AireOSワイヤレスLANコントローラ(WLC)でのMACフィルタの設定

内容

はじめに

このドキュメントでは、ワイヤレスLANコントローラ(WLC)でMACフィルタを設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- LAPおよびCisco WLCの設定
- Cisco Unified Wirelessセキュリティソリューション

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いています。

- 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ました。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。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

表記法

表記法の詳細については、『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。

背景説明

このドキュメントでは、ワイヤレスLANコントローラ(WLC)でMACフィルタを設定する方法について、設定例を使用して説明します。このドキュメントでは、AAA サーバに対して Lightweight アクセス ポイント（LAP）を認可する方法について説明します。

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サーバで使用される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と、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

これらすべてのタイプのユーザは、設定された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。

```
<#root>

<Cisco Controller>

config database size ?

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

または、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認証を設定する前に、WLCを基本動作用に設定し、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。新規ユーザが、WLCでLAPとの基本動作用に設定を試みる場合は、『WLCに加入できないLightweight APのトラブルシューティング』を参照してください。

> 注:MAC認証をサポートするためにワイヤレスクライアントで必要な特別な設定はありません。

WLAN の設定と MAC フィルタリングの有効化

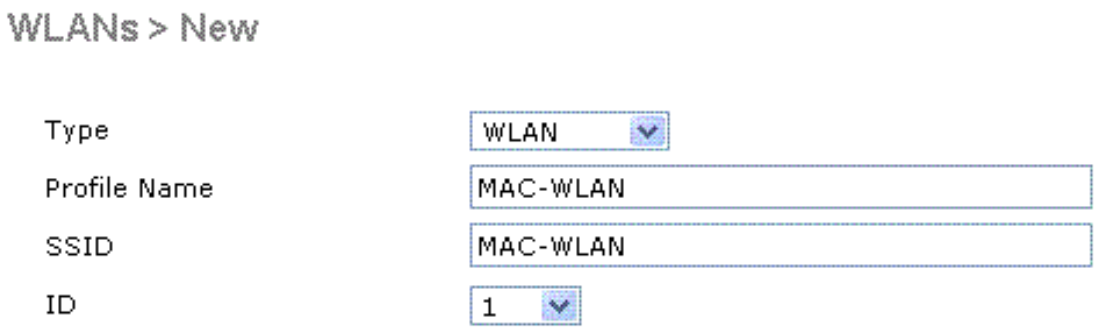
MACフィルタリングを使用してWLANを設定するには、次の手順を実行します。

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。

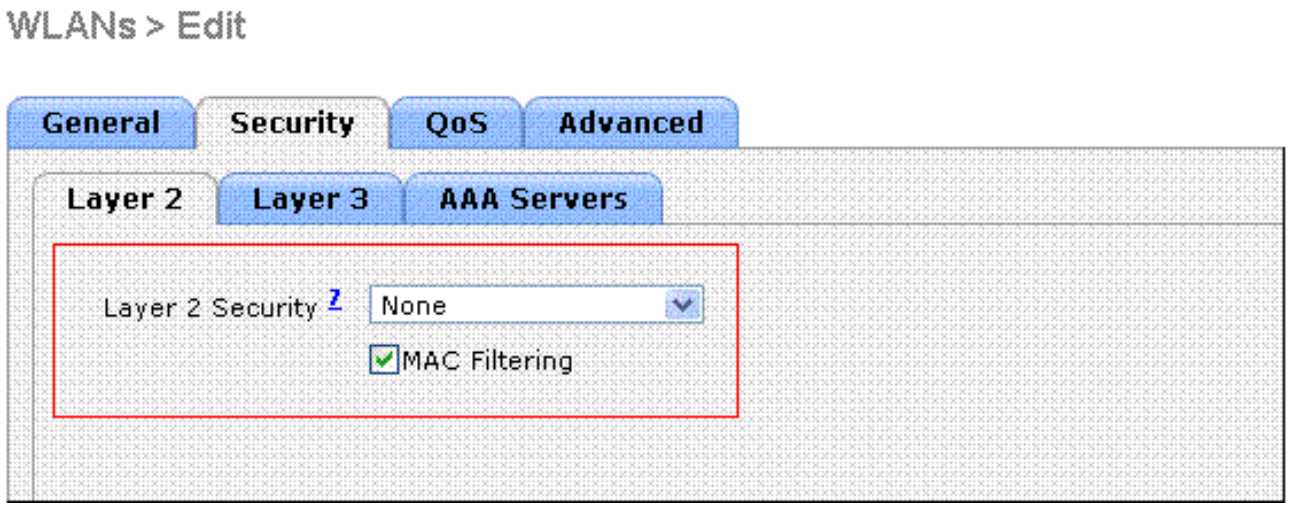
   この例では、WLAN に MAC-WLAN と名前を付けており、WLAN ID は 1 です。



WLANの設定MACフィルタリングの有効化

3. [APPLY] をクリックします。

