# WLANコントローラ(WLC)でのEAP認証の設定

## 内容



## 概要

このドキュメントでは、外部 RADIUS サーバで使用する拡張認証プロトコル（EAP）認証のためにワイヤレス LAN コントローラ（WLC）を設定する方法について説明します。この設定例では、ユーザ クレデンシャルを検証するために、Cisco Secure Access Control Server（ACS）を外部 RADIUS サーバとして使用しています。

## 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。

- Lightweight Access Point（AP; アクセス ポイント）および Cisco WLC の設定に関する基本的な知識。
- Lightweight AP Protocol（LWAPP）に関する基本的な知識。
- Cisco Secure ACS などの外部 RADIUS サーバの設定方法に関する知識。

## 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いています。

- Cisco Aironet 1232AG シリーズ Lightweight AP
- ファームウェア 5.1 が稼働している Cisco 4400 シリーズ WLC
- バージョン 4.1 が稼働している Cisco Secure ACS
- Cisco Aironet 802.11 a/b/g クライアント アダプタ
- ファームウェア 4.2 が稼働している Cisco Aironet Desktop Utility（ADU）

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、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実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。

# 設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

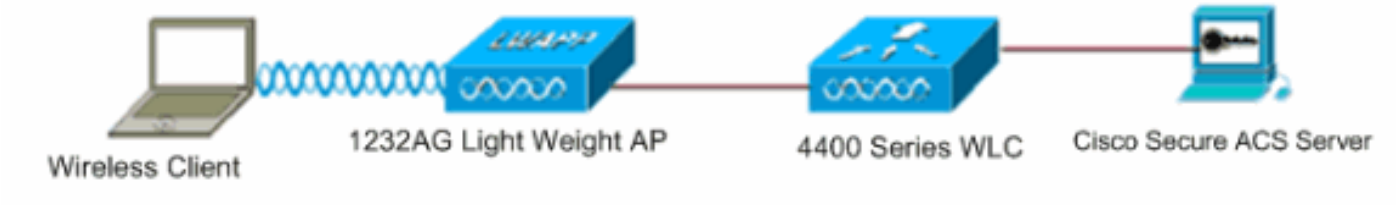
**注：このド**キュメントで使用されるコマンドの詳細を調べるには、Command Lookup Tool(登録ユーザ専用)を使用してください。

EAP 認証用にデバイスを設定するには、次の手順を実行します。

1. WLC を基本動作に設定し、コントローラに Lightweight AP を登録します。
2. 外部 RADIUS サーバを使用した RADIUS 認証用に WLC を設定します。
3. WLAN パラメータを設定します。
4. 外部 RADIUS サーバとして Cisco Secure ACS を設定し、認証クライアント用のユーザ データベースを作成します。

## ネットワーク図

この構成では、Cisco 4400 WLC と Lightweight AP はハブ経由で接続されています。外部 RADIUS サーバ（Cisco Secure ACS）も同じハブに接続します。すべてのデバイスは同じサブネット内にあります。最初に AP をコントローラに登録します。WLC と AP を、Lightweight Extensible Authentication Protocol（LEAP）認証用に設定する必要があります。AP に接続するクライアントは、AP との関連付けに LEAP 認証を使用します。RADIUS 認証を実行するには、Cisco Secure ACS を使用します。



## WLC の基本動作用の設定およびコントローラへの Lightweight AP の登録

WLC を基本動作用に設定するには、Command-Line Interface ( CLI; コマンドライン インターフェイス ) 上でスタートアップ コンフィギュレーション ウィザードを使用します。この他、GUI を使用して WLC を設定することもできます。このドキュメントでは、CLI 上でスタートアップ コンフィギュレーション ウィザードを使用した、WLC 上の設定について説明します。

WLC が初めて起動すると、スタートアップ コンフィギュレーション ウィザードに直接入ります。基本設定には、コンフィギュレーション ウィザードを使用します。このウィザードは、CLI または GUI で実行できます。次の出力は、CLI 上でのスタートアップ コンフィギュレーション ウィザードの例を示します。

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
System Name [Cisco_33:84:a0]: WLC-1
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (24 characters max): *****
Management Interface IP Address: 10.77.244.204
Management Interface Netmask: 255.255.255.224
Management Interface Default Router: 10.77.244.220
Management Interface VLAN Identifier (0 = untagged):
Management Interface Port Num [1 to 4]: 1
Management Interface DHCP Server IP Address: 10.77.244.220
AP Manager Interface IP Address: 10.77.244.205
AP-Manager is on Management subnet, using same values
AP Manager Interface DHCP Server (10.77.244.220):
Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: Test
Network Name (SSID): Cisco123
Allow Static IP Addresses [YES][no]: yes
Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.
Enter Country Code (enter 'help' for a list of countries) [US]:
Enable 802.11b Network [YES][no]: yes
Enable 802.11a Network [YES][no]: yes
Enable 802.11g Network [YES][no]: yes
Enable Auto-RF [YES][no]: yes

