



# Forescout

## Network Module: Wireless Plugin

### Configuration Guide

**Version 2.0.1**



## Contact Information

Forescout Technologies, Inc.

190 West Tasman Drive

San Jose, CA 95134 USA

<https://www.Forescout.com/support/>

Toll-Free (US): 1.866.377.8771

Tel (Intl): 1.408.213.3191

Support: 1.708.237.6591

## About the Documentation

- Refer to the Technical Documentation page on the Forescout website for additional documentation: <https://www.Forescout.com/company/technical-documentation/>
- Have feedback or questions? Write to us at [documentation@forescout.com](mailto:documentation@forescout.com)

## Legal Notice

© 2020 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at <https://www.Forescout.com/company/legal/intellectual-property-patents-trademarks>. Other brands, products, or service names may be trademarks or service marks of their respective owners.

2020-07-08 13:50

## Table of Contents

<b>About the Wireless Plugin .....</b>	<b>5</b>
Wireless Network Access Device Terminology .....	7
How It Works.....	7
About WLAN Controller/Lightweight Access Points .....	8
Overlapping IP Address Support .....	9
IPv6 Support .....	9
Failover Clustering Support .....	9
Appliance Management Processing Load.....	10
Supported Vendor Products .....	10
What to Do.....	10
<b>Requirements.....</b>	<b>10</b>
Forescout Requirements.....	10
Networking Requirements .....	11
WLAN Device – Read/Write Settings .....	11
Required WLAN Device Configuration .....	12
<b>Configure the Plugin.....</b>	<b>12</b>
Configuration.....	13
WLAN Device Management Configuration .....	14
Enable Forescout RADIUS-only Management of Wireless Clients .....	21
802.1X Integration .....	23
Control Plugin Query about Lightweight Access Points .....	24
Verify That the Plugin Is Running .....	24
Test the Plugin Configuration for WLAN Device Management.....	25
Troubleshooting .....	26
Verify Plugin Processing of SNMP Traps .....	26
Wireless Pane Display .....	26
Wireless Pane Information and Failover Clustering.....	28
Duplicate a Configuration .....	29
Import and Export Configurations.....	30
Scheduled Component Backup of Wireless Plugin Configuration.....	31
Change Connecting Appliance of WLAN Device .....	31
Centralized Web Authentication with Cisco Wireless LAN Controllers .....	32
<b>Display Wireless Detection Information at the Console.....</b>	<b>32</b>
<b>Create Policies to Handle Detected Wireless Clients.....</b>	<b>35</b>
Wireless Client Properties .....	36
Wireless SNMP Trap Criteria .....	39
WLAN Device Properties .....	40
Wireless Admission Events .....	40
Policy Template: VR WPA2 KRACK .....	41
WLAN Actions .....	41
WLAN Block Action .....	42
WLAN Role Action.....	43
<b>Sample Policies .....</b>	<b>50</b>

Wireless User Notification – Company Security and Privacy Policy.....	50
Block Wireless Clients Exhibiting Malicious Intent .....	54
Prevent Wireless Client Access to Organizational Server Farm.....	58
<b>Displaying Wireless Inventory Information.....</b>	<b>61</b>
<b>Appendix 1: MIBs Used by the Wireless Plugin .....</b>	<b>63</b>
<b>Network Module Information .....</b>	<b>66</b>
<b>Additional Fore Scout Documentation.....</b>	<b>66</b>
Documentation Downloads .....	66
Documentation Portal .....	67
Fore Scout Help Tools.....	67

## About the Wireless Plugin

The Wireless Plugin is a component of the Forescout® Network Module. See [Network Module Information](#) for details.

The plugin provides Forescout's device visibility and control capabilities for 802.11 WLAN controllers and autonomous access points in your organization's network.

In this document, the term *Wireless LAN (WLAN) device* refers to either WLAN controllers or autonomous access points, or to both types of wireless network access management devices.

Wireless Plugin IP address range entries enable the Forescout RADIUS server to provide RADIUS-only management of wireless clients attempting to connect to the network via WLAN devices of any vendor.

Readers of this document should have a solid understanding of Forescout platform functionality and Forescout policies.

The Forescout device visibility and control capabilities that the Wireless Plugin provides include:

- Managing WLAN devices deployed in a network. The plugin can resolve WLAN device properties that classify the various types of WLAN devices in the network – controllers, autonomous access points and lightweight access points.
- Detecting lightweight access points that are being managed by a plugin-managed WLAN controller. Information about detected lightweight access points is reported in the Console.
- Displaying information about wireless clients connected to your network. For example:
  - Wireless client IP address and MAC address.
  - The wireless network name (SSID) to which the wireless client is connected.
  - The name of the wireless access point to which the wireless client is connected.
  - The wireless client's authentication method, for example, 802.1X, WPA, none.
  - The IP address of plugin-managed WLAN devices.

**All Hosts** 1bfb Online/Offline ☐ Show only unassigned

Host	IPv4 Address	Segment	MAC Address	Comment	Display Name
1bfb	10.31.1.123	10.31.1.12_2	48f5ad6d4719b1		

**Profile** Compliance All Policies

**IPv4 Address:** 10.31.1.123  
**MAC Address:** 48f5ad6d4719b1

Search  ^ v

**General**

General

Network Access

More

IPv4 Address: 10.31.1.123

Admission: Wireless Host Connected

MAC Address: 48f5ad6d4719b1

NIC Vendor: HON HAI PRECISION IND. CO.,LTD.

Windows SecureConnector Version: None

**Network Access**

WLAN AP Location: E-118 (In front of QA Networking team room)

WLAN AP Name: AP54a2.74f7.2737

WLAN Association Status: Associated/AUTHZ\_WAIT

WLAN Authentication Method: WPA2/openSystem/notavailable

WLAN BSSID: f0b2e6437390

WLAN Client Role: VLAN0311

WLAN Client User Agent: N/A

WLAN Client Username: NA

WLAN Client VLAN: 311

WLAN Client Connectivity Status: Yes

WLAN Device IP/Name: WLC31.dom31.lab.forescout.com

WLAN Device Vendor: Cisco

WLAN Detected Client Type: N/A

WLAN SSID: SWC311

More

- Assigning wireless clients a controller-defined role.
- Blocking wireless clients from connecting to the organizational network.

**All Hosts** 1bfb Online/Offline ☐ Show only unassigned

Host	IPv4 Address	Segment	MAC Address	Actions	Comment	Display Name
1bfb	10.31.1.123	10.31.1.12_2	48f5ad6d4719b1	block	block	

**WLAN Block**  
Action triggered by: policy WBlock  
Action Status: Success - OK (q31c7emha-1.Wireless)  
Press 'F2' for focus

**Profile** Compliance All Policies

**IPv4 Address:** 10.31.1.123  
**MAC Address:** 48f5ad6d4719b1

Search  ^ v

**General**

General

Network Access

More

IPv4 Address: 10.31.1.123

Admission: Wireless Host Connected

Comment: block

MAC Address: 48f5ad6d4719b1

## Wireless Network Access Device Terminology

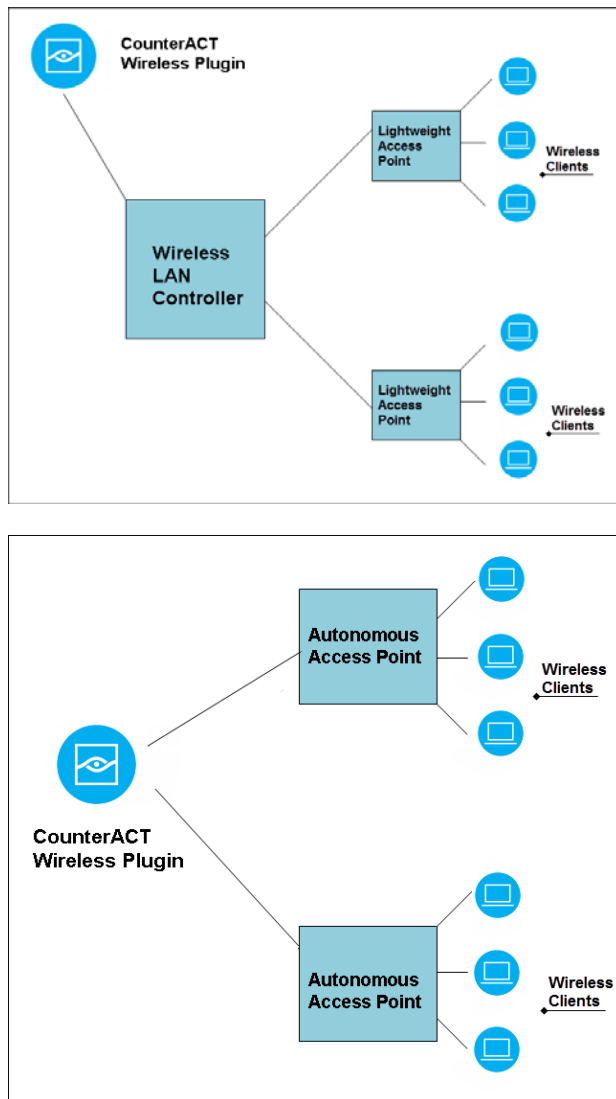
The following table describes the wireless devices referred to in this document:


Term	Short Name/Acronym	Description
<b>Autonomous Access Point</b>	<ul style="list-style-type: none"><li>▪ Autonomous AP</li><li>▪ AAP</li></ul>	<p>The autonomous access point is an access point device that supports standalone network configurations, where all configuration settings are maintained locally on the device.</p> <p>Configure the Wireless Plugin to manage autonomous access points.</p>
<b>Light Weight Access Point</b>	<ul style="list-style-type: none"><li>▪ Lightweight AP</li><li>▪ LAP</li></ul>	<p>The lightweight access point is a device that is managed by a WLAN controller and cannot act independently of the controller. Lightweight APs have no configuration until they associate with a controller. LAPs are <i>zero touch</i> deployed and are not individually configured.</p> <p>The Wireless Plugin learns of and reports information about lightweight access points that are managed by a plugin-managed WLAN controller.</p>
<b>Wireless LAN Controller</b>	<ul style="list-style-type: none"><li>▪ WLAN controller</li><li>▪ Controller</li><li>▪ WLC</li></ul>	<p>A device that manages one or more lightweight access point in the WLAN.</p> <p>The WLAN controller performs all the traditional roles of an AP, such as association or authentication of wireless clients.</p> <p>The WLAN controller provides all the configuration parameters and firmware that the lightweight access point needs in the registration process.</p> <p>Configure the Wireless Plugin to manage WLAN controllers.</p>
<b>Wireless Client</b>	<ul style="list-style-type: none"><li>▪ Wireless client</li></ul>	<p>An endpoint that attempts to connect to or is currently connected to a WLAN device or a lightweight AP.</p>

## How It Works

The Wireless Plugin polls WLAN devices for information about connected wireless clients. The information can be used to construct policy rules.

The Forescout platform can instruct the WLAN device to carry out a *Block MAC* command, for example when wireless clients are not compliant with Forescout platform policies. Blocking is based on the wireless client's MAC address. Detected MAC addresses are blocked on all wireless controllers that are configured to communicate with the plugin.



 Blocked wireless clients can be viewed at controllers as well as at the Console.

## About WLAN Controller/Lightweight Access Points

WLAN controllers are enterprise-class wireless switching platforms that manage 802.11 access points. The controller acts as a central management platform for the connected lightweight access points and wireless clients. Each controller operates a single wireless local area network (WLAN) or multiple WLANs. Each WLAN is identified by a unique Service Set Identifier (SSID). An SSID identifies a specific WLAN that is available for access by wireless clients.

The Wireless Plugin detects and reports information about the lightweight APs of the following supported vendors:

- Aruba
- Cisco
- Ruckus



## Overlapping IP Address Support

The Wireless Plugin supports working with networks that use overlapping IP addresses. For details about enabling and configuring the Forescout platform's support of overlapping IP address use in an enterprise's network, refer to the *Forescout Working with Overlapping IP Addresses How-to Guide*. See [Additional Forescout Documentation](#) for information on how to access this document.

## IPv6 Support

The Wireless Plugin provides IPv6-related support for the managed WLAN devices of all supported wireless vendors, as follows:

- The plugin can manage both dual-stack WLAN devices and IPv6-only WLAN devices, as WLAN device management is accomplished using either a WLAN device IPv4 address or a WLAN device IPv6 address.
- The plugin reports IPv6 address information [IPv6 addresses and IPv6 link-local address] of IPv6 endpoints that are connected to Aruba, Cisco and Cisco Aironet WLAN devices. This support is provided for both **IPv6-only endpoints** and **dual-stack endpoints**.
- Plugin-provided WLAN actions can be applied on connected IPv6-only endpoints and connected dual-stack endpoints.

For information about overall Forescout IPv6-related support, refer to the *Forescout Administration Guide*. For information about required configurations for the Forescout platform's handling of IPv6 endpoints, refer to the *Work with IPv6 Addressable Endpoints How-to Guide*. See [Additional Forescout Documentation](#) for information on how to access these guides.

## Failover Clustering Support

The Wireless Plugin supports the Forescout platform's Failover Clustering functionality. Failover Clustering provides for the continuous operational availability of the Forescout platform's service, in the event of Appliance failure (one Appliance, many Appliances or an entire data center of Appliances). Both endpoints handled by and WLAN devices managed by the failed Appliance(s) are automatically transferred to designated Appliances having available capacity. Refer to the *Forescout Resiliency and Recovery Solutions User Guide* for detailed information about this feature. See [Additional Forescout Documentation](#) for information on how to access this guide.

To work with Failover Clustering, ensure that you have the relevant product license that supports the feature. The type of license required depends on which licensing mode your deployment is using. Refer to the *Forescout Resiliency and Recovery Solutions User Guide* for more information.

In support of the Forescout platform's Failover Clustering, the Wireless Plugin provides continuity of WLAN device handling, including applied WLAN actions, in the event of Appliance *failover* to a *recipient* Appliance and subsequent *fallback* to the reconnected *original* Appliance.

For details about the effect of Failover Clustering on Wireless Plugin processing, see [Wireless Pane Information and Failover Clustering](#).

## Appliance Management Processing Load

Deploying Wireless Plugin operation in your Forescout Appliances requires you to be aware of the management processing load that is required of these Appliances and, if necessary, adjust that processing load among Appliances.

For the recommended maximum number of WLAN devices that an Appliance can manage, refer to the [Appliance Specifications](#). Use the provided information to plan for the use of Wireless Plugin operation in Forescout devices.

## Supported Vendor Products

For information about the vendor models (hardware/software) and versions (product/OS) that are validated for integration with this Forescout component, refer to the [Forescout Compatibility Matrix](#).

## What to Do

To work with the Wireless Plugin, do the following:

1. Verify that all requirement are met. See [Requirements](#).
2. [Configure the plugin](#).
3. Set up your WLAN device to communicate with the Forescout platform. See [WLAN Device – Read/Write Settings](#).
4. [Verify the plugin is running](#).
5. [Test the plugin](#).
6. Set up the Forescout platform to view wireless client detections. See [Display Wireless Detection Information at the Console](#).
7. Create Forescout platform policies that manage wireless clients. See [Create Policies to Handle Detected Wireless Clients](#).

## Requirements

This section describes the requirements for configuring and running the Forescout Wireless Plugin.

### Forescout Requirements

The following Forescout platform and component versions must be running in your Enterprise Manager and your Appliances:

- Forescout interim release 8.2.1
- Network Module 1.2.1 with the Wireless Plugin
- In order for Wireless Plugin *IP address range* to enable Forescout RADIUS-only management of wireless clients, the Authentication Module 1.2.1 with the RADIUS Plugin running is required.

## Networking Requirements

Network connectivity between the ForeScout Appliance and a WLAN device is required for plugin management of the WLAN device.

## WLAN Device – Read/Write Settings

For Wireless Plugin management of a WLAN device, configuration of the following read/write settings in the WLAN device is required:

WLAN Device	Read/Write Setting Configuration
<b>AeroHive Access Point</b>	<ul style="list-style-type: none"> <li>▪ SNMP read access to perform queries</li> <li>▪ SSH or Telnet write access to apply the <i>WLAN Block</i> action on wireless clients</li> </ul>
<b>Aruba Networks Controller</b>	<ul style="list-style-type: none"> <li>▪ SNMP or CLI (SSH or Telnet) read access to perform queries</li> <li>▪ SSH or Telnet write access to apply the WLAN management actions, <i>WLAN Block</i> and <i>WLAN Role</i>, on wireless clients</li> </ul>
<b>Cisco Controller</b>	<ul style="list-style-type: none"> <li>▪ SNMP read access to perform queries</li> <li>▪ To apply WLAN management actions, <i>WLAN Block</i> and <i>WLAN Role</i>, on connected wireless clients, the plugin uses any of the following methods: <ul style="list-style-type: none"> <li>- CLI (SSH or Telnet) privilege mode write access</li> <li>- SNMP write access</li> </ul> </li> </ul> <p><i>Note: The WLAN Role action is not supported for use on Cisco controllers that run the IOS-XE operating system.</i></p>
<b>Cisco Aironet Access Point</b>	<ul style="list-style-type: none"> <li>▪ SNMP or CLI (SSH or Telnet) read access to perform queries. <ul style="list-style-type: none"> <li>- Plugin CLI read access is required for the plugin to obtain/report the IPv6 address information of connected IPv6 endpoints</li> </ul> </li> <li>▪ SSH or Telnet write access to apply the <i>WLAN Block</i> action on wireless clients</li> </ul>
<b>Extreme Controller (Enterasys)</b>	<ul style="list-style-type: none"> <li>▪ SNMP read access to perform queries</li> </ul>
<b>HP Controller</b>	<ul style="list-style-type: none"> <li>▪ CLI (SSH or Telnet) read access to perform queries.</li> <li>▪ CLI (SSH or Telnet) write access to apply the <i>WLAN Block</i> action on wireless clients</li> </ul>
<b>Huawei Controllers</b>	<ul style="list-style-type: none"> <li>▪ SNMP read access to perform queries</li> <li>▪ SSH or Telnet write access to apply the <i>WLAN Block</i> action on wireless clients</li> </ul>
<b>Meru Networks Controller</b>	<ul style="list-style-type: none"> <li>▪ SNMP read access to perform queries</li> <li>▪ SSH or Telnet write access to apply the <i>WLAN Block</i> action on wireless clients</li> </ul>
<b>Extreme Controller (Motorola)</b>	<ul style="list-style-type: none"> <li>▪ SNMP or CLI (SSH or Telnet) read access to perform queries</li> <li>▪ SSH or Telnet write access to apply the <i>WLAN Block</i> action on wireless clients</li> <li>▪ CLI Read and Write access to apply <i>WLAN Role</i> action on wireless clients. The plugin edits the Wireless Client Role Policy in the Extreme Controller (Motorola), and assigns a VLAN.</li> </ul>

WLAN Device	Read/Write Setting Configuration
<b>Ruckus Controller</b>	<ul style="list-style-type: none"> <li>▪ SNMP read access to perform queries</li> <li>▪ SSH or Telnet write access to apply the <i>WLAN Block</i> action on wireless clients</li> </ul>
<b>Siemens Controller</b>	<ul style="list-style-type: none"> <li>▪ SNMP or CLI (SSH or Telnet) read access to perform queries</li> <li>▪ SSH or Telnet write access to apply the WLAN management actions, <i>WLAN Block</i> and <i>WLAN Role</i>, on wireless clients</li> </ul>
<b>Xirrus Controller</b>	<ul style="list-style-type: none"> <li>▪ SNMP read access to perform queries</li> <li>▪ SNMP write access to apply the <i>WLAN Block</i> action on wireless clients</li> </ul>

In addition to the configuration of its read/write settings, plugin-managed WLAN devices need to be configured to allow them to send SNMP traps to the Forescout platform/Wireless Plugin.

