CHAPTER 10

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 ページ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」（P.10-2）
- 「Web 認証証明書の入手」（P.10-7）
- 「Web 認証プロセス」（P.10-10）
- 「Web 認証ログイン ページの選択」（P.10-12）
- 「有線ゲスト アクセスの設定」（P.10-27）

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、限定的な設定権限を持ち、ゲスト アカウントを管理するために使用する Web ページのみにアクセスできます。

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（デフォルト値）に制限されています（[Security] > [AAA] > [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）、ローカル ネットワーク ユーザ（ゲスト ユーザを含む）、MAC フィルタ エントリ、除外リスト エントリ、およびアクセス ポイントの認可リスト エントリで共有します。これらを合わせて、設定されている最大値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

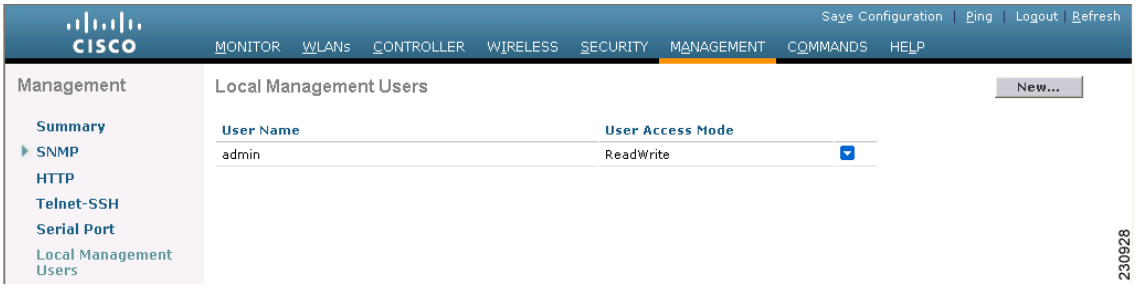
GUI または CLI を使用して、コントロール上にロビー アンバサダー アカウントを作成することができます。

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] の順に選択して、[Local Management Users] ページを開きます（図 10-1 を参照）。

図 10-1　[Local Management Users] ページ

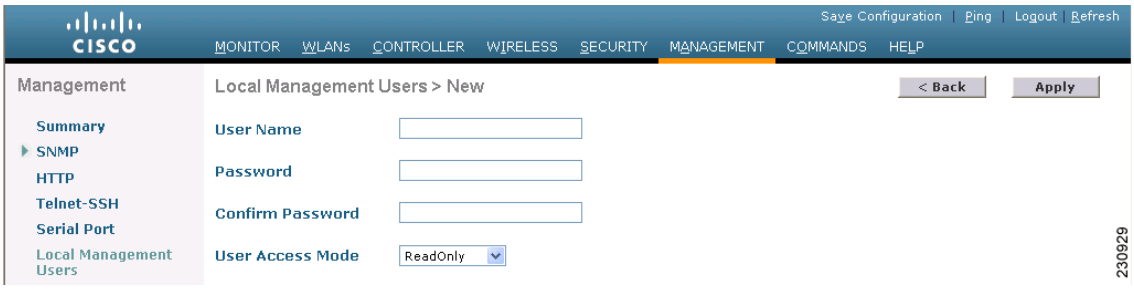


このページには、ローカル管理ユーザの名前やアクセス権限の一覧が表示されます。

（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 10-2 を参照）。

図 10-2　[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、次のコマンドを入力します。

config mgmtuser add *lobbyadmin_username lobbyadmin_pwd* **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。

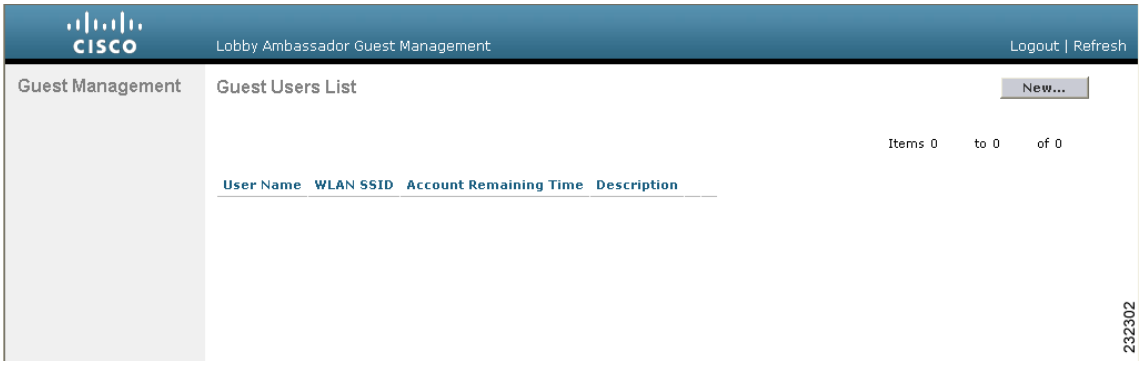
ロビー アンバサダーとしてのゲスト ユーザ アカウントの作成

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。

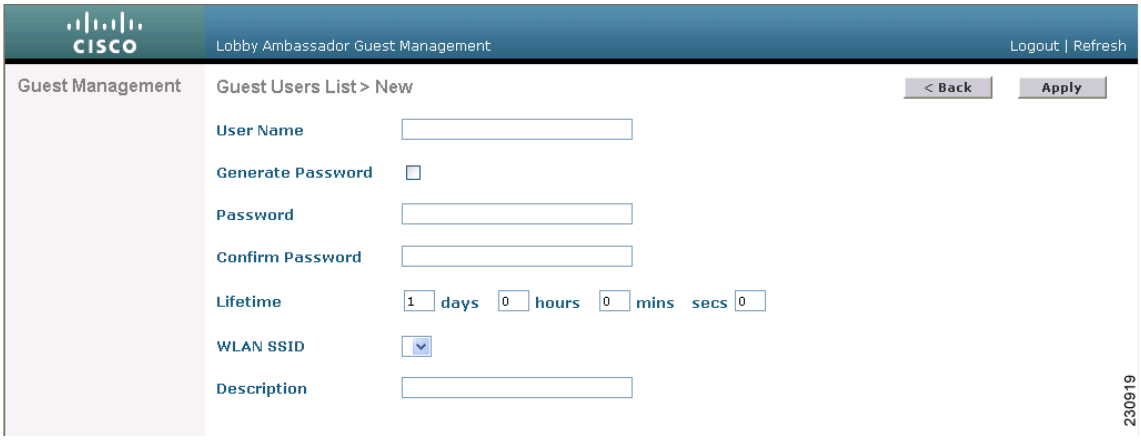
ステップ 1　上記の「ロビー アンバサダー アカウントの作成」の項で指定されたユーザ名およびパスワードを使用して、ロビー アンバサダーとしてコントローラにログインします。[Lobby Ambassador Guest Management] > [Guest Users List] ページが表示されます（図 10-3 を参照）。

図 10-3　[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 10-4 を参照）。

図 10-4　[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オンにします。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オフのままにし、[Password] および [Confirm Password] の両フィールド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、永続的な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、コントローラ GUI を使用してゲスト ユーザ アカウントを永続的なアカウントにするには、そのアカウントを一度削除した後、再度アカウントを作成しなければなりません。必要に応じて、**config netuser lifetime** *user_name* **0** CLI コマンドを使用すれば、アカウントを削除してから再度作成することなく、ゲスト ユーザ アカウントを永続的なアカウントにすることができます。

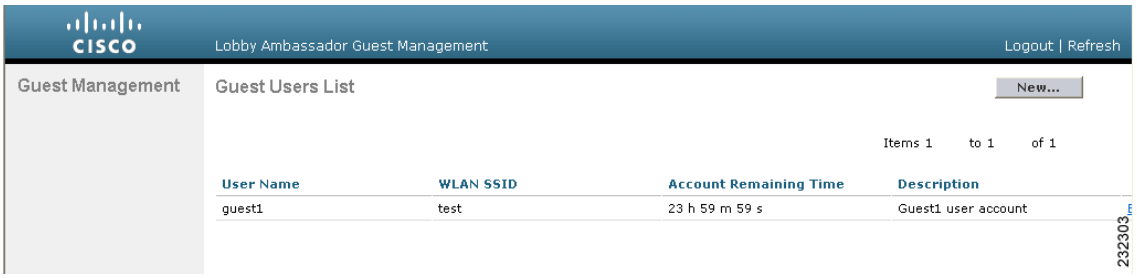
ステップ 6　[WLAN SSID] ドロップダウン ボックスから、ゲスト ユーザが使用する SSID を選択します。表示された WLAN のみにレイヤ 3 の Web 認証が設定されています。

（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 10-5 を参照）。

図 10-5　[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] を選択します。[Local Net Users] ページが表示されます（図 10-6 を参照）。