Configuration saved!
Resetting system with new configuration..
```

これらのパラメータにより、WLC が基本動作用に設定されます。この設定例では、WLC で管理インターフェイス IP アドレスとして 10.77.244.204 が使用され、AP マネージャ インターフェイス IP アドレスとして 10.77.244.205 が使用されています。

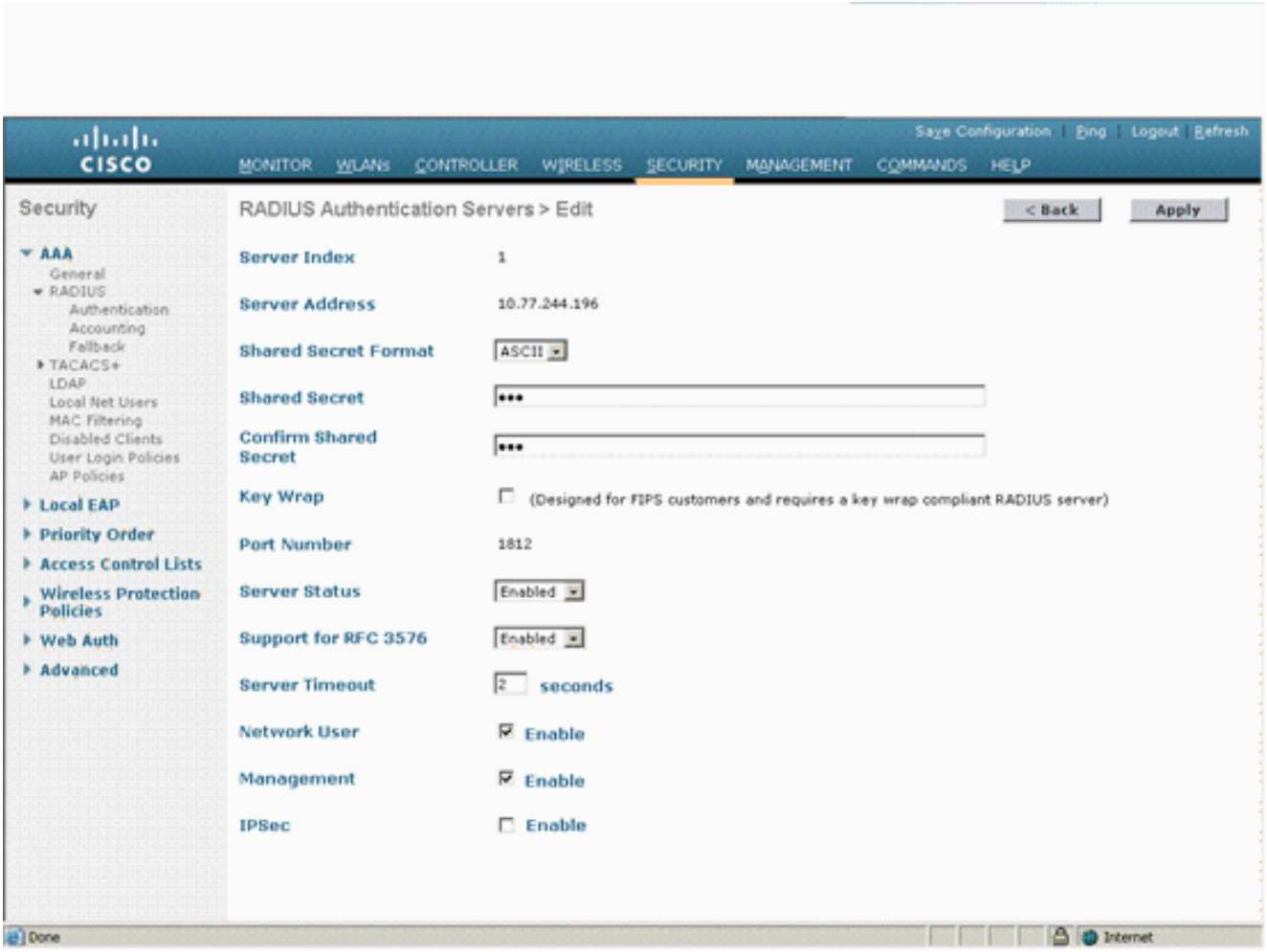
WLC でその他の機能を設定するには、事前に Lightweight AP を WLC に登録する必要があります。このドキュメントでは、Lightweight AP が WLC に登録されていることが前提となっています。Lightweight AP を WLC に登録する方法についての詳細は、『ワイヤレス LAN コントローラ ( WLC ) への Lightweight AP ( LAP ) の登録』を参照してください。

## 外部 RADIUS サーバによる RADIUS 認証用の WLC の設定

ユーザ クレデンシャルを外部 RADIUS サーバに転送するには、WLC を設定する必要があります。そうすると、外部 RADIUS サーバは、ユーザのクレデンシャルを検証し、ワイヤレス クライアントにアクセス権を付与します。

外部 RADIUS サーバ用に WLC 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 から [Security]、[RADIUS]、[Authentication] を選択して、[RADIUS Authentication Servers] ページを表示します。次に、[New] をクリックして、RADIUS サーバを定義します。




2. [RADIUS Authentication Servers] > [New] ページで RADIUS サーバのパラメータを定義します。RADIUS サーバ IP アドレス、共有秘密、ポート番号、サーバ ステータスなどのパラメータがあります。[Network User] チェックボックスと [Management] チェックボックスでは、WLC 管理とネットワーク ユーザに RADIUS ベースの認証を適用するかどうかを指定します。この例では、次のように、Cisco Secure ACS を IP アドレスが 10.77.244.196 である RADIUS サーバとして使用しています。
3. これで、WLC では認証に RADIUS サーバを使用できます。[Security] > [Radius] > [Authentication] の順に選択すると、RADIUS サーバが表示されて確認できます。


RFC 3576 は、Cisco CNS Access Registrar（CAR）RADIUS サーバではサポートされてい

ますが、Cisco Secure ACS Server バージョン 4.0 以前ではサポートされていません。ローカル RADIUS サーバ機能を使用して、ユーザを認証することもできます。ローカル RADIUS サーバは、バージョン 4.1.171.0 のコードで導入されました。これより前のバージョンが稼働する WLC には、ローカル RADIUS の機能はありません。ローカル EAP は認証方法であり、これを使用して、ユーザとワイヤレス クライアントをローカルに認証できます。この機能は、バックエンド システムが中断したり外部認証サーバが停止したりした場合でもワイヤレス クライアントとの接続を維持する必要があるリモート オフィスでの使用を想定して作られています。