Wi-Fi Protected Access (WPA) em um exemplo da configuração de rede do Cisco Unified Wireless

Índice

Introdução

Este documento descreve como configurar o Wi-Fi Protected Access (WPA) em uma rede de Cisco Unified Wireless.

Pré-requisitos

Requisitos

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

- WPA
- Soluções da Segurança do Wireless LAN (WLAN)**Nota:** Refira a vista geral da Segurança de LAN do Cisco Wireless 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 de pouco peso do Cisco 1000 Series (REGAÇO)
- Controlador do Wireless LAN de Cisco 4404 (WLC) esse firmware 4.2.61.0 das corridas
- Adaptador cliente de Cisco 802.11a/b/g que executa o firmware 4.1
- Utilitário de Desktop de Aironet (ADU) esse firmware 4.1 das corridas
- Versão de servidor 4.1 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.

Apoio WPA e WPA2

A rede de Cisco Unified Wireless inclui o apoio para as certificações WPA e WPA2 de Alliance do Wi-fi. O WPA foi introduzido pelo Wi-fi Alliance em 2003. O WPA2 foi introduzido pelo Wi-fi Alliance em 2004. Todo o Wi-fi do Produtos certificado para o WPA2 é exigido ser interoperáveis com Produtos que é Wi-fi certificado para o WPA.

O WPA e o WPA2 oferecem um nível alto do acreditação para utilizadores finais e administradores de rede que seus dados permanecerão privados e que o acesso a suas redes estará restringido aos usuários autorizados. Ambos têm pessoais e o modo de empreendimento de operação que encontram as necessidades distintas dos dois segmentos de mercado. O modo de empreendimento de cada um usa o IEEE 802.1X e o EAP para a autenticação. O Modo pessoal de cada um usa a chave pré-compartilhada (PSK) para a autenticação. Cisco não recomenda o Modo pessoal para disposições do negócio ou do governo porque usa um PSK para a autenticação de usuário. O PSK não é seguro para ambientes de empreendimento.

O WPA endereça todas as vulnerabilidades conhecidas WEP na implementação de segurança original do IEEE 802.11 que traz uma solução imediata da Segurança aos WLAN na empresa e nos ambientes do small office/home office (SOHO). O WPA usa o TKIP para a criptografia.

O WPA2 é a próxima geração de Segurança do Wi-fi. É a aplicação interoperáveis de Alliance do Wi-fi do padrão ratificado da IEEE 802.11i. Executa o algoritmo de criptografia de AES recomendado do National Institute of Standards and Technology (NIST) usando o modo contrário com protocolo do código de autenticação de mensagens do Cipher Block Chaining (CCMP). O WPA2 facilita a conformidade do governo FIP 140-2.

Comparação dos tipos de modo WPA e WPA2

	WPA	WPA2
Modo de empreendimento (negócio, governo,	• Autenticação: IEEE 802.1X/E	• Autenticação: IEEE 802.1X/E

educação)	AP • Criptografia: TKIP/MIC	AP • Criptografia: AES-CCMP
Modo pessoal (SOHO, HOME/pessoal)	• Autenticação: PSK • Criptografia: TKIP/MIC	• Autenticação: PSK • Criptografia: AES-CCMP

No modo de empreendimento da operação WPA e WPA2 uso 802.1X/EAP para a autenticação. o 802.1X fornece WLAN o forte, autenticação mútua entre um cliente e um Authentication Server. Além, o 802.1X fornece o usuário per., por sessão chaves de criptografia dinâmicos, removendo a sobrecarga administrativa e as questões de segurança que cercam chaves de criptografia estáticas.

Com 802.1X, as credenciais usadas para a autenticação, tal como senhas do fazer logon, são transmitidas nunca na claro, ou sem criptografia, sobre o media wireless. Quando os tipos do autenticação do 802.1X fornecerem a autenticação forte para o Sem fio LAN, o TKIP ou o AES estão precisados para a criptografia além do que o 802.1X desde a criptografia de WEP padrão do 802.11, são vulnerável aos ataques de rede.

Diversos tipos do autenticação do 802.1X existem, cada um que fornece uma aproximação diferente à autenticação ao confiar na mesmos estrutura e EAP para uma comunicação entre um cliente e um Access point. O Produtos do Cisco Aironet apoia mais tipos da autenticação de EAP do 802.1X do que todos os outros produtos wlan. Os tipos suportados incluem:

- Cisco LEAP
- Autenticação Flexível de EAP através do Tunelamento seguro (EAP-FAST)
- Segurança da camada do EAP-transporte (EAP-TLS)
- Protocolo extensible authentication protegido (PEAP)
- TLS EAP-em túnel (EAP-TTLS)
- Módulo de identidade de assinante EAP (EAP-SIM)

Um outro benefício da autenticação do 802.1X é gerenciamento centralizado para grupos de usuário WLAN, incluindo a rotação chave com base em política, a atribuição de chave dinâmica, a atribuição do VLAN dinâmico, e a limitação SSID. Estas características gerenciem as chaves de criptografia.

No Modo pessoal de operação, uma chave pré-compartilhada (senha) é usada para a autenticação. O Modo pessoal exige somente um Access point e um dispositivo do cliente, quando o modo de empreendimento exigir tipicamente um RAIO ou o outro Authentication Server na rede.

Este documento fornece exemplos configurando WPA2 (modo de empreendimento) e WPA2-PSK (Modo pessoal) em uma rede de Cisco Unified Wireless.

Instalação de rede

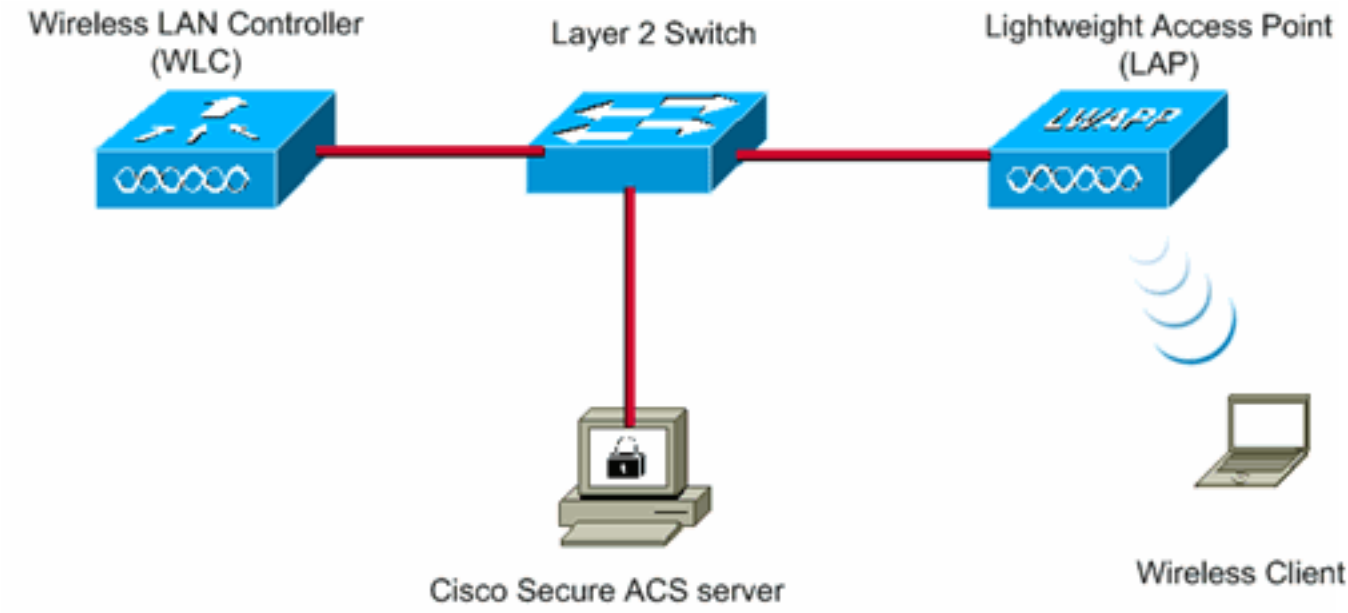
Nesta instalação, Cisco 4404 WLC e um REGAÇO do Cisco 1000 Series são conectados através de um switch de Camada 2. Um servidor de raio externo (Cisco Secure ACS) é conectado

igualmente ao mesmo interruptor. Todos os dispositivos estão na mesma sub-rede. O Access point (REGAÇO) é registrado inicialmente ao controlador. Dois LAN wireless, um para o modo de empreendimento WPA2 e o outro para o Modo pessoal WPA2, precisam de ser criados.

Modo WLAN WPA2-Enterprise (SSID: WPA2-Enterprise) usará EAP-FAST autenticando os clientes Wireless e o AES para a criptografia. O server do Cisco Secure ACS será usado como o servidor de raio externo autenticando os clientes Wireless.

Modo WLAN WPA2-Personal (SSID: WPA2-PSK) usará WPA2-PSK para a autenticação com a chave pré-compartilhada “abcdefghijk”.

Você precisa de configurar os dispositivos para esta instalação:



WLC Management IP address:	10.77.244.204
WLC AP Manager IP address:	10.77.244.205
Wireless Client IP address:	10.77.244.221
Cisco Secure ACS server IP address	10.77.244.196
Subnet Mask used in this example	255.255.255.224

Configurar os dispositivos para o modo de empreendimento WPA2

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

Execute estas etapas a fim configurar os dispositivos para o modo de empreendimento WPA2 de operação:

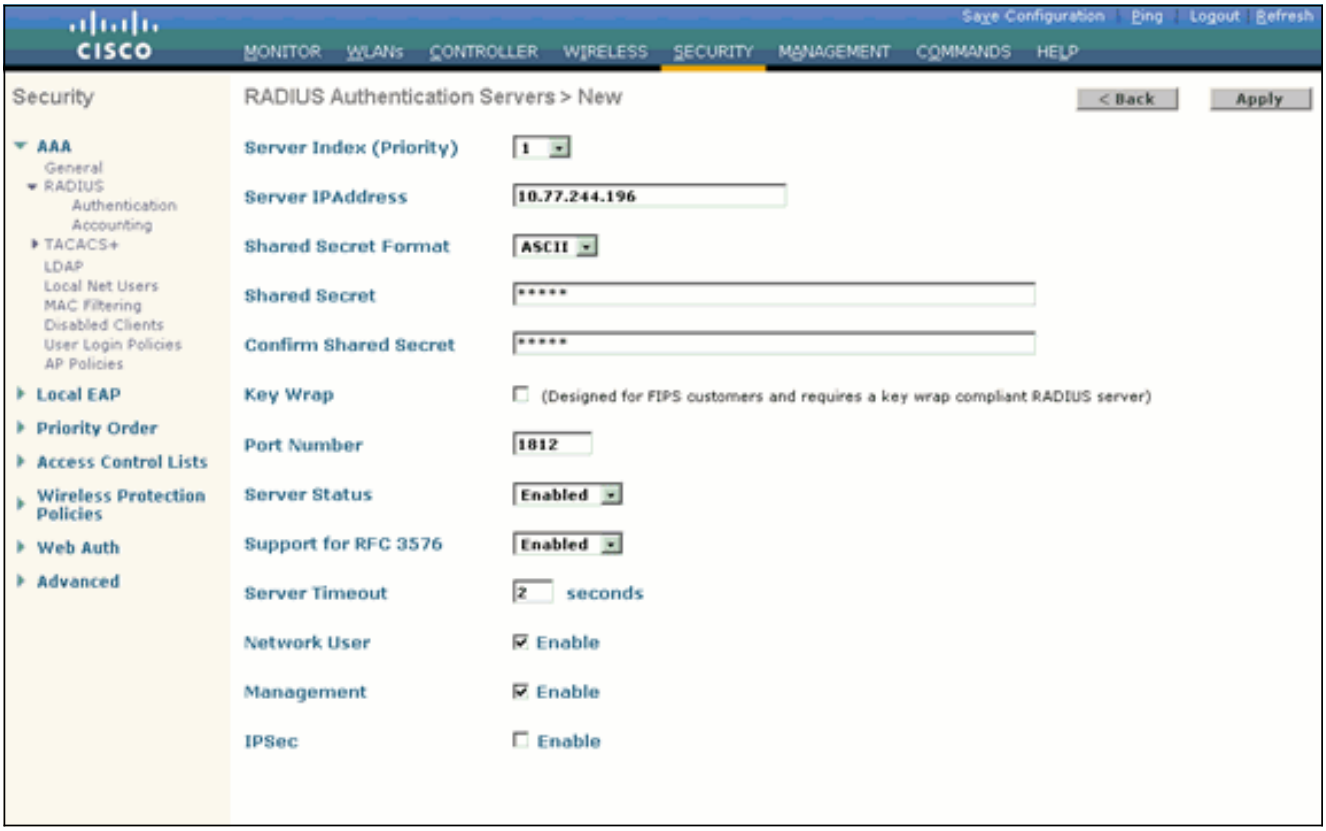
1. Configurar o WLC para a autenticação RADIUS através de um servidor de raio externo
2. Configurar o WLAN para a autenticação do modo de empreendimento WPA2 (EAP-FAST)
3. Configurar o cliente Wireless para o modo de empreendimento WPA2

Configurar o WLC para a autenticação RADIUS através de um servidor de raio externo

O WLC precisa de ser configurado a fim enviar as credenciais do usuário a um servidor de raio externo. O servidor de raio externo então valida a utilização das credenciais do usuário EAP-FAST e fornece o acesso aos clientes Wireless.

Termine estas etapas a fim configurar o WLC para um servidor de raio externo:

1. Escolha a **Segurança** e a **autenticação RADIUS do** controlador GUI indicar a página dos servidores de autenticação RADIUS. Então, clique **novo** a fim definir um servidor Radius.
2. Defina os parâmetros do servidor Radius nos **servidores de autenticação RADIUS >** página **nova**. Estes parâmetros incluem:Endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor Radiusshared secretnúmero da portaStatus de servidorEste documento usa o servidor ACS com um endereço IP de Um ou Mais Servidores Cisco ICM NT de 10.77.244.196.



