

使用无线局域网控制器(WLC)配置MAC过滤器

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[背景信息](#)

[WLC 上的 MAC 地址过滤器 \(MAC 身份验证 \)](#)

[在 WLC 上配置本地 MAC 身份验证](#)

[配置 WLAN 并启用 MAC 过滤](#)

[使用客户端 MAC 地址在 WLC 上配置本地数据库](#)

[使用RADIUS服务器配置MAC身份验证](#)

[配置 WLAN 并启用 MAC 过滤](#)

[使用客户端 MAC 地址配置 RADIUS 服务器](#)

[使用 CLI 在 WLC 上配置 MAC 过滤器](#)

[为已禁用客户端配置超时](#)

[验证](#)

[故障排除](#)

[相关信息](#)

简介

本文档介绍如何使用无线LAN控制器(WLC)配置MAC过滤器。

先决条件

要求

Cisco 建议您了解以下主题：

- LAP和Cisco WLC的配置
- 思科统一无线安全解决方案

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行软件版本 5.2.178.0 的 Cisco 4400 WLC
- Cisco 1230AG 系列 LAP
- 具有固件 4.4 的 802.11 a/b/g 无线客户端适配器
- Aironet Desktop Utility (ADU) 版本 4.4

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

本文档通过配置示例介绍如何使用无线局域网控制器(WLC)配置MAC过滤器。本文档还讨论如何根据 AAA 服务器授权轻量接入点 (LAP)。

WLC 上的 MAC 地址过滤器（MAC 身份验证）

在 WLC 上创建 MAC 地址过滤器时，将根据用户所使用的客户端的 MAC 地址允许或拒绝他们访问 WLAN 网络。

WLC 上支持两种类型的 MAC 身份验证：

- 本地 MAC 身份验证
- RADIUS服务器使用的MAC身份验证

使用本地 MAC 身份验证，用户 MAC 地址存储在 WLC 上的数据库中。当用户尝试访问为 MAC 过滤配置的 WLAN 时，将根据 WLC 上的本地数据库对客户端 MAC 地址进行验证，如果身份验证成功，则授权该客户端访问 WLAN。

默认情况下，WLC 本地数据最多支持 512 个用户条目。

本地用户数据库限制为最多2048个条目。本地数据库存储下列项的条目：

- 本地管理用户，包括接待大使
- 本地网络用户，包括访客用户
- MAC过滤器条目
- 排除列表条目
- 接入点授权列表条目

所有这些类型的用户都不能超过配置的数据库大小。

要增加本地数据库，请从CLI使用以下命令：

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

或者，也可以使用RADIUS服务器执行MAC地址身份验证。唯一的不同之处是，用户 MAC 地址数据库存储在 RADIUS 服务器而不是 WLC 中。当用户数据库存储在 RADIUS 服务器中时，WLC 将客户端 MAC 地址转发到 RADIUS 服务器进行客户端验证。然后，RADIUS 服务器根据它所拥有的数据库验证 MAC 地址。如果客户端身份验证成功，则授予该客户端访问 WLAN 的权限。可以使用支持 MAC 地址身份验证的任何 RADIUS 服务器。

在 WLC 上配置本地 MAC 身份验证

要在WLC上配置本地MAC身份验证，请执行以下操作：

1. [配置WLAN并启用MAC过滤](#)。
2. [在WLC上使用客户端MAC地址配置本地数据库](#)。注意：在配置MAC身份验证之前，必须配置WLC进行基本操作并将LAP注册到WLC。本文档假设已针对基本操作配置了WLC且LAP已注册到WLC中。如果您是新用户，并且希望尝试设置WLC以便使用LAP执行基本操作，请参阅[排除无法加入WLC的轻量AP故障](#)。注意：无线客户端不需要特殊配置即可支持MAC身份验证。

配置 WLAN 并启用 MAC 过滤

要配置具有MAC过滤功能的WLAN，请执行以下操作：

1. 要创建 WLAN，请从控制器 GUI 中单击 WLANs。随即显示 WLAN 窗口。该窗口列出了控制器中配置的 WLAN。
2. 要配置新的 WLAN，请单击 New。在本示例中，WLAN 命名为 *MAC-WLAN* 且 WLAN ID 为 1。

