RADIUS サーバおよびワイヤレス LAN コントローラを使用したダイナミック VLAN 割り当ての設定例

目次

概要

このドキュメントでは、ダイナミック VLAN 割り当ての概念について説明します。 また、Wireless LAN（WLAN; ワイヤレス LAN）クライアントを特定の VLAN にダイナミックに割り当てるようにワイヤレス LAN コントローラ（WLC）および RADIUS サーバを設定する方法について説明します。

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。

- WLC および Lightweight アクセス ポイント（LAP）に関する基本的な知識があること
- AAA サーバに関する実務的な知識があること

- ワイヤレス ネットワークとワイヤレスのセキュリティ問題に関する全般的な知識があること
- Lightweight AP Protocol（LWAPP; Lightweight AP プロトコル）に関する基本的な知識があること

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。

- ファームウェア リリース 5.2 が稼動している Cisco 4400 WLC
- Cisco 1130 シリーズ LAP
- ファームウェア リリース 4.4 が稼動している Cisco 802.11a/b/g ワイヤレス クライアント アダプタ
- バージョン 4.4 が稼動している Cisco Aironet Desktop Utility（ADU）
- バージョン 4.1 が稼動している CiscoSecure Access Control Server（ACS）
- Cisco 2950 シリーズ スイッチ

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。

RADIUS サーバによるダイナミック VLAN 割り当て

一般的な WLAN システムでは、Service Set Identifier（SSID）（コントローラの用語では WLAN）に関連付けられたすべてのクライアントに適用されるスタティックなポリシーが各 WLAN に存在します。 この方式は強力ですが、異なる QoS ポリシーやセキュリティ ポリシーを継承するために各クライアントを異なる SSID に関連付ける必要があるので、さまざまな制約があります。

一方、Cisco WLAN ソリューションでは、アイデンティティ ネットワーキングがサポートされています。 この場合、ネットワーク上で 1 つの SSID のみをアドバタイズすることにより、特定のユーザはユーザ クレデンシャルに基づいて異なる QoS ポリシーやセキュリティ ポリシーを継承できるようになります。

ダイナミック VLAN 割り当ては、ユーザが入力したクレデンシャルに基づいてワイヤレス ユーザを特定の VLAN に割り当てる機能です。 ユーザを特定の VLAN に割り当てるタスクは、CiscoSecure ACS などの RADIUS 認証サーバによって処理されます。 たとえば、この機能を利用すると、キャンパス ネットワーク内を移動するワイヤレス ホストを同じ VLAN に割り当てることができます。

したがって、クライアントがコントローラに登録済みの LAP への関連付けを試みると、LAP から RADIUS サーバにユーザのクレデンシャルが渡されて検証されます。 認証に成功すると、RADIUS サーバからユーザに特定の Internet Engineering Task Force（IETF）属性が渡されます。 これらの RADIUS 属性により、ワイヤレス クライアントに割り当てられる VLAN ID が決定されます。 ユーザはこの事前設定済みの VLAN ID に常に割り当てられるので、クライアントの SSID（WLC の用語では WLAN）は無視されます。

VLAN ID の割り当てに使用される RADIUS ユーザ属性は次のとおりです。

- IETF 64（Tunnel Type）：これを VLAN に設定します。
- IETF 65（Tunnel Medium Type）：これを 802 に設定します。
- IETF 81（Tunnel Private Group ID）：これを VLAN ID に設定します。

VLAN ID は 12 ビットで、1 ~ 4094 の値（両端を含む）を取ります。 トンネル Private グループ ID がストリングとして IEEE 802.1X と併用するための RFC2868 で定義されたようにタイプ ストリング、VLAN ID 整数値情報符号化されるであるので。 これらのトンネル属性が送信される際には、Tag フィールドの値を設定する必要があります。

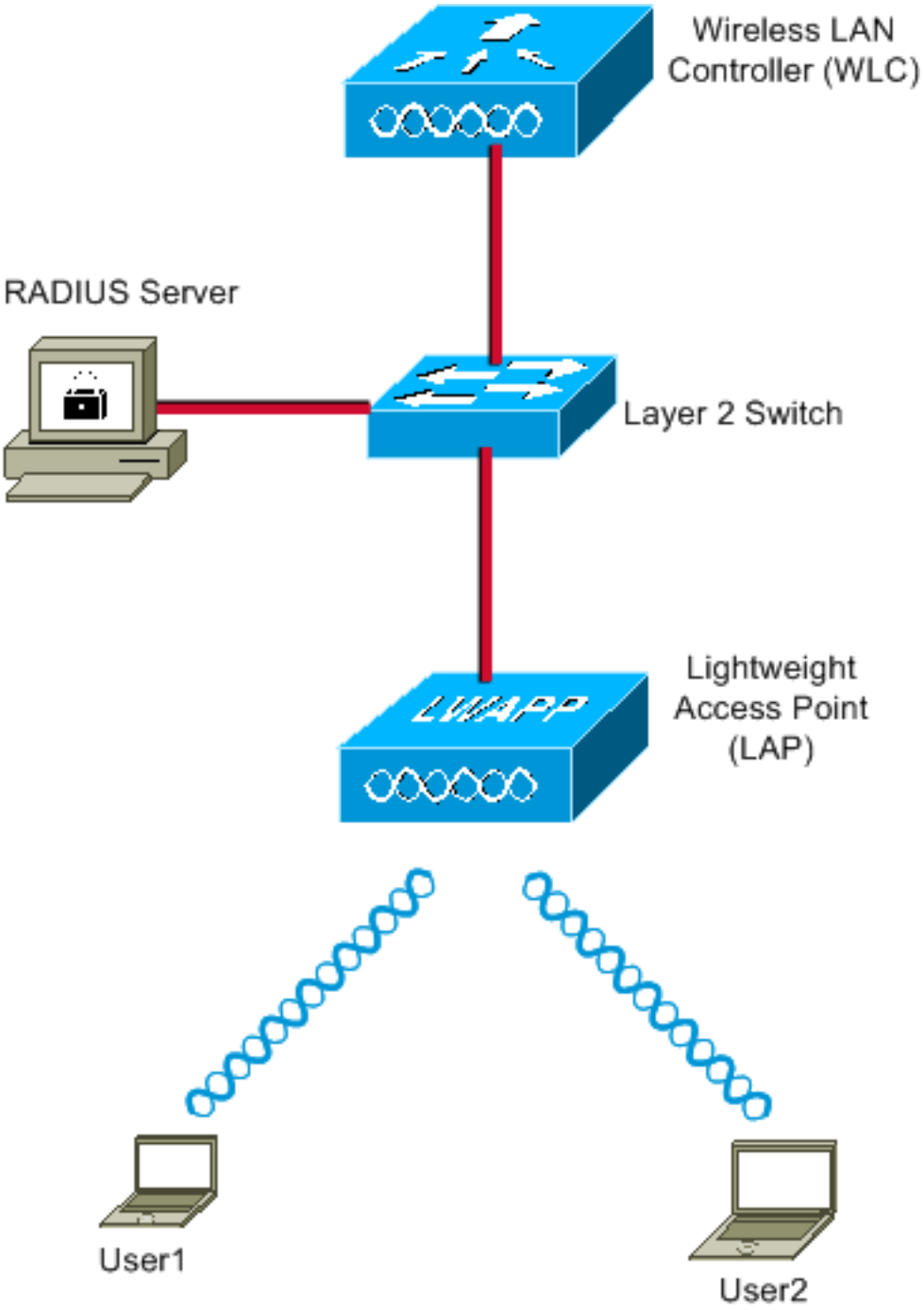
RFC2868 のセクション 3.1 で述べられているように、**Tag フィールドは 1 オクテットの長さを持ち、同じトンネルを参照する同じパケット内の属性をグループ化する手段を提供することを目的としています。** このフィールドで有効な値は、0x01 ~ 0x1F（両端を含む）です。 Tag フィールドを使用しない場合は、このフィールドをゼロ（0x00）に設定する必要があります。 すべての RADIUS 属性の詳細は、RFC 2868 を参照してください。

設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。



この図で使用されているコンポーネントの設定の詳細は、次のとおりです。

- ACS (RADIUS) サーバの IP アドレスは 172.16.1.1 です。
- WLC の管理インターフェイス アドレスは 172.16.1.30 です。
- WLC の AP マネージャ インターフェイス アドレスは 172.16.1.31 です。
- DHCPサーバ アドレス 172.16.1.1 が LWAPP に IP アドレスを割り当てるのに使用されています。 **コントローラの内部 DHCP サーバは、ワイヤレス クライアントに IP アドレスを割り当てる目的に使用されます。**
- VLAN10 および VLAN11 は、この設定全体を通じて使用されます。 RADIUS サーバにより user1 は VLAN10 に割り当てられ、user2 は VLAN11 に割り当てられるように設定されています。**注:** このドキュメントに記載されているのは、user1 に関連する全設定情報のみです。このドキュメントに記載されている手順を user2 に対しても実施してください。
- このドキュメントでは、セキュリティ メカニズムとして 802.1x と LEAP を使用します。**注** : WLAN をセキュアにするため、EAP-FAST や EAP-TLS などの高度な認証方式を使用することを推奨します。 このドキュメントでは、説明を簡単にするため、LEAP を使用しています

。

設定

このドキュメントでは、設定を開始する前に LAP が WLC にすでに登録されていることが前提となっています。 詳細は、『ワイヤレス LAN コントローラと Lightweight アクセス ポイントの基本設定例』を参照してください。 必要な登録手順については、『ワイヤレス LAN コントローラ（WLC）への Lightweight AP（LAP）の登録』を参照してください。

設定手順

この設定は、次の 4 つのカテゴリに分類されます。

1. RADIUS サーバの設定
2. 複数の VLAN を使用するためのスイッチの設定
3. WLC の設定
4. Wireless Client Utility の設定

RADIUS サーバの設定

設定には次の手順が必要です。

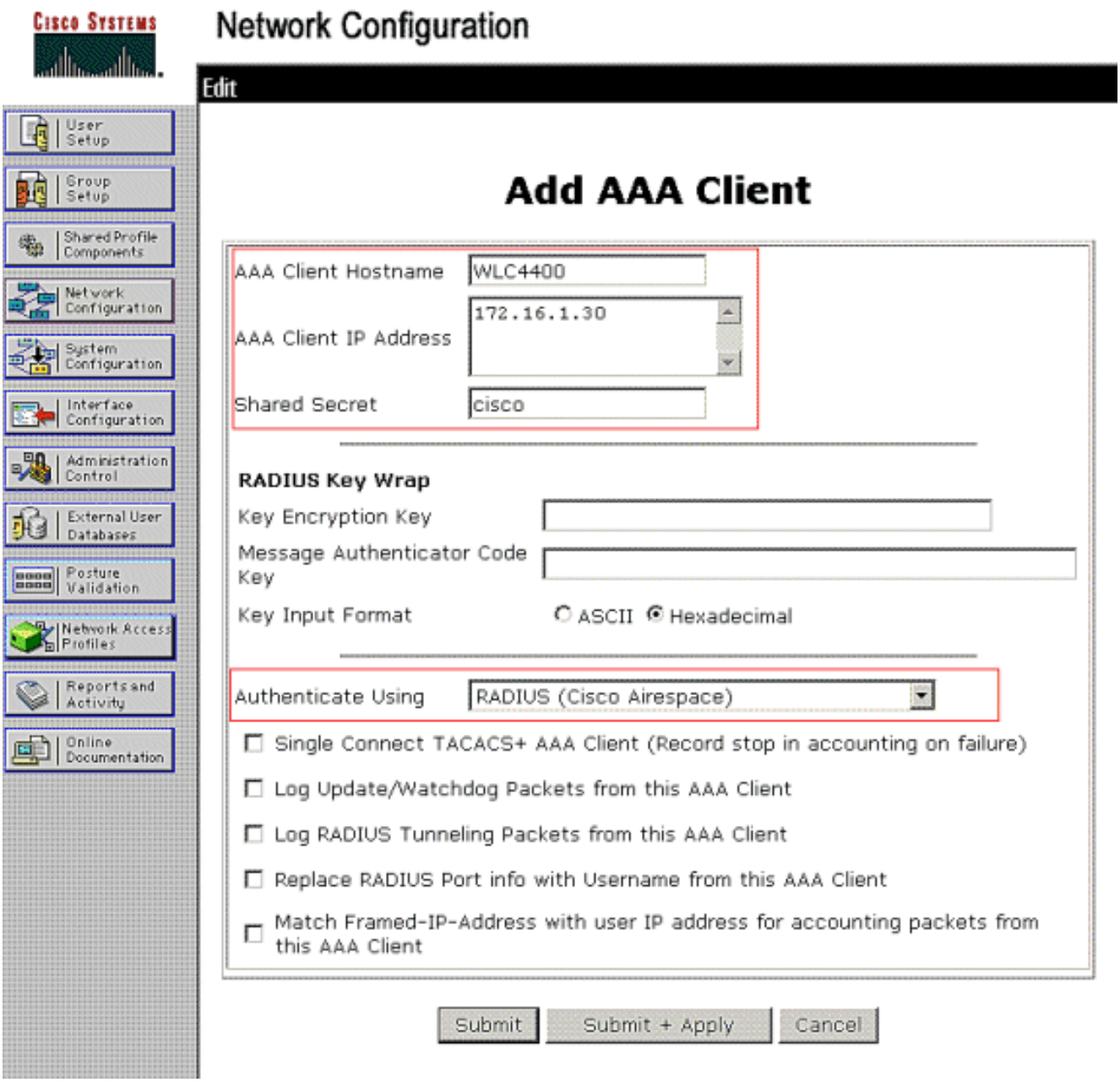
- RADIUSサーバの AAA クライアントで WLC を設定して下さい
- RADIUS サーバでのダイナミック VLAN 割り当てに使用するユーザと RADIUS（IETF）アトリビュートの設定

