

# Filtros MAC com exemplo de configuração dos controladores do Wireless LAN (WLC)

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Filtro do MAC address \(autenticação de MAC\) em WLC](#)

[Configurar a autenticação do MAC local em WLC](#)

[Configurar um WLAN e permita a filtração MAC](#)

[Configurar o base de dados local no WLC com endereços MAC de cliente](#)

[Configurar a autenticação de MAC usando um servidor Radius](#)

[Configurar um WLAN e permita a filtração MAC](#)

[Configurar o servidor Radius com endereços MAC de cliente](#)

[Use o CLI para configurar o filtro MAC no WLC](#)

[Configurar um intervalo para clientes deficientes](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

## [Introdução](#)

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

## [Pré-requisitos](#)

### [Requisitos](#)

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

- Conhecimento básico da configuração dos LAPs e dos WLCs da Cisco
- Conhecimento básico de soluções da Segurança do Cisco Unified Wireless

### [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
- Regaços do Cisco 1230AG Series
- adaptador de cliente Wireless do a/b/g do 802.11 com firmware 4.4
- Versão 4.4 do utilitário de Desktop de Aironet (ADU)

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 sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

## Convenções

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos.

## Filtro do MAC address (autenticação de MAC) em WLC

Quando você cria um filtro do MAC address em WLC, os usuários estão concedidos ou o acesso negado à rede de WLAN é baseado no MAC address do cliente que se usam.

Há dois tipos de autenticação de MAC que são apoiados em WLC:

- Autenticação do MAC local
- Autenticação de MAC usando um servidor Radius

Com autenticação do MAC local, os endereços do usuário MAC são armazenados em um base de dados no WLC. Quando um usuário tenta alcançar o WLAN que está configurado para o MAC que filtra, o endereço MAC de cliente é validado contra o base de dados local no WLC, e o cliente está concedido o acesso ao WLAN se a autenticação é bem sucedida.

À revelia, os apoios de base de dados local WLC até 512 entradas de usuário.

A base de dados de usuário local é limitada a um máximo de 2048 entradas. O base de dados local armazena entradas para estes artigos:

- Usuários do gerenciamento local, que inclui embaixadores da entrada
- Usuários da rede local, que inclui usuários convidado
- Entradas do filtro MAC
- Entradas de lista da exclusão
- Entradas de lista da autorização do Access point

Junto, todos estes tipos de usuários não podem exceder o tamanho de base de dados configurado.

A fim aumentar o base de dados local, use este comando do CLI:

```
<Cisco Controller>config database size ? <count> Enter the maximum number of entries (512-2048)
```

Alternativamente, a autenticação do MAC address pode igualmente ser executada usando um servidor Radius. A única diferença é que o base de dados do MAC address dos usuários está armazenado no servidor Radius em vez do WLC. Quando uma base de dados de usuário for armazenada em um servidor Radius o WLC para a frente o MAC address do cliente ao servidor Radius para a validação do cliente. Então, o servidor Radius valida o MAC address baseado no base de dados que tem. Se a autenticação do cliente é bem sucedida, o cliente está concedido o

acesso ao WLAN. Todo o servidor Radius que apoiar a autenticação do MAC address pode ser usado.

## [Configurar a autenticação do MAC local em WLC](#)

Termine estas etapas a fim configurar a autenticação do MAC local nos WLC:

1. [Configurar um WLAN e permita a filtração MAC](#)
2. [Configurar o base de dados local no WLC com endereços MAC de cliente](#)**Nota:** Antes que você configure a autenticação de MAC, você deve configurar o WLC para a operação básica e registrar os regaços ao WLC. Este documento supõe que o WLC está configurado já para a operação básica e que os regaços estão registrados ao 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 \(Wireless LAN Controller\)](#).**Nota:** Não há nenhuma configuração especial necessária no cliente Wireless a fim apoiar a autenticação de MAC.

## [Configurar um WLAN e permita a filtração MAC](#)

Termine estas etapas a fim configurar um WLAN com filtração MAC:

1. Clique **WLAN** do controlador GUI a fim criar um WLAN.A janela WLANs aparece. Este indicador alista os WLAN configurados no controlador.
2. Clique **novo** a fim configurar um WLAN novo.Neste exemplo, o WLAN é nomeado *MAC-WLAN* e o ID de WLAN é 1.