3. Clique em Apply.

Configurar o WLAN para o modo de empreendimento WPA2 de operação

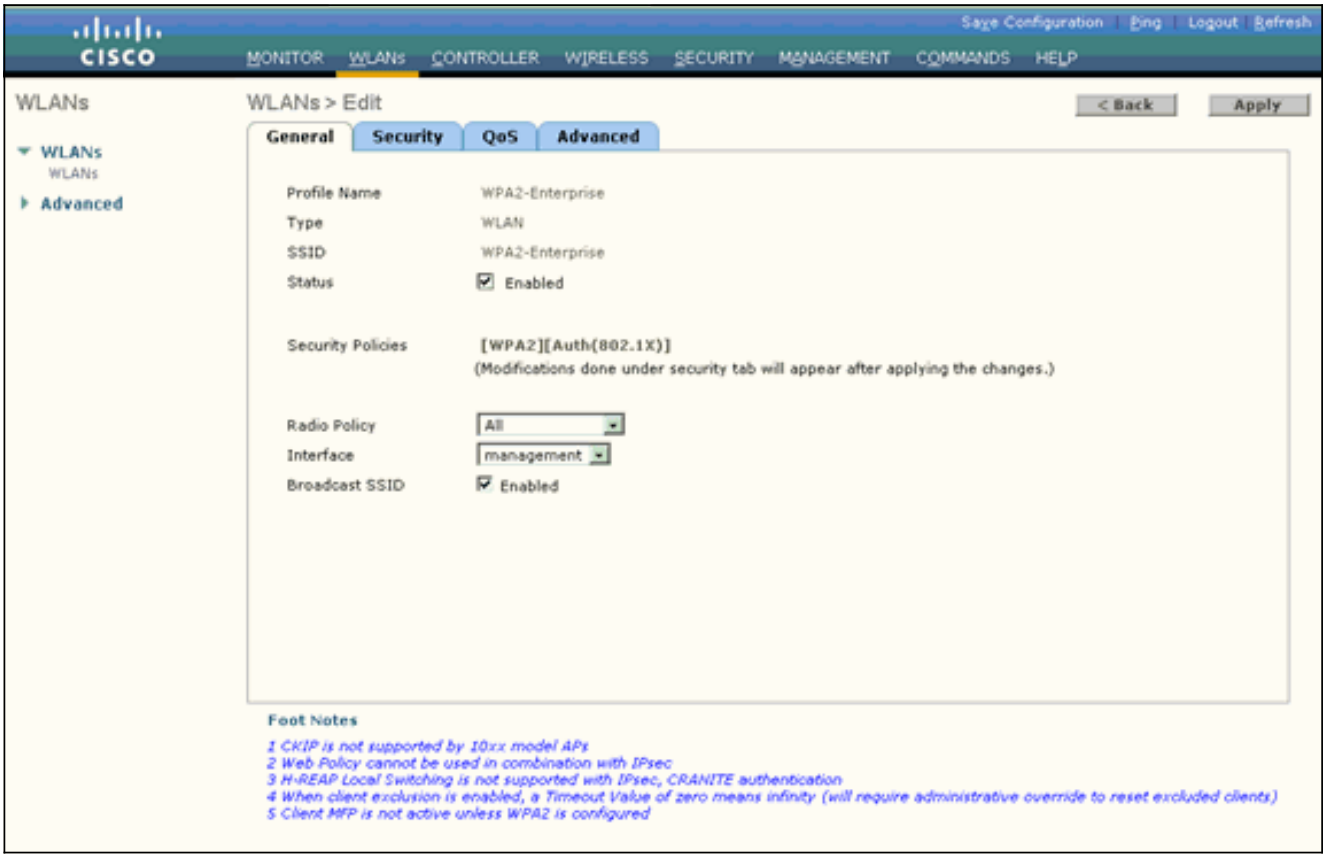
Em seguida, configurar o WLAN que os clientes se usarão para conectar à rede Wireless. O WLAN SSID para o modo de empreendimento WPA2 será WPA2-Enterprise. Este exemplo atribui este WLAN à interface de gerenciamento.

Termine estas etapas a fim configurar o WLAN e seus parâmetros relacionados:

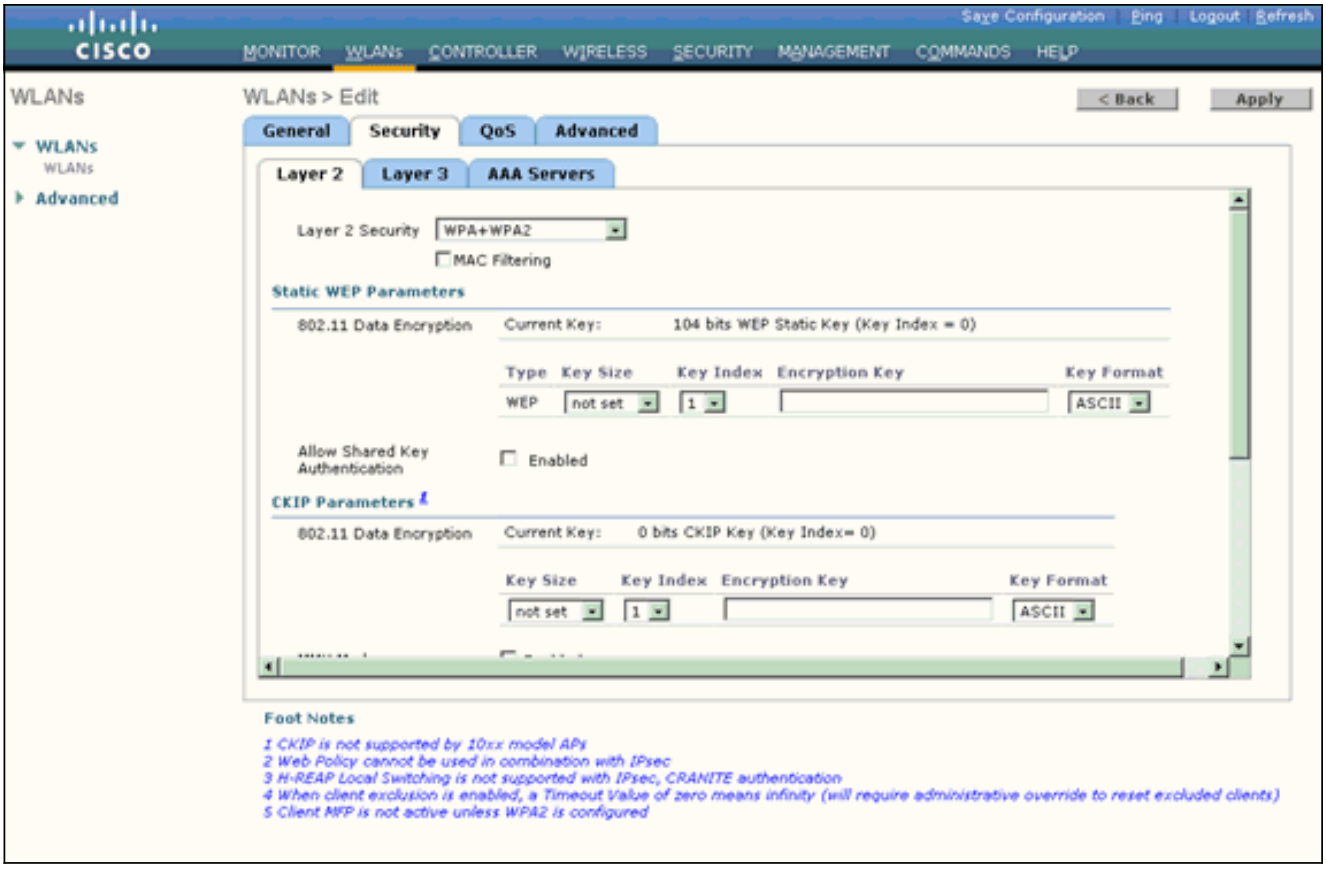
1. Clique **WLAN do** GUI do controlador a fim indicar a página WLAN.Esta página alista os WLAN que existem no controlador.
2. Clique **novo** a fim criar um WLAN novo.

3. Dê entrada com o nome WLAN SSID, e o nome de perfil no **WLAN >** página **nova**. Então, o clique **aplica-se**.Este exemplo usa **WPA2-Enterprise** como o SSID.

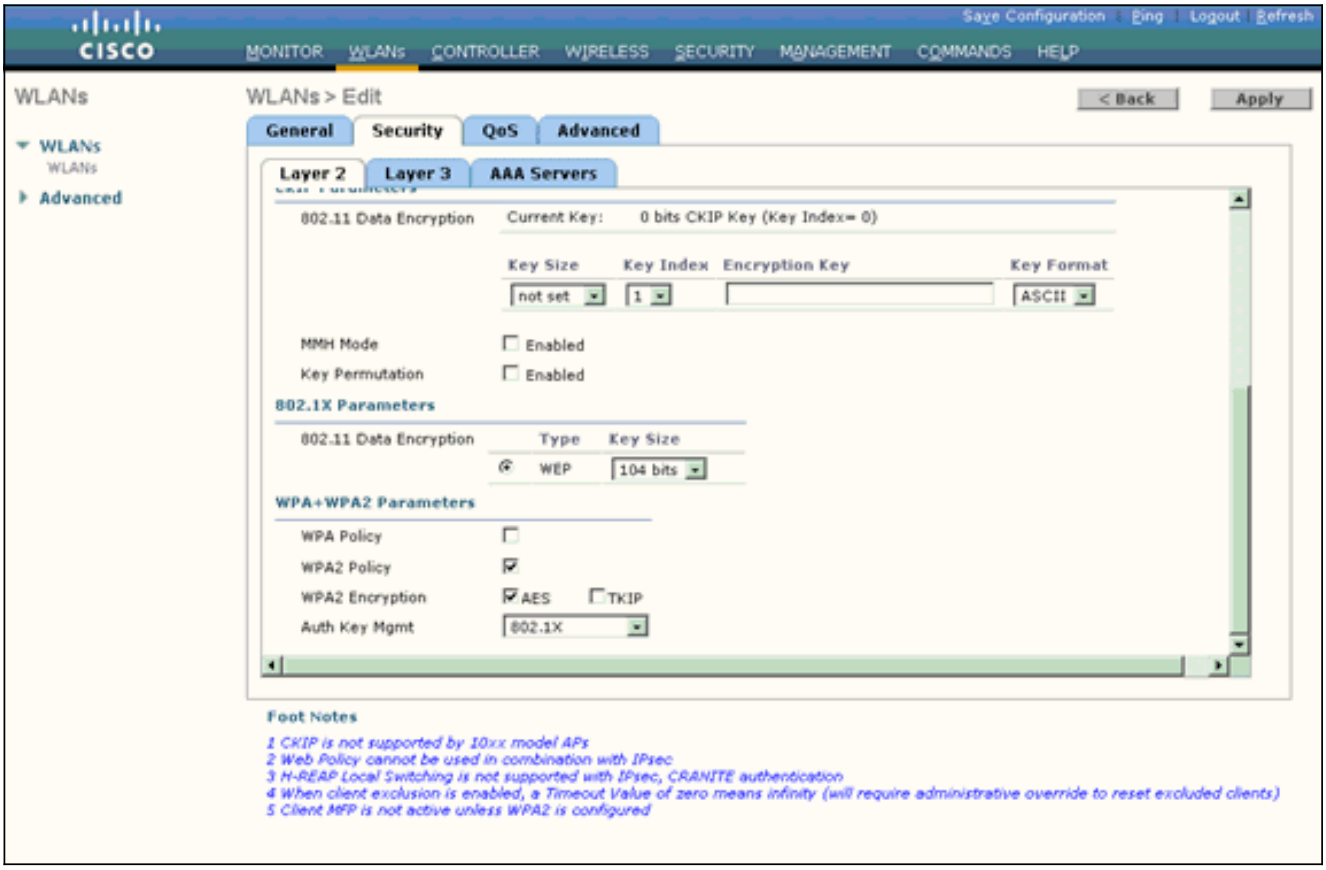
4. Uma vez que você cria um WLAN novo, o **WLAN > edita a** página para o WLAN novo aparece. Nesta página, você pode definir os vários parâmetros específicos a este WLAN. Isto inclui políticas gerais, políticas de segurança, políticas de QoS e parâmetros avançados.
5. Sob políticas gerais, verifique a caixa de **verificação de status** a fim permitir o WLAN.



6. Se você quer o AP transmitir o SSID em seus beacon frame, verifique a **caixa de verificação SSID da transmissão**.
7. Clique na guia Security. Sob a Segurança da camada 2, escolha **WPA+WPA2**.Isto permite a autenticação WPA para o WLAN.

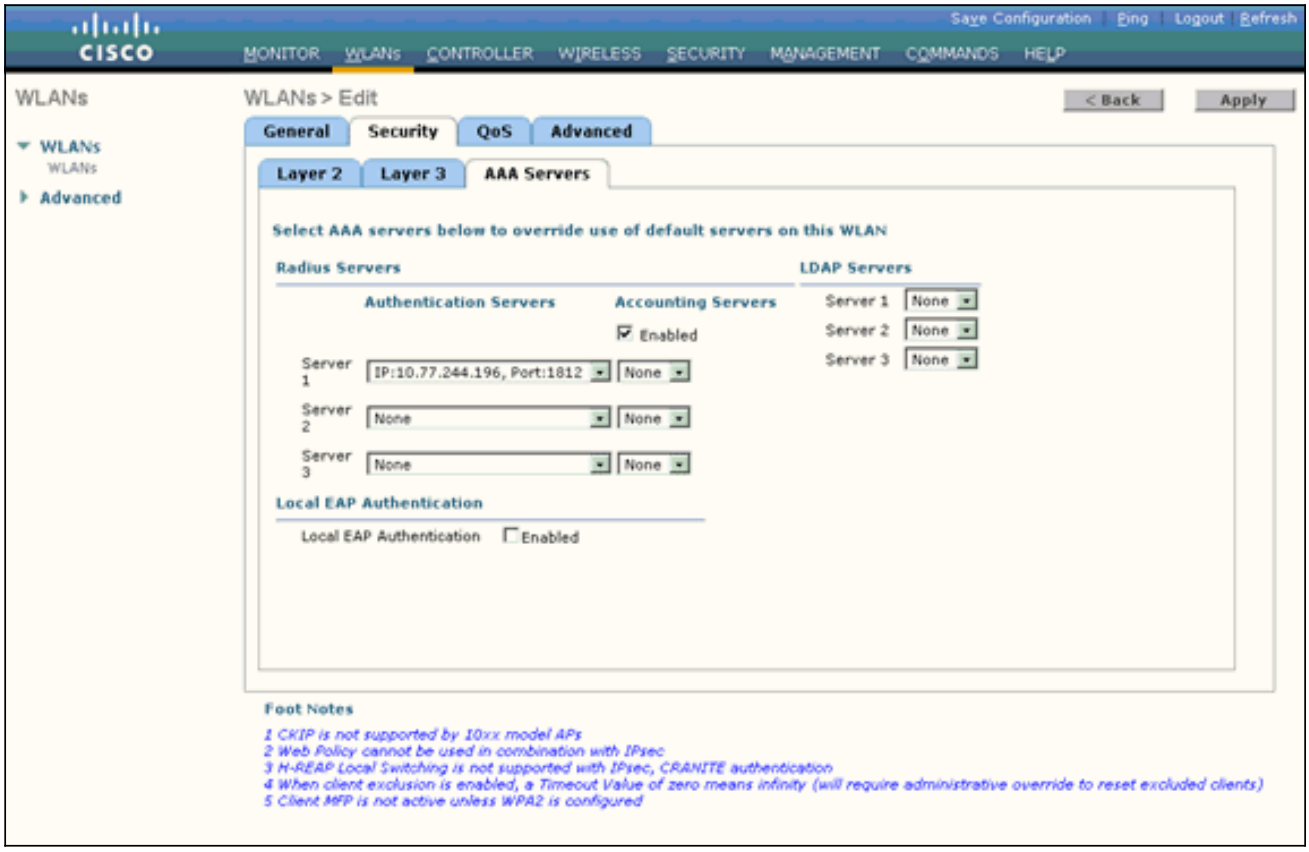


8. Enrole para baixo a página para alterar os **parâmetros WPA+WPA2**.Neste exemplo, a política WPA2 e a criptografia de AES são selecionadas.



