# Autenticação externa da Web usando um servidor RADIUS

## Contents



# Introduction

Este documento explica como executar a autenticação de web externa usando um servidor RADIUS externo.

# Prerequisites

## Requirements

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

- Conhecimento básico da configuração de Pontos de Acesso Lightweight (LAPs) e Cisco

WLCs
- Conhecimento de como instalar e configurar um servidor Web externo
- Conhecimento de como configurar o Cisco Secure ACS

## Componentes Utilizados

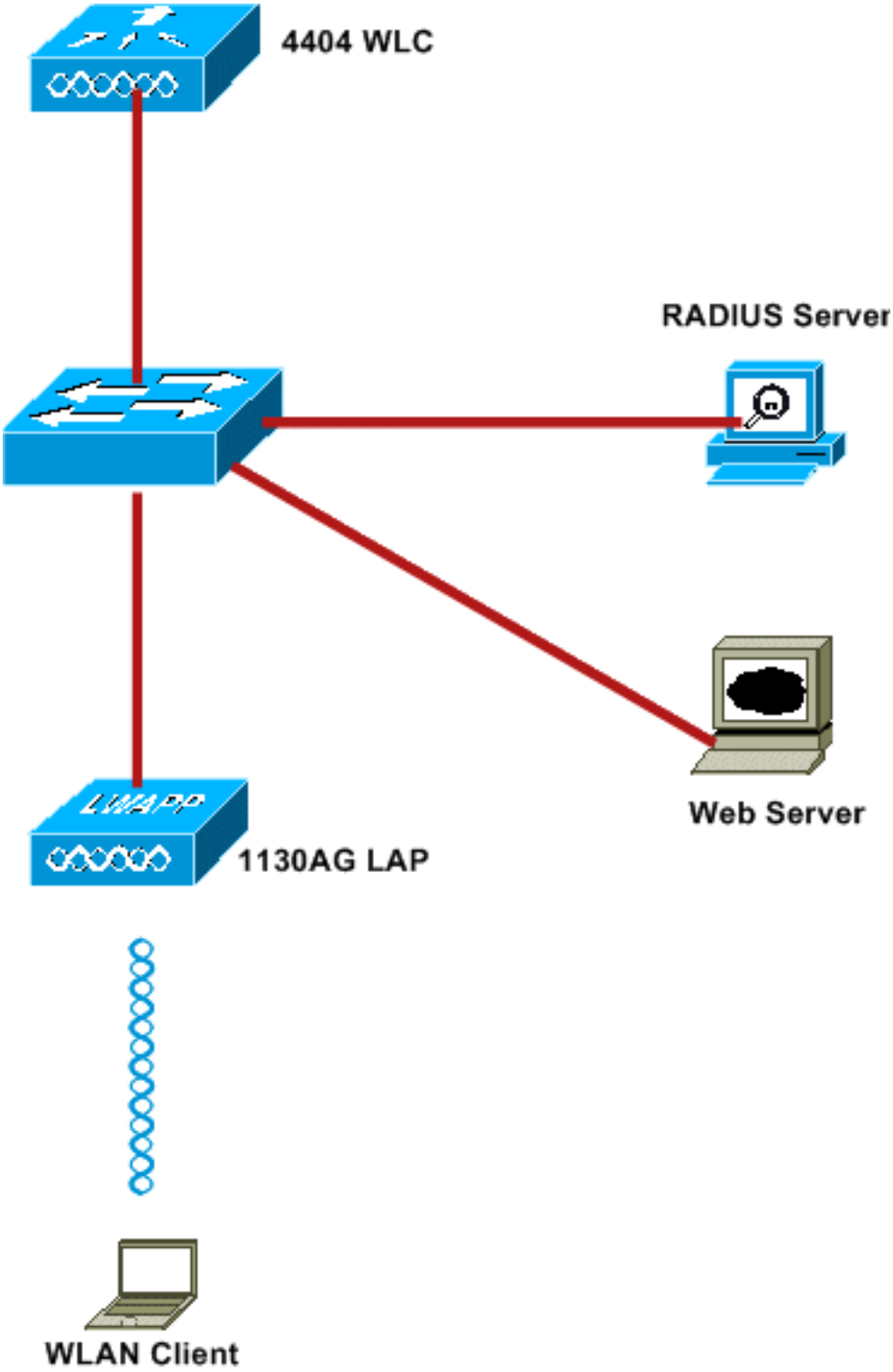
As informações neste documento são baseadas nestas versões de software e hardware:

- Controladora de LAN sem fio com firmware versão 5.0.148.0
- LAP Cisco 1232 Series
- Adaptador de cliente sem fio 3.6.0.61 Cisco 802.11a/b/g
- Servidor Web externo que hospeda a página de logon da autenticação da Web
- Versão do Cisco Secure ACS que executa o firmware versão 4.1.1.24

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.

## Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:




Estes são os endereços IP usados neste documento:

- A WLC usa o endereço IP 10.77.244.206
- O LAP está registrado na WLC com o endereço IP 10.77.244.199
- O Servidor Web usa o endereço IP 10.77.244.210
- O servidor Cisco ACS usa o endereço IP 10.77.244.196
- O cliente recebe um endereço IP da interface de gerenciamento que é mapeado para a WLAN - 10.77.244.208

## Conventions

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

# Autenticação externa da Web

A Autenticação da Web é um mecanismo de autenticação da Camada 3 usado para autenticar usuários convidados para acesso à Internet. Os usuários autenticados usando esse processo não poderão acessar a Internet até que concluam com êxito o processo de autenticação. Para obter informações completas sobre o processo de autenticação externa da Web, leia a seção Processo de Autenticação Externa da Web do documento Exemplo de Configuração de Autenticação Externa da Web com Controladoras Wireless LAN.

Neste documento, examinamos um exemplo de configuração, no qual a autenticação da Web externa é executada usando um servidor RADIUS externo.

# Configurar o WLC

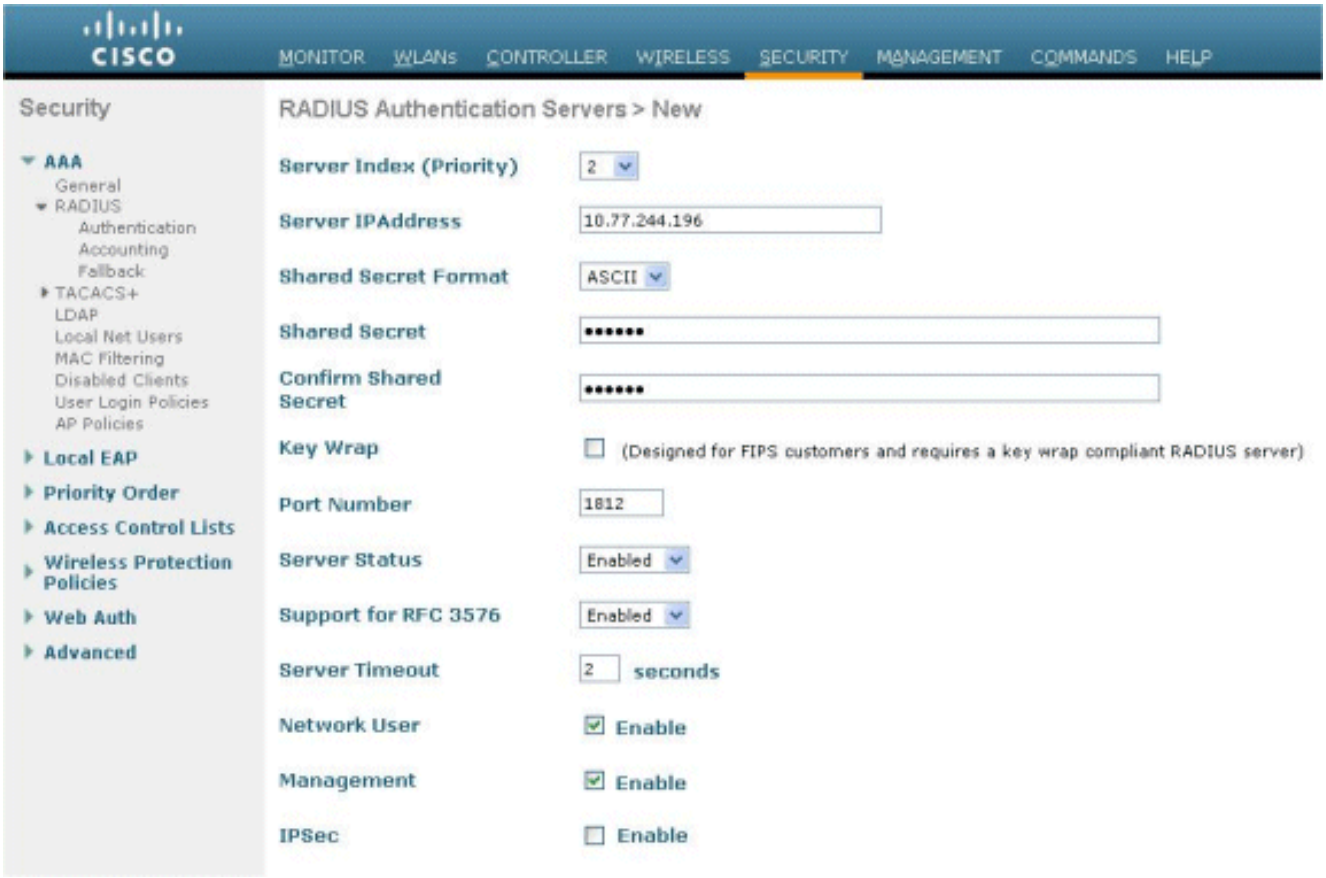
Neste documento, supomos que a WLC já está configurada e tem um LAP registrado para a WLC. Este documento supõe ainda que a WLC esteja configurada para operação básica e que os LAPs estejam registrados na WLC. Se você for um novo usuário que está tentando configurar o WLC para operação básica com LAPs, consulte Registro do LAP (Lightweight AP) em um WLC (Wireless LAN Controller). Para visualizar os LAPs que estão registrados na WLC, navegue para **Wireless > All AP**.

