Autenticação do web externa usando um servidor Radius

Índice

Introdução

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

Pré-requisitos

Requisitos

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

- Conhecimento básico da configuração do Lightweight Access Points (regaços) e do Cisco

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

Componentes Utilizados

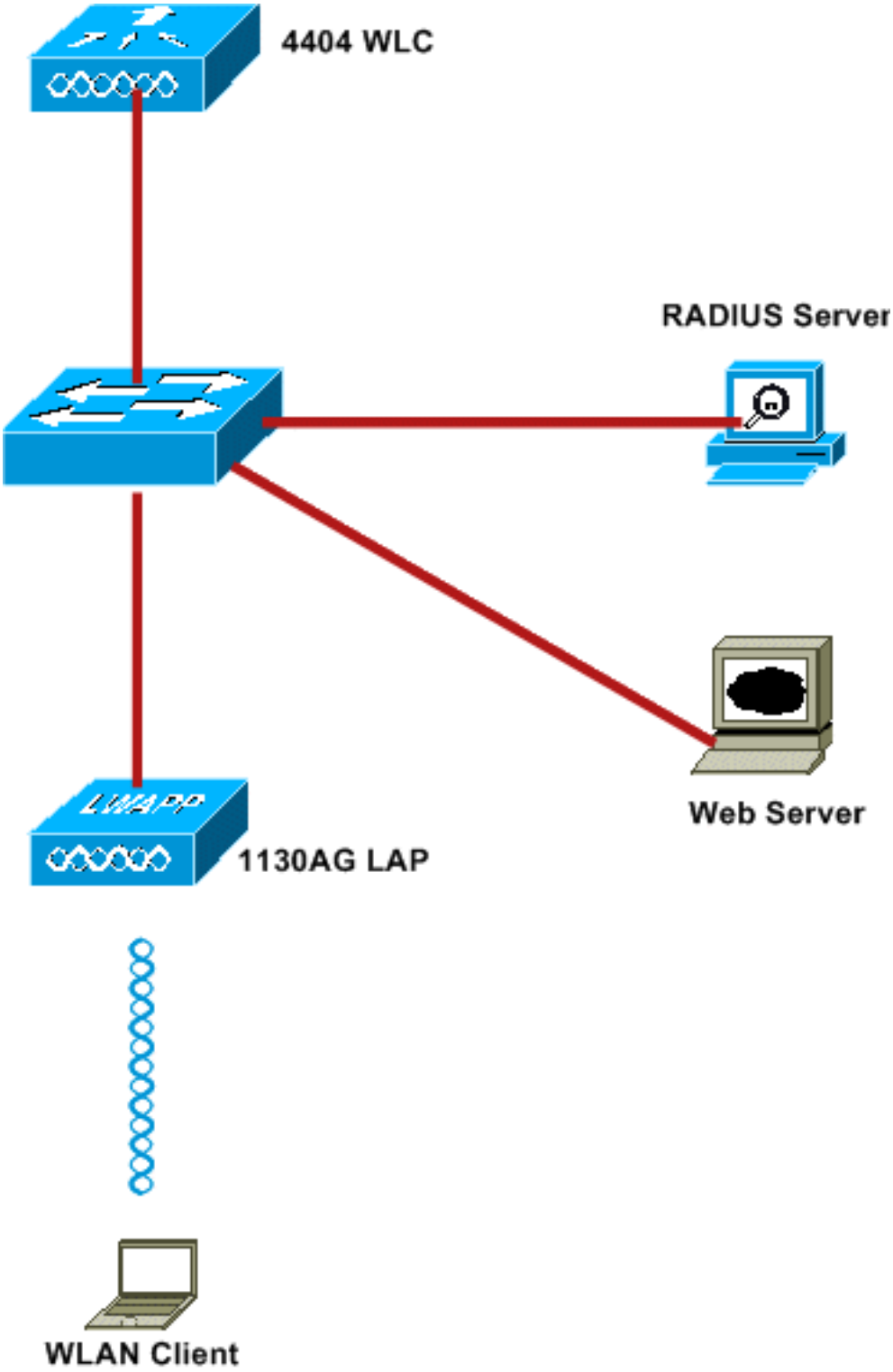
As informações neste documento são baseadas nestas versões de software e hardware:

- Controlador do Wireless LAN que executa a versão de firmware 5.0.148.0
- REGAÇO do Cisco 1232 Series
- Adaptador de cliente Wireless 3.6.0.61 de Cisco 802.11a/b/g
- Servidor de Web externo que hospeda a página de login da autenticação da Web
- Versão do Cisco Secure ACS que executa a versão de firmware 4.1.1.24

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos usados neste original começaram com uma configuração cancelada (do padrão). Se sua rede está viva, certifique-se de que você compreende o impacto potencial do comando any.

Diagrama da rede

Este documento utiliza a seguinte configuração de rede:



Estes são os endereços IP usados neste documento:

- WLC usa o IP address 10.77.244.206
- O REGAÇO é registrado a WLC com IP address 10.77.244.199
- O servidor de Web usa o IP address 10.77.244.210
- O servidor ACS de Cisco usa o IP address 10.77.244.196
- O cliente recebe um IP address da interface de gerenciamento que é traçada ao WLAN - 10.77.244.208

Convenções

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

Autenticação do web externa

A autenticação da Web é um mecanismo da autenticação da camada 3 usado para autenticar usuários convidado para o acesso à internet. Os usuários autenticados usando este processo não poderão alcançar o Internet até eles terminam com sucesso o processo de autenticação. Para obter informações completas sobre do processo de autenticação do web externa, leia o processo de autenticação do web externa da seção da autenticação do web externa do original com exemplo de configuração dos controladores do Wireless LAN.

Neste original, nós olhamos um exemplo de configuração, em que a autenticação do web externa é executada usando um servidor de raio externo.

Configurar o WLC

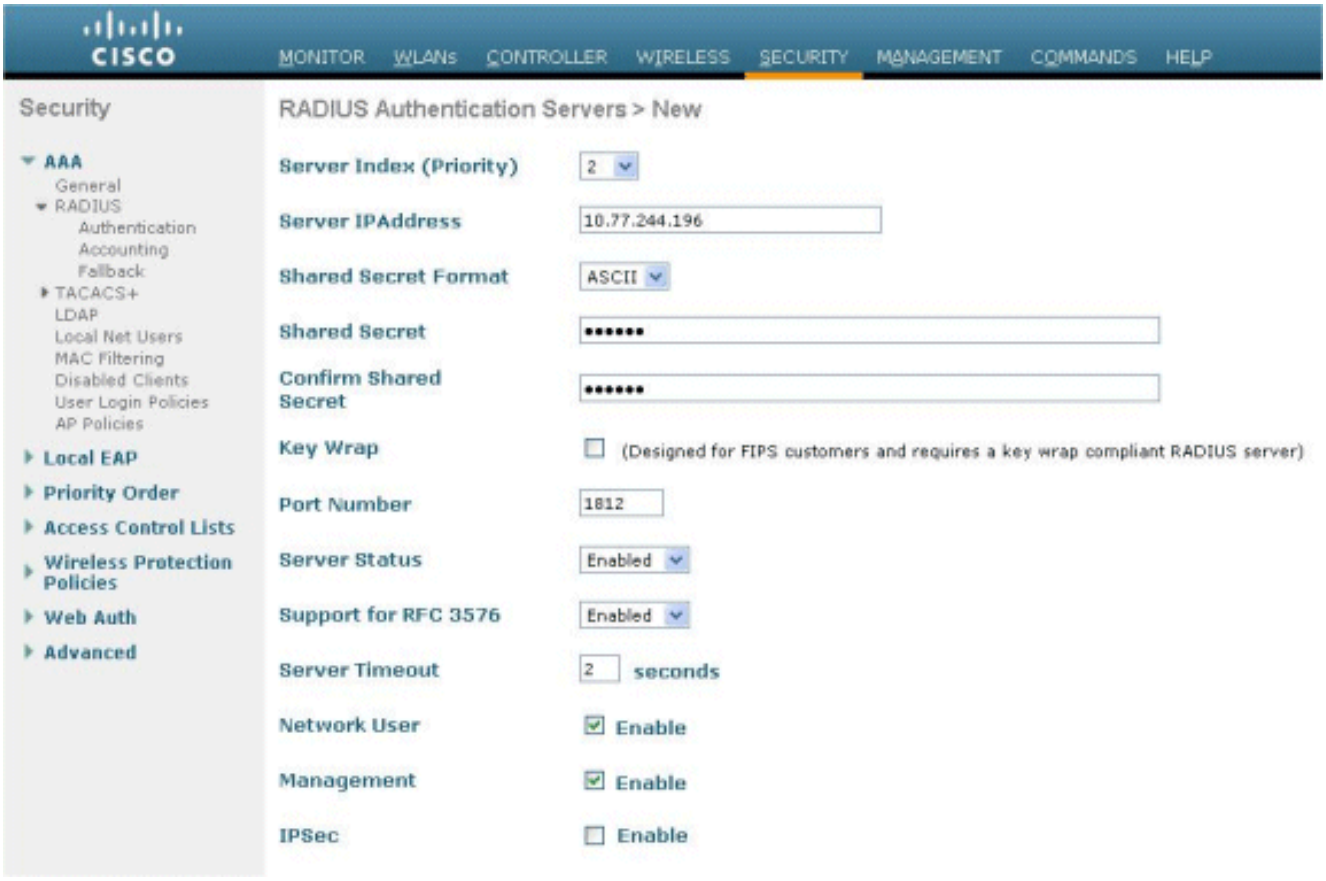
Neste original, nós supomos que o WLC já está configurado e tem um REGAÇO registrado ao WLC. Este original mais adicional supõe que o WLC está configurado para a operação básica e que os regaços estão registrados ao WLC. Se você é um novo usuário que tenta estabelecer o WLC para a operação básica com regaços, refira o registro de pouco peso AP (REGAÇO) a um controlador do Wireless LAN (WLC). Para ver os regaços que são registrados ao WLC, navegue ao **Sem fio > todos os APs**.

