

# WAP571またはWAP571Eでのキャプティブポータルの設定

## 目的

キャプティブポータル(CP)では、ワイヤレスユーザが確認されるまで、ワイヤレスネットワークへのアクセスを制限できます。ユーザがWebブラウザを開くと、ログインページにリダイレクトされ、ユーザ名とパスワードを入力する必要があります。ネットワークへのアクセスを許可するユーザには、次の2種類があります。認証されたユーザとゲスト認証されたユーザは、ローカルデータベースまたはRADIUSサーバのデータベースに一致するユーザ名とパスワードを入力する必要があります。ユーザ名やパスワードを入力する必要はありません。

この記事では、ワイヤレスアクセスポイント(WAP)でキャプティブポータルを設定する方法について説明します。

## 該当するデバイス

- WAP500シリーズ – WAP571、WAP571E

## [Software Version]

- 1.0.0.15 - WAP571、WAP571E

## キャプティブポータルの設定

キャプティブポータルの基本設定はセットアップウィザードで設定でき、詳細設定はWebベースのユーティリティで設定できます。迅速で基本的なセットアップを行うには、セットアップウィザードを使用して機能を有効にします。次の手順を参照してください。

注：次の図は、WAP571からキャプチャしたものです。

### セットアップウィザードの使用

ステップ1:Webベースのユーティリティにログインし、[Run Setup Wizard]をクリックします。

**Getting Started**

**Run Setup Wizard**

- ▶ Status and Statistics
- ▶ Administration
- ▶ LAN
- ▶ Wireless
- ▶ Spectrum Analyzer
- ▶ System Security
- ▶ Client QoS
- ▶ ACL
- ▶ SNMP
- ▶ Captive Portal
- ▶ Single Point Setup

## Getting Started

Use the following links to quickly configure your access

### Initial Setup

- [Run Setup Wizard](#)
- [Configure Radio Settings](#)
- [Configure Wireless Network Settings](#)
- [Configure LAN Settings](#)
- [Configure Single Point Setup](#)

### Device Status

注：WAPを初めて設定する場合、セットアップウィザードが自動的にポップアップ表示されます。

ステップ2：セットアップウィザード画面の指示に従います。セットアップウィザードを使用してWAPを段階的に設定するには、[ここをクリックして手順を確認](#)してください。

## Welcome

Thank you for choosing Cisco Systems, Inc. This setup wizard will help you install your Cisco Systems, Inc Access Point.

To setup this access point manually you can cancel this wizard at any time (Not recommended).



**Note:** This Setup Wizard provides simplified options to help you quickly get your access point up and running. If there is any option or capability that you do not see while running the setup wizard, click the learning link provided on many of the setup wizard pages. To set further options as you require or as seen in the learning link, cancel the setup wizard and go to the web-based configuration utility.

Click **Next** to continue

Back

Next

Cancel

ステップ3:[Enable Captive Portal - Create Your Guest Network]画面が表示されたら、[Yes]を選択し、[Next]をクリックします。

## Enable Captive Portal - Create Your Guest Network

Use Captive Portal to set up a guest network, which means that wireless users need to be authenticated before they can access the Internet. For example, a hotel can create a guest network to redirect new wireless users to a page for authentication.

Do you want to create your guest network now?

- Yes  
 No, thanks.

[? Learn more about captive portal guest networks](#)

Click **Next** to continue

Back

Next

ステップ4 : ゲストネットワーク名を入力し、[Next]をクリックします。

注 : デフォルトのゲストネットワーク名はciscosb-guestです。

## Enable Captive Portal - Name Your Guest Network

Your guest network needs a new name, known as an SSID. The name identifies your guest network so that wireless users can find it.

Enter a name for your guest network:

- Radio:
- Radio 1 (5 GHz)
  - Radio 2 (2.4 GHz)

Guest Network name:

For example: MyGuestNetwork

[? Learn more about network names](#)

Click **Next** to continue

Back

Next

ステップ5 : ワイヤレスゲストネットワークのセキュリティタイプを選択します。

注 : 次の例では、最高のセキュリティ(WPA2 Personal - AES)が選択されています。

## Enable Captive Portal - Secure Your Guest Network

Select your guest network security strength.

- Best Security (WPA2 Personal - AES)**  
Recommended for new wireless computers and devices that support this option.  
Older wireless devices might not support this option.
- Better Security (WPA/WPA2 Personal - TKIP/AES)  
Recommended for older wireless computers and devices that might not support WPA2.
- No Security (Not recommended)

ステップ6 : セキュリティキーを入力し、[Next]をクリックします。

## Enable Captive Portal - Secure Your Guest Network

Select your guest network security strength.

- Best Security (WPA2 Personal - AES)  
Recommended for new wireless computers and devices that support this option.  
Older wireless devices might not support this option.
- Better Security (WPA/WPA2 Personal - TKIP/AES)  
Recommended for older wireless computers and devices that might not support WPA2.
- No Security (Not recommended)

Enter a security key with 8 - 63 characters.



Show Key as Clear Text

[? Learn more about your network security options](#)

Click **Next** to continue

Back

Next

ステップ7 : ゲストネットワークのVLAN IDを入力し、[Next]をクリックします。

## Enable Captive Portal - Assign The VLAN ID

We strongly recommend that you assign different VLAN ID for your guest network than the management VLAN ID. By doing that, your guest will have no access to your private network.

