ACL por usuário com controladores de LAN sem fio e exemplo de configuração do Cisco Secure ACS

Contents

Introduction

Este documento explica com um exemplo como criar listas de controle de acesso (ACL) nos WLC e aplicá-las aos usuários dependentes da autorização do RADIUS.

Prerequisites

Requirements

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

- Conhecimento básico de como configurar um servidor Cisco Secure ACS para autenticar clientes sem fio

- Conhecimento da configuração dos Access Points (LAPs) Lightweight Cisco Aironet e Cisco Wireless LAN Controllers (WLCs)
- Conhecimento das soluções Cisco Unified Wireless Security

Componentes Utilizados

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

- Controlador de LAN sem fio Cisco 4400 Series que executa a versão 5.0.148.0
- Pontos de acesso Lightweight Cisco Aironet série 1231 (LAPs)
- Adaptador cliente Cisco Aironet 802.11 a/b/g Cisco Wireless LAN que executa a versão 3.6
- Cisco Aironet Desktop Utility versão 3.6
- Cisco Secure ACS Server versão 4.1
- Roteador de serviços integrados Cisco 2800 Series que executa a versão 12.4(11)T do IOS® IOS®
- Switch Cisco Catalyst 2900XL Series que executa a versão 12.0(5)WC3b

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.

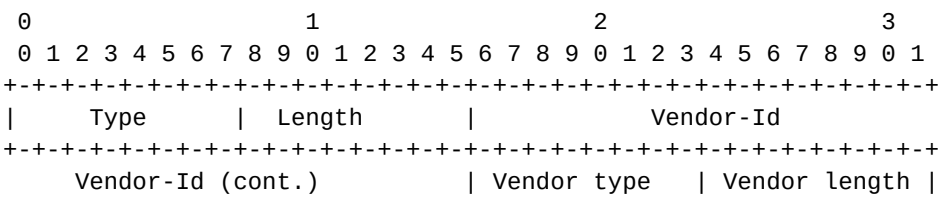
Informações de Apoio

A ACL (Access Control List, lista de controle de acesso) por usuário faz parte da rede Cisco Identity. A Cisco Wireless LAN Solution suporta redes de identidade, que, embora permita que a rede anuncie um único SSID, também permite que usuários específicos herdem diferentes políticas com base em seus perfis de usuário.

O recurso ACL por usuário fornece a capacidade de aplicar uma ACL configurada no Wireless LAN Controller a um usuário com base na autorização RADIUS. Isso é feito com o Airespace-ACL-Name Vendor Specific Attribute (VSA).

Este atributo indica o nome da ACL a ser aplicada ao cliente. Quando o atributo ACL está presente na Aceitação de Acesso RADIUS, o sistema aplica o ACL-Name à estação cliente depois de se autenticar. Isso substitui qualquer ACL atribuída à interface. Ignora a interface ACL atribuída e aplica a nova.

Um resumo do formato ACL-Name Attribute é mostrado abaixo. Os campos são transmitidos da esquerda para a direita



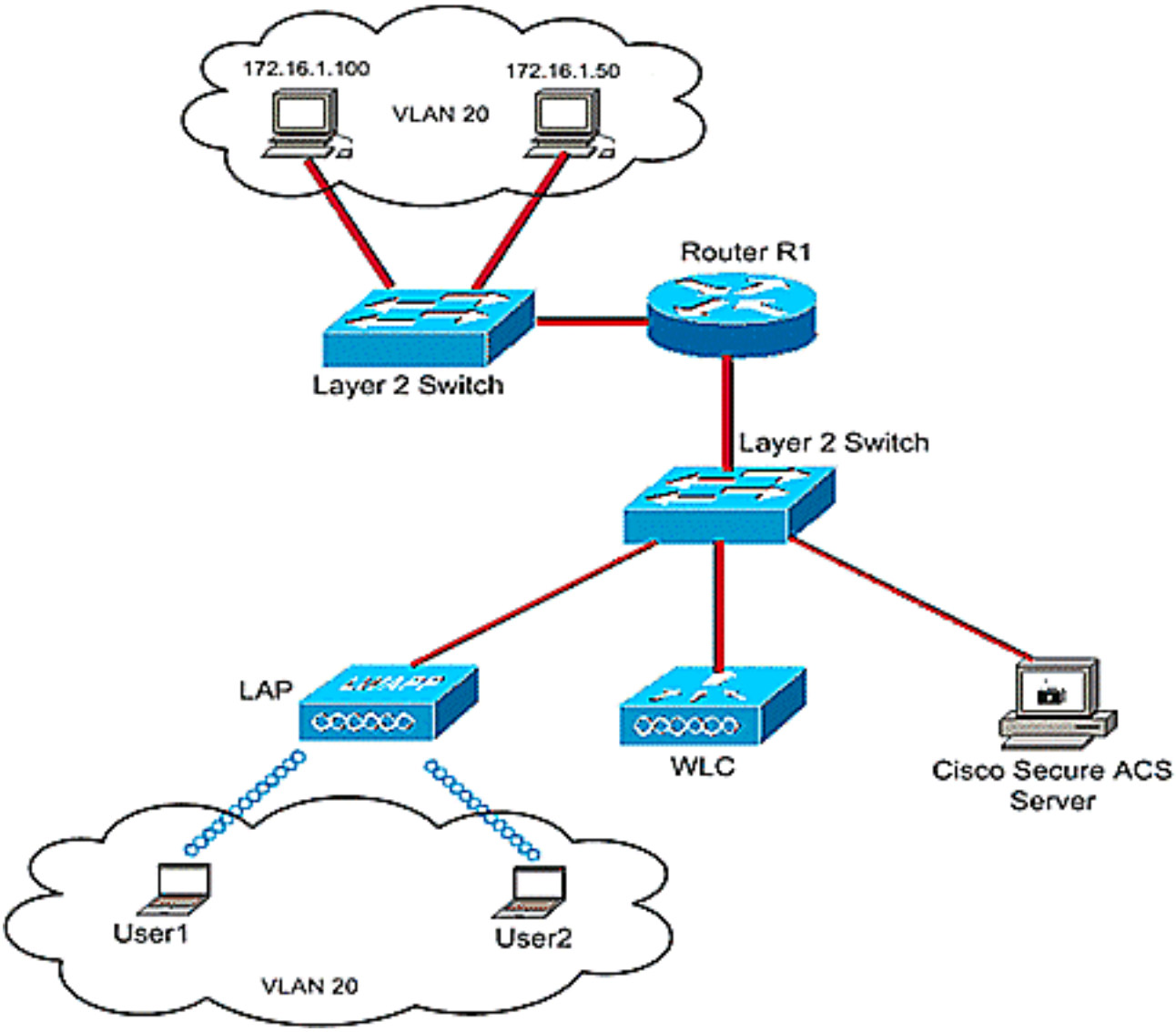
```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        ACL Name...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
• Type - 26 for Vendor-Specific
• Length - >7
• Vendor-Id - 14179
• Vendor type - 6
• Vendor length - >0
• Value - A string that includes the name of the ACL to use for the client.
   The string is case sensitive.
```

Para obter mais informações sobre o Cisco Unified Wireless Network Identity Networking, consulte a seção Configuração de redes de identidade do documento Configuração de soluções de segurança.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

Nesta configuração, a WLC e o LAP da controladora de LAN sem fio são usados para fornecer serviços sem fio aos usuários do Departamento A e do Departamento B. Todos os usuários sem fio usam um escritório comum de WLAN (SSID) para acessar a rede e estão na VLAN Office-VLAN.



O servidor Cisco Secure ACS é usado para autenticar usuários sem fio. A autenticação EAP é usada para autenticar usuários. O servidor WLC, LAP e Cisco Secure ACS estão conectados a um Switch de Camada 2 como mostrado.

O roteador R1 conecta os servidores no lado com fio através do Switch de Camada 2, como mostrado. O roteador R1 também atua como um servidor DHCP, que fornece endereços IP para clientes sem fio da sub-rede 172.16.0.0/16.

Você precisa configurar os dispositivos para que isso ocorra:

O Usuário1 do Departamento A tem acesso somente ao servidor 172.16.1.100

O Usuário2 do Departamento B tem acesso somente ao servidor 172.16.1.50

Para fazer isso, você precisa criar 2 ACLs na WLC: um para User1 e outro para User2. Depois que as ACLs forem criadas, você precisará configurar o servidor Cisco Secure ACS para retornar o atributo de nome da ACL para a WLC após a autenticação bem-sucedida do usuário Wireless. Em seguida, a WLC aplica a ACL ao usuário e, portanto, à rede é restrita dependendo do perfil do usuário.

Observação: este documento usa autenticação LEAP para autenticar usuários. O Cisco LEAP é vulnerável a ataques de dicionários. Em redes em tempo real, devem ser usados métodos de autenticação mais seguros, como EAP FAST. Como o foco do documento é explicar como configurar o recurso ACL por usuário, o LEAP é usado para simplificar.

A próxima seção fornece instruções passo a passo para configurar os dispositivos para essa configuração.

Configurar

Antes de configurar o recurso ACL por usuário, você deve configurar a WLC para a operação básica e registrar os LAPs na WLC. Este documento pressupõe que o WLC foi configurado para operação básica e que os LAPs foram registrados no WLC. Se você for um novo usuário, que tenta configurar a WLC para a operação básica com LAPs, consulte Registro de AP Lightweight (LAP) em um Controlador de LAN Wireless (WLC).

Depois que os LAPs estiverem registrados, faça o seguinte para configurar os dispositivos para esta configuração:

1. Configure o controlador de LAN sem fio.
2. Configure o servidor Cisco Secure ACS.
3. Verificar a configuração.

Observação: este documento discute a configuração necessária no lado Wireless. O documento pressupõe que a configuração com fio está estabelecida.

Configurar o controlador de LAN sem fio

Na controladora Wireless LAN, você precisa fazer o seguinte:

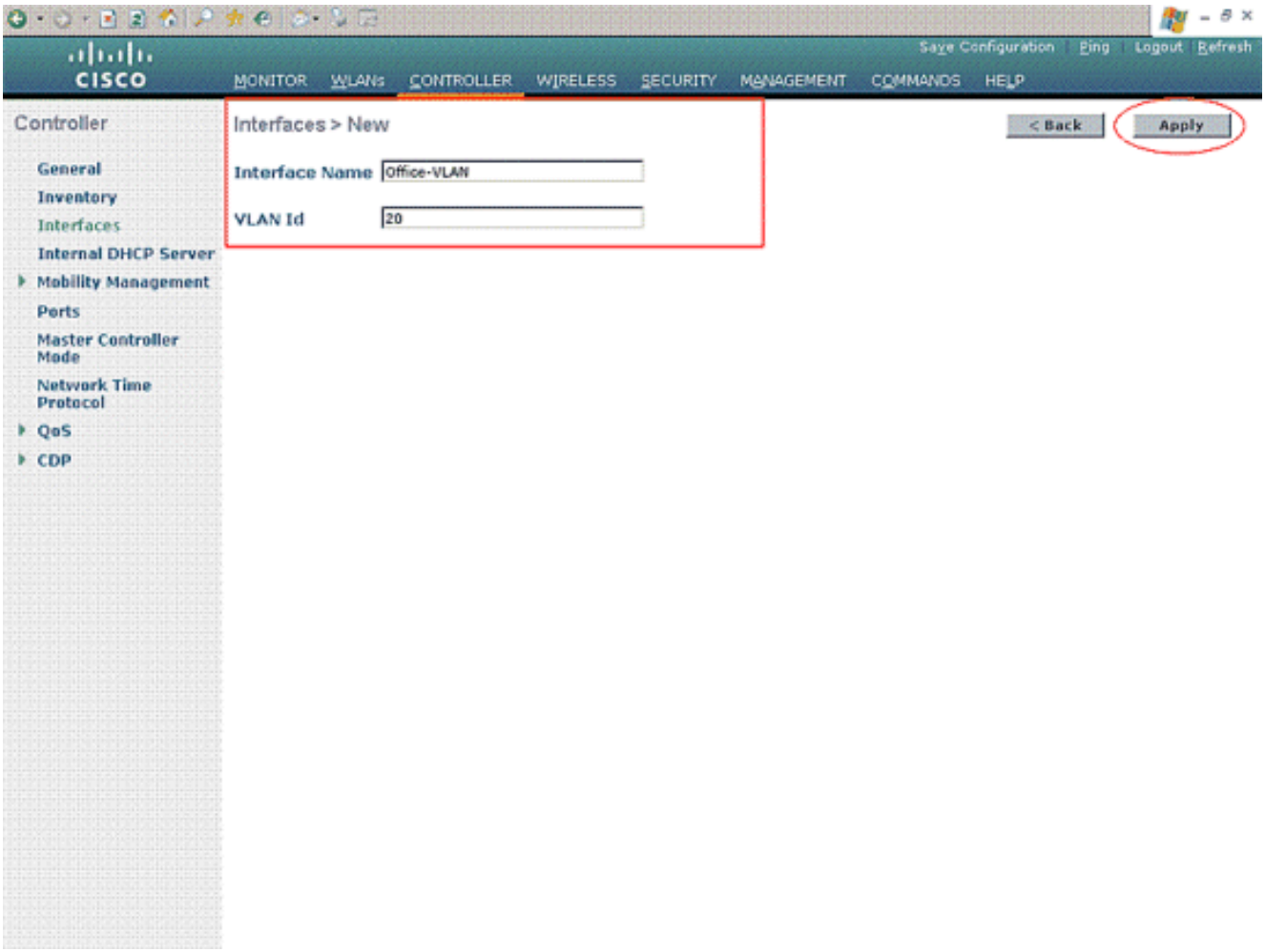
- Crie uma VLAN para os usuários sem fio.

- Configure a WLC para autenticar usuários sem fio com o Cisco Secure ACS.
- Crie uma nova WLAN para os usuários sem fio.
- Defina as ACLs para os usuários sem fio.

