A página do respingo do controlador do Wireless LAN reorienta o exemplo de configuração

Índice

Introdução

Este documento descreve como configurar a característica de redirecionamento da página de abertura nos Controllers de LAN Wireless.

Pré-requisitos

Requisitos

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

- Conhecimento de soluções da Segurança LWAPP
- Conhecimento de como configurar o Cisco Secure ACS

Componentes Utilizados

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

- O controlador do Wireless LAN do Cisco 4400 Series (WLC) esse executa a versão de firmware 5.0

- Access point de pouco peso do Cisco 1232 Series (REGAÇO)
- Adaptador de cliente Wireless do Cisco Aironet 802.a/b/g que executa a versão de firmware 4.1
- Server do Cisco Secure ACS que executa a versão 4.1
- Algum servidor de Web externo da terceira

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

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

Informações de Apoio

A Web da página do respingo reorienta é uma característica introduzida com versão 5.0 do controlador do Wireless LAN. Com esta característica, o usuário está reorientado a um página da web particular depois que a autenticação do 802.1x terminou. A reorientação ocorre quando o usuário abre um navegador (configurado com um Home Page de padrão) ou tentativas para alcançar uma URL. Depois que a reorientação ao página da web está completa, o usuário tem o acesso direto à rede.

Você pode especificar a página da reorientação no server do Remote Authentication Dial-In User Service (RADIUS). O servidor Radius deve ser configurado para retornar o par Cisco AV URL-reorienta o atributo RADIUS ao controlador do Wireless LAN em cima da autenticação bem sucedida do 802.1x.

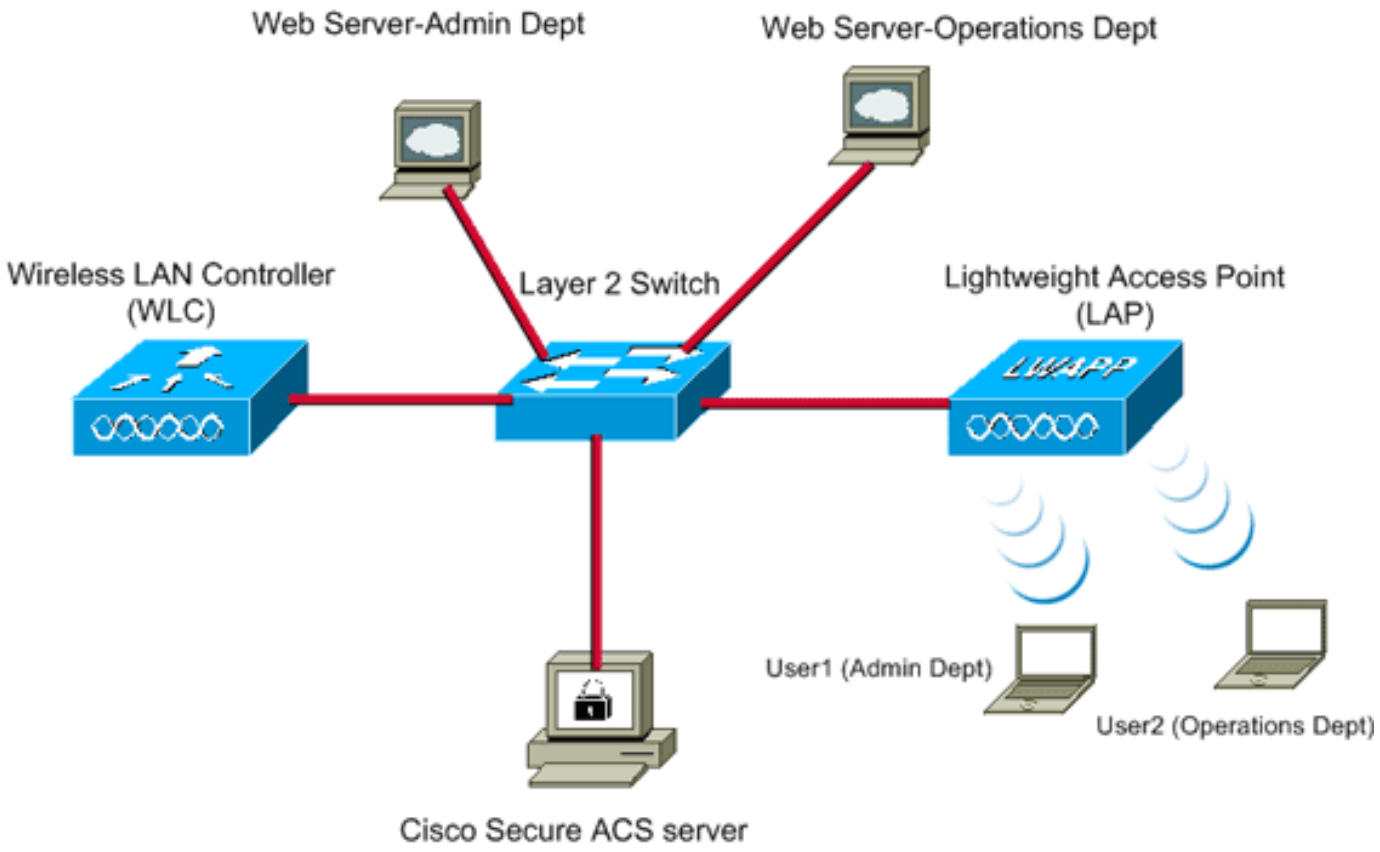
A Web da página do respingo reorienta a característica está disponível somente para os WLAN configurados para o 802.1x ou WPA/WPA2 a Segurança da camada 2.

Instalação de rede

Neste exemplo, Cisco 4404 WLC e um REGAÇO do Cisco 1232 Series são conectados através de um switch de Camada 2. O server do Cisco Secure ACS (que atua como um servidor de raio externo) é conectado igualmente ao mesmo interruptor. Todos os dispositivos estão na mesma sub-rede.

O REGAÇO é registrado inicialmente ao controlador. Você deve criar dois WLAN: um para os usuários do **departamento administrativo** e o outro para os usuários do **departamento de operações**. Ambos os uso WPA2/ AES do Sem fio LAN (EAP-FAST é usado para a autenticação). Ambos os WLAN usam a página do respingo reorientam a característica a fim reorientar usuários ao Home Page apropriado URL (em servidores de Web externos).

Este documento utiliza a seguinte configuração de rede:



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

A próxima seção explica como configurar os dispositivos para esta instalação.

Configurar

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

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Termine estas etapas a fim configurar os dispositivos para usar a página do respingo reorientam a característica:

1. Configurar o WLC para a autenticação RADIUS através do server do Cisco Secure ACS.
2. Configurar os WLAN para os departamentos Admin e de operações.
3. Configurar o Cisco Secure ACS para apoiar a página do respingo reorientam a característica.

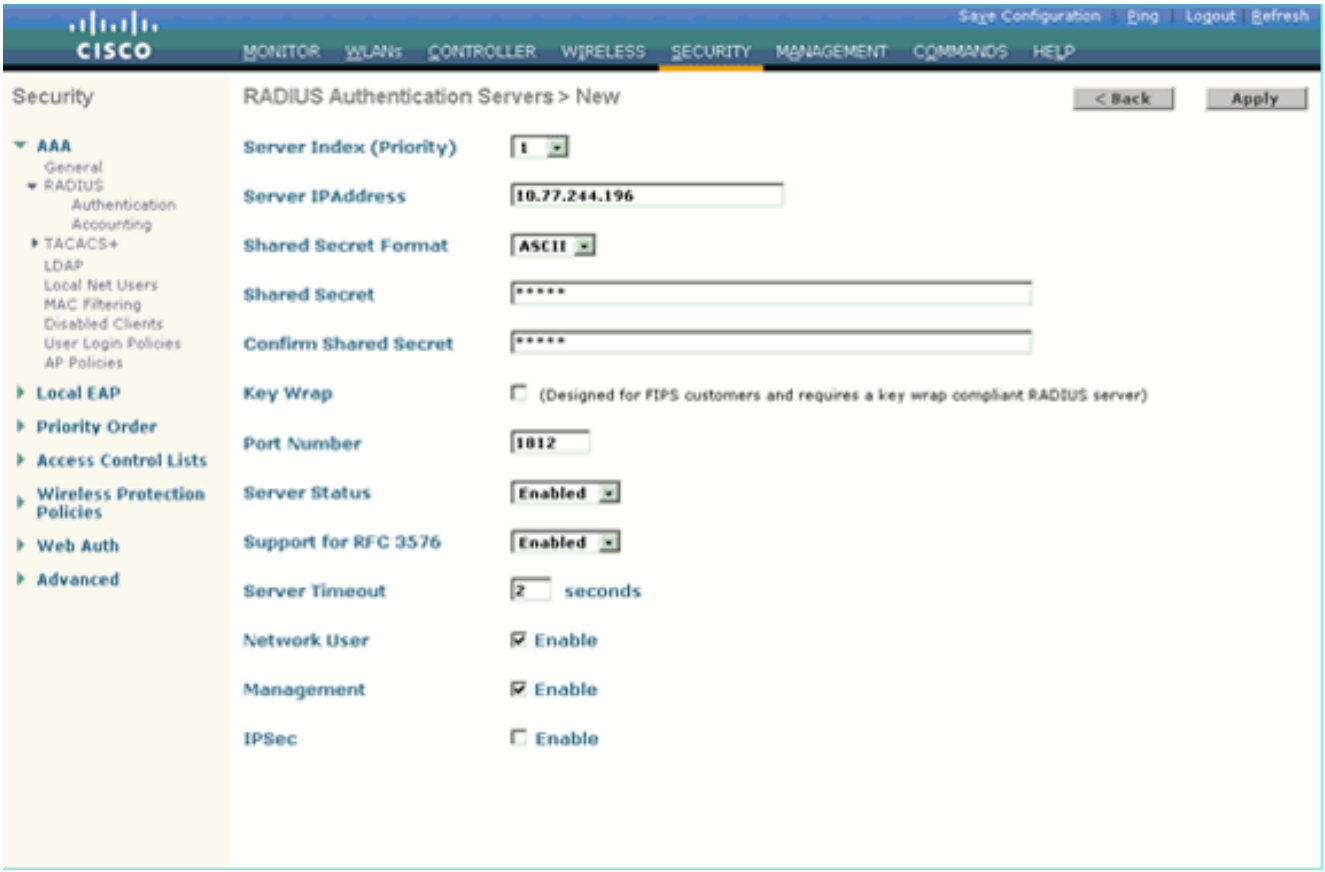
Etapa 1. Configurar o WLC para a autenticação RADIUS através do server do

