

# Autenticação em exemplos de configuração dos controladores do Wireless LAN

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Autenticação em WLC](#)

[Soluções do Layer 1](#)

[Soluções da camada 2](#)

[Soluções da camada 3](#)

[Exemplos de configuração](#)

[Soluções da Segurança do Layer 1](#)

[Soluções da Segurança da camada 2](#)

[Soluções da Segurança da camada 3](#)

[Troubleshooting](#)

[Comandos para Troubleshooting](#)

[Informações Relacionadas](#)

## [Introdução](#)

Este documento fornece os exemplos de configuração que explicam como configurar tipos diferentes de Layer 1, a camada 2, e mergulham 3 métodos de autenticação nos controladores do Wireless LAN (WLC).

## [Pré-requisitos](#)

### [Requisitos](#)

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

- Conhecimento da configuração do Lightweight Access Points (regaços) e do Cisco WLC
- Conhecimento dos padrões de segurança 802.11i

### [Componentes Utilizados](#)

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

- Cisco 4400 WLC que executa a versão de firmware 6.0.182.0
- Cisco 1000 Series LAPs
- Adaptador de cliente Wireless de Cisco 802.11a/b/g que executa a versão de firmware 2.6
- Versão de servidor 3.2 do Cisco Secure ACS

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.

## Autenticação em WLC

A solução da Segurança da rede de Cisco Unified Wireless (UWN) empacota Layer 1 potencialmente complicado, a camada 2, e mergulha 3 componentes da Segurança do Access Point (AP) do 802.11 em um gerente simples da política que personalize políticas de segurança sistema-largas em uma base do por-Sem fio LAN (WLAN). A solução da Segurança de Cisco UWN fornece ferramentas de Gerenciamento de segurança simples, unificadas, e sistemáticas.

Estes mecanismos de segurança podem ser executados em WLC.

### Soluções do Layer 1

Restrinja o acesso do cliente baseado no número de falhas de tentativa consecutivas.

### Mergulhe 2 soluções

**Nenhum autenticação** — Quando esta opção é selecionada da lista de drop-down da Segurança da camada 2, nenhuma autenticação da camada 2 está executada no WLAN. Este é o mesmo que a autenticação aberta do padrão do 802.11.

**WEP Estática** — Com a Wired Equivalent Privacy (WEP) estática, todos os APs e as NICs de rádio clientes em uma WLAN devem usar a mesma chave de criptografia. Cada estação de envio cifra o corpo de cada quadro com uma chave de WEP antes da transmissão, e a estação de recepção decifra-a que usa uma chave idêntica em cima da recepção.

**802.1x** — Configura a WLAN para usar a autenticação 802.1x. O uso do IEEE 802.1X oferece uma estrutura eficaz a fim autenticar e controlar o tráfego de usuário a uma rede protegida, assim como varia dinamicamente chaves de criptografia. o 802.1X amarra um protocolo chamado Extensible Authentication Protocol (EAP) aos media prendido e WLAN e apoia métodos de autenticação múltipla.

**WEP Estática + 802.1x** — Esta opção de segurança da camada 2 habilita a 802.1x e a WEP estática. Os clientes podem usar a autenticação do WEP estático ou do 802.1x a fim conectar à rede.

**Wi-Fi Protected Access (WPA)** — O WPA, ou WPA1, e o WPA2 são soluções de segurança

baseadas em padrões da Wi-Fi Alliance que fornecem proteção de dados e controle de acesso para sistemas de WLAN. WPA1 é compatível com o padrão da IEEE 802.11i mas foi executado antes da ratificação do padrão. O WPA 2 é a implementação da Wi-Fi Alliance do padrão IEEE 802.11i ratificado.

À revelia, WPA1 usa o Temporal Key Integrity Protocol (TKIP) e o Message Integrity Check (MIC) para a proteção de dados. O WPA2 usa o algoritmo de criptografia mais forte do Advanced Encryption Standard usando o modo contrário com protocolo do código de autenticação de mensagens do Cipher Block Chaining (AES-CCMP). WPA1 e o WPA2 usam o 802.1X para o gerenciamento chave autenticado à revelia. Contudo, estas opções estão igualmente disponíveis: PSK, CCKM, e CCKM+802.1x. Se você seleciona o CCKM, Cisco permite somente os clientes que apoiam o CCKM. Se você seleciona CCKM+802.1x, Cisco permite os clientes NON-CCKM igualmente.

**CKIP** — Cisco fecha o protocolo da integridade (CKIP) é um protocolo de segurança proprietário Cisco para media de criptografia do 802.11. CKIP melhora a Segurança do 802.11 no modo de infraestrutura usando a permutação chave, o MIC, e o número de sequência de mensagem. O Software Release 4.0 apoia CKIP com chave estática. Para que esta característica opere-se corretamente, você deve permitir os elementos de informação de Aironet (IE) para o WLAN. Os ajustes CKIP especificados em um WLAN são imperativos para todo o cliente que tentar associar. Se o WLAN é configurado para a permutação chave CKIP e o MMH MIC, o cliente deve apoiar ambos. Se o WLAN é configurado para somente uma destas características, o cliente deve apoiar somente esta característica CKIP. Os WLC apoiam somente CKIP estático (como o WEP estático). Os WLC não apoiam CKIP com 802.1x (CKIP dinâmico).

### Soluções da camada 3

**Nenhum** — Quando esta opção é selecionada da lista de drop-down da Segurança da camada 3, nenhuma autenticação da camada 3 está executada no WLAN.

**Nota:** O exemplo de configuração para nenhuma autenticação da camada 3 e nenhuma autenticação da camada 2 é explicado no [nenhuns](#) seção da [autenticação](#).

**Política da Web (Autenticação da Web e Web Passthrough)** — A autenticação da Web é normalmente usada por clientes que desejam implementar uma rede com acesso de convidados. Em uma rede do convidado-acesso, há uma autenticação inicial do nome de usuário e senha, mas a Segurança não é exigida para o tráfego subsequente. As implementações típicas podem incluir lugar do “ponto ativo”, tais como T-Mobile ou Starbucks.

A autenticação da Web para Cisco WLC é feita localmente. Você cria uma relação e associa então um identificador do conjunto WLAN/service (SSID) com essa relação.

A autenticação da Web fornece a autenticação simples sem um suplicante ou um cliente. Tenha em mente que a autenticação da Web não proporciona a criptografia de dados. A autenticação da Web é usada tipicamente como um acesso simples de convidado a um "hot spot" ou à atmosfera de campus, onde o único interesse é a conectividade.

A transmissão da Web é uma solução através de que os usuários Wireless estão reorientados a uma página aceitável da política de utilização sem ter que autenticar quando conectam ao Internet. Esta reorientação é tomada de pelo WLC próprio. A única exigência é configurar o WLC para a transmissão da Web, que é basicamente autenticação da Web sem ter que incorporar todas as credenciais.

[VPN Passthrough](#) — O VPN Passthrough é um recurso que permite que um cliente estabeleça um túnel somente com um servidor VPN específico. Conseqüentemente, se você precisa de alcançar firmemente o servidor de VPN configurado assim como um outro servidor de VPN ou o Internet, isto não é possível com a transmissão VPN permitida no controlador.

Nas próximas seções, os exemplos de configuração são fornecidos para cada um dos mecanismos da autenticação.

## Exemplos de configuração

Antes que você configure os WLAN e os tipos do autenticação, você deve configurar o WLC para a operação básica e registrar os regaços ao WLC. Este documento supõe que o WLC está configurado para a operação básica e que os regaços estão registrados ao WLC. Se você é um novo usuário que tenta setup o WLC para a operação básica com regaços, refira o [registro de pouco peso AP \(REGAÇO\) a um controlador do Wireless LAN \(WLC\)](#).

## Soluções da Segurança do Layer 1

Os clientes Wireless podem ser acesso restrito baseado no número de falhas de tentativa consecutivas alcançar a rede de WLAN. A exclusão do cliente ocorre nestas circunstâncias à revelia. Estes valores não podem ser mudados.

- Falha de autenticação consecutiva do 802.11 (as épocas 5 consecutivas, a 6a tentativa é excluída)
- Falhas consecutivas da associação do 802.11 (as épocas 5 consecutivas, a 6a tentativa é excluída)
- Falhas de autenticação consecutivas do 802.1x (3 vezes consecutivas, a 4o tentativa é excluída)
- Falha externo do servidor da política
- Tentativa de usar o endereço IP de Um ou Mais Servidores Cisco ICM NT já atribuído a um outro dispositivo (roubo IP ou reutilização IP)
- Autenticação da Web consecutiva (3 vezes consecutivas, a 4o tentativa é excluída)

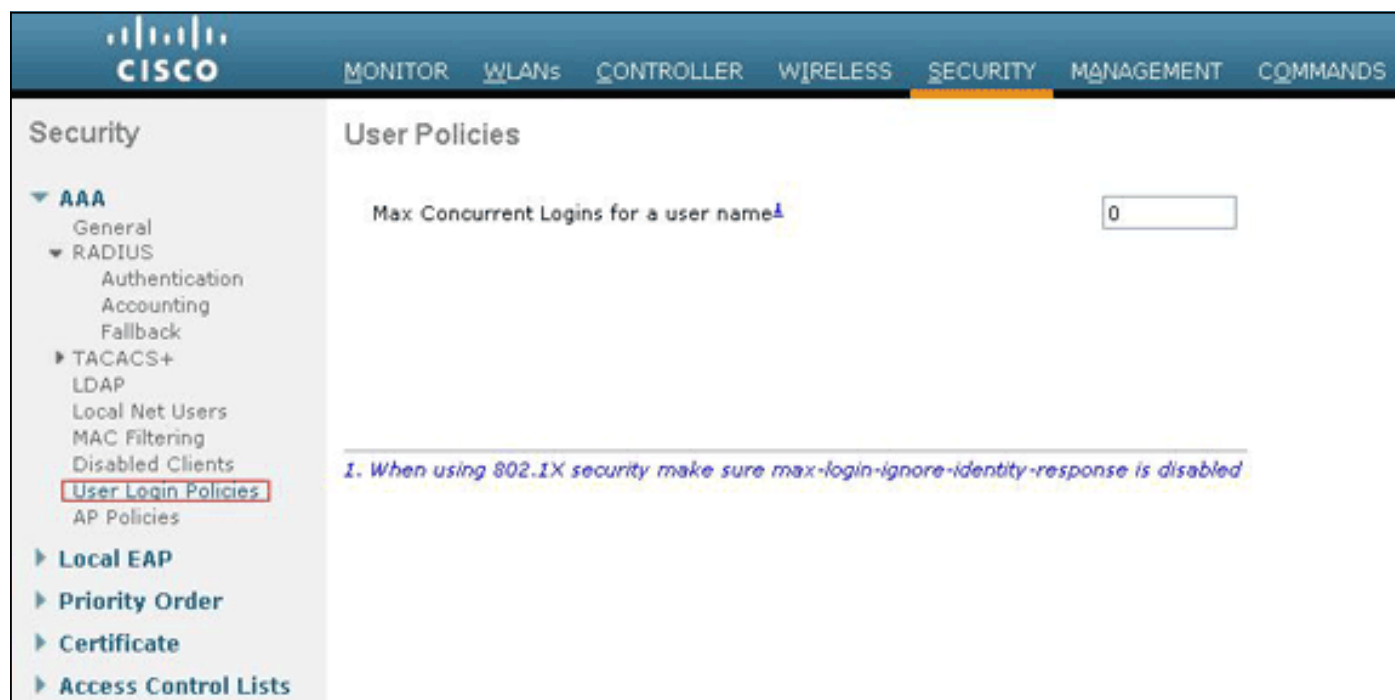
A fim encontrar as políticas da exclusão do cliente, a **Segurança do clique** no menu superior, e escolher então **políticas wireless da proteção > políticas da exclusão do cliente** a navegação no lado esquerdo da página.

The screenshot shows the Cisco Security configuration interface. The top navigation bar includes MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, and MANAGEMENT. The left sidebar shows a tree view under Security, with 'Client Exclusion Policies' highlighted in a red box. The main content area, titled 'Client Exclusion Policies', lists five checked options: Excessive 802.11 Association Failures, Excessive 802.11 Authentication Failures, Excessive 802.1X Authentication Failures, IP Theft or IP Reuse, and Excessive Web Authentication Failures.

O temporizador da exclusão pode ser configurado. As opções da exclusão podem ser permitidas ou desabilitado pelo controlador. O temporizador da exclusão pode ser permitido ou desabilitado pelo WLAN.

The screenshot shows the Cisco WLANs configuration interface. The top navigation bar includes MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The left sidebar shows 'WLANs > Edit' with 'Advanced' selected. The main content area has tabs for General, Security, QoS, and Advanced. Under the Advanced tab, the 'Client Exclusion' option is checked and highlighted in a red box, with a '60' value entered in the 'Timeout Value (secs)' field. Other settings include 'Allow AAA Override' (unchecked), 'Coverage Hole Detection' (checked), 'Enable Session Timeout' (checked, 1800), 'Aironet IE' (checked), 'Diagnostic Channel' (unchecked), 'IPv6 Enable' (unchecked), 'Override Interface ACL' (None), 'P2P Blocking Action' (Forward-UpStream), 'VoIP Snooping and Reporting' (unchecked), 'DHCP' (DHCP Server unchecked, DHCP Addr. Assignment unchecked), 'Management Frame Protection (MFP)' (Infrastructure MFP Protection checked, MFP Client Protection Optional), 'DTIM Period (in beacon intervals)' (802.11a/n 1, 802.11b/g/n 1), and 'NAC' (State unchecked).

O número máximo de inícios de uma sessão simultâneos para um nome de usuário único é à revelia 0. Você pode incorporar qualquer valor entre 0 e 8. Este parâmetro pode ser ajustado em **políticas da SEGURANÇA > AAA > do login de usuário** e permite que você especifiquem o número máximo de inícios de uma sessão simultâneos para um único nome do cliente, entre um e oito, ou 0 = ilimitado. Aqui está um exemplo:



The screenshot shows the Cisco Security configuration interface. The top navigation bar includes MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY (highlighted), MANAGEMENT, and COMMANDS. The left sidebar shows the Security menu with AAA expanded, and User Login Policies highlighted. The main content area is titled 'User Policies' and contains a field for 'Max Concurrent Logins for a user name' with a value of 0. A note below the field reads: '1. When using 802.1X security make sure max-login-ignore-identity-response is disabled'.

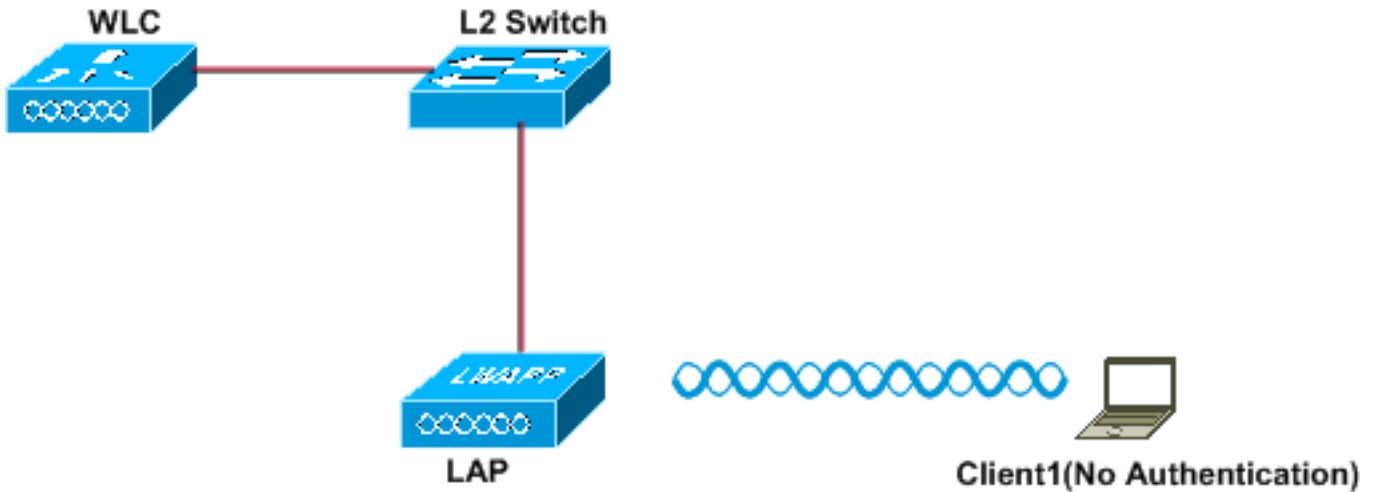
## [Soluções da Segurança da camada 2](#)

### [Nenhuma Autenticação](#)

Este exemplo mostra um WLAN configurado sem autenticação.

**Nota:** Este exemplo igualmente trabalha para nenhuma autenticação da camada 3.

## Wireless LAN With No Authentication



Layer 2 Security: None

Layer 3 Security: None

SSID:NullAuthentication

### [Configurar o WLC para nenhuma autenticação](#)

Termine estas etapas a fim configurar o WLC para esta instalação:

1. Clique **WLAN** do controlador GUI a fim criar um WLAN.A janela WLANs aparece. Este indicador alista os WLAN configurados no controlador.
2. O clique **vai** a fim configurar um WLAN novo.
3. Incorpore os parâmetros para o WLAN. Este exemplo mostra a configuração para este WLAN.