## Required WLAN Device Configuration

In addition to configuring the Wireless Plugin to manage supported vendor WLAN devices, the WLAN devices themselves must be properly configured to work with the Forescout platform.

- When configuring WLAN devices for network deployment, do not use an SSID value as a WLAN device host name (<WLAN device hostname> **must NEVER** = <an SSID in your wireless network>)

For additional information about the necessary WLAN device configurations, refer to the following Forescout documents:

- AeroHive: [Forescout® Wireless Plugin Integration with AeroHive Access Points Configuration Guide](#)
- Aruba Networks: [Forescout® Wireless Plugin Integration with Aruba Controllers Configuration Guide](#)
- Cisco: [Forescout® Wireless Plugin Integration with Cisco Wireless Management Configuration Guide](#)
- Meru Networks: [Forescout® Wireless Plugin Integration with Meru Wireless Controllers Configuration Guide](#)
- Motorola (Extreme): [Forescout® Wireless Plugin Integration with Motorola Controllers Configuration Guide](#)
- Xirrus: [Forescout® Wireless Plugin Integration with Xirrus Wireless Controllers Configuration Guide](#)

## Configure the Plugin

The plugin configuration lets you connect WLAN devices to Forescout Appliances and assign the read/write permissions used to query and block wireless clients.

## Configuration

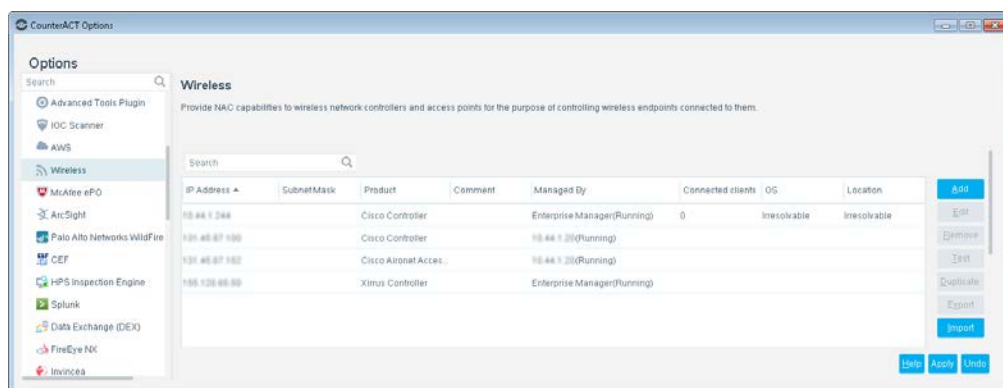
Configure the Wireless Plugin to manage WLAN devices. The configured Wireless Plugin running on Forescout Appliances is then able to execute the following plugin activities:

- Connect to the WLAN devices
- Assign read/write permissions used for querying the devices for information.
- Apply WLAN actions to detected wireless clients that are connected to a plugin-managed WLAN device. Forescout

This section describes how to configure the Wireless Plugin.

### To configure the plugin:

1. From the Console **Tools** menu, select **Options > Modules > Network > Wireless > Configure**. The Wireless pane opens.



2. Select **Add**. The Add Wireless Device wizard opens and displays the General pane.

**Add wireless - Step 1**

**Add Wireless Device**

**General**

Configure the Wireless Plugin to do any of the following:

1. Manage supported WLAN devices
2. Enable ForeScout RADIUS authentication/authorization of connecting wireless clients. Select **RADIUS-only Management** in the Product field and define the IP address range of the WLAN devices

Product: Aruba Controller

Address:

Connecting Appliance: Enterprise Manager

IP Reuse Domain: (none)

Comment:

**Read Connection Method**

☒ SNMP

☐ Command Line

**Write Permission**

☒ Enable WLAN management actions using Command Line

**Miscellaneous**

☐ Without colons, i.e: 00016ccc8a6d

☒ With colons, i.e: 00:01:6c:cc:8a:6d

Help Previous Next Finish Cancel

At this point in the configuration process, the following configuration paths are available:

- **WLAN Device Management Configuration:** Configure a WLAN device for Wireless Plugin management. To continue with this configuration process flow, see [WLAN Device Management Configuration](#).
- **IP Address Range Configuration:** Configure a Wireless Plugin IP address range entry. IP address range information enables the ForeScout RADIUS server to provide RADIUS-only management of wireless clients attempting to connect to the network via WLAN devices of any vendor. To continue with this configuration process flow, see [Enable ForeScout RADIUS-only Management of Wireless Clients](#).

## WLAN Device Management Configuration

This section provides the configuration process to use in order to configure the Wireless Plugin to manage a supported WLAN device.

## General Configuration

### In the General pane:

1. In the **Product** field, select a supported WLAN device vendor.
2. In the **Address** field, enter the IP/FQDN of the WLAN device that the plugin is to manage. This entry can be any of the following:
  - An IPv4 address
  - A fully qualified domain name (FQDN)
  - An IPv6 address

The value you configure is then used throughout the Console to identify the WLAN device entry.

When an FQDN is provided, the Forescout platform resolves the FQDN to learn the IP address of the WLAN device.

Forescout platform support of networks with overlapping IP addresses deals with the overlap of IPv4 addresses only.

When the Forescout platform is enabled to support overlapping IP addresses, you can configure the plugin to manage multiple WLAN devices all having the same IP address, however for this to be valid, each of these WLAN devices must be located within a different IP Reuse Domain (IRD). See the General pane's [IP Reuse Domain field](#).

3. In the **Connecting Appliance** field, select a Forescout device. If your Forescout deployment includes multiple Appliances connected to an Enterprise Manager, it is recommended to select an Appliance that is physically close to the WLAN device you are adding.
4. The **IP Reuse Domain** field only appears in the *General* pane/tab when the Forescout platform is enabled to support overlapping IP addresses. The field is view-only.

*IP Reuse Domains* are used to distinguish several instances of an overlapping IP address. IP addresses are unique in each IP Reuse Domain and cannot overlap within a domain.

In order for this field to display an IP Reuse Domain, the following conditions must both be true:

- a. The selected Connecting Appliance has an assigned IP Reuse Domain
- b. The WLAN device's IP address is located within the Connecting Appliance's IP segment assignment (scope) that is assigned to the IP Reuse Domain

Otherwise, the field displays the value (*none*) that identifies that the WLAN device is not located within an IRD but, rather, is located within the enterprise's default/global network.

5. In the *optional Comment* field, enter descriptive text about the WLAN device and/or the configuration.
6. If either *Aruba*, *Siemens* or *Motorola Controller*, or *Aironet Access Point* is selected in the **Product** field, then define the following:
  - a. The **Read Connection Method** section - define the method the plugin must use to connect to the WLAN device. Available options: either **SNMP** or **Command Line**.
  - b. The **Write Permission** section - enable or disable the plugin's ability to apply available WLAN management actions. Either select or clear the **Enable WLAN management actions using Command Line** checkbox.
  - c. The **Miscellaneous** section (*Aruba Controller only*) - specify the format that the plugin must use when sending the MAC address of wireless clients to an Aruba Controller. Available options: either **Without colons** or **With colons**. By default, colons are used as delimiters in the MAC address.
7. If either *Cisco Controller* or *Xirrus Controller* is selected in the **Product** field, then define following in the **Write Permission** section:

Enable or disable the plugin's ability to apply available WLAN management actions. Either select or clear the **Enable WLAN management actions** checkbox.
8. If either *an AeroHive Controller*, *a Meru Controller*, *a Huawei Controller*, or *a Ruckus Controller* is selected in the **Product** field, then define the following in the **Write Permission** section:

Enable or disable the plugin's ability to apply available WLAN management actions. Either select or clear the **Enable WLAN management actions using Command Line** checkbox.
9. Select **Next**. The SNMP pane opens.

When the **Enable WLAN management actions** option is disabled for any managed WLAN device of any supported product vendor, the Wireless Plugin does not apply WLAN management actions (*WLAN Block* and *WLAN Role*) on wireless clients that are connected to the managed WLAN device. See [WLAN Actions](#) for information about the support for use of the WLAN management actions. See [Create Policies to Handle Detected Wireless Clients](#) for more information about blocking wireless clients.



## SNMP Configuration

The plugin uses the information defined in the SNMP pane to connect to and query the managed WLAN device and retrieve information about its connected wireless clients. One example of retrieved information is the wireless network to which the wireless client is connected. See [WLAN Device – Read/Write Settings](#).

The information that you configure in the SNMP pane must match the SNMP configurations defined in the WLAN device.

**Add Wireless Device**

General

SNMP

Command Line

802.1X

**SNMP**

The information defined here is used by the plugin to retrieve information about hosts connected to the wireless device, and to apply management actions to endpoints.

Wireless Query Interval (Seconds) 60

SNMP Version V1

Community

Confirm Community

Help Previous Next Finish Cancel

### In the SNMP pane:

1. For AeroHive, Aruba, Cisco, Motorola and Ruckus controllers, the SNMP pane makes available the **Enable Notification Traps** checkbox. Select this checkbox to instruct the plugin to accept receipt of SNMP notification traps that are sent to it by the managed WLAN device.

**Add Wireless Device**

General

SNMP

Command Line

802.1X

**SNMP**

The information defined here is used by the plugin to retrieve information about hosts connected to the wireless device.

☒ Enable Notification Traps

Wireless Query Interval (Seconds) 600

SNMP Version V1

Community

Confirm Community

Help Previous Next Finish Cancel

Notification of newly connected wireless clients, via these traps, is received from the managed WLAN devices in near real-time.

A received trap includes the MAC address and the IP address of the wireless client; the plugin can then query the WLAN device for all other wireless client information.

2. In the **Wireless Query Interval** field, specify in seconds the WLAN device query interval.
  - a. For AeroHive, Aruba, Cisco, Motorola and Ruckus controllers, the default, query interval value is 600 seconds (10 minutes), due to their support of SNMP traps.
  - b. For all other WLAN devices, the default value is 60 seconds (1 minute).
3. In the **SNMP Version** field, select the SNMP version from the drop-down menu.


For an Aruba, Siemens or Motorola controller, or Cisco Aironet access point, if the **Command Line** option is selected in the **Read Connection Method** section of the General pane, both the **SNMP Version** and **Community** fields are not available for data entry. For an HP controller, both the **SNMP Version** and **Community** fields are not available for data entry, as the plugin read method is CLI for this product.

- a. When either **V1** or **V2** is selected, in the **Community** field enter a community relevant to your SNMP version selection. Continue with step [5](#).
- b. When **V3** is selected, the following fields display:

The screenshot shows a configuration form for SNMP V3. The 'SNMP Version' dropdown is set to 'V3'. Below it are fields for 'User', 'Use Authentication' (checkbox), 'Authentication Protocol' (set to 'HMAC-SHA'), 'Password', 'Confirm Password', 'Use Privacy' (checkbox), 'Privacy Protocol' (set to 'DES'), 'Password', 'Confirm Password', 'Use Explicit Engine ID' (checkbox), and 'Engine ID Value' (set to '0').

Continue with step [4](#).

4. For plugin SNMP **V3** communication, configure the following fields:
  - a. In the **User** field, enter a user name.
  - b. Select **Use Authentication** to enable authentication. Enter applicable password and select the authentication protocol to use. Plugin-supported authentication protocols:
    - > HMAC-MD5
    - > HMAC-SHA

- c. Select **Use Privacy** to enable privacy. Enter applicable password and select the encryption protocol to use. Plugin-supported encryption protocols:
  - > DES
  - > AES
-  *Configuring the plugin to use **Privacy** requires that you also configure the plugin to use **Authentication**.*
- d. In SNMPv3 communication, the Engine ID uniquely identifies each SNMP agent for queries and trap handling. Engine ID configuration options:
  - > When managed WLAN devices in the network use default engine IDs, then the plugin automatically discovers the engine ID value. In this case, clear the **Use Explicit Engine ID** checkbox.
  - > When managed WLAN devices use operator-assigned engine ID values, automatic discovery of engine IDs by the plugin might not succeed. In this case, explicitly specify an engine ID value by selecting the **Use Explicit Engine ID** checkbox and specifying the **Engine ID Value**. For example, an explicit engine ID must be specified to define the Fore Scout platform as a Trap Receiver in Aruba 620 controllers.

5. Select **Next**. The Command Line pane opens.

### Command Line Configuration

In the Command Line pane, configure the connection method and log in credentials that the Wireless Plugin uses when managing the WLAN device with CLI. Plugin management activities includes querying the managed WLAN device for information and applying WLAN management actions - the *WLAN Block* and the *WLAN Role* actions - on wireless clients that are connected to the managed WLAN device. See [WLAN Device – Read/Write Settings](#).

In the Command Line pane, the **Use Command Line** checkbox is available:

- For Aruba, Siemens or Motorola controllers, or Cisco Aironet access points, when either one of the following General pane options is selected:
  - The **Command Line** option
  - The **Enable WLAN management actions using Command Line** checkbox
- For Cisco controllers, when the **Enable WLAN management actions** checkbox is selected in the General pane.
- For AeroHive, Meru, *Huawei*, and Ruckus controllers, when the **Enable WLAN management actions using Command Line** checkbox is selected in the General pane.

With Xirrus controllers the Command Line pane displays, however, all its fields are disabled. The plugin only uses SNMP to apply WLAN management actions on Xirrus controllers.

**Add Wireless Device**

General  
SNMP  
Command Line 802.1X

**Command Line**

Select **Use Command Line**  
Select SSH or Telnet and enter login and privilege mode credentials for managing Command Line options defined in the **General tab**. Define the maximum time for the plugin to wait for a response from the device.

☐ Use Command Line

**Login Parameters**

Connection method: SSH

User:

Password:

Confirm password:

☒ Enable privilege

Privileged password:

Confirm privileged password:

CLI timeout (seconds): 5

Help Previous Next Finish Cancel

#### In the Command Line pane:

1. Select the **Use Command Line** checkbox. When selected, the rest of the fields in the pane are enabled.
2. In the **Connection method** field, select SSH or Telnet to define the method that the plugin uses to establish a connection for management via CLI.
3. In the **User** and **Password** fields, enter the login credentials that the plugin uses to access the WLAN device.
4. If managing the WLAN device requires the Wireless Plugin to use CLI privilege mode write access and the provided login credentials are not of the privilege mode type, do the following:
  - a. Select the **Enable privilege** checkbox.  
This option is not needed for plugin management of an HP controller.
  - b. In the **Privileged password** field, enter the privilege mode password.
  - c. In the **CLI timeout** field, specify in seconds the maximum amount of time that the plugin must wait to receive the response of the managed WLAN device, after sending it a CLI command.
    - > For Motorola controllers, the default CLI timeout value is 60 seconds (1 minute).
    - > For all other, managed WLAN devices, the default CLI timeout value is 5 seconds.
5. Do one of the following:
  - a. If the Forescout RADIUS Plugin is not installed, select **Finish**.
  - b. If the Forescout RADIUS Plugin is installed, select **Next** and continue with the section [RADIUS Integration](#).

At some point in the future, if you need to disable the **Use Command Line** option for the managed controller, make sure that *BEFORE* disabling this option

you first cancel all *WLAN Block* actions. Accomplish this action cancellation using any of the following methods:

- Stop the Wireless Plugin
- Stop all policies that use the *WLAN Block* action
- Cancel all manually applied *WLAN Block* actions

## Enable Forescout RADIUS-only Management of Wireless Clients

Using the Wireless Plugin, you can configure an IP address range of WLAN devices, which enables the following Forescout RADIUS-only management use cases:

- Enable the RADIUS-only authentication and authorization of wireless clients associating with any one of a group of access points that are deployed in the configured IP address range. The group of access points can be of any vendor and must support RADIUS.

This use case requires the configuration of an IP address range that combines:

- An *<IP address network segment>* with a subnet mask=*<a value between 1 - 31>*.

- Enable the RADIUS-only authentication and authorization of wireless clients associating with a specific, single wireless controller. The wireless controller can be of any vendor and must support RADIUS.

This use case requires the configuration of a single IP address composed as follows:

- An *<IP address network segment>* with the subnet mask=32.

Wireless Plugin actions and properties are not available with either of these RADIUS-only integrations, since the plugin does not manage the WLAN devices that are deployed in these types of integrations.

This section provides the process for configuring Wireless Plugin IP address range entries. For details about configuring the Forescout RADIUS server to provide RADIUS-only authentication and authorization, refer to the *Forescout RADIUS Plugin Configuration Guide*, which is provided by the required Authentication Module version. See [Additional Forescout Documentation](#) for information on how to access this guide.

## General Configuration

### In the General pane:

1. In the **Product** field, select the option ***RADIUS-only Management***. The General pane changes.

2. In the **NAS Vendor** field, select the type of NAS device to which these settings apply. Based on this setting, RADIUS requests and other interactions use the format and attribute-value pairs expected for devices of the specified vendor.
3. In the **Address** field, define an IPv4 or IPv6 address range in address/netmask format.

