ARISTA

Solution Brief

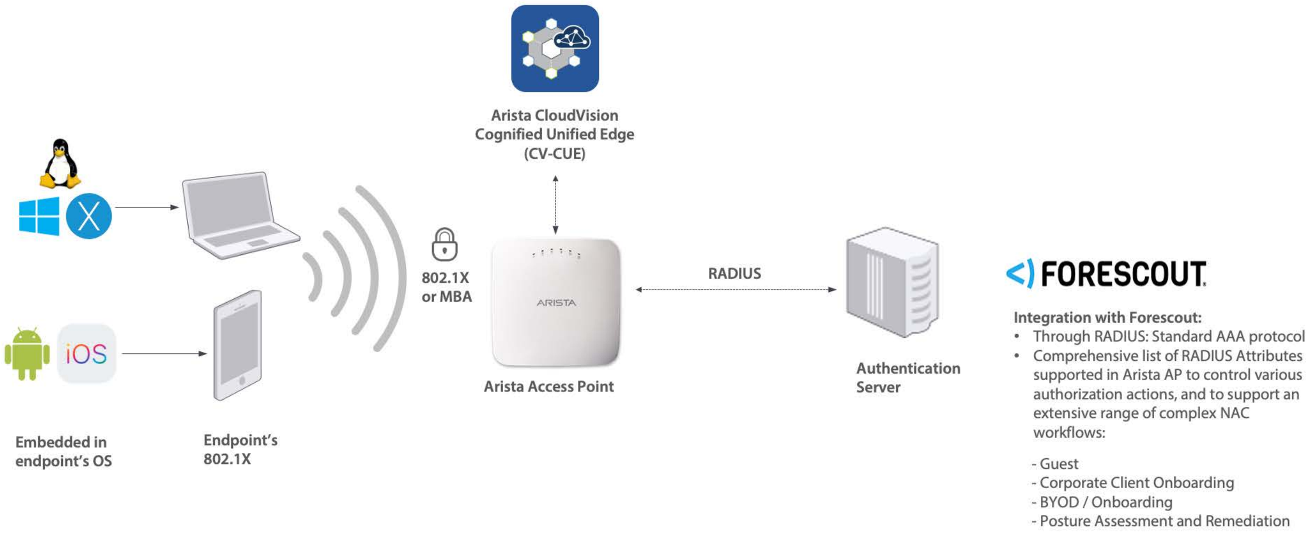
Forescout Integration with Arista Wi-Fi

FORESCOUT

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 .

