



a Hewlett Packard
Enterprise company

Aruba Central PoC Integrating Purple

Adolfo Bolivar
January 2019



a Hewlett Packard
Enterprise company

Agenda


- Setup Guest WiFi on Aruba Central and points to Purple Cloud service
- Setup Purple Dashboard
- Test Guest Access





a Hewlett Packard
Enterprise company

Task: Setup Guest WiFi on Aruba Central and points to Purple Cloud service

Create new WiFi network

 Central

 **CURRENT APP**
WIRELESS MANAGEMENT

 **Search Current App**
Find devices, clients and networks

Networks
Add and edit networks


Access Points
View APs and set device parameters

RF
Set Aruba Adaptive Radio Management

Wireless IDS/IPS
Manage intrusion detection and prevention


Security
Set advanced security parameters

VPN
Manage controller VPN connections

 **FILTER WIRELESS MANAGEMENT**
Home CI 159 (3 Total Devices | 1 Offline APs | 0 Offline SWITCHES | 0 Offline GATEWAYS) ▼

Networks

Networks			
NAME	TYPE	SECURITY	ACCESS TYPE
Familia Bolivar2	employee	wpa2-psk-aes	unrestricted
wired-SetMeUp	guest		network-based
default_wired_port_profile	employee		unrestricted



Set WiFi as Guest

aruba | Central

CURRENT APP
WIRELESS MANAGEMENT

Search Current App
Find devices, clients and networks

Networks
Add and edit networks

Access Points
View APs and set device parameters

RF
Set Aruba Adaptive Radio Management

Wireless IDS/IPS
Manage Intrusion detection and prevention

Security
Set advanced security parameters

FILTER WIRELESS MANAGEMENT
Home CI 159 (3 Total Devices | 1 Offline APs | 0 Offline SWITCHES | 0 Offline GATEWAYS) ▼

Create a New Network

1 General **2 VLANs** **3 Security** **4 Access**

Basic Settings

Name (SSID):


ESSID:

Type: ☒ Wireless ☐ Wired


Primary Usage: ☐ Employee ☒ Guest ☐ Voice

Broadcast/Multicast


Click next



aruba Central



CURRENT APP
WIRELESS MANAGEMENT


 **Search Current App**
Find devices, clients and networks

Networks
Add and edit networks

Access Points
View APs and set device parameters

RF
Set Aruba Adaptive Radio Management

Wireless IDS/IPS
Manage intrusion detection and prevention

 **FILTER WIRELESS MANAGEMENT**
Home CI 159 (3 Total Devices | 1 Offline APs | 0 Offline SWITCHES | 0 Offline GATEWAYS) ▼

Create a New Network

1 General

2 VLANs

3 Security

4 Access

Client IP Assignment

☒ Virtual Controller Assigned

☐ Network Assigned

Client VLAN Assignment

☒ Default

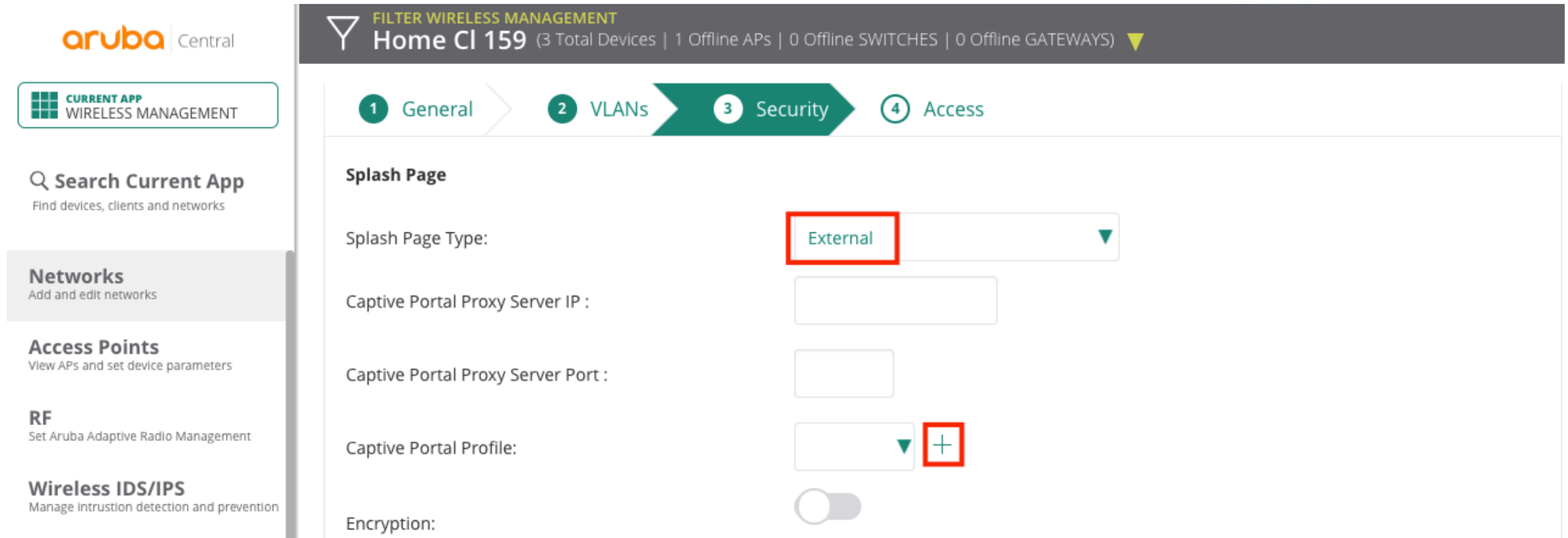
☐ Custom

Cancel

Back

Next

Set Splash Page as External, create new profile



The screenshot displays the Aruba Central management console. On the left is a sidebar with navigation options: 'aruba Central', 'CURRENT APP WIRELESS MANAGEMENT', 'Search Current App', 'Networks', 'Access Points', 'RF', and 'Wireless IDS/IPS'. The main content area is titled 'FILTER WIRELESS MANAGEMENT' and 'Home CI 159'. It features a breadcrumb trail with four steps: '1 General', '2 VLANs', '3 Security' (the active step), and '4 Access'. Under the 'Security' step, the 'Splash Page' configuration is shown. It includes a 'Splash Page Type' dropdown menu set to 'External', two empty input fields for 'Captive Portal Proxy Server IP' and 'Captive Portal Proxy Server Port', a 'Captive Portal Profile' dropdown menu with a '+' icon to add a new profile, and an 'Encryption' toggle switch.

aruba Central

CURRENT APP WIRELESS MANAGEMENT

Search Current App
Find devices, clients and networks

Networks
Add and edit networks

Access Points
View APs and set device parameters

RF
Set Aruba Adaptive Radio Management

Wireless IDS/IPS
Manage intrusion detection and prevention

FILTER WIRELESS MANAGEMENT
Home CI 159 (3 Total Devices | 1 Offline APs | 0 Offline SWITCHES | 0 Offline GATEWAYS)

1 General 2 VLANs 3 Security 4 Access

Splash Page

Splash Page Type: External


Captive Portal Proxy Server IP :


Captive Portal Proxy Server Port :


Captive Portal Profile: +

Encryption: ☐

New Captive portal profile

Central

CURRENT APP
WIRELESS MANAGEMENT

 Search Current App
Find devices, clients and networks


Networks
Add and edit networks

Access Points
View APs and set device parameters

RF
Set Aruba Adaptive Radio Management

Wireless IDS/IPS
Manage intrusion detection and prevention

Security
Set advanced security parameters

 FILTER WIRELESS MANAGEMENT
Home CI 159 (3 Total Devices | 1 Offline APs | 0 Offline SWITCHES | 0 Offline GATEWAYS) ▼

EXTERNAL CAPTIVE PORTAL - NEW

Name:

Purple

Type:

RADIUS Authentication ▼

IP or Hostname:

region1.purpleportal.n

← region1.purpleportal.net

URL:

/access/

Port:

80

Use HTTPS:

☐

Captive Portal Failure:

Deny Internet ▼

Redirect URL:

https://region1.purple

← https://region1.purpleportal.net/access/?res=success

Add Authentication server

The screenshot shows the Aruba Central web interface. On the left is a sidebar with the 'aruba Central' logo and navigation links for 'CURRENT APP WIRELESS MANAGEMENT', 'Search Current App', 'Networks', and 'Access Points'. The main content area has a dark header bar with a funnel icon, the text 'FILTER WIRELESS MANAGEMENT', and a status bar for 'Home CI 159' showing device counts. Below this, the 'Authentication' section features a toggle switch for 'MAC Authentication' and a 'Primary Server' dropdown menu currently set to 'Internal Server'. A red square highlights a '+' icon next to the dropdown. The 'Users' section shows '0 Users' and a 'Manage Users' link. An information icon and a note state: 'Only registered users of type 'Guest' will be able to access this network.'

aruba Central

CURRENT APP
WIRELESS MANAGEMENT

Search Current App
Find devices, clients and networks

Networks
Add and edit networks

Access Points
View APs and set device parameters

Authentication

MAC Authentication: ☐

Primary Server: Internal Server ▼ **+**

Users:

0 Users [Manage Users](#)

i Only registered users of type 'Guest' will be able to access this network.

Enter Primary Server information

arubaCentral

CURRENT APP
WIRELESS MANAGEMENT

Search Current App
Find devices, clients and networks

Networks
Add and edit networks

Access Points
View APs and set device parameters

RF
Set Aruba Adaptive Radio Management

Wireless IDS/IPS
Manage intrusion detection and prevention

Security
Set advanced security parameters

VPN
Manage controller VPN connections

DHCP
Manage DHCP scopes

FILTER WIRELESS MANAGEMENT
Home CI 159 (3 Total Devices | 1 Offline APs | 0 Offline SWITCHES | 0 Offline GATEWAYS)

NEW SERVER

☒ RADIUS☐ LDAP

Name:

PurpleServer

Timeout:

5

sec

IP Address:

54.217.112.62

Retry Count:

3

Shared Key:

.....

NAS IP Address:

optional

Retype Key:

.....