Uma vez que o WLC é configurado para a operação básica e tem uns ou vários regaços registrados a ele, você pode configurar o WLC para a autenticação do web externa usando um servidor de Web externo. Em nosso exemplo, nós estamos usando uma versão 4.1.1.24 do Cisco Secure ACS como o servidor Radius. Primeiramente, nós configuraremos o WLC para este servidor Radius, e então nós olharemos a configuração exigida no Cisco Secure ACS para esta instalação.

Configurar o WLC para o Cisco Secure ACS

Execute estas etapas a fim adicionar o servidor Radius no WLC:

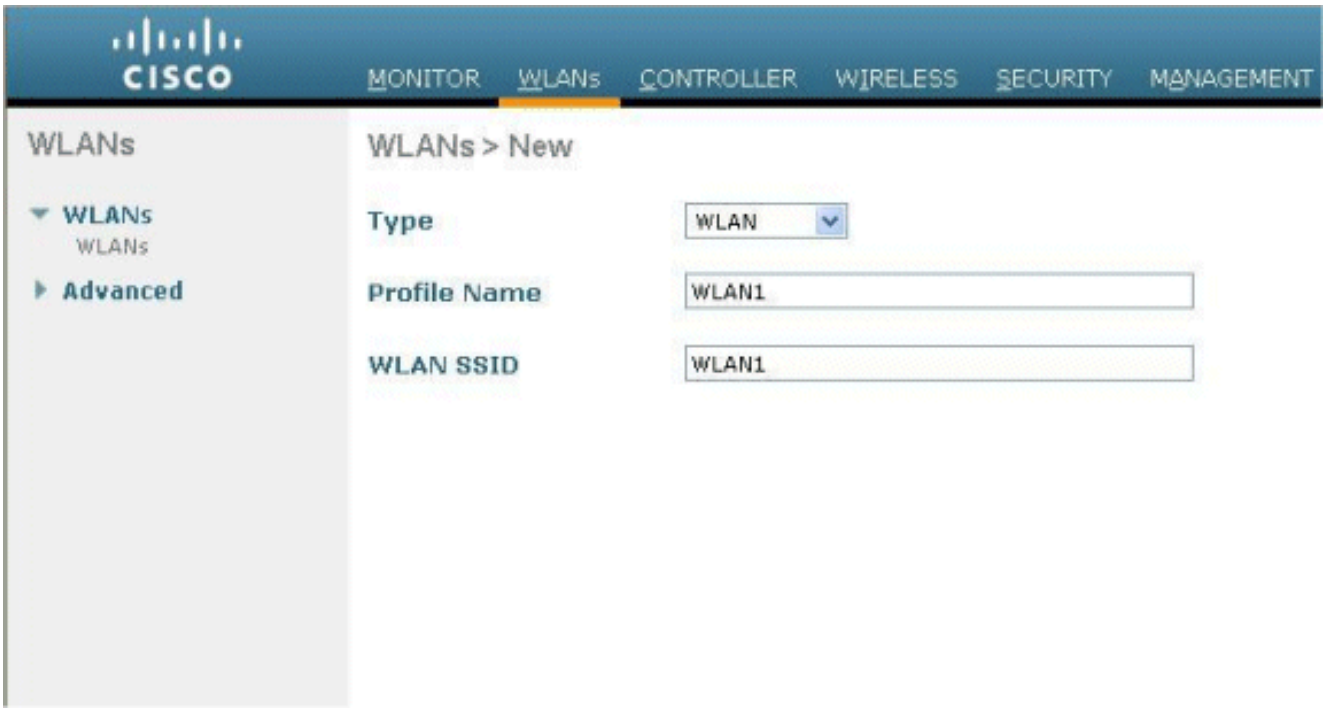
1. Do WLC GUI, clique o **menu Segurança**.
2. Sob o **menu AAA**, navegue ao submenu do **raio >** da **autenticação**.
3. Clique **novo**, e incorpore o IP address do servidor Radius. Neste exemplo, o IP address do server é *10.77.244.196*.
4. Incorpore o segredo compartilhado ao WLC. O segredo compartilhado deve ser configurado o mesmos no WLC.
5. Escolha o **ASCII** ou **encantar** para o formato secreto compartilhado. O mesmo formato precisa de ser escolhido no WLC.
6. **1812** são o número de porta usado para a autenticação RADIUS.
7. Assegure-se de que a opção do status de servidor esteja ajustada ao **permitido**.
8. Verifique o usuário de rede **permitem a** caixa de autenticar os usuários de rede.
9. O clique **aplica-se**.



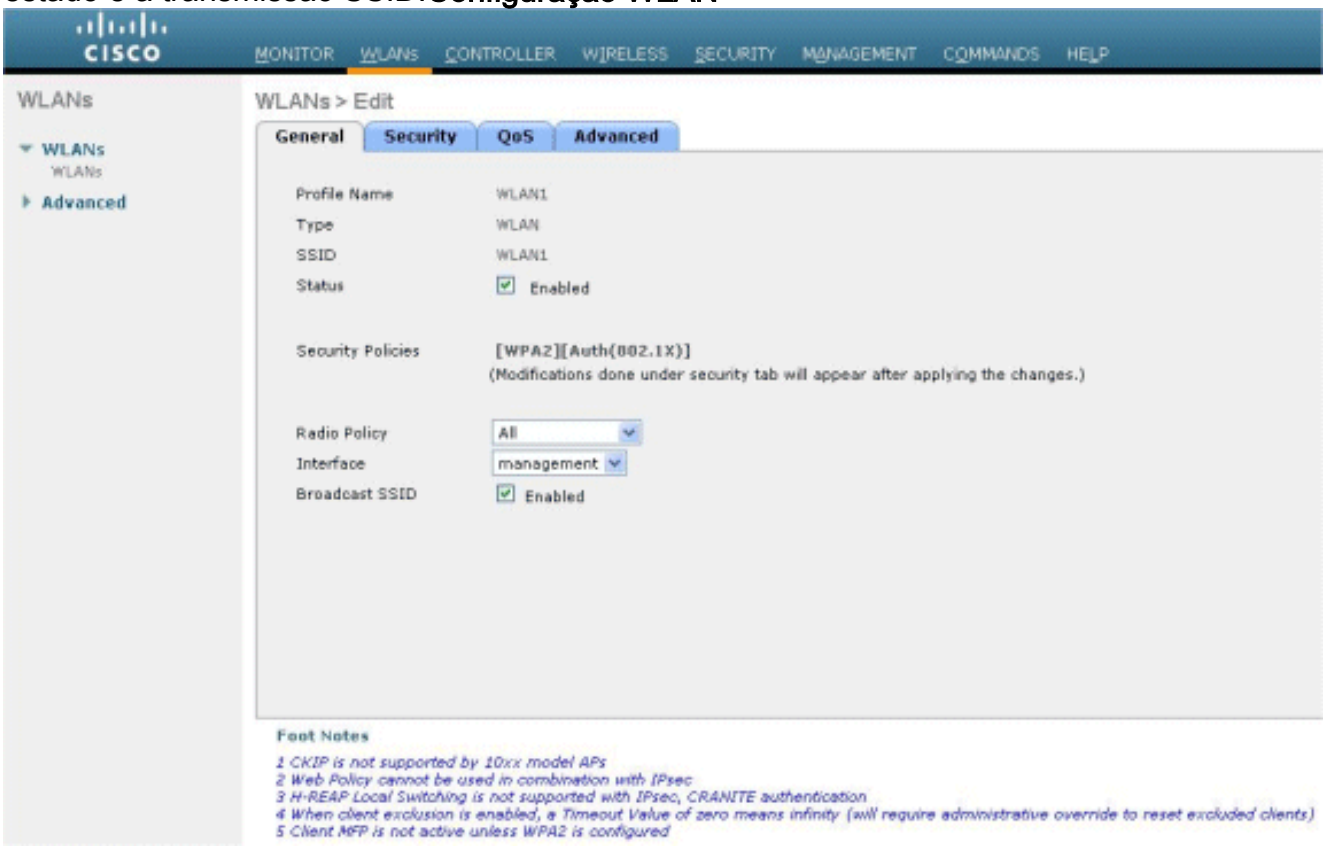
Configurar o WLAN em WLC para a autenticação da Web

A próxima etapa é configurar o WLAN para a autenticação da Web em WLC. Execute estas etapas a fim configurar o WLAN em WLC:

