

外部ワイヤレスLANコントローラのWeb認証の設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[Web 認証](#)

[Web 認証プロセス](#)

[ネットワーク構成](#)

[Web 認証用のコントローラの設定](#)

[VLAN インターフェイスの作成](#)

[内部 Web 認証用の WLC の設定](#)

[WLAN インスタンスの追加](#)

[Web 認証でユーザを認証する 3 とおりの方法](#)

[ローカル認証](#)

[Web 認証用の RADIUS サーバ](#)

[ACS の設定](#)

[Cisco WLC への RADIUS サーバ情報の入力](#)

[RADIUSサーバを使用したWLANの設定](#)

[ACSの確認](#)

[LDAP サーバ](#)

[Web 認証を使用するための WLAN クライアントの設定](#)

[クライアントの設定](#)

[クライアントログイン](#)

[Web 認証のトラブルシューティング](#)

[ACSのトラブルシューティング](#)

[IPv6ブリッジングでのWeb認証](#)

[関連情報](#)

はじめに

このドキュメントでは、内部Web認証をサポートするようにCisco 4400シリーズワイヤレスLAN(WLAN)コントローラ(WLC)を設定する方法について説明します。

前提条件

要件

4400 WLCを初期設定することをお勧めします。

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。

- バージョン 7.0.116.0 が稼働している 4400 シリーズ WLC
- Microsoft® Windows 2003 Server にインストールされている Cisco Secure Access Control Server (ACS) バージョン 4.2
- Cisco Aironet 1131AG シリーズ Lightweight アクセス ポイント
- バージョン 4.0 が稼働する Cisco Aironet 802.11 a/b/g CardBus ワイヤレス アダプタ

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

ドキュメント表記の詳細は、『[テクニカルティップスのフォーマット表記法の使用とその他のコンテンツ](#)』を参照してください。

Web 認証

Web認証は、有効なユーザ名とパスワードが正しく入力されるまで、特定のクライアントからのIPトラフィック (DHCPおよびDNS関連のパケットを除く) をコントローラで許可しないようにするレイヤ3セキュリティ機能です。これは、サブリカントやクライアントユーティリティを必要としない簡単な認証方式です。一般に、Web 認証はゲスト アクセス ネットワークを展開する場合に使用されます。一般的な導入には、T-Mobile®やStarbucks®が提供するような「ホットスポット」の場所が含まれます。

Web 認証はデータ暗号化を提供しないことを注意してください。Web認証は、接続性だけが問題となるホットスポットまたはキャンパス環境での単純なゲストアクセスとして使用されます。

Web認証は次のコマンドを使用して実行できます。

- WLCのデフォルトログインウィンドウ
- WLCのデフォルトログインウィンドウの変更バージョン
- 外部Webサーバで設定するカスタマイズされたログインウィンドウ (外部Web認証)
- コントローラにダウンロードするカスタマイズされたログインウィンドウ

このマニュアルでは、内部 Web 認証用のワイヤレス LAN コントローラが設定されています。

Web 認証プロセス

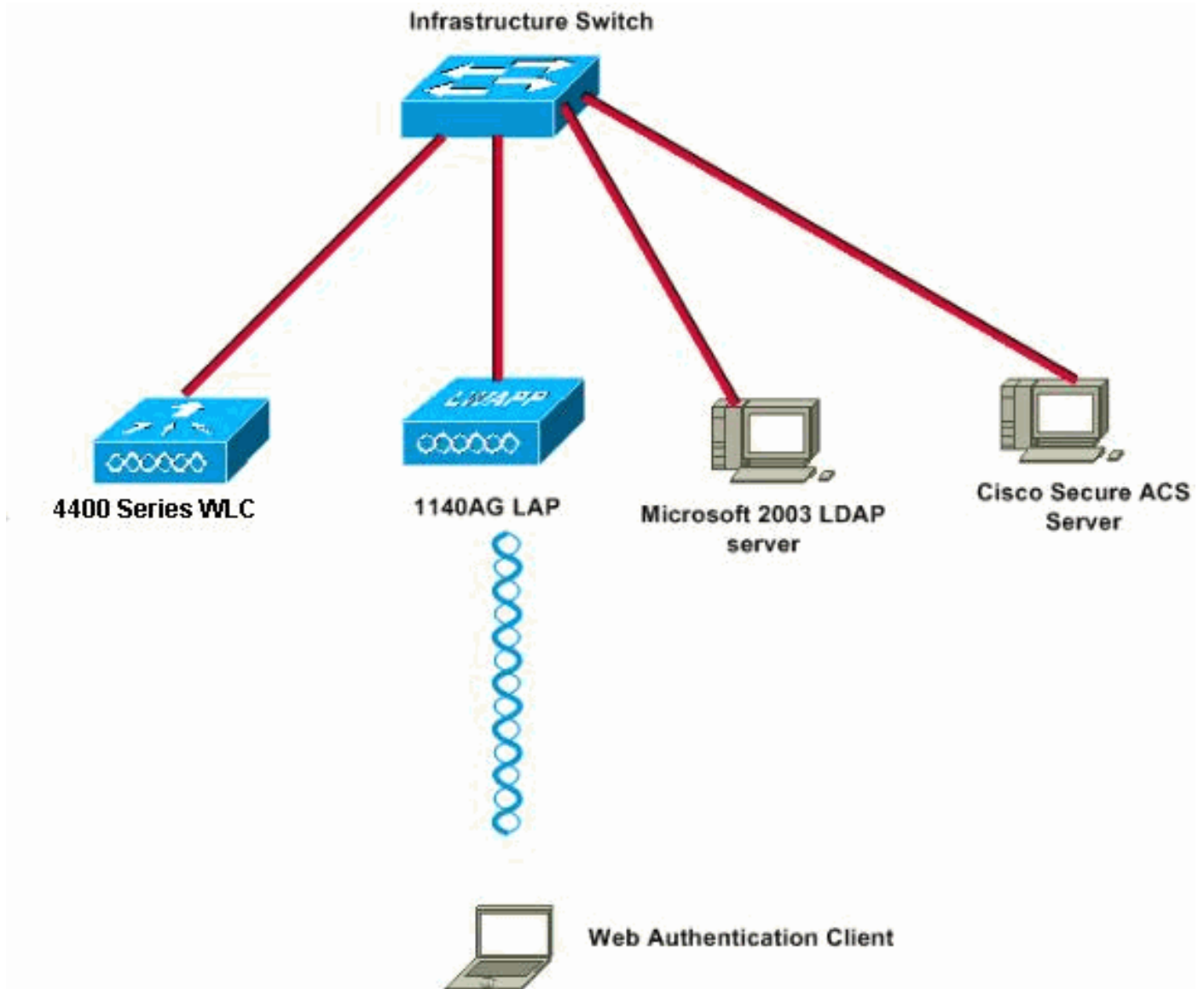
ユーザが Web 認証用に設定された WLAN に接続する場合は、次のようになります。

- ユーザは、Web ブラウザを開き、URL として、たとえば、`http://www.cisco.com` を入力します。クライアントは、宛先の IP を取得するため、この URL の DNS 要求を送信します。WLC は DNS サーバに DNS 要求をバイパスし、DNS サーバは宛先 `www.cisco.com` の IP アドレスを含む DNS 応答で返答します。次にこれがワイヤレス クライアントに転送されます。
- 続いて、クライアントは宛先 IP アドレスを使用して TCP 接続を開始しようとします。`www.cisco.com` の IP アドレスを宛先とする TCP SYN パケットが送信されます。
- WLC にはクライアント用に設定されたルールがあるため、`www.cisco.com` のプロキシとして機能します。WLC は、`www.cisco.com` の IP アドレスを送信元とする TCP SYN-ACK パケットをクライアントに戻します。クライアントは、3 ウェイ TCP ハンドシェイクを完了するために、TCP ACK パケットを返し、TCP 接続が完全に確立されます。
- クライアントは、宛先が `www.cisco.com` である HTTP GET パケットを送信します。WLC はこのパケットをインターセプトして、リダイレクト処理用送信します。HTTP アプリケーション ゲートウェイは、HTML 本文を準備し、クライアントから要求された HTTP GET への応答として返します。この HTML により、クライアントは WLC のデフォルト Web ページの URL (たとえば、`http://<Virtual-Server-IP>/login.html.`) に転送されます。
- クライアントは、たとえば、`www.cisco.com` などの IP アドレスとの TCP 接続を閉じます。
- ここで、クライアントが `http://10.1.1.1/login.html` に移動したいとします。そのため、クライアントは WLC の仮想 IP アドレスとの TCP 接続を開こうとします。WLC に `10.1.1.1` の TCP SYN パケットを送信します。
- WLC は TCP SYN-ACK で返答し、クライアントはハンドシェイクを完了するために、TCP ACK を WLC に戻します。
- クライアントは、ログインページを要求するために、`10.1.1.1`を宛先とする、`/login.html`の HTTP GETを送信します。
- この要求はWLCのWebサーバで許可され、サーバはデフォルトログインページで応答します。クライアントは、ユーザがログインできるログインページをブラウザウィンドウで受け取ります。

Web認証プロセスの説明については、『[CiscoワイヤレスLANコントローラ\(WLC\)でのWeb認証](#)』を参照してください。

ネットワーク構成

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。



ネットワーク構成

Web 認証用のコントローラの設定

このドキュメントでは、WLAN は Web 認証用に設定され、専用 VLAN にマップされています。以下に示すのは、Web 認証用の WLAN の設定に関する手順です。