- The provided IP address network segment cannot overlap with that of any existing IP address range entry.*
- You cannot define an IP range that contains the IP address of an existing managed WLAN device. However, you can define an individual device with an IP address within the range of an existing RADIUS-only configuration profile.*
- The identical SNMP Community information and the identical RADIUS Secret must be configured for all access points, of all vendors, in the specified IP address range. **The plugin does not validate for this requirement.***

4. In the *optional* **Comment** field, enter descriptive text.
5. Select **Next**. The SNMP pane opens.

## SNMP Configuration

The purpose of this pane is to configure valid SNMP credentials so the Fore Scout RADIUS server, in the RADIUS Plugin, can use SNMP, in addition to using the RADIUS CoA and RADIUS POD protocols, to issue wireless client re-authentication requests to an AP. Configuration of SNMP credentials is **optional**.

The information that you configure in the SNMP pane must match the SNMP configurations defined in the WLAN device.

- The identical SNMP Community information must be configured for all WLAN devices (both individual Wireless Plugin-managed and Access Point IP Address Range) that are deployed in the same IP address range. **The plugin does not validate for this requirement.***

**In the SNMP pane:**

1. Select the **Use SNMP** checkbox. When selected, the rest of the fields in the pane are enabled.
2. In the **SNMP Version** field, select the SNMP version.
  - a. When either **V1** or **V2** is selected, in the **Community** field enter a community relevant to your SNMP version selection. Continue with step 4.
  - b. When **V3** is selected, the following fields display:

SNMP Version: V3 ▼

User:

☒ Use Authentication

Authentication Protocol: HMAC-SHA ▼

Password:

Confirm Password:

☐ Use Privacy

Privacy Protocol: DES ▼

Password:

Confirm Password:

Continue with step 3.


3. For plugin SNMP **V3** communication, configure the following fields:
  - a. In the **User** field, enter a user name.
  - b. Select **Use Authentication** to enable authentication. Enter applicable password and select the authentication protocol to use. Plugin-supported authentication protocols:
    - > HMAC-MD5
    - > HMAC-SHA
  - c. Select **Use Privacy** to enable privacy. Enter applicable password and select the encryption protocol to use. Plugin-supported encryption protocols:
    - > DES
    - > AES

 *Configuring the plugin to use **Privacy** requires that you also configure the plugin to use **Authentication**.*

4. Select **Next**. The 802.1X pane opens.

## 802.1X Integration

Configure the fields in this tab if your Forescout deployment provides RADIUS-based authentication and authorization of detected endpoints that connect to your organization's network switches.

 To ensure consistent 802.1X behavior, review 802.1X integration settings in the RADIUS Plugin before you configure the options of this pane. In the Console, select **Tools** > **Options** > **Modules.** > **Authentication** > **RADIUS**. Review the RADIUS plugin configuration and select **Help** to learn more about the RADIUS implementation options that are supported.

The 802.1X tab contains the following settings:

<b>RADIUS Secret as configured in switches</b>	<p>The RADIUS secret for communication between the Forescout RADIUS server and switches managed by the plugin.</p> <ul style="list-style-type: none"> <li>Specify the same RADIUS Secret for all switch devices in the same IP address range. <b>The plugin does not validate for this requirement.</b></li> </ul>
<b>CoA Port</b>	<p>The port used for Change of Authorization requests.</p>
<b>CoA Identification Attributes</b>	<p>Specify the attribute-value pairs included in Change of Authorization requests.</p> <ul style="list-style-type: none"> <li>Select Vendor Defaults to use the default Session Identification attributes and NAS Identification attributes that the Forescout platform has learned for devices of this vendor.</li> <li>Select Custom to manually specify the Session Identification attributes and NAS Identification attributes that are included in CoA requests.</li> </ul>

## Control Plugin Query about Lightweight Access Points

In order for the Wireless Plugin to detect and resolve property information about supported vendors' lightweight access points, the Wireless Plugin queries the relevant WLAN controller about the lightweight access points that the controller manages. The following Forescout property controls the frequency with which the Wireless Plugin queries a relevant WLAN controller about the lightweight access points that are under its management:

- `conf.wireless_query_aps_interval.value`

This property is defined per Appliance and its property's default value is 600 seconds (10 minutes).

### To modify the query frequency property value:

- Log in to the CLI on the Appliance
- Run the following command using an SSH connection:

```
fstool wireless set_property
conf.wireless_query_aps_interval.value <number of seconds>
```

## Verify That the Plugin Is Running

After configuring the plugin, verify that it is running.

### To verify:

- Select **Tools**>**Options** and then select **Modules**.
- Navigate to the plugin and select **Start** if the plugin is not running.



## Test the Plugin Configuration for WLAN Device Management

The Wireless Plugin test verifies the following:

- Connectivity between the Forescout platform and the WLAN Device:
  - SSH/Telnet protocols: Tests connectivity using the credentials defined in the plugin.
  - SNMP protocol: Tests connectivity to the WLAN device and tests access to the WLAN device OIDs required for querying and retrieving information on connected wireless clients.
- WLAN Device Query: Identifies how many wireless clients are connected to the configured WLAN device.
- SNMP Traps: This test is performed for AeroHive, Aruba, Cisco, Motorola, and Ruckus controllers. The test verifies whether or not the **Enable Notification Traps** option is selected in the plugin configuration for management of the controller.

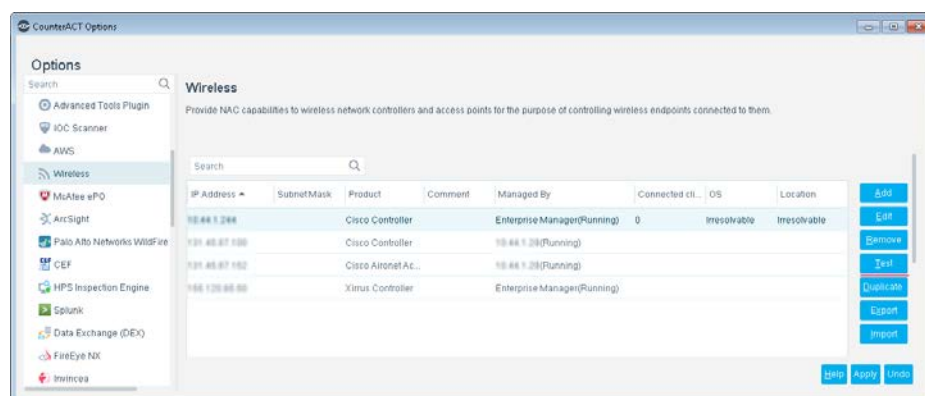
Test the plugin configuration for managing:

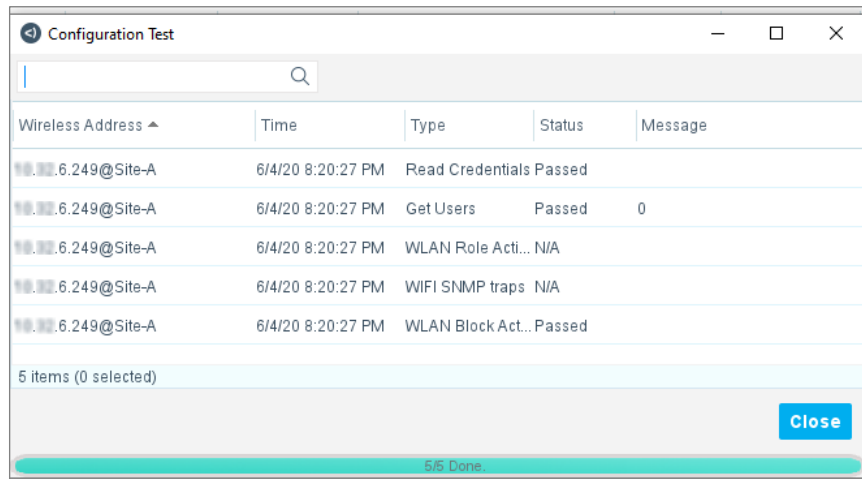
- A WLAN device
- Multiple WLAN devices

The plugin configuration test is not available to perform for Access Point IP Address Range entries.

### To run a test:

1. Select **Options** from the **Tools** menu. The Options pane opens.
2. Open the **Modules** folder and select **Wireless**. The Wireless pane opens.
3. Select one or more WLAN devices and then select **Test**.





Wireless Address ^	Time	Type	Status	Message
10.10.10.6.249@Site-A	6/4/20 8:20:27 PM	Read Credentials	Passed	
10.10.10.6.249@Site-A	6/4/20 8:20:27 PM	Get Users	Passed	0
10.10.10.6.249@Site-A	6/4/20 8:20:27 PM	WLAN Role Acti...	N/A	
10.10.10.6.249@Site-A	6/4/20 8:20:27 PM	WIFI SNMP traps	N/A	
10.10.10.6.249@Site-A	6/4/20 8:20:27 PM	WLAN Block Act..	Passed	

5 items (0 selected)

Close

5/5 Done

When a tested WLAN device is located within an IP Reuse Domain (IRD), its entry in the Wireless Address column displays that IRD as a suffix of the WLAN device's IP address, in the form <IP address>@<IRD>.

## Troubleshooting

- **The device is not assigned to a Forescout Appliance.** This can occur when you import predefined device settings. No Forescout Appliance manages the device, so the test of communication with the Forescout platform does not complete successfully. In this case, the value in the Managed By column is **Unassigned** for the device.

Select the device and select **Edit** to assign the device to a Forescout Appliance.

- Due to the nature of the response to the plugin's *Get Users* test that is sent from the WLAN device of some vendors, when the device's User table is empty, the plugin reports this test as *failed* with the accompanying message *Failed to read mobile client mibs, SNMP error [Requested table is empty or does not exist]*. In the given scenario, the *Get Users* test actually succeeds; the plugin uses the appropriate MIB OID to retrieve the device's User table, however, the table happens to be empty at that point in time. Take note that there can be legitimate test failure scenarios for which the plugin reports the same failure message.

## Verify Plugin Processing of SNMP Traps

When your Forescout platform deployment is operating, if the Wireless Plugin is configured to receive SNMP traps from plugin-managed WLAN devices, you can *optionally* verify that the plugin is correctly processing these received traps. See [Wireless SNMP Trap Criteria](#)

## Wireless Pane Display

The Console's *Wireless* pane displays information about the WLAN devices that the plugin is configured to manage. Access the *Wireless* pane via the following Console selections: **Tools** menu > **Options** > **Modules** > **Network** > **Wireless** > **Configure**.

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

Search

IP Address ▲	SubnetMask	Product	Comment	Managed By	Connected clients	OS	Location	IP Reuse Domain
1.1.1.1		Aruba Controller		Enterprise Manager(Running)	0			
2.2.2.2		Aruba Controller		192.168.210.23	0			
3.3.3.3		Aruba Controller		Enterprise Manager(Running)	0			

3 items (0 selected)

The **Wireless** pane can display the following WLAN device information:

Column	Description
<b>Comment</b>	The presented text is taken from the <i>Comment</i> field of the <i>General</i> pane/tab.
<b>Connected clients</b>	The number of wireless clients that are connected to the wireless device.
<b>IP Address</b>	The IP address of the plugin-managed wireless device. This information is defined in the <i>IP Address</i> field of the <i>General</i> pane/tab.  When the WLAN device is located within an IP Reuse Domain (IRD), that IRD displays as a suffix of the IP address, in the form <i>&lt;IP address&gt;@&lt;IRD&gt;</i> . For example, 192.168.2.202@SITE – B.
<b>IP Reuse Domain</b>	This column is only available for display in the <i>Wireless</i> pane when the Forescout platform is enabled to support overlapping IP addresses.  Displays the IRD in which the WLAN device is located.  A blank entry identifies that the WLAN device is located within the enterprise's default/global network.
<b>Last Trap Received</b>	Time of plugin receipt of the most recent SNMP trap from the wireless device.
<b>Location</b>	
<b>Managed APs</b>	The number of lightweight access points that are being managed by the plugin-managed WLAN controller.
<b>Managed By</b>	The Forescout device (either the Enterprise Manager or an Appliance), which is identified either by name or address (IP/FQDN), currently responsible for managing the wireless device and either one of the following statuses: <ul style="list-style-type: none"> <li>The status of the Wireless Plugin on the Enterprise Manager/Appliance</li> <li>The status of the Enterprise Manager/Appliance, currently responsible for managing the wireless device when that Enterprise Manager/Appliance is disconnected.</li> </ul>
<b>OS</b>	Operating system information of the wireless device.

Column	Description
<b>Product</b>	The vendor wireless device. This information is defined in the <i>Product</i> field of the <i>General</i> pane/tab.
<b>Subnet Mask</b>	The subnet mask that is provided in the <i>Address</i> field of the <i>General</i> pane/tab, when defining the IP address range for RADIUS-only management of wireless clients.

📄 *Not all columns display by default. To edit the display, right-click a column heading and select **Add/Remove Columns**.*

## Wireless Pane Information and Failover Clustering

Plugin configuration definitions of managed WLAN devices are displayed in the Wireless pane. During a failover scenario, the Wireless pane displays the following information in the **Managed By** column for managed WLAN devices that are currently failed over to a *recipient* Appliance:

- *<current managing Appliance, after failover> \*(<current managing Appliance status>)*

Wireless						
Provide NAC capabilities to wireless network controllers and access points for the purpose of controlling wireless endpoints connected to them.						
Search						
IP Address ▲	Product	Comment	Managed By	Connected clients	OS	Location
24.10.1.1	Aruba Controller		15.10.5.50 *(Running)	0	ArubaOS (MODEL: Aruba...	QA Lab
24.10.1.1	Cisco Controller	ios-XE	15.10.5.50 *(Running)	0	Cisco IOS Software, IOS-...	Lab-Q2
24.10.1.1	Cisco Controller		15.10.5.50 *(Running)	0	Cisco Controller (7.0.240.0)	Lab-QA2

A **Managed By** column tooltip is displayed for managed WLAN devices that are currently failed over to a *recipient* Appliance. The tooltip contains the following information:

- **Current:** Current managing Appliance, after failover.
- **Original:** Original managing Appliance, prior to failover.
- **Plugin status:** *The plugin status on the current Appliance is <plugin status>.*

d access points for the purpose of controlling wireless endpoints connected to		
Managed By	Connected clients	OS
15.10.5.50 *(Running)	0	ArubaOS (MODE
15.10.5.50		Cisco IOS Softwa
15.10.5.50		Cisco Controller

For information about the Forescout platform's *Failover Clustering* and the Wireless Plugin, see [Failover Clustering Support](#).

## Duplicate a Configuration

Often, controllers in a network share the same basic configuration. After you configure communication with a controller of a certain type, use the Duplicate option to apply that configuration to other instances of the same controller. For example, you can configure and test connection parameters for Motorola controllers, then duplicate these settings for all Motorola controllers in the network. You provide the IP/FQDN of each new WLAN device, which can be any of the following:

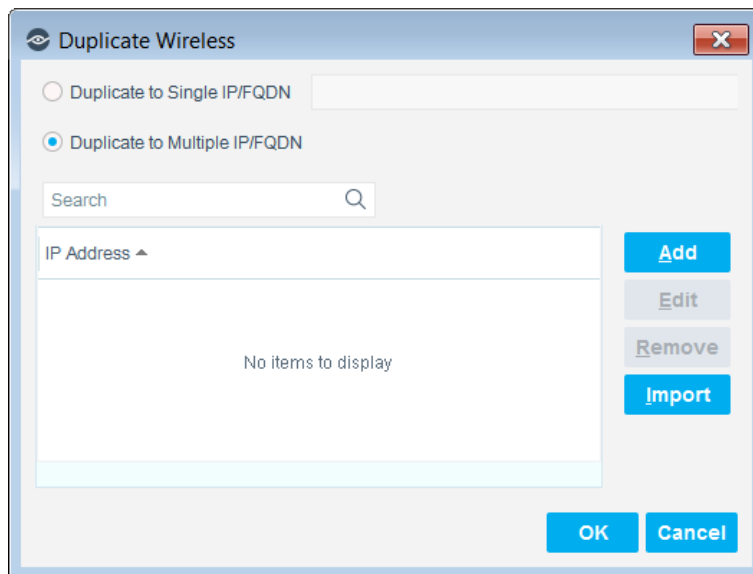
- An IPv4 address
- An FQDN
- An IPv6 address

Alternatively, you can import a list of IP/FQDN from a CSV file rather than having to manually enter them.

You cannot duplicate the configuration of Access Point IP Address Range entries.

### To duplicate a configuration:

1. Select **Options** from the **Tools** menu at the Console.
2. Select **Wireless**. The Wireless pane opens.
3. Select a wireless device configuration. Then select **Duplicate**. The Duplicate Wireless dialog appears.



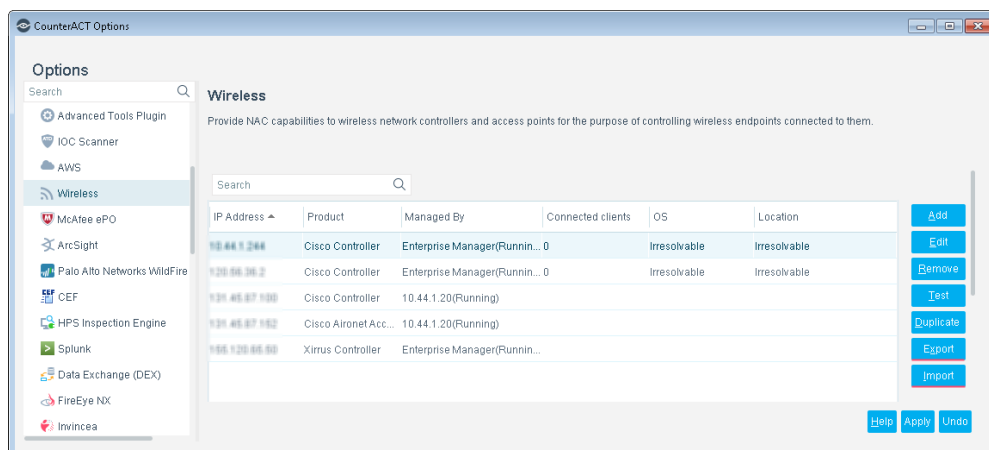
4. Do one of the following:
  - a. To create a single new instance of the selected controller (the default selection), enter the IP/FQDN of the new controller in the **Duplicate to Single IP/FQDN** field.
  - a. To create multiple new instances of the selected controller, select the **Duplicate to Multiple IP/FQDN** option and select **Add** to add the IP/FQDN of the new WLAN devices one-by-one. You can select **Import** to import a list of IP/FQDN from a CSV file.
5. Select **OK**. The Forescout platform creates a wireless device for each new IP address, and applies the configuration settings of the existing controller to these devices.

