Configuring Captive Portal on the WAP351 and WAP371 Access Points

Objective

Captive Portal allows you to require that users sign in to your wireless network using their web browser before accessing network resources or the Internet. This can be useful if you would like to have users agree to terms of use, or you would like to create user accounts for your wireless network.

The objective of this document is to show you how to configure captive portal on the WAP351 and WAP371.

Note: This document assumes that you have previously configured a VAP. For additional information on configuring a VAP, see *Configuring a VAP on the WAP351, WAP371, and WAP371*.

Applicable Devices

- WAP351
- WAP371

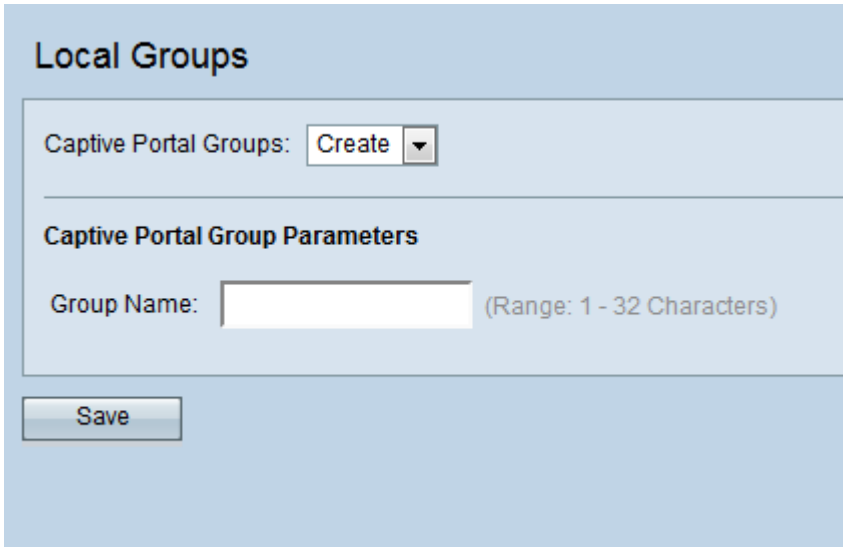
Create a Captive Portal

Create a New Local Group

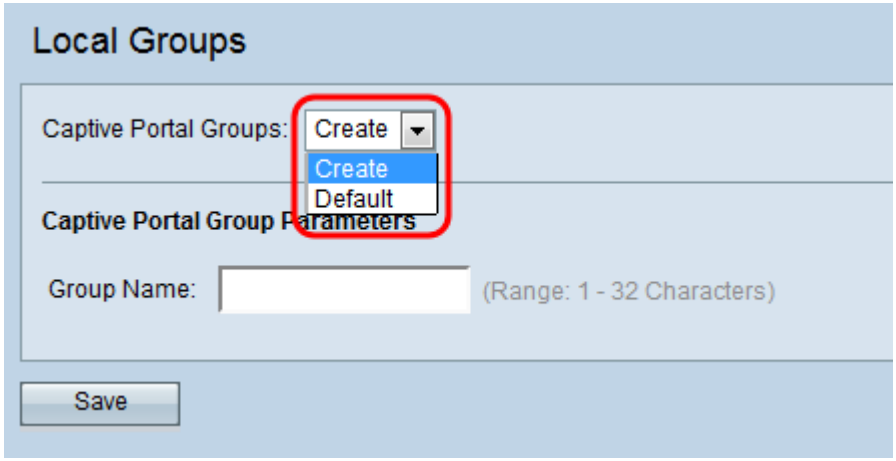
In order to allow authentication through the captive portal, local user accounts must be created on the WAP351/WAP371. Each local user must then be assigned to a user group, which can then be assigned to a captive portal instance. If you do not wish to create User Accounts, skip this section and proceed to *Create a Captive Portal Instance*.

Note: Optionally, you may choose to use the Default group. The Default group is built-in and cannot be removed. If you wish to use the Default group, skip this section and proceed to *Create a New Local User*.

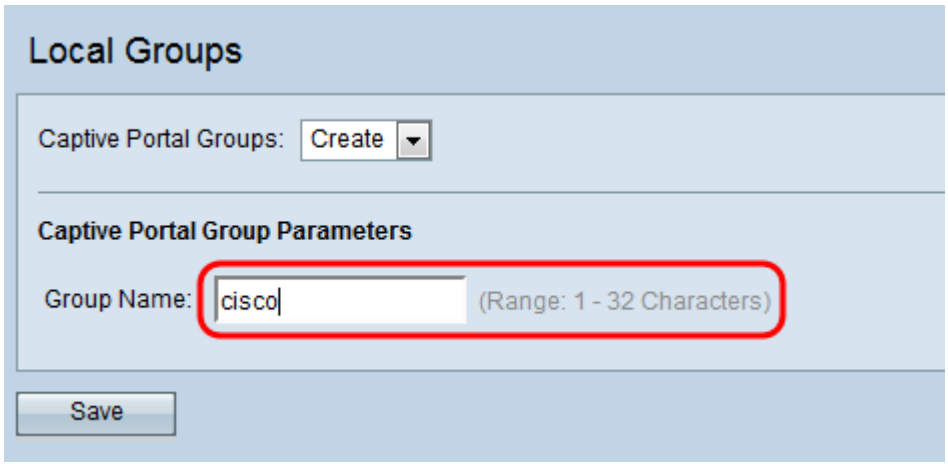
Step 1. Log in to the web configuration utility and choose **Captive Portal > Local Groups**. The *Local Groups* page appears:



Step 2. To create a new group, select **Create** from the *Captive Portal Groups* drop-down box.



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

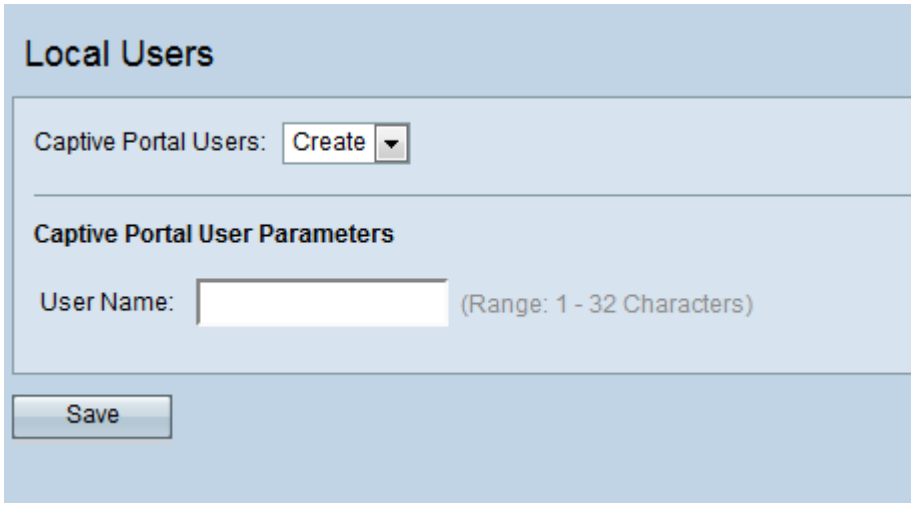


Step 4. Click **Save**.

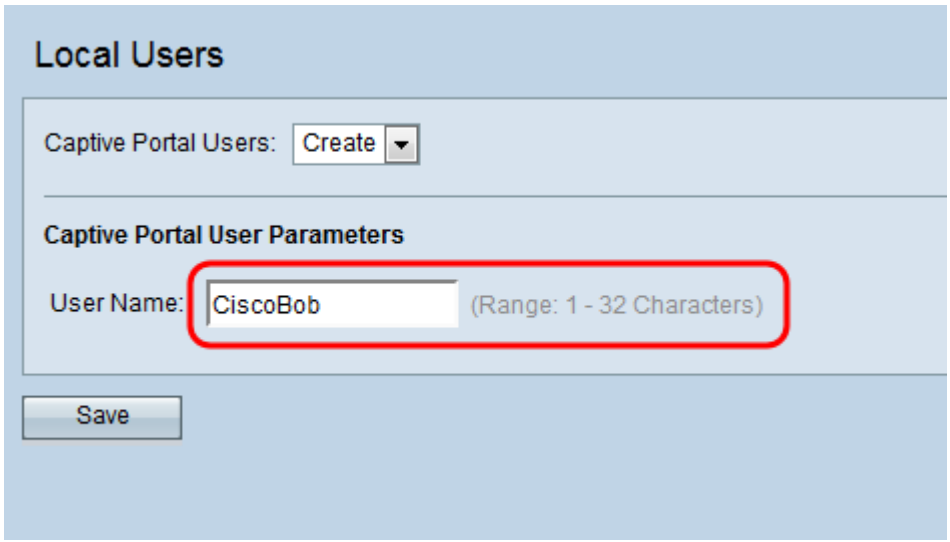
Create a New Local User

Users must be created in order to be authenticated and assigned to a group within the Captive Portal. Up to 128 authorized users can be created within the local database. If more than 128 users are desired, a RADIUS server must be used.

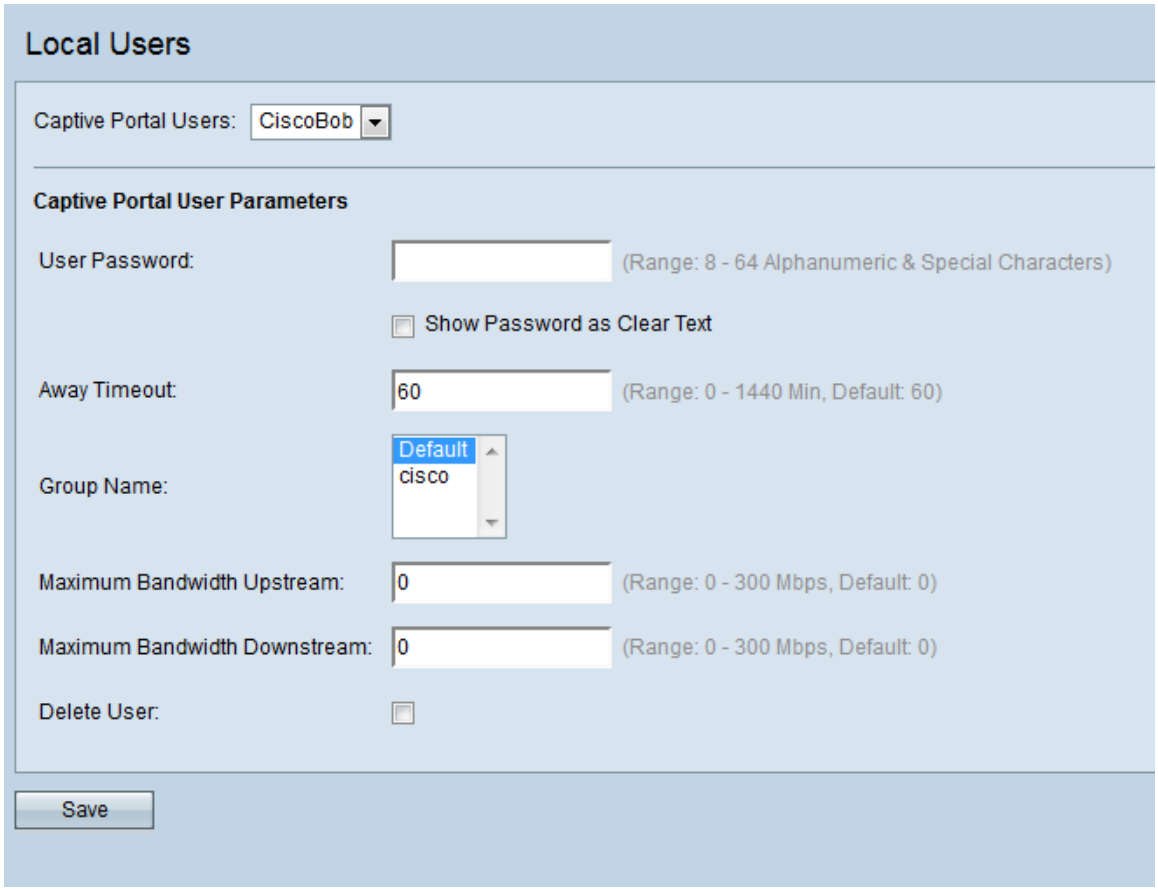
Step 1. Navigate to **Captive Portal > Local Users**. The *Local Users* page appears.



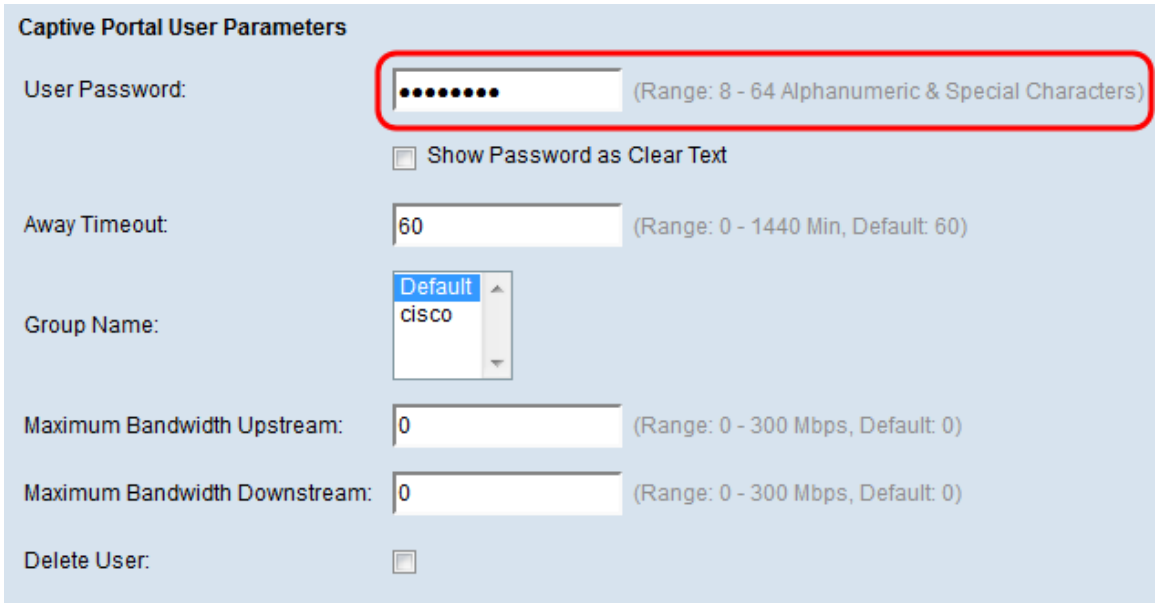
Step 2. Enter the desired user account name in the *User Name* field.