NAS Identifier:

optional

Cancel

↑

6n8!5ETGb^nd

Save

Add Authentication server

The screenshot displays the Aruba Central web interface for configuring authentication servers. The left sidebar contains navigation links for 'aruba Central', 'CURRENT APP WIRELESS MANAGEMENT', 'Search Current App', 'Networks', and 'Access Points'. The main content area is titled 'Home CI 159' and includes a status bar with device counts. Under the 'Authentication' section, there is a toggle switch for 'MAC Authentication' and dropdown menus for 'Primary Server' (set to 'PurpleServer') and 'Secondary Server' (set to '-- Select --'). A red square highlights a plus icon next to the 'Secondary Server' dropdown, indicating where to click to add a new server. An 'Accounting' section with a plus icon is also visible at the bottom.

aruba Central

CURRENT APP
WIRELESS MANAGEMENT

Search Current App
Find devices, clients and networks

Networks
Add and edit networks

Access Points
View APs and set device parameters

FILTER WIRELESS MANAGEMENT
Home CI 159 (3 Total Devices | 1 Offline APs | 0 Offline SWITCHES | 0 Offline GATEWAYS)

Authentication

MAC Authentication: ☐

Primary Server: PurpleServer ▼ +

Secondary Server: -- Select -- ▼ **+**

Accounting +

Enter Secondary Server information

arubaCentral

CURRENT APP
WIRELESS MANAGEMENT

Search Current App
Find devices, clients and networks

Networks
Add and edit networks

Access Points
View APs and set device parameters

RF
Set Aruba Adaptive Radio Management

Wireless IDS/IPS
Manage intrusion detection and prevention

Security
Set advanced security parameters

VPN
Manage controller VPN connections

DHCP
Manage DHCP scopes

FILTER WIRELESS MANAGEMENT
Home CI 159 (3 Total Devices | 1 Offline APs | 0 Offline SWITCHES | 0 Offline GATEWAYS)

NEW SERVER

☒ RADIUS☐ LDAP

Name:

PurpleServer2

Timeout:

5

sec

IP Address:

176.34.118.13

Retry Count:

3

Shared Key:

.....

NAS IP Address:

optional

Retype Key:

.....

NAS Identifier:


optional

Cancel


6n8!5ETGb^nd

Save

Enable Accounting



Central



CURRENT APP
WIRELESS MANAGEMENT

Search Current App

Find devices, clients and networks

Networks

Add and edit networks

Access Points

View APs and set device parameters

RF

Set Aruba Adaptive Radio Management

Wireless IDS/IPS

Manage Intrusion detection and prevention

Security




Set advanced security parameters


VPN

Manage controller VPN connections


DHCP

Manage DHCP scopes





FILTER WIRELESS MANAGEMENT
Home CI 159 (3 Total Devices | 1 Offline APs | 0 Offline SWITCHES | 0 Offline GATEWAYS) ▼



Accounting

ACCOUNTING:


Accounting Mode:

Accounting Interval:


Use authentication servers ▼

Authentication ▼


3 Min



Walled Garden



Disable if uplink type is



Advanced

Reauth Interval:

24

hrs ▼


Blacklisting:

Enforce DHCP:


Use IP for Calling Station ID :

Need Help? ^


Add whitelist sites



Central



CURRENT APP
WIRELESS MANAGEMENT

 Search Current App

Find devices, clients and networks

Networks

Add and edit networks

Access Points

View APs and set device parameters

RF

Set Aruba Adaptive Radio Management

Wireless IDS/IPS

Manage intrusion detection and prevention

Security


Set advanced security parameters

VPN

Manage controller VPN connections


DHCP

Manage DHCP scopes

 FILTER WIRELESS MANAGEMENT


Home CI 159 (3 Total Devices | 1 Offline APs | 0 Offline SWITCHES | 0 Offline GATEWAYS) ▼

⊖ Walled Garden



Blacklist

BLACKLIST




No data to display


+


Whitelist


WHITELIST




No data to display




 Disable if uplink type is

 Advanced

Whitelist domains



aruba Central



CURRENT APP
WIRELESS MANAGEMENT

Search Current App

Find devices, clients and networks

Networks

Add and edit networks

Access Points

View APs and set device parameters

RF


Set Aruba Adaptive Radio Management


Wireless IDS/IPS


Manage Intrusion detection and prevention


Security

Set advanced security parameters


 FILTER WIRELESS MANAGEMENT


Home CI 159 (3 Total Devices | 1 Offline APs | 0 Offline SWITCHES | 0 Offline GATEWAYS) 

 Walled Garden




Blacklist


BLACKLIST 



No data to display



Whitelist

WHITELIST 


region1.purpleportal.net

cloudfront.net

openweathermap.org

venuewifi.com

stripe.com



Role Based Access

aruba Central

CURRENT APP
WIRELESS MANAGEMENT

Search Current App
Find devices, clients and networks

Networks
Add and edit networks

Access Points
View APs and set device parameters

RF
Set Aruba Adaptive Radio Management

Wireless IDS/IPS
Manage intrusion detection and prevention

Security
Set advanced security parameters

VPN
Manage controller VPN connections

FILTER WIRELESS MANAGEMENT
Home CI 159 (3 Total Devices | 1 Offline APs | 0 Offline SWITCHES | 0 Offline GATEWAYS)

Create a New Network

1 General 2 VLANs 3 Security 4 Access

Access Rules:

☒ Role Based ☐ Network Based ☐ Unrestricted

Roles

ROLE
Familia Bolivar2
default_wired_port_...
wired-SetMeUp

Access Rules For Selected Roles

- Allow any to all destinations

+

+

Enter new Role

The screenshot displays the Aruba Central web interface. On the left is a sidebar with navigation options: 'aruba Central', 'CURRENT APP WIRELESS MANAGEMENT', 'Search Current App' (Find devices, clients and networks), 'Networks' (Add and edit networks), 'Access Points' (View APs and set device parameters), 'RF' (Set Aruba Adaptive Radio Management), and 'Wireless IDS/IPS' (Manage intrusion detection and prevention). The main header area shows a filter icon, 'FILTER WIRELESS MANAGEMENT', and 'Home CI 159 (3 Total Devices | 1 Offline APs | 0 Offline SWITCHES | 0 Offline GATEWAYS)'. A modal dialog titled 'ADD ROLE' is open, featuring a close button (X) in the top right. Inside the dialog, the 'Roles:' label is followed by a text input field containing 'PreAuth'. At the bottom of the dialog are 'Cancel' and 'OK' buttons. Below the dialog, a list of roles is partially visible, including 'default_wired_port_...' and 'wired-SetMeUp', with a green plus icon at the bottom left for adding new roles.

aruba Central

CURRENT APP WIRELESS MANAGEMENT

Search Current App
Find devices, clients and networks

Networks
Add and edit networks

Access Points
View APs and set device parameters

RF
Set Aruba Adaptive Radio Management

Wireless IDS/IPS
Manage intrusion detection and prevention

FILTER WIRELESS MANAGEMENT
Home CI 159 (3 Total Devices | 1 Offline APs | 0 Offline SWITCHES | 0 Offline GATEWAYS)

ADD ROLE

Roles: PreAuth

Cancel OK

default_wired_port_...

wired-SetMeUp

+

Add rules for PreAuth Role

The screenshot shows the Aruba Central interface for configuring wireless management. The left sidebar contains navigation links: **aruba** Central, **CURRENT APP WIRELESS MANAGEMENT**, **Search Current App** (Find devices, clients and networks), **Networks** (Add and edit networks), **Access Points** (View APs and set device parameters), **RF** (Set Aruba Adaptive Radio Management), **Wireless IDS/IPS** (Manage Intrusion detection and prevention), and **Security** (Set advanced security parameters).

The main content area is titled **FILTER WIRELESS MANAGEMENT Home CI 159** (3 Total Devices | 1 Offline APs | 0 Offline SWITCHES | 0 Offline GATEWAYS). It features a navigation bar with four tabs: **1 General**, **2 VLANs**, **3 Security**, and **4 Access** (which is highlighted).

Under the **Access** tab, the **Access Rules** section shows a slider and three radio buttons: **Role Based** (selected), **Network Based**, and **Unrestricted**. Below this, the **Roles** table lists the following roles:

ROLE
wired-SetMeUp
Guest
PreAuth

To the right of the roles table, the **Access Rules For Selected Roles** section shows a list of rules. The first rule is **Allow any to all destinations**, which has edit and delete icons. Below this list, a red box highlights a **+** icon, indicating where to click to add a new rule.

Add domain names

arubaCentral

CURRENT APP
WIRELESS MANAGEMENT

Search Current App
Find devices, clients and networks

Networks
Add and edit networks

Access Points
View APs and set device parameters

RF
Set Aruba Adaptive Radio Management

Wireless IDS/IPS
Manage intrusion detection and prevention

Security
Set advanced security parameters

VPN
Manage controller VPN connections

FILTER WIRELESS MANAGEMENT
Home CI 159 (3 Total Devices | 1 Offline APs | 0 Offline SWITCHES | 0 Offline GATEWAYS)

ACCESS RULE

Rule Type:
Access Control

Service:
☒ Network
☐ App Category
☐ Application
☐ Web Category
☐ Web Reputation

Any

Destination:
To a Domain Name

Domain Name:
region1.purpleportal.net

Options:
Cancel

Allow

region1.purpleportal.net

Save

Add rules for PreAuth Role

aruba Central

CURRENT APP
WIRELESS MANAGEMENT

Search Current App
Find devices, clients and networks

Networks
Add and edit networks

Access Points
View APs and set device parameters

RF
Set Aruba Adaptive Radio Management

Wireless IDS/IPS
Manage intrusion detection and prevention

Security
Set advanced security parameters

FILTER WIRELESS MANAGEMENT
Home CI 159 (3 Total Devices | 1 Offline APs | 0 Offline SWITCHES | 0 Offline GATEWAYS)

1 General **2 VLANs** **3 Security** **4 Access**

Access Rules:

Role Based Network Based Unrestricted

Roles

ROLE
wired-SetMeUp
Guest
PreAuth

Access Rules For Selected Roles

Allow any on domain region1.purpleportal.net	^	v	edit	delete
Allow any on domain cloudfront.net	^	v	edit	delete
Allow any on domain instagram.com	^	v	edit	delete
Allow any on domain venuewifi.com	^	v	edit	delete
Allow any on domain stripe.com	^	v	edit	delete
Deny any to all destinations	^	v	edit	delete


Define pre-authentication role as PreAuth


The screenshot shows the Aruba Central interface for configuring a pre-authentication role. The left sidebar contains navigation options: **aruba Central**, **CURRENT APP WIRELESS MANAGEMENT**, **Search Current App** (Find devices, clients and networks), **Networks** (Add and edit networks), **Access Points** (View APs and set device parameters), **RF** (Set Aruba Adaptive Radio Management), **Wireless IDS/IPS** (Manage intrusion detection and prevention), **Security** (Set advanced security parameters), **VPN** (Manage controller VPN connections), and **DHCP** (Manage DHCP scopes).


The main content area is titled **FILTER WIRELESS MANAGEMENT Home CI 159** (3 Total Devices | 1 Offline APs | 0 Offline SWITCHES | 0 Offline GATEWAYS). It displays a list of roles: **Guest** and **PreAuth**. Below the roles is a **Role Assignment Rules** section. The **ROLE ASSIGNMENT RULES** table shows a **Default role: Guest**. Below this, the **ASSIGN PRE-AUTHENTICATION ROLE:** section features a dropdown menu with a checkmark icon and the text **PreAuth**, which is highlighted with a red box.

At the bottom right, there are three buttons: **Cancel**, **Back**, and **Finish**. The **Finish** button is highlighted with a red box.

