Configurar filtros MAC com controladoras Wireless LAN (WLCs) AireOS

Contents

Introdução

Este documento descreve como configurar filtros MAC com controladoras Wireless LAN (WLCs).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração de LAPs e Cisco WLCs
- Soluções Cisco Unified Wireless Security

Componentes Utilizados

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

- Cisco 4400 WLC que executa a versão de software 5.2.178.0
- LAPs Cisco 1230AG Series
- Adaptador de cliente sem fio 802.11 a/b/g com firmware 4.4
- Aironet Desktop Utility (ADU) versão 4.4

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Conventions

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

Informações de Apoio

Este documento descreve como configurar filtros MAC com controladoras Wireless LAN (WLCs) com um exemplo de configuração. Este documento também discute como autorizar Lightweight Access Points (LAPs) contra um servidor AAA.

Filtro de Endereço MAC (Autenticação MAC) em WLCs

Quando você cria um filtro de endereços MAC nas WLCs, os usuários recebem ou não acesso à rede WLAN com base no endereço MAC do cliente que usam.

Há dois tipos de autenticação MAC que são suportados nas WLCs:

- Autenticação MAC local
- Autenticação MAC usada com um servidor RADIUS

Com a autenticação MAC local, os endereços MAC do usuário são armazenados em um banco de dados na WLC. Quando um usuário tenta acessar a WLAN configurada para filtragem MAC, o endereço MAC do cliente é validado em relação ao banco de dados local na WLC e o cliente recebe acesso à WLAN se a autenticação for bem-sucedida.

Por padrão, o banco de dados local da WLC suporta até 512 entradas de usuário.

O banco de dados de usuário local é limitado a um máximo de 2048 entradas. O banco de dados local armazena entradas para estes itens:

- Usuários de gerenciamento local, o que inclui embaixadores de lobby
- Usuários da rede local, incluindo usuários convidados

- Entradas de filtro MAC
- Entradas da lista de exclusão
- Entradas da lista de autorização do ponto de acesso

Todos esses tipos de usuários não podem exceder o tamanho de banco de dados configurado.

Para aumentar o banco de dados local, use este comando da CLI:

```
<#root>

<Cisco Controller>

config database size ?

<count>        Enter the maximum number of entries (512-2048)
```

Como alternativa, a autenticação do endereço MAC também pode ser executada com um servidor RADIUS. A única diferença é que o banco de dados de endereços MAC dos usuários é armazenado no servidor RADIUS em vez do WLC. Quando um banco de dados de usuário é armazenado em um servidor RADIUS, a WLC encaminha o endereço MAC do cliente para o servidor RADIUS para validação do cliente. Em seguida, o servidor RADIUS valida o endereço MAC com base no banco de dados que ele possui. Se a autenticação do cliente for bem-sucedida, o cliente receberá acesso à WLAN. Qualquer servidor RADIUS que suporte autenticação de endereço MAC pode ser usado.

Configurar a autenticação MAC local em WLCs

Para configurar a autenticação MAC local nas WLCs:

1. Configure uma WLAN e ative a filtragem MAC.
2. Configure o banco de dados local na WLC com endereços MAC de cliente.

> Observação: antes de configurar a autenticação MAC, você deve configurar a WLC para a operação básica e registrar os LAPs na WLC. Este documento supõe que a WLC já esteja configurada para operação básica e que os LAPs estejam registrados na WLC. Se você for um usuário novo e quiser tentar configurar a WLC para a operação básica com LAPs, consulte Troubleshooting de um AP Lightweight que Falha ao Ingressar em uma WLC.

> Observação: não é necessária nenhuma configuração especial no cliente sem fio para oferecer suporte à autenticação MAC.

Configurar uma WLAN e Habilitar a Filtragem MAC

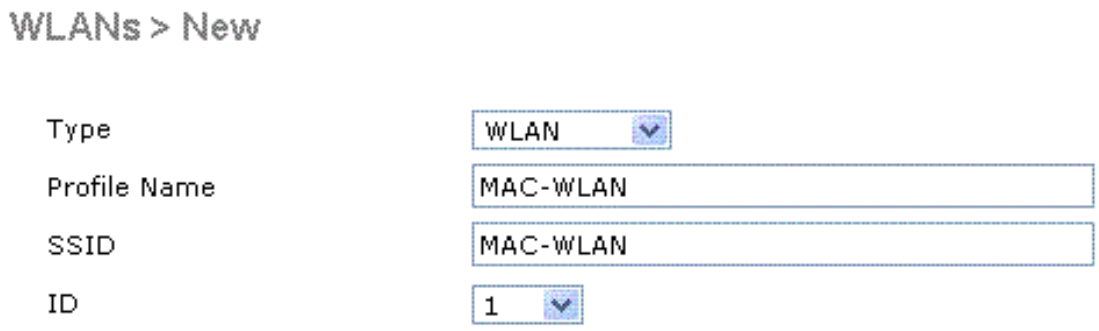
Para configurar uma WLAN com filtragem MAC:

1. Clique em WLANs na GUI do controlador para criar uma WLAN.

   A janela WLANs será exibida. Essa janela lista as WLANs configuradas no controlador.

2. Clique em Novo para configurar uma nova WLAN.

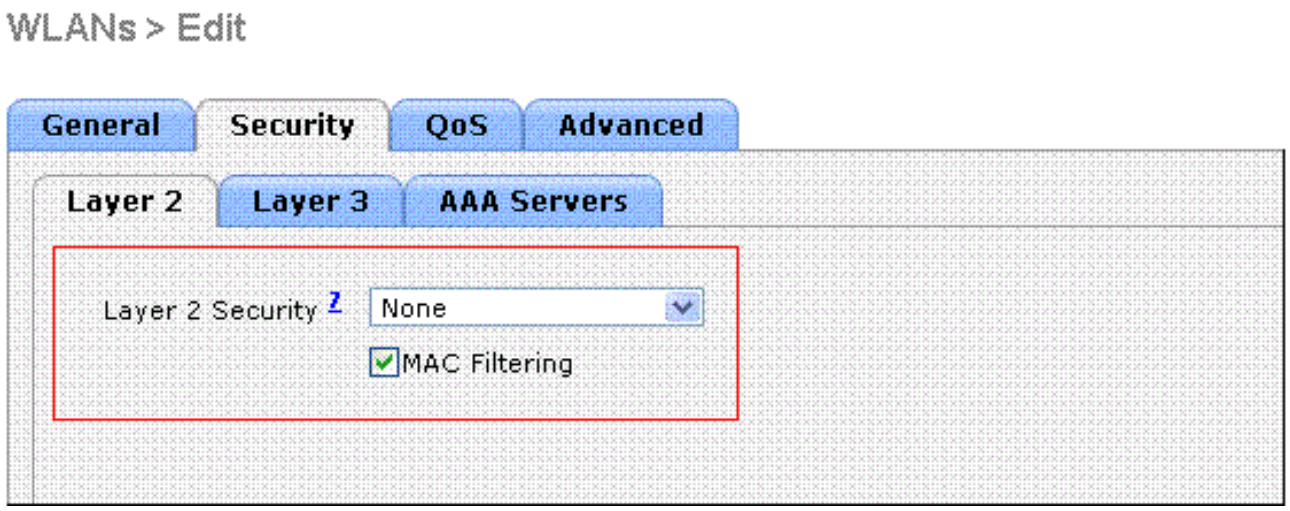
   Neste exemplo, a WLAN é chamada de MAC-WLAN e o ID da WLAN é 1.



