Anzeigen fehlgeschlagener Authentifizierungs-Clients im Captive Portal des WAP321

Ziel

Über das Captive Portal kann ein Administrator Clients, die mit dem WAP-Netzwerk verbunden sind, blockieren. Clients sehen eine spezielle Webseite für Authentifizierungszwecke, bevor sie das Internet normal nutzen dürfen. Die Überprüfung des Captive Portals ist sowohl für Gäste als auch für authentifizierte Benutzer möglich. Captive Portal nutzt den Webbrowser und verwandelt ihn in ein Authentifizierungsgerät. Captive Portale werden besonders an vielen Wi-Fi-Hotspots genutzt, um Benutzer für den Zugang zum Internet zu belasten.

In diesem Artikel wird beschrieben, wie Sie fehlerhafte authentifizierte Clients auf Captive Portal (CP) des WAP321-Access Points anzeigen.

Hinweis: Um zu erfahren, welche Clients durch das Captive Portal authentifiziert werden, lesen Sie den Artikel *View Authenticated Clients in Captive Portal auf WAP321 Access Points.*

Anwendbares Gerät

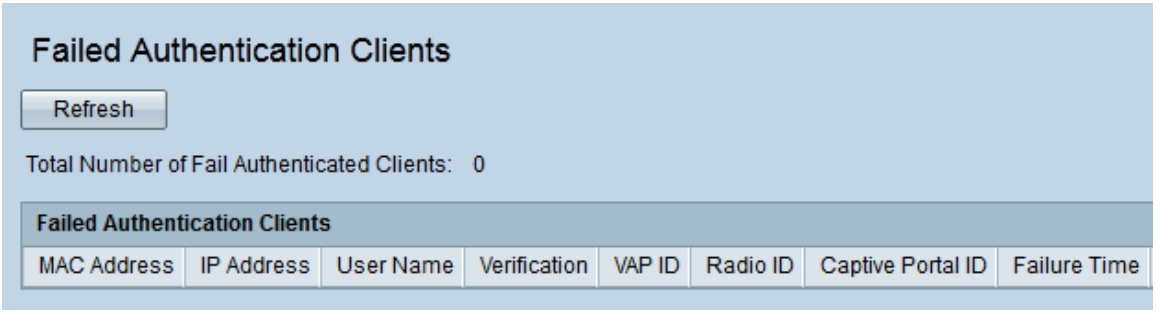
WAP321

Softwareversion

·1,0/3,4

Captive Portal-Gruppen

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, um **Captive Portal > Failed Authentication Clients** auszuwählen. Die Seite *Fehlgeschlagene Authentifizierungsclients* wird geöffnet.



In den Clients für fehlgeschlagene Authentifizierung sind diese Informationen verfügbar:

·Gesamtanzahl der authentifizierten Clients (Fail Authenticated Clients) - Zeigt die Anzahl der Clients an, die keine Authentifizierung erhalten haben.

·MAC Address (MAC-Adresse): Zeigt die MAC-Adresse des fehlgeschlagenen Authentifizierungsclients an.

·IP Address (IP-Adresse): Zeigt die IP-Adresse des fehlgeschlagenen Authentifizierungsclients an.

·Benutzername: Zeigt den Captive Portal-Benutzernamen der Clients für fehlgeschlagene Authentifizierung an.

·Verification (Verifizierung): Zeigt die Methode an, mit der der Client versucht hat, sich im Captive Portal zu authentifizieren. Es hat folgende Werte:

- Guest (Gast): Der Benutzer benötigt keine Authentifizierung.

- Local (Lokal): Das WAP-Gerät verwendet eine lokale Datenbank, um Benutzer zu authentifizieren.

- RADIUS - Das WAP-Gerät verwendet einen Remote-RADIUS-Server zur Authentifizierung von Benutzern.

·VAP-ID: Zeigt den virtuellen Access Point an, dem der Client zugeordnet ist.

·Radio ID (Funkerkennung): Zeigt die Identifikationsnummer des Funkmoduls an.

·Captive Portal ID (Captive Portal-ID): Zeigt die Instanz des Captive Portals an, dem der Client zugeordnet ist.

·Failure Time (Ausfallzeit): Zeigt einen Zeitstempel an, der die Zeit anzeigt, zu der die Authentifizierung fehlgeschlagen ist.

Schritt 2 (optional). Um die aktuellsten Daten abzurufen, klicken Sie auf **Aktualisieren**.