Cisco Secure ACS.

O WLC precisa de ser configurado a fim enviar as credenciais do usuário a um servidor de raio externo.

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 a fim indicar a página dos servidores de autenticação RADIUS.
2. Clique **novo** a fim definir um servidor Radius.
3. 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 servidor



Este documento usa o servidor ACS com um endereço IP de Um ou Mais Servidores Cisco ICM NT de 10.77.244.196.

4. Clique em Apply.

Etapa 2. Configurar os WLAN para o departamento Admin e de operações.

Nesta etapa, você configura os dois WLAN (um para o departamento administrativo e o outro para o departamento de operações) que os clientes usarão a fim conectar à rede Wireless.

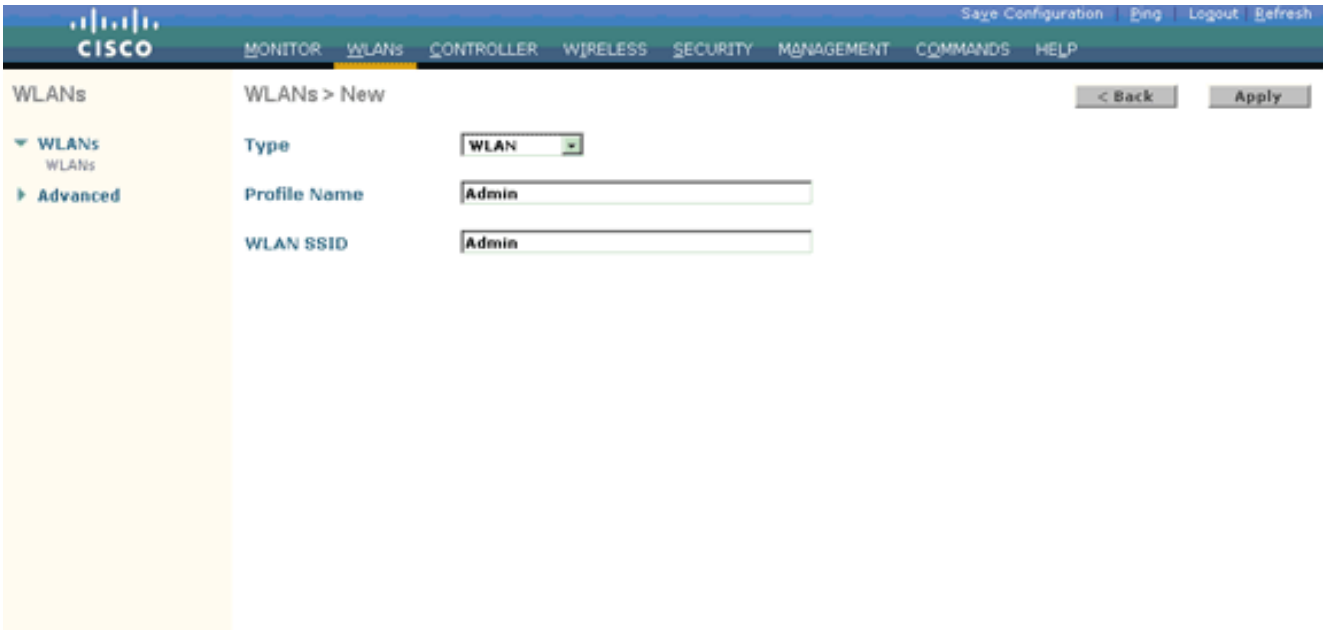
O WLAN SSID para o departamento administrativo será *Admin*. O WLAN SSID para o departamento de operações será operações.

Use a autenticação EAP-FAST a fim permitir o WPA2 como o mecanismo de segurança da camada 2 em ambos os WLAN e na política da Web - a Web da página do respingo reorienta a

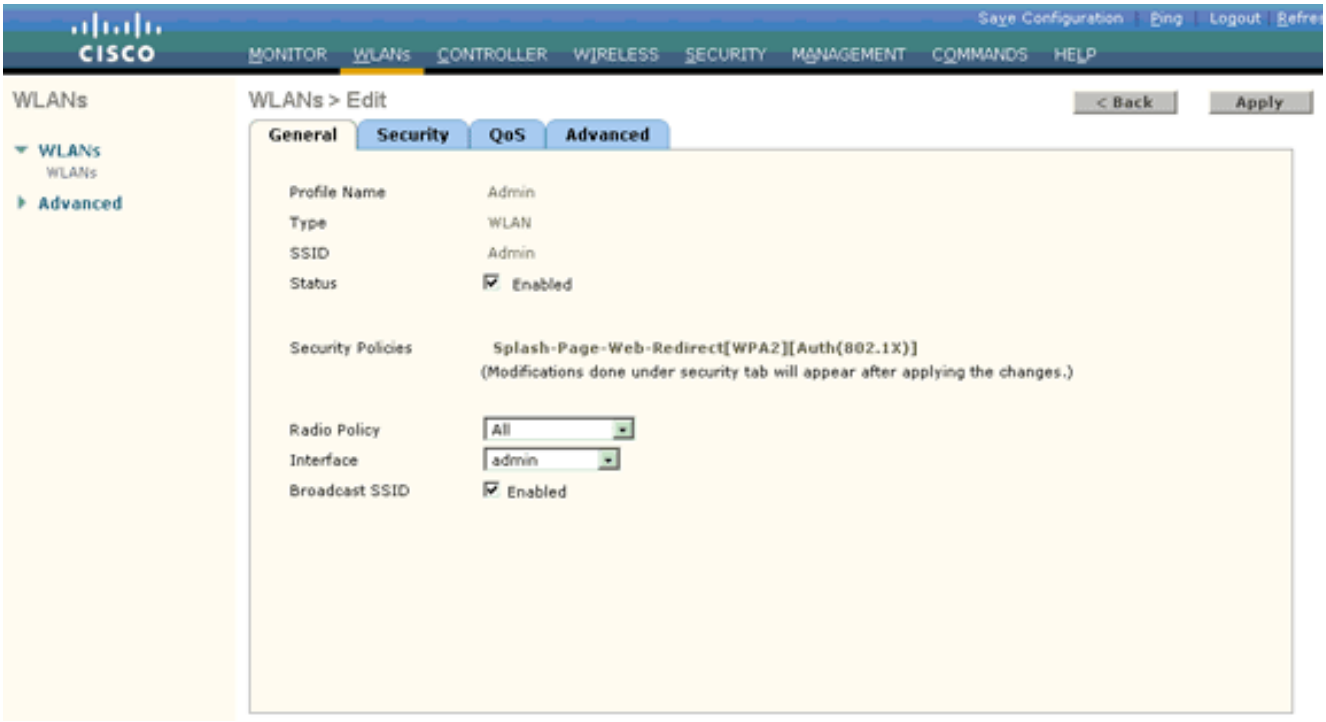
característica como o método de segurança da camada 3.