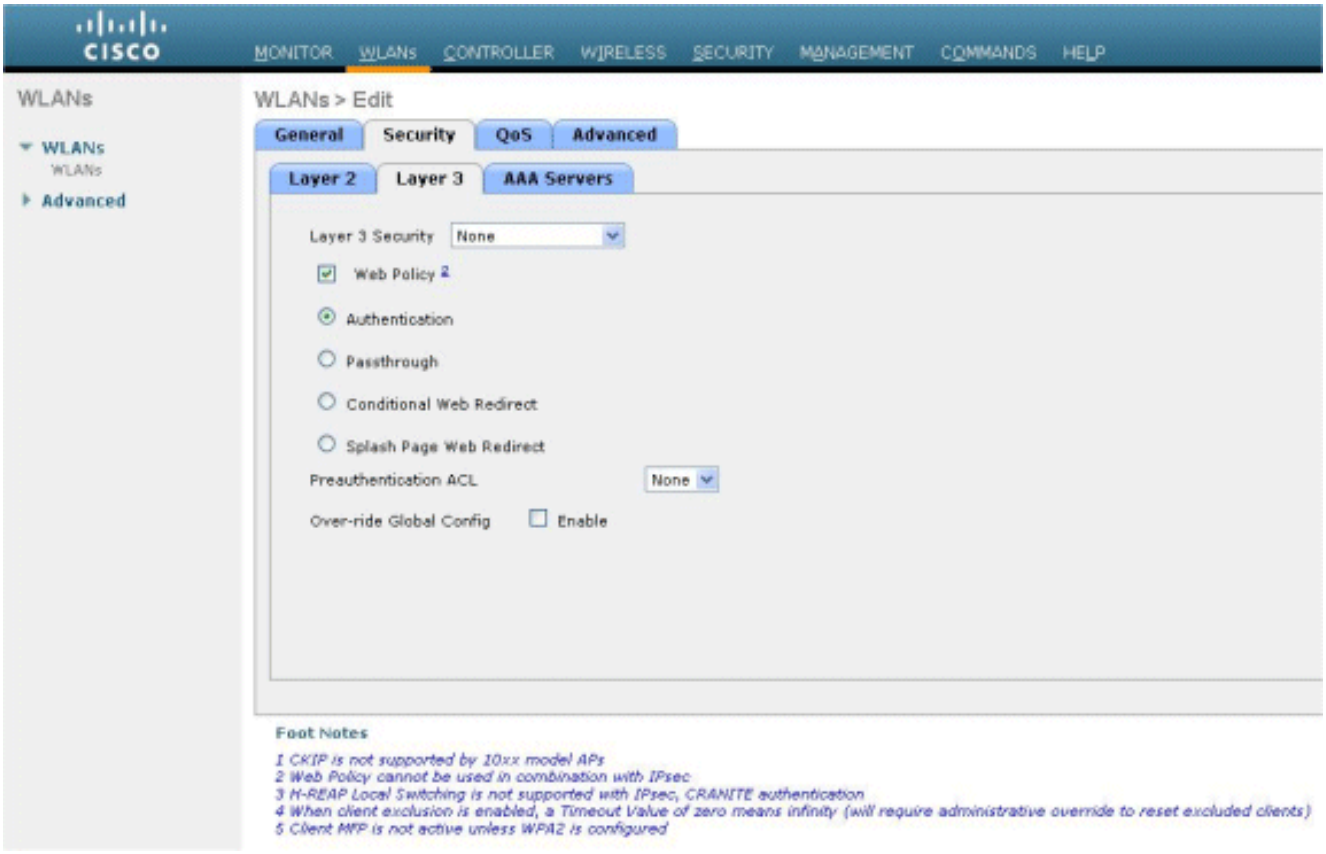
1. Clique o menu **WLAN do** controlador GUI, e escolha **novo**.
2. Escolha o **WLAN** para o tipo.
3. Incorpore um nome de perfil e um WLAN SSID de sua escolha, e o clique **aplica-se**.**Note**: O WLAN SSID é diferenciando maiúsculas e minúsculas.



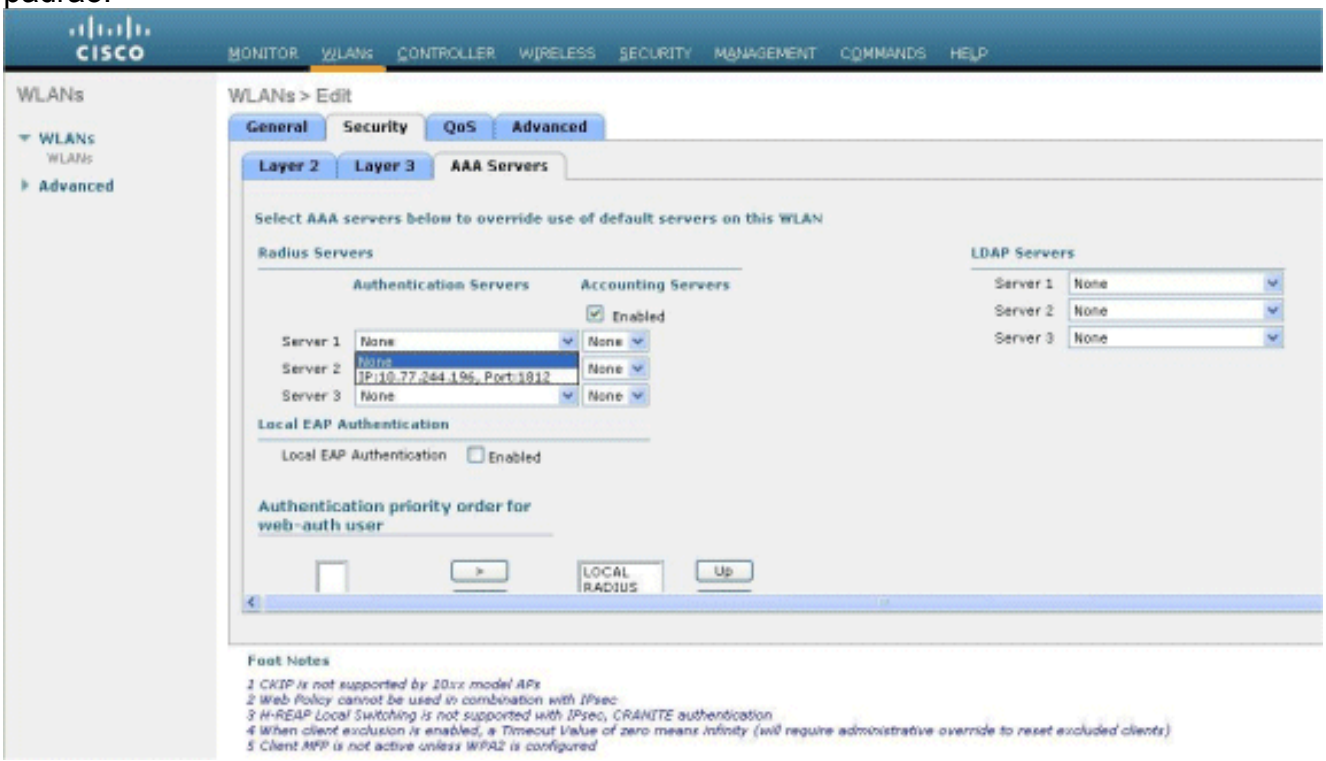
4. Sob o **tab geral**, certifique-se de que a opção **permitida** está verificada para ver se há o estado e a transmissão SSID.**Configuração WLAN**



5. Escolha uma relação para o WLAN. Tipicamente, uma relação configurada em um VLAN original é traçada ao WLAN de modo que o cliente receba um IP address nesse VLAN. Neste exemplo, nós usamos o *Gerenciamento* para a relação.
6. Escolha a **ABA de segurança**.
7. Sob o menu da **camada 2**, não escolha **nenhuns** para a Segurança da camada 2.
8. Sob o menu da **camada 3**, não escolha **nenhuns** para a Segurança da camada 3. Verifique a **caixa de verificação de Política da web**, e escolha a **autenticação**.



9. Sob o menu dos **servidores AAA**, para o Authentication Server, escolha o servidor Radius que foi configurado neste WLC. Outros menus devem permanecer em valores padrão.