Depois que a WLC estiver configurada para operação básica e tiver um ou mais LAPs registrados, você poderá configurar a WLC para autenticação externa da Web usando um servidor Web externo. Em nosso exemplo, estamos usando uma versão 4.1.1.24 do Cisco Secure ACS como o servidor RADIUS. Primeiro, configuraremos a WLC para esse servidor RADIUS e depois procuraremos a configuração necessária no Cisco Secure ACS para essa configuração.

## Configurar a WLC para o Cisco Secure ACS

Execute estes passos para adicionar o servidor RADIUS na WLC:

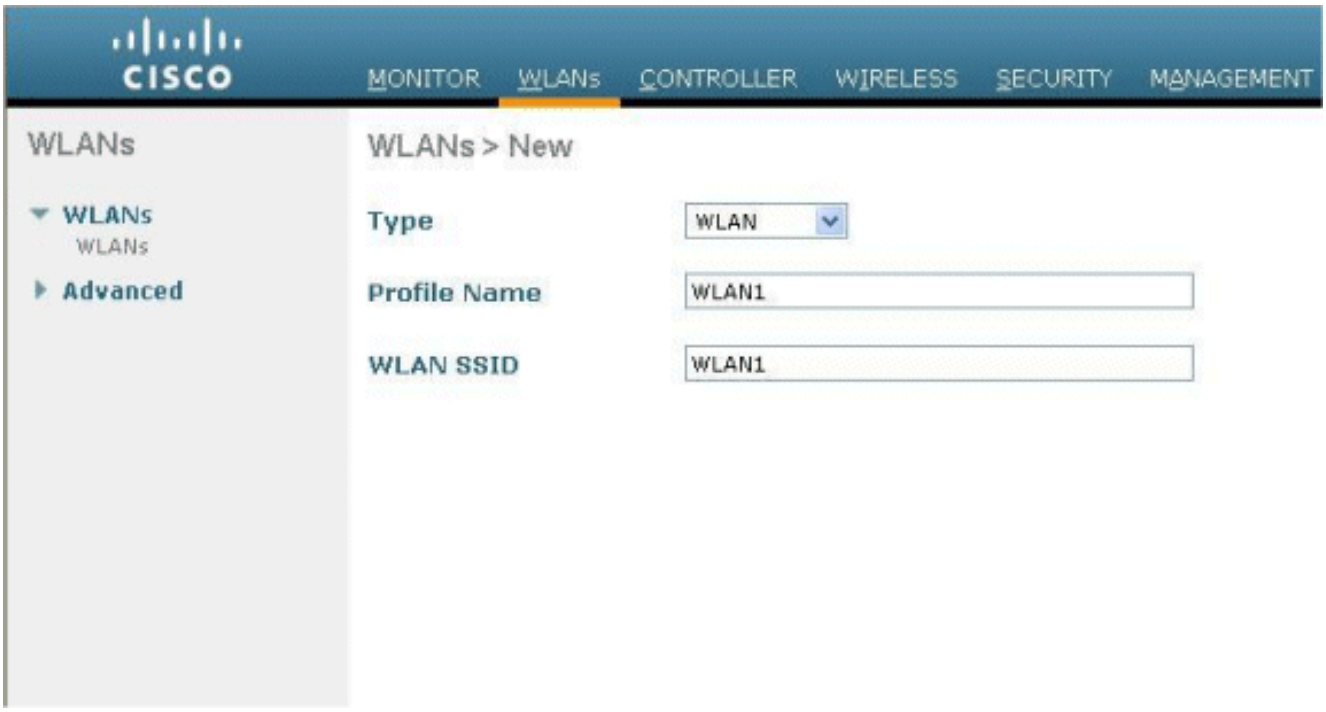
1. Na GUI da WLC, clique no menu **SECURITY**.
2. No menu **AAA**, navegue para o submenu **Radius > Authentication**.
3. Clique em **New** e insira o endereço IP do servidor RADIUS. Neste exemplo, o endereço IP do servidor é *10.77.244.196*.
4. Insira o segredo compartilhado na WLC. O segredo compartilhado deve ser configurado da mesma forma no WLC.
5. Escolha **ASCII** ou **Hex** para o formato de segredo compartilhado. O mesmo formato precisa ser escolhido no WLC.
6. **1812** é o Número da Porta usado para autenticação RADIUS.
7. Verifique se a opção Status do servidor está definida como **Enabled**.
8. Marque a caixa Network User **Enable** para autenticar os usuários da rede.
9. Clique em
   Apply.



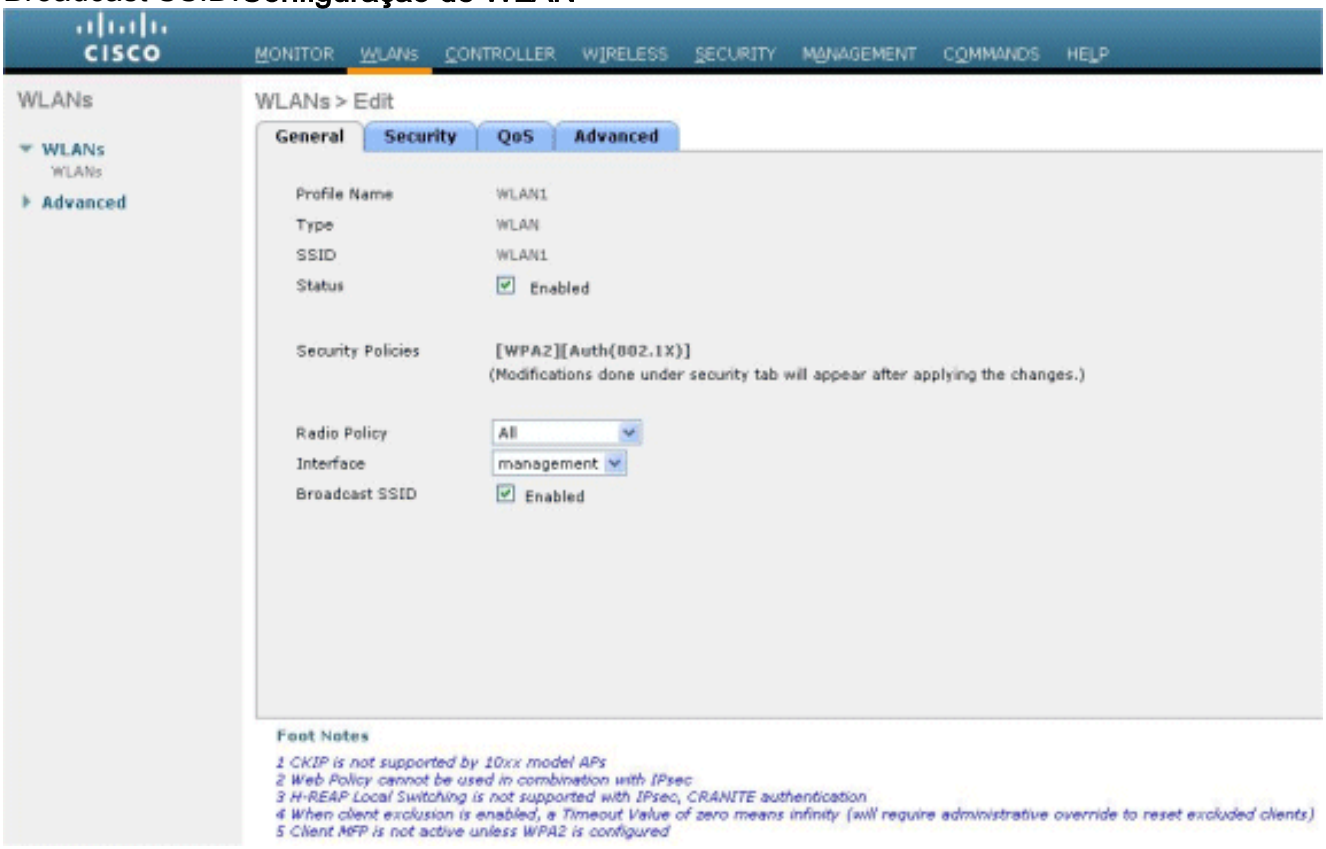

## Configurar a WLAN na WLC para a autenticação da Web

A próxima etapa é configurar a WLAN para a autenticação da Web na WLC. Execute estes passos para configurar a WLAN no WLC:

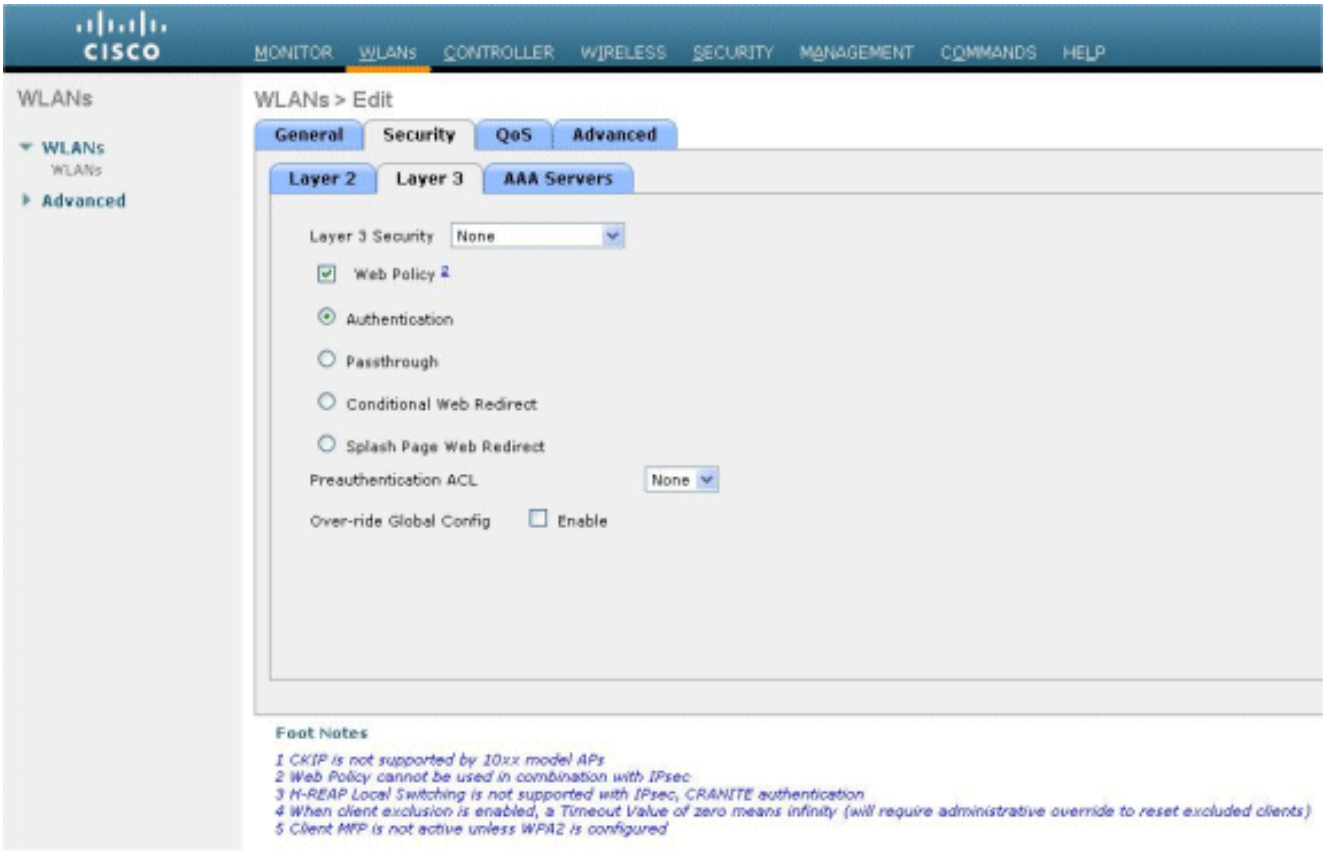
1. Clique no menu **WLANs** na GUI da controladora e escolha **New**.
2. Escolha **WLAN** para Tipo.
3. Insira um Nome de perfil e um SSID de WLAN de sua escolha e clique em **Aplicar**.**Observação:** o SSID da WLAN diferencia maiúsculas de minúsculas.



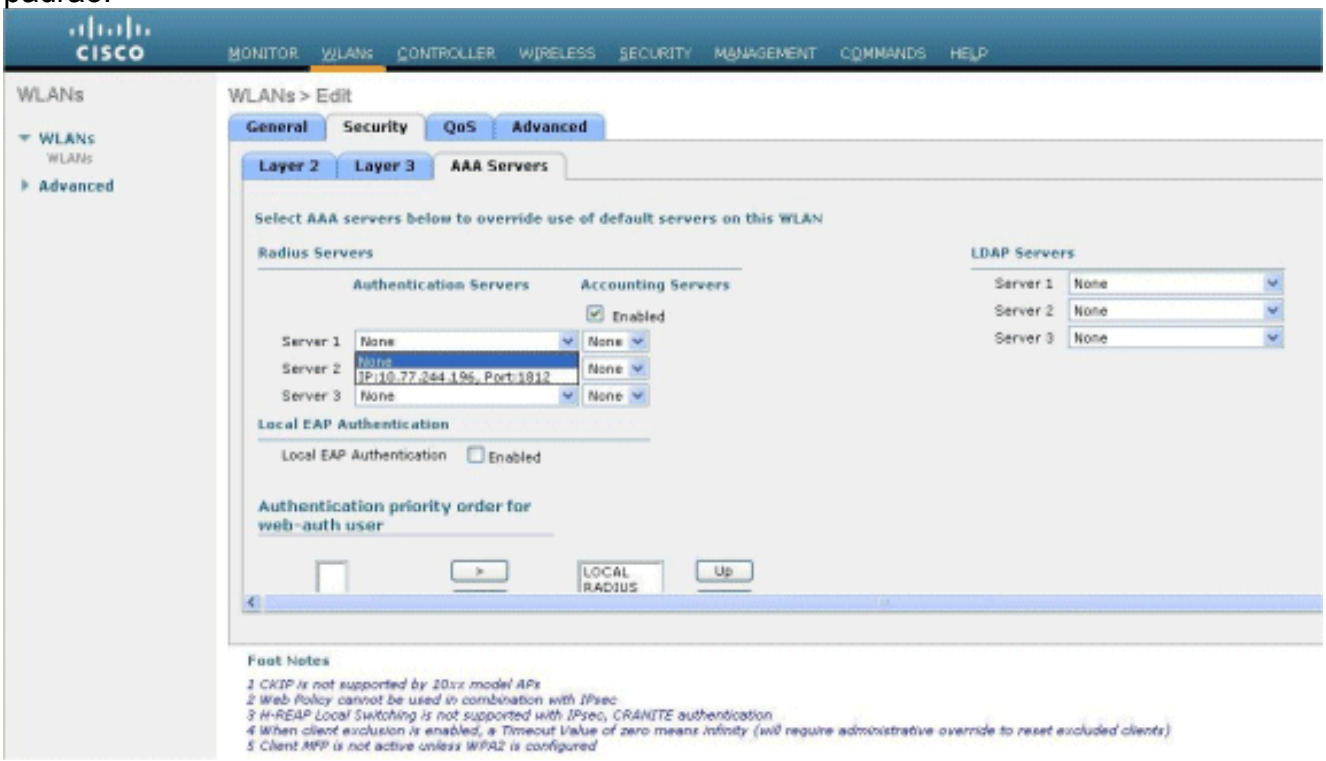
4. Na guia **General**, certifique-se de que a opção **Enabled** esteja marcada para Status e Broadcast SSID.**Configuração de WLAN**




5. Escolha uma interface para a WLAN. Normalmente, uma interface configurada em uma VLAN exclusiva é mapeada para a WLAN de modo que o cliente receba um endereço IP nessa VLAN. Neste exemplo, usamos o *gerenciamento* para a Interface.
6. Escolha a guia **Segurança**.
7. No menu **Layer 2**, escolha **None** para Layer 2 Security.
8. No menu **Layer 3**, escolha **None** para Layer 3 Security. Marque a caixa de seleção **Web Policy** e escolha **Authentication**.




9. No menu **AAA servers**, para Authentication Server, escolha o servidor RADIUS que foi configurado nesta WLC. Outros Menus devem permanecer com os valores padrão.

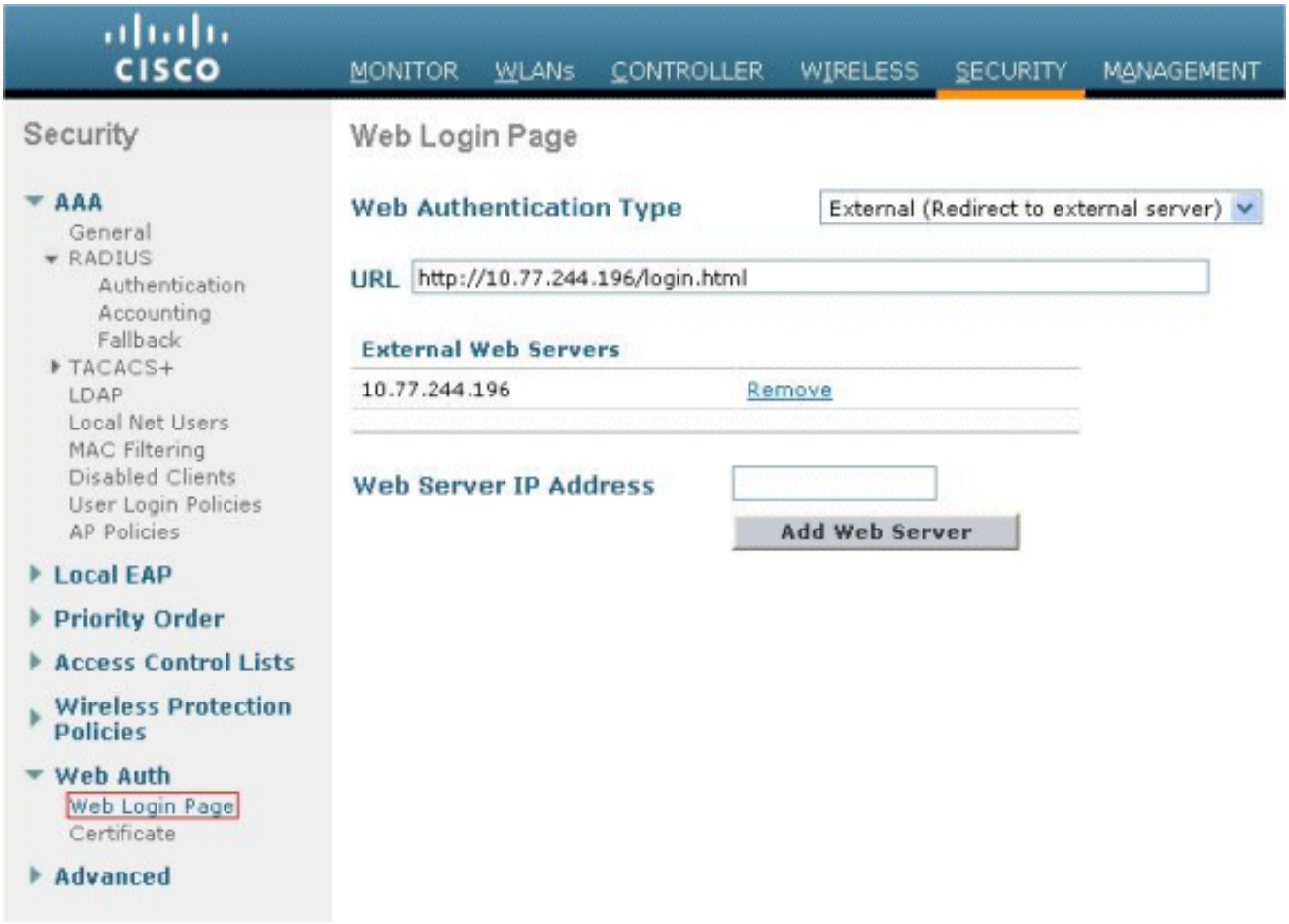



## Configurar as informações do servidor Web no WLC

O servidor Web que hospeda a página de autenticação da Web deve ser configurado no WLC. Execute estas etapas para configurar o servidor Web:

