

無線 LAN コントローラ (WLC) を使用した MAC フィルタの設定例

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[WLC での MAC アドレス フィルタ \(MAC 認証 \)](#)

[WLC でのローカル MAC 認証の設定](#)

[WLAN の設定と MAC フィルタリングの有効化](#)

[クライアントの MAC アドレスを使用した WLC でのローカル データベースの設定](#)

[RADIUS サーバを使用した MAC 認証の設定](#)

[WLAN の設定と MAC フィルタリングの有効化](#)

[クライアントの MAC アドレスを使用した RADIUS サーバの設定](#)

[WLC で MAC フィルタを設定する CLI の使用](#)

[無効なクライアントのタイムアウトの設定](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

概要

このドキュメントでは、無線 LAN コントローラ (WLC) を使用した MAC フィルタの設定方法と設定例について説明しています。また、このドキュメントでは、AAA サーバに対して Lightweight Access Point (LAP; Lightweight アクセス ポイント) を認可する方法についても説明しています。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- LAP および Cisco WLC の設定に関する基本的な知識
- Cisco Unified Wireless Security Solutions についての基本的な知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- ソフトウェア バージョン 5.2.178.0 を実行する Cisco 4400 WLC
- Cisco 1230AG シリーズ LAP
- ファームウェア 4.4 が稼働する 802.11 a/b/g のワイヤレス クライアントのアダプタ
- Aironet Desktop Utility (ADU) バージョン 4.4

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

[表記法](#)

ドキュメント表記の詳細は、『[シスコテクニカルティップスの表記法](#)』を参照してください。

[WLC での MAC アドレス フィルタ \(MAC 認証 \)](#)

WLC で MAC アドレス フィルタを作成すると、使用しているクライアントの MAC アドレスに基づいてユーザによる WLAN ネットワークへのアクセスを許可または拒否できます。

WLC でサポートされている MAC 認証には、次の 2 つのタイプがあります。

- ローカル MAC 認証
- RADIUS サーバを使用した MAC 認証

ローカル MAC 認証では、ユーザの MAC アドレスが WLC 上のデータベースに記録されます。MAC フィルタリングを行うように設定された WLAN にユーザがアクセスしようとする、クライアントの MAC アドレスが WLC 上のローカル データベースで照合され、認証に成功した場合は、WLAN へのアクセスが許可されます。

デフォルトでは、WLC のローカル データベースは最大 512 個のユーザ エントリをサポートします。

ローカル ユーザ データベースは最大 2048 エントリに制限されます。ローカル データベースでは次の項目のエントリを保存します：

- ローカル管理ユーザ (ロビー アンバサダーを含む)
- ローカル ネットワーク ユーザ (ゲスト ユーザを含む)
- MAC フィルタ エントリ
- 除外リスト エントリ
- アクセス ポイントの許可リスト エントリ

これらのすべてのタイプのユーザの合計が、設定されているデータベース サイズを超えることはできません。

ローカル データベースを増やす場合は、CLI から次のコマンドを使用します。

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

また、RADIUS サーバを使用して MAC アドレス認証を実行することもできます。唯一の違いは、MAC アドレス データベースが WLC ではなく RADIUS サーバに保存されることです。ユーザ データベースが RADIUS サーバに保存される場合、WLC はクライアントを検証するために RADIUS サーバにクライアントの MAC アドレスを転送します。その後、RADIUS サーバは自身

のデータベースに基づいて MAC アドレスを照合します。クライアント認証に成功すると、クライアントに対して WLAN へのアクセスが許可されます。MAC アドレス認証をサポートする RADIUS サーバであれば、任意のサーバを使用できます。

WLC でのローカル MAC 認証の設定

WLC でローカル MAC 認証を設定するには、次の手順を実行します。

1. [WLAN の設定と MAC フィルタリングの有効化](#)
2. [クライアントの MAC アドレスを使用した WLC でのローカル データベースの設定](#)注: MAC 認証の設定を行う前に、WLC の基本動作を設定し、WLC に LAP を登録する必要があります。このドキュメントでは、WLC では基本動作が設定されており、WLC に LAP が登録されていることを前提としています。WLC で LAP との基本動作を初めて設定する場合は、「[Wireless LAN Controller \(WLC \) への Lightweight AP \(LAP \) の登録](#)」を参照してください。注: MAC 認証をサポートするために無線クライアントで特別な設定を行う必要はありません。