9. Sob a chave Mgmt do AUTH, escolha o **802.1x**.Isto permite o WPA2 usando a autenticação 802.1x/EAP e a criptografia de AES para o WLAN.
10. Clique a aba dos **servidores AAA**. Sob Authentication Server, escolha o endereço IP do servidor apropriado.Neste exemplo, 10.77.244.196 é usado como o servidor

Radius.



11. Clique em Apply.**Nota:** Este é o único ajuste EAP que precisa de ser configurado no controlador para a autenticação de EAP. Todas configurações restantes específicas à necessidade EAP-FAST de ser feito no servidor Radius e nos clientes que precisam de ser autenticadas.

Configurar o servidor Radius para a autenticação do modo de empreendimento WPA2 (EAP-FAST)

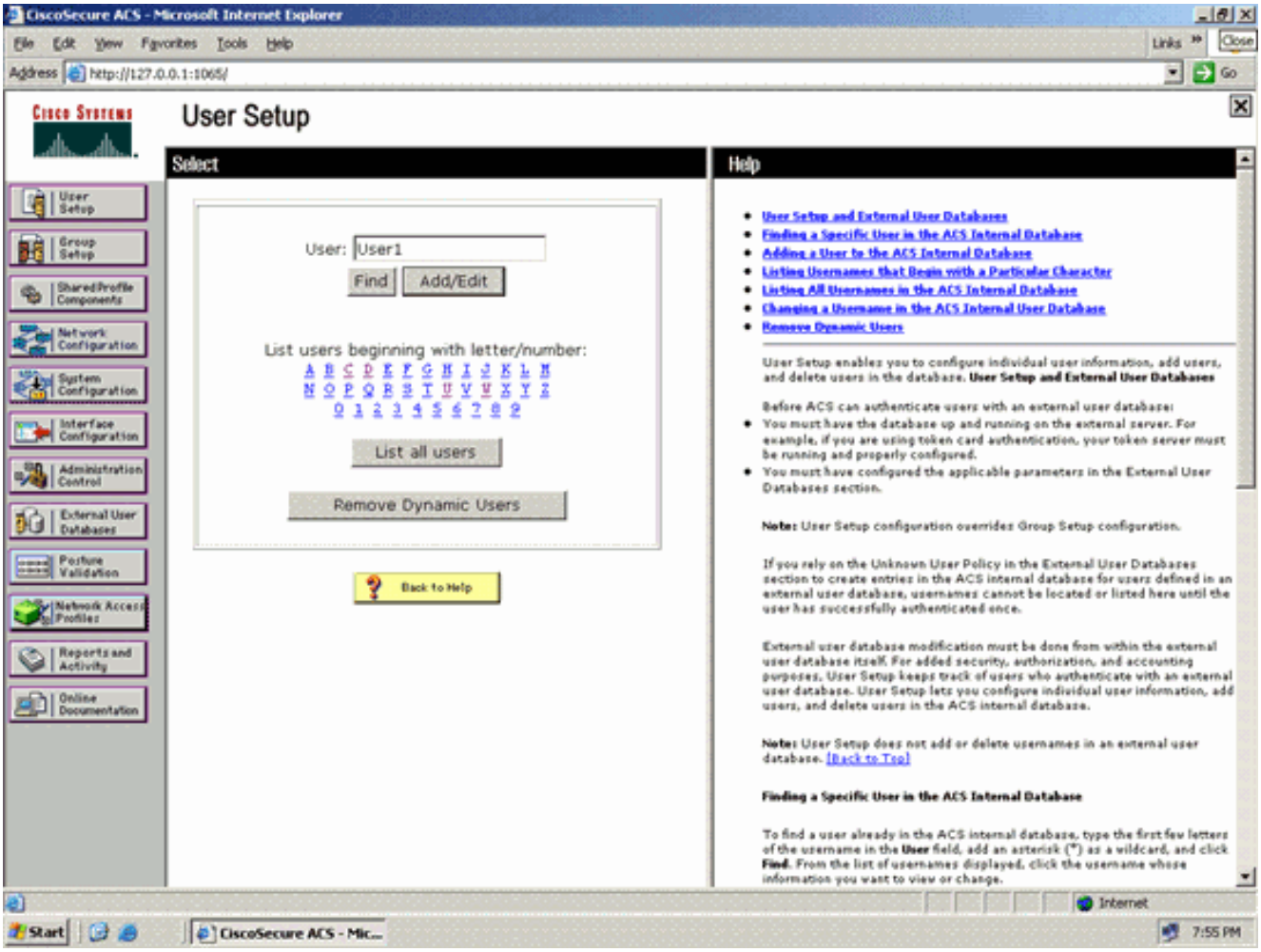
Neste exemplo, o Cisco Secure ACS é usado como o servidor de raio externo. Execute estas etapas a fim configurar o servidor Radius para a autenticação EAP-FAST:

1. Crie uma base de dados de usuário para autenticar clientes
2. Adicionar o WLC como o cliente de AAA ao servidor Radius
3. Configurar a autenticação EAP-FAST no servidor Radius com abastecimento anônimo da Em-faixa PAC**Nota:** EAP-FAST pode ser configurado com abastecimento anônimo da Em-faixa PAC ou abastecimento autenticado da Em-faixa PAC. Este exemplo usa o abastecimento anônimo da Em-faixa PAC. Para a informação detalhada e os exemplos em configurar o EAP RAPIDAMENTE com abastecimento anônimo da Em-faixa PAC e abastecimento autenticado da Em-faixa, refira a autenticação EAP-FAST com exemplo de configuração dos controladores e do servidor de raio externo do Wireless LAN.

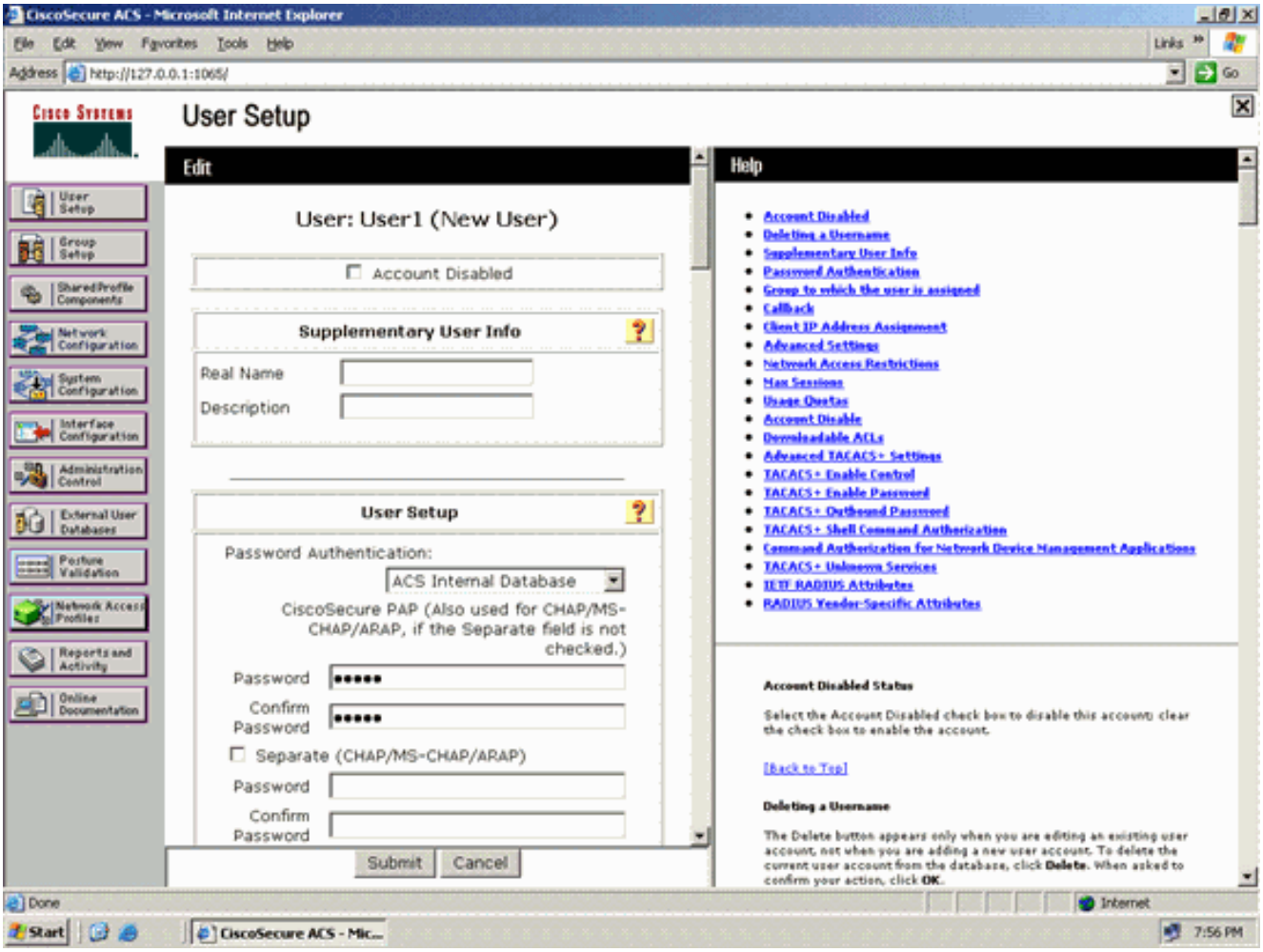
Crie uma base de dados de usuário para autenticar clientes EAP-FAST

Termine estas etapas a fim criar uma base de dados de usuário para clientes EAP-FAST no ACS. Este exemplo configura o nome de usuário e senha do cliente EAP-FAST como o usuário1 e o usuário1, respectivamente.

1. Do ACS GUI na barra de navegação, selecione a **instalação de usuário**. Crie um Sem fio do novo usuário, e clique-o então **adicionam/editam** a fim ir à página da edição deste usuário.



2. Da instalação de usuário edite a página, configurar o nome real e a descrição assim como as configurações de senha segundo as indicações deste exemplo.Este documento usa o **base de dados interno ACS** para a autenticação de senha.

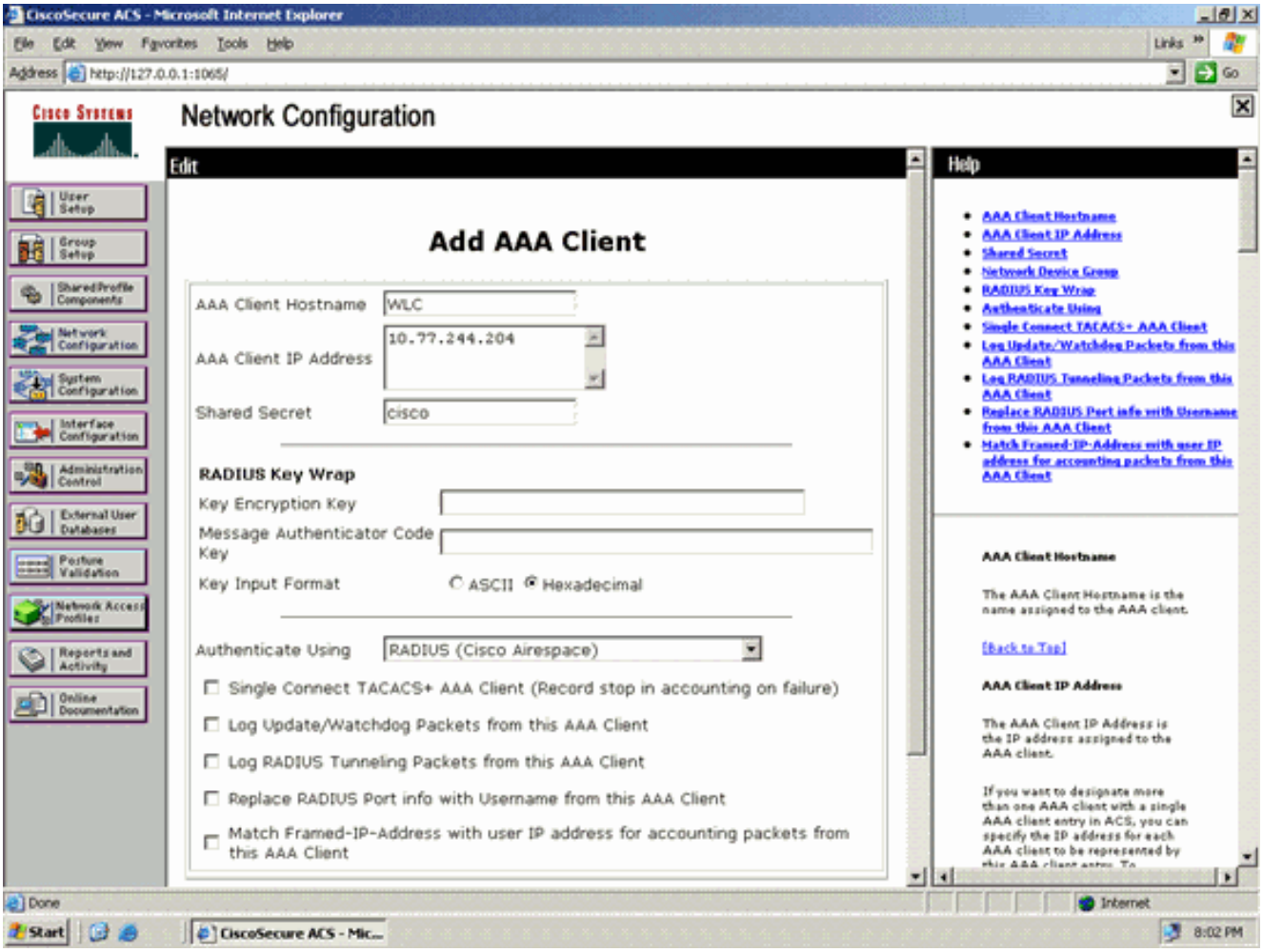


3. Escolha o **base de dados interno ACS da** caixa suspensa da autenticação de senha.
4. Configurar todos os parâmetros requerido restantes e o clique **submete-se**.

