Captive Portal Instance Configuration on WAP321 Access Point

Objective

The captive portal allows you to block clients connected to the WAP network. Clients see a special web page for authentication purposes before they are allowed to use the Internet normally. Captive Portal verification is for both guests and authenticated users, and makes use of the web browser by turning it into an authentication device. Captive portal instances are a defined set of configurations that are used to authenticate clients on the WAP network. Different instances (maximum up to two) can be configured to respond differently to users as they attempt to access the associated virtual access point. Captive portals are used at many Wi-Fi hotspots to charge users to get access to the Internet.

This document explains how to configure captive portal global configuration on the WAP321 access point.

Applicable Devices

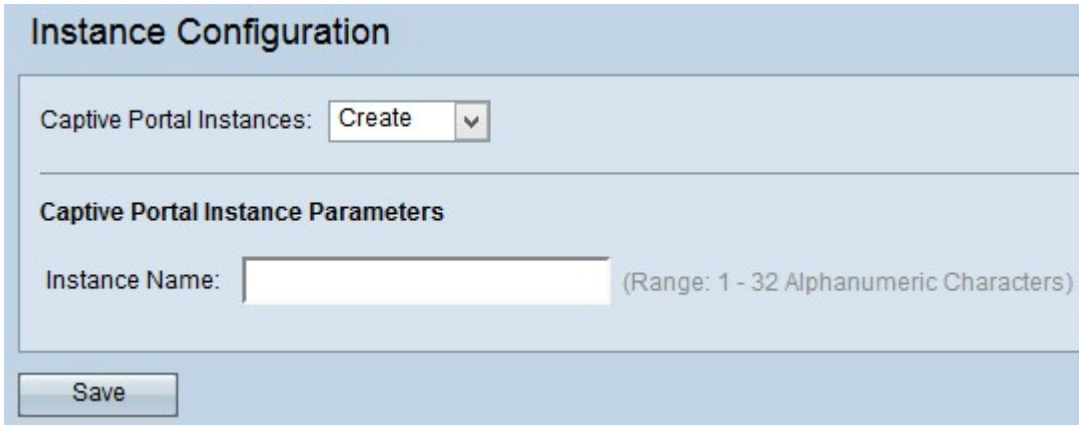
- WAP321

Software Version

- 1.0.3.4

Captive Portal 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 if you want to create a new configuration. To edit the current configuration, choose the current instance from the drop-down list and skip to Step 5.

Note: You can create up to a maximum of two configurations.

Step 3. Enter a name for the configuration in the Instance Name field. The range is 1 to 32 alphanumeric characters.

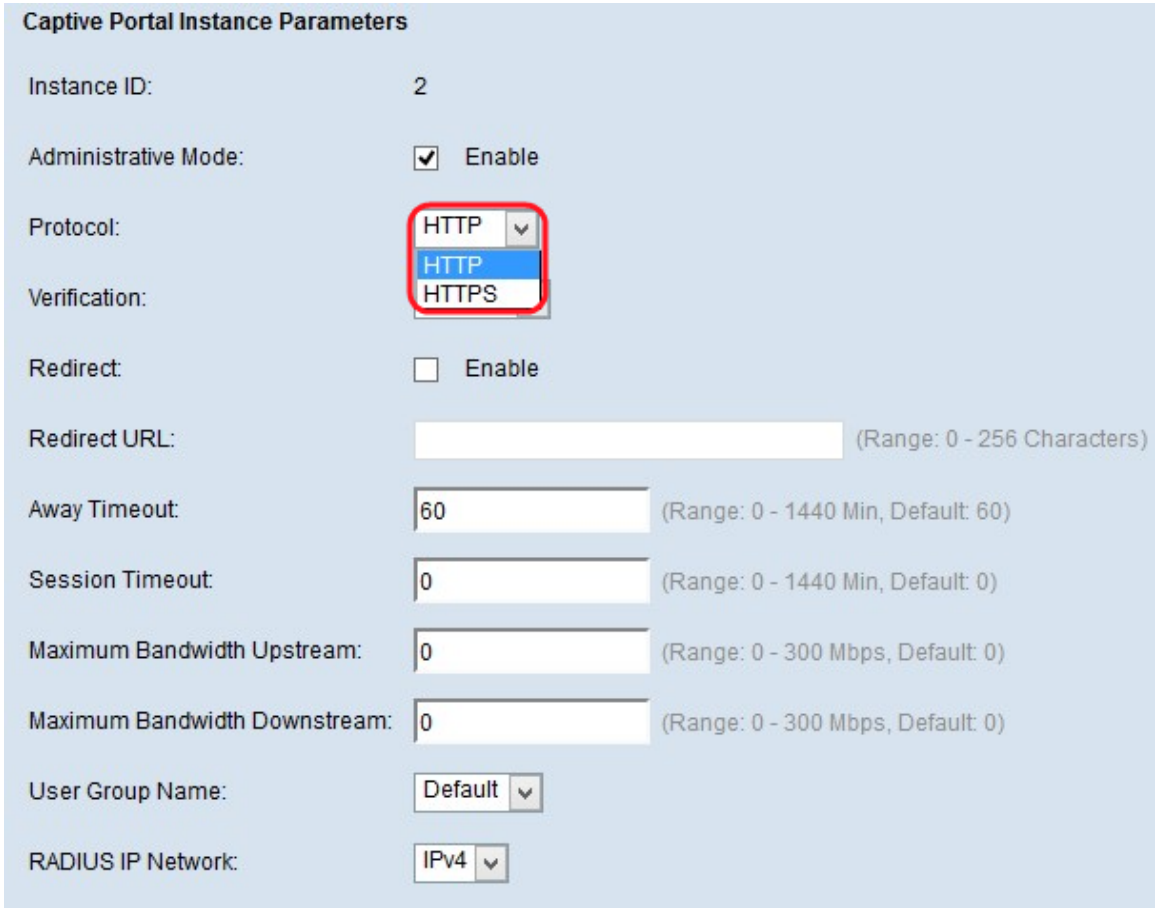
Step 4. Click **Save** to save the changes made. The page re-displays with additional fields for instance configuration.

