

使用AireOS無線LAN控制器(WLC)設定MAC過濾器

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[背景資訊](#)

[WLC上的MAC位址過濾器 \(MAC驗證 \)](#)

[在WLC上配置本地MAC身份驗證](#)

[配置WLAN並啟用MAC過濾](#)

[在WLC上使用客戶端MAC地址配置本地資料庫](#)

[使用RADIUS伺服器配置MAC身份驗證](#)

[配置WLAN並啟用MAC過濾](#)

[使用客戶端MAC地址配置RADIUS伺服器](#)

[使用CLI設定WLC上的MAC過濾器](#)

[為已禁用的客戶端配置超時](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

簡介

本文件說明如何使用無線 LAN 控制器 (WLC) 設定 MAC 篩選器。

必要條件

需求

思科建議您瞭解以下主題：

- LAP和Cisco WLC的配置
- 思科整合無線安全解決方案

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco 4400 WLC (執行軟體版本5.2.178.0)
- Cisco 1230AG系列LAP
- 採用韌體4.4的802.11 a/b/g無線使用者端配接器
- Aironet案頭實用程式(ADU)版本4.4

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

背景資訊

本檔案介紹如何透過組態範例使用無線LAN控制器(WLC)設定MAC過濾器。本文還討論了如何針對AAA伺服器授權輕量型存取點(LAP)。

WLC上的MAC位址過濾器 (MAC驗證)

當您在WLC上建立MAC位址過濾器時，系統會根據使用者使用的使用者端的MAC位址，授予或拒絕使用者存取WLAN網路的許可權。

WLC支援兩種型別的MAC驗證：

- 本地MAC身份驗證
- 用於RADIUS伺服器的MAC身份驗證

透過本地MAC驗證，使用者MAC位址儲存在WLC上的資料庫中。使用者嘗試存取設定為MAC過濾的WLAN時，會對WLC上的本機資料庫驗證使用者端MAC位址，如果驗證成功，便會授予使用者端存取WLAN的權力。

預設情況下，WLC本地資料庫最多支援512個使用者條目。

本地使用者資料庫最多限制為2048個條目。本地資料庫儲存以下專案的條目：

- 本地管理使用者，包括游說大使
- 本地網路使用者，包括訪客使用者
- MAC過濾器條目
- 排除清單條目
- 接入點授權清單條目

所有這些型別的使用者都不能超過配置的資料庫大小。

要增加本地資料庫，請從CLI使用以下命令：

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

或者，也可以使用RADIUS伺服器執行MAC位址驗證。唯一的區別是使用者的MAC位址資料庫儲存在RADIUS伺服器而不是WLC中。使用者資料庫儲存在RADIUS伺服器上時，WLC會將使用者端的MAC位址轉送到RADIUS伺服器以進行使用者端驗證。然後，RADIUS伺服器根據它擁有的資料庫驗證MAC地址。如果使用者端驗證成功，則使用者端會獲得存取WLAN的授權。可以使用支援MAC地址身份驗證的任何RADIUS伺服器。

在WLC上配置本地MAC身份驗證

在WLC上配置本地MAC身份驗證：

1. [配置WLAN並啟用MAC過濾](#)。
2. [在WLC上使用客戶端MAC地址配置本地資料庫](#)。



注意：在配置MAC身份驗證之前，必須配置WLC進行基本操作並將LAP註冊到WLC。本檔案假設WLC已設定為基本操作，且LAP已註冊到WLC。如果您是新使用者，並且想要嘗試設定WLC以對LAP執行基本操作，請參閱[對無法加入WLC的輕量AP進行故障排除](#)。