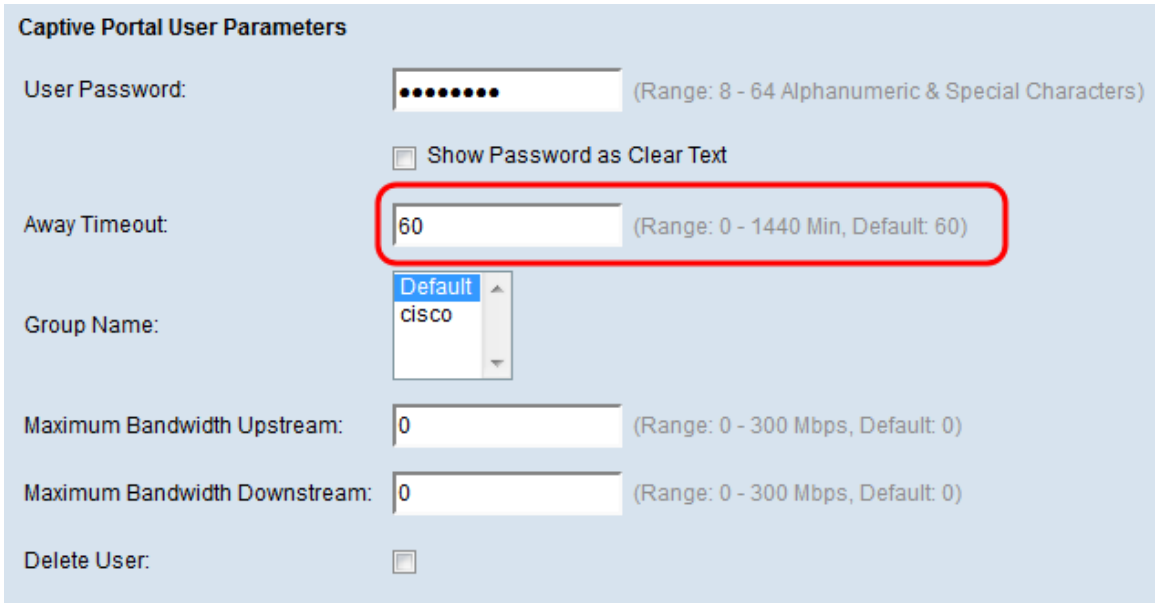
Step 3. Click **Save**. The *Captive Portal User Parameters* additional fields appear:



Step 4. Enter a password in the *User Password* field.

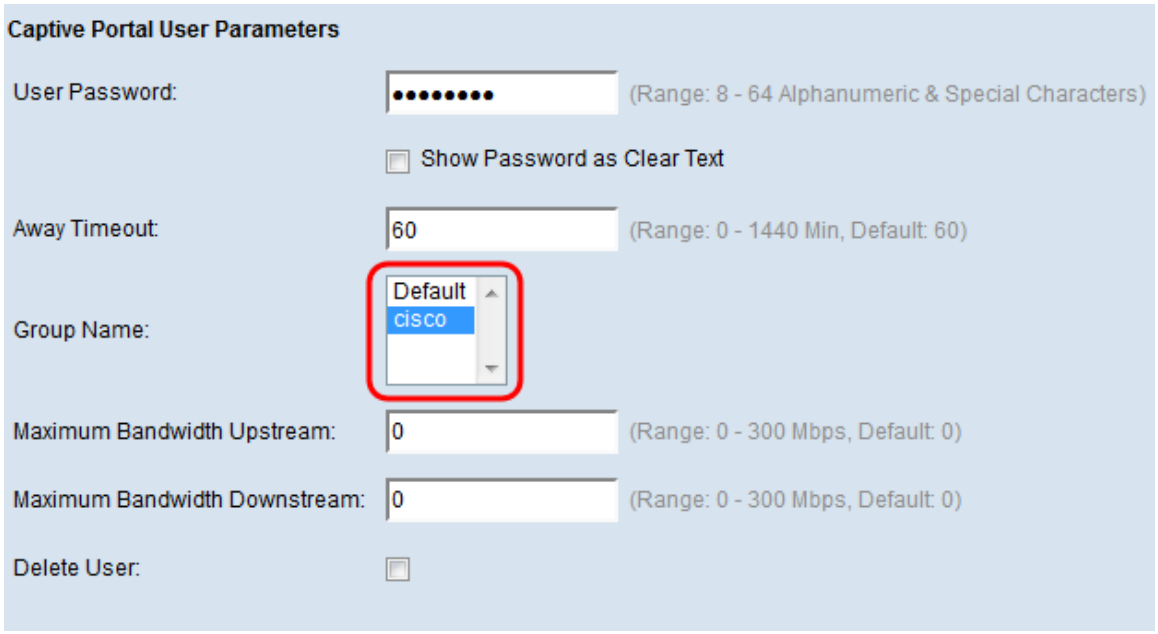


Step 5. In the *Away Timeout* field, enter the amount of time in minutes that the user remains logged after disconnecting from the device. If the user attempts to connect to the device within this period, they will not be prompted for a password. The default value for this field is 60, and the maximum is 1440.

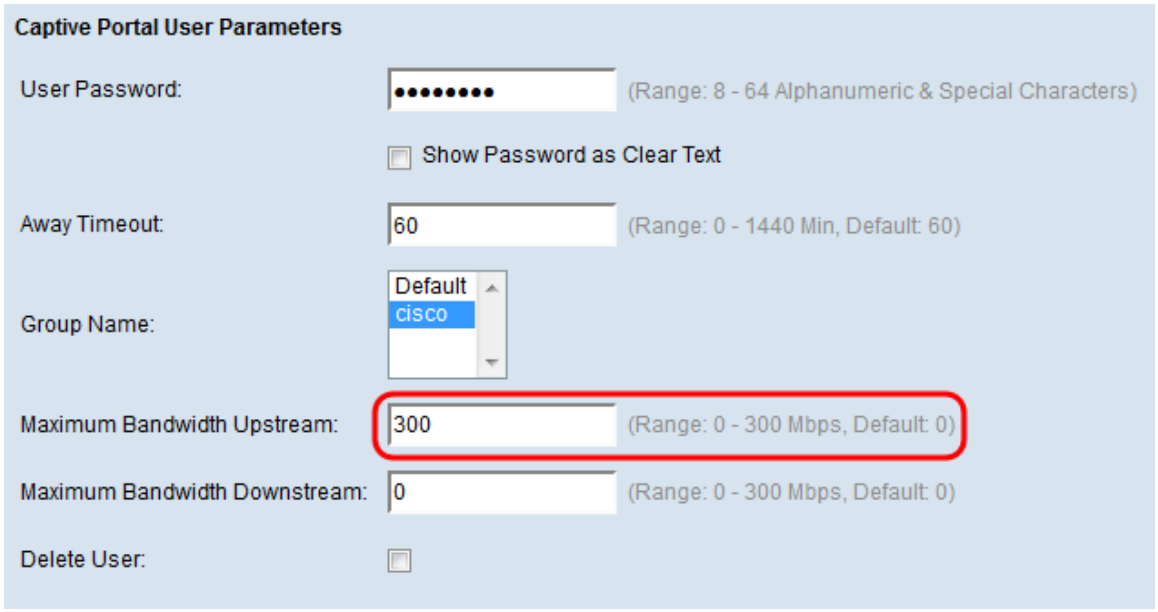


Note: A value of 0 in this box will cause the device to use the value set in Captive Portal Instance Configuration (configured later in this guide). This may be useful to set if you wish to set all users to the same value.

Step 6. In the *Group Name* field, select the group that the user belongs to.

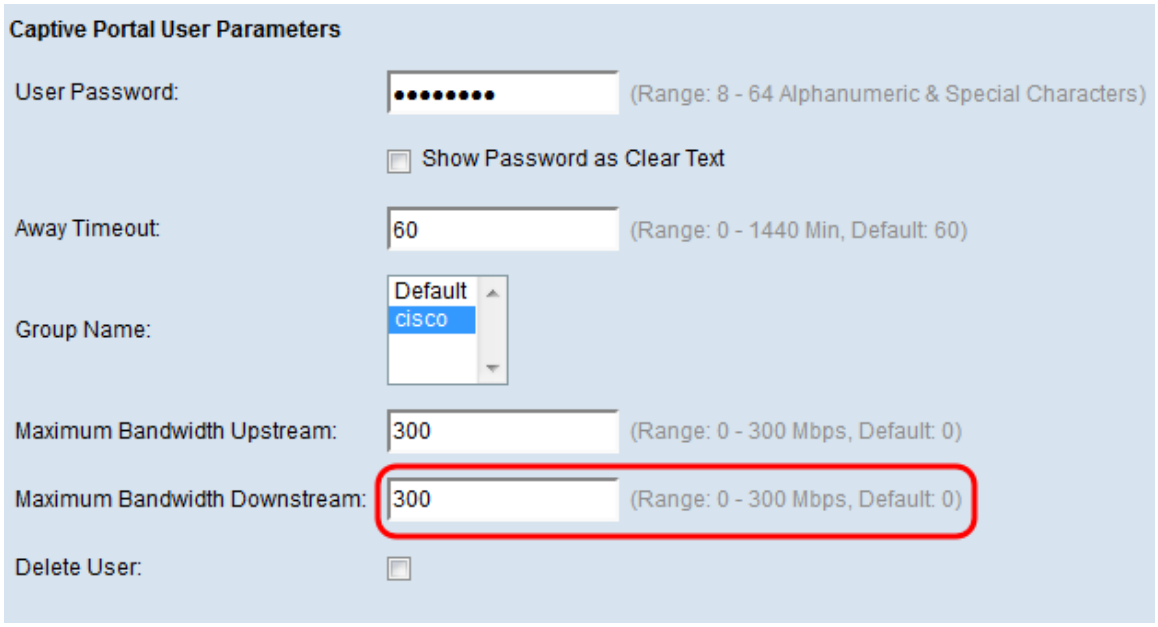


Step 7. In the *Maximum Bandwidth Upstream* field, enter the maximum upload speed in megabits that the client will be allowed to upload at. The default value is 0 and the maximum is 300.



Note: A value of 0 in this box will cause the device to use the value set in Captive Portal Instance Configuration (configured later in this guide). This may be useful to set if you wish to set all users to the same value.

Step 8. In the *Maximum Bandwidth Downstream* field, enter the maximum upload speed in megabits that the client should be allowed to upload at. The default value is 0 and the maximum is 300.



Note: A value of 0 in this box will cause the device to use the value set in Captive Portal Instance Configuration (configured later in this guide). This may be useful to set if you wish to set all users to the same value.

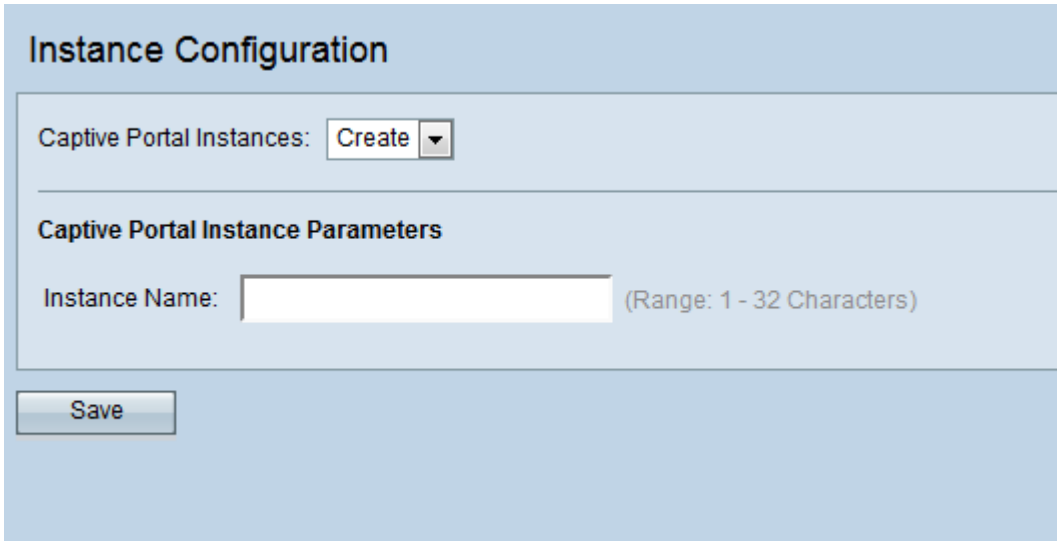
Step 9. Click **Save**.

Create a New Captive Portal Instance

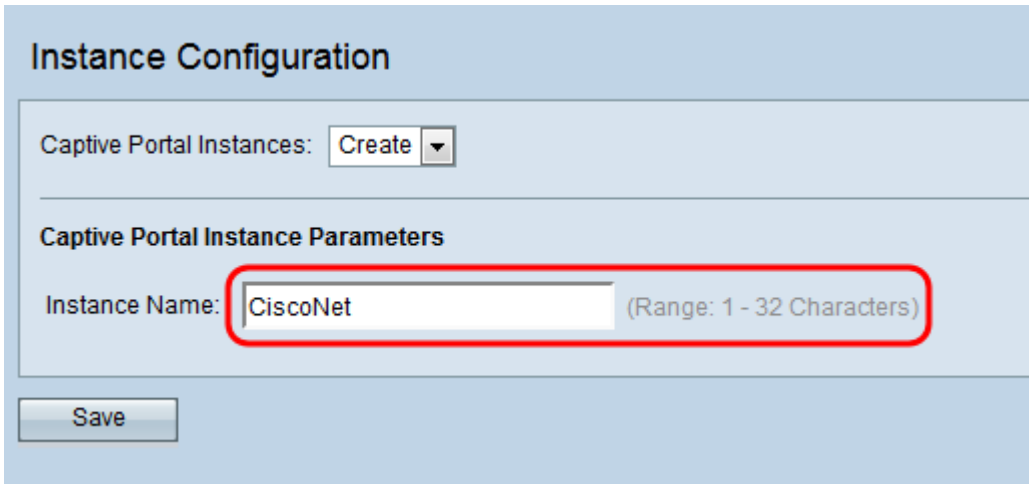
A Captive Portal Instance allows you to specify various configuration options associated with how users connect to the Captive Portal.