## Import and Export Configurations

In some cases it is useful and more efficient to copy and edit existing configurations. For example, to quickly duplicate settings on all Forescout devices:

1. Export configurations.
2. Edit IP/FQDN and other device-specific fields.
3. Import the new definitions to another device. The Forescout platform creates new configurations based on imported data.

The Forescout platform uses a simple XML format to represent the settings and fields of the configuration screens.



### To export configurations:

1. Select **Options** from the **Tools** menu at the Console.
2. Select **Wireless**. The Wireless pane opens.
3. Select the wireless device configurations you want to export. Then select **Export**. The Exporting wireless devices dialog appears.
4. Specify a name for the exported file, browse to a target directory, and select **Save**.

An XML file containing the selected device configurations is saved to the target directory.

### To import configurations:

1. Select **Options** from the **Tools** menu at the Console.
2. Select **Wireless**. The Wireless pane opens.
3. Select **Import**. The Import wireless devices dialog appears.
4. Browse to the wireless device configuration file you want to import and select it. Then select **Import**.

The Forescout platform creates wireless device configurations using the content imported from the XML file.

## Scheduled Component Backup of Wireless Plugin Configuration

Wireless Plugin information is included as part of the Forescout platform's component backup processing (see [Forescout Requirements](#)). At a scheduled interval, the Forescout platform backs-up and then exports the Wireless Plugin's configuration, if the Forescout platform user has enabled the component backup feature and defined the various component backup settings in the Component Backup tab of the Backup pane (**Options** > **Advanced** > **Backup**).

The component backup feature encrypts sensitive fields of the configuration, as done for a regular export. To import the backup files, use the password specified in the **Encryption Password** section of the Component Backup tab.

## Change Connecting Appliance of WLAN Device

The following procedure is provided for changing the *Connecting Appliance* of a managed WLAN device. Use of this procedure is especially necessary when plugin actions are currently applied on wireless clients that are connected to the managed WLAN device; as actions applied by a plugin running on Forescout device <n> can only be canceled by that plugin/Forescout device <n>.

### To change the connecting appliance of a managed WLAN device:

1. In the Console Modules pane, double-click on the **Wireless** entry. The Wireless - Appliances Installed window opens.
2. Select the Forescout device that is the currently assigned *Connecting Appliance* of the managed WLAN device and select **Stop**.  
  
Doing so results in the plugin, which is running on the currently assigned *Connecting Appliance*, first canceling all the actions that it applied on the WLAN devices that it managed and then stopping.
3. In the Wireless pane, select a managed WLAN device and select **Edit**. The Edit Wireless Device window opens.
4. In the General tab, select from the **Connecting Appliance** drop-down menu a different Connecting Appliance IP address for the managed WLAN device.
5. Select **OK**. The Edit Wireless Device window closes.
6. In the Wireless pane, select **Apply** to save the modified plugin configuration.  
  
Doing so results in the plugin that is running on the newly assigned *Connecting Appliance* to interoperate with the managed WLAN device - apply WLAN actions and query for WLAN device information.
7. In the Console Modules pane, double-click on the **Wireless** entry. The Wireless - Appliances Installed window opens.
8. Select the Forescout device that was the previously assigned *Connecting Appliance* of the managed WLAN device and select **Start**.  
  
Doing so results in the plugin, currently stopped on that Forescout device, to restart and run again.

## Centralized Web Authentication with Cisco Wireless LAN Controllers

Centralized web authentication is a method that is used to accomplish the redirection of guest endpoints for the purposes of managing these endpoints, which have requested wireless access to your organization's network. For details about deploying the ForeScout centralized web authentication with Cisco WLCs, refer to the *ForeScout RADIUS Plugin Configuration Guide*, which is provided by the required Authentication Module version. See [Additional ForeScout Documentation](#) for information on how to access this guide.

## Display Wireless Detection Information at the Console

Information learned by the Wireless Plugin, about plugin-managed WLAN devices and the endpoints (wireless clients) that are connected to them, displays in the Console *Home* tab's *All Hosts* pane.

(Aruba, Cisco, and Ruckus only) The plugin reports detected lightweight access point(s) as entries in the *All Hosts* pane.

The screenshot displays the ForeScout console interface. At the top, the 'All Hosts' pane shows a table with columns: Host, IPv4 Address, Segment, MAC Address, Comment, and Display Name. A single host is listed with a green dot icon, IPv4 Address 10.20.1.123, Segment 10.20.1.123\_2, and MAC Address 405a0a274172737.

Below the table, the 'Profile' tab is selected, showing details for the host. The profile includes a search bar and a 'General' section. The 'General' section displays the following information:

- IPv4 Address:** 10.20.1.123
- MAC Address:** 405a0a274172737
- Admission:** Wireless Host Connected
- Network Access:** New Host
- MAC Address:** 405a0a274172737
- NIC Vendor:** HON HAI PRECISION IND. CO.,LTD.
- Windows SecureConnector Version:** None
- WLAN AP Location:** E-118 (In front of QA Networking team room)
- WLAN AP Name:** AP54a2.7417.2737
- WLAN Association Status:** Associated/AUTHZ\_WAIT
- WLAN Authentication Method:** WPA2/openSystem/notavailable
- WLAN BSSID:** f0b2e5437390
- WLAN Client Role:** VLAN0311
- WLAN Client User Agent:** N/A
- WLAN Client Username:** NA
- WLAN Client VLAN:** 311
- WLAN Client Connectivity Status:** Yes
- WLAN Device IP/Name:** WLC31.dom31.lab.forescout.com
- WLAN Device Vendor:** Cisco
- WLAN Detected Client Type:** N/A
- WLAN SSID:** SWC311

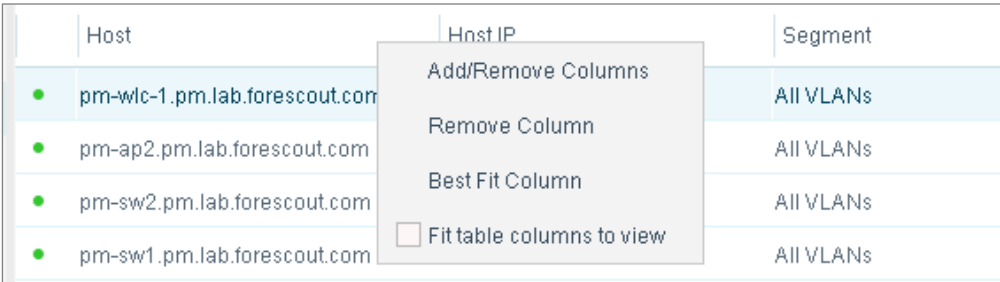


Presented information in the *All Hosts* pane includes:

- Wireless client IP address and MAC address
  - For connected IPv6 endpoints, whether **IPv6-only endpoints** or **dual-stack endpoints**, IP address information includes IPv6 Addresses and IPv6 Link-Local Address
- The wireless network name (SSID) to which the client is connected
- The wireless access point name to which the client is connected
- The client's authentication method, for example, 802.1X, WPA, none
- The IP address of the plugin-managed WLAN device
- (Aruba, Cisco, and Ruckus only) For a detected endpoint, report the IP address of detected lightweight access point(s) to which it is connected.
- **WLAN Device Vendor** property information is reported for both of the following *All Hosts* pane entries:
  - Plugin-managed WLAN devices
  - Detected, connected wireless clients

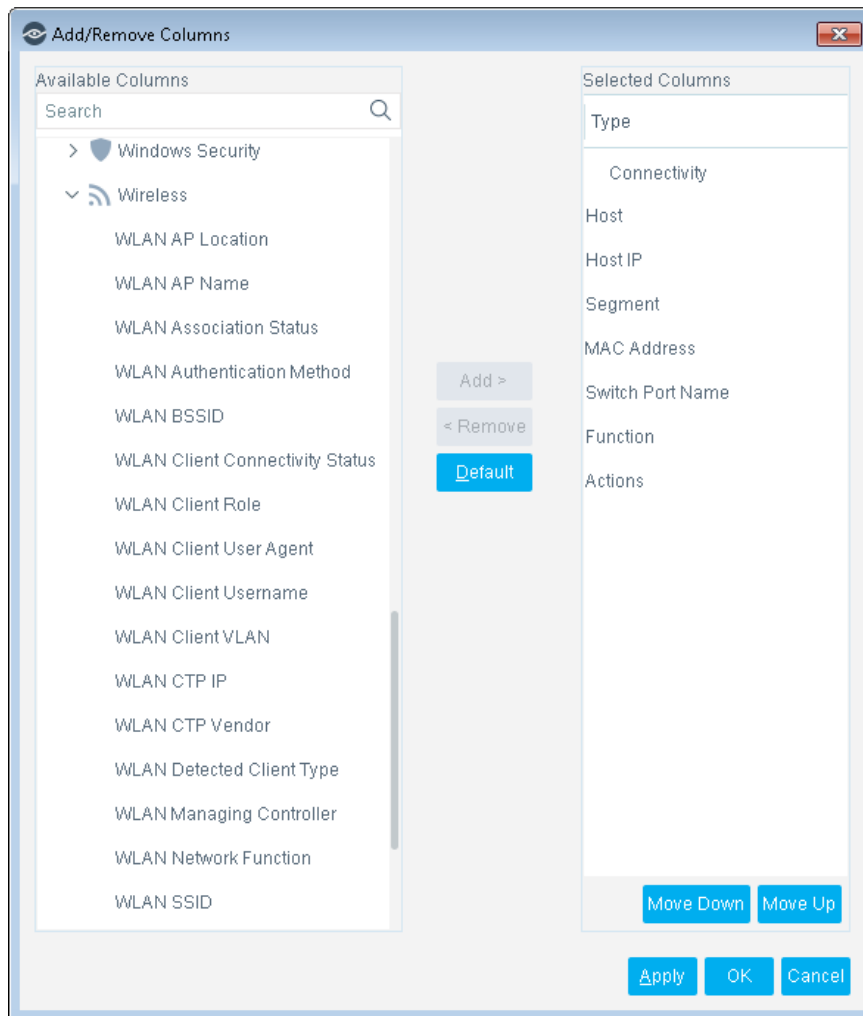
**To display/remove the display of wireless information:**

1. In the *All Hosts* pane, right-click a table column heading.



Host	Host IP	Segment
pm-wlc-1.pm.lab.forescout.com		All VLANs
pm-ap2.pm.lab.forescout.com		All VLANs
pm-sw2.pm.lab.forescout.com		All VLANs
pm-sw1.pm.lab.forescout.com		All VLANs

2. Select **Add/Remove Columns**. The Add/Remove Columns window opens.
3. In the navigation tree of the *Available Columns* pane, click the **Properties** folder to expand it and display its content.
4. In the Properties folder, click the **Wireless** folder to expand it and display its content.



5. To add wireless information to the *All Hosts* pane display:
  - a. In the expanded *Wireless* folder, select from among the available wireless information columns.
  - b. Select **Add**. The added information columns display in the *Selected Columns* pane.
6. To add the *IPv6 Address* column to the *All Hosts* display:
  - a. In *Properties* folder, select the **Device Information** folder to display its content.
  - b. Select **IPv6 Address** and select **Add**. The column displays in the *Selected Columns* pane.  
 The *IPv6 Address* column displays the IPv6 address of the following pane entries:
    - > Detected/connected endpoints
    - > Managed WLAN devices, when the plugin is configured with the FQDN of the device and the FQDN is associated with an IPv6 address
 The *IPv6 Address* column does not display by default.
7. To remove information from the *All Hosts* pane display:
  - a. In the *Selected Columns* pane, select from among the information columns currently selected for display.

- b. Select **Remove**. The removed information columns display in the *Available Columns* pane.
8. In the Add/Remove Columns window, select **Apply** and then select **OK**. The *All Hosts* pane display reflects your column updates.

**To promptly remove the display of wireless information:**

1. In the *All Hosts* pane, right-click a wireless information column heading.

Host	Host IP	Segment
pm-wlc-1.pm.lab.forescout.com		All VLANs
pm-ap2.pm.lab.forescout.com		All VLANs
pm-sw2.pm.lab.forescout.com		All VLANs
pm-sw1.pm.lab.forescout.com		All VLANs

2. Select **Remove Column**. The column is immediately removed from the *All Hosts* pane display.

## Create Policies to Handle Detected Wireless Clients

You can use Forescout platform policy tools to detect, evaluate and impose control on wireless clients connected to a WLAN device. For example:

- Create a policy that detects wireless clients infected with malware and block them via the WLAN device.
- Send email to network administrators regarding wireless policy violations.
- Communicate directly with users at wireless clients via email or web session redirection.

This section presents the following topics:

- [Wireless Client Properties](#)
- [Wireless SNMP Trap Criteria](#)
- [WLAN Device Properties](#)
- [Wireless Admission Events](#)
- [Policy Template: VR WPA2 KRACK](#)
- [WLAN Actions](#)

## Wireless Client Properties

The plugin provides the following wireless client properties for use in Forescout policies:

Property	Description
<b>WLAN AP Location*</b>	Property only supported for Aruba and Cisco controllers. Identifies the physical location of the access point to which the wireless client is connected.
<b>WLAN AP Name</b>	Identifies the name of the access point to which the wireless client is connected.
<b>WLAN AP Name Change</b>	Identifies that a change in value occurred in the <b>WLAN AP Name</b> property.
<b>WLAN Association Status</b>	Property only supported for Aruba, Siemens, and Cisco controllers. Identifies whether the wireless client is associated with an access point and is authenticated. For other supported vendors, this property is resolved with any of the following values: <ul style="list-style-type: none"> <li>Unknown</li> <li>Blacklisted (<i>WLAN Block</i> action is applied)</li> <li>Disassociated (wireless client is disconnected/offline)</li> </ul> Values vary by wireless equipment vendor. Refer to the vendor-specific configuration guides for this plugin and vendor documentation.
<b>WLAN Association Status Change</b>	Property only supported for Aruba and Cisco controllers. Identifies that a change in value occurred in the <b>WLAN Association Status</b> property.
<b>WLAN Authentication Method</b>	Identifies the authentication method used by the wireless client to authenticate with the access point. The possible values differ depending on the access point vendor. Resolution of this property for managed Aruba WLAN devices requires the plugin's <b>Read Connection Method</b> to be SNMP or CLI. <ul style="list-style-type: none"> <li>When using CLI read, identifies the encryption method used by the wireless client to authenticate with the access point</li> <li>When using SNMP read, identifies the authentication method used by the wireless client to authenticate with the access point.</li> </ul>
<b>WLAN Authentication Method Change</b>	Identifies that a change in value occurred in the <b>WLAN Authentication Method</b> property.
<b>WLAN BSSID*</b>	Property only supported for Aruba, Siemens, and Cisco controllers. Identifies the BSSID of the access point to which the wireless client is connected.
<b>WLAN BSSID Change</b>	Property only supported for Aruba and Cisco controllers. Identifies that a change in value occurred in the <b>WLAN BSSID</b> property.
<b>WLAN Client Role*</b>	Property only supported for Aruba, Cisco, Siemens, and Motorola controllers. Identifies the role assigned by the access point to the wireless client.
<b>WLAN Client Role Change</b>	Property only supported for Aruba and Cisco controllers. Identifies that a change in value occurred in the <b>WLAN Client Role</b> property.

Property	Description
<b>WLAN Client User Agent*</b>	Property only supported for Aruba mobility controllers running ArubaOS version 6.0.1 or later. Identifies the user agent running on the wireless client.
<b>WLAN Client User Agent Change</b>	Property only supported for Aruba mobility controllers running ArubaOS version 6.0.1 or later. Identifies that a change in value occurred in the <b>WLAN Client User Agent</b> property.
<b>WLAN Client Username*</b>	Property only supported for Aruba, Siemens, and Cisco controllers. Identifies the username employed by the wireless client to authenticate with the access point.
<b>WLAN Client Username Change</b>	Property only supported for Aruba and Cisco controllers. Identifies that a change in value occurred in the <b>WLAN Client Username</b> property.
<b>WLAN Client VLAN*</b>	Property only supported for Aruba, Cisco, Siemens, and Motorola controllers. Identifies the VLAN to which the wireless client is connected.
<b>WLAN Client VLAN Change</b>	Property only supported for Aruba, Cisco, and Motorola controllers. Identifies that a change in value occurred in the <b>WLAN Client VLAN</b> property.
<b>WLAN Client Connectivity Status</b>	Identifies whether the wireless client is connected to an access point.
<b>WLAN Client Connectivity Status Change</b>	Identifies that a change in value occurred in the <b>WLAN Client Connectivity Status</b> property.
<b>WLAN Device IP/FQDN</b>	Identifies either the IP address or the fully qualified domain name of the WLAN device to which the wireless client is connected.
<b>WLAN Device IP/FQDN Change</b>	Identifies that a change in value occurred in the <b>WLAN Device IP/FQDN</b> property.
<b>WLAN Device Software</b>	Identifies the software release that is running on the lightweight AP to which the wireless client is connected. Only supported for lightweight AP of vendors Aruba and Cisco.
<b>WLAN Device Vendor</b>	Identifies the vendor of the plugin-managed WLAN device to which the wireless client is connected.
<b>WLAN Detected Client Type*</b>	Property only supported for Aruba mobility controllers running ArubaOS version 6.0.1 or later, and Siemens controllers. Identifies the operating system of the wireless client.
<b>WLAN Detected Client Type Change</b>	Property only supported for Aruba mobility controllers running ArubaOS version 6.0.1 or later. Identifies that a change in value occurred in the <b>WLAN Detected Client Type</b> property.
<b>WLAN SSID</b>	Identifies the SSID (service set identifier) to which the wireless client is connected.

Property	Description
<b>WLAN SSID Change</b>	Identifies that a change in value occurred in the <b>WLAN SSID</b> property.

\* For Aruba Instant (autonomous) access points and for controllers of other supported vendors, the plugin resolves the property with the text string **N/A** and a relevant code.

