# Captive Portal Global Configuration für WAP321 Access Point

## Ziel

Über das Captive Portal können Sie mit dem WAP-Netzwerk verbundene Clients blockieren. Clients sehen eine spezielle Webseite für Authentifizierungszwecke, bevor sie das Internet normal nutzen dürfen. Die Captive Portal-Verifizierung richtet sich sowohl an Gäste als auch an authentifizierte Benutzer und nutzt den Webbrowser, indem er ihn in ein Authentifizierungsgerät verwandelt. Die Datenbank der authentifizierten Benutzer wird lokal auf dem WAP-Gerät oder auf dem RADIUS-Server gespeichert. Captive Portale werden an vielen Wi-Fi-Hotspots verwendet, um Benutzern den Zugang zum Internet in Rechnung zu stellen. Die globale Konfigurationsseite wird verwendet, um den Verwaltungsstatus der Captive Portal-Funktion zu steuern und globale Einstellungen zu konfigurieren, die sich auf alle auf dem WAP-Gerät konfigurierten Captive Portal-Instanzen auswirken.

In diesem Dokument wird erläutert, wie die globale Konfiguration des Captive Portals auf dem WAP321 Access Point konfiguriert wird.

## Anwendbare Geräte

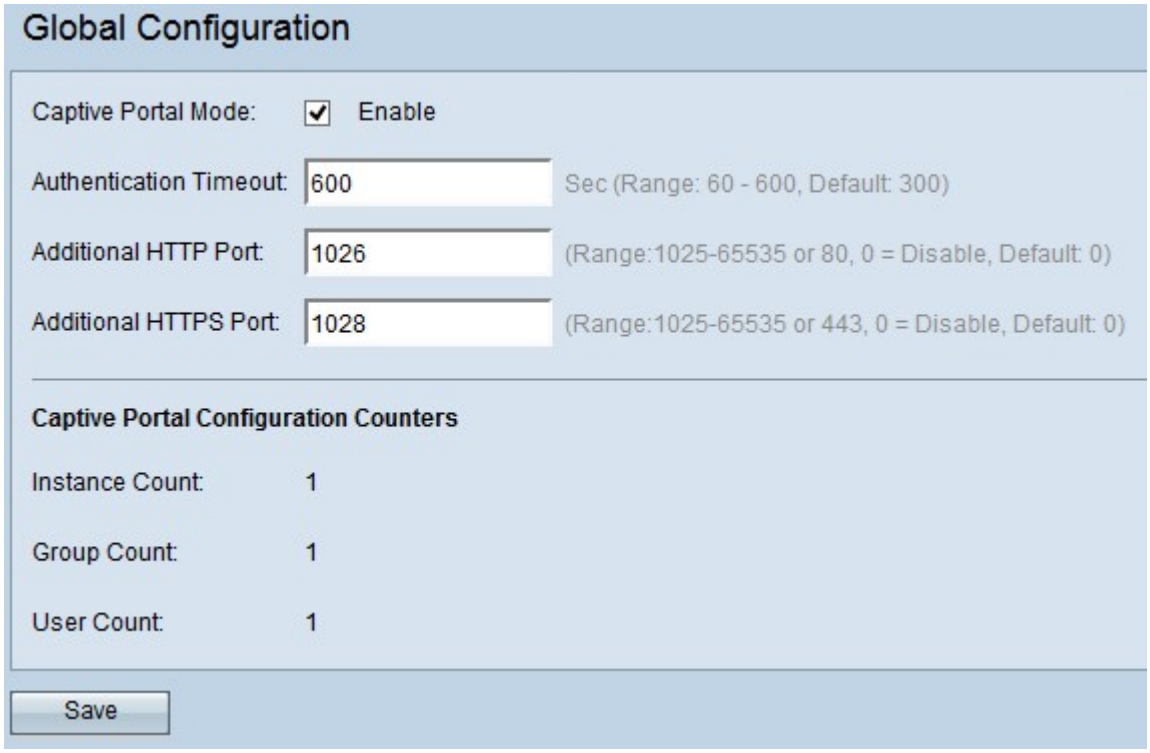
WAP321

## Softwareversion

·1,0/3,4

## Captive Portal - Globale Konfiguration

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Captive Portal > Global Configuration aus**. Die Seite *"Globale Konfiguration*" wird geöffnet:




Die Seite *Global Configuration* enthält einige nicht konfigurierbare Felder, die die folgenden Informationen anzeigen:

·Instanzanzahl - Gibt die Anzahl der CP-Instanzen (Captive Portal) an, die aktuell auf dem WAP-Gerät konfiguriert sind. Es können bis zu zwei Instanzen konfiguriert werden.

·Gruppenanzahl - Gibt die Anzahl der CP-Gruppen an, die aktuell auf dem WAP-Gerät konfiguriert sind. Es können bis zu zwei Gruppen konfiguriert werden.

·Benutzeranzahl - Gibt die Anzahl der CP-Benutzer an, die derzeit auf dem WAP-Gerät konfiguriert sind. Es können bis zu 128 Benutzer konfiguriert werden.

Schritt 2: Aktivieren Sie das Kontrollkästchen **Aktivieren**, um den Captive Portal-Modus zu aktivieren.

Schritt 3: Geben Sie die Anzahl der Sekunden in das Feld Authentication Timeout (Authentifizierungs-Timeout) ein, in dem der Access Point die Authentifizierungssitzung mit dem verknüpften Wireless-Client offen halten soll. Der Standard-Authentifizierungs-Timeout ist 300 Sekunden. Der Bereich liegt zwischen 60 und 600 Sekunden.

Schritt 4: Geben Sie die Portnummer im Feld "Zusätzlicher HTTP-Port" ein, wenn Sie einen zusätzlichen Port für HTTP-Datenverkehr verwenden möchten. Der Standardwert ist 0 (deaktiviert). Der Bereich liegt zwischen 0 und 65.535.

Schritt 5: Geben Sie die Portnummer im Feld Zusätzlicher HTTPS-Port ein, wenn Sie einen zusätzlichen Port für HTTPS-Datenverkehr (HTTP-Datenverkehr über SSL) verwenden möchten. Der Standardwert ist 0 (deaktiviert). Der Bereich liegt zwischen 0 und 65.535.

**Hinweis**: Diese zusätzlichen Ports werden ausschließlich für den anderen Netzwerkverkehr verwendet. Die Portnummer 80 oder 443 kann nicht verwendet werden, da sie für HTTP bzw. HTTP Standard sind. Außerdem können die HTTP- und HTTPS-Ports nicht identisch sein.

Schritt 6: Klicken Sie auf **Speichern**, um alle vorgenommenen Konfigurationen zu speichern.