Enter a VLAN ID for your guest network:

VLAN ID:

Range: 1 - 4094)

[? Learn more about vlan ids](#)

Click **Next** to continue

Back

Next

ステップ8: ( オプション ) ユーザがウェルカムページからサービス利用規約に同意した後に表示する特定のWebページがある場合は、[リダイレクトURLを有効にする]チェックボックスをオンにします。URLを入力し、[次へ]をクリックします。

注 : URLは会社のWebサイトにすることができます。

## Enable Captive Portal - Enable Redirect URL

If you enable a redirect URL, when new wireless users have completed the authentication process, they can be redirected to an alternate startup page.

Enable Redirect URL

Redirect URL :

[? Learn more about redirect urls](#)

Click **Next** to continue

Back

Next

ステップ9 : 設定を確認して確認し、[送信]をクリックします。



## Summary - Confirm Your Settings

Security Key:	Cisco1234\$
VLAN ID:	1
Radio 2 (2.4 GHz)	
Network Name (SSID):	ciscosb
Network Security Type:	WPA2 Personal - AES
Security Key:	*****
VLAN ID:	1

### Captive Portal (Guest Network) Summary

Guest Network Radio:	Radio 1
Network Name (SSID):	ciscosb-guest
Network Security Type:	WPA2 Personal - AES
Security Key:	*****
Verification:	Guest
Redirect URL:	https://cisco.com

Click **Submit** to enable settings on your Cisco Systems, Inc Access Point

Back

Submit

ステップ10:[Device Setup Complete]画面が表示されたら、[Finish]をクリックしてセットアップウィザードを閉じます。

## Device Setup Complete



Congratulations, your access point has been set up successfully. We strongly recommend that you save these settings by writing them down or by copying and pasting them into a text document. You will need these settings later when you add other wireless computers or devices to your network.

Cluster Name:	ciscosb-cluster
Radio 1 (5 GHz)	
Network Name (SSID):	ciscosb
Network Security Type:	WPA2 Personal - AES
Security Key:	*****
Radio 2 (2.4 GHz)	
Network Name (SSID):	ciscosb
Network Security Type:	WPA2 Personal - AES
Security Key:	*****



Click **Finish** to close this wizard.

Back

Finish

これで、WAPのキャプティブポータル機能の基本設定が完了したはずですよ。

## Webベースユーティリティの使用

WAPでキャプティブポータルの詳細設定を設定するには、次の手順に従う必要があります。

キャプティブポータルをグローバルに有効にする：キャプティブポータルを有効にできません。

キャプティブポータルインスタンスの作成：キャプティブポータルインスタンスは、ユーザが仮想アクセスポイント(VAP)にログオンする方法を制御する一連のパラメータです。

キャプティブポータルインスタンスとVAPの関連付け：VAPにアクセスしようとするユーザは、インスタンスに設定されているパラメータに従う必要があります。

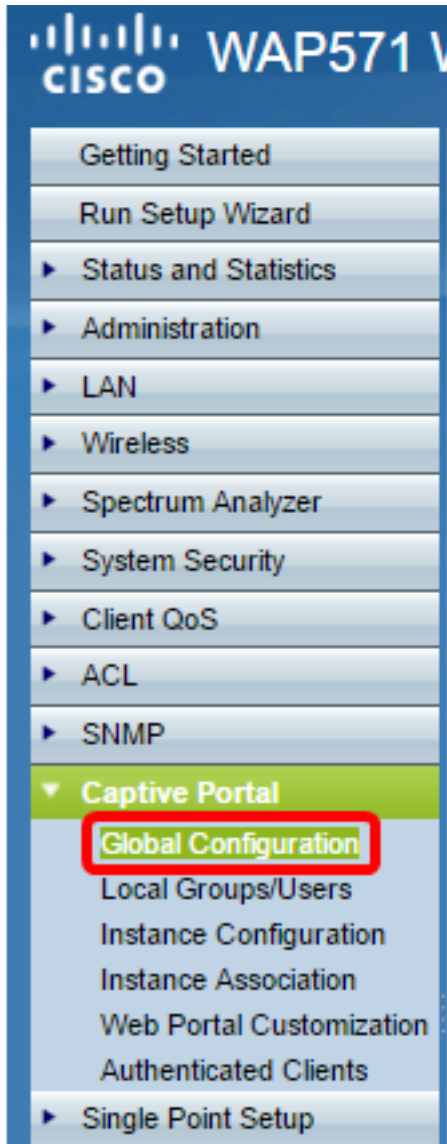
Webポータルのカスタマイズ：Webポータルは、ユーザがVAPにログインしようとするときリダイレクトされるWebページです。

[Create Local Group]：ローカルグループはインスタンスに割り当てることができます。このインスタンスは、そのグループに属するユーザを受け入れます。

[ローカルユーザの作成(Create Local User)] : ローカルユーザがローカルグループに追加され、グループが設定されているキャプティブポータルへのアクセスが許可されます。

## キャプティブポータルをグローバルに有効にする

ステップ1: Webベースのユーティリティで、[Captive Portal] > [Global Configuration]を選択します。



ステップ2: ( オプション ) WAPが認証セッションを閉じる前にユーザが認証情報を入力する必要がある秒数を[Authentication Timeout]フィールドに入力します。

## Global Configuration

Captive Portal Mode:  Enable

Authentication Timeout:  Sec (Range: 60 - 600, Default: 300)

Additional HTTP Port:  (Range: 1025 - 65535 or 80, 0 = Disable, Default: 0)

Additional HTTPS Port:  (Range: 1025 - 65535 or 443, 0 = Disable, Default: 0)

ステップ3: ( オプション ) WAPとクライアント間のHTTP情報に、デフォルト以外の別のポートを使用する場合は、追加するHTTPポート番号を[Additional HTTP Port]フィールドに入力します。HTTPおよびその他のインターネットプロトコルは、ポートを使用して、デバイスが特定のプロトコルの場所を認識していることを確認します。オプションは80、1025 ~ 65535です。無効にするには0を入力します。HTTPポートとHTTPSポートを同じにすることはできません。