図 10-6　[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 認証証明書の入手

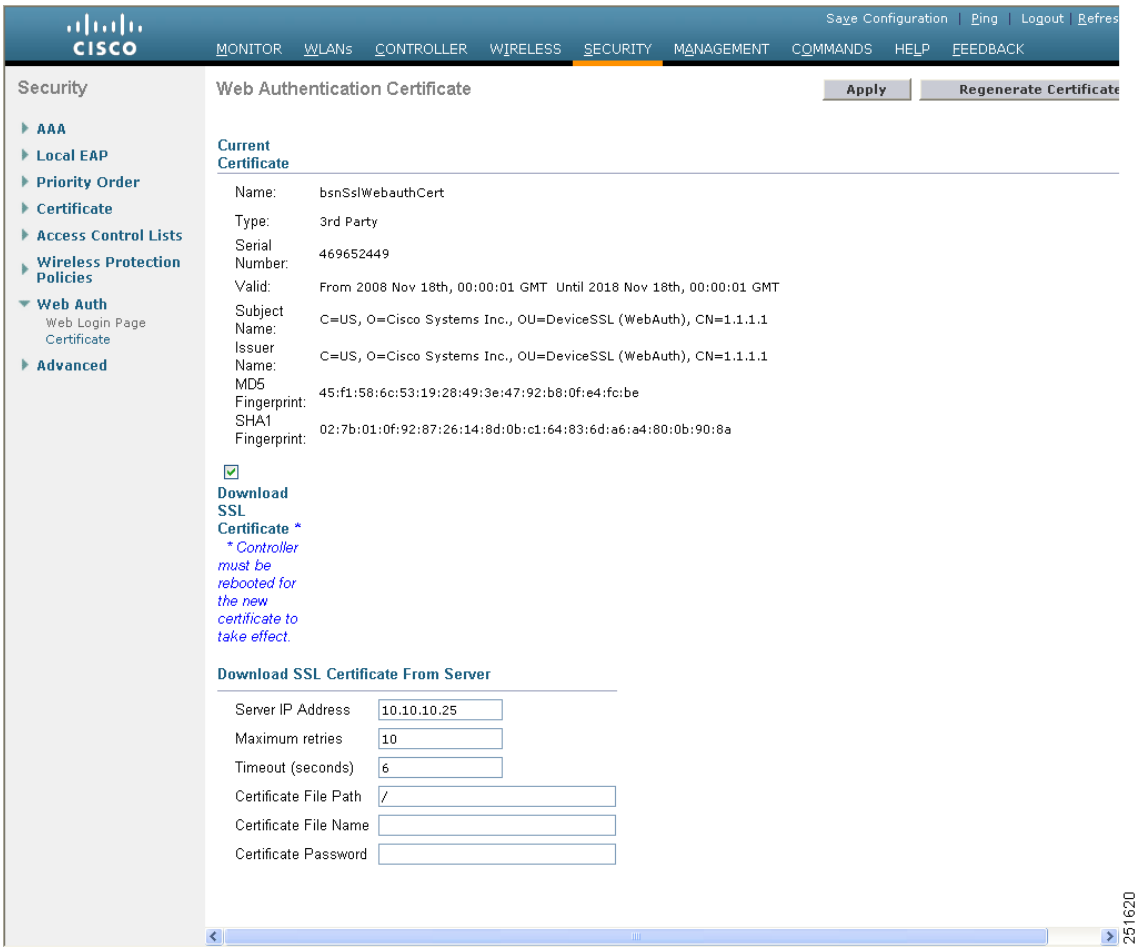
コントローラのオペレーティング システムが十分な機能を持つ Web 認証証明書を自動的に生成するため、何もすることなく、レイヤ 3 Web 認証で証明書を使用することができます。ただし、必要に応じて、新しい Web 認証証明書を生成するようにオペレーティング システムに指示したり、外部で生成された SSL 証明書をダウンロードすることもできます。

GUI を使用した Web 認証証明書の入手

コントローラ GUI を使用して、現在の Web 認証証明書を表示したり、新しい証明書を生成したり、または外部で生成された証明書をダウンロードする手順は、次のとおりです。

ステップ 1　[Security] > [Web Auth] > [Certificate] を選択して、[Web Authentication Certificate] ページを開きます（図 10-7 を参照）。

図 10-7　[Web Authentication Certificate] ページ



このページには、現在の Web 認証証明書の詳細が示されます。

ステップ 2　オペレーティング システムで生成された新しい Web 認証証明書を使用する手順は、次のとおりです。

a. [Regenerate Certificate] をクリックします。オペレーティング システムが新しい Web 認証証明書を生成し、Web 認証証明書の生成が完了したことを示すメッセージが表示されます。

b. コントローラをリブートして、新しい証明書を登録します。

ステップ 3　外部で生成された Web 認証証明書を使用する手順は、次のとおりです。

a. コントローラが TFTP サーバに ping を送ることができることを確認します。

b. [Download SSL Certificate] チェックボックスをオンにします。

c. [Server IP Address] フィールドに、TFTP サーバの IP アドレスを入力します。

d. [Maximum Retries] フィールドの 10 回の再試行および [Timeout] フィールドの 6 秒というデフォルト値は、調整しなくても適切に機能します。ただし、これらの値は変更できます。そのためには、各ダウンロードを試行できる最大回数を [Maximum Retries] フィールドに、各ダウンロードに許容される時間（秒単位）を [Timeout] フィールドに入力します。

e. [Certificate File Path] フィールドに、証明書のディレクトリ パスを入力します。

f. [Certificate File Name] フィールドに、証明書の名前を入力します（*certname*.pem）。

g. [Certificate Password] フィールドに、証明書のパスワードを入力します。

h. [Apply] をクリックして、変更を適用します。オペレーティング システムが TFTP サーバから新しい証明書をダウンロードします。

i. コントローラをリブートして、新しい証明書を登録します。

CLI を使用した Web 認証証明書の入手

コントローラ CLI を使用して、現在の Web 認証証明書を表示したり、新しい証明書を生成したり、または外部で生成された証明書をダウンロードする手順は、次のとおりです。

ステップ 1　現在の Web 認証証明書を表示するには、次のコマンドを入力します。

show certificate summary

次のような情報が表示されます。

```
Web Administration Certificate..................... Locally Generated
Web Authentication Certificate..................... Locally Generated
Certificate compatibility mode:................ off
```

ステップ 2　オペレーティング システムで新しい Web 認証証明書を生成する手順は、次のとおりです。

a. 新しい証明書を生成するには、次のコマンドを入力します。

config certificate generate webauth

b. コントローラをリブートして、新しい証明書を登録するには、次のコマンドを入力します。

reset system

ステップ 3　外部で生成された Web 認証証明書を使用する手順は、次のとおりです。

（注）　クライアントのブラウザが Web 認証 URL と Web 認証証明書のドメインを照合できるように、外部で生成された Web 認証証明書の通常名（CN）は 1.1.1.1（または相当する仮想インターフェイス IP アドレス）にすることをお勧めします。

a. ダウンロードする証明書の名前、パス、およびタイプを指定するには、次のコマンドを入力します。

transfer download mode tftp

transfer download datatype webauthcert

transfer download serverip *server_ip_address*

transfer download path *server_path_to_file*

transfer download filename *certname*.pem

transfer download certpassword *password*

transfer download tftpMaxRetries *retries*

transfer download tftpPktTimeout *timeout*

（注）　10 回の再試行および 6 秒のタイムアウトというデフォルト値は、調整しなくても適切に機能します。ただし、これらの値は変更できます。そのためには、各ダウンロードを試行できる最大回数を *retries* パラメータに、各ダウンロードに許容される時間（秒単位）を *timeout* パラメータに入力します。

b. ダウンロード プロセスを開始するには、次のコマンドを入力します。

transfer download start

c. コントローラをリブートして、新しい証明書を登録するには、次のコマンドを入力します。

reset system

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 ページ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 10-8 は一般的なセキュリティ警告を示しています。

図 10-8　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 ページが表示されます（図 10-9 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] ページで [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] ページの下部で、[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。

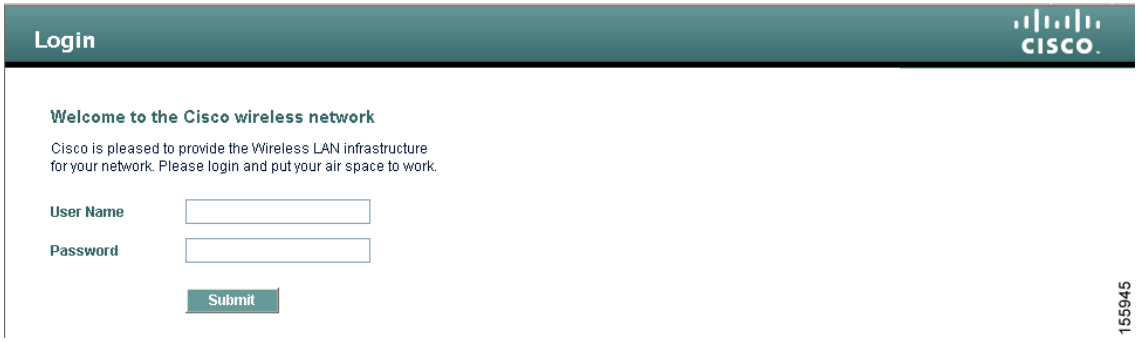
ステップ 8　[Next] > [Finish] の順にクリックします。

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] の順に選択し、[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 認証を試みるときには、ログイン ページが表示されます（図 10-9 を参照）。

