Junivo WiFi360° Integration with Aruba Networks WiFi Infrastructure

Feb, 2017

Junivo

Contents

Introduction

Junivo's cloud-based WiFi360°, combines Wi-Fi technology with other data sources like door count, POS, and takes advantage of existing Aruba WiFi infrastructure. It is a full suite of Social Wi-Fi Hotspot, In-store Analytics and Marketing Automation solution connects the physical store with digital shopping experience.

Aruba customers have the ability to extract additional value from their existing infrastructure by running WiFi360° as part of their deployments. A joint solution creates an integrated user experience that enable brick and mortar retailers to engage with mobile customers along their purchase path and also leads to more effective marketing, new revenue opportunities, better customer service, improved operational efficiency, competitive advantages over rival organizations and other business benefits.

This document details WiFi360° integration with Aruba ALE (Analytics & Location Engine) and AirWave

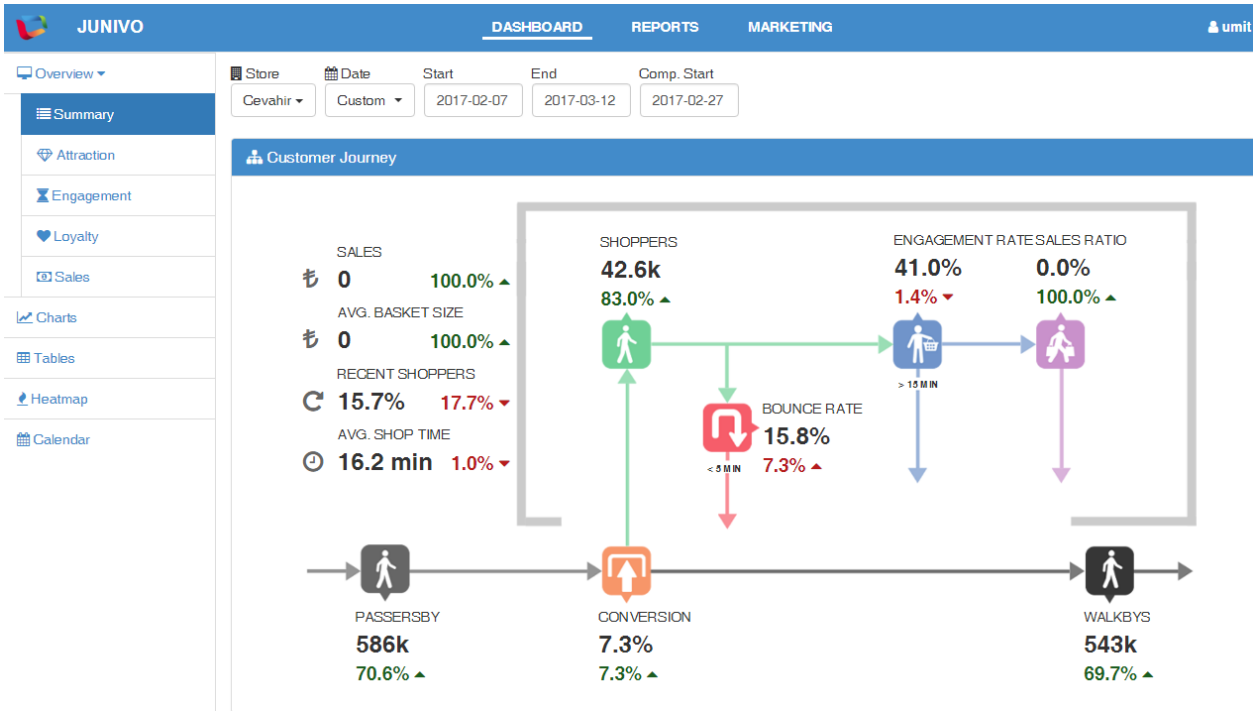


Figure 1 - An overview screenshot from WiFi360 dashboard

Prerequisites

The following Aruba components are needed to enable Junivo WiFi360° solution.

- Mobility Controller (ArubaOS 6.3 or higher) and Access Points (ArubaOS 6.3 or higher) or Instant Access Points (Aruba InstantOS 4.0 or higher).
- Airwave Network Management Suite
- Analytics and Location Engine Server (ALE 1.3 or higher)

Overview

The Aruba Analytics and Location Engine (ALE) is a virtual context aggregation and location engine that collects data about Wi-Fi-enabled mobile devices that are nearby or connected to an Aruba WLAN. This data is made available to Junivo WiFi360° platform through high-performance APIs.

Insights about traffic patterns-including most traversed paths, dwell times and repeat visitor frequency – are correlated with other data sources, such as sensors, loyalty databases, and point-of-sale systems.