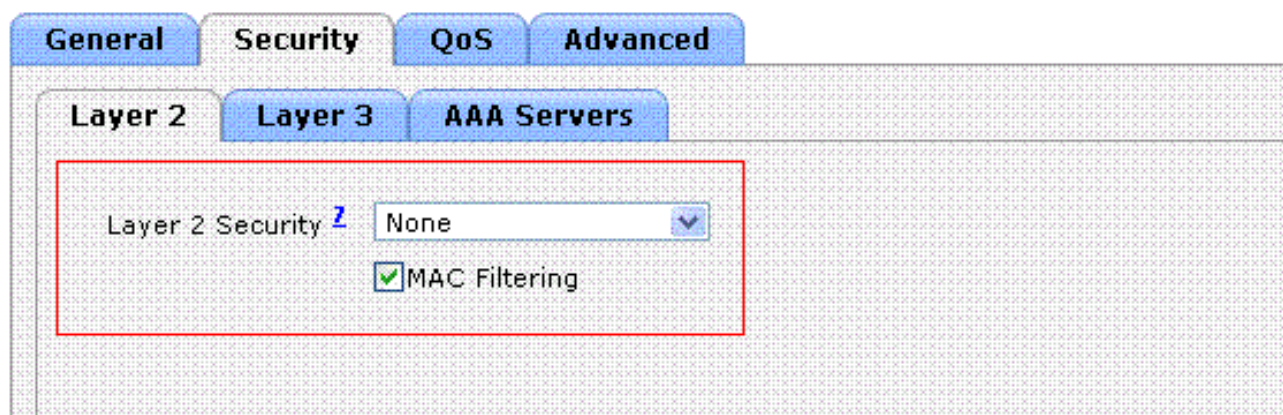
WLANs > New

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

配置WLAN启用MAC过滤

3. 单击 Apply。
4. 在“WLANs > Edit”窗口中，定义特定于该 WLAN 的参数。

WLANs > Edit



The screenshot shows the 'WLANs > Edit' configuration window. The 'Security' tab is selected, and within it, the 'Layer 2' sub-tab is active. Under 'Layer 2 Security Policies', the 'Layer 2 Security' dropdown menu is set to 'None'. Below this, the 'MAC Filtering' checkbox is checked. A red rectangular box highlights the 'Layer 2 Security' dropdown and the 'MAC Filtering' checkbox.

定义参数

在**Security > Layer 2 > Layer 2 Security Policies**下，选中**MAC Filtering**复选框。这将为WLAN 启用 MAC 身份验证。在**General > Interface name**下，选择WLAN映射到的接口。在本例中，WLAN 被映射到管理接口。根据 WLAN 的设计要求选择其他参数。单击 Apply。

GeneralSecurityQoSAdvanced

Profile NameMAC-WLAN

TypeWLAN

SSIDMAC-WLAN

Status☒ Enabled

Security PoliciesMAC Filtering

Radio PolicyAll

Interfacemanagement

Broadcast SSID☒ Enabled

(Modifications done under security tab will appear after applying th

映射到接口的WLAN

下一步是使用客户端 MAC 地址在 WLC 上配置本地数据库。

有关如何在 WLC 上配置动态接口 (VLAN) 的详细信息，请参阅[无线 LAN 控制器上的 VLAN 配置示例](#)。

使用客户端 MAC 地址在 WLC 上配置本地数据库

要在WLC上使用客户端MAC地址配置本地数据库，请执行以下操作：

1. 在控制器 GUI 中单击 **Security**，然后单击左侧菜单中的 **MAC Filtering**。此时将显示 MAC Filtering 窗口。

MAC Filtering

RADIUS Compatibility ModeCisco ACS

MAC DelimiterNo Delimiter

(In the Radius Access Request packet, use the MAC address.)

