Forescout

Network Module: Wireless Plugin

Configuration Guide

Version 1.9.1
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 Resources page on the Forescout website for additional technical documentation: https://www.forescout.com/company/resources/
- Have feedback or questions? Write to us at documentation@forescout.com

Legal Notice
© 2019 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.
Table of Contents

About the Wireless Plugin ............................................................................ 5
  Wireless Network Access Device Terminology ............................................. 7
  How It Works .................................................................................................. 7
    About WLAN Controller/Lightweight Access Points ..................................... 8
  Supported Wireless Integrations ................................................................... 9
    Required WLAN Device Configuration ....................................................... 9
  IPv6 Support .................................................................................................. 9
  Failover Clustering Support .......................................................................... 10
  Appliance Management Processing Load ..................................................... 10
  What to Do .................................................................................................... 10

Hardware and Software Requirements .......................................................... 11
  Forescout Requirements .............................................................................. 11
  Networking Requirements ............................................................................ 11
  WLAN Device – Read/Write Settings .......................................................... 11

Configure the Plugin .................................................................................... 12
  Configuration ............................................................................................... 12
    WLAN Device Management Configuration ............................................... 14
    Enable Forescout RADIUS-based Management of Wireless Clients .......... 20
    RADIUS Integration ................................................................................ 23
    Control Plugin Query about Lightweight Access Points ............................ 24
  Verify That the Plugin Is Running ............................................................... 25
  Plugin Testing .............................................................................................. 25
    Troubleshooting ...................................................................................... 26
  Duplicate a Configuration ........................................................................... 27
  Import and Export Configurations ............................................................... 28
  Wireless Pane Information and Failover Clustering ..................................... 29
  Scheduled Component Backup of Wireless Plugin Configuration ............... 30
  Change Connecting Appliance of WLAN Device ........................................... 30
  Centralized Web Authentication with Cisco Wireless LAN Controllers ........... 31

Display Wireless Detection Information at the Console ............................. 31

Create Policies to Handle Detected Wireless Clients ..................................... 34
  Wireless Client Properties ......................................................................... 35
  Wireless SNMP Trap Criteria ..................................................................... 38
  WLAN Device Properties .......................................................................... 38
  Wireless Admission Events ....................................................................... 39
  Policy Template: VR WPA2 KRACK ........................................................... 39
  WLAN Actions ............................................................................................ 40
    WLAN Block Action ............................................................................... 40
    WLAN Role Action ............................................................................... 41
Sample Policies ......................................................... 46
  Wireless User Notification – Company Security and Privacy Policy .......... 46
  Block Wireless Clients Exhibiting Malicious Intent ................................. 51
  Prevent Wireless Client Access to Organizational Server Farm.................. 56

Displaying Wireless Inventory Information ............................................. 60

Network Module Information ................................................................. 61

Additional Forescout Documentation ..................................................... 61
  Documentation Downloads ...................................................................... 61
  Documentation Portal ........................................................................... 62
  Forescout Help Tools ........................................................................... 62
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-based management of wireless clients attempting to connect to the network via WLAN devices of any vendor.

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.
- Assigning wireless clients a controller-defined role.
- Blocking wireless clients from connecting to the organizational network.
Wireless Network Access Device Terminology

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

<table>
<thead>
<tr>
<th>Term</th>
<th>Short Name/Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Autonomous Access Point</td>
<td>• Autonomous AP</td>
<td>The autonomous access point is an access point device that supports standalone network configurations, where all configuration settings are maintained locally on the device. Configure the Wireless Plugin to manage autonomous access points.</td>
</tr>
<tr>
<td></td>
<td>• AAP</td>
<td></td>
</tr>
<tr>
<td>Light Weight Access Point</td>
<td>• Lightweight AP</td>
<td>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 zero touch deployed and are not individually configured. The Wireless Plugin learns of and reports information about lightweight access points that are managed by a plugin-managed WLAN controller.</td>
</tr>
<tr>
<td></td>
<td>• LAP</td>
<td></td>
</tr>
<tr>
<td>Wireless LAN Controller</td>
<td>• WLAN controller</td>
<td>A device that manages one or more lightweight access point in the WLAN. The WLAN controller performs all the traditional roles of an AP, such as association or authentication of wireless clients. The WLAN controller provides all the configuration parameters and firmware that the lightweight access point needs in the registration process. Configure the Wireless Plugin to manage WLAN controllers.</td>
</tr>
<tr>
<td></td>
<td>• Controller</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• WLC</td>
<td></td>
</tr>
<tr>
<td>Wireless Client</td>
<td>• Wireless client</td>
<td>An endpoint that attempts to connect to or is currently connected to a WLAN device or a lightweight AP.</td>
</tr>
</tbody>
</table>

