

OpenRoaming set up guide for Arista Wi-Fi solution



Table of Contents

Introduction	3
1. What is OpenRoaming?.....	4
2. Benefits of OpenRoaming.....	5
2.1 Network operators.....	5
2.2 Users.....	5
2.3 Enterprises.....	5
3. How to configure Arista APs for OpenRoaming.....	6
3.1 Step 1: Setup firewall rules.....	6
3.2 Step 2: Add a Hotspot 2.0 SSID.....	6
3.2.1 WLAN Settings.....	7
3.2.2 Hotspot 2.0 Settings.....	8-9
3.3 Step 3: Step 3: Configure RADIUS server.....	10
3.3 Step 4: Download client profile.....	11
3.4 Step 5: Connect client to OpenRoaming SSID.....	11

Users should be able to automatically connect to Wi-Fi networks seamlessly and securely.

Introduction

Secure, seamless roaming between Wi-Fi and cellular networks is a necessity in today's hyper-connected world to provide users uninterrupted connectivity wherever they are - at events, on the road, in airports, shopping malls, universities or sports arenas. The key requirement of such seamless connectivity is that users should be able to automatically 'connect' to Wi-Fi networks without the need for entering passwords and exposing themselves to cyber attacks.



What is OpenRoaming?

The OpenRoaming framework facilitates Wi-Fi users to connect to the Wi-Fi network owned by any Access Network Provider (ANP) who is a part of the OpenRoaming consortium. The users can use access credentials provided by Identity Providers (IDPs) which are part of the OpenRoaming consortium. OpenRoaming is built on top of Passpoint technology and creates a standardized federation policy to establish a scalable, one-to-many relationship between multiple IDPs and ANPs. The configuration effort is done one time and for all the federation participations, offering scalable roaming across networks of multiple ANPs.

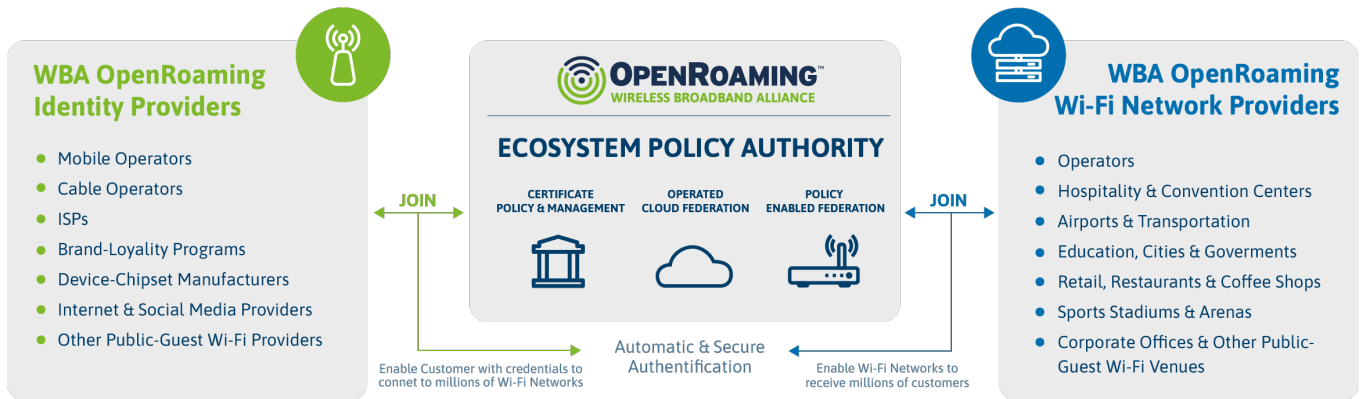


Fig 1: OpenRoaming framework of Identity Providers and Access Network Providers for seamless roaming and onboarding

Source: Wireless Broadband Alliance

Benefits of OpenRoaming

The OpenRoaming capability of Arista APs benefits all the stakeholders in a network - network operators, users and enterprises alike.

