# Autenticação de EAP com exemplo de configuração dos controladores de WLAN (WLC)

## Índice



## Introdução

Este documento explica como configurar o Controller da LAN Wireless (WLC) para a autenticação Extensible Authentication Protocol (EAP) com o uso de um servidor RADIUS externo. Este exemplo de configuração usa o Serviço de controle de acesso Cisco Secure (ACS) como o servidor de raio externo a fim validar as credenciais do usuário.

## Pré-requisitos

### Requisitos

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

- Conhecimento básico da configuração do Lightweight Access Points (AP) e do Cisco WLC.
- Conhecimento básico do protocolo de pouco peso AP (LWAPP).
- Conhecimento de como configurar um servidor de raio externo como o Cisco Secure ACS.

## Componentes Utilizados

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

- Série AP de pouco peso do Cisco Aironet 1232AG
- Cisco 4400 Series WLC que executa o firmware 5.1
- Cisco Secure ACS que executa a versão 4.1
- Adaptador cliente do a/b/g do 802.11 do Cisco Aironet
- Utilitário de desktop do Cisco Aironet (ADU) esse firmware 4.2 das corridas

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.

# Configurar

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

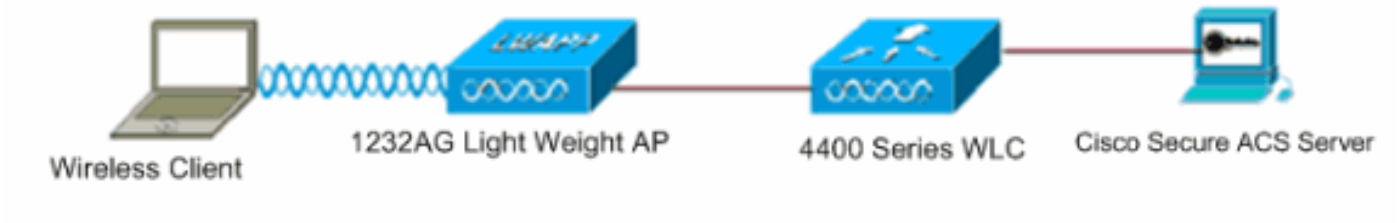
**Nota:** Use a ferramenta de consulta de comandos (clientes registrados somente) a fim encontrar mais informação nos comandos usados neste documento.

Termine estas etapas a fim configurar os dispositivos para a autenticação de EAP:

1. Configurar o WLC para a operação básica e registrar os AP de pouco peso ao controlador.
2. Configurar o WLC para a autenticação RADIUS através de um servidor de raio externo.
3. Configurar os parâmetros WLAN.
4. Configurar o Cisco Secure ACS como o servidor de raio externo e crie uma base de dados de usuário para clientes de autenticação.

## Diagrama de Rede

Nesta instalação, Cisco 4400 WLC e um AP de pouco peso é conectado através de um hub. Um servidor de raio externo (Cisco Secure ACS) é conectado igualmente ao mesmo hub. Todos os dispositivos estão na mesma sub-rede. O AP é registrado inicialmente ao controlador. Você deve configurar o WLC e o AP para a autenticação do protocolo lightweight extensible authentication (PULO). Os clientes que conectam à autenticação de leap do uso AP a fim associar com o AP. O Cisco Secure ACS é usado a fim executar a autenticação RADIUS.




## Configurar o WLC para a operação básica e registrar os AP de pouco peso ao controlador

Use o assistente da configuração de inicialização no comando line interface(cli) a fim configurar o WLC para a operação básica. Alternativamente, você pode igualmente usar o GUI a fim configurar o WLC. Este documento explica a configuração no WLC com o assistente da configuração de inicialização no CLI.

Após as botas WLC pela primeira vez, participa diretamente no assistente da configuração de inicialização. Use o wizard de configuração a fim configurar configurações básicas. Você pode executar o assistente no CLI ou no GUI. Esta saída mostra um exemplo do assistente da configuração de inicialização no CLI:

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
System Name [Cisco_33:84:a0]: WLC-1 Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (24 characters max): ***** Management Interface IP Address:
10.77.244.204 Management Interface Netmask: 255.255.255.224 Management Interface Default Router:
10.77.244.220 Management Interface VLAN Identifier (0 = untagged): Management Interface Port Num
[1 to 4]: 1 Management Interface DHCP Server IP Address: 10.77.244.220 AP Manager Interface IP
Address: 10.77.244.205 AP-Manager is on Management subnet, using same values AP Manager
Interface DHCP Server (10.77.244.220): Virtual Gateway IP Address: 1.1.1.1 Mobility/RF Group
Name: Test Network Name (SSID): Cisco123 Allow Static IP Addresses [YES][no]: yes Configure a
RADIUS Server now? [YES][no]: no Warning! The default WLAN security policy requires a RADIUS
server. Please see documentation for more details. Enter Country Code (enter 'help' for a list
of countries) [US]: Enable 802.11b Network [YES][no]: yes Enable 802.11a Network [YES][no]: yes
Enable 802.11g Network [YES][no]: yes Enable Auto-RF [YES][no]: yes Configuration saved!
Resetting system with new configuration..
```

Estes parâmetros estabelecem o WLC para a operação básica. Neste exemplo de configuração, o WLC usa 10.77.244.204 como o endereço IP de Um ou Mais Servidores Cisco ICM NT da interface de gerenciamento e 10.77.244.205 como o endereço IP de Um ou Mais Servidores Cisco ICM NT da relação do gerenciador AP.

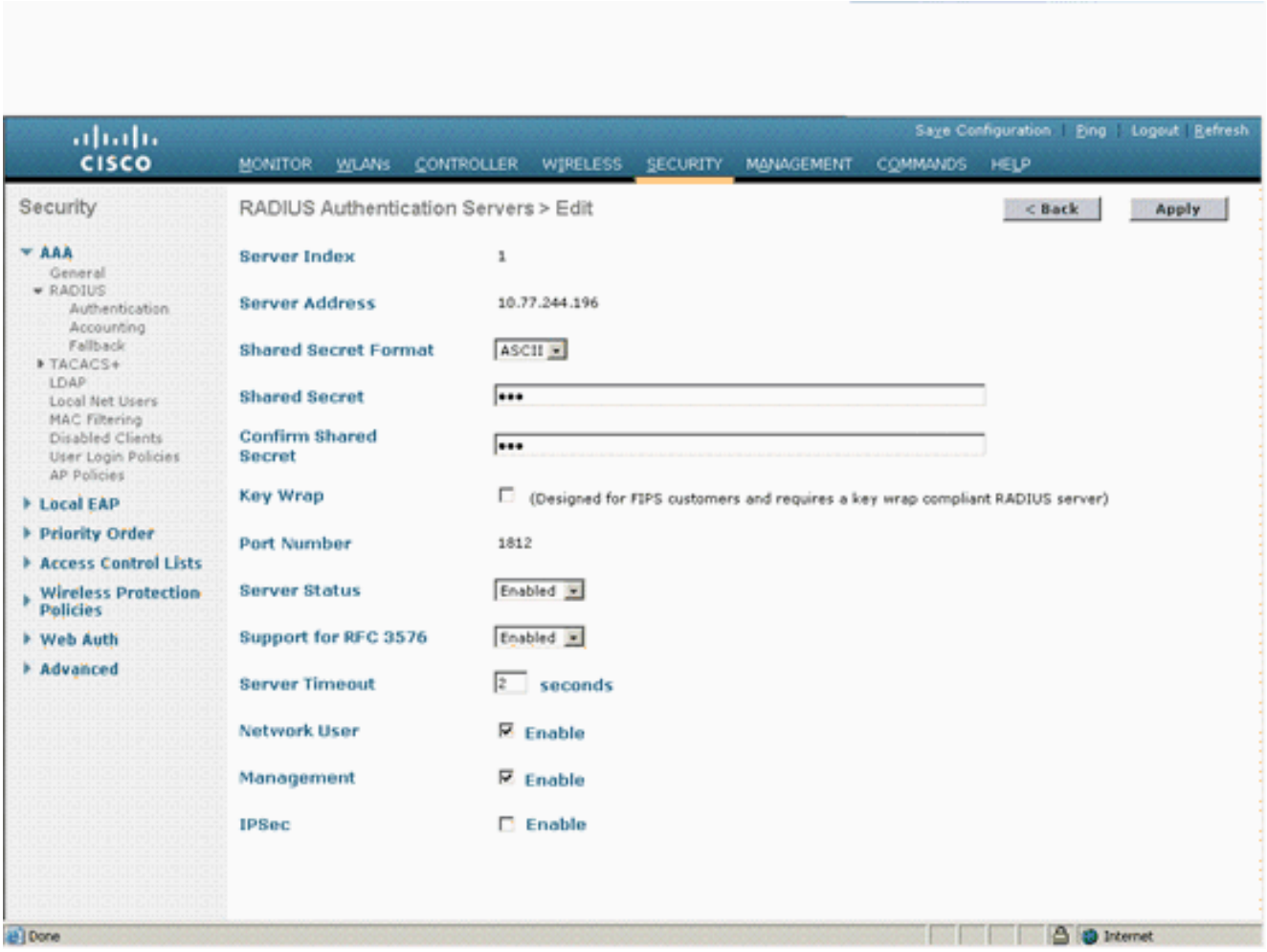
Antes que todos os outros recursos possam ser configurados nos WLC, os AP de pouco peso têm que registrar-se com o WLC. Este documento supõe que o AP de pouco peso está registrado ao WLC. Refira o registro de pouco peso AP (REGAÇO) a um controlador do Wireless LAN (WLC) para obter mais informações sobre de como os AP de pouco peso se registram com o WLC.

## 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 as credenciais do usuário 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. Clique então **novo** a fim definir um servidor Radius.




2. Defina os parâmetros do servidor Radius nos servidores de autenticação RADIUS > página nova. Estes parâmetros incluem o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor Radius, o segredo compartilhado, o número de porta, e o status de servidor.O usuário de rede e as caixas de verificação de gerenciamento determinam se a autenticação Raio-baseada se aplica para o Gerenciamento e os usuários de rede WLC. Este exemplo usa o Cisco Secure ACS como o servidor Radius com endereço IP 10.77.244.196.
3. O servidor Radius pode agora ser usado pelo WLC para a autenticação. Você pode encontrar o servidor Radius alistado se você escolhe a **Segurança > o raio > a autenticação**.


O RFC 3576 é apoiado no servidor Radius do Registrar de Acesso CNS Cisco (CAR), mas não na versão de servidor 4.0 do Cisco Secure ACS e mais adiantado.Você pode