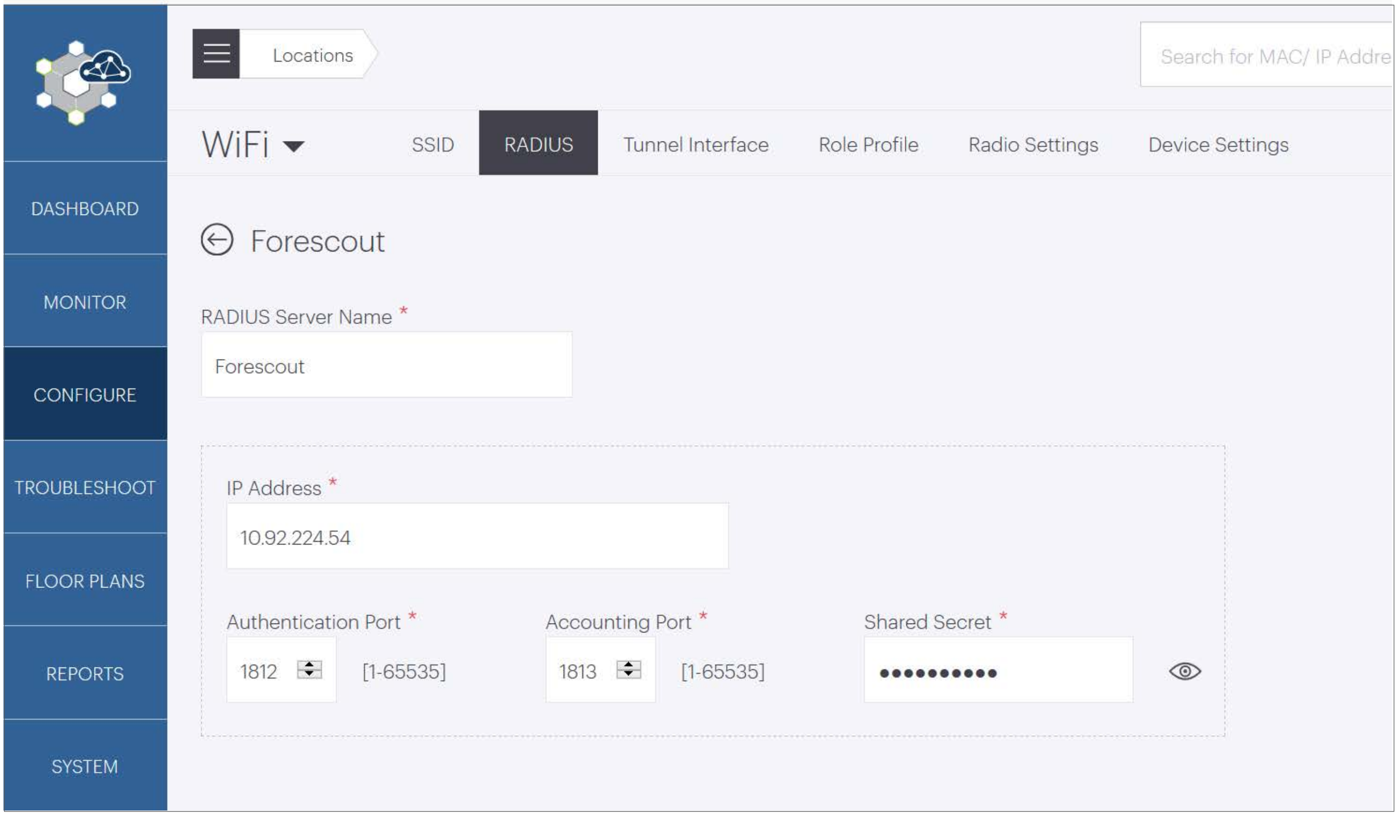
This document describes the steps to integrate Arista APs with the Forescout NAC by appropriately configuring CloudVision Cognitive Unified Edge (CV-CUE) and Forescout. The information in this document holds for Arista Wi-Fi version 8.8.1 and Forescout version 8.1.0 (and later versions of these).

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.



