CHAPTER 9

ユーザ アカウントの管理

この章では、ゲスト ユーザ アカウントの作成および管理方法、Web 認証プロセス、および、Web 認証ログイン ウィンドウのカスタマイズ手順について説明します。この章の内容は、次のとおりです。

ゲスト ユーザ アカウントの作成

コントローラは、WLAN 上でゲスト ユーザ アクセスを提供できます。ゲスト ユーザ アカウント作成の最初の手順では、ロビー アンバサダー アカウントとしても知られる、ロビー管理者アカウントを作成します。このアカウントを作成すると、ロビー アンバサダーはゲスト ユーザ アカウントをコントローラ上で作成および管理できます。ロビー アンバサダーは、ゲスト アカウントを管理するために使用する Web ページのみの設定権限やアクセスを制限します。

ロビー アンバサダーは、ゲスト ユーザ アカウントを利用できる時間を指定できます。指定した時間を経過すると、ゲスト ユーザ アカウントは、自動的に無効になります。

ローカル ユーザ データベースは、最大エントリ数が 2048 に制限され、デフォルト値は、512 エントリです（Security > General ページ）。データベースは、ローカル管理ユーザ（ロビー アンバサダーを含む）、ネット ユーザ（ゲスト ユーザを含む）、MAC フィルタ エントリ、および無効になったクライアントで共有します。これらを合わせて、設定済みのデータベース容量を超えることはできません。

ロビー アンバサダー アカウントの作成

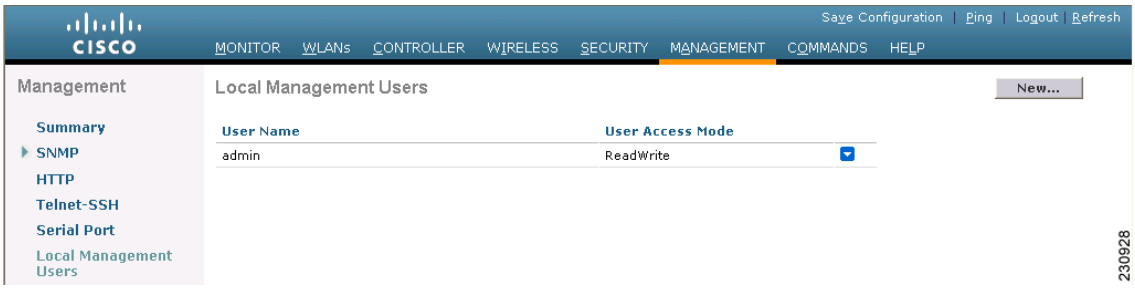
GUI または CLI を使用して、コントロール上にロビー アンバサダー アカウントを作成することができます。

GUI を使用したロビー アンバサダー アカウントの作成

コントローラ GUI を使用してロビー アンバサダー アカウントを作成する手順は、次のとおりです。

ステップ 1　**Management** > **Local Management Users** をクリックして、Local Management Users ページにアクセスします（図 9-1 を参照）。

図 9-1　Local Management Users ページ

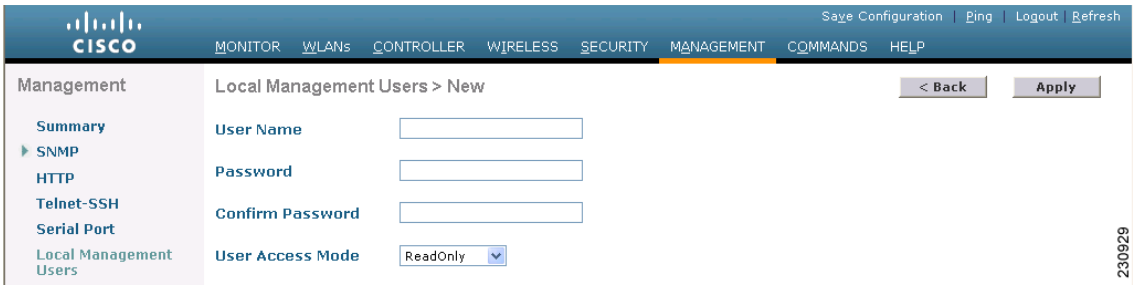


このページは、ローカル管理ユーザの名前やアクセス権限の一覧表示です。

（注）　コントローラから任意のユーザ アカウントを削除するには、青いドロップダウンの矢印の上にカーソルを置いて、**Remove** を選択します。ただし、デフォルトの管理ユーザを削除すると、GUI および CLI によるコントローラへのアクセスは両方とも禁止されます。したがって、デフォルトのユーザを削除する前に、管理権限（ReadWrite）を持つユーザを作成しなければなりません。

ステップ 2　ロビー アンバサダー アカウントを作成するには、**New** をクリックします。Local Management Users > New ページが表示されます（図 9-2 を参照）。

図 9-2　Local Management Users > New ページ



ステップ 3　User Name フィールドに、ロビー アンバサダー アカウントのユーザ名を入力します。

（注）　管理ユーザ名は、すべて単一データベース内に保存されるため、一意である必要があります。

ステップ 4　Password フィールドおよび Confirm Password フィールドに、ロビー アンバサダー アカウントのパスワードを入力します。

（注）　パスワードは大文字と小文字が区別されます。

ステップ 5　User Access Mode ドロップダウン ボックスから **LobbyAdmin** を選択します。このオプションを使用すると、ロビー アンバサダーでゲスト ユーザ アカウントを生成できます。

（注）　**ReadOnly** オプションでは、読み取り専用の権限を持つアカウントを作成し、**ReadWrite** オプションでは、読み取りと書き込みの両方の権限を持つ管理アカウントを作成します。

ステップ 6　**Apply** をクリックして、変更を適用します。ローカル管理ユーザのリストに、新しいロビー アンバサダー アカウントが表示されます。

ステップ 7　**Save Configuration** をクリックして、変更内容を保存します。

CLI を使用したロビー アンバサダー アカウントの作成

コントローラ CLI を使用してロビー アンバサダー アカウントを作成するには、以下のコマンドを入力します。

config mgmtuser add < ロビー管理者ユーザ名 > < ロビー管理者パスワード > **lobby-admin**

（注）　**lobby-admin** を **read-only** に置き換えると、読み取り専用の権限を持つアカウントを作成します。**lobby-admin** を **read-write** に置き換えると、読み取りと書き込みの両方の権限を持つ管理アカウントを作成します。

