

RADIUS サーバを使用した外部 Web 認証

内容

[概要](#)

[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 WLC の設定](#)

[Web 認証用の WLC 上での WLAN の設定](#)

[WLC 上での Web サーバ情報の設定](#)

[Cisco Secure ACS の設定](#)

[Cisco Secure ACS 上でのユーザ情報の設定](#)

[Cisco Secure ACS 上での WLC 情報の設定](#)

[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 の確認](#)

[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](#)

概要

このドキュメントでは、外部 RADIUS サーバを使用した外部 Web 認証を実行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。

- 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 サーバのセットアップ方法および設定方法に関する知識

- 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

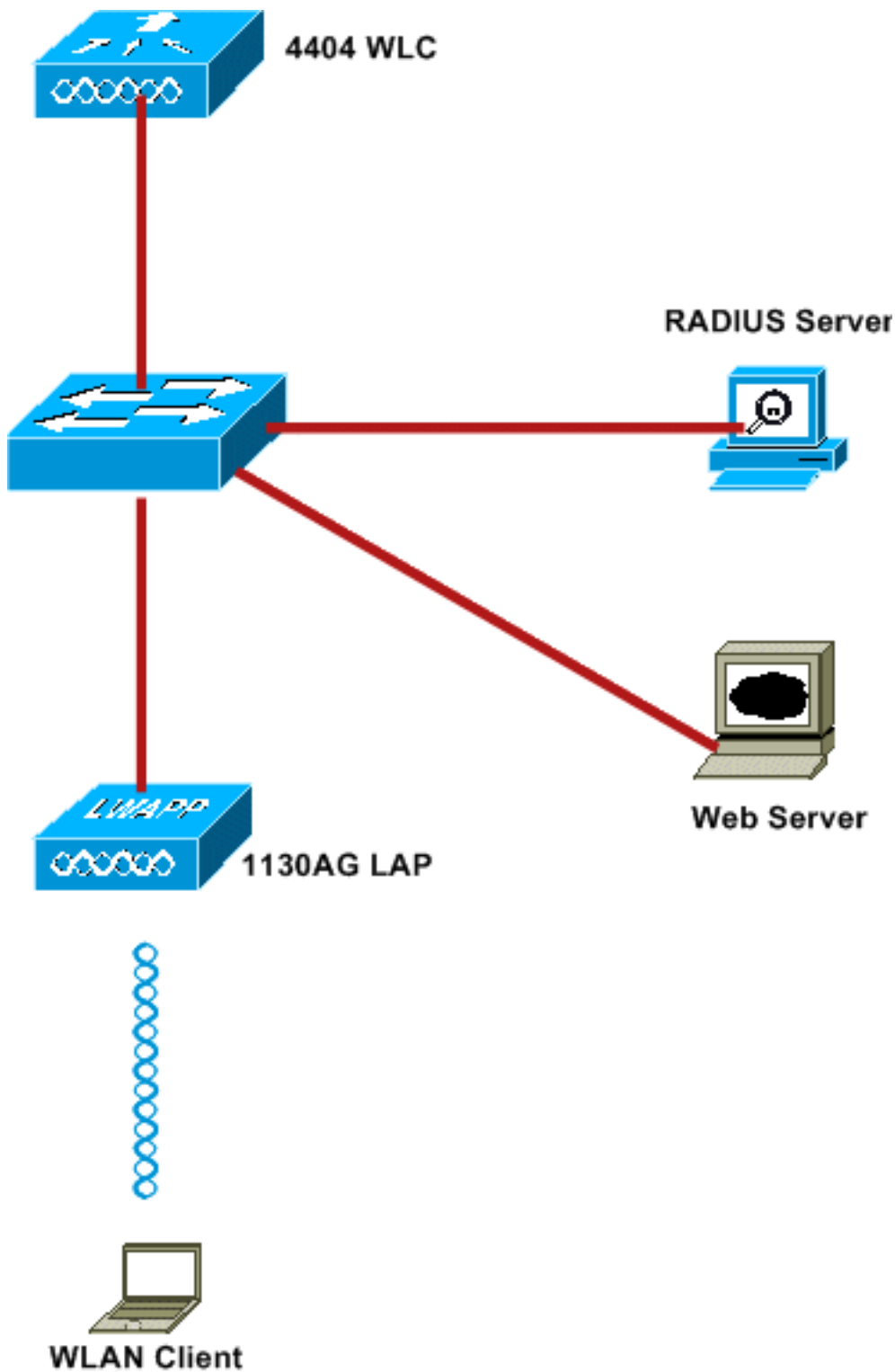
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ファームウェア バージョン 5.0.148.0 が稼働するワイヤレス 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 が稼働する Cisco Secure ACS のバージョン

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。

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 セットアップを使用します。



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 WLC に IP アドレス 10.77.244.199 で登録されています。
- 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 にマッピングされている IP アドレス 10.77.244.208 を管理インターフェイスから受信します。

表記法

ドキュメント表記の詳細については、『[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。

[外部 Web 認証](#)

Web 認証は、インターネット アクセスのゲスト ユーザ認証に使用される、レイヤ 3 認証メカニズムです。このプロセスを使用して認証されるユーザは、認証プロセスが正常に完了するまで、インターネットにアクセスできません。外部 Web 認証プロセスの詳細については、『[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](#)』ドキュメントの「[外部 Web 認証プロセス](#)」セクションを参照してください。

このドキュメントでは、外部 RADIUS サーバを使用して外部 Web 認証を実行する設定例を考察します。

[WLC の設定](#)

このドキュメントでは、WLC が設定済みであり、LAP が WLC に登録済みであると想定しています。さらにこのドキュメントでは、基本動作用に WLC 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。WLC に登録されている LAP を表示するには、[Wireless] > [All APs] に移動します。

WLC を基本動作用に設定し、1 つ以上の LAP が登録されたら、外部 Web サーバを使用する外部 Web 認証用に WLC を設定できます。この例では、Cisco Secure ACS バージョン 4.1.1.24 を RADIUS サーバとして使用しています。まず、この RADIUS サーバ用に WLC を設定し、次に、このセットアップ用の Cisco Secure ACS 上で必要な設定を確認します。

[Cisco Secure ACS の WLC の設定](#)

