

aruba

a Hewlett Packard
Enterprise company

Junivo WiFi360° Integration with Aruba Networks WiFi Infrastructure

Feb, 2017

Junivo



Contents

Introduction	3
Prerequisites	3
Overview	3
Configuring Aruba Components	4
1. Configuring Aruba Analytics & Location Engine (ALE)	4
2. Configuring Aruba Instant Access Point (IAP) for Analytics.....	5
3. Configuring IAP for Junivo Captive Portal.....	6

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

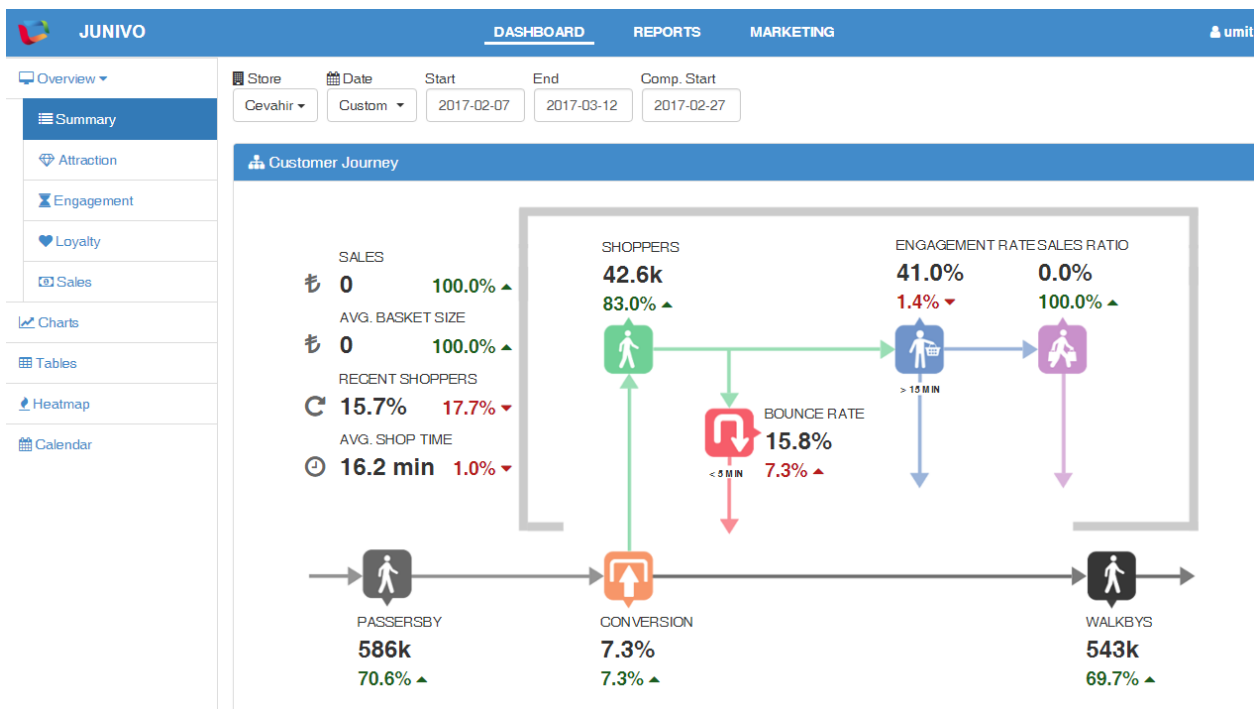


Figure 1 - An overview screenshot from WiFi360 dashboard

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.