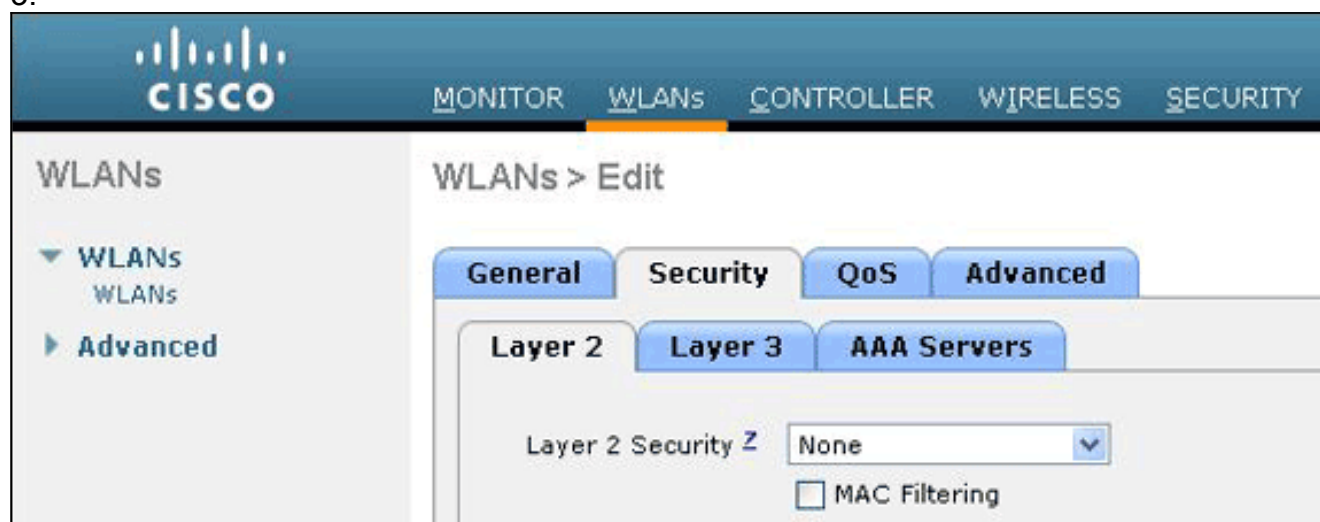
The screenshot shows the Cisco WLC GUI with the 'WLANs' tab selected. The 'WLANs > New' configuration page is displayed, showing the following fields:

Type	WLAN
Profile Name	WLAN1
SSID	NullAuthentication
ID	1

4. Clique em Apply.
5. No o WLAN > edita o indicador, define os parâmetros específicos ao WLAN.
6. Clique a **ABA de segurança**, e não escolha **nenhuns** para a Segurança da camada 2 e da

camada

3.



**Nota:** Para que um WLAN torne-se ativo, o estado deve ser permitido. Para permiti-lo, verifique a caixa de **verificação de status** sob o tab geral. Isto não permite nenhuma autenticação para este WLAN.

7. Escolha outros parâmetros baseados em seus requisitos de projeto. Este exemplo usa os valores padrão.
8. Clique em Apply.

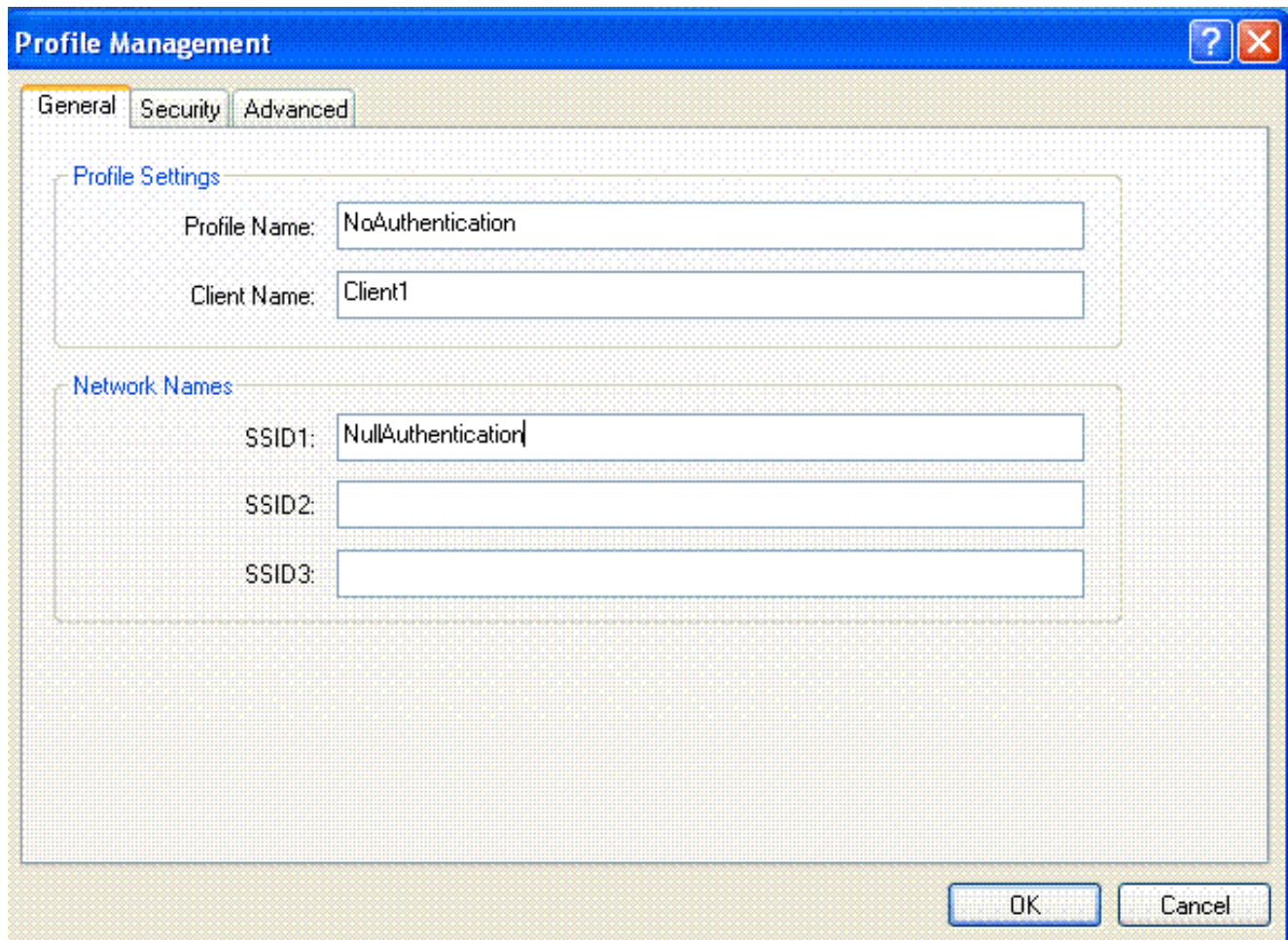
### [Configurar o cliente Wireless para nenhuma autenticação](#)

Termine estas etapas a fim configurar o cliente do Wireless LAN para esta instalação:

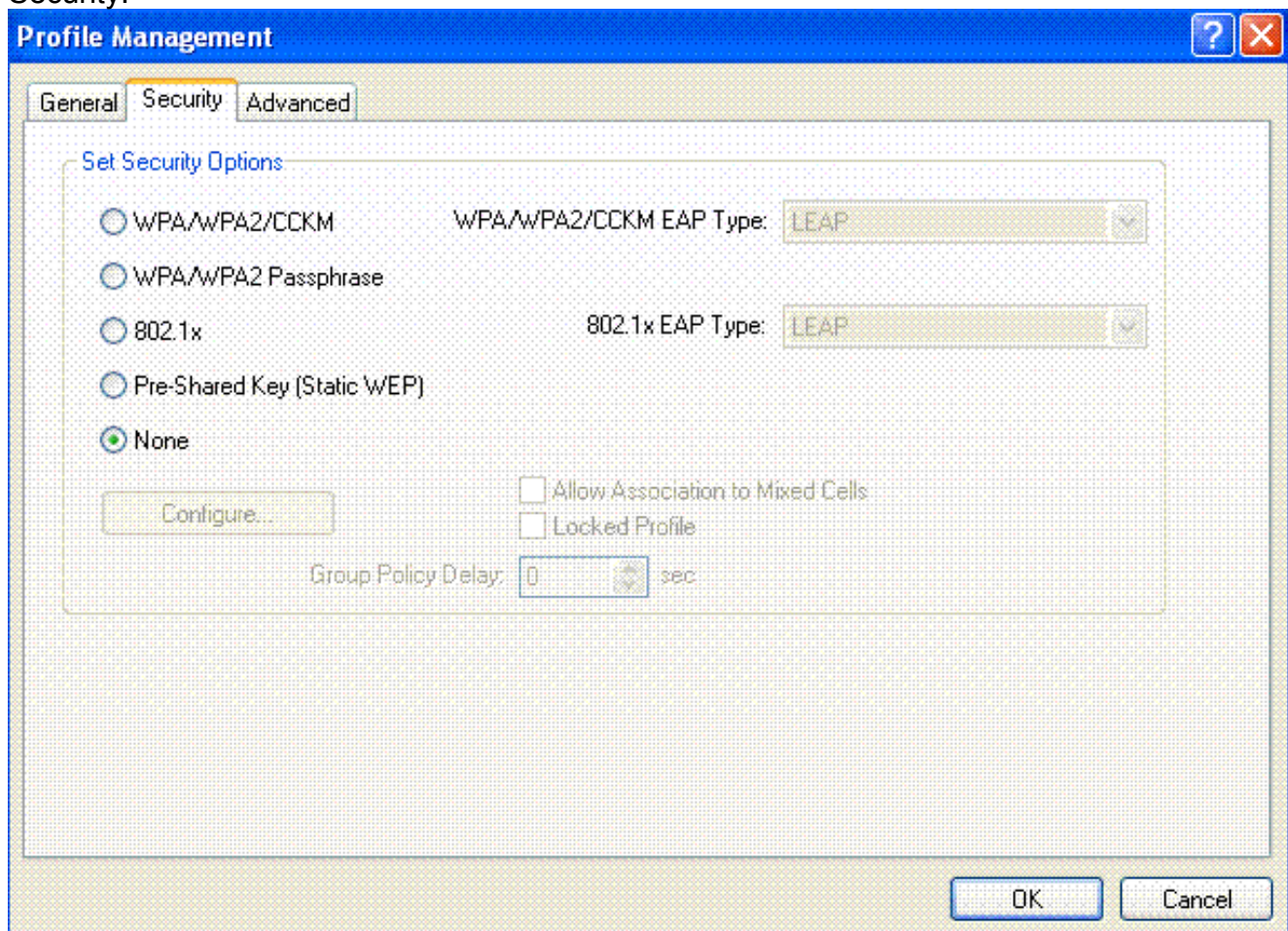
**Nota:** Este documento usa um adaptador cliente de Aironet 802.11a/b/g que execute o firmware 3.5 e explique a configuração do adaptador cliente com versão ADU 3.5.

1. A fim criar um perfil novo, clique a aba do **Gerenciamento do perfil no ADU**.
2. Clique em **New**.
3. Quando os indicadores (gerais) do indicador do Gerenciamento do perfil, terminarem estas etapas a fim ajustar o nome de perfil, o nome do cliente, e o SSID: Dê entrada com o nome do perfil no campo de nome de perfil. Este exemplo usa *NoAuthentication* como o nome de perfil. Dê entrada com o nome do cliente no campo de nome do cliente. O nome do cliente é usado para identificar o cliente Wireless na rede de WLAN. Esta configuração usa o *cliente1* para o nome do cliente. Sob nomes de rede, incorpore o SSID que deve ser usada para este perfil. O SSID é o mesmo que o SSID que você configurou no WLC. O SSID neste exemplo é *NullAuthentication*.

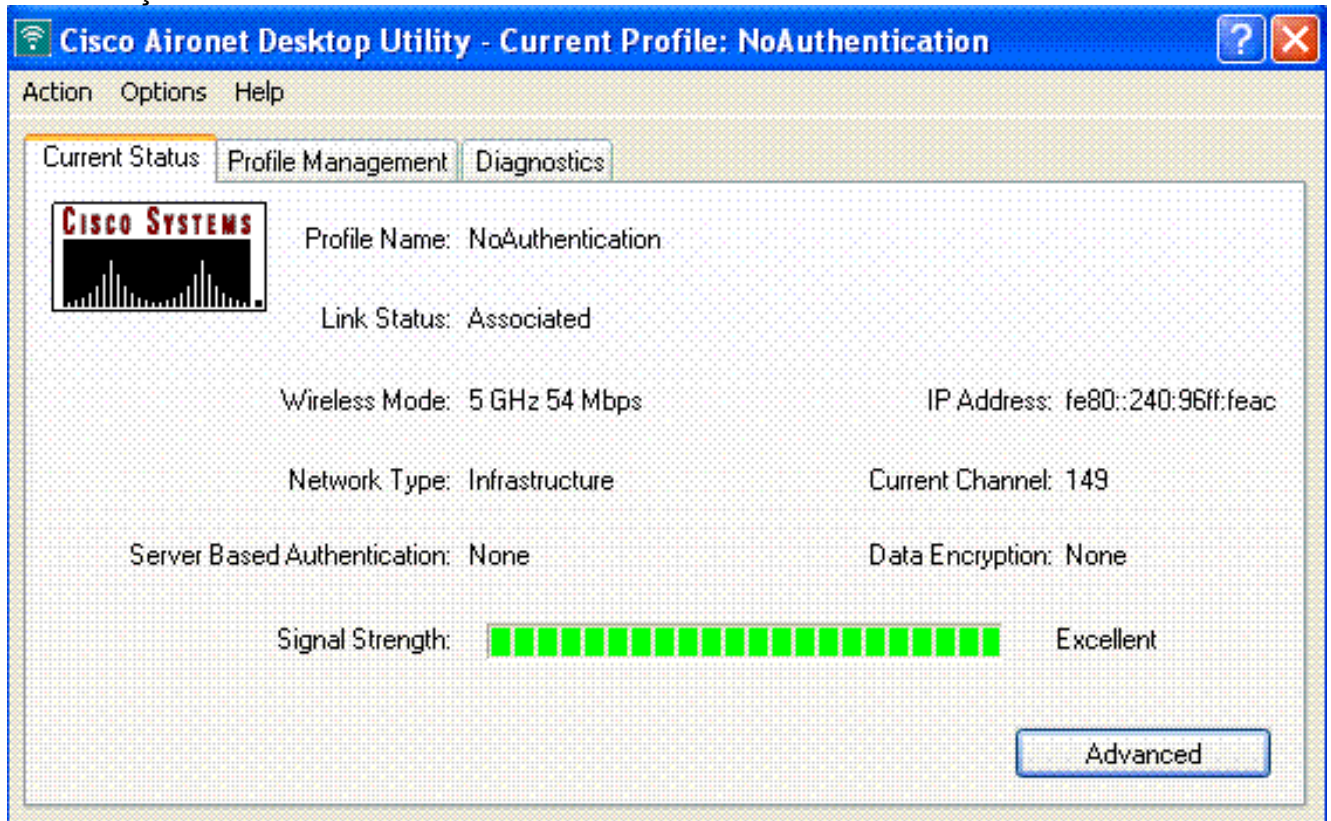




4. Clique na guia Security.



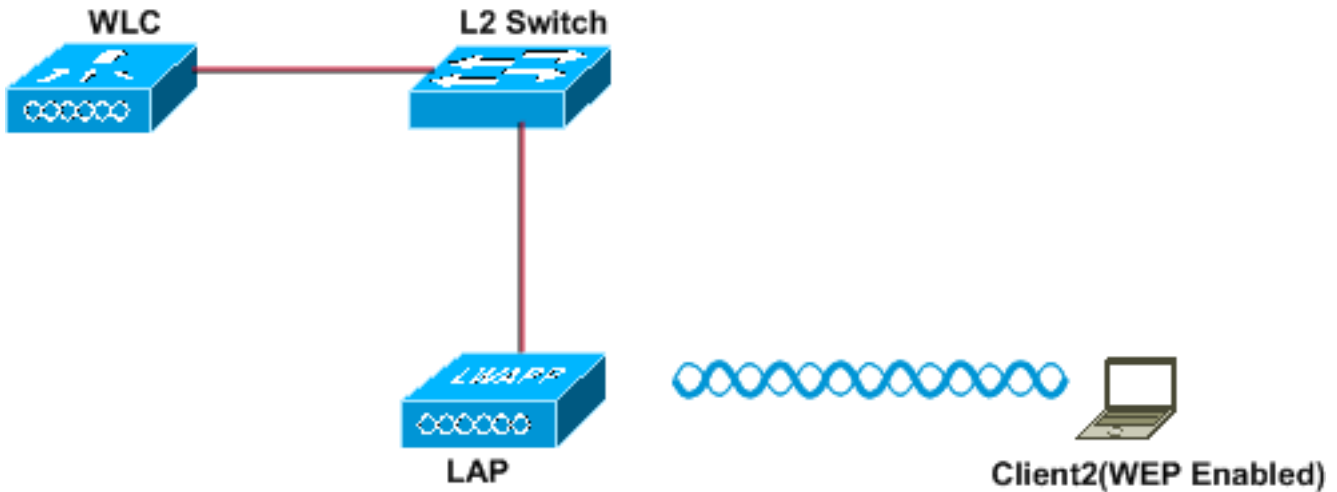
5. Não clique o **nenhuns** botão de rádio sob opções de segurança do grupo, e clique então a **APROVAÇÃO**. Quando o SSID é ativado, o cliente Wireless conecta ao WLAN sem nenhuma autenticação.