igualmente usar a característica local do servidor Radius a fim autenticar usuários. O servidor Radius local foi introduzido com código de 4.1.171.0 da versão. Os WLC que executam versões anterior não têm a característica local do raio. O EAP local é um método de autenticação que permita os usuários e os clientes Wireless a ser autenticados localmente. É projetado para o uso nos escritórios remotos que querem manter a Conectividade aos clientes Wireless quando o sistema backend se torna interrompido ou o servidor de autenticação externa vai para baixo. O EAP local recupera credenciais do usuário da base de dados de usuário local ou do base de dados da parte posterior LDAP para autenticar usuários. Os apoios locais EAP PULAM, EAP-FAST com os PAC, EAP-FAST com Certificados, e autenticação EAP-TLS entre o controlador e os clientes Wireless.O EAP local é projetado como um sistema de autenticação alternativo. Se algum servidor Radius é configurado no controlador, o controlador tenta autenticar primeiramente os clientes Wireless com os servidores Radius. O EAP local é tentado somente se nenhum servidor Radius é encontrado, tampouco porque os servidores Radius cronometrados para fora ou nenhum servidor Radius foi configurado.Refira a autenticação de EAP local no controlador do Wireless LAN com exemplo de configuração EAP-FAST e do servidor ldap para obter mais informações sobre de como configurar o EAP local em controladores do Wireless LAN.

## Configurar parâmetros WLAN

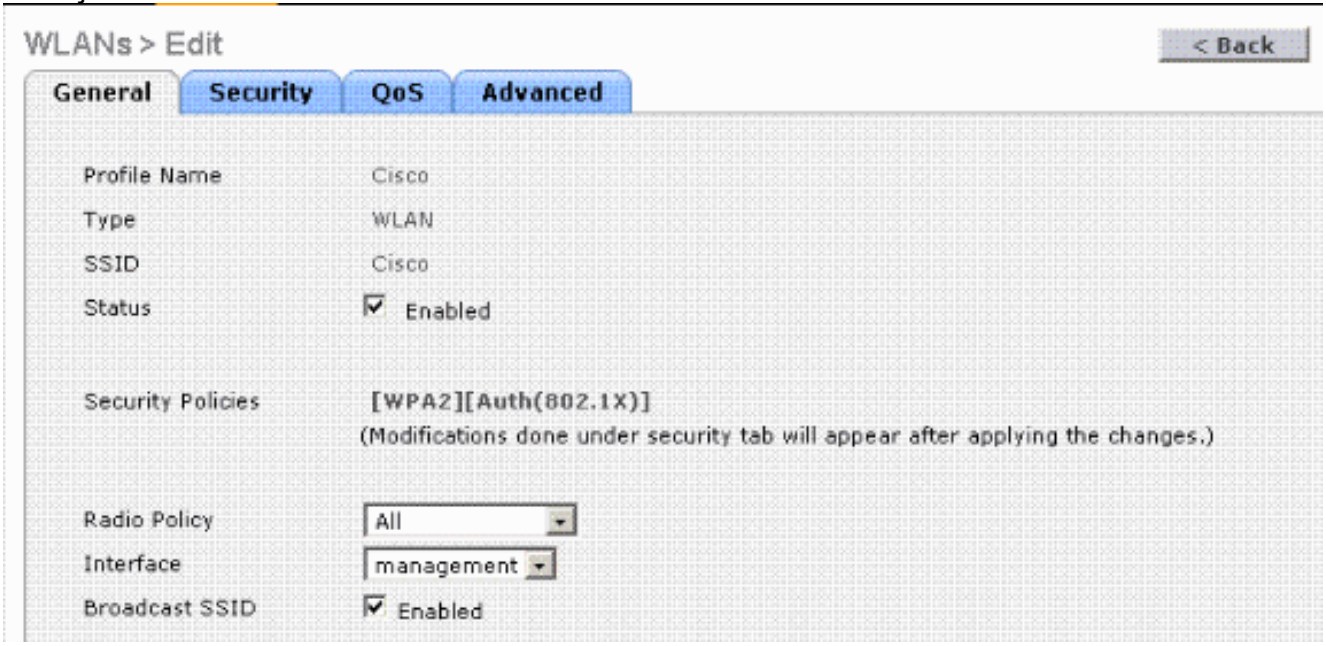
Em seguida, configurar o WLAN que os clientes se usam para conectar à rede Wireless. Quando você configurou os parâmetros básicos para o WLC, você igualmente configurou o SSID para o WLAN. Você pode usar este SSID para o WLAN ou criar um SSID novo. Neste exemplo, você cria um SSID novo.

**Nota:** Você pode configurar até dezesseis WLAN no controlador. A solução de Cisco WLAN pode controlar até dezesseis WLAN para AP de pouco peso. Cada WLAN pode ser atribuído as políticas de segurança originais. Os AP de pouco peso transmitem toda a solução ativa WLAN SSID de Cisco WLAN e reforçam as políticas que você define para cada WLAN.

Termine estas etapas para configurar um WLAN novo e seus parâmetros relacionados:

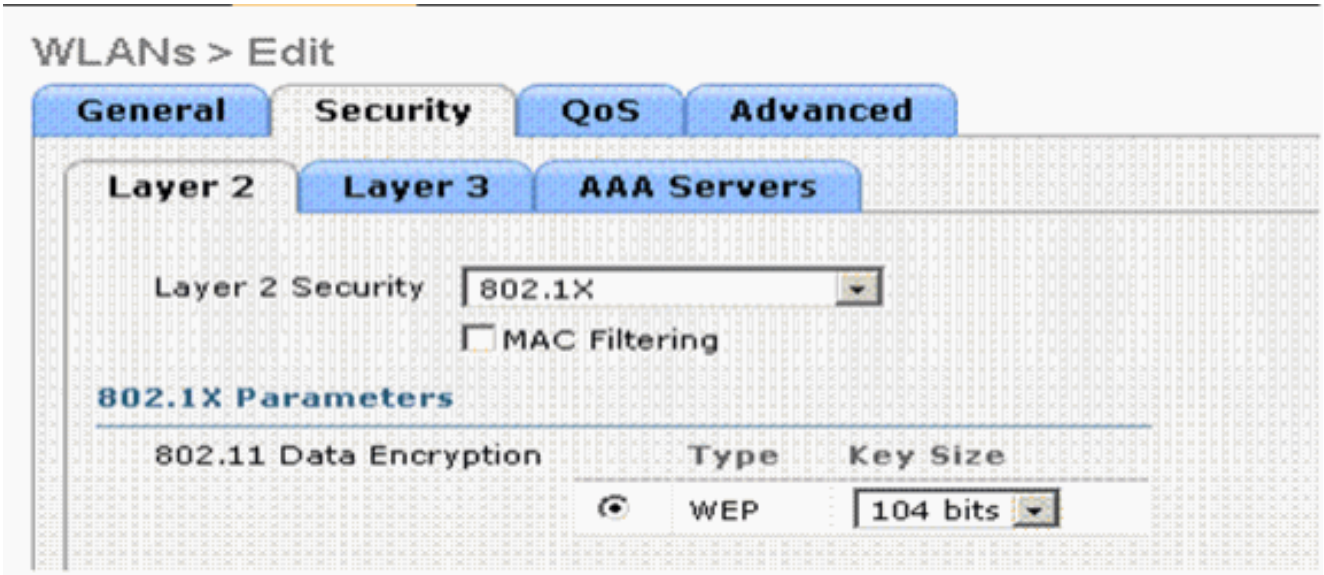
1. Clique **WLAN do** GUI do controlador a fim indicar a página WLAN.Esta página alista os WLAN que existe no controlador.
2. Escolha **novo** a fim criar um WLAN novo. Dê entrada com o nome de perfil e o WLAN SSID para o WLAN e o clique **aplica-se**. Este exemplo usa Cisco como o SSID.

3. 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 que inclui políticas gerais, políticas de segurança, políticas de QoS e outros parâmetros avançados.

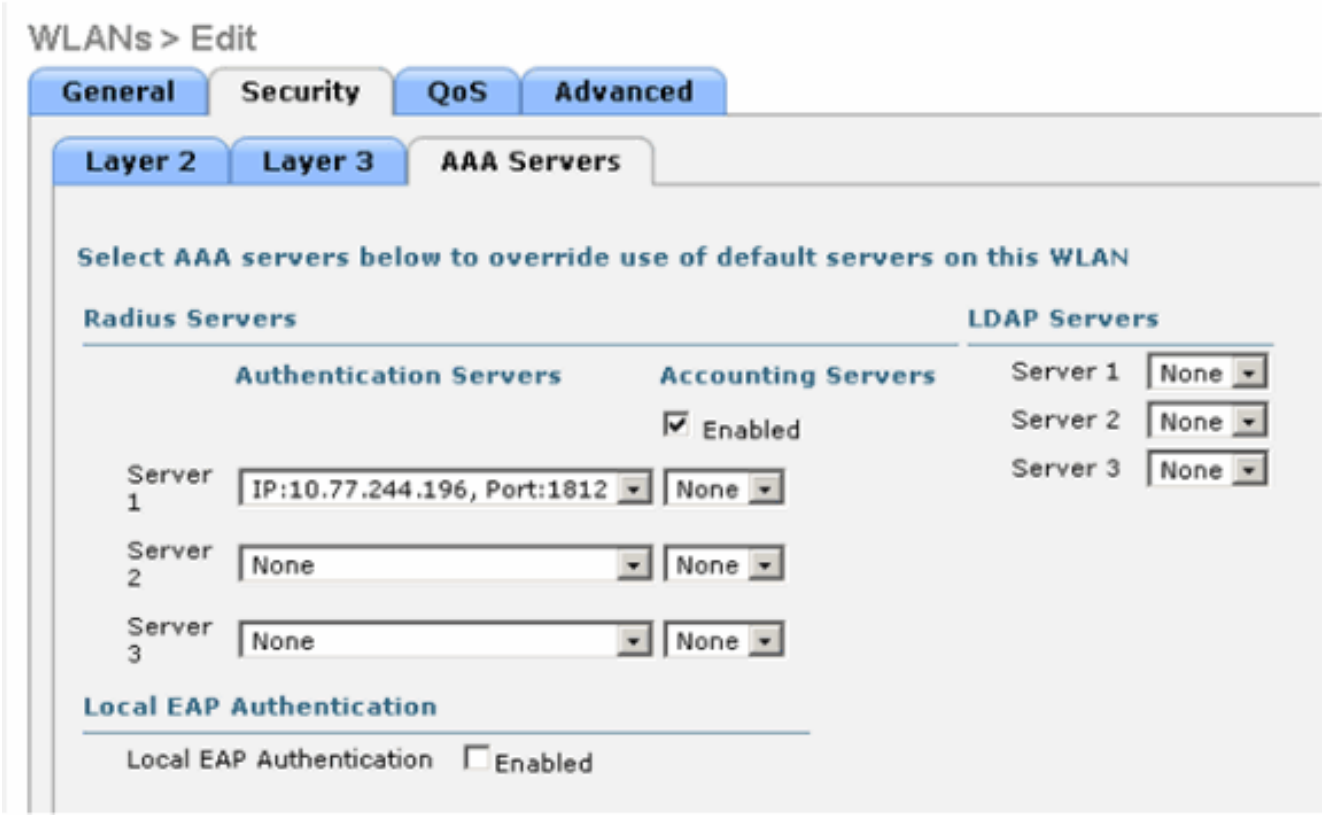



Escolha a relação apropriada do menu suspenso. Os outros parâmetros podem ser alterados basearam na exigência da rede de WLAN.Verifique a caixa do **estado** sob políticas gerais a fim permitir o WLAN.

4. Clique a **ABA de segurança** e escolha a **Segurança da camada 2**. Do menu suspenso da Segurança da camada 2, escolha o **802.1x**. Nos parâmetros do 802.1x, escolha o tamanho da chave de WEP. Este exemplo usa a chave de WEP do 128-bit, que é chave de WEP the104-bit mais o vetor de inicialização 24-
bit.




5. Escolha a aba dos **servidores AAA**. Do menu suspenso dos Authentication Server (RAIO), escolha o servidor Radius apropriado. Este server é usado para autenticar os clientes Wireless.

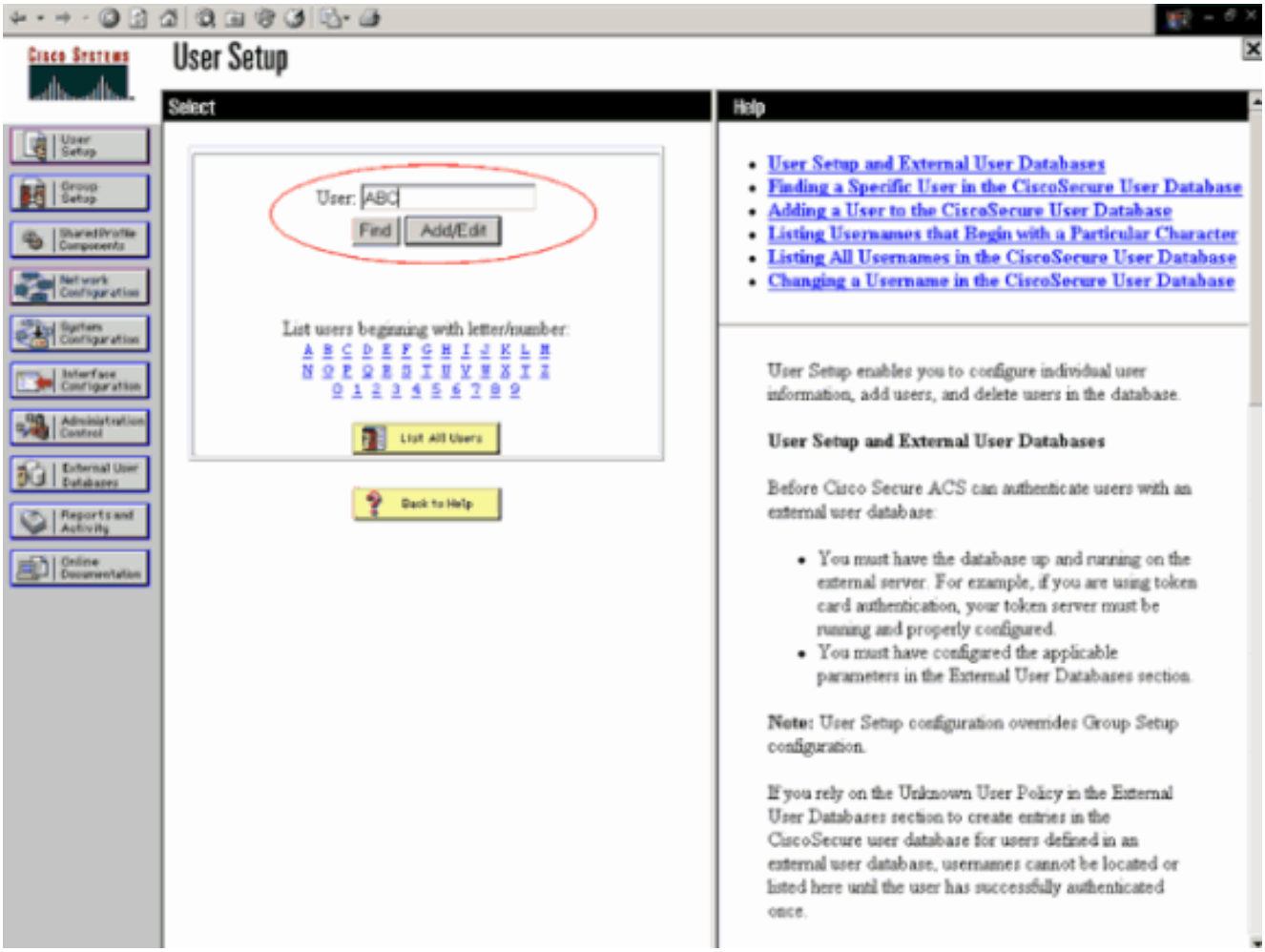



6. O clique **aplica-se** a fim salvar a configuração.

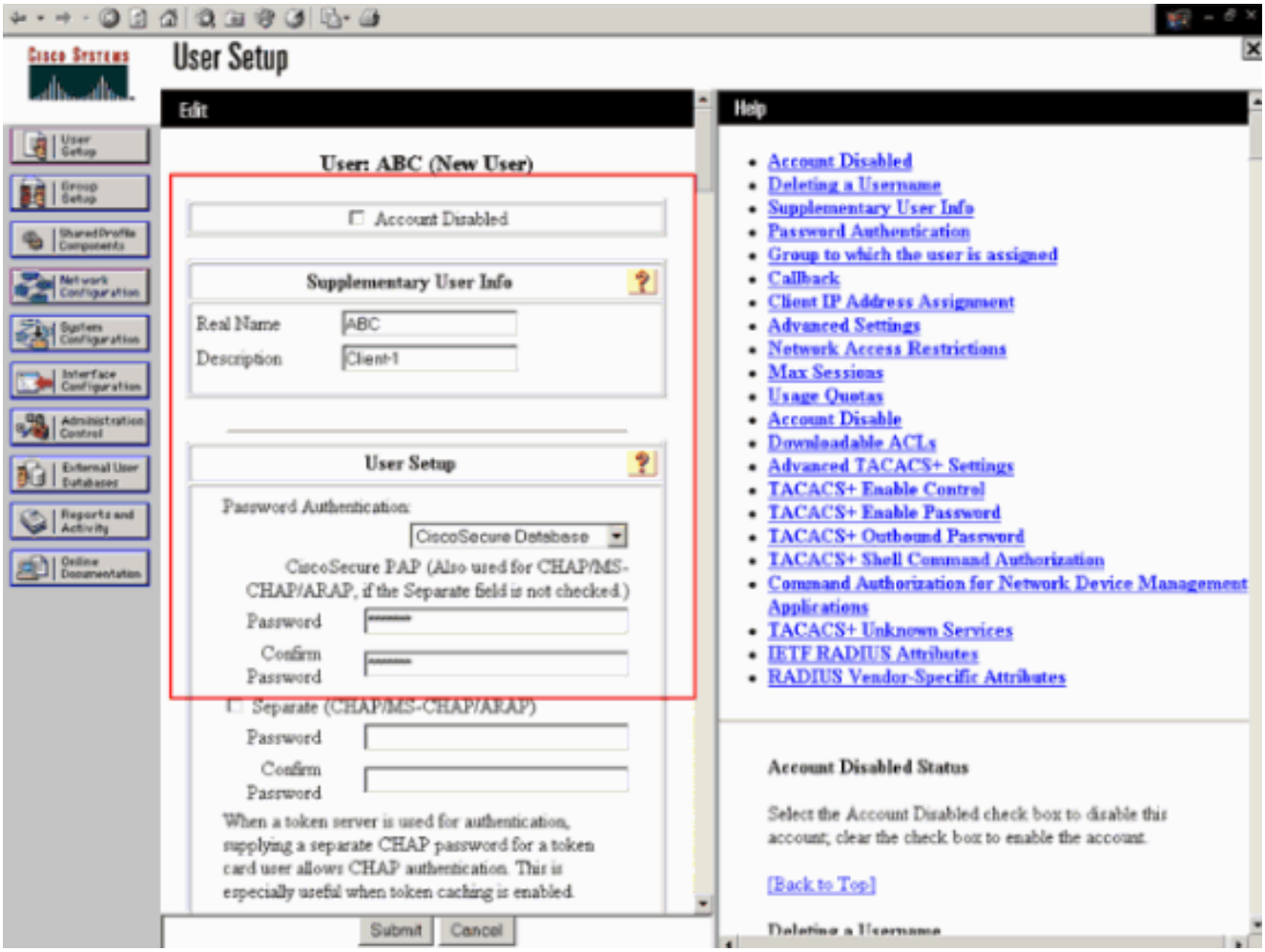
## Configurar o Cisco Secure ACS como o servidor de raio externo e crie uma base de dados de usuário para clientes de autenticação

Termine estas etapas para criar a base de dados de usuário e para permitir a autenticação de EAP no Cisco Secure ACS:

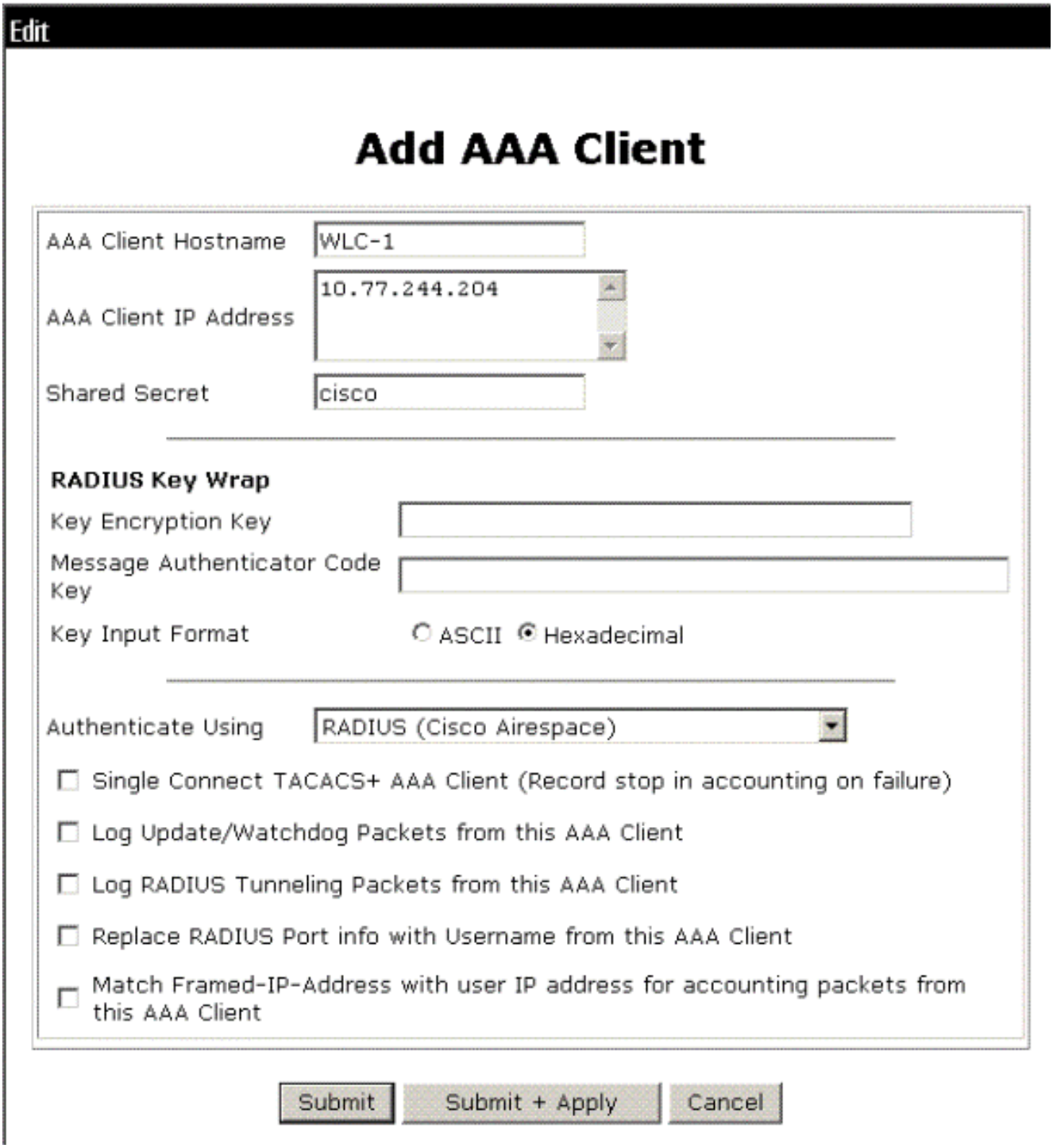
1. Escolha a **instalação de usuário do** ACS GUI, incorpore o username, e o clique **adiciona/edita**. Neste exemplo o usuário é **ABC.**



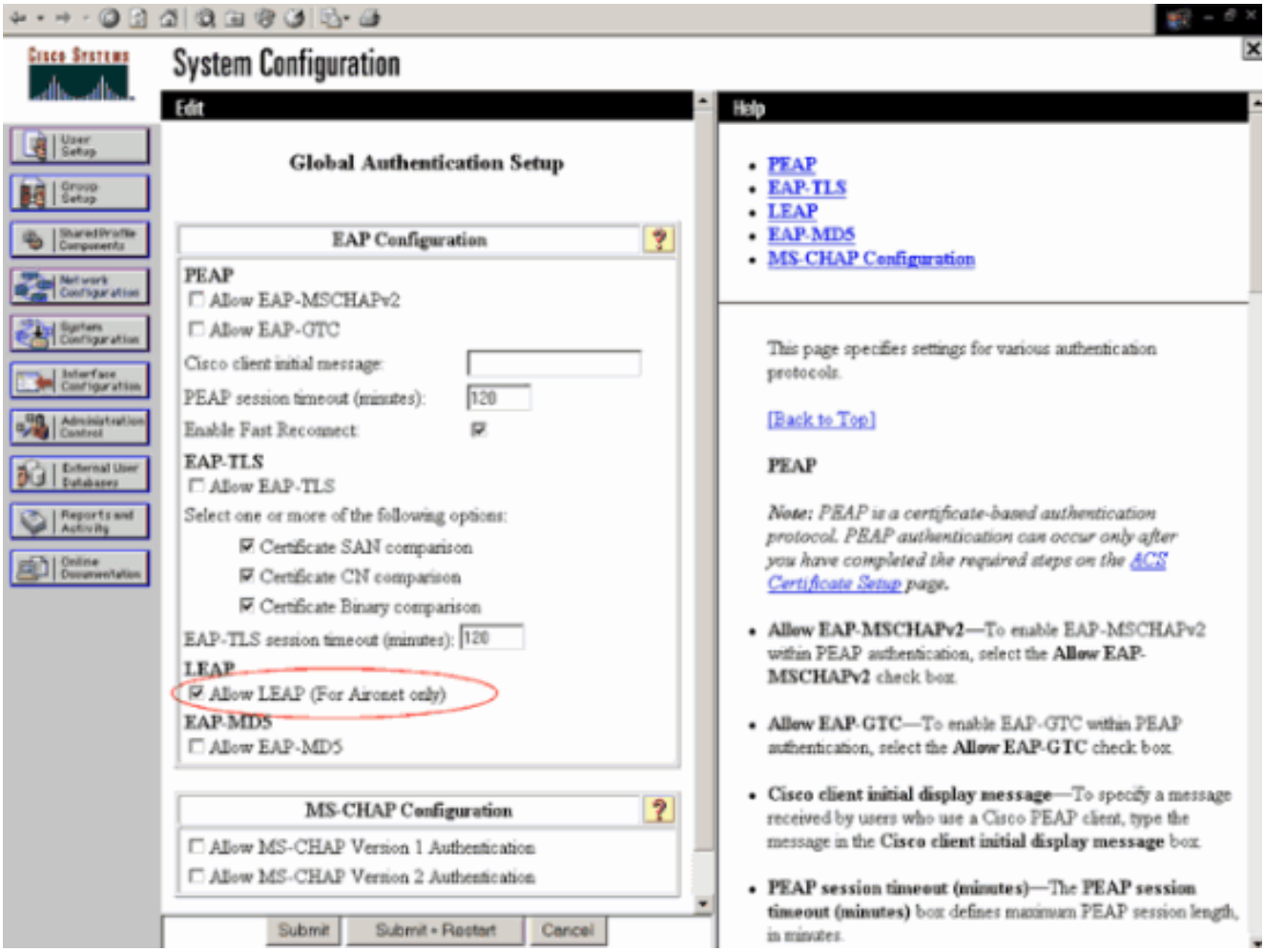

2. Quando a página da instalação de usuário se publica, defina todos os parâmetros específicos ao usuário. Neste exemplo o username, a senha e a informação sobre o usuário suplementar são configurados porque você precisa somente este parâmetros para a autenticação de EAP.Clique **submetem** e repetem o mesmo processo a fim adicionar mais usuários ao base de dados. À revelia todos os usuários são agrupados sob o grupo padrão e atribuídos a mesma política que definidos para o grupo. Refira a seção de gerenciamento do grupo de usuário do Guia do Usuário para o server 3.2 do Cisco Secure ACS for Windows para mais informação se você quer atribuir usuários específicos aos grupos diferentes.




3. Defina o controlador como um cliente de AAA no servidor ACS. Clique a **configuração de rede do** ACS GUI.Quando a página da configuração de rede se publica, defina o nome do WLC, do endereço IP de Um ou Mais Servidores Cisco ICM NT, do segredo compartilhado e do método de autenticação (RAIO 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.




4. **A configuração de sistema** e a **autenticação global do** clique **Setup** a fim assegurar-se de que o Authentication Server esteja configurado para executar o método de autenticação de EAP desejado. Sob os ajustes de configuração EAP, escolha o método de EAP apropriado. Este exemplo usa a autenticação de leap. O clique **submete-se** quando você é feito.

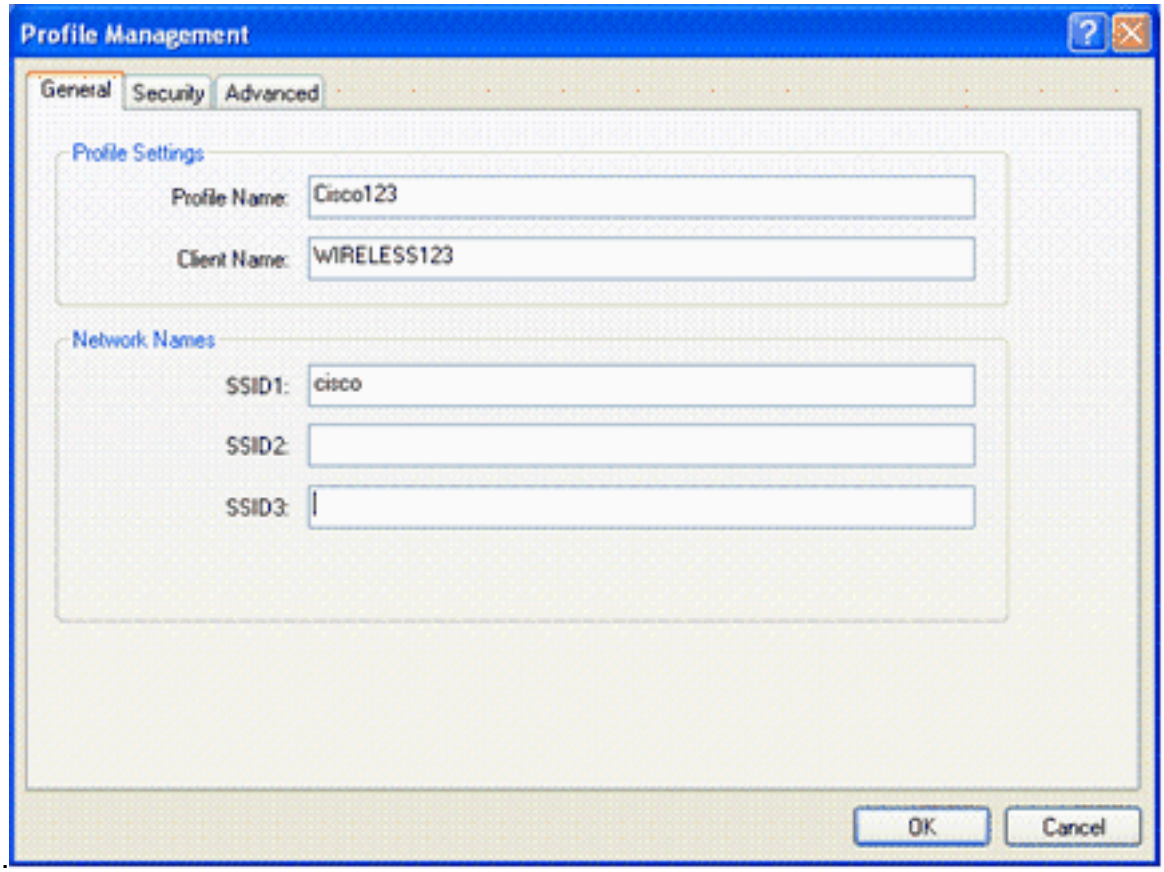



## Configurar o cliente

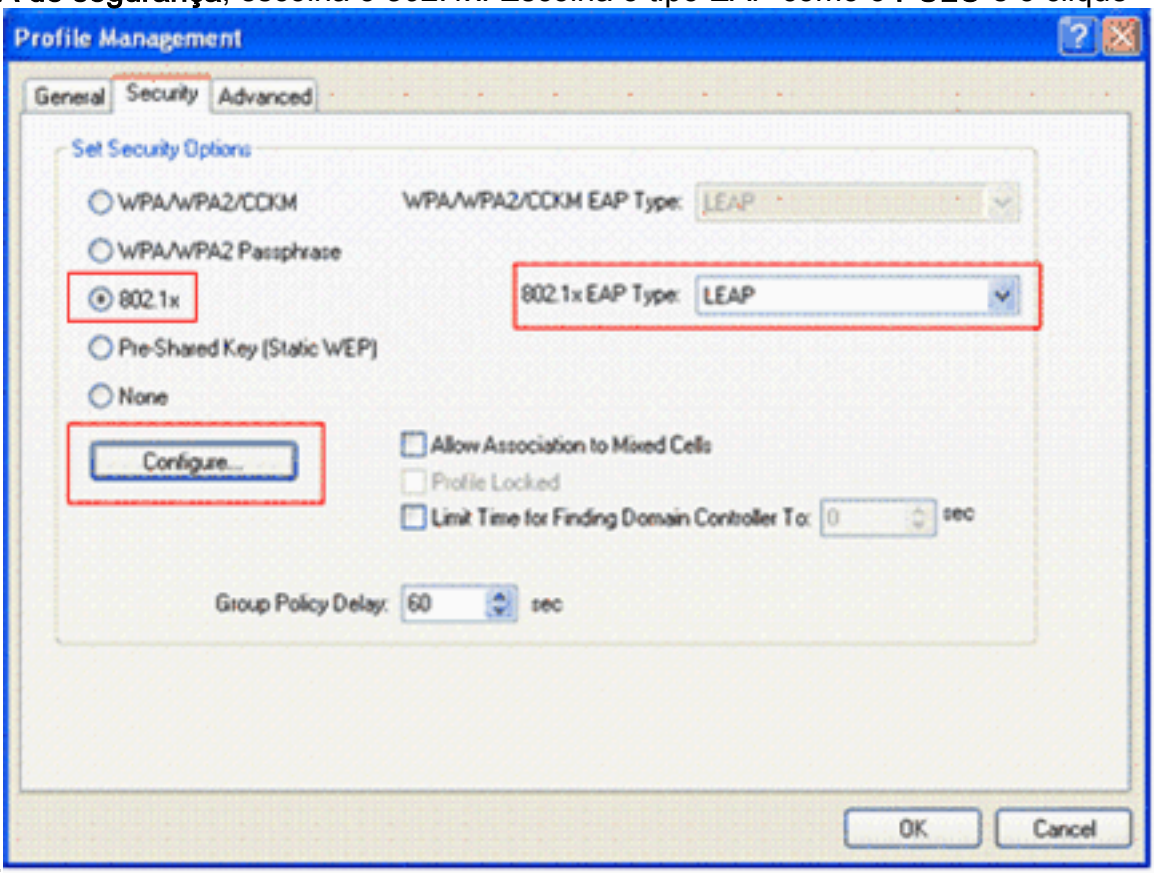
O cliente deve igualmente ser configurado para o tipo apropriado EAP. O cliente propõe o tipo EAP ao server durante o processo de negociação EAP. Se os suportes de servidor que o tipo EAP, ele reconhece o tipo EAP. Se o tipo EAP não é apoiado, envia um reconhecimento negativo e o cliente negocia outra vez com um método de EAP diferente. Este processo continua até que um tipo apoiado EAP esteja negociado. Este exemplo usa o PULO como o tipo EAP.

Termine estas etapas a fim configurar o PULO no cliente com utilitário de Desktop de Aironet.

1. Fazer duplo clique no ícone **de serviço público de Aironet** a fim abri-lo.
2. Clique a aba do **Gerenciamento do perfil**.
3. Clique sobre um perfil e escolha-o **alteram**.
4. Sob o tab geral, escolha um *nome de perfil*. Incorpore o **SSID do**

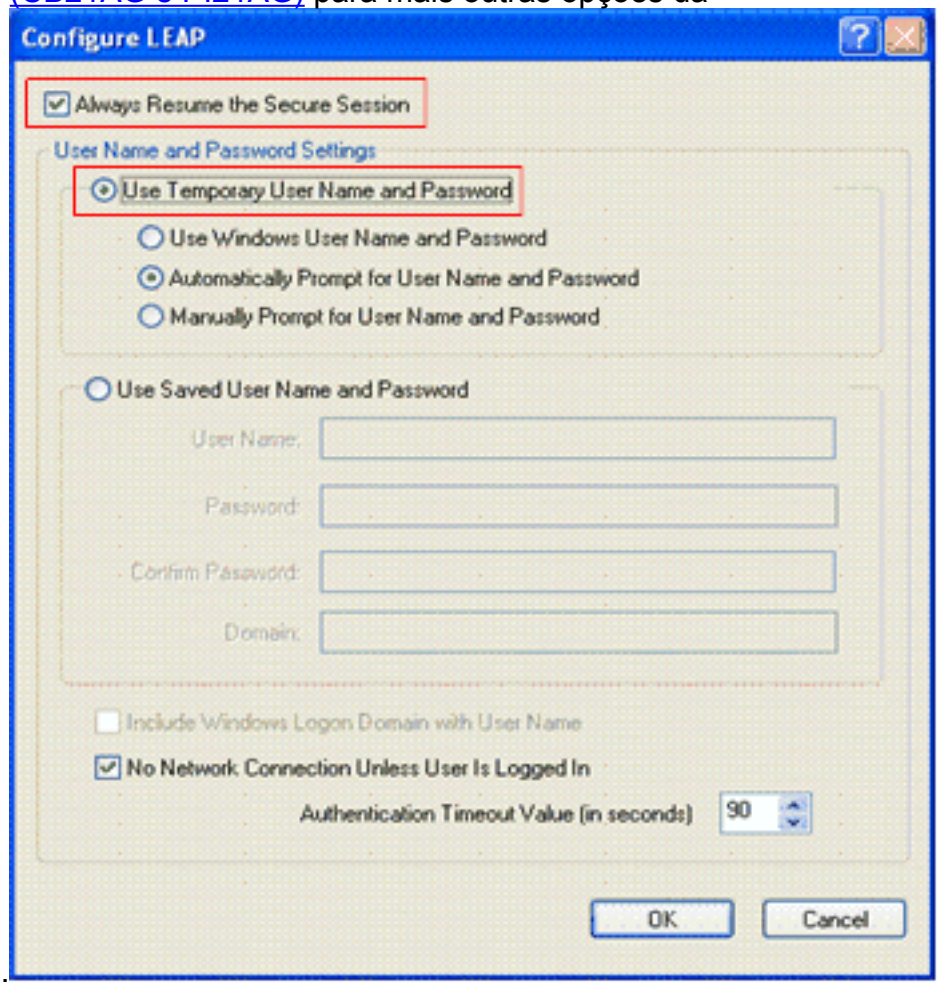
WLAN. 

**Nota:** O SSID é diferenciando maiúsculas e minúsculas e precisa de combinar exatamente com o SSID configurado no WLC.

5. Sob a **ABA de segurança**, escolha o *802.1x*. Escolha o tipo EAP como o **PULO** e o clique **configura**. 

6. Escolha o **nome de usuário e senha provisório do uso**, que o alerta entrar cada vez nos cerdentials do usuário as repartições do computador.Verifique uma das três opções dadas aqui. Este exemplo usa **automaticamente a alerta para o nome de usuário e senha**, que o exige incorporar as credenciais do *usuário LEAP* além do que o *nome de usuário do*