WLAN の設定と MAC フィルタリングの有効化

MAC フィルタリングを行うように WLAN を設定するには、次の手順を実行します。

1. WLAN を作成するために、コントローラの GUI で [WLANs] をクリックします。[WLANs] ウィンドウが表示されます。このウィンドウには、コントローラに設定されている WLAN の一覧が表示されます。
2. 新しい WLAN を設定するために [New] をクリックします。この例では、WLAN に MAC-WLAN と名前を付けており、WLAN ID は 1 です。

WLANs > New

Type	<input type="text" value="WLAN"/>
Profile Name	<input type="text" value="MAC-WLAN"/>
SSID	<input type="text" value="MAC-WLAN"/>
ID	<input type="text" value="1"/>

3. [Apply] をクリックします。
4. [WLAN] > [Edit] ウィンドウで、WLAN 固有のパラメータを定義します。

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.

[Security Policies] > [Layer 2 Security] で、[MAC Filtering] チェックボックスにチェックマークを付けます。これにより、WLAN に対して MAC 認証が有効になります。[General Policies] > [Interface Name] で、WLAN をマッピングするインターフェイスを選択します。この例では、WLAN を管理インターフェイスにマッピングしています。WLAN の設計要件に応じて、その他のパラメータを選択します。[Apply] をクリックします。

WLANs > Edit

The screenshot shows the 'WLANs > Edit' configuration page with the 'Security' tab selected. The 'Status' checkbox is checked and labeled 'Enabled'. The 'Security Policies' dropdown is set to 'MAC Filtering'. The 'Interface' dropdown is set to 'management'. A red box highlights the 'Status', 'Security Policies', and 'Interface' settings.

Profile Name	MAC-WLAN
Type	WLAN
SSID	MAC-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

次に、クライアントの MAC アドレスを使用して WLC 上のローカル データベースを設定します。

WLC でダイナミック インターフェイス (VLAN) を設定する方法については、『[無線 LAN コントローラでの VLAN の設定例 \(VLANs on Wireless LAN Controllers Configuration Example \)](#)』を参照してください。

クライアントの MAC アドレスを使用した WLC でのローカル データベースの設定

WLC でクライアントの MAC アドレスを使用してローカル データベースを設定するには、次の手順を実行します。

1. コントローラの GUI で **Security** をクリックし、左側のメニューで **MAC Filtering** をクリックします。MAC Filtering ウィンドウが表示されます。

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. **New** をクリックして、WLC 上のローカル データベースに MAC アドレス エントリを作成します。
3. [MAC Filters] > [New] ウィンドウで、クライアントの MAC アドレス、プロファイル名、説明、インターフェイス名を入力します。次に例を示します。

MAC Filters > New

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

4. [Apply] をクリックします。
5. さらに多くのクライアントをローカル データベースに追加するには、ステップ 2 ~ 4 を繰り返します。クライアントがこの WLAN に接続すると、WLC によってクライアントの MAC アドレスがローカル データベースに照合され、認証に成功した場合は、クライアントに対してネットワークへのアクセスが許可されます。注: この例では、他のレイヤ 2 セキュリティ メカニズムのない MAC アドレスのフィルタのみを使用しました。MAC アドレス認証は、他のレイヤ 2 またはレイヤ 3 のセキュリティ方式と組み合わせて使用することを推奨いたします。MAC アドレス認証で提供されるセキュリティ メカニズムは強力なものではないので、MAC アドレス認証のみを使用して WLAN ネットワークを保護することは推奨され

ません。

RADIUS サーバを使用した MAC 認証の設定

RADIUS サーバを使用する MAC 認証を設定するには、次の手順を実行します。この例では、RADIUS サーバとして Cisco Secure ACS サーバを使用しています。

1. [WLAN の設定と MAC フィルタリングの有効化](#)
2. [クライアントの MAC アドレスを使用した RADIUS サーバの設定](#)