図 10-9　デフォルトの Web 認証ログイン ページ



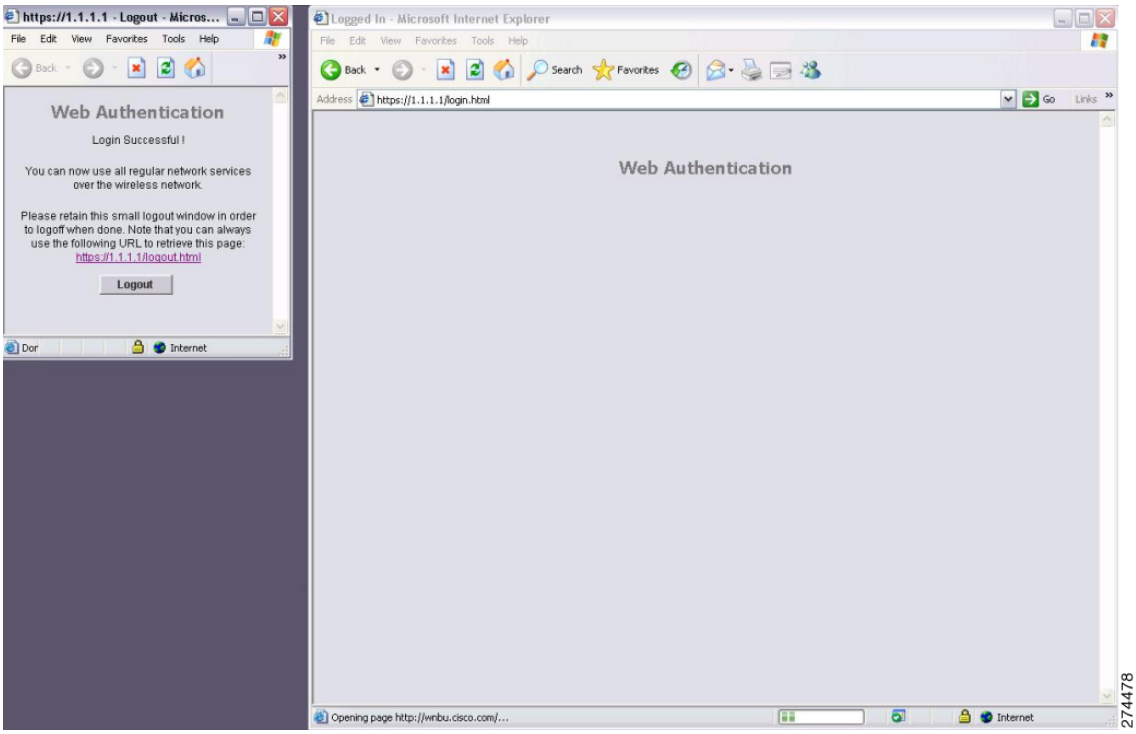
デフォルトのログイン ページには、Cisco ロゴや Cisco 特有のテキストが表示されます。Web 認証システムが次のいずれかを表示するように選択できます。

- デフォルトのログイン ページ
- デフォルトのログイン ページの変更バージョン
- 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 ページ
- 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 ページ

「Web 認証ログイン ページの選択」（P.10-12）には、Web 認証ログイン ページの表示方法を選択する手順が記載されています。

Web 認証ログイン ページで、ユーザが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ページを表示し、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 10-10 は一般的なログイン成功ページを示しています。

図 10-10　ログイン成功ページ



デフォルトのログイン成功ページには、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 ページのリダイレクト 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については、第 3 章を参照）。

Web 認証ログイン ページの選択

この項では、Web 認証ログイン ページの内容および外観を指定する手順を説明します。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 ページを選択します。

- 「デフォルトの Web 認証ログイン ページの選択」（P.10-13）
- 「カスタマイズされた Web 認証ログイン ページの作成」（P.10-17）
- 「外部 Web サーバでのカスタマイズされた Web 認証ログイン ページの使用」（P.10-19）
- 「カスタマイズされた Web 認証ログイン ページのダウンロード」（P.10-21）
- 「WLAN ごとのログイン ページ、ログイン失敗ページ、およびログアウト ページの割り当て」（P.10-25）

（注）　ユーザが SSLv2 専用に設定されているブラウザを使用して Web ページに接続するのを防止する場合は、**config network secureweb cipher-option sslv2 disable** コマンドを入力して、Web 認証に対して SSLv2 を無効にできます。このコマンドを使用すると、ユーザは、SSLv3 以降などのよりセキュアなプロトコルを使用するように設定したブラウザを使用しなければなりません。デフォルト値は有効（enable）です。

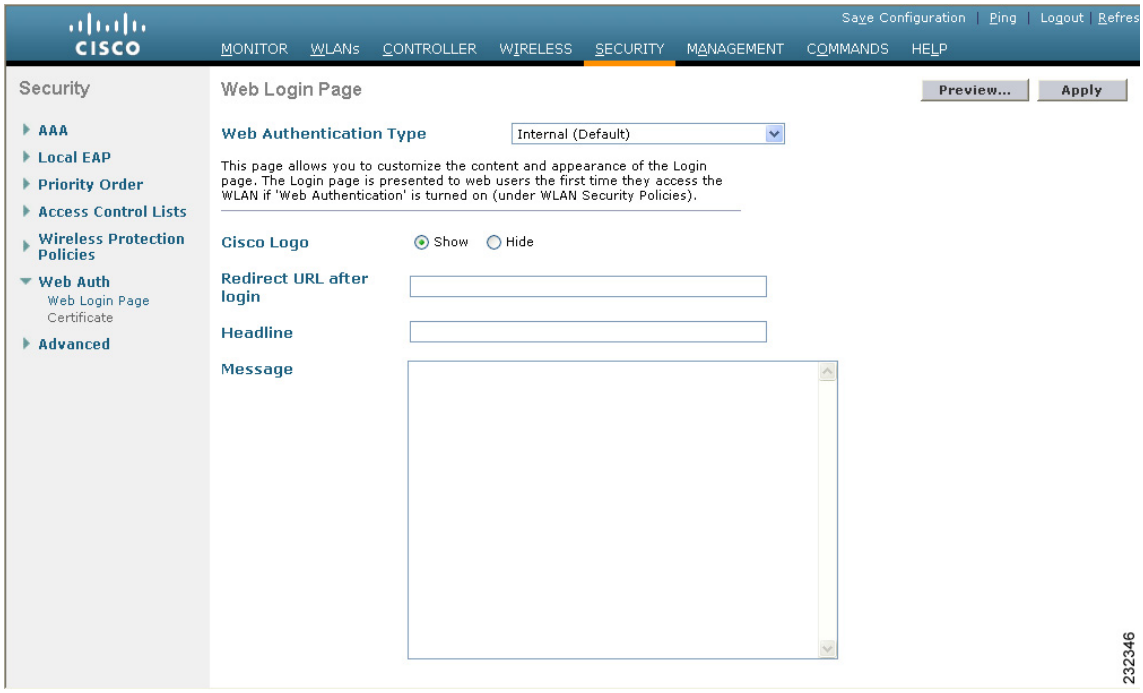
デフォルトの Web 認証ログイン ページの選択

デフォルトの Web 認証ログイン ページをそのまま使用する場合（図 10-9 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 ページの選択

ステップ 1　[Security] > [Web Auth] > [Web Login Page] の順に選択して、[Web Login Page] を開きます（図 10-11 を参照）。

図 10-11　[Web Login Page]



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 ページ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 ページを変更する場合、ステップ 4 に進みます。

ステップ 4　デフォルト ページの右上に表示されている Cisco ロゴを非表示にするには、[Cisco Logo] の [Hide] オプションを選択します。表示する場合は、[Show] オプションをクリックします。

ステップ 5　ログイン後にユーザを特定の 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。

（注）　コントローラでは、HTTP（HTTP over TCP）サーバへの Web 認証リダイレクトのみがサポートされています。HTTPS（HTTP over SSL）サーバへの Web 認証リダイレクトはサポートしていません。

ステップ 6　ログイン ページ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 ページ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 ページを表示します。

ステップ 10　ログイン ページ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 ページの選択

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 ページ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 ページを変更する場合、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 ページ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）に転送させる場合、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。

（注）　コントローラでは、HTTP（HTTP over TCP）サーバへの Web 認証リダイレクトのみがサポートされています。HTTPS（HTTP over SSL）サーバへの Web 認証リダイレクトはサポートしていません。

ステップ 5　ログイン ページ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 *title*

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 ページで独自のメッセージを作成する場合、次のコマンドを入力します。

config custom-web webmessage *message*

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 ページ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。そうでない場合は、コントローラ上に静的ルートを作成する必要があります。
- 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 30 キロビット以内です。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。

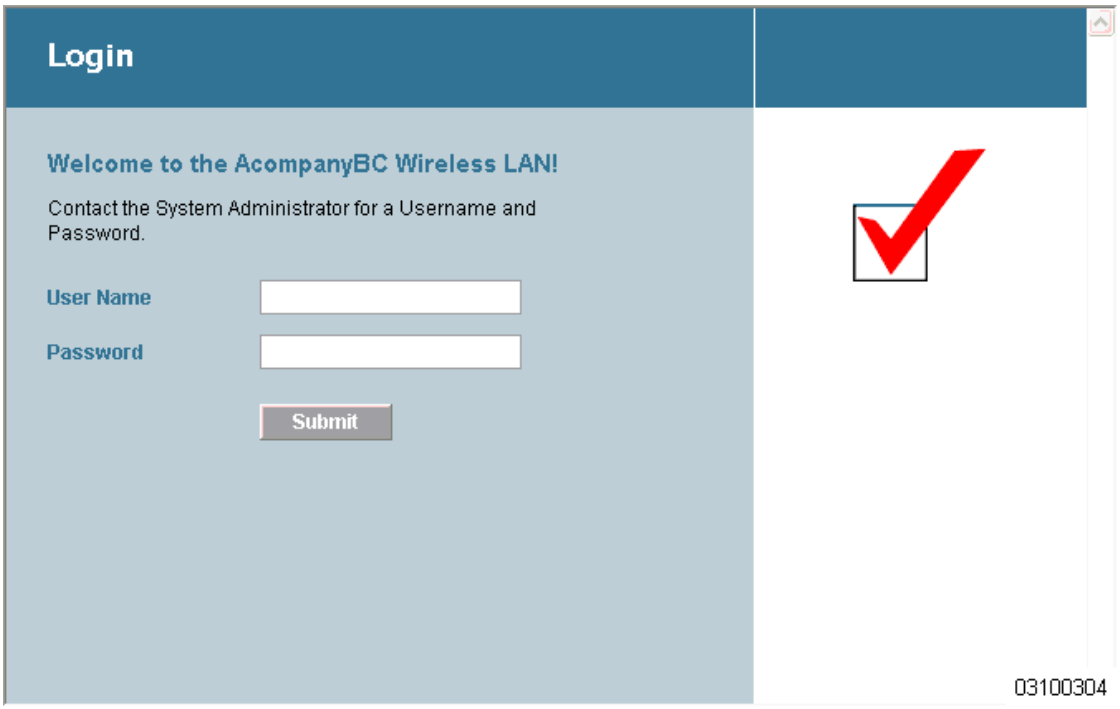
（注）　Web 認証ログイン ページからロゴを削除するには、**clear webimage** と入力します。