註：無線客戶端不需要特殊配置即可支援MAC身份驗證。

配置WLAN並啟用MAC過濾

要使用MAC過濾配置WLAN，請執行以下操作：

1. 從控制器GUI中按一下WLANs，以便建立WLAN。

出現WLANs視窗。此視窗列出控制器上設定的WLAN。

2. 按一下New以設定新的WLAN。

在本範例中，WLAN命名為MAC-WLAN，而WLAN ID為1。

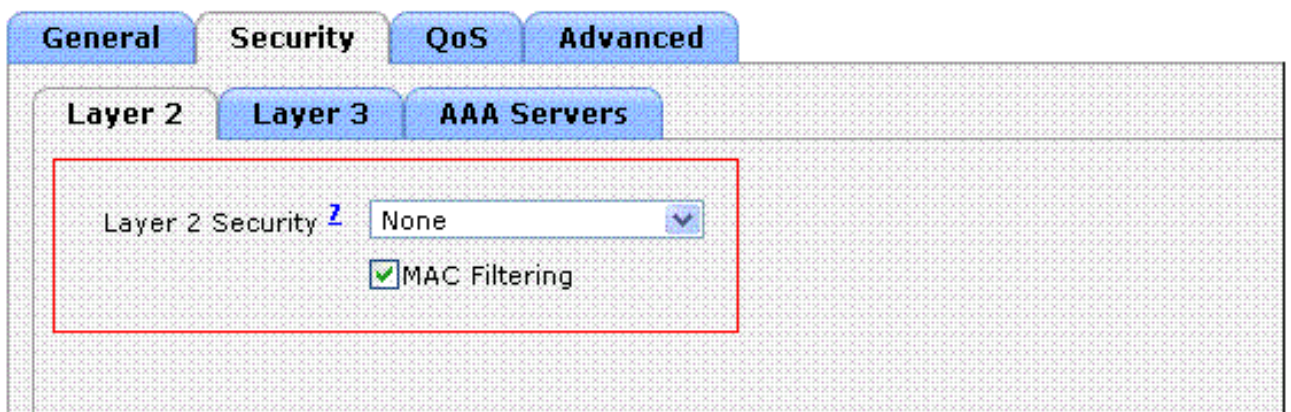
WLANs > New

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

配置WLAN啟用MAC過濾

- 按一下「Apply」。
- 在「WLANs > Edit」視窗中，定義特定於WLAN的引數。

WLANs > Edit



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

定義引數

- 在Security > Layer 2 > Layer 2 Security Policies下，選中MAC Filtering覈取方塊。
這將為WLAN啟用MAC身份驗證。
- 在General > Interface name下，選擇WLAN對映到的介面。
在此範例中，WLAN對映到管理介面。
- 選擇其他引數，這些引數取決於WLAN的設計要求。
- 按一下「Apply」。

WLANs > Edit

General Security QoS Advanced

Profile Name: MAC-WLAN
Type: WLAN
SSID: MAC-WLAN
Status: Enabled
Security Policies: **MAC Filtering**
(Modifications done under security tab will appear after applying th
Radio Policy: All
Interface: management
Broadcast SSID: Enabled

對映到介面的WLAN

下一步是使用客戶端MAC地址配置WLC上的本地資料庫。

有關如何在WLC上設定動態介面(VLAN)的資訊，請參閱[無線LAN控制器上的VLAN組態範例](#)。

在WLC上使用客戶端MAC地址配置本地資料庫

使用WLC上的客戶端MAC地址配置本地資料庫：

1. 在控制器GUI上按一下Security，然後從左側選單中按一下MAC Filtering。

出現「MAC Filtering (MAC過濾)」視窗。

MAC Filtering

RADIUS Compatibility Mode

Cisco ACS

(In the Radius Access Reques
MAC address.)