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

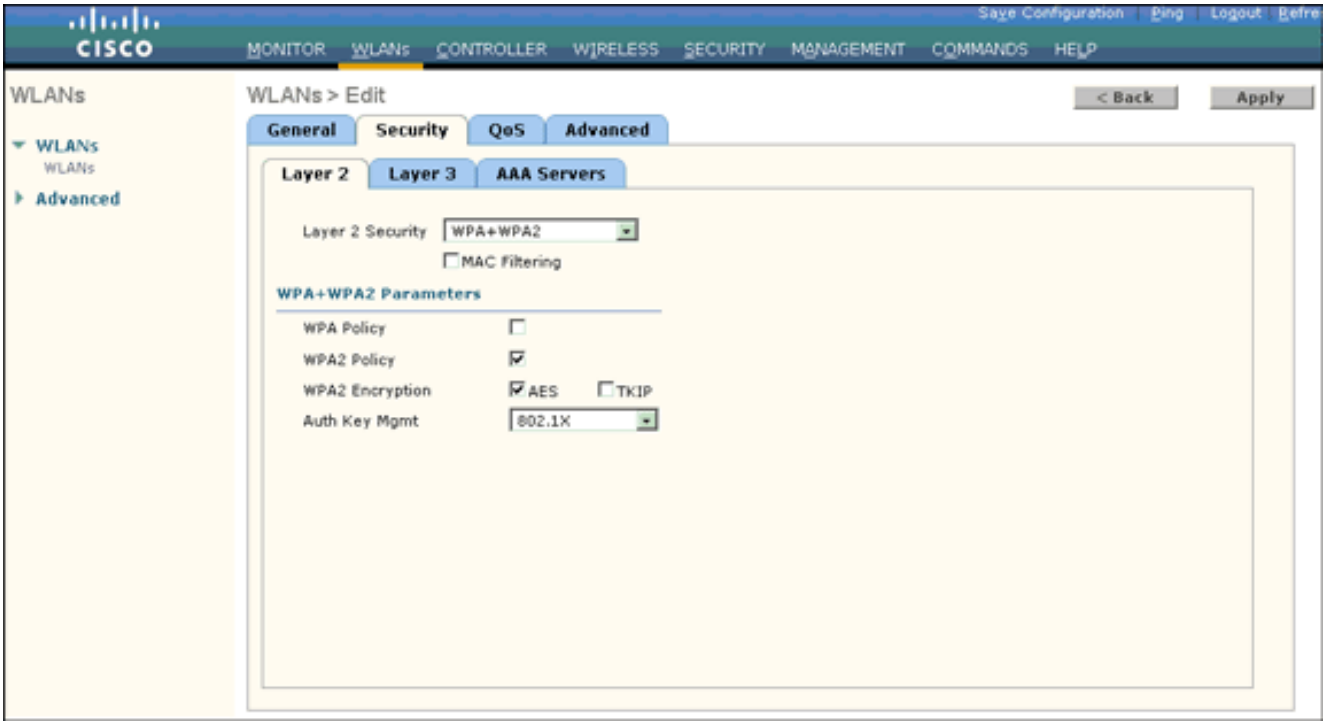
1. Clique **WLAN do** GUI do controlador a fim indicar a página WLAN.Esta página alista os WLAN que existem no controlador.
2. Clique **novo** a fim criar um WLAN novo.



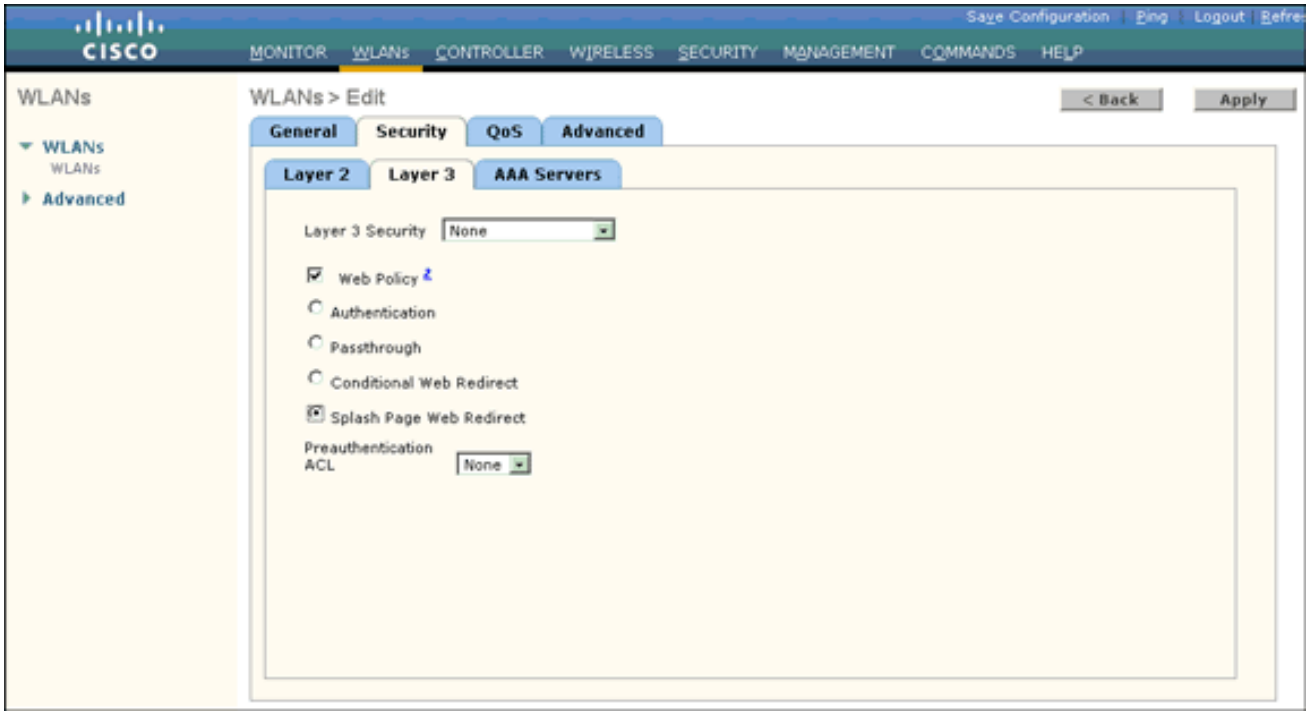
3. Dê entrada com o nome WLAN SSID e o nome de perfil no WLAN > página nova.
4. Clique em Apply.
5. Deixe-nos primeiramente criam o WLAN para o departamento administrativo.Uma vez que você cria um WLAN novo, o WLAN > edita a página para o WLAN novo aparece. Nesta página, você pode definir os vários parâmetros específicos a este WLAN. Isto inclui políticas gerais, políticas de segurança, políticas de QoS, e parâmetros avançados.
6. Sob políticas gerais, verifique a caixa de **verificação de status** a fim permitir o WLAN.



7. Clique a **ABA de segurança**, e clique então a aba da **camada 2**.
8. Escolha **WPA+WPA2 da** lista de drop-down da Segurança da camada 2.Esta etapa permite a autenticação WPA para o WLAN.
9. Sob os parâmetros WPA+WPA2, verifique as caixas de seleção da **política WPA2** e da **criptografia de AES**.

