

Configurer Captive Portal sur un WAP571 ou WAP571E

Objectif

Un portail captif (CP) vous permet de restreindre l'accès à votre réseau sans fil jusqu'à ce que les utilisateurs sans fil aient été vérifiés. Lorsqu'un utilisateur ouvre un navigateur Web, il est redirigé vers une page de connexion où il doit entrer son nom d'utilisateur et son mot de passe. Deux types d'utilisateurs peuvent être autorisés à accéder à votre réseau ; utilisateurs authentifiés et invités. Les utilisateurs authentifiés doivent fournir un nom d'utilisateur et un mot de passe correspondant à une base de données locale ou à la base de données d'un serveur RADIUS. Les invités n'ont pas besoin de fournir de nom d'utilisateur ou de mot de passe.

Cet article explique comment configurer le portail captif sur votre point d'accès sans fil (WAP).

Périphériques pertinents

- Gamme WAP500 - WAP571, WAP571E

Version du logiciel

- 1.0.0.15 - WAP571, WAP571E

Configurer le portail captif

Les paramètres de base du portail captif peuvent être configurés via l'assistant de configuration, tandis que les paramètres avancés peuvent être configurés via l'utilitaire Web. Pour une configuration rapide et de base, vous pouvez utiliser l'assistant de configuration pour activer la fonctionnalité. Reportez-vous aux étapes ci-dessous :

Note: Les images ci-dessous sont capturées à partir du WAP571.

Utilisation de l'Assistant de configuration


Étape 1. Connectez-vous à l'utilitaire Web, puis cliquez sur **Exécuter l'Assistant de configuration**.

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**

Note: Si c'est la première fois que vous configurez votre WAP, l'assistant de configuration s'affiche automatiquement.

Étape 2. Suivez les instructions des écrans de l'assistant de configuration. Pour une configuration pas à pas de votre WAP à l'aide de l'assistant de configuration, cliquez [ici](#) pour obtenir des instructions.

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

Étape 3. Lorsque l'écran Enable Captive Portal - Create Your Guest Network (Activer le portail captif - Créer votre réseau invité) s'affiche, sélectionnez **Yes** (Oui), puis cliquez sur **Next** (Suivant).

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

Étape 4. Entrez le nom du réseau invité, puis cliquez sur **Suivant**.

Note: Le nom de réseau invité par défaut est ciscosb-guest.

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

Étape 5. Choisissez un type de sécurité pour votre réseau invité sans fil.

Note: La meilleure sécurité (WPA2 Personal - AES) est choisie comme exemple ci-dessous.

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)

Étape 6. Entrez votre clé de sécurité, puis cliquez sur **Suivant**.

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

Étape 7. Entrez un ID de VLAN pour votre réseau invité, puis cliquez sur **Suivant**.

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

Étape 8. (Facultatif) Si vous avez une page Web spécifique à afficher après que les utilisateurs ont accepté les conditions d'utilisation de la page d'accueil, cochez la case **Activer l'URL de redirection**. Entrez l'URL, puis cliquez sur **Suivant**.

Note: L'URL peut être le site Web de votre société.

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

Étape 9. Vérifiez et confirmez vos paramètres, puis cliquez sur **Soumettre**.

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

Étape 10. Une fois l'écran Device Setup Complete (Configuration du périphérique terminée) affiché, cliquez sur **Finish** (Terminer) pour fermer l'assistant de configuration.

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

Vous devez maintenant avoir configuré les paramètres de base de la fonctionnalité Captive Portal de votre WAP.

Utilisation de l'utilitaire Web

Pour configurer les paramètres avancés du portail captif sur le WAP, procédez comme suit :

Globally Enable the Captive Portal : permet aux portails captifs de prendre effet.

Créer une instance de portail captif : une instance de portail captif est un ensemble de paramètres qui contrôle la manière dont un utilisateur se connecte à un point d'accès virtuel (VAP).

Associer une instance de portail captif à un VAP : les utilisateurs qui tentent d'accéder au VAP doivent suivre les paramètres configurés pour l'instance.

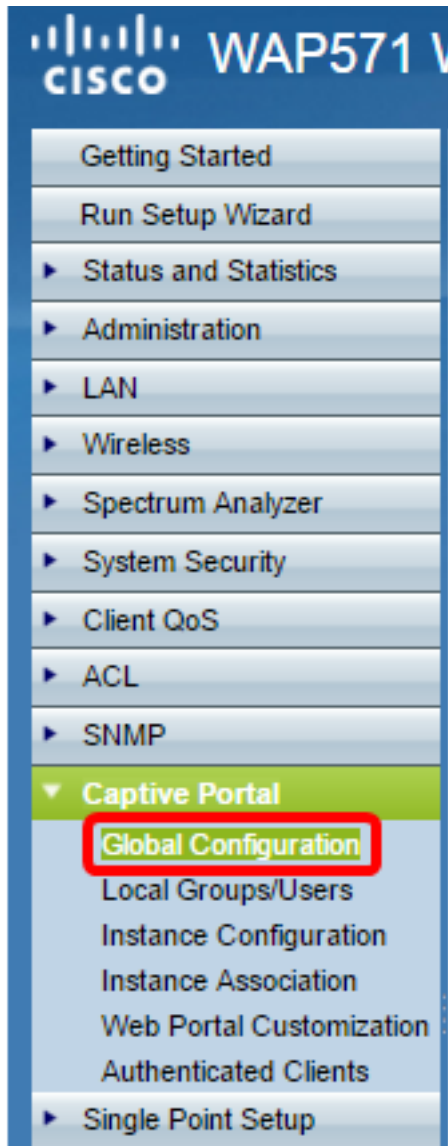
Personnaliser le portail Web : le portail Web est la page Web sur laquelle les utilisateurs sont redirigés lorsqu'ils tentent de se connecter au VAP.