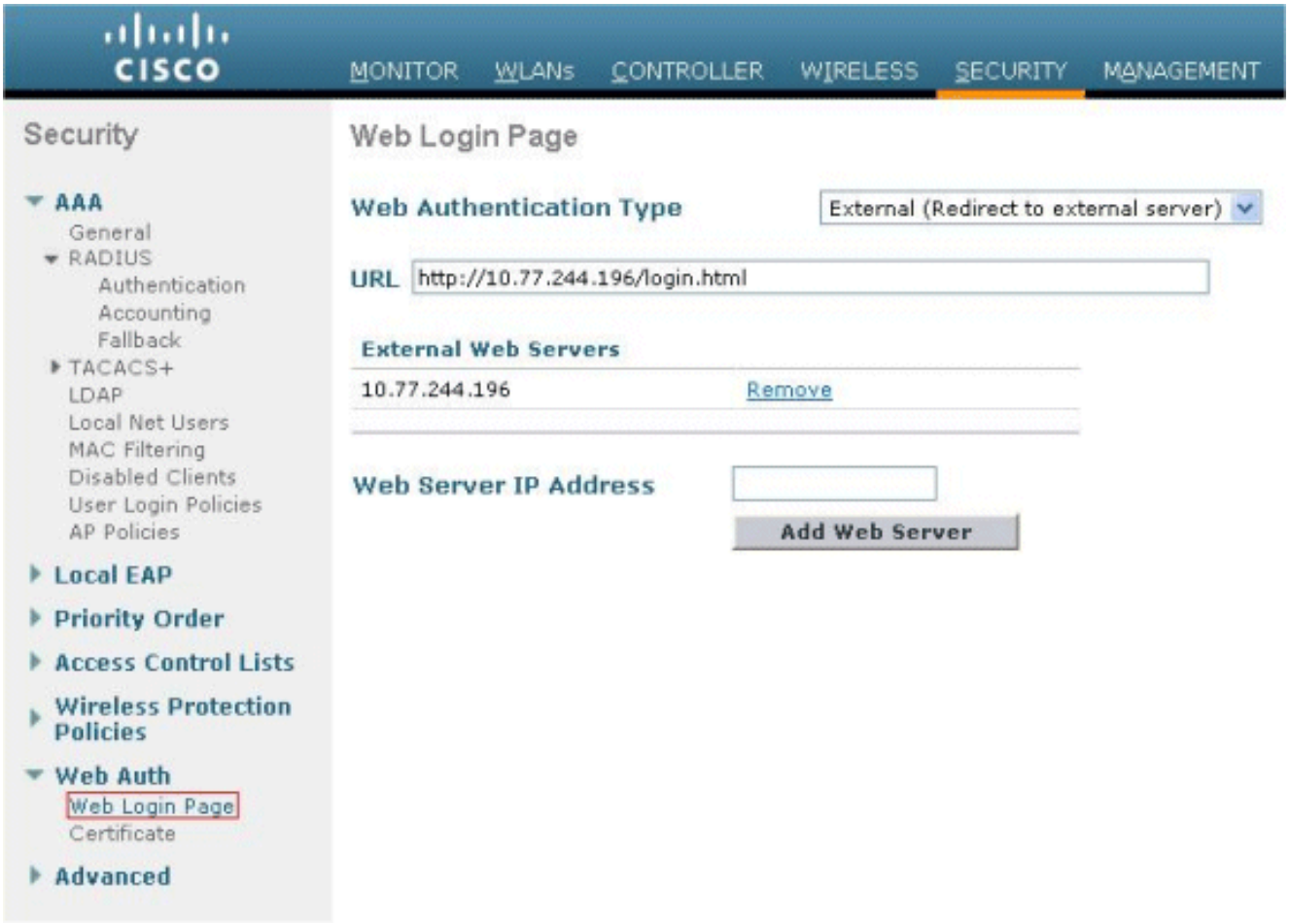


Configurar a informação do servidor de Web em WLC

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

1. Clique a **ABA de segurança**. Vá ao **AUTH da Web >** à **página de login da Web**.

2. Ajuste o tipo da autenticação da Web como **externo**.
3. No campo do IP address do servidor de Web, incorpore o IP address do server que hospeda a página da autenticação da Web, e o clique **adiciona o servidor de Web**. Neste exemplo, o IP address é *10.77.244.196*, que aparece sob servidores de Web externos.
4. Incorpore a URL para a página da autenticação da Web (neste exemplo, *http://10.77.244.196/login.html) no* campo URL.



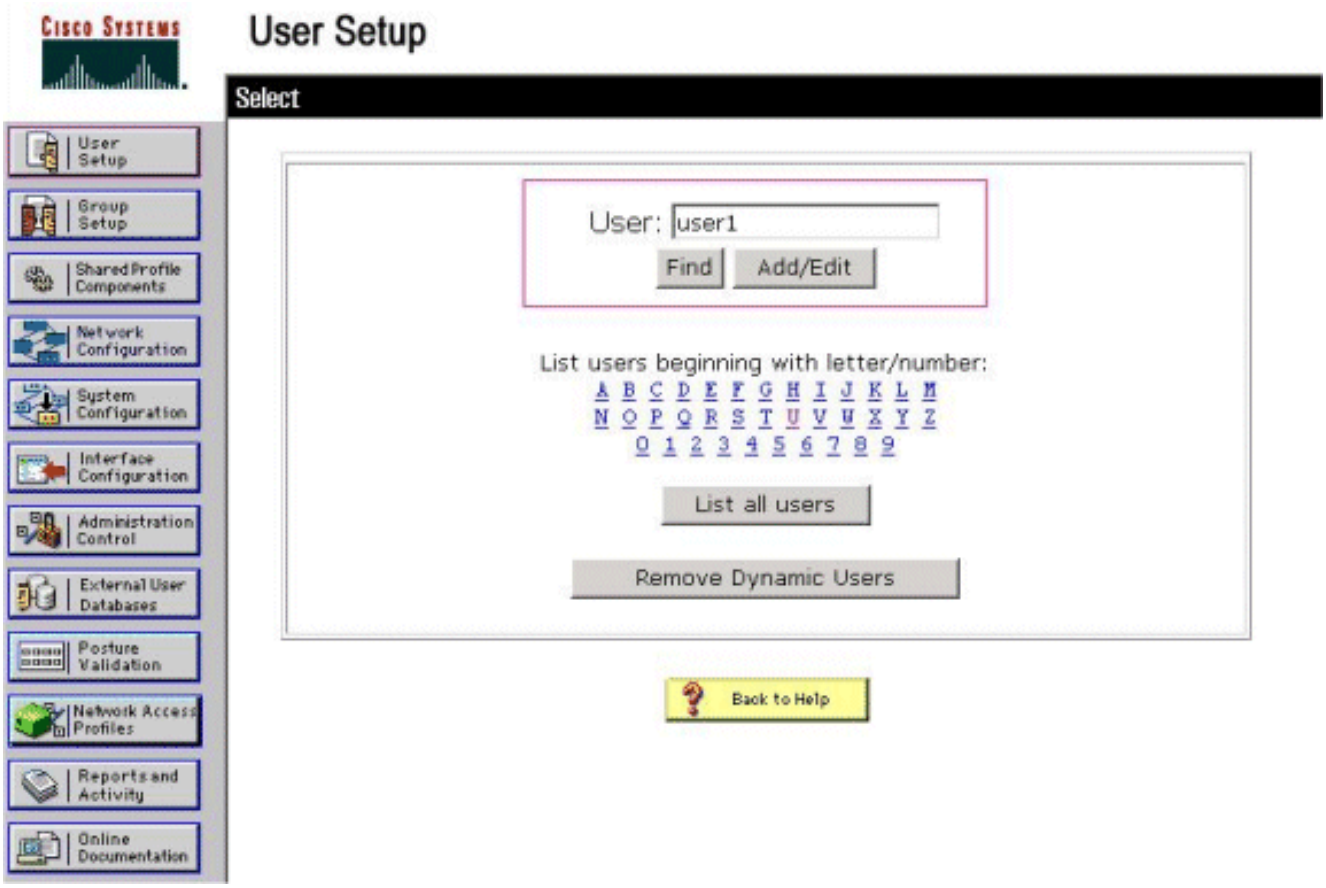
Configurar o Cisco Secure ACS

Neste original nós supomos que o server do Cisco Secure ACS é já instalado e sendo executado em uma máquina. Para mais informação como setup o Cisco Secure ACS refira o manual de configuração para o Cisco Secure ACS 4.2.

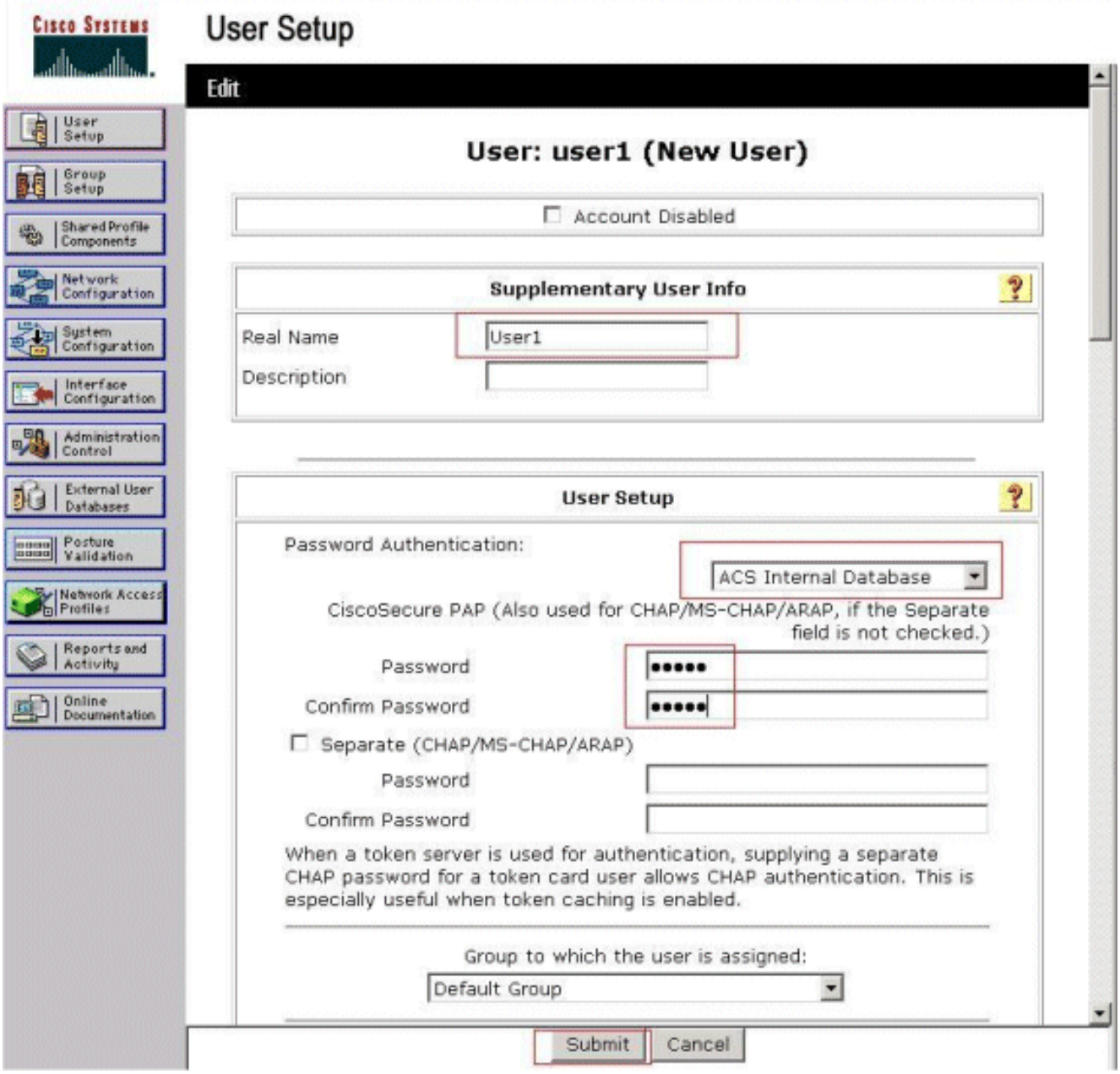
Configurar a informação de usuário no Cisco Secure ACS