WLC 上に RADIUS サーバを追加するには、次の手順を実行します。

1. WLC GUI で、[SECURITY] メニューをクリックします。
2. [AAA] メニューの下で、[Radius] > [Authentication] サブメニューに移動します。
3. [New] をクリックし、RADIUS サーバの IP アドレスを入力します。この例では、サーバの IP アドレスは `10.77.244.196` です。
4. WLC での共有秘密を [Shared Secret] に入力します。共有秘密は、WLC 上と同じものを設定する必要があります。
5. [Shared Secret Format] で [ASCII] または [Hex] のいずれかを選択します。WLC 上と同じ形式を選択する必要があります。
6. `1812` は、RADIUS 認証に使用するポート番号です。
7. [Server Status] オプションが [Enabled] に設定されていることを確認します。
8. ネットワーク ユーザを認証するには、[Network User] の [Enable] ボックスをオンにします。
9. [Apply] をクリックします。

The screenshot shows the Cisco WLC GUI for configuring a new RADIUS Authentication Server. The left sidebar is under 'Security' > 'AAA' > '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 認証用の WLC 上での WLAN の設定

次の手順では、WLC 上で Web 認証用に WLAN を設定します。WLC 上で WLAN を設定するには、次の手順を実行します。

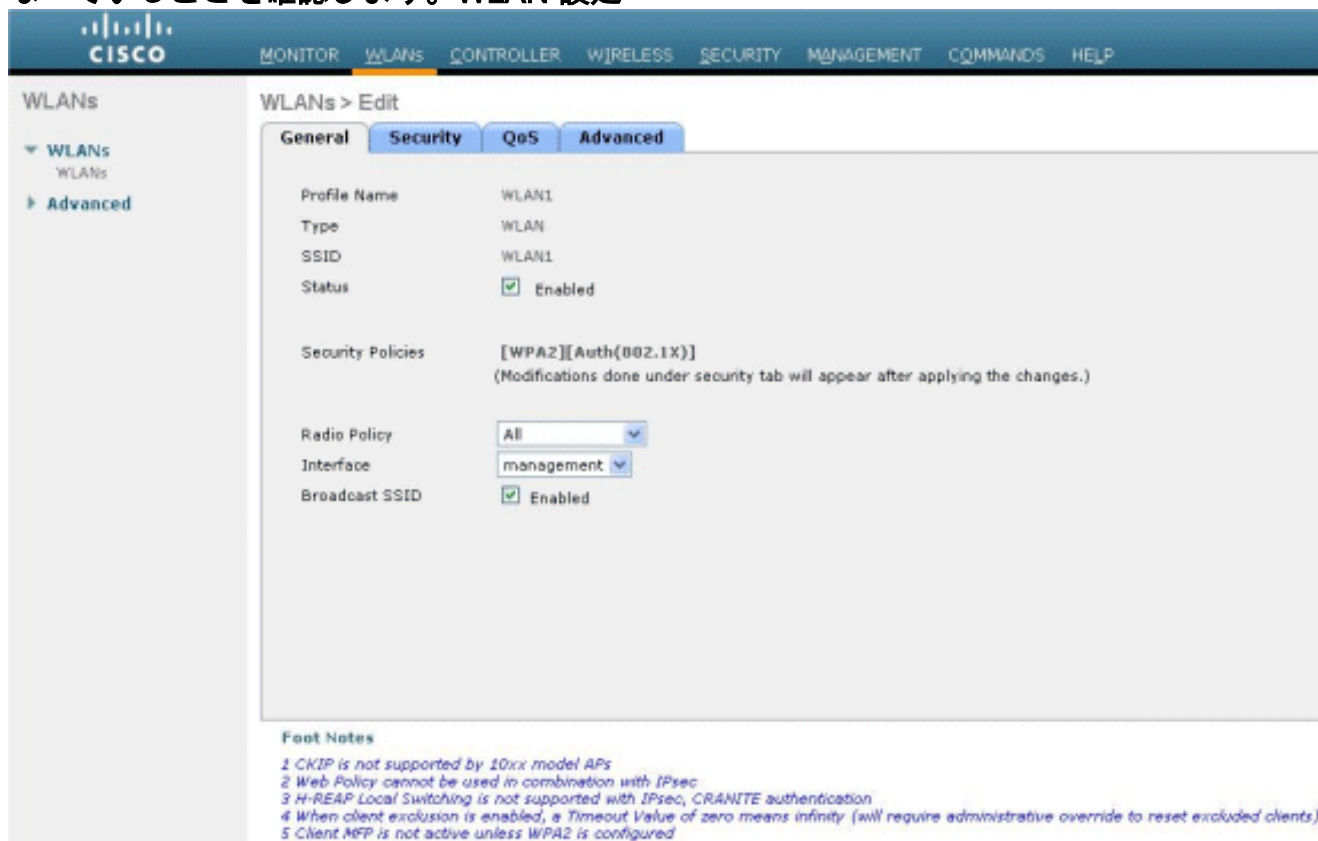
1. コントローラ GUI の [WLANs] メニューをクリックし、[New] を選択します。
2. [Type] で [WLAN] を選択します。
3. 任意のプロファイル名と WLAN SSID を入力し、[Apply] をクリックします。注：WLAN SSIDでは大文字と小文字が区別されます。

The screenshot shows the Cisco WLC GUI for configuring a new WLAN. The left sidebar is under 'WLANs' > 'WLANs'. 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、[Status] と [Broadcast SSID] の両方の [Enabled] オプションがオンに