1. [VLAN インターフェイスの作成](#)
2. [内部 Web 認証用の WLC の設定](#)
3. [WLAN インスタンスの追加](#)
4. [認証タイプの設定 \(Web 認証でユーザを認証する 3 とおりの方法 \)](#)

この項では、Web認証用にコントローラを設定する方法を中心に説明します。

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 の IP アドレスは 10.77.244.204 です。

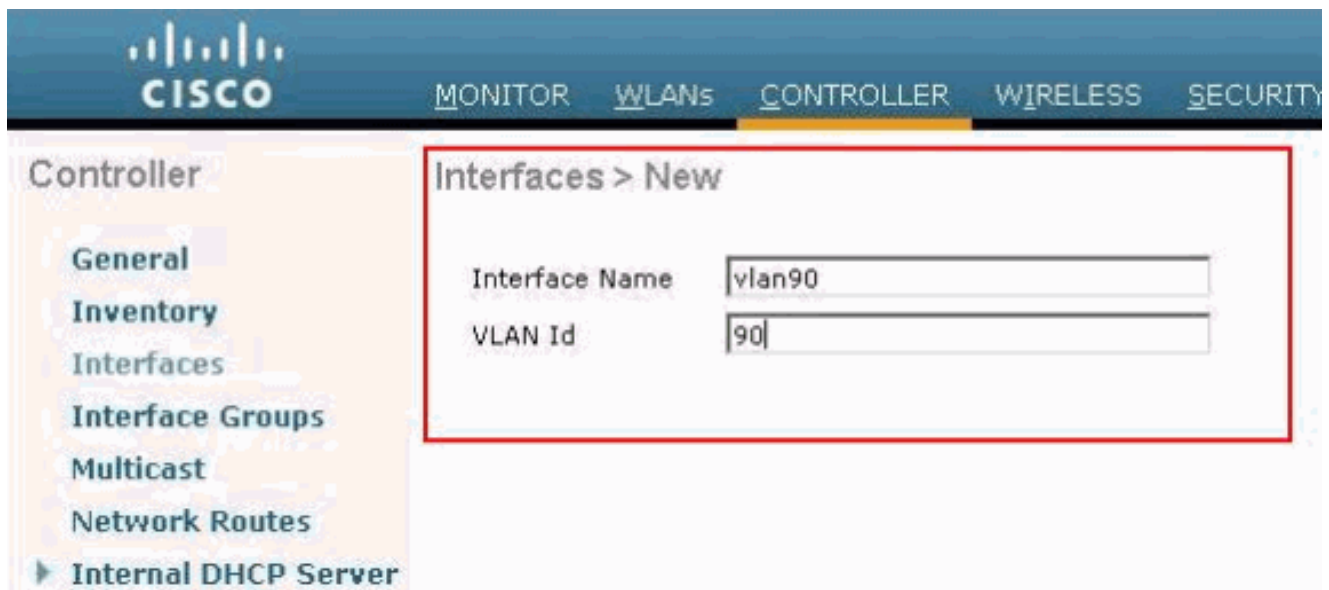
- ACS サーバの IP アドレスは 10.77.244.196 です。

VLAN インターフェイスの作成

次のステップを実行します。

1. ワイヤレス LAN コントローラ GUI で、上部のメニューから [Controller] を選択し、左側のメニューから [Interfaces] を選択し、ウィンドウの右上の [New] をクリックして、新しい動的インターフェイスを作成します。

[Interfaces] > [New] ウィンドウが表示されます。この例では、[Interface Name] には vlan90 を、[VLAN ID] には 90 をそれぞれ使用しています。




「インタフェース」 > 「新規ウィンドウ」の順に開く

2. VLAN インターフェイスを作成するには、[Apply] をクリックします。

[Interfaces] > [Edit] ウィンドウが表示され、インターフェイス固有の情報を入力することが求められます。

3. このドキュメントでは、次のパラメータを使用します。

- IP アドレス : 10.10.10.2
- ネットマスク : 255.255.255.0 (24 ビット)
- ゲートウェイ : 10.10.10.1
- ポート番号 : 2
- プライマリ DHCP サーバ : 10.77.244.204

 注 : このパラメータは、RADIUSサーバまたはDHCPサーバのIPアドレスである必要があります。この例では、内部 DHCP スコープが WLC 上で設定されてい

✎ るため、WLC の管理アドレスは DHCP サーバとして使用されます。

- セカンダリ DHCP サーバ : 0.0.0.0

✎ 注 : この例ではセカンダリDHCPサーバがないため、0.0.0.0を使用しています。
設定にセカンダリ DHCP サーバがあれば、そのサーバ IP アドレスをこのフィールドに追加します。

- ACL 名 : なし

The screenshot displays the Cisco WLC configuration interface for editing the 'vlan90' interface. The left sidebar shows the navigation menu with 'Interfaces' selected. The main content area is titled 'Interfaces > Edit' and contains several configuration sections:

- General Information:** Interface Name: vlan90, MAC Address: 00:0b:85:48:53:c0
- Configuration:** Guest Lan: , Quarantine: , Quarantine Vlan Id: 0
- Physical Information:** Port Number: 2, Backup Port: 0, Active Port: 0, Enable Dynamic AP Management:
- Interface Address:** VLAN Identifier: 90, IP Address: 10.10.10.2, Netmask: 255.255.255.0, Gateway: 10.10.10.1
- DHCP Information:** Primary DHCP Server: 10.77.244.204, Secondary DHCP Server: (empty)
- Access Control List:** ACL Name: none

Interfaces > Editウィンドウの一般情報

4. Apply をクリックして変更を保存します。

内部 Web 認証用の WLC の設定

次の手順では、内部 Web 認証用の WLC を設定します。内部 Web 認証は、WLC 上でのデフォルトの Web 認証タイプです。このパラメータが変更されていなければ、内部 Web 認証を有効にするための設定は必要ありません。Web 認証パラメータが以前に変更されている場合には、内部 Web 認証用に WLC を設定するために、次の手順を実行します。


1. コントローラのGUIから、Security > Web Auth > Web Login Page の順に選択して、Web Login Pageにアクセスします。
2. [Web Authentication Type] ドロップダウン ボックスから、[Internal Web Authentication] を選択します。
3. Redirect URL after loginフィールドに、認証が成功した後にエンドユーザがリダイレクトされるページのURLを入力します。

The screenshot shows the Cisco WLC configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY' (highlighted with a red box), 'MANAGEMENT', and 'COMMANDS'. On the left, the 'Security' menu is expanded to 'Web Auth', with 'Web Login Page' selected (also highlighted with a red box). The main content area is titled 'Web Login Page' and contains the following fields:

- Web Authentication Type: Internal (Default)
- Redirect URL after login: www.cisco.com

Below these fields is a descriptive text: "This page allows you to customize the content and appearance of the Login page. The Login page is presented to web users the first time they access the WLAN if 'Web Authentication' is turned on (under WLAN Security Policies)." Underneath, there are sections for 'Cisco Logo' (with 'Show' and 'Hide' radio buttons), 'Headline', and 'Message'.

ログイン後のリダイレクトURL

 注:WLCバージョン5.0以降では、Web認証用のログアウトページもカスタマイズできます。

WLAN インスタンスの追加

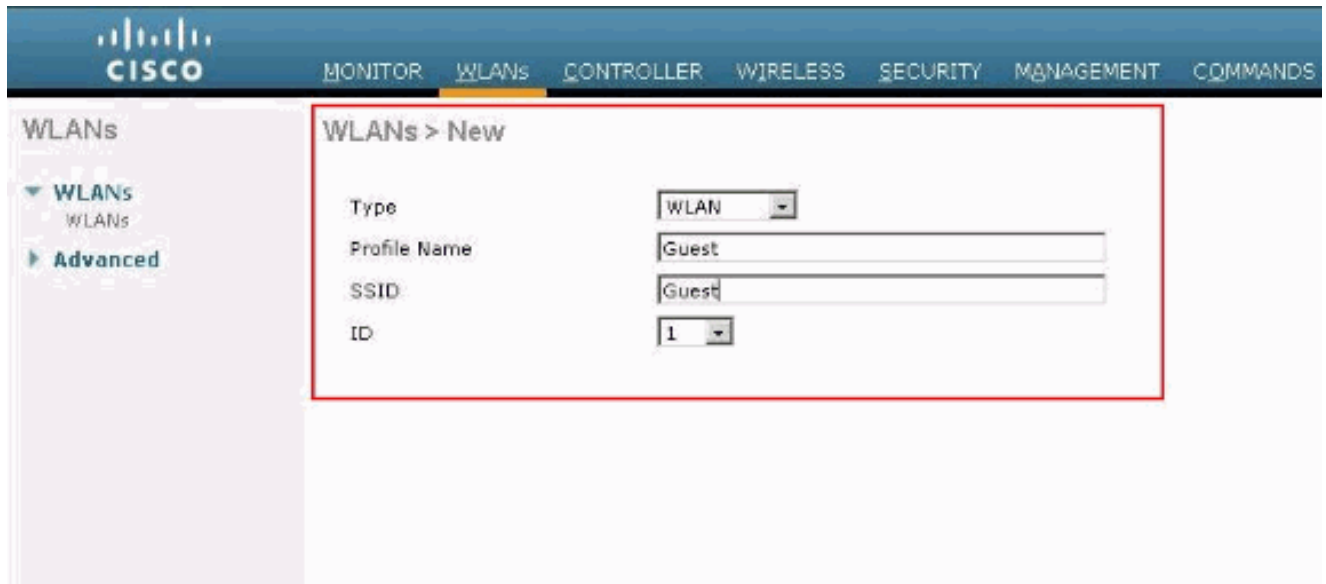
内部 Web 認証が有効になっており、Web 認証専用の VLAN があるので、Web 認証ユーザをサポ