### [WEP estático](#)

Este exemplo mostra um WLAN configurado com WEP estático.

# Wireless LAN With Static WEP



Layer 2 Security: Static-WEP  
Layer 3 Security: None

SSID:Static-WEP  
WEP-Key Size: 128-bit  
WEP Key:1234567890abc

## [Configurar o WLC para o WEP estático](#)

Termine estas etapas a fim configurar o WLC para esta instalação:

1. Clique **WLAN** do controlador GUI a fim criar um WLAN.A janela WLANs aparece. Este indicador alista os WLAN configurados no controlador.
2. Clique **novo** a fim configurar um WLAN novo.
3. Incorpore o ID de WLAN e o WLAN SSID.Neste exemplo, o WLAN é nomeado *StaticWEP* e o ID de WLAN é 2.

CISCO

MONITOR **WLANs** CONTROLLER WIRELESS SECURITY MANAGEMENT

WLANs

WLANs > New

Type: WLAN

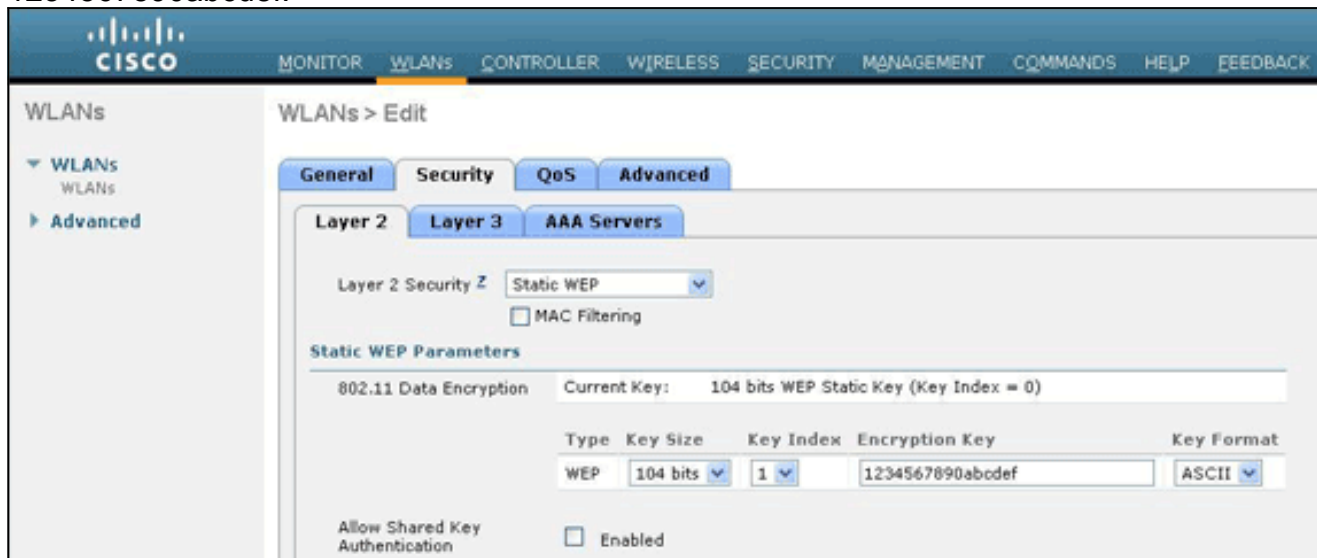
Profile Name: WLAN2

SSID: StaticWEP

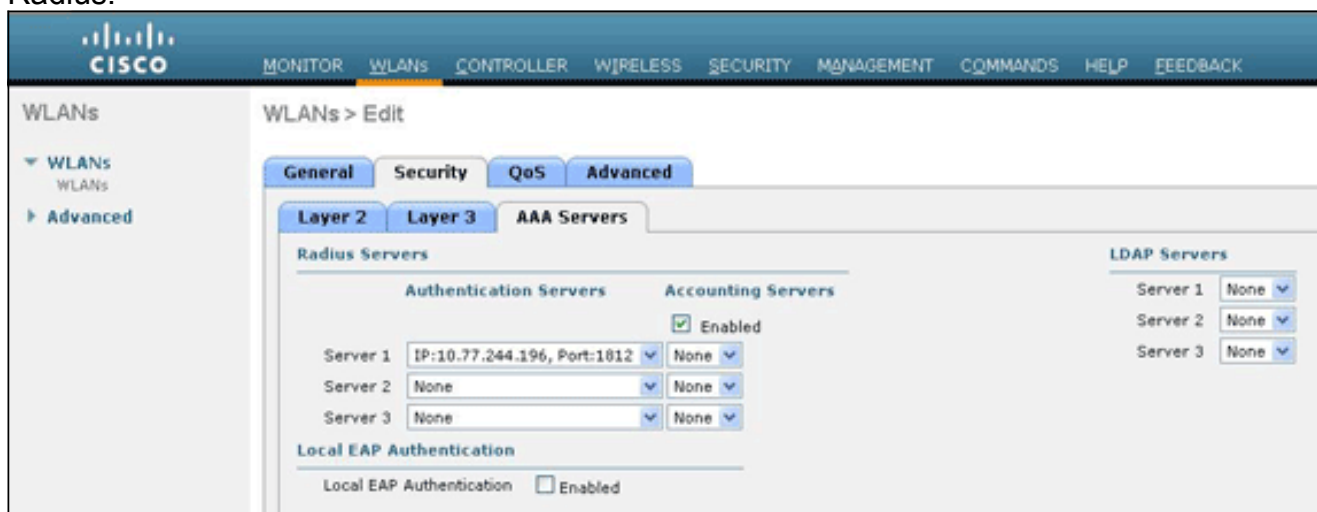
ID: 2

4. Clique em Apply.

5. No o WLAN > edita o indicador, define os parâmetros específicos ao WLAN. Da lista de drop-down da camada 2, escolha o **WEP estático**. Isto permite o WEP estático para este WLAN. Sob parâmetros do WEP estático, escolha o deslocamento predeterminado do tamanho da chave de WEP e o chave, e incorpore a chave de criptografia do WEP estático. O tamanho chave pode ser 40 bit ou 104 bit. O deslocamento predeterminado chave pode estar entre 1 e 4. Um deslocamento predeterminado de chave de WEP original pode ser aplicado a cada WLAN. Porque há somente quatro deslocamentos predeterminados de chave de WEP, simplesmente quatro WLAN podem ser configurados para a criptografia da camada 2 do WEP estático. Neste exemplo, 104 o bit WEP é usado e a chave de WEP usada é 1234567890abcdef.



Verifique se o servidor Radius é configurado para a autenticação. O servidor Radius pode ser configurado na **ABA de segurança** encontrada em **AAA > raio > autenticação**. Uma vez que configurado, o servidor Radius deve ser atribuído ao WLAN para a autenticação. Vá ao **> segurança > aos servidores AAA WLAN** a fim atribuir o servidor Radius ao WLAN para a autenticação. Neste exemplo, 10.77.244.196 é o servidor Radius.



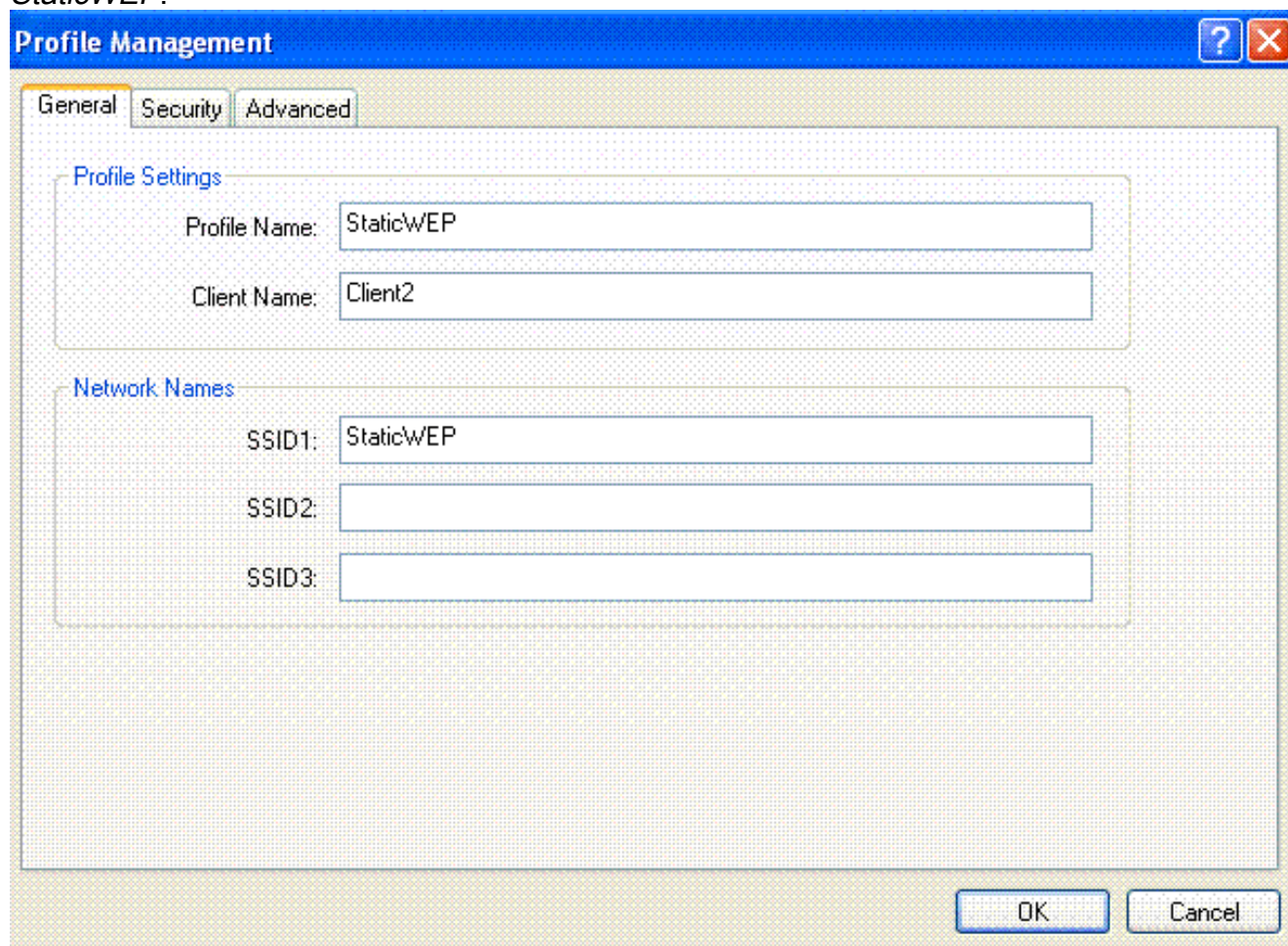
6. Escolha outros parâmetros baseados em seus requisitos de projeto. Este exemplo usa os valores padrão.
7. Clique em Apply. **Nota:** O WEP é representado sempre no hexadecimal (encantar). Quando você incorpora a chave de WEP ao ASCII, a corda ASCII WEP está convertida para encantar, que é usada para cifrar o pacote. Não há nenhum método padrão que os

vendedores executam para converter encantam ao ASCII, porque alguns farão acolchoar quando outro não. Consequentemente, para a compatibilidade máxima do inter-vendedor, o uso encanta para suas chaves de WEP. **Nota:** Se você quer permitir a autenticação de chave compartilhada para o WLAN, verifique a caixa de verificação da **autenticação de chave compartilhada reservar** sob parâmetros do WEP estático. Esta maneira, se o cliente é configurado igualmente para a autenticação de chave compartilhada, autenticação de chave compartilhada seguida pela criptografia de WEP dos pacotes ocorrerá no WLAN.

### Configurar o cliente Wireless para o WEP estático

Termine estas etapas a fim configurar o cliente do Wireless LAN para esta instalação:

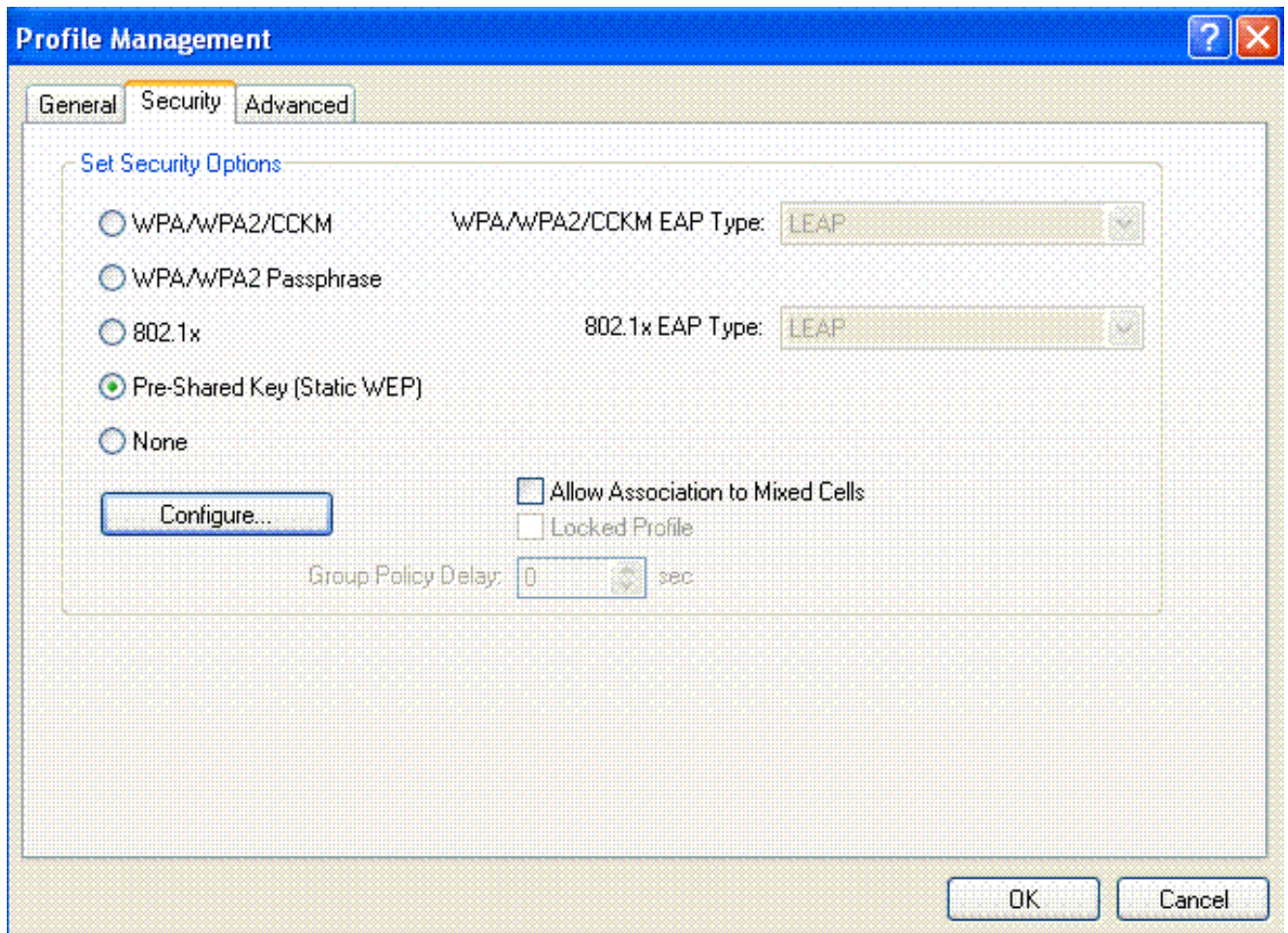
1. A fim criar um perfil novo, clique a aba do **Gerenciamento do perfil** no ADU.
2. Clique em **New**.
3. Quando os indicadores (gerais) do indicador do Gerenciamento do perfil, terminarem estas etapas a fim ajustar o nome de perfil, o nome do cliente, e o SSID: Dê entrada com o nome do perfil no campo de nome de perfil. Este exemplo usa *StaticWEP* como o nome de perfil. Dê entrada com o nome do cliente no campo de nome do cliente. O nome do cliente é usado para identificar o cliente Wireless na rede de WLAN. Esta configuração usa o *cliente 2* para o nome do cliente. Sob nomes de rede, incorpore o SSID que deve ser usada para este perfil. O SSID é o mesmo que o SSID que você configurou no WLC. O SSID neste exemplo é *StaticWEP*.