なっていることを確認します。WLAN 設定



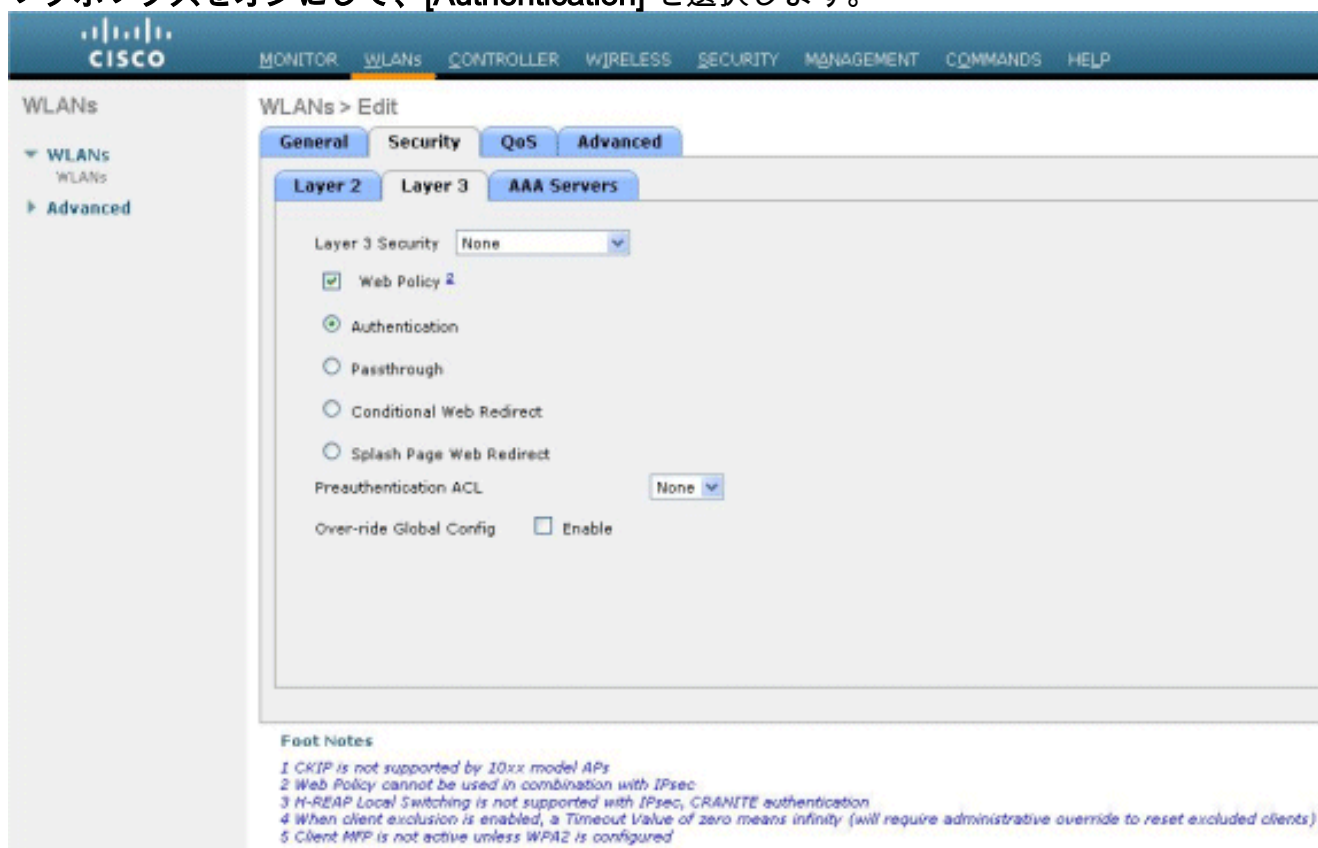
The screenshot shows the Cisco WLAN configuration interface. The top navigation bar includes MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, and HELP. The left sidebar shows the WLANs menu with options for WLANs and Advanced. The main content area is titled 'WLANs > Edit' and has 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 のインターフェイスを選択します。通常は、一意の VLAN 内に設定されているインターフェイスが WLAN にマッピングされ、クライアントはその VLAN 内の IP アドレスを受け取ります。この例では、[Interface] に *management* を使用します。
6. [Security] タブを選択します。
7. [Layer 2] メニューで、[Layer 2 Security] に対して [None] を選択します。
8. [Layer 3] メニューで、[Layer 3 Security] に対して [None] を選択します。[Web Policy] チェックボックスをオンにして、[Authentication] を選択します。



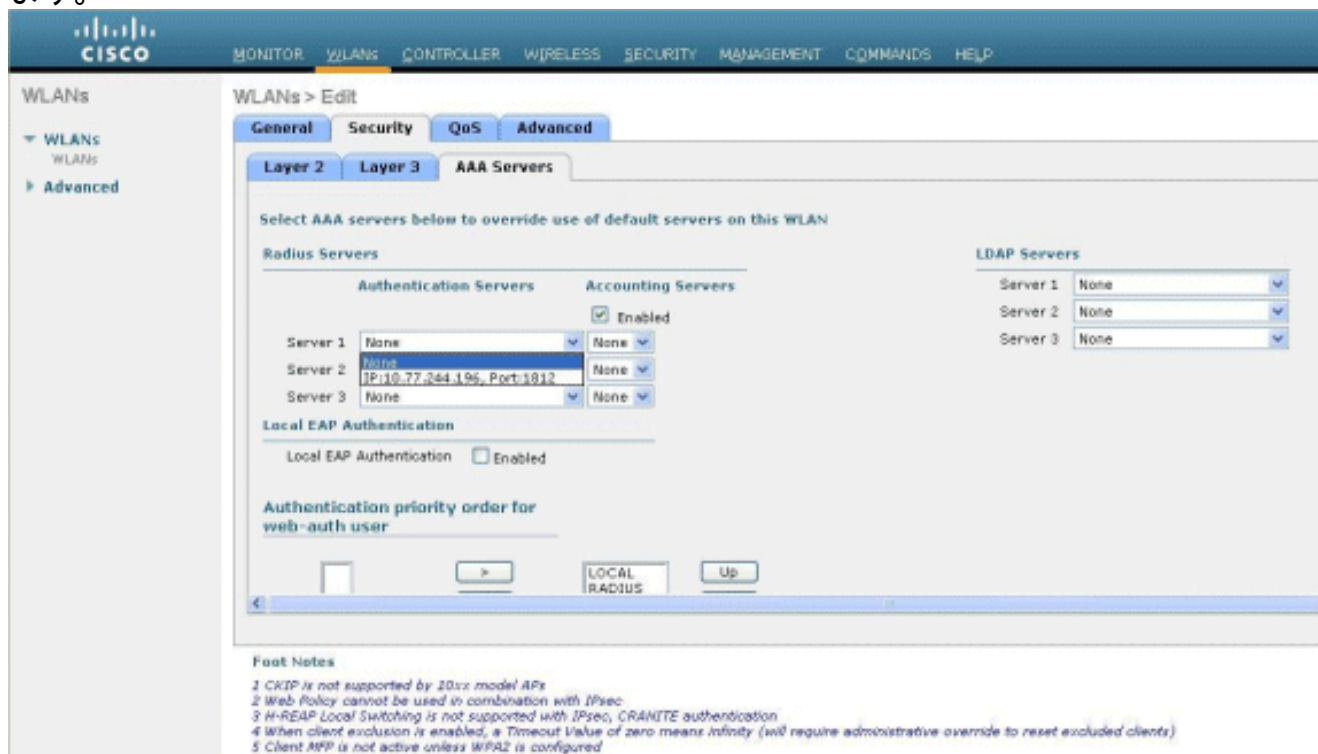
The screenshot shows the Cisco WLAN configuration interface, specifically the Layer 3 Security tab. The top navigation bar and left sidebar are the same as in the previous screenshot. The main content area is titled 'WLANs > Edit' and has tabs for General, Security, QoS, and Advanced. The Security tab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