Créer un groupe local : le groupe local peut être affecté à une instance, qui accepte les utilisateurs appartenant à ce groupe.

Créer un utilisateur local : les utilisateurs locaux sont ajoutés à un groupe local et sont autorisés à accéder au portail captif auquel le groupe est configuré.

Activer le portail captif dans le monde entier

Étape 1. Dans l'utilitaire Web, sélectionnez **Captive Portal > Global Configuration**.



Étape 2. (Facultatif) Entrez le nombre de secondes que l'utilisateur doit saisir pour entrer les informations d'authentification avant que le WAP ferme la session d'authentification dans le champ *Authentication Timeout*.

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)

Étape 3. (Facultatif) Si vous souhaitez que les informations HTTP entre le WAP et le client utilisent un autre port en plus de la valeur par défaut, saisissez le numéro de port HTTP que vous souhaitez ajouter dans le champ *Port HTTP supplémentaire*. HTTP et d'autres protocoles Internet utilisent des ports pour s'assurer que les périphériques savent où trouver un protocole donné. Les options sont 80, entre 1025 et 65535, ou saisissez 0 pour désactiver. Le port HTTP et le port HTTPS ne peuvent pas être identiques.

Étape 4. (Facultatif) Si vous souhaitez que les informations HTTP entre le WAP et le client utilisent un autre port en plus de la valeur par défaut, saisissez le numéro de port HTTPS que vous souhaitez ajouter dans le champ *Port HTTPS supplémentaire*. Les options sont 443, entre 1025 et 65535, ou saisissez 0 pour désactiver. Le port HTTP et le port HTTPS ne peuvent pas être identiques.

Les informations suivantes s'affichent dans la zone Compteurs de configuration du portail captif et ne peuvent pas être configurées.

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

Nombre d'instances : nombre d'instances CP configurées sur le périphérique WAP. Un maximum de deux PC peut être configuré sur le WAP.

Group Count : nombre de groupes CP configurés sur le périphérique WAP. Vous pouvez configurer jusqu'à deux groupes. Impossible de supprimer le groupe par défaut.

User Count : nombre d'utilisateurs CP configurés sur le périphérique WAP. Un maximum de 128 utilisateurs peut être configuré sur le WAP.

Étape 5. Cliquez **Save**.

Note: Les modifications sont enregistrées dans la configuration de démarrage.

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)

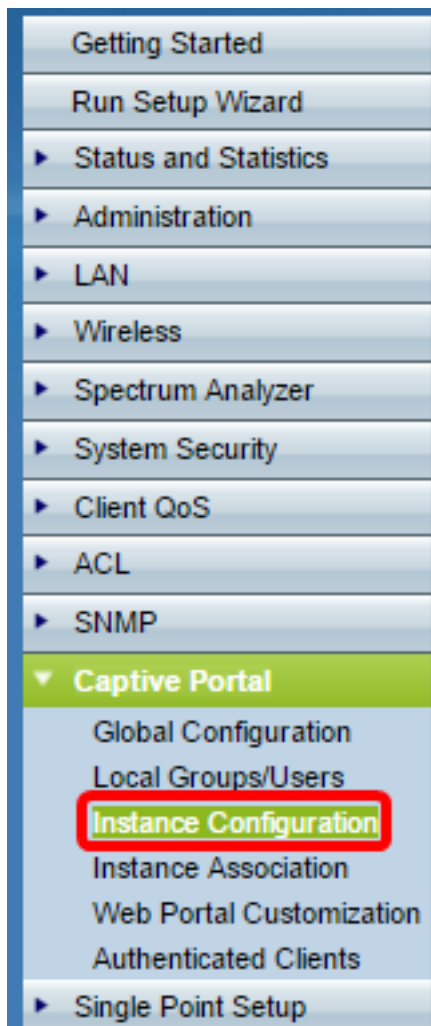
Additional HTTPS Port: (Range: 1025 - 65535 or 443, 0 = Disable, Default: 0)

Captive Portal Configuration Counters

Instance Count:	0
Group Count:	1
User Count:	0

Configuration de l'instance

Étape 6. Dans l'utilitaire Web, sélectionnez **Captive Portal > Instance Configuration**.



Étape 7. Dans la liste déroulante Instances du portail captif, notez l'instance wiz-cp-inst1. Vous pouvez choisir ce nom ou créer un nouveau nom pour votre configuration d'instance.

Étape 8. (Facultatif) Dans le champ *Nom de l'instance*, saisissez un nom pour la configuration, puis cliquez sur **Enregistrer**.

Note: Dans cet exemple, une nouvelle instance est créée.