Step 1. Navigate to **Captive Portal > Instance Configuration**. The *Instance Configuration*

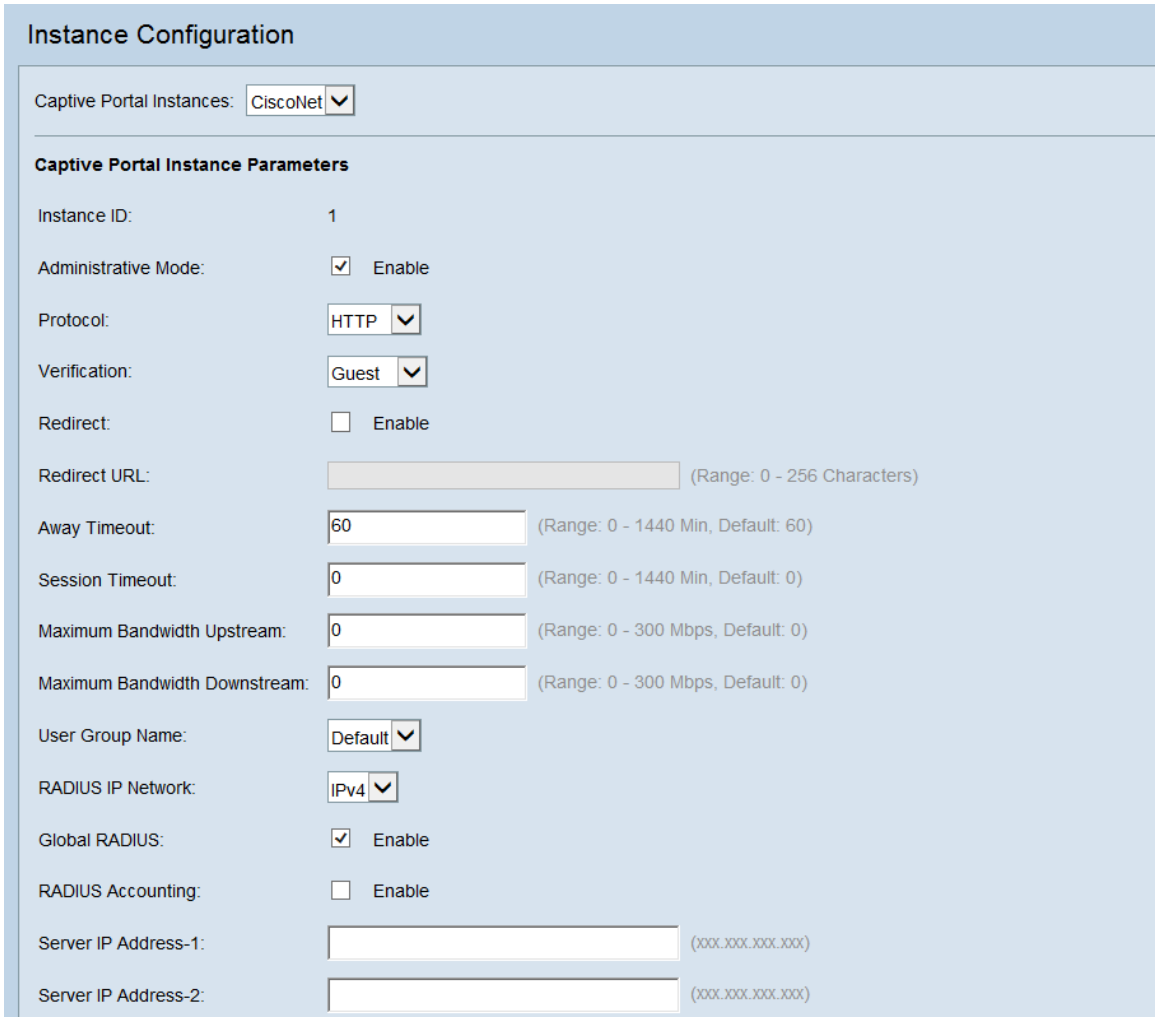
screen appears:



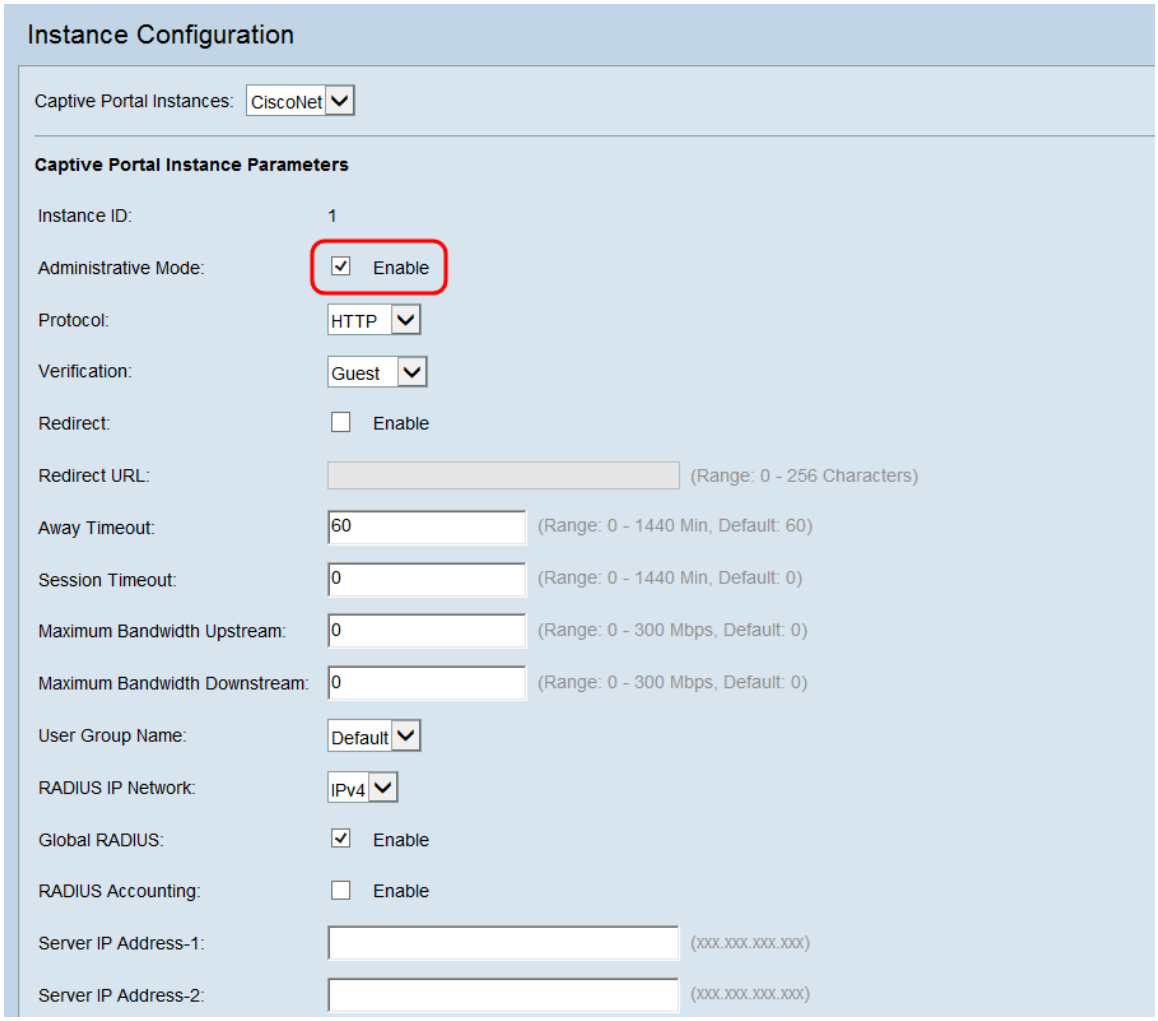
Step 2. Enter the desired name for the new Captive Portal Instance in the *Instance Name* field.



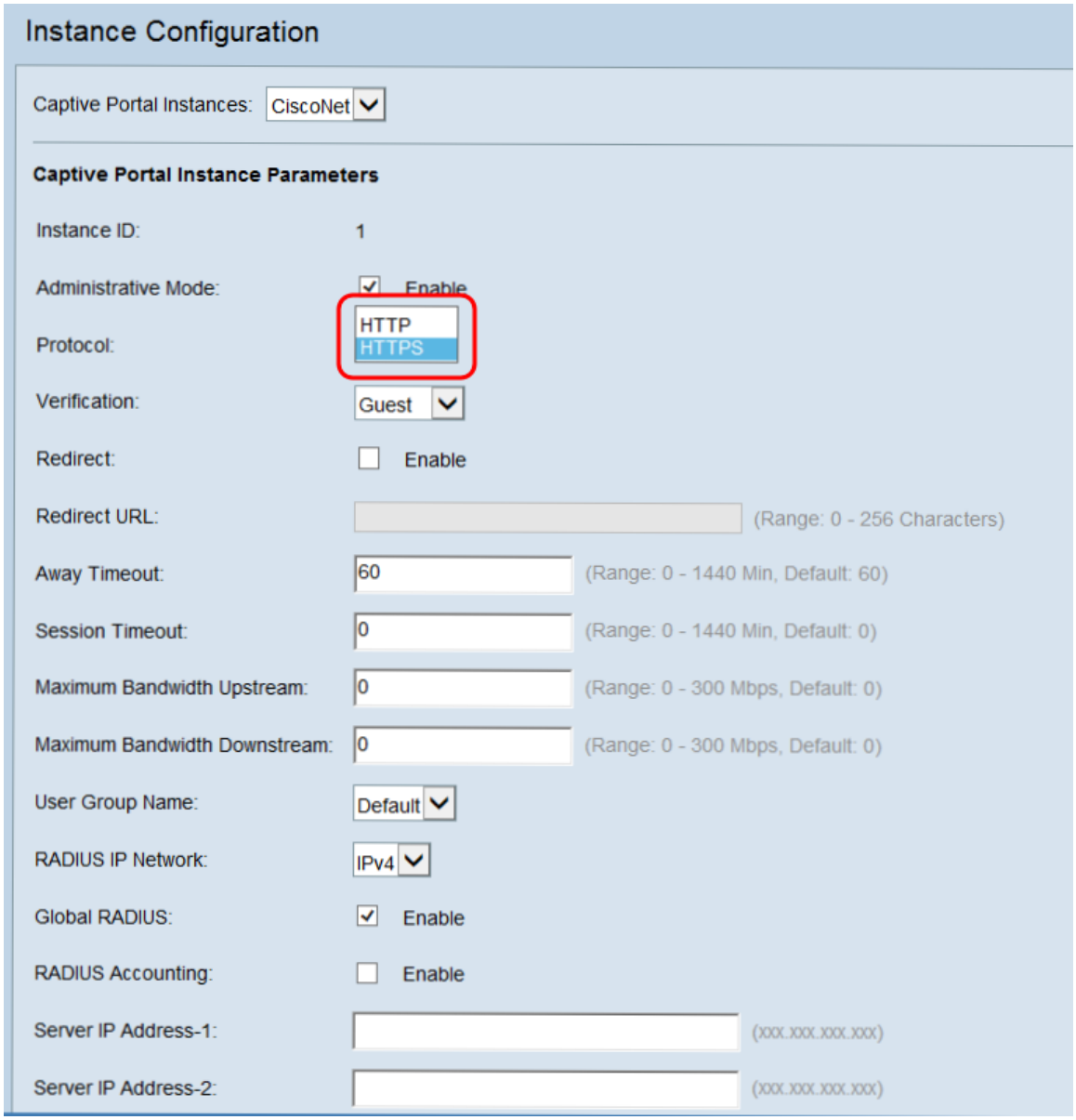
Step 3. Click **Save**. The *Captive Portal Instance Parameters* additional fields appear:



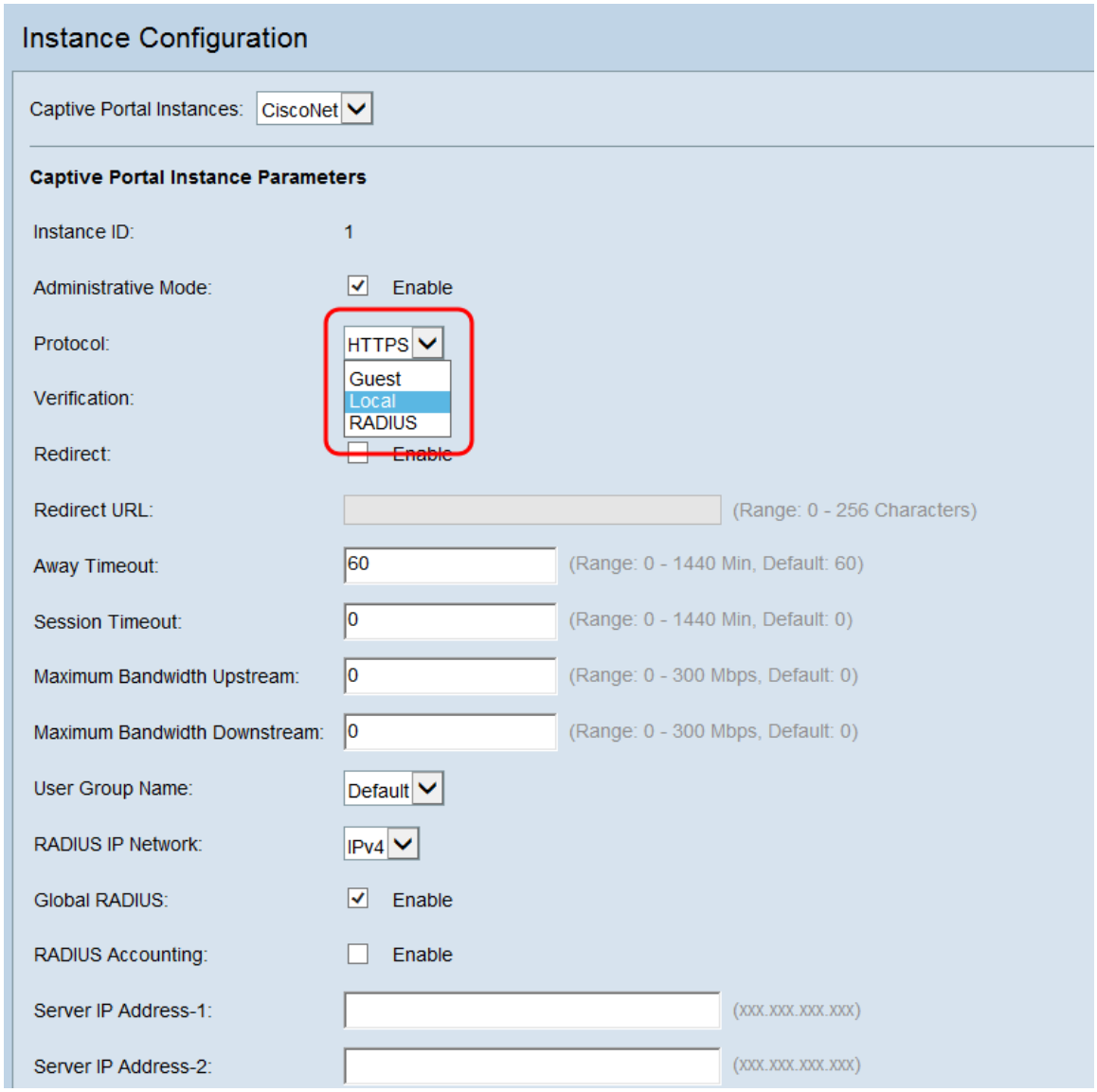
Step 4. Ensure that the *Administrative Mode* check box is selected to enable the Captive Portal instance.



