Configurar a autenticação EAP com controladores WLAN (WLC)

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Conventions](#)
[Configurar](#)
[Diagrama de Rede](#)
[Configurar a WLC para Operação Básica e Registrar os APs Lightweight no Controlador](#)
[Configurar a WLC para autenticação RADIUS através de um servidor RADIUS externo](#)
[Configurar parâmetros de WLAN](#)
[Configure o Cisco Secure ACS como o servidor RADIUS externo e crie um banco de dados de usuário para clientes de autenticação](#)
[Configurar o cliente](#)
[Verificar](#)
[Troubleshoot](#)
[Dicas para Troubleshooting](#)
[Manipular temporizadores EAP](#)
[Extraindo o arquivo de pacote do servidor ACS RADIUS para solução de problemas](#)
[Informações Relacionadas](#)

Introduction

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 Cisco Secure Access Control Server (ACS) como o servidor RADIUS externo para validar as credenciais do usuário.

Prerequisites

Requirements

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

- Conhecimento básico da configuração de access points (APs) Lightweight e WLCs da Cisco.
- Conhecimento básico do Lightweight AP Protocol (LWAPP).
- Conhecimento de como configurar um servidor RADIUS externo como o Cisco Secure ACS.

Componentes Utilizados

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

- AP leve Cisco Aironet 1232AG Series
- Cisco 4400 Series WLC que executa o firmware 5.1
- Cisco Secure ACS que executa a versão 4.1
- Adaptador de cliente Cisco Aironet 802.11 a/b/g
- Cisco Aironet Desktop Utility (ADU) que executa o firmware 4.2

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.

Configurar

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

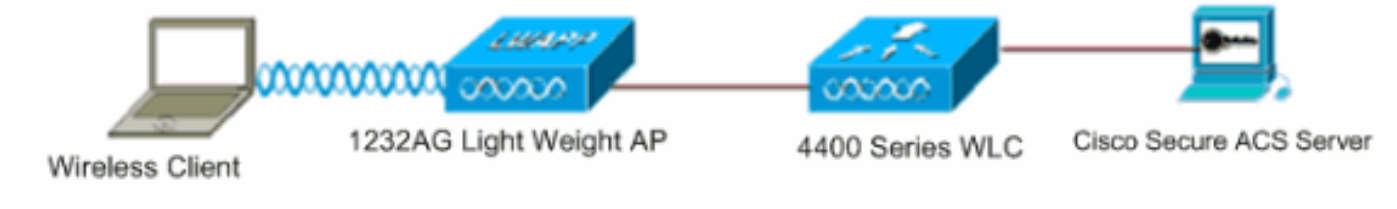
Observação: use a Command Lookup Tool (somente clientes registrados) para encontrar mais informações sobre os comandos usados neste documento.

Conclua estes passos para configurar os dispositivos para autenticação EAP:

1. Configure a WLC para operação básica e registre os APs Lightweight na controladora.
2. Configure a WLC para autenticação RADIUS através de um servidor RADIUS externo.
3. Configure os parâmetros da WLAN.
4. Configure o Cisco Secure ACS como o servidor RADIUS externo e crie um banco de dados de usuário para autenticar clientes.

Diagrama de Rede

Nessa configuração, uma WLC Cisco 4400 e um AP leve são conectados por meio de um hub. Um servidor RADIUS externo (Cisco Secure ACS) também está conectado ao mesmo hub. Todos os dispositivos estão na mesma sub-rede. O AP é inicialmente registrado no controlador. Você deve configurar a WLC e o AP para a autenticação LEAP (Lightweight Extensible Authentication Protocol). Os clientes que se conectam ao AP usam a autenticação LEAP para se associar ao AP. O Cisco Secure ACS é usado para executar a autenticação RADIUS.



Configurar a WLC para Operação Básica e Registrar os APs Lightweight no Controlador

Use o assistente de configuração de inicialização na interface de linha de comando (CLI) para configurar a WLC para a operação básica. Como alternativa, você também pode usar a GUI para configurar a WLC. Este documento explica a configuração na WLC com o assistente de configuração de inicialização na CLI.