WLANs > New

Type	WLAN
Profile Name	MAC-WLAN
SSID	MAC-WLAN
ID	1

3. Clique em Apply.
4. No o WLAN > edita o indicador, define os parâmetros específicos ao WLAN.

## WLANs > Edit

The screenshot shows the 'WLANs > Edit' configuration page. The 'Security' tab is selected, and the 'Layer 2' sub-tab is active. A red box highlights the 'Layer 2 Security' dropdown menu, which is set to 'None', and the 'MAC Filtering' checkbox, which is checked.

Sob políticas de segurança > Segurança da camada 2, verifique a caixa de verificação de **filtração MAC**. Isto permite a autenticação de MAC para o WLAN. Sob políticas gerais > nome da relação, selecione a relação a que o WLAN é traçado. Neste exemplo, o WLAN é traçado à interface de gerenciamento. Selecione os outros parâmetros, que dependem dos requisitos de projeto do WLAN. Clique em Apply.

## WLANs > Edit

The screenshot shows the 'WLANs > Edit' configuration page. The 'Security' tab is selected. The 'General' sub-tab is active. A red box highlights the 'Status' checkbox, which is checked and labeled 'Enabled', and the 'Security Policies' dropdown menu, which is set to 'MAC Filtering'. Below this, a note states: '(Modifications done under security tab will appear after applying the)'. Another red box highlights the 'Interface' dropdown menu, which is set to 'management'. Other visible settings include 'Profile Name' (MAC-WLAN), 'Type' (WLAN), 'SSID' (MAC-WLAN), 'Radio Policy' (All), and 'Broadcast SSID' (Enabled).

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

Refira [VLAN no exemplo de configuração dos controladores do Wireless LAN](#) para obter informações sobre de como configurar as interfaces dinâmica (VLAN) em WLC.

[Configurar o base de dados local no WLC com endereços MAC de cliente](#)

Termine estas etapas a fim configurar o base de dados local com um endereço MAC de cliente no WLC:

1. Clique a **Segurança** do controlador GUI, e clique então o **MAC que filtra** do menu do lado esquerdo. O indicador de filtração MAC aparece.

## MAC Filtering

RADIUS Compatibility Mode

Cisco ACS

(In the Radius Access Request MAC address.)

MAC Delimiter

No Delimiter

## Local MAC Filters

MAC Address	Profile Name	Interface	Description
-------------	--------------	-----------	-------------

2. Clique **novo** a fim criar uma entrada de endereço MAC do base de dados local no WLC.
3. No MAC filtra > nova janela, dão entrada com o MAC address, o nome de perfil, a descrição e o nome da relação para o cliente. Aqui está um exemplo:

### MAC Filters > New

MAC Address: 00:0b:85:7f:47:00

Profile Name: MAC-WLAN

Description: User1

Interface Name: management

4. Clique em Apply.
5. Repita etapas 2-4 a fim adicionar mais clientes ao base de dados local. Agora, quando os clientes conectam a este WLAN, o WLC valida o MAC address dos clientes contra o base de dados local e se a validação é bem sucedida, o cliente é concedido o acesso à rede. **Nota:** Neste exemplo, somente um filtro do MAC address sem qualquer outro mecanismo de segurança da camada 2 foi usado. Cisco recomenda que a autenticação do MAC address deve ser usada junto com outros métodos de segurança da camada 2 ou da camada 3. Não é aconselhável usar somente a autenticação do MAC address para fixar sua rede de WLAN porque não fornece um mecanismo de forte segurança.

## [Configurar a autenticação de MAC usando um servidor Radius](#)

Termine estas etapas a fim configurar a autenticação de MAC usando um servidor Radius. Neste exemplo, o server do Cisco Secure ACS é usado como o servidor Radius.