ローカル EAP は、ローカル ユーザ データベースまたは LDAP バックエンド データベースからユーザのクレデンシャルを取得してユーザを認証します。ローカル EAP では、コントローラとワイヤレス クライアントとの間で、LEAP、PAC を使用する EAP-FAST、証明書を使用する EAP-FAST、および EAP-TLS 認証がサポートされています。ローカル EAP は、バックアップ認証システムとして設計されています。コントローラに RADIUS サーバが設定されている場合、コントローラでは最初に、RADIUS サーバでのワイヤレス クライアントの認証が試みられます。ローカル EAP が試されるのは、RADIUS サーバがタイムアウトしたため、または RADIUS サーバが設定されていないために、RADIUS サーバが検出されない場合のみです。ワイヤレス LAN コントローラでローカル EAP を設定する方法についての詳細は、『EAP-FAST および LDAP サーバを使用したワイヤレス LAN コントローラでのローカル EAP 認証の設定例』を参照してください。

## WLAN パラメータの設定

次に、ワイヤレス ネットワークに接続するためにクライアントが使用する WLAN を設定します。WLC の基本パラメータを設定する際に、WLAN の SSID も設定してあります。この SSID を WLAN に使用することも、新しい SSID を作成することもできます。この例では、新しい SSID を作成します。

**注：コントロ**ーラには最大16のWLANを設定できます。Cisco WLAN Solution では、Lightweight AP 用に最大で 16 の WLAN を制御できます。各 WLAN には一意のセキュリティ ポリシーを割り当てることができます。Lightweight AP では、すべてのアクティブな Cisco WLAN Solution WLAN SSID がブロードキャストされ、各 WLAN に定義されているポリシーが適用されます。

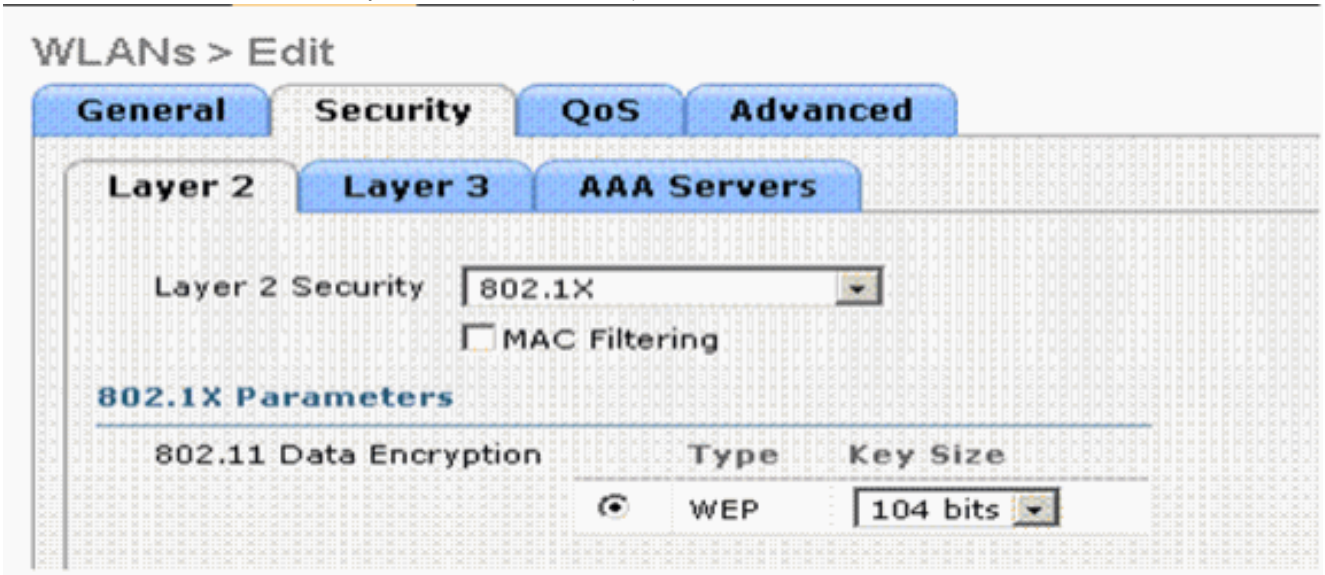
新しい WLAN およびそれに関連するパラメータを設定するには、次の手順を実行してください。

1. コントローラの GUI で [WLANs] をクリックして、[WLANs] ページを表示します。このページには、コントローラに存在する WLAN の一覧が表示されます。
2. 新しい WLAN を作成するには、[New] をクリックします。WLAN のプロファイル名と WLAN SSID を入力し、**Apply** をクリックします。この例では、SSID として Cisco を使用しています。

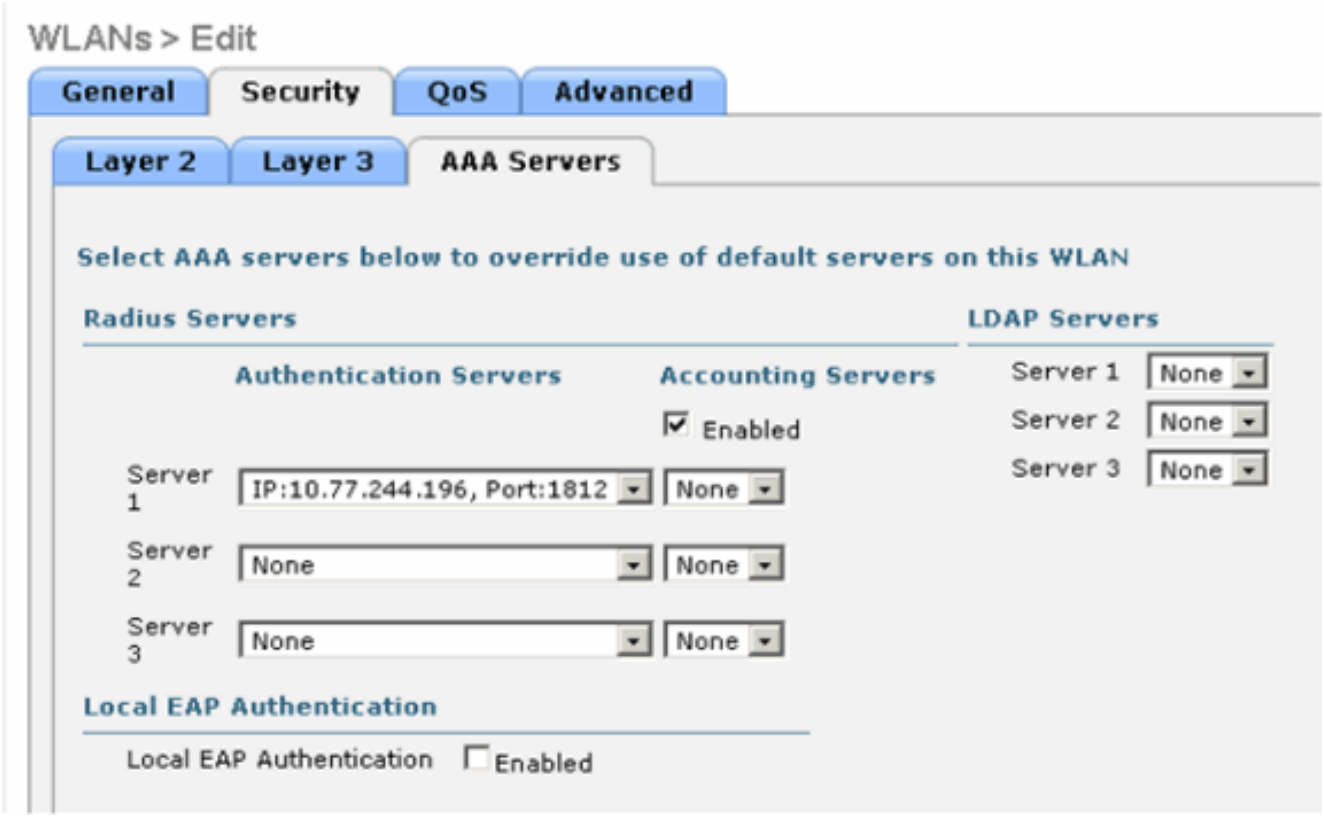
3. 新しい WLAN を作成すると、新しい WLAN に対する [WLAN] > [Edit] ページが表示されます。このページでは、全般ポリシー、セキュリティ ポリシー、QOS ポリシー、およびその他の高度なパラメータを含む、この WLAN に固有の各種パラメータを定義できます。


ドロップダウン メニューから適切な Interface を選択します。WLAN ネットワークの要件に基づいて、その他のパラメータを変更できます。WLAN をイネーブルにするには、General Policies の下の **Status** ボックスにチェックマークを入れます。