ステップ 9　「CLI を使用した Web 認証ログイン ページの設定の確認」（P.10-24）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 ページの例

図 10-12 は、デフォルトの Web 認証ログイン ページを変更した例を示しています。

図 10-12　変更されたデフォルトの Web 認証ログイン ページの例



このログイン ページは、次の CLI コマンドを使用して作成されます。

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 ページの作成

この項では、カスタマイズされた Web 認証ログイン ページの作成について説明します。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。

Web 認証ログイン ページのテンプレートを次に示します。カスタマイズされたページを作成する際に、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="https://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 ページ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 サーバでのカスタマイズされた Web 認証ログイン ページの使用

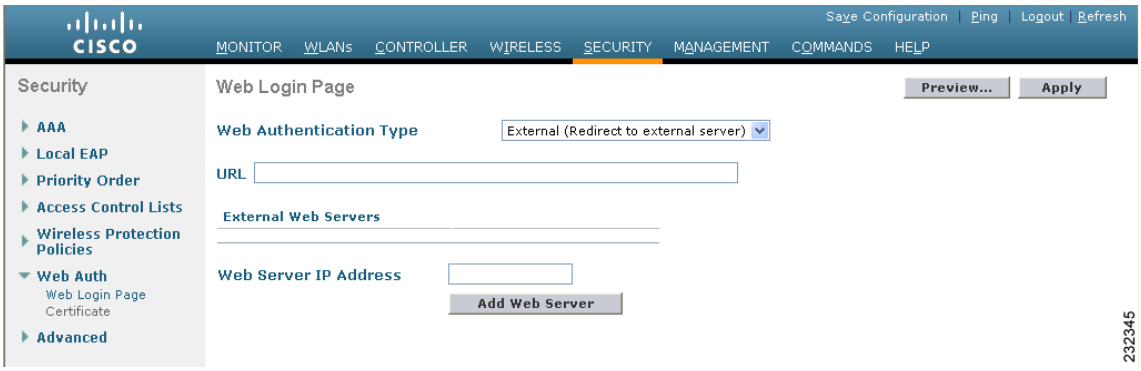
外部 Web サーバでカスタマイズされた Web 認証ログイン ページを使用する場合、次の GUI または CLI 手順の指示に従ってください。この機能を有効にすると、ユーザは、外部 Web サーバ上のカスタマイズされたログイン ページへダイレクトされます。

（注） 5500 シリーズ コントローラ、2100 シリーズ コントローラ、およびコントローラ ネットワーク モジュールでは、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 の詳細については、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 ページの選択

ステップ 1　[Security] > [Web Auth] > [Web Login Page] を選択して、[Web Login Page] を開きます（図 10-13 を参照）。

図 10-13　[Web Login Page]



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 サーバ上でカスタマイズされた Web 認証ログイン ページの 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 ページ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 ページの選択

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 サーバ上でカスタマイズされた Web 認証ログイン ページの 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**} *server_IP_address*

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 ページの設定の確認」（P.10-24）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 ページのダウンロード

Web 認証ログイン ページに使用するページやイメージ ファイルを .tar ファイルに圧縮してコントローラへダウンロードできます。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。

（注） 設定のバックアップには、webauth bundle や外部ライセンスなど、ダウンロードしてコントローラに格納した付加的なファイルやコンポーネントは含まれないため、このようなファイルやコンポーネントの外部バックアップ コピーは手動で保存する必要があります。

カスタマイズされたログイン ページ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」とする。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）が相対パスであることを確認する。

ログイン ページ例を 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。手順については、『*Cisco Wireless Control System Configuration Guide, Release 6.0*』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 ページ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 Web 認証ログイン ページのダウンロード

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 ページの選択」（P.10-14）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] の順に選択して、[Download File to Controller] ページ（図 10-14 を参照）を開きます。

図 10-14　[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　[Transfer Mode] ドロップダウン ボックスから、[TFTP] または [FTP] を選択します。

ステップ 6　[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 7　TFTP サーバを使用している場合は、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 [Maximum Retries] フィールドに入力します。

範囲：1 ～ 254

デフォルト：10

ステップ 8　TFTP サーバを使用している場合は、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 [Timeout] フィールドに入力します。

範囲：1 ～ 254 秒

デフォルト：6 秒

ステップ 9　[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 10　[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 11　FTP サーバを使用している場合は、次の手順に従います。

a.　[Server Login Username] フィールドにユーザ名を入力し、FTP サーバにログインします。

b.　[Server Login Password] フィールドにパスワードを入力し、FTP サーバにログインします。

c.　[Server Port Number] フィールドに、ダウンロードが発生する FTP サーバのポート番号を入力します。デフォルト値は 21 です。

ステップ 12　[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 13　[Security] > [Web Auth] > [Web Login Page] の順に選択して、[Web Login Page] を開きます。

ステップ 14　[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 15　[Apply] をクリックして、変更を適用します。

ステップ 16　[Preview] をクリックして、カスタマイズされた Web 認証ログイン ページを表示します。

ステップ 17　ログイン ページ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 Web 認証ログイン ページのダウンロード

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 ページの選択」（P.10-14）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。

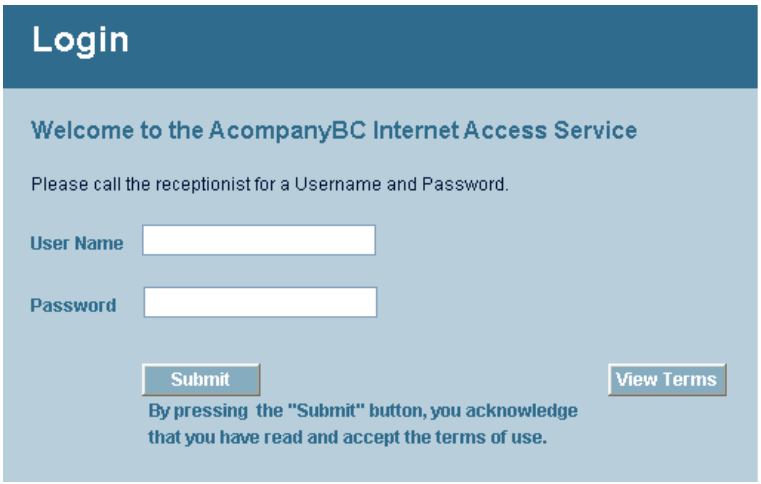
ステップ 10　**save config** と入力して、設定を保存します。

ステップ 11　「CLI を使用した Web 認証ログイン ページの設定の確認」（P.10-24）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 ページの例

図 10-15 は、カスタマイズされた Web 認証ログイン ページの例を示しています。

図 10-15　カスタマイズされた Web 認証ログイン ページの例



CLI を使用した Web 認証ログイン ページの設定の確認

show custom-web と入力して、Web 認証ログイン ページに対する変更を確認します。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
```

この例では、構成設定が変更された際に表示する情報を示します。