Network operators

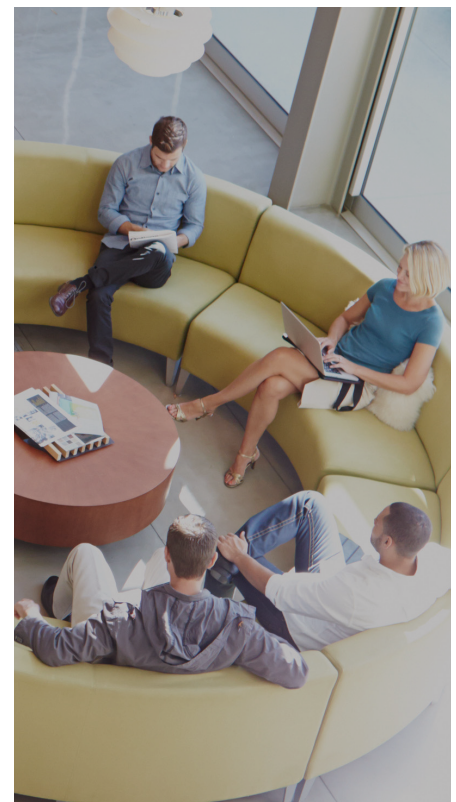
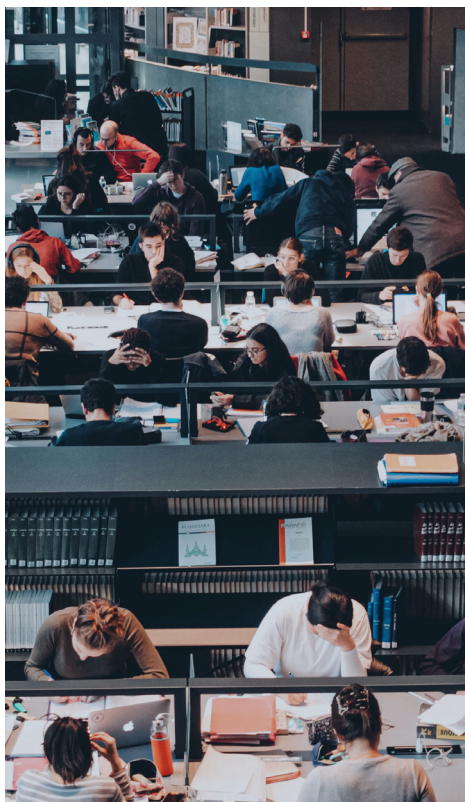
- **Wi-Fi offload:** Dense deployments where a cellular network's capacity falls deficient from the heavy traffic demands can benefit by offloading traffic seamlessly to Wi-Fi hotspots.
- **Differentiated user experience:** Operators can improve customer engagement through personalization and value-added services such as loyalty integration and locationing services.
- **Advanced analytics:** Seamless roaming across multiple IDPs and ANPs provides a richer data pool of users for extracting meaningful insights.

Users

- **Enhanced experience:** Users are spared from the risks of joining public networks through streamlined onboarding and security procedures.
- **Personalisation:** OpenRoaming facilitates personalized user experiences through integration with loyalty and payment applications.

Enterprises

- **Scalability:** Large enterprises and universities often receive a sizable footfall of guest users from other Identity Providers, or need to allow their users to roam to third-party networks. OpenRoaming guarantees this scalability and roaming capability.
- **Secure network:** OpenRoaming ensures that only authorized users get connected to the enterprise network via an 'active directory' or a user's allow-listing mechanism that can be integrated in the enterprise's AAA.
- **Easy user management:** User lifecycle management is simplified due to the federated architecture. through integration with loyalty and payment applications.