1. Clique na guia Security. Vá para **Web Auth > Web Login Page**.

2. Defina o Tipo de autenticação da Web como **Externo**.
3. No campo Endereço IP do servidor Web, insira o endereço IP do servidor que hospeda a página de autenticação da Web e clique em **Adicionar servidor Web**. Neste exemplo, o endereço IP é *10.77.244.196*, que aparece em Servidores Web Externos.
4. Insira o URL da página de autenticação da Web (neste exemplo, *http://10.77.244.196/login.html*) no campo URL.



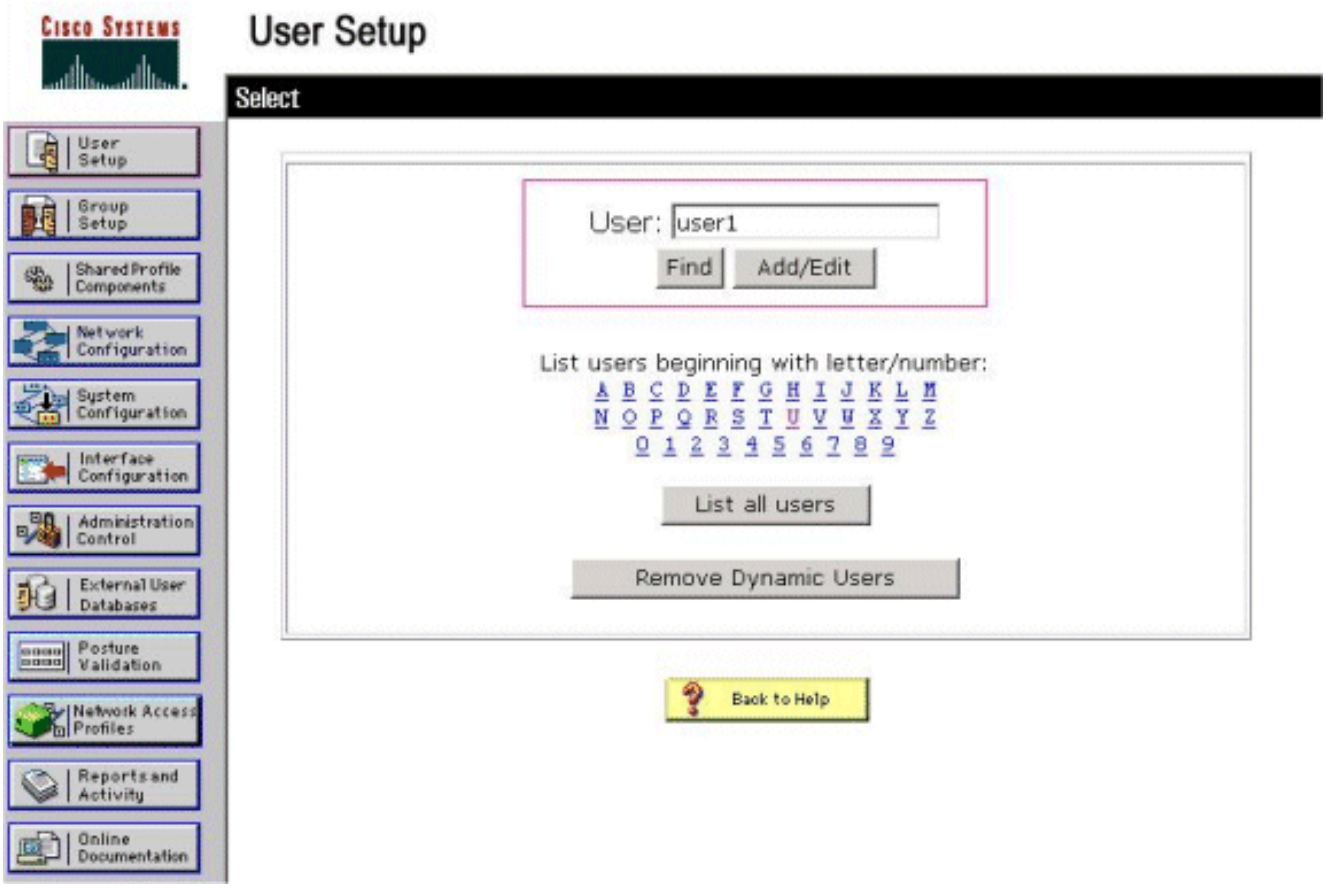

# Configurar o Cisco Secure ACS

Neste documento, supomos que o Cisco Secure ACS Server já esteja instalado e em execução em uma máquina. Para obter mais informações sobre como configurar o Cisco Secure ACS, consulte o Guia de Configuração do Cisco Secure ACS 4.2.

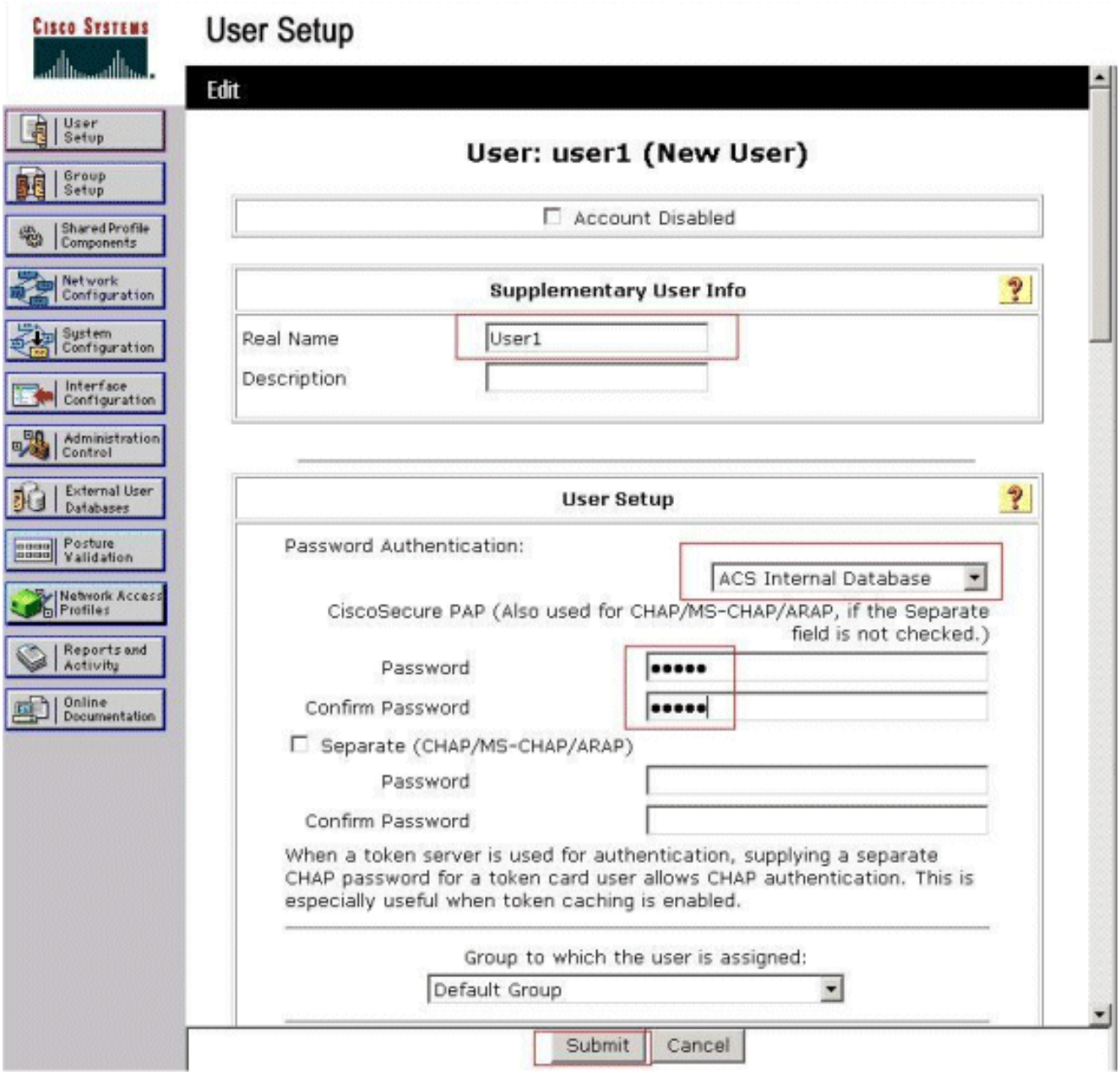
## Configure as informações do usuário no Cisco Secure ACS

Execute estas etapas para configurar usuários no Cisco Secure ACS:

1. Escolha **User Setup** na GUI do Cisco Secure ACS, insira um nome de usuário e clique em **Add/Edit**. Neste exemplo, o usuário é *user1*.