```
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
```

WLAN ごとのログイン ページ、ログイン失敗ページ、およびログアウト ページの割り当て

ユーザに対して、WLAN ごとに異なる Web 認証ログイン ページ、ログイン失敗ページ、ログアウト ページを表示できます。この機能を使用すると、ゲスト ユーザや組織内のさまざまな部署の従業員など、さまざまなネットワーク ユーザに対し、ユーザ固有の Web 認証ページを表示できます。

すべての Web 認証タイプ（[Internal]、[External]、[Customized]）で異なるログイン ページを使用できます。ただし、Web 認証タイプで [Customized] を選んだ場合に限り、異なるログイン失敗ページとログアウト ページを指定できます。

GUI を使用した WLAN ごとのログイン ページ、ログイン失敗ページ、ログアウト ページの割り当て

コントローラの GUI を使用して WLAN に Web ログイン ページ、ログイン失敗ページ、ログアウト ページを割り当てる手順は、次のとおりです。

ステップ 1　[WLANs] を選択して、[WLANs] ページを開きます。

ステップ 2　Web ログイン ページ、ログイン失敗ページ、またはログアウト ページを割り当てる WLAN の ID 番号をクリックします。

ステップ 3　[Security] > [Layer 3] の順に選択します。

ステップ 4　[Web Policy] と [Authentication] が選択されていることを確認します。

ステップ 5　Web 認証ページに設定されているグローバル認証設定を無効にするには、[Override Global Config] チェックボックスをオンにします。

ステップ 6　[Web Auth Type] ドロップダウン ボックスが表示されたら、次のオプションのいずれかを選択して、無線ゲスト ユーザ用の Web 認証ページを定義します。

- [Internal]：コントローラのデフォルト Web ログイン ページを表示します。これはデフォルト値です。
- [Customized]：カスタム Web ログイン ページ、ログイン失敗ページ、ログアウト ページを表示します。このオプションを選択すると、ログイン ページ、ログイン失敗ページ、ログアウト ページに対して 3 つの個別のドロップダウン ボックスが表示されます。3 つのオプションすべてに対してカスタマイズしたページを定義する必要はありません。カスタマイズしたページを表示しないオプションに対しては、該当するドロップダウン ボックスで [None] を選択します。

  （注）　これらオプションのログイン ページ、ログイン失敗ページ、ログアウト ページは、webauth.tar ファイルとしてコントローラにダウンロードされます。カスタム ページのダウンロードの詳細については、「カスタマイズされた Web 認証ログイン ページのダウンロード」（P.10-21）を参照してください。

- [External]：認証のためにユーザを外部サーバにリダイレクトします。このオプションを選択する場合、[URL] フィールドに外部サーバの URL も入力する必要があります。

  [WLANs > Edit]（[Security] > [AAA Servers]）ページで、外部認証を行う特定の RADIUS サーバまたは LDAP サーバを選択できます。また、サーバによる認証の優先順位を定義することもできます。

ステップ 7　ステップ 6 で、Web 認証タイプとして [External] を選択した場合は、[AAA Servers] を選択して、ドロップダウン ボックスから最大 3 つまでの RADIUS サーバおよび LDAP サーバを選択してください。

（注）　RADIUS および LDAP の外部サーバは、[WLANs > Edit]（[Security] > [AAA Servers]）ページでオプションを選択できるようにするため、あらかじめ設定しておく必要があります。[RADIUS Authentication Servers] ページと [LDAP Servers] ページでこれらのサーバを設定できます。

ステップ 8　Web 認証で接続するサーバの優先順位を指定する手順は、次のとおりです。デフォルトでは、[Local]、[RADIUS]、[LDAP] の順になっています。

a. [Up] ボタンと [Down] ボタンの隣にあるボックスで、最初に接続するサーバの種類（[Local]、[Radius]、[LDAP]）を強調表示します。

b. 希望のサーバ タイプがボックスの一番上に表示されるように [Up] ボタンおよび [Down] ボタンをクリックします。

c. [<] 矢印をクリックして、そのサーバ タイプを左側の優先順位ボックスに移動します。

d. この手順を繰り返して他のサーバにも優先順位を割り当てます。

ステップ 9　[Apply] をクリックして、変更を適用します。

ステップ 10　[Save Configuration] をクリックして、変更を保存します。

CLI を使用した WLAN ごとのログイン ページ、ログイン失敗ページ、ログアウト ページの割り当て

コントローラの CLI を使用して、WLAN に Web ログイン ページ、ログイン失敗ページ、ログアウト ページを割り当てる手順は、次のとおりです。

ステップ 1　Web ログイン ページ、ログイン失敗ページ、ログアウト ページを割り当てる WLAN の ID 番号を決定するには、次のコマンドを入力します。

show wlan summary

ステップ 2　カスタマイズされた Web ログイン ページ、ログイン失敗ページ、ログアウト ページに無線ゲスト ユーザをログインさせる場合は、次のコマンドを入力して Web 認証ページのファイル名および表示する WLAN を指定します。

- **config wlan custom-web login-page** *page_name wlan_id*：指定した WLAN に対するカスタマイズしたログイン ページを定義します。
- **config wlan custom-web loginfailure-page** *page_name wlan_id* ：指定した WLAN に対するカスタマイズしたログイン失敗ページを定義します。

（注）　コントローラのデフォルトのログイン失敗ページを使用するには、**config wlan custom-web loginfailure-page none** *wlan_id* コマンドを入力します。

- **config wlan custom-web logout-page** *page_name wlan_id* ：指定した WLAN に対するカスタマイズしたログアウト ページを定義します。

（注）　コントローラのデフォルトのログアウト ページを使用するには、**config wlan custom-web logout-page none** *wlan_id* コマンドを入力します。

ステップ 3　Web ログイン ページにアクセスする前に無線ゲスト ユーザを外部サーバにリダイレクトする場合は、次のコマンドを入力して、外部サーバの URL を指定します。

config wlan custom-web ext-webauth-url *ext_web_url wlan_id*

ステップ 4　Web 認証サーバの接続順序を定義するには、次のコマンドを入力します。

config wlan security web-auth server-precedence *wlan_id* {**local** | **ldap** | **radius**} {**local** | **ldap** | **radius**} {**local** | **ldap** | **radius**}

サーバの Web 認証は、デフォルトではローカル、RADIUS、LDAP の順になっています。

（注）　すべての外部サーバをコントローラで事前に設定しておく必要があります。[RADIUS Authentication Servers] ページと [LDAP Servers] ページでこれらを設定できます。

ステップ 5　無線ゲスト ユーザ用の Web 認証ページを定義するには、次のコマンドを入力します。

config wlan custom-web webauth-type {**internal** | **customized** | **external**} *wlan_id*

- **internal** は、コントローラのデフォルト Web ログイン ページを表示します。これはデフォルト値です。
- **customized** は、ステップ 2 で設定したカスタム Web ログイン ページを表示します。

（注）　ログイン失敗ページとログアウト ページは常にカスタマイズされているため、ステップ 5 で Web 認証タイプを定義する必要はありません。

- **external** は、ステップ 3 で設定された URL にユーザをリダイレクトします。

ステップ 6　グローバル カスタム Web 設定ではなく、WLAN 固有のカスタム Web 設定を使用するには、次のコマンドを入力します。

config wlan custom-web global disable *wlan_id*

（注）　**config wlan custom-web global enable** *wlan_id* コマンドを入力すると、カスタム Web 認証がグローバル レベルで設定されます。

ステップ 7　変更を保存するには、次のコマンドを入力します。

save config

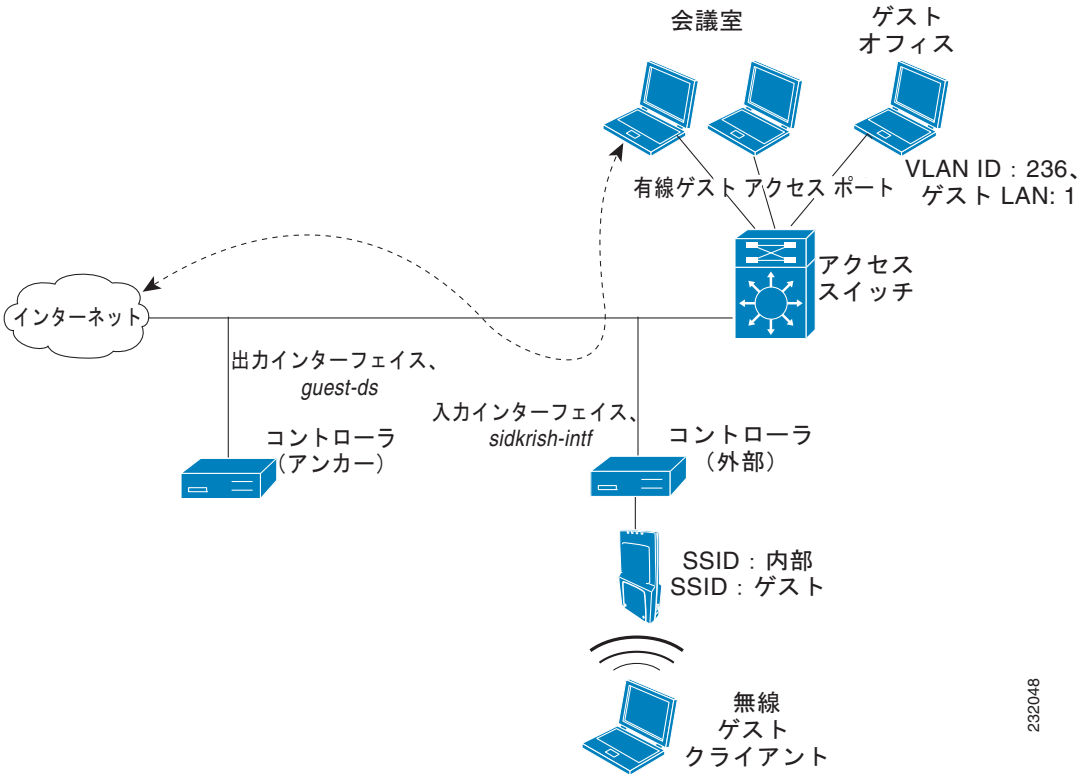
有線ゲスト アクセスの設定

有線ゲスト アクセスにより、ゲスト ユーザはゲスト アクセス用に指定および設定されている有線イーサネット接続からゲスト アクセス ネットワークに接続できます。有線ゲスト アクセス ポートは、ゲスト オフィスからまたは会議室の特定のポートを介して利用することもできます。無線ゲスト ユーザ アカウントと同様に、有線ゲスト アクセス ポートは、ロビー アンバサダー機能を使用してネットワークに追加されます。

有線ゲスト アクセスは、スタンドアロン設定または、アンカー コントローラと外部コントローラの両方を使用するデュアル コントローラ設定で設定できます。この後者の設定は、有線ゲスト アクセス トラフィックをさらに隔離するために使用されますが、有線ゲスト アクセスの展開には必須ではありません。