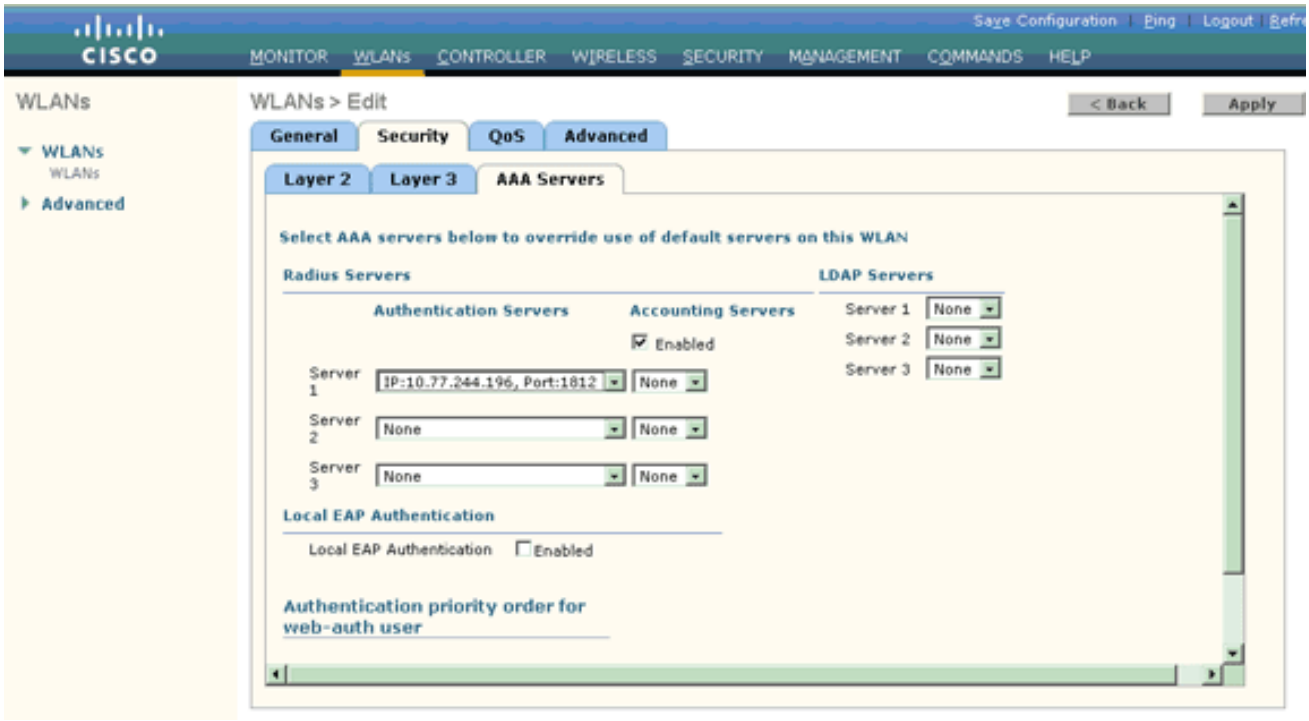


10. Escolha o **802.1x da** lista de drop-down de Mgmt da chave do AUTH. Esta opção permite o WPA2 com autenticação 802.1x/EAP e criptografia de AES para o WLAN.
11. Clique a **ABA de segurança da camada 3**.
12. Verifique a caixa da **política da Web**, e clique então a **Web da página do respingo reorientam o** botão de rádio.Esta opção permite a Web da página do respingo reorienta a característica.



13. Clique a aba dos **servidores AAA**.
14. Sob Authentication Server, escolha o endereço IP do servidor apropriado da lista de drop-

down do
servidor1.



Neste exemplo, 10.77.244.196 é usado como o servidor Radius.

15. Clique em Apply.
16. Repita etapas 2 a 15 a fim criar o WLAN para o departamento de operações.Os WLAN paginam lista os dois WLAN que você
criou.

Observe que as políticas de segurança incluem a página do respingo reorientam.

Etapa 3. Configurar o Cisco Secure ACS para apoiar a página do respingo reorientam a característica.

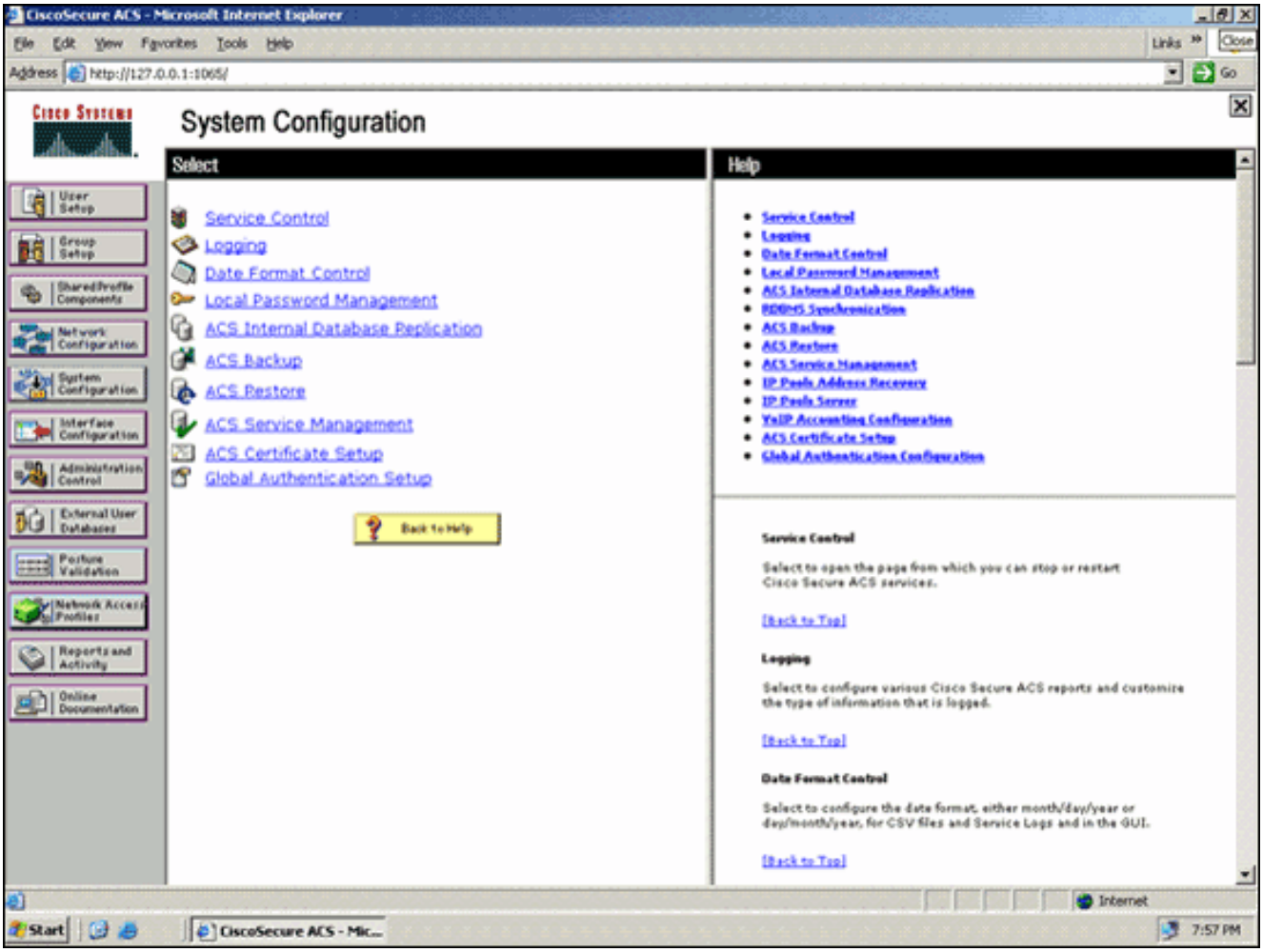
A próxima etapa é configurar o servidor Radius para esta característica. O servidor Radius precisa de executar a autenticação EAP-FAST a fim validar as credenciais do cliente, e em cima da autenticação bem sucedida, para reorientar o usuário à URL (no servidor de Web externo) especificada no par Cisco AV URL-***reoriente o*** atributo RADIUS.

Configurar o Cisco Secure ACS para a autenticação EAP-FAST

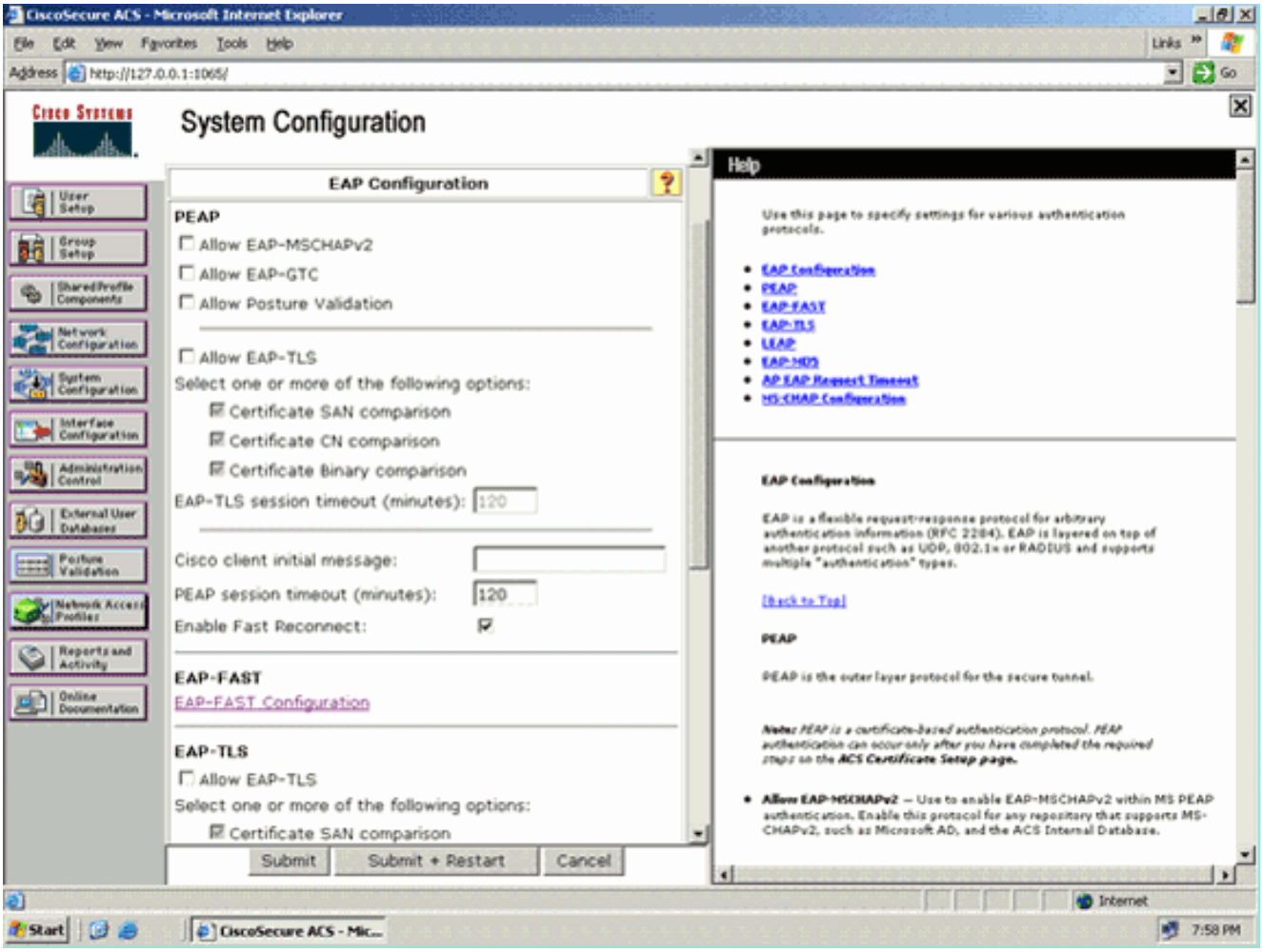
Nota: Este documento supõe que o controlador do Wireless LAN está adicionado ao Cisco Secure ACS como um cliente de AAA.