Depois que a WLC é inicializada pela primeira vez, ela entra diretamente no assistente de configuração de inicialização. Use o assistente de configuração para definir as configurações básicas. Você pode executar o assistente na CLI ou na GUI. Esta saída mostra um exemplo do assistente de configuração de inicialização na 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..
```

Esses parâmetros configuram a WLC para a operação básica. Neste exemplo de configuração, a WLC usa 10.77.244.204 como o endereço IP da interface de gerenciamento e 10.77.244.205 como o endereço IP da interface do gerenciador de AP.

Antes que qualquer outro recurso possa ser configurado nas WLCs, os APs Lightweight devem se registrar na WLC. Este documento supõe que o AP Lightweight está registrado no WLC. Consulte o Registro de AP Lightweight (LAP) em uma Controladora de LAN Wireless (WLC) para obter mais informações sobre como os APs Lightweight se registram na WLC.

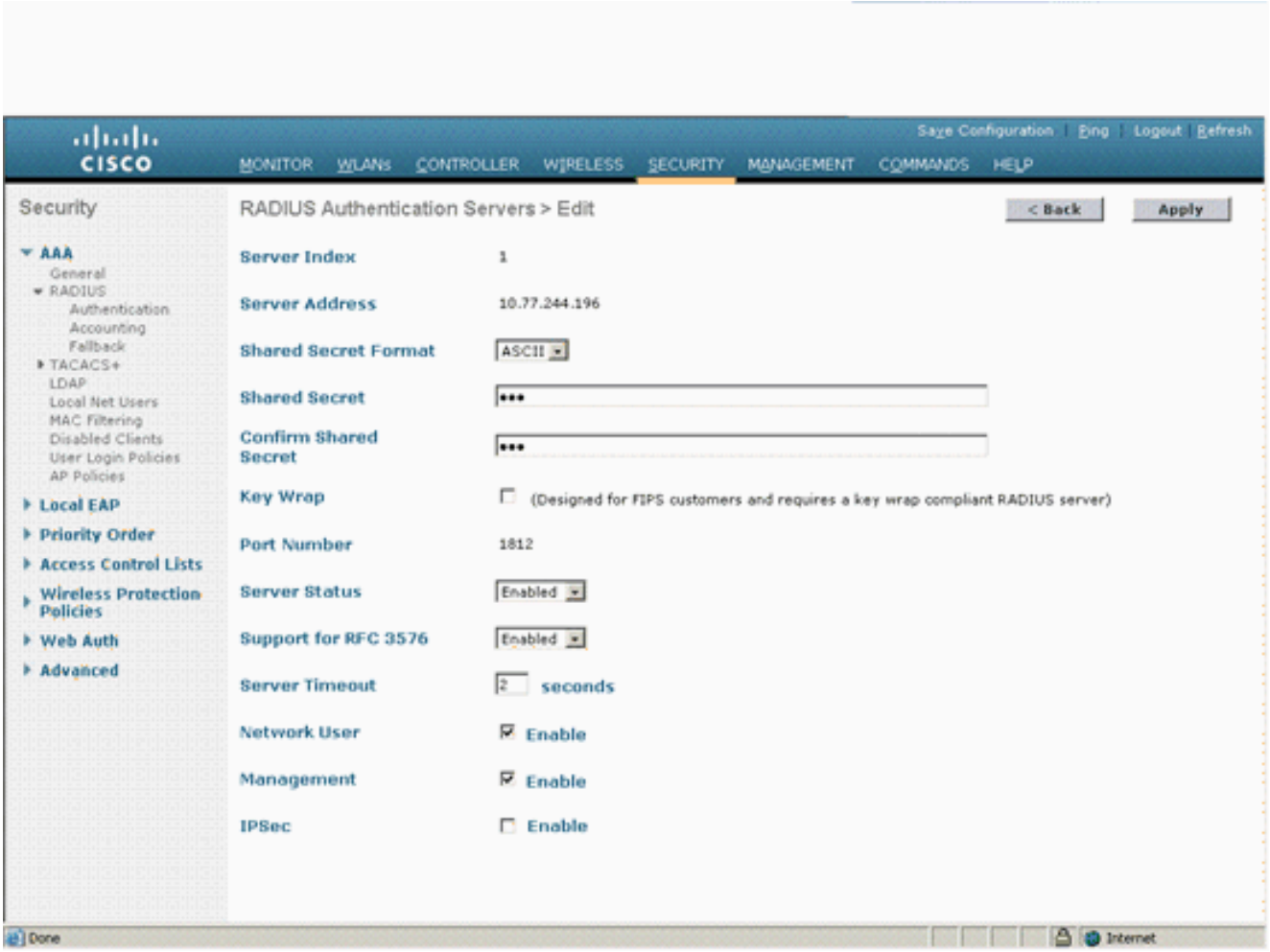
Configurar a WLC para autenticação RADIUS através de um servidor RADIUS externo

A WLC precisa ser configurada para encaminhar as credenciais do usuário a um servidor

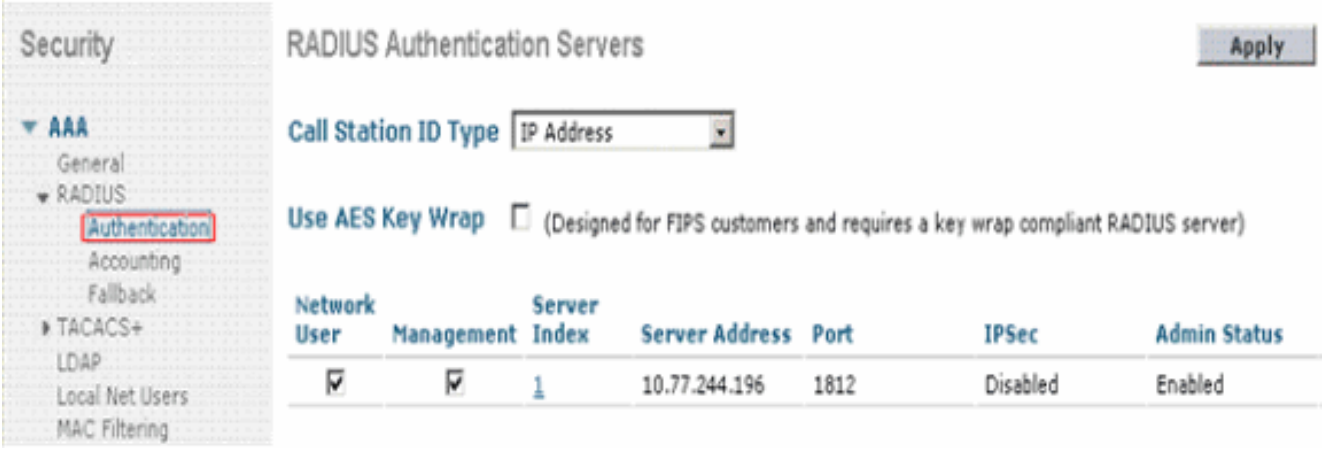
RADIUS externo. O servidor RADIUS externo valida as credenciais do usuário e fornece acesso aos clientes sem fio.

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

1. Escolha **Segurança** e **Autenticação RADIUS** na GUI do controlador para exibir a página Servidores de Autenticação RADIUS. Em seguida, clique em **New** para definir um servidor RADIUS.



2. Defina os parâmetros do servidor RADIUS na página RADIUS Authentication Servers > New. Esses parâmetros incluem o endereço IP do servidor RADIUS, o segredo compartilhado, o número da porta e o status do servidor.As caixas de seleção Network User and Management determinam se a autenticação baseada em RADIUS se aplica ao gerenciamento de WLC e aos usuários da rede. Este exemplo usa o Cisco Secure ACS como o servidor RADIUS com endereço IP 10.77.244.196.