2. Por padrão, o PAP é usado para autenticar clientes. A senha do usuário é inserida em **User Setup > Password Authentication > Cisco Secure PAP**. Certifique-se de escolher **Banco de Dados Interno do ACS** para Autenticação de
Senha.

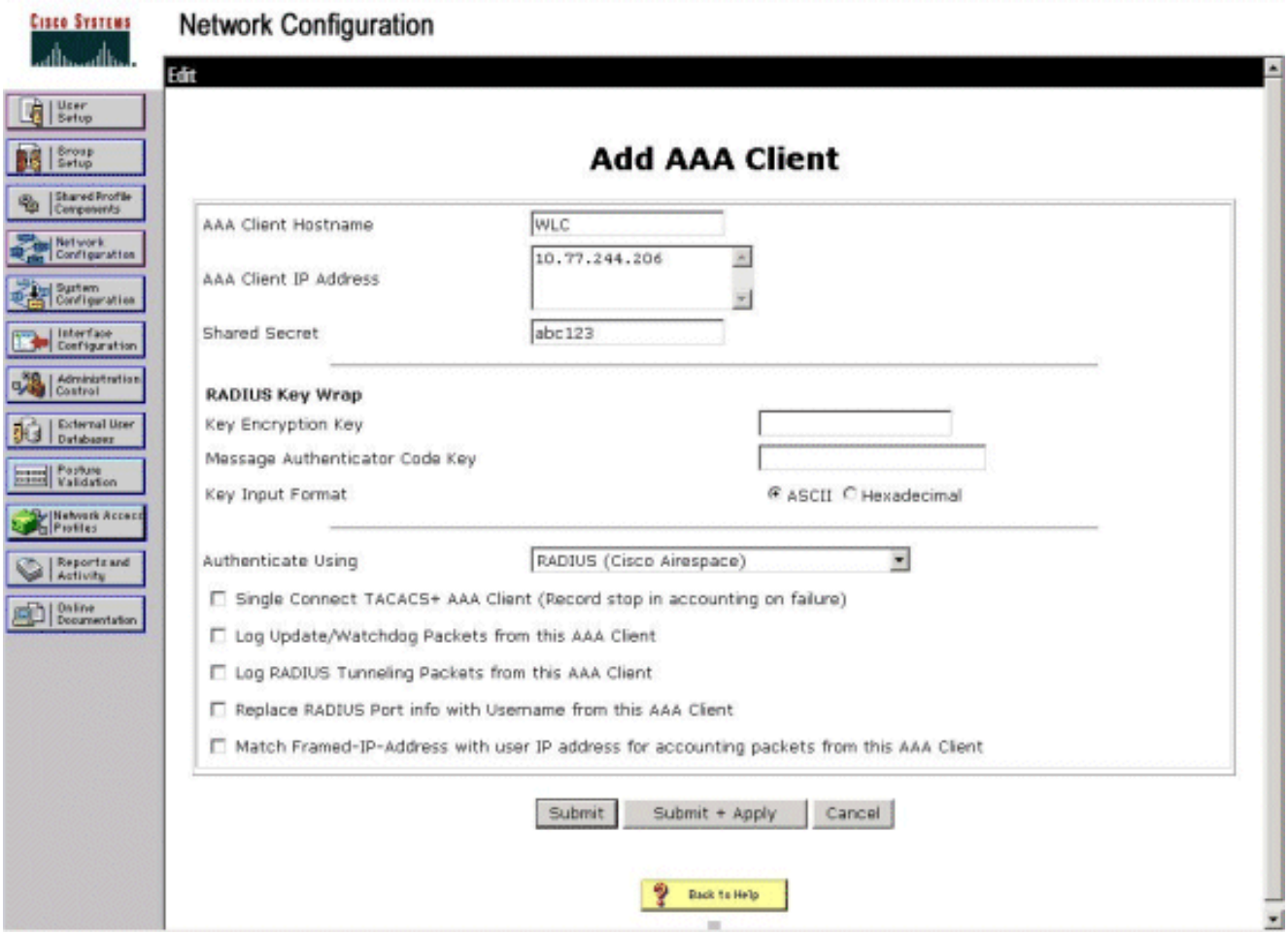



3. O usuário precisa ser atribuído a um grupo ao qual ele pertence. Escolha o **Grupo padrão**.
4. Clique em Submit.

## Configurar as informações de WLC no Cisco Secure ACS

Execute estas etapas para configurar as informações de WLC no Cisco Secure ACS:

1. Na GUI do ACS, clique na guia **Network Configuration** e clique em **Add Entry**.
2. A tela Add AAA client (Adicionar cliente AAA) é exibida.
3. Digite o nome do cliente. Neste exemplo, usamos *WLC*.
4. Digite o endereço IP do cliente. O endereço IP da WLC é *10.77.244.206*.
5. Insira a chave Shared Secret e o formato da chave. Isso deve corresponder à entrada feita no menu **Security** do WLC.
6. Escolha **ASCII** para o formato de entrada de chave, que deve ser o mesmo na WLC.
7. Escolha **RADIUS (Cisco Airespace)** para Authenticate Using para definir o protocolo usado entre o WLC e o servidor RADIUS.
8. Clique em **Enviar e aplicar.**