Local MAC Filters

MAC Address	Profile Name	Interface	Description
MAC过滤窗口			

2. 单击 New 以在 WLC 上创建一个本地数据库 MAC 地址条目。
3. 在 MAC Filters > New 窗口中，输入客户端的 MAC 地址、配置文件名称、说明和接口名称。

示例如下

:

为MAC地址创建本地数据库

MAC Filters > New

MAC Address

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

Profile Name

MAC-WLAN

Description

User1

Interface Name

management

为MAC地址创建本地数据库

4. 单击 Apply。
5. 要向本地数据库中添加更多客户端，请重复步骤 2 到 4。现在，当客户端连接到此 WLAN 时，WLC 将根据本地数据库验证客户端 MAC 地址。如果验证成功，则授权该客户端访问网络。
注意：在本示例中，仅使用没有其他第2层安全机制的MAC地址过滤器。Cisco建议必须将MAC地址身份验证与其他第2层或第3层安全方法配合使用。不建议只使用 MAC 地址身份验证来保护您的 WLAN 网络，因为它不提供强有力的安全机制。

使用RADIUS服务器配置MAC身份验证

要使用RADIUS服务器配置MAC身份验证，请使用以下链路。在本示例中，使用 Cisco Secure ACS 服务器作为 RADIUS 服务器。

1. [配置 WLAN 并启用 MAC 过滤](#)
2. [使用客户端 MAC 地址配置 RADIUS 服务器](#)

配置 WLAN 并启用 MAC 过滤

要配置具有MAC过滤功能的WLAN，请执行以下操作：

1. 要创建 WLAN，请从控制器 GUI 中单击 WLANs。随即显示 WLAN 窗口。该窗口列出了控制器中配置的 WLAN。
2. 要配置新的 WLAN，请单击 New。在本示例中，WLAN 命名为 MAC-ACS-WLAN 且 WLAN ID 为 2。

WLANs > New

Type

WLAN

Profile Name

MAC-ACS-WLAN

SSID

MAC-ACS-WLAN

ID

2

3. 单击 **Apply**。
4. 在“WLANs > Edit”窗口中，定义特定于该 WLAN 的参数。在 **Security > Layer 2 > Layer 2 Security Policies** 下，选中 **MAC Filtering** 复选框。这将为 WLAN 启用 MAC 身份验证。在 **General > Interface name** 下，选择 WLAN 映射到的接口。在 **安全 > AAA 服务器 > RADIUS 服务器** 下，选择可用于 MAC 身份验证的 RADIUS 服务器。

WLANs > Edit

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	None
Server 2	None	None
Server 3	None	None

选择要用于MAC身份验证的RADIUS服务器。

注：从 **WLAN > Edit** 窗口选择 RADIUS 服务器之前，必须在 **Security > Radius Authentication** 窗口中定义 RADIUS 服务器并启用 RADIUS 服务器。

RADIUS Authentication Servers

Call Station ID Type: IP Address

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
☒	☒	1	10.77.244.196	1812	Enabled	Enabled

Radius身份验证服务器根据 WLAN 的设计要求选择其他参数。单击 **Apply**。

WLANs > Edit

The screenshot shows the 'WLANs > Edit' configuration page with the 'Security' tab selected. The 'Status' is 'Enabled' and 'Security Policies' is 'MAC Filtering'. A red box highlights the 'Status' and 'Security Policies' sections.

General	Security	QoS	Advanced
Profile Name	MAC-ACS-WLAN		
Type	WLAN		
SSID	MAC-ACS-WLAN		
Status	☒ Enabled		
Security Policies	MAC Filtering (Modifications done under security tab will appear after applying the)		
Radio Policy	All		
Interface	management		
Broadcast SSID	☒ Enabled		

设计需求参数

5. 单击 Security > MAC Filtering。
6. 在 MAC Filtering 窗口中，在 RADIUS Compatibility Mode 下选择 RADIUS 服务器的类型。本示例使用 Cisco ACS。
7. 从 MAC Delimiter 下拉菜单中，选择 MAC delimiter。本示例使用 Colon。
8. 单击 Apply。

MAC Filtering

The screenshot shows the 'MAC Filtering' configuration page. The 'RADIUS Compatibility Mode' is 'Cisco ACS' and the 'MAC Delimiter' is 'Colon'. A note on the right says '(In the Radius Access Request packet, the MAC address is used as the username.)'.

