

Exemplo de configuração do WPA 2 (Wi-Fi Protected Access 2)

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Informações de Apoio](#)

[Suporte a WPA 2 com equipamento Cisco Aironet](#)

[Configurar no modo empresarial](#)

[Instalação de rede](#)

[Configurar o AP](#)

[Configuração de CLI](#)

[Configurar o adaptador cliente](#)

[Verificar](#)

[Troubleshoot](#)

[Configurar no modo pessoal](#)

[Instalação de rede](#)

[Configurar o AP](#)

[Configurar o adaptador cliente](#)

[Verificar](#)

[Troubleshoot](#)

[Informações Relacionadas](#)

[Introduction](#)

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.

Observação: o WPA funciona com o Extensible Authentication Protocol (EAP).

[Prerequisites](#)

[Requirements](#)

Verifique se você tem o conhecimento básico desses tópicos antes de experimentar esta

configuração:

- WPA
- Soluções de segurança WLAN **Observação:** consulte [Visão geral da segurança de LAN sem fio do Cisco Aironet](#) para obter informações sobre as soluções de segurança da Cisco WLAN.

Componentes Utilizados

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

- Access point (AP)/ponte Cisco Aironet 1310G que executa o software Cisco IOS® versão 12.3(2)JA
- Adaptador cliente Aironet 802.11a/b/g CB21AG que executa o firmware 2.5
- Aironet Desktop Utility (ADU) que executa o firmware versão 2.5

Observação: o software do adaptador cliente Aironet CB21AG e PI21AG não é compatível com outro software do adaptador cliente Aironet. Você deve usar o ADU com as placas CB21AG e PI21AG, e o Aironet Client Utility (ACU) com todos os outros adaptadores clientes Aironet.

Consulte [Instalação do adaptador cliente](#) para obter mais informações sobre como instalar a placa CB21AG e o ADU.

Observação: este documento usa um AP/uma ponte com uma antena integrada. Se você usar um AP/uma ponte que exige uma antena externa, certifique-se de que as antenas estejam conectadas ao AP/à ponte. Caso contrário, o AP/a ponte não consegue se conectar à rede sem fio. Alguns modelos de AP/ponte vêm com antenas integradas, enquanto outros precisam de uma antena externa para operações em geral. Para obter informações sobre os modelos de AP/ponte com antenas internas ou externas, consulte o guia de pedidos/guia de produto do dispositivo apropriado.

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.

Conventions

Consulte as [Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos](#).

Informações de Apoio

O WPA é uma solução de segurança padrão da Wi-Fi Alliance que resolve as vulnerabilidades nas WLANs nativas. O WPA oferece proteção avançada de dados e controle de acesso para sistemas WLAN. O WPA resolve todas as vulnerabilidades conhecidas de Wired Equivalent Privacy (WEP) na implementação de segurança IEEE 802.11 original e oferece uma solução de segurança imediata para WLANs em ambientes empresariais e de escritórios de pequeno porte e home offices (SOHO).

O WPA 2 é a próxima geração de segurança de Wi-Fi. O WPA 2 é a implementação interoperável da Wi-Fi Alliance do padrão IEEE 802.11i ratificado. O WPA 2 implementa o algoritmo de criptografia do Advanced Encryption Standard (AES) recomendado pelo National Institute of Standards and Technology (NIST) usando o modo de contador com o Cipher Block Chaining

Message Authentication Code Protocol (CCMP). O modo de contador do AES é uma cifra de bloco que criptografa blocos de dados de 128 bits de cada vez com uma chave de criptografia de 128 bits. O algoritmo do CCMP produz um código de integridade de mensagem (MIC) que fornece autenticação de origem de dados e integridade de dados para o quadro sem fio.

Observação: o CCMP também é conhecido como CBC-MAC.

O WPA 2 oferece um nível de segurança maior do que o WPA, pois o AES oferece uma criptografia mais robusta do que o Temporal Key Integrity Protocol (TKIP). O TKIP é o algoritmo de criptografia usado pelo WPA. O WPA 2 cria novas chaves de sessão em cada associação. As chaves de criptografia usadas para cada cliente na rede são exclusivas e específicas para esse cliente. Por fim, cada pacote enviado remotamente é criptografado com uma chave exclusiva. A segurança é aprimorada com o uso de uma chave de criptografia nova e exclusiva, pois não há reutilização de chaves. O WPA ainda é considerado seguro e o TKIP não foi interrompido. No entanto, a Cisco recomenda que os clientes façam a transição para o WPA 2 assim que possível.

O WPA e o WPA 2 são compatíveis com dois modos de operação:

- Modo empresarial
- Modo pessoal

Este documento aborda a implementação desses dois modos com o WPA 2.

[Suporte a WPA 2 com equipamento Cisco Aironet](#)

O WPA 2 é compatível com estes equipamentos:

- Aironet 1130AG AP series e 1230AG AP series
- Aironet 1100 AP series
- Aironet 1200 AP series
- Aironet 1300 AP series

Observação: equipe esses APs com rádios 802.11g e use o software Cisco IOS versão 12.3 (2) JA ou posterior.

O WPA 2 e o AES também são compatíveis com:

- Módulos de rádio Aironet 1200 series com os números de peça AIR-RM21A e AIR-RM22A**Observação:** o módulo de rádio Aironet 1200 com o número de peça AIR-RM20A não é compatível com o WPA 2.
- Adaptadores clientes Aironet 802.11a/b/g com o firmware versão 2.5

Observação: os produtos Cisco Aironet 350 series não são compatíveis com o WPA 2, pois os rádios não oferecem suporte a AES.

Observação: as pontes sem fio Cisco Aironet 1400 Series não são compatíveis com o WPA 2 ou o AES.

[Configurar no modo empresarial](#)

O termo **modo empresarial** se refere a produtos testados quanto à interoperabilidade nos modos de operação Pre-Shared Key (PSK) e IEEE 802.1x para autenticação. O 802.1x é considerado mais seguro do que qualquer uma das estruturas de autenticação antigas, devido à flexibilidade

no suporte a uma variedade de mecanismos de autenticação e algoritmos de criptografia mais robustos. O WPA 2 no modo empresarial executa a autenticação em duas fases. A configuração da autenticação aberta ocorre na primeira fase. A segunda fase é a autenticação 802.1x com um dos métodos do EAP. O AES fornece o mecanismo de criptografia.

No modo empresarial, os clientes e os servidores de autenticação são autenticados usando um método de autenticação do EAP, e o cliente e o servidor geram uma Pairwise Master Key (PMK). Com o WPA 2, o servidor gera a PMK dinamicamente e passa para o AP.

Esta seção aborda a configuração necessária para implementar o WPA 2 no modo empresarial de operação.