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

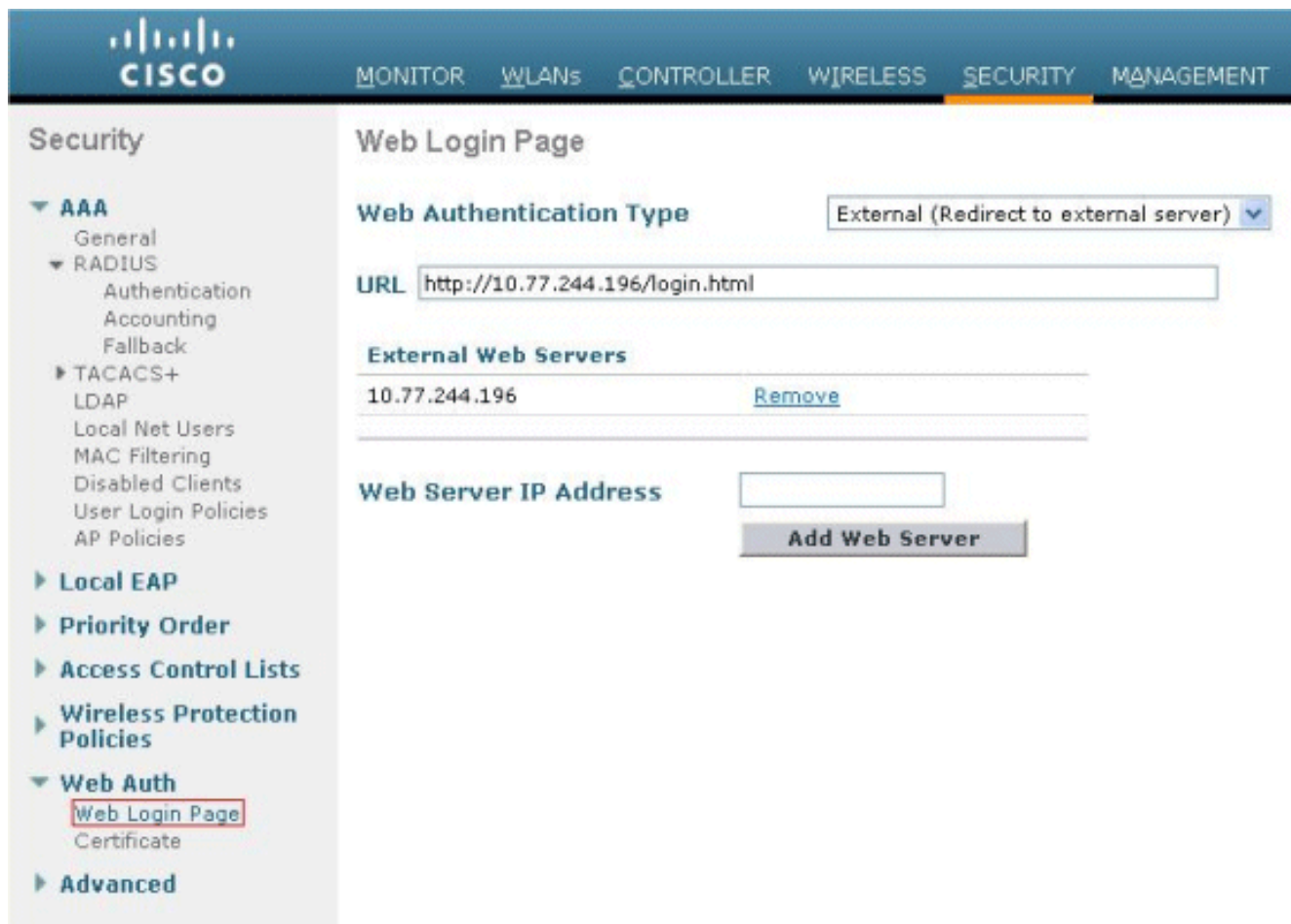
9. [AAA servers] メニューの下で、[Authentication Server] に対して、この WLC 上で設定した RADIUS サーバを選択します。他のメニューは、デフォルト値のままにしておく必要があります。



WLC 上での Web サーバ情報の設定

[Web Authentication] ページをホストする Web サーバは、この WLC 上に設定する必要があります。次の手順を実行して Web サーバを設定します。

1. [Security] タブをクリックします。[Web Auth] > [Web Login Page] に移動します。
2. [Web Authentication Type] を [External] に設定します。
3. [Web Server IP Address] フィールドに、[Web Authentication] ページをホストするサーバの IP アドレスを入力し、[Add Web Server] をクリックします。この例では、IP アドレスは 10.77.244.196 です。このアドレスは、[External Web Servers] の下に表示されます。
4. [URL] フィールドに [Web Authentication] ページの URL (この例では `http://10.77.244.196/login.html`) を入力します。



Cisco Secure ACS の設定

このドキュメントでは、Cisco Secure ACS サーバがすでにインストールされており、マシン上で稼働していると想定しています。Cisco Secure ACS のセットアップ方法の詳細については、『[Cisco Secure ACS 4.2 コンフィギュレーションガイド](#)』を参照してください。

Cisco Secure ACS 上でのユーザ情報の設定

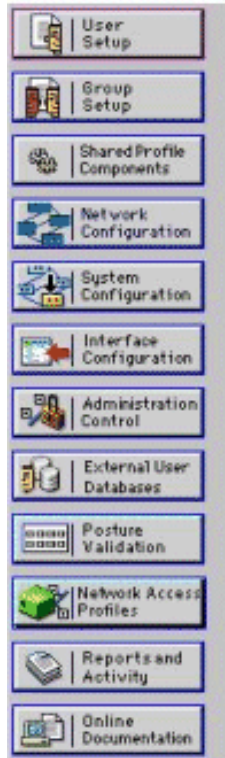
Cisco Secure ACS 上でユーザを設定するには、次の手順を実行します。

1. Cisco Secure 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、ユーザ名は *user1* です。



User Setup

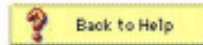
Select



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			



- デフォルトでは、PAP がクライアントの認証に使用されます。ユーザのパスワードは、**[User Setup] > [Password Authentication] > [Cisco Secure PAP]** の下で入力します。**[Password Authentication]** では、必ず **[ACS Internal Database]** を選択します。

Edit

User: user1 (New User)

Account Disabled

Supplementary User Info ?