WLAN の設定と MAC フィルタリングの有効化

MAC フィルタリングを行うように WLAN を設定するには、次の手順を実行します。

1. WLAN を作成するために、コントローラの GUI で [WLANs] をクリックします。[WLANs] ウィンドウが表示されます。このウィンドウには、コントローラに設定されている WLAN の一覧が表示されます。
2. 新しい WLAN を設定するために [New] をクリックします。この例では、WLAN に MAC-ACS-WLAN と名前を付けており、WLAN ID は 2 です。

WLANs > New

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

3. [Apply] をクリックします。
4. [WLAN] > [Edit] ウィンドウで、WLAN 固有のパラメータを定義します。[Security Policies] > [Layer 2 Security] で、[MAC Filtering] チェックボックスにチェックマークを付けます。これにより、WLAN に対して MAC 認証が有効になります。[General Policies] > [Interface Name] で、WLAN をマッピングするインターフェイスを選択します。RADIUS servers で、MAC 認証に使用する RADIUS サーバを選択します。

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
Server 2	None	None
Server 3	None	None

注: WLAN > Edit ウィンドウで RADIUS サーバを選択する前に、Security > Radius Authentication ウィンドウで RADIUS サーバを定義し、RADIUS サーバを有効にする必要があります。

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

WLAN の設計要件に応じて、その他のパラメータを選択します。[Apply] をクリックします。

General	Security	QoS	Advanced
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 <input type="button" value="v"/>		
Interface	management <input type="button" value="v"/>		
Broadcast SSID	<input checked="" type="checkbox"/> Enabled		

5. [Security] > [MAC Filtering] をクリックします。
6. MAC Filtering ウィンドウの RADIUS Compatibility Mode で、RADIUS サーバの種類を選択します。この例では Cisco ACS を使用しています。
7. MAC Delimiter プルダウン メニューから、MAC デリミタを選択します。この例では Colon を使用しています。
8. [Apply] をクリックします。

MAC Filtering

RADIUS Compatibility Mode	Cisco ACS <input type="button" value="v"/>	(In the Radius Access Reques MAC address.)
MAC Delimiter	Colon <input type="button" value="v"/>	

次に、クライアントの MAC アドレスを使用して ACS サーバを設定します。

クライアントの MAC アドレスを使用した RADIUS サーバの設定

ACS に MAC アドレスを追加するには、次の手順を実行します。

1. ACS サーバで WLC を AAA クライアントとして定義します。ACS の GUI で [Network Configuration] をクリックします。
2. Network Configuration ウィンドウが表示されたら、WLC の名前、IP アドレス、共有秘密鍵、認証方式 (RADIUS Cisco Aironet または RADIUS Airespace) を定義します。ACS 以外の他の認証サーバについては、メーカーのマニュアルを参照してください。

Network Configuration

Add AAA Client

AAA Client Hostname:

AAA Client IP Address:

Key:

Authenticate Using:

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

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

注: WLC と ACS サーバで設定する共有秘密キーは一致している必要があります。共有秘密では、大文字と小文字が区別されます。

3. ACS のメイン メニューで、**User Setup** をクリックします。

4. ユーザ データベースに追加する MAC アドレスを User テキスト ボックスに入力します。

User Setup

User:

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

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

注: この MAC アドレスは、ユーザ名とパスワードの両方に関して WLC によって送信されるものと完全に一致している必要があります。認証に失敗する場合は、ログを参照して MAC が WLC によってどのように報告されているかを確認してください。誤った文字が混入する可能性があるため、MAC アドレスをカット アンド ペーストで入力しないでください。

5. User Setup ウィンドウで、Secure-PAP password テキスト ボックスに MAC アドレスを入力します。

The screenshot shows the Cisco User Setup GUI. The main window is titled "User Setup" and displays configuration for a new user named "00:40:96:AC:E6:57". A checkbox labeled "Account Disabled" is visible. The "User Setup" section is highlighted with a red box and 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.):** This section contains two text input fields: "Password" and "Confirm Password".
- Separate (CHAP/MS-CHAP/ARAP):** This section contains two text input fields: "Password" and "Confirm Password".