When the plugin uses SNMP as its read method for managing an Aruba WLAN controller, the following limitations are in effect for wireless client property resolution:

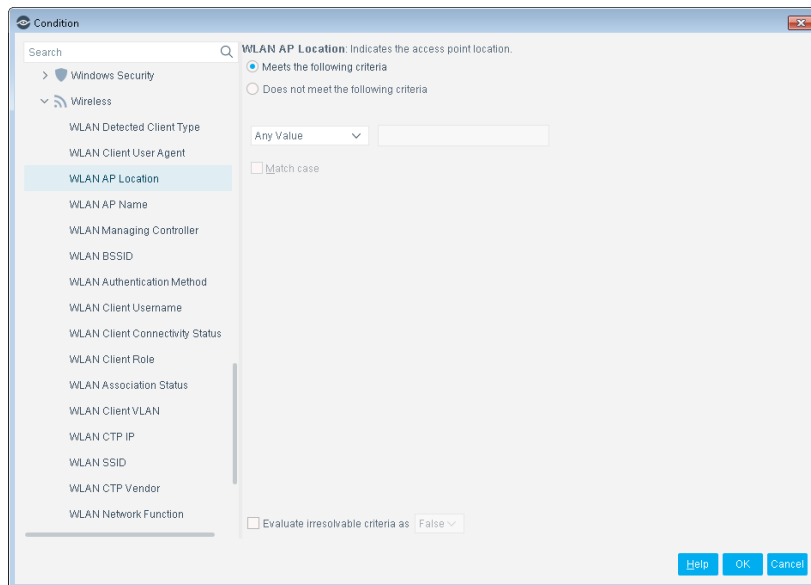
- For all connected endpoints, the plugin cannot resolve (*Irresolvable*) the properties:
  - **WLAN Client User Agent**
  - **WLAN Client User Agent Change**
  - **WLAN Detected Client Type**
  - **WLAN Detected Client Type Change**
- For connected **IPv6-only** endpoints, the plugin also cannot resolve (*Irresolvable*) the properties:
  - **WLAN AP Location**
  - **WLAN AP Name**
  - **WLAN AP Name Change**
  - **WLAN Authentication Method**
  - **WLAN Authentication Method Change**
  - **WLAN Client VLAN**

When the plugin uses SNMP as its read method for managing a Siemens WLAN controller, the following limitations are in effect for wireless client property resolution:

- For all connected endpoints, the plugin cannot resolve (*Irresolvable*) the properties:
  - **WLAN Client Role**
  - **WLAN Client VLAN**

#### To use these properties:

1. Create or edit a policy.
2. In the **Main Rule/Sub-Rule** dialog box, select **Add** from the **Condition** section. The Condition dialog box opens.
3. Expand the **Wireless** folder and/or the **Track Changes** folder and choose a property.

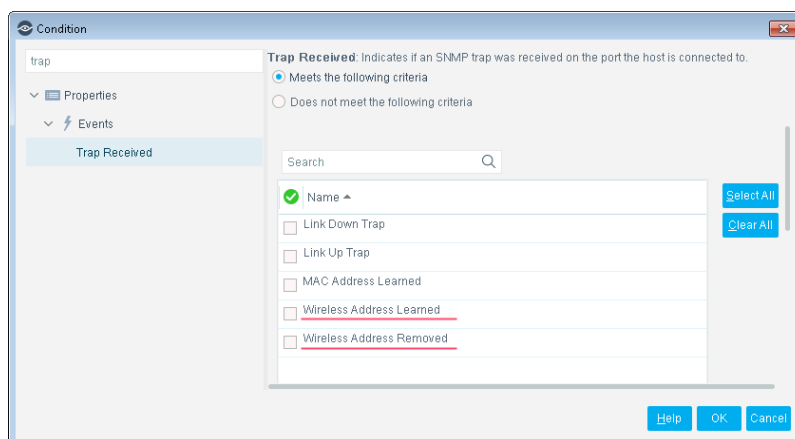


## Wireless SNMP Trap Criteria

The **Trap Received** property is used to define conditions based on SNMP trap events. The Wireless Plugin provides the following SNMP trap event criteria for use with the **Trap Received** property:

Create Forescout policies that evaluate detected endpoints for a match on the **Trap Received** property containing any of the following, resolved property information:

- *Wireless Address Learned* – syslog event received, notifying of endpoint connection to a wireless access point
- *Wireless Address Removed* - syslog event received, notifying of endpoint disconnection from a wireless access point



Use these criteria in policies to apply actions to wireless clients based on SNMP traps related to wireless devices. For example, apply actions to wireless clients when the Wireless Plugin first detects an SNMP trap for them.

## WLAN Device Properties

The plugin provides the following WLAN device properties for use in Forescout policies:

Property	Description
<b>WLAN Device Software</b>	Identifies the software release that is running on a: <ul style="list-style-type: none"> <li>▪ Plugin-managed WLAN device</li> <li>▪ Lightweight AP of vendors Aruba and Cisco</li> </ul>
<b>WLAN Device Vendor</b>	Identifies the vendor of a: <ul style="list-style-type: none"> <li>▪ Plugin-managed WLAN device</li> <li>▪ Lightweight AP of vendors Aruba, Siemens, Cisco, and Ruckus</li> </ul>
<b>WLAN Device Vendor and Type</b>	The vendor and the device type of a managed WLAN device or a detected lightweight access point. Examples: <i>Cisco Controller</i> or <i>Cisco Lightweight AP</i> . Currently, this property is only available for use in/resolved by a policy that is created using a <b>Vulnerability and Response</b> (VR) policy template.
<b>WLAN Managing Controller</b>	Property is only supported for the wireless products of the supported vendors Aruba, Cisco, and Ruckus. Identifies either the IP address or the fully qualified domain name of the WLAN controller managing the lightweight AP.
<b>WLAN Managing Controller Change</b>	Identifies that a change in value occurred in the <b>WLAN Managing Controller</b> property.
<b>WLAN Network Function</b>	The plugin resolves this property for the WLAN devices of all supported WLAN vendors with any of the following values: <ul style="list-style-type: none"> <li>▪ <b>Controller</b> - the plugin-managed WLAN device is determined to be a WLAN controller</li> <li>▪ <b>Autonomous AP</b> - the plugin-managed WLAN device is determined to be an autonomous access point.</li> <li>▪ <b>Lightweight AP</b> - the device is determined to be a lightweight access point that is associated with (managed by) a plugin-managed WLAN controller</li> <li>▪ <b>Other</b> - the device is determined to be a connected wireless client.</li> </ul>

## Wireless Admission Events

Use Forescout admission events to identify and evaluate the occurrence of specific network events. The Wireless Plugin makes available the following admission events:

Admission Event	Description
<b>WLAN lightweight AP connected</b>	Event only supported for the lightweight APs of vendors Aruba, Cisco, and Ruckus. Identifies that a lightweight access point is newly connected to a plugin-managed WLAN controller.
<b>Wireless Host Connected</b>	Identifies that an endpoint is newly connected to a plugin-managed WLAN device.



Incorporate these wireless admission events as criteria for evaluation in policy conditions, either in a policy main rule and/or in a policy sub-rule.

## Policy Template: VR WPA2 KRACK

Use the VR WPA2 KRACK policy template (*Policy* tab > *Add* > *Vulnerability and Response*) to create a policy that classifies the following items according to their KRACK vulnerability:

- Plugin-managed WLAN devices of vendors Aruba and Cisco
- Lightweight APs of vendors Aruba and Cisco
- Wireless clients (endpoints) connected to any of the above and running one of the following operating systems:
  - Windows (both HPS-managed and unmanaged endpoints)
  - Android
  - Linux
  - iOS
  - Macintosh

The policy evaluates WLAN devices and Lightweight APs based on their installed software version and evaluates connected wireless clients based on the October 2017 Microsoft Security Updates being present on these wireless clients.


- Effective policy evaluation requires that the Primary Classification policy be also running on your Forescout devices.

Policies created from the VR WPA2 KRACK policy template include use of the **WLAN Device Software** property to detect KRACK vulnerability. Customize the policy, as necessary, to address your organization's specific network security requirements; customization includes configuring the policy to apply a plugin-provided WLAN action on detected, vulnerable endpoints. Refer to the *Forescout Security Policy Templates Configuration Guide* for detailed requirements information about the VR WPA2 KRACK policy template. See [Additional Forescout Documentation](#) for information on how to access this guide.

## WLAN Actions

The Wireless Plugin provides the following actions that can be applied on detected wireless clients:

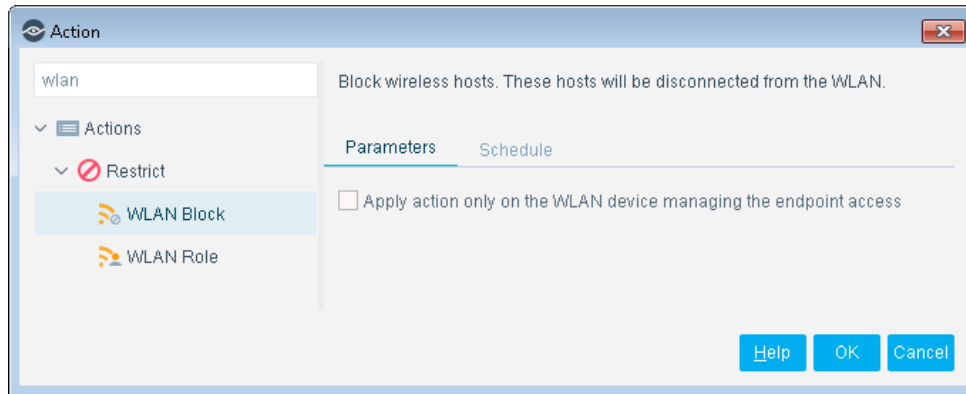
- [WLAN Block Action](#)
- [WLAN Role Action](#)

 *If the Wireless Plugin attempts to apply an action on a connected endpoint that it did not detect, but the endpoint was detected by either the Centralized Network Controller Plugin or the Network Controller Plugin, be aware that action application does not succeed and remains in a **pending** state until Forescout platform action timeout occurs.*

If you are using Flexx licensing, ensure that you have a valid Forescout eyeControl license to use these actions. Refer to the *Forescout Flexx Licensing How-to Guide* for more information about managing licenses.

## WLAN Block Action

Apply the *WLAN Block* action on wireless clients to block them from accessing a wireless network. The applied action can be cancelled on detected, wireless clients.



- This action is **not supported** for use on Aruba Instant access points.

When you use the *WLAN Block* action in a policy, wireless clients that match the policy conditions are blocked. Blocking is accomplished using the wireless client MAC address. When a policy re-check is performed, wireless clients found to no longer match policy conditions are unblocked (released).

See [Block Wireless Clients Exhibiting Malicious Intent](#) for a sample policy using this action.

### Apply Action Only on Managing WLAN Device

The Parameters tab of the *WLAN Block* action contains the following option:

- **Apply action only on the WLAN device managing the endpoint access**

The option is disabled by default. Enabling this option instructs the plugin to apply the action in the following manner:

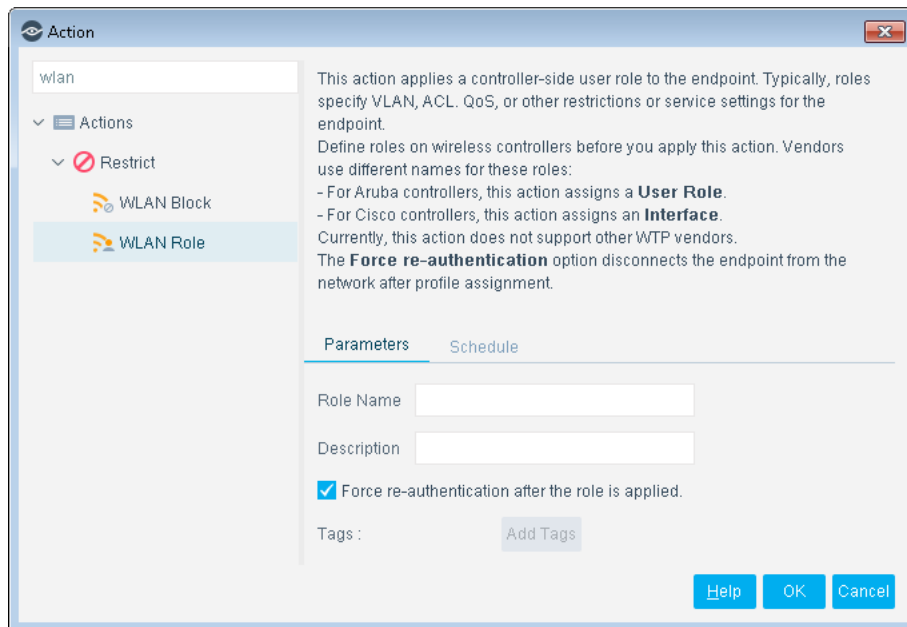
- Only block endpoint access on the WLAN device that is currently responsible for managing the access of the matching/targeted endpoint.
  - When a blocked endpoint moves such that a different WLAN device is now responsible for managing its wireless network access, endpoint access continues to be blocked on all previous, managing WLAN devices, in addition to being blocked on the currently responsible, managing WLAN device.

When the option is disabled, the plugin applies the *WLAN Block* action in the following manner:

- Block endpoint access -
  - on the WLAN device that is currently responsible for managing the access of the matching/targeted endpoint and on all other WLAN devices being managed by the same Forescout Appliance
  - and on all WLAN devices being managed by the Forescout Appliance whose IP assignment includes the IP address of the matching/targeted endpoint

## WLAN Role Action

Apply the *WLAN Role* action to assign the wireless client a controller-defined role. Typically, roles specify VLAN, ACL, QoS or other restrictions or service settings for the wireless client. You must define roles on the WLAN Controllers, in order for the plugin to apply this action.



The *WLAN Role* action is **supported** for use on the following WLAN devices:

- Aruba WLAN Controllers, excluding Aruba Instant access points
- Cisco WLAN Controllers, excluding Cisco controllers that run the IOS-XE operating system
- Motorola WLAN Controllers
- Siemens WLAN Controllers

Each vendor uses a different term for the role assignment by the *WLAN Role* action:

- For Aruba and Siemens WLAN Controllers, the *WLAN Role* action assigns a *User Role*.
- For Cisco WLAN Controllers, the *WLAN Role* action assigns an *Interface*.
- For Motorola WLAN Controllers, the *WLAN Role* action assigns a *VLAN*

When you use this action in a policy, the specified role overrides the role assigned by wireless devices for wireless clients that match the policy conditions. When wireless clients no longer match policy conditions, the Forescout platform cancels the action and the relevant WLAN device, once again, determines the role that is assigned to the wireless client.

To use the *WLAN Role* action, specify the following fields and options:

Action Fields	Description
<b>Role Name</b>	The name of the role, as defined on the WLAN device. <ul style="list-style-type: none"> <li>For Aruba and Siemens WLAN Controllers, this is the name of a <i>User Role</i>.</li> <li>For Cisco WLAN Controllers, this is the name of an <i>Interface</i>.</li> <li>For Motorola WLAN Controllers, this is the numerical <i>VLAN ID</i>.</li> </ul>
<b>Description</b>	(Optional) A description of the role, or the situation that prompted role assignment. This comment is stored in the controller's log.
<b>Force re-authentication after the role is applied</b>	When this option is selected, existing wireless client WLAN sessions are disconnected after role assignment. This generates <i>disconnect</i> and <i>reconnect</i> traps when the wireless client reconnects. The Fore Scout platform authenticates the wireless client with its new role. <ul style="list-style-type: none"> <li>VoIP and media sessions are dropped when the wireless client is disconnected.</li> </ul>

Only one role can be assigned to a wireless client at any time. If this action has been used several times to assign different roles to a wireless client:

- Each *WLAN Role* action overwrites the previous action, and the wireless client receives only the most recently specified role.
- When the most recent *WLAN Role* action no longer applies to the wireless client, the relevant controllers are restored to their original configuration before the Fore Scout platform assigned *any* roles to the wireless client.

When the *WLAN Block* action applies to a wireless client, you cannot assign a role to the wireless client. However, you can block a wireless client after a role has been assigned to it.

To ensure that the specified role remains assigned to the wireless client, the *WLAN Role* action is automatically re-applied to a wireless client when there is a change in the following wireless client properties:

- WLAN Device IP/FQDN**
- Current **WLAN Client Role**
- WLAN Client Connectivity Status**

See the following sections for vendor-specific deployment considerations:

- [Using the WLAN Role Action with Aruba WLAN Controllers](#)
- [Using the WLAN Role Action with Cisco WLAN Controllers](#)
- [Using the WLAN Role Action with Motorola WLAN Controllers](#)
- [Using the WLAN Role Action with Siemens WLAN Controllers](#)

### Using the WLAN Role Action with Aruba WLAN Controllers

To implement the *WLAN Role* action, the plugin adds a role derivation rule to the AAA profile used by the wireless client. The rule applies a previously defined *user role* to the wireless client.

- The string you enter in the **Description** field of the action is used to label the role derivation rule.

- When you select the **Force re-authentication** option, the plugin removes the wireless client from the user table of the controller to initiate re-authentication.

The *WLAN Role* action is **not supported** for use on Aruba Instant access points.

In order for the plugin to apply the *WLAN Role* action on wireless clients that are connected to Aruba controllers that are both running ArubaOS 8 and deployed in a master/managed topology, the following is required:


- The Wireless Plugin must manage both the master controller and the managed controllers, and have read and write permissions for accessing all these controllers. (In Aruba OS 8, the master controller acts as a single touchpoint for configuration changes performed on managed controllers. Therefore, the plugin redirects the *WLAN Role* action to the master controller.)

For deployments in which the Wireless Plugin does not manage the master controller, you must instruct the plugin to not redirect the *WLAN Role* action to the master controller, but to send a local command to the managed controller.

#### To instruct the plugin to send the local command:

1. Log in to the CLI on the Forescout device hosting the Wireless Plugin that manages the managed controller(s):
2. Run the following fstool commands using an SSH connection:

```
fstool wireless set_property
conf.aruba_os8_use_default_assign_role_method.value 0
fstool wireless restart
```

 When the Wireless Plugin manages only the managed controller, the plugin does not apply the *WLAN Role* action by adding a role derivation rule to the AAA profile used by the wireless client. Instead, the plugin applies the action by sending the following command to the managed controller: **aaa user add <client-ip> role <role-name>**

#### Plugin Configuration

When configuring plugin management of an Aruba controller:

- Applying this action requires command line interface (CLI) communication with the controller. Make sure to:
  - Select *Command Line* as the **Read Connection Method** and select the **Enable WLAN management actions using Command Line** option.
  - Specify command line credentials.

#### Controller Configuration

Perform the following configuration task for all controllers and WLANs that will implement the action:

- Define the desired User Role(s) and enable them.

#### Default AAA Profile

In some cases the action is applied to a wireless client before it is associated with a AAA profile. Similarly, it may be unclear which AAA profile to roll back to when the action no longer applies to a wireless client. You can define a default profile that the plugin uses in these cases.

