

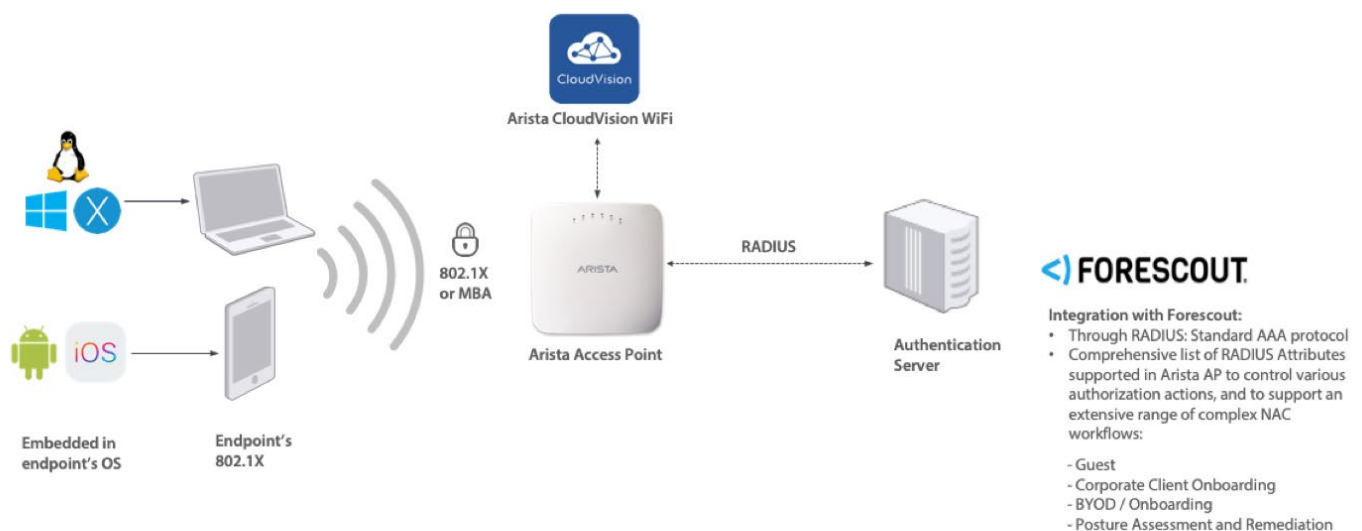
# Forescout Integration with Arista WiFi



Arista WiFi supports WiFi 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.



An Arista access point (AP) supports WiFi 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 WiFi (CVW) and Forescout. The information in this document holds for Arista WiFi version 8.8.1 and Forescout version 8.1.0 (and later versions of these).

### Configure CloudVision WiFi for Forescout

The CVW 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 > WiFi > RADIUS.

Click Add RADIUS Server.

Enter the Forescout server name, IP address, authentication and accounting ports, and shared secret.

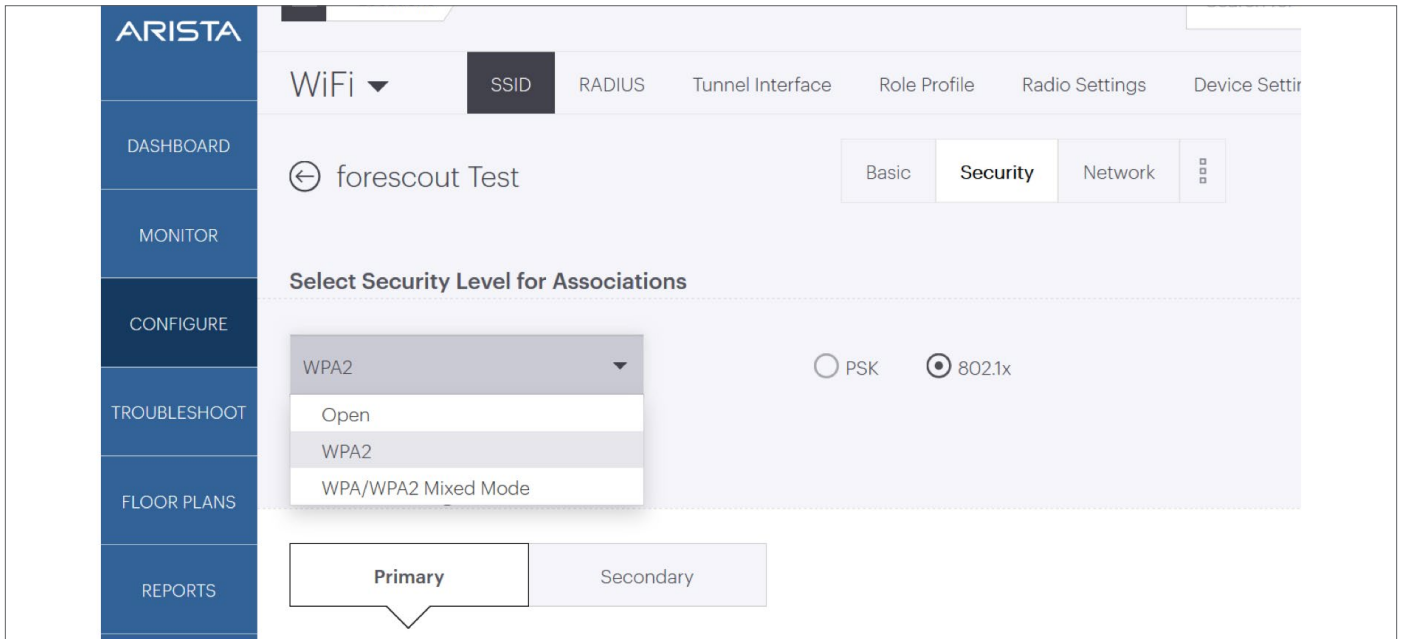
The screenshot shows the Arista CloudVision configuration interface. On the left is a navigation menu with options: ARISTA, DASHBOARD, MONITOR, CONFIGURE (highlighted), TROUBLESHOOT, FLOOR PLANS, and REPORTS. The main content area is titled 'WiFi' and has tabs for SSID, RADIUS (selected), Tunnel Interface, Role Profile, Radio Settings, and Device Settings. Under the RADIUS tab, there is a section for 'Forescout' with the following fields:

- RADIUS Server Name \***: A text input field containing 'Forescout'.
- IP Address \***: A text input field containing '10.92.224.54'.
- Authentication Port \***: A dropdown menu showing '1812' and a range '[1-65535]'.
- Accounting Port \***: A dropdown menu showing '1813' and a range '[1-65535]'.
- Shared Secret \***: A password input field with a masked view icon (eye with a slash).

## Configure the Corporate SSID

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

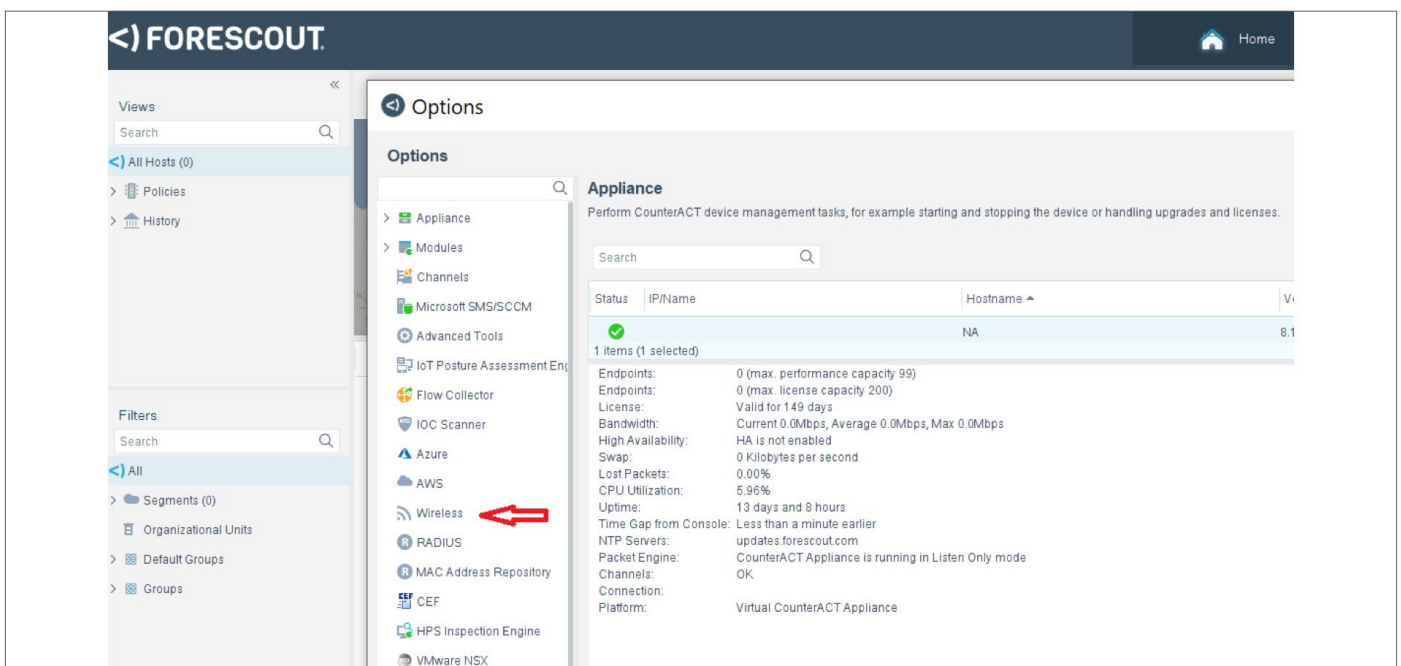
1. Go to **Configure > WiFi** and select the SSID you want to configure or add a new SSID.
2. On the **Security** tab, under **Select Security Level for Associations**, select **WPA2** or **WPA3** and select the **802.1X** radio button.
3. Select the Fore Scout server you added in the previous section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



## Configure Forescout for Arista WiFi

The basic configuration involves adding Arista WiFi 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.



