Create Captive Portal on the WAP561 and WAP551

Objective

A captive portal allows you to restrict access to your network until wireless users have been verified. When a user opens their web browser, they are redirected to a login page where they must enter their username and password. Two types of users can be authorized to access your network, authenticated users and guests. Authenticated users must provide a username and password that matches either a local database, or the database of a RADIUS server. Guests do not need to provide a username or password. This article explains how to create a captive portal on both the WAP561 and WAP551.

To create a captive portal on the Wireless Access Point (WAP), you must follow several steps:

- Globally enable captive portals on the WAP. This allows captive portals to take effect.
- Create a captive portal instance. A captive portal instance is a set of parameters that control how a user logs on to a virtual access point (VAP).
- Associate a captive portal instance with a VAP. Users who attempt to access the VAP have to follow the parameters that are configured for the instance.
- Customize the web portal. The web portal is the web page that users are taken to when they attempt to log on to the VAP.
- Create local group. The local group can be assigned to an instance, which accepts users who belong to that group.
- Create local user. Local users are added to a local group and are allowed to access the captive portal that the group is configured to.

Applicable Devices

- WAP551
- WAP561

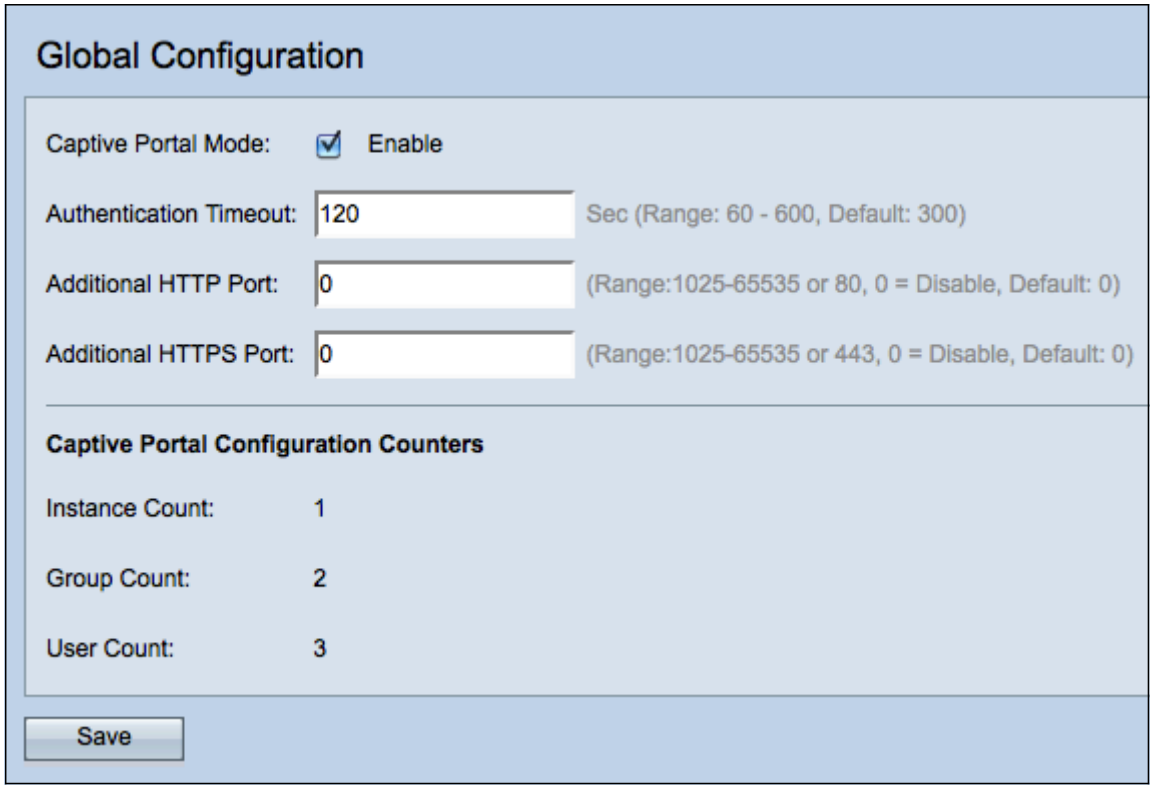
Software Version

- v1.0.4.2

Create Guest Captive Portal

Enable Global Configuration

Step 1. Log in to the web configuration utility to choose **Captive Portal > Global Configuration**. The *Global Configuration*page opens:



Step 2. Check the **Enable** check box in the *Captive Portal Mode* field to enable captive portal (CP) on the WAP.

Step 3. Enter the number of seconds that the user has to enter authentication information before the WAP closes the authentication session in the *Authentication Timeout* field.

Step 4. (Optional) If you would like HTTP information between the WAP and the client to use a different port besides the default, enter the HTTP port number you would like to add in the *Additional HTTP Port* field. HTTP and other Internet protocols use ports to make sure devices know where to find a certain protocol. The options are 80, between 1025 and 65535, or enter 0 to disable. The HTTP port and HTTPS port cannot be the same.

Step 5. (Optional) If you would like HTTP information between the WAP and the client to use a different port besides the default, enter the HTTPS port number you would like to add in the *Additional HTTPS Port* field. The options are 443, between 1025 and 65535, or enter 0 to disable. The HTTP port and HTTPS port cannot be the same.

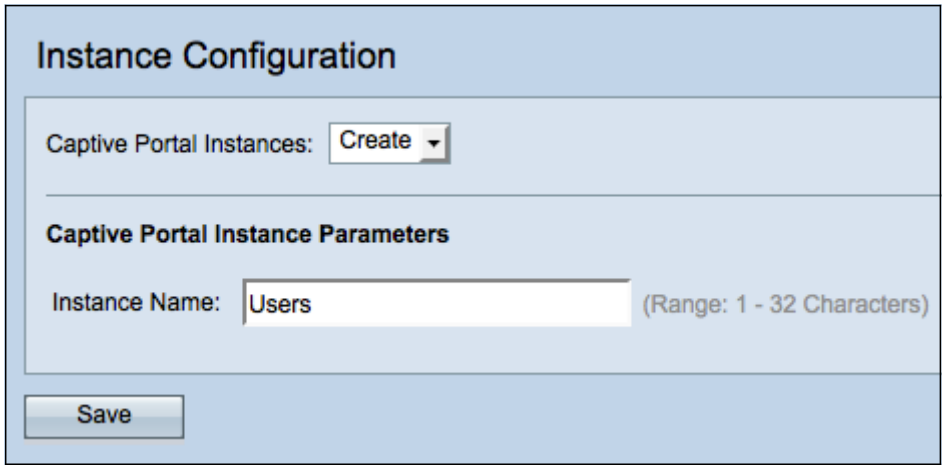
The following information is displayed in the *Captive Portal Configuration Counters* field and cannot be configured.