4. **[Security]** タブをクリックし、**[Layer 2 Security]** を選択します。[Layer 2 Security] ドロップダウン メニューから、**[802.1x]** を選択します。802.1x のパラメータでは、WEP 鍵のサイズを選択します。この例では 128 ビットの WEP キーを使用します。これは 104 ビットの WEP キーと 24 ビットの初期化ベクトルです。




5. **AAA Servers** タブを選択します。[Authentication Servers (RADIUS)] ドロップダウン メニューから、適切な RADIUS サーバを選択します。このサーバは、ワイヤレス クライアントを認証するために使用されます。

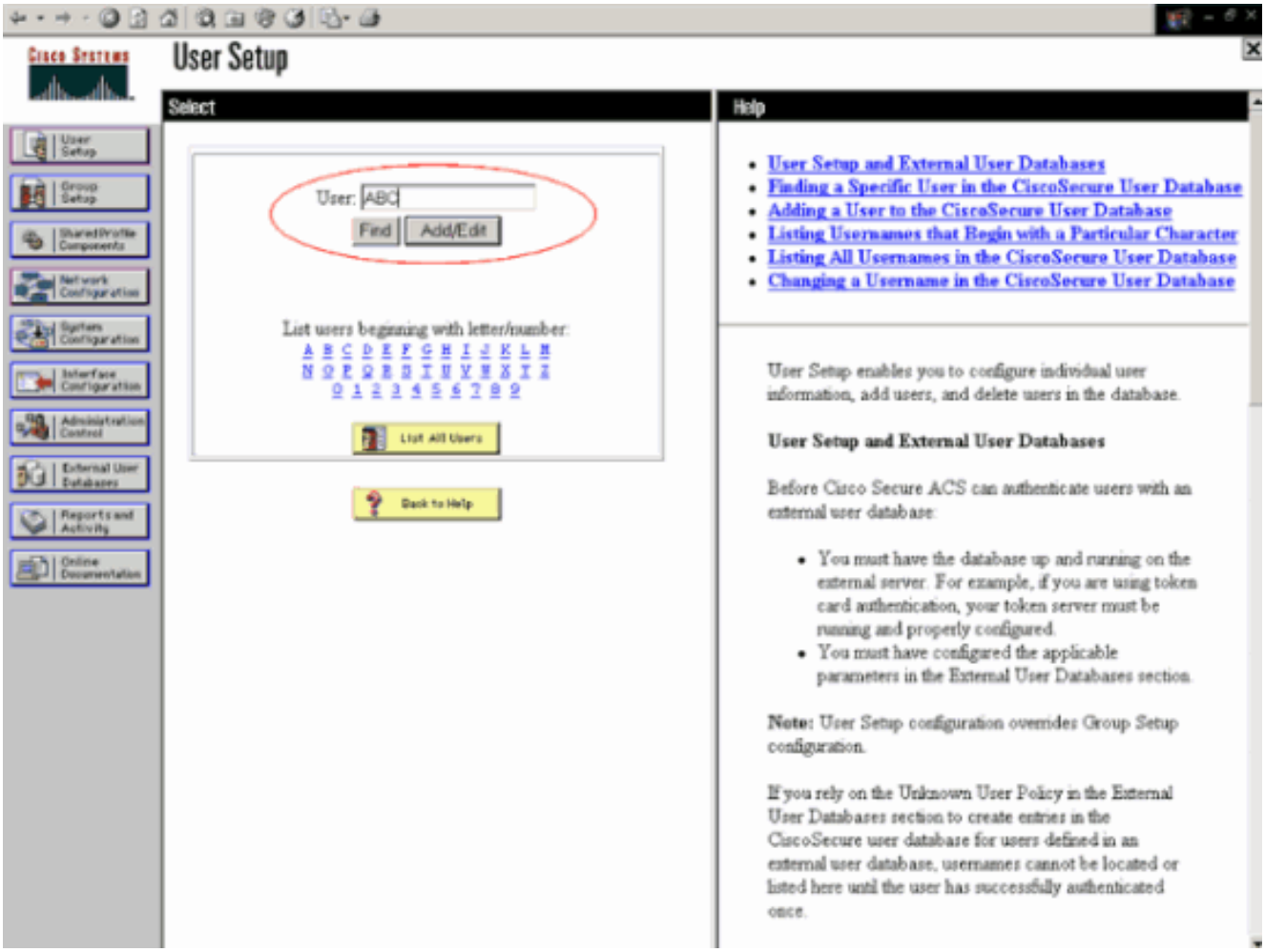



6. [Apply] をクリックして、設定を保存します。

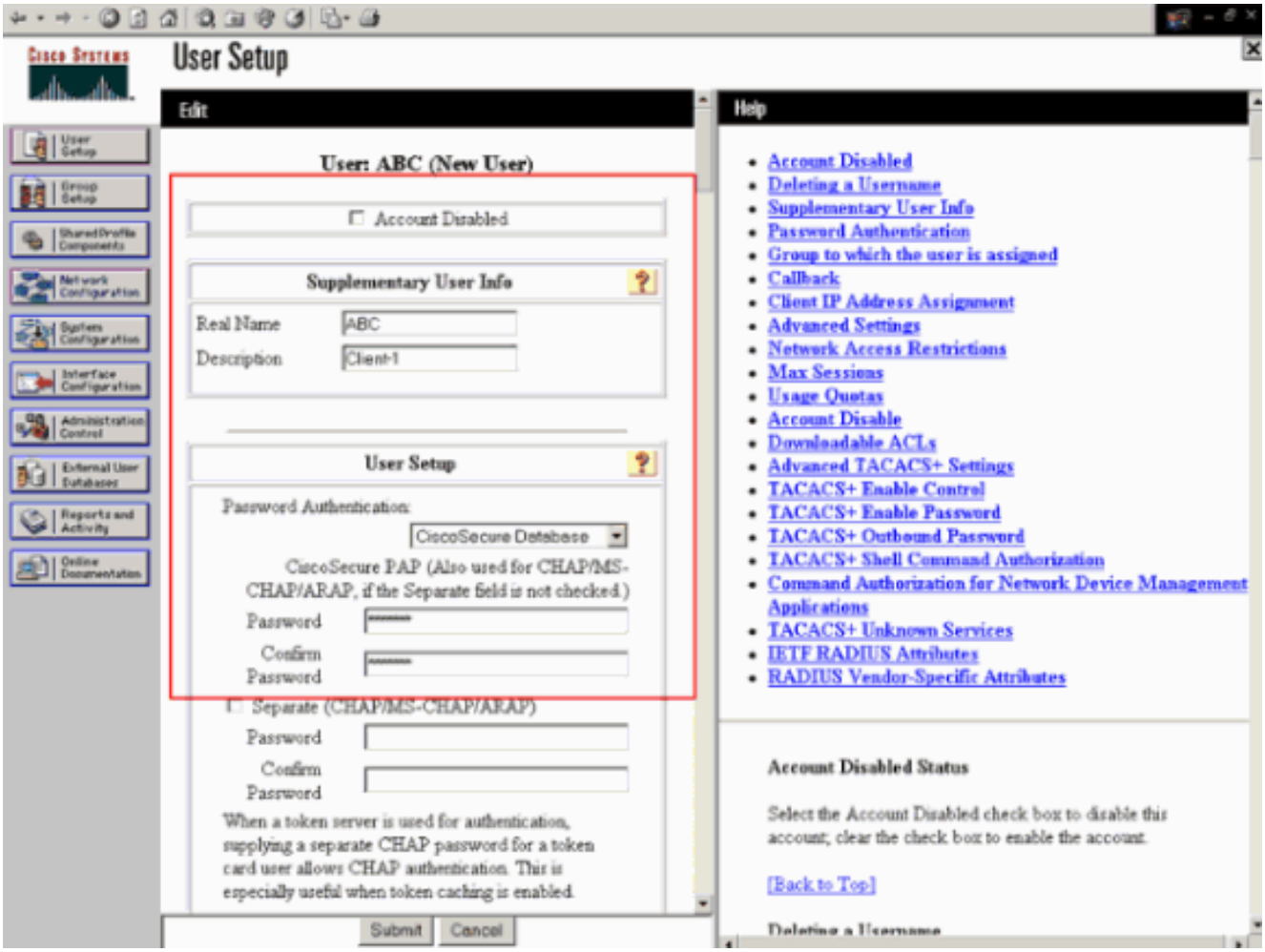
## 外部 RADIUS サーバとしての Cisco Secure ACS の設定および認証クライアント用のユーザ データベースの作成

Cisco Secure ACS でユーザ データベースを作成して EAP 認証を有効にするには、次の手順を実行します。

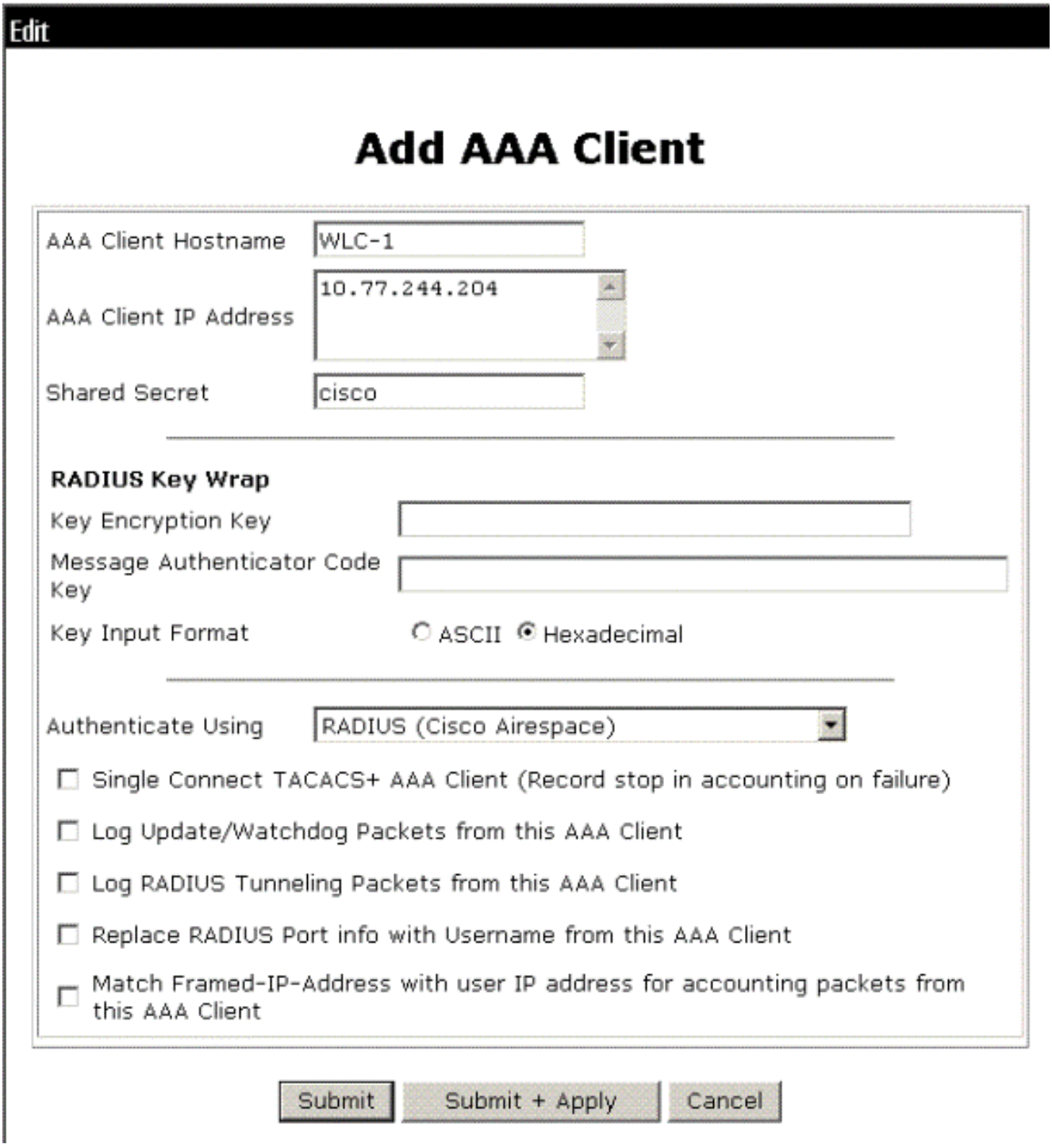
1. ACS GUI から [User Setup] を選択し、ユーザ名を入力して、[Add/Edit] をクリックします。この例では、ユーザは **ABC です。**



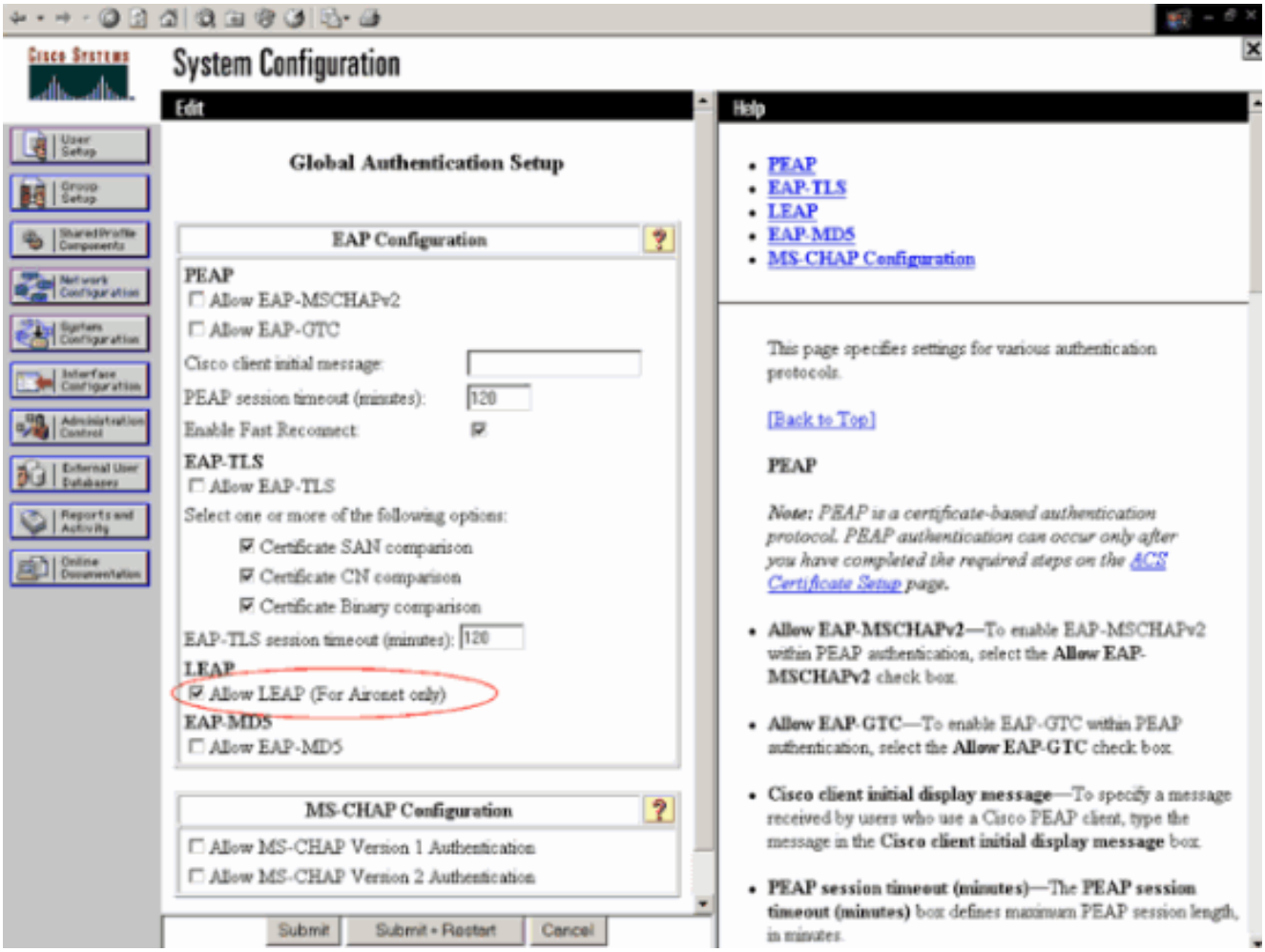

2. [User Setup] ページが表示されたら、ユーザに固有のすべてのパラメータを定義します。この例では、ユーザ名、パスワード、および補足ユーザ情報（Supplementary User Information）を設定しています。EAP 認証に必要なのは、これらのパラメータだけです。さらにデータベースにユーザを追加するには、[**送信**] をクリックしてから同じ手順を繰り返します。デフォルトでは、すべてのユーザはデフォルト グループの下にグループ化され、グループに定義されている同じポリシーが割り当てられます。特定のユーザを別のグループに割り当てる場合についての詳細は、『Cisco Secure ACS for Windows Server 3.2 ユーザ ガイド』の「ユーザ グループ管理」セクションを参照してください。




3. ACS サーバ上の AAA クライアントとして、コントローラを定義します。ACS の GUI で [Network Configuration] をクリックします。[Network Configuration] ページが表示されたら、WLC の名前、IP アドレス、共有秘密鍵、および認証方式（RADIUS Cisco 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。**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。




4. 意図した EAP 認証方法を実行するように認証サーバが設定されていることを確認するには、[System Configuration] 、[Global Authentication Setup] **をクリックします。**EAP の設定で、適切な EAP 方法を選択します。この例では、LEAP 認証を使用しています。設定が終了したら、[Submit] をクリックします。