RADIUS サーバでの WLC の AAA クライアントの設定

この手順では、WLC から RADIUS サーバにユーザ クレデンシャルを渡せるように、RADIUS サーバで AAA クライアントとして WLC を追加する方法について説明します。

次の手順を実行します。

1. ACS の GUI で、[Network Configuration] をクリックします。
2. [AAA Clients] フィールドの下にある [**Add Entry**] セクションをクリックします。
3. AAA クライアントの IP アドレスとキーを入力します。ここで入力する IP アドレスは、WLC の管理インターフェイスの IP アドレスと一致している必要があります。ここで入力するキーは、[セキュリティ] ウィンドウで WLC に対して設定されているキーと一致している必要があります。 これは AAA クライアント（WLC）と RADIUS サーバの間の通信で使用される秘密キーです。
4. [Authenticate Using] フィールドで、認証タイプとして [RADIUS (Cisco Airespace)] を選択します。

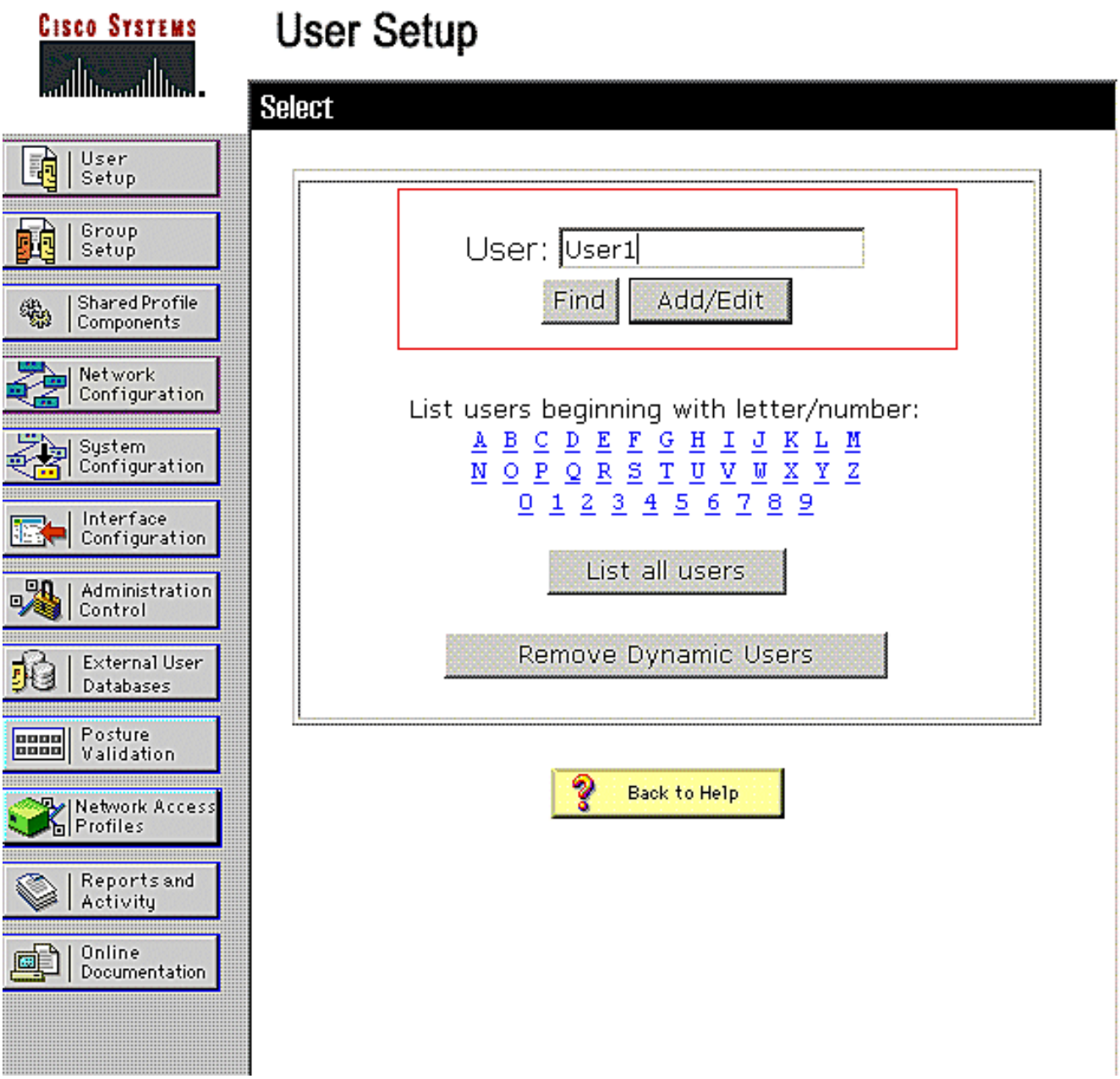


RADIUS サーバでのダイナミック VLAN 割り当てに使用するユーザと RADIUS (IETF) アトリビュートの設定

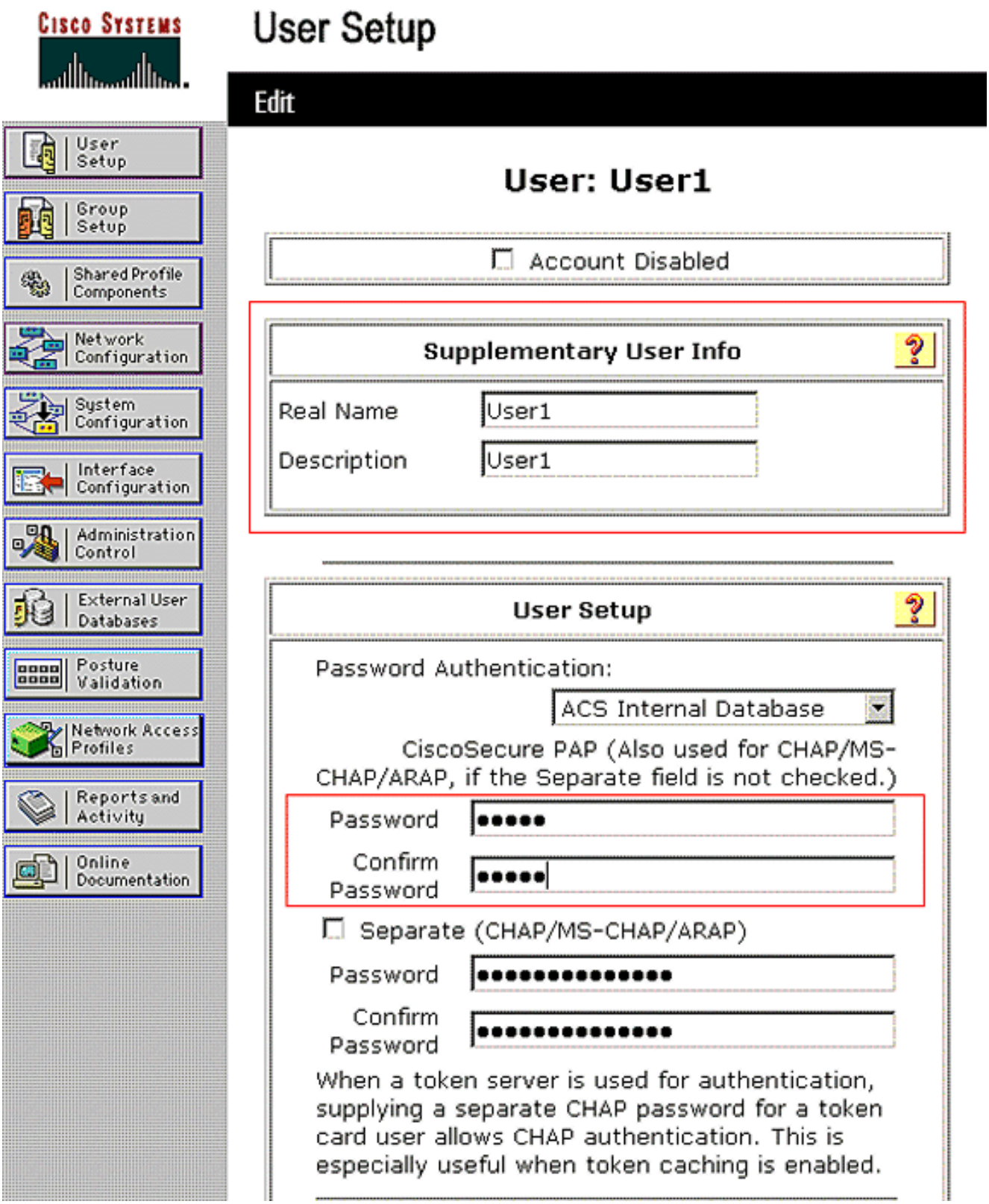
この手順では、RADIUS サーバのユーザと、それらのユーザに VLAN ID を割り当てるための RADIUS (IETF) アトリビュートを設定する方法について説明します。

