

WPA (Wi-Fi Protected Access) em um Exemplo de Configuração de Rede Wireless Unificada da Cisco

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Suporte a WPA e WPA2](#)

[Instalação de rede](#)

[Configurar os dispositivos para o modo empresarial WPA2](#)

[Configurar a WLC para autenticação RADIUS através de um servidor RADIUS externo](#)

[Configurar a WLAN para o Modo de Operação WPA2 Enterprise](#)

[Configurar o servidor RADIUS para a autenticação do modo empresarial WPA2 \(EAP-FAST\)](#)

[Configurar o cliente sem fio para o modo de operação WPA2 Enterprise](#)

[Configure os dispositivos para o modo WPA2-Personal](#)

[Troubleshoot](#)

[Informações Relacionadas](#)

Introduction

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

Prerequisites

Requirements

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

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

Componentes Utilizados

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

- Pontos de acesso Lightweight (LAP) Cisco 1000 Series
- Controladora de LAN sem fio (WLC) Cisco 4404 com firmware 4.2.61.0
- Adaptador cliente Cisco 802.11a/b/g com firmware 4.1
- Aironet Desktop Utility (ADU) que executa o firmware versão 4.1
- Servidor Cisco Secure ACS versão 4.1

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](#).

Suporte a WPA e WPA2

O Cisco Unified Wireless Network inclui suporte para as certificações WPA e WPA2 da Wi-Fi Alliance. A WPA foi introduzida pela Wi-Fi Alliance em 2003. A WPA2 foi introduzida pela Wi-Fi Alliance em 2004. Todos os produtos com certificação Wi-Fi para WPA2 precisam ser interoperáveis com os produtos com certificação Wi-Fi para WPA.

A WPA e a WPA2 oferecem um alto nível de garantia para usuários finais e administradores de rede de que seus dados permanecerão privados e de que o acesso a suas redes será restrito a usuários autorizados. Ambos têm modos de operação pessoais e corporativos que atendem às necessidades distintas dos dois segmentos de mercado. O Modo Empresarial de cada um usa IEEE 802.1X e EAP para autenticação. O modo pessoal de cada um usa a chave pré-compartilhada (PSK) para a autenticação. A Cisco não recomenda o Modo Pessoal para implantações empresariais ou governamentais porque ele usa uma PSK para autenticação de usuário. A PSK não é segura para ambientes corporativos.

A WPA aborda todas as vulnerabilidades WEP conhecidas na implementação de segurança IEEE 802.11 original, trazendo uma solução de segurança imediata para as WLANs em ambientes corporativos e de pequenos escritórios/escritórios residenciais (SOHO). A WPA usa TKIP para criptografia.

A WPA2 é a próxima geração de segurança Wi-Fi. É a implementação interoperável da Wi-Fi Alliance do padrão IEEE 802.11i ratificado. Ele implementa o algoritmo de criptografia AES recomendado pelo National Institute of Standards and Technology (NIST) usando o Counter Mode com o Cipher Block Chaining Message Authentication Code Protocol (CCMP). O WPA2 facilita a conformidade com FIPS 140-2 do governo.

Comparação dos tipos de modo WPA e WPA2

	WPA	WPA2
Modo corporativo (empresarial, governamental, educacional)	<ul style="list-style-type: none">• Autenticação: IEEE 802.1X/E AP• Criptograf	<ul style="list-style-type: none">• Autenticação: IEEE 802.1X/E AP

	ia: TKIP/MIC	• Criptografia: AES-CCMP
Modo pessoal (SOHO, Início/Pessoal)	• Autenticação: PSK • Criptografia: TKIP/MIC	• Autenticação: PSK • Criptografia: AES-CCMP

No modo de operação empresarial, a WPA e a WPA2 usam 802.1X/EAP para autenticação. O 802.1X fornece às WLANs uma autenticação forte e mútua entre um cliente e um servidor de autenticação. Além disso, o 802.1X fornece chaves de criptografia dinâmicas por usuário e por sessão, eliminando a carga administrativa e os problemas de segurança relacionados às chaves de criptografia estáticas.

Com o 802.1X, as credenciais usadas para autenticação, como senhas de logon, nunca são transmitidas sem criptografia, ou sem criptografia, pelo meio sem fio. Embora os tipos de autenticação 802.1X forneçam autenticação forte para LANs sem fio, o TKIP ou o AES são necessários para criptografia, além do 802.1X, já que a criptografia WEP 802.11 padrão é vulnerável a ataques de rede.

Existem vários tipos de autenticação 802.1X, cada um fornecendo uma abordagem diferente para a autenticação, contando com a mesma estrutura e EAP para comunicação entre um cliente e um ponto de acesso. Os produtos Cisco Aironet suportam mais tipos de autenticação EAP 802.1X do que qualquer outro produto WLAN. Os tipos suportados incluem:

- [Cisco LEAP](#)
- [Autenticação EAP flexível via encapsulamento seguro \(EAP-FAST\)](#)
- EAP-Transport Layer Security (EAP-TLS)
- [Protocolo de autenticação extensível protegido \(PEAP\)](#)
- TLS em túnel EAP (EAP-TTLS)
- EAP-Módulo de identidade do assinante (EAP-SIM)

Outro benefício da autenticação 802.1X é o gerenciamento centralizado para grupos de usuários de WLAN, incluindo rotação de chaves baseada em políticas, atribuição de chaves dinâmicas, atribuição de VLAN dinâmica e restrição de SSID. Esses recursos alternam as chaves de criptografia.

No modo Pessoal de operação, uma chave pré-compartilhada (senha) é usada para autenticação. O modo pessoal requer apenas um ponto de acesso e um dispositivo cliente, enquanto o modo empresarial normalmente requer um RADIUS ou outro servidor de autenticação na rede.

Este documento fornece exemplos para a configuração de WPA2 (modo Empresarial) e WPA2-PSK (modo Pessoal) em uma rede Cisco Unified Wireless.

[Instalação de rede](#)

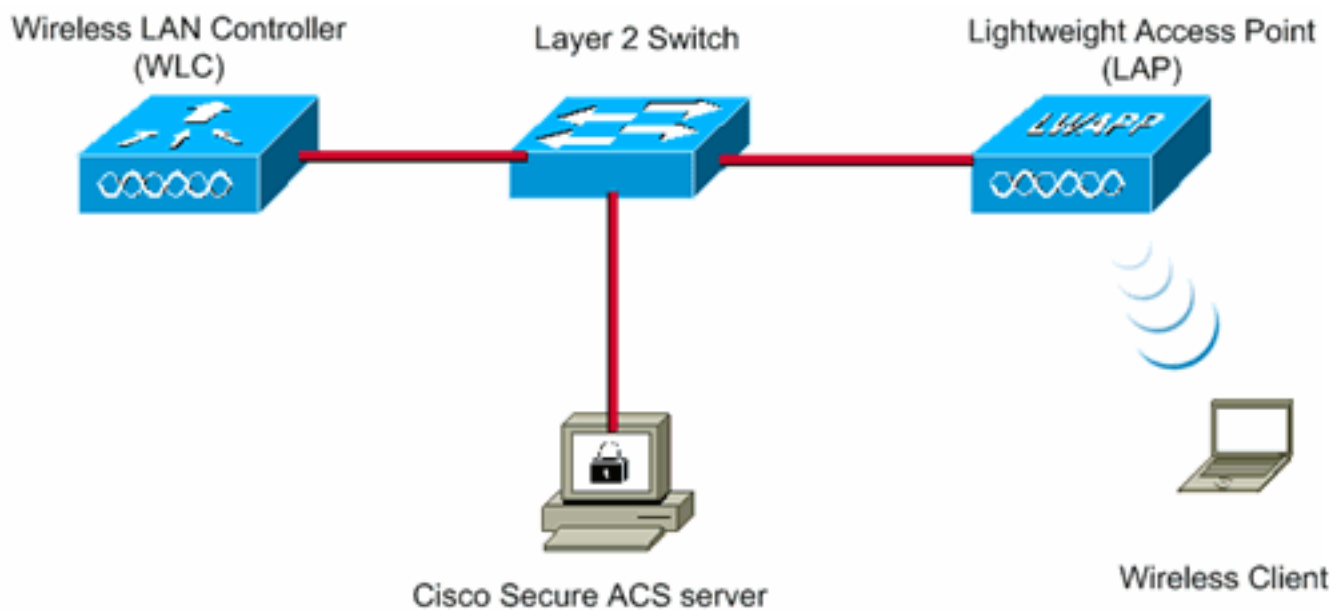
Nesta configuração, uma WLC Cisco 4404 e um LAP Cisco 1000 Series são conectados através de um Switch de Camada 2. Um servidor RADIUS externo (Cisco Secure ACS) também está conectado ao mesmo switch. Todos os dispositivos estão na mesma sub-rede. O ponto de acesso (LAP) é registrado inicialmente na controladora. É necessário criar duas LANs sem fio, uma para

o modo WPA2 Enterprise e outra para o modo WPA2 Personal.

A WLAN do modo WPA2-Enterprise (SSID: WPA2-Enterprise) usará EAP-FAST para autenticar os clientes Wireless e o AES para criptografia. O servidor Cisco Secure ACS será usado como o servidor RADIUS externo para autenticar os clientes sem fio.

A WLAN do modo WPA2-Personal (SSID: WPA2-PSK) usará a WPA2-PSK para autenticação com a chave pré-compartilhada "abcdefghijk".

Você precisa configurar os dispositivos para esta configuração:



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 empresarial WPA2](#)

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

Execute estas etapas para configurar os dispositivos para o modo de operação WPA2 Enterprise:

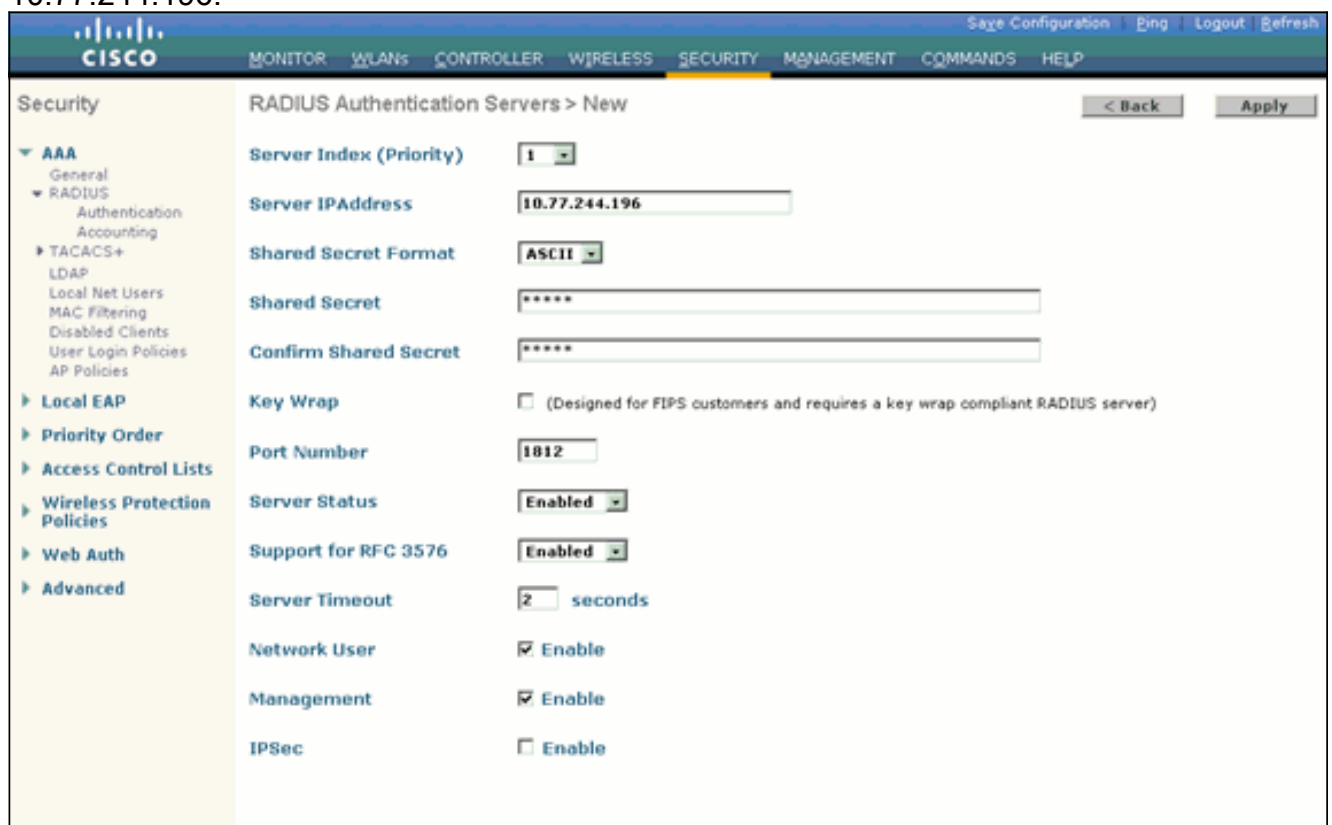
1. [Configurar a WLC para autenticação RADIUS através de um servidor RADIUS externo](#)
2. [Configurar a WLAN para a Autenticação do Modo Empresarial WPA2 \(EAP-FAST\)](#)
3. [Configurar o cliente sem fio para o modo WPA2-Enterprise](#)

[Configurar a WLC para autenticação RADIUS através de um servidor RADIUS externo](#)

A WLC precisa ser configurada para encaminhar as credenciais do usuário a um servidor RADIUS externo. O servidor RADIUS externo valida as credenciais do usuário usando EAP-FAST e fornece acesso aos clientes sem fio.