Adicionar o WLC como o cliente de AAA ao servidor Radius

Termine estas etapas a fim definir o controlador como um cliente de AAA no servidor ACS:

1. Clique a **configuração de rede do** ACS GUI. Sob a seção do cliente de AAA adicionar da página da configuração de rede, o clique **adiciona a entrada** a fim adicionar o WLC como o cliente de AAA ao servidor Radius.
2. Da página do cliente de AAA, defina o nome do WLC, do endereço IP de Um ou Mais Servidores Cisco ICM NT, do segredo compartilhado e do método de autenticação (RADIUS/Cisco Airespace). Refira a documentação do fabricante para outros Authentication Server NON-
ACS.



Nota: A chave secreta compartilhada que você configura no WLC e no servidor ACS deve combinar. O segredo compartilhado é diferenciando maiúsculas e minúsculas.

3. Clique **Submit+Apply**.

[Configurar a autenticação EAP-FAST no servidor Radius com abastecimento anônimo da Em-faixa PAC]

Abastecimento anônimo da Em-faixa

Este é um dos dois métodos do abastecimento da em-faixa em que o ACS estabelece uma conexão fixada com o cliente do utilizador final com a finalidade de fornecer o cliente um PAC novo. Esta opção permite um handshake de TLS anônimo entre o cliente do utilizador final e o ACS.

Este método opera o interior um túnel autenticado do protocolo do acordo de Diffie-HellmanKey (ADHP) antes que o par autentique o servidor ACS.

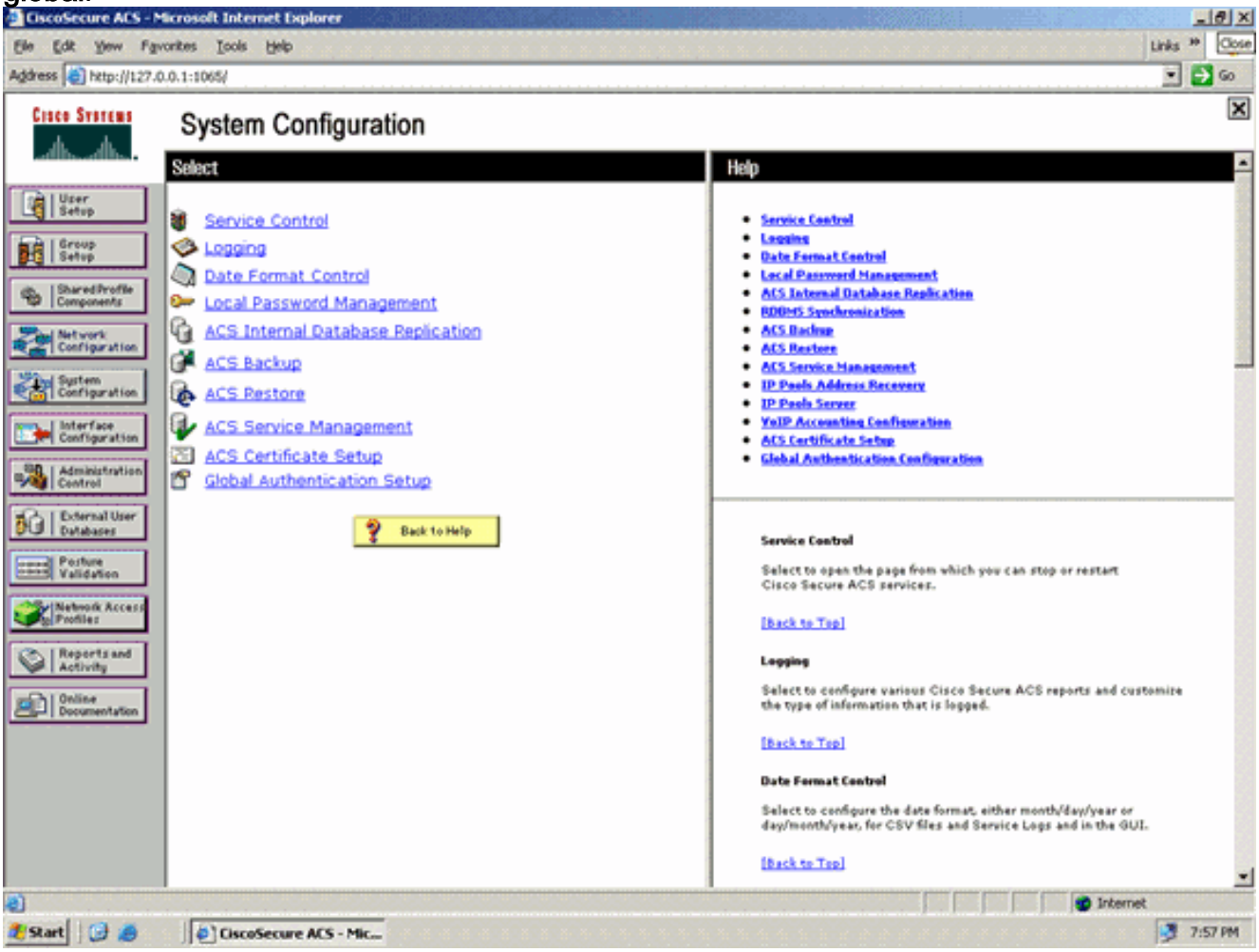
Então, o ACS exige a autenticação EAP-MS-CHAPv2 do usuário. Na autenticação de usuário bem sucedida, o ACS estabelece um túnel de Diffie-Hellman com o cliente do utilizador final. O ACS gerencie um PAC para o usuário e envia-o ao cliente do utilizador final neste túnel, junto com a informação sobre este ACS. Este método do abastecimento usa o EAP-MSCHAPv2 como o método de autenticação na fase zero e EAP-GTC na fase dois.

Porque um server não-autenticado é fornecida, não é possível usar uma senha do texto simples. Consequentemente, somente as credenciais MS-CHAP podem ser usadas dentro do túnel. MS-CHAPv2 é usado para provar a identidade do par e para receber um PAC para umas sessões

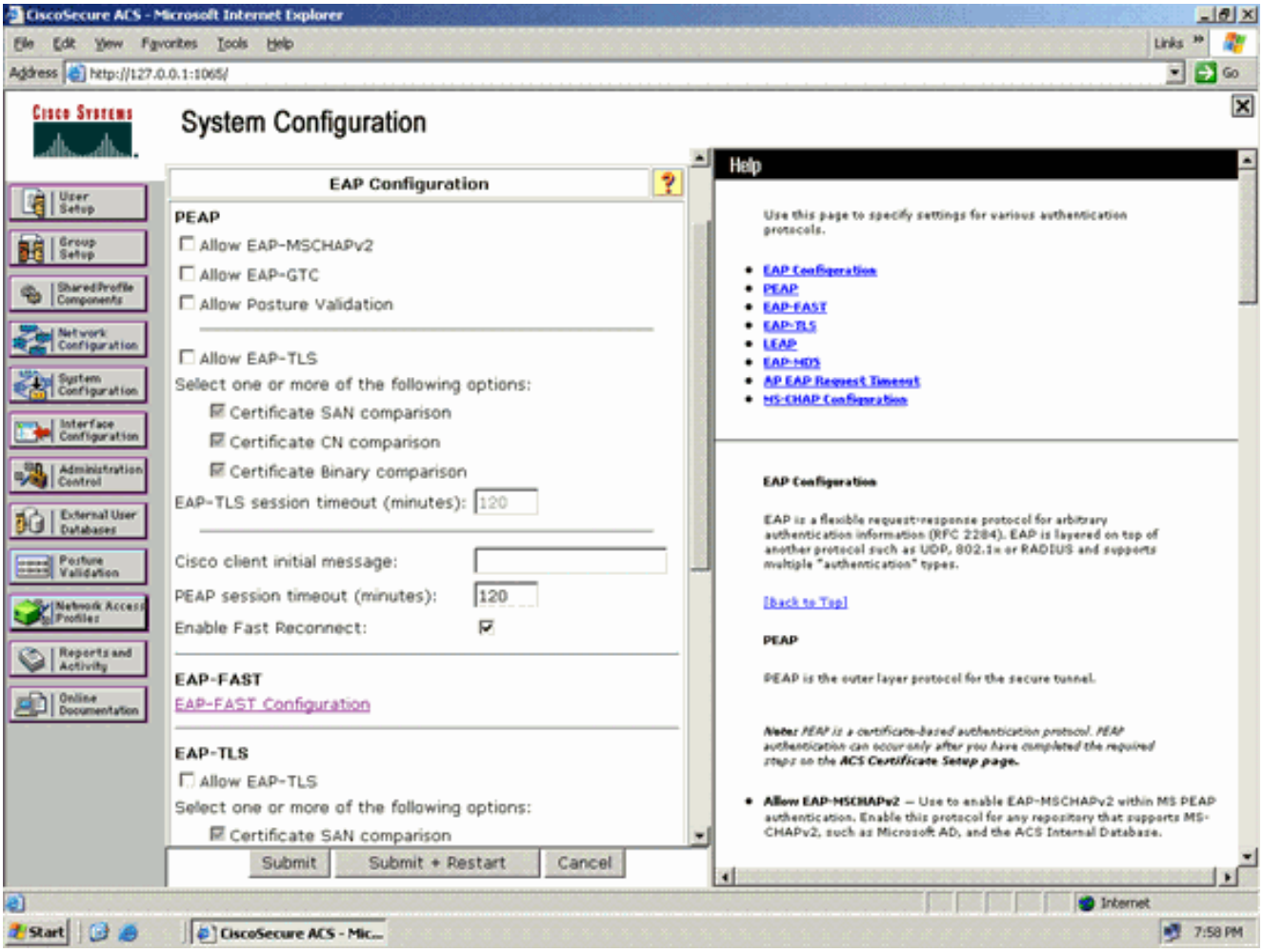
mais adicionais da autenticação (EAP-MS-CHAP será usado como o método interno somente).

Termine estas etapas a fim configurar a autenticação EAP-FAST no servidor Radius para o abastecimento anônimo da em-faixa:

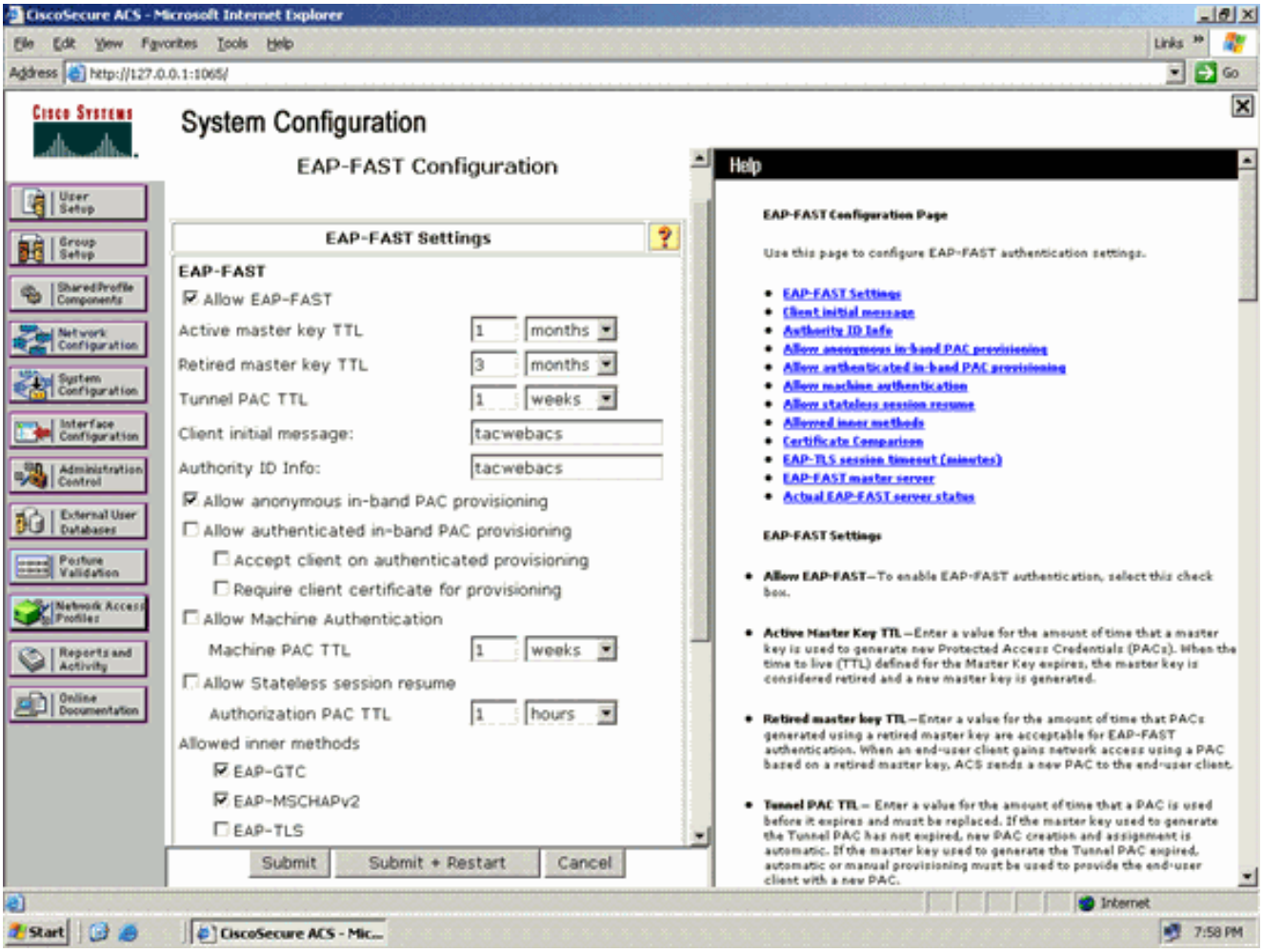
1. Clique a **configuração de sistema do** servidor Radius GUI. Da página da configuração de sistema, escolha a **instalação da autenticação global**.



2. Da página de instalação da autenticação global, clique a **configuração EAP-FAST** a fim ir à página EAP-FAST dos ajustes.