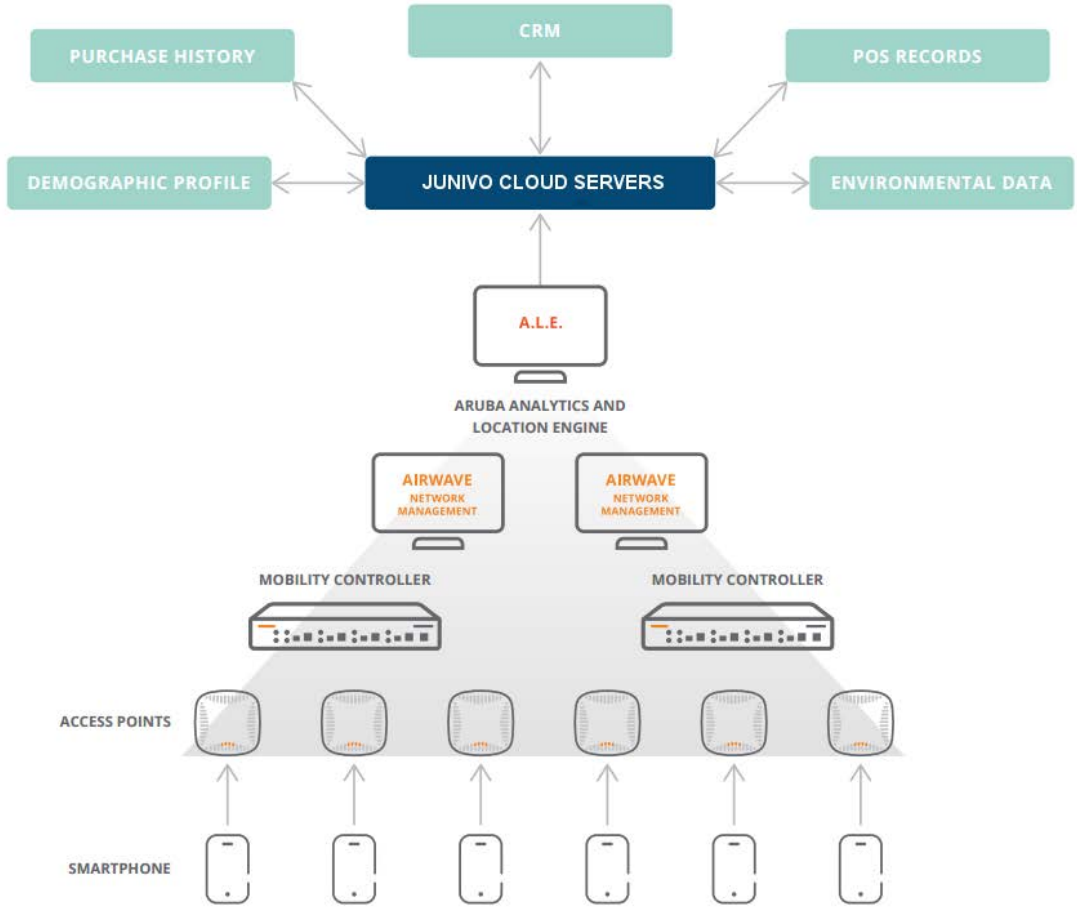


Figure 2 - Junivo Analytics and Aruba WLAN Infrastructure

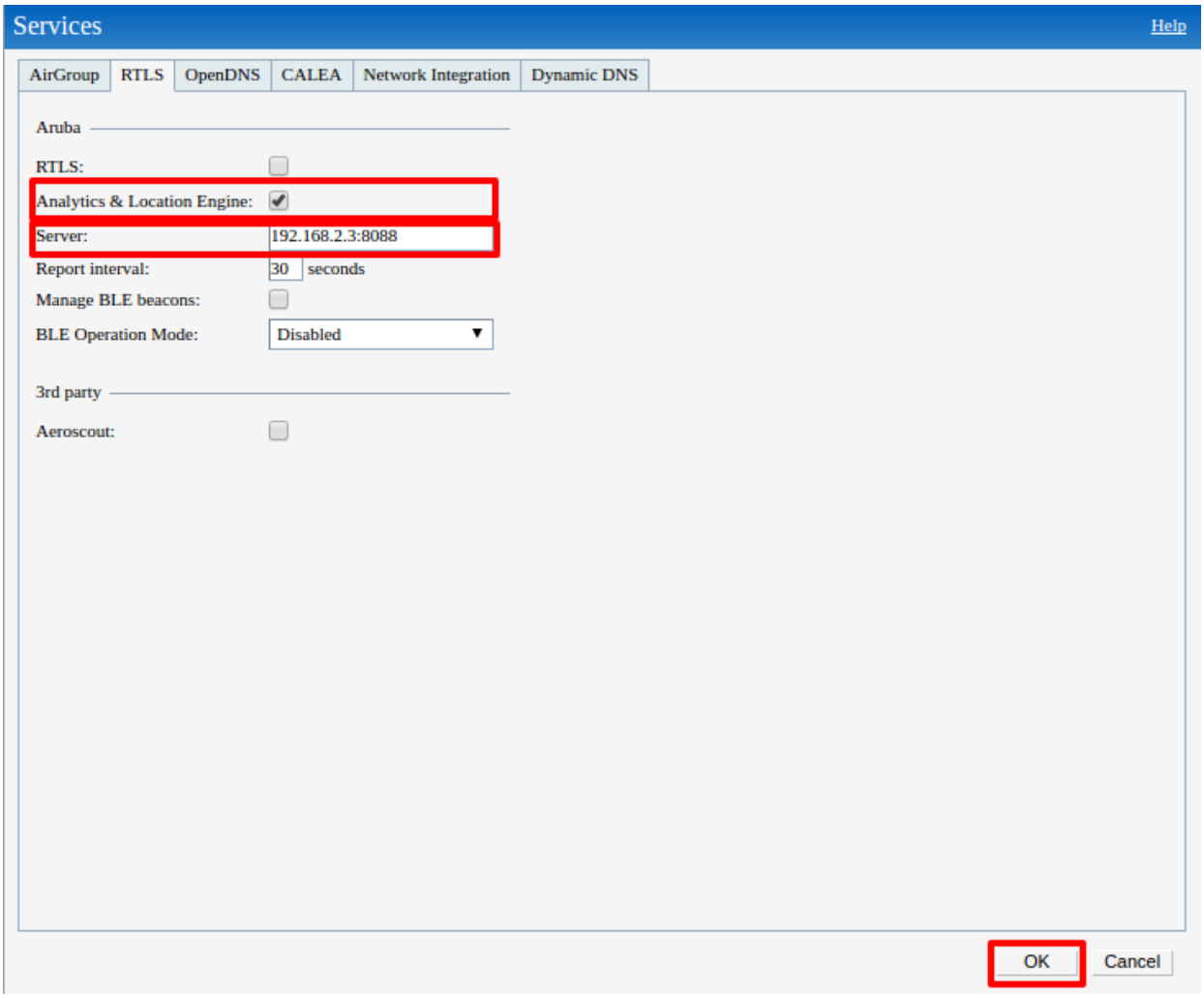
Configuring Aruba Components

1. Configuring Aruba Analytics & Location Engine (ALE)

1. Login to ALE dashboard
2. Navigate to **Configuration→ Mode**
3. Select **Context (station, application, proximity)** option
4. Click **Apply** button
5. Navigate to **Configuration → Options**
6. Under **General** section, turn off **Enable Anonymization**
7. Under **Remote Endpoint** section, click the **plus button (+)**
8. Enter **Remote endpoint url** as **northbound.junivo.com**, enter **Port** as **443**
9. Click **Apply** button

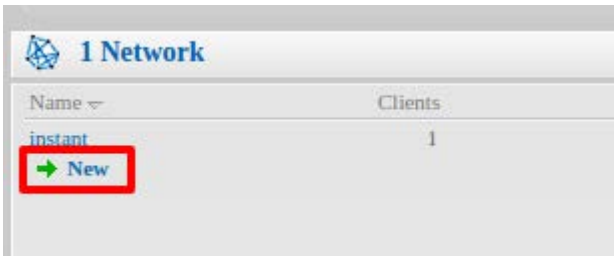
2. Configuring Aruba Instant Access Point (IAP) for Analytics

1. Login to IAP dashboard
2. Navigate to **More** → **Services** → **RTLS**
3. Turn on **Analytics & Location Engine**
4. Enter **your ALE Server's IP address and port** to **Server**. (e.g. 192.168.2.3:8088)
5. Click **OK**