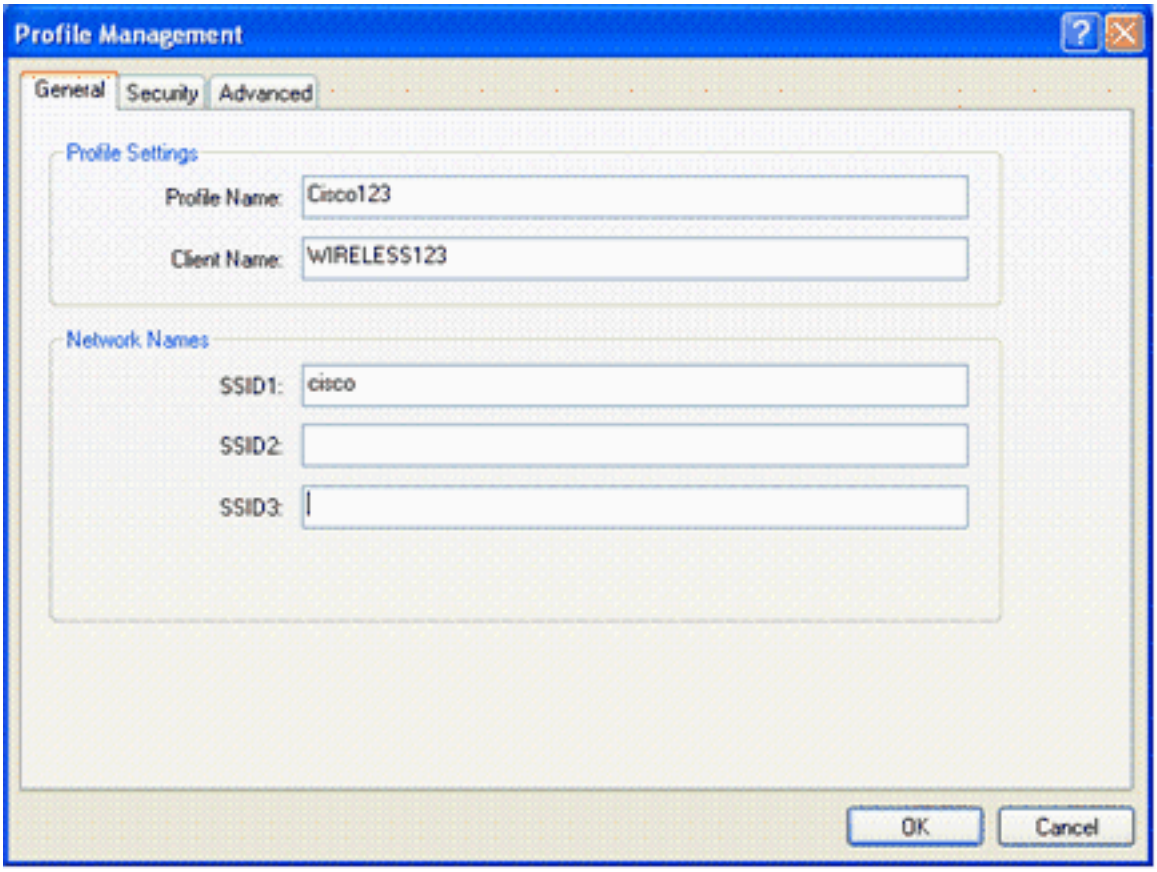



## クライアントの設定

適切な EAP の種類用にクライアントも設定する必要があります。クライアントは EAP ネゴシエーション プロセス中に EAP の種類をサーバに提示します。サーバがその EAP の種類をサポートしている場合、サーバはその EAP の種類に対して確認応答します。EAP の種類がサポートされていない場合、サーバは否定応答を送信し、クライアントは再度別の EAP 方式を使用してネゴシエートします。このプロセスは、サポートされている EAP の種類がネゴシエートされるまで継続します。この例では、EAP の種類として LEAP を使用しています。

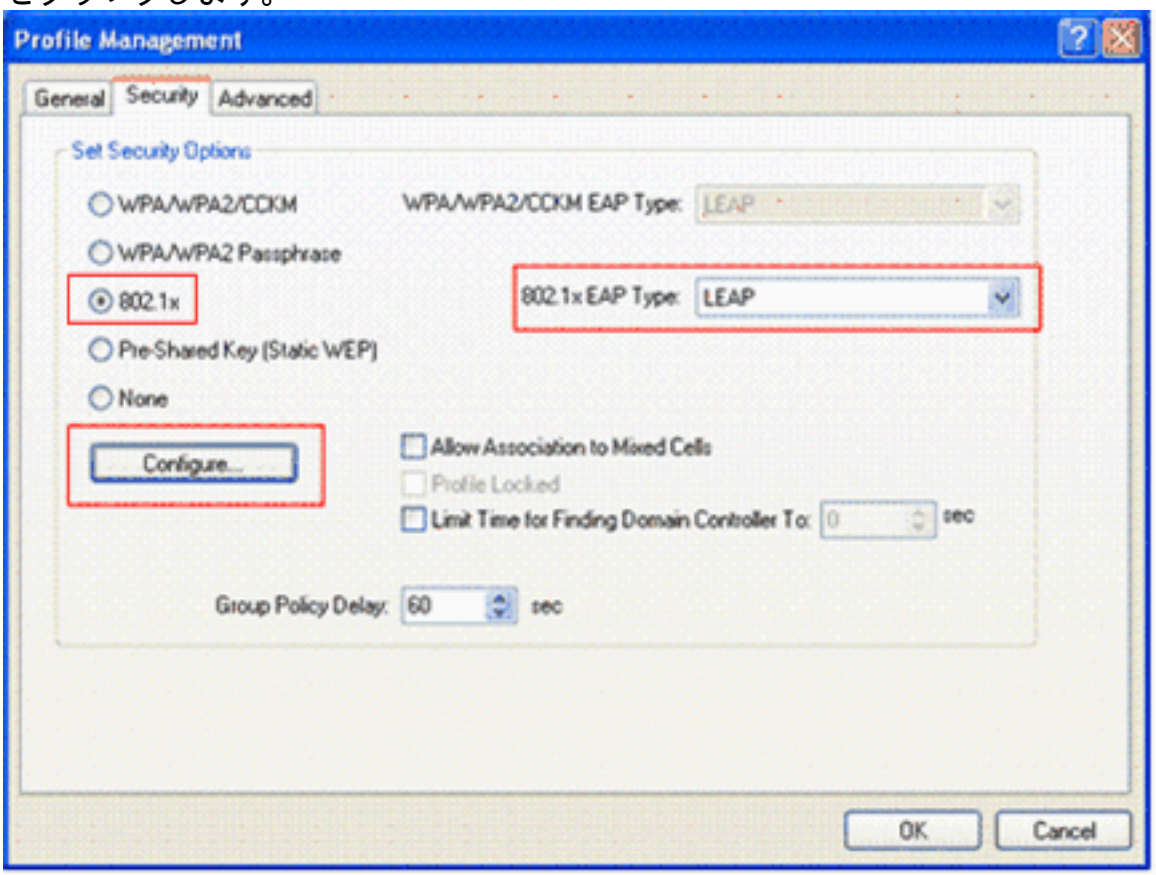
Aironet Desktop Utility を使用してクライアント上で LEAP を設定するには、次の手順を実行します。

1. [Aironet Utility] アイコンをダブルクリックして Aironet Utility を開きます。
2. **[Profile Management]**タブをクリックします。
3. プロファイルをクリックし、**[Modify]** を選択します。
4. [General] タブでプロファイル名を選択します。WLAN の **SSID** を入力します。



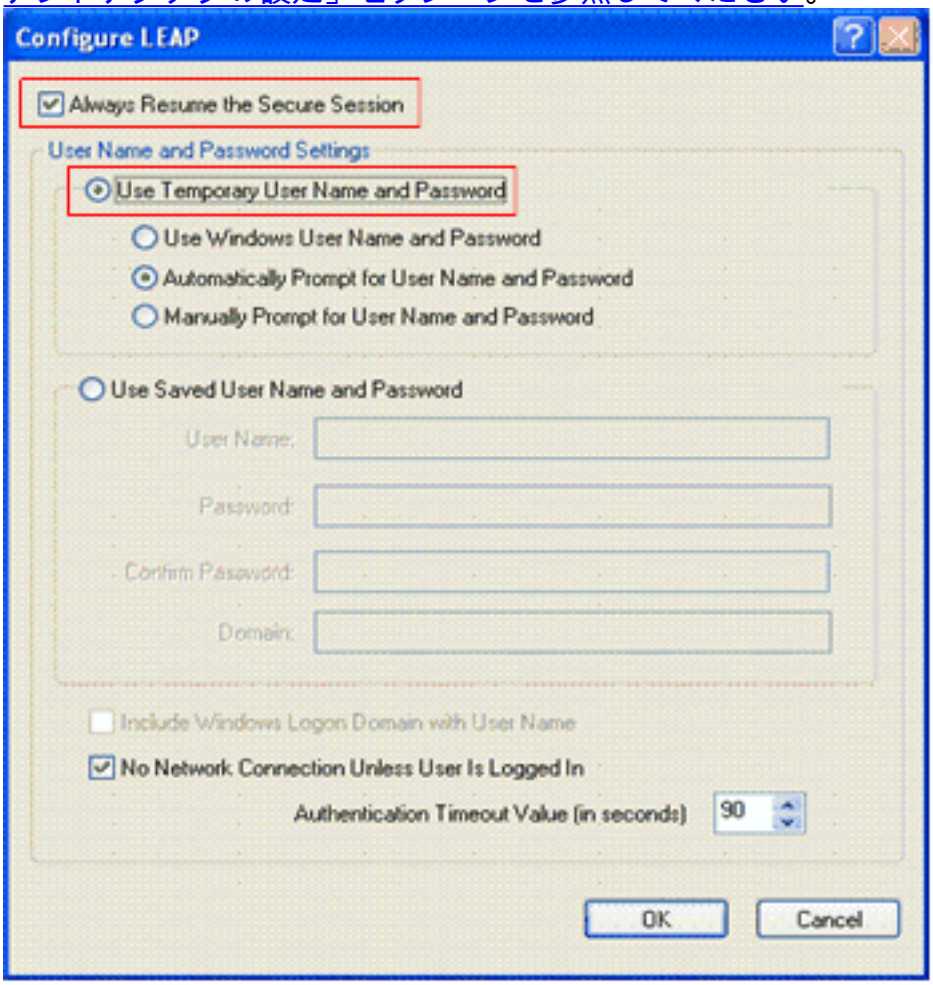

**注**：SSIDは大文字と小文字が区別され、WLCで設定されているSSIDと完全に一致する必要があります。

5. [Security] タブで、[*802.1x*] を選択します。EAP の種類として [**LEAP**] を選択し、[**Configure**] をクリックします。




6. [**Use Temporary Username and Password**] を選択します。これによりコンピュータが再起動するたびにユーザ クレデンシャルを入力するよう求められます。ここに表示されている 3 つのオプションのいずれかをクリックします。この例では Automatically Prompt for

**Username and Password** を使用します。これにより、Windows にログインする前に *Windows のユーザ名とパスワード*を入力する以外にも *LEAP* のユーザ クレデンシャルを入力する必要があります。クライアント アダプタがローミングし、ネットワークへの再関連付けを行うたびに、クレデンシャルを再入力させるためのプロンプトを出す必要なく、常に LEAP サプリカントに以前のセッションの再開を試行させる場合は、ウィンドウの最上部の **[Always Resume the Secure Session]** チェックボックスにチェックマークを入れます。**注：その他のオプション**の詳細については、『Cisco Aironet 802.11a/b/gワイヤレスLANクライアントアダプタ（CB21AGおよびPI21AG）インストールおよび設定ガイド』の「クライアントアダプタの設定」セクションを参照してください。




7. [Advanced] タブでは、プリアンブル、Aironet 拡張機能、および出力、周波数などその他の 802.11 のオプションを設定できます。
8. [OK] をクリックします。これでクライアントは設定済みのパラメータを使用して関連付けを行います。

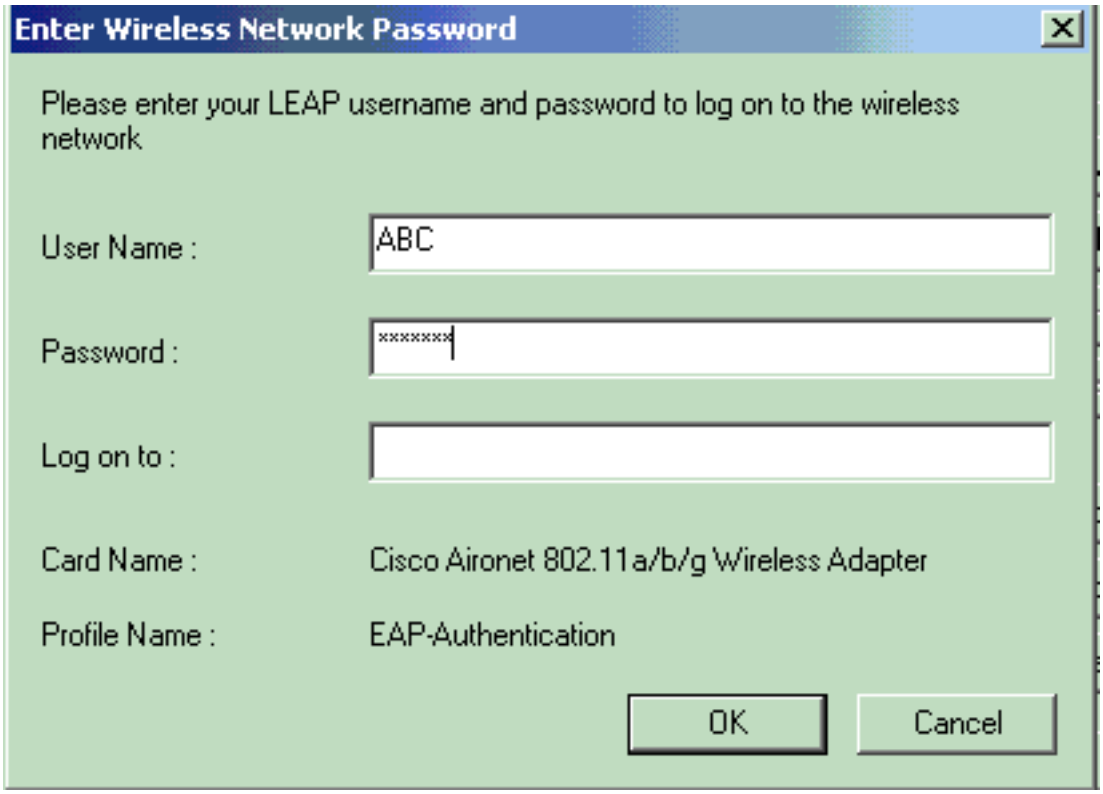
## 確認

ここでは、設定が正常に機能しているかどうかを確認します。

