



## Web 認証の管理

---

- Web 認証証明書の入手, 1 ページ
- Web 認証プロセス, 3 ページ
- デフォルトの Web 認証ログイン ページの選択, 6 ページ
- 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, 14 ページ
- 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, 15 ページ
- 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, 19 ページ
- スリープ状態にあるクライアントの認証の設定, 22 ページ

## Web 認証証明書の入手

### Web 認証証明書について

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。

### チェーン証明書のサポート

Cisco WLC では、Web 認証用にデバイス証明書をチェーン証明書としてダウンロードできます（レベル 2 まで）。ワイルドカード証明書もサポートされます。チェーン証明書の詳細については、[http://www.cisco.com/en/US/products/ps6366/products\\_configuration\\_example09186a0080a77592.shtml](http://www.cisco.com/en/US/products/ps6366/products_configuration_example09186a0080a77592.shtml)で『Generate CSR for Third-Party Certificates and Download Chained Certificates to the WLC』を参照してください。

## Web 認証証明書の入手 (GUI)

- 
- 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。このページには、現在の Web 認証証明書の詳細が表示されます。
- 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。
- [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。
  - 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。
- 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。
  - [Download SSL Certificate] チェックボックスをオンにします。
  - [Server IP Address] テキスト ボックスに、TFTP サーバの IP アドレスを入力します。  
[Maximum Retries] テキスト ボックスの 10 回の再試行および [Timeout] テキスト ボックスの 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。
  - 各ダウンロードを試行できる最大回数を [Maximum Retries] テキスト ボックスに入力し、各ダウンロードに許容される時間 (秒単位) を [Timeout] テキスト ボックスに入力します。
  - [Certificate File Path] テキスト ボックスに、証明書のディレクトリ パスを入力します。
  - [Certificate File Name] テキスト ボックスに、証明書の名前を入力します (**certname.pem**)。
  - [Certificate Password] テキスト ボックスに、証明書のパスワードを入力します。
  - [Apply] をクリックして、変更を確定します。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。
  - 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。
- 

## Web 認証証明書の入手 (CLI)

- 
- ステップ 1** 次のコマンドを入力して、現在の Web 認証証明書を表示します。
- show certificate summary**

以下に類似した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 Common Name (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) にすることを推奨します。