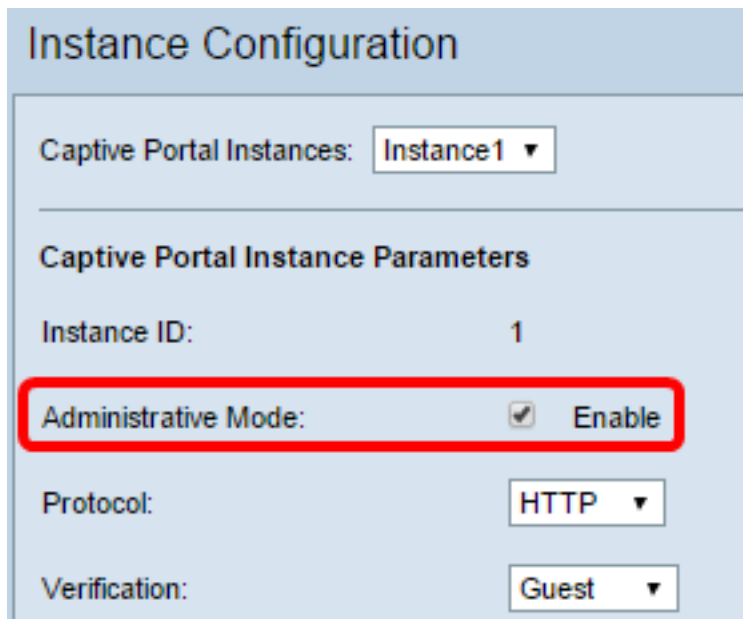
The 'Instance Configuration' window has a light blue header. Below it, 'Captive Portal Instances:' is followed by a 'Create' button with a dropdown arrow. A horizontal line separates this from the 'Captive Portal Instance Parameters' section. In this section, the 'Instance Name:' label is followed by a text input field containing 'Instance1|', which is highlighted with a red box. To the right of the field is the text '(Range: 1 - 32 Characters)'. At the bottom left is a 'Save' button.

Note: Vous pouvez créer un maximum de deux configurations. Si vous avez déjà créé deux instances, vous devez choisir une instance à modifier.

Étape 9. La fenêtre Configuration de l'instance affiche des informations supplémentaires.

L'ID d'instance est un champ non configurable qui affiche l'ID d'instance de l'instance actuelle.

Étape 10. Cochez la case **Activer** dans le mode administratif pour activer l'instance CP.



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 a section titled 'Captive Portal Instance Parameters'. The 'Instance ID' is displayed as '1'. The 'Administrative Mode' checkbox is checked and labeled 'Enable', and this entire row is highlighted with a red rectangular border. Below this, the 'Protocol' dropdown is set to 'HTTP' and the 'Verification' dropdown is set to 'Guest'.

Étape 11. Dans la liste déroulante Protocole, sélectionnez le protocole que vous souhaitez utiliser pour le processus d'authentification.

HTTP : ne chiffre pas les informations utilisées dans le processus d'authentification.

HTTPS : fournit le chiffrement des informations utilisées dans le processus d'authentification.

Note: Dans cet exemple, HTTP est utilisé.

Étape 12. Choisissez une méthode d'authentification que CP doit utiliser dans la liste déroulante Vérification.

Invité : l'utilisateur n'a pas besoin de fournir d'authentification.

Local : le WAP vérifie les informations d'authentification fournies par l'utilisateur par rapport à une base de données locale stockée sur le WAP.

RADIUS : le WAP vérifie les informations d'authentification fournies par l'utilisateur par rapport à la base de données d'un serveur RADIUS distant.

Économiseur de temps : Si vous choisissez Local ou Guest, passez à l'[étape 28](#).

Étape 13. (Facultatif) Si vous souhaitez rediriger les utilisateurs vérifiés vers une URL configurée, cochez la case **Activer** redirection. Si cette option est désactivée, les utilisateurs vérifiés verront une page d'accueil spécifique aux paramètres régionaux.

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)

Étape 14. (Facultatif) Saisissez l'URL vers laquelle vous souhaitez rediriger les utilisateurs vérifiés.

Note: Cette étape ne s'applique que si vous avez activé Redirection à l'[étape 13](#).

Étape 15. Dans le champ *Délai d'expiration de mise hors service*, saisissez la durée (en minutes) pendant laquelle un utilisateur peut être dissocié du WAP et rester dans la liste des clients authentifiés du WAP. Si l'utilisateur n'est pas connecté au WAP plus longtemps que la valeur de délai d'attente Absent, il doit être réautorisé avant de pouvoir utiliser le WAP.

Étape 16. Dans le champ *Session Timeout*, saisissez le temps (en minutes) que le WAP attend avant de mettre fin à la session. La valeur 0 signifie que le délai d'attente n'est pas appliqué.

Étape 17. Dans le champ *Bande passante maximale en amont*, saisissez la vitesse de téléchargement maximale (en Mbits/s) qu'un client peut envoyer des données via le portail captif.

Étape 18. Dans le champ *Bande passante maximale en aval*, saisissez la vitesse de téléchargement maximale (en Mbits/s) qu'un client peut recevoir des données via le portail captif.

Étape 19. Dans la liste déroulante Nom du groupe d'utilisateurs, sélectionnez le groupe que vous souhaitez affecter à l'instance CP. Tout utilisateur membre du groupe que vous choisissez est autorisé à accéder au WAP.

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

Note: Le mode Vérification de l'[étape 12](#) doit être Local ou RADIUS pour affecter un groupe.

Étape 20. Dans la liste déroulante Réseau IP RADIUS, sélectionnez le type de protocole Internet utilisé par le client RADIUS.

IPv4 : l'adresse du client RADIUS sera au format xxx.xxx.xxx.xxx (192.0.2.10).

IPv6 : l'adresse du client RADIUS sera au format

xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (2001:DB8::CAD5:7D91).

Étape 21. (Facultatif) Cochez la case **Activer** RADIUS global si vous voulez utiliser la liste de serveurs RADIUS globaux pour l'authentification. Si vous souhaitez utiliser un ensemble distinct de serveurs RADIUS, ne cochez pas cette case et configurez les serveurs RADIUS sur cette page.

Économiseur de temps : Passez à l'[étape 28](#) si vous activez RADIUS global.

Note: Dans cet exemple, Global RADIUS n'est pas activé.

Étape 22. (Facultatif) Cochez la case **Activer la comptabilité** RADIUS si vous voulez suivre et mesurer le temps et l'utilisation des données des clients sur le réseau WAP.

Note: Si la case Global RADIUS a été activée à l'[étape 21](#), vous n'avez pas besoin de configurer des serveurs RADIUS supplémentaires.