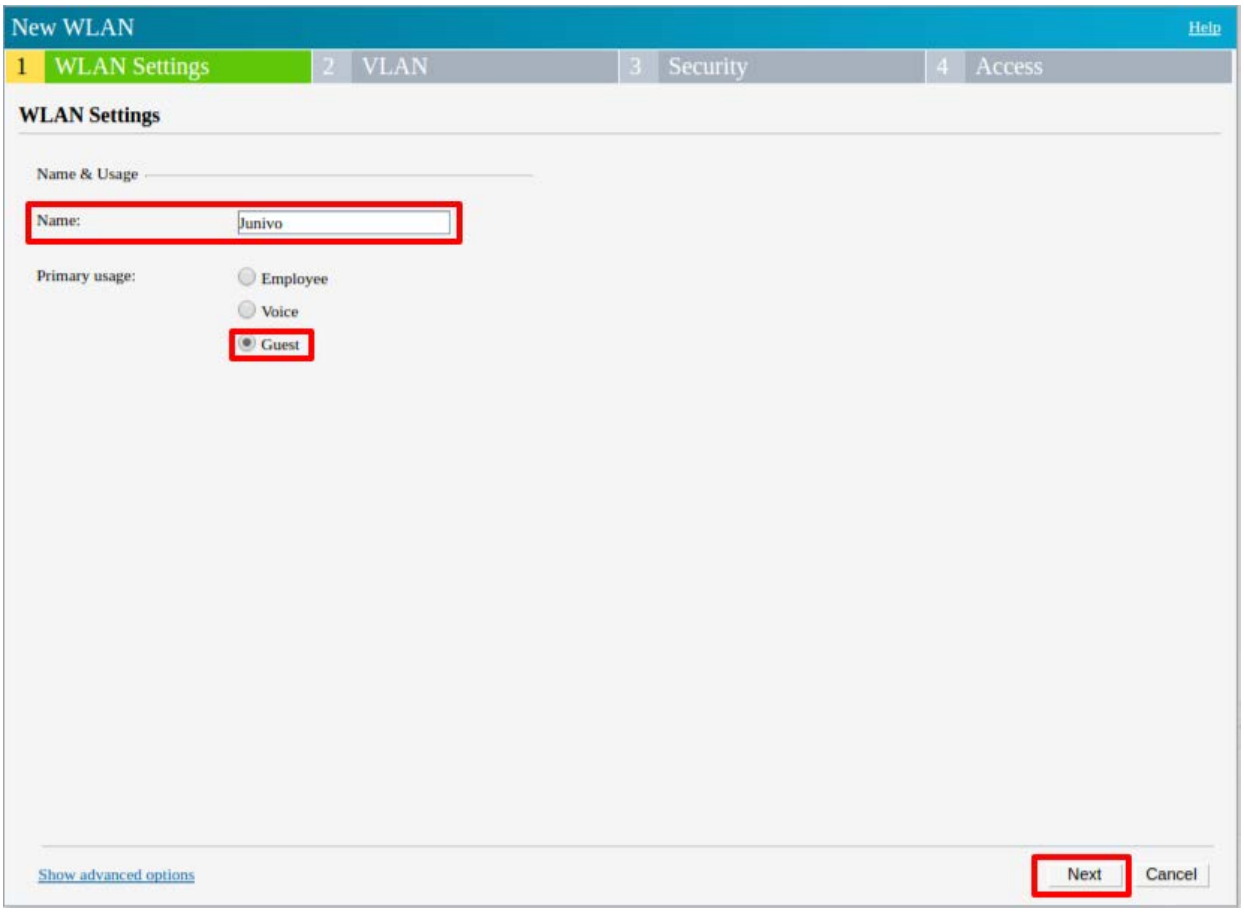


3. Configuring IAP for Junivo Captive Portal

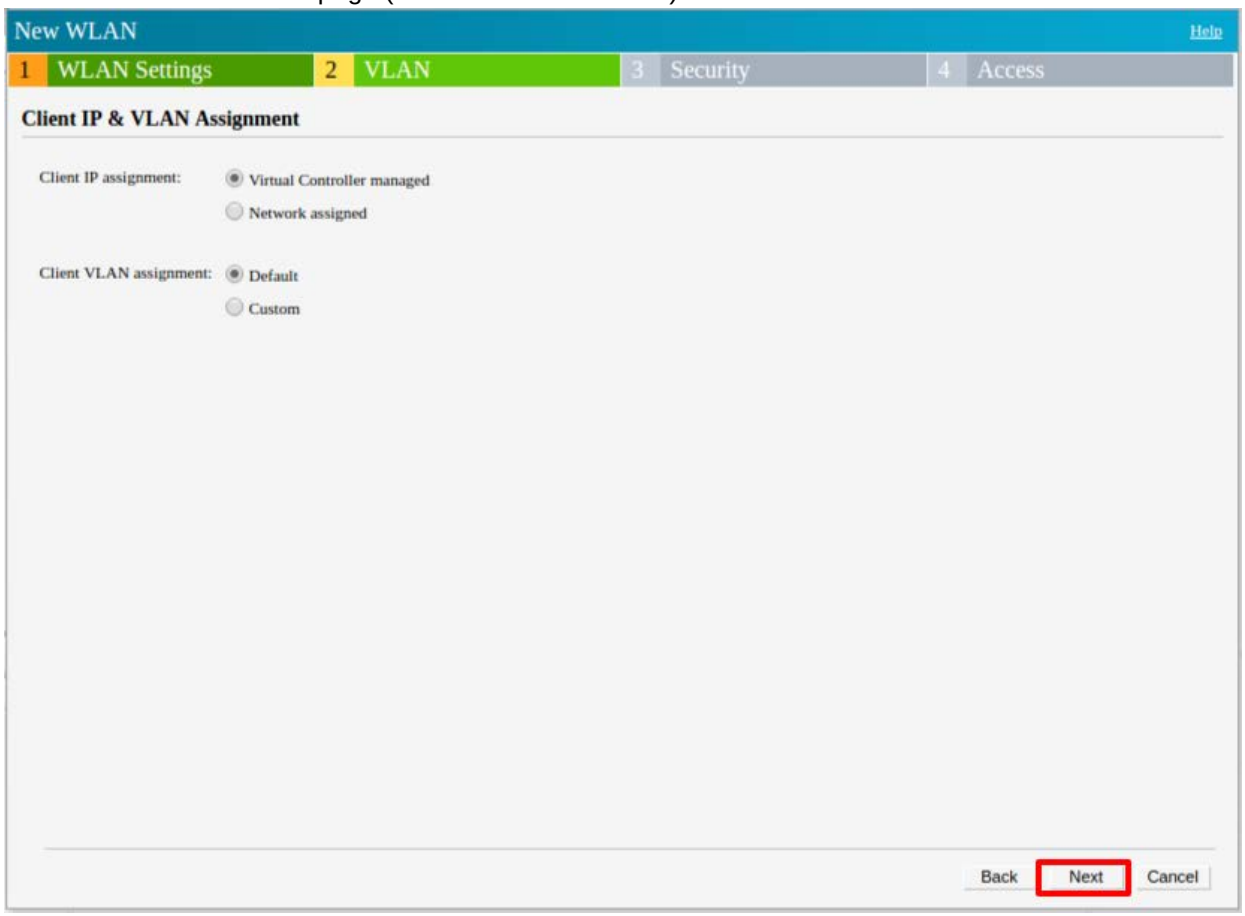
1. Login to IAP dashboard
2. Click **New** under **Network** section