4. WLANs > Editウィンドウで、WLANに固有のパラメータを定義します。



パラメータの定義

   a. Security > Layer 2 > Layer 2 Security Policiesの下で、MAC Filteringチェックボックスにチェックマークを付けます。

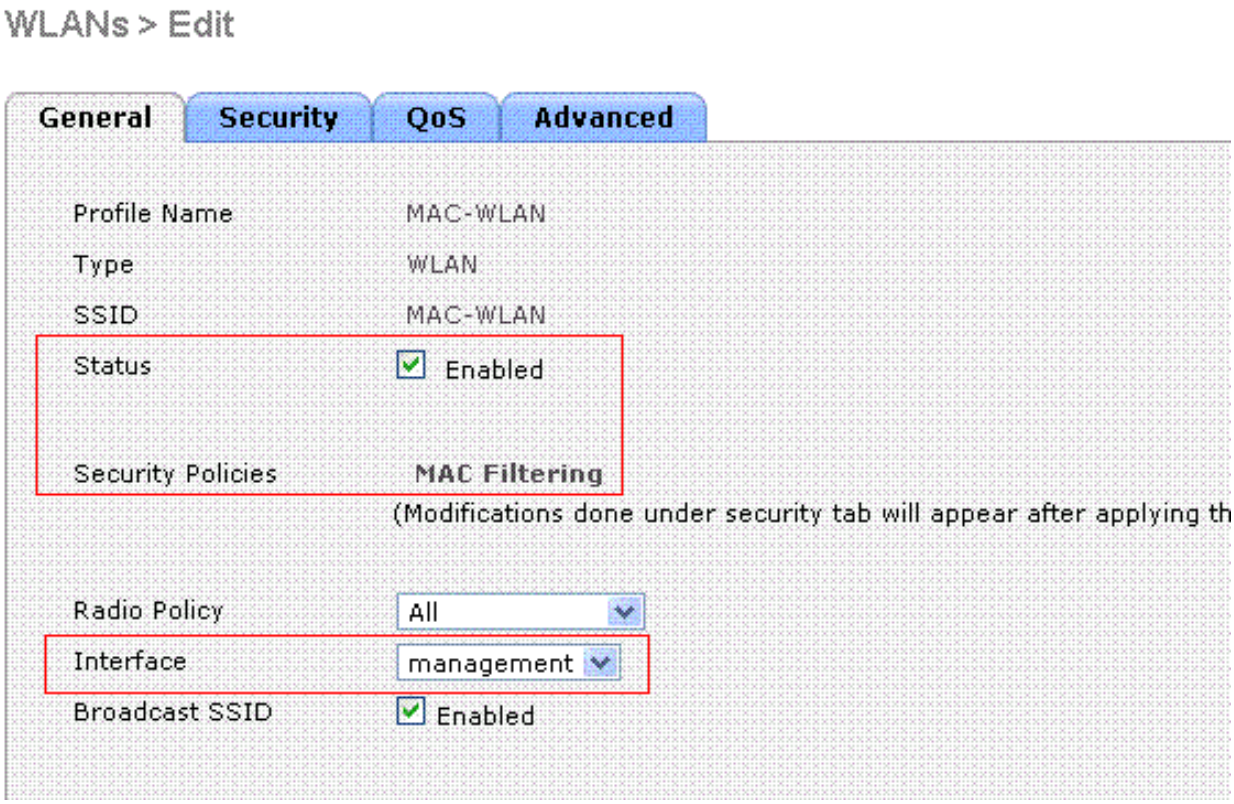
      これにより、WLAN に対して MAC 認証が有効になります。

   b. General > Interface nameで、WLANがマッピングされてい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。

c. 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。

d. [APPLY] をクリックします。



インターフェイスにマッピングされたWLAN

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。

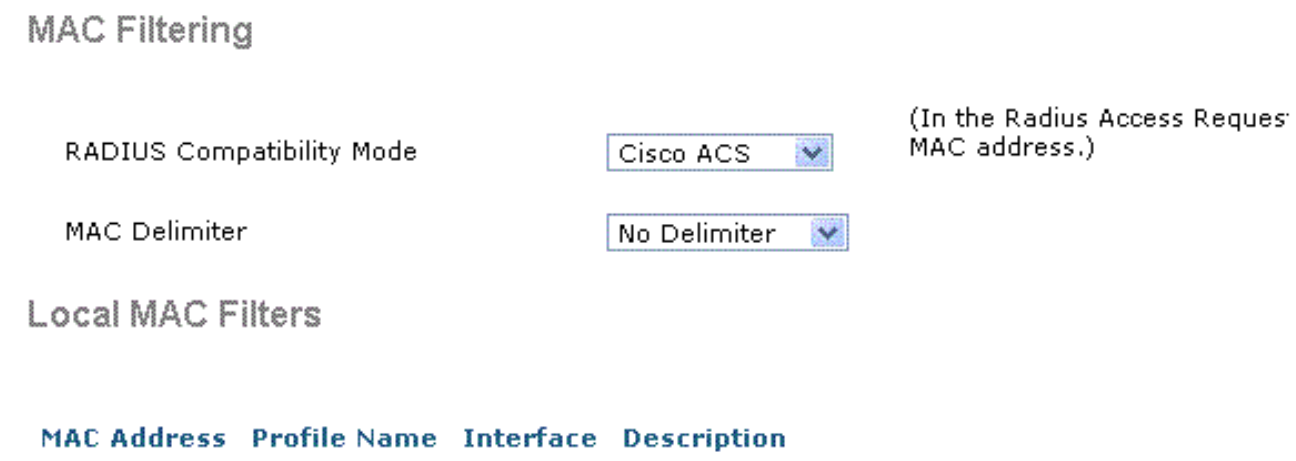
WLC でダイナミック インターフェイス（VLAN）を設定する方法については、『無線 LAN コントローラでの VLAN の設定例（VLANs on Wireless LAN Controllers Configuration Example）』を参照してください。

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。

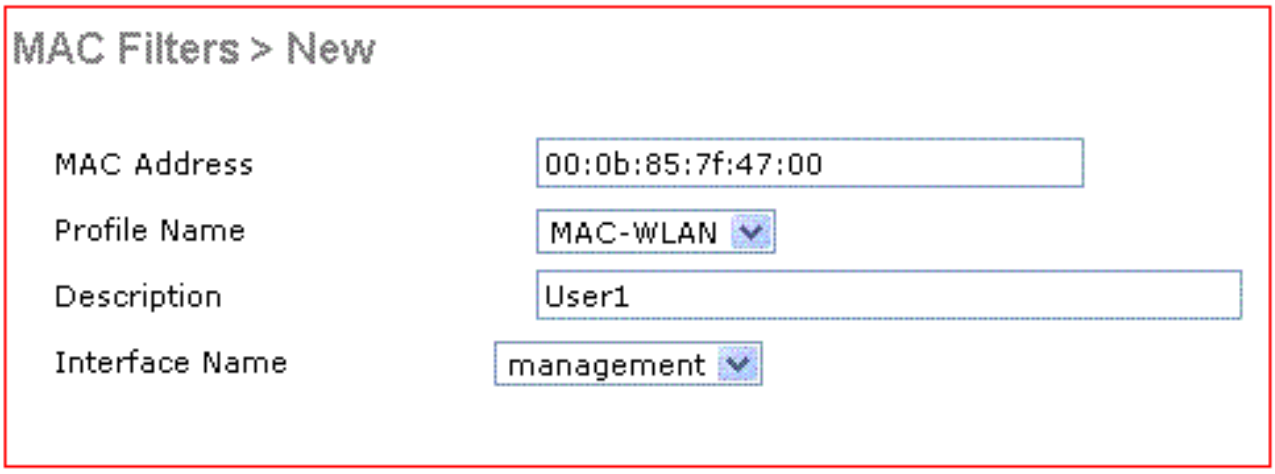


