

WAP125およびWAP581の1.0.1リリースの機能

目的

この記事の目的は、ワイヤレスアクセスポイント(WAP)のファームウェアアップデートの新機能を強調し、概要を説明することです。

該当するデバイス

- WAP125
- WAP581

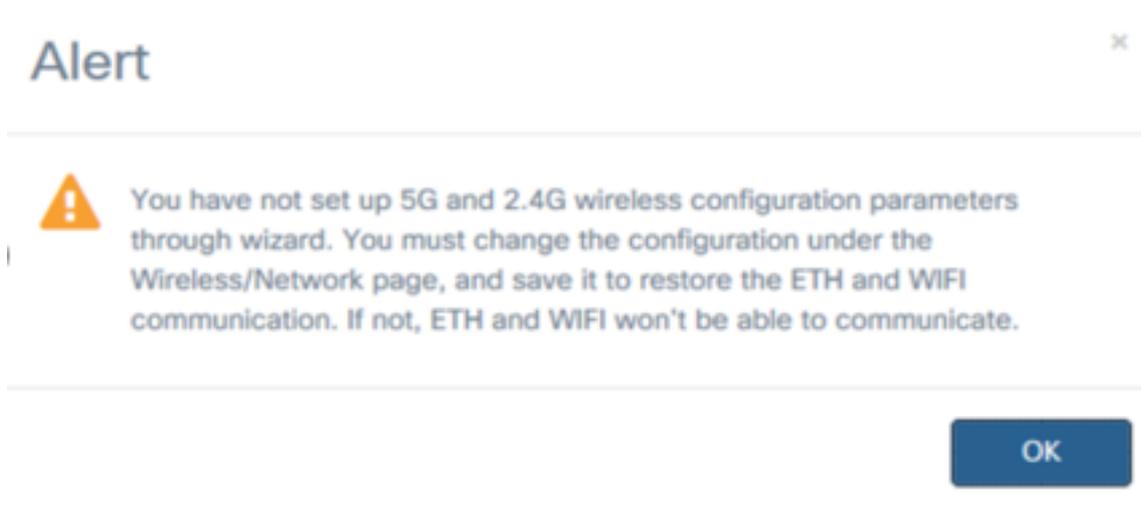
[Software Version]

- 1.0.1

セットアップウィザード

以前のバージョンのWAP125およびWAP581では、セットアップウィザードをキャンセルすると、WAPからログアウトされます。

1.0.1ファームウェアでは、セットアップウィザードをキャンセルできます。アラートが送信されます。



アラートの確認後、WAPのローカルパスワードを設定できます。

Change Password

You may also change the username. A valid username contains 1-32 alphanumeric, hyphens, or underscore characters.

Username:

For security reasons, you should change the password from its default settings.

The minimum requirements are as follows:

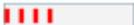
- * Cannot be the same as the user name.
- * Cannot be the same as the current password.
- * Minimum length is 8.
- * Minimum number of character classes is 3.

Character classes are upper case, lower case, numeric, and special characters.

Old Password:

New Password:

Confirm Password:

Password Strength Meter  Below Minimum

Password Complexity: Disable

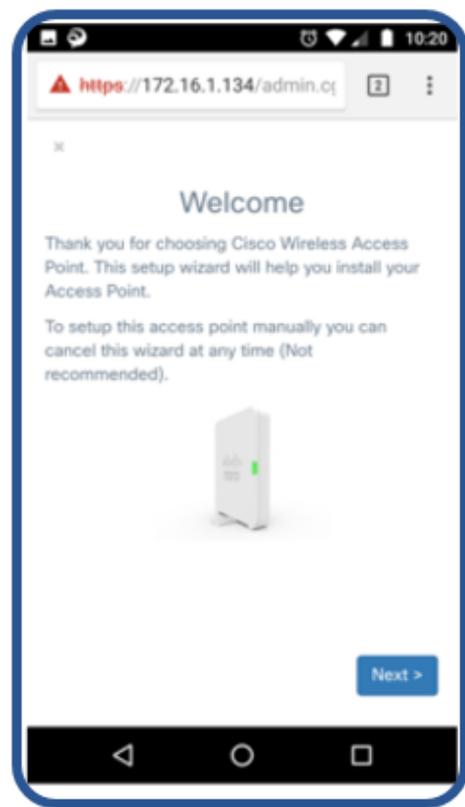
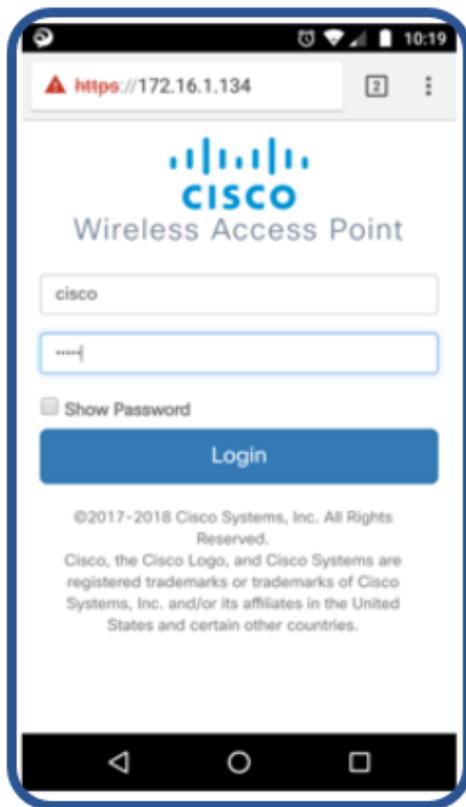
すべての設定を別の時点で手動で設定できます。