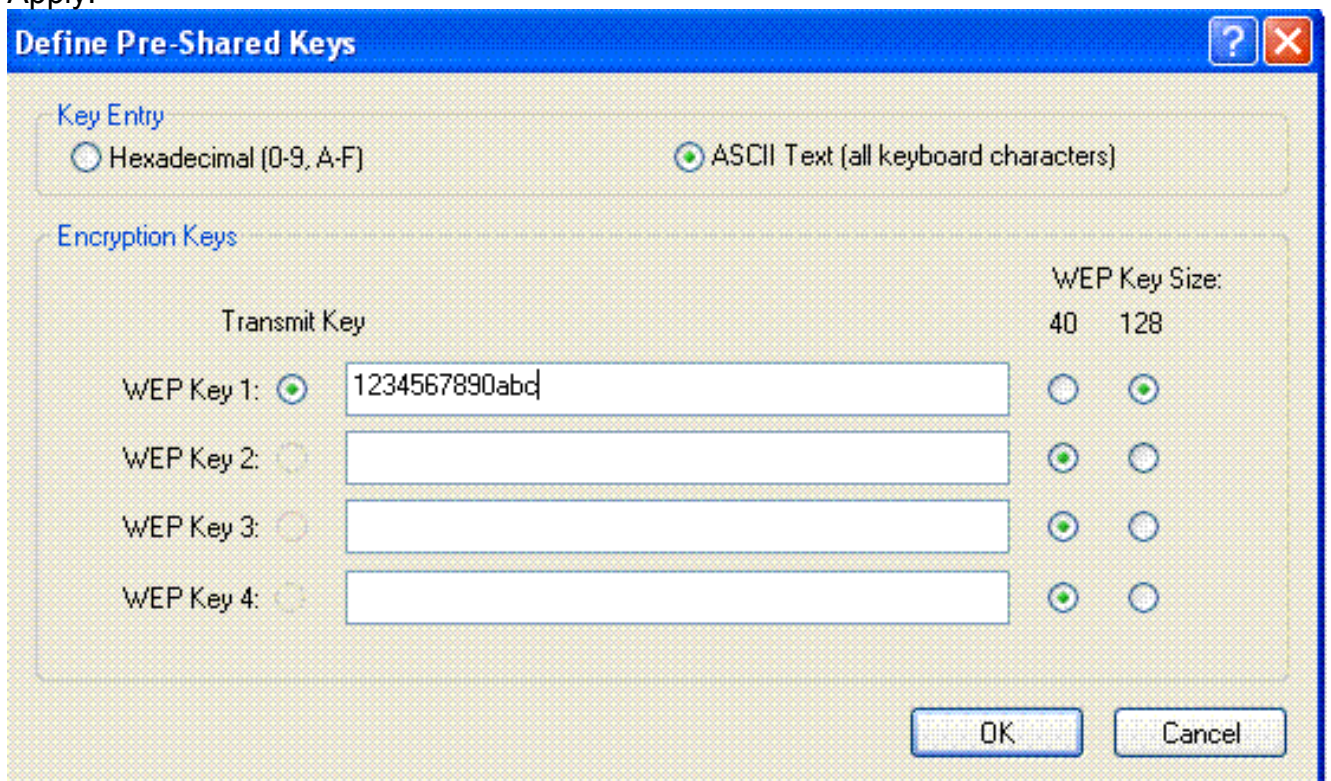
The screenshot shows a 'Profile Management' dialog box with three tabs: 'General', 'Security', and 'Advanced'. The 'General' tab is selected. It contains two sections: 'Profile Settings' and 'Network Names'. In 'Profile Settings', 'Profile Name' is 'StaticWEP' and 'Client Name' is 'Client2'. In 'Network Names', 'SSID1' is 'StaticWEP', 'SSID2' is empty, and 'SSID3' is empty. 'OK' and 'Cancel' buttons are at the bottom right.

Field	Value
Profile Name	StaticWEP
Client Name	Client2
SSID1	StaticWEP
SSID2	
SSID3	

4. Clique na guia **Security**.

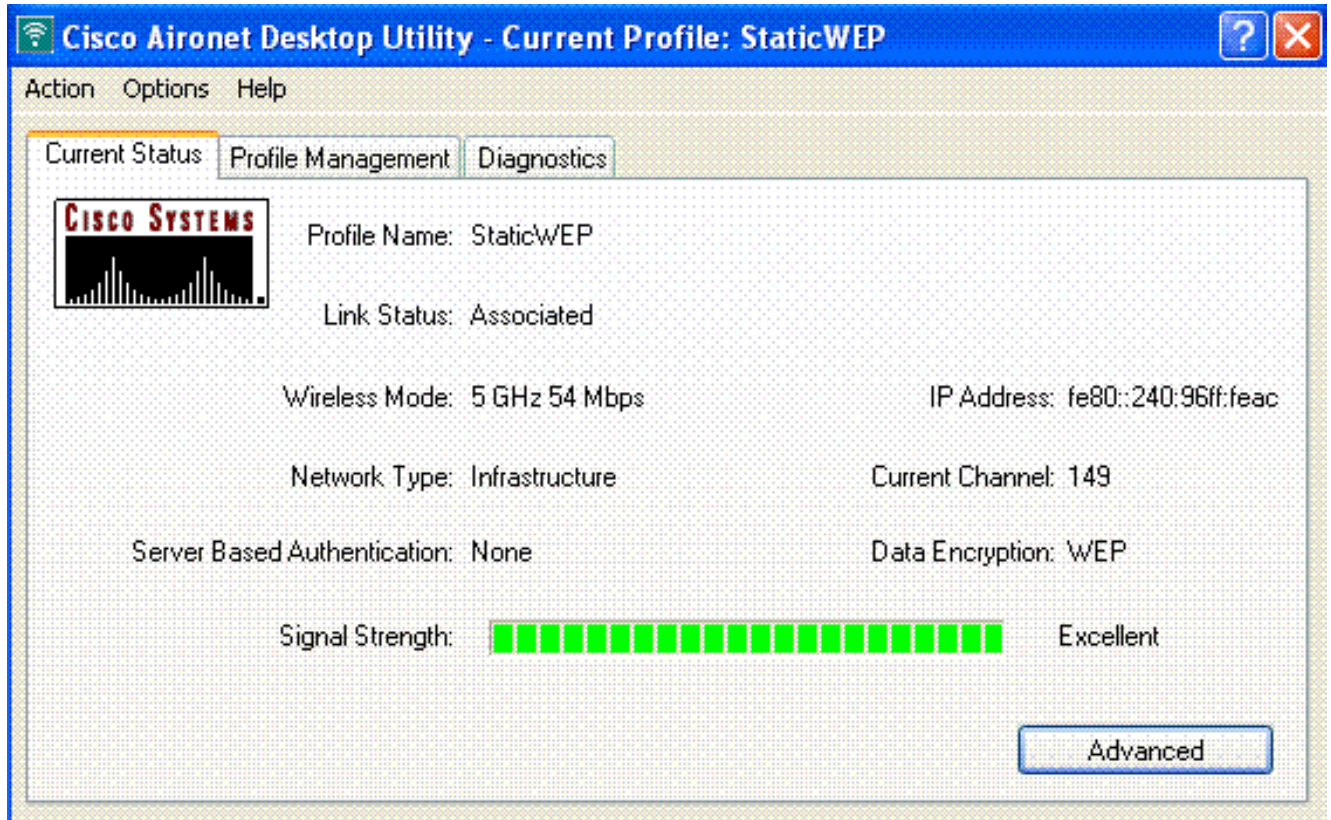


5. Escolha a **chave pré-compartilhada (WEP estático)** sob opções de segurança do grupo.
6. O clique **configura**, e define o tamanho da chave de WEP e a chave de WEP. Isto deve combinar com a chave de WEP configurada no WLC para este WLAN.
7. Clique em **Apply**.



Quando o SSID é ativado, o cliente Wireless conecta ao WLAN e os pacotes são cifrados usando a chave de WEP

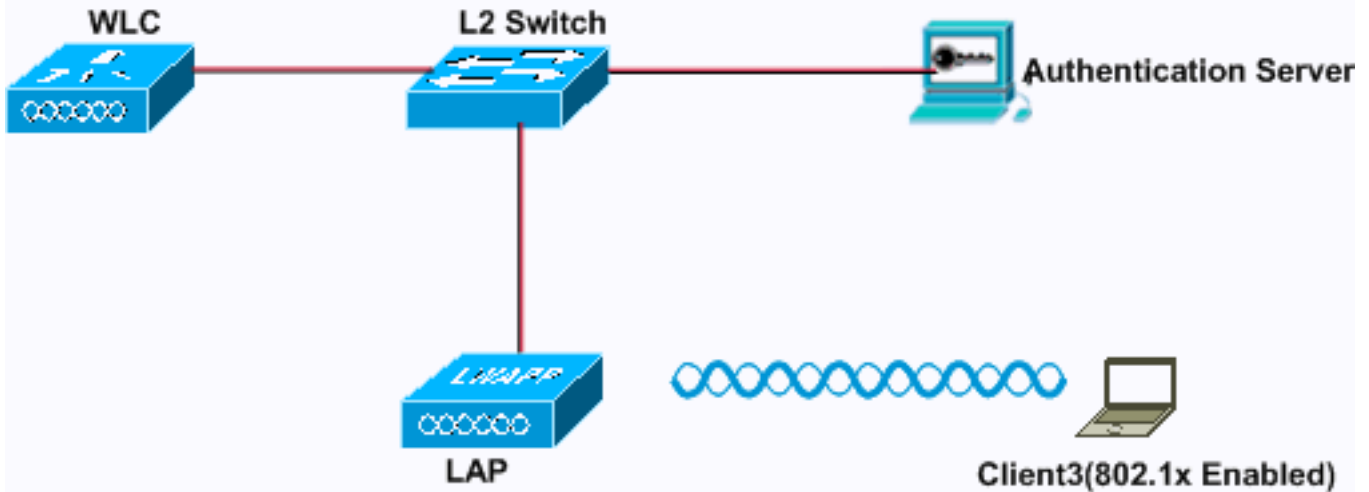
estático.



### [autenticação do 802.1x](#)

Este exemplo mostra um WLAN configurado com autenticação do 802.1x.

## Wireless LAN With 802.1x Authentication



Layer 2 Security: 802.1x  
Layer 3 Security: None

SSID: 802.1x  
WEP-Key Size: 128-bit

### [Configurar o WLC para a autenticação do 802.1x](#)

Termine estas etapas a fim configurar o WLC para esta instalação:

1. Clique **WLAN** do controlador GUI a fim criar um WLAN.A janela WLANs aparece. Este indicador alista os WLAN configurados no controlador.
2. Clique **novo** a fim configurar um WLAN novo.Neste exemplo, o WLAN é nomeado *802.1x*, e o ID de WLAN é 3. Um nome de perfil deve igualmente ser adicionado.

CISCO

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT

WLANs

WLANs > New

Type: WLAN

Profile Name: WLAN3

SSID: 802.1x

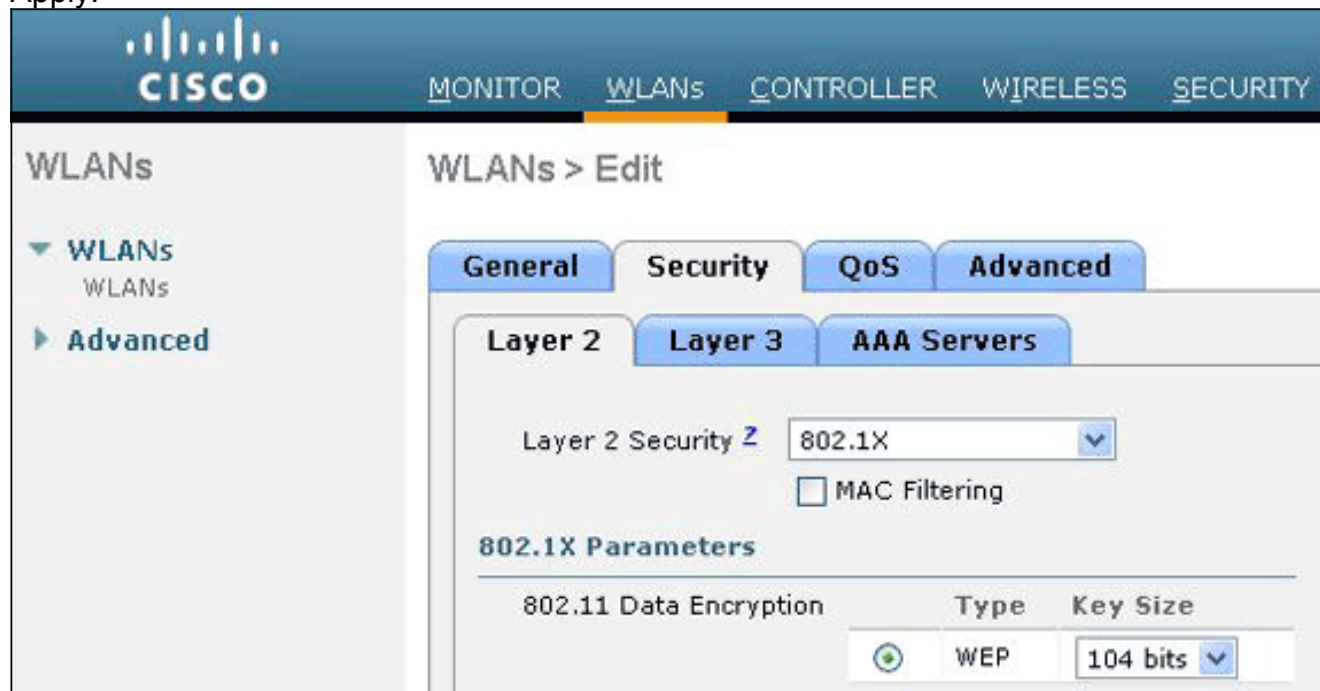
ID: 3

3. Clique em Apply.
4. No o WLAN > edita o indicador, define os parâmetros específicos ao WLAN.Da lista de drop-down da camada 2, escolha o **802.1x**.**Nota:** Somente a criptografia de WEP está disponível



com 802.1x. Escolha 40 bit ou 104 bit para a criptografia, e certifique-se que Segurança da camada 3 está ajustada a nenhuns. Isto permite a autenticação do 802.1x para este WLAN. Sob parâmetros do servidor Radius, selecione o servidor Radius que será usado para autenticar as credenciais do cliente. Escolha outros parâmetros baseados em seus requisitos de projeto. Este exemplo usa os valores padrão.

5. Clique em Apply.



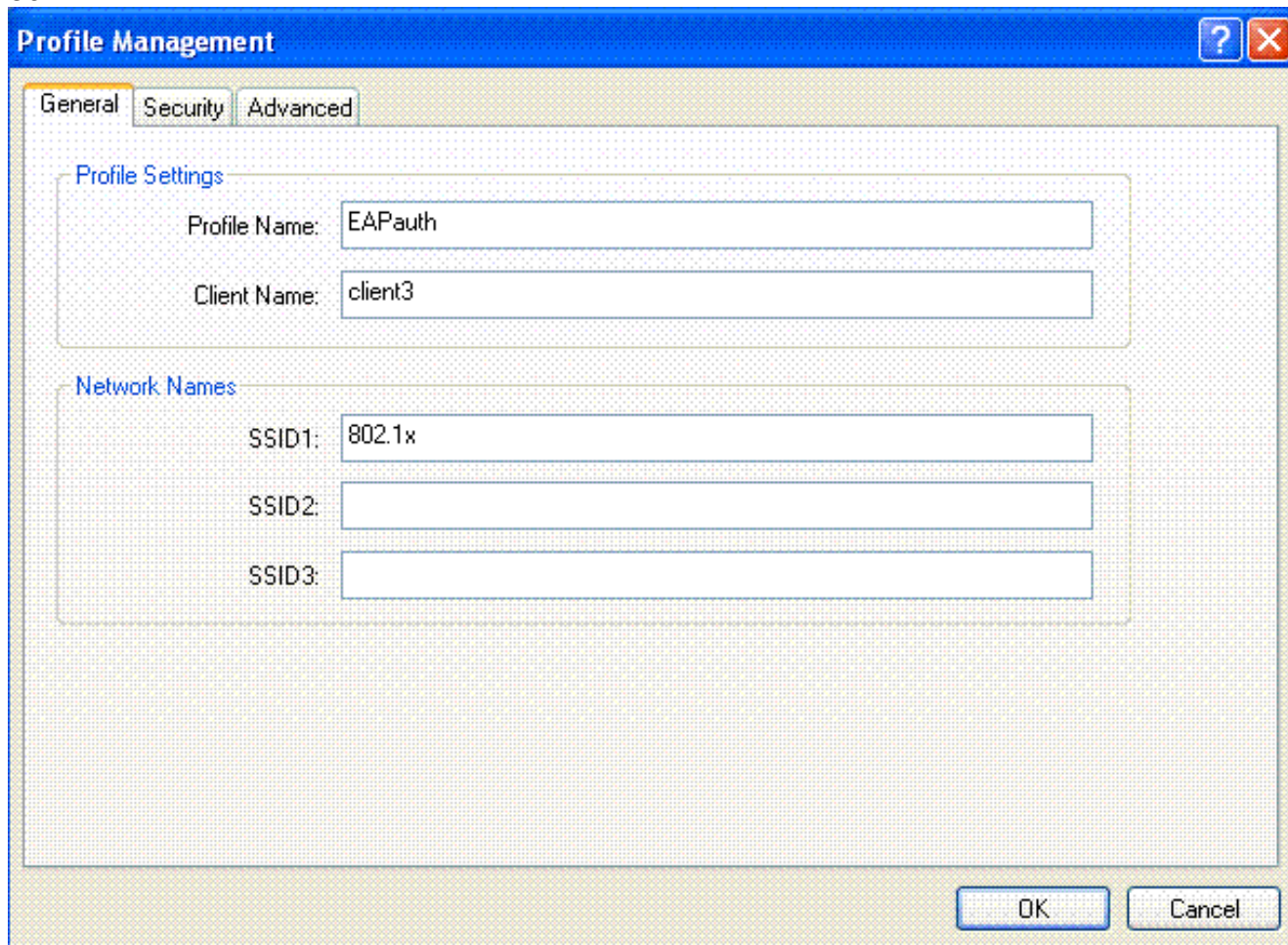
**Notas:** Se você escolhe o 802.1x para a Segurança da camada 2, o CCKM não pode ser usado. Se você escolhe WPA 1 ou WPA2 para a Segurança da camada 2, estas opções aparecem sob o gerenciamento chave do AUTH: 802.1x+CCKM — Se você escolhe esta opção, os clientes CCKM ou NON-CCKM estão apoiados (CCKM opcional). 802.1x — Se você escolhe esta opção, simplesmente os clientes do 802.1x estão apoiados. CCKM — Se você escolhe esta opção, simplesmente os clientes CCKM estão apoiados, onde os clientes são dirigidos a um servidor interno para a autenticação. PSK — Se você escolhe esta opção, uma chave pré-compartilhada está usada para o WLC e o cliente. Também, todos os padrões são ajustados para ser usados antes dos PRE-padrões; por exemplo, WPA/WPA2 toma o precedente sobre o CCKM quando usado simultaneamente. O tipo de autenticação de EAP usado para validar os clientes é dependente do tipo EAP configurado no servidor Radius e nos clientes Wireless. Uma vez que o 802.1x é permitido no WLC, o WLC permite que todos os tipos de pacotes EAP fluam entre o REGAÇO, o cliente Wireless e o servidor Radius. Estes documentos fornecem exemplos de configuração em alguns dos tipos da autenticação de EAP: [PEAP sob redes Wireless unificadas com ACS 4.0 e Windows 2003](#), [EAP-TLS em Redes Wireless Unificadas com o ACS 4.0 e o Windows 2003](#), [Autenticação de EAP com exemplo de configuração dos controladores de WLAN \(WLC\)](#)