Termine estas etapas a fim configurar a autenticação EAP-FAST no servidor Radius:

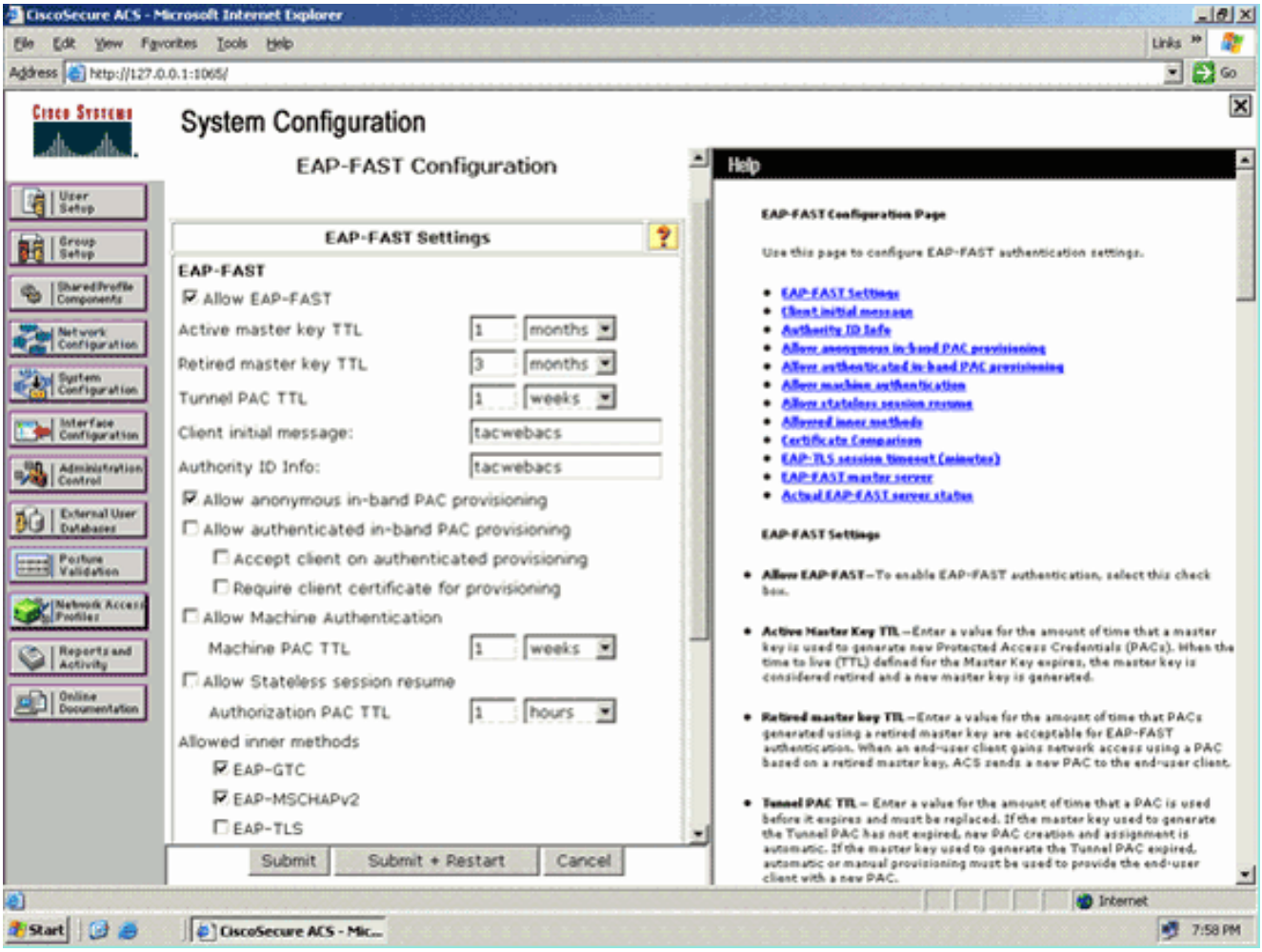
1. Clique a **configuração de sistema do** servidor Radius GUI, e escolha-a então escolhem a **autenticação global Setup da** página da configuração de sistema.



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** a fim permitir EAP-FAST no servidor
   Radius.



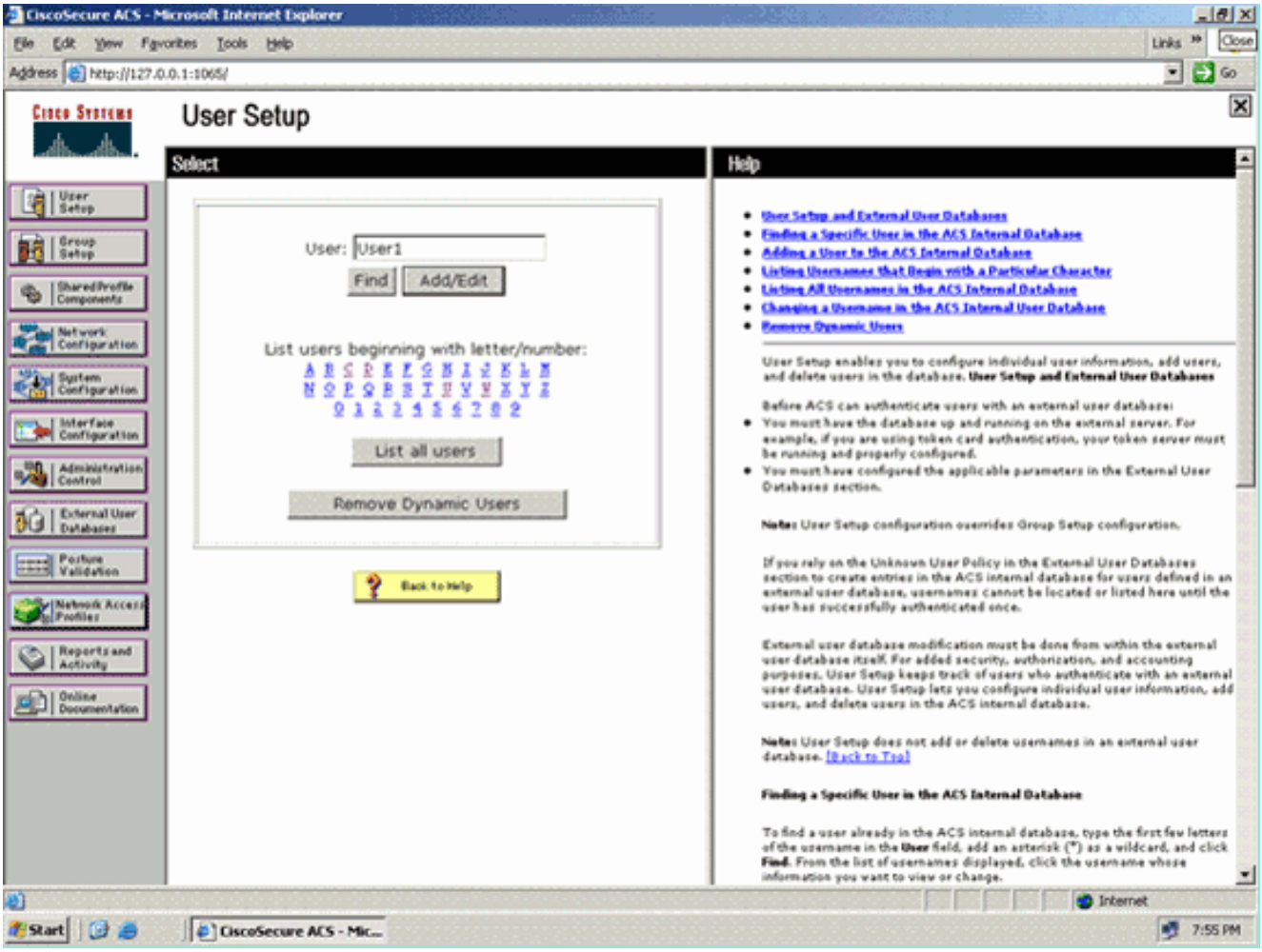
4. Configurar o Active/valores aposentados do chave mestre TTL (tempo ao vivo) como desejado, ou ajuste-os ao valor padrão segundo as indicações deste exemplo.O campo de informação de ID da autoridade representa a identidade textual deste servidor ACS, que um utilizador final pode usar para determinar 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. A opção *interna permitida dos métodos* 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).
7. Clique em Submit.**Nota:** Para a informação detalhada e os exemplos sobre como configurar o EAP JEJUE com abastecimento anônimo da Em-faixa PAC e o abastecimento autenticado da Em-faixa, refere a autenticação EAP-FAST com exemplo de configuração dos controladores e do servidor de raio externo do Wireless LAN.