ステップ4: ( オプション ) WAPとクライアント間のHTTP情報にデフォルト以外の別のポートを使用する場合は、追加するHTTPSポート番号を[Additional HTTPS Port]フィールドに入力します。オプションは443、1025 ~ 65535です。無効にするには0を入力します。HTTPポートとHTTPSポートを同じにすることはできません。

次の情報は[キャプティブポータル設定カウンタ(Captive Portal Configuration Counters)]エリアに表示され、設定できません。

Captive Portal Configuration Counters	
Instance Count:	0
Group Count:	1
User Count:	0

Instance Count:WAPデバイスで設定されたCPインスタンスの数。WAPには最大2つのCPを設定できます。

Group Count:WAPデバイスで設定されたCPグループの数。最大2つのグループを設定できます。デフォルトグループは削除できません。

[User Count]:WAPデバイスに設定されているCPユーザの数。WAPでは最大128ユーザを設定できます。

ステップ5:[Save]をクリックします。

注：変更内容がスタートアップコンフィギュレーションに保存されます。

## Global Configuration

Captive Portal Mode:  Enable

Authentication Timeout:  Sec (Range: 60 - 600, Default: 300)

Additional HTTP Port:  (Range: 1025 - 65535 or 80, 0 = Disable, Default: 0)

Additional HTTPS Port:  (Range: 1025 - 65535 or 443, 0 = Disable, Default: 0)

### Captive Portal Configuration Counters

Instance Count: 0

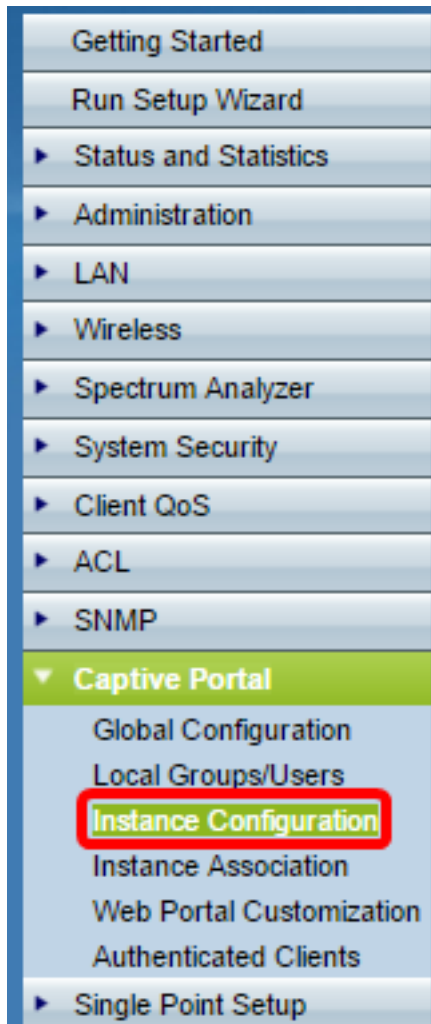
Group Count: 1

User Count: 0

Save

## インスタンス設定

ステップ6:Webベースのユーティリティで、[キャプティブポータル(Captive Portal)] > [インスタンス設定(Instance Configuration)]を選択します。



ステップ7:[Captive Portal Instances]ドロップダウンリストで、wiz-cp-inst1インスタンスに注目します。この名前を選択するか、インスタンス構成の新しい名前を作成できます。

ステップ8: ( オプション ) [インスタンス名]フィールドに構成の名前を入力し、[保存]をクリックします。

注：この例では、新しいインスタンスが作成されます。

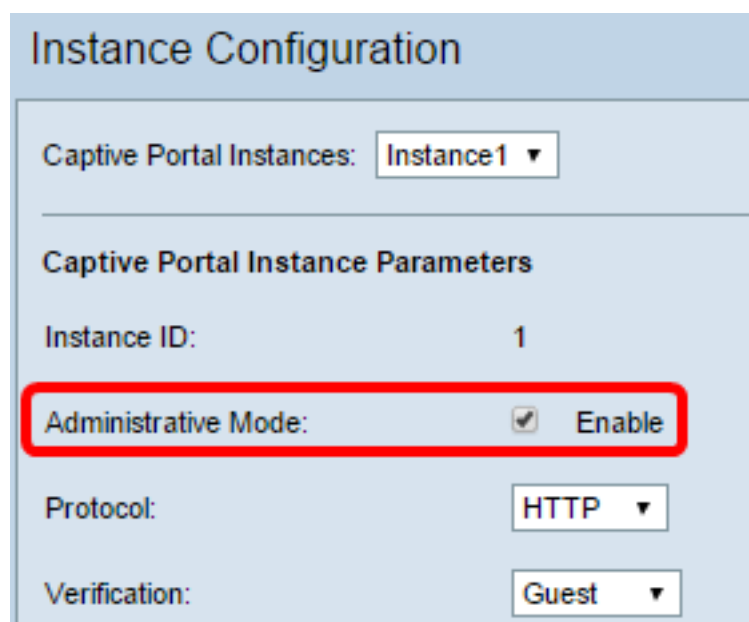
A screenshot of the 'Instance Configuration' window. At the top, it says 'Instance Configuration'. Below that, there is a section for 'Captive Portal Instances' with a 'Create' button and a dropdown arrow. Underneath is the 'Captive Portal Instance Parameters' section. The 'Instance Name' field is highlighted with a red box and contains the text 'Instance1'. To the right of the field, it says '(Range: 1 - 32 Characters)'. At the bottom left, there is a 'Save' button.