Step 5. In the *Protocol* drop-down list, select the protocol you would like to use during the verification process. HTTP transmits information in plaintext, while HTTPS encrypts the data that is transmitted. HTTPS is recommended.



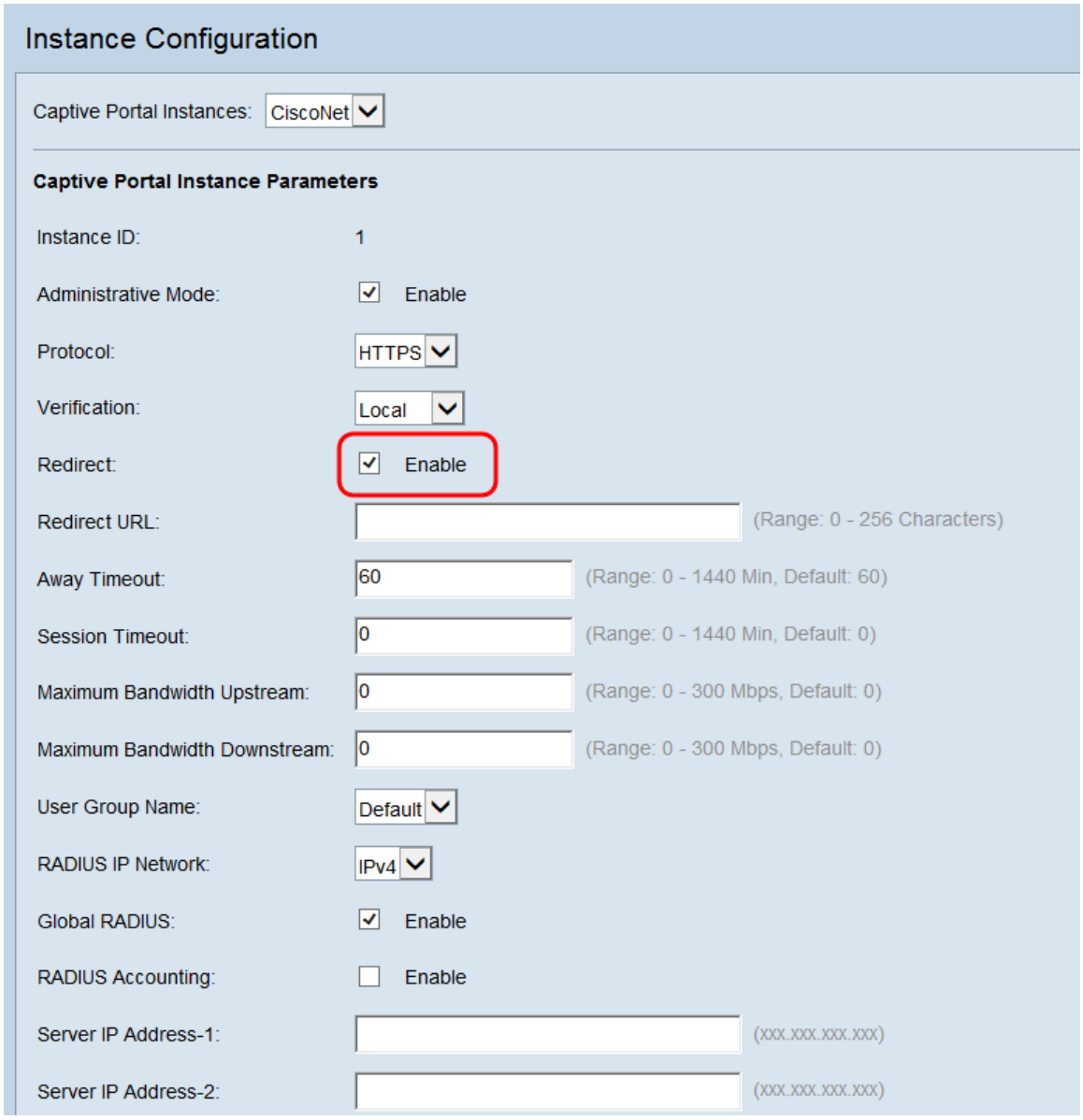
Step 6. In the *Verification* drop-down list, select the method of authentication that the Captive Portal will use.



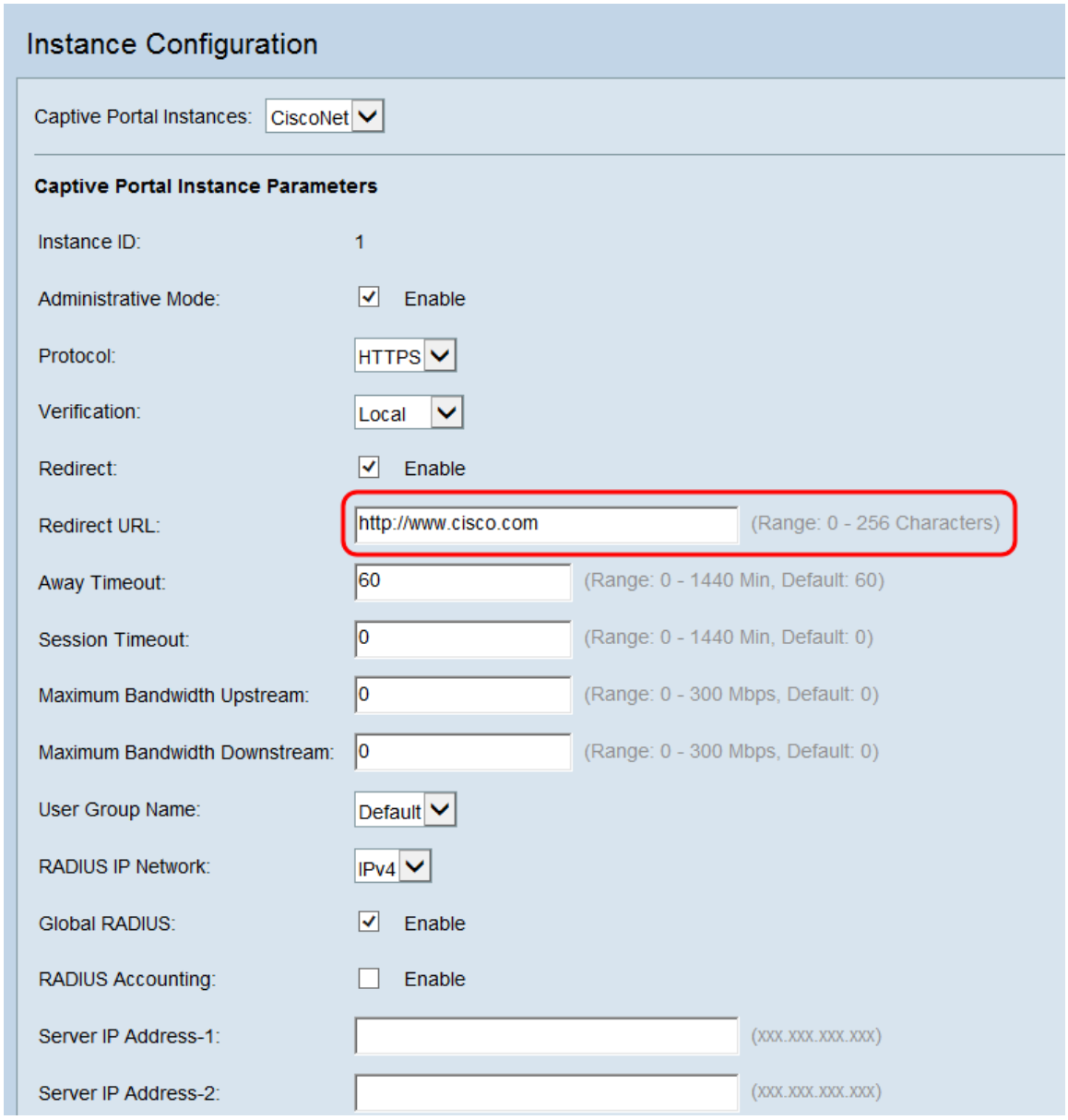
The available options are defined as follows:

- Guest — No database authentication is required. Users will not be required to specify an account when connecting.
- Local — Users will be required to provide a username and password. The user will be authenticated using a local database.
- RADIUS — Users will be required to provide a username and password. The user will be authenticated on a remote RADIUS server.

Step 7. If you would like to redirect clients to another URL once they are authenticated, check the *Redirect* check box. Skip to step 9 if you do not wish to enable redirection.

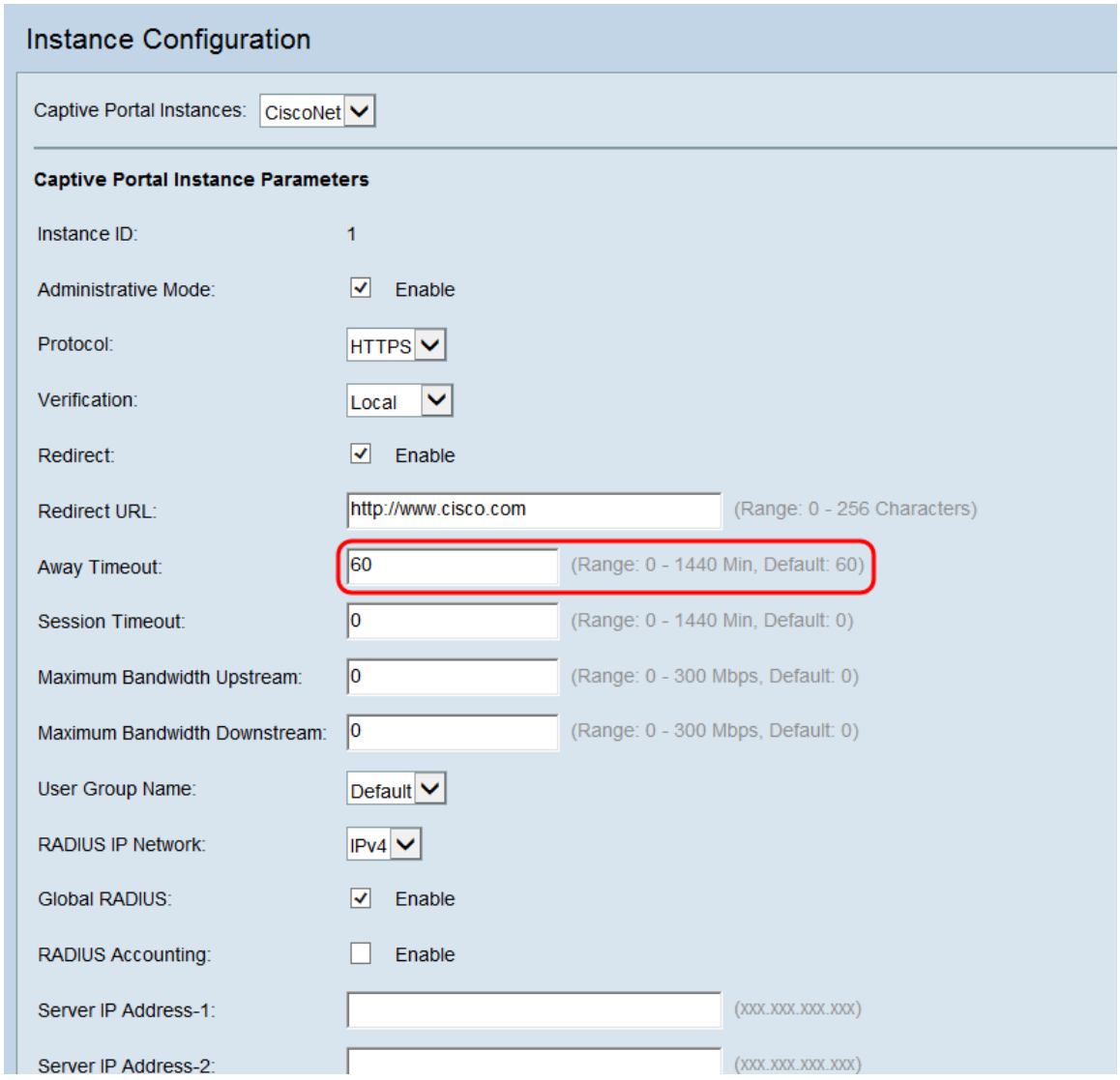


Step 8. In the *Redirect URL* field, enter the URL that you would like send clients to once they have been authenticated.



Step 9. In the *Away Timeout* field, enter the time in minutes that a user will remain authenticated to the WAP after they have disconnected. If a user reconnects before this time expires, they will not need to enter authentication information.