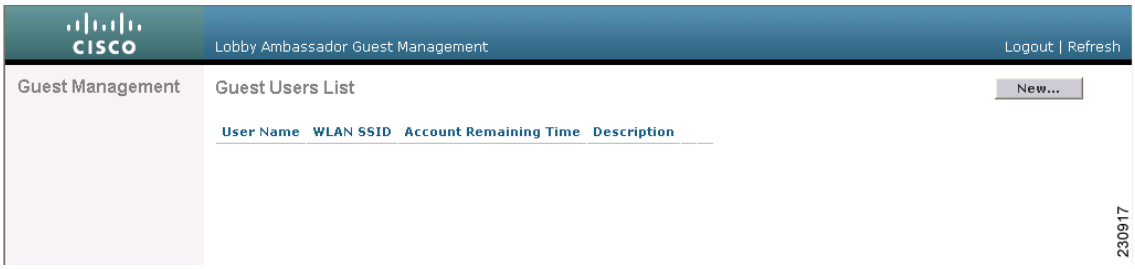
ロビー アンバサダーとしてのゲスト ユーザ アカウントの作成

ロビー アンバサダーは、次の手順に従ってゲスト ユーザ アカウントを作成します。

（注）　ロビー アンバサダーは、コントローラの CLI インタフェースにアクセスできないため、コントローラの GUI からのみゲスト ユーザ アカウントを作成できます。

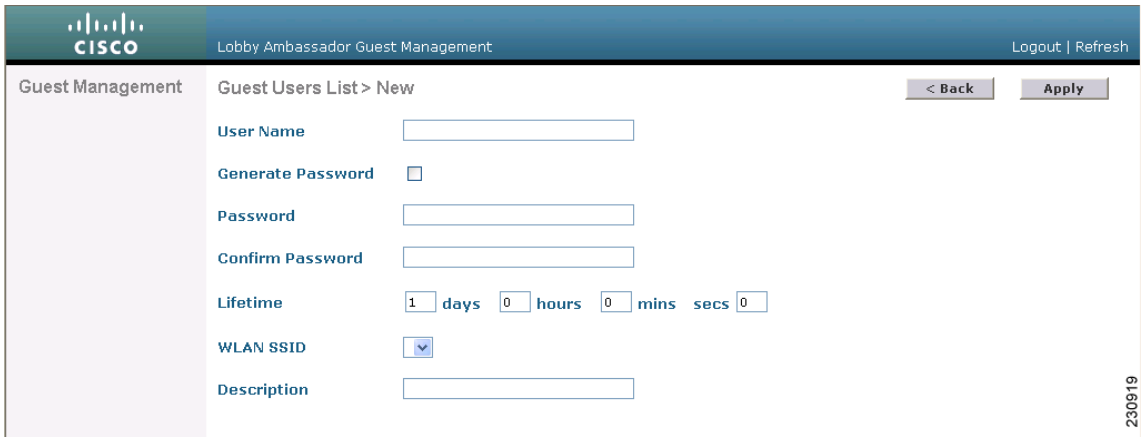
ステップ 1　上記の「ロビー アンバサダー アカウントの作成」の項で指定されたユーザ名およびパスワードを使用して、ロビー アンバサダーとしてコントローラにログインします。Lobby Ambassador Guest Management > Guest Users List ページが表示されます（図 9-3 を参照）。

図 9-3　Lobby Ambassador Guest Management > Guest Users List ページ



ステップ 2　**New** をクリックして、ゲスト ユーザ アカウントを作成します。Lobby Ambassador Guest Management > Guest Users List > New ページが表示されます（図 9-4 を参照）。

図 9-4　Lobby Ambassador Guest Management > Guest Users List > New ページ



ステップ 3　User Name フィールドに、ゲスト ユーザの名前を入力します。最大 24 文字を入力することができます。

ステップ 4　次のいずれかの操作を行います。

- このゲスト　ユーザ用のパスワードを自動的に生成する場合は、**Generate Password** チェック ボックスを選択します。生成されたパスワードは、Password フィールドおよび Confirm Password フィールドに自動的に入力されます。
- このゲスト ユーザ用にパスワードを作成する場合は、**Generate Password** チェック ボックスを選択せずに、Password フィールドおよび Confirm Password フィールドの両方にパスワードを入力します。

（注）　パスワードは最大 24 文字まで含めることができ、大文字と小文字が区別されます。

ステップ 5　Lifetime ドロップダウン ボックスから、このゲスト ユーザ アカウントをアクティブにする時間（日数、時間数、分数、秒数）を選択します。4 つのフィールド値をすべてゼロ（0）にすると、永久アカウントとなります。

デフォルト：1 日

範囲：5 分から 30 日

（注）　小さい方の値、またはゲスト アカウントが作成された WLAN であるゲスト WLAN のセッション タイムアウトが、優先します。たとえば、WLAN セッションのタイムアウトが 30 分でも、ゲスト アカウントのライフタイムが 10 分の場合、アカウントはゲスト アカウントの失効に従い、10 分で削除されます。同様に、WLAN セッションがゲスト アカウントのライフタイムより前にタイムアウトする場合、クライアントは、再認証を要求するセッション タイムアウトを繰り返すことになります。

（注）　ゼロ以外の値がライフタイムに設定されているゲスト ユーザ アカウントの値は、アカウントがアクティブになっている間、いつでも別の値に変更できます。しかし、ゲスト ユーザ アカウントを永久アカウントにするため、または、永久アカウントをゲスト アカウントにするためには、そのアカウントを削除してから再度アカウントを作成しなければなりません。

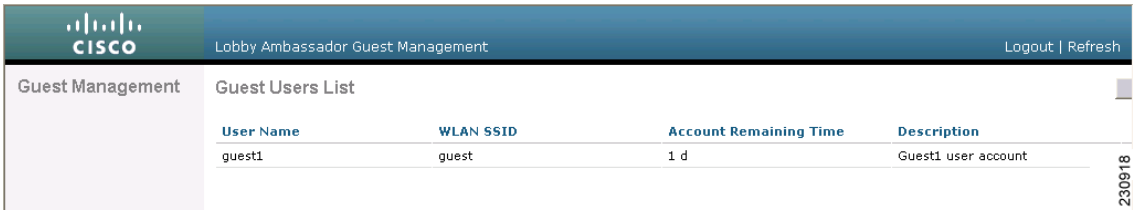
ステップ 6　WLAN SSID ドロップダウン ボックスから、ゲスト ユーザが使用する SSID を選択します。リストアップされた WLAN のみにレイヤ 3 の Web 認証が設定されています。

（注）　潜在的な競合を阻止するために、システム管理者が特定のゲスト WLAN を作成することをお勧めします。ゲスト アカウントの有効期限が切れ、RADIUS サーバ上でアカウント名が競合し、両アカウントとも同じ WLAN 上にある場合、両アカウントにアソシエートしているユーザのアソシエートが解除されてから、ゲスト アカウントが削除されます。