ートするために新しい WLAN/SSID を提供する必要があります。

新しい WLAN/SSID を作成するには、次の手順を実行します。

1. WLC GUI から、最上部のメニューで [WLAN] をクリックし、右上にある [New] をクリックします。

[Type] で [WLAN] を選択します。Web 認証用のプロファイル名と WLAN SSID を選択します。この例では、Profile NameとWLAN SSIDの両方にGuestを使用しています。



プロファイル名とWLAN SSID

2. [APPLY] をクリックします。


新しい [WLANs] > [Edit] ウィンドウが表示されます。

WLANs > Edit 'Guest'

General	Security	QoS	Advanced
Profile Name	Guest		
Type	WLAN		
SSID	Guest		
Status	<input checked="" type="checkbox"/> Enabled		
Security Policies	None (Modifications done under security tab will appear after applying the changes.)		
Radio Policy	All		
Interface/Interface Group(G)	vlan90		
Multicast Vlan Feature	<input type="checkbox"/> Enabled		
Broadcast SSID	<input checked="" type="checkbox"/> Enabled		

WLANs > Editウィンドウが表示されます


3. WLAN のステータス ボックスをオンにして、WLAN を有効にします。[Interface] メニューで、以前に作成した VLAN インターフェイスの名前を選択します。この例では、インターフェイス名は vlan90 です。

 注：この画面の他のパラメータは、デフォルト値のままにします。

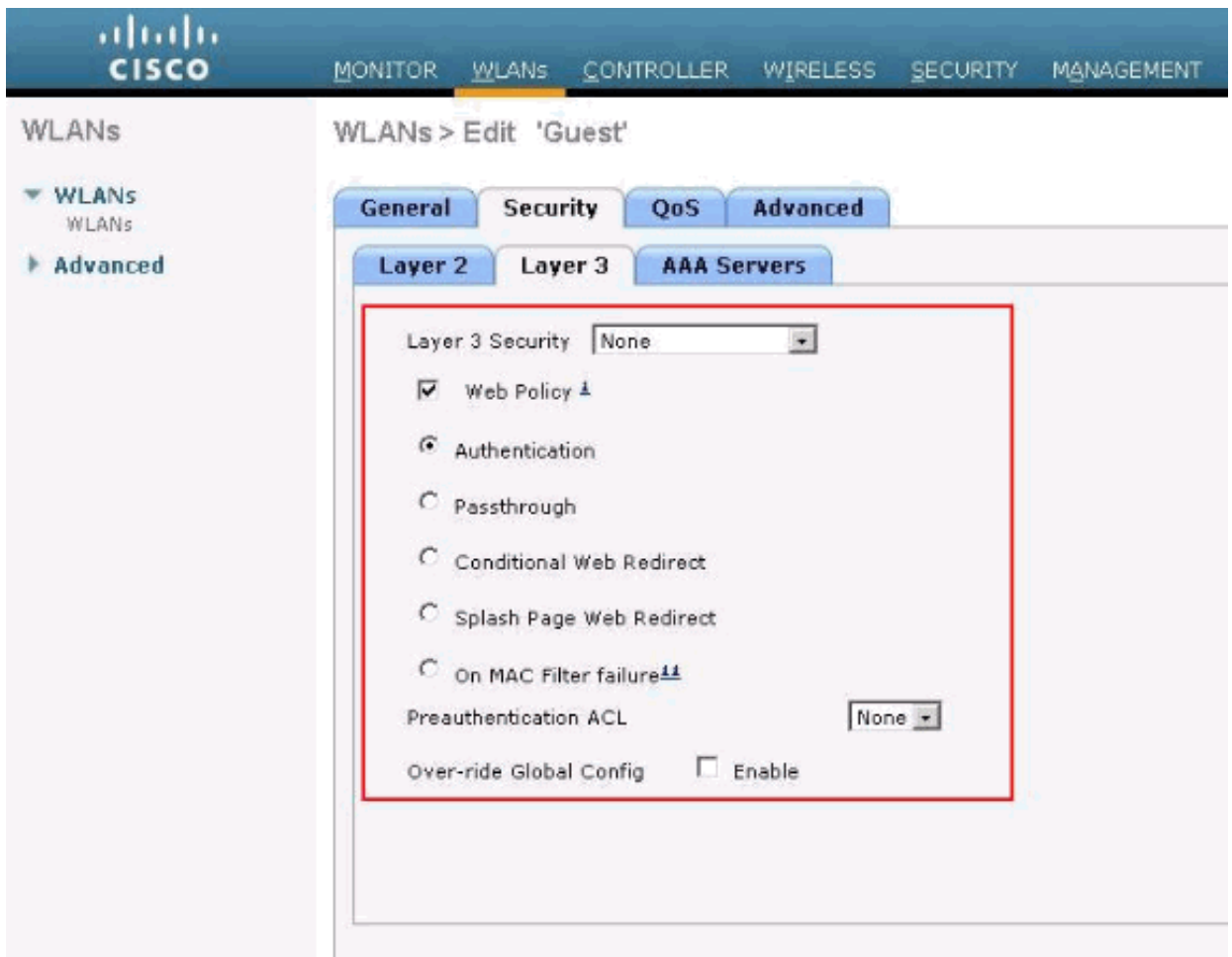
4. [Security] タブをクリックします。

次の手順を実行して、Web 認証を設定します。

- a. [Layer 2] タブをクリックして、セキュリティを [None] に設定します。

 注:WLANでは、Webパススルーをレイヤ3セキュリティとして802.1xを使用するように設定したり、WPA/WPA2をレイヤ2セキュリティとして設定したりすることはできません。ワイヤレスLANコントローラレイヤ2およびレイヤ3セキュリティの互換性については、『[ワイヤレスLANコントローラレイヤ2レイヤ3セキュリティの互換性マトリクス](#)』を参照してください

- b. [レイヤ3 (Layer 2)] タブをクリックします[Web Policy] ボックスをオンにして、次に示す [Authentication] オプションを選択します。



Layer 3」タブをクリックし、Web Policyボックスにチェックマークを付けます

- c. [Apply] をクリックして、WLAN を保存します。
- d. WLAN 概要ウィンドウに戻ります。SSID ゲストの WLAN テーブルの [Security Policies] 列の下で、Web 認証が有効になっていることを確認します。

Web 認証でユーザを認証する 3 とおりの方法

Web 認証を使用する場合には、ユーザを認証する 3 とおりの方法があります。ローカル認証によって、Cisco WLC のユーザを認証することができます。さらに、外部 RADIUS サーバまたは LDAP サーバをバックエンド データベースとして使用してユーザを認証することもできます。

このドキュメントでは、3 つすべての方法での設定例を示しています。

ローカル認証

ゲストユーザのユーザデータベースは、WLCのローカルデータベースに保存されます。ユーザは、次のデータベースに対してWLCによって認証されます。

1. WLC GUI で [Security] を選択します。
2. 左側の [AAA] メニューから [Local Net Users] をクリックします。

The screenshot shows the Cisco Security configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', and 'COMMANDS'. The 'SECURITY' tab is active. On the left, a 'Security' menu is expanded to show 'Local Net Users' highlighted with a red box. The main content area is titled 'Local Net Users' and contains a table with the following headers: 'User Name', 'WLAN Profile', 'Guest User', 'Role', and 'Description'. The table is currently empty.

左側のメニューからローカルネットユーザをクリックします

3. Newをクリックして新しいユーザを作成します。

新しいウィンドウが表示され、ユーザ名とパスワード情報の入力が求められます。

4. 新しいユーザを作成するためにユーザ名とパスワードを入力し、使用するパスワードを確認します。

この例では、User1 というユーザを作成します。

5. 説明を追加します。

この例では、Guest User1 を使用します。

6. Applyをクリックして、新しいユーザ設定を保存します。

Security

- AAA
 - General
 - RADIUS
 - Authentication
 - Accounting
 - Fallback
 - TACACS+
 - LDAP
 - Local Net Users
 - MAC Filtering
 - Disabled Clients
 - User Login Policies
 - AP Policies
 - Password Policies
- Local EAP
- Priority Order
- Certificate
- Access Control Lists
- Wireless Protection Policies
- Web Auth
- Advanced

Local Net Users > New

User Name: User1

Password: [masked]

Confirm Password: [masked]

Guest User:

Lifetime (seconds): 86400

Guest User Role:

WLAN Profile: Guest

Description: GuestUser1

新しいユーザ設定の保存への適用

Security

- AAA
 - General
 - RADIUS
 - Authentication
 - Accounting
 - Fallback
 - TACACS+
 - LDAP
 - Local Net Users
 - MAC Filtering
 - Disabled Clients

Local Net Users


User Name	WLAN Profile	Guest User Role	Description
User1	Guest	Yes	GuestUser1


Local Net Users

7. データベースにさらにユーザーを追加するには、手順3-6を繰り返します。

Web 認証用の RADIUS サーバ

このドキュメントは、RADIUS サーバとして Windows Server 2003 上のワイヤレス ACS を使用します。ネットワークで現在展開されている使用可能な任意の RADIUS サーバを使用できます。

 注:ACSはWindows NTまたはWindows 2000 Serverで設定できます。Cisco.comからACSをダウンロードするには、『Software Center (ダウンロード) – Cisco Secure Software』を参照してください。ソフトウェアをダウンロードするには、Cisco Web アカウントが必要です。