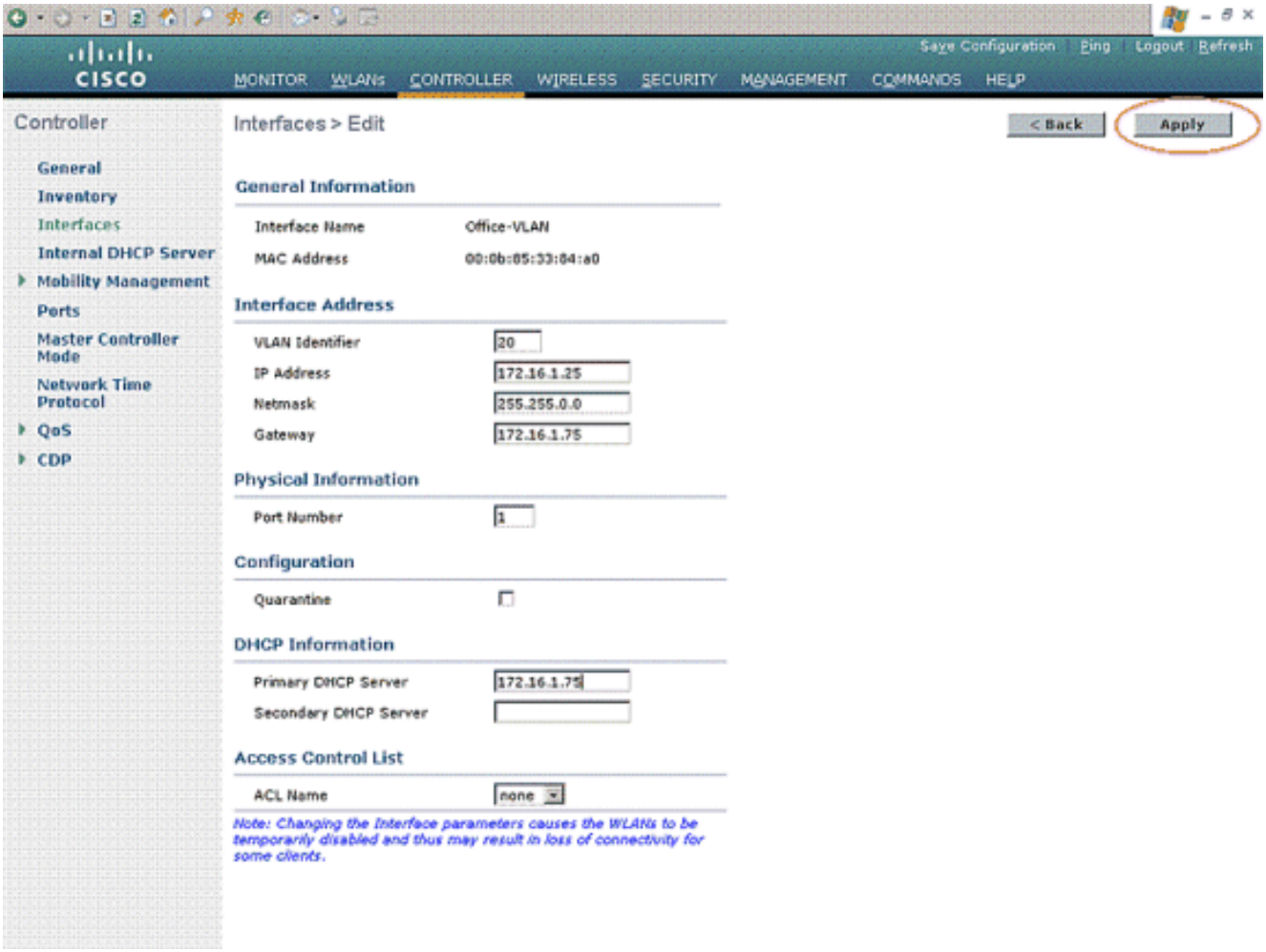
Crie uma VLAN para os usuários sem fio

Para criar uma VLAN para os usuários sem fio, faça o seguinte.

1. Vá para a GUI da WLC e escolha **Controller > Interfaces**. A janela Interfaces é exibida. Essa janela lista as interfaces configuradas no controlador.
2. Clique em **New** para criar uma nova interface dinâmica.
3. Na janela **Interfaces > New**, insira o nome da interface e o ID da VLAN. Em seguida, clique em Aplicar. Neste exemplo, a interface dinâmica é denominada Office-VLAN, e a ID da VLAN é atribuída a
20.



4. Na janela **Interfaces > Edit**, insira o endereço IP, a máscara de sub-rede e o gateway padrão da interface dinâmica. Atribua a uma porta física na WLC e insira o endereço IP do servidor DHCP. Em seguida, clique em
Aplicar.



Para este exemplo, estes parâmetros são usados para a interface Office-VLAN:

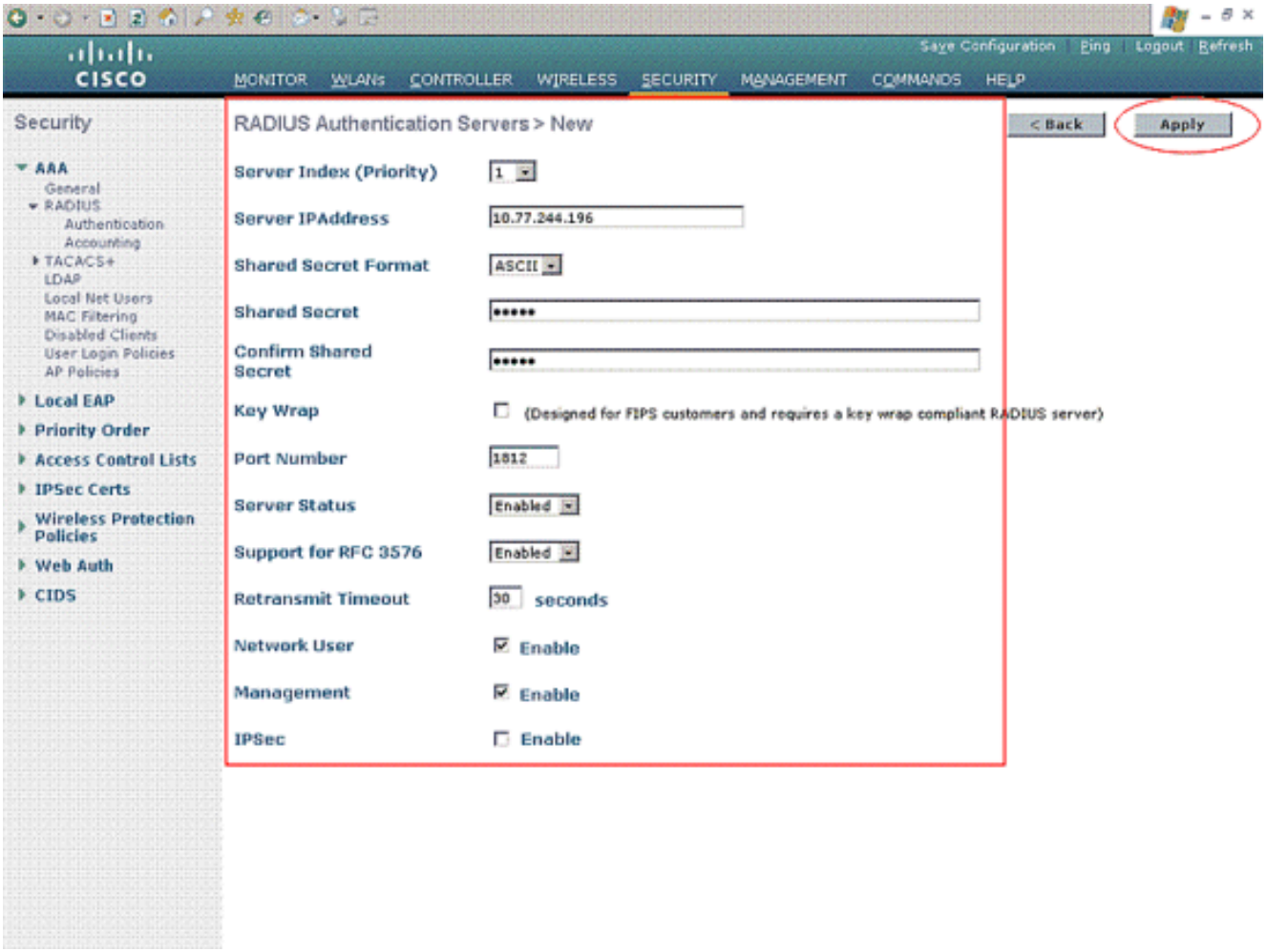
```
Office-VLAN
IP address: 172.16.1.25
Netmask: 255.255.0.0
Default gateway: 172.16.1.75 (sub-interface on Router R1)
Port on WLC: 1
DHCP server: 172.16.1.75
```

Configurar a WLC para autenticação com o Cisco Secure ACS

A WLC precisa ser configurada para encaminhar as credenciais do usuário a um servidor RADIUS externo (neste caso, o Cisco Secure ACS). O servidor RADIUS valida as credenciais do usuário e retorna o atributo de nome da ACL para a WLC após a autenticação bem-sucedida do usuário sem fio.

Conclua estes passos para configurar a WLC para o servidor RADIUS:

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 **Servidores de Autenticação RADIUS > Novo**. Esses parâmetros incluem o endereço IP do servidor RADIUS, o segredo compartilhado, o número da porta e o status do servidor.

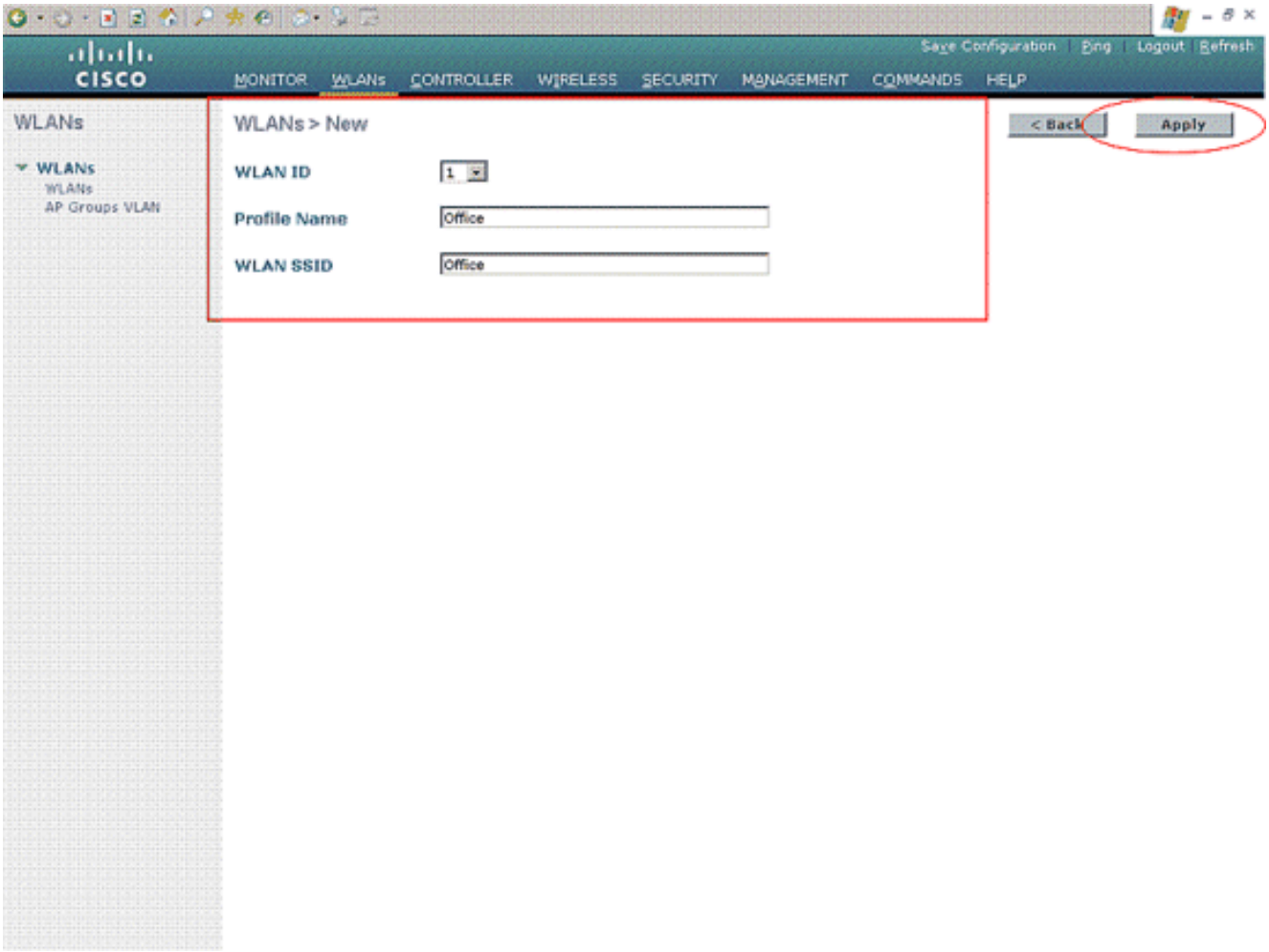


3. As caixas de seleção **Network User** and **Management** determinam se a autenticação baseada em RADIUS se aplica a usuários de gerenciamento e rede. Este exemplo usa o Cisco Secure ACS como o servidor RADIUS com endereço IP 10.77.244.196. Clique em Apply.

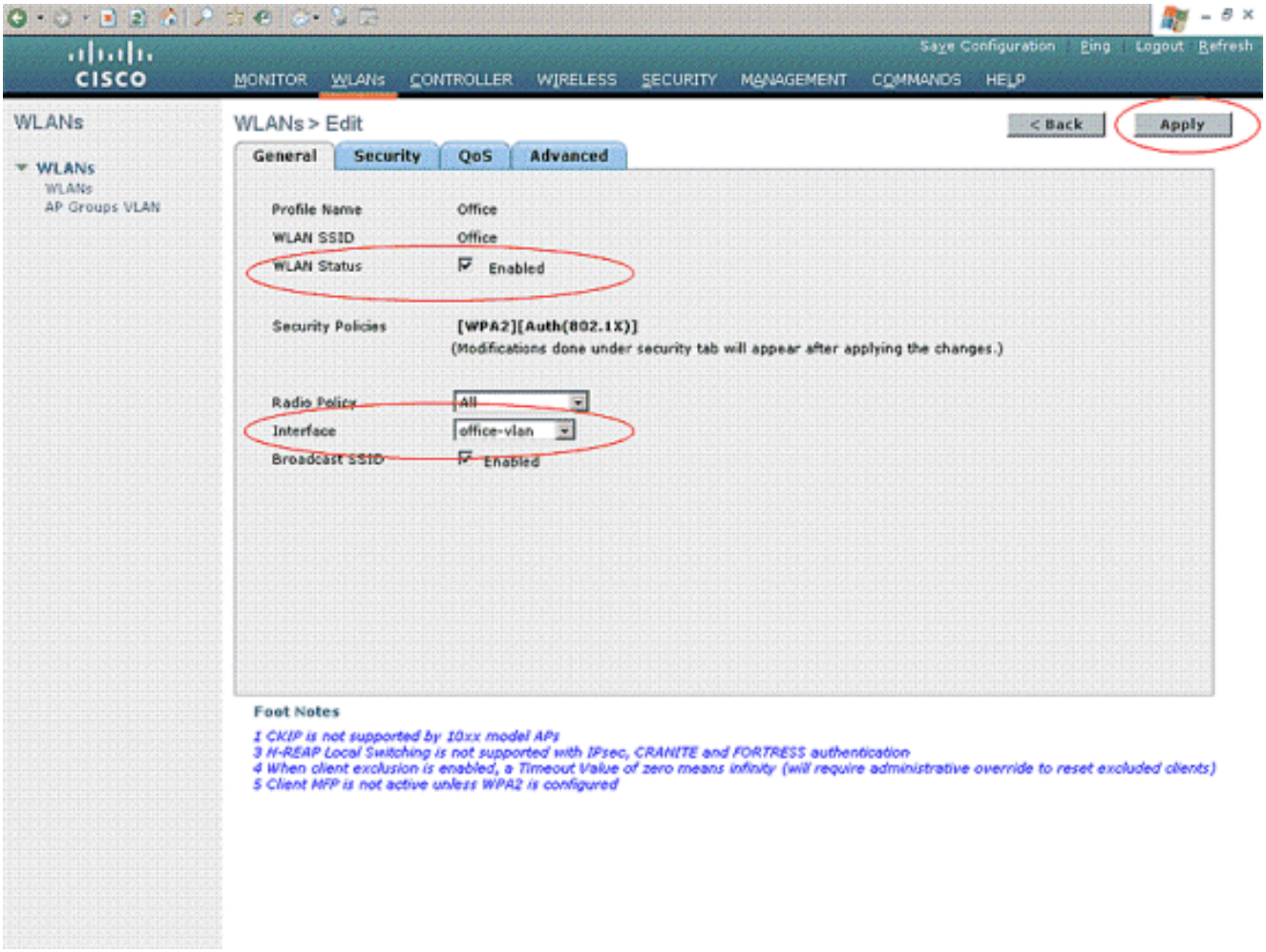
Crie uma nova WLAN para os usuários sem fio

Em seguida, é necessário criar uma WLAN à qual os usuários sem fio possam se conectar. Para criar uma nova WLAN, faça o seguinte:

1. Na GUI da controladora Wireless LAN, clique em **WLANs**. Esta página lista as WLANs que existem na controladora.
2. Escolha **New** para criar uma nova WLAN. Insira o ID da WLAN, o Nome do perfil e o SSID da WLAN para a WLAN e clique em **Aplicar**. Para esta configuração, crie um WLAN **Office**.