ステップ 7　Description フィールドに、ゲスト ユーザ アカウントの説明を入力します。最大 32 文字を入力することができます。

ステップ 8　**Apply** をクリックして、変更を適用します。新しいゲスト ユーザ アカウントが、Guest Users List ページのゲスト ユーザ リストに表示されます（図 9-5 を参照）。

図 9-5　Lobby Ambassador Guest Management > Guest Users List ページ



このページから、すべてのゲスト ユーザ アカウント、それぞれの WLAN SSID およびライフタイムを表示できます。また、ゲスト ユーザ アカウントを編集、または削除することができます。ゲスト ユーザ アカウントを削除する場合、ゲスト WLAN を使用し、そのアカウントのユーザ名を使用してログインしているクライアントはすべて削除されます。

ステップ 9　新しいゲスト ユーザ アカウントを作成するには、この手順を繰り返します。

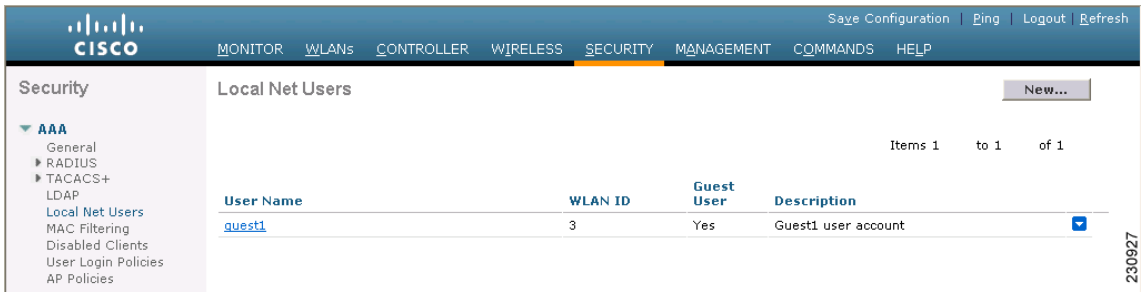
ゲスト ユーザ アカウントの表示

ロビー アンバサダーがゲスト ユーザ アカウントを作成後、システム管理者は、コントローラの GUI または CLI からそれらのアカウントを表示できます。

GUI を使用したゲスト アカウントの表示

コントローラ GUI を使用してゲスト ユーザ アカウントを表示するには、**Security** > **AAA** > **Local Net Users** をクリックします。Local Net Users ページが表示されます（図 9-6 を参照）。

図 9-6　Local Net Users ページ



このページから、システム管理者はすべてのローカル ネット ユーザ アカウント（ゲストユーザアカウントを含む）を表示し、必要に応じて編集または削除することができます。ゲスト ユーザ アカウントを削除する場合、ゲスト WLAN を使用し、そのアカウントのユーザ名を使用してログインしているクライアントはすべて削除されます。

CLI を使用したゲスト アカウントの表示

コントローラ CLI を使用して、すべてのローカル ネット ユーザ アカウント（ゲスト ユーザ アカウントを含む）を表示するには、次のコマンドを入力します。

show netuser summary

Web 認証プロセス

Web 認証は、レイヤ 3 セキュリティ機能です。これにより、コントローラは、クライアントが有効なユーザ名およびパスワードを正しく提供しない限り、そのクライアントに対する IP トラフィック（DHCP 関連パケットを除く）を許可しません。Web 認証を使用してクライアントを認証する場合、各クライアントのユーザ名とパスワードを定義する必要があります。クライアントは、無線 LAN に接続する際に、ログイン画面の指示に従ってユーザ名とパスワードを入力する必要があります。

Web 認証が（レイヤ 3 セキュリティ下で）有効になっている場合、ユーザが、最初にある URL にアクセスしようとした際に、Web ブラウザにセキュリティ警告が表示されることがあります。図 9-7 は一般的なセキュリティ警告を示しています。

図 9-7　一般的な Web ブラウザ セキュリティ警告ウィンドウ

ユーザが **Yes** をクリックして続行した後、（または、クライアントのブラウザにセキュリティ警告が表示されない場合）、Web 認証システムのログイン画面が表示されます（図 9-8 を参照）。

セキュリティ警告が表示されないようにするために、次の手順を実行できます。

ステップ 1　Security Alert ウィンドウで **View Certificate** をクリックします。

ステップ 2　**Install Certificate** をクリックします。

ステップ 3　Certificate Import Wizard が表示されたら、**New** をクリックします。

ステップ 4　**Place all certificates in the following store** を選択して、**Browse** をクリックします。

ステップ 5　Select Certificate Store ウィンドウの下部で、**Show Physical Stores** チェック ボックスをオンにします。

ステップ 6　**Trusted Root Certification Authorities** フォルダを展開して、**Local Computer** を選択します。

ステップ 7　**OK** をクリックします。

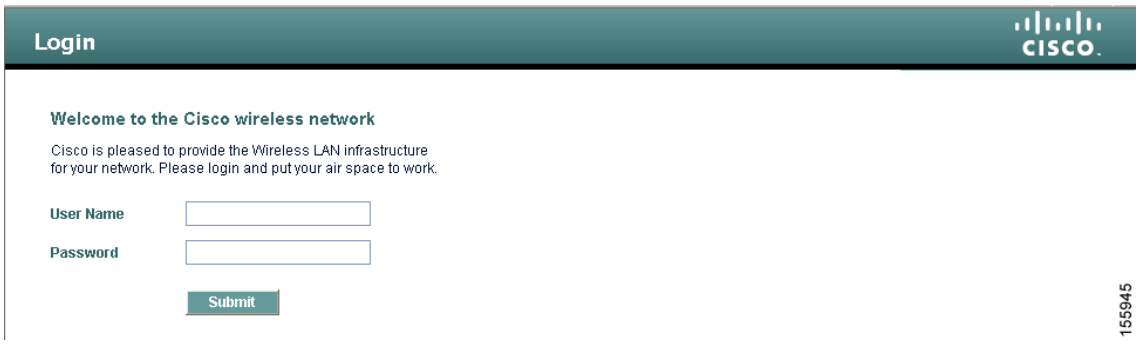
ステップ 8　**Next** > **Finish** の順にクリックします。

ステップ 9　"The import was successful" というメッセージが表示されたら、**OK** をクリックします。

ステップ 10　コントローラの自己署名証明書の issuer フィールドは空白であるため、Internet Explorer を開いて、**Tools** > **Internet Options** > **Advanced** の順にクリックし、Security の下の **Warn about Invalid Site Certificates** チェック ボックスをオフにして、**OK** をクリックします。

ステップ 11　PC をリブートします。次回 Web 認証を試みると、ログイン ウィンドウが表示されます（図 9-8 を参照）。

図 9-8　デフォルト Web 認証ログイン ウィンドウ



デフォルトのログイン ウィンドウには、Cisco ロゴや Cisco 特有のテキストが表示されます。Web 認証システムが次のいずれかを表示するように選択できます。