### [Configurar o cliente Wireless para a autenticação do 802.1x](#)

Termine estas etapas a fim configurar o cliente do Wireless LAN para esta instalação:

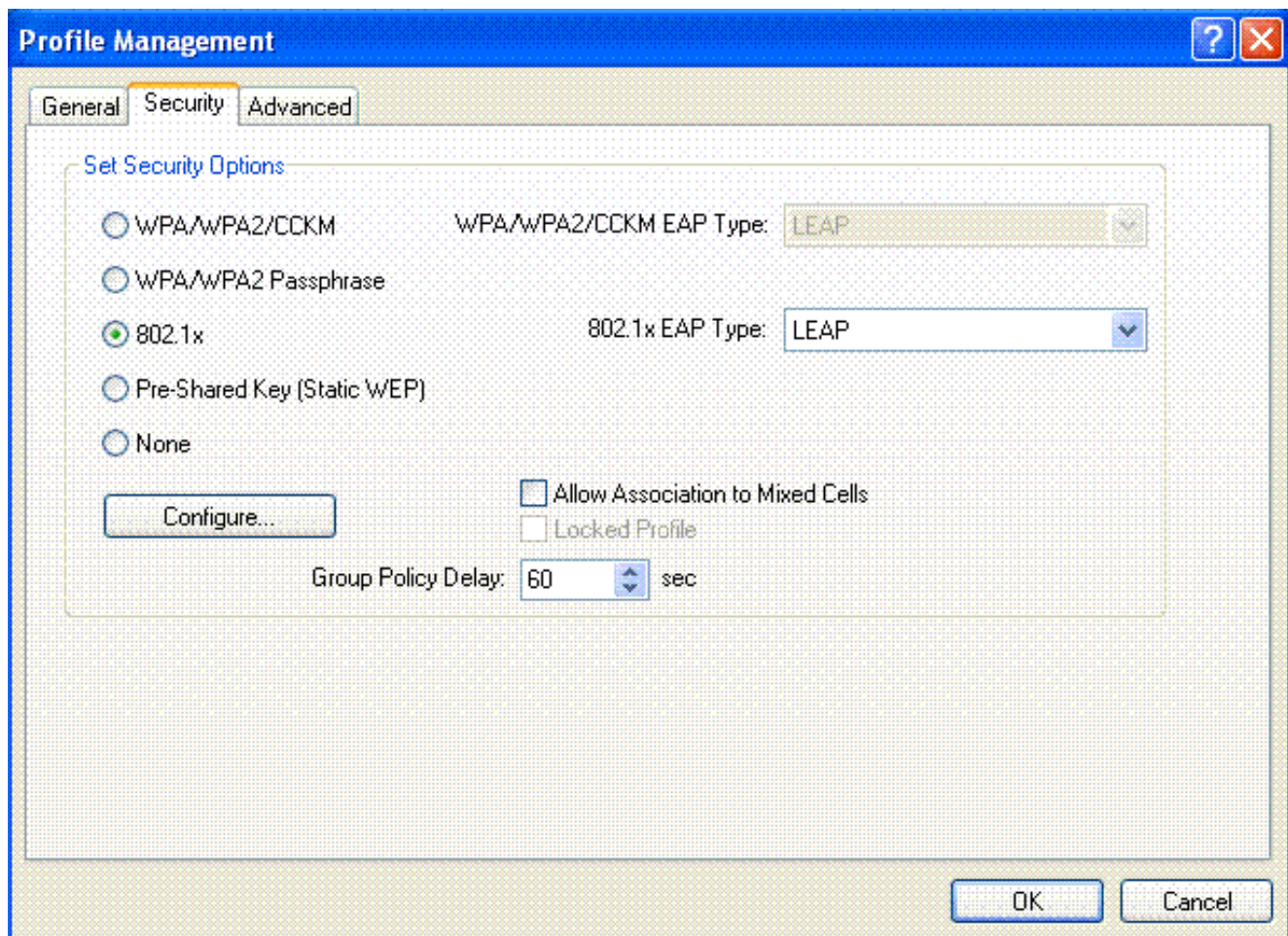
1. A fim criar um perfil novo, clique a aba do **Gerenciamento do perfil** no ADU.
2. Clique em **New**.

- Quando os indicadores (gerais) do indicador do Gerenciamento do perfil, terminarem estas etapas a fim ajustar o nome de perfil, o nome do cliente, e o SSID:Dê entrada com o nome do perfil no campo de nome de perfil.Este exemplo usa *EAPAuth* como o nome de perfil.Dê entrada com o nome do cliente no campo de nome do cliente.O nome do cliente é usado para identificar o cliente Wireless na rede de WLAN. Esta configuração usa o *cliente 3* para o nome do cliente.Sob nomes de rede, incorpore o SSID que deve ser usada para este perfil.O SSID é o mesmo que o SSID que você configurou no WLC. O SSID neste exemplo é *802.1x*.



The image shows a screenshot of the 'Profile Management' dialog box, specifically the 'General' tab. The dialog has a blue title bar with a question mark and a close button. Below the title bar are three tabs: 'General', 'Security', and 'Advanced'. The 'General' tab is selected. The dialog is divided into two main sections: 'Profile Settings' and 'Network Names'. In the 'Profile Settings' section, there are two text input fields: 'Profile Name' with the value 'EAPAuth' and 'Client Name' with the value 'client3'. In the 'Network Names' section, there are three text input fields: 'SSID1' with the value '802.1x', 'SSID2' which is empty, and 'SSID3' which is empty. At the bottom right of the dialog are two buttons: 'OK' and 'Cancel'.

- Clique na guia Security.



5. Clique o botão de rádio do **802.1x**.
6. Do 802.1x EAP datilografe a lista de drop-down, escolhem o tipo EAP usado.
7. O clique **configura** a fim configurar os parâmetros específicos ao tipo selecionado EAP.

**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:

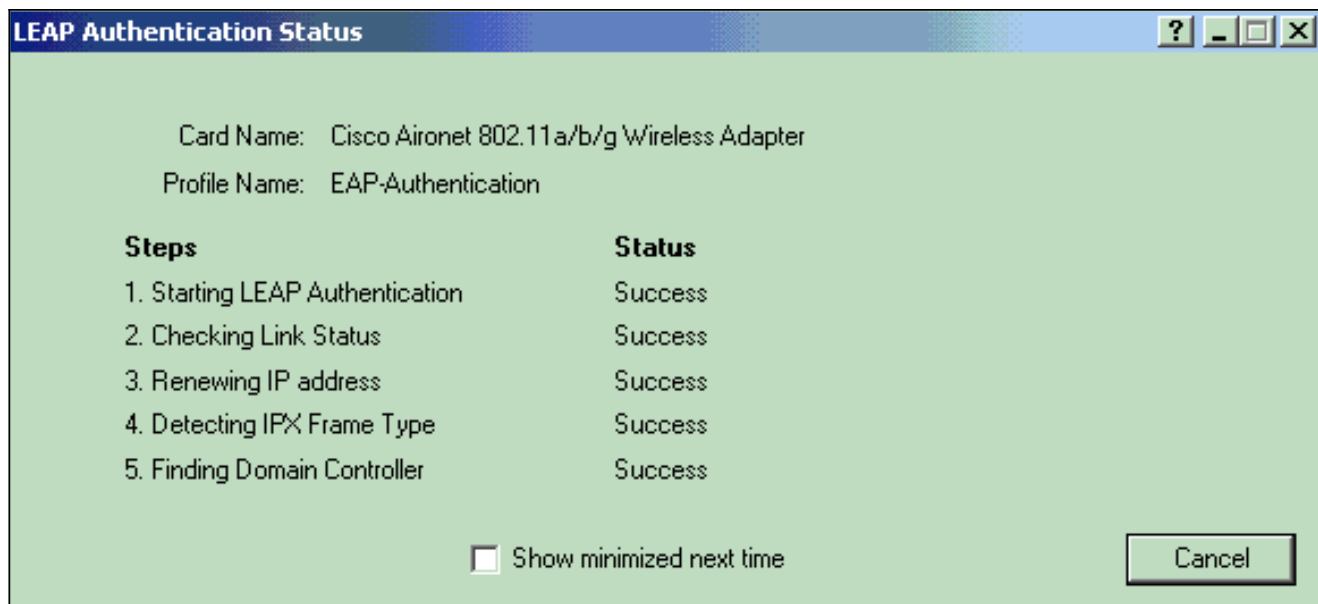
Include Windows Logon Domain with User Name

No Network Connection Unless User Is Logged In

Authentication Timeout Value (in seconds)

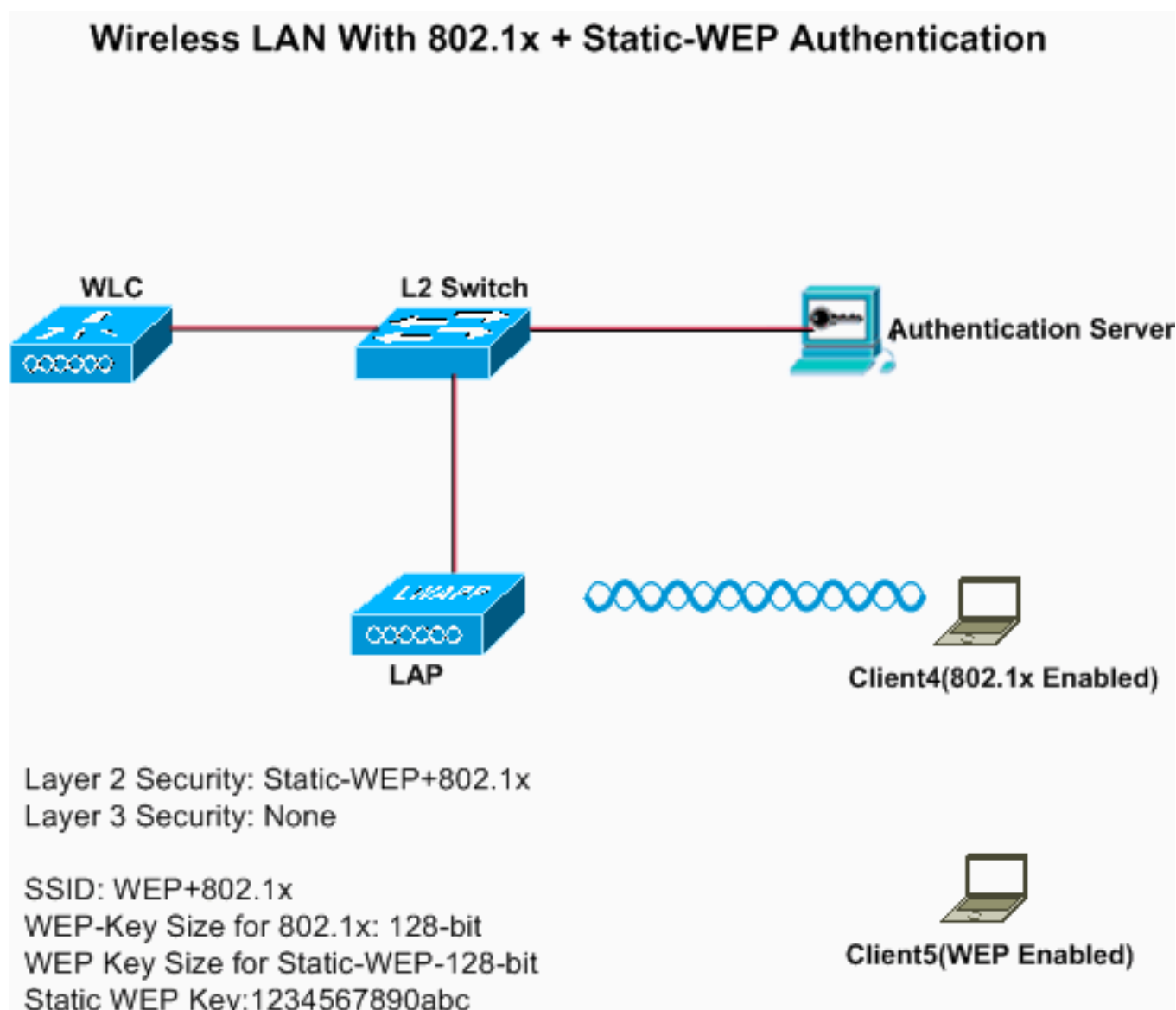
OK Cancel

8. Clique em Apply. Quando o SSID é ativado, o cliente Wireless conecta ao WLAN usando a autenticação do 802.1x. As chaves de WEP dinâmicas são usadas para as sessões.



### [Autenticação do WEP estático + do 802.1x](#)

Este exemplo mostra um WLAN configurado com autenticação do WEP estático + do 802.1x.



Termine estas etapas a fim configurar o WLC para esta instalação:

1. Clique **WLAN** do controlador GUI a fim criar um WLAN.A janela WLANs aparece. Este indicador alista os WLAN configurados no controlador.
2. Clique **novo** a fim configurar um WLAN novo.
3. Incorpore o ID de WLAN e o WLAN SSID.Neste exemplo, o WLAN é nomeado **WEP+802.1x**, e o ID de WLAN é 4.



The screenshot shows the Cisco WLAN configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', and 'MANAGEMENT'. The main content area is titled 'WLANs > New' and contains the following fields:

Type	WLAN
Profile Name	WLAN 4
SSID	Static WEP + 802.1x
ID	4

4. Clique em Apply.
5. No o WLAN > edita o indicador, define os parâmetros específicos ao WLAN.Da lista de drop-down da camada 2, escolha **Static-WEP+802.1x**.Isto permite o WEP estático e a autenticação do 802.1x para este WLAN.Sob parâmetros do servidor Radius, selecione o servidor Radius que será usado para autenticar as credenciais do cliente usando o 802.1x, e configurar o servidor Radius segundo as indicações do exemplo anterior.Sob parâmetros do WEP estático, selecione o deslocamento predeterminado do tamanho da chave de WEP e o chave, e incorpore a chave de criptografia do WEP estático segundo as indicações da imagem anterior.Escolha outros parâmetros baseados em seus requisitos de projeto.Este exemplo usa os valores padrão.

### [Configurar o cliente Wireless para o WEP estático e o 802.1x](#)

Veja o [cliente Wireless configurar para a autenticação do 802.1x](#) e [configurar o cliente Wireless para](#) seções do [WEP estático](#) para obter informações sobre de como configurar o cliente Wireless.