注：最大2つの設定を作成できます。すでに2つのインスタンスを作成している場合は、編集するインスタンスを選択する必要があります。

ステップ9:[Instance Configuration]ウィンドウに追加情報が表示されます。インスタンス

IDは、現在のインスタンスのインスタンスIDを表示する設定不可能なフィールドです。

ステップ10：管理モードで[Enable] チェックボックスをオンにして、CPインスタンスを有効にします。



The screenshot shows the 'Instance Configuration' interface. At the top, there is a dropdown menu for 'Captive Portal Instances' set to 'Instance 1'. Below this is the 'Captive Portal Instance Parameters' section. It includes an 'Instance ID' field with the value '1'. The 'Administrative Mode' checkbox is checked and labeled 'Enable', and this entire row is highlighted with a red rectangular border. Below it, the 'Protocol' dropdown is set to 'HTTP', and the 'Verification' dropdown is set to 'Guest'.

ステップ11:[Protocol]ドロップダウンリストから、認証プロセスに使用するプロトコルを選択します。

HTTP：認証プロセスで使用される情報を暗号化しません。

HTTPS：認証プロセスで使用される情報の暗号化を提供します。

注：この例では、HTTPが使用されています。

ステップ12:[Verification]ドロップダウンリストから、使用するCPの認証方法を選択します。

[Guest]：ユーザは認証を提供する必要はありません。

[ローカル(Local)]:WAPは、ユーザから提供された認証情報を、WAPに保存されているローカルデータベースと照合します。

RADIUS:WAPは、ユーザから提供された認証情報をリモートRADIUSサーバのデータベースと照合します。

タイムサーバ：[ローカル]または[ゲスト]を選択した場合は、ステップ[28に進みます](#)。

ステップ13: ( オプション ) 設定されたURLに確認されたユーザーをリダイレクトする場合は、[リダイレクトを有効にする]チェックボックスをオンにします。このオプションを無効にすると、確認したユーザにはローカル固有のウェルカムページが表示されます。

Redirect:	<input type="checkbox"/> Enable
Redirect URL:	<input type="text"/> (Range: 0 - 256 Characters)
Away Timeout:	<input type="text" value="60"/> (Range: 0 - 1440 Min, Default: 60)
Session Timeout:	<input type="text" value="0"/> (Range: 0 - 1440 Min, Default: 0)
Maximum Bandwidth Upstream:	<input type="text" value="0"/> (Range: 0 - 1300 Mbps, Default: 0)
Maximum Bandwidth Downstream:	<input type="text" value="0"/> (Range: 0 - 1300 Mbps, Default: 0)

ステップ14: ( オプション ) 検証済みユーザをリダイレクトするURLを入力します。

注：この手順は、ステップ13でリダイレクトを有効にした場合にのみ適用されます。

ステップ15:[Away Timeout] フィールドに、ユーザがWAPから関連付けを解除し、WAP認証クライアントリストに残ることができる時間 ( 分 ) を入力します。ユーザがAway Timeout値よりも長くWAPに接続していない場合は、WAPを使用する前に再認証する必要があります。

ステップ16:[Session Timeout]フィールドに、WAPがセッションを終了するまで待機する時間 ( 分 ) を入力します。値が0の場合は、タイムアウトは適用されません。

ステップ17:[Maximum Bandwidth Upstream]フィールドに、キャプティブポータル経由でクライアントがデータを送信できる最大アップロード速度(Mbps)を入力します。

ステップ18:[Maximum Bandwidth Downstream]フィールドに、キャプティブポータル経由でクライアントがデータを受信できる最大ダウンロード速度(Mbps)を入力します。

ステップ19:[User Group Name]ドロップダウンリストから、CPインスタンスに割り当てるグループを選択します。選択したグループのメンバーであるユーザは、WAPにアクセスできます。

User Group Name:	<input type="text" value="Group1"/>
RADIUS IP Network:	<input type="text" value="IPv4"/>
Global RADIUS:	<input checked="" type="checkbox"/> Enable

注：グループを割り当てるには、[ステップ12](#)の検証モードをローカルまたはRADIUSにする必要があります。

ステップ20:[RADIUS IP Network]ドロップダウンリストから、RADIUSクライアントで使用されるインターネットプロトコルのタイプを選択します。

IPv4:RADIUSクライアントのアドレスは、xxx.xxx.xxx.xxx(192.0.2.10)の形式になります。

IPv6:RADIUSクライアントのアドレスの形式は、xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx(2001:DB8::CAD5:7D91)です。

ステップ21: ( オプション ) 認証にグローバルRADIUSサーバリストを使用する場合は、



[Enable Global RADIUS]チェックボックスをオンにします。別のRADIUSサーバセットを使用する場合は、このチェックボックスをオフにして、このページでRADIUSサーバを設定します。

タイムサーバ：グローバルRADIUSを有効にした場合は、ステップ28に進みます。

注：この例では、グローバルRADIUSは有効になっていません。

ステップ22: ( オプション ) WAPネットワーク上のクライアントの時間とデータ使用量を追跡および測定する場合は、[RADIUSアカウントingの有効化(Enable RADIUS Accounting)]チェックボックスをオンにします。

注：[ステップ](#)21で[Global RADIUS]チェックボックスが有効になっている場合は、追加のRADIUSサーバを設定する必要はありません。

ステップ23:[Server IP Address-1]フィールドに、プライマリサーバとして使用するRADIUSサーバのIPアドレスを入力します。IPアドレスは、IPv4またはIPv6のそれぞれのアドレス形式に準拠している必要があります。