Guest WiFi Network ready



CURRENT APP
WIRELESS MANAGEMENT

 **Search Current App**
Find devices, clients and networks


Networks
Add and edit networks

Access Points
View APs and set device parameters

RF
Set Aruba Adaptive Radio Management

Wireless IDS/IPS
Manage intrusion detection and prevention

Security
Set advanced security parameters

 **FILTER WIRELESS MANAGEMENT**
Home CI 159 (3 Total Devices | 1 Offline APs | 0 Offline SWITCHES | 0 Offline GATEWAYS) ▼

Networks

Networks			
NAME	TYPE	SECURITY	ACCESS TYPE
Guest	guest	open system	role-based
Familia Bolivar2	employee	wpa2-psk-aes	unrestricted
wired-SetMeUp	guest		network-based
default_wired_port_profile	employee		unrestricted

Add speed limit rule to 1Mbps

The screenshot shows the Aruba Central interface for managing wireless devices. The left sidebar contains navigation links for various management areas. The main content area is titled 'Home CI 159' and shows a list of roles. The 'Guest' role is selected, and the 'Access Rules For Selected Roles' panel is open, showing a single rule 'Allow any to all destinations'. A red box highlights a '+' button in the 'Access Rules' panel, indicating where to click to add a new rule.

aruba Central

CURRENT APP
WIRELESS MANAGEMENT

Search Current App
Find devices, clients and networks

Networks
Add and edit networks

Access Points
View APs and set device parameters

RF
Set Aruba Adaptive Radio Management

Wireless IDS/IPS
Manage intrusion detection and prevention

Security
Set advanced security parameters

VPN
Manage controller VPN connections

FILTER WIRELESS MANAGEMENT
Home CI 159 (3 Total Devices | 1 Offline APs | 0 Offline SWITCHES | 0 Offline GATEWAYS)

> Authentication Servers

> User For Internal Server

✓ Roles

Roles
ROLE
Familia Bolivar2
Guest
PreAuth
default_wired_port_pr...
wired-SetMeUp

+

Access Rules For Selected Roles

● Allow any to all destinations

+

Speed limit rule -> 1Mbps


The image shows the Aruba Central web interface. On the left is a sidebar with navigation links: **aruba** Central, **CURRENT APP WIRELESS MANAGEMENT**, **Search Current App** (Find devices, clients and networks), **Networks** (Add and edit networks), **Access Points** (View APs and set device parameters), **RF** (Set Aruba Adaptive Radio Management), **Wireless IDS/IPS** (Manage intrusion detection and prevention), **Security** (Set advanced security parameters), and **VPN** (Manage controller VPN connections).


The main content area has a header **FILTER WIRELESS MANAGEMENT** and a sub-header **Home CI 159** (3 Total Devices | 1 Offline APs | 0 Offline SWITCHES | 0 Offline GATEWAYS). Below this is a modal window titled **ACCESS RULE** with a close button (X). The modal contains three sections, each highlighted with a red box:


- Rule Type:** A dropdown menu showing **Bandwidth Cor** with a downward arrow.
- Service:** Two input fields: **Downstream:** 1000 Kbps and **Upstream:** 1000 Kbps.
- BANDWIDTH CONTRACT:** Two checkboxes, both checked, labeled **Per User**.

At the bottom of the modal are **Cancel** and **Save** buttons. Below the modal, a list of items is visible: **PreAuth**, **default_wired_port_pr...**, and **wired-SetMeUp**, with a plus sign (+) at the bottom.

Rule limit applied



 CURRENT APP
WIRELESS MANAGEMENT

 Search Current App
Find devices, clients and networks

Networks
Add and edit networks

Access Points
View APs and set device parameters

RF
Set Aruba Adaptive Radio Management




Wireless IDS/IPS
Manage intrusion detection and prevention


Security
Set advanced security parameters

VPN
Manage controller VPN connections

DHCP
Manage DHCP scopes

Services
Enable additional Central services


 FILTER WIRELESS MANAGEMENT
Home CI 159 (3 Total Devices | 1 Offline APs | 0 Offline SWITCHES | 0 Offline GATEWAYS) ▼

> Authentication Servers

> User For Internal Server

▼ Roles

Roles

ROLE	
Familia Bolivar2	
Guest	
PreAuth	
default_wired_port_pr...	
wired-SetMeUp	

+

> Blacklisting

> Firewall Settings

Access Rules For Selected Roles

→ Bandwidth Contract: upstream 1000 kbps (peruser) downstream 1000 kbps (peruser)

● Allow any to all destinations

+

Need Help? ▲

Cancel

Save Settings

Take note of MAC Address

The screenshot displays the Aruba Central web interface for monitoring a specific device, 'Home CI 159'. The interface is divided into a left sidebar with navigation options and a main content area with detailed device and network information.

Left Sidebar:

- aruba Central**
- CURRENT APP MONITORING & REPORTS**
- Search Current App** (Find devices, clients and networks)
- Network Overview** (View Aruba device performance and security)
- Network Health** (View potential network issues)
- Clients** (View clients list)
- Client Overview** (View detailed information on connected clients)
- Application Visibility** (View application and website usage)
- VisualRF** (RF Heatmaps)

Main Content Area:

Header: FILTER MONITORING & REPORTS | Home CI 159 (3 Total Devices | 1 Offline APs | 0 Offline SWITCHES | 0 Offline GATEWAYS) | TEMPORAL FILTER 3 HOURS

Summary Row:

- Access Points:** Tenerife AP305, No downtime in the last 16 days
- DEVICE HEALTH:** Good
- RADIO 0 (5 GHz):** Good
- RADIO 1 (2.4 GHz):** Good
- VIRTUAL CONTROLLER:** VC Tenerife

Tabs: OVERVIEW (selected), USAGE, CLIENTS, RF, VPN, LOCATION, EVENTS, GO LIVE

DEVICE INFORMATION:

AP MODEL	COUNTRY CODE
AP-305	CO

MAC	SERIAL NUMBER
24:f[redacted]	CN[redacted]

FIRMWARE VERSION	CONFIGURATION STATUS
8.3.0.0_64659 Last Updated on May 21 2018 13:08:56	Unsynchronized Last Config Changed on Jan 14 2019 10:51:02

UPTIME	GROUP
16 Days 2 Hours	Home CI 159

LABEL	SITE
Home	Bogota

NETWORK INFORMATION:

ETH 0	SPEED (Mbps) / DUPLEX	IP ADDRESS
Up	Auto / Auto	192[redacted]

CURRENT UPLINK	UPLINK STATUS
Ethernet	Up

IP ADDRESS	PUBLIC IP ADDRESS
192[redacted]	18[redacted]

DNS NAME SERVERS	IPv4 DEFAULT GATEWAY
192[redacted]	192[redacted]



a Hewlett Packard
Enterprise company









Task: Setup Purple Dashboard

Enter <https://purple.ai/get-started/smb/> and complete the form








purple


The perfect WiFi solution for growing businesses
Purple SMB

Fields marked with an * are required

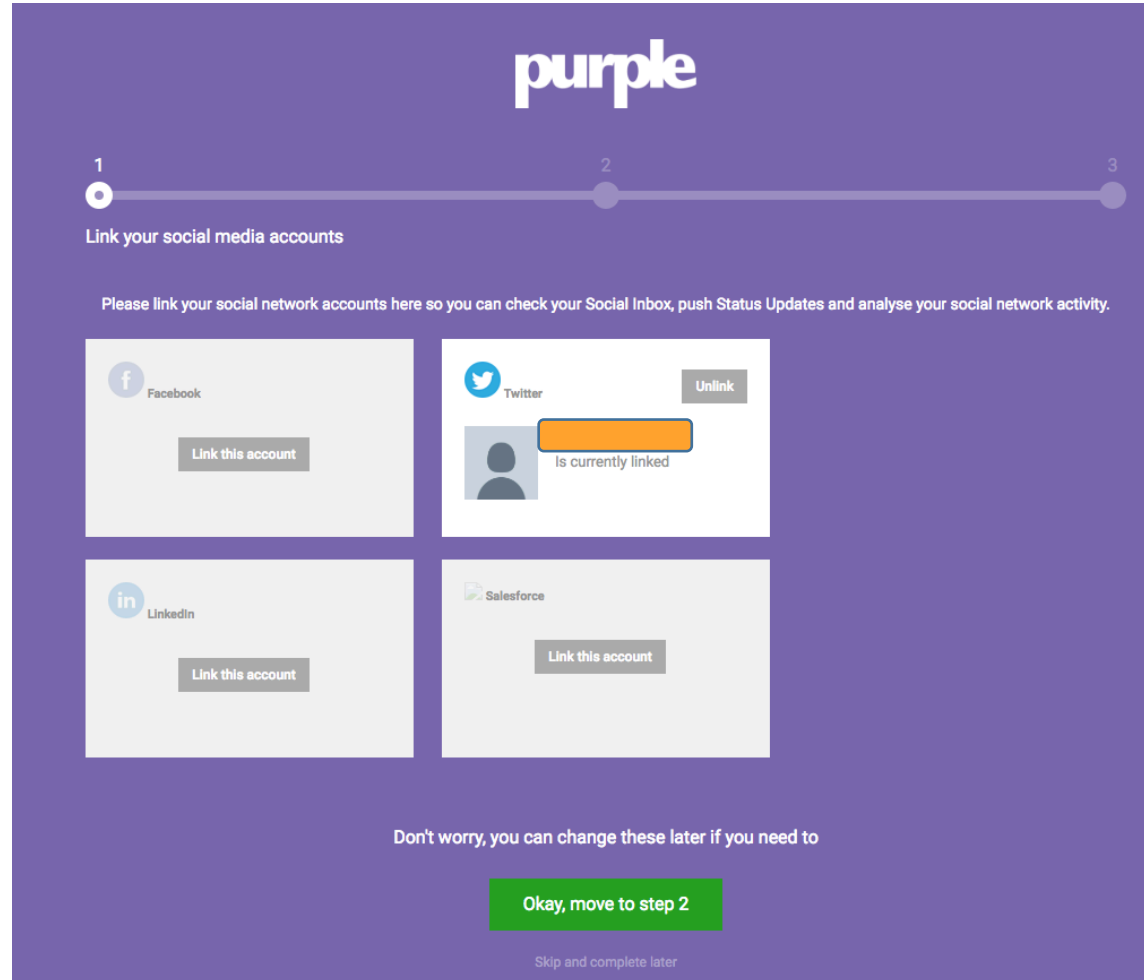
 CC	 IE
 ccied <input type="text" value="ccied@purple.ai"/> 	 <input type="text" value="571 234 5678"/> 
 Own	 IT

About your Venue

 Home		
 <input type="text" value="Bogota"/>	 Bogota	
 <input type="text" value="Bogota"/>	Colombia	
Services 	1 - 5	

 [Get Started](#)