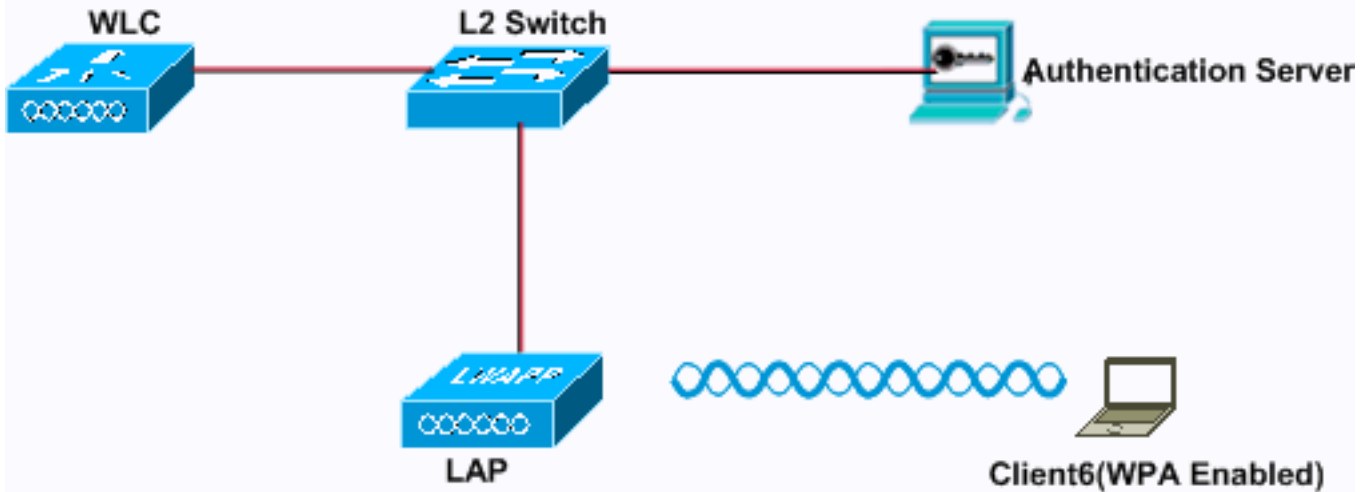
Uma vez que os perfis do cliente são criados, os clientes que são configurados para o associado do WEP estático com o REGAÇO. Use o SSID WEP+802.1x a fim conectar à rede.

Similarmente, os clientes Wireless que são configurados para usar a autenticação do 802.1x são autenticados usando o EAP e para alcançar a rede com o mesmo SSID WEP+802.1x.

### [Acesso protegido por wi-fi](#)

Este exemplo mostra a um WLAN qual é configurado com o WPA com 802.1x.

## Wireless LAN With WPA



Layer 2 Security: WPA1+WPA2  
Layer 3 Security: None

SSID: WPA  
Auth key Management: 802.1x  
WPA1 Encryption: TKIP

### [Configurar o WLC para o WPA](#)

Termine estas etapas a fim configurar o WLC para esta instalação:

1. Clique **WLAN** do controlador GUI a fim criar um WLAN. A janela WLANs aparece. Este indicador alista os WLAN configurados no controlador.
2. O clique **vai** a fim configurar um WLAN novo. Escolha o tipo e o nome de perfil. Neste exemplo, o WLAN é nomeado *WPA*, e o ID de WLAN é 5.

CISCO

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS

WLANs

WLANs > New

Type: WLAN

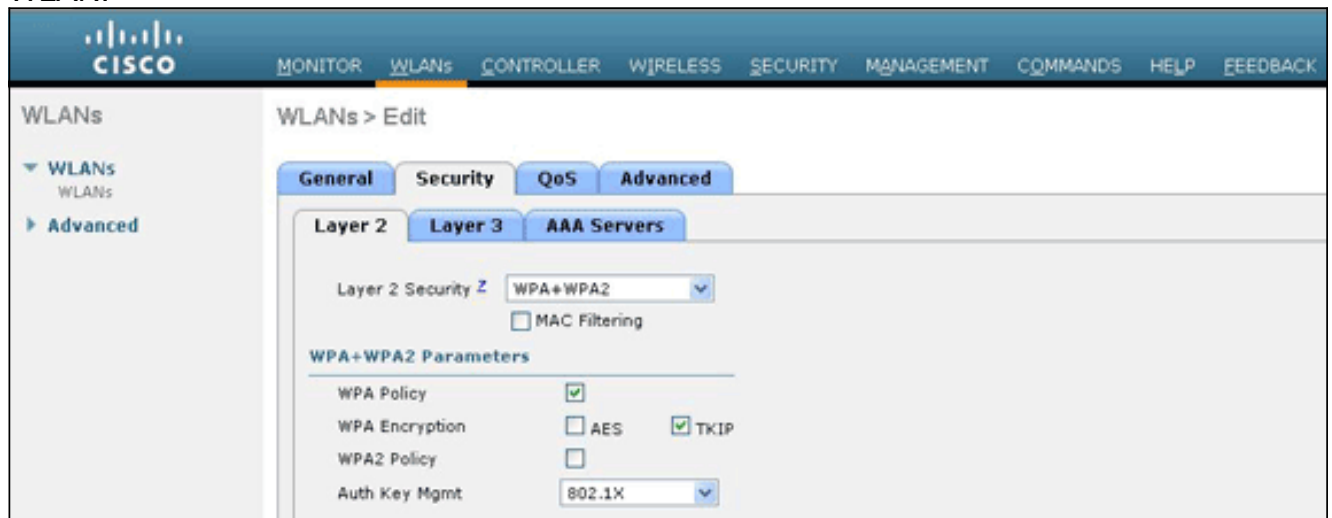
Profile Name: WLAN 5

SSID: WPA

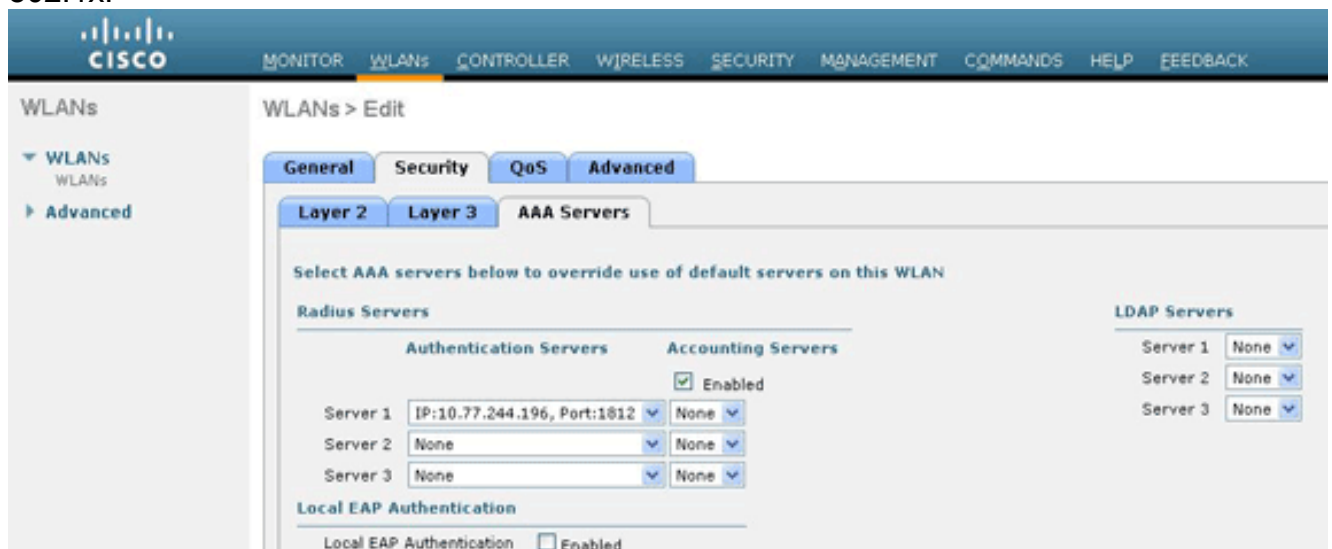
ID: 5

3. Clique em Apply.
4. No o WLAN > edita o indicador, define os parâmetros específicos ao

## WLAN.



Clique a **ABA de segurança**, clique a aba da **camada 2**, e escolha **WPA1+WPA2** da lista de drop-down da Segurança da camada 2. Sob os parâmetros WPA1+WPA2, verifique a caixa de verificação da **política WPA1** a fim permitir WPA1, verificar a caixa de verificação da **política WPA2** a fim permitir o WPA2, ou verificar ambas as caixas de seleção a fim permitir WPA1 e WPA2. O valor padrão é desabilitado para WPA1 e WPA2. Se você deixa WPA1 e WPA2 desabilitado, os Access point anunciam em seus balizas e elementos de informação de resposta da ponta de prova somente para o método que de Gerenciamento da chave de autenticação você escolhe. Verifique a caixa de verificação **AES** a fim permitir a criptografia de dados AES ou a caixa de verificação **TKIP** a fim permitir a criptografia de dados TKIP para WPA1, WPA2, ou ambos. Os valores padrão são TKIP para WPA1 e AES para o WPA2. Escolha um destes métodos de gerenciamento chave da lista de drop-down de Mgmt da chave do AUTH: **802.1X** — Se você escolhe esta opção, simplesmente os clientes do 802.1x estão apoiados. **CCKM** — Se você escolhe esta opção, simplesmente os clientes CCKM estão apoiados, onde os clientes são dirigidos a um servidor interno para a autenticação. **PSK** — Se você escolhe esta opção, uma chave pré-compartilhada está usada para o WLC e o cliente. Também, todos os padrões são ajustados para ser usados antes dos PRE-padrões; por exemplo, WPA/WPA2 toma o precedente sobre o CCKM quando usado simultaneamente. **802.1X+CCKM** — Se você escolhe esta opção, os clientes CCKM ou NON-CCKM estão apoiados (CCKM opcional). Este exemplo usa o 802.1x.



**Nota:** Se você escolhe o PSK, escolha o **ascii** ou **encantar** da lista de drop-down do formato



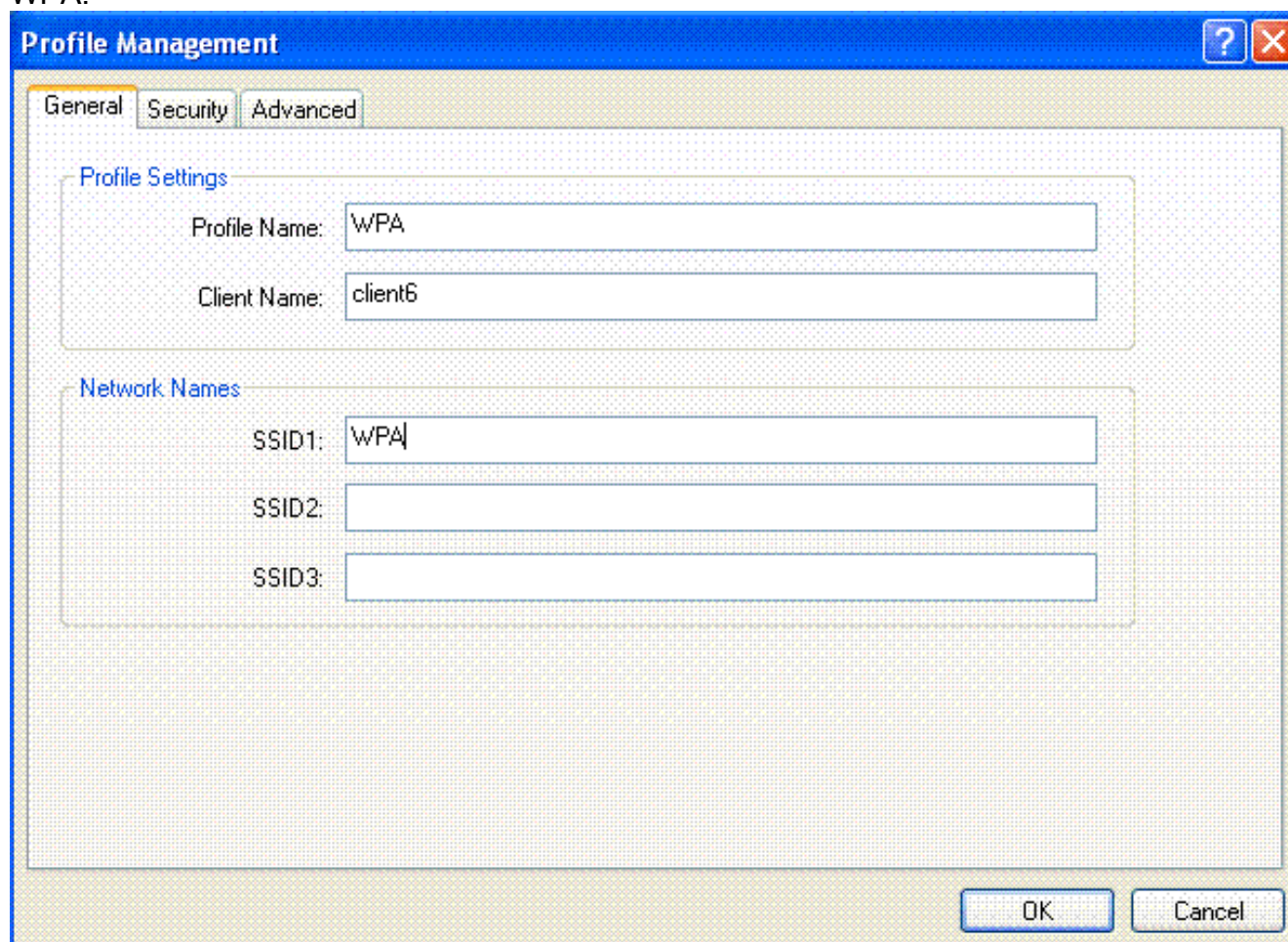
PSK, e incorpore então uma chave pré-compartilhada ao campo em branco. As chaves pré-compartilhada WPA devem conter 8 a 63 caracteres do texto de ASCII ou 64 encantam caracteres.

5. O clique **aplica-se** a fim aplicar suas mudanças.

### Configurar o cliente Wireless para o WPA

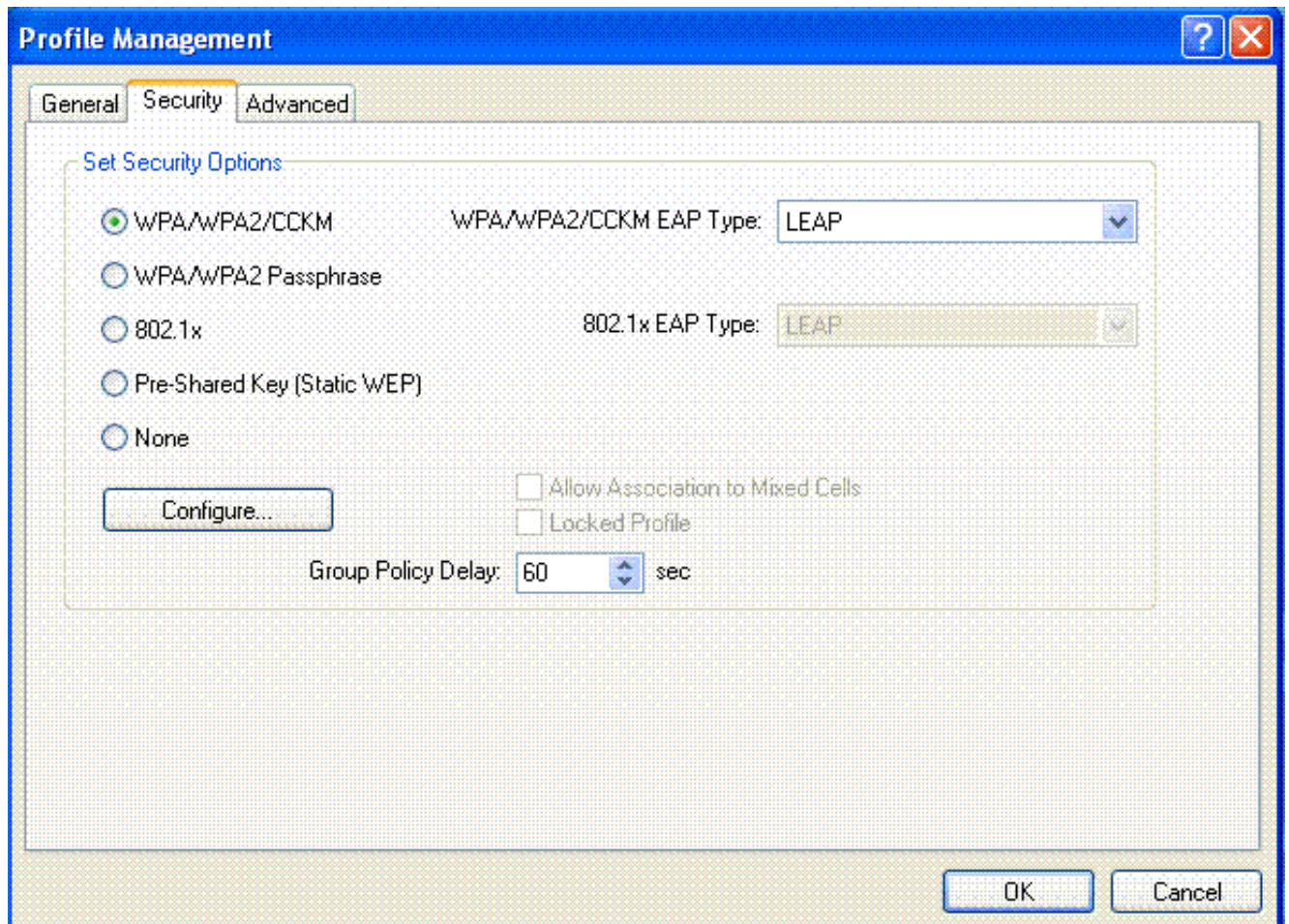
Termine estas etapas a fim configurar o cliente do Wireless LAN para esta instalação:

1. Na janela de gerenciamento do perfil no ADU, clique **novo** a fim criar um perfil novo.
2. Clique o **tab geral**, e incorpore o nome de perfil e o SSID que o adaptador cliente usará. Neste exemplo, o nome de perfil e o SSID são *WPA*. O SSID deve combinar o SSID que você configurou no WLC para o WPA.