[Instalação de rede](#)

Nessa configuração, um AP/uma ponte Aironet 1310G que executa o Cisco Lightweight Extensible Authentication Protocol (LEAP) autentica um usuário com um adaptador cliente compatível com o WPA 2. O gerenciamento de chaves ocorre usando o WPA 2, em que a criptografia AES-CCMP está configurada. O AP é configurado como servidor RADIUS local que executa a autenticação LEAP. Você deve configurar o adaptador cliente e o AP para implementar essa configuração. As seções [Configurar o AP](#) e [Configurar o adaptador cliente](#) mostram a configuração no AP e no adaptador cliente.

[Configurar o AP](#)

Siga estas etapas para configurar o AP usando a GUI:

1. Configure o AP como servidor RADIUS local que executa a autenticação LEAP. Escolha **Segurança > Gerenciador do servidor** no menu à esquerda e defina o endereço IP, as portas e o segredo compartilhado do servidor RADIUS. Como essa configuração define o AP como servidor RADIUS local, use o endereço IP do AP. Use as portas 1812 e 1813 para a operação do servidor RADIUS local. Na área Prioridades do servidor padrão, defina a prioridade de autenticação do EAP padrão como 10.0.0.1. **Observação:** 10.0.0.1 é o servidor RADIUS local.

Cisco Aironet 1300 Series Wireless Bridge

SERVER MANAGER GLOBAL PROPERTIES

Hostname bridge bridge uptime is 7 minutes

Security: Server Manager

Backup RADIUS Server

Backup RADIUS Server: (Hostname or IP Address)

Shared Secret:

Apply Delete Cancel

Corporate Servers

Current Server List

RADIUS

Server	Shared Secret
< NEW > 10.0.0.1	<input type="text"/>

Delete

Authentication Port (optional): 1812 (0-65536)

Accounting Port (optional): 1813 (0-65536)

Apply Cancel

Default Server Priorities

EAP Authentication MAC Authentication Accounting

Priority 1: 10.0.0.1 Priority 1: < NONE > Priority 1: < NONE >

2. Escolha **Segurança > Gerenciador de criptografia** no menu à esquerda e siga estas etapas: No menu Cifra, escolha **AES CCMP**. Essa opção ativa a criptografia do AES usando o modo de contador com o CBC-MAC.

Cisco Aironet 1300 Series Wireless Bridge

SECURITY Encryption Manager

Hostname bridge bridge uptime is 5 minutes

Security: Encryption Manager

Encryption Modes

None

WEP Encryption Optional

Cisco Compliant TKIP Features: Enable Message Integrity Check (MIC)

Enable Per Packet Keying (PPK)

Cipher AES CCMP

Encryption Keys

	Transmit Key	Encryption Key (Hexadecimal)	Key Size
Encryption Key 1:	<input type="radio"/>	<input type="text"/>	<input type="text"/> 128 bit
Encryption Key 2:	<input type="radio"/>	<input type="text"/>	<input type="text"/> 128 bit
Encryption Key 3:	<input type="radio"/>	<input type="text"/>	<input type="text"/> 128 bit
Encryption Key 4:	<input type="radio"/>	<input type="text"/>	<input type="text"/> 128 bit

Clique em Apply.

- Escolha **Segurança > Gerenciador de SSID** e crie um novo Service Set Identifier (SSID) para uso com o WPA 2. Marque a caixa de seleção **EAP de rede** na área Métodos de autenticação aceitos.

The screenshot displays the configuration interface for a Cisco Aironet 1300 Series Wireless Bridge. The page title is "Cisco Aironet 1300 Series Wireless Bridge" and the hostname is "bridge". The bridge uptime is 6 minutes. The left sidebar shows a navigation menu with categories like HOME, EXPRESS SET-UP, SECURITY, SERVICES, and WIRELESS SERVICES. The main content area is titled "Security: SSID Manager" and "SSID Properties". Under "Current SSID List", there is a list with entries: "< NEW >", "WPA2" (highlighted), and "autoinstall". To the right, the "SSID:" field is set to "WPA2", "VLAN:" is set to "< NONE >", and "Network ID:" is set to "(0-4096)". Below this, the "Authentication Settings" section shows "Authentication Methods Accepted:" with three options: "Open Authentication:" (unchecked), "Shared Authentication:" (unchecked), and "Network EAP:" (checked). Red circles highlight the "WPA2" SSID field and the "Network EAP:" checkbox.

Observação: use estas diretrizes ao configurar o tipo de autenticação na interface de rádio: Clientes Cisco – Use o Network EAP. Clientes de terceiros (que incluem produtos compatíveis com Cisco Compatible Extensions [CCX]) – Use a Open Authentication com o EAP. Uma combinação de clientes da Cisco e de terceiros – Escolha o Network EAP e a Open Authentication com o EAP. Role para baixo na janela Segurança: gerenciador de SSID até a área Gerenciamento de chaves autenticadas e siga estas etapas: No menu Gerenciamento de chaves, escolha **Obrigatório**. Marque a caixa de seleção **WPA** à direita. Clique em Apply. **Observação:** a definição de VLANs é opcional. Se você definir VLANs, os dispositivos clientes associados ao uso desse SSID serão agrupados na VLAN. Consulte [Configuração de VLANs](#) para obter mais informações sobre como implementar VLANs.

Authenticated Key Management

Key Management: CCCKM WPA

WPA Pre-shared Key: ASCII Hexadecimal

Accounting Settings

Enable Accounting

Accounting Server Priorities:

Use Defaults [Define Defaults](#)

Customize

Priority 1:

Priority 2:

Priority 3:

General Settings

Advertise Extended Capabilities of this SSID

- Advertise Wireless Provisioning Services (WPS) Support
- Advertise this SSID as a Secondary Broadcast SSID

Enable IP Redirection on this SSID

IP Address:

IP Filter (optional): [Define Filter](#)

4. Escolha **Segurança > Servidor Radius local** e siga estas etapas: Clique na guia **Configuração geral** localizada na parte superior da janela. Marque a caixa de seleção **LEAP** e clique em **Aplicar**. Na área Servidores de acesso à rede, defina o endereço IP e o segredo compartilhado do servidor RADIUS. Para o servidor RADIUS local, use o endereço IP do AP.

The screenshot shows the configuration page for a Cisco Aironet 1300 Series Wireless Bridge. The page is titled "Cisco Aironet 1300 Series Wireless Bridge" and has three tabs: "STATISTICS", "GENERAL SET-UP", and "EAP-FAST SET-UP". The "GENERAL SET-UP" tab is active. The page displays the following information:

- Hostname: bridge
- bridge uptime is 0 minutes
- Security: Local RADIUS Server - General Set-Up
- Local Radius Server Authentication Settings
- Enable Authentication Protocols:
 - EAP FAST
 - LEAP
 - MAC
- Network Access Servers (AAA Clients)
- Current Network Access Servers
 - < NEW >
 - 10.0.0.1
- Network Access Server: 10.0.0.1 (IP Address)
- Shared Secret: [Redacted]

Red circles highlight the "LEAP" checkbox and the "Network Access Server" and "Shared Secret" fields.

Clique em Apply.

5. Role para baixo na janela Configuração geral até a área Usuários individuais e defina os usuários individuais. A definição dos grupos de usuários é opcional.