モバイル最適化セットアップウィザード

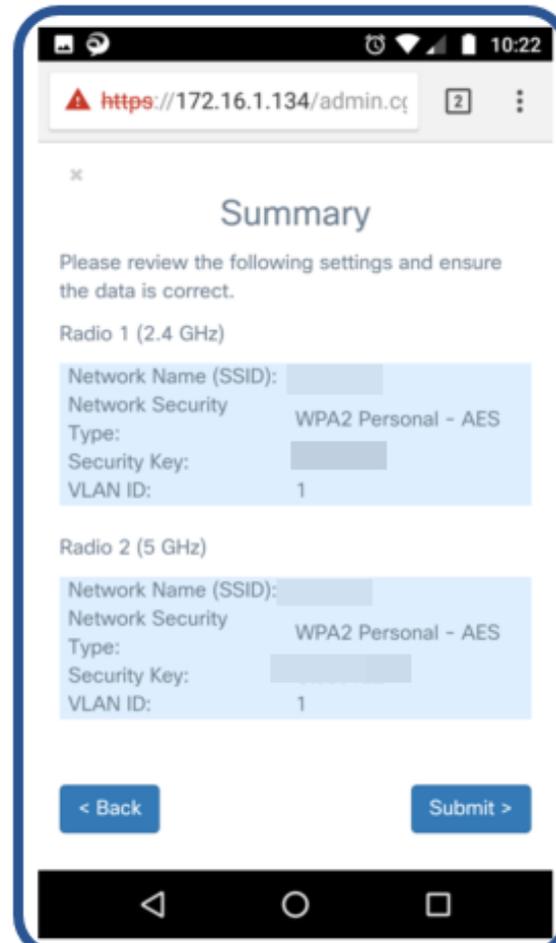
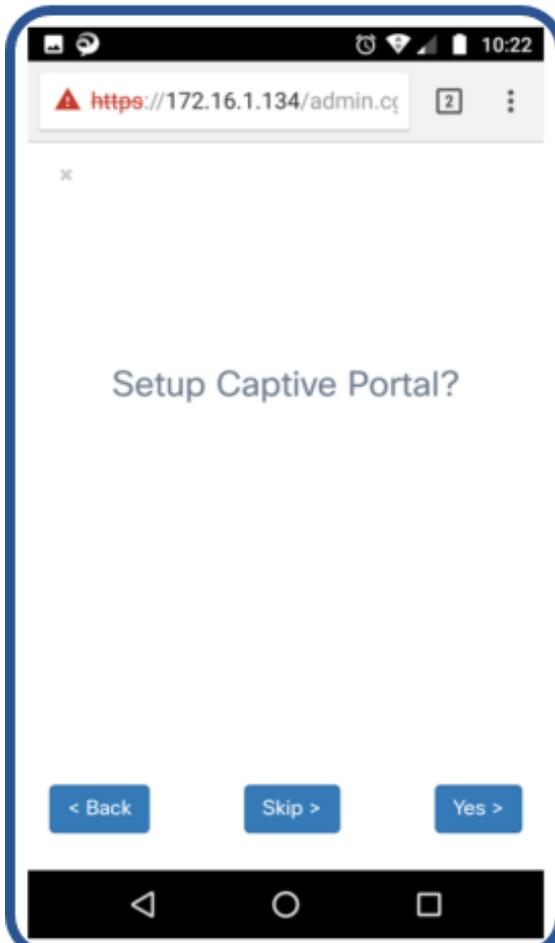
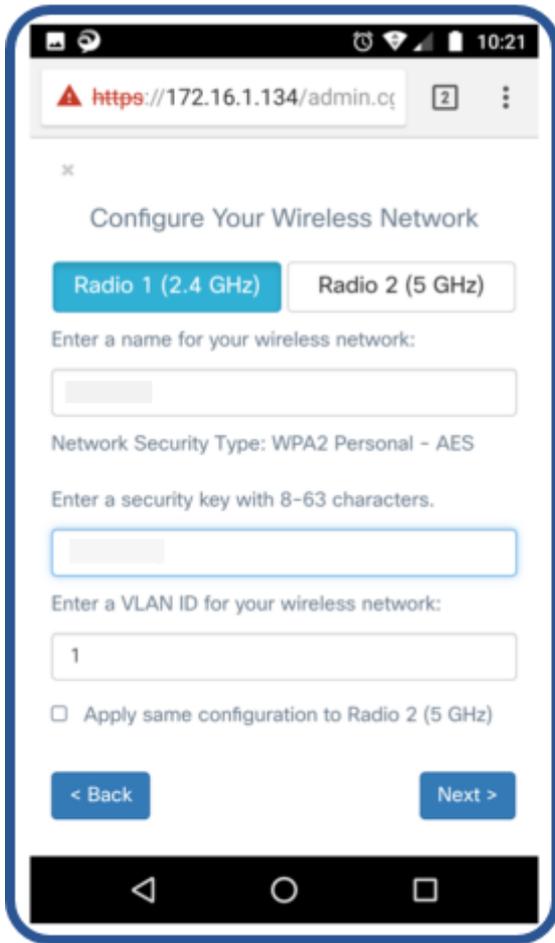
WAP125およびWAP581デバイスには、管理ページ、キャプティブポータルページ、およびモバイルデバイス用に最適化されたセットアップウィザードが含まれています。

新しいモバイル最適化セットアップページを使用して、モバイルデバイスからセットアップウィザードを実行してWAPを設定できます。

ciscoSB-Setup SSIDに接続し、WAPのIPアドレスまたはデフォルトIP 192.168.1.245に移動してデバイスを設定します。



セットアップウィザードは、モバイル最適化ページの標準ページと同じです。



サードパーティゲスト認証

サードパーティのゲスト認証では、FacebookまたはGoogle認証を使用してゲストネットワークを設定できます。これは、サードパーティによって検証されたセキュアな認証です。WAP125では1つのゲストアクセスインスタンスが許可され、WAP581では複数のインスタンスが許可されます。

要件：

- FacebookまたはGoogleへのインターネット接続
- ユーザは、パブリックプロフィールへのFacebookまたはGoogleアカウントとワイヤレスアクセスを所有または作成する必要があります
- エンドユーザがログインしてクレデンシャルを検証できるようにするには、認証が完了する前にFacebookまたはGoogleにアクセスできる必要があります。