The *Instance Configuration* page has some non-configurable fields which displays the following information:

- Instance ID — Specifies the rank number of CP instance currently configured on the WAP device.
- Locale Count — Specifies the number of locales (set of language and country specific

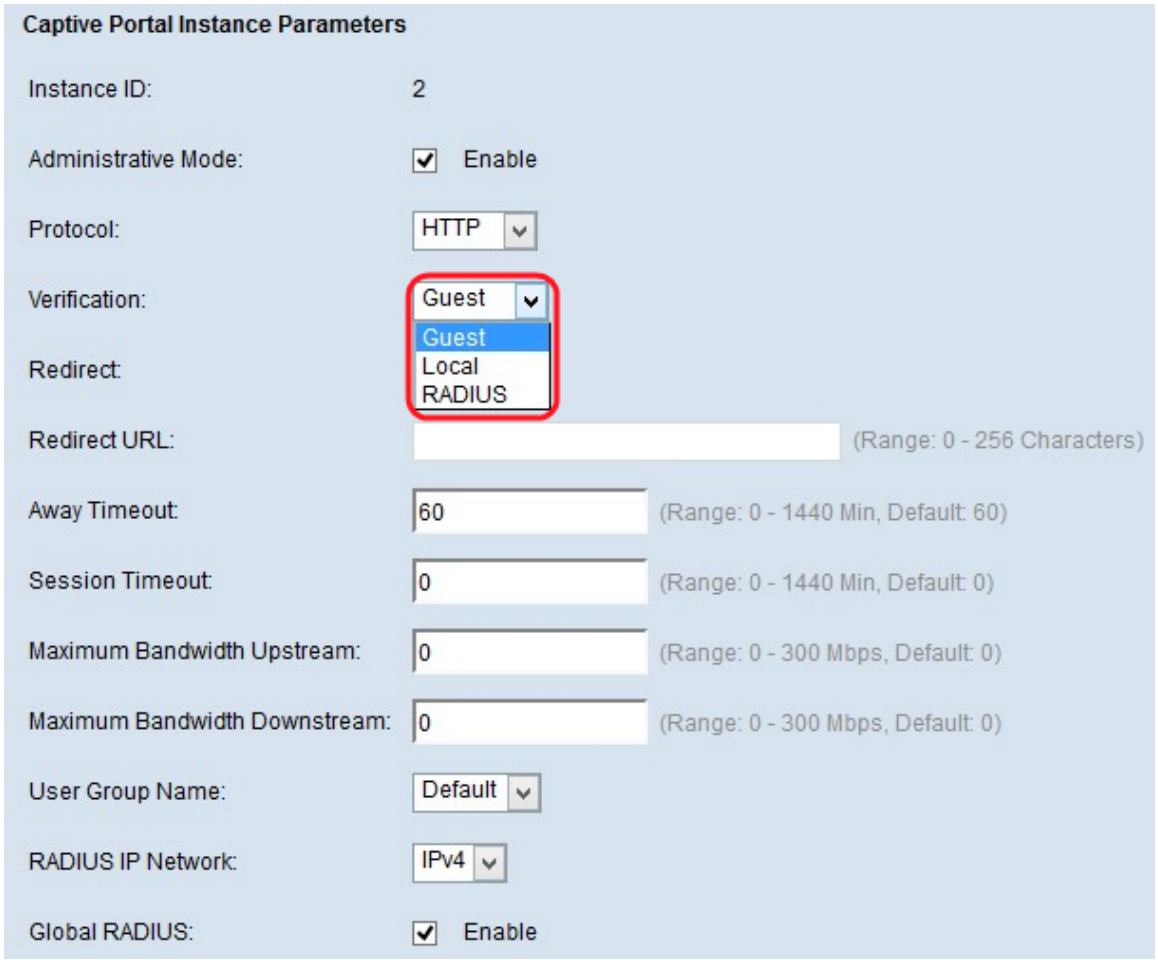
parameters of user preferences) associated with the instance.