1. [Configurar um WLAN e permita a filtração MAC](#)
2. [Configurar o servidor Radius com endereços MAC de cliente](#)

### [Configurar um WLAN e permita a filtração MAC](#)

Termine estas etapas a fim configurar um WLAN com filtração MAC:

1. Clique **WLAN** do controlador GUI a fim criar um WLAN. A janela WLANs aparece. Este indicador alista os WLAN configurados no controlador.
2. Clique **novo** a fim configurar um WLAN novo. Neste exemplo, o WLAN é nomeado *MAC-ACS-WLAN* e o ID de WLAN é

2.

WLANs > New

Type	WLAN
Profile Name	MAC-ACS-WLAN
SSID	MAC-ACS-WLAN
ID	2

3. Clique em Apply.
4. No o WLAN > edita o indicador, define os parâmetros específicos ao WLAN. Sob políticas de segurança > Segurança da camada 2, verifique a caixa de verificação de **filtração MAC**. Isto permite a autenticação de MAC para o WLAN. Sob políticas gerais > nome da relação, selecione a relação a que o WLAN é traçado. Sob servidores Radius, selecione o servidor Radius que será usado para a autenticação de MAC.

## WLANs > Edit

**General** **Security** **QoS** **Advanced**

**Layer 2** **Layer 3** **AAA Servers**

Select AAA servers below to override use of default servers on this WLAN

**Radius Servers**

	Authentication Servers	Accounting Servers
Server 1	IP:10.77.244.196, Port:1812	<input checked="" type="checkbox"/> Enabled None
Server 2	None	None
Server 3	None	None

**Nota:** Antes que você possa selecionar o servidor Radius do WLAN > edite o indicador, você deve definir o servidor Radius no indicador da Segurança > da autenticação RADIUS e permitir o servidor Radius.

### RADIUS Authentication Servers

Call Station ID Type

Use AES Key Wrap  (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

Network User	Management	Server Index	Server Address	Port	IPSec	Admin Status
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">1</a>	10.77.244.196	1812	Enabled	Enabled <input checked="" type="checkbox"/>

Selecione os outros parâmetros, que dependem dos requisitos de projeto do WLAN. Clique em Apply.

## WLANs > Edit

The screenshot shows the 'Security' tab of the WLAN configuration interface. The 'Status' is checked and set to 'Enabled'. Under 'Security Policies', 'MAC Filtering' is selected, with a note that modifications will appear after applying. Other settings include 'Radio Policy' set to 'All', 'Interface' set to 'management', and 'Broadcast SSID' checked and 'Enabled'.

General	Security	QoS	Advanced
Profile Name	MAC-ACS-WLAN		
Type	WLAN		
SSID	MAC-ACS-WLAN		
Status	<input checked="" type="checkbox"/> Enabled		
Security Policies	<b>MAC Filtering</b> (Modifications done under security tab will appear after applying the)		
Radio Policy	All		
Interface	management		
Broadcast SSID	<input checked="" type="checkbox"/> Enabled		

### 5. Segurança do clique > filtração MAC.

6. No indicador de filtração MAC, escolha o tipo de servidor Radius sob o modo de compatibilidade do RAIO. Este exemplo usa Cisco ACS.

7. Do delimitador MAC puxe para baixo o menu, escolhem o delimitador MAC. Este exemplo usa dois pontos.

8. Clique em

Apply.

### MAC Filtering

The screenshot shows the 'MAC Filtering' configuration interface. 'RADIUS Compatibility Mode' is set to 'Cisco ACS' and 'MAC Delimiter' is set to 'Colon'. A note indicates that in the Radius Access Request, the MAC address should be used.

RADIUS Compatibility Mode	Cisco ACS	(In the Radius Access Request MAC address.)
MAC Delimiter	Colon	

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

## [Configurar o servidor Radius com endereços MAC de cliente](#)

Termine estas etapas a fim adicionar um MAC address ao ACS:

1. Defina o WLC como um cliente de AAA no servidor ACS. Clique a **configuração de rede do ACS GUI**.
2. Quando o indicador da configuração de rede aparece, defina o nome do WLC, do endereço IP de Um ou Mais Servidores Cisco ICM NT, do segredo compartilhado e do método de autenticação (Cisco Aironet do RAIO ou RAIO Airespace). Refira a documentação do



fabricante para outros Authentication Server NON-ACS.