Link the account to your social media

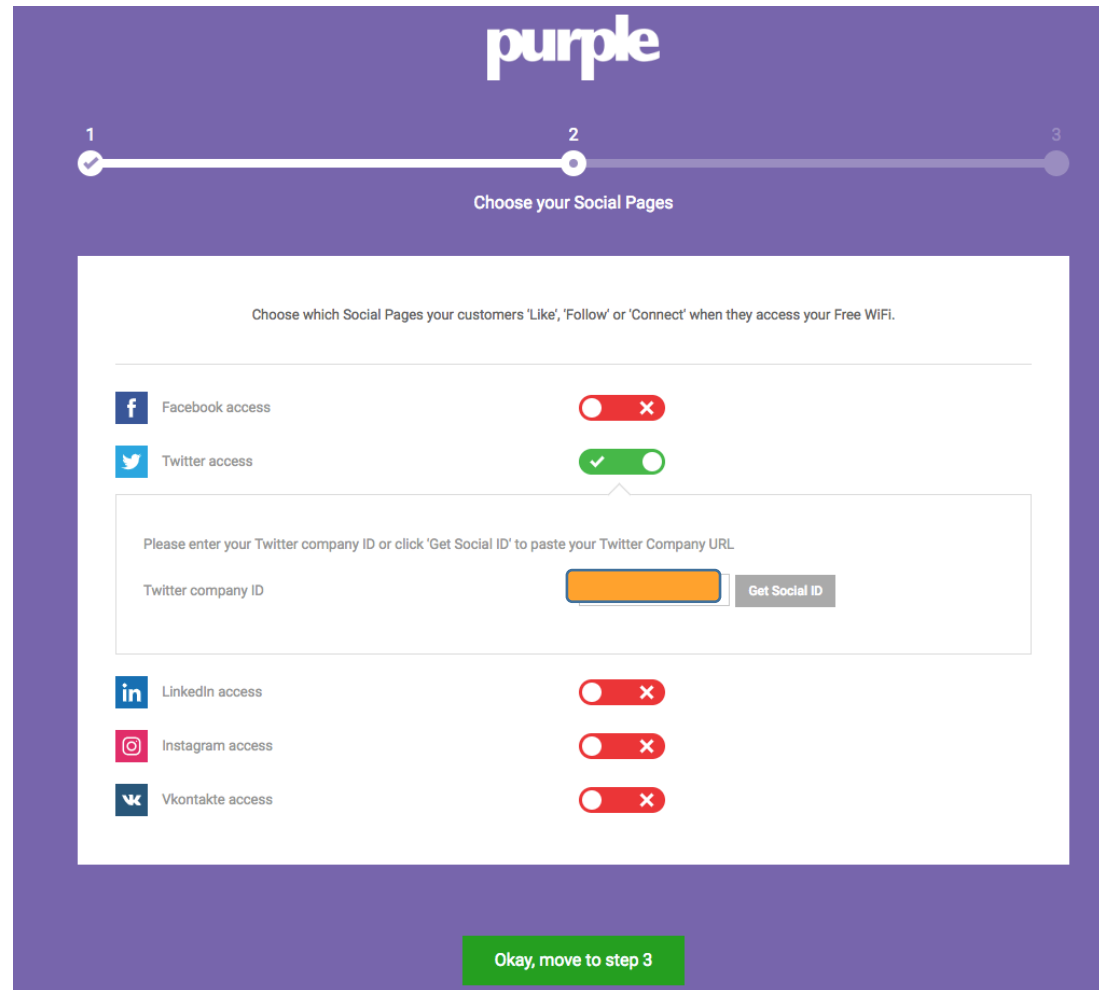


The screenshot shows the 'purple' app interface for linking social media accounts. At the top, a progress bar with three steps is shown, with step 1 'Link your social media accounts' being the current step. Below the progress bar, a message states: 'Please link your social network accounts here so you can check your Social Inbox, push Status Updates and analyse your social network activity.' There are four account linking options arranged in a 2x2 grid:

- Facebook:** A light gray box with the Facebook 'f' logo, the text 'Facebook', and a 'Link this account' button.
- Twitter:** A white box with the Twitter bird logo, the text 'Twitter', an 'Unlink' button, a placeholder profile picture, and the text 'Is currently linked'.
- LinkedIn:** A light gray box with the LinkedIn 'in' logo, the text 'LinkedIn', and a 'Link this account' button.
- Salesforce:** A light gray box with the Salesforce logo, the text 'Salesforce', and a 'Link this account' button.

At the bottom of the screen, there is a message: 'Don't worry, you can change these later if you need to'. Below this message are two buttons: a green 'Okay, move to step 2' button and a smaller, faint 'Skip and complete later' link.

Click move to step 3



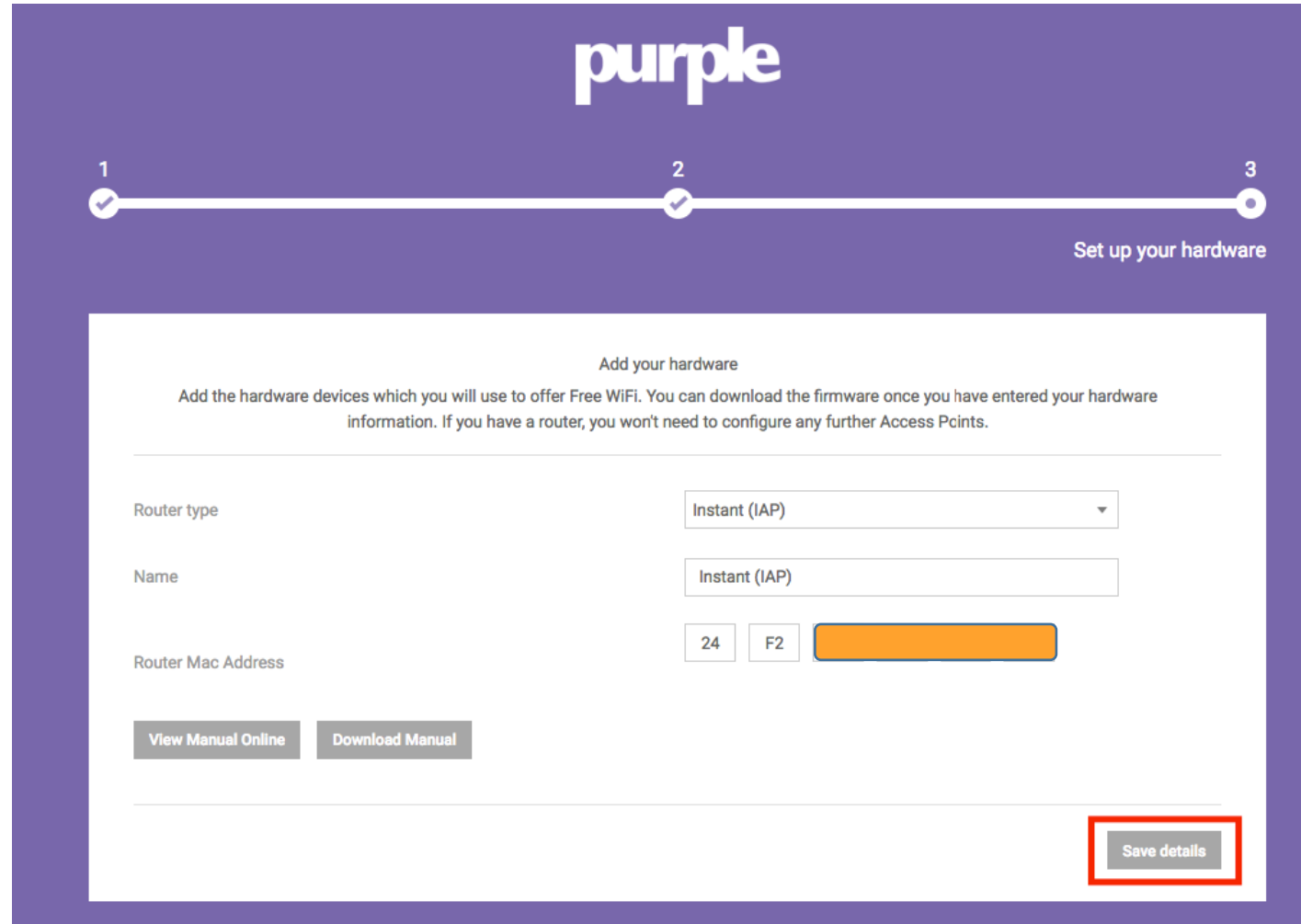
The screenshot shows a purple-themed interface for configuring a WiFi network. At the top, the 'purple' logo is displayed. Below it, a progress bar with three steps is shown: Step 1 is completed (marked with a checkmark), Step 2 is the current step (marked with a circle), and Step 3 is the next step (marked with a circle). The title 'Choose your Social Pages' is centered below the progress bar. The main content area has a heading: 'Choose which Social Pages your customers 'Like', 'Follow' or 'Connect' when they access your Free WiFi.' Below this heading, there are five social media options, each with a toggle switch and a red 'X' icon:

- Facebook access: Toggle switch is off (red).
- Twitter access: Toggle switch is on (green) with a white checkmark.
- LinkedIn access: Toggle switch is off (red).
- Instagram access: Toggle switch is off (red).
- Vkontakte access: Toggle switch is off (red).

Below the Twitter access toggle, there is a text input field labeled 'Twitter company ID' and a button labeled 'Get Social ID'. The text above the input field reads: 'Please enter your Twitter company ID or click 'Get Social ID' to paste your Twitter Company URL.'

At the bottom of the screen, there is a green button labeled 'Okay, move to step 3'.

Add MAC Address of AP



The screenshot shows the 'purple' logo at the top. Below it is a progress bar with three steps: 1 (checked), 2 (checked), and 3 (active). The text 'Set up your hardware' is positioned to the right of the progress bar. The main content area is titled 'Add your hardware' and contains instructions: 'Add the hardware devices which you will use to offer Free WiFi. You can download the firmware once you have entered your hardware information. If you have a router, you won't need to configure any further Access Points.' Below this, there are three input fields: 'Router type' (a dropdown menu showing 'Instant (IAP)'), 'Name' (a text field showing 'Instant (IAP)'), and 'Router Mac Address' (a field with '24' and 'F2' in separate boxes, followed by an orange input box). At the bottom left are two buttons: 'View Manual Online' and 'Download Manual'. At the bottom right, the 'Save details' button is highlighted with a red rectangle.

purple

1 2 3

Set up your hardware

Add your hardware

Add the hardware devices which you will use to offer Free WiFi. You can download the firmware once you have entered your hardware information. If you have a router, you won't need to configure any further Access Points.

