# Forescout Integration with Arista Wi-Fi

# 

Arista Wi-Fi supports Wi-Fi client authentication with Forescout NAC server using standard RADIUS protocol. The Forescout NAC solution offers the following advantages:

- Comprehensive visibility of all devices connected to the network
- Automated posture assessment and compliance
- Flexible policy enforcement across heterogenous networks

The following figure shows the logical architecture and the possible workflows.





#### Integration with Forescout:

 Through RADIUS: Standard AAA protocol
 Comprehensive list of RADIUS Attributes supported in Arista AP to control various authorization actions, and to support an extensive range of complex NAC workflows:

#### - Guest

- Corporate Client Onboarding
- BYOD / Onboarding
- Posture Assessment and Remediation



An Arista access point (AP) supports Wi-Fi client authentication using 802.1X or MAC-Based Authentication (MBA) and exchanges RADIUS messages with Forescout. The following workflows are supported:

- Guest Onboarding
- Corporate client onboarding
- BYOD (Bring Your Own Device)
- MAC Authentication
- Posture assessment and remediation

Arista APs also support RADIUS attributes for various authorization actions such as role-based access control (RBAC), dynamic VLAN assignment, dynamic bandwidth assignment, and session timeout.

This document describes the steps to integrate Arista APs with the Forescout NAC by appropriately configuring CloudVision Cognitive Unified Edge (CV-CUE) and Forescout. The information in this document holds for Arista Wi-Fi version 8.8.1 and Forescout version 8.1.0 (and later versions of these).

#### **Configure CV-CUE Wi-Fi for Forescout**

The CV-CUE configuration broadly consists of two steps: add Forescout NAC server as the RADIUS server and configure the SSID to use this server for the client authentication workflow. The workflow described here is the corporate client using 802.1X.

#### Add Forescout as RADIUS Server

The steps to add RADIUS server are as follows: Go to Configure > Wi-Fi > RADIUS. Click Add RADIUS Server. Enter the Forescout server name, IP address, authentication and accounting ports, and shared secret.

		Search	Search for MAC/ IP Addre		
	WiFi 🔸 ssid	RADIUS Tunnel Interfa	ace Role Profile Radio	Settings Device S	ettings
DASHBOARD	⊖ Forescout				
MONITOR	RADIUS Server Name *				
CONFIGURE	Forescout				
TROUBLESHOOT	IP Address *				
FLOOR PLANS	10.92.224.54		ol		
REPORTS	Authentication Port *	Accounting Port "	Shared Secret "	0	
SYSTEM					



# Configure the Corporate SSID

The steps to configure the Corporate SSID for 802.1X are as follows:

- 1. Go to **Configure > Wi-Fi** and select the SSID you want to configure or add a new SSID.
- 2. On the Security tab, under Select Security Level for Associations, select WPA2 or WPA3 and select the 802.1X radio button.
- 3. Select the Forescout server you added in the previous section as the **Authentication Server** in the **Primary** tab. You can similarly configure the secondary server.

	Locations			Search for
	WiFi - ssid radius	Tunnel Interface Role Prof	file Radio Settings	Device Settir
DASHBOARD	⊖ forescout Test	Basic	Security Network	0
MONITOR				
CONFICURE	Select Security Level for Association	15		
	WPA2.	O PSK 💿	802.1x	
TROUBLESHOOT	Open			
FLOOR PLANS	WPA2 WPA/WPA2 Mixed Mode			
REPORTS	Primary Seconda	ary		
SYSTEM	Authentication Server *	Accounting S	erver	
	Forescout	None	-	
	Add/Edit	Add/Edit		

## **Configure Forescout for Arista Wi-Fi**

The basic configuration involves adding Arista Wi-Fi as a NAS entity in the Forescout server so as to enable RADIUS authentication with Arista APs. The steps to do so are as follows:

- 1. Log in to the Forescout console. Click on the **Options** wheel on the top right corner of the page. The Options window appears.
- 2. Select Wireless in the Options window as shown in the following figure.