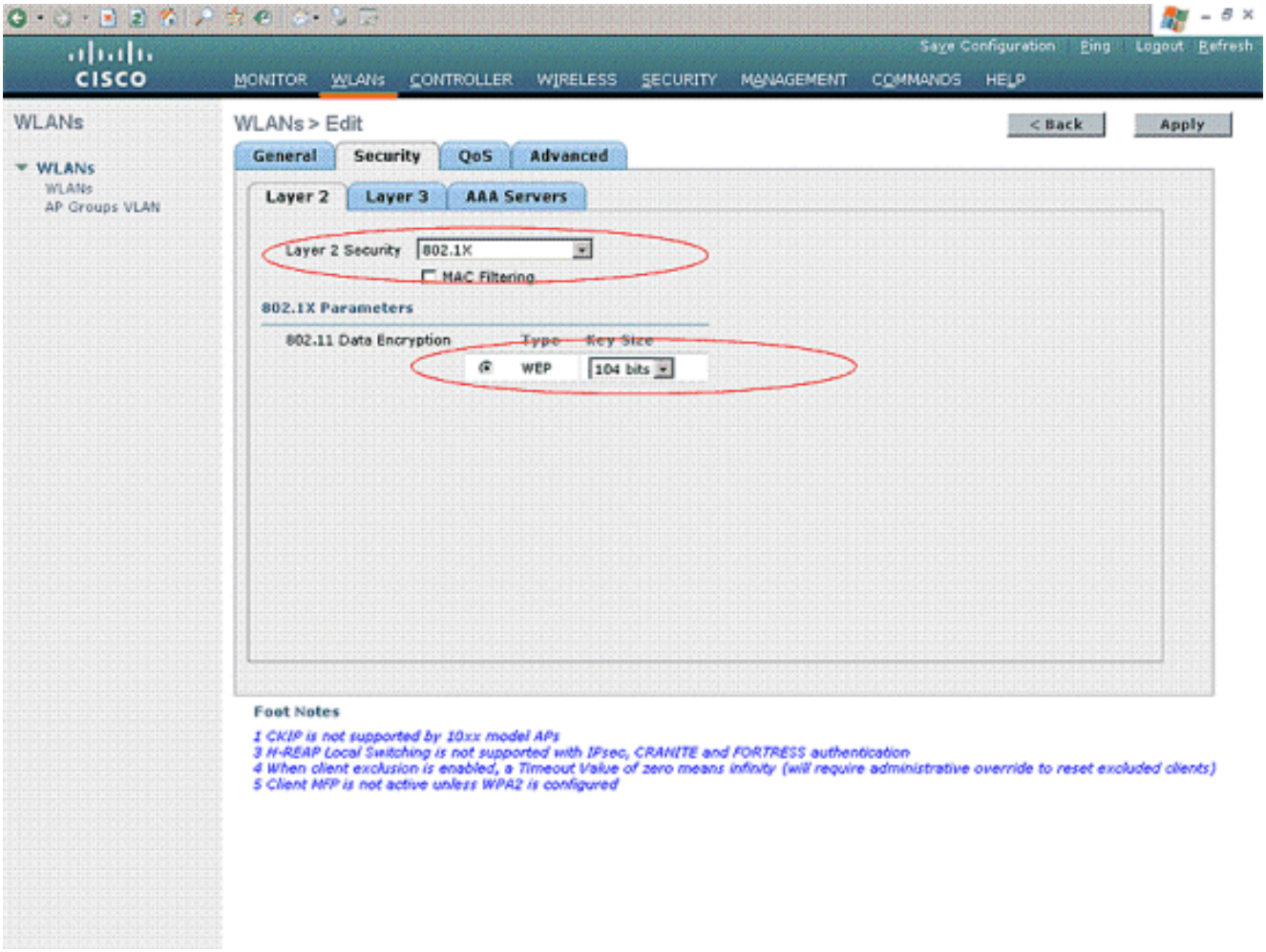


3. Depois de criar uma nova WLAN, a página **WLAN > Edit** para a nova WLAN é exibida. Nesta página, você pode definir vários parâmetros específicos para esta WLAN que incluem políticas gerais, segurança, QoS e parâmetros avançados.

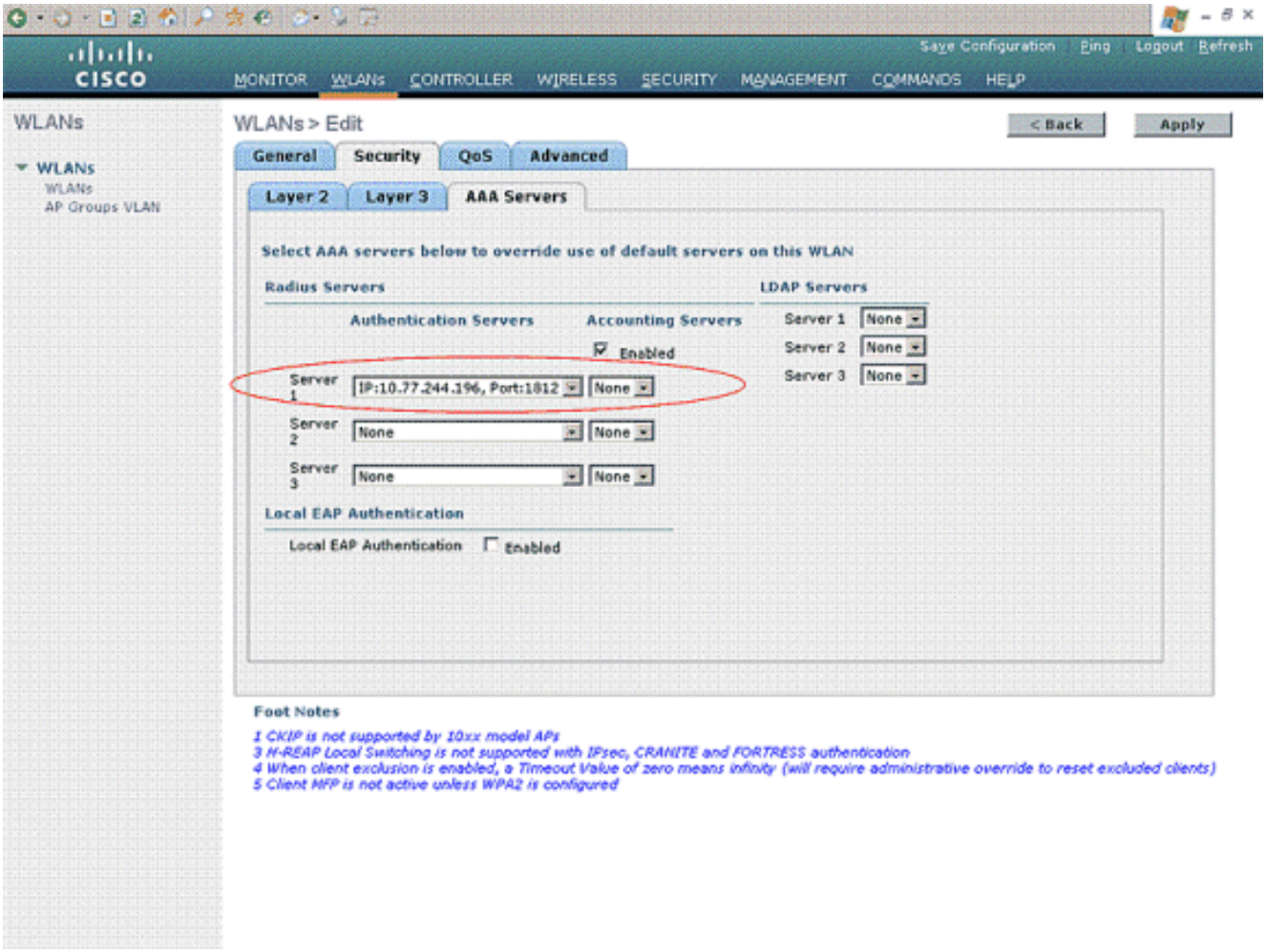


Verifique **WLAN Status** em General policies (Políticas gerais) para habilitar a WLAN. Escolha a interface apropriada no menu suspenso. Neste exemplo, use a interface **Office-vlan**. Os outros parâmetros desta página podem ser modificados com base no requisito da rede WLAN.

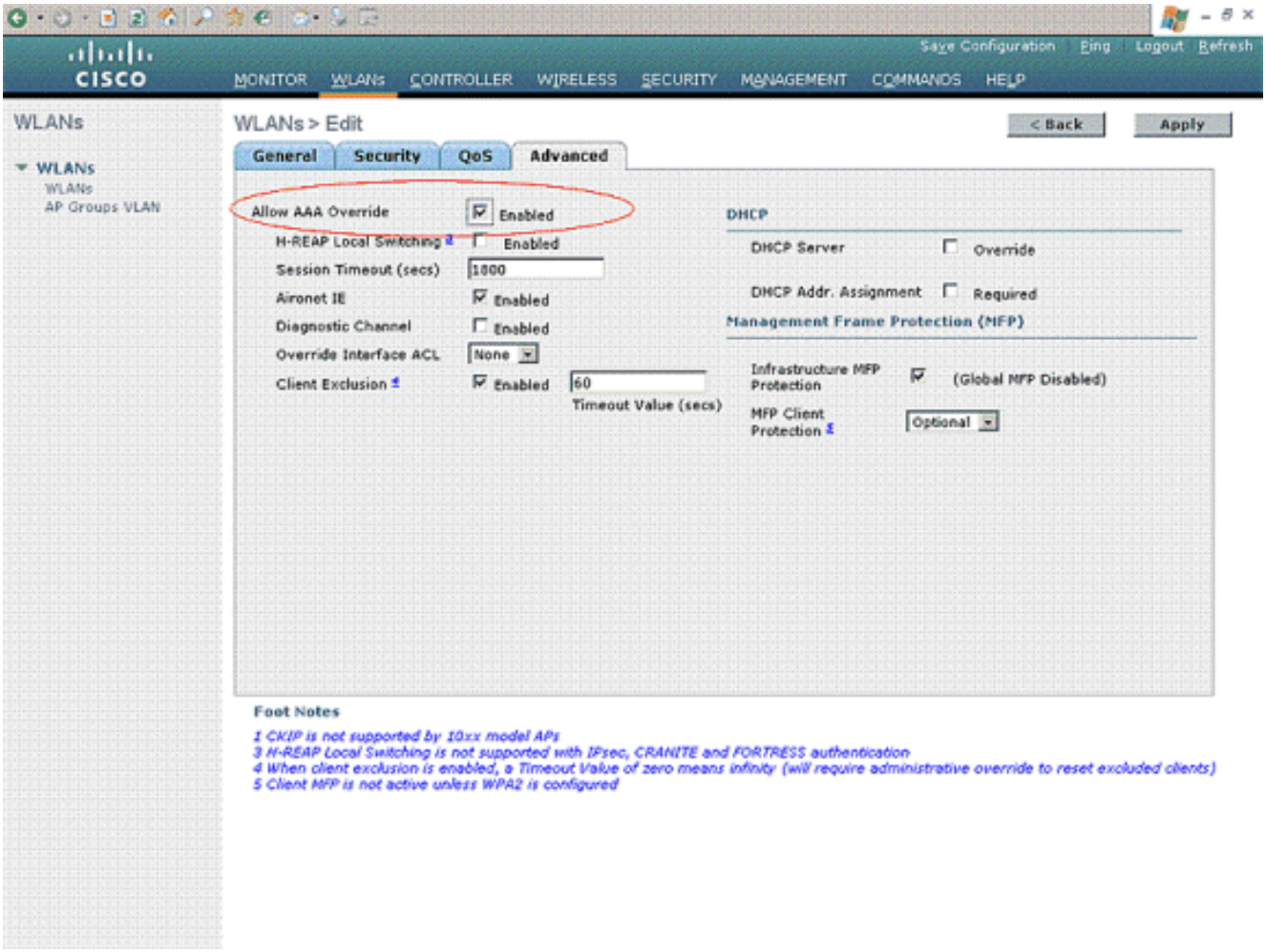
4. Escolha a **guia Segurança**. Escolha **802.1x** no menu suspenso de segurança da Camada 2 (já que essa é uma autenticação LEAP). Escolha o tamanho apropriado da chave WEP em parâmetros
802.1x.



5. Na guia Segurança, escolha a subguia **servidor AAA**. Escolha o servidor AAA usado para autenticar clientes sem fio. Neste exemplo, use o servidor ACS 10.77.244.196 para autenticar clientes sem
fio.



6. Escolha a guia **Avançado**. Marque **Permitir substituição de AAA** para configurar a substituição de política de usuário através da AAA em uma LAN sem fio.



Quando a substituição de AAA está habilitada e um cliente tem parâmetros conflitantes de autenticação de LAN sem fio de controlador AAA e Cisco Wireless LAN, a autenticação do cliente é executada pelo servidor AAA. Como parte dessa autenticação, o sistema operacional move os clientes da VLAN LAN sem fio da solução de LAN sem fio da Cisco para uma VLAN retornada pelo servidor AAA e predefinida na configuração da interface do controlador de LAN sem fio da Cisco, o que acontece somente quando configurada para filtragem de MAC, 802.1X e/ou operação WPA. Em todos os casos, o sistema operacional também usa QoS, DSCP, valores de marca de prioridade 802.1p e ACL fornecidos pelo servidor AAA, desde que sejam predefinidos na configuração da interface do controlador Cisco Wireless LAN.