Global RADIUS:	<input type="checkbox"/>	Enable
RADIUS Accounting:	<input checked="" type="checkbox"/>	Enable
Server IP Address-1:	<input type="text" value="202.123.123.123"/>	(xxx.xxx.xxx.xxx)
Server IP Address-2:	<input type="text"/>	(xxx.xxx.xxx.xxx)
Server IP Address-3:	<input type="text"/>	(xxx.xxx.xxx.xxx)
Server IP Address-4:	<input type="text"/>	(xxx.xxx.xxx.xxx)

ステップ24: ( オプション ) 一致が見つかるまで順番にチェックされるバックアップRADIUSサーバを最大3つ設定できます。一致するものが見つからなかった場合、ユーザはアクセスを拒否されます。[Server IP Address-(2 ~ 4)]フィールドに、プライマリサーバで認証が失敗した場合に使用するバックアップRADIUSサーバのIPアドレスを入力します。

ステップ25:[Key-1]フィールドに、WAPデバイスがプライマリRADIUSサーバへの認証に使用する共有秘密キーを入力します。これは、RADIUSサーバで設定されたものと同じキーである必要があります。

Key-1:	<input type="text" value="....."/>	(Range
Key-2:	<input type="text" value="....."/>	(Range
Key-3:	<input type="text"/>	(Range
Key-4:	<input type="text"/>	(Range
Locale Count:	0	
Delete Instance:	<input type="checkbox"/>	

ステップ26：残りの[Key]フィールド(2 ~ 4)に、WAPデバイスがそれぞれのバックアップ RADIUSサーバに対して認証するために使用する共有秘密キーを入力します。

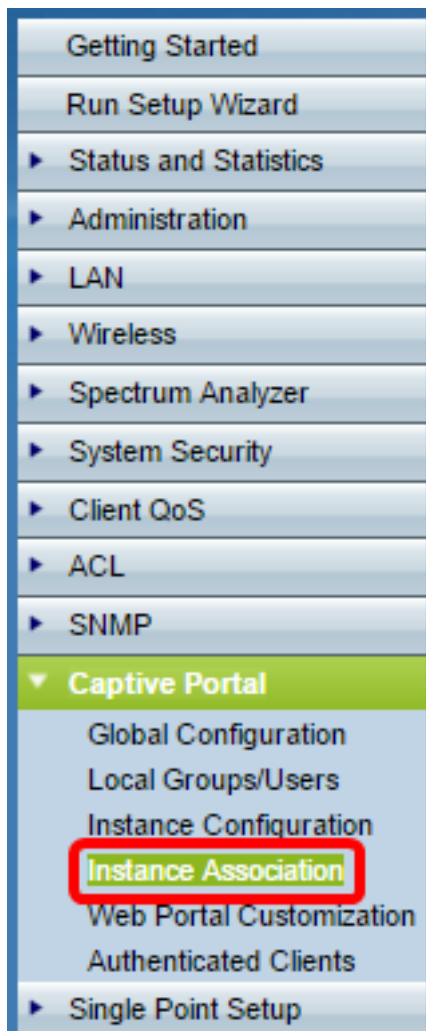
注：[ロケールカウント(Locale Count)]は、このインスタンスに関連付けられているロケールの数を表示する設定不可能なフィールドです。

ステップ27: ( オプション ) 現在のインスタンスを削除するには、[インスタンスの削除]チェックボックスをオンにします。

ステップ28:[Save]をクリックします。

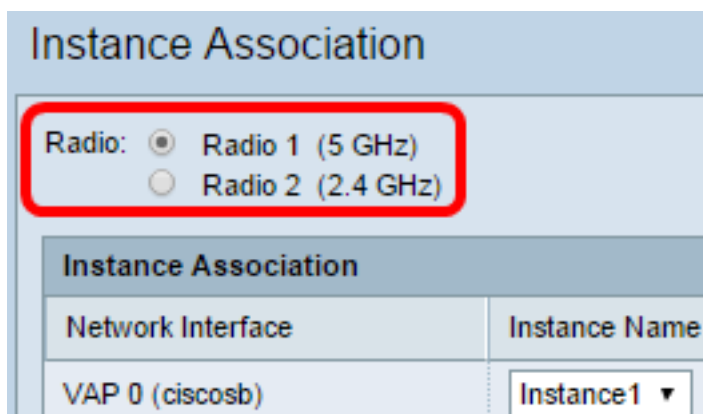
## インスタンスとVAPの関連付け

ステップ29:Webベースのユーティリティで、[キャプティブポータル(Captive Portal)] > [インスタンスの関連付け(Instance Association)]を選択します。



ステップ30:[Radio]エリアで、インスタンスを関連付ける無線のオプションボタンをクリックします。

注：この例では、無線1(5 GHz)が選択されています。



ステップ31:[Instance Name]ドロップダウンリストからインスタンス設定を選択し、特定のVAPに関連付けます。

注：この例では、[ステップ8](#)で作成したInstance1をVAP 1 ( 仮想アクセスポイント2 ) に使用します。

Instance Association	
Network Interface	Instance Name
VAP 0 (CHICCO)	<input type="text"/>
VAP 1 (Virtual Access Point 2)	Instance 1
VAP 2 (Virtual Access Point 3)	<input type="text"/>
VAP 3 (Virtual Access Point 4)	Instance 1
VAP 4 (Virtual Access Point 5)	<input type="text"/>