3. Enter **Junivo** as **Name (SSID)**
4. Select **Guest** as **Primary usage**
5. Click **Next** under **WLAN Settings** page

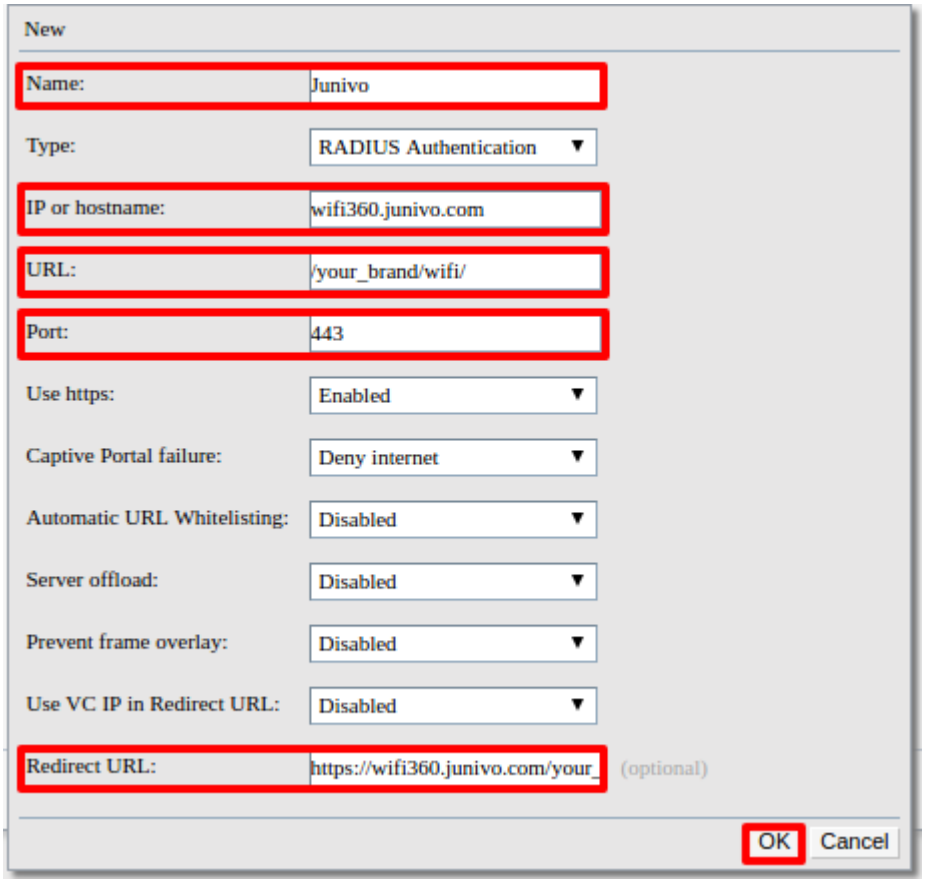


6. Click **Next** under **VLAN** page (no modification needed)

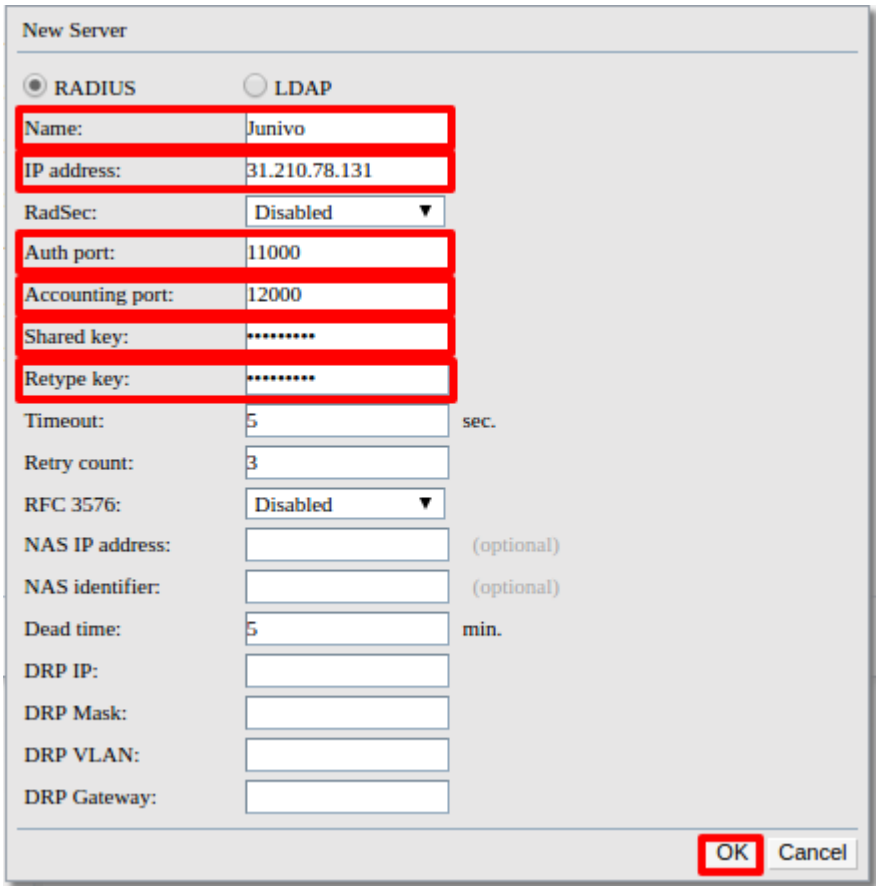


7. Select **External** as **Splash page type**

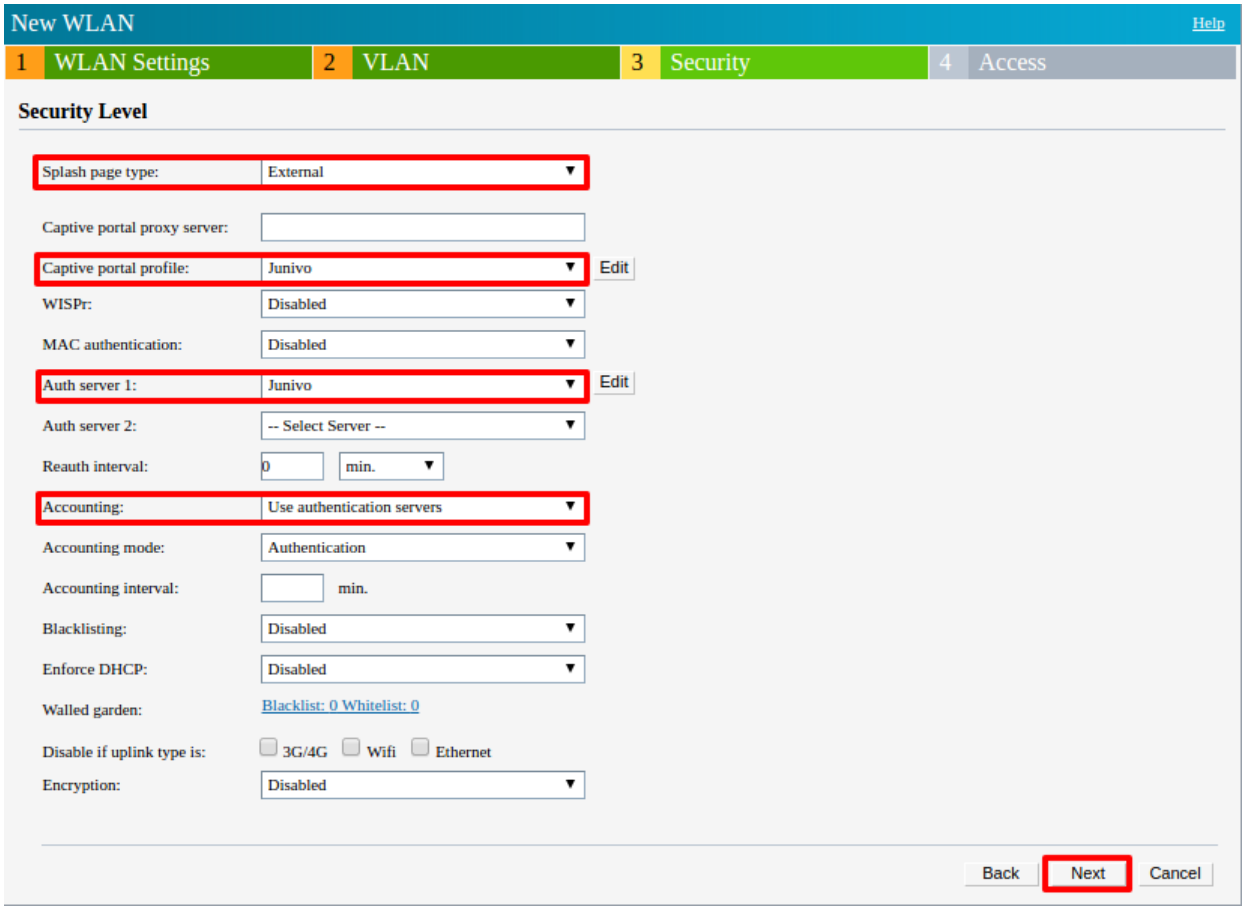
8. Select **New** as **Captive portal profile,** a small window will open:
    i. Enter **Junivo** as **Name**
    ii. Enter **wifi360.junivo.com** as **IP or hostname**
    iii. Enter **/your_brand/wifi/** as **URL** (use your brand name instead of your_brand)
    iv. Enter **443** as **Port**
    v. Enter **https://wifi360.junivo.com/your_brand/wifi/landing/** as **Redirect URL**
    vi. Click **OK,** small window will close