- デフォルトのログイン ウィンドウ
- デフォルトのログイン ウィンドウの変更バージョン
- 外部の Web サーバに設定する、カスタマイズされたログイン ウィンドウ
- 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

「Web 認証ログイン ウィンドウの選択」の項（P. 9-11）には、Web 認証ログイン ウィンドウの表示方法を選択する手順が記載されています。

ユーザが、Web 認証ログイン ウィンドウで有効なユーザ名とパスワードを入力し、**Submit** をクリックすると、Web 認証システムは、ログインに成功したことを示すウィンドウを表示し、認証されたクライアントは要求した URL にリダイレクトされます。図 9-9 は一般的なログイン成功ウィンドウを示します。

図 9-9　ログイン成功ウィンドウ

デフォルトのログイン成功ウィンドウには、仮想ゲートウェイ アドレスの URL（https://1.1.1.1/logout.html）が表示されます。コントローラの仮想インターフェイスに設定した IP アドレスは、ログイン ウィンドウのリダイレクト アドレスとして機能します（仮想インターフェイスの詳細は、第 3 章を参照）。

Web 認証ログイン ウィンドウの選択

この項では、Web 認証ログイン ウィンドウの内容および外観を指定するための手順を説明します。いずれかの項の手順に従って、コントローラ GUI または CLI を使用して Web 認証ログイン ウィンドウを選択します。

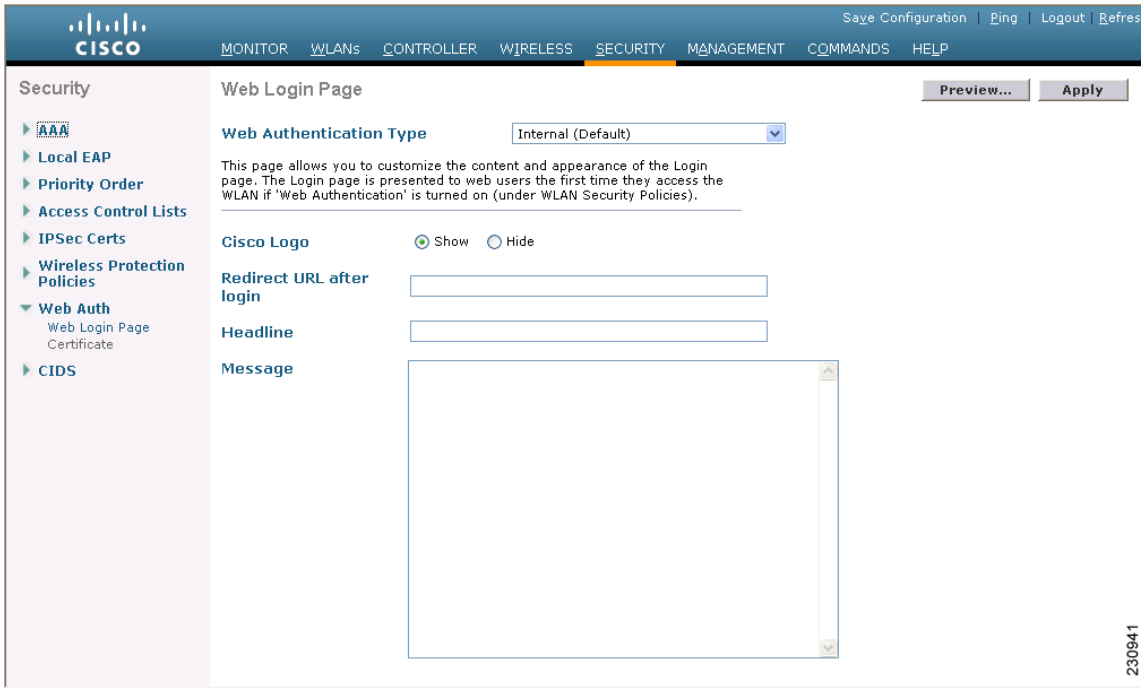
デフォルト Web 認証ログイン ウィンドウの選択

デフォルトの Web 認証ログイン ウィンドウをそのまま使用する場合（図 9-8 を参照）、または、多少変更を加えて使用する場合、次の GUI または CLI 手順の指示に従ってください。

GUI を使用したデフォルト Web 認証ログイン ウィンドウの選択

ステップ 1　**Security** > **Web Auth** > **Web Login Page** をクリックして、Web ログイン ページにアクセスします（図 9-10 を参照）。

図 9-10　Web ログイン ページ



ステップ 2　Web Authentication Type ドロップダウン ボックスから **Internal (Default)** を選択します。

ステップ 3　デフォルトの Web 認証ログイン ウィンドウをそのまま使用する場合、ステップ 8 に進みます。デフォルトのログイン ウィンドウを変更する場合、ステップ 4 に進みます。

ステップ 4　デフォルト ウィンドウの右上に表示されている Cisco ロゴを非表示にする場合、Cisco Logo **Hide** オプションを選択します。それ以外の場合は、**Show** オプションをクリックします。

ステップ 5　ユーザをログイン後に特定の URL（会社の URL など）にダイレクトさせる場合、Redirect URL After Login フィールドに必要な URL（www.AcompanyBC.com など）を入力します。最大 254 文字を入力することができます。

ステップ 6　ログイン ウィンドウで独自のヘッドラインを作成する場合、Headline フィールドに必要なテキストを入力します。最大 127 文字を入力することができます。デフォルトのヘッドラインは、「Welcome to the Cisco wireless network.」です。

ステップ 7　ログイン ウィンドウで独自のメッセージを作成する場合、Message フィールドに必要なテキストを入力します。最大 2047 文字を入力することができます。デフォルトのメッセージは、「Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your air space to work.」です。

ステップ 8　**Apply** をクリックして、変更を適用します。

ステップ 9　**Preview** をクリックして、Web 認証ログイン ウィンドウを表示します。

ステップ 10　ログイン ウィンドウの内容と外観に満足したら、**Save Configuration** をクリックして変更を保存します。納得いかない場合は、納得する結果を得られるように必要に応じて上記手順を繰り返します。

CLI を使用したデフォルトの Web 認証ログイン ウィンドウの選択

ステップ 1　デフォルトの Web 認証タイプを指定するには、次のコマンドを入力します。

config custom-web webauth_type internal

ステップ 2　デフォルトの Web 認証ログイン ウィンドウをそのまま使用する場合、ステップ 7 に進みます。デフォルトのログイン ウィンドウを変更する場合、ステップ 3 に進みます。