RADIUS Compatibility Mode	Cisco ACS	(In the Radius Access Request packet, the MAC address is used as the username.)
MAC Delimiter	Colon	

选择RADIUS服务器类型

下一步是使用客户端 MAC 地址配置 ACS 服务器。

使用客户端 MAC 地址配置 RADIUS 服务器

要将MAC地址添加到ACS，请执行以下操作：

1. 在 ACS 服务器上将 WLC 定义为 AAA 客户端。从 ACS GUI 中单击 **Network Configuration**。
2. 当出现 Network Configuration 窗口时，定义 WLC 的名称、IP 地址、共享密钥和身份验证方法 (RADIUS Cisco Aironet 或 RADIUS Airespace)。有关其他非 ACS 身份验证服务器的信息，请参阅制造商提供的文档。

Network Configuration

User Setup

Group Setup

Shared Profile Components

Network Configuration

System Configuration

Interface Configuration

Administration Control

External User Databases

Reports and Activity

Online Documentation

Edit

Add AAA Client

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

Submit

Submit + Restart

Cancel

Back to Help

Help

- [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](#)

AAA Client Hostname

The AAA Client Hostname is the name assigned to the AAA client.

[\[Back to Top\]](#)

AAA Client IP Address

The AAA Client IP Address is the IP address assigned to the AAA client.

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

添加AAA客户端

注：您在WLC上配置的共享密钥必须与ACS服务器匹配。共享密钥区分大小写。

3. 从 ACS 主菜单中，单击 **User Setup**。

4. 在 User 文本框，输入 MAC 地址以添加到用户数据库。

User Setup

User Setup

Group Setup

Shared Profile Components

Network Configuration

System Configuration

Interface Configuration

Administration Control

External User Databases

Reports and Activity

Online Documentation

Select

User: 00:40:96:ACE6:57

Find

Add/Edit

List users beginning with letter/number:

A B C D E F G H I J K L M

N O P Q R S T U V W X Y Z

0 1 2 3 4 5 6 7 8 9

List All Users

Back to Help

Help

- [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](#)

User Setup and External User Databases

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.

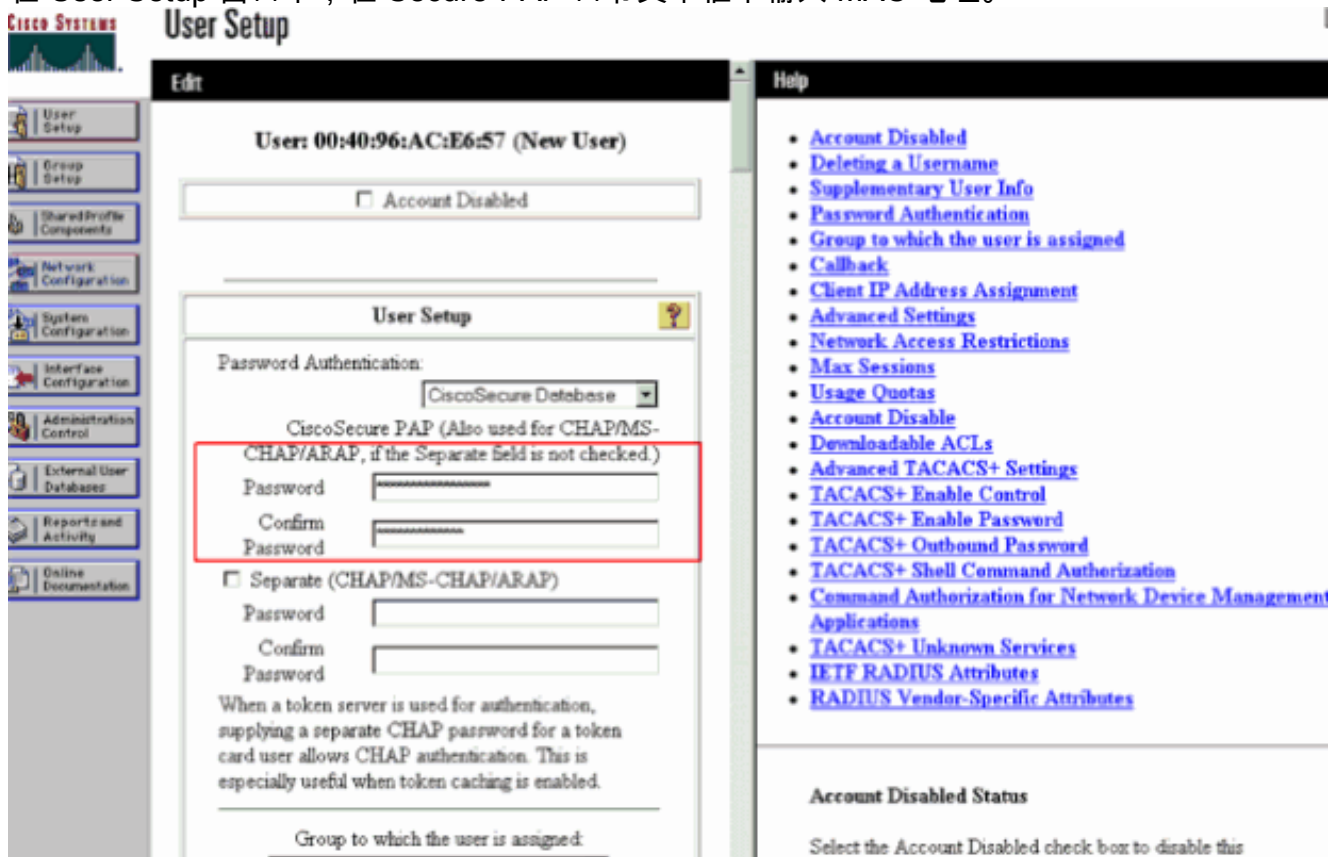
Note: User Setup configuration overrides Group Setup configuration.