Real Name

Description

User Setup ?

Password Authentication:

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

Separate (CHAP/MS-CHAP/ARAP)

Password
 Confirm Password

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. ユーザは、そのユーザが属しているグループに割り当てられる必要があります。[Default Group] を選択します。
4. [Submit] をクリックします。

Cisco Secure ACS 上での WLC 情報の設定

Cisco Secure ACS で WLC 情報を設定するには、次の手順を実行します。

1. ACS の GUI で、[Network Configuration] タブをクリックし、[Add Entry] をクリックします。
2. [Add AAA Client] 画面が表示されます。
3. クライアントの名前を入力します。この例では、WLC を使用します。
4. クライアントの IP アドレスを入力します。WLC の IP アドレスは、10.77.244.206 です。
5. 共有秘密鍵および鍵形式を入力します。この値は、WLC の [Security] メニューでの入力値と一致している必要があります。
6. [Key Input Format] で [ASCII] を選択します。これは WLC 上と同じ指定にする必要があります。
7. WLC と RADIUS サーバの間で使用するプロトコルを設定するために、[Authenticate Using]

- で [RADIUS (Cisco Airespace)] を選択します。
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 page is titled 'Add AAA Client' and is part of the 'Network Configuration' section. The form contains 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:

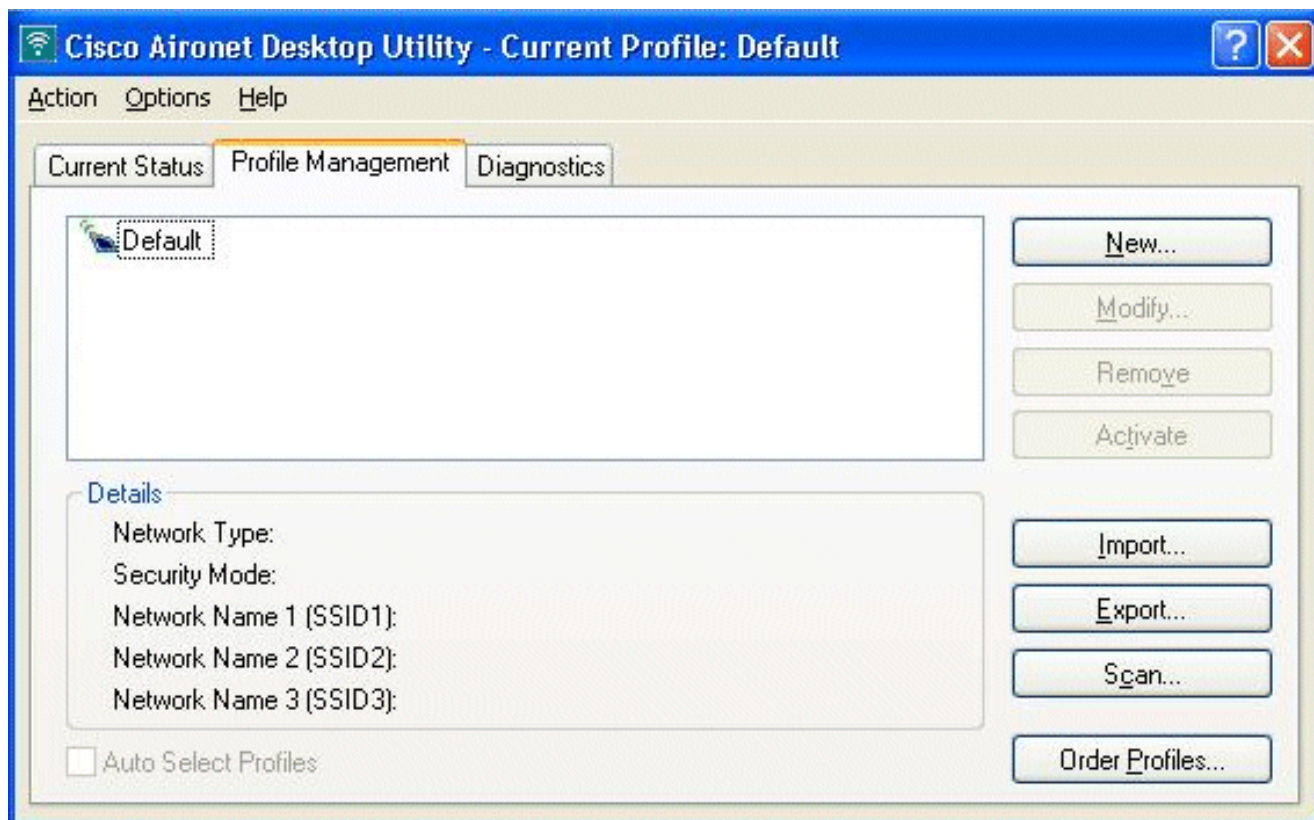
At the bottom of the form, there are three buttons: 'Submit', 'Submit + Apply', and 'Cancel'. Below the buttons is a 'Back to Help' button.