- 1 次のコマンドを入力して、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。

- 2 次のコマンドを入力して、ダウンロードプロセスを開始します。

```
transfer download start
```

- 3 次のコマンドを入力して、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。

```
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、ワイヤレス 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。



- (注) クライアントが使用する DNS 解決済みアドレスが 20 を超えると、コントローラは、Mobile Station Control Block (MSCB) テーブルの最初のアドレス空間で 21 番目のアドレスを上書きしますが、最初のアドレスはクライアントに保持されます。クライアントが最初のアドレスを再び使用しようとする、コントローラにはクライアントの MSCB テーブルの許可アドレスリストにこのアドレスがないため、使用できません。



- (注) ワンタイム パスワード (OTP) は、Web 認証ではサポートされていません。

## Web 認証プロセスのセキュリティ アラートの無効化

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 1：一般的な Web ブラウザセキュリティ警告ウィンドウ



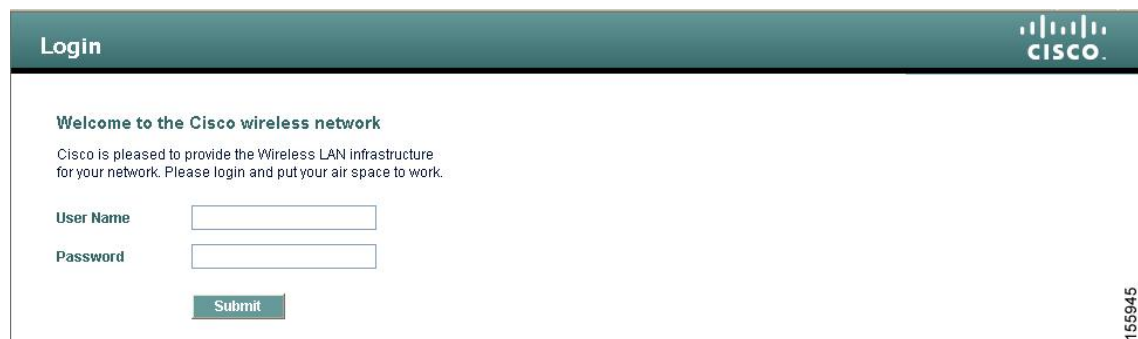
- (注) VPN ユーザを許可するよう設定されている事前認証 ACL でクライアントが WebAuth SSID に接続すると、クライアントは数分ごとに SSID から切断されます。Webauth SSID の接続には、Web ページでの認証が必要です。

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。

- 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 [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 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。  
コントローラの自己署名証明書の issuer テキストボックスは空白であるため、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 10 PC をリブートします。次回 Web 認証を試みるときは、ログイン ページが表示されます。

次の図は、デフォルトの Web 認証ログイン ページを示しています。

図 2: デフォルトの Web 認証ログイン ページ



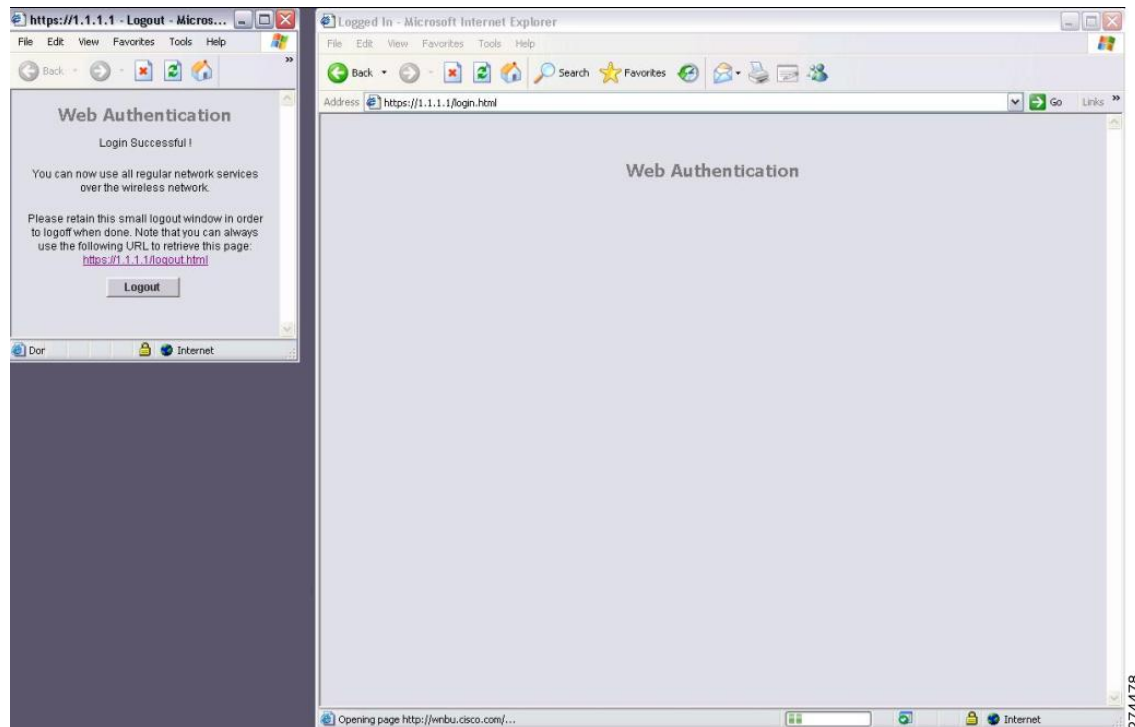
デフォルトのログイン ページには、Cisco ロゴや Cisco 特有のテキストが表示されます。Web 認証システムが次のいずれかを表示するように選択できます。

- 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

デフォルトの Web 認証ログイン ページのセクションを選択すると、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 3：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、`https://<IP address>/logout.html` 形式で仮想ゲートウェイ アドレスの URL へのポインタが表示されます。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。

## 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 ページについて

内部コントローラの Web サーバによって処理されるカスタムの webauth bundle を使用する場合は、ページに 5 つを超える要素（HTML、CSS、イメージなど）を含めることはできません。これは、内部コントローラの Web サーバが実装する DoS 保護メカニズムにより、各クライアントが開く同時 TCP 接続が負荷に応じて最大 5 つに制限されるためです。ブラウザが DoS 保護を処理する方法によっては、ページに多くの要素が含まれているためにページのロードが遅くなること

があり、一部のブラウザは、同時に 5 つを超える TCP セッションを開こうとすることがあります (Firefox 4 など)。

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 以降のリリースなどに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 [disabled] です。



(注) Cisco TAC はカスタム Web 認証バンドルを作成する責任を負いません。

複雑なカスタムの Web 認証モジュールが存在する場合は、コントローラ上の外部 Web 認証設定を使用して、完全なログインページが外部 Web サーバでホストされるようにすることを推奨します。

## デフォルトの Web 認証ログイン ページの選択 (GUI)

- ステップ 1 [Security] > [Web Auth] > [Web Login Page] の順に選択して、[Web Login] ページを開きます。
- ステップ 2 [Web Authentication Type] ドロップダウン リストから [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は、[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] テキスト ボックスに必要な URL 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] テキスト ボックス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] テキスト ボックス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、変更を確定します。
- 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。

## デフォルトの Web 認証ログイン ページの選択 (CLI)

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