3. Dos ajustes EAP-FAST pagine, verifique a caixa de verificação **EAP-FAST reservar** para permitir EAP-FAST no servidor
   Radius.



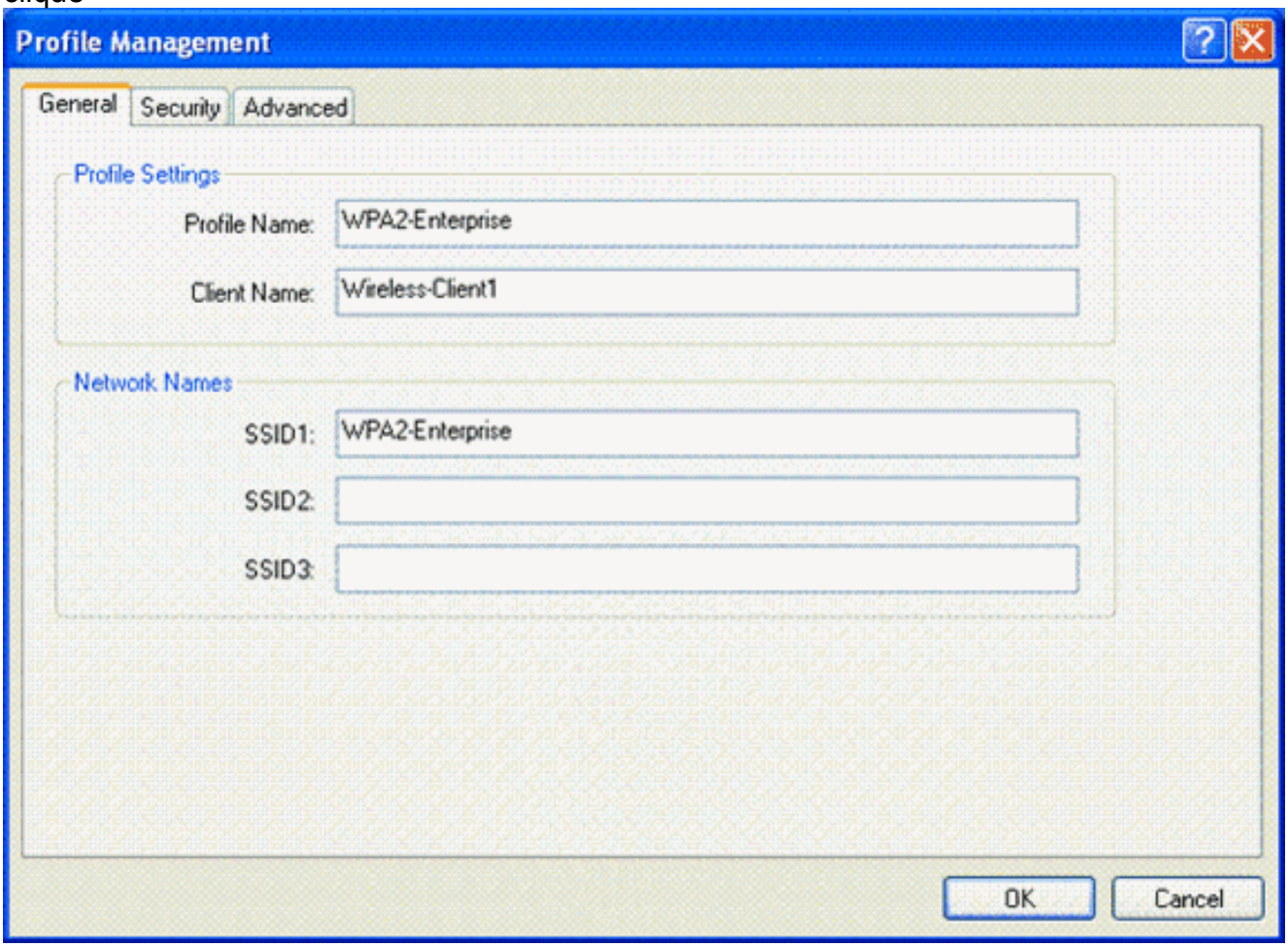
4. Configurar o Active/valores aposentados do chave mestre TTL (tempo ao vivo) como desejado, ou ajuste-os ao valor padrão segundo as indicações deste exemplo.Refira chaves mestres para obter informações sobre do Active e dos chaves mestres aposentados. Também, refira os chaves mestres e o PAC TTL para mais informação.O campo de informação de ID da autoridade representa a identidade textual deste servidor ACS, que um utilizador final pode usar para determinar que servidor ACS a ser autenticado contra. Encher-se neste campo é imperativo.O campo da mensagem do indicador da inicial do cliente especifica uma mensagem a ser enviada aos usuários que autenticam com um cliente EAP-FAST. O comprimento máximo é 40 caráteres. Um usuário verá a mensagem inicial somente se os suportes ao cliente do utilizador final o indicador.
5. Se você quer o ACS executar o abastecimento anônimo da em-faixa PAC, verifique a caixa de verificação **anônima do abastecimento da em-faixa PAC reservar**.
6. **Métodos internos permitidos** — Esta opção determina que métodos de EAP internos podem ser executado dentro do túnel EAP-FAST TLS. Para o abastecimento anônimo da em-faixa, você deve permitir o EAP-GTC e o EAP-MS-CHAP para a compatibilidade retrógrada. Se você seleciona permita o abastecimento anônimo da em-faixa PAC, você deve selecionar EAP-MS-CHAP (fase zero) e EAP-GTC (fase dois).

Configurar o cliente Wireless para o modo de empreendimento WPA2 de operação

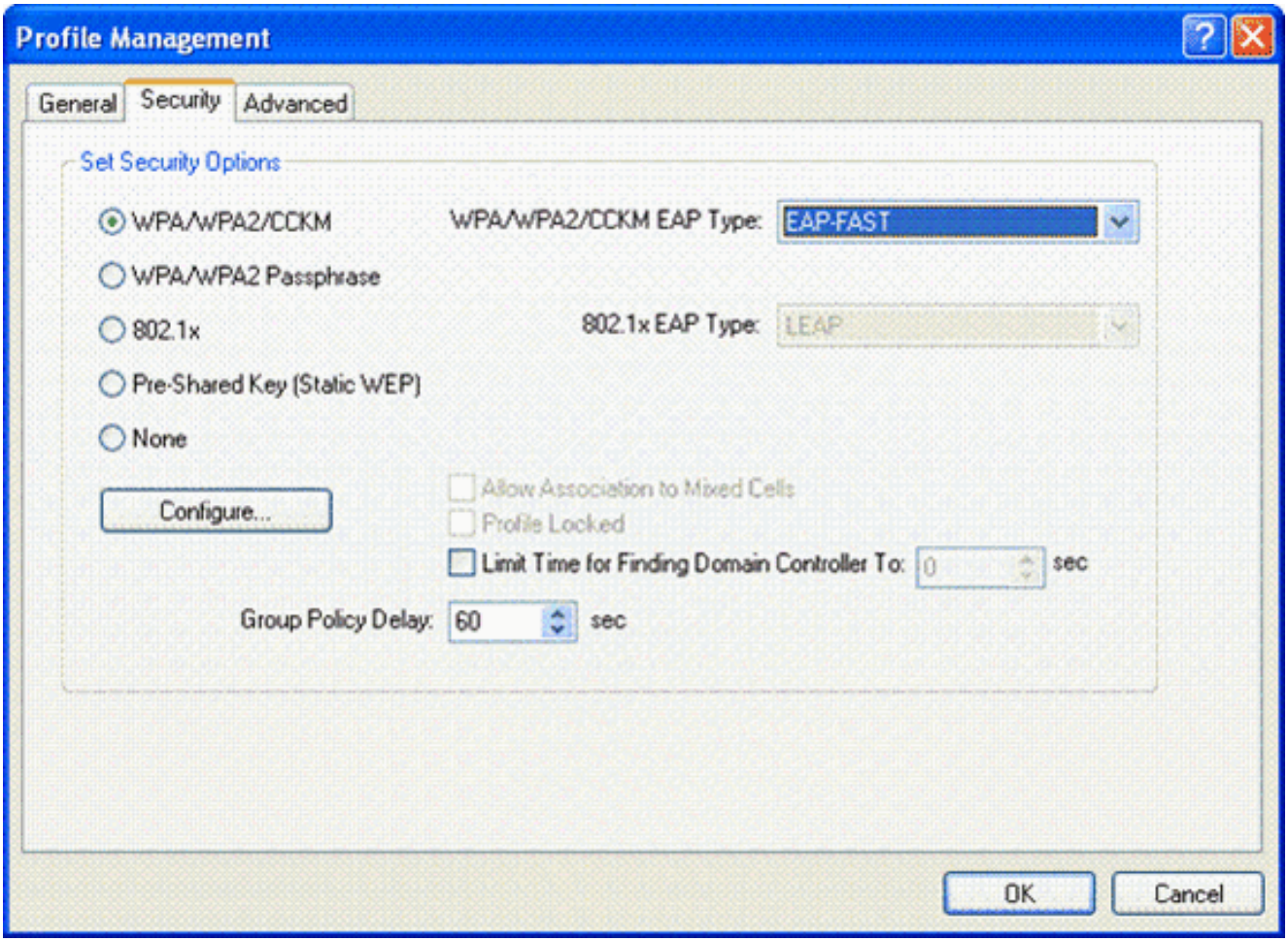
A próxima etapa é configurar o cliente Wireless para o modo de empreendimento WPA2 de operação.

Termine estas etapas a fim configurar o cliente Wireless para o modo de empreendimento WPA2.

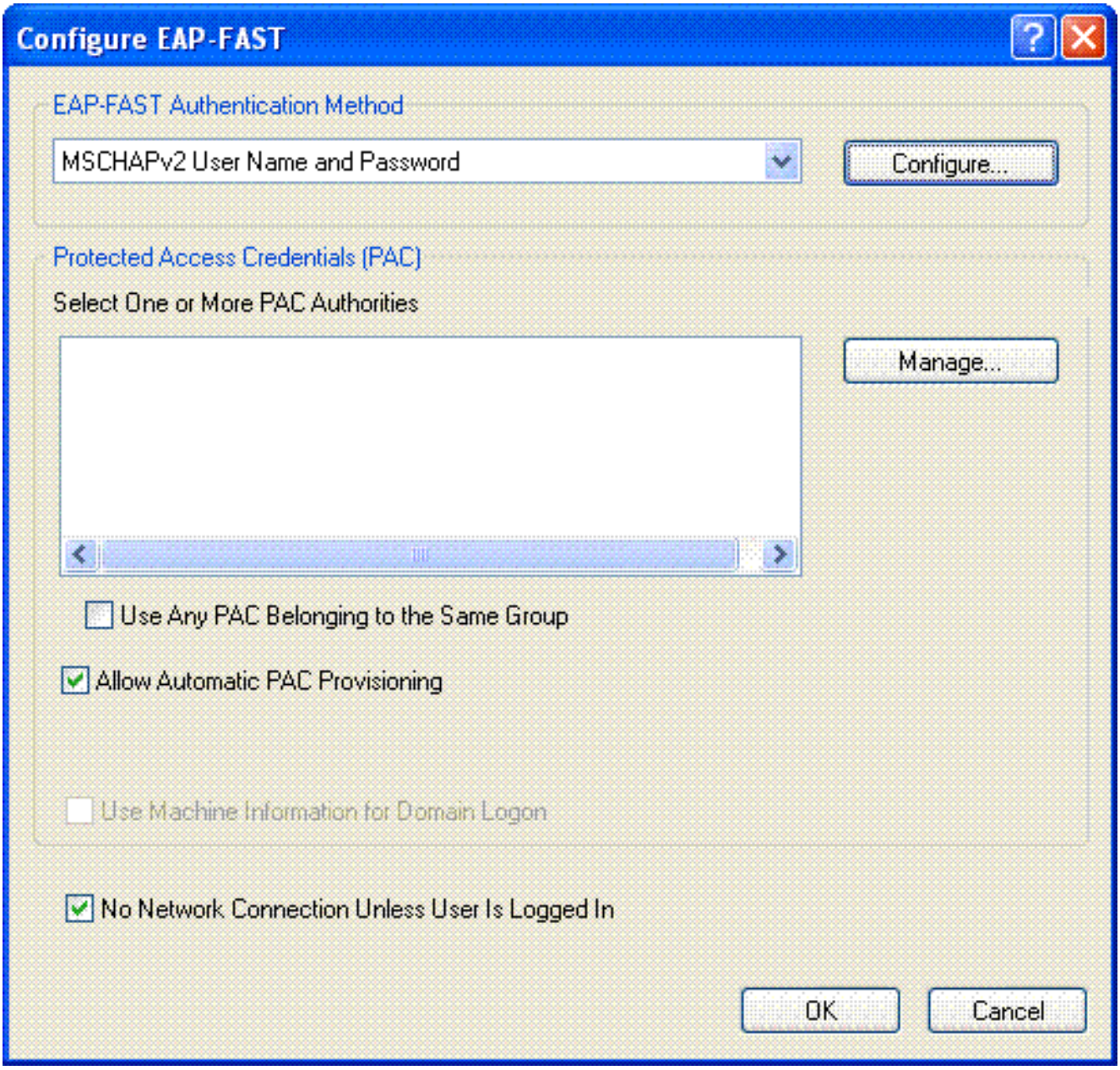
1. Do indicador do utilitário de Desktop de Aironet, clique o **Gerenciamento do perfil > novo** a fim criar um perfil para o usuário WPA2-Enterprise WLAN.Como mencionado mais cedo, este documento usa o nome WLAN/SSID como **WPA2-Enterprise** para o cliente Wireless.
2. Da janela de gerenciamento do perfil, clique o **tab geral** e configurar o nome de perfil, o nome do cliente e o nome SSID segundo as indicações deste exemplo. Então, **APROVAÇÃO do**
   clique