Configurar WLAN Habilitar Filtragem MAC

3. Clique em Apply.

4. Na janela WLANs > Edit, defina os parâmetros específicos da WLAN.



Definir Parâmetros

   a. Em Security > Layer 2 > Layer 2 Security Policies, marque a caixa de seleção MAC Filtering.

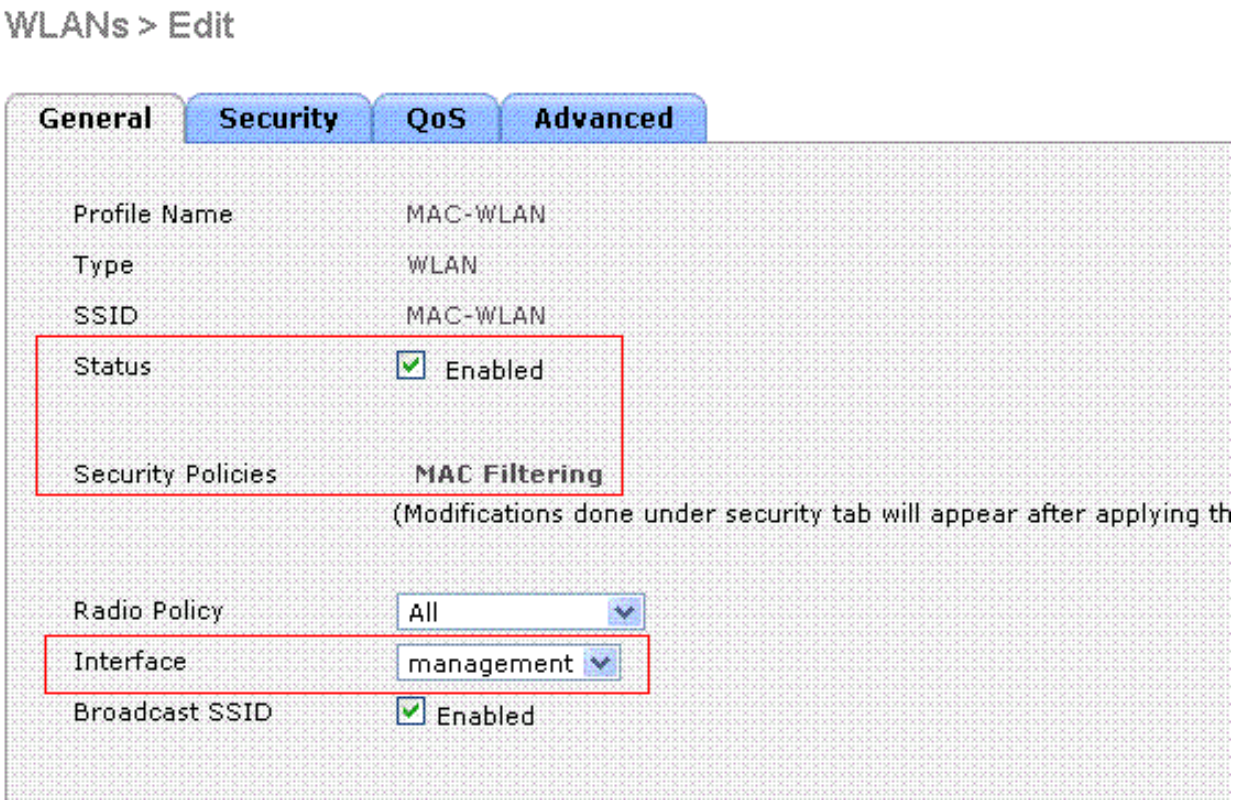
      Isso ativa a autenticação MAC para a WLAN.

b. Em General > Interface name, selecione a interface para a qual a WLAN está mapeada.

   Neste exemplo, a WLAN é mapeada para a interface de gerenciamento.

c. Selecione os outros parâmetros, que dependem dos requisitos do projeto da WLAN.

d. Clique em Apply.



WLAN mapeada para a interface

A próxima etapa é configurar o banco de dados local no WLC com os endereços MAC do cliente.

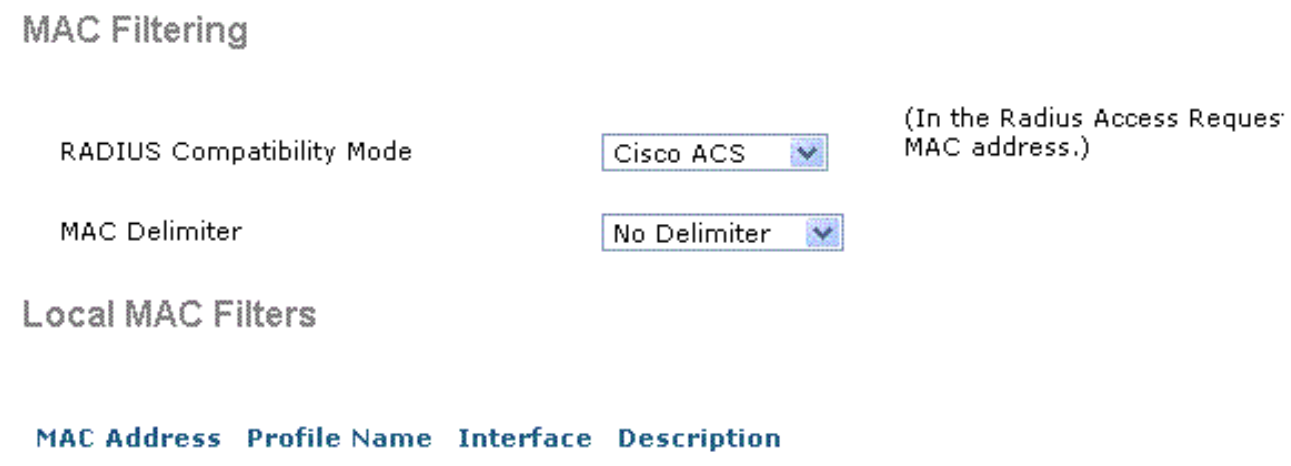
Consulte Exemplo de Configuração de VLANs em Wireless LAN Controllers para obter informações sobre como configurar interfaces dinâmicas (VLANs) em WLCs.