MAC Delimiter

No Delimiter

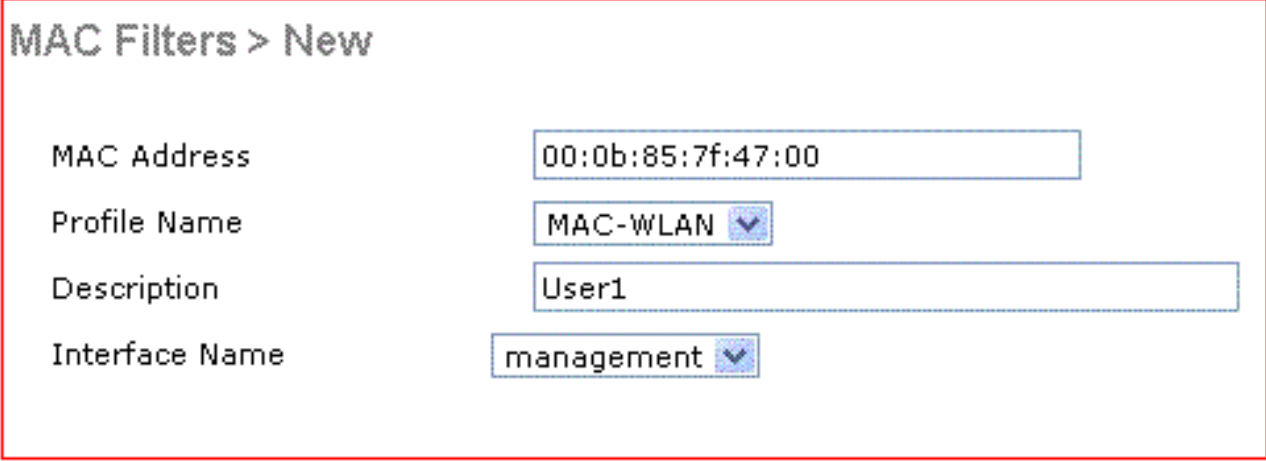
Local MAC Filters

MAC Address Profile Name Interface Description

MAC Filtering視窗

2. 按一下「New」，在WLC上建立本機資料庫MAC位址專案。
3. 在「MAC Filters > New」視窗中，輸入客戶端的MAC地址、配置檔名稱、說明和介面名稱。

以下是範例：




MAC Filters > New

MAC Address	00:0b:85:7f:47:00
Profile Name	MAC-WLAN
Description	User1
Interface Name	management

為MAC地址建立本地資料庫

4. 按一下「Apply」。
5. 重複步驟2-4，以便向本地資料庫新增更多客戶端。

現在，當客戶端連線到此WLAN時，WLC會根據本地資料庫驗證客戶端MAC地址，如果驗證成功，則授予客戶端訪問網路的許可權。

 **注意：**在本示例中，只使用了一個沒有其他第2層安全機制的MAC地址過濾器。Cisco建議必須將MAC位址驗證與其他第2層或第3層安全方法一起使用。不建議僅使用MAC地址身份驗證來保護您的WLAN網路，因為它不提供強的安全機制。

使用RADIUS伺服器配置MAC身份驗證

要使用RADIUS伺服器配置MAC身份驗證，請使用以下連結。在本示例中，Cisco Secure ACS伺服器用作RADIUS伺服器。

1. [配置WLAN並啟用MAC過濾](#)
2. [使用客戶端MAC地址配置RADIUS伺服器](#)

配置WLAN並啟用MAC過濾

要使用MAC過濾配置WLAN，請執行以下操作：

1. 從控制器GUI中按一下WLANs，以便建立WLAN。

出現WLANs視窗。此視窗列出控制器上設定的WLAN。

2. 按一下New以設定新的WLAN。

在本範例中，WLAN命名為MAC-ACS-WLAN，WLAN ID為2。

WLANs > New

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

配置新的WLAN啟用MAC過濾

3. 按一下「Apply」。

4. 在「WLANs > Edit」視窗中，定義特定於WLAN的引數。

a. 在Security > Layer 2 > Layer 2 Security Policies下，選中MAC Filtering覈取方塊。

這將為WLAN啟用MAC身份驗證。

b. 在General > Interface name下，選擇WLAN對映到的介面。

c. 在Security > AAA Servers > RADIUS servers下，選擇可用於MAC身份驗證的RADIUS伺服器。

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	None
Server 2	None	None
Server 3	None	None

Enabled

選擇要用於MAC身份驗證的RADIUS伺服器。

 註：從WLAN > Edit視窗選擇RADIUS伺服器之前，必須在Security > Radius Authentication視窗中定義RADIUS伺服器並啟用RADIUS伺服器。

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"/>	1	10.77.244.196	1812	Enabled	Enabled <input checked="" type="checkbox"/>

Radius驗證伺服器

- d. 選擇其他引數，這些引數取決於WLAN的設計要求。
- e. 按一下「Apply」。

WLANs > Edit

The screenshot shows the 'Security' tab of the WLAN configuration page. The 'Security Policies' section is highlighted with a red box. It shows 'MAC Filtering' selected, with a note: '(Modifications done under security tab will appear after applying the...)'

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

設計需求引數

5. 按一下Security > MAC Filtering。
6. 在「MAC Filtering (MAC過濾)」視窗中，在「RADIUS Compatibility Mode (RADIUS相容模式)」下選擇RADIUS伺服器的型別。

此示例使用Cisco ACS。

7. 從MAC分隔符下拉選單中，選擇MAC分隔符。

本示例使用冒號。

8. 按一下「Apply」。

MAC Filtering

The screenshot shows the 'MAC Filtering' configuration window. It has two dropdown menus: 'RADIUS Compatibility Mode' set to 'Cisco ACS' and 'MAC Delimiter' set to 'Colon'. A note on the right says: '(In the Radius Access Request packet, use the following MAC address.)'