If you rely on the Unknown User Policy in the External User Databases section to create entries in the

输入MAC地址

注:MAC地址必须与WLC为用户名和密码发送的地址完全相同。如果身份验证失败，请检查失败的尝试日志以查看 WLC 如何报告 MAC。请不要剪切并粘贴 MAC 地址，因为这可能引入虚拟字符。

5. 在 User Setup 窗口中，在 Secure-PAP 口令文本框中输入 MAC 地址。



在 Secure-PAP Password 字段中输入 MAC 地址

注: MAC 地址必须与 WLC 为用户名和密码发送的地址完全相同。如果身份验证失败，请检查失败的尝试日志以查看 AP 如何报告 MAC。请不要剪切并粘贴 MAC 地址，因为这可能引入虚拟字符。

6. 单击“Submit”。
7. 要向 ACS 数据库中添加更多用户，请重复步骤 2 到 5。现在，当客户端连接到此 WLAN 时，WLC 会将凭据传送给 ACS 服务器。ACS 服务器根据 ACS 数据库验证这些凭据。如果数据库中不存在客户端 MAC 地址，ACS RADIUS 服务器会向 WLC 返回身份验证成功，并且客户端可以获准访问 WLAN。

使用 CLI 在 WLC 上配置 MAC 过滤器

本文档前面已讨论如何使用 WLC GUI 配置 MAC 过滤器。您也可以使用 CLI 在 WLC 上配置 MAC 过滤器。要在 WLC 上配置 MAC 过滤器，请执行以下操作：

- 发出 **config wlan mac-filtering enable wlan_id** 命令以启用 MAC 过滤。输入 **show wlan** 命令以验证是否已为 WLAN 启用 MAC 过滤。
- config macfilter add** 命令：使用 **config macfilter add** 命令可以添加 macfilter、接口、说明等。使用 **config macfilter add** 命令可在 Cisco 无线 LAN 控制器上创建 MAC 过滤器条目。使用此命令可在 Cisco 无线 LAN 控制器上添加无线 LAN 的本地客户端。此过滤器将绕过 RADIUS 身份验证过程。

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

示例输入一个静态 MAC 到 IP 的地址映射。执行该操作可支持被动客户端，即，不使用 DHCP 也不传输未经请求的 IP 数据包的客户端。

(Cisco Controller) >**config macfilter add 00:E0:77:31:A3:55 1 lab02 "labconnect" 10.92.125.51**

- config macfilter ip-address** 命令 **config macfilter ip-address** 命令可将 MAC 过滤器映射到 IP 地址。使用以下命令可将 IP 地址配置到本地 MAC 过滤器数据库中：

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

示例

```
(Cisco Controller) >config macfilter ip-address 00:E0:77:31:A3:55 10.92.125.51
```

为已禁用客户端配置超时

可以为已禁用的客户端配置超时。在尝试关联时三次未能进行身份验证的客户端将自动禁用，以防止进一步尝试关联。超时时间过后，允许客户端重试身份验证，直到其关联或身份验证失败并再次被排除。输入**config wlan exclusionlist wlan_id timeout**命令，以便为已禁用的客户端配置超时。超时值可以是1到65535秒，也可以输入0以永久禁用客户端。