MACフィルタリングウィンドウ

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。

   ランダム データの例は次のとおりです。



MACアドレス用のローカルデータベースの作成

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アドレスフィルタのみが使用されています。シスコでは、MACアドレス認証を他のレイヤ2またはレイヤ3セキュリティ方式とともに使用することを推奨しています。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サーバでMAC認証を設定するには、次のリンクを使用します。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

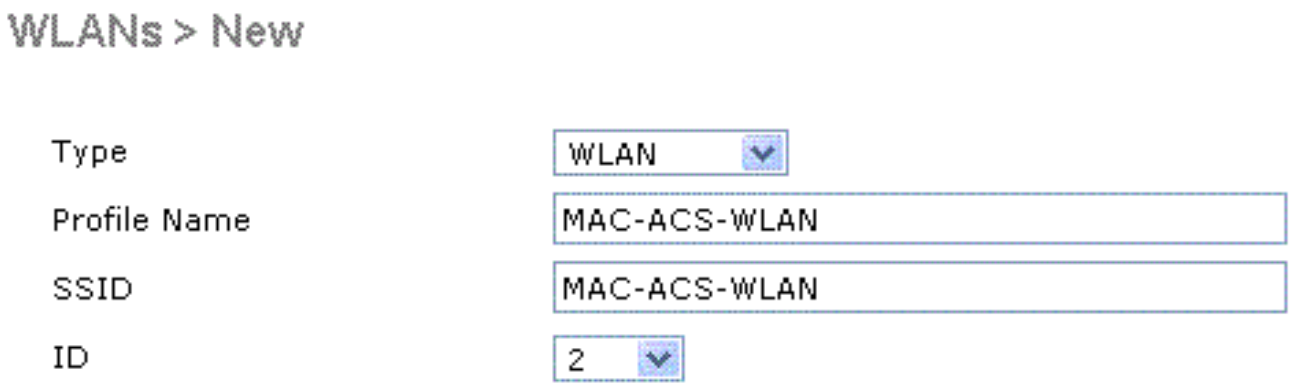
MACフィルタリングを使用してWLANを設定するには、次の手順を実行します。

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。



新しいWLANの設定によるMACフィルタリングの有効化

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

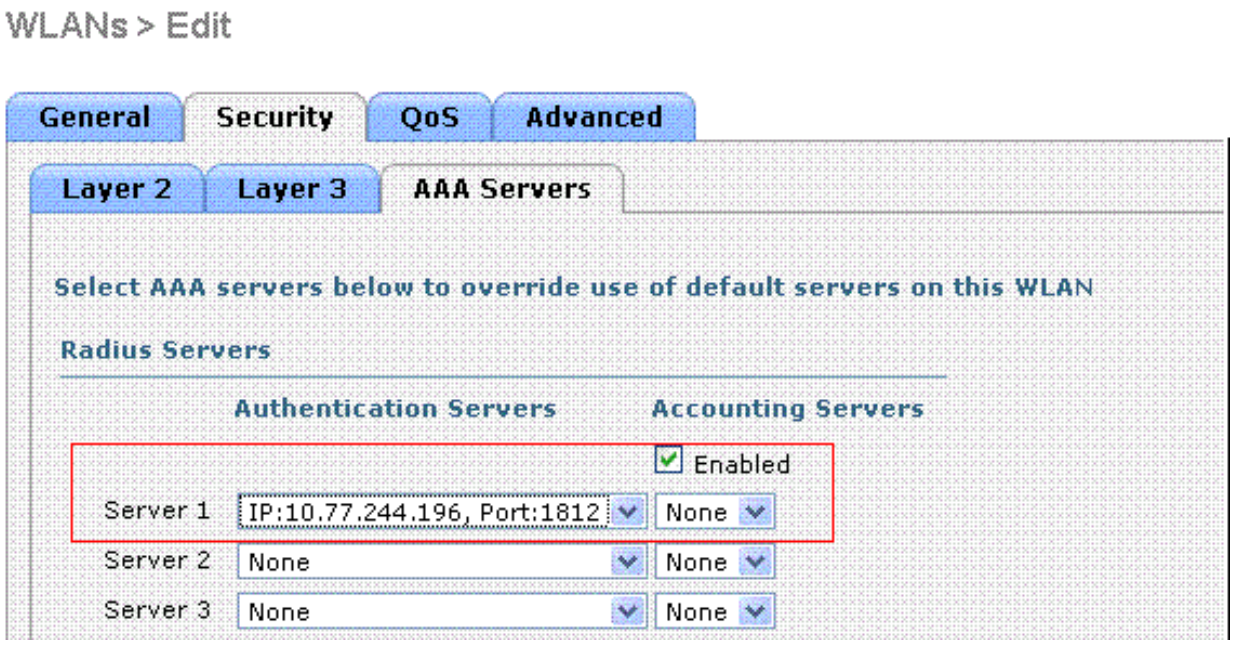
   a. Security > Layer 2 > Layer 2 Security Policiesの下で、MAC Filteringチェックボックス

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。