ステップ 3　デフォルトのログイン ウィンドウの右上に表示されている Cisco ロゴの表示 / 非表示を切り替えるには、次のコマンドを入力します。

config custom-web weblogo {**enable** | **disable**}

ステップ 4　ユーザをログイン後に特定の URL （会社の URL など）にダイレクトさせる場合、次のコマンドを入力します。

config custom-web redirecturl *url*

URL には最大 130 文字を入力することができます。リダイレクト先をデフォルトの設定に戻すには、**clear redirecturl** と入力します。

ステップ 5　ログイン ウィンドウで独自のヘッドラインを作成する場合、次のコマンドを入力します。

config custom-web webtitle < タイトル >

最大 130 文字を入力することができます。デフォルトのヘッドラインは、「Welcome to the Cisco wireless network.」です。ヘッドラインをデフォルトの設定に戻すには、**clear webtitle** と入力します。

ステップ 6　ログイン ウィンドウで独自のヘッドラインを作成する場合、次のコマンドを入力します。

config custom-web webmessage < メッセージ >

最大 130 文字を入力することができます。デフォルトのメッセージは、「Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your air space to work.」です。メッセージをデフォルトの設定に戻すには、**clear webmessage** と入力します。

ステップ 7　**save config** と入力して、設定を保存します。

ステップ 8　独自のロゴを Web 認証ログイン ウィンドウにインポートする場合、次の手順に従ってください。

a. Trivial File Transfer Protocol（TFTP）サーバがダウンロードのために使用可能であることを確認します。TFTP サーバをセットアップする際の注意事項は次のとおりです。

- サービス ポート経由でダウンロードする場合、サービス ポートはルーティングできないため、TFTP サーバはサービス ポートと同じサブネット上になければなりません。
- ディストリビューション システム ネットワーク ポートを経由してダウンロードする場合、ディストリビューション システム ポートはルーティング可能なので、TFTP サーバは同じサブネット上にあっても、別のサブネット上にあってもかまいません。
- サードパーティの TFTP サーバと WCS 内蔵型 TFTP サーバは同じ通信ポートを使用するため、サードパーティの TFTP サーバは Cisco WCS と同じコンピュータ上で実行できません。

b. **ping ip-address** を入力して、コントローラが TFTP サーバと通信可能であることを確認します。

c. TFTP サーバのデフォルト ディレクトリにロゴ ファイル（.jpg、.gif、または .png 形式）を移動します。ファイル サイズは 30KB 以内です。うまく収まるようにするには、ロゴは、横 180 ピクセル X 縦 360 ピクセル前後の大きさにします。

d. ダウンロード モードを指定するには、**transfer download mode tftp** と入力します。

e. ダウンロードするファイルのタイプを指定するには、**transfer download datatype image** と入力します。

f. TFTP サーバの IP アドレスを指定するには、**transfer download serverip** *tftp-server-ip-address* と入力します。

（注）　TFTP サーバによっては、TFTP サーバ IP アドレスにスラッシュ（/）を入力するだけで、自動的に適切なディレクトリへのパスが判別されるものもあります。

g. ダウンロード パスを指定するには、**transfer download path** *absolute-tftp-server-path-to-file* と入力します。

h. ダウンロードするファイルを指定するには、**transfer download filename** {*filename.jpg* | *filename.gif* | *filename.png*} と入力します。

i. **transfer download start** と入力して更新した設定を表示し、プロンプトに **y** と応答して現在のダウンロード設定を確認し、ダウンロードを開始します。次のような情報が表示されます。

```
Mode..................................... TFTP
Data Type................................ Login Image
TFTP Server IP........................... xxx.xxx.xxx.xxx
TFTP Path................................ <directory path>
TFTP Filename............................ <filename.jpg|.gif|.png>
This may take some time.
Are you sure you want to start?(y/n) y
TFTP Image transfer starting.
Image installed.
```

j. **save config** と入力して、設定を保存します。

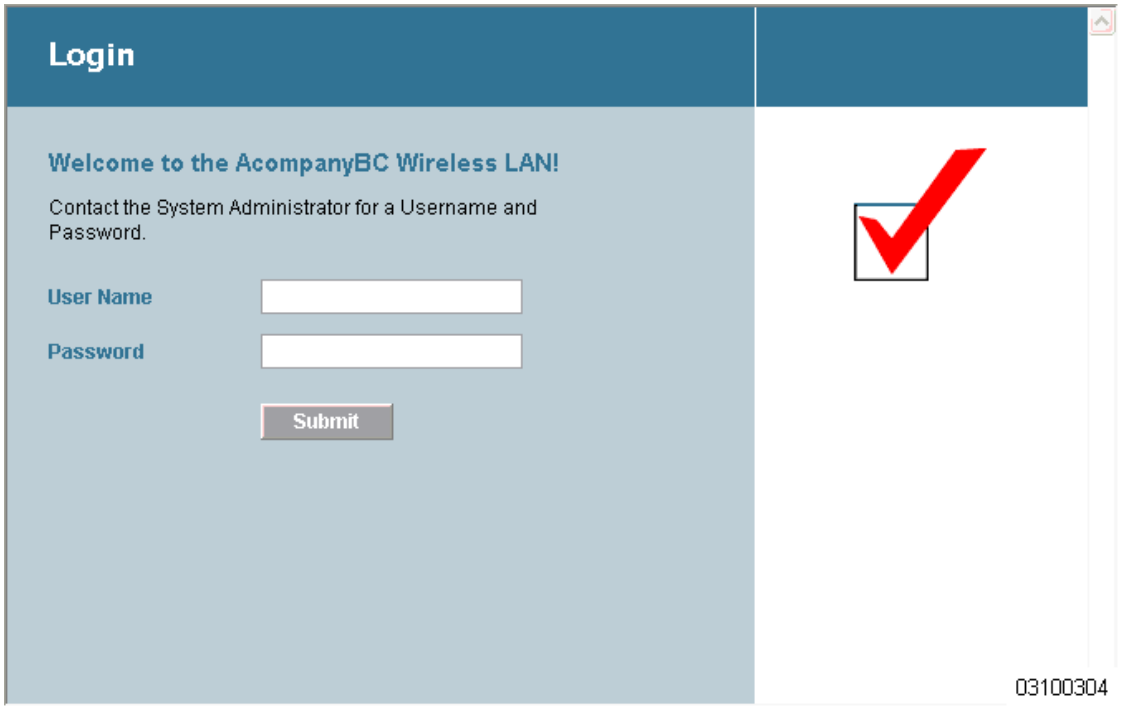
（注）　Web 認証ログイン ウィンドウからロゴを削除するには、**clear webimage** と入力します。