ステップ32:[Save]をクリックします。

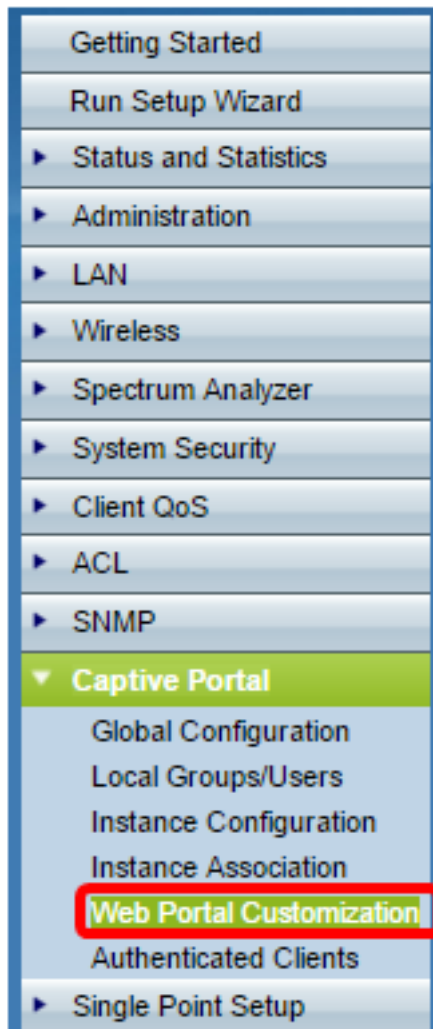
VAP 11 (Virtual Access Point 12)	<input type="text"/>
VAP 12 (Virtual Access Point 13)	<input type="text"/>
VAP 13 (Virtual Access Point 14)	<input type="text"/>
VAP 14 (Virtual Access Point 15)	<input type="text"/>
VAP 15 (Virtual Access Point 16)	<input type="text"/>

Save

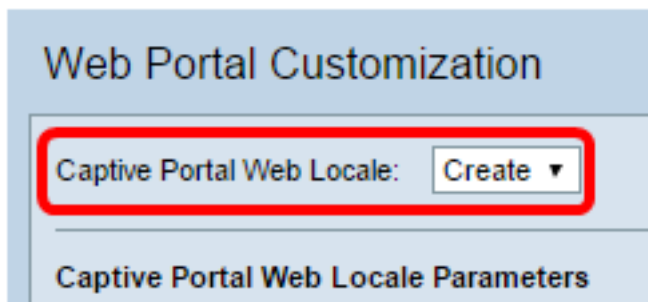
## Web ポータルのカスタマイズ

ロケール ( 認証Webページ ) は、WAPユーザがインターネットにアクセスしようとしたときに表示されるWebページです。[Web Portal Customization]ページでは、ロケールをカスタマイズし、キャプティブポータルインスタンスに割り当てることができます。

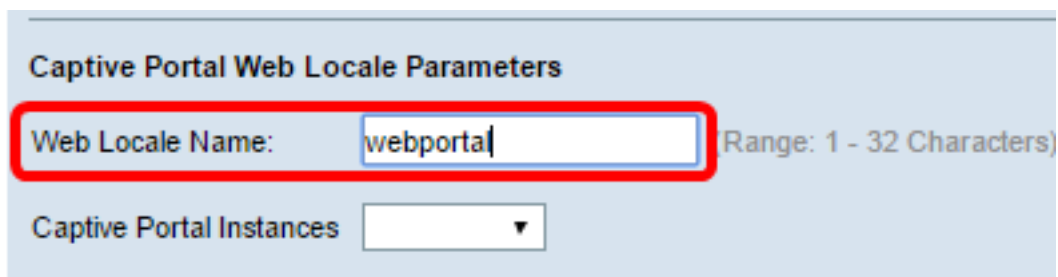
ステップ33:Webベースのユーティリティで、[キャプティブポータル(Captive Portal)] > [Webポータルカスタマイズ(Web Portal Customization)]を選択します。



ステップ34:[キャプティブポータルWebロケール(Captive Portal Web Locale)]ドロップダウンリストから[作成(Create)]を選択し、新しいロケールを作成します。



ステップ35:[Web Locale Name]フィールドにロケール名を入力します。



ステップ36:[Captive Portal Instances]ドロップダウンリストから、ロケールが関連付けられているキャプティブポータルインスタンスを選択します。複数のロケールを1つのキャプティブポータルインスタンスに関連付けることができます。リンクをクリックすると、別のロケールに切り替えることができます。

### Web Portal Customization

Captive Portal Web Locale:

---

#### Captive Portal Web Locale Parameters

Web Locale Name:  (Range: 1 - 32 Characters)

**Captive Portal Instances**

ステップ37:[Save]をクリックして新しいロケールを作成します。

注 : [Web Portal Customization]ページに、追加情報が表示されます。

### Web Portal Customization

Captive Portal Web Locale:

---

#### Captive Portal Web Locale Parameters

Locale ID: 1

Instance Name: Instance1

Background Image Name:

Logo Image Name:

Foreground Color:  (Range: 1 - 32 Characters, Default: #999999)

Background Color:  (Range: 1 - 32 Characters, Default: #BFBFBF)

Separator:  (Range: 1 - 32 Characters, Default: #BFBFBF)

Locale Label:  (Range: 1 - 32 Characters, Default: English)

Locale:  (Range: 1 - 32 Characters, Default: en)

ロケールIDは、現在のロケールのID番号を表示する設定不可能なフィールドです。

[インスタンス名(Instance Name)]は、ロケールに関連付けられたキャプティブポータルインスタンス名を表示する設定不可能なフィールドです。

ステップ38:[Background Image Name]ドロップダウンリストから、ロケールの背景に表示

するイメージを選択します。[カスタムイメージのアップロード/削除]ボタンをクリックして、独自のイメージを追加します。詳細については、「カスタムイメージのアップロード/削除」の項を参照してください。

ステップ39:[Logo Image Name ( ロゴイメージ名 )]ドロップダウンリストから、ページの左上に表示するイメージを選択します。

ステップ40:[前景色(Foreground Color)]フィールドに、ロケールの前景色に対応する6桁のハイパーテキスト転送プロトコル(HTML)コードを入力します。