- Instance Count — The number of CP instances configured on the WAP device. A maximum of two CPs can be configured on the WAP.
- Group Count — The number of CP groups configured on the WAP device. Up to two groups can be configured. The Default Group cannot be deleted.
- User Count — The number of CP users configured on the WAP device. A maximum of 128 users can be configured on the WAP.

Step 6. Click **Save** to save your changes.

Instance Configuration

Step 1. Log in to the web configuration utility and choose **Captive Portal > Instance Configuration**. The *Instance Configuration* page opens:

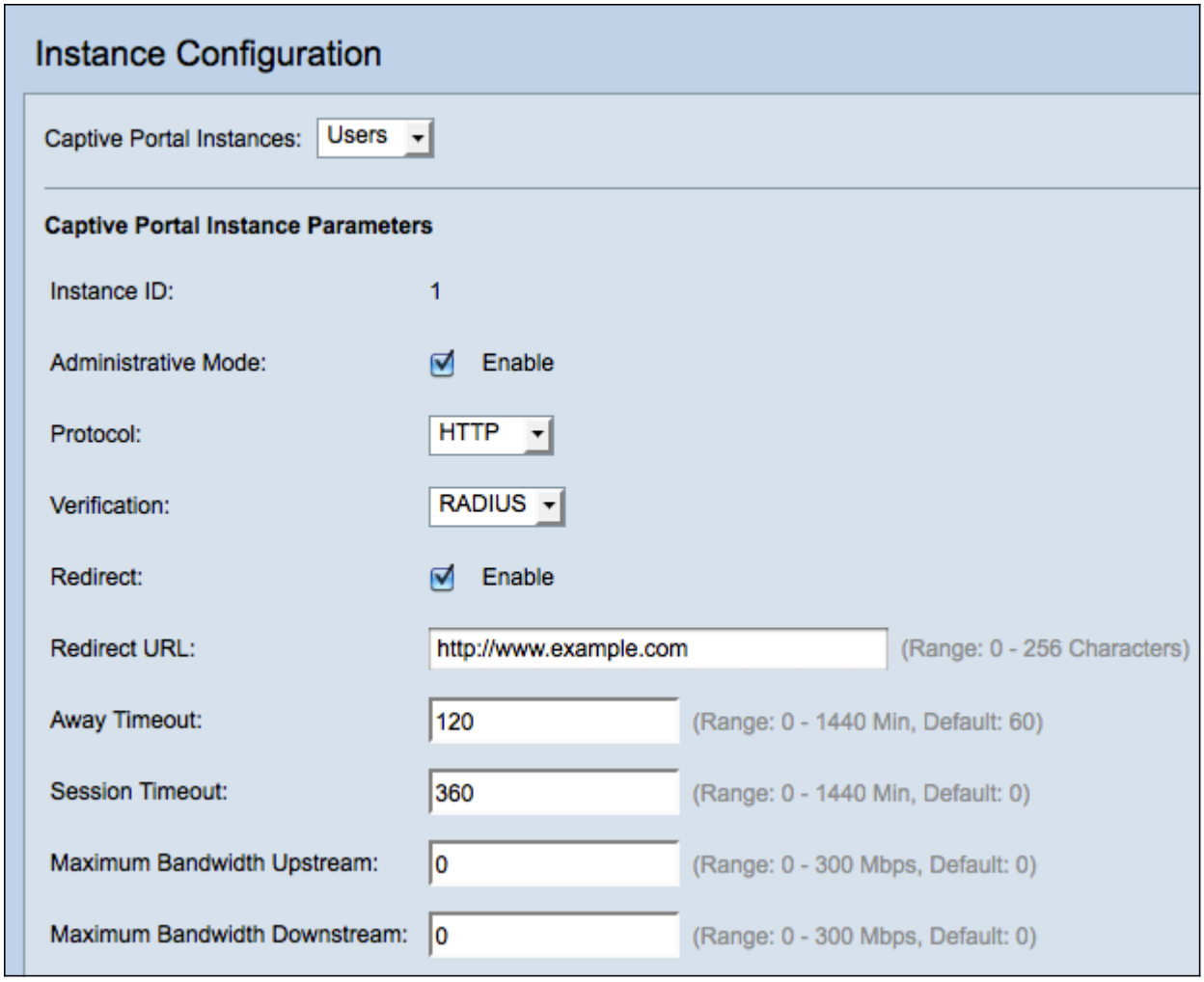


Step 2. Choose **Create** from the *Captive Portal Instances* drop-down list to create a new instance.

Step 3. In the *Instance Name* field, enter a name for the configuration.

Note: You can create a maximum of up to two configurations. If you have already created two instances, you have to choose an instance to edit.

Step 4. Click **Save** to create the instance. The *Instance Configuration* page displays additional information. The Instance ID is a non-configurable field that shows the instance ID of the current instance.



Step 5. (Optional) Choose a different instance to configure from the *Captive Portal Instances* drop-down list.

Step 6. Check the **Enable** check box in the *Administrative Mode* field to enable the CP instance.

Step 7. From the *Protocol* drop-down list, choose the protocol you would like to use for the authentication process.

- HTTP — Does not encrypt information used in the authentication process.
- HTTPS — Provides encryption for information used in the authentication process.

Step 8. Choose an authentication method for CP to use from the *Verification* drop-down list.

- Guest — The user does not need to provide any authentication.
- Local — The WAP checks the authentication information provided by the user against a local database that is stored on the WAP.
- RADIUS — The WAP checks the authentication information provided by the user against the database of a remote RADIUS server.

Step 9. (Optional) If you want to redirect users who are verified to a configured URL, check the **Enable** check box in the *Redirect* field. If this option is disabled, verified users will see a locale-specific welcome page.

Step 10. Enter the URL to which you would like to redirect verified users to. This step is only

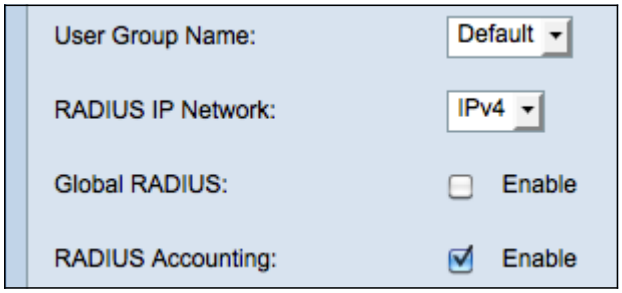
applicable if you enabled **Redirect** in Step 9.