3. O servidor Radius agora pode ser usado pela WLC para autenticação. Você pode encontrar o servidor Radius listado se escolher **Security > Radius > Authentication**.



O RFC 3576 é suportado no servidor RADIUS do Cisco CNS Access Registrar (CAR), mas não no Cisco Secure ACS Server versão 4.0 e anterior.Você também pode usar o recurso de servidor RADIUS local para autenticar usuários. O servidor RADIUS local foi introduzido com o código da versão 4.1.171.0. As WLCs que executam versões anteriores não têm o recurso de raio local. O EAP local é um método de autenticação que permite que usuários e clientes sem fio sejam autenticados localmente. Ele foi projetado para uso em escritórios remotos que desejam manter a conectividade com clientes sem fio quando o sistema de backend for interrompido ou o servidor de autenticação externo cair. O EAP local recupera as credenciais do usuário do banco de dados de usuário local ou do banco de dados de back-end LDAP para autenticar usuários. O EAP local suporta LEAP, EAP-FAST com PACs, EAP-FAST com certificados e autenticação EAP-TLS entre o controlador e os clientes sem fios.O EAP local é projetado como um sistema de autenticação de backup. Se algum servidor RADIUS estiver configurado no controlador, o controlador tentará autenticar os clientes sem fio com os servidores RADIUS primeiro. O EAP local é tentado somente se nenhum servidor RADIUS for encontrado, porque os servidores RADIUS excederam o tempo limite ou nenhum servidor RADIUS foi configurado.Consulte Autenticação EAP Local no Controlador de LAN Wireless com Exemplo de Configuração de Servidor EAP-FAST e LDAP para obter mais informações sobre como configurar o EAP Local em Controladores de LAN Wireless.

Configurar parâmetros de WLAN

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

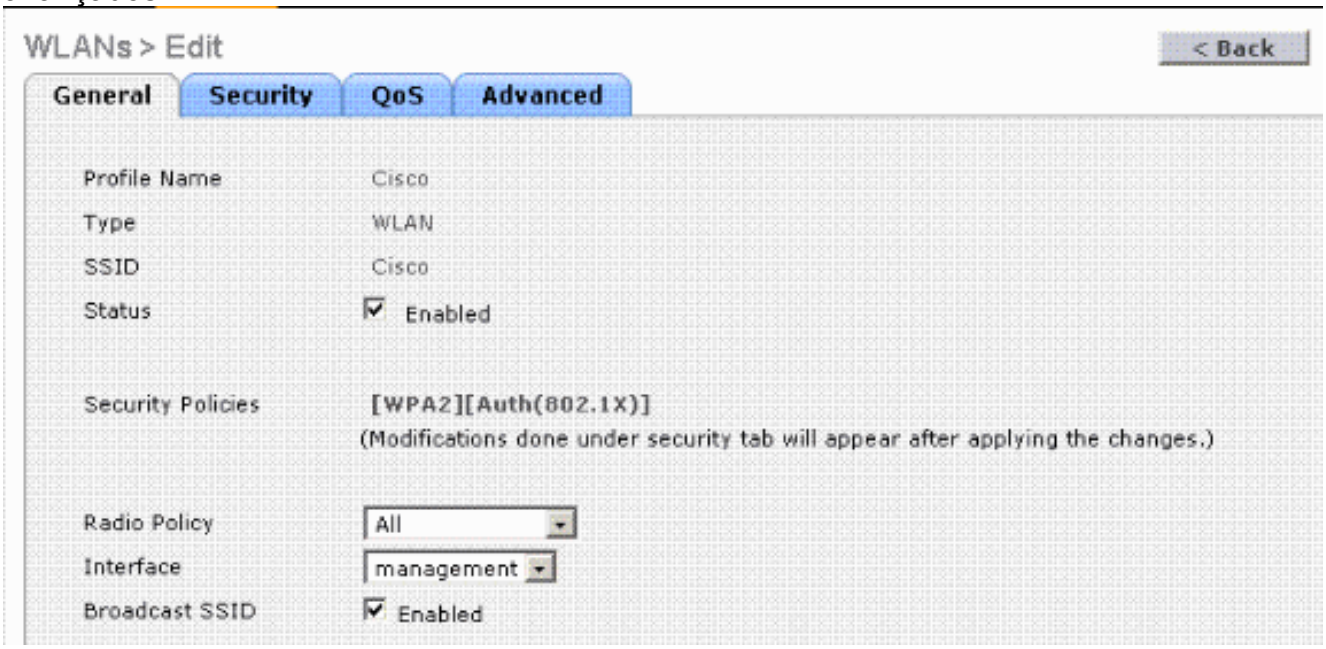
Observação: você pode configurar até dezesseis WLANs na controladora. A solução de WLAN da Cisco pode controlar até dezesseis WLANs para APs leves. Cada WLAN pode receber políticas de segurança exclusivas. Os APs leves transmitem todos os SSIDs ativos da WLAN da Cisco WLAN Solution e aplicam as políticas definidas para cada WLAN.