Étape 23. Dans le champ *Server IP Address-1*, saisissez l'adresse IP du serveur RADIUS que vous souhaitez utiliser comme serveur principal. L'adresse IP doit être conforme au format d'adresse IPv4 ou IPv6.

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)

Étape 24. (Facultatif) Vous pouvez configurer jusqu'à trois serveurs RADIUS de sauvegarde qui seront vérifiés dans l'ordre jusqu'à ce qu'une correspondance soit trouvée. Si aucune correspondance n'est trouvée, l'accès sera refusé à l'utilisateur. Dans les champs Server IP Address (Adresse IP du serveur) (2 à 4), saisissez l'adresse IP des serveurs RADIUS de sauvegarde à utiliser si l'authentification échoue avec le serveur principal.

Étape 25. Dans le champ *Key-1*, saisissez la clé secrète partagée que le périphérique WAP utilise pour s'authentifier auprès du serveur RADIUS principal. Il doit s'agir de la même clé qui a été configurée sur le serveur RADIUS.

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"/>	

Étape 26. Dans le reste des champs Key (2-4), saisissez la clé secrète partagée que le périphérique WAP utilise pour s'authentifier auprès des serveurs RADIUS de sauvegarde respectifs.

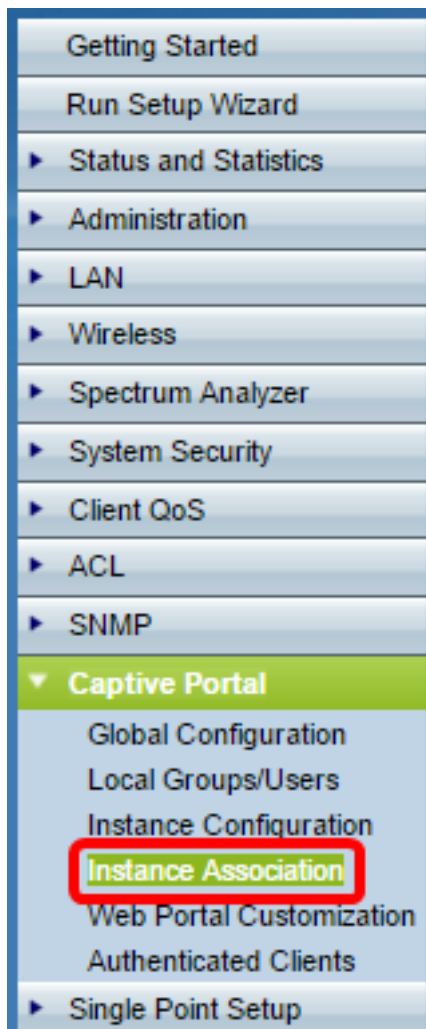
Note: Le nombre de paramètres régionaux est un champ non configurable qui affiche le nombre de paramètres régionaux associés à cette instance.

Étape 27. (Facultatif) Pour supprimer l'instance actuelle, cochez la case **Supprimer l'instance**.

Étape 28. Cliquez **Save**.

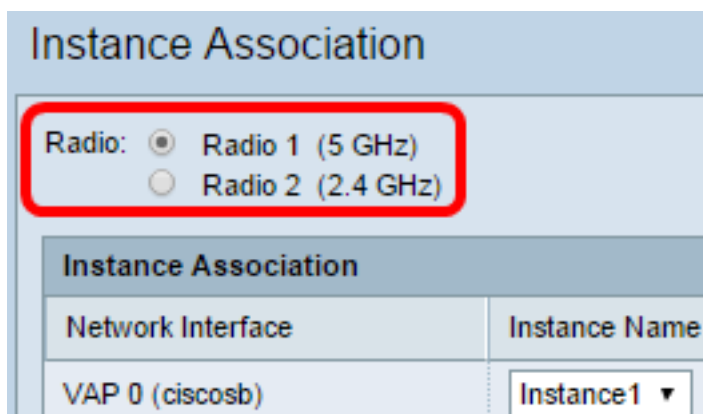
Associer une instance à VAP

Étape 29. Dans l'utilitaire Web, sélectionnez **Captive Portal > Instance Association**.



Étape 30. Cliquez sur la case d'option de la case d'option à laquelle vous souhaitez associer une instance dans la zone Radio.

Note: Dans cet exemple, Radio 1 (5 GHz) est sélectionné.



Étape 31. Choisissez une configuration d'instance dans la liste déroulante Nom d'instance à associer au VAP donné.

Note: Dans cet exemple, l'instance 1 créée à l'[étape 8](#) est utilisée pour VAP 1 (Virtual Access Point 2).

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"/>

Étape 32. Cliquez sur **Save**.

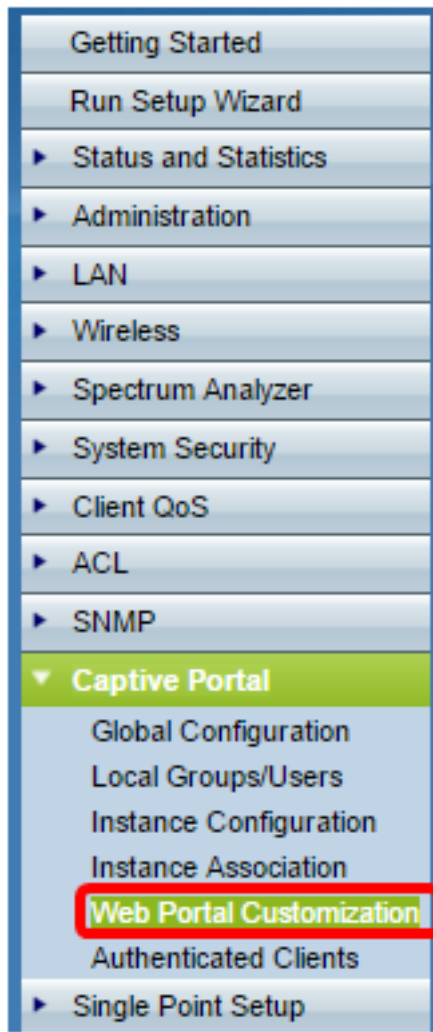
VAP 11 (Virtual Access Point 12)	<input type="text"/>
VAP 12 (Virtual Access Point 13)	<input type="text"/>
VAP 13 (Virtual Access Point 14)	<input type="text"/>
VAP 14 (Virtual Access Point 15)	<input type="text"/>
VAP 15 (Virtual Access Point 16)	<input type="text"/>