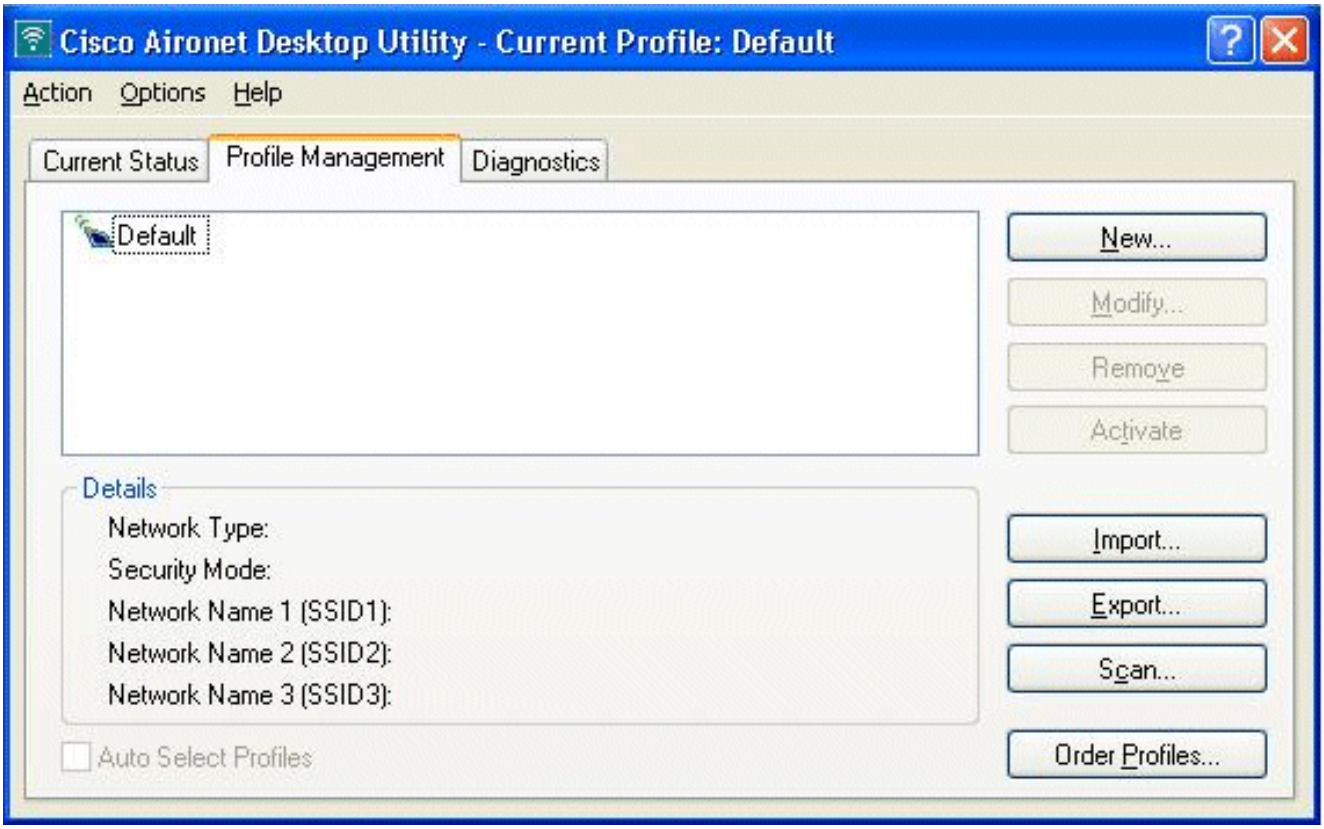



# Processo de autenticação do cliente

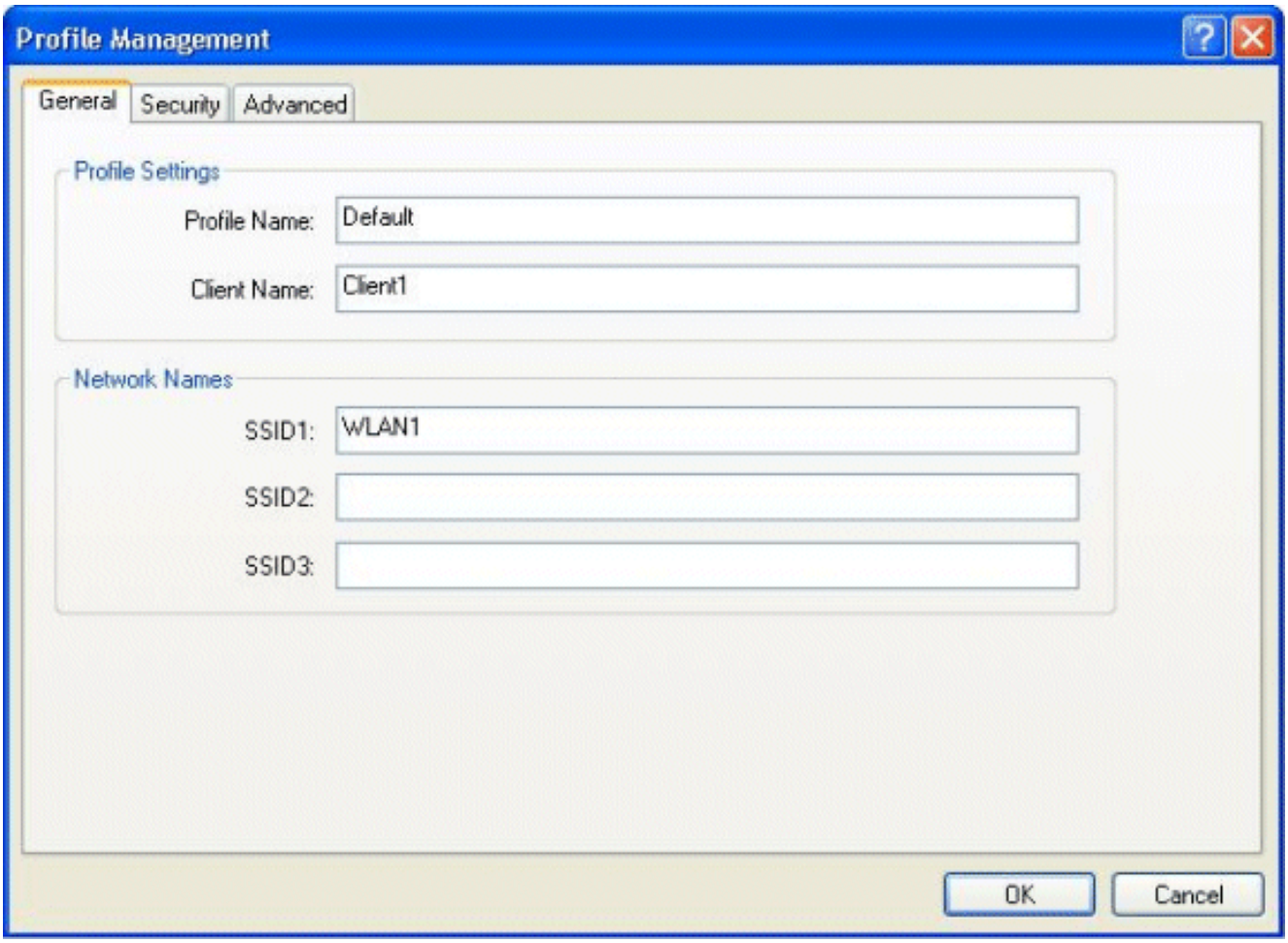
## Configuração do Cliente

Neste exemplo, usamos o Cisco Aironet Desktop Utility para executar a autenticação da Web. Execute estas etapas para configurar o Aironet Desktop Utility.

1. Abra o Aironet Desktop Utility em **Start > Cisco Aironet > Aironet Desktop Utility**.
2. Clique na guia **Gerenciamento de perfil**.

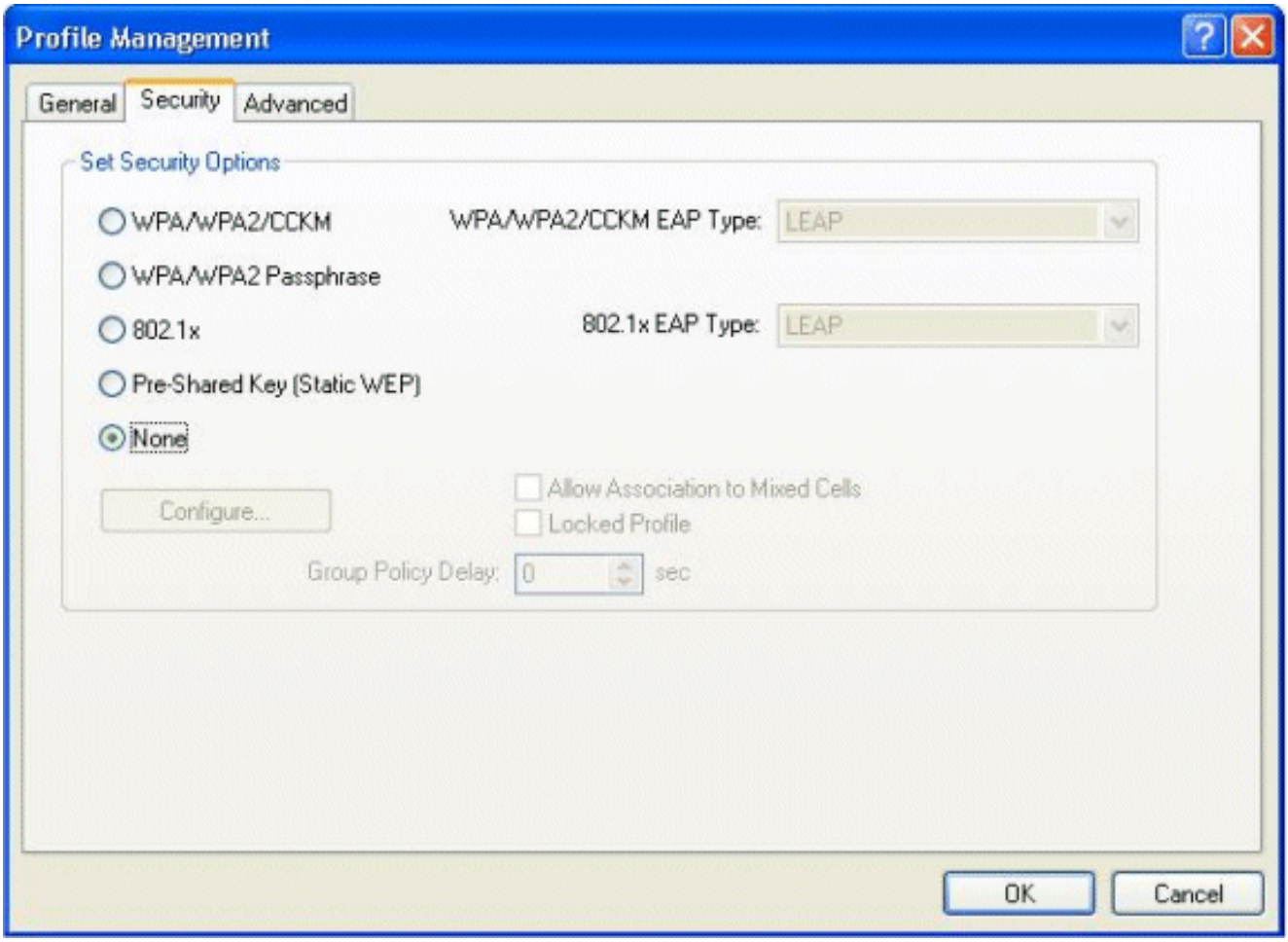



3. Escolha o perfil **Default** e clique em **Modify**.Clique na guia **Geral.**Configure um nome de perfil. Neste exemplo, *Default* é usado.Configure o SSID em Nomes de rede. Neste exemplo, *WLAN1* é
usado.

