

RADIUSサーバを使用する外部 Web 認証

目次

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[ネットワーク図](#)

[表記法](#)

[外部 Web 認証](#)

[WLC の設定](#)

[Cisco Secure ACS のための WLC を設定して下さい](#)

[Web 認証のための WLC の WLAN を設定して下さい](#)

[WLC の Webサーバ 情報を設定して下さい](#)

[Cisco Secure ACS の設定](#)

[ユーザ情報 Secure ACS を on Cisco 設定して下さい](#)

[WLC 情報 Secure ACS を on Cisco 設定して下さい](#)

[クライアント認証 プロセス](#)

[クライアントの設定](#)

[クライアントログイン プロセス](#)

[確認](#)

[ACS の確認](#)

[WLC を確認して下さい](#)

[トラブルシューティング](#)

[トラブルシューティングのためのコマンド](#)

[関連情報](#)

[はじめに](#)

この資料に外部 RADIUSサーバを使用して外部 Web 認証を行う方法を説明されています。

[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 アクセス ポイント (LAP) および Cisco WLC の設定に関する基礎知識
- 外部 Webサーバをセットアップおよび設定する方法のナレッジ
- Cisco Secure ACS の設定方法に関する知識

使用するコンポーネント

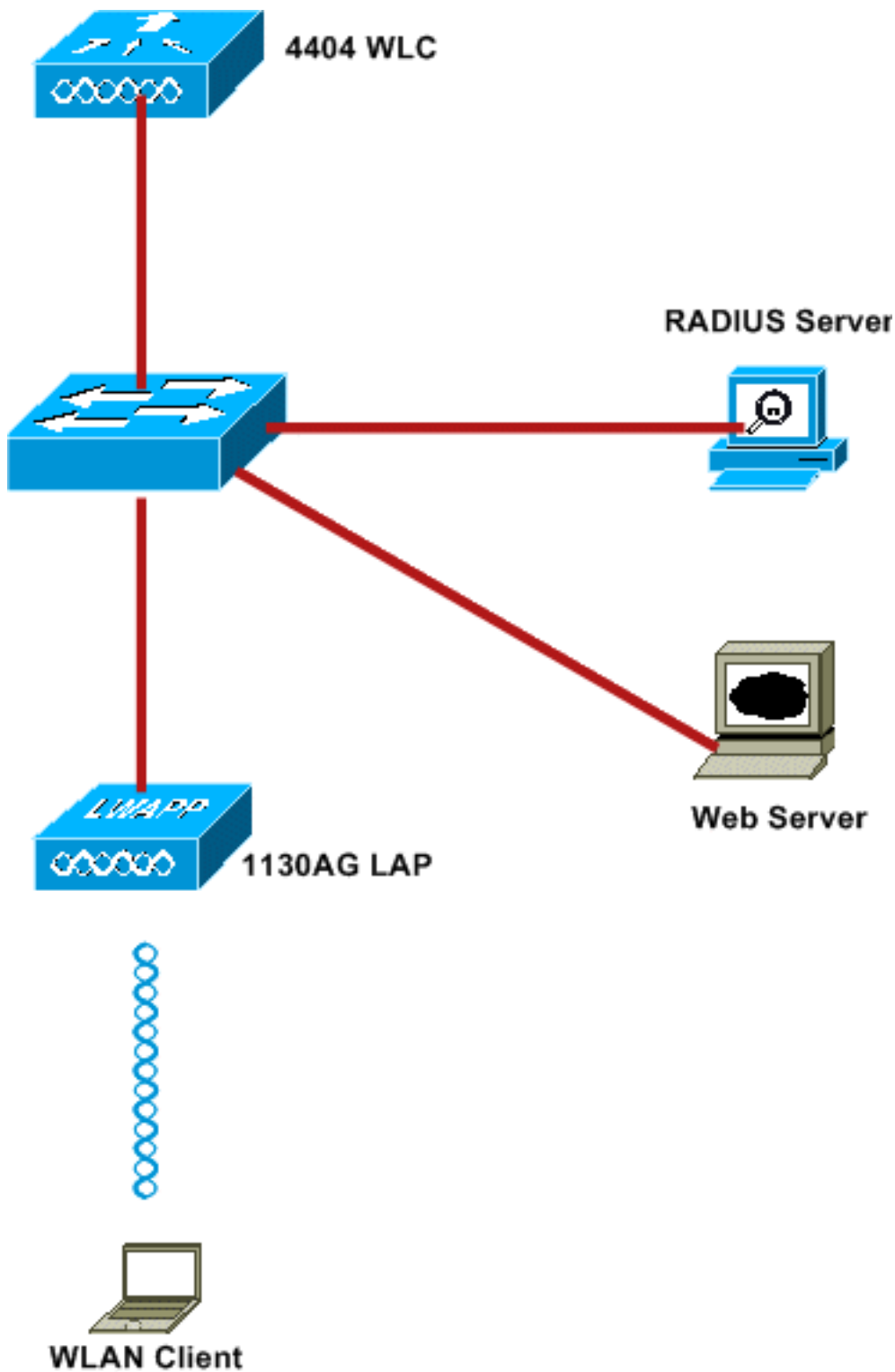
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- ファームウェア バージョン 5.0.148.0 を実行するワイヤレス LAN コントローラ
- Cisco 1232 シリーズ LAP
- Cisco 802.11a/b/g ワイヤレスクライアントアダプタ 3.6.0.61
- Web 認証ログイン ページをホストする外部 Web サーバ
- ファームウェア バージョン 4.1.1.24 を実行する Cisco Secure ACS バージョン

本書の情報は、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、初期（デフォルト）設定の状態から起動しています。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

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。



このドキュメントで使用する IP アドレスは次のとおりです。

- WLC は IP アドレス 10.77.244.206 を使用します
- LAP は IP アドレス 10.77.244.199 の WLC に登録されています
- Webサーバは IP アドレス 10.77.244.210 を使用します
- Cisco ACS サーバは IP アドレス 10.77.244.196 を使用します
- クライアントは WLAN に- 10.77.244.208 マップされる管理インターフェイスから IP アドレスを受け取ります

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。

[外部 Web 認証](#)

Web 認証はインターネット アクセスのためのゲスト ユーザを認証するのに使用されるレイヤ3 認証機構です。このプロセスを使用して認証されたユーザは彼らまでのインターネットにアクセス正常に完了しません認証プロセスをできません。外部 Web 認証プロセスの完全情報に関しては、[ワイヤレス LAN コントローラ 設定例の資料](#)[外部 Web 認証](#)のセクション[外部 Web 認証プロセス](#)を読んで下さい。

この資料では、外部 Web 認証が外部 RADIUSサーバを使用して実行された 設定例を検知します。

[WLC の設定](#)

この資料では、WLC は既に設定され、WLC に登録されている LAP がっていると仮定します。それ以上のこの資料は WLC が基本動作のために設定されると、そしてラップが WLC に登録されていると仮定します。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。WLC に登録されているラップを、移動ワイヤレスに表示するため > **すべての AP**。