企業は、認証の前にビジネスWebサイトなどの他のサイトを使用することもできます。

[Access Control] > [Guest Access]をクリックし、プラス記号をクリックします。

次の各番号について簡単に説明します。

1. Active Directoryの名前を追加します
2. キャプティブポータルページを設定して、HTTPではなくHTTPSを使用するようにします。HTTPを選択すると、暗号化されていないクリアテキストでユーザ名とパスワードを空中で送信することによって、誤ってユーザ名とパスワードを公開してしまう可能性があります。セキュアなHTTPSキャプティブポータルページが推奨されます。
3. [Rd Party Credentials]を選択します。
4. 目のグラフィックをクリックして、認可された認証情報と正しいWebサイトを選択します。
5. ここで、別のゲストアクセスインスタンスを追加する場合にクリックします。
6. 必ず保存してください。

Enable	Guest Access Instance	Protocol	Authentication Method	Guest Group	Redirect URL	Session Timeout (Min)	Web Portal Locale
<input checked="" type="checkbox"/>	AD	HT	443	Active D	Default	0	Default

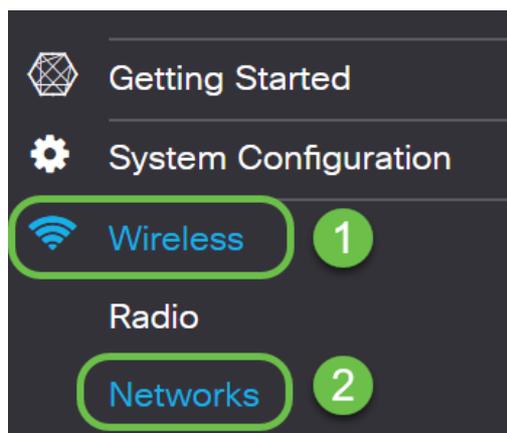
この例では、FacebookとGoogleが選択されています。WebサイトはWalled Gardenに掲載されています。

3rd Party Credentials

Accepted credentials: Facebook Google

Walled Garden:

次に、ナビゲーションペインで[Wireless] > [Networks]に移動し、ゲストアクセスインスタンスをActive Directoryの名前に追加または変更する必要があります。

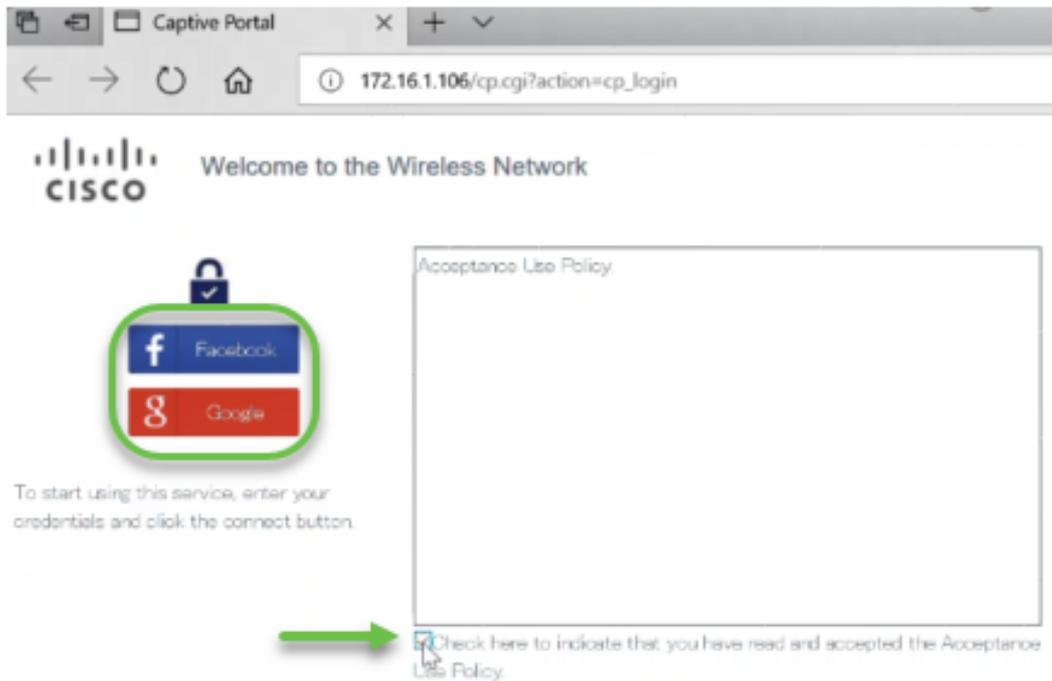


注：WAP125では1つのゲストアクセスインスタンスを使用できるため、サードパーティ認証またはActive Directory認証のどちらに設定するかを決定する必要があります。WAP581では、複数の認証手段を使用できます。