Step 11. In the *Away Timeout* field, enter the amount of time (in minutes) that a user can be disassociated from the WAP and remain on the WAP authenticated client list. If the user is not connected to the WAP for longer then the *Away Timeout* value, they have to be reauthorized before they can use the WAP.

Step 12. In the *Session Timeout* field, enter the amount of time (in minutes) that the WAP waits before it terminates the session. A value of 0 means the timeout is not enforced.

Step 13. In the *Maximum Bandwidth Upstream* field, enter the maximum upload speed (in Mbps) that a client can send data via the captive portal.

Step 14. In the *Maximum Bandwidth Downstream* field, enter the maximum download speed (in Mbps) that a client can receive data via the captive portal.



Step 15. From the *User Group Name* drop-down list, choose the group that you wish to assign to the CP instance. Any user that is a member of the group you choose is allowed to access the WAP.

Note: The Verification mode in Step 8 must be either Local or RADIUS to assign a group.

Timesaver: If you chose **Local** or **Guest** as your verification in Step 8, skip to Step 23.

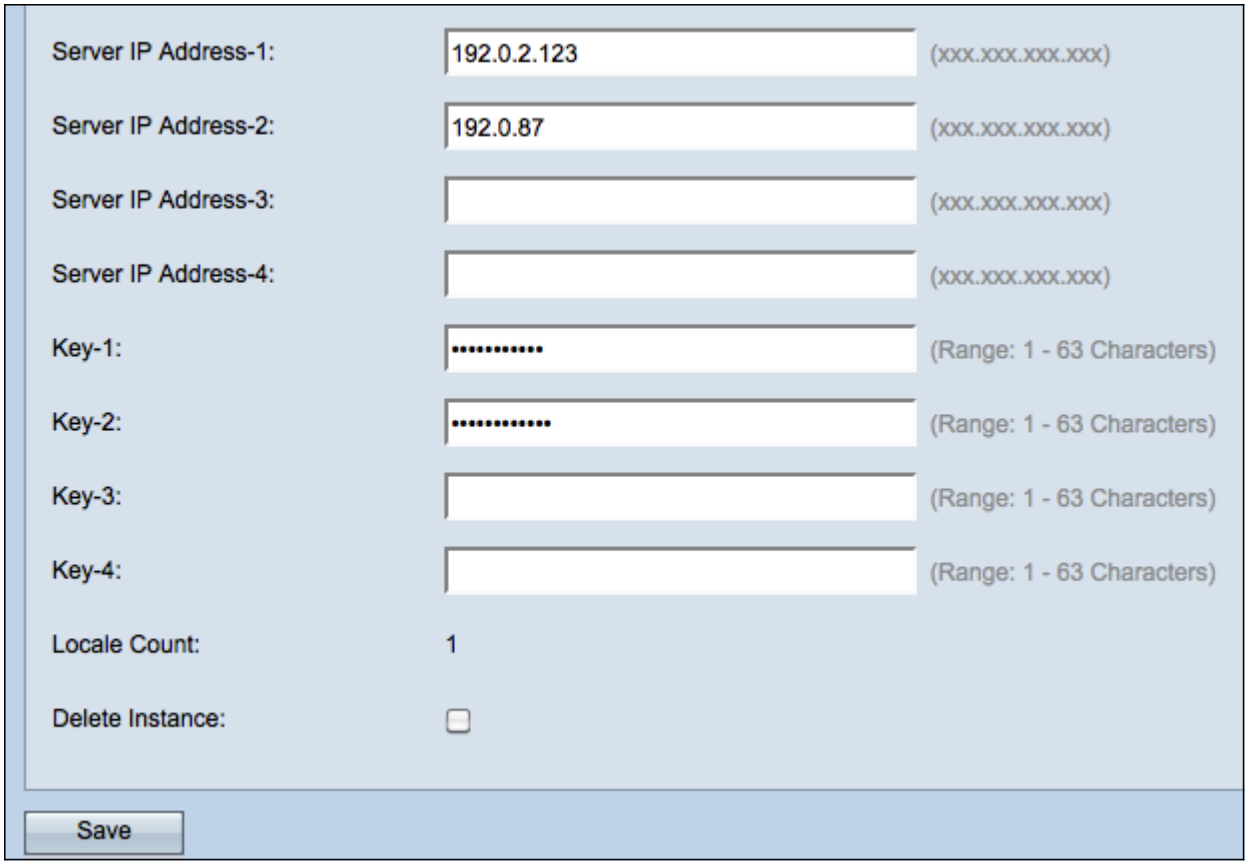
Step 16. From the *RADIUS IP Network* field, choose the type of Internet protocol that is used by the RADIUS client.

- IPv4 — The address of the RADIUS client will be in the format xxx.xxx.xxx.xxx (192.0.2.10).
- IPv6 — The address of the RADIUS client will be in the format xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (2001:DB8::CAD5:7D91).

Step 17. In the *Global RADIUS* field, check the **Enable** check box if you want to use the global radius server list for authentication. If you want to use a separate set of RADIUS servers, leave the check box unchecked and configure the RADIUS servers on this page.

Timesaver: Skip to Step 23 if you enable **Global RADIUS.**

Step 18. In the *RADIUS Accounting* field, check the **Enable** check box if you want to track and measure the time and data usage of the clients on the WAP network.



Note: If the **Global RADIUS** check box was enabled in Step 17, you do not need to configure additional RADIUS servers.

Step 19. In the *Server IP Address-1* field, enter the IP address of the RADIUS server which you want to use as the primary server. The IP address should conform with the respective address format of IPv4 or IPv6.

Step 20. (Optional) You can configure up to three backup RADIUS servers which will be checked in sequence until a match is found. If no match is found, the user will be denied access. In the *Server IP Address-(2 to 4)* fields, enter the IP address of the backup RADIUS servers to use if authentication fails with the primary server.

Step 21. In the *Key-1* field, enter the shared secret key that the WAP device uses to authenticate to the primary RADIUS server. This needs to be the same key that was configured on the RADIUS server.

Step 22. In the rest of the *Key fields (2-4)*, enter the shared secret key that the WAP device uses to authenticate to the respective backup radius servers.

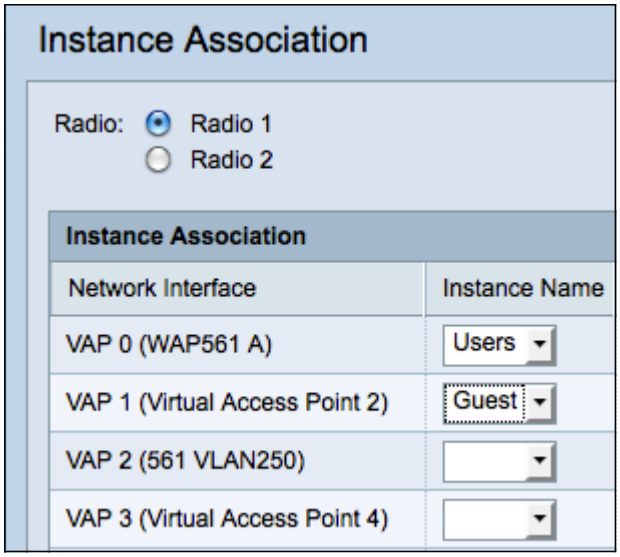
Note:*Locale Count* is a non-configurable field that displays the number of locales associated with this instance.