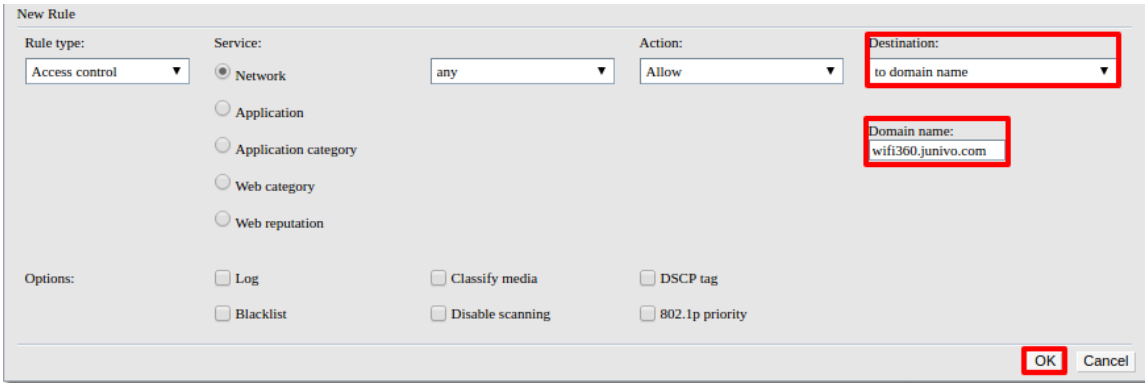
9. Select **New** as **Auth server 1,** another small window will open
    i. Enter **Junivo** as **Name**
    ii. Enter **31.210.78.131** as **Server address**
    iii. Enter provided **Auth port** (e.g. 11000)
    iv. Enter provided **Accounting port** (e.g. 12000)
    v. Enter provided **Shared secret**
    vi. Click **OK**, small window will close



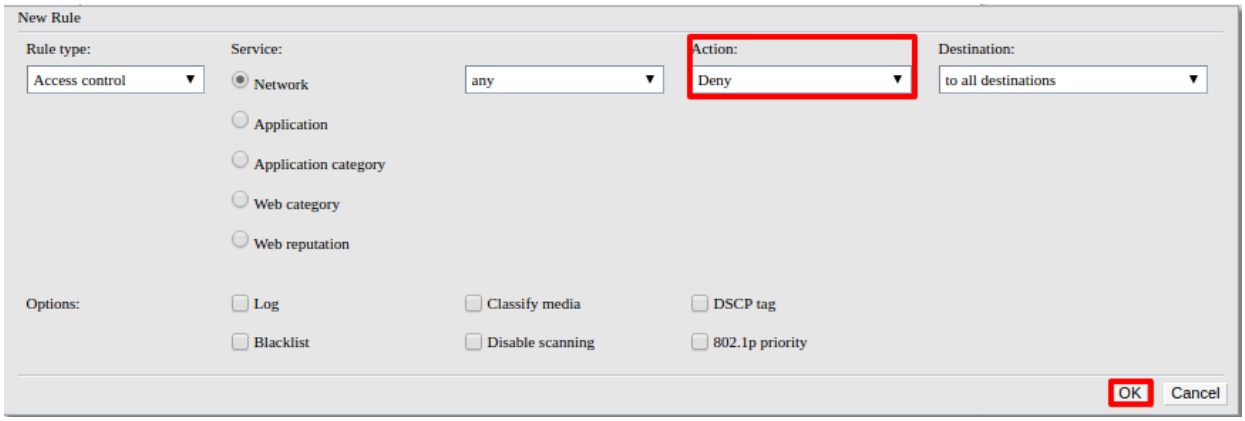
10. **Select Use authentication servers** under **Accounting**
11. Click **Next**