Step 5. Check the **Enable** check box to enable the CP instance in the Administrative Mode field.



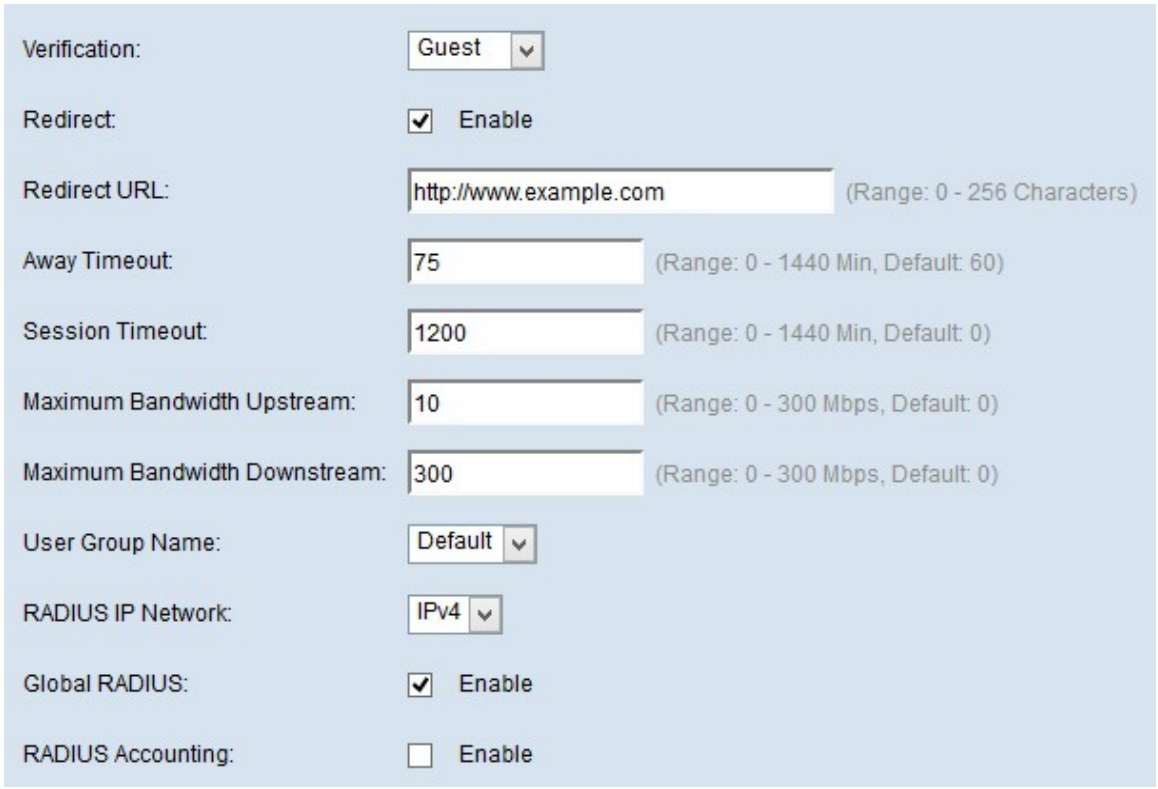
Step 6. Choose the protocol which you want the CP instance to use for verification at the Protocol field. The possible values are:

- HTTP — Does not encrypt information for the verification process.
- HTTPS — Uses the Secure Sockets Layer (SSL), which requires a certificate to provide encryption used in the authentication process.



