Captive Portal Global 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. The database of the authenticated users is stored locally on the WAP device or on the RADIUS server. Captive portals are used at many Wi-Fi hotspots to charge users to get access to the Internet.
The global configuration page is used to control the administrative state of the Captive Portal feature and to configure global settings that will affect all captive portal instances configured on WAP device.

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

Applicable Devices

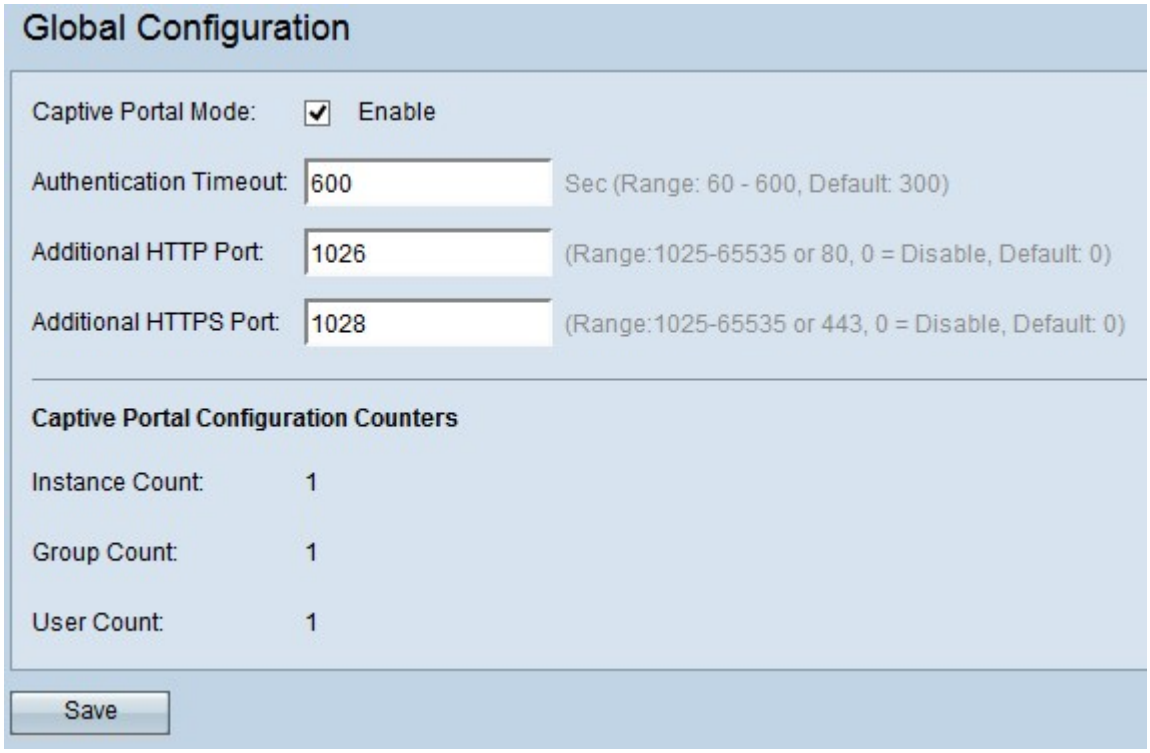
- WAP321

Software Version

- 1.0.3.4

Captive Portal Global Configuration

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



The *Global Configuration* page has some non-configurable fields, which display the following information:

- Instance Count — Specifies the number of CP (Captive Portal) instances currently configured on the WAP device. Up to two instances can be configured.
- Group Count — Specifies the number of CP groups currently configured on the WAP device. Up to two groups can be configured.
- User Count — Specifies the number of CP users currently configured on the WAP device. Up to 128 users can be configured.

Step 2. Check the **Enable** check box to enable the captive portal mode.

Step 3. Enter the number of seconds in the Authentication Timeout field that you want the access point to keep the authentication session open with the associated wireless client. The default authentication timeout is 300 seconds. The range is from 60 to 600 seconds.

Step 4. Enter the port number in the Additional HTTP Port field if you want to use an additional port for HTTP traffic. The default value is 0 (disabled). The range is from 0 to 65535.

Step 5. Enter the port number in the Additional HTTPS Port field if you want to use an additional port for HTTPS traffic (HTTP traffic over SSL). The default value is 0 (disabled). The range is from 0 to 65535.

Note: These additional ports are exclusively used for all other network traffic. Port number 80 or 443 cannot be used as they are default for HTTP and HTTPs respectively. Also, the HTTP and HTTPS ports cannot be the same.

Step 6. Click **Save** to save all the configurations made.