The screenshot shows the 'Network Configuration' page in Cisco Secure ACS. The main content area is titled 'Add AAA Client' and contains a form with the following fields and options:

- AAA Client Hostname: WirelessLANController
- AAA Client IP Address: 10.77.244.210
- Key: cisco
- Authenticate Using: RADIUS (Cisco Aironet)
- Single Connect TACACS+ AAA Client (Record stop in accounting on failure):
- Log Update/Watchdog Packets from this AAA Client:
- Log RADIUS Tunneling Packets from this AAA Client:
- Replace RADIUS Port info with Username from this AAA Client:

Buttons at the bottom include 'Submit', 'Submit + Restart', 'Cancel', and 'Back to Help'.

The right-hand 'Help' pane contains the following links:

- AAA Client Hostname
- AAA Client IP Address
- Key
- Network Device Group
- Authenticate Using
- Single Connect TACACS+ AAA Client
- Log Update/Watchdog Packets from this AAA Client
- Log RADIUS Tunneling Packets from this AAA Client
- Replace RADIUS Port info with Username from this AAA Client

The 'AAA Client Hostname' help text states: 'The AAA Client Hostname is the name assigned to the AAA client.' It includes a '[Back to Top]' link.

The 'AAA Client IP Address' help text states: 'The AAA Client IP Address is the IP address assigned to the AAA client.' It also includes a note: 'If you want to designate more than one AAA client with a single AAA client entry in Cisco Secure ACS, you can specify the IP address for each AAA client to be represented by this AAA client entry. To separate each IP'.

**Nota:** A chave secreta compartilhada que você configura no WLC e no servidor ACS deve combinar. O segredo compartilhado é diferenciando maiúsculas e minúsculas.

3. Do menu principal ACS, **instalação de usuário** do clique.
4. Na caixa de texto do usuário, incorpore o MAC address a fim adicionar à base de dados de usuário.

The screenshot shows the 'User Setup' page in Cisco Secure ACS. The main content area is titled 'Select' and contains a search form with the following elements:

- User: 00:40:96:ACE6:57 (circled in red)
- Buttons: 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
- Buttons: List All Users, Back to Help

The right-hand 'Help' pane contains the following links:

- User Setup and External User Databases
- Finding a Specific User in the CiscoSecure User Database
- Adding a User to the CiscoSecure User Database
- Listing Usernames that Begin with a Particular Character
- Listing All Usernames in the CiscoSecure User Database
- Changing a Username in the CiscoSecure User Database

The 'User Setup' help text states: 'User Setup enables you to configure individual user information, add users, and delete users in the database.'

The 'User Setup and External User Databases' help text states: 'Before Cisco Secure 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

**Nota:** O MAC address deve ser exatamente enquanto é enviado pelo WLC para o username e a senha. Se a autenticação falha, verifique o log das falhas de tentativa para ver como o MAC é relatado pelo WLC. Não cortare-col o MAC address, como isto pode introduzir caracteres fantasmas.

5. No indicador da instalação de usuário, incorpore o MAC address à caixa de texto da senha Seguro-PAP.

The screenshot shows the Cisco User Setup interface. The main window is titled 'User Setup' and displays the user '00:40:96:AC:E6:57 (New User)'. There is a checkbox for 'Account Disabled'. Below this, the 'User Setup' section is highlighted with a red box. It contains the following fields and options:

- Password Authentication:** A dropdown menu set to 'CiscoSecure Database'.
- CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)**
- Password:** A text input field.
- Confirm Password:** A text input field.
- Separate (CHAP/MS-CHAP/ARAP)**
- Password:** A text input field.
- Confirm Password:** A text input field.

Below the 'Separate' section, there is a note: '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.'

At the bottom, there is a field for 'Group to which the user is assigned:'.

On the right side, there is a 'Help' sidebar with a list of links:

- 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

At the bottom of the sidebar, there is a section titled 'Account Disabled Status' with the text: 'Select the Account Disabled check box to disable this'.

**Nota:** O MAC address deve ser exatamente enquanto é enviado pelo WLC para o username e a senha. Se a autenticação falha, verifique o log das falhas de tentativa para ver como o MAC é relatado pelo AP. Não cortare-col o MAC address, como isto pode introduzir caracteres fantasmas.