 注：シスコの内部ツールおよび情報にアクセスできるのは、シスコの登録ユーザーのみです。


「ACS の設定」のセクションでは、RADIUS 用に ACS を設定する方法を示しています。ドメイン名システム (DNS) および RADIUS サーバがある、完全に機能するネットワークが必要です。

ACS の設定

このセクションでは、RADIUS 用に ACS を設定するための情報を提供します。

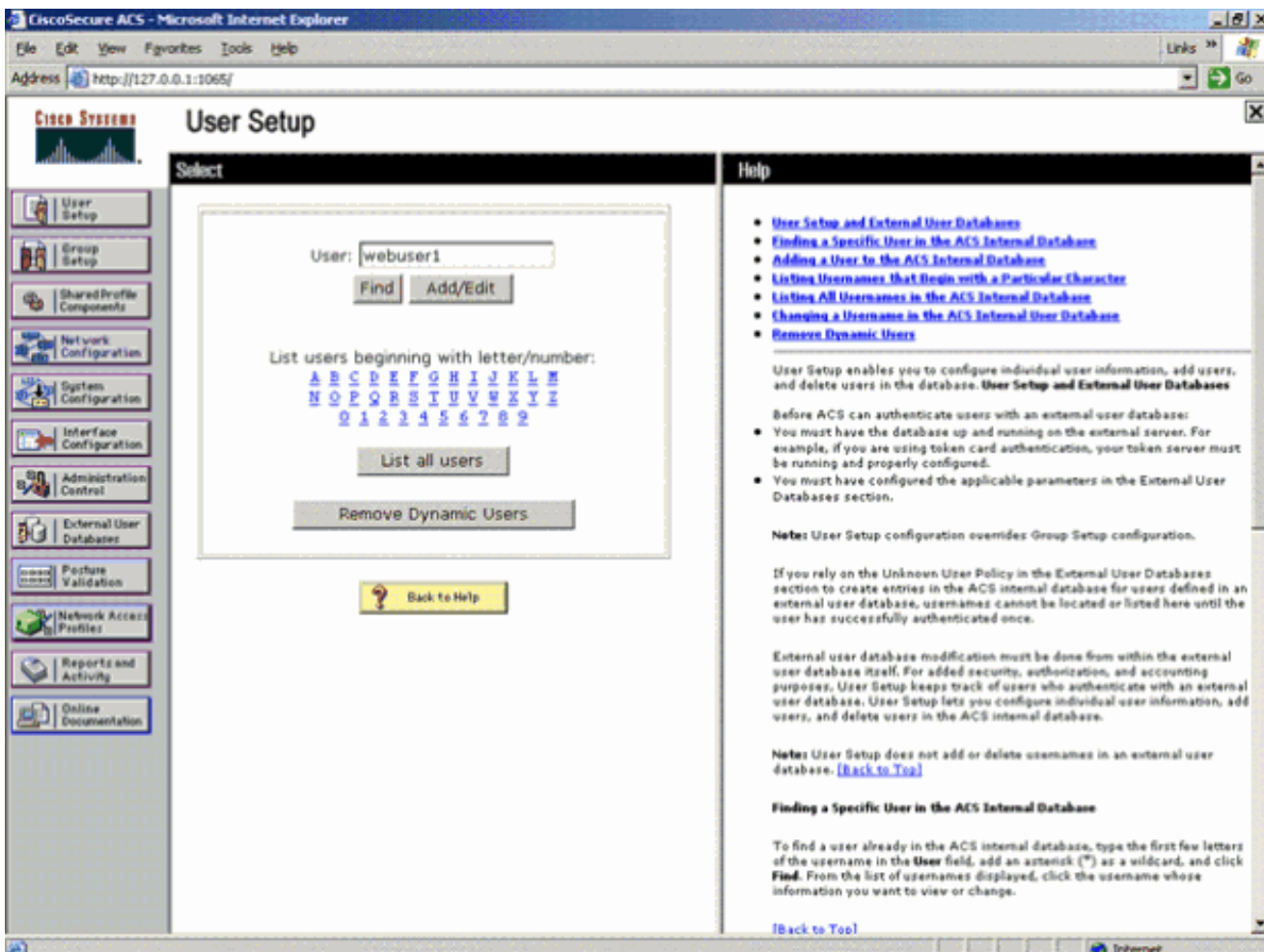
サーバ上で ACS を設定し、認証用のユーザを作成するために次の手順を実行します。

1. ACS によりブラウザ ウィンドウで ACS を開いて設定するかどうか尋ねられた場合は、[yes] をクリックします。

 注:ACSをセットアップすると、デスクトップにもアイコンが表示されます。

2. 左側のメニューで、[User Setup] をクリックします。

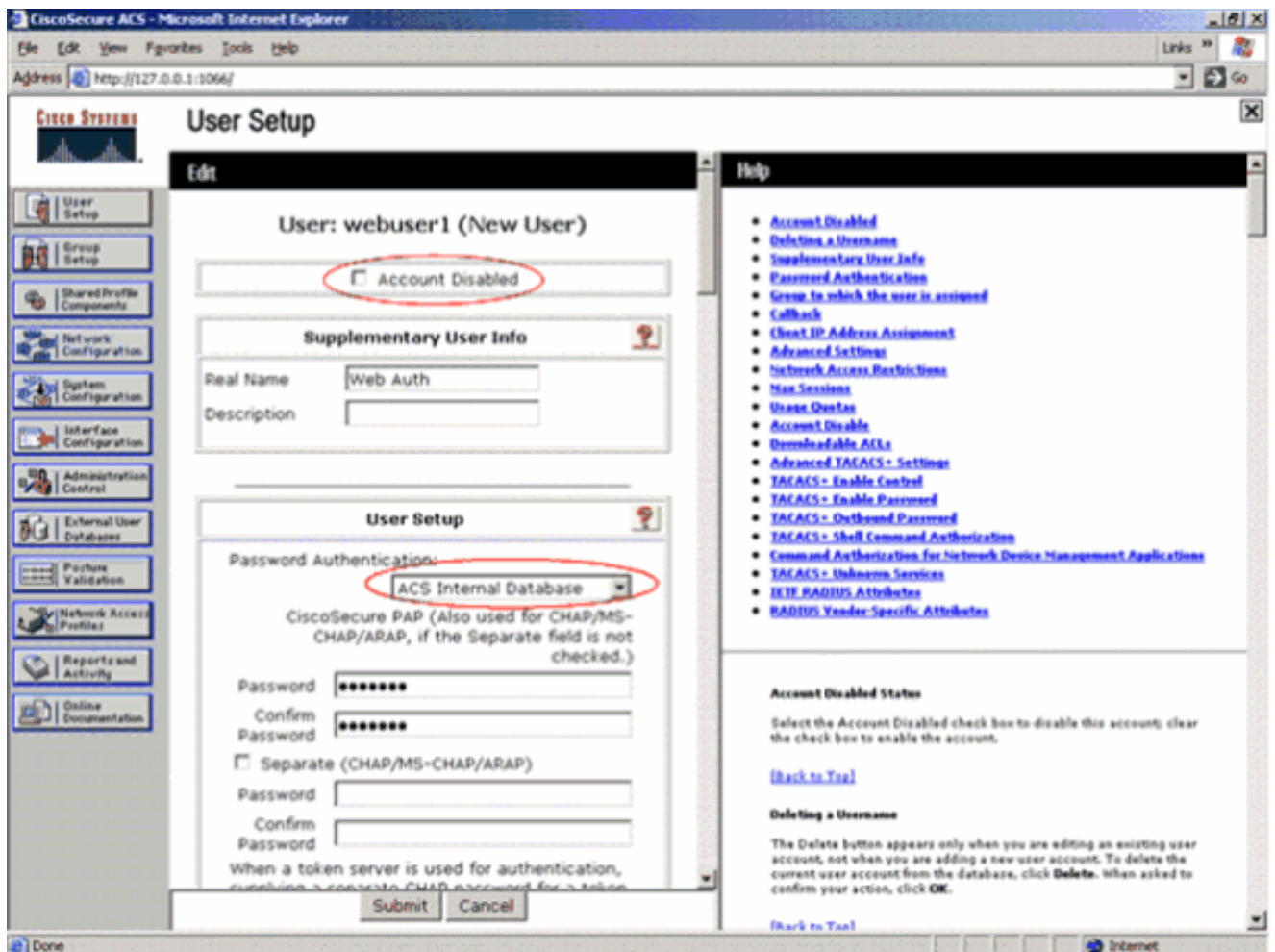
このアクションにより、次に示す [User Setup] 画面が表示されます。



User Setup画面

3. Web 認証に使用するユーザを入力して、[Add/Edit] をクリックします。

ユーザの作成後に、次に示す 2 番目のウィンドウが表示されます。



ユーザが作成されると、2番目のウィンドウが開きます

4. 上部の [Account Disabled] ボックスがオンになっていないことを確認します。

5. [Password Authentication] オプションに [ACS Internal Database] を選択します。

6. パスワードを入力します。管理者には、PAP/CHAPまたはMD5-CHAP認証を設定して、ACS内部データベースにユーザを追加するオプションがあります。PAPは、コントローラ上のWeb認証ユーザのための、デフォルトの認証タイプです。管理者は、次のCLIコマンドを使用して、認証方式をchap/md5-chapに柔軟に変更できます。

```
config custom-web radiusauth <auth method>
```