Step 7. Choose the authentication method for the CP to use for verification from the Verification drop-down list. Authentication methods are used to deny malicious users access to the device. The chosen authentication method is used to verify the clients. The possible values are:

- Guest — Does not use any authentication.
- Local — Uses a local database for authentication.
- RADIUS — Uses a remote RADIUS server database for authentication.



Step 8. Check the **Enable** check box in the Redirect field if you want to redirect the newly authenticated client to a configured URL.

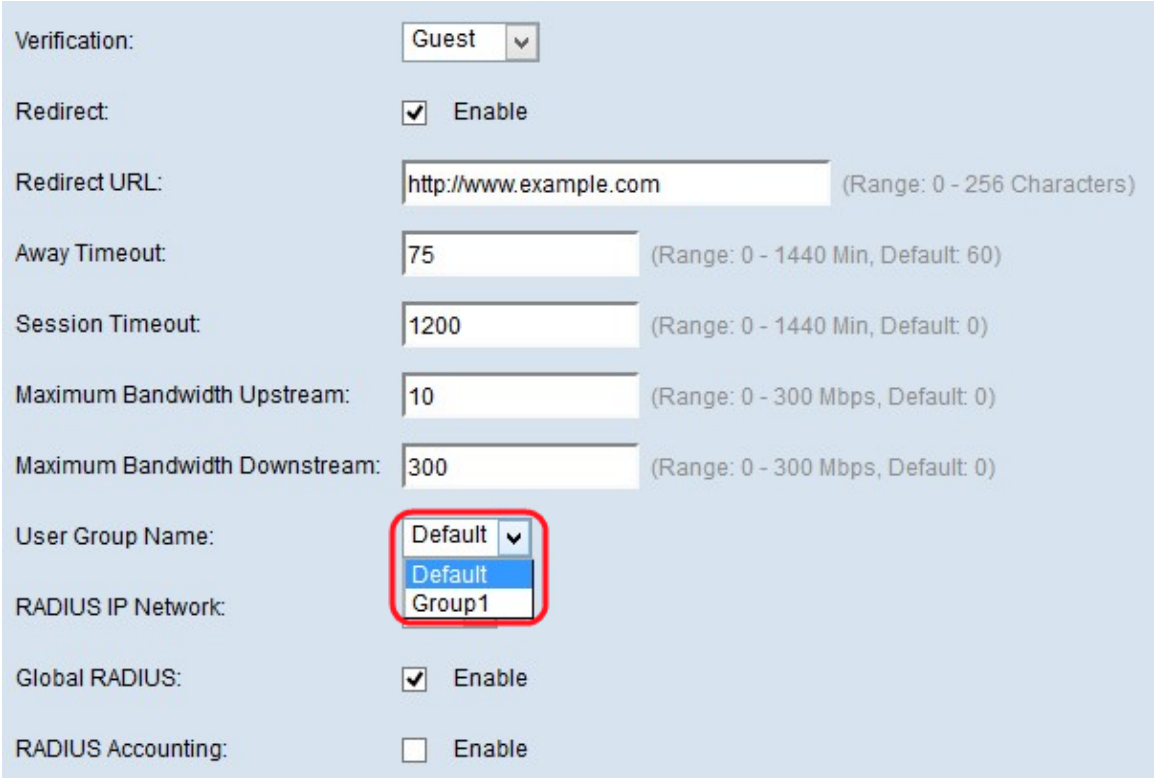
Step 9. Enter the URL with the prefix "http://" to which the newly authenticated client will be redirected in the Redirect URL field. The range is from 0 to 256 characters.

Step 10. Enter the amount of time a user can remain idle before automatically being logged out at the Away Timeout field. If the value is set to 0, the timeout is not enforced. The range is from 0 to 1440 minutes. The default value is 60 minutes.