Router type Instant (IAP)

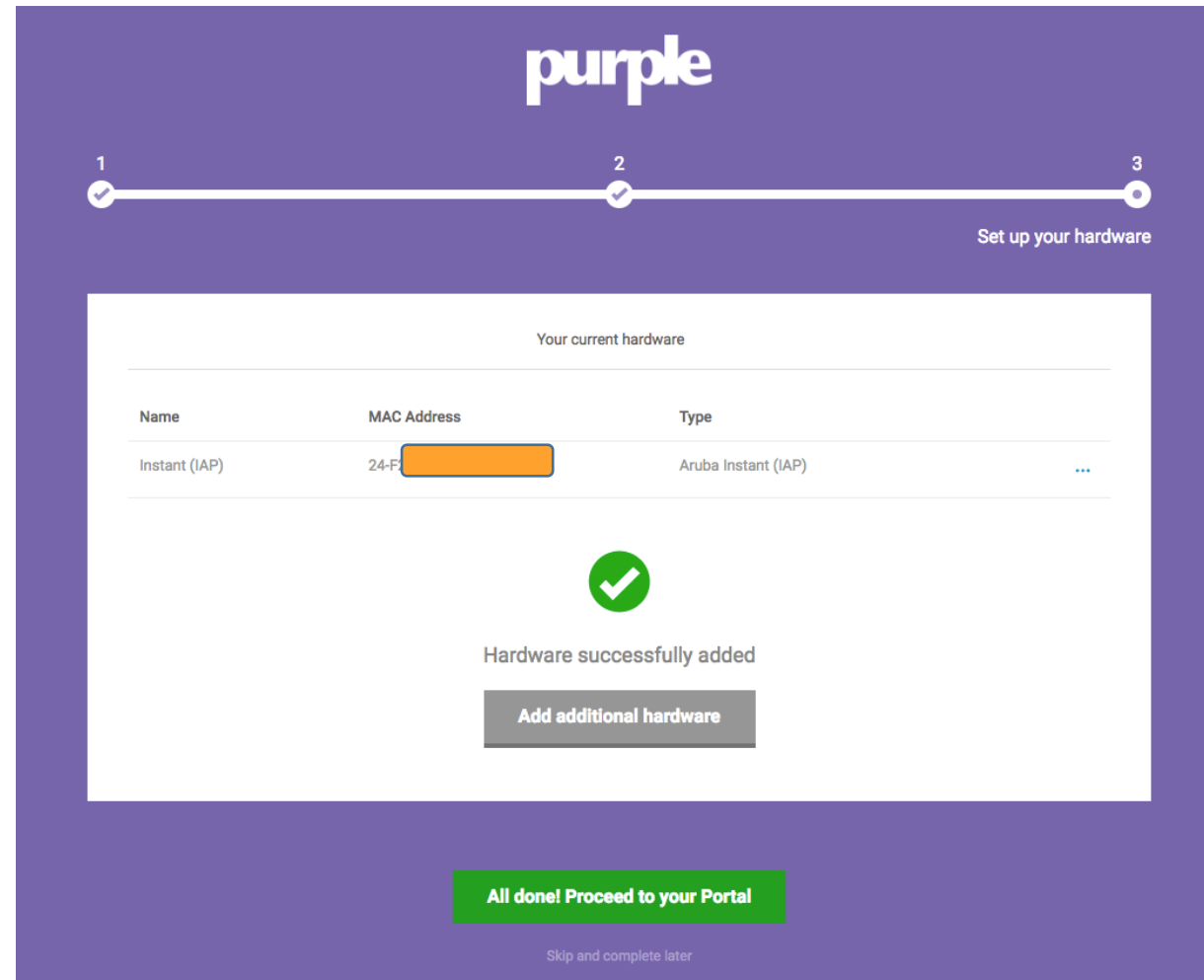
Name Instant (IAP)

Router Mac Address 24 F2

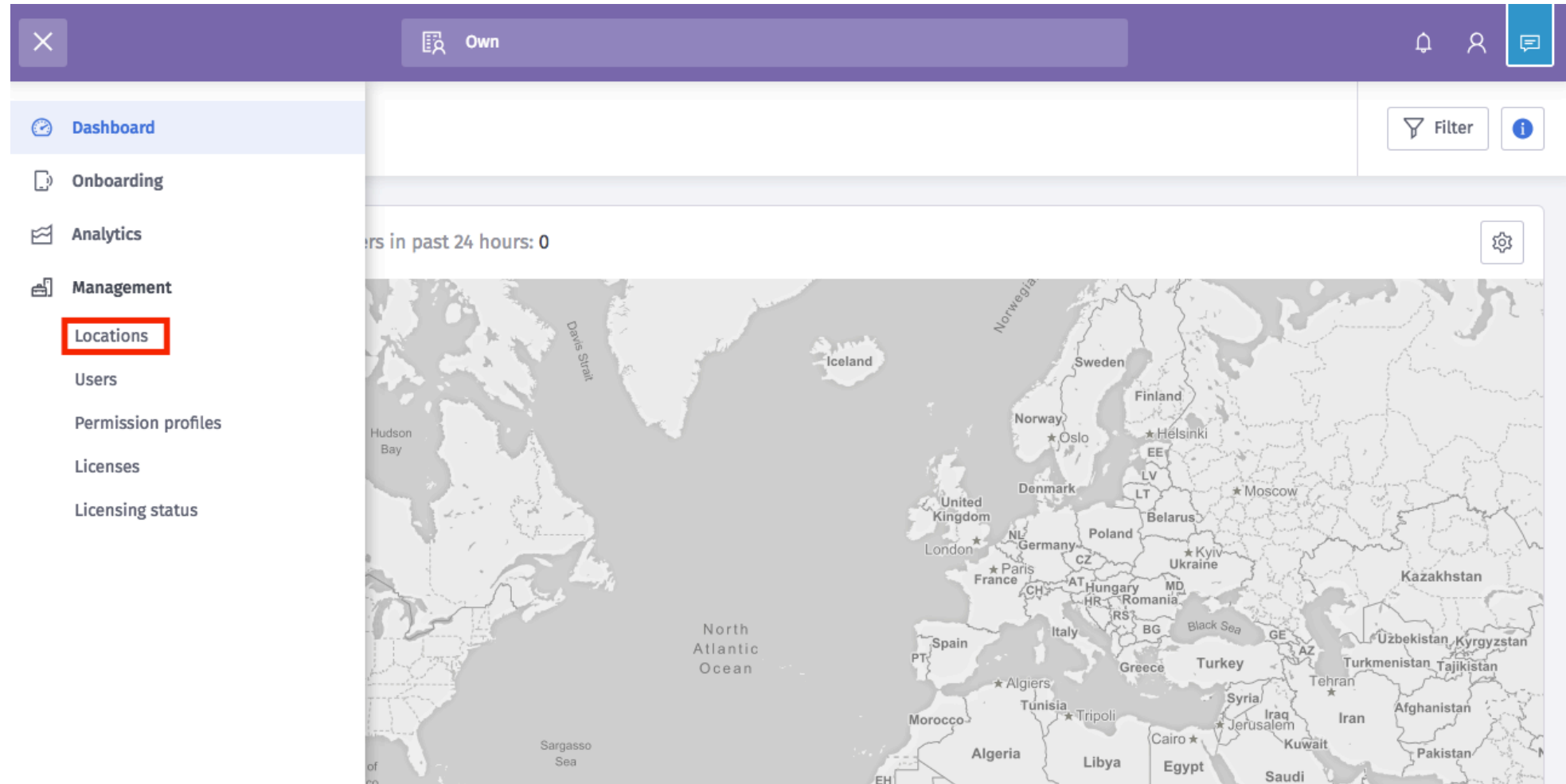
View Manual Online Download Manual

Save details

Dashboard created



Click on Locations



Click on Venues

Own

Venues and Groups Details Settings Tiered Bandwidth Webhooks

Own

Impersonate Save changes i

+

-

Q

Nicaragua

Costa Rica

Panama

Medellín

Bogotá

Colombia

Venezuela

Caracas

Curaçao

Grenada

Trinidad and Tobago

Georgetown

Paramaribo

Guyana

Suriname

French Guiana

Roraima

Amapá

Belém

Manaus

Quito

Ecuador

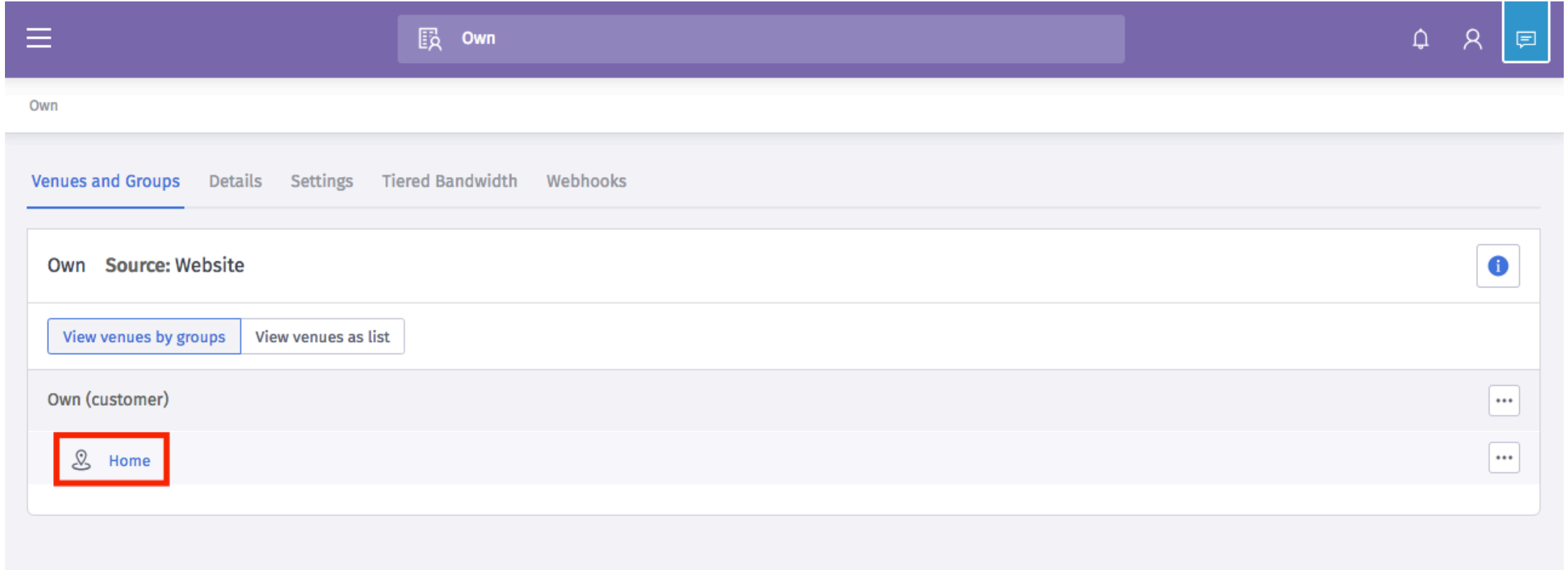
Terra Indígena Alto Rio Negro

Galápagos Marine Reserve

Barbados

Lat: 4.570868 Long: -74.297333

Click on “Home” venue




The screenshot shows a web application interface with a purple header bar. On the left of the header is a hamburger menu icon. In the center is a search bar with a magnifying glass icon and the text "Own". On the right are icons for a bell, a user profile, and a chat bubble. Below the header, the word "Own" is displayed. A navigation bar contains links for "Venues and Groups" (which is underlined), "Details", "Settings", "Tiered Bandwidth", and "Webhooks". The main content area shows a section titled "Own Source: Website" with an information icon. Below this are two buttons: "View venues by groups" and "View venues as list". A list of venues follows, starting with "Own (customer)" and an ellipsis menu. The next item is "Home", which is highlighted with a red rectangular box and includes a location pin icon and an ellipsis menu.

