de Aironet (ADU) esse firmware 2.5 das corridas

Nota: Aironet CB21AG e o software do adaptador cliente PI21AG são incompatíveis com o outro software do adaptador de cliente Aironet. Você deve usar o ADU com os cartões CB21AG e PI21AG, e você deve usar o Aironet Client Utility (ACU) todos adaptadores de cliente Aironet restantes. Refira a instalação do adaptador cliente para obter mais informações sobre de como instalar o cartão CB21AG e o ADU.

Nota: Este documento usa um AP/bridge que tenha uma antena integrada. Se você usa um AP/bridge que exija uma antena externa, assegure-se de que as Antenas estejam conectadas ao AP/bridge. Se não, o AP/bridge é incapaz de conectar à rede Wireless. Determinados modelos do AP/bridge vêm com Antenas integradas, visto que outro precisam uma antena externa para a operação geral. Para obter informações sobre dos modelos do AP/bridge que vêm com interno ou as antenas externas, refira o guia/guia de produtos pedindo do dispositivo apropriado.

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.

Convenções

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

Informações de Apoio

O WPA é uma solução com base em padrões da Segurança do Wi-fi Alliance que enderece as vulnerabilidades em WLAN nativos. O WPA fornece a proteção de dados e o controle de acesso aumentados para sistemas de WLAN. O WPA endereça todas as vulnerabilidades conhecidas do Wired Equivalent Privacy (WEP) na implementação de segurança original do IEEE 802.11 e traz uma solução imediata da Segurança aos WLAN em ambientes da empresa e do escritório pequeno, escritório home (SOHO).

O WPA2 é a próxima geração de Segurança do Wi-fi. O WPA2 é a aplicação interoperáveis de Alliance do Wi-fi do padrão ratificado da IEEE 802.11i. O WPA2 executa o National Institute of Standards and Technology (NIST) - algoritmo de criptografia recomendado do Advanced Encryption Standard (AES) com o uso do modo contrário com protocolo do código de

autenticação de mensagens do Cipher Block Chaining (CCMP). O modo de contador AES é uma cifra de bloco que cifre blocos do 128-bit de dados em um momento com uma chave de criptografia do 128-bit. O algoritmo CCMP produz um código da integridade de mensagem (MIC) que forneça a autenticação de origem de dados e a integridade de dados para o wireless frame.

Nota: O CCMP é referido igualmente como CBC-MAC.

O WPA2 oferece um de mais alto nível da Segurança do que o WPA porque o AES oferece uma criptografia mais forte do que o Temporal Key Integrity Protocol (TKIP). O TKIP é o algoritmo de criptografia que o WPA usa. O WPA2 cria chaves de sessão frescas em cada associação. As chaves de criptografia que são usadas para cada cliente na rede são originais e específicas a esse cliente. Finalmente, cada pacote que é enviado sobre o ar é cifrado com uma chave original. A Segurança é aumentada com o uso de uma chave de criptografia nova e original porque não há nenhuma reutilização chave. O WPA é considerado ainda seguro e o TKIP não foi quebrado. Contudo, Cisco recomenda essa transição de clientes ao WPA2 o mais cedo possível.

O WPA e o WPA2 ambos apoiam o modo dois de operação:

- Modo de empreendimento
- Modo pessoal

Este documento discute a aplicação destes dois modos com o WPA2.

Apoio WPA2 com equipamento de Aironet Cisco

O WPA2 é apoiado neste equipamento:

- Série de Aironet 1130AG AP e série 1230AG AP
- Aironet 1100 séries AP
- Aironet 1200 séries AP
- Aironet 1300 séries AP

Nota: Equipe estes AP com os rádios 802.11g e use o Cisco IOS Software Release 12.3(2)JA ou Mais Recente.

O WPA2 e o AES são apoiados igualmente sobre:

- O 1200 Series de Aironet transmite por rádio os módulos com os part numbers AIR-RM21A e AIR-RM22A**Nota:** O módulo de rádio de Aironet 1200 com o part number AIR-RM20A não apoia o WPA2.
- Adaptadores cliente de Aironet 802.11a/b/g com versão de firmware 2.5

Nota: O Produtos do Cisco Aironet série 350 não apoia o WPA2 porque seu apoio da falta AES dos rádios.

Nota: Os bridges Wireless do Cisco Aironet série 1400 não apoiam o WPA2 ou o AES.

Configurar no modo de empreendimento

O modo de empreendimento do termo refere o Produtos que é testado para ser interoperáveis no modo da chave pré-compartilhada (PSK) e do IEEE 802.1X de operação para a autenticação. O 802.1x é considerado ser mais seguro do que alguns dos framework de autenticação do legado devido a sua flexibilidade a favor de uma variedade de mecanismos da autenticação e algoritmos

de criptografia mais fortes. O WPA2 no modo de empreendimento executa a autenticação em duas fases. A configuração da autenticação aberta ocorre na primeira fase. A segunda fase é autenticação do 802.1x com um dos métodos de EAP. O AES fornece o mecanismo de criptografia.

No modo de empreendimento, os clientes e os Authentication Server autenticam-se com o uso de um método de autenticação de EAP, e o cliente e servidor gerencie por pares um chave mestre (PMK). Com WPA2, o server gerencie o PMK dinamicamente e passa o PMK ao AP.

Esta seção discute a configuração que é necessária para executar o WPA2 no modo de empreendimento de operação.

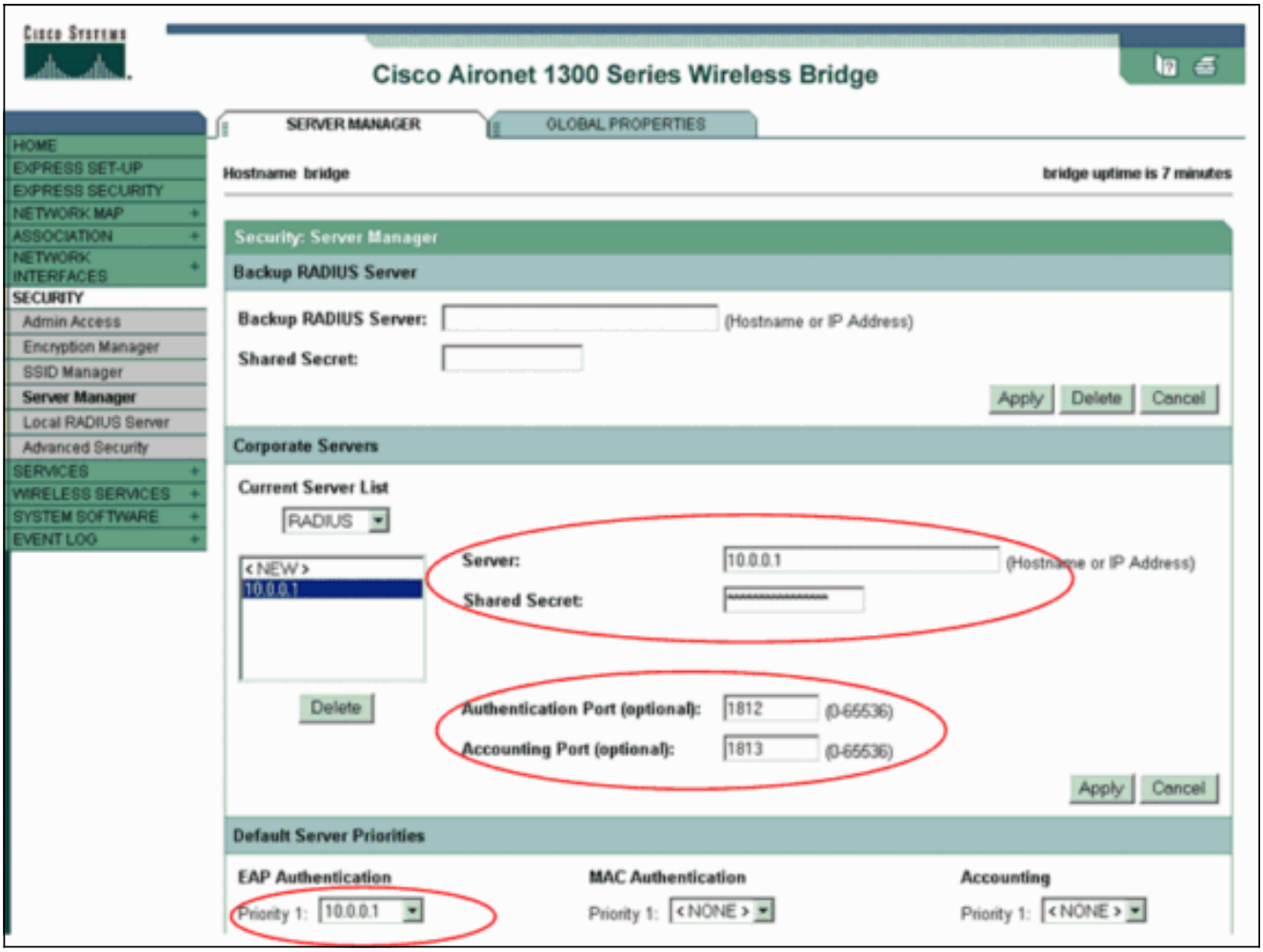
Instalação de rede

Nesta instalação, um AP/bridge de Aironet 1310G que seja executado protocolo extensible authentication da leve Cisco (PULO) autentica um usuário com um adaptador cliente WPA 2-compatible. O gerenciamento chave ocorre com o uso do WPA2, em que a criptografia AES-CCMP é configurada. O AP é configurado como um servidor Radius local que execute a autenticação de leap. Você deve configurar o adaptador cliente e o AP a fim executar esta instalação. As seções configuram o AP e configuram a mostra do adaptador cliente a configuração no AP e no adaptador cliente.