Conclua estes passos para configurar uma nova 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. Escolha **New** para criar uma nova WLAN. Insira o nome do perfil e o SSID da WLAN para a WLAN e clique em **Apply** (**Aplicar**). Este exemplo usa a Cisco como

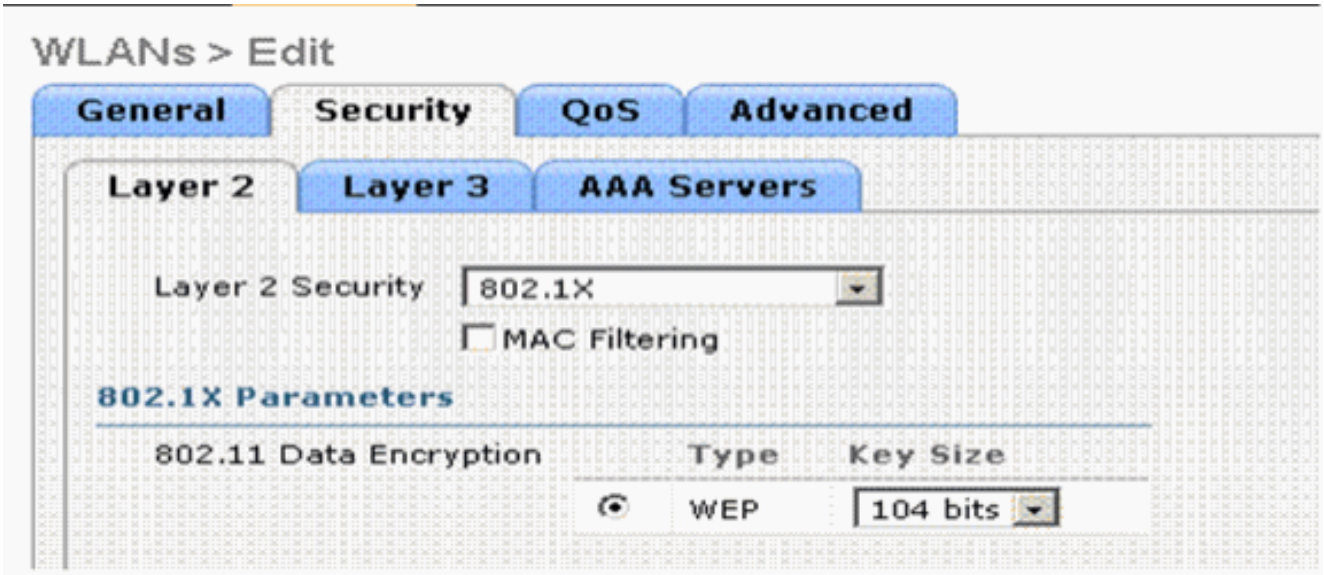
SSID.

3. Quando você cria uma nova WLAN, a página WLAN > Edit da nova WLAN é exibida. Nesta página, você pode definir vários parâmetros específicos para esta WLAN que incluem políticas gerais, políticas de segurança, políticas de QOS e outros parâmetros avançados.

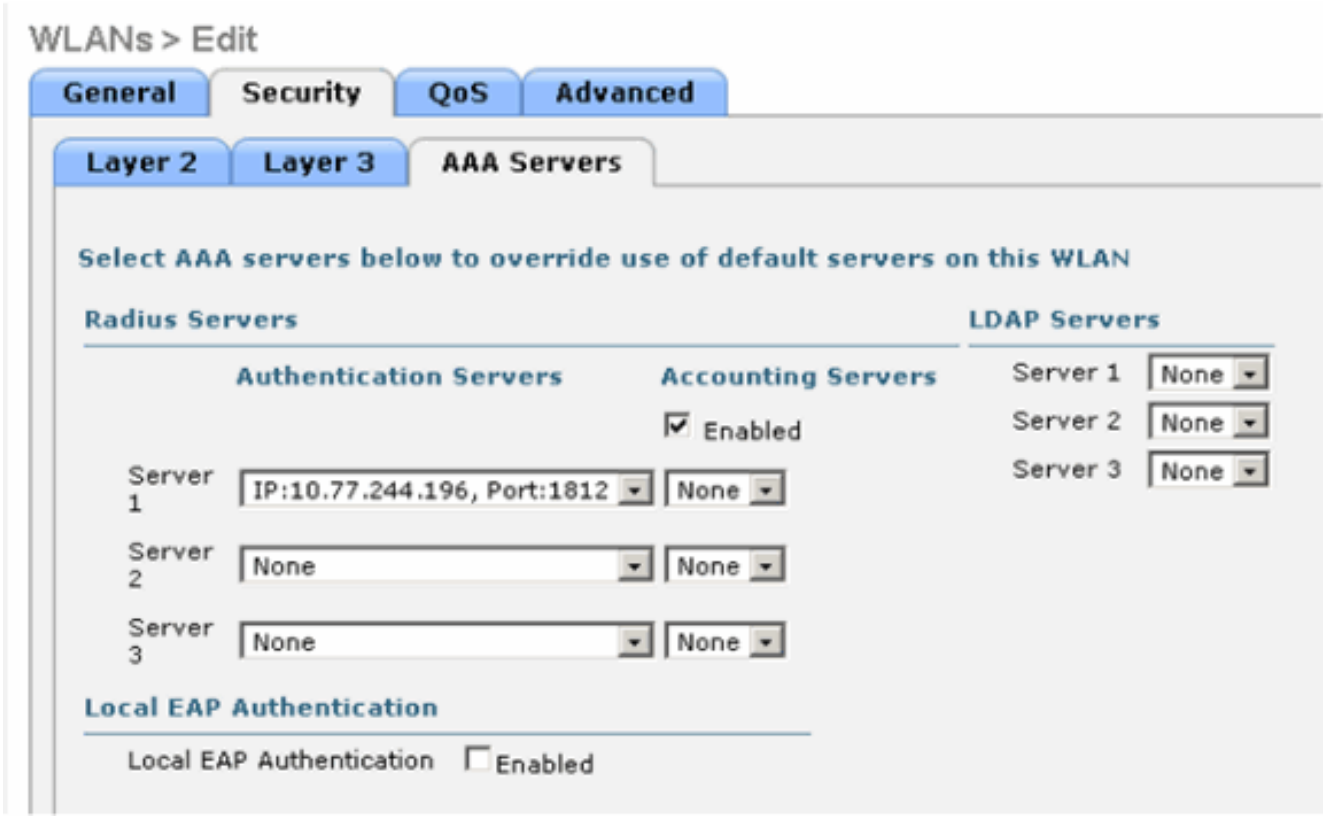


Escolha a interface apropriada no menu suspenso. Os outros parâmetros podem ser modificados com base no requisito da rede WLAN.Marque a caixa **Status** em General Policies para habilitar a WLAN.

4. Clique na guia **Security** e escolha **Layer 2 Security**. No menu suspenso Layer 2 Security, escolha **802.1x**. Nos parâmetros 802.1x, escolha o tamanho da chave WEP. Este exemplo usa a chave WEP de 128 bits, que é a chave WEP de 104 bits mais o vetor de Inicialização de 24
bits.



5. Escolha a guia **Servidores AAA**. No menu suspenso Authentication Servers (RADIUS), escolha o servidor RADIUS apropriado. Este servidor é usado para autenticar os clientes sem
fio.

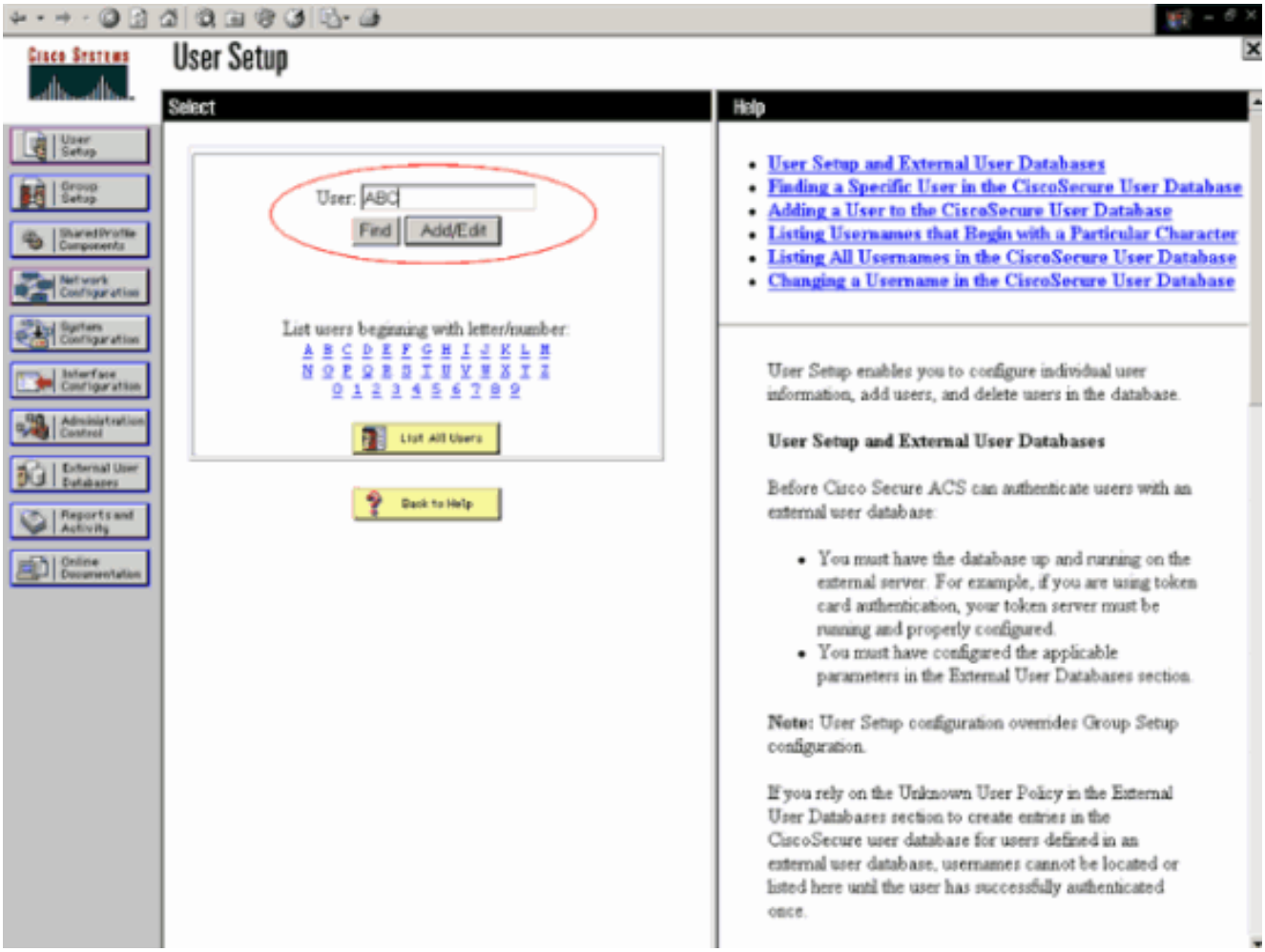


6. Clique em **Apply** para salvar a configuração.

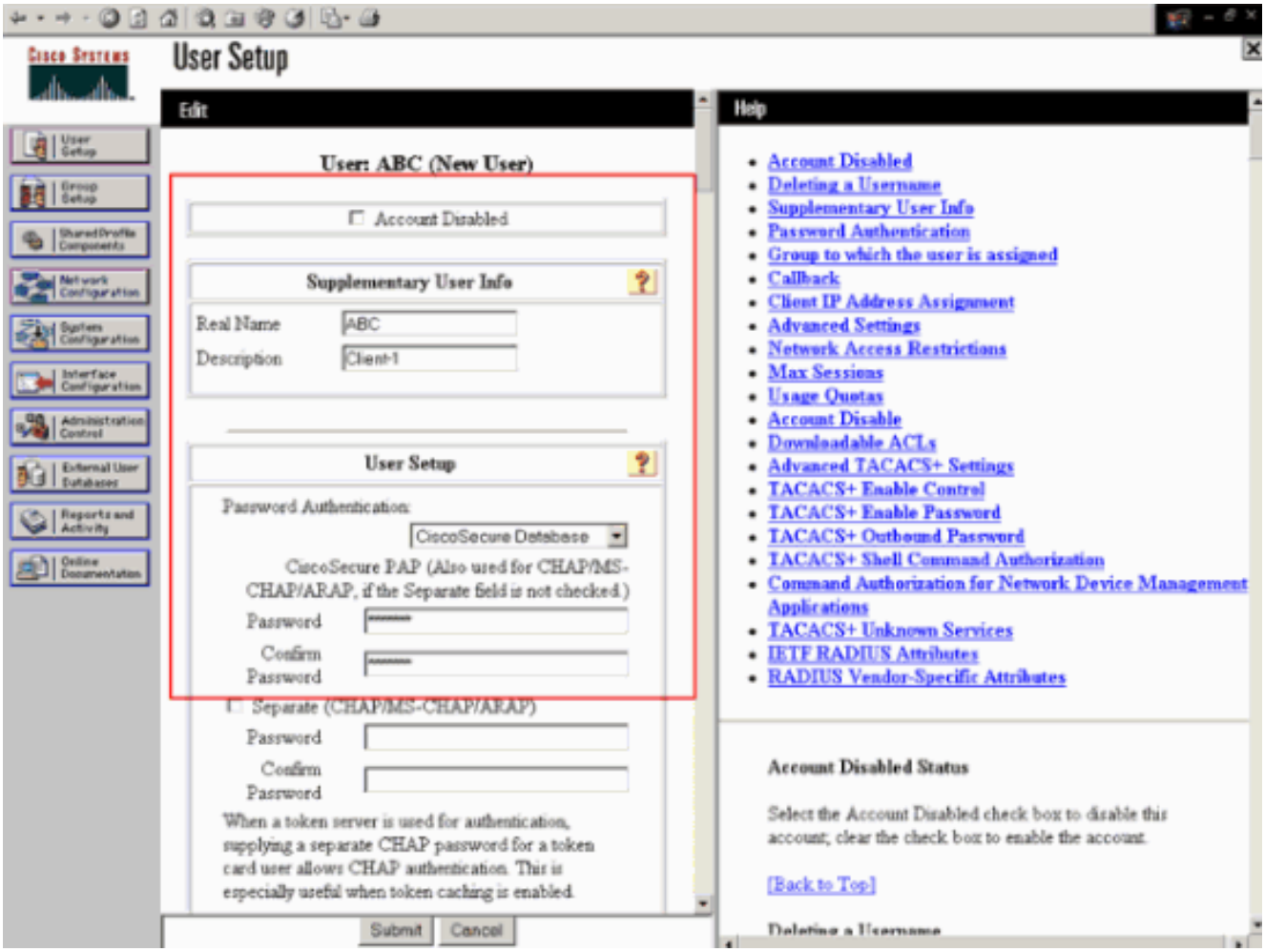
Configure o Cisco Secure ACS como o servidor RADIUS externo e crie um banco de dados de usuário para clientes de autenticação

Conclua estes passos para criar o banco de dados de usuários e habilitar a autenticação EAP no Cisco Secure ACS:

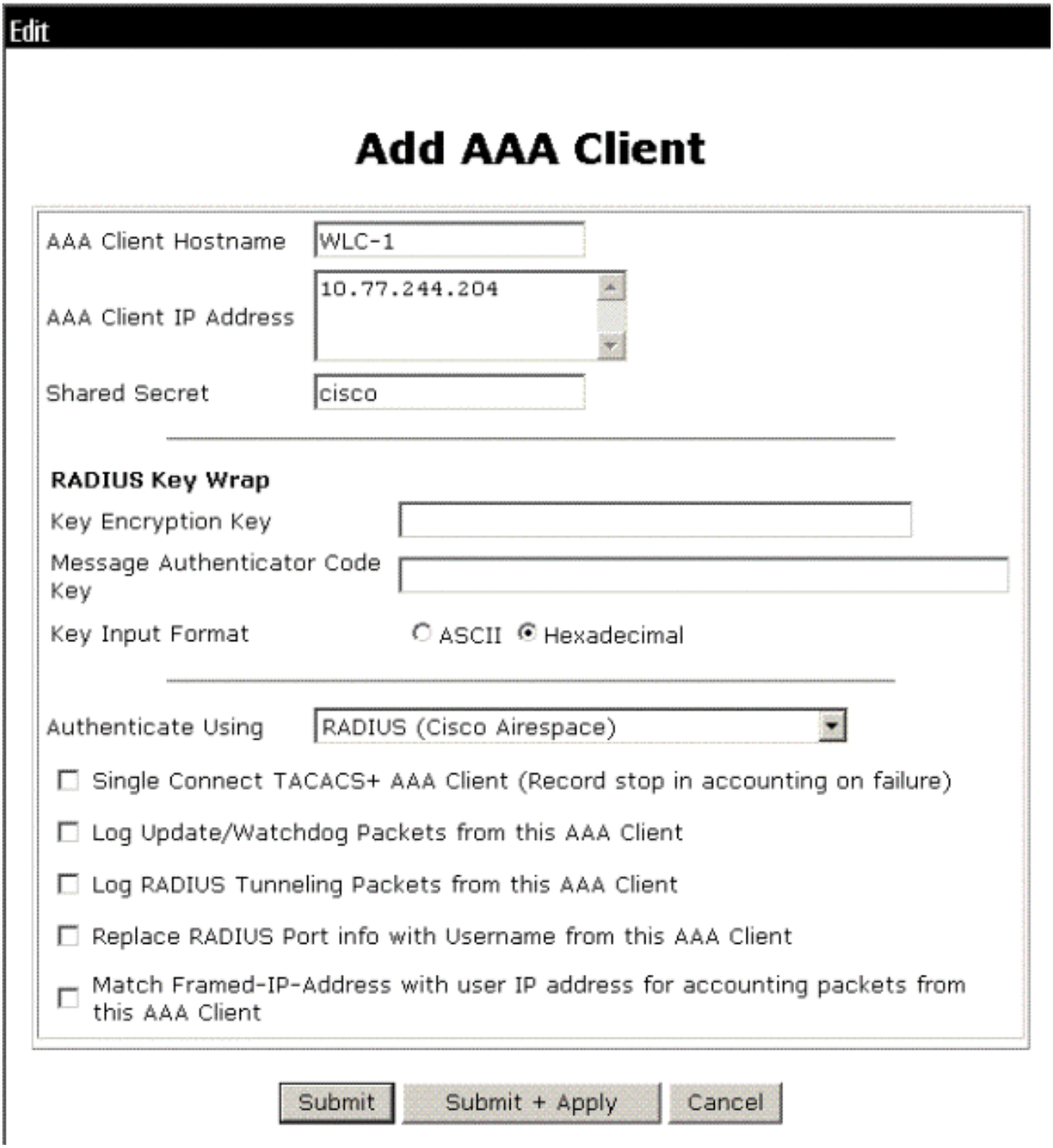
1. Escolha **User Setup** na GUI do ACS, digite o nome de usuário e clique em **Add/Edit**. Neste exemplo, o usuário é
ABC.



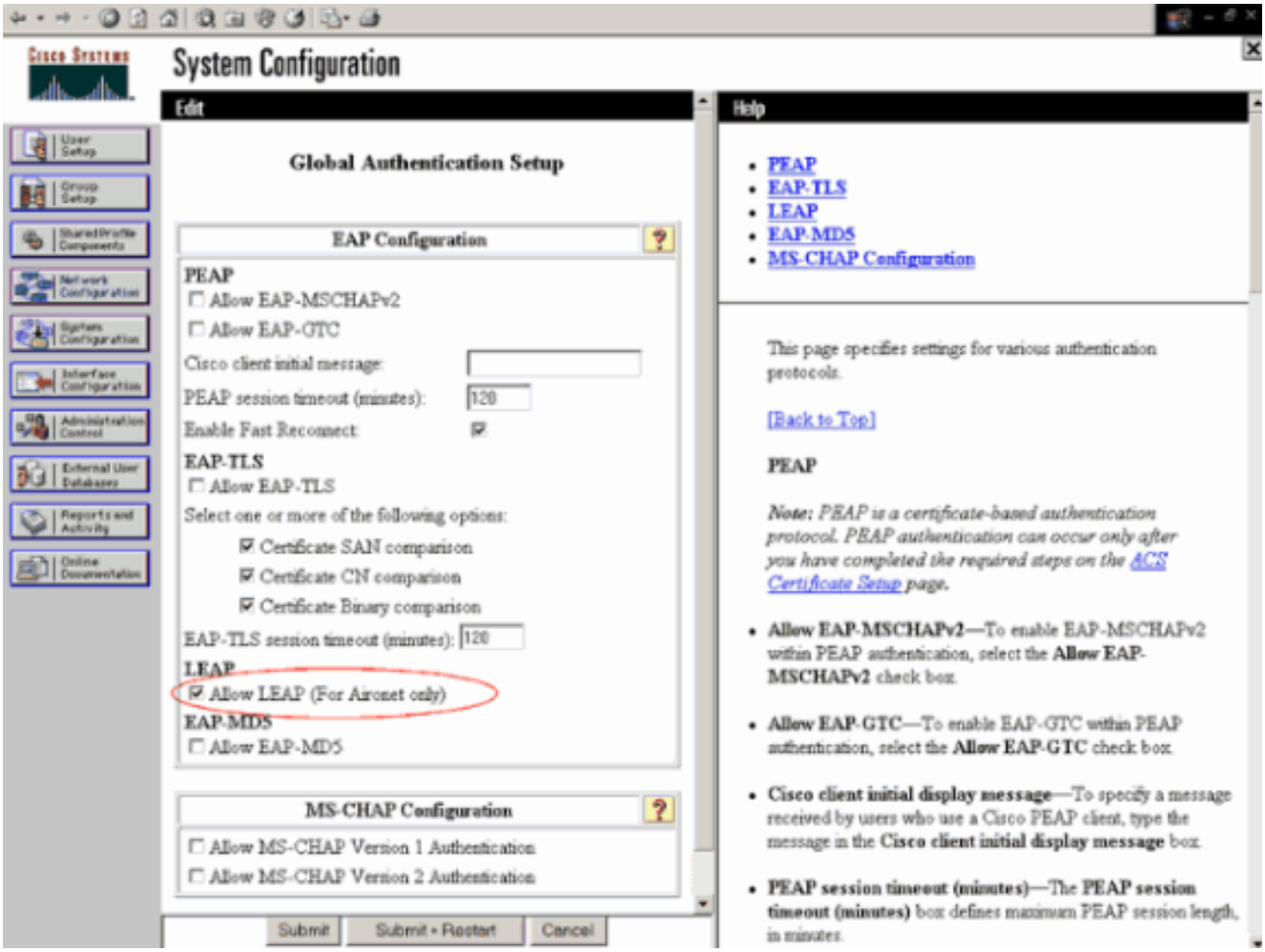
