

Configuración global porta prisionera en el Punto de acceso WAP321

Objetivo

El portal prisionero permite que usted bloquee a los clientes conectados con la red WAP. Los clientes ven una página web especial para los fines de autenticación antes de que se les permita utilizar Internet normalmente. La verificación porta prisionera está para ambos invitados y usuarios autenticados, y hace uso del buscador Web dándole vuelta en un dispositivo de la autenticación. La base de datos de los usuarios autenticados se salva localmente en el dispositivo WAP o en el servidor de RADIUS. Los portales prisioneros se utilizan en muchos hotspots del Wi-Fi para cargar a los usuarios conseguir el acceso a Internet. La página de la configuración global se utiliza para controlar al estado administrativo de la característica porta prisionera y para configurar las configuraciones globales que afectarán a todos los casos porta prisioneros configurados en el dispositivo WAP.

Este documento explica cómo configurar la configuración global porta prisionera en el Punto de acceso WAP321.

Dispositivos aplicables

- WAP321

Versión de software

- 1.0.3.4

Configuración global porta prisionera

Paso 1. Ábrase una sesión a la utilidad de configuración de la red y elija el **portal prisionero > la configuración global**. La página de la *configuración global* se abre:

Global Configuration

Captive Portal Mode: Enable

Authentication Timeout: Sec (Range: 60 - 600, Default: 300)

Additional HTTP Port: (Range: 1025-65535 or 80, 0 = Disable, Default: 0)

Additional HTTPS Port: (Range: 1025-65535 or 443, 0 = Disable, Default: 0)

Captive Portal Configuration Counters

Instance Count: 1

Group Count: 1

User Count: 1

La página de la *configuración global* tiene algunos campos no-configurables, que visualizan la siguiente información:

- Cuenta del caso — Especifica el número de casos CP (portal prisionero) configurados actualmente en el dispositivo WAP. Hasta dos casos pueden ser configurados.
- Cuenta del grupo — Especifica el número de grupos CP configurados actualmente en el dispositivo WAP. Hasta dos grupos pueden ser configurados.
- Cuenta del usuario — Especifica el número de usuarios CP configurados actualmente en el dispositivo WAP. Hasta el 128 los usuarios pueden ser configurados.

Paso 2. Controle la casilla de verificación del **permiso** para activar el modo porta prisionero.

Paso 3. Ingrese el número de segundos en el campo del descanso de la autenticación que usted quisiera que el Punto de acceso mantuviera la sesión de la autenticación abierta con el cliente de red inalámbrica asociado. El descanso de la autenticación del valor por defecto es 300 segundos. El rango es a partir 60 a 600 segundos.

Paso 4. Ingrese el número del puerto en el campo de puerto adicional HTTP si usted quiere utilizar un puerto adicional para el tráfico HTTP. El valor predeterminado es 0 (inhabilitado). El rango es a partir la 0 a 65535.

Paso 5. Ingrese el número del puerto en el campo de puerto adicional HTTPS si usted quiere utilizar un puerto adicional para el tráfico HTTPS (tráfico HTTP sobre el SSL). El valor predeterminado es 0 (inhabilitado). El rango es a partir la 0 a 65535.

Note: Estos puertos adicionales se utilizan exclusivamente para el tráfico de cualquier otra red. El número del puerto 80 o 443 no puede ser utilizado pues son valor por defecto para el HTTP y HTTPS respectivamente. También, los puertos HTTP y HTTPS no pueden ser lo mismo.

Paso 6. Salvaguardia del teclado para salvar todas las configuraciones hechas.