Individual Users

Current Users

<NEW>
user1

Delete

Username: user1

Password: Text NT Hash

Confirm Password:

Group Name: <NONE >

MAC Authentication Only

Apply Cancel

User Groups

Current User Groups

<NEW>

Delete

Group Name:

Session Timeout (optional): (1-4294967295 sec)

Failed Authentications before Lockout (optional): (1-4294967295)

Lockout (optional): Infinite Interval (1-4294967295 sec)

VLAN ID (optional):

SSID (optional): Add

Delete

Essa configuração define um usuário com o nome "user1" e uma senha. Além disso, a configuração seleciona NT hash como senha. Após a conclusão do procedimento nesta seção, o AP está pronto para aceitar as solicitações 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 nhash password1
    group testuser
    !--- Individual user user user2 nhash 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](#)

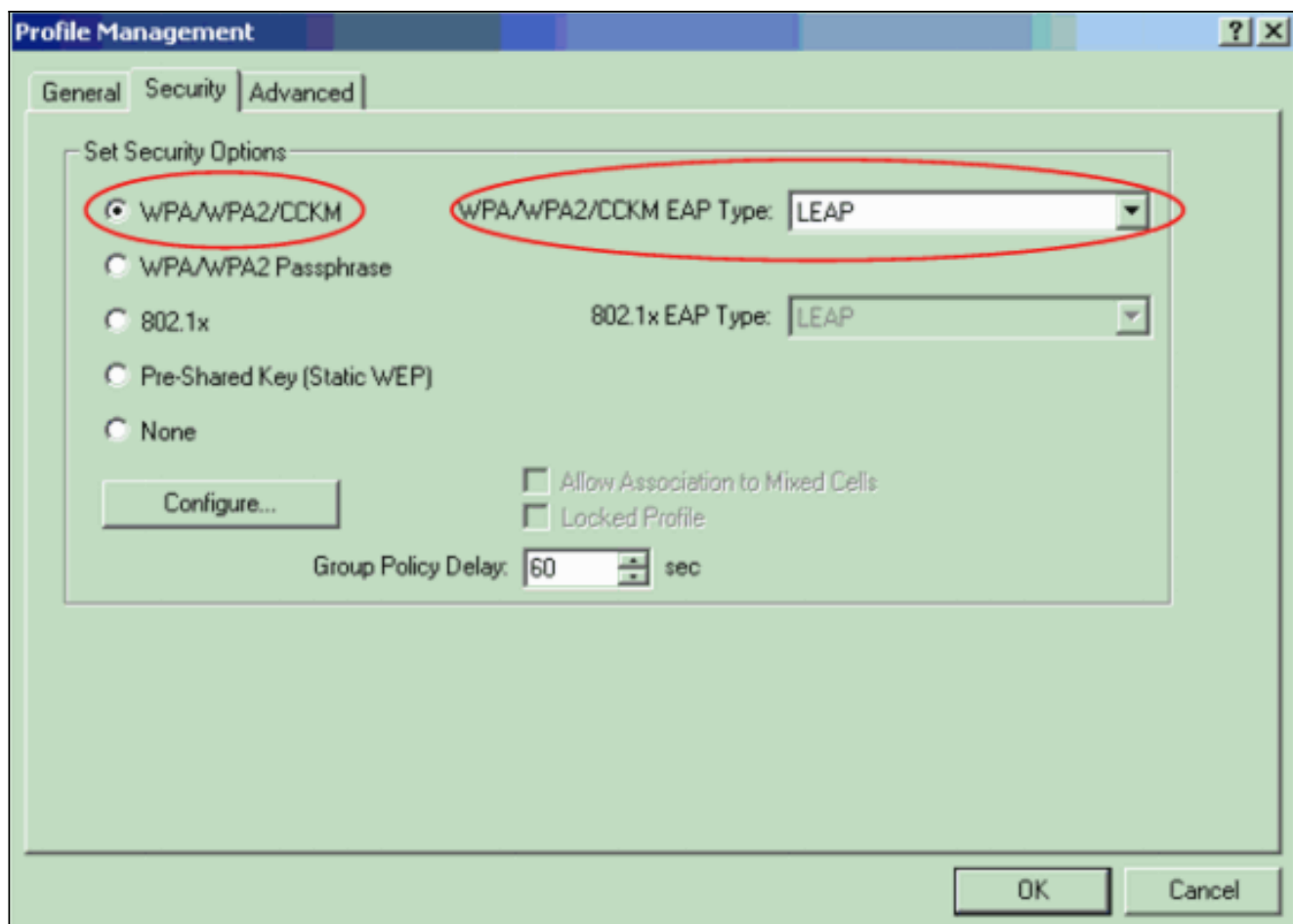
Conclua estes passos:

Observação: este documento usa um adaptador cliente Aironet 802.11a/b/g que executa o firmware 2.5 e explica a configuração do adaptador cliente com a ADU versão 2.5.

1. Na janela Gerenciamento de perfil na ADU, clique em **Novo** para criar um novo perfil. Será exibida uma nova janela em que você poderá definir a configuração para a operação no modo empresarial do WPA 2. Na guia Geral, insira o nome do perfil e o SSID que o adaptador cliente usará. Neste exemplo, o nome do perfil e o SSID são WPA2: **Observação:** o SSID deve corresponder ao SSID que você configurou no AP para WPA
- 2.

The image shows a screenshot of the 'Profile Management' dialog box. The 'General' tab is selected. Under 'Profile Settings', the 'Profile Name' field contains 'WPA2' and the 'Client Name' field contains 'CODC3-LAPTOP'. Under 'Network Names', the 'SSID1' field contains 'WPA2', while 'SSID2' and 'SSID3' are empty. The 'OK' and 'Cancel' buttons are visible at the bottom right.

2. Clique na guia **Segurança**, clique em **WPA/WPA2/CCKM** e escolha **LEAP** no menu Tipo de EAP do WPA/WPA2/CCKM. Essa ação ativa o WPA ou o WPA 2, o que você configurar no AP.



3. Clique em **Configurar** para definir as configurações do LEAP.
4. Escolha as configurações apropriadas de nome do usuário e senha de acordo com os requisitos e clique em **OK**. Essa configuração escolhe a opção Solicitar nome do usuário e senha automaticamente. Essa opção permite que você insira manualmente o nome do usuário e a senha no momento da autenticação LEAP.