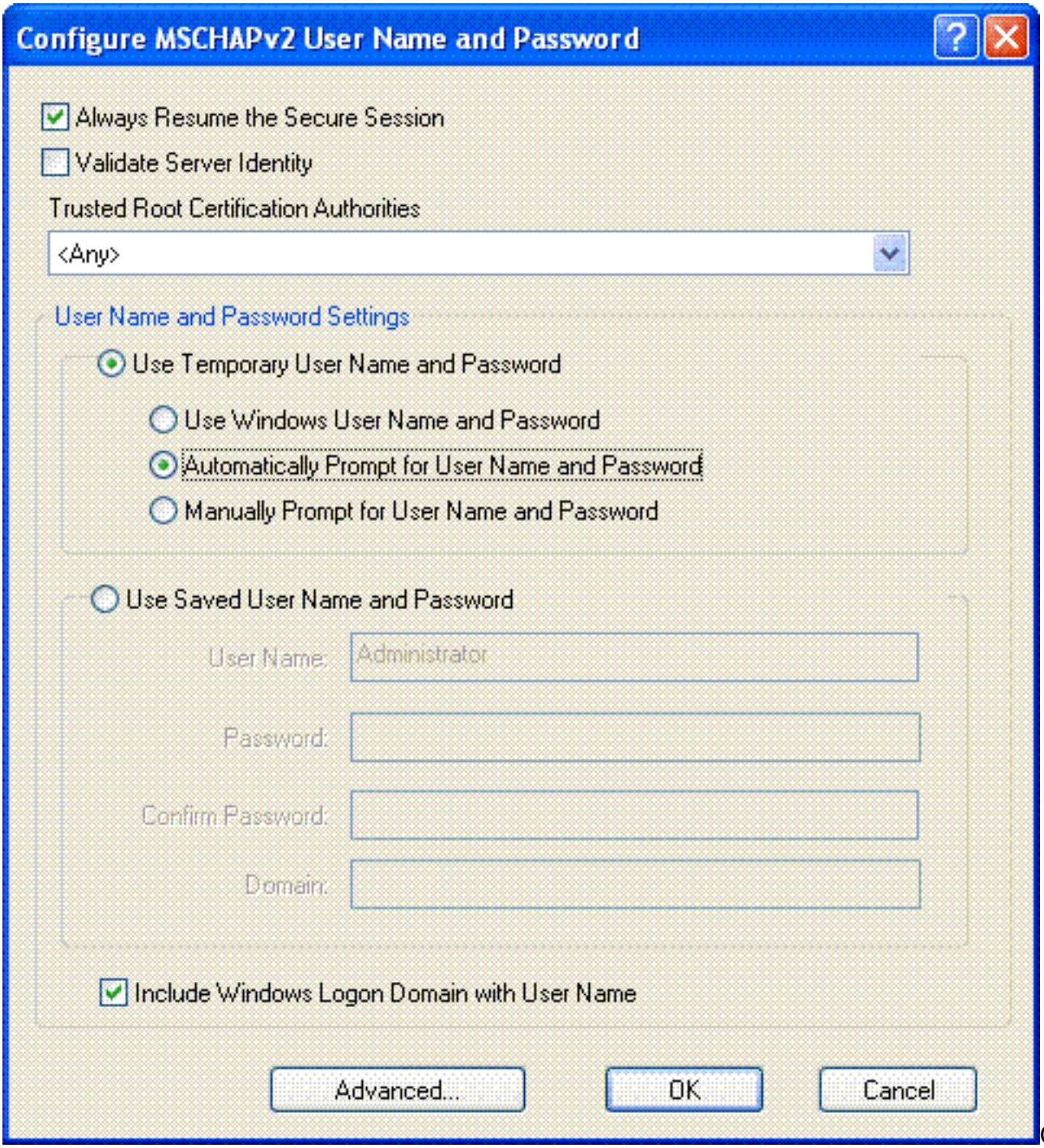
3. Clique a **ABA de segurança** e escolha **WPA/WPA2/CCKM** permitir o modo WPA2 de operação. Sob o tipo WPA/WPA2/CCKM EAP, escolha **EAP-FAST**. O clique **configura** a fim configurar o ajuste EAP-
   FAST.



4. Do indicador EAP-FAST configurar, verifique a caixa de verificação **automática do abastecimento reservar PAC**. Se você quer configurar o abastecimento anônimo PAC, EAP-MS-CHAP estará usado como o único método interno na fase zero.



5. Escolha o nome de usuário MSCHAPv2 e a senha como o método de autenticação da caixa suspensa EAP-FAST do método de autenticação. Clique em Configurar.
6. Do nome de usuário e da janela de senha configurar MSCHAPv2, escolha os ajustes apropriados do nome de usuário e senha.Este exemplo escolhe **automaticamente a alerta para o nome de usuário e a senha**.



O mesmo nome de usuário e a senha devem ser registrados no ACS. Como mencionado mais cedo, este exemplo usa o usuário1 e o usuário1 respectivamente como o nome de usuário e senha. Também, note que este é um abastecimento anônimo da em-faixa. Consequentemente, o cliente não pode validar o certificado de servidor. Você precisa de certificar-se de que a caixa de verificação da identidade do server da validação está desmarcada.

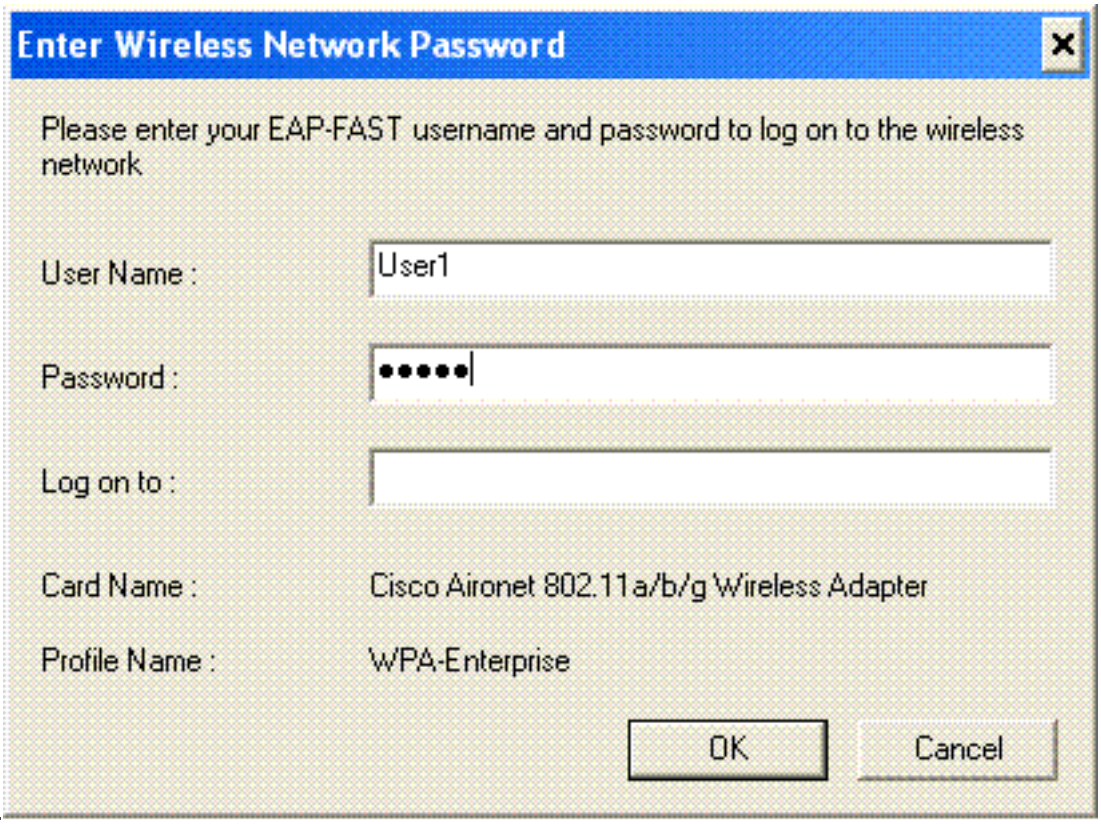
7. Clique em **OK**.

Verifique o modo de empreendimento WPA2 de operação

Termine estas etapas a fim verificar se sua configuração do modo de empreendimento WPA2 trabalha corretamente:

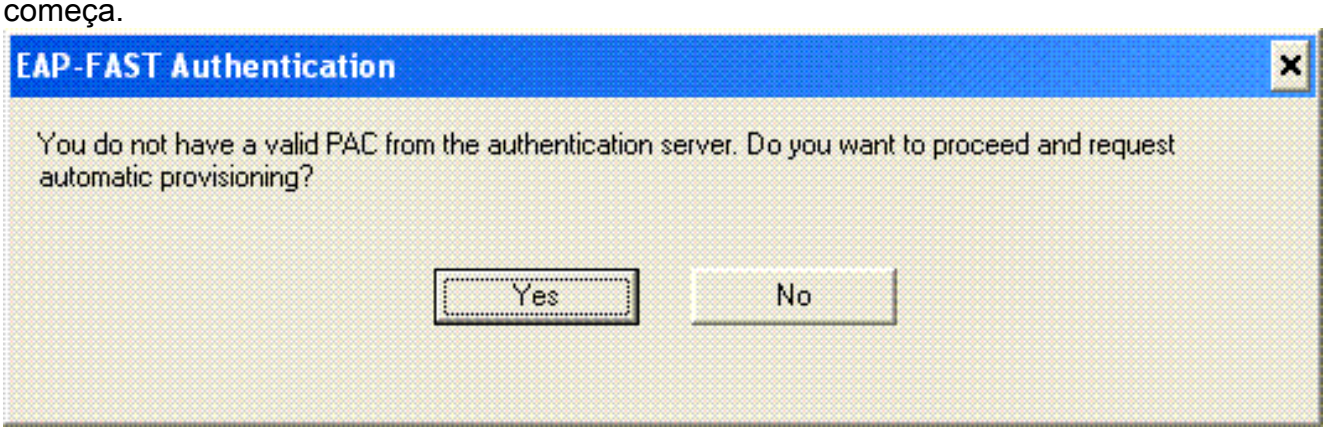
1. Do indicador do utilitário de Desktop de Aironet, selecione o perfil **WPA2-Enterprise** e o clique **ativam** a fim ativar o perfil do cliente Wireless.

2. Se você permitiu MS-CHAP ver2 como sua autenticação, a seguir o cliente alertará para o nome de usuário e

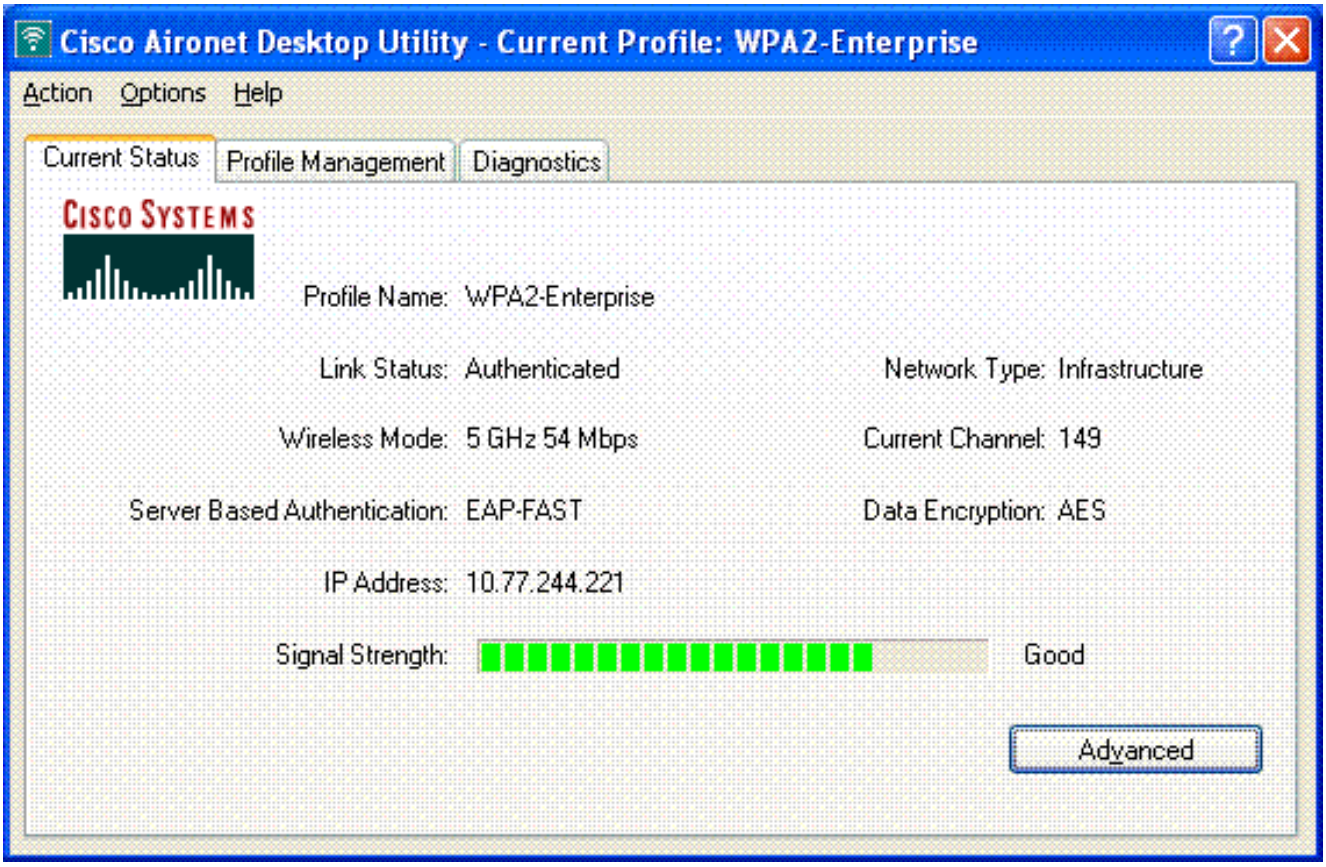


senha.

3. Durante o processamento EAP-FAST do usuário, você será alertado pelo cliente pedir o PAC do servidor Radius. Quando você clica **sim**, o abastecimento PAC começa.



4. Após o abastecimento bem sucedido PAC na fase zero, fase um e dois siga e um procedimento da autenticação bem sucedida ocorre.Em cima da autenticação bem sucedida o cliente Wireless obtém associado ao WLAN WPA2-Enterprise. Está aqui o tiro de tela:



Você pode igualmente verificar se o servidor Radius recebe e valida o pedido de autenticação do cliente Wireless. Verifique os relatórios passados das autenticações e das falhas de tentativa no servidor ACS a fim realizar isto. Estes relatórios estão disponíveis sob relatórios e atividades no servidor ACS.