Conclua estes passos para configurar o WLC para um servidor RADIUS externo:

1. Escolha **Security** e **RADIUS Authentication** na GUI da controladora para exibir a página RADIUS Authentication Servers. Em seguida, clique em **New** para definir um servidor RADIUS.
2. Defina os parâmetros do servidor RADIUS na página **Servidores de autenticação RADIUS > Novo**. Esses parâmetros incluem: Endereço IP do servidor RADIUS, número da porta, status do servidor, suporte para RFC 3576, tempo de espera do servidor, usuário da rede, gerenciamento e IPsec. Este documento usa o servidor ACS com um endereço IP 10.77.244.196.



The screenshot shows the Cisco WLC GUI for configuring a new RADIUS Authentication Server. The navigation menu on the left includes AAA, RADIUS, TACACS+, LDAP, Local Net Users, MAC Filtering, Disabled Clients, User Login Policies, AP Policies, Local EAP, Priority Order, Access Control Lists, Wireless Protection Policies, Web Auth, and Advanced. The main content area is titled "RADIUS Authentication Servers > New" and contains the following configuration fields:

Server Index (Priority)	1
Server IP Address	10.77.244.196
Shared Secret Format	ASCII
Shared Secret	*****
Confirm Shared Secret	*****
Key Wrap	<input type="checkbox"/> (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number	1812
Server Status	Enabled
Support for RFC 3576	Enabled
Server Timeout	2 seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input checked="" type="checkbox"/> Enable
IPsec	<input type="checkbox"/> Enable

3. Clique em **Apply**.

[Configurar a WLAN para o Modo de Operação WPA2 Enterprise](#)

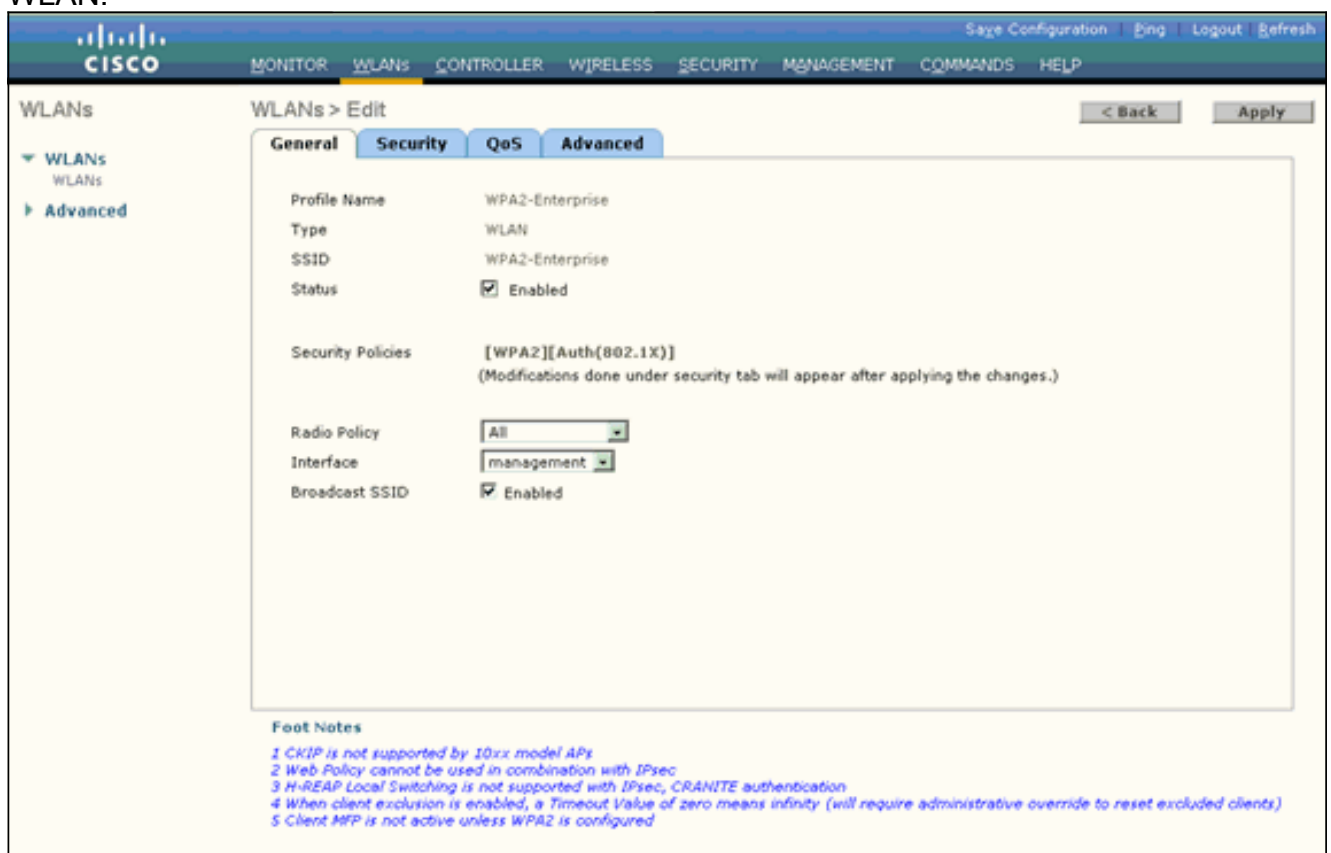
Em seguida, configure a WLAN que os clientes usarão para se conectar à rede sem fio. O SSID da WLAN para o modo WPA2-Empresa será WPA2-Empresa. Este exemplo atribui esta WLAN à interface de gerenciamento.

Conclua estes passos para configurar a WLAN e seus parâmetros relacionados:

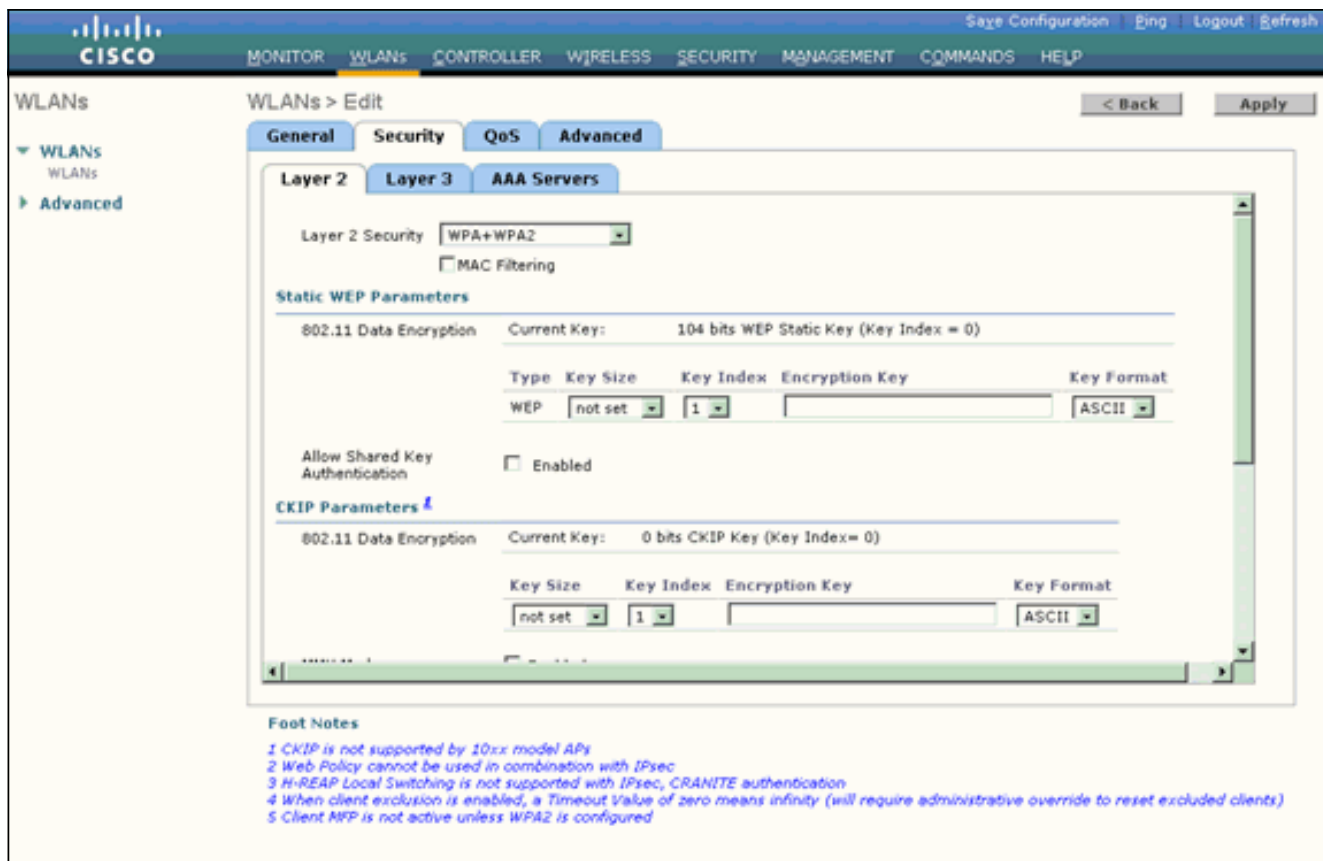
1. Clique em **WLANs** na GUI do controlador para exibir a página WLANs. Esta página lista as WLANs que existem na controladora.
2. Clique em **New** para criar uma nova WLAN.
3. Insira o nome SSID da WLAN e o nome do perfil na página **WLANs > New**. Em seguida, clique em **Apply**. Este exemplo usa **WPA2-Enterprise** como o SSID.



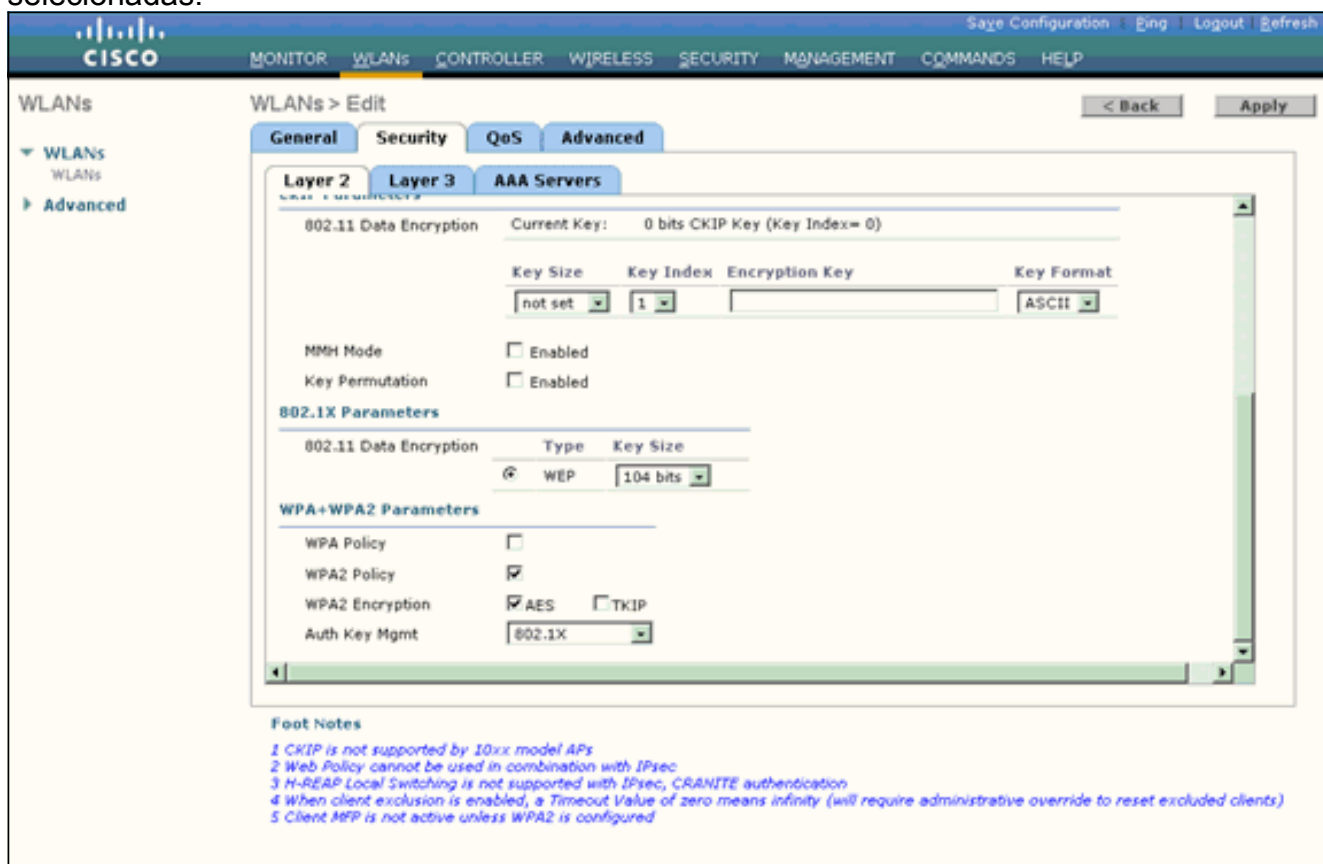
4. Quando você criar uma nova WLAN, a página **WLAN > Edit** da nova WLAN será exibida. Nesta página, você pode definir vários parâmetros específicos para esta WLAN. Isso inclui políticas gerais, políticas de segurança, políticas de QoS e parâmetros avançados.
5. Em General Policies (Regras gerais), marque a caixa de seleção **Status** para habilitar a WLAN.



6. Se você quiser que o AP transmita o SSID em seus quadros beacon, marque a caixa de seleção **SSID de broadcast**.
7. Clique na guia Security. Em Layer 2 Security, selecione **WPA+WPA2**. Isso ativa a autenticação WPA para a WLAN.



8. Role a página para baixo para modificar os parâmetros WPA+WPA2. Neste exemplo, a política WPA2 e a criptografia AES estão selecionadas.