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
Supported Wireless Integrations

For detailed information about specific WLAN device vendor models and operating system versions that are validated for Wireless Plugin management, refer to the WLAN Integrations section in the Forescout Network Devices Compatibility Matrix. Access this matrix from the Forescout Resources Page.

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

- Aruba Networks: Forescout® Wireless Plugin Integration with Aruba Controllers Configuration Guide
- Cisco: Forescout® Wireless Plugin Integration with Cisco Controllers Configuration Guide
- Meru Networks: Forescout® Wireless Plugin Integration with Meru Wireless Controllers Configuration Guide
- Motorola: Forescout® Wireless Plugin Integration with Motorola Controllers Configuration Guide
- Xirrus: Forescout® Wireless Plugin Integration with Xirrus Wireless Controllers Configuration Guide

IPv6 Support

The Wireless Plugin provides IPv6-related support for the managed WLAN devices of all supported wireless vendors. For the list of supported wireless vendors, refer to the WLAN Integrations section in the Forescout Network Devices Compatibility Matrix. Access this matrix from the Forescout Resources Page.

The Wireless Plugin provides the following IPv6-related support:

- 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 Release Notes. 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 failback 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 CounterACT 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 CounterACT Appliances.

What to Do

To work with the Wireless Plugin, do the following:

1. Verify that all requirement are met. See Hardware and Software 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.

### Hardware and Software Requirements

This section describes software and hardware requirements.

- A basic understanding of the Forescout platform’s functionally and policy features is required of readers of this document.
- For the read/write permissions required by the Wireless Plugin to work with managed wireless devices, see WLAN Device – Read/Write Settings.

### Forescout Requirements

The following Forescout version must be running in your Enterprise Manager and your Appliances:

- Forescout 8.1.2
- In order for Wireless Plugin IP address range to enable Forescout RADIUS-based management of wireless clients, the Authentication Module version 1.1 or above with the RADIUS Plugin running is required.

### Networking Requirements

Network connectivity between the CounterACT 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:

<table>
<thead>
<tr>
<th>WLAN Device</th>
<th>Read/Write Setting Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>AeroHive Access Point</td>
<td>• SNMP read access to perform queries</td>
</tr>
<tr>
<td></td>
<td>• SSH or Telnet management (write) access to apply the WLAN Block action on wireless clients</td>
</tr>
<tr>
<td>Aruba Networks Controller</td>
<td>• SNMP or CLI (SSH or Telnet) read access to perform queries</td>
</tr>
<tr>
<td></td>
<td>• SSH or Telnet management (write) access to apply the WLAN management actions (WLAN Block and WLAN Role) on wireless clients</td>
</tr>
</tbody>
</table>
## Configure the Plugin

The plugin configuration lets you connect WLAN devices to CounterACT 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 CounterACT Appliances is then able to execute the following plugin activities:

- Connect to the WLAN devices

---

### WLAN Device | Read/Write Setting Configuration
---

**Cisco Controller**
- SNMP read access to perform queries
- To apply WLAN management actions (*WLAN Block* and *WLAN Role*) on connected wireless clients, the plugin uses any of the following methods:
  - CLI (SSH or Telnet) privilege mode write access
  - SNMP write access

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

**Cisco Aironet Access Point**
- SNMP or CLI (SSH or Telnet) read access to perform queries.
  - Plugin CLI read access is required for the plugin to obtain/report the IPv6 address information of connected IPv6 endpoints
- SSH or Telnet management (write) access to apply the *WLAN Block* action on wireless clients