Configurar os dispositivos para o Modo pessoal WPA2

Execute estas etapas a fim configurar os dispositivos para o modo WPA2-Personal de operação:

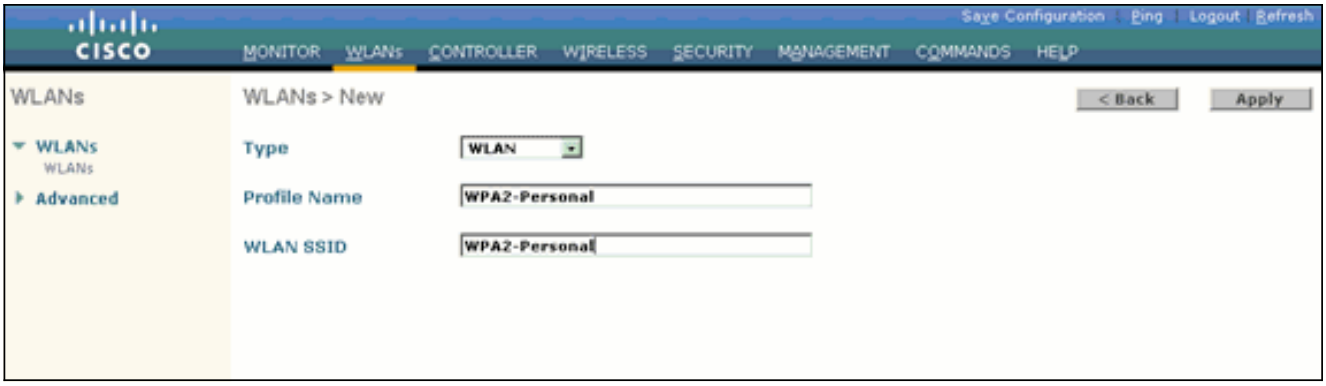
1. Configurar o WLAN para a autenticação do Modo pessoal WPA2
2. Configurar o cliente Wireless para o Modo pessoal WPA2

Configurar o WLAN para o Modo pessoal WPA2 de operação

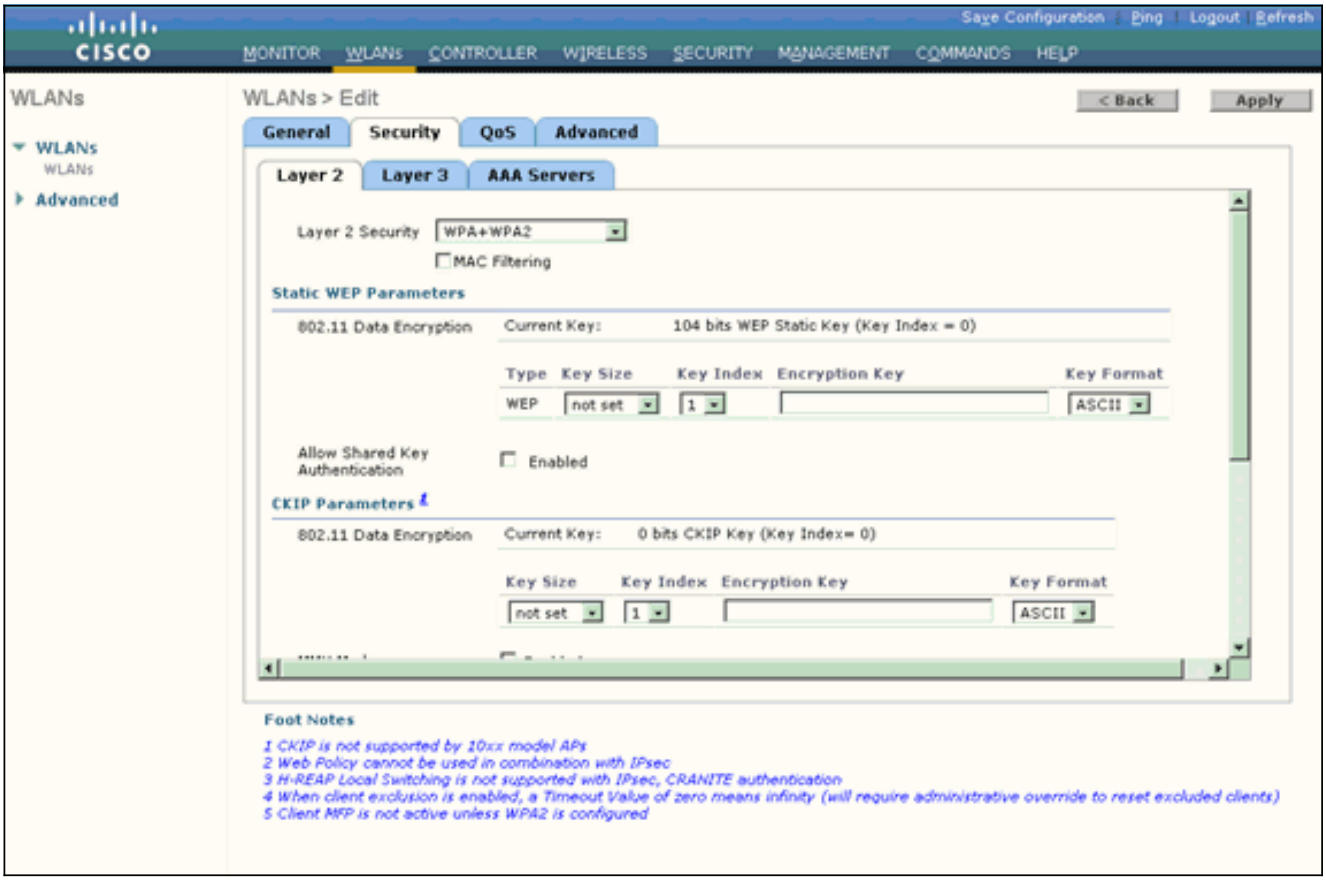
Você precisa de configurar o WLAN que os clientes se usarão para conectar à rede Wireless. O WLAN SSID para o Modo pessoal WPA2 será WPA2-Personal. Este exemplo atribui este WLAN à interface de gerenciamento.

Termine estas etapas a fim configurar o WLAN e seus parâmetros relacionados:

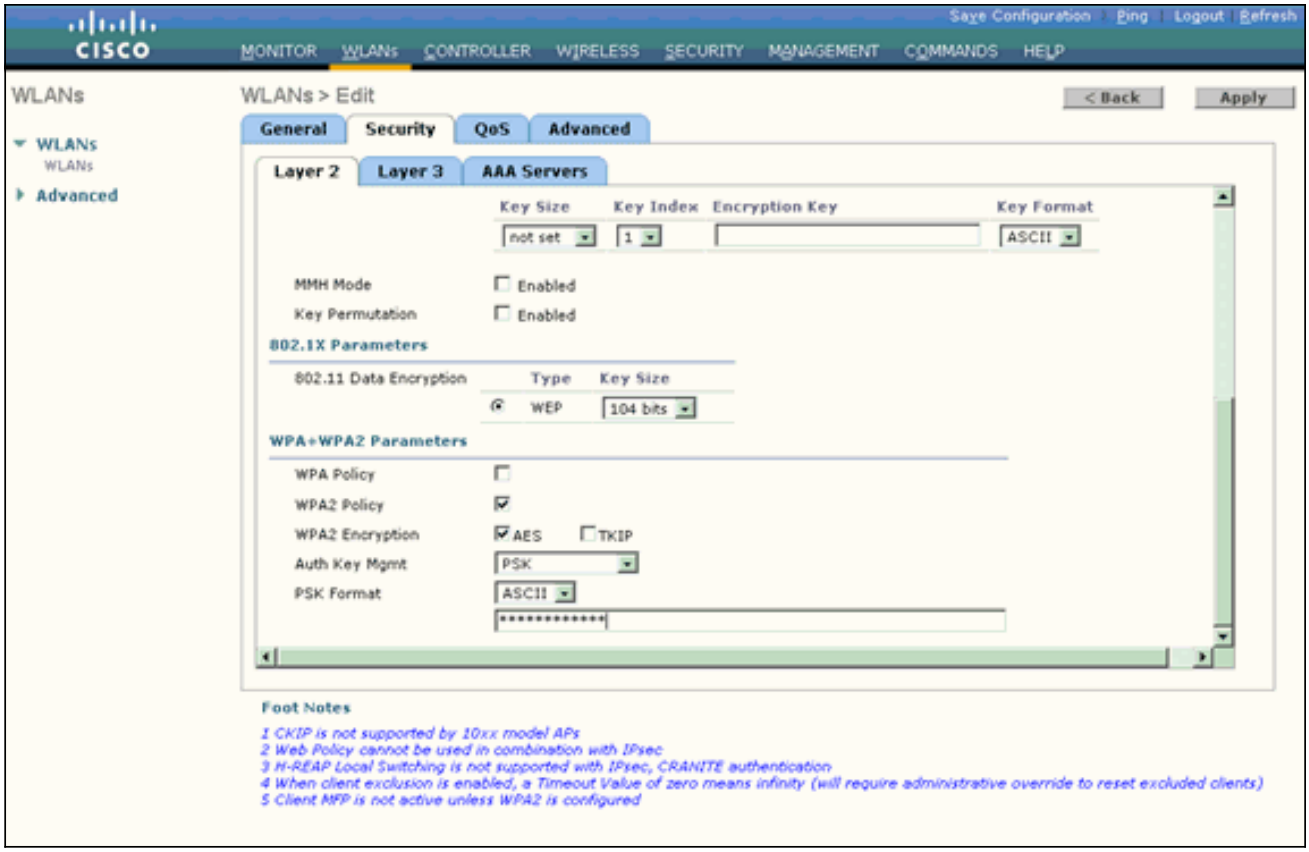
1. Clique **WLAN do** GUI do controlador a fim indicar a página WLAN.Esta página alista os WLAN que existem no controlador.
2. Clique **novo** a fim criar um WLAN novo.
3. Entre no nome, no nome de perfil e no ID de WLAN WLAN SSID no WLAN > página nova. Então, o clique **aplica-se**.Este exemplo usa **WPA2-Personal** como o SSID.



4. Uma vez que você cria um WLAN novo, o **WLAN > edita a** página para o WLAN novo aparece. Nesta página, você pode definir os vários parâmetros específicos a este WLAN. Isto inclui políticas gerais, políticas de segurança, políticas de QoS e parâmetros avançados.
5. Sob políticas gerais, verifique a caixa de **verificação de status** a fim permitir o WLAN.
6. Se você quer o AP transmitir o SSID em seus beacon frame, verifique a **caixa de verificação SSID da transmissão**.
7. Clique na guia Security. Sob a Segurança da camada, escolha **WPA+WPA2**.Isto permite a autenticação WPA para o
WLAN.



8. Enrole para baixo a página para alterar os **parâmetros WPA+WPA2**.Neste exemplo, a política WPA2 e a criptografia de AES são selecionadas.
9. Sob a chave Mgmt do AUTH, escolha o **PSK** a fim permitir WPA2-PSK.
10. Incorpore a chave pré-compartilhada ao campo apropriado como mostrado.



Nota: A chave pré-compartilhada usada no WLC deve combinar com esse configurado nos clientes Wireless.

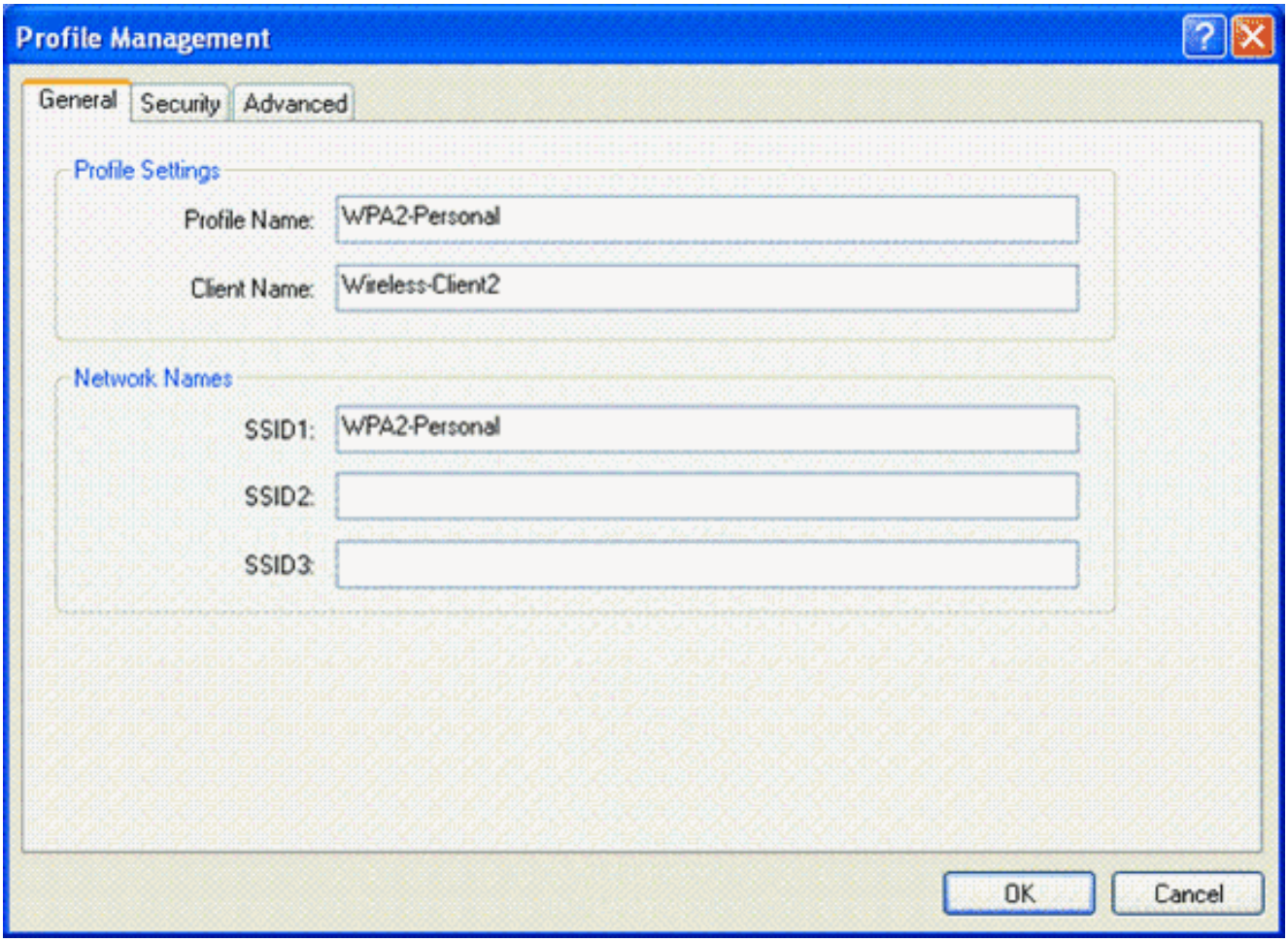
11. Clique em Apply.