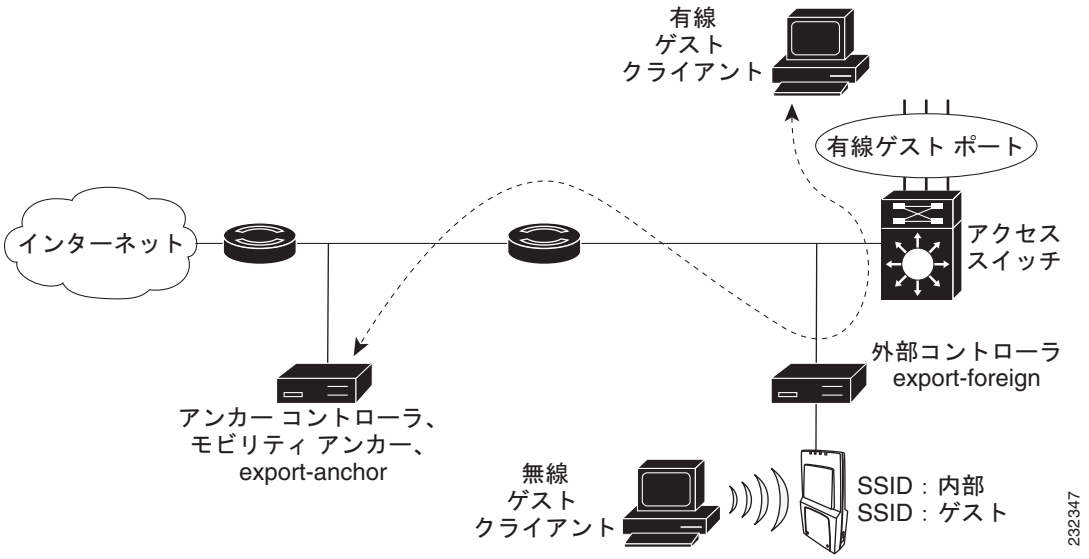
有線ゲスト アクセス ポートは最初、レイヤ 2 アクセス スイッチ上で、または有線ゲスト アクセス トラフィック用の VLAN インターフェイスで設定されているスイッチ ポート上で終端します。有線ゲスト トラフィックはその後、アクセス スイッチからコントローラへトランクされます。このコントローラは、アクセス スイッチ上で有線ゲスト アクセス VLAN にマップされているインターフェイスを使用して設定されます。図 10-16 を参照してください。

図 10-16　　1 つのコントローラを使用した有線ゲスト アクセスの例



2 つのコントローラが使用されている場合、有線ゲスト トラフィックをアクセス スイッチから受信する外部コントローラは、アンカー コントローラへそのトラフィックを転送します。このトラフィックを処理するために、外部コントローラとアンカー コントローラとの間で双方向 EoIP トンネルが確立されます。図 10-17 を参照してください。

図 10-17　　2 つのコントローラを使用した有線ゲスト アクセスの例



（注）　2 つのコントローラが展開されるとき、有線ゲスト アクセスはアンカーと外部アンカーによって管理されますが、有線ゲスト アクセス クライアントではモビリティがサポートされていません。この場合、DHCP およびクライアントの Web 認証は、アンカー コントローラによって処理されます。

（注）　QoS ロールと帯域幅コントラクトを設定することにより、ネットワーク内の有線ゲスト ユーザに割り当てられている帯域幅の量を指定できます。これらの機能の設定の詳細については、「Quality of Service ロールの設定」（P.4-70）を参照してください。

設定の概要

無線ネットワーク上で有線ゲスト アクセスを設定する手順は、次のとおりです。

1. 有線ゲスト ユーザ アクセス用の動的インターフェイス（VLAN）を設定します。
2. ゲスト ユーザ アクセス用の有線 LAN を作成します。
3. コントローラを設定します。
4. アンカー コントローラを設定します（別のコントローラでトラフィックを終端する場合）。
5. ゲスト LAN 用のセキュリティを設定します。
6. 設定を確認します。

設定のガイドライン

ネットワーク上で有線ゲスト アクセスを使用するには、次のガイドラインに従ってください。

- 有線ゲスト アクセスは、5500 および 4400 シリーズ コントローラ、Cisco WiSM、Catalyst 3750G 統合型無線 LAN コントローラ スイッチでだけサポートされます。
- 有線ゲスト アクセス インターフェイスは、タグ付きである必要があります。

- 有線ゲスト アクセス ポートは、外部コントローラと同じレイヤ 2 ネットワークになければなりません。
- コントローラ上で、最大 5 つの有線ゲスト アクセス LAN を設定できます。
- 有線ゲスト アクセス クライアントに対して、レイヤ 3 Web 認証と Web パススルーがサポートされています。レイヤ 2 セキュリティはサポートされていません。
- Catalyst 3750G 統合型無線 LAN コントローラ スイッチのゲスト VLAN を複数のコントローラにトランクしないでください。この方法で、冗長性を実現することはできません。

GUI を使用した有線ゲスト アクセスの設定

コントローラの GUI を使用して、ネットワーク上で有線ゲスト ユーザ アクセスを設定する手順は、次のとおりです。

ステップ 1　有線ゲスト ユーザ アクセス用の動的インターフェイスを作成するために、[Controller] > [Interfaces] の順に選択します。[Interfaces] ページが表示されます。

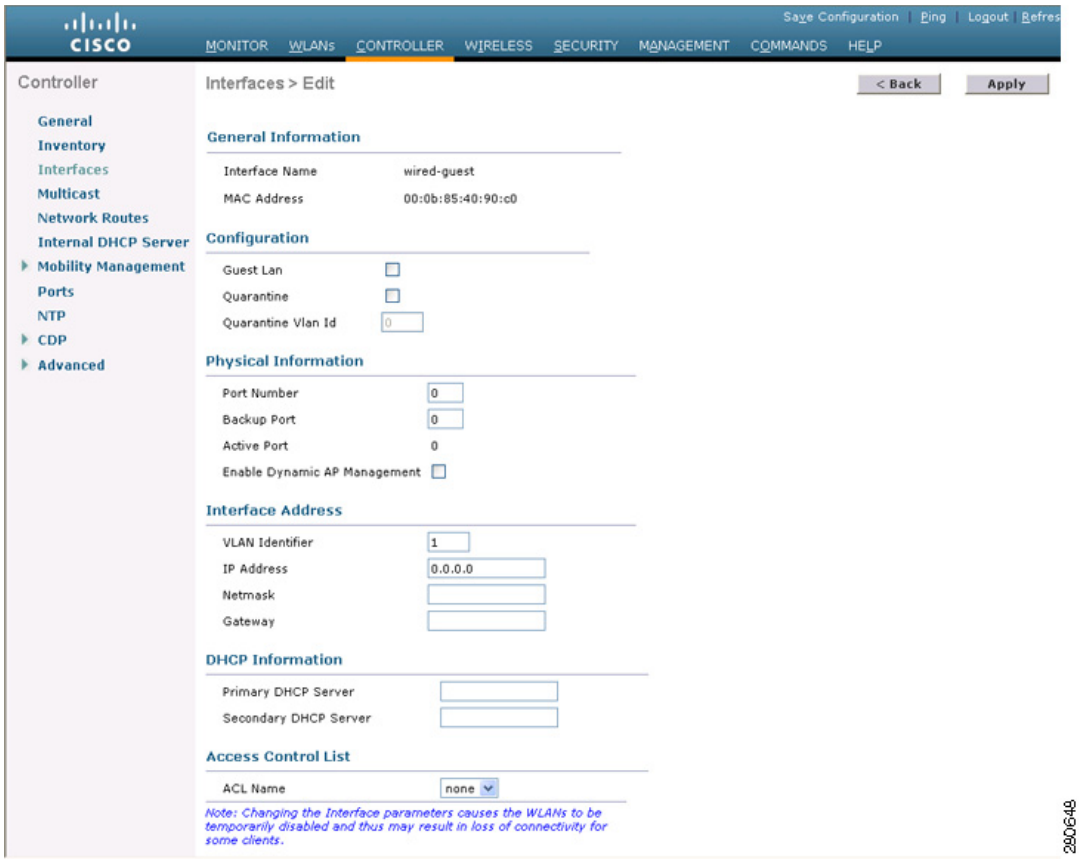
ステップ 2　[New] をクリックして、[Interfaces > New] ページを開きます。

ステップ 3　新しいインターフェイスの名前と VLAN ID を入力します。

ステップ 4　[Apply] をクリックして、変更を適用します。

ステップ 5　[Interfaces > Edit] ページで、インターフェイスの IP アドレス、ネットマスク、およびゲートウェイ アドレスを入力します（図 10-18 を参照）。

図 10-18　[Interfaces > Edit] ページ



ステップ 6　[Port Number] フィールドに、有効なポート番号を入力します。0 ～ 25（両端の値を含む）の数値を入力できます。

ステップ 7　[Guest LAN] チェックボックスをオンにします。

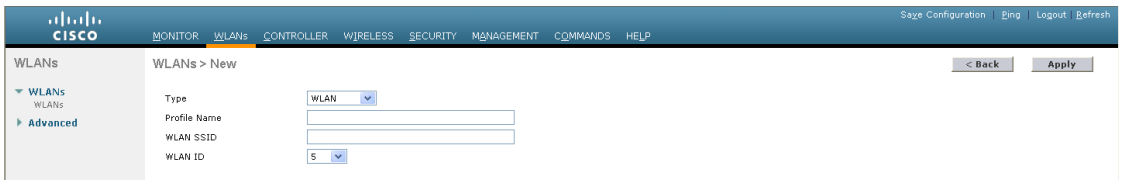
ステップ 8　プライマリ DHCP サーバの IP アドレスを入力します。

ステップ 9　[Apply] をクリックして、変更を適用します。

ステップ 10　ゲスト ユーザ アクセス用に有線 LAN を作成するために、[WLANs] を選択します。

ステップ 11　[WLANs] ページで、ドロップダウン ボックスから [Create New] を選択して、[Go] をクリックします。[WLANs > New] ページが表示されます（図 10-19 を参照）。

図 10-19　[WLANs > New] ページ



ステップ 12　[Type] ドロップダウン ボックスから、[Guest LAN] を選択します。

ステップ 13　[Profile Name] フィールドに、ゲスト LAN を識別する名前を入力します。スペースを使用しないでください。

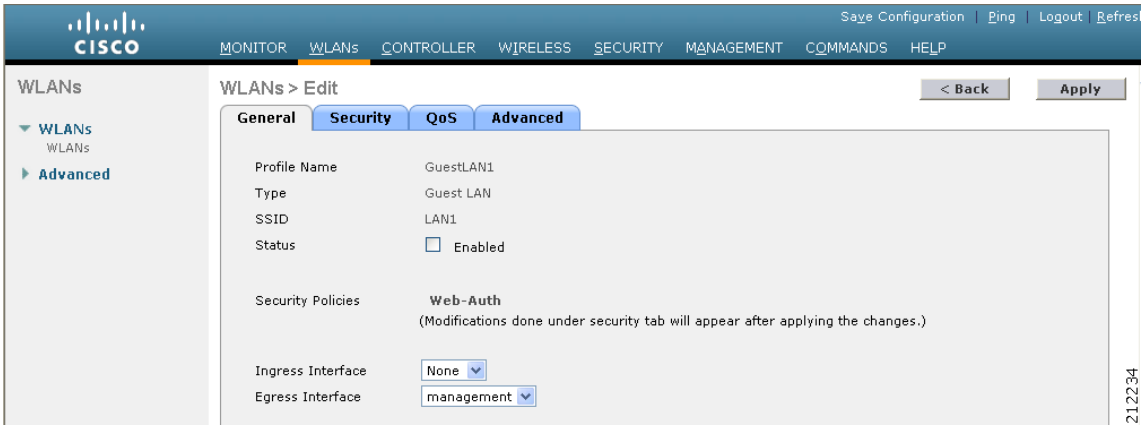
ステップ 14　[WLAN SSID] フィールドに、ゲスト LAN を識別する SSID を入力します。スペースを使用しないでください。

ステップ 15　[WLAN ID] ドロップダウン ボックスから、このゲスト LAN の ID 番号を選択します。

（注）　最大 5 つのゲスト LAN を作成できるので、[WLAN ID] オプションは 1 ～ 5（両端の値を含む）です。

ステップ 16　[Apply] をクリックして、変更を適用します。[WLANs > Edit] ページが表示されます（図 10-20 を参照）。

図 10-20　[WLANs > Edit] ページ



ステップ 17　[Status] パラメータに対する [Enabled] チェックボックスをオンにします。

ステップ 18　Web 認証（[Web-Auth]）は、デフォルトのセキュリティ ポリシーです。これを Web パススルーに変更する場合は、ステップ 19 とステップ 20 を終了してから、[Security] タブを選択します。

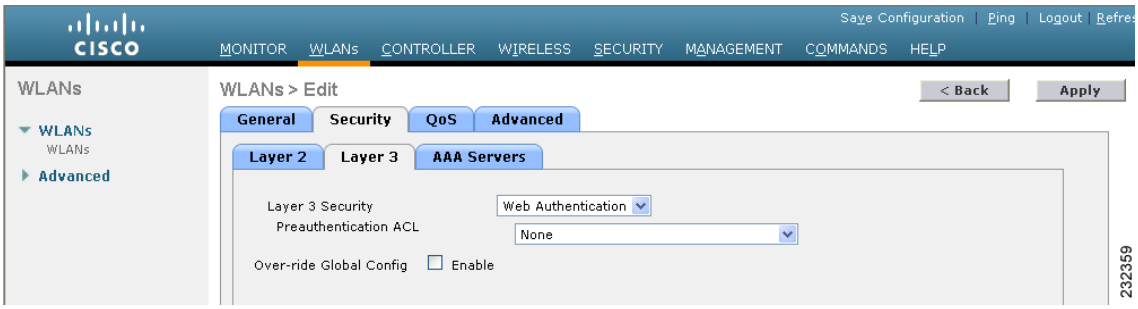
ステップ 19　[Ingress Interface] ドロップダウン ボックスから、ステップ 3 で作成した VLAN を選択します。この VLAN は、レイヤ 2 アクセス スイッチを経由して、有線ゲスト クライアントとコントローラとの間のパスを提供します。

ステップ 20　[Egress Interface] ドロップダウン ボックスから、インターフェイスの名前を選択します。この WLAN は、有線ゲスト クライアント トラフィックのコントローラから送信されるパスを提供します。

（注）　設定でコントローラが 1 つしかない場合は、[Egress Interface] ドロップダウン ボックスから [management] を選択します。

ステップ 21　認証方式を変更する（たとえば、Web 認証から Web パススルーへ）場合、[Security] > [Layer 3] の順に選択します。[WLANs > Edit]（[Security] > [Layer 3]）ページが表示されます（図 10-21 を参照）。

図 10-21　[WLANs > Edit]（[Security] > [Layer 3]）ページ



ステップ 22　[Layer 3 Security] ドロップダウン ボックスから、次のいずれかを選択します。

- [None]：レイヤ 3 セキュリティが無効になっています。
- [Web Authentication]：無線ネットワークに接続する際に、ユーザにユーザ名とパスワードの入力を求めます。これはデフォルト値です。
- [Web Passthrough]：ユーザがユーザ名とパスワードを入力せずに、ネットワークにアクセスすることを許可します。

ステップ 23　[Web Passthrough] オプションを選択する場合、[Email Input] チェックボックスが表示されます。ユーザがネットワークに接続を試みているときに、電子メール アドレスの入力を求める場合、このチェックボックスをオンにします。

ステップ 24　[Web Login Page] に設定されているグローバル認証設定を無効にするには、[Override Global Config] チェックボックスをオンにします。

ステップ 25　[Web Auth Type] ドロップダウン ボックスが表示されたら、次のオプションのいずれかを選択して、有線ゲスト ユーザ用の Web 認証ページを定義します。

- [Internal]：コントローラのデフォルト Web ログイン ページを表示します。これはデフォルト値です。
- [Customized]：カスタム Web ログイン ページ、ログイン失敗ページ、ログアウト ページを表示します。このオプションを選択すると、ログイン ページ、ログイン失敗ページ、ログアウト ページに対して 3 つの個別のドロップダウン ボックスが表示されます。3 つのオプションすべてに対してカスタマイズしたページを定義する必要はありません。カスタマイズしたページを表示しないオプションに対しては、該当するドロップダウン ボックスで [None] を選択します。

  （注）　これらのオプションのログイン ページ、ログイン失敗ページ、ログアウト ページは、webauth.tar ファイルとしてコントローラにダウンロードされます。

- [External]：認証のためにユーザを外部サーバにリダイレクトします。このオプションを選択する場合、[URL] フィールドに外部サーバの URL も入力する必要があります。