WLC は基本動作のために設定され、それに登録されている 1つ以上のラップがあれば外部 Webサーバを使用して外部 Web 認証のための WLC を設定できます。例では、RADIUSサーバとして Cisco Secure ACS バージョン 4.1.1.24 を使用しています。最初に、この RADIUSサーバのための WLC を設定し、それからこの設定用の Cisco Secure ACS で必要な設定を検知します。

[Cisco Secure ACS のための WLC を設定して下さい](#)

WLC に RADIUSサーバを追加するためにこれらのステップを実行して下さい:

1. WLC GUI から、**Security** メニューをクリックして下さい。
2. **AAA** メニューの下で、に **Radius > 認証**サブメニュー ナビゲートして下さい。
3. 『New』 をクリックし、RADIUSサーバの IP アドレスを入力して下さい。この例では、サーバの IP アドレスは `10.77.244.196` です。
4. WLC で共用シークレットを入力して下さい。共用シークレットは WLC で同じ設定する必要があります。
5. 共用秘密形式のための **ASCII** か **Hex** を選択して下さい。同じは WLC で選択される必要をフォーマットします。
6. RADIUS認証に使用するポート番号は **1812** あります。
7. サーバステータス オプションが**イネーブル**になったに設定されるようにして下さい。
8. ネットワーク ユーザを認証するためにネットワーク ユーザ **Enable** チェックボックスをチェックして下さい。
9. [Apply] をクリックします。

The screenshot shows the Cisco WLC configuration interface for a new RADIUS Authentication Server. The left sidebar is under 'Security' with 'AAA' expanded to 'RADIUS'. The main area is titled 'RADIUS Authentication Servers > New' and contains the following fields:

- Server Index (Priority): 2
- Server IP Address: 10.77.244.196
- Shared Secret Format: ASCII
- Shared Secret: [Redacted]
- Confirm Shared Secret: [Redacted]
- Key Wrap: (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
- Port Number: 1812
- Server Status: Enabled
- Support for RFC 3576: Enabled
- Server Timeout: 2 seconds
- Network User: Enable
- Management: Enable
- IPSec: Enable

Web 認証のための WLC の WLAN を設定して下さい

次のステップは WLC の Web 認証のための WLAN を設定することです。WLC の WLAN を設定するためにこれらのステップを実行して下さい:

1. コントローラ GUI からの **WLAN メニュー** をクリックし、『New』を選択して下さい。
2. 型のために『WLAN』を選択して下さい。
3. 選択のプロファイル名および WLAN SSID を入力し、『Apply』をクリックして下さい。注: WLAN SSID は大文字/小文字の区別があります。

The screenshot shows the Cisco WLC configuration interface for a new WLAN. The left sidebar is under 'WLANs' with 'WLANs' expanded. The main area is titled 'WLANs > New' and contains the following fields:

- Type: WLAN
- Profile Name: WLAN1
- WLAN SSID: WLAN1

4. **General** タブの下で、イネーブルになったオプションがステータスおよびブロードキャスト

両方 SSID があるように確認されることを確かめて下さい。WLAN 設定

The screenshot shows the Cisco WLAN configuration interface. The top navigation bar includes MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, and HELP. The left sidebar shows the navigation tree with WLANs > Advanced selected. The main content area is titled 'WLANs > Edit' and has tabs for General, Security, QoS, and Advanced. The General tab is active, showing the following configuration:

Profile Name	WLAN1
Type	WLAN
SSID	WLAN1
Status	<input checked="" type="checkbox"/> Enabled
Security Policies	[WPA2][Auth(002.1X)] (Modifications done under security tab will appear after applying the changes.)
Radio Policy	All
Interface	management
Broadcast SSID	<input checked="" type="checkbox"/> Enabled

Foot Notes:

- 1 CKIP is not supported by 10xx model APs
- 2 Web Policy cannot be used in combination with IPsec
- 3 H-REAP Local Switching is not supported with IPsec, CRANITE authentication
- 4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
- 5 Client MFP is not active unless WPA2 is configured

5. WLAN のためのインターフェイスを選択して下さい。通常、ユニークな VLAN で設定されるインターフェイスは WLAN にクライアントがその VLAN の IP アドレスを受け取るようにマップされます。この例では、インターフェイスのために管理を使用します。
6. [Security] タブを選択します。
7. レイヤ2 メニューの下で、レイヤ2 セキュリティ用に『None』を選択して下さい。
8. レイヤ3 メニューの下で、レイヤ3 セキュリティ用に『None』を選択して下さい。Web ポリシー チェックボックスをチェックし、**認証**を選択して下さい。

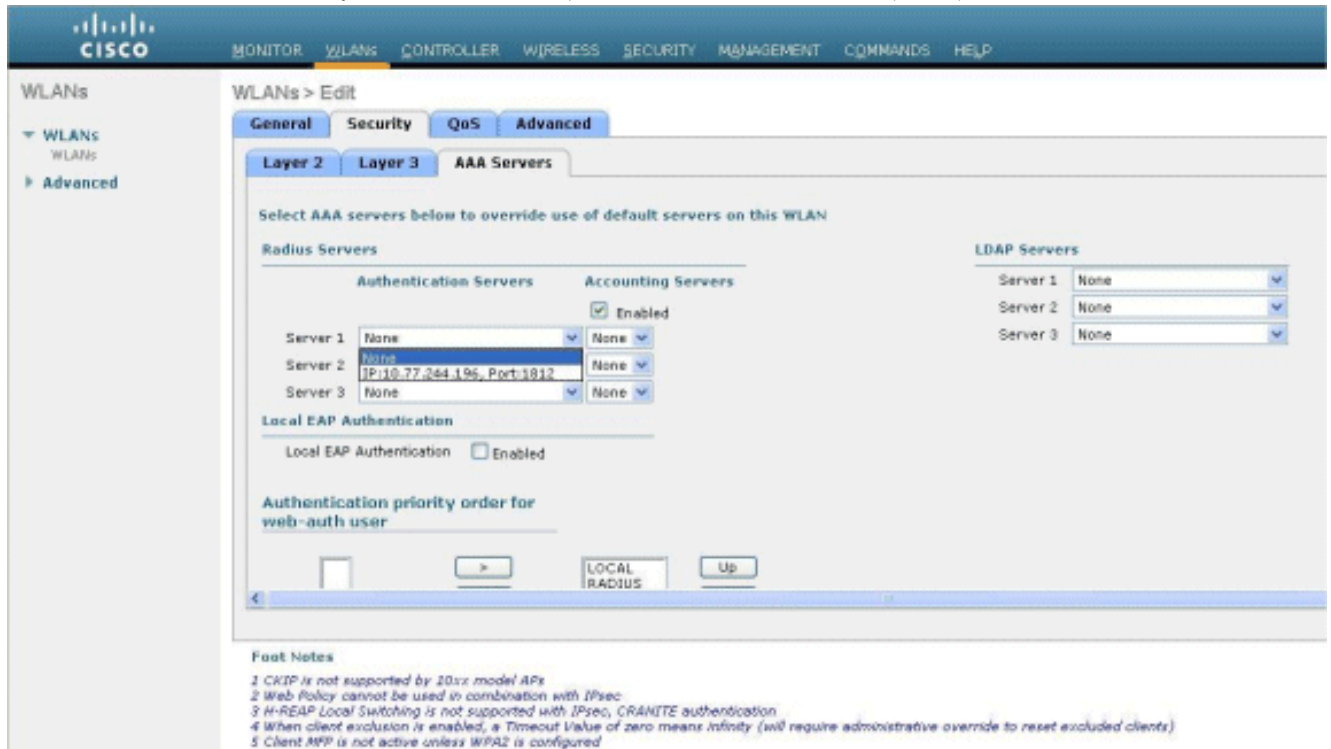
The screenshot shows the Cisco WLAN configuration interface, specifically the Security tab. The top navigation bar and left sidebar are the same as in the previous screenshot. The main content area is titled 'WLANs > Edit' and has tabs for General, Security, QoS, and Advanced. The Security tab is active, and the 'Layer 3' sub-tab is selected. The configuration is as follows:

Layer 3 Security	None
<input checked="" type="checkbox"/> Web Policy ²	
<input checked="" type="radio"/> Authentication	
<input type="radio"/> Passthrough	
<input type="radio"/> Conditional Web Redirect	
<input type="radio"/> Splash Page Web Redirect	
Preauthentication ACL	None
Over-ride Global Config	<input type="checkbox"/> Enable

Foot Notes:

- 1 CKIP is not supported by 10xx model APs
- 2 Web Policy cannot be used in combination with IPsec
- 3 H-REAP Local Switching is not supported with IPsec, CRANITE authentication
- 4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
- 5 Client MFP is not active unless WPA2 is configured

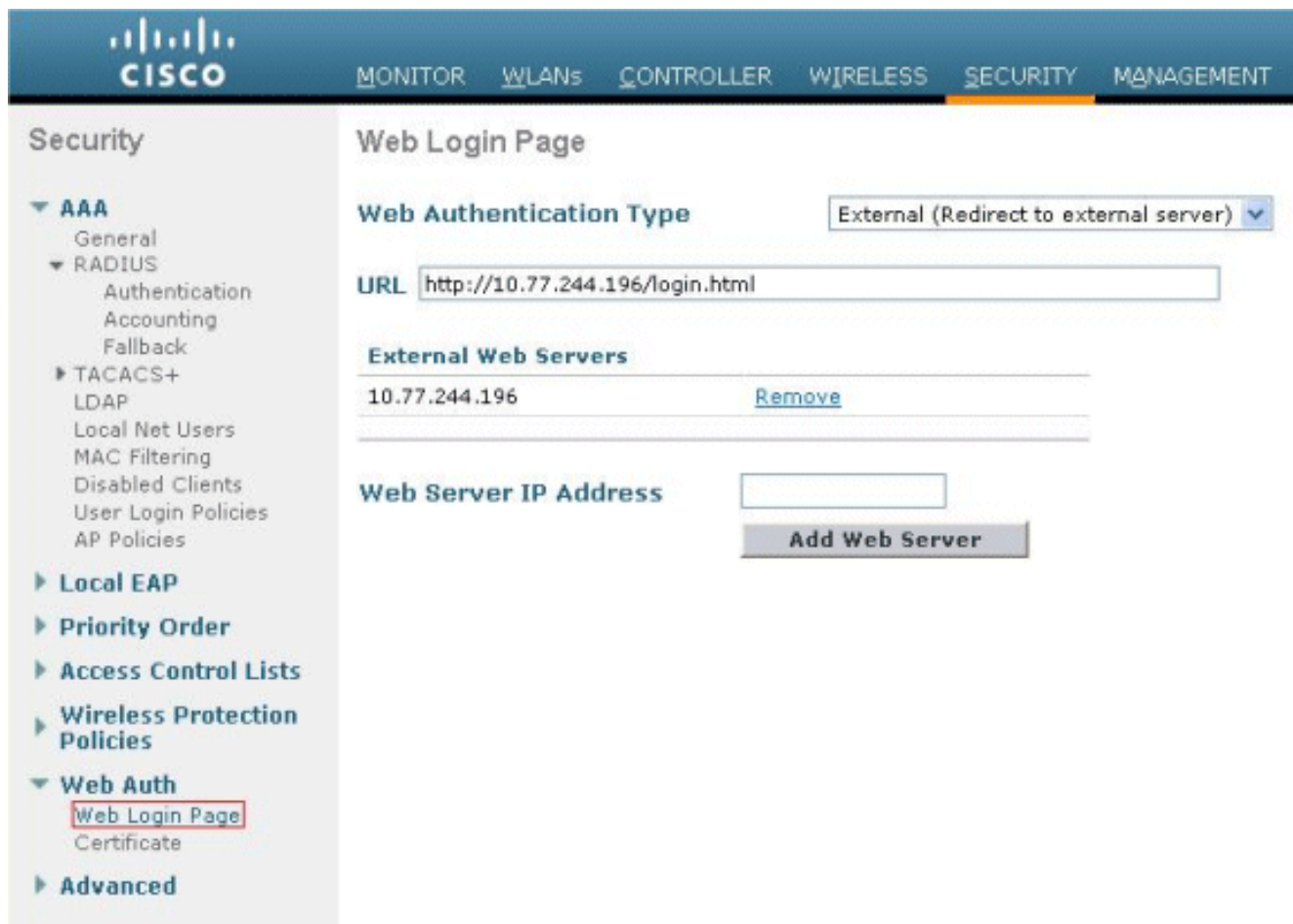
9. AAA サーバメニューの下で、認証サーバのために、この WLC で設定された RADIUSサーバを選択して下さい。他のメニューはデフォルト値に残るはずです。



WLC の Webサーバ 情報を設定して下さい

Web 認証ページをホストする Webサーバは WLC で設定する必要があります。Webサーバを設定するためにこれらのステップを実行して下さい:

1. [Security] タブをクリックします。 **Login ページ Web Auth > Web** に行ってください。
2. **外部**として Web 認証種別を設定して下さい。
3. Web 認証ページをホストする入力し、**Webサーバ**を『Add』 をクリックして下さい Webサーバ IP address フィールドでは、サーバの IP アドレスを。外部 Webサーバの下で現われるこの例では、IP アドレスは **10.77.244.196**です。
4. Web 認証ページのための URL を入力して下さい (この例で、URL フィールドの **http://10.77.244.196/login.html**)。



Cisco Secure ACS の設定

この資料で仮定しま Cisco Secure ACS サーバがであると既にインストールされ、マシンで動作します。詳細については Cisco Secure ACS を設定する方法を [Cisco Secure ACS 4.2 のためのコンフィギュレーションガイド](#)を参照して下さい。