3. The Add wireless - Step 1 window appears.
  - 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 wireless - Step 1**

### Add Wireless Device

**General**

Configure the Wireless Plugin to manage a supported WLAN device.  
OR  
Select the Product field option 'Generic (RADIUS-based)' to enable CounterACT RADIUS-based authentication and authorization of connecting wireless clients.

Product: Generic (RADIUS-based) ▾

Address: 10.10.1.1/24

Examples:

- 192.168.1.0/24
- fd00::/8

Comment: Arista WIFI

Buttons: Help, Previous, Next, Finish, Cancel

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 CVW when adding Forescout as the RADIUS server.

**Add wireless - Step 3 of 3**

### Add Wireless Device

**802.1X**

Configure 802.1X settings

General ✓

SNMP ✓

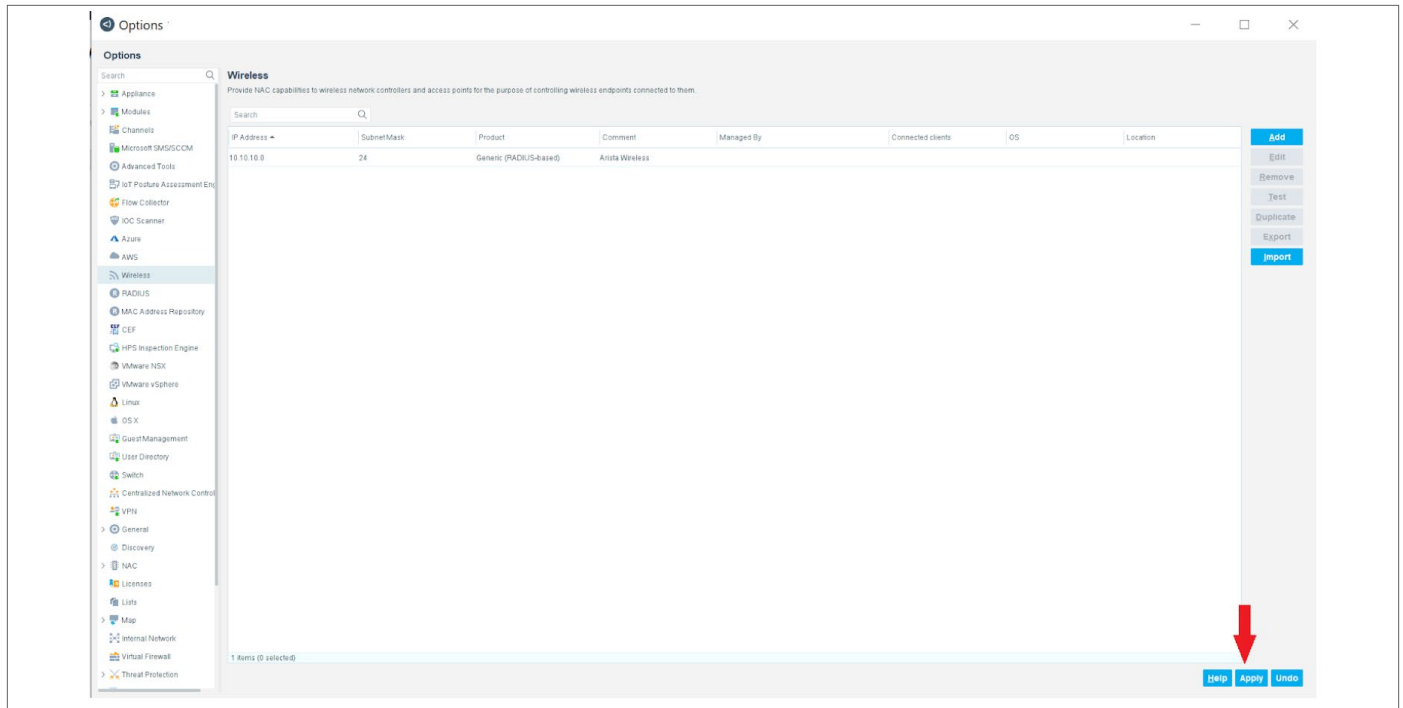
802.1X

RADIUS Secret as configured in WLAN Device: \*\*\*\*\*

Retype RADIUS Secret as configured in WLAN Device: \*\*\*\*\*

Buttons: Help, Previous, Next, Finish, Cancel

7. Click **Next**.
8. A table summarizing the configuration settings appears. Click **Apply**.



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](mailto: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 © 2020 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 September 30, 2020