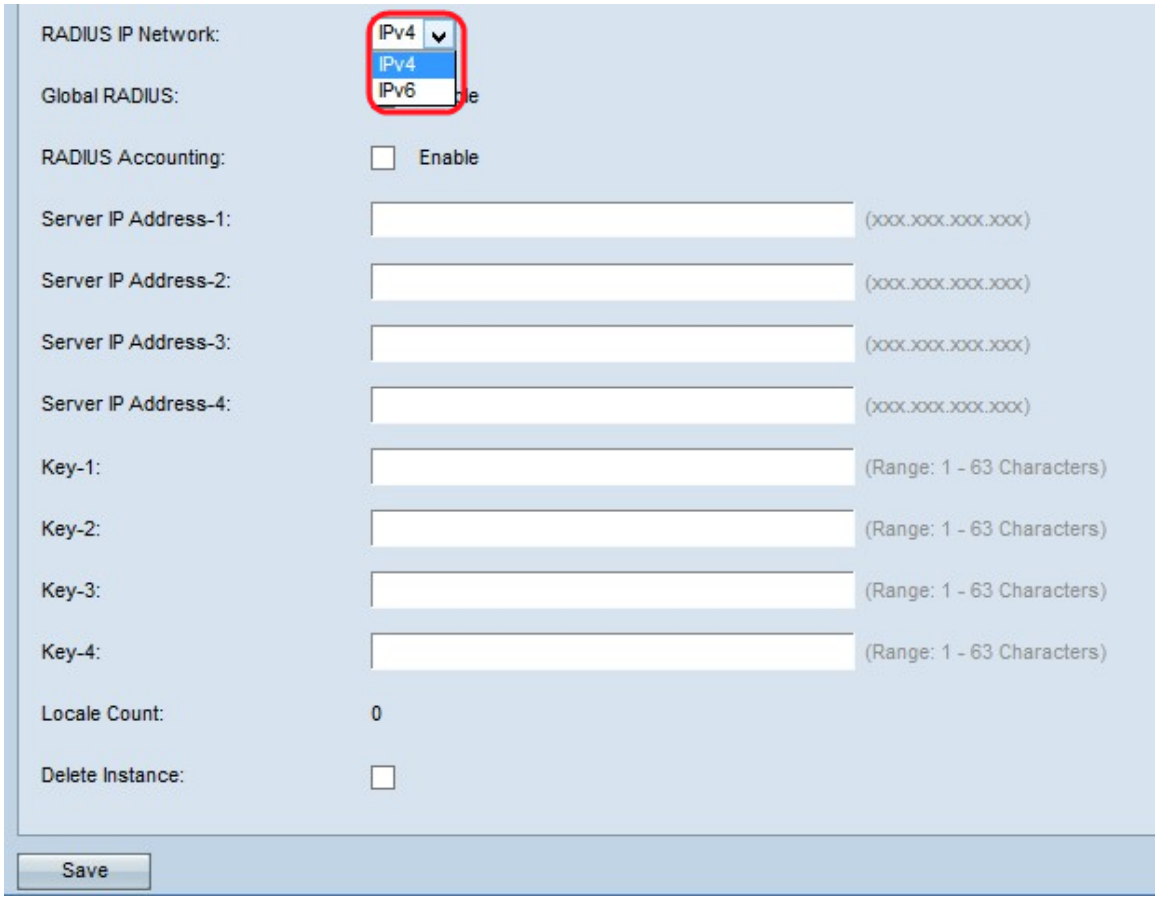
Step 11. Enter the amount of time to wait before the session terminates in the Session Timeout field. The range is from 0 to 1440 minutes. The default value is 0, which means timeout is not enforced.

Step 12. Enter the maximum upload speed that a client can send data via the captive portal in the Maximum Bandwidth Upstream field. The range is from 0 to 300 Mbps. The default value is 0.

Step 13. Enter the maximum download speed that a client can receive data via the captive portal in the Maximum Bandwidth Downstream field. The range is from 0 to 300 Mbps. The default value is 0.