Configurar o banco de dados local na WLC com endereços MAC do cliente

Para configurar o banco de dados local com um endereço MAC do cliente no WLC:

1. Clique em Security na GUI do controlador e, em seguida, clique em MAC Filtering no menu à esquerda.

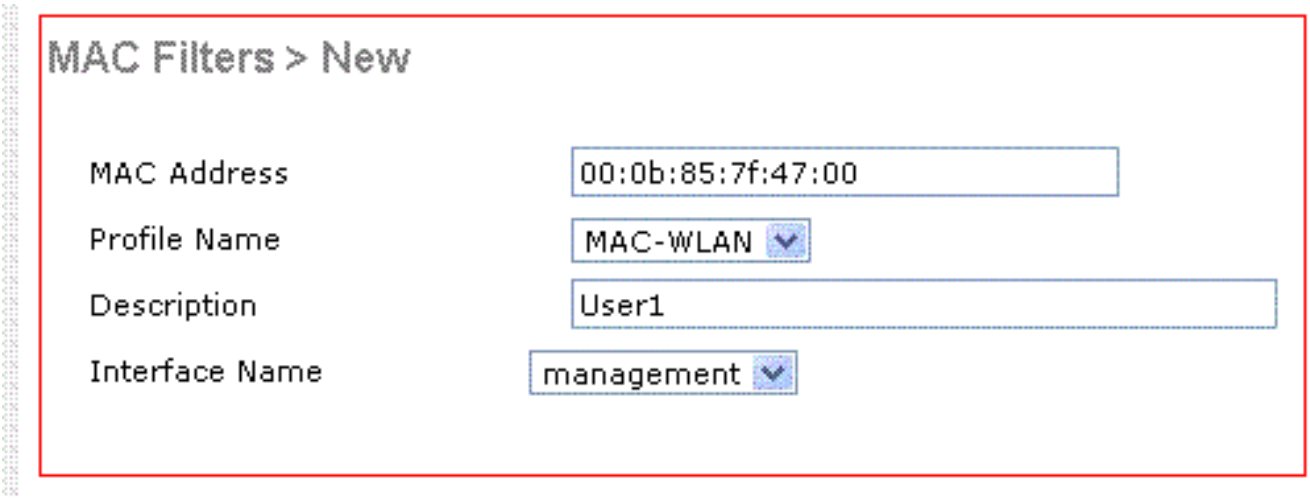
   A janela MAC Filtering (Filtragem de MACs) é exibida.



Janela de Filtragem MAC

2. Clique em New para criar uma entrada de endereço MAC de banco de dados local na WLC.
3. Na janela MAC Filters > New, insira o endereço MAC, o nome do perfil, a descrição e o nome da interface do cliente.

   Aqui está um exemplo:



Criar um Banco de Dados Local para Endereço MAC

4. Clique em Apply.
5. Repita as etapas de 2 a 4 para adicionar mais clientes ao banco de dados local.

   Agora, quando os clientes se conectam a essa WLAN, a WLC valida o endereço MAC dos clientes em relação ao banco de dados local e, se a validação for bem-sucedida, o cliente receberá acesso à rede.

Observação: neste exemplo, foi usado apenas um filtro de endereço MAC sem qualquer outro mecanismo de Segurança de Camada 2. A Cisco recomenda que a autenticação de endereço MAC deve ser usada juntamente com outros métodos de segurança da Camada 2 ou Camada 3. Não é aconselhável usar apenas a autenticação de endereço MAC para proteger sua rede WLAN, pois ela não fornece um mecanismo de segurança forte.

Configurar a autenticação MAC com um servidor RADIUS

Para configurar a autenticação MAC com um servidor RADIUS, use estes links. Neste exemplo, o servidor Cisco Secure ACS é usado como o servidor RADIUS.

1. Configurar uma WLAN e Habilitar a Filtragem MAC
2. Configurar o servidor RADIUS com endereços MAC do cliente

Configurar uma WLAN e Habilitar a Filtragem MAC

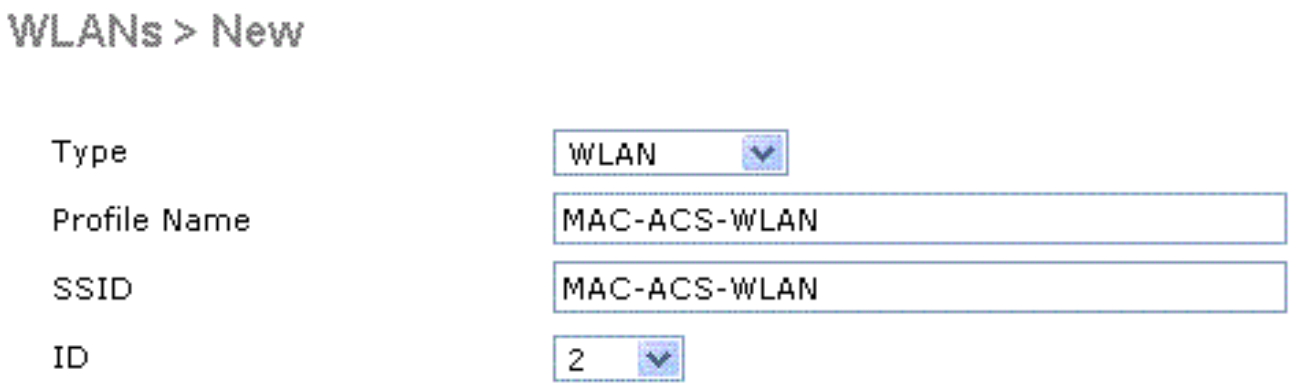
Para configurar uma WLAN com filtragem MAC:

1. Clique em WLANs na GUI do controlador para criar uma WLAN.

   A janela WLANs será exibida. Essa janela lista as WLANs configuradas no controlador.

2. Clique em Novo para configurar uma nova WLAN.

   Neste exemplo, a WLAN é chamada de MAC-ACS-WLAN e o ID da WLAN é 2.