9. Em Auth Key Mgmt, selecione 802.1x. Isso habilita a WPA2 usando a autenticação 802.1x/EAP e a criptografia AES para a WLAN.

10. Clique na guia Servidores AAA. Em Authentication Servers, escolha o endereço IP do servidor apropriado. Neste exemplo, 10.77.244.196 é usado como o servidor

RADIUS.

The screenshot shows the Cisco WLAN configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', and 'HELP'. The main content area is titled 'WLANs > Edit' and has tabs for 'General', 'Security', 'QoS', and 'Advanced'. Under the 'Advanced' tab, there are sub-tabs for 'Layer 2', 'Layer 3', and 'AAA Servers'. The 'AAA Servers' tab is active, showing a section for 'Select AAA servers below to override use of default servers on this WLAN'. This section is divided into 'Radius Servers' and 'LDAP Servers'. Under 'Radius Servers', there are columns for 'Authentication Servers' and 'Accounting Servers'. 'Server 1' is configured with 'IP:10.77.244.196, Port:1812' for authentication and 'None' for accounting. 'Server 2' and 'Server 3' are both set to 'None'. There is a checkbox for 'Enabled' which is checked. Under 'LDAP Servers', 'Server 1', 'Server 2', and 'Server 3' are all set to 'None'. Below the server configuration is a section for 'Local EAP Authentication' with a checkbox for 'Enabled' which is unchecked. At the bottom, there are 'Foot Notes' with five numbered items.

Foot Notes

- 1 CRIP is not supported by 10xx model APs
- 2 Web Policy cannot be used in combination with IPsec
- 3 H-REAP Local Switching is not supported with IPsec, CRANITE authentication
- 4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
- 5 Client MFP is not active unless WPA2 is configured

11. Clique em Apply. **Observação:** essa é a única configuração EAP que precisa ser configurada na controladora para autenticação EAP. Todas as outras configurações específicas do EAP-FAST precisam ser feitas no servidor RADIUS e nos clientes que precisam ser autenticados.

[Configurar o servidor RADIUS para a autenticação do modo empresarial WPA2 \(EAP-FAST\)](#)

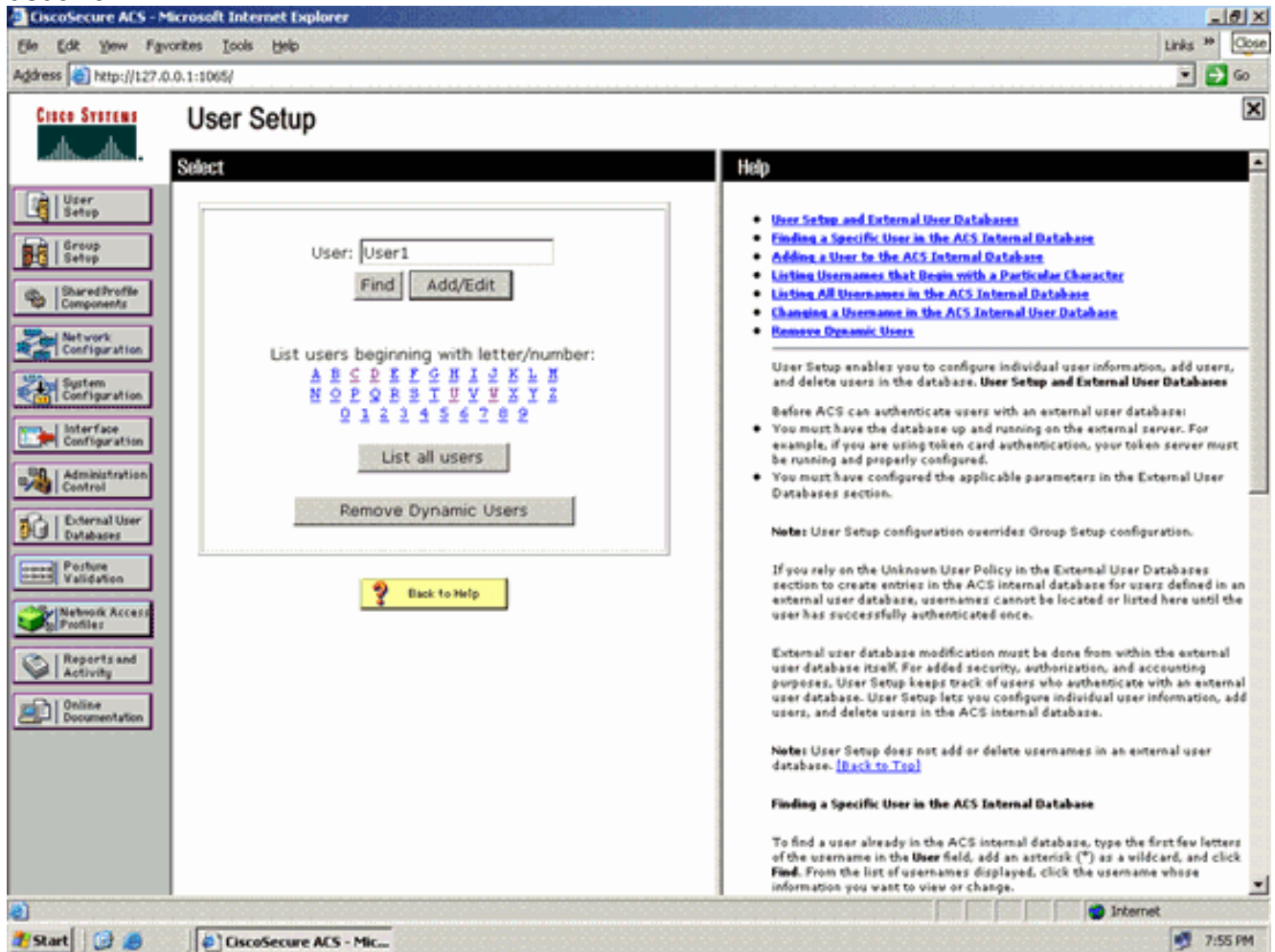
Neste exemplo, o Cisco Secure ACS é usado como o servidor RADIUS externo. Execute estas etapas para configurar o servidor RADIUS para autenticação EAP-FAST:

1. [Crie um banco de dados de usuário para autenticar clientes](#)
2. [Adicione a WLC como AAA Client ao servidor RADIUS](#)
3. [Configurar a autenticação EAP-FAST no servidor RADIUS com o provisionamento de PAC anônimo em banda](#) **Observação:** o EAP-FAST pode ser configurado com o Provisionamento de PAC In-band anônimo ou Provisionamento de PAC In-band autenticado. Este exemplo usa o Provisionamento PAC Anônimo In-band. Para obter informações detalhadas e exemplos sobre como configurar o EAP FAST com Provisionamento PAC In-band Anônimo e Provisionamento In-band Autenticado, consulte [Autenticação EAP-FAST com Controladoras Wireless LAN e Exemplo de Configuração de Servidor RADIUS Externo](#).

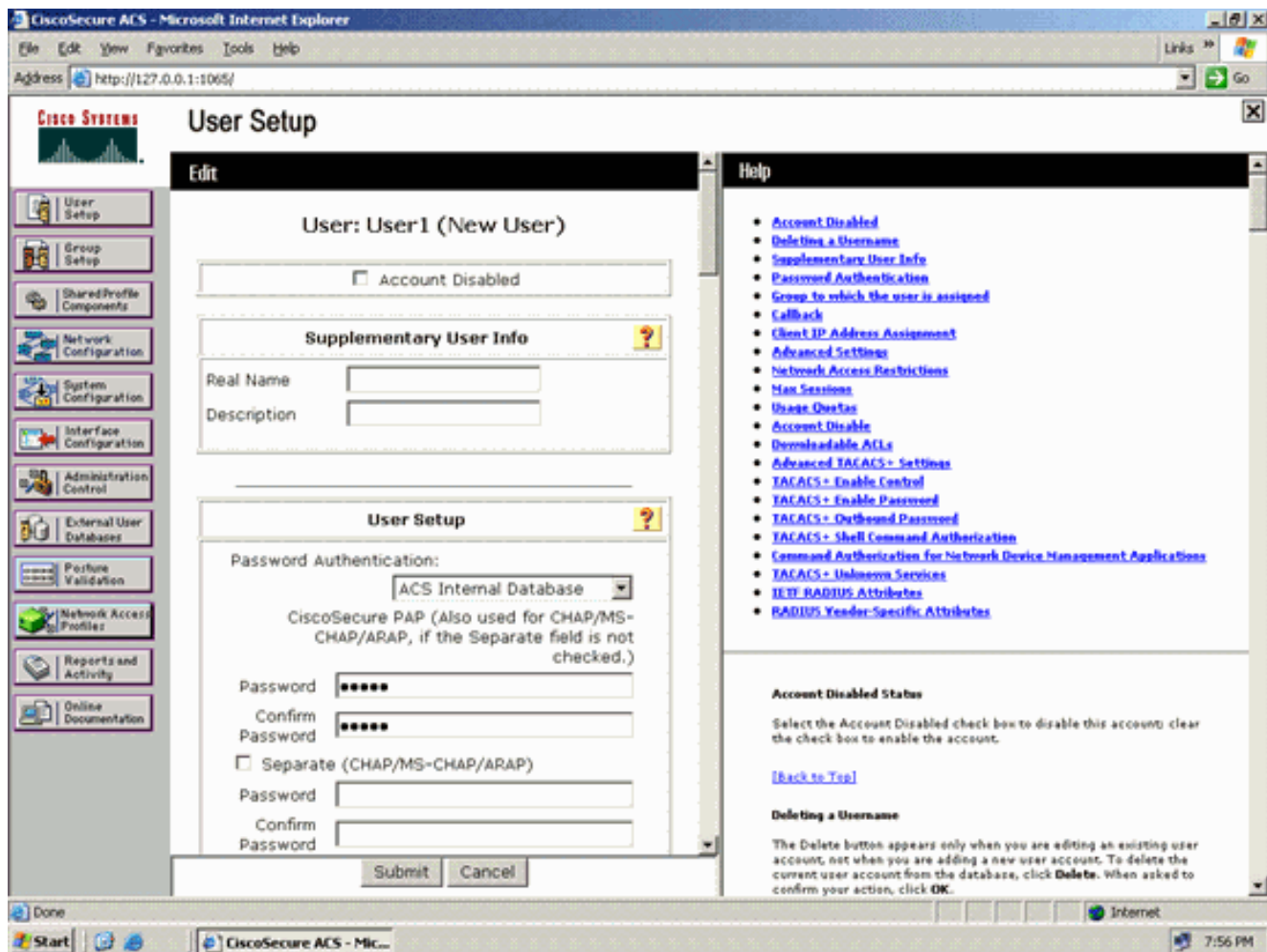
[Crie um banco de dados de usuário para autenticar clientes EAP-FAST](#)

Conclua estas etapas para criar um banco de dados de usuário para clientes EAP-FAST no ACS. Este exemplo configura o nome de usuário e a senha do cliente EAP-FAST como User1 e User1, respectivamente.

1. Na GUI do ACS na barra de navegação, selecione **User Setup**. Crie um novo usuário sem fio e clique em **Add/Edit** para ir para a página Edit deste usuário.



2. Na página User Setup Edit, configure Real Name e Description, bem como as configurações de Password, conforme mostrado neste exemplo. Este documento usa o **banco de dados interno do ACS** para autenticação de senha.

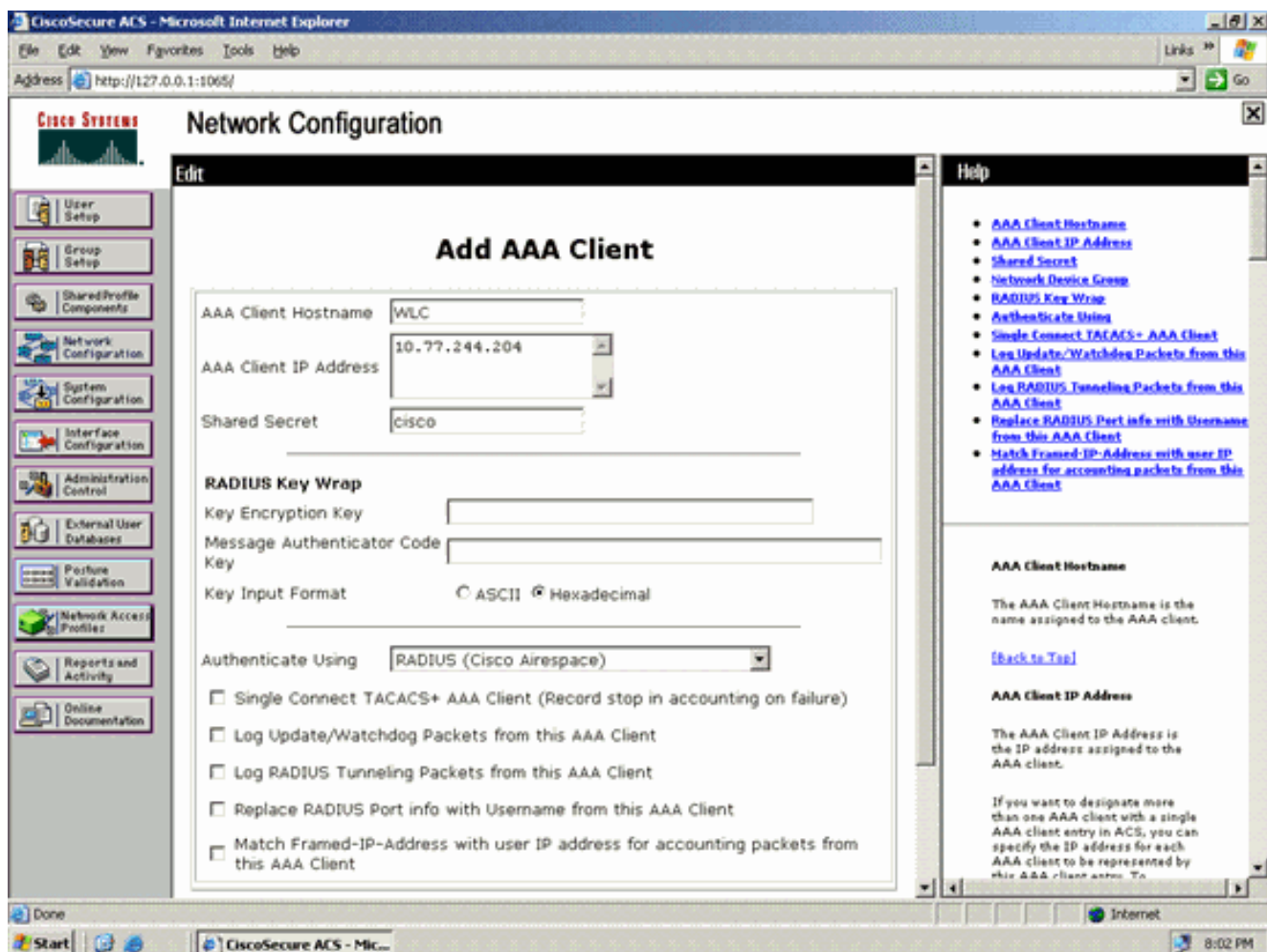


3. Escolha **ACS Internal Database** na caixa suspensa Password Authentication.
4. Configure todos os outros parâmetros necessários e clique em **Enviar**.