Forescout

RADIUS Server Name *
Forescout

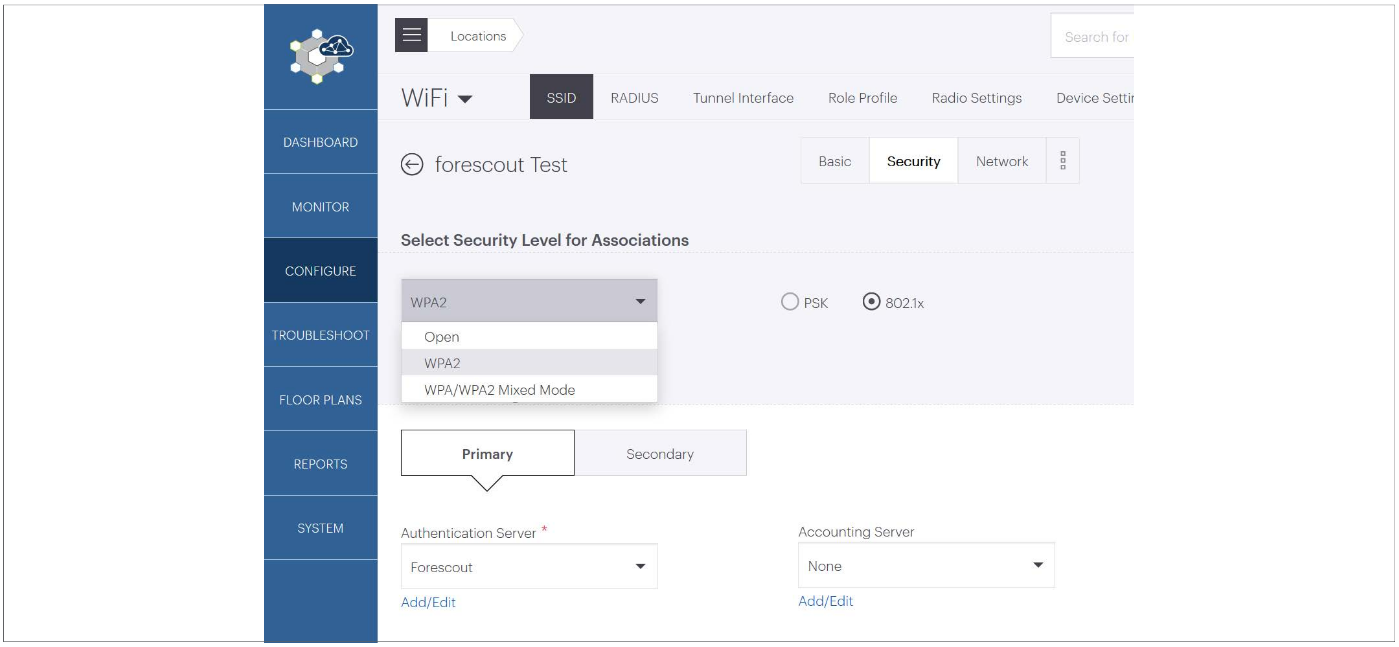
IP Address *
10.92.224.54

Authentication Port * 1812 [1-65535]
Accounting Port * 1813 [1-65535]
Shared Secret * ●●●●●●●●●●●

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.



forescout Test

Select Security Level for Associations

WPA2 ○ PSK ● 802.1x

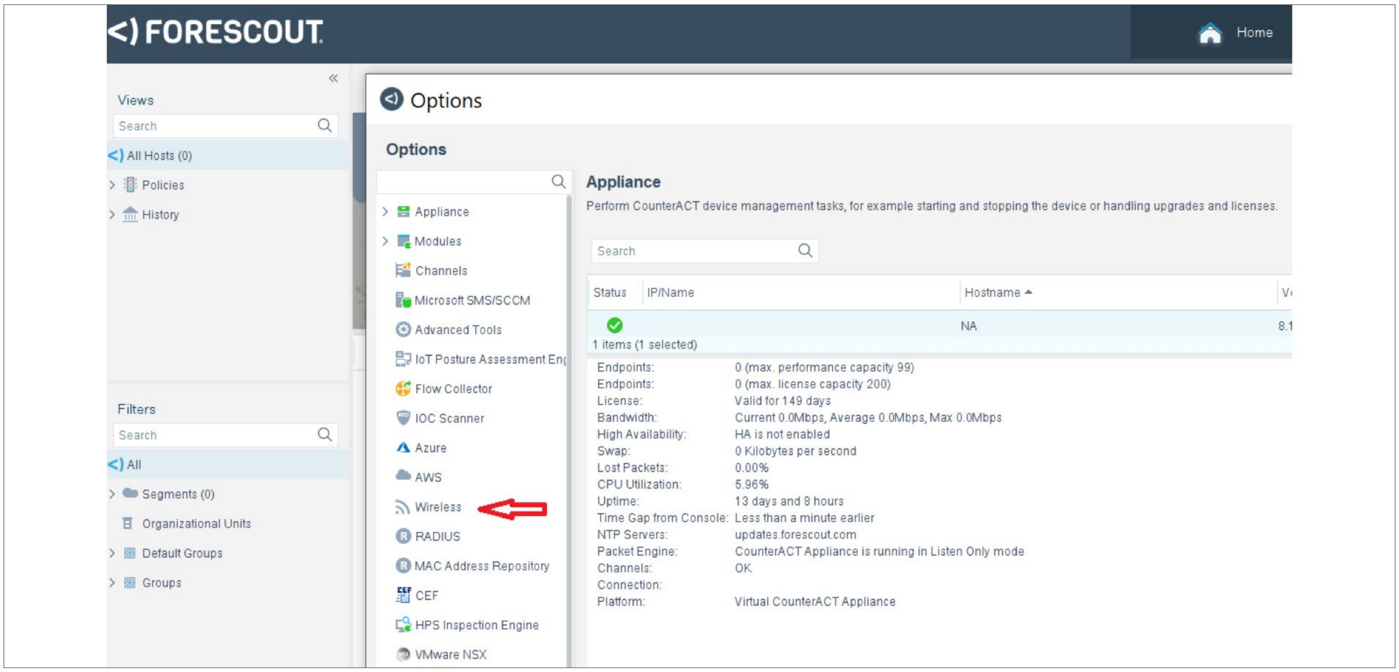
Authentication Server * Forescout

Accounting Server None

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.