2. Quando a página User Setup for exibida, defina todos os parâmetros específicos do usuário. Neste exemplo, o nome de usuário, a senha e as Informações de usuário suplementares são configurados porque você só precisa desses parâmetros para autenticação EAP.Clique em **Submit** e repita o mesmo processo para adicionar mais usuários ao banco de dados. Por padrão, todos os usuários são agrupados no grupo padrão e recebem a mesma política definida para o grupo. Consulte a seção Gerenciamento de grupos de usuários do Guia do usuário do Cisco Secure ACS for Windows Server 3.2 para obter mais informações se desejar atribuir usuários específicos a diferentes
grupos.



3. Defina o controlador como um cliente AAA no servidor ACS. Clique em **Network Configuration** na GUI do ACS.Quando a página Configuração de rede for exibida, defina o nome da WLC, do endereço IP, do segredo compartilhado e do método de autenticação (RADIUS Cisco Airespace). Consulte a documentação do fabricante para outros servidores de autenticação não-ACS.**Observação:** a chave secreta compartilhada configurada no WLC e no servidor ACS deve ser igual. O segredo compartilhado diferencia maiúsculas e minúsculas.



4. Clique em **Configuração do sistema** e **Configuração de autenticação global** para garantir que o servidor de autenticação esteja configurado para executar o método de autenticação EAP desejado. Nas definições de configuração do EAP, escolha o método EAP apropriado. Este exemplo usa autenticação LEAP. Clique em **Enviar** quando terminar.

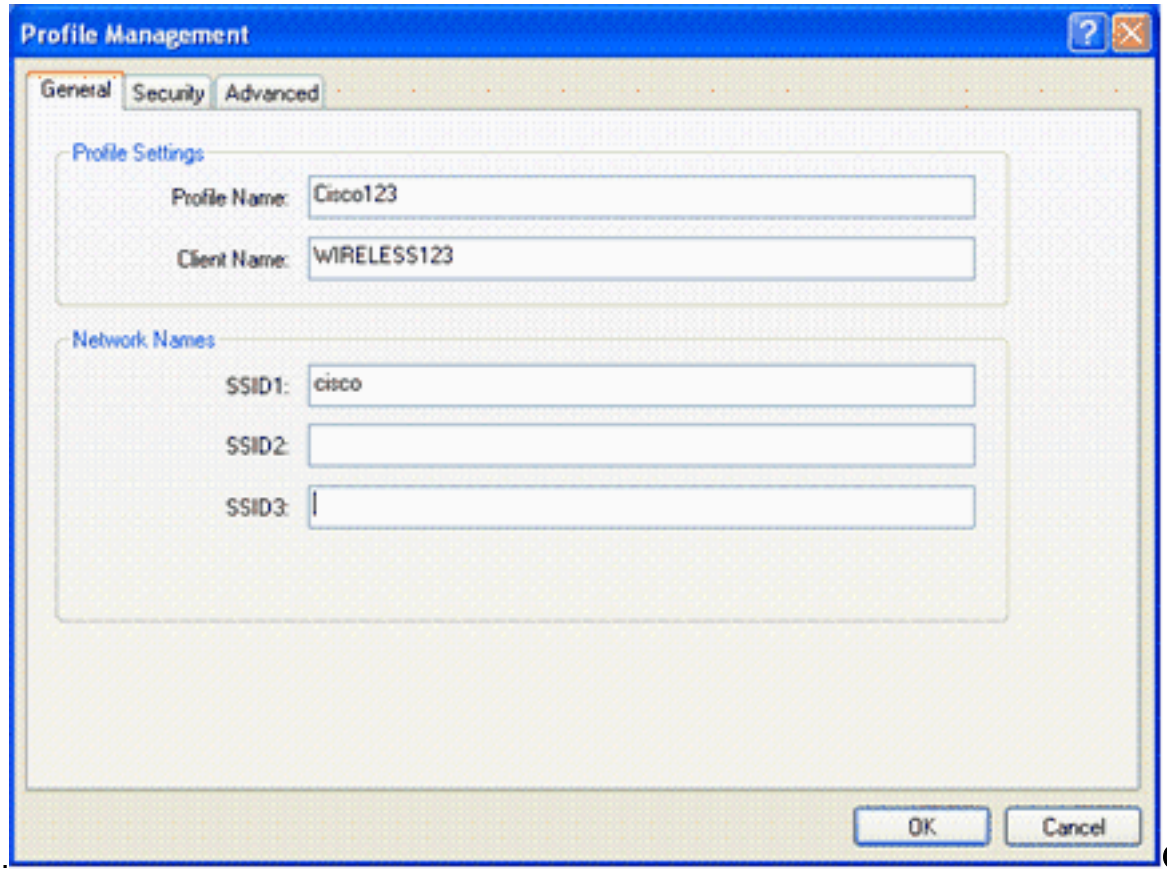


Configurar o cliente

O cliente também deve ser configurado para o tipo de EAP apropriado. O cliente propõe o tipo de EAP para o servidor durante o processo de negociação de EAP. Se o servidor suportar esse tipo de EAP, ele confirmará o tipo de EAP. Se o tipo de EAP não for suportado, ele enviará uma confirmação negativa e o cliente negociará novamente com um método EAP diferente. Esse processo continua até que um tipo de EAP suportado seja negociado. Este exemplo usa LEAP como o tipo EAP.

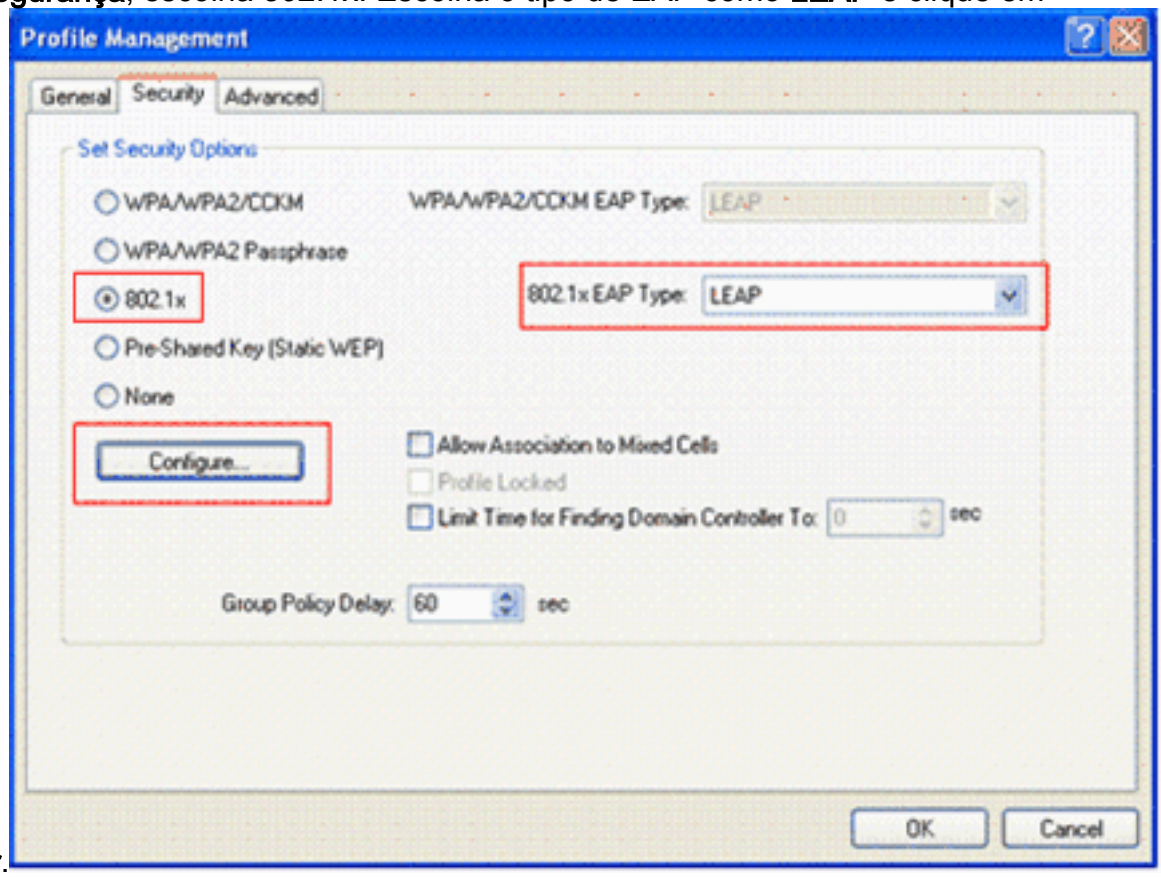
Conclua estes passos para configurar o LEAP no cliente com o Aironet Desktop Utility .

1. Clique duas vezes no ícone **Aironet Utility** para abri-lo.
2. Clique na guia **Gerenciamento de perfis**.