Execute estas etapas a fim configurar usuários no Cisco Secure ACS:

1. Escolha a **instalação de usuário do** Cisco Secure ACS GUI, incorpore um username, e o clique **adiciona/edita**. Neste exemplo, o usuário é *user1*.



2. Àrevelia, o PAP é usado para clientes de autenticação. A senha para o usuário é incorporada sob a **instalação de usuário** > a **autenticação de senha** > o **Cisco PAP seguro**. Certifique-se de você escolher o **base de dados interno ACS** para a autenticação de senha.



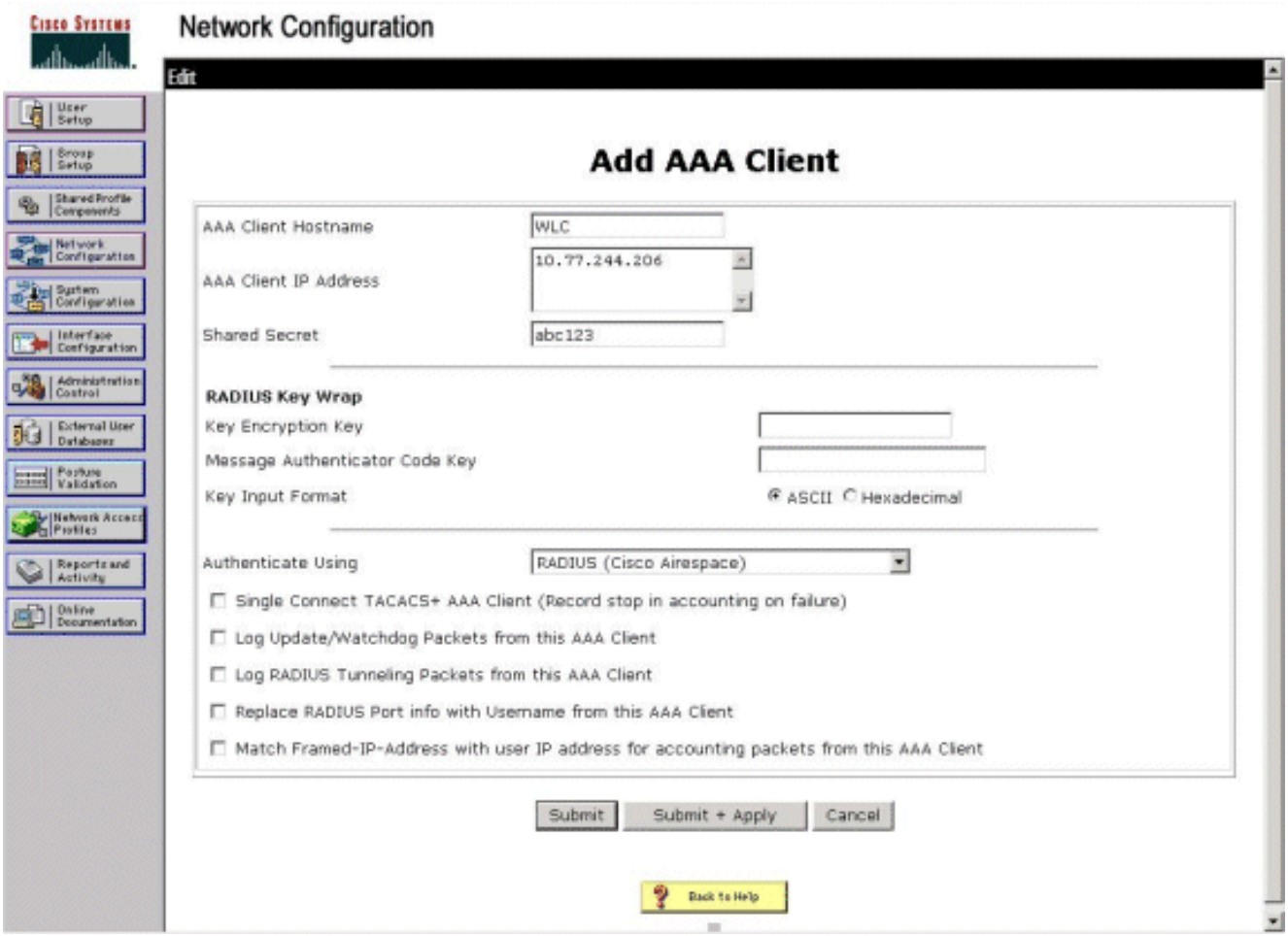
3. O usuário precisa de ser atribuído um grupo a que o usuário pertence. Escolha o **grupo padrão**.
4. Clique em Submit.

Configurar a informação WLC no Cisco Secure ACS

Execute estas etapas a fim configurar a informação WLC no Cisco Secure ACS:

1. No ACS GUI, clique a aba da **configuração de rede**, e o clique **adiciona a entrada**.
2. A tela do cliente de AAA adicionar aparece.
3. Dê entrada com o nome do cliente. Neste exemplo, nós usamos *WLC*.
4. Incorpore o IP address do cliente. O IP address Do WLC é *10.77.244.206*.
5. Incorpore a chave secreta compartilhada e o formato chave. Isto deve combinar a entrada feita no **menu Segurança do** WLC.
6. Escolha o **ASCII** para o formato da entrada chave, que deve ser o mesmo no WLC.
7. Escolha o **RAIO (Cisco Airespace)** para Authenticate usando-se a fim ajustar o protocolo usado entre o WLC e o servidor Radius.
8. O clique **submete-se + aplica-**

se.