LEAP Settings [?] [X]

Always Resume the Secure Session

Username and Password Settings

Use Temporary User Name and Password

Use Windows User Name and Password

Automatically Prompt for User Name and Password

Manually Prompt for User Name and Password

Use Saved User Name and Password

User Name:

Password:

Confirm Password:

Domain:

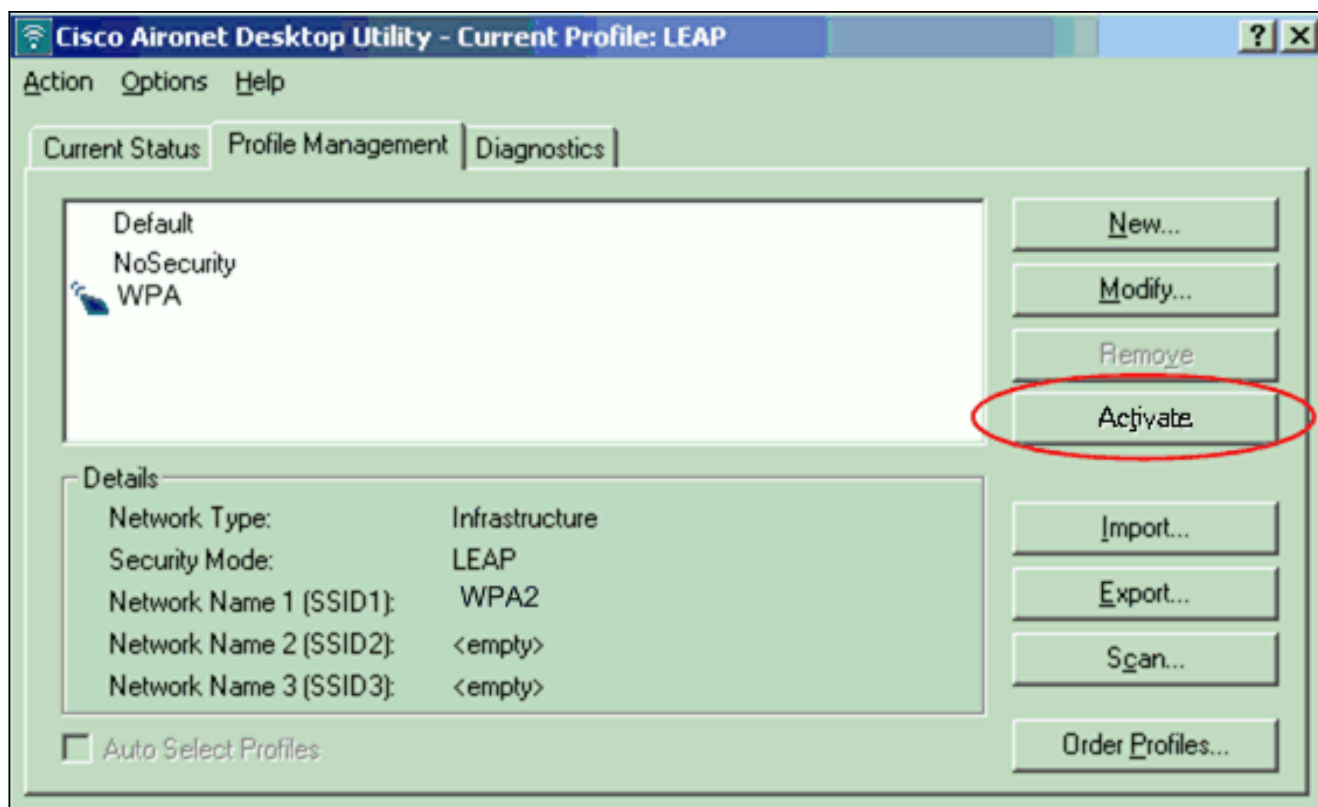
Include Windows Logon Domain with User Name

No Network Connection Unless User Is Logged In

Authentication Timeout Value (in seconds)

OK Cancel

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



Observação: se você usar o Microsoft Wireless Zero Configuration (WZC) para configurar o adaptador cliente, por padrão, o WPA 2 não estará disponível com o WZC. Portanto, para permitir que clientes habilitados para WZC executem o WPA 2, você deve instalar um hot fix para o Microsoft Windows XP. Consulte o [Microsoft Download Center – Atualização para Windows XP \(KB893357\)](#) para obter a instalação. Depois de instalar o hot fix, você poderá configurar o WPA 2 com o WZC.

Verificar

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

1. Quando a janela Inserir senha de rede sem fio for exibida, insira o nome do usuário e a

Enter Wireless Network Password

Please enter your LEAP username and password to log on to the wireless network

User Name : user1

Password : xxxxxxx

Log on to :

Card Name : Cisco Aironet 802.11 a/b/g Wireless Adapter

Profile Name : WPA2

OK Cancel

senha.

A

próxima janela é Status de autenticação LEAP. Esta fase verifica as credenciais do usuário em relação ao servidor RADIUS local.

2. Verifique a área Status para ver o resultado da autenticação.

LEAP Authentication Status

Card Name: Cisco Aironet 802.11 a/b/g Wireless Adapter

Profile Name: WPA2

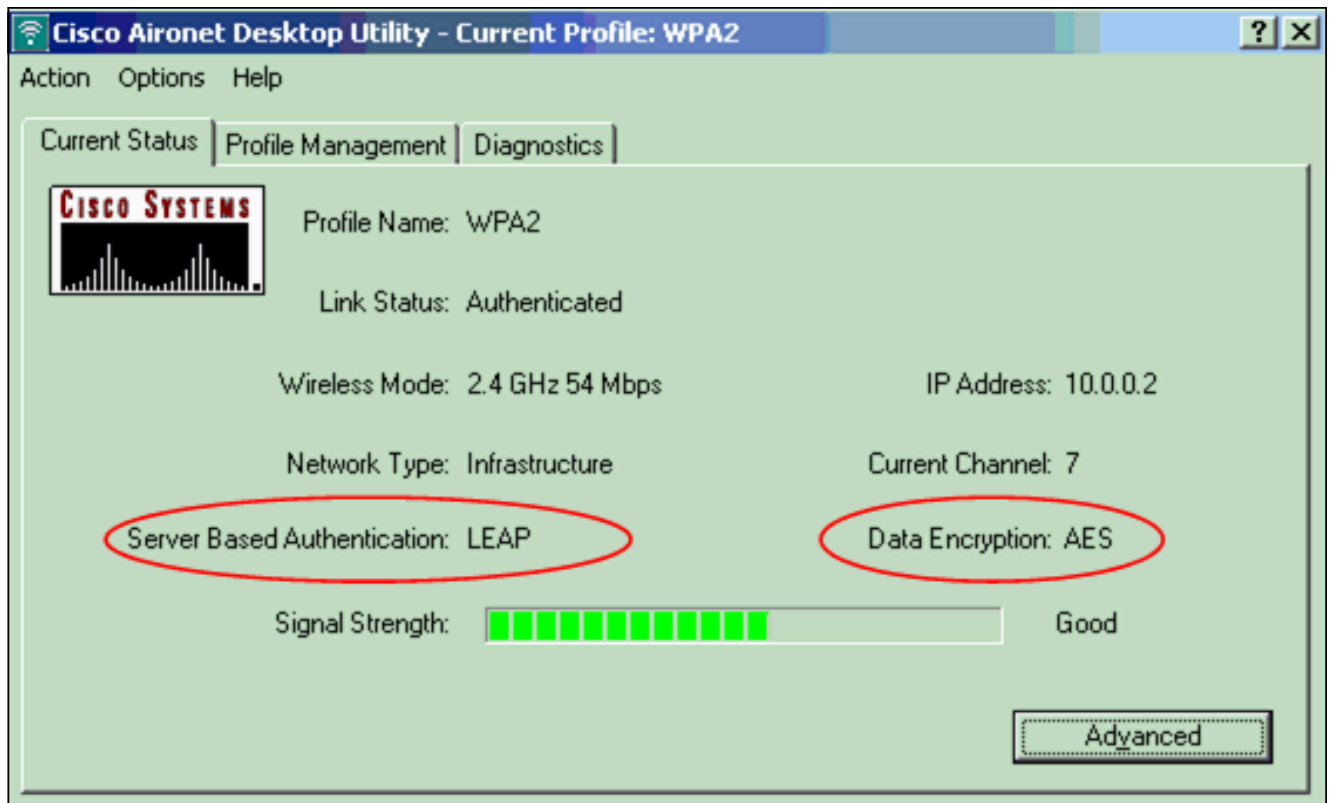
Steps	Status
1. Starting LEAP Authentication	Success
2. Checking Link Status	Success
3. Renewing IP address	Success
4. Detecting IPX Frame Type	Success
5. Finding Domain Controller	Success