7. Escolha os outros parâmetros com base nos requisitos da rede. Clique em Apply.

Definir as ACLs para os usuários

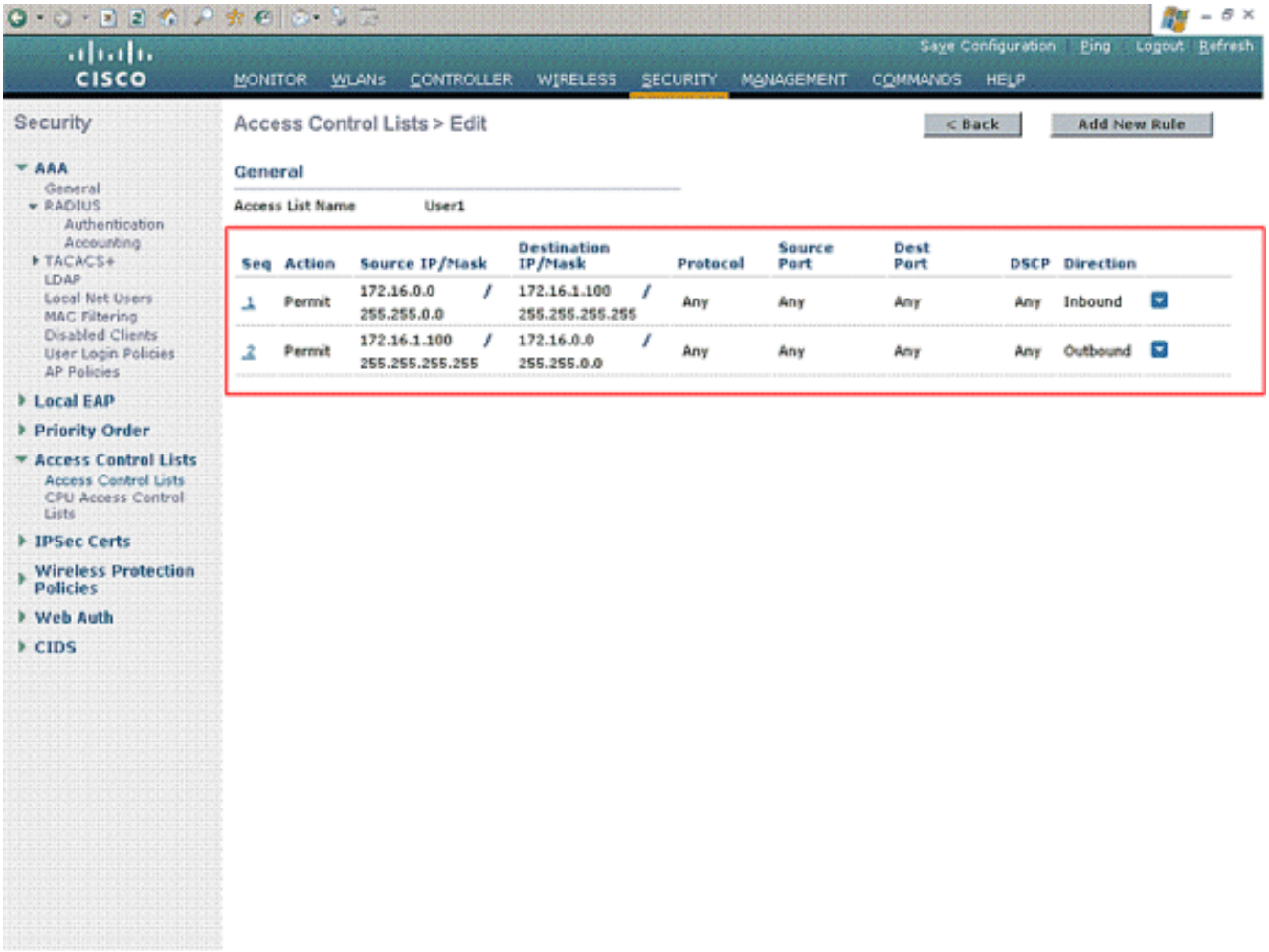
Você precisa criar duas ACLs para esta configuração:

- ACL1: Para fornecer acesso a User1 somente ao servidor 172.16.1.100
- ACL2: Para fornecer acesso ao Usuário2 ao servidor somente 172.16.1.50

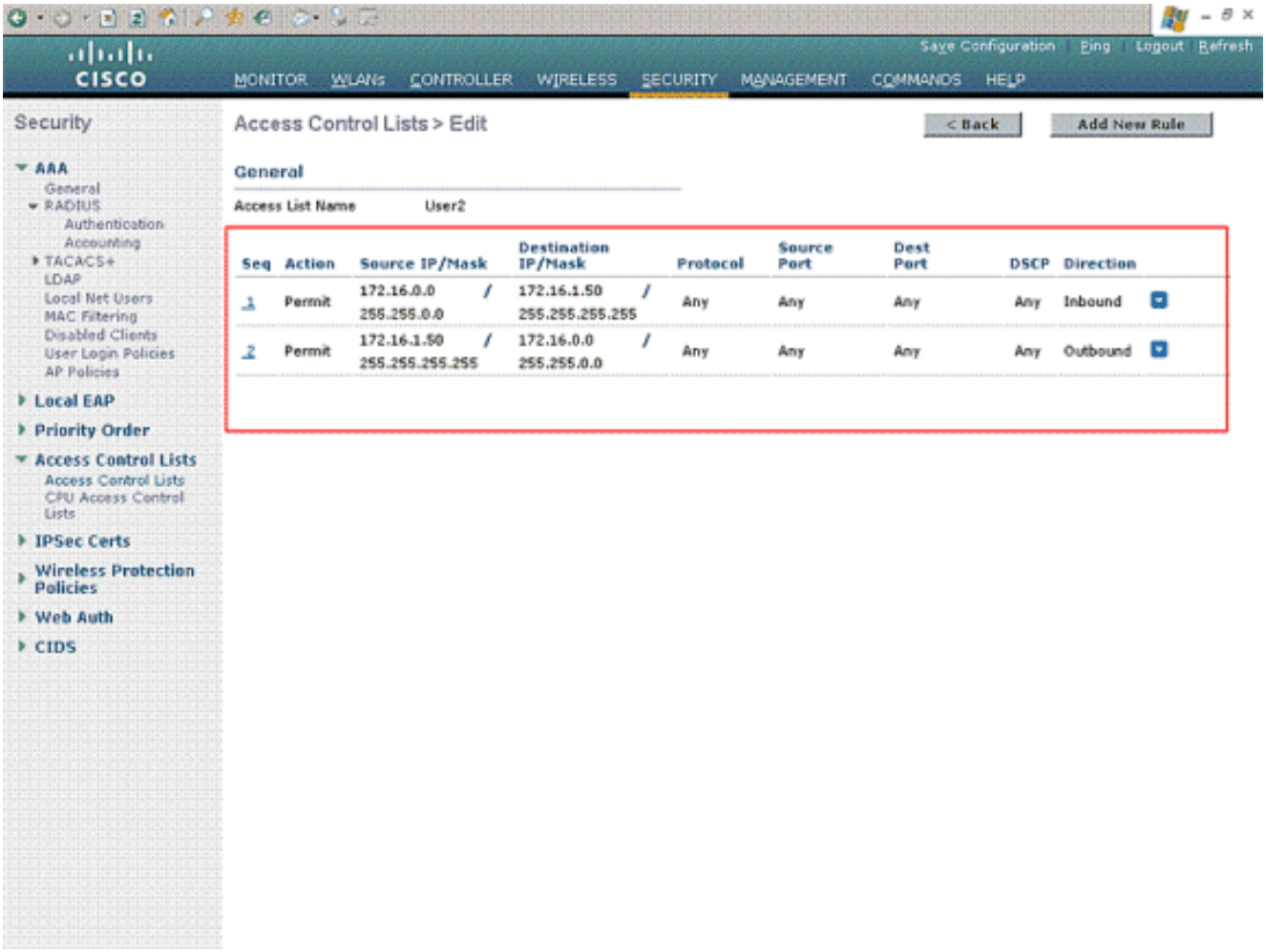
Conclua estes passos para configurar as ACLs na WLC:

1. Na GUI do WLC, escolha **Security > Access Control Lists**. A página Listas de controle de acesso é exibida. Esta página lista as ACLs configuradas na WLC. Também permite editar ou remover qualquer uma das ACLs. Para criar uma nova ACL, clique em **Novo**.
2. Esta página permite criar novas ACLs. Digite o nome da ACL e clique em **Apply** (**Aplicar**). Depois que a ACL for criada, clique em **Editar** para criar regras para a ACL.

3. O usuário1 precisa ter acesso somente ao servidor 172.16.1.100 e deve ter acesso negado a todos os outros dispositivos. Para isso, você precisa definir essas regras.Consulte o Exemplo de Configuração de ACLs em Wireless LAN Controller para obter mais informações sobre como configurar ACLs em Wireless LAN Controllers.



4. Da mesma forma, você precisa criar uma ACL para User2, que permita que User2 acesse somente o servidor 172.16.1.50. Esta é a ACL necessária para o User2.



Agora você configurou o Wireless LAN Controller para esta configuração. A próxima etapa é configurar o servidor Cisco Secure Access Control para autenticar os clientes sem fio e retornar o atributo Nome da ACL para a WLC após a autenticação bem-sucedida.

Configurar o servidor Cisco Secure ACS

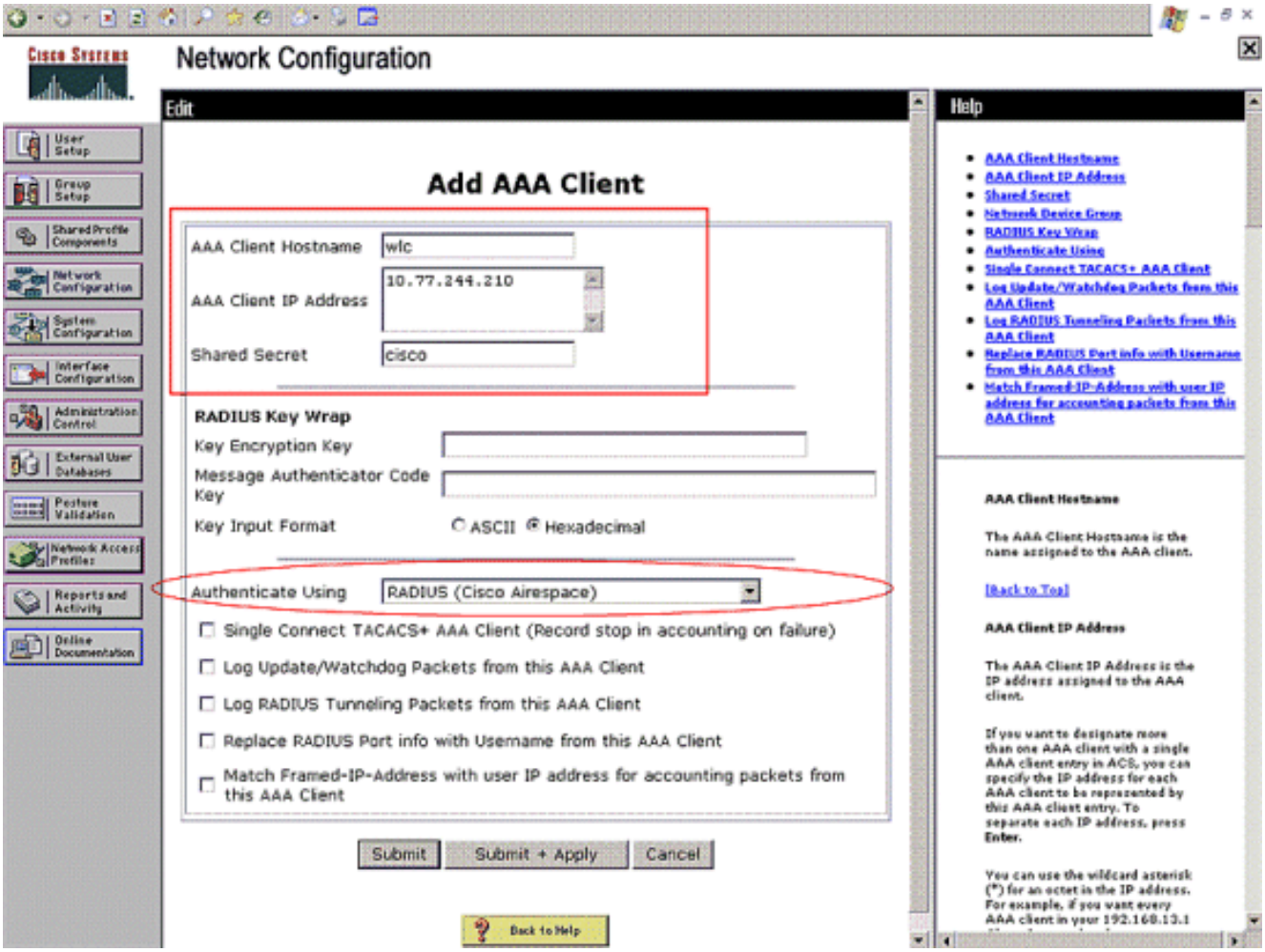
Para que o Cisco Secure ACS possa autenticar clientes sem fio, você precisa concluir estas etapas:

- Configure o Wireless LAN Controller como um cliente AAA no Cisco Secure ACS.
- Configure os perfis de usuário e usuários no Cisco Secure ACS.