Configurar a base de dados de usuário e defina o atributo RADIUS da URL-*reorientação*

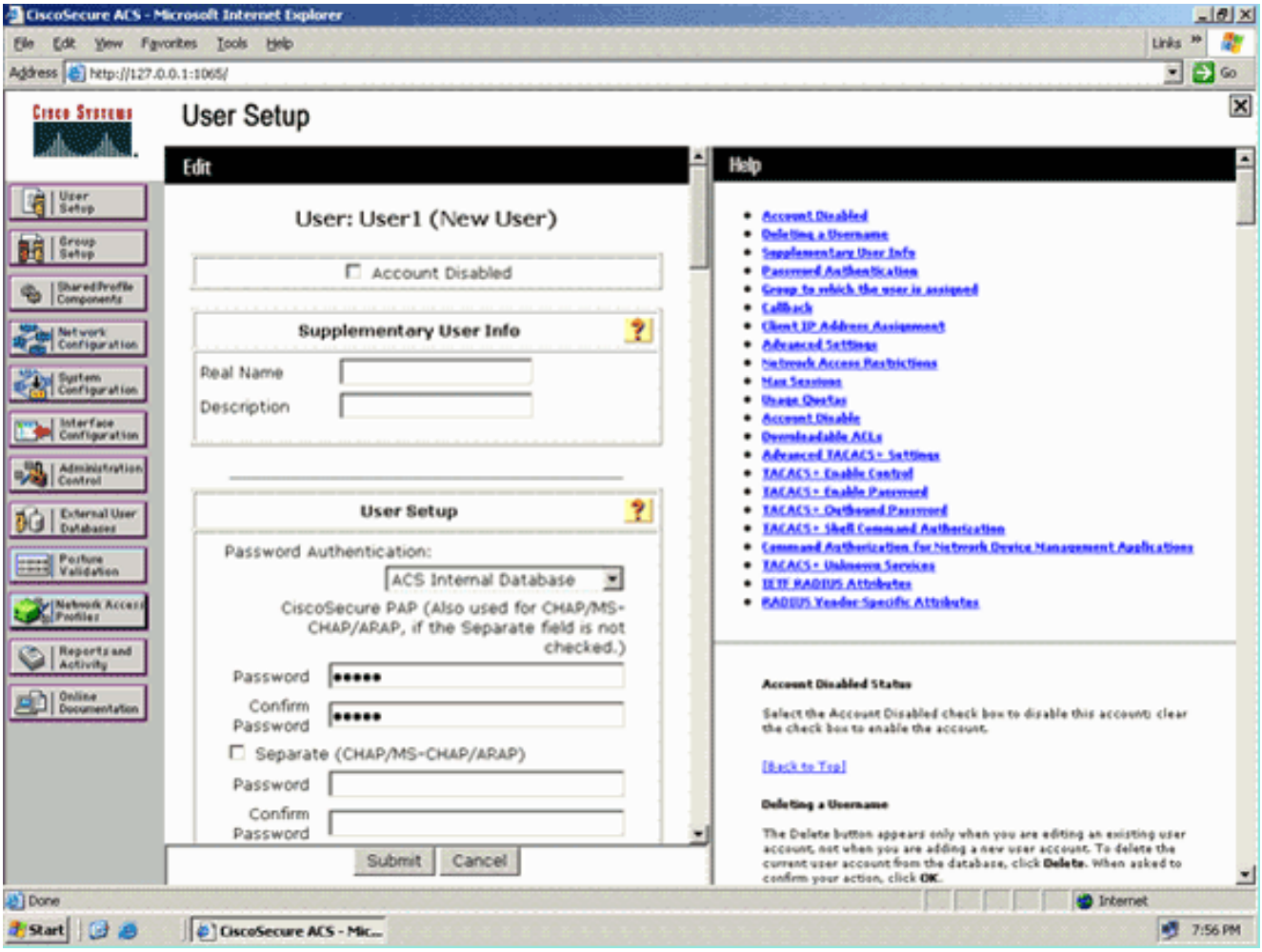
Este exemplo configura o nome de usuário e senha do cliente Wireless como o usuário1 e o usuário1, respectivamente.

Termine estas etapas a fim criar uma base de dados de usuário:

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



3. 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.



4. Enrole para baixo a página para alterar os atributos RADIUS.
5. Verifique a caixa de verificação do **Cisco-av-pair [009\001]**.
6. Inscreva estes pares Cisco AV na caixa de edição do Cisco-av-pair [009\001] a fim especificar a URL a que o usuário é reorientado:url-redirect=http://10.77.244.196/Admin-Login.html

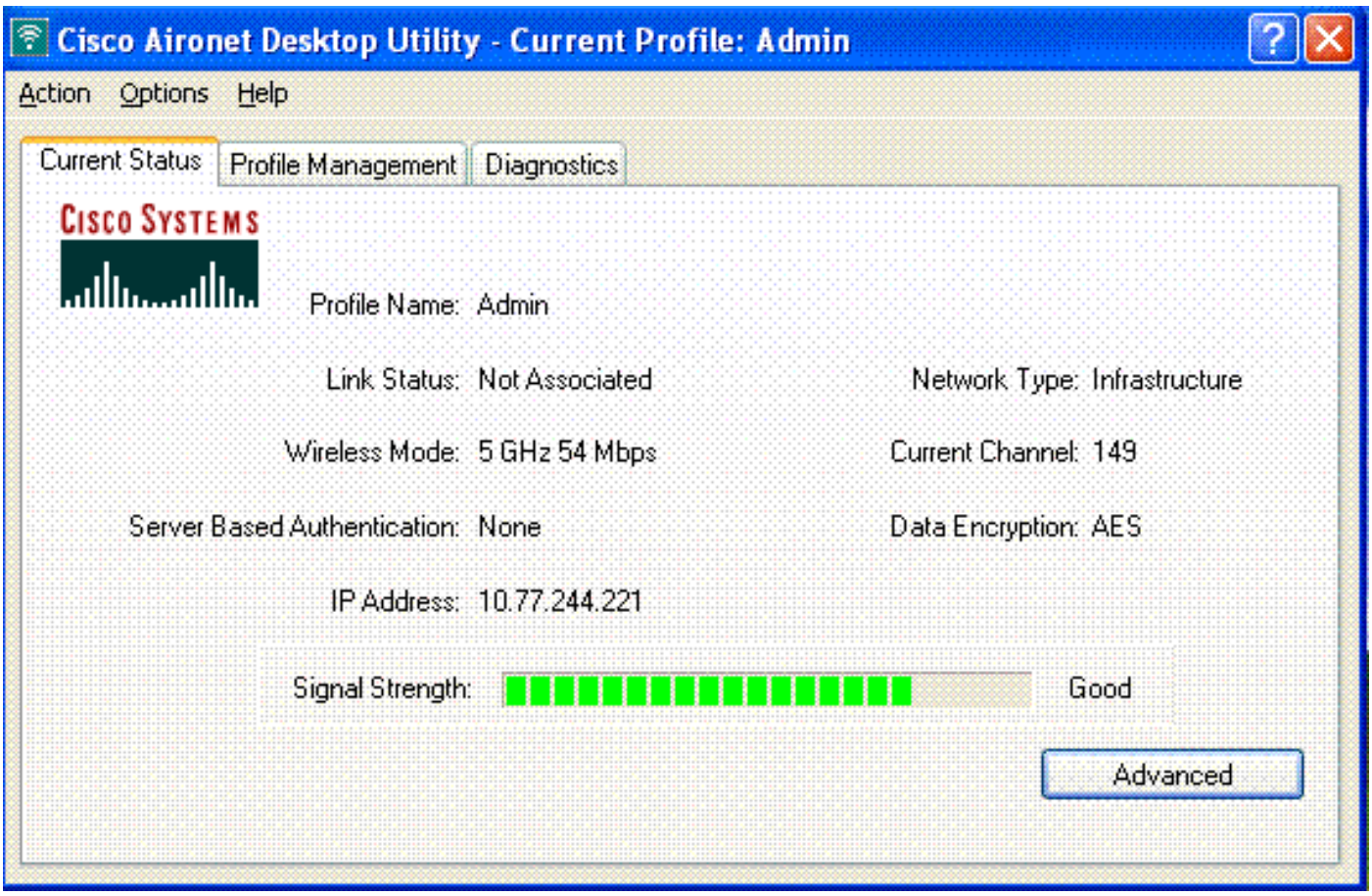
Este é o Home Page dos usuários do departamento administrativo.