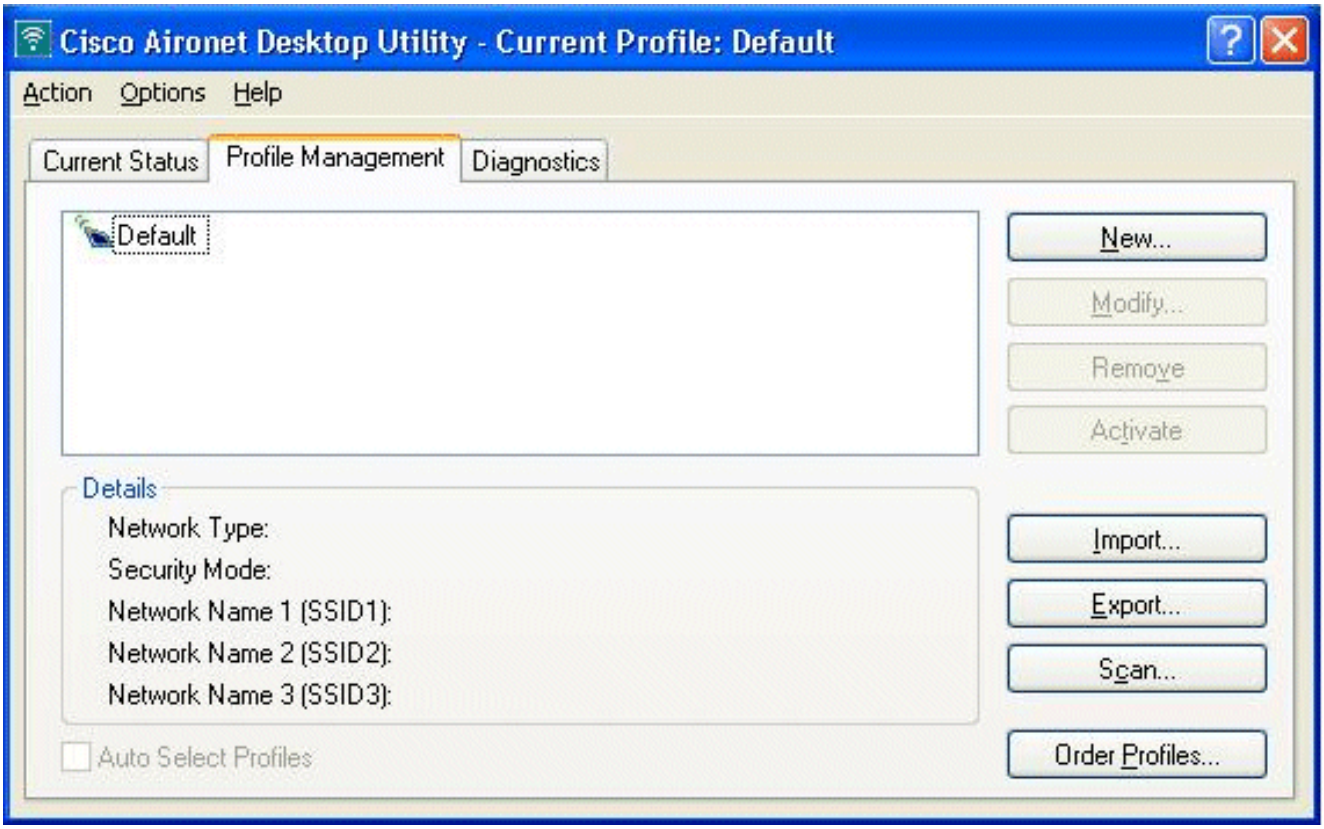


Processo de authenticação do cliente

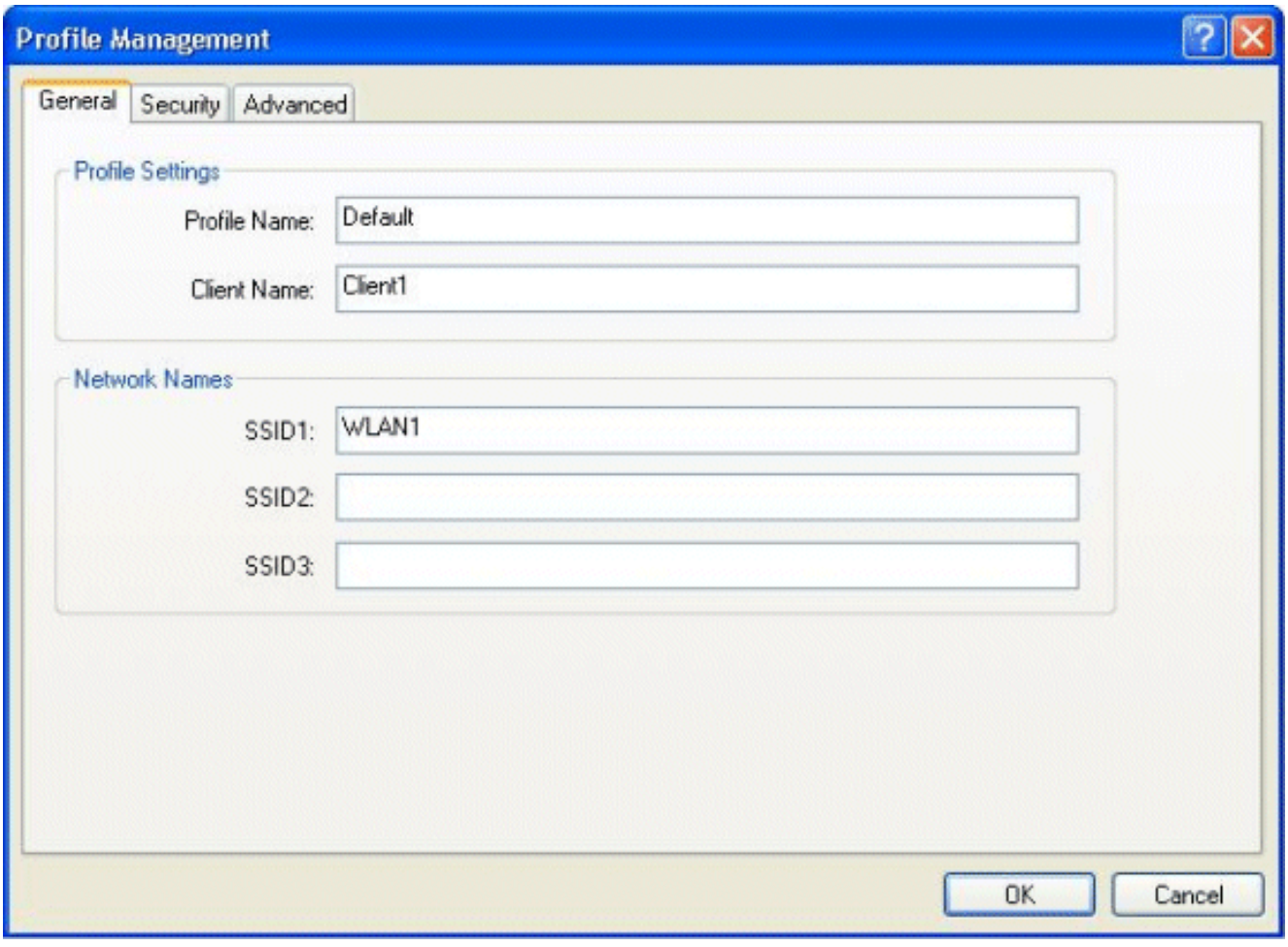
Configuração do Cliente

Neste exemplo, nós usamos o utilitário de desktop do Cisco Aironet para executar a autenticação da Web. Execute estas etapas a fim configurar o utilitário de desktop de Aironet.

1. Abra o utilitário de desktop de Aironet do **começo** > do **Cisco Aironet** > do **utilitário de desktop de Aironet**.
2. Clique sobre a aba do **Gerenciamento do perfil**.

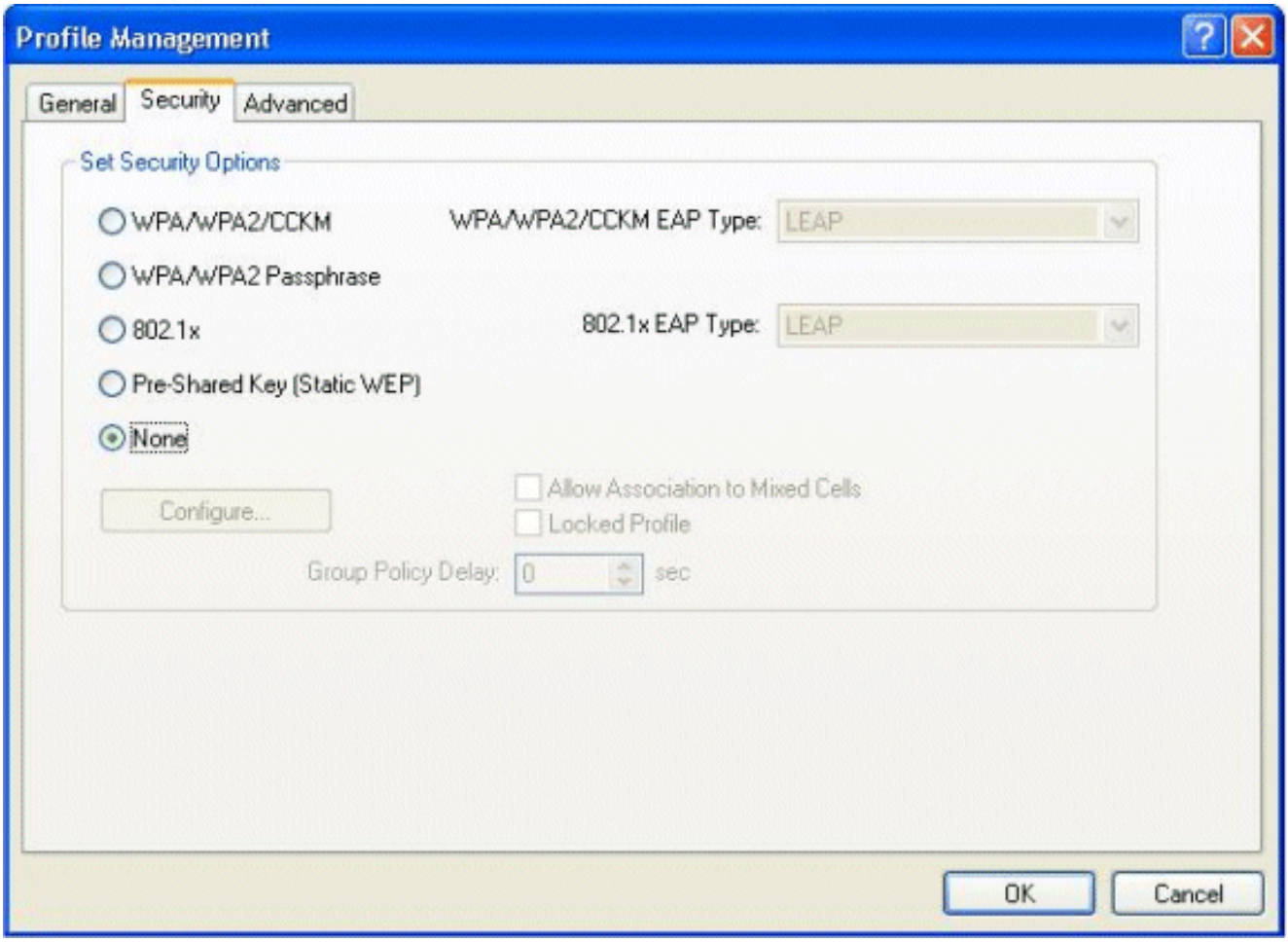


3. Escolha o **perfil padrão**, e o clique **altera**.Clique o **tab geral**.Configurar um nome de perfil. Neste exemplo, o *padrão* é usado.Configurar o SSID sob nomes de rede. Neste exemplo, *WLAN1* é
usado.