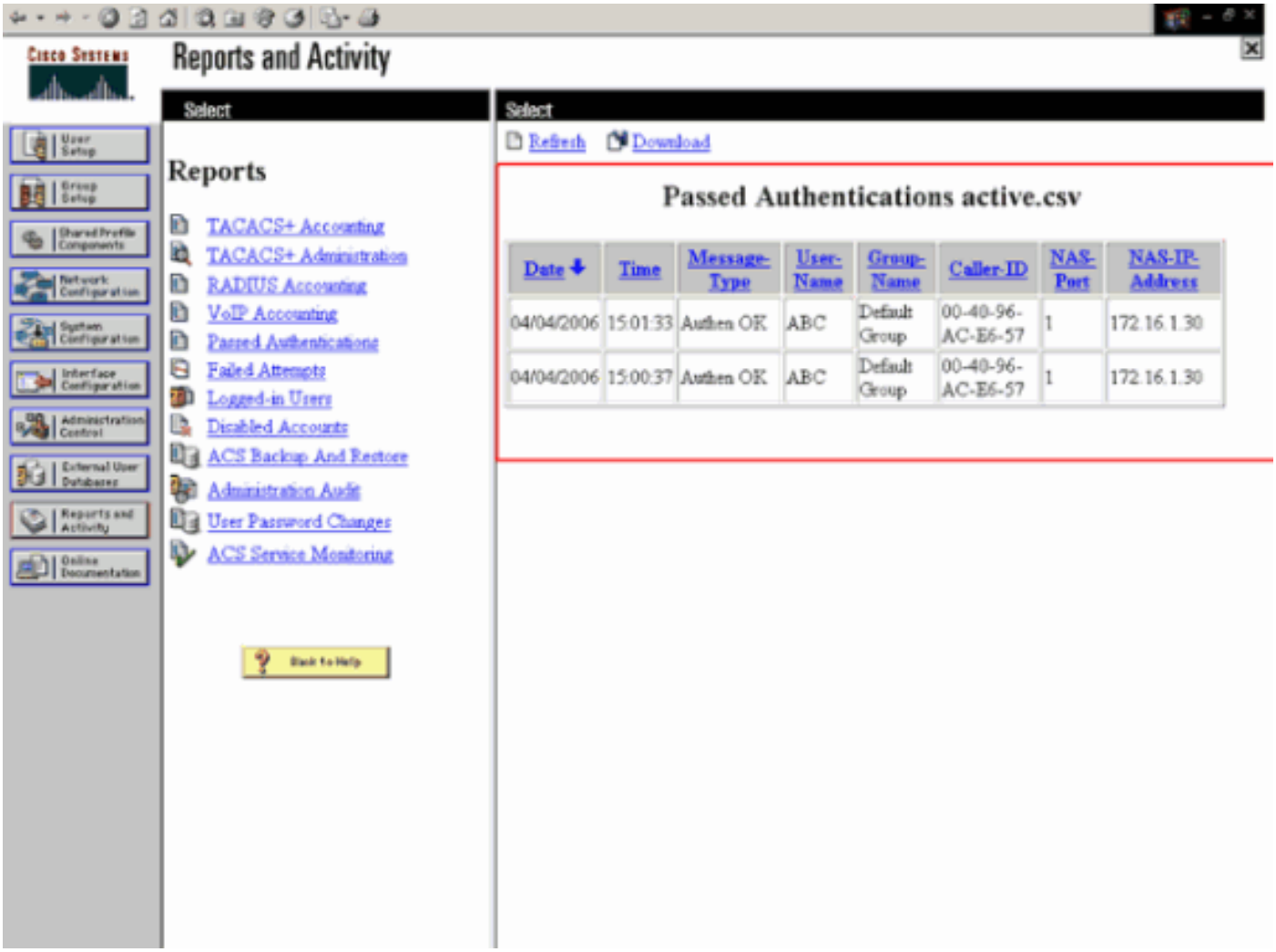
設定が意図したとおりに動作することを確認するには、LEAP 認証を使用して、ワイヤレス クライアントと Lightweight AP の関連付けを試みます。

**注：このドキュメント**では、クライアントプロファイルがLEAP認証用に設定されていることを前提としています。802.11 a/b/g ワイヤレス クライアント アダプタを LEAP 認証用に設定する方法についての詳細は、EAP 認証の使用方法を参照してください。

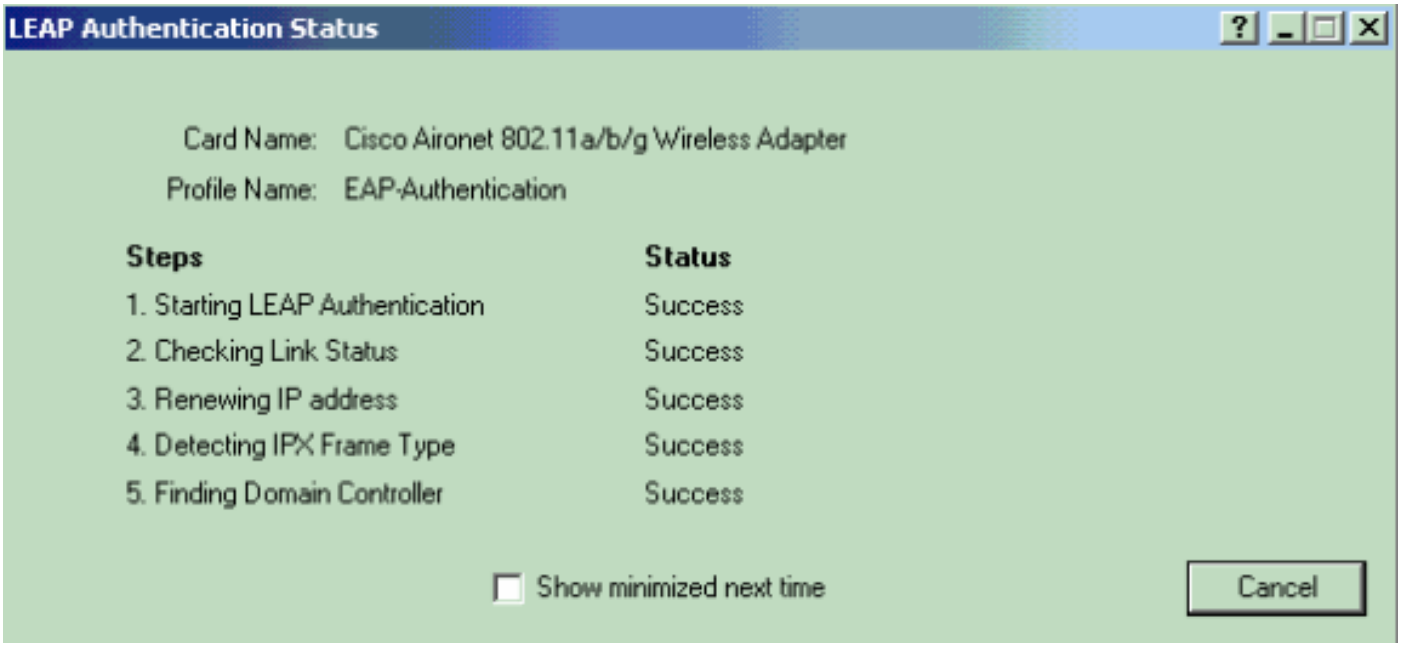
ワイヤレス クライアントのプロファイルをアクティブにすると、ユーザは LEAP 認証のためのユーザ名とパスワードの入力を求められます。以下が一例です。




Lightweight AP および続いて WLC が、クレデンシャルを検証するために、ユーザのクレデンシャルを外部 RADIUS サーバ（Cisco Secure ACS）に渡します。ユーザ クレデンシャルを検証するため、RADIUS サーバはデータをユーザ データベースと比較し、ユーザ クレデンシャルが有効であれば、ワイヤレス クライアントにアクセス権を付与します。ACS サーバ上の Passed Authentication レポートには、クライアントが RADIUS 認証をパスしたことが示されます。以下が一例です。




RADIUS 認証に成功すると、ワイヤレス クライアントは Lightweight AP と関連付けられます。

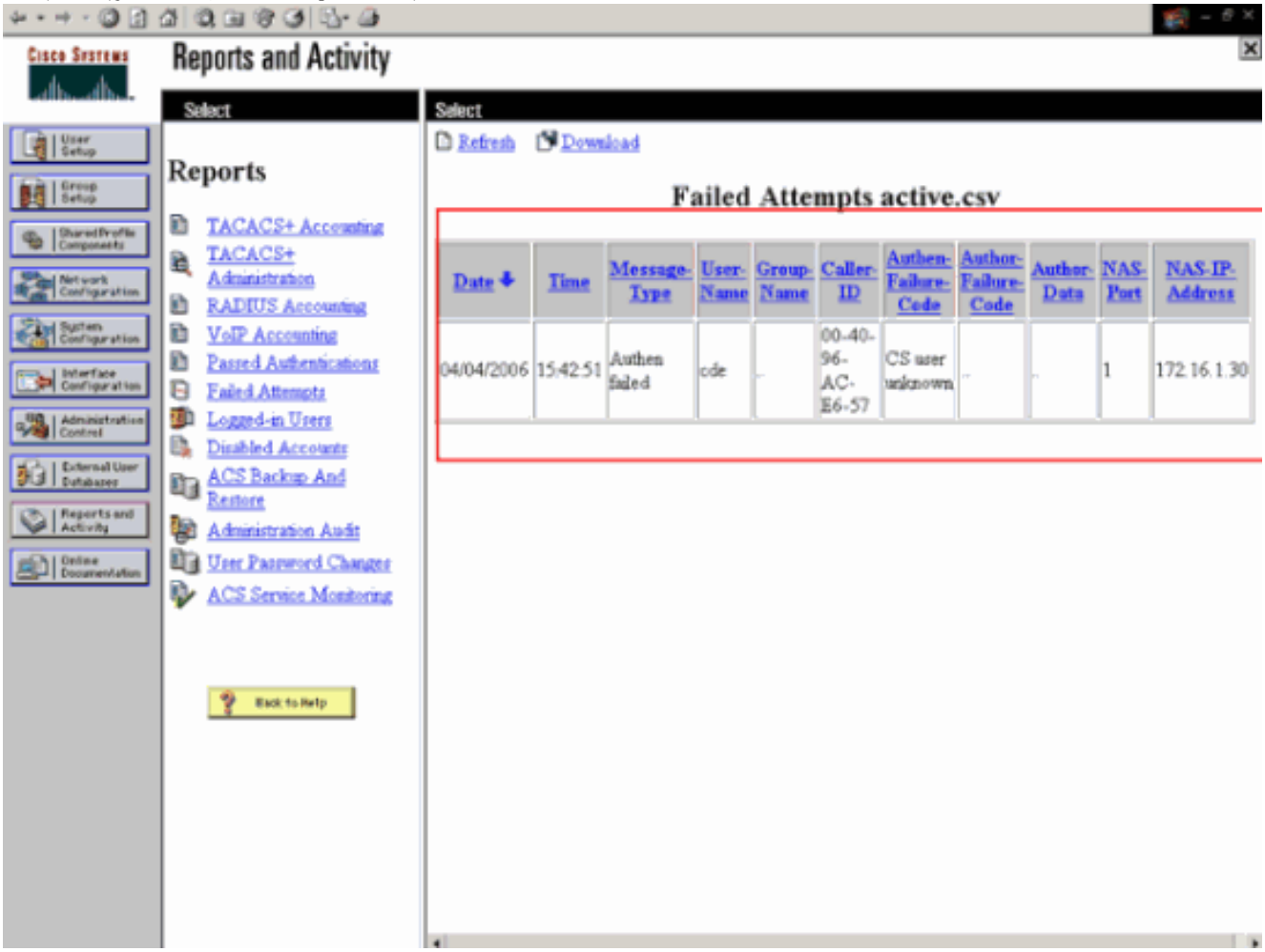



WLC GUI の [Monitor] タブの下でこれを確認することもできます。[Monitor] > [Clients] の順に選択し、クライアントの MAC アドレスを確認します。


## トラブルシュート

設定をトラブルシューティングするには、次の手順を実行します。

1. AP が WLC に登録されているかどうかを確認するには、**debug lwapp events enable** コマンドを使用します。
2. RADIUS サーバがワイヤレス クライアントから認証要求を受信して検証するかどうかを確認します。WLC が RADIUS サーバにアクセスできたかどうかを確認するには、NAS-IP-Address、日付および時刻を確認します。そのためには、ACS サーバで Passed Authentications レポートと Failed Attempts レポートを調べます。これらのレポートは、ACS サーバの [Reports and Activities] で見ることができます。RADIUS サーバでの認証が失敗する場合の例を次に示します。




**注：Cisco Secure ACSのトラブルシューティング**方法およびデバッグ情報の取得方法につ

いては、『Cisco Secure ACS for Windowsのバージョンおよ びAAAデバッグ情報の取得』を参照してください。

3. また、次の **debug** コマンドを使用して、AAA 認証のトラブルシューティングを行うこともできます。**debug aaa all enable**：すべての AAA メッセージのデバッグを設定します。**debug dot1x packet enable**：すべての dot1x パケットのデバッグをイネーブルにします。次に **debug 802.1x aaa enable** コマンドの出力例を示します。