```
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は、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** コマンドを入力します。

(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ダ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。デフォルトのヘッダラインは、「Welcome to the Cisco wireless network」です。ヘッダラインをデフォルトの設定に戻すには、**clear webtitle** コマンドを入力します。

**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** コマンドを入力します。

**ステップ 7** [web authentication logout] ポップアップ ウィンドウ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 custom-web logout-popup {enable | disable}
```

**ステップ 8** **save config** コマンドを入力して、設定を保存します。

**ステップ 9** 次の手順で独自のロゴを Web 認証ログイン ページにインポートします。

1 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ときには、次のガイドラインに従ってください。

- 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 サーバを Cisco Prime Infrastructure と同じ PC 上で実行することはできません。Prime Infrastructure 内蔵 TFTP サーバとサードパーティの TFTP サーバのどちらも、同じ通信ポートを使用するからです。

- 2 次のコマンドを入力して、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。

**ping ip-address**

- 3 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。

- 4 次のコマンドを入力して、ダウンロード モードを指定します。

**transfer download mode tftp**

- 5 次のコマンドを入力して、ダウンロードするファイルのタイプを指定します。

**transfer download datatype image**

- 6 次のコマンドを入力して、TFTP サーバの IP アドレスを指定します。

**transfer download serverip tftp-server-ip-address**

(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。

- 7 次のコマンドを入力して、ダウンロード パスを指定します。

**transfer download path absolute-tftp-server-path-to-file**

- 8 次のコマンドを入力して、ダウンロードするファイルを指定します。

**transfer download filename {filename.jpg | filename.gif | filename.png}**

- 9 次のコマンドを入力して、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。

**transfer download start**

- 10 次のコマンドを入力して、設定を保存します。

**save config**

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

ステップ 10 「Web 認証ログイン ページの設定の確認 (CLI) , (19 ページ)」の項の指示に従って、設定を確認します。

## 例：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 = "";

    if (document.forms[0].action == "") {
        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);
        }
        document.forms[0].action = args.switch_url;
    }

    if(equalIndex >= 0) {
        equalIndex += searchString.length;
        redirectUrl = "";
        redirectUrl += link.substring(equalIndex);
    }
    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
```

[illegible]

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。

使用できるステータス 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.」
- 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.」
- 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?」
- ステータス コード 4：「You have been excluded.」
- ステータス コード 5：「The User Name and Password combination you have entered is invalid. Please try again.」