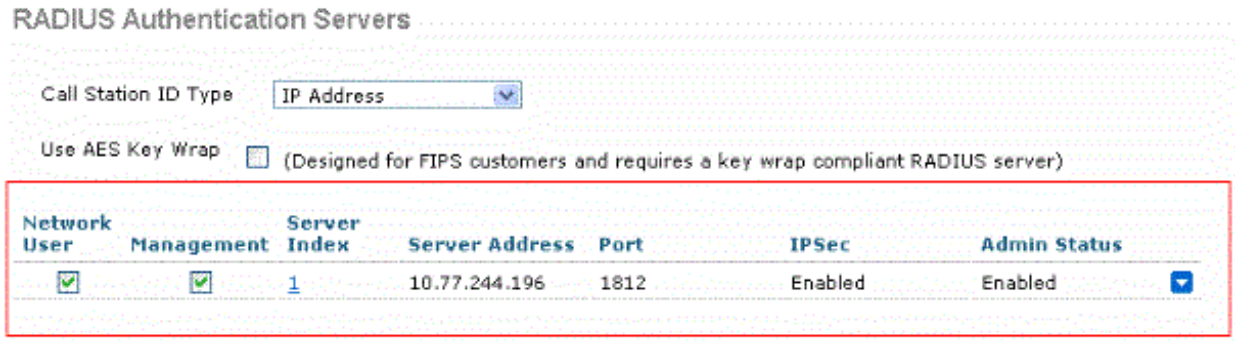
b. General > Interface nameで、WLANがマッピングされているインターフェイスを選択します。

c. Security > AAA Servers > RADIUS serversの順に選択し、MAC認証に使用できるRADIUSサーバを選択します。



MAC認証に使用するRADIUSサーバを選択します。

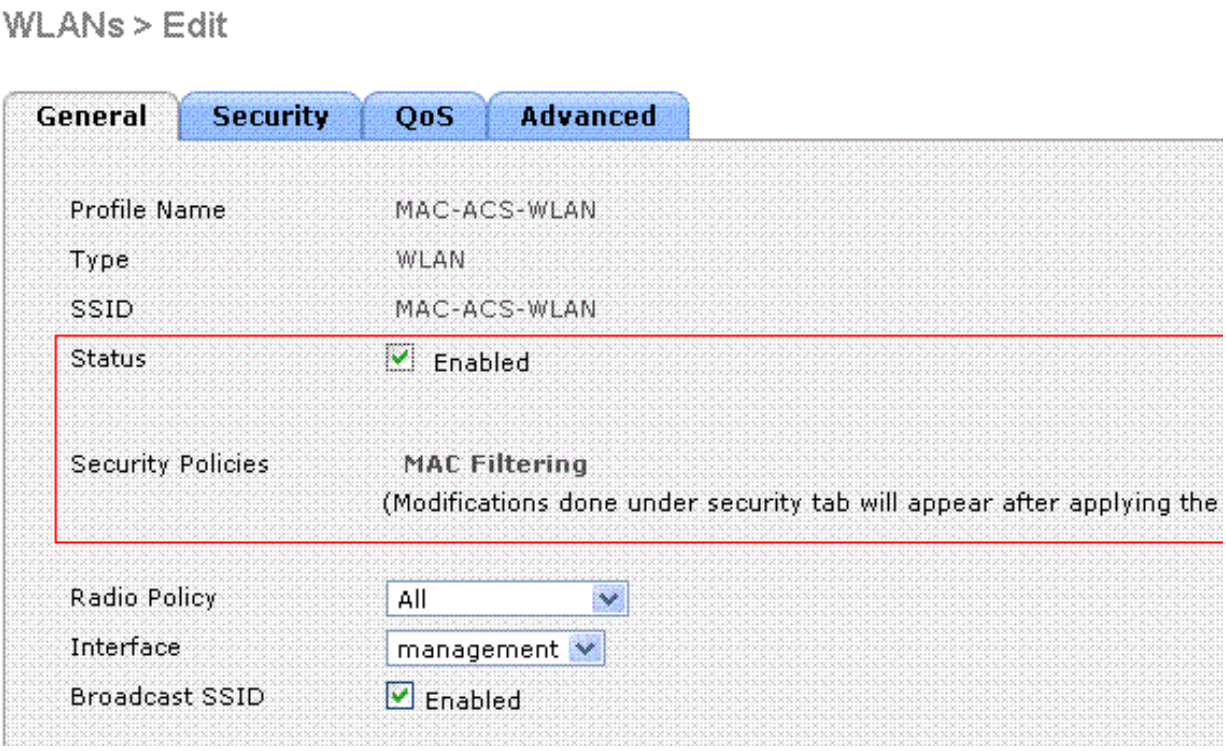
注:WLAN > EditウィンドウでRADIUSサーバを選択する前に、Security > Radius AuthenticationウィンドウでRADIUSサーバを定義し、RADIUSサーバを有効にする必要があります。



Radius認証サーバ

d. 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。

e. [APPLY] をクリックします。

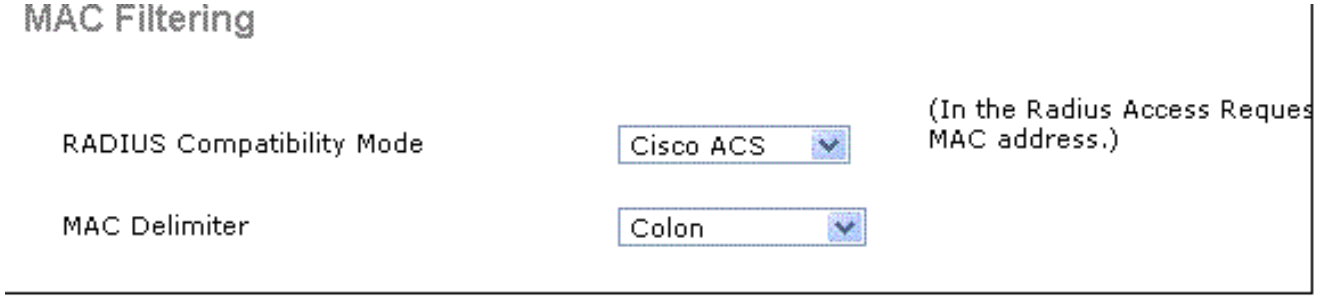


設計要件パラメータ

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。



RADIUSサーバタイプの選択

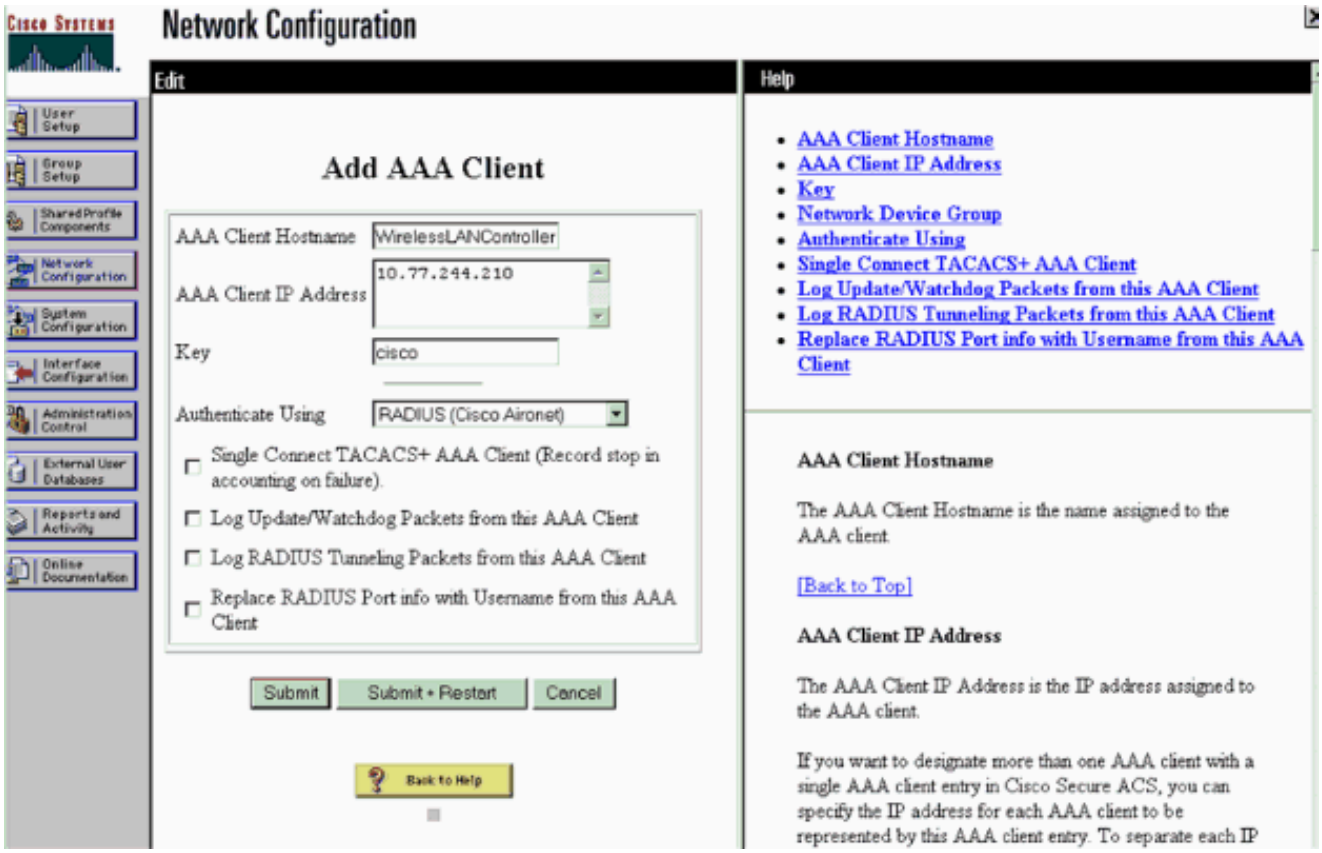
次に、クライアントの MAC アドレスを使用して ACS サーバを設定します。

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。

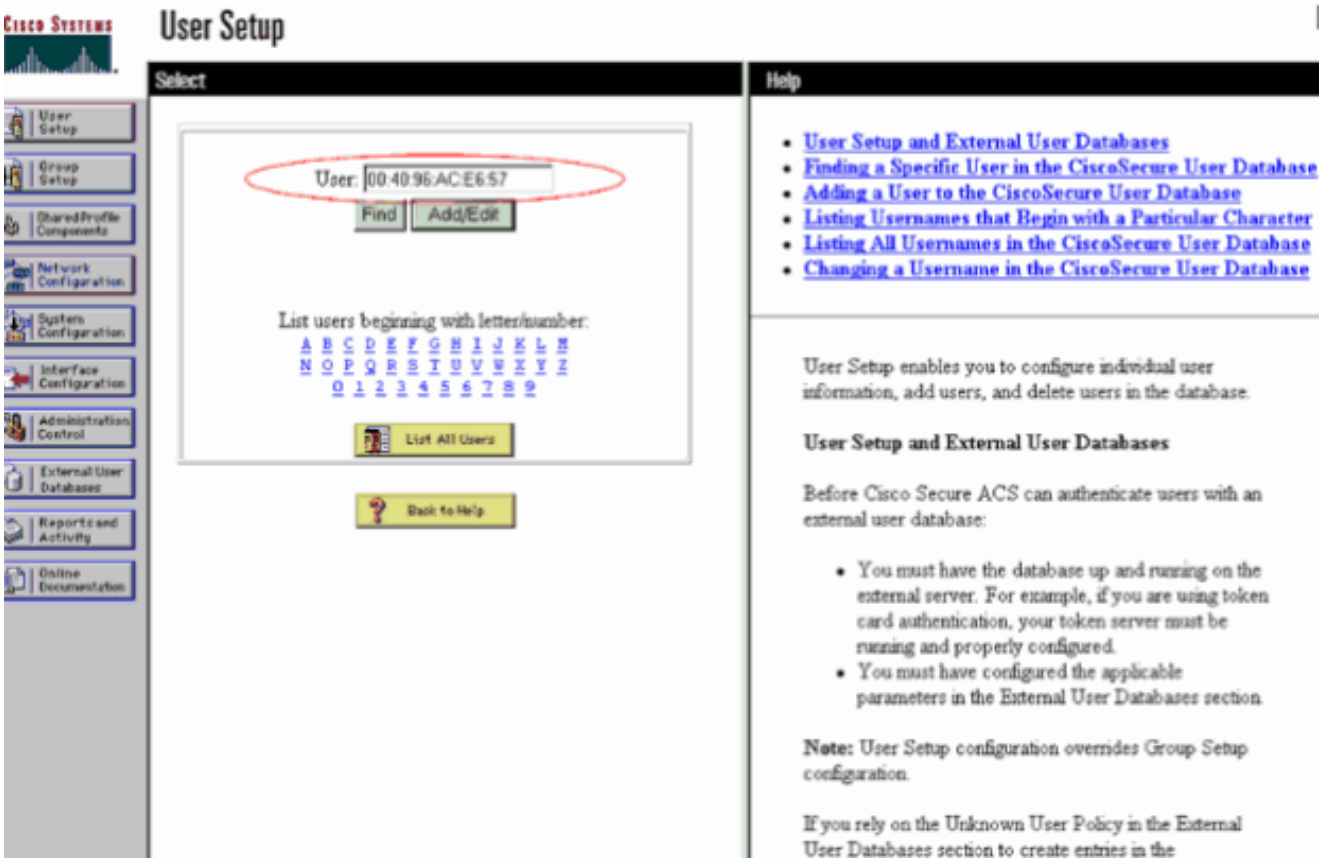