7. 「発行」をクリックします。

Cisco WLC への RADIUS サーバ情報の入力

次のステップを実行します。

1. 上部のメニューで [Security] をクリックします。
2. 左側のメニューで [RADIUS Authentication] をクリックします。
3. Newをクリックして、ACS/RADIUSサーバのIPアドレスを入力します。この例では、ACSサーバのIPアドレスは 10.77.244.196 です。
4. RADIUS サーバの共有秘密を入力します。この秘密鍵が、WLC の RADIUS サーバで入力した秘密鍵と同じであることを確認します。
5. ポート番号はデフォルトの 1812 のままにしておきます。
6. [Server Status] オプションが [Enabled] であることを確認します。
7. このRADIUSサーバをワイヤレスネットワークユーザの認証に使用するために、Network User Enableボックスにチェックマークを付けます。
8. [適用 (Apply)] をクリックします。

Security

AAA

- General
- RADIUS
 - Authentication
 - Accounting
 - Fallback
- TACACS+
- LDAP
- Local Net Users
- MAC Filtering
- Disabled Clients
- User Login Policies
- AP Policies
- Password Policies

Local EAP

Priority Order

Certificate

Access Control Lists

Wireless Protection Policies

Web Auth

Advanced

RADIUS Authentication Servers > New

Server Index (Priority) 1

Server IP Address 10.77.244.196

Shared Secret Format ASCII

Shared Secret

Confirm Shared Secret

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

Network User Enableボックス

Network User ボックスにチェックマークが付いていて、Admin Status がEnabledになっていることを確認します。

The screenshot shows the 'RADIUS Authentication Servers' configuration page. On the left is a navigation menu with 'Security' expanded to 'AAA' and 'RADIUS' selected. The main content area includes settings for 'Call Station ID Type' (set to 'IP Address'), 'Use AES Key Wrap' (unchecked), and 'MAC Delimiter' (set to 'Hyphen'). Below these is a table with columns: Network User, Management, Server Index, Server Address, Port, IPSec, and Admin Status. A single row is visible with 'Network User' checked, 'Management' checked, 'Server Index' 1, 'Server Address' 10.77.244.196, 'Port' 1812, 'IPSec' Disabled, and 'Admin Status' Enabled. A note at the bottom states: '1. Call Station ID Types will be applicable only for non 802.1x authentication only.'

Network Userボックスにチェックマークを入れて、Admin Statusを有効にします

RADIUSサーバを使用したWLANの設定

RADIUS サーバが WLC 上で設定されたので、この RADIUS サーバを Web 認証に使用するように WLAN を設定する必要があります。RADIUS サーバで WLAN を設定するには、次の手順を実行します。

1. WLC ブラウザを開き、[WLANs] をクリックします。これにより、WLC 上で設定されているすべての WLAN のリストが表示されます。Web 認証用に作成された WLAN のゲストをクリックします。
2. WLANs > Edit ページで、Security タブをクリックします。[Security] の下の [AAA Servers] タブをクリックします。次に、RADIUS サーバを選択します。この例では 10.77.244.196 です。

The screenshot shows the 'WLANs > Edit 'Guest'' configuration page. The 'Security' tab is selected, and the 'AAA Servers' sub-tab is active. It displays 'Radius Servers' configuration with 'Radius Server Overwrite interface' unchecked. Below, there are columns for 'Authentication Servers' and 'Accounting Servers'. 'Server 1' is configured with 'IP:10.77.244.196, Port:1812' for authentication and is checked as 'Enabled'. 'Server 2' and 'Server 3' are set to 'None'. To the right, 'LDAP Servers' are all set to 'None'. At the bottom, 'Local EAP Authentication' is unchecked.

Securityタブをクリックしてから、AAA Serversタブをクリックします

3. [APPLY] をクリックします。

ACS の確認

ACS を設定するときには、最新のパッチと最新のコードをすべて必ずダウンロードしてください。これにより、差し迫った問題を解決できます。RADIUS認証を使用する場合は、WLCがAAAクライアントの1つとしてリストされていることを確認します。これを確認するには、左側の [Network Configuration] メニューをクリックします。[AAA Client] をクリックし、設定されているパスワードと認証タイプを確認します。

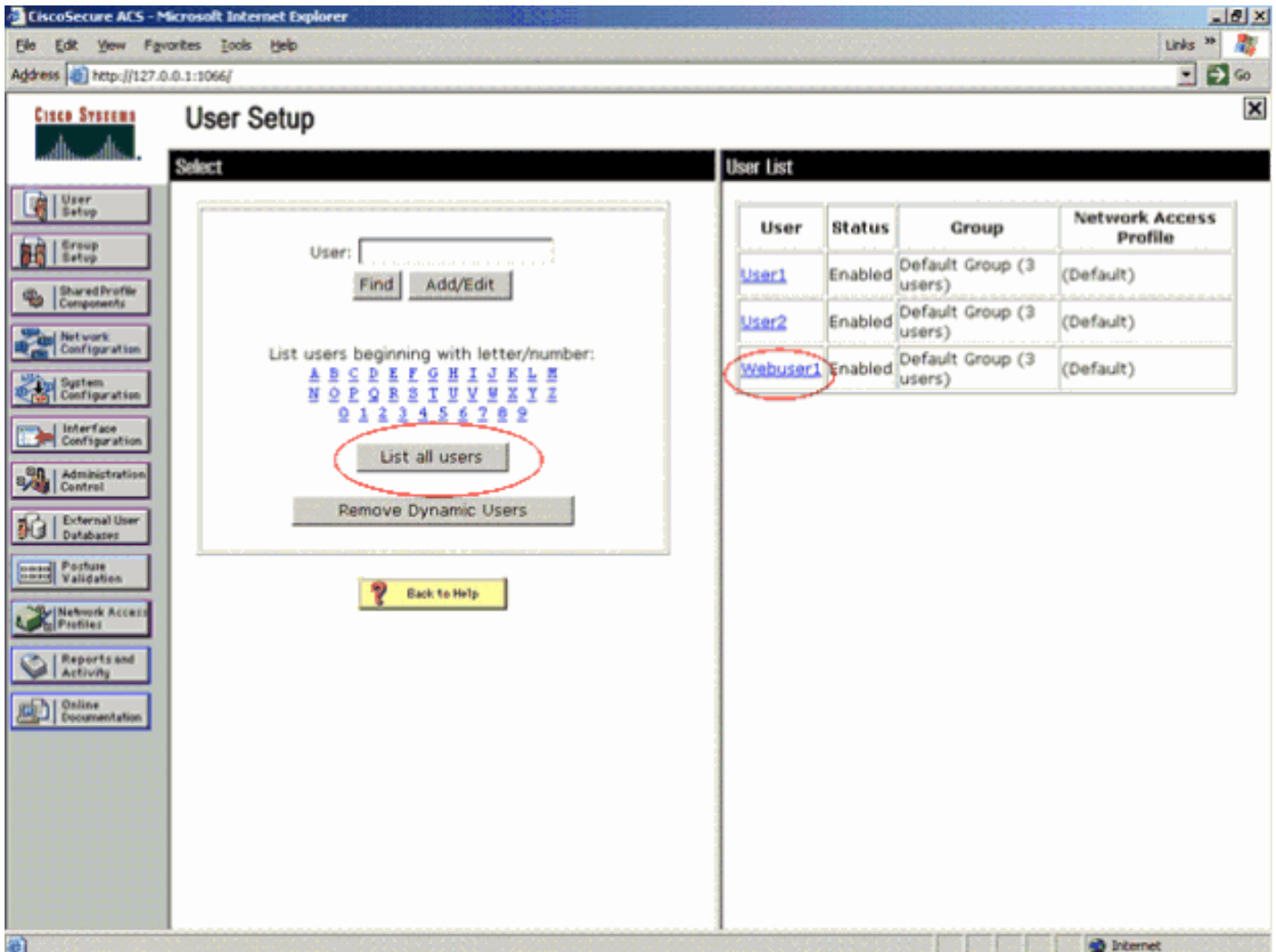
The screenshot shows the CiscoSecure ACS Network Configuration page. The main content area is divided into three sections:

- AAA Clients:** A table with columns: AAA Client Hostname, AAA Client IP Address, and Authenticate Using. It contains two entries: 'wlc' (IP: 10.77.244.204) and 'wlc210' (IP: 10.77.244.210), both using RADIUS (Cisco Airespace) authentication. The 'wlc' and its IP address are circled in red.
- AAA Servers:** A table with columns: AAA Server Name, AAA Server IP Address, and AAA Server Type. It contains one entry: 'ts-web' (IP: 10.77.244.196) of type CiscoSecure ACS.
- Proxy Distribution Table:** A table with columns: Character String, AAA Servers, Strip, and Account. It contains one entry: '(Default)' with 'ts-web' servers, 'No' strip, and 'Local' account.

The left sidebar contains a navigation menu with options like User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Posture Validation, Network Access Profiles, Reports and Activity, and Online Documentation. The right sidebar contains a Help panel with a list of links and a note about the page's content depending on the interface configuration.