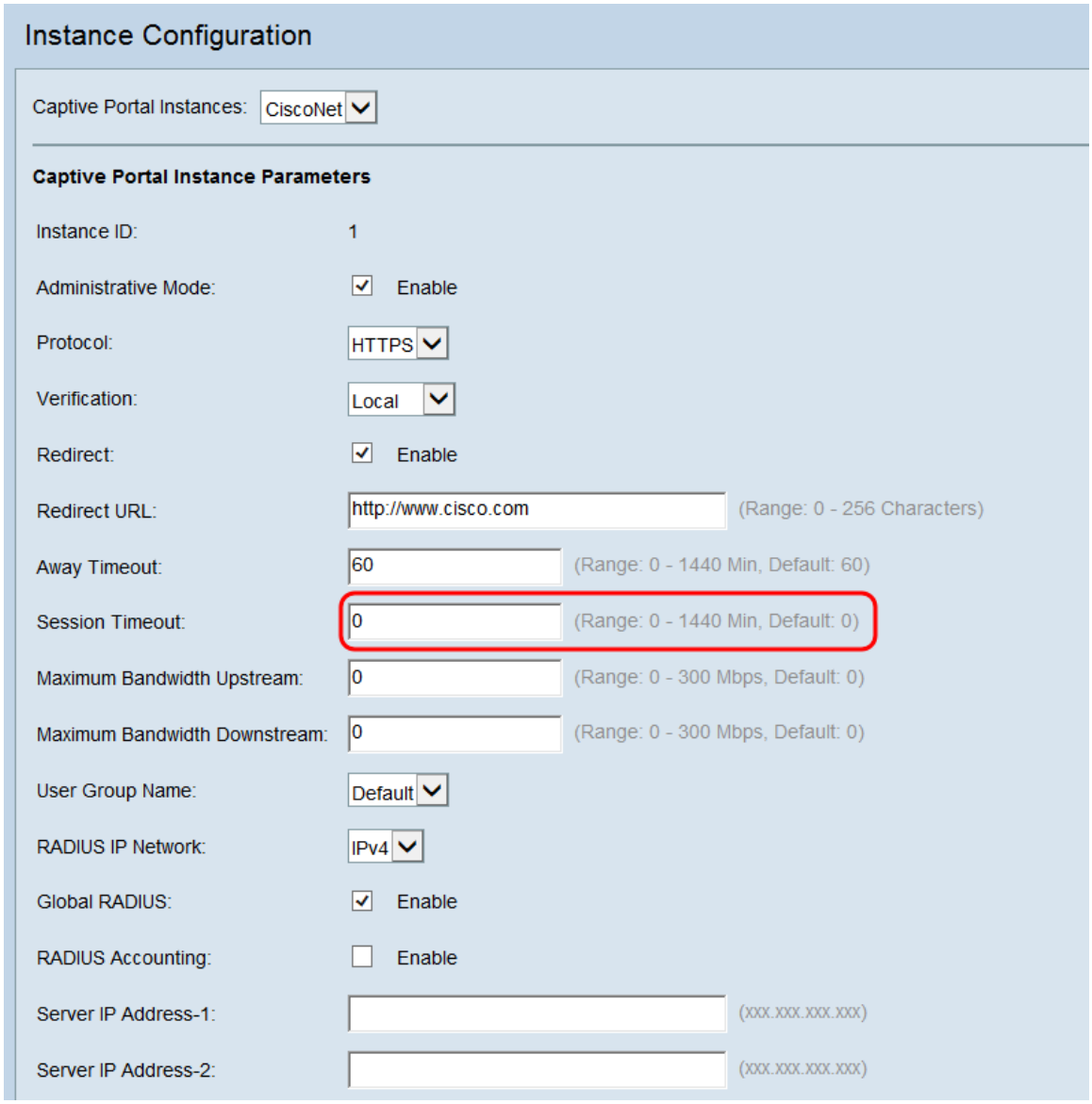
Note: Entering a value of 0 in this field will disable the timeout.



Note: If you have entered away timeouts for a Local User, then the timeouts set for the Local User will take precedence over what is set for the Captive Portal instance.

Step 10. In the *Session Timeout* field, enter the time in minutes until the WAP will force a user to log off, even if they are still connected. The default value is 0.

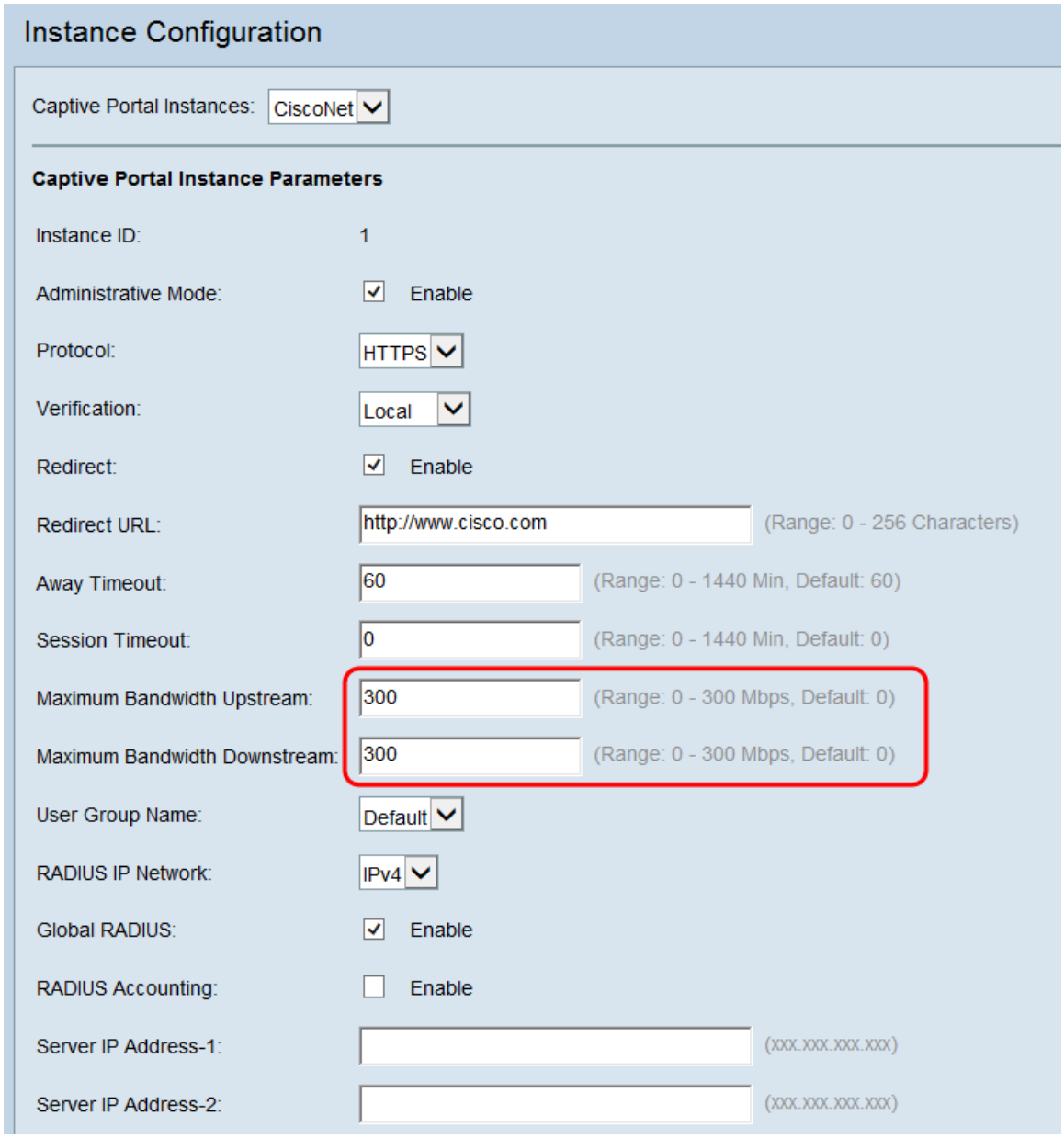
Note: Entering a value of 0 in this field will disable the timeout.



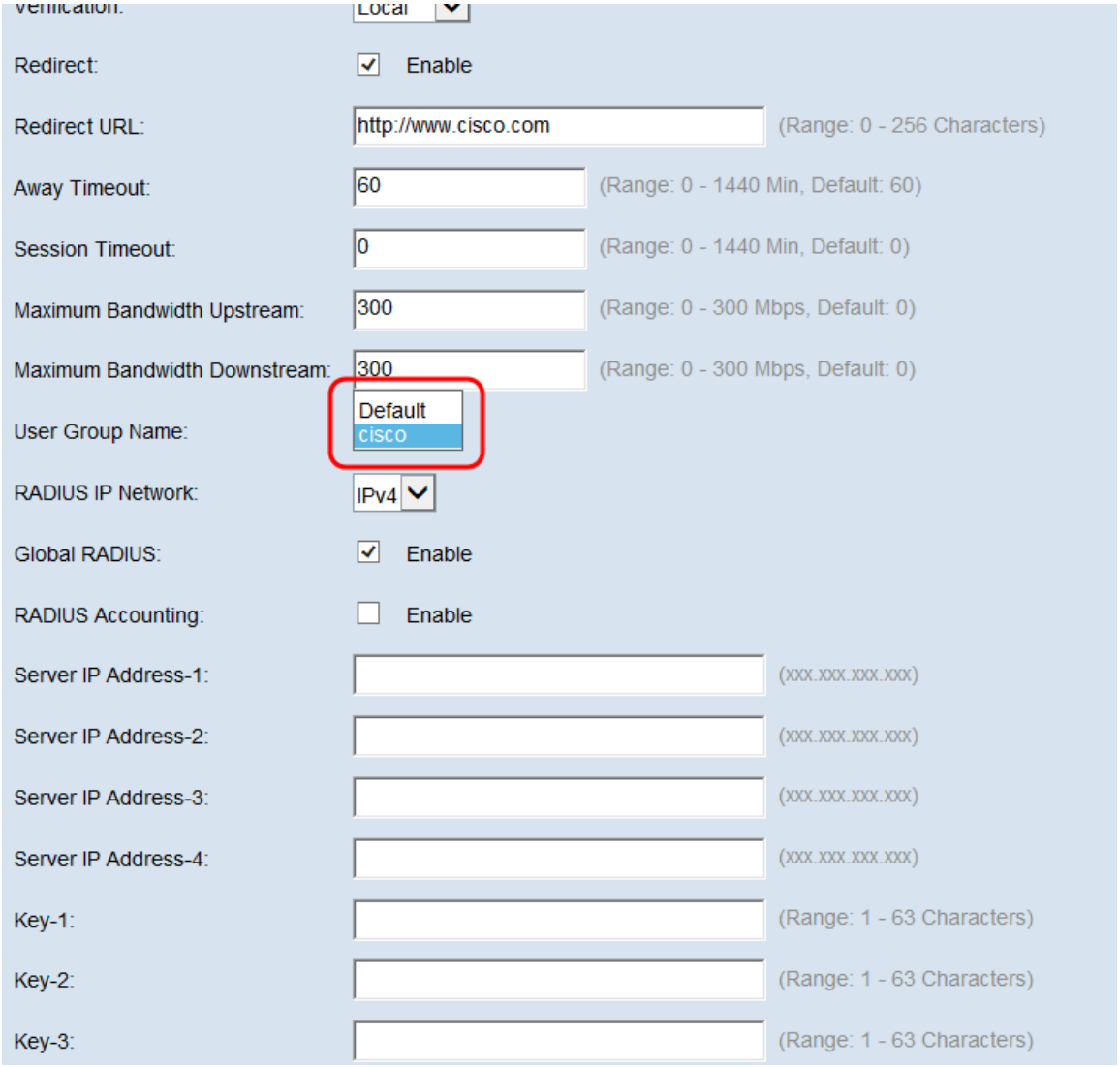
Step 11. In the *Maximum Bandwidth Upstream* and *Maximum Bandwidth Downstream* fields, enter the maximum bandwidth in Mbps that users should be allowed to transmit data at over the wireless network. The default value is 0.

Note: Entering a value of 0 in this field specifies that the bandwidth should not be limited.

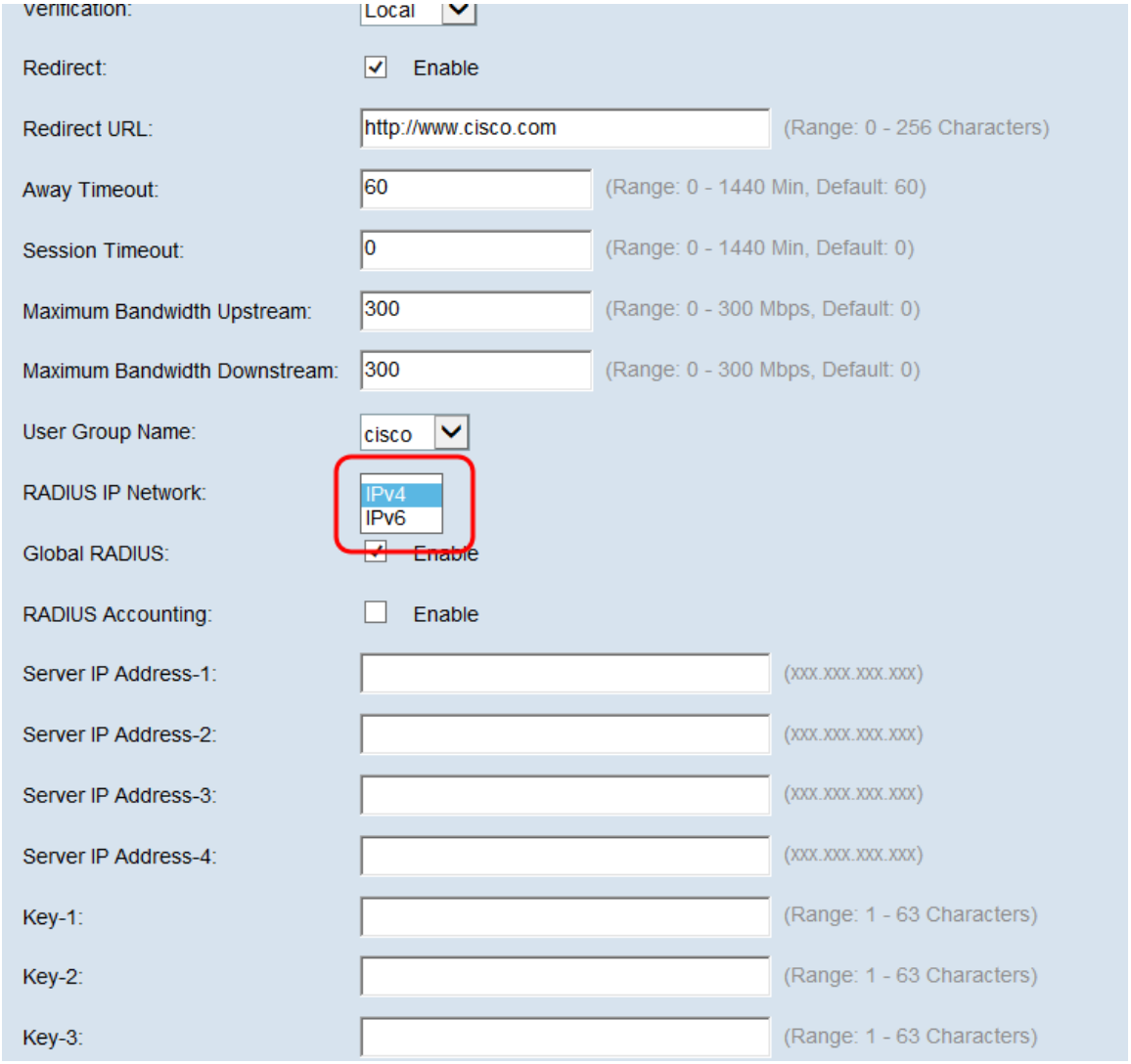
Note: If you have entered maximum bandwidth values for a Local User, then the maximum bandwidth values set for the Local User will take precedence over what is set for the Captive Portal instance.