---

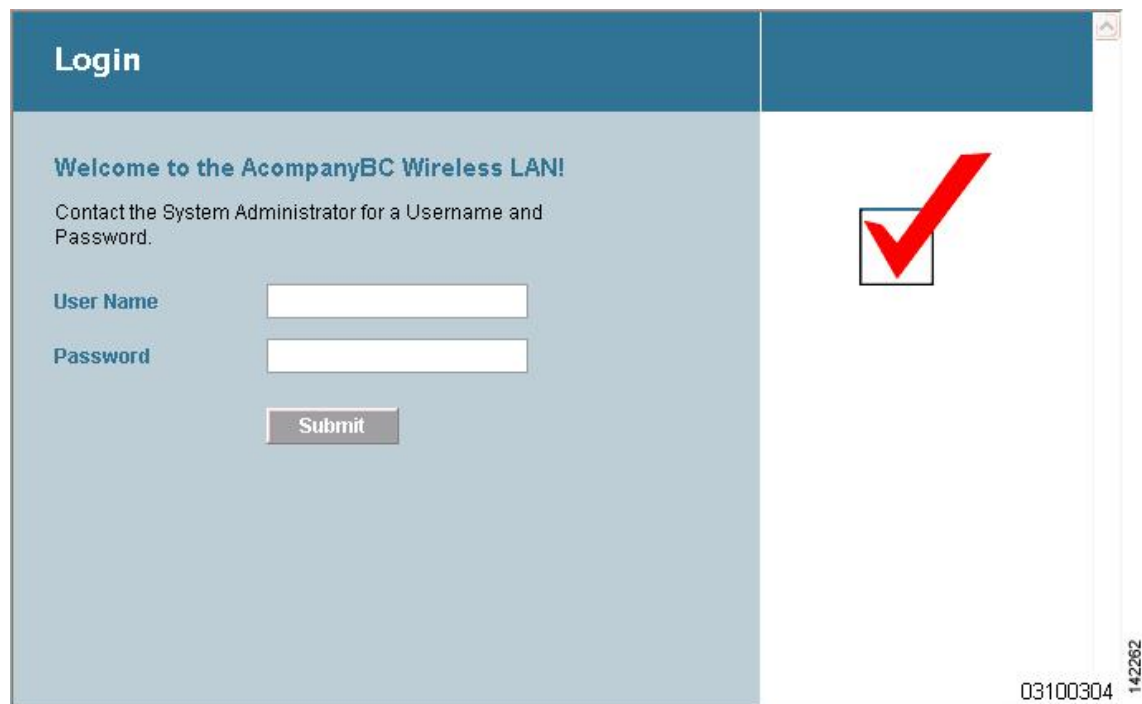
(注) 詳細については、次の URL にある『*External Web Authentication with Wireless LAN Controllers Configuration Example*』を参照してください。 [http://www.cisco.com/en/US/tech/tk722/tk809/technologies\\_configuration\\_example09186a008076f974.shtml](http://www.cisco.com/en/US/tech/tk722/tk809/technologies_configuration_example09186a008076f974.shtml)

---

## 例：変更されたデフォルトの Web 認証ログイン ページの例

次の図に、変更されたデフォルトの Web 認証ログイン ページの例を示します。

図 4：変更されたデフォルトの Web 認証ログイン ページの例



The screenshot shows a web browser window displaying a custom login page. The page has a blue header with the word "Login". Below the header, the text "Welcome to the AcompanyBC Wireless LAN!" is displayed in blue. Underneath, it says "Contact the System Administrator for a Username and Password." There are two input fields: "User Name" and "Password". Below these fields is a "Submit" button. A large red checkmark is overlaid on the right side of the page. The bottom right corner of the page shows the text "03100304" and "142262".

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した。

- `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`
- `config custom-web redirecturl url`

# 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

## カスタマイズされた Web 認証ログイン ページについて

Web 認証ログイン ページをカスタマイズして、外部 Web サーバにリダイレクトすることができます。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。

外部 Web サーバに対して、WLAN 上で事前認証アクセスコントロールリスト (ACL) を設定し、[Security Policies > Web Policy on the WLANs > Edit] ページで、WLAN 事前認証 ACL としてこの ACL を選択する必要があります。