6. Clique em Submit.
7. Repita etapas 2-5 a fim adicionar mais usuários ao base de dados ACS. Agora, quando os clientes conectam a este WLAN, o WLC passa as credenciais ao servidor ACS. O servidor ACS valida as credenciais contra o base de dados ACS. Se o endereço MAC de cliente esta presente no base de dados, o servidor Radius ACS retorna um sucesso de autenticação ao WLC e o cliente será concedido o acesso ao WLAN.

## [Use o CLI para configurar o filtro MAC no WLC](#)

Este documento discutido previamente como usar o WLC GUI para configurar filtros MAC. Você pode igualmente usar o CLI a fim configurar filtros MAC no WLC. Você pode usar estes comandos a fim configurar o filtro MAC no WLC:

- Emita a **configuração que a MAC-filtração wlan permite** o comando do **wlan\_id** a fim permitir a filtração MAC. o bEnter o comando **wlan da mostra** a fim verificar que você tem a filtração MAC permitiu para o WLAN.
- comando **add do macfilter da configuração:** O comando **add do macfilter da configuração**

deixa-o adicionar um macfilter, relação, descrição, e assim por diante. Use o **comando add do macfilter da configuração** a fim criar uma entrada do filtro MAC no controlador de LAN do Cisco Wireless. Use este comando a fim adicionar localmente um cliente a um Wireless LAN no controlador de LAN do Cisco Wireless. Este filtro contorneia o processo de autenticação RADIUS.

```
config macfilter add MAC_address wlan_id [interface_name] [description] [IP address]
```

**Exemplo:** Incorpore um mapeamento de endereço MAC-à-IP estático. Isto pode ser feito para apoiar um *cliente passivo*, isto é, um que não usa o DHCP e não transmite pacotes IP espontâneos. >config macfilter add 00:E0:77:31:A3:55 1 lab02 "labconnect" 10.92.125.51

- **comando ip-address do macfilter da configuração** O comando **ip-address do macfilter da configuração** deixa-o traçar um MAC-filtro existente a um endereço IP de Um ou Mais Servidores Cisco ICM NT. Use este comando a fim configurar um endereço IP de Um ou Mais Servidores Cisco ICM NT no base de dados do filtro do MAC local:

```
config macfilter ip-address MAC_address IP address Exemplo: >config macfilter add 00:E0:77:31:A3:55 1 lab02 "labconnect" 10.92.125.51
```

## Configurar um intervalo para clientes deficientes

Você pode configurar um intervalo para clientes deficientes. Os clientes que não autenticam três vezes durante tentativas de associar são desabilitados automaticamente de umas tentativas mais adicionais da associação. Após o período de timeout expira, é permitido experimentar de novo a autenticação até que associe ou falhe a autenticação e excluído ao cliente outra vez.

Inscreva o **comando timeout wlan do wlan\_id do exclusionlist da configuração** a fim configurar o intervalo para clientes deficientes. O valor de timeout pode ser 1 a 65535 segundos, ou você pode incorporar 0 a fim desabilitar permanentemente o cliente.

## Verificar

Use estes comandos a fim verificar se o filtro MAC é configurado corretamente:

A [Output Interpreter Tool \(apenas para clientes registrados\)](#) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

- **mostre o sumário do macfilter** — Indica um sumário de todas as entradas do filtro MAC.
- **mostre a detalhe do macfilter o MAC address <client >** — Indicador detalhado de uma entrada do filtro MAC.