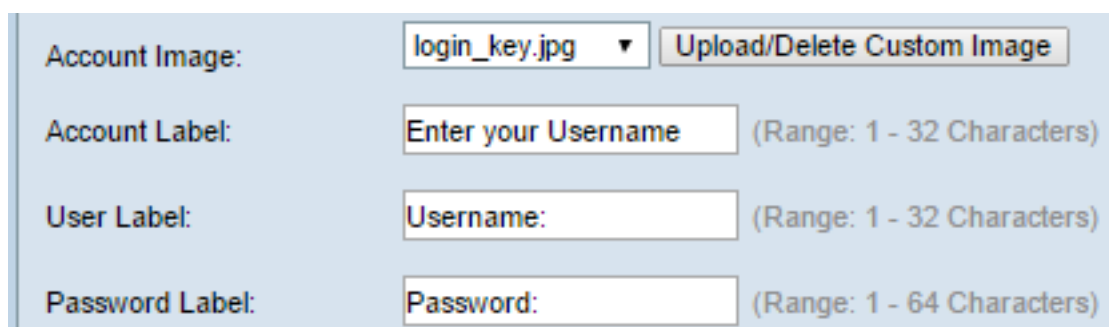
ステップ41:[背景の色]フィールドに、ロケールの背景色として6桁のHTMLコードを入力します。

ステップ42:[セパレータ]フィールドに、ページのヘッダーとページ本体を区切る水平線の色を6桁のHTMLコードで入力します。

ステップ43:[ロケールラベル(Locale Label)]フィールドに、ロケールの内容を表す名前を入力します。複数のロケールがある場合、これはロケールを変更するためにクリックするリンクの名前です。たとえば、英語とスペイン語のロケールを使用している場合は、ロケール名で示す必要があります。

ステップ44:[Locale]フィールドにロケールの省略形を入力します。

ステップ45:[Account Image]ドロップダウンリストから、ログインフィールドの上に表示するイメージを選択します。



Account Image:	login_key.jpg ▼	Upload/Delete Custom Image
Account Label:	Enter your Username	(Range: 1 - 32 Characters)
User Label:	Username:	(Range: 1 - 32 Characters)
Password Label:	Password:	(Range: 1 - 64 Characters)

ステップ46:[アカウントラベル(Account Label)]フィールドに、ユーザにユーザ名の入力を要求する指示を入力します。

ステップ47:[ユーザラベル]フィールドに、ユーザ名テキストボックスのラベルを入力します。

ステップ48:[パスワード・ラベル]フィールドに、パスワード・テキスト・ボックスのラベルを入力します。

ステップ49:[ボタンラベル]フィールドに、ユーザがクリックしてユーザ名とパスワードを送信するボタンのラベルを入力します。

Button Label:	<input type="text" value="Connect"/>	(Range: 2 - 32 Characters, Default: Connect)
Fonts:	<input type="text" value="'MS UI Gothic', arial, sans-serif"/>	(Range: 1 - 512 C)
Browser Title:	<input type="text" value="Captive Portal"/>	(Range: 1 - 128 C)
Browser Content:	<input type="text" value="Welcome to the Wireless Network"/>	(Range: 1 - 128 C)
Content:	<input type="text" value="To start using this service, enter your credentials and click the connect button."/>	(Range: 1 - 256 C)
Acceptance Use Policy:	<input type="text" value="Acceptance Use Policy."/>	(Range: 1 - 4096)

ステップ50:[フォント]フィールドに、ロケールに使用するフォント名を入力します。複数のフォント名をカンマで区切って入力できます。クライアントデバイスで最初のフォントスタイルが見つからない場合は、次のフォントが使用されます。フォント名にスペースで区切られた複数の単語がある場合は、一重引用符で囲んでフォント名を囲みます。例えば、「MS UI Gothic」、MS UI Gothic、MS UI Gothic、MS UI Gothic、MS UI Gothic、MS Pゴシック、sans-serifなど。

ステップ51:[ブラウザのタイトル]フィールドに、ブラウザのタイトルバーに表示するテキストを入力します。

ステップ52:[ブラウザのコンテンツ]フィールドに、ページヘッダーに表示するテキストを入力します。

ステップ53:[コンテンツ]フィールドに、ユーザに何を行うかを指示するテキストを入力します。このフィールドは、ユーザ名とパスワードのテキストボックスの下に表示されます。

ステップ54:[受け入れポリシー(Acceptance Use Policy)]フィールドに、ユーザがWAPにアクセスする場合に同意する必要がある条件を入力します。



ステップ55:[Accept Label]フィールドに、ユーザーが承認使用ポリシーを読み取り、承認したことを確認するように指示するテキストを入力します。

Accept Label:	Check here to indicate that you have read and accepted the Acceptance Use Policy. (Range: 1 - 128)
No Accept Text:	Error: You must acknowledge the Acceptance Use Policy before connecting! (Range: 1 - 128)
Work In Progress Text:	Connecting, please be patient... (Range: 1 - 128)
Denied Text:	Error: Invalid Credentials, please try again! (Range: 1 - 128)
Welcome Title:	Congratulations! (Range: 1 - 128)

ステップ56:[No Accept Text]フィールドに、ログイン資格情報を送信しても受け入れポリシーを受け入れない場合にユーザにプロンプトを表示するテキストを入力します。

ステップ57:[Work In Progress Text]フィールドに、WAPが所定のクレデンシャルを確認するときに表示されるテキストを入力します。

ステップ58:[Denied Text]フィールドに、ユーザが認証に失敗したときに表示されるテキストを入力します。

ステップ59:[ウェルカムタイトル(Welcome Title)]フィールドに、クライアントが正常に認証されたときに表示されるタイトルテキストを入力します。

ステップ60:[Welcome Content] フィールドに、ネットワークに接続しているクライアントに表示されるテキストを入力します。

Welcome Title: Congratulations! (Range: 1 - 12)

Welcome Content: You are now authorized and connected to the network. (Range: 1 - 25)

Delete Locale:

Save Preview...