[Adicione a WLC como AAA Client ao servidor RADIUS](#)

Conclua estas etapas para definir o controlador como um cliente AAA no servidor ACS:

1. Clique em **Network Configuration** na GUI do ACS. Na seção Add AAA client da página Network Configuration, clique em **Add Entry** para adicionar a WLC como o cliente AAA ao servidor RADIUS.
2. Na página AAA Client, defina o nome da WLC, o endereço IP, o segredo compartilhado e o método de autenticação (RADIUS/Cisco Airespace). Consulte a documentação do fabricante para outros servidores de autenticação não ACS.



Observação: a chave secreta compartilhada que você configura no WLC e no servidor ACS deve corresponder. O segredo compartilhado diferencia maiúsculas de minúsculas.

3. Clique em **Enviar e aplicar**.

[Configurar a autenticação EAP-FAST no servidor RADIUS com o provisionamento de PAC anônimo em banda](#)

Provisionamento anônimo em banda

Este é um dos dois métodos de provisionamento em banda em que o ACS estabelece uma conexão segura com o cliente usuário final com a finalidade de fornecer ao cliente uma nova PAC. Essa opção permite um handshake TLS anônimo entre o cliente do usuário final e o ACS.

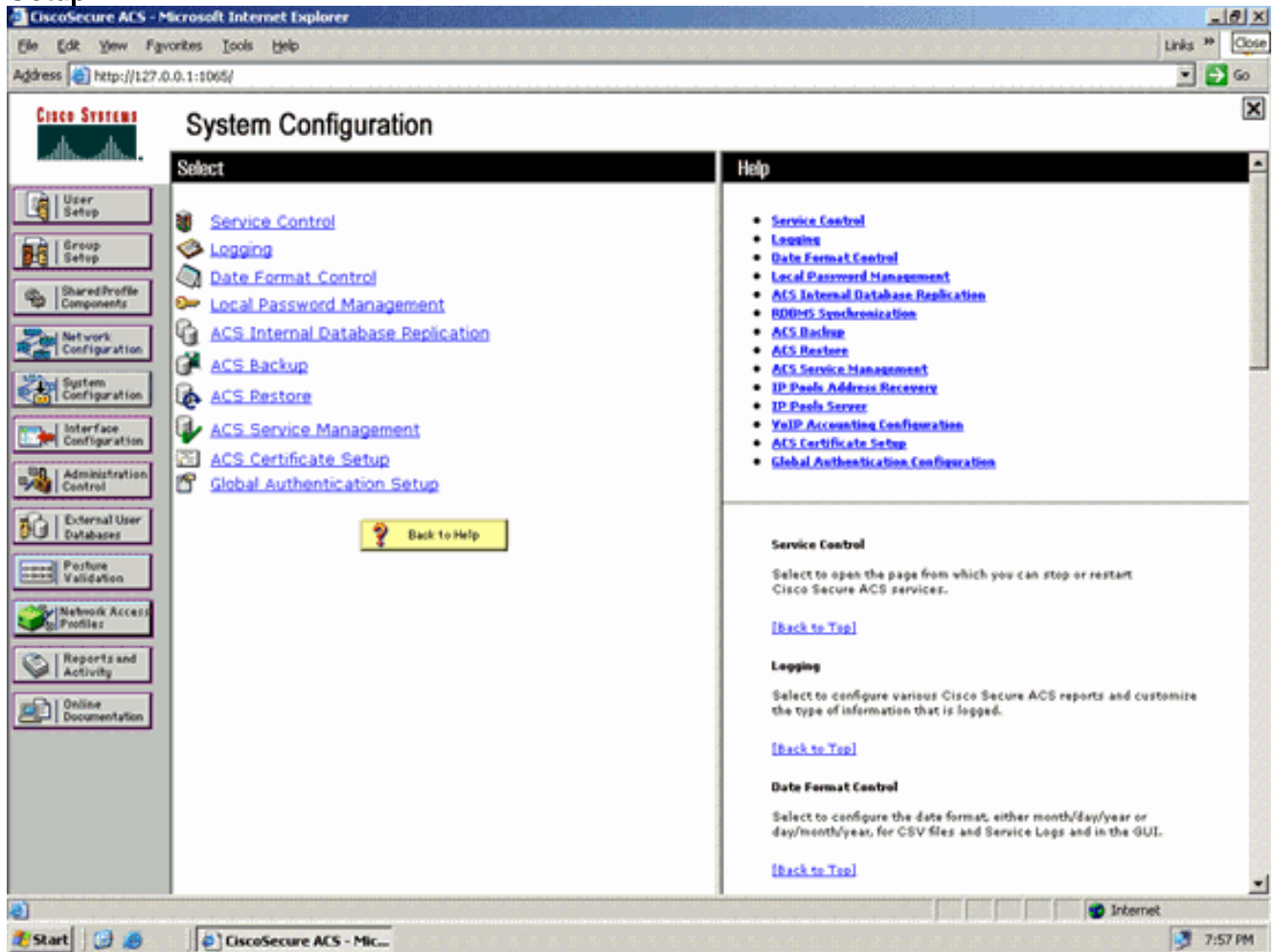
Este método opera dentro de um túnel do protocolo de acordo Diffie-HellmanKey (ADHP) autenticado antes que o peer autentique o servidor ACS.

Em seguida, o ACS requer a autenticação EAP-MS-CHAPv2 do usuário. Na autenticação de usuário bem-sucedida, o ACS estabelece um túnel Diffie-Hellman com o cliente de usuário final. O ACS gera uma PAC para o usuário e a envia ao cliente usuário final nesse túnel, juntamente com informações sobre esse ACS. Esse método de provisionamento usa EAP-MSCHAPv2 como o método de autenticação na fase zero e EAP-GTC na fase dois.

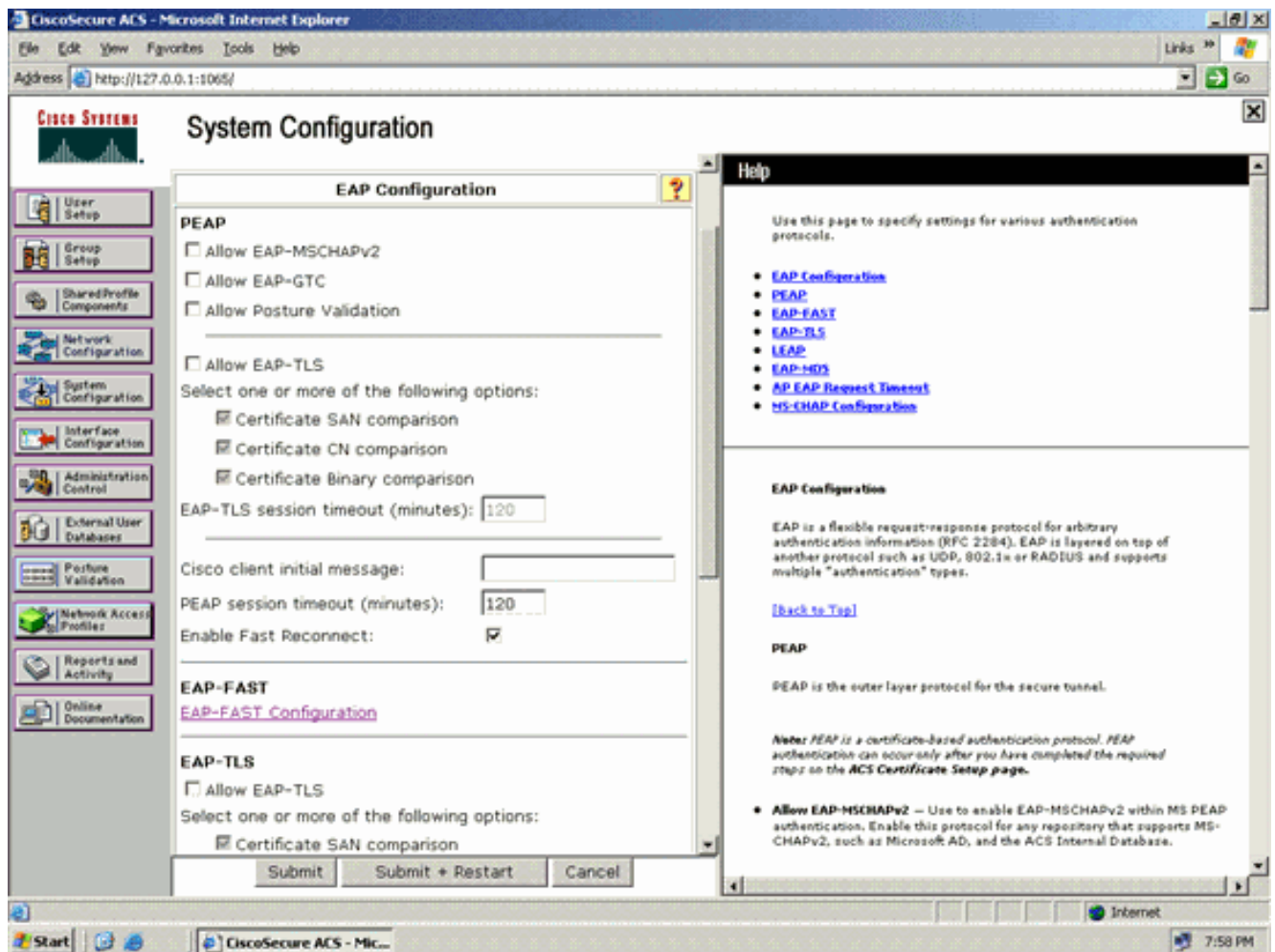
Como um servidor não autenticado é provisionado, não é possível usar uma senha de texto simples. Portanto, somente as credenciais MS-CHAP podem ser usadas dentro do túnel. O MS-CHAPv2 é usado para provar a identidade do par e receber uma PAC para outras sessões de autenticação (EAP-MS-CHAP será usado apenas como método interno).

Conclua estas etapas para configurar a autenticação EAP-FAST no servidor RADIUS para provisionamento anônimo em banda:

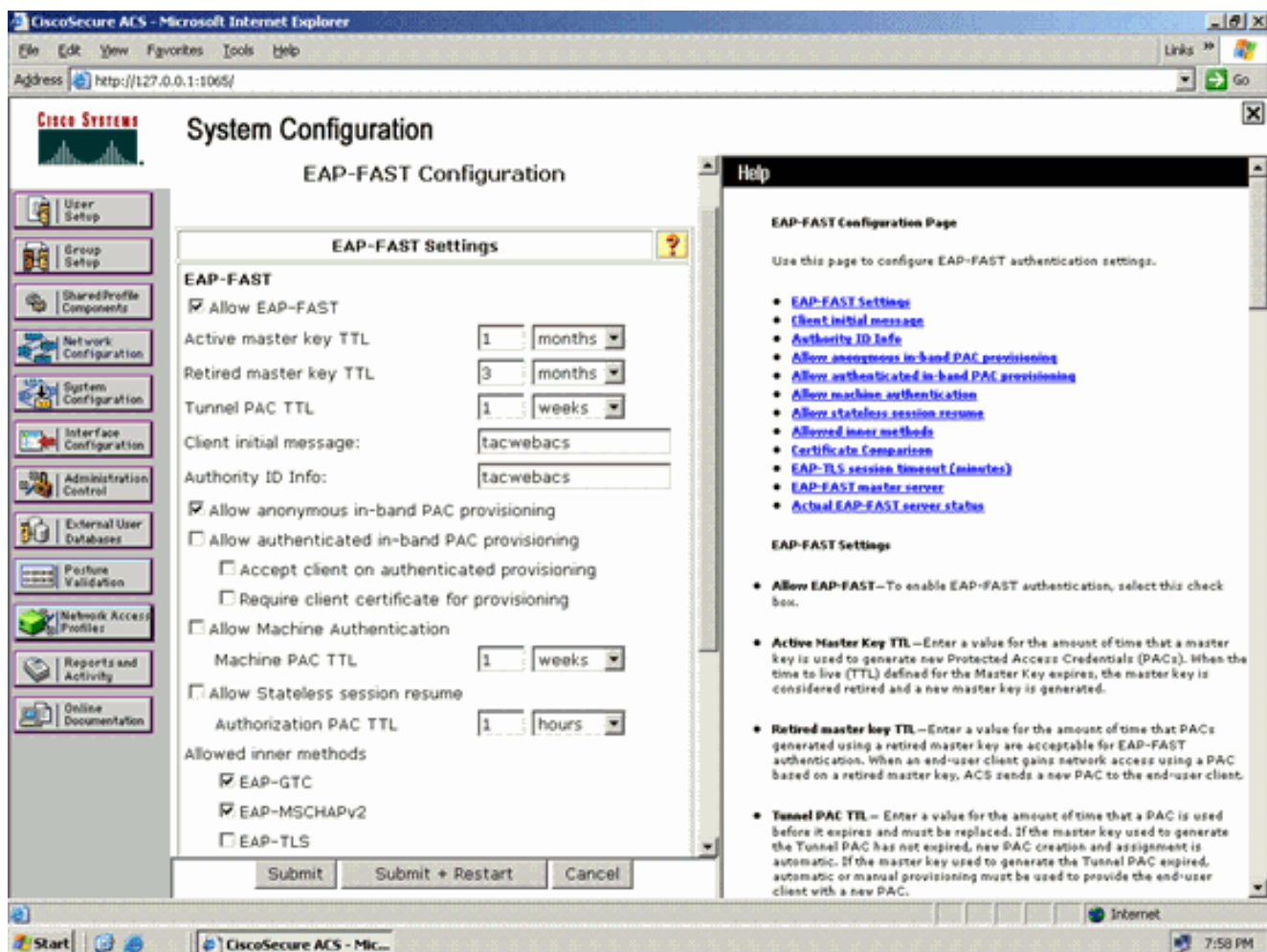
1. Clique em **System Configuration** na GUI do servidor RADIUS. Na página System Configuration, escolha **Global Authentication Setup**.