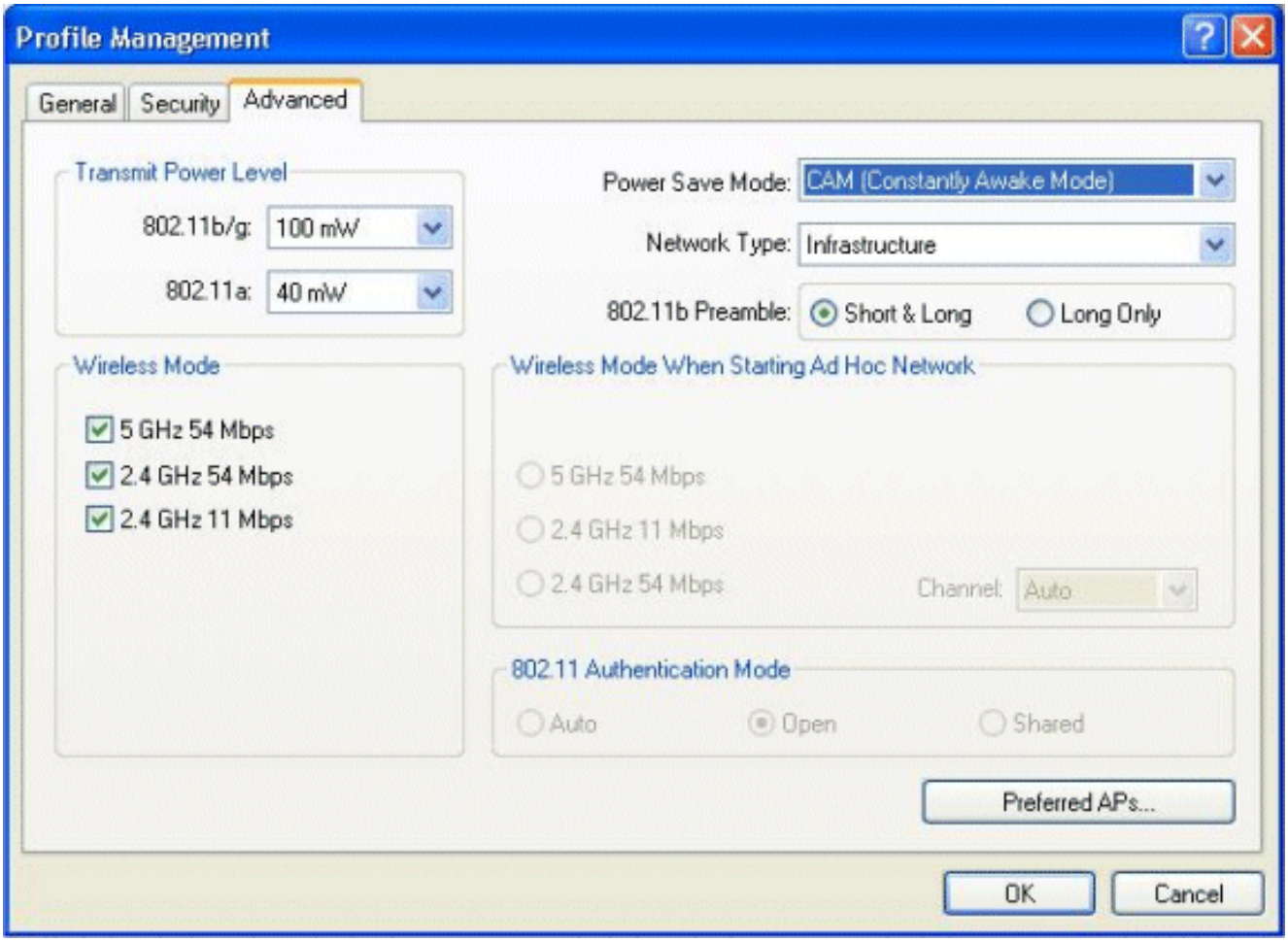


Note: O SSID é diferenciando maiúsculas e minúsculas e deve combinar o WLAN configurado no WLC.Clique a **ABA de segurança**.Não escolha **nenhuns** como a Segurança

para a autenticação da
Web.



Clique o **guia avançada**.Sob o menu **sem fio do modo**, escolha a frequência em que o cliente Wireless se comunica com o REGAÇO.Sob o **nível de potência de transmissão**, escolha a potência que é configurada no WLC.Deixe o valor padrão para o modo de economia de energia.Escolha a **infraestrutura** como o tipo de rede.Ajuste o preâmbulo 802.11b como **curto & longo** para a melhor compatibilidade.Click
OK.



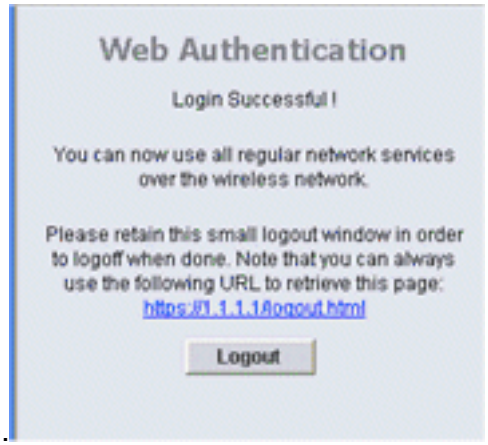
4. Uma vez que o perfil é configurado no software do cliente, o cliente está associado com sucesso e recebe um IP address do pool VLAN configurado para a interface de gerenciamento.

Processo do login do cliente

Esta seção explica como o login do cliente ocorre.

1. Abra uma janela de navegador e incorpore toda a URL ou IP address. Isto traz a página da autenticação da Web ao cliente. Se o controlador está executando qualquer liberação mais cedo do que o 3.0, o usuário deve entrar em *https://1.1.1.1/login.html* para trazer acima a página da autenticação da Web. Uma janela de alerta de segurança é exibida.
2. Clique **Yes** para continuar.
3. Quando o indicador do início de uma sessão aparece, incorpore o nome de usuário e senha que é configurado no servidor Radius. Se seu início de uma sessão é bem sucedido, você verá duas janelas de navegador. O indicador maior indica o login bem-sucedido, e você pode este indicador consultar o Internet. Use a janela menor para encerrar a sessão quando

seu uso da rede guest estiver concluído.