ユーザ情報 Secure ACS を on Cisco 設定して下さい

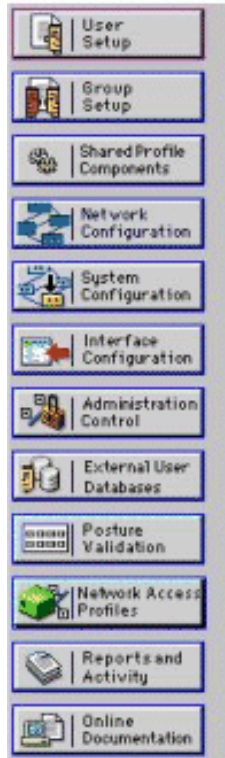
Cisco Secure ACS のユーザを設定するためにこれらのステップを実行して下さい:

1. Cisco Secure ACS GUI から『User Setup』を選択し、ユーザー名を入力し、『Add/Edit』をクリックして下さい。この例では、ユーザは *user1* です。



User Setup

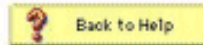
Select



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			



2. デフォルトで、PAP は認証クライアントのために使用されます。ユーザ向けのパスワードはユーザセットアップ > パスワード認証 > Cisco Secure PAP の下で入力されます。パスワード認証のための ACS 内部 データベースを選択するために確かめて下さい。

Edit

User: user1 (New User)

Account Disabled

Supplementary User Info ?

Real Name

Description

User Setup ?

Password Authentication: ACS Internal Database

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password

Confirm Password

Separate (CHAP/MS-CHAP/ARAP)

Password

Confirm Password

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.

Group to which the user is assigned:

3. ユーザが属するグループは割り当てられることをユーザーのニーズ。デフォルトグループを選択して下さい。
4. [Submit] をクリックします。

WLC 情報 Secure ACS を on Cisco 設定して下さい

WLC 情報 Secure ACS を on Cisco 設定するためにこれらのステップを実行して下さい:

1. ACS GUI では、**Network Configuration** タブをクリックし、『Add Entry』 をクリックして下さい。
2. 追加 AAA Client 画面は現われます。
3. クライアントの名前を入力して下さい。この例では、WLC を使用します。
4. クライアントの IP アドレスを入力して下さい。WLC の IP アドレスは 10.77.244.206 です。
5. 共有秘密鍵およびキー形式を入力して下さい。これは WLC の **Security** メニューで作成されるエントリを一致する必要があります。
6. WLC に同じであるはずであるキー入力形式のための **ASCII** を選択して下さい。
7. WLC と RADIUSサーバの間で使用されるプロトコルを設定するために認証するために

(Cisco Airespace) を使用して『RADIUS』を選択して下さい。

8. [Submit+Apply] をクリックします。

The screenshot shows the 'Add AAA Client' configuration page in the Cisco Network Configuration utility. The form includes the following fields and options:

- AAA Client Hostname: WLC
- AAA Client IP Address: 10.77.244.206
- Shared Secret: abc123
- RADIUS Key Wrap**
 - Key Encryption Key: [Empty field]
 - Message Authenticator Code Key: [Empty field]
 - Key Input Format: ASCII Hexadecimal
- Authenticate Using: RADIUS (Cisco Airespace)
- 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:
- Match Framed-IP-Address with user IP address for accounting packets from this AAA Client:

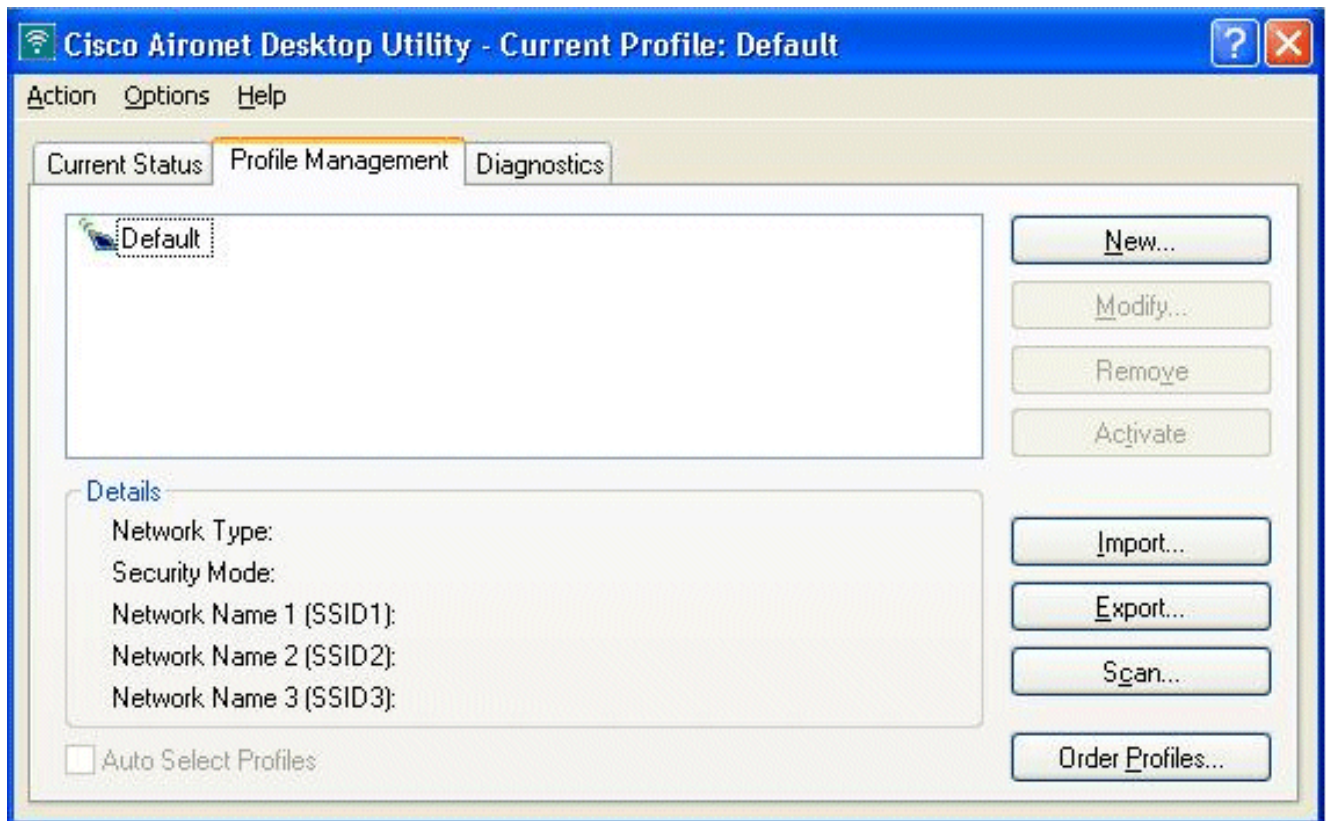
Buttons at the bottom: Submit, Submit + Apply, Cancel, and a Back to Help button.