Configurar uma nova WLAN Habilitar Filtragem MAC

3. Clique em Apply.
4. Na janela WLANs > Edit, defina os parâmetros específicos da WLAN.

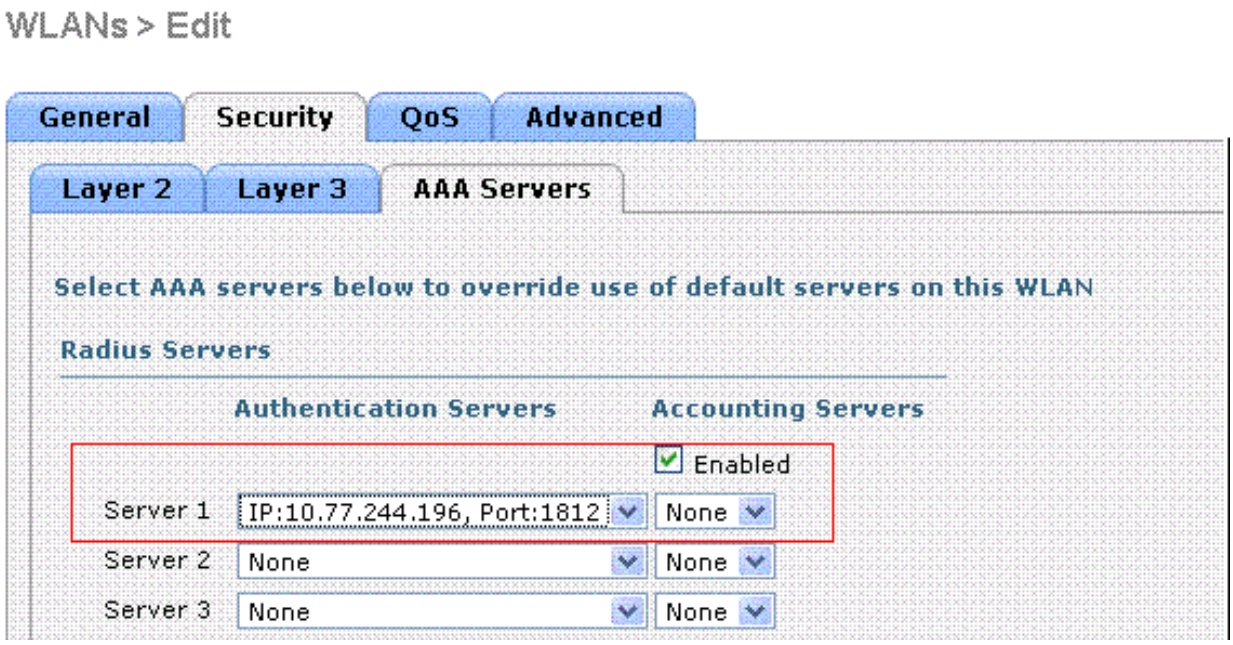
   a. Em Security > Layer 2 > Layer 2 Security Policies, marque a caixa de seleção MAC

Filtering.

Isso ativa a autenticação MAC para a WLAN.

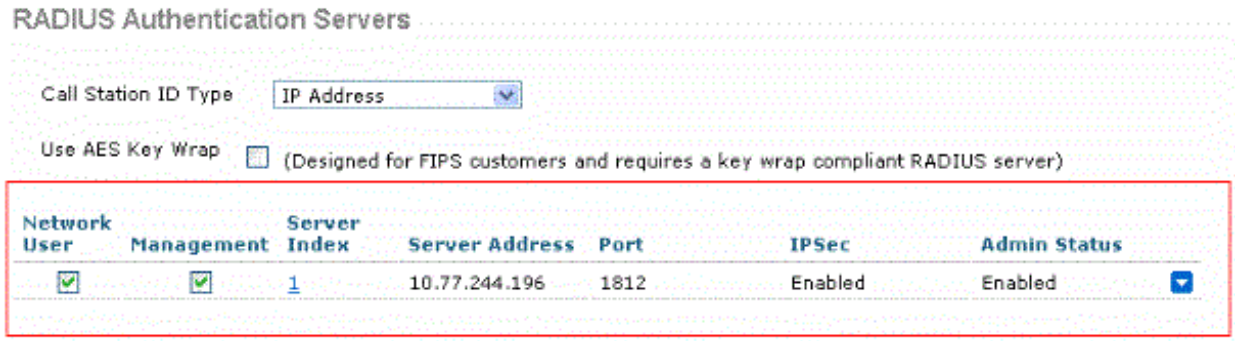
b. Em General > Interface name, selecione a interface para a qual a WLAN está mapeada.

c. Em Security > AAA Servers > RADIUS servers , selecione o servidor RADIUS que pode ser usado para a autenticação MAC.



Selecione o servidor RADIUS a ser usado para a Autenticação MAC.

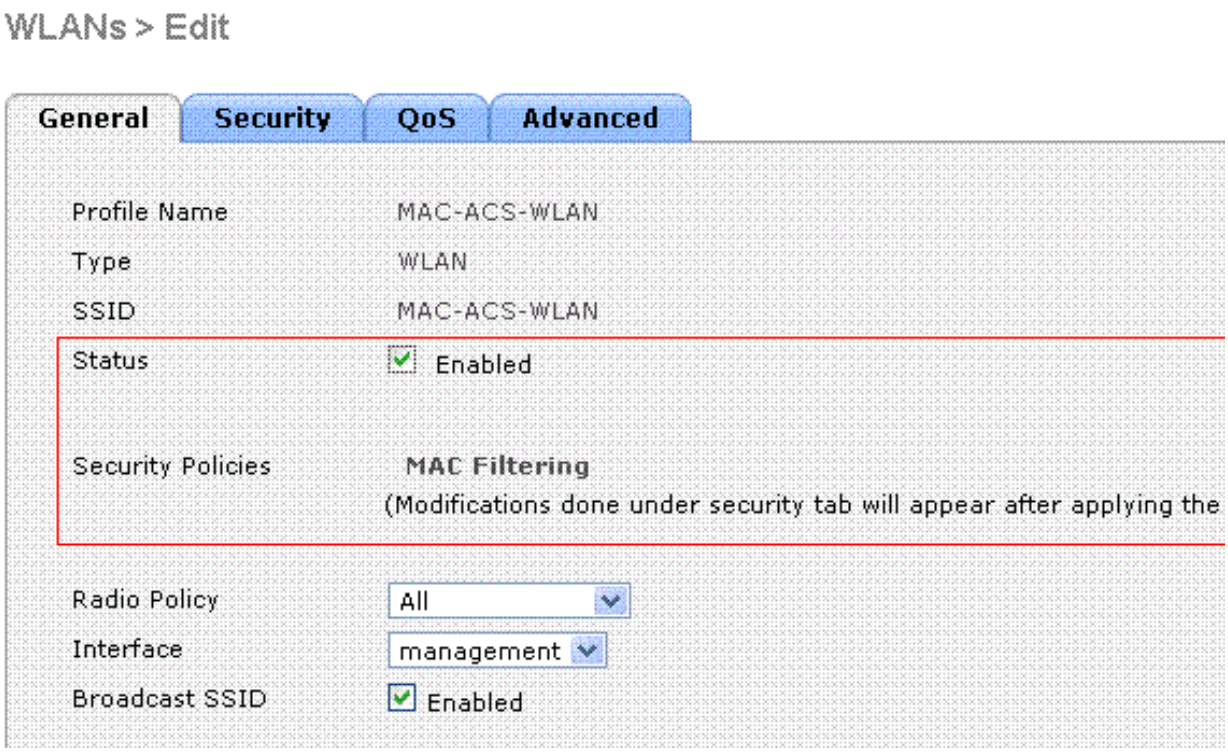
Observação: antes de selecionar o servidor RADIUS na janela WLAN > Edit, você deve definir o servidor RADIUS na janela Security > Radius Authentication e habilitar o servidor RADIUS.