Configure o controlador de LAN sem fio como um cliente AAA no Cisco Secure ACS

Para configurar o Wireless LAN Controller como um cliente AAA no Cisco Secure ACS, faça o seguinte:

1. Clique em **Network Configuration > Add AAA client**. A página **Adicionar cliente AAA** é exibida. Nesta página, defina o nome do sistema WLC, o endereço IP da Interface de Gerenciamento, o segredo compartilhado e autentique usando o **Radius Airespace**. Aqui está um
exemplo:



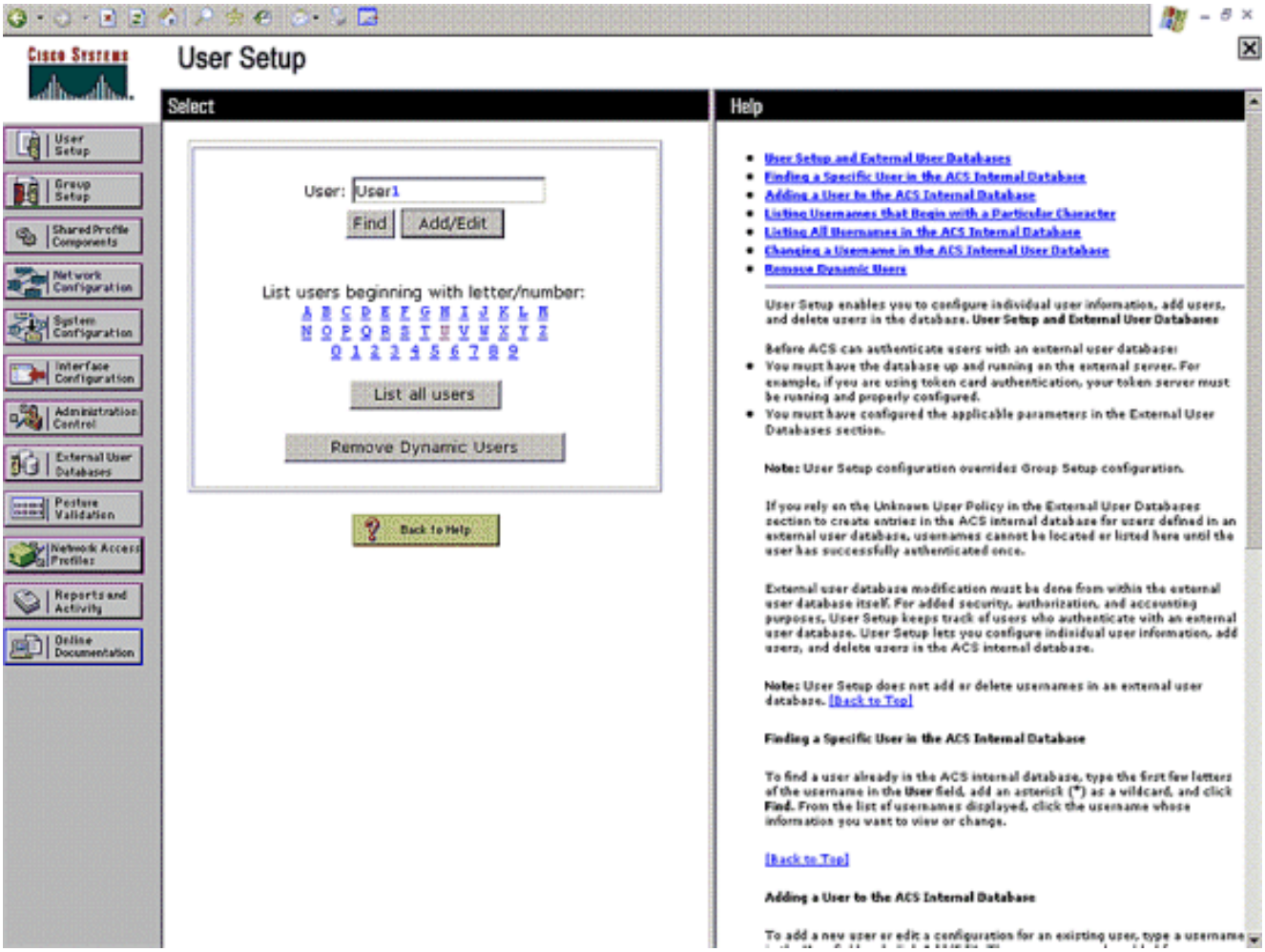
Observação: o segredo compartilhado configurado no Cisco Secure ACS deve corresponder ao segredo compartilhado configurado na WLC em **RADIUS Authentication Servers > New**.

2. Clique em **Enviar+Aplicar**.

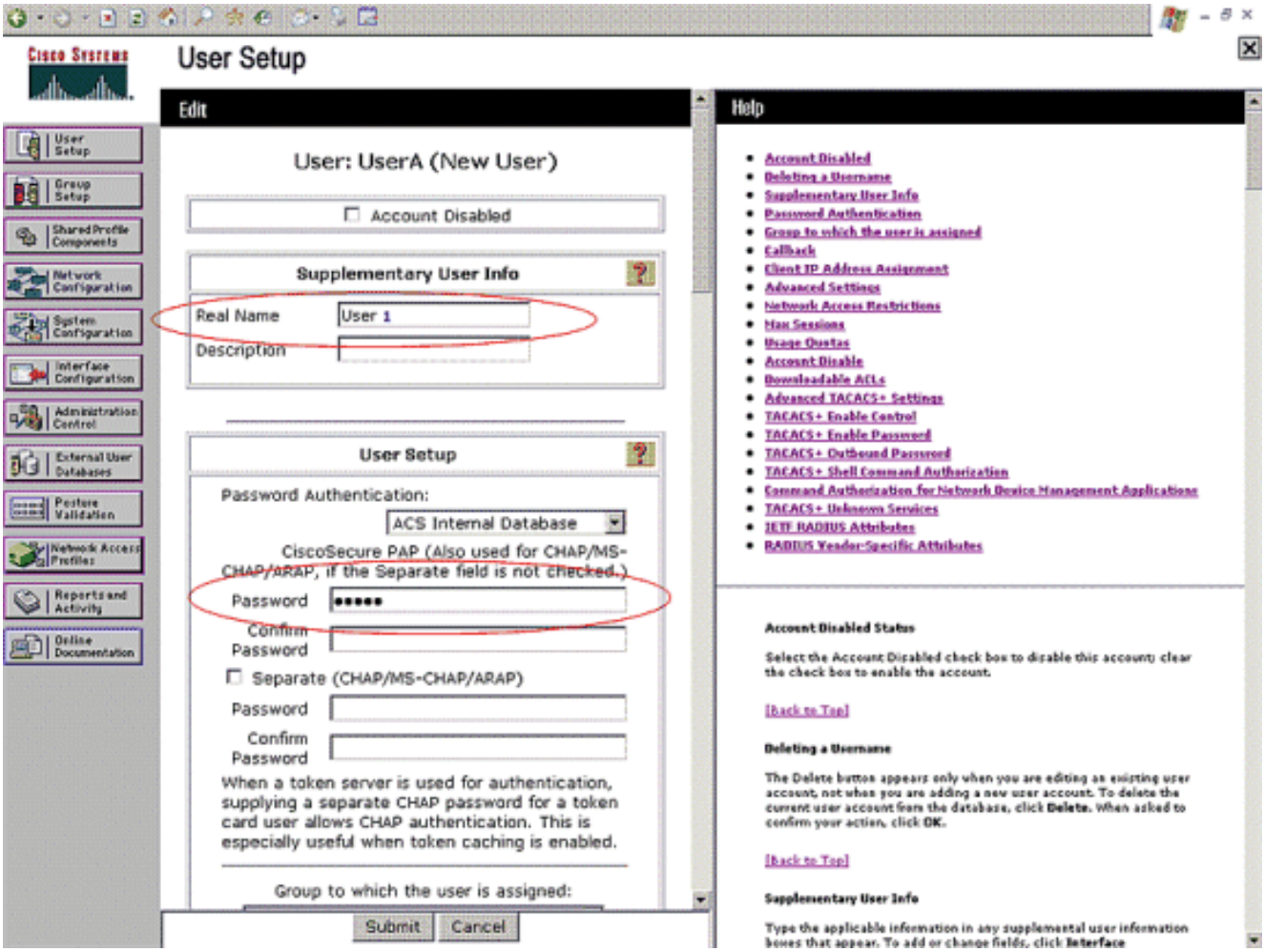
Configurar usuários e perfil de usuário no Cisco Secure ACS

Para configurar usuários no Cisco Secure ACS, faça o seguinte:

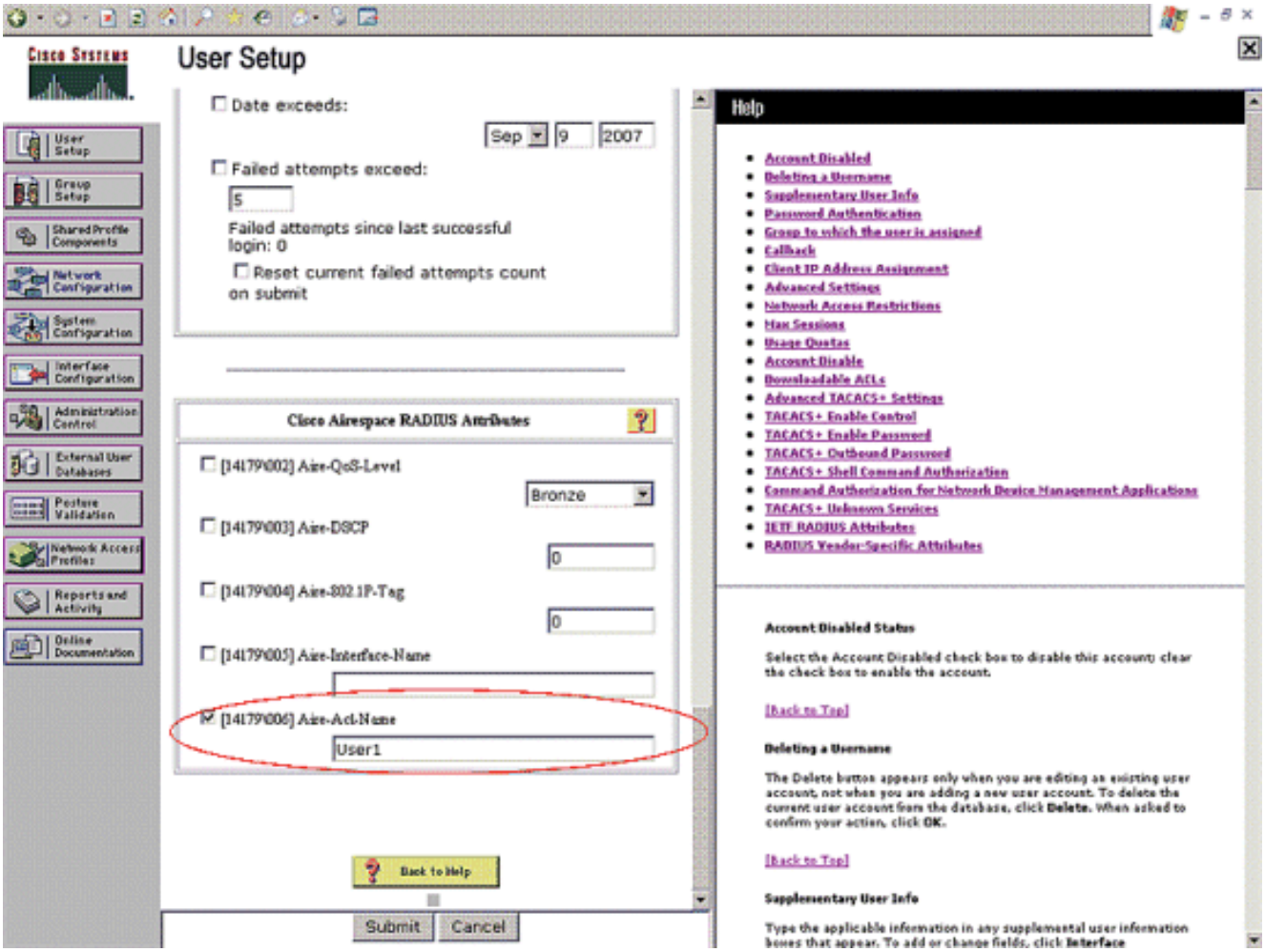
1. Escolha **User Setup** na GUI do ACS, digite o nome de usuário e clique em **Add/Edit**. Neste exemplo, o usuário é
User1.



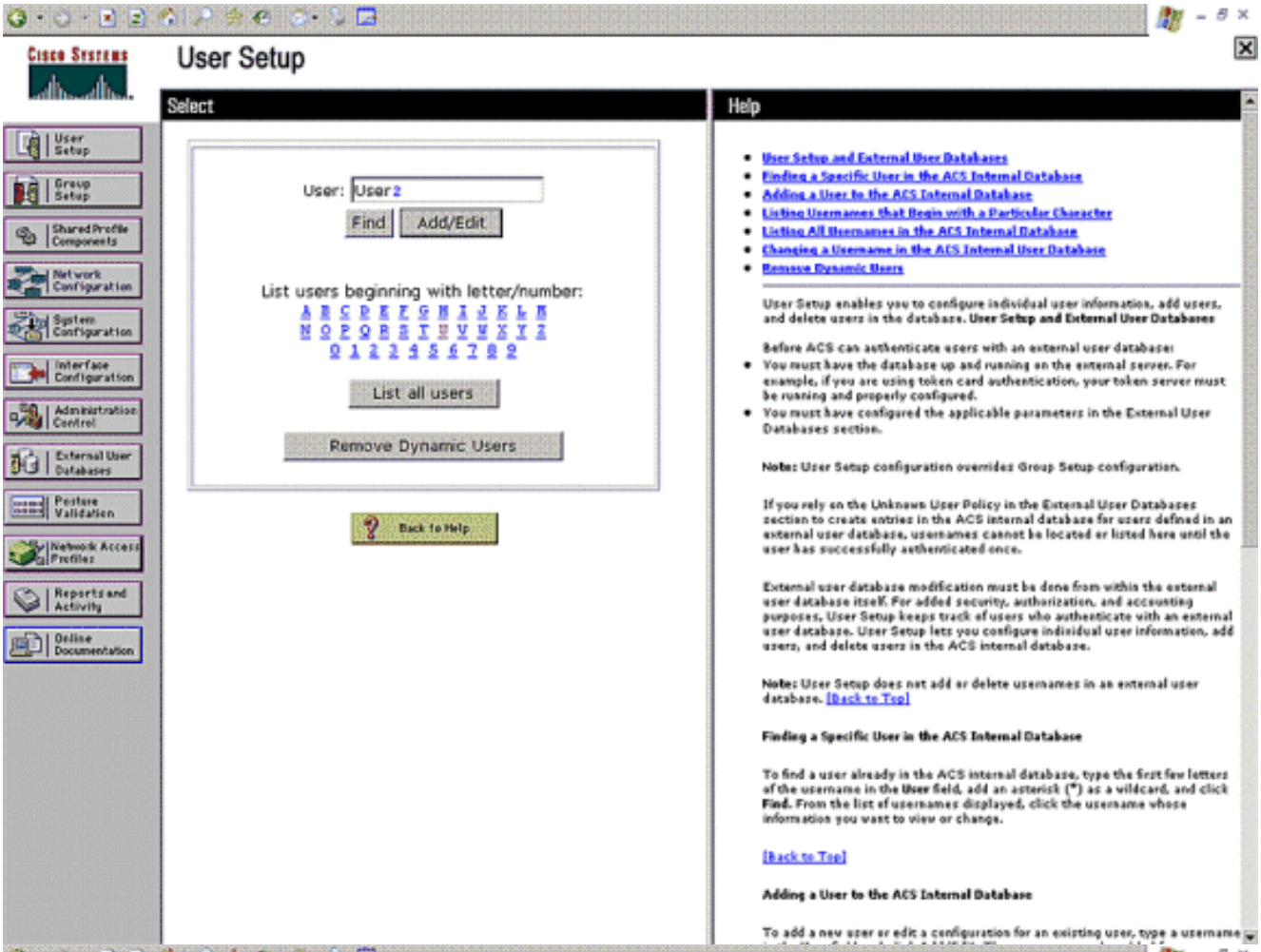
2. Quando a página **User Setup** for exibida, defina todos os parâmetros específicos do usuário. Neste exemplo, os atributos nome de usuário, senha, Informações de usuário suplementares e RADIUS estão configurados porque você só precisa desses parâmetros para autenticação EAP.