  [WLANs > Edit]（[Security] > [AAA Servers]）ページで、外部認証を行う特定の RADIUS サーバまたは LDAP サーバを選択できます。また、サーバによる認証の優先順位を定義することもできます。

ステップ 26　ステップ 25 で、Web 認証タイプとして [External] を選択した場合は、[AAA Servers] を選択して、ドロップダウン ボックスから最大 3 つまでの RADIUS サーバおよび LDAP サーバを選択してください。

（注）　RADIUS および LDAP の外部サーバは、[WLANs > Edit]（[Security] > [AAA Servers]）ページでオプションを選択できるようにするため、あらかじめ設定しておく必要があります。[RADIUS Authentication Servers] ページと [LDAP Servers] ページでこれらのサーバを設定できます。

ステップ 27　Web 認証で接続するサーバの優先順位を指定する手順は、次のとおりです。デフォルトでは、[Local]、[RADIUS]、[LDAP] の順になっています。

a. [Up] ボタンと [Down] ボタンの隣にあるボックスで、最初に接続するサーバの種類（[Local]、[Radius]、[LDAP]）を強調表示します。

b. 希望のサーバ タイプがボックスの一番上に表示されるように [Up] ボタンおよび [Down] ボタンをクリックします。

c. [<] 矢印をクリックして、そのサーバ タイプを左側の優先順位ボックスに移動します。

d. この手順を繰り返して他のサーバにも優先順位を割り当てます。

ステップ 28　[Apply] をクリックして、変更を適用します。

ステップ 29　[Save Configuration] をクリックして、変更を保存します。

ステップ 30　2 番目の（アンカー）コントローラがネットワークで使用中の場合は、このプロセスを繰り返します。

CLI を使用した有線ゲスト アクセスの設定

コントローラの CLI を使用して、ネットワーク上で有線ゲスト ユーザ アクセスを設定する手順は、次のとおりです。

ステップ 1　有線ゲスト ユーザのアクセス用の動的インターフェイス（VLAN）を作成するには、次のコマンドを入力します。

config interface create *interface_name vlan_id*

ステップ 2　リンク集約トランクが設定されていない場合、次のコマンドを入力して、物理ポートをインターフェイスにマッピングします。

config interface port *interface_name primary_port* {*secondary_port*}

ステップ 3　ゲスト LAN VLAN を有効または無効にするには、次のコマンドを入力します。

config interface guest-lan *interface_name* {**enable** | **disable**}

この VLAN は、ステップ 5 で作成する入力インターフェイスに後でアソシエートされます。

ステップ 4　有線クライアント トラフィックを作成してインターフェイスにアソシエートさせるには、次のコマンドを入力します。

config guest-lan create *guest_lan_id interface_name*

ゲスト LAN ID は、1 ～ 5（両端の値を含む）にする必要があります。

（注）　有線ゲスト LAN を削除するには、**config guest-lan delete** *guest_lan_id* コマンドを入力します。

ステップ 5　レイヤ 2 アクセス スイッチ経由で有線ゲスト クライアントとコントローラ間のパスを提供する、有線ゲスト VLAN の入力インターフェイスを設定するには、次のコマンドを入力します。

config guest-lan ingress-interface *guest_lan_id interface_name*

ステップ 6　コントローラから有線ゲスト トラフィックを送信する出力インターフェイスを設定するには、次のコマンドを入力します。

config guest-lan interface *guest_lan_id interface_name*

（注）　有線ゲスト トラフィックが別のコントローラで終端する場合は、終点の（アンカー）コントローラに対してステップ 4 とステップ 6 を繰り返し、起点の（外部）コントローラに対してステップ 1 ～ステップ 5 を繰り返します。さらに、両方のコントローラに対して次のコマンドを設定します。
config mobility group anchor add {**guest-lan** *guest_lan_id* | **wlan** *wlan_id*} *IP_address*

ステップ 7　有線ゲスト LAN のセキュリティ ポリシーを設定するには、次のコマンドを入力します。

config guest-lan security {**web-auth enable** *guest_lan_id* | **web-passthrough enable** *guest_lan_id*}

（注）　Web 認証はデフォルト設定です。

ステップ 8　有線ゲスト LAN を有効または無効にするには、次のコマンドを入力します。

config guest-lan {**enable** | **disable**} *guest_lan_id*

ステップ 9　カスタマイズされた Web ログイン ページ、ログイン失敗ページ、ログアウト ページに有線ゲスト ユーザをログインさせる場合は、次のコマンドを入力して、Web 認証ページのファイル名および表示するゲスト LAN を指定します。

- **config guest-lan custom-web login-page** *page_name guest_lan_id* : Web ログイン ページを定義します。
- **config guest-lan custom-web loginfailure-page** *page_name guest_lan_id* : Web ログイン失敗ページを定義します。

  （注）　コントローラのデフォルトのログイン失敗ページを使用するには、**config guest-lan custom-web loginfailure-page none** *guest_lan_id* コマンドを入力します。

- **config guest-lan custom-web logout-page** *page_name guest_lan_id* : Web ログアウト ページを定義します。

  （注）　コントローラのデフォルトのログアウト ページを使用するには、**config guest-lan custom-web logout-page none** *guest_lan_id* コマンドを入力します。

ステップ 10　有線ゲスト ユーザが Web ログイン ページにアクセスする前に有線ゲスト ユーザを外部サーバにリダイレクトする場合は、次のコマンドを入力して、外部サーバの URL を指定します。

config guest-lan custom-web ext-webauth-url *ext_web_url guest_lan_id*

ステップ 11　ローカル（コントローラ）または外部（RADIUS、LDAP）の Web 認証サーバの接続順序を定義するには、次のコマンドを入力します。

config wlan security web-auth server-precedence *wlan_id* {**local** | **ldap** | **radius**} {**local** | **ldap** | **radius**} {**local** | **ldap** | **radius**}

サーバの Web 認証は、デフォルトではローカル、RADIUS、LDAP の順になっています。

（注）　すべての外部サーバをコントローラで事前に設定しておく必要があります。[RADIUS Authentication Servers] ページまたは [LDAP Servers] ページでこれらを設定できます。

ステップ 12　有線ゲスト ユーザ用の Web ログイン ページを定義するには、次のコマンドを入力します。

config guest-lan custom-web webauth-type {**internal** | **customized** | **external**} *guest_lan_id*

- **internal** は、コントローラのデフォルト Web ログイン ページを表示します。これはデフォルト値です。
- **customized** では、ステップ 9 で設定したカスタム Web ページ（ログイン ページ、ログイン失敗ページ、またはログアウト ページ）が表示されます。
- **external** は、ステップ 10 で設定された URL にユーザをリダイレクトします。

ステップ 13　グローバル カスタム Web 設定ではなく、ゲスト LAN 固有のカスタム Web 設定を使用するには、次のコマンドを入力します。

config guest-lan custom-web global disable *guest_lan_id*

（注）　**config guest-lan custom-web global enable** *guest_lan_id* コマンドを入力すると、カスタム Web 認証がグローバル レベルで設定されます。

ステップ 14　変更を保存するには、次のコマンドを入力します。

save config

（注）　設定された Web 認証ページの情報は、**show run-config** コマンドおよび **show running-config** コマンドの両方に表示されます。

ステップ 15　特定のゲスト LAN に対するカスタマイズ Web 認証設定を表示するには、次のコマンドを入力します。

show custom-web {**all** | **guest-lan** *guest_lan_id*}

（注）　内部の Web 認証が設定されていると、Web Authentication Type は、外部（コントローラ レベル）またはカスタマイズ（WLAN プロファイル レベル）ではなく内部として表示されます。

show custom-web all コマンドに対しては、次のような情報が表示されます。