*Windows e a senha* antes que você entre aos indicadores.Verifique **sempre o resumo a** caixa de verificação **segura da sessão na** parte superior do indicador se você quer o suplicante do PULO tentar sempre recomeçar a sessão precedente sem a necessidade do alertar reenter suas credenciais sempre que o adaptador cliente vagueia e reassocia à rede.**Nota:** Refira configurar a seção do adaptador cliente do Guia de Instalação e Configuração dos adaptadores cliente do Wireless LAN do Cisco Aironet 802.11a/b/g do documento (CB21AG e PI21AG) para mais outras opções da




informação.

7. Sob o **guia avançada**, você pode configurar o preâmbulo, a extensão Aironet e as outras opções do 802.11 tais como a potência, frequência e assim por diante.
8. **Aprovação do** clique. O cliente tenta agora associar com os parâmetros configurados.

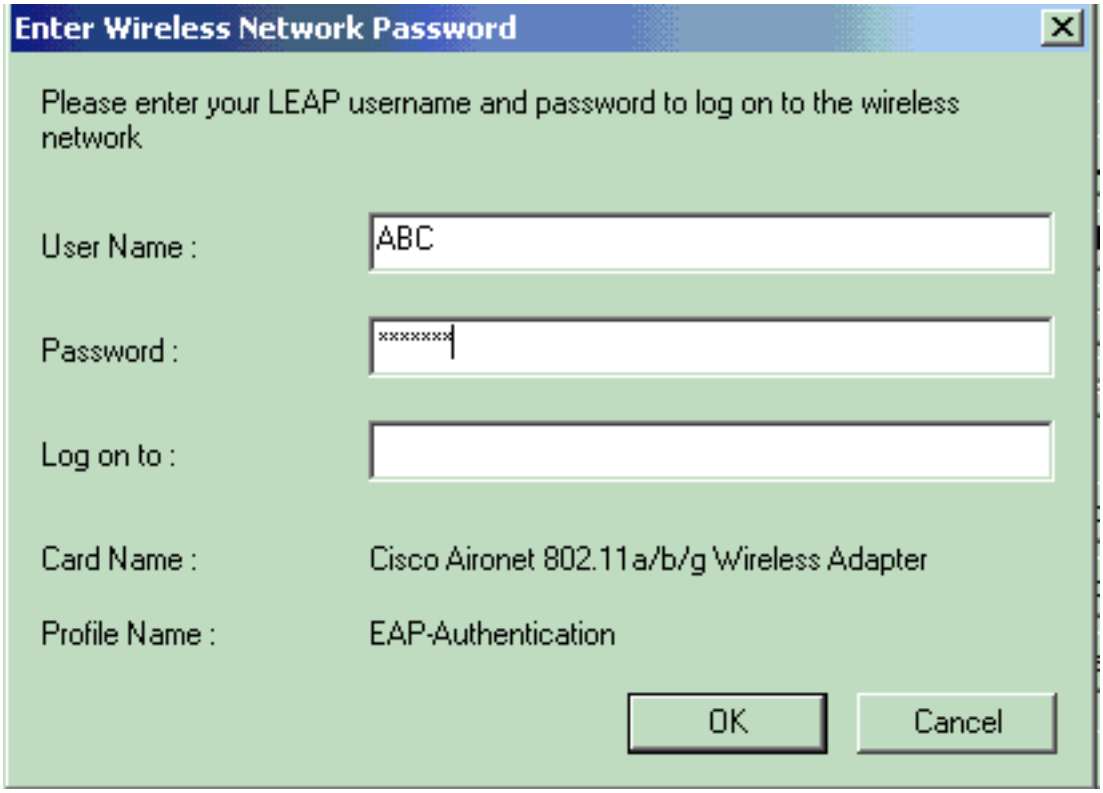
## Verificar

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

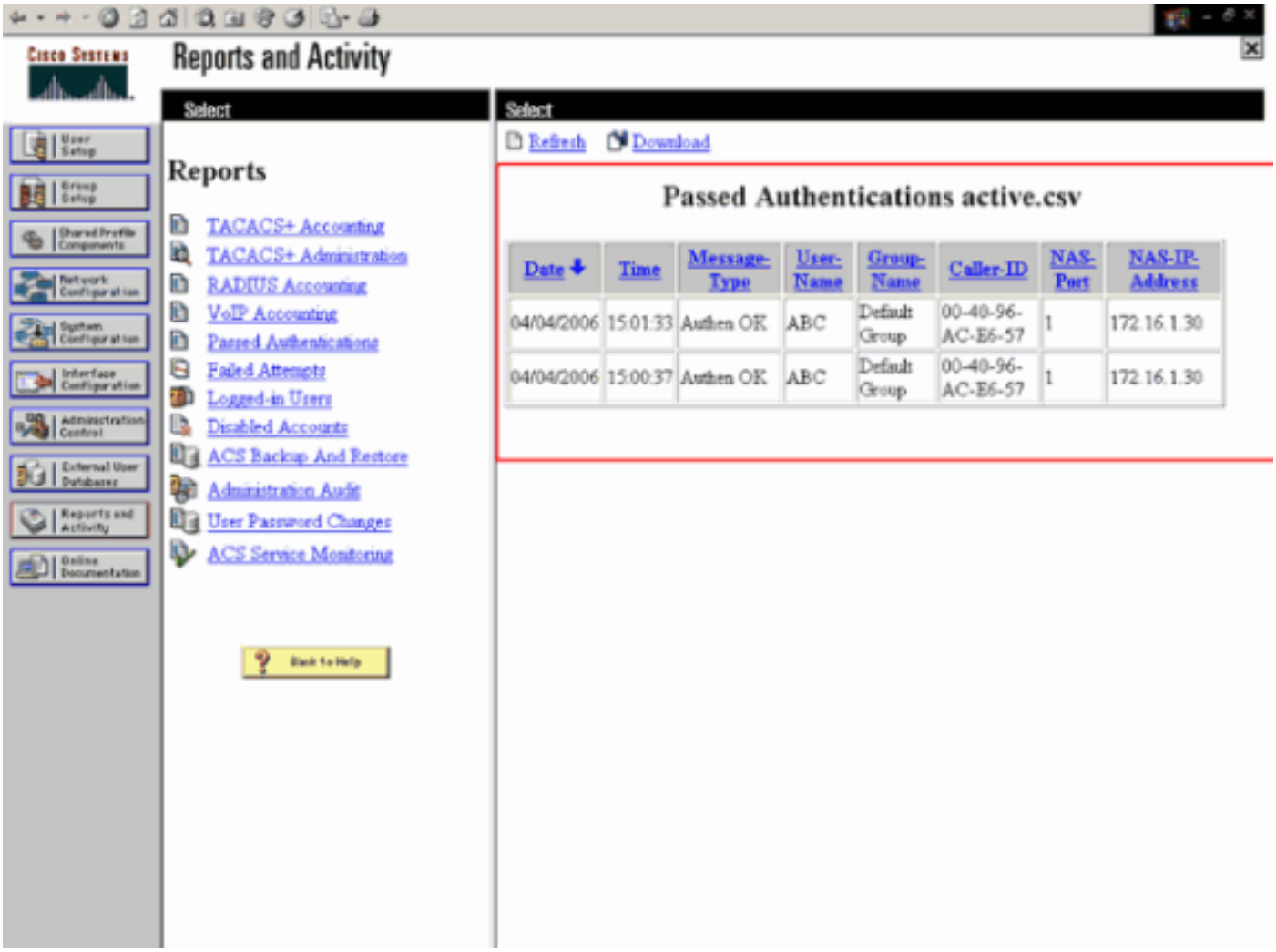
Tente associar um cliente Wireless com o AP de pouco peso usando a autenticação de leap a fim verificar se a configuração trabalha como esperado.

**Nota:** Este documento supõe que o perfil do cliente está configurado para a autenticação de leap. Refira a utilização da autenticação de EAP para obter mais informações sobre de como configurar o adaptador de cliente Wireless do a/b/g do 802.11 para a autenticação de leap.

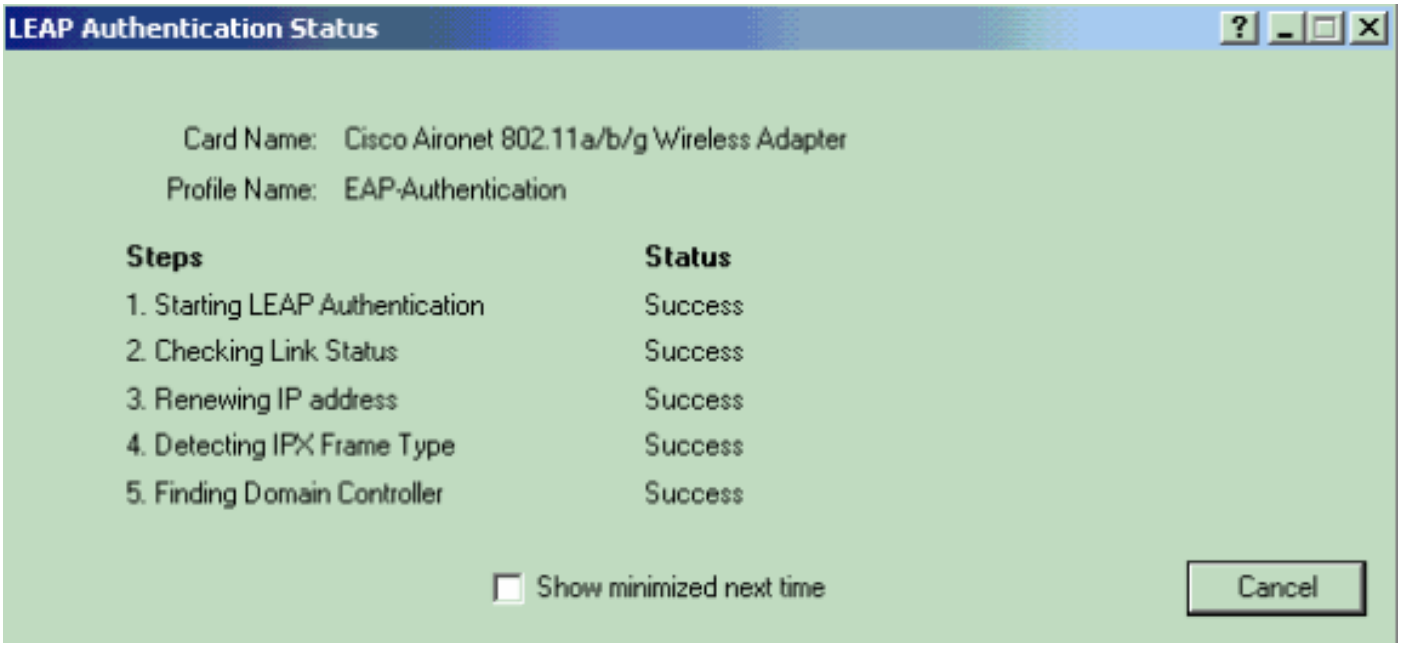
O perfil para o cliente Wireless é ativado uma vez, o usuário é pedido para fornecer o username/senha para a autenticação de leap. Aqui está um exemplo:




O AP de pouco peso e então o WLC passa sobre as credenciais do usuário ao servidor de raio externo (Cisco Secure ACS) a fim validar as credenciais. O servidor Radius compara os dados com a base de dados de usuário e fornece o acesso ao cliente Wireless sempre que as credenciais do usuário são válidas a fim verificar as credenciais do usuário. O relatório passado da autenticação no servidor ACS mostra que o cliente passou a autenticação RADIUS. Aqui está um exemplo:




Em cima da autenticação RADIUS bem sucedida o cliente Wireless associa com o AP de pouco peso.

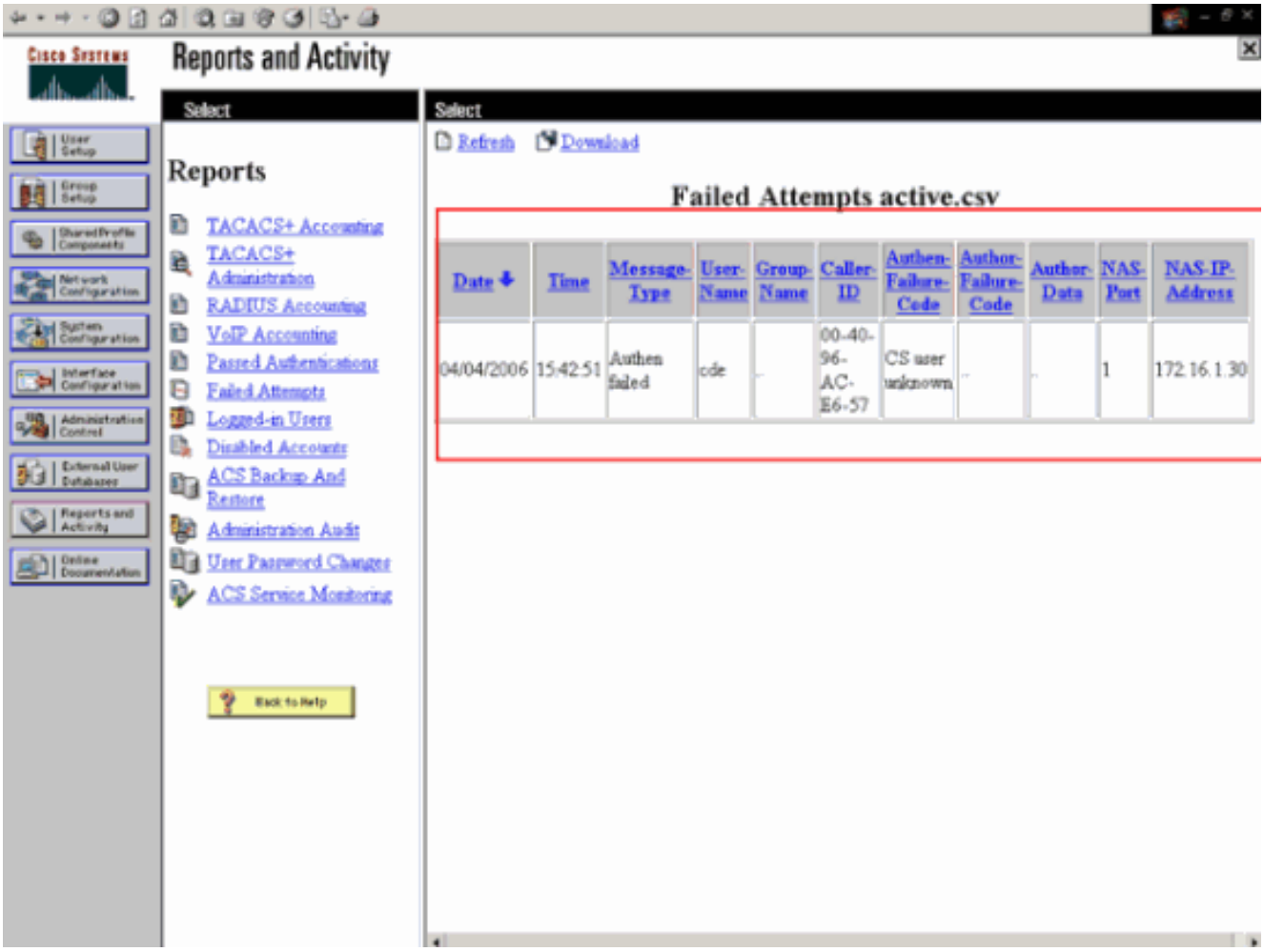



Isto pode igualmente ser verificado sob a aba do **monitor de** WLC GUI. Escolha o **monitor > os clientes** e verifique-os para ver se há o MAC address do cliente.


# Troubleshooting

Termine estas etapas para pesquisar defeitos as configurações:

1. Use o **comando debug lwapp events enable** a fim verificar se o AP se registra com o WLC.
2. Verifique se o servidor Radius recebe e valida o pedido de autenticação do cliente Wireless. Verifique o Nas-ip-address, data e hora a fim verificar se o WLC podia alcançar o servidor Radius.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. Está aqui um exemplo quando a autenticação de servidor Radius falha:




**Nota:** Refira a obtenção da versão e o AAA debuga a informação para o Cisco Secure ACS for Windows para obter informações sobre de como pesquisar defeitos e para obter debugar

a informação no Cisco Secure ACS.

3. Você pode igualmente usar estes **comandos debug** a fim pesquisar defeitos a autenticação de AAA:**debugar o aaa que todos permitem** — Configura debugar de todos os mensagens AAA.**debugar o pacote do dot1x permitem** — Permite debugar de todos os pacotes do dot1x.Está aqui um exemplo de saída do **comando enable aaa do 802.1x debugar**:

```
(Cisco Controller) >debug dot1x aaa enable *Sep 23 15:15:43.792: 00:40:96:ac:dd:05 Adding
AAA_ATT_USER_NAME(1) index=0 *Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding
AAA_ATT_CALLING_STATION_ID(31) index=1 *Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding
AAA_ATT_CALLED_STATION_ID(30) index=2 *Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding
AAA_ATT_NAS_PORT(5) index=3 *Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding
AAA_ATT_NAS_IP_ADDRESS(4) index=4 *Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding
AAA_ATT_NAS_IDENTIFIER(32) index=5 *Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding
AAA_ATT_VAP_ID(1) index=6 *Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding
AAA_ATT_SERVICE_TYPE(6) index=7 *Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding
AAA_ATT_FRAMED_MTU(12) index=8 *Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding
AAA_ATT_NAS_PORT_TYPE(61) index=9 *Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding
AAA_ATT_EAP_MESSAGE(79) index=10 *Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding
AAA_ATT_MESS_AUTH(80) index=11 *Sep 23 15:15:43.794: 00:40:96:ac:dd:05 AAA EAP Packet
created request = 0x1533a288.. !!!! *Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Sending EAP
Attribute (code=2, length=8, id=2) for mobile 00:40:96:ac:dd:05 *Sep 23 15:15:43.794:
00000000: 02 02 00 08 01 41 42 43 .....ABC *Sep 23 15:15:43.794: 00:40:96:ac:dd:05 [BE-req]
Sending auth request to 'RADIUS' (proto 0x140001) *Sep 23 15:15:43.799: 00:40:96:ac:dd:05
[BE-resp] AAA response 'Interim Response' *Sep 23 15:15:43.799: 00:40:96:ac:dd:05 [BE-resp]
Returning AAA response *Sep 23 15:15:43.799: 00:40:96:ac:dd:05 AAA Message 'Interim
Response' received for mobile 00:40:96:ac:dd:05 *Sep 23 15:15:43.799: 00:40:96:ac:dd:05
Received EAP Attribute (code=1, length=19,id=3, dot1xcb->id = 2) for mobile
00:40:96:ac:dd:05 *Sep 23 15:15:43.799: 00000000: 01 03 00 13 11 01 00 08 42 3a 8e d1 18 24
e8 9f ........B:... *Sep 23 15:15:43.799: 00000010: 41 42 43 ABC *Sep 23 15:15:43.799:
00:40:96:ac:dd:05 Skipping AVP (0/80) for mobile 00:40:96:ac:dd:05 *Sep 23 15:15:43.901:
00:40:96:ac:dd:05 Adding AAA_ATT_USER_NAME(1) index=0 *Sep 23 15:15:43.901:
00:40:96:ac:dd:05 Adding AAA_ATT_CALLING_STATION_ID(31) index=1 *Sep 23 15:15:43.901:
00:40:96:ac:dd:05 Adding AAA_ATT_CALLED_STATION_ID(30) index=2 *Sep 23 15:15:43.901:
00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT(5) index=3 *Sep 23 15:15:43.901:
00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IP_ADDRESS(4) index=4 *Sep 23 15:15:43.901:
00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IDENTIFIER(32) index=5 *Sep 23 15:15:43.901:
00:40:96:ac:dd:05 Adding AAA_ATT_VAP_ID(1) index=6 *Sep 23 15:15:43.901: 00:40:96:ac:dd:05
Adding AAA_ATT_SERVICE_TYPE(6) index=7 *Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding
AAA_ATT_FRAMED_MTU(12) index=8 *Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Adding
AAA_ATT_NAS_PORT_TYPE(61) index=9 *Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Adding
AAA_ATT_EAP_MESSAGE(79) index=10 *Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Adding
AAA_ATT_RAD_STATE(24) index=11 *Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Adding
AAA_ATT_MESS_AUTH(80) index=12 *Sep 23 15:15:43.902: 00:40:96:ac:dd:05 AAA EAP Packet
created request = 0x1533a288.. !!!! *Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Sending EAP
Attribute (code=2, length=35, id=3) for mobile 00:40:96:ac:dd:05 *Sep 23 15:15:43.902:
00000000: 02 03 00 23 11 01 00 18 83 f1 5b 32 cf 65 04 ed ...#......[2.e.. *Sep 23
15:15:43.902: 00000010: da c8 4f 95 b4 2e 35 ac c0 6b bd fa 57 50 f3 13 ..O...5..k..WP..
*Sep 23 15:15:43.904: 00000020: 41 42 43 ABC *Sep 23 15:15:43.904: 00:40:96:ac:dd:05 [BE-
req] Sending auth request to 'RADIUS' (proto 0x140001) *Sep 23 15:15:43.907:
00:40:96:ac:dd:05 [BE-resp] AAA response 'Interim Response' *Sep 23 15:15:43.907:
00:40:96:ac:dd:05 [BE-resp] Returning AAA response *Sep 23 15:15:43.907: 00:40:96:ac:dd:05
AAA Message 'Interim Response' received for mobile 00:40:96:ac:dd:05 *Sep 23 15:15:43.907:
00:40:96:ac:dd:05 Received EAP Attribute (code=3, length=4,id=3, dot1xcb->id = 3) for
mobile 00:40:96:ac:dd:05 *Sep 23 15:15:43.907: 00000000: 03 03 00 04 .... *Sep 23
15:15:43.907: 00:40:96:ac:dd:05 Skipping AVP (0/80) for mobile 00:40:96:ac:dd:05 *Sep 23
15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_USER_NAME(1) index=0 *Sep 23 15:15:43.912:
00:40:96:ac:dd:05 Adding AAA_ATT_CALLING_STATION_ID(31) index=1 *Sep 23 15:15:43.912:
00:40:96:ac:dd:05 Adding AAA_ATT_CALLED_STATION_ID(30) index=2 *Sep 23 15:15:43.912:
00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT(5) index=3 *Sep 23 15:15:43.912:
00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IP_ADDRESS(4) index=4 *Sep 23 15:15:43.912:
00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IDENTIFIER(32) index=5 *Sep 23 15:15:43.912:
00:40:96:ac:dd:05 Adding AAA_ATT_VAP_ID(1) index=6 *Sep 23 15:15:43.912: 00:40:96:ac:dd:05
Adding AAA_ATT_SERVICE_TYPE(6) index=7 *Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding
```