Servidores de autenticação Radius

d. Selecione os outros parâmetros, que dependem dos requisitos do projeto da WLAN.

e. Clique em Apply.

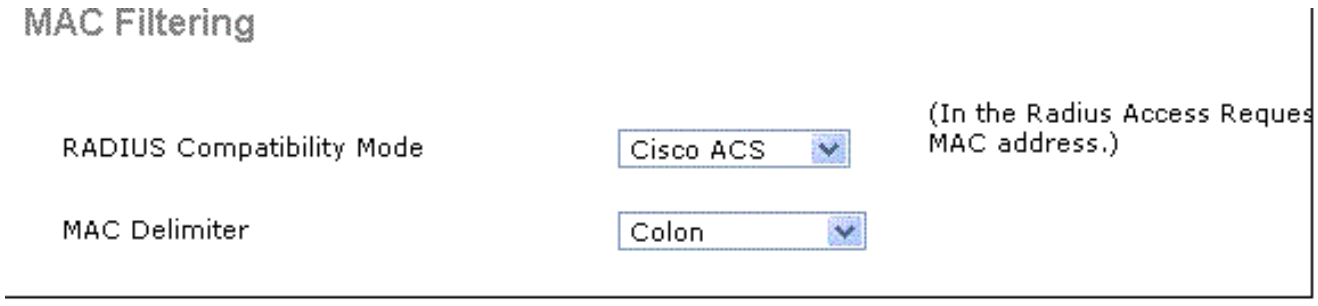


Parâmetros de Requisitos de Design

5. Clique em Security > MAC Filtering.
6. Na janela MAC Filtering (Filtragem MAC), escolha o tipo de servidor RADIUS em RADIUS Compatibility Mode (Modo de compatibilidade RADIUS).

   Este exemplo usa o Cisco ACS.
7. No menu suspenso Delimitador de MAC, escolha o delimitador de MAC.

   Este exemplo usa dois-pontos.
8. Clique em Apply.



Escolha o tipo de servidor RADIUS

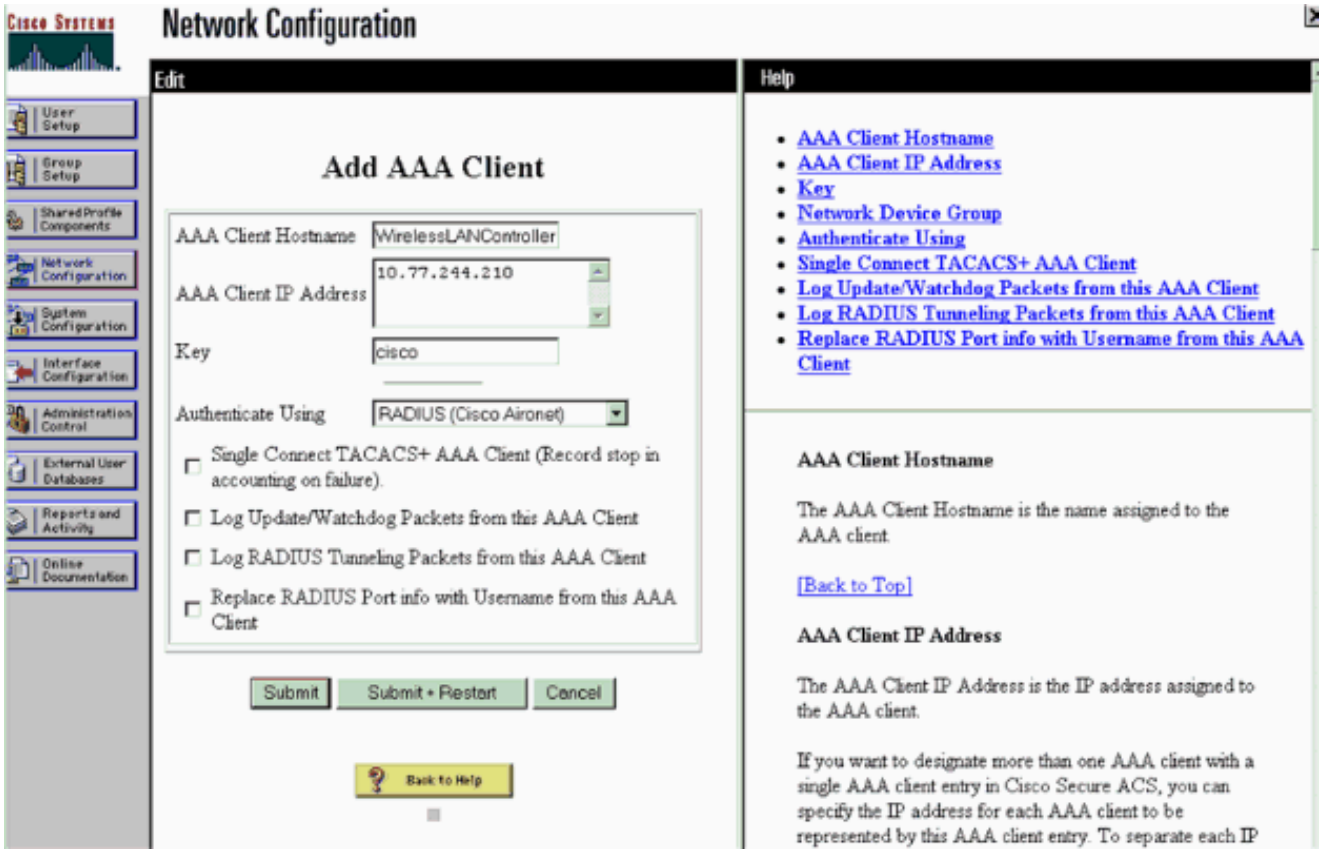
A próxima etapa é configurar o servidor ACS com os endereços MAC do cliente.

Configurar o servidor RADIUS com endereços MAC do cliente

Para adicionar um endereço MAC ao ACS:

1. Defina a WLC como um cliente AAA no servidor ACS. Clique em Network Configuration na GUI do ACS.
2. Quando a janela Network Configuration for exibida, defina o nome da WLC, o endereço IP, o segredo compartilhado e o método de autenticação (RADIUS Cisco Aironet ou RADIUS Airespace).