3. Clique em um perfil e escolha **Modificar**.
4. Na guia Geral, escolha um *Nome de perfil*. Digite o **SSID** da



WLAN. **Observação:** o SSID diferencia maiúsculas de minúsculas e precisa corresponder exatamente ao SSID configurado na WLC.

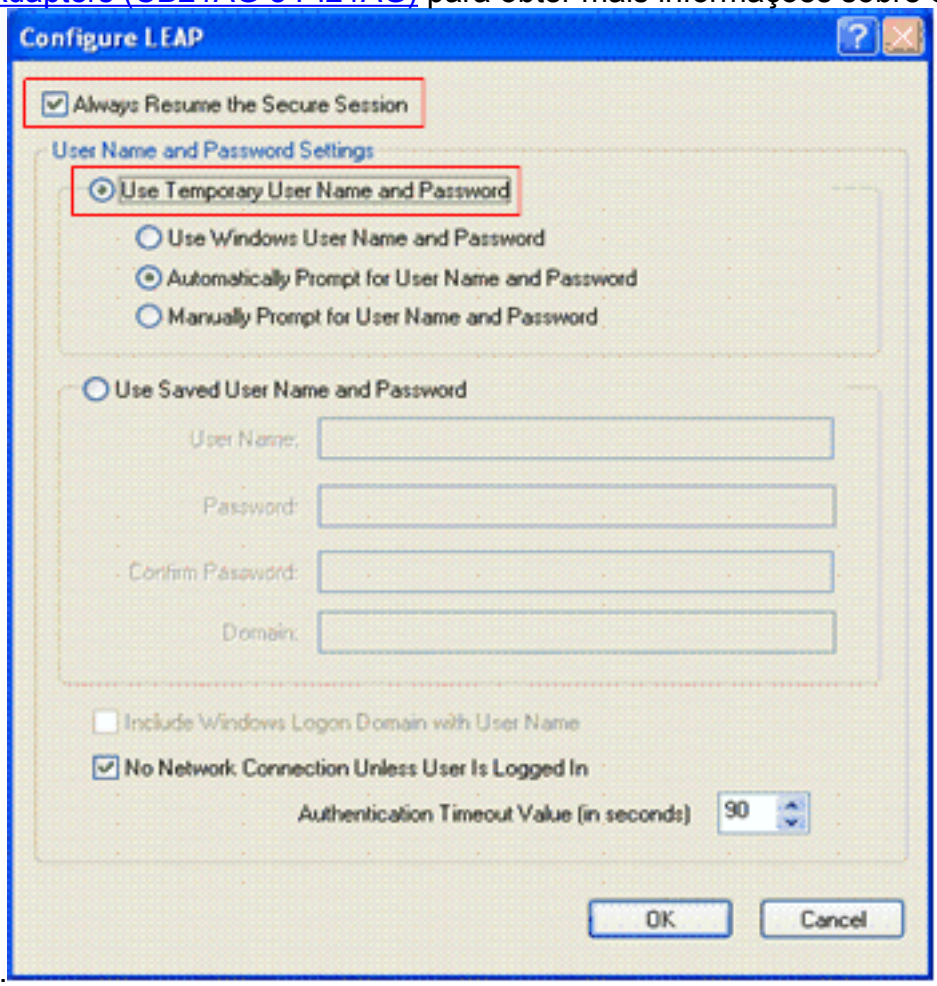
5. Na guia **Segurança**, escolha *802.1x*. Escolha o tipo de EAP como **LEAP** e clique em



Configurar.

6. Escolha **Usar nome de usuário temporário e senha**, o que solicitará que você insira as credenciais de usuário toda vez que o computador for reinicializado.Verifique uma das três opções fornecidas aqui. Este exemplo usa **Solicitar Automaticamente o Nome de Usuário e a Senha**, o que exige que você digite as credenciais de usuário *LEAP* além do *Nome de*

Usuário e Senha do Windows antes de fazer login no Windows.Marque a caixa de seleção **Sempre Retomar a Sessão Segura** na parte superior da janela se desejar que o solicitante LEAP tente sempre retomar a sessão anterior sem a necessidade de solicitar que você digite novamente suas credenciais sempre que o adaptador cliente for roaming e se associar novamente à rede.**Observação:** consulte a seção Configuração do Adaptador Cliente do documento Guia de Instalação e Configuração do Cisco Aironet 802.11a/b/g Wireless LAN Client Adapters (CB21AG e PI21AG) para obter mais informações sobre outras opções.



7. Na guia **Avançado**, você pode configurar o Preâmbulo, a extensão Aironet e outras opções 802.11, como Alimentação, Frequência e assim por diante.
8. Click **OK**. O cliente agora tenta se associar aos parâmetros configurados.

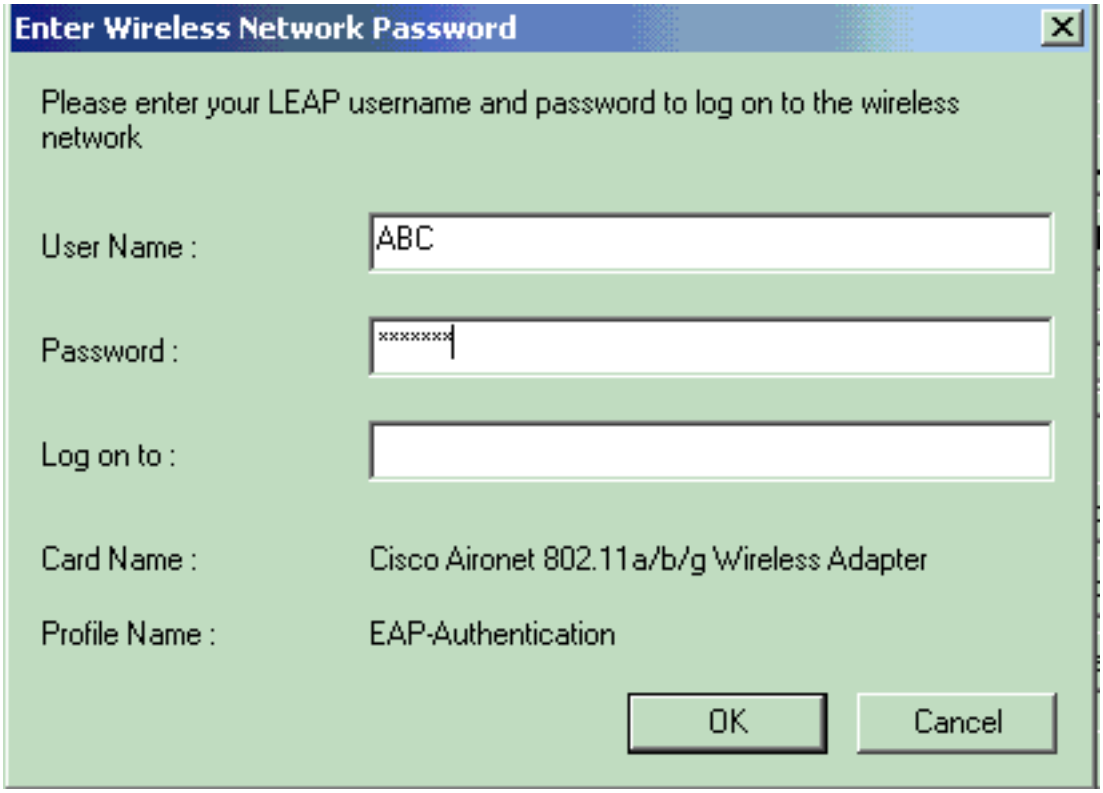
Verificar

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

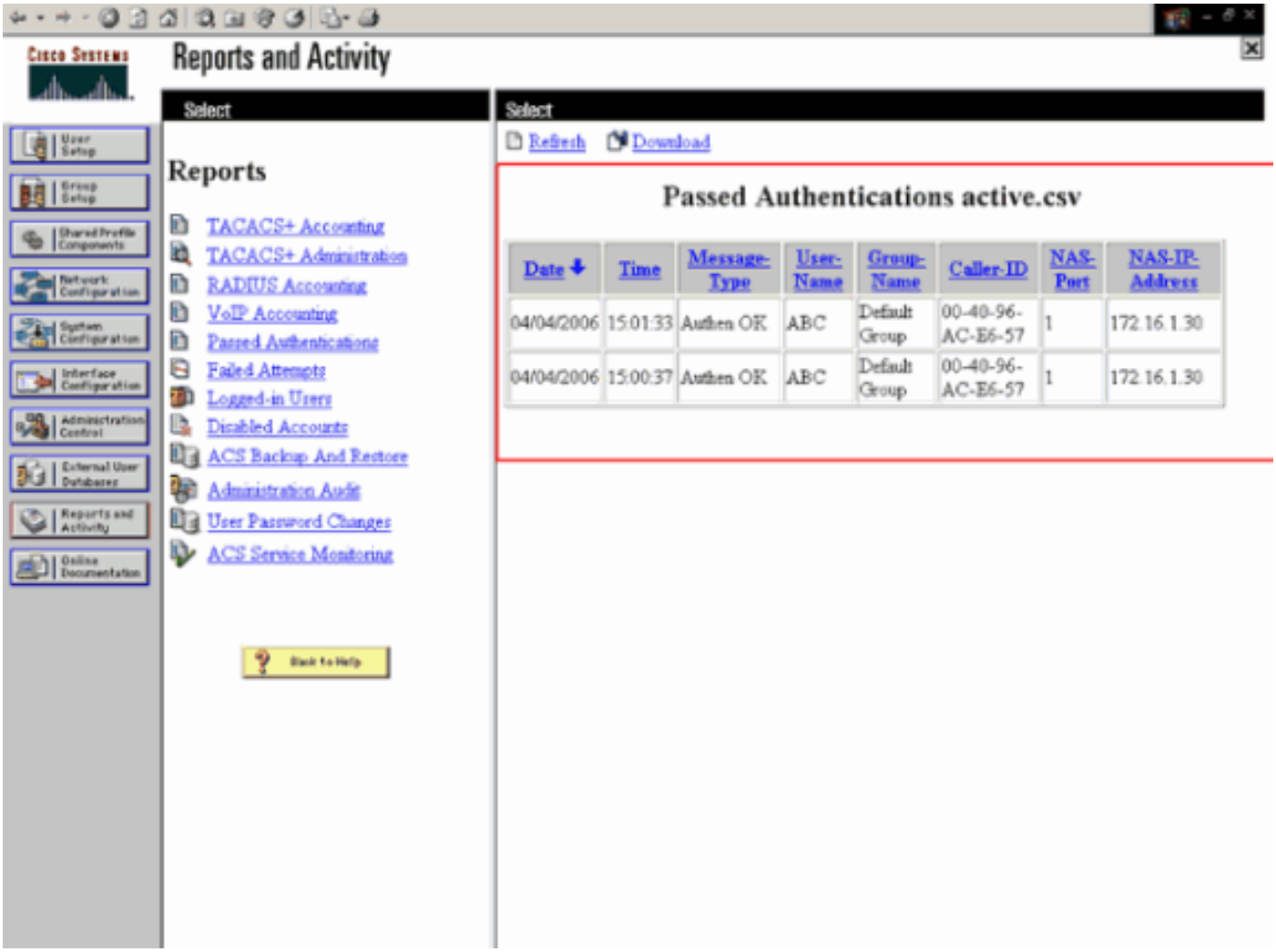
Tente associar um cliente sem fio ao Lightweight AP usando a autenticação LEAP para verificar se a configuração funciona como esperado.

Observação: este documento pressupõe que o perfil do cliente está configurado para autenticação LEAP. Consulte Usando a Autenticação EAP para obter mais informações sobre como configurar o Adaptador de Cliente Wireless 802.11 a/b/g para autenticação LEAP.