**To define a default AAA profile:**

1. Log in to the Enterprise Manager and open the `local.properties` file in the following directory:  
`/usr/local/forescout/plugin/wireless/local.properties`
2. Add the following line to the file:  
`conf.aruba_default_profile.value =`
3. Specify a default profile. The profile you specify must exist on the controller.
4. Save the file.

**Using the WLAN Role Action with Cisco WLAN Controllers**


To implement the *WLAN Role* action, the plugin defines a MAC Filter entry that selects the wireless client and applies an *interface* that is currently defined for the controller. The plugin adds this entry to the MAC Filter table using either one of the following options, when applying the *WLAN Role* action to a connected wireless client:

- **Any WLAN Connection** option - when the plugin creates or updates the wireless client's MAC Filtering entry in the controller, the entry is defined to apply to the wireless client regardless of the WLAN to which the wireless client is connected. This is the **default** option.
- **Current WLAN Connection** option - when the plugin creates or updates the wireless client's MAC Filtering entry in the controller, the entry is defined to apply to the wireless client only when connected to the specific WLAN.

The option available for plugin use is enabled per Appliance on which the plugin runs.

The string you enter in the **Description** field of the *WLAN Role* action is used to label the MAC Filter entry.

When you select the **Force re-authentication** option, the plugin sends a **deauthenticate** command for the wireless client to the controller.

 *RADIUS authentication is not compatible with MAC filtering. This means the WLAN Role action does not work with Cisco controllers in typical environments that use RADIUS authentication. It is recommended to use the Forescout RADIUS Plugin for VLAN/Interface assignment.*

Cisco controllers cannot simultaneously apply Blacklist and MAC Filtering features to a wireless client. When you apply the *WLAN Block* action to a wireless client to which the *WLAN Role* action is already applied, the MAC Filter entry corresponding to the assigned role is removed from the controller database. When the *WLAN Block* action is removed, the *WLAN Role* Action is re-applied to the wireless client using the last role assigned to the wireless client.

The *WLAN Role* action is **not supported** for use on Cisco controllers that run the IOS-XE operating system.

### Plugin Configuration

When configuring plugin management of a Cisco controller:

- Applying this action requires SNMP communication with the controller. Make sure to:
  - Select the **Enable WLAN management actions** option.
  - Specify SNMP credentials.

### Appliance Configuration

The MAC Filter entry option used by the plugin when applying the *WLAN Role* action to a connected wireless client is enabled per Appliance on which the plugin runs. The enabled option is available for all Cisco wireless controllers being managed by a specific Appliance. Per Appliance, **Any WLAN Connection** is the option that is enabled by **default**.

#### To enable the **Current WLAN Connection** option for an Appliance:

1. Log in to the CLI on the Appliance
2. Run the following command using an SSH connection:

```
fstool wireless set_property  
conf.cisco_associated_wlan_in_role.value 1
```

#### To re-enable the default **Any WLAN Connection** option for an Appliance:

1. Log in to the CLI on the Appliance
2. Run the following command using an SSH connection:

```
fstool wireless set_property  
conf.cisco_associated_wlan_in_role.value 0
```

### Controller Configuration

Perform the following configuration tasks for all controllers and WLANs that will implement the action. Refer to Cisco documentation for detailed instructions and configuration options.

- Define the desired Interface(s) and enable them.
  - In the configuration GUI, navigate to **WLANs > Edit > General** and select the Interface in the **Interface/Interface Group** field.
  - From the command line submit the following command:  

```
config interface create <interface name> <wlan-id>
```
- Enable AAA override to allow override of the WLAN default interface.
  - In the configuration GUI, navigate to **WLANs > Edit > Advanced** and select the **Allow AAA override** checkbox.
  - From the command line submit the following command:  

```
config wlan aaa-override enable <wlan-id>
```
- Enable MAC Filtering for Layer 2 security.
  - In the configuration GUI, navigate to **WLANs > Edit > Security > Layer 2** and select the **MAC Filtering** checkbox.
  - From the command line submit the following command:  

```
config wlan mac-filtering enable <wlan-id>
```

- Enable Web Policy on MAC Filtering failure for Layer 3 security. If MAC Filtering does not identify the wireless client and it remains Associated but not Authenticated, the Fore Scout platform applies the action based on the Association trap.
  - In the configuration GUI, navigate to **WLANs > Edit > Security > Layer 3** and select the **Web Policy** checkbox.  
Select the **On MAC filter failure** option. In the **Preauthentication ACL** field, select an ACL which allows the Fore Scout platform to inspect the wireless client.
  - From the command line submit the following commands:  

```
config wlan security web-auth on-macfilter-failure <wlan-id>  
config wlan security web-auth acl <wlan-id> <ACL_name>
```
- (Optional) When a controller handles large numbers of wireless clients, it may be necessary to increase the size of the controller database to accommodate filtering entries created by the Fore Scout platform. If the controller database cannot accept new MAC Filtering entries, the *WLAN Role* action is not applied to any more wireless clients on the controller and the Fore Scout platform issues the following error message:  

Assign Role action failed. Wireless plugin failed to create MAC Filter entry on *WLAN device <IP address of the WLAN device>*. Verify that the interface referenced by the role is defined on the controller, and the maximum size of the *WLAN device* database is not exceeded.

If you encounter this error condition, consider increasing the size of the controller database. Refer to your vendor's product documentation.

### Using the WLAN Role Action with Motorola WLAN Controllers

To implement the *WLAN Role* action, the Wireless Plugin edits the *Wireless Client Role Policy* in the Motorola WLAN Controller. For Motorola WLAN Controllers, the *WLAN Role* action assigns a VLAN to a wireless client.

When configuring the *Wireless Client Role Policy* in a Motorola WLAN Controller:

- Make sure that the *Wireless Client Role Policy* is already applied to a profile, and that the profile is actively applied to a WLAN device.
- The *Wireless Client Role Policy* must be active for role changes to take effect on the wireless client.

#### Appliance Configuration

The *WLAN Role* action to a connected wireless client is enabled per Fore Scout Appliance on which the Wireless Plugin runs. The *WLAN Role* action is available for all Motorola WLAN Controllers being managed by a specific Appliance.

#### To enable the WLAN Role action for an Appliance:

1. Using an SSH connection, log in to the CLI of the Appliance hosting the Wireless Plugin that manages the WLAN Controller(s).
2. Run the following command:  

```
fstool wireless set_property  
conf.motorola_cli_client_detail.value 1
```
3. (Optional) If you need the plugin to apply the *Role Policy* to all existing profiles in the WLAN Controller, run the following command.



```
fstool wireless set_property
conf.motorola_apply_role_to_all_profiles.value 1
```

Do not run this command if you need to assign the *Role Policy* to profiles manually (to prevent the Wireless Plugin from overriding pre-existing configurations).

4. (Optional) If you need to use a pre-existing *Role Policy*, run the following command, and specify the *Role Policy Name*. If you do not specify the *Role Policy Name*, the *Forescout\_Client\_Role* is applied by default.

```
fstool wireless set_property conf.motorola_role_policy_name.value
NAC-ROLES
```

5. (Optional) run the following command to apply roles to all existing profiles in the WLAN Controller:


```
fstool wireless set_property
conf.motorola_apply_role_to_all_profiles.value 1
```

### Plugin Configuration

Before configuring the Wireless Plugin for a Motorola Wireless Controller, you must first complete the [Appliance Configuration](#).

When configuring plugin management of a Motorola WLAN Controller:

- In the **Read Connection Method** section of the *General* pane, define the method that the plugin uses to connect to the WLAN device as **Command Line**.
- In the *Command Line* pane:
  - Enter the necessary CLI login parameters.  
Since managing the WLAN device requires the Wireless Plugin to use CLI privilege mode write access, and the provided login credentials are not of the privilege mode type, select the **Enable privilege** checkbox.
- Forescout recommends to enable SNMP Trap processing. In the *SNMP* pane, select the **Enable Notification Traps** checkbox. When this option is enabled, the plugin accepts, and processes SNMP notification traps sent from the managed WLAN device.

 *Note: The correct SNMP Traps configuration must already exist in the Motorola (Extreme) WLAN Controller.*

### Using the WLAN Role Action with Siemens WLAN Controllers

To implement the *WLAN Role* action, the plugin adds a role derivation rule to the WLAN profile used by the wireless client. The rule applies a previously defined Role-based *access-rule* to the connected wireless client.

- The string that you enter in the **Role Name** field of the action must match a pre-defined access-rule name on the Siemens WLAN Controller created via its CLI or through its configuration website.  
Refer to the *Siemens Scalance CLI and UI Manual* for more information.
- The **Description** field and **Force re-authentication** option of the action are not used.

### Plugin Configuration

When configuring plugin management of a Siemens WLAN Controller:

- Applying this action requires command line interface (CLI) communication with the Siemens WLAN Controller. Make sure to:
  - Select **Command Line** as the **Read Connection Method**, and select the **Enable WLAN management actions using Command Line** option.
  - Specify command line credentials.

#### Controller Configuration

Perform the following configuration task for all Siemens WLAN Controllers that implement the action:

- Pre-define the required access-rule(s) via the Siemens WLAN Controller's CLI, or through its configuration website:
  - From the Siemens WLAN Controller's CLI, run the following command:  
**wlan access-rule <rule-name>**
  - In the Siemens WLAN Controller's configuration website, navigate to **Configuration > Security > Roles > Add a new Role**, and then update it with required access rules.

## Sample Policies

This section guides you through the creation of the following useful Forescout policies:

- [Wireless User Notification – Company Security and Privacy Policy](#)
- [Block Wireless Clients Exhibiting Malicious Intent](#)
- [Prevent Wireless Client Access to Organizational Server Farm](#)

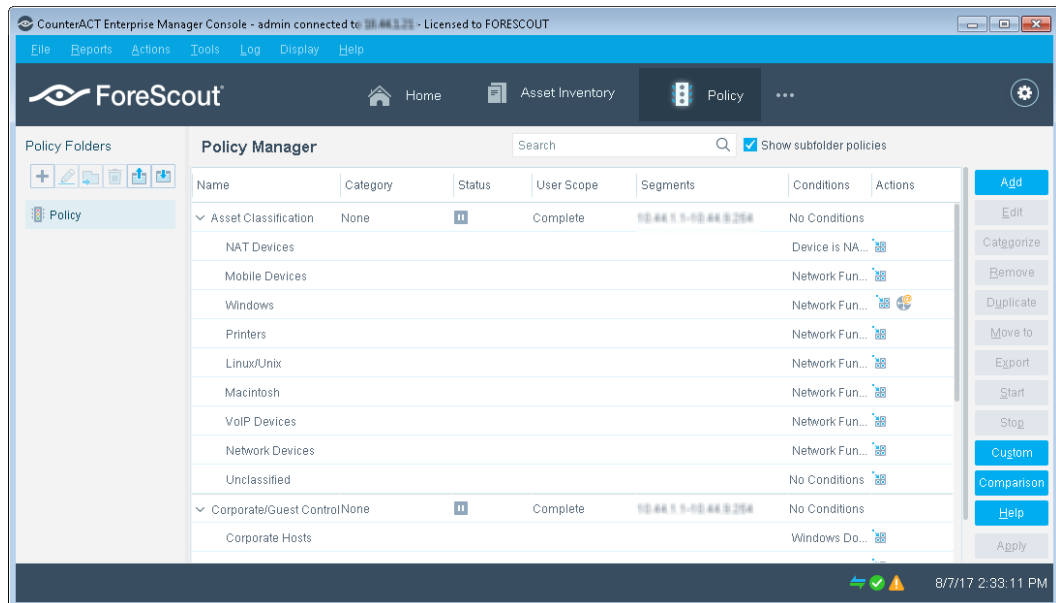
### Wireless User Notification – Company Security and Privacy Policy

Create a policy that lets administrators introduce wireless device users to the company security and privacy policy. Notification is carried out by redirecting wireless client Web sessions to a customized message. The user's session is redirected when attempting to access the Web and released when the user confirms reading the message. If the user rejects the message, web access is blocked. For this policy to be effective, the traffic coming to and from the wireless clients must be monitored by a Forescout Appliance.

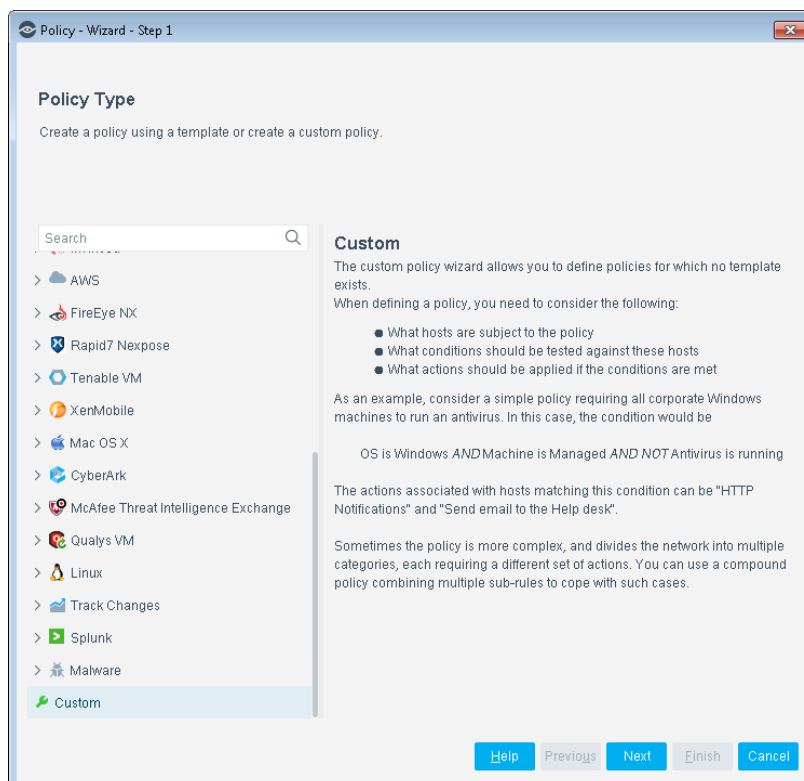


## To create the policy:

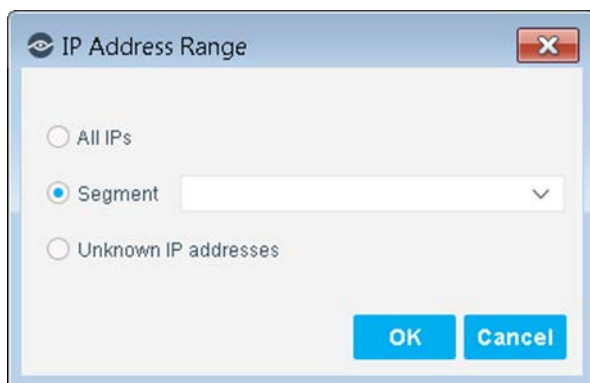
1. Select the **Policy** tab from the Console toolbar. The Policy Manager opens.



2. Select **Add**. The Policy Wizard opens.



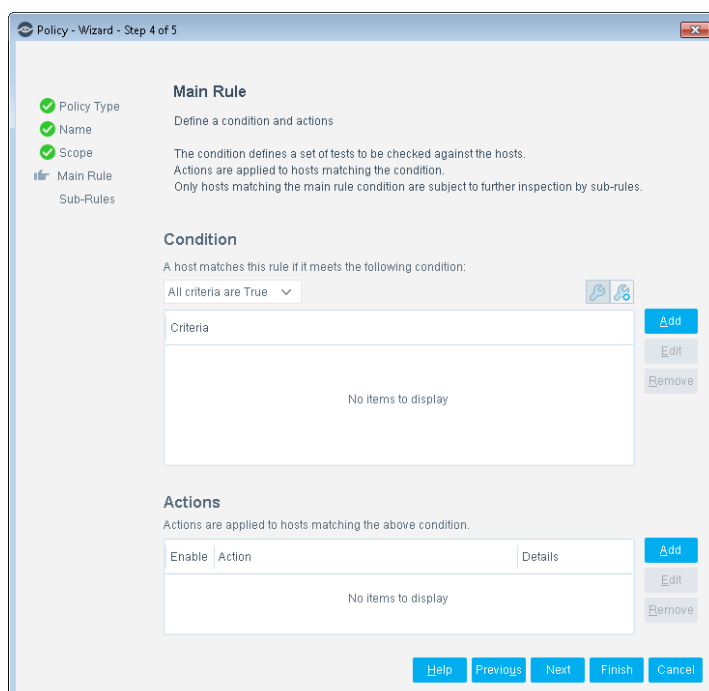
3. Select **Custom**. Select **Next**. The Name page opens.
4. Enter a policy name and description.
5. Select **Next**. The Scope page opens.
6. Use the IP Address Range dialog box to define which endpoints are inspected.



The following options are available:

- **All IPs:** Include all IP addresses in the Internal Network.
- **Segment:** Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the Scope pane.
- **Unknown IP addresses:** Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

7. Select **OK** and then select **Next**. The Main Rule page opens.



8. In the **Condition** section, select **Add**.

9. Expand the **Wireless** group and then select **WLAN SSID**.

10. Define the property:

- a. Verify that **Meets the following criteria** is selected.
- b. Select **Matches** from the drop-down list and then enter the SSID the expected wireless clients will use for this policy (for example *Production* as shown below). (The SSID must be defined in the controller.)

c. Select **Match case**.

The 'Condition' dialog box shows the 'WLAN SSID' condition selected in the left pane. The right pane has the following settings:

- WLAN SSID:** Indicates the host SSID association.
- ☒ Meets the following criteria
- ☐ Does not meet the following criteria
- Matches:** A dropdown menu set to 'Matches'.
- Production:** A text box containing 'Production'.
- ☒ Match case
- ☐ Evaluate irresolvable criteria as: False

Buttons at the bottom: Help, OK, Cancel.

11. Select **OK** to return to the Main Rule page.

12. Select **Add** from the **Actions** section.

13. Expand the **Notify** group and then select **HTTP Notification**.

The 'Action' dialog box shows the 'HTTP Notification' action selected in the left pane. The right pane has the following settings:

- Message Text:** A large text box for the message content.
- Button Text:** A text box containing 'I confirm reading the message'.
- Confirmation Identifier:** A text box containing 'Notification confirmed'.
- ☒ Attempt to open a browser at the detected endpoint
- Tags:** A text box with an 'Add Tags' button.

Buttons at the bottom: Help, OK, Cancel.

14. In the **Message Text** text box, enter your message to wireless users. Select **Help** on the dialog box for information about additional HTTP Notification.