Step 23. (Optional) To delete the currant instance, check the **Delete Instance** check box.

Step 24 Click **Save** to save your changes.

Associate Instance with VAP

Step 1. Log in to the web configuration utility and choose **Captive Portal > Instance Association**. The *Instance Association* page opens:



Step 2. Click the radio button of the radio to which you would like to associate an instance in the *Radio* field.

Note: Step 2 is only applicable for the WAP561, because the WAP551 only has one radio.

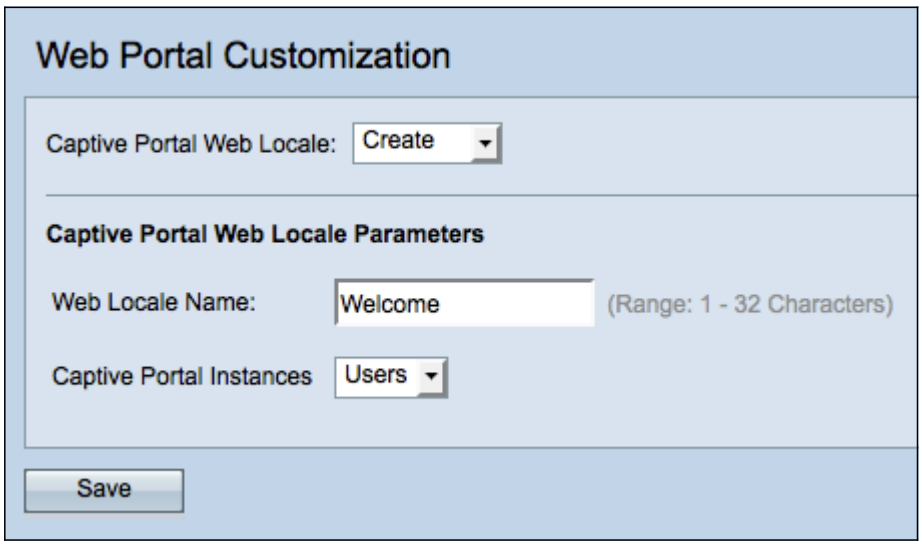
Step 3. Choose an instance configuration from the *Instance Name* drop-down list to associate with the given VAP.

Step 4. Click **Save** to save your changes.

Customize Web Portal

A locale (authentication web page) is the web page that the WAP user sees when they attempt to access the Internet. The *Web Portal Customization* page allows you to customize a locale and assign it to a captive portal instance.

Step 1. Log in to the web configuration utility and choose **Captive Portal > Web Portal Customization**. The *Web Portal Customization* page opens:

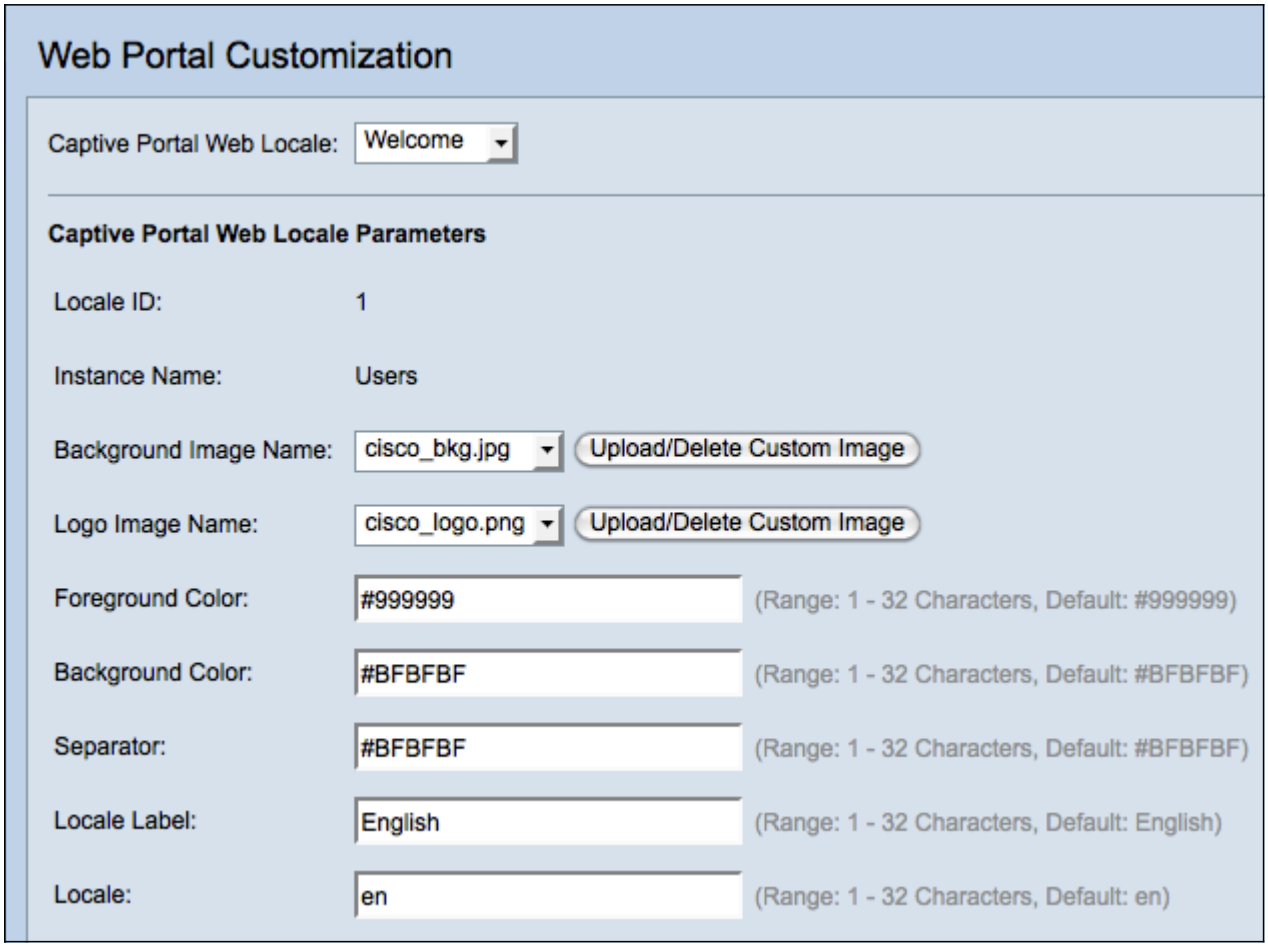


Step 2. Choose **Create** from the *Captive Portal Web Locale* drop-down list to create a new locale.