## 外部 Web サーバでのカスタマイズされた Web 認証ログイン ページの選択 (GUI)

- 
- ステップ 1 [Security] > [Web Auth] > [Web Login Page] の順に選択して、[Web Login] ページを開きます。
  - ステップ 2 [Web Authentication Type] ドロップダウン リストから [External (Redirect to external server)] を選択します。
  - ステップ 3 [Redirect URL after login] テキスト ボックスに、ログイン後にユーザをリダイレクトさせる URL を入力します。  
たとえば、会社の URL を入力すると、ユーザがログインした後にその URL へ転送されます。最大入力長は 254 文字です。デフォルトでは、ユーザは、ログイン ページが機能する前にユーザのブラウザに入力された URL にリダイレクトされます。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 [External Webauth URL] テキスト ボックスに、外部 Web 認証に使用する URL を入力します。
  - ステップ 5 [Apply] をクリックします。
  - ステップ 6 [Save Configuration] をクリックします。
-

## 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選択 (CLI)

- ステップ 1 次のコマンドを入力して、Web 認証タイプを指定します。
- ```
config custom-web webauth_type external
```
- ステップ 2 次のコマンドを入力して、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 次のコマンドを入力して、Web サーバの IP アドレスを指定します。
- ```
config custom-web ext-webserver {add | delete} server_IP_address
```
- ステップ 4 **save config** コマンドを入力して、設定を保存します。
- ステップ 5 「[Web 認証ログインページの設定の確認 \(CLI\)](#) , (19 ページ)」の項の指示に従って、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、展開済みファイルとして取り込まれます。

ログインページ例を Cisco Prime インフラストラクチャからダウンロードし、カスタマイズされたログイン・ページの開始点として利用できます。詳細については、Cisco Prime インフラストラクチャのドキュメントを参照してください。



(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推奨します。



- (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。



- (注) カスタマイズされた webauth bundle に異なる要素が 4 つ以上含まれる場合は、コントローラ上の TCP レート制限ポリシーが原因で発生するページの読み込み上の問題を防ぐために、外部サーバを使用してください。

## カスタマイズされた Web 認証ログイン ページのダウンロードの前提条件

- ログイン ページの名前を login.html とします。コントローラは、この名前に基づいて 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テキスト ボックスを提供する。
- 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ているすべてのパス（たとえば、イメージを参照するパス）を確認する。
- バンドル内のすべてのファイル名が 30 文字以内であることを確認する。

## 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（GUI）

- ステップ 1** ログイン ページが含まれる .tar ファイルを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 2** [Commands] > [Download File] の順に選択して、[Download File to Controller] ページを開きます。
- ステップ 3** [File Type] ドロップダウン リストから、[Webauth Bundle] を選択します。
- ステップ 4** [Transfer Mode] ドロップダウン リストで、次のオプションから選択します。
- TFTP
  - FTP



- SFTP (7.4 以降のリリースで利用可能)

- ステップ 5** [IP Address] テキスト ボックスに、サーバの IP アドレスを入力します。
- ステップ 6** 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] テキスト ボックスに入力します。  
指定できる範囲は 1 ～ 254 です。  
デフォルトは 10 です。
- 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試行がタイムアウトするまでの時間 (秒数) を [Timeout] テキスト ボックスに入力します。  
指定できる範囲は 1 ～ 254 秒です。  
デフォルトは 6 秒です。
- ステップ 8** [File Path] テキスト ボックスに、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] テキスト ボックスに、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** FTP サーバを使用している場合は、次の手順に従います。
- 1 [Server Login Username] テキスト ボックスに、FTP サーバにログインするためのユーザ名を入力します。
  - 2 [Server Login Password] テキスト ボックスに、FTP サーバにログインするためのパスワードを入力します。
  - 3 [Server Port Number] テキスト ボックスに、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 11** [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 12** [Security] > [Web Auth] > [Web Login Page] の順に選択して、[Web Login] ページを開きます。
- ステップ 13** [Web Authentication Type] ドロップダウン リストから [Customized (Downloaded)] を選択します。
- ステップ 14** [Apply] をクリックします。
- ステップ 15** [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 16** 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 (CLI)

- ステップ 1** ログイン ページが含まれる .tar ファイルを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 2** 次のコマンドを入力して、ダウンロード モードを指定します。
- ```
transfer download mode {tftp | ftp | sftp}
```