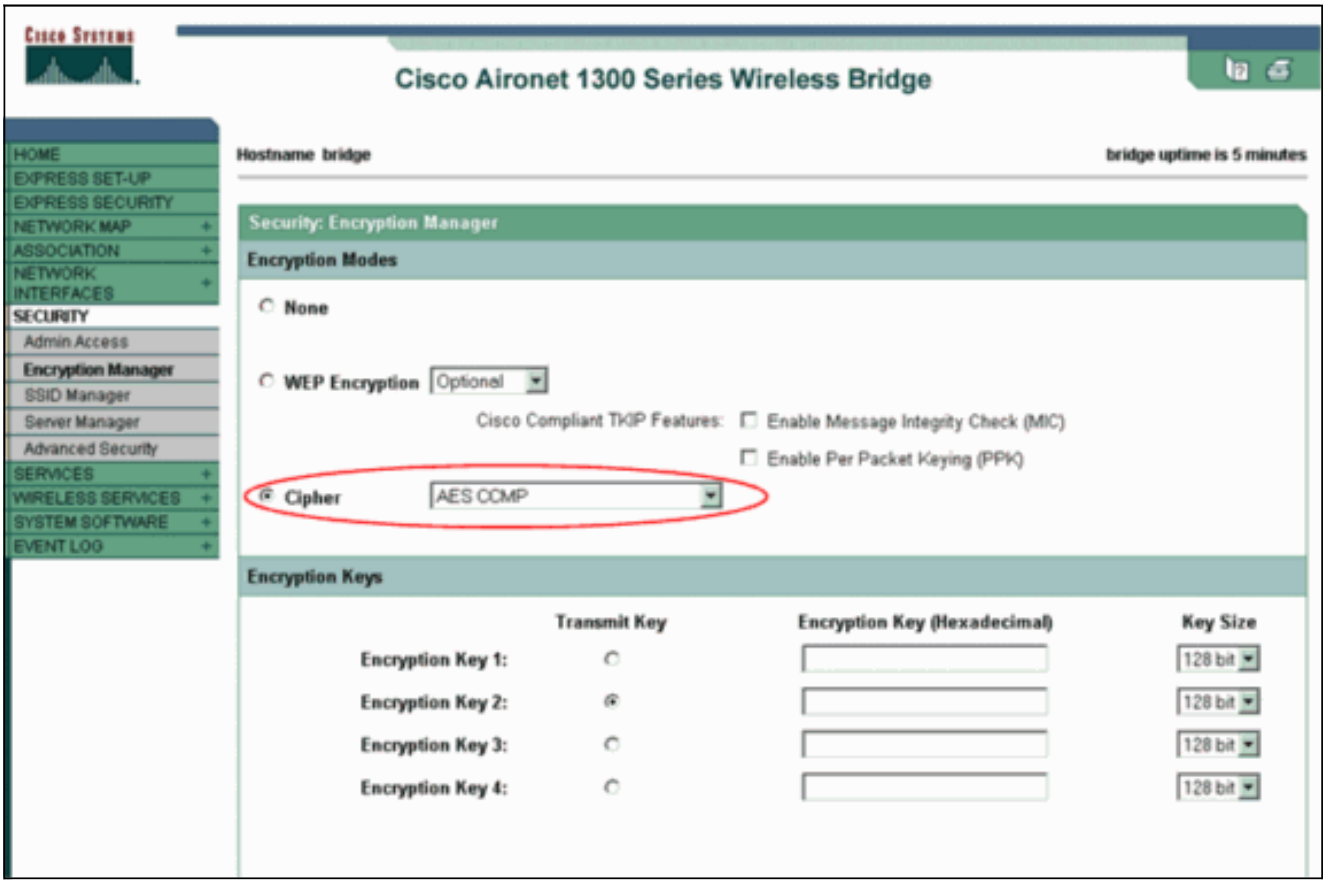
Configurar o AP

Termine estas etapas para configurar o AP usando o GUI:

1. Configurar o AP como um servidor Radius local que execute a autenticação de leap.Escolha a **Segurança > o gerenciador do servidor no** menu à esquerda e defina o endereço IP de Um ou Mais Servidores Cisco ICM NT, as portas, e o segredo compartilhado do servidor Radius.Porque esta configuração configura o AP como um servidor Radius local, use o endereço IP de Um ou Mais Servidores Cisco ICM NT do AP. Use as portas 1812 e 1813 para a operação local do servidor Radius.Na área de prioridades do server do padrão, defina a prioridade da autenticação de EAP do padrão como 10.0.0.1.**Nota:** 10.0.0.1 é o servidor Radius
local.

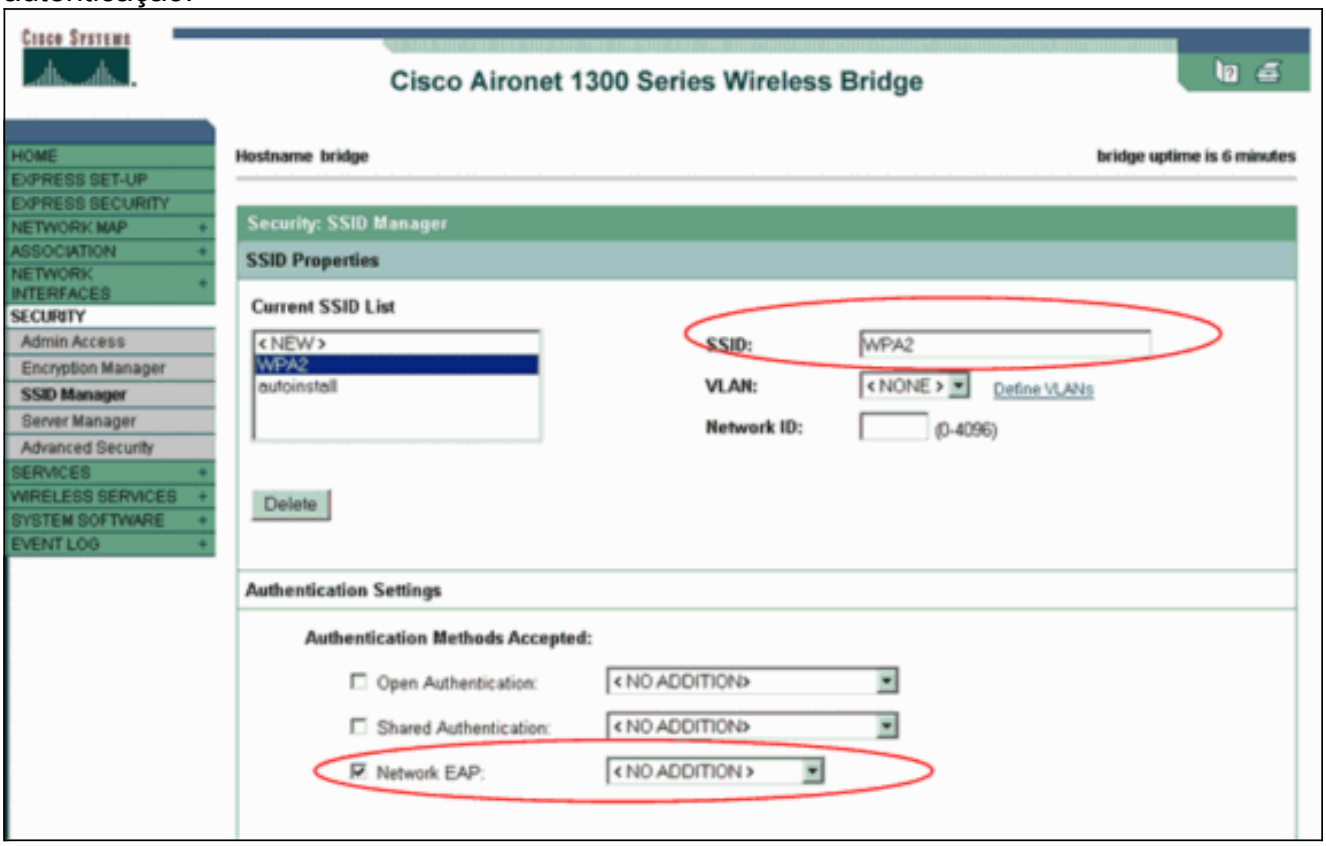


2. Escolha a **Segurança > o gerenciador de criptografia do** menu à esquerda e termine estas etapas:Do menu da cifra, escolha **AES CCMP**.Esta opção permite a criptografia de AES com o uso do modo contrário com CBC-
MAC.



Clique em Apply.

3. Escolha a **Segurança > o gerenciador de SSID** e crie um Service Set Identifier (SSID) novo para o uso com o WPA2.Verifique a **caixa de verificação de EAP de rede na** área aceitada métodos de autenticação.