Own


Own Source: Website


View venues by groups View venues as list




Own (customer)

 Home

Click on Hardware to check MAC Address of AP



 Own




Own / Home



Details **Hardware** Access Methods Linked Networks Settings

Associated hardware

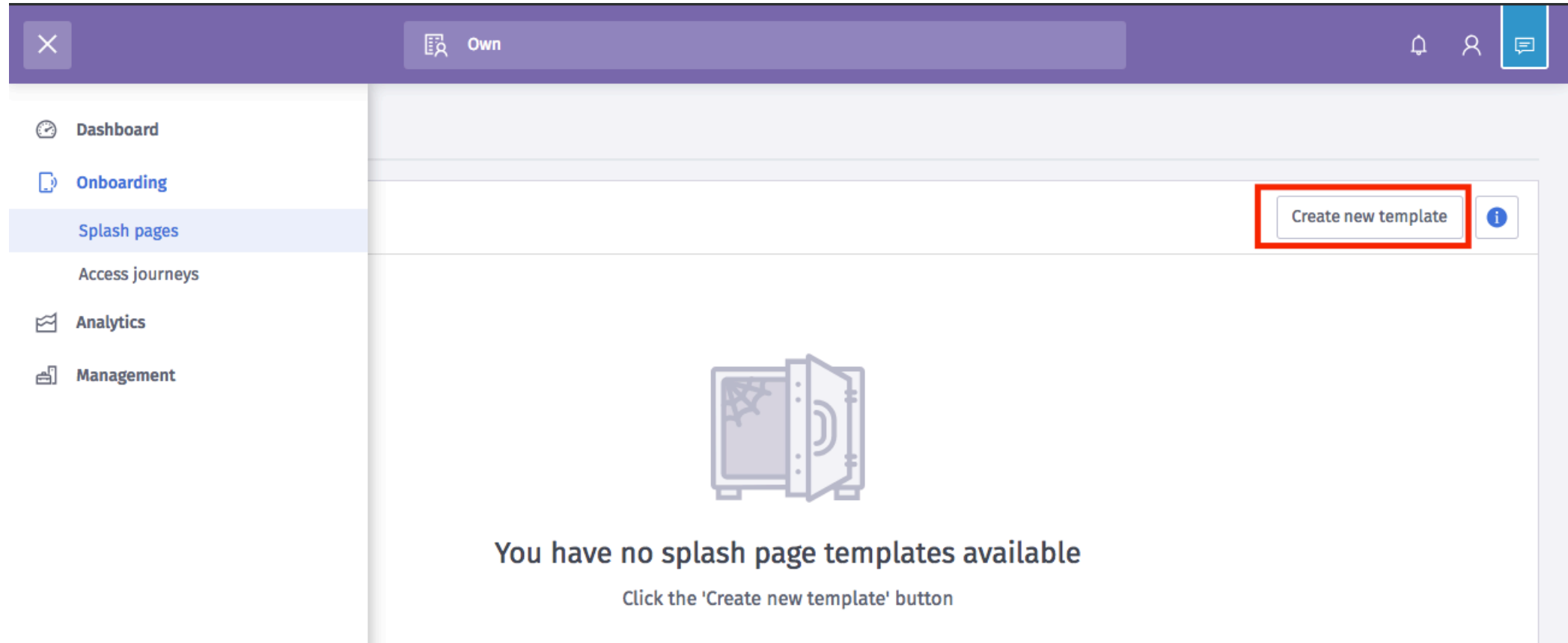
Add hardware

Renew license



Name	MAC	Type	License	Actions
Instant (IAP)	24-F2 	Aruba Instant (IAP)	Free mode	

Click on Splash pages and Create new template



Click on Create New template

The screenshot shows a web application interface with a dark purple header. On the left, there is a sidebar with a menu icon and two tabs: 'Your templates' (active) and 'System templates'. The main content area is titled 'Your templates' and contains a large empty space. A modal dialog box titled 'Create a new template' is open in the center. The dialog has five form fields: 'Name' (text input with 'DemoTemplate'), 'Use' (dropdown with 'Offline'), 'Ownership scope' (dropdown with 'Location'), 'Owned by' (dropdown with 'Home'), and 'Type' (dropdown with 'Standard'). Each dropdown menu has a blue question mark icon to its right. At the bottom right of the dialog, there are two buttons: 'Close' and 'Create New'. The 'Create New' button is highlighted with a red rectangular border. In the background, to the right of the dialog, there is a button labeled 'Create new template' and an information icon.

Create a new template

Name

Use ?

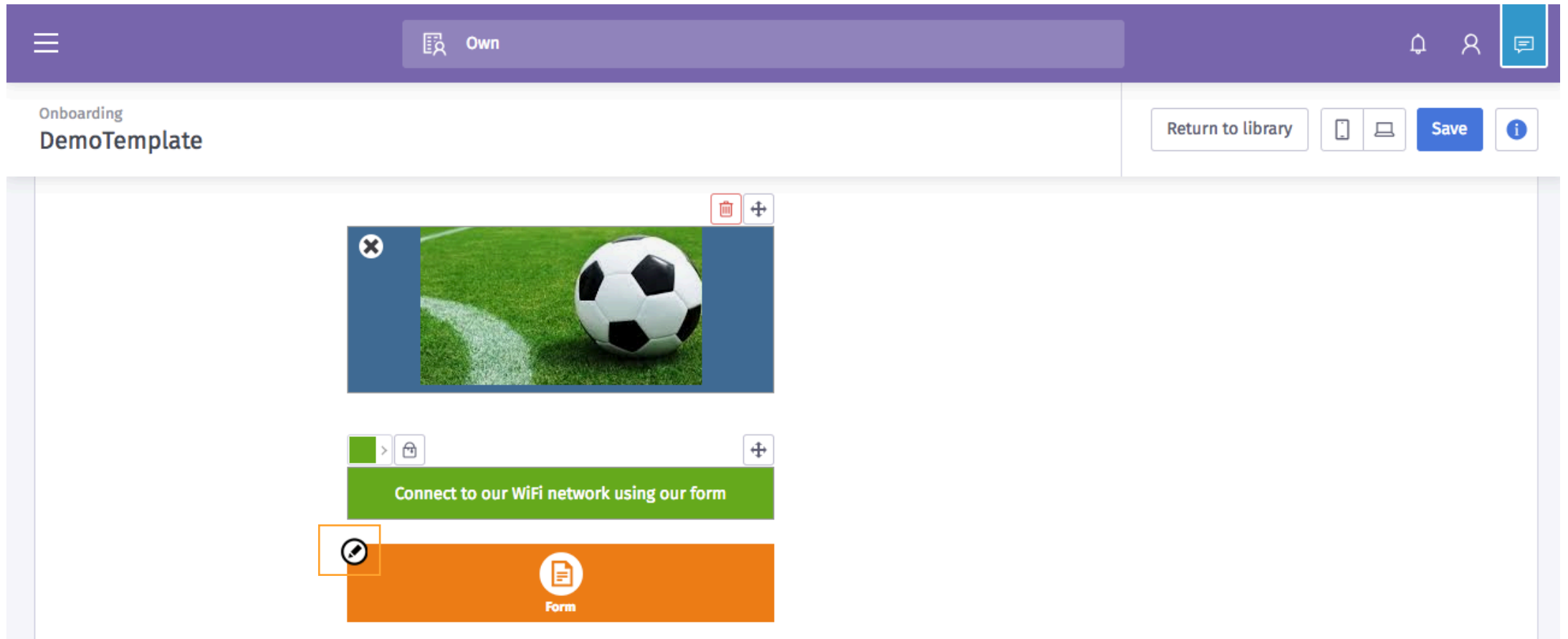
Ownership scope ?

Owned by ?





Type ?

Close **Create New**


Upload images, change colors




Template created

 Own   

[Your templates](#) [System templates](#)

Your templates Create new template 

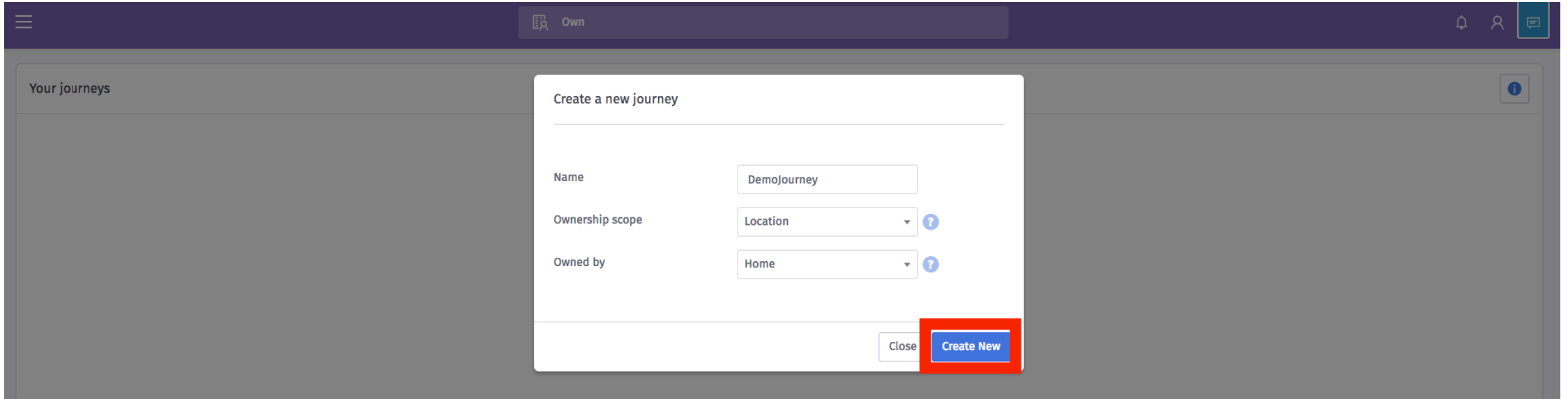
Template name	Language	Created	Type	
DemoTemplate	0	1/14/19 Home (Venue)	Offline Standard	

Click on Access journeys

The screenshot shows a software interface with a purple header bar. On the left is a navigation menu with items: Dashboard, Onboarding, Splash pages, Access journeys (highlighted with a red rectangle), Analytics, and Management. Under Management are sub-items: Locations, Users, Permission profiles, Licenses, and Licensing status. The main area has a search bar labeled 'Own' and a 'Create new template' button. Below is a table with one row of data.

Language	Created	Type
0	1/14/19 Home (Venue)	Offline Standard

Create the new journey



The screenshot shows a software interface with a dark purple header bar. On the left, a sidebar contains the text "Your journeys". The main area is a light gray. A white modal dialog box titled "Create a new journey" is centered. It contains three form fields: "Name" with the value "DemoJourney", "Ownership scope" with a dropdown menu showing "Location", and "Owned by" with a dropdown menu showing "Home". Each dropdown menu has a blue question mark icon to its right. At the bottom right of the dialog, there are two buttons: a "Close" button and a "Create New" button. The "Create New" button is highlighted with a red rectangular border.