Está aqui um exemplo do **comando summary do macfilter da mostra:**

```
(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) >show macfilter detail 00:40:96:ac:e6:57
```

Está aqui um exemplo do **comando detail do macfilter da mostra:**

```
(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 pesquisar defeitos sua configuração:

**Nota:** Consulte [Informações Importantes sobre Comandos de Depuração](#) antes de usar comandos **debug**.

- **debugar o aaa que todos permitem** — Fornece a eliminação de erros de todos os mensagens AAA.
- **debugar o <Client-MAC-endereço xx do ADDR do Mac: xx: xx: xx: xx: xx >** — A fim configurar a eliminação de erros MAC, use o comando **mac debugar**.

Está aqui um exemplo do comando **debug aaa all enable**:

```
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 Wireless não está atual no base de dados do MAC address no WLC (base de dados local) ou no servidor Radius tenta associar ao WLAN, esse cliente será excluído. Está aqui um exemplo do comando **debug aaa all enable** para uma autenticação de MAC mal sucedida:

```
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:
```

**Os clientes Wireless que tentam autenticar pelo MAC address são rejeitados; O relatório da autenticação falha mostra erros internos**

Quando você usa o ACS 4.1 que é executado em um servidor de empreendimento de Microsoft Windows 2003, os clientes que tentam autenticar pelo MAC address são rejeitados. Isto ocorre quando um cliente de AAA envia o valor de atributo Service-Type=10 ao servidor AAA. Isto é devido à identificação de bug Cisco [CSCsh62641 \(clientes registrados somente\)](#). Os clientes de AAA afetados por este erro incluem os WLC e o Switches que usam o desvio da autenticação de MAC.

As soluções são:

- Degrade a ACS 4.0.ou
- Adicionar os endereços MAC a ser autenticados a uma proteção do acesso de rede (SESTA) sob a tabela de endereços MAC interna ACS DB.

### Não capaz de adicionar um filtro MAC usando o WLC GUI

Isto pode acontecer becaue da identificação de bug Cisco [CSCsj98722](#) ([clientes registrados somente](#)). O erro é fixado na liberação 4.2 do código. Se você é versões running mais cedo de 4.2, você pode promover o firmware a 4.2 ou para usar estas duas ações alternativas para esta edição.

- Use o CLI a fim configurar o filtro MAC com este comando:  
`config macfilter add <MAC address> <WLAN ID#> <Interface>`
- Da Web GUI do controlador, escolha **todo o WLAN** sob a ABA de segurança e incorpore o MAC address a ser filtrado.

### Cliente silencioso não colocado no estado de corrida

Se o DHCP exigido não é configurado no controlador, os AP aprendem o endereço IP de Um ou Mais Servidores Cisco ICM NT dos clientes Wireless quando os clientes Wireless mandam o primeiro pacote IP ou ARP. Se os clientes Wireless são dispositivos passivos, por exemplo, os dispositivos que não iniciam uma comunicação, a seguir os AP não aprendem o endereço IP de Um ou Mais Servidores Cisco ICM NT dos dispositivos Wireless. Em consequência, o controlador espera dez segundos pelo cliente para enviar um pacote IP. Se não há nenhuma resposta do pacote do cliente, então o controlador deixa cair todos os pacotes aos clientes Wireless passivos. Esta edição é documentada na identificação de bug Cisco [CSCsq46427](#) (o [clientes registrados somente](#))

Enquanto uma solução recomendada para dispositivos passivos como impressoras, PLC wireless bombeia e assim por diante, você precisa de ajustar o WLAN para o MAC que filtra e de ter a ultrapassagem AAA verificada a fim permitir que estes dispositivos estejam conectados.

Um filtro do MAC address pode ser criado no controlador que traça o MAC address do dispositivo Wireless a um endereço IP de Um ou Mais Servidores Cisco ICM NT.

**Nota:** Isto exige o MAC address que filtra para ser permitido na configuração WLAN para a Segurança da camada 2. Iguamente exige `permite` que o AAA Override seja permitido nos ajustes avançados da configuração WLAN.

Do CLI, incorpore este comando a fim criar o filtro do MAC address:

```
config macfilter add <STA MAC addr> <WLAN id> [interface name] [description] [STA IP address]
```

Aqui está um exemplo:

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

## [Informações Relacionadas](#)

- [ACL no exemplo da configuração de controle do Wireless LAN](#)
- [Autenticação em exemplos de configuração dos controladores do Wireless LAN](#)
- [VLAN no exemplo de configuração dos controladores do Wireless LAN](#)
- [Guia de configuração do Cisco Wireless LAN Controller, versão 4.1](#)
- [Página de suporte da tecnologia Wireless](#)

- [Suporte Técnico e Documentação - Cisco Systems](#)