The screenshot shows the 'Profile Management' dialog box with the 'General' tab selected. The 'Profile Settings' section contains two text boxes: 'Profile Name' with the value 'WPA' and 'Client Name' with the value 'client6'. The 'Network Names' section contains three text boxes: 'SSID1' with the value 'WPA', 'SSID2' which is empty, and 'SSID3' which is empty. At the bottom right, there are 'OK' and 'Cancel' buttons.

3. Na ABA de segurança, clique o botão de rádio **WPA/WPA2/CCKM**, e escolha o tipo apropriado EAP do tipo lista de drop-down WPA/WPA2/CCKM EAP. Esta etapa permite o WPA.



4. O clique **configura** a fim definir os ajustes EAP específicos ao tipo de EAP selecionado.

**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:

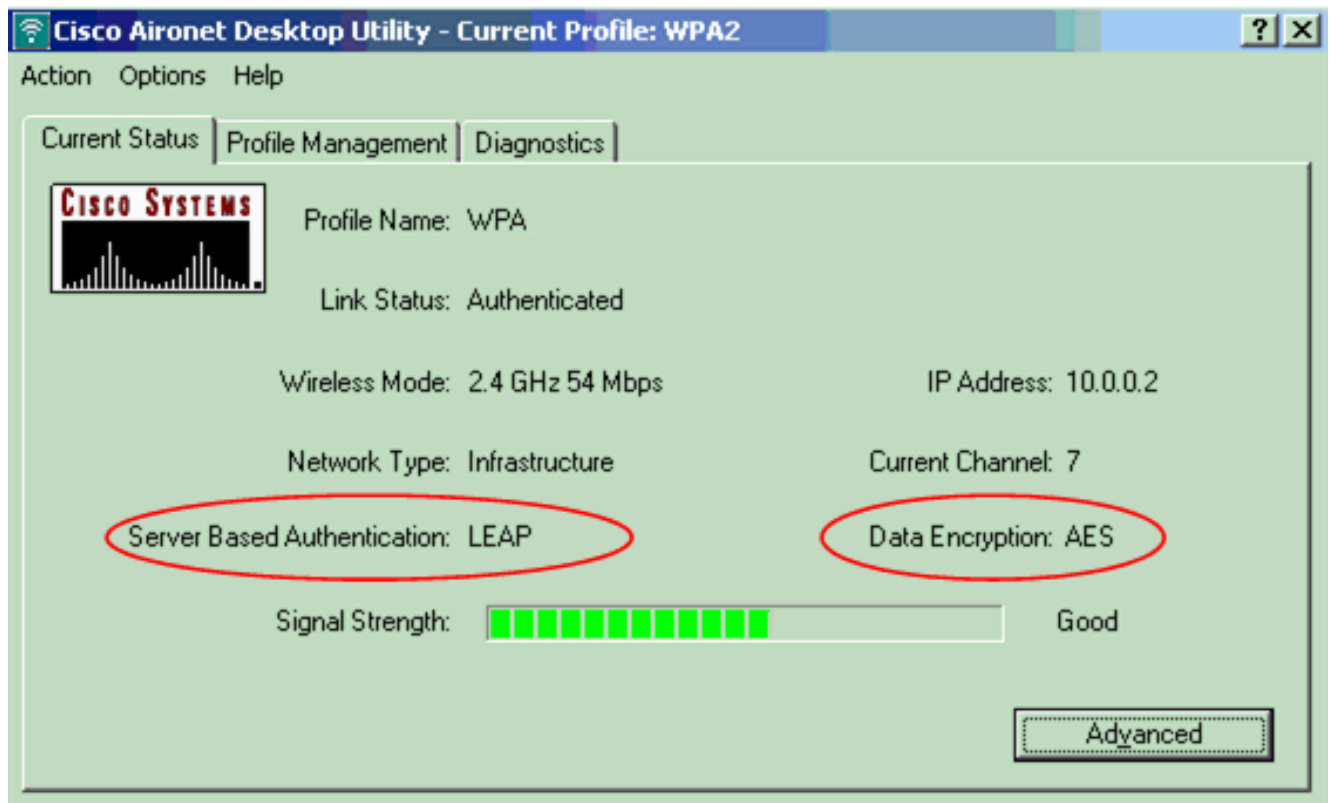
Include Windows Logon Domain with User Name

No Network Connection Unless User Is Logged In

Authentication Timeout Value (in seconds)

OK Cancel

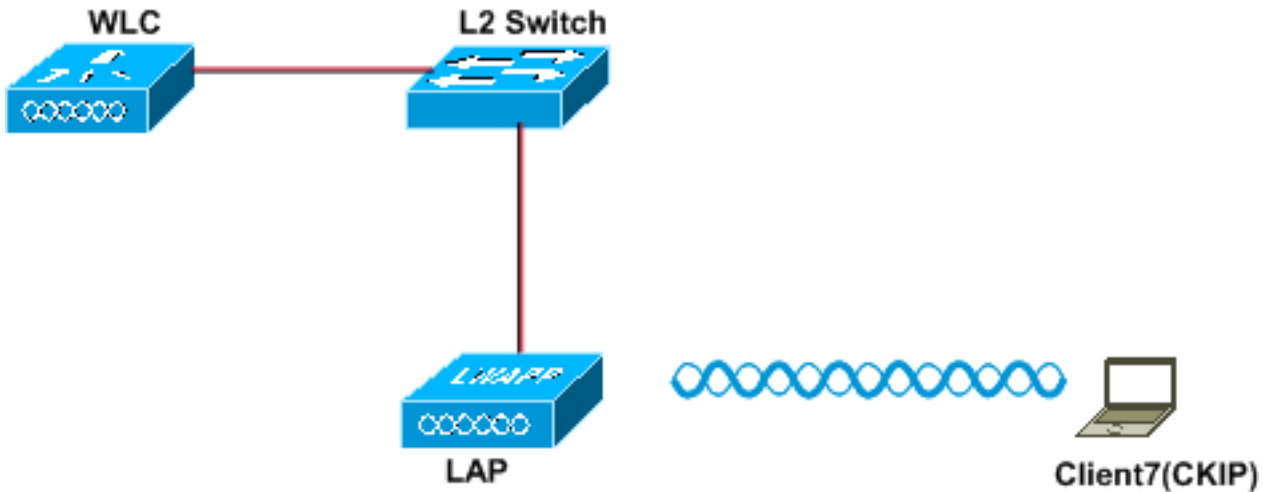
5. Clique em **OK**. **Nota:** Quando este perfil é ativado, o cliente está autenticado usando o 802.1x e quando a autenticação é bem sucedida, o cliente conecta ao WLAN. Verifique o status atual ADU a fim verificar que o cliente usa a criptografia TKIP (criptografia do padrão usada por WPA1) e a autenticação de EAP.



## [CKIP](#)

Este exemplo mostra um WLAN configurado com CKIP.

# Wireless LAN With CKIP



Layer 2 Security: CKIP  
Layer 3 Security: None  
SSID: CKIP

## [Configurar o WLC para CKIP](#)

Termine estas etapas a fim configurar o WLC para esta instalação:

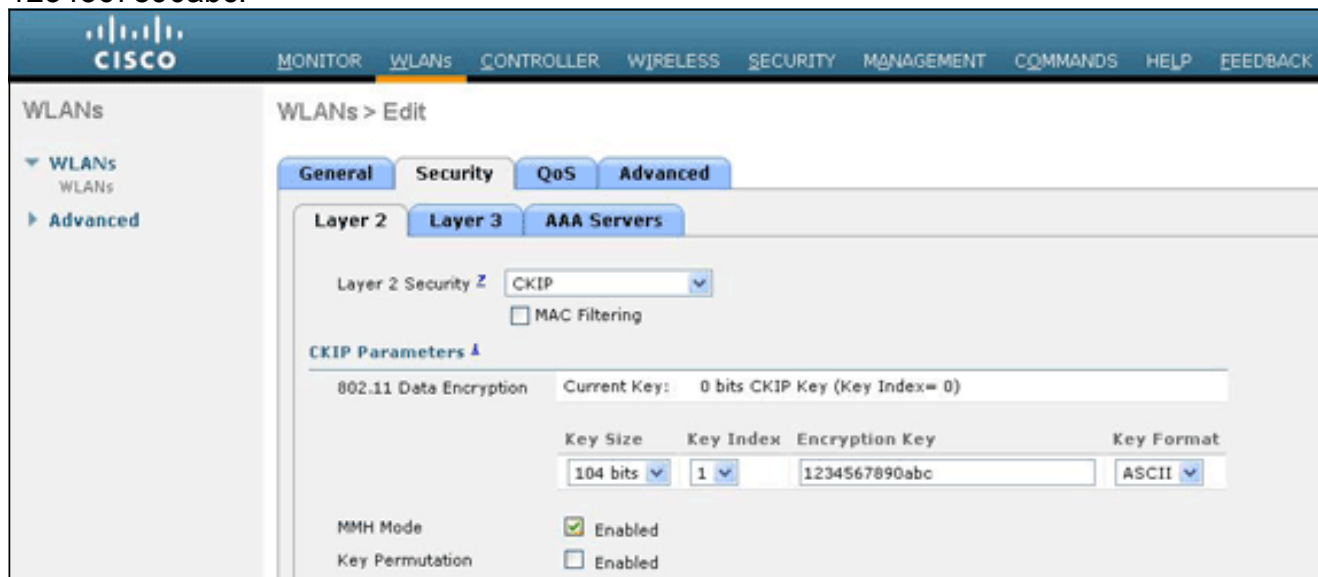
1. Clique **WLAN** do controlador GUI a fim criar um WLAN.A janela WLANs aparece. Este indicador alista os WLAN configurados no controlador.
2. Clique **novo** a fim configurar um WLAN novo.Escolha o tipo e o nome de perfil. Neste exemplo, o WLAN é nomeado *CKIP* e o ID de WLAN é 6.

The screenshot shows the Cisco WLC GUI configuration page for creating a new WLAN. The page is titled 'WLANs > New' and includes the following fields:

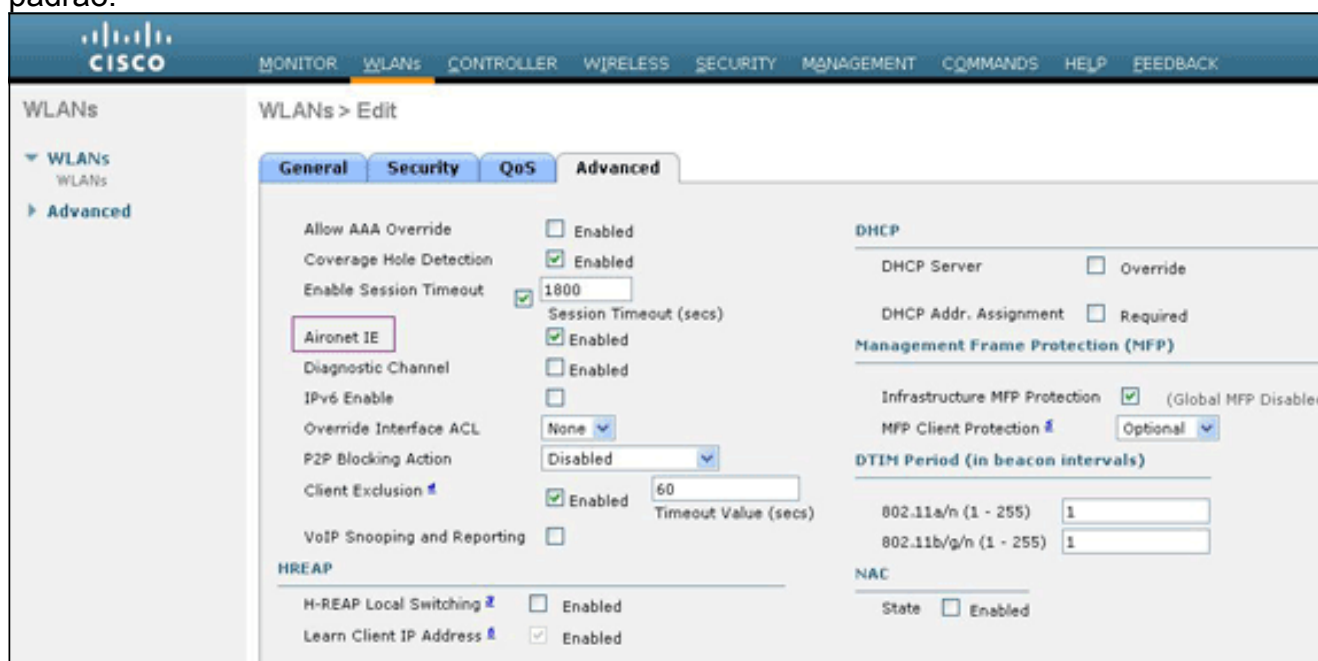
Type	WLAN
Profile Name	WLAN 6
SSID	CKIP
ID	6

3. No o WLAN > edita o indicador, define os parâmetros específicos ao WLAN.Da lista de drop-down da camada 2, escolha **CKIP**.Esta etapa permite CKIP para este WLAN.Sob os parâmetros CKIP, selecione o deslocamento predeterminado do tamanho chave e o chave, e incorpore a chave de criptografia estática.O tamanho chave pode ser 40 bit, 104 bit, ou bit

128. O deslocamento predeterminado chave pode estar entre 1 e 4. Um deslocamento predeterminado de chave de WEP original pode ser aplicado a cada WLAN. Porque há somente quatro deslocamentos predeterminados de chave de WEP, simplesmente quatro WLAN podem ser configurados para a criptografia da camada 2 do WEP estático. Para CKIP, escolha a opção do modo MMH, ou a opção chave da permutação, ou ambos. **Nota:** Um destes parâmetros ou ambos deve ser selecionado para que CKIP trabalhe como esperado. Se estes parâmetros não são selecionados, o WLAN fica no estado desabilitado. Neste exemplo, o bit 104 chave é usado, e a chave é 1234567890abc.



4. Escolha outros parâmetros baseados em seus requisitos de projeto. Este exemplo usa os valores padrão.

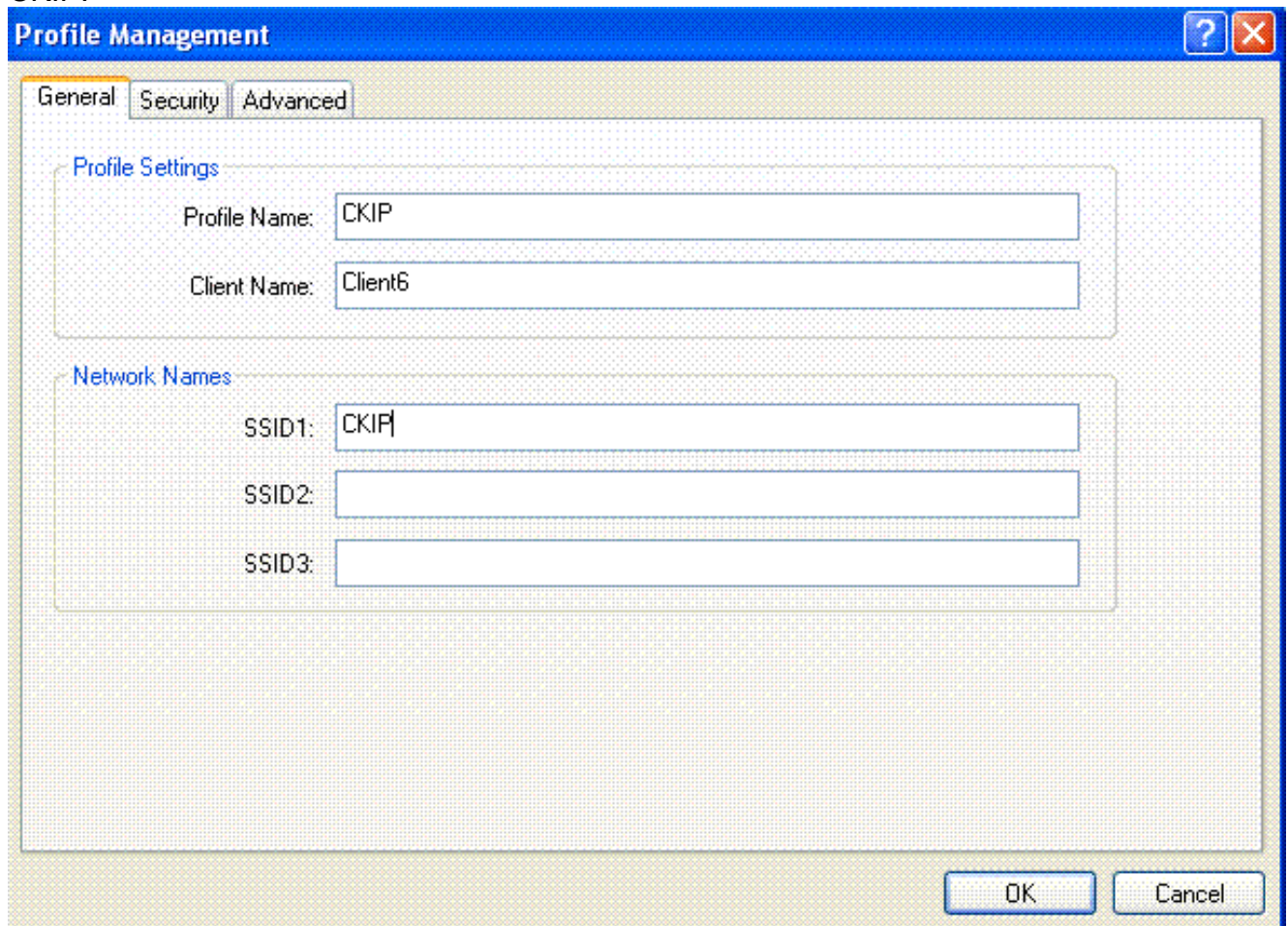


5. Clique em Apply. **Nota:** CKIP é funcional nos 1100, 1130, e 1200 AP, mas não AP 1000. Aironet IE precisa de ser permitido para que esta característica trabalhe. CKIP expande as chaves de criptografia a 16 bytes.