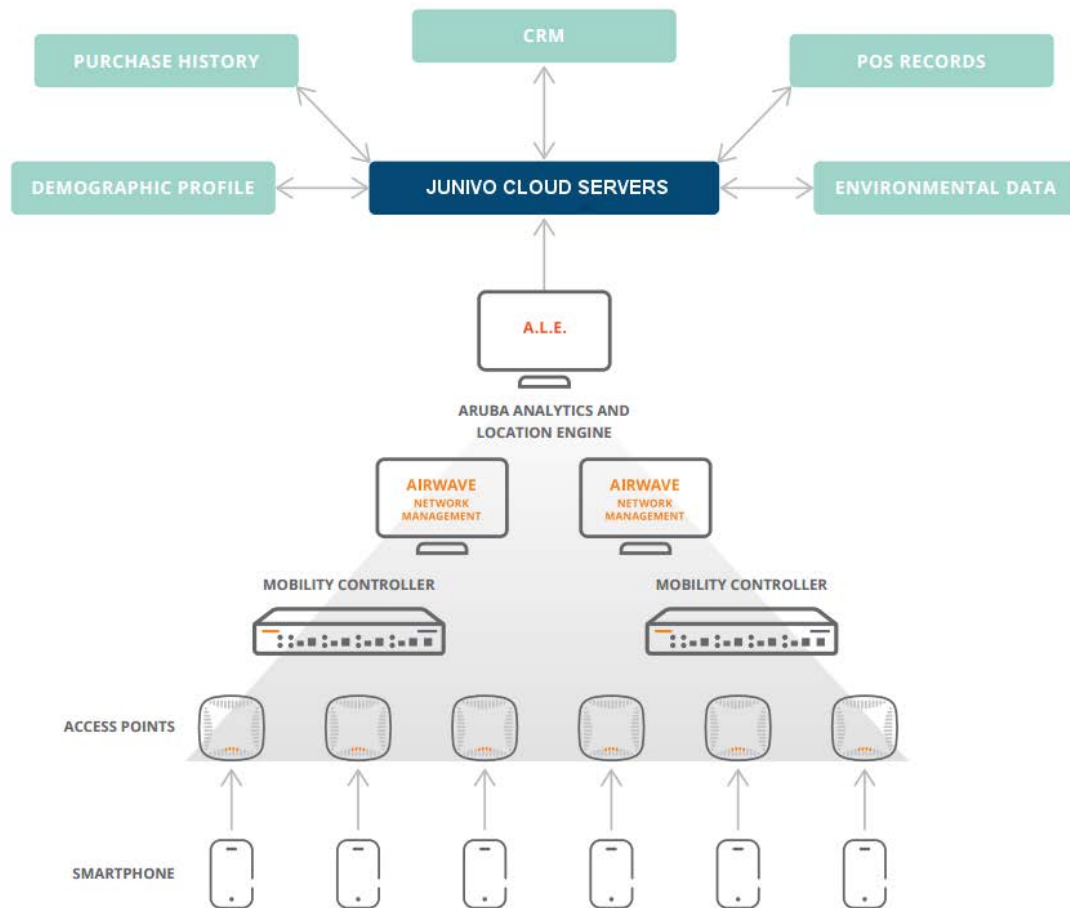


Figure 2 - Junivo Analytics and Aruba WLAN Infrastructure

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

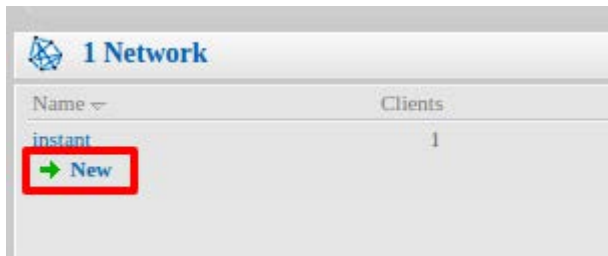
1. Login to IAP dashboard
2. Navigate to **More** → **Services** → **RTLS**
3. Turn on **Analytics & Location Engine**
4. Enter **your ALE Server's IP address and port** to **Server**. (e.g. 192.168.2.3:8088)
5. Click **OK**

The screenshot shows the 'Services' configuration page for an Aruba IAP. The 'RTLS' tab is selected. Under the 'Aruba' section, the 'Analytics & Location Engine' checkbox is checked, and the 'Server' field is set to '192.168.2.3:8088'. The 'Report interval' is set to '30 seconds'. Under the '3rd party' section, the 'Aeroscout' checkbox is unchecked. The 'OK' button is highlighted with a red box.

Category	Option	Value
Aruba	RTLS:	<input type="checkbox"/>
Aruba	Analytics & Location Engine:	<input checked="" type="checkbox"/>
Aruba	Server:	192.168.2.3:8088
Aruba	Report interval:	30 seconds
Aruba	Manage BLE beacons:	<input type="checkbox"/>
Aruba	BLE Operation Mode:	Disabled
3rd party	Aeroscout:	<input type="checkbox"/>

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

The screenshot displays the 'New WLAN' configuration interface. At the top, there are four tabs: '1 WLAN Settings' (highlighted in green), '2 VLAN', '3 Security', and '4 Access'. Below the tabs, the 'WLAN Settings' section is visible. Under 'Name & Usage', the 'Name' field contains the text 'Junivo'. Below this, the 'Primary usage' section has three radio button options: 'Employee', 'Voice', and 'Guest'. The 'Guest' option is selected and highlighted with a red box. At the bottom right of the page, there are two buttons: 'Next' (highlighted with a red box) and 'Cancel'. A link for 'Show advanced options' is located at the bottom left.