Below the input fields, 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".

The right sidebar contains a "Help" section 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, and RADIUS Vendor-Specific Attributes.

At the bottom right, there is an "Account Disabled Status" section with the instruction: "Select the Account Disabled check box to disable this".

注: この MAC アドレスは、ユーザ名とパスワードの両方に関して WLC によって送信されるものと完全に一致している必要があります。認証に失敗する場合は、ログを参照して MAC が AP によってどのように報告されているかを確認してください。誤った文字が混入する場合がありますため、MAC アドレスをカット アンド ペーストで入力しないでください。

6. [Submit] をクリックします。
7. さらに多くのユーザを ACS データベースに追加するには、ステップ 2 ~ 5 を繰り返します。クライアントがこの WLAN に接続すると、WLC から ACS サーバにクレデンシャルが渡されます。ACS サーバは、ACS データベースに対してこれらのクレデンシャルを照合します。クライアントの MAC アドレスがデータベースに存在する場合は、ACS RADIUS サーバから WLC に認証成功のメッセージが返され、クライアントは WLAN へのアクセスを許可されます。

WLC で MAC フィルタを設定する CLI の使用

このドキュメントの前半で、WLC GUI を使用して MAC フィルタを設定する方法を説明しました。WLC で MAC フィルタを設定するには CLI を使用することもできます。WLC で MAC フィルタを設定するには、次のコマンドを使用できます：

- MAC フィルタリングをイネーブルにするには、`config wlan mac-filtering enable wlan_id` コマンドを実行します。WLAN での MAC フィルタリングをイネーブルにしたことを確認するには、`show wlan` コマンドを入力します。
- `config macfilter add` コマンド：`config macfilter add` コマンドにより、MAC フィルタ、インターフェイス、説明などを追加することができます。シスコワイヤレス LAN コントローラで MAC フィルタ エントリを作成するには、`config macfilter add` コマンドを使用します。シスコワイヤレス LAN コントローラの無線 LAN にクライアントをローカルに追加するには、このコマンドを使用します。このフィルタは RADIUS 認証プロセスをバイパスします。

`config macfilter add MAC_address wlan_id [interface_name] [description] [IP address]` **例**
: MAC-to-IP 静的アドレス マッピングを入力します。これはパッシブのクライアントをサポートするために実行できます。パッシブのクライアントとは、DHCP を使用せず、未承諾の IP パケットを送信していないクライアントです。>`config macfilter add 00:E0:77:31:A3:55 1 lab02 "labconnect" 10.92.125.51`

- `config macfilter ip-address` コマンド `config macfilter ip-address` コマンドは IP アドレスに既存の MAC フィルタをマップすることができます。ローカル MAC フィルタ データベースに IP アドレスを設定するには、次のコマンドを使用してください :

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

無効なクライアントのタイムアウトの設定

無効なクライアントに対してタイムアウトを設定できます。アソシエートしようとした際に認証で 3 回失敗したクライアントは、それ以降のアソシエーションの試みでは自動的に無効にされます。タイムアウト期間が経過すると、クライアントは認証の再試行を許可され、アソシエートすることができます。このとき、認証に失敗すると再び排除されます。

無効なクライアントのタイムアウトを設定するには、`config wlan exclusionlist wlan_id timeout` コマンドを入力します。タイムアウト値は 1 ~ 65535 秒です。または完全にクライアントを無効化するには、0 を入力することもできます。

確認

MAC フィルタが正しく設定されているかどうかを確認するには、次のコマンドを使用します。

[Output Interpreter Tool](#) (OIT) ([登録ユーザ専用](#)) では、特定の `show` コマンドがサポートされています。OIT を使用して、`show` コマンド出力の解析を表示できます。

- `show macfilter summary` : すべての MAC フィルタ エントリの概要が表示されます。
- `show macfilter detail <client MAC Address>` : 特定の MAC フィルタ エントリの詳細が表示されます。

次に `show macfilter summary` コマンドの例を示します。

```
(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
```

次に `show macfilter detail` コマンドの例を示します。

```
(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
```