   ACS 以外の他の認証サーバについては、メーカーのマニュアルを参照してください。



AAAクライアントの追加

> 注:WLCに設定する共有秘密キーとACSサーバは一致する必要があります。共有秘密では、大文字と小文字が区別されます。

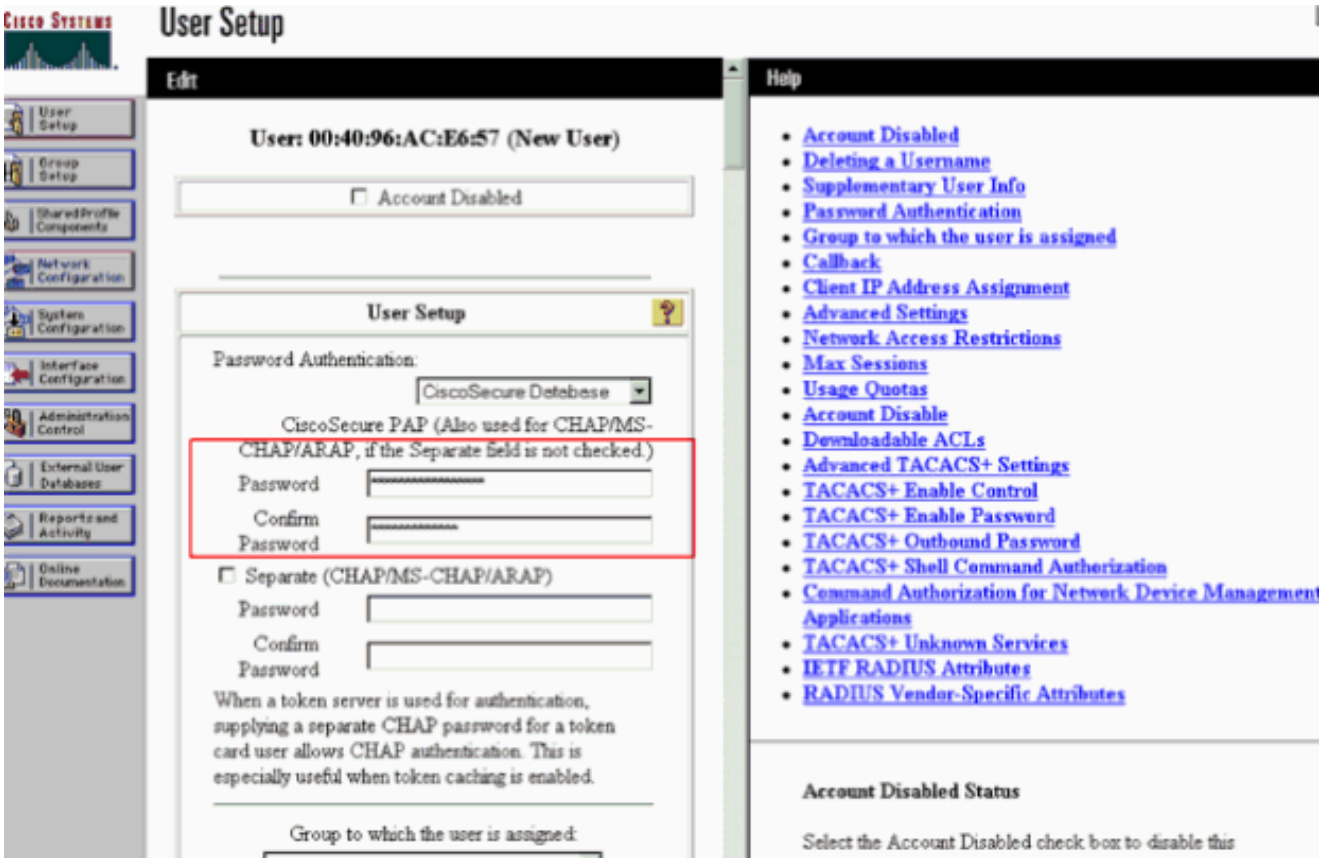
3. ACS のメイン メニューで、[User Setup] をクリックします。
4. ユーザ データベースに追加する MAC アドレスを User テキスト ボックスに入力します。



MACアドレスを入力します

注:MACアドレスは、ユーザ名とパスワードの両方についてWLCから送信されるものと正確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場合があるため、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。



Secure-PAP PasswordフィールドにMACアドレスを入力する

> 注:MACアドレスは、ユーザ名とパスワードの両方についてWLCから送信されるものと正確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。

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、ACS RADIUSサーバはWLCに認証成功を返し、クライアントにWLANへのアクセス権を付与できます。

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、次の手順を実行します。

- 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に対してMACフィルタリングが有効になっている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コマンドを使用すると、macfilter、インターフェイス、説明などを追加できます。

  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。

  <#root>

  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。

  <#root>

  (Cisco Controller) >

  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コマンドを使用すると、MACフィルタをIPアドレスにマッピングできます。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：

  <#root>

  config macfilter ip-address

  <MAC_address> <IP_address>

例

<#root>

(Cisco Controller) >

config macfilter ip-address

00:E0:77:31:A3:55 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、次の手順を実行します。

- 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。

<#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) >
```