2. Na página de configuração Autenticação global, clique em **Configuração EAP-FAST** para ir para a página de configurações EAP-FAST.



3. Na página Configurações de EAP-FAST, marque a caixa de seleção **Permitir EAP-FAST** para ativar o EAP-FAST no servidor RADIUS.



4. Configure os valores TTL (Time-to-Live) da chave mestra ativa/desativada conforme desejado ou defina-a com o valor padrão conforme mostrado neste exemplo. Consulte Chaves mestre para obter informações sobre chaves mestre ativas e desativadas. Além disso, consulte Chaves mestras e TTLs PAC para obter mais informações. O campo Authority ID Info (Informações de ID da autoridade) representa a identidade textual desse servidor ACS, que um usuário final pode usar para determinar em qual servidor ACS será autenticado. O preenchimento deste campo é obrigatório. O campo Mensagem de exibição inicial do cliente especifica uma mensagem a ser enviada aos usuários que se autenticam em um cliente EAP-FAST. O comprimento máximo é de 40 caracteres. Um usuário verá a mensagem inicial apenas se o cliente do usuário final suportar a exibição.
5. Se desejar que o ACS execute o fornecimento de PAC anônimo dentro da banda, marque a caixa de seleção **Permitir fornecimento de PAC anônimo dentro da banda**.
6. **Métodos internos permitidos** — Essa opção determina quais métodos EAP internos podem ser executados dentro do túnel EAP-FAST TLS. Para provisionamento anônimo em banda, você deve habilitar EAP-GTC e EAP-MS-CHAP para compatibilidade com versões anteriores. Se você selecionar Permitir fornecimento de PAC anônimo em banda, deverá selecionar EAP-MS-CHAP (fase zero) e EAP-GTC (fase dois).

[Configurar o cliente sem fio para o modo de operação WPA2 Enterprise](#)

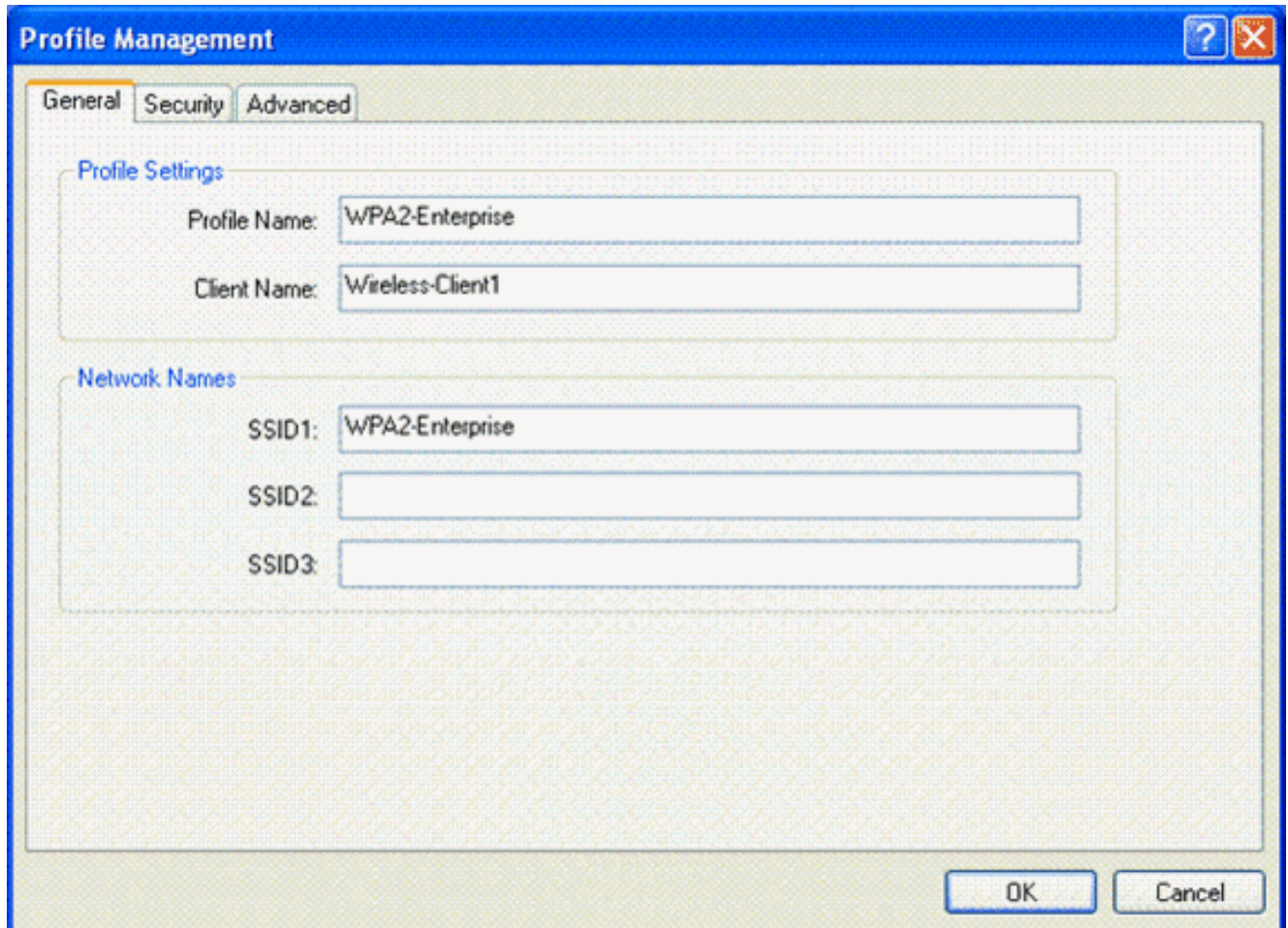
A próxima etapa é configurar o cliente sem fio para o modo de operação WPA2 Enterprise.

Conclua estas etapas para configurar o cliente sem fio para o modo WPA2 Enterprise.

1. Na janela Aironet Desktop Utility, clique em **Profile Management > New** para criar um perfil

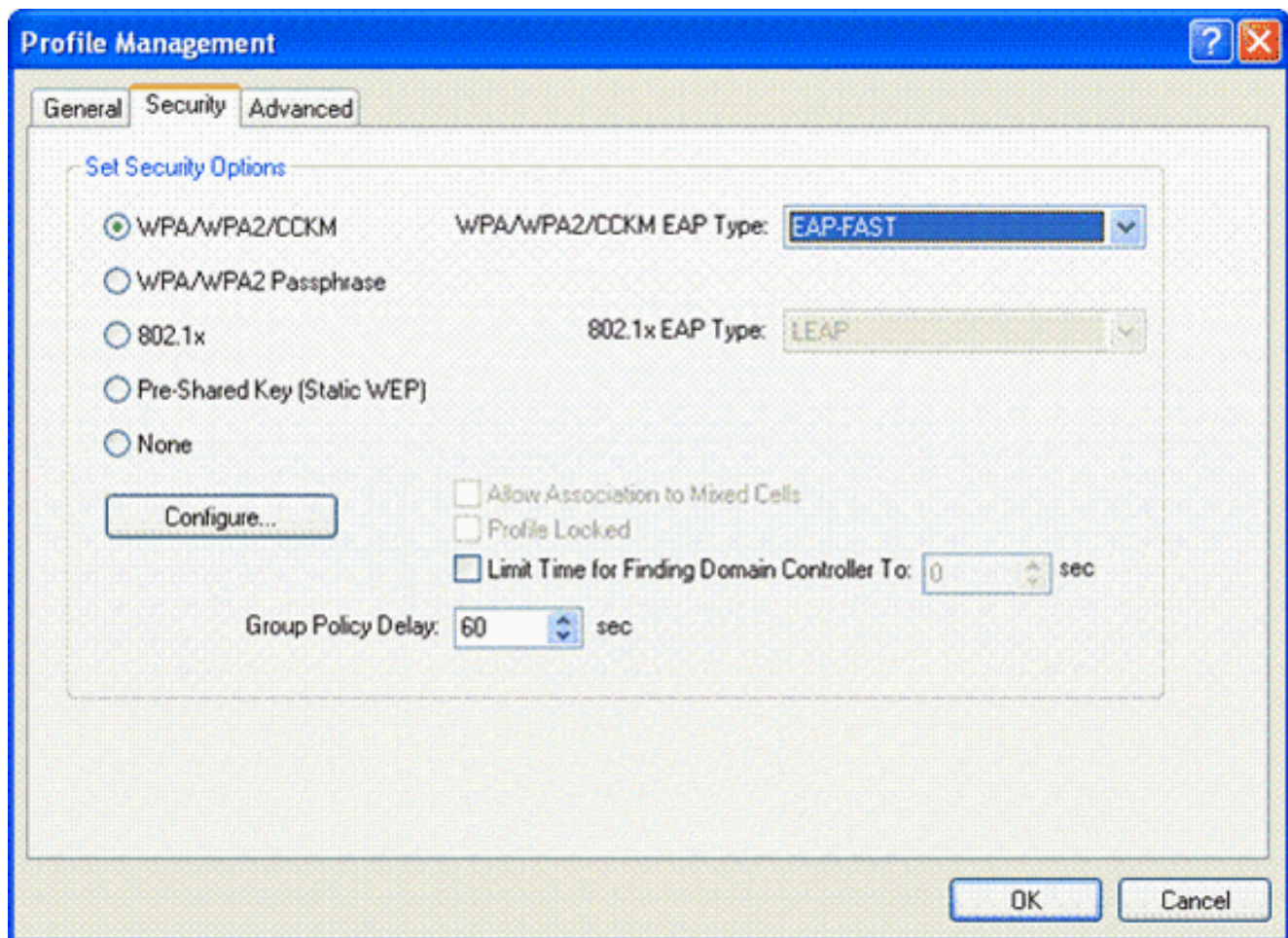
para o usuário WPA2-Enterprise WLAN. Como mencionado anteriormente, este documento usa o nome WLAN/SSID como **WPA2-Enterprise** para o cliente sem fio.

2. Na janela Gerenciamento de perfil, clique na guia **Geral** e configure o Nome do perfil, o Nome do cliente e o nome SSID como mostrado neste exemplo. Clique em **OK**