WLCがAAAクライアントとしてリストされる

[User Setup] を選択したら、ユーザが実際に存在していることを再度確認します。[List All Users] をクリックします。次に示すウィンドウが表示されます。作成したユーザがリスト内にあることを確認します。



すべてのユーザーを一覧表示

LDAP サーバ

この項では、Lightweight Directory Access Protocol (LDAP) サーバを、RADIUS データベースやローカル ユーザ データベースに類似したバックエンド データベースとして設定する方法について説明します。LDAP バックエンド データベースでは、コントローラは、特定のユーザのクレデンシアル (ユーザ名とパスワード) について LDAP サーバに照会することができます。このクレデンシアルはユーザの認証に使用されます。

コントローラのGUIを使用してLDAPを設定するには、次の手順を実行します。

1. [Security] > [AAA] > [LDAP] をクリックして、LDAP サーバを開きます。

このページでは、これまでに設定されたすべての LDAP サーバが表示されます。

- 現在のLDAPサーバを削除する場合は、そのサーバの青いドロップダウン矢印の上にカーソルを移動し、Removeを選択します。
- コントローラが特定のサーバに到達できることを確認するには、そのサーバの青いドロップダウンの矢印の上にカーソルを置いて、[Ping] を選択します。

2. 次のいずれかのオプションを実行します。

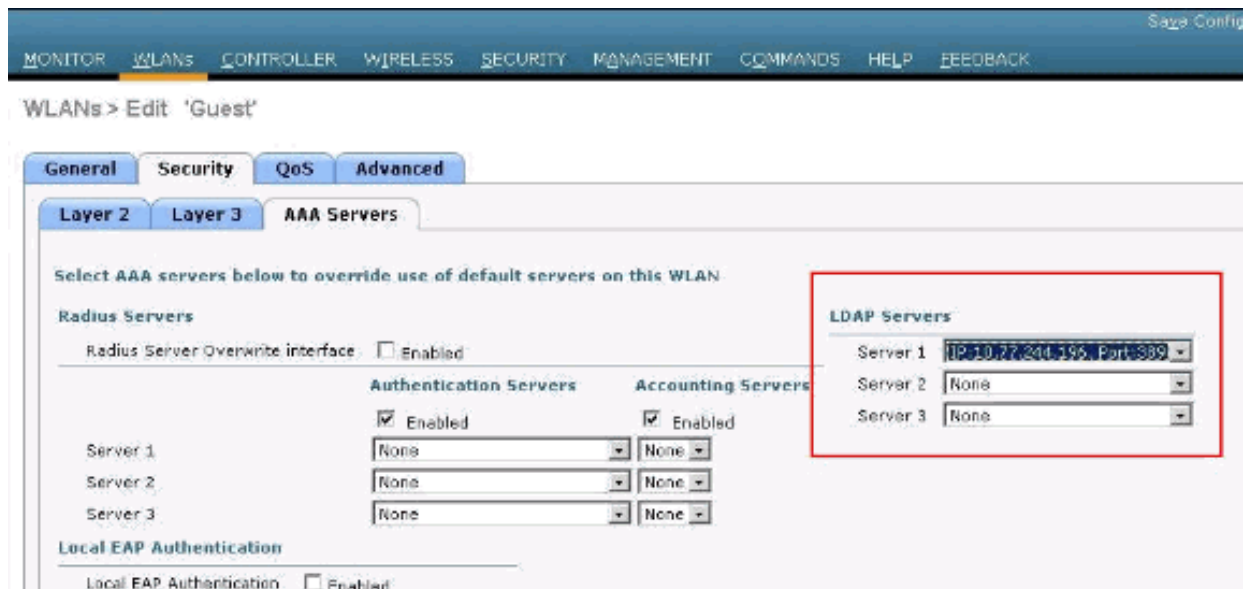
- 現在のLDAPサーバを編集するには、そのサーバのインデックス番号をクリックします。[LDAP Servers > Edit] ページが表示されます。
- LDAP サーバを追加するには、[New] をクリックします。[LDAP Servers > New] ページが表示されます。

Server Index (Priority)	1
Server IP Address	10.77.244.196
Port Number	389
Simple Bind	Authenticated
Bind Username	user2
Bind Password	*****
Confirm Bind Password	*****
User Base DN	ou=active,ou=employees,ou=people,o=cisco.com
User Attribute	uid
User Object Type	person
Server Timeout	2 seconds
Enable Server Status	Enabled

LDAPサーバの追加

3. 新しいサーバを追加する場合は、Server Index (Priority) ドロップダウンボックスから番号を選択して、他の設定済みLDAPサーバに対するこのサーバの優先順位を指定します。サーバは最大 17 個まで設定できます。コントローラが最初のサーバに接続できない場合、リストの 2 番目のサーバへの接続を試行する、というようになります。
4. 新しいサーバを追加する場合は、Server IP Address フィールドにLDAPサーバのIPアドレスを入力します。
5. 新しいサーバを追加する場合は、LDAPサーバのTCPポート番号をポート番号フィールドに入力します。有効な範囲は 1 ~ 65535 で、デフォルト値は 389 です。
6. Enable Server Status チェックボックスにチェックマークを入れてこのLDAPサーバを有効にするか、チェックマークを外して無効にします。デフォルト値は無効です。
7. [Simple Bind] ドロップダウン ボックスから、[Anonymous] または [Authenticated] を選択して、LDAP サーバ用のローカル認証バインド方式を指定します。匿名方式では LDAP サーバへの匿名アクセスが可能です。一方、認可方式ではユーザ名とパスワードを入力してアクセスをセキュリティで保護する必要があります。デフォルトでは [Anonymous] になっています。
8. 手順 7 で [Authenticated] を選択した場合は、次の手順に従ってください。

- a. [Bind Username] フィールドに、LDAP サーバに対するローカル認証に使用されるユーザ名を入力します。
 - b. [Bind Password] フィールドおよび [Confirm Bind Password] フィールドには、LDAP サーバに対するローカル認証で使用されるパスワードを入力します。
9. [User Base DN] フィールドに、すべてのユーザのリストを含む LDAP サーバ内のサブツリーの識別名 (DN) を入力します。たとえば、ou=organizational unit、.ou=next organizational unit、o=corporation.example のようになります。ユーザを含むツリーがベース DN である場合は、「o=corporation.example」または「dc=corporation, dc=com」と入力します。
 10. [User Attribute] フィールドに、ユーザ名を含むユーザレコード内の属性の名前を入力します。この属性はディレクトリサーバから取得できます。
 11. [User Object Type] フィールドに、対象のレコードをユーザとして特定する LDAP objectType 属性の値を入力します。多くの場合、ユーザレコードには objectType 属性の値が複数あり、そのうちのいくつかはユーザに固有であり、また、いくつかは他のオブジェクトタイプと共有されています。
 12. [Server Timeout] フィールドに、再送信の間隔 (秒数) を入力します。有効な範囲は 2 ~ 30 秒であり、デフォルト値は 2 秒です。
 13. [Apply] をクリックして、変更を確定します。
 14. [Save Configuration] をクリックして変更を保存します。
 15. 特定の LDAP サーバを WLAN に割り当てるには、次の手順を実行します。
 - a. ClickWLANs をクリックして、WLANs ページを開きます。
 - b. 必要な WLAN の ID 番号をクリックします。
 - c. [WLANs] > [Edit] ページが表示されたら [Security] > [AAA Servers] タブをクリックし、[WLANs] > [Edit] ([Security] > [AAA Servers]) ページを開きます。



Security > AAA Servers Tabsをクリックします

- d. [LDAP Servers] ドロップダウン ボックスから、この WLAN に使用する LDAP サーバを選択します。最大 3 台の LDAP サーバを選択できます。これらのサーバは優先順位に従って試行されます。
- e. [Apply] をクリックして、変更を確定します。
- f. [Save Configuration] をクリックして変更を保存します。

Web 認証を使用するための WLAN クライアントの設定

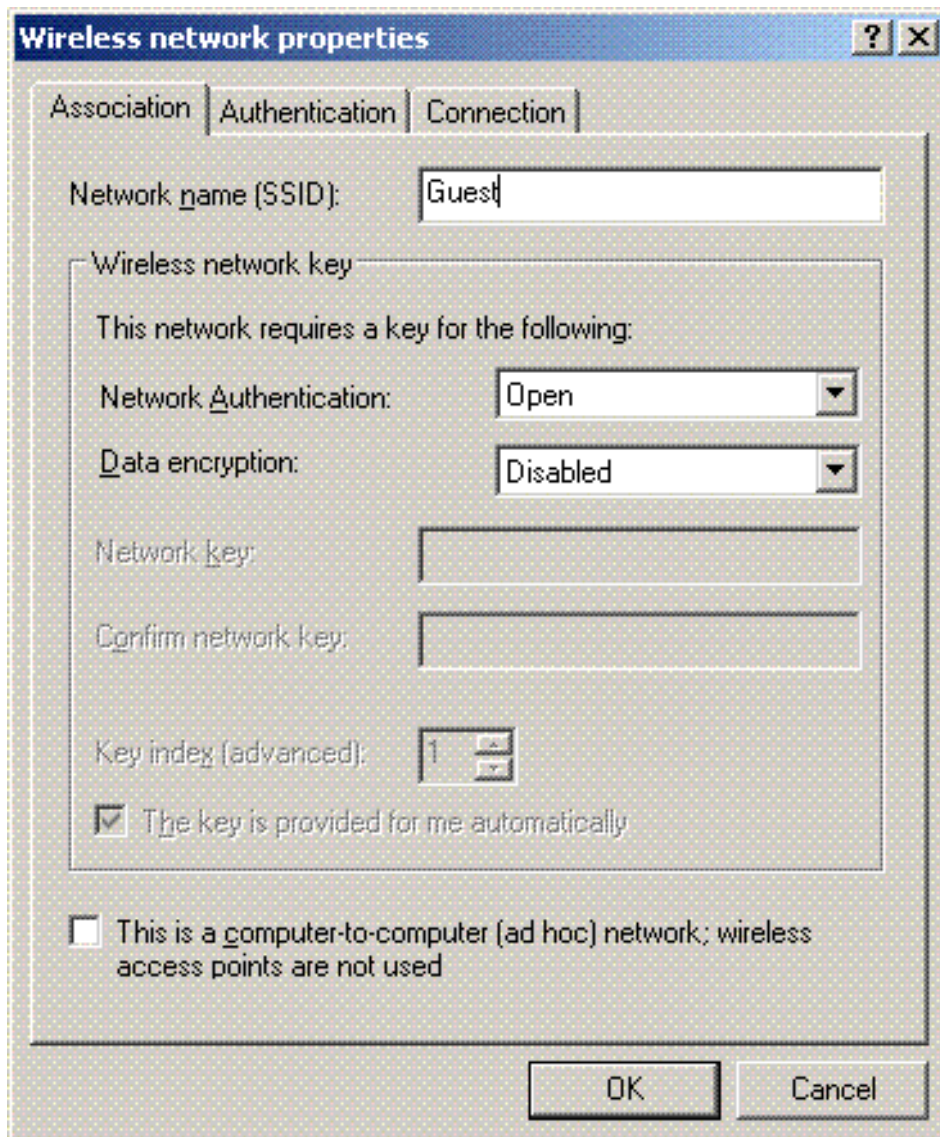
WLC を設定したら、クライアントは Web 認証用に正しく設定される必要があります。このセクションでは、Web 認証用に Windows システムを設定するための情報を提供します。