トラブルシューティング

設定のトラブルシューティングを行うには、次のコマンドを使用できます。

注: [debug](#) コマンドを使用する前に、『[debug コマンドの重要な情報](#)』を参照してください。

- `debug aaa all enable` : すべての AAA メッセージのデバッグを行います。

- `debug mac addr <Client-MAC-address xx: xx: xx: xx: xx>` : MAC のデバッグを設定するには、`debug mac` コマンドを使用します。

次に `debug aaa all enable` コマンドの例を示します。

```
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'
```

無線クライアントが WLC 上の MAC アドレス データベース (ローカル データベース) に存在しない場合、または RADIUS サーバが WLAN への関連付けを試みた場合、そのクライアントは除外されます。次に、MAC 認証に失敗する場合の `debug aaa all enable` コマンドの例を示します。

```
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:
```

MAC アドレスによる認証を試みた無線クライアントの拒否 : 失敗した認証のレポートでの内部エラーの表示

Microsoft Windows 2003 Enterprise サーバ上で実行されている ACS 4.1 を使用している場合、MAC アドレスによる認証を試みたクライアントは拒否されます。この現象は AAA クライアントから AAA サーバに Service-Type=10 属性値が送信されるときに発生します。これは、Cisco Bug ID [CSCsh62641](#) ([登録ユーザ専用](#)) が原因です。このバグの影響を受ける AAA クライアントには、MAC 認証バイパスを使用するスイッチや WLC が含まれます。

回避策は次のとおりです。

- ACS 4.0 にダウングレードする。または
- 内部 ACS DB MAC アドレス テーブルの Network Access Protection (NAP) に、認証する MAC アドレスを追加する。

WLC の GUI を使用して MAC フィルタを追加できない

この問題は、Cisco Bug ID [CSCsj98722](#) ([登録ユーザ専用](#)) によるものです。この不具合は、リリース 4.2 のコードで修正されています。4.2 より古いバージョンを実行している場合は、ファ

ームウェアを 4.2 にアップグレードするか、この問題に対する下記 2 つの回避策を使用できます。

- CLI で、次のコマンドにより MAC フィルタを設定する。
`config macfilter add <MAC address> <WLAN ID#> <Interface>`
- コントローラの GUI で、[Security] タブにある [Any WLAN] を選択し、フィルタを適用する MAC アドレスを入力する。

RUN 状態にないサイレント クライアント

要求された DHCP がコントローラで設定されていない場合、ワイヤレス クライアントが最初の IP パケットまたは ARP を送信すると、AP はワイヤレス クライアントの IP アドレスを取得します。ワイヤレス クライアントがパッシブ デバイス (通信を開始しないデバイスなど) の場合、AP は、ワイヤレス デバイスの IP アドレスの取得に失敗します。そのため、コントローラはクライアントが IP パケットを送信するまで 10 秒間待ちます。クライアントからのパケットから応答がない場合、コントローラはパッシブのワイヤレス クライアントにパケットをドロップします。この問題は、Cisco Bug ID [CSCsq46427](#) ([登録ユーザ専用](#)) に記述されています。

プリンタやワイヤレス PLC ポンプなどのパッシブ デバイスの推奨されている回避策として、これらのデバイスの接続を可能にするには、MAC フィルタリングの WLAN を設定し、AAA のオーバーライドを検査する必要があります。

MAC アドレス フィルタは、ワイヤレス デバイスの MAC アドレスを IP アドレスへマッピングするコントローラで作成できます。

注: これには、レイヤ 2 セキュリティの WLAN 設定で MAC アドレス フィルタリングをイネーブルにする必要があります。また、Allow AAA Override を WLAN 設定の詳細設定でイネーブルにする必要があります。

CLI から、MAC アドレス フィルタを作成するには、次のコマンドを入力してください：

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

次に例を示します。

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

関連情報

- [Wireless LAN Controller での ACL の設定例](#)
- [ワイヤレス LAN コントローラでの認証の設定例](#)
- [無線 LAN コントローラでの VLAN の設定例](#)
- [Cisco Wireless LAN Controller コンフィギュレーション ガイド、リリース 4.1](#)
- [ワイヤレス テクノロジーに関するサポート ページ](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)