```
AAA_ATT_FRAMED_MTU(12) index=8 *Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding
AAA_ATT_NAS_PORT_TYPE(61) index=9 *Sep 23 15:15:43.915: 00:40:96:ac:dd:05 Adding
AAA_ATT_EAP_MESSAGE(79) index=10 *Sep 23 15:15:43.915: 00:40:96:ac:dd:05 Adding
AAA_ATT_RAD_STATE(24) index=11 *Sep 23 15:15:43.915: 00:40:96:ac:dd:05 Adding
AAA_ATT_MESS_AUTH(80) index=12 *Sep 23 15:15:43.915: 00:40:96:ac:dd:05 AAA EAP Packet
created request = 0x1533a288.. !!!! *Sep 23 15:15:43.915: 00:40:96:ac:dd:05 Sending EAP
Attribute (code=1, length=19, id=3) for mobile 00:40:96:ac:dd:05 *Sep 23 15:15:43.915:
00000000: 01 03 00 13 11 01 00 08 29 23 be 84 e1 6c d6 ae ........)#...l.. *Sep 23
15:15:43.915: 00000010: 41 42 43 ABC *Sep 23 15:15:43.915: 00:40:96:ac:dd:05 [BE-req]
Sending auth request to 'RADIUS' (proto 0x140001) *Sep 23 15:15:43.918: 00:40:96:ac:dd:05
[BE-resp] AAA response 'Success' *Sep 23 15:15:43.918: 00:40:96:ac:dd:05 [BE-resp]
Returning AAA response *Sep 23 15:15:43.918: 00:40:96:ac:dd:05 AAA Message 'Success'
received for mobile 00:40:96:ac:dd:05 *Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing
avps[0]: attribute 8, vendorId 0, valueLen 4 *Sep 23 15:15:43.918: 00:40:96:ac:dd:05
processing avps[1]: attribute 79, vendorId 0, valueLen 35 *Sep 23 15:15:43.918:
00:40:96:ac:dd:05 Received EAP Attribute (code=2, length=35,id=3) for mobile
00:40:96:ac:dd:05 *Sep 23 15:15:43.918: 00000000: 02 03 00 23 11 01 00 18 03 66 2c 6a b3 a6
c3 4c ...#.....f,j...L *Sep 23 15:15:43.918: 00000010: 98 ac 69 f0 1b e8 8f a2 29 eb 56 d6
92 ce 60 a6 ..i.....).V...`. *Sep 23 15:15:43.918: 00000020: 41 42 43 ABC *Sep 23
15:15:43.918: 00:40:96:ac:dd:05 processing avps[2]: attribute 1, vendorId 9, valueLen 16
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[3]: attribute 25, vendorId 0,
valueLen 21 *Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[4]: attribute 80,
vendorId 0, valueLen 16
```

**Nota:** Algumas das linhas no resultado do debug foram envolvido devido às limitações do espaço.

4. Monitore entra o WLC a fim verificar se o servidor Radius recebe as credenciais do usuário. Clique o **monitor** a fim verificar os logs do WLC GUI. Do menu do lado esquerdo, clique **estatísticas** e clique o **servidor Radius da** lista de opções.Isto é muito importante porque em alguns casos, o servidor Radius nunca recebe as credenciais do usuário se a configuração de servidor RADIUS no WLC está incorreta.Isto é como os logs aparecem no WLC se os parâmetros radius são configurados incorretamente:


Você pode usar uma combinação do **comando show wlan summary** a fim reconhecer quais de seus WLAN empregam a autenticação de servidor Radius. Então você pode ver o **comando show client summary** a fim ver que endereços MAC (clientes) são autenticados com sucesso no RAIO WLAN. Você pode igualmente correlacionar este com seu Cisco Secure ACS passado tentativas ou logs das falhas de tentativa.

## Dicas para Troubleshooting

- Verifique no controlador que o servidor Radius está no estado `ativo`, e não no `apoio` ou `desabilitado`.
- Use o **comando ping** a fim verificar se o servidor Radius é alcançável do WLC.

- Verifique se o servidor Radius é selecionado do menu de gota para baixo do WLAN (SSID).
- Se você usa o WPA, a seguir você tem que instalar a correção dinâmica de WPA a mais atrasada de Microsft para Windows XP SP2. Também, você deve promover o direcionador para seu suplicante do cliente ao mais atrasado.
- Se você faz o PEAP, por exemplo Certificados com XP, o SP2 onde os cartões são controlados pela utilidade de Microsoft wireless-0, você precisa de obter a correção de programa KB885453 de Microsoft.Se você usa a configuração de Windows/suplicante zero do cliente, o desabilitação **permite reconecta rapidamente**. Você pode fazer este se você escolhe **propriedades > redes Wireless de conexão de rede Wireless > redes preferidas**. Escolha então **SSID > propriedades > aberto > WEP > autenticação > tipo EAP > PEAP > propriedades > permitem reconectam rapidamente**. Você pode então encontrar a opção para permitir ou desabilitar na extremidade do indicador.
- Se você tem cartões de Intel 2200 ou 2915, refira as indicações no Web site de Intel sobre os problemas conhecidos com seus cartões:Conexão de rede de Intel® PRO/Wireless 2200BGConexão de rede de Intel® PRO/Wireless 2915ABGTransfira os direcionadores os mais atuais de Intel a fim evitar todas as edições. Você pode transferir direcionadores de Intel em http://downloadcenter.intel.com/
- Se o recurso **failover agressivo** estiver habilitado na WLC, a WLC será muito agressiva para marcar o servidor AAA como não respondendo. Mas, isto não deve ser feito porque o servidor AAA não é possivelmente responsivo somente a esse cliente específico, se você faz o descarte silencioso. Pode ser uma resposta a outros clientes válidos com certificados válidos. Mas, o WLC pode ainda marcar o servidor AAA como `não respondendo` e `não funcional`.Para resolver isso, desabilite o recurso de **failover agressivo**. Execute o comando **config radius aggressive-failover disable** na GUI da controladora para fazer isso. Se isto é desabilitado, a seguir o controlador falha somente sobre ao servidor AAA seguinte se há três clientes consecutivos que não recebem uma resposta do servidor Radius.

## Temporizadores de manipulação EAP

Durante a autenticação do 802.1x, o usuário pôde ver o `DOT1X-1-MAX_EAPOL_KEY_RETRANS_FOR_MOBILE: As retransmissões da EAPOL-chave M1 MAX alcançaram para o móbil xx: xx: xx: xx:` Mensagem de Erro `xx`.

Este os Mensagens de Erro indicam que o cliente não respondeu a tempo ao controlador durante a negociação da chave WPA (802.1x). O controlador ajusta um temporizador para uma resposta durante a negociação chave. Tipicamente, quando você vê esta mensagem, é devido a uma edição com o suplicante. Certifique-se de que você executa as versões as mais atrasadas dos driveres de cliente e do firmware. No WLC, há alguns temporizadores EAP que você pode manipular para ajudar com authenticação do cliente. Estes temporizadores EAP incluem:

```
EAP-Identity-Request Timeout
EAP-Identity-Request Max Retries
EAP-Request Timeout (seconds)
EAP-Request Max Retries
EAPOL-Key Timeout
EAPOL-Key Max Retries
```

Antes que você possa manipular estes valores, você precisa de compreender o que faz, e como o mudar impactará a rede:

- **Intervalo do EAP-Identidade-pedido:**Influências deste temporizador quanto tempo você

espera entre pedidos da identidade EAP. À revelia, este é segundo (4.1 e mais baixo) e 30 segundos (4.2 e maior). A razão para esta mudança era porque alguns clientes, helds da mão, telefones, varredores etc., tiveram uma dificuldade que responde rapidamente bastante. Os dispositivos como portáteis, geralmente não exigem uma manipulação destes valores. O valor disponível é 1 a 120.Assim, que acontece quando este atributo é ajustado a um valor de 30? Quando o cliente conecta primeiramente, envia um começo EAPOL à rede, e o WLC envia abaixo de um pacote EAP, pedindo a identidade do usuário ou da máquina. Se o WLC não recebe a resposta da identidade, envia a um outro pedido da identidade 30 segundos após os primeiros. Isto acontece na conexão inicial, e quando o cliente vaguear.Que acontece quando nós aumentamos este temporizador? Se tudo é bom, não há nenhum impacto. Contudo, se há uma edição na rede (que inclui problemas de cliente, edições AP, ou edições RF), pode causar atrasos na conectividade de rede. Por exemplo, se você ajusta o temporizador ao valor máximo de 120 segundos, o WLC espera 2 minutos entre pedidos da identidade. Se o cliente está vagueando, e a resposta não é recebida pelo WLC, a seguir nós criamos, pelo menos, uma indisponibilidade de dois-minuto para este cliente.As recomendações para este temporizador são *5.* Neste tempo, não há nenhuma razão colocar este temporizador em seu valor máximo.

- **Retries máximo do EAP-Identidade-pedido:**O valor de Retries máximo é o número de vezes que o WLC enviará o pedido da identidade ao cliente, antes de remover sua entrada do MSCB. Uma vez que o Retries máximo é alcançado, o WLC envia um quadro da de-autenticação ao cliente, forçando os para reiniciar o processo EAP. O valor disponível é 1 a 20. Em seguida, nós olharemos este com maiores detalhes.O Retries máximo trabalha com o intervalo da identidade. Se você tem seu intervalo da identidade ajustado a 120, e seu Retries máximo a 20 quanto tempo faz ele toma 2400 (ou 120 * 20). Isto significa que tomaria 40 minutos para que o cliente esteja removido, e começaria o processo EAP sobre outra vez. Se você ajusta o intervalo da identidade a 5, com um valor de Retries máximo de 12, a seguir ele tomará 60 (ou 5 * 12). Em contraste com o exemplo anterior, há um minuto até que o cliente esteja removido e tiver que começar o EAP sobre.As recomendações para o Retries máximo são *12*.
- **Intervalo da EAPOL-chave:**Para o valor de timeout da EAPOL-chave, o padrão é 1 segundo ou 1000 milissegundos. Isto significa que quando as chaves EAPOL são trocadas entre o AP e o cliente, o AP enviará a chave e a espera até 1 segundo à revelia para que o cliente responda. Após ter esperado o valor de horário definido, o AP retransmitirá a chave outra vez. Você pode usar o comando **avançado configuração do** *<time> do EAPOL-chave-* **intervalo do eap** a fim alterar este ajuste. Os valores disponíveis em 6.0 realizam-se entre 200 e 5000 milissegundos, quando os códigos antes de 6.0 permitirem valores entre 1 e segundos 5. Mantenha na mente que se você tem um cliente que não esteja respondendo a uma tentativa chave, estendendo os temporizadores para fora pode lhes dar um pouco de mais hora de responder. Contudo, isto poderia igualmente prolongar o tempo onde toma para o WLC/AP ao deauthenticate o cliente para que o processo inteiro do 802.1x comece de novo.
- **Retries máximo da EAPOL-chave:**Para o valor de Retries máximo da EAPOL-chave, o padrão é 2. Isto significa que nós experimentaremos de novo a tentativa chave original ao cliente duas vezes. Este ajuste pode ser alterado usando o comando **avançado configuração do** *<retries> do EAPOL-chave-***Retries do eap**. Os valores disponíveis estão entre 0 e 4 novas tentativas. Usando o valor padrão para o intervalo da EAPOL-chave (isto é, 1 segundo) e o valor padrão para a nova tentativa da EAPOL-chave (2) o processo iria como segue se um cliente não responde à tentativa chave inicial:O AP envia uma tentativa chave ao

cliente.Espera o segundo por uma resposta.Se não há nenhuma resposta, a seguir a primeira nova tentativa da EAPOL-chave está enviada.Espera o segundo por uma resposta.Se não há nenhuma resposta, a seguir a segunda nova tentativa da EAPOL-chave está enviada.Se não há ainda nenhuma resposta do cliente e o valor de nova tentativa está encontrado, a seguir o cliente deauthenticated. Além disso, como com o intervalo da EAPOL-chave, estender o valor de nova tentativa da EAPOL-chave podia, em algumas circunstâncias, ser benéfico. Contudo, ajustá-lo ao máximo pode outra vez ser prejudicial porque a mensagem do deauthenticate seria prolongada.

### Extraindo o arquivo de pacote do servidor Radius ACS para pesquisar defeitos

Se você usa o ACS como o servidor de raio externo, esta seção pode ser usada para pesquisar defeitos sua configuração. O package.cab é um arquivo zip que contenha todos os arquivos necessários necessários a fim pesquisar defeitos eficientemente o ACS. Você pode usar o utilitário CSSupport.exe para criar o package.cab ou pode obter os arquivos manualmente.

Refira a criação de uma seção de arquivo do package.cab de ObtainingVersion *e o AAA debuga a informação para o Cisco Secure ACS for Windows para obter mais informações sobre de* como criar e extrair o arquivo de pacote do WCS.

## Informações Relacionadas

- Failover do controlador de WLAN para o exemplo de configuração do Lightweight Access Points
- Atualização do software do Wireless LAN Controller (WLC)
- Referência de comandos do controlador de LAN do Cisco Wireless
- Suporte Técnico e Documentação - Cisco Systems