ステップ 9　「CLI を使用した、Web 認証ログイン ウィンドウ設定の確認」の項（P. 9-23）の指示に従って、設定を確認します。

変更されたデフォルトの Web 認証ログイン ウィンドウの例

図 9-11 は、変更されたデフォルトの Web 認証ログイン ウィンドウの例を示しています。

図 9-11　変更されたデフォルトの Web 認証ログイン ウィンドウの例



次の CLI コマンドは、このウィンドウの作成に使用されたものです。

config custom-web weblogo disable

config custom-web webtitle Welcome to the AcompanyBC Wireless LAN!

config custom-web webmessage Contact the System Administrator for a Username and Password.

transfer download start

```
Mode..................................... TFTP
Data Type.................................Login Image
TFTP Server IP............................... xxx.xxx.xxx.xxx
TFTP Path.................................... /
TFTP Filename.................................Logo.gif
This may take some time.
Are you sure you want to start?(y/n) y
TFTP Image transfer starting.
Image installed.
```

config custom-web redirecturl http://www.AcompanyBC.com

show custom-web

```
Cisco Logo.................. Disabled
CustomLogo..................00_logo.gif
Custom Title................Welcome to the AcompanyBC Wireless LAN!
Custom Message .............Contact the System Administrator for a Username and
Password.
Custom Redirect URL......... http://www.AcompanyBC.com
Web Authentication Mode.....Disabled
Web Authentication URL........Disabled
```

カスタマイズされた Web 認証ログイン ウィンドウの作成

この項では、カスタマイズされた Web 認証ログイン ウィンドウを作成するための情報を提供します。作成後は、外部 Web サーバからアクセスできるようになります。

次に、Web 認証ログイン ウィンドウのテンプレートを示します。カスタマイズされたウィンドウを作成する際に、モデルとして使用できます。

```
<html>
<head>
<meta http-equiv="Pragma" content="no-cache">
<meta HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=iso-8859-1">
<title>Web Authentication</title>
<script>

function submitAction(){
      var link = document.location.href;
      var searchString = "redirect=";
      var equalIndex = link.indexOf(searchString);
      var redirectUrl = "";
      var urlStr = "";
      if(equalIndex > 0) {
            equalIndex += searchString.length;
            urlStr = link.substring(equalIndex);
            if(urlStr.length > 0){
               redirectUrl += urlStr;
               if(redirectUrl.length > 255)
                   redirectUrl = redirectUrl.substring(0,255);
               document.forms[0].redirect_url.value = redirectUrl;
           }
      }

      document.forms[0].buttonClicked.value = 4;
      document.forms[0].submit();
}

function loadAction(){
      var url = window.location.href;
      var args = new Object();
      var query = location.search.substring(1);
      var pairs = query.split("&");
      for(var i=0;i<pairs.length;i++){
          var pos = pairs[i].indexOf('=');
          if(pos == -1) continue;
          var argname = pairs[i].substring(0,pos);
          var value = pairs[i].substring(pos+1);
          args[argname] = unescape(value);
      }
      //alert( "AP MAC Address is " + args.ap_mac);
      //alert( "The Switch URL to post user credentials is " + args.switch_url);
      //document.forms[0].action = args.switch_url;

      // This is the status code returned from webauth login action
      // Any value of status code from 1 to 5 is error condition and user
      // should be shown error as below or modify the message as it suits
      // the customer
      if(args.statusCode == 1){
        alert("You are already logged in. No further action is required on your
part.");
      }
      else if(args.statusCode == 2){
        alert("You are not configured to authenticate against web portal. No further
action is required on your part.");
      }
      else if(args.statusCode == 3){
        alert("The username specified cannot be used at this time. Perhaps the
username is already logged into the system?");
      }
```

```
      else if(args.statusCode == 4){
        alert("The User has been excluded. Please contact the administrator.");
      }
      else if(args.statusCode == 5){
        alert("Invalid username and password. Please try again.");
      }

}

</script>
</head>
<body topmargin="50" marginheight="50" onload="loadAction();">
<form method="post" action="http://1.1.1.1/login.html">
<input TYPE="hidden" NAME="buttonClicked" SIZE="16" MAXLENGTH="15" value="0">
<input TYPE="hidden" NAME="redirect_url" SIZE="255" MAXLENGTH="255" VALUE="">
<input TYPE="hidden" NAME="err_flag" SIZE="16" MAXLENGTH="15" value="0">

<div align="center">
<table border="0" cellspacing="0" cellpadding="0">
<tr> <td> </td></tr>

<tr align="center"> <td colspan="2"><font size="10" color="#336699">Web
Authentication</font></td></tr>

<tr align="center">

<td colspan="2"> User Name    <input type="TEXT" name="username"
SIZE="25" MAXLENGTH="63" VALUE="">
</td>
</tr>
<tr align="center" >
<td colspan="2"> Password      <input type="Password"
name="password" SIZE="25" MAXLENGTH="24">
</td>
</tr>

<tr align="center">
<td colspan="2"><input type="button" name="Submit" value="Submit" class="button"
onclick="submitAction();">
</td>
</tr>
</table>
</div>

</form>
</body>
</html>
```

ユーザのインターネット ブラウザがカスタマイズされたログイン ウィンドウにリダイレクトされるときに、次のパラメータが URL に追加されます。

- **ap_mac**：無線ユーザがアソシエートされているアクセス ポイントの MAC アドレス。
- **switch_url**：ユーザの資格情報を記録するコントローラの URL。
- **redirect**：認証に成功した後、ユーザがリダイレクトされる URL。
- **statusCode**：コントローラの Web 認証サーバから戻されるステータス コード。
- **wlan**：無線ユーザがアソシエートされている WLAN SSID。

使用可能なステータス コードは次のとおりです。

- ステータス コード 1 : "You are already logged in. No further action is required on your part."（すでにログインしています。これ以上の操作は不要です。）
- ステータス コード 2 : "You are not configured to authenticate against web portal. No further action is required on your part."（Web ポータルに対して認証するように設定されていません。これ以上の操作は不要です。）

- ステータス コード 3："The username specified cannot be used at this time. Perhaps the username is already logged into the system?"（指定されたユーザ名は、今回使用できません。ユーザ名はすでにログインされている可能性があります。）
- ステータス コード 4："You have been excluded."（除外されています。）
- ステータス コード 5："The User Name and Password combination you have entered is invalid. Please try again."（入力したユーザ名とパスワードの組み合わせが無効です。再入力してください。）

（注）　詳細は、次の URL にある『External Web Authentication with Wireless LAN Controllers Configuration Example』を参照してください。
http://www.cisco.com/en/US/partner/tech/tk722/tk809/technologies_configuration_example09186a008076f974.shtml