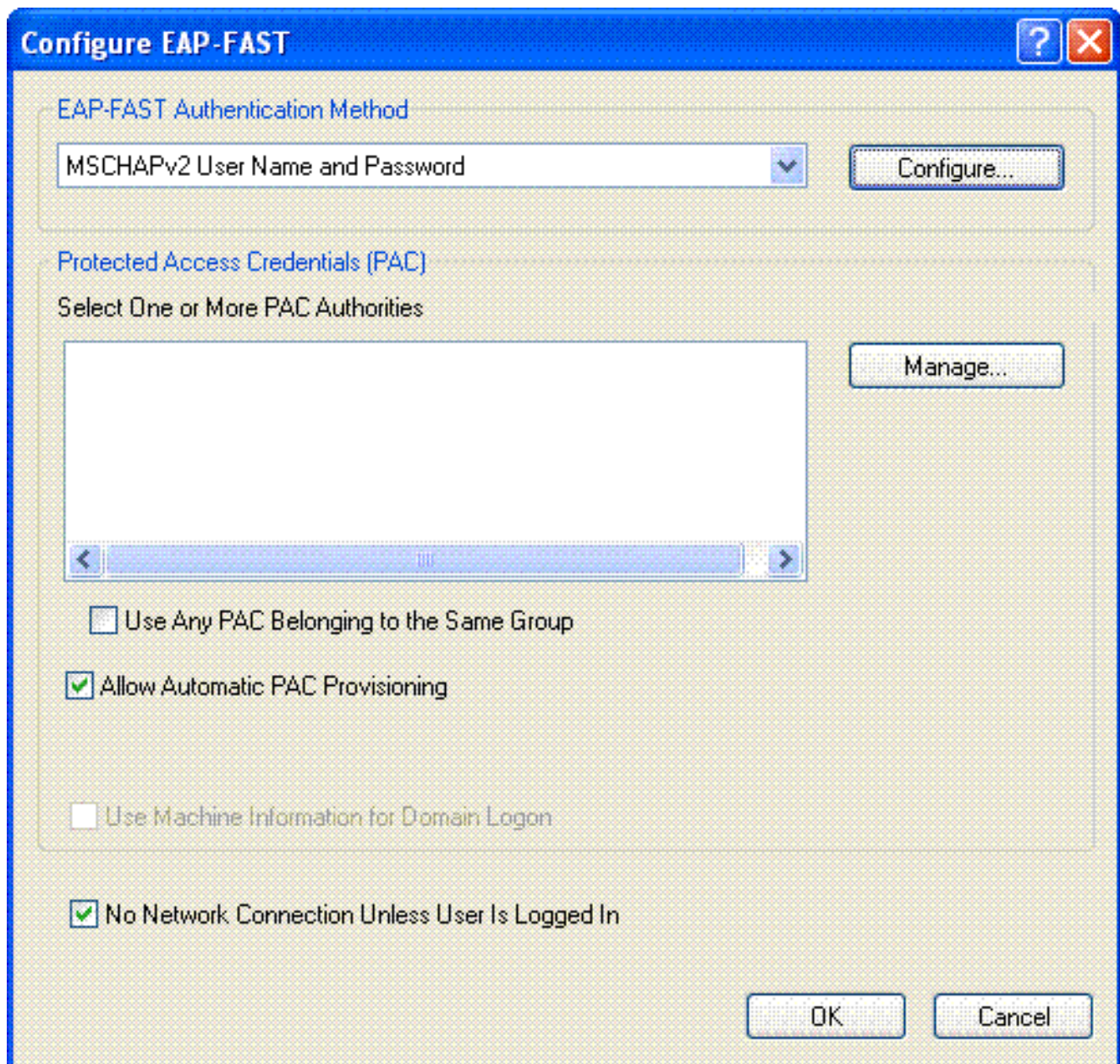


The image shows a screenshot of the 'Profile Management' dialog box, specifically the 'General' tab. The dialog has a blue title bar with a question mark and a close button. Below the title bar are three tabs: 'General', 'Security', and 'Advanced'. The 'General' tab is selected. The dialog is divided into two main sections: 'Profile Settings' and 'Network Names'. In the 'Profile Settings' section, there are two text input fields: 'Profile Name' containing 'WPA2-Enterprise' and 'Client Name' containing 'Wireless-Client1'. In the 'Network Names' section, there are three text input fields: 'SSID1' containing 'WPA2-Enterprise', 'SSID2' which is empty, and 'SSID3' which is empty. At the bottom right of the dialog are two buttons: 'OK' and 'Cancel'.

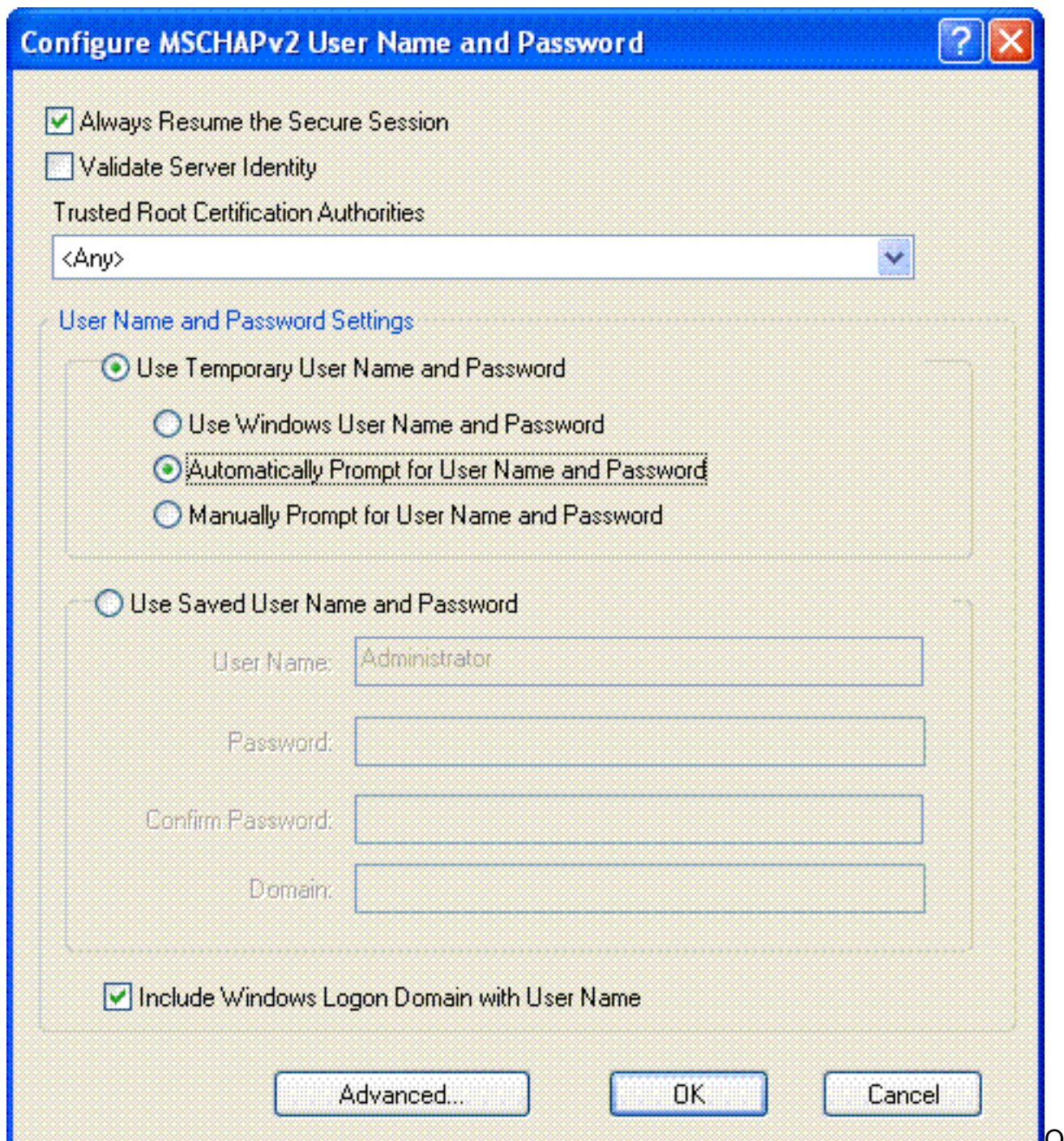
3. Clique na guia **Security** e escolha **WPA/WPA2/CCKM** para habilitar o modo de operação WPA2. Em WPA/WPA2/CCKM EAP Type, selecione **EAP-FAST**. Clique em **Configure** para definir a configuração EAP-FAST.



4. Na janela Configurar EAP-FAST, marque a caixa de seleção **Permitir Provisionamento Automático de PAC**. Se você quiser configurar o fornecimento de PAC anônimo, EAP-MS-CHAP será usado como o único método interno na fase zero.



5. Escolha Nome de usuário e Senha MSCHAPv2 como o método de autenticação na caixa suspensa Método de autenticação EAP-FAST. Clique em Configurar.
6. Na janela Configure MSCHAPv2 User Name and Password (Configurar nome de usuário e senha MSCHAPv2), escolha as configurações apropriadas de nome de usuário e senha. Este exemplo escolhe **Solicitar automaticamente o nome do usuário e a senha**.



mesmo nome de usuário e senha devem ser registrados no ACS. Como mencionado anteriormente, este exemplo usa User1 e User1 respectivamente como nome de usuário e senha. Além disso, observe que esse é um provisionamento anônimo dentro da banda. Portanto, o cliente não pode validar o certificado do servidor. É necessário verificar se a caixa de seleção Validar identidade do servidor está desmarcada.

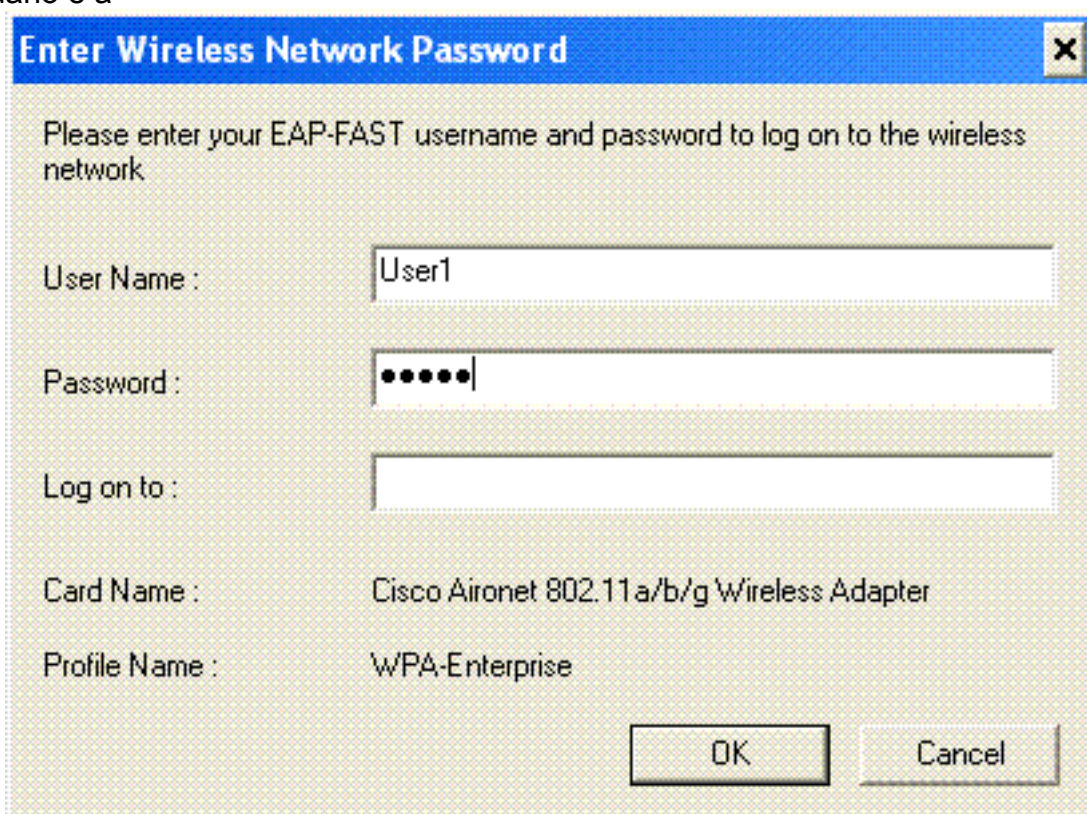
7. Click **OK**.

[Verificar o Modo de Operação do WPA2 Enterprise](#)

Conclua estas etapas para verificar se a configuração do modo WPA2 Enterprise está funcionando corretamente:

1. Na janela do Aironet Desktop Utility, selecione o perfil **WPA2-Enterprise** e clique em **Ativate** para ativar o perfil do cliente sem fio.
2. Se você tiver habilitado o MS-CHAP ver2 como sua autenticação, o cliente solicitará o nome

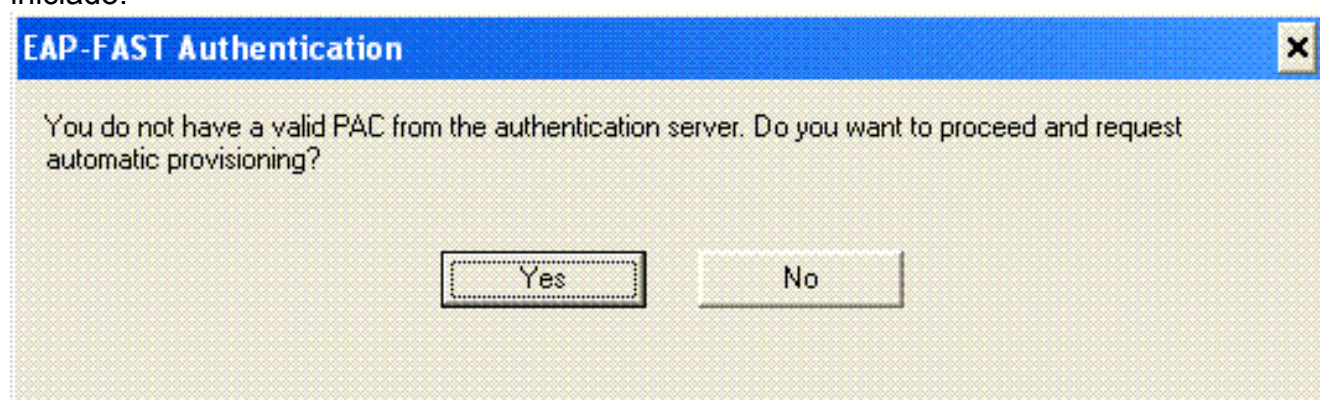
de usuário e a



The screenshot shows a dialog box titled "Enter Wireless Network Password". The text inside reads: "Please enter your EAP-FAST username and password to log on to the wireless network". There are three input fields: "User Name" containing "User1", "Password" containing six dots, and "Log on to" which is empty. Below the input fields, the "Card Name" is "Cisco Aironet 802.11 a/b/g Wireless Adapter" and the "Profile Name" is "WPA-Enterprise". At the bottom right, there are "OK" and "Cancel" buttons.