次の手順を実行します。

1. ACS の GUI で、[**User Setup**] をクリックします。
2. [User Setup] ウィンドウで、[User] フィールドにユーザ名を入力し、[**Add/Edit**] をクリックします。

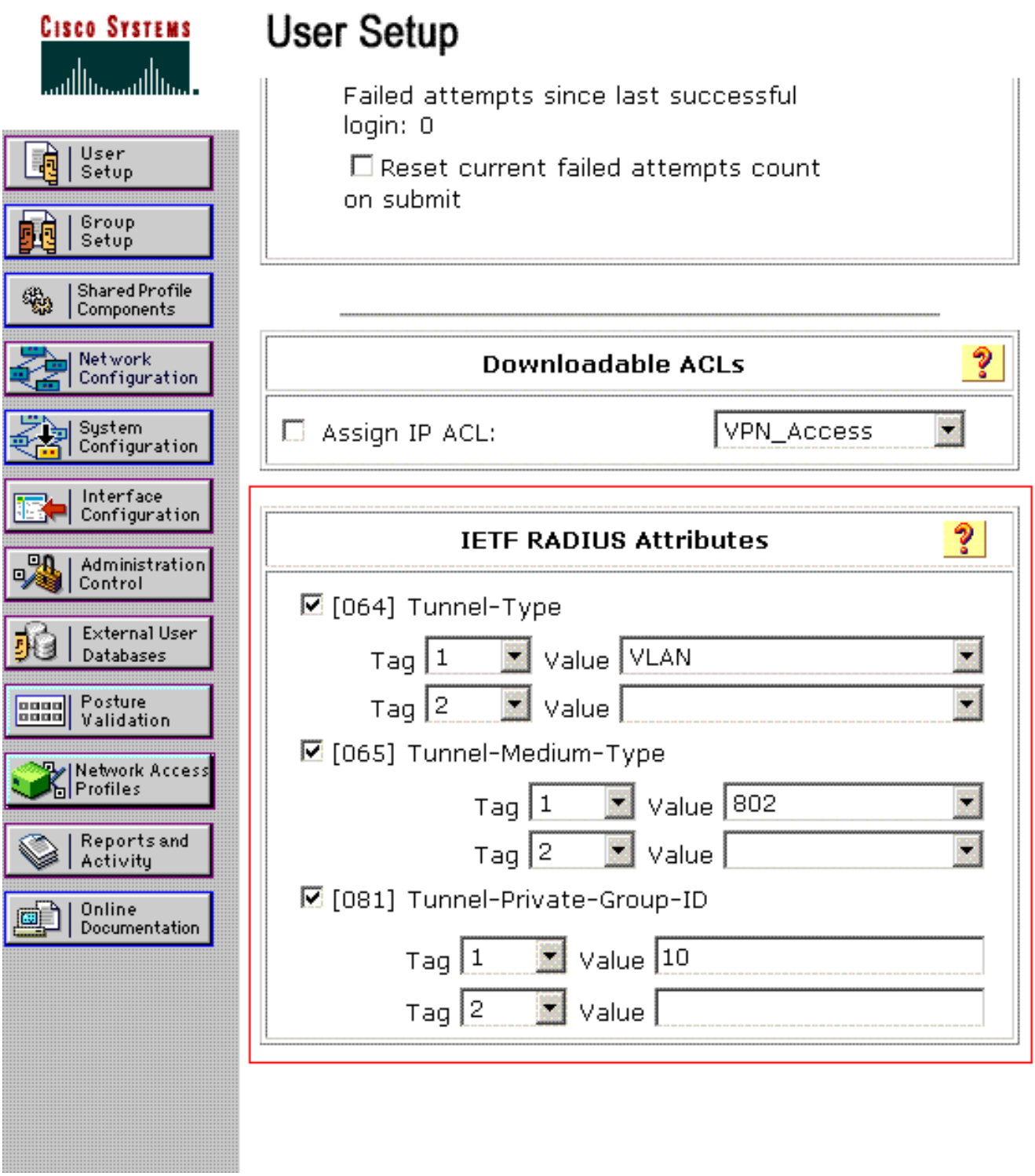


3. [Edit] ページで、図に示すように必要なユーザ情報を入力します。

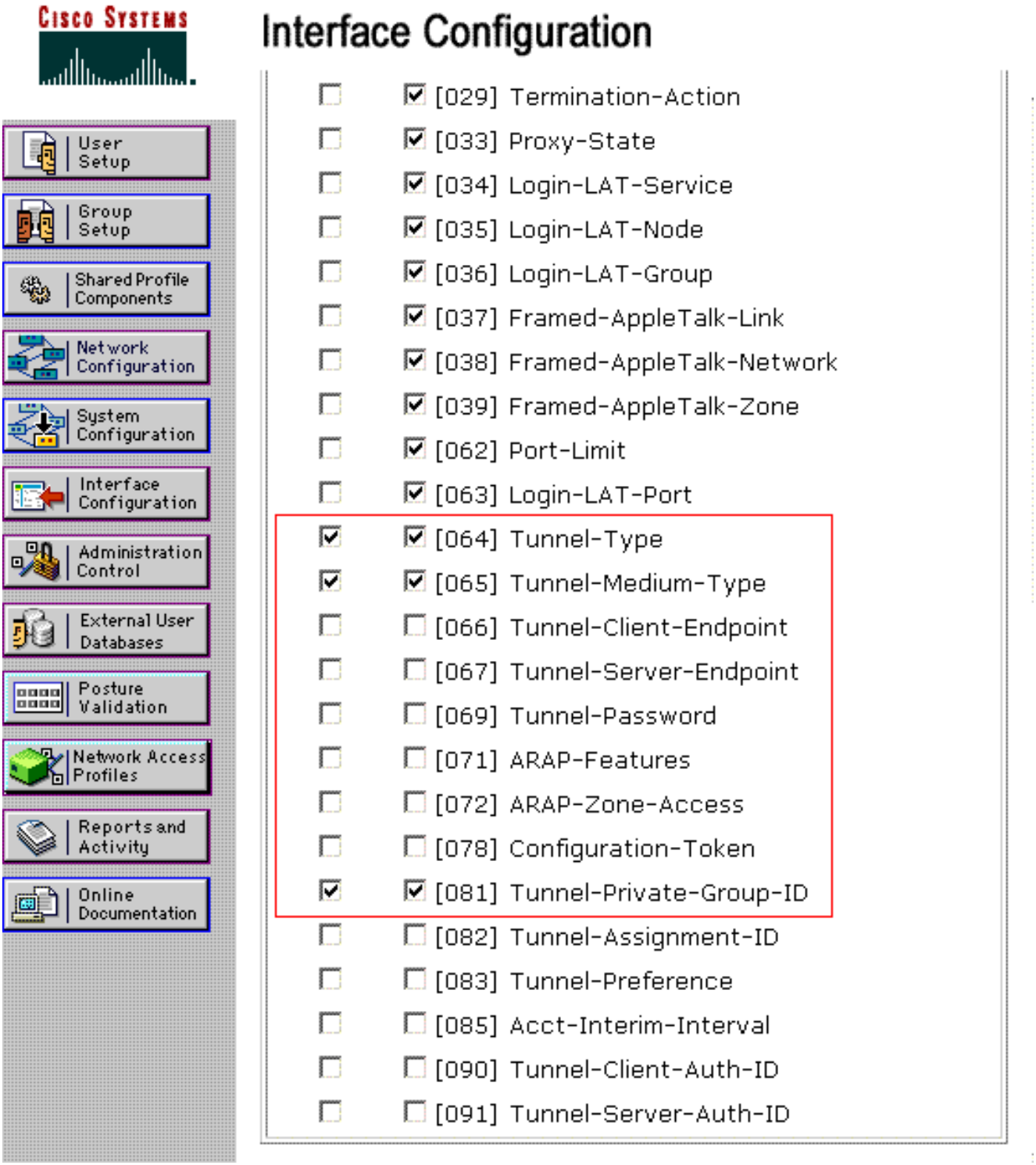


User Setup セクションで入力したパスワードと、ユーザ認証時にクライアント側で入力するパスワードは一致している必要があります。

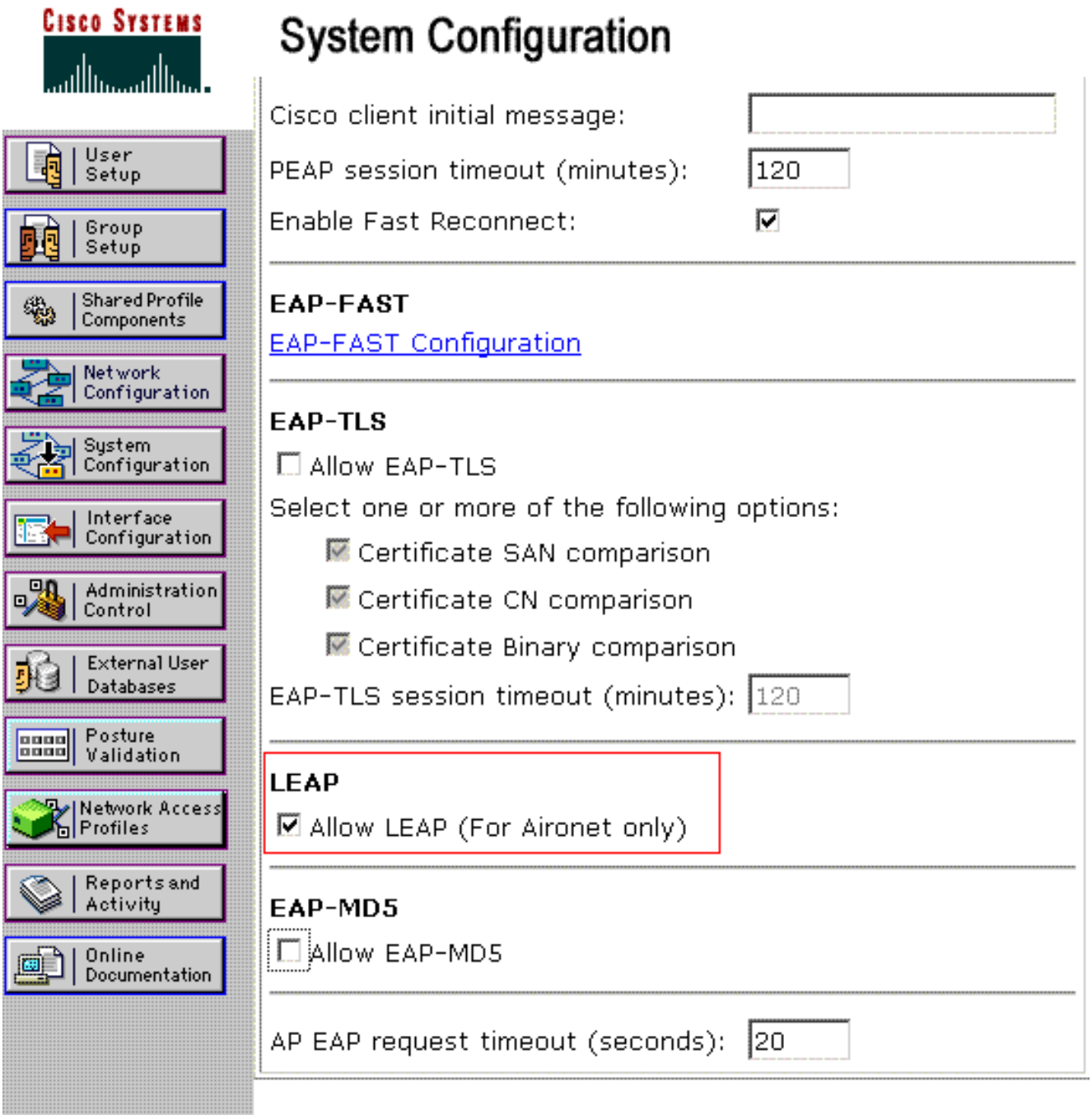
4. [Edit] ページを下にスクロールして、[**IETF RADIUS Attributes**] フィールドを探します。
5. [IETF RADIUS Attributes] フィールドで、3 つのトンネル アトリビュートの横にあるチェック ボックスにチェックマークを付け、図に示すようにアトリビュート値を設定します。



注: ACS サーバの初期設定では、IETF RADIUS 属性が表示されない場合があります。IETF アトリビュートを有効にするために、ユーザ設定ウィンドウで **[Interface Configuration] > [RADIUS (IETF)]** の順に選択します。次に、アトリビュート **64、65、および 81** の [User] 列と [Group] 列のチェック ボックスにチェックマークを付けます。



注: クライアントを特定の VLAN にダイナミックに割り当てるように RADIUS サーバを設定するには、**RADIUS サーバの IETF 81 (Tunnel-Private-Group-ID) フィールドで設定した VLAN ID が WLC 上に存在している必要があります。**RADIUS サーバでユーザごとの設定を有効にするために、[Interface Configuration] > [Advanced Options] の順に選択し、[Per User TACACS+/RADIUS] アトリビュート チェック ボックスをオンにします。また、認証プロトコルとして LEAP を使用するので、図に示すように RADIUS サーバの [System Configuration] ウィンドウで LEAP が有効になっていることを確認します。