ステップ61: ( オプション ) 現在のロケールを削除するには、[ロケールの削除]チェックボックスをオンにします。

ステップ62:[Save]をクリックします。

ステップ63. ( オプション ) 現在のロケールを表示するには、[プレビュー]をクリックします。変更を行う場合は、プレビューする前に[保存]をクリックして変更を更新します。

注 : キャプティブポータルログイン画面は、次の図のようになります。



Welcome to the Wireless Network



Enter your Username

Username:

To start using this service, enter your credentials and click the connect button.

Acceptance Use Policy.

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

## ローカルグループの作成

ゲスト以外のキャプティブポータルでは、ユーザのユーザ名とパスワードに基づいてログインする必要があります。WAPは、ローカルユーザのグループを含むローカルグループを作成します。その後、ローカルグループがインスタンスに関連付けられます。ローカルグループのメンバーであるローカルユーザは、キャプティブポータルを介してアクセスできます。デフォルトローカルグループは常にアクティブであり、削除することはできません。WAPには最大2つのローカルグループを追加できます。

ステップ64:Webベースのユーティリティで、[キャプティブポータル(Captive Portal)] > [ローカルグループ/ユーザ(Local Groups/Users)]を選択します。



ステップ65:[キャプティブポータルグループ(Captive Portal Groups)] ドロップダウンリストから[作成(Create)]を選択します。

The 'Local Groups/Users' configuration page. Under 'Local Groups Settings', the 'Captive Portal Groups:' dropdown menu is set to 'Create' and is highlighted with a red box. Below it is a text input field for 'Group Name:' with a note '(Range: 1 - 32 Characters)'. At the bottom is an 'Add Group' button.

ステップ66:[Group Name]フィールドにローカルグループの名前を入力します。

Local Groups/Users

Local Groups Settings

Captive Portal Groups: Create ▾

Group Name: Group1 (Range: 1 - 32 Characters)

Add Group

ステップ67:[グループの追加]をクリックして、グループを保存します。

Local Groups/Users

Local Groups Settings

Captive Portal Groups: Create ▾

Group Name: (Range: 1 - 32 Characters)

Add Group

注：「インスタンスの構成」セクションの[ステップ19](#)で、[インスタンスにローカルグループを割り当てることができます。](#)

### ローカルユーザの作成

ローカルユーザがローカルグループに追加されます。これらのユーザは、ローカルグループが設定されたインスタンスを持つキャプティブポータルにアクセスできます。[ローカルユーザ(Local Users)]ページで設定されている情報の一部は、[インスタンスの設定(Instance Configuration)]ページでも設定されます。ローカルユーザに設定された値は、インスタンスに設定された値よりも優先されます。ローカルデータベースには、最大128の許可ユーザを設定できます。

ステップ68:[キャプティブポータルユーザ(Captive Portal Users)] ドロップダウンリストから[作成(Create)]を選択します。

Local Users Settings

Captive Portal Users: Create ▾

User Name: (Range: 1 - 32 Characters)

Add User

ステップ69:[ユーザ名]フィールドに、追加するユーザ名を入力します。

Local Users Settings

Captive Portal Users: Create ▾

User Name: User1 (Range: 1 - 32 Characters)

Add User

ステップ70:[ユーザの追加]をクリックして、新しいユーザを作成します。[ローカルユーザの設定(Local Users Settings)]ウィンドウに追加情報が表示されます。

Local Users Settings

Captive Portal Users: User1 ▾

User Password: (Range: 8 - 64 Alphanumeric & Special)

Show Password as Clear Text

Away Timeout: 60 (Range: 0 - 1440 Min, Default: 60)

Group Name: Default  
Group1

Maximum Bandwidth Upstream: 0 (Range: 0 - 1300 Mbps, Default: 0)

Maximum Bandwidth Downstream: 0 (Range: 0 - 1300 Mbps, Default: 0)

Delete User:

Save

ステップ71:[ユーザパスワード(User Password)]フィールドに、ユーザに関連付けられたパスワードを入力します。

ステップ72: ( オプション ) パスワードをクリアテキストで表示するには、[パスワードをクリアテキストとして表示]チェックボックスをオンにします。このチェックボックスをオフにすると、パスワードがマスクされます。

ステップ73:[Away Timeout] フィールドに、ユーザがWAPからアソシエーションを解除し、WAP認証クライアントリストに残ることができる時間 ( 分 ) を入力します。ユーザがAway Timeoutよりも長くWAPに接続していない場合は、WAPを使用する前に再認証する必要があります。

ステップ74:[グループ名]フィールドで、ユーザーに参加させるローカルグループをクリックします。

ステップ75:[Maximum Bandwidth Upstream]フィールドで、クライアントがキャプティブポ

ータル経由でデータを送信できる最大アップロード速度をMbpsで入力します。

ステップ76:[*Maximum Bandwidth Downstream*]フィールドに、キャプティブポータルを介してクライアントがデータを受信できる最大ダウンロード速度をMbpsで入力します。

ステップ77: ( オプション ) ローカルユーザを削除するには、[ユーザの削除]チェックボックスをオンにします。

ステップ78:[Save]をクリックします。

これで、WAP571またはWAP571Eの高度なキャプティブポータル設定が完了したはずですよ。