クライアント認証プロセス

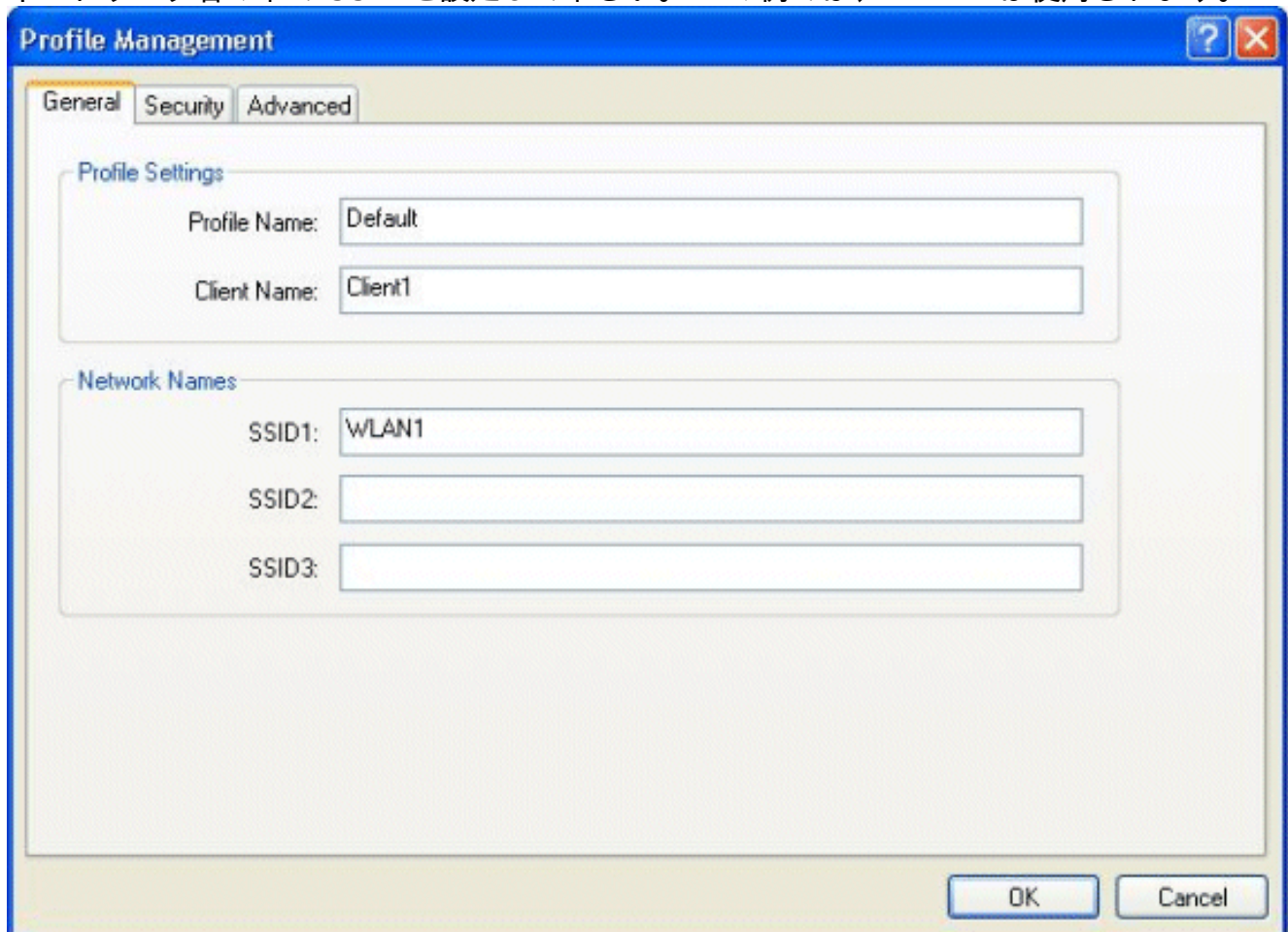
クライアントの設定

この例では、Web 認証を行うのに Cisco Aironet デスクトップ ユーティリティを使用します。Aironet デスクトップ ユーティリティを設定するためにこれらのステップを実行して下さい。

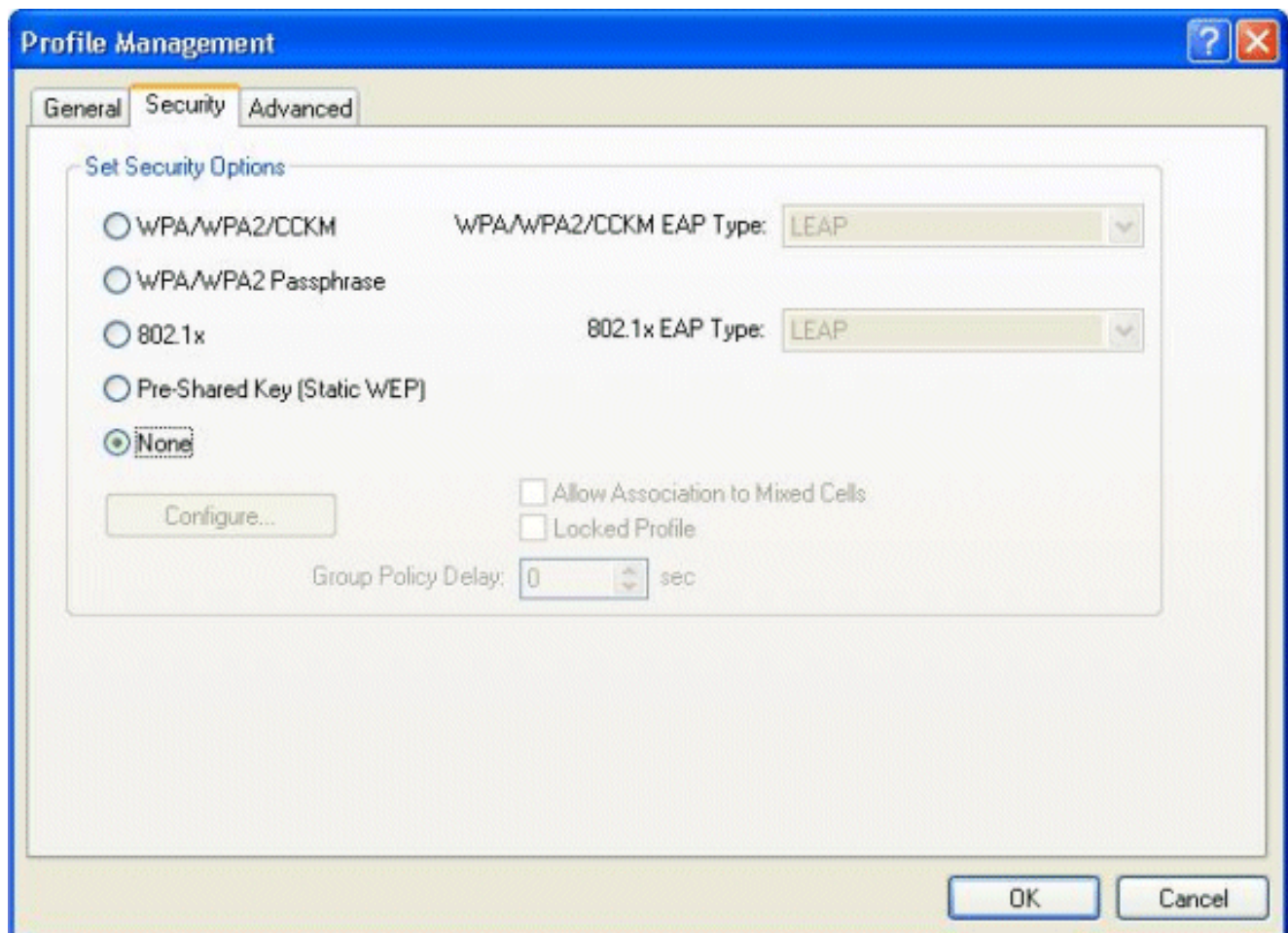
1. Start > Cisco Aironet > Aironet デスクトップ ユーティリティからの Aironet デスクトップ ユーティリティを開いて下さい。
2. プロファイル 管理タブをクリックして下さい。