クライアント認証プロセス

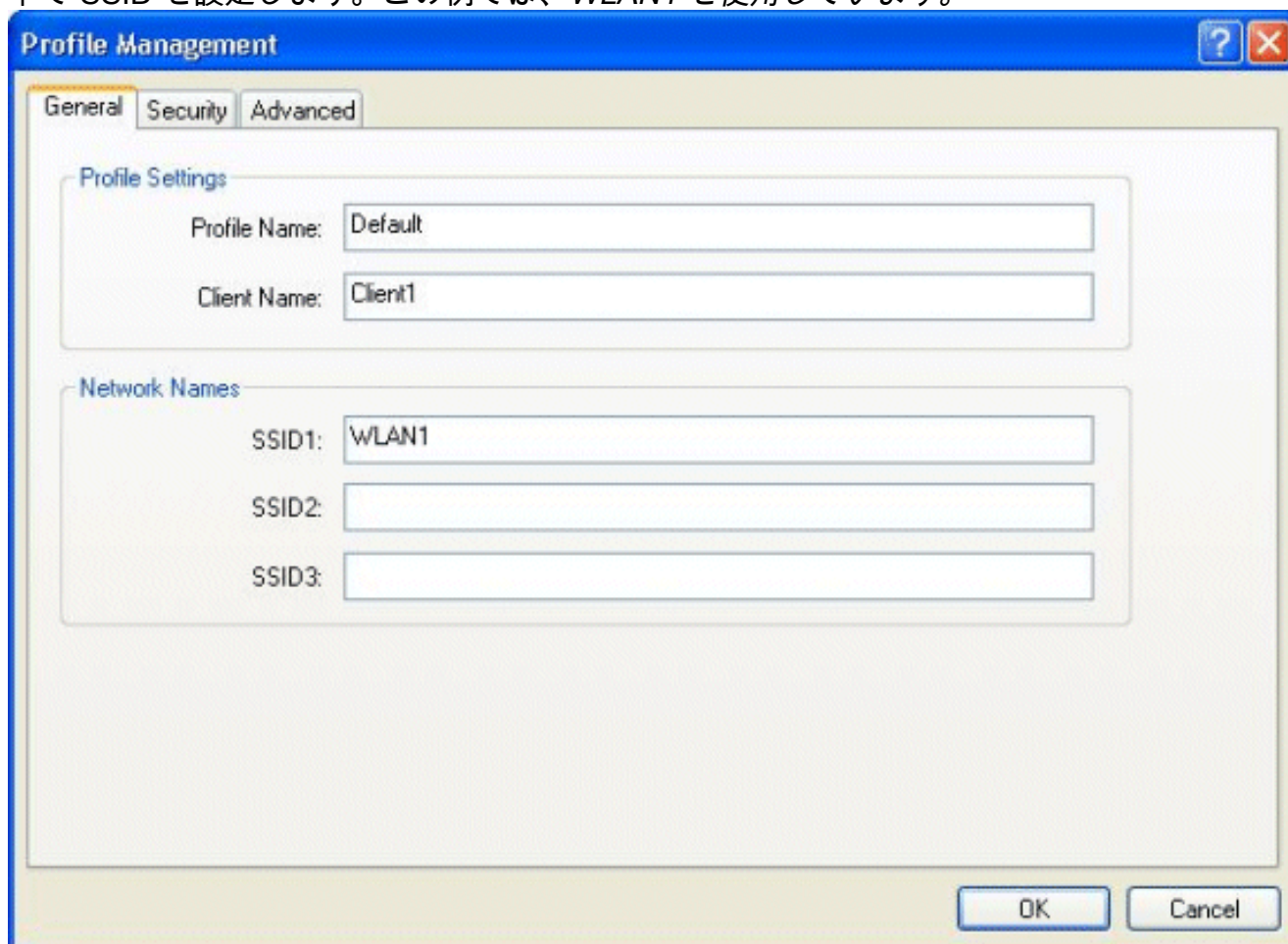
クライアントの設定

この例では、Cisco Aironet Desktop Utility を使用して Web 認証を実行します。Aironet Desktop Utility を設定するには、次の手順を実行します。

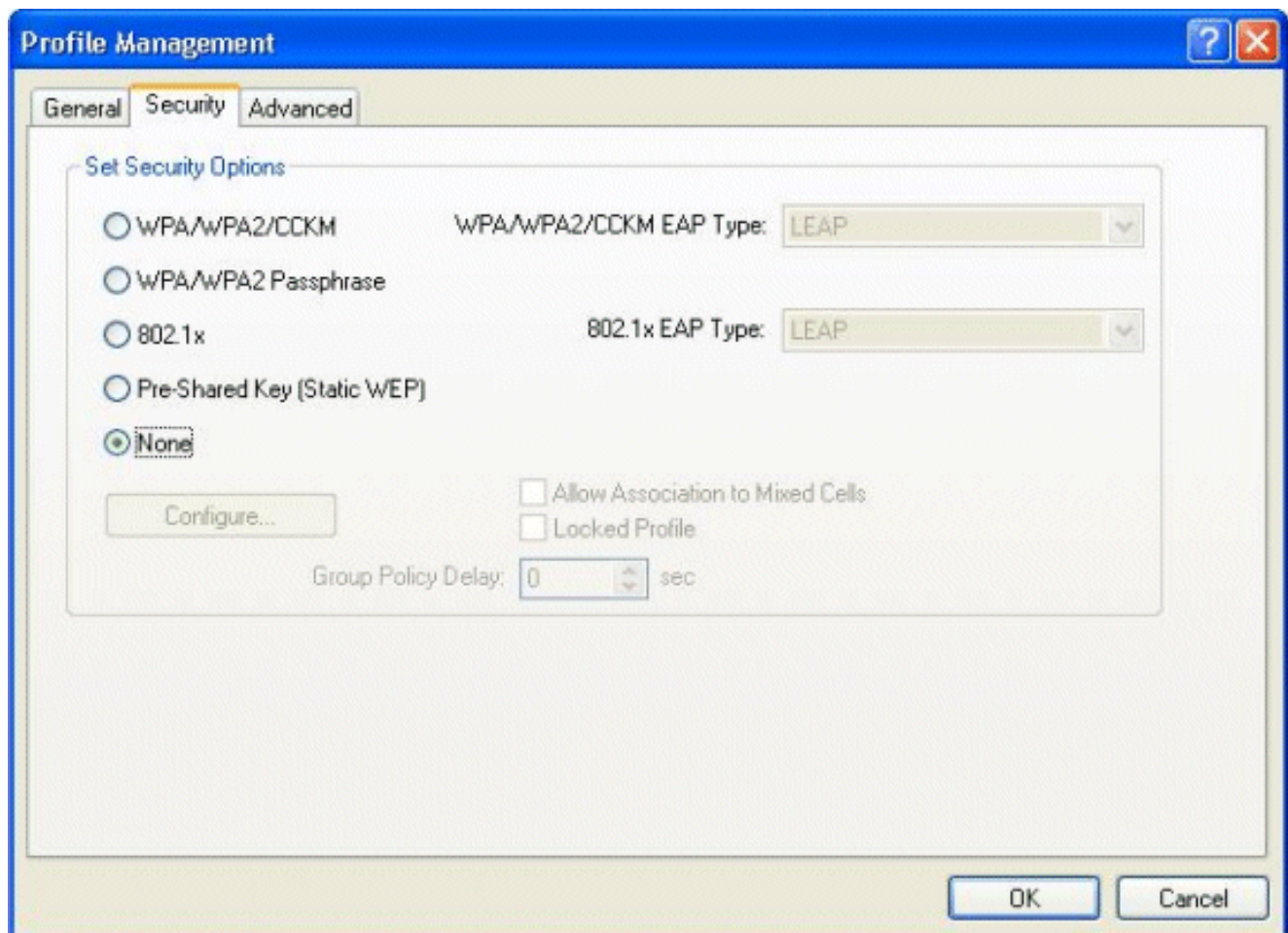
1. [Start] > [Cisco Aironet] > [Aironet Desktop Utility] から、Aironet Desktop Utility を開きます。
2. [Profile Management] タブをクリックします。