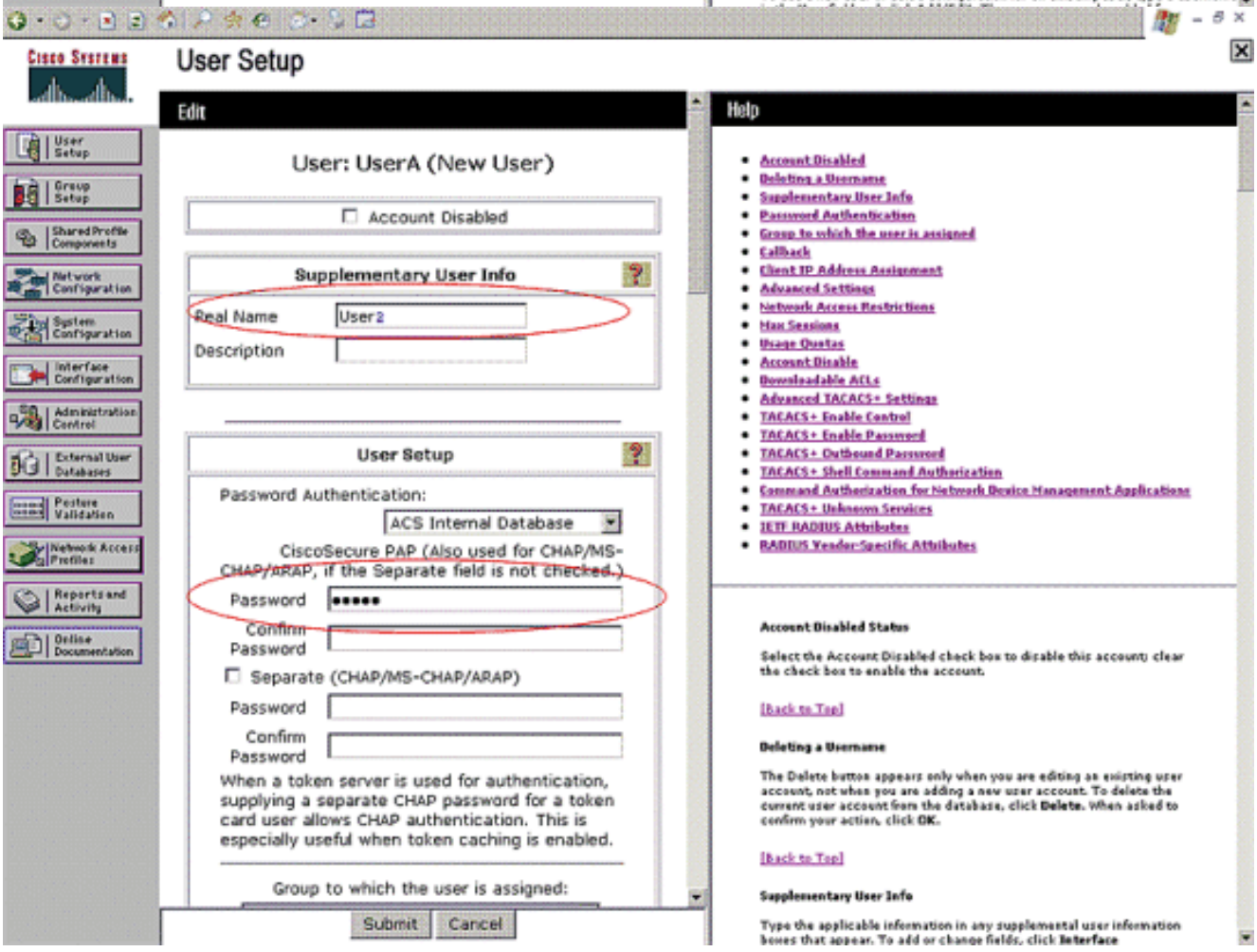


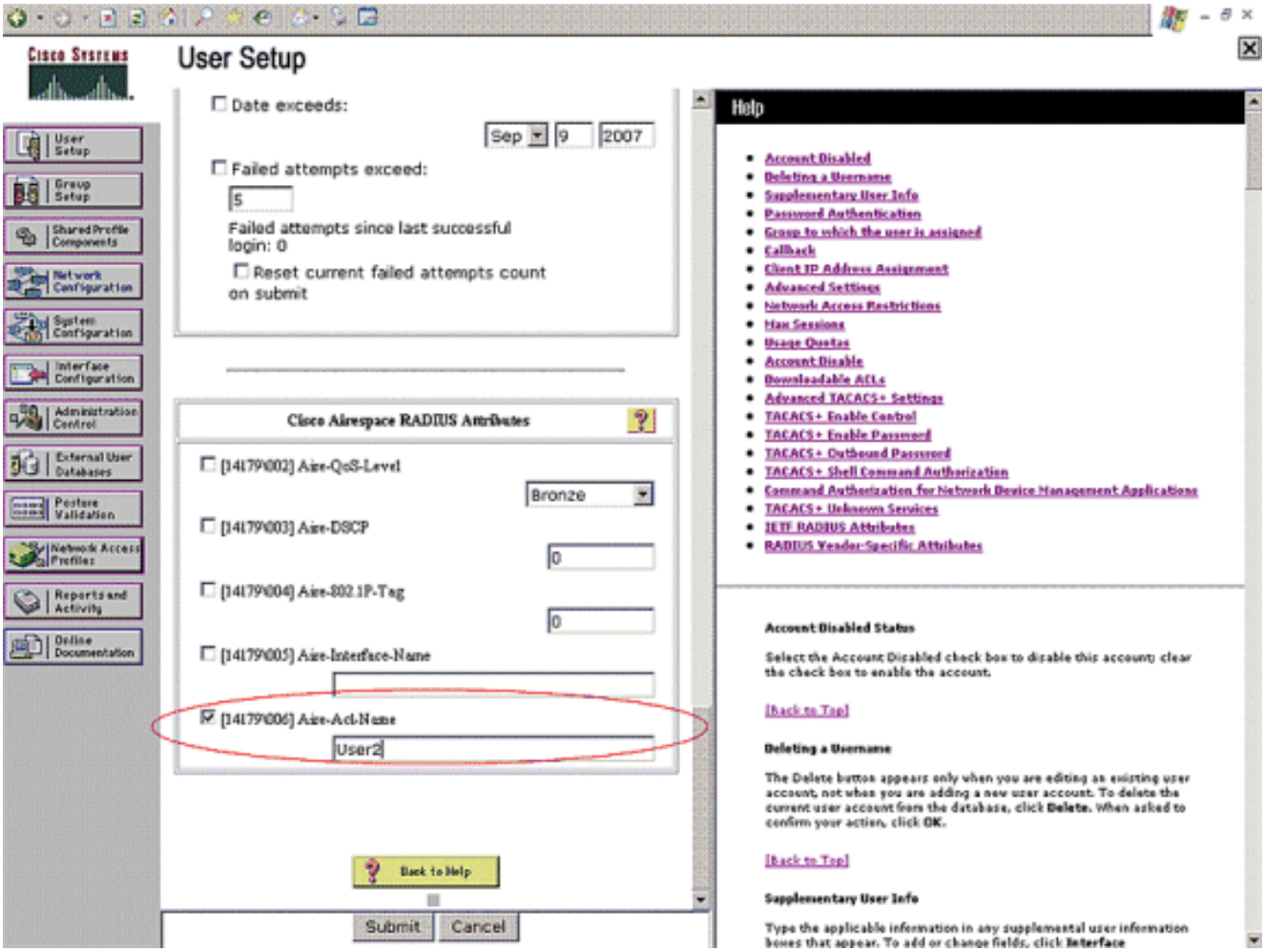
Role para baixo até ver os atributos do Cisco Airespace RADIUS específicos ao usuário. Verifique o **Aire-ACL-Name** para permitir que o ACS retorne o nome da ACL ao WLC juntamente com a resposta de autenticação bem-sucedida. Para User1, crie um ACL User1 na WLC. Insira o nome da ACL como
User1.



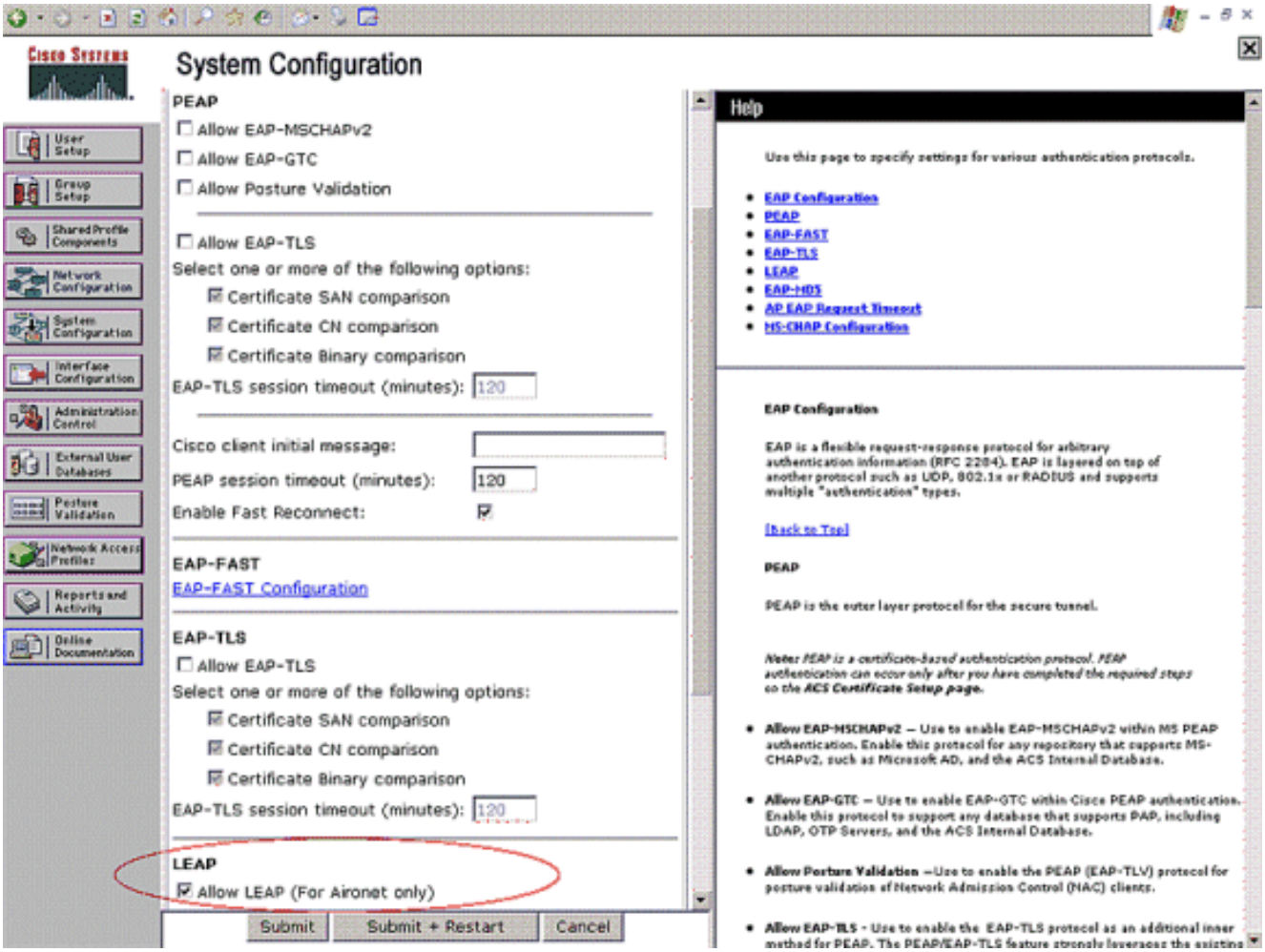
3. Repita o mesmo procedimento para criar User2 como mostrado aqui.


Cisco Systems
User Setup
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
Select
User: User2
Find
Add/Edit
List users beginning with letter/number:
A B C D E F G H I J K L M
N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9
List all users
Remove Dynamic Users
Back to Help
Help
User Setup and External User Databases
Finding a Specific User in the ACS Internal Database
Adding a User to the ACS Internal Database
Listing Usernames that Begin with a Particular Character
Listing All Usernames in the ACS Internal Database
Changing a Username in the ACS Internal User Database
Remove Dynamic Users
User Setup enables you to configure individual user information, add users, and delete users in the database. User Setup and External User Databases
Before ACS can authenticate users with an external user database:
You must have the database up and running on the external server. For example, if you are using token card authentication, your token server must be running and properly configured.
You must have configured the applicable parameters in the External User Databases section.
Note: User Setup configuration overrides Group Setup configuration.
If you rely on the Unknown User Policy in the External User Databases section to create entries in the ACS internal database for users defined in an external user database, usernames cannot be located or listed here until the user has successfully authenticated once.
External user database modification must be done from within the external user database itself. For added security, authorization, and accounting purposes, User Setup keeps track of users who authenticate with an external user database. User Setup lets you configure individual user information, add users, and delete users in the ACS internal database.
Note: User Setup does not add or delete usernames in an external user database. [Back to Top]
Finding a Specific User in the ACS Internal Database
To find a user already in the ACS internal database, type the first few letters of the username in the User field, add an asterisk (*) as a wildcard, and click Find. From the list of usernames displayed, click the username whose information you want to view or change.
[Back to Top]
Adding a User to the ACS Internal Database
To add a new user or edit a configuration for an existing user, type a username


Cisco Systems
User Setup
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
Edit
User: UserA (New User)
Account Disabled
Supplementary User Info
Real Name
User2
Description
User Setup
Password Authentication:
ACS Internal Database
CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)
Password
Confirm Password
Separate (CHAP/MS-CHAP/ARAP)
Password
Confirm Password
When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.
Group to which the user is assigned:
Submit
Cancel
Help
Account Disabled
Deleting a Username
Supplementary User Info
Password Authentication
Group to which the user is assigned
Callback
Client IP Address Assignment
Advanced Settings
Network Access Restrictions
Max Sessions
Usage Quotas
Account Disable
Downloadable ACLs
Advanced TACACS+ Settings
TACACS+ Enable Control
TACACS+ Enable Password
TACACS+ Outbound Password
TACACS+ Shell Command Authorization
Command Authorization for Network Device Management Applications
TACACS+ Unknown Services
IETF RADIUS Attributes
RADIUS Vendor-Specific Attributes
Account Disabled Status
Select the Account Disabled check box to disable this account; clear the check box to enable the account.
[Back to Top]
Deleting a Username
The Delete button appears only when you are editing an existing user account, not when you are adding a new user account. To delete the current user account from the database, click Delete. When asked to confirm your action, click OK.
[Back to Top]
Supplementary User Info
Type the applicable information in any supplemental user information boxes that appear. To add or change fields, click Interface



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.