**Meru Networks Controller**
- SNMP read access to perform queries
- SSH or Telnet management (write) access to apply the *WLAN Block* action on wireless clients

**Motorola Controller**
- SNMP or CLI (SSH or Telnet) read access to perform queries
- SSH or Telnet management (write) access to apply the *WLAN Block* action on wireless clients

**Ruckus Controller**
- SNMP read access to perform queries
- SSH or Telnet management (write) access to apply the *WLAN Block* action on wireless clients

**Xirrus Controller**
- SNMP read access to perform queries
- SNMP write access to apply the *WLAN Block* action on wireless clients

In addition, WLAN device typically needs to be configured to allow it to send SNMP traps to the Forescout platform.

For detailed information about specific, wireless vendor models and operating system versions that are validated for Wireless Plugin management, refer to the *WLAN Integrations* section in the *Forescout Network Devices Compatibility Matrix*. Access this matrix from the [Forescout Resources Page](#).

---
• 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. Select **Options** from the **Tools** menu at the Console.

3. Select **Add**. The Add Wireless Device wizard opens and displays the General pane.
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 CounterACT RADIUS server to provide RADIUS-based 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-based 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**

![Add wireless - Step 1](image)

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.

3. In the **Connecting Appliance** field, select a CounterACT 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. In the **optional Comment** field, enter descriptive text about the WLAN device and/or the configuration.

5. If either *Aruba Controller*, *Cisco Aironet Access Point* or *Motorola Controller* 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.

6. 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.

7. If either *an AeroHive Controller*, a *Meru 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.

8. 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.
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.

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 controller, a Cisco Aironet access point or a Motorola controller, 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.

   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:

   ![SNMP V3 Configuration](image)

   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 Forescout 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 controllers, Cisco Aironet access points and Motorola controllers, 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 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.
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.
   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** the RADIUS 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-based Management of Wireless Clients**

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

- Enable the RADIUS-based 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-based 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-based 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-based authentication and authorization, refer to the **Forescout RADIUS Plugin Configuration Guide**, version 4.3. 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 **Generic (RADIUS-based)**. The General pane then re-displays.
2. In the **Address** field, define an IP address range:
   
   a. Enter the starting IP address of the network segment. This entry can be any of the following:
      
      > An IPv4 address
      > An IPv6 address
   
   b. Append to the IP address a forward slash (/), followed by the subnet mask value. Valid values are 1 - 32.

   - The provided IP address network segment cannot overlap with that of any existing IP address range entry.

   - The provided combination of <IP address network segment> and subnet mask=32 is invalid if it conflicts with the IP address of an existing, managed WLAN device. For example, in the event of the provided combination 168.75.168.109/32 and the existing, managed WLAN device entry 168.75.168.109.

   - Individual managed WLAN devices can have an IP address that falls within an existing IP address range entry.

   - The identical SNMP Community information and the identical RADIUS Secret must be configured for all the multi-vendor access points that are deployed in the same IP address range. **The plugin does not validate for this requirement.**

3. In the **optional Comment** field, enter descriptive text.

4. Select **Next**. The SNMP pane opens.

**SNMP Configuration**

The purpose of this pane is to configure valid SNMP credentials so the Forescout 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.
   - When either **V1** or **V2** is selected, in the **Community** field enter a community relevant to your SNMP version selection. Continue with step 4.
   - When **V3** is selected, the following fields display:
     - **User** field
     - **Use Authentication** checkbox
     - **Authentication Protocol** field
     - **Password** field
     - **Confirm Password** field
     - **Use Privacy** checkbox
     - **Encryption Protocol** field
     - **Password** field
     - **Confirm Password** field

     Continue with step 3.

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

RADIUS Integration

Following the

- Command Line pane in the WLAN Device Management Configuration process flow

or the

- SNMP pane in the Enable Forescout RADIUS-based Management of Wireless Clients process flow,

Forescout the Add Wireless Device wizard opens the 802.1X pane. Configure the fields in the 802.1X pane if your CounterACT deployment is responsible for providing RADIUS-based authentication and authorization of detected, wireless clients attempting to connect to your organization’s network via its WLAN devices.