- ステップ 3** 次のコマンドを入力して、ダウンロードするファイルのタイプを指定します。  
**transfer download datatype webauthbundle**
- ステップ 4** 次のコマンドを入力して、TFTP サーバの IP アドレスを指定します。  
**transfer download serverip tftp-server-ip-address**  
 (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 5** 次のコマンドを入力して、ダウンロードパスを指定します。  
**transfer download path absolute-tftp-server-path-to-file**
- ステップ 6** 次のコマンドを入力して、ダウンロードするファイルを指定します。  
**transfer download filename filename.tar**
- ステップ 7** 次のコマンドを入力して、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。  
**transfer download start**
- ステップ 8** 次のコマンドを入力して、Web 認証タイプを指定します。  
**config custom-web webauth\_type customized**
- ステップ 9** **save config** コマンドを入力して、設定を保存します。

## 例：カスタマイズされた Web 認証ログイン ページ

次の図に、カスタマイズされた Web 認証ログイン ページの例を示します。

図 5: カスタマイズされた Web 認証ログイン ページの例

## Web 認証ログイン ページの設定の確認 (CLI)

次のコマンドを入力して、Web 認証ログイン ページに対する変更内容を確認します。

```
show custom-web
```

## 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

### 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 ページの割り当てについて

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。

## 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 (GUI)

- 
- 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 グローバル認証設定 Web 認証ページを無効にするには、[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 リストが表示されたら、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 リストが表示されます。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 リストで [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。

- [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] テキスト ボックスに外部サーバの 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 リストから最大 3 つの RADIUS サーバおよび LDAP サーバを選択します。

(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** 次の手順で、Web 認証で接続するサーバの優先順位を指定します。

(注) デフォルトでは、[Local]、[RADIUS]、[LDAP] の順になっています。

- 1 [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。
- 2 希望のサーバタイプがボックスの先頭になるまで、[Up] および [Down] をクリックします。
- 3 [<] 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。
- 4 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、変更を確定します。

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

## 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 (CLI)

**ステップ 1** 次のコマンドを入力して、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** 次のコマンドを入力して外部サーバの URL を指定することにより、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します。

**config wlan custom-web ext-webauth-url** *ext\_web\_url wlan\_id*

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

**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** 次のコマンドを入力して、無線ゲスト ユーザ用の Web 認証 ページを定義します。

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

値は次のとおりです。

- **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 で設定した URL にユーザをリダイレクトします。

**ステップ 6** 次のコマンドを入力して、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 レベルで使用されます。

**ステップ 7** 次のコマンドを入力して、変更を保存します。  
**save config**

## スリープ状態にあるクライアントの認証の設定

### スリープ状態にあるクライアントの認証について

Web 認証に成功したゲストアクセスを持つクライアントは、ログインページから別の認証プロセスを実行せずにスリープおよび復帰することを許可されています。再認証が必要になるまでスリープ状態にあるクライアントが記録される期間を設定できます。有効な範囲は 1 時間から 720 時間 (30 日) で、デフォルトは 12 時間です。WLAN にマッピングされるユーザ グループ ポリシーと WLAN に、期間を設定できます。スリープ タイマーは、アイドル タイムアウト後に有効になります。クライアント タイムアウトが WLAN のスリープ タイマーに設定された時間より短い場合、クライアントのライフタイムがスリープ時間として使用されます。



(注) スリープ タイマーは 6 分ごとに期限切れになります。

この機能は FlexConnect のローカルスイッチング、中央認証のシナリオでサポートされています。



**注意** スリープ モードに切り替わったクライアント MAC アドレスがスプーフィングされた場合、ラップトップなどの偽のデバイスを認証することができます。

次に、モビリティ シナリオでの注意事項を示します。

- 同じサブネットの L2 ローミングがサポートされています。
- アンカー スリープ タイマーを適用できます。
- スリープ状態にあるクライアントの情報は、クライアントがアンカー間を移動する場合に、複数の自動アンカー間で共有されます。

リリース 8.0 以降のハイ アベイラビリティ シナリオでは、スリープ タイマーがアクティブとスタンバイの間で同期されます。

#### サポートされるモビリティ シナリオ

スリープ状態にあるクライアントは、次のシナリオでは再認証が必要ありません。

- モビリティ グループに 2 台のコントローラがあるとしします。1 台のコントローラに関連付けられているクライアントがスリープ状態になり、その後復帰して他方のコントローラに関連付けられます。