Appliance

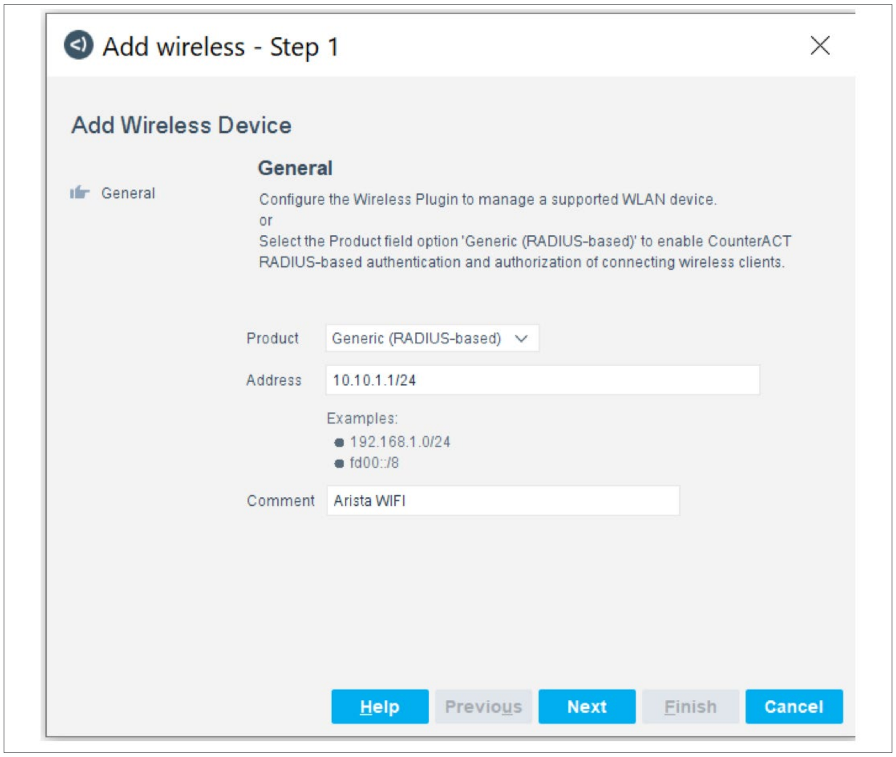
Perform CounterACT device management tasks, for example starting and stopping the device or handling upgrades and licenses.

Status	IP/Name	Hostname	Ve
✓		NA	8.1

1 items (1 selected)

```
Endpoints:              0 (max. performance capacity 99)
Endpoints:              0 (max. license capacity 200)
License:                Valid for 149 days
Bandwidth:              Current 0.0Mbps, Average 0.0Mbps, Max 0.0Mbps
High Availability:      HA is not enabled
Swap:                   0 Kilobytes per second
Lost Packets:           0.00%
CPU Utilization:        5.96%
Uptime:                 13 days and 8 hours
Time Gap from Console:  Less than a minute earlier
NTP Servers:            updates.forescout.com
Packet Engine:          CounterACT Appliance is running in Listen Only mode
Channels:               OK
Connection:
Platform:               Virtual CounterACT Appliance
```

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.

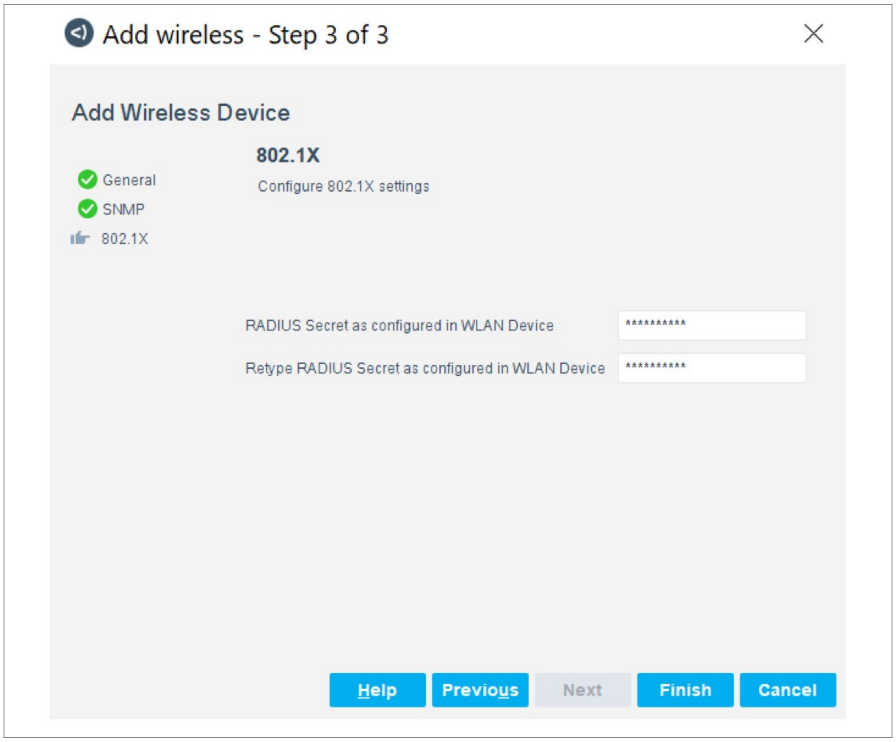
Product: Generic (RADIUS-based)