ダイナミック VLAN 割り当て用の Cisco Airespace VSA アトリビュートによる ACS の設定

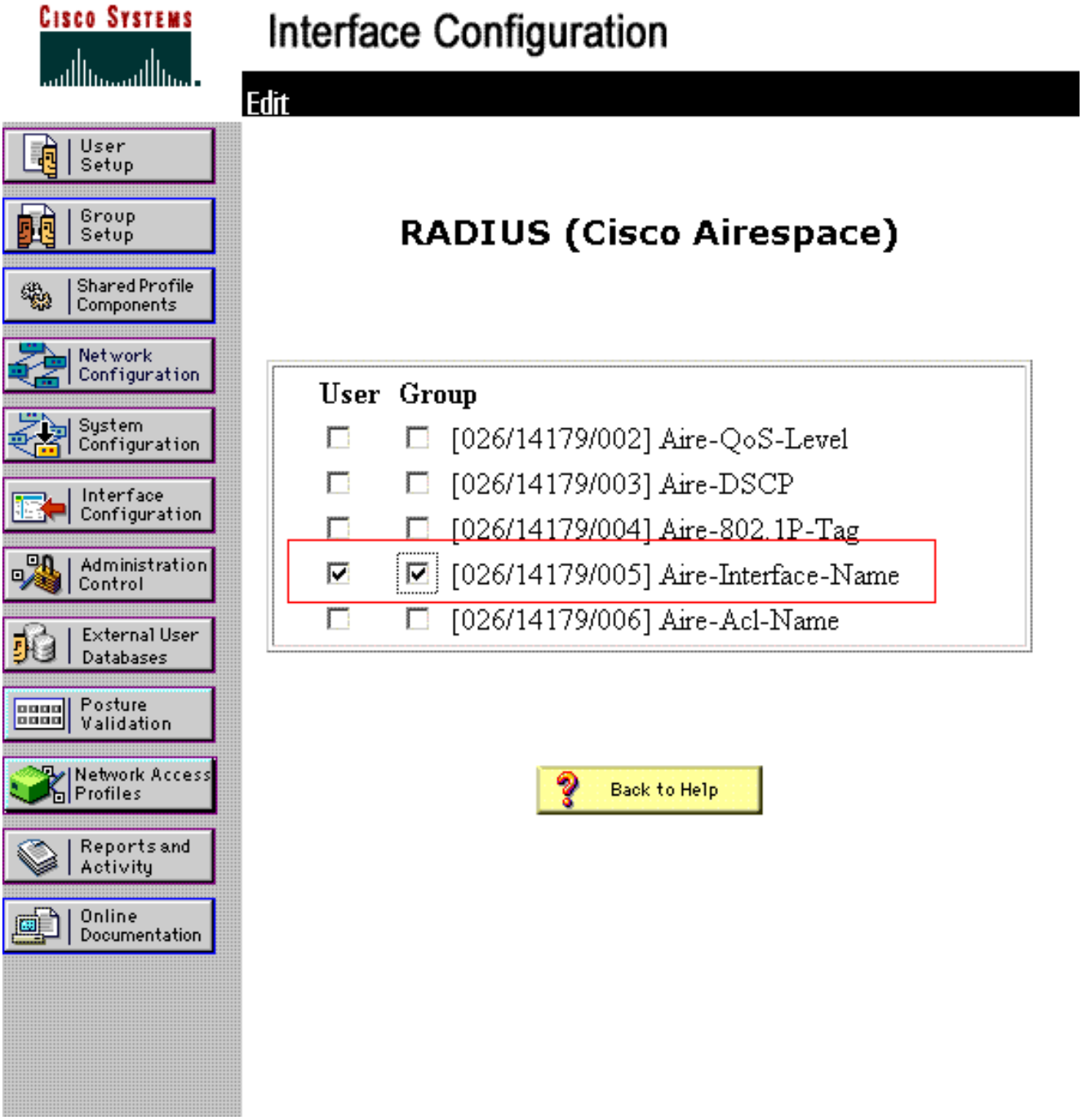
最新の ACS バージョンでは、また Cisco Airespace [（ベンダー別） VSA できます設定] ACS のユーザコンフィギュレーションによって VLANインターフェイス名前（ない VLAN ID）によって認証済みユーザを正常に割り当てるアトリビュート。 これを実現するには、このセクションで説明する手順を実行する必要があります。

注: このセクションでは、ACS 4.1 バージョンを使用して Cisco Airespace VSA アトリビュートを設定します。

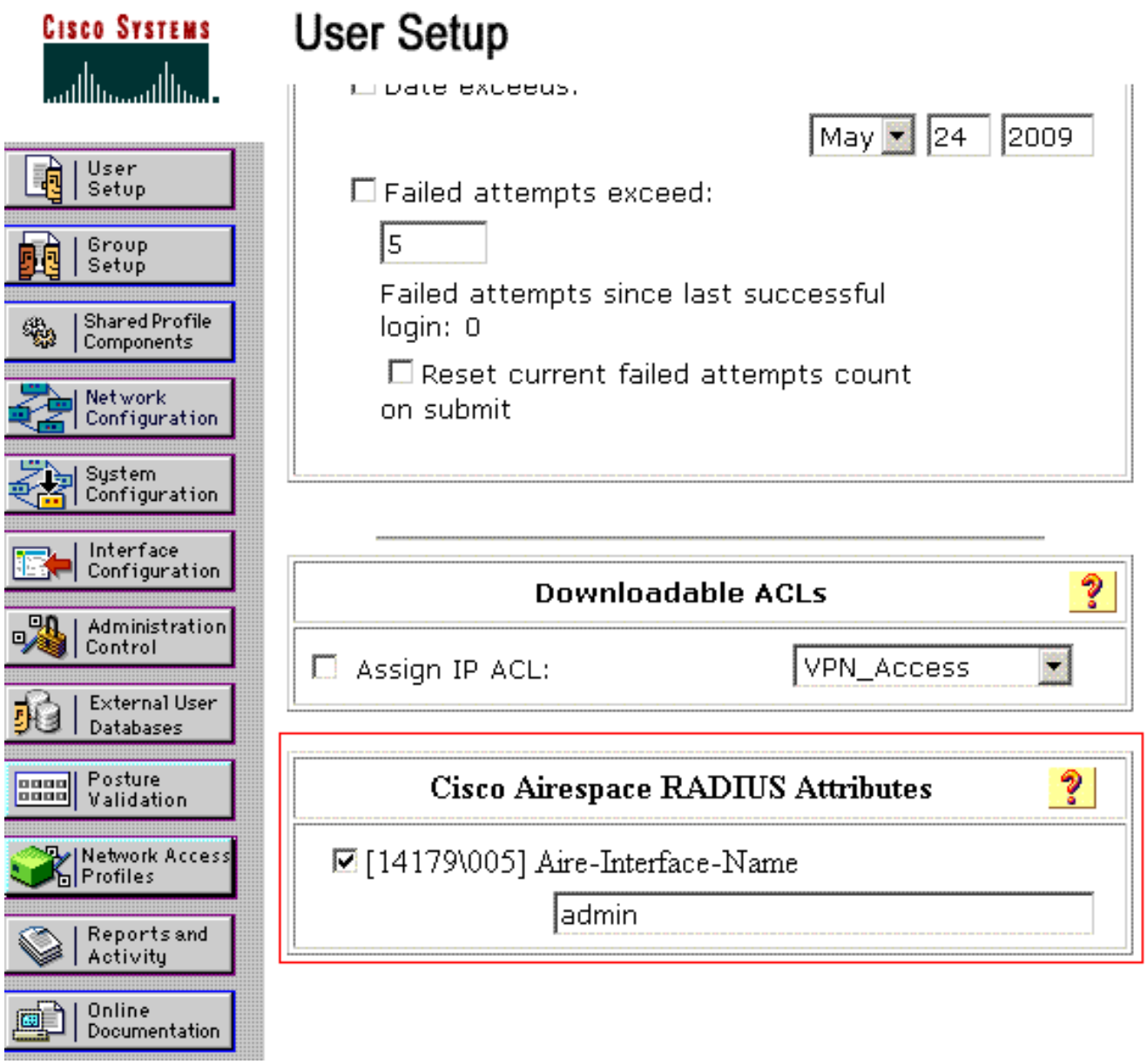
Cisco Airespace VSA アトリビュート オプションを使用した ACS グループの設定

次の手順を実行します。

1. ACS 4.1 の GUI で、ナビゲーション バーから [Interface Configuration] をクリックします。次に、Cisco Airespace アトリビュート オプションを設定するために、[Interface Configuration] ページで **[RADIUS (Cisco Airespace)]**を選択します。
2. [RADIUS (Cisco Airespace)] ウィンドウで、[User Edit] ページで表示するために、[Aire-Interface-Name] の横の [User] チェック ボックス (必要に応じて [Group] チェック ボックス) をオンにします。 次に **Submit** をクリックします。



3. user1 の Edit ページに移動します。
4. [User Edit] ページで、[Cisco Airespace RADIUS Attributes] セクションまで下にスクロールします。 **[Aire-Interface-Name]** アトリビュートの横のチェック ボックスにチェックマークを付け、ユーザ認証が成功した場合に割り当てるダイナミック インターフェイスの名前を指定します。次の例では、ユーザを **admin** VLAN に割り当てています。



5. [Submit] をクリックします。

複数の VLAN を使用するためのスイッチの設定

複数の VLAN がスイッチを通過できるようにするには、次のコマンドを発行して、コントローラに接続されたスイッチ ポートを設定する必要があります。

1. Switch(config-if)#**switchport mode trunk**
2. Switch(config-if)#**switchport trunk encapsulation dot1q**

注: ほとんどのスイッチでは、そのスイッチ上で作成されたすべての VLAN に対してトランク ポートを通過することがデフォルトで許可されます。

これらのコマンドは、Catalyst オペレーティング システム（CatOS）スイッチによって異なります。

スイッチに有線ネットワークが接続されている場合は、有線ネットワークに接続されたスイッチ ポートに対しても同じ設定を適用できます。 これにより、有線ネットワークとワイヤレス ネットワークの同じ VLAN 間での通信が可能になります。

注: このドキュメントでは VLAN 間通信については説明しません。 これはこのドキュメントの範

囲外です。 VLAN 間ルーティングを行うには、レイヤ 3 スイッチまたは VLAN およびトランキングが適切に設定された外部ルータが必要になります。 VLAN 間ルーティングの設定に関して説明しているドキュメントはいくつかあります。

WLC の設定

設定には次の手順が必要です。

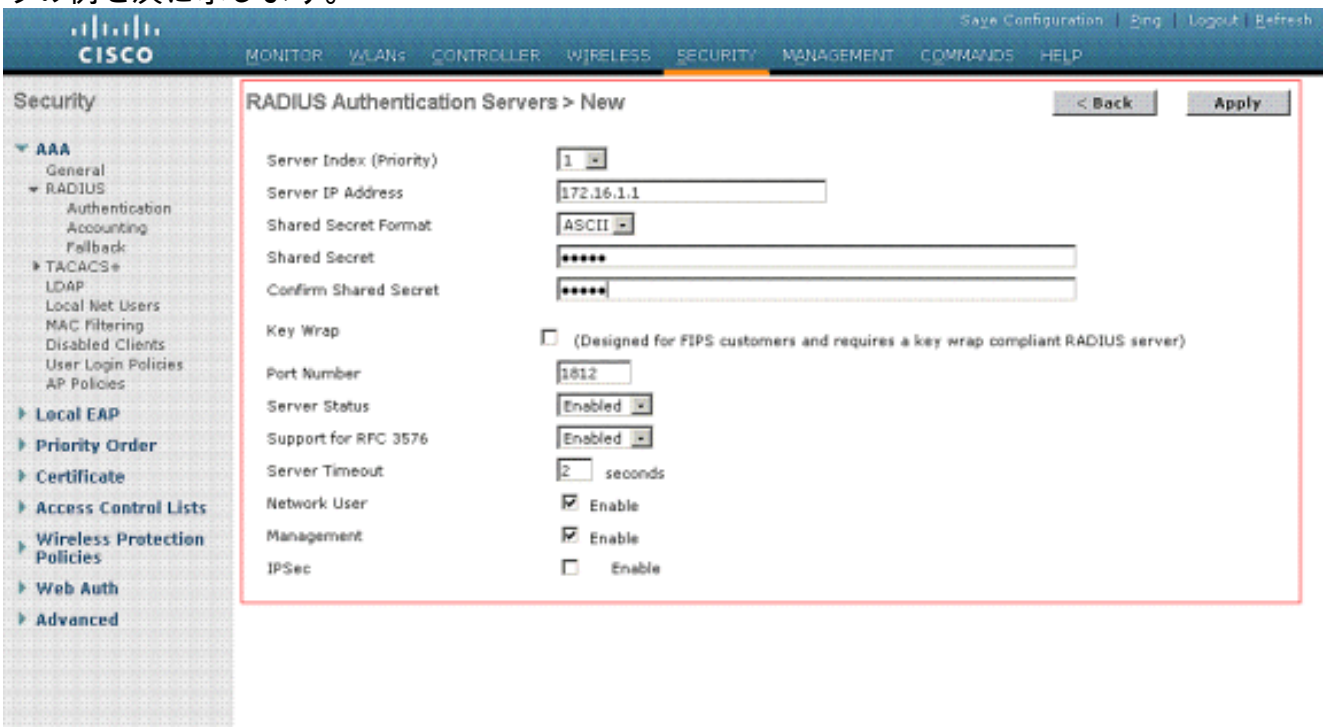
- 認証サーバの詳細を使用した WLC の設定
- ダイナミック インターフェイス (VLAN) の設定
- WLAN (SSID) の設定