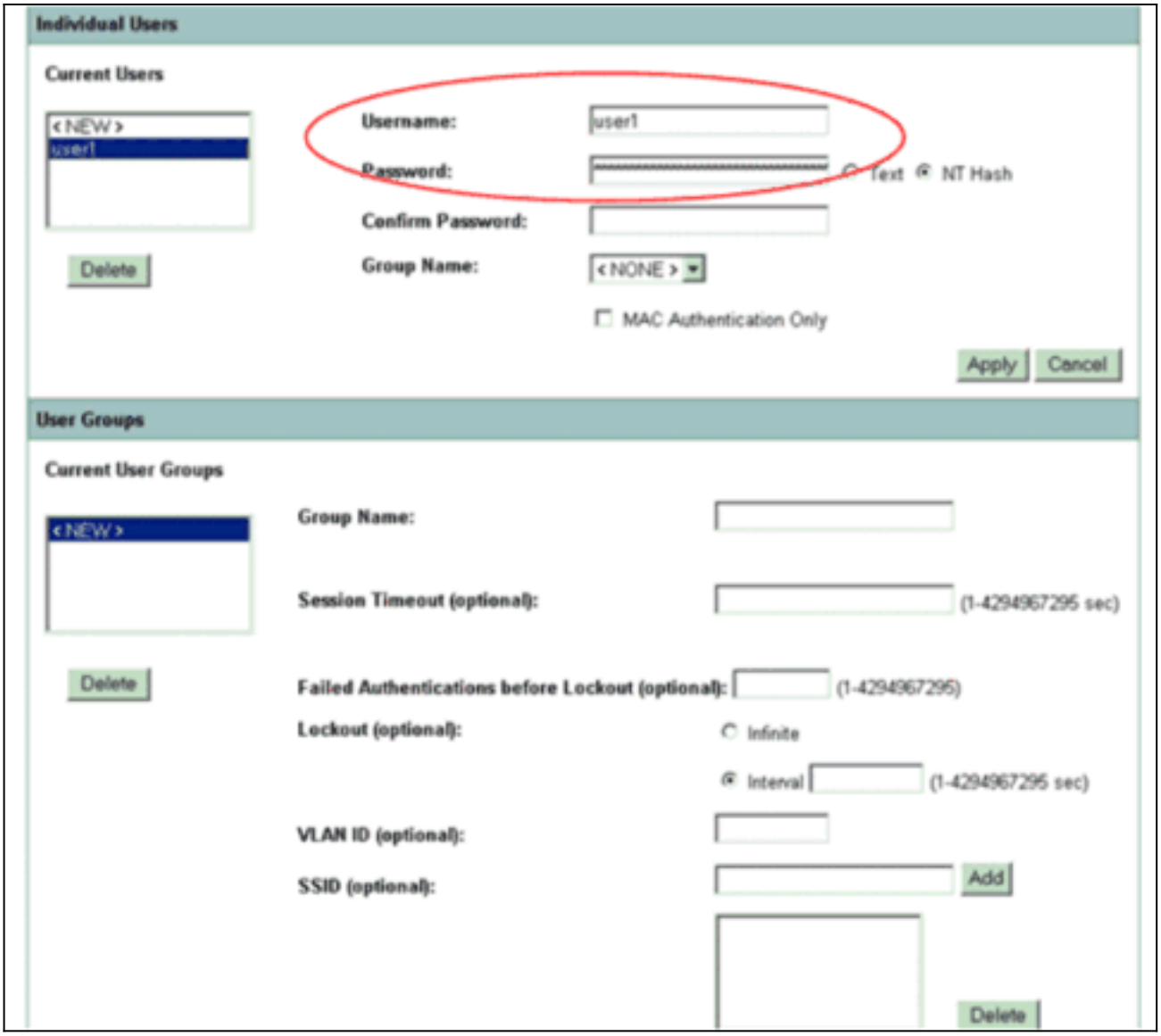


Nota: Use estas diretrizes quando você configura o tipo do autenticação na interface de rádio:Clientes Cisco — Use a rede EAP.Clientes da terceira (que incluem extensões compatível Cisco que o [CCX] - produtos em conformidade) — usa a autenticação aberta com EAP.Uma combinação de ambo o Cisco e clientes da terceira — escolha a rede EAP e a autenticação aberta com EAP.Enrole para baixo o indicador do gerenciador de SSID da Segurança a área autenticada do gerenciamento chave e termine estas etapas:Do menu do gerenciamento chave, escolha **imperativo**.Verifique a **caixa de verificação WPA** à direita.Clique em Apply.**Nota:** A definição dos VLAN é opcional. Se você define VLAN, os dispositivos do cliente que associam com o uso deste SSID estão agrupados no VLAN. Refira configurar VLAN para obter mais informações sobre de como executar VLAN.

4. Escolha a **Segurança > servidor Radius local** e termine estas etapas:Clique a aba **geral da instalação** situada na parte superior do indicador.Verifique a caixa de verificação do **PULO** e o clique **aplica-se**.Na área dos servidores do acesso de rede, defina o endereço IP de Um ou Mais Servidores Cisco ICM NT e o segredo compartilhado do servidor Radius.Para o servidor Radius local, use o endereço IP de Um ou Mais Servidores Cisco ICM NT do AP.

Clique em Apply.

5. Enrole para baixo o indicador geral da instalação a área de usuários individuais e defina os usuários individuais.A definição dos grupos de usuário é opcional.



Esta configuração define um usuário com o nome "user1" e uma senha. Também, a configuração seleciona a mistura de NT para a senha. Após conclusão do procedimento nesta seção, o AP está pronto para aceitar pedidos de autenticação dos clientes. A próxima etapa é configurar o adaptador cliente.

Configuração de CLI

Ponto de acesso

```
ap#show running-config Building configuration... . . .
aaa new-model !--- This command reinitializes the
authentication, !--- authorization and accounting
functions. ! ! aaa group server radius rad_eap server
10.0.0.1 auth-port 1812 acct-port 1813 !--- A server
group for RADIUS is created called "rad_eap" !--- that
uses the server at 10.0.0.1 on ports 1812 and 1813. . .
. aaa authentication login eap_methods group rad_eap !--
- Authentication [user validation] is to be done for !--
- users in a group called "eap_methods" who use server
group "rad_eap". . . . ! bridge irb ! interface
Dot11Radio0 no ip address no ip route-cache ! encryption
vlan 1 key 1 size 128bit 12345678901234567890123456
transmit-key !---This step is optional !--- This value
seeds the initial key for use with !--- broadcast
[255.255.255.255] traffic. If more than one VLAN is !---
used, then keys must be set for each VLAN. encryption
```

```
vlan 1 mode wep mandatory !--- This defines the policy
for the use of Wired Equivalent Privacy (WEP). !--- If
more than one VLAN is used, !--- the policy must be set
to mandatory for each VLAN. broadcast-key vlan 1 change
300 !--- You can also enable Broadcast Key Rotation for
each vlan and Specify the time after which Brodacst key
is changed. If it is disabled Broadcast Key is still
used but not changed. ssid cisco vlan 1 !--- Create a
SSID Assign a vlan to this SSID authentication open eap
eap_methods authentication network-eap eap_methods !---
Expect that users who attach to SSID "cisco" !---
request authentication with the type 128 Open EAP and
Network EAP authentication !--- bit set in the headers
of those requests, and group those users into !--- a
group called "eap_methods." ! speed basic-1.0 basic-2.0
basic-5.5 basic-11.0 rts threshold 2312 channel 2437
station-role root bridge-group 1 bridge-group 1
subscriber-loop-control bridge-group 1 block-unknown-
source no bridge-group 1 source-learning no bridge-group
1 unicast-flooding bridge-group 1 spanning-disabled . .
. interface FastEthernet0 no ip address no ip route-
cache duplex auto speed auto bridge-group 1 no bridge-
group 1 source-learning bridge-group 1 spanning-disabled
! interface BVI1 ip address 10.0.0.1 255.255.255.0 !---
The address of this unit. no ip route-cache ! ip
default-gateway 10.77.244.194 ip http server ip http
help-path
http://www.cisco.com/warp/public/779/smbiz/prodconfig/he
lp/eag/ivory/1100 ip radius source-interface BVI1 snmp-
server community cable RO snmp-server enable traps tty
radius-server local !--- Engages the Local RADIUS Server
feature. nas 10.0.0.1 key shared_secret !--- Identifies
itself as a RADIUS server, reiterates !--- "localness"
and defines the key between the server (itself) and the
access point(itself). ! group testuser !--- Groups are
optional. ! user user1 nthash password1 group testuser
!--- Individual user user user2 nthash password2 group
testuser !--- Individual user !--- These individual
users comprise the Local Database ! radius-server host
10.0.0.1 auth-port 1812 acct-port 1813 key shared_secret
!--- Defines where the RADIUS server is and the key
between !--- the access point (itself) and the server.
radius-server retransmit 3 radius-server attribute 32
include-in-access-req format %h radius-server
authorization permit missing Service-Type radius-server
vsa send accounting bridge 1 route ip ! ! line con 0
line vty 5 15 ! end
```

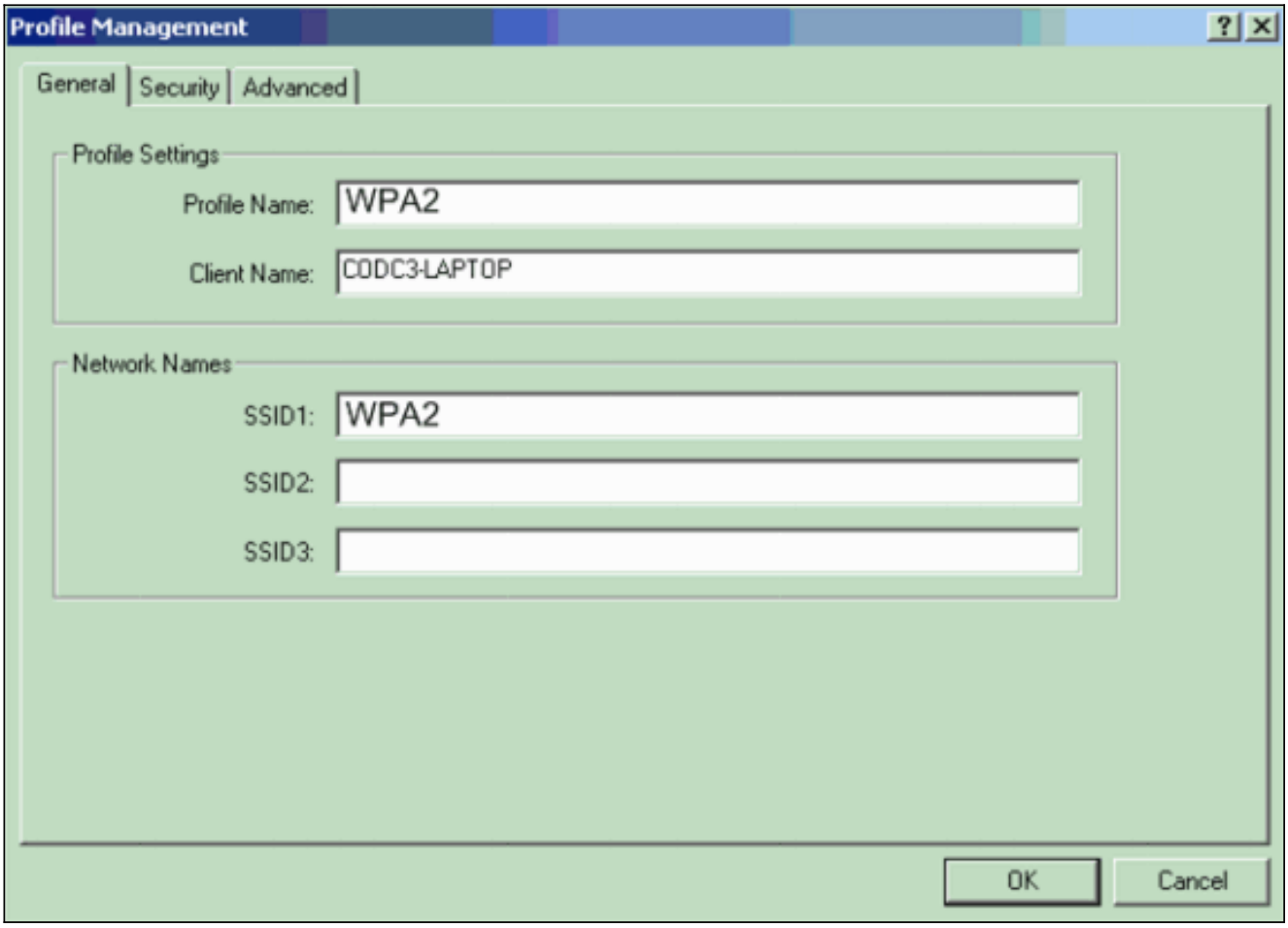
Configurar o adaptador cliente

Conclua estes passos:

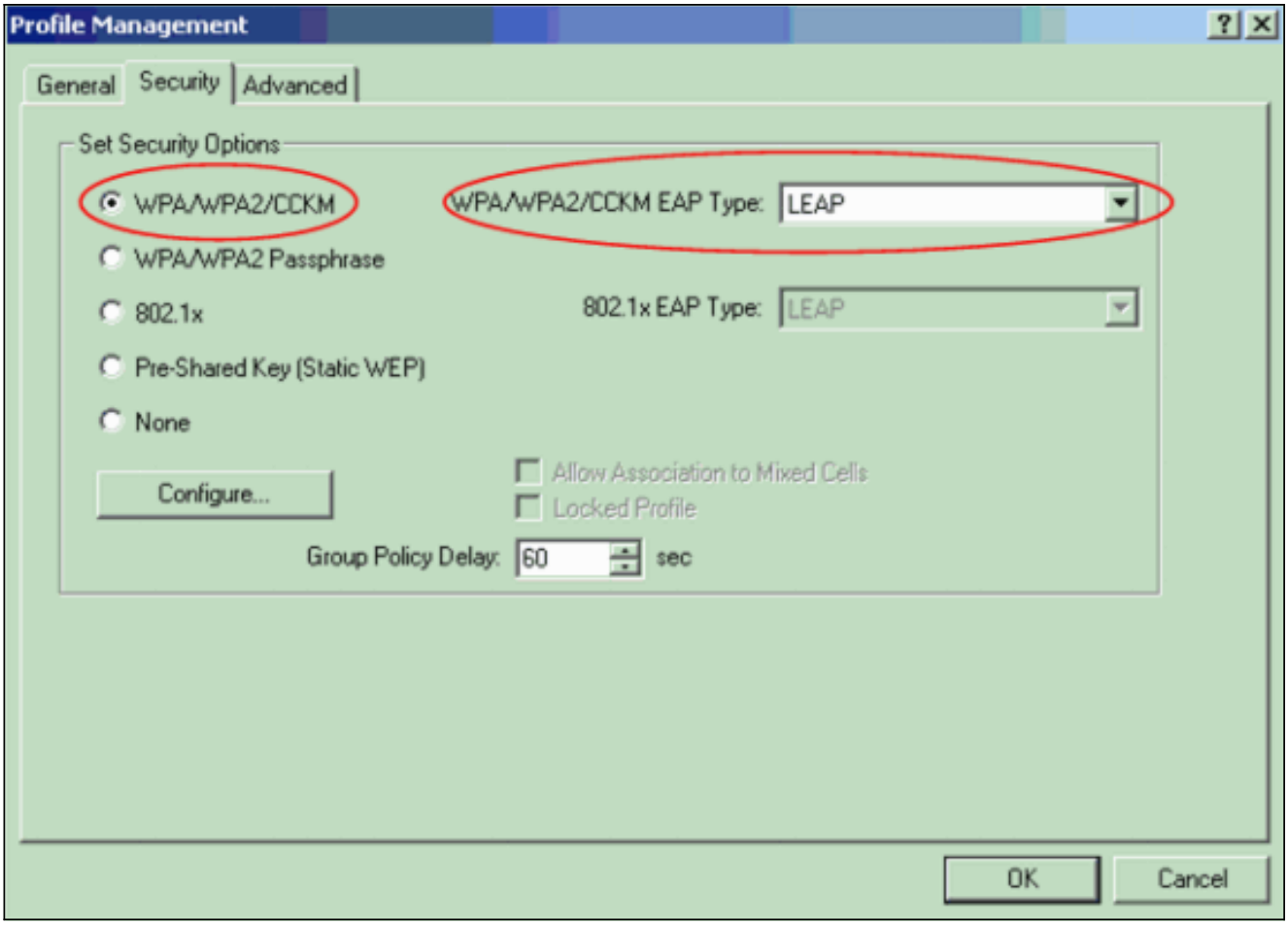
Nota: Este documento usa um adaptador cliente de Aironet 802.11a/b/g que execute o firmware 2.5 e explique a configuração do adaptador cliente com versão ADU 2.5.

1. Na janela de gerenciamento do perfil no ADU, clique **novo** a fim criar um perfil novo.Indicadores de uma nova janela onde você pode ajustar a configuração para a operação de modo de empreendimento WPA2. Sob o tab geral, incorpore o nome de perfil e o SSID que o adaptador cliente usará.Neste exemplo, o nome de perfil e o SSID são WPA2:**Nota:** O SSID deve combinar o SSID que você configurou no AP para o

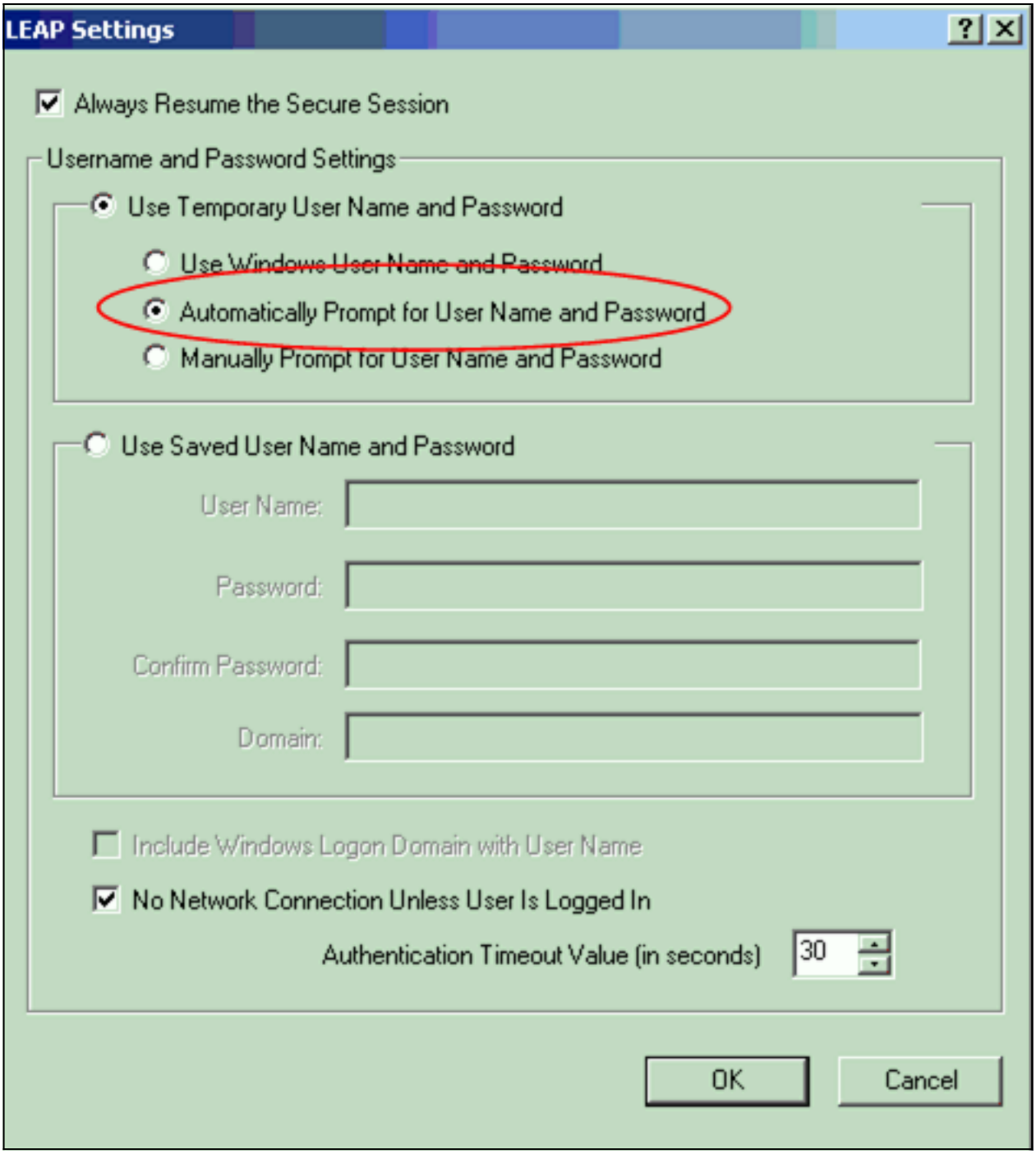
WPA2.