Save

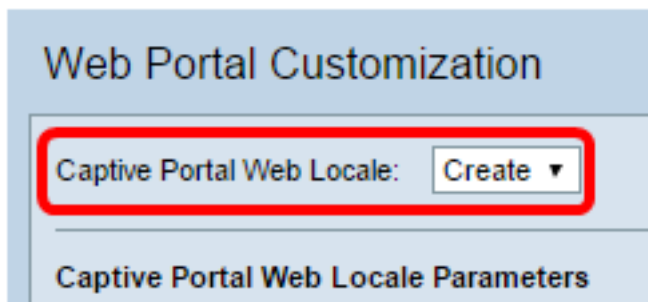
Personnaliser le portail Web

Un paramètre régional (page Web d'authentification) est la page Web que l'utilisateur WAP voit lorsqu'il tente d'accéder à Internet. La page Web Portal Customization vous permet de personnaliser un paramètre régional et de l'affecter à une instance de portail captive.

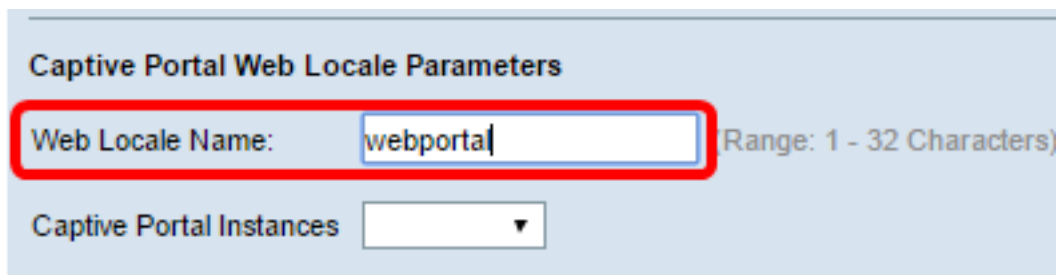
Étape 33. Dans l'utilitaire Web, sélectionnez **Captive Portal > Web Portal Customization**.



Étape 34. Choisissez **Create** dans la liste déroulante Captive Portal Web Locale pour créer un nouveau paramètre régional.

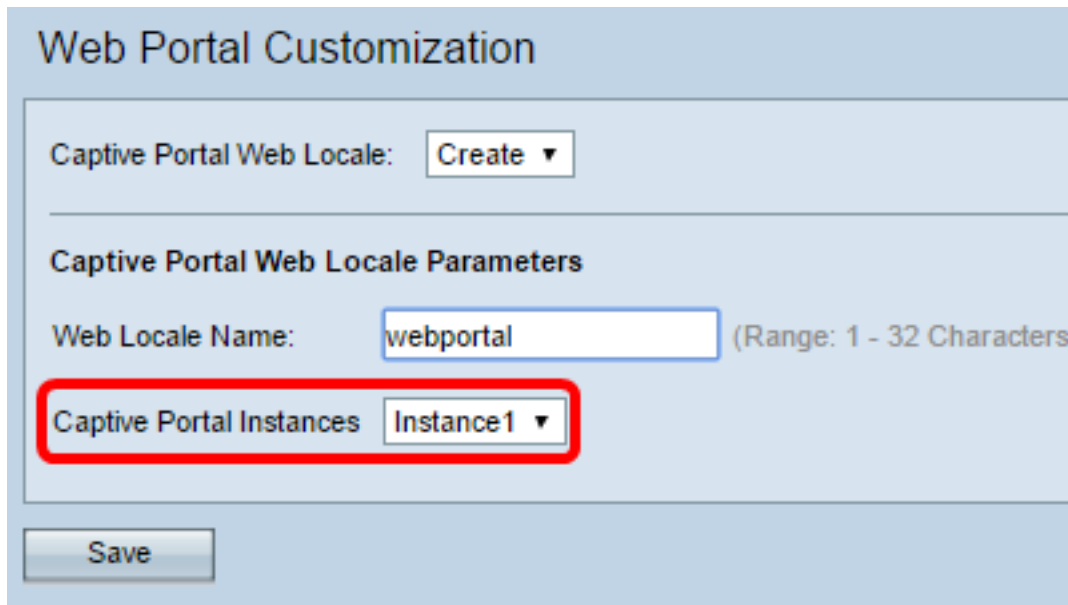


Étape 35. Entrez le nom des paramètres régionaux dans le champ *Nom des paramètres régionaux Web*.



Étape 36. Choisissez une instance de portail captif à laquelle les paramètres régionaux sont associés dans la liste déroulante Instances de portail captif. Vous pouvez associer plusieurs paramètres régionaux à une seule instance de portail captif. L'utilisateur peut

cliquer sur un lien pour passer à un autre paramètre régional.