In the 802.1X pane:

1. In the RADIUS Secret as configured in the WLAN device field, enter the necessary RADIUS secret to allow communication between the Forescout RADIUS server and the WLAN device.

The identical RADIUS Secret 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.

a. Select Finish. The Wireless Pane re-displays containing the configured entry, either managed WLAN device or IP address range entry.

Review information about RADIUS and wireless integration before working with this capability.
To review RADIUS Plugin information:

1. In the Console, select Tools > Options > Modules. The Module pane opens.

2. In the Modules pane, select the Authentication module. The plugins, which are installed as part of the Forescout Authentication Module, display beneath the Authentication entry.

3. In the Module pane, select the RADIUS entry from the table listing.

4. Select Help.

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 CounterACT 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`

The property is defined per Appliance and the property's default value is 600 seconds (10 minutes). Run the following command to modify the value of this property (query frequency):

- `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:**

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

**Plugin Testing**

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 and Motorola 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**.
Troubleshooting

- **The device is not assigned to a CounterACT Appliance.** This can occur when you import predefined device settings. No CounterACT 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 CounterACT 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.
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.
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.
   b. 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 CounterACT 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.

![Image of Forescout Options and Wireless Pane]

**To export configurations:**

1. Select **Options** from the **Tools** menu at the Console.
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.
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.

### 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>)`  

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>`.

For information about the Forescout platform's **Failover Clustering** and the Wireless Plugin, see [Failover Clustering Support](#).
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, CounterACT backs-up and then exports the Wireless Plugin's configuration, if the CounterACT 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 CounterACT device <n> can only be canceled by that plugin/CounterACT 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 CounterACT 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.


8. Select the CounterACT 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 CounterACT 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, version 4.3. 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.
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.

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

   9. 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’s 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 CounterACT policies:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WLAN AP Location*</td>
<td>Property only supported for Aruba and Cisco controllers. Identifies the physical location of the access point to which the wireless client is connected.</td>
</tr>
<tr>
<td>WLAN AP Name</td>
<td>Identifies the name of the access point to which the wireless client is connected.</td>
</tr>
<tr>
<td>WLAN AP Name Change</td>
<td>Identifies that a change in value occurred in the WLAN AP Name property.</td>
</tr>
</tbody>
</table>
| WLAN Association Status    | Property only supported for Aruba 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:  
  - Unknown  
  - Blacklisted (WLAN Block action is applied)  
  - Disassociated (wireless client is disconnected/offline)  
  Values vary by wireless equipment vendor. Refer to the vendor-specific configuration guides for this plugin and vendor documentation. |
<p>| WLAN Association Status Change | Identifies that a change in value occurred in the WLAN Association Status property.                                                              |
| WLAN Authentication Method | 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 Read Connection Method to be SNMP. |
| WLAN Authentication Method Change | Identifies that a change in value occurred in the WLAN Authentication Method property.                                                                  |
| WLAN BSSID*                | Property only supported for Aruba and Cisco controllers. Identifies the BSSID of the access point to which the wireless client is connected.       |
| WLAN BSSID Change          | Identifies that a change in value occurred in the WLAN BSSID property.                                                                            |
| WLAN Client Role*          | Property only supported for Aruba and Cisco controllers. Identifies the role assigned by the access point to the wireless client.                   |
| WLAN Client Role Change    | Identifies that a change in value occurred in the WLAN Client Role property.                                                                      |
| WLAN Client User Agent*    | Property only supported for Aruba mobility controllers running ArubaOS version 6.0.1 or later. Identifies the user agent running on the wireless client. |</p>
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WLAN Client User Agent Change</td>
<td>Identifies that a change in value occurred in the WLAN Client User Agent property.</td>
</tr>
<tr>
<td>WLAN Client Username*</td>
<td>Property only supported for Aruba and Cisco controllers. Identifies the username employed by the wireless client to authenticate with the access point.</td>
</tr>
<tr>
<td>WLAN Client Username Change</td>
<td>Identifies that a change in value occurred in the WLAN Client Username property.</td>
</tr>
<tr>
<td>WLAN Client VLAN*</td>
<td>Property only supported for Aruba and Cisco controllers. Identifies the VLAN to which the wireless client is connected.</td>
</tr>
<tr>
<td>WLAN Client VLAN Change</td>
<td>Identifies that a change in value occurred in the WLAN Client VLAN property.</td>
</tr>
<tr>
<td>WLAN Client Connectivity Status</td>
<td>Identifies whether the wireless client is connected to an access point.</td>
</tr>
<tr>
<td>WLAN Client Connectivity Status Change</td>
<td>Identifies that a change in value occurred in the WLAN Client Connectivity Status property.</td>
</tr>
<tr>
<td>WLAN Device IP/FQDN</td>
<td>Identifies either the IP address or the fully qualified domain name of the WLAN device to which the wireless client is connected.</td>
</tr>
<tr>
<td>WLAN Device IP/FQDN Change</td>
<td>Identifies that a change in value occurred in the WLAN Device IP/FQDN property.</td>
</tr>
<tr>
<td>WLAN Device Software</td>
<td>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.</td>
</tr>
<tr>
<td>WLAN Device Vendor</td>
<td>Identifies the vendor of the plugin-managed WLAN device to which the wireless client is connected.</td>
</tr>
<tr>
<td>WLAN Detected Client Type*</td>
<td>Property only supported for Aruba mobility controllers running ArubaOS version 6.0.1 or later. Identifies the operating system of the wireless client.</td>
</tr>
<tr>
<td>WLAN Detected Client Type Change</td>
<td>Identifies that a change in value occurred in the WLAN Detected Client Type property.</td>
</tr>
<tr>
<td>WLAN SSID</td>
<td>Identifies the SSID (service set identifier) to which the wireless client is connected.</td>
</tr>
<tr>
<td>WLAN SSID Change</td>
<td>Identifies that a change in value occurred in the WLAN SSID property.</td>
</tr>
</tbody>
</table>