How to configure Arista APs for OpenRoaming

STEP 1

Setup firewall rules

Ensure that the following ports are open in firewall/security group:

- TCP: 80, 443, 1812, 1813, 2083, 3306, 11812, 11813
- UDP: 1812, 1813, 2083, 11812, 11813

STEP 2

Add a Hotspot 2.0 SSID

Create a Hotspot 2.0 SSID by navigating to Configure → Hotspot 2.0. Add an SSID (eg., WBA-Test in the above screenshot) with appropriate Security levels to support Hotspot 2.0, following the below WLAN settings

The screenshot displays the Arista configuration interface for a Hotspot 2.0 SSID. The left sidebar contains navigation options: DASHBOARD, MONITOR, CONFIGURE (selected), TROUBLESHOOT, FLOOR PLAN, REPORTS, and SYSTEM. The main content area shows the configuration for 'WBA-Test' under the 'WiFi' section. A yellow warning banner at the top states: "Changes will restart the SSID if it is on. The changes will affect all groups and folders using this SSID." Below this, the 'WLAN' dropdown menu is open, showing 'WLAN' and 'Hotspot 2.0' options. The 'Hotspot 2.0' tab is selected, and the configuration fields are as follows:

- SSID Name *: WBA-Test
- Profile Name *: Test

The interface also includes a search bar at the top for MAC/ IP Address/ User Name/ Device Name, and various status indicators (0, 1, 0, 111, 0) and a 'More' menu.