Step 3. Enter the name of the locale in the *Web Locale Name* field.

Step 4. Choose a captive portal instance that the locale is associated with from the *Captive Portal Instances* drop-down list. You may associate multiple locales to a single captive portal instance. The user can click a link to switch to a different locale.

Step 5. Click **Save** to create a new locale. The *Web Portal Customization* page displays additional information.



Note: Locale ID is a non-configurable field that displays the ID number of the current locale.

Note: *Instance Name* is a non-configurable field that displays the captive portal instance name that is associated with the locale.

Step 6. From the *Background Image Name* drop-down list, choose an image to display in the locale background. Click **Upload/Delete Custom Image** to add your own image. Go to the section *Upload/Delete Custom Image* for more information.

Step 7. From the *Logo Image Name* drop-down list, choose an image to display in the top left corner.

Step 8. In the *Foreground Color* field, enter the 6-digit HTML code for the foreground color of the locale.

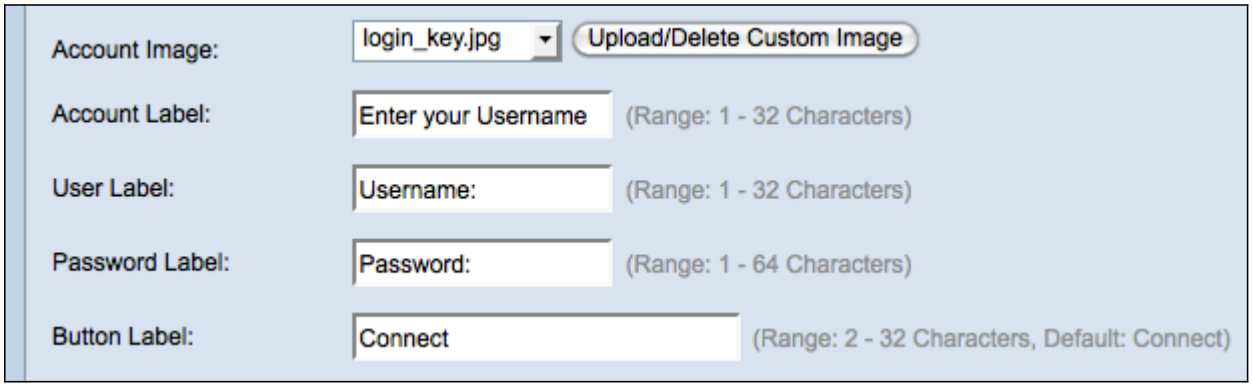
Step 9. In the *Background Color* field, enter the 6-digit HTML code for the background color of the locale.

Step 10. In the *Separator* field, enter the 6-digit HTML code for the color of the horizontal line that separates the page header from the page body.

Step 11. Enter a descriptive name for the locale in the *Locale Label* field. If you have multiple

locales, this is the name of the link you click to change between locales. For example, if you have an English and Spanish locale, you may want to signify that in your locale name.

Step 12. Enter an abbreviation for the locale in the *Locale* field.



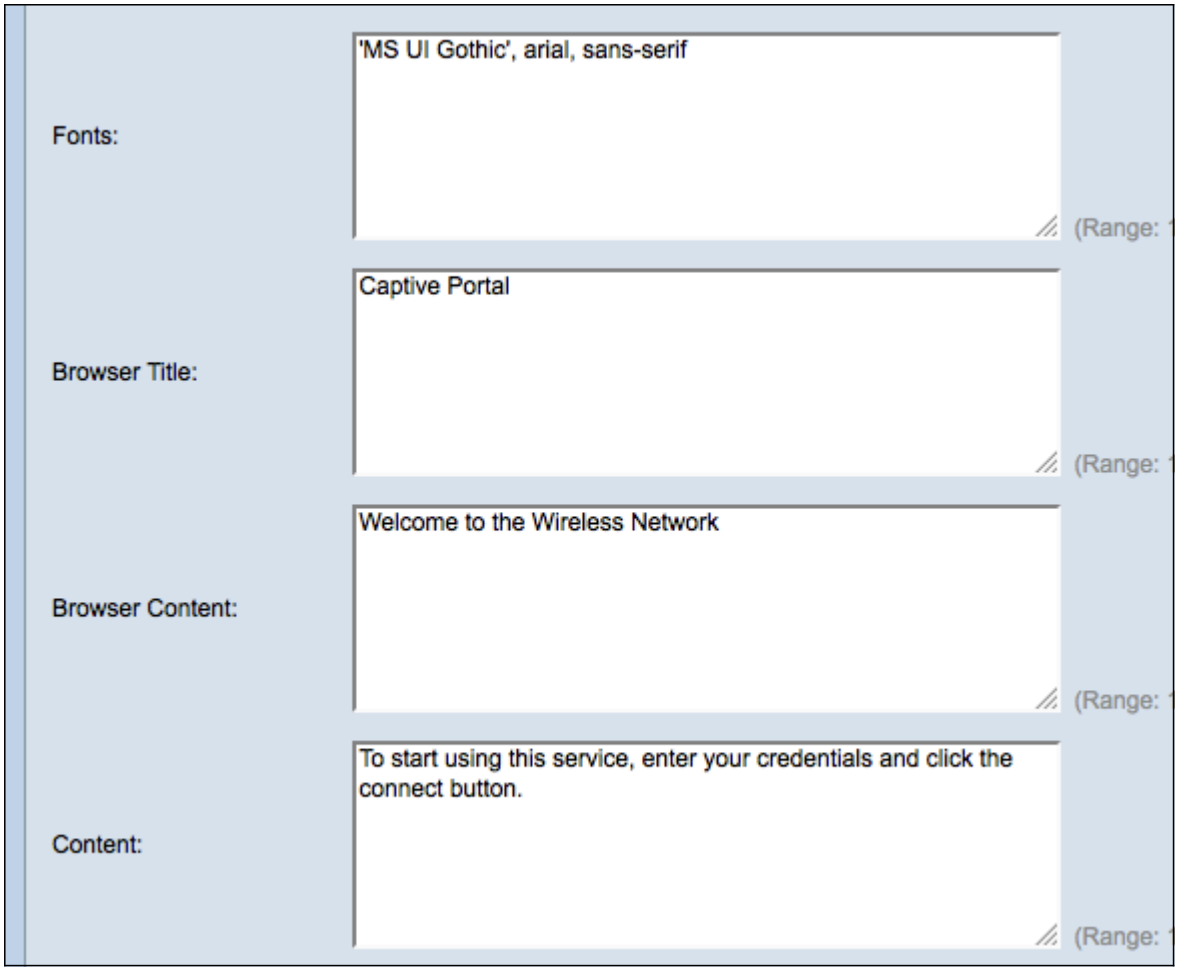
Step 13. From the *Account Image* drop-down list, choose an image to display above the login field.