Show minimized next time

Cancel

Quando a autenticação é realizada com sucesso, o cliente é conectado à LAN sem fio.

3. Verifique o status atual da ADU para ver se o cliente usa a criptografia AES e a autenticação LEAP. Isso mostra que você implementou o WPA 2 com a autenticação LEAP e a criptografia AES na WLAN.



4. Verifique o registro de eventos do AP/da ponte para ver se o cliente foi autenticado com sucesso usando o WPA
- 2.



Troubleshoot

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

Configurar no modo pessoal

O termo **modo pessoal** se refere a produtos testados quanto à interoperabilidade no modo de

operação somente PSK para autenticação. Esse modo exige a configuração manual de um PSK no AP e nos clientes. O PSK autentica os usuários por meio de uma senha ou um código de identificação na estação cliente e no AP. Não é necessário um servidor de autenticação. Um cliente pode obter acesso à rede somente se a senha do cliente corresponder à senha do AP. A senha também fornece o material de codificação que o TKIP ou o AES usa para gerar uma chave de criptografia para a criptografia dos pacotes de dados. O modo pessoal é indicado para ambientes de SOHO e não é considerado seguro para ambientes empresariais. Esta seção fornece a configuração necessária para implementar o WPA 2 no modo de operação pessoal.

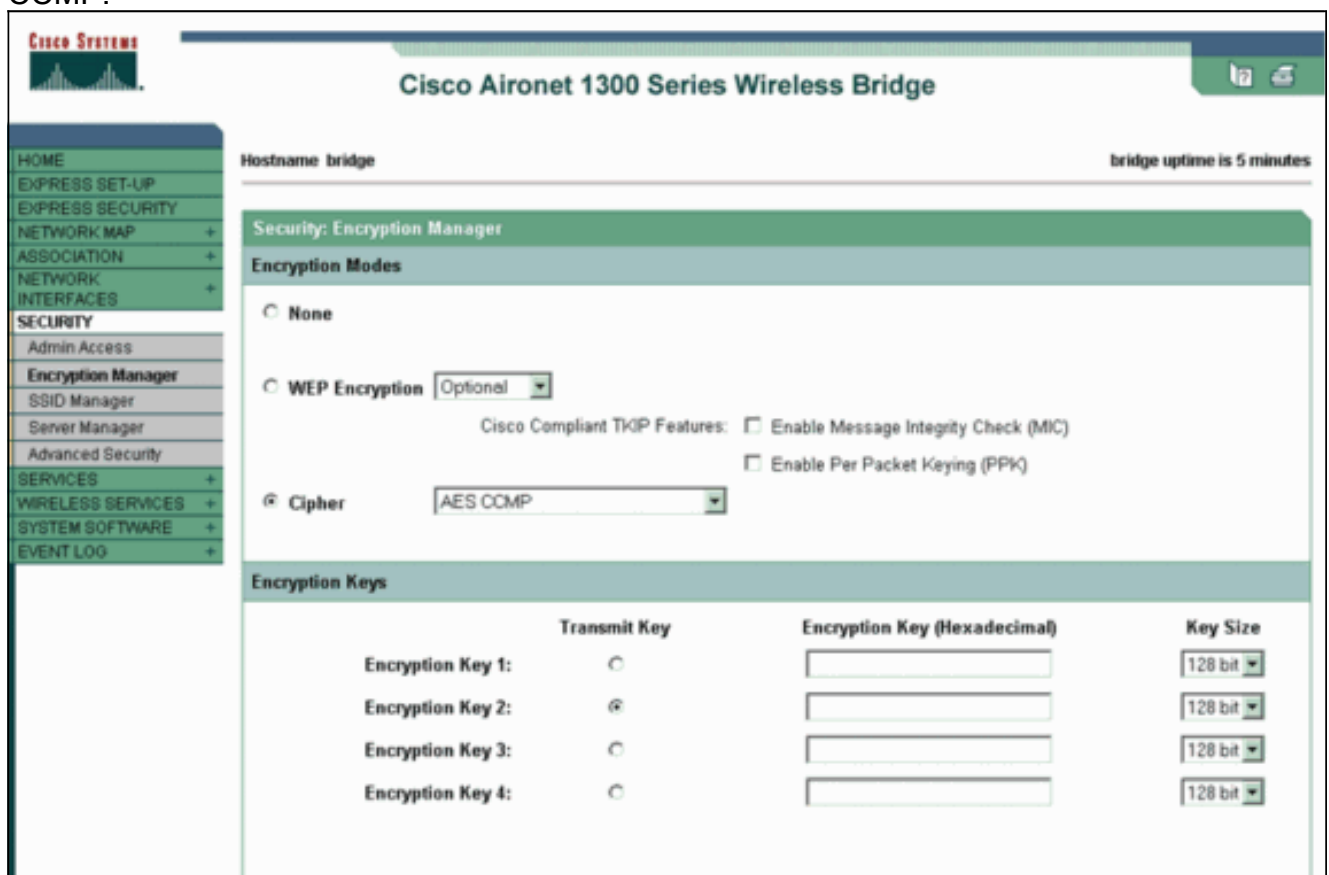
[Instalação de rede](#)

Nessa configuração, um usuário com um adaptador cliente compatível com WPA 2 autentica em um AP/uma ponte Aironet 1310G. O gerenciamento de chaves ocorre usando o PSK do WPA 2, com a criptografia AES-CCMP configurada. As seções [Configurar o AP](#) e [Configurar o adaptador cliente](#) mostram a configuração no AP e no adaptador cliente.

[Configurar o AP](#)

Conclua estes passos:

1. Escolha **Segurança > Gerenciador de criptografia** no menu à esquerda e siga estas etapas: No menu Cifra, escolha **AES CCMP**. Essa opção ativa a criptografia do AES usando o modo de contador com o CCMP.