```
Radius Authentication Method..................... PAP
Cisco Logo....................................... Enabled
CustomLogo....................................... None
Custom Title..................................... None
Custom Message................................... None
Custom Redirect URL.............................. None
Web Authentication Type..............            External
External Web Authentication URL............       http:¥¥9.43.0.100¥login.html

External Web Server list
Index IP Address
----- ---------------
1       9.43.0.100
2       0.0.0.0
3       0.0.0.0
4       0.0.0.0
5       0.0.0.0
```

```
...
20      0.0.0.0

Configuration Per Profile:

WLAN ID: 1
    WLAN Status..................................... Enabled
    Web Security Policy............................ Web Based Authentication
    Global Status.................................. Disabled
    WebAuth Type................................... Customized
    Login Page..................................... login1.html
    Loginfailure page name....................... loginfailure1.html
    Logout page name............................... logout1.html

WLAN ID: 2
WLAN Status..................................... Enabled
    Web Security Policy............................ Web Based Authentication
    Global Status.................................. Disabled
    WebAuth Type................................... Internal
    Loginfailure page name......................... None
    Logout page name............................... None

WLAN ID: 3
WLAN Status..................................... Enabled
    Web Security Policy............................ Web Based Authentication
    Global Status.................................. Disabled
    WebAuth Type................................... Customized
    Login Page..................................... login.html
    Loginfailure page name......................... LF2.html
    Logout page name............................... LG2.html
```

show custom-web guest-lan *guest_lan_id* コマンドに対しては、次のような情報が表示されます。

```
Guest LAN ID: 1
Guest LAN Status............................... Disabled
Web Security Policy............................ Web Based Authentication
Global Status.................................. Enabled
WebAuth Type................................... Internal
Loginfailure page name......................... None
Logout page name............................... None
```

ステップ 16　ローカル インターフェイスの要約を表示するには、次のコマンドを入力します。

show interface summary

次のような情報が表示されます。

```
Interface Name                  Port Vlan Id  IP Address      Type    Ap Mgr Guest
------------------------------- ---- -------- --------------- ------- ------ -----
ap-manager                      1    untagged 1.100.163.25    Static  Yes    No

management                      1    untagged 1.100.163.24    Static  No     No

service-port                    N/A  N/A      172.19.35.31    Static  No     No

virtual                         N/A  N/A      1.1.1.1         Static  No     No

wired                           1    20       10.20.20.8      Dynamic No     No

wired-guest                     1  236     10.20.236.50   Dynamic No    Yes
```

（注）　この例の有線ゲスト LAN のインターフェイス名は、*wired-guest* 、VLAN ID は 236 です。

ステップ 17　詳細なインターフェイス情報を表示するには、次のコマンドを入力します。

show interface detailed *interface_name*

次のような情報が表示されます。

```
Interface Name................................. wired-guest
MAC Address.................................... 00:11:92:ff:e7:eb
IP Address..................................... 10.20.236.50
IP Netmask..................................... 255.255.255.0
IP Gateway..................................... 10.50.236.1
VLAN........................................... 236
Quarantine-vlan................................ no
Active Physical Port........................... LAG (29)
Primary Physical Port.......................... LAG (29)
Backup Physical Port........................... Unconfigured
Primary DHCP Server............................ 10.50.99.1
Secondary DHCP Server.......................... Unconfigured
DHCP Option 82................................. Disabled
ACL............................................ Unconfigured
AP Manager..................................... No
Guest Interface.............................. Yes
```

ステップ 18　特定の有線ゲスト LAN の設定を表示するには、次のコマンドを入力します。

show guest-lan *guest_lan_id*

次のような情報が表示されます。

```
Guest LAN Identifier........................... 1
Profile Name................................... guestlan
Network Name (SSID)............................ guestlan
Status......................................... Enabled
AAA Policy Override............................ Disabled
Number of Active Clients....................... 1
Exclusionlist Timeout.......................... 60 seconds
Session Timeout................................ Infinity
Interface...................................... wired
Ingress Interface.............................. wired-guest
WLAN ACL....................................... unconfigured
DHCP Server.................................... 10.20.236.90
DHCP Address Assignment Required............... Disabled
Quality of Service............................. Silver (best effort)
Security
    Web Based Authentication...................... Enabled
    ACL........................................... Unconfigured
    Web-Passthrough............................... Disabled
    Conditional Web Redirect...................... Disabled
    Auto Anchor................................... Disabled
Mobility Anchor List
GLAN ID IP Address Status
------- --------------- ------
```

（注）　コントローラ上で設定されているすべての有線ゲスト LAN を表示するには、**show guest-lan summary** と入力します。

ステップ 19　アクティブな有線ゲスト LAN クライアントを表示するには、次のコマンドを入力します。

show client summary guest-lan

次のような情報が表示されます。

```
Number of Clients................................ 1
MAC Address        AP Name Status     WLAN  Auth Protocol  Port Wired
------------------ ------- ---------- ----- ----- --------- ----- ------
00:16:36:40:ac:58   N/A   Associated   1    No    802.3     1    Yes
```

ステップ 20　特定のクライアントの詳細情報を表示するには、次のコマンドを入力します。

show client detail *client_mac*

次のような情報が表示されます。

```
Client MAC Address.............................. 00:40:96:b2:a3:44
Client Username ................................ N/A
AP MAC Address.................................. 00:18:74:c7:c0:90
Client State.................................... Associated
Wireless LAN Id................................. 1
BSSID........................................... 00:18:74:c7:c0:9f
Channel......................................... 56
IP Address...................................... 192.168.10.28
Association Id.................................. 1
Authentication Algorithm........................ Open System
Reason Code..................................... 0
Status Code..................................... 0
Session Timeout................................. 0
Client CCX version.............................. 5
Client E2E version.............................. No E2E support
Diagnostics Capability.......................... Supported
S69 Capability.................................. Supported
Mirroring....................................... Disabled
QoS Level....................................... Silver
...
```