Step 14. In the *Account Label* field, enter the instructions that tell the user to enter their username.

Step 15. In the *User Label* field, enter the label for the user name text box.

Step 16. in the *Password Label* field, enter the label for the password text box.

Step 17. In the *Button Label* field, enter for label for the button that the users click to submit their username and password.

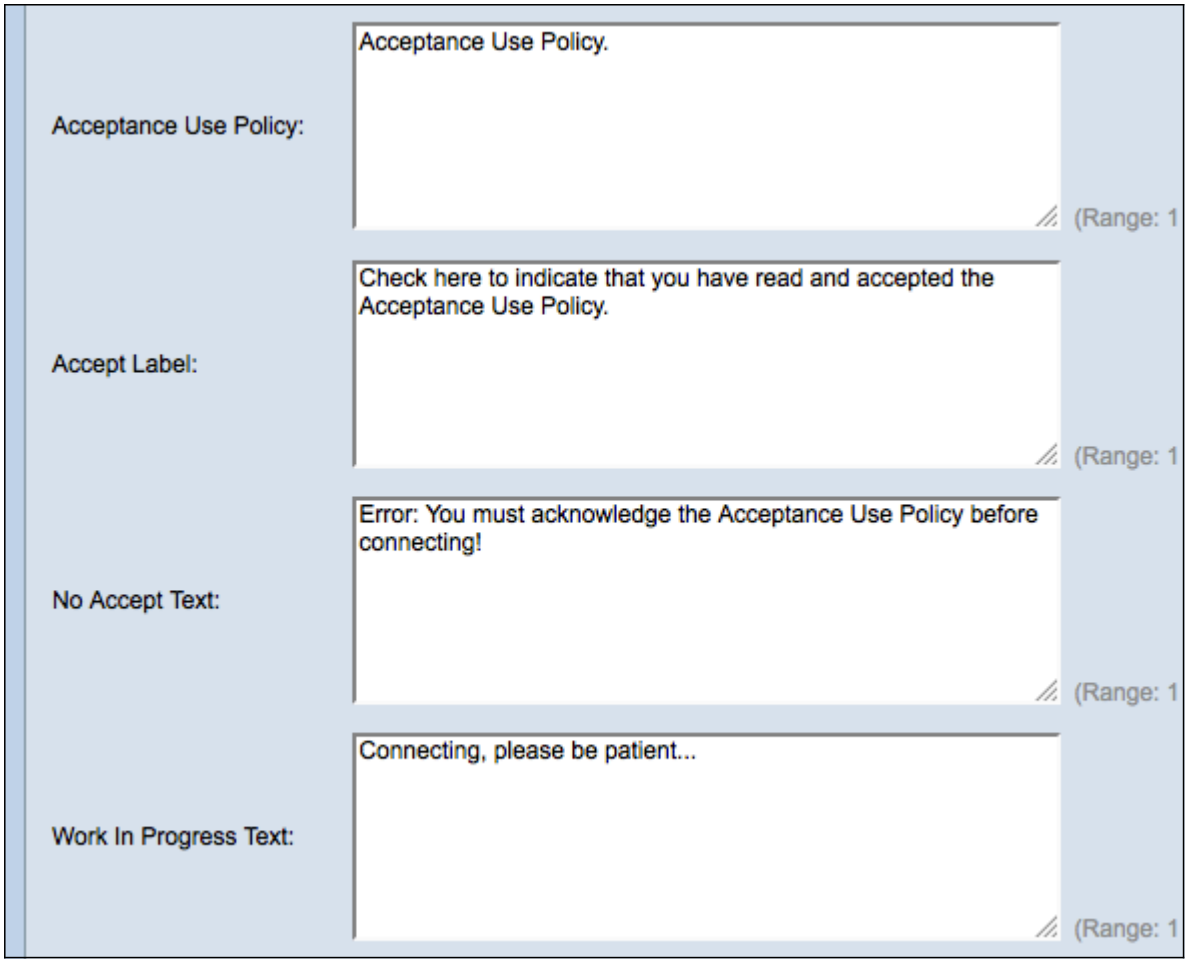


Step 18. In the *Fonts* field, enter the font name used for the locale. You may enter several font names separated by a comma. If the first font style is not found by the client device, the next font is used. If a font name has multiple words separated by spaces, use single quotes to surround the font name.

Step 19. In the *Browser Title* field, enter the text you would like to display in the browser title bar.

Step 20. In the *Browser Content* field, enter the text you would like to display in the page header.

Step 21. In the *Content* field,enter the text that instructs the user on what to do. This field is shown below the user name and password text boxes.