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

選擇RADIUS伺服器型別

下一步是使用客戶端MAC地址配置ACS伺服器。

使用客戶端MAC地址配置RADIUS伺服器

要將MAC地址新增到ACS，請執行以下操作：

1. 將WLC定義為ACS伺服器上的AAA客戶端。在ACS GUI上按一下Network Configuration。
2. 出現「Network Configuration (網路配置)」視窗時，定義WLC的名稱、IP地址、共用金鑰和身份驗證方法 (RADIUS Cisco Aironet或RADIUS Airespace)。

請參閱製造商提供的文檔，瞭解其它非ACS身份驗證伺服器。

The screenshot shows the 'Add AAA Client' configuration window in the Cisco ACS GUI. The window is titled 'Network Configuration' and has an 'Edit' header. The main content area is titled 'Add AAA Client' and contains 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:

At the bottom of the dialog, there are three buttons: 'Submit', 'Submit + Restart', and 'Cancel'. Below these buttons is a 'Back to Help' button with a question mark icon.

The right-hand side of the window contains a 'Help' section with a list of 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, and Replace RADIUS Port info with Username from this AAA Client. Below the links, there are two sections: 'AAA Client Hostname' and 'AAA Client IP Address', each with a brief description of the field and a '[Back to Top]' link.

新增AAA客戶端



註：在WLC上配置的共用金鑰必須與ACS伺服器匹配。共用金鑰區分大小寫。

3. 在ACS主選單中，按一下User Setup。
4. 在使用者文本框中，輸入MAC地址以新增到使用者資料庫。

User Setup

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 enables you to configure individual user information, add users, and delete users in the 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

輸入MAC地址

 註:MAC位址必須與WLC為使用者名稱和密碼所傳送的位址完全相同。如果驗證失敗，請檢查嘗試失敗日誌以檢視WLC如何報告MAC。請勿剪下和貼上MAC地址，因為這樣可能會引入幻像字元。

5. 在「使用者設定」視窗中，在Secure-PAP密碼文本框中輸入MAC地址。

在Secure-PAP密碼欄位中輸入MAC地址

 註:MAC位址必須與WLC為使用者名稱和密碼所傳送的位址完全相同。如果身份驗證失敗，請檢查失敗的嘗試日誌以檢視AP如何報告MAC。請勿剪下和貼上MAC地址，因為這樣可能會引入幻像字元。

6. 按一下Submit。
7. 重複步驟2-5，以便向ACS資料庫新增更多使用者。

現在，當客戶端連線到此WLAN時，WLC會將憑證傳遞到ACS伺服器。ACS伺服器根據ACS資料庫驗證憑證。如果資料庫中存在客戶端MAC地址，則ACS RADIUS伺服器會向WLC返回身份驗證成功，並且可授予客戶端訪問WLAN的許可權。

使用CLI設定WLC上的MAC過濾器

本檔案先前曾討論如何使用WLC GUI設定MAC過濾器。您還可以使用CLI在WLC上設定MAC過濾器。在WLC上設定MAC過濾器：

- 發出config wlan mac-filtering enable wlan_id 命令以啟用MAC過濾。輸入 show wlan命令以驗證是否已為WLAN啟用MAC過濾。
- config macfilter add命令：

config macfilter add 命令可讓您新增macfilter、介面、說明等。

使用config macfilter add 指令，在思科無線LAN控制器上建立MAC過濾器專案。使用以下命令將使用者端本地新增至思科無線LAN控制器上的無線LAN。此過濾器會繞過RADIUS驗證程式。

```
<#root>
```

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

範例

輸入靜態MAC到IP地址對映。這樣做是為了支援被動客戶端，即不使用DHCP且不傳輸未經請求的IP資料包的客戶端。

```
<#root>
```

```
(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 命令可將MAC過濾器對映到IP地址。使用以下命令將IP位址設定為本地MAC過濾器資料庫：