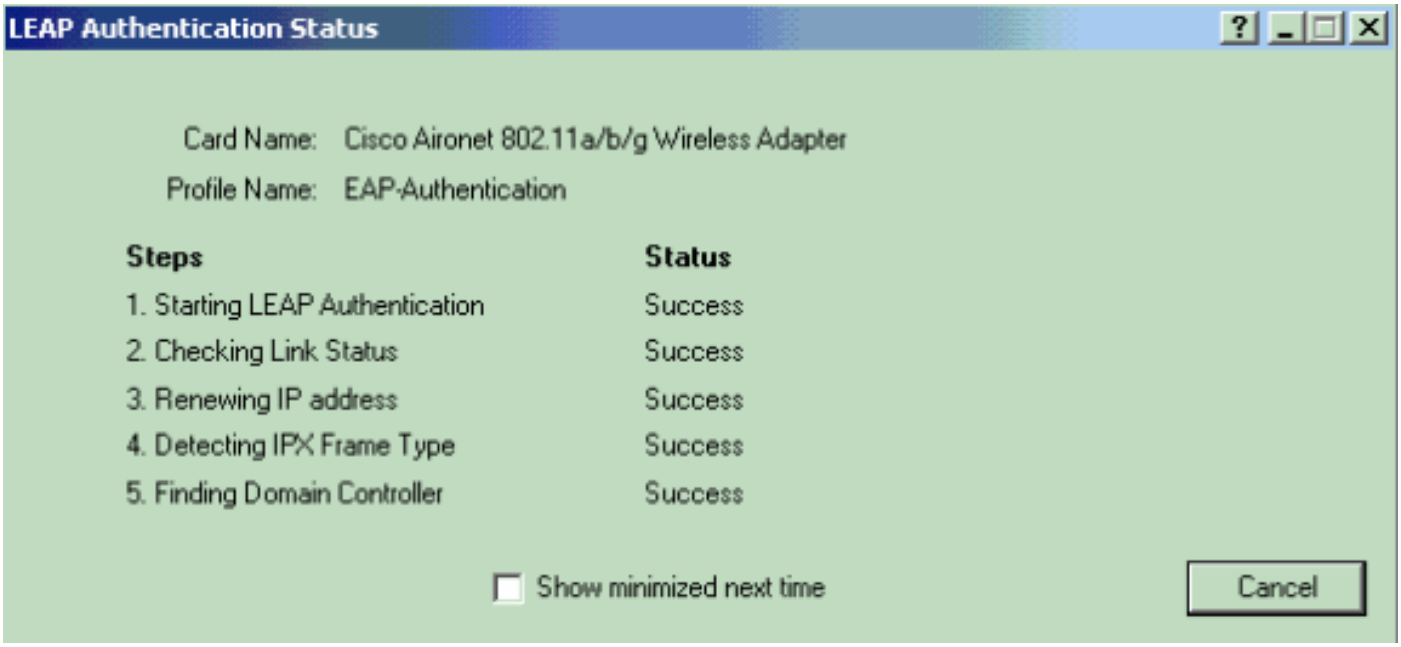
Quando o perfil do cliente sem fio for ativado, o usuário será solicitado a fornecer o nome de usuário/senha para a autenticação LEAP. Aqui está um exemplo:



O AP leve e, em seguida, a WLC transmitem as credenciais do usuário ao servidor RADIUS externo (Cisco Secure ACS) para validar as credenciais. O servidor RADIUS compara os dados com o banco de dados do usuário e fornece acesso ao cliente sem fio sempre que as credenciais do usuário são válidas para verificar as credenciais do usuário. O relatório de autenticação aprovada no servidor ACS mostra que o cliente passou na autenticação RADIUS. Aqui está um exemplo:



Após a autenticação RADIUS bem-sucedida, o cliente sem fio associa-se ao AP Lightweight.

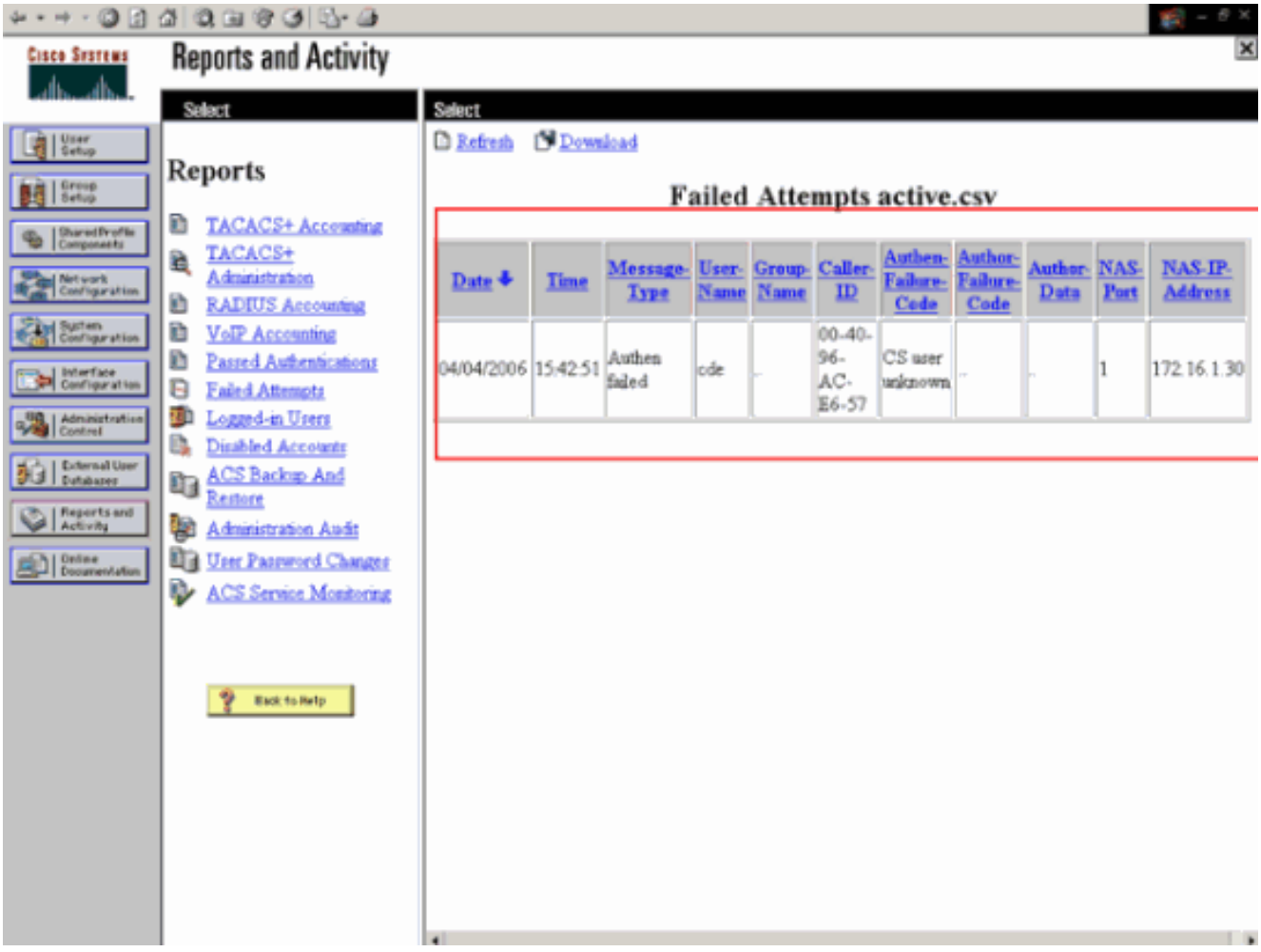


Isso também pode ser verificado na guia **Monitor** da GUI da WLC. Escolha **Monitor > Clients** e verifique o endereço MAC do cliente.

Troubleshoot

Conclua estes passos para solucionar problemas das configurações:

1. Use o comando **debug lwapp events enable** para verificar se o AP se registra na WLC.
2. Verifique se o servidor RADIUS recebe e valida a solicitação de autenticação do cliente sem fio. Verifique o NAS-IP - endereço, data e hora para verificar se a WLC conseguiu acessar o servidor Radius.Verifique os relatórios Autenticações aprovadas e Tentativas com falha no servidor ACS para fazer isso. Esses relatórios estão disponíveis em Relatórios e atividades no servidor ACS. Aqui está um exemplo quando a autenticação do servidor RADIUS falha:



Observação: consulte Obtendo informações de versão e depuração AAA para Cisco Secure ACS para Windows para obter informações sobre como solucionar problemas e obter

informações de depuração no Cisco Secure ACS.

3. Você também pode usar estes comandos **debug** para solucionar problemas de autenticação AAA:**debug aaa all enable** — Configura a depuração de todas as mensagens AAA.**debug dot1x packet enable**—Habilita a depuração de todos os pacotes dot1x.Aqui está um exemplo de saída do comando **debug 802.1x aaa enable**:

```
(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
```

Observação: algumas das linhas na saída de depuração foram encapsuladas devido a restrições de espaço.

4. Monitore os logs na WLC para verificar se o servidor RADIUS recebe as credenciais do usuário. Clique em **Monitor** para verificar os registros da GUI da WLC. No menu à esquerda, clique em **Statistics** e clique em **Radius server** na lista de opções.Isso é muito importante porque em alguns casos, o servidor RADIUS nunca recebe as credenciais do usuário se a configuração do servidor RADIUS na WLC estiver incorreta.Éassim que os registros aparecem na WLC se os parâmetros RADIUS estiverem configurados incorretamente:

Você pode usar uma combinação do comando **show wlan summary** para reconhecer qual das suas WLANs emprega a autenticação de servidor RADIUS. Em seguida, você pode exibir o comando **show client summary** para ver quais endereços MAC (clientes) foram autenticados com êxito em WLANs RADIUS. Você também pode correlacionar isso com as tentativas aprovadas ou os registros de tentativas com falha do Cisco Secure ACS.

Dicas para Troubleshooting

- Verifique no controlador se o servidor RADIUS está no estado `ativo` e não no `modo de espera` ou `desativado`.
- Use o comando **ping** para verificar se o servidor Radius pode ser alcançado na WLC.
- Verifique se o servidor RADIUS está selecionado no menu suspenso da WLAN (SSID).
- Se você usa WPA, é necessário instalar a correção WPA mais recente da Microsoft para o Windows XP SP2. Além disso, você deve atualizar o driver para o suplicante do cliente para o mais recente.
- Se você fizer o PEAP, por exemplo, certificados com XP, SP2 onde as placas são gerenciadas pelo utilitário Microsoft wireless-0, será necessário obter o patch KB885453 da Microsoft.Se você usar o suplicante de cliente/Configuração Zero do Windows, desabilite **Habilitar Reconexão Rápida**. Você pode fazer isso escolhendo **Propriedades da Conexão de Rede Sem Fio > Redes Sem Fio > Redes Preferenciais**. Em seguida, escolha **SSID > Properties > Open > WEP > Authentication > EAP type > PEAP > Properties > Enable Fast Reconnect** . Você pode então encontrar a opção de ativar ou desativar no final da janela.
- Se você tiver placas Intel 2200 ou 2915, consulte as declarações no site da Intel sobre os problemas conhecidos com suas placas:Conexão de rede Intel® PRO/Wireless 2200BGConexão de rede Intel® PRO/Wireless 2915ABGDescarregue os drivers Intel mais

atuais para evitar problemas. Você pode descarregar os drivers 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 isso não deve ser feito porque o servidor AAA possivelmente não responde somente a esse cliente específico, se você fizer o descarte silencioso. Pode ser uma resposta para outros clientes válidos com certificados válidos. Mas a WLC ainda pode 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 isso estiver desabilitado, o controlador só fará failover para o próximo servidor AAA se houver três clientes consecutivos que não receberem uma resposta do servidor RADIUS.

Manipular temporizadores EAP

Durante a autenticação 802.1x, o usuário pode ver o `DOT1X-1-MAX_EAPOL_KEY_RETRANS_FOR_MOBILE: Máximo de retransmissões M1 EAPOL-Key acessadas para a` mensagem de erro `mobile xx:xx:xx:xx:xx`.

Essa mensagem de erro indica que o cliente não respondeu a tempo ao controlador durante a negociação da chave WPA (802.1x). O controlador define um temporizador para uma resposta durante a negociação de chave. Normalmente, quando você vê esta mensagem, ela é devido a um problema com o requerente. Certifique-se de executar as versões mais recentes de drivers e firmware do cliente. Na WLC, há alguns temporizadores EAP que você pode manipular para ajudar na autenticação do cliente. Esses 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 de manipular esses valores, você precisa entender o que eles fazem e como alterá-los afetará a rede:

- **EAP-Identity-Request Timeout:**Esse temporizador afeta o tempo que você espera entre as solicitações de identidade EAP. Por padrão, esse é um segundo (4.1 e inferior) e 30 segundos (4.2 e superior). A razão para esta mudança foi porque alguns clientes, portáteis, telefones, scanners etc. tinham dificuldade em responder rápido o suficiente. Dispositivos como laptops, geralmente não exigem a manipulação desses valores. O valor disponível é de 1 a 120.Então, o que acontece quando este atributo é definido para um valor de 30? Quando o cliente se conecta pela primeira vez, ele envia um EAPOL Start para a rede e o WLC envia um pacote EAP, solicitando a Identidade do usuário ou da máquina. Se a WLC não receber a Resposta de identidade, ela enviará outra Solicitação de identidade 30 segundos após a primeira. Isso acontece na conexão inicial e quando o cliente faz roaming.O que acontece quando aumentamos esse temporizador? Se tudo é bom, não há impacto. No entanto, se houver um problema na rede (incluindo problemas de cliente, problemas de AP ou problemas de RF), isso pode causar atrasos na conectividade da rede. Por exemplo, se você definir o temporizador para o valor máximo de 120 segundos, a WLC esperará 2 minutos entre as Solicitações de identidade. Se o cliente estiver em roaming e a Resposta não for recebida

pela WLC, então criamos, no mínimo, uma interrupção de dois minutos para esse cliente.As recomendações para este temporizador são *5*. No momento, não há motivo para colocar esse temporizador em seu valor máximo.

- **Tentativas máximas de EAP-Identity-Request:**O valor Máximo de Tentativas é o número de vezes que a WLC enviará a Solicitação de Identidade ao cliente, antes de remover sua entrada do MSCB. Quando o Máximo de Tentativas é alcançado, a WLC envia um quadro de não autenticação ao cliente, forçando-o a reiniciar o processo EAP. O valor disponível é de 1 a 20. Em seguida, vamos analisar isso com mais detalhes.O Máximo de Tentativas funciona com o Tempo Limite da Identidade. Se o tempo limite de identidade for definido como 120 e o número máximo de novas tentativas for 20, quanto tempo levará 2400 (ou 120 * 20). Isso significa que levaria 40 minutos para o cliente ser removido e iniciar o processo EAP novamente. Se você definir o tempo limite de identidade como 5, com um valor máximo de Tentativas de 12, então ele levará 60 (ou 5 * 12). Em contraste com o exemplo anterior, há um minuto até que o cliente seja removido e tenha que iniciar o EAP novamente.Recomendações para o Máximo de Tentativas é *12*.
- **Tempo limite da chave EAPOL:**Para o valor de tempo limite EAPOL-Key, o padrão é 1 segundo ou 1000 milissegundos. Isso significa que quando as chaves EAPOL são trocadas entre o AP e o cliente, o AP enviará a chave e aguardará até 1 segundo por padrão para que o cliente responda. Depois de aguardar o valor de tempo definido, o AP retransmitirá a chave novamente. Você pode usar o comando **config advanced eap eapol-key-timeout** ***<time> para alterar essa configuração.*** Os valores disponíveis em 6.0 estão entre 200 e 5000 milissegundos, enquanto os códigos anteriores a 6.0 permitem valores entre 1 e 5 segundos. Lembre-se de que se você tiver um cliente que não esteja respondendo a uma tentativa importante, estender os temporizadores para fora poderá dar a eles um pouco mais de tempo para responder. No entanto, isso também pode prolongar o tempo que leva para a WLC/AP desautenticar o cliente para que todo o processo 802.1x comece novamente.
- **Tentativas máximas de teclas EAPOL:**Para o valor de Tentativas máximas de EAPOL-Key, o padrão é 2. Isso significa que tentaremos a chave original novamente no cliente duas vezes. Essa configuração pode ser alterada usando o comando **config advanced eap eapol-key-retries** ***<retries>.*** Os valores disponíveis estão entre 0 e 4 novas tentativas. Usando o valor padrão para o Tempo Limite da Chave EAPOL (ou seja, 1 segundo) e o valor padrão para a Tentativa da Chave EAPOL (2), o processo seria como se um cliente não respondesse à tentativa de chave inicial:O AP envia uma tentativa chave ao cliente.Espera um segundo para uma resposta.Se não houver resposta, a primeira Tentativa de chave EAPOL será enviada.Espera um segundo para uma resposta.Se não houver resposta, a segunda Tentativa de chave EAPOL será enviada.Se ainda não houver resposta do cliente e o valor de nova tentativa for atendido, o cliente será desautenticado. Mais uma vez, tal como no EAPOL-Key Timeout, a extensão do valor da repetição EAPOL-Key poderia, em algumas circunstâncias, ser benéfica. No entanto, defini-la como o máximo pode ser prejudicial novamente, pois a mensagem de desautenticação seria prolongada.

Extraindo o arquivo de pacote do servidor ACS RADIUS para solução de problemas

Se você usar o ACS como o servidor radius externo, esta seção poderá ser usada para solucionar problemas de sua configuração. O package.cab é um arquivo Zip que contém todos os arquivos necessários para solucionar problemas do ACS com eficiência. Você pode usar o utilitário CSSupport.exe para criar o package.cab ou pode obter os arquivos manualmente.

Consulte a seção Criação de um arquivo package.cab de *Obtenção de Informações de Versão e de Depuração AAA para Cisco Secure ACS para Windows* para obter mais informações sobre como criar e extrair o arquivo de pacote do WCS.

Informações Relacionadas

- Exemplo de Configuração de Failover do Controlador WLAN para Pontos de Acesso Lightweight
- Atualização do software do Wireless LAN Controller (WLC)
- Referência de comando do Cisco Wireless LAN Controller
- Suporte Técnico e Documentação - Cisco Systems