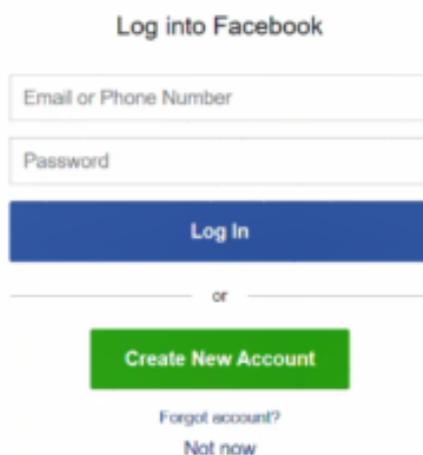
サードパーティクライアント認証

クライアントがクリックしてワイヤレス接続に参加すると、キャプティブポータルが開きます。この例では、FacebookとGoogleがオプションです。お客様は、受け入れ使用ポリシーを読み取って受け入れたことを示すボックスをオンにして、ログインするにはFacebookまたはGoogleオプションをオンにする必要があります。

注：クライアントに初めてログインすると、キャプティブポータルを使用するかどうかを尋ねる質問が表示されます。[はい]を選択する必要があります。



クライアントはクレデンシャルを入力できます。この例では、Facebookが使用されています。



これで、クライアントはインターネットを使用できるようになります。



Active Directoryゲスト認証

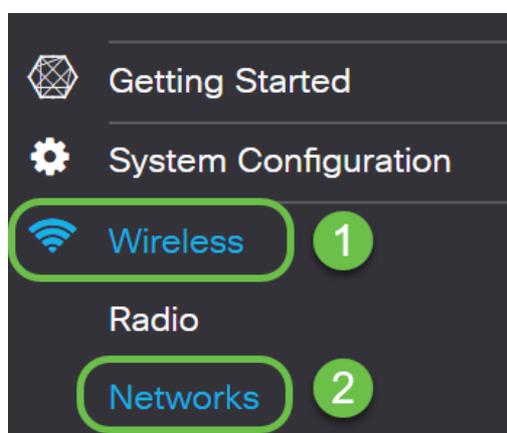
Active Directory認証をサポートするには、WAPが認証を提供するためにWindowsドメインコントローラと通信する必要があります。管理者は、WAP581上で通信できるように最大3つのWindowsドメインコントローラ(WDC)を設定できます。

[Access Control] > [Guest Access]をクリックし、プラス記号をクリックします。

次の各番号について簡単に説明します。

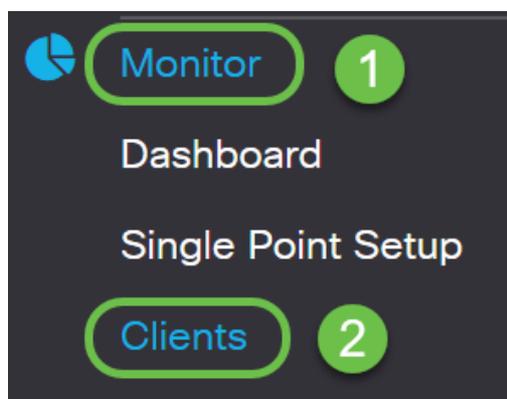
1. Active Directoryの名前を追加します
2. キャプティブポータルページを設定して、HTTPではなくHTTPSを使用するようにします。HTTPを選択すると、暗号化されていないクリアテキストでユーザ名とパスワードを空中で送信することによって、誤ってユーザ名とパスワードを公開してしまう可能性があります。セキュアなHTTPSキャプティブポータルページが推奨されます。
3. Active Directoryサービスの選択
4. 目の画像をクリックしてIPアドレスを追加します。そこからテストを実行して、接続を確認できます。
5. ここで、別のゲストアクセスインスタンスを追加する場合にクリックします。
6. 必ず保存してください。