Web Portal Customization

Captive Portal Web Locale: Create ▾

Captive Portal Web Locale Parameters

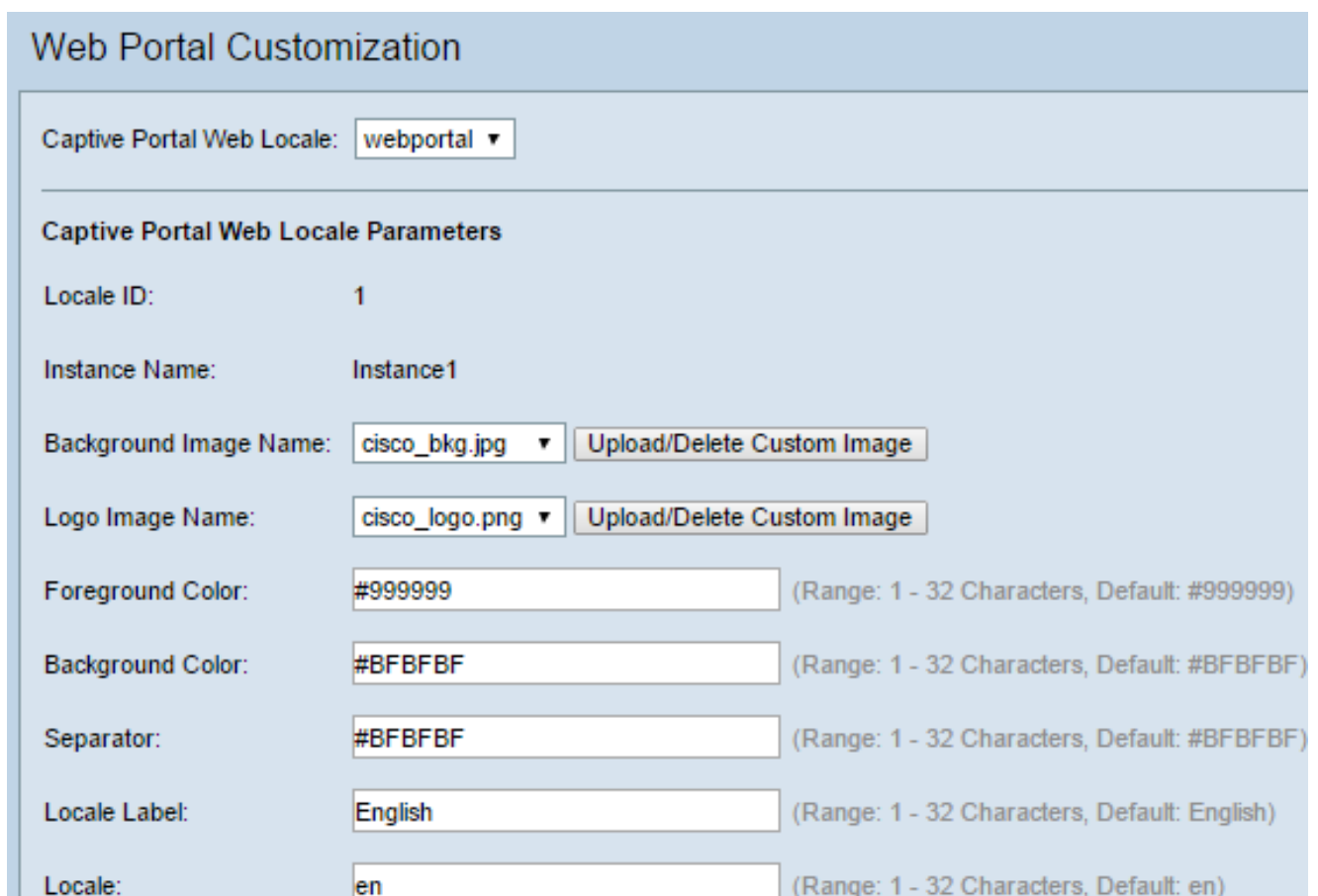
Web Locale Name: webportal (Range: 1 - 32 Characters)

Captive Portal Instances Instance1 ▾

Save

Étape 37. Cliquez sur **Enregistrer** pour créer un nouveau paramètre régional.

Note: La page Web Portal Customization affiche des informations supplémentaires.



Web Portal Customization

Captive Portal Web Locale: webportal ▾

Captive Portal Web Locale Parameters

Locale ID: 1

Instance Name: Instance1

Background Image Name: cisco_bkg.jpg ▾ Upload/Delete Custom Image

Logo Image Name: cisco_logo.png ▾ Upload/Delete Custom Image

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

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

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

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

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

L'ID de paramètres régionaux est un champ non configurable qui affiche le numéro d'ID des paramètres régionaux actuels.

Nom d'instance est un champ non configurable qui affiche le nom d'instance de portail captif associé aux paramètres régionaux.

Étape 38. Dans la liste déroulante Nom de l'image d'arrière-plan, sélectionnez une image à afficher en arrière-plan des paramètres régionaux. Cliquez sur le bouton **Télécharger/Supprimer une image personnalisée** pour ajouter votre propre image. Accédez à la section Télécharger/Supprimer une image personnalisée pour plus d'informations.

Étape 39. Dans la liste déroulante Nom de l'image du logo, sélectionnez une image à afficher dans le coin supérieur gauche de la page.

Étape 40. Dans le champ *Couleur de premier plan*, saisissez le code HTML (Hyper Text Transfer Protocol) à 6 chiffres pour la couleur de premier plan des paramètres régionaux.