外部 Web サーバでカスタマイズされた Web 認証ログイン ウィンドウの使用

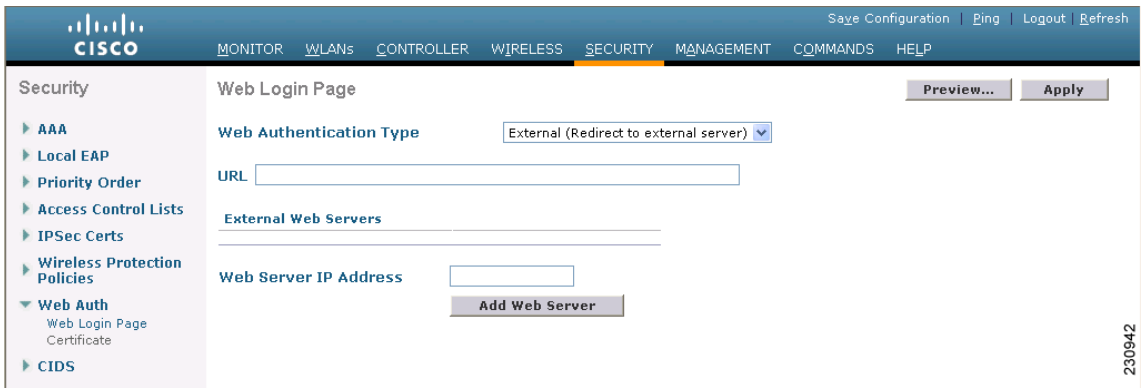
外部 Web サーバで設定した、カスタマイズされた Web 認証ログイン ウィンドウを使用する場合、次の GUI または CLI 手順の指示に従ってください。この機能を有効にすると、ユーザは、外部 Web サーバ上のカスタマイズされたログイン ウィンドウへダイレクトされます。

（注）　外部 Web サーバに対して、事前認証アクセス コントロール リスト（ACL）を WLAN 上で設定してから、Security Policies > Web Policy on the WLANs > Edit ページで、WLAN 事前認証 ACL としてその ACL を選択する必要があります。ACL の詳細は、第 5 章を参照してください。

GUI を使用した、外部 Web サーバでカスタマイズされた Web 認証ログイン ウィンドウの選択

ステップ 1　**Security** > **Web Auth** > **Web Login Page** をクリックして、Web ログイン ページにアクセスします（図 9-12 を参照）。

図 9-12　Web ログイン ページ



ステップ 2　Web Authentication Type ドロップダウン ボックスから **External (Redirect to external server)** を選択します。

ステップ 3　URL フィールドに、Web サーバ上のカスタマイズされた Web 認証ログイン ウィンドウの URL を入力します。最大 252 文字を入力することができます。

ステップ 4　Web Server IP Address フィールドに、Web サーバの IP アドレスを入力します。Web サーバは、コントローラ サービス ポート ネットワークとは異なるネットワーク上に存在しなくてはなりません。

ステップ 5　**Add Web Server** をクリックします。このサーバは、外部 Web サーバ リスト上に表示されます。

ステップ 6　**Apply** をクリックして、変更を適用します。

ステップ 7　ログイン ウィンドウの内容と外観に満足したら、**Save Configuration** をクリックして変更を保存します。

CLI を使用した、外部 Web サーバでカスタマイズされた Web 認証ログイン ウィンドウの選択

ステップ 1　Web 認証タイプを指定するには、次のコマンドを入力します。

config custom-web webauth_type external.

ステップ 2　Web サーバ上のカスタマイズされた Web 認証ログイン ウィンドウの URL を指定するには、次のコマンドを入力します。

config custom-web ext-webauth-url <url>

URL には最大 252 文字を入力することができます。

ステップ 3　Web サーバの IP アドレスを指定するには、次のコマンドを入力します。

config custom-web ext-webserver {**add** | **delete**} < サーバ IP アドレス >

ステップ 4　**save config** と入力して、設定を保存します。

ステップ 5　「CLI を使用した、Web 認証ログイン ウィンドウ設定の確認」の項（P. 9-23）の指示に従って、設定を確認します。

カスタマイズされた Web 認証ログイン ウィンドウのダウンロード

Web 認証ログイン ウィンドウで使用するページやイメージ ファイルをコントローラへダウンロードするために .tar ファイルに圧縮できます。これらのファイルは、*webauth bundle* と呼ばれています。ファイルの最大許容サイズは、非圧縮の状態で 1 MB です。.tar ファイルがローカル TFTP サーバからダウンロードされる際、コントローラのファイル システムには、展開済みファイルとして取り込まれます。

（注）　webauth bundle を GNU に準拠していない .tar 圧縮アプリケーションでロードすると、コントローラはこの bundle のファイルを解凍できず、「Extracting error」および「TFTP transfer failed」というエラー メッセージが表示されます。このため、PicoZip など GNU 標準に準拠するアプリケーションを使用して、webauth bundle の .tar ファイルを圧縮することをお勧めします。

カスタマイズされたログイン ウィンドウを作成する際のガイドラインは、次のとおりです。

- ログイン ページの名前を「login.html」とします。コントローラは、この名前に基づき Web 認証 URL を作成します。webauth bundle の展開後にこのファイルが見つからない場合、bundle は破棄され、エラー メッセージが表示されます。
- ユーザ名とパスワードの両方に入力フィールドを提供する。
- リダイレクト先の URL を元の URL から抽出後、非表示入力アイテムとして保持する。
- 元の URL からアクション URL を抽出して、ページに設定する。
- リターン ステータス コードをデコードするスクリプトを提供する。
- メインページで使用されるすべてのパス（たとえば、イメージへの参照など）が相対タイプであることを確認する。

サンプルのログイン ページを Cisco WCS からダウンロードし、カスタマイズの足がかりとして利用できます。手順は、『Cisco Wireless Control System Configuration Guide, Release 4.0』の「Using Templates」の章の「Downloading a Customized Web Auth Page」を参照してください。

カスタマイズされた Web 認証ログイン ウィンドウをコントローラにダウンロードする場合、次の GUI または CLI 手順の指示に従ってください。

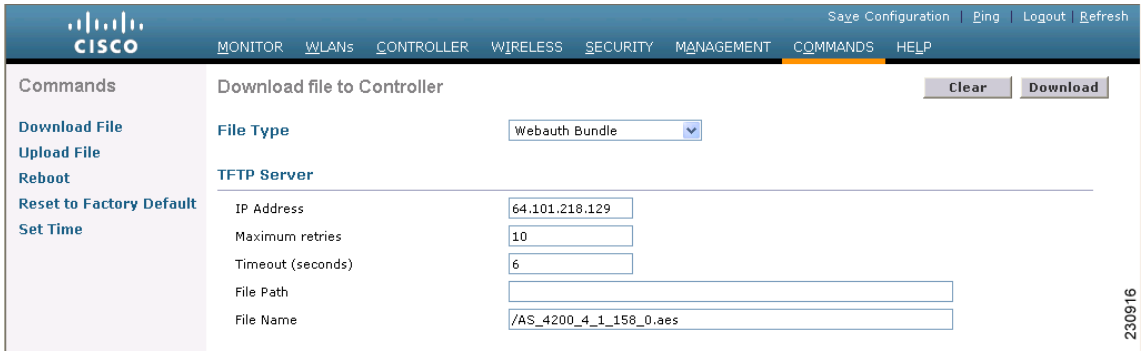
GUI を使用した、カスタマイズされた Web 認証ログイン ウィンドウのダウンロード