Views		Options				
Search	Q	Options				
> III Policies		Q	Appliance			
		> 🌉 Modules	Search Status IP/Name	Q	Hostname 🔺	v
		Microsoft SMS/SCCM     Advanced Tools	V 1 items (1 selected)		NA	8.1
Filters Search	Q	GF IOL Posture Assessment Eng GF Flow Collector IOC Scanner	Endpoints: Endpoints: License: Bandwidth: High Availability:	0 (max. performance capacity 99) 0 (max. license capacity 200) Valid for 149 days Current 0.0Mbps, Average 0.0Mbps, HA is not enabled	Max 0.0Mbps	
<) All  C Segments (0)  C Organizational Units  S Default Groups  S Groups		AWS AWS RADIUS MAC Address Repository CEF HPS Inspection Engine	Swap: Lost Packets: CPU Utilization: Uptime: Time Gap from Console: NTP Servers: Packet Engine: Channels: Connection: Platform:	o Kliosytes per second 0.00% 5.96% 13 days and 8 hours Less than a minute earlier updates.forescout.com CounterACT Appliance is running in OK Virtual CounterACT Appliance	Listen Only mode	

3. The Add wireless - Step 1 window appears.

ARISTA

- a. Select Generic (RADIUS-based) in the Product dropdown.
- b. In the Address field, add IP addresses of the APs that will perform RADIUS authentication with Forescout. You can bulk import the list of IP addresses from a ".csv" file or you can enter the subnet used by the APs as shown in the following figure.

Add wirel	ess - Step	1	×
Add Wireless	Device		
🖆 General	Genera Configure or Select the RADIUS-	al e the Wireless Plugin to manage a supported WLAN device. e Product field option 'Generic (RADIUS-based)' to enable CounterACT based authentication and authorization of connecting wireless clients.	
	Product Address	Generic (RADIUS-based) ➤ 10.10.1.1/24 Examples: • 192.168.1.0/24 • fd00::/8	
	Comment	Arista WIFI	
		Help Previous Next Finish Can	cel

- 4. Click Next to move to Add wireless Step 2.
- 5. In the Add wireless Step 2 of 3 window, leave the Use SNMP box unchecked, and simply click Next to move to Step 3.
- 6. In the Step 3 window, enter the same shared secret that you configured in CV-CUE when adding Forescout as the RADIUS

Add wirele	ss - Step 3 of 3	×
Add Wireless [	Device	
General SNMP 16 802.1X	802.1X Configure 802.1X settings	
	RADIUS Secret as configured in WLAN Device Retype RADIUS Secret as configured in WLAN Device	****

server.

# ARISTA

### 7. Click Next.

8. A table summarizing the configuration settings appears. Click Apply.

Options									
Search Q	Wireless								
> E Appliance	Provide NAC capabilities to	wireless network controllers and ac	ess points for the purpose of controlling wi	reless endpoints connected to ther	n.				
> Modules	Search	0							
E Channels			Province -	Annual I	11000012	Concernant and the second			
Microsoft SMS/SCCM	IP Address +	SubnetMask	Product	Comment	Managed By	Connected clients	US	Location	Add
Advanced Tools	10.10.10.0	24	Generic (RADIUS-based)	Arista Wireless					Edit
B7 IoT Posture Assessment Eng									Remove
😂 Flow Collector									Test
IOC Scanner									Duplicat
A Azure									Export
AWS									Import
S Wireless									
B RADIUS									
MAC Address Repository									
留 CEF									
😭 HPS Inspection Engine									
WMware NSX									
Wware vSphere									
∆ Linux									
e osx									
Guest Management									
User Directory									
we switch									
M Centralized Network Control									
General									
@ Discovery									
> II NAC									
Licenses									
C Lists									
> 🕎 Map									
N Internal Network									-
100000000000000000000000000000000000000									

The Arista APs with the IP addresses you entered have now been added to Forescout as NAS entities.

## 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 © 2022 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. 05-0047-01 May 10, 2022