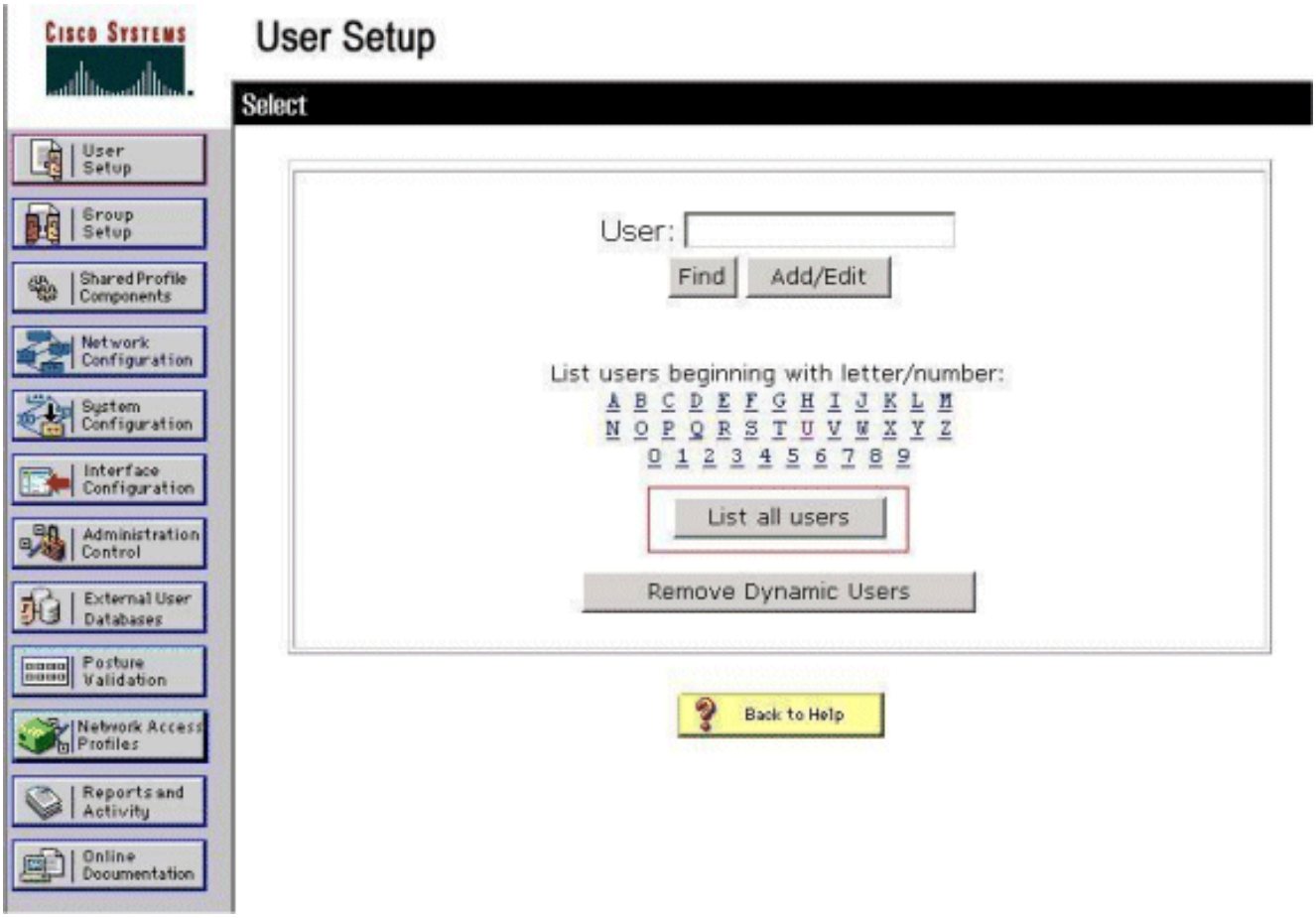


Verificar

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

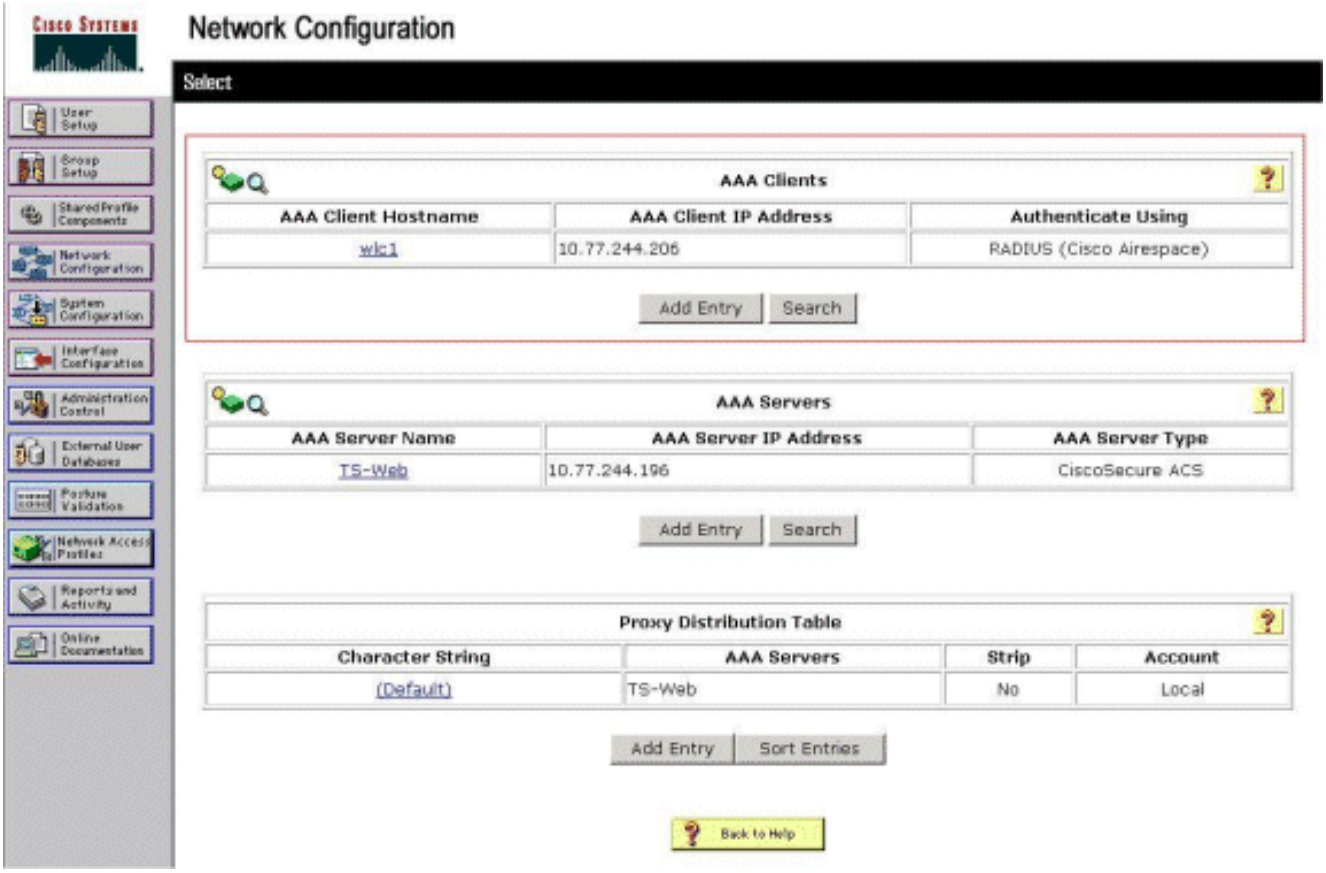
Verificar o ACS

1. Clique a **instalação de usuário**, e clique então a **lista todos os usuários no** ACS GUI.



Certifique-se que o estado do usuário *está permitido* e que o grupo padrão está traçado ao usuário.

2. Clique a aba da **configuração de rede**, e o olhar na tabela dos **clientes de AAA** a fim verificar que o WLC está configurado como um cliente de AAA.

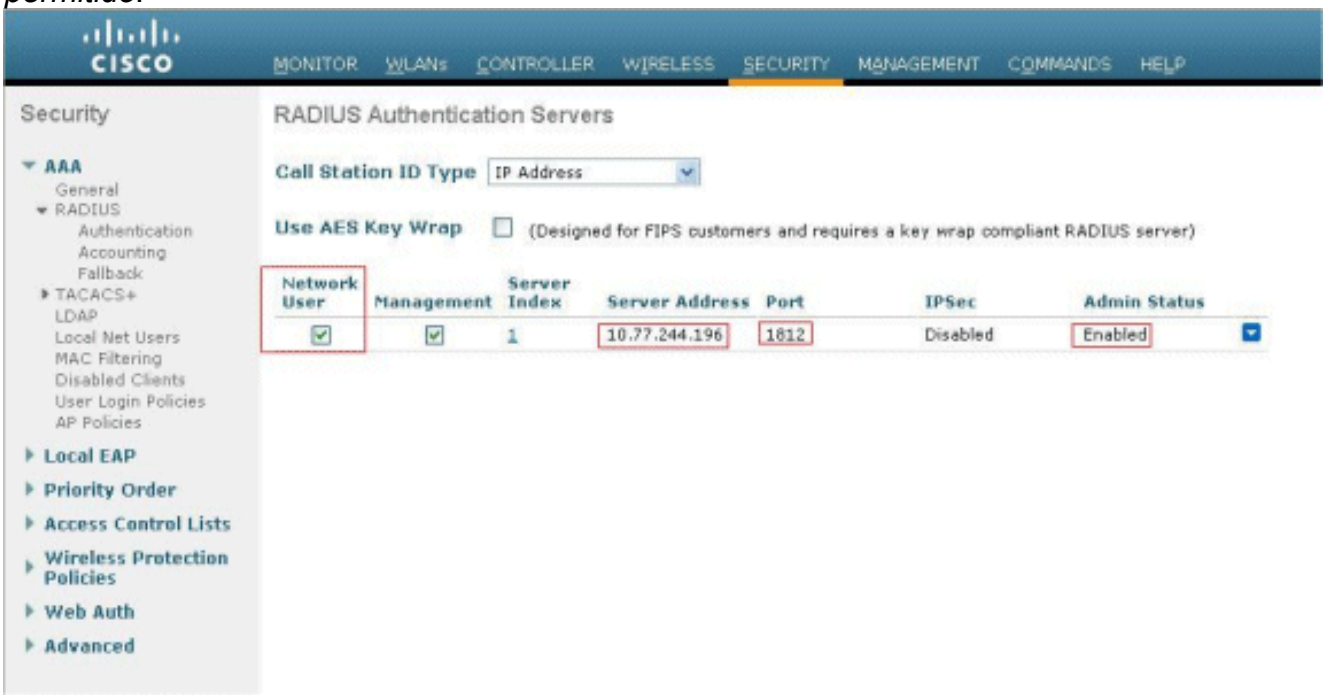


Verifique WLC

1. Clique o menu **WLAN do** WLC GUI.Certifique-se que o WLAN usado para a autenticação da Web está alistado na página.Certifique-se que o status administrativo para o WLAN *está permitido*.Certifique-se da política de segurança para o Web-*AUTH das* mostras WLAN.

2. Clique o **menu Segurança do** WLC GUI.Certifique-se que o Cisco Secure ACS

(10.77.244.196) está alistado na página.Certifique-se que a caixa do usuário de rede está verificada.Certifique-se que a porta é *1812* e que o status administrativo *está permitido*.



Troubleshooting

Há muitas razões pelas quais uma autenticação da Web não é bem sucedida. A autenticação da Web do Troubleshooting do original em um controlador do Wireless LAN (WLC) explica claramente aquelas razões em detalhe.

Comandos para Troubleshooting

Note: Refira a informação importante em comandos Debug antes que você use estes **comandos debug**.

O telnet no WLC e emite estes comandos pesquisar defeitos a 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)
```

- **debugar o detalhe aaa permitem**

As tentativas da autenticação falha são alistadas no menu situado em **relatórios e em atividade >** em **falhas de tentativa**.

Informações Relacionadas

- Exemplo de configuração da autenticação da Web do controlador do Wireless LAN
- Pesquisar defeitos a autenticação da Web em um controlador do Wireless LAN (WLC)
- Exemplo de configuração de autenticação de web externa com Wireless LAN Controllers
- Autenticação da Web usando o LDAP no exemplo de configuração dos controladores do Wireless LAN (WLCs)
- Suporte técnico & documentação - Cisco Systems