[Configurar o cliente Wireless para CKIP](#)

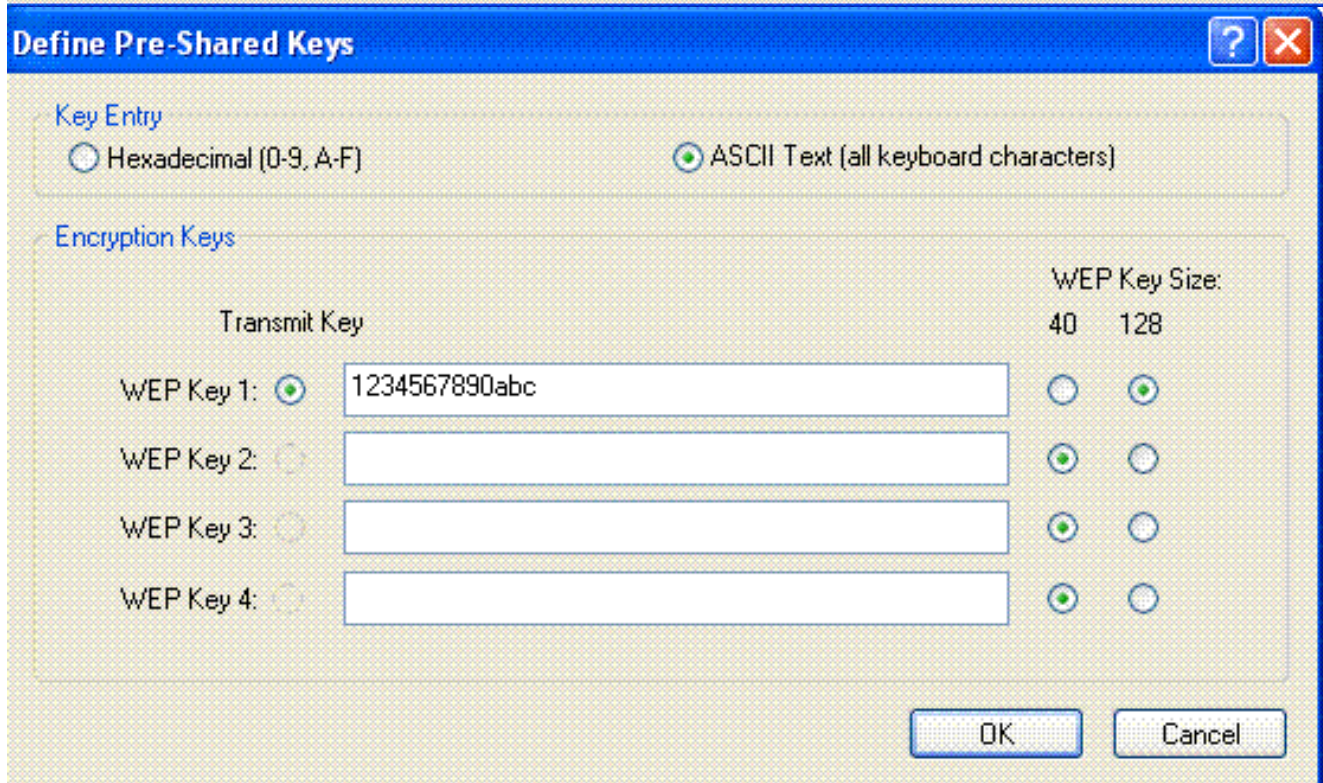
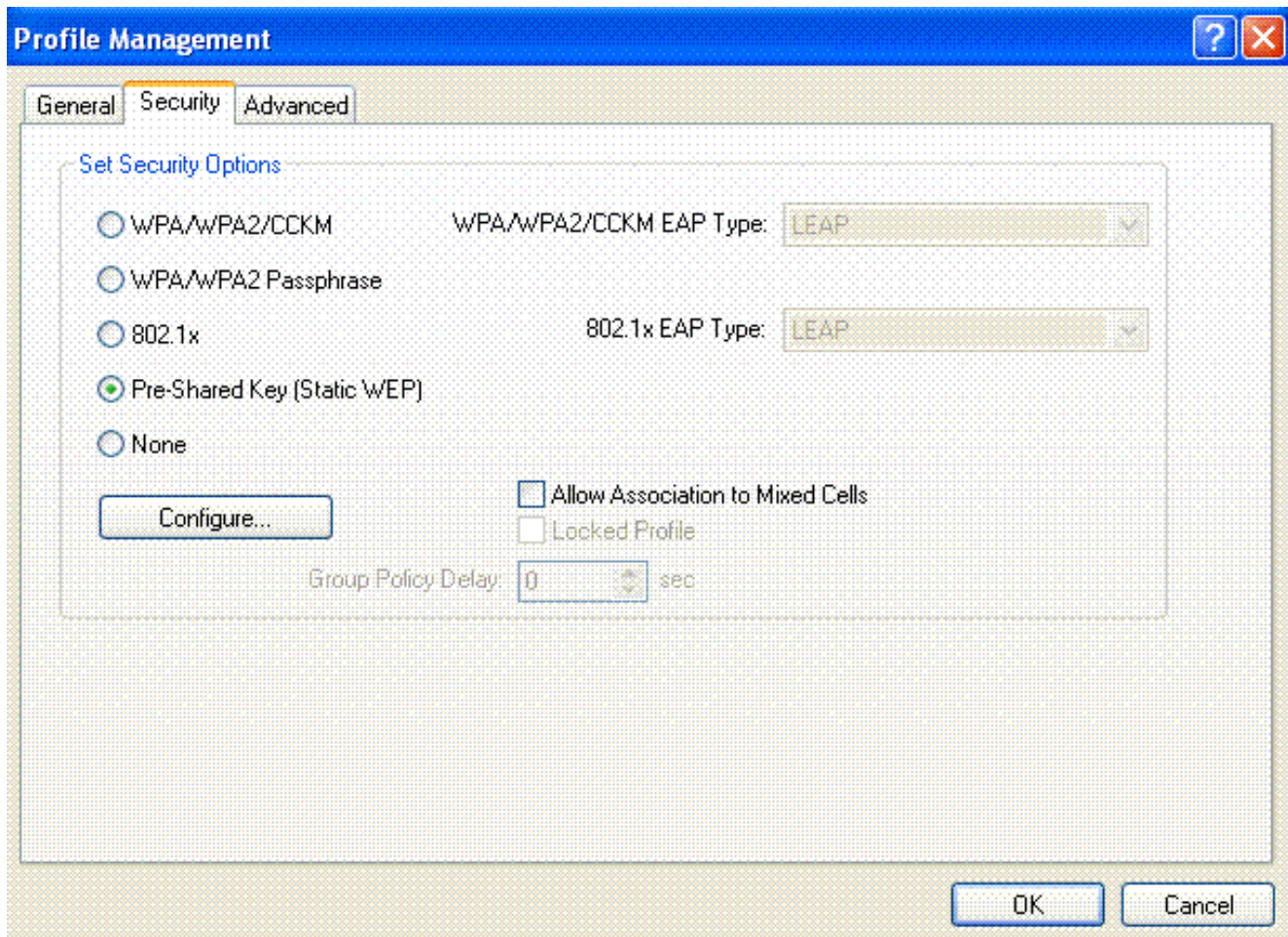
Termine estas etapas a fim configurar o cliente do Wireless LAN para esta instalação:

1. A fim criar um perfil novo, clique a aba do **Gerenciamento do perfil no ADU**, e clique então **novo**.
2. Quando os indicadores (gerais) do indicador do Gerenciamento do perfil, terminarem estas etapas a fim ajustar o nome de perfil, o nome do cliente, e o SSID: Dê entrada com o nome do perfil no campo de nome de perfil. Este exemplo usa *CKIP* como o nome de perfil. Dê entrada com o nome do cliente no campo de nome do cliente. O nome do cliente é usado para identificar o cliente Wireless na rede de WLAN. Esta configuração usa *Client6* para o nome do cliente. Sob nomes de rede, incorpore o SSID que deve ser usada para este perfil. O SSID é o mesmo que o SSID que você configurou no WLC. O SSID neste exemplo é *CKIP*.



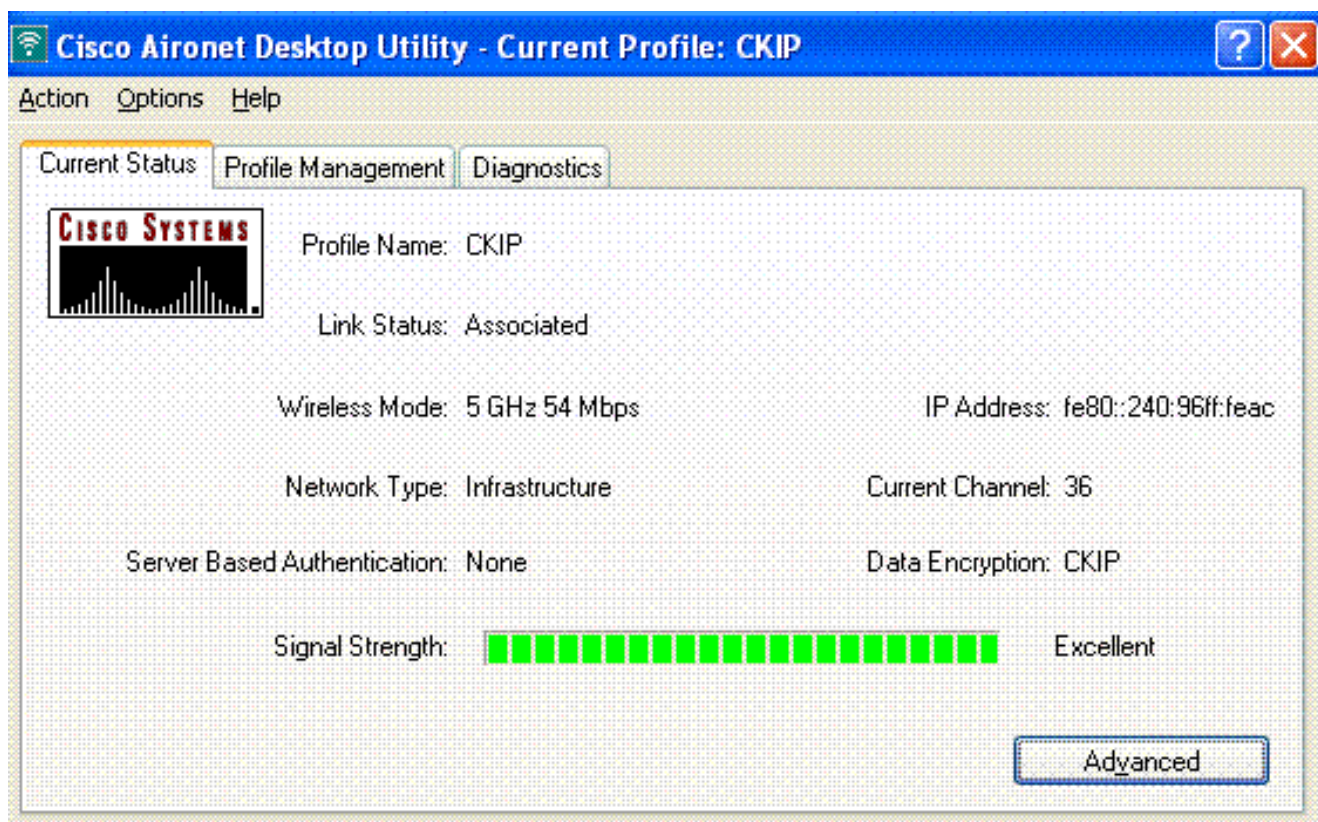
The screenshot shows a 'Profile Management' dialog box with three tabs: 'General', 'Security', and 'Advanced'. The 'General' tab is selected. It contains two sections: 'Profile Settings' and 'Network Names'. In 'Profile Settings', the 'Profile Name' field contains 'CKIP' and the 'Client Name' field contains 'Client6'. In 'Network Names', the 'SSID1' field contains 'CKIP', while 'SSID2' and 'SSID3' are empty. At the bottom right, there are 'OK' and 'Cancel' buttons.

3. Clique na guia Security.
4. Escolha a **chave pré-compartilhada (WEP estático)** sob opções de segurança do grupo, o clique **configura**, e define o tamanho da chave de WEP e a chave de WEP. Estes valores devem combinar com a chave de WEP configurada no WLC para este WLAN.



5. Clique em **OK**. Quando o SSID é ativado, o cliente Wireless negocia com o REGAÇO e o WLC para usar CKIP para a criptografia os pacotes.





## [Soluções da Segurança da camada 3](#)

### [Política da Web \(Autenticação da Web e Web Passthrough\)](#)

Refira o [exemplo de configuração da autenticação da Web do controlador do Wireless LAN](#) para obter informações sobre de como permitir a autenticação da Web em uma rede de WLAN.

Refira a [autenticação do web externa com exemplo de configuração dos controladores do Wireless LAN](#) para obter informações sobre de como configurar a autenticação do web externa e a autenticação da transmissão da Web em um WLAN.

Refira o [exemplo de configuração da transmissão da Web do controlador do Wireless LAN](#) para obter mais informações sobre de como permitir a transmissão da Web em uma rede de WLAN.

O mecanismo da página do respingo é um mecanismo de segurança da camada 3 introduzido na versão 5.0 WLC usada para a autenticação do cliente. Refira o [controlador do Wireless LAN a página do respingo que reorienta o exemplo de configuração](#) para mais informação.

### [Transmissão VPN](#)

Consulte [Exemplo de Configuração de VPN Cliente via LAN Wireless com WLC](#) para obter informações de como configurar o VPN em uma WLAN.

## [Troubleshooting](#)

### [Comandos para Troubleshooting](#)

Você pode usar estes **comandos debug** pesquisar defeitos sua configuração.

## Debuga para a autenticação da Web:

- **debugar o <client-MAC-*endereço xx do ADDR do Mac: xx: xx: xx: xx: xx*>** — Configura a eliminação de erros do MAC address para o cliente.
- **debugar o *aaa que todos permitem*** — Configura a eliminação de erros de todos os mensagens AAA.
- **debugar o estado PEM permitem** — Configure debuga da máquina de estado do gerente da política
- **debugar eventos PEM permitem** — Configure debuga de eventos do gerente da política.
- **debugar o mensagem DHCP permitem** — Use este comando a fim indicar a informação sobre debugging sobre as atividades de cliente do protocolo de configuração dinâmica host (DHCP) e monitorar o estado dos pacotes DHCP.
- **debugar o pacote DHCP permitem** — Use este comando a fim indicar a informação nivelada do pacote DHCP.
- **debugar pm SSH-appgw permitem** — Configure debuga dos gateway de aplicativo.
- **debugar pm SSH-TCP permitem** — Configure debuga da manipulação tcp do gerente da política

**Debuga para o WEP:** Nenhum debugar para o WEP porque é executado no AP, gerenciem debugam sobre o **dot11 que todos permitem**.

## Debuga pondo em esconderijo 802.1X/WPA/RSN/PMK:

- **debugar o <client-MAC-*endereço xx do ADDR do Mac: xx: xx: xx: xx: xx*>** — Configura a eliminação de erros do MAC address para o cliente.
- **debugar o dot1x que todos permitem** — Use este comando a fim indicar a informação sobre debugging do 802.1X.
- **debugar o dot11 que todos permitem** — Use este comando a fim permitir a eliminação de erros das funções de rádio.
- **debugar eventos PEM permitem** — Configure debuga de eventos do gerente da política.
- **debugar o estado PEM permitem** — Configure debuga da máquina de estado do gerente da política.
- **debugar o mensagem DHCP permitem** — Use este comando a fim indicar a informação sobre debugging sobre as atividades de cliente do protocolo de configuração dinâmica host (DHCP) e monitorar o estado dos pacotes DHCP.
- **debugar o pacote DHCP permitem** — Use este comando a fim indicar a informação nivelada do pacote DHCP.
- **debugar a entrega da mobilidade permitem (para o intra-interruptor que vagueia)** — Configure debugam de pacotes da mobilidade.
- **show client detail <mac>** — Exibe informações detalhadas para um cliente por endereço MAC. Verifique configuração do timeout de sessão WLAN e de RAI0.

## Informações Relacionadas

- [Restrinja o acesso WLAN baseado no SSID com WLC e exemplo de configuração do Cisco Secure ACS](#)
- [ACL no exemplo da configuração de controle do Wireless LAN](#)
- [Guia de Configuração da Cisco Wireless LAN Controller Release 4.0](#)
- [Página de Suporte Wireless](#)

- [Suporte Técnico e Documentação - Cisco Systems](#)