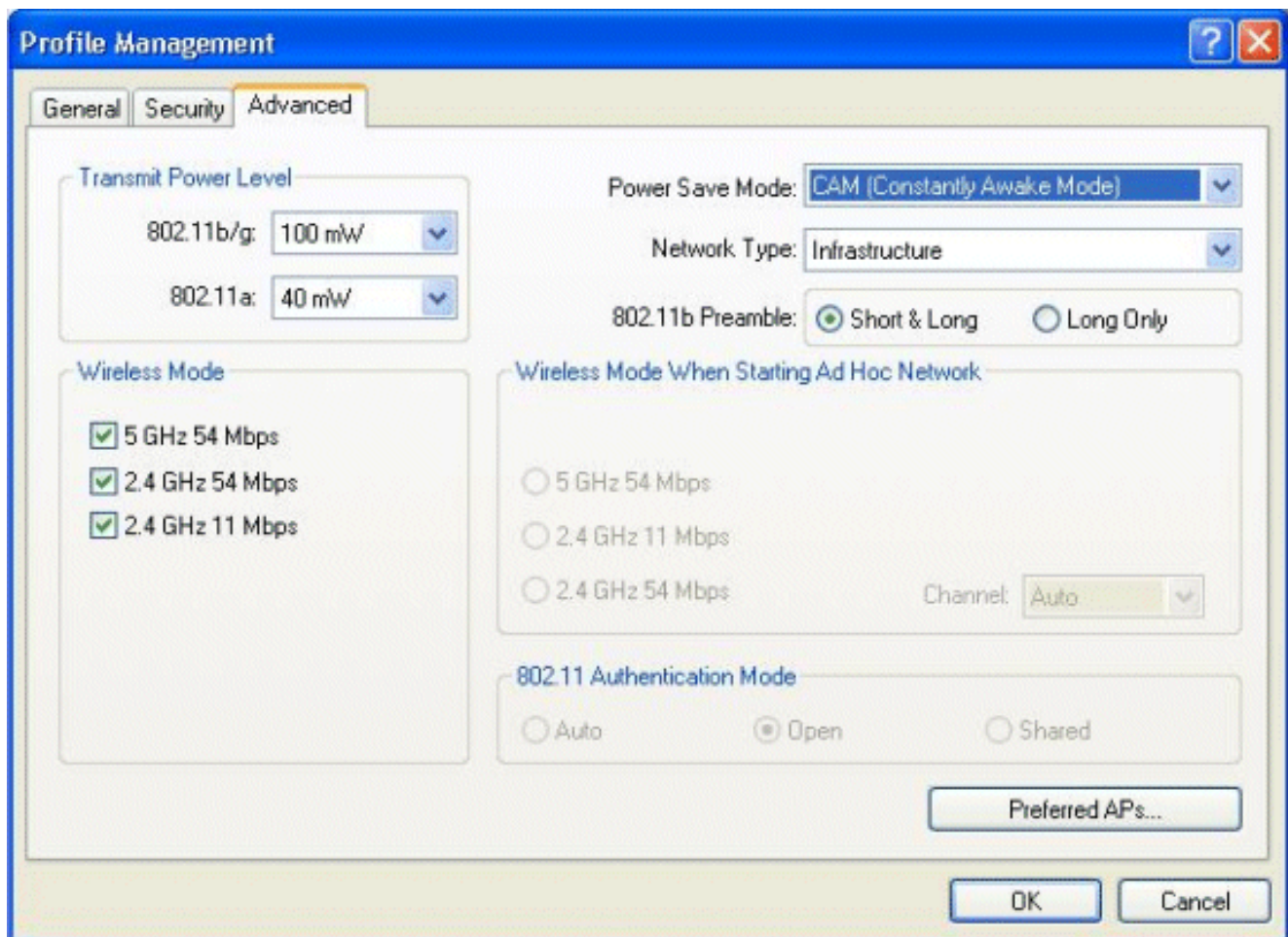
3. [Default profile] を選択し、[Modify] をクリックします。General タブをクリックします。[Profile Name] を設定します。この例では、Default を使用しています。[Network Names] の下で SSID を設定します。この例では、WLAN1 を使用しています。



注：SSIDでは大文字と小文字が区別されるため、WLCで設定されているWLANと一致している必要があります。[Security] タブをクリックします。Web 認証のセキュリティとして [None] 選択します。



[Advanced] タブをクリックします。[Wireless Mode] メニューの下で、ワイヤレスクライアントが LAP と通信する周波数を選択します。[Transmit Power Level] の下で、WLC 上で設定されている電力を選択します。[Power Save Mode] はデフォルト値のままにしておきます。[Network Type] として [Infrastructure] を選択します。互換性を向上させるために、[802.11b Preamble] に [Short & Long] を設定します。[OK] をクリックします。

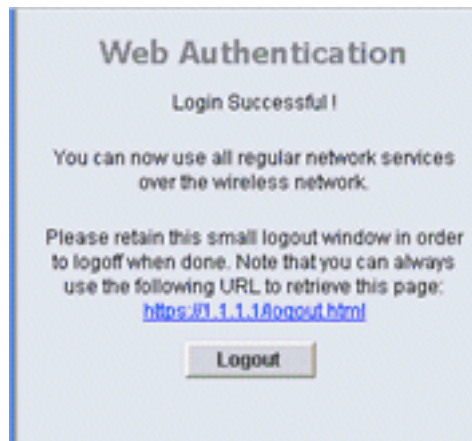


4. クライアント ソフトウェアにプロファイルが設定されると、クライアントは正常に関連付けられ、管理インターフェイス用に設定されている VLAN プールから IP アドレスを受け取ります。