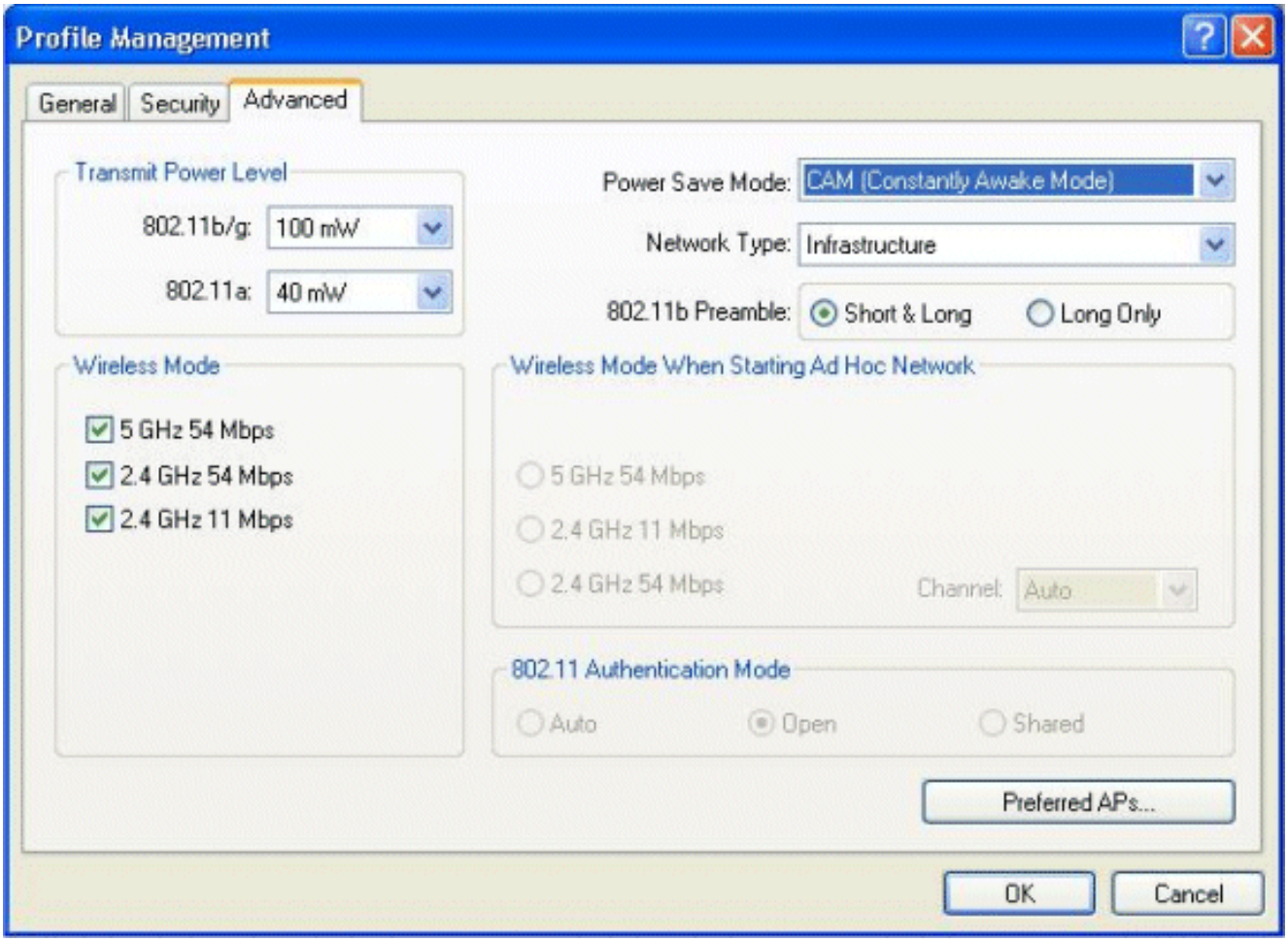



**Observação:** o SSID diferencia maiúsculas de minúsculas e deve corresponder à WLAN configurada na WLC.Clique na guia Security.Escolha **None** como Security para a

autenticação da
Web.




Clique na guia Advanced.No menu **Wireless Mode**, escolha a frequência com que o cliente sem fio se comunica com o LAP.Em **Transmit Power Level**, escolha a potência configurada na WLC.Deixe o valor padrão para Modo de economia de energia.Escolha **Infrastructure** como o tipo de rede.Defina o preâmbulo 802.11b como **curto e longo** para obter uma melhor compatibilidade.Click
**OK**.



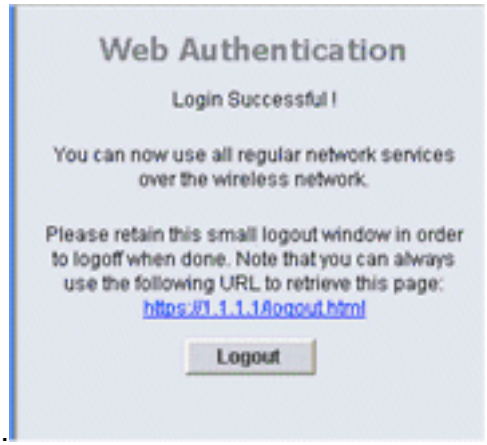

4. Depois que o Perfil é configurado no software cliente, o cliente é associado com êxito e recebe um endereço IP do pool de VLANs configurado para a interface de gerenciamento.

## Processo de Logon do Cliente

Esta seção explica como ocorre o login do cliente.

1. Abra uma janela do navegador e digite qualquer URL ou endereço IP. Com isso, a página de autenticação da Web é levada ao cliente. Se a controladora estiver executando qualquer versão anterior à 3.0, o usuário deverá digitar *https://1.1.1.1/login.html* para abrir a página de autenticação da Web. Uma janela de alerta de segurança é exibida.
2. Clique **Yes para continuar.**
3. Quando a janela Login for exibida, insira o nome de usuário e a senha configurados no servidor RADIUS. Se o login for bem-sucedido, você verá duas janelas do navegador. A janela maior indica que o login foi bem-sucedido e você pode usar essa janela para navegar na Internet. Use a janela menor para encerrar a sessão quando seu uso da rede guest

estiver concluído.

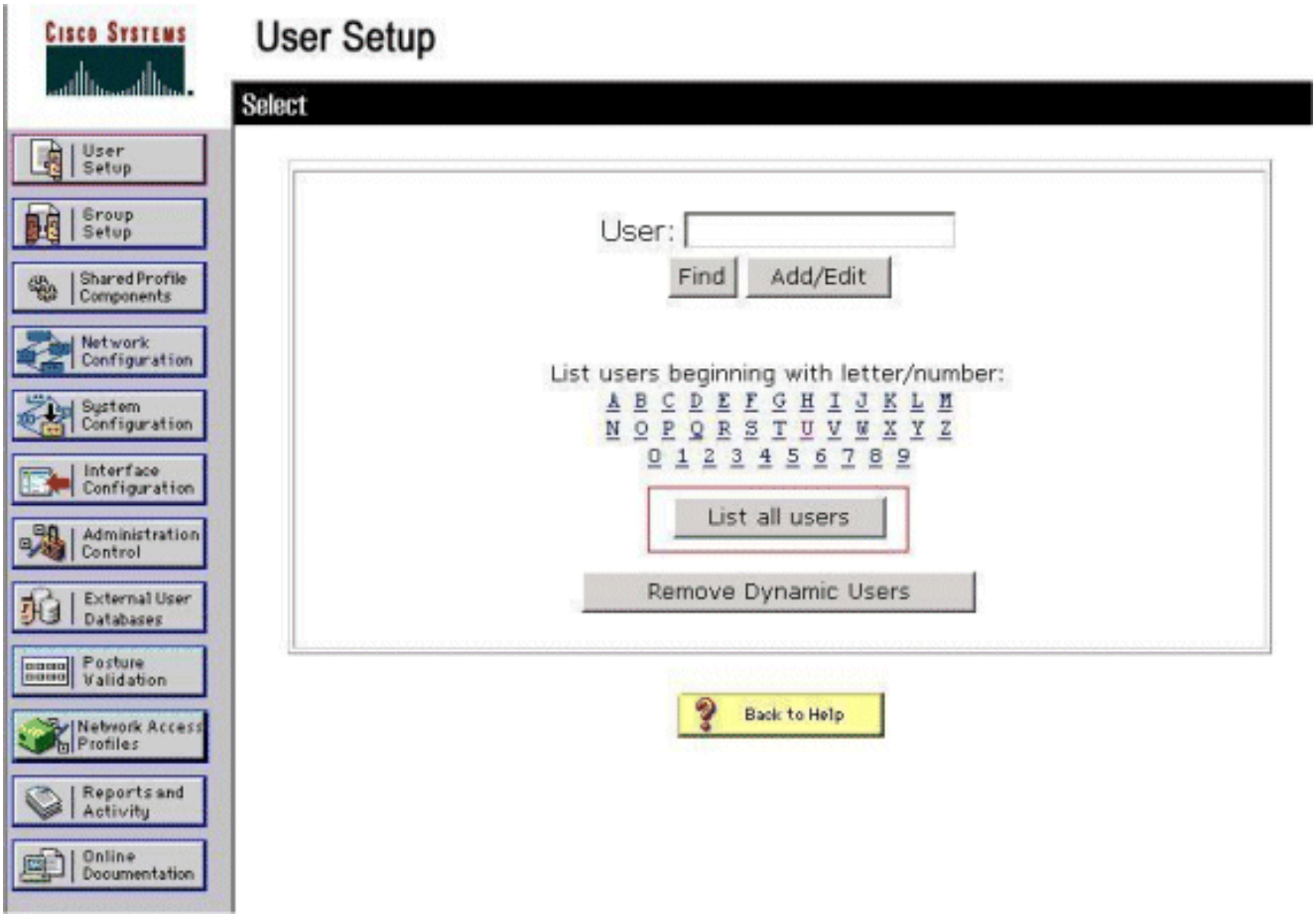



# Verificar

Para uma autenticação da Web bem-sucedida, você precisa verificar se os dispositivos estão configurados de maneira apropriada. Esta seção explica como verificar os dispositivos usados no processo.