12. Select **Role Based**
13. Click **New** under **Roles** section
14. Enter **Preauth** and click **OK**
15. Repeat this for the following domain name list:
    i. Click **New** under **Access Rules for Preauth** section
    ii. Select **to domain name** as **Destination**
    iii. Enter a domain name to **Domain name**
        1. **wifi360.junivo.com**
        2. **facebook.com**
        3. **facebook.net**
        4. **fbcdn.net**
        5. **akamaihd.net**
    iv. Click **OK**

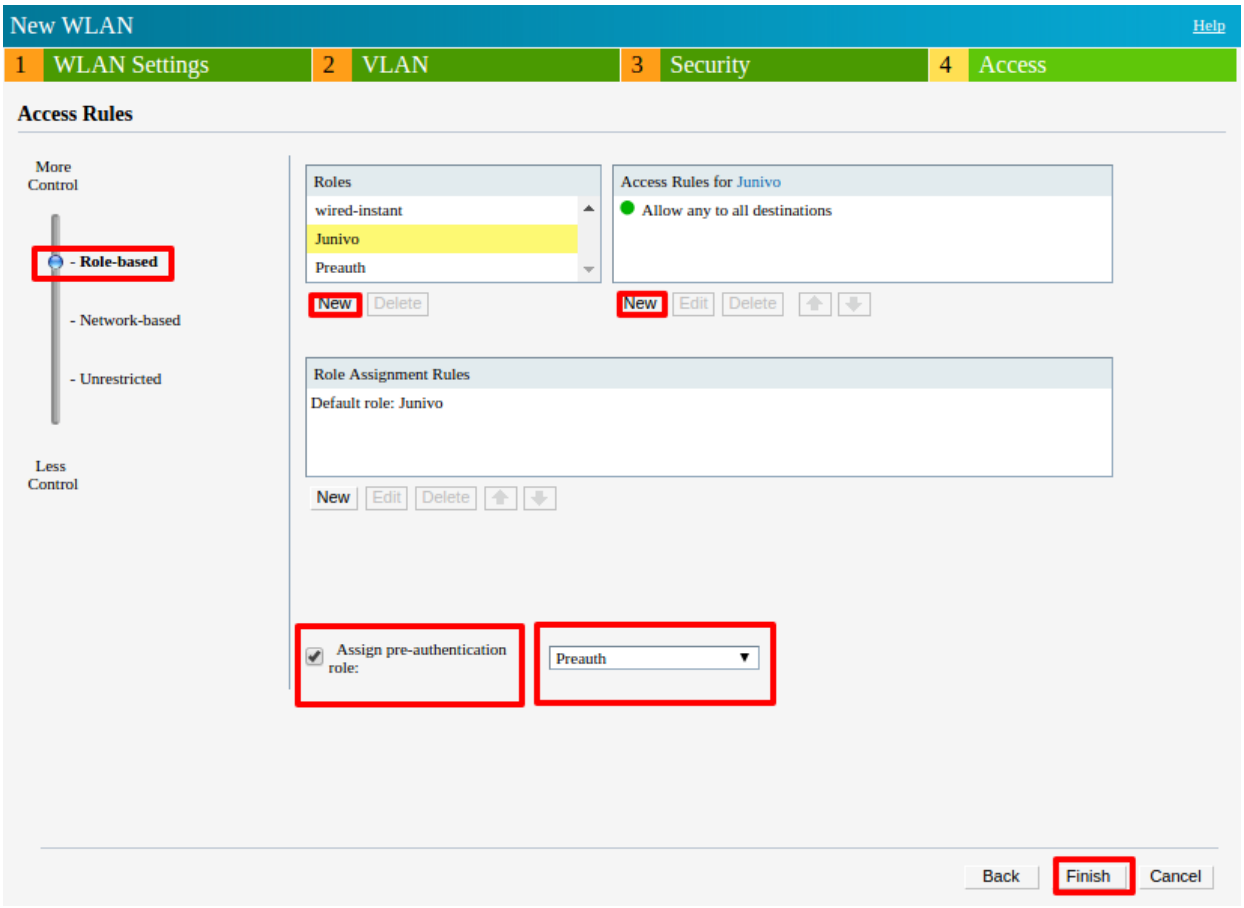


16. Click **New** under **Access Rules for Preauth** section
17. Select **Deny** as **Action**
18. Click **OK**



19. Select **Allow any to all destinations** under **Access rules for Preauth** section
20. Click **Delete**
21. Select **Junivo** under **Roles** section
22. **Enable Assign pre-authentication role** and select **Preauth**

23. Click **Finish**



24. Navigate to **Security** → **Walled Garden**
25. Click **New** button under **Blacklist** section
26. Enter **clients3.google.com** as **New regular expression for Blacklist**
27. Click **OK** in the small box

28. Click **OK** in the **Services** window