验证

要验证MAC过滤器是否配置正确，请执行以下操作：

- **show macfilter summary** - 显示所有 MAC 过滤器条目的概要。
- **show macfilter detail <client MAC Address>** - MAC 过滤器条目的详细显示。

以下是 **show macfilter summary** 命令的一个示例：

```
(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) >
```

以下是**show macfilter detail**command的示例：

```
(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
```

故障排除

您可以使用以下命令来排除配置问题：

注意：使用debug命令[之前，请参阅有关](#)调试命令的**重要信息**。

- **debug aaa all enable** - 提供所有 AAA 消息的调试。
- **debug mac addr <Client-MAC-address xx:xx:xx:xx:xx:xx>** — 要配置MAC调试，请使用**debug maccommand**命令。

以下是 **debug aaa all enable** 命令的一个示例：

```

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: -1dataAvgC: -1, rTAVGC: -1, dataBurstC:

```

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

当无线客户端不存在于WLC的MAC地址数据库中（本地数据库）或RADIUS服务器尝试与WLAN关联时，可以排除该客户端。以下是针对不成功 MAC 身份验证的 **debug aaa all enable** 命令的一个示例：

```

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:

```

错误：尝试通过MAC地址进行身份验证的无线客户端被拒绝；失败的身份验证报告显示内部错误

当您在Microsoft Windows 2003 Enterprise服务器上使用ACS 4.1时，尝试通过MAC地址进行身份验证的客户端会被拒绝。当 AAA 客户端向 AAA 服务器发送 Service-Type=10 属性值时会发生这种情况。这是因为Cisco Bug ID [CSCsh62641](#)。受此 bug 影响的 AAA 客户端包括 WLC 和使用 MAC 身份验证旁路的交换机。

解决方法如下：

- 降级到 ACS 4.0。或
- 在内部 ACS DB MAC 地址表下，将要进行身份验证的 MAC 地址添加到网络访问保护 (NAP) 中。

错误：无法使用WLC GUI添加MAC过滤器

由于Cisco Bug ID [CSCsj98722](#)（仅限注册用户），可能会发生这种情况。此 bug 在 4.2 代码版本中得到修复。如果运行的版本早于4.2，您可以将固件升级到4.2或使用以下两种解决方法解决此问题。

- 使用 CLI，通过以下命令配置 MAC 过滤器：
`config macfilter add <MAC_address> <WLAN_id> <Interface_name>`
- 在控制器的 Web GUI 中，在 Security 选项卡中选择 **Any WLAN** 并输入要过滤的 MAC 地址。

错误：静默客户端未置于运行状态

如果未在控制器上配置必需的 DHCP，则当无线客户端发送出第一个 IP 数据包或 ARP 时，AP 可获知该无线客户端的 IP 地址。如果无线客户端是被动设备，例如，不启动通信的设备，则 AP 无法获知无线设备的 IP 地址。结果，控制器会等待十秒以等待客户端发送 IP 数据包。如果没有来自客户端的数据包响应，则控制器将丢弃发往被动无线客户端的任何数据包。此问题记录在思科漏洞ID [CSCsq46427](#)中。

注意：只有思科注册用户才能访问内部工具和信息。

作为针对打印机、无线 PLC 泵等被动设备的建议解决方法，您需要针对 MAC 过滤设置 WLAN 并选中 AAA 覆盖以允许连接这些设备。

可以在将无线设备的 MAC 地址映射到 IP 地址的控制器上创建 MAC 地址过滤器。

注：这要求在第2层安全的WLAN配置上启用MAC地址过滤。它还要求在WLAN配置的高级设置中启用AAA。

在 CLI 中，请输入以下命令来创建 MAC 地址过滤器：

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

示例如下：

```
(Cisco Controller) > config macfilter add 00:01:02:03:04:05 1 my_interface "Zebra Printer" 192.168.1.1
```

相关信息

- [无线 LAN 控制器中的 ACL 配置示例](#)
- [无线局域网控制器认证的配置示例](#)
- [无线局域网控制器上的 VLAN 配置示例](#)
- [思科无线LAN控制器配置指南4.1版停用通知](#)
- [无线技术支持页](#)
- [技术支持和下载 — Cisco Systems](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。