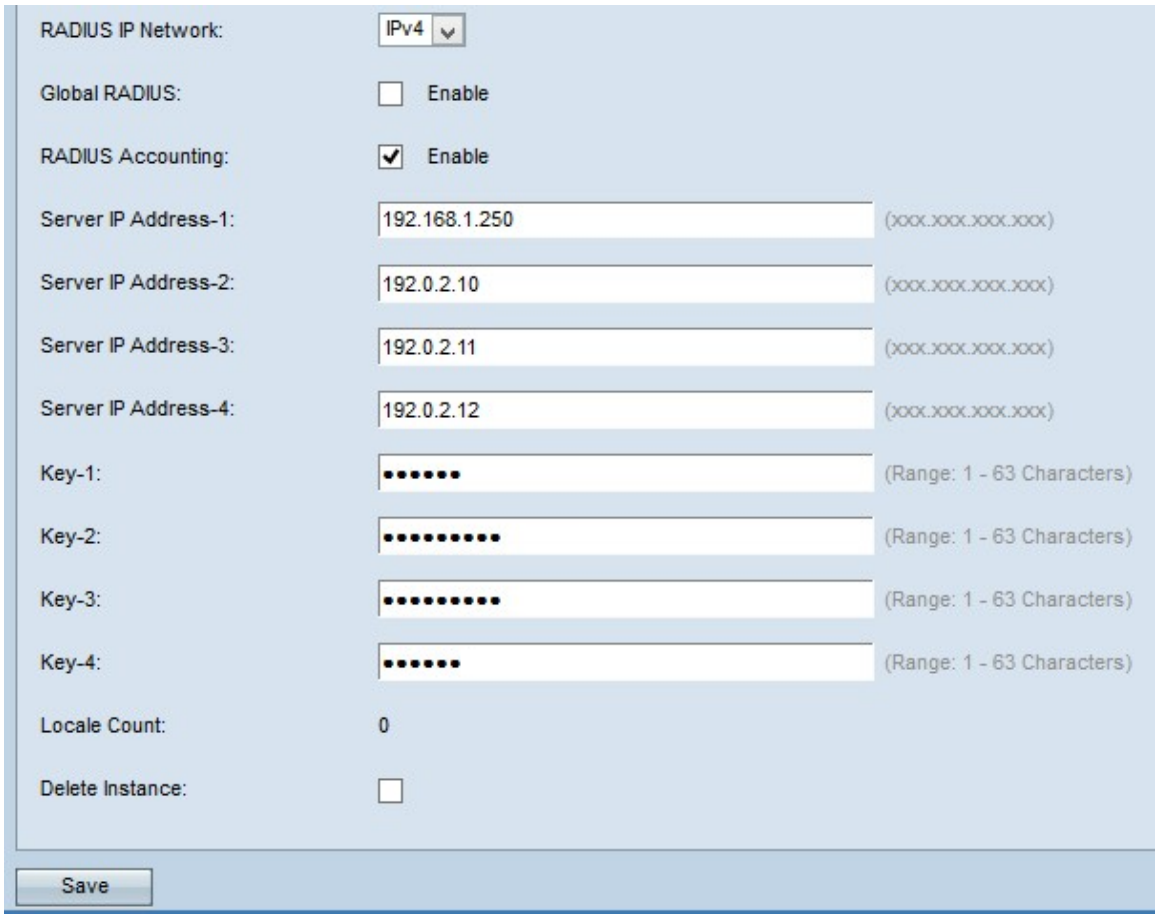
Step 14. Choose the desired group in the User Group Name field, which you wish to assign to the CP instance from the drop-down list of pre-configured groups.



Step 15. Choose the type of Internet protocol at the RADIUS IP Network field, that will be used by CP instance from the RADIUS IP network drop-down list. The possible values are:

- IPv4 — The address of the RADIUS client will be in the fourth version of IP with the address format xxx.xxx.xxx.xxx (192.0.2.10).

• IPv6 — The address of the RADIUS client will be in the sixth version of the IP with the address format xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (2001:DB8::CAD5:7D91).



Step 16. Check the **Enable** check box in the Global RADIUS field if you want to use the global RADIUS server list for authentication.

Timesaver: Skip to Step 22 if you choose global RADIUS. You don't need to enter the RADIUS server IP if you have enabled Global RADIUS option as CP feature will use the pre-configured global RADIUS servers.

Step 17. Check the **Enable** check box in the RADIUS Accounting field if you want to track and measure the time and data usage of the clients on the WAP network.

Step 18. Enter the IP address of the RADIUS server that you want to use as the primary server in the Server IP Address-1 field. The IP address should be in the format of IPv4 or IPv6 depending upon what you have chosen in RADIUS IP Network in Step 15.

Step 19. (Optional) Enter the backup RADIUS server IP addresses in the Server IP Address-2 to Server IP Address-4 fields. These servers are used if authentication fails with the primary server. You can configure up to three backup IP servers which will be authenticated in sequence if the predecessor fails.

Step 20. Enter the shared secret key in the Key-1 field that the WAP device uses to authenticate to the primary RADIUS server. You can use up to 63 standard alphanumeric and special characters. The key is case sensitive.

Step 21. (Optional) Enter the shared secret key in the Key 2 to 4 fields that the WAP device uses to authenticate to the respective backup RADIUS servers.

The Locale Count field displays the number of locales associated with the current instance.

Three different locales can be created and assigned to each instance from the web customization page.

Step 22. (Optional) If you want to delete the currently configured instance, check the **Delete Instance** check box to delete the currently configured instance.

Step 23. Click **Save** to save all the changes made.