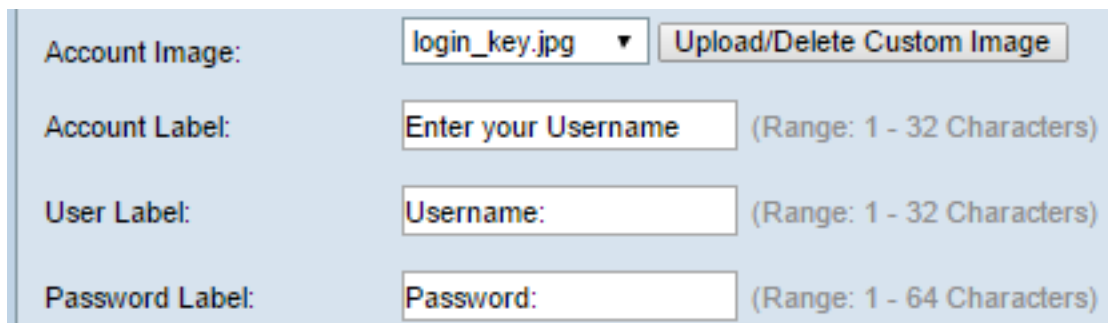
Étape 41. Dans le champ *Couleur d'arrière-plan*, saisissez le code HTML à 6 chiffres pour la couleur d'arrière-plan des paramètres régionaux.

Étape 42. Dans le champ *Séparateur*, saisissez le code HTML à 6 chiffres pour la couleur de la ligne horizontale qui sépare l'en-tête de page du corps de la page.

Étape 43. Entrez un nom descriptif pour les paramètres régionaux dans le champ *Étiquette de paramètres régionaux*. Si vous avez plusieurs paramètres régionaux, il s'agit du nom du lien que vous cliquez pour changer entre les paramètres régionaux. Par exemple, si vous avez des paramètres régionaux anglais et espagnol, vous pouvez indiquer cela dans votre nom de paramètres régionaux.

Étape 44. Entrez une abréviation pour les paramètres régionaux dans le champ *Paramètres régionaux*.

Étape 45. Dans la liste déroulante Image du compte, sélectionnez une image à afficher au-dessus du champ de connexion.



The image shows a light blue form with the following fields:

- Account Image:** A dropdown menu showing 'login_key.jpg' and a button labeled 'Upload/Delete Custom Image'.
- Account Label:** A text input field containing 'Enter your Username' with a character range '(Range: 1 - 32 Characters)'.
- User Label:** A text input field containing 'Username:' with a character range '(Range: 1 - 32 Characters)'.
- Password Label:** A text input field containing 'Password:' with a character range '(Range: 1 - 64 Characters)'.

Étape 46. Dans le champ *Libellé du compte*, entrez les instructions qui demandent à l'utilisateur d'entrer son nom d'utilisateur.

Étape 47. Dans le champ *Étiquette utilisateur*, saisissez l'étiquette de la zone de texte Nom d'utilisateur.

Étape 48. Dans le champ *Password Label*, saisissez l'étiquette de la zone de texte password.

Étape 49. Dans le champ *Bouton Étiquette*, saisissez l'étiquette du bouton sur lequel les utilisateurs cliquent pour envoyer leur nom d'utilisateur et leur mot de passe.

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)

Étape 50. Dans le champ *Polices*, saisissez le nom de police utilisé pour les paramètres régionaux. Vous pouvez entrer plusieurs noms de police séparés par une virgule. Si le périphérique client ne trouve pas le premier style de police, la police suivante est utilisée. Si un nom de police comporte plusieurs mots séparés par des espaces, utilisez des guillemets simples pour entourer le nom de police. Par exemple, 'MS UI Gothic' , arial, sans-serif, et ainsi de suite.

Étape 51. Dans le champ *Titre du navigateur*, saisissez le texte que vous souhaitez afficher dans la barre de titre du navigateur.

Étape 52. Dans le champ *Contenu du navigateur*, saisissez le texte que vous souhaitez afficher dans l'en-tête de la page.

Étape 53. Dans le champ *Contenu*, saisissez le texte qui indique à l'utilisateur ce qu'il doit faire. Ce champ est affiché sous les zones de texte nom d'utilisateur et mot de passe.

Étape 54. Dans le champ *Politique d'utilisation des acceptations*, saisissez les conditions auxquelles les utilisateurs doivent accepter s'ils veulent accéder au WAP.

Étape 55. Dans le champ *Accepter l'étiquette*, saisissez le texte qui demande aux utilisateurs de vérifier qu'ils ont lu et accepté la politique d'utilisation d'acceptation.

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)

Étape 56. Dans le champ *Aucun texte accepté*, saisissez le texte qui invite un utilisateur à envoyer des informations d'identification de connexion mais qui n'accepte pas la politique d'utilisation d'acceptation.

Étape 57. Dans le champ *Work In Progress Text*, saisissez le texte affiché pendant que le WAP vérifie les informations d'identification fournies.

Étape 58. Dans le champ *Texte refusé*, saisissez le texte affiché lorsqu'un utilisateur échoue à l'authentification.

Étape 59. Dans le champ *Titre de bienvenue*, saisissez le texte de titre qui s'affiche lorsqu'un client est authentifié avec succès.

Étape 60. Dans le champ *Welcome Content*, saisissez le texte affiché à un client qui s'est connecté au réseau.

Welcome Title: (Range: 1 - 12)

Welcome Content: (Range: 1 - 25)

Delete Locale:

Étape 61. (Facultatif) Pour supprimer les paramètres régionaux actuels, cochez la case **Supprimer les paramètres régionaux**.

Étape 62. Cliquez sur **Save**.

Étape 63. (Facultatif) Pour afficher vos paramètres régionaux actuels, cliquez sur **Aperçu**. Si vous apportez des modifications, cliquez sur **Enregistrer** avant d'afficher l'aperçu pour mettre à jour les modifications.