クライアント ログイン プロセス

このセクションでは、クライアント ログインのプロセスを説明します。

1. ブラウザ ウィンドウを開き、URL または IP アドレスを入力します。こうするとクライアントに Web 認証ページが表示されます。コントローラが 3.0 より前のリリースを実行している場合には、ユーザは `https://1.1.1.1/login.html` を入力して、Web 認証ページを起動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. [Yes] をクリックして続行します。
3. [Login] ウィンドウが表示されたら、RADIUS サーバで設定したユーザ名とパスワードを入力します。ログインが成功すると、2つのブラウザ ウィンドウが表示されます。大きいほうのウィンドウはログインが正常に実行されたことを示し、このウィンドウでインターネットをブラウズできます。小さいほうのウィンドウは、ゲスト ネットワークの使用が完了した



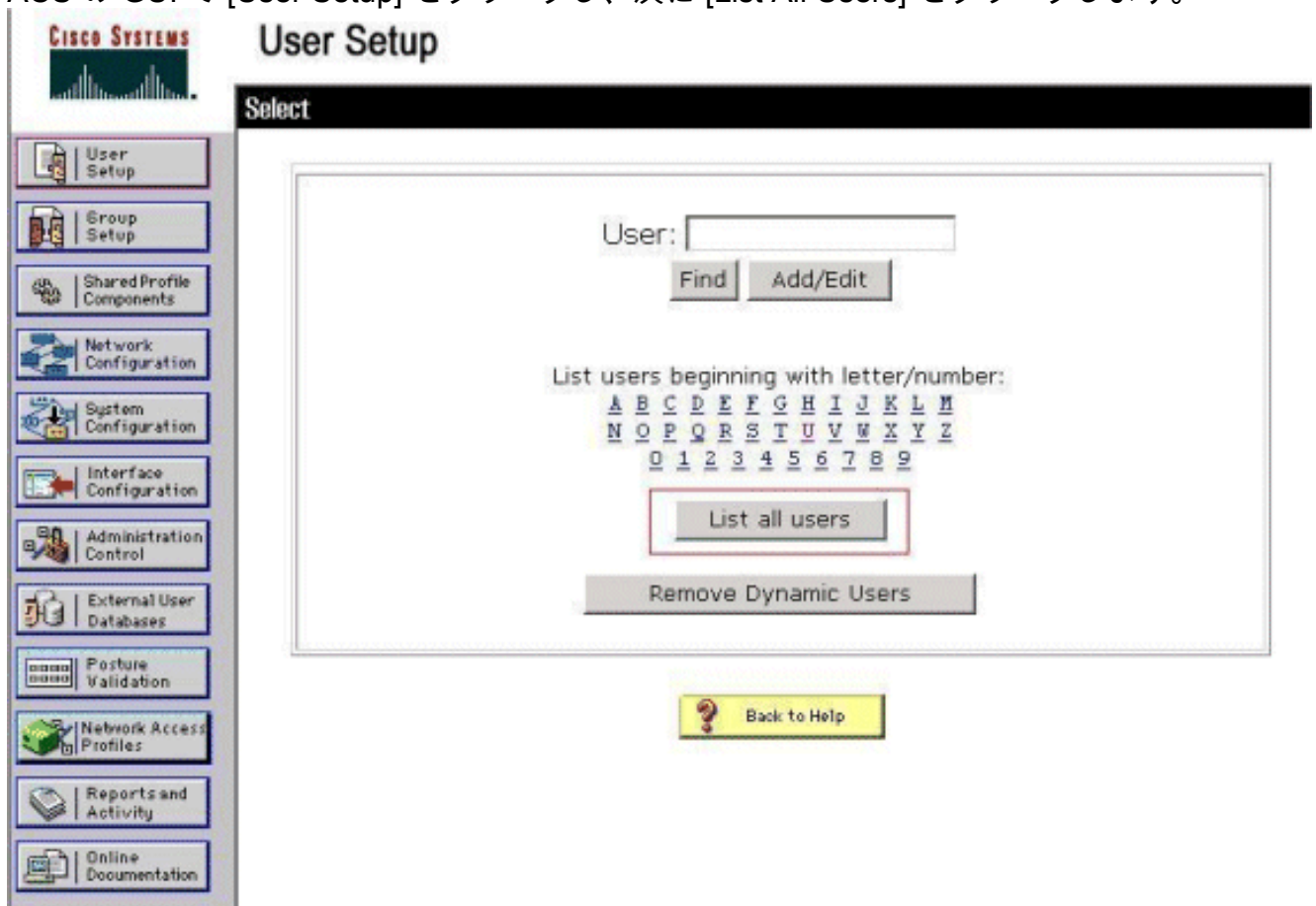
ときのログアウトに使用します。

確認

Web 認証が正常に実行されるようにするには、デバイスが適切な方法で設定されていることを確認する必要があります。このセクションでは、認証のプロセスで使用するデバイスを確認する方法を説明します。

ACS の確認

1. ACS の GUI で [User Setup] をクリックし、次に [List All Users] をクリックします。



[User] の [Status] が [Enabled] であり、[Default Group] がユーザにマッピングされていることを確認します。

User List

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

2. [Network Configuration] タブをクリックし、[AAA Clients] テーブルを参照して、WLC が AAA クライアントとして設定されていることを確認します。

The screenshot shows the Cisco Systems Network Configuration interface. On the left is a navigation menu with options like User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configurations, Administration Control, External User Databases, Profile Validation, Network Access Profiles, Reports and Activity, and Online Documentation. The main content area is titled 'Network Configuration' 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)'. Below the table are 'Add Entry' and 'Search' buttons.
- 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'. Below the table are 'Add Entry' and 'Search' buttons.
- 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'. Below the table are 'Add Entry' and 'Sort Entries' buttons.

At the bottom of the main content area is a 'Back to Help' button.

WLC の確認

1. WLC の GUI で [WLANs] メニューをクリックします。Web 認証で使用する WLAN がページ上にリストされていることを確認します。WLAN の [Admin Status] が [Enabled] であることを確認します。WLAN の [Security Policy] が [Web-Auth] と示されていることを確認します

The screenshot shows the Cisco WLC GUI with the 'WLANs' menu selected. The main content area displays a table of WLAN configurations:

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

2. WLC の GUI で [SECURITY] メニューをクリックします。Cisco Secure ACS (10.77.244.196) がページ上にリストされていることを確認します。[Network User]


```

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**

失敗した認証の試行は、[Reports and Activity] > [Failed Attempts] にあるメニューにリストされま
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](#)

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。