The screenshot shows the configuration interface for a Cisco Aironet 1300 Series Wireless Bridge. The page title is "Cisco Aironet 1300 Series Wireless Bridge" and the hostname is "bridge". The "Security: Encryption Manager" section is active. Under "Encryption Modes", the "Cipher" option is selected, and the dropdown menu shows "AES CCMP". Below this, there are checkboxes for "Cisco Compliant TKIP Features": "Enable Message Integrity Check (MIC)" and "Enable Per Packet Keying (PPK)". The "Encryption Keys" section contains a table with four rows, each representing an encryption key. The "Transmit Key" column has radio buttons, and the "Encryption Key (Hexadecimal)" column has input fields. The "Key Size" column has dropdown menus, all set to "128 bit".

	Transmit Key	Encryption Key (Hexadecimal)	Key Size
Encryption Key 1:	<input type="radio"/>	<input type="text"/>	128 bit
Encryption Key 2:	<input checked="" type="radio"/>	<input type="text"/>	128 bit
Encryption Key 3:	<input type="radio"/>	<input type="text"/>	128 bit
Encryption Key 4:	<input type="radio"/>	<input type="text"/>	128 bit

Clique em Apply.

2. Escolha **Segurança > Gerenciador de SSID** e crie um novo SSID para uso com o WPA 2. Marque a caixa de seleção **Open Authentication**.

The screenshot displays the configuration interface for a Cisco Aironet 1300 Series Wireless Bridge. The page title is "Cisco Aironet 1300 Series Wireless Bridge". The hostname is "bridge" and the uptime is "7 minutes". The left sidebar contains a navigation menu with categories like HOME, EXPRESS SET-UP, SECURITY, SERVICES, and WIRELESS SERVICES. The main content area is titled "Security: SSID Manager" and "SSID Properties". It shows a "Current SSID List" with a table containing a new entry "WPA2PSK" and an existing entry "tsunami". To the right, the "SSID:" field is set to "WPA2PSK", the "VLAN:" dropdown is set to "< NONE >", and the "Network ID:" is set to "(0-4096)". Below this, the "Authentication Settings" section shows "Authentication Methods Accepted:" with three options: "Open Authentication" (checked), "Shared Authentication", and "Network EAP". Each option has a dropdown menu set to "< NO ADDITION >".

Role para baixo na janela Segurança: Gerenciador de SSID até a área Gerenciamento de chaves autenticadas e siga estas etapas: No menu Gerenciamento de chaves, escolha **Obrigatório**. Marque a caixa de seleção **WPA** à direita.

Authenticated Key Management

Key Management: Mandatory CCKM WPA

WPA Pre-shared Key: ASCII Hexadecimal

Accounting Settings

Enable Accounting

Accounting Server Priorities:

Use Defaults [Define Defaults](#)

Customize

Priority 1:

Priority 2:

Priority 3:

General Settings

Advertise Extended Capabilities of this SSID

- Advertise Wireless Provisioning Services (WPS) Support
- Advertise this SSID as a Secondary Broadcast SSID

Enable IP Redirection on this SSID

IP Address:

IP Filter (optional): [Define Filter](#)

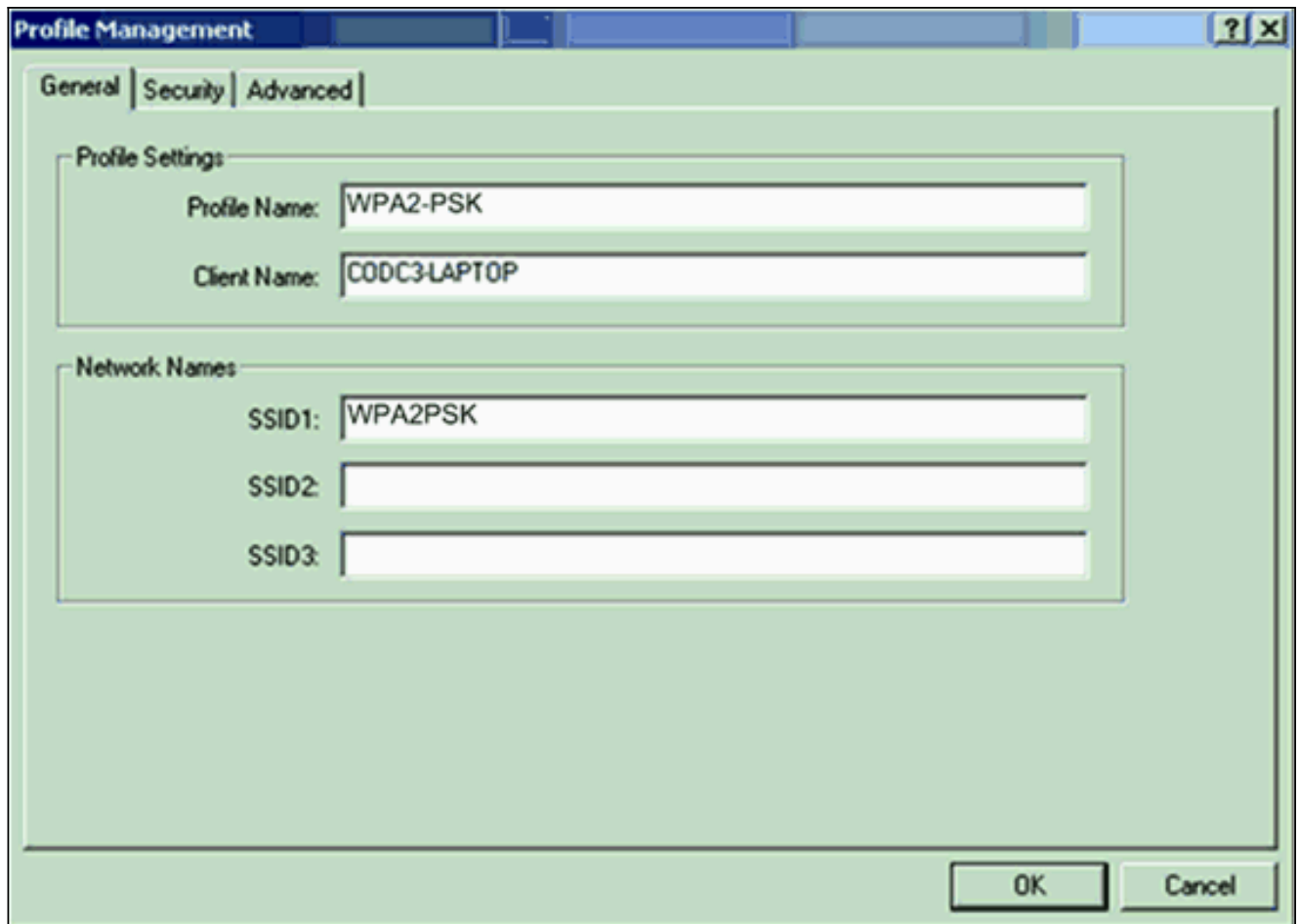
Insira a chave secreta compartilhada do PSK do WPA ou a chave da frase secreta do PSK do WPA. Essa chave deve corresponder à chave do PSK do WPA configurada no adaptador cliente. Clique em Apply.