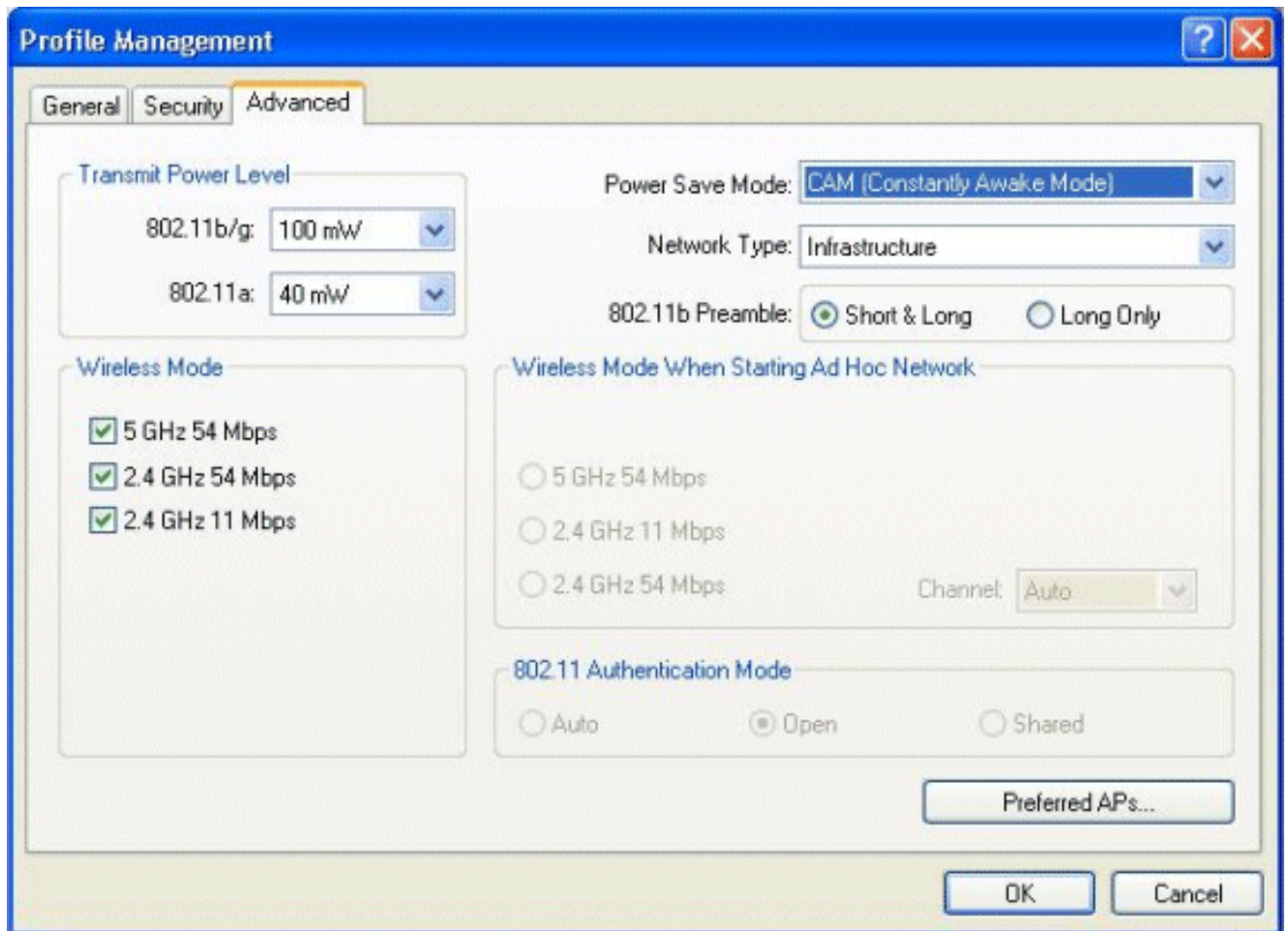
3. 既定値のプロファイルを選択し、『Modify』をクリックして下さい。[General] タブをクリックしますプロファイル名を設定して下さい。この例では、デフォルトは使用されます。ネットワーク名の下で SSID を設定して下さい。この例では、WLAN1 は使用されます。



注: SSID は大文字/小文字の区別があり、WLC で設定される WLAN を一致する必要があります。[Security] タブをクリックします。Web 認証のためのセキュリティとして『None』を選択して下さい。



[Advanced] タブをクリックします。ワイヤレス Mode メニューの下で、無線クライアントが LAP と通信する周波数を選択して下さい。送信電力電力レベルの下で、WLC で設定される電源を選択して下さい。省電力モードのデフォルト値を残して下さい。ネットワークの種類としてインフラストラクチャを選択して下さい。よりよい互換性のための長くとして 802.11b プリアンブルを及び長く設定して下さい。[OK] をクリックします。

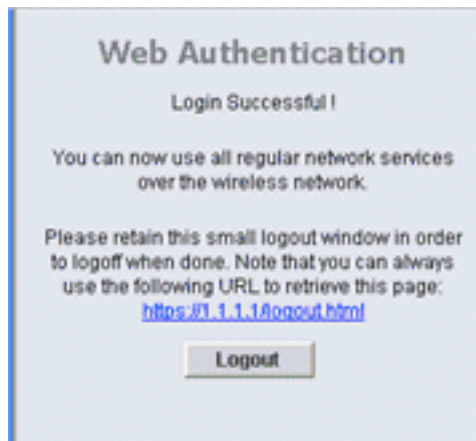


4. プロファイルがクライアントソフトウェアで設定されれば、クライアントは正常に関連付けられ、管理インターフェイスのために設定される VLAN プールから IP アドレスを受け取ります。

クライアントログインプロセス

このセクションはクライアントログインがどのように発生するか説明します。

1. ブラウザ ウィンドウを開いて、URL または IP アドレスを入力します。これによって、クライアントに Web 認証ページが表示されます。コントローラが以前のリリースを 3.0 実行する場合、ユーザは始動に Web 認証ページ <https://1.1.1.1/login.html> を入力する必要があります。セキュリティ アラート ウィンドウが表示されます。
2. 先に進むには、[Yes] をクリックします。
3. Login ウィンドウが現われるとき、RADIUSサーバで設定されるユーザ名 および パスワードを入力して下さい。ログオンが正常である場合、2つのブラウザウィンドウが表示されます。より大きいウィンドウは正常なログインを示し、インターネットを参照このウィンドウできます。ゲスト ネットワークの使用が終了してログアウトするには、小さい方のウイン