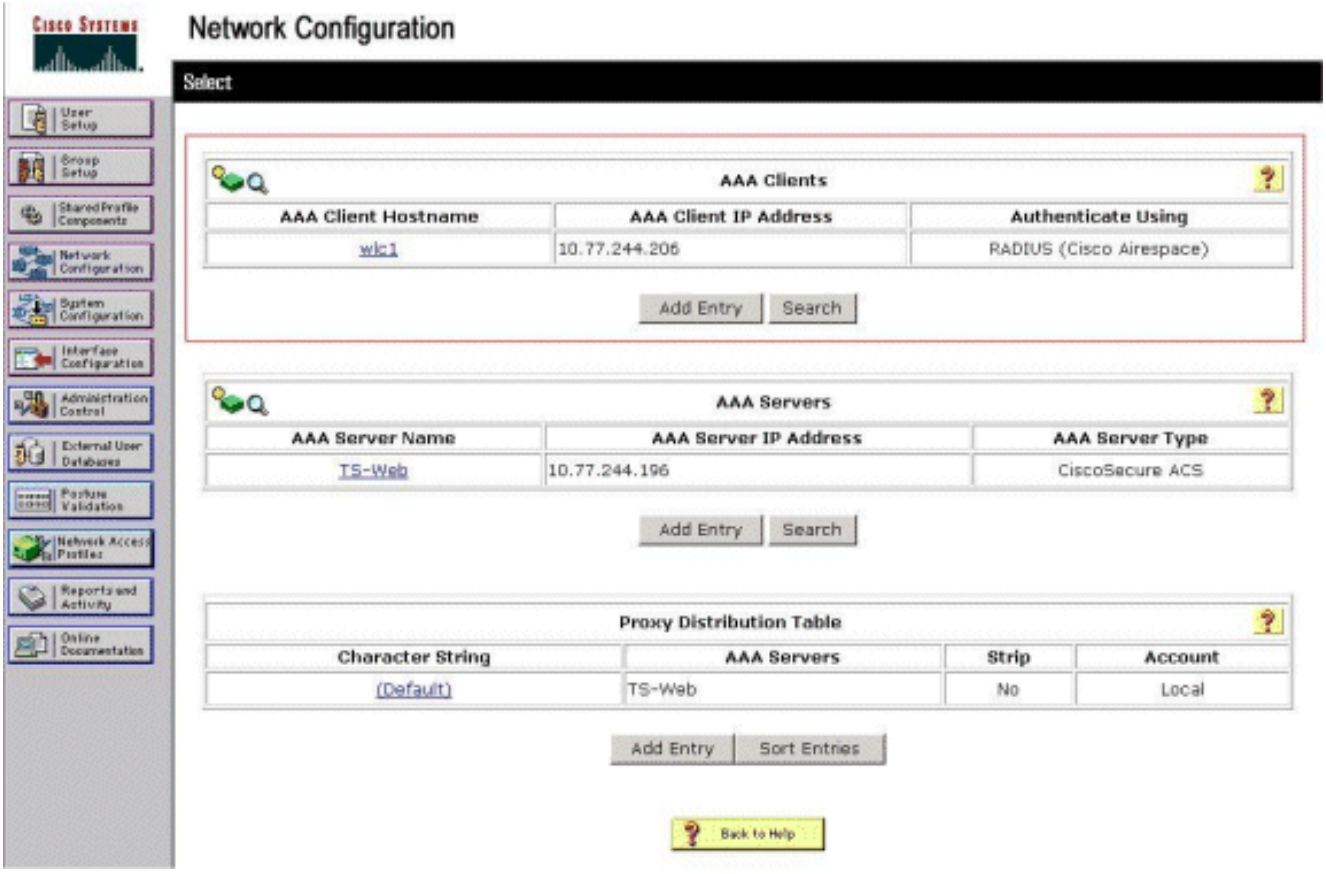
## Verificar o ACS

1. Clique em **User Setup** e, em seguida, clique em **List All Users** na GUI do ACS.




Certifique-se de que o Status do usuário seja *Enabled* e que o grupo Default esteja mapeado para o
usuário.


2. Clique na guia **Network Configuration** e examine a tabela **AAA Clients** para verificar se a WLC está configurada como um cliente AAA.

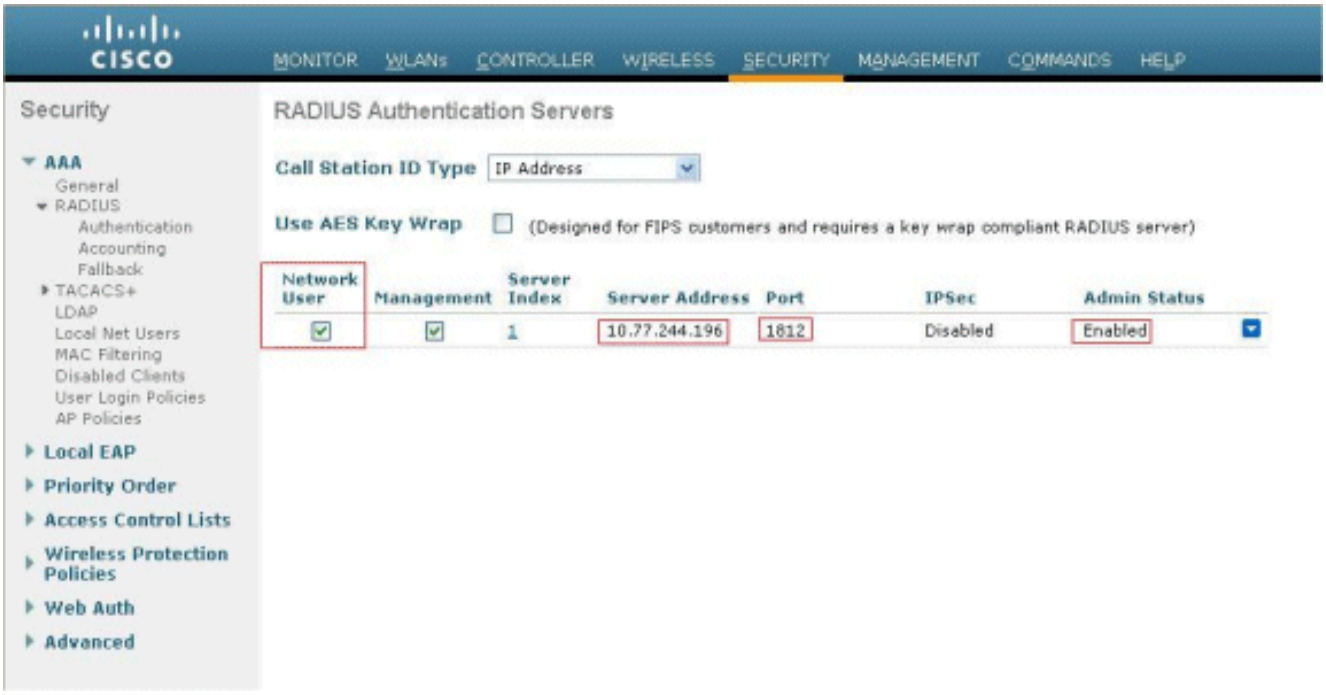



## Verificar a WLC

1. Clique no menu **WLANs** na GUI da WLC.Verifique se a WLAN usada para autenticação da Web está listada na página.Verifique se o status administrativo da WLAN está *habilitado*.Certifique-se de que a Política de Segurança para a WLAN mostra *Web-Auth*.


2. Clique no menu **SECURITY** na GUI da WLC.Verifique se o Cisco Secure ACS

(10.77.244.196) está listado na página.Certifique-se de que a caixa Network User esteja marcada.Certifique-se de que a porta seja *1812* e que o status de administrador seja *Enabled*.




# Troubleshoot

Há muitas razões pelas quais uma autenticação da Web não é bem-sucedida. O documento Troubleshooting de Autenticação da Web em um Wireless LAN Controller (WLC) explica claramente esses motivos em detalhes.

## Comandos para Troubleshooting

**Observação:** consulte Informações Importantes sobre Comandos de Depuração antes de usar esses comandos debug.

Faça Telnet no WLC e emita estes comandos para solucionar problemas de autenticação:

- **debug aaa all enable**

```
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Successful transmission of Authentic
ation Packet (id 1) to 10.77.244.196:1812, proxy state 00:40:96:ac:dd:05-00:01
Fri Sep 24 13:59:52 2010: 00000000: 01 01 00 73 00 00 00 00  00 00 00 00 00 00 0
0 00  ...s............
Fri Sep 24 13:59:52 2010: 00000010: 00 00 00 00 01 07 75 73  65 72 31 02 12 93 c
3 66  ......user1....f
Fri Sep 24 13:59:52 2010: 00000030: 75 73 65 72 31
      user1
Fri Sep 24 13:59:52 2010: ****Enter processIncomingMessages: response code=2
Fri Sep 24 13:59:52 2010: ****Enter processRadiusResponse: response code=2
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Access-Accept received from RADIUS s
erver 10.77.244.196 for mobile 00:40:96:ac:dd:05 receiveId = 0
Fri Sep 24 13:59:52 2010: AuthorizationResponse: 0x12238db0
Fri Sep 24 13:59:52 2010:       structureSize.............................89
Fri Sep 24 13:59:52 2010:       resultCode................................0
Fri Sep 24 13:59:52 2010:       protocolUsed..............................0x0
0000001
Fri Sep 24 13:59:52 2010:       proxyState................................00:
```

```
40:96:AC:DD:05-00:00
Fri Sep 24 13:59:52 2010:       Packet contains 2 AVPs:
Fri Sep 24 13:59:52 2010:           AVP[01] Framed-IP-Address..................
.....0xffffffff (-1) (4 bytes)
Fri Sep 24 13:59:52 2010:           AVP[02] Class..............................
.....CACS:0/5183/a4df4ce/user1 (25 bytes)
Fri Sep 24 13:59:52 2010: Authentication failed for user1, Service Type: 0
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Applying new AAA override for statio
n 00:40:96:ac:dd:05
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Override values for station 00:40:96
:ac:dd:05
                source: 48, valid bits: 0x1
        qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1

dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
                                                              vlanIfName: '',
aclName:
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Unable to apply override policy for
station 00:40:96:ac:dd:05 - VapAllowRadiusOverride is FALSE
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Sending Accounting request (0) for s
tation 00:40:96:ac:dd:05
Fri Sep 24 13:59:52 2010: AccountingMessage Accounting Start: 0x1500501c
Fri Sep 24 13:59:52 2010:       Packet contains 12 AVPs:
Fri Sep 24 13:59:52 2010:           AVP[01] User-Name..........................
.....user1 (5 bytes)
Fri Sep 24 13:59:52 2010:           AVP[02] Nas-Port...........................
.....0x00000002 (2) (4 bytes)
Fri Sep 24 13:59:52 2010:           AVP[03] Nas-Ip-Address.....................
.....0x0a4df4ce (172881102) (4 bytes)
Fri Sep 24 13:59:52 2010:           AVP[04] Framed-IP-Address..................
.....0x0a4df4c7 (172881095) (4 bytes)
```

- **debug aaa detail enable**

As tentativas de autenticação com falha são listadas no menu localizado em **Reports and Activity > Failed Attempts**.

# Informações Relacionadas

- Exemplo de configuração de autenticação da Web para o controlador da LAN sem fio
- Solução de problemas de autenticação da Web em controladores de LAN sem fio (WLC)
- Exemplo de configuração de autenticação de web externa com Wireless LAN Controllers
- Exemplo de configuração da autenticação da Web usando LDAP em controladores de LAN sem fio (WLCs)
- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.