認証サーバの詳細を使用した WLC の設定

WLC と RADIUS サーバの間でクライアントの認証やその他のトランザクションを行えるように、WLC を設定する必要があります。

次の手順を実行します。

1. コントローラの GUI で、[Security] をクリックします。
2. RADIUS サーバの IP アドレスと、RADIUS サーバと WLC の間で使用する共有秘密キーを入力します。この共有秘密キーは、RADIUS サーバの [Network Configuration] > [AAA Clients] > [Add Entry] で設定されたキーと一致している必要があります。 WLC のウィンドウの例を次に示します。



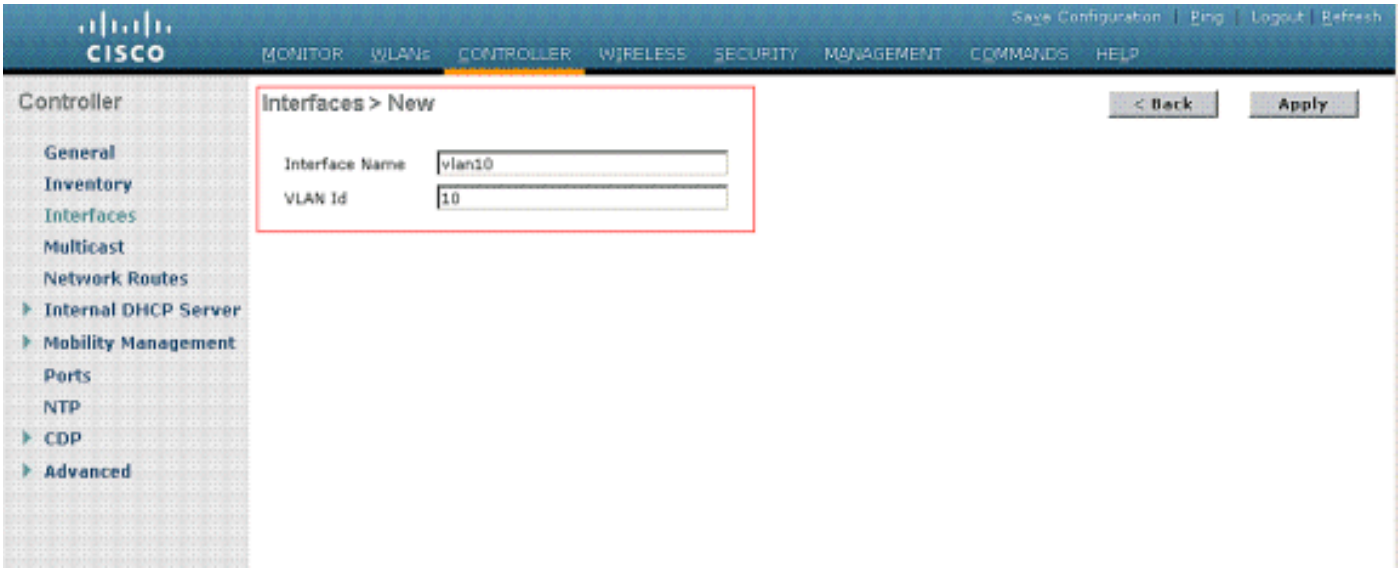
ダイナミック インターフェイス (VLAN) の設定

この手順では、WLC でダイナミック インターフェイスを設定する方法について説明します。 このドキュメントですでに説明したように、RADIUS サーバの Tunnel-Private-Group ID 属性で指定された VLAN ID が WLC 内にも存在している必要があります。

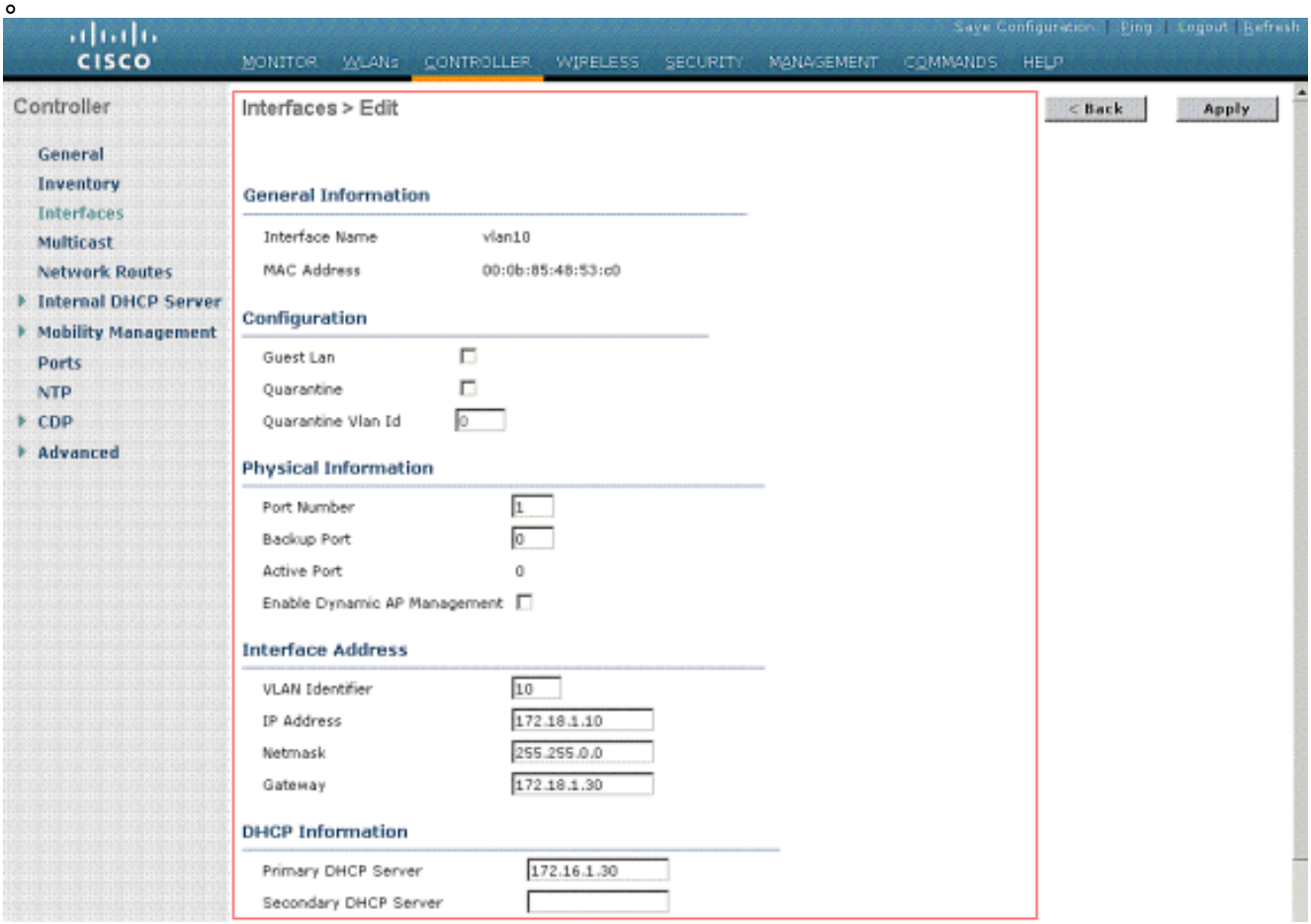
この例では、user1 の **Tunnel-Private-Group ID** は RADIUS サーバ上で 10 (VLAN =10) に設定さ

れています。 user1 の [User Setup] ウィンドウの [IETF RADIUS Attributes] セクションを参照してください。

この例では、WLC でも同じダイナミック インターフェイス (VLAN=10) が設定されていることを確認できます。 ダイナミック インターフェイスの設定は、コントローラの GUI の Controller > Interfaces ウィンドウで行います。



1. このウィンドウで **[Apply]**をクリックします。このダイナミック インターフェイス (この例では VLAN 10) の [Edit] ウィンドウが開きます。
2. このダイナミック インターフェイスの IP アドレスとデフォルト ゲートウェイを入力します。



注: このドキュメントでは、コントローラの内部 DHCP サーバを使用しているので、このウィンドウの Primary DHCP Server フィールドでは WLC の管理インターフェイスそのものが

指定されています。 ワイヤレス クライアントに対する DHCP サーバとしては、外部 DHCP サーバ、ルータ、または RADIUS サーバ自体を使用することもできます。 その場合、プライマリ DHCP サーバのフィールドには、DHCP サーバとして使用するデバイスの IP アドレスを指定します。 詳細については、DHCP サーバのマニュアルを参照してください。

3. [Apply] をクリックします。これで WLC にダイナミック インターフェイスが設定されます。 同様の方法で、WLC に複数のダイナミック インターフェイスを設定することもできます。 ただし、クライアントに割り当てる特定の VLAN の VLAN ID が RADIUS サーバ内にも存在している必要があります。