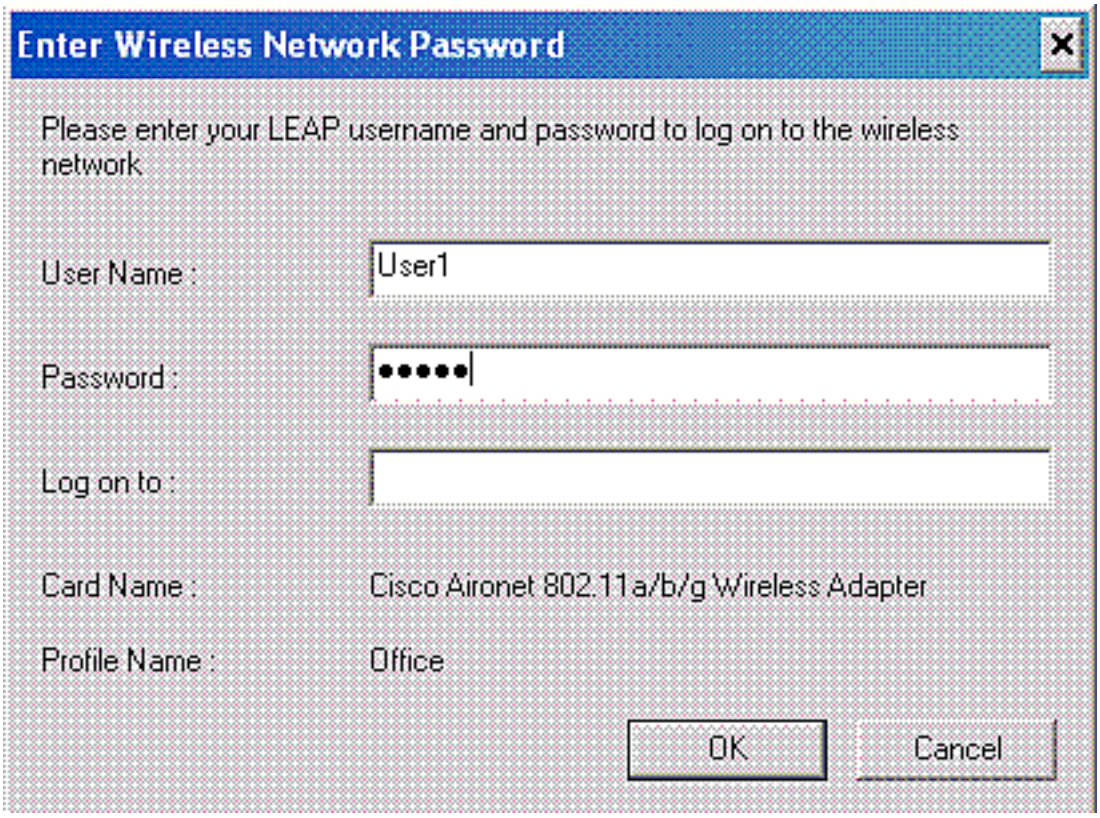
Verificar

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

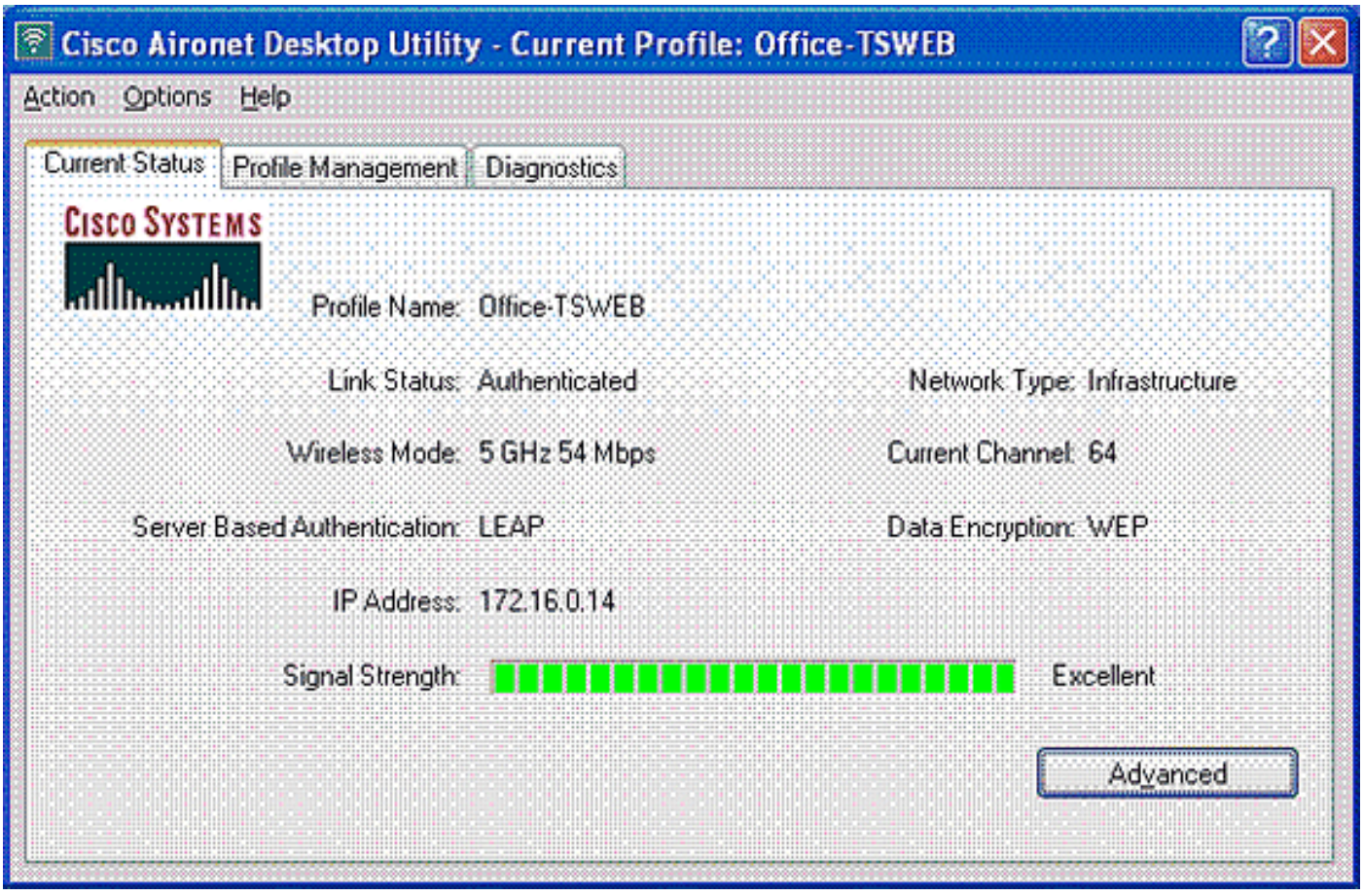
Tente associar um cliente sem fio ao AP Lightweight com autenticação LEAP para verificar se a configuração funciona como esperado.

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. Isso é o que acontece quando o Usuário1 tenta autenticar no LAP.



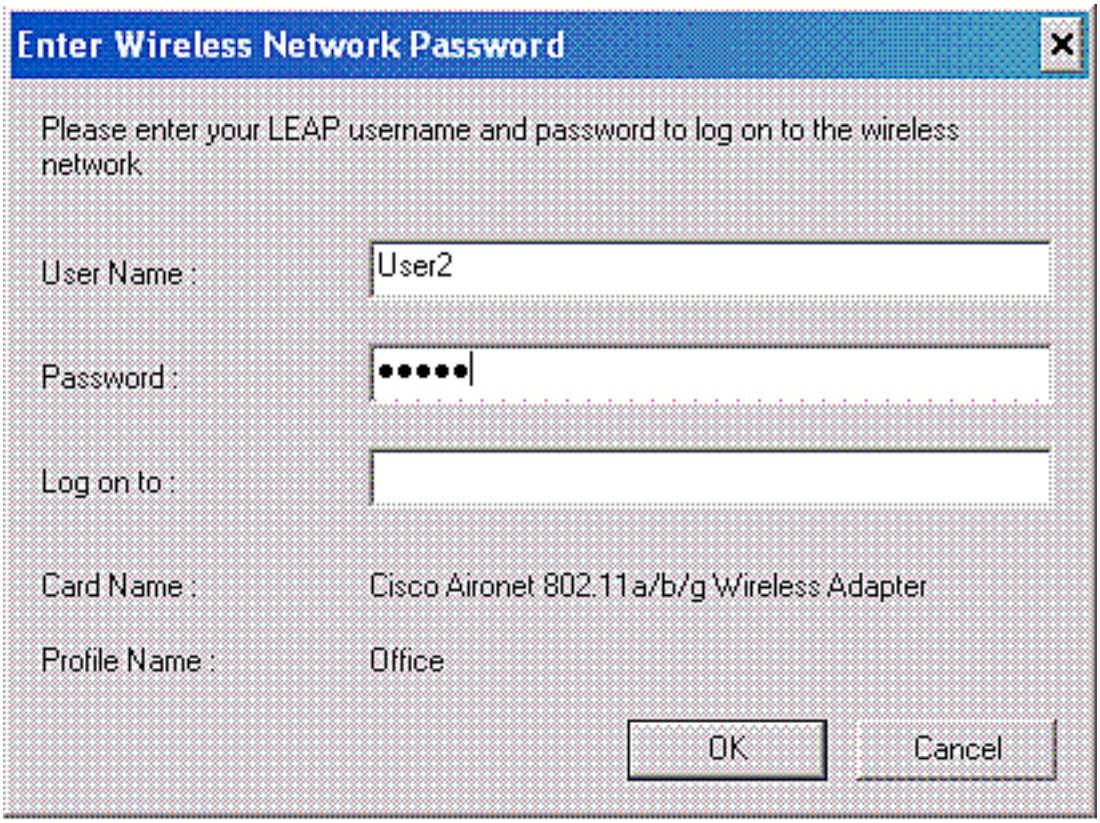
O AP leve e, em seguida, a WLC transmitem as credenciais do usuário ao servidor RADIUS externo (Cisco Secure ACS) para validar as credenciais. O servidor RADIUS compara os dados com o banco de dados do usuário e, após a autenticação bem-sucedida, retorna o nome da ACL configurado para o usuário para a WLC. Nesse caso, a ACL User1 é retornada à WLC.

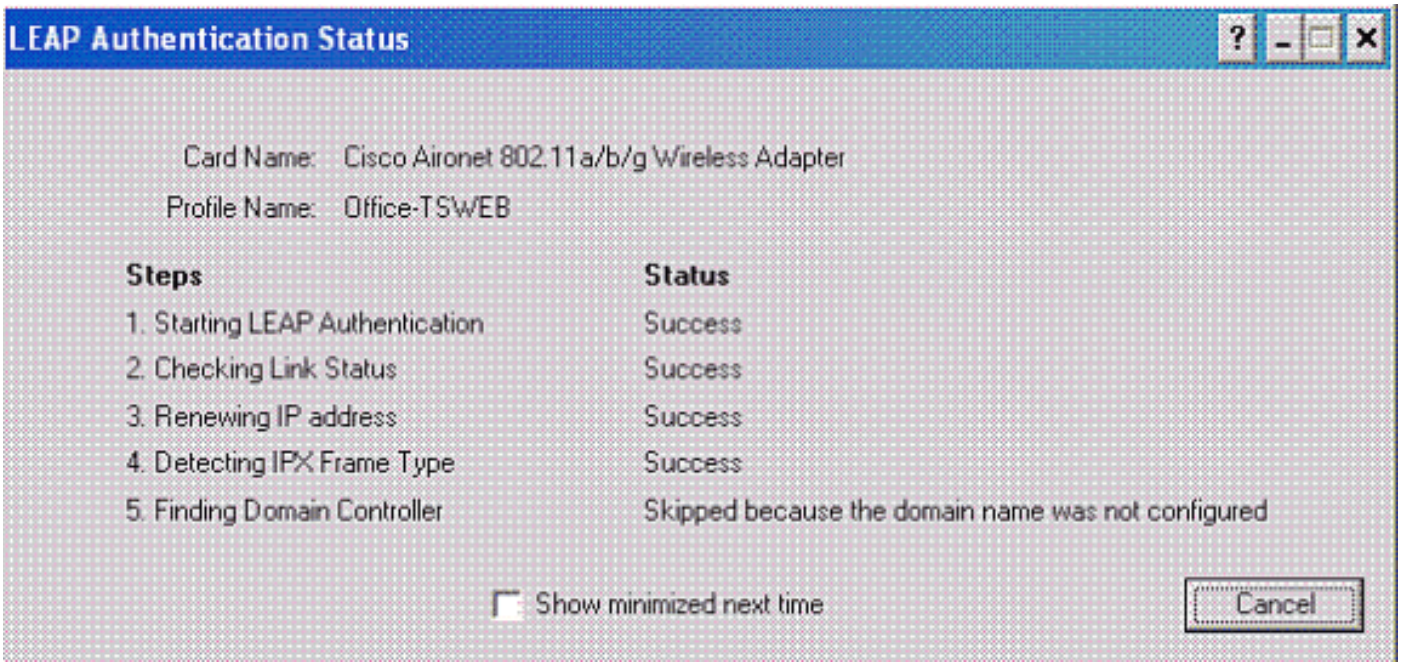


A controladora Wireless LAN aplica essa ACL ao User1. Esta saída de ping mostra que User1 pode acessar somente o servidor 172.16.1.100, mas não qualquer outro dispositivo.

```
D:\Documents and Settings\Administrator>ping 172.16.1.100

Pinging 172.16.1.100 with 32 bytes of data:

Reply from 172.16.1.100: bytes=32 time=3ms TTL=255
Reply from 172.16.1.100: bytes=32 time=1ms TTL=255
Reply from 172.16.1.100: bytes=32 time=1ms TTL=255
Reply from 172.16.1.100: bytes=32 time=1ms TTL=255

Ping statistics for 172.16.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 3ms, Average = 1ms

D:\Documents and Settings\Administrator>ping 172.16.1.50

Pinging 172.16.1.50 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.16.1.50:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Da mesma forma, quando o User2 tenta acessar a WLAN, o servidor RADIUS, após a autenticação bem-sucedida, retorna a ACL User2 para a WLC.





A controladora Wireless LAN aplica essa ACL ao User2. Esta saída de ping mostra que User2 é capaz de acessar somente o servidor 172.16.1.50, mas não qualquer outro dispositivo.