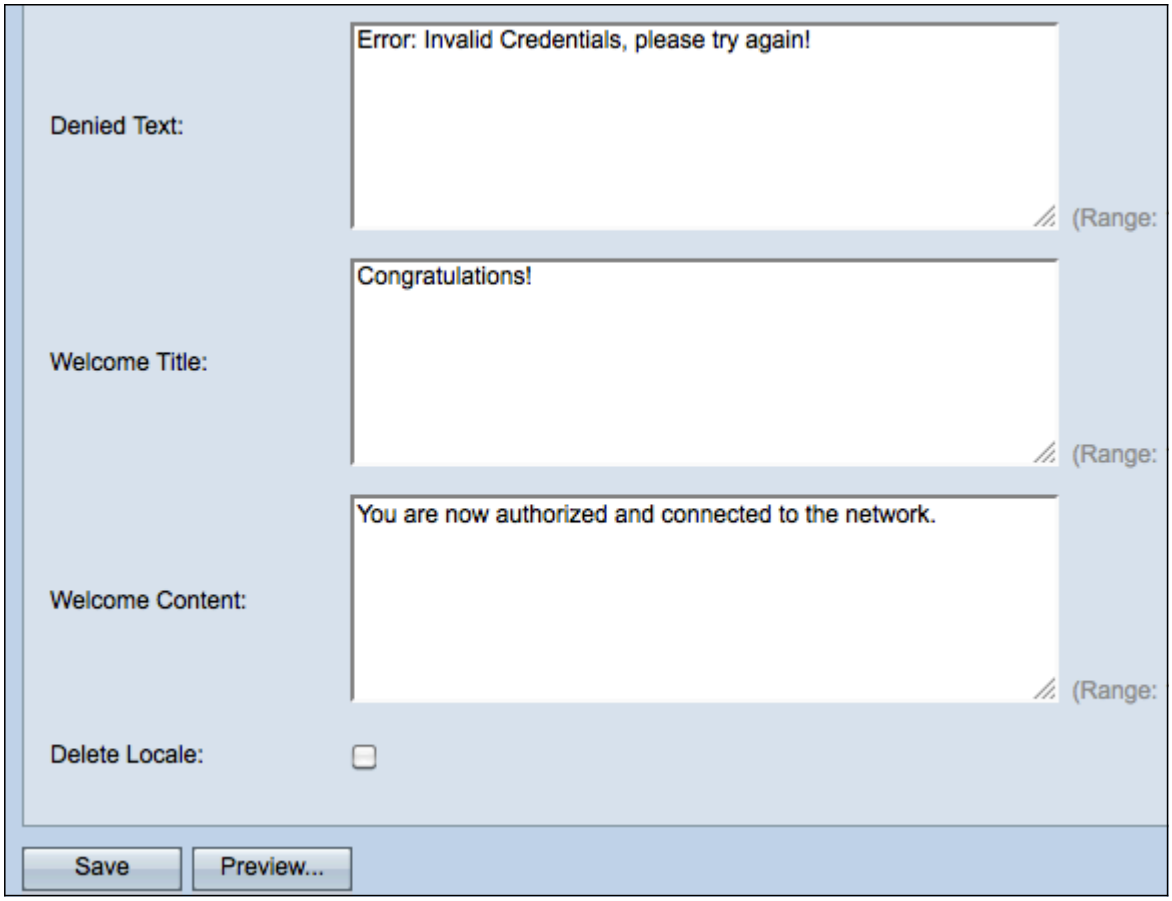


Step 22. In the *Acceptance Use Policy*, enter the terms that users must agree to if they want to access the WAP.

Step 23. In the *Accept Label* field, enter the text that instructs users to check that they have read and accept the Acceptance Use Policy.

Step 24. In the *No Accept Test* field, enter the text that warns a user if they submit login credentials but do not accept the Acceptance Use Policy.

Step 25. In the *Work In Progress Text* field, enter the text that is shown while the WAP checks the given credentials.



Step 26. In the *Denied Text* field, enter the text that is shown when a user fails authentication.

Step 27. In the *Welcome Title* field, enter the title text that is shown when a client is successfully authenticated.

Step 28. In the *Welcome Content* field, enter the text that is shown to a client who has connected to the network.

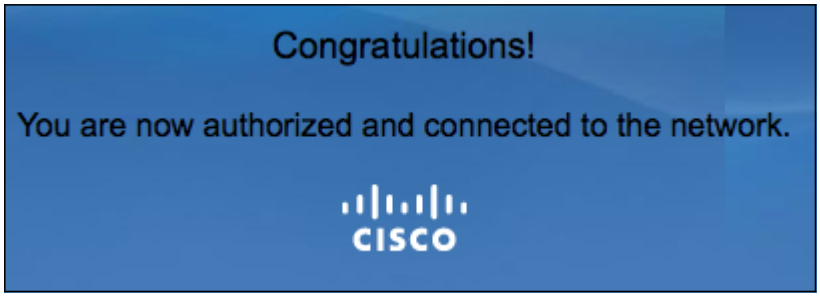
Step 29. (Optional) To delete the currant locale, check the **Delete Locale** check box.

Step 30. Click **Save** to save your changes.

Step 31. (Optional) To view your current locale, click **Preview**. If you make changes, click **Save** before you preview to update the changes.

Note: The captive portal login screen looks similar to the following image:

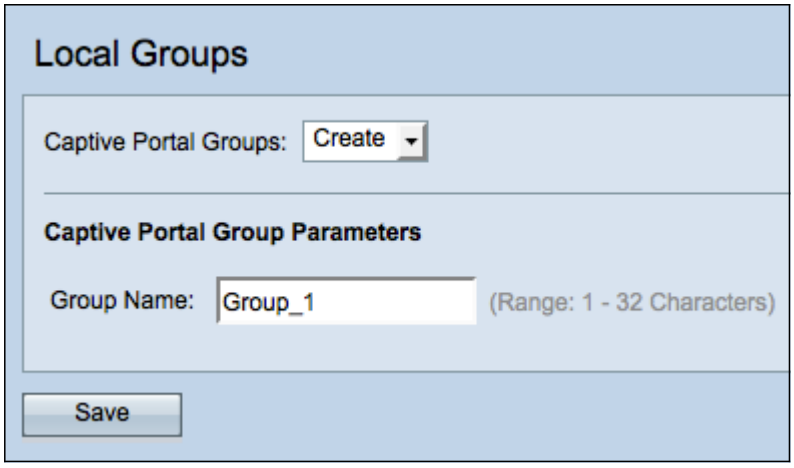
Note: Successful completion of the captive portal should result in the display of a window similar to the following:



Create Local Group

Note: A non-guest captive portal requires users to log in based on their username and password. The WAP creates a local group that contains a group of local users. The local group is then attached to an instance. Local users that are a member of the local group are able to gain access through the captive portal. The Default local group is always active and cannot be deleted. Up to two additional local groups can be added to the WAP.

Step 1. Log in to the web configuration utility and choose **Captive Portal > Local Groups**. The *Local Groups* page opens:



Step 2. Choose **Create** from the *Captive Portal Groups* drop-down list.

Step 3. Enter the name of the local group in the *Group Name* field.

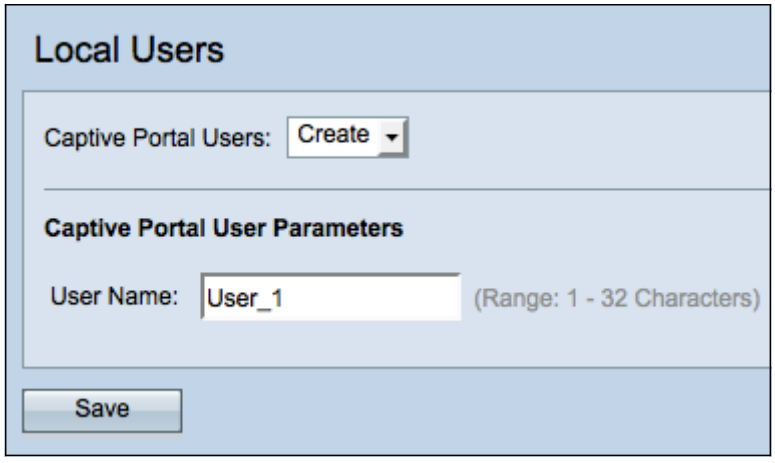
Step 4. Click **Save** to save the group.