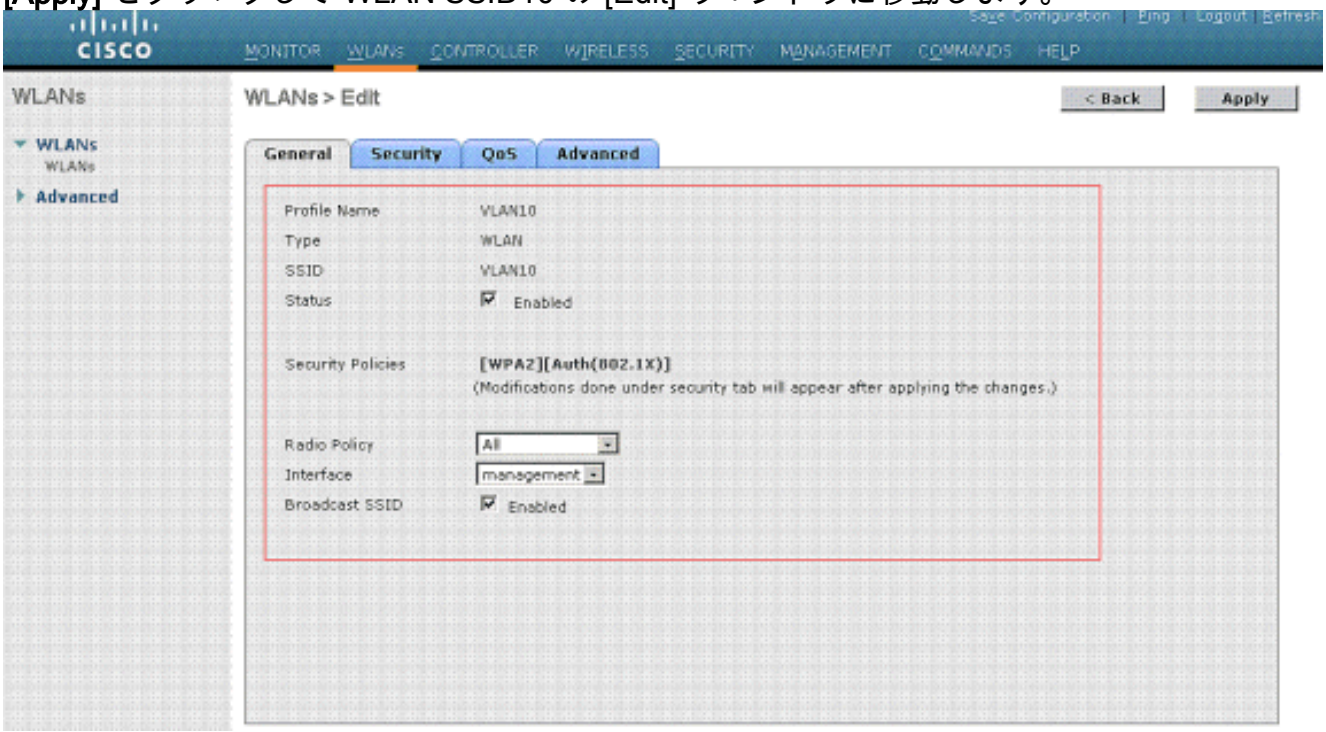
WLAN (SSID) の設定

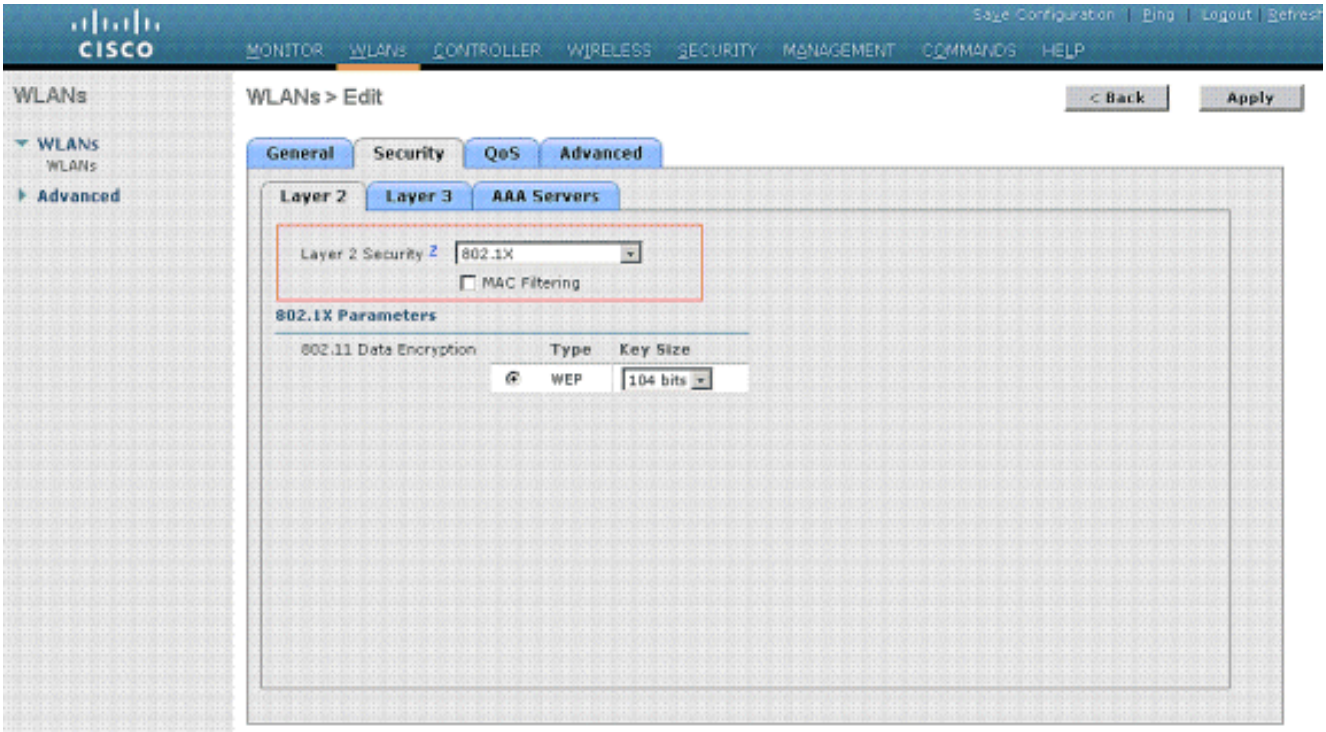
この手順では、WLC で WLAN を設定する方法について説明します。

次の手順を実行します。

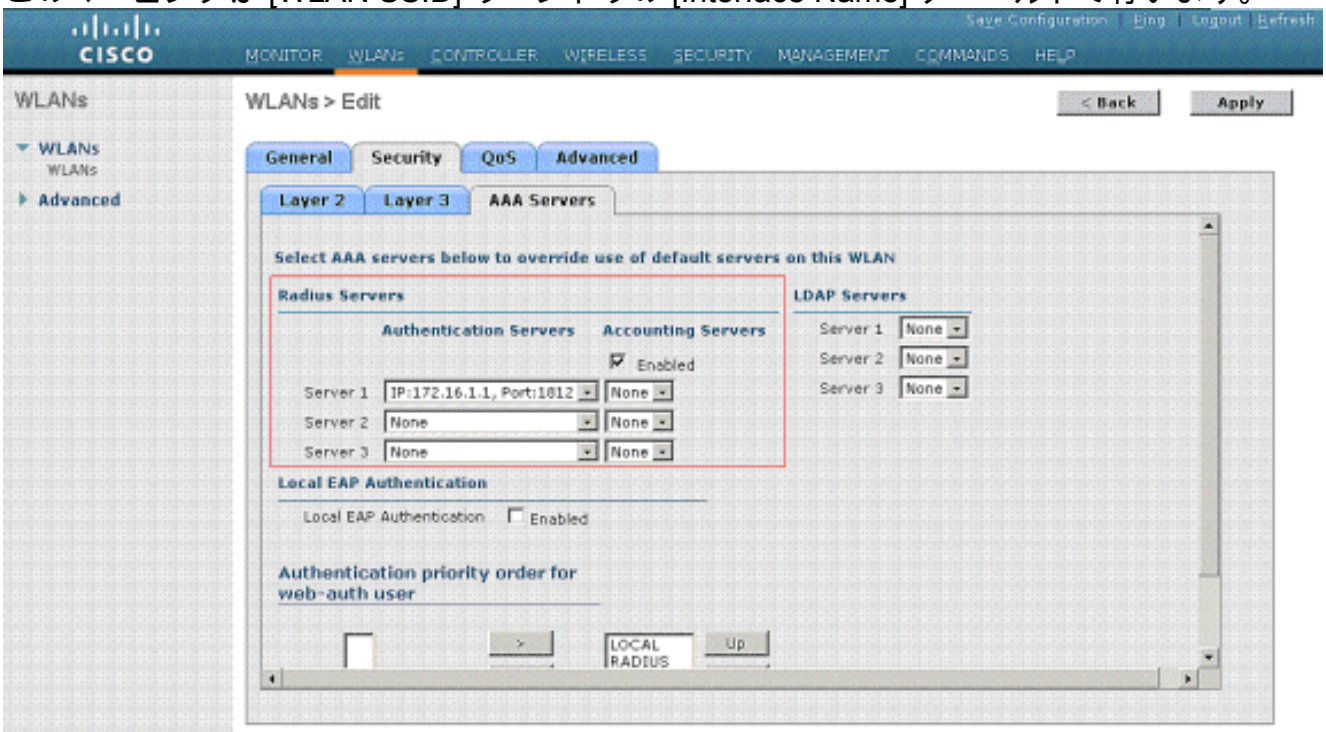
1. 新規の WLAN を作成するには、コントローラの GUI で [WLANs] > [New] の順に選択します。新規の WLAN のウィンドウが表示されます。
2. WLAN ID と WLAN SSID 情報を入力します。WLAN SSID には任意の名前を入力できます。 この例では、WLAN SSID として VLAN10 を使用しています。

3. **[Apply]** をクリックして WLAN SSID10 の [Edit] ウィンドウに移動します。



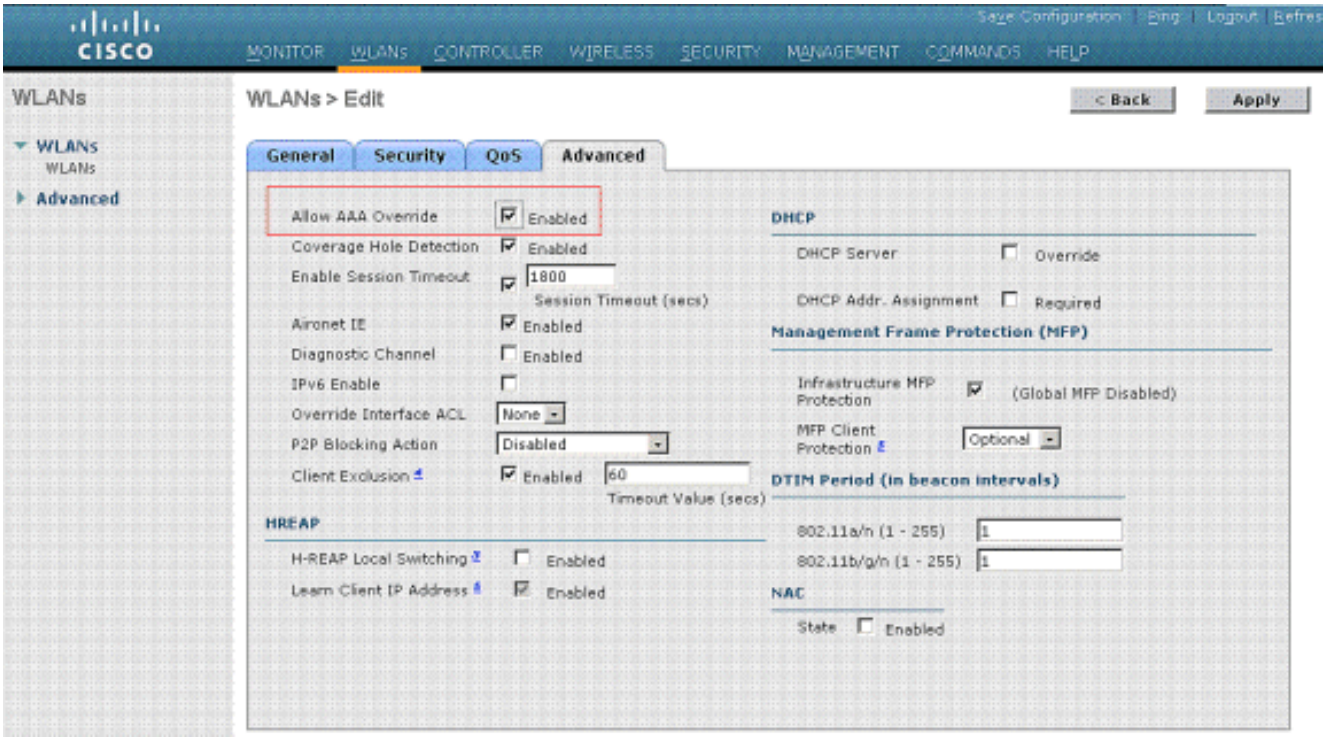


通常、ワイヤレス LAN コントローラでは、WLAN に属する特定のユーザが特定の VLAN に割り当てられるように、各 WLAN が特定の VLAN (SSID) にマッピングされます。 通常、このマッピングは [WLAN SSID] ウィンドウの [Interface Name] フィールドで行います。



この例では、認証の成功後にワイヤレス クライアントを特定の VLAN に割り当てるタスクは RADIUS サーバによって処理されます。 WLAN は WLC 上で特定のダイナミック インターフェイスにマッピングされている必要はありません。 WLC で WLAN がダイナミック インターフェイスにマッピングされている場合でも、RADIUS サーバはこのマッピングを無視し、その WLAN からアクセスしているユーザを、RADIUS サーバでそのユーザの [**Tunnel-Group-Private-ID**] フィールドに指定されている VLAN に割り当てます。

4. WLC の設定を RADIUS サーバで無視するために、[Allow AAA Override] チェック ボックスをオンにします。
5. 設定されている WLAN (SSID) ごとにコントローラで [Allow AAA Override] を有効にします。