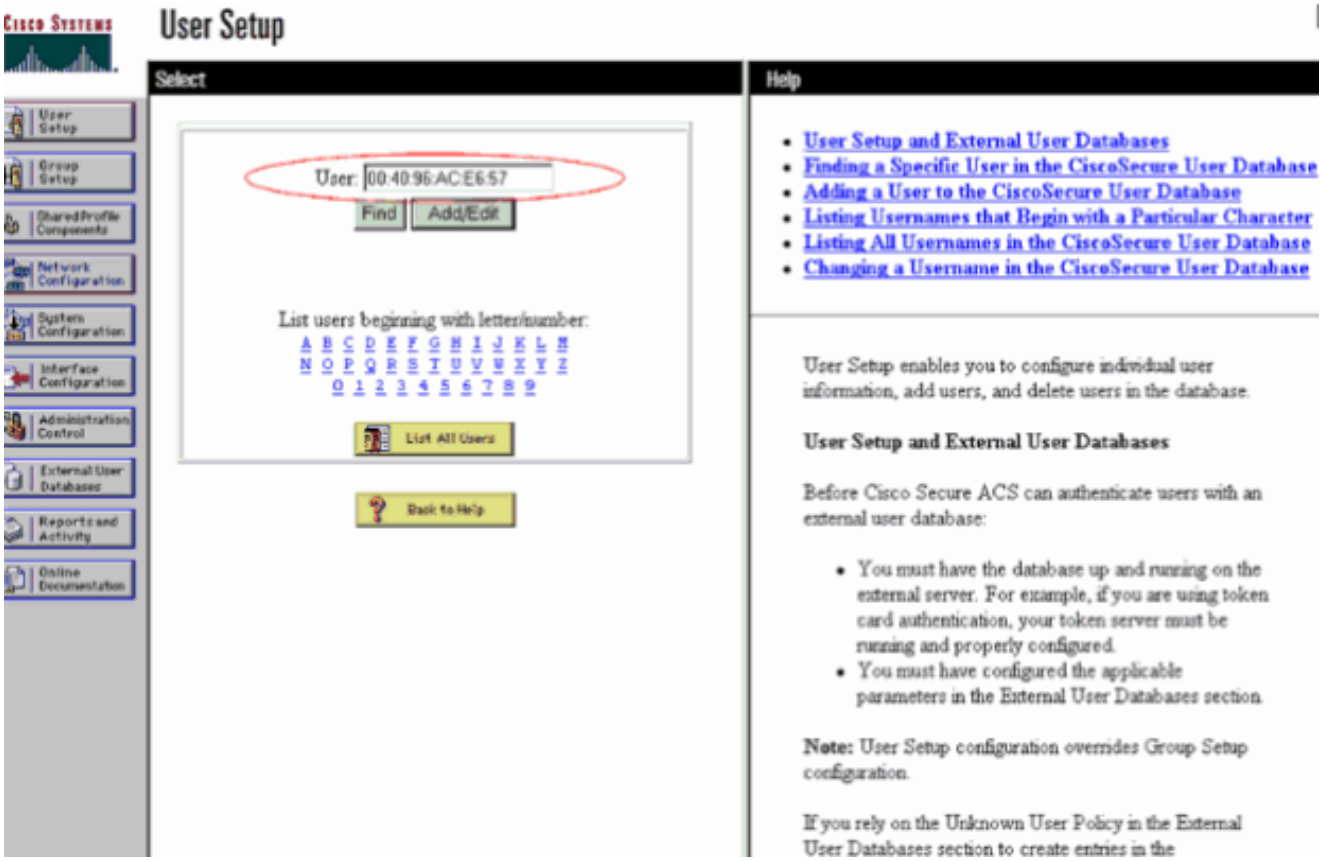
   Consulte a documentação do fabricante para outros servidores de autenticação não ACS.



Adicionar um cliente AAA

> Observação: a chave secreta compartilhada que você configura no WLC e o servidor ACS devem ser correspondentes. O segredo compartilhado diferencia maiúsculas de minúsculas.

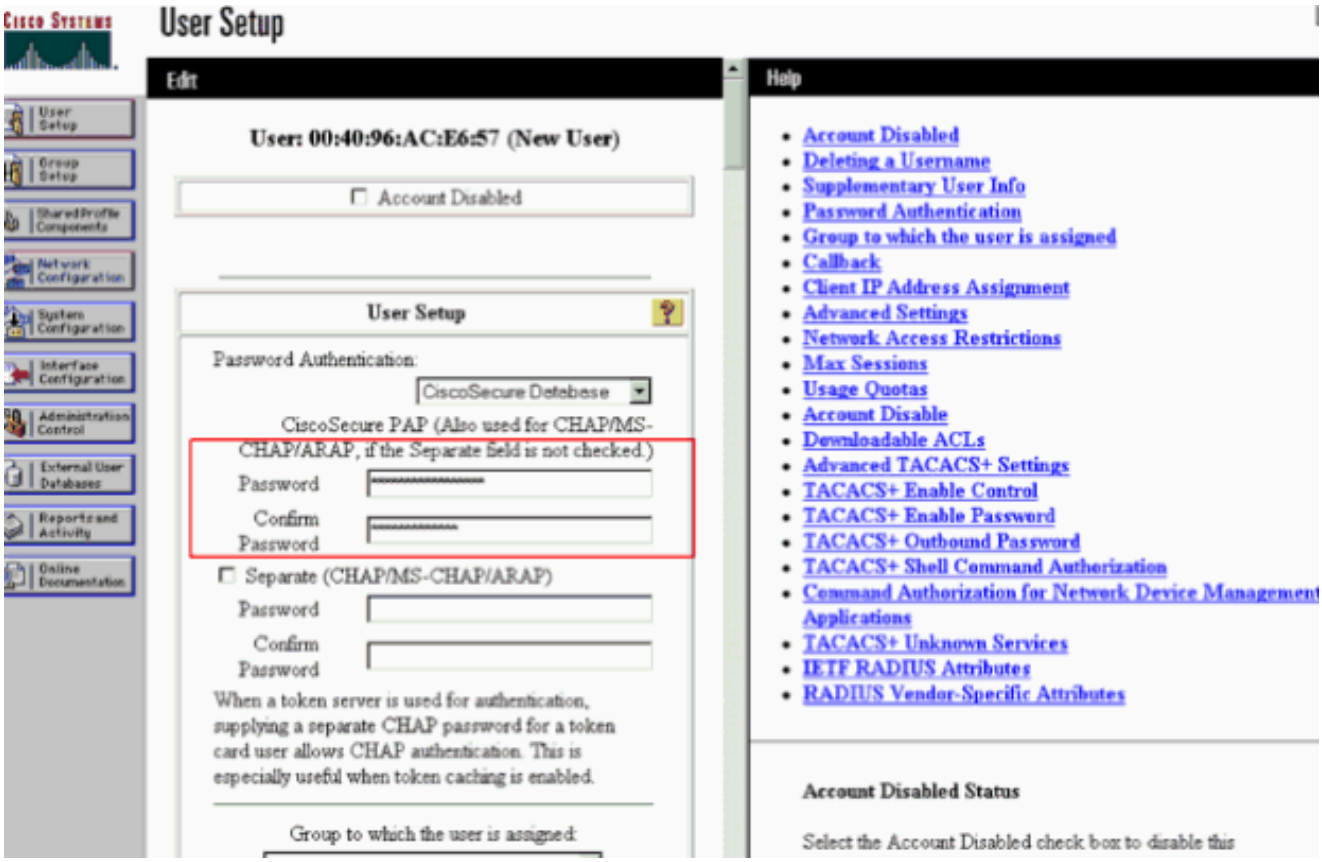
3. No menu principal do ACS, clique em User Setup .
4. Na caixa de texto User, insira o endereço MAC para adicionar ao banco de dados do usuário.