Header: Own

Left sidebar: Your journeys

Modal title: Create a new journey

Form fields:

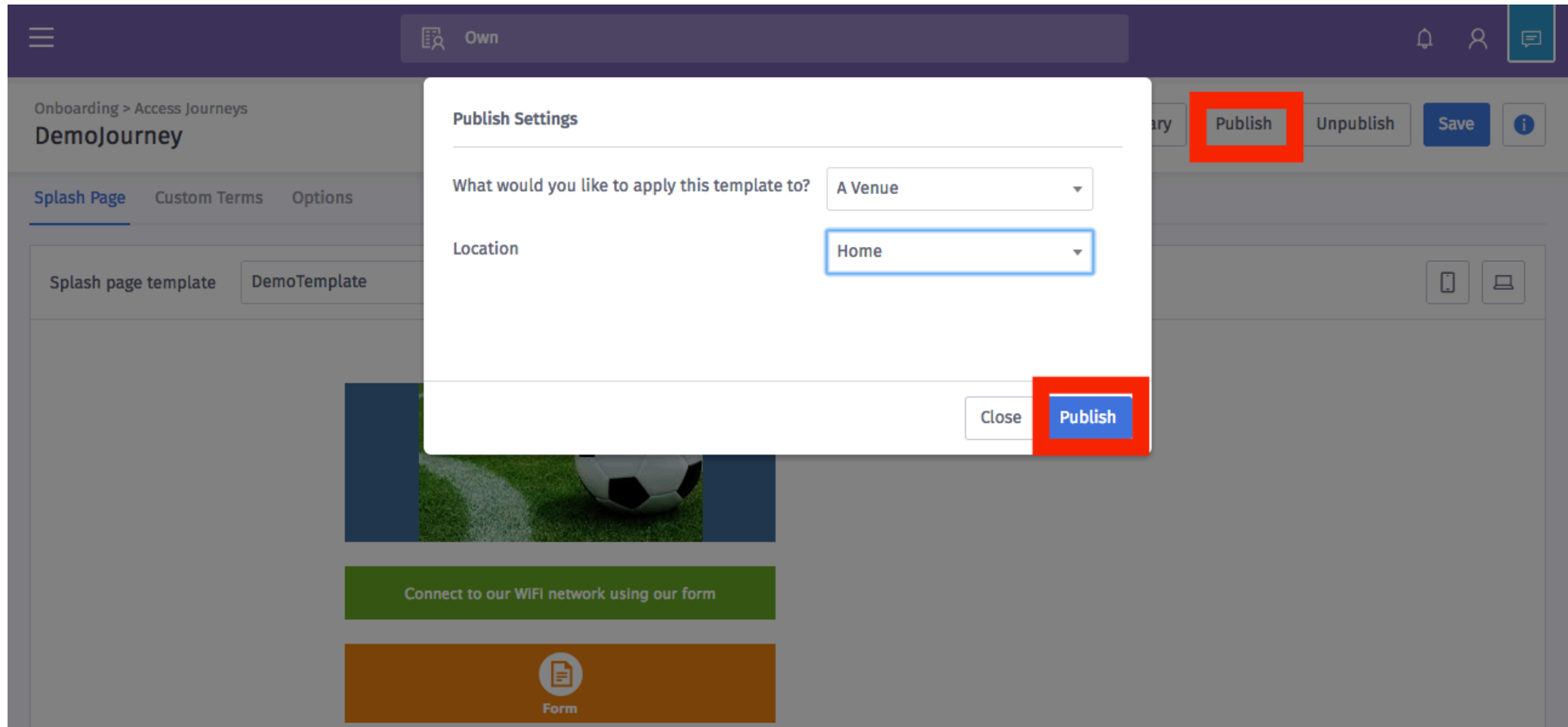
- Name: DemoJourney
- Ownership scope: Location
- Owned by: Home

Buttons: Close, Create New


Select template and then click on save journey


The screenshot displays the Microsoft Access Journeys interface. At the top, a purple header bar contains a menu icon, a search bar with the text 'Own', and notification, user, and chat icons. Below the header, the breadcrumb 'Onboarding > Access Journeys' and the title 'DemoJourney' are visible. To the right of the title are buttons for 'Return to library', 'Publish', 'Unpublish', and 'Save'. The 'Save' button is highlighted with a red box. A dropdown menu is open from the 'Save' button, showing 'Save journey' (highlighted with a red box) and 'Create language version'. Below the header, there are tabs for 'Splash Page', 'Custom Terms', and 'Options'. The 'Splash Page' tab is active. Under this tab, there is a 'Splash page template' dropdown menu with 'DemoTemplate' selected (highlighted with a red box). The main content area shows a preview of the splash page with a soccer ball image, a green button with the text 'Connect to our WiFi network using our form', and an orange button with a document icon and the text 'Form'.




Publish the journey




Journey published





 Own



Your journeys

Create new journey 

Journey name	Splash Page	Created	Published
DemoJourney	DemoTemplate 0 languages	1/14/19 Home (Venue)	<div>PUBLISHED  1</div> 

Go to locations, Home and set timeout to 30min

The screenshot shows the 'Settings' page for a location named 'Home'. The page has a purple header with a menu icon, a search bar containing 'Own', and notification, user, and chat icons. Below the header, a breadcrumb trail shows 'Own / Home'. The main content area has tabs for 'Details', 'Hardware', 'Access Methods', 'Linked Networks', and 'Settings' (which is active). The 'Home' settings section includes a 'Save Options' button in the top right. A red box highlights the 'Custom user timeout' toggle, which is turned on. Below this, the 'Session timeout' is set to '30 minutes' and the 'Idle timeout' is set to '5 minutes', both highlighted by red boxes. At the bottom, there is a 'MAC authentication' toggle (turned off) and an 'Enable Profile Portal' section with 'Inherit' selected from a set of buttons (Disable, Inherit, Enable).

Own / Home

Details Hardware Access Methods Linked Networks **Settings**

Home Save Options

☒ Custom user timeout ?

Session timeout 30 minutes ?

Idle timeout 5 minutes ?

☐ MAC authentication ?

Enable Profile Portal (Inherits: Disabled) Disable **Inherit** Enable ?



a Hewlett Packard
Enterprise company

Task: Test Guest Access

Android phone connected to the Guest SSID

Smartphone in “PreAuth” Role

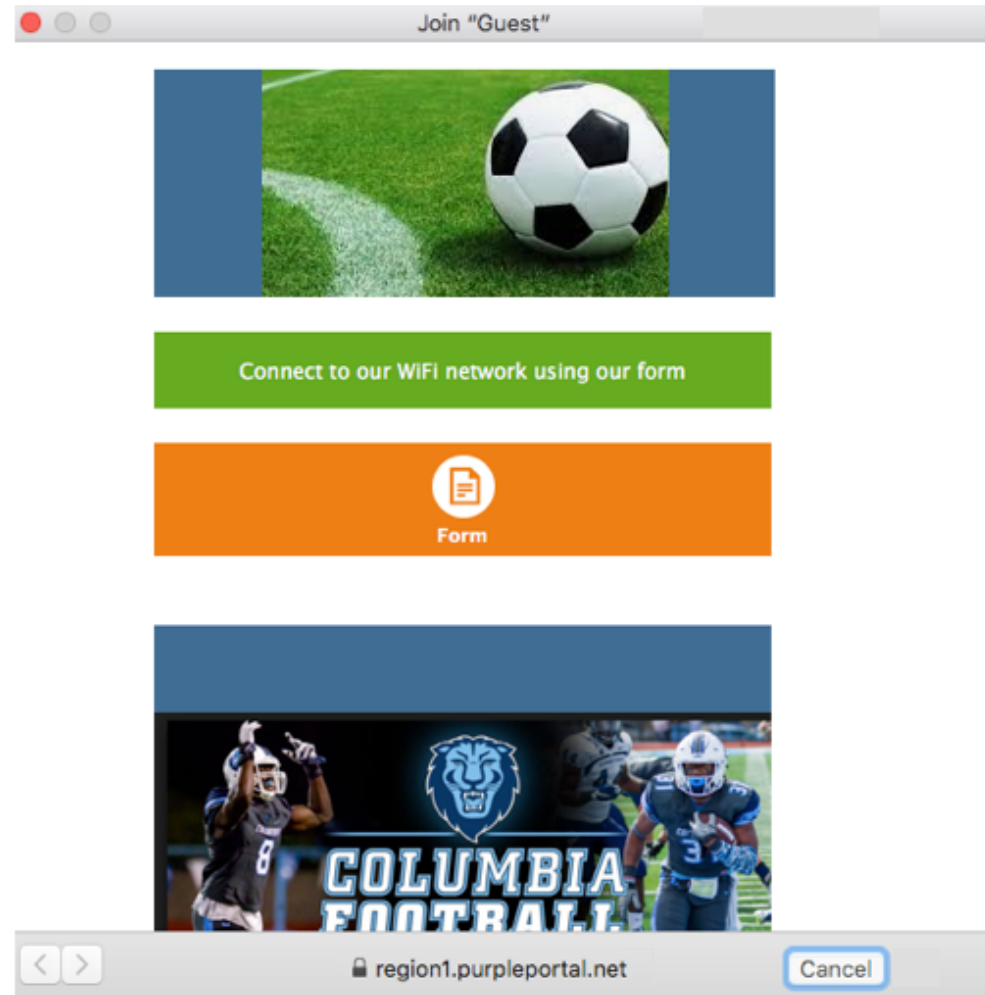
Tenerife AP305# show clients

Client List

Name	IP Address	MAC Address	OS	ESSID	Access Point	Channel	Type	Role	IPv6 Address	Signal	Speed (mbps)
939 [redacted]	17 [redacted]	8c:85: [redacted]	OS X	Guest	Tenerife AP305	157+	AC	Guest	fe80:: [redacted]	36(good)	400(good)
b1d [redacted]	17 [redacted]	2c:0e: [redacted]	Android	Guest	Tenerife AP305	157+	AC	PreAuth	fe80:: [redacted]	31(good)	121(ok)

Tenerife AP305#

Captive portal working as expected



Form must be completed

The image shows a mobile application interface for registering an account. At the top, a blue header bar contains the text "Sign in to Wi-Fi network" and a "MORE" link. Below this is a grey bar with a back arrow and the word "Back". The main content area is white and features the title "Register an account". Below the title, there is a link "Sign in now" preceded by the text "Already have an account?". The form consists of four required fields: "GENDER" (a dropdown menu currently showing "Male"), "FIRST NAME" (a text field containing "Ad"), "LAST NAME" (a text field containing "Bol"), and "DATE OF BIRTH" (a date picker). A virtual keyboard is displayed at the bottom of the screen, indicating that the "DATE OF BIRTH" field is currently active.