次に、ナビゲーションペインで[Wireless] > [Networks]に移動し、ゲストアクセスインスタンスをActive Directoryの名前に追加または変更する必要があります。



ネットワーク上のクライアントを表示するには、ナビゲーションペインで[Monitor] > [Clients]をクリックします。

1. Monitorは、接続されているクライアントの数を示します
2. クライアントは、クライアントの詳細を表示します。接続している人の記録を保持する場合は、これらをエクスポートできます。

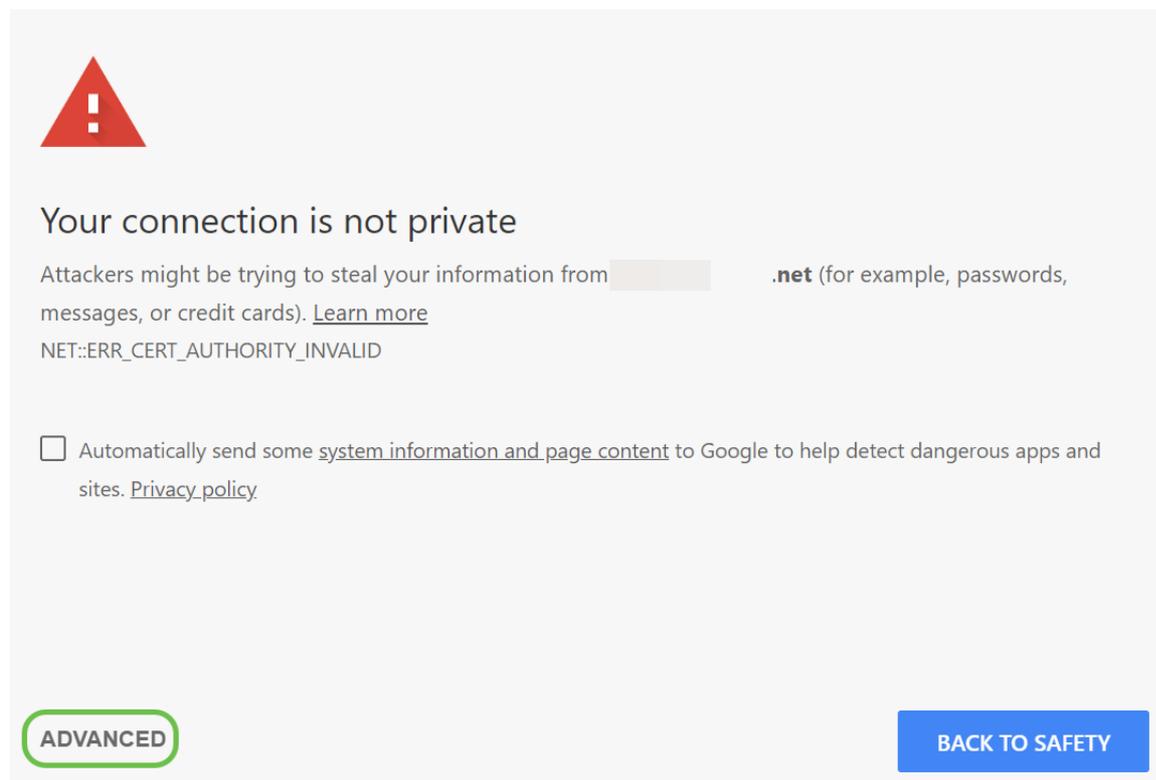


ゲストの監視方法の詳細については、[ここをクリックしてください](#)。

Active Directoryクライアント認証

クライアントがActive Directory内にある場合、WAPにログインしてインターネットにアクセスできます。ワイヤレスアクセスポイントを選択すると、使用しているWebブラウザによ

っては、次のような警告メッセージが表示されることがあります。この警告は、信頼できる認証局によってページに割り当てられた証明書がない場合に発生します。クライアントは [ADVANCED] をクリックする必要があります。