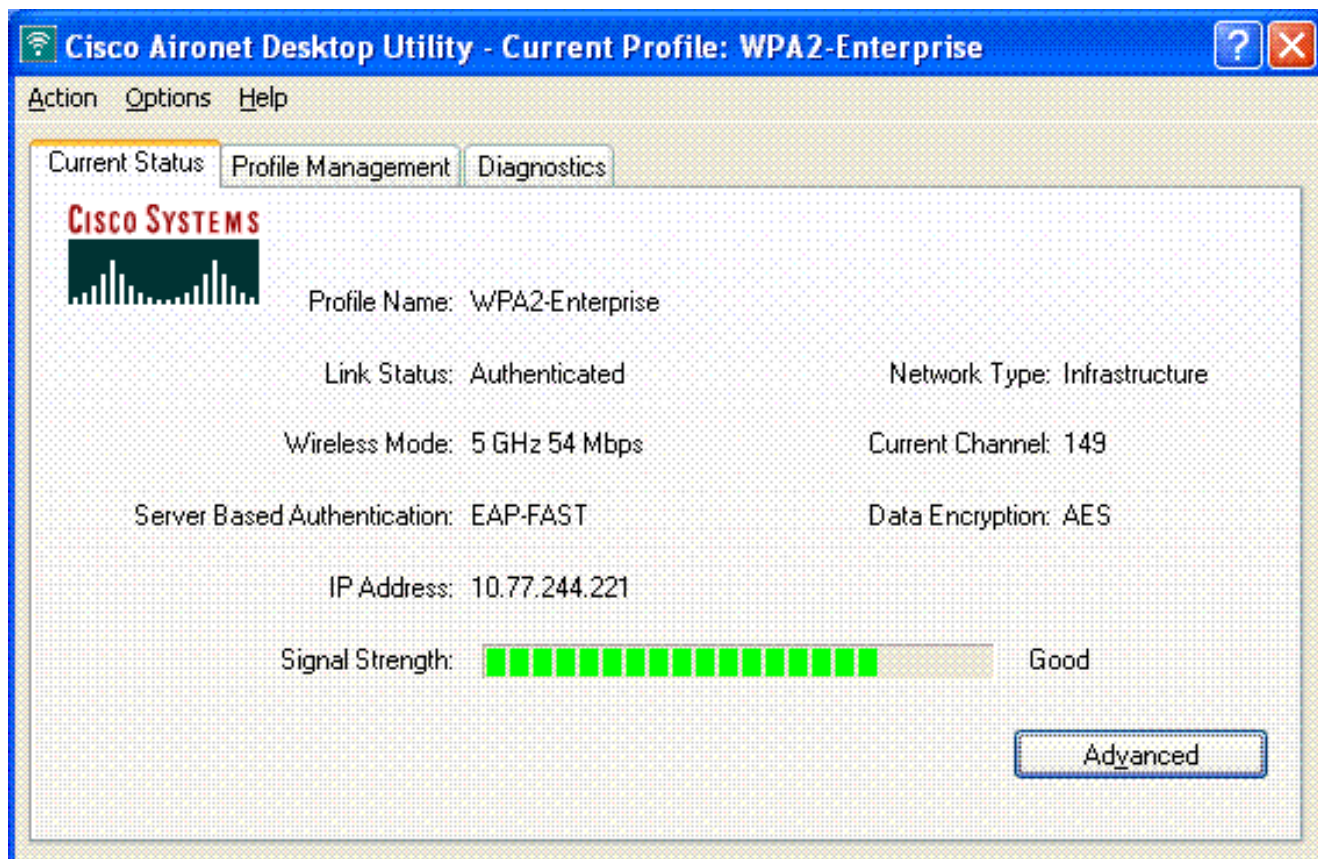
senha.

3. Durante o processamento EAP-FAST do usuário, o cliente solicitará uma PAC ao servidor RADIUS. Quando você clica em **Sim**, o fornecimento de PAC é iniciado.



The screenshot shows a dialog box titled "EAP-FAST Authentication". The text inside reads: "You do not have a valid PAC from the authentication server. Do you want to proceed and request automatic provisioning?". At the bottom, there are two buttons: "Yes" and "No".

4. Após o fornecimento bem-sucedido da PAC na fase zero, as fases um e dois são seguidas e ocorre um procedimento de autenticação bem-sucedido. Após a autenticação bem-sucedida, o cliente sem fio é associado à WLAN WPA2-Enterprise. Aqui está a captura de tela:



Você também pode verificar se o servidor RADIUS recebe e valida a solicitação de autenticação do cliente sem fio. Verifique os relatórios Passed Authentications e Failed Attempts no servidor ACS para fazer isso. Esses relatórios estão disponíveis em Relatórios e atividades no servidor ACS.

[Configure os dispositivos para o modo WPA2-Personal](#)

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

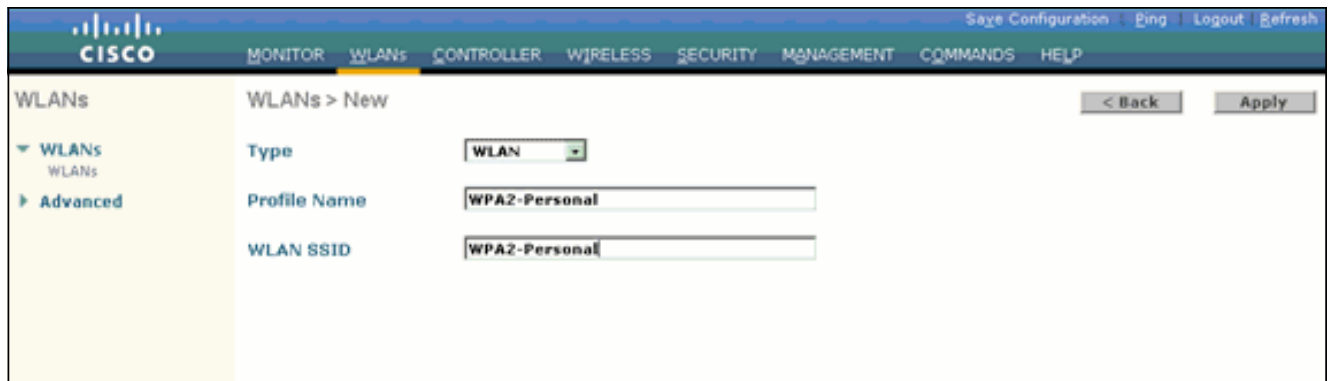
1. [Configurar a WLAN para a Autenticação do Modo WPA2-Personal](#)
2. [Configurar o cliente sem fio para o modo WPA2-Personal](#)

[Configurar a WLAN para o Modo de Operação Pessoal WPA2](#)

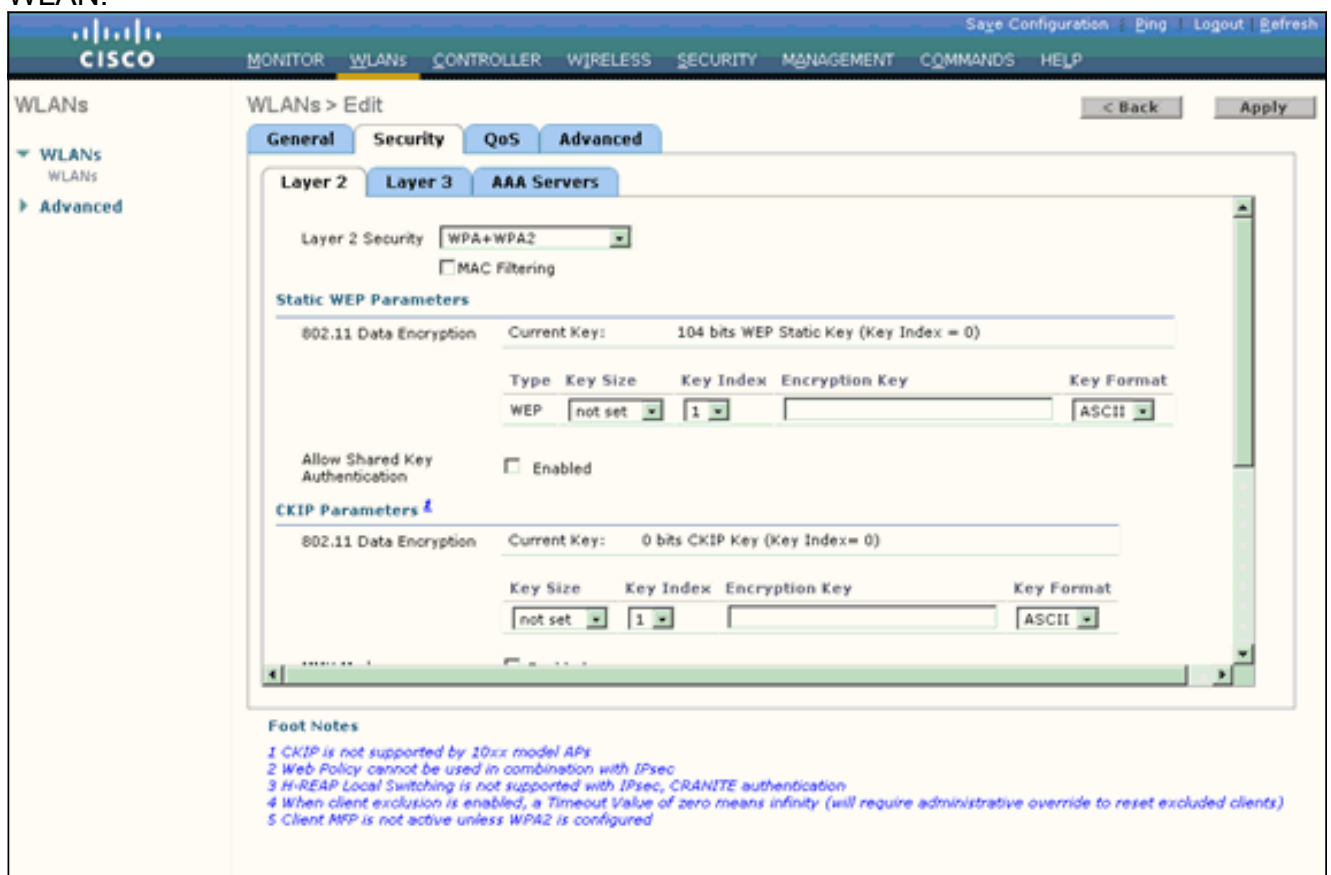
Você precisa configurar a WLAN que os clientes usarão para se conectar à rede sem fio. O SSID da WLAN para o modo WPA2-Personal será WPA2-Personal. Este exemplo atribui esta WLAN à interface de gerenciamento.

Conclua estes passos para configurar a WLAN e seus parâmetros relacionados:

1. Clique em **WLANs** na GUI do controlador para exibir a página WLANs. Esta página lista as WLANs que existem na controladora.
2. Clique em **New** para criar uma nova WLAN.
3. Insira o nome SSID da WLAN, o nome do perfil e a ID da WLAN na página WLANs > New (WLANs > Novo). Em seguida, clique em **Apply**. Este exemplo usa **WPA2-Personal** como SSID.



4. Quando você criar uma nova WLAN, a página **WLAN > Edit** da nova WLAN será exibida. Nesta página, você pode definir vários parâmetros específicos para esta WLAN. Isso inclui políticas gerais, políticas de segurança, políticas de QoS e parâmetros avançados.
5. Em General Policies (Regras gerais), marque a caixa de seleção **Status** para habilitar a WLAN.
6. Se você quiser que o AP transmita o SSID em seus quadros beacon, marque a caixa de seleção **SSID de broadcast**.
7. Clique na guia Security. Em Layer Security, escolha **WPA+WPA2**. Isso ativa a autenticação WPA para a WLAN.



8. Role a página para baixo para modificar os **parâmetros WPA+WPA2**. Neste exemplo, a política WPA2 e a criptografia AES estão selecionadas.
9. Em Auth Key Mgmt, selecione **PSK** para habilitar WPA2-PSK.
10. Insira a chave pré-compartilhada no campo apropriado, conforme mostrado.

WLANs > Edit

General Security QoS Advanced

Layer 2 Layer 3 AAA Servers

Key Size: not set Key Index: 1 Encryption Key: Key Format: ASCII

MMH Mode: Enabled
Key Permutation: Enabled

802.1X Parameters

802.11 Data Encryption	Type	Key Size
<input checked="" type="radio"/>	WEP	104 bits

WPA+WPA2 Parameters

WPA Policy:
WPA2 Policy:
WPA2 Encryption: AES TKIP
Auth Key Mgmt: PSK
PSK Format: ASCII

Foot Notes

- 1 TKIP is not supported by 10xx model APs
- 2 Web Policy cannot be used in combination with IPsec
- 3 H-REAP Local Switching is not supported with IPsec, CRANITE authentication
- 4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
- 5 Client MFP is not active unless WPA2 is configured

Observação: a chave pré-compartilhada usada no WLC deve corresponder à configurada nos clientes sem fio.