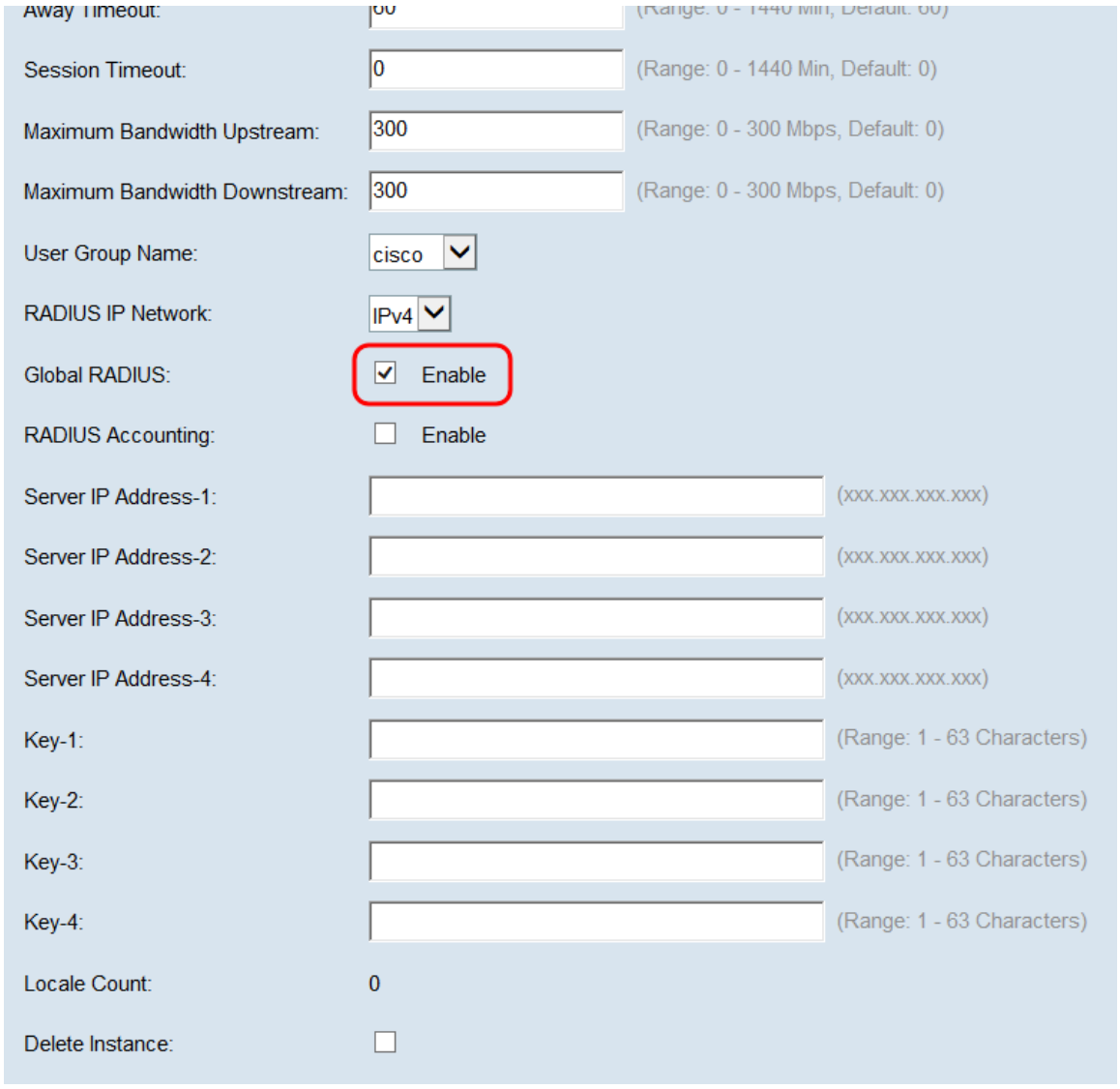
Step 12. In the *User Group Name* drop-down list, select the user group that you would like to associate the Captive Portal instance with. If you have selected guest verification in Step 6, you may skip this step.



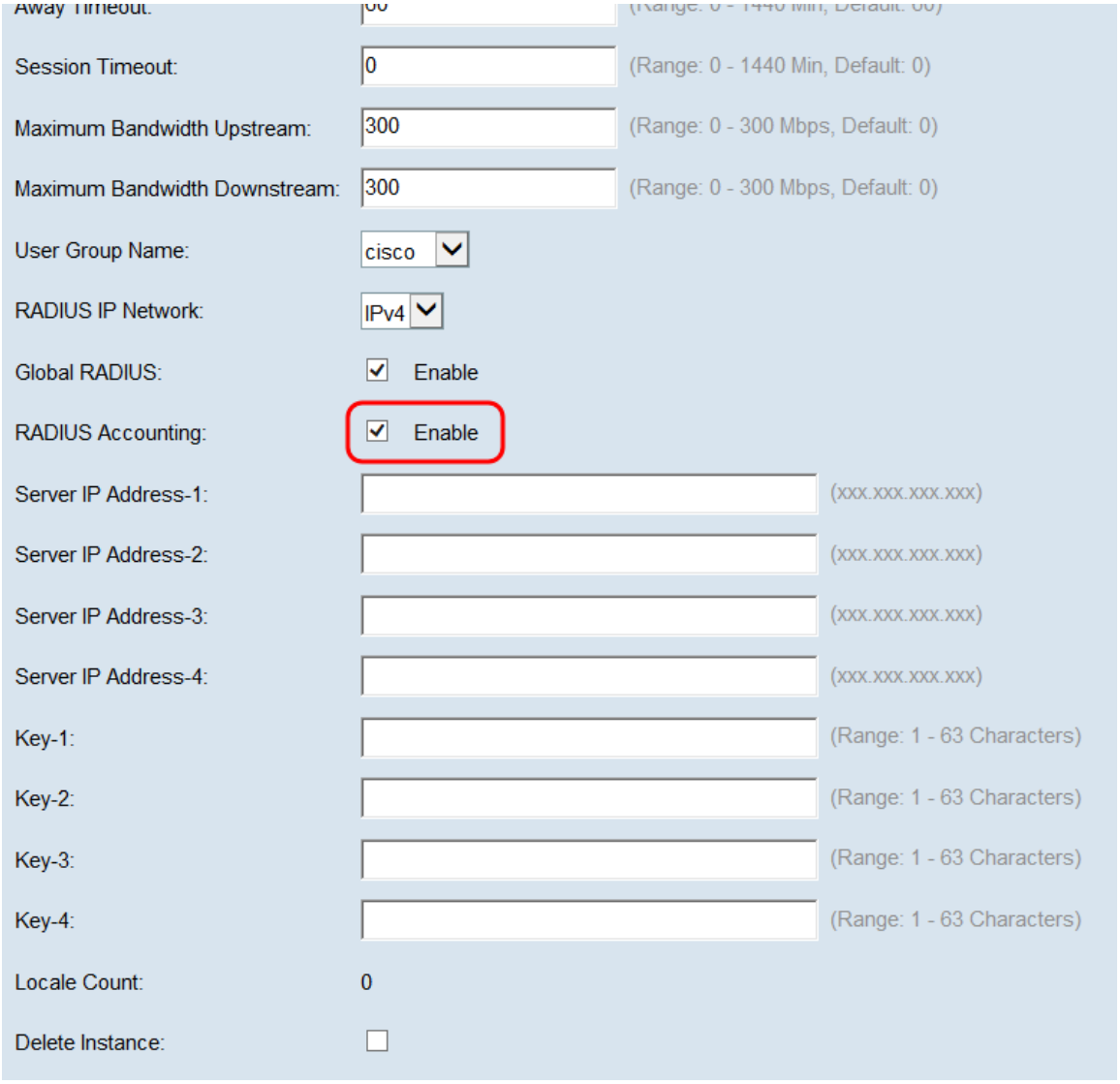
Step 13. Select from the *RADIUS IP Network* drop-down box the IP version your RADIUS server uses. If you do not use a RADIUS server for authentication, skip ahead to Step 17.



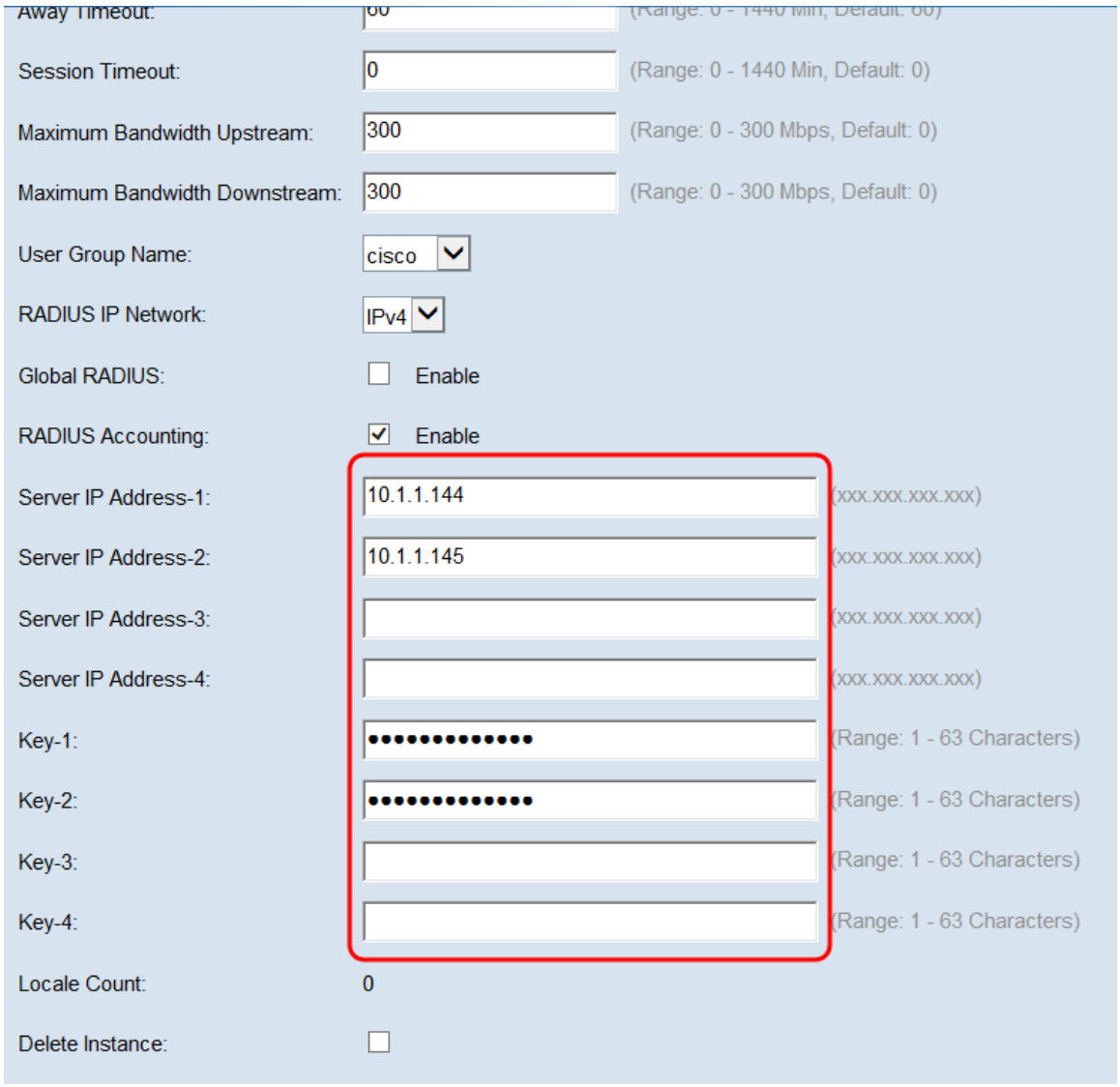
Step 14. If you have configured global RADIUS on your device, you can check the *Global RADIUS* check box to authenticate using the globally defined RADIUS server. For more information refer to *Configuring a Globally Defined RADIUS Server on the WAP131 and WAP351* and *Configuring RADIUS Server Settings on the WAP371*.