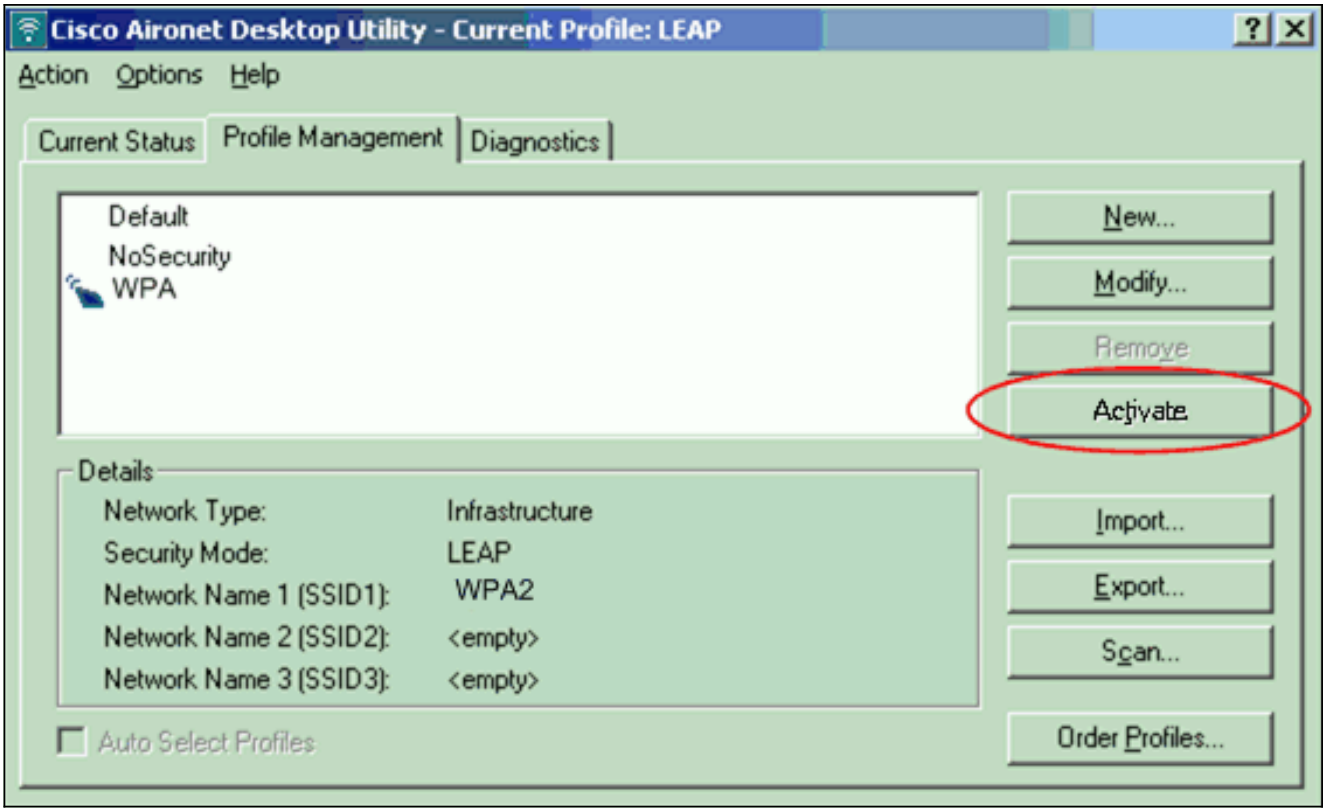
2. Clique a **ABA de segurança**, clique **WPA/WPA2/CCKM**, e escolha o **PULO do** tipo menu WPA/WPA2/CCKM EAP.Esta ação permite o WPA ou o WPA2, qualquer você configura no AP.



3. O clique **configura** a fim definir ajustes do PULO.
4. Escolha os ajustes apropriados do nome de usuário e senha, com base nas exigências, e clique a **APROVAÇÃO**.Esta configuração escolhe a opção alerta automaticamente para o nome de usuário e a senha. Esta opção permite-o de incorporar manualmente o nome de usuário e a senha quando a autenticação de leap
ocorre.



5. APROVAÇÃO do clique a fim retirar a janela de gerenciamento do perfil.
6. O clique ativa a fim permitir este perfil no adaptador cliente.

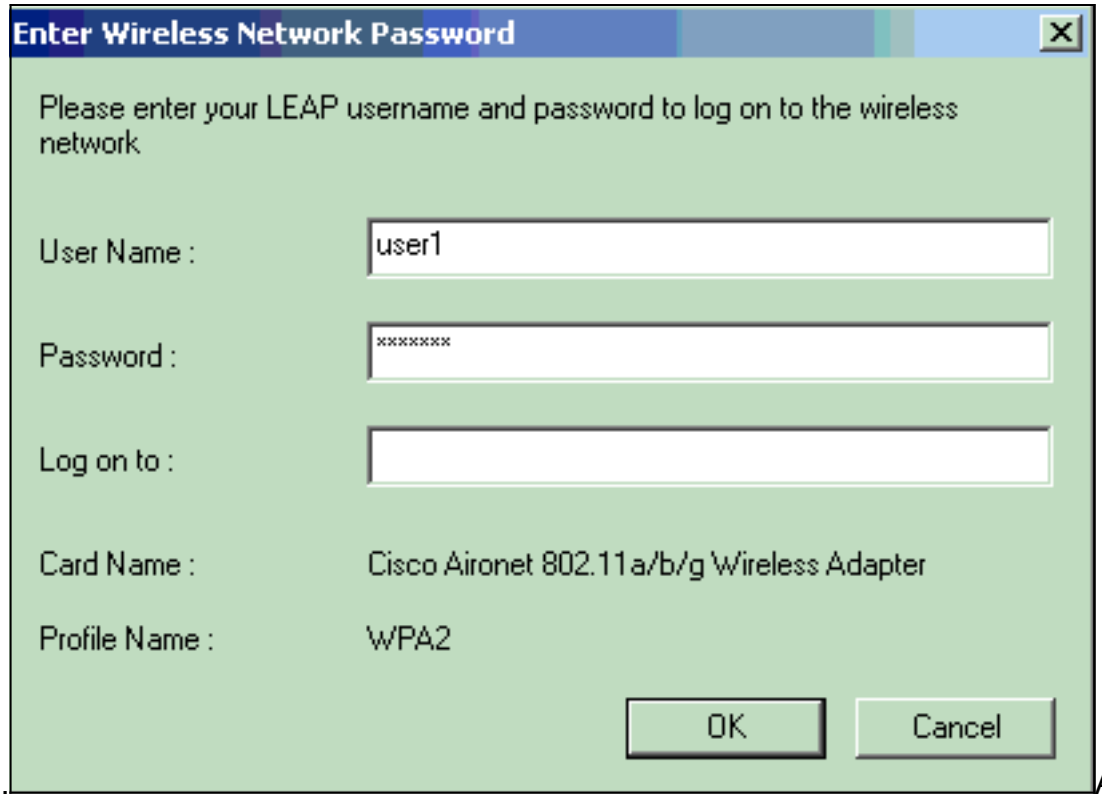


Nota: Se você usa a configuração do Sem fio zero de Microsoft (WZC) para configurar o adaptador cliente, à revelia, o WPA2 não está disponível com WZC. Assim, a fim reservar WZC-permitiu clientes de executar o WPA2, você deve instalar um reparo quente para o Microsoft Windows XP. Refira o centro da transferência de Microsoft - Atualização para Windows XP (KB893357) para a instalação.Depois que você instala o reparo quente, você pode configurar o WPA2 com WZC.

Verificar

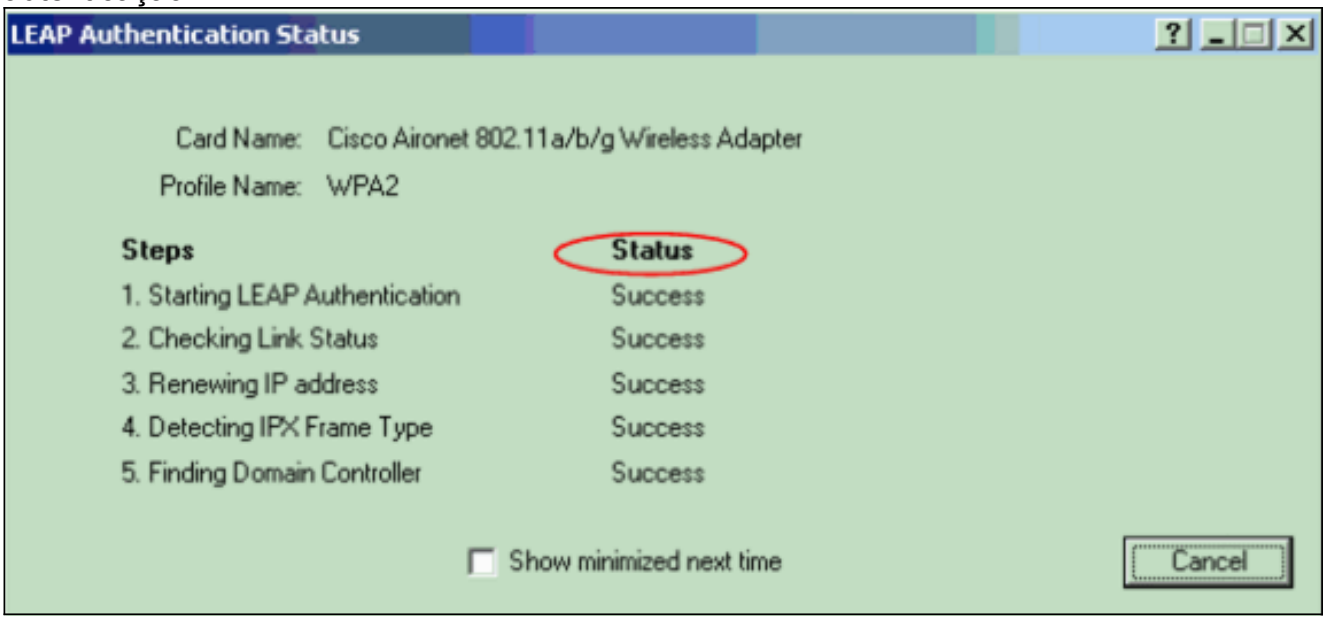
Use esta seção para confirmar se a sua configuração funciona corretamente.