クライアントの設定

Microsoft ワイヤレス クライアントの設定は、このサブスクリバの場合はほとんど変更されません。適切な WLAN/SSID 設定情報を追加するだけで済みます。次のステップを実行します。


1. Windows の [Start] メニューから、[Settings] > [Control Panel] > [Network and Internet Connections] を選択します。
2. [Network Connections] アイコンをクリックします。
3. [LAN Connection] アイコンを右クリックして、[Disable] を選択します。
4. [Wireless Connection] アイコンを右クリックして、[Enable] を選択します。
5. [Wireless Connection] アイコンを再度右クリックして、[Properties] を選択します。
6. [Wireless Network Connection Properties] ウィンドウから、[Wireless Networks] をクリックします。

7. 推奨されるネットワーク エリアの下で、[Add] をクリックして、Web 認証 SSID を設定します。
8. [Association] タブの下で、Web 認証に使用するネットワーク名 (WLAN/SSID) の値を入力します。



The screenshot shows the 'Wireless network properties' dialog box with the 'Association' tab selected. The 'Network name (SSID)' field is filled with 'Guest'. Under the 'Wireless network key' section, 'Network Authentication' is set to 'Open' and 'Data encryption' is set to 'Disabled'. The 'Network key' and 'Confirm network key' fields are empty. The 'Key index (advanced)' is set to 1. The checkbox 'The key is provided for me automatically' is checked. The checkbox 'This is a computer-to-computer (ad hoc) network; wireless access points are not used' is unchecked. The 'OK' and 'Cancel' buttons are at the bottom.

Associationタブでネットワーク名を入力します。

 注：デフォルトでは、Data EncryptionはWired Equivalent Privacy(WEP)です。Web認証が機能するように、データ暗号化を無効にします。


9. ウィンドウの下部にある [OK] をクリックして、設定を保存します。


WLAN と通信する場合は、[Preferred Network] ボックスにビーコン アイコンが表示されます。


これは Web 認証とのワイヤレス接続が正常であることを示します。WLC は、ワイヤレス Windows クライアントに IP アドレスを提供済みです。




WLCが提供するIPアドレス

 注：ワイヤレスクライアントがVPNエンドポイントでもあり、Web認証をWLAN用のセキュリティ機能として設定している場合、ここで説明されているWeb認証プロセスが完了するまで、VPNトンネルは確立されません。VPNトンネルを確立するには、クライアントはまずWeb認証のプロセスを正常に完了する必要があります。その場合にのみ、VPNトンネルは成功します。

 注：ログインに成功した後、ワイヤレスクライアントがアイドル状態で他のデバイスと通信しない場合、クライアントはアイドルタイムアウト期間の後に認証を解除されます。タイムアウト時間はデフォルトで300秒であり、CLIコマンド `config network usertimeout`

 <seconds>で変更できます。タイムアウトになると、クライアント エントリはコントローラから削除されます。クライアントは、再度関連付けられると、Webauth_Reqd状態に戻ることができます。

 注：ログインに成功した後、クライアントがアクティブである場合は、そのWLANに設定されたセッションタイムアウト期間(たとえば、デフォルトでは1800秒ですが、CLIコマンド `config wlan session-timeout <WLAN ID> <seconds>`を使用して変更できます)が経過した後も、クライアントは認証を解除してコントローラからエントリを削除できます。タイムアウトになると、クライアント エントリはコントローラから削除されます。クライアントは、再度関連付けられると、Webauth_Reqd状態に戻ります。

クライアントがWebauth_Reqd状態の場合、クライアントがアクティブかアイドルかに関係なく、web-auth required timeout期間(たとえば、300秒で、この時間はユーザが設定できないなど)の後にクライアントの認証が解除される場合があります。クライアントからのすべてのトラフィック(事前認証ACLを介して許可される)が中断されます。クライアントは、再度関連付けられると、Webauth_Reqd状態に戻ります。

クライアントログイン

次のステップを実行します。

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、ユーザはWeb認証ページを表示するために<https://10.1.1.1/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. [Yes]をクリックして次に進みます。
3. [Login] ウィンドウが表示されたら、作成したローカル ネット ユーザのユーザ名とパスワードを入力します。

Login

Welcome to the Cisco wireless network

Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your unified wireless solution to work.

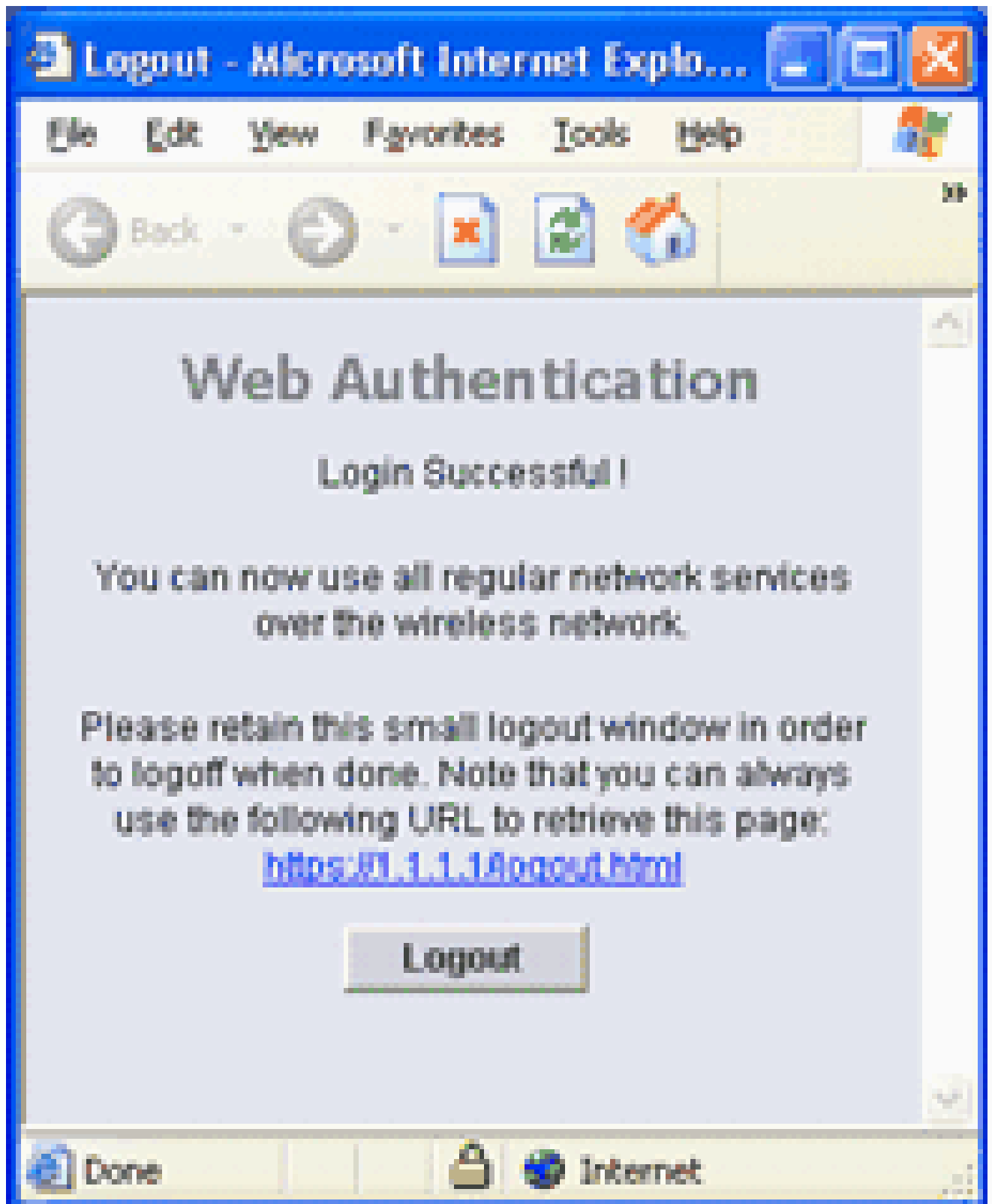
User Name	<input type="text" value="User1"/>
Password	<input type="password" value="*****"/>
	<input type="submit" value="Submit"/>

ログインウィンドウ

ログインに成功すると、2つのブラウザウィンドウが表示されます。大きい方のウィンドウはログインに成功したことを示し、このウィンドウを使用して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。