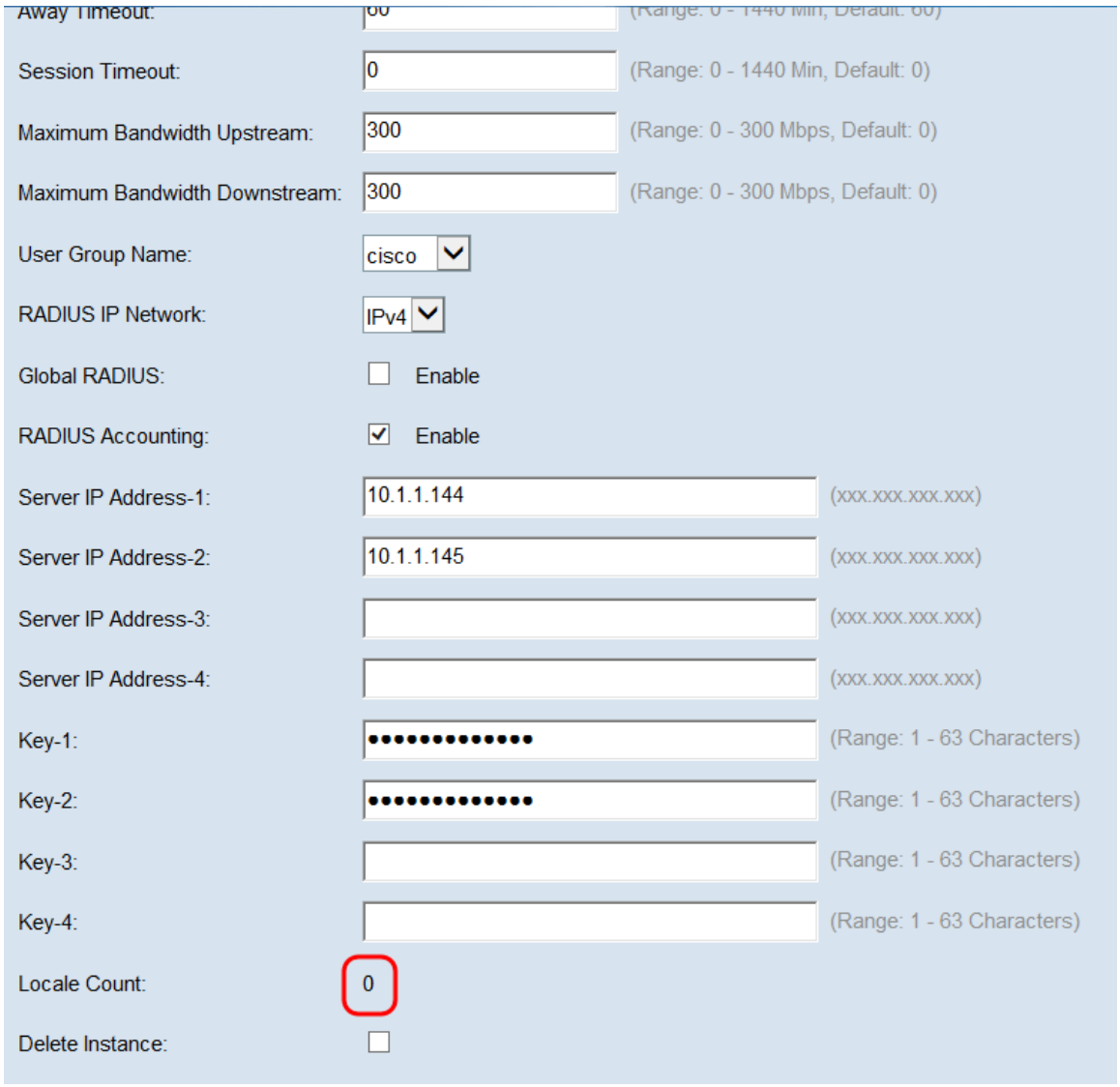
Step 15. If you would like your RADIUS server to collect data on user network usage, check the *RADIUS Accounting* check box.



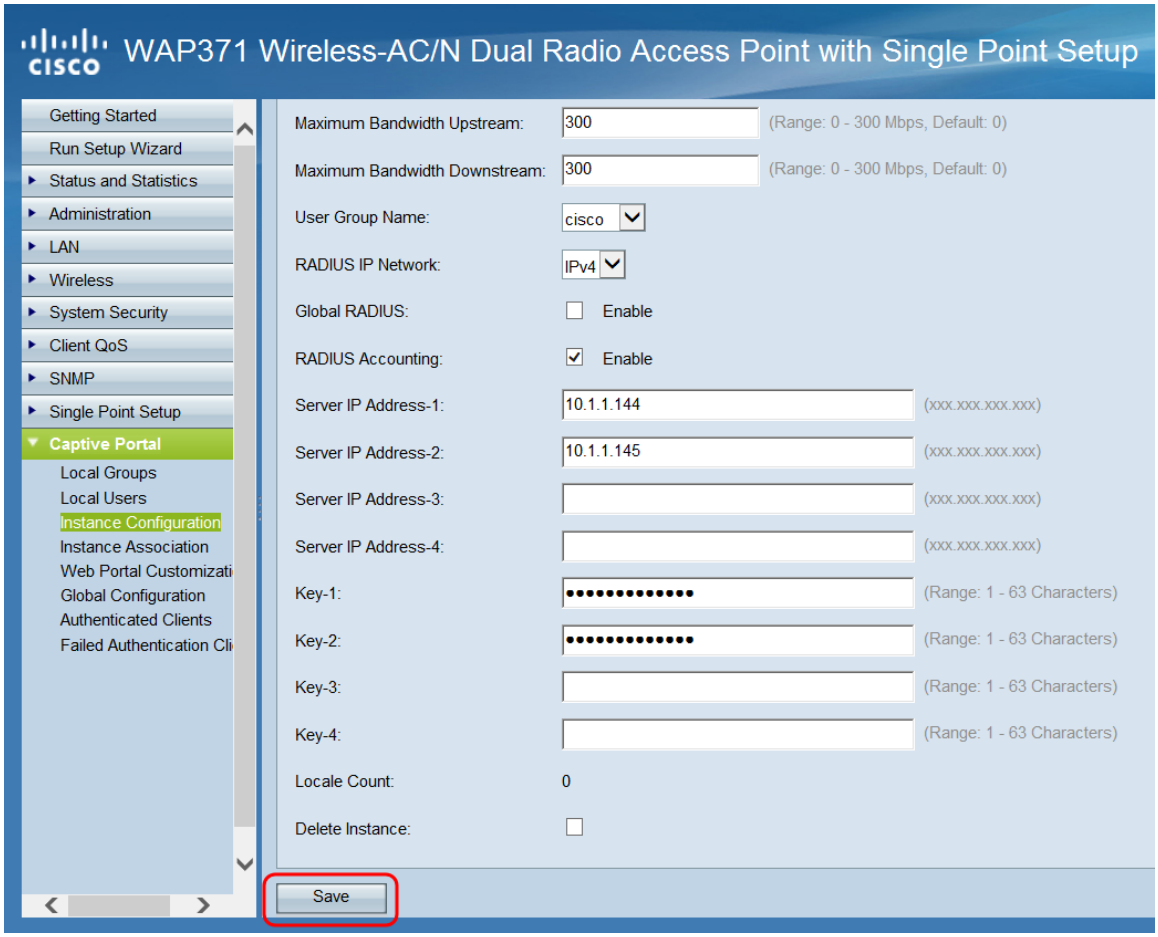
Step 16. If you have not enabled Global RADIUS in Step 14, enter the IPs and keys for the RADIUS servers you would like to associate with this specific Captive Portal instance. *Key-1* is associated with *Server IP Address-1*, *Key-2* is associated with *Server IP Address-2*, and so on.



Note: The *Locale Count* field displays the number of locales that are configured for this Captive Portal instance. A default locale will be configured later in this article. More advanced information on configuring locales can be found in *Configuring Locales on the WAP351 and WAP371 Access Points*.



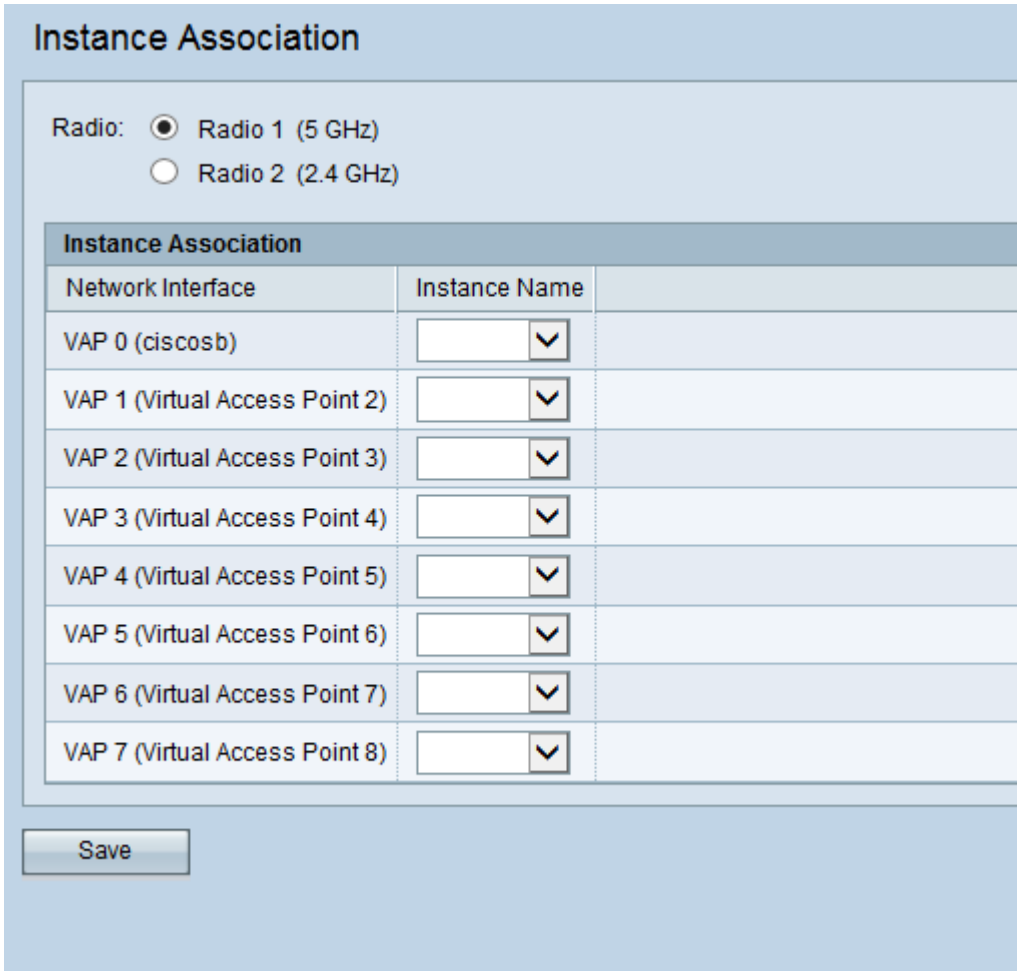
Step 17. Click **Save**.



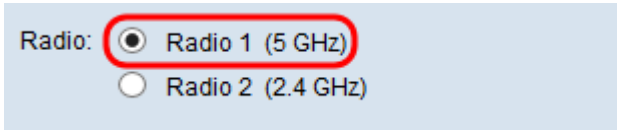
Associating a Captive Portal Instance with an SSID

Once created, a Captive Portal Instance must be assigned with a VAP in order to allow clients to connect to it.

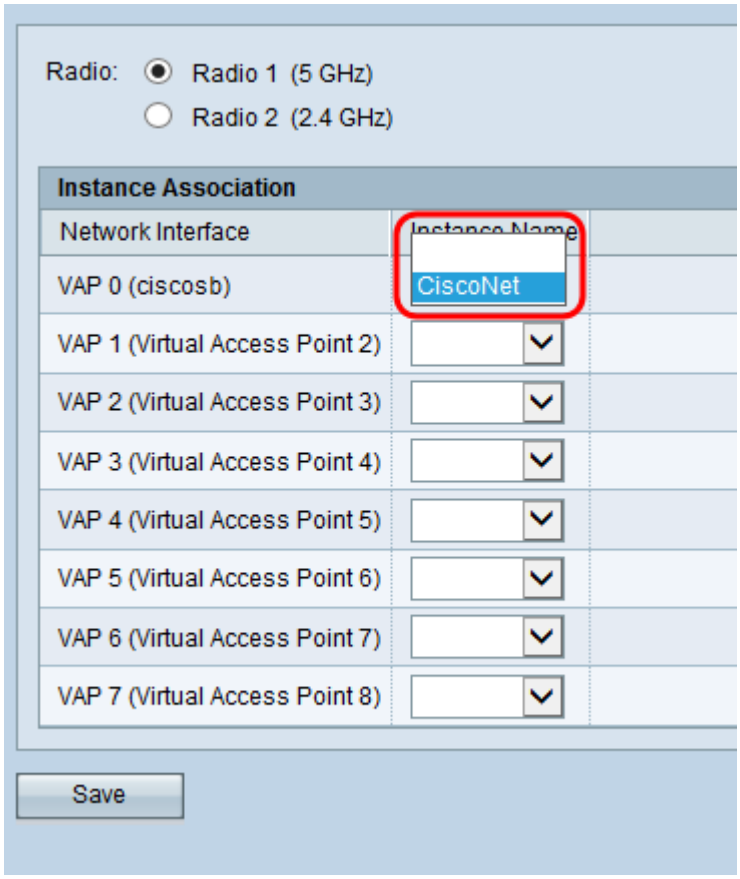
Step 1. Navigate to **Captive Portal > Instance Association**. The *Instance Association* screen appears:



Step 2. In the *Radio* field, select the radio button corresponding with the radio band that you wish to use. 5GHz provides a higher bandwidth over a shorter range, and may be incompatible with older wireless clients. 2.4 GHz provides a lower bandwidth, but larger range and compatibility.



Step 3. Under the *Instance Name* column, select the drop-down box corresponding with the VAP that you wish to use the Captive Portal on.

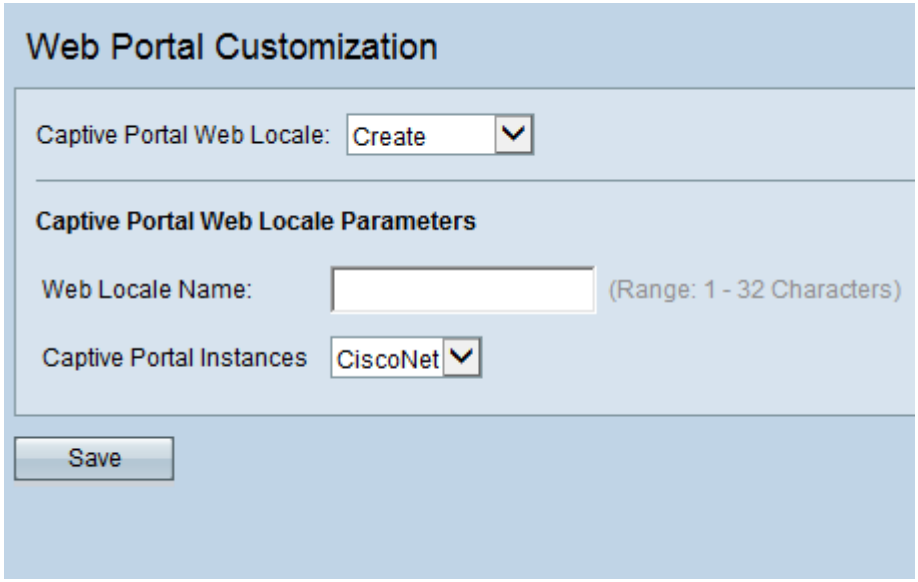


Step 4. Click **Save**.