```
(Cisco Controller) >debug dot1x aaa enable

*Sep 23 15:15:43.792: 00:40:96:ac:dd:05 Adding AAA_ATT_USER_NAME(1) index=0
*Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLING_STATION_ID(31)
    index=1
*Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLED_STATION_ID(30)
    index=2
*Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT(5) index=3
*Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IP_ADDRESS(4) index=4
*Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IDENTIFIER(32)
    index=5
*Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_VAP_ID(1) index=6
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_SERVICE_TYPE(6) index=7
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_FRAMED_MTU(12) index=8
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT_TYPE(61) index=9
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_EAP_MESSAGE(79) index=10
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_MESS_AUTH(80) index=11
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 AAA EAP Packet created request =
    0x1533a288.. !!!!
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Sending EAP Attribute (code=2, length=8,
    id=2) for mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.794: 00000000: 02 02 00 08 01 41 42 43
    .....ABC
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 [BE-req] Sending auth request to
    'RADIUS' (proto 0x140001)
*Sep 23 15:15:43.799: 00:40:96:ac:dd:05 [BE-resp] AAA response 'Interim
    Response'
*Sep 23 15:15:43.799: 00:40:96:ac:dd:05 [BE-resp] Returning AAA response
*Sep 23 15:15:43.799: 00:40:96:ac:dd:05 AAA Message 'Interim Response' received
    for mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.799: 00:40:96:ac:dd:05 Received EAP Attribute (code=1,
    length=19,id=3, dot1xcb->id = 2) for mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.799: 00000000: 01 03 00 13 11 01 00 08  42 3a 8e d1 18 24 e8 9f
    ........B:...
*Sep 23 15:15:43.799: 00000010: 41 42 43
    ABC
*Sep 23 15:15:43.799: 00:40:96:ac:dd:05 Skipping AVP (0/80) for mobile
    00:40:96:ac:dd:05
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_USER_NAME(1) index=0
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLING_STATION_ID(31)
    index=1
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLED_STATION_ID(30)
    index=2
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT(5) index=3
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IP_ADDRESS(4) index=4
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IDENTIFIER(32)
    index=5
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_VAP_ID(1) index=6
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_SERVICE_TYPE(6) index=7
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_FRAMED_MTU(12) index=8
*Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT_TYPE(61) index=9
*Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Adding AAA_ATT_EAP_MESSAGE(79) index=10
*Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Adding AAA_ATT_RAD_STATE(24) index=11
*Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Adding AAA_ATT_MESS_AUTH(80) index=12
*Sep 23 15:15:43.902: 00:40:96:ac:dd:05 AAA EAP Packet created request =
    0x1533a288.. !!!!
```

```
*Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Sending EAP Attribute (code=2,
    length=35, id=3) for mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.902: 00000000: 02 03 00 23 11 01 00 18  83 f1 5b 32 cf 65 04 ed
    ...#......[2.e..
*Sep 23 15:15:43.902: 00000010: da c8 4f 95 b4 2e 35 ac  c0 6b bd fa 57 50 f3 13
    ..O...5..k..WP..
*Sep 23 15:15:43.904: 00000020: 41 42 43
    ABC
*Sep 23 15:15:43.904: 00:40:96:ac:dd:05 [BE-req] Sending auth request to
    'RADIUS' (proto 0x140001)
*Sep 23 15:15:43.907: 00:40:96:ac:dd:05 [BE-resp] AAA response 'Interim
    Response'
*Sep 23 15:15:43.907: 00:40:96:ac:dd:05 [BE-resp] Returning AAA response
*Sep 23 15:15:43.907: 00:40:96:ac:dd:05 AAA Message 'Interim Response' received
    for mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.907: 00:40:96:ac:dd:05 Received EAP Attribute (code=3,
    length=4,id=3, dot1xcb->id = 3) for mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.907: 00000000: 03 03 00 04
    ....
*Sep 23 15:15:43.907: 00:40:96:ac:dd:05 Skipping AVP (0/80) for mobile
    00:40:96:ac:dd:05
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_USER_NAME(1) index=0
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLING_STATION_ID(31)
    index=1
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLED_STATION_ID(30)
    index=2
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT(5) index=3
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IP_ADDRESS(4) index=4
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IDENTIFIER(32)
    index=5
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_VAP_ID(1) index=6
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_SERVICE_TYPE(6) index=7
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_FRAMED_MTU(12) index=8
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT_TYPE(61) index=9
*Sep 23 15:15:43.915: 00:40:96:ac:dd:05 Adding AAA_ATT_EAP_MESSAGE(79) index=10
*Sep 23 15:15:43.915: 00:40:96:ac:dd:05 Adding AAA_ATT_RAD_STATE(24) index=11
*Sep 23 15:15:43.915: 00:40:96:ac:dd:05 Adding AAA_ATT_MESS_AUTH(80) index=12
*Sep 23 15:15:43.915: 00:40:96:ac:dd:05 AAA EAP Packet created request =
    0x1533a288.. !!!!
*Sep 23 15:15:43.915: 00:40:96:ac:dd:05 Sending EAP Attribute (code=1,
    length=19, id=3) for mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.915: 00000000: 01 03 00 13 11 01 00 08  29 23 be 84 e1 6c d6 ae
    ........)#...l..
*Sep 23 15:15:43.915: 00000010: 41 42 43
    ABC
*Sep 23 15:15:43.915: 00:40:96:ac:dd:05 [BE-req] Sending auth request to
    'RADIUS' (proto 0x140001)
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 [BE-resp] AAA response 'Success'
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 [BE-resp] Returning AAA response
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 AAA Message 'Success' received for
    mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[0]: attribute 8,
    vendorId 0, valueLen 4
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[1]: attribute 79,
    vendorId 0, valueLen 35
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 Received EAP Attribute (code=2,
    length=35,id=3) for mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.918: 00000000: 02 03 00 23 11 01 00 18  03 66 2c 6a b3 a6 c3 4c
    ...#.....f,j...L
*Sep 23 15:15:43.918: 00000010: 98 ac 69 f0 1b e8 8f a2  29 eb 56 d6 92 ce 60 a6
    ..i.....).V...`.
*Sep 23 15:15:43.918: 00000020: 41 42 43
    ABC
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[2]: attribute 1,
```