上の図は、Web認証のリダイレクトが成功した状態を示しています。

次の図は、認証が発生すると表示されるLogin Successfulウィンドウを示しています。



ログイン成功！

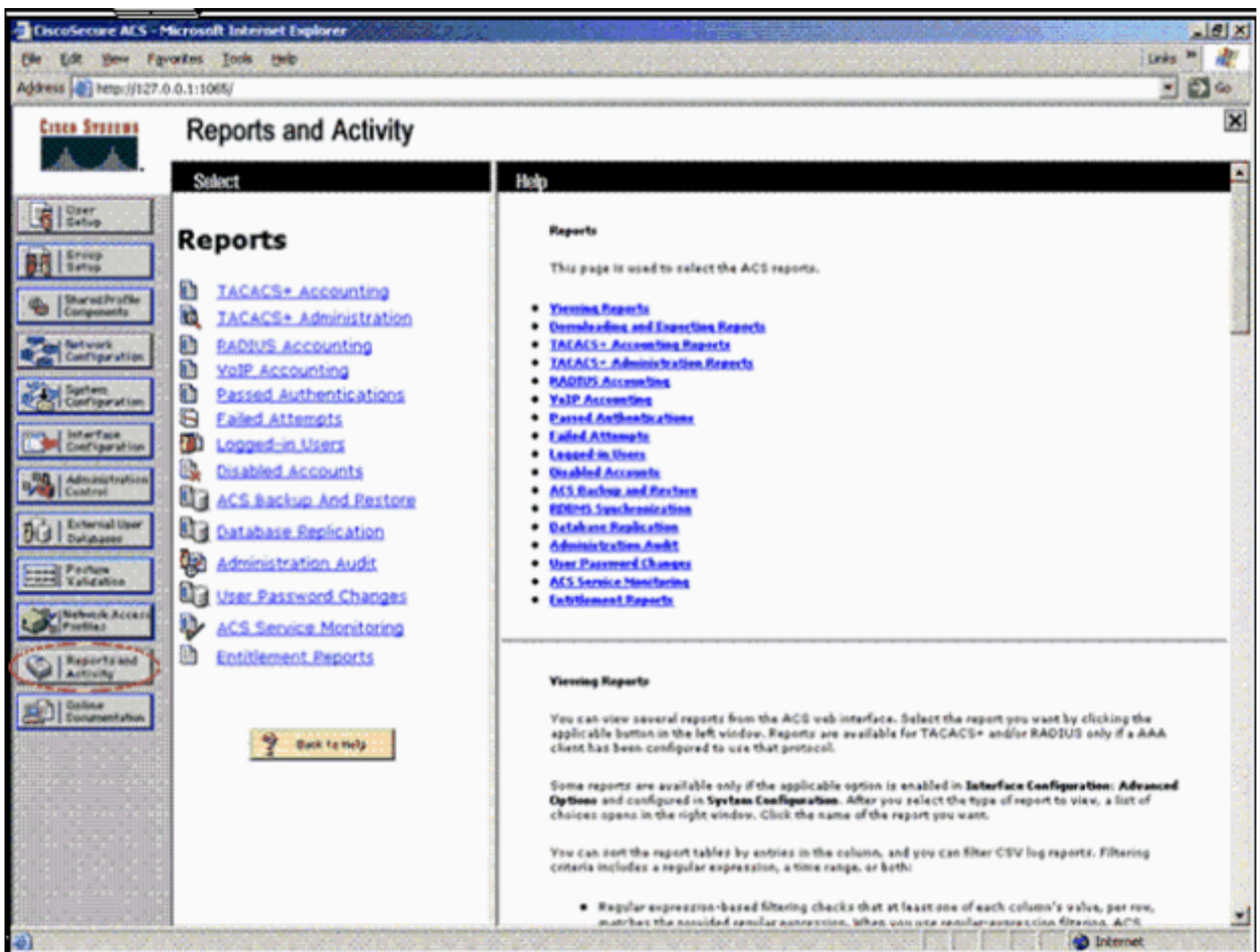
Cisco 4404/WiSMコントローラは、125の同時Web認証ユーザログインをサポートし、最大5000のWeb認証クライアントまで拡張できます。

Cisco 5500コントローラは、150の同時Web Authユーザログインをサポートできます。


Web 認証のトラブルシューティング

ACS のトラブルシューティング

パスワード認証で問題が発生する場合は、ACS の 左下にある [Reports and Activity] をクリックして、使用可能なすべてのレポートを開きます。レポートウィンドウを開いた後で、RADIUS Accounting、Failed Attempts for log in、Passed Authentications、Logged-in Users、およびその他のレポートを開くオプションがあります。これらのレポートは .csv ファイルであり、ご使用のマシン上でローカルに開くことができます。レポートは、認証の問題（ユーザ名やパスワードの誤りなど）を検出するために役立ちます。ACS には、オンラインドキュメントが付属しています。ライブネットワークに接続しておらず、サービスポートを定義していない場合、ACS はサービスポートにイーサネットポートの IP アドレスを使用します。ネットワークに接続していない場合、たいていは Windows 169.254.x.x のデフォルト IP アドレスを使用することになります。



レポートとアクティビティウィンドウ

 注：外部URLを入力すると、WLCによって内部Web認証ページに自動的に接続されます。自動接続が機能しない場合には、URL バーで WLC の管理 IP アドレスを入力するとトラブルシューティングができます。ブラウザの上部で Web 認証のリダイレクトについて通知するメッセージを確認します。

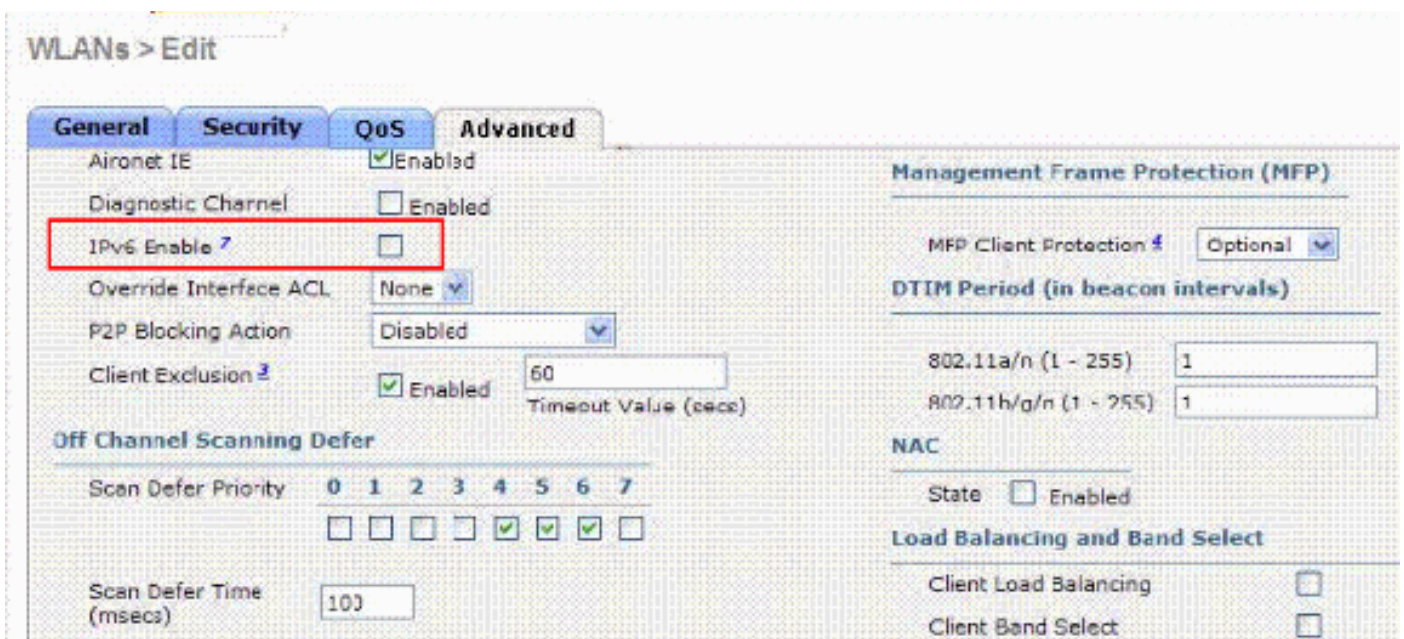
Web認証のトラブルシューティングの詳細については、『[ワイヤレスLANコントローラ\(WLC\)で](#)

[のWeb認証のトラブルシューティング』](#)を参照してください。

IPv6ブリッジングでのWeb認証

WLANをIPv6ブリッジング用に設定するには、コントローラGUIから[WLANs]に移動します。次に、目的のWLANを選択し、[WLANs]>[Edit]ページから[Advanced]を選択します。

このWLANに接続するクライアントがIPv6パケットを受け入れることができるようにするには、IPv6 Enableチェックボックスをオンにします。それ以外の場合、このチェックボックスはオフ(デフォルト値)のままにしておきます。IPv6チェックボックスを無効にする(またはオフにする)と、IPv6は認証後にのみ許可されます。IPv6を有効にすると、コントローラはクライアント認証なしでIPv6トラフィックを渡せるようになります。



目的のWLANを選択し、Advancedを選択します

関連情報

- [WLCを使用した外部Web認証の設定](#)
- [ワイヤレスLANコントローラ\(WLC\)でのWeb認証のトラブルシューティング](#)
- [Cisco ワイヤレス LAN](#)
- [Cisco WLANコントローラを使用した有線ゲストアクセスの設定例](#)
- [CiscoワイヤレスLANコントローラの廃止に関する通知](#)
- [RADIUSサーバを介したワイヤレスLANコントローラのロビー管理者の認証](#)
- [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。