15. Select **OK** to return to the Main Rule page.

16. Select **Finish** to create the policy.

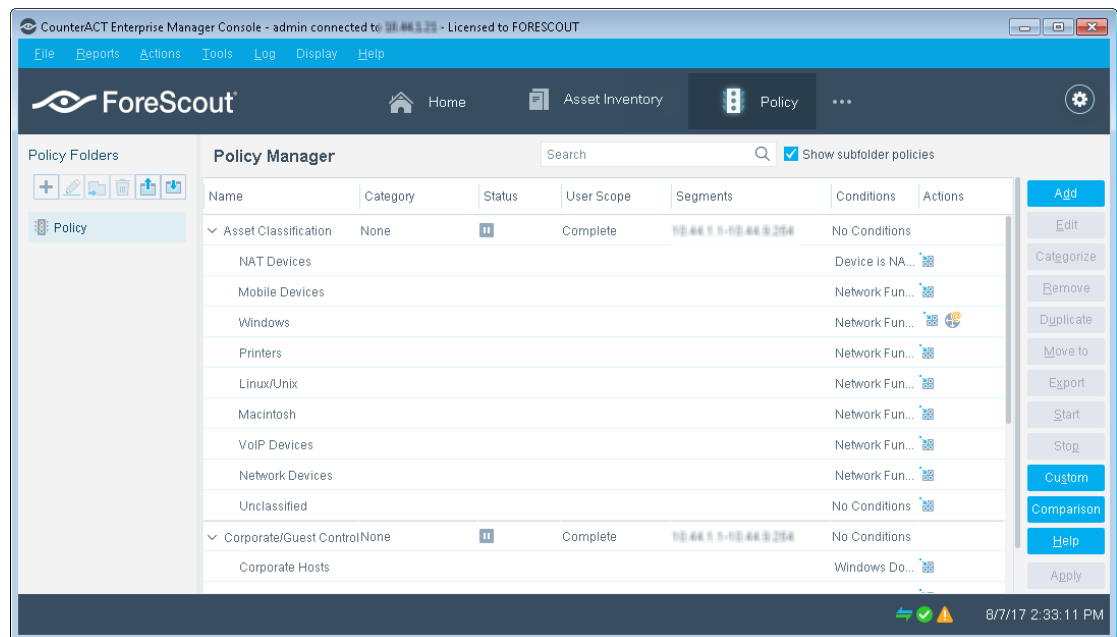
17. In the Policy Manager, select **Apply**.

## Block Wireless Clients Exhibiting Malicious Intent

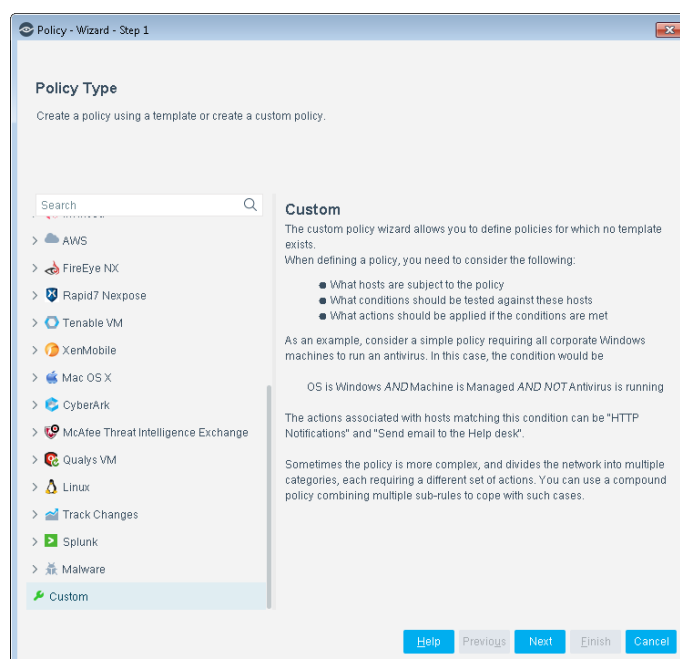
Create a policy that disconnects wireless clients from WLAN controllers when malicious activity (worms, hackers, self-propagating malware) is detected at the wireless client.

**To create the policy:**

1. Select the **Policy** tab from the Console toolbar. The Policy Manager opens.



2. Select **Add**. The Policy Wizard opens.



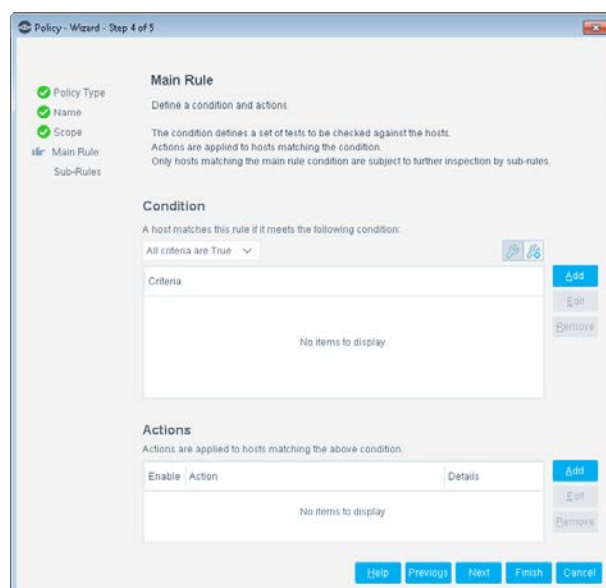
3. Select **Custom**. Select **Next**. The Name page opens.

4. Enter a policy name and description.
5. Select **Next**. The Scope page opens.
6. Use the IP Address Range dialog box to define which endpoints are inspected.

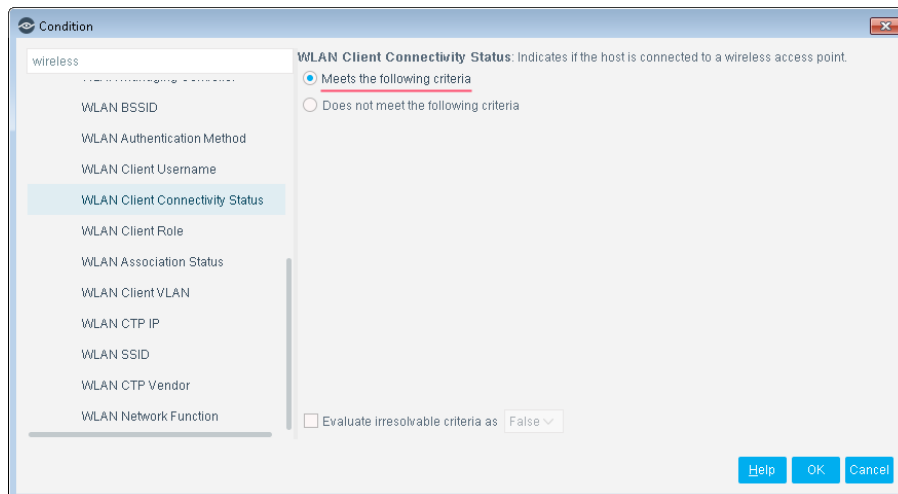


The following options are available:

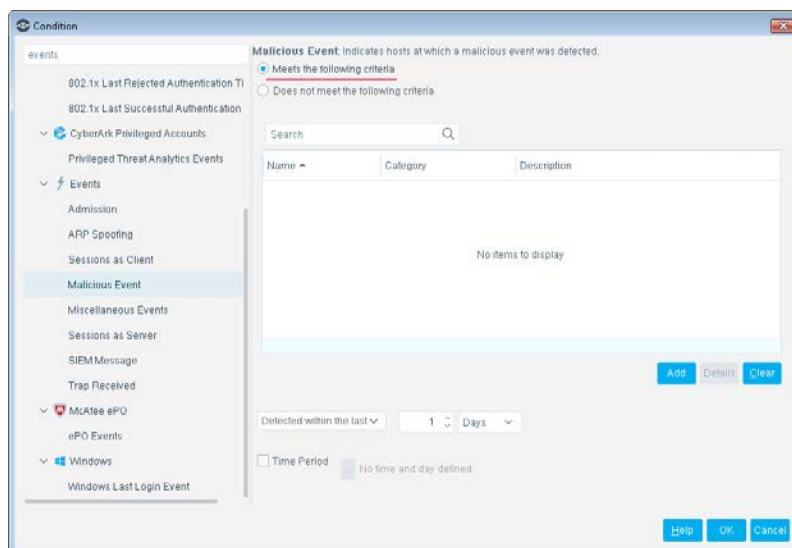
- **All IPs**: Include all IP addresses in the Internal Network.
  - **Segment**: Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the Scope pane.
  - **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.
7. Select **OK** and then select **Next**. The Main Rule page opens.



8. In the **Condition** section, select **Add**.
9. Expand the **Wireless** group and then select **WLAN Client Connectivity Status**.
10. Verify that **Meets the following criteria** is selected.

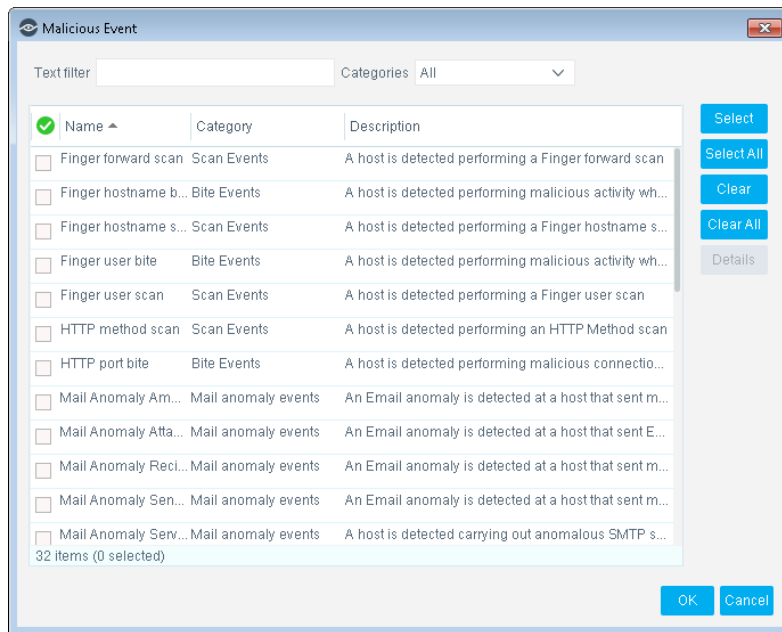


11. Select **OK** to return to the Main Rule page.
12. Select **Add** from the **Condition** section again. The Condition dialog box opens.
13. Expand the **Events** group and select **Malicious Event**.
14. Verify that **Meets the following criteria** is checked.



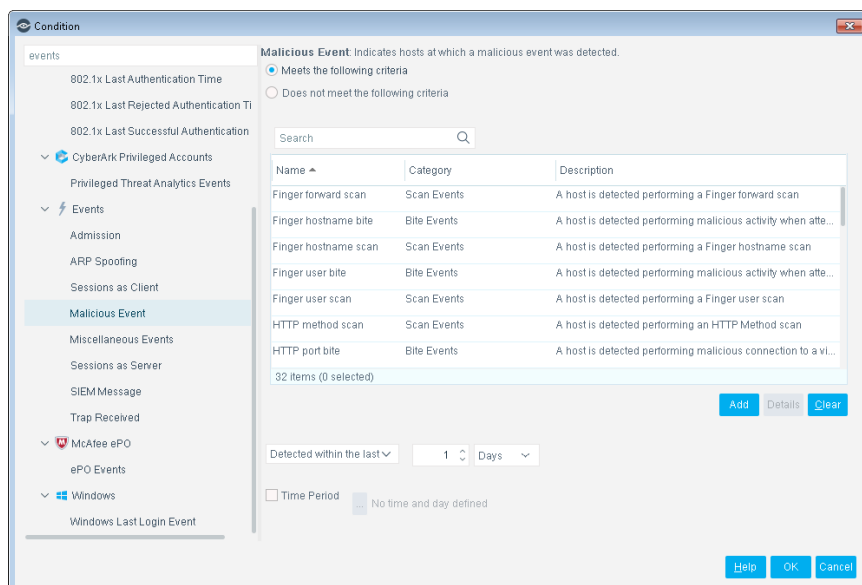
15. Select **Add**. The Malicious Event dialog box opens.





16. Select **Select All**.

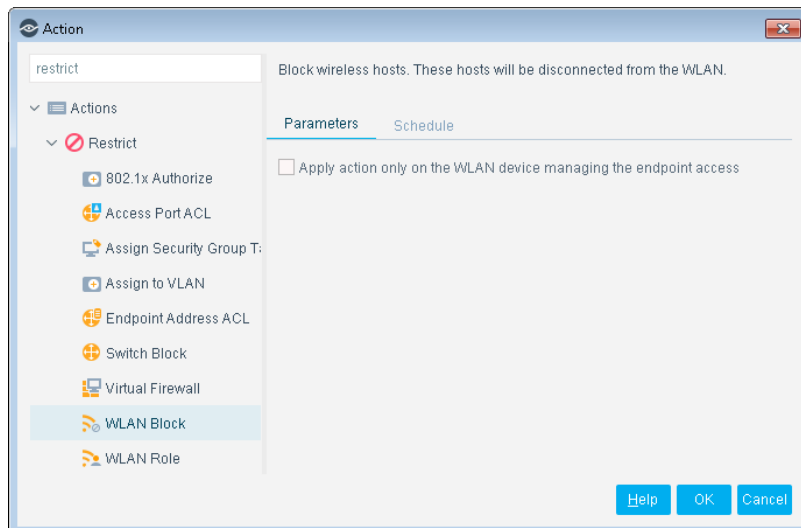
17. Select **OK**. All the events appear in the Condition dialog box.



18. Select **OK** to return to the Main Rule page.

19. Select **Add** from the **Actions** sections. The Action dialog box opens.

20. Select **Restrict** and then **WLAN Block**.



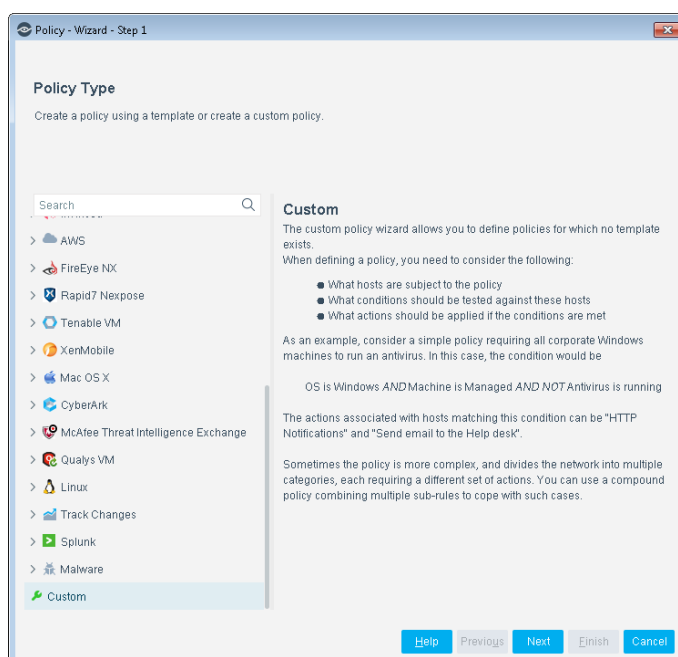
21. Select **OK** to return to the Main Rule page.
22. Select **Finish** to return to the Policy Manager.
23. Select **Apply**.

## Prevent Wireless Client Access to Organizational Server Farm

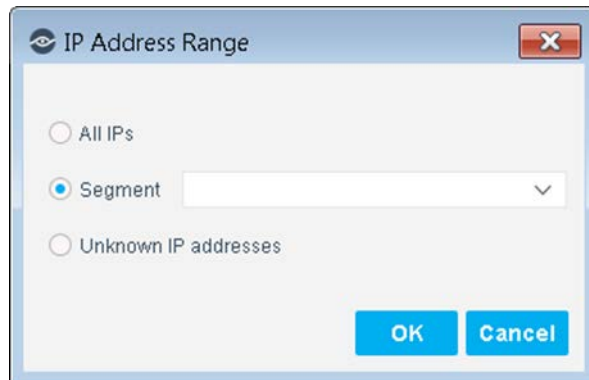
Create a policy that prevents wireless clients in a specific building from connecting to a server farm.

**To create the policy:**

1. Select the **Policy** tab from the Console toolbar. The Policy Manager opens.
2. Select **Add**.
3. Select **Custom**.

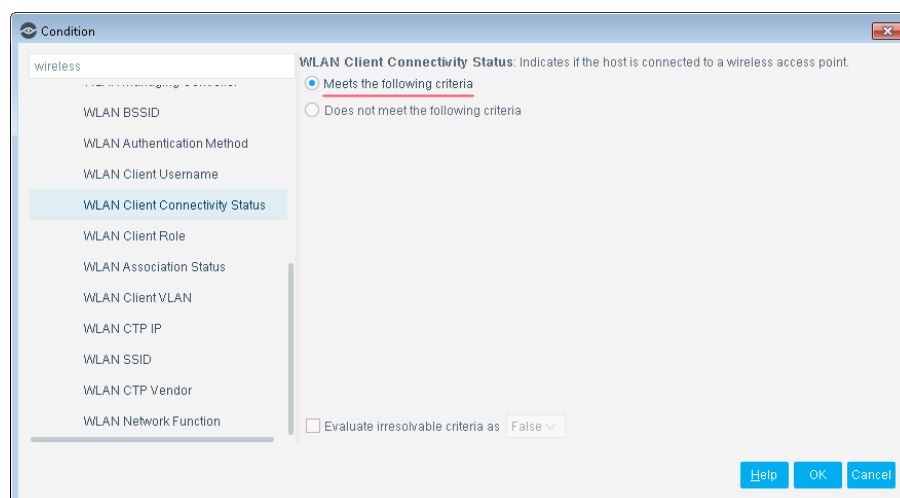


4. Select **Next**. The Name page opens.
5. Enter a policy name and description.
6. Select **Next**. The Scope page opens.
7. Use the IP Address Range dialog box to define which endpoints are inspected.