Your connection is not private

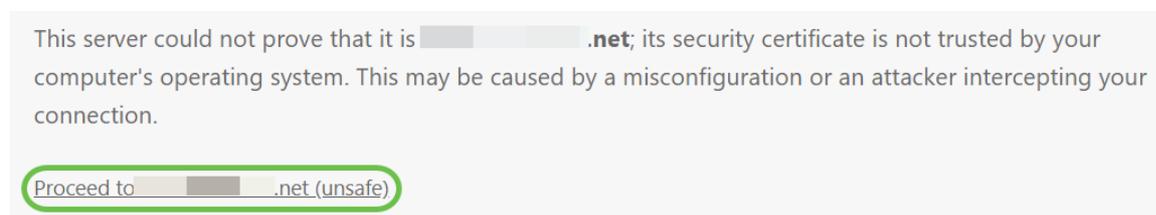
Attackers might be trying to steal your information from [redacted].net (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR_CERT_AUTHORITY_INVALID

Automatically send some [system information and page content](#) to Google to help detect dangerous apps and sites. [Privacy policy](#)

ADVANCED **BACK TO SAFETY**

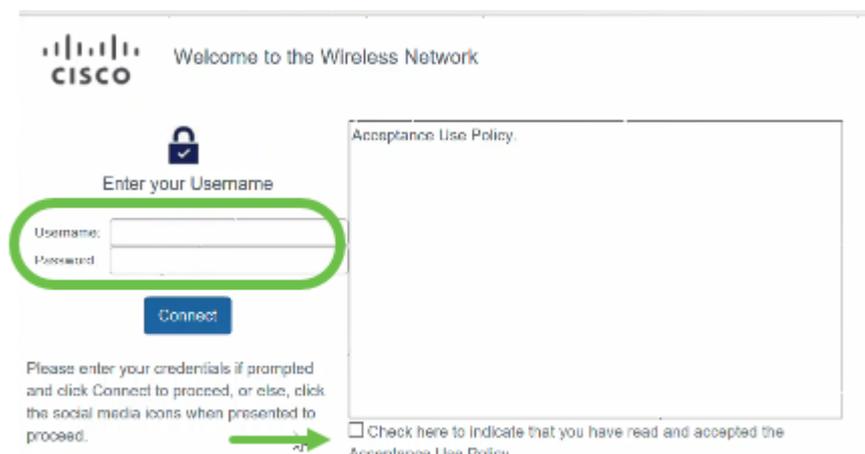
その後、クライアントに次のような警告メッセージが表示されることがあります。



This server could not prove that it is [redacted].net; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to [redacted].net (unsafe)

ポータルページが起動されました。このページでは、認証情報を入力し、チェックボックスをオンにして、承認使用ポリシーの読み取りと受け入れが完了したことを示します。



 Welcome to the Wireless Network

 Enter your Username

Username:

Password:

Connect

Please enter your credentials if prompted and click **Connect** to proceed, or else, click the social media icons when presented to proceed.

Check here to indicate that you have read and accepted the Acceptance Use Policy.

ウェルカムメッセージが届き、インターネットを安全に利用できるようになります。

Congratulations!

You are now authorized and connected to the network.



最新のWAP125およびWAP581アップデートに付属する最新の機能の一部を理解しました。

これらの機能およびその他の新機能の詳細については、以下の関連記事リンクをクリックしてください。

[WAP125またはWAP581でのセットアップウィザードの使用](#)

[WAP125またはWAP581のモバイルデバイスでのセットアップウィザードの使用](#)

[How To : Cisco Umbrella統合](#)

[How To : Cisco CloudSharkの統合](#)

[How To : WAP125またはWAP581でサードパーティ認証設定を設定する](#)

[How To : Microsoft Active Directoryゲスト認証](#)

[How To : Umbrella - APIキーシークレットを失った場合に新しいデバイスを登録する](#)

[キャプティブポータルの外観をカスタマイズするには](#)

[この記事に関連するビデオを表示...](#)

[シスコのその他のテクニカルトークを表示するには、ここをクリックしてください](#)