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

The screenshot shows a configuration interface for a new WLAN. At the top, there is a blue header with the text "New WLAN" and a "Help" link. Below the header is a navigation bar with four steps: "1 WLAN Settings", "2 VLAN", "3 Security", and "4 Access". The "VLAN" step is currently active. The main content area is titled "Client IP & VLAN Assignment" and contains two sections of radio button options:

- Client IP assignment:**
 - Virtual Controller managed
 - Network assigned
- Client VLAN assignment:**
 - Default
 - Custom

At the bottom right of the form, there are three buttons: "Back", "Next", and "Cancel". The "Next" button is highlighted with a red rectangular box.

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

The screenshot shows a 'New' configuration window for a captive portal profile. The fields are as follows:

Name:	Junivo
Type:	RADIUS Authentication
IP or hostname:	wifi360.junivo.com
URL:	/your_brand/wifi/
Port:	443
Use https:	Enabled
Captive Portal failure:	Deny internet
Automatic URL Whitelisting:	Disabled
Server offload:	Disabled
Prevent frame overlay:	Disabled
Use VC IP in Redirect URL:	Disabled
Redirect URL:	https://wifi360.junivo.com/your_ (optional)

Buttons: OK, Cancel

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

The screenshot shows a 'New Server' configuration window. At the top, there are two radio buttons: 'RADIUS' (selected) and 'LDAP'. Below this, several fields are visible, with the following values entered:

Name:	Junivo	
IP address:	31.210.78.131	
RadSec:	Disabled	
Auth port:	11000	
Accounting port:	12000	
Shared key:	*****	
Retype key:	*****	
Timeout:	5	sec.
Retry count:	3	
RFC 3576:	Disabled	
NAS IP address:		(optional)
NAS identifier:		(optional)
Dead time:	5	min.
DRP IP:		
DRP Mask:		
DRP VLAN:		
DRP Gateway:		

At the bottom right, there are two buttons: 'OK' and 'Cancel'. The 'OK' button is highlighted with a red box.

10. Select **Use authentication servers** under **Accounting**

11. Click **Next**

The screenshot shows the 'New WLAN' configuration interface. At the top, there are four tabs: 'WLAN Settings', 'VLAN', 'Security', and 'Access'. The 'Security' tab is active. Below the tabs, the 'Security Level' section contains various configuration options. The 'Accounting' dropdown is highlighted with a red box and set to 'Use authentication servers'. Other options include 'Splash page type' (External), 'Captive portal profile' (Junivo), 'Auth server 1' (Junivo), 'Auth server 2' (-- Select Server --), 'Reauth interval' (0 min.), 'Accounting mode' (Authentication), 'Accounting interval' (min.), 'Blacklisting' (Disabled), 'Enforce DHCP' (Disabled), 'Walled garden' (Blacklist: 0 Whitelist: 0), 'Disable if uplink type is' (3G/4G, Wifi, Ethernet), and 'Encryption' (Disabled). At the bottom right, there are three buttons: 'Back', 'Next' (highlighted with a red box), and 'Cancel'.

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**

New Rule

Rule type: Access control

Service: Network

any

Action: Allow

Destination: to domain name

Domain name: wifi360.junivo.com

Options: Log, Classify media, DSCP tag, Blacklist, Disable scanning, 802.1p priority

OK Cancel

16. Click **New** under **Access Rules for Preauth** section

17. Select **Deny** as **Action**

18. Click **OK**

New Rule

Rule type: Access control

Service: Network

any

Action: Deny

Destination: to all destinations

Options: Log, Classify media, DSCP tag, Blacklist, Disable scanning, 802.1p priority

OK Cancel

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**

New WLAN Help

1 WLAN Settings 2 VLAN 3 Security 4 Access

Access Rules

More Control

- Role-based

- Network-based

- Unrestricted

Less Control

Roles

wired-instant

Junivo

Preauth

New Delete

Access Rules for Junivo

● Allow any to all destinations

New Edit Delete ↑ ↓

Role Assignment Rules

Default role: Junivo

New Edit Delete ↑ ↓

Assign pre-authentication role: Preauth

Back **Finish** Cancel

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