次に、show macfilterの詳細コマンドの例を示します。

<#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
```

トラブルシュート

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:xx>:MACのデバッグを設定するには、debug maccommand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。

<#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'
```

ワイヤレスクライアントがWLC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は、そのクライアントを除外できます。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。

<#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:
```

エラー： MACアドレスによる認証を試みたワイヤレスクライアントが拒否され、認証失敗レポートに内部エラーが表示される

Microsoft Windows 2003 EnterpriseサーバでACS 4.1を使用すると、MACアドレスによる認証を試行する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。

エラー：WLC GUIでMACフィルタを追加できない

これは、Cisco Bug ID CSCsj98722が原因で発生します。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より前の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、この問題に対して次の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。

  <#root>

  config macfilter add

  <MAC_address> <WLAN_id> <Interface_name>

- 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。

エラー：サイレントクライアントが実行状態になっていません

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に記載されています。

注：内部ツールおよび情報にアクセスできるのは、登録済みのシスコユーザーのみです。

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：このためには、レイヤ2セキュリティ用のWLAN設定でMACアドレスフィルタリングを有効にする必要があります。また、WLAN設定の詳細設定で`Allow AAA Override`を有効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>
```

ランダム データの例は次のとおりです。

```
<#root>

(Cisco Controller) >

 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廃止のお知らせ
- ワイヤレス テクノロジーに関するサポート ページ
- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。