- モビリティ グループに 3 台のコントローラがあるとしします。1 台目のコントローラにアンカーされた 2 台目のコントローラに関連付けられたクライアントは、スリープ状態から復帰して、3 台目のコントローラに関連付けられます。
- クライアントはスリープ状態から復帰して、エクスポートアンカーにアンカーされた同じまたは別のエクスポート外部コントローラに関連付けられます。

## スリープ状態にあるクライアントの認証に関する制限

- スリープ状態にあるクライアントは WLAN ごとにのみ設定できます。
- スリープ状態にあるクライアントの認証機能は、レイヤ 2 セキュリティおよび Web 認証が有効な場合はサポートされません。
- スリープ状態にあるクライアントの認証機能は、レイヤ 3 セキュリティが有効な WLAN でのみサポートされています。
- スリープ状態にあるクライアントの中央 Web 認証はサポートされていません。
- スリープ状態にあるクライアントの認証機能は、ゲスト LAN およびリモート LAN ではサポートされていません。
- ローカル ユーザ ポリシーを持つスリープ状態のゲスト アクセス クライアントはサポートされません。この場合、WLAN 固有のタイマーが適用されます。
- ハイ アベイラビリティのシナリオでは、クライアント エントリがアクティブとスタンバイの間で同期されますが、スリープ タイマーは同期されません。アクティブ コントローラに障害が発生した場合、クライアントはスタンバイ コントローラにアソシエートするときに再認証される必要があります。
- サポートされるスリープ状態にあるクライアントの数は、コントローラプラットフォームによって異なります。
  - Cisco 2500 シリーズ ワイヤレス LAN コントローラ : 500
  - Cisco 5500 シリーズ ワイヤレス LAN コントローラ : 1000
  - Cisco Flex 7500 シリーズ ワイヤレス LAN コントローラ : 9000
  - Cisco 8500 シリーズ ワイヤレス LAN コントローラ : 9000
  - Cisco WiSM2 : 1000
  - Cisco 仮想ワイヤレス LAN コントローラ : 500
  - Cisco Services Ready Engine (SRE) の Cisco ワイヤレス コントローラ : 500
- 新しいモビリティはサポートされていません。

## スリープ状態のクライアントの認証の設定 (GUI)

- 
- ステップ 1** [WLANs] を選択します。
- ステップ 2** 対応する WLAN ID をクリックします。  
[WLANs > Edit] ページが表示されます。
- ステップ 3** [Security] タブをクリックして、[Layer 3] タブをクリックします。
- ステップ 4** スリープ状態のクライアントに対する認証を有効にするには、[Sleeping Client] チェックボックスをオンにします。
- ステップ 5** 再認証が必要になる前にスリープ状態にあるクライアントを記録する期間を [Sleeping Client Timeout] に入力します。  
デフォルトのタイムアウトは 12 時間です。
- ステップ 6** [Apply] をクリックします。
- ステップ 7** [Save Configuration] をクリックします。
- 

## スリープ状態のクライアントの認証の設定 (CLI)

- 次のコマンドを入力して、WLAN のスリープ状態のクライアントの認証を有効または無効にします。  
**config wlan custom-web sleep-client {enable | disable} wlan-id**
- 次のコマンドを入力して、WLAN にスリープ状態のクライアントのタイムアウトを設定します。  
**config wlan custom-web sleep-client timeout wlan-id duration**
- 次のコマンドを入力して、WLAN のスリープ状態のクライアントの設定を表示します。  
**show wlan wlan-id**
- 次のコマンドを入力して、不要なスリープ状態のクライアントのエントリを削除します。  
**config custom-web sleep-client delete client-mac-addr**
- 次のコマンドを入力して、すべてのスリープ状態にあるクライアントのエントリの要約を表示します。  
**show custom-web sleep-client summary**
- 次のコマンドを入力して、クライアント MAC アドレスに基づいてスリープ状態にあるクライアントのエントリの詳細を表示します。  
**show custom-web sleep-client detail client-mac-addr**