Configurar o cliente Wireless para o Modo pessoal WPA2

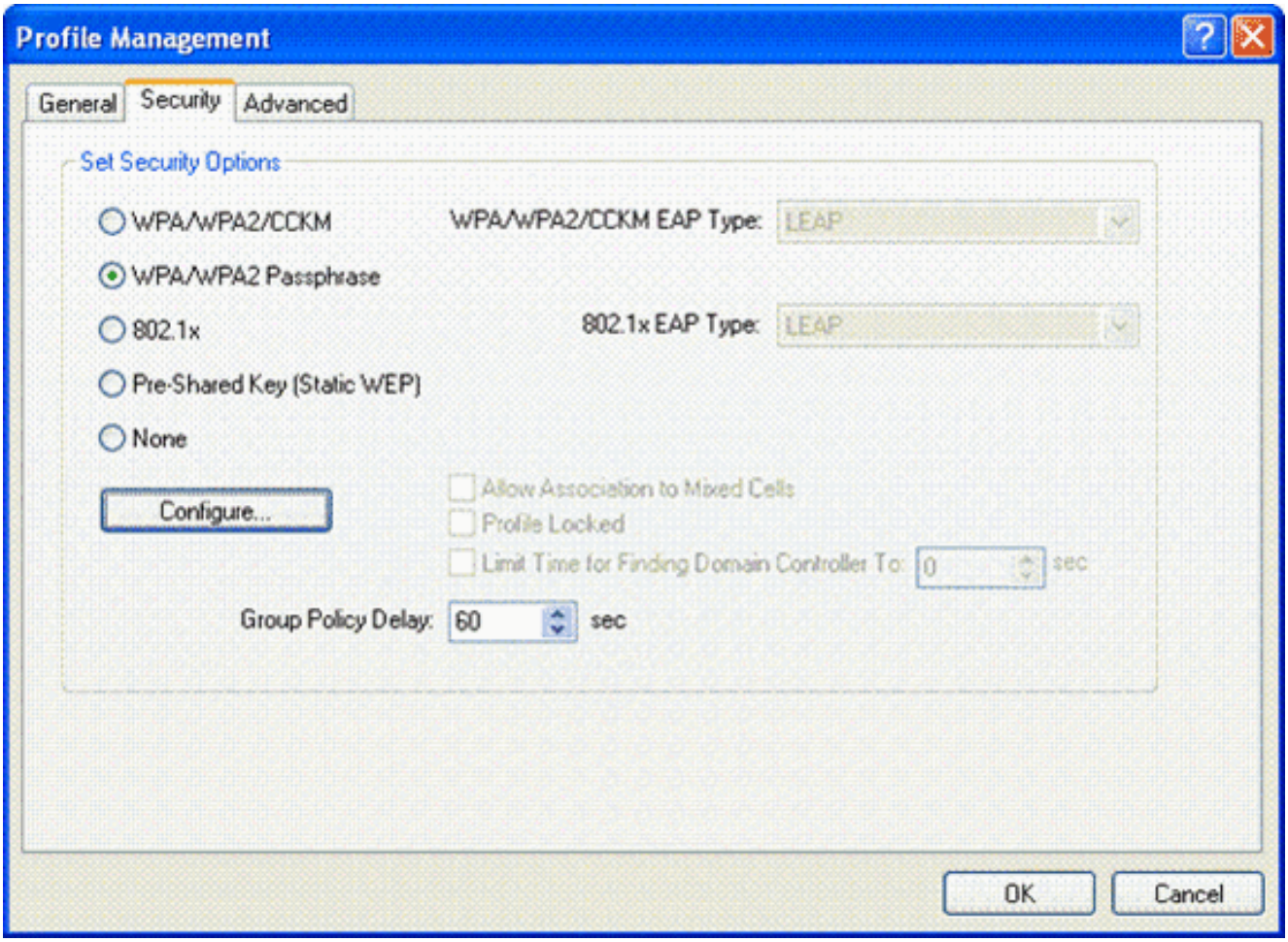
A próxima etapa é configurar o cliente Wireless para o modo WPA2-Personal de operação.

Termine estas etapas a fim configurar o cliente Wireless para o modo WPA2-Personal:

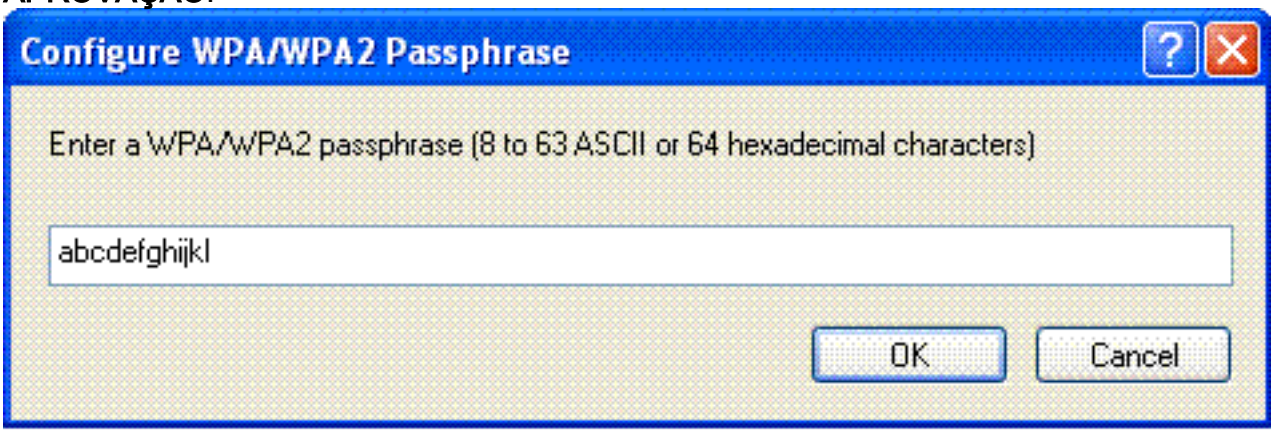
1. Do indicador do utilitário de Desktop de Aironet, clique o **Gerenciamento do perfil > novo** a fim criar um perfil para o usuário WPA2-PSK WLAN.
2. Da janela de gerenciamento do perfil, clique o **tab geral** e configurar o nome de perfil, o nome do cliente e o nome SSID segundo as indicações deste exemplo. Então, **APROVAÇÃO do**
clique.



3. Clique a **ABA de segurança** e escolha a **frase de passagem WPA/WPA2** permitir o modo WPA2-PSK de operação. O clique **configura** a fim configurar a chave pré-compartilhada WPA-
PSK.



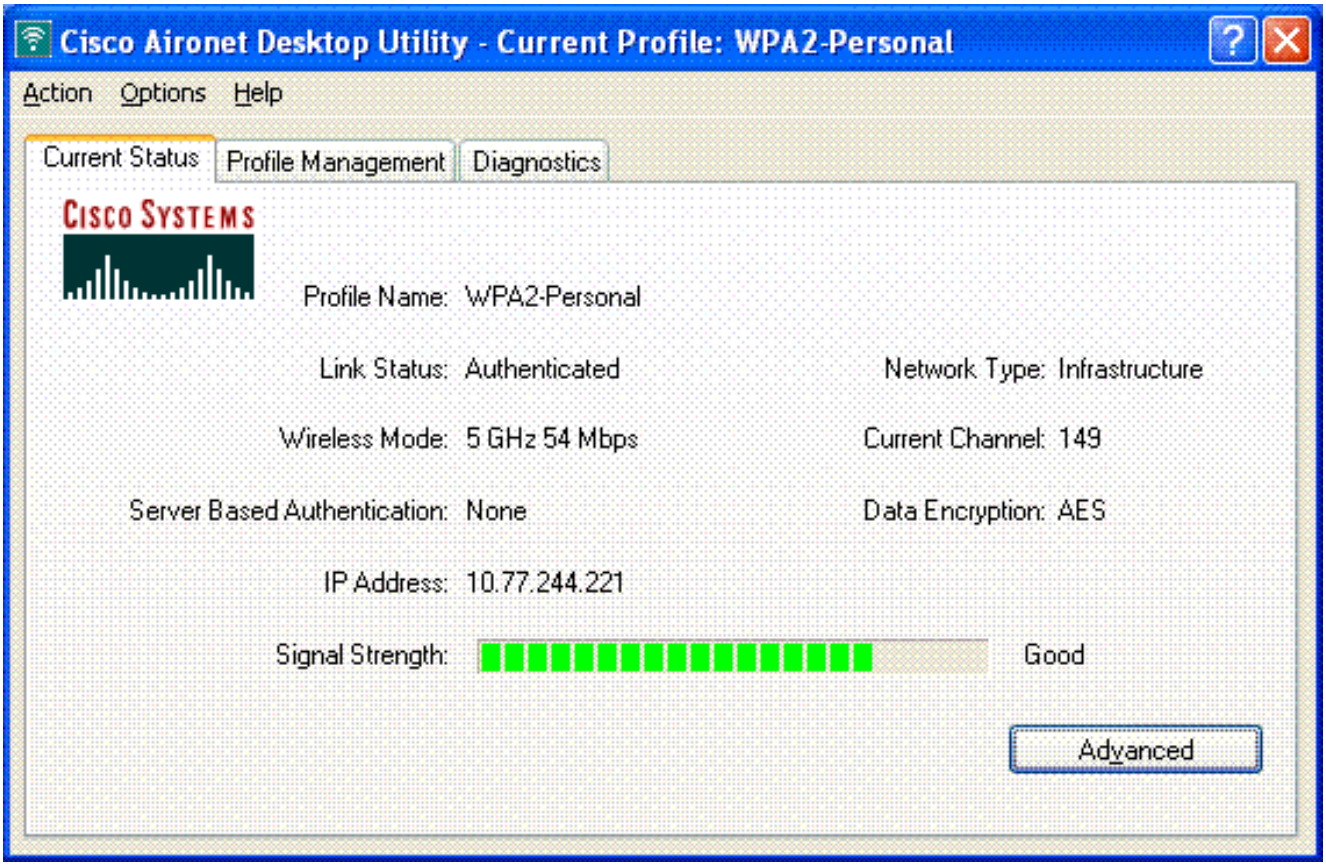
4. Incorpore a chave preshared e clique a **APROVAÇÃO**.



Verifique o modo WPA2-Personal de operação

Termine estas etapas a fim verificar se sua configuração de modo WPA2-Enterprise trabalha corretamente:

1. Do indicador do utilitário de Desktop de Aironet, selecione o perfil **WPA2-Personal** e o clique **ativam** a fim ativar o perfil do cliente Wireless.
2. Uma vez que o perfil é ativado, o cliente Wireless associa ao WLAN em cima da autenticação bem sucedida.Está aqui o tiro de tela:



Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Estes **comandos debug** serão úteis para pesquisar defeitos a configuração:

Nota: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug**.

- **debugar eventos do dot1x permitem** — Permite debugar de todos os eventos do dot1x. Está aqui um resultado do debug do exemplo baseado na autenticação bem sucedida:**Nota:** Algumas das linhas desta saída foram segundas linhas movidas devido às limitações de espaço.`(Cisco Controller)>`**`debug dot1x events enable`** `Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Sending EAP -Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 1) Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93` **`Received EAPOL START from mobile 00:40:96:af:3e:93`** `Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93` **`Sending EAP-Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 2)`** `Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Received EAP Response packet with mismatching id (currentid=2, eapid=1) from mobile 00:40:96:af:3e:93 Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93` **`Received Identity Response (count=2) from mobile 00:40:96:af:3e:93`** `Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93` **`Processing Access-Challenge for mobile 00:40:96:af:3e:93`**
`.....`
`.....`
`.....`
`..... Wed Feb 20 14:20:00 2007: 00:40:96:af:3e:93` **`Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 19, EAP Type 43)`** `Wed Feb 20 14:20:00 2007: 00:40:96:af:3e:93` **`Processing Access-Challenge for mobile 00:40:96:af:3e:93`** `Wed Feb 20 14:20:00 2007: 00:40:96:af:3e:93` **`Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 20)`** `Wed Feb 20 14:20:01 2007: 00:40:96:af:3e:93` **`Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 20, EAP Type 43)`** `Wed Feb 20`

14:20:29 2007: Creating dot1x interface with key 00:0b:85:91:c3:c0 -0 Wed Feb 20 14:20:29 2007: Resetting the group key timer for 3689 seconds on AP 00:0b:85:91:c3:c0 Wed Feb 20 14:20:29 2007: Creating dot1x interface with key 00:0b:85:91:c3:c0 -1 Wed Feb 20 14:20:29 2007: Resetting the group key timer for 3696 seconds on AP 00:0b:85:91:c3:c0 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received EAPOL START from mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 22) Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received Identity Response (count=3) from mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 WARNING: updated EAP-Identifer 22 ===> 19 for STA 00:40:96:af:3e:93 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 19) Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 19, EAP Type 3) Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 20) Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 20, EAP Type 43) Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 21) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 21, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 22) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 22, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 23) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 23, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 24) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 24, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 25) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 25, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 26) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 26, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 27) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 27, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Reject for mobile00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Failure to mobile 00:4096:af:3e:93 (EAP Id 27) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Setting quiet timer for 5 seconds for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 1) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 1) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAPOL START from mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 2) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received Identity Response (count=2) from mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 WARNING: updated EAP-Identifer 2 ===> 20 for STA 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 20) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 20, EAP Type 3) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 21) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 21, EAP Type 43) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 22) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93

```
(EAP Id 22, EAP Type 43) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-
Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 WARNING:
updated EAP-Identifer 22 ===> 24 for STA 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007:
00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 24) Wed
Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93
(EAP Id 24, EAP Type 43) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-
Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending
EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 25) Wed Feb 20 14:20:32 2007:
00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 25, EAP Type
43) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Accept for mobile
00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Creating a new PMK Cache Entry
for tation 00:40:96:af:3e:93 (RSN 0) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending
EAP-Success to mobile 00:40:96:af:3e:93 (EAP Id 25) Wed Feb 20 14:20:32 2007:
00:40:96:af:3e:93 Sending default RC4 key to mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32
2007: 00:40:96:af:3e:93 Sending Key-Mapping RC4 key to mobile 00:40:96:af:3e:93 Wed Feb 20
14:20:32 2007: 00:40:96:af:3e:93 Received Auth Success while in Authenticating state for
mobile 00:40:96:af:3e:93
```

- **debugar o pacote do dot1x permitem** — Permite debugar de mensagens de pacote do 802.1x.
- **debugar eventos aaa permitem** — Permite o resultado do debug de todos os eventos aaa.

Informações Relacionadas

- WPA2 - Acesso protegido por wi-fi 2
- Autenticação EAP-FAST com exemplo de configuração dos controladores e do servidor de raio externo do Wireless LAN
- Autenticação de EAP com exemplo de configuração dos controladores de WLAN (WLC)
- Visão Geral da Configuração do WPA
- Suporte de produtos Wireless
- Suporte Técnico e Documentação - Cisco Systems