Insira o endereço MAC

Observação: o endereço MAC deve ser exatamente como é enviado pelo WLC para o nome de usuário e a senha. Se a autenticação falhar, verifique o registro de tentativas falhas para ver como o MAC é relatado pelo WLC. Não recorte e cole o endereço MAC, pois isso pode introduzir caracteres fantasmas.

5. Na janela User Setup, insira o endereço MAC na caixa de texto Secure-PAP password.



Insira o endereço MAC no campo Senha do Secure-PAP

> Observação: o endereço MAC deve ser exatamente como é enviado pelo WLC para o nome de usuário e a senha. Se a autenticação falhar, verifique o registro de tentativas falhas para ver como o MAC é relatado pelo AP. Não recorte e cole o endereço MAC, pois isso pode introduzir caracteres fantasmas.

6. Clique em Submit.
7. Repita as etapas de 2 a 5 para adicionar mais usuários ao banco de dados do ACS.

   Agora, quando os clientes se conectam a essa WLAN, a WLC passa as credenciais para o servidor ACS. O servidor ACS valida as credenciais em relação ao banco de dados ACS. Se o endereço MAC do cliente estiver presente no banco de dados, o servidor RADIUS ACS retornará um êxito de autenticação para a WLC e o cliente poderá receber acesso à WLAN.

Usar a CLI para configurar o filtro MAC no WLC

Este documento discutiu anteriormente como usar a GUI da WLC para configurar filtros MAC. Você também pode usar a CLI para configurar filtros MAC na WLC. Para configurar o filtro MAC no WLC:

- Execute o comando config wlan mac-filtering enable wlan_id para habilitar a filtragem MAC. Insira o comando show wlan para verificar se a filtragem MAC está habilitada para a WLAN.

- comando config macfilter add:

  O comando config macfilter add permite adicionar um macfilter, uma interface, uma descrição, etc.

  Use o comando config macfilter add para criar uma entrada de filtro MAC no controlador de LAN sem fio da Cisco. Use este comando para adicionar um cliente localmente a uma LAN sem fio no controlador de LAN sem fio da Cisco. Este filtro ignora o processo de autenticação RADIUS.

  <#root>

  ```
  config macfilter add
  <MAC_address> <WLAN_id> <Interface_name> <description> <IP_address>
  ```

  Exemplo

  Insira um mapeamento estático de endereço MAC para IP. Isso pode ser feito para suportar um cliente passivo, isto é, que não use DHCP e não transmita pacotes IP não solicitados.

  <#root>

  ```
  (Cisco Controller) >
  config macfilter add
  ```

  00:E0:77:31:A3:55 1 lab02 "labconnect" 10.92.125.51

- comando config macfilter ip-address

  O comando config macfilter ip-address permite mapear um filtro MAC para um endereço IP. Use este comando para configurar um endereço IP no banco de dados de filtros MAC local:

  <#root>

  ```
  config macfilter ip-address
  <MAC_address> <IP_address>
  ```

  Exemplo

  <#root>

```
(Cisco Controller) >
config macfilter ip-address


00:E0:77:31:A3:55 10.92.125.51
```

Configurar um tempo limite para clientes desativados

Você pode configurar um tempo limite para clientes desativados. Os clientes que não conseguirem autenticar três vezes durante as tentativas de associação são automaticamente desativados de outras tentativas de associação. Depois que o período de tempo limite expirar, o cliente poderá repetir a autenticação até associar ou falhar a autenticação e ser excluído novamente. Insira o comando config wlan exclusionlist wlan_id timeout para configurar o timeout para clientes desativados. O valor de tempo limite pode ser de 1 a 65535 segundos ou você pode digitar 0 para desativar permanentemente o cliente.

Verificar

Para verificar se o filtro MAC está configurado corretamente:

- show macfilter summary — Exibe um resumo de todas as entradas de filtros MAC.
- show macfilter detail < client MAC Address > — Exibição detalhada de uma entrada de filtro MAC.

Aqui está um exemplo do comando show macfilter summary:

```
<#root>
(Cisco Controller) >
show macfilter summary


MAC Filter RADIUS Compatibility mode..... Cisco ACS
MAC Filter Delimiter..................... None

Local Mac Filter Table

MAC Address               WLAN Id          Description
-----------------------   --------------   --------------------------------
00:40:96:ac:e6:57           1              Guest


(Cisco Controller) >
```

Aqui está um exemplo do comando show macfilter detail:

<#root>

```
(Cisco Controller) >
```

show macfilter detail 00:40:96:ac:e6:57

```
MAC Address..................................... 00:40:96:ac:e6:57
WLAN Identifier................................. 1
Interface Name.................................. mac-client
Description..................................... Guest
```

Troubleshooting

Você pode usar estes comandos para solucionar problemas de configuração:

Nota:Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos debug.

- debug aaa all enable — Fornece a depuração de todas as mensagens AAA.
- debug mac addr <Client-MAC-address xx:xx:xx:xx:xx:xx>—Para configurar a depuração MAC, use o comando debug maccommand.