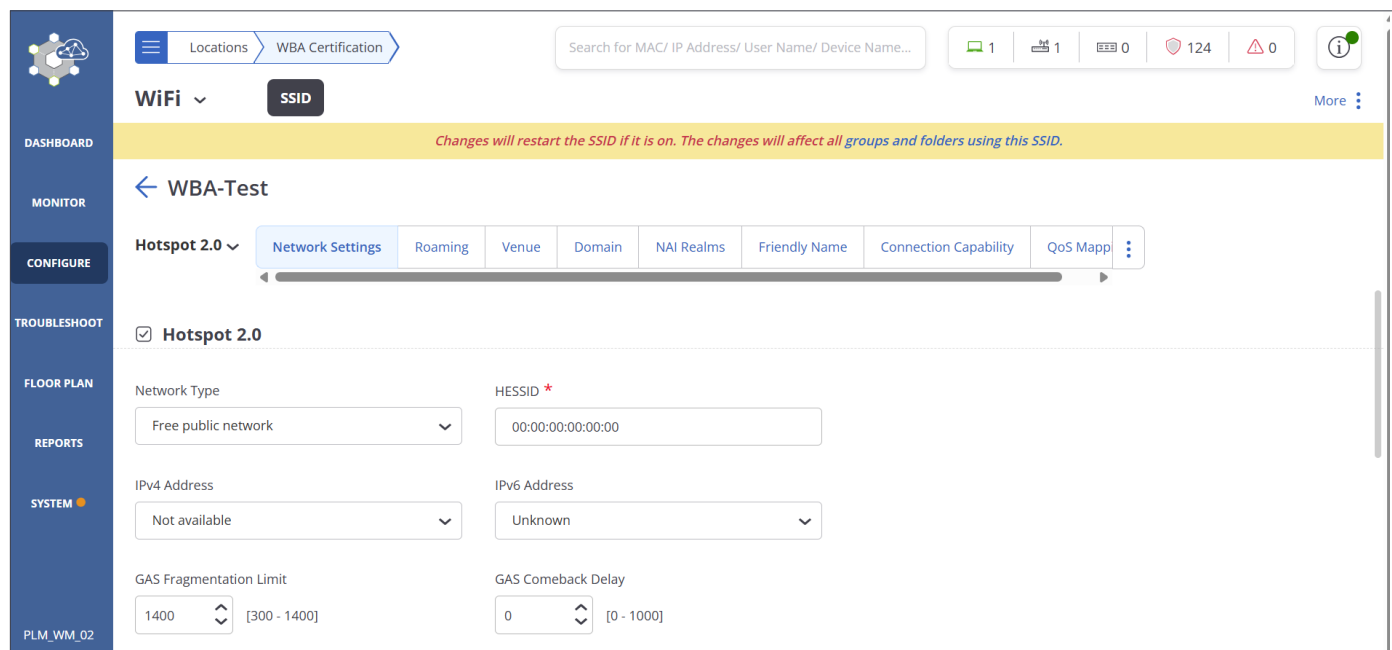
WLAN Settings

Parameter	Setting/Value
Security	
Security Level	WPA3 Transition mode
RADIUS Authentication Server	WBA
RADIUS Accounting Server	WBA
RADIUS	
RADIUS Server Name	WBA
Authentication Port	1812
Accounting Port	1813
Network	
Network Mode	Bridged
Traffic Shaping & QoS	
Enforce WMM Admission Control	Uncheck

Table 1: WLAN Settings

Hotspot 2.0 Settings

The configuration parameters required for enabling OpenRoaming on the Arista AP can be set under Hotspot 2.0. The parameters to be set on each tab and their representative values are listed in the table below. The parameters can be set to appropriate values as per the deployment choices.



Parameter	Setting/Value
Network Settings	
Network Type	Free Public Network
HESSID	00:00:00:00:00:00
IPv4 Address	Not available
IPv6 Address	Unknown
Internet Access	Check
Network Authentication Type	Not configured
Roaming	
Roaming consortiums	5A03BA0000 004096 (Cisco)

Table 2: Hotspot 2.0 Settings

Parameter	Setting/Value
Venue	
Venue Group	Business
Venue Type	Unspecified Business
Venue Name	WBA
Language Code	ENG
Domain	
Domain	google.openroaming.net apple.openroaming.net Openroaming.goog idp.openroamingconnect.org
NAI Realms	
	None required
Friendly Name	
	None required
Connection Capability	
	None required
QoS Mapping	
	None required

Table 2: Hotspot 2.0 Settings

Step 3: Configure RADIUS server

Go to Configure → Network Profiles → RADIUS. Configure the RADIUS settings as below:

Parameter	Setting/Value
RADIUS Server Name	WBA
Authentication Port	1812
Accounting Port	1813

Table 3: RADIUS Settings

The screenshot shows the Arista configuration interface for RADIUS settings. The breadcrumb path is 'Locations' > 'WBA Certification' > 'Network Profiles' > 'RADIUS'. A search bar is present at the top right. The left sidebar contains navigation options: DASHBOARD, MONITOR, CONFIGURE (selected), TROUBLESHOOT, FLOOR PLAN, REPORTS, and SYSTEM. The main content area shows the configuration for 'WBA' under 'Network Profiles'. A yellow warning banner states: 'Changes to this RADIUS Server will affect all SSIDs and LAN Ports that use this RADIUS Server. SSIDs and LAN Ports using this RADIUS server'. The configuration fields are:

- RADIUS Server Name*: WBA
- IP Address/FQDN*: 34.172.215.201
- RadSec: ON, OFF
- Authentication Port*: 1812 (range [1-65535])
- Accounting Port*: 1813 (range [1-65535])
- Shared Secret*: radsec

STEP
3

Download client profile

Download and install client profile on the client from one of the following urls:

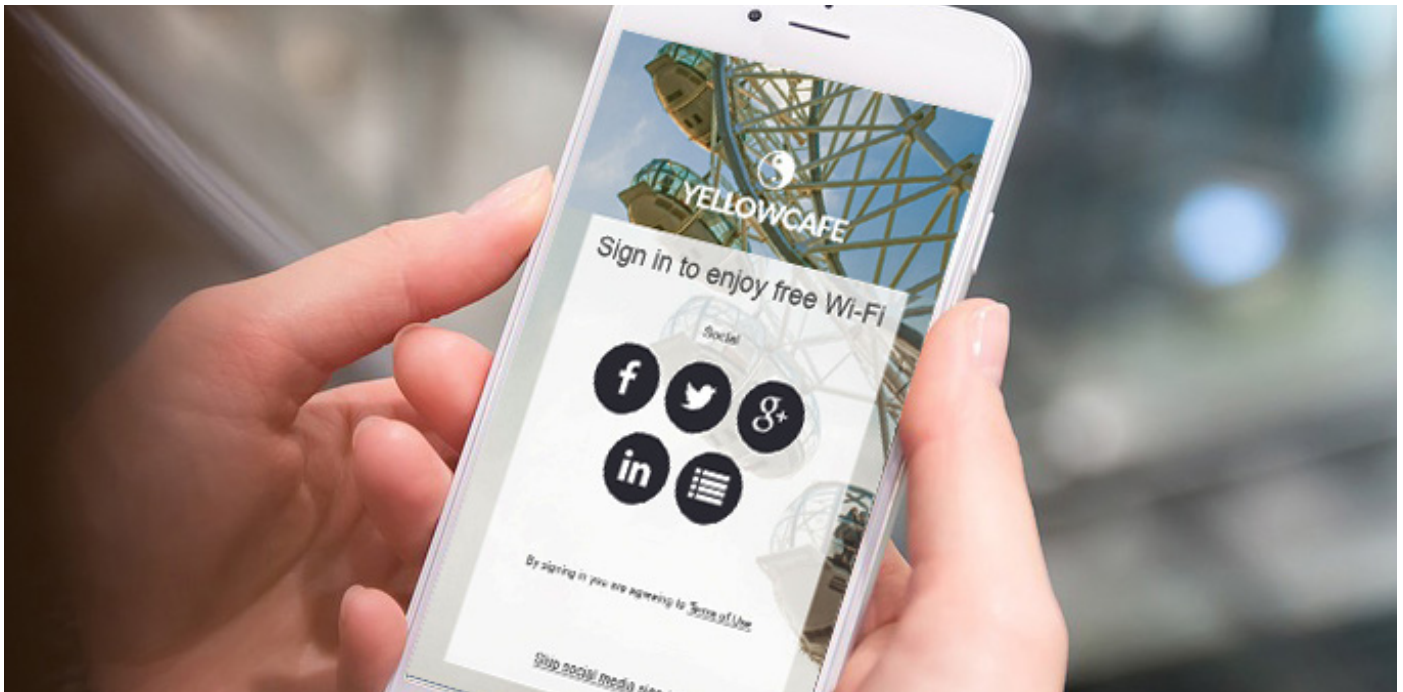
<https://provision.connectionassist.com/wba>

<https://www.openroamingconnect.org/register>

STEP
4

Connect client to OpenRoaming SSID

On the client Wi-Fi settings, choose the configured Hotspot 2.0 SSID and connect.



Santa Clara—Corporate Headquarters

5453 Great America Parkway,
Santa Clara, CA 95054

Phone: +1-408-547-5500

Fax: +1-408-538-8920

Email: info@arista.com

Ireland—International Headquarters

3130 Atlantic Avenue
Westpark Business Campus
Shannon, Co. Clare
Ireland

Vancouver—R&D Office

9200 Glenlyon Pkwy, Unit 300
Burnaby, British Columbia
Canada V5J 5J8

San Francisco—R&D and Sales Office 1390

Market Street, Suite 800
San Francisco, CA 94102

India—R&D Office

Global Tech Park, Tower A & B, 11th Floor

Marathahalli Outer Ring Road
Devarabeesanahalli Village, Varthur Hobli
Bangalore, India 560103

Singapore—APAC Administrative Office

9 Temasek Boulevard

#29-01, Suntec Tower Two
Singapore 038989

Nashua—R&D Office

10 Tara Boulevard
Nashua, NH 03062



Copyright ©2026 Arista Networks, Inc. All rights reserved. CloudVision, and EOS are registered trademarks and Arista Networks is a trademark of Arista Networks, Inc. All other company names are trademarks of their respective holders. Information in this document is subject to change without notice. Certain features may not yet be available. Arista Networks, Inc. assumes no responsibility for any errors that may appear in this document. 7 April, 2026