1. Quando os indicadores da janela de senha da rede Wireless da entrada, incorporarem o nome de usuário e a



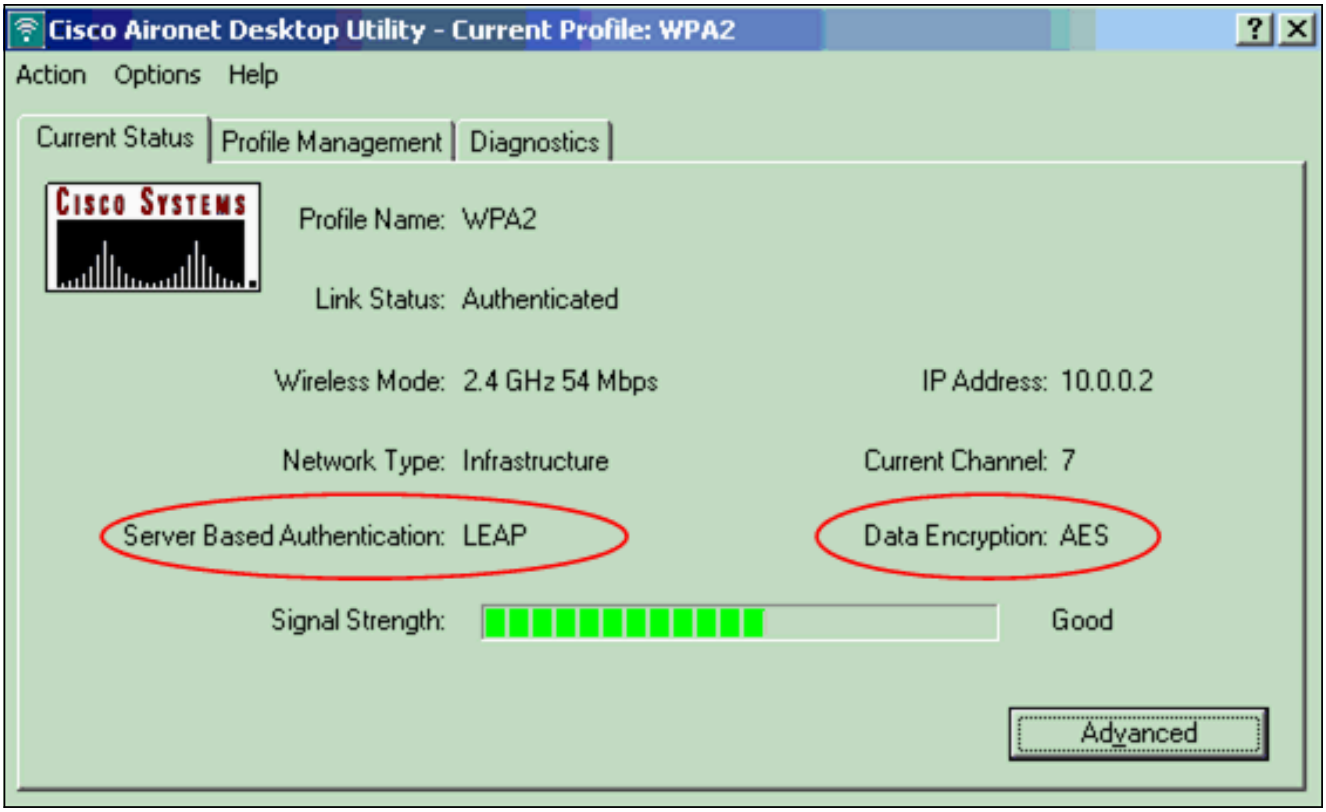
senha. A próxima janela é estado da autenticação de leap. Esta fase verifica as credenciais do usuário contra o servidor Radius local.

2. Verifique a área de status a fim ver o resultado da autenticação.



Quando a autenticação é bem sucedida, o cliente conecta ao Wireless LAN.

3. Verifique o status atual ADU a fim verificar que o cliente usa a criptografia de AES e a autenticação de leap.Isto mostra que você executou o WPA2 com autenticação de leap e criptografia de AES no WLAN.



4. Verifique a ordem do início de uma sessão do evento do AP/bridge para verificar que o cliente esteve autenticado com sucesso com WPA2.

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Configurar no Modo pessoal

O modo pessoal do termo refere o Produtos que é testado para ser interoperáveis no modo PSK-

somente de operação para a autenticação. Este modo exige a configuração manual de um PSK no AP e nos clientes. O PSK autentica usuários através de uma senha, ou código de identificação, na estação do cliente e no AP. Nenhum Authentication Server é necessário. Um cliente pode aceder à rede somente se as compatibilidades de senha do cliente a senha AP. A senha igualmente fornece o material de ajuste que o TKIP ou o AES se usam para gerar uma chave de criptografia para a criptografia dos pacotes de dados. O Modo pessoal é visado aos ambientes SOHO e não considerado seguro para ambientes de empreendimento. Esta seção fornece a configuração que você precisa de executar o WPA2 no modo pessoal de operação.

Instalação de rede

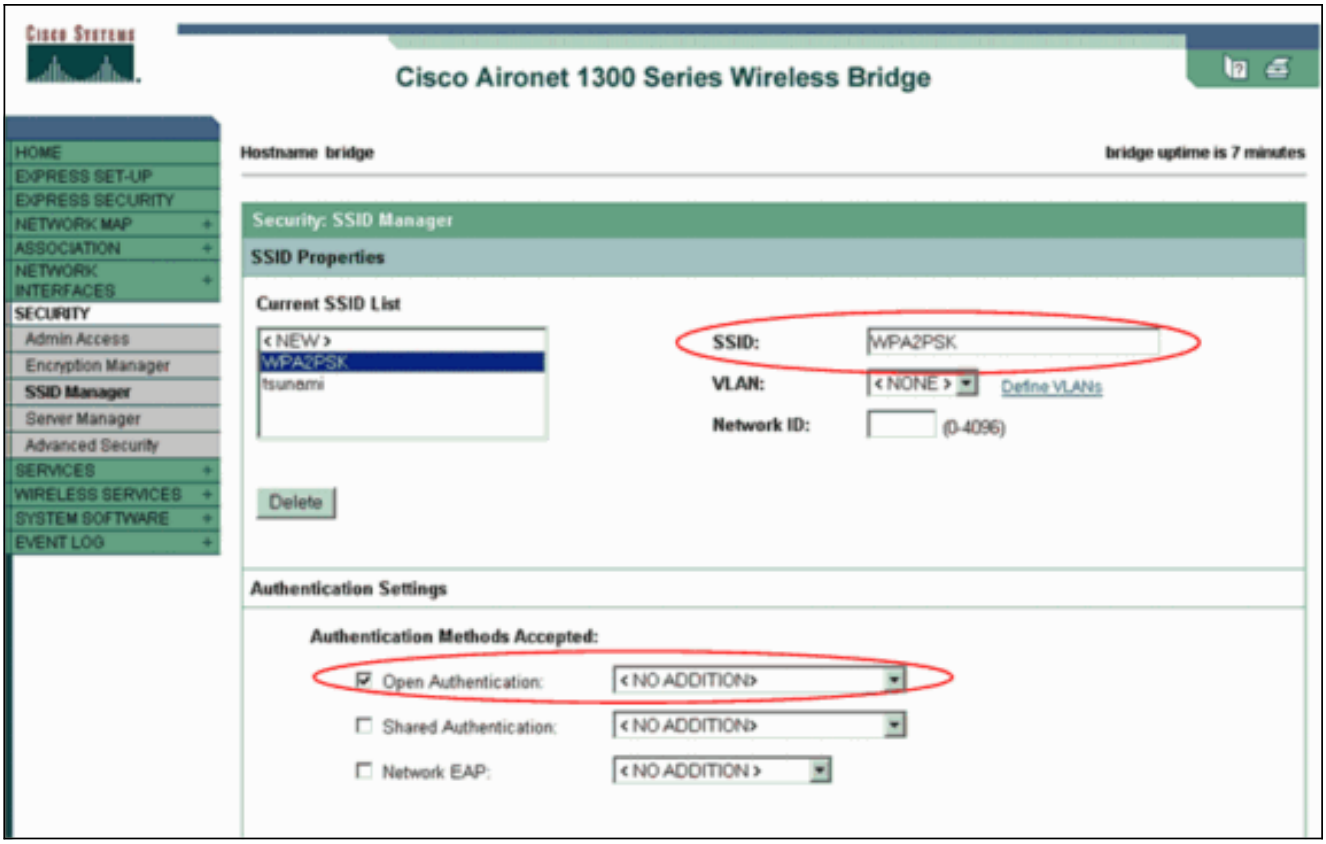
Nesta instalação, um usuário com um adaptador cliente WPA 2-compatible autentica a Aironet 1310G um AP/bridge. O gerenciamento chave ocorre com o uso de WPA2 PSK, com a criptografia AES-CCMP configurada. As seções configuram o AP e configuram a mostra do adaptador cliente a configuração no AP e no adaptador cliente.

Configurar o AP

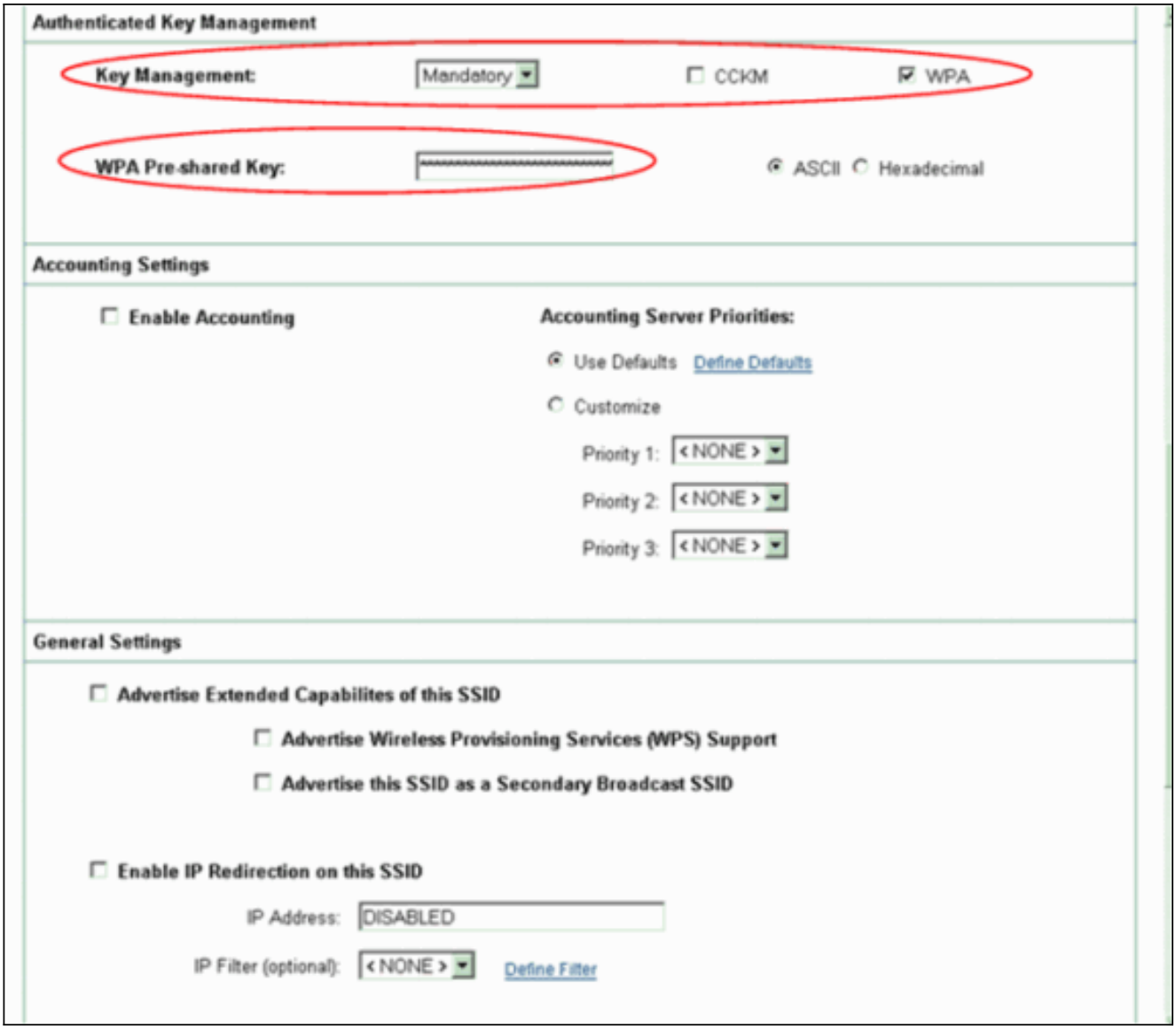
Conclua estes passos:

1. Escolha a **Segurança > o gerenciador de criptografia no** menu à esquerda e termine estas etapas:Do menu da cifra, escolha **AES CCMP**.Esta opção permite a criptografia de AES com o uso do modo contrário com
   CCMP.
   

   Clique em Apply.
2. Escolha a **Segurança > o gerenciador de SSID** e crie um SSID novo para o uso com o WPA2.Verifique a **caixa de verificação de autenticação aberta**.



Enrole para baixo a Segurança: O indicador do gerenciador de SSID à área autenticada do gerenciamento chave e termina estas etapas:Do menu do gerenciamento chave, escolha **imperativo**.Verifique a **caixa de verificação WPA** à direita.



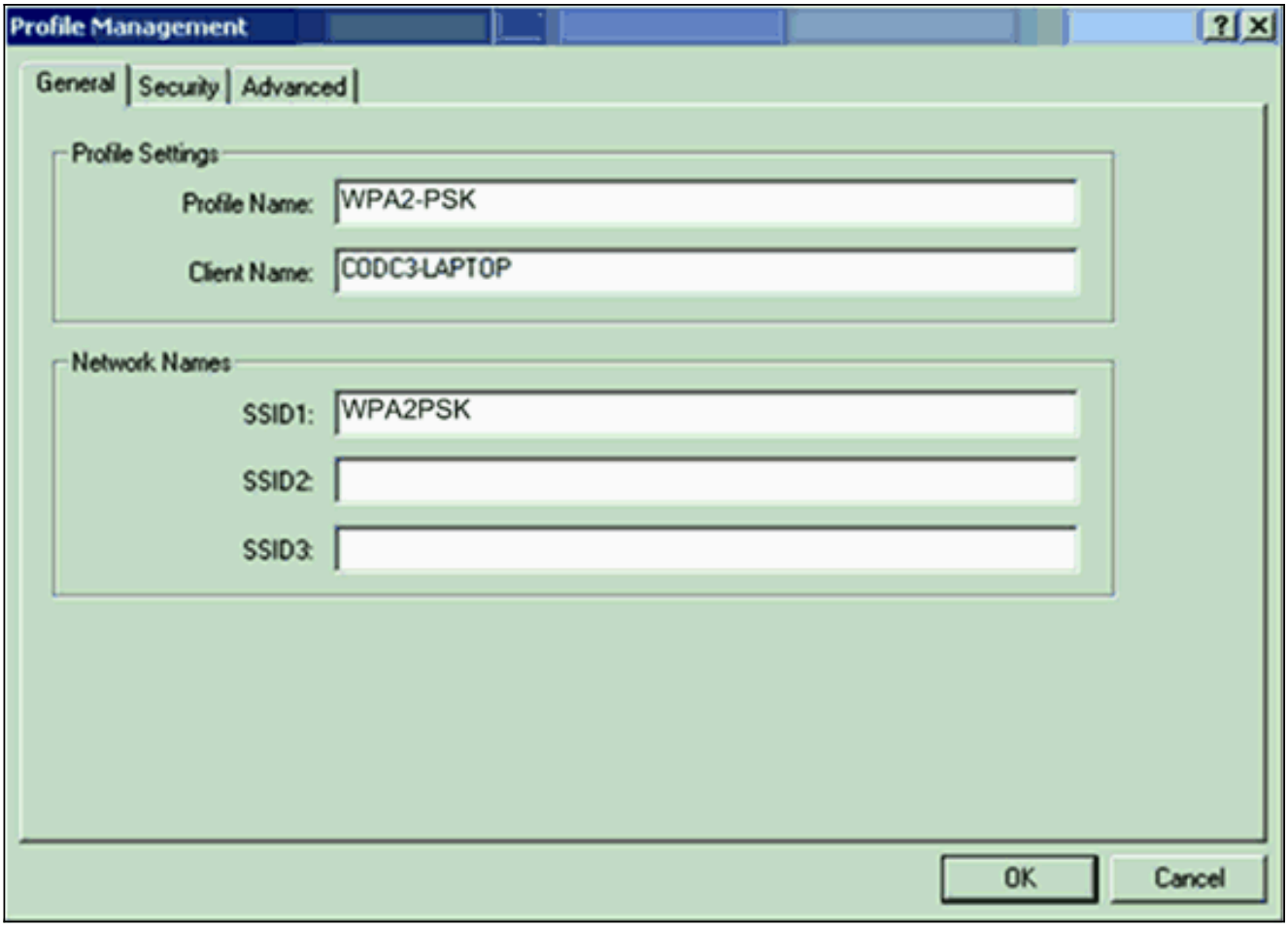
Incorpore a chave secreta compartilhada PSK WPA ou a chave da frase de passagem WPA PSK.Esta chave deve combinar a chave WPA PSK que você configura no adaptador cliente.Clique em Apply.

O AP pode agora receber pedidos de autenticação dos clientes Wireless.

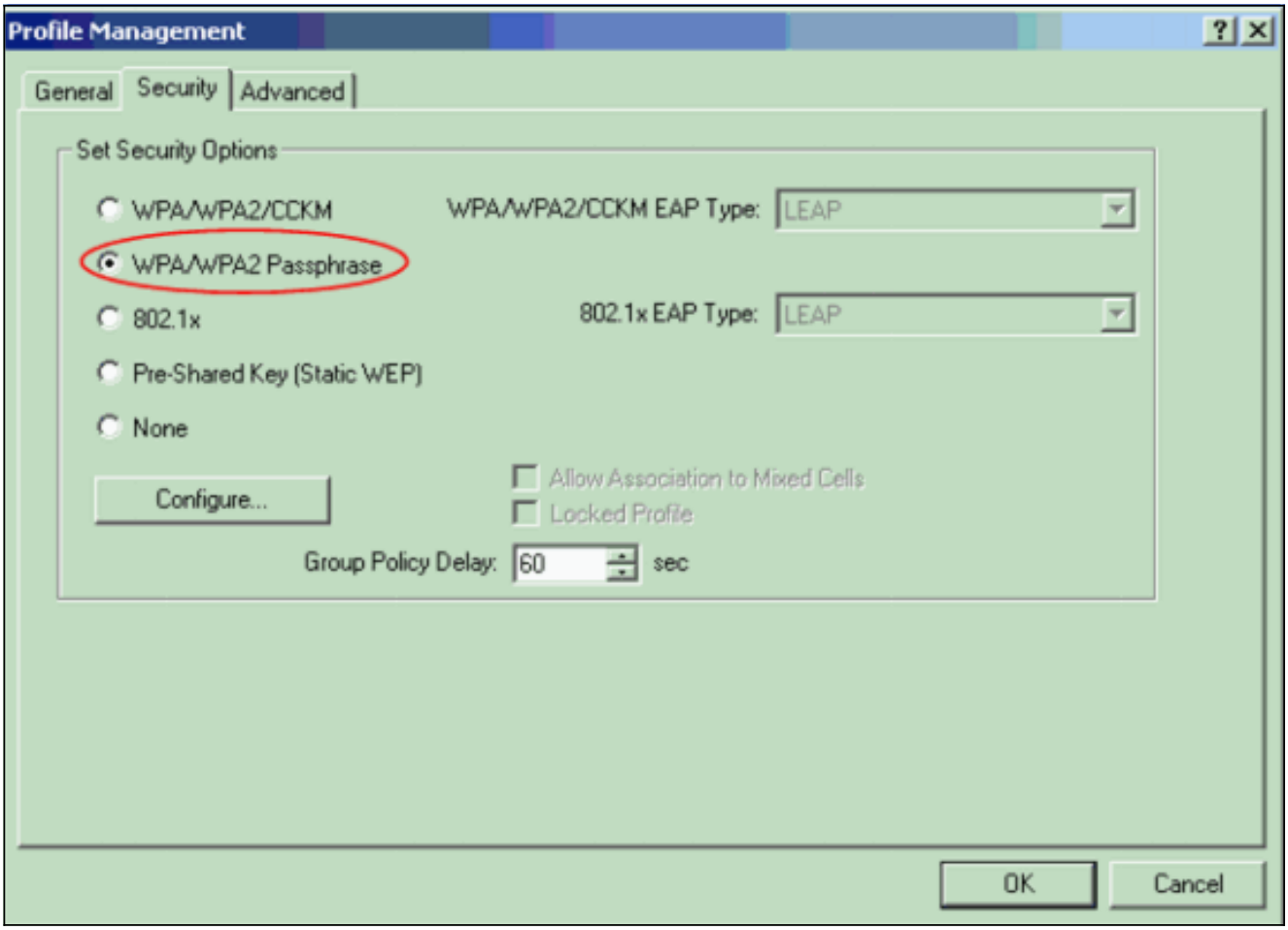
Configurar o adaptador cliente

Conclua estes passos:

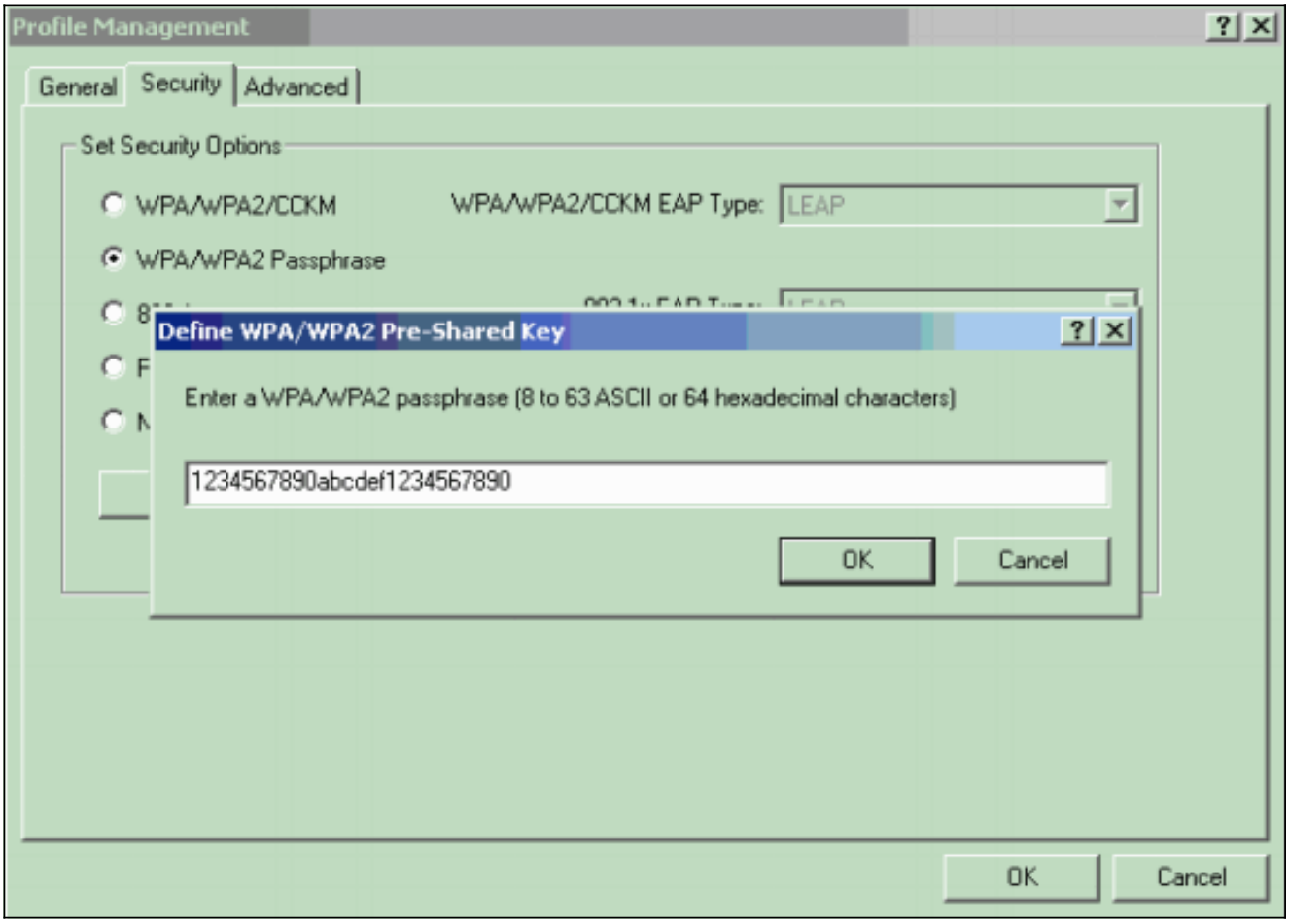
1. Na janela de gerenciamento do perfil no ADU, clique **novo** a fim criar um perfil novo.Indicadores de uma nova janela onde você pode ajustar a configuração para o modo WPA2 PSK de operação. Sob o tab geral, incorpore o nome de perfil e o SSID que o adaptador cliente usará.Neste exemplo, o nome de perfil é WPA2-PSK e o SSID é WPA2PSK:**Nota:** O SSID deve combinar o SSID que você configurou no AP para WPA2 PSK.



2. Clique a **ABA de segurança** e clique a **frase de passagem WPA/WPA2**.Esta ação permite WPA PSK ou WPA2 PSK, qualquer você configura no AP.



3. Clique em Configurar.Os indicadores do indicador da chave pré-compartilhada da definição WPA/WPA2.
4. Obtenha a frase de passagem WPA/WPA2 de seu administrador de sistema e inscreva a frase de passagem no campo da frase de passagem WPA/WPA2.Obtenha a frase de passagem para o AP em uma rede de infraestrutura ou a frase de passagem para outros clientes em uma rede ad-hoc.Use estas diretrizes a fim entrar em uma frase de passagem:As frases de passagem WPA/WPA2 devem conter entre 8 e 63 caráteres do texto de ASCII ou 64 caracteres hexadecimais.Sua frase de passagem do adaptador cliente WPA/WPA2 deve combinar a frase de passagem do AP com que você planeia se comunicar.



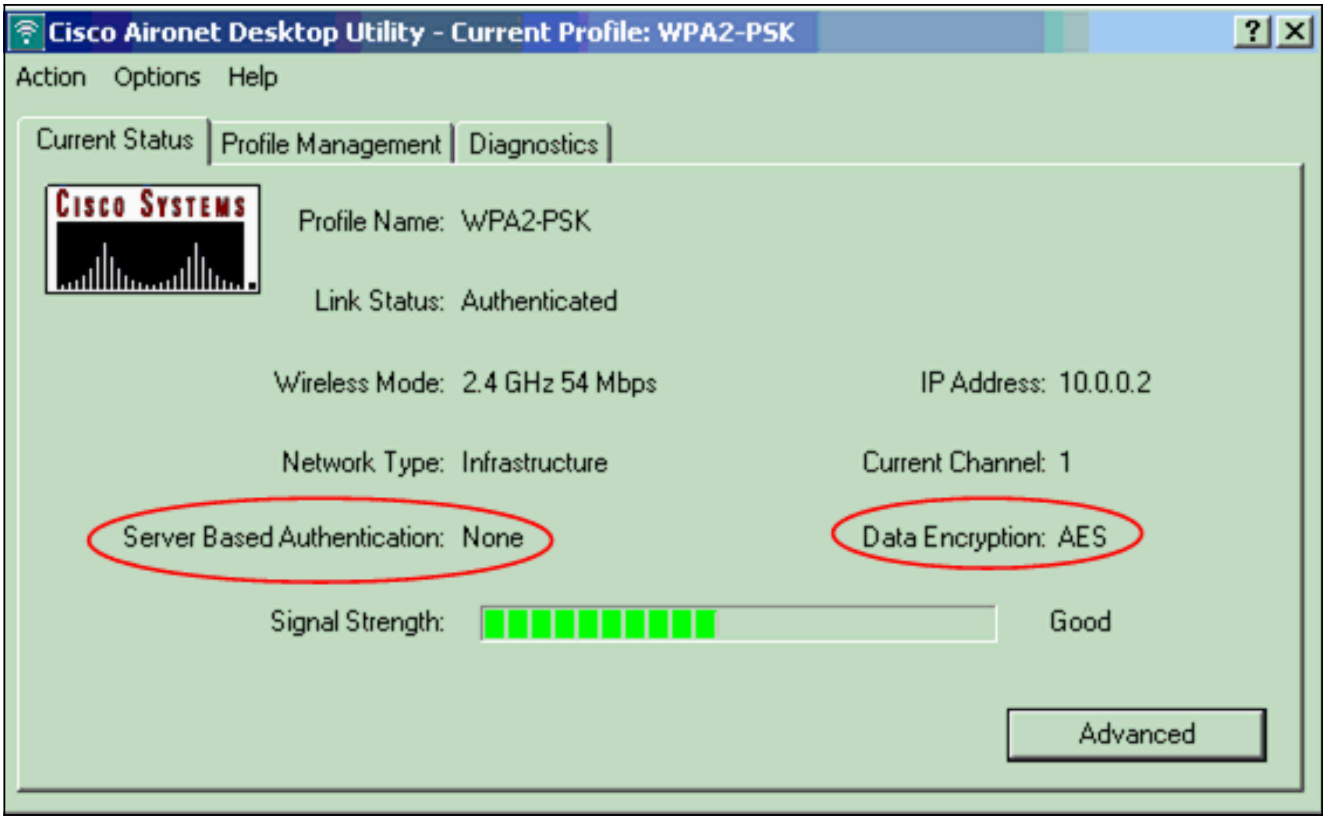
5. Clique a **APROVAÇÃO** a fim salvar a frase de passagem e retornar à janela de gerenciamento do perfil.

Verificar

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

Depois que o perfil WPA2 PSK é ativado, o AP autentica o cliente baseado na frase de passagem WPA2 (PSK) e fornece o acesso ao WLAN.

1. Verifique o status atual ADU a fim verificar a autenticação bem sucedida.Este indicador fornece um exemplo. O indicador mostra que a criptografia que é usada é AES e que nenhuma autenticação baseada em servidor está executada:



2. Verifique a ordem do início de uma sessão do evento do AP/bridge para verificar que o cliente esteve autenticado com sucesso com modo de autenticação WPA2 PSK.

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Configurando conjuntos de cifras e o WEP
- Configurando tipos de autenticação
- Visão Geral da Configuração do WPA
- WPA2 - Acesso protegido por wi-fi 2
- O que são operação de modo misturada WPA, e como mim a configura em meu AP
- Página de Suporte Wireless
- Suporte Técnico e Documentação - Cisco Systems