```
<#root>
```

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

範例

```
<#root>
```

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

為已禁用的客戶端配置超時

您可以為已禁用的客戶端配置超時。在嘗試關聯期間三次未能進行身份驗證的客戶端將自動禁止進一步的關聯嘗試。超時時間過後，允許客戶端重試身份驗證，直到它關聯或身份驗證失敗並再次被排除。輸入config wlan exclusionlist wlan_id timeout 命令，為已禁用的使用者端設定逾時。逾時值可以是1到65535秒，也可以輸入0以永久停用使用者端。

驗證

驗證MAC過濾器是否配置正確：

- show macfilter summary — 顯示所有MAC過濾器條目的摘要。
- show macfilter detail < client MAC Address> - MAC過濾器條目的詳細顯示。

以下是show macfilter summary命令的示例：

<#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) >

以下是show macfilter detailcommand的範例：

<#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
```

疑難排解

您可以使用以下命令對組態進行疑難排解：

 附註：使用 debug 指令之前，請先參閱有關 Debug 指令的重要資訊。

- debug aaa all enable — 提供所有AAA消息的調試。
- debug mac addr <Client-MAC-address xx:xx:xx:xx:xx:xx> — 要配置MAC調試，請使用debug maccommand。

以下是debug aaa all enable 指令的範例：

```
<#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'
```

當無線使用者端不存在於WLC上的MAC位址資料庫（本機資料庫）或RADIUS伺服器嘗試與WLAN相關聯時，可以排除該使用者端。以下是debug aaa all enable 命令用於不成功的MAC身份驗證的示例：

<#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:

錯誤：嘗試通過MAC地址進行身份驗證的無線客戶端被拒絕；失敗的身份驗證報告顯示內部錯誤

在Microsoft Windows 2003 Enterprise伺服器上使用ACS 4.1時，嘗試使用MAC地址進行身份驗證的客戶端將被拒絕。當AAA客戶端向AAA伺服器傳送Service-Type=10屬性值時會發生這種情況。這是因為思科錯誤ID [CSCsh62641](#)。受此錯誤影響的AAA使用者端包括使用MAC驗證略過的WLC和交換器。

解決方法如下：

- 降級到ACS 4.0。

或

- 將要進行身份驗證的MAC地址新增到內部ACS資料庫MAC地址表下的網路訪問保護(NAP)中。

錯誤：無法使用WLC GUI新增MAC過濾器

發生這種情況是由於思科錯誤ID [CSCsj9872](#)。錯誤已在4.2版本的程式碼中修正。如果運行的版本早於4.2，您可以將韌體升級到4.2，或者使用這兩個解決方法來解決此問題。

- 使用CLI使用以下命令設定MAC過濾器：

<#root>


config macfilter add

<MAC_address> <WLAN_id> <Interface_name>

- 在控制器的Web GUI中，選擇Security索引標籤下的Any WLAN，然後輸入要過濾的MAC地址。

錯誤：靜默客戶端未置於運行狀態

如果在控制器上未配置所需的DHCP，則當無線客戶端傳送第一個IP資料包或ARP時，AP會獲知無線客戶端的IP地址。如果無線客戶端是被動裝置（例如，不發起通訊的裝置），則AP無法獲知無線裝置的IP地址。因此，控制器會等待使用者端傳送IP封包十秒。如果來自使用者端的封包沒有回應，控制器就會捨棄傳送到被動無線使用者端的封包。此問題已記錄在Cisco錯誤ID [CSCsq46427](#)中。

 備註：只有註冊的思科使用者能夠存取內部工具與資訊。

作為印表機、無線PLC泵等無源裝置的建議解決方法，您需要設定WLAN以進行MAC過濾，並選中AAA覆蓋以允許連線這些裝置。

可以在控制器上建立MAC地址過濾器，將無線裝置的MAC地址對映到IP地址。

 註：這要求在第2層安全的WLAN配置上啟用MAC地址過濾。它還要求在WLAN配置的高級設定中啟用Allow AAA Override。

在CLI中，輸入以下命令以建立MAC位址過濾器：

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

以下是範例：

```
<#root>
```

```
(Cisco Controller) >
```

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

相關資訊

- [無線LAN控制器上的ACL組態範例](#)
- [無線LAN控制器上的驗證組態範例](#)
- [無線LAN控制器上的VLAN組態範例](#)
- [思科無線LAN控制器組態設定指南4.1版停用通知](#)
- [無線技術支援頁面](#)

- [思科技術支援與下載](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。