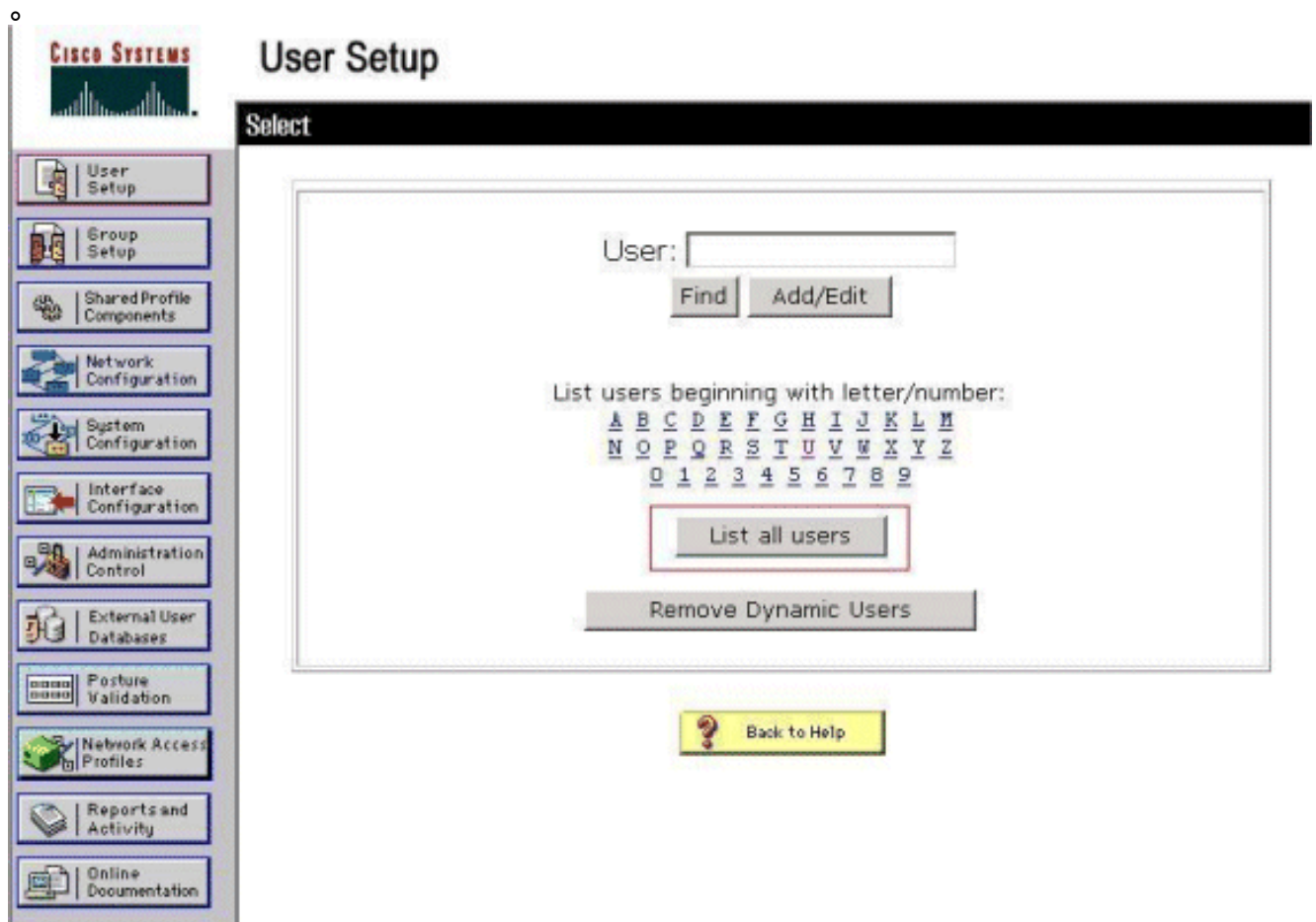
ドウを使用します。

確認

正常な Web 認証に関しては、デバイスが適切な方法で設定されるかどうか確認する必要があります。このセクションはプロセスで使用されるデバイスを確認する方法を説明します。

ACS の確認

1. 『User Setup』 をクリックし、次に ACS GUI で 『List All Users』 をクリックして下さい



ユーザのステータスが有効になることデフォルトグループがユーザにマップされることを確かめれば。

User List

User	Status	Group	Network Access Profile
user1	Enabled	Default Group (2 users)	(Default)

2. WLC が AAA クライアントで設定されることを確認するために AAA クライアント表の Network Configuration タブおよび一見をクリックして下さい。

The screenshot shows the 'Network Configuration' page in the Cisco WLC GUI. The left sidebar contains navigation options: User Setup, Group Setup, Shared Profile Components, Network Configuration (selected), System Configuration, Interface Configurations, Administration Control, External User Databases, Posture Validation, Network Access Profiles, Reports and Activity, and Online Documentation. The main content area is titled 'Select' and contains three tables:

- AAA Clients:** A table with columns 'AAA Client Hostname', 'AAA Client IP Address', and 'Authenticate Using'. It contains one entry: 'wlc1' with IP '10.77.244.206' and 'RADIUS (Cisco Airespace)'. Buttons for 'Add Entry' and 'Search' are below.
- AAA Servers:** A table with columns 'AAA Server Name', 'AAA Server IP Address', and 'AAA Server Type'. It contains one entry: 'TS-Web' with IP '10.77.244.196' and 'CiscoSecure ACS'. Buttons for 'Add Entry' and 'Search' are below.
- Proxy Distribution Table:** A table with columns 'Character String', 'AAA Servers', 'Strip', and 'Account'. It contains one entry: '(Default)' with 'TS-Web', 'No', and 'Local'. Buttons for 'Add Entry' and 'Sort Entries' are below.

A 'Back to Help' button is located at the bottom of the main content area.