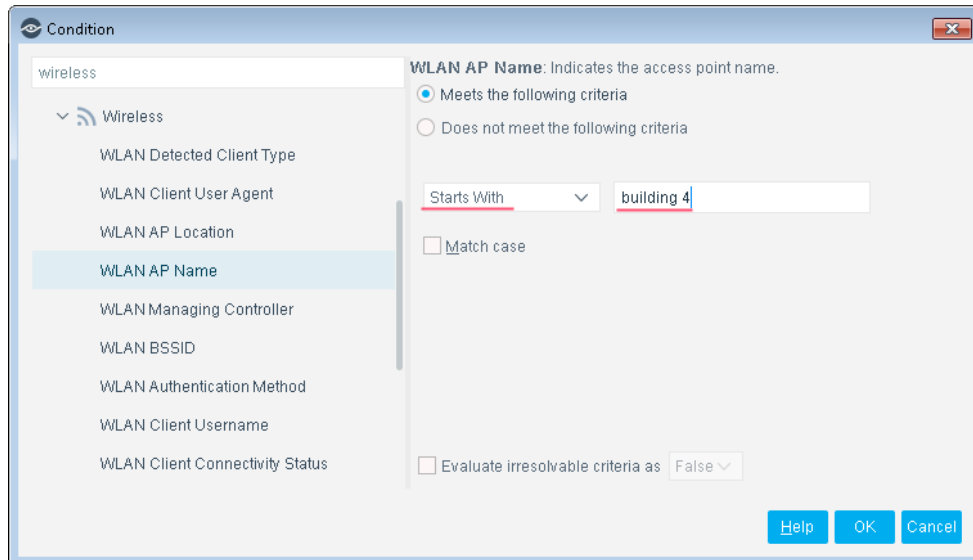
The following options are available:

- **All IPs**: Include all IP addresses in the Internal Network.
  - **Segment**: Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the Scope pane.
  - **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.
8. Select **OK** and then select **Next**. The Main Rule page reopens.
  9. In the **Condition** section, select **Add**.
  10. Expand the **Wireless** group and then select **WLAN Client Connectivity Status**.
  11. Verify that **Meets the following criteria** is selected.

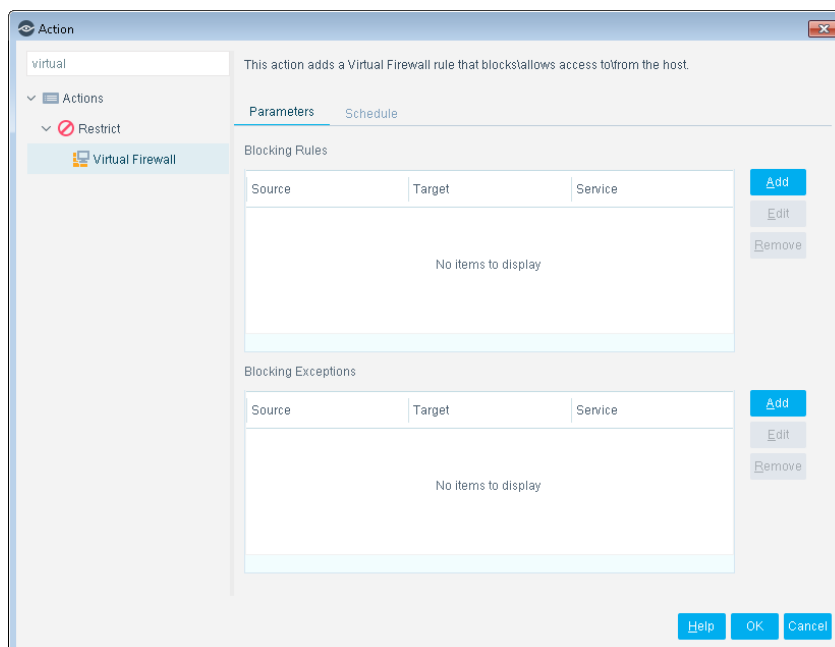


12. Select **OK** to return to the Main Rule page.
13. Select **Add** from the **Condition** section again. The Condition dialog box opens.

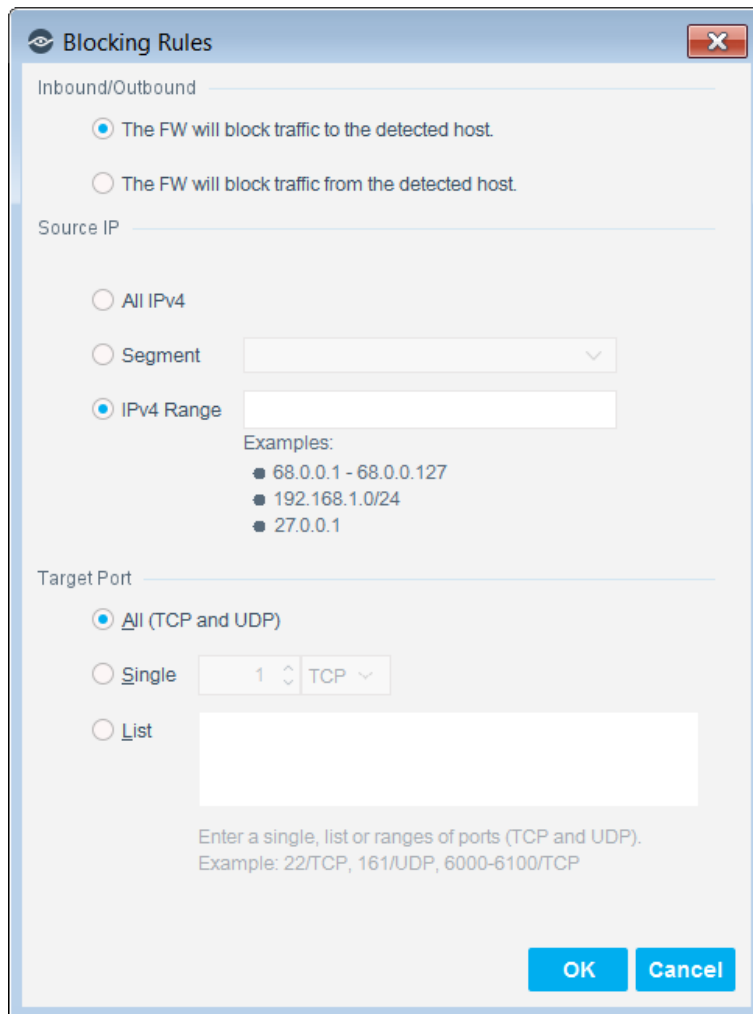
14. Expand the **Wireless** group and select **WLAN AP Name**.
15. Define the property:
  - a. Verify that **Meets the following criteria** is selected.
  - b. In the drop-down list select *Starts With* and select the access point name. (Provided this naming scheme is used for the access points.)



16. Select **OK** to return to the Main Rule page.
17. In the **Actions** section select **Add**. The Action dialog box opens.
18. Select **Restrict** and then **Virtual Firewall**.



19. Create **Blocking Rules** to your server farm from wireless clients in locations that you defined.
  - a. Select **Add**. The Blocking Rules dialog box opens.



**Blocking Rules**

Inbound/Outbound

☒ The FW will block traffic to the detected host.

☐ The FW will block traffic from the detected host.

Source IP

☐ All IPv4

☐ Segment

☒ IPv4 Range

Examples:

- 68.0.0.1 - 68.0.0.127
- 192.168.1.0/24
- 27.0.0.1

Target Port

☒ All (TCP and UDP)

☐ Single

☐ List

Enter a single, list or ranges of ports (TCP and UDP).  
Example: 22/TCP, 161/UDP, 6000-6100/TCP

**OK** **Cancel**

b. Define a required rule.

c. Select **OK**.

Repeat until you have defined all required rules.

20. Select **OK** to return to the Main Rule page.

21. Select **Finish** to return to the Policy Manager.

22. Select **Apply**.

Select **Help** for more information about working with the **Virtual Firewall** action.


## Displaying Wireless Inventory Information

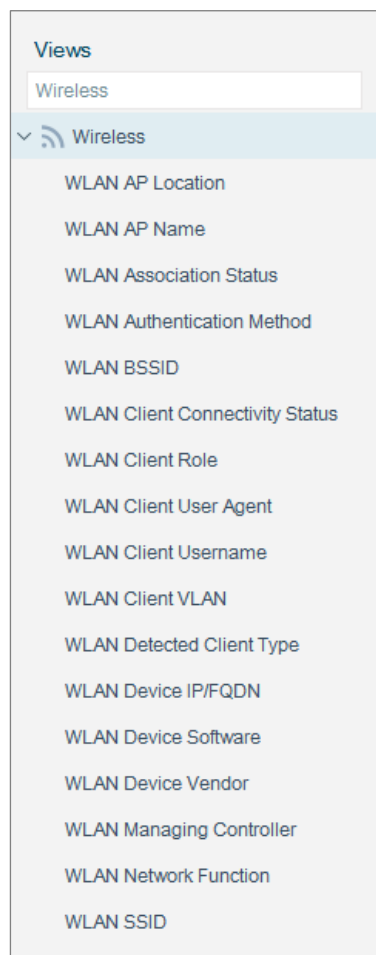
Use the Console *Asset Inventory* to view a real-time display of wireless device network activity at multiple levels. The *Asset Inventory* lets you:

- Broaden your view of the organizational network from device-specific to activity-specific.
- View wireless devices that have been detected with specific attributes.
- Incorporate inventory detections into policies.

**To access the inventory:**

1. Select the **Asset Inventory** tab from the Console toolbar.
2. In *Views*, navigate to **Wireless**. The entries provided by the *Wireless* view are based on the wireless client properties that the plugin resolves.

 Refer to Working at the Console > Working with Inventory Detections in the *Forescout Administration Guide* or the *Console, Online Help* for information about how to work with the *Forescout Inventory*.



## Appendix 1: MIBs Used by the Wireless Plugin

This section lists wireless device MIB requirements. If the plugin configuration test fails for a Wireless LAN device, the device might not meet specific MIB requirements. Use the following procedure to determine whether a required MIB exists on a Wireless WLAN device or not:

1. Log in to the CLI of the Enterprise Manager/Appliance.
2. Run the following command:

```
fstool run snmpwalk <wireless_device_ip_address> -v <version> -c  
<community> <oid>
```

Required MIBs for the wireless devices of the following vendors:

- [General MIBs](#)
- [Aerohive](#)
- [Aironet](#)
- [Aruba](#)
- [Cisco](#)
- [Extreme](#)
- [HP](#)
- [Huawei](#)
- [Meru](#)
- [Motorola](#)
- [Ruckus](#)
- [Siemens](#)
- [Xirrus](#)

### General MIBs

1.3.6.1.2.1.1.3.0  
1.3.6.1.2.1.1.6.0  
1.3.6.1.2.1.1.1.0  
1.3.6.1.6.3.1.1.4.1.0  
1.3.6.1.2.1.1.5  
1.3.6.1.2.1.4.22.1.2  
1.3.6.1.2.1.1.2.0  
1.3.6.1.2.1.47.1.1.1.1.10.1

### Aerohive

1.3.6.1.4.1.26928.1.1.1.2.1.2.1  
1.3.6.1.4.1.26928.1.1.1.2.1.1.1.2  
1.3.6.1.4.1.26928.1.1.1.1.2  
1.3.6.1.4.1.26928.1.1.1.1.1

**Aironet**

1.3.6.1.4.1.9.9.273.1.2.1.1.16  
1.3.6.1.4.1.9.9.273.1.2.1.1.19

**Aruba**

1.3.6.1.4.1.14823.2.2.1.14.1.2.1  
1.3.6.1.4.1.14823.2.2.1.4.1.2.1  
1.3.6.1.4.1.14823.2.2.1.5.2.1.4  
1.3.6.1.4.1.14823.2.2.1.5.2.2.1.1  
1.3.6.1.4.1.14823.2.3.3.1.2.1.1  
1.3.6.1.4.1.14823.2.3.3.1.2.3.1  
1.3.6.1.4.1.14823.2.3.3.1.2.4.1  
1.3.6.1.4.1.14823.2.2.1.1.2.1  
1.3.6.1.4.1.14823.2.3.1.11.1.1  
1.3.6.1.4.1.14823.2.3.3.1.200.1  
1.3.6.1.4.1.14823.2.2.1.1.100  
1.3.6.1.4.1.14823.1.1.23.0  
1.3.6.1.4.1.14823.2.3.1.11.1.2  
1.3.6.1.4.1.14823.2.3.3.1.200.2

**Cisco**

1.3.6.1.4.1.14179.2.1.4.1  
1.3.6.1.4.1.14179.2.1.11.1  
1.3.6.1.4.1.14179.2.2.1.1  
1.3.6.1.4.1.14179.2.5.6.1  
1.3.6.1.4.1.14179.2.5.9.1  
1.3.6.1.4.1.14179.2.1.1.1  
1.3.6.1.4.1.9.9.599.1.3.1.1  
1.3.6.1.4.1.9.9.513.1.1.1.1  
1.3.6.1.4.1.14179.2.2.1  
1.3.6.1.4.1.9.9.599.1.2  
1.3.6.1.4.1.14179.2.6.2  
1.3.6.1.4.1.9.9.599.0  
1.3.6.1.4.1.14179.2.6.3

**Extreme**

1.3.6.1.4.1.4329.15.3.6.2.1  
1.3.6.1.4.1.4329.15.3.5.1.2.1  
1.3.6.1.4.1.4329.15.3.4.1.1.1  
1.3.6.1.4.1.4329.15.3.3.4.6.1.1  
1.3.6.1.4.1.4329.15.3.3.4.7.1.1

**HP**

None



**Huawei**

1.3.6.1.4.1.2011.6.139.18.1.2.1  
1.3.6.1.4.1.2011.6.139.13.3.3.1  
Meru  
1.3.6.1.4.1.15983.1.1.4.4.1.1  
1.3.6.1.2.1.4.22.1.4  
1.3.6.1.4.1.15983.1.1.3.1.7.1  
1.3.6.1.4.1.15983.1.1.4.13.1.1

**Meru**

1.3.6.1.4.1.15983.1.1.4.4.1.1  
1.3.6.1.2.1.4.22.1.4  
1.3.6.1.4.1.15983.1.1.3.1.7.1  
1.3.6.1.4.1.15983.1.1.4.13.1.1

**Motorola**

1.3.6.1.4.1.388.50.1.3.17.1.1.1  
1.3.6.1.4.1.388.50.1.3.4.1.1  
1.3.6.1.4.1.388.50.1.4.3.2.3.1.1  
1.3.6.1.4.1.388.50.1.2.1  
1.3.6.1.4.1.388.50.0.11.0

**Ruckus**

1.3.6.1.4.1.25053.1.2.2.1.1.3.1.1  
1.3.6.1.4.1.25053.1.2.2.1.1.1.1.1  
1.3.6.1.4.1.25053.1.2.2.4.1.1.1.1  
1.3.6.1.4.1.25053.1.2.2.1.1.2.1.1  
1.3.6.1.4.1.25053.2.1.2  
1.3.6.1.4.1.25053.2.1.1

**Siemens**

1.3.6.1.4.1.4329.20.2.1.2.2.2.3.3.1.2.1.1  
1.3.6.1.4.1.4329.20.2.1.2.2.2.3.3.1.2.3.1  
1.3.6.1.4.1.4329.20.2.1.2.2.2.3.3.1.2.4.1

**Xirrus**

1.3.6.1.4.1.21013.1.2.22.1.1  
1.3.6.1.4.1.21013.1.2.2.2.1  
1.3.6.1.4.1.21013.1.2.22.3.0  
1.3.6.1.4.1.21013.1.2.2.1

## Network Module Information

The Wireless Plugin is installed with the Forescout Network Module.

The Forescout® Network Module provides network connectivity, visibility and control through the following plugin integrations:

- Centralized Network Controller Plugin
- Network Controller Plugin
- Rogue Device Plugin
- Switch Plugin
- VPN Concentrator Plugin
- Wireless Plugin

The Network Module is a Forescout Base Module. Base Modules are delivered with each Forescout release. This module is automatically installed when you upgrade the Forescout version or perform a clean installation of Forescout.

The plugins listed above are installed and rolled back with the Network Module.

## Additional Forescout Documentation

For information about other Forescout features and modules, refer to the following resources:

- [Documentation Downloads](#)
- [Documentation Portal](#)
- [Forescout Help Tools](#)

### Documentation Downloads

Documentation downloads can be accessed from the [Technical Documentation Page](#), and one of two Forescout portals, depending on which licensing mode your deployment is using.

- **Per-Appliance Licensing Mode** – [Product Updates Portal](#)
- **Flexx Licensing Mode** – [Customer Support Portal](#)

 *Software downloads are also available from these portals.*

**To identify your licensing mode:**

- From the Console, select **Help > About Forescout**.

### Technical Documentation Page

The Forescout Technical Documentation page provides a link to the searchable, web-based [Documentation Portal](#), as well as links to a wide range of Forescout technical documentation in PDF format.

**To access the Technical Documentation page:**

- Go to <https://www.Forescout.com/company/technical-documentation/>

## Product Updates Portal

The Product Updates Portal provides product and documentation downloads for Forescout platform releases, Base Modules, Content Modules, and eyeExtend modules. The portal also provides additional documentation.

### To access the Product Updates Portal:

- Go to <https://updates.forescout.com/support/index.php?url=counteract> and select the version you want to discover.

## Customer Support Portal

The Downloads page on the Forescout Customer Support Portal provides product and documentation downloads for Forescout platform releases, Base Modules, Content Modules, and eyeExtend modules. Software and related documentation only appear on the Downloads page if you have a license entitlement for the software.

### To access documentation on the Customer Support Portal:

- Go to <https://Forescout.force.com/support/> and select **Downloads**.

## Documentation Portal

The Forescout Documentation Portal is a searchable, web-based library containing information about Forescout tools, features, functionality, and integrations.

### To access the Documentation Portal:

- Go to [https://updates.forescout.com/support/files/counteract/docs\\_portal/](https://updates.forescout.com/support/files/counteract/docs_portal/)

## Forescout Help Tools

You can access individual documents, as well as the [Documentation Portal](#), directly from the Console.

### *Console Help Buttons*

- Use context sensitive *Help* buttons to quickly access information about the tasks and topics you are working with in the Console.

### *Forescout Administration Guide*

- Select **Administration Guide** from the **Help** menu.

### *Plugin Help Files*

- After the plugin is installed, select **Tools** > **Options** > **Modules**, select the plugin, and then select **Help**.

### *Content Module, eyeSegment Module, and eyeExtend Module Help Files*

- After the component is installed, select **Tools** > **Options** > **Modules**, select the component, and then select **Help**.

### *Documentation Portal*

- Select **Documentation Portal** from the **Help** menu.