7. Clique em Submit.
8. Repita este procedimento a fim adicionar User2 (usuário do departamento de operações).
9. Repita etapas 1 com 6 a fim adicionar mais usuários dos usuários do departamento administrativo e do departamento de operações ao base de dados.**Nota:** Os atributos RADIUS podem ser configurados a nível de usuário ou nível do grupo no Cisco Secure ACS.

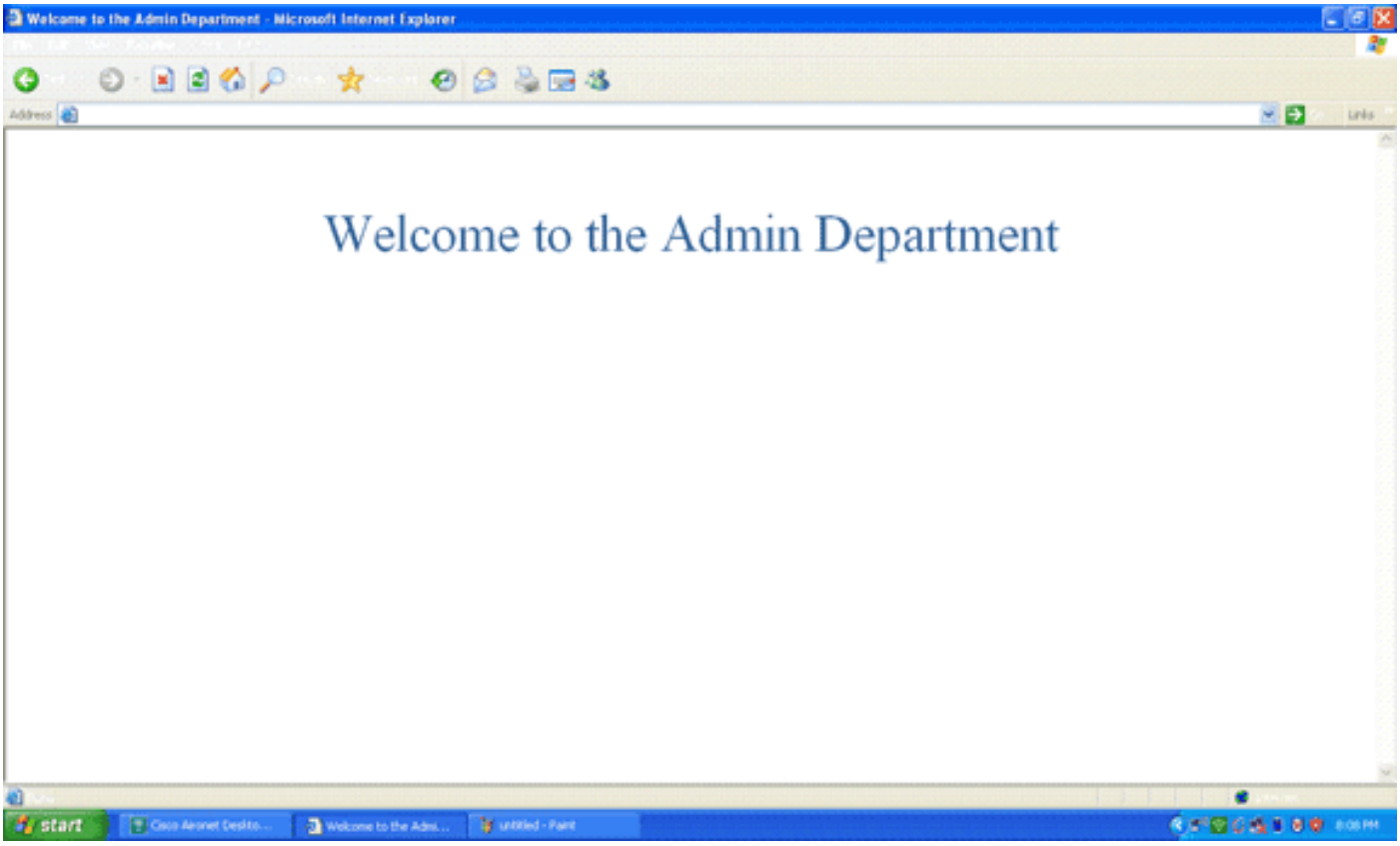
Verificar

A fim verificar a configuração, associe um cliente de WLANs do departamento administrativo e do departamento de operações a seus WLAN apropriados.

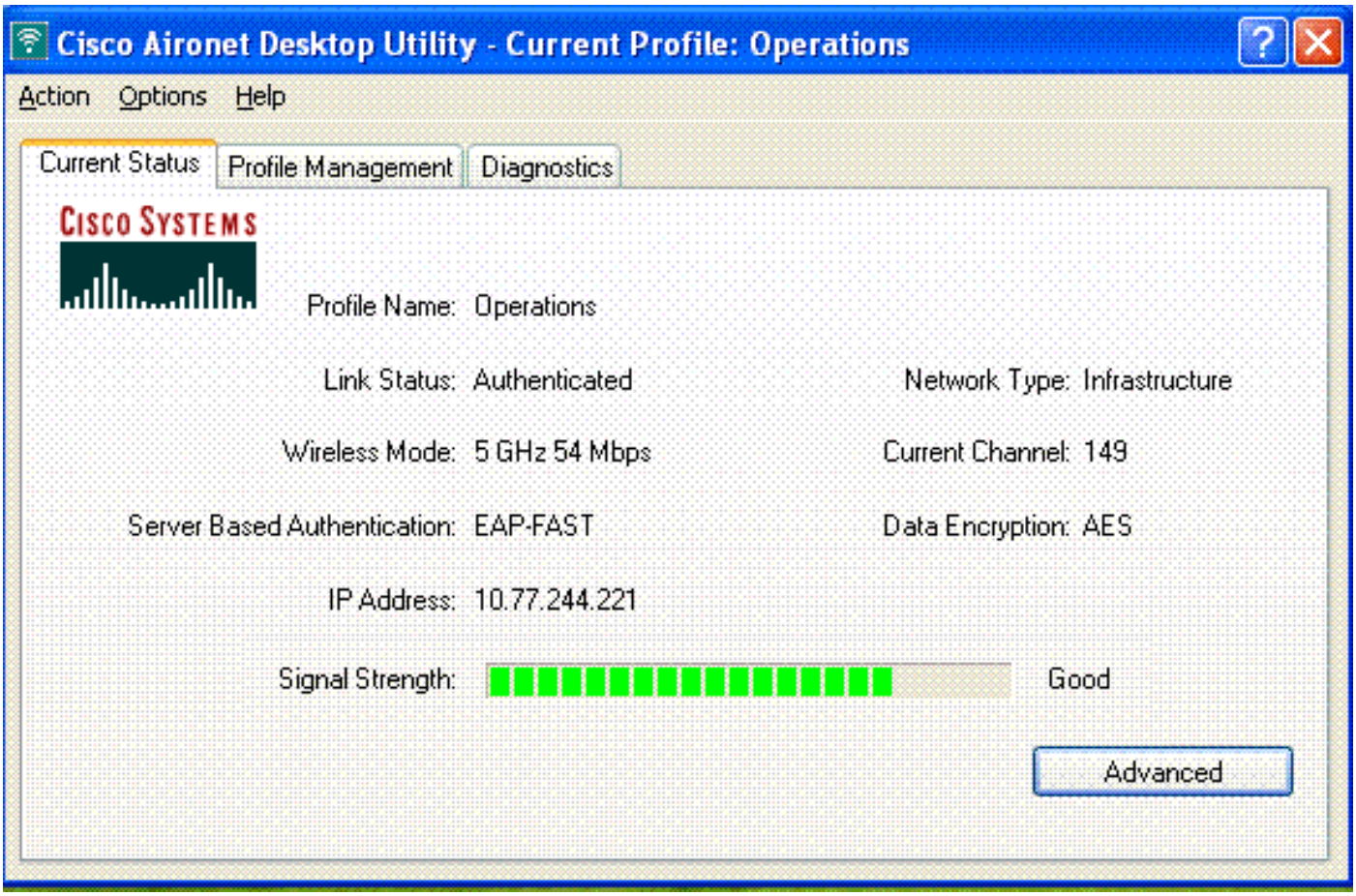
Quando um usuário do departamento administrativo conecta ao Wireless LAN Admin, o usuário está alertado para as credenciais do 802.1x (credenciais EAP-FAST em nosso caso). Uma vez que o usuário fornece as credenciais, o WLC passa aquelas credenciais ao server do Cisco Secure ACS. O server do Cisco Secure ACS valida as credenciais do usuário contra o base de dados, e em cima da autenticação bem sucedida, retorna o atributo da URL-reorientação ao controlador do Wireless LAN. A autenticação está completa nesta fase.