```
D:\Documents and Settings\Administrator>ping 172.16.1.50

Pinging 172.16.1.50 with 32 bytes of data:

Reply from 172.16.1.50: bytes=32 time=3ms TTL=255
Reply from 172.16.1.50: bytes=32 time=18ms TTL=255
Reply from 172.16.1.50: bytes=32 time=1ms TTL=255
Reply from 172.16.1.50: bytes=32 time=1ms TTL=255

Ping statistics for 172.16.1.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 18ms, Average = 5ms

D:\Documents and Settings\Administrator>ping 172.16.1.100

Pinging 172.16.1.100 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.16.1.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Troubleshoot

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

No Wireless LAN Controller, você também pode usar esses 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
- **debug client <MAC Address>** — Habilita a depuração do cliente sem fio

Aqui está um exemplo do comando **debug aaa all enable**

Observação: algumas das linhas na saída foram movidas para a segunda linha devido a restrições de espaço.

```
Thu Aug 16 14:42:54 2007: AuthenticationRequest: 0xb1ab104
Thu Aug 16 14:42:54 2007:       Callback.....0x85ed228
Thu Aug 16 14:42:54 2007:       protocolType.....0x00140001
Thu Aug 16 14:42:54 2007:       proxyState.....00:40:96:AF:3E:93-03:01
Thu Aug 16 14:42:54 2007:       Packet contains 16 AVPs (not shown)
Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93
Successful transmission of Authentication Packet
   (id 1) to 10.77.244.196:1812, proxy state 00:40:96:af:3e:93-00:00
Thu Aug 16 14:42:54 2007: 00000000: 01 01 00 d0 2d 34 f5 99  b4 19 27 28 eb 5f 35 9c
   ....-4....'(._5.
Thu Aug 16 14:42:54 2007: 00000010: 8f a9 00 dd 01 07 75 73  65 72 31 1f 13 30 30 2d
   ......user1..00-
Thu Aug 16 14:42:54 2007: 00000020: 34 30 2d 39 36 2d 41 46  2d 33 45 2d 39 33 1e 20
   40-96-AF-3E-93..
Thu Aug 16 14:42:54 2007: 00000030: 30 30 2d 30 42 2d 38 35  2d 35 42 2d 46 42 2d 44
   00-0B-85-5B-FB-D
Thu Aug 16 14:42:54 2007: 00000040: 30 3a 4f 66 66 69 63 65  2d 54 53 57 45 42 05 06
   0:Office-TSWEB..
Thu Aug 16 14:42:54 2007: 00000050: 00 00 00 01 04 06 0a 4d  f4 d2 20 05 77 6c 63 1a
   .......M....wlc.
Thu Aug 16 14:42:54 2007: 00000060: 0c 00 00 37 63 01 06 00  00 00 01 06 06 00 00 00
   ...7c...........
Thu Aug 16 14:42:54 2007: 00000070: 02 0c 06 00 00 05 14 3d  06 00 00 00 13 40 06 00
   .......=.....@..
Thu Aug 16 14:42:54 2007: 00000080: 00 00 0d 41 06 00 00 00  06 51 04 32 30 4f 27 02
   ...A.....Q.20O'.
Thu Aug 16 14:42:54 2007: 00000090: 01 00 25 11 01 00 18 1d  87 9d 0b f9 dd e5 39 0d
   ..%...........9.
Thu Aug 16 14:42:54 2007: 000000a0: 2e 82 eb 17 c6 23 b7 96  dc c3 55 ff 7c 51 4e 75
   .....#....U.|QNu
Thu Aug 16 14:42:54 2007: 000000b0: 73 65 72 31 18 0a 53 56  43 3d 30 2e 31 3b 50 12
   ser1..SVC=0.1;P.
Thu Aug 16 14:42:54 2007: 000000c0: 1a d5 3b 35 5e 93 11 c0  c6 2f 5e f5 65 e9 3e 2d
   ..;5^..../^.e.>-
Thu Aug 16 14:42:54 2007: 00000000: 0b 01 00 36 8c 31 6a b4  27 e6 d4 0e 1b 8e 5d 19
   ...6.1j.'.....].
Thu Aug 16 14:42:54 2007: 00000010: 60 1c c2 16 4f 06 03 01  00 04 18 0a 53 56 43 3d
   ...O.......SVC=
Thu Aug 16 14:42:54 2007: 00000020: 30 2e 31 3b 50 12 6c fb  90 ec 48 9b fb d7 ce ca
   0.1;P.l...H.....
Thu Aug 16 14:42:54 2007: 00000030: 3b 64 93 10 fe 09      ;d....
Thu Aug 16 14:42:54 2007: ****Enter processIncomingMessages: response code=11
Thu Aug 16 14:42:54 2007: ****Enter processRadiusResponse: response code=11
Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93
Access-Challenge received from RADIUS server
   10.77.244.196 for mobile 00:40:96:af:3e:93 receiveId = 3
Thu Aug 16 14:42:54 2007: AuthorizationResponse: 0x9c27800
Thu Aug 16 14:42:54 2007:       structureSize.....104
Thu Aug 16 14:42:54 2007:       resultCode.....255
Thu Aug 16 14:42:54 2007:       protocolUsed.....0x00000001
Thu Aug 16 14:42:54 2007:       proxyState.....
   00:40:96:AF:3E:93-03:01
```

```
Thu Aug 16 14:42:54 2007:       Packet contains 3 AVPs (not shown)
Thu Aug 16 14:42:54 2007: AuthenticationRequest: 0xb1ab104
Thu Aug 16 14:42:54 2007:       Callback.................0x85ed228
Thu Aug 16 14:42:54 2007:       protocolType.............0x00140001
Thu Aug 16 14:42:54 2007:       proxyState.......................
   00:40:96:AF:3E:93-03:02
Thu Aug 16 14:42:54 2007:       Packet contains 16 AVPs (not shown)
Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93
Successful transmission of Authentication Packet (id 2) to 10.77.244.196:1812,
proxy state 00:40:96:af:3e:93-00:00
Thu Aug 16 14:42:54 2007: 00000000: 01 02 00 c0 38 b6 b2 20  ff 5b f2 16 64 df 02 61
   ....8....[..d..a
Thu Aug 16 14:42:54 2007: 00000010: cf f5 93 4b 01 07 75 73  65 72 31 1f 13 30 30 2d
   ...K..User1..00-
Thu Aug 16 14:42:54 2007: 00000020: 34 30 2d 39 36 2d 41 46  2d 33 45 2d 39 33 1e 20
   40-96-AF-3E-93..
Thu Aug 16 14:42:54 2007: 00000030: 30 30 2d 30 42 2d 38 35  2d 35 42 2d 46 42 2d 44
   00-0B-85-5B-FB-D
Thu Aug 16 14:42:54 2007: 00000040: 30 3a 4f 66 66 69 63 65  2d 54 53 57 45 42 05 06
   0:Office..
Thu Aug 16 14:42:54 2007: 00000050: 00 00 00 01 04 06 0a 4d  f4 d2 20 05 77 6c 63 1a
   .......M....wlc.
Thu Aug 16 14:42:54 2007: 00000060: 0c 00 00 37 63 01 06 00  00 00 01 06 06 00 00 00
   ...7c...........
Thu Aug 16 14:42:54 2007: 00000070: 02 0c 06 00 00 05 14 3d  06 00 00 00 13 40 06 00
   .......=.....@..
Thu Aug 16 14:42:54 2007: 00000080: 00 00 0d 41 06 00 00 00  06 51 04 32 30 4f 17 01
   ...A.....Q.20O..
Thu Aug 16 14:42:54 2007: 00000090: 01 00 15 11 01 00 08 0f  14 05 65 1b 28 61 c9 75
   ..........e.(a.u
Thu Aug 16 14:42:54 2007: 000000a0: 73 65 72 31 18 0a 53 56  43 3d 30 2e 31 3b 50 12
   ser1..SVC=0.1;P.
Thu Aug 16 14:42:54 2007: 000000b0: 05 ba 6b af fe a4 b0 d1  a2 94 f8 39 80 ca 3c 96
   ..k........9..<.
Thu Aug 16 14:42:54 2007: 00000000: 02 02 00 ce c9 3d 5d c8  6c 07 8e fb 58 84 8d f6
   .....=].l...X...
Thu Aug 16 14:42:54 2007: 00000010: 33 6d 93 21 08 06 ff ff  ff ff 4f 27 02 01 00 25
   3m.!......O'...%
Thu Aug 16 14:42:54 2007: 00000020: 11 01 00 18 e5 e5 31 1e  33 b5 4e 69 90 e7 84 25
   ......1.3.Ni...%
Thu Aug 16 14:42:54 2007: 00000030: 42 a9 20 ac 84 33 9f 87  ca dc c9 b3 75 73 65 72
   B....3......user
Thu Aug 16 14:42:54 2007: 00000040: 31 1a 3b 00 00 00 09 01  35 6c 65 61 70 3a 73 65
   1.;.....5leap:se
Thu Aug 16 14:42:54 2007: 00000050: 73 73 69 6f 6e 2d 6b 65  79 3d 29 80 1d 2c 1c 85
   ssion-key=)..,..
Thu Aug 16 14:42:54 2007: 00000060: db 1c 29 7e 40 8a b8 93  69 2a 55 d2 e5 46 89 8b
   ..)~@...i*U..F..
Thu Aug 16 14:42:54 2007: 00000070: 2c 3b 65 49 3e 44 cf 7e  95 29 47 54 1a 1f 00 00
   ,;eI>D.~.)GT....
Thu Aug 16 14:42:54 2007: 00000080: 00 09 01 19 61 75 74 68  2d 61 6c 67 6f 2d 74 79
   ....auth-algo-ty
Thu Aug 16 14:42:54 2007: 00000090: 70 65 3d 65 61 70 2d 6c  65 61 70 1a 0d 00 00 37
   pe=eap-leap....7
Thu Aug 16 14:42:54 2007: 000000a0: 63 06 07 55 73 65 72 31  19 14 43 41 43 53 3a 30
   c..User1..CACS:0
Thu Aug 16 14:42:54 2007: 000000b0: 2f 39 2f 61 34 64 66 34  64 32 2f 31 50 12 9a 71
   /9/a4df4d2/1P..q
Thu Aug 16 14:42:54 2007: 000000c0: 09 99 7d 74 89 ad af e5  c8 b1 71 94 97 d1
   ..}t......q...
Thu Aug 16 14:42:54 2007: ****Enter processIncomingMessages: response code=2
Thu Aug 16 14:42:54 2007: ****Enter processRadiusResponse: response code=2
Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93
Access-Accept received from RADIUS server
```

```
   10.77.244.196 for mobile 00:40:96:af:3e:93 receiveId = 3
Thu Aug 16 14:42:54 2007: AuthorizationResponse: 0x9c27800
Thu Aug 16 14:42:54 2007:       structureSize............236
Thu Aug 16 14:42:54 2007:       resultCode..............0
Thu Aug 16 14:42:54 2007:       protocolUsed............0x0
0000001
Thu Aug 16 14:42:54 2007:       proxyState..............00:
40:96:AF:3E:93-03:02
Thu Aug 16 14:42:54 2007:  Packet contains 6 AVPs:
Thu Aug 16 14:42:54 2007:  AVP[01] Framed-IP-Address.........0xffffffff (-1)
   (4 bytes)
Thu Aug 16 14:42:54 2007:  AVP[02] EAP-Message...............DATA (37 bytes)
Thu Aug 16 14:42:54 2007:  AVP[03] Cisco / LEAP-Session-Key...DATA (16 bytes)
Thu Aug 16 14:42:54 2007:  AVP[04] Airespace / ACL-Name.......User1 (5 bytes)
Thu Aug 16 14:42:54 2007:  AVP[05] Class.....................CACS:0/9/a4df4d2/1
   (18 bytes)
Thu Aug 16 14:42:54 2007:  AVP[06] Message-Authenticator......DATA (16 bytes)
Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93 Applying new AAA override
   for station 00:40:96:af:3e:93
Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93 Override values
   for station 00:40:96:af:3e:93
               source: 4, valid bits: 0x400
        qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1

dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
                                                    vlanIfName: '',
aclName:User1
Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93
   Inserting new RADIUS override into chain for station 00:40:96:af:3e:93
```

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 nas WLANs RADIUS. Você também pode correlacionar isso com as tentativas aprovadas ou os registros de tentativas com falha do Cisco Secure ACS.

A Cisco recomenda que você teste suas configurações de ACL com um cliente sem fio para garantir que você as tenha configurado corretamente. Se eles não funcionarem corretamente, verifique as ACLs na página da Web da ACL e se as alterações da ACL foram aplicadas à interface do controlador.

Você também pode usar estes comandos show para verificar sua configuração:

- **show acl summary** — Para exibir as ACLs configuradas no controlador, use o comando **show acl summary**.

Aqui está um exemplo:

```
(Cisco Controller) >show acl summary

ACL Name                         Applied
-------------------------------- -------
User1                                 Yes
User2                                 Yes
```

- **show acl detailed** <ACL_Name> — Exibe informações detalhadas sobre as ACLs

configuradas.Aqui está um exemplo:**Observação:** algumas das linhas na saída foram movidas para a segunda linha devido a restrições de espaço.

```
Cisco Controller) >show acl detailed User1

                    Source                          Destination
   Source Port   Dest Port
I  Dir       IP Address/Netmask              IP Address/Netmask
   Prot    Range       Range    DSCP   Action
-- --- ------------------------------ ------------------------------
   ---- ---------- ---------- ----    ------
 1  In      172.16.0.0/255.255.0.0        172.16.1.100/255.255.255.255
   Any  0-65535       0-65535   Any    Permit
 2 Out    172.16.1.100/255.255.255.255      172.16.0.0/255.255.0.0
   Any  0-65535       0-65535   Any    Permit


(Cisco Controller) >show acl detailed User2

                    Source                          Destination
   Source Port   Dest Port
I  Dir       IP Address/Netmask              IP Address/Netmask
   Prot    Range       Range    DSCP Action
-- --- ------------------------------ ------------------------------
   ---- ---------- ---------- ---- ------
1  In      172.16.0.0/255.255.0.0         172.16.1.50/255.255.255.255
   Any   0-65535       0-65535    Any  Permit
2 Out     172.16.1.50/255.255.255.255      172.16.0.0/255.255.0.0
   Any   0-65535       0-65535    Any  Permit
```

- **show client detail** <MAC Address of the client> - Exibe informações detalhadas sobre o cliente Wireless.

Dicas para Troubleshooting

Use estas dicas para solucionar problemas:

- Verifique no controlador se o servidor RADIUS está no estado ativo e não no modo de espera ou desativado.
- No controlador, verifique se o servidor RADIUS está selecionado no menu suspenso da WLAN (SSID).
- Verifique se o servidor RADIUS recebe e valida a solicitação de autenticação do cliente sem fio.
- 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.

Informações Relacionadas

- ACLs em Wireless LAN Controllers: Regras, limitações e exemplos
- Exemplo de configuração de ACLs em Wireless LAN Controller
- Exemplo de Configuração de Filtros MAC com Controladores Wireless LAN (WLCs)
- Guia de configuração do Controlador de LAN sem fio da Cisco, versão 5.2
- Suporte Técnico e Documentação - Cisco Systems