WLC を確認して下さい

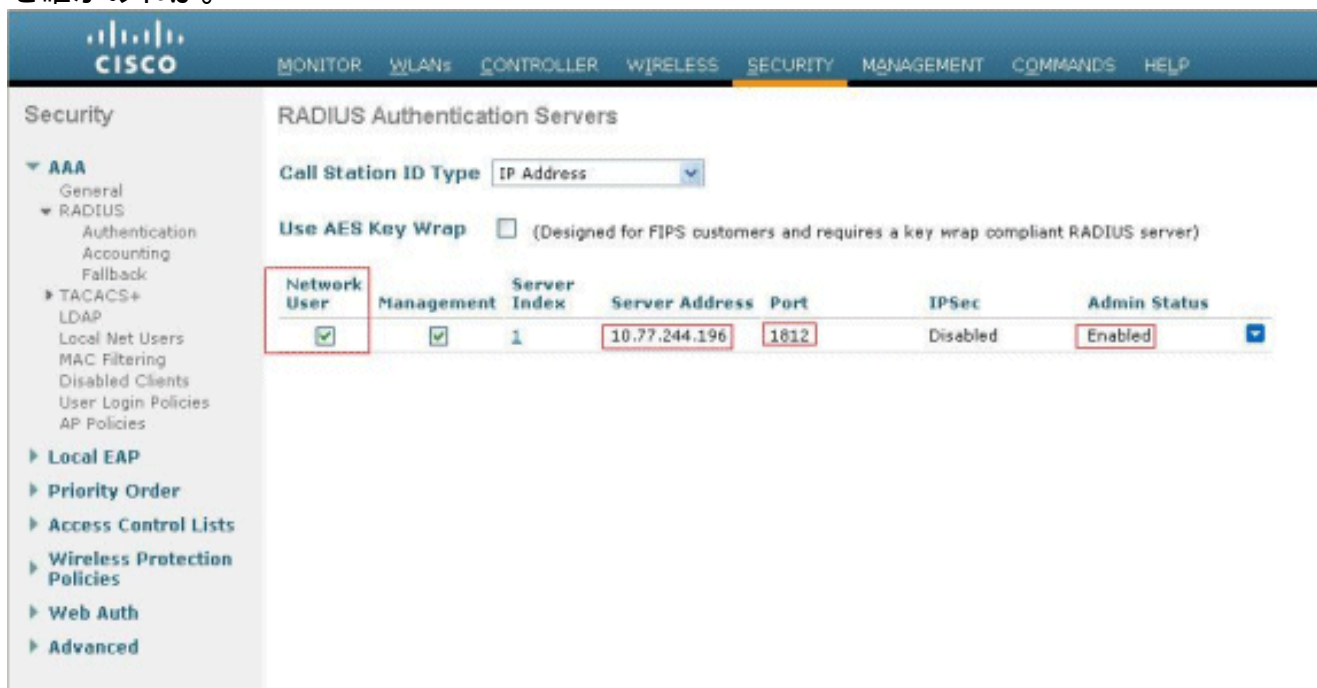
1. WLC GUI からの WLAN メニューをクリックして下さい。Web 認証に使用する WLAN がページにリストされていることを確かめて下さい。WLAN のための管理状態が有効になることを確かめて下さい。WLAN のためのセキュリティポリシーが WebAuth を示すことを確かめて下さい。

The screenshot shows the 'WLANs' configuration page in the Cisco WLC GUI. The top navigation bar includes: MONITOR, WLANs (selected), CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, and HELP. The left sidebar shows: WLANs, > WLANs, WLANs, and > Advanced. The main content area is titled 'WLANs' and contains a table:

Profile Name	Type	WLAN SSID	Admin Status	Security Policies
WLAN1	WLAN	WLAN1	Enabled	Web-Auth

2. WLC GUI からの Security メニューをクリックして下さい。Cisco Secure ACS を確かめて下さい (10.77.244.196) ページにリストされています。ネットワーク ユーザー ボックスが

チェックされることを確かめて下さい。ポートが 1812 あること管理状態が有効になることを確かめれば。



トラブルシューティング

Web 認証が正常なわけではないか多くの原因があります。 [ワイヤレス LAN コントローラ \(WLC\) の Web 認証を解決する](#) 資料は明確にそれらの原因を詳しく説明したものです。

トラブルシューティングのためのコマンド

注: これらの 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](#)して下さい。

WLC に Telnet で接続し、認証を解決するこれらのコマンドを発行して下さい:

- **debug aaa all enable**

```
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Successful transmission of Authentic
ation Packet (id 1) to 10.77.244.196:1812, proxy state 00:40:96:ac:dd:05-00:01
Fri Sep 24 13:59:52 2010: 00000000: 01 01 00 73 00 00 00 00 00 00 00 00 00 00 0
0 00 ...s.....
Fri Sep 24 13:59:52 2010: 00000010: 00 00 00 00 01 07 75 73 65 72 31 02 12 93 c
3 66 .....user1....f
Fri Sep 24 13:59:52 2010: 00000030: 75 73 65 72 31
user1
Fri Sep 24 13:59:52 2010: ****Enter processIncomingMessages: response code=2
Fri Sep 24 13:59:52 2010: ****Enter processRadiusResponse: response code=2
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Access-Accept received from RADIUS s
erver 10.77.244.196 for mobile 00:40:96:ac:dd:05 receiveId = 0
Fri Sep 24 13:59:52 2010: AuthorizationResponse: 0x12238db0
Fri Sep 24 13:59:52 2010: structureSize.....89
Fri Sep 24 13:59:52 2010: resultCode.....0
Fri Sep 24 13:59:52 2010: protocolUsed.....0x0
0000001
Fri Sep 24 13:59:52 2010: proxyState.....00:
40:96:AC:DD:05-00:00
Fri Sep 24 13:59:52 2010: Packet contains 2 AVPs:
Fri Sep 24 13:59:52 2010: AVP[01] Framed-IP-Address.....
.....0xffffffff (-1) (4 bytes)
```

```

Fri Sep 24 13:59:52 2010: AVP[02] Class.....
.....CACs:0/5183/a4df4ce/user1 (25 bytes)
Fri Sep 24 13:59:52 2010: Authentication failed for user1, Service Type: 0
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Applying new AAA override for station
00:40:96:ac:dd:05
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Override values for station 00:40:96
:ac:dd:05
source: 48, valid bits: 0x1
qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1

dataAvgC: -1, rTavgC: -1, dataBurstC: -1, rTimeBurstC: -1
vlanIfName: '',
aclName:
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Unable to apply override policy for
station 00:40:96:ac:dd:05 - VapAllowRadiusOverride is FALSE
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Sending Accounting request (0) for s
tation 00:40:96:ac:dd:05
Fri Sep 24 13:59:52 2010: AccountingMessage Accounting Start: 0x1500501c
Fri Sep 24 13:59:52 2010: Packet contains 12 AVPs:
Fri Sep 24 13:59:52 2010: AVP[01] User-Name.....
.....user1 (5 bytes)
Fri Sep 24 13:59:52 2010: AVP[02] Nas-Port.....
.....0x00000002 (2) (4 bytes)
Fri Sep 24 13:59:52 2010: AVP[03] Nas-Ip-Address.....
.....0x0a4df4ce (172881102) (4 bytes)
Fri Sep 24 13:59:52 2010: AVP[04] Framed-IP-Address.....
.....0x0a4df4c7 (172881095) (4 bytes)

```

- debug aaa detail enable

レポートおよびアクティビティ > 失敗した試行の壊れる認証の試みは見つけられるにメニュー リストされています。

関連情報

- [ワイヤレス LAN コントローラの Web 認証の設定例](#)
- [ワイヤレス LAN コントローラ \(WLC\) 上の Web 認証のトラブルシューティング](#)
- [ワイヤレス LAN コントローラを使用した外部 Web 認証の設定例](#)
- [ワイヤレス LAN コントローラ \(WLC\) 上での LDAP を使用した Web 認証の設定例](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)