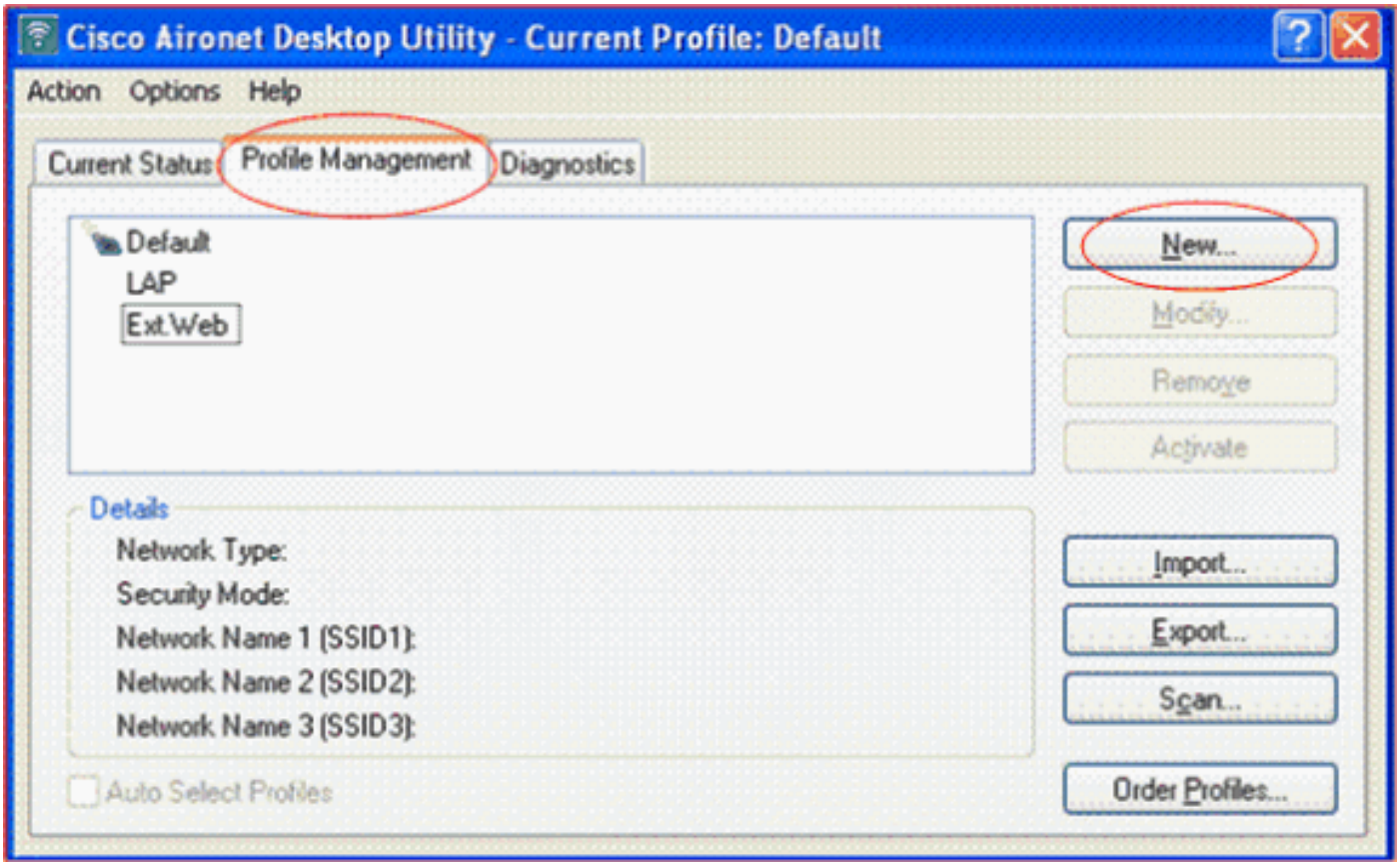
AAA Override を有効にしていて、クライアントの AAA とコントローラの WLAN の認証パラメータが競合する場合は、クライアント認証は AAA (RADIUS) サーバで実行されます。この認証の一環として、オペレーティング システムにより、AAA サーバから返された VLAN にクライアントが移動されます。 これはコントローラ インターフェイス設定で事前に定義されています。たとえば、VLAN 2 に割り当てられた管理インターフェイスが企業 WLAN でメインとして使用されていて、AAA Override により VLAN 100 へのリダイレクトが返された場合は、VLAN 100 が割り当てられている物理ポートが使用できない場合でも、オペレーティング システムにより、すべてのクライアント通信が VLAN 100 にリダイレクトされます。 AAA Override を無効にすると、コントローラの認証パラメータ設定がすべてのクライアント認証においてデフォルトで使用され、コントローラ WLAN にクライアント固有の認証パラメータがない場合は、AAA サーバのみによって認証が実行されます。

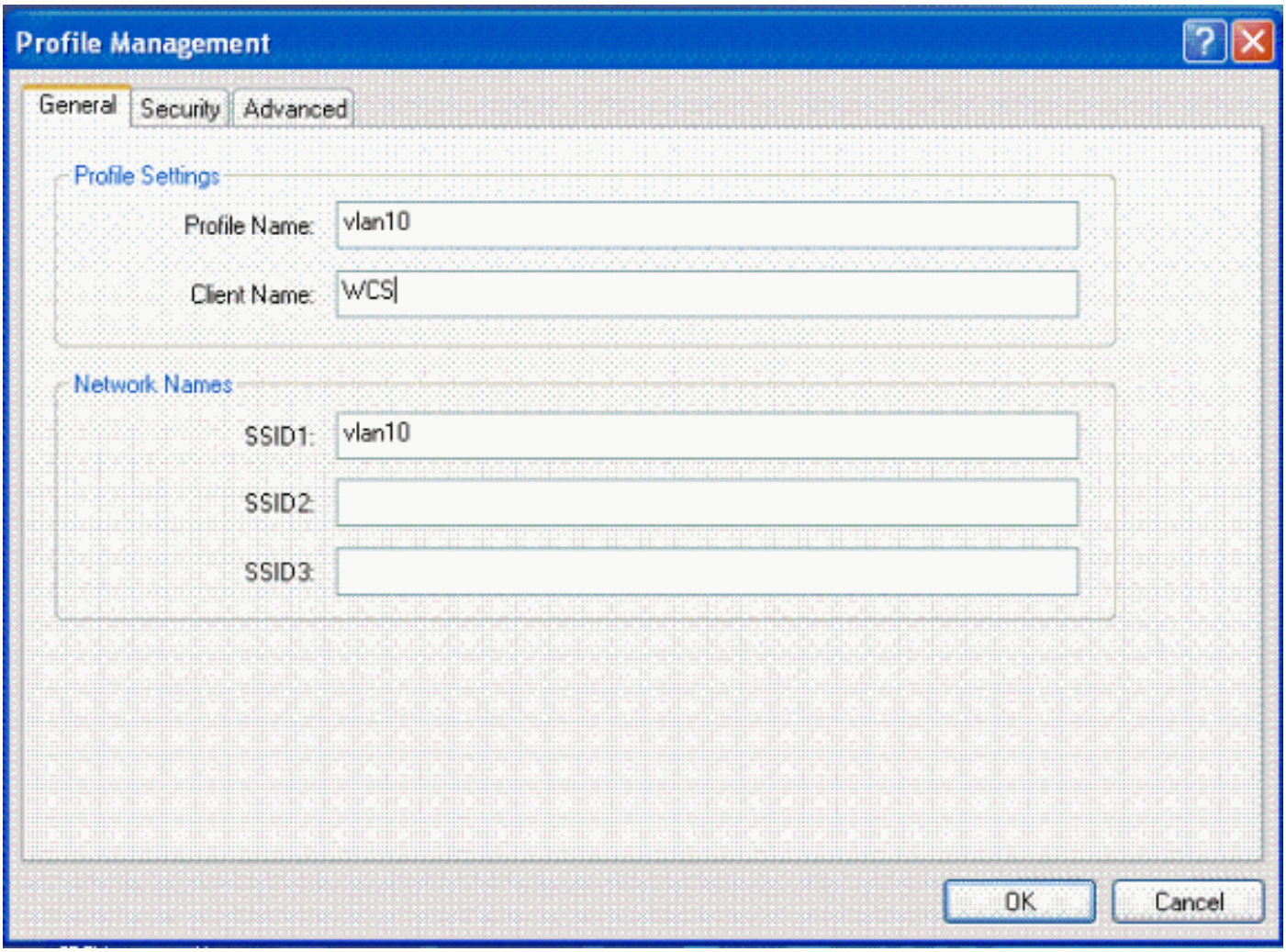
Wireless Client Utility の設定

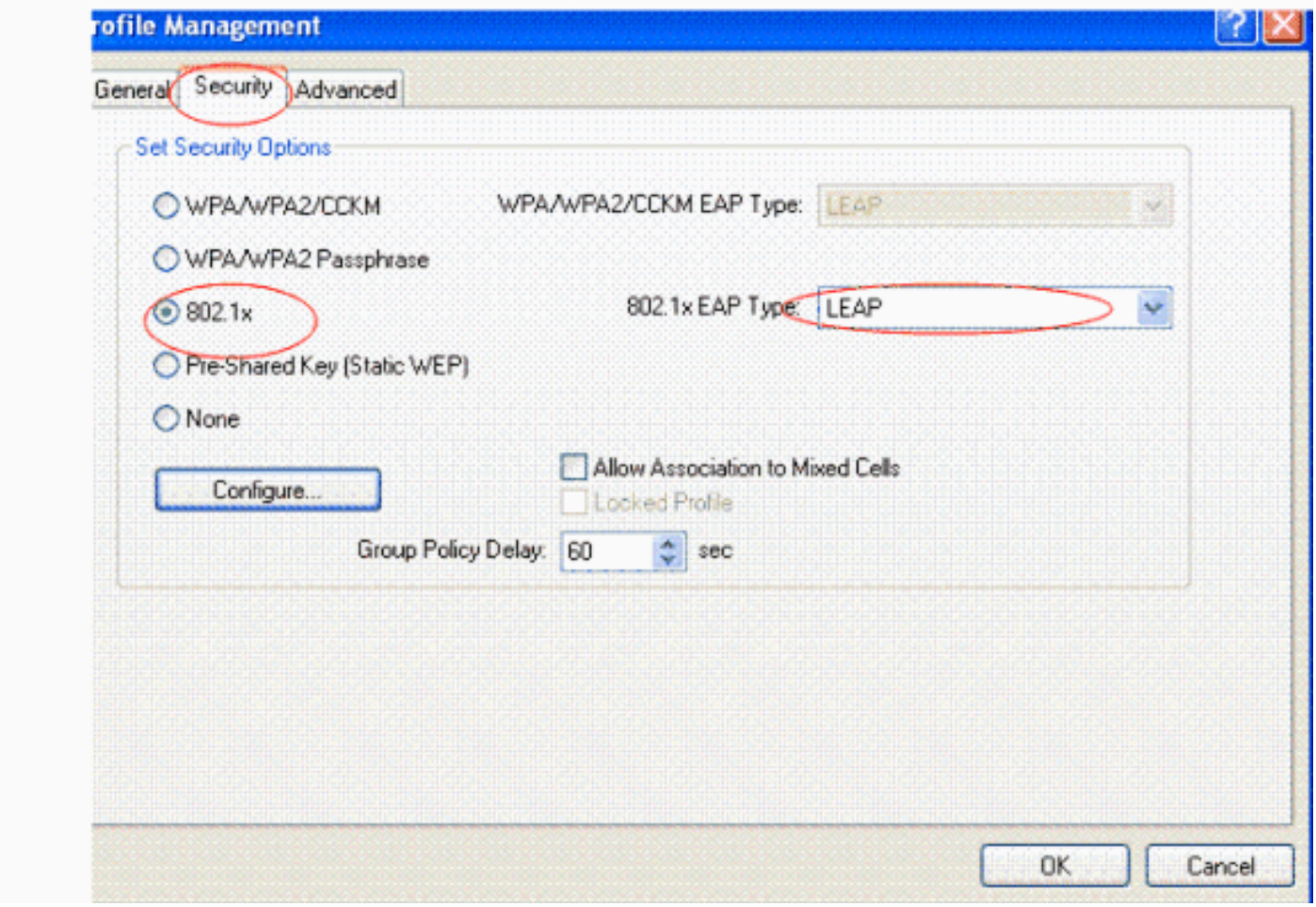
このドキュメントでは、ユーザ プロファイルを設定するためのクライアント ユーティリティとして ADU を使用します。 さらに、この設定では認証プロトコルとして LEAP を使用します。 このセクションで説明するとおりに ADU を設定してください。

新規のプロファイルを作成するには、ADU のメニューバーで [Profile Management] > [New] の順に選択します。

この例で使用されているクライアントは、SSID VLAN10 の一部として設定されています。 クライアント上でユーザ プロファイルを設定する方法を以降の図で示します。


Cisco Aironet Desktop Utility - Current Profile: Default
Action Options Help
Current Status
Profile Management
Diagnostics
Default
LAP
Ext.Web
New...
Modify...
Remove
Activate
Details
Network Type:
Security Mode:
Network Name 1 (SSID1):
Network Name 2 (SSID2):
Network Name 3 (SSID3):
Import...
Export...
Scan...
Auto Select Profiles
Order Profiles...