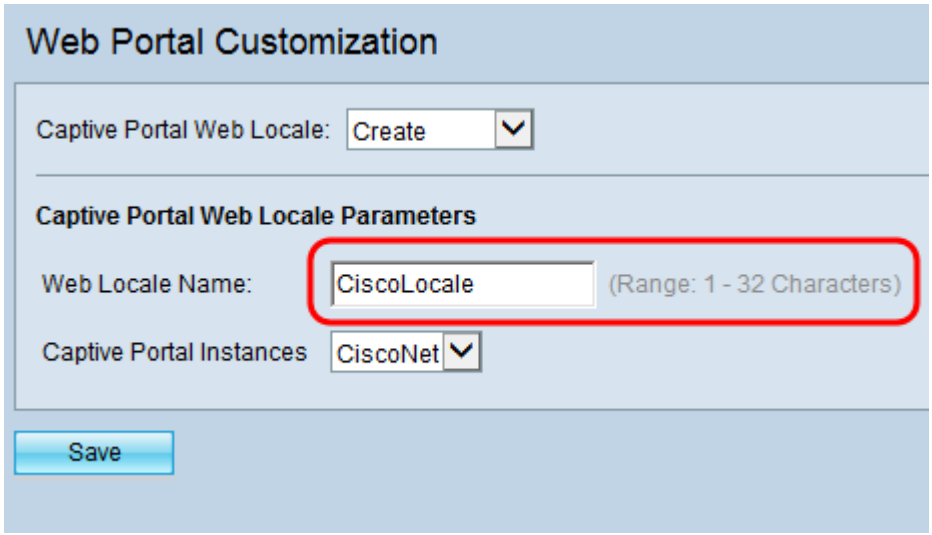
Create a New Captive Portal Locale

A locale allows you to modify what is displayed to the user when they are prompted for a login. You can have up to 3 locales configured to each Captive Portal Instance.

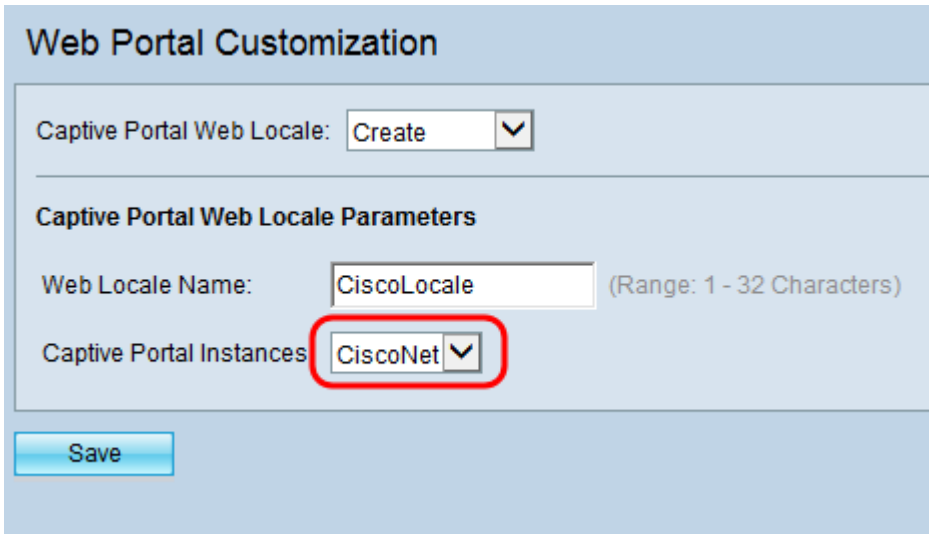
Step 1. Navigate to **Captive Portal > Web Portal Customization**. The *Web Portal Customization* page appears:



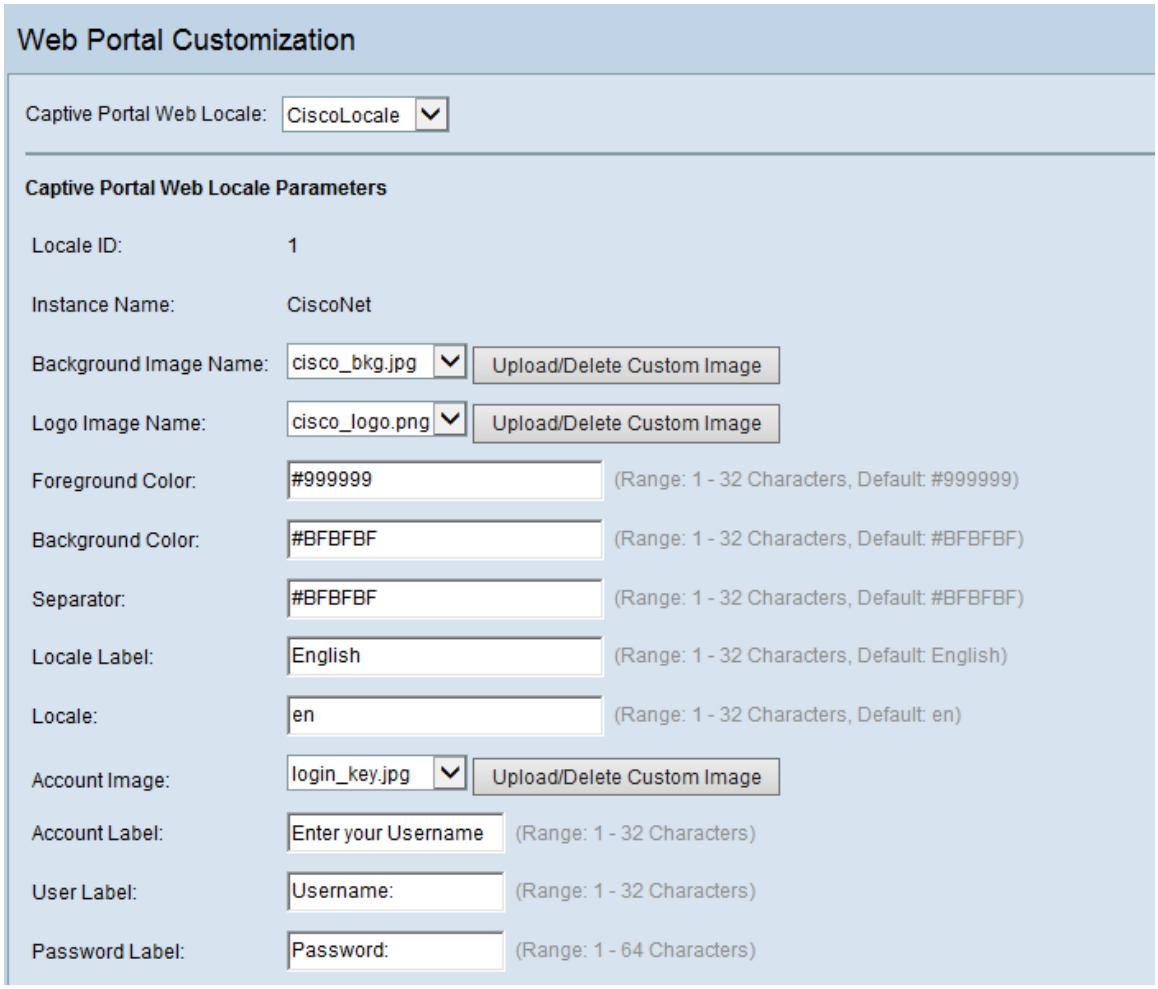
Step 2. Enter a name for the locale in the *Web Locale Name* field.



Step 3. Select the appropriate Captive Portal Instance that you would like to associate the locale with from the *Captive Portal Instances* drop-down box.



Step 4. Click **Save**. Additional parameters appear allowing the login page to be modified. For additional information on modifying locales, see *Configuring Locales on the WAP351 and WAP371 Access Points*.

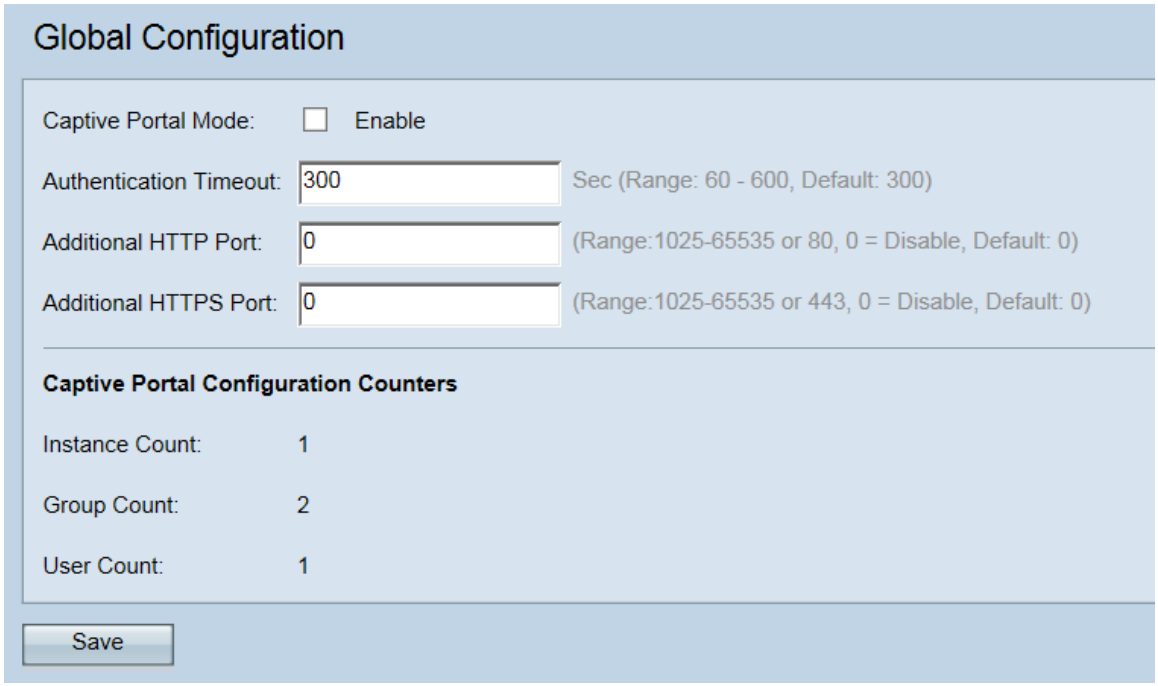


Step 5. When finished modifying the locale, press **Save**.

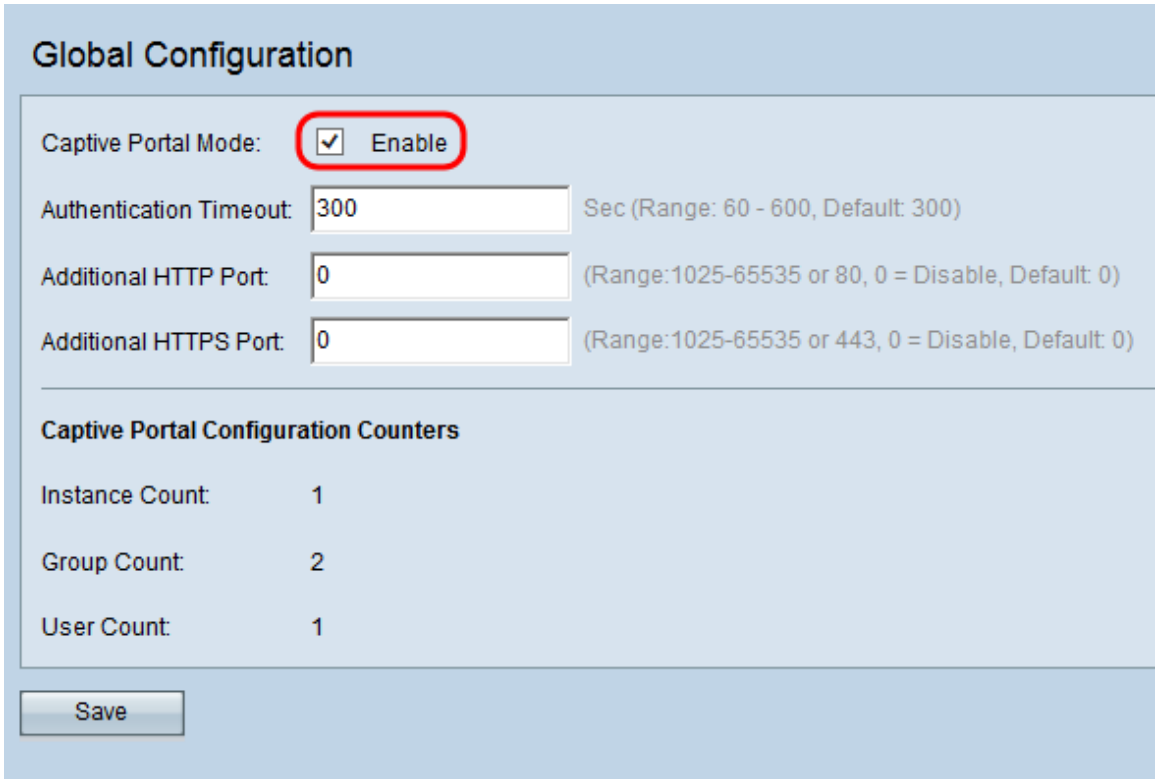
Enabling Captive Portal

Once configured, the Captive Portal mode must be enabled.

Step 1. Navigate to **Captive Portal > Global Configuration**. The *Global Configuration* screen appears:



Step 2. In the *Captive Portal Mode* field, select the **Enable** checkbox to activate the Captive Portal.



Step 3. Click **Save** to finalize your changes.

View a video related to this article...

[Click here to view other Tech Talks from Cisco]