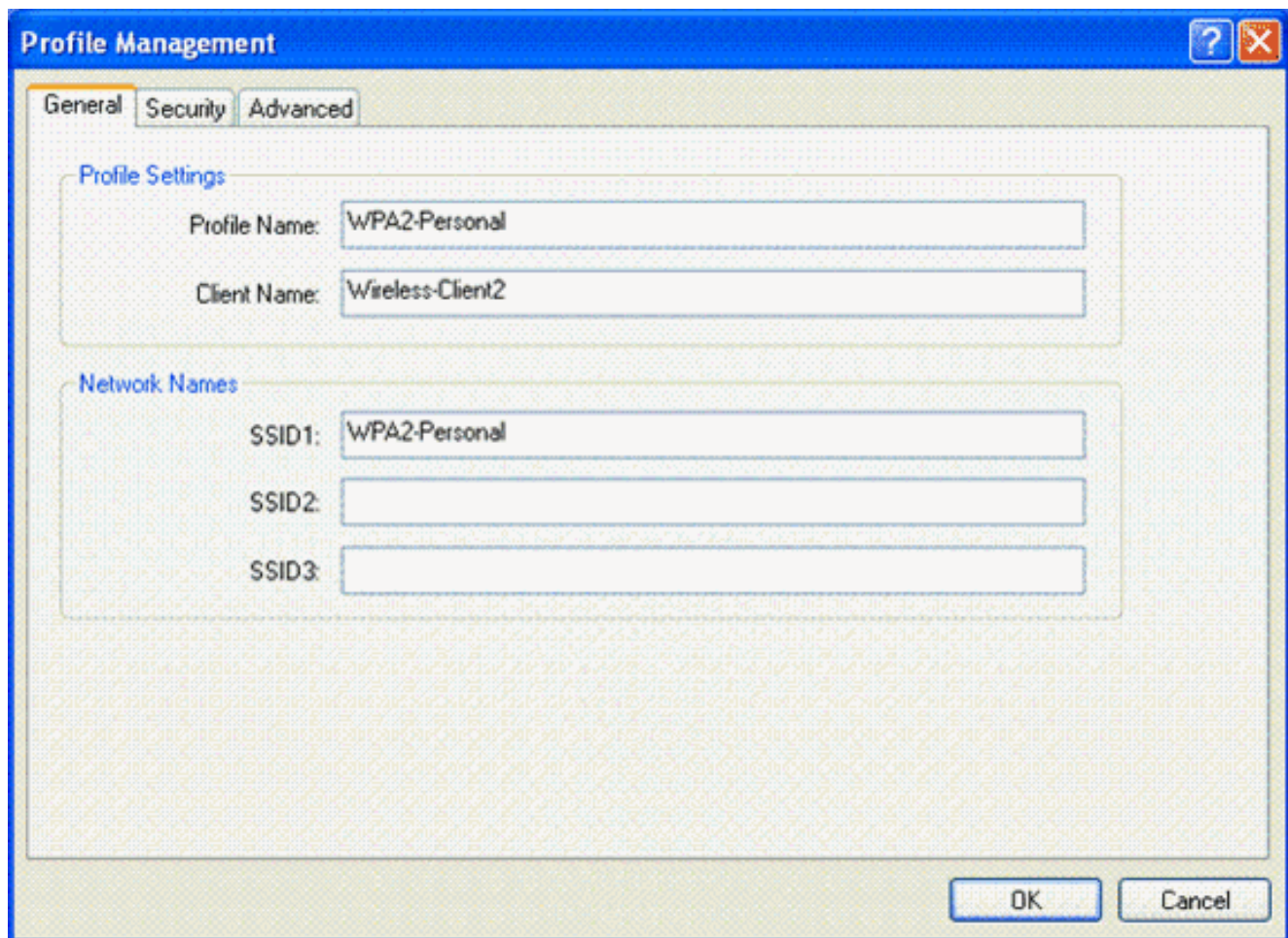
11. Clique em Apply.

[Configurar o cliente sem fio para o modo WPA2-Personal](#)

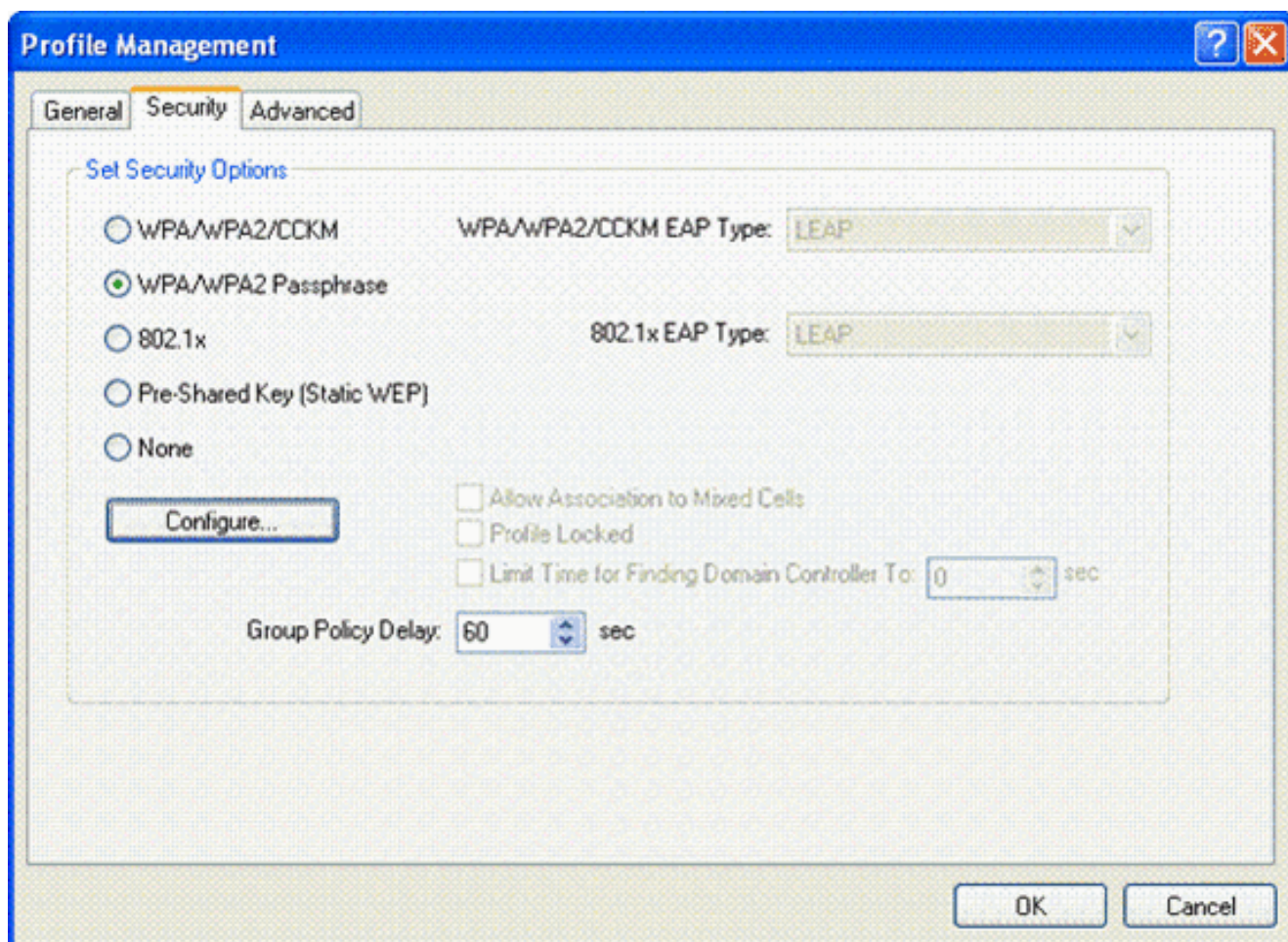
A próxima etapa é configurar o cliente sem fio para o modo de operação WPA2-Personal.

Conclua estas etapas para configurar o cliente sem fio para o modo WPA2-Personal:

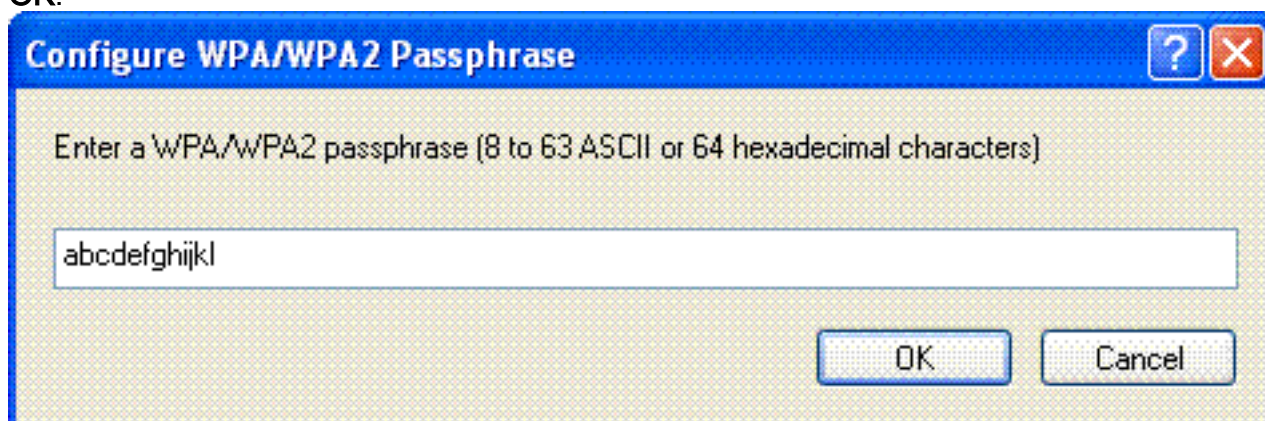
1. Na janela Aironet Desktop Utility, clique em **Profile Management > New** para criar um perfil para o usuário WPA2-PSK WLAN.
2. Na janela Gerenciamento de perfil, clique na guia **Geral** e configure o Nome do perfil, o Nome do cliente e o nome SSID como mostrado neste exemplo. Em seguida, clique em **OK**.



3. Clique na guia **Security** e escolha **WPA/WPA2 Passphrase** para habilitar o modo de operação WPA2-PSK. Clique em **Configure** para configurar a chave pré-compartilhada WPA-PSK.



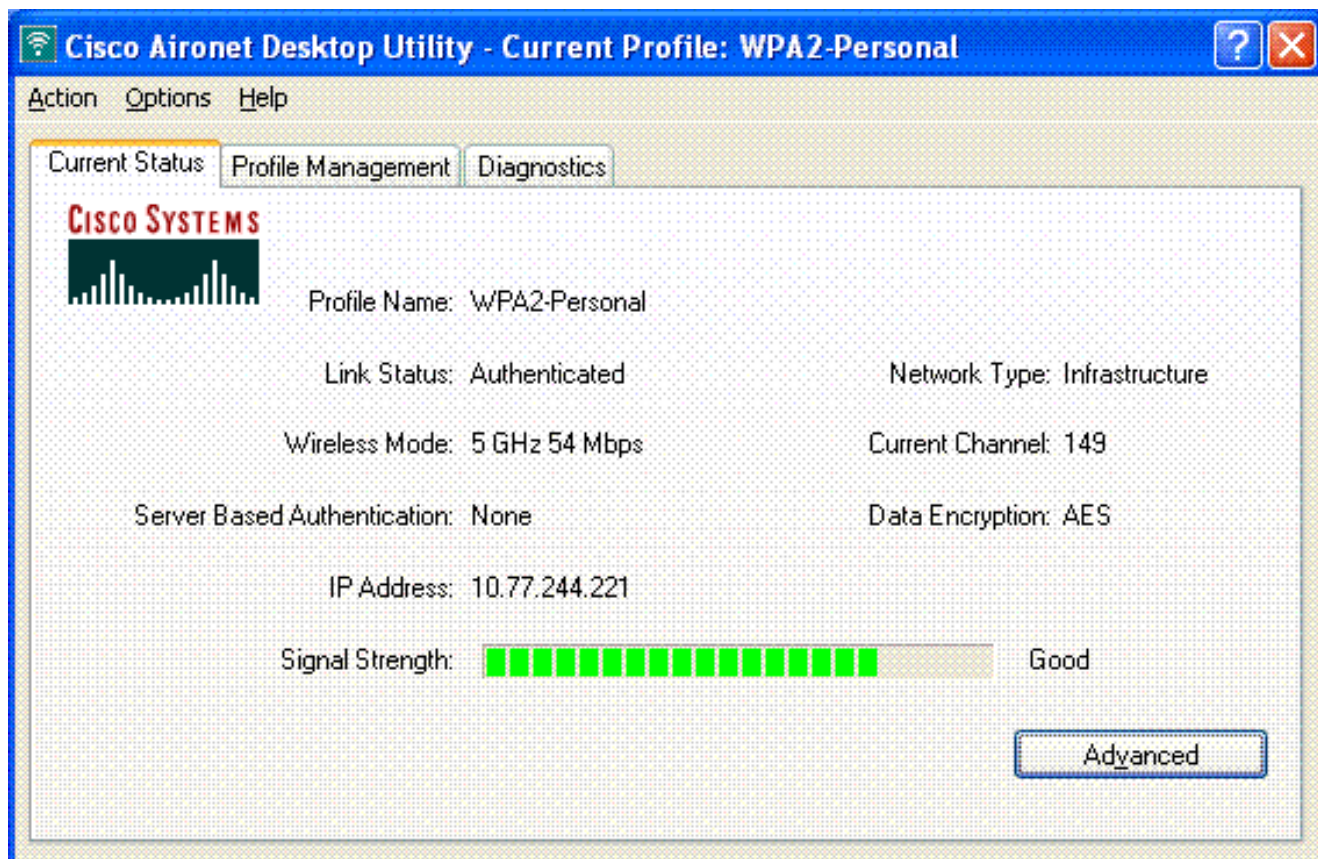
4. Insira a chave pré-compartilhada e clique em OK.



[Verificar o modo de operação WPA2-Personal](#)

Conclua estas etapas para verificar se a configuração do modo WPA2-Enterprise está funcionando corretamente:

1. Na janela do Aironet Desktop Utility, selecione o perfil **WPA2-Personal** e clique em **Ativate** para ativar o perfil do cliente sem fio.
2. Quando o perfil é ativado, o cliente sem fio se associa à WLAN após a autenticação bem-sucedida. Aqui está a captura de tela:



Troubleshoot

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

Estes comandos **debug** serão úteis para solucionar problemas de configuração:

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

- **debug dot1x events enable** — Ativa a depuração de todos os eventos dot1x. Aqui está um exemplo de saída de depuração com base na autenticação bem-sucedida: **Observação:** algumas das linhas desta saída foram movidas para duas linhas devido a 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**

- **debug dot1x packet enable** — Habilita a depuração de mensagens de pacote 802.1x.
- **debug aaa events enable** — Ativa a saída de depuração de todos os eventos aaa.

[Informações Relacionadas](#)

- [WPA2 – Wi-Fi Protected Access 2](#)
- [Exemplo de Autenticação EAP-FAST com Controladoras Wireless LAN e Servidor RADIUS Externo](#)
- [Exemplo de Configuração de Autenticação EAP com WLAN Controllers \(WLC\)](#)
- [Visão Geral da Configuração do WPA](#)
- [Suporte de produtos 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.