Agora o AP pode receber solicitações de autenticação dos clientes sem fio.

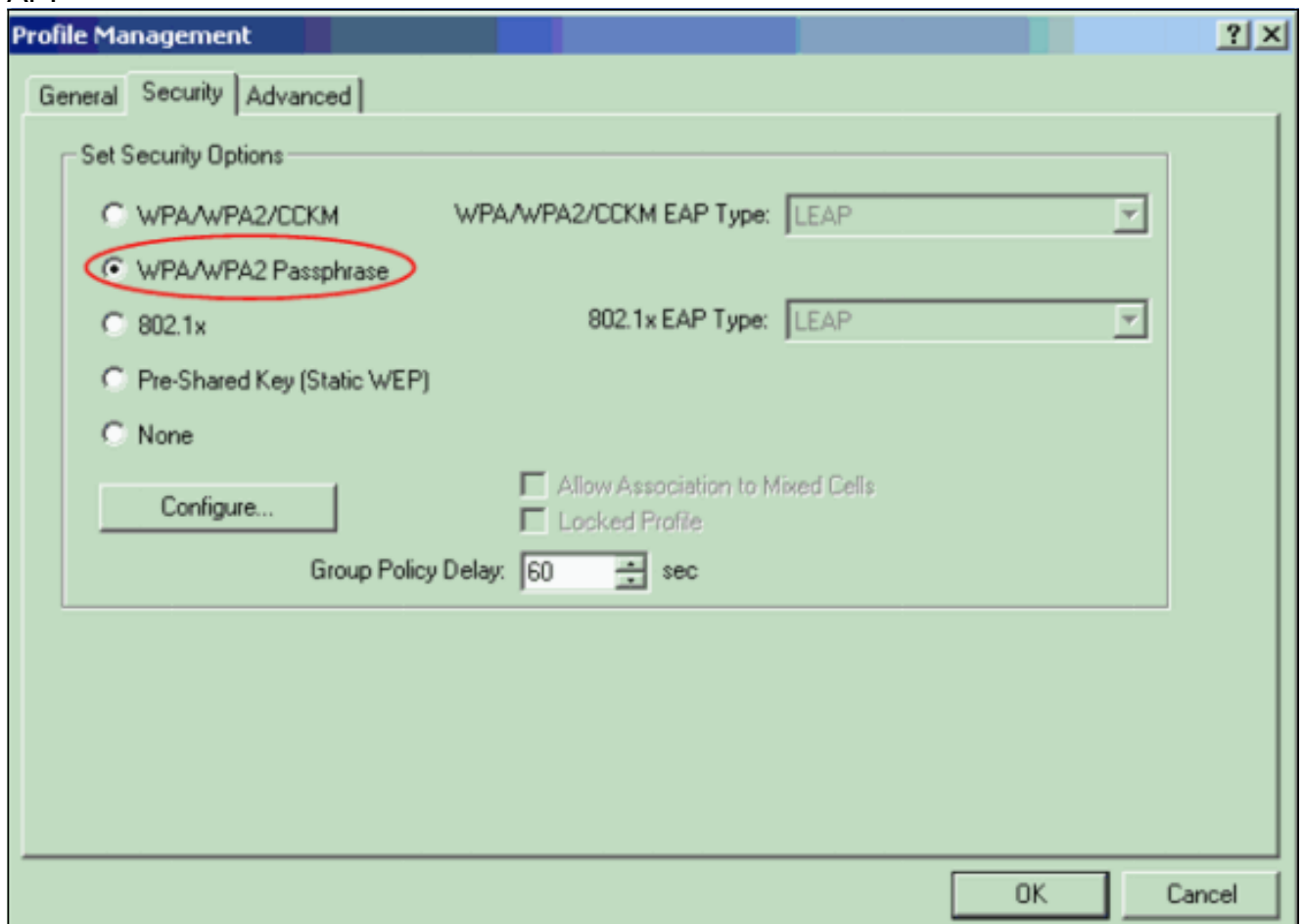
[Configurar o adaptador cliente](#)

Conclua estes passos:

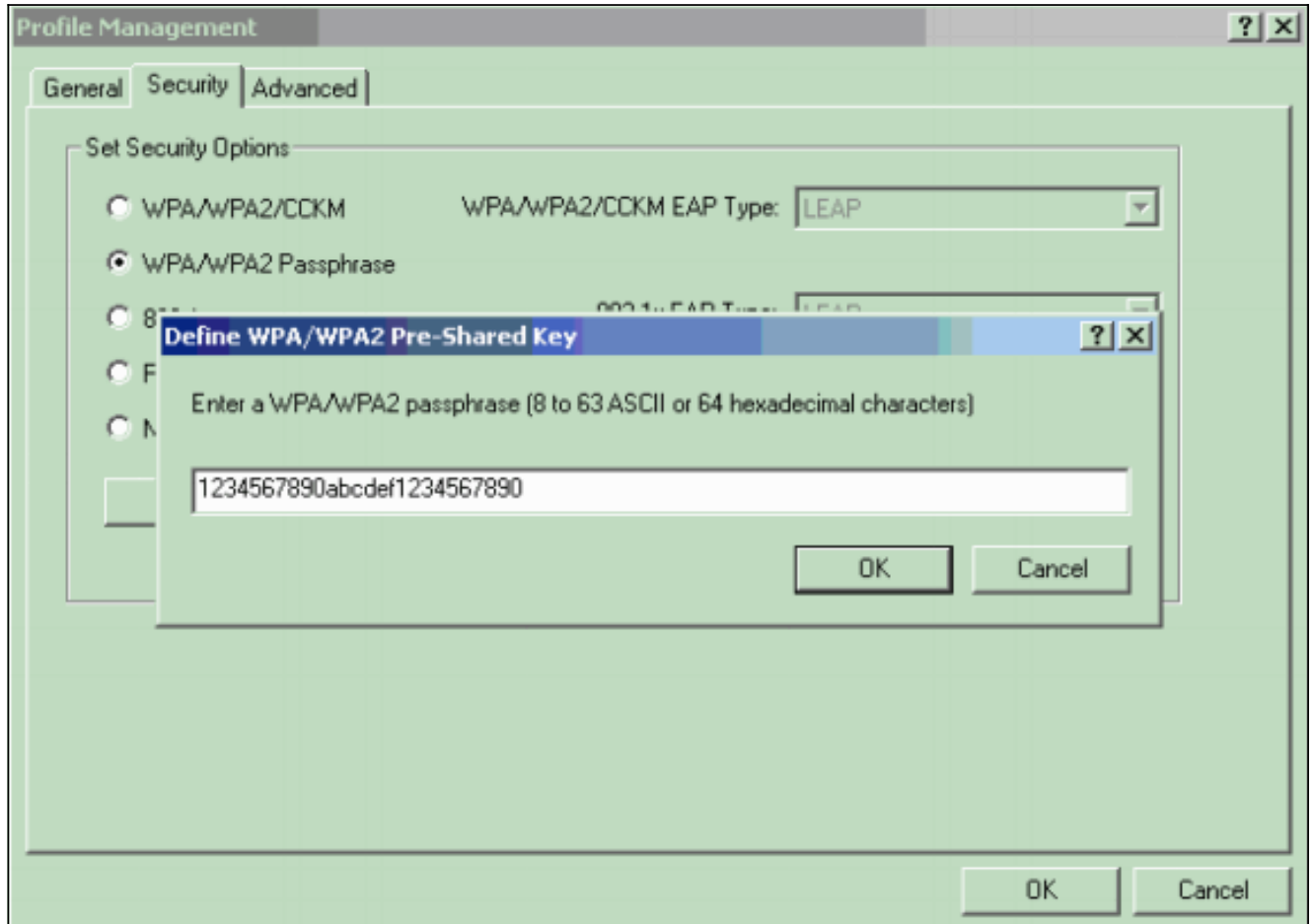
1. Na janela Gerenciamento de perfil na ADU, clique em **Novo** para criar um novo perfil. Será exibida uma nova janela em que você poderá definir a configuração do modo de operação PSK do WPA
2. Na guia Geral, insira o nome do perfil e o SSID que o adaptador cliente usará. Neste exemplo, o nome do perfil é WPA2-PSK e o SSID é WPA2PSK: **Observação:** o SSID deve corresponder ao SSID que você configurou no AP para PSK do WPA