Address: 10.10.1.1/24

Examples:
- 192.168.1.0/24
- fd00::/8

Comment: Arista WIFI

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 server.



Add wireless - Step 3 of 3

Add Wireless Device

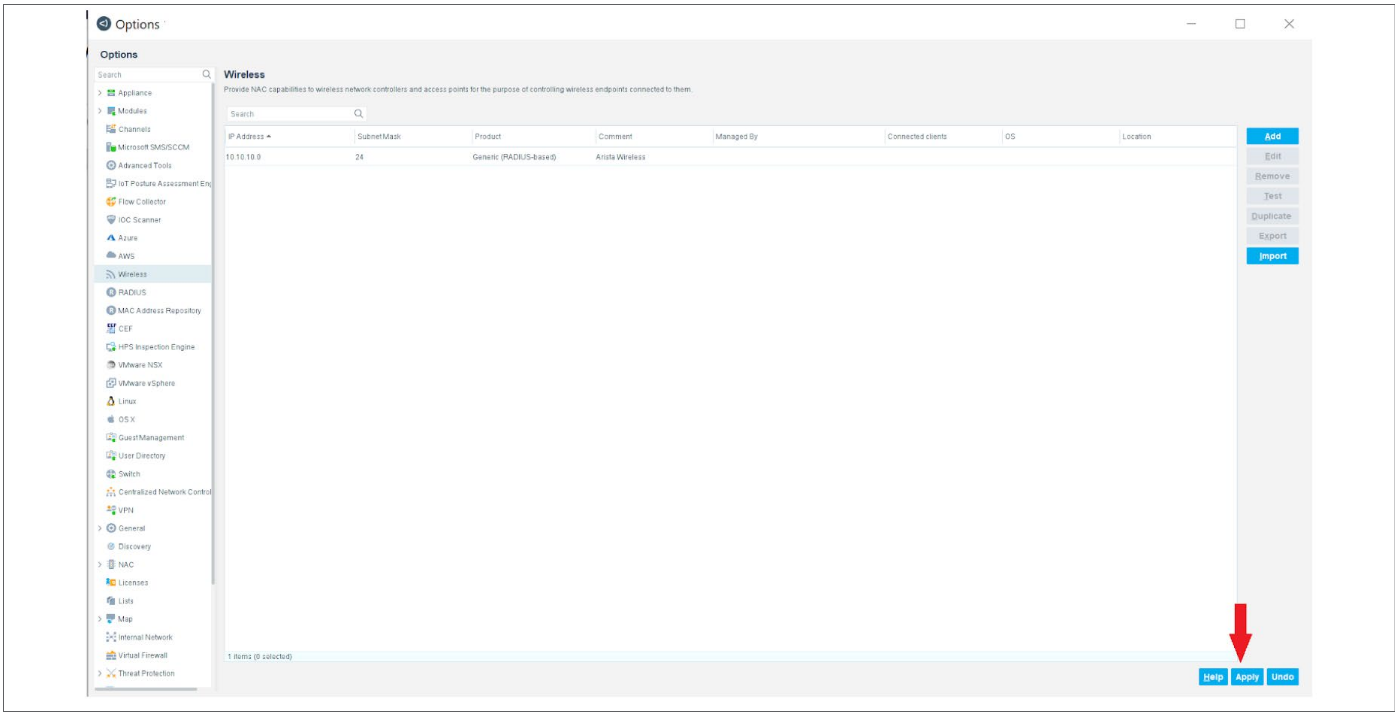
802.1X

Configure 802.1X settings

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

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

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



Wireless

Provide NAC capabilities to wireless network controllers and access points for the purpose of controlling wireless endpoints connected to them.

IP Address ▲	Subnet Mask	Product	Comment	Managed By	Connected clients	OS	Location
10.10.10.0	24	Generic (RADIUS-based)	Arista Wireless				

1 items (0 selected)

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