```
    vendorId 9, valueLen 16
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[3]: attribute 25,
    vendorId 0, valueLen 21
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[4]: attribute 80,
    vendorId 0, valueLen 16
```

**注：**デバッグ出力の一部の行は、スペースの制約によりラップされています。

4. RADIUS サーバがユーザのクレデンシャルを受信しているかどうかを調べるには、WLC でログを監視します。WLC GUI からログを確認するには、**Monitor** をクリックします。左側のサイド メニューから、[Statistics] をクリックし、オプションのリストから [Radius server] をクリックします。WLC での RADIUS サーバの設定が正しくないと、RADIUS サーバでユーザ クレデンシャルが受信されない場合があるので、この監視は非常に重要です。RADIUS パラメータの設定が正しくない場合の WLC でのログの表示を次に示します。


**show wlan summary** コマンドを組み合わせて使用することで、どの WLAN で RADIUS サーバ認証が使用されているかがわかります。その後、**show client summary** コマンドを使用すると、RADIUS WLAN での認証に成功した MAC アドレス（クライアント）がわかります。また、この情報を、Cisco Secure ACS の成功した試行または失敗した試行のログと相関させることもできます。

## トラブルシューティングのヒント

- コントローラで、RADIUS サーバが active 状態であり、standby や disabled ではないことを確認します。
- RADIUS サーバが WLC からアクセスできるかどうかを調べるには、**ping** コマンドを使用します。
- WLAN（SSID）のドロップダウン メニューで RADIUS サーバが選択されていることを確認します。
- WPAを使用する場合は、Windows XP SP2用の最新のMicrosoft WPAホットフィックスをインストールする必要があります。また、クライアントサプリカント用のドライバを最新にアップグレードする必要があります。
- Microsoft wireless-0 ユーティリティによってカードが管理されている XP SP2 での証明書などのように、PEAP を行う場合は、Microsoft から KB885453 パッチを入手する必要があります。Windows Zero Config/client サプリカントを使用する場合は、[**Enable Fast Reconnect**] を無効にします。この設定を行うには、[Wireless Network Connection Properties] > [Wireless Networks] > [Preferred networks] の順に選択します。次に、[SSID] > [Properties] > [Open] > [WEP] > [Authentication] > [EAP type] > [PEAP] > [Properties] > [Enable Fast Reconnect] の順に選択します。設定を有効または無効にするためのオプションは、ウィンドウの最後にあります。
- Intel 2200 または 2915 カードを使用する場合は、Intel の Web サイトで、次のカードに関す

る既知の問題についての説明を参照してください。Intel® PRO/Wireless 2200BG Network ConnectionIntel® PRO/Wireless 2915ABG Network Connection問題の発生を防ぐため、最新の Intel ドライバをダウンロードしてください。Intel ドライバは、http://downloadcenter.intel.com/ からダウンロードできます。

- アグレッシブ フェールオーバー機能を WLC でイネーブルにすると、WLC は非常にアグレッシブになるため、AAA サーバが not responding であるとマーキングされてしまいます。ただし、サイレント破棄を行う場合は、AAA サーバはその特定のクライアントに対してのみ応答しない可能性があるので、これを行わないようにする必要があります。有効な証明書を持つ他の有効なクライアントには応答する可能性があります。しかし、その場合でも WLC により AAA サーバが「not responding」および「not functional」としてマークされる可能性があります。これを解決するために、アグレッシブなフェールオーバー機能を無効にします。そのためには、コントローラの GUI から **config radius aggressive-failover disable** コマンドを実行します。この機能を無効にすると、その RADIUS サーバからの応答の受信を 3 つのクライアントが連続して失敗する場合にのみ、コントローラは次の AAA サーバにフェールオーバーします。

## EAP タイマーの操作

802.1x 認証時に DOT1X-1-MAX_EAPOL_KEY_RETRANS_FOR_MOBILE: `MAX EAPOL-Key M1 retransmissions reached for mobile xx:xx:xx:xx:xx`

このエラー メッセージは、クライアントが WPA ( 802.1x ) キー ネゴシエーション中にコントローラに対して時間内に応答しなかったことを示しています。コントローラは、キー ネゴシエーション中の応答用にタイマーを設定します。このメッセージが表示される場合、通常はサプリカントに関する問題に原因があります。最新バージョンのクライアントのドライバおよびファームウェアを稼働していることを確認します。WLC には、クライアント認証を支援するために操作可能な EAP タイマーがいくつか提供されています。これらの EAP タイマーには次のようなものがあります。

```
EAP-Identity-Request Timeout
EAP-Identity-Request Max Retries
EAP-Request Timeout (seconds)
EAP-Request Max Retries
EAPOL-Key Timeout
EAPOL-Key Max Retries
```

これらの値を操作する前に、それぞれの処理内容、および値を変更した場合にネットワークにどのような影響があるかを理解しておく必要があります。

- **EAP-Identity-Request Timeout**：このタイマーは、EAP アイデンティティ要求間の待ち時間に作用します。デフォルトは、4.1 以前の場合 1 秒、4.2 以降の場合 30 秒です。 この変更を行う理由は、一部のクライアント、ハンド ヘルド、電話、スキャナなどに、十分な速さで応答できないものがあるためです。ラップトップなどのデバイスでは、通常これらの値の操作は不要です。使用できる値は 1 ~ 120 です。ここで、この属性に 30 という値を設定した場合は、次のようなことが起こります。クライアントは最初の接続時に EAPOL Start をネットワークに送信し、WLC は EAP パケットを送信して、ユーザまたはマシンの ID を要求します。WLC は、ID 応答を受信しなかった場合、最初の要求から 30 秒後にもう一度 ID 要求を送信します。最初の接続時、およびクライアントのローミング時には、このようなやり取りがあります。このタイマーを長く設定した場合は、次のようなことが起こります。すべてが適当に設定されていれば、何も影響しません。ただし、クライアント、AP、RF などの問題を

含め、ネットワーク内に問題がある場合は、ネットワーク接続の遅延の原因になる可能性があります。たとえば、タイマーを最大値である 120 秒に設定した場合、WLC の ID 要求間の待ち時間は 2 秒です。クライアントがローミング中で、その応答を WLC が受信しない場合、このクライアントに対して最低でも 2 分間の停止が生じます。このタイマーの推奨値は*5*です。現時点では、このタイマーを最大値に設定する理由はありません。

- **EAP-Identity-Request Max Retries**：最大試行回数の値は、MSCB からエントリが削除されるまでに、WLC が ID 要求をクライアントに送信する回数です。最大試行回数に達すると、WLC は認証解除フレームをクライアントに送信し、クライアントに EAP プロセスを再起動させます。使用可能な値は1 ~ 20です。次に、この値について詳しく説明します。最大試行回数は、ID タイムアウトと連動します。ID タイムアウトを 120 に、最大試行回数を 20 に設定した場合、かかる時間は 2400（つまり、120 X 20）になります。 これは、クライアントが削除され、EAP プロセスを再起動させるのに 40 分かかることになります。ID タイムアウトを 5 に設定し、最大試行回数の値が 12 の場合は、60（つまり、5 X 12）になります。 前の例とは対照的に、クライアントが削除され EAP の再起動が必要になるまで 1 分です。最大試行回数の推奨値は *12* です。
- **EAPOL-Key Timeout**：EAPOL-Key Timeout の値は、デフォルトで 1 秒または 1000 ミリ秒です。これは、AP とクライアント間での EAPOL キーの交換時に、AP がキーを送信し、クライアントの応答をデフォルトで最大 1 秒待機することを意味します。定義された時間待機した後、AP はキーを再送信します。**config advanced eap eapol-key-timeout <time> コマンドを使用して、この設定を変更できます。**6.0 で使用できる値は 200 ~ 5000 ミリ秒で、6.0 よりも前のコードで使用できる値は 1 ~ 5 秒です。キーの試行に応答していないクライアントがある場合は、タイマーを長くすることで、クライアントにもう少しだけ時間が許され応答できる可能性があることに留意してください。ただし、802.1x プロセス全体を新しく開始するため、WLC および AP によるクライアントの認証解除に時間がかかる場合もあります。
- **EAPOL-Key Max Retries**：EAPOL-Key Max Retriesの値の場合、デフォルトは2です。これは、クライアントに対して元のキーの試行を2回再試行することを意味します。この設定は、**config advanced eap eapol-key-retries <retries> コマンドを使用して変更できます。**使用できる値は 0 ~ 4 の試行回数です。EAPOL-Key Timeout のデフォルト値（1 秒）および EAPOL-Key Retry のデフォルト値（2 回）を使用して、クライアントが最初のキー試行に応答しない場合、次のようにプロセスが進みます。AP はクライアントにキー試行を送信します。AP は応答を 1 秒待機します。応答がない場合、最初の EAPOL-Key Retry が送信されます。AP は応答を 1 秒待機します。応答がない場合、2 回目の EAPOL-Key Retry が送信されます。それでもクライアントからの応答がなく、再試行回数の値に達した場合、クライアントは認証解除されます。一方で、EAPOL-Key Timeout と同様に、EAPOL-Key Retry 値を増やすと、状況によっては便利になることがあります。ただし、この場合も最大値に設定すると、認証解除のメッセージが先延ばしされるため、弊害が生じることがあります。

## トラブルシューティングのための ACS RADIUS サーバからのパッケージ ファイルの抽出

ACS を外部 RADIUS サーバとして使用する場合は、このセクションの説明を使用して設定のトラブルシューティングを行うことができます。package.cab は、ACS を効率よくトラブルシューティングするために必要なすべてのファイルを含む ZIP ファイルです。CSSupport.exe ユーティリティを使用して package.cab を作成したり、手動でファイルを収集したりできます。

パッケージ ファイルの作成方法および WCS からの抽出方法については、『Cisco Secure ACS for Windows のバージョン情報および AAA デバッグ情報の取得』の「package.cab ファイルの作成」セクションを参照してください。

## 関連情報

- Lightweight アクセス ポイントの WLAN コントローラ フェールオーバーの設定例
- ワイヤレス LAN コントローラ ( WLC ) ソフトウェアのアップグレード
- Cisco ワイヤレス LAN コントローラ コマンド リファレンス
- テクニカル サポートとドキュメント – Cisco Systems