Profile Management
General
Security
Advanced
Profile Settings
Profile Name:
vlan10
Client Name:
WCS
Network Names
SSID1:
vlan10
SSID2:
SSID3:
OK
Cancel



確認

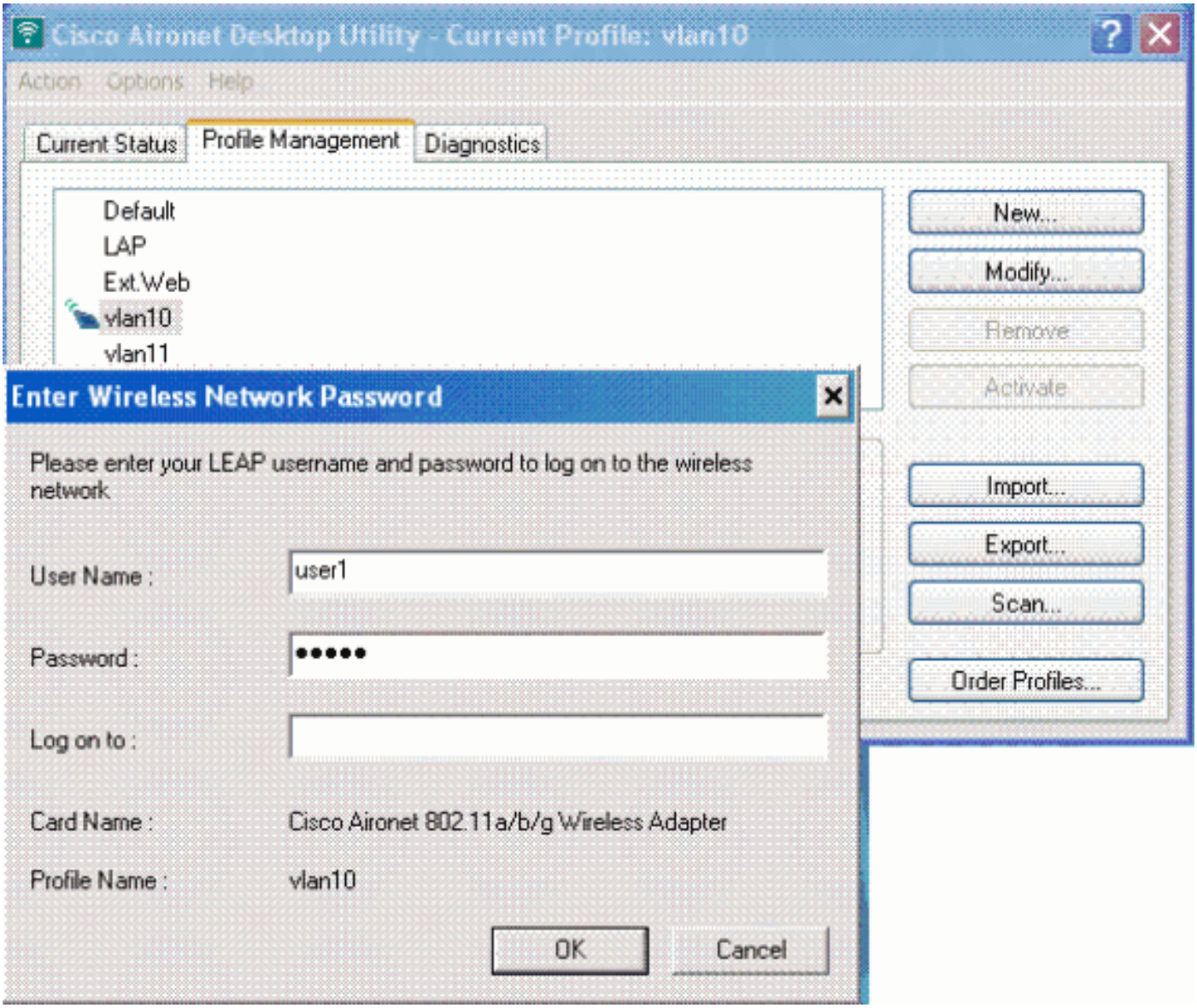
ADU で設定したユーザ プロファイルをアクティブにします。 設定に基づいて、ユーザ名とパスワードの入力を求められます。 ADU に対して Windows ユーザ名とパスワードを認証に使用するように指示することもできます。 クライアントが認証を受けるためのオプションはいくつか用意されています。 これらのオプションは、作成したユーザ プロファイルの [Security] > [Configure] タブで設定できます。

上の例では、RADIUS サーバで指定されているとおりに、user1 は VLAN10 に割り当てられます。

この例では、クライアントの認証と RADIUS サーバによる VLAN への割り当てを実行するために、クライアント側からの次のユーザ名とパスワードを使用します。

- ユーザ名 = user1
- パスワード = user1

この例は、SSID VLAN10 がどのようにユーザ名とパスワードの入力を求められるかを示しています。 この例では、ユーザ名とパスワードがすでに入力されています。

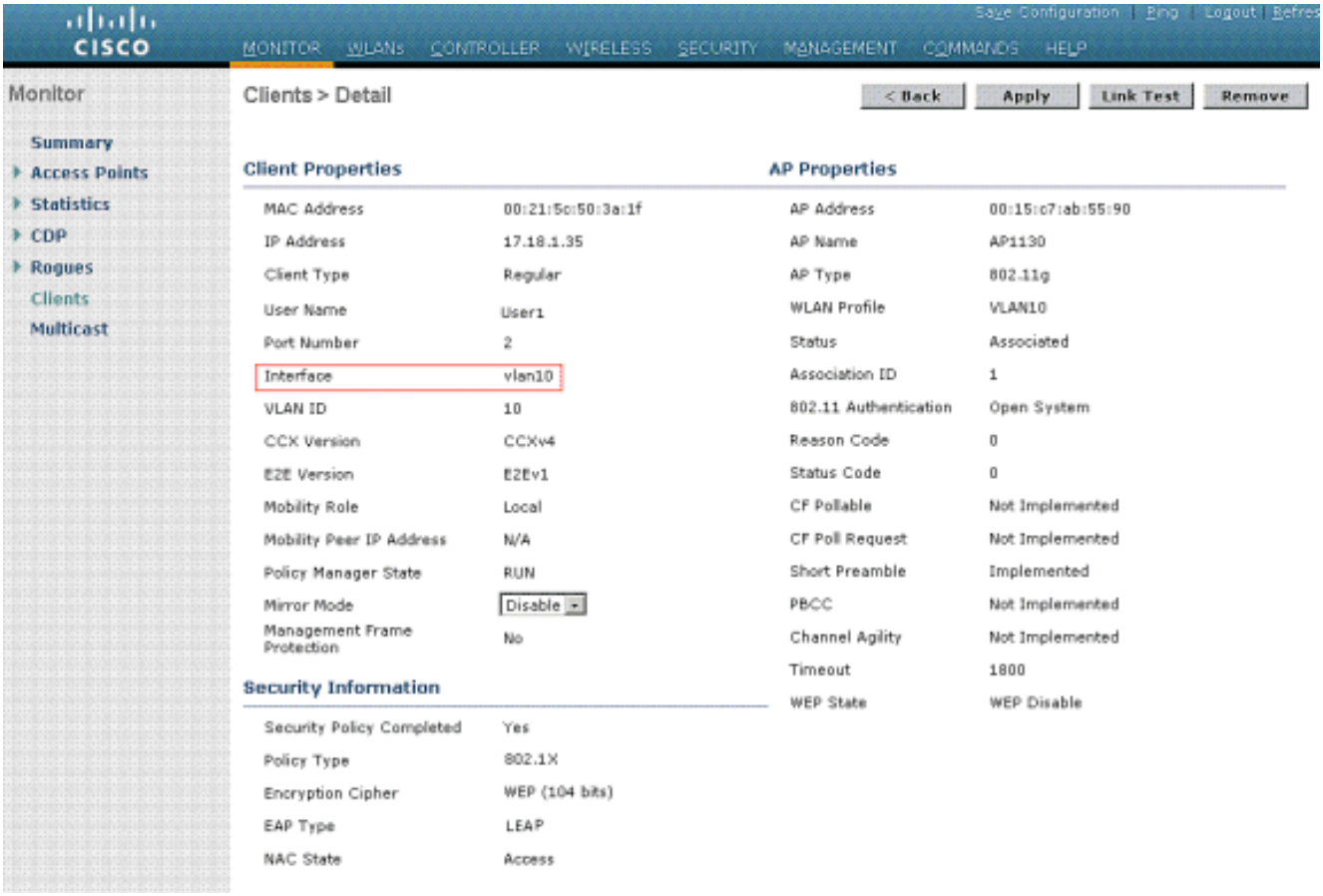


認証と確認に成功すると、成功のステータス メッセージが返されます。

次に、送信された RADIUS アトリビュートに従ってクライアントが適切な VLAN に割り当てられたことを確認する必要があります。 これを行うには、次の手順を実行します。

1. コントローラの GUI で、**[Wireless] > [AP]** の順に選択します。
2. [Access Points (APs)] ウィンドウの左隅にある **[Clients]** をクリックします。クライアントの統計情報が表示されます。

3. このクライアントの IP アドレスや、このクライアントが割り当てられている VLAN などの詳細を確認するには、**[Details]** をクリックします。この例では、クライアント user1 の詳細が表示されています。



このウィンドウでは、RADIUS サーバに設定された RADIUS アトリビュートに従って、このクライアントが VLAN10 に割り当てられたかどうかを確認できます。**注:** ダイナミック VLAN 割り当てが **Cisco Airespace VSA アトリビュート**の設定に基づいている場合、クライアント詳細ページにはこの例のように、**インターフェイス名が admin として表示**されます。

ここでは、設定が正常に動作していることを確認します。

- **debug aaa events enable**：このコマンドを使用すると、コントローラを介して RADIUS アトリビュートがクライアントに正常に転送されたことを確認できます。 デバッグ出力に次の部分が含まれている場合は、RADIUS アトリビュートの転送に成功したことを意味しています。

```
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[0]:
attribute 64, vendorId 0, valueLen 4
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[1]:
attribute 65, vendorId 0, valueLen 4
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[2]:
attribute 81, vendorId 0, valueLen 3
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[3]:
attribute 79, vendorId 0, valueLen 32
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 Received EAP Attribute
(code=2, length=32,id=0) for mobile 00:40:96:ac:e6:57
Fri Jan 20 02:25:08 2006: 00000000: 02 00 00 20 11 01 00 18
4a 27 65 69 6d e4 05 f5
........J'eim...00000010: d0 98 0c cb 1a 0c 8a 3c
........44 a9 da 6c 36 94 0a f3  <D..l6...
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[4]: attribute 1, vendorId 9,
valueLen 16 Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[5]: attribute 25,
vendorId 0, valueLen 28 Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[6]:
attribute 80, vendorId 0, valueLen 16 Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 Tunnel-
Type 16777229 should be 13 for STA 00:40:96:ac:e6:57 Fri Jan 20 02:25:08 2006:
00:40:96:ac:e6:57 Tunnel-Medium-Type 16777222 should be 6 for STA 00:40:96:ac:e6:57 Fri Jan
20 02:30:00 2006: 00:40:96:ac:e6:57 Station 00:40:96:ac:e6:57 setting dot1x reauth timeout =
1800
```

- 次のコマンドも使用できます。**debug dot1x aaa enabledebug aaa packets enable**

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

注: ダイナミック VLAN 割り当ては WLC からの Web 認証のためにはたらきません。

関連情報

- RADIUS サーバとの EAP 認証
- Cisco LEAP
- Cisco ワイヤレス LAN コントローラ コンフィギュレーション ガイド、リリース 4.0
- テクニカルサポートとドキュメント - Cisco Systems