Aqui está um exemplo do comando debug aaa all enable:

<#root>

```
Wed May 23 11:13:55 2007:
```

Looking up local blacklist 004096ace657

```
Wed May 23 11:13:55 2007: Looking up local blacklist 004096ace657
Wed May 23 11:13:55 2007:
```

User 004096ace657 authenticated

```
Wed May 23 11:13:55 2007: 00:40:96:ac:e6:57
```

Returning AAA Error 'Success' (0)
for mobile 00:40:96:ac:e6:57

```
Wed May 23 11:13:55 2007: AuthorizationResponse: 0xbadff97c
Wed May 23 11:13:55 2007:     structureSize...............................76
Wed May 23 11:13:55 2007:     resultCode..................................0
Wed May 23 11:13:55 2007:     protocolUsed................................0x00000008
Wed May 23 11:13:55 2007:     proxyState..................................
                                00:40:96:AC:E6:57-00:00
Wed May 23 11:13:55 2007:     Packet contains 2 AVPs:
Wed May 23 11:13:55 2007:         AVP[01] Service-Type.............................
                                  0x0000000a (10) (4 bytes)
Wed May 23 11:13:55 2007:         AVP[02] Airespace / Interface-Name..............
                                  staff-vlan (10 bytes)
Wed May 23 11:13:55 2007: 00:40:96:ac:e6:57 processing avps[0]: attribute 6
Wed May 23 11:13:55 2007: 00:40:96:ac:e6:57 processing avps[1]: attribute 5
Wed May 23 11:13:55 2007: 00:40:96:ac:e6:57 Applying new AAA override for
                          station 00:40:96:ac:e6:57
```

```
Wed May 23 11:13:55 2007: 00:40:96:ac:e6:57 Override values for station 00:40:96:ac:e6:57
source: 2, valid bits: 0x200 qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff,
sessionTimeout: -1    dataAvgC: -1, rTAvgC: -1, dataBurstC:

-1, rTimeBurstC: -1    vlanIfName: 'mac-client'
```

Quando um cliente sem fio não está presente no banco de dados de endereços MAC no WLC (banco de dados local) ou no servidor RADIUS tenta se associar à WLAN, esse cliente pode ser excluído. Aqui está um exemplo do comando debug aaa all enable para uma autenticação MAC malsucedida:

<#root>

```
Wed May 23 11:05:06 2007:

Unable to find requested user entry for 004096ace657

Wed May 23 11:05:06 2007: AuthenticationRequest: 0xa620e50
Wed May 23 11:05:06 2007:     Callback.....................................0x807e724
Wed May 23 11:05:06 2007:     protocolType.................................0x00000001
Wed May 23 11:05:06 2007:     proxyState...................................
                                00:40:96:AC:E6:57-00:00
Wed May 23 11:05:06 2007:     Packet contains 14 AVPs (not shown)
Wed May 23 11:05:06 2007: 00:40:96:ac:e6:57

Returning AAA Error 'No Server' (-7)
                          for mobile 00:40:96:ac:e6:57

Wed May 23 11:05:06 2007: AuthorizationResponse: 0xbadff7e4
Wed May 23 11:05:06 2007:     structureSize................................28
Wed May 23 11:05:06 2007:     resultCode...................................-7
Wed May 23 11:05:06 2007:     protocolUsed.................................0xffffffff
Wed May 23 11:05:06 2007:     proxyState...................................
                                00:40:96:AC:E6:57-00:00
Wed May 23 11:05:06 2007:     Packet contains 0 AVPs:
```

Erro: Os Clientes Sem Fio que Tentam Autenticar por Endereço MAC foram Rejeitados; o Relatório de Falha de Autenticação mostra Erros Internos

Quando você usa o ACS 4.1 em um servidor Microsoft Windows 2003 Enterprise, os clientes que tentam se autenticar pelo endereço MAC são rejeitados. Isso ocorre quando um cliente AAA envia o valor do atributo Service-Type=10 para o servidor AAA. Isso se deve ao bug da Cisco ID CSCsh62641. Os clientes AAA afetados por esse bug incluem WLCs e switches que usam o desvio de autenticação MAC.

As soluções são:

- Faça o downgrade para o ACS 4.0.

  or

- Adicione os endereços MAC a serem autenticados em uma NAP (Proteção de Acesso à

Rede) na tabela de endereços MAC do banco de dados do ACS interno.

Erro: não é possível adicionar um filtro MAC com a GUI da WLC

Isso pode acontecer devido à ID de bug da Cisco CSCsj98722. O bug foi corrigido na versão 4.2 do código. Se você executar versões anteriores à 4.2, poderá atualizar o firmware para a 4.2 ou usar essas duas soluções para esse problema.

- Use a CLI para configurar o filtro MAC com este comando:

```
<#root>

config macfilter add

 <MAC_address> <WLAN_id> <Interface_name>
```

- Na GUI da Web do controlador, escolha Any WLAN na guia Security e insira o endereço MAC a ser filtrado.

Erro: cliente silencioso não colocado em estado de execução

Se o DHCP exigido não estiver configurado no controlador, os APs aprendem o endereço IP dos clientes sem fio quando os clientes sem fio enviam o primeiro pacote IP ou ARP. Se os clientes sem fio forem dispositivos passivos, por exemplo, dispositivos que não iniciam uma comunicação, os APs falharão ao aprender o endereço IP dos dispositivos sem fio. Como resultado, o controlador aguarda dez segundos para que o cliente envie um pacote IP. Se não houver resposta do pacote do cliente, o controlador descartará todos os pacotes para os clientes sem fio passivos. Esse problema está documentado na ID de bug da Cisco CSCsq46427.

Observação: somente usuários registrados da Cisco podem acessar ferramentas e informações internas.

Como uma solução alternativa recomendada para dispositivos passivos como impressoras, bombas PLC sem fio e assim por diante, você precisa definir a WLAN para filtragem MAC e ter o AAA override verificado para permitir que esses dispositivos sejam conectados.

Um filtro de endereço MAC pode ser criado no controlador que mapeia o endereço MAC do dispositivo sem fio para um endereço IP.

Observação: isso exige que a filtragem de endereços MAC seja habilitada na configuração de WLAN para Segurança de Camada 2. Também exige que `Allow AAA Override` esteja habilitado nas configurações avançadas da configuração da WLAN.

Na CLI, insira este comando para criar o filtro de endereço MAC:

```
config macfilter add <STA MAC addr> <WLAN_id> <Interface_name> <description> <STA IP address>
```

Aqui está um exemplo:

<#root>

```
(Cisco Controller) >
```

config macfilter add 00:01:02:03:04:05 1 my_interface "Zebra Printer" 192.168.1.1

Informações Relacionadas

- Exemplo de configuração de ACLs nos Wireless LAN Controllers
- Exemplos de Configuração de Autenticação em Controladores Wireless LAN
- VLANs no exemplo de configuração de Wireless LAN Controllers
- Guia de configuração do Cisco Wireless LAN Controller, Aviso de desativação da versão 4.1
- Página de suporte à tecnologia sem fio
- Suporte técnico e downloads da Cisco

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.