ステップ 1　ファイルのダウンロードで TFTP サーバを使用できることを確認します。「CLI を使用したデフォルトの Web 認証ログイン ウィンドウの選択」の項（P. 9-12）のステップ 8 にある TFTP サーバのセットアップのガイドラインを参照してください。

ステップ 2　ログイン ページが含まれる .tar ファイルを TFTP サーバのデフォルトディレクトリに移動します。

ステップ 3　**Commands** > **Download File** をクリックして、Download File to Controller ページ（図 9-13 を参照）にアクセスします。

図 9-13　Download File to Controller ページ



ステップ 4　File Type ドロップダウン ボックスから、**Webauth Bundle** を選択します。

ステップ 5　IP Address フィールドに、TFTP サーバの IP アドレスを入力します。

ステップ 6　Maximum Retries フィールドに、コントローラによる .tar ファイルのダウンロードの最大試行回数を入力します。

範囲：1 ～ 254

デフォルト：10

ステップ 7　Timeout フィールドに、コントローラによる *.tar ファイルのダウンロード試行がタイムアウトするまでの時間（秒数）を入力します。

範囲：1 ～ 254 秒

デフォルト：6 秒

ステップ 8　File Path フィールドに、ダウンロードする .tar ファイルのパスを入力します。デフォルト値は「/」です。

ステップ 9　File Name フィールドに、ダウンロードする .tar ファイルの名前を入力します。

ステップ 10　**Download** をクリックして、.tar ファイルをコントローラへダウンロードします。

ステップ 11　**Security** > **Web Auth** > **Web Login Page** をクリックして、Web ログイン ページにアクセスします。

ステップ 12　Web Authentication Type ドロップダウン ボックスから **Customized (Downloaded)** を選択します。

ステップ 13　**Apply** をクリックして、変更を適用します。

ステップ 14　**Preview** クリックして、カスタマイズされた Web 認証ログイン ウィンドウを表示します。

ステップ 15　ログイン ウィンドウの内容と外観に満足したら、**Save Configuration** をクリックして変更を保存します。

CLI を使用した、カスタマイズされた Web 認証ログイン ウィンドウのダウンロード

ステップ 1　ファイルのダウンロードで TFTP サーバを使用できることを確認します。「CLI を使用したデフォルトの Web 認証ログイン ウィンドウの選択」の項（P. 9-12）のステップ 8 にある TFTP サーバのセットアップのガイドラインを参照してください。

ステップ 2　ログイン ページが含まれる .tar ファイルを TFTP サーバのデフォルトディレクトリに移動します。

ステップ 3　ダウンロード モードを指定するには、**transfer download mode tftp** と入力します。

ステップ 4　ダウンロードするファイルのタイプを指定するには、**transfer download datatype webauthbundle** と入力します。

ステップ 5　TFTP サーバの IP アドレスを指定するには、**transfer download serverip** *tftp-server-ip-address* と入力します。

（注）　TFTP サーバによっては、TFTP サーバ IP アドレスにスラッシュ（/）を入力するだけで、自動的に適切なディレクトリへのパスが判別されるものもあります。

ステップ 6　ダウンロード パスを指定するには、**transfer download path** *absolute-tftp-server-path-to-file* と入力します。

ステップ 7　ダウンロードするファイルを指定するには、**transfer download filename** *filename.tar* と入力します。

ステップ 8　**transfer download start** と入力して更新した設定を表示し、プロンプトに **y** と応答して現在のダウンロード設定を確認し、ダウンロードを開始します。

ステップ 9　Web 認証タイプを指定するには、**config custom-web webauth_type customized** と入力します。

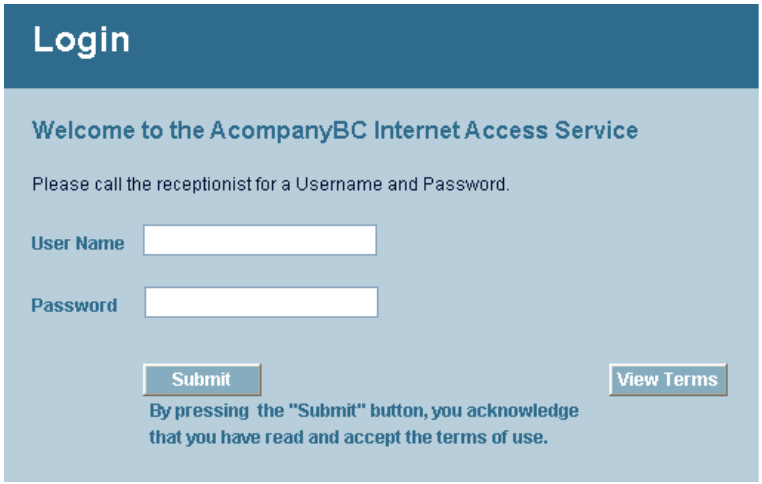
ステップ 10　**save config** と入力して、設定を保存します。

ステップ 11　「CLI を使用した、Web 認証ログイン ウィンドウ設定の確認」の項（P. 9-23）の指示に従って、設定を確認します。

カスタマイズされた Web 認証ログイン ウィンドウの例

図 9-14 は、カスタマイズされた Web 認証ログイン ウィンドウの例を示しています。

図 9-14　カスタマイズされた Web 認証ログイン ウィンドウの例



CLI を使用した、Web 認証ログイン ウィンドウ設定の確認

show custom-web と入力して、Web 認証ログイン ウィンドウへの変更を確認します。次の例は、構成設定がデフォルト値に設定されている際に表示する情報を示します。

```
Cisco Logo..................................... Enabled
CustomLogo..................................... Disabled
Custom Title................................... Disabled
Custom Message................................. Disabled
Custom Redirect URL............................ Disabled
Web Authentication Mode........................ Disabled
Web Authentication URL......................... Disabled

This example shows the information that appears when the configuration settings have
been modified:
Cisco Logo..................................... Disabled
CustomLogo..................................... 00_logo.gif
Custom Title................................... Welcome to the AcompanyBC Wireless
LAN!
Custom Message................................. Contact the System Administrator for a
                                                Username and Password.
Custom Redirect URL............................ http://www.AcompanyBC.com
Web Authentication Mode........................ Internal
Web Authentication URL........................... Disabled
```