Sign in to Wi-Fi network MORE

< Back

Register an account

Already have an account? [Sign in now](#)

GENDER *

Male

FIRST NAME *

Ad

LAST NAME *

Bol

DATE OF BIRTH *

1 2 3 4 5 6 7 8 9 0

+ x = / < > []

q w e r t y u i o p

! @ # \$ % & * ()

a s d f g h j k l

↑ z x c v b n m ↵

Sym ⚙ , English(US) . Go

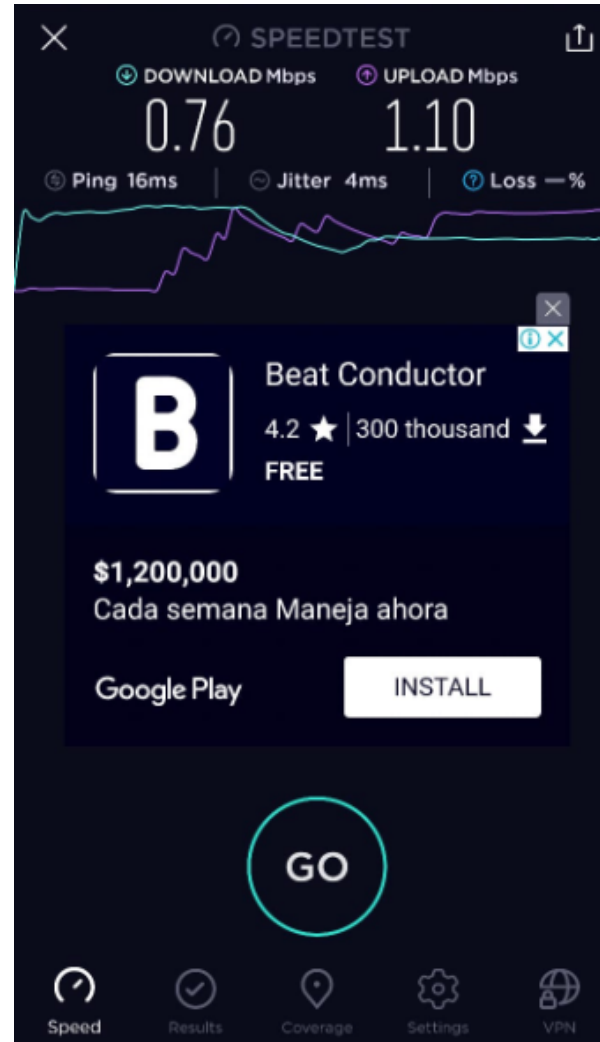
After submit the form -> Role changes from “Preauth” to “Guest”

Smartphone in “Guest” Role:

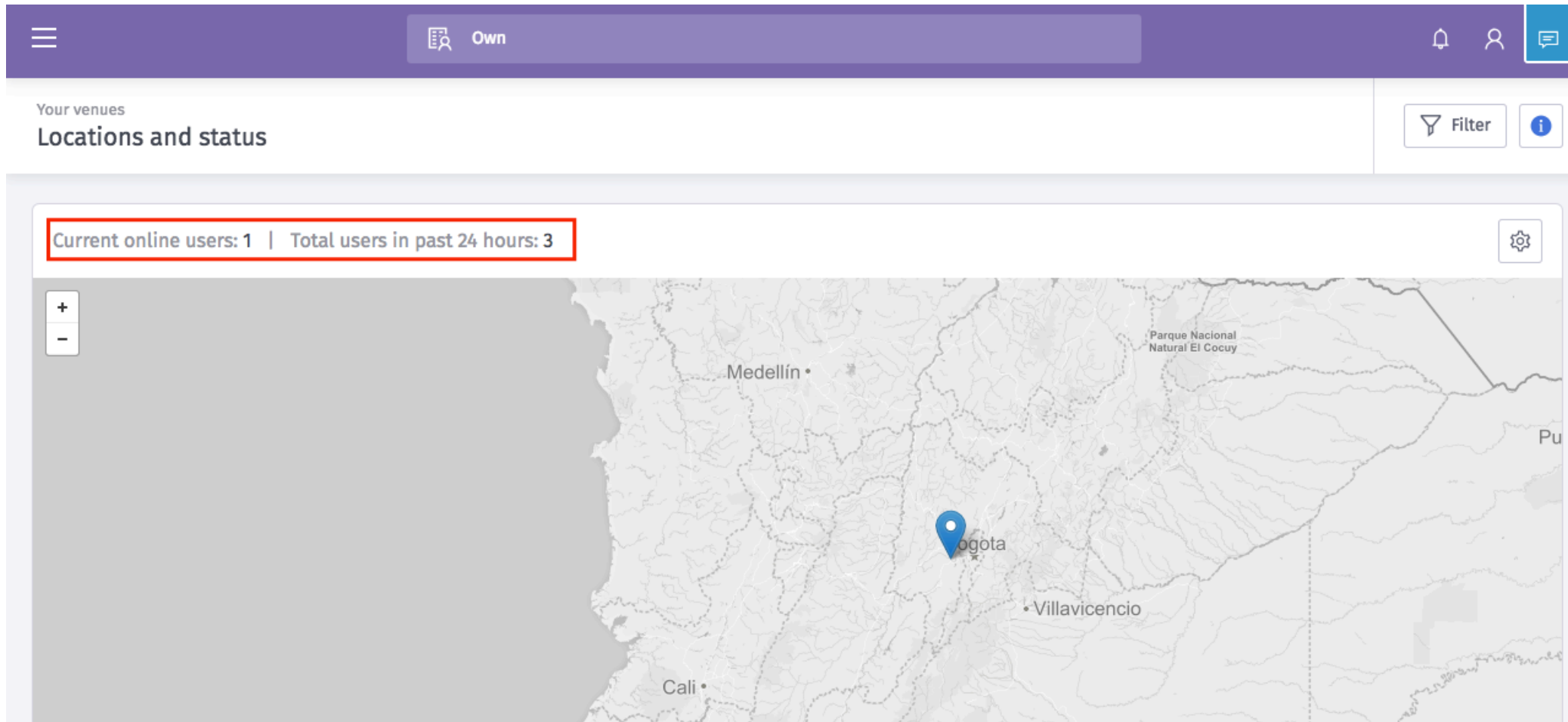
Tenerife AP305# show clients

Client List											
Name	IP Address	MAC Address	OS	ESSID	Access Point	Channel	Type	Role	IPv6 Address	Signal	Speed (mbps)
b1ee0 [redacted]	172. [redacted]	2c:0 [redacted]	Android	Guest	Tenerife AP305	157+	AC	Guest	fe80:: [redacted]	32(good)	200(good)

Speed test successful -> 1Mbps



Purple Dashboard shows Users connected





a Hewlett Packard
Enterprise company

Task: Checking Radius packets

Packet capture – Radius protocol

radius						
No.	Time	Source	Destination	Protocol	Length	Info
430	15.481042	192. [redacted]	54.217.112.62	RADIUS	294	Access-Request(1) (id=155, l=248)
432	15.703118	54.217.112.62	192. [redacted]	RADIUS	84	Access-Accept(2) (id=155, l=38)
433	15.721599	192. [redacted]	54.217.112.62	RADIUS	314	Accounting-Request(4) (id=156, l=268)
435	15.899584	54.217.112.62	192. [redacted]	RADIUS	66	Accounting-Response(5) (id=156, l=20)

▶ Internet Protocol Version 4, Src: 192. [redacted], Dst: 54.217.112.62

▶ User Datagram Protocol, Src Port: 65424, Dst Port: 1812

▼ RADIUS Protocol

Code: Access-Request (1)
Packet identifier: 0x9b (155)
Length: 248
Authenticator: 912 [redacted]
[\[The response to this request is in frame 432\]](#)

▼ Attribute Value Pairs

- ▶ AVP: l=6 t=NAS-IP-Address(4): 192. [redacted]
- ▶ AVP: l=6 t=NAS-Port(5): 0
- ▶ AVP: l=6 t=NAS-Port-Type(61): Wireless-802.11(19)
- ▶ AVP: l=52 t=User-Name(1): cdf [redacted]
- ▶ AVP: l=34 t=User-Password(2): Encrypted
- ▶ AVP: l=6 t=Service-Type(6): Login(1)
- ▶ AVP: l=14 t=Calling-Station-Id(31): c8 [redacted]
- ▼ AVP: l=14 t=Called-Station-Id(30): 24f [redacted]

Type: 30
Length: 14
Called-Station-Id: 24 [redacted]

- ▶ AVP: l=6 t=Framed-IP-Address(8): 172 [redacted]
- ▶ AVP: l=13 t=Vendor-Specific(26) v=Aruba Networks Inc(14823)
- ▶ AVP: l=22 t=Vendor-Specific(26) v=Aruba Networks Inc(14823)
- ▶ AVP: l=19 t=Vendor-Specific(26) v=Aruba Networks Inc(14823)
- ▼ AVP: l=12 t=Vendor-Specific(26) v=Aruba Networks Inc(14823)

Type: 26
Length: 12
Vendor ID: Aruba Networks Inc (14823)

- ▶ VSA: l=6 t=Aruba-Device-Type(12): iPad
- ▶ AVP: l=18 t=Message-Authenticator(80): d73f [redacted]

Purple - Radius Server

MAC Address of Instant AP305

Device Type

Packet capture – Radius protocol

radius						
No.	Time	Source	Destination	Protocol	Length	Info
430	15.481042	192. [redacted]	54.217.112.62	RADIUS	294	Access-Request(1) (id=155, l=248)
432	15.703118	54.217.112.62	192. [redacted]	RADIUS	84	Access-Accept(2) (id=155, l=38)
433	15.721599	192. [redacted]	54.217.112.62	RADIUS	314	Accounting-Request(4) (id=156, l=268)
435	15.899584	54.217.112.62	192. [redacted]	RADIUS	66	Accounting-Response(5) (id=156, l=20)

► Internet Protocol Version 4, Src: 54.217.112.62, Dst: 192. [redacted]
► User Datagram Protocol, Src Port: 1812, Dst Port: 65424
▼ RADIUS Protocol

Code: Access-Accept (2)
Packet identifier: 0x9b (155)
Length: 38
Authenticator: 27ba [redacted]
[\[This is a response to a request in frame 430\]](#)
[Time from request: 0.222076000 seconds]

▼ Attribute Value Pairs

▼ AVP: l=6 t=Session-Timeout(27): 2100
Type: 27
Length: 6

Session-Timeout: 2100

▼ AVP: l=6 t=Idle-Timeout(28): 300
Type: 28
Length: 6
Idle-Timeout: 300
▼ AVP: l=6 t=Acct-Interim-Interval(85): 120
Type: 85
Length: 6
Acct-Interim-Interval: 120

Purple - Radius Server

Maximum number of seconds to re-authentication

NEW SERVER

☒ RADIUS

☐ LDAP

Name:

PurpleServer

IP Address:

54.217.112.62

☒ Custom user timeout ?

Session timeout

30 minutes

Idle timeout

5 minutes



a Hewlett Packard
Enterprise company

Thanks

References

User Guide for Aruba Instant (IAP) from Purple

<https://region1.purpleportal.net/hardware/firmware/download/48/userguide>