* For the Aruba (autonomous AP) Instant model and for the 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

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:

- *Wireless Address Learned*
- *Wireless Address Removed*

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 Forescout platform first detects an SNMP trap for them.

WLAN Device Properties

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

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>WLAN Device Software</strong></td>
<td>Identifies the software release that is running on a:</td>
</tr>
<tr>
<td></td>
<td>- Plugin-managed WLAN device</td>
</tr>
<tr>
<td></td>
<td>- Lightweight AP of vendors Aruba and Cisco</td>
</tr>
<tr>
<td><strong>WLAN Device Vendor</strong></td>
<td>Identifies the vendor of a:</td>
</tr>
<tr>
<td></td>
<td>- Plugin-managed WLAN device</td>
</tr>
<tr>
<td></td>
<td>- Lightweight AP of vendors Aruba, Cisco and Ruckus</td>
</tr>
<tr>
<td><strong>WLAN Device Vendor and Type</strong></td>
<td>The vendor and the device type of a managed WLAN device or a detected lightweight access point. Examples: <em>Cisco Controller</em> or <em>Cisco Lightweight AP</em>.*</td>
</tr>
<tr>
<td></td>
<td>Currently, this property is only available for use in/resolved by a policy that is created using a <strong>Vulnerability and Response</strong> (VR) policy template.</td>
</tr>
<tr>
<td><strong>WLAN Managing Controller</strong></td>
<td>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.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>WLAN Managing Controller Change</td>
<td>Identifies that a change in value occurred in the <strong>WLAN Managing Controller</strong> property.</td>
</tr>
</tbody>
</table>
| WLAN Network Function                        | The plugin resolves this property for the WLAN devices of all supported WLAN vendors with any of the following values:  
  - **Controller** - the plugin-managed WLAN device is determined to be a WLAN controller  
  - **Autonomous AP** - the plugin-managed WLAN device is determined to be an autonomous access point.  
  - **Lightweight AP** - the device is determined to be a lightweight access point that is associated with (managed by) a plugin-managed WLAN controller  
  - **Other** - the device is determined to be a connected wireless client. |