Note: L'écran de connexion au portail captif ressemble à l'image suivante :

Welcome to the Wireless Network

Enter your Username

Username:

Acceptance Use Policy.

Check here to indicate th the Acceptance Use Policy.

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

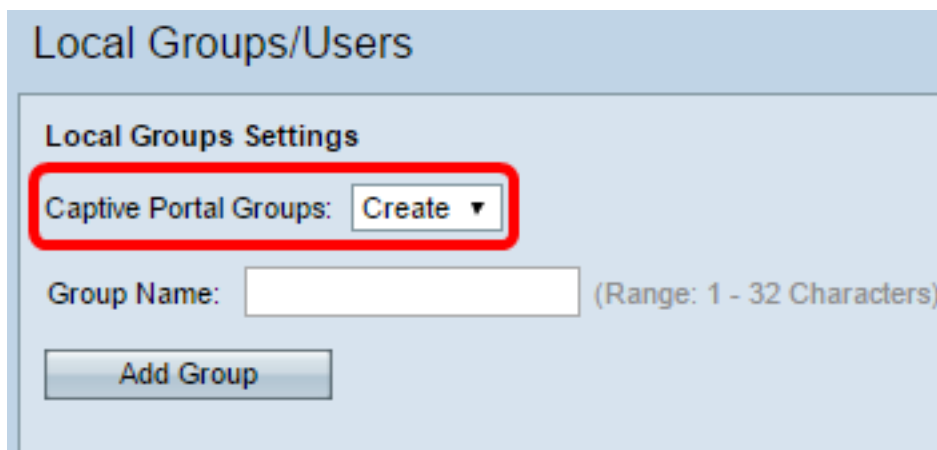
Créer un groupe local

Un portail captif non invité nécessite que les utilisateurs se connectent en fonction de leur nom d'utilisateur et de leur mot de passe. Le WAP crée un groupe local qui contient un groupe d'utilisateurs locaux. Le groupe local est ensuite attaché à une instance. Les utilisateurs locaux qui sont membres du groupe local peuvent accéder au portail captif. Le groupe local par défaut est toujours actif et ne peut pas être supprimé. Vous pouvez ajouter jusqu'à deux groupes locaux supplémentaires au WAP.

Étape 64. Dans l'utilitaire Web, sélectionnez **Captive Portal > Local Groups/Users**.



Étape 65. Choisissez **Créer** dans la liste déroulante Groupes de portails captifs.



Étape 66. Entrez le nom du groupe local dans le champ *Nom du groupe*.

Local Groups/Users

Local Groups Settings

Captive Portal Groups: Create ▾

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

Add Group

Étape 67. Cliquez sur **Ajouter un groupe** pour enregistrer le groupe.

Local Groups/Users

Local Groups Settings

Captive Portal Groups: Create ▾

Group Name: (Range: 1 - 32 Characters)

Add Group

Note: Vous pouvez affecter un groupe local à une instance à l'[étape 19](#) de la section Configuration d'instance.

Créer un utilisateur local

Les utilisateurs locaux sont ajoutés à un groupe local. Ces utilisateurs peuvent accéder à un portail captif dont une instance est configurée avec leur groupe local. Certaines informations configurées dans la page Utilisateurs locaux sont également configurées dans la page Configuration de l'instance. La valeur configurée pour un utilisateur local a priorité sur la valeur configurée pour une instance. Vous pouvez configurer jusqu'à 128 utilisateurs autorisés dans la base de données locale.

Étape 68. Choisissez **Créer** dans la liste déroulante Utilisateurs du portail captif.

Local Users Settings

Captive Portal Users: Create ▾

User Name: (Range: 1 - 32 Characters)

Add User

Étape 69. Dans le champ *Nom d'utilisateur*, saisissez le nom d'utilisateur à ajouter.

Local Users Settings

Captive Portal Users:

User Name: (Range: 1 - 32 Characters)

Étape 70. Cliquez sur **Ajouter un utilisateur** pour créer le nouvel utilisateur. La fenêtre Paramètres des utilisateurs locaux affiche des informations supplémentaires.

Local Users Settings

Captive Portal Users:

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

Show Password as Clear Text

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

Group Name:

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

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

Delete User:

Étape 71. Dans le champ *Mot de passe utilisateur*, saisissez le mot de passe associé à l'utilisateur.

Étape 72. (Facultatif) Pour afficher le mot de passe en texte clair, cochez la case **Afficher le mot de passe en texte clair**. Si la case est décochée, le mot de passe est masqué.

Étape 73. Dans le champ *Délai d'expiration de mise hors service*, saisissez la durée (en minutes) pendant laquelle un utilisateur peut être dissocié du WAP et rester dans la liste des clients authentifiés du WAP. Si l'utilisateur n'est pas connecté au WAP plus longtemps que le délai d'attente absent, il doit être réautorisé avant de pouvoir utiliser le WAP.

Étape 74. Dans le champ *Nom du groupe*, cliquez sur le groupe local auquel vous souhaitez que l'utilisateur se connecte.

Étape 75. Dans le champ *Bande passante maximale en amont*, saisissez la vitesse de téléchargement maximale en Mbits/s qu'un client peut envoyer des données via le portail

captif.

Étape 76. Dans le champ *Bande passante maximale en aval*, saisissez la vitesse de téléchargement maximale en Mbits/s qu'un client peut recevoir des données via le portail captif.

Étape 77. (Facultatif) Pour supprimer un utilisateur local, cochez la case **Supprimer un utilisateur**.

Étape 78. Cliquez **Save**.

Vous devez maintenant configurer les paramètres avancés du portail captif de votre WAP571 ou WAP571E.