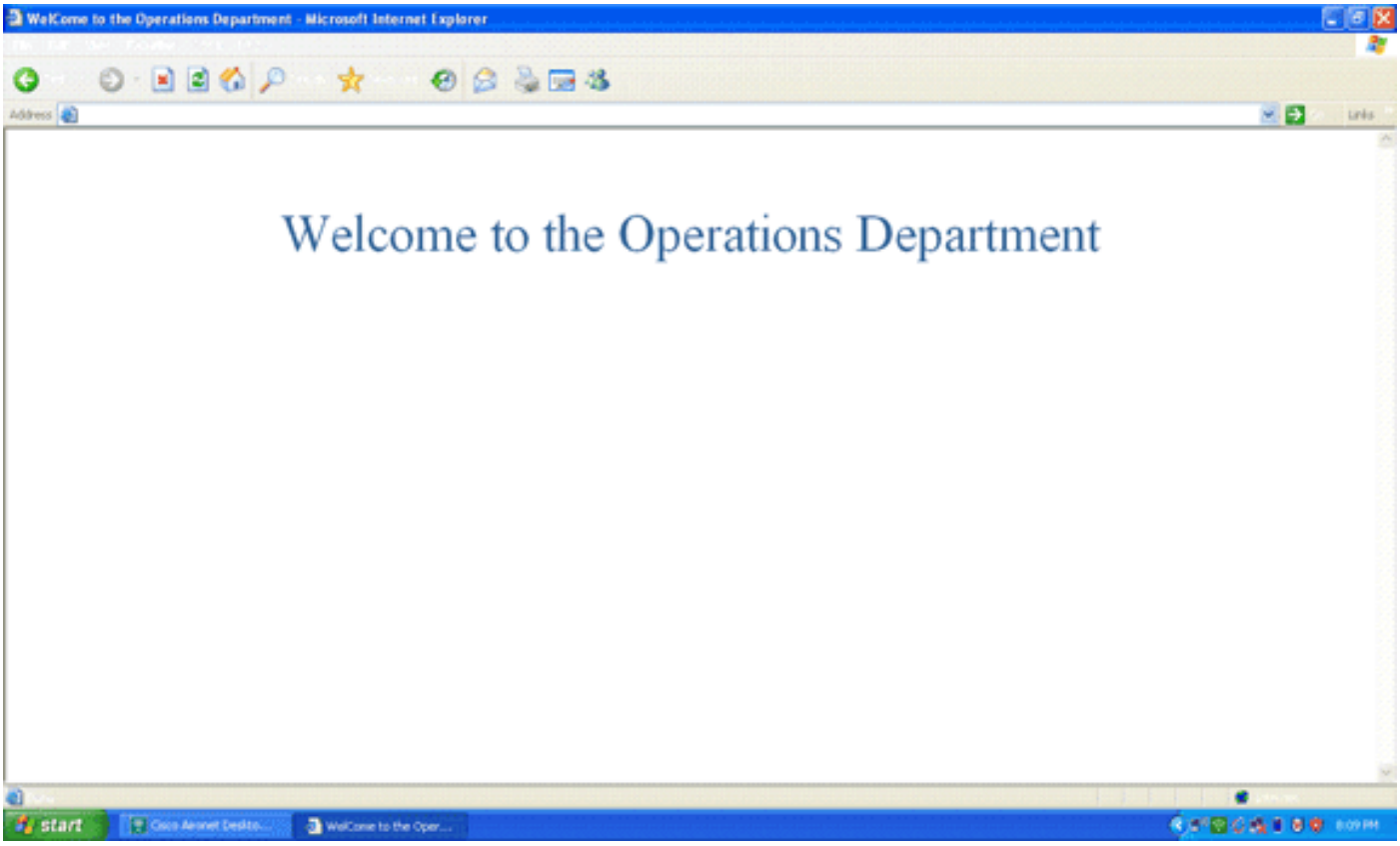


Quando o usuário abre um navegador da Web, o usuário está reorientado ao Home Page URL do departamento administrativo. (Esta URL é retornada ao WLC com o atributo do Cisco-av-pair). Depois que a reorientação, o usuário tem o acesso direto à rede. Estão aqui os screenshots:



As mesmas sequências de evento ocorrem quando um usuário do departamento de operações conecta às operações WLAN.





Troubleshooting

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

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

Você pode usar os comandos seguintes pesquisar defeitos sua configuração.

- **mostre o wlan_id wlan** — Indica o estado da Web reorientam características para um WLAN particular.Aqui está um exemplo:

```
WLAN Identifier.................................. 1
Profile Name..................................... Admin
Network Name (SSID).............................. Admin
...
Web Based Authentication......................... Disabled
Web-Passthrough.................................. Disabled
Conditional Web Redirect......................... Disabled
Splash-Page Web Redirect......................... Enabled
```

- **debugar eventos do dot1x permitem** — Permite debugar de mensagens de pacote do 802.1x.Aqui está um exemplo:

```
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Sending EAP Request from AAA to
    mobile 00:40:96:ac:dd:05 (EAP Id 16)
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Received EAPOL EAPPKT from
    mobile 00:40:96:ac:dd:05
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Received EAP Response from
    mobile 00:40:96:ac:dd:05 (EAP Id 16, EAP Type 43)
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Processing Access-Challenge for
    mobile 00:40:96:ac:dd:05
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Setting re-auth timeout to 1800
```

```
    seconds, got from WLAN config.
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Station 00:40:96:ac:dd:05
    setting dot1x reauth timeout = 1800
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Creating a new PMK Cache Entry
    for station 00:40:96:ac:dd:05 (RSN 2)
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Adding BSSID 00:1c:58:05:e9:cf
    to PMKID cache for station 00:40:96:ac:dd:05
Fri Feb 29 10:27:16 2008: New PMKID: (16)
Fri Feb 29 10:27:16 2008:      [0000] 79 ee 88 78 9c 71 41 f0 10 7d 31 ca
    fb fa 8e 3c
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Disabling re-auth since PMK
    lifetime can take care of same.
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Sending EAP-Success to mobile
    00:40:96:ac:dd:05 (EAP Id 17)
Fri Feb 29 10:27:16 2008: Including PMKID in M1  (16)
Fri Feb 29 10:27:16 2008:      [0000] 79 ee 88 78 9c 71 41 f0 10 7d 31 ca
    fb fa 8e 3c
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Sending EAPOL-Key Message to
    mobile 00:40:96:ac:dd:05
    state INITPMK (message 1), replay counter 00.00.00.00.00.00.00.00
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Received Auth Success while
    in Authenticating state for mobile 00:40:96:ac:dd:05
```

- **debugar eventos aaa permitem** — Permite o resultado do debug de todos os eventos aaa.Aqui está um exemplo:

```
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Successful transmission of
    Authentication Packet (id 103) to 10.77.244.196:1812, proxy state
    00:40:96:ac:dd:05-00:00
Thu Feb 28 07:55:18 2008: ****Enter processIncomingMessages: response code=11
Thu Feb 28 07:55:18 2008: ****Enter processRadiusResponse: response code=11
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Access-Challenge received from
    RADIUS server 10.77.244.196 for mobile 00:40:96:ac:dd:05 receiveId = 3
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Successful transmission of
    Authentication Packet (id 104) to 10.77.244.196:1812, proxy state
    00:40:96:ac:dd:05-00:00
Thu Feb 28 07:55:18 2008: ****Enter processIncomingMessages: response code=2
Thu Feb 28 07:55:18 2008: ****Enter processRadiusResponse: response code=2
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Access-Accept received from
    RADIUS server 10.77.244.196 for mobile 00:40:96:ac:dd:05 receiveId = 3
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 AAA Override Url-Redirect
    'http://10.77.244.196/Admin-login.html' set
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Applying new AAA override for
    station 00:40:96:ac:dd:05
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Override values for station
    00:40:96:ac:dd:05
       source: 4, valid bits: 0x0
       qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1
       dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
       vlanIfName: '', aclName: '
```

Informações Relacionadas

- Manual de configuração do controlador de LAN do Cisco Wireless, liberação 5.0
- Exemplo de configuração de autenticação da Web para o controlador da LAN sem fio
- Exemplo de configuração de autenticação de web externa com Wireless LAN Controllers
- Página de Suporte Wireless
- Suporte Técnico e Documentação - Cisco Systems