**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:

<table>
<thead>
<tr>
<th>Admission Event</th>
<th>Description</th>
</tr>
</thead>
</table>
| WLAN lightweight AP connected | 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. |
| Wireless Host Connected     | 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 is also running on your CounterACT 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**

(Flexx licensing) To use these actions, ensure that you have a valid Forescout eyeControl license. 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 CounterACT Appliance
  - and on all WLAN devices being managed by the CounterACT 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 wireless controllers, in order for the plugin to apply this action.
The *WLAN Role* action is **supported** for use on the following WLAN devices:

- Aruba controllers, excluding Aruba Instant Access Points
- Cisco controllers, excluding Cisco controllers that run the IOS-XE operating system

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

- For Aruba controllers, the *WLAN Role* action assigns a *User Role*.
- For Cisco controllers, the *WLAN Role* action assigns an *Interface*.

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 wireless 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:

<table>
<thead>
<tr>
<th>Action Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Role Name</strong></td>
<td>The name of the role, as defined on the WLAN device.</td>
</tr>
<tr>
<td></td>
<td>- For Aruba controllers, this is the name of a <em>User Role</em>.</td>
</tr>
<tr>
<td></td>
<td>- For Cisco controllers, this is the name of an <em>Interface</em>.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td><em>(Optional)</em> A description of the role, or the situation that prompted role assignment. This comment is stored in the controller's log.</td>
</tr>
<tr>
<td><strong>Force re-authentication after the role is applied</strong></td>
<td>When this option is selected, existing wireless client WLAN sessions are disconnected after role assignment. This generates <code>disconnect</code> and <code>reconnect</code> traps when the wireless client reconnects. The Forescout platform authenticates the wireless client with its new role.</td>
</tr>
<tr>
<td></td>
<td>- VoIP and media sessions are dropped when the wireless client is disconnected.</td>
</tr>
</tbody>
</table>
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 Forescout 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 Controllers](#)
- [Using the WLAN Role Action with Cisco Controllers](#)

### Using the WLAN Role Action with Aruba 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.

### 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 an 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 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, run the following command:

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

To re-enable the default **Any WLAN Connection** option for an Appliance, run the following command:

```
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 Forescout 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 Forescout 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 Forescout 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 Forescout 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.

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 wireless clients should be monitored by a CounterACT Appliance.
To create the policy:

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

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.

![Main Rule Page](image1)

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.

![Condition Dialog](image2)

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 Dialog Box]
   
   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’s 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. Navigate to the Wireless entries. The wireless Asset Inventory view is 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.
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
- 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

Access documentation downloads from the Forescout Resources Page, or 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 Portal

> Software downloads are also available from these portals.

**To identify your licensing mode:**

- From the Console, select Help > About Forescout.

Forescout Resources Page

The Forescout Resources Page provides links to the full range of technical documentation.
To access the Forescout Resources Page:

Product Updates Portal
The Product Updates Portal provides links to Forescout version releases, Base and Content Modules, and eyeExtend products, as well as related documentation. The portal also provides a variety of 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 Portal
The Downloads page on the Forescout Customer Portal provides links to purchased Forescout version releases, Base and Content Modules, and eyeExtend products, as well as related documentation. Software and related documentation only appear on the Downloads page if you have a license entitlement for the software.

To access documentation on the Forescout Customer 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.

⚠️ If your deployment is using Flexx Licensing Mode, you may not have received credentials to access this portal.

To access the Documentation Portal:
- Go to https://updates.forescout.com/support/files/counteract/docs_portal/ and use your customer support credentials to log in.

Forescout Help Tools
Access information directly from the Console.

Console Help Buttons
Use context-sensitive Help buttons to access information about tasks and topics quickly.

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

Plugin Help Files
- After installing the plugin, select Tools > Options > Modules, select the plugin, and then select Help.
Online Documentation

- Select **Online Documentation** from the **Help** menu to access either the **Forescout Resources Page** (Flexx licensing) or the **Documentation Portal** (Per-Appliance licensing).