2. Clique na guia **Segurança** e clique em **Frase secreta do WPA/WPA2**. Essa ação ativa o PSK do WPA ou o PSK do WPA 2, o que você configurar no AP.



3. Clique em Configurar. A janela Definir chave pré-compartilhada do WPA/WPA2 será exibida.
4. Obtenha a frase secreta do WPA/WPA2 com o administrador do sistema e insira a frase secreta no campo WPA/WPA2. Obtenha a frase secreta do AP em uma rede de infraestrutura ou a frase secreta de outros clientes em uma rede ad hoc. Use estas diretrizes para inserir uma frase secreta: As frases secretas do WPA/WPA2 devem conter entre 8 e 63 caracteres de texto ASCII ou 64 caracteres hexadecimais. A frase secreta do WPA/WPA2 do adaptador cliente deve corresponder à frase secreta do AP com que você planeja se comunicar.



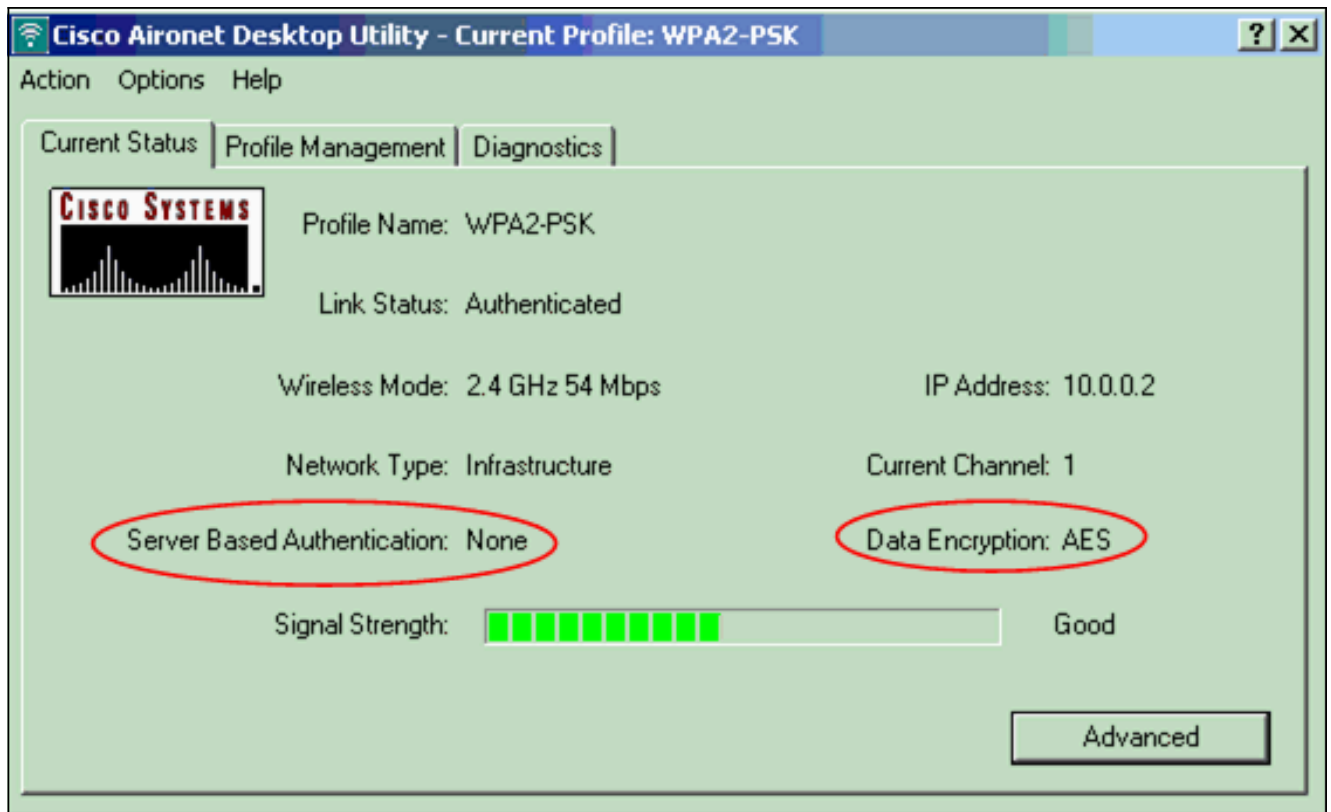
5. Clique em OK para salvar a frase secreta e retornar à janela Gerenciamento de perfil.

Verificar

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

Depois que o perfil do PSK do WPA 2 é ativado, o AP autentica o cliente com base na frase secreta do WPA 2 (PSK) e fornece acesso à WLAN.

1. Verifique o status atual da ADU para ver se a autenticação foi realizada com sucesso. Esta janela oferece um exemplo. A janela mostra que a criptografia usada é AES e que uma autenticação baseada em servidor não foi realizada:



2. Verifique o registro de eventos do AP/da ponte para ver se o cliente foi autenticado com sucesso usando o modo de autenticação do PSK do WPA

2.



Troubleshoot

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 – Wi-Fi Protected Access 2](#)
- [O que é o modo de operação combinado do WPA e como configurá-lo no AP](#)
- [Página de Suporte Wireless](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)

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.