Note: You assign a local group to an instance in Step 15 of the section titled *Instance Configuration*.

Create Local User

Note: Local users are added to a local group. These users are able to access a captive portal that has an instance with their local group configured. Some information that is configured in the *Local Users* page is also configured in the *Instance Configuration* page. The value configured for a local user has precedence over the value configured for an instance.

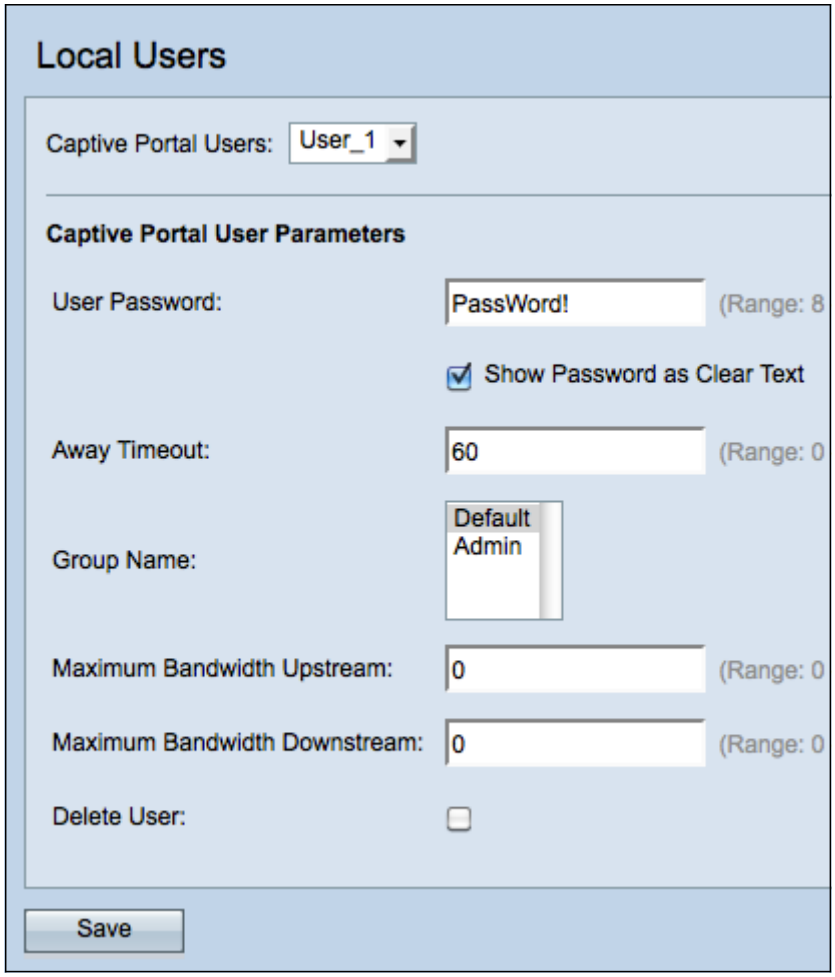
Step 1. Log in to the web configuration utility and choose **Captive Portal > Local Users**. The *Local Users* page opens:



Step 2. Choose **Create** from the *Captive Portal Users* drop-down list.

Step 3. In the *User Name* field, enter the user name you want to add.

Step 4. Click **Save** to create the new user. The *Local Users* page displays additional information.



Step 5. In the *User Password* field, enter the password associated with the user.

Step 6. (Optional) To have the password be displayed in clear text, check the **Show Password as Clear Text** check box. If the check box is unchecked, the password is masked.

Step 7. In the *Away Timeout* field, enter the amount of time a user can be disassociated from the WAP and remain on the WAP authenticated client list. If the user is not connected to the WAP for longer then the Away Timeout, they have to be reauthorized before they can use the WAP.

Step 8. In the *Group Name* field, click the local group you would like the user to join.

Step 9. In the *Maximum Bandwidth Upstream* field, enter the maximum upload speed in Mbps that a client can send data via the captive portal.

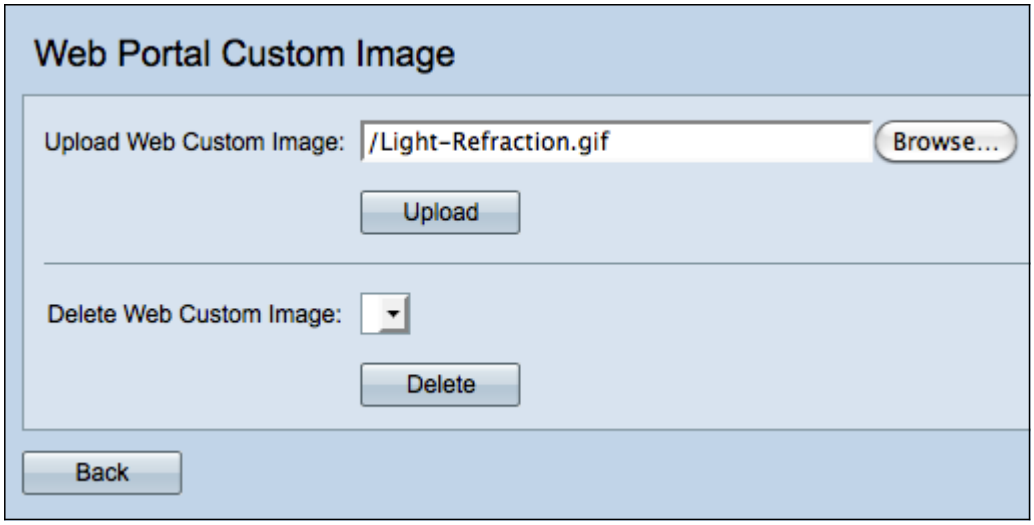
Step 10. In the *Maximum Bandwidth Downstream* field, enter the maximum download speed in Mbps that a client can receive data via the captive portal.

Step 11. (Optional) To delete a local user, check the **Delete User** check box.

Step 12. Click **Save** to save your changes.

Upload/Delete Custom Image

If you clicked the **Upload/Delete Custom Image** button in the *Background Image Name, Logo Image Name*, or *Account Image* field, the *Web Portal Custom Image* page opens:



Step 1. Click **Browse** in the *Upload Web Custom Image* field to browse your directory for a GIF or JPG image. Images must be 5 kilobytes or less in size.

Step 2. Click **Upload** to upload your image.

Step 3. (Optional) To delete an image, choose an image from the *Delete Custom Web Image* drop-down list and click **Delete**.

Step 4. Click **Back** to